

13. ELK Stack Project

```
root@61d65b3d5f2a:/etc/ansible# ansible-playbook install.elk.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly
calculated text widths that can cause Display to print incorrect line lengths

PLAY [Configure Elk VM with Docker] *****

TASK [Gathering Facts] *****
ok: [10.3.0.4]

TASK [Install docker.io] *****
changed: [10.3.0.4]

TASK [Install python3-pip] *****
changed: [10.3.0.4]

TASK [Install Docker module] *****
changed: [10.3.0.4]

TASK [Increase virtual memory] *****
changed: [10.3.0.4]

TASK [Use more memory] *****
changed: [10.3.0.4]

TASK [download and launch a docker elk container] *****
[DEPRECATION WARNING]: The container_default_behavior option will change its default value from
"compatibility" to "no_defaults" in community.docker 2.0.0. To remove this warning, please specify an
explicit value for it now. This feature will be removed from community.docker in version 2.0.0.
Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
changed: [10.3.0.4]

TASK [Enable service docker on boot] *****
ok: [10.3.0.4]

PLAY RECAP *****
10.3.0.4 : ok=8 changed=6 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@61d65b3d5f2a:/etc/ansible#
```

```
ansible@ELK-VM:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS
3eb3f406ab8f   sebp/elk:761  "/usr/local/bin/star...  9 minutes ago  Up 9 minutes  0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp
ansible@ELK-VM:~$
```

```
Last login: Tue Jun 15 00:35:18 2021 from 10.1.0.4
ansible@ELK-VM:~$ 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
ansible@ELK-VM:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS        NAMES
3eb3f406ab8f   sebp/elk:761  "/usr/local/bin/star...  9 minutes ago  Up 9 minutes  0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp  elk
ansible@ELK-VM:~$
```

13. ELK Stack Project

Kibana

Not secure | 104.210.56.238:5601/app/kibana#/home/tutorial/systemLogs

Apps | HLRI | Shahi | Manage Profile | rlp... | Cyber | Reading list

Add data / System logs

From the installation directory, run:

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

Copy snippet

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.

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

Copy snippet

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

13. ELK Stack Project

The screenshot shows the Kibana web interface in a browser. The address bar indicates the URL is `104.210.56.238:5601/app/kibana#/home/tutorial_directory/sampleData`. The page title is "Add Data to Kibana". Below the title, there are tabs for "All", "Logs", "Metrics", "SIEM", and "Sample data", with "Sample data" being the active tab. The main content area displays three sample data sources, each with a preview of its dashboard and an "Add data" button.

- Sample eCommerce orders:** The preview shows a dashboard with four gauges (Orders / day: 139, Average order price: \$75.23, Average order size: 2.183, Average order weight: \$77,638.33) and a line chart for "Average order price over time".
- Sample flight data:** The preview shows a dashboard with a gauge for "Total flights" (68), a bar chart for "Flights by destination", and a line chart for "Flights by origin".
- Sample web logs:** The preview shows a dashboard with a gauge for "Total requests" (801), a bar chart for "Requests by status", and a line chart for "Requests by method".

13. ELK Stack Project

Kibana

Not secure | 104.210.56.238:5601/app/kibana#/home/tutorial/systemLogs

Apps | HLRI | Shahi | Manage Profile | rlp... | Cyber | Reading list

Add data / System logs

From the installation directory, run:

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

Copy snippet

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.

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

Copy snippet

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

13. ELK Stack Project

Bonus

```
root@61d65b3d5f2a: /etc/ansible/roles
***10.1.0.5 : ok=3 changed=2 unreachable=0 failed=1 skipped=0 rescued=0 ignored=0
10.1.0.6 : ok=3 changed=2 unreachable=0 failed=1 skipped=0 rescued=0 ignored=0
10.1.0.9 : ok=3 changed=2 unreachable=0 failed=1 skipped=0 rescued=0 ignored=0

root@61d65b3d5f2a:/etc/ansible/roles# nano metricbeat-playbook.yml
root@61d65b3d5f2a:/etc/ansible/roles# ansible-playbook metricbeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated te
t widths that can cause Display
to print incorrect line lengths

PLAY [Install metric beat] *****
TASK [Gathering Facts] *****
ok: [10.1.0.6]
ok: [10.1.0.9]

TASK [Download metricbeat] *****
changed: [10.1.0.9]
changed: [10.1.0.5]

TASK [install metricbeat] *****
changed: [10.1.0.5]
changed: [10.1.0.9]

TASK [drop in metricbeat config] *****
changed: [10.1.0.5]
changed: [10.1.0.9]

TASK [enable and configure docker module for metric beat] *****
changed: [10.1.0.6]
changed: [10.1.0.9]

TASK [setup metric beat] *****
changed: [10.1.0.6]
changed: [10.1.0.5]

TASK [start metric beat] *****
changed: [10.1.0.5]
changed: [10.1.0.9]

TASK [enable service metricbeat on boot] *****
changed: [10.1.0.5]
changed: [10.1.0.9]

PLAY RECAP *****
10.1.0.5 : ok=8 changed=7 unreachable=0 failed=0 ski
ped=0 rescued=0 ignored=0
10.1.0.6 : ok=8 changed=7 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0
10.1.0.9 : ok=8 changed=7 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@61d65b3d5f2a:/etc/ansible/roles#
```

13. ELK Stack Project

