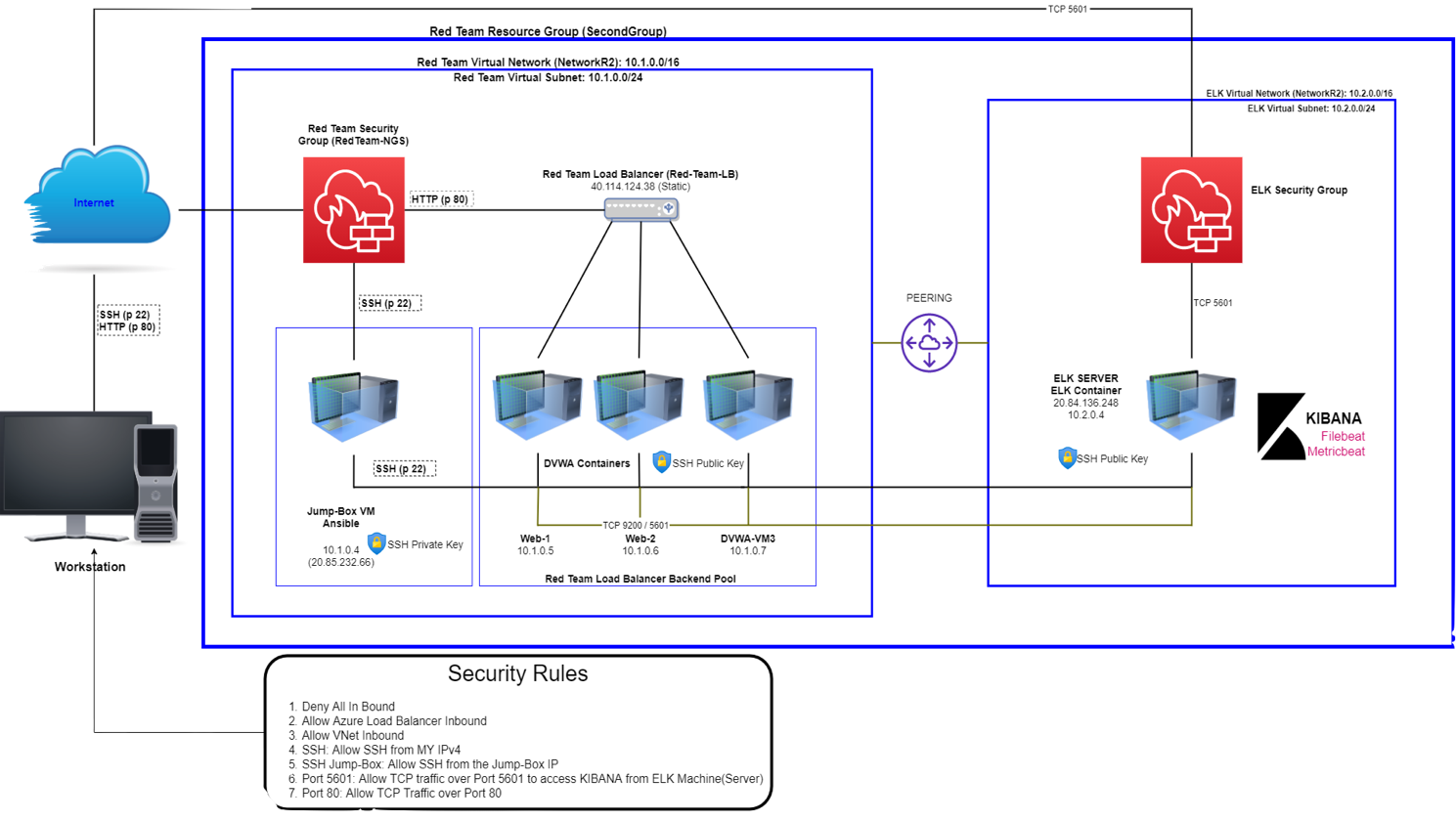
**Automated ELK Stack Deployment**

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



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 **yml and config** file may be used to install only certain pieces of it, such as Filebeat.

* My First Playbook
* Hosts
* Ansible Configuration
* Ansible ELK Installation and VM Configuration
* Filebeat Config
* Filebeat Playbook
* Metricbeat Config
* Metricbeat Playbook

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 **functional and available**, in addition to restricting **traffic** to the network.

* What aspect of security do load balancers protect?
  + **Load balancers add resiliency by rerouting live traffic from one server to another if a server falls prey to a DDoS attack or otherwise becomes unavailable.**
* What is the advantage of a jump box?
  + **A Jump Box Provisioner is also important as it prevents Azure VMs from being exposed via a public IP Address. This allows us to do monitoring and logging on a single box. We can also restrict the IP addresses able to communicate with the Jump Box, as we've done here.**

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

* What does Filebeat watch for?
  + **Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.**
* What does Metricbeat record?
  + **Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.**

The configuration details of each machine may be found below.

| **Name** | **Function** | **IP Address** | **Operating System** |
| --- | --- | --- | --- |
| Jump Box | Gateway | 10.1.0.4 / 20.85.232.66 | Linux |
| Web-1 | UbuntuServer | 10.1.0.5 / 40.114.124.38 | Linux |
| Web-2 | UbuntuServer | 10.1.0.6 / 40.114.124.38 | Linux |
| DVWA-VM3 | UbuntuServer | 10.1.0.7 / 40.114.124.38 | Linux |
| ELKserver | UbuntuServer | 10.2.0.4 / 20.84.136.248 | Linux |

## **Access Policies**

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

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

* **Workstation MY Public IP through TCP 5601.**

Machines within the network can only be accessed by **Workstation and Jump-Box-Provisioner through SSH Jump-Box.**

* Which machine did you allow to access your ELK VM?
  + **Jump-Box-Provisioner IP : 10.1.0.4 via SSH port 22**
* What was its IP address?
  + **Workstation MY Public IP via port TCP 5601**

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

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes | 20.85.232.66 (Workstation IP on SSH 22) |
| Web-1 | No | 10.1.0.4 on SSH 22 |
| Web-2 | No | 10.1.0.4 on SSH 22 |
| DVWA-VM3 | No | 10.1.0.4 on SSH 22 |
| ELKserver | No | Workstation MY Public IP using TCP 5601 |

## **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?
  + **There are multiple advantages, Ansible lets you quickly and easily deploy multitier applications through a YAML playbook.**
  + **You don't need to write custom code to automate your systems.**
  + **Ansible will also figure out how to get your systems to the state you want them to be in.**

The playbook implements the following tasks:

* In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.
  + Specify a different group of machines:

- name: Config elk VM with Docker

hosts: elk

become: true

tasks:

* + Install Docker.io

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker.io

state: present

* + Install Python-pip

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

`docker`, which is the Docker Python pip module.

* + Increase Virtual Memory

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: '262144'

state: present

reload: yes

* + Download and Launch ELK Docker Container (image sebp/elk)

- name: Download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

* + Published ports 5044, 5601 and 9200 were made available

published\_ports:

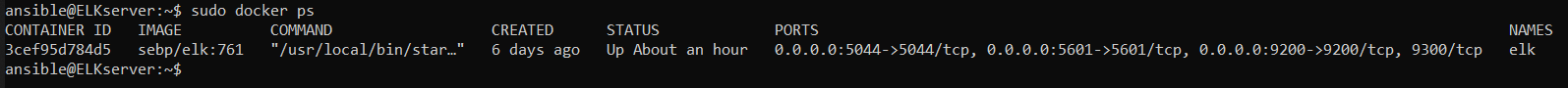
- 5601:5601

- 9200:9200

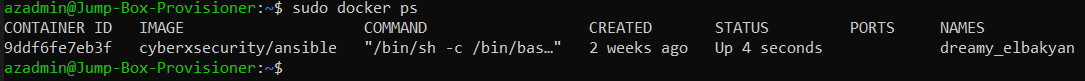
- 5044:5044

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

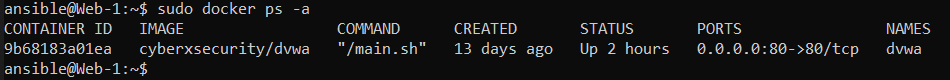
**ELKserver**



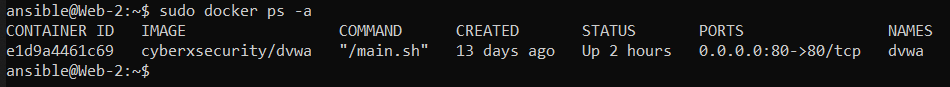
**Jump-Box-Provisioner**



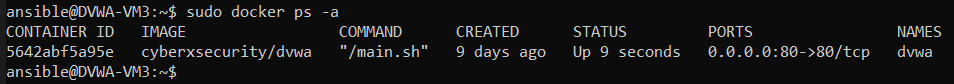
**Web-1**



## **Web-2**



## **DVWA-VM3**



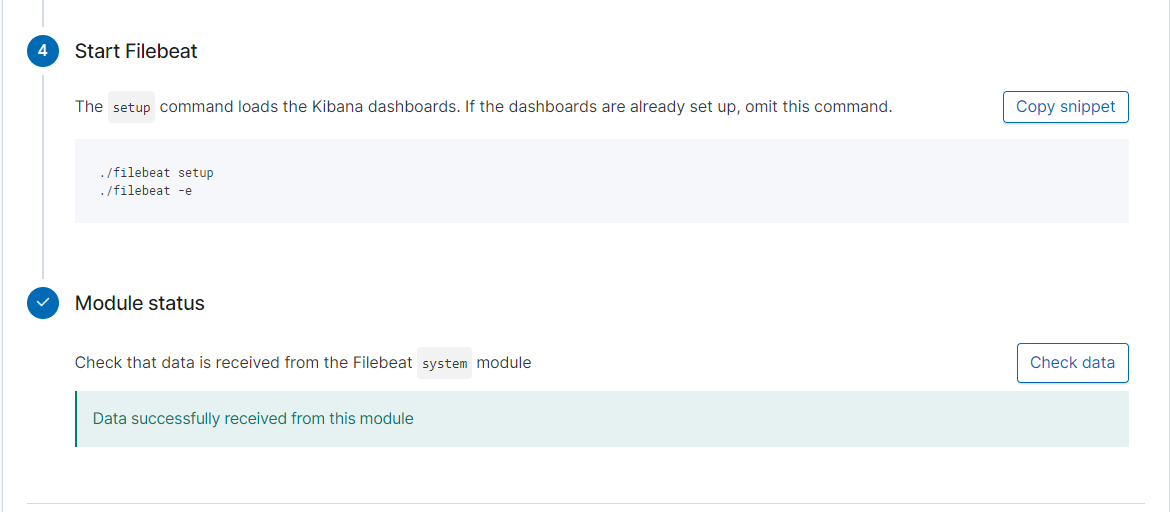
## **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

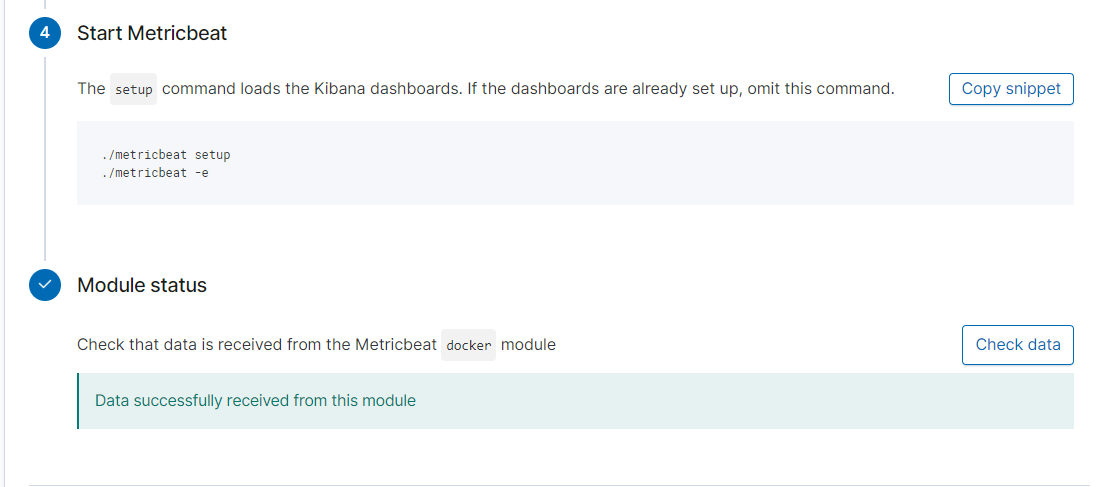
* List the IP addresses of the machines you are monitoring
  + Web-1: 10.1.0.5
  + Web-2: 10.1.0.6
  + DVWA-VM3: 10.1.0.7

We have installed the following Beats on these machines:

* Filebeat
  + Filebeat Module Status Screenshot

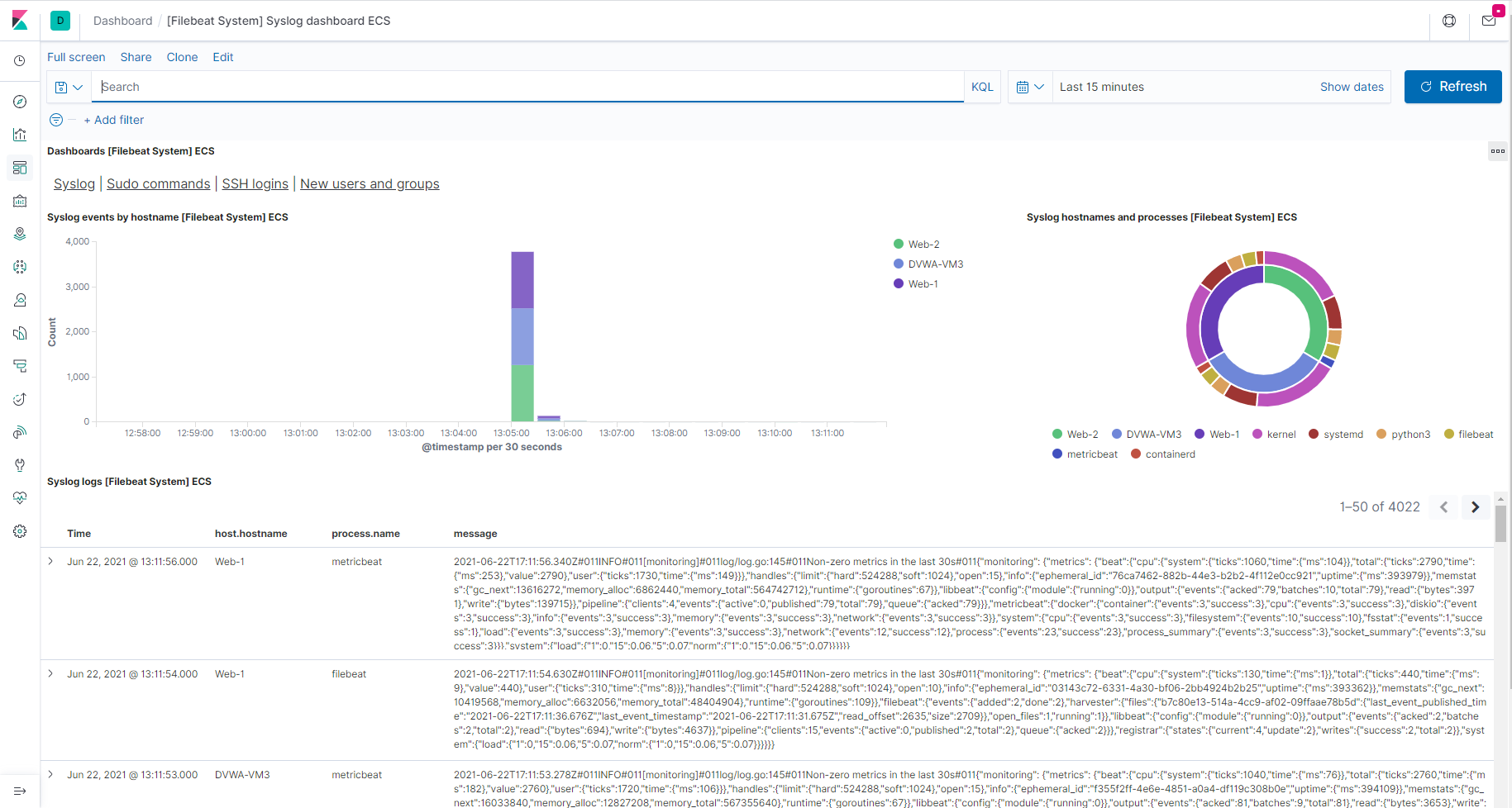


* Metricbeat
  + Metricbeat Module Status Screenshot

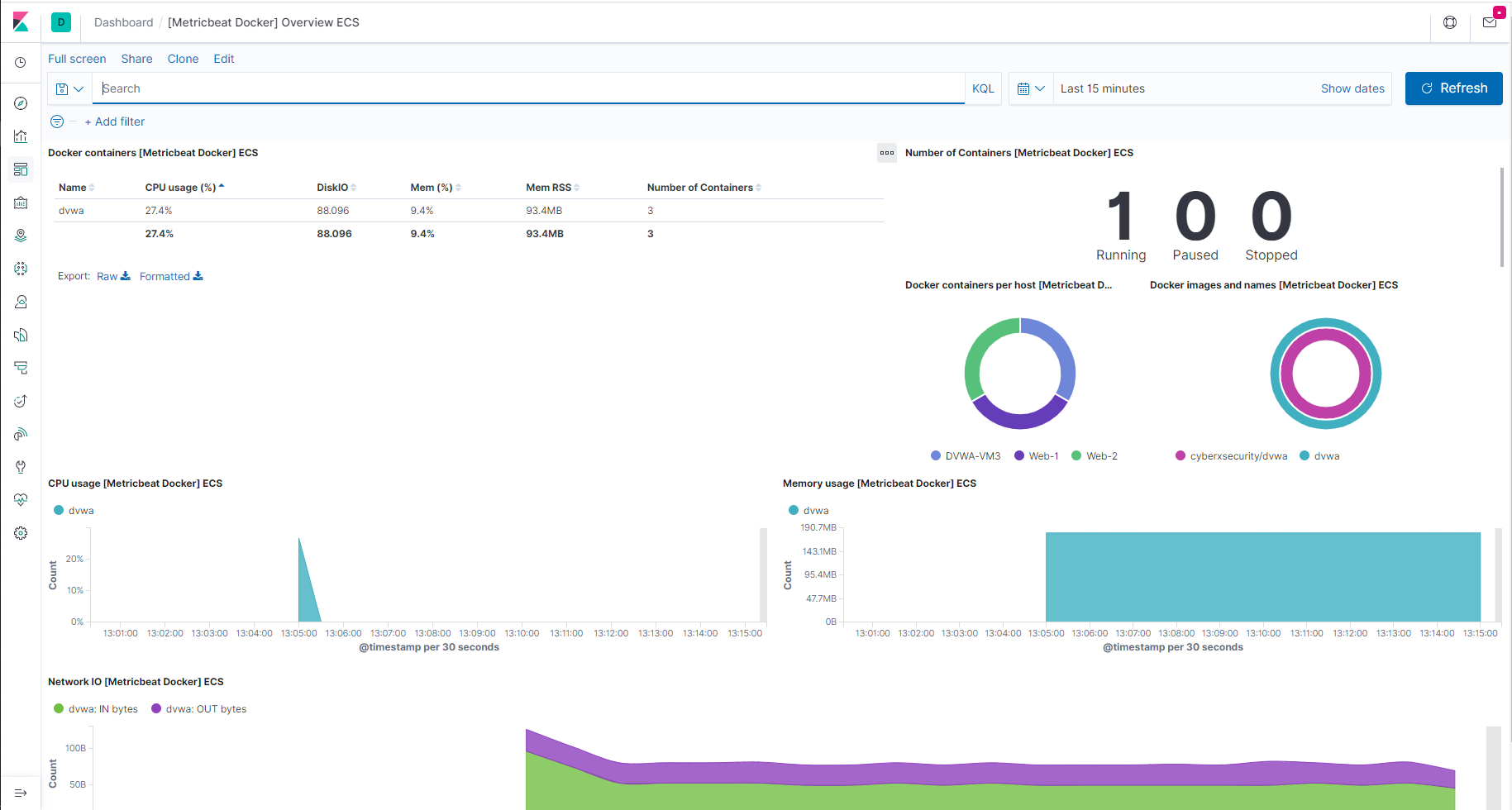


These Beats allow us to collect the following information from each machine:

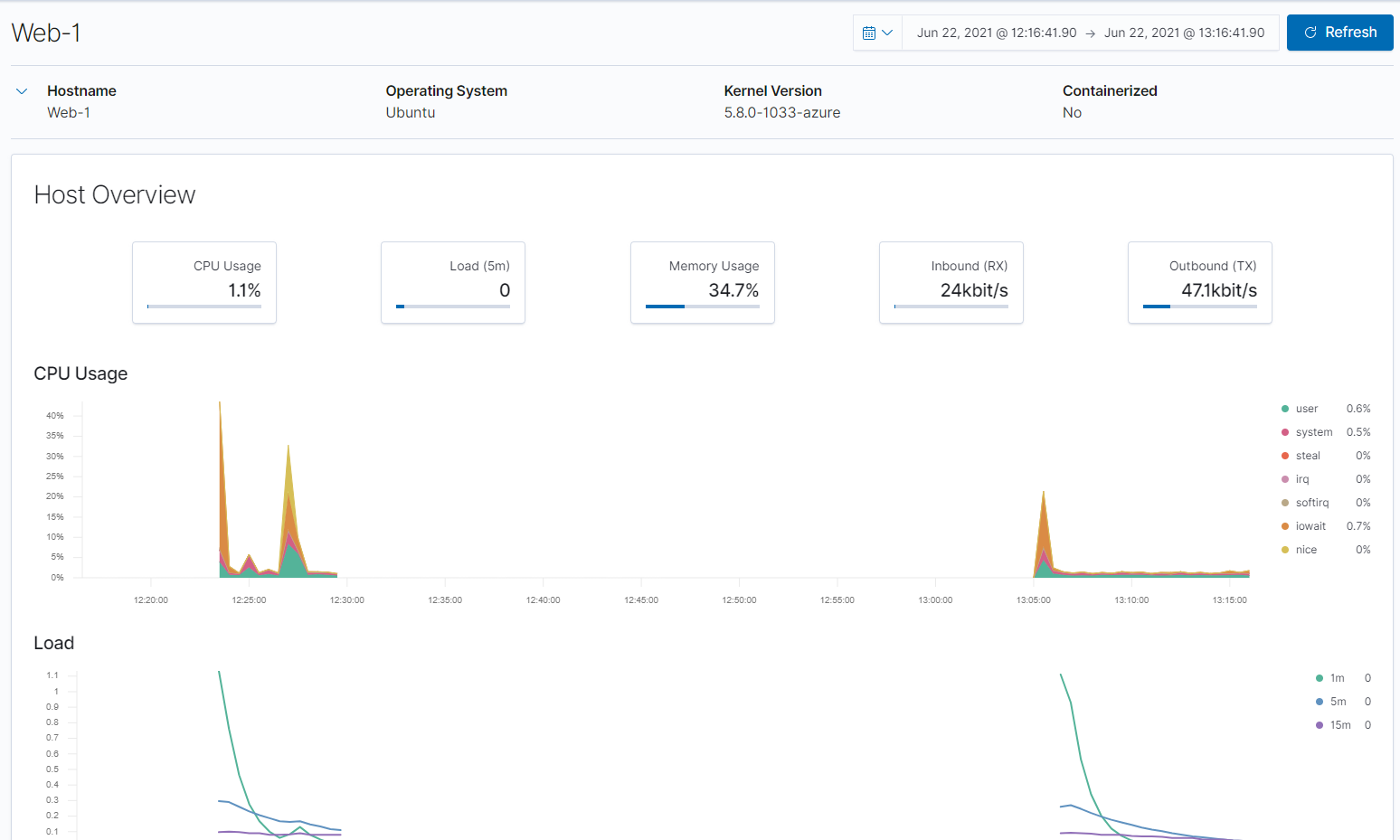
* Filebeat will be used to collect log files from very specific files such as Apache, Microsft Azure tools and web servers, MySQL databases.
  + Filebeat Module Kibana Dashboard Screenshot



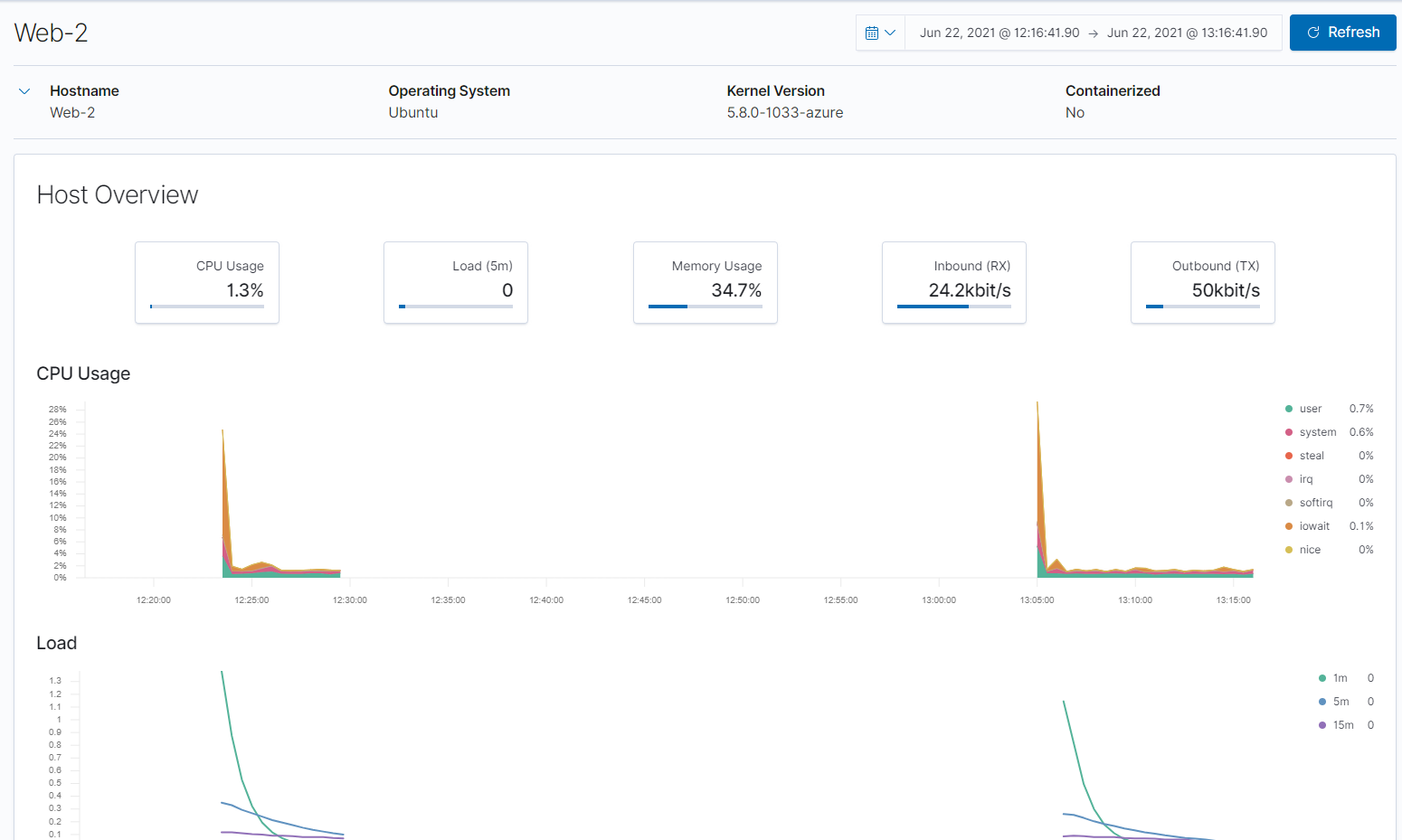
* Metericbeat will be used to monitor VM stats, per CPU core stats, per filesystem stats, memory stats and network stats.
  + Metricbeat Module Kibana - Metricbeat Docker Overview ECS Dashboard

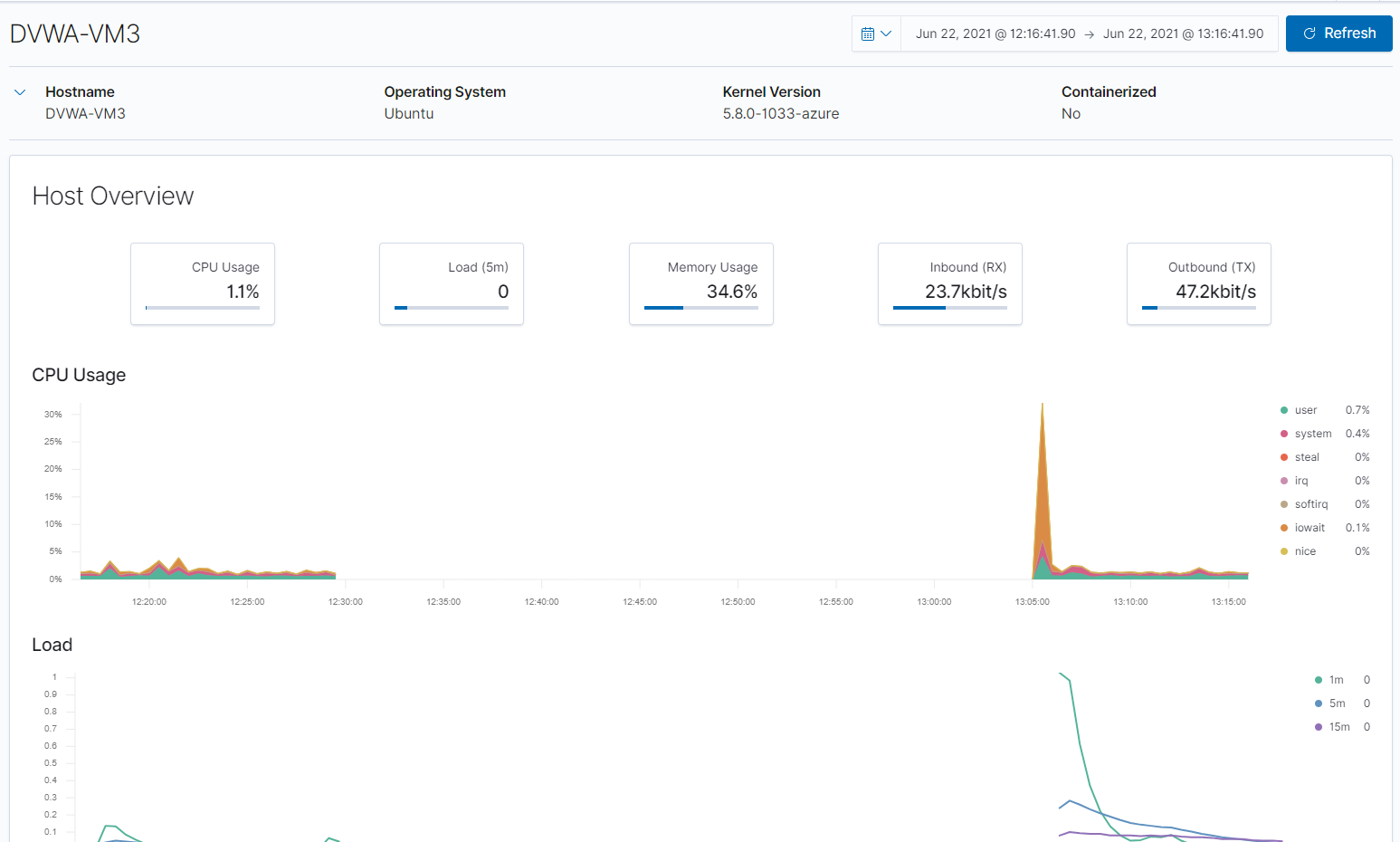


* + - Metricbeat Module Kibana - Metricbeat Docker Web-1 metrics



* + - Metricbeat Module Kibana - Metricbeat Docker Web-2 metrics



* + - Metricbeat Module Kibana - Metricbeat Docker DVWA-VM3 metrics
* 

## **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:

* Verify the Public IP address to see if it has changed. [What Is My IP?](https://www.whatismyip.com/)
* If changed then update the Security Rules that uses the My Public IPv4

SSH into the control node and follow the steps below:

* Copy the **yml** file to **ansible folder.**
* Update the **config** file to include **remote users and ports.**
* Run the playbook, and navigate to **Kibana ((Your IP Address):5601)** to check that the installation worked as expected.

### **For ELK VM Configuration:**

* Copy the ELK Installation and VM Configuration
* Run the playbook using this command : ansible-playbook /etc/ansible/install-elk.yml

### **For Filebeat**

* Download Filebeat playbook usng this command:
  + curl -L -O https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/filebeat-config.yml
* Copy the **Filebeat Config** file to **/etc/ansible**
* Update the **filebeat-config.yml** file to include the **ELK private IP 10.2.0.4** as below from root@9ddf6fe7eb3f:~# nano /etc/ansible/filebeat-config.yml

output.elasticsearch:

# Boolean flag to enable or disable the output module.

#enabled: true

# Array of hosts to connect to.

# Scheme and port can be left out and will be set to the default (http and 9200)

# In case you specify and additional path, the scheme is required: http://localhost:9200/path

# IPv6 addresses should always be defined as: https://[2001:db8::1]:9200

hosts: ["10.2.0.4:9200"]

username: "elastic"

password: "changeme" # TODO: Change this to the password you set

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.

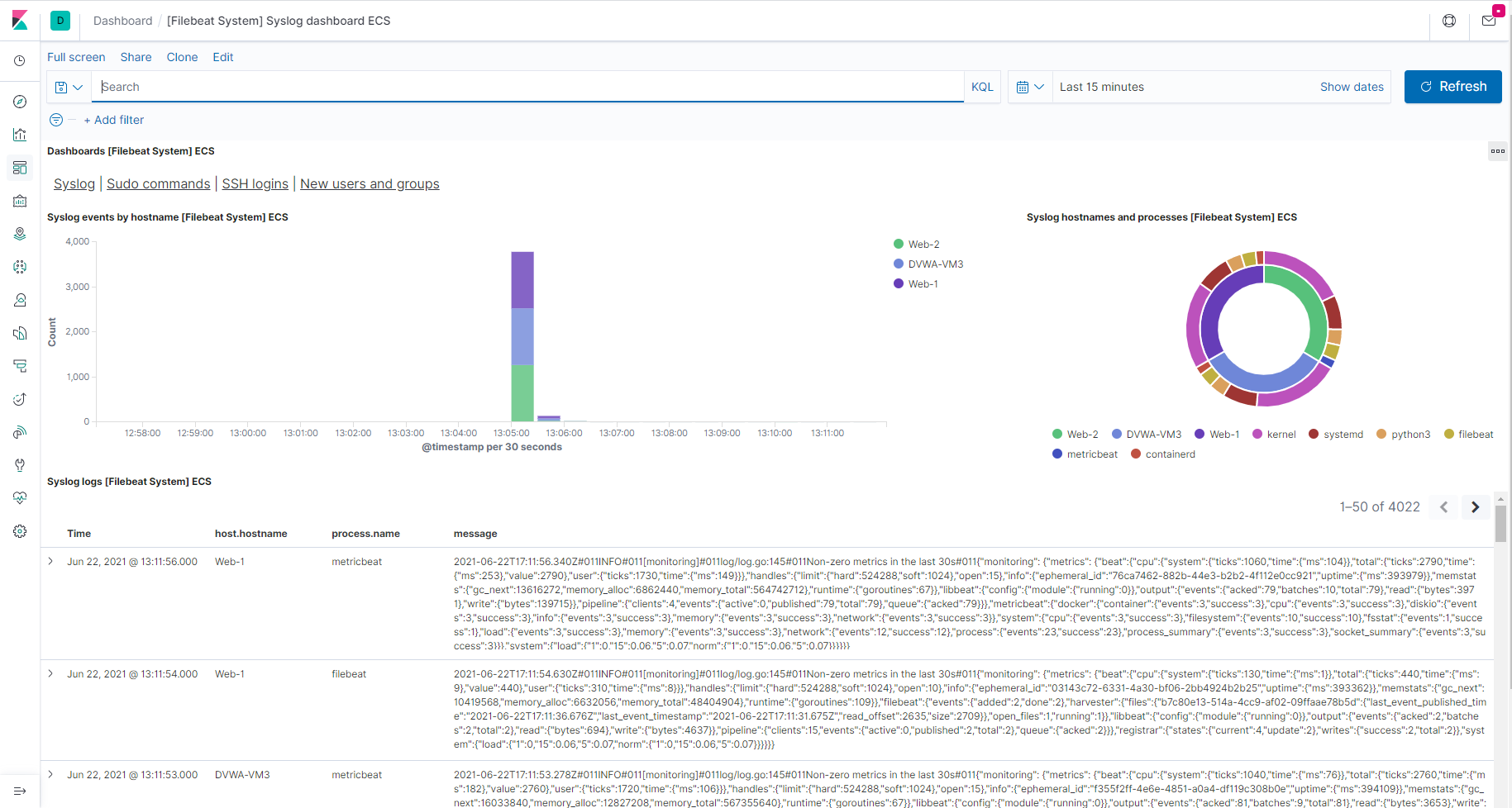
# This requires a Kibana endpoint configuration.

setup.kibana:

host: "10.2.0.4:5601"

# TODO: Change this to the IP address of your ELK server

* Run the playbook using this command ansible-playbook filebeat-playbook.yml and navigate to [Kibana](http://20.84.136.248:5601/app/kibana) > Logs : Add log data > System logs (DEB) > 5:Module Status > Check Incoming data on Kibana to check that the installation worked as expected.
  + Filebeat Module Kibana Dashboard Screenshot



### **For Metricbeat**

* Download Metricbeat playbook using this command:
  + curl -L -O https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e744c54513616966affb5e9d96f5e12f73/metricbeat > /etc/ansible/files/metricbeat-config.yml Copy the **Metricbeat Config** file to **/etc/ansible**
* Update the **metricbeat-config.yml** file to include the **ELK private IP 10.2.0.4** as below from root@9ddf6fe7eb3f:~# nano /etc/ansible/metricbeat-config.yml

#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.

# This requires a Kibana endpoint configuration.

setup.kibana:

host: "10.2.0.4:5601"

#-------------------------- Elasticsearch output ------------------------------

output.elasticsearch:

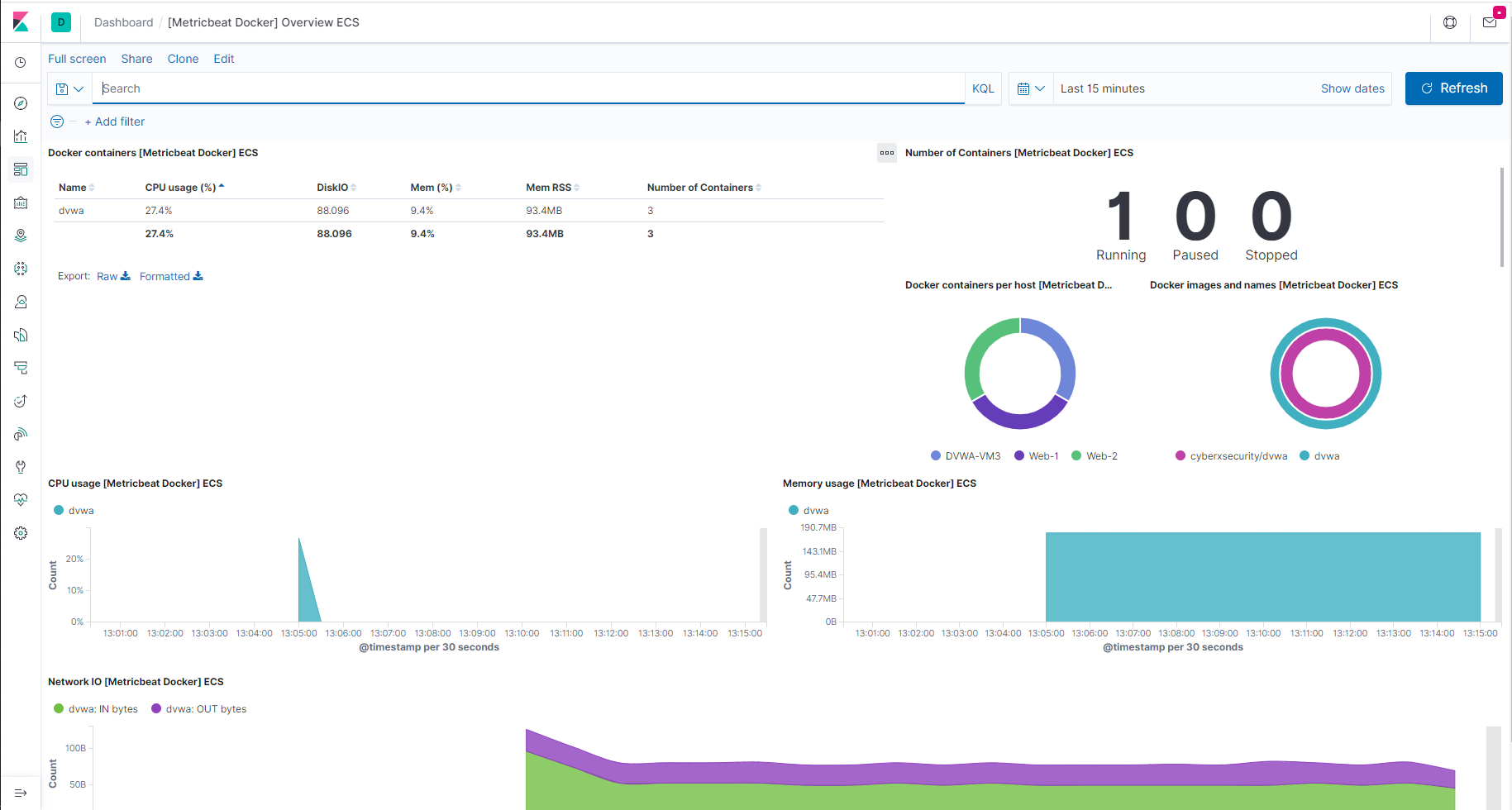
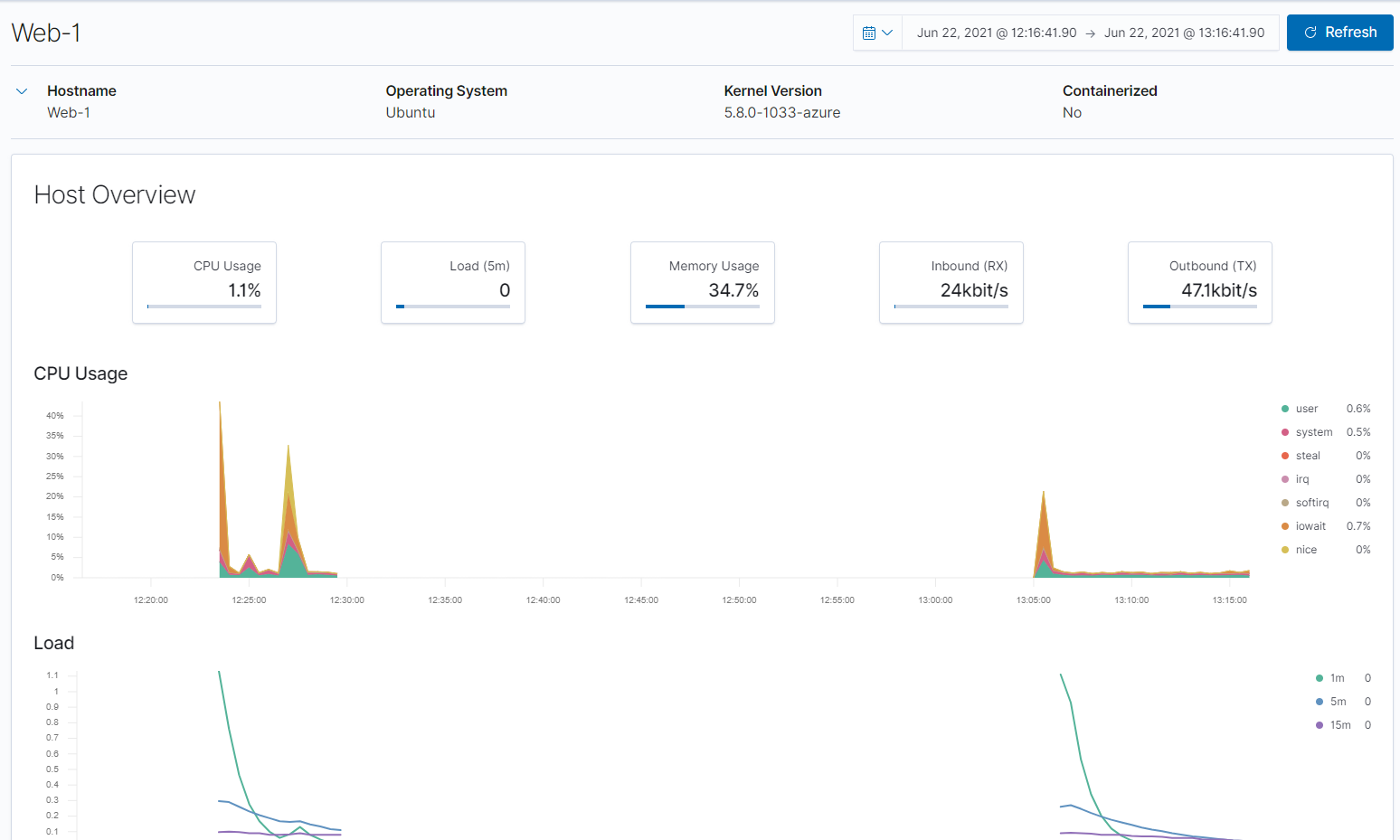
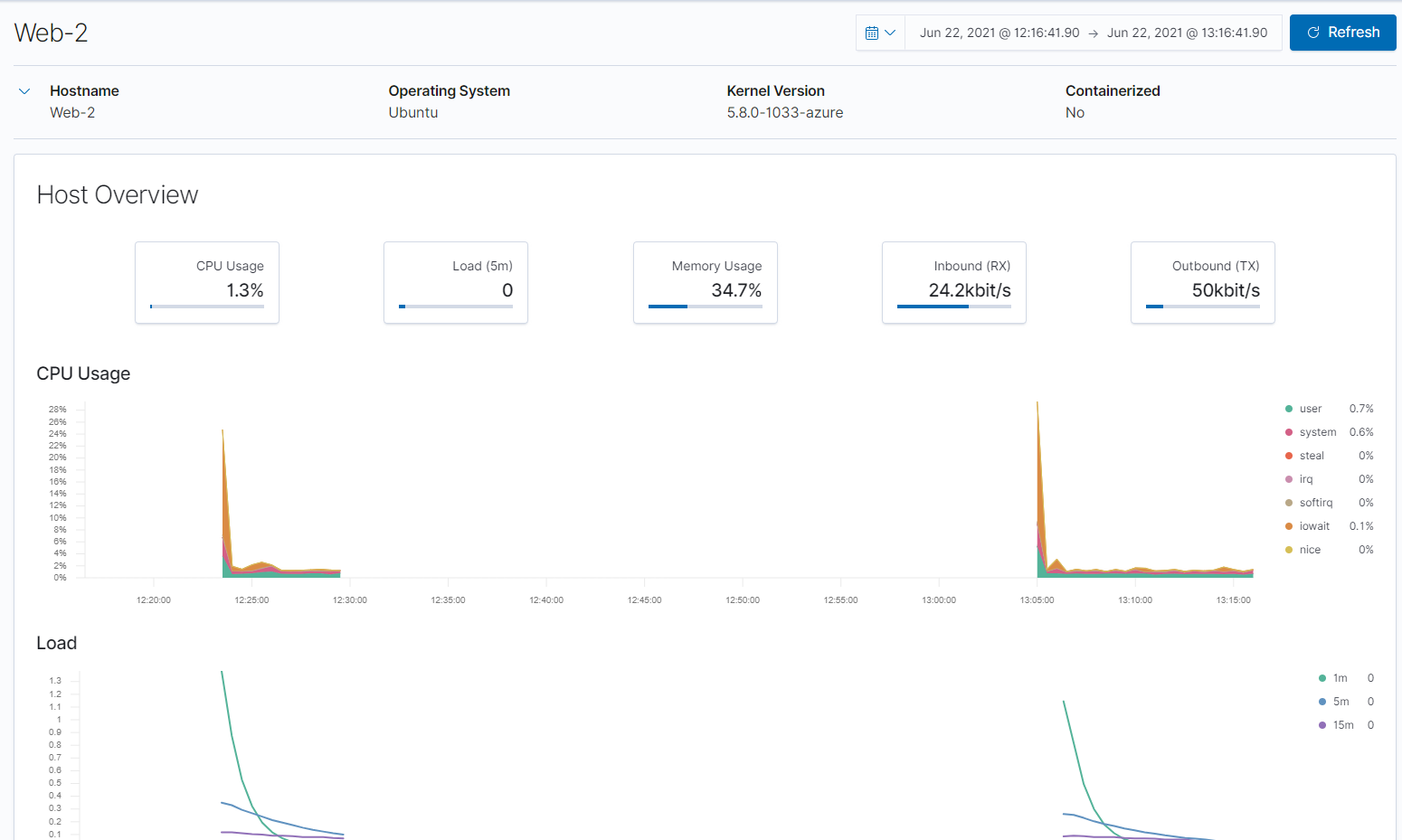
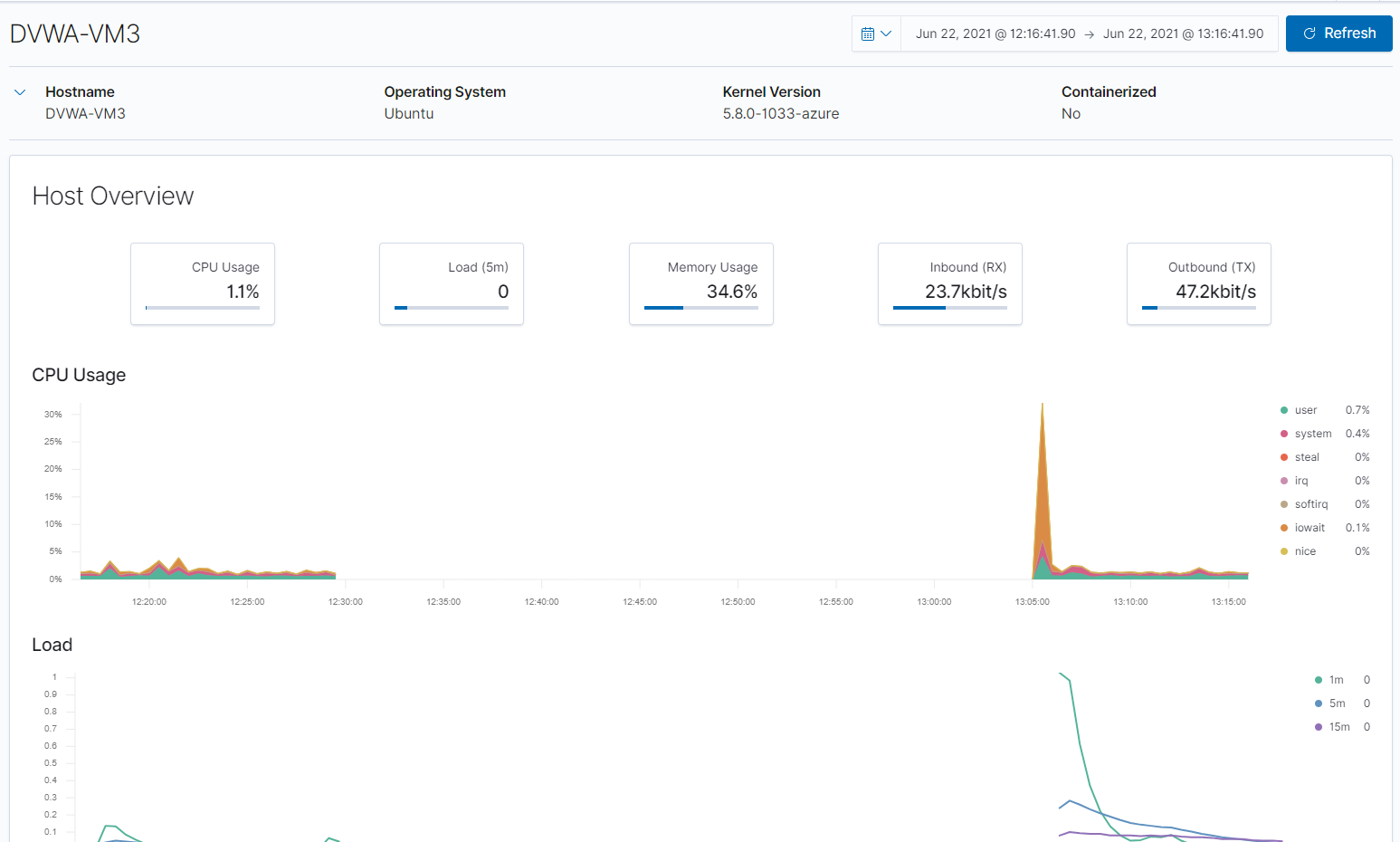
# TODO: Change the hosts IP address to the IP address of your ELK server

# TODO: Change password from `changem` to the password you created

hosts: ["10.2.0.4:9200"]

username: "elastic"

password: "changeme"

* Run the playbook using this command ansible-playbook metricbeat-playbook.yml and navigate to [Kibana](http://20.84.136.248:5601/app/kibana) > Logs : Add Metric data > Docker Metrics (DEB) > 5:Module Status > Check data\_on Kibana to check that the installation worked as expected.
  + [Metricbeat Module Kibana - Metricbeat Docker Overview ECS Dashboard](https://github.com/karma-786/ELK-Stack-Deployment-Project/blob/main/Diagrams/Images/ELK_VM_Configuration_Screenshots/Metricbeat_Docker_Overview_ECS_dashboard.PNG)
* 
  + - [Metricbeat Module Kibana - Metricbeat Docker Web-1 metrics](https://github.com/karma-786/ELK-Stack-Deployment-Project/blob/main/Diagrams/Images/ELK_VM_Configuration_Screenshots/Metricbeat_Docker_Web-1_metrics.PNG)
* 
  + - [Metricbeat Module Kibana - Metricbeat Docker Web-2 metrics](https://github.com/karma-786/ELK-Stack-Deployment-Project/blob/main/Diagrams/Images/ELK_VM_Configuration_Screenshots/Metricbeat_Docker_Web-2_metrics.PNG)
* 
  + - [Metricbeat Module Kibana - Metricbeat Docker DVWA-VM3 metrics](https://github.com/karma-786/ELK-Stack-Deployment-Project/blob/main/Diagrams/Images/ELK_VM_Configuration_Screenshots/Metricbeat_Docker_DVWA-VM3_metrics.PNG)
* 

### **Install Filebeat onto VM's**

1. Login to Kibana > Logs : Add log data > System logs > DEB > Getting started
2. Copy: curl -L -O <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb>  
   (Download the Filebeat to the VM)

### **Install Metricbeat onto VM's**

1. Login to Kibana > Add Metric Data > Docker Metrics > DEB > Getting Started
2. Copy: curl -L -O <https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb>  
   (Download the Metricbeat to the VM)

* Answer the following questions to fill in the blanks:
* Which file is the playbook?
  + For Ansible create **My First Playbook**
  + For Filebeat create **Filebeat Playbook**
  + For Metricbeat create **Metricbeat Playbook** - Where do you copy it?
  + **/etc/ansible/**
* Which file do you update to make Ansible run the playbook on a specific machine?
  + **/etc/ansible/hosts file (IP of the Virtual Machines).**
* How do I specify which machine to install the ELK server on versus which to install Filebeat on?
  + **I have specified two separate groups in the etc/ansible/hosts file. One of the group will be webservers which has the IPs of the 3 VMs that I will install Filebeat to. The other group is named ELKserver which will have the IP of the VM I will install ELK to.**
* Which URL do you navigate to in order to check that the ELK server is running?
  + [***http://20.84.136.248:5601//app/kibana***](http://20.84.136.248:5601//app/kibana)

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

* The specific commands the user will need to run in order to download the playbook and configuration files, update the files, etc:

| **COMMAND** | **PURPOSE** |
| --- | --- |
| ssh-keygen | create a ssh key for setup VM's |
| sudo cat .ssh/id\_rsa.pub | to view the ssh public key |
| ssh azadmin@Jump-Box-Provisioner IP address | to log into the Jump-Box-Provisioner |
| sudo docker container list -a | list all docker containers |
| sudo docker start dremy\_elbakyan | start docker container dremy\_elbakyan |
| sudo docker ps -a | list all active/inactive containers |
| sudo docker attach dremy\_elbakyan | effectively sshing into the dremy\_elbakyan container |
| cd /etc/ansible | Change directory to the Ansible directory |
| ls -laA | List all file in directory (including hidden) |
| nano /etc/ansible/hosts | to edit the hosts file |
| nano /etc/ansible/ansible.cfg | to edit the ansible.cfg file |
| nano /etc/ansible/pentest.yml | to edit the My-Playbook |
| ansible-playbook [location][filename] | to run the playbook |
| sudo lsof /var/lib/dpkg/lock-frontend | unlocking a locked file |
| ssh ansible@Web-1 IP address | to log into the Web-1 VM |
| ssh ansible@Web-2 IP address | to log into the Web-2 VM |
| ssh ansible@DVWA-VM3 IP address | to log into the DVWA-VM3 VM |
| ssh ansible@ELKserver IP address | to log into the ELKserver VM |
| exit | to exit out of docker containers/Jump-Box-Provisioners |
| nano /etc/ansible/ansible.cfg | to edit the ansible.cfg file |
| nano /etc/ansible/hosts | to edit the hosts file |
| nano /etc/ansible/pentest.yml | to edit the My-Playbook |
| ansible-playbook [location][filename] | to run the playbook |
| sudo apt-get update | this will update all packages |
| sudo apt install docker.io | install docker application |
| sudo service docker start | start the docker application |
| sudo systemctl status docker | status of the docker application |
| sudo systemctl start docker | start the docker service |
| sudo docker pull cyberxsecurity/ansible | pull the docker container file |
| sudo docker run -ti cyberxsecurity/ansible bash | run and create a docker container image |
| ansible -m ping all | check the connection of ansible containers |
| curl -L -O [location of the file on the web] | to download a file from the web |
| dpkg -i [filename] | to install the file i.e. (filebeat & metricbeat) |
| http://20.84.136.248:5601//app/kibana | Open web browser and navigate to Kibana Logs |
| nano filebeat-config.yml | create and edit filebeat config file |
| nano filebeat-playbook.yml | write YAML file to install filebeat on webservers |
| nano metricbeat-config.yml | create metricbeat config file and edit it |
| nano metricbeat-playbook.yml | write YAML file to install metricbeat on webservers |

### Sites Used for References and Knowledge for the Project

* [Elastic: The Elastic Stack.](https://www.elastic.co/elastic-stack)
* [Elastic: Filebeat.](https://www.elastic.co/beats/filebeat)
* [ELK Docker Documentation.](https://elk-docker.readthedocs.io/)
* [Microsoft Azure: Global vNet Peering](https://azure.microsoft.com/en-ca/blog/global-vnet-peering-now-generally-available/)
* [Microsoft Docs: How to open a support ticket](https://docs.microsoft.com/en-us/azure/azure-portal/supportability/how-to-create-azure-support-request)
* [Peachpit.com: Split-Half Search](https://www.peachpit.com/articles/article.aspx?p=420908&seqNum=3)
* [Elastic: Filebeat Container Documentation](https://www.elastic.co/beats/filebeat)
* [Phoenixnap.com: Docker Commands Cheat Sheet](https://phoenixnap.com/kb/list-of-docker-commands-cheat-sheet)
* [Docker and Ansible Cloud Week Cheat Sheet](https://www.bogotobogo.com/DevOps/Docker/Docker-Cheat-Sheet.php)
* [Ansible: Roles Playbook Reuse Roles](https://docs.ansible.com/ansible/latest/user_guide/playbooks_reuse_roles.html)
* [Elastic: Getting Started with the Elastic Stack](https://www.elastic.co/guide/en/elastic-stack-get-started/current/get-started-elastic-stack.html)