

Dashboard | X | Post Att... | X | Slack | X | class_2/We... | X | Intro to pla... | X | https://gist... | X | class_2/We... | X | Kibana | X | Web-1 - M... | X | How to Cop... | X | +

Not secure | 40.77.103.23:5601/app/kibana#/home/tutorial/systemLogs

Home / Add data / System logs

Modify the settings in the `/etc/filebeat/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](#)

```
sudo filebeat setup
sudo service filebeat start
```

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](#)

Type here to search

9:15 PM 2020-12-16

Dashboard | X | Post Att... | X | Slack | X | class_2/We... | X | Intro to pla... | X | https://... | X | class_2/... | X | Filebeat | X | Web-1 | X | How to... | X | Inbox | X | Nataraj... | X | +

Not secure | 40.77.103.23:5601/app/kibana#/dashboard/Filebeat-syslog-dashboard-ecs?_g=(refreshInterval:(pause:1t,value:0),time:(from:now-15m,to:...))

Dashboard | [Filebeat System] Syslog dashboard ECS

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

Syslog hostnames and processes [Filebeat System] ECS

Syslog logs [Filebeat System] ECS

Time	host.hostname	process.name	message
Dec 16, 2020 @ 21:20:30.000	Web-2	filebeat	2020-12-17T02:20:30.707Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring":{"metrics":{"beat":{"cpu":{"system":{"ticks":250,"time":{"ms":10}},"total":{"ticks":160,"time":{"ms":10},"value":1160},"user":{"ticks":910},"handles":{"limit":{"hard":4096,"soft":1024},"open":12},"info":{"ephemeral_id":"257a2907-1916-4205-800c-dd37339dc357","uptime":{"ms":360086}},"memstats":{"gc_next":11550056,"memory_alloc":9581920,"memory_total":103611648,"runtime":{"goroutines":117}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"files":{"9cb3366f-5100-4a10-bd12-544efcd168bc":{"last_event_published_time":"2020-12-17T02:20:06.819Z","last_event_timestamp":"2020-12-17T02:20:01.819Z","read_offset":1278,"size":1646},"open_files":2,"running":2}},"libbeat":{"config":{"module":{"running":

1-50 of 446

Type here to search

9:21 PM 2020-12-16

Dashboard / Home / Add data / Docker metrics

```
sudo metricbeat modules enable docker
```

Modify the settings in the `/etc/metricbeat/modules.d/docker.yml` file.

4 Start Metricbeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command. [Copy snippet](#)

```
sudo metricbeat setup
sudo service metricbeat start
```

Module status

Check that data is received from the Metricbeat `docker` module [Check data](#)

Data successfully received from this module

When all steps are complete, you're ready to explore your data. [Docker metrics dashboard](#)

Dashboard [Metricbeat Docker] Overview ECS

Full screen Share Clone Edit

Search KQL ~ 15 minutes ago → now [Refresh](#)

+ Add filter

Docker containers [Metricbeat Docker] ECS

Name	CPU usage (%)	DiskIO	Mem (%)	Mem RSS	Number of Containers
dvwa	0.1%	0	9.4%	98.2MB	2
	0.1%	0	9.4%	98.2MB	2

Export: [Raw](#) [Formatted](#)

Number of Containers [Metricbeat Docker] ECS

100
Running Paused Stopped

Docker containers per host [Metricbeat Docker] ECS

Donut chart showing distribution across hosts: Web-1, Web-2.

Docker images and names [Metricbeat Docker] ECS

Donut chart showing distribution across images: cybersecurity/dvwa, dvwa.

CPU usage [Metricbeat Docker] ECS

Line chart showing CPU usage for dvwa over time.

Memory usage [Metricbeat Docker] ECS

Line chart showing memory usage for dvwa over time.