

```

azadmin@Elk: ~
root@10567efb547e:/etc/ansible# ssh azadmin@10.2.0.6
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-1033-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Jun 17 00:55:24 UTC 2021

System load:  0.71               Processes:    144
Usage of /:   15.3% of 28.9GB    Users logged in: 0
Memory usage: 17%              IPv4 address for docker0: 172.17.0.1
Swap usage:   0%                IPv4 address for eth0: 10.2.0.6

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Thu Jun 17 00:52:03 2021 from 10.0.0.4
azadmin@Elk:~$ docker sh
docker: 'sh' is not a docker command.
See 'docker --help'
azadmin@Elk:~$ docker ps
Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json: dial unix /var/run/docker.sock: connect: permission denied
azadmin@Elk:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED    STATUS    PORTS                               NAMES
3350c7b3ea2d   sebp/elk:761  "/usr/local/bin/star..."  9 minutes ago    Up 28 seconds    0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp    elk
azadmin@Elk:~$

```

Virtual machines - Microsoft Azure | What is My IP Address - See You | What is a vnc scan on the kill chain | The 3 Types Of Security Controls | Cannot access Kibana on port 51 | Kibana

104.44.135.128:5601/app/kibana#/home/tutorial/systemLogs

Apps | Dashboard | Bootstr... | Projects - Dashboar... | DU Email | GitHub | My Drive - Google... | Denver University... | Cyber security succ... | Summary - Cyberse... | Create Account | SL | LinkedIn | Google Docs | e-certification-road... | Exam Objectives | Reading list

Home | Add data | System logs

4 Start Filebeat

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

```

sudo filebeat setup
sudo service filebeat start

```

Module status

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

Data successfully received from this module

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

System logs dashboard

README.zip | Network Security (...rdp) | Network Security (...rdp) | information-11-00...pdf | Show all

Elk-Demo - Microsoft Azure

Dashboard | Bootcamp Spot

1-Lessons/Week_13/Activities/5

whats a vnc scan on the kill cha

Untitled Diagram.drawio - diag

Kibana

← → Not secure | 104.44.135.128:5601/app/kibana#/home/tutorial/dockerMetrics

Apps Dashboard | Bootca... Projects - Dashboar... DU Email GitHub My Drive - Google... Denver University... Cyber security succ... Summary - Cyberse... Create Account | Sl... LinkedIn Google Docs it-certification-road... Exam Objectives Reading list

Home / Add data / Docker metrics

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

3

Enable and configure the docker module

Copy snippet

sudo metricbeat modules enable docker

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

4

Start Metricbeat

Copy snippet

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

sudo metricbeat setup
sudo service metricbeat start

✓

Module status

Check data

Check that data is received from the Metricbeat docker module

Data successfully received from this module

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

Docker metrics dashboard