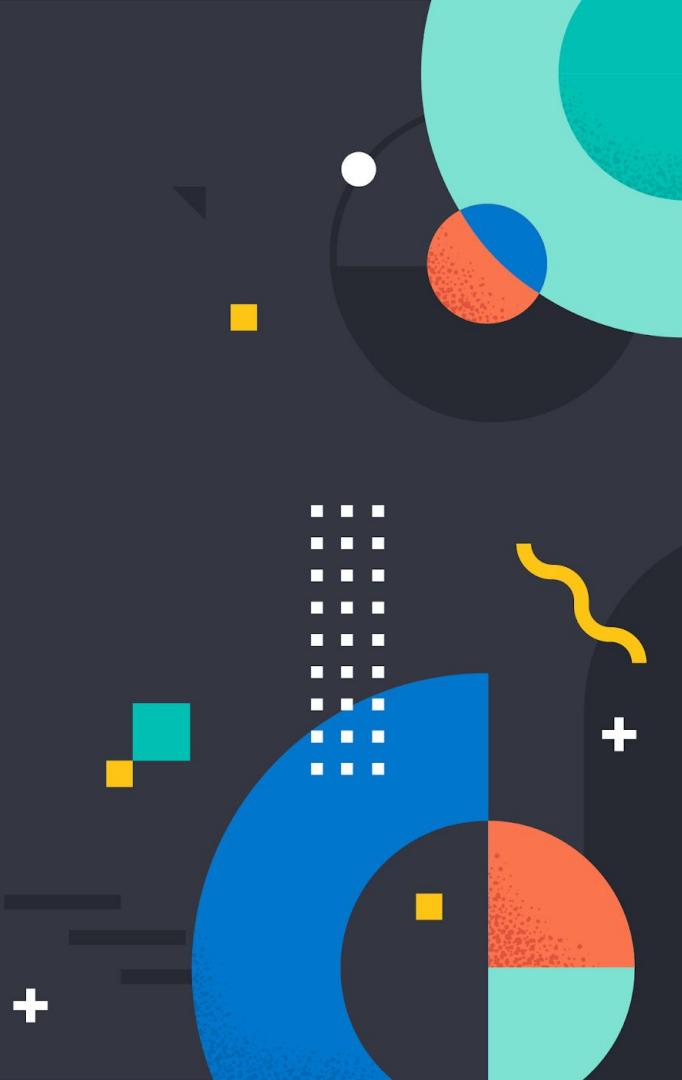




Introduction to Logging with the ELK Stack

Amy Ghate
Solutions Architect





logs

+



metrics

=



apm



ObservaBLT
Observability

Elastic Approach to Observability

Dev & Ops Teams



Log Data

Web Logs
App Logs
Database Logs
Container Logs

Metrics Data

Container Metrics
Host Metrics
Database Metrics
Network Metrics
Storage Metrics

APM Data

Real User Monitoring
Txn Perf Monitoring
Distributed Tracing

Uptime Data

Uptime
Response Time



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 — 100x19
$ > 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"
sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fee1cf24171 code=0x50000
```

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 — 270x28

```
@c19b776f8156:/usr/share/filebeat -- -ssh gcpbuild ... +  
ea5431889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
ea5446171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
dd911b889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
dd9130171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
e2d609889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
958b37889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
958b4c171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
26787e889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
267893171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
f450fd889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
f45112171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
37fe6f889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
37fe84171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
7b38c5889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
7b38da171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
a39bb4889 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
a39bc9171 code=0x50000  
    gid=0 ses=4294967295 subj=system_u:sys  
client: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
lient: Connection reset by peer  
ection with an open transaction  
onitoring": {"metrics": {"beat": [{"c  
{"ticks":1143011,"time":{"ms":502}  
46816,"memory_alloc":15465384,"mem  
ut":{"events":{"acked":50,"batches  
d":1,"published":50,"total":51}, "l  
sst":{"events":1,"success":1}, "l  
s":25,"success":25}, "process_summary":
```

```
  {"monitoring": {"metrics": {"beat": {"count": 662}, "user": {"ticks": 1143500, "time": {"ms": 489}}, "gc_next": 25381968, "memory_alloc": 17019480, "memnning": 0}, "output": {"events": {"acked": 42, "batch_size": 0, "alive": 42, "published": 42, "total": 42}, "queue": {"array": {"events": 3, "success": 3}, "network": {"events": 3, "success": 3}}}, "system": {}}
```

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

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

The screenshot shows the Elastic Cloud interface with a sidebar of icons on the left and a main dashboard area.

Observability

- APM**: APM automatically collects in-depth performance metrics and errors from inside your applications. [Add APM](#)
- Logs**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. [Add log data](#)
- Metrics**: Collect metrics from the operating system and services running on your servers. [Add metric data](#)

Security

- SIEM**: Centralize security events for interactive investigation in ready-to-go visualizations. [Add events](#)

Visualize and Explore Data

- APM**: Automatically collect in-depth performance metrics. [View details](#)
- Canvas**: Showcase your data in a pixel-perfect way. [View details](#)

Manage and Administer the Elastic Stack

- Console**: Skip cURL and use this JSON interface to work. [View details](#)
- Index Patterns**: Manage the index patterns that help retrieve your data. [View details](#)

Click on the Logging Button

Works the same in the cloud or running the default distribution

The screenshot shows the Elastic Stack interface with several sections:

- Observability** section:
 - Logs**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. This section is highlighted with a yellow box around the "Add log data" button.
 - Metrics**: Collect metrics from the operating system and services running on your servers. Includes "Add metric data" button.
 - SIEM**: Centralize security events for interactive investigation in ready-to-go visualizations. Includes "Add events" button.
- APM**: APM automatically collects in-depth performance metrics and errors from inside your applications. Includes "Add APM" button.
- Data Import Options**:
 - Add sample data: Load a data set and a Kibana dashboard.
 - Upload data from log file: Import a CSV, NDJSON, or log file.
 - Use Elasticsearch data: Connect to your Elasticsearch index.
- Visualize and Explore Data**:
 - APM**: Automatically collect in-depth performance metrics.
 - Canvas**: Showcase your data in a pixel-perfect way.
- Manage and Administer the Elastic Stack**:
 - Console**: Skip cURL and use this JSON interface to work.
 - Index Patterns**: Manage the index patterns that help retrieve your data.

Many choices

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

The screenshot shows the Kibana interface with the title "Add Data to Kibana". The top navigation bar includes icons for Home, Add data, and other settings. Below the title, there are tabs for All, Logging, Metrics, SIEM, and Sample data, with "Logging" selected. The main area displays a grid of log collection options:

- Apache logs**: Collect and parse access and error logs created by the Apache HTTP server.
- Cloudwatch Logs**: Collect Cloudwatch logs with Functionbeat.
- 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.
- Nats logs**: Collect and parse logs created by Nats.
- 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. This option is highlighted with a yellow border.
- Traefik logs**: Collect and parse access logs created by the Traefik Proxy.

Detailed instructions

Context-aware instructions for cloud or on-prem installs

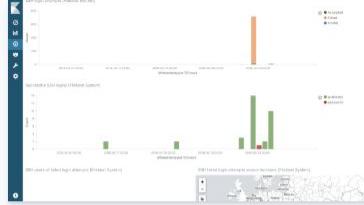
Home / Add data System logs

System logs

The `system` Filebeat module collects and parses logs created by the system logging service of common Unix/Linux based distributions. This module is not available on Windows. [Learn more](#).

[View exported fields](#)

[Self managed](#) [Elastic Cloud](#)



Getting Started

macOS DEB RPM

1 Download and install Filebeat

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

[Copy snippet](#)

```
curl -L -O 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/
```

2 Edit the configuration

Modify `filebeat.yml` to set the connection information:

[Copy snippet](#)

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!

The screenshot shows a documentation page for "Filebeat" under the "Getting Started" section. The top navigation bar includes icons for search, refresh, and user profile, along with links for "Add data" and "System logs". The main content area has a sidebar on the left containing various configuration and monitoring icons. The "macOS" tab is selected in the top navigation bar.

Getting Started

macOS DEB RPM

1 Download and install Filebeat

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

Copy snippet

```
curl -L -o 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/
```

2 Edit the configuration

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

Copy snippet

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

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

3 Enable and configure the system module

From the installation directory, run:

Copy snippet

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

4 Start Filebeat

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/
```

macOS DEB RPM

1 Download and install Filebeat

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

[Copy snippet](#)

```
curl -L -O 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/
```

Steps

Edit the configuration

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

Add data / System logs

macOS DEB RPM

Getting Started

1 Download and install Filebeat

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

`curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-x86_64.tar.gz
tar xzvf filebeat-7.5.0-darwin-x86_64.tar.gz
cd filebeat-7.5.0-darwin-x86_64/`

2 Edit the configuration

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

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

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

3 Enable and configure the system module

From the installation directory, run:

`./filebeat modules enable system`

Modify the settings in the `modules.d/system.yml` file.

4 Start Filebeat

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>"
```

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

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

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

Edit the configuration

Copy the snippet, paste in the password

Terminal — 100x19

```
#===== 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"  ←
```

2 Edit the configuration

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

[Copy snippet](#)

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

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

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!

The screenshot shows a documentation page for setting up the system module with Filebeat. The top navigation bar includes icons for search, refresh, and user profile, along with links for 'Add data' and 'System logs'. The main content area has a sidebar with various system-related icons.

Getting Started

macOS DEB RPM

- 1 Download and install Filebeat**

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

`curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-x86_64.tar.gz
tar xzvf filebeat-7.5.0-darwin-x86_64.tar.gz
cd filebeat-7.5.0-darwin-x86_64/`

- 2 Edit the configuration**

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

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

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

- 3 Enable and configure the system module**

From the installation directory, run:

`./filebeat modules enable system`

Modify the settings in the `modules.d/system.yml` file.

- 4 Start Filebeat**

Enable the system module

Again, just copy and paste the snippet

Terminal — 100x19

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

3 Enable and configure the system module

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

[Copy snippet](#)

Enable the system module

Again, just copy and paste the snippet

Terminal — 100x19

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

3 Enable and configure the system module

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

[Copy snippet](#)

Enable the system module

Check your work

Terminal — 100x19

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

```
# Can also verify
```

3 Enable and configure the system module

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

[Copy snippet](#)

Enable the system module

Check your work

Terminal — 100x19

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

```
# Can also verify
```

```
$ ./filebeat modules list
```

3 Enable and configure the system module

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

[Copy snippet](#)

Enable the system module

All good

Terminal — 100x19

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

```
# Can also verify
```

```
$ ./filebeat modules list  
Enabled:  
system
```

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

3 Enable and configure the system module

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

[Copy snippet](#)

Steps

Start Filebeat

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

The screenshot shows a documentation page for "Filebeat" under the "Getting Started" section. The top navigation bar includes icons for search, refresh, and user profile, along with links for "Add data" and "System logs". The main content area has a sidebar on the left with various icons corresponding to different beats and modules.

Getting Started

macOS DEB RPM

1 Download and install Filebeat

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

[Copy snippet](#)

```
curl -L -O 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/
```

2 Edit the configuration

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

[Copy snippet](#)

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

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

3 Enable and configure the system module

From the installation directory, run:

[Copy snippet](#)

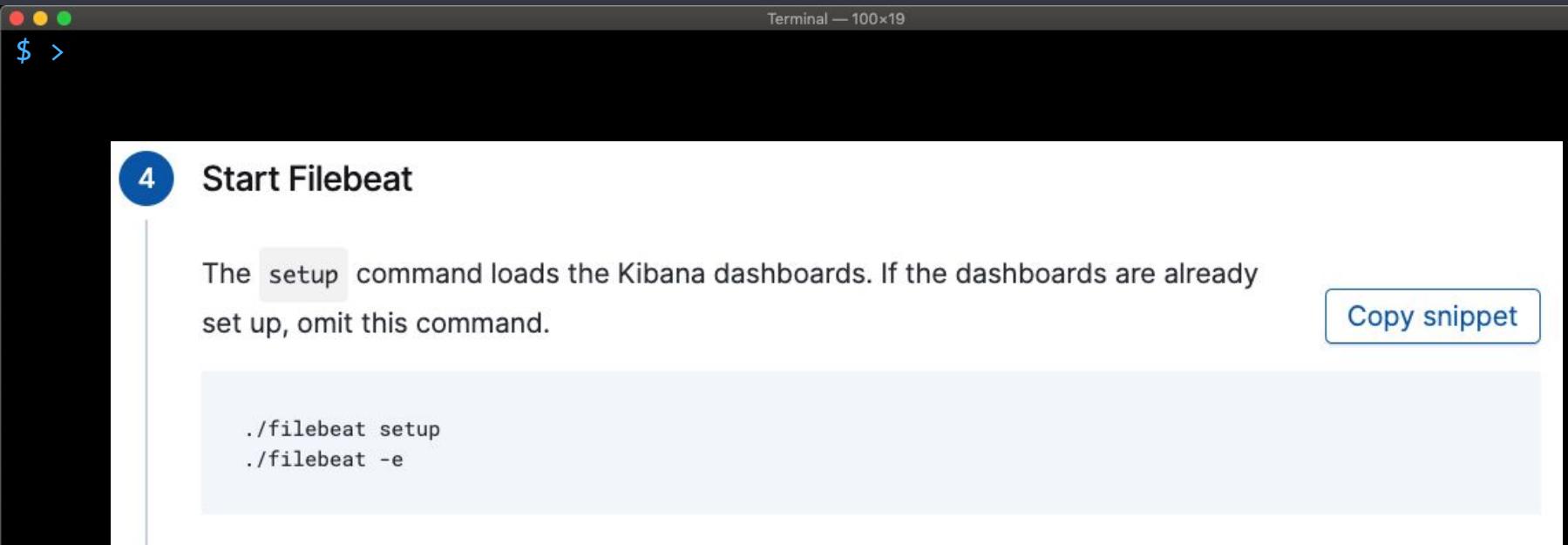
```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

4 Start Filebeat

And start it up!

Startup steps



A screenshot of a macOS terminal window titled "Terminal — 100x19". The window shows a command line with "\$ >" followed by a blank line. Overlaid on the terminal are several UI elements: a blue circular icon with the number "4" indicating a step; the text "Start Filebeat"; a descriptive paragraph about the "setup" command; a "Copy snippet" button; and a code block containing two commands: "./filebeat setup" and "./filebeat -e".

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 — 100x19  
$ ./filebeat setup
```

4 Start Filebeat

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

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

[Copy snippet](#)

First run the setup process

Setup preps dashboards and indices



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

Terminal — 100x19

4 Start Filebeat

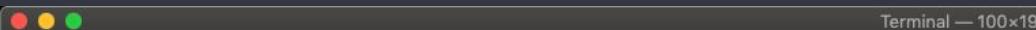
The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

[Copy snippet](#)

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

First run the setup process

Setup preps dashboards and indices



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

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

4 Start Filebeat

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

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

[Copy snippet](#)

Finally, start it!

-e tells it to send messages to console

```
Terminal — 100x19  
$ ./filebeat -e
```

4 Start Filebeat

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

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

[Copy snippet](#)

Finally, start it!

-e tells it to send messages to console

```
Terminal — 100x19  
$ ./filebeat -e
```

```
2019-12-09T18:02:42.500Z INFO instance/beat.go:610 Home 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:618 Beat 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-smith-build"}, "machine": {"type": "n1-standard-8"}, "project": {"id": "elastic-product-marketing"}, "provider": "gcp"}  
2019-12-09T18:02:42.564Z INFO [seccomp] seccomp/seccomp.go:124 Syscall filter successfully  
installed  
(...)
```

4 Start Filebeat

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

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

[Copy snippet](#)

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

Needs for log analytics

Easy setup for variety of log sources

Home / Add data

Add Data to Kibana

All Logging Metrics SIEM Sample data

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

 **Cloudwatch Logs**
Collect Cloudwatch logs with Functionbeat

 **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.

 **Nats logs**
Collect and parse logs created by Nats.

 **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.

Needs for log analytics

Correlating and cross referencing

The screenshot shows a log analysis interface with two main sections: a stream view on the left and a detailed view on the right.

Stream View (Left):

- Header:** Stream, Log Rate (BETA), Settings.
- Search Bar:** Search for log entries... (e.g. host.name:host-1).
- Table Headers:** Timestamp, Message.
- Log Entries:** A list of log entries from January 14, 2020, at 08:37:08.790 to 08:37:09.520. Examples include: [INFO] received ad request (context_words=[Cookware]), [INFO] Cache miss for category: Cookware, [redis.log][verbose] Accepted 10.48.4.11:36760, etc.

Detailed View (Right):

Field	Value
@timestamp	2020-01-14T13:37:08.838Z
_id	1xVFpG8BvYbYXls0t_E1
_index	filebeat-7.5.1-2020.01.14-000048
agent.ephemeral_id	4b0464e0-cf97-498c-a2bb-61cdbaba36b6
agent.hostname	filebeat-6xktz
agent.id	520ddfa4-f182-44c9-b919-2f344cd00ca5
agent.type	filebeat
agent.version	7.5.1
cloud.availability_zone	us-central1-a
cloud.instance.id	2567286355104662140
cloud.instance.name	gke-eden-prod-default-pool-ef9bba0b-5bqx
cloud.machine.type	n1-standard-8
cloud.project.id	elastic-product
cloud.provider	gcp
container.id	f8b2b863ceb9b839f85bf7785d09cf43ac8001e6ecaee45ce3742

Needs for log analytics

Searching, filtering, and highlighting

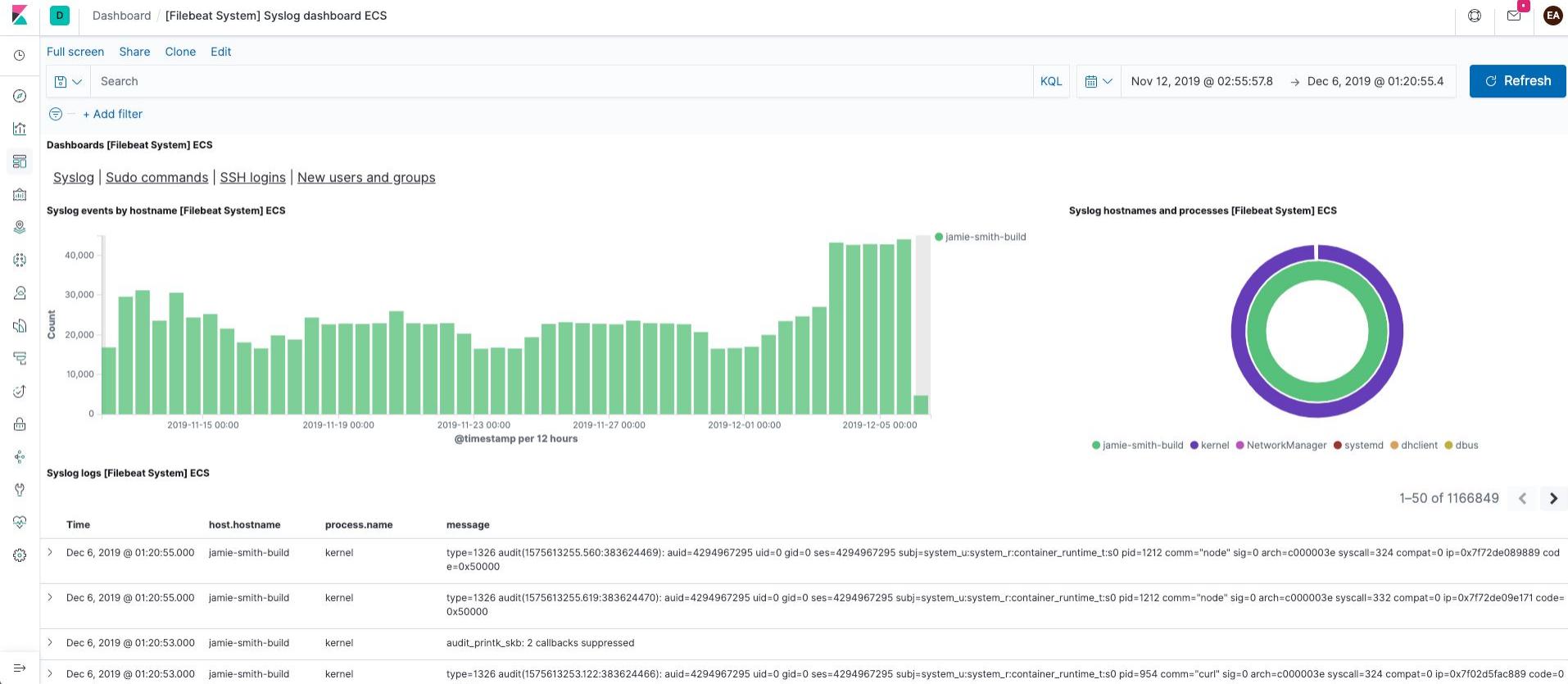
The screenshot shows a log analysis interface with the following features and data:

- Header:** Includes a logo, a 'Logs' tab, and various navigation icons.
- Toolbar:** Contains 'Stream' (selected), 'Log Rate (BETA)', 'Settings', a search bar ('Search for log entries... (e.g. host.name:host-1)'), and a timestamp ('01/14/2020 8:37:08 AM').
- Table:** Displays log entries in a table with columns: 'Timestamp', 'Message', and 'kubernetes.container.name'. The table includes 30 rows of log entries from January 14, 2020, at 08:37:08.790 to 08:37:09.520.
- Timeline:** A vertical timeline on the right side shows the progression of time from 09 PM to 06 PM on January 14, 2020.

Timestamp	Message	kubernetes.container.name
Jan 14, 2020 @ 08:37:08.790	[INFO] received ad request (context_words=[Cookware])	adservice
Jan 14, 2020 @ 08:37:08.790	[INFO] Cache miss for category: Cookware	adservice
Jan 14, 2020 @ 08:37:08.792	[redis.log][verbose] Accepted 10.48.4.11:36760	redis-master
Jan 14, 2020 @ 08:37:08.800	[redis.log][verbose] Client closed connection	redis-master
Jan 14, 2020 @ 08:37:08.811	[INFO] Adding 2 items to cache	adservice
Jan 14, 2020 @ 08:37:08.811	[INFO] Items 9081 now in cache	adservice
Jan 14, 2020 @ 08:37:08.811	[INFO] Returning 2 ads	adservice
Jan 14, 2020 @ 08:37:08.820	[INFO] received conversion request	currencyservice
Jan 14, 2020 @ 08:37:08.823	[INFO] conversion request successful	currencyservice
Jan 14, 2020 @ 08:37:08.829	[INFO] Getting supported currencies...	currencyservice
Jan 14, 2020 @ 08:37:08.836	[DEBUG] request complete	frontend
Jan 14, 2020 @ 08:37:08.838	[INFO] Adding 1 items to cache	adservice
Jan 14, 2020 @ 08:37:08.838	[INFO] Items 9082 now in cache	adservice
Jan 14, 2020 @ 08:37:08.838	[INFO] Returning 1 ads	adservice
Jan 14, 2020 @ 08:37:08.844	[DEBUG] request complete	frontend
Jan 14, 2020 @ 08:37:08.938	[DEBUG] request started	frontend
Jan 14, 2020 @ 08:37:08.946	[DEBUG] view user cart	frontent
Jan 14, 2020 @ 08:37:08.948	[INFO] GetCartAsync called with userId=\"59aee2be-5279-449f-86d0-a40733b41bcd\"	cartservice
Jan 14, 2020 @ 08:37:09.280	[INFO] received conversion request	currencyservice
Jan 14, 2020 @ 08:37:09.304	[INFO] conversion request successful	currencyservice
Jan 14, 2020 @ 08:37:09.340	[INFO] Getting supported currencies...	currencyservice
Jan 14, 2020 @ 08:37:09.347	[INFO] listing products	productcatalogservice
Jan 14, 2020 @ 08:37:09.452	[INFO] [Recv ListRecommendations] product_ids=[u'6E92ZMYYFZ', u'0PUK6V6EV0', u'2ZYFJ3GM2N', u'9SIQT8TOJO', u'OLJCESPC7Z']	recommendationservice
Jan 14, 2020 @ 08:37:09.520	[INFO] Getting product with ID 6E92ZMYYFZ	productcatalogservice

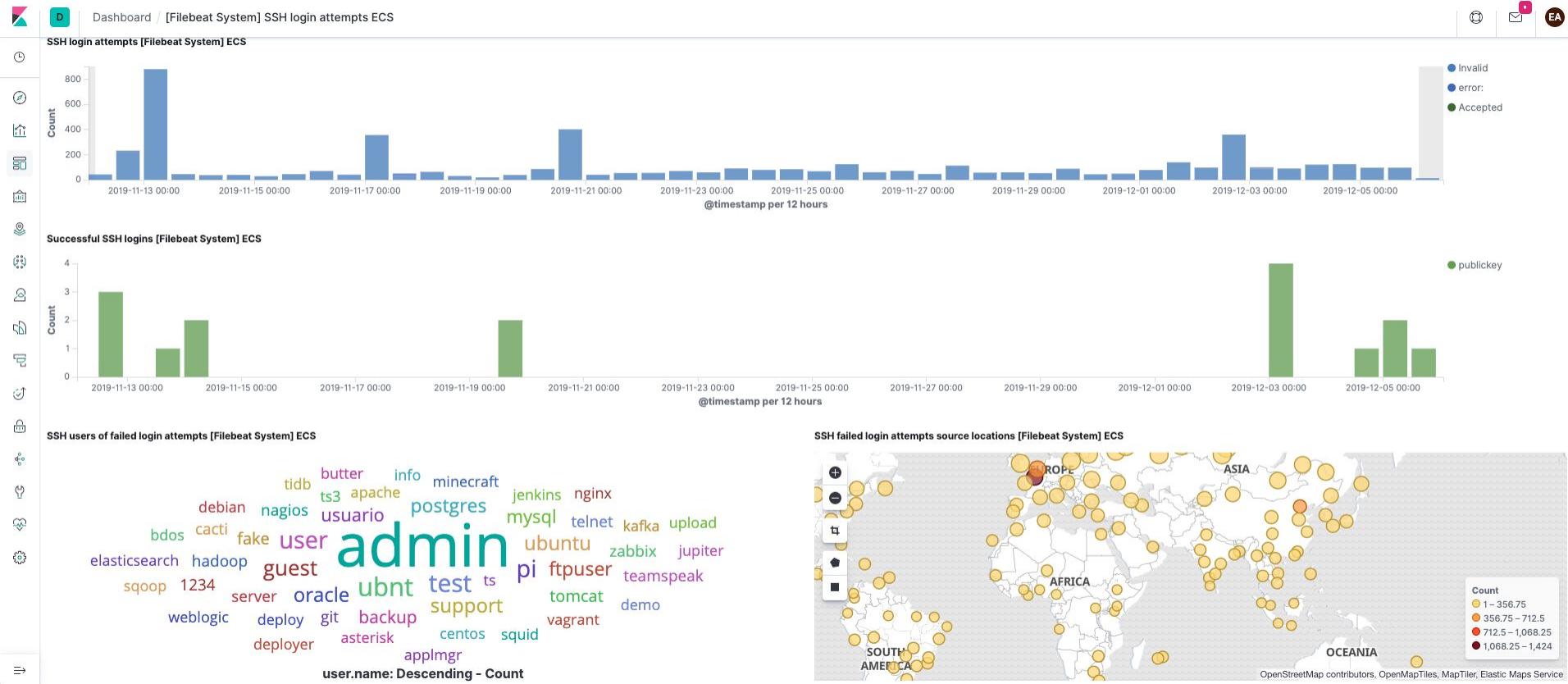
Needs for log analytics

Visualize



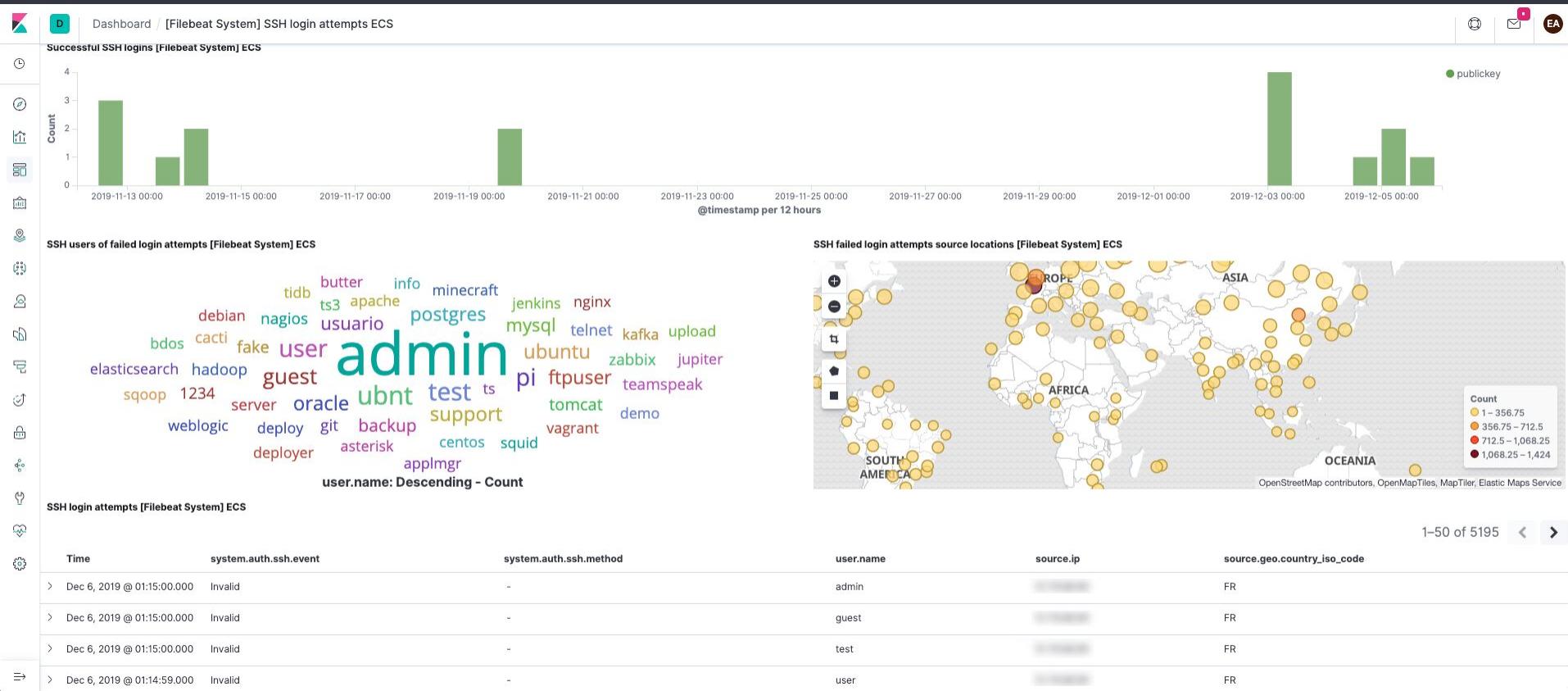
Needs for log analytics

Visualize



Needs for log analytics

Visualize



Anomaly detection and alerting

Can't stare at the screen all day



Needs for log analytics

Flexible retention

The screenshot shows the Elasticsearch Index Lifecycle Policies page in Kibana. The left sidebar includes links for Elasticsearch (Index Management, Index Lifecycle Policies, Rollup Jobs, Transforms, Watcher, Snapshot and Restore, 8.0 Upgrade Assistant), Kibana (Index Patterns, Saved Objects, Spaces, Reporting, Advanced Settings), Logstash (Pipelines), Beats (Central Management), Machine Learning (Jobs list), and Security (Users, Roles). The main content area is titled "Edit index lifecycle policy filebeat-7.5.1". It explains that the policy automates four phases of the index lifecycle. A note states: "You are editing an existing policy. Any changes you make will affect the indices that are attached to this policy. Alternatively, you can save these changes in a new policy." A "Save as new policy" button is available. The "Hot phase" is currently active. The "Enable rollover" checkbox is checked, with a note explaining it adds the new index to the alias. Below are fields for "Maximum index size" (10 gigabytes), "Maximum documents" (1000), and "Maximum age" (6 hours). An "Index priority" section allows setting priorities for recovering indices after a node restart.

Kibana

Elasticsearch

- Index Management
- [Index Lifecycle Policies](#)
- Rollup Jobs
- Transforms
- Watcher
- Snapshot and Restore
- 8.0 Upgrade Assistant

Kibana

- Index Patterns
- Saved Objects
- Spaces
- Reporting
- Advanced Settings

Logstash

- Pipelines

Beats

- Central Management

Machine Learning

- Jobs list

Security

- Users
- Roles

Edit index lifecycle policy filebeat-7.5.1

Use an index policy to automate the four phases of the index lifecycle, from actively writing to the index to deleting it. [Learn about the index lifecycle](#).

You are editing an existing policy. Any changes you make will affect the indices that are attached to this policy. Alternatively, you can save these changes in a new policy.

Save as new policy

Hot phase Active

This phase is required. You are actively querying and writing to your index. For faster updates, you can roll over the index when it gets too big or too old.

Enable rollover
The new index created by rollover is added to the index alias and designated as the write index.
[Learn about rollover](#)

Maximum index size
10 gigabytes

Maximum documents

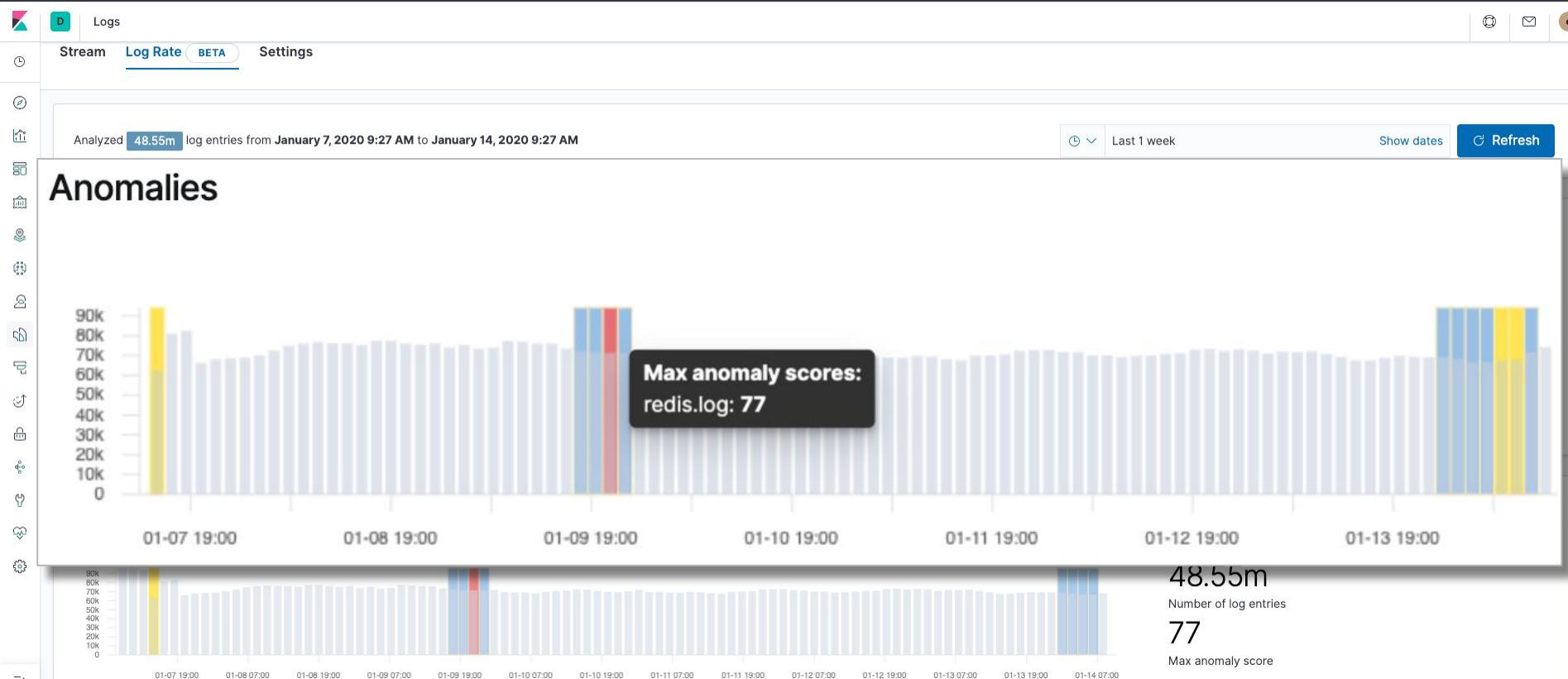
Maximum age
6 hours

Index priority
Set the priority for recovering your indices after a node restart. Indices with higher priorities are recovered before indices with lower priorities. [Learn more](#)

Index priority (optional)

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

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

The screenshot shows the Elastic Stack Home page with several sections:

- Observability** section:
 - APM**: APM automatically collects in-depth performance metrics and errors from inside your applications. [Add APM](#)
 - Logs**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. [Add log data](#)
 - Metrics**: Collect metrics from the operating system and services running on your servers. [Add metric data](#)
- Security** section:
 - SIEM**: Centralize security events for interactive investigation in ready-to-go visualizations. [Add events](#)
- Add sample data**: Load a data set and a Kibana dashboard.
- Upload data from log file**: Import a CSV, NDJSON, or log file.
- Use Elasticsearch data**: Connect to your Elasticsearch index.
- Visualize and Explore Data** section:
 - APM**: Automatically collect in-depth performance metrics. 
 - Canvas**: Showcase your data in a pixel-perfect way. 
- Manage and Administer the Elastic Stack** section:
 - Console**: Skip cURL and use this JSON interface to work. 
 - Index Patterns**: Manage the index patterns that help retrieve your data. 

Many integrations

For example, system metrics

The screenshot shows the Kibana interface with the title "Add Data to Kibana". The top navigation bar includes icons for Home, Add data, and other settings. Below the title, there are tabs for All, Logging, Metrics (which is selected), SIEM, and Sample data. A sidebar on the left contains various icons representing different data sources.

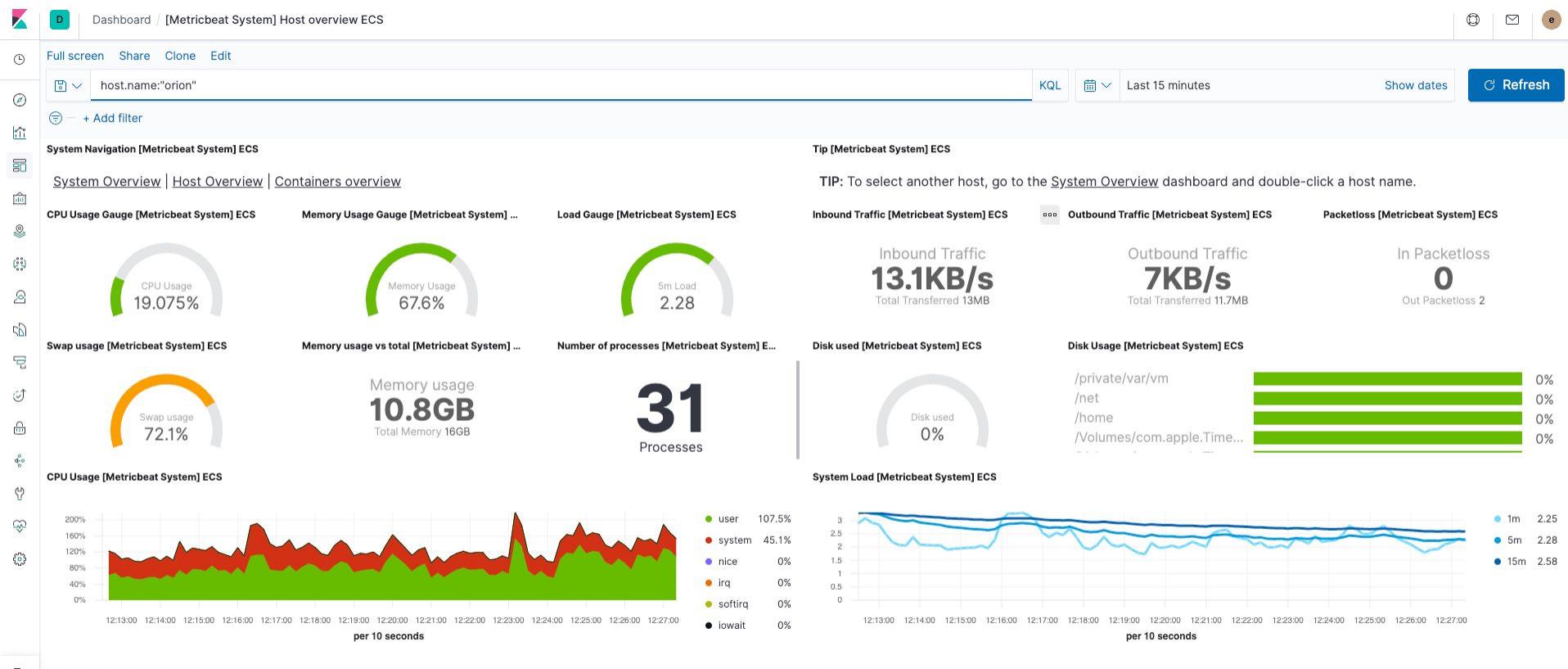
A callout box highlights the "System metrics" section, which is described as "Collect CPU, memory, network, and disk statistics from the host." It also notes that metrics are fetched from a Logstash server.

The main area displays a grid of 18 cards, each representing a different system metric integration:

- Aerospike metrics**: Fetch internal metrics from the Aerospike server.
- Apache metrics**: Fetch internal metrics from the Apache 2 HTTP server.
- AWS metrics**: Fetch monitoring metrics for EC2 instances from the AWS APIs and Cloudwatch.
- Ceph metrics**: Fetch internal metrics from the Ceph server.
- CoreDNS metrics**: Fetch monitoring metrics from the CoreDNS server.
- Couchbase metrics**: Fetch internal metrics from Couchbase.
- CouchDB metrics**: Fetch monitoring metrics from the CouchDB server.
- 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.
- Kafka metrics**: Fetch internal metrics from the Kafka server.
- Kibana metrics**: Fetch internal metrics from Kibana.
- Kubernetes metrics**: Fetch metrics from your Kubernetes installation.
- Memcached metrics**: Fetch internal metrics from the Memcached server.
- Microsoft SQL Server Metrics**: Fetch monitoring metrics from a Microsoft SQL Server instance.
- MongoDB metrics**: Fetch internal metrics from MongoDB.

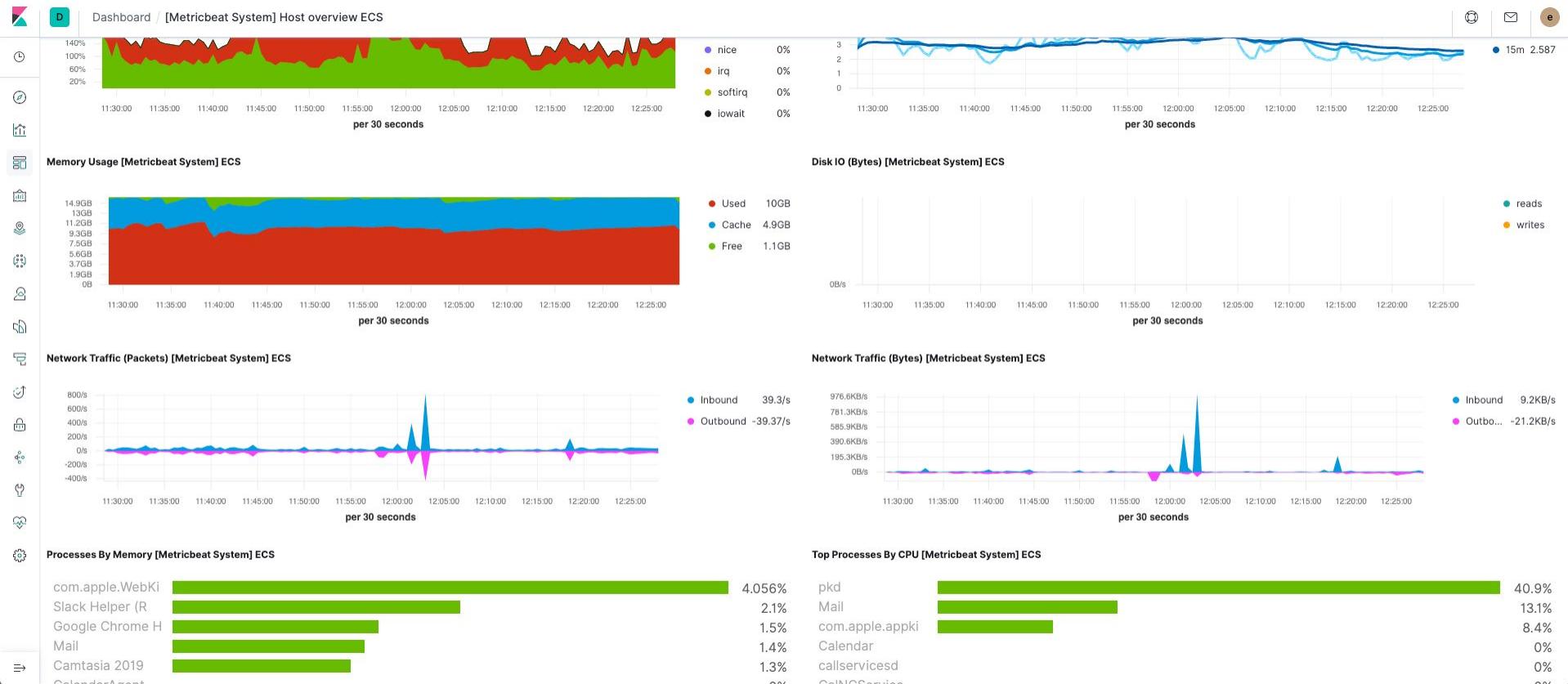
Metrics

Visualizing metrics



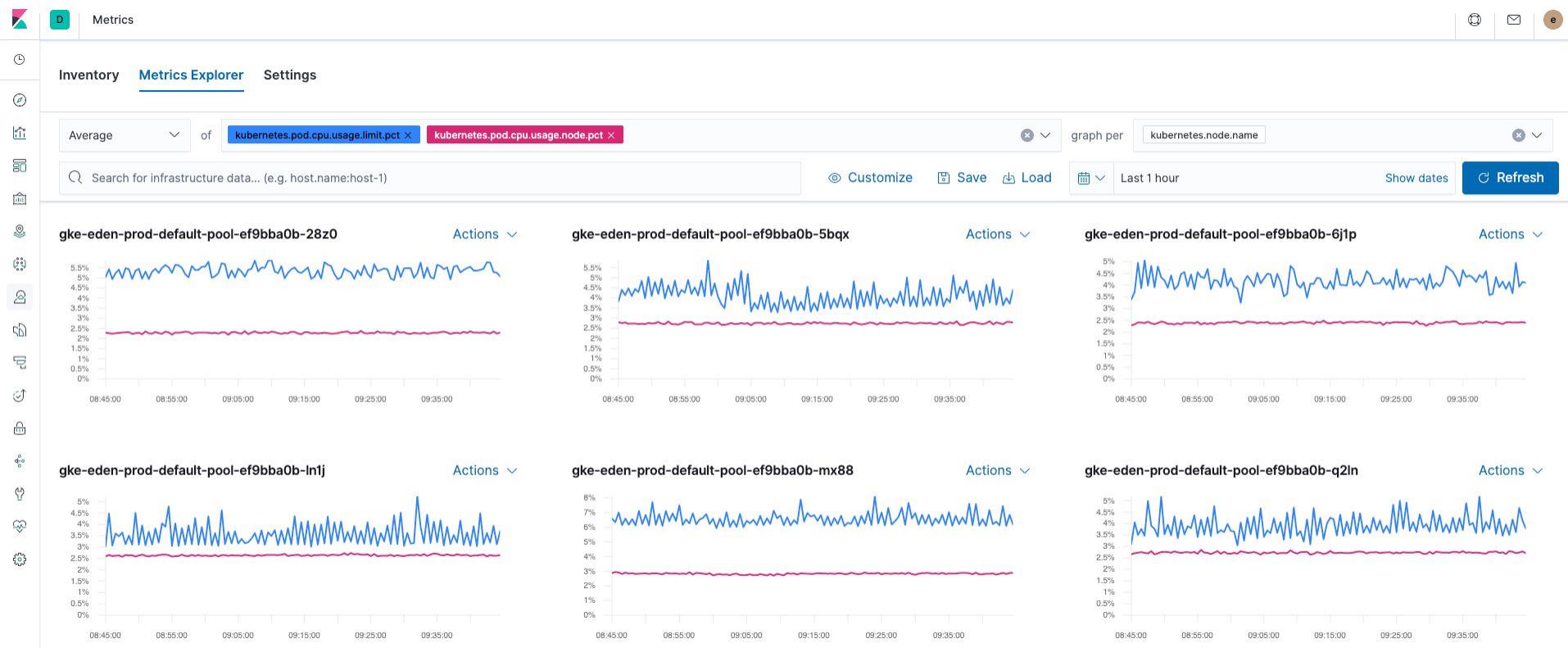
Metrics

Visualizing metrics



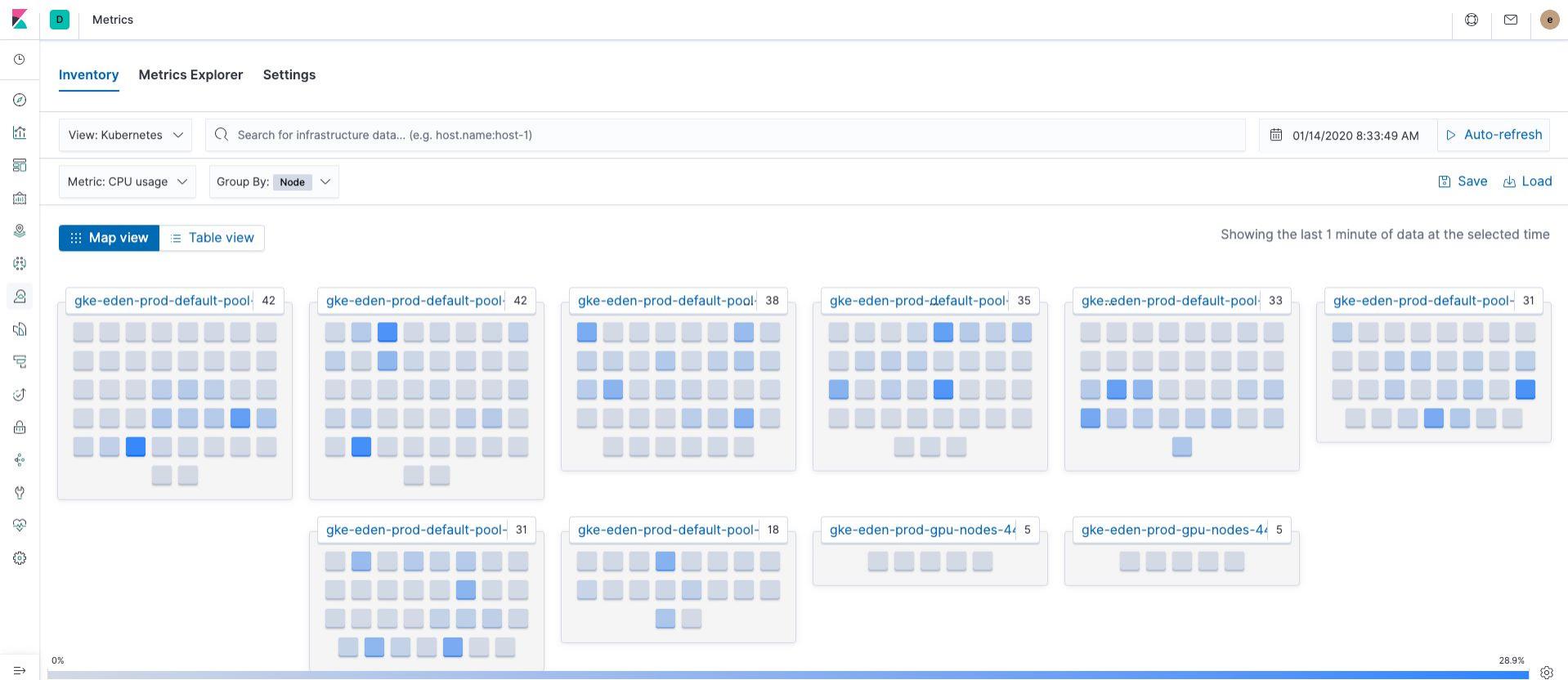
Metrics

Exploring metrics



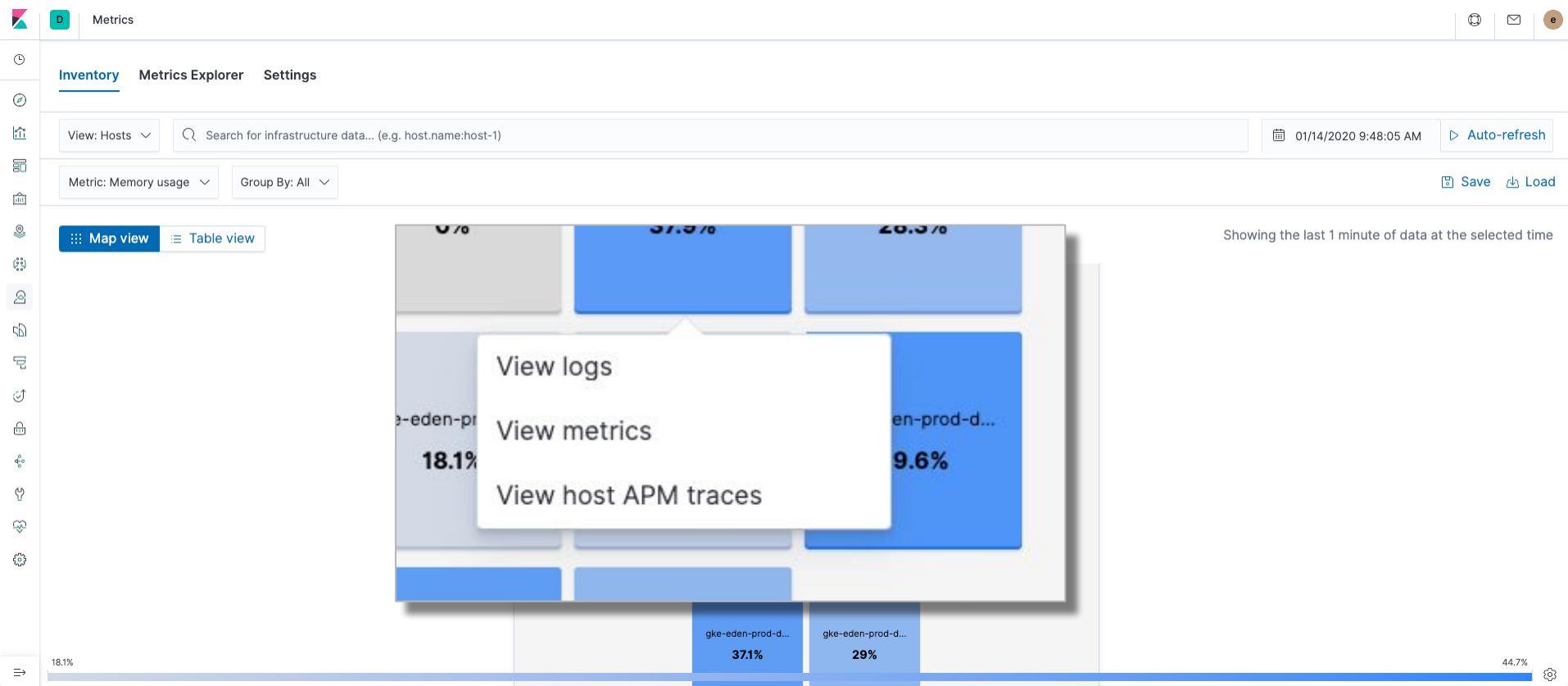
Metrics

Inventory view with multiple perspectives



Integrated Experience

Observability with one datastore



Setting up APM

Instructions in Kibana

K D Home ⚙️ 📧 a

Observability

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

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

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

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

SIEM
Add sample data
Load a data set and a Kibana dashboard

Add log data

Add metric data

Add events

Add sample data
Load a data set and a Kibana dashboard

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

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

APM
Automatically collect in-depth performance metrics

Canvas
Showcase your data in a pixel-perfect way

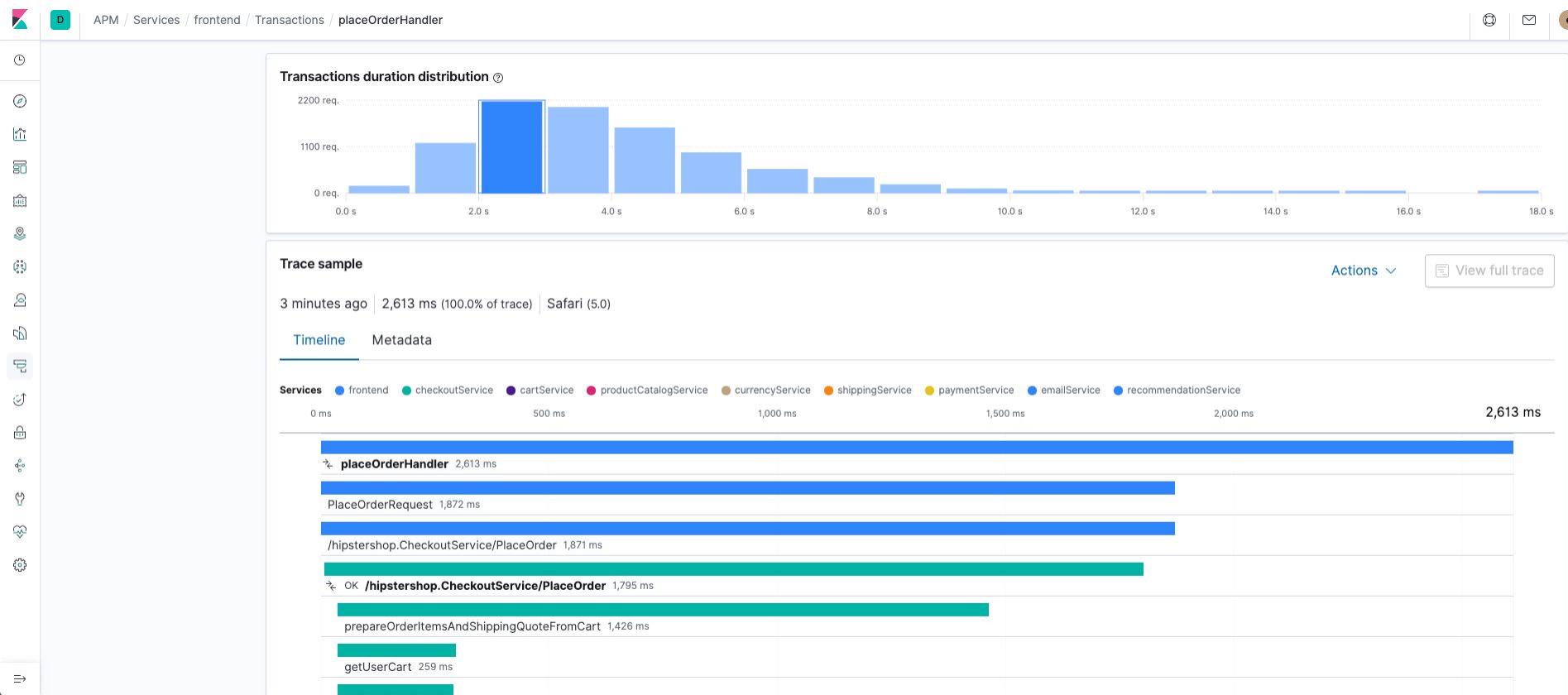
Manage and Administer the Elastic Stack

Console
Skip cURL and use this JSON interface to work

Index Patterns
Manage the index patterns that help retrieve your

Application Performance Monitoring

Distributed Tracing



Uptime Monitoring

Service availability

Uptime

Overview

Last 15 minutes Show dates Refresh

Search monitor IDs, names, and protocol types...

Up Down Location 0 Port 13 Scheme 3

1/22 monitors are down

Down 1 Up 21

Pings over time

Status	Name	URL	Downtime history	Integrations
Up 8 minutes ago	adservice-7bcd956677-7ftmb	tcp://10.48.0.48:10000		...
Down a few seconds ago	apm-server-969d845bc-pjc2d	http://10.48.3.115:8200		...
Up a few seconds ago	Unnamed - auto-http-0X4FA94B0313EE0BC4-78ebd16eaca0565d	https://www.bbc.com		...
Up a few seconds ago	Unnamed - auto-http-0X4FA94B0313EE0BC4-c7eca2f6ea089820	https://github.com		...
Up a few seconds ago	Unnamed - auto-http-0X4FA94B0313EE0BC4-debdfecc4c62e9997	https://demo.elastic.co/status		...
Up a few seconds ago	Unnamed - auto-http-0X4FA94B0313EE0BC4-f2bd00f715add916	https://www.elastic.co		...

Uptime Monitoring

Service availability

D Uptime

7/33 monitors are down

● Down 7
● Up 25

Pings over time

Monitor status

Status	Name	URL	Downtime history	Integrations
● Up a few seconds ago	Unnamed - auto-http-0X14D5C52E77FA69FF	https://www.elastic.co/		... ▼
● Up a few seconds ago	Unnamed - auto-http-0X1BEDFC9AB574F394	http://192.168.64.11:3000		... ▼
● Down a few seconds ago	Website Monitor - Infra Error	https://www.elastic.co/products/infrastructure-monitoring		... ▼
● Up a few seconds ago	NodeJS	http://opbeans-node:3000/api/customers		... ▼
● Up a few seconds ago	NodeJS	http://opbeans-node:3000/api/stats		... ▼
● Up a few seconds ago	NodeJS	http://opbeans-node:3000/api/orders		... ▼
● Down a few seconds ago	SecurityContents	https://www.elastic.co/products/siem		... ▼
● Up	Unnamed - auto-http-0X41B780B30A375E3D	http://192.168.64.12:3000		... ▼

Uptime Monitoring

Integrated experience

D Uptime

7/33 monitors are down

● Down 7
● Up 25

Pings over time

Check APM for domain

Show host metrics

Show pod metrics

Show container metrics

Show host logs

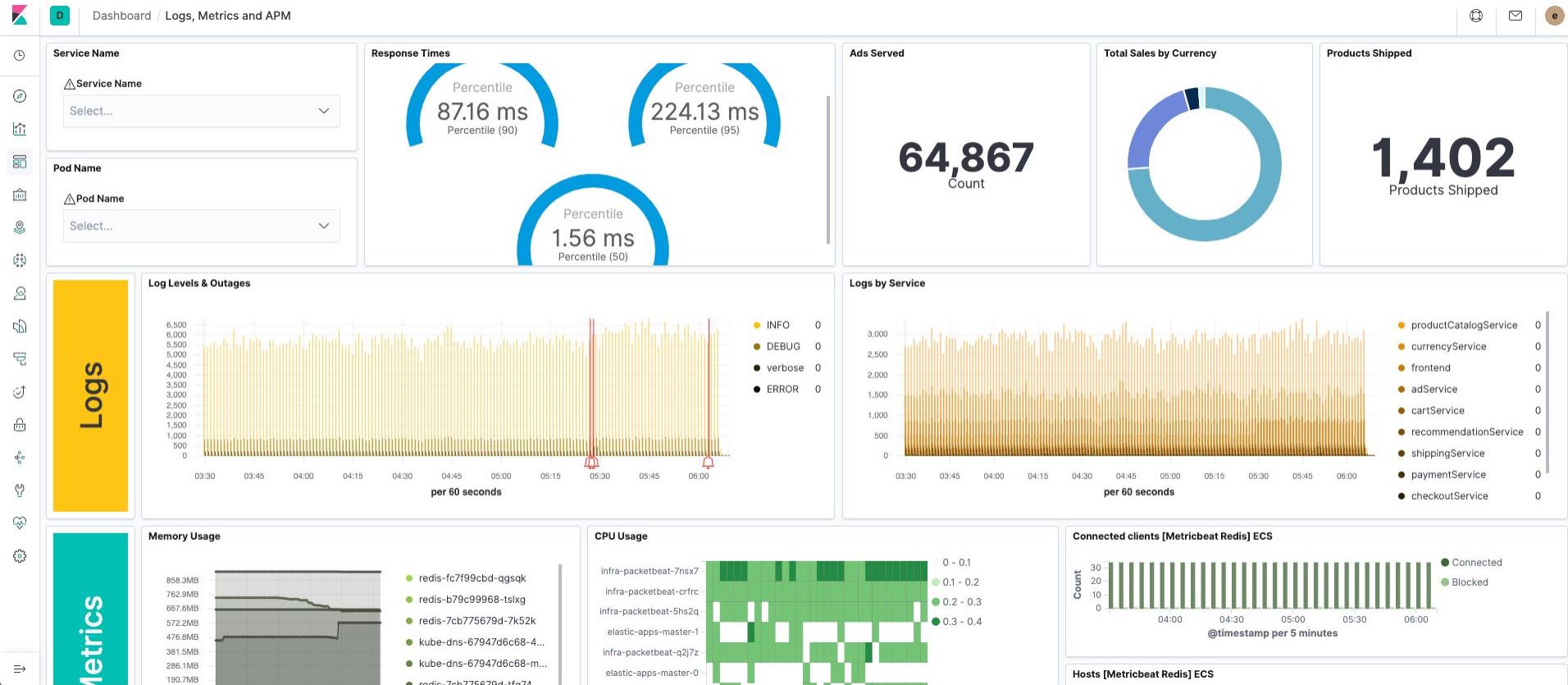
Show pod logs

Show container logs

Status	Name	URL	Downtime history
● Up a few seconds ago	Unnamed - auto-http-0X14D5C52E77FA69FF	https://www.elastic.co/	
● Up a few seconds ago	Unnamed - auto-http-0X1BEDFC9AB574F394	http://192.168.64.11:3000	
● Down a few seconds ago	Website Monitor - Infra Error	https://www.elastic.co/products/infrastructure-monitoring	
● Up a few seconds ago	NodeJS	http://opbeans-node:3000/api/customers	
● Up a few seconds ago	NodeJS	http://opbeans-node:3000/api/stats	
● Up a few seconds ago	NodeJS	http://opbeans-node:3000/api/orders	
● Down a few seconds ago	SecurityContents	https://www.elastic.co/products/siem	
● Up	Unnamed - auto-http-0X41B780B30A375E3D	http://192.168.64.12:3000	

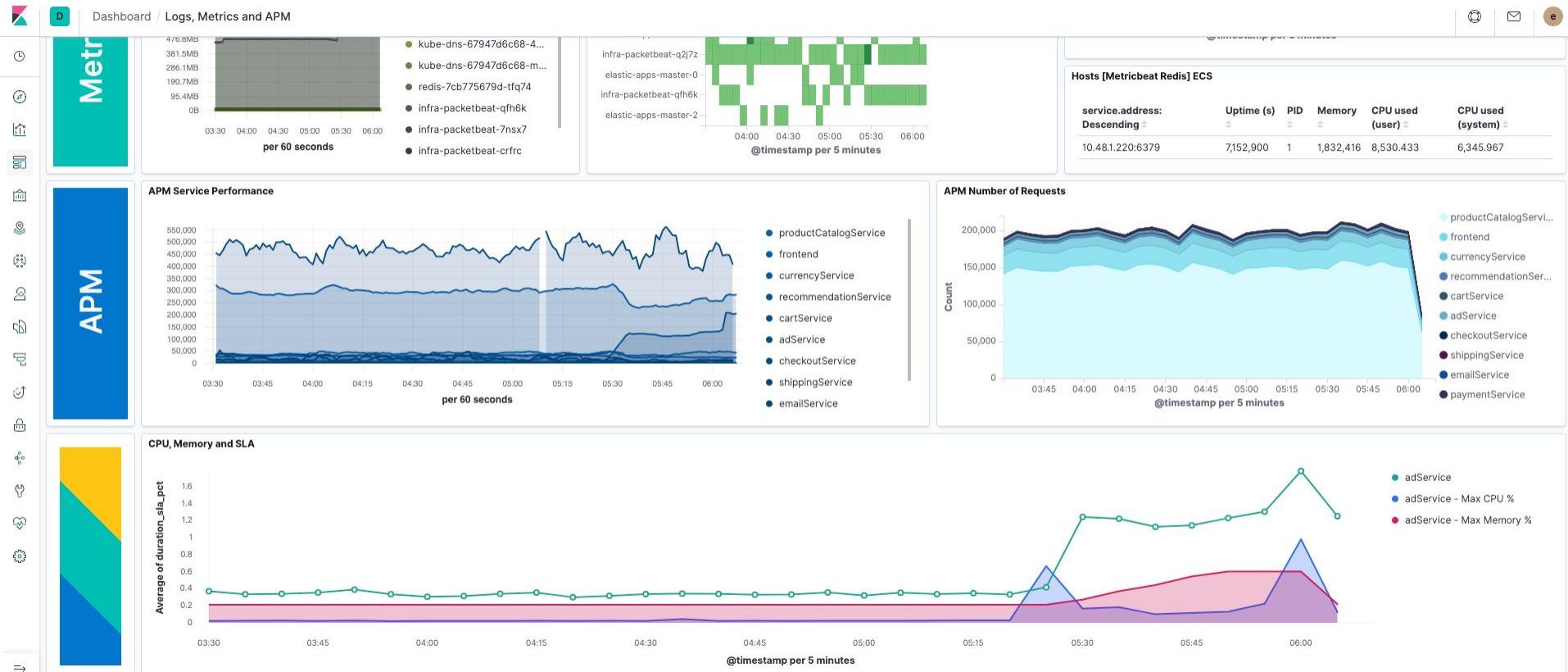
Integrated Experience

Observability with one datastore



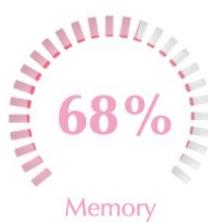
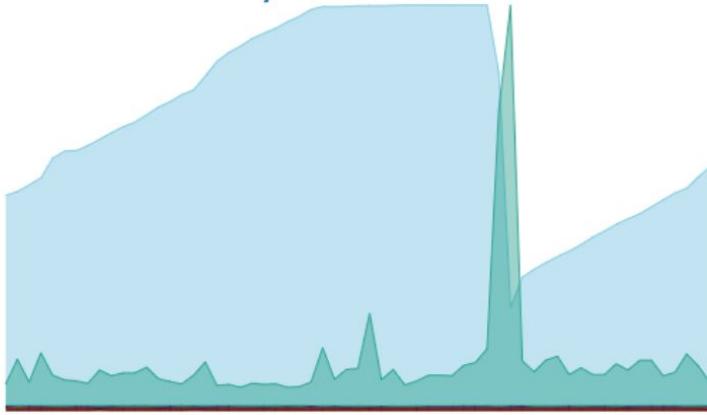
Integrated Experience

Observability with one datastore



Deployment Observability

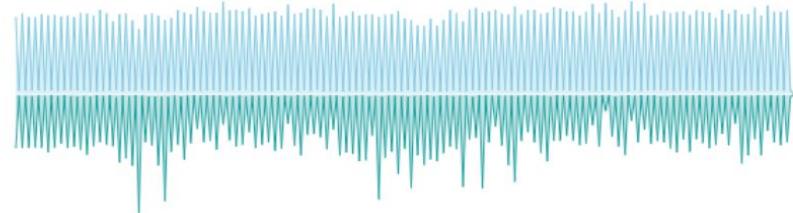
CPU/Memory



Network

Traffic In

Traffic Out



Disk IO

Read

Write



Services

10

Containers

141

Errors

19413

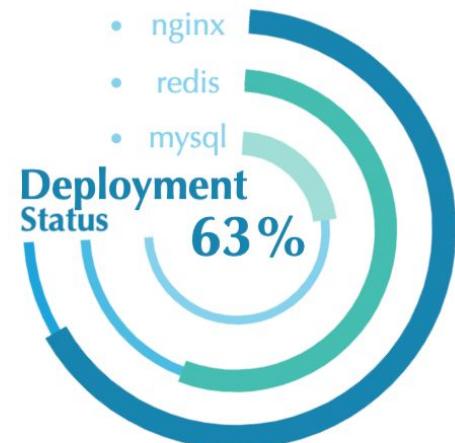
Pods

70

- nginx
- redis
- mysql

Deployment Status

63%



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

The screenshot shows a sidebar with various icons and a main content area titled "Getting Started". The "macOS" tab is selected. The content is divided into four numbered steps:

- 1 Download and install Filebeat**

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

```
curl -L -o https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-x86_64.tar.gz
tar xzvf filebeat-7.5.0-darwin-x86_64.tar.gz
cd filebeat-7.5.0-darwin-x86_64/
```

[Copy snippet](#)
- 2 Edit the configuration**

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

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

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

[Copy snippet](#)
- 3 Enable and configure the system module**

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

[Copy snippet](#)
- 4 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

The screenshot shows the Elasticsearch 'Edit role' interface. At the top, it displays the role name 'beats_writer' and its associated 'Index Management' privilege. Below this, the 'Cluster privileges' section lists actions: 'monitor', 'read_ilm', 'manage_index_templates', and 'manage_pipeline'. The 'Index privileges' section is expanded, showing 'Indices' set to '*beat-*' and 'Privileges' set to 'index', 'view_index_metadata', and 'create_index'. There are also options to 'Grant access to specific fields' and 'Grant read privileges to specific documents'.

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

The screenshot shows the Elasticsearch Management interface with the 'Management / Users' tab selected. On the left, there's a sidebar with icons for Elasticsearch, Index Management, Index Lifecycle Policies, Rollup Jobs, Transforms, Watcher, Snapshot and Restore, 8.0 Upgrade Assistant, Kibana, Index Patterns, and Saved Objects. The main area is titled 'Users' with a search bar containing 'beats'. A table lists one user: 'Beats Writer' with 'User Name' 'beats-writer', 'Email Address' 'na@na.com', and 'Roles' 'beats_system, beats_writer'. A 'Create user' button is in the top right.

This screenshot is similar to the one above, but a modal window is overlaid on the bottom right. The modal has a title 'Users' and a search bar with 'beats'. It contains the same user entry as the main table. At the bottom of the modal, there's a 'Security' section with three tabs: 'Users' (which is highlighted in blue), 'Roles', and 'API Keys'. An orange arrow points from the bottom left towards the 'Users' tab in the modal.



Set up the keystore

Hiding credentials for beats-writer

```
Terminal — 100x19
$ >./filebeat keystore
Manage secrets keystore

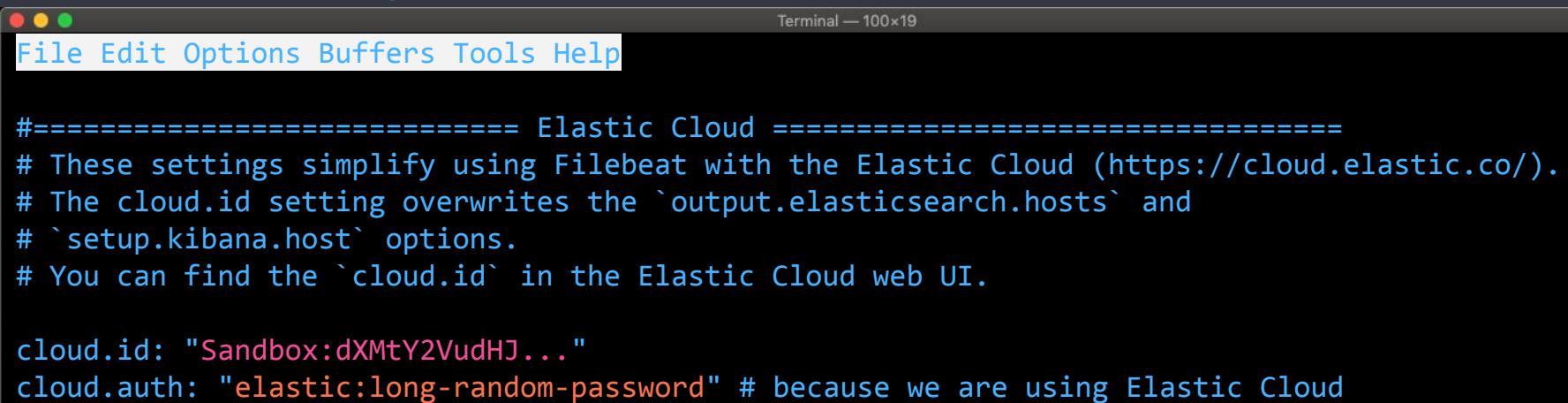
Usage:
  filebeat keystore [command]

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



A screenshot of a terminal window titled "Terminal — 100x19". The window shows a configuration file for Filebeat. The file starts with a header "#===== Elastic Cloud =====" followed by comments explaining the use of Elastic Cloud settings. It then defines "cloud.id" and "cloud.auth" variables. The "cloud.id" value is a placeholder string starting with "Sandbox:", and the "cloud.auth" value is a placeholder string starting with "elastic:long-random-password".

```
#===== 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
```

Parameterize the user

Had the user & password hardcoded

```
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
```



And the password

No more plain text!

```
Terminal — 100x19
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
```



Starts the same way

Automatically picks up the keystore

```
Terminal — 100x19  
$ ./filebeat -e
```

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
```

Finally, start it!

assumes that you've run setup

```
Terminal — 100x19
```

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

```
2019-12-09T18:02:42.500Z INFO instance/beat.go:610 Home 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:618 Beat 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-smith-build"}, "machine": {"type": "n1-standard-8"}, "project": {"id": "elastic-product-marketing"}, "provider": "gcp"}  
2019-12-09T18:02:42.564Z INFO [seccomp] seccomp/seccomp.go:124 Syscall filter successfully  
installed  
(...)
```

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
```

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!

