

README

Project #1: Cloud Security



December 22, 2020

Cybersecurity

Table of Contents

[Enter the playbook files 4](#_Toc59539344)

[**1.** **Description of the Topology** 5](#_Toc59539345)

[*a) What aspect of security do load balancers protect? 5*](#_Toc59539346)

[*b) What is the advantage of a jump box? 5*](#_Toc59539347)

[*c) What does Filebeat watch for? 6*](#_Toc59539348)

[*d) What does Metricbeat record? 6*](#_Toc59539349)

[**2.** **Access Policies** 7](#_Toc59539350)

[*a) Add whitelisted IP addresses: 7*](#_Toc59539351)

[*b) Which machine did you allow to access your ELK VM? What was its IP address? 7*](#_Toc59539352)

[**3.** **Elk Configuration** 8](#_Toc59539353)

[*a) What is the main advantage of automating configuration with Ansible? 8*](#_Toc59539354)

[*b) In 3-5 bullets, explain the steps of the ELK installation play. 8*](#_Toc59539355)

[**4.** **Target Machines & Beats** 9](#_Toc59539356)

[*a) List the IP addresses of the machines you are monitoring\_ 9*](#_Toc59539357)

[*b) Specify which Beats you successfully installed\_ 9*](#_Toc59539358)

[*c) In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.\_ 10*](#_Toc59539359)

[**5.** **Using the Playbook** 14](#_Toc59539360)

[*a) SSH into the control node and follow the steps below: 14*](#_Toc59539361)

[*b) Answer the following questions to fill in the blanks 14*](#_Toc59539362)

[**6.**  **\*\*Bonus\*\*** 16](#_Toc59539363)

[**7.** **Appendix – Playbooks & Host file** 18](#_Toc59539364)

[*a) my\_playbook.yml 18*](#_Toc59539365)

[*b) metricbeat-playbook.yml 19*](#_Toc59539366)

[*c) filebeat-playbook.yml 19*](#_Toc59539367)

[*d) my\_elkplaybook.yml 20*](#_Toc59539368)

[*e) hosts (ansible) 21*](#_Toc59539369)

[**8.** **Appendix – Accessing DVWA Website via the Load-Balancer** 22](#_Toc59539370)

Automated ELK Stack Deployment

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

[UTCyberMasgu/Project-1: Repository for storing the project files related to CyberSecurity Project #1 (Cloud Security) (github.com)](https://github.com/UTCyberMasgu/Project-1)

Diagram

Description automatically generated

*Diagram 1*

**Images/SKARIA\_ALEXANDER - C2W14 - Project-1.JPG**

*The Network Topology of the initial network deployed with DVWA container in Web-1 and Web-2 servers that are only accessible via the Load-Balancer.*

*Diagram

Description automatically generated*

*Diagram 2*

**Images/** **SKARIA\_ALEXANDER - C2W12 - Cloud Security HW-Diagram**

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 **filebeat-playbook.yml** file may be used to install only certain pieces of it, such as Filebeat.

## **Enter the playbook files**

* **my\_playbook.yml -** Used to define the DVWA container on docker in the Web-1 and Web-2 servers
* **filebeat-playbook.yml -** Used to download, install and configure filebeat in the Web-1 and Web-2 servers
* **metricbeat-playbook.yml –** Used to download, install and configure metricbeat in the Web-1 and Web-2 servers
* **my\_elkplaybook.yml -** Used to install, and configure the ELK container on the ELK Server

This document contains the following details:

1. **Description of the Topology**
2. **Access Policies**
3. **ELK Configuration**
4. **Beats in Use**
5. **Machines Being Monitored**
6. **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 **secure and** **available**, in addition to restricting **access** to the network.

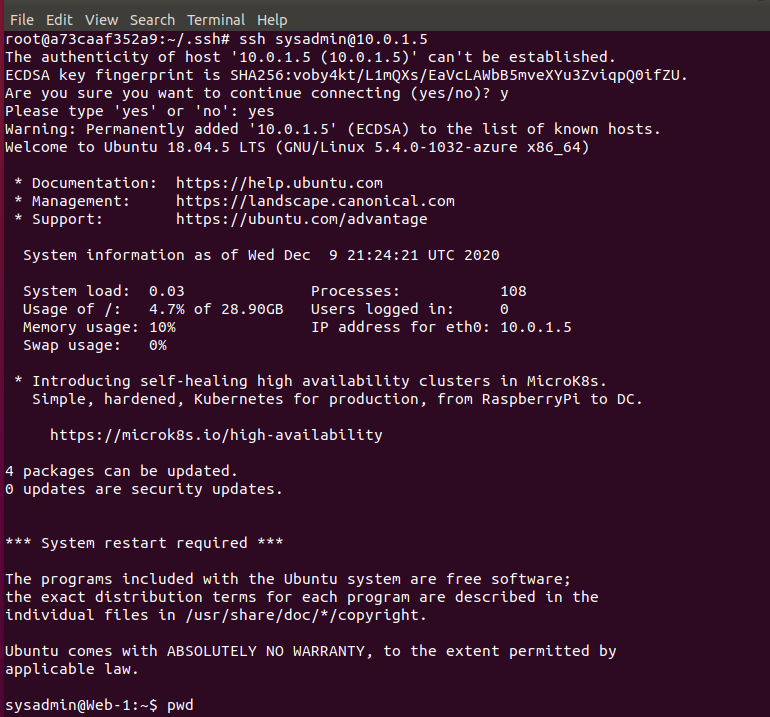
## **What aspect of security do load balancers protect?**

Load balancers protect organization against DDoS attacks by distributing traffic across multiple servers. This process also prevents any one server from getting overloaded and potentially unable to respond to requests.

## **What is the advantage of a jump box?**

Jump Box functions as a secure host that is used to conduct administrative tasks. Jump box is an intermediary host that functions as a gateway via SSH to internal networks. The existence of a Jump box *(Jump-box-provisioner)* segregates direct access to the internal network in this case to Web-1, Web-2 and the ELK Server

*For instance: Snapshot of SSH access from Jump-Box-Provisioner running Ansible container to Web-1*



*For instance: Snapshot of SSH access from Jump-Box-Provisioner running Ansible container to the ELK Server*



*In reference to Diagram #1 above, the Jump box is used as an intermediary to:*

* *install, configure and launch the DVWA Containers on Docker resident on Web-1 (10.0.1.5) and Web-2 (10.0.1.6)*
* *install, configure and launch the ELK Container on the ELK Server (10.1.0.4)*
* *install, configure and launch the Filebeat & Metricbeat features on Web-1 and Web-2 to send logs to the skaria-ProjectVM (ELK Server).*

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 watches and monitors the log files or user-specified locations, collects log events and forwards them to Elasticsearch of Logstash for indexing. Filebeat is a medium to forward and centralize log data.

## **What does Metricbeat record?**

Metricbeat records changes to user specified system and configuration files. Metricbeat ships metric data of the changes for monitoring system and the processes running on the system.

The configuration details of each machine may be found below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Function** | **Public IP Address** | **IP Address** | **Operating System** |
| Jump-Box-Provisioner | Gateway | 52.255.162.156 | 10.0.1.4 | Linux |
| Web-1 | DVWA Host, Filebeat, Metricbeat | 52.188.20.100 | 10.0.1.5 | Linux |
| Web-2 | 10.0.1.6 | Linux |
| skaria-projectVM | ELK Server | 104.210.15.174 | 10.1.0.4 | Linux |

# **Access Policies**

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

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

## **Add whitelisted IP addresses:**

184.145.3.76

Machines within the network can only be accessed by **Jump Box**.

## **Which machine did you allow to access your ELK VM? What was its IP address?**

Skaria-projectVM (ELK VM) can be accessed only by the Jump-Box-Provisioner (Jump Box VM) via the Ansible Container on Docker. The IP address of the Jump Box is 10.0.1.4.

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP addresses** |
| Jump-Box-Provisioner | Yes | 10.0.1.5 10.0.1.6 |
|  |  |  |

# **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?**

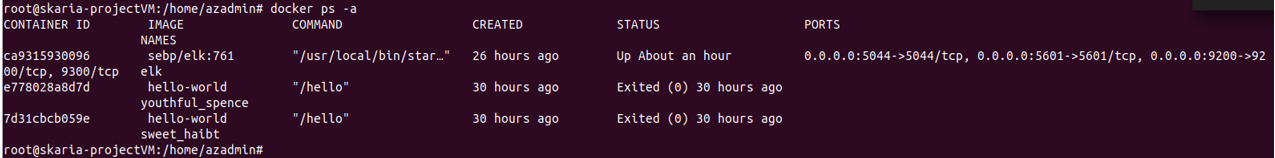
The automated configuration via Ansible ensures that the DVWA Containers, Filebeat and Metricbeat processes are automatically launched when the VM is re-started. There is no manual intervention required each time the VMs are started.

The playbook implements the following tasks:

## **In 3-5 bullets, explain the steps of the ELK installation play.**

1. Installs the apt packages - Docker engine (docker.io) used for running containers and the package to install Python software (python3-pip)
2. Installs the Python client for Docker
3. Sets the Memory Size of the ELK Server to use more memory
4. Downloads the Docker container for ELK **called sepb/elk:761** and configures the container to start at specific port mappings (5601:5601, 9200:9200, 5044:5044)
5. Starts the Container

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



# **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

## **List the IP addresses of the machines you are monitoring\_**

We have installed the following Beats on these machines:

|  |  |  |
| --- | --- | --- |
| **Name** | **Function** | **IP Addresses** |
| Web-1 | DVWA Container | 10.0.1.5 |
| Web-2 | DVWA Container | 10.0.1.6 |

## **Specify which Beats you successfully installed\_**

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

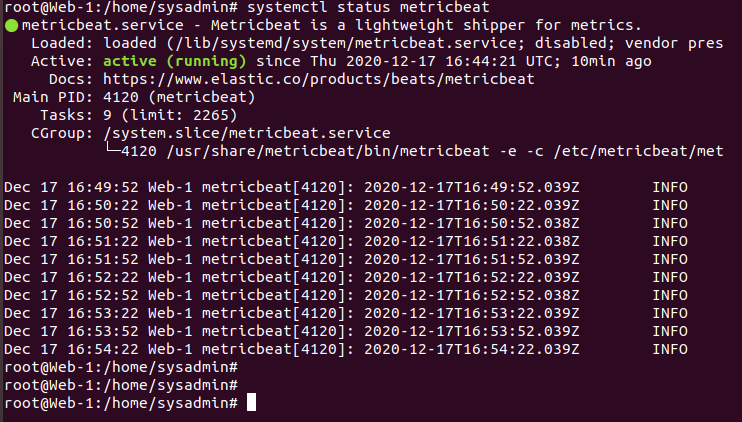
* **Filebeat**

*Filebeat watches and monitors the log files or user-specified locations, collects log events on Web-1 and Web-2; and forwards them to skaria-projectVM ~ Elasticsearch of Logstash for indexing.*



* **Metribeat**

*Metricbeat records changes to user specified system and configuration files on Web-1 and Web-2 that hosts the DVWA Container. Metricbeat ships metric data of the changes to skaria-projectVM (ELK Server) for monitoring system and the processes running on the system.*

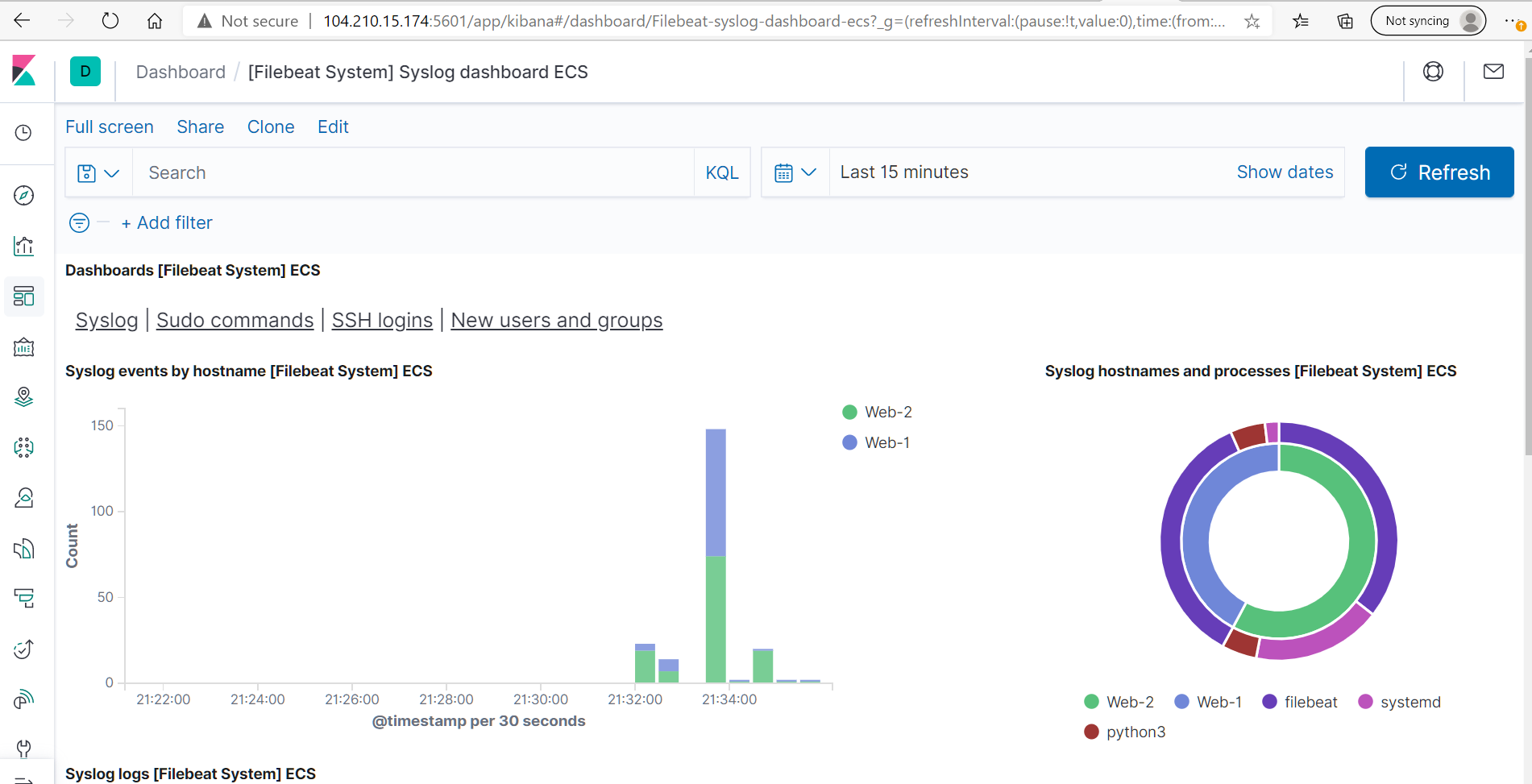


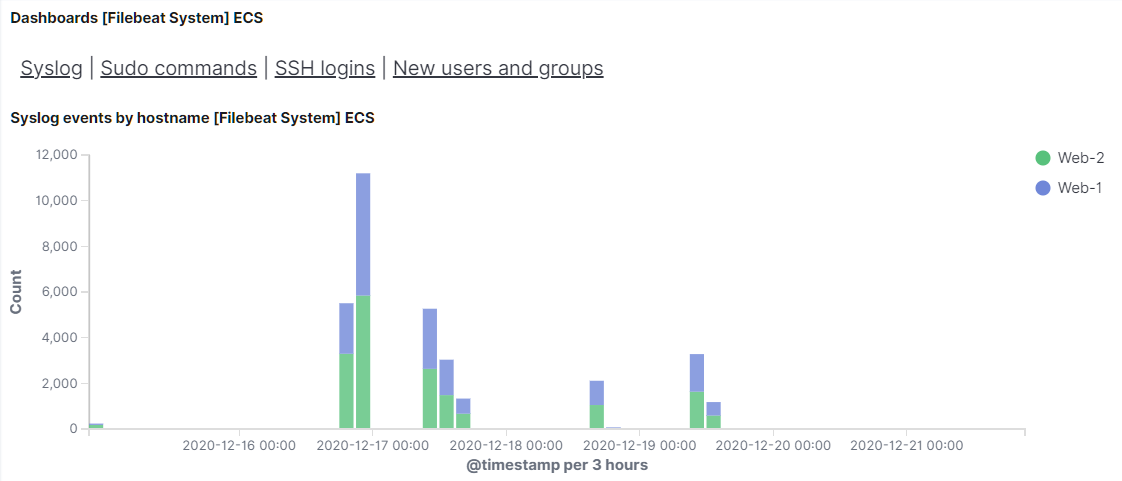
## **In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.\_**

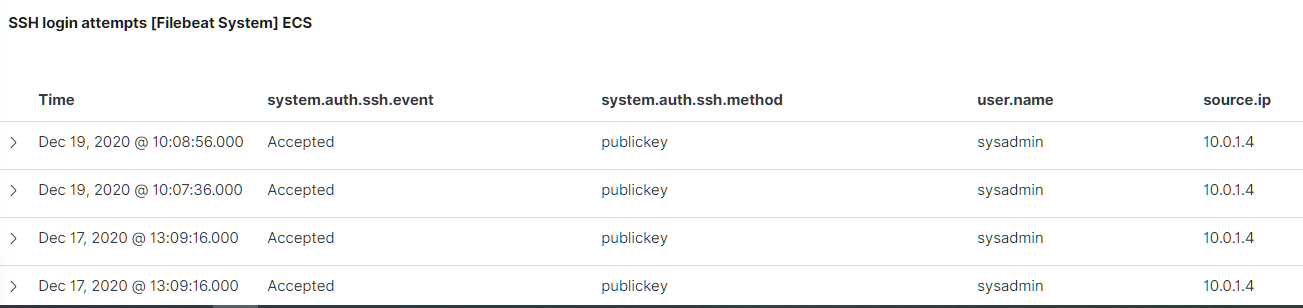
In our network topology, Filebeat is configured to monitor changes to System Logs.

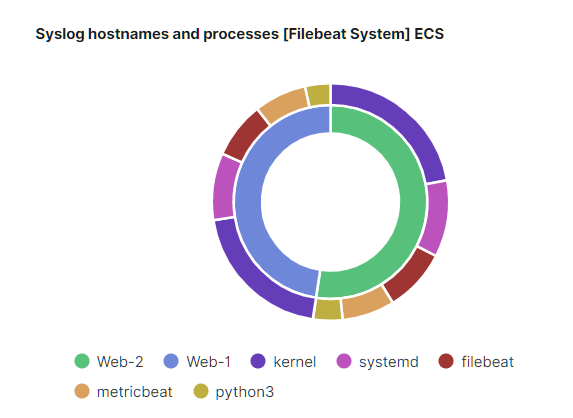
*For instance,*

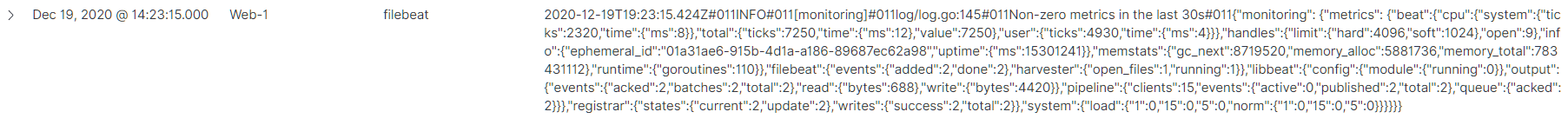
* SSH Login attempts, Successful SSH logins, SSH user of failed login attempts
* Top SUDO commands, Sudo commands by user
* Syslog events by hostname

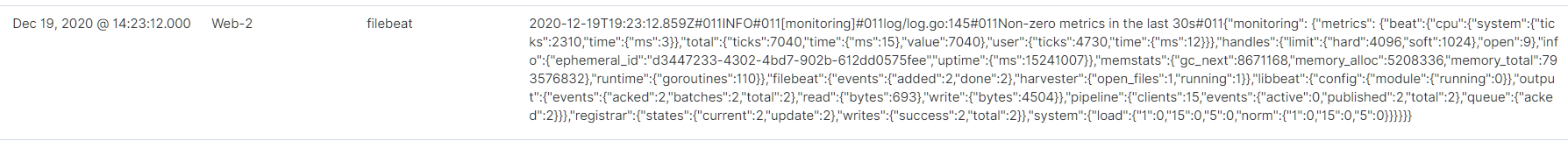








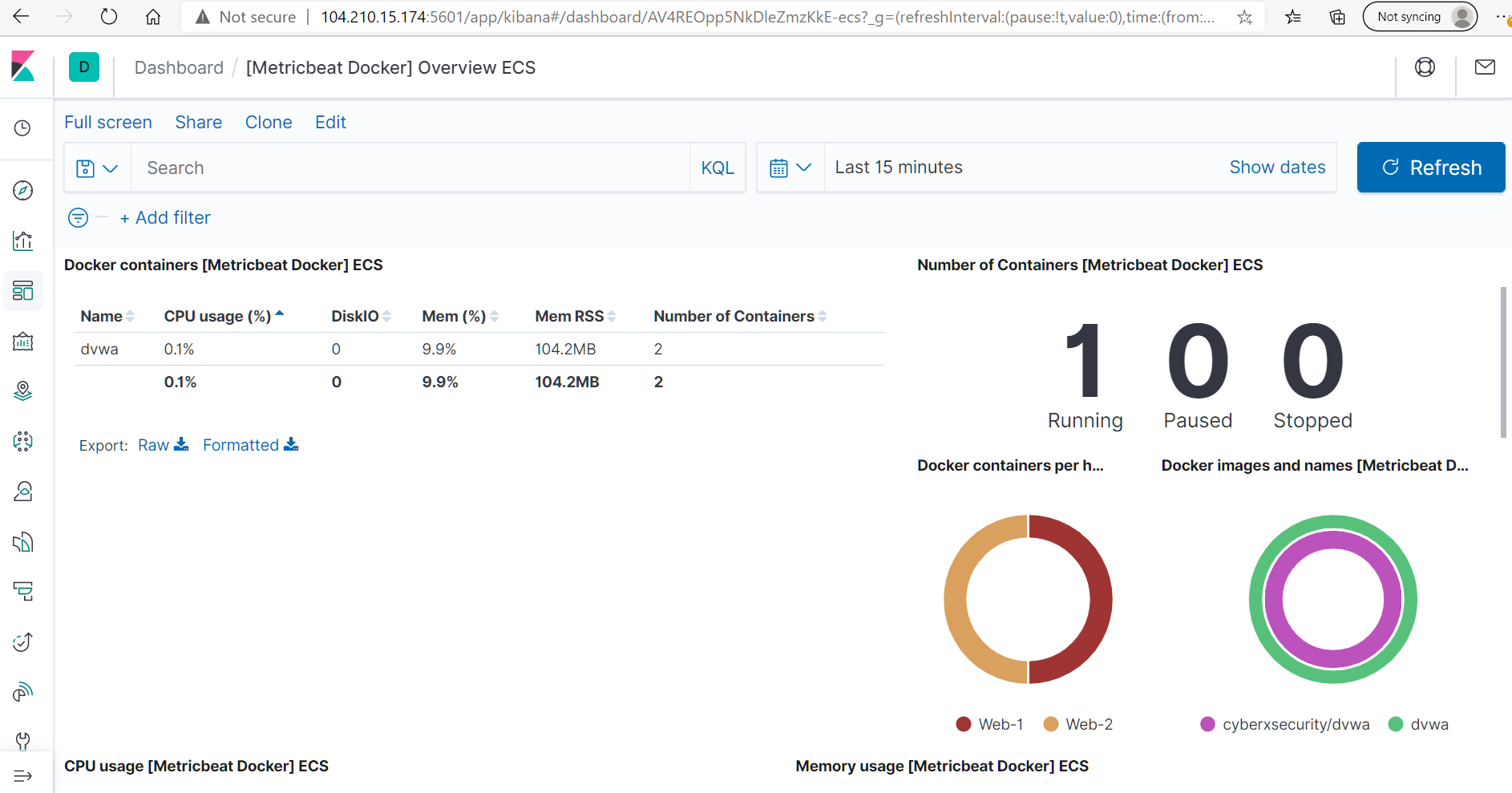


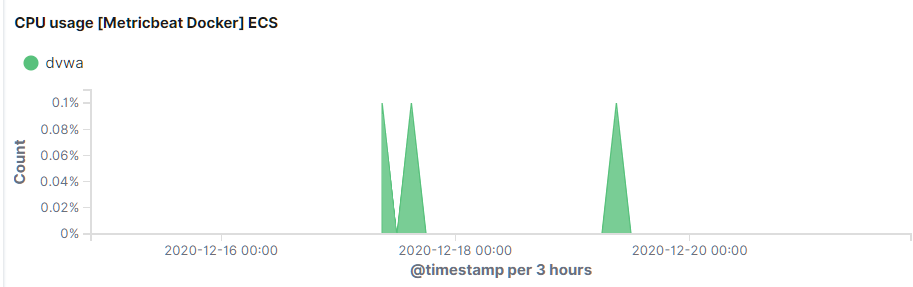


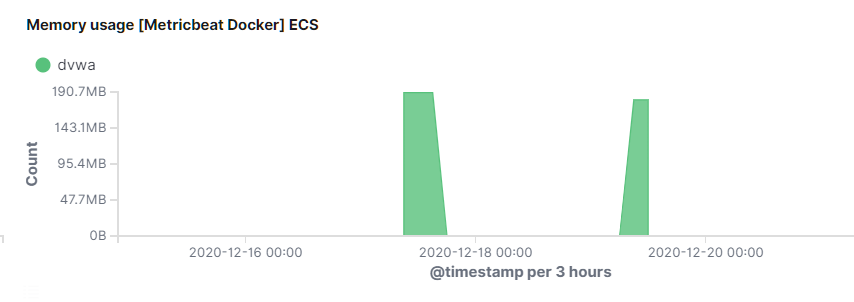
In our network topology, Metricbeat is configured to monitor Docker container metrics.

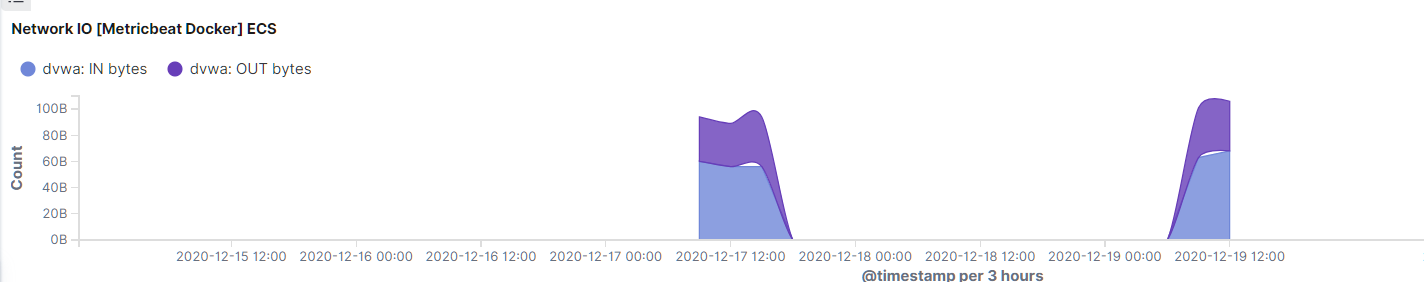
*For instance,*

* CPU Usage
* Memory Usage
* Network I/O









# **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 **my\_playbook.yml** file to the **ansible container hosted on the Jump-Box-Provisioner**\_\_\_\_\_.
* Update the **ansible.cfg** file to **include the IP Addresses of Web-1 (10.0.1.5) and Web-2 (10.0.1.6)**
* Run the playbook, and navigate to [**http://104.210.15.174:5601/app/kibana**](http://104.210.15.174:5601/app/kibana) to check that the installation worked as expected.

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

* **Which file is the playbook? Where do you copy it?**
* filebeat-playbook.yml
* metricbeat-playbook.yml
* The playbooks are copied in the ansible container to the /etc/ansible/roles directory
* **Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on?**
* The **hosts** file resident in the directory **/etc/ansible** on the ansible container
* Update the hosts file to specify the machines to install the Filebeat on

**[webservers]**

10.0.1.5 ansible\_python\_interpreter=/usr/bin/python3

10.0.1.6 ansible\_python\_interpreter=/usr/bin/python3

* Update the hosts file to specify the machine to install the ELK server on

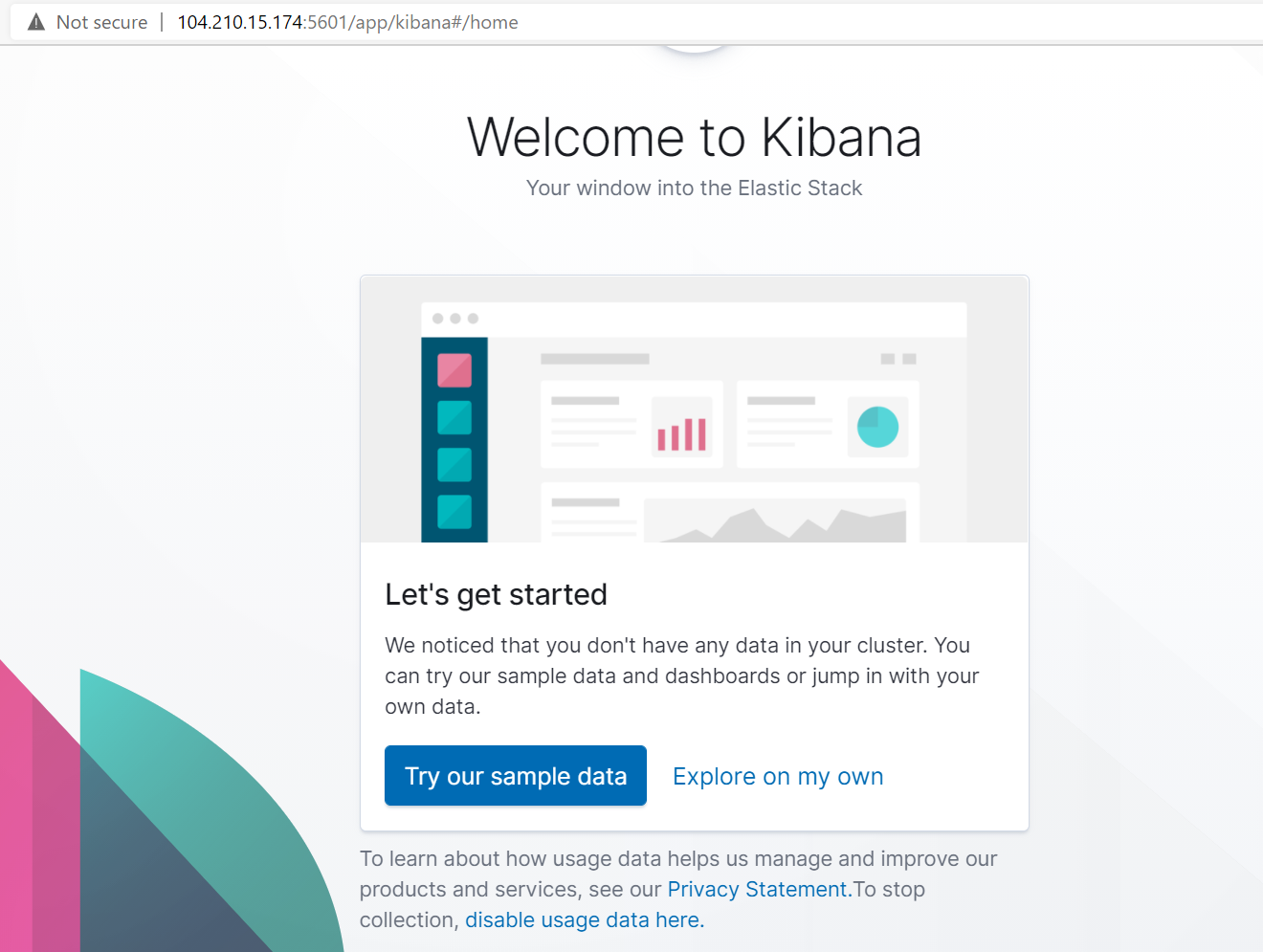
**[elk]**

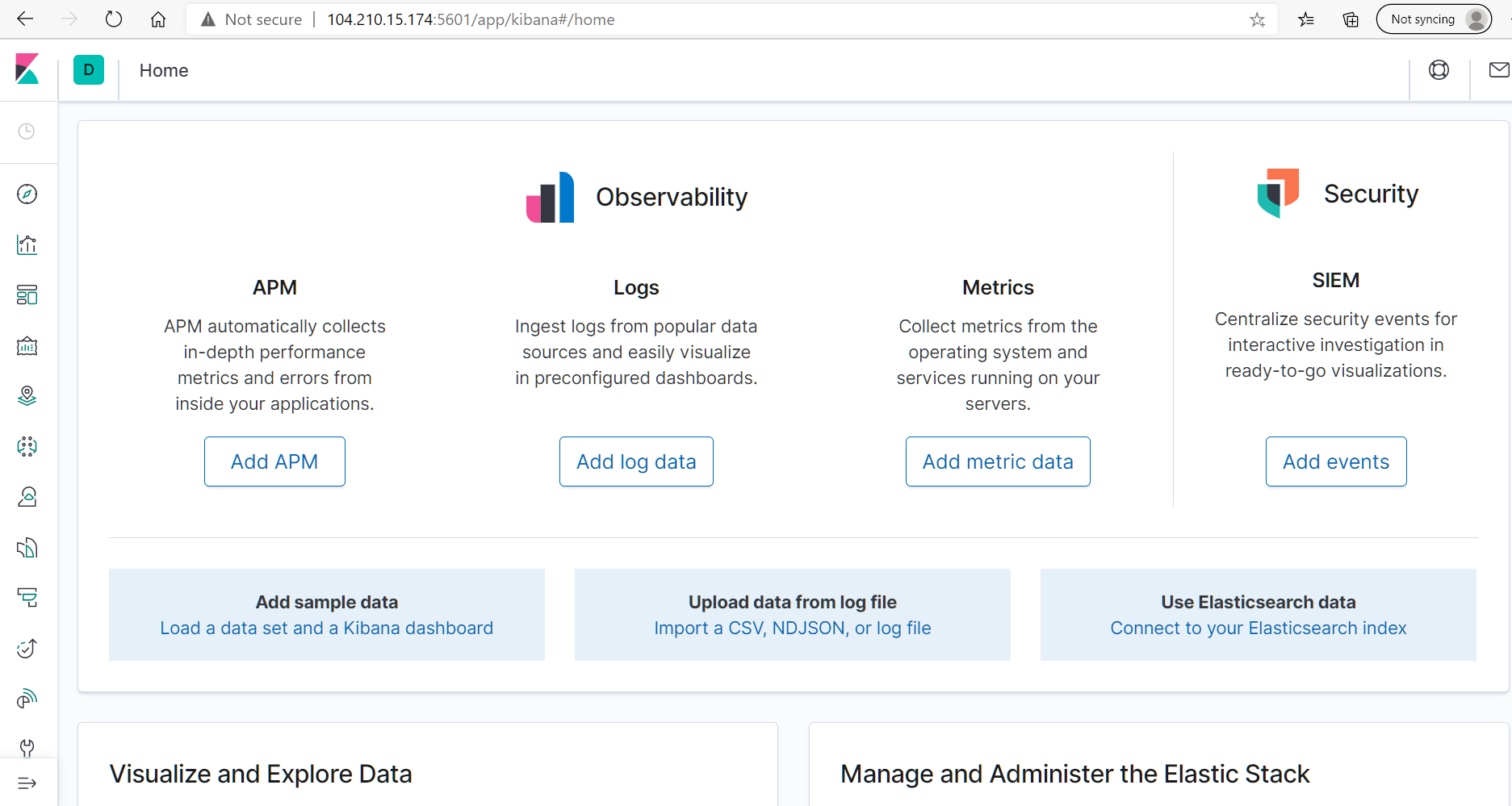
10.1.0.4 ansible\_python\_interpreter=/usr/bin/python3

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

[*http://104.210.15.174:5601/app/kibana*](http://104.210.15.174:5601/app/kibana)

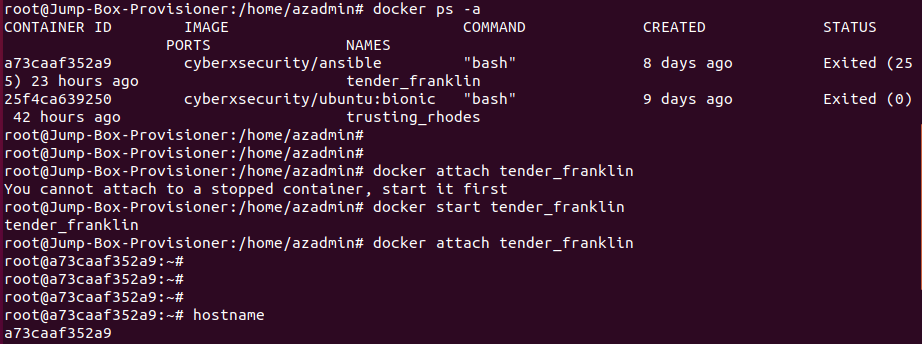
*Where 104.210.15.174 is the Public IP address of skaria-projectVM-IP*





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

First, login to the Jumb-box-provisioner and ensure ansible is running and attach to the ansible container.

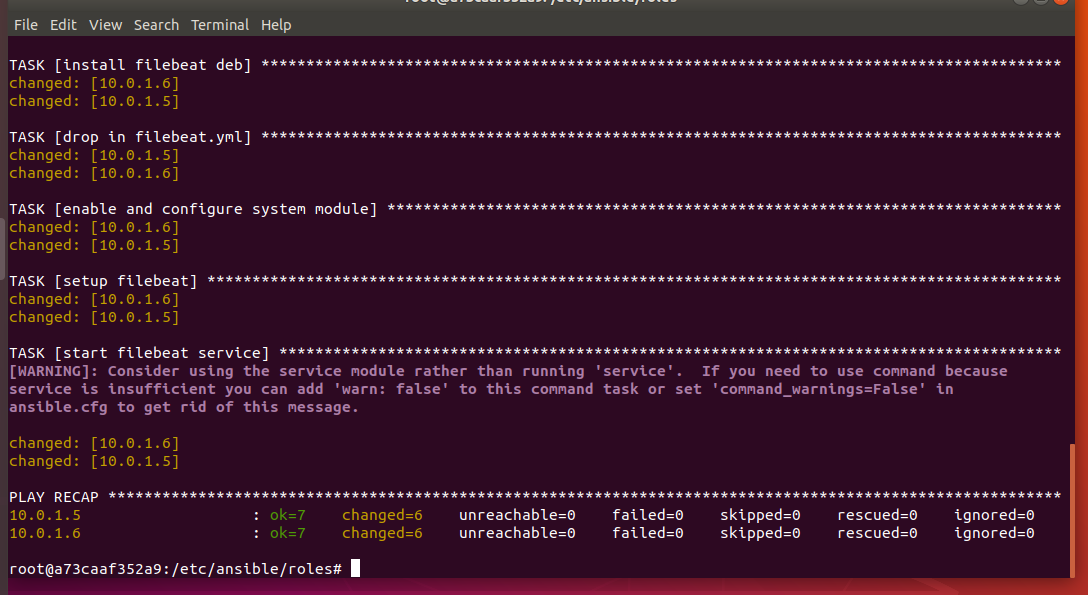


Update the hosts file in /etc/ansible/hosts to include the specific machines on which to download, install and configure filebeat.

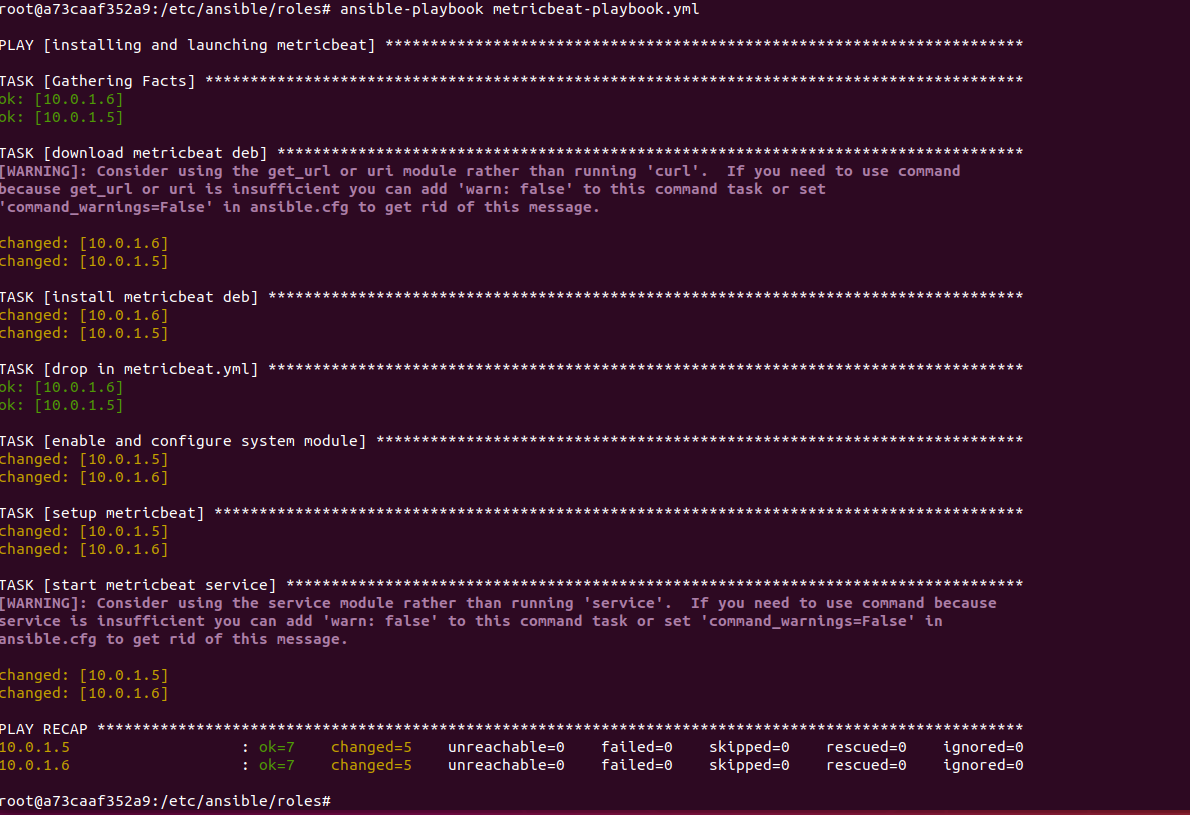
Next navigate to the directory /etc/ansible/roles

**To run the filebeat-playbook.yml**

**ansible-playbook filebeat-playbook.yml**

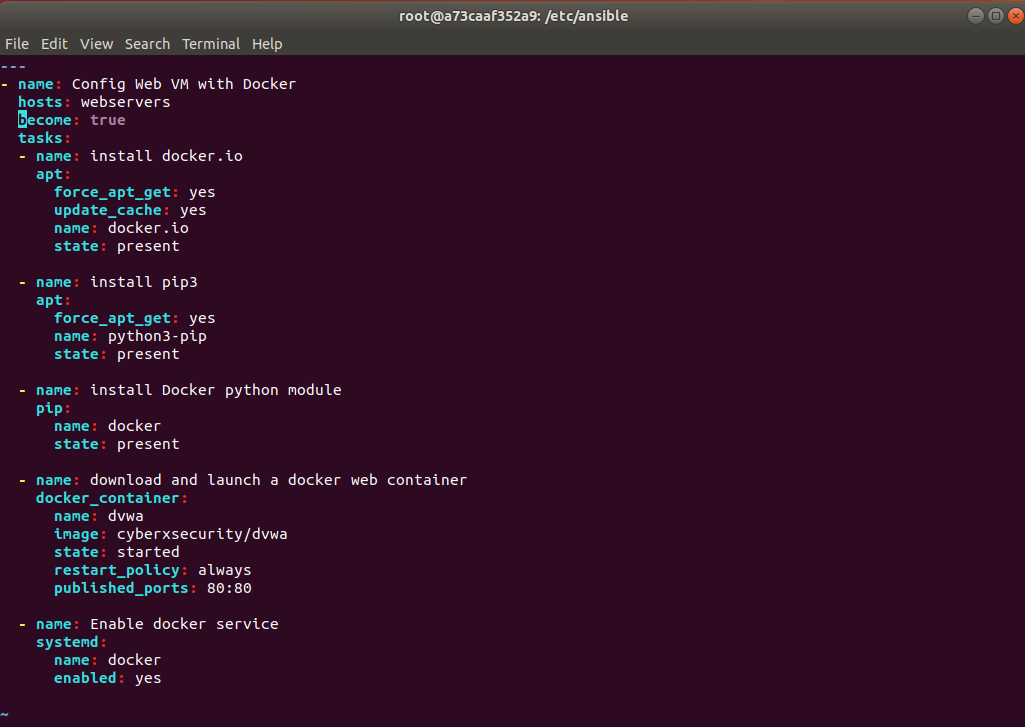


**ansible-playbook metricbeat-playbook.yml**

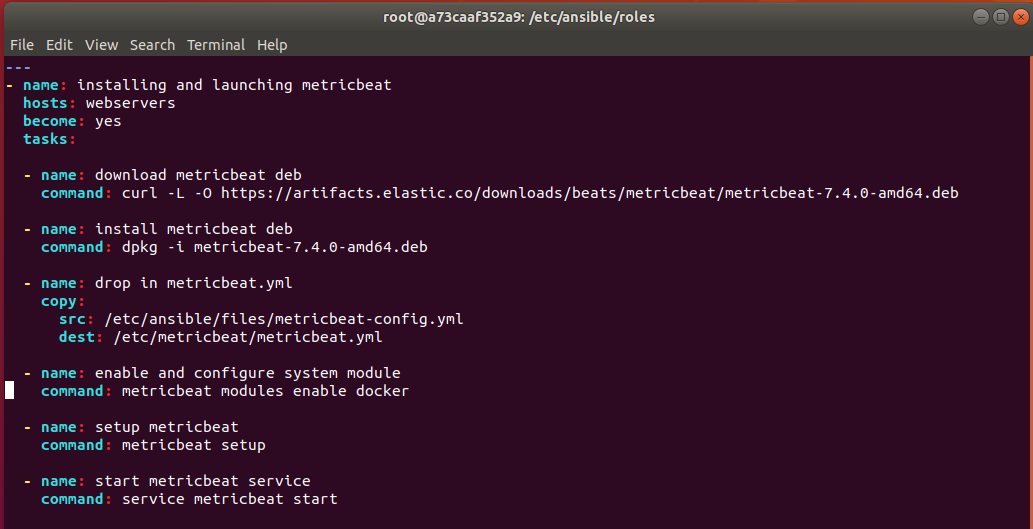


# **Appendix – Playbooks & Host file**

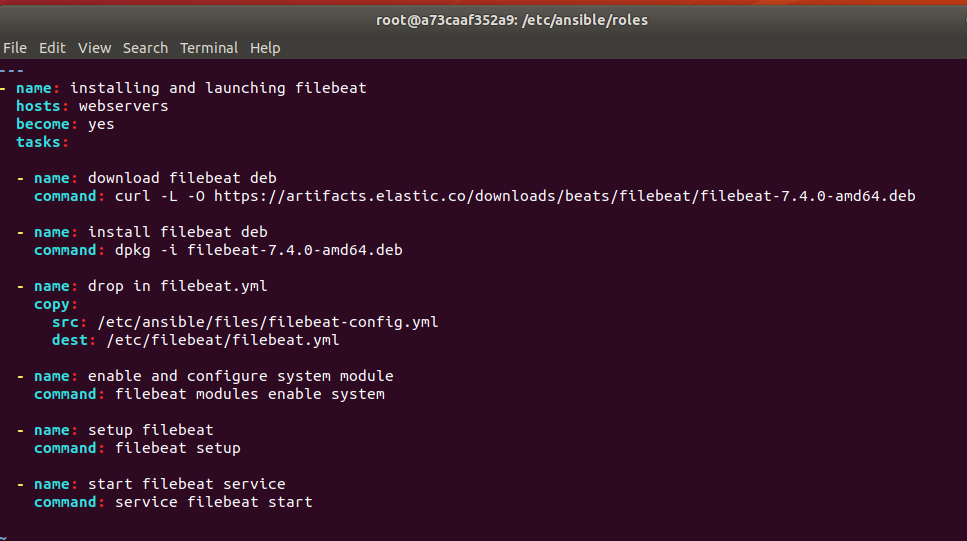
## **my\_playbook.yml**



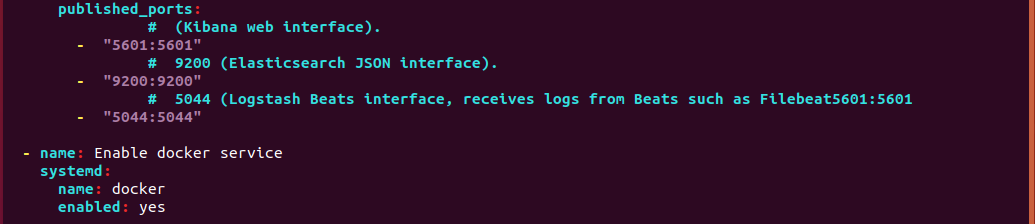
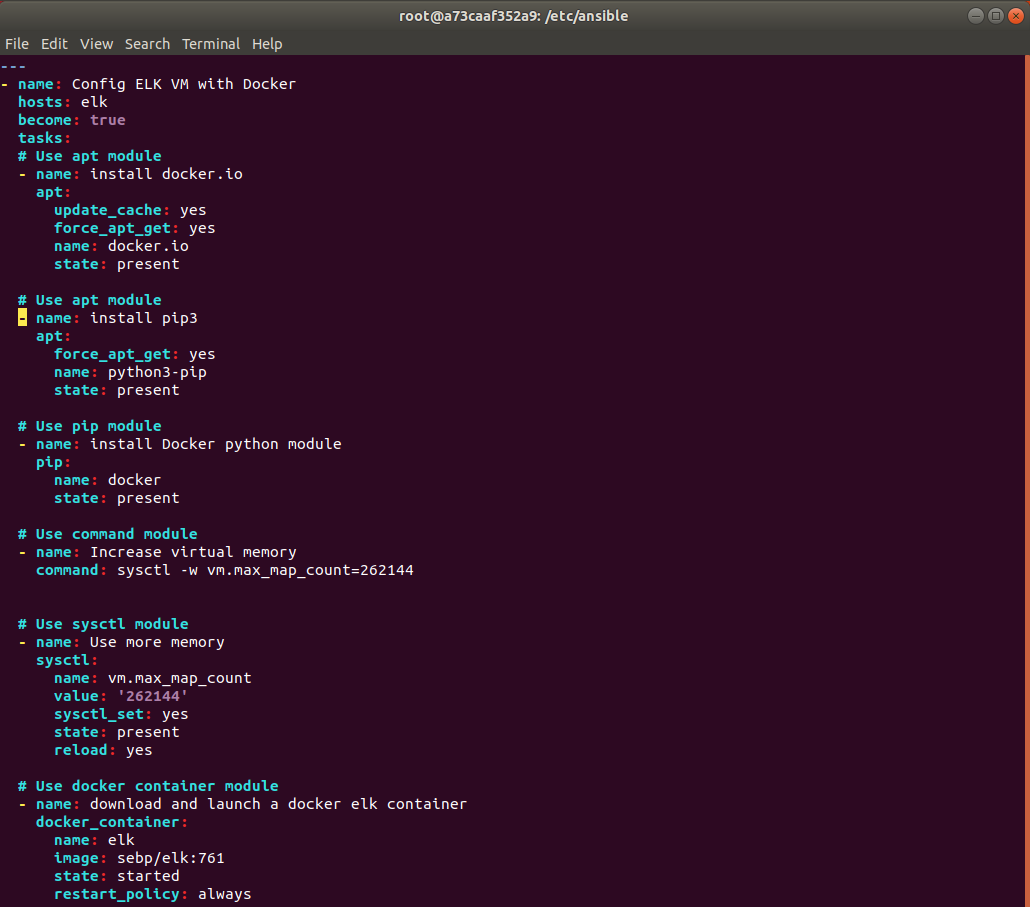
## **metricbeat-playbook.yml**



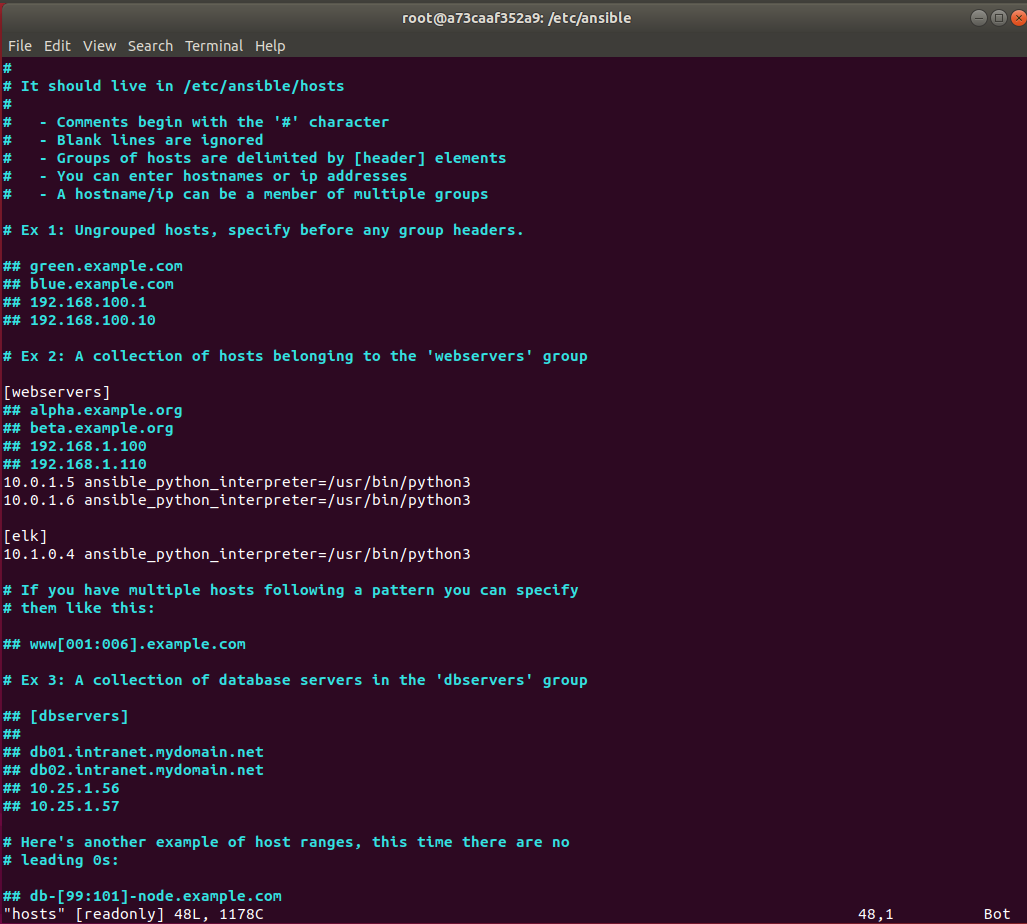
## **filebeat-playbook.yml**



## **my\_elkplaybook.yml**



## **hosts (ansible)**



# **Appendix – Accessing DVWA Website via the Load-Balancer**

