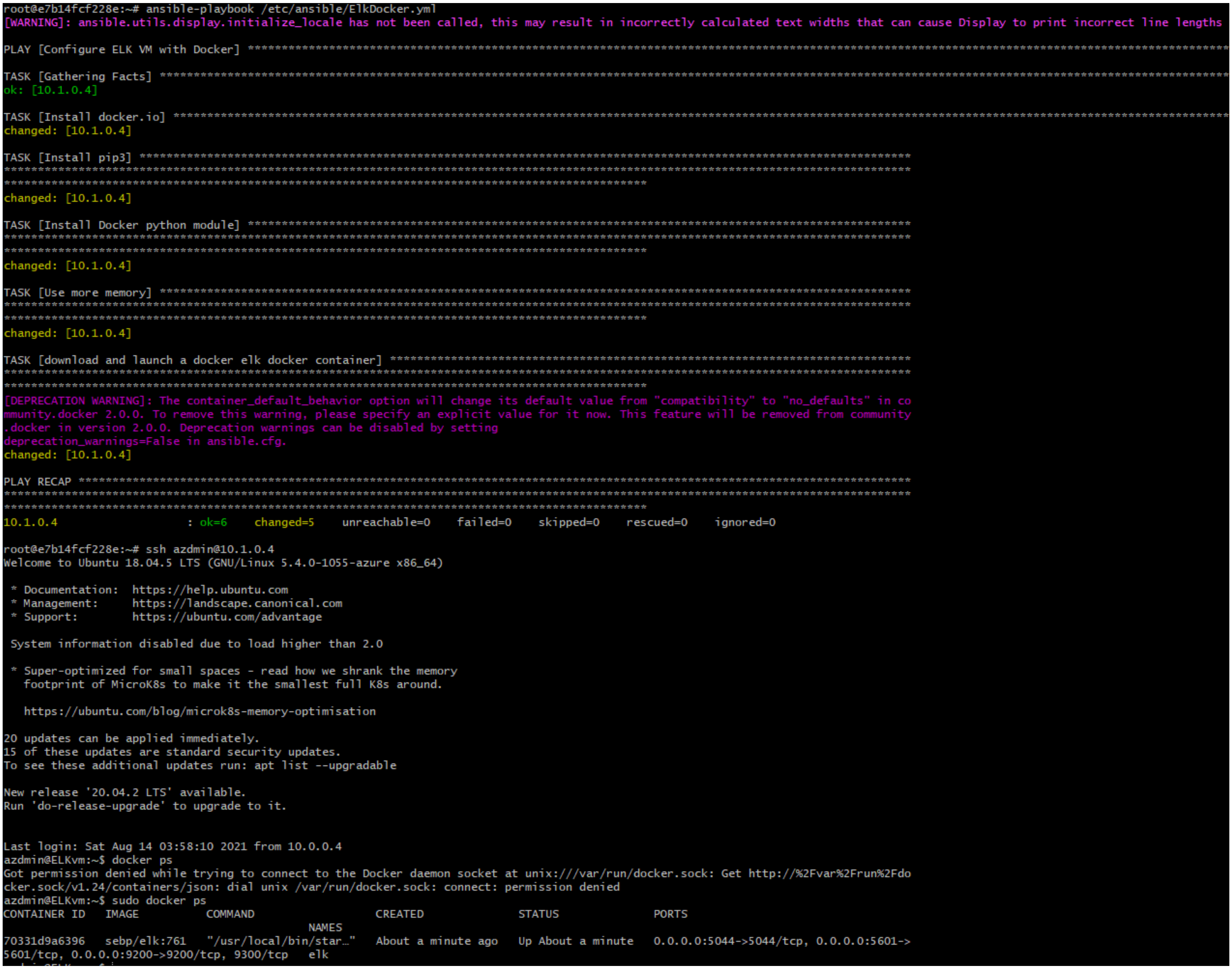
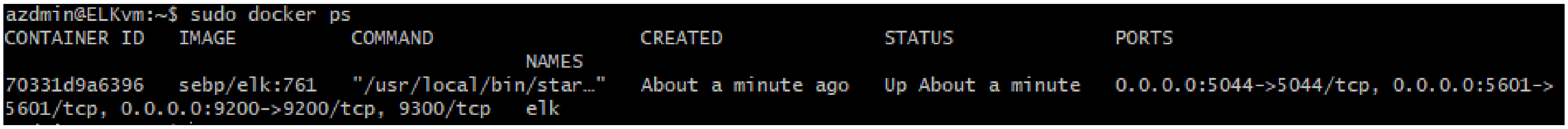
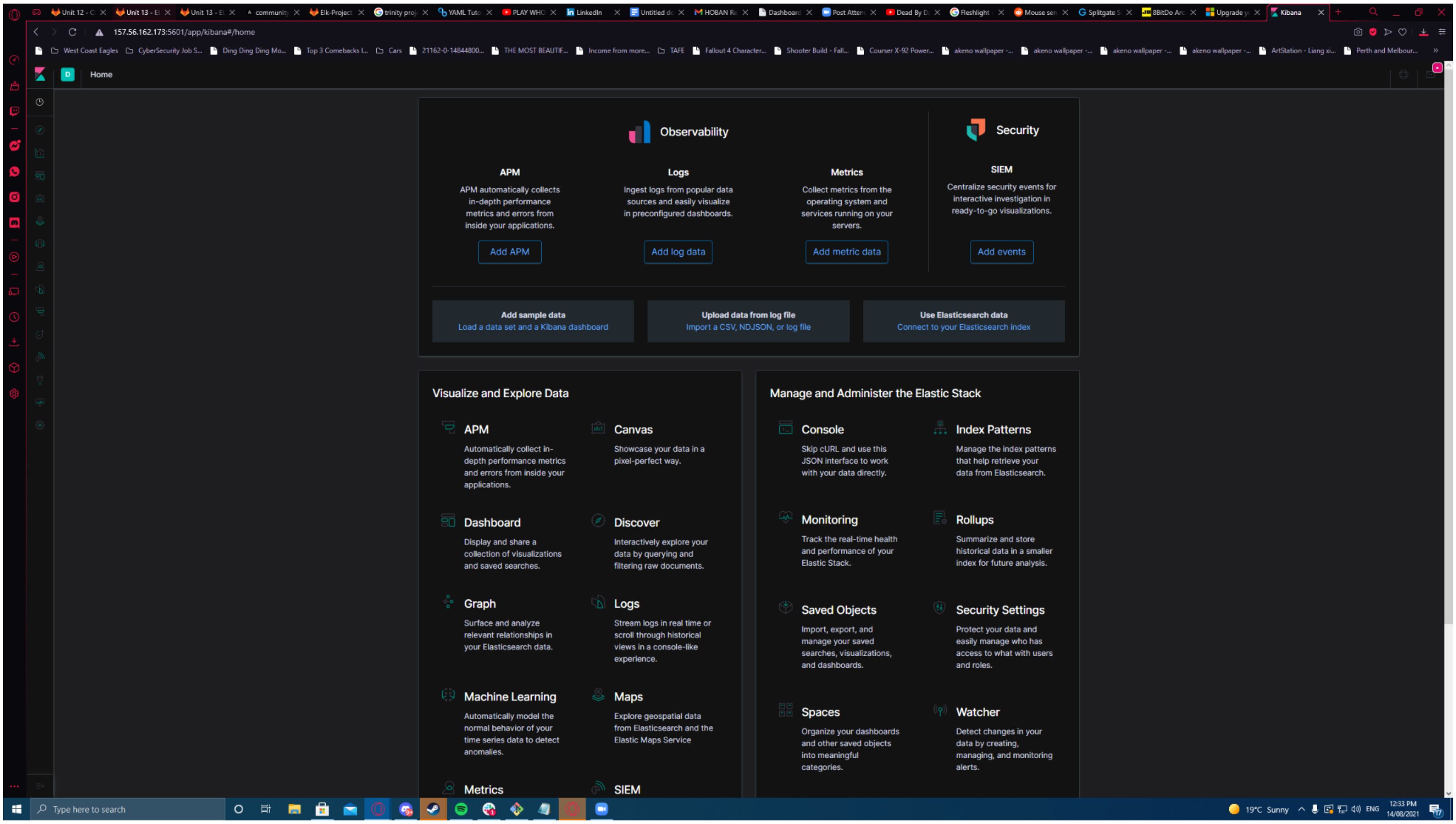
Project 1 - Day 1



```
root@e7b14fcf228e:~# ansible-playbook /etc/ansible/ElkDocker.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: [10.1.0.4]

TASK [Install docker.io] ****************************************************************************************************************************************************
changed: [10.1.0.4]

TASK [Install pip3] ******************************************************************************************************************
**************************************************************************************************************************************
***********************************************************************************************
changed: [10.1.0.4]

TASK [Install Docker python module] **************************************************************************************************
**************************************************************************************************************************************
***********************************************************************************************
changed: [10.1.0.4]

TASK [Use more memory] ***************************************************************************************************************
**************************************************************************************************************************************
***********************************************************************************************
changed: [10.1.0.4]

TASK [download and launch a docker elk docker container] *****************************************************************************
**************************************************************************************************************************************
***********************************************************************************************
[DEPRECATION WARNING]: The container_default_behavior option will change its default value from "compatibility" to "no_defaults" in co
mmunity.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: [10.1.0.4]

PLAY RECAP ***************************************************************************************************************************
**************************************************************************************************************************************
***********************************************************************************************
10.1.0.4                   : ok=6    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@e7b14fcf228e:~# ssh azdmin@10.1.0.4
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1055-azure x86_64)

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

 System information disabled due to load higher than 2.0

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

20 updates can be applied immediately.
15 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Aug 14 03:58:10 2021 from 10.0.0.4
azdmin@ELKvm:~$ docker ps
Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get http://%2Fvar%2Frun%2Fdo
cker.sock/v1.24/containers/json: dial unix /var/run/docker.sock: connect: permission denied
azdmin@ELKvm:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED              STATUS              PORTS
                                       NAMES
70331d9a6396   sebp/elk:761   "/usr/local/bin/star…"   About a minute ago   Up About a minute   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->
5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
```



```
azdmin@ELKvm:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED              STATUS              PORTS
                                       NAMES
70331d9a6396   sebp/elk:761   "/usr/local/bin/star…"   About a minute ago   Up About a minute   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->
5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
```



Observability

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

Security

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add events

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

APM
Automatically collect in-depth performance metrics and errors from inside your applications.

Canvas
Showcase your data in a pixel-perfect way.

Dashboard
Display and share a collection of visualizations and saved searches.

Discover
Interactively explore your data by querying and filtering raw documents.

Graph
Surface and analyze relevant relationships in your Elasticsearch data.

Logs
Stream logs in real time or scroll through historical views in a console-like experience.

Machine Learning
Automatically model the normal behavior of your time series data to detect anomalies.

Maps
Explore geospatial data from Elasticsearch and the Elastic Maps Service

Metrics

SIEM

Manage and Administer the Elastic Stack

Console
Skip cURL and use this JSON interface to work with your data directly.

Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.

Monitoring
Track the real-time health and performance of your Elastic Stack.

Rollups
Summarize and store historical data in a smaller index for future analysis.

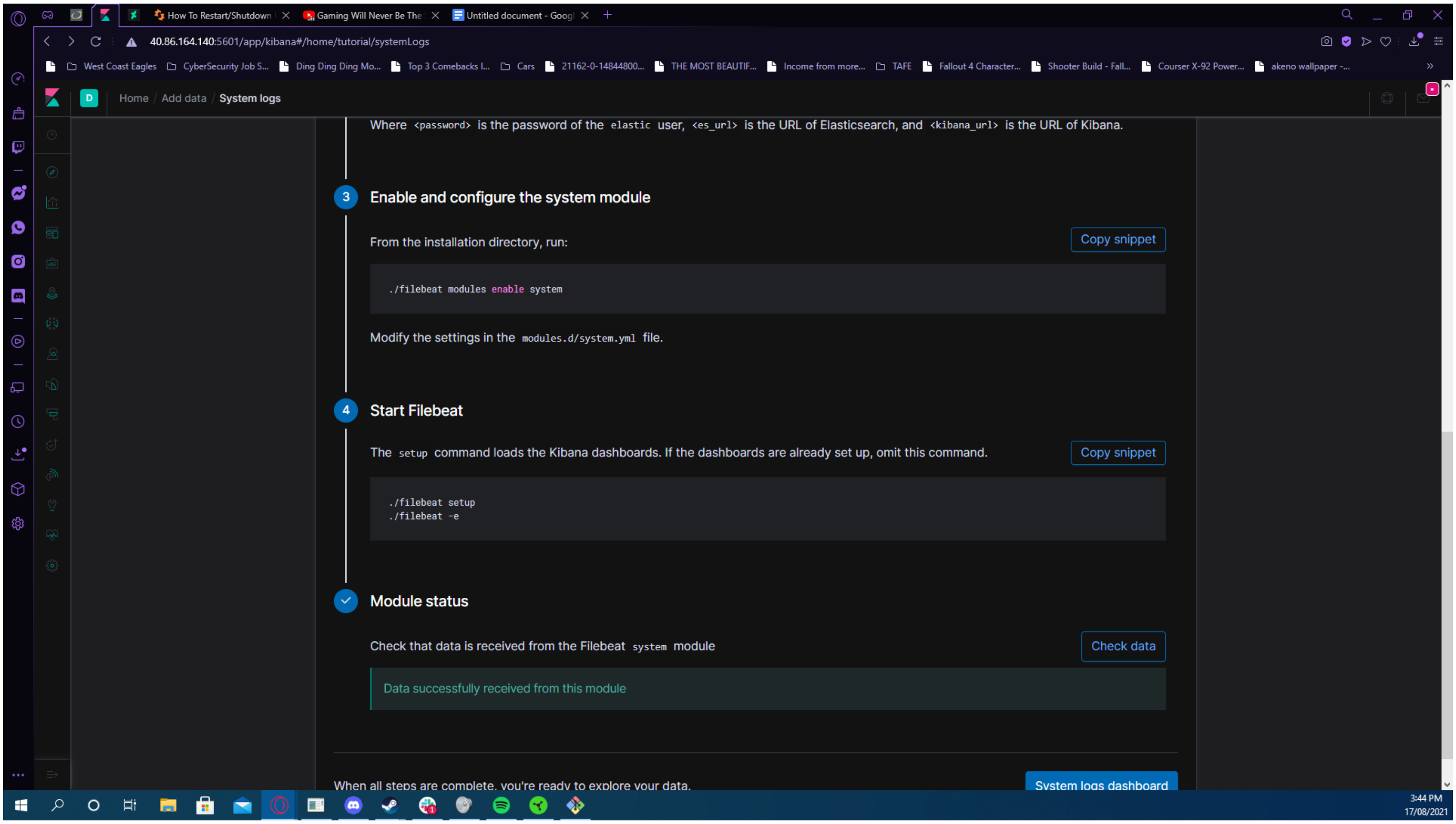
Saved Objects
Import, export, and manage your saved searches, visualizations, and dashboards.

Security Settings
Protect your data and easily manage who has access to what with users and roles.

Spaces
Organize your dashboards and other saved objects into meaningful categories.

Watcher
Detect changes in your data by creating, managing, and monitoring alerts.

Project 1 - Day 2



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 system module

From the installation directory, run:

```
./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.

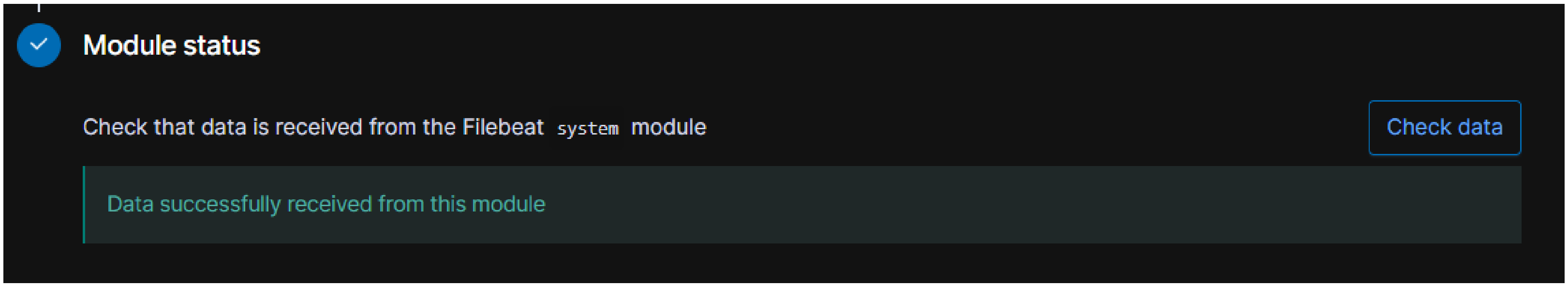
```
./filebeat setup
./filebeat -e
```

✓ Module status

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

Data successfully received from this module

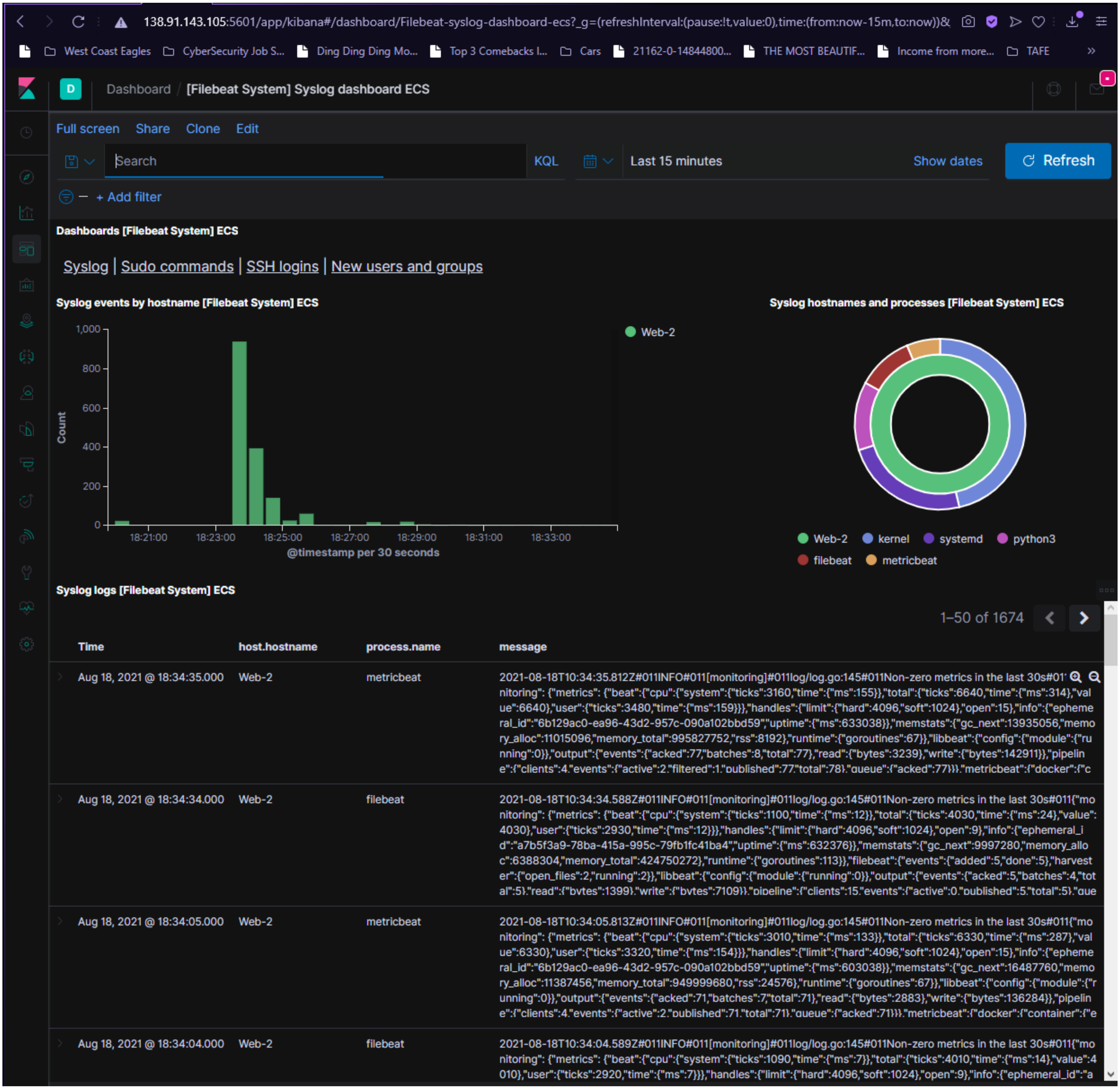
When all steps are complete, you're ready to explore your data.



✓ Module status

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

Data successfully received from this module



Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

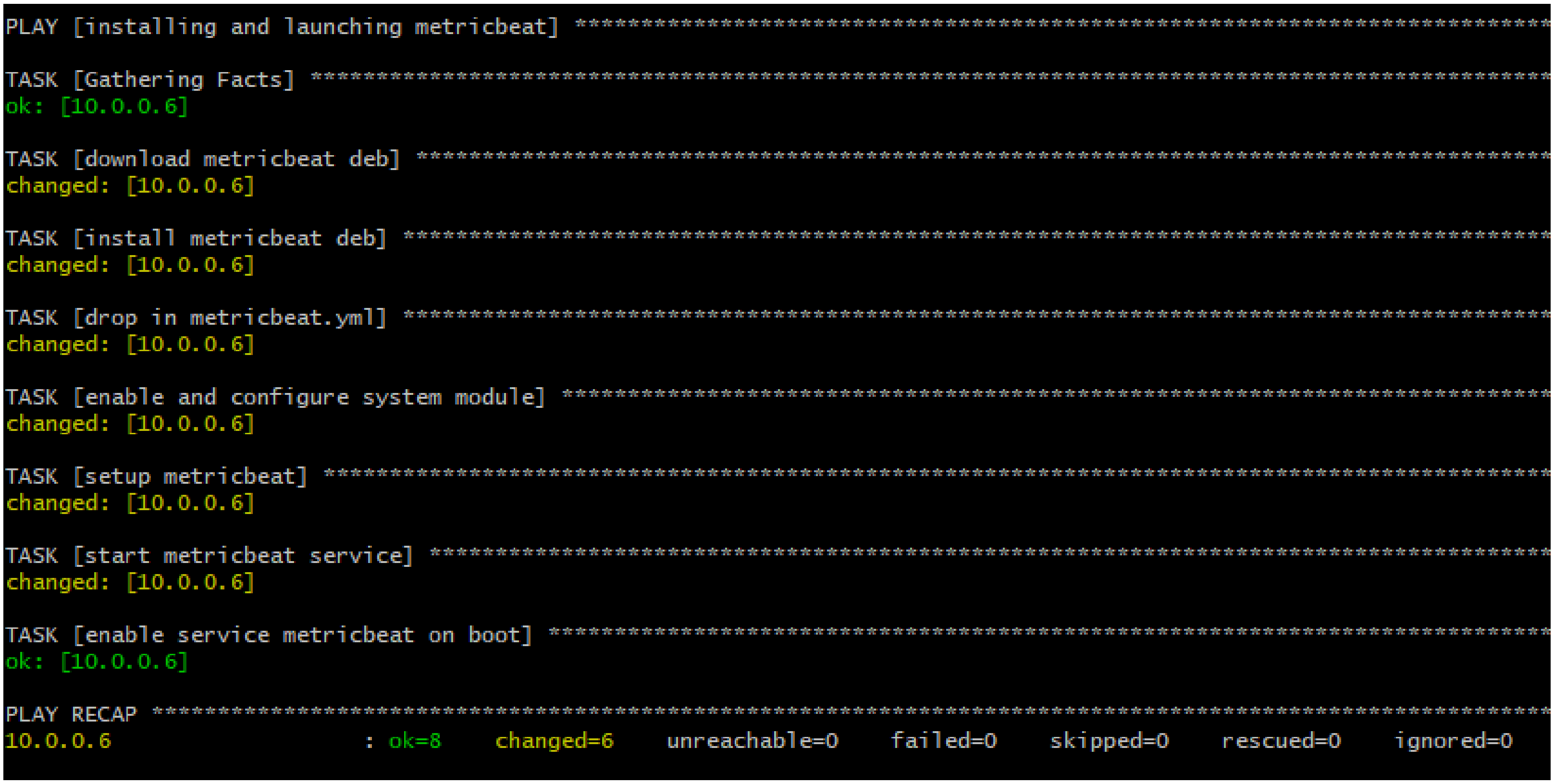
Syslog events by hostname [Filebeat System] ECS

Syslog hostnames and processes [Filebeat System] ECS

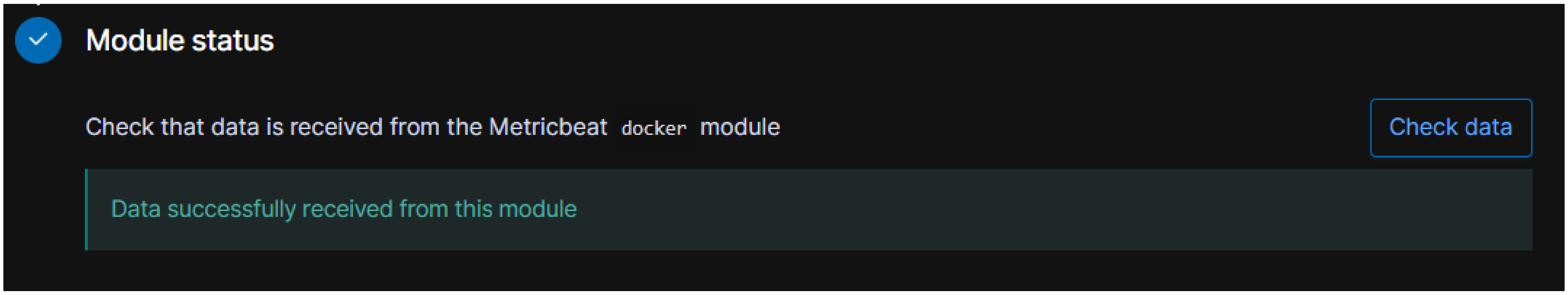
Syslog logs [Filebeat System] ECS

1–50 of 1674

Time	host.hostname	process.name	message
Aug 18, 2021 @ 18:34:35.000	Web-2	metricbeat	2021-08-18T10:34:35.812Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#01 nitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":3160,"time":{"ms":155}},"total":{"ticks":6640,"time":{"ms":314},"value":6640},"user":{"ticks":3480,"time":{"ms":159}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":15},"info":{"ephemeral_id":"6b129ac0-ea96-43d2-957c-090a102bbd59","uptime":{"ms":633038}},"memstats":{"gc_next":13935056,"memory_alloc":11015096,"memory_total":995827752,"rss":8192},"runtime":{"goroutines":67}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":77,"batches":8,"total":77},"read":{"bytes":3239},"write":{"bytes":142911}},"pipeline":{"clients":4,"events":{"active":2,"filtered":1,"published":77,"total":78},"queue":{"acked":77}}},"metricbeat":{"docker":{"c
Aug 18, 2021 @ 18:34:34.000	Web-2	filebeat	2021-08-18T10:34:34.588Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":1100,"time":{"ms":12}},"total":{"ticks":4030,"time":{"ms":24},"value":4030},"user":{"ticks":2930,"time":{"ms":12}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":9},"info":{"ephemeral_id":"a7b5f3a9-78ba-415a-995c-79fb1fc41ba4","uptime":{"ms":632376}},"memstats":{"gc_next":9997280,"memory_alloc":6388304,"memory_total":424750272},"runtime":{"goroutines":113}},"filebeat":{"events":{"added":5,"done":5},"harvester":{"open_files":2,"running":2}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":5,"batches":4,"total":5},"read":{"bytes":1399},"write":{"bytes":7109}},"pipeline":{"clients":15,"events":{"active":0,"published":5,"total":5},"que
Aug 18, 2021 @ 18:34:05.000	Web-2	metricbeat	2021-08-18T10:34:05.813Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":3010,"time":{"ms":133}},"total":{"ticks":6330,"time":{"ms":287},"value":6330},"user":{"ticks":3320,"time":{"ms":154}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":15},"info":{"ephemeral_id":"6b129ac0-ea96-43d2-957c-090a102bbd59","uptime":{"ms":603038}},"memstats":{"gc_next":16487760,"memory_alloc":11387456,"memory_total":949999680,"rss":24576},"runtime":{"goroutines":67}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":71,"batches":7,"total":71},"read":{"bytes":2883},"write":{"bytes":136284}},"pipeline":{"clients":4,"events":{"active":2,"published":71,"total":71},"queue":{"acked":71}}},"metricbeat":{"docker":{"container":{"e
Aug 18, 2021 @ 18:34:04.000	Web-2	filebeat	2021-08-18T10:34:04.589Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":1090,"time":{"ms":7}},"total":{"ticks":4010,"time":{"ms":14},"value":4010},"user":{"ticks":2920,"time":{"ms":7}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":9},"info":{"ephemeral_id":"a



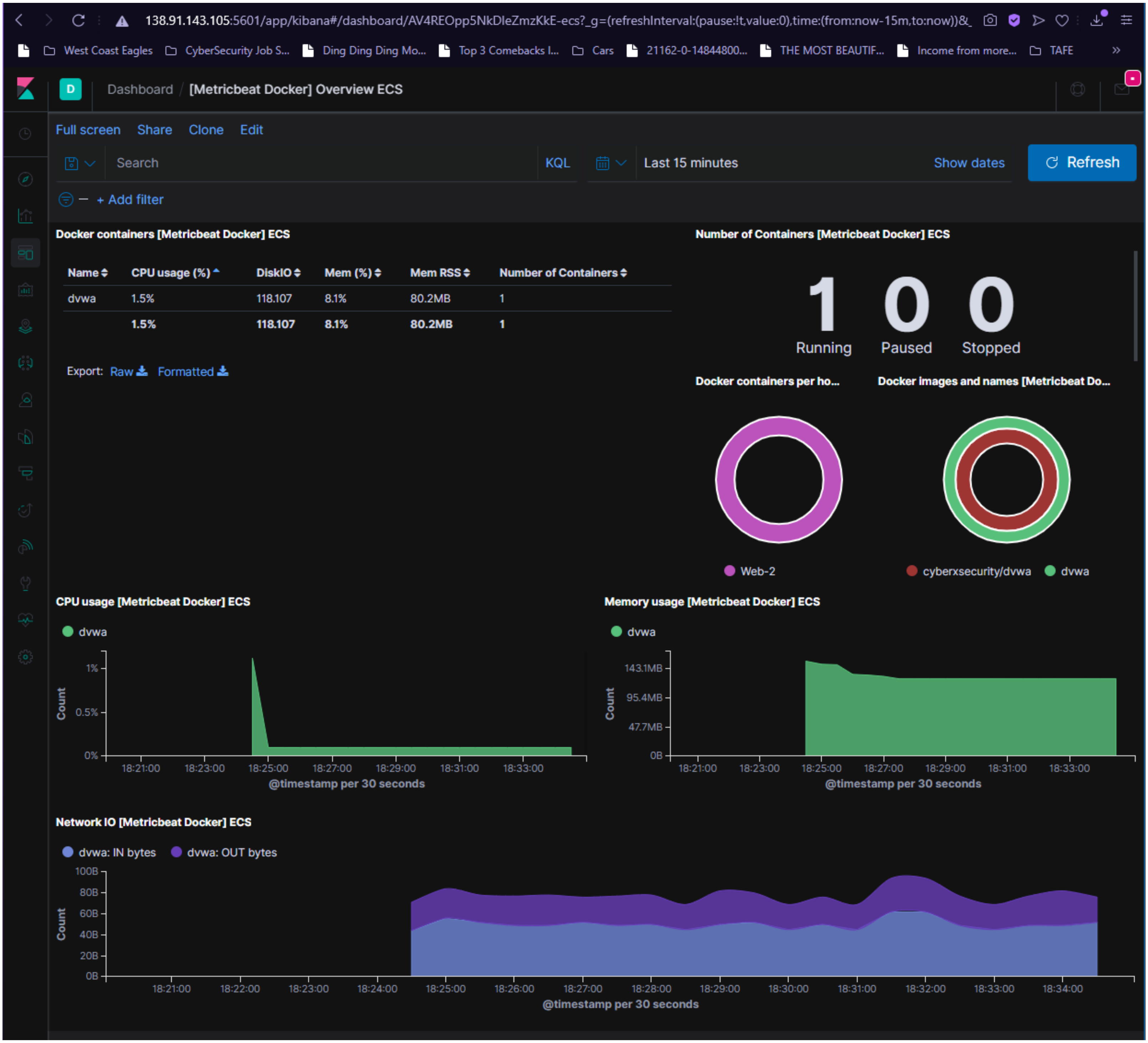
```
PLAY [installing and launching metricbeat] ***********************************************************************

TASK [Gathering Facts] *******************************************************************************************
ok: [10.0.0.6]

TASK [download metricbeat deb] ***********************************************************************************
changed: [10.0.0.6]

TASK [install metricbeat deb] ************************************************************************************
changed: [10.0.0.6]

TASK [drop in metricbeat.yml] ************************************************************************************
changed: [10.0.0.6]

TASK [enable and configure system module] ************************************************************************
changed: [10.0.0.6]

TASK [setup metricbeat] ******************************************************************************************
changed: [10.0.0.6]

TASK [start metricbeat service] **********************************************************************************
changed: [10.0.0.6]

TASK [enable service metricbeat on boot] *************************************************************************
ok: [10.0.0.6]

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



Module status

Check that data is received from the Metricbeat `docker` module

Data successfully received from this module



Docker containers [Metricbeat Docker] ECS

Name	CPU usage (%)	DiskIO	Mem (%)	Mem RSS	Number of Containers
dvwa	1.5%	118.107	8.1%	80.2MB	1
	1.5%	**118.107**	**8.1%**	**80.2MB**	**1**

Number of Containers [Metricbeat Docker] ECS

Docker containers per ho...

Docker images and names [Metricbeat Do...

CPU usage [Metricbeat Docker] ECS

Memory usage [Metricbeat Docker] ECS

Network IO [Metricbeat Docker] ECS