elastic

Introduction to Logging with the ELK Stack

Amy Ghate
Solutions Architect

logs

+

metrics

+

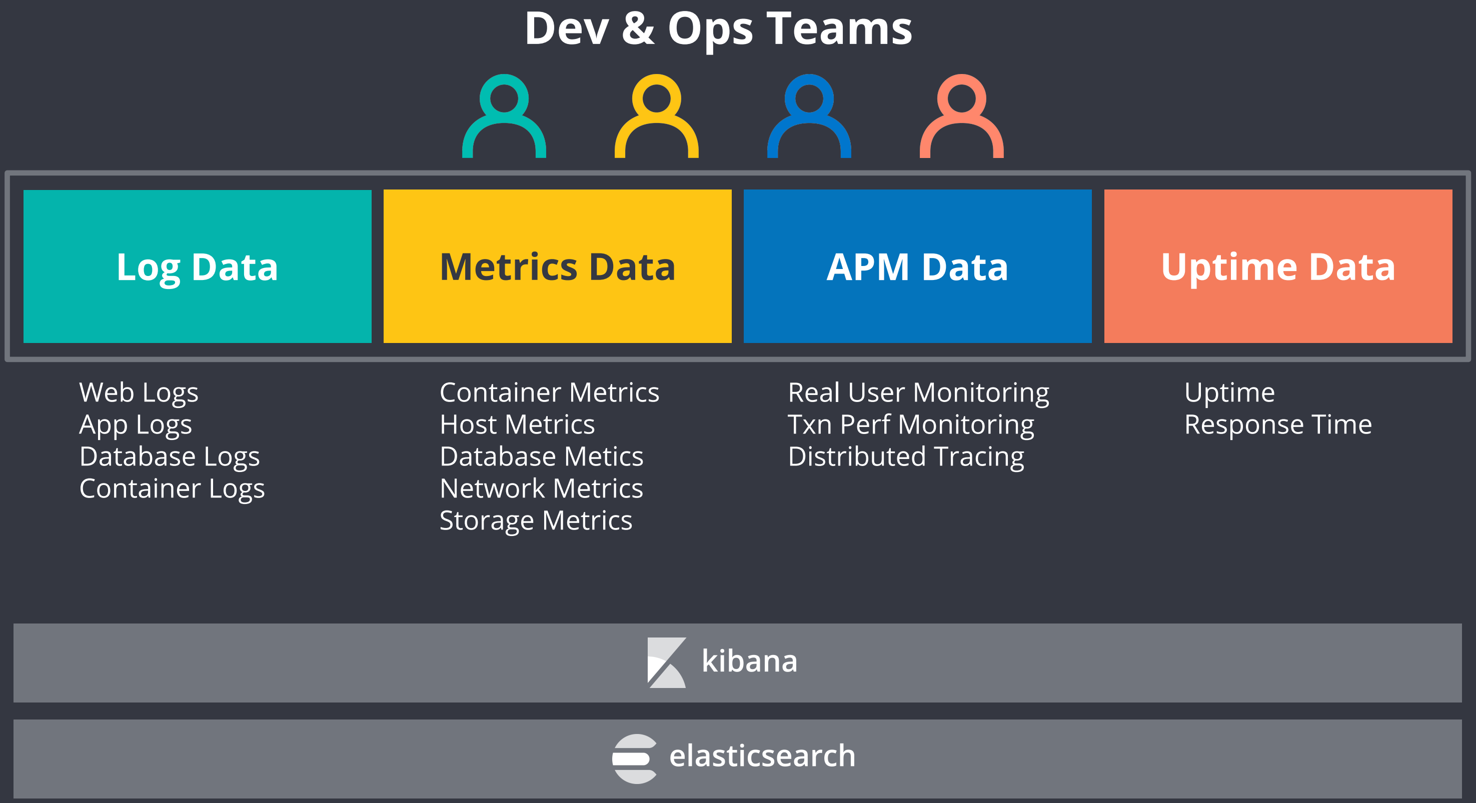
apm

=

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 Metics
Network Metrics
Storage Metrics

APM Data

Real User Monitoring
Txn Perf Monitoring
Distributed Tracing

Uptime Data

Uptime
Response Time

kibana

elasticsearch

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

elastic

Agenda

Challenges with log analytics

1 Challenges with log analytics

2 Sending logs to Elasticsearch

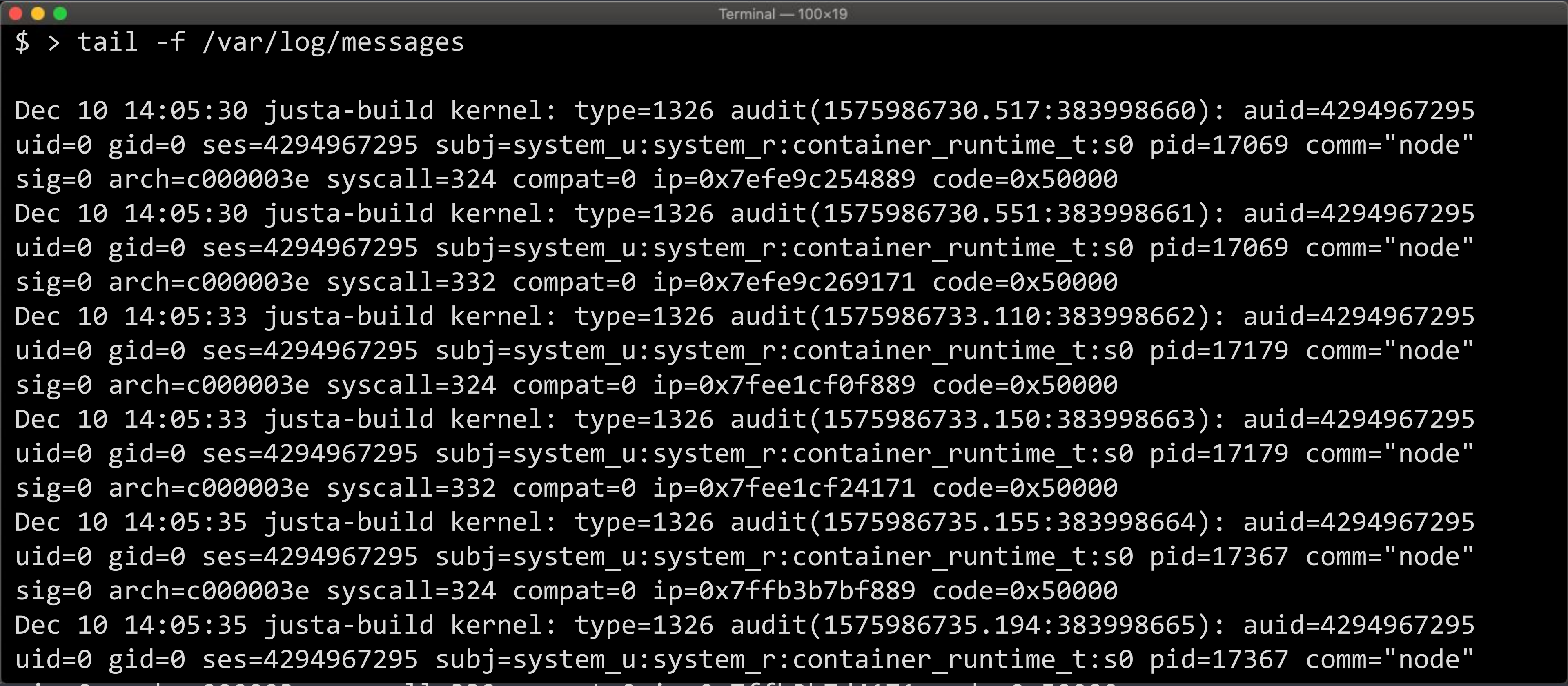
3 Beyond logging: Observability

4 Leveraging Elastic security

elastic

Logs for one host or app

This is fairly straightforward

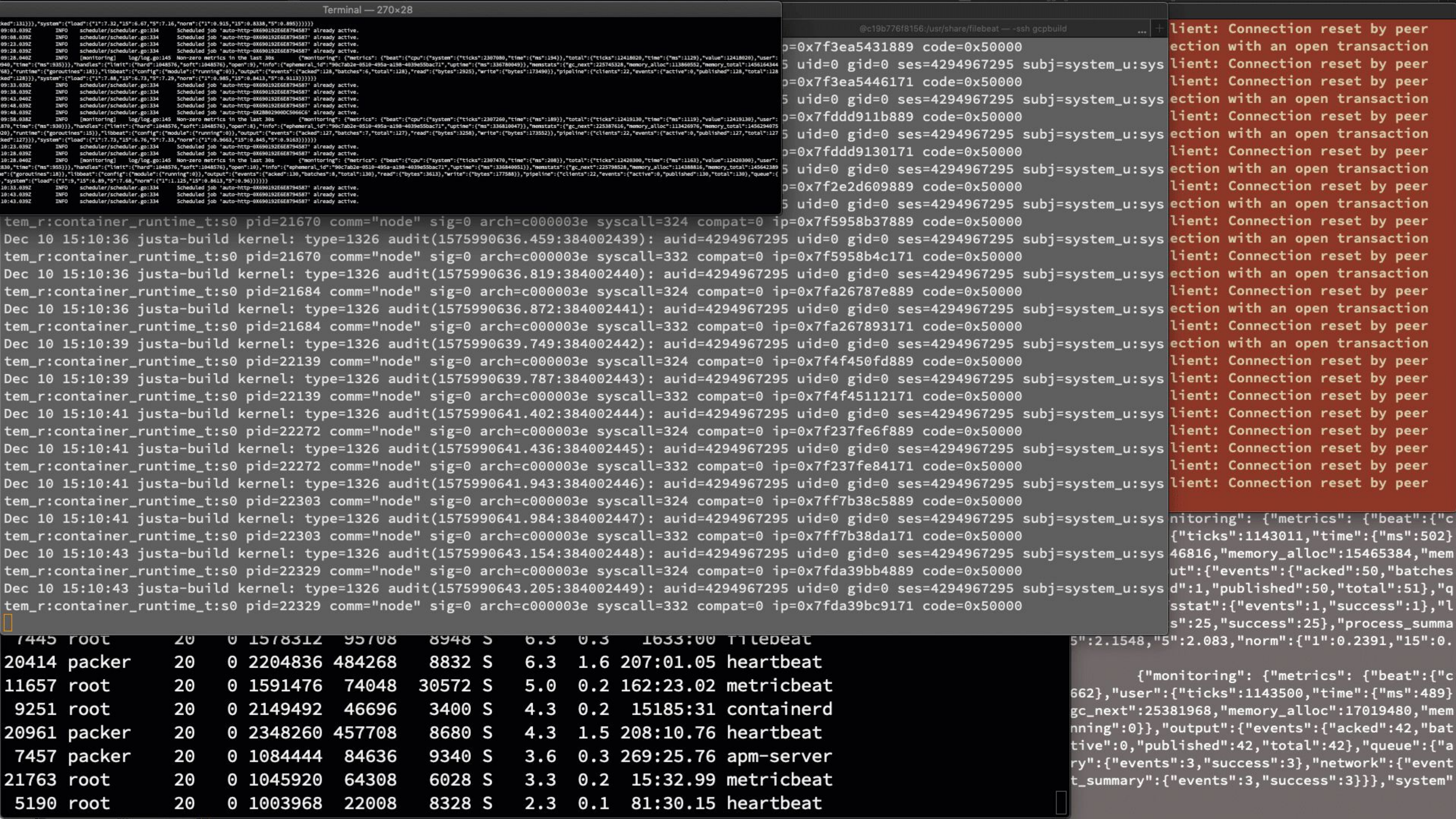


```
$ > tail -f /var/log/messages

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

```
ked":131}}},"system":{"load":{"1":7.32,"15":6.67,"5":7.16,"norm":{"1":0.915,"15":0.8338,"5":0.895}}}}}}
09:03.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:08.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307080,"time":{"ms":194}},"total":{"ticks":12418020,"time":{"ms":1129},"value":12418020},"user":
940,"time":{"ms":935}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":9},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336780049}},"memstats":{"gc_next":225745328,"memory_alloc":113860552,"memory_total":1456164344
68},"runtime":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":128,"batches":6,"total":128},"read":{"bytes":2925},"write":{"bytes":173490}},"pipeline":{"clients":22,"events":{"active":0,"published":128,"total":128
ked":128}}},"system":{"load":{"1":7.88,"15":6.73,"5":7.29,"norm":{"1":0.985,"15":0.8413,"5":0.9113}}}}}}
09:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:38.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:43.040Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X2BB02900DC5066C6' already active.
09:58.038Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307260,"time":{"ms":189}},"total":{"ticks":12419130,"time":{"ms":1119},"value":12419130},"user":
870,"time":{"ms":930}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":8},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336810047}},"memstats":{"gc_next":225387616,"memory_alloc":113426976,"memory_total":1456294075
20},"runtime":{"goroutines":15}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":127,"batches":7,"total":127},"read":{"bytes":3258},"write":{"bytes":173552}},"pipeline":{"clients":22,"events":{"active":0,"published":127,"total":127
ked":127}}},"system":{"load":{"1":7.73,"15":6.76,"5":7.33,"norm":{"1":0.9663,"15":0.845,"5":0.9163}}}}}}
10:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307470,"time":{"ms":208}},"total":{"ticks":12420300,"time":{"ms":1163},"value":12420300},"user":
830,"time":{"ms":955}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":10},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336840051}},"memstats":{"gc_next":225798528,"memory_alloc":114388816,"memory_total":145642389
e":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":130,"batches":8,"total":130},"read":{"bytes":3613},"write":{"bytes":177588}},"pipeline":{"clients":22,"events":{"active":0,"published":130,"total":130},"queue":{
,"system":{"load":{"1":9,"15":6.89,"5":7.68,"norm":{"1":1.125,"15":0.8613,"5":0.96}}}}}}
10:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
```

@c19b776f8156:/usr/share/filebeat — -ssh gcpbuild

```
p=0x7f3ea5431889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f3ea5446171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7fddd911b889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7fddd9130171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f2e2d609889 code=0x50000
5 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
```

```
lient: Connection reset by peer
ection with an open transaction
lient: Connection reset by peer
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
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
```

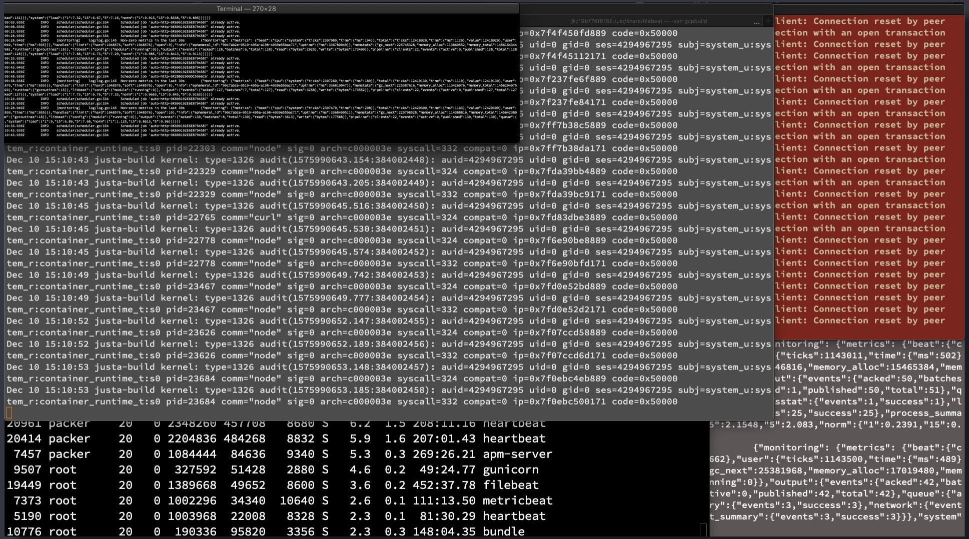
```
 7445 root      20   0 1578312  95708   8948 S   6.3  0.3   1633:00 filebeat
20414 packer    20   0 2204836 484268   8832 S   6.3  1.6 207:01.05 heartbeat
11657 root      20   0 1591476  74048  30572 S   5.0  0.2 162:23.02 metricbeat
 9251 root      20   0 2149492  46696   3400 S   4.3  0.2  15185:31 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
```

```
nitoring": {"metrics": {"beat":{"c
{"ticks":1143011,"time":{"ms":502}
46816,"memory_alloc":15465384,"mem
ut":{"events":{"acked":50,"batches
d":1,"published":50,"total":51},"q
sstat":{"events":1,"success":1},"l
s":25,"success":25},"process_summa
5":2.1548,"5":2.083,"norm":{"1":0.2391,"15":0.

      {"monitoring": {"metrics": {"beat":{"c
662},"user":{"ticks":1143500,"time":{"ms":489}
gc_next":25381968,"memory_alloc":17019480,"mem
nning":0}},"output":{"events":{"acked":42,"bat
tive":0,"published":42,"total":42},"queue":{"a
ry":{"events":3,"success":3},"network":{"event
t_summary":{"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



```
ked":131}}},"system":{"load":{"1":7.32,"15":6.67,"5":7.16,"norm":{"1":0.915,"15":0.8338,"5":0.895}}}}}
09:03.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:08.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307080,"time":{"ms":194}},"total":{"ticks":12418020,"time":{"ms":1129},"value":12418020},"user":
940,"time":{"ms":935}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":9},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336780049}},"memstats":{"gc_next":225745328,"memory_alloc":113860552,"memory_total":1456164344
68},"runtime":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":128,"batches":6,"total":128},"read":{"bytes":2925},"write":{"bytes":173490}},"pipeline":{"clients":22,"events":{"active":0,"published":128,"total":128
ked":128}}},"system":{"load":{"1":7.88,"15":6.73,"5":7.29,"norm":{"1":0.985,"15":0.8413,"5":0.9113}}}}}
09:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:38.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:43.040Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X2B802900DC5066C6' already active.
09:58.038Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307260,"time":{"ms":189}},"total":{"ticks":12419130,"time":{"ms":1119},"value":12419130},"user":
870,"time":{"ms":930}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":8},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336810047}},"memstats":{"gc_next":225387616,"memory_alloc":113426976,"memory_total":1456294075
20},"runtime":{"goroutines":15}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":127,"batches":7,"total":127},"read":{"bytes":3258},"write":{"bytes":173552}},"pipeline":{"clients":22,"events":{"active":0,"published":127,"total":127
ked":127}}},"system":{"load":{"1":7.73,"15":6.76,"5":7.33,"norm":{"1":0.9663,"15":0.845,"5":0.9163}}}}}
10:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307470,"time":{"ms":208}},"total":{"ticks":12420300,"time":{"ms":1163},"value":12420300},"user":
830,"time":{"ms":955}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":10},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336840051}},"memstats":{"gc_next":225798528,"memory_alloc":114388816,"memory_total":145642389
e":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":130,"batches":8,"total":130},"read":{"bytes":3613},"write":{"bytes":177588}},"pipeline":{"clients":22,"events":{"active":0,"published":130,"total":130},"queue":{
,"system":{"load":{"1":9,"15":6.89,"5":7.68,"norm":{"1":1.125,"15":0.8613,"5":0.96}}}}}
10:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
```

```
p=0x7f4f450fd889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f4f45112171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f237fe6f889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f237fe84171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7ff7b38c5889 code=0x50000
5 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
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.516:384002450): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22765 comm="curl" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fd83dbe3889 code=0x50000
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.530:384002451): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22778 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f6e90be8889 code=0x50000
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.574:384002452): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22778 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f6e90bfd171 code=0x50000
Dec 10 15:10:49 justa-build kernel: type=1326 audit(1575990649.742:384002453): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23467 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fd0e52bd889 code=0x50000
Dec 10 15:10:49 justa-build kernel: type=1326 audit(1575990649.777:384002454): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23467 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fd0e52d2171 code=0x50000
Dec 10 15:10:52 justa-build kernel: type=1326 audit(1575990652.147:384002455): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23626 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f07ccd58889 code=0x50000
Dec 10 15:10:52 justa-build kernel: type=1326 audit(1575990652.189:384002456): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23626 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f07ccd6d171 code=0x50000
Dec 10 15:10:53 justa-build kernel: type=1326 audit(1575990653.148:384002457): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23684 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f0ebc4eb889 code=0x50000
Dec 10 15:10:53 justa-build kernel: type=1326 audit(1575990653.185:384002458): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23684 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f0ebc500171 code=0x50000
```

```
lient: Connection reset by peer
ection with an open transaction
lient: Connection reset by peer
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
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
```

```
nitoring": {"metrics": {"beat":{"c
{"ticks":1143011,"time":{"ms":502}
46816,"memory_alloc":15465384,"mem
ut":{"events":{"acked":50,"batches
d":1,"published":50,"total":51},"q
sstat":{"events":1,"success":1},"l
s":25,"success":25},"process_summa
5":2.1548,"5":2.083,"norm":{"1":0.2391,"15":0.

       {"monitoring": {"metrics": {"beat":{"c
662},"user":{"ticks":1143500,"time":{"ms":489}
gc_next":25381968,"memory_alloc":17019480,"mem
nning":0}},"output":{"events":{"acked":42,"bat
tive":0,"published":42,"total":42},"queue":{"a
ry":{"events":3,"success":3},"network":{"event
t_summary":{"events":3,"success":3}}},"system"
```

```
20961 packer    20   0 2348260 457708   8680 S   6.2  1.5 208:11.16 heartbeat
20414 packer    20   0 2204836 484268   8832 S   5.9  1.6 207:01.43 heartbeat
 7457 packer    20   0 1084444  84636   9340 S   5.3  0.3 269:26.21 apm-server
 9507 root      20   0  327592  51428   2880 S   4.6  0.2  49:24.77 gunicorn
19449 root      20   0 1389668  49652   8600 S   3.6  0.2 452:37.78 filebeat
 7373 root      20   0 1002296  34340  10640 S   2.6  0.1 111:13.50 metricbeat
 5190 root      20   0 1003968  22008   8328 S   2.3  0.1  81:30.29 heartbeat
10776 root      20   0  190336  95820   3356 S   2.3  0.3 148:04.35 bundle
```

Agenda

Things we're going to cover

1 Challenges with log analytics

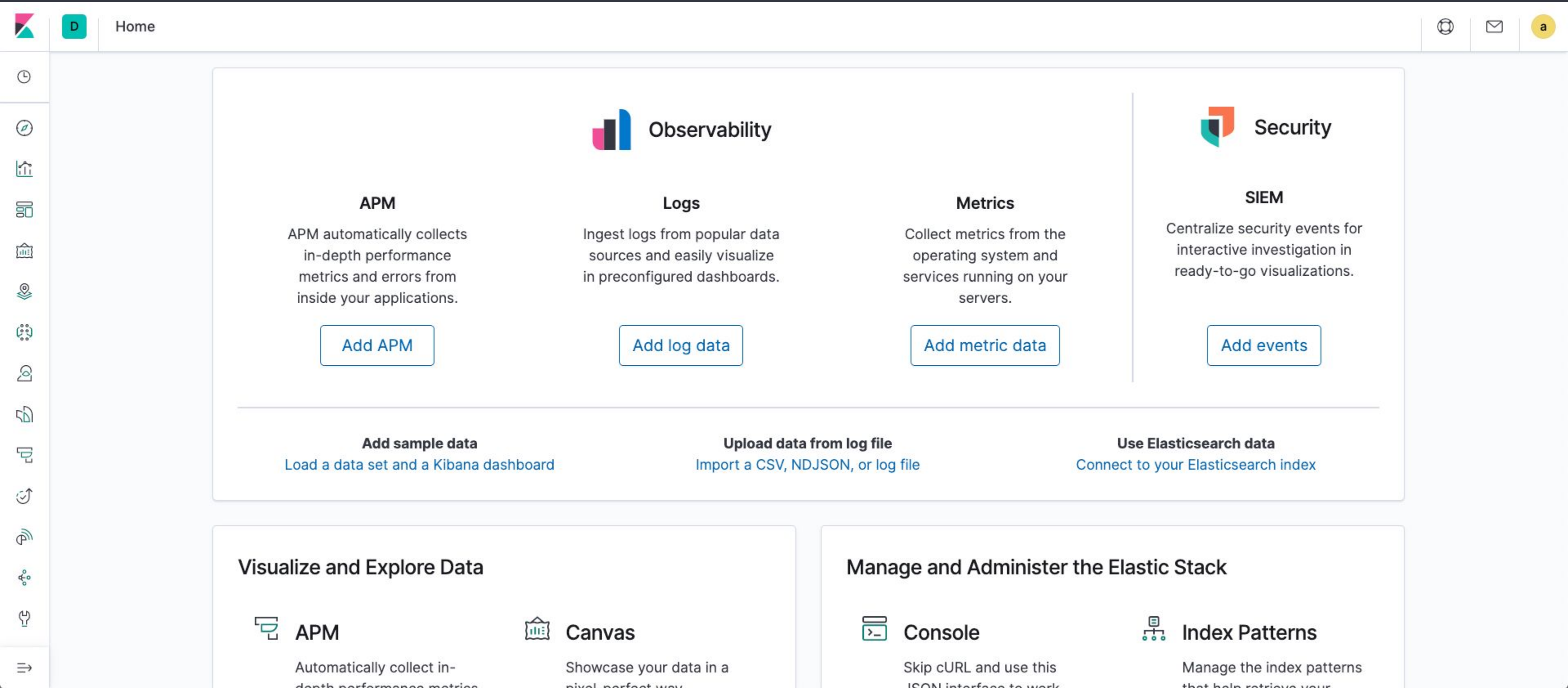
2 Sending logs to Elasticsearch

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



Observability

Security

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

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

APM

Automatically collect in-depth performance metrics

Canvas

Showcase your data in a pixel-perfect way

Manage and Administer the Elastic Stack

Console

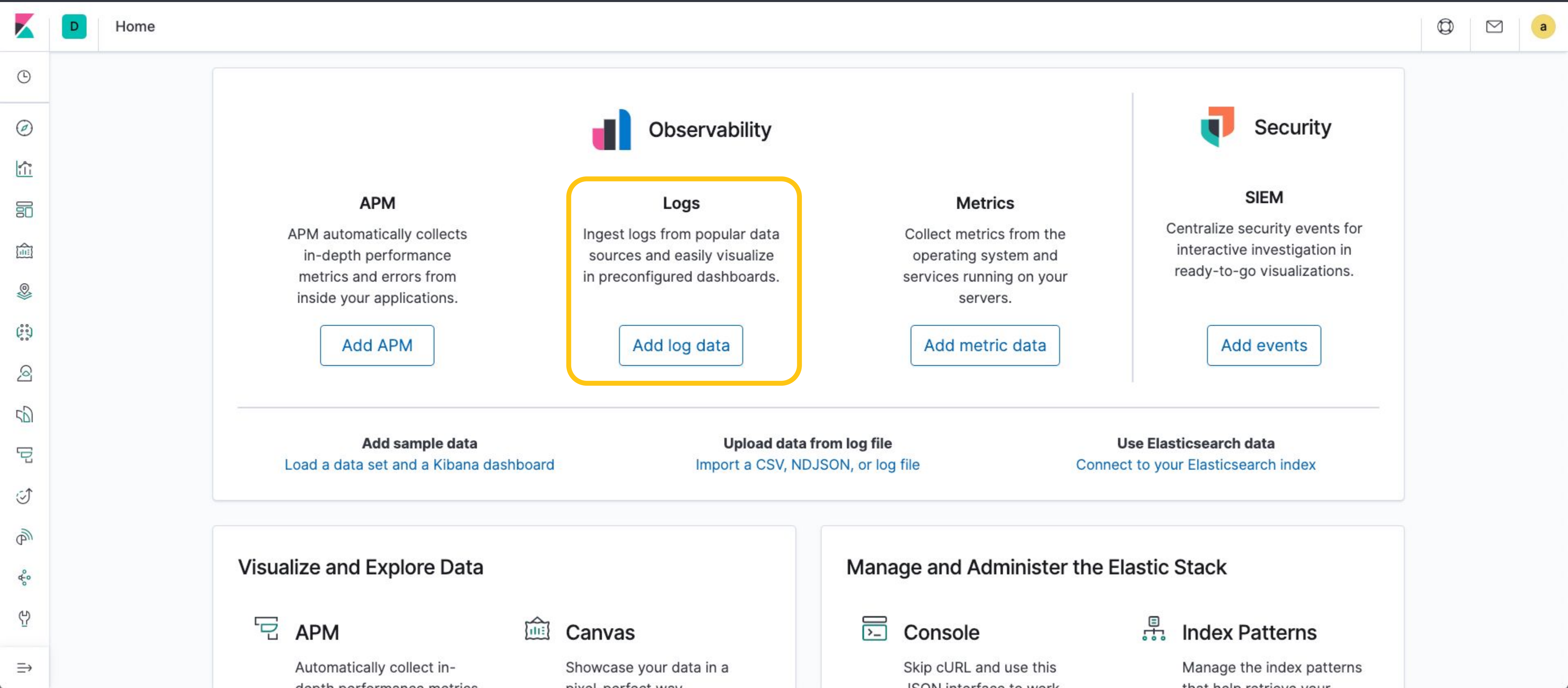
Skip cURL and use this JSON interface to work

Index Patterns

Manage the index patterns that help retrieve your

Click on the Logging Button

Works the same in the cloud or running the default distribution



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.

SIEM

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

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

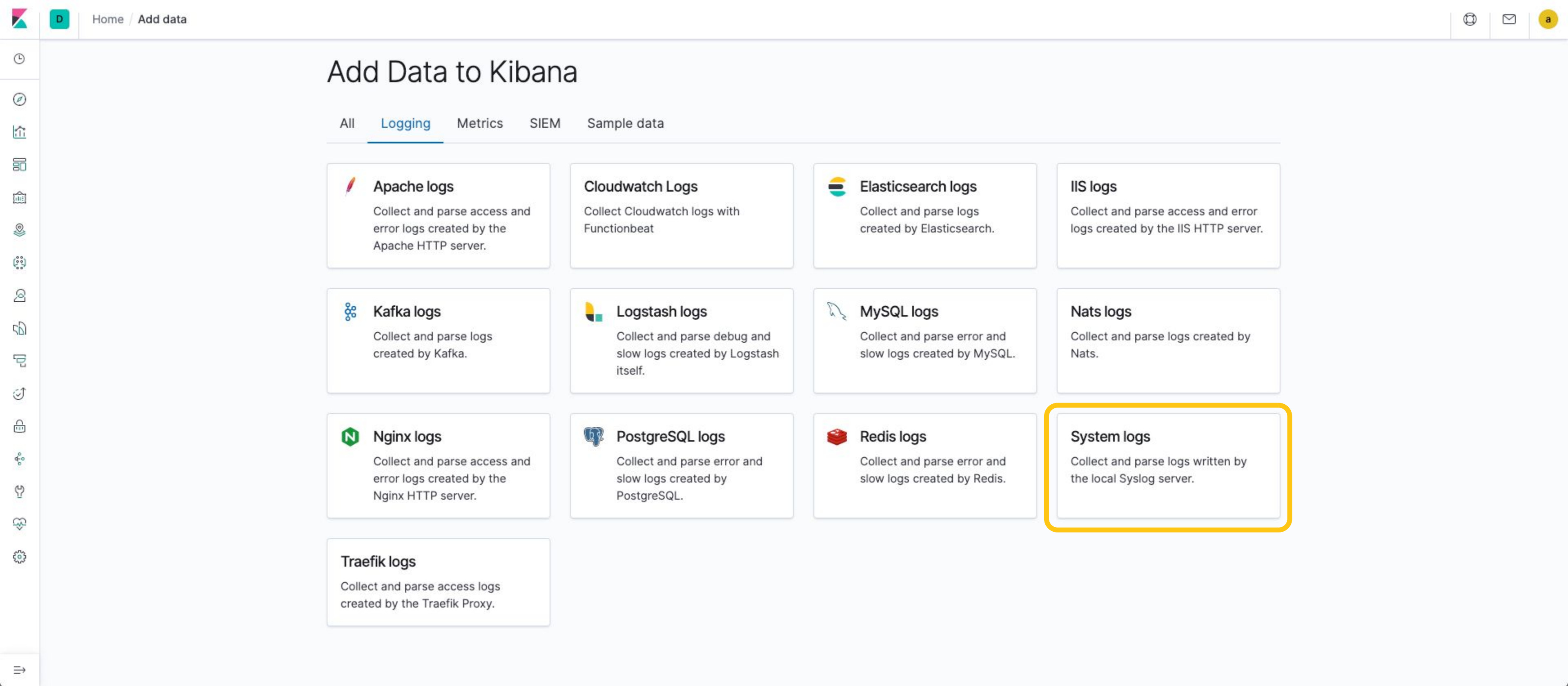
Manage and Administer the Elastic Stack

Console
Skip cURL and use this JSON interface to work

Index Patterns
Manage the index patterns that help retrieve your

Many choices

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



Add Data to Kibana

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.

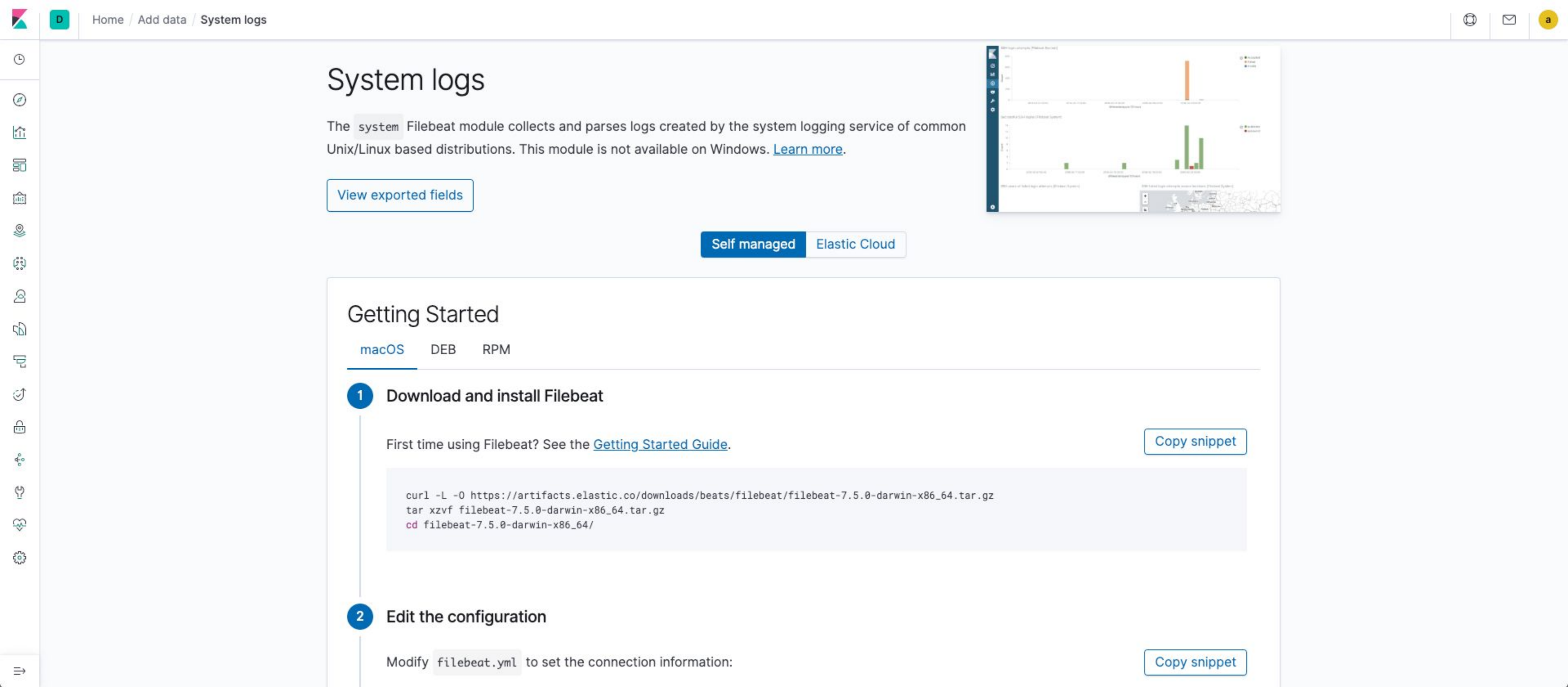
Redis logs
Collect and parse error and slow logs created by Redis.

System logs
Collect and parse logs written by the local Syslog server.

Traefik logs
Collect and parse access logs created by the Traefik Proxy.

Detailed instructions

Context-aware instructions for cloud or on-prem installs



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.

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/
```

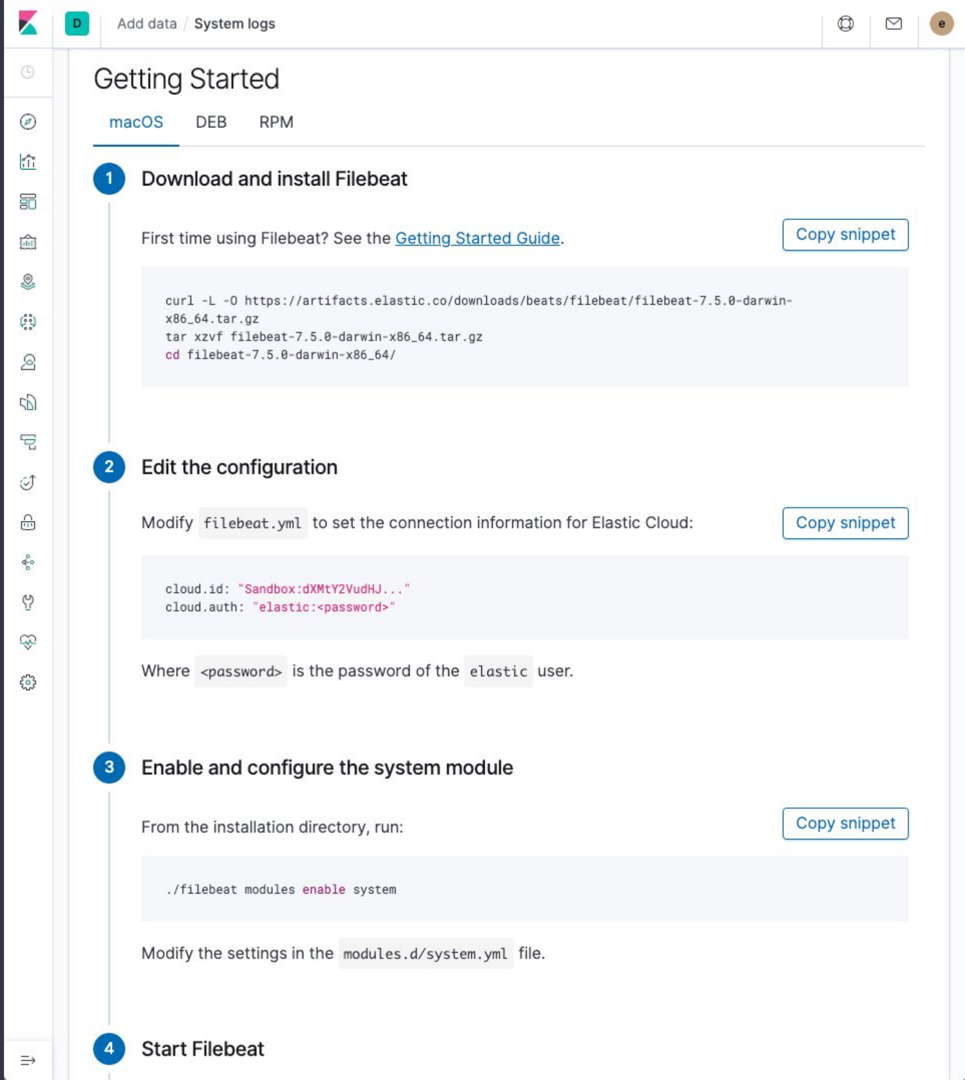
2 Edit the configuration

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

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!



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:

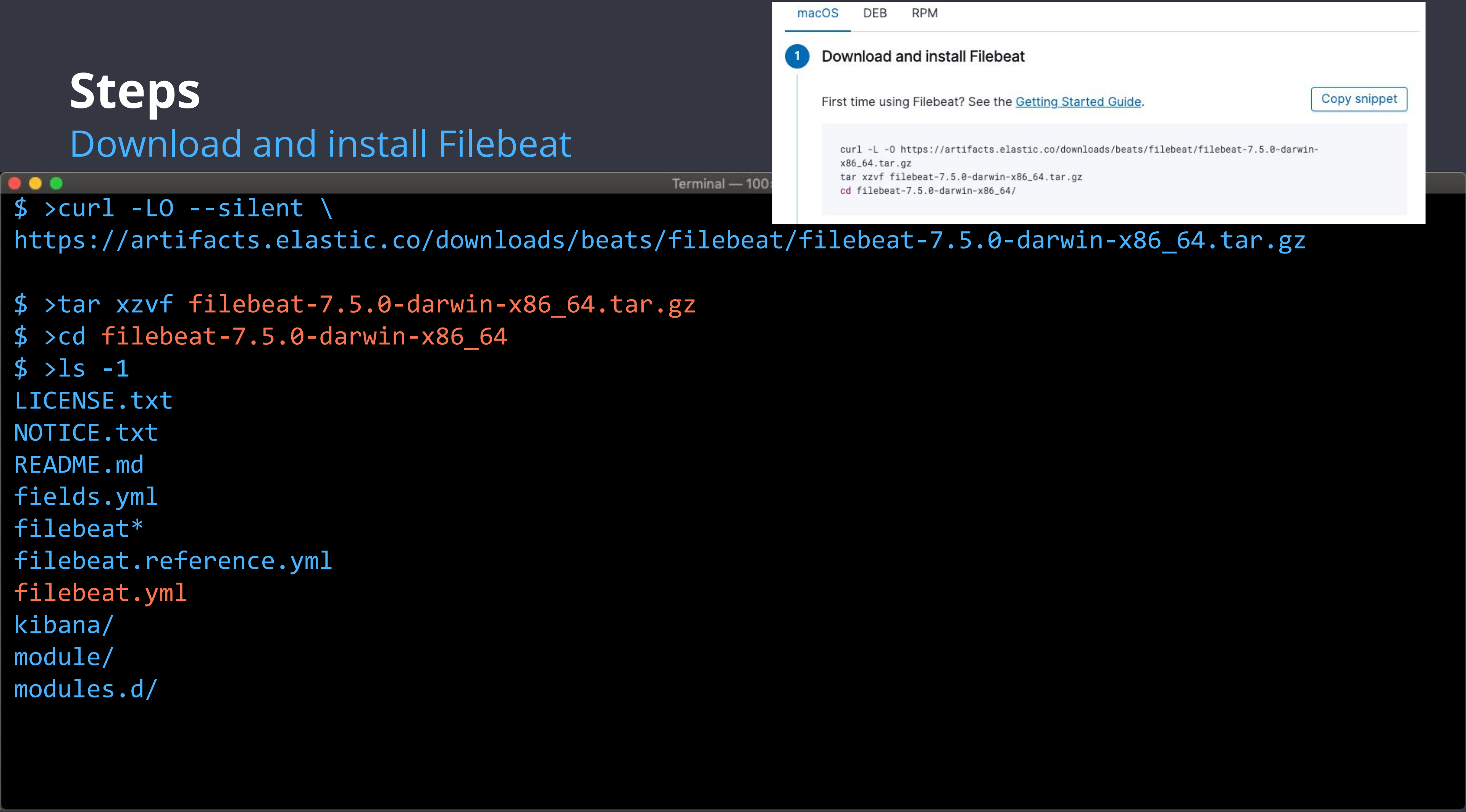
```
./filebeat modules enable system
```

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

4 Start Filebeat

Steps

Download and install Filebeat



1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

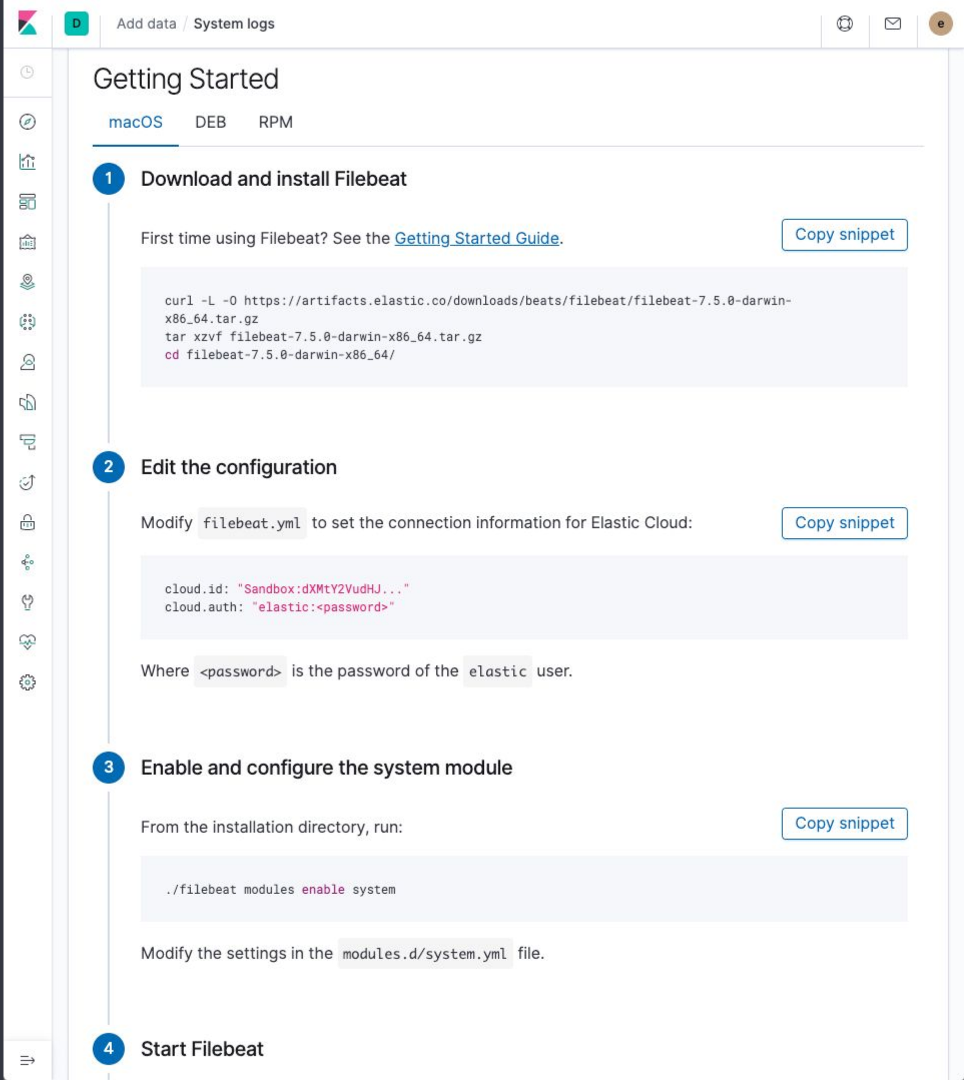
```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-
x86_64.tar.gz
tar xzvf filebeat-7.5.0-darwin-x86_64.tar.gz
cd filebeat-7.5.0-darwin-x86_64/
```

```
$ >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!



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:

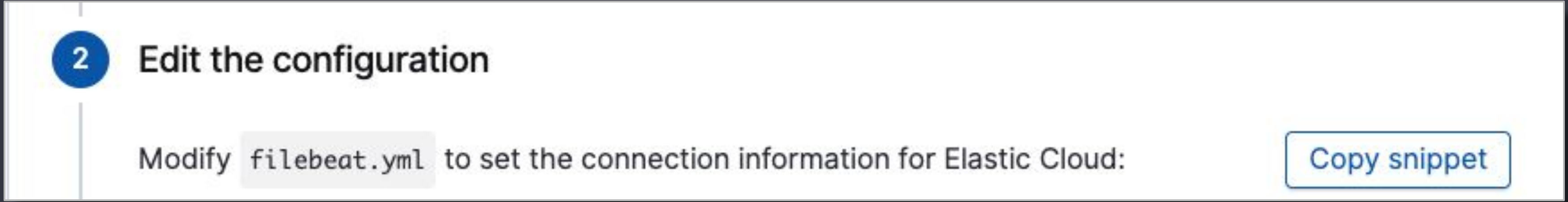
```
./filebeat modules enable system
```

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

4 Start Filebeat

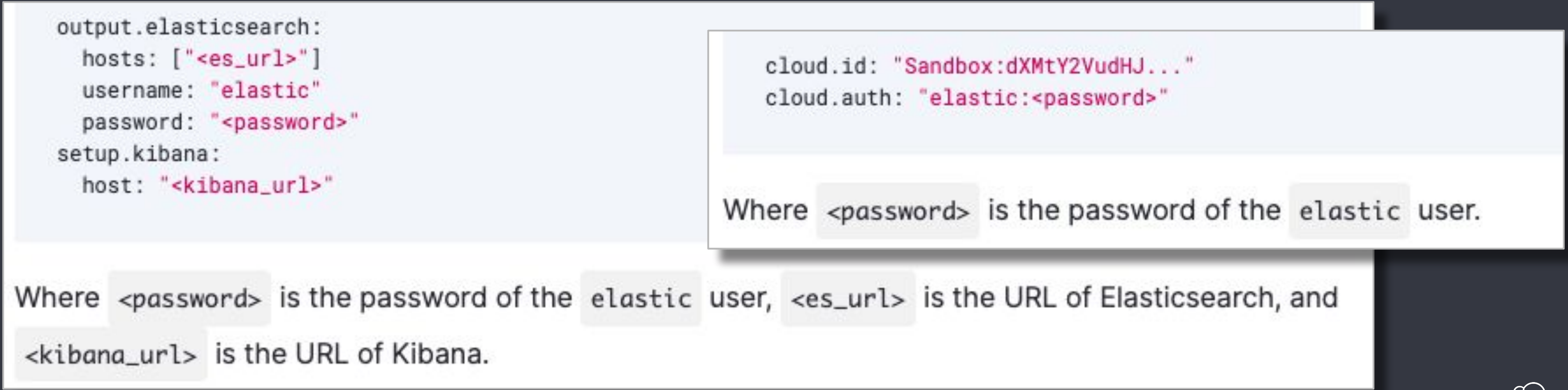
Configuration

Cloud aware - using superuser



2 Edit the configuration

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



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

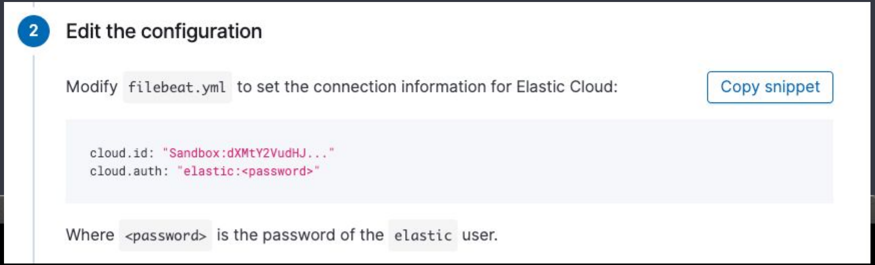
Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

```
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

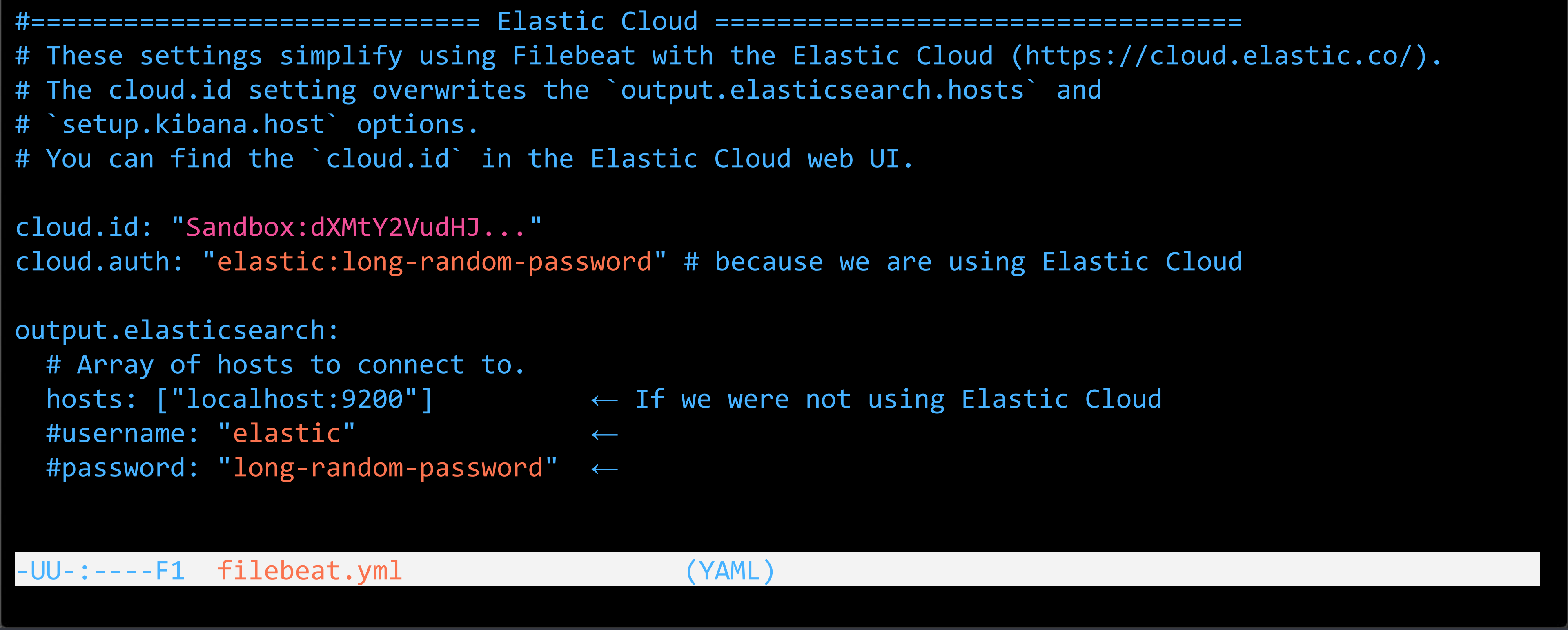


2 Edit the configuration

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.

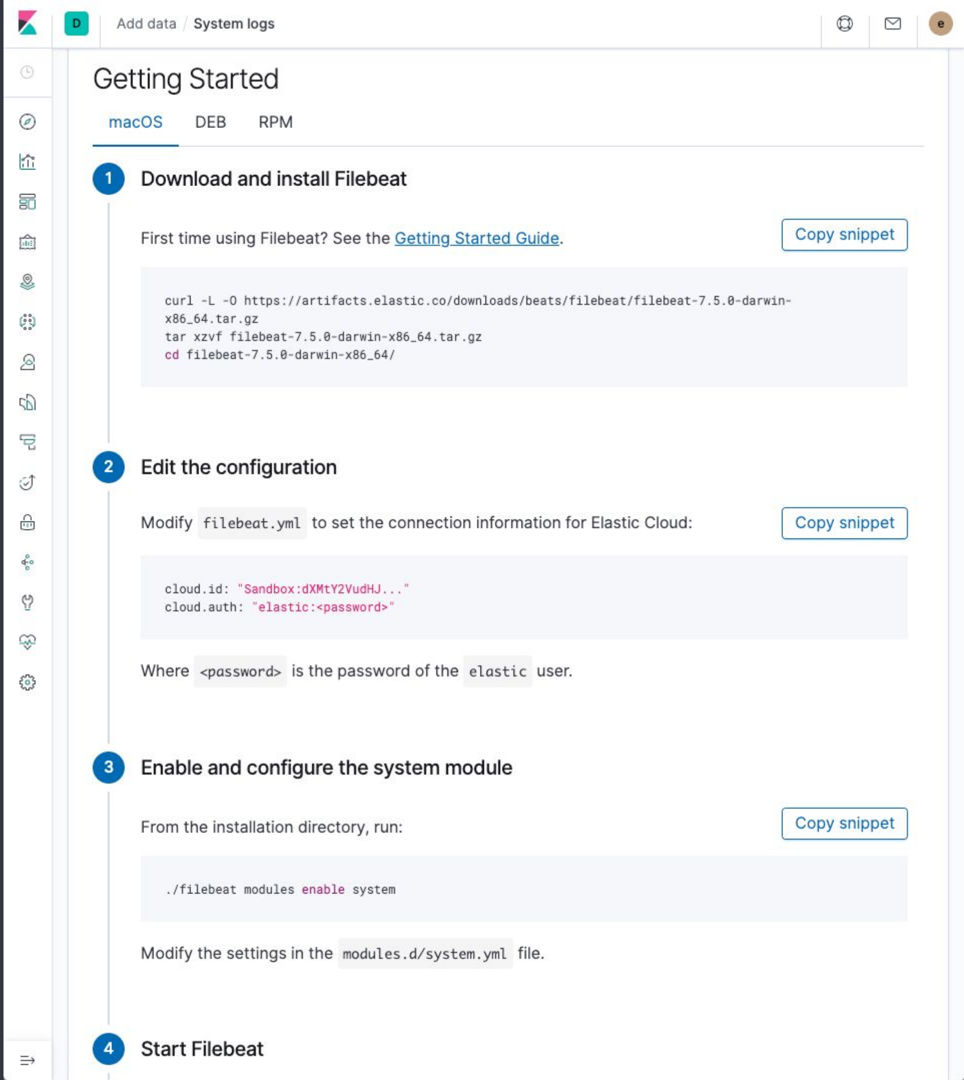


```
#============================== Elastic Cloud ==================================
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id`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



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:

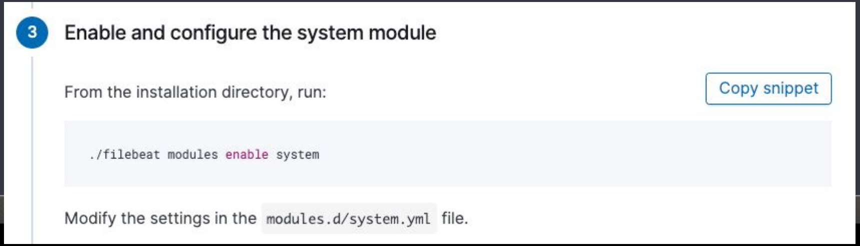
```
./filebeat modules enable system
```

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

4 Start Filebeat

Enable the system module

Again, just copy and paste the snippet

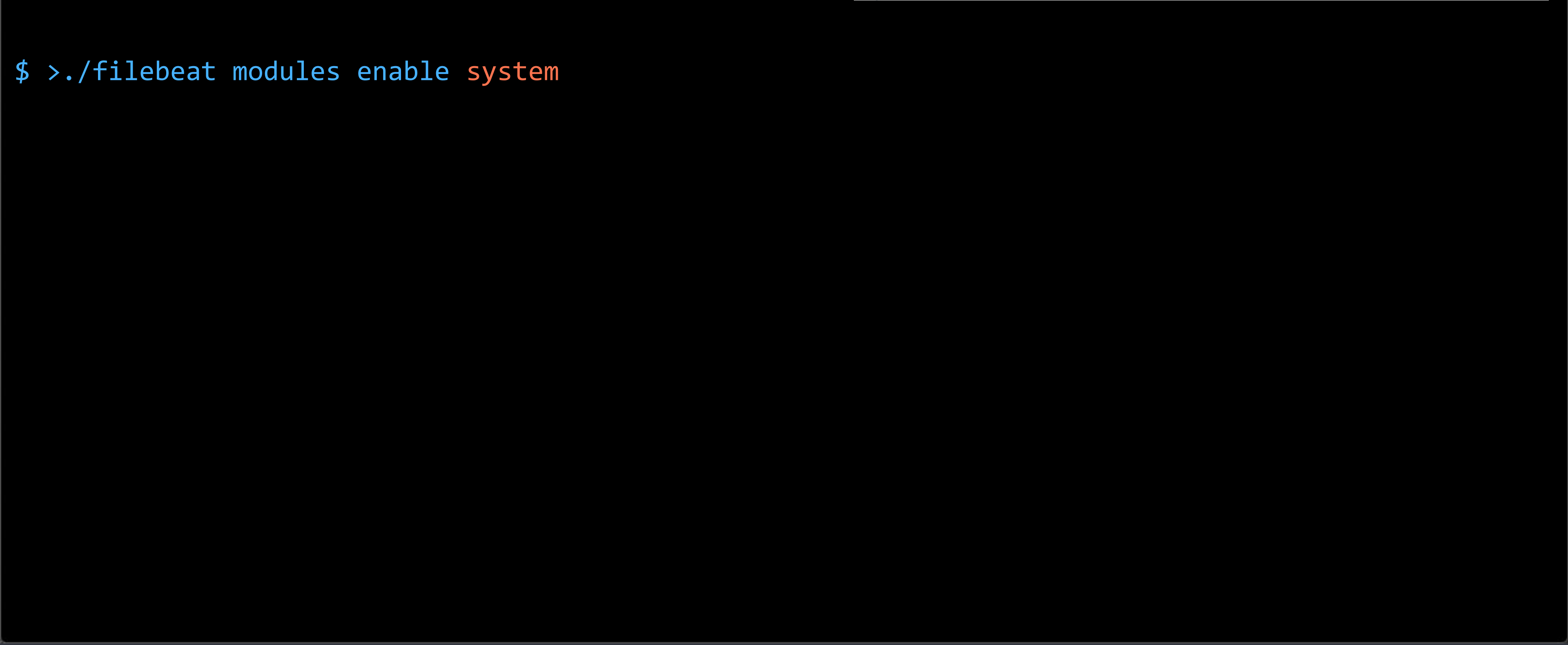


3 Enable and configure the system module

From the installation directory, run:

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

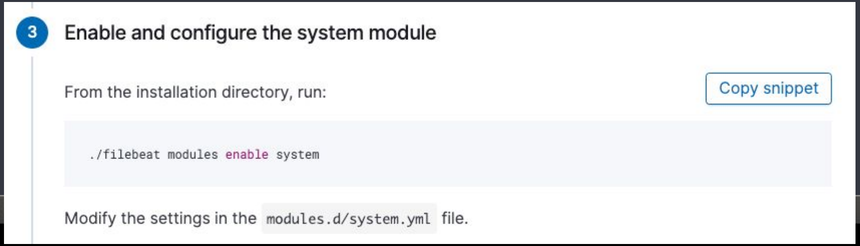
Modify the settings in the `modules.d/system.yml` file.



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

Enable the system module

Again, just copy and paste the snippet

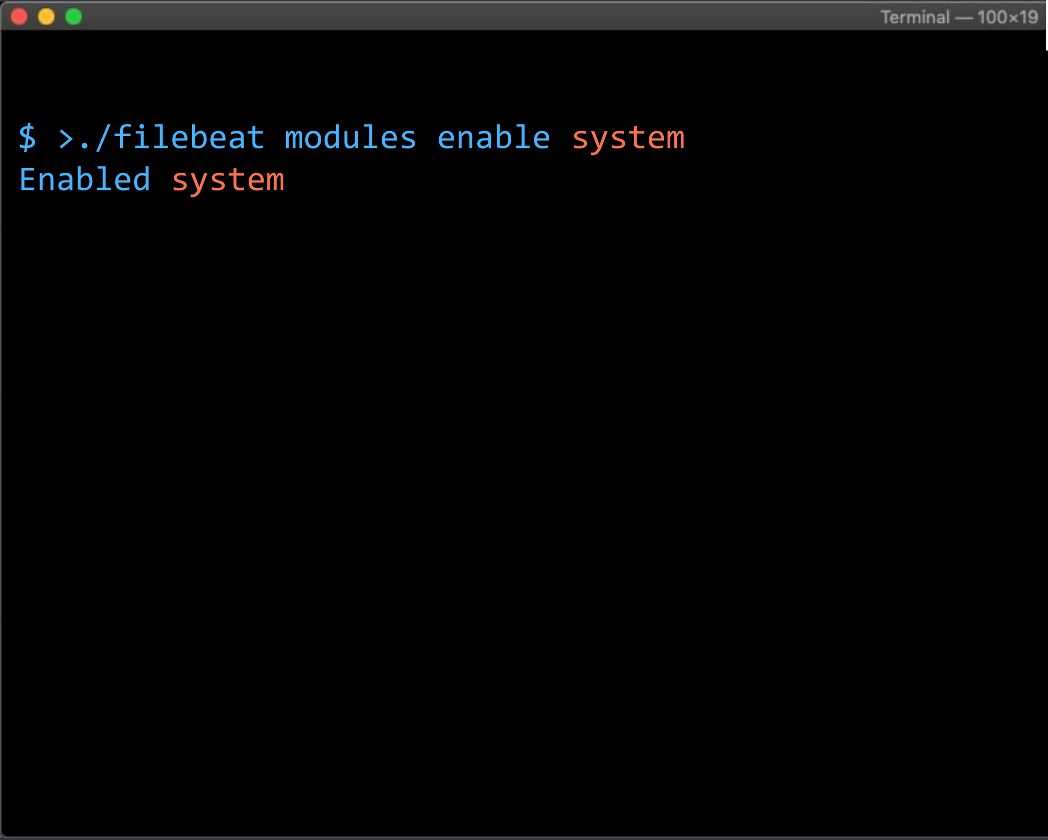


3 Enable and configure the system module

From the installation directory, run:

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

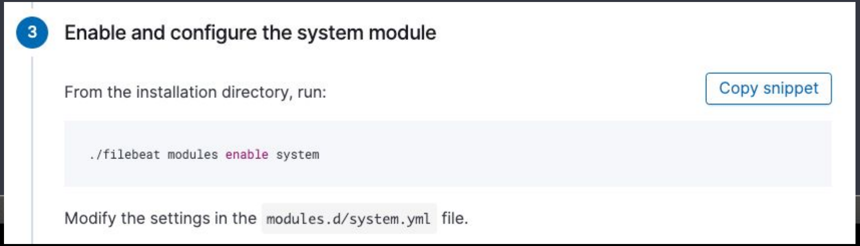
Modify the settings in the `modules.d/system.yml` file.



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

Enable the system module

Check your work

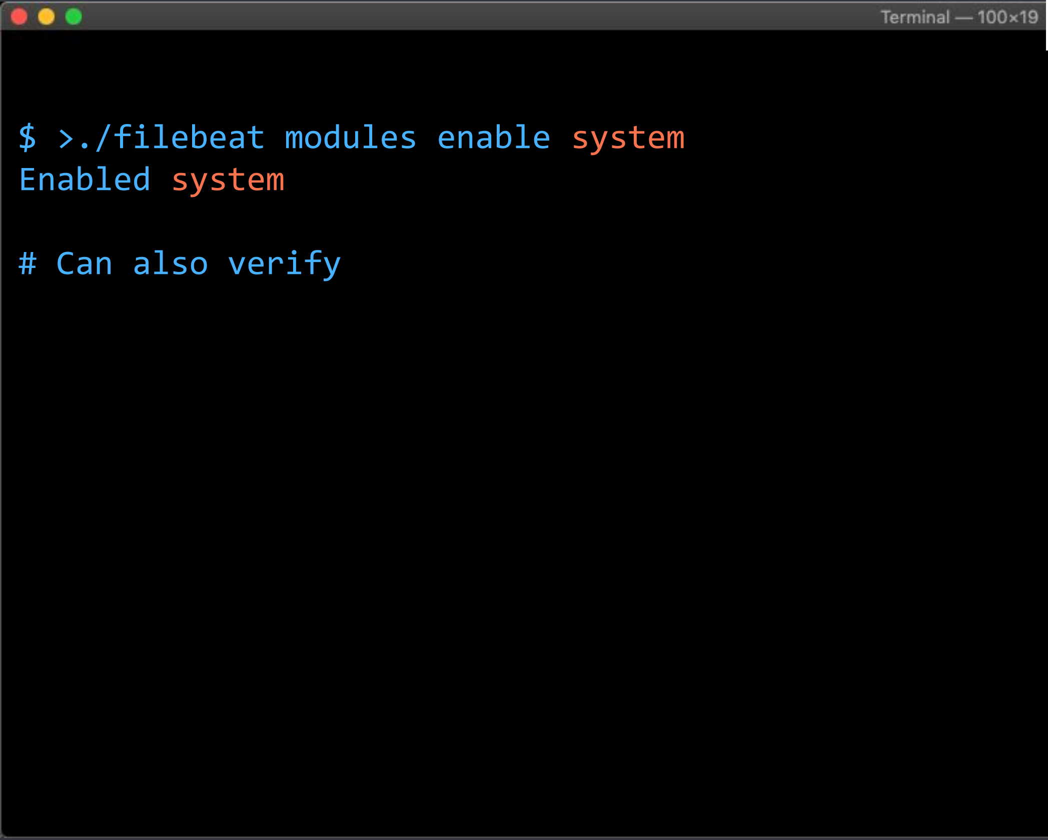


3 Enable and configure the system module

From the installation directory, run:

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

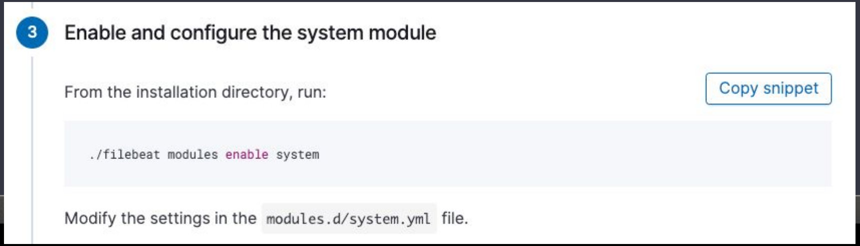
Modify the settings in the `modules.d/system.yml` file.



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

# Can also verify
```

Enable the system module

Check your work

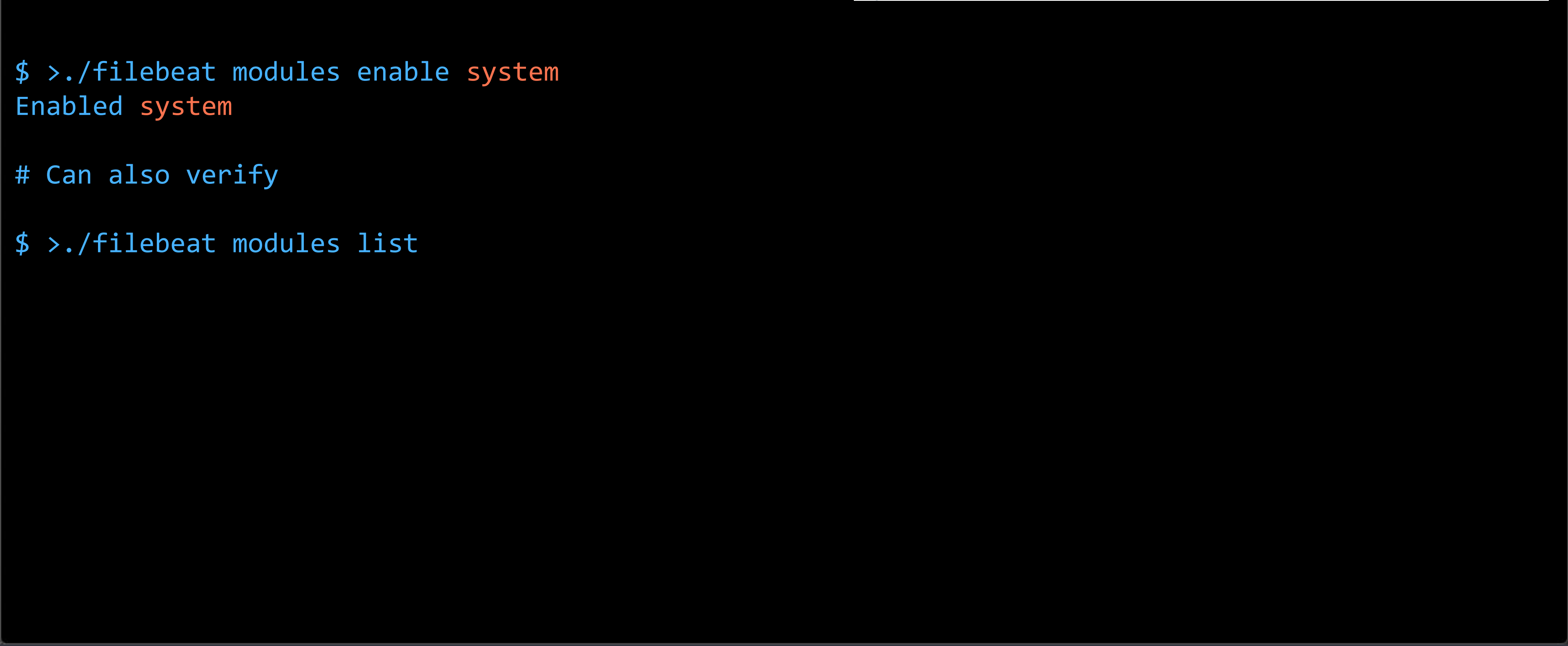


3 Enable and configure the system module

From the installation directory, run:

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

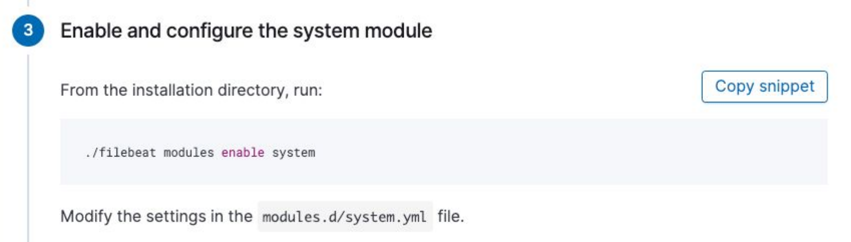
Modify the settings in the `modules.d/system.yml` file.



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

# Can also verify

$ >./filebeat modules list
```

Enable the system module

All good

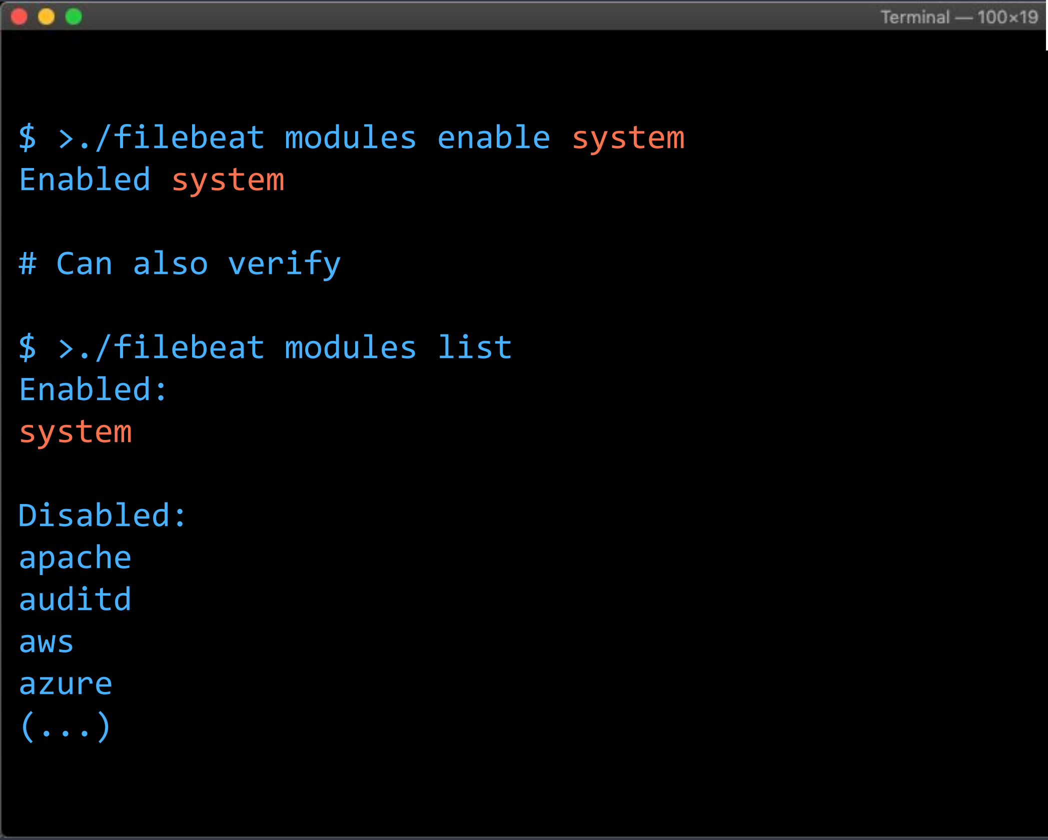


Enable and configure the system module

From the installation directory, run:

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

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

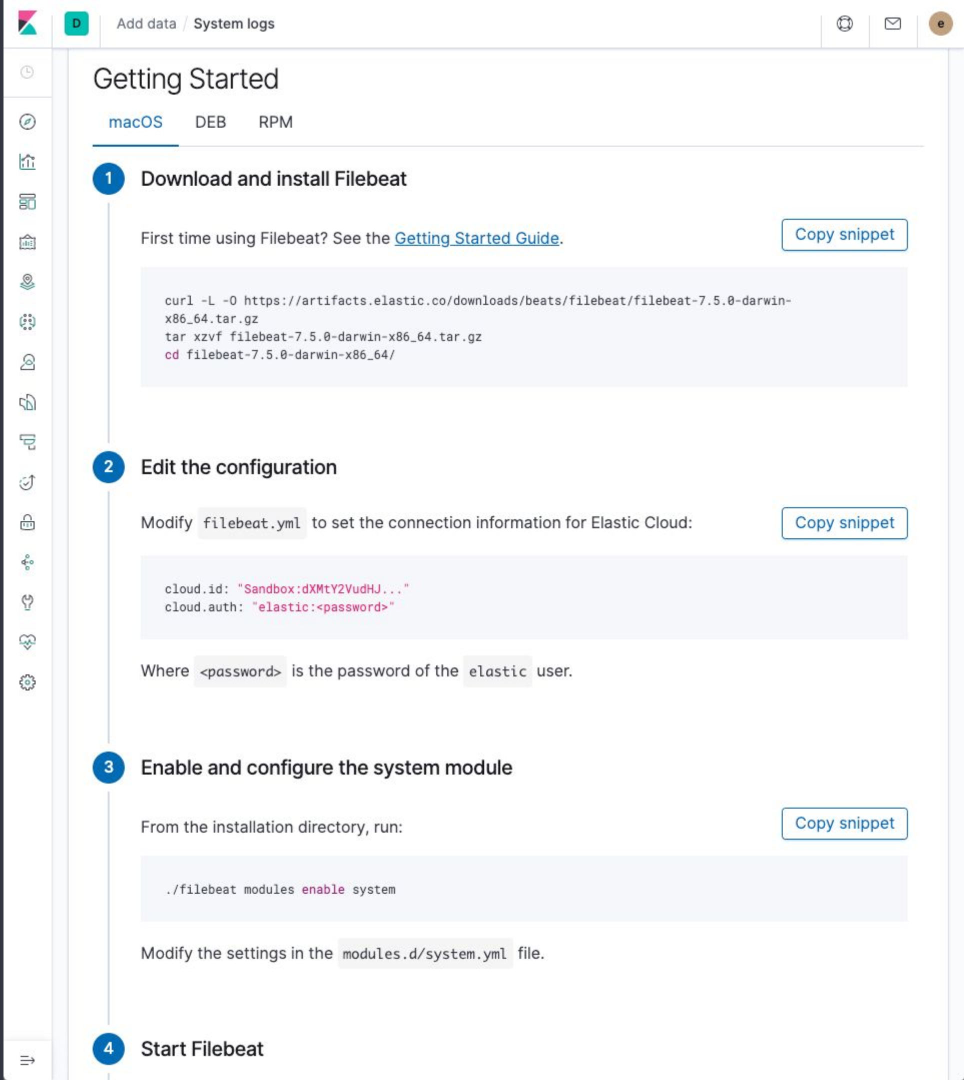


```
$ >./filebeat modules enable system
Enabled system

# 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!



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:

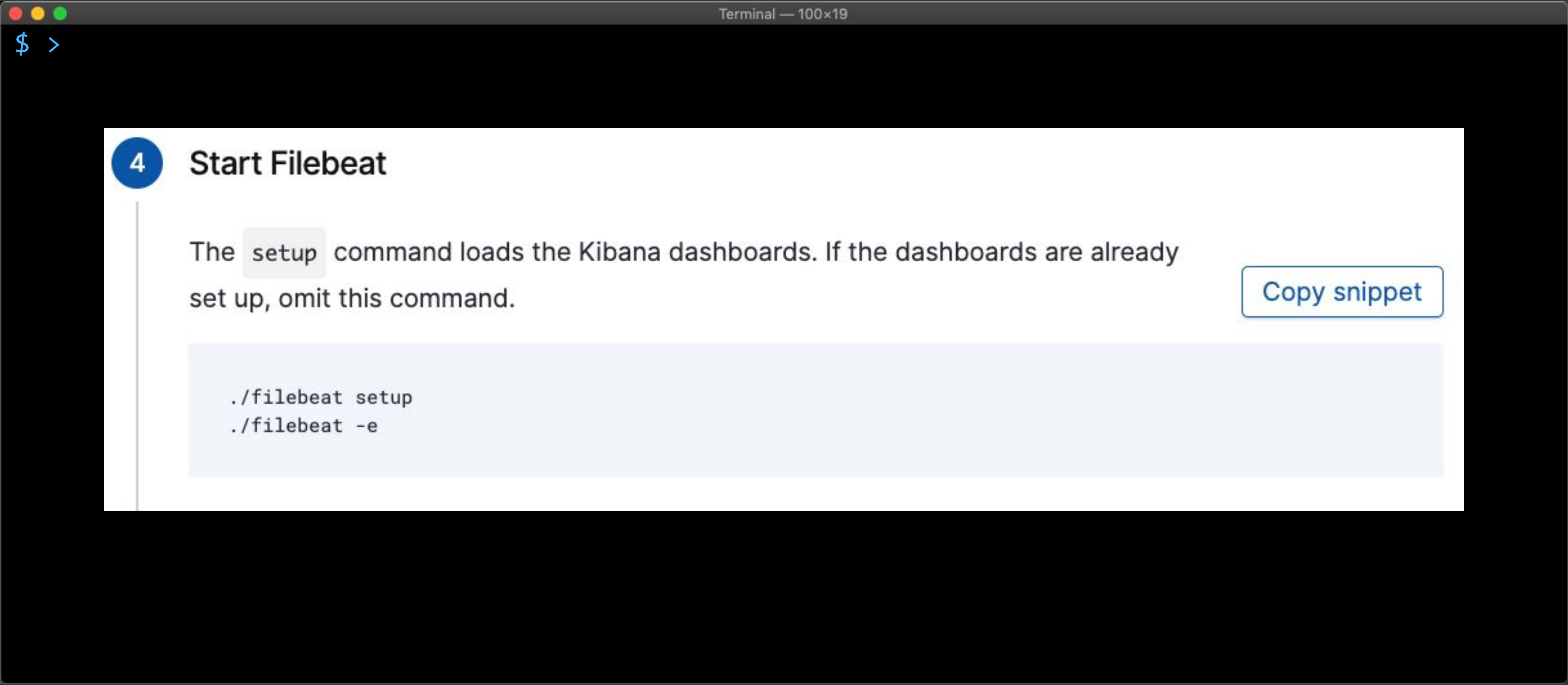
```
./filebeat modules enable system
```

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

4 Start Filebeat

And start it up!

Startup steps



```
$ >
```

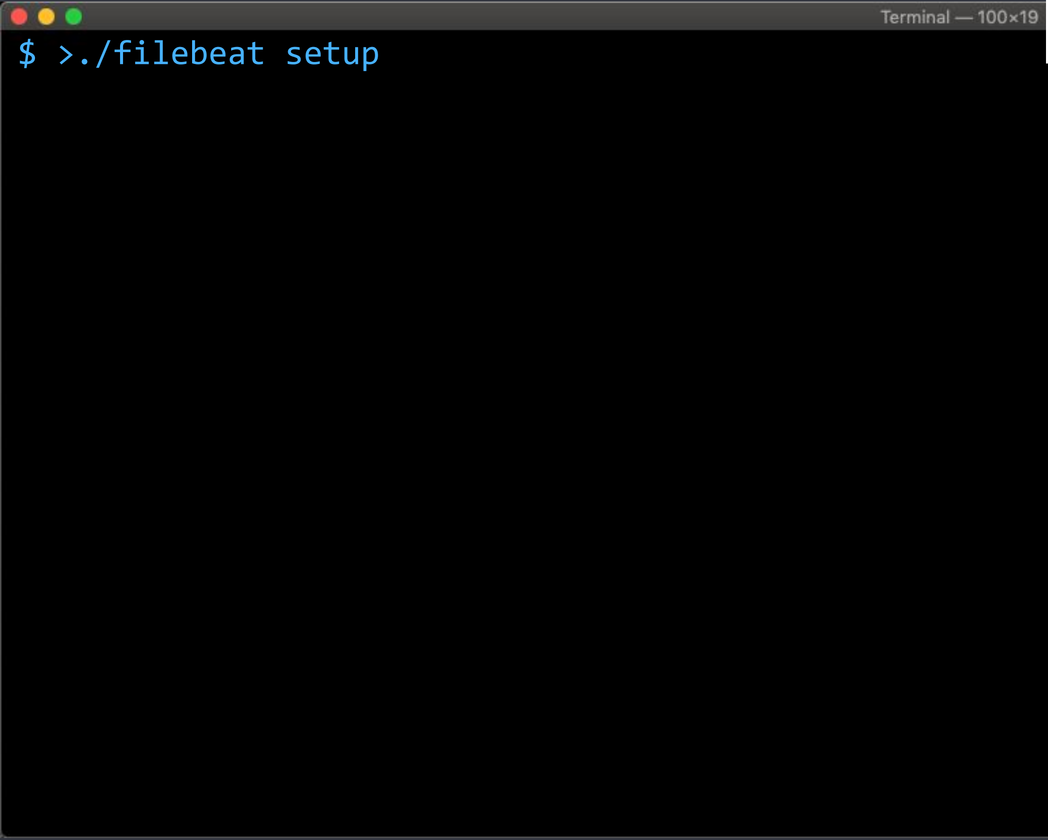
4 Start Filebeat

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

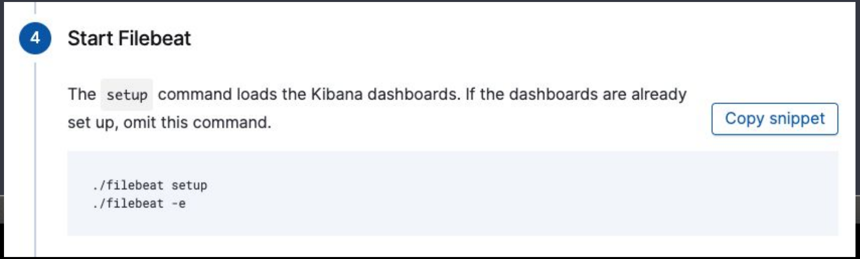
```
./filebeat setup
./filebeat -e
```

First run the setup process

Setup preps dashboards and indices



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



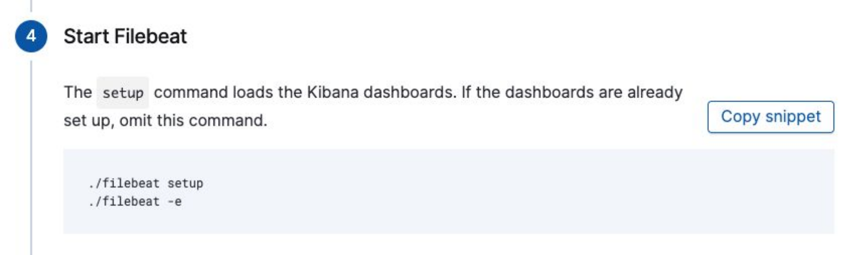
4 Start Filebeat

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

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

First run the setup process

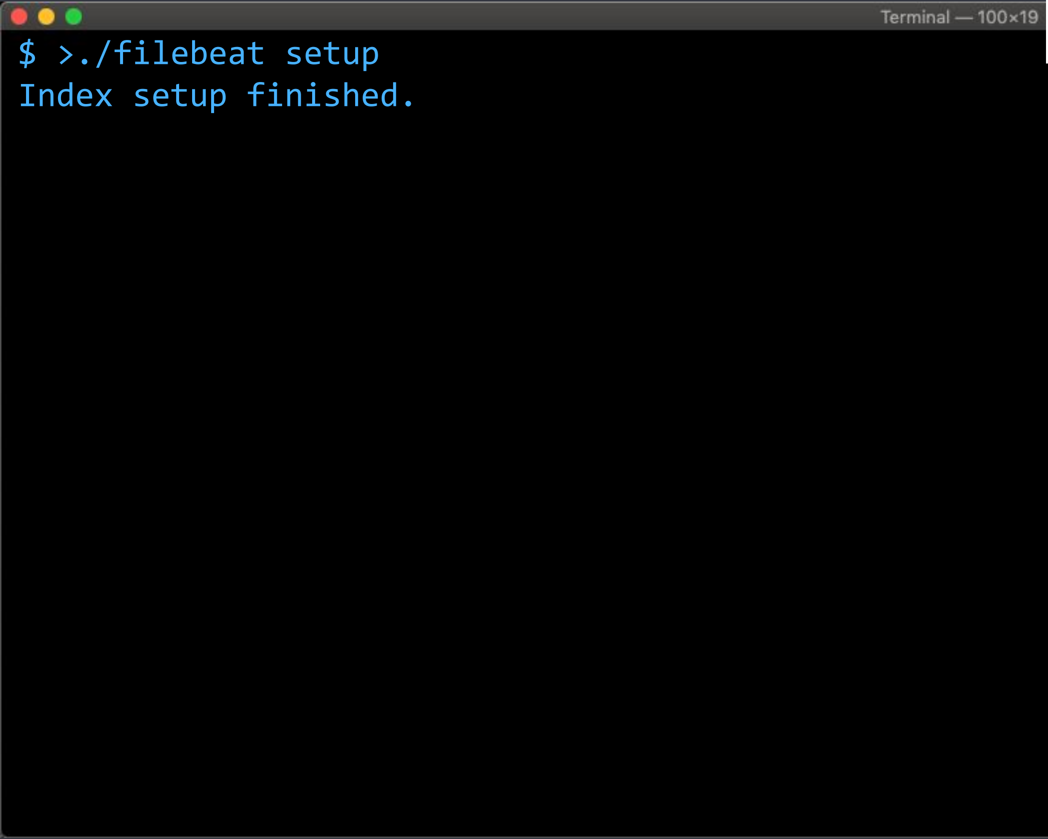
Setup preps dashboards and indices



4 Start Filebeat

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

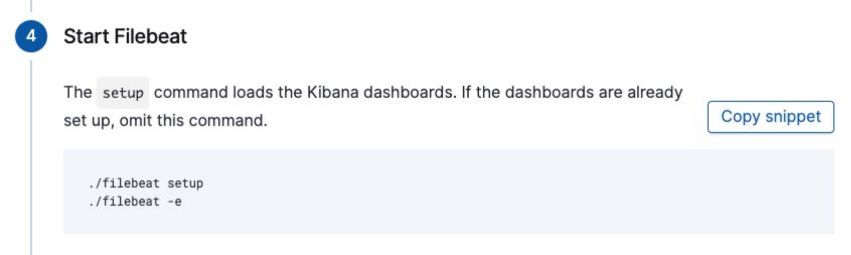
```
./filebeat setup
./filebeat -e
```



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

First run the setup process

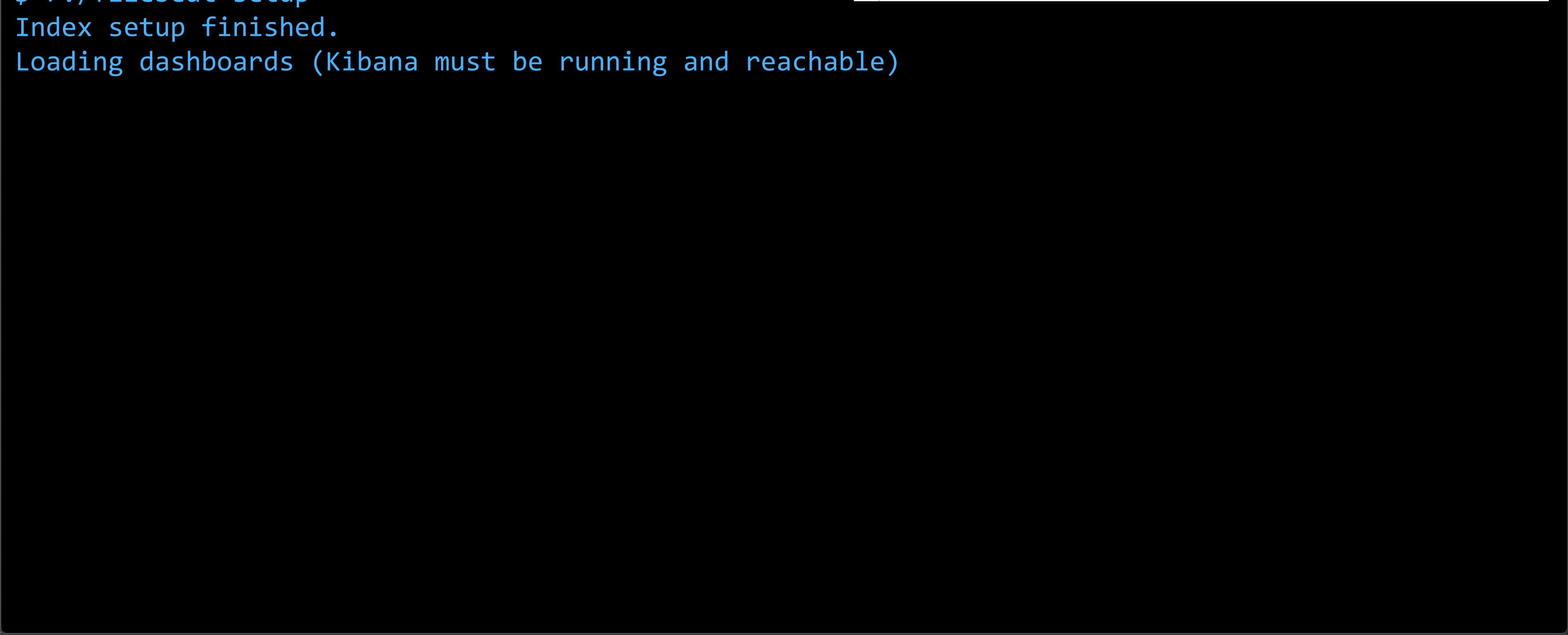
Setup preps dashboards and indices



4 Start Filebeat

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

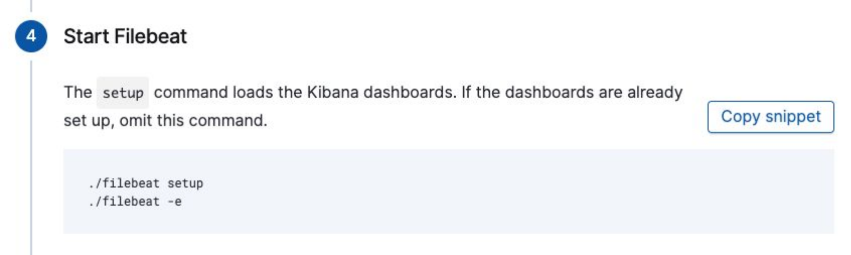
```
./filebeat setup
./filebeat -e
```



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

First run the setup process

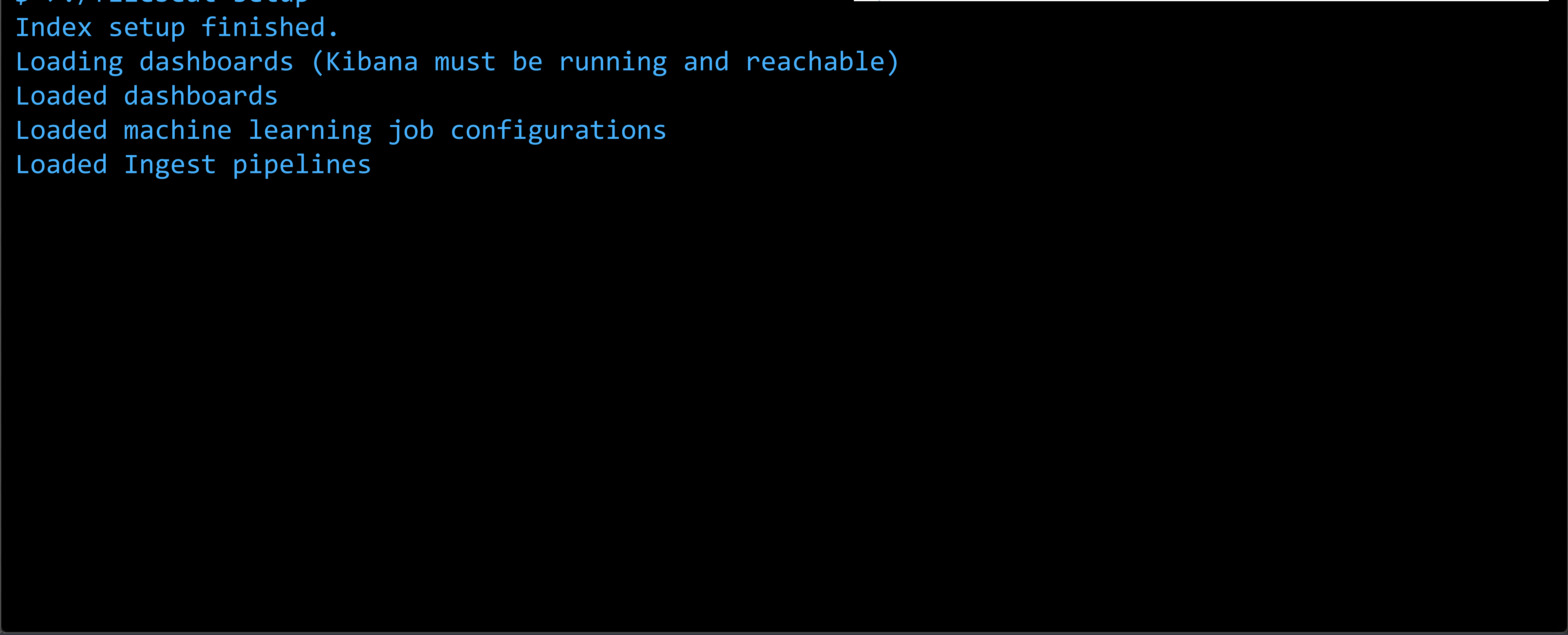
Setup preps dashboards and indices



4 Start Filebeat

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

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



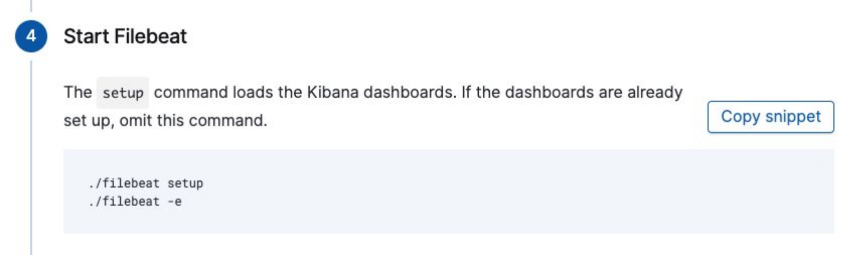
```
$ >./filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
```

Finally, start it!

-e tells it to send messages to console

Terminal — 100×19

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



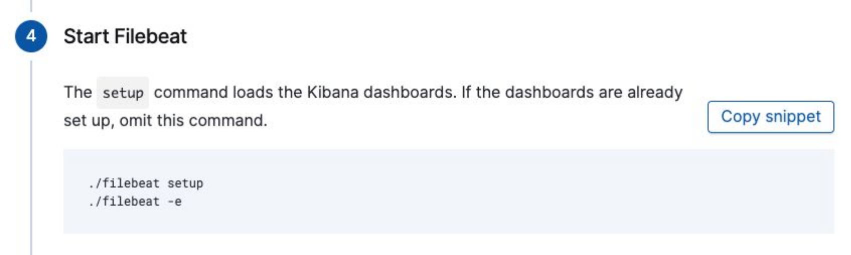
4 Start Filebeat

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

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

Finally, start it!

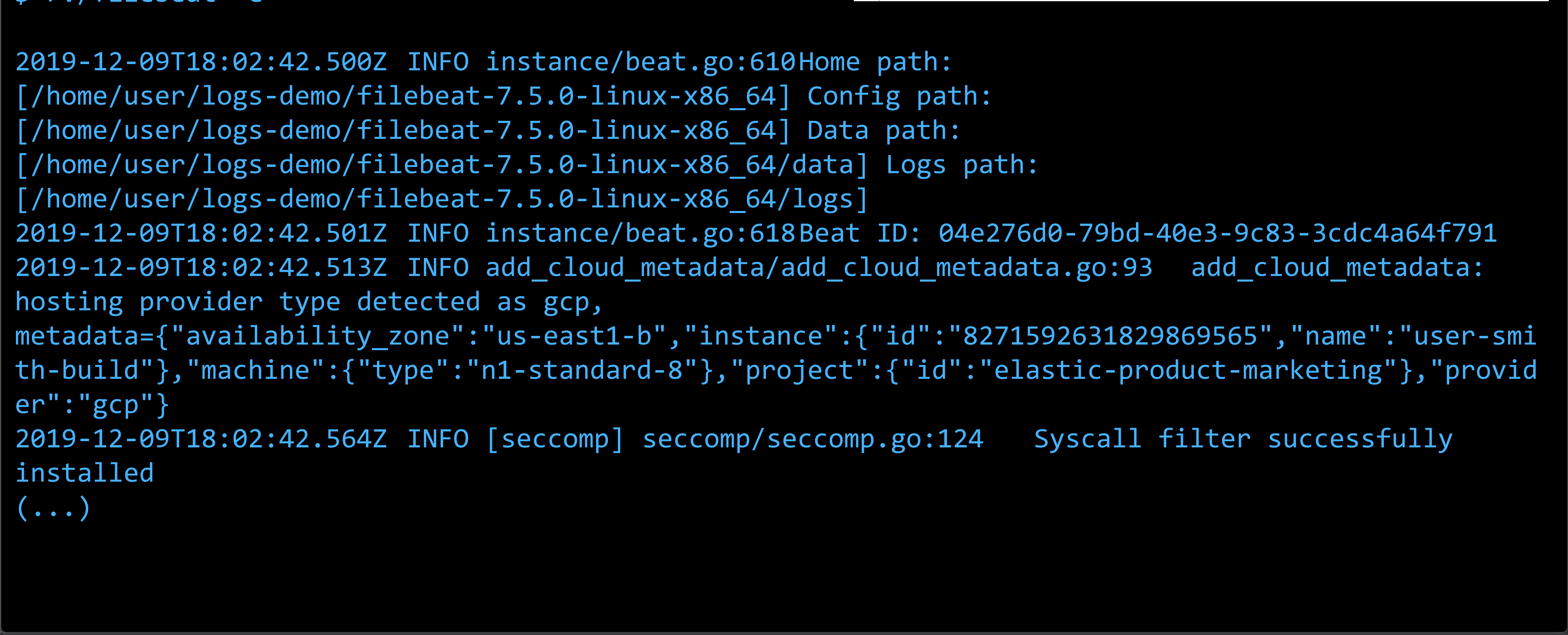
-e tells it to send messages to console



4 Start Filebeat

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

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

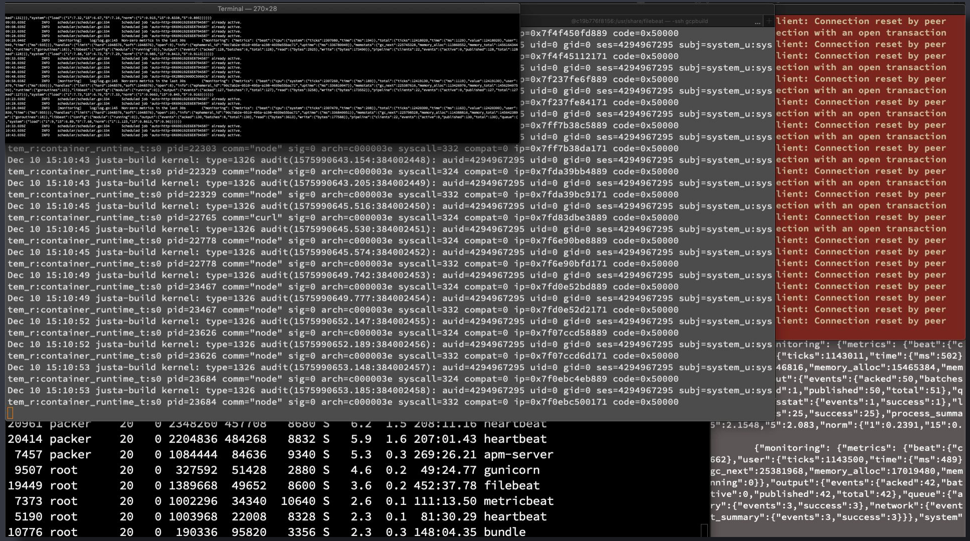


```
$ >./filebeat -e

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



Terminal — 270×28

```
ked":131}}},"system":{"load":{"1":7.32,"15":6.67,"5":7.16,"norm":{"1":0.915,"15":0.8338,"5":0.895}}}}}
09:03.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:08.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307080,"time":{"ms":194}},"total":{"ticks":12418020,"time":{"ms":1129},"value":12418020},"user":
940,"time":{"ms":935}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":9},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336780049}},"memstats":{"gc_next":225745328,"memory_alloc":113860552,"memory_total":1456164344
68},"runtime":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":128,"batches":6,"total":128},"read":{"bytes":2925},"write":{"bytes":173490}},"pipeline":{"clients":22,"events":{"active":0,"published":128,"total":128
ked":128}}},"system":{"load":{"1":7.88,"15":6.73,"5":7.29,"norm":{"1":0.985,"15":0.8413,"5":0.9113}}}}}
09:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:38.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:43.040Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X2B802900DC5066C6' already active.
09:58.038Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307260,"time":{"ms":189}},"total":{"ticks":12419130,"time":{"ms":1119},"value":12419130},"user":
870,"time":{"ms":930}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":8},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336810047}},"memstats":{"gc_next":225387616,"memory_alloc":113426976,"memory_total":1456294075
20},"runtime":{"goroutines":15}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":127,"batches":7,"total":127},"read":{"bytes":3258},"write":{"bytes":173552}},"pipeline":{"clients":22,"events":{"active":0,"published":127,"total":127
ked":127}}},"system":{"load":{"1":7.73,"15":6.76,"5":7.33,"norm":{"1":0.9663,"15":0.845,"5":0.9163}}}}}
10:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307470,"time":{"ms":208}},"total":{"ticks":12420300,"time":{"ms":1163},"value":12420300},"user":
830,"time":{"ms":955}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":10},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336840051}},"memstats":{"gc_next":225798528,"memory_alloc":114388816,"memory_total":145642389
e":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":130,"batches":8,"total":130},"read":{"bytes":3613},"write":{"bytes":177588}},"pipeline":{"clients":22,"events":{"active":0,"published":130,"total":130},"queue":{
,"system":{"load":{"1":9,"15":6.89,"5":7.68,"norm":{"1":1.125,"15":0.8613,"5":0.96}}}}}
10:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
```

@c19b776f8156:/usr/share/filebeat — -ssh gcpbuild

```
p=0x7f4f450fd889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f4f45112171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f237fe6f889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f237fe84171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7ff7b38c5889 code=0x50000
5 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
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.516:384002450): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22765 comm="curl" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fd83dbe3889 code=0x50000
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.530:384002451): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22778 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f6e90be8889 code=0x50000
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.574:384002452): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22778 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f6e90bfd171 code=0x50000
Dec 10 15:10:49 justa-build kernel: type=1326 audit(1575990649.742:384002453): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23467 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fd0e52bd889 code=0x50000
Dec 10 15:10:49 justa-build kernel: type=1326 audit(1575990649.777:384002454): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23467 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fd0e52d2171 code=0x50000
Dec 10 15:10:52 justa-build kernel: type=1326 audit(1575990652.147:384002455): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23626 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f07ccd58889 code=0x50000
Dec 10 15:10:52 justa-build kernel: type=1326 audit(1575990652.189:384002456): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23626 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f07ccd6d171 code=0x50000
Dec 10 15:10:53 justa-build kernel: type=1326 audit(1575990653.148:384002457): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23684 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f0ebc4eb889 code=0x50000
Dec 10 15:10:53 justa-build kernel: type=1326 audit(1575990653.185:384002458): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23684 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f0ebc500171 code=0x50000
```

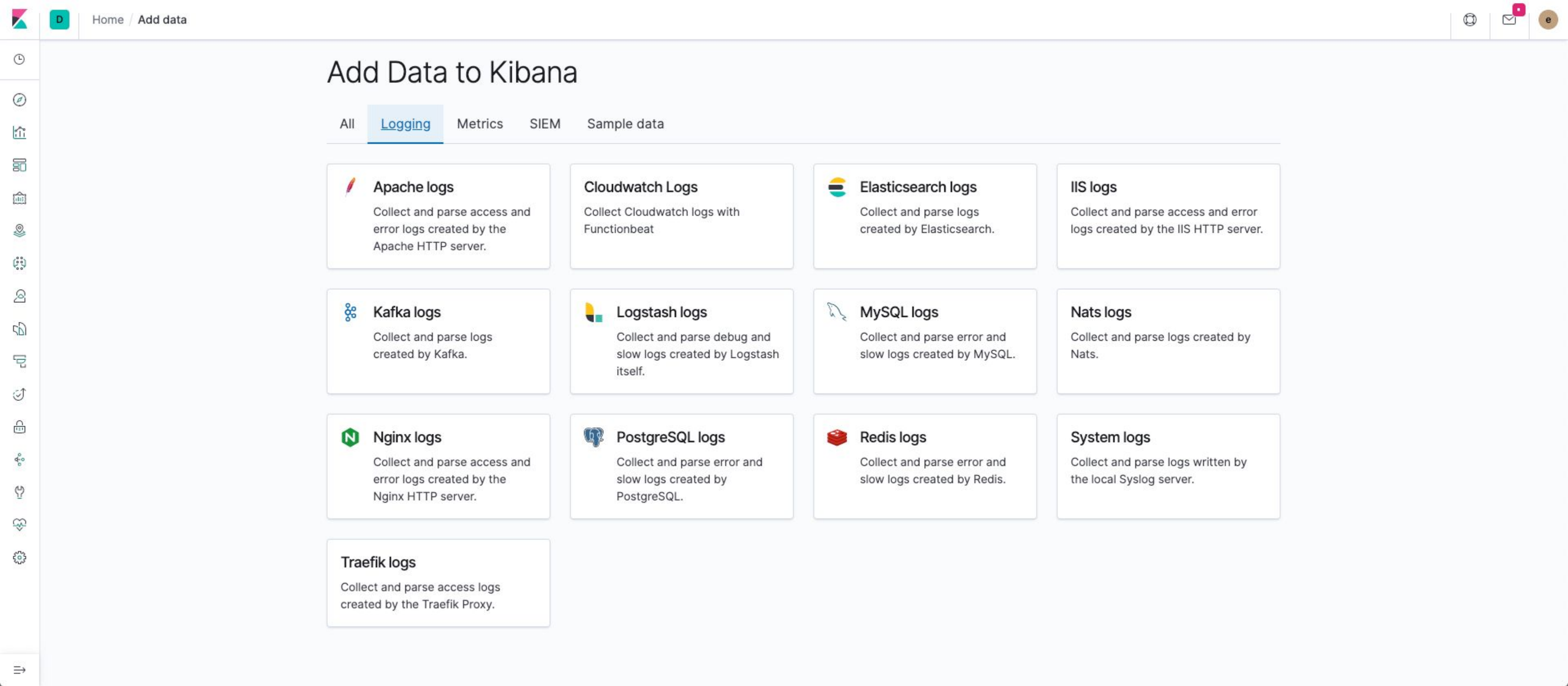
```
lient: Connection reset by peer
ection with an open transaction
lient: Connection reset by peer
lient: Connection reset by peer
ection with an open transaction
lient: Connection reset by peer
ection with an open transaction
lient: Connection reset by peer
ection with an open transaction
lient: Connection 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
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
```

```
nitoring": {"metrics": {"beat":{"c
{"ticks":1143011,"time":{"ms":502}
46816,"memory_alloc":15465384,"mem
ut":{"events":{"acked":50,"batches
d":1,"published":50,"total":51},"q
sstat":{"events":1,"success":1},"l
s":25,"success":25},"process_summa
5":2.1548,"5":2.083,"norm":{"1":0.2391,"15":0.

        {"monitoring": {"metrics": {"beat":{"c
662},"user":{"ticks":1143500,"time":{"ms":489}
gc_next":25381968,"memory_alloc":17019480,"mem
nning":0}},"output":{"events":{"acked":42,"bat
tive":0,"published":42,"total":42},"queue":{"a
ry":{"events":3,"success":3},"network":{"event
t_summary":{"events":3,"success":3}}},"system"
```

```
20961 packer    20   0 2348260 457708   8680 S   6.2  1.5 208:11.16 heartbeat
20414 packer    20   0 2204836 484268   8832 S   5.9  1.6 207:01.43 heartbeat
 7457 packer    20   0 1084444  84636   9340 S   5.3  0.3 269:26.21 apm-server
 9507 root      20   0  327592  51428   2880 S   4.6  0.2  49:24.77 gunicorn
19449 root      20   0 1389668  49652   8600 S   3.6  0.2 452:37.78 filebeat
 7373 root      20   0 1002296  34340  10640 S   2.6  0.1 111:13.50 metricbeat
 5190 root      20   0 1003968  22008   8328 S   2.3  0.1  81:30.29 heartbeat
10776 root      20   0  190336  95820   3356 S   2.3  0.3 148:04.35 bundle
```

Needs for log analytics

Easy setup for variety of log sources



Add Data to Kibana

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.

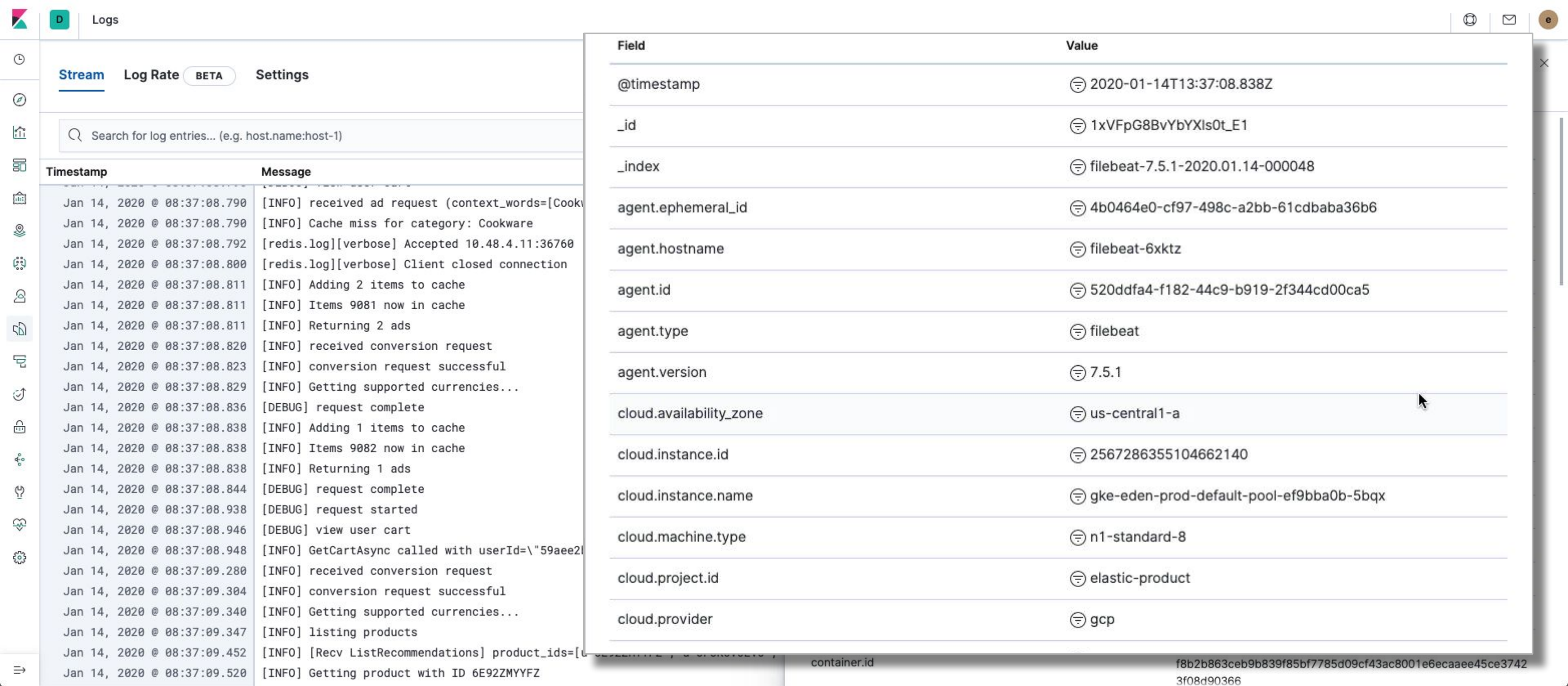
Redis logs
Collect and parse error and slow logs created by Redis.

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



Timestamp	Message

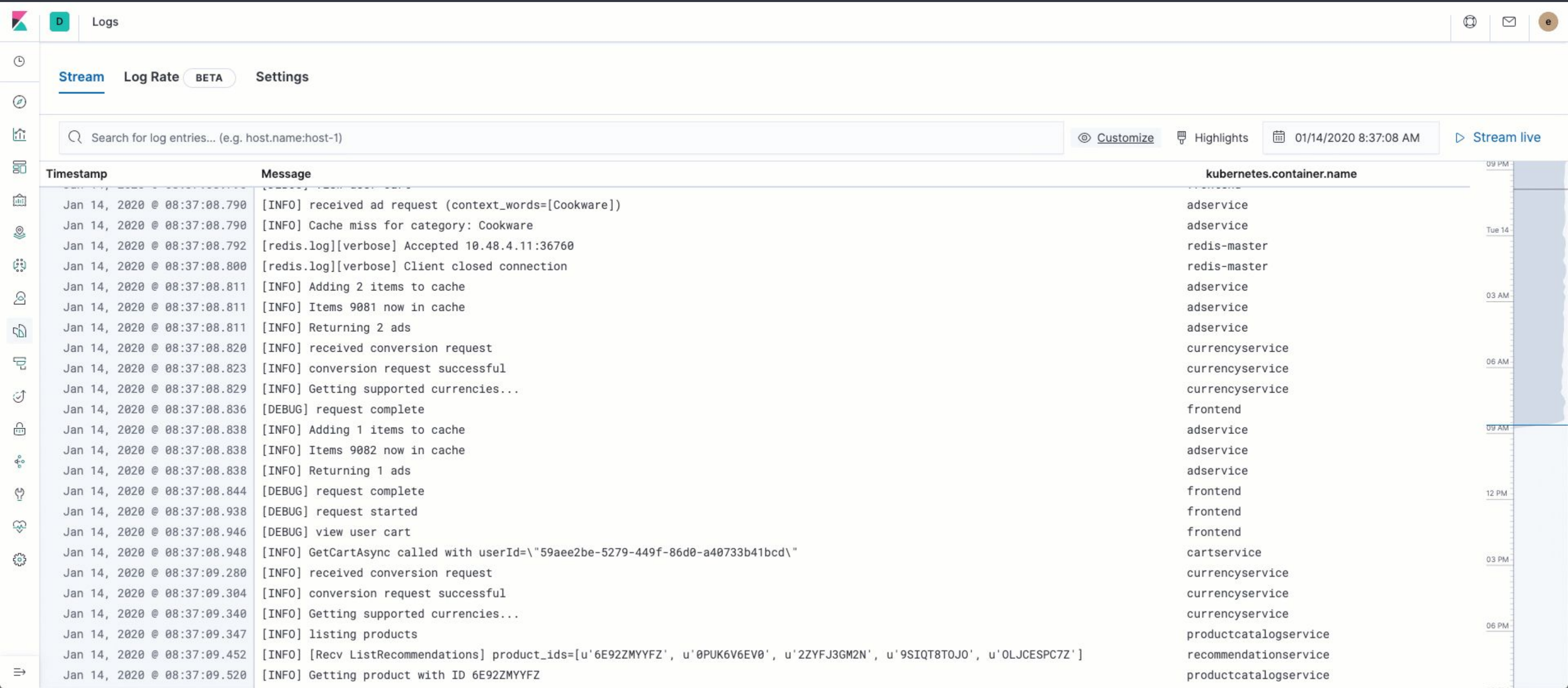
```
Jan 14, 2020 @ 08:37:08.790  [INFO] received ad request (context_words=[Cook
Jan 14, 2020 @ 08:37:08.790  [INFO] Cache miss for category: Cookware
Jan 14, 2020 @ 08:37:08.792  [redis.log][verbose] Accepted 10.48.4.11:36760
Jan 14, 2020 @ 08:37:08.800  [redis.log][verbose] Client closed connection
Jan 14, 2020 @ 08:37:08.811  [INFO] Adding 2 items to cache
Jan 14, 2020 @ 08:37:08.811  [INFO] Items 9081 now in cache
Jan 14, 2020 @ 08:37:08.811  [INFO] Returning 2 ads
Jan 14, 2020 @ 08:37:08.820  [INFO] received conversion request
Jan 14, 2020 @ 08:37:08.823  [INFO] conversion request successful
Jan 14, 2020 @ 08:37:08.829  [INFO] Getting supported currencies...
Jan 14, 2020 @ 08:37:08.836  [DEBUG] request complete
Jan 14, 2020 @ 08:37:08.838  [INFO] Adding 1 items to cache
Jan 14, 2020 @ 08:37:08.838  [INFO] Items 9082 now in cache
Jan 14, 2020 @ 08:37:08.838  [INFO] Returning 1 ads
Jan 14, 2020 @ 08:37:08.844  [DEBUG] request complete
Jan 14, 2020 @ 08:37:08.938  [DEBUG] request started
Jan 14, 2020 @ 08:37:08.946  [DEBUG] view user cart
Jan 14, 2020 @ 08:37:08.948  [INFO] GetCartAsync called with userId=\"59aee2
Jan 14, 2020 @ 08:37:09.280  [INFO] received conversion request
Jan 14, 2020 @ 08:37:09.304  [INFO] conversion request successful
Jan 14, 2020 @ 08:37:09.340  [INFO] Getting supported currencies...
Jan 14, 2020 @ 08:37:09.347  [INFO] listing products
Jan 14, 2020 @ 08:37:09.452  [INFO] [Recv ListRecommendations] product_ids=[
Jan 14, 2020 @ 08:37:09.520  [INFO] Getting product with ID 6E92ZMYYFZ
```

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 f8b2b863ceb9b839f85bf7785d09cf43ac8001e6ecaaee45ce3742 3f08d90366

Needs for log analytics

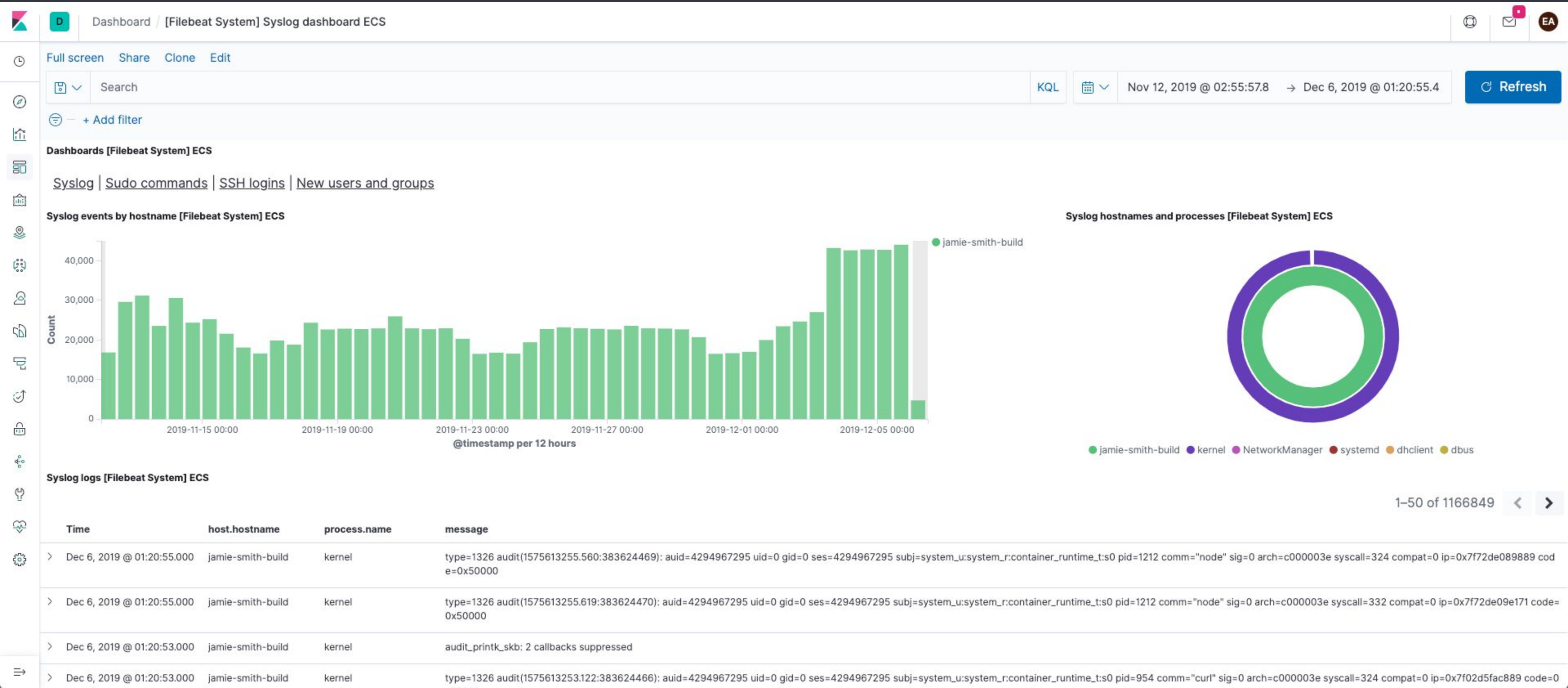
Searching, filtering, and highlighting



```
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                                                                             frontend
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



Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Syslog events by hostname [Filebeat System] ECS

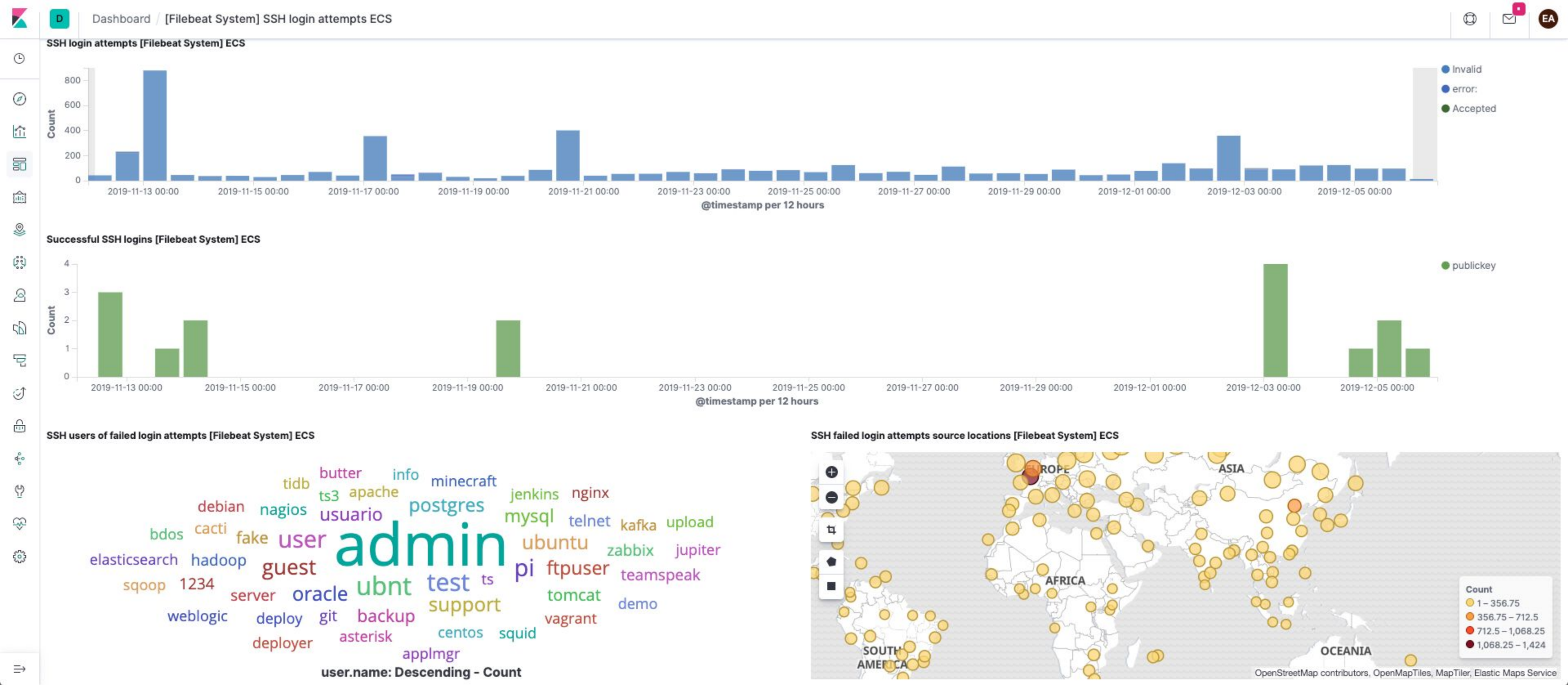
Syslog hostnames and processes [Filebeat System] ECS

Syslog logs [Filebeat System] ECS

Time	host.hostname	process.name	message
Dec 6, 2019 @ 01:20:55.000	jamie-smith-build	kernel	type=1326 audit(1575613255.560:383624469): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=1212 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f72de089889 code=0x50000
Dec 6, 2019 @ 01:20:55.000	jamie-smith-build	kernel	type=1326 audit(1575613255.619:383624470): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=1212 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f72de09e171 code=0x50000
Dec 6, 2019 @ 01:20:53.000	jamie-smith-build	kernel	audit_printk_skb: 2 callbacks suppressed
Dec 6, 2019 @ 01:20:53.000	jamie-smith-build	kernel	type=1326 audit(1575613253.122:383624466): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=954 comm="curl" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f02d5fac889 code=0

Needs for log analytics

Visualize



Dashboard / [Filebeat System] SSH login attempts ECS

SSH login attempts [Filebeat System] ECS

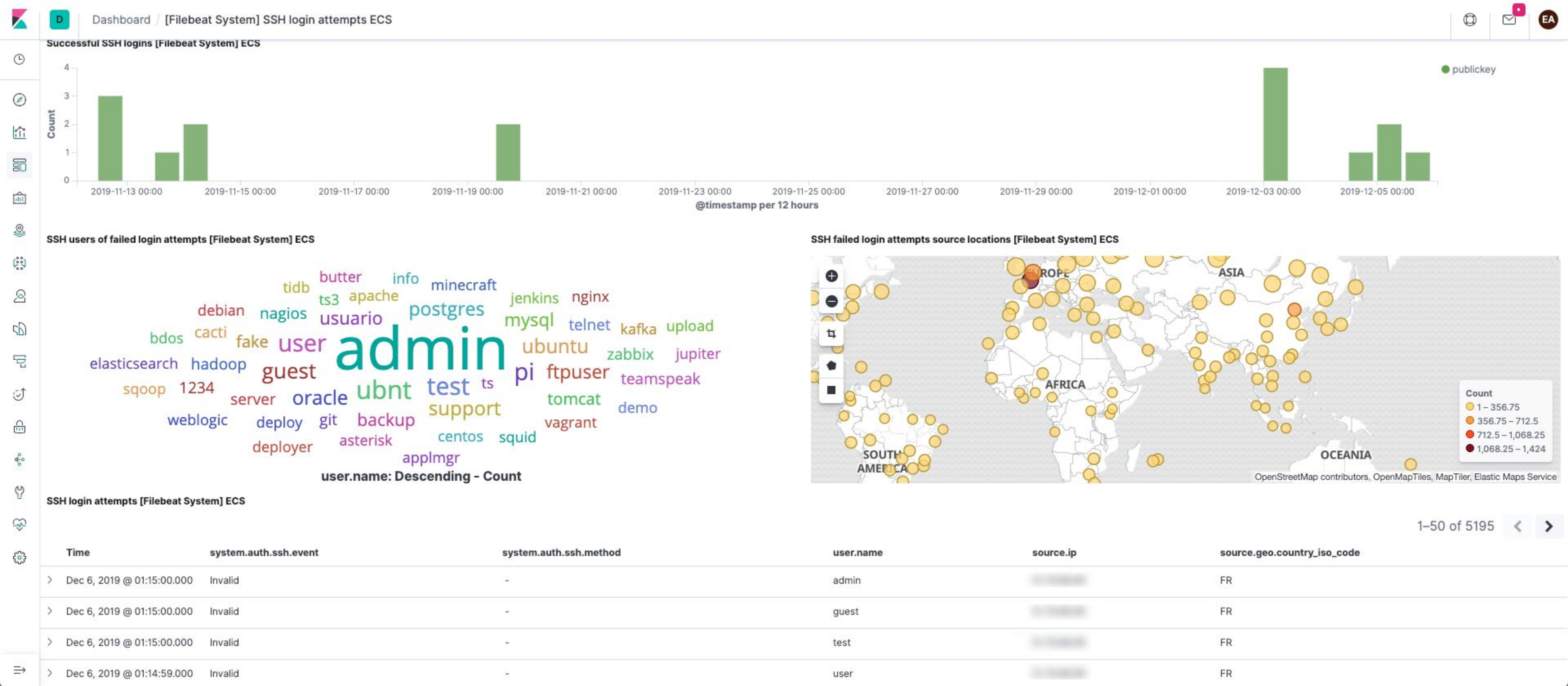
Successful SSH logins [Filebeat System] ECS

SSH users of failed login attempts [Filebeat System] ECS

SSH failed login attempts source locations [Filebeat System] ECS

Needs for log analytics

Visualize



Dashboard / [Filebeat System] SSH login attempts ECS

Successful SSH logins [Filebeat System] ECS

SSH users of failed login attempts [Filebeat System] ECS

SSH failed login attempts source locations [Filebeat System] ECS

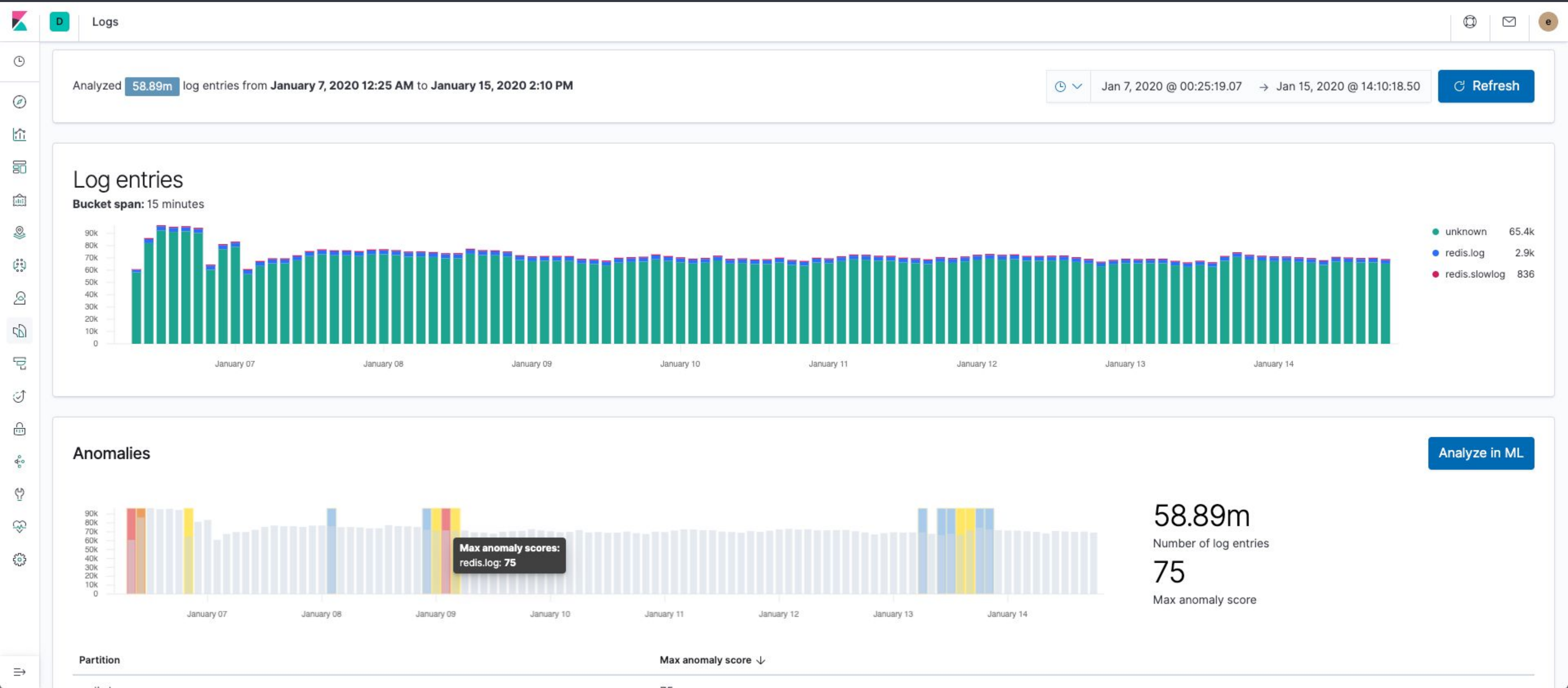
SSH login attempts [Filebeat System] ECS

1–50 of 5195

Time	system.auth.ssh.event	system.auth.ssh.method	user.name	source.ip	source.geo.country_iso_code
Dec 6, 2019 @ 01:15:00.000	Invalid	-	admin	[redacted]	FR
Dec 6, 2019 @ 01:15:00.000	Invalid	-	guest	[redacted]	FR
Dec 6, 2019 @ 01:15:00.000	Invalid	-	test	[redacted]	FR
Dec 6, 2019 @ 01:14:59.000	Invalid	-	user	[redacted]	FR

Anomaly detection and alerting

Can't stare at the screen all day



Analyzed **58.89m** log entries from **January 7, 2020 12:25 AM** to **January 15, 2020 2:10 PM**

Log entries

Bucket span: 15 minutes

● unknown	65.4k
● redis.log	2.9k
● redis.slowlog	836

Anomalies

Max anomaly scores:
redis.log: **75**

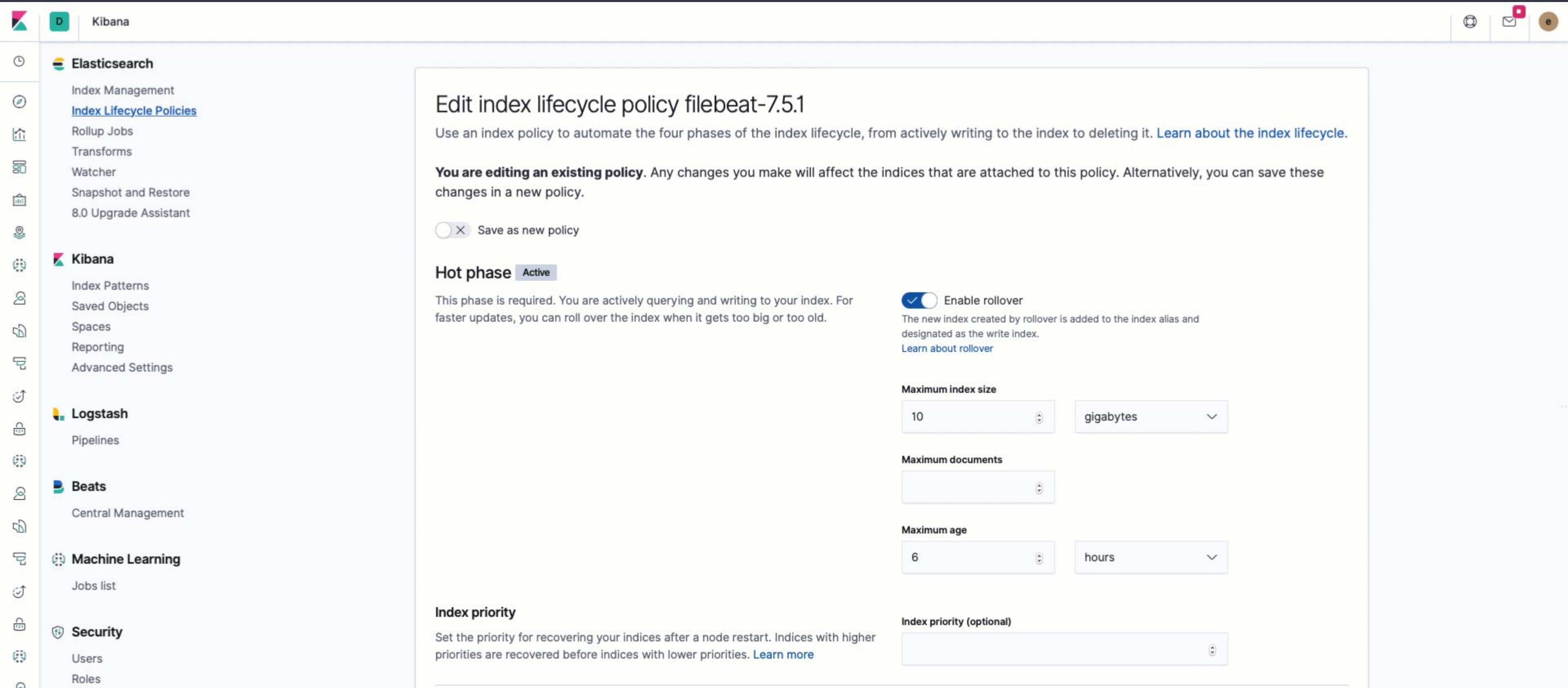
58.89m
Number of log entries

75
Max anomaly score

Partition	Max anomaly score ↓

Needs for log analytics

Flexible retention



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

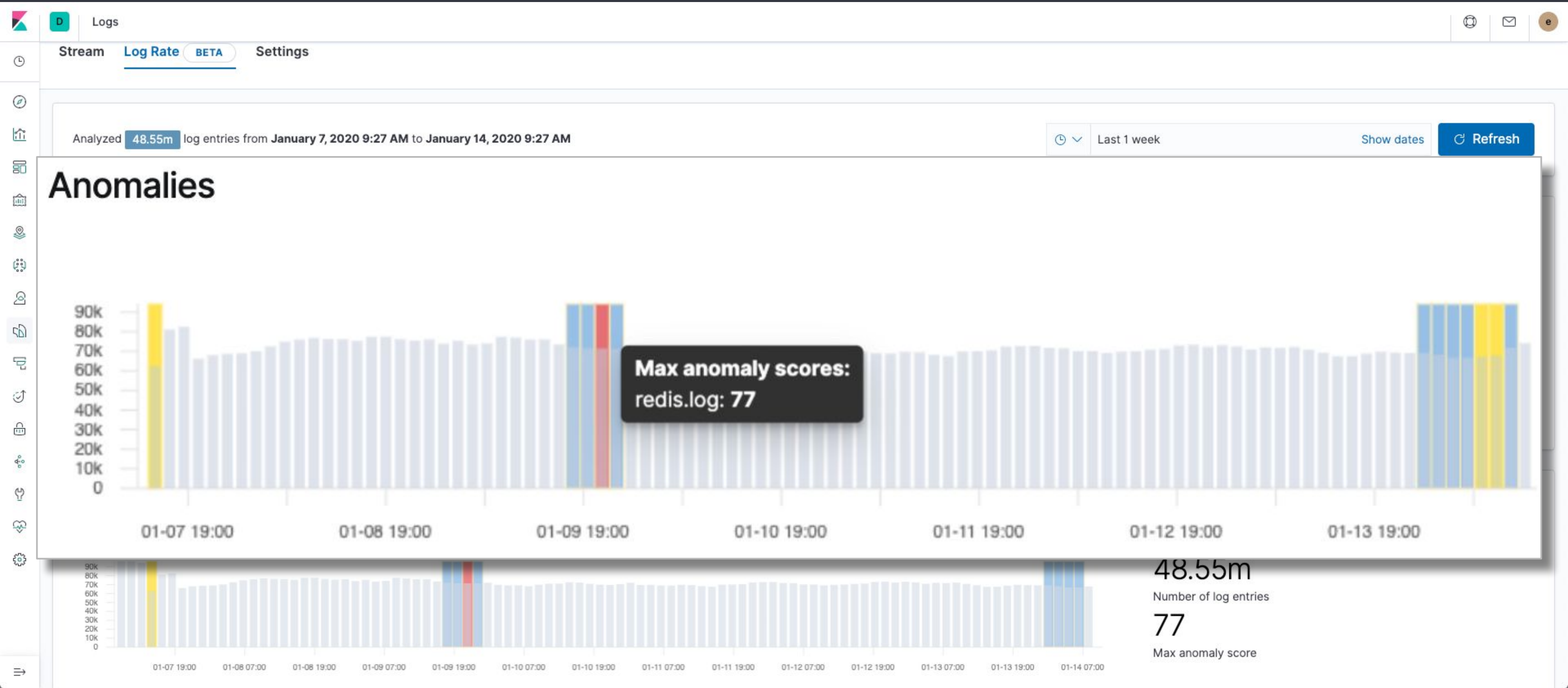
Index priority

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



Analyzed 48.55m log entries from **January 7, 2020 9:27 AM** to **January 14, 2020 9:27 AM**

Anomalies

Max anomaly scores:
redis.log: **77**

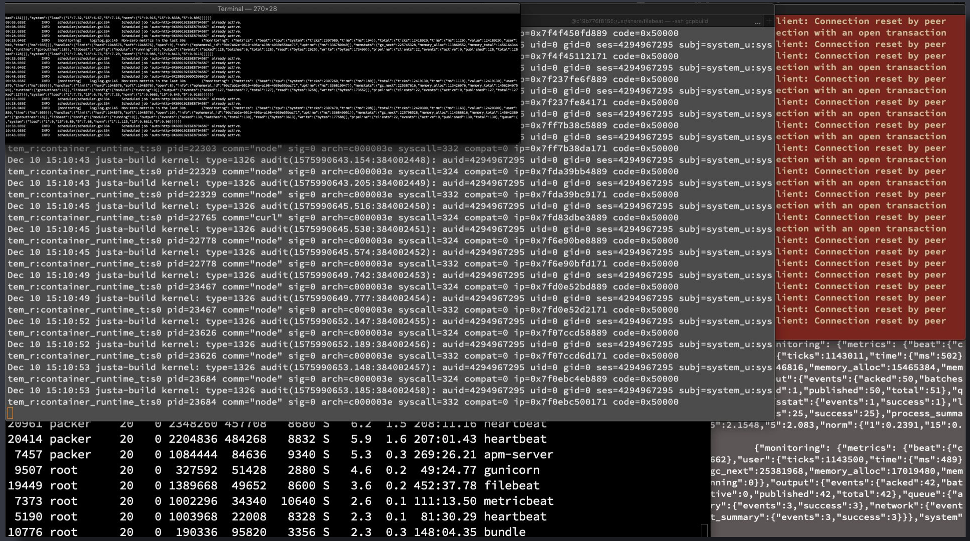
48.55m
Number of log entries

77
Max anomaly score

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



```
ked":131}}},"system":{"load":{"1":7.32,"15":6.67,"5":7.16,"norm":{"1":0.915,"15":0.8338,"5":0.895}}}}}
09:03.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:08.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307080,"time":{"ms":194}},"total":{"ticks":12418020,"time":{"ms":1129},"value":12418020},"user":
940,"time":{"ms":935}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":9},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336780049}},"memstats":{"gc_next":225745328,"memory_alloc":113860552,"memory_total":1456164344
68},"runtime":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":128,"batches":6,"total":128},"read":{"bytes":2925},"write":{"bytes":173490}},"pipeline":{"clients":22,"events":{"active":0,"published":128,"total":128
ked":128}}},"system":{"load":{"1":7.88,"15":6.73,"5":7.29,"norm":{"1":0.985,"15":0.8413,"5":0.9113}}}}}
09:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:38.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:43.040Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
09:48.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X2B802900DC5066C6' already active.
09:58.038Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307260,"time":{"ms":189}},"total":{"ticks":12419130,"time":{"ms":1119},"value":12419130},"user":
870,"time":{"ms":930}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":8},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336810047}},"memstats":{"gc_next":225387616,"memory_alloc":113426976,"memory_total":1456294075
20},"runtime":{"goroutines":15}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":127,"batches":7,"total":127},"read":{"bytes":3258},"write":{"bytes":173552}},"pipeline":{"clients":22,"events":{"active":0,"published":127,"total":127
ked":127}}},"system":{"load":{"1":7.73,"15":6.76,"5":7.33,"norm":{"1":0.9663,"15":0.845,"5":0.9163}}}}}
10:23.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:28.040Z      INFO    [monitoring]    log/log.go:145  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":2307470,"time":{"ms":208}},"total":{"ticks":12420300,"time":{"ms":1163},"value":12420300},"user":
830,"time":{"ms":955}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":10},"info":{"ephemeral_id":"90c7ab2e-0510-495a-a198-4039e55bac71","uptime":{"ms":336840051}},"memstats":{"gc_next":225798528,"memory_alloc":114388816,"memory_total":145642389
e":{"goroutines":18}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":130,"batches":8,"total":130},"read":{"bytes":3613},"write":{"bytes":177588}},"pipeline":{"clients":22,"events":{"active":0,"published":130,"total":130},"queue":{
,"system":{"load":{"1":9,"15":6.89,"5":7.68,"norm":{"1":1.125,"15":0.8613,"5":0.96}}}}}
10:33.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
10:43.039Z      INFO    scheduler/scheduler.go:334      Scheduled job 'auto-http-0X690192E6E8794587' already active.
```

```
p=0x7f4f450fd889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f4f45112171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f237fe6f889 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7f237fe84171 code=0x50000
5 uid=0 gid=0 ses=4294967295 subj=system_u:sys
p=0x7ff7b38c5889 code=0x50000
5 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
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.516:384002450): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22765 comm="curl" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fd83dbe3889 code=0x50000
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.530:384002451): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22778 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f6e90be8889 code=0x50000
Dec 10 15:10:45 justa-build kernel: type=1326 audit(1575990645.574:384002452): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=22778 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f6e90bfd171 code=0x50000
Dec 10 15:10:49 justa-build kernel: type=1326 audit(1575990649.742:384002453): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23467 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fd0e52bd889 code=0x50000
Dec 10 15:10:49 justa-build kernel: type=1326 audit(1575990649.777:384002454): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23467 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fd0e52d2171 code=0x50000
Dec 10 15:10:52 justa-build kernel: type=1326 audit(1575990652.147:384002455): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23626 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f07ccd58889 code=0x50000
Dec 10 15:10:52 justa-build kernel: type=1326 audit(1575990652.189:384002456): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23626 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f07ccd6d171 code=0x50000
Dec 10 15:10:53 justa-build kernel: type=1326 audit(1575990653.148:384002457): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23684 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7f0ebc4eb889 code=0x50000
Dec 10 15:10:53 justa-build kernel: type=1326 audit(1575990653.185:384002458): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:sys
tem_r:container_runtime_t:s0 pid=23684 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7f0ebc500171 code=0x50000
```

```
lient: Connection reset by peer
ection with an open transaction
lient: Connection reset by peer
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
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
lient: Connection reset by peer
```

```
nitoring": {"metrics": {"beat":{"c
{"ticks":1143011,"time":{"ms":502}
46816,"memory_alloc":15465384,"mem
ut":{"events":{"acked":50,"batches
d":1,"published":50,"total":51},"q
sstat":{"events":1,"success":1},"l
s":25,"success":25},"process_summa
5":2.1548,"5":2.083,"norm":{"1":0.2391,"15":0.

       {"monitoring": {"metrics": {"beat":{"c
662},"user":{"ticks":1143500,"time":{"ms":489}
gc_next":25381968,"memory_alloc":17019480,"mem
nning":0}},"output":{"events":{"acked":42,"bat
tive":0,"published":42,"total":42},"queue":{"a
ry":{"events":3,"success":3},"network":{"event
t_summary":{"events":3,"success":3}}},"system"
```

```
20961 packer    20   0 2348260 457708   8680 S   6.2  1.5 208:11.16 heartbeat
20414 packer    20   0 2204836 484268   8832 S   5.9  1.6 207:01.43 heartbeat
 7457 packer    20   0 1084444  84636   9340 S   5.3  0.3 269:26.21 apm-server
 9507 root      20   0  327592  51428   2880 S   4.6  0.2  49:24.77 gunicorn
19449 root      20   0 1389668  49652   8600 S   3.6  0.2 452:37.78 filebeat
 7373 root      20   0 1002296  34340  10640 S   2.6  0.1 111:13.50 metricbeat
 5190 root      20   0 1003968  22008   8328 S   2.3  0.1  81:30.29 heartbeat
10776 root      20   0  190336  95820   3356 S   2.3  0.3 148:04.35 bundle
```

elastic

Agenda

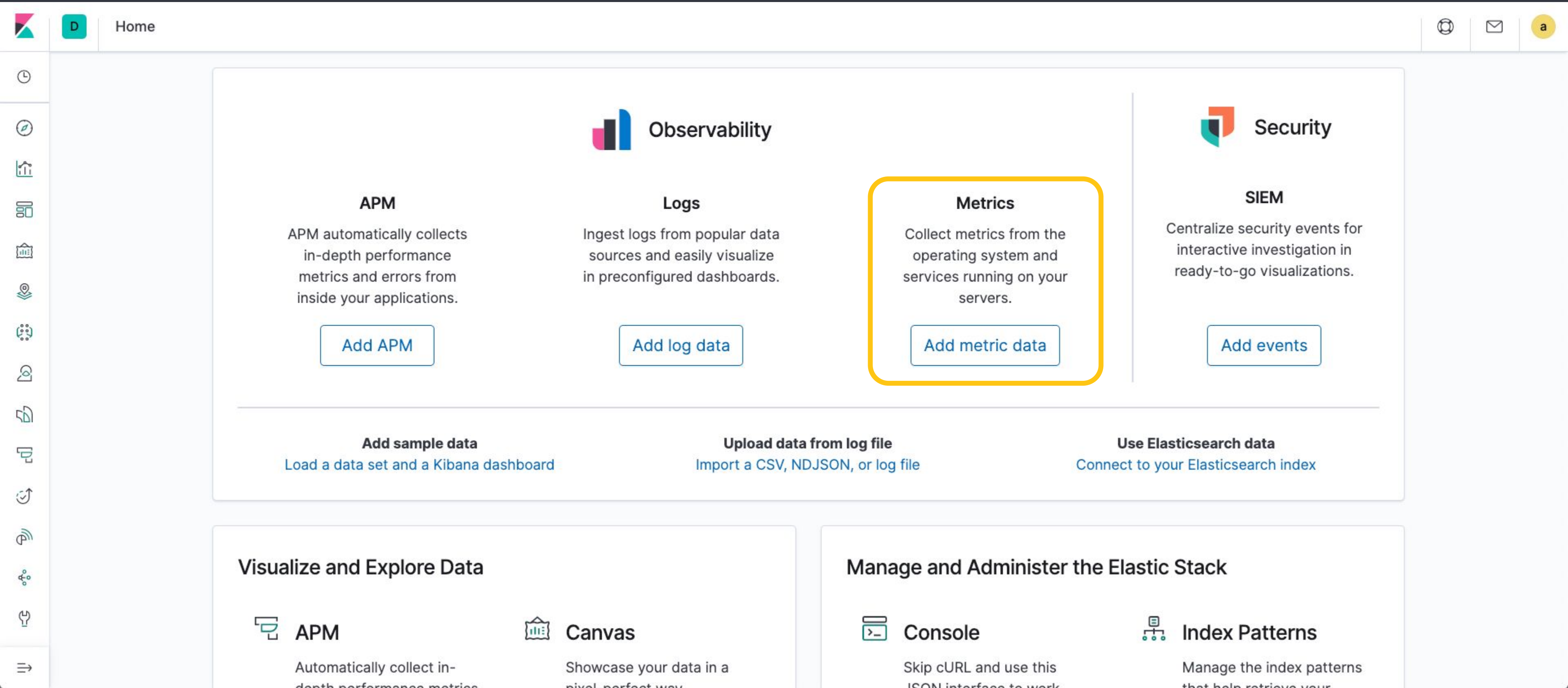
Beyond logging: Observability

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

elastic

You can add metrics in the same manner

Select your integration



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

SIEM

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

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

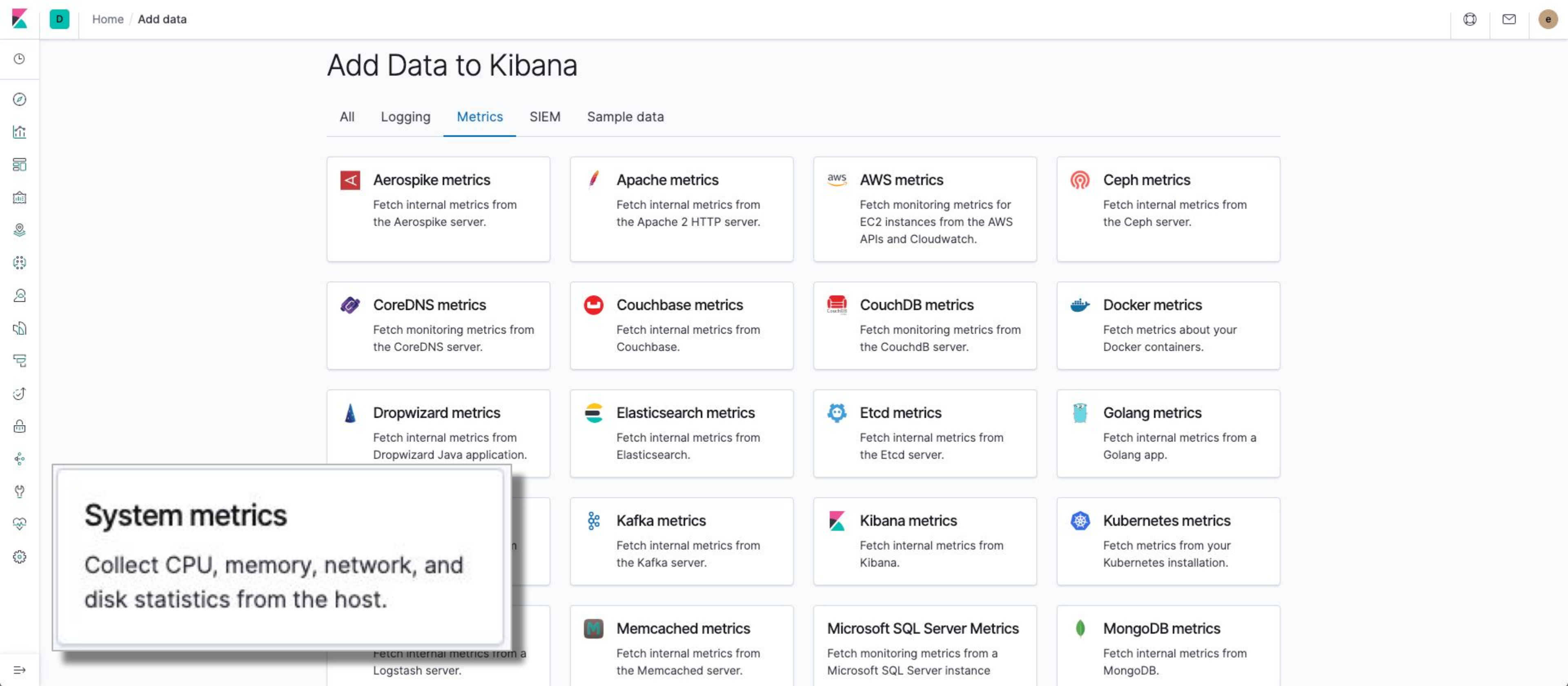
Skip cURL and use this JSON interface to work

Index Patterns

Manage the index patterns that help retrieve your

Many integrations

For example, system metrics



Add Data to Kibana

All | Logging | Metrics | SIEM | Sample data

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.

Fetch internal metrics from a Logstash server.

Memcached metrics
Fetch internal metrics from the Memcached server.

Microsoft SQL Server Metrics
Fetch monitoring metrics from a Microsoft SQL Server instance

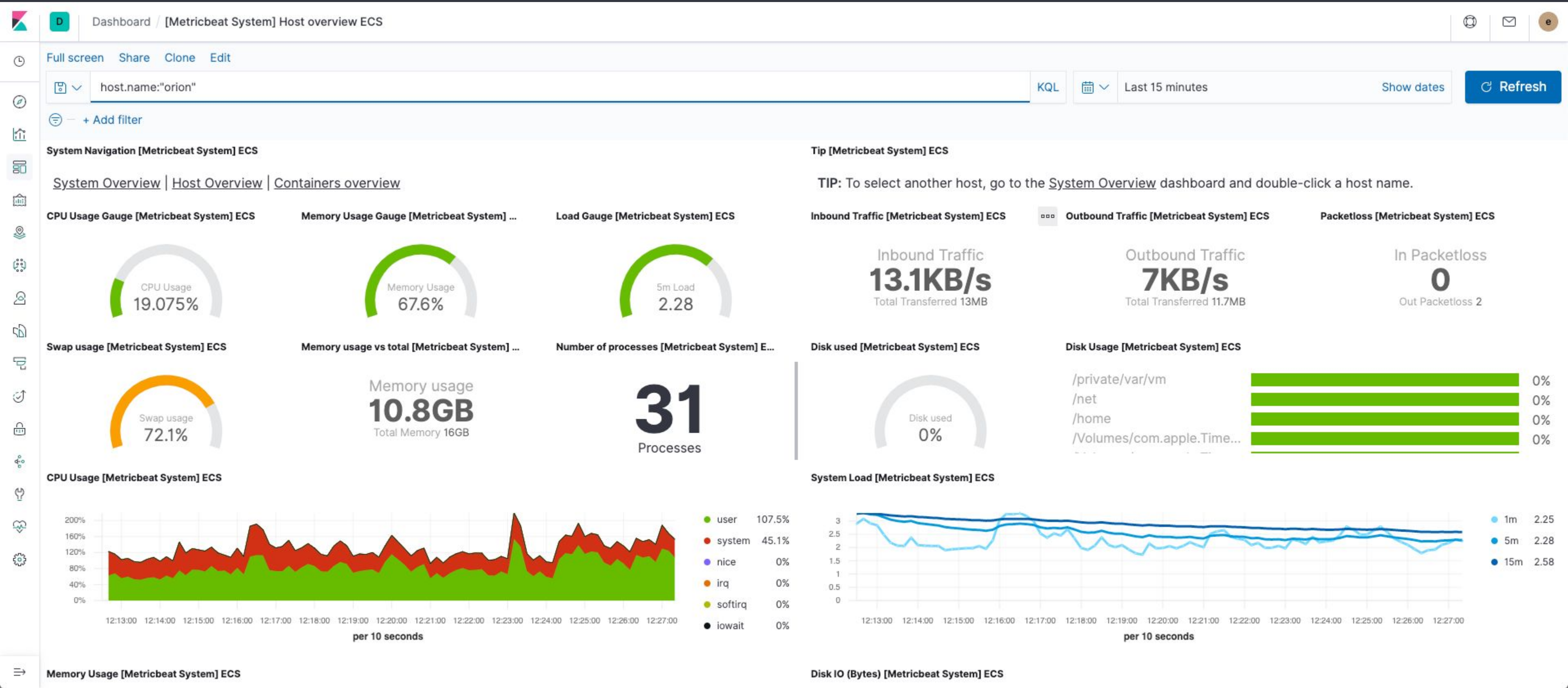
MongoDB metrics
Fetch internal metrics from MongoDB.

System metrics

Collect CPU, memory, network, and disk statistics from the host.

Metrics

Visualizing metrics



Dashboard / [Metricbeat System] Host overview ECS

Full screen Share Clone Edit

host.name:"orion"

KQL

Last 15 minutes

Show dates

Refresh

+ Add filter

System Navigation [Metricbeat System] ECS

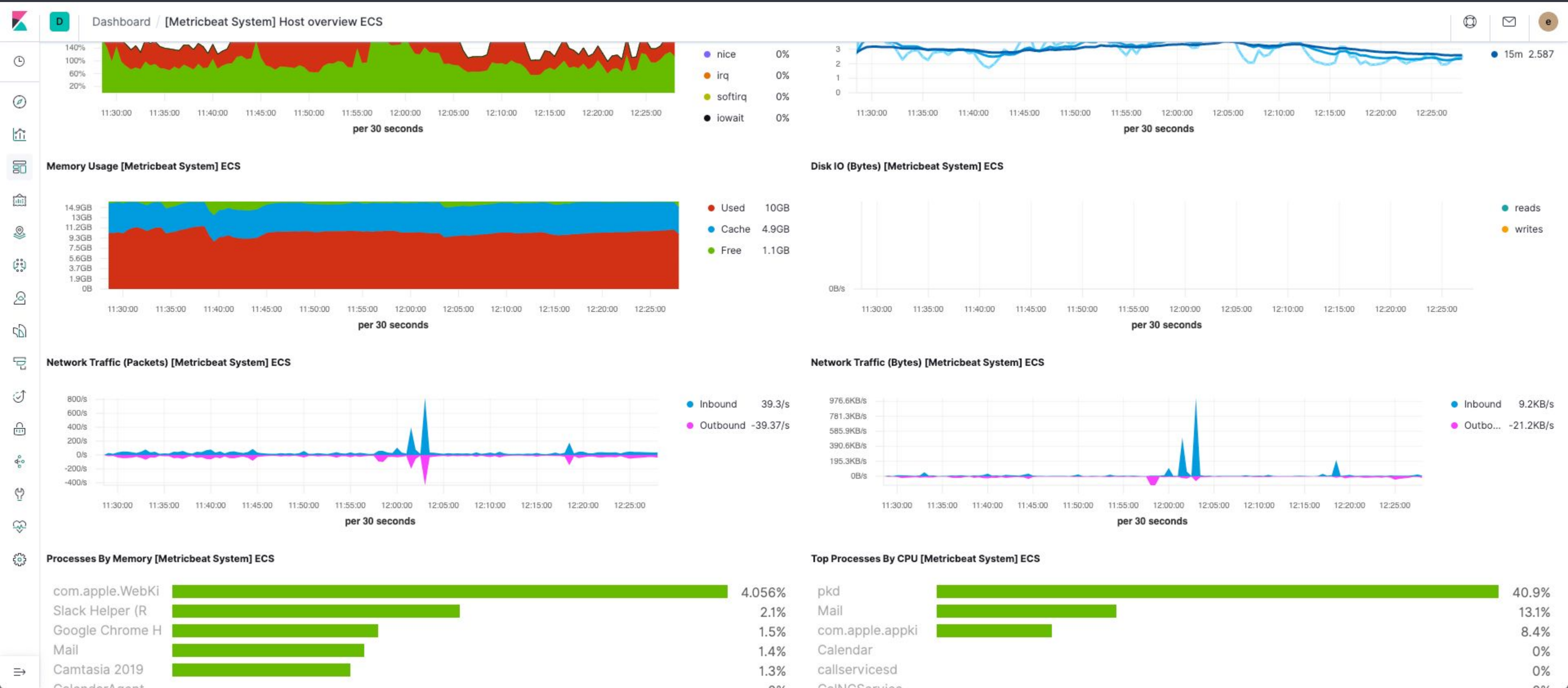
System Overview | Host Overview | Containers overview

Tip [Metricbeat System] ECS

TIP: To select another host, go to the System Overview dashboard and double-click a host name.

Metrics

Visualizing metrics



Dashboard / [Metricbeat System] Host overview ECS

● nice	0%
● irq	0%
● softirq	0%
● iowait	0%

● 15m 2.587

Memory Usage [Metricbeat System] ECS

● Used	10GB
● Cache	4.9GB
● Free	1.1GB

Disk IO (Bytes) [Metricbeat System] ECS

● reads
● writes

Network Traffic (Packets) [Metricbeat System] ECS

● Inbound	39.3/s
● Outbound	-39.37/s

Network Traffic (Bytes) [Metricbeat System] ECS

● Inbound	9.2KB/s
● Outbo...	-21.2KB/s

Processes By Memory [Metricbeat System] ECS

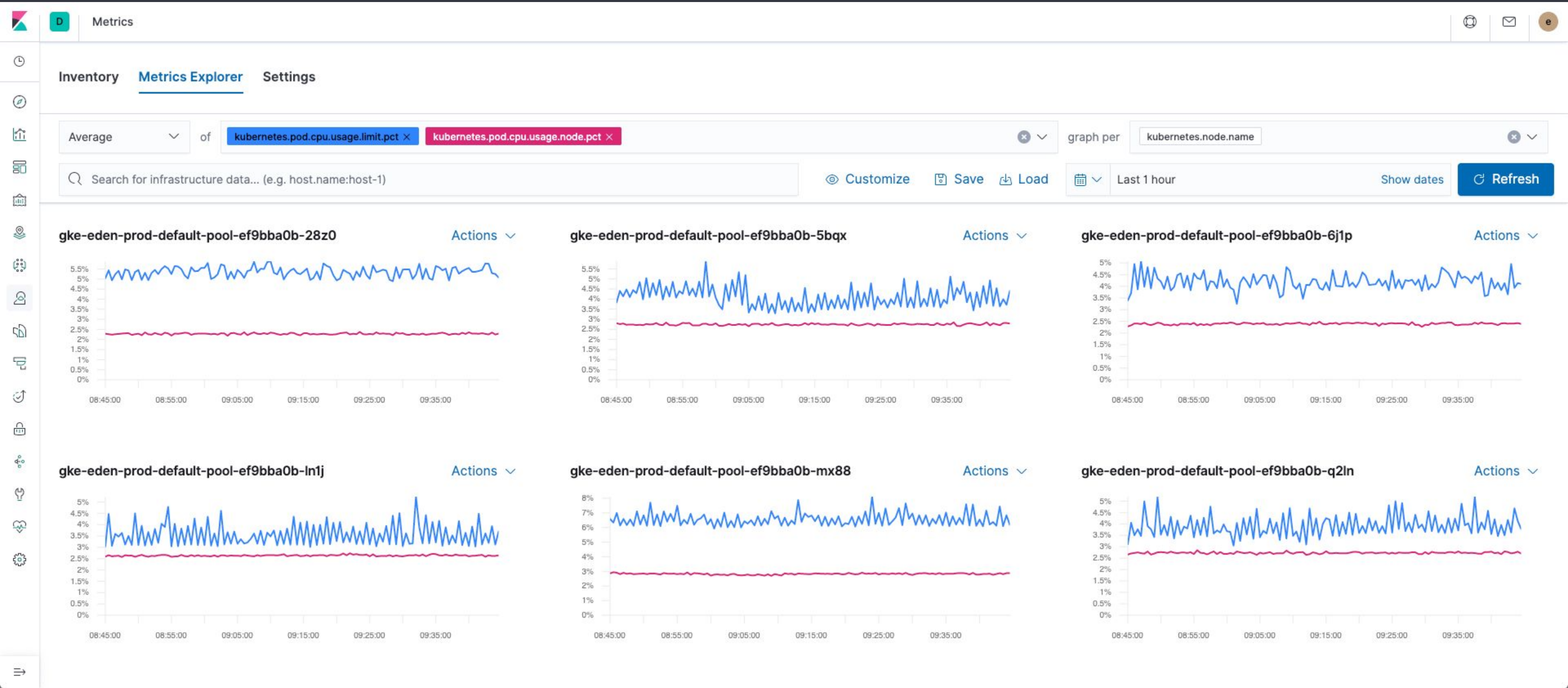
com.apple.WebKi	4.056%
Slack Helper (R	2.1%
Google Chrome H	1.5%
Mail	1.4%
Camtasia 2019	1.3%

Top Processes By CPU [Metricbeat System] ECS

pkd	40.9%
Mail	13.1%
com.apple.appki	8.4%
Calendar	0%
callservicesd	0%

Metrics

Exploring metrics



Average of kubernetes.pod.cpu.usage.limit.pct × kubernetes.pod.cpu.usage.node.pct × graph per kubernetes.node.name

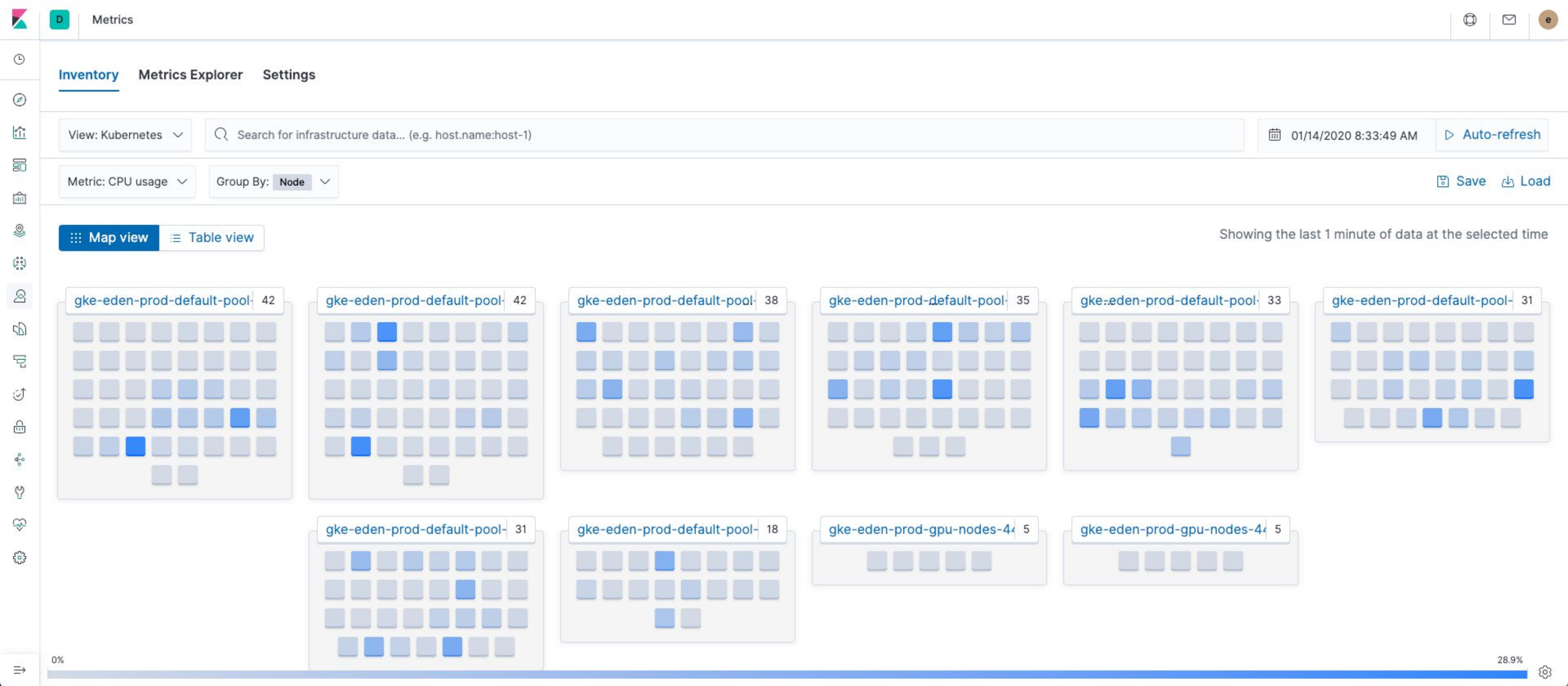
Search for infrastructure data... (e.g. host.name:host-1)

Last 1 hour

D
Metrics
Inventory
Metrics Explorer
Settings
Customize
Save
Load
Show dates
Refresh
gke-eden-prod-default-pool-ef9bba0b-28z0
Actions
5.5%
5%
4.5%
4%
3.5%
3%
2.5%
2%
1.5%
1%
0.5%
0%
08:45:00
08:55:00
09:05:00
09:15:00
09:25:00
09:35:00
gke-eden-prod-default-pool-ef9bba0b-5bqx
Actions
gke-eden-prod-default-pool-ef9bba0b-6j1p
Actions
gke-eden-prod-default-pool-ef9bba0b-ln1j
Actions
gke-eden-prod-default-pool-ef9bba0b-mx88
Actions
8%
7%
6%
5%
4%
3%
2%
1%
0%
gke-eden-prod-default-pool-ef9bba0b-q2ln
Actions
e

Metrics

Inventory view with multiple perspectives



View: Kubernetes

Search for infrastructure data... (e.g. host.name:host-1)

01/14/2020 8:33:49 AM

Metric: CPU usage

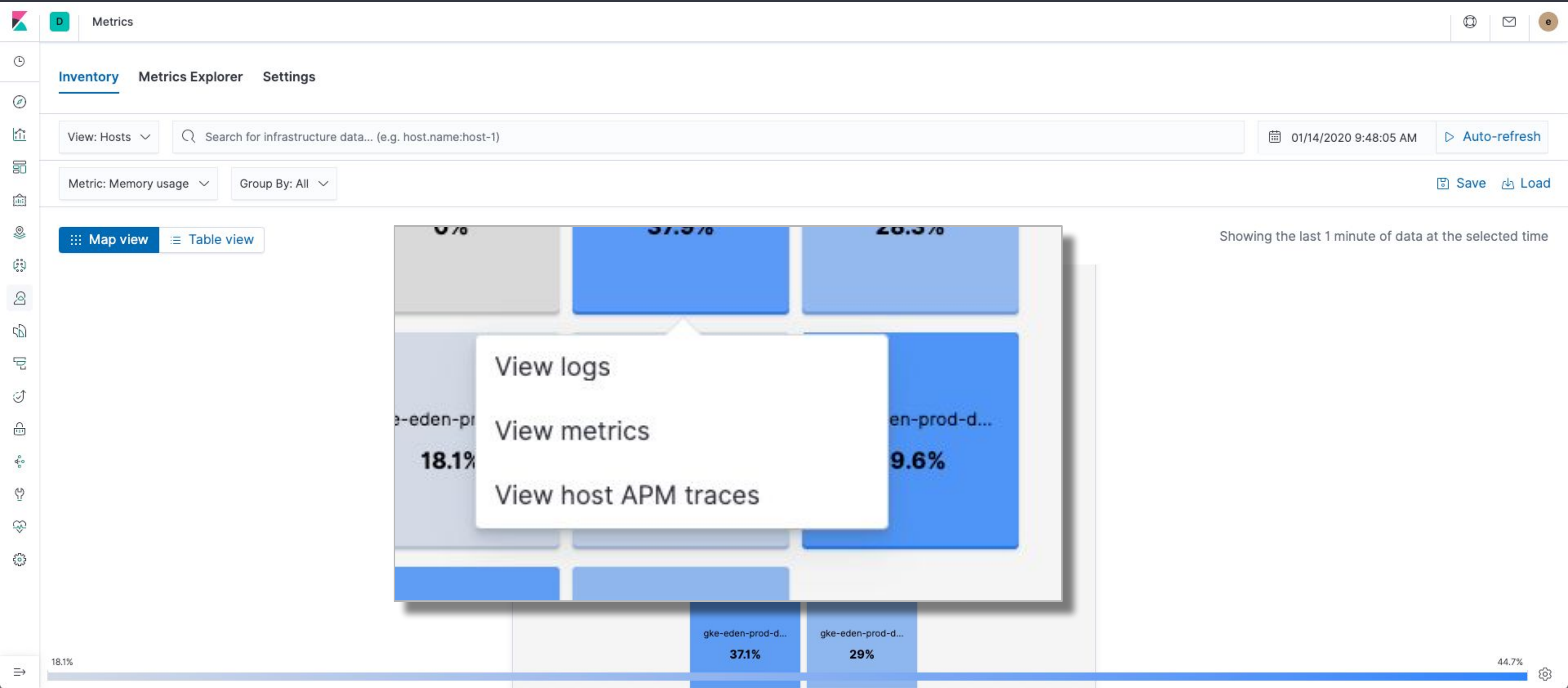
Group By: Node

Showing the last 1 minute of data at the selected time

gke-eden-prod-default-pool-	42
gke-eden-prod-default-pool-	42
gke-eden-prod-default-pool-	38
gke-eden-prod-default-pool-	35
gke-eden-prod-default-pool-	33
gke-eden-prod-default-pool-	31
gke-eden-prod-default-pool-	31
gke-eden-prod-default-pool-	18
gke-eden-prod-gpu-nodes-4	5
gke-eden-prod-gpu-nodes-4	5

Integrated Experience

Observability with one datastore



View: Hosts

Search for infrastructure data... (e.g. host.name:host-1)

01/14/2020 9:48:05 AM

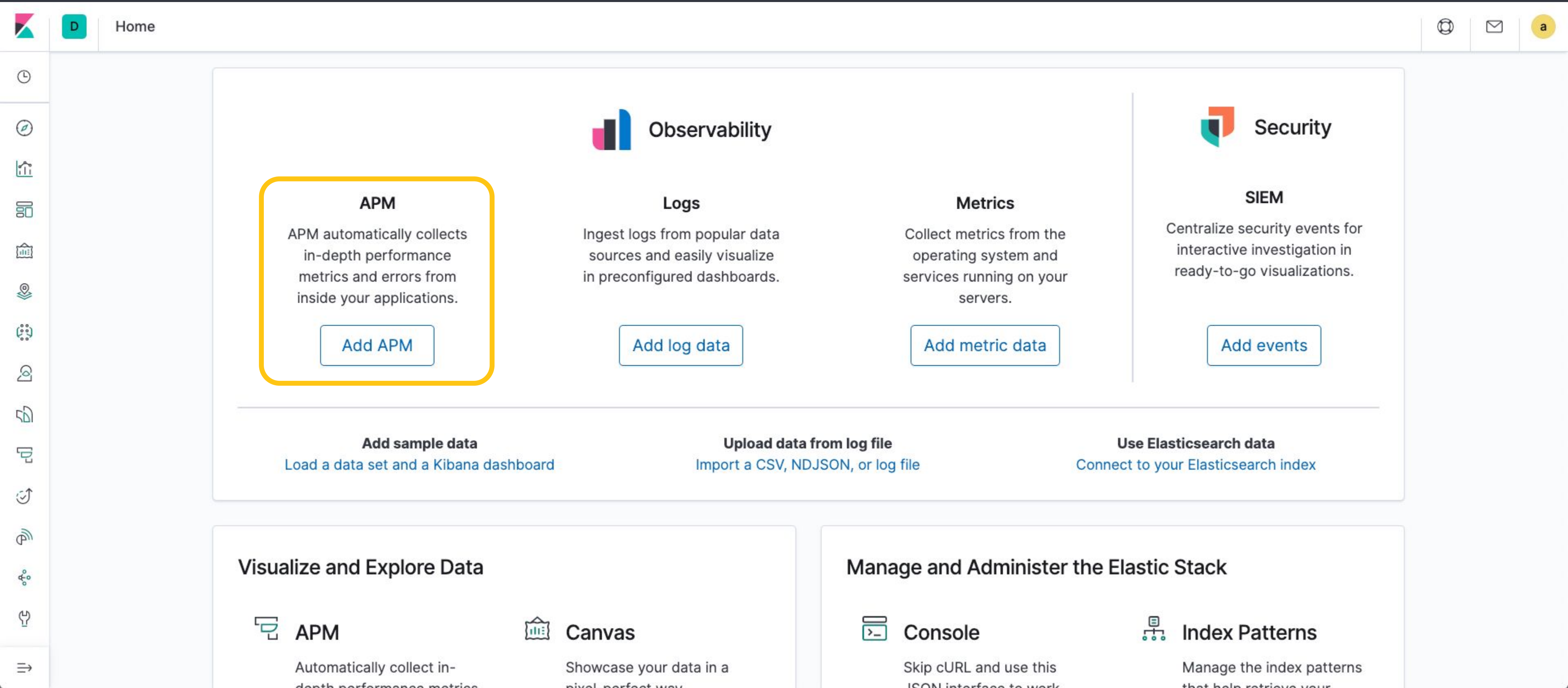
Metric: Memory usage

Group By: All

Showing the last 1 minute of data at the selected time

Setting up APM

Instructions in Kibana



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

SIEM

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

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

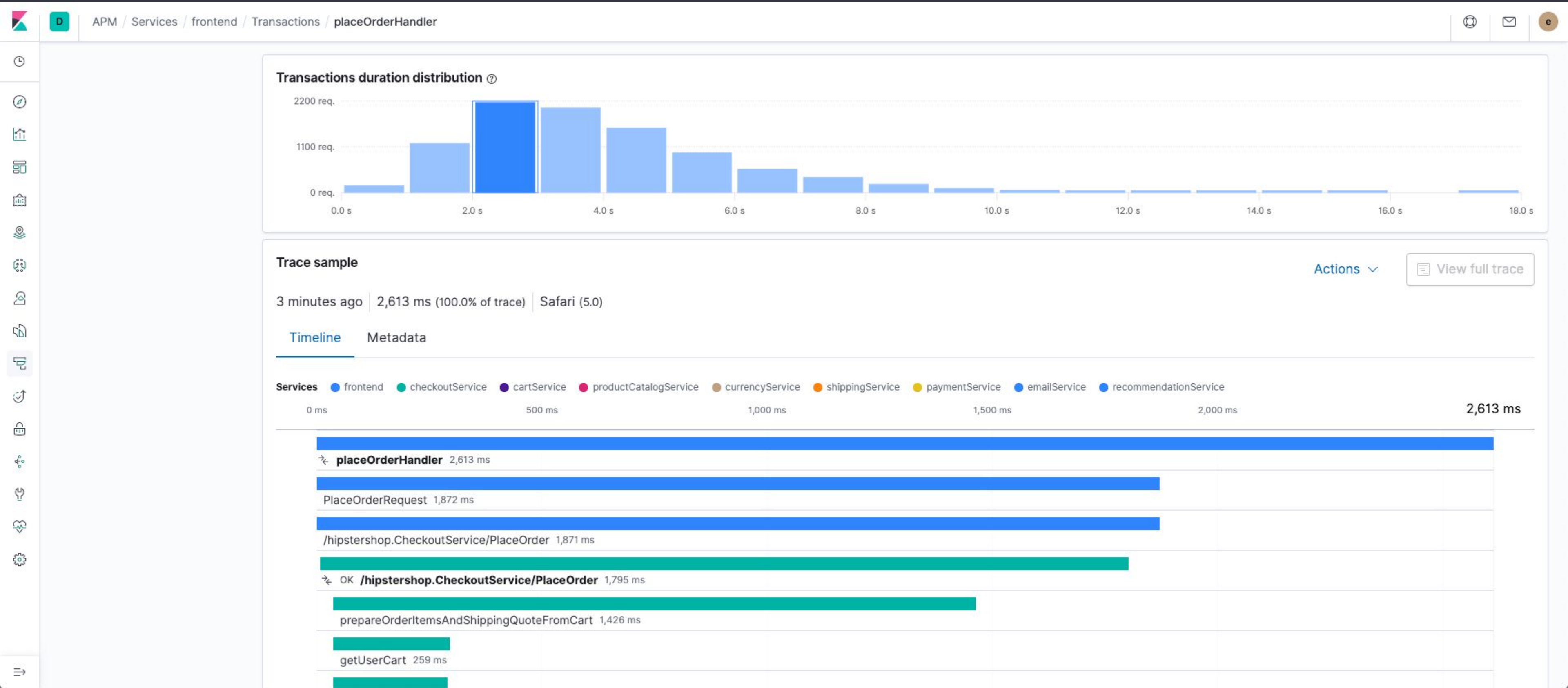
Skip cURL and use this JSON interface to work

Index Patterns

Manage the index patterns that help retrieve your

Application Performance Monitoring

Distributed Tracing



APM / Services / frontend / Transactions / placeOrderHandler

Transactions duration distribution

Trace sample

3 minutes ago | 2,613 ms (100.0% of trace) | Safari (5.0)

Services ● frontend ● checkoutService ● cartService ● productCatalogService ● currencyService ● shippingService ● paymentService ● emailService ● recommendationService

placeOrderHandler 2,613 ms

PlaceOrderRequest 1,872 ms

/hipstershop.CheckoutService/PlaceOrder 1,871 ms

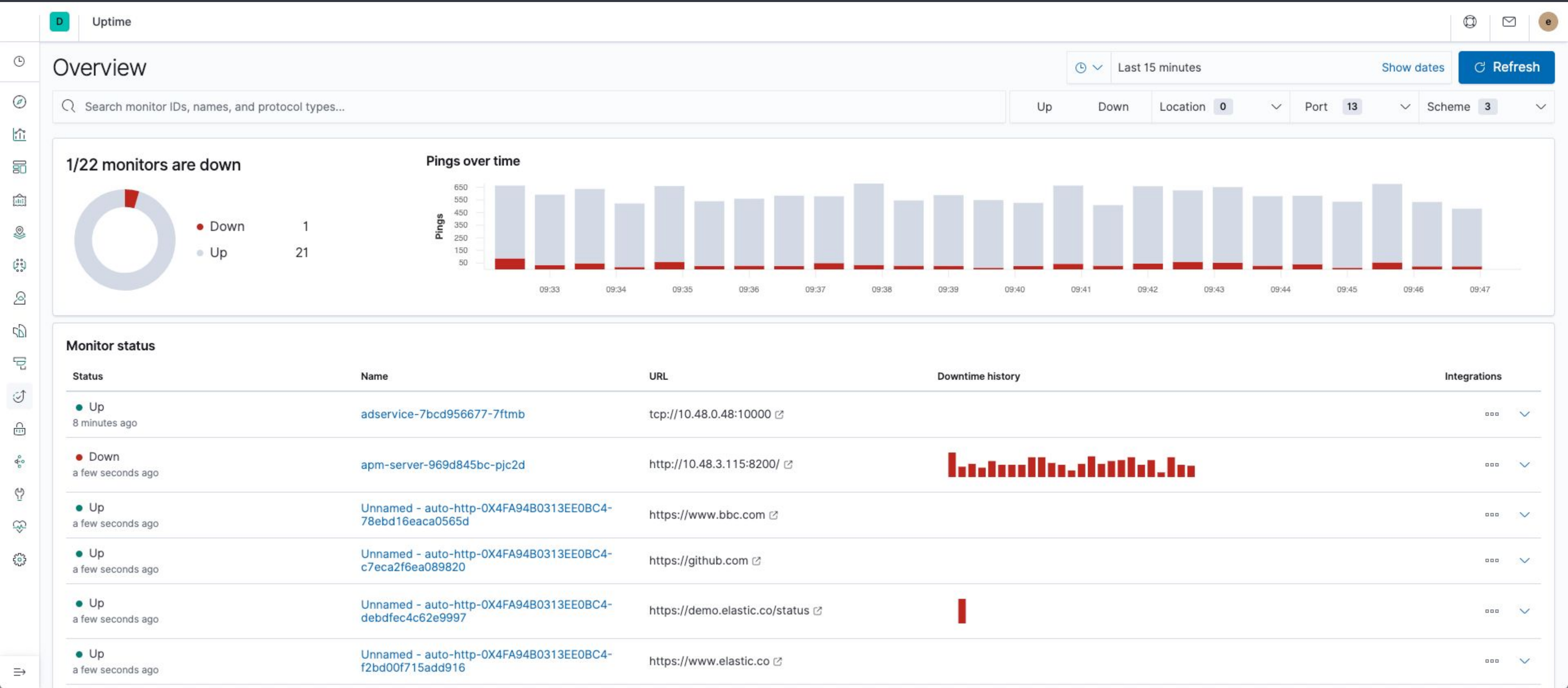
OK **/hipstershop.CheckoutService/PlaceOrder** 1,795 ms

prepareOrderItemsAndShippingQuoteFromCart 1,426 ms

getUserCart 259 ms

Uptime Monitoring

Service availability



1/22 monitors are down

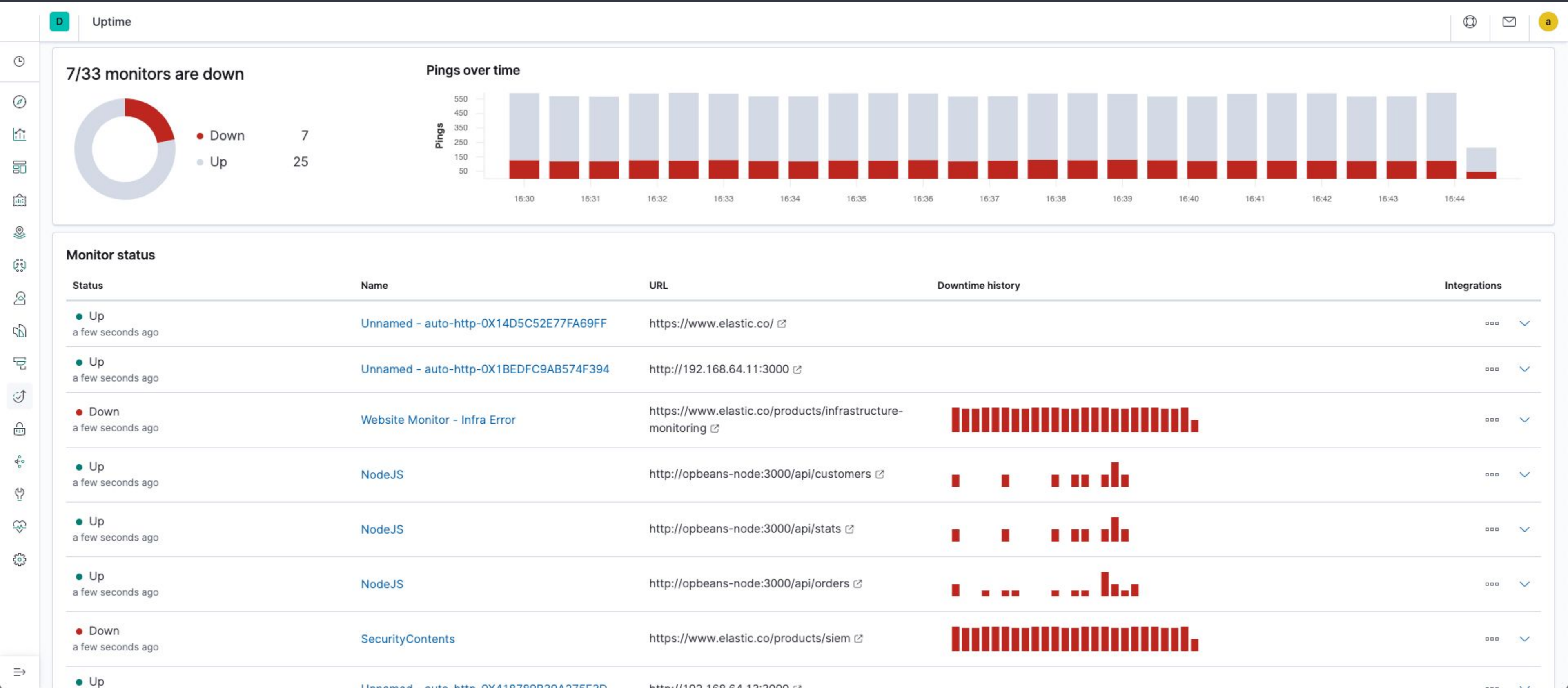
● Down	1
● Up	21

Monitor status

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-debdfec4c62e9997	https://demo.elastic.co/status		
● Up a few seconds ago	Unnamed - auto-http-0X4FA94B0313EE0BC4-f2bd00f715add916	https://www.elastic.co		

Uptime Monitoring

Service availability



7/33 monitors are down

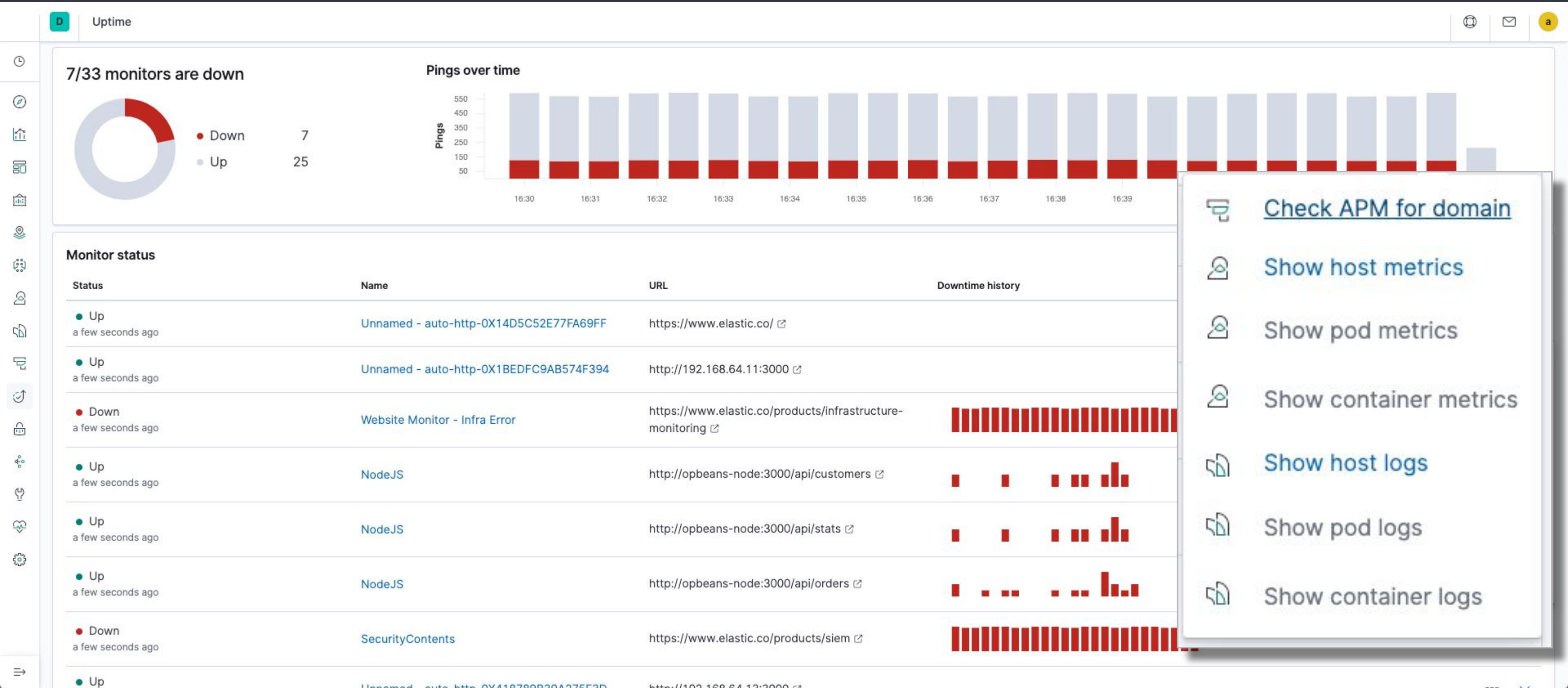
● Down	7
● Up	25

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				

Uptime Monitoring

Integrated experience



7/33 monitors are down

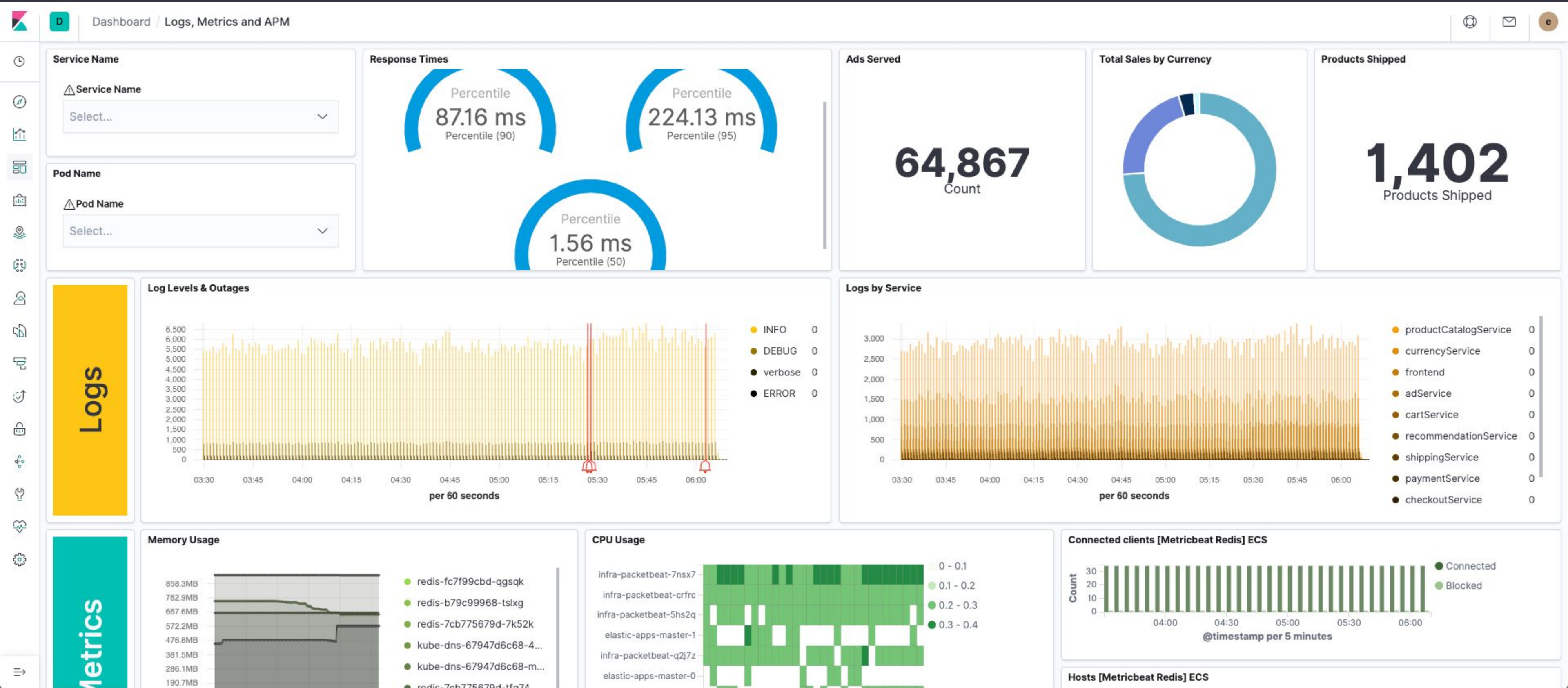
● Down	7
● Up	25

Monitor status

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			

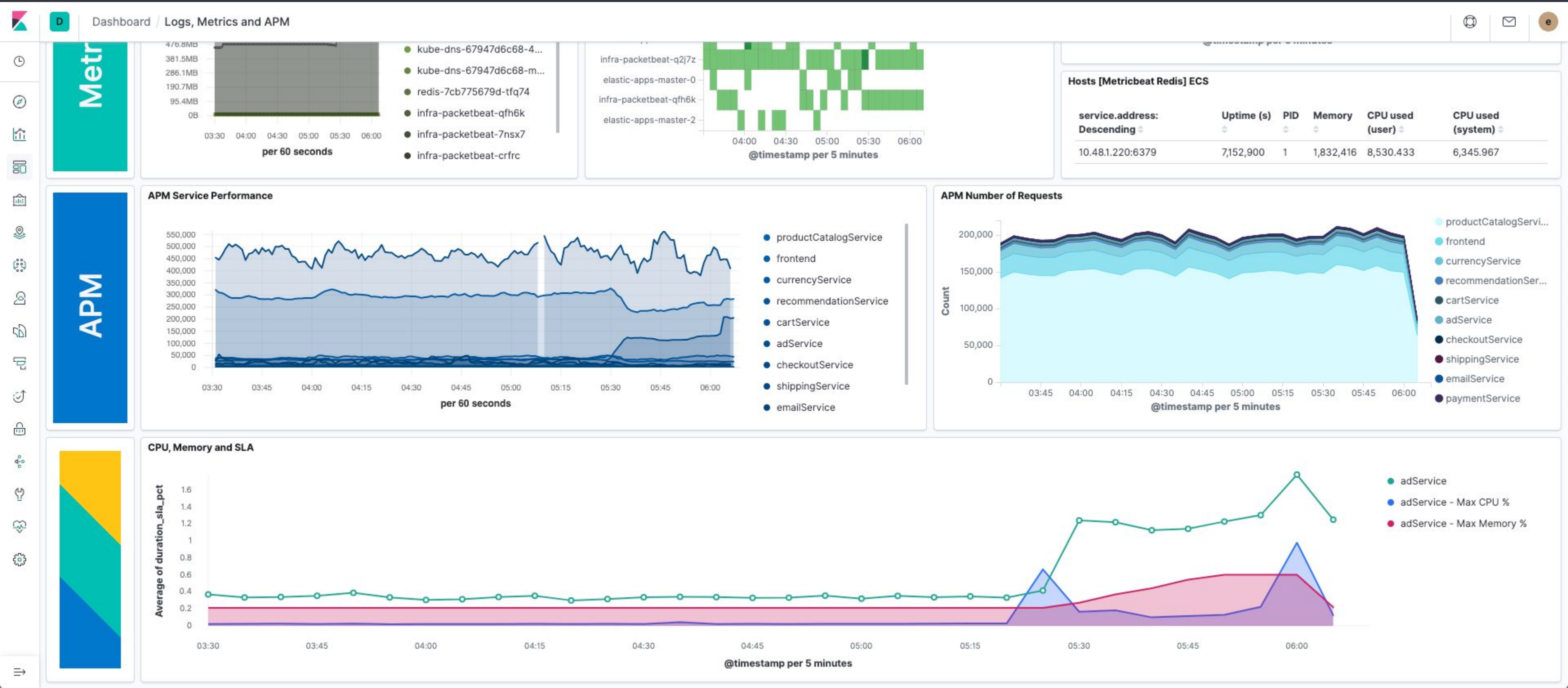
Integrated Experience

Observability with one datastore



Integrated Experience

Observability with one datastore



Dashboard / Logs, Metrics and APM

Hosts [Metricbeat Redis] ECS

service.address: Descending	Uptime (s)	PID	Memory	CPU used (user)	CPU used (system)
10.48.1.220:6379	7,152,900	1	1,832,416	8,530.433	6,345.967

APM Service Performance

APM Number of Requests

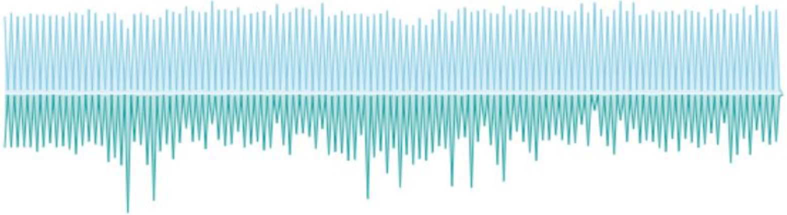
CPU, Memory and SLA

Deployment Observability

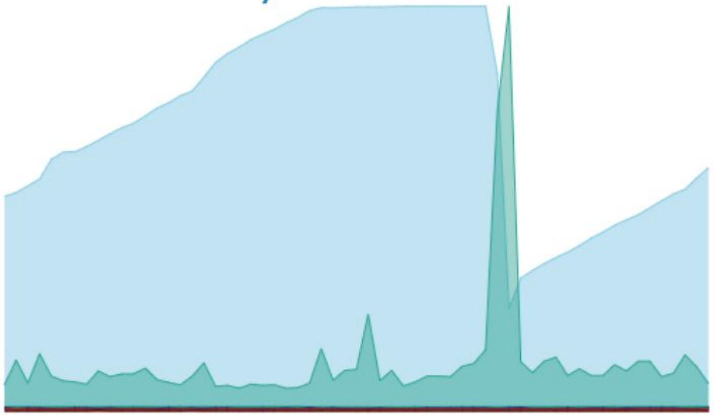
Network

Traffic In

Traffic Out



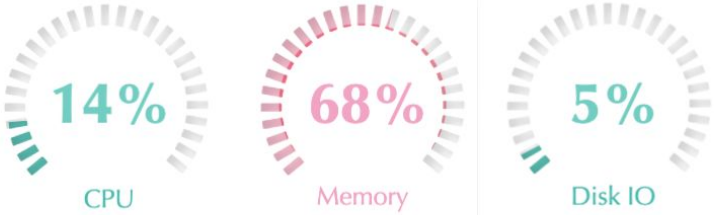
CPU/Memory



Disk IO

Read

Write

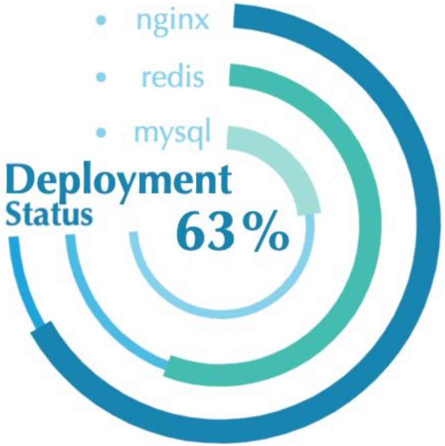


Services 10

Containers 141

Errors 19413

Pods 70



Agenda

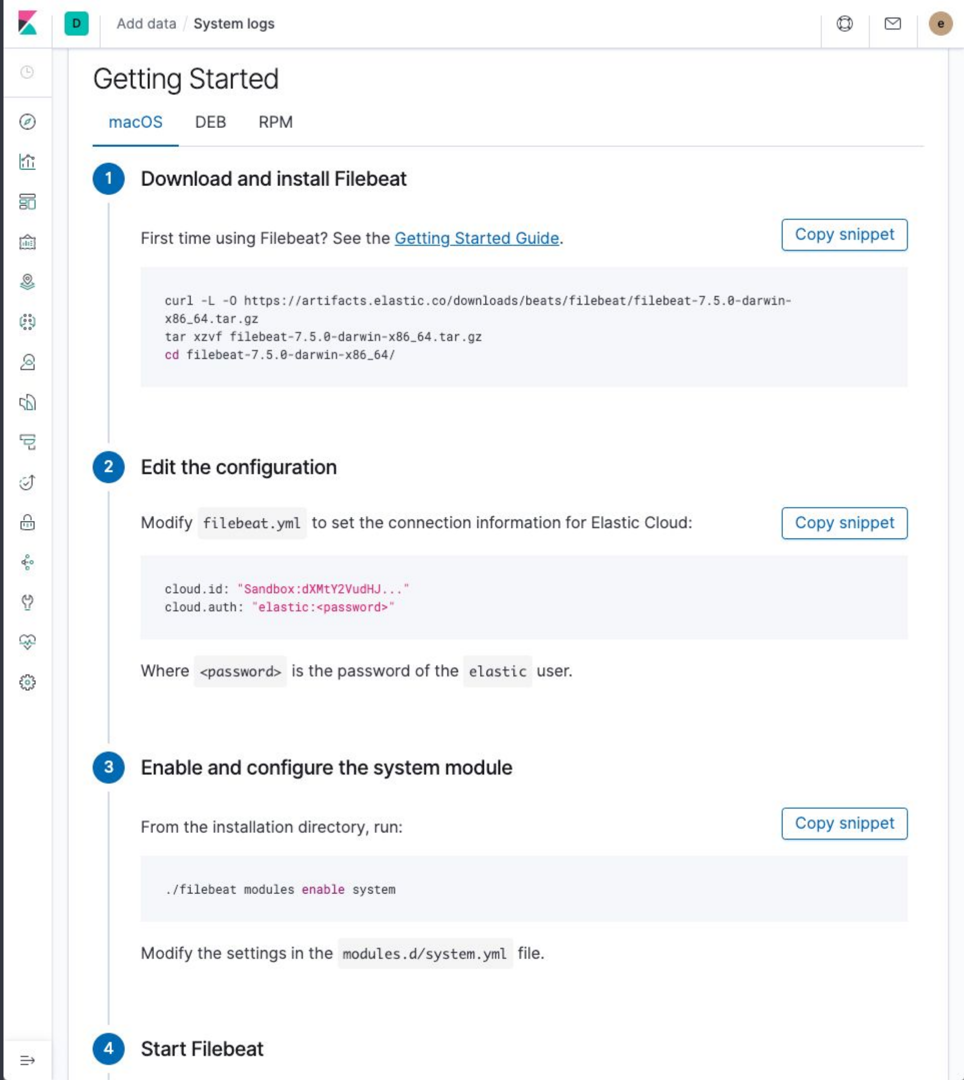
Securing your Beats

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



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
```

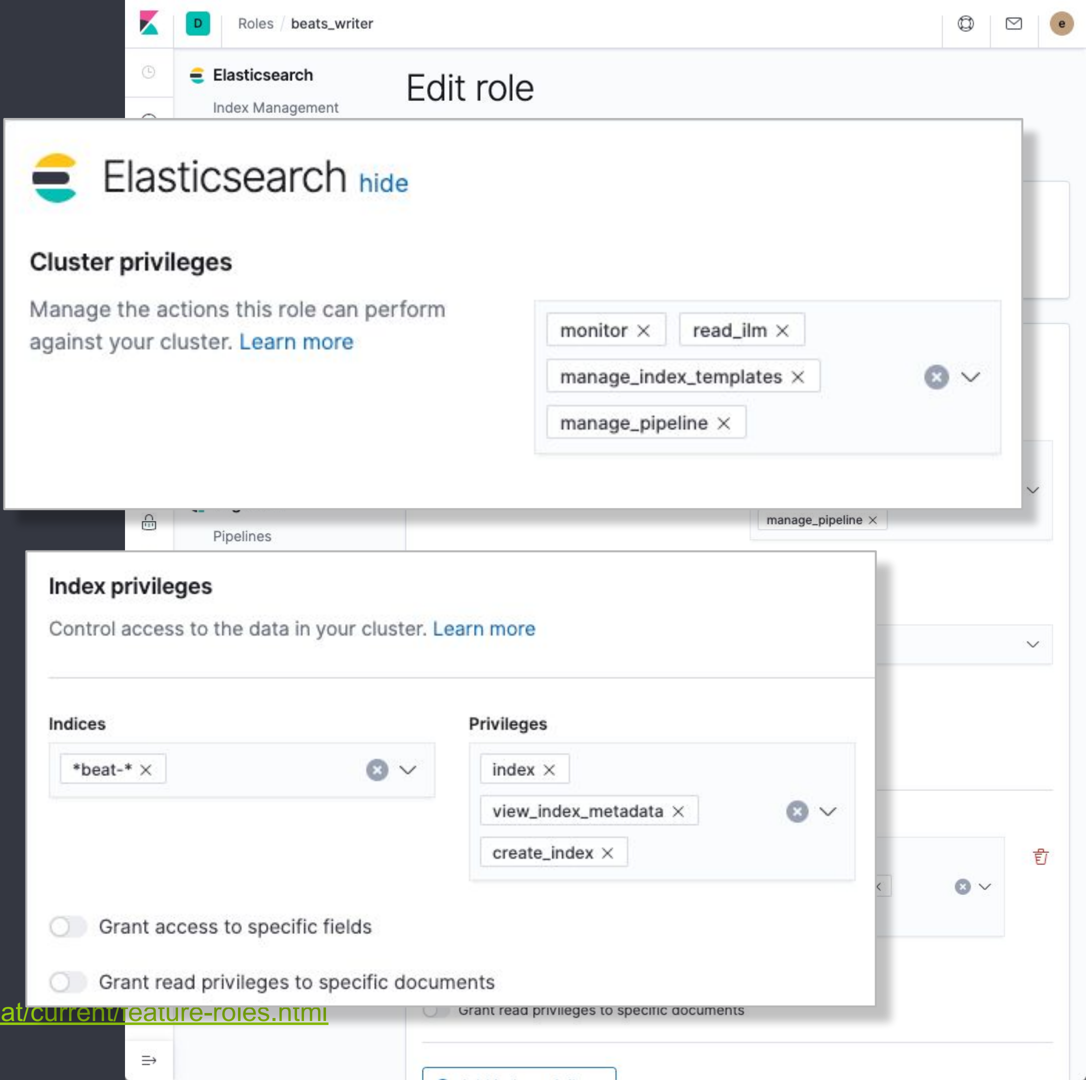
Modify the settings in the `modules.d/system.yml` file.

4 Start Filebeat

beats_writer Role

Required permissions

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



Elasticsearch hide

Cluster privileges

Manage the actions this role can perform against your cluster. Learn more

monitor × read_ilm × manage_index_templates × manage_pipeline ×

Index privileges

Control access to the data in your cluster. Learn more

Indices: *beat-* ×

Privileges: index × view_index_metadata × create_index ×

○ Grant access to specific fields

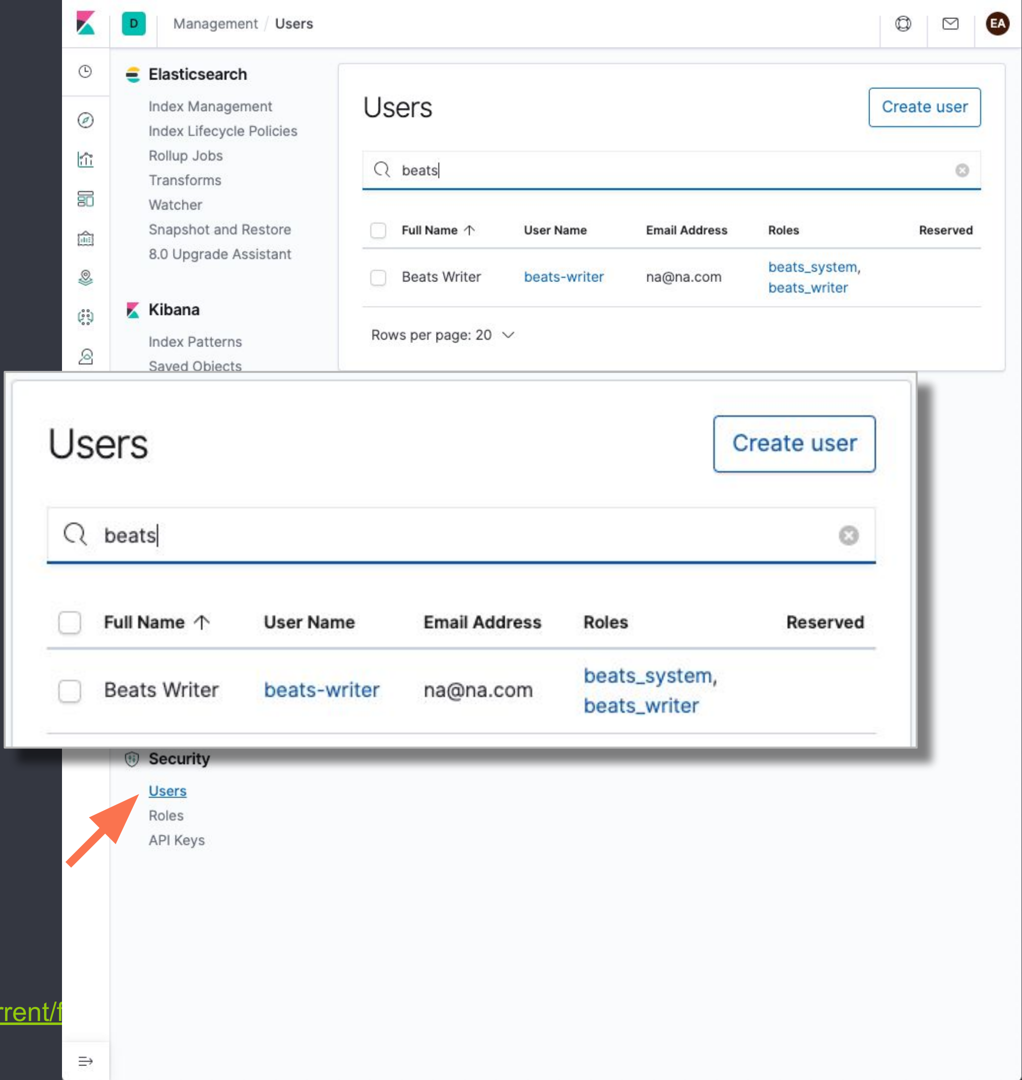
○ Grant read privileges to specific documents

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



Users

beats

Full Name ↑	User Name	Email Address	Roles	Reserved
Beats Writer	beats-writer	na@na.com	beats_system, beats_writer	

Users

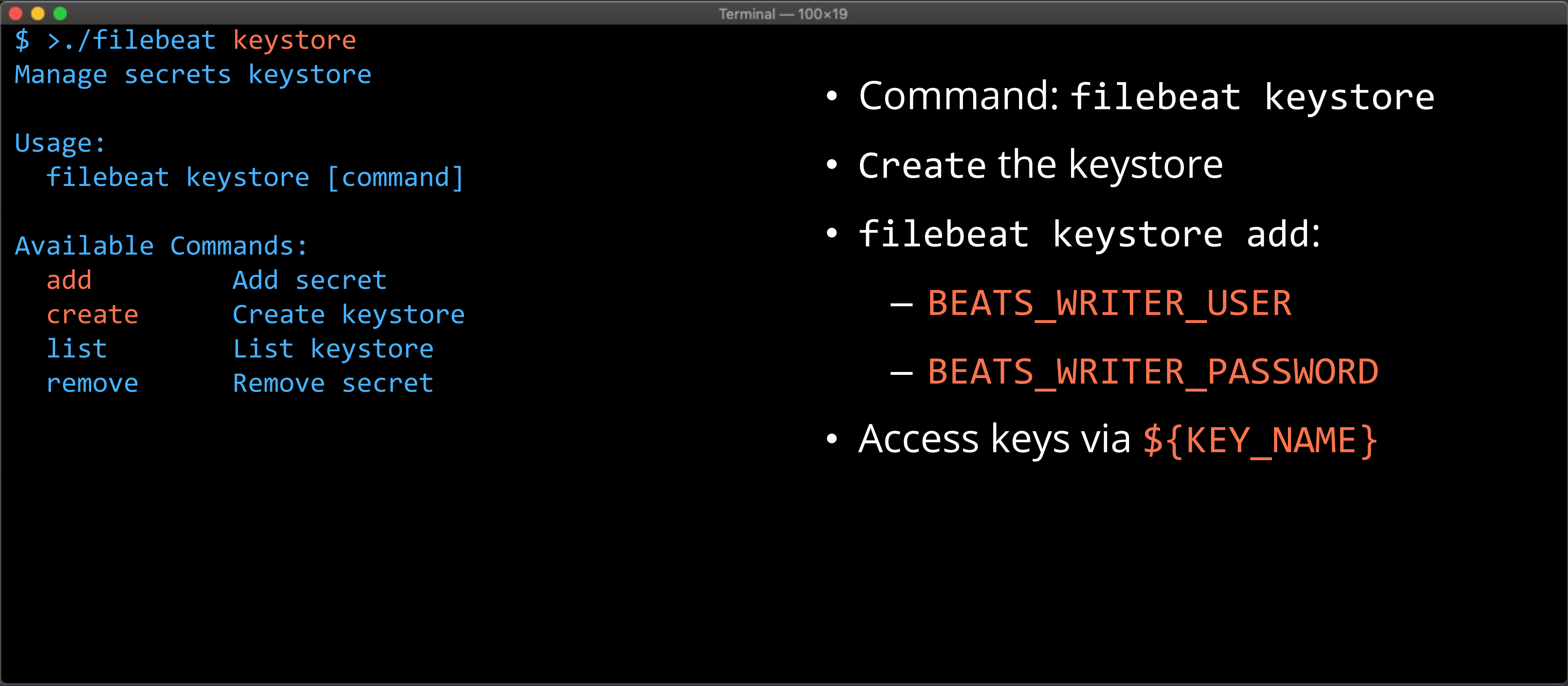
beats

Full Name ↑	User Name	Email Address	Roles	Reserved
Beats Writer	beats-writer	na@na.com	beats_system, beats_writer	

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

Set up the keystore

Hiding credentials for beats-writer

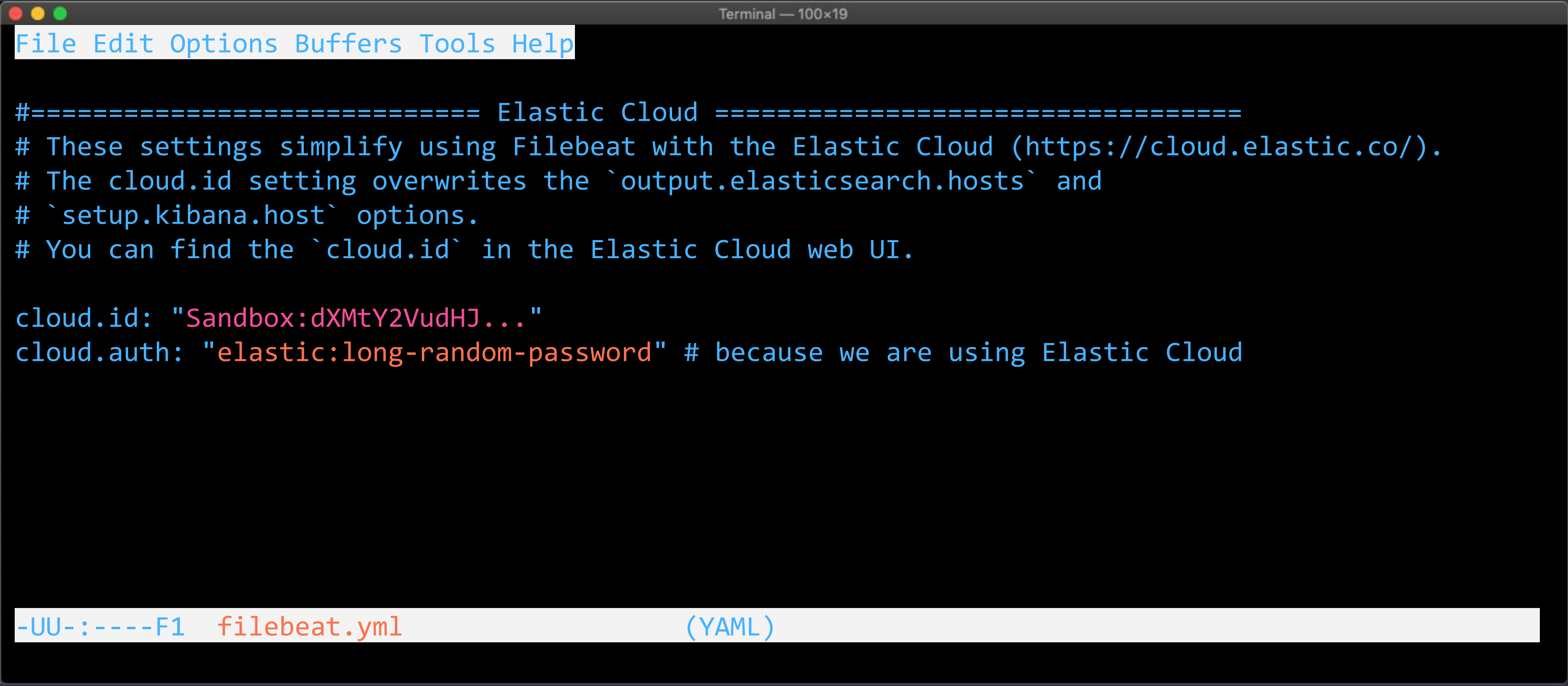


```
$ >./filebeat keystore
Manage secrets keystore

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



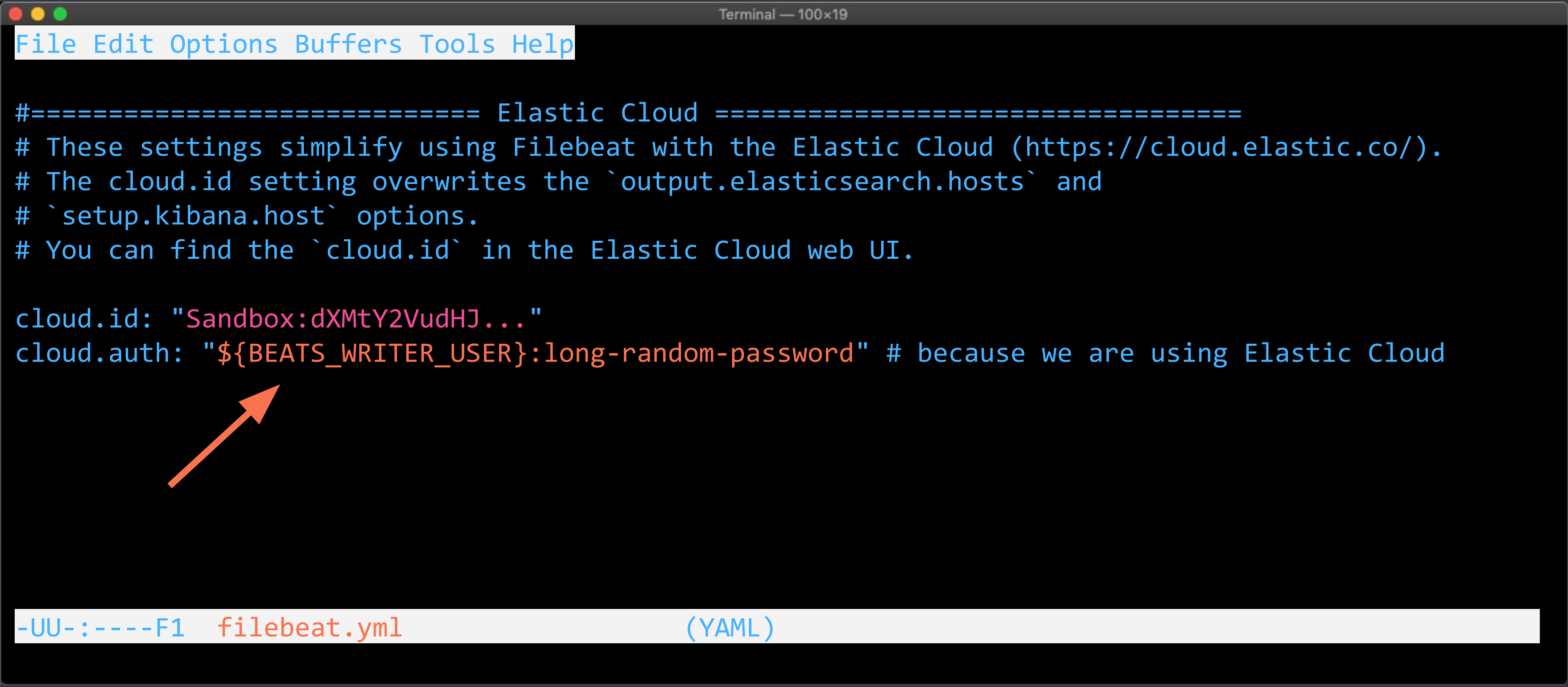
Terminal — 100×19
File Edit Options Buffers Tools Help

```
#============================== 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: "elastic:long-random-password" # because we are using Elastic Cloud
```

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

Parameterize the user

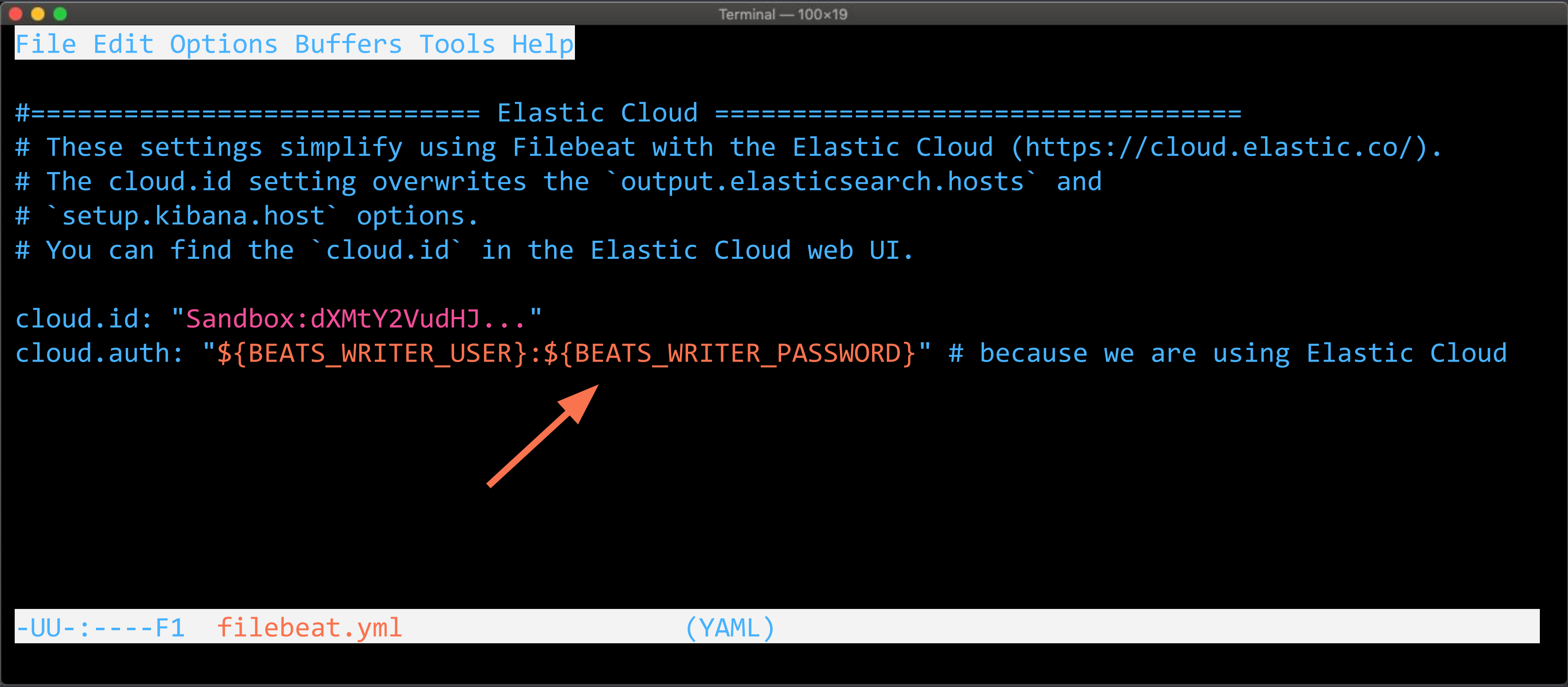
Had the user & password hardcoded



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

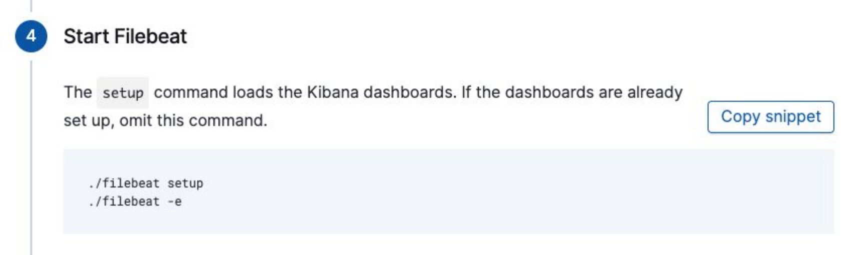
No more plain text!



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

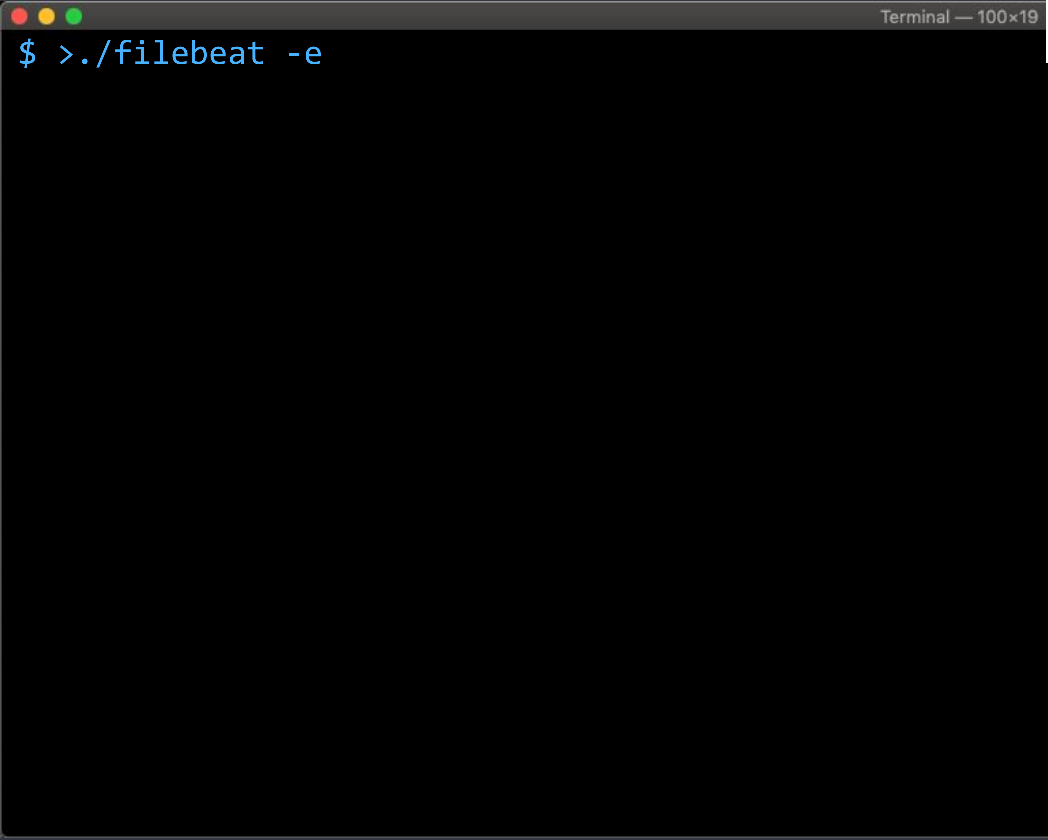
Automatically picks up the keystore



4 Start Filebeat

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

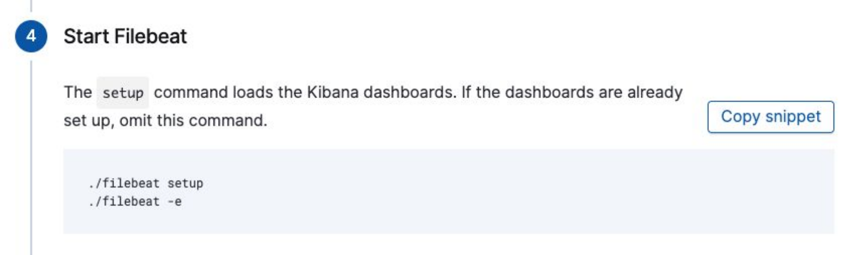
```
./filebeat setup
./filebeat -e
```



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

Finally, start it!

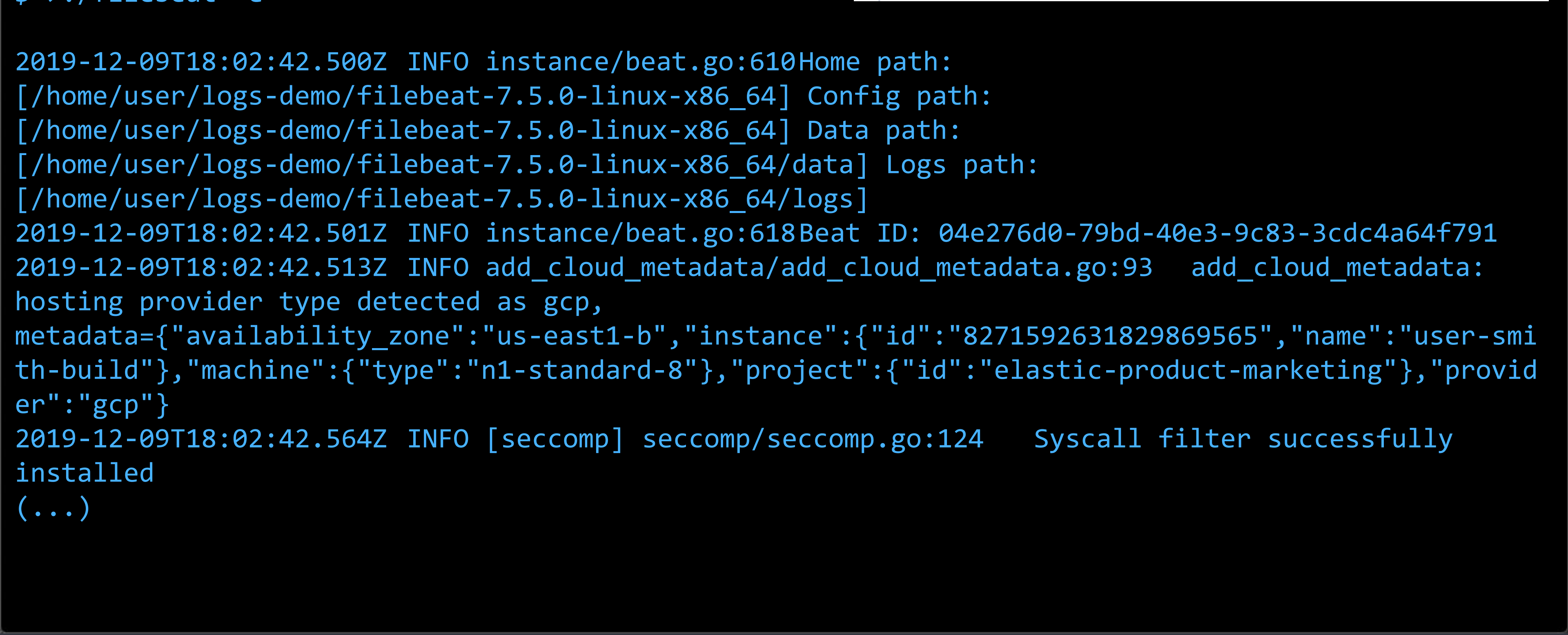
assumes that you've run setup



4 Start Filebeat

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

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



```
$ >./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!