# Filebeat/Metricbeat- Create

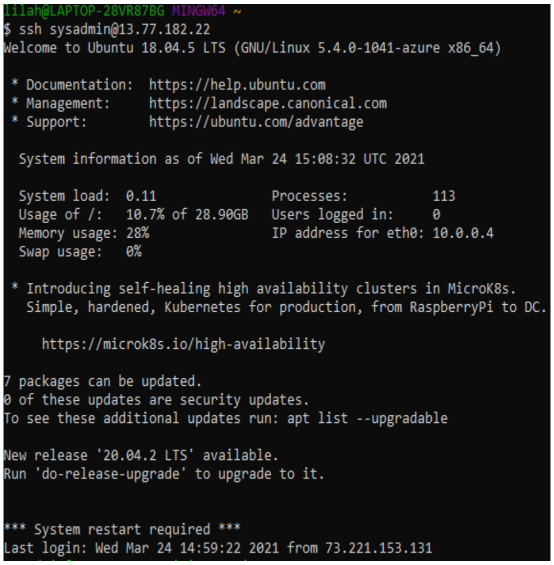
```
curl
https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat
```

Create another Ansible playbook that accomplishes the Linux Filebeat installation instructions.

The playbook should:
Download the .deb file from artifacts.elastic.co.
Install the .deb file using the dpkg command shown below:
dpkg -i filebeat-7.4.0-amd64.deb
Copy the Filebeat configuration file from your Ansible container to your WebVM's where you just installed Filebeat.
You can use the Ansible module copy to copy the entire configuration file into the correct place.
You will need to place the configuration file in a directory called files in your Ansible directory.
Run the filebeat modules enable system command.
Run the filebeat setup command.
Run the service filebeat start command.
Enable the Filebeat service on

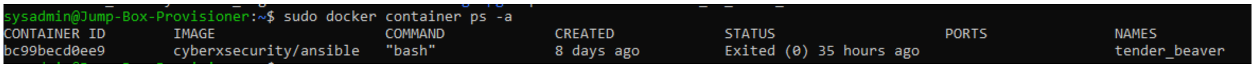
Logging into the containers:

First login to Jumpbox:



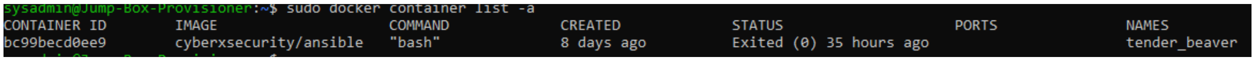
```
lilah@LAPTOP-28VR87BG MINGW64 ~
$ ssh sysadmin@13.77.182.22
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-azure x86_64)

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

  System information as of Wed Mar 24 15:08:32 UTC 2021

  System load:  0.11               Processes:           113
  Usage of /:   10.7% of 28.90GB   Users logged in:     0
  Memory usage: 28%                IP address for eth0: 10.0.0.4
  Swap usage:   0%

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

7 packages can be updated.
0 of these updates are 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.


*** System restart required ***
Last login: Wed Mar 24 14:59:22 2021 from 73.221.153.131
```

To view containers:



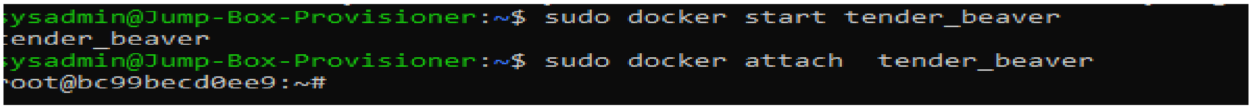
```
sysadmin@Jump-Box-Provisioner:~$ sudo docker container ps -a
CONTAINER ID        IMAGE                   COMMAND             CREATED             STATUS                       PORTS               NAMES
bc99becd0ee9        cyberxsecurity/ansible   "bash"              8 days ago          Exited (0) 35 hours ago                          tender_beaver
```

OR



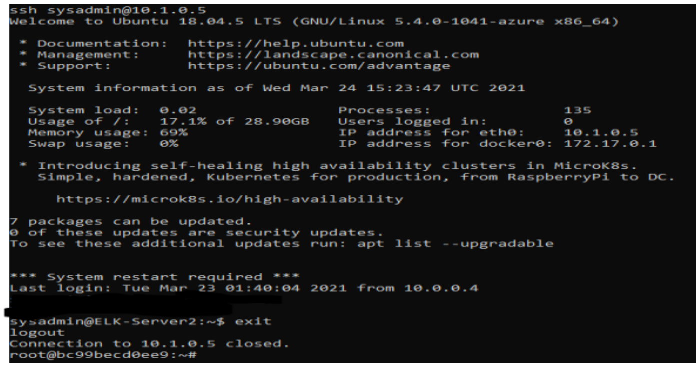
```
sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID        IMAGE                   COMMAND             CREATED             STATUS                       PORTS               NAMES
bc99becd0ee9        cyberxsecurity/ansible   "bash"              8 days ago          Exited (0) 35 hours ago                          tender_beaver
```

## Start and Attach to Container:



```
ysadmin@Jump-Box-Provisioner:~$ sudo docker start tender_beaver
ender_beaver
ysadmin@Jump-Box-Provisioner:~$ sudo docker attach  tender_beaver
oot@bc99becd0ee9:~#
```

## Verify Elk is running / EXIT

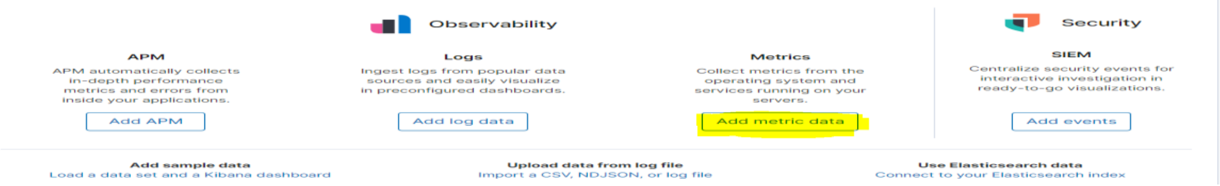


```
ssh sysadmin@10.1.0.5
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-azure x86_64)

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

  System information as of Wed Mar 24 15:23:47 UTC 2021

  System load:  0.02               Processes:              135
  Usage of /:   17.1% of 28.90GB   Users logged in:        0
  Memory usage: 69%                IP address for eth0:    10.1.0.5
  Swap usage:   0%                 IP address for docker0: 172.17.0.1

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

7 packages can be updated.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Tue Mar 23 01:40:04 2021 from 10.0.0.4
[redacted]
sysadmin@ELK-Server2:~$ exit
logout
Connection to 10.1.0.5 closed.
root@bc99becd0ee9:~#
```

## Remain in Ansible Container to add Filebeat and Metricbeat:

From the homepage of your ELK site: - Click **Add Metric Data**. - Click **Docker Metrics**. - Click the **DEB** tab under **Getting Started** for the correct Linux instructions.

Kibana GUI:



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

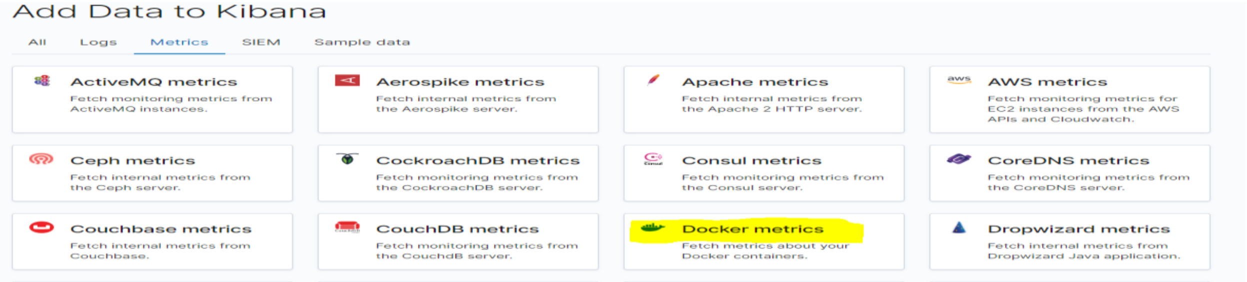
Security

**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



Add Data to Kibana

All | Logs | Metrics | SIEM | Sample data

**ActiveMQ metrics**
Fetch monitoring metrics from ActiveMQ instances.

**Aerospike metrics**
Fetch internal metrics from the Aerospike server.

**Apache metrics**
Fetch internal metrics from the Apache 2 HTTP server.

**AWS metrics**
Fetch monitoring metrics for EC2 instances from the AWS APIs and Cloudwatch.

**Ceph metrics**
Fetch internal metrics from the Ceph server.

**CockroachDB metrics**
Fetch monitoring metrics from the CockroachDB server.

**Consul metrics**
Fetch monitoring metrics from the Consul server.

**CoreDNS metrics**
Fetch monitoring metrics from the CoreDNS server.

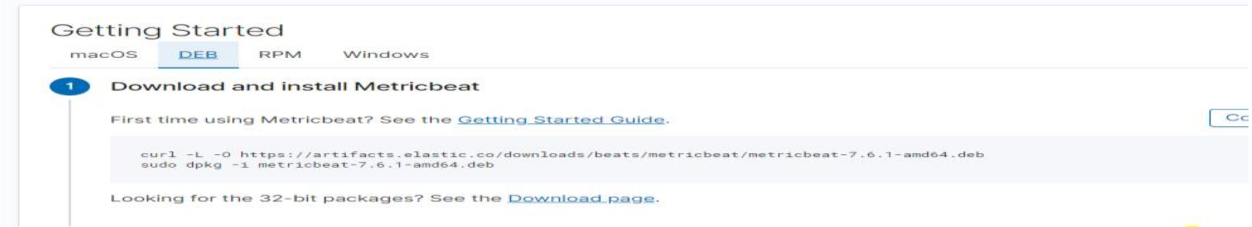
**Couchbase metrics**
Fetch internal metrics from Couchbase.

**CouchDB metrics**
Fetch monitoring metrics from the CouchdB server.

**Docker metrics**
Fetch metrics about your Docker containers.

**Dropwizard metrics**
Fetch internal metrics from Dropwizard Java application.

## Choose your set-up:



Download and install Metricbeat

First time using Metricbeat? See the Getting Started Guide.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb
sudo dpkg -i metricbeat-7.6.1-amd64.deb
```

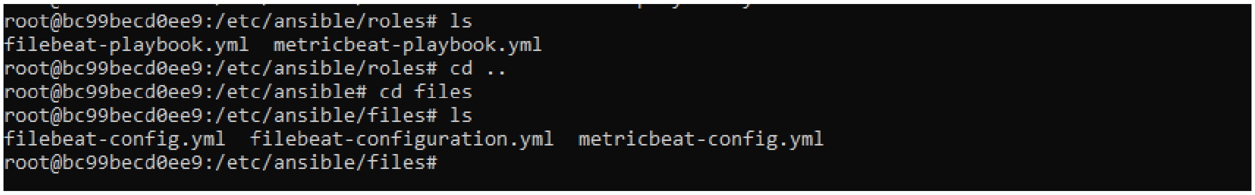
Looking for the 32-bit packages? See the Download page.

Update ansible hosts file:

```
#
#   - Comments begin with the '#' character
#   - Blank lines are ignored
#   - Groups of hosts are delimited by [header] elements
#   - You can enter hostnames or ip addresses
#   - A hostname/IP can be a member of multiple groups
# You need only a [webservers] and [elkservers] group.

# List the IP Addresses of your webservers
# You should have at least 2 IP addresses
[webservers]
10.0.0.4 ansible_python_interpreter=/usr/bin/python3
10.0.0.5 ansible_python_interpreter=/usr/bin/python3
10.0.0.6 ansible_python_interpreter=/usr/bin/python3

# List the IP address of your ELK server
# There should only be one IP address
[elk]
10.1.0.5 ansible_python_interpreter=/usr/bin/python3
```

Create config.yml in files directory and playbook.yml in roles directory:

The .yml files can be found (for filebeat conf can do a search in github)



```
root@bc99becd0ee9:/etc/ansible/roles# ls
filebeat-playbook.yml  metricbeat-playbook.yml
root@bc99becd0ee9:/etc/ansible/roles# cd ..
root@bc99becd0ee9:/etc/ansible# cd files
root@bc99becd0ee9:/etc/ansible/files# ls
filebeat-config.yml  filebeat-configuration.yml  metricbeat-config.yml
root@bc99becd0ee9:/etc/ansible/files#
```

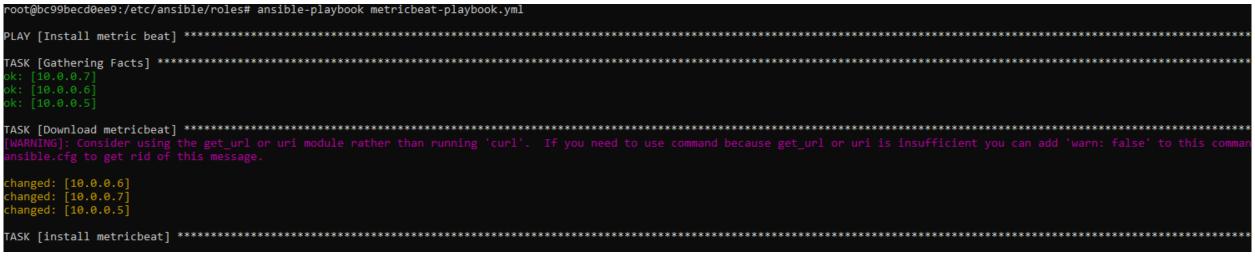
Update config.yml line #1106 with your ELK server IP and save in /etc/ansible/files/filebeat-config.yml (ctrl/shift/- allows you to jump to line#):

```
output.elasticsearch:
hosts: ["10.1.0.5:9200"]
username: "elastic"
password: "changeme"
```

And line #1806

```
setup.kibana:
host: "10.1.0.5:5601"
```

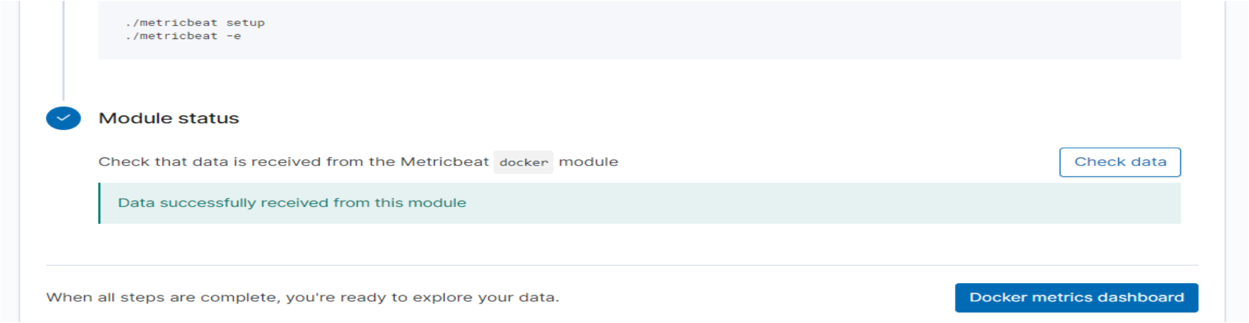
Run the playbook.yml…



```
root@bc99becd0ee9:/etc/ansible/roles# ansible-playbook metricbeat-playbook.yml

PLAY [Install metric beat] *********************************************************************************************************************

TASK [Gathering Facts] *************************************************************************************************************************
ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.5]

TASK [Download metricbeat] *********************************************************************************************************************
[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you need to use command because get_url or uri is insufficient you can add 'warn: false' to this comman
ansible.cfg to get rid of this message.

changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.5]

TASK [install metricbeat] **********************************************************************************************************************
```

Confirm in Kibana:

Click “add metric data” -> Docker metrics -> Module status -> Check data



```
./metricbeat setup
./metricbeat -e
```

Module status

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.

Example of .yml’s

filebeat-playbook.yml filebeat-configuration.yml metricbeat-configuration.yml metricbeat-playbook.yml