Introduction to Logging with the ELK Stack

Amy Ghate
Solutions Architect

logs

+

metrics

+

apm

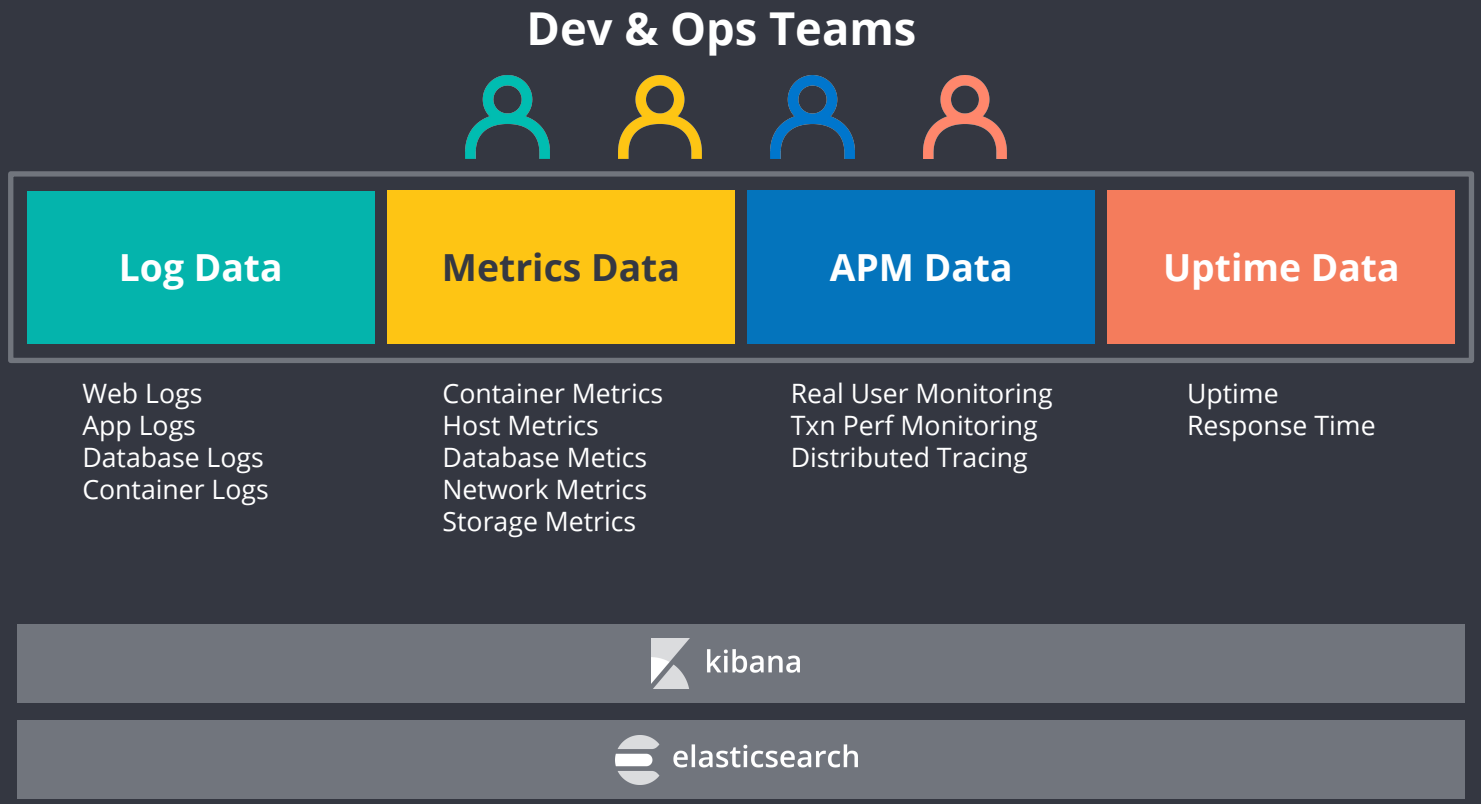
=

ObservaBLT

Observability

elastic

Elastic Approach to Observability



Agenda

Things we're going to cover

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security

Agenda

Challenges with log analytics

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security

Logs for one host or app

This is fairly straightforward

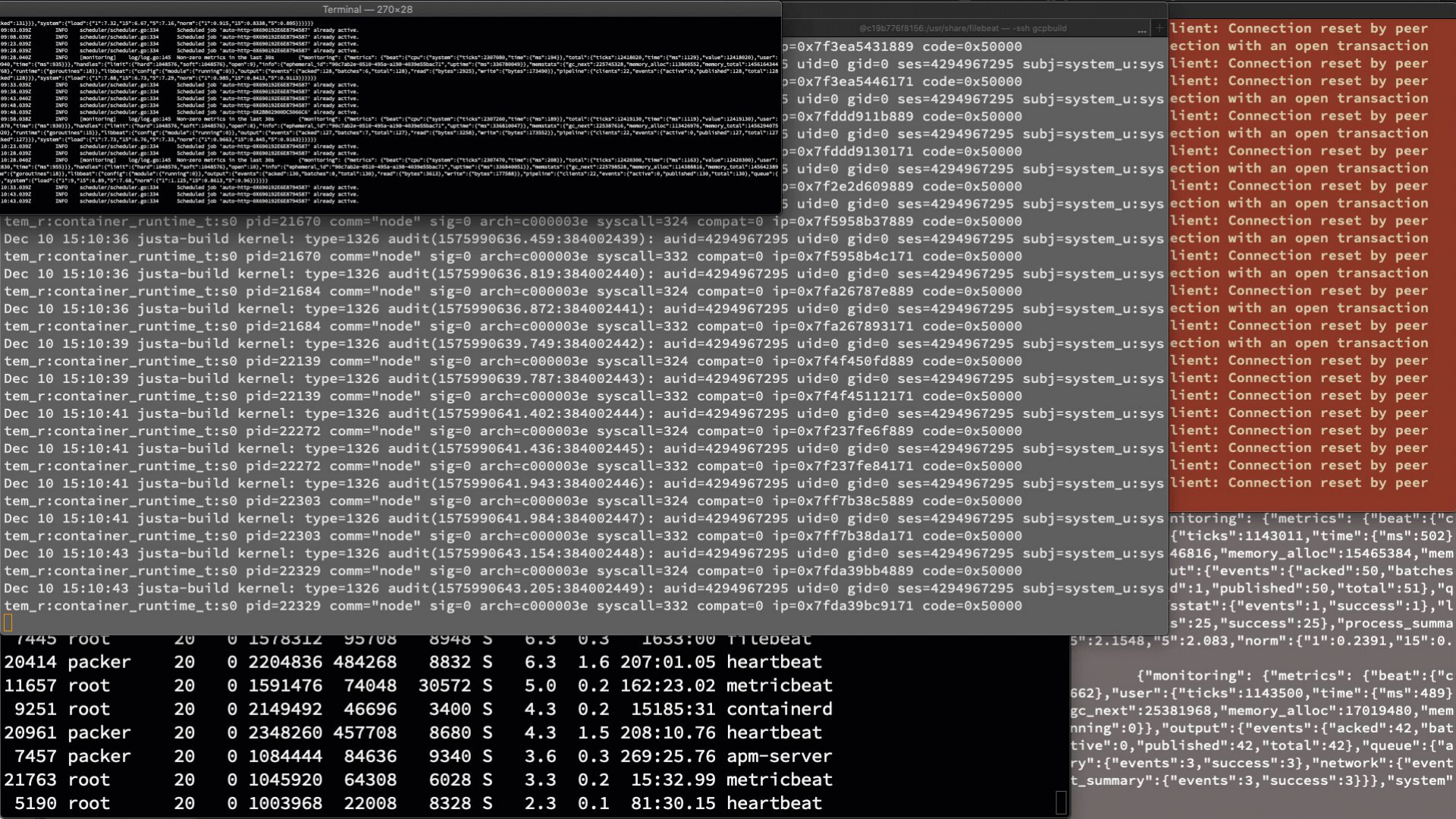
Terminal — 100×19

```
$ > tail -f /var/log/messages

Dec 10 14:05:30 justa-build kernel: type=1326 audit(1575986730.517:383998660): auid=4294967295
uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17069 comm="node"
sig=0 arch=c000003e syscall=324 compat=0 ip=0x7efe9c254889 code=0x50000
Dec 10 14:05:30 justa-build kernel: type=1326 audit(1575986730.551:383998661): auid=4294967295
uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17069 comm="node"
sig=0 arch=c000003e syscall=332 compat=0 ip=0x7efe9c269171 code=0x50000
Dec 10 14:05:33 justa-build kernel: type=1326 audit(1575986733.110:383998662): auid=4294967295
uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17179 comm="node"
sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fee1cf0f889 code=0x50000
Dec 10 14:05:33 justa-build kernel: type=1326 audit(1575986733.150:383998663): auid=4294967295
uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17179 comm="node"
sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fee1cf24171 code=0x50000
Dec 10 14:05:35 justa-build kernel: type=1326 audit(1575986735.155:383998664): auid=4294967295
uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17367 comm="node"
sig=0 arch=c000003e syscall=324 compat=0 ip=0x7ffb3b7bf889 code=0x50000
Dec 10 14:05:35 justa-build kernel: type=1326 audit(1575986735.194:383998665): auid=4294967295
uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17367 comm="node"
```

Interacting with logs

Built-in tools for log viewing

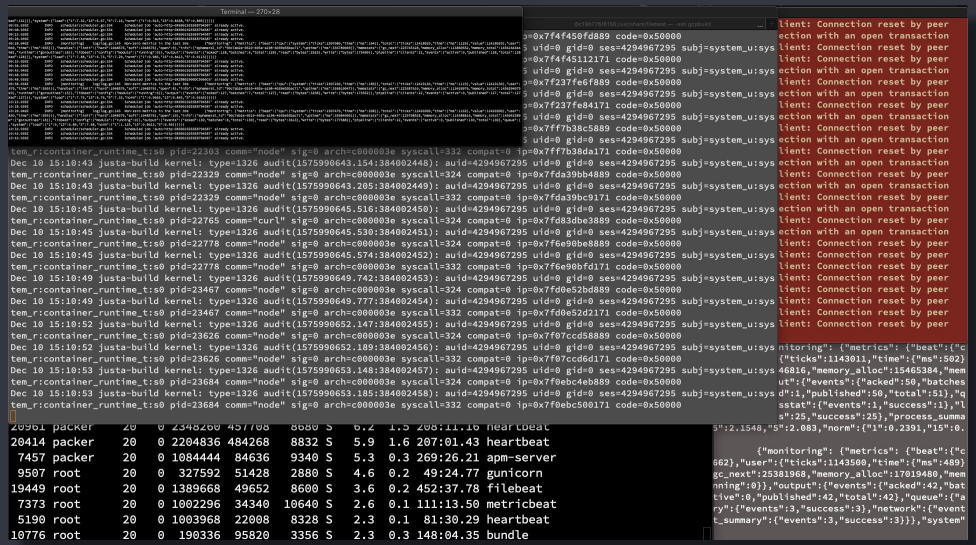
- grep
- tail
- cat / less / more / type
- sed / awk / perl
- vim / notepad / event viewer
- clever combinations of the above


Terminal — 270×28
@c19b776f8156:/usr/share/filebeat — -ssh gcpbuild
Dec 10 15:10:36 justa-build kernel: type=1326 audit(1575990636.459:384002439): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=21670 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f5958b37889 code=0x50000
Dec 10 15:10:36 justa-build kernel: type=1326 audit(1575990636.459:384002439): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=21670 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f5958b4c171 code=0x50000
Dec 10 15:10:36 justa-build kernel: type=1326 audit(1575990636.819:384002440): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=21684 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fa26787e889 code=0x50000
Dec 10 15:10:36 justa-build kernel: type=1326 audit(1575990636.872:384002441): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=21684 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fa267893171 code=0x50000
Dec 10 15:10:39 justa-build kernel: type=1326 audit(1575990639.749:384002442): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22139 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f4f450fd889 code=0x50000
Dec 10 15:10:39 justa-build kernel: type=1326 audit(1575990639.787:384002443): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22139 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f4f45112171 code=0x50000
Dec 10 15:10:41 justa-build kernel: type=1326 audit(1575990641.402:384002444): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22272 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f237fe6f889 code=0x50000
Dec 10 15:10:41 justa-build kernel: type=1326 audit(1575990641.436:384002445): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22272 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f237fe84171 code=0x50000
Dec 10 15:10:41 justa-build kernel: type=1326 audit(1575990641.943:384002446): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22303 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7ff7b38c5889 code=0x50000
Dec 10 15:10:41 justa-build kernel: type=1326 audit(1575990641.984:384002447): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22303 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7ff7b38da171 code=0x50000
Dec 10 15:10:43 justa-build kernel: type=1326 audit(1575990643.154:384002448): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22329 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fda39bb4889 code=0x50000
Dec 10 15:10:43 justa-build kernel: type=1326 audit(1575990643.205:384002449): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22329 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fda39bc9171 code=0x50000
7445 root 20 0 1578312 95708 8948 S 6.3 0.3 1633:00 filebeat
20414 packer 20 0 2204836 484268 8832 S 6.3 1.6 207:01.05 heartbeat
11657 root 20 0 1591476 74048 30572 S 5.0 0.2 162:23.02 metricbeat
9251 root 20 0 2149492 46696 3400 S 4.3 0.2 15185:31 containerd
20961 packer 20 0 2348260 457708 8680 S 4.3 1.5 208:10.76 heartbeat
7457 packer 20 0 1084444 84636 9340 S 3.6 0.3 269:25.76 apm-server
21763 root 20 0 1045920 64308 6028 S 3.3 0.2 15:32.99 metricbeat
5190 root 20 0 1003968 22008 8328 S 2.3 0.1 81:30.15 heartbeat

Immediate needs for log analytics

What's missing from the previous desktop

- Easy setup for a variety of sources
- Correlating and cross referencing
- Searching, filtering, and highlighting
- Visualize
- Anomaly detection and alerting
- Flexible retention



elastic

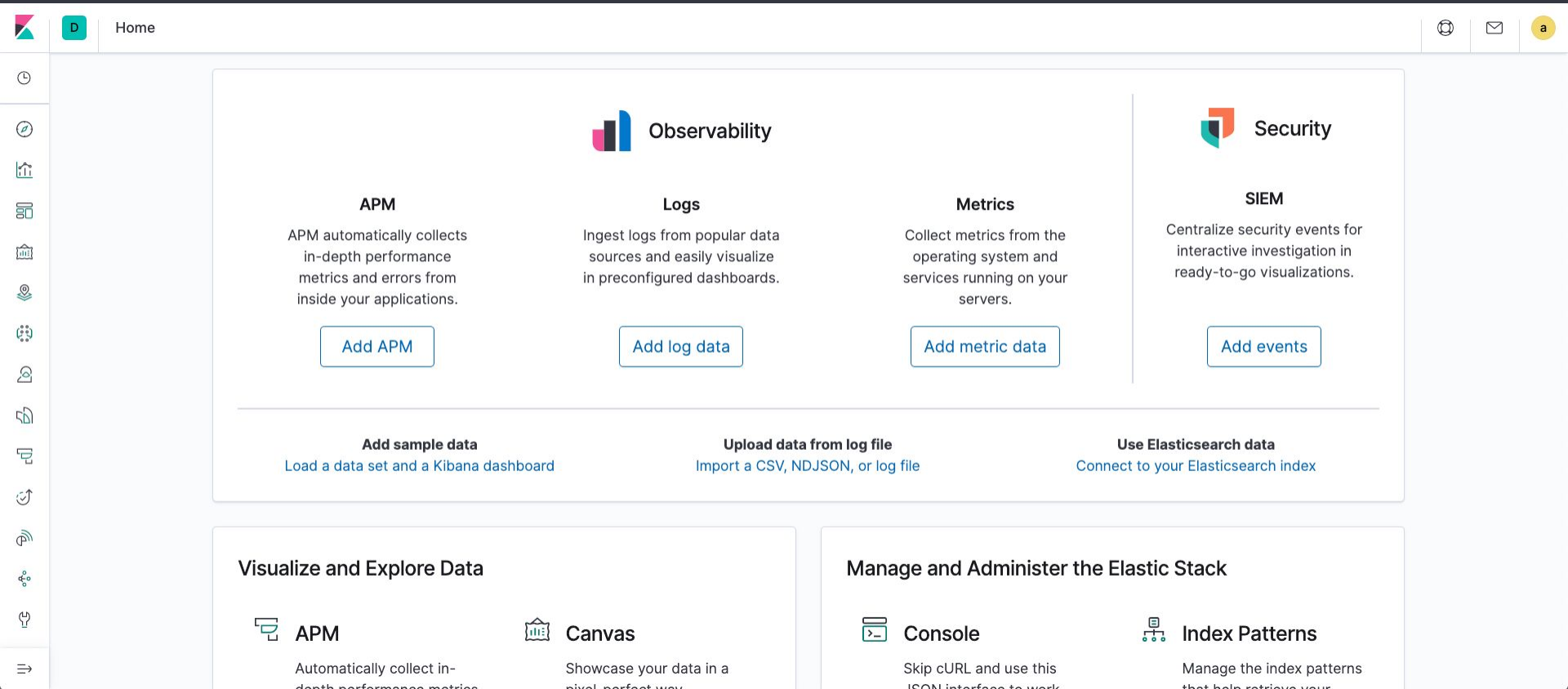
Agenda

Things we're going to cover

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security

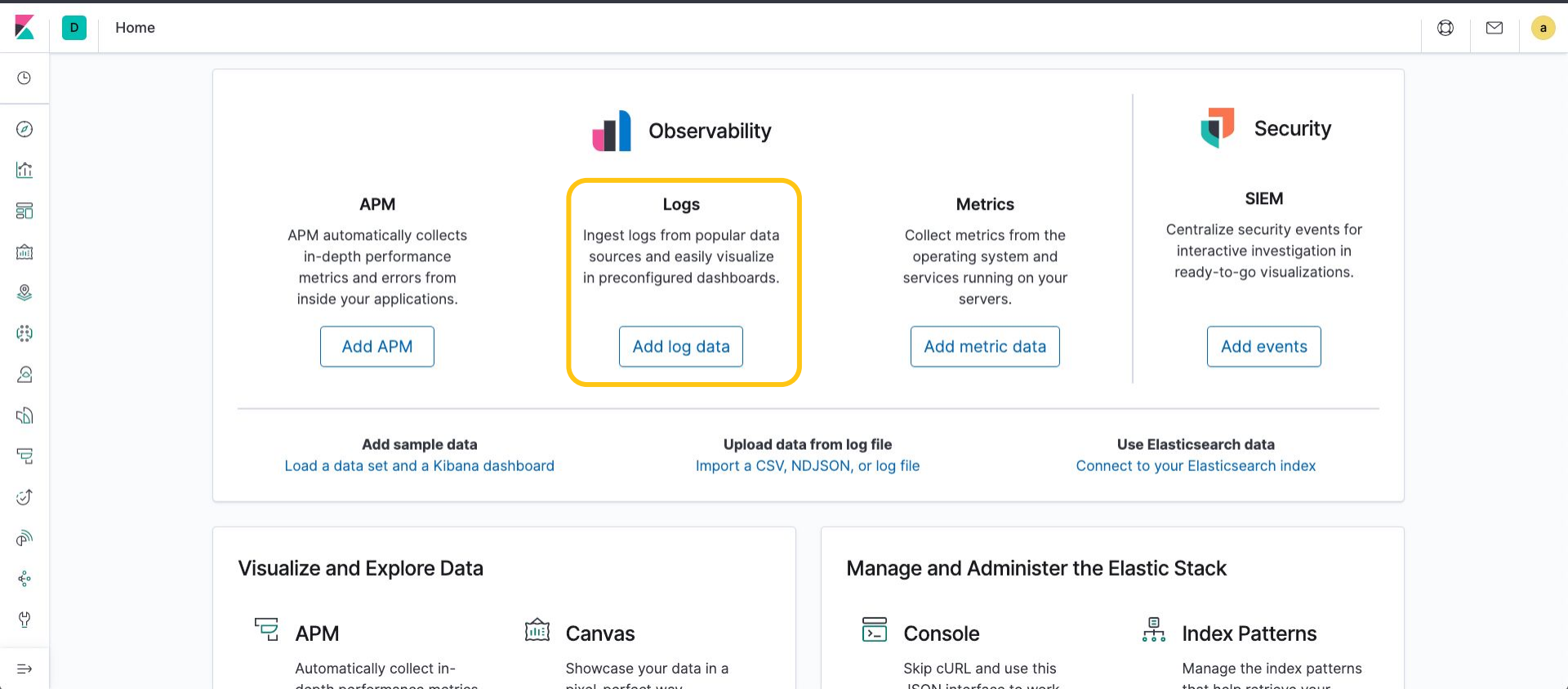
We're running in Elastic Cloud

Works the same in the cloud or running the default distribution



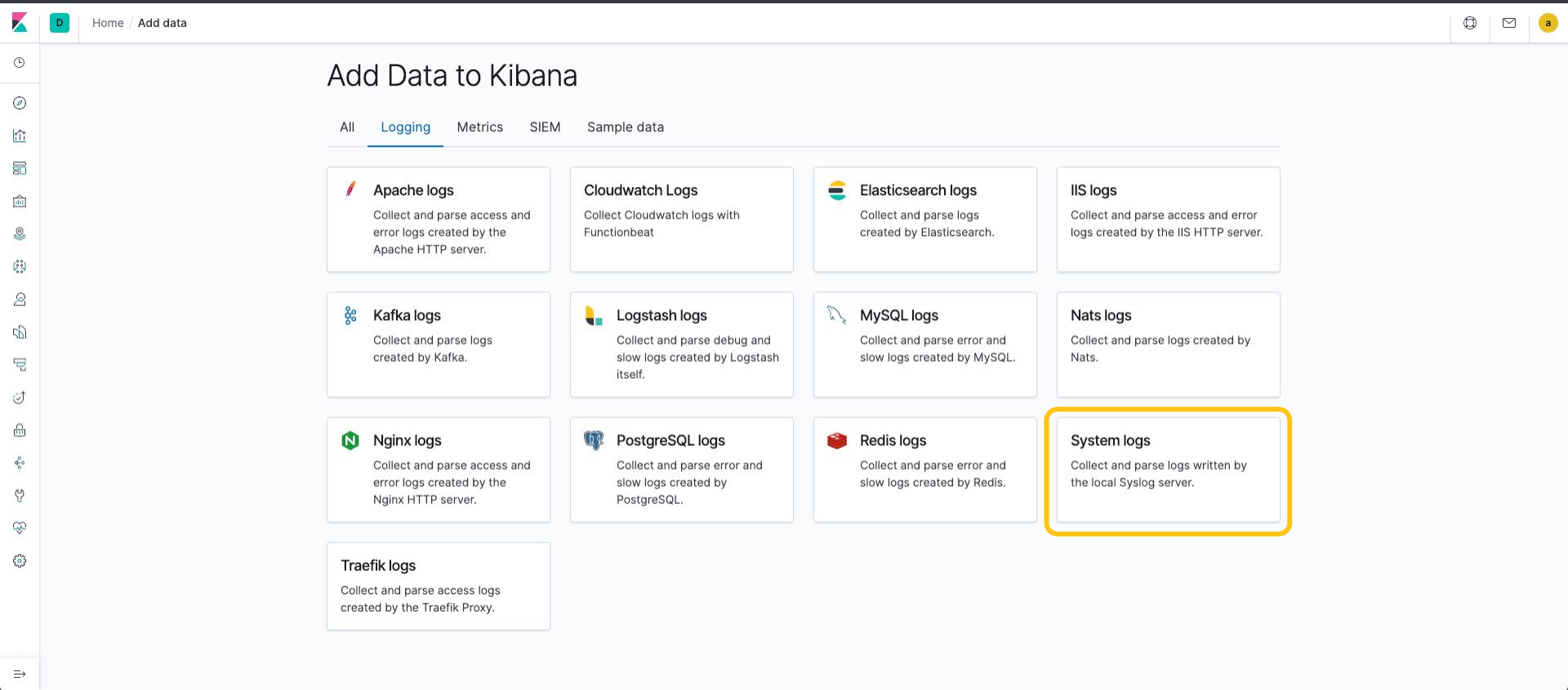
Click on the Logging Button

Works the same in the cloud or running the default distribution



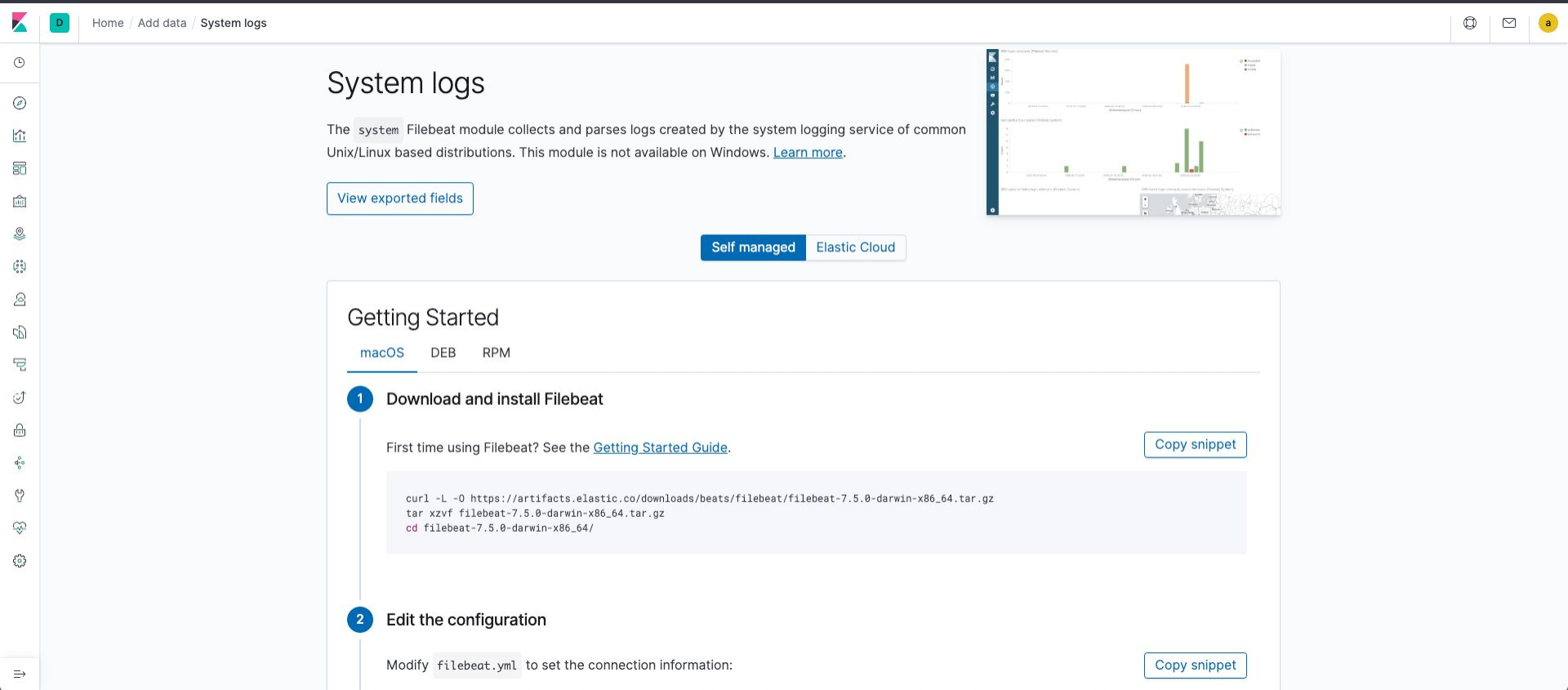
Many choices

We're going to ingest the **System logs**



Detailed instructions

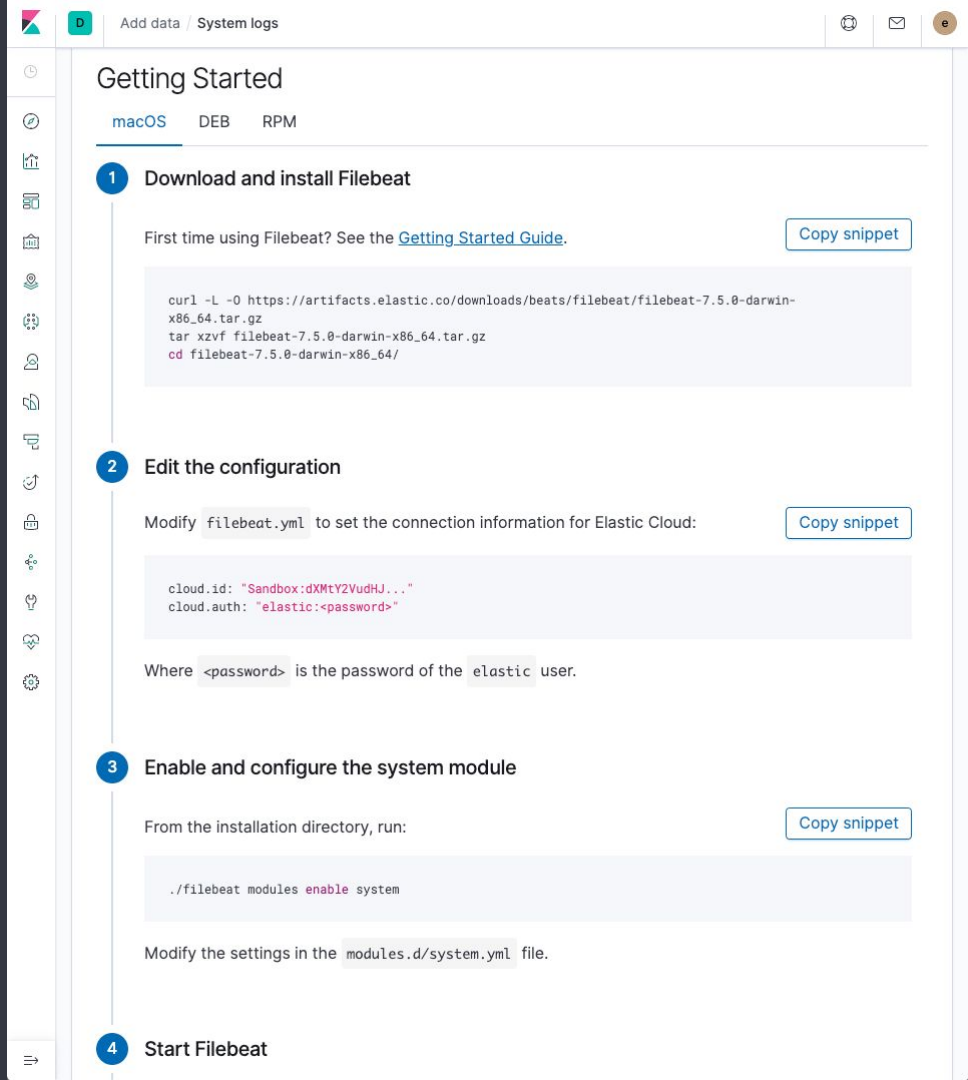
Context-aware instructions for cloud or on-prem installs



Getting Started

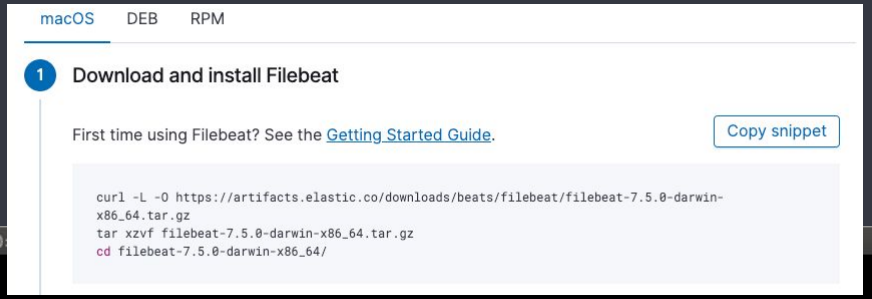
Cloud or on-prem installs

- **Download and install Filebeat**
- Edit the configuration
- Enable and configure the system module
- Start Filebeat
- Check out the dashboard!



Steps

Download and install Filebeat

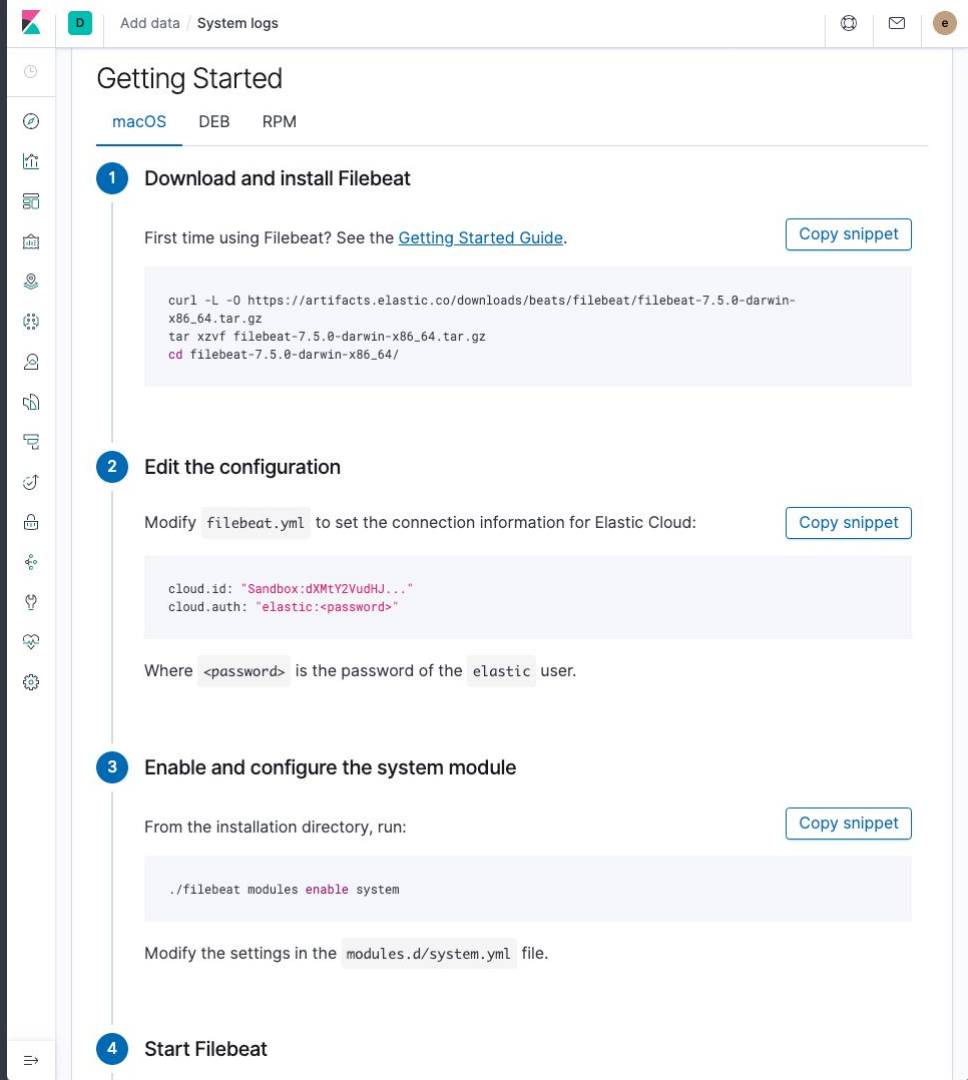



```
$ >curl -LO --silent \
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-x86_64.tar.gz

$ >tar xzvf filebeat-7.5.0-darwin-x86_64.tar.gz
$ >cd filebeat-7.5.0-darwin-x86_64
$ >ls -1
LICENSE.txt
NOTICE.txt
README.md
fields.yml
filebeat*
filebeat.reference.yml
filebeat.yml
kibana/
module/
modules.d/
```

Steps

Edit the configuration

- Download and install Filebeat
- **Edit the configuration**
- Enable and configure the system module
- Start Filebeat
- Check out the dashboard!



Configuration

Cloud aware - using superuser

2 Edit the configuration

Modify `filebeat.yml` to set the connection information for Elastic Cloud: Copy snippet

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

```
cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "elastic:<password>"
```

Where `<password>` is the password of the `elastic` user.

Edit the configuration

Copy the snippet, paste in the password

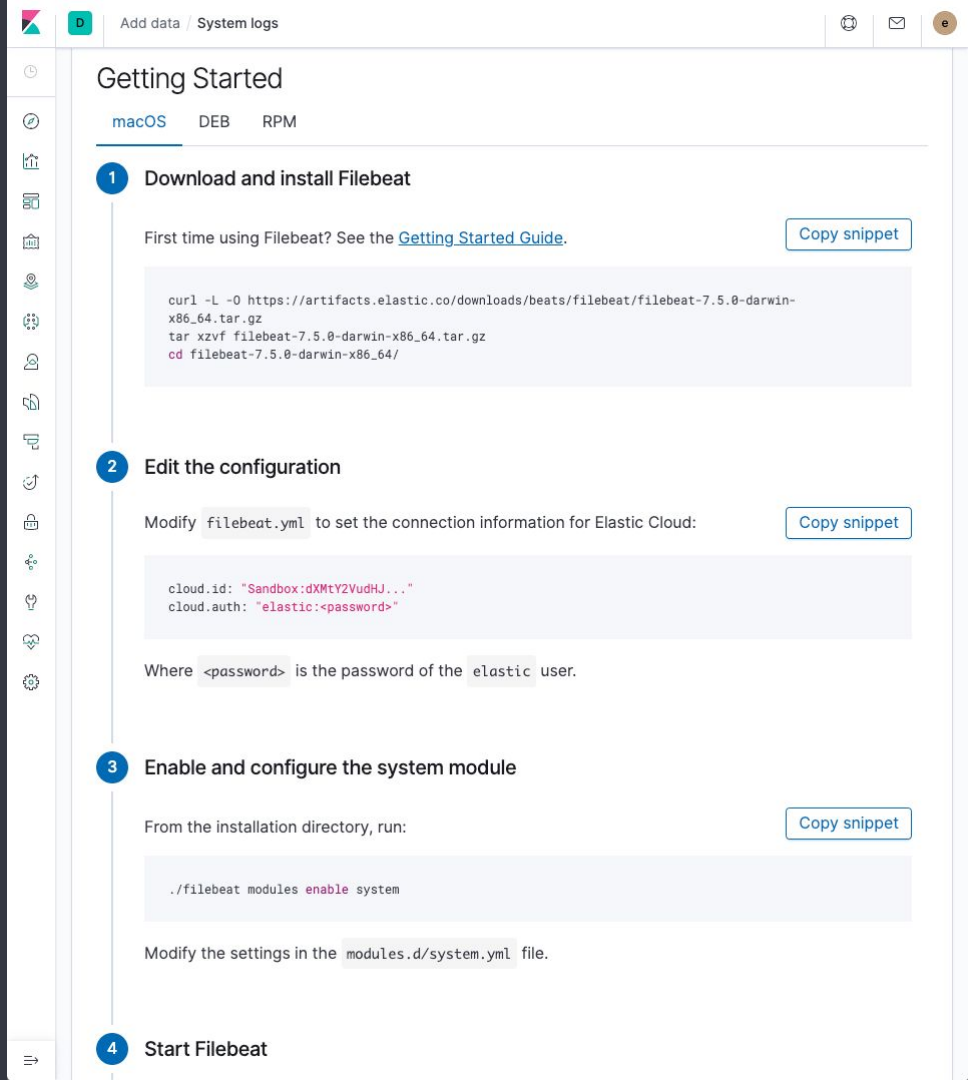
Terminal — 100×19

```
#============================ Elastic Cloud ================================
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "elastic:long-random-password" # because we are using Elastic Cloud

output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]          ← If we were not using Elastic Cloud
  #username: "elastic"               ←
  #password: "long-random-password"  ←


-UU-:----F1  filebeat.yml                (YAML)
```

Steps

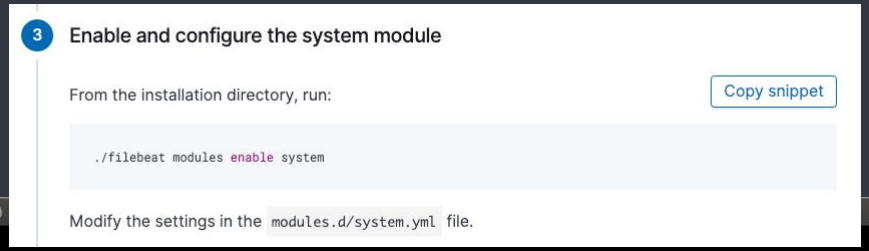
Set up the system module

- Download and install Filebeat
- Edit the configuration
- **Enable and configure the system module**
- Start Filebeat
- Check out the dashboard!



Enable the system module

Again, just copy and paste the snippet

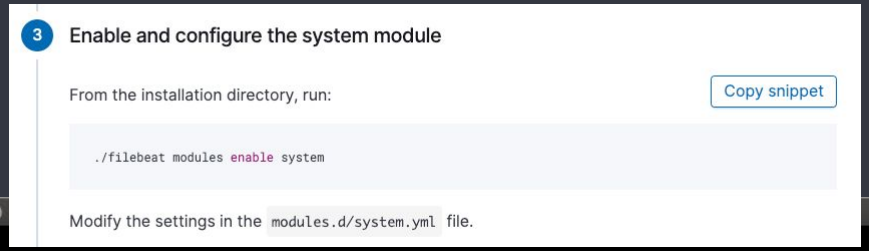


Terminal — 100×19

```
$ >./filebeat modules enable system
```

Enable the system module

Again, just copy and paste the snippet

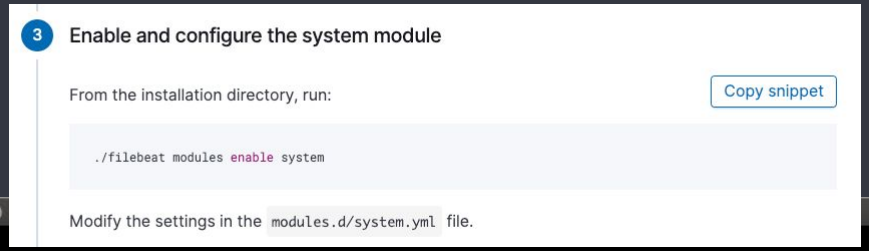


Terminal — 100×19

```
$ >./filebeat modules enable system
Enabled system
```

Enable the system module

Check your work

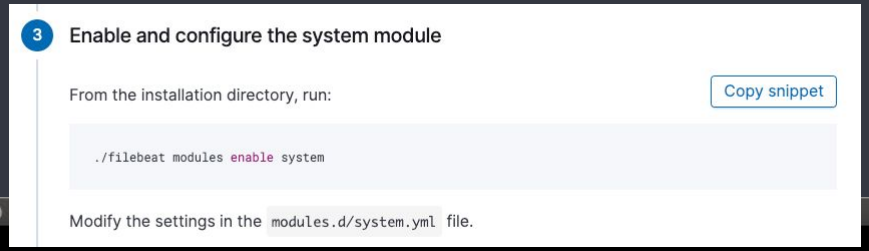


Terminal — 100×19

```
$ >./filebeat modules enable system
Enabled system

# Can also verify
```

Enable the system module

Check your work

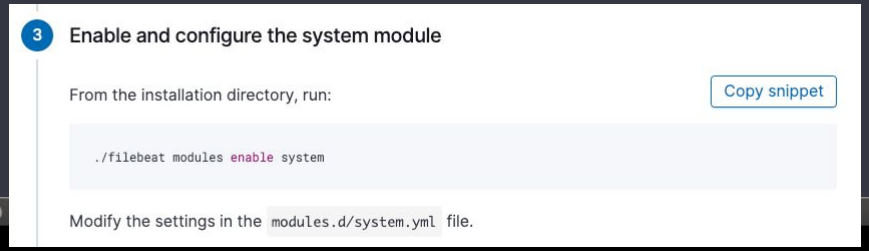


Terminal — 100×19

```
$ >./filebeat modules enable system
Enabled system

# Can also verify

$ >./filebeat modules list
```

Enable the system module

All good



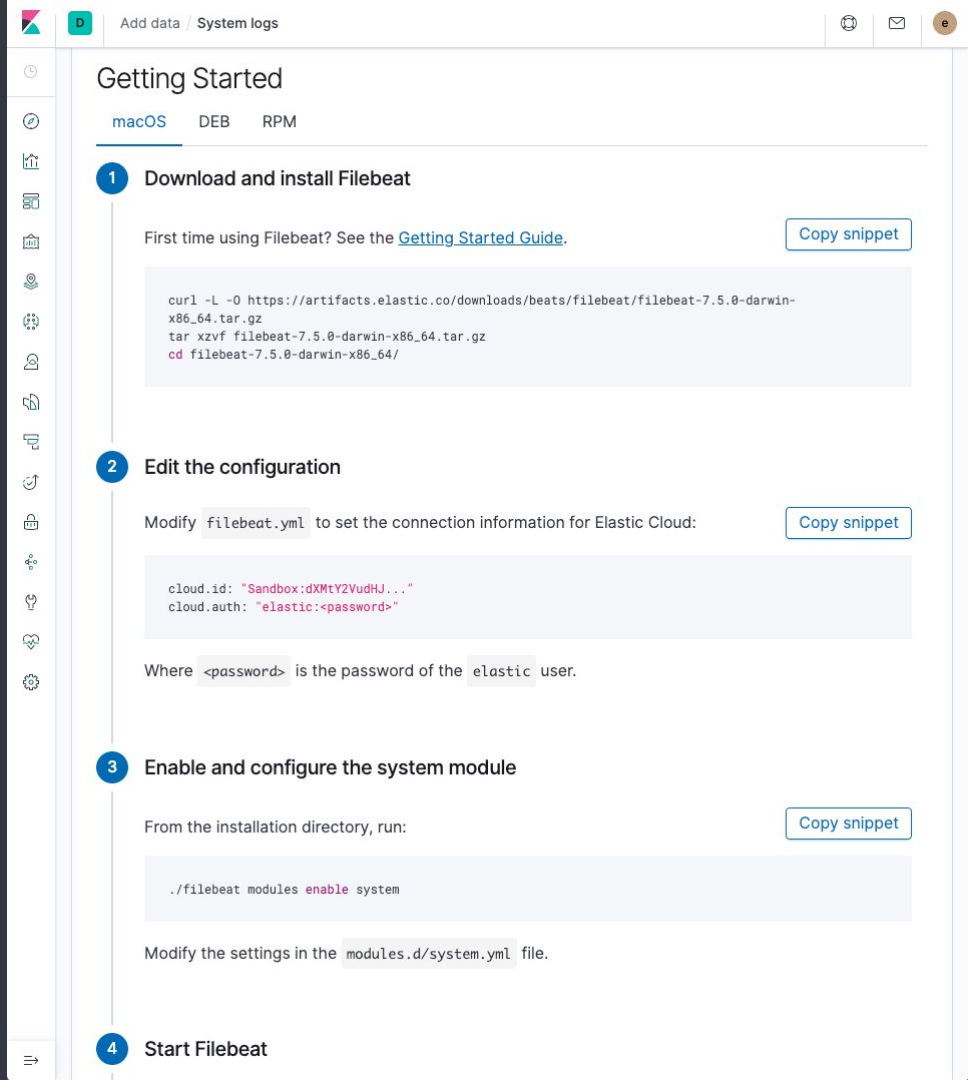
Terminal — 100×19

```
$ >./filebeat modules enable system
Enabled system

# Can also verify

$ >./filebeat modules list
Enabled:
system

Disabled:
apache
auditd
aws
azure
(...)
```

Steps

Start Filebeat

- Download and install Filebeat
- Edit the configuration
- Enable and configure the system module
- **Start Filebeat**
- Check out the dashboard!



And start it up!

Startup steps

Terminal — 100×19

```
$ >
```

4 Start Filebeat

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

Copy snippet

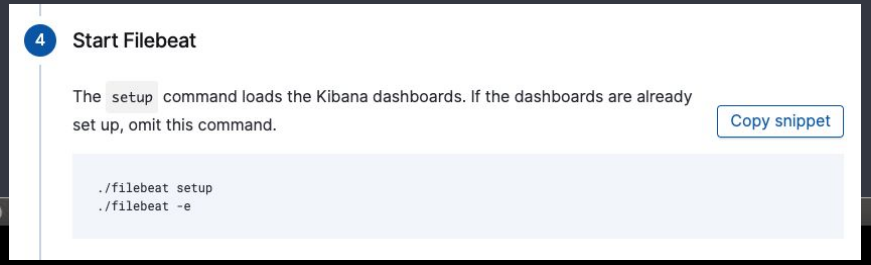
```
./filebeat setup
./filebeat -e
```

First run the setup process

Setup preps dashboards and indices

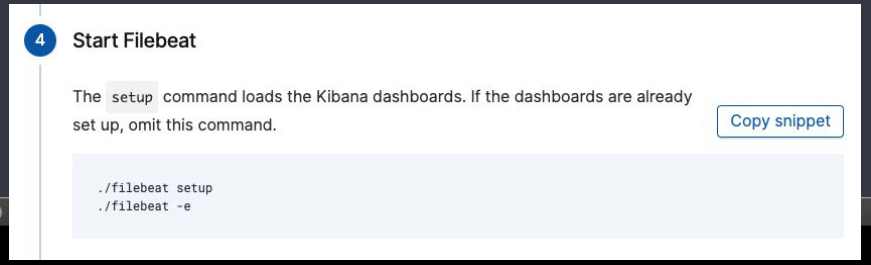
Terminal — 100×19

```
$ >./filebeat setup
```



First run the setup process

Setup preps dashboards and indices

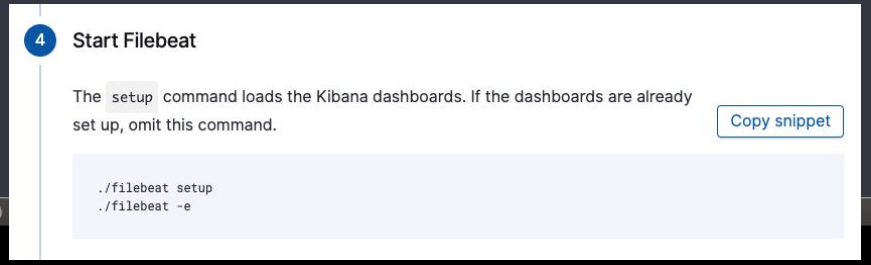


Terminal — 100×19

```
$ >./filebeat setup
Index setup finished.
```

First run the setup process

Setup preps dashboards and indices

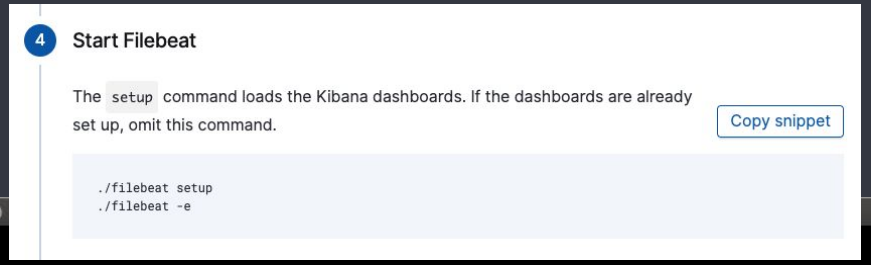


Terminal — 100×19

```
$ >./filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
```

First run the setup process

Setup preps dashboards and indices

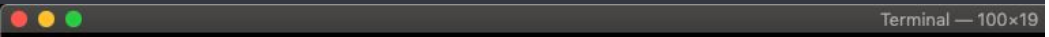


Terminal — 100×19

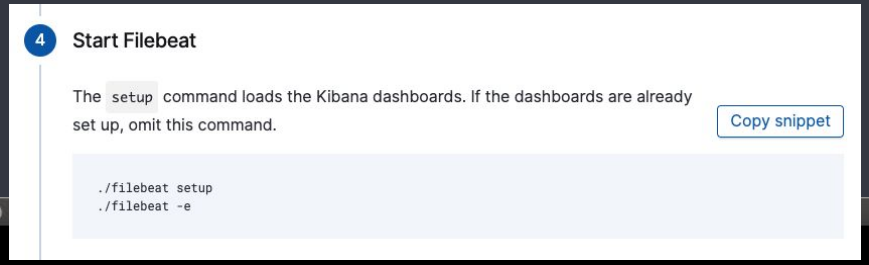
```
$ >./filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
```

Finally, start it!

-e tells it to send messages to console

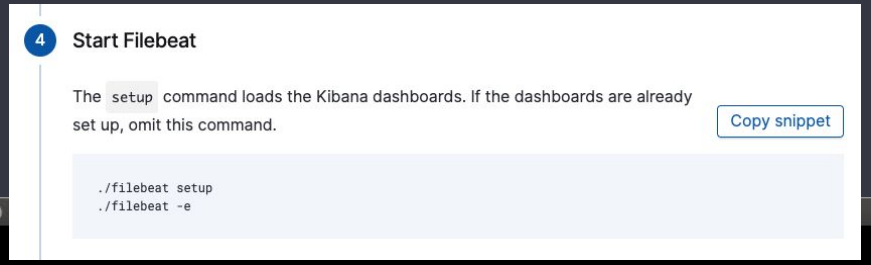



```
$ >./filebeat -e
```



Finally, start it!

-e tells it to send messages to console



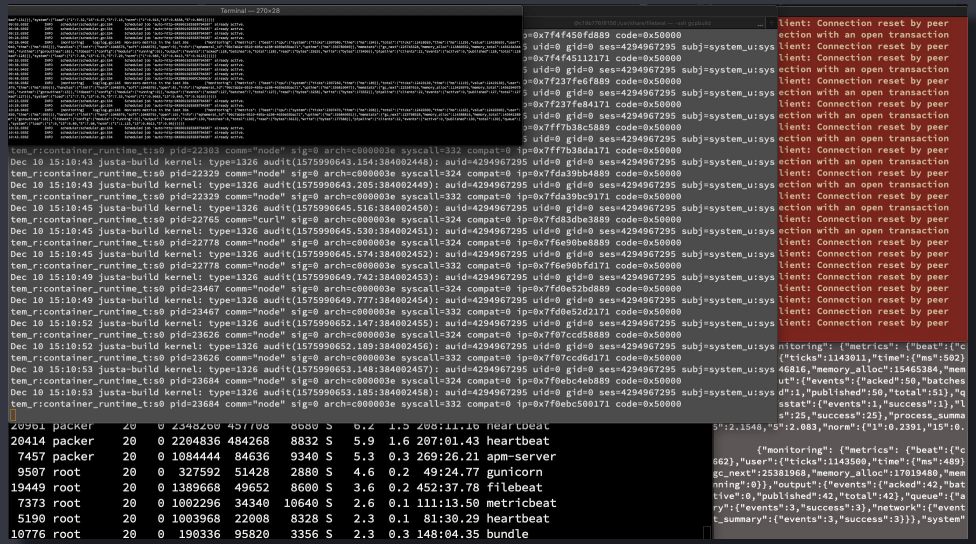
Terminal — 100×19

```
$ >./filebeat -e

2019-12-09T18:02:42.500Z INFO instance/beat.go:610Home path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64] Config path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64] Data path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64/data] Logs path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64/logs]
2019-12-09T18:02:42.501Z INFO instance/beat.go:618Beat ID: 04e276d0-79bd-40e3-9c83-3cdc4a64f791
2019-12-09T18:02:42.513Z INFO add_cloud_metadata/add_cloud_metadata.go:93   add_cloud_metadata:
hosting provider type detected as gcp,
metadata={"availability_zone":"us-east1-b","instance":{"id":"8271592631829869565","name":"user-smi
th-build"},"machine":{"type":"n1-standard-8"},"project":{"id":"elastic-product-marketing"},"provid
er":"gcp"}
2019-12-09T18:02:42.564Z INFO [seccomp] seccomp/seccomp.go:124   Syscall filter successfully
installed
(...)
```

Essential needs for log analytics

Recall the earlier list

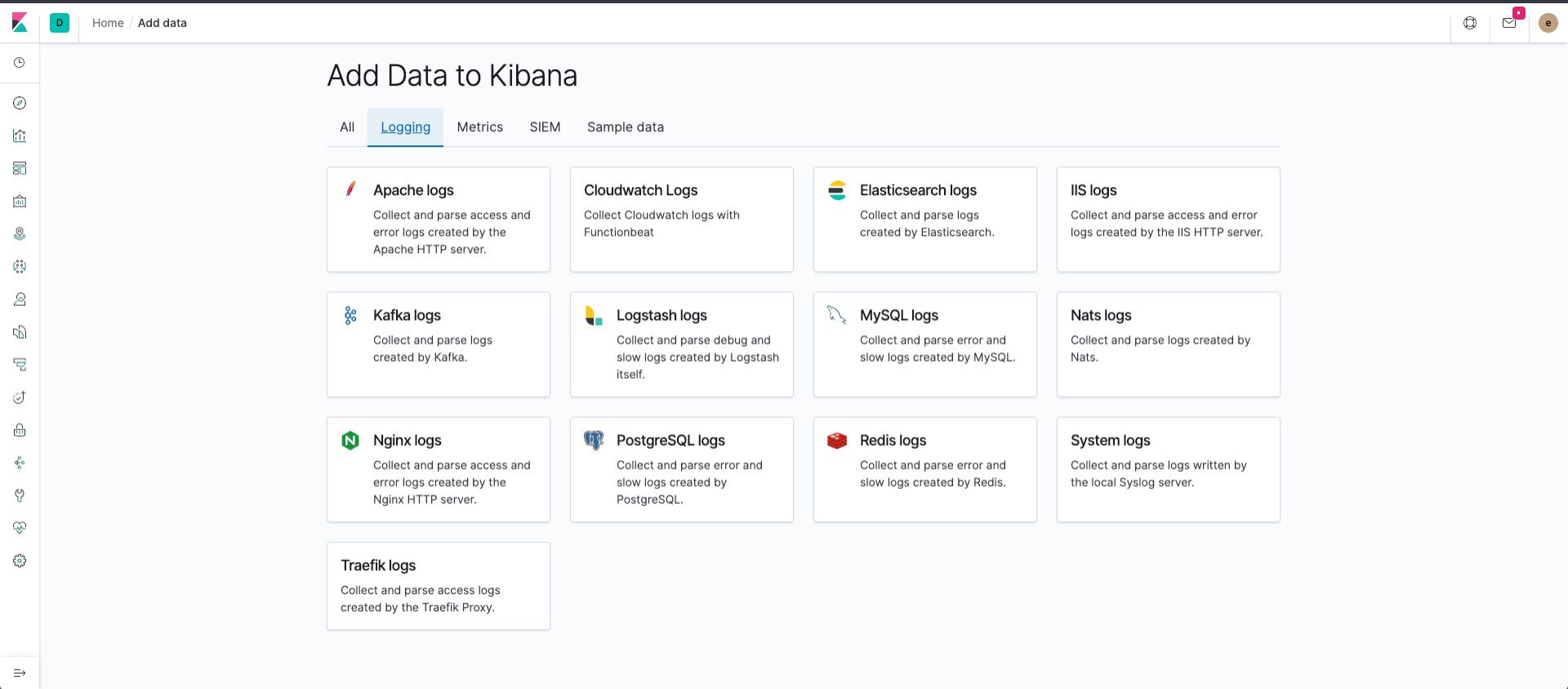
- Easy setup for a variety of sources
- Correlating and cross referencing
- Searching, filtering, and highlighting
- Visualize
- Anomaly detection and alerting
- Flexible retention



elastic

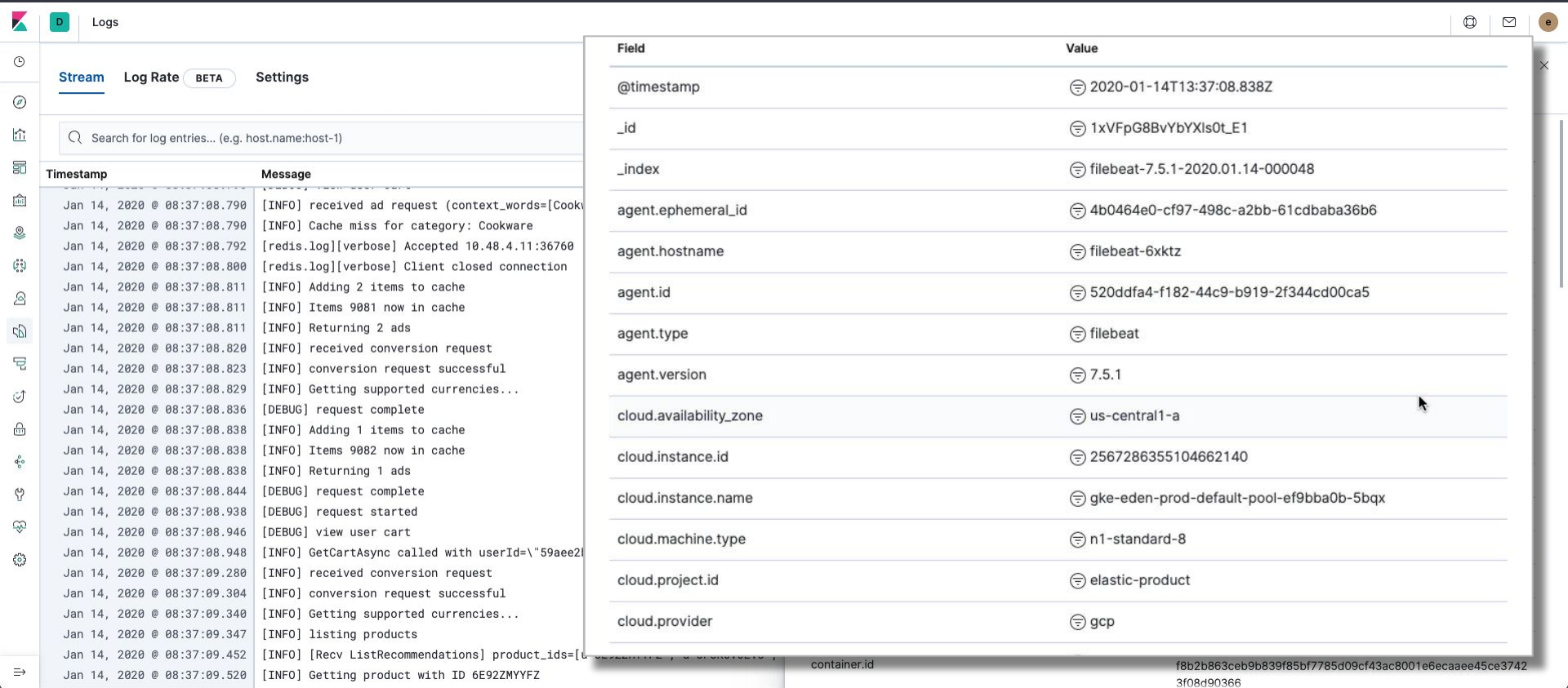
Needs for log analytics

Easy setup for variety of log sources



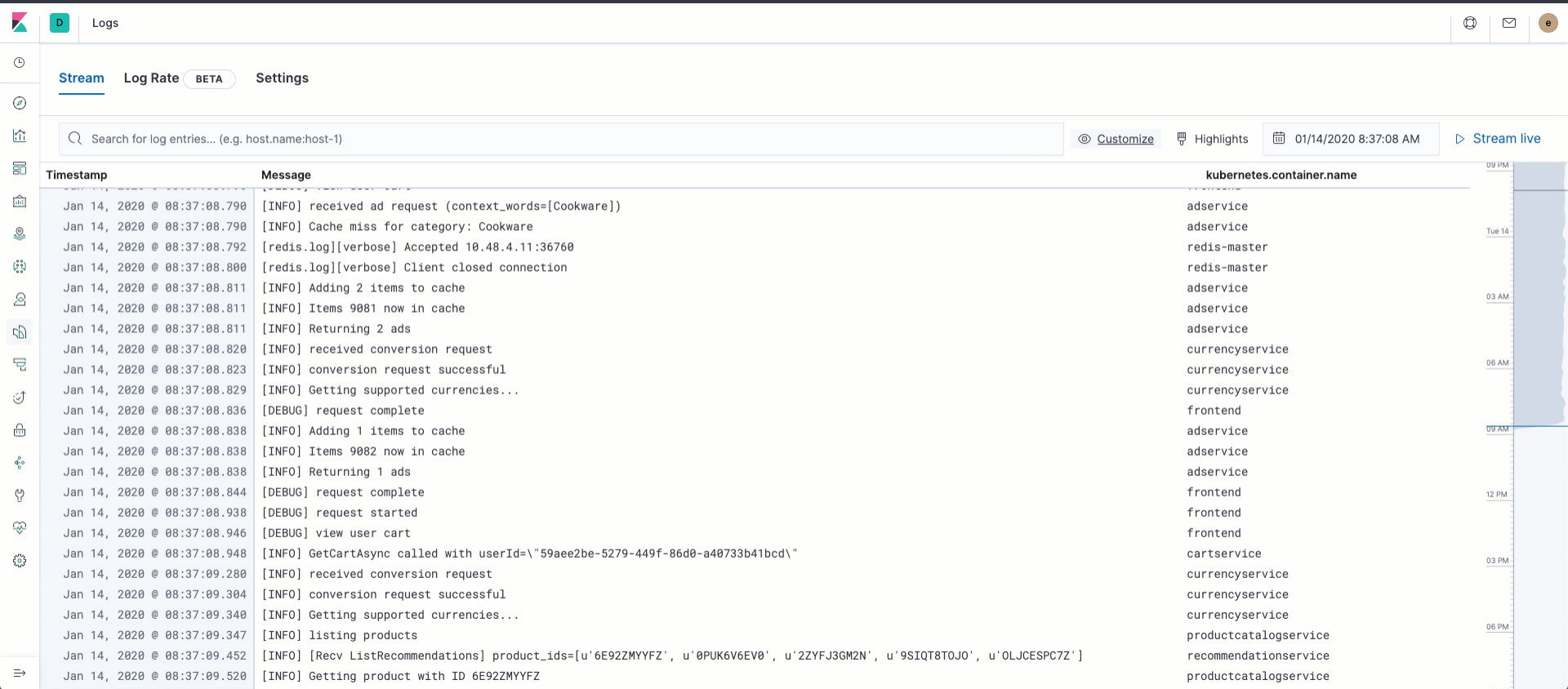
Needs for log analytics

Correlating and cross referencing



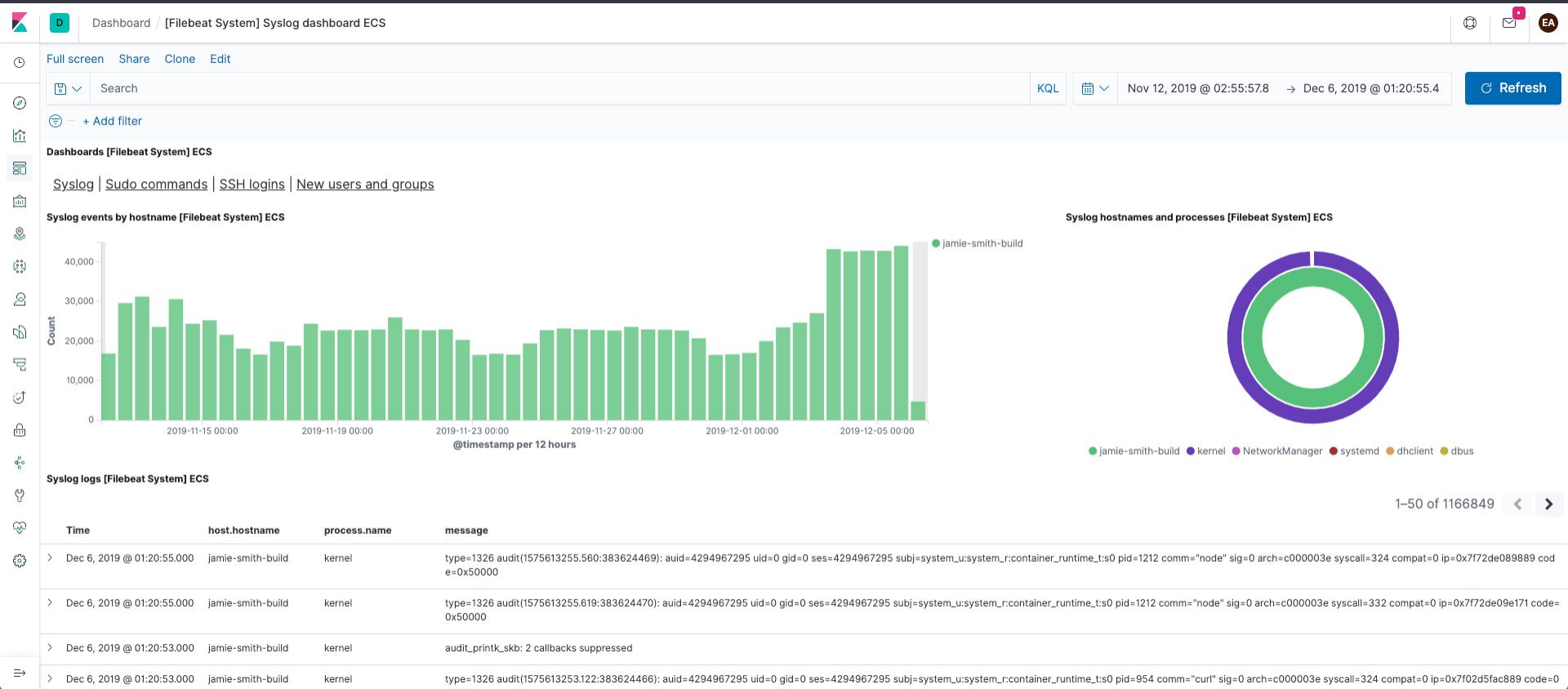
Needs for log analytics

Searching, filtering, and highlighting



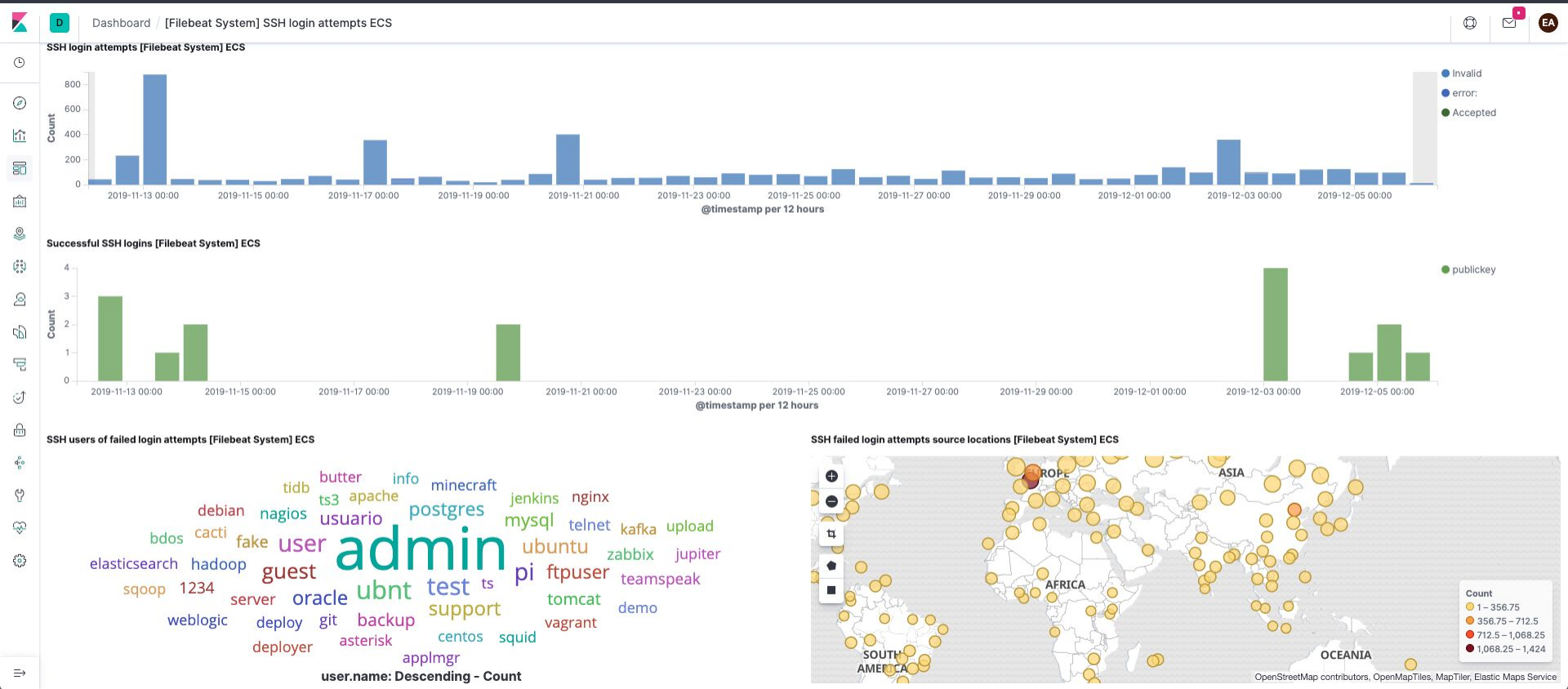
Needs for log analytics

Visualize



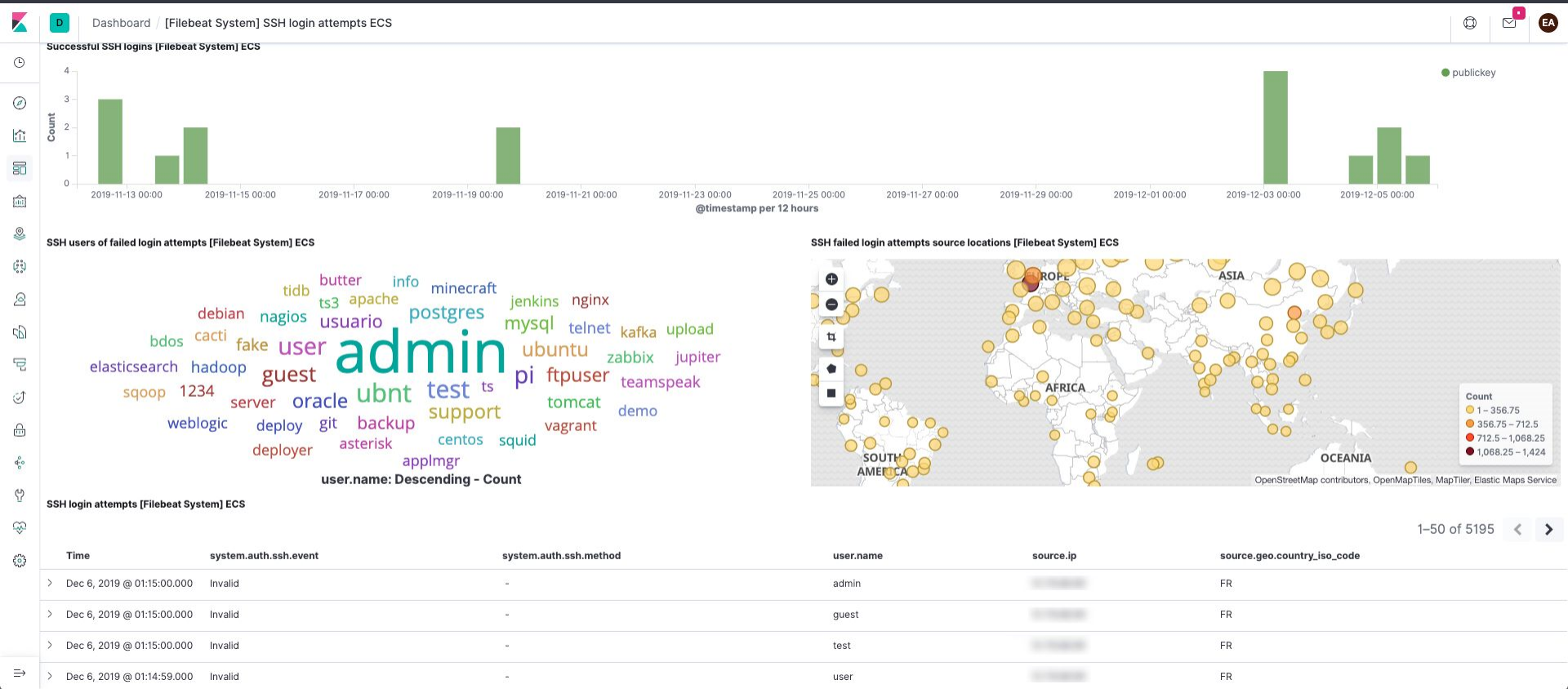
Needs for log analytics

Visualize



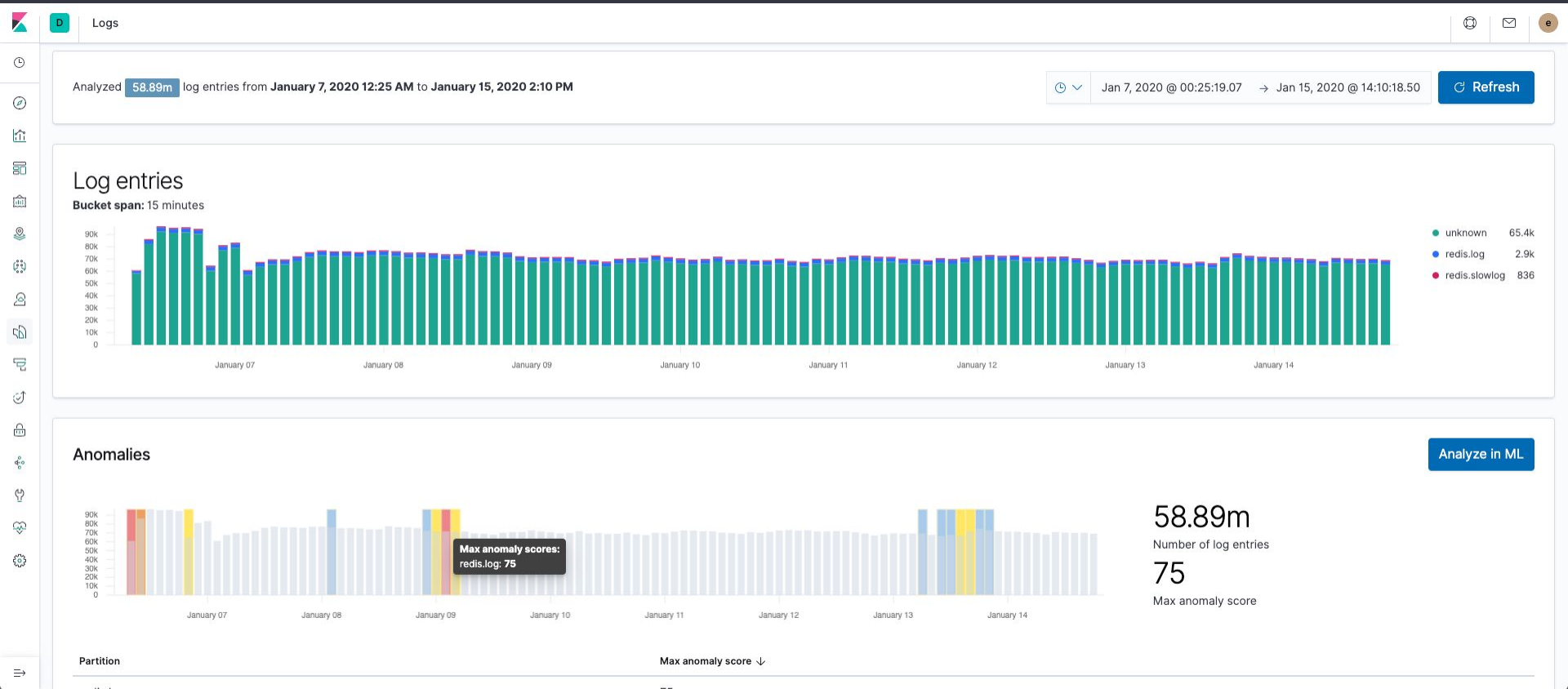
Needs for log analytics

Visualize



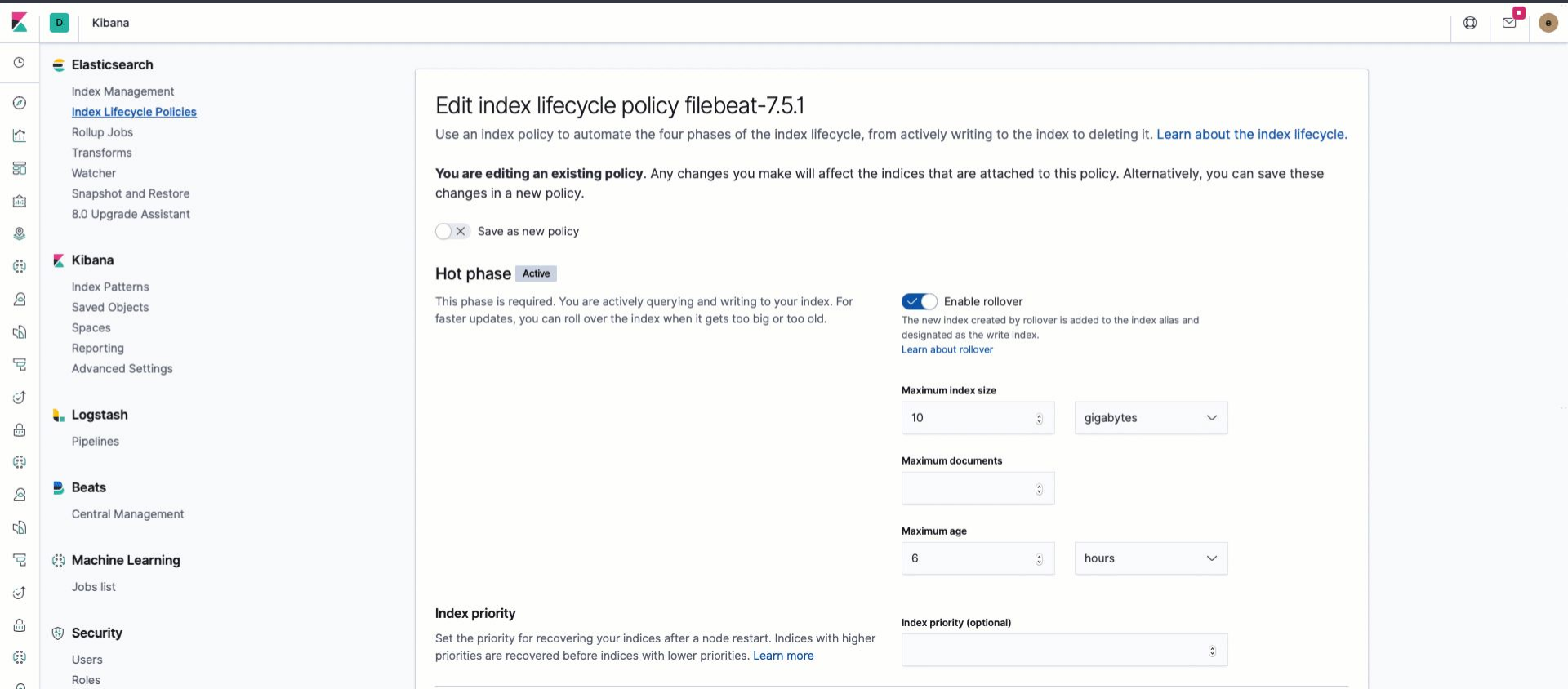
Anomaly detection and alerting

Can't stare at the screen all day



Needs for log analytics

Flexible retention



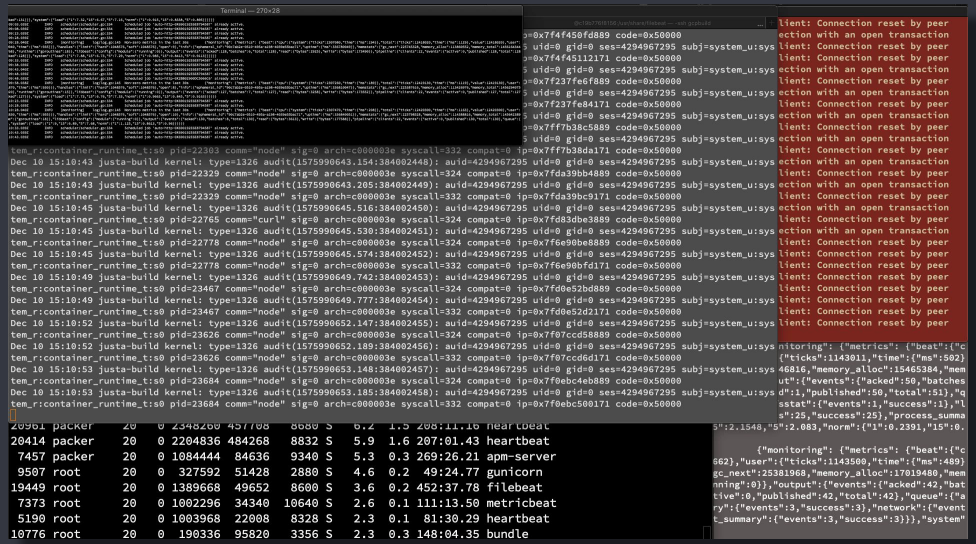
Needs for log analytics

Anomaly detection and alerting

Essential needs for log analytics

From the earlier list

- ✓ Easy setup for a variety of sources
- ✓ Correlating and cross referencing
- ✓ Searching, filtering, and highlighting
- ✓ Visualize
- ✓ Anomaly detection and alerting
- ✓ Flexible retention



elastic

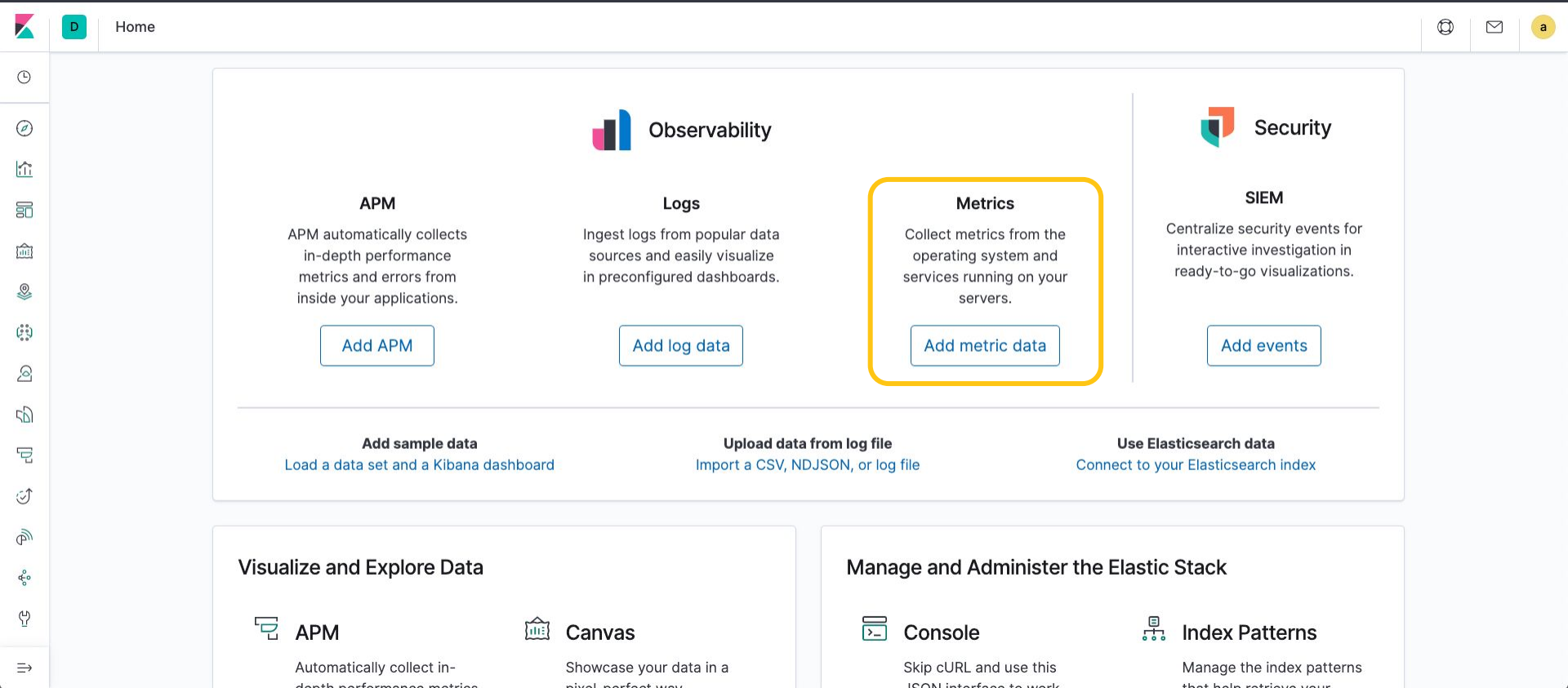
Agenda

Beyond logging: Observability

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security

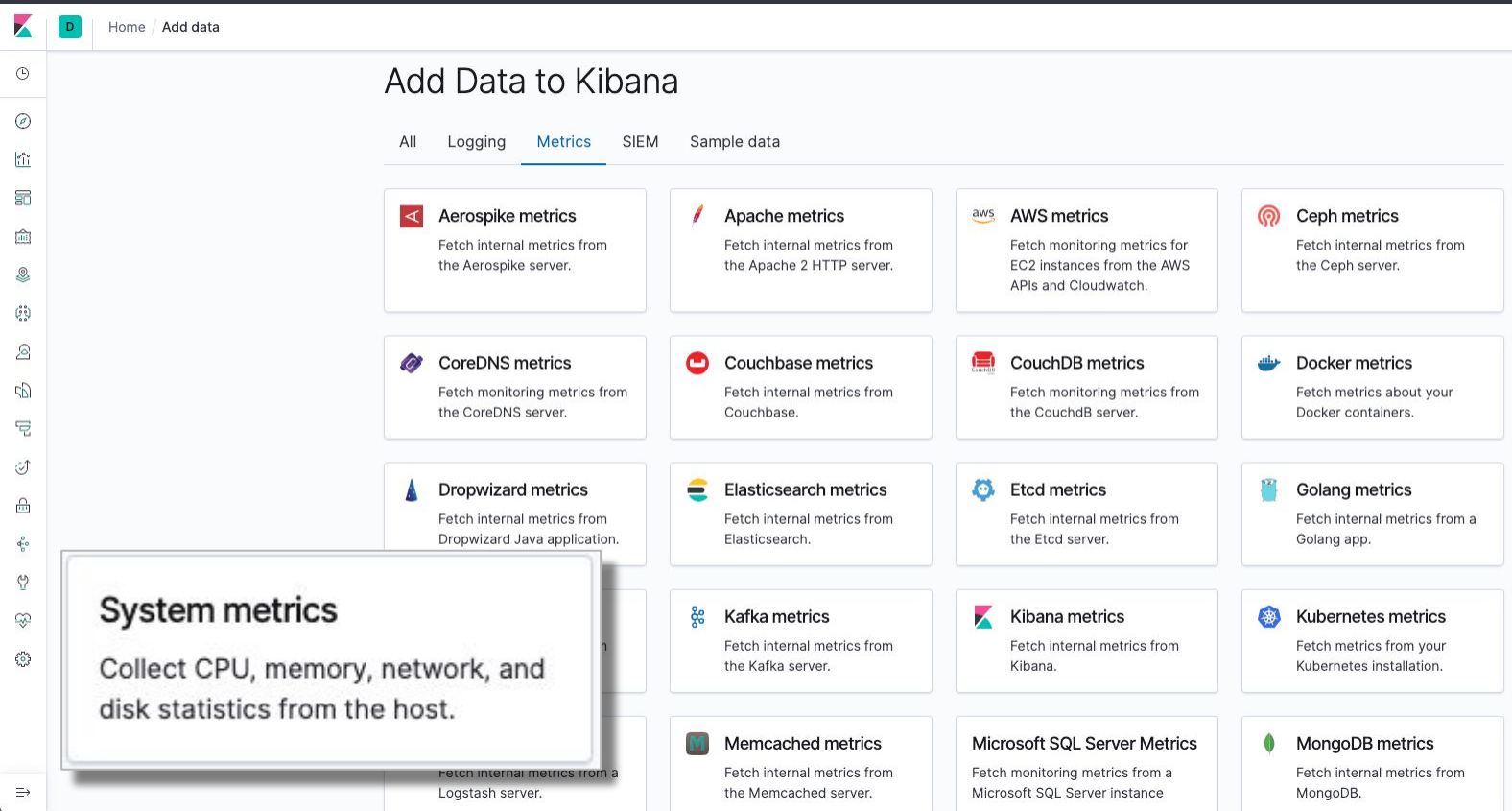
You can add metrics in the same manner

Select your integration



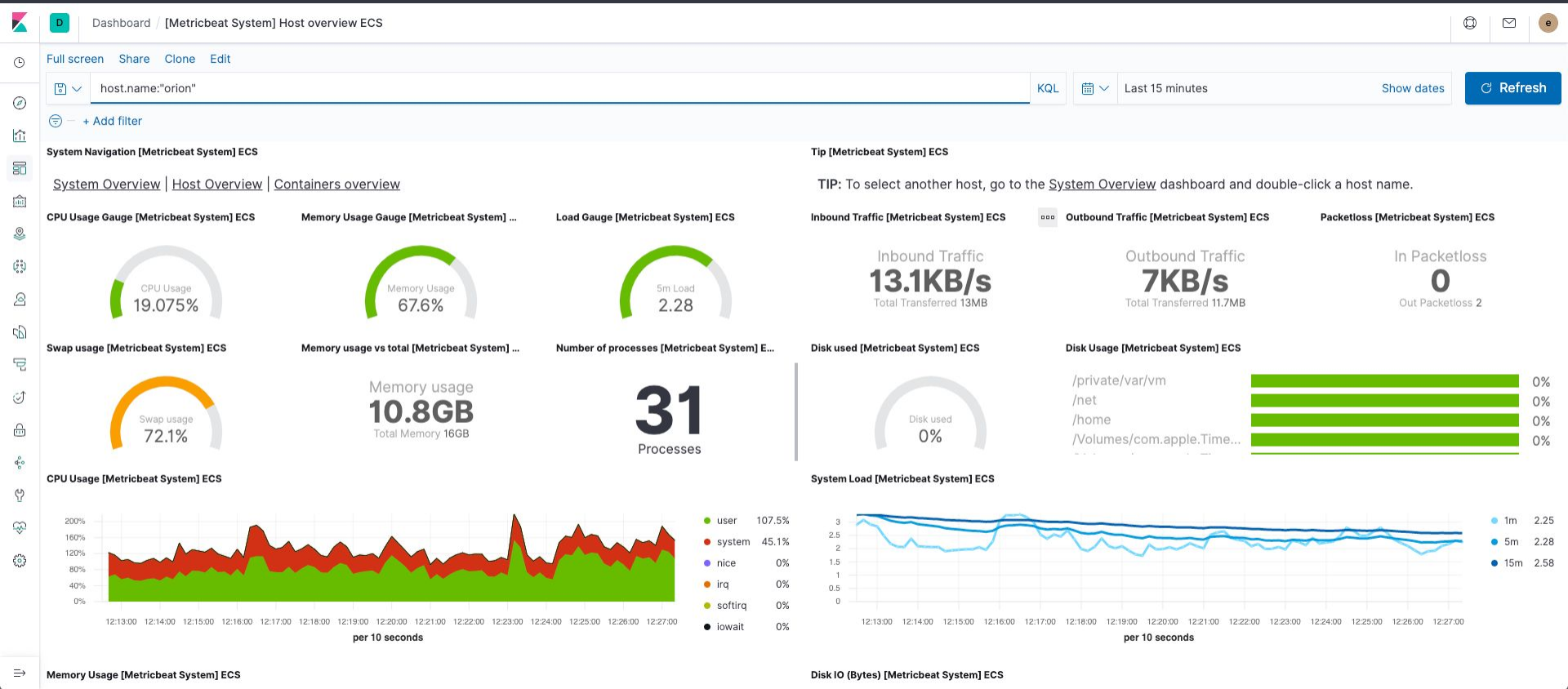
Many integrations

For example, system metrics



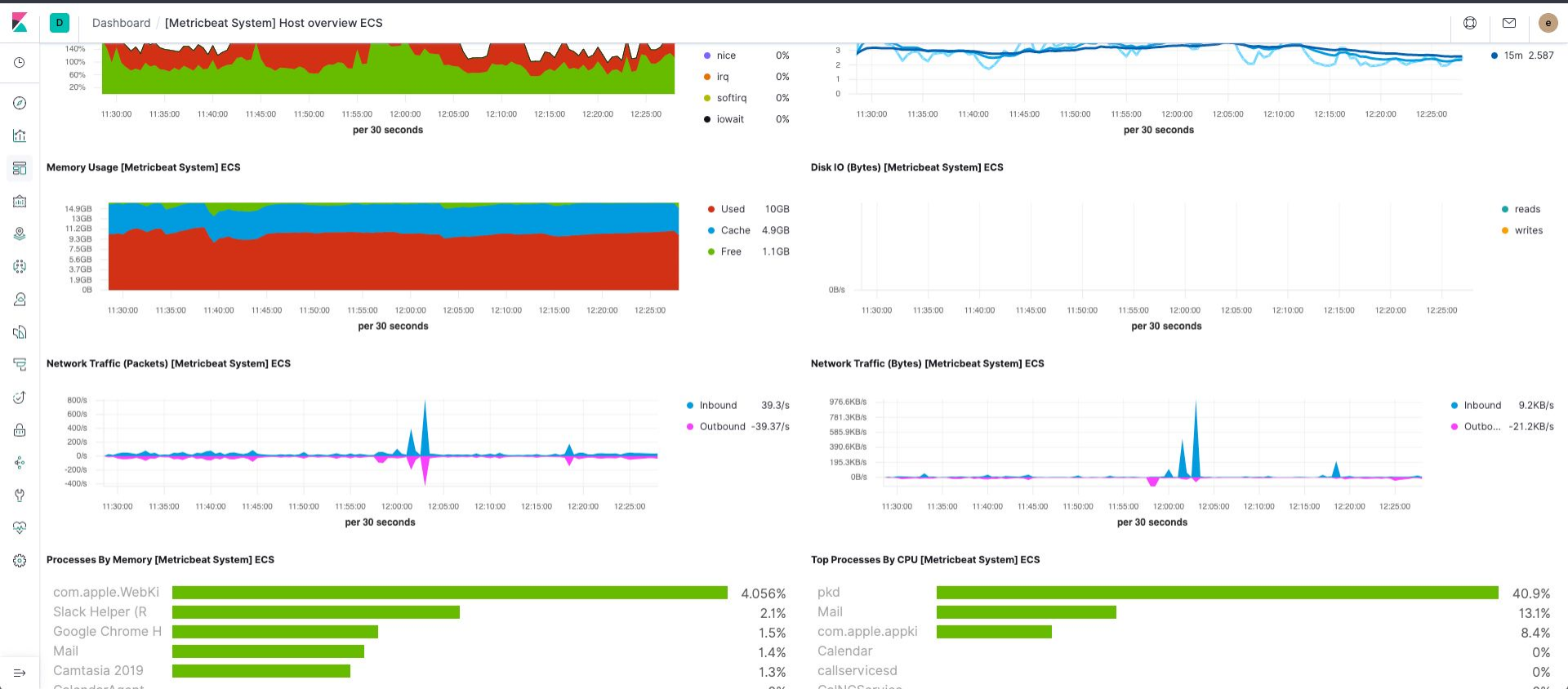
Metrics

Visualizing metrics



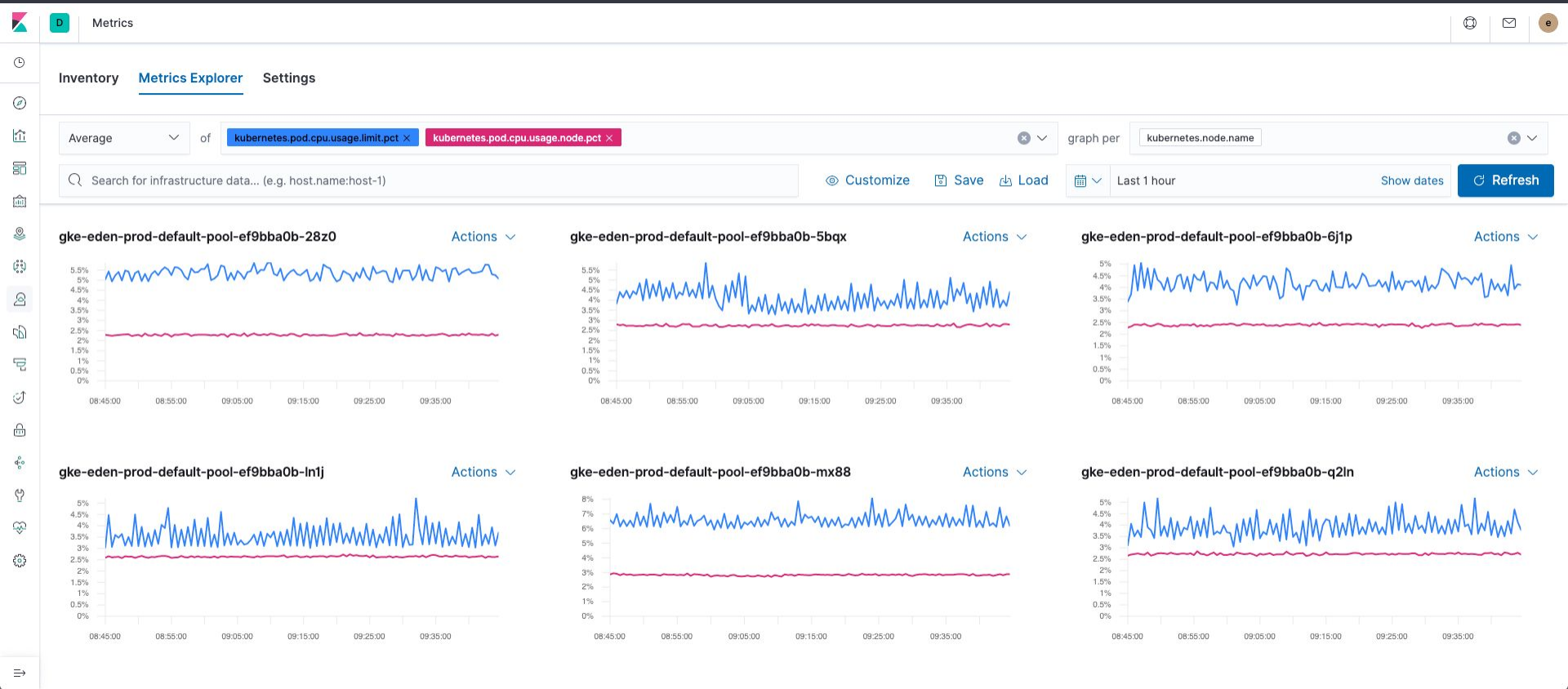
Metrics

Visualizing metrics



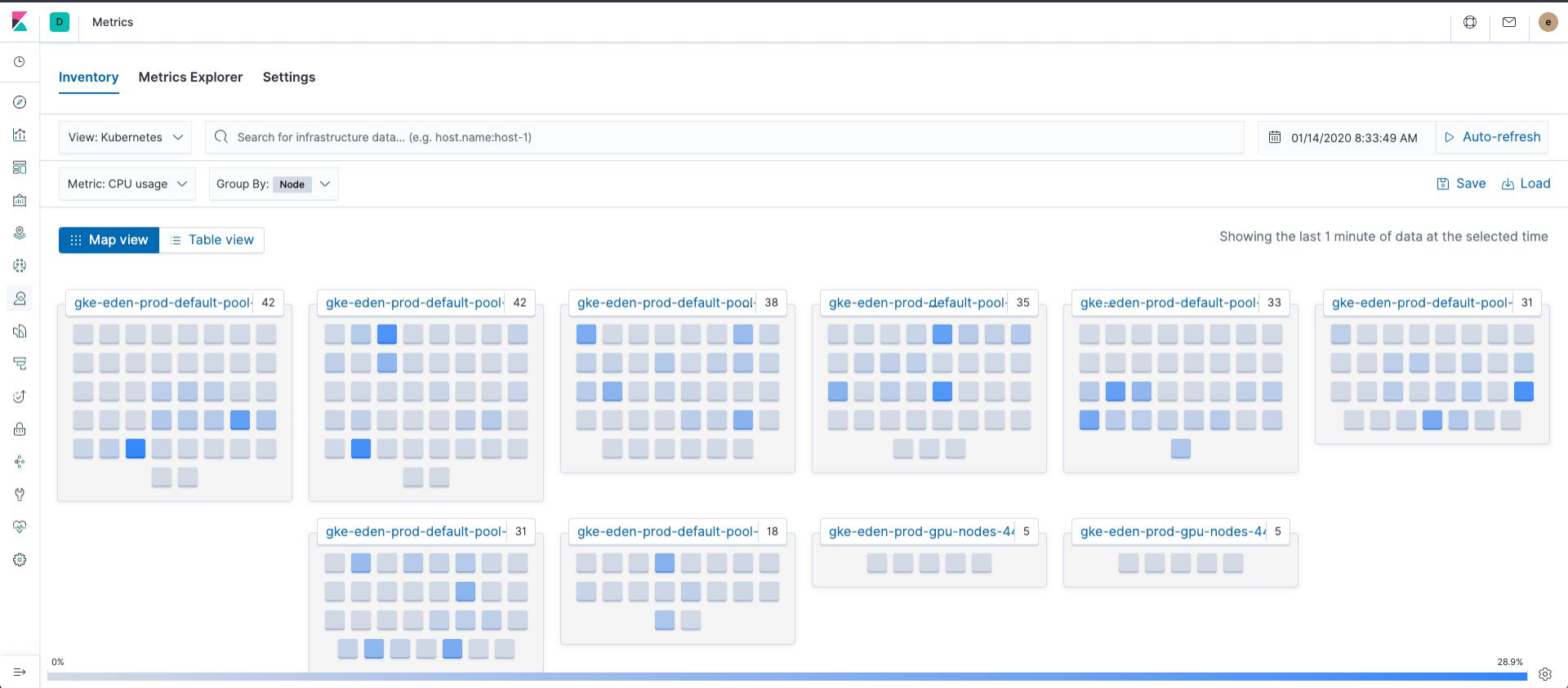
Metrics

Exploring metrics



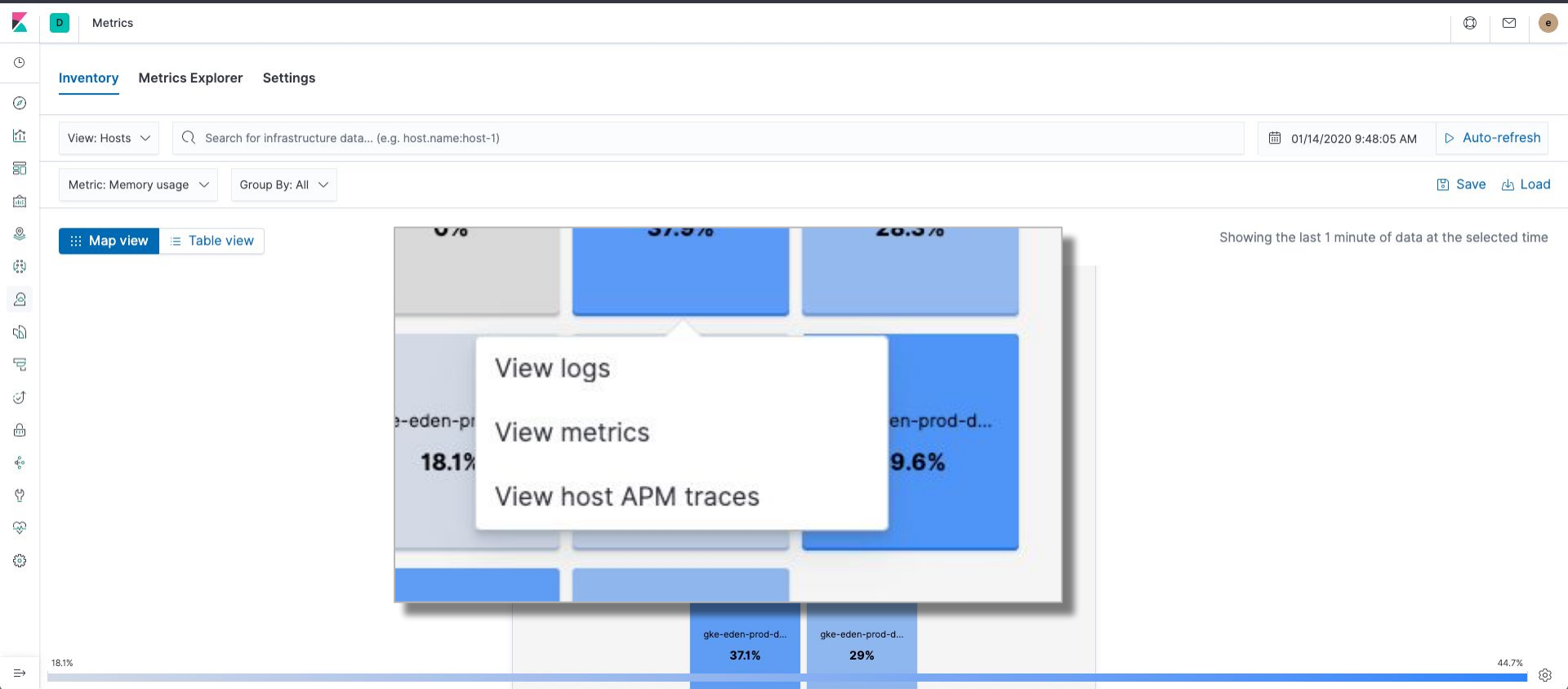
Metrics

Inventory view with multiple perspectives



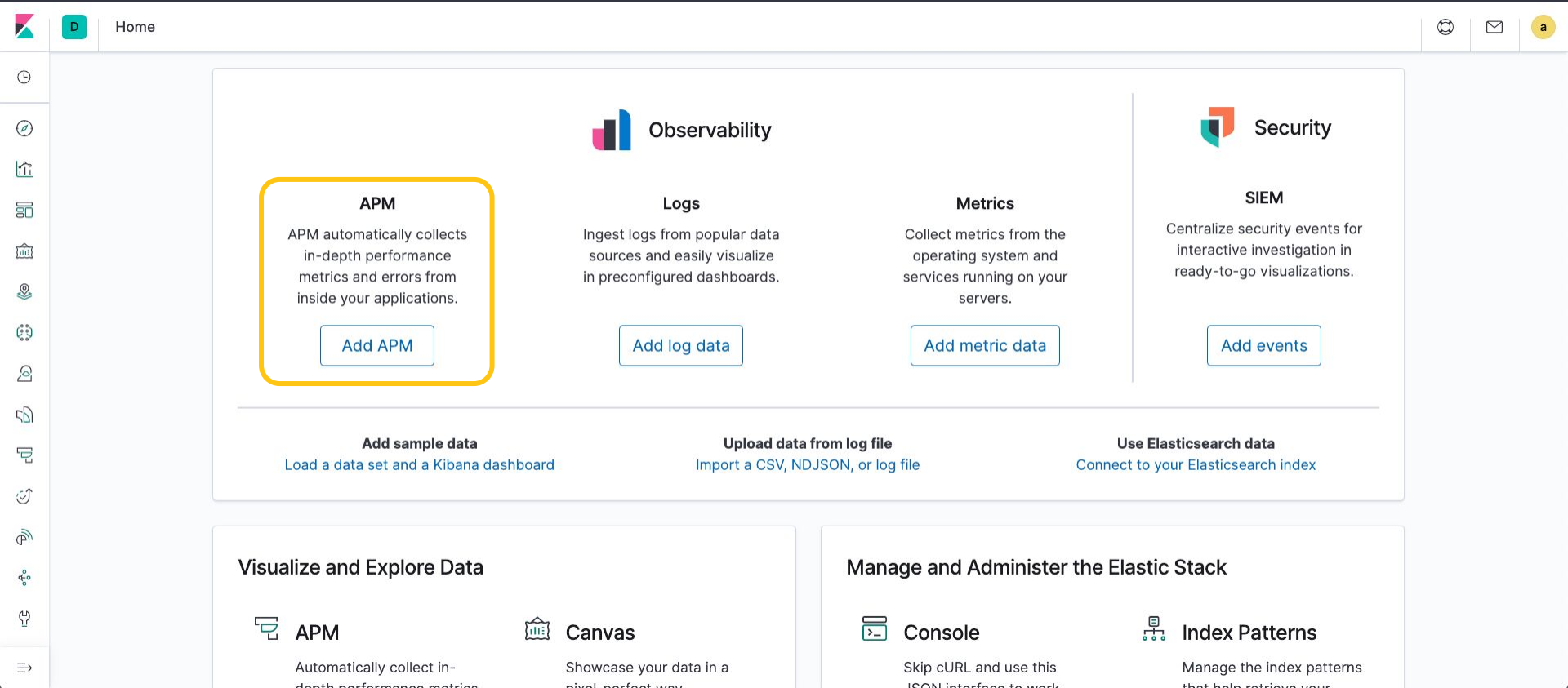
Integrated Experience

Observability with one datastore



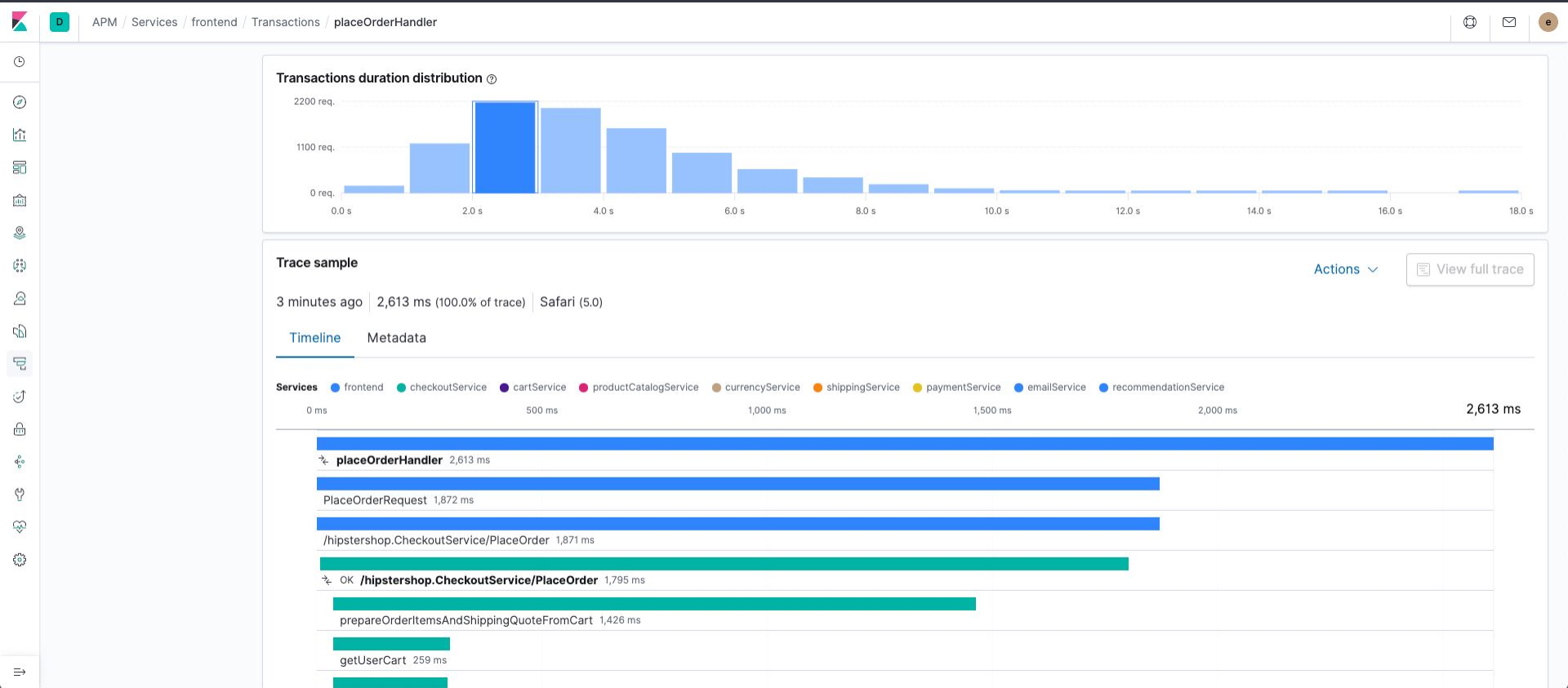
Setting up APM

Instructions in Kibana



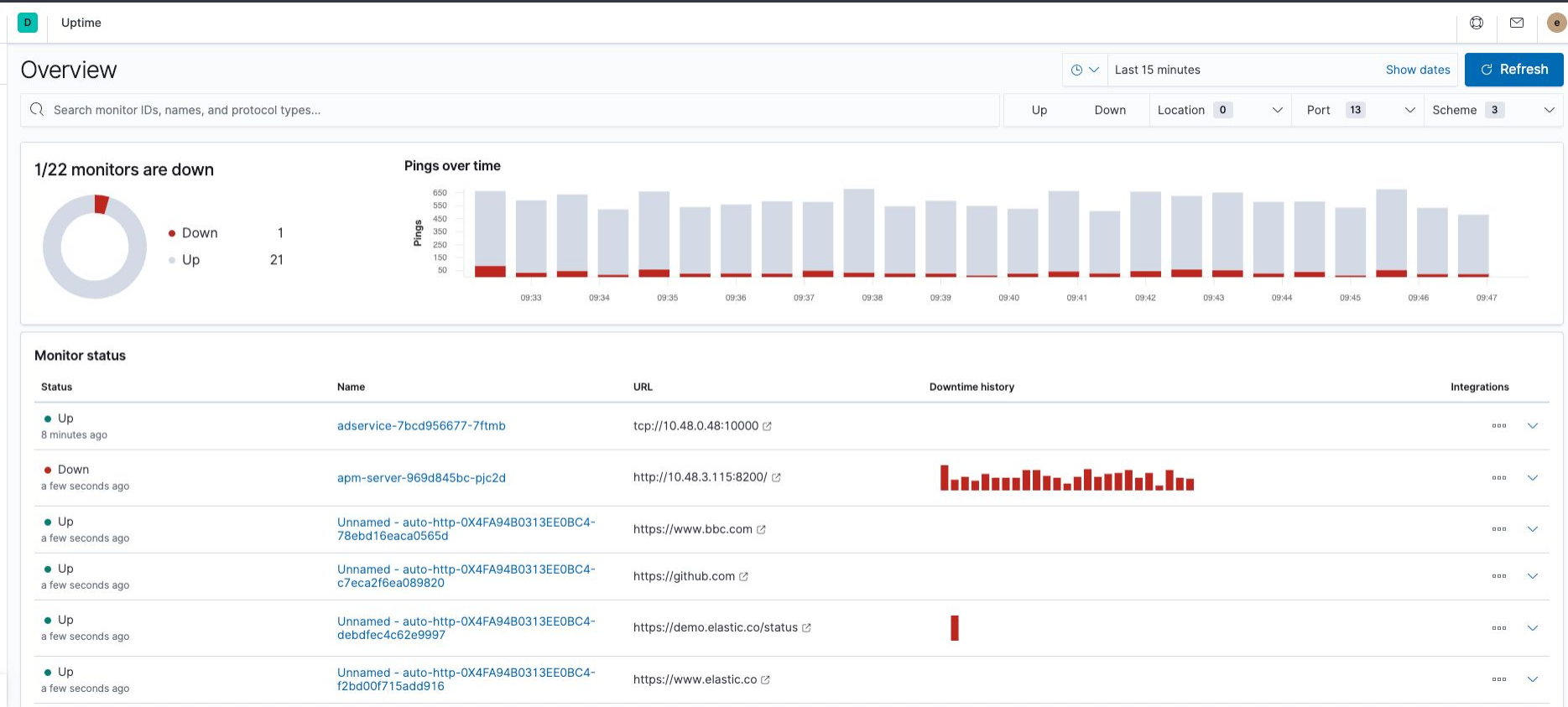
Application Performance Monitoring

Distributed Tracing



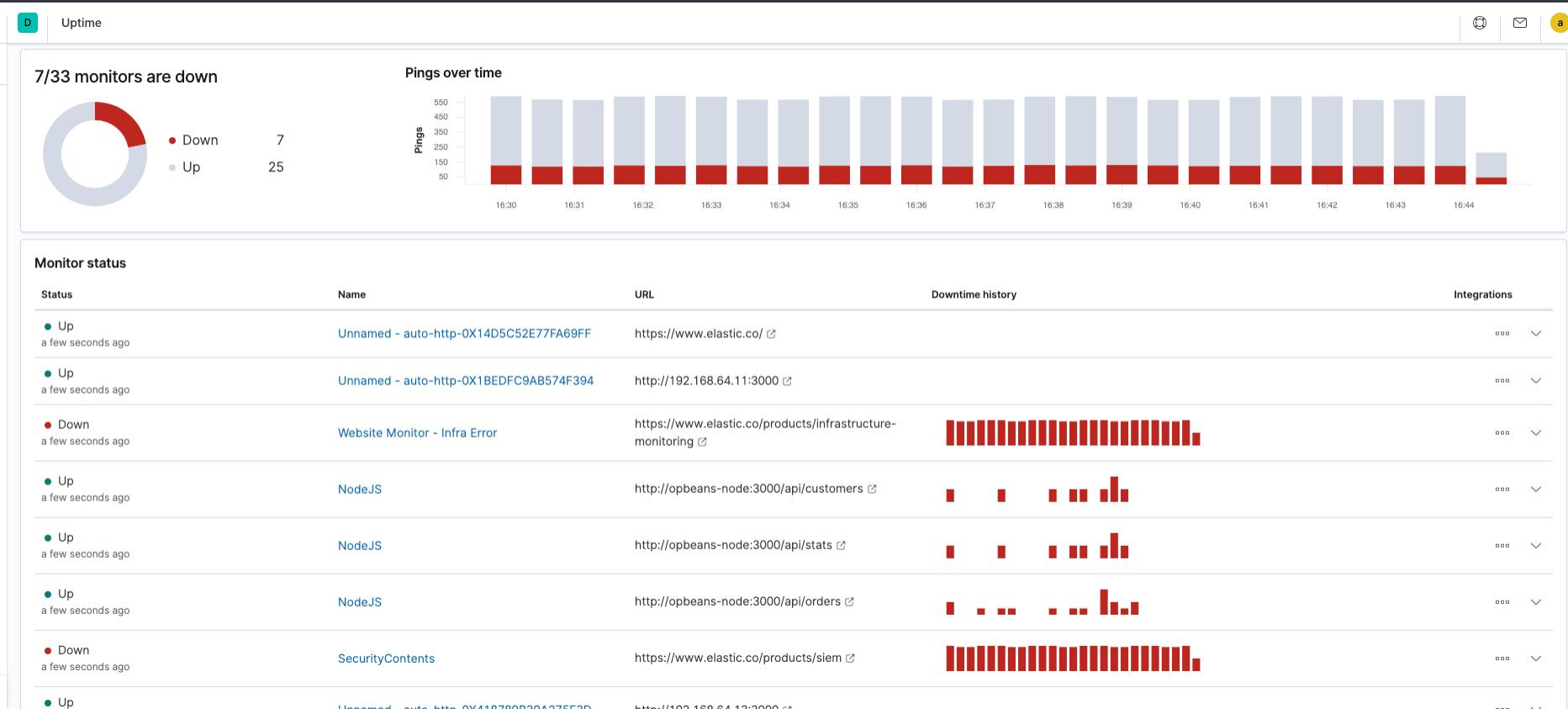
Uptime Monitoring

Service availability



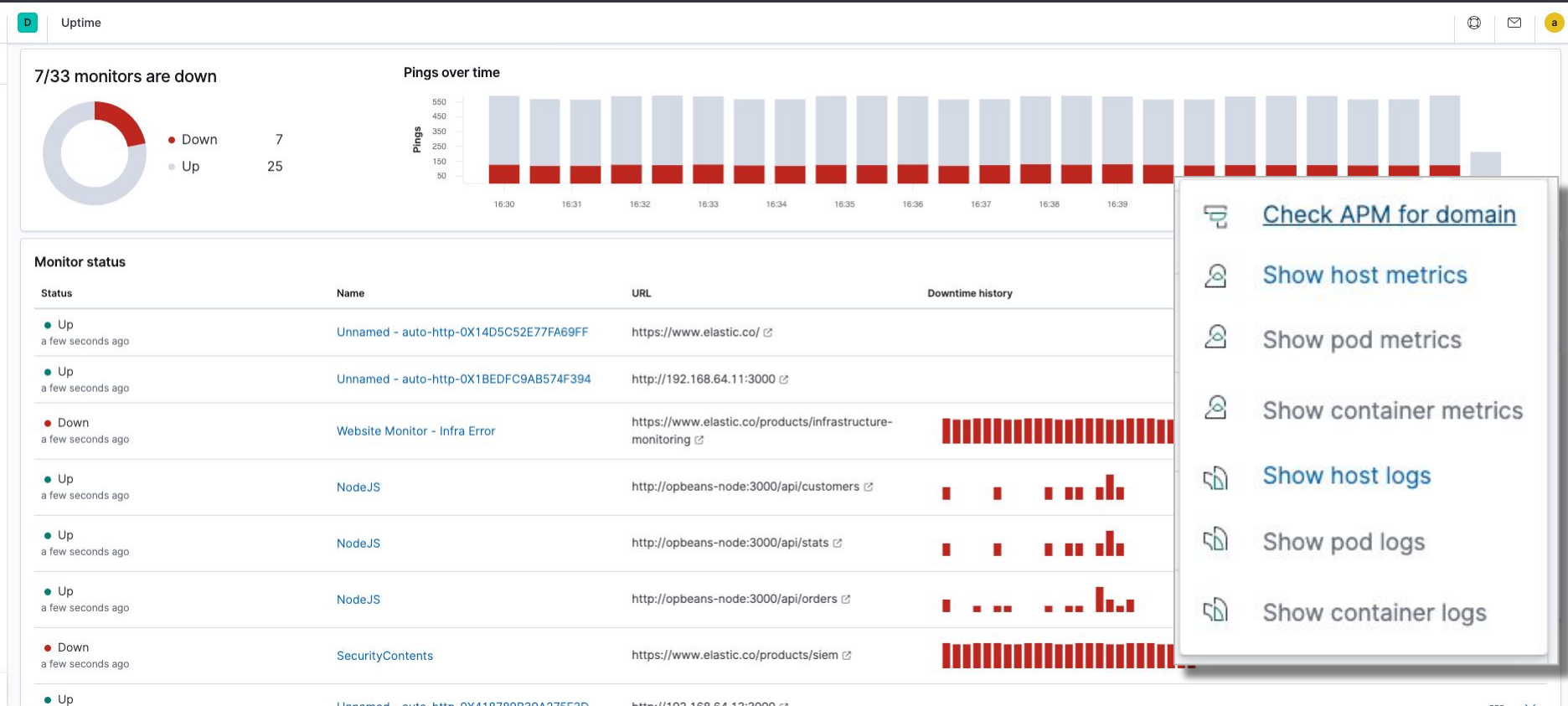
Uptime Monitoring

Service availability



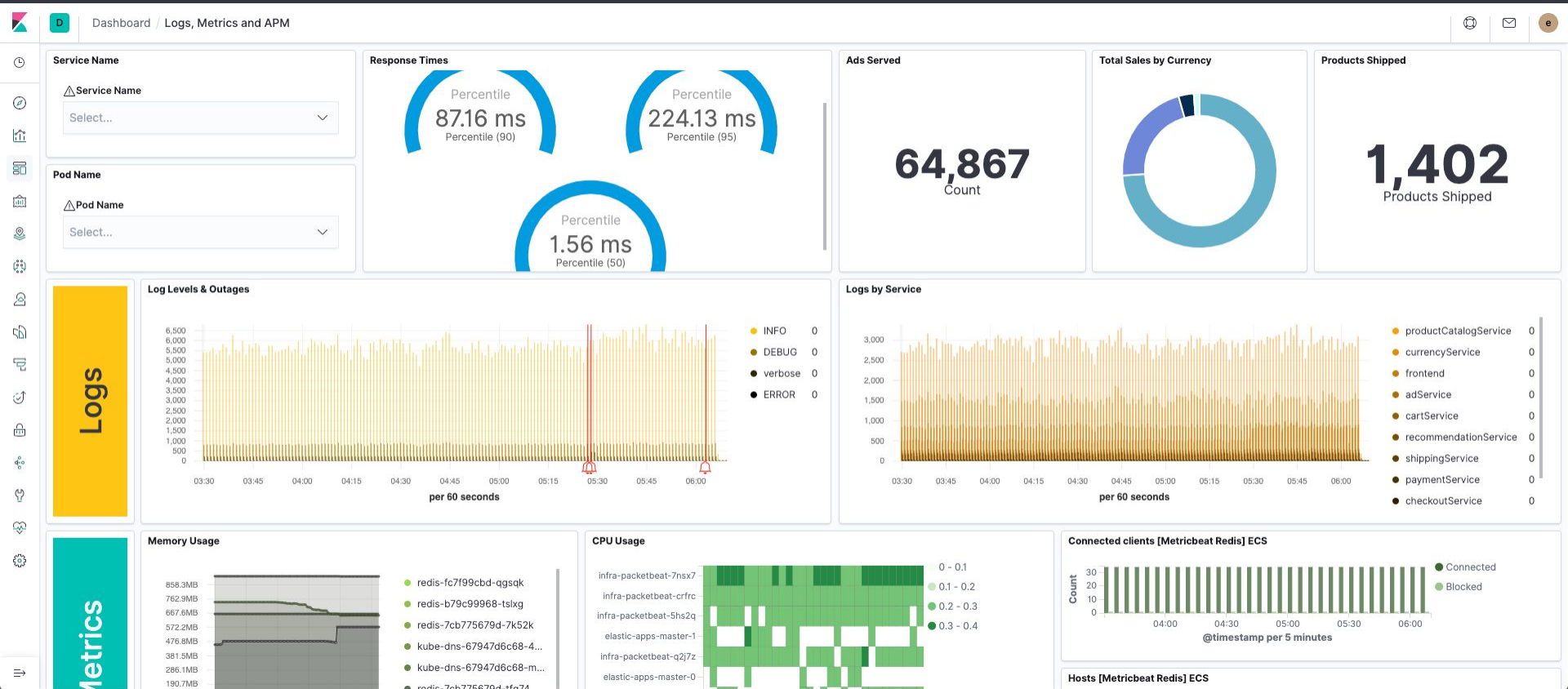
Uptime Monitoring

Integrated experience



Integrated Experience

Observability with one datastore



Integrated Experience

Observability with one datastore

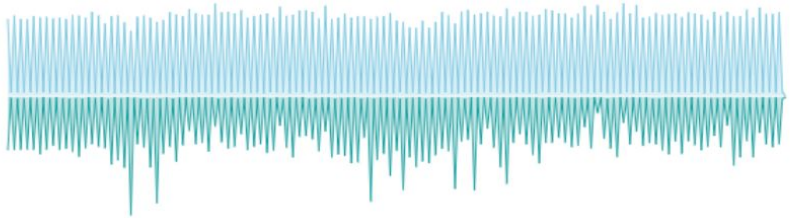
Deployment

Observability

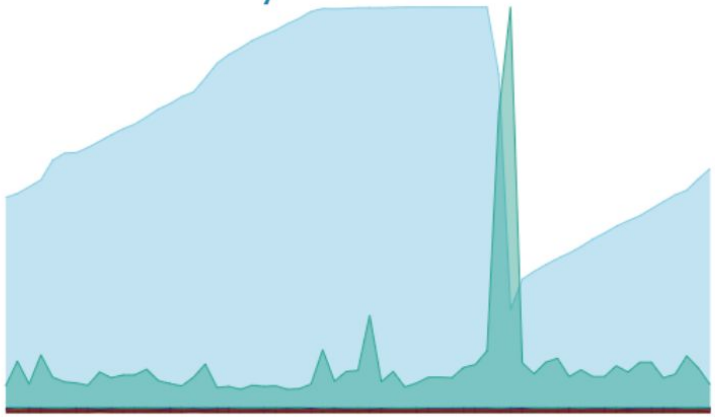
Network

Traffic In

Traffic Out



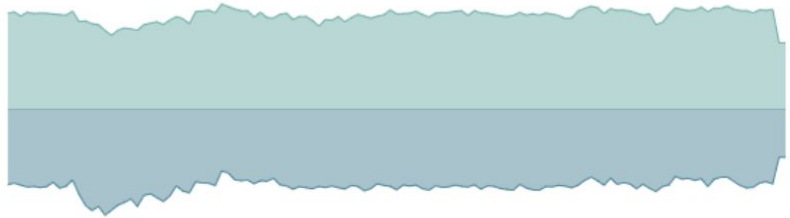
CPU/Memory



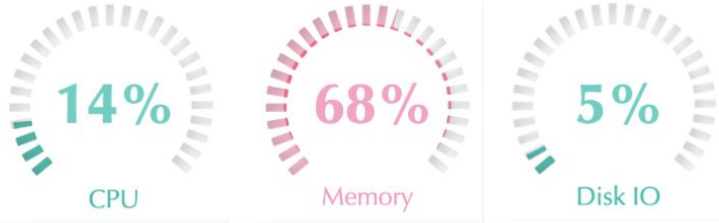
Disk IO

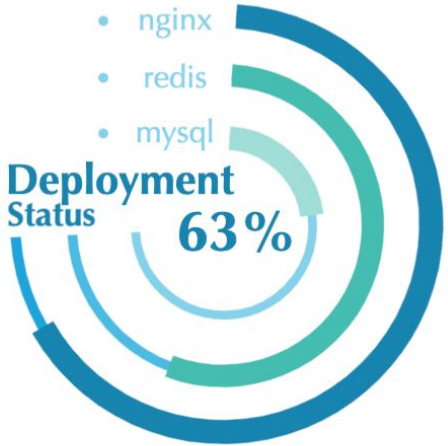
Read

Write



Services	Containers
10	141
Errors	**Pods**
19413	70





Agenda

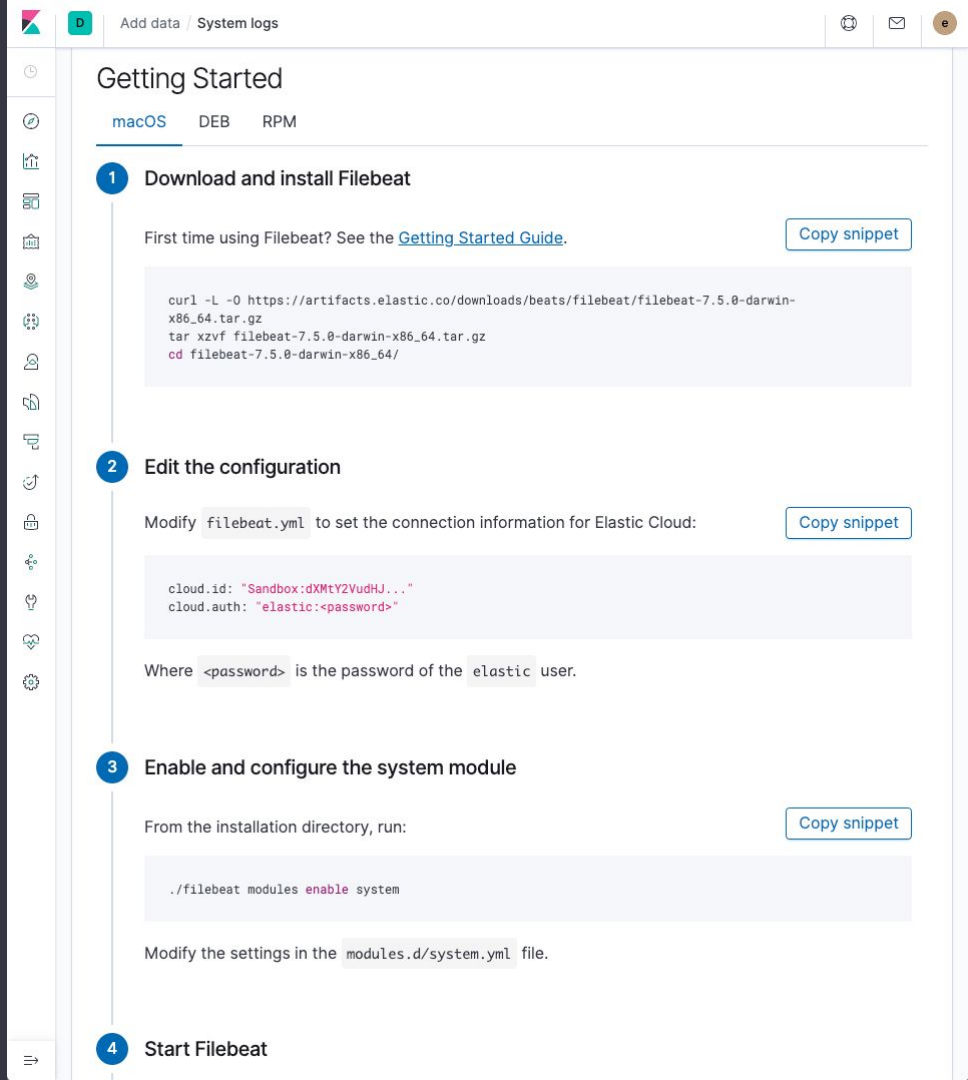
Securing your Beats

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security

Recall the Filebeat steps

Use parameterized credentials

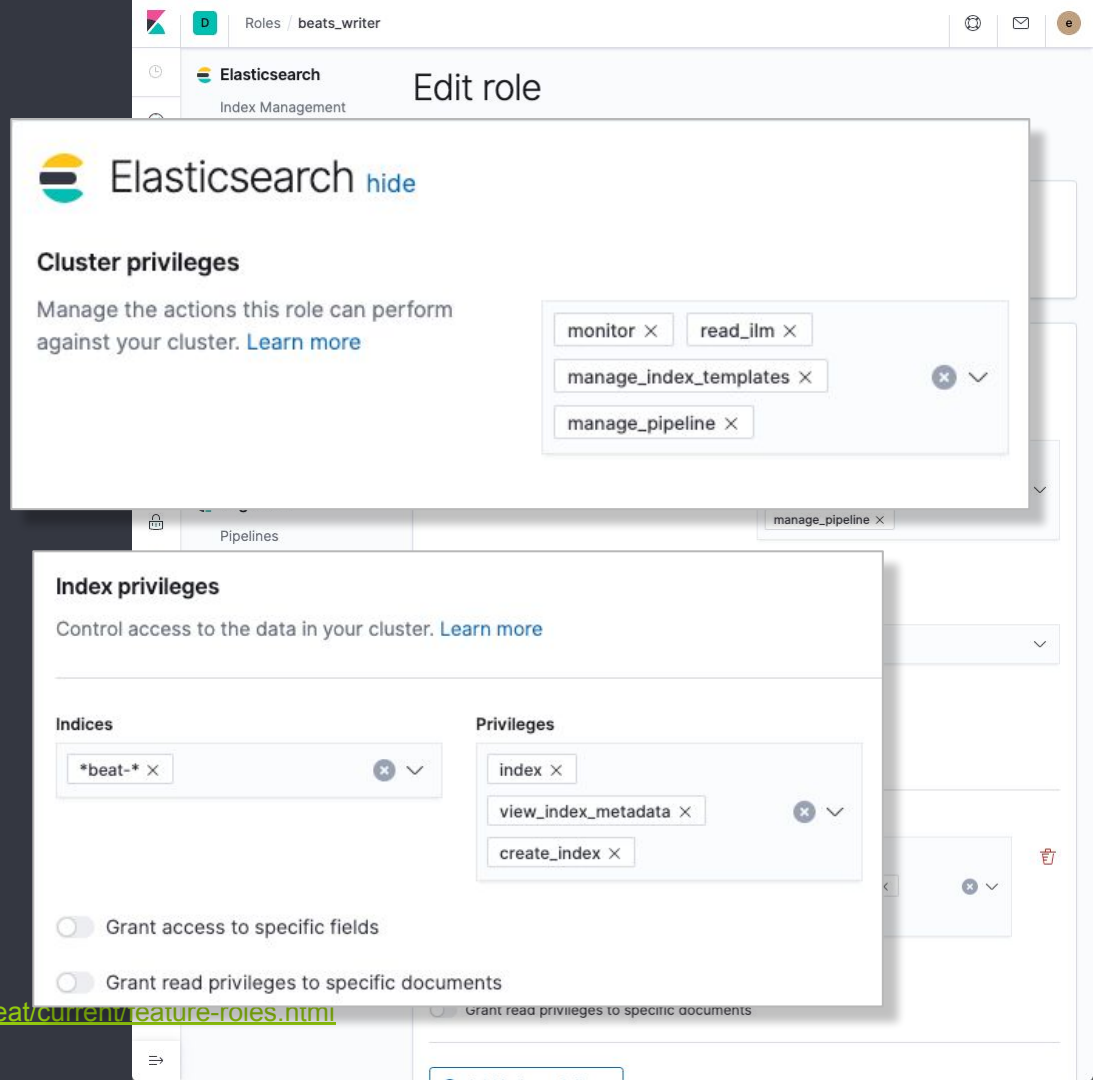
- Download and install Filebeat
- Edit the configuration
- Enable and configure the system module
- Start Filebeat



`beats_writer` Role

Required permissions

- Cluster Permissions:
  - monitor
  - read_ilm
  - manage_index_templates
  - manage_pipeline
- Index Privileges (*beat-*)
  - create_index
  - index
  - view_index_metadata

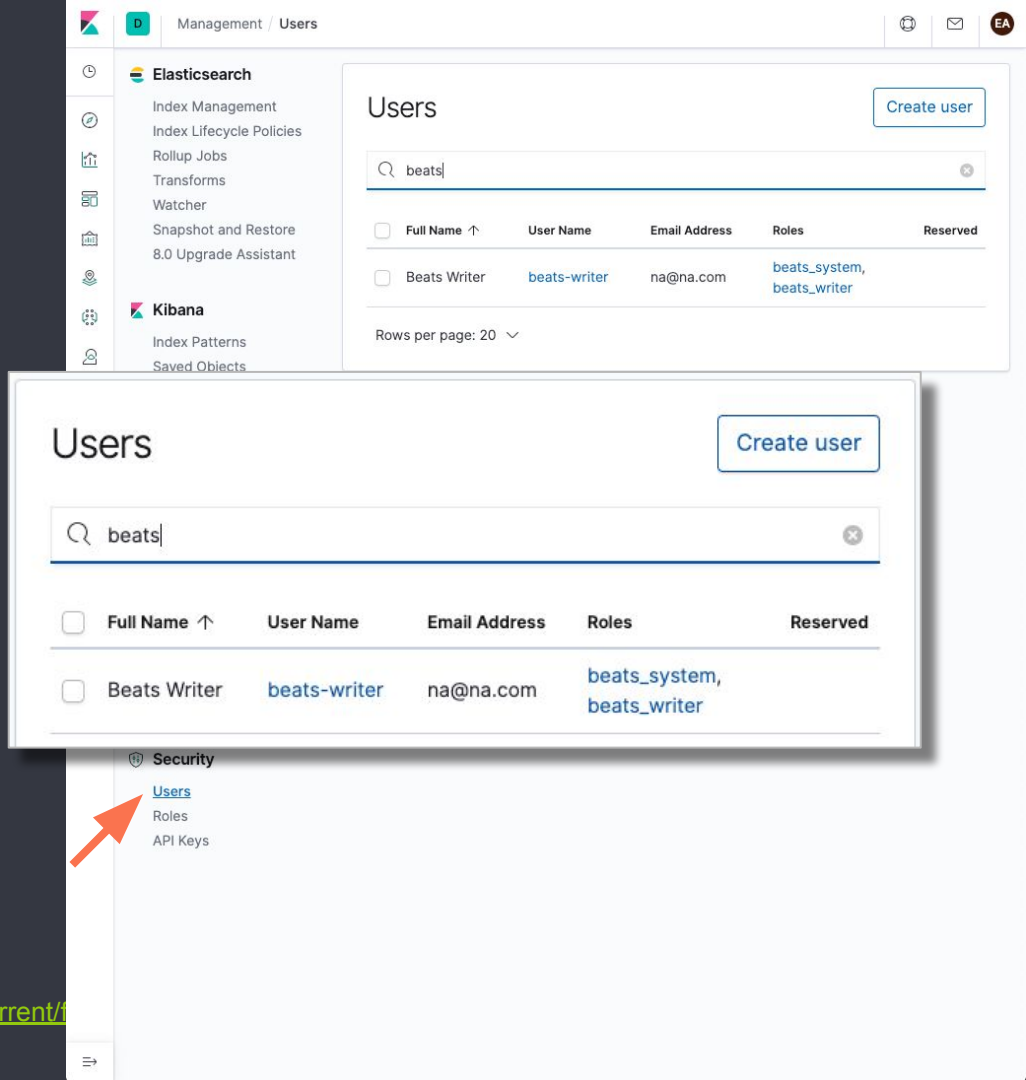


https://www.elastic.co/guide/en/beats/filebeat/current/feature-roles.html

Corresponding User

Tying roles to users

- Give the user the corresponding roles
- Create a secure password
- `beats-writer` gets the writer role we created, plus the shipped `beats_system` role



https://www.elastic.co/guide/en/beats/filebeat/current/f

Set up the keystore

Hiding credentials for `beats-writer`

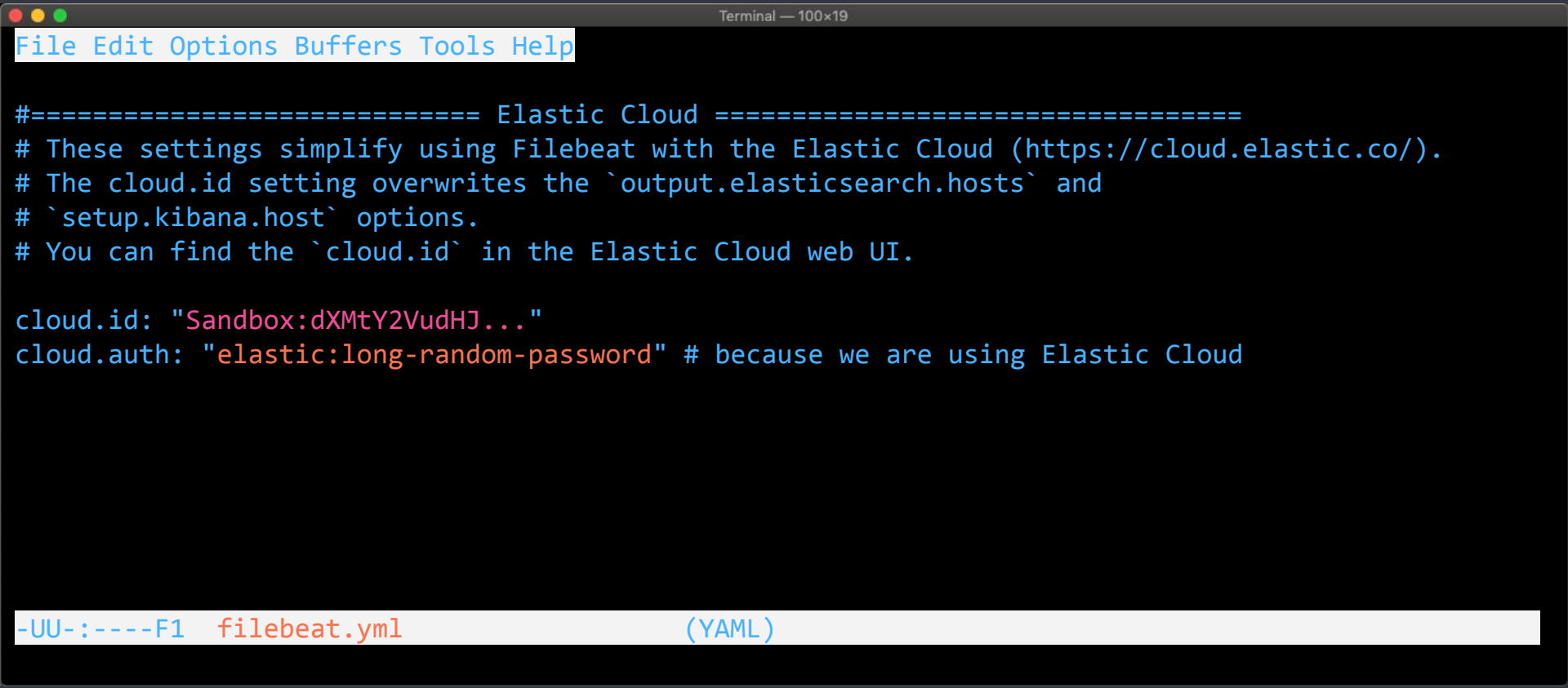
Terminal — 100×19

```
$ >./filebeat keystore
Manage secrets keystore

Usage:
  filebeat keystore [command]

Available Commands:
  add         Add secret
  create      Create keystore
  list        List keystore
  remove      Remove secret
```

- Command: `filebeat keystore`
- `Create` the keystore
- `filebeat keystore add`:
  - `BEATS_WRITER_USER`
  - `BEATS_WRITER_PASSWORD`
- Access keys via `${KEY_NAME}`

Previous Configuration

Had the user & password hardcoded



Parameterize the user

Had the user & password hardcoded

Terminal — 100×19

```
File Edit Options Buffers Tools Help

#============================ Elastic Cloud ==================================
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "${BEATS_WRITER_USER}:long-random-password" # because we are using Elastic Cloud
```

```
-UU-:----F1  filebeat.yml                  (YAML)
```

And the password

No more plain text!

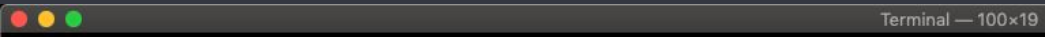
Terminal — 100×19

```
File Edit Options Buffers Tools Help

#============================ Elastic Cloud ================================
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "${BEATS_WRITER_USER}:${BEATS_WRITER_PASSWORD}" # because we are using Elastic Cloud
```

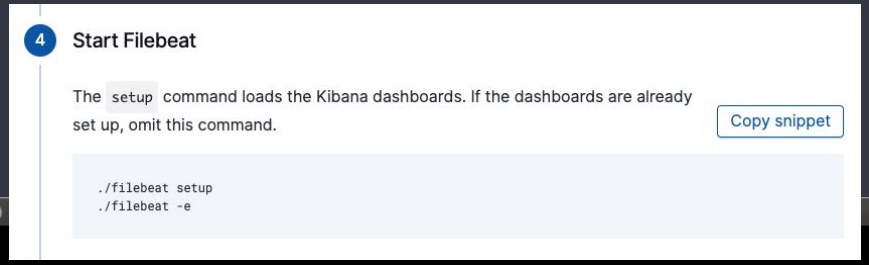
```
-UU-:----F1  filebeat.yml                  (YAML)
```

Starts the same way

Automatically picks up the keystore

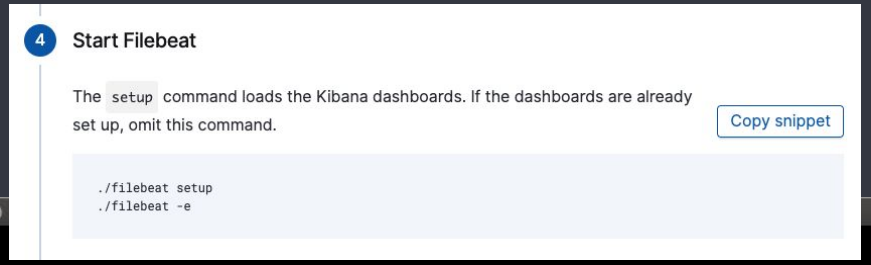



```
$ >./filebeat -e
```



Finally, start it!

assumes that you've run setup



Terminal — 100×19

```
$ >./filebeat -e

2019-12-09T18:02:42.500Z INFO instance/beat.go:610Home path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64] Config path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64] Data path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64/data] Logs path:
[/home/user/logs-demo/filebeat-7.5.0-linux-x86_64/logs]
2019-12-09T18:02:42.501Z INFO instance/beat.go:618Beat ID: 04e276d0-79bd-40e3-9c83-3cdc4a64f791
2019-12-09T18:02:42.513Z INFO add_cloud_metadata/add_cloud_metadata.go:93   add_cloud_metadata:
hosting provider type detected as gcp,
metadata={"availability_zone":"us-east1-b","instance":{"id":"8271592631829869565","name":"user-smi
th-build"},"machine":{"type":"n1-standard-8"},"project":{"id":"elastic-product-marketing"},"provid
er":"gcp"}
2019-12-09T18:02:42.564Z INFO [seccomp] seccomp/seccomp.go:124   Syscall filter successfully
installed
(...)
```

Continuing your Journey

Where to find more information

- Spin up a cluster
  - Hosted: cloud.elastic.co
  - Self managed - elastic.co/downloads
- Explore live examples @ elastic.co/demos
- Watch webinars @ elastic.co/videos
- Chat with us @ Forums : https://discuss.elastic.co/
- Go deeper with documentation @ elastic.co/guide
- Sign up for training @ elastic.co/training
- Attend a local meetup or Elastic{ON}

Q & A

Thank you!