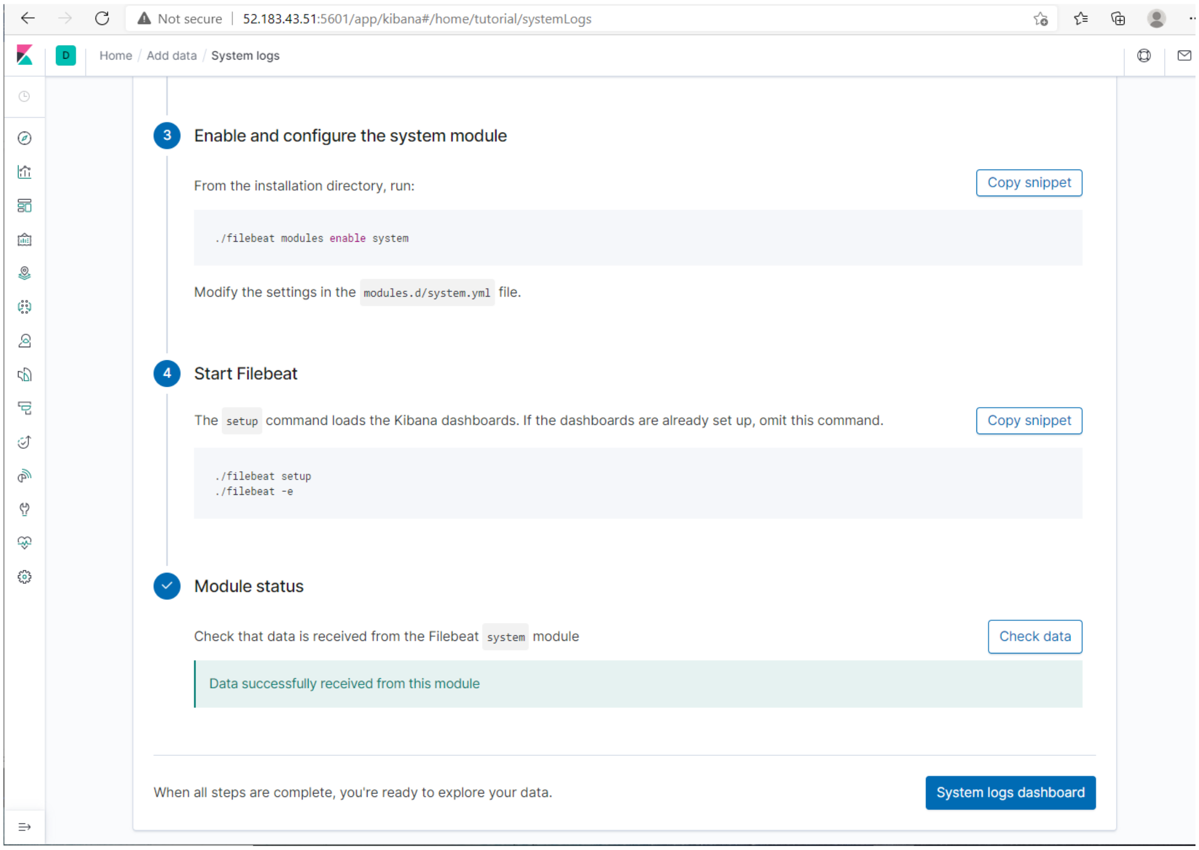
The screen shot below shows the successful run on the filebeat:


Not secure | 52.183.43.51:5601/app/kibana#/home/tutorial/systemLogs
D
Home / Add data / System logs

3 Enable and configure the system module

From the installation directory, run:

Copy snippet

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

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

4 Start Filebeat

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

Copy snippet

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

✓ Module status

Check that data is received from the Filebeat `system` module

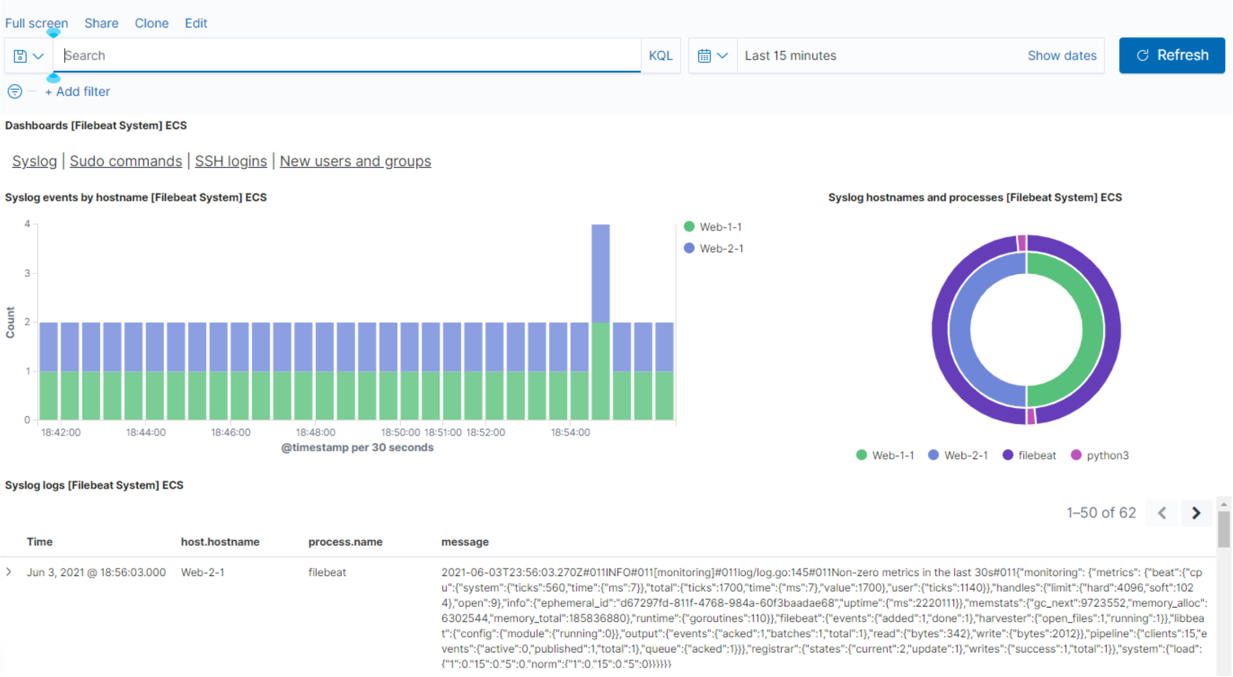
Check data

Data successfully received from this module

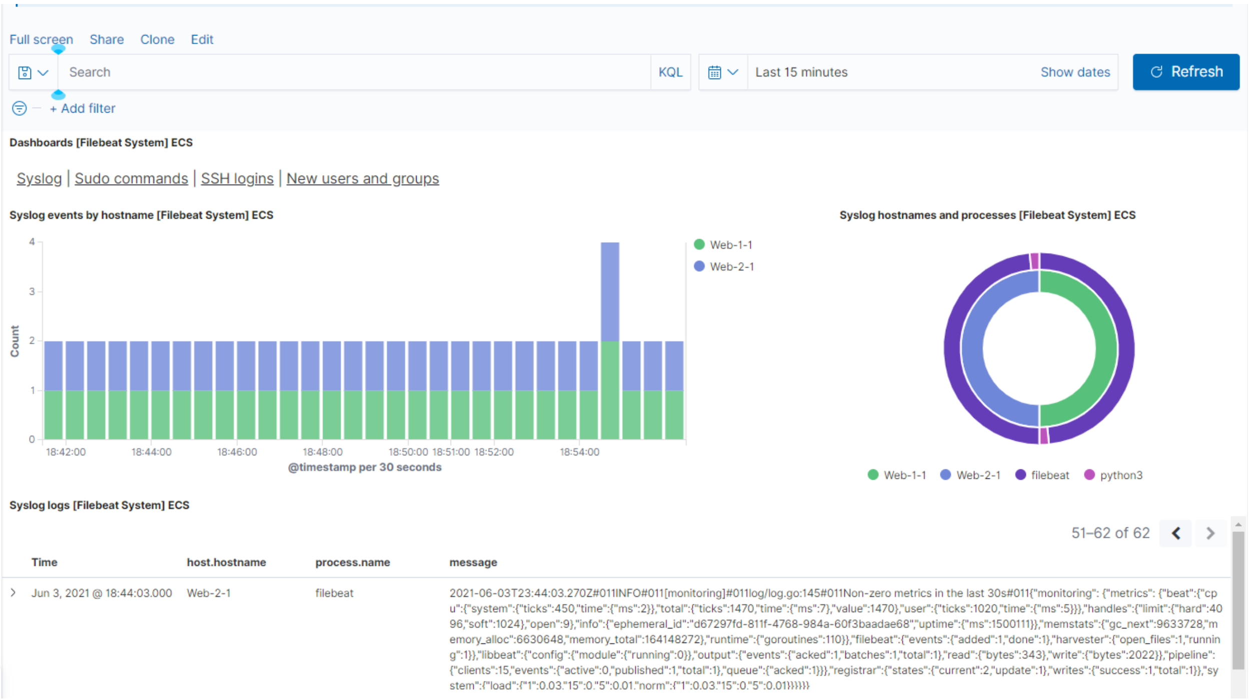
When all steps are complete, you're ready to explore your data.

System logs dashboard

The screen shots below show the system log dashboard from the successful running of the filebeat:


Full screen Share Clone Edit
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
Dashboards [Filebeat System] ECS
Syslog | Sudo commands | SSH logins | New users and groups
Syslog events by hostname [Filebeat System] ECS
4
3
2
1
0
Count
18:42:00
18:44:00
18:46:00
18:48:00
18:50:00 18:51:00 18:52:00
18:54:00
@timestamp per 30 seconds
● Web-1-1
● Web-2-1
Syslog hostnames and processes [Filebeat System] ECS
● Web-1-1 ● Web-2-1 ● filebeat ● python3
Syslog logs [Filebeat System] ECS
1–50 of 62

Time	host.hostname	process.name	message
Jun 3, 2021 @ 18:56:03.000	Web-2-1	filebeat	2021-06-03T23:56:03.270Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":560,"time":{"ms":7}},"total":{"ticks":1700,"time":{"ms":7},"value":1700},"user":{"ticks":1140}},"handles":{"limit":{"hard":4096,"soft":1024},"open":9},"info":{"ephemeral_id":"d67297fd-811f-4768-984a-60f3baadae68","uptime":{"ms":2220111}},"memstats":{"gc_next":9723552,"memory_alloc":6302544,"memory_total":185836880},"runtime":{"goroutines":110}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":1,"batches":1,"total":1},"read":{"bytes":342},"write":{"bytes":2012}},"pipeline":{"clients":15,"events":{"active":0,"published":1,"total":1},"queue":{"acked":1}}},"registrar":{"states":{"current":2,"update":1},"writes":{"success":1,"total":1}},"system":{"load":{"1":0."15":0."5":0."norm":{"1":0."15":0."5":0}}}}}}



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
Jun 3, 2021 @ 18:44:03.000	Web-2-1	filebeat	2021-06-03T23:44:03.270Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":450,"time":{"ms":2}},"total":{"ticks":1470,"time":{"ms":7},"value":1470},"user":{"ticks":1020,"time":{"ms":5}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":9},"info":{"ephemeral_id":"d67297fd-811f-4768-984a-60f3baadae68","uptime":{"ms":1500111}},"memstats":{"gc_next":9633728,"memory_alloc":6630648,"memory_total":164148272},"runtime":{"goroutines":110}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":1,"batches":1,"total":1},"read":{"bytes":343},"write":{"bytes":2022}},"pipeline":{"clients":15,"events":{"active":0,"published":1,"total":1},"queue":{"acked":1}}},"registrar":{"states":{"current":2,"update":1},"writes":{"success":1,"total":1}},"system":{"load":{"1":0.03,"15":0,"5":0.01,"norm":{"1":0.03,"15":0,"5":0.01}}}}}}