

3 Enable and configure the system module

Copy snippet

```
sudo filebeat modules enable system
```

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

ENVM-rng - Microsoft Azure | [Filebeat System] Syslog dashb... | kernelanders/EKConfiguration... | Launch 1...

Apps UCSD Cyber Dashb... Azure Lab Services

Dashboard / [Filebeat System] Syslog dashboard ECS

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

1-50 of 260

Time	Web-1 Count	Web-2 Count
16:43:00	0	0
16:44:00	0	0
16:45:00	0	0
16:46:00	0	0
16:47:00	0	0
16:48:00	0	0
16:49:00	0	0
16:50:00	0	0
16:51:00	0	25
16:52:00	140	0
16:53:00	25	0
16:54:00	0	0
16:55:00	0	0
16:56:00	0	0
16:57:00	0	0

Category	Count
Web-1	140
Web-2	25
filebeat	25
systemd	0
python3	0

Time	host.hostname	process.name	message
Sep 14, 2020 @ 16:57:01.000	Web-2	filebeat	2020-09-14T23:57:01.787Z#011NFOR01logharvester.go:276#011File is inactive: /var/log/syslog.1. Closing because close_inactive of 5m0s reached.
Sep 14, 2020 @ 16:57:01.000	Web-1	filebeat	2020-09-14T23:57:01.742Z#011NFOR01logharvester.go:276#011File is inactive: /var/log/syslog.1. Closing because close_inactive of 5m0s reached.
Sep 14, 2020 @ 16:56:50.000	Web-2	filebeat	2020-09-14T23:56:50.814Z#011NFOR01logharvester.go:145#011Non-zero metrics in the last 30s#011{"monitoring":{"metrics":{"beat":{"cpu":{"system":{"ticks":140,"time":{"ms":8},"total":{"ticks":202,"time":{"ms":10},"value":70},"user":{"ticks":560,"time":{"ms":20},"handles":{"limit":4096,"soft":1024},"open":{"open":1},"info":{"ephemeral_id":"995e8bcc-0690-4e06-974e-356242616104"},"uptime":{"ms":300097},"memstats":{"gc_next":9715216,"memory_alloc":6250264,"memory_total":80726408},"runtime":{"goroutines":120},"filebeat":{"events":{"added":1,"done":0},"harvester":{"open_files":3,"running":3},"libbeat":{"config":{"module":{"running":0},"output":{"events":{"acked":1,"batches":1,"total":1},"tea":{"bytes":343},"write":{"bytes":2012},"pipeline":{"clients":15,"events":{"active":0,"published":1,"total":0},"queue":{"acked":0},"registrar":{"states":{"current":3,"update":0},"writes":{"success":1,"total":1},"system":{"load":{"1":0,"15":0,"5":0.02}}}}}}}}}
Sep 14, 2020 @ 16:56:50.000	Web-1	filebeat	2020-09-14T23:56:50.814Z#011NFOR01logharvester.go:145#011Non-zero metrics in the last 30s#011{"monitoring":{"metrics":{"beat":{"cpu":{"system":{"ticks":170,"time":{"ms":2},"total":{"ticks":650,"time":{"ms":12},"value":65},"user":{"ticks":480,"time":{"ms":10},"handles":{"limit":4096,"soft":1024},"open":{"open":1},"info":{"ephemeral_id":"995e8bcc-0690-4e06-974e-356242616104"},"uptime":{"ms":300097},"memstats":{"gc_next":9748848,"memory_alloc":535972,"memory_total":81521600},"runtime":{"goroutines":100},"filebeat":{"events":{"added":1,"done":0},"harvester":{"open_files":3,"running":3},"libbeat":{"config":{"module":{"running":0},"output":{"events":{"acked":1,"batches":1,"total":1},"tea":{"bytes":344},"write":{"bytes":2000},"pipeline":{"clients":15,"events":{"active":0,"published":1,"total":0},"queue":{"acked":0},"registrar":{"states":{"current":3,"update":0},"writes":{"success":1,"total":1},"system":{"load":{"1":0,"15":0,"5":0.02}}}}}}}}}
Sep 14, 2020 @ 16:56:20.000	Web-1	filebeat	2020-09-14T23:56:20.814Z#011NFOR01logharvester.go:145#011Non-zero metrics in the last 30s#011{"monitoring":{"metrics":{"beat":{"cpu":{"system":{"ticks":170,"time":{"ms":10},"total":{"ticks":650,"time":{"ms":17},"value":65},"user":{"ticks":480,"time":{"ms":10},"handles":{"limit":4096,"soft":1024},"open":{"open":1},"info":{"ephemeral_id":"995e8bcc-0690-4e06-974e-356242616104"},"uptime":{"ms":300097},"memstats":{"gc_next":9748848,"memory_alloc":535972,"memory_total":81521600},"runtime":{"goroutines":100},"filebeat":{"events":{"added":1,"done":0},"harvester":{"open_files":3,"running":3},"libbeat":{"config":{"module":{"running":0},"output":{"events":{"acked":1,"batches":1,"total":1},"tea":{"bytes":344},"write":{"bytes":2000},"pipeline":{"clients":15,"events":{"active":0,"published":1,"total":0},"queue":{"acked":0},"registrar":{"states":{"current":3,"update":0},"writes":{"success":1,"total":1},"system":{"load":{"1":0,"15":0,"5":0.02}}}}}}}}}