Dynnis Feliciano

**Automated ELK Stack Deployment**

The files in this repository were used to configure the network depicted below.

CloudDiagram.png

These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the *playbook* file may be used to install only certain pieces of it, such as Filebeat.

*Ansible/Filebeat-playbook.yml*

Ansible/

This document contains the following details:

* Description of the Topology
* Access Policies
* ELK Configuration

- Beats in Use

- Machines Being Monitored

* How to Use the Ansible Build

**Description of the Topology**

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D\*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly *protected*, in addition to restricting *traffic* to the network.

**What aspect of security do load balancers protect?** *Load balancers adds security layers to a website from emerging threats to include hackers and daily rule updates similar to a virus scanner without changes to its application. Load Balancing performs security role by defending an organization against distributed denial-of-service (DDoS) attacks. Its primary purpose of load balancing is to prevent any single server from getting overloaded.*

**What is the advantage of a jump box?** *A jumpbox improve security in a Microsoft Azure deployment by blocking public IP address automatically associated with any VMs. It is a secure computer that you connect before performing administrative task to connect to other servers. It also serves as an intermediary host or an SSH gateway to a remote network.*

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the *logs* and system *traffic*.

**What does Filebeat watch for?** *Filebeat monitors and forwards log data to a location that users specify, collects log events, and forwards them either to Elastisearch or Logstash for indexing.*

**What does Metricbeat record?** *Metricbeat collects the metrics and statistics that it collects and ships them to the output that you specify; Elasticsearch or Logtash. This tool helps monitor servers by collecting metrics from system and services running on the service such as Apache.*

The configuration details of each machine may be found below.

(Note: Use the Markdown Table Generator (http://www.tablesgenerator.com/markdown\_tables) to add/remove values from the table)

|

| **Name** | **Function** | **IP Address** | **Operating System** |
| --- | --- | --- | --- |
| Jump Box | Ansible | 10.1.0.4 | Linux |
| Web-1 | DVWA | 10.1.0.5 | Linux |
| Web-2 | DVWA | 10.1.0.6 | Linux |
| Web-3 | DVWA | 10.1.0.7 | Linux |
| Web-4 | ELK | 10.2.0.7 | Linux |

**Access Policies**

The machines on the internal network are not exposed to the public Internet.

Only the *Jumpbox* machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

Add whitelisted IP addresses: 75.169.36.147

Machines within the network can only be accessed by *Jumpbox*.

**Which machine did you allow to access your ELK VM?**  *The Jumpbox is allowed to access the ELK (Web-4) VM. The private IP address is* 10.1.0.4.

**What was its IP address?** 75.169.36.147

A summary of the access policies in place can be found in the table below.

|

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes | 10.1.0.5; 10.1.0.6; 10.1.0.7 |
| ELK (Web-4) | Yes | 10.2.0.7 |

**Elk Configuration**

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

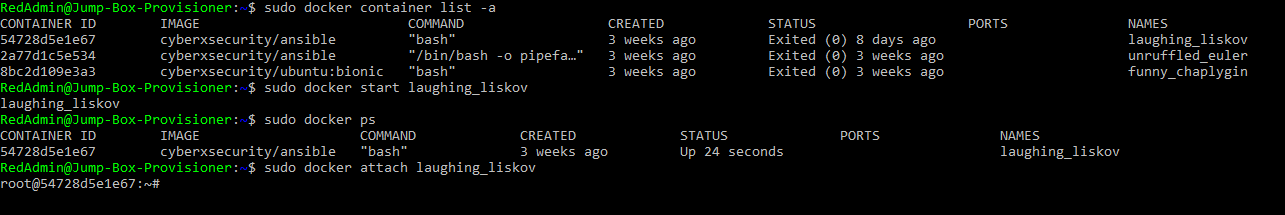
**What is the main advantage of automating configuration with Ansible?** *This time-saving tool allows for a reliable VM infrastructure which automates all your IT environments / configurations, applications, provisioning, etc. from a single tool.*

**The playbook implements the following tasks:**

* *Install Python3-pip*
* *Install Docker using pip*
* *Install Elk*
* *Enable docker service on restart*

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

Update the path with the name of your screenshot of docker ps output](Images/docker\_ps\_output.png)



**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

*- List the IP addresses of the machines you are monitoring:*

10.1.0.5

10.1.0.6

10.1.0.7

10.2.0.7

We have installed the following Beats on these machines:

*- Specify which Beats you successfully installed:*

*Filebeat*

*Metricbeat*

These Beats allow us to collect the following information from each machine:

*Filebeat monitors and forwards log data to a location that users specify, collects log events, and forwards them either to Elastisearch or Logstash for indexing.*

*Metricbeat collects the metrics and statistics that it collects and ships them to the output that you specify; Elasticsearch or Logtash. This tool helps monitor servers by collecting metrics from system and services running on the service such as Apache.*

**Using the Playbook**

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

**SSH into the control node and follow the steps below:**

* Copy the *Playbook.yml* file *to ansible container in the Jumpbox.*
* Update the *ansible.cfg* file to include *Private IP addresses of the four VMs.*

**Web-1: 10.1.0.5**

**Web-2: 10.1.0.6**

**Web-3: 10.1.0.7**

**Web-4: 10.2.0.7**

* Run the playbook and navigate to **http://23.99.220.146:5601/app/kibana** to check that the installation worked as expected.

**Answer the following questions to fill in the blanks:**

Which file is the playbook?

*Filebeat and Metricbeat playbooks.*

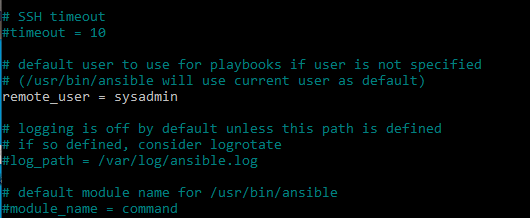
Where do you copy it?

*The Filebeat and Metricbeat playbooks are copied in the ansible container*

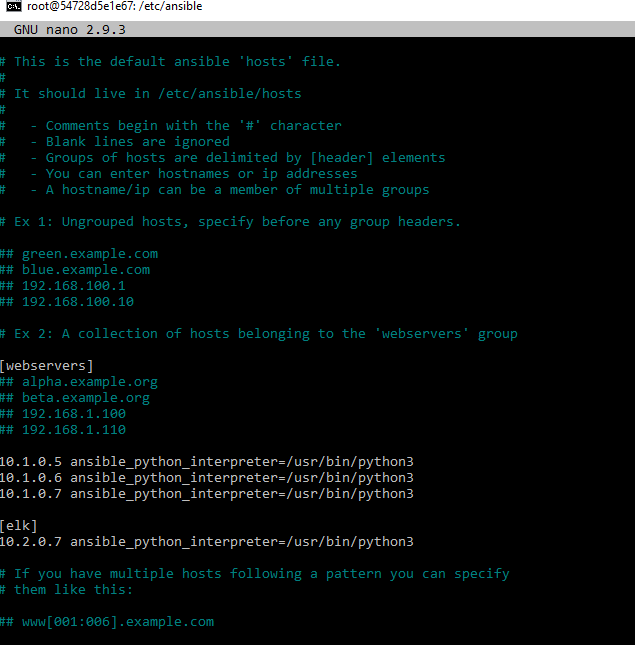
Which file do you update to make Ansible run the playbook on a specific machine?

*Ansible.cfg file*

*Using the sudo docker container list -a, once you’ve successfully attached to the docker container (i.e., laughing\_liskov : root@54728d5e1e67), you can modify the ansible.cfg in /etc/ansible/ and use nano ansible.cfg to create a default user for the playbook. See attached figure below.*



*etc/ansible/hosts*



How do I specify which machine to install the ELK server on versus which to install Filebeat on?

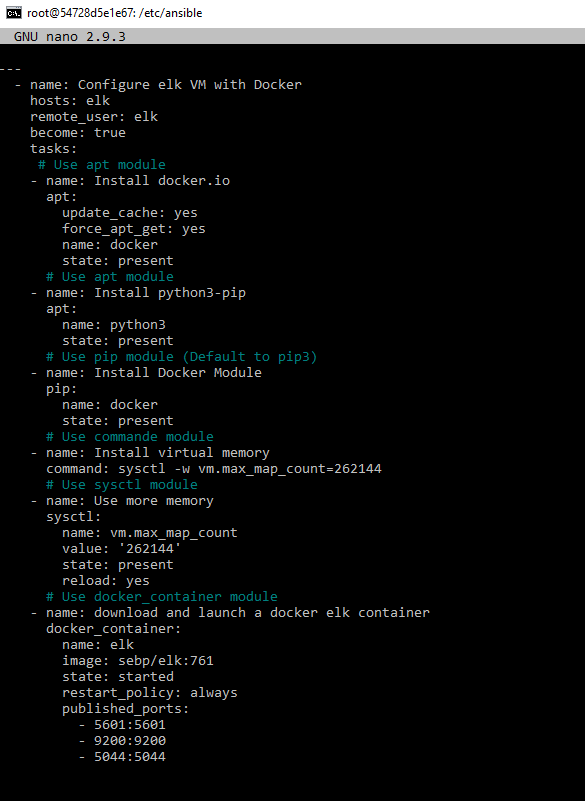
*By adding the ELKs Private IP address to the ansible.cfg file*

Which URL do you navigate to in order to check that the ELK server is running?

**http://23.99.220.146:5601/app/kibana**

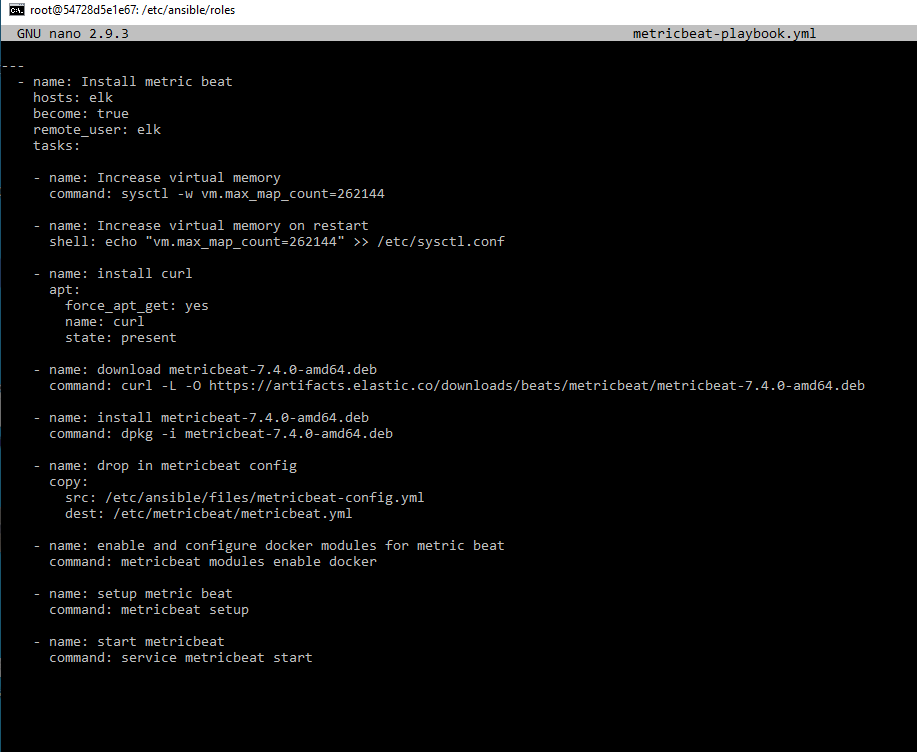
\_As a \*\*Bonus\*\*, provide the specific commands the user will need to run to download the playbook, update the files, etc.

**Using the Docker Container prompt: nano install-elk.yml**



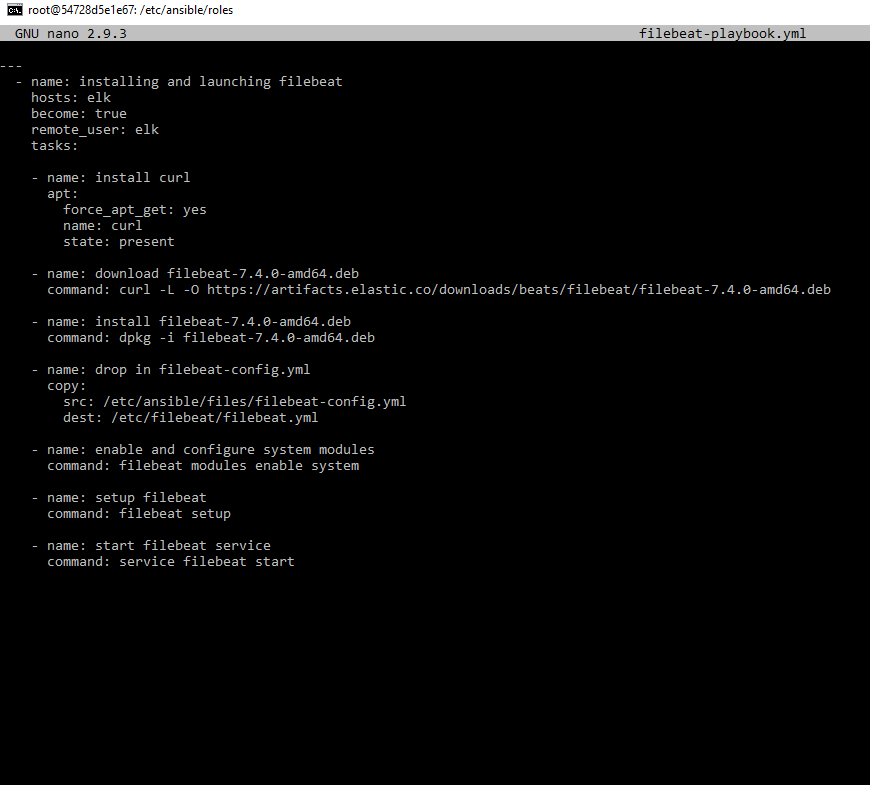
**Using the Docker Container prompt: nano metricbeat-playbook.yml**

**Using the Docker Container prompt: ansible-playbook metricbeat-playbook.yml**

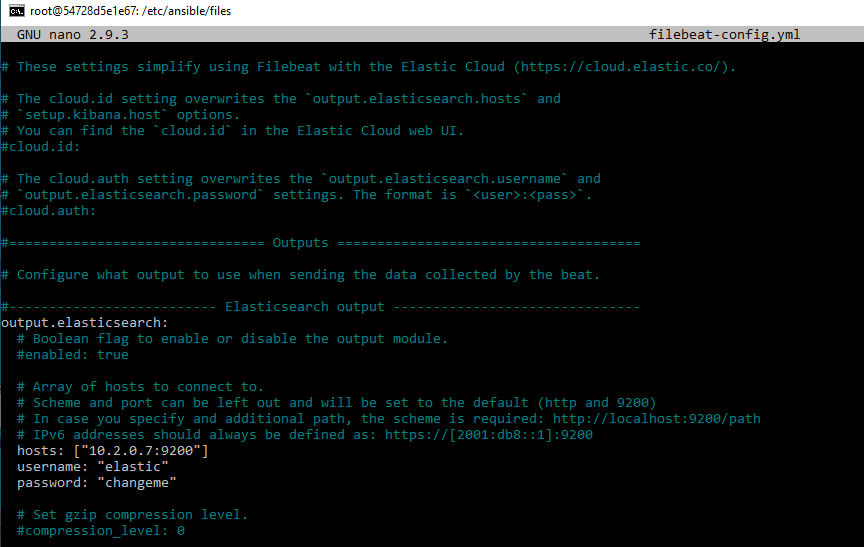


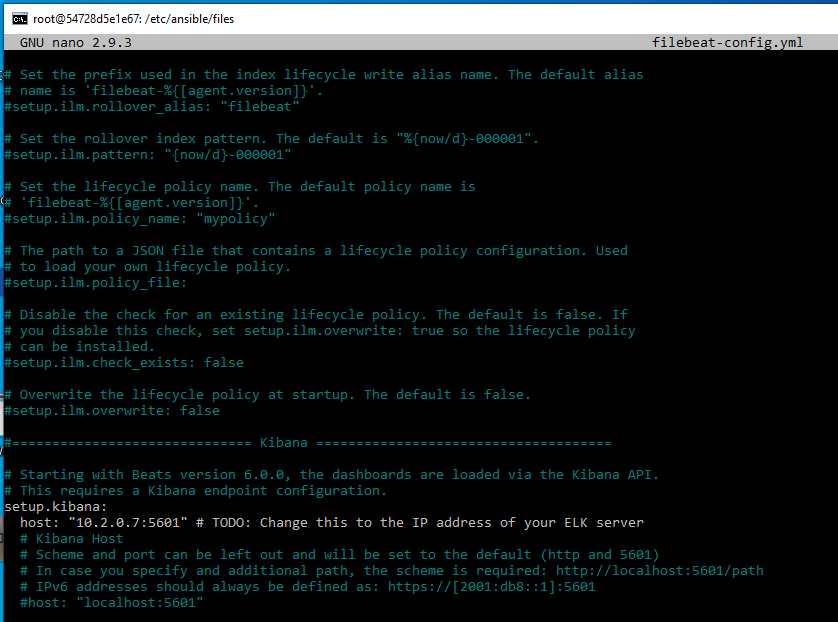
**Using the Docker Container prompt: nano filebeat-playbook.yml**

**Using the Docker Container prompt: ansible-playbook filebeat-playbook.yml**

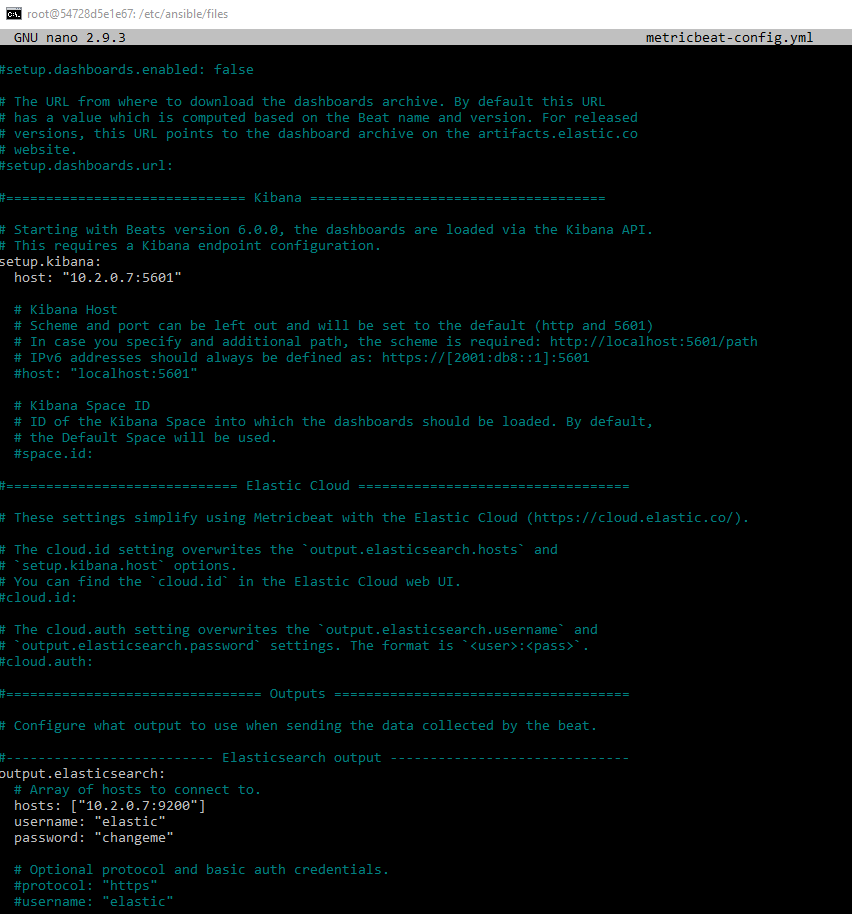


**Using the Docker Container prompt: nano filebeat-config.yml**

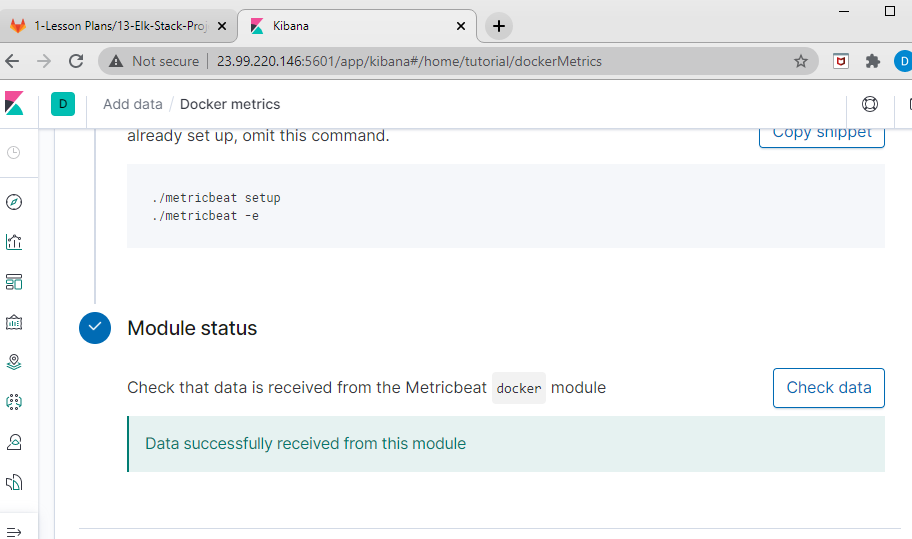




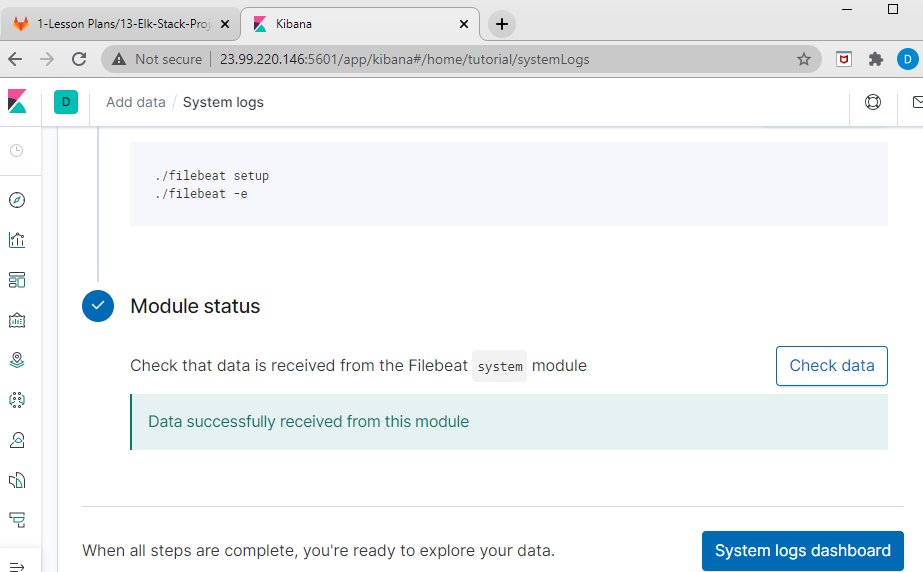
**Using the Docker Container prompt: nano metricbeat-config.yml**



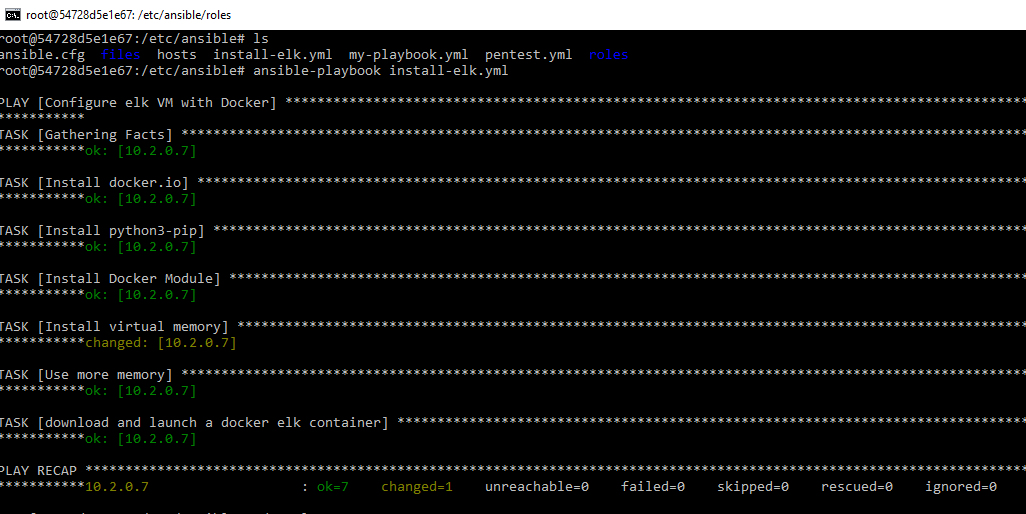
**Kibana Metricbeat Docker**



**Kibana Metricbeat Docker**



**Using the Docker Container promopt: ansible-playbook install-elk.yml**



**Using the Docker Container promopt: ansible-playbook filebeat-playbook.yml**



**Using the Docker Container promopt: ansible-playbook metricbeat-playbook.yml**

