**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.

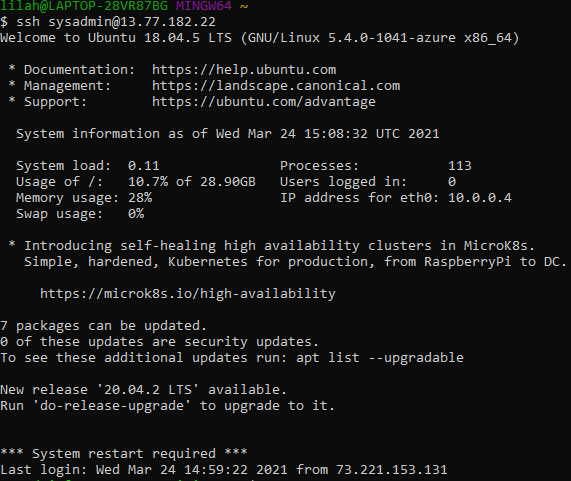
Run the filebeat setup command.

Run the service filebeat start command.

Enable the Filebeat service on

Logging into the containers:

First login to Jumpbox:



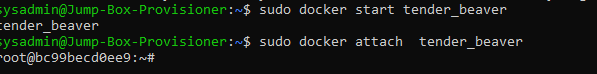
To view containers:



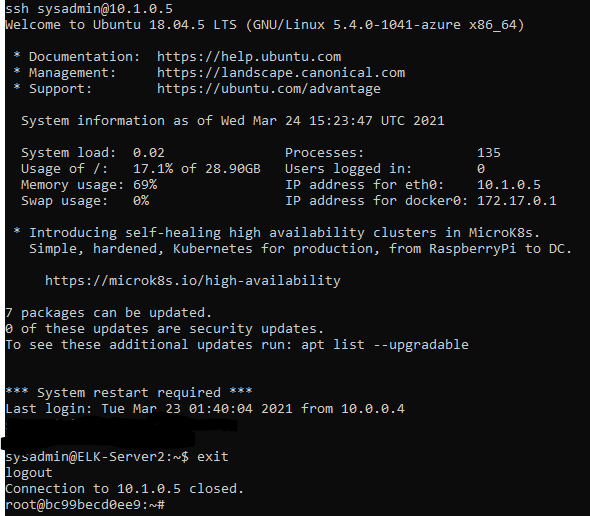
OR



Start and Attach to Container:



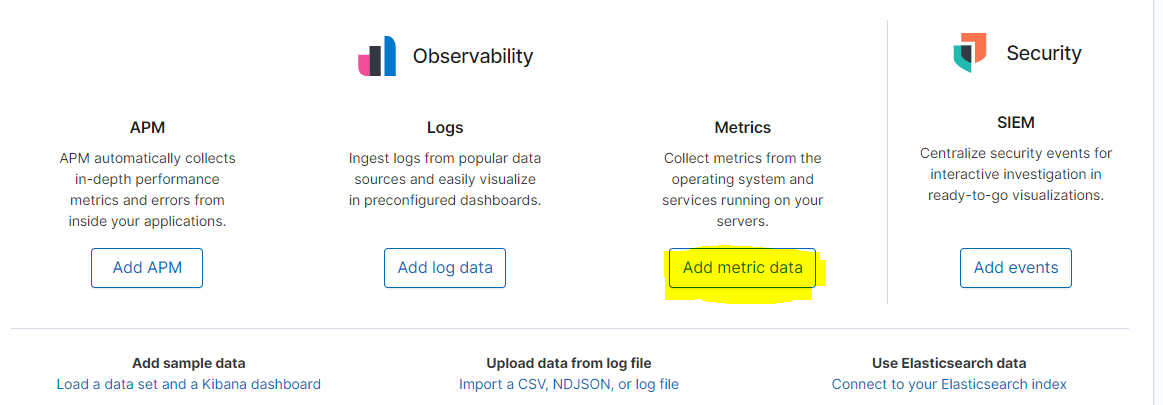
Verify Elk is running / EXIT

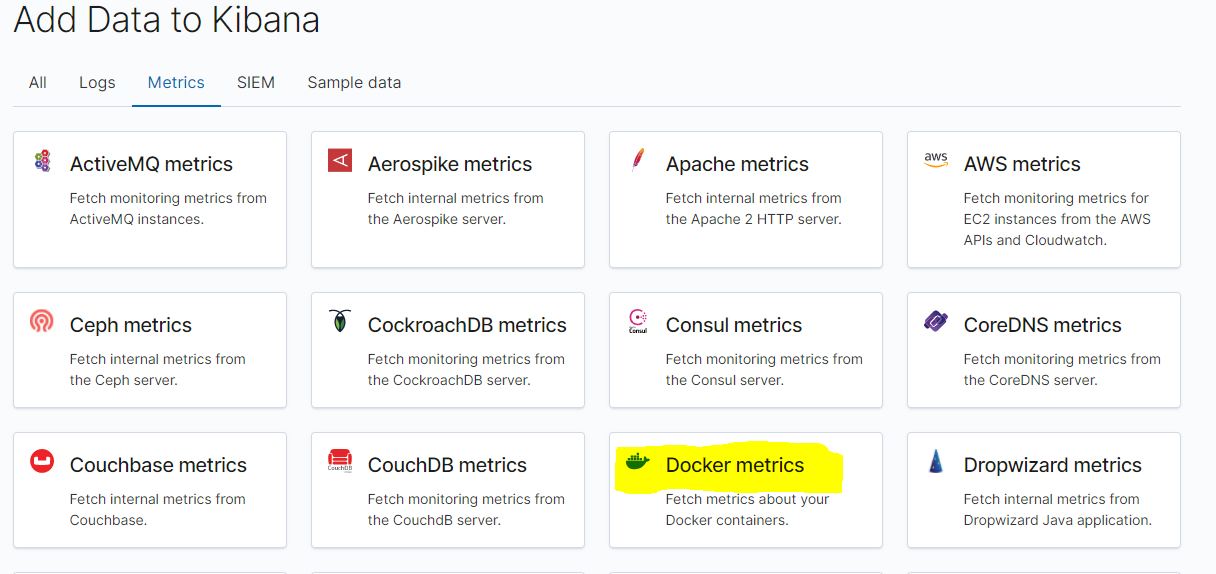


Remain in Ansible Container to add Filebeat and Metricbeat:

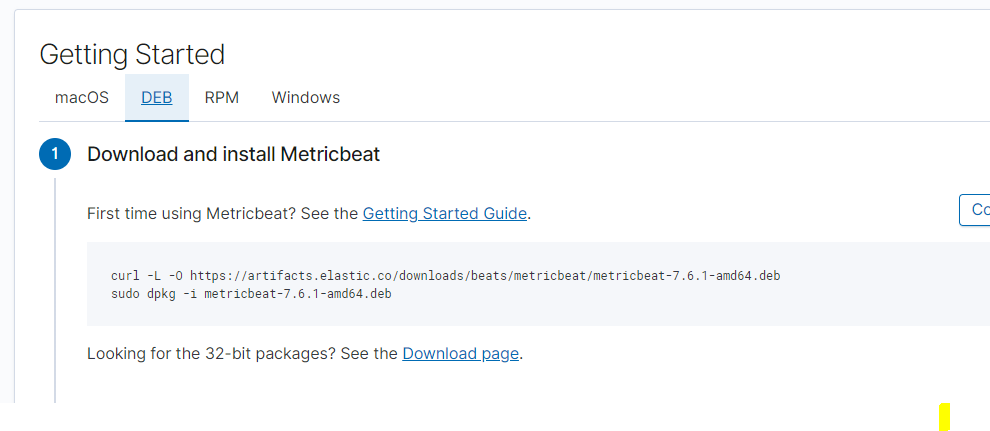
From the homepage of your ELK site: - Click **Add Metric Data**. - Click **Docker Metrics**. - Click the **DEB** tab under **Getting Started** for the correct Linux instructions.

Kibana GUI:





Choose your set-up:



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

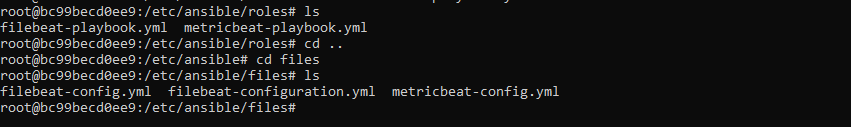
# There should only be one IP address

[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](https://d.docs.live.net/4ffd3b91036a0892/Documents/filebeat%20conf) can do a search in github)



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"

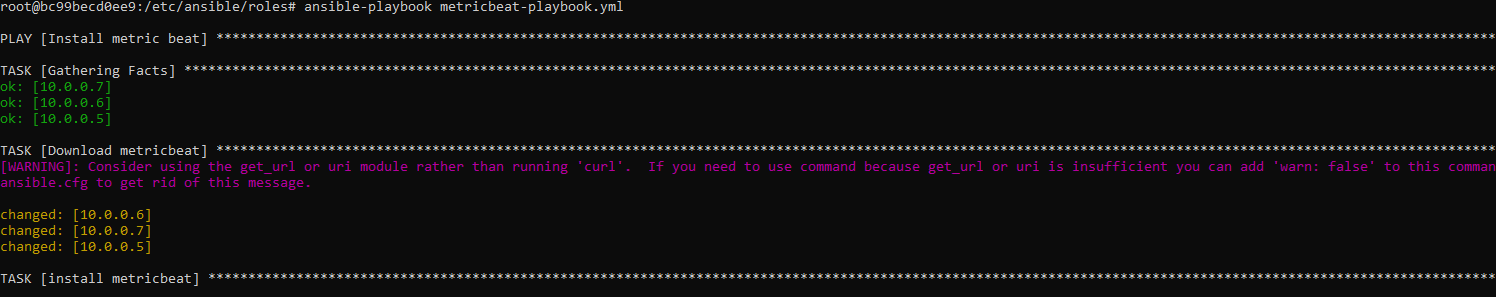
password: "changeme"

And line #1806

setup.kibana:

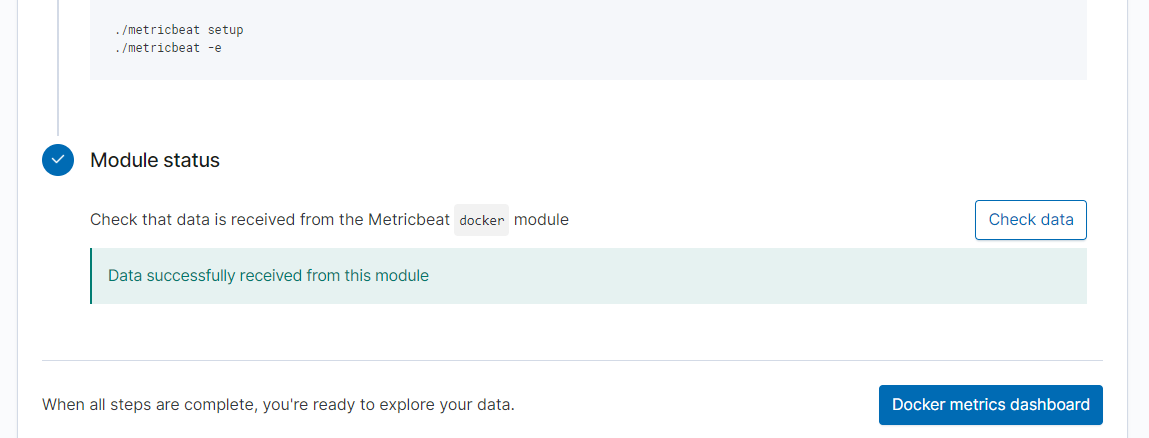
host: "10.1.0.5:5601"

Run the playbook.yml…



Confirm in Kibana:

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



Example of .yml’s

