**Project – 1**

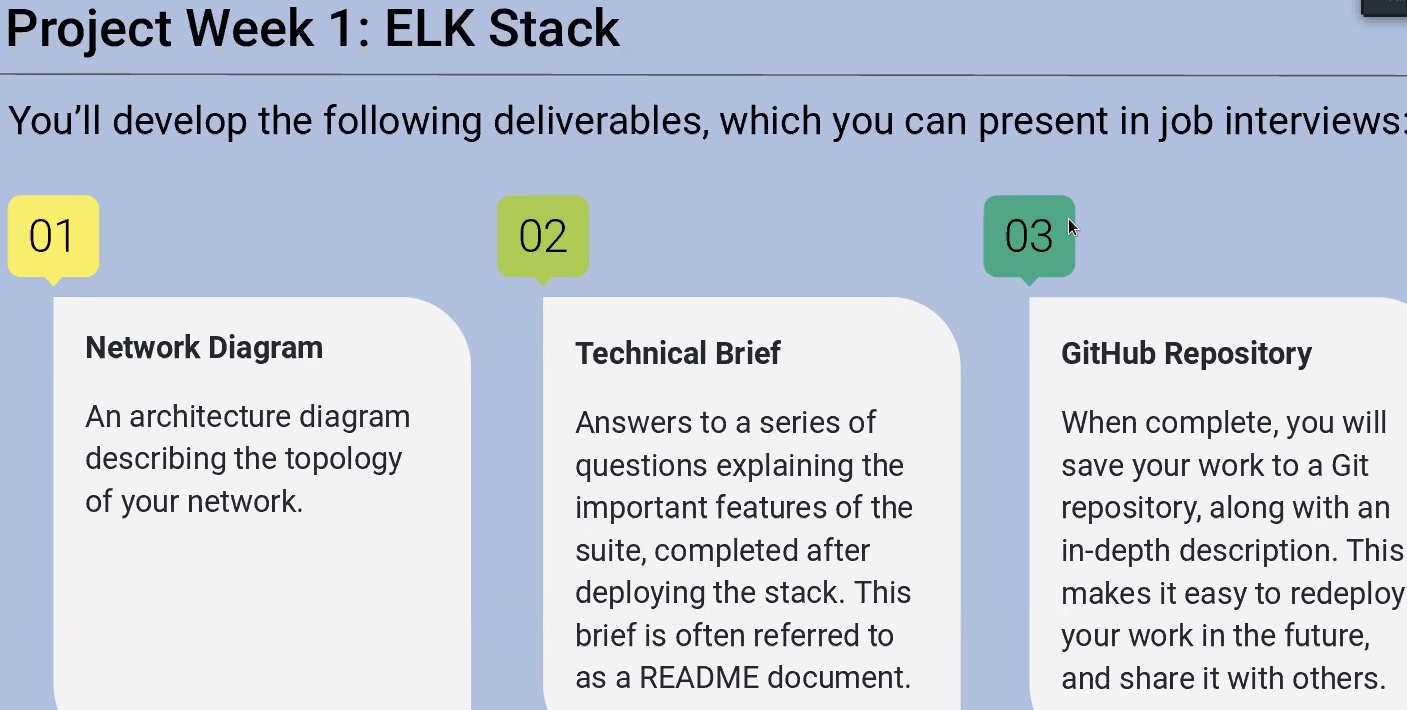
***Building ELK (Elastic-Search, LogStash, Kibana) Stack in-the-Cloud***

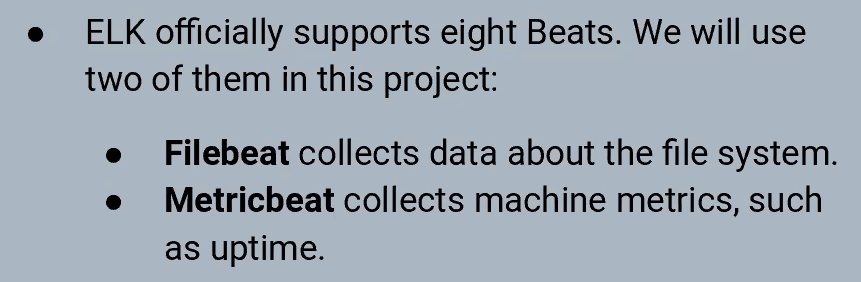
*Identification, Detection, Logging, Monitoring, Protection, Response*

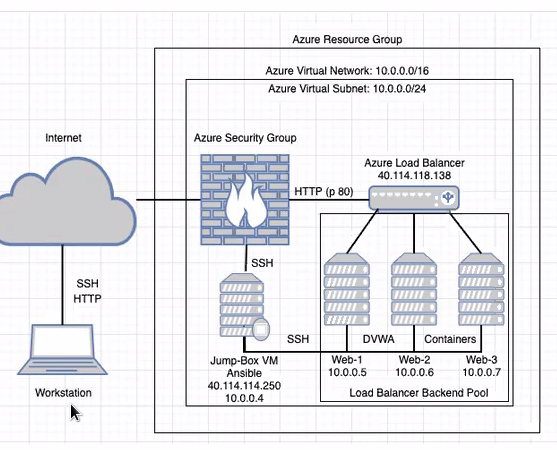
SIEM tools ~ Slugworks, Summologic,

Keep logs for at least 3 years ~ help non-repudiation, monitor networks, do ad-hoc querying etc.

1. Building a new Availability Zone (VM)
2. Spinning-up ELK gathering telemetry
3. Generating Events ~ sent from Agent to the ELK server
4. Demonstrate achievement (individual) ~ a tangible achievement





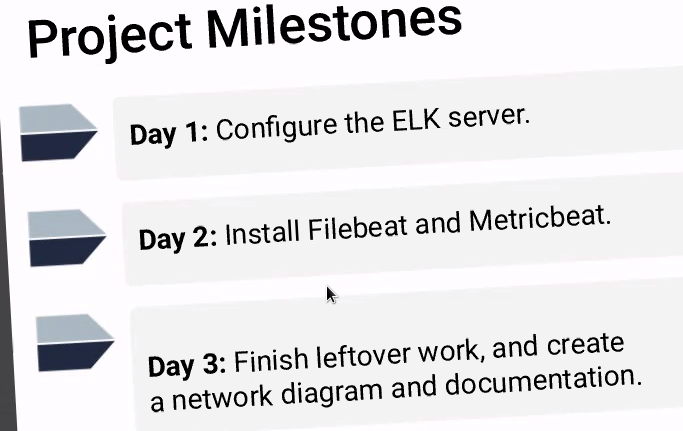


Single NSG -

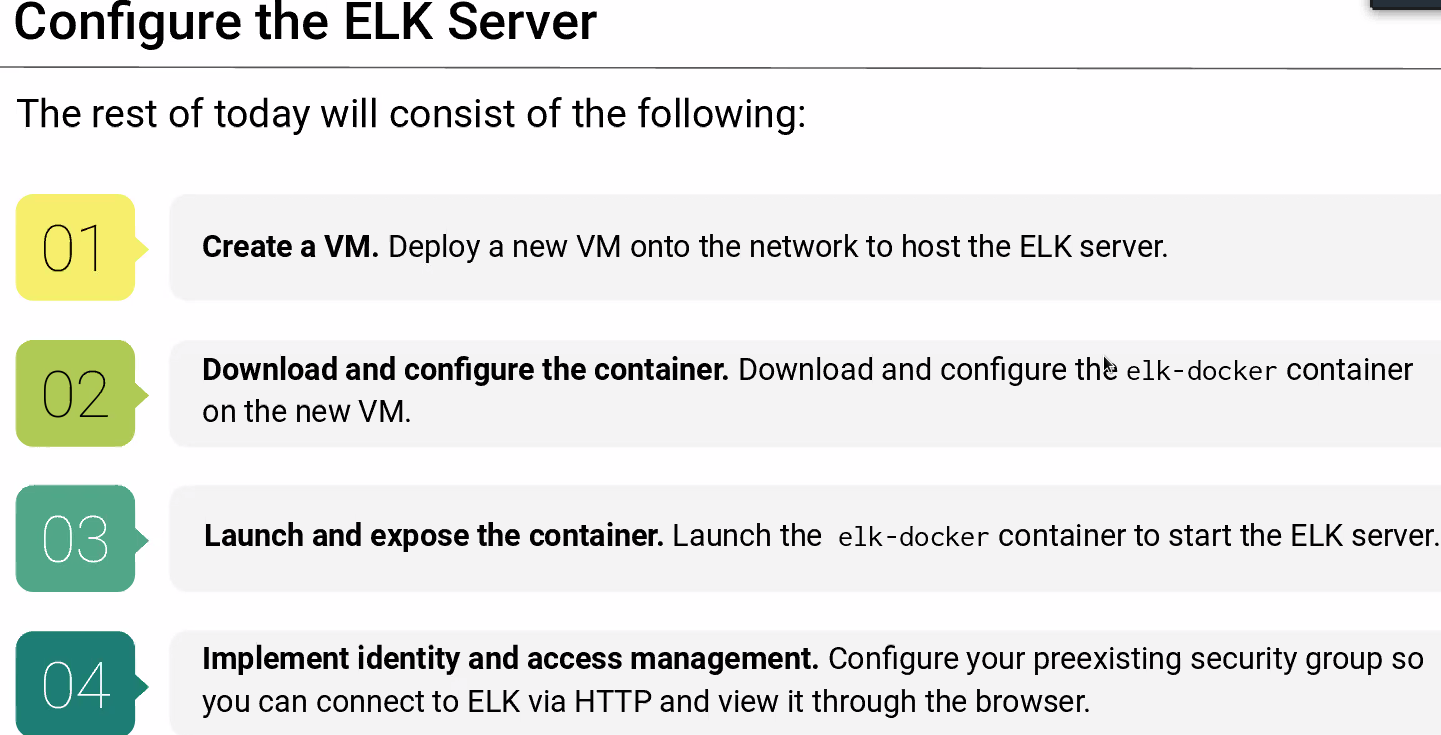
*Azure does not allow more than 4 CPU’s installed in a Single region*

For ELK - Separate ENV in a +Separate Geographical region

We need a separate network ~ 2 dual-core processors; 8GB RAM; (Very resource intensive)



Monitor all the traffic on the WebVM’s since they are exposed to the Internet



**\*\* when you deploy ELK VM - Do Not deploy with less than 2 CPU’s (2 CPU minimum) and less than 4GB RAM’s (8GB is recommended)**

**Port TCP 5901 – ELK listens on (Not Port 80!!)**

***Entitlements, Identity and Governance ~ SalePoint (very popular)***

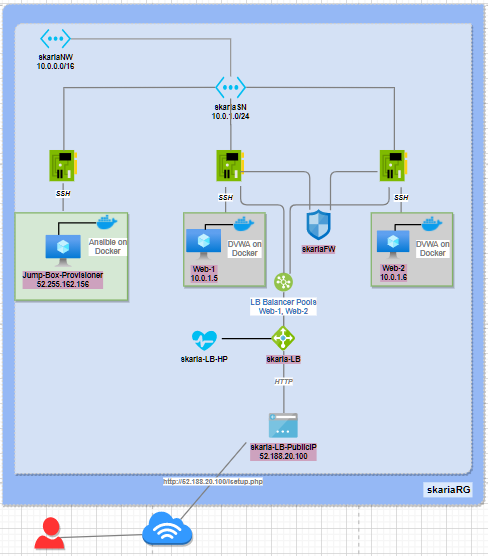
104.210.15.174

Public IP For new VM

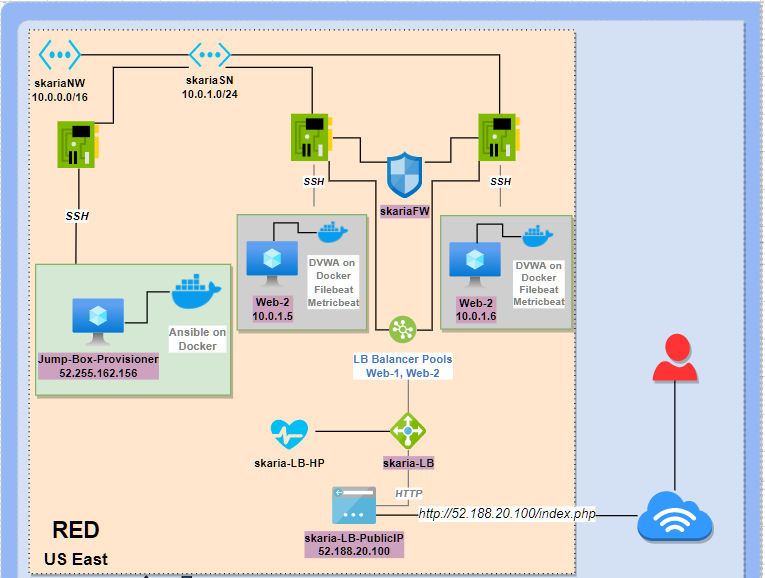
[sysctl - Manage entries in sysctl.conf. — Ansible Documentation](https://docs.ansible.com/ansible/2.5/modules/sysctl_module.html)

[elk-docker (elk-docker.readthedocs.io)](https://elk-docker.readthedocs.io/#installation)

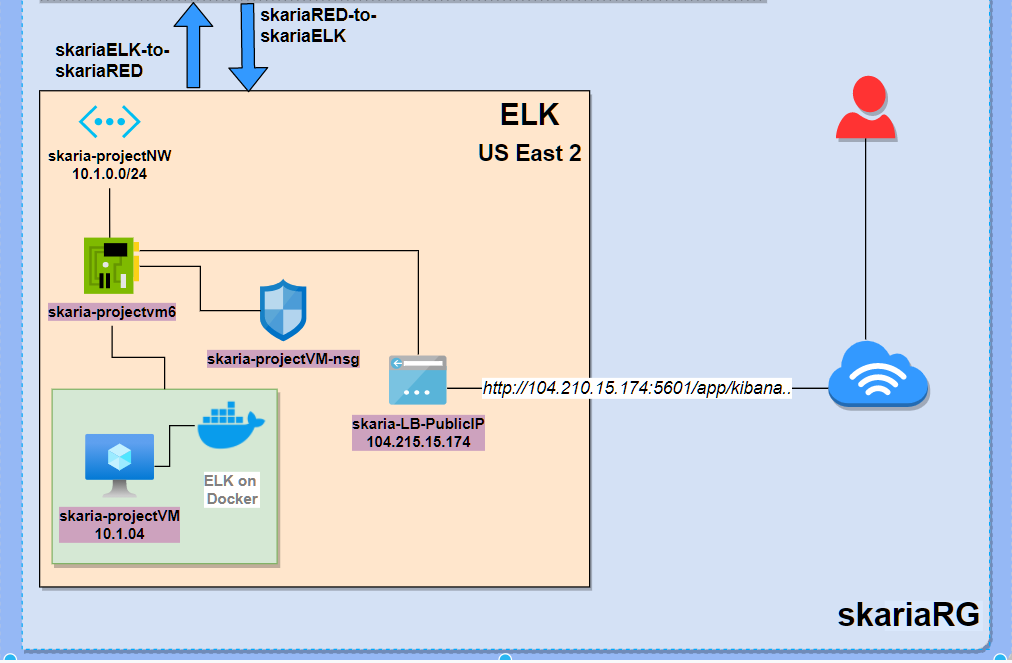
[Virtual memory | Elasticsearch Reference [5.0] | Elastic](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/vm-max-map-count.html#vm-max-map-count)



*Diagram 1*



*Continuation…*

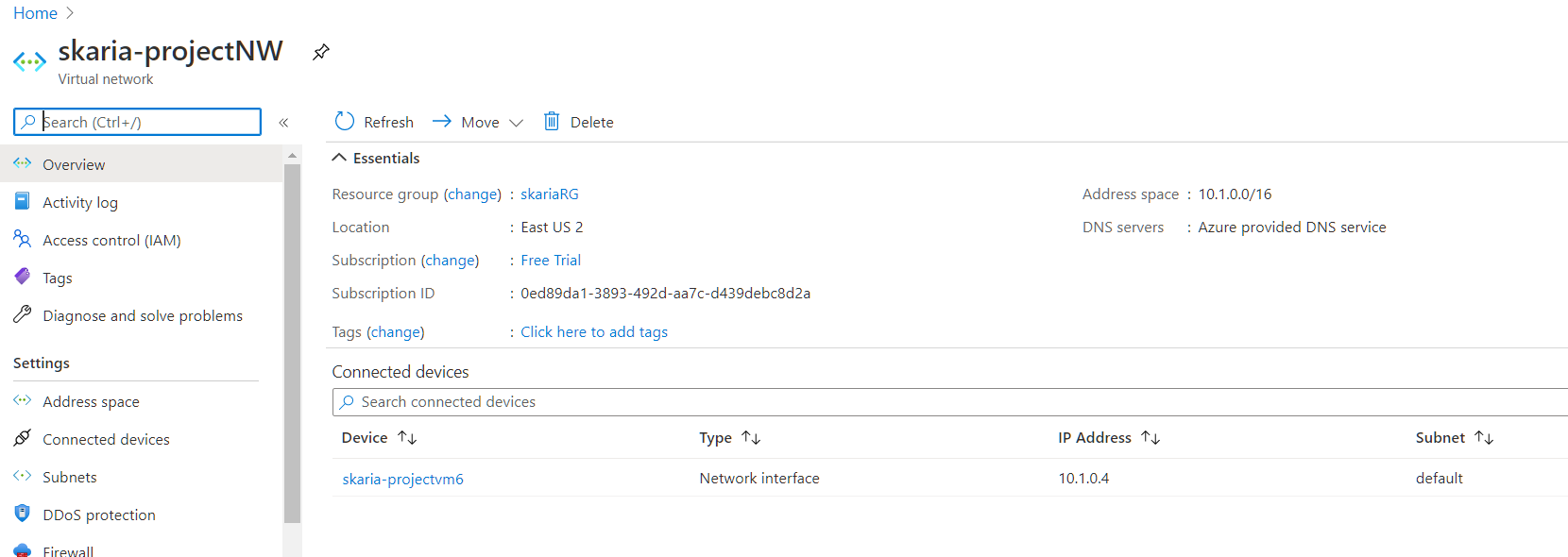


*Diagram 2*

# **Part 1: Creating a new Virtual Network**

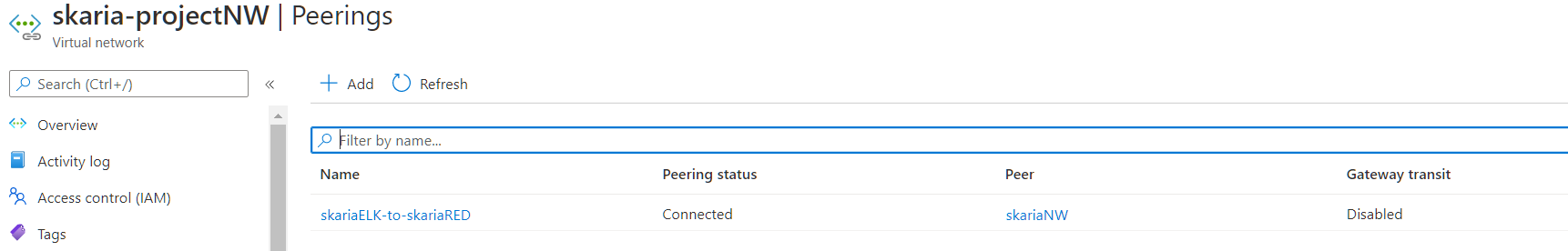
## New vNet located in the same resource group as per *Diagram 1*

* **Existing Record Group :** skariaRG
* **New Virtual Network :** skaria-projectNW
* **New Region :** US East 2



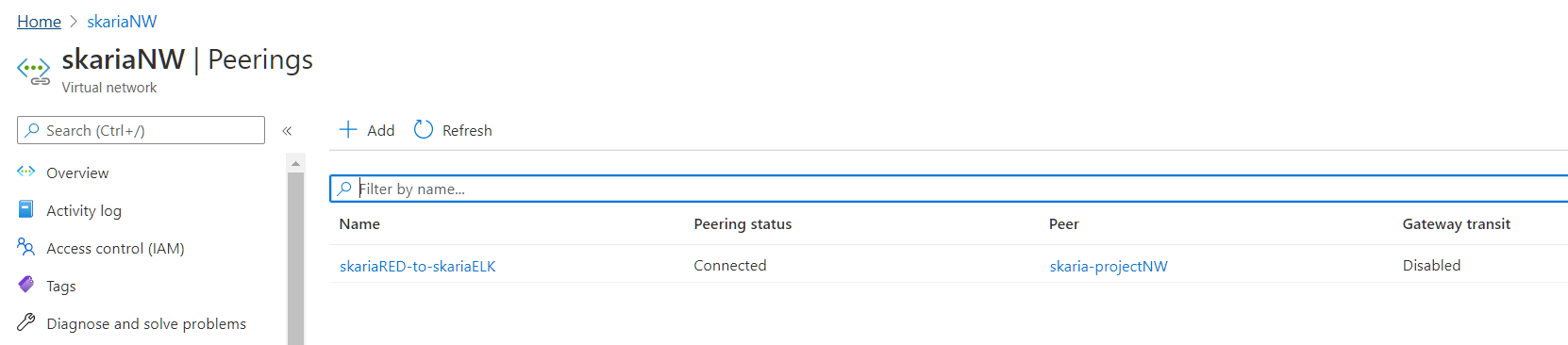
## Create a peer connection from new vNet to old vNet

* **skariaELK-to-skariaRED :** skaria-projectNW -to- skariaNW



## Create a peer connection from old vNet to new vNet

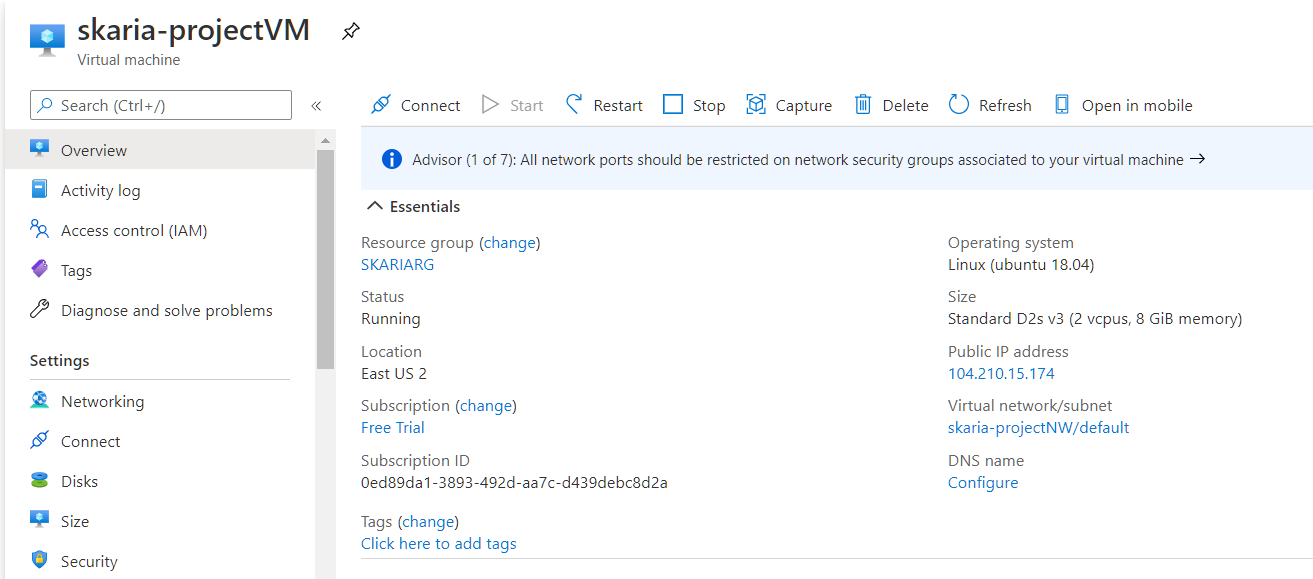
* **skariaRED-to-skariaELK :** skariaNW -to- skaria-projectNW



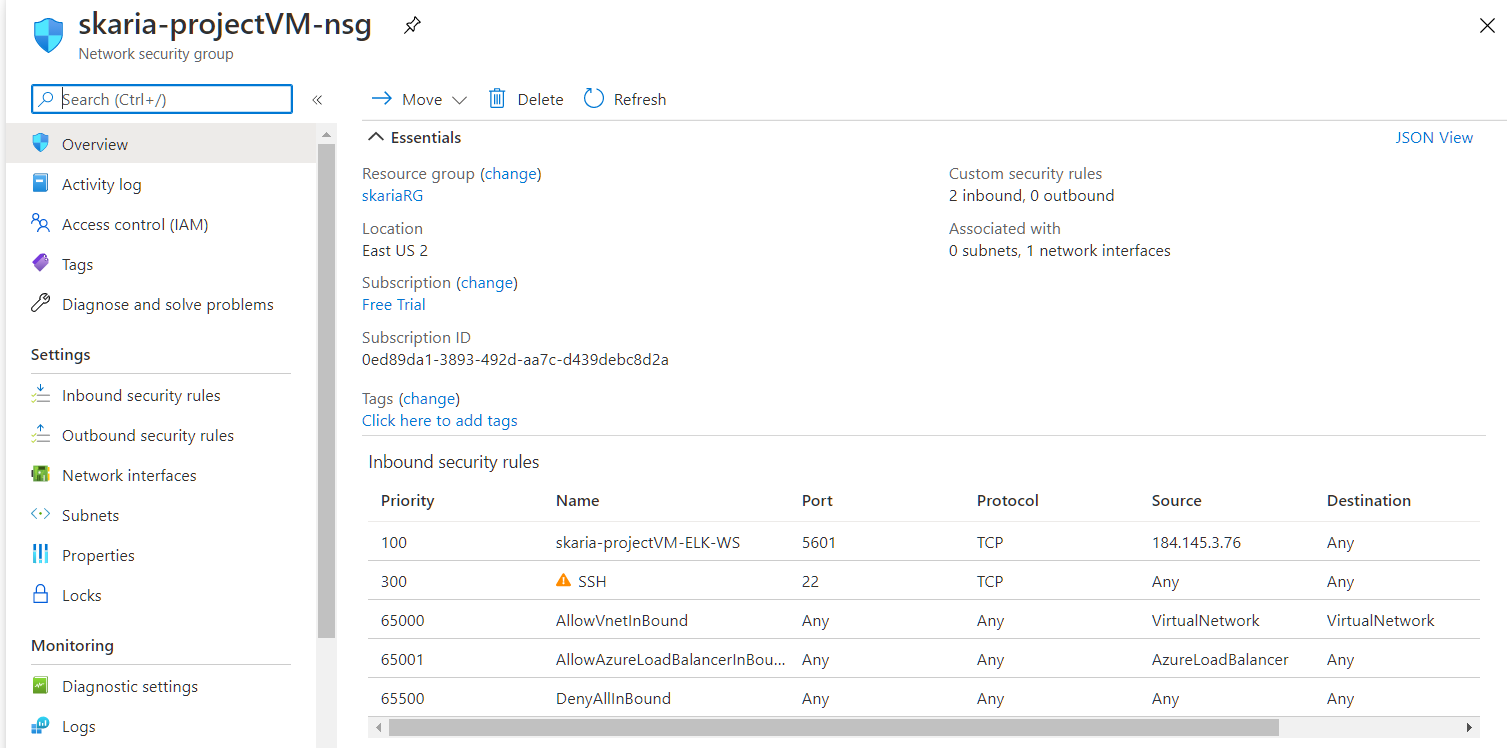
# **Part 2: Creating a new Virtual Machine**

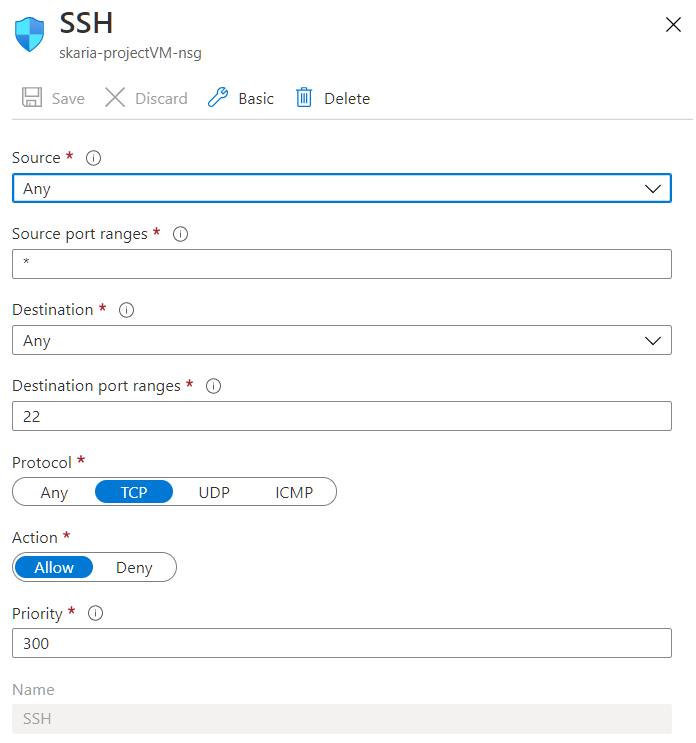
## Create a new vNet located in the same resource group you have been using

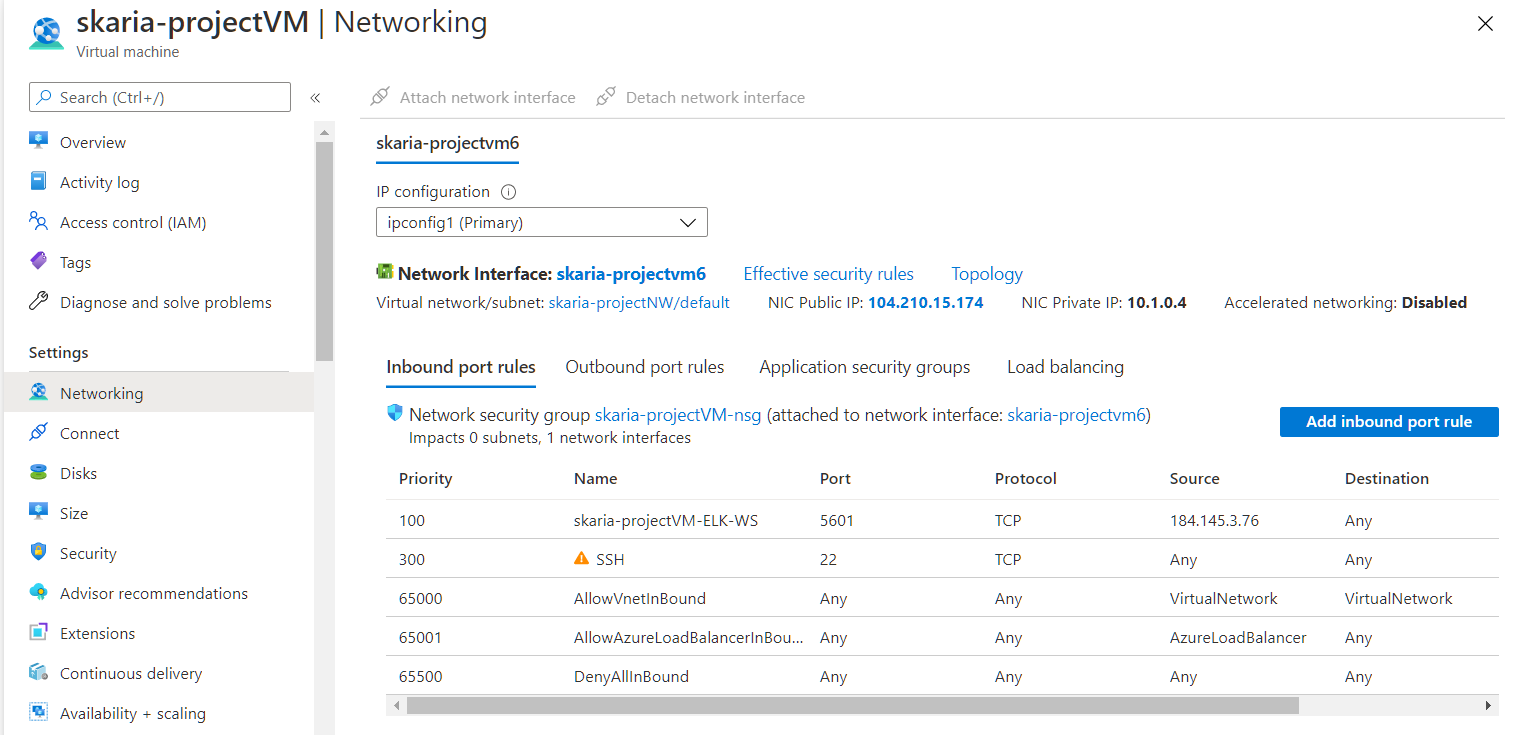
* **Existing Resource Group :** skariaRG
* **New Virtual Machine :** skaria-projectVM
* **New Region :** US East 2
* **Public IP (Static) :** 104.210.15.174



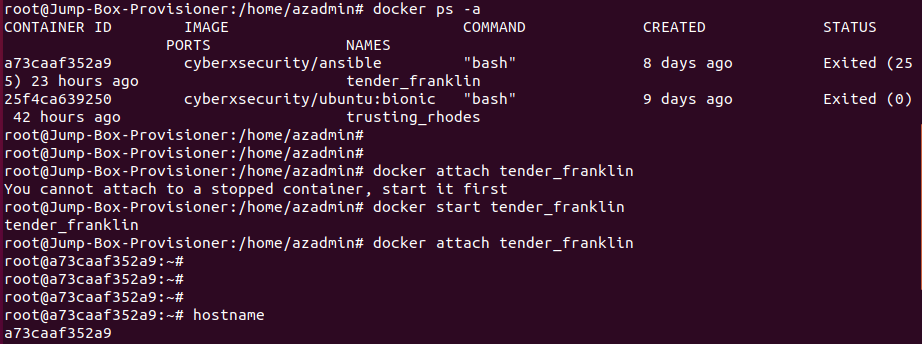
## Add SSH to in-bound rules to the new VM using the SSH Public Key from the Ansible Container running on the Jumpbox-Provisioner







## After creating the new VM in Azure, verify that it works as expected by connecting via SSH from the *Ansible container* on your jump box VM.

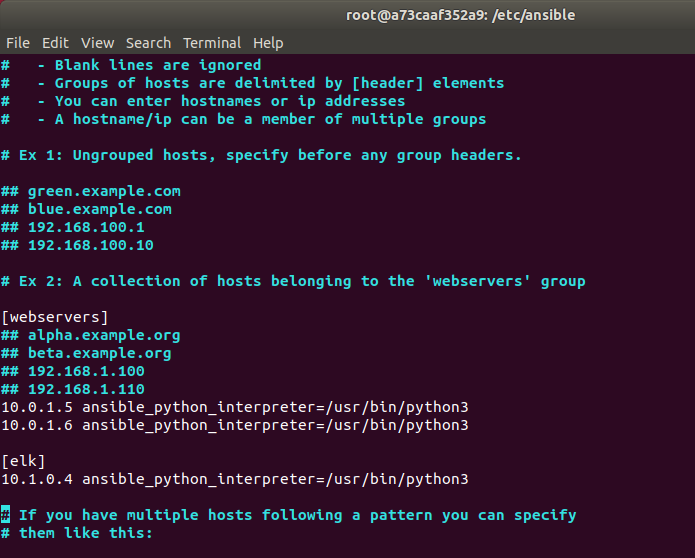


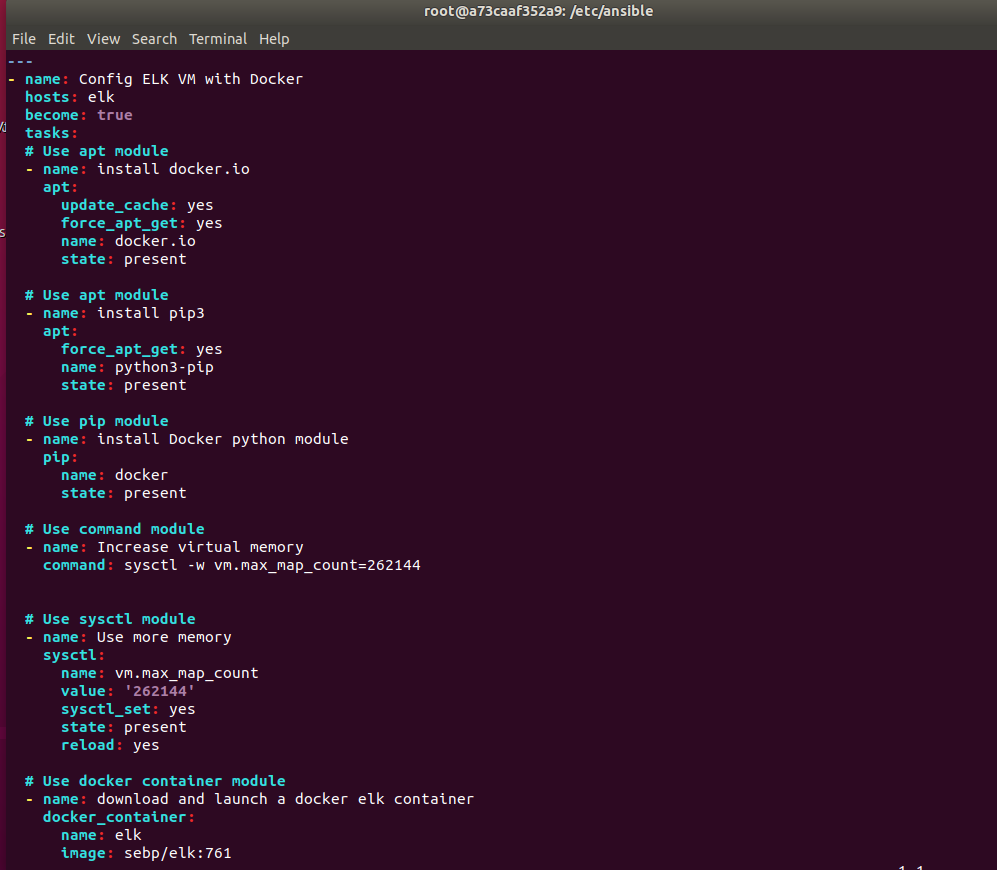


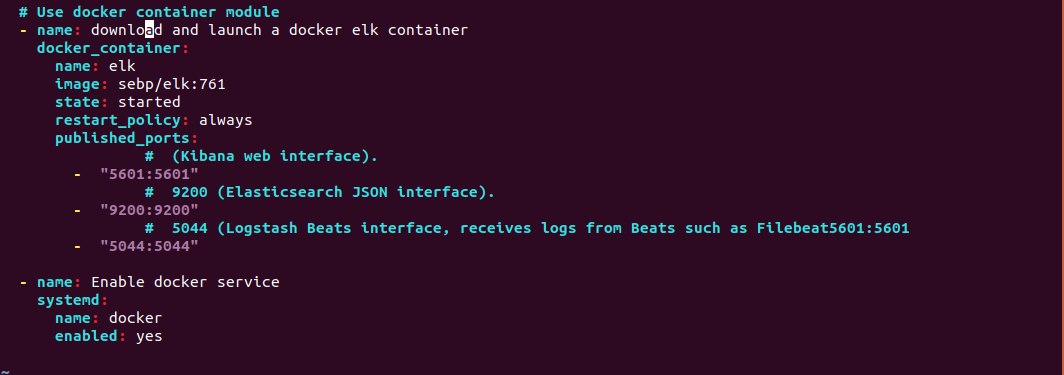
# **Part 3: Downloading and Configuring the Container**

## Using Ansible, configure the newly created VM.

## New VM will run your ELK stack. In order to use Ansible to configure this machine, you must add it to the list of machines Ansible can discover and connect to.

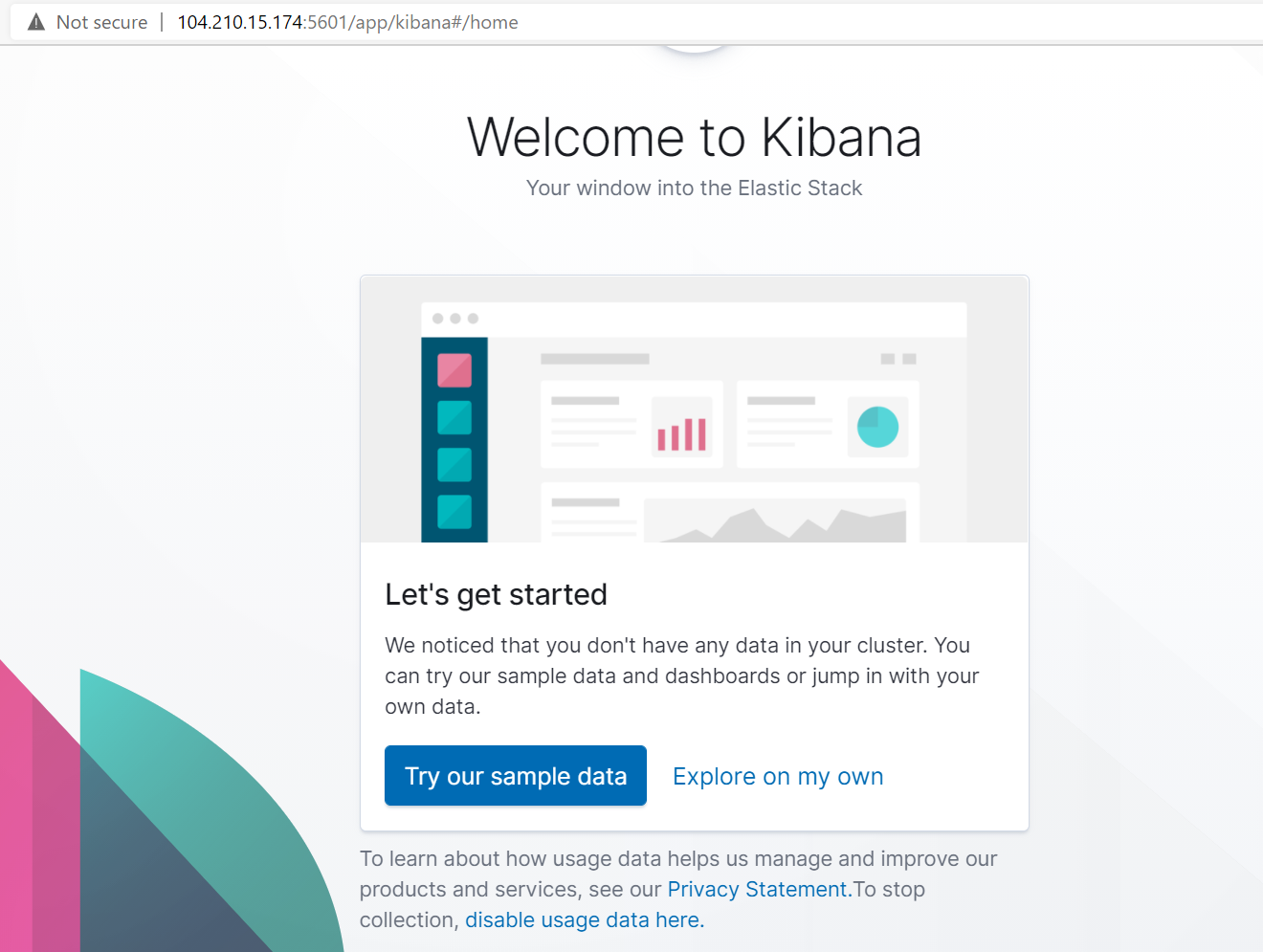


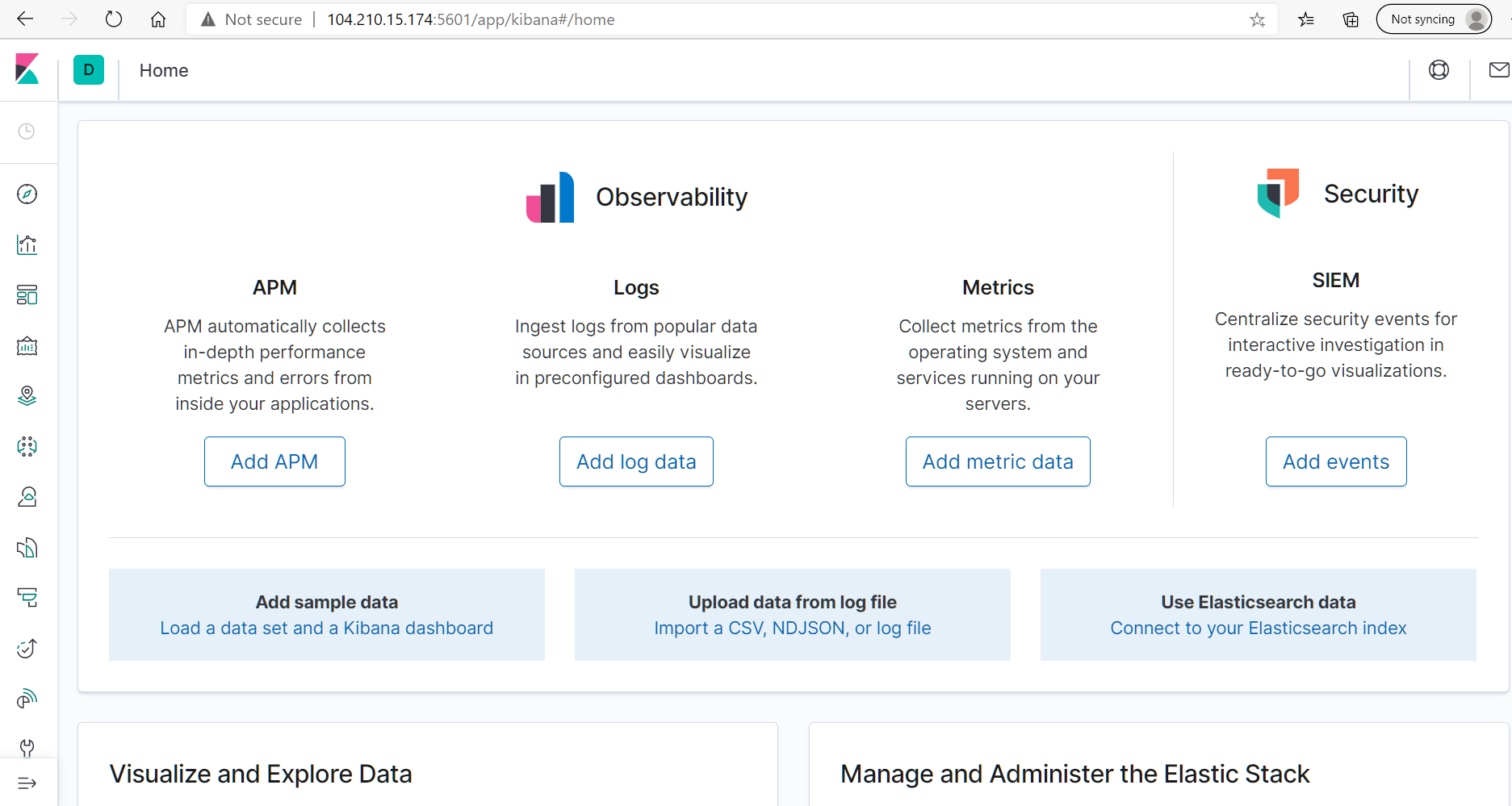




# **Part 4: Launching and Exposing the Container**

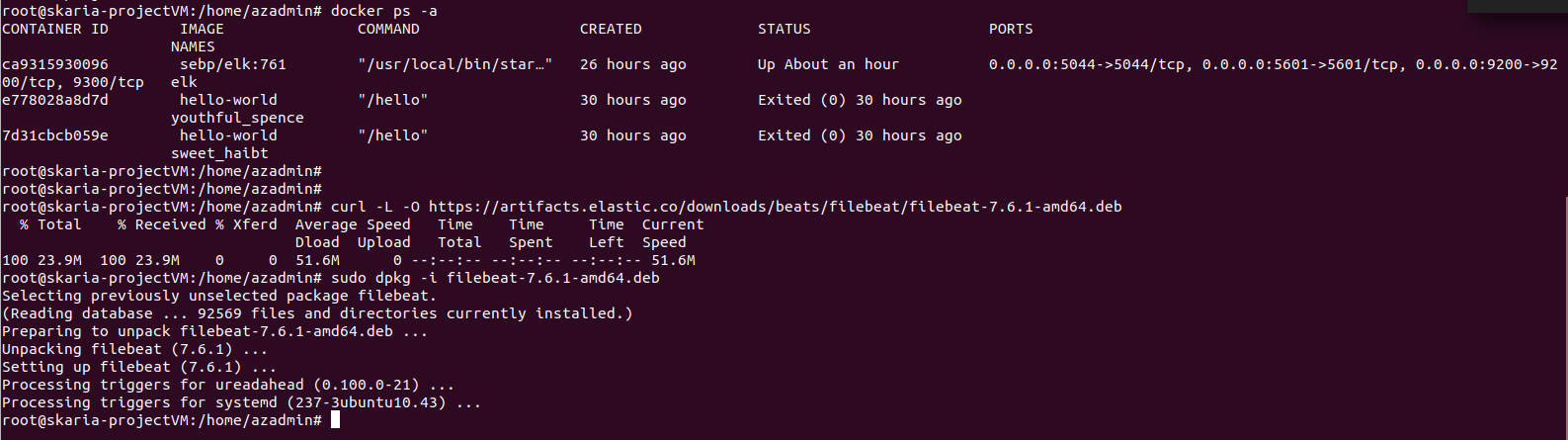
## Accessing Kibana running on ELK Container hosted on skaria-projectVM.





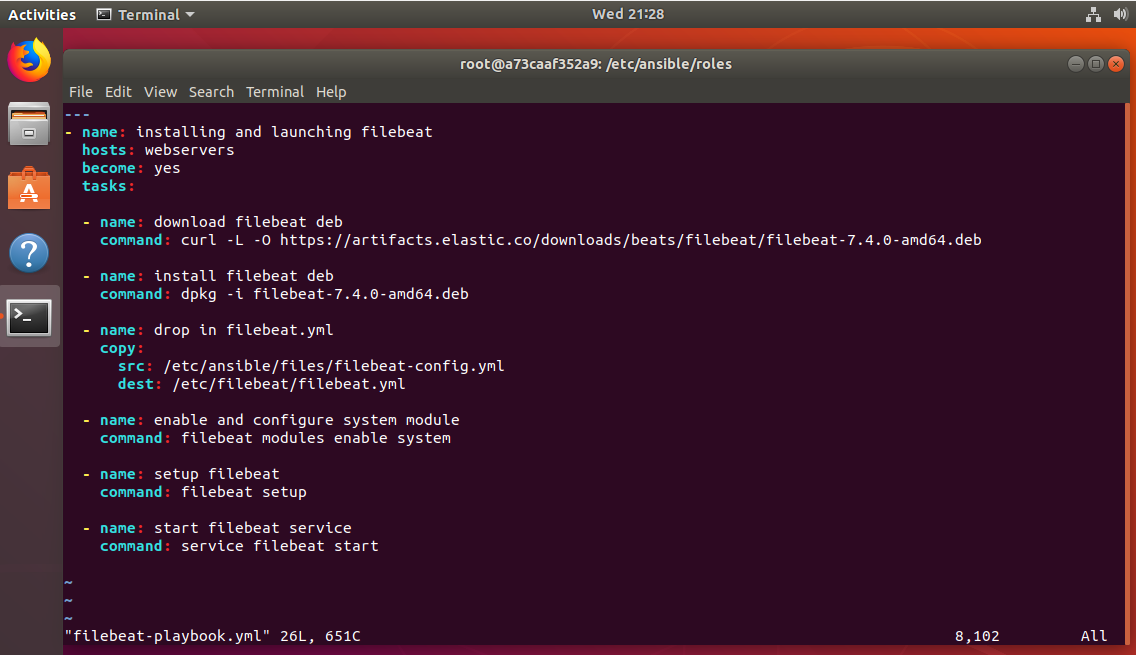
# **Part 5: Installing Filebeat on the Web VM’s running the DVWA Container**

## Downlaod filebeat and verify if ELK container is running on docker on ELK VM

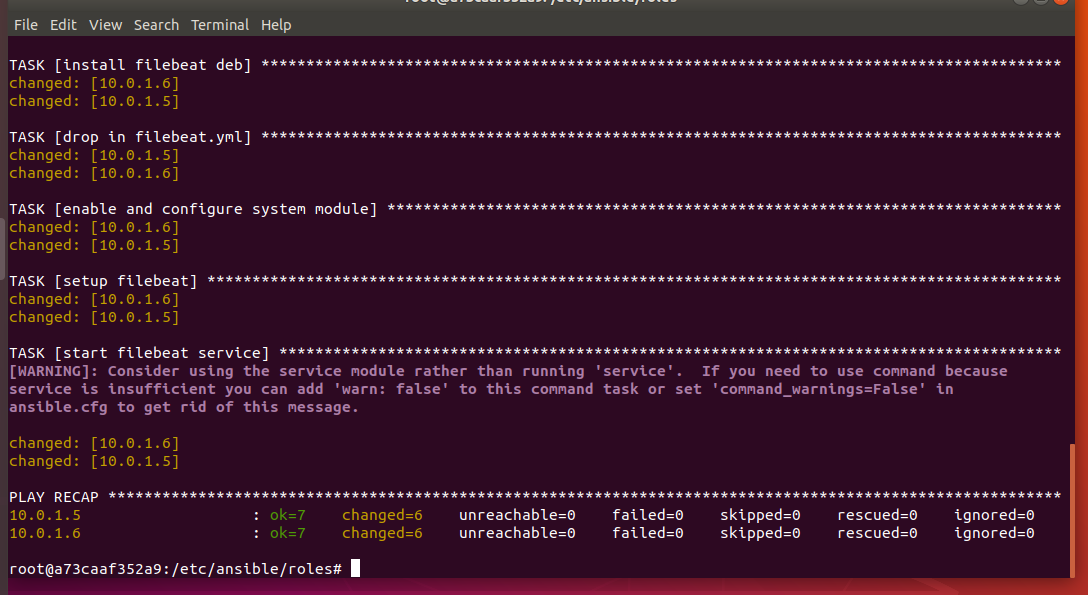




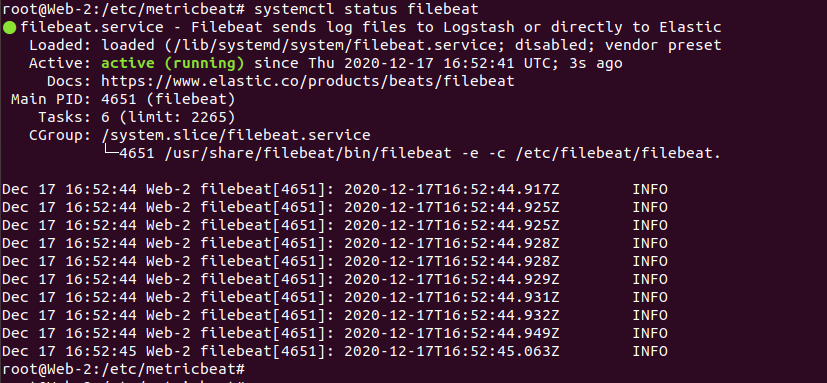
## Write playbook to download Filebeat and install on Web VM’s running the DVWA container



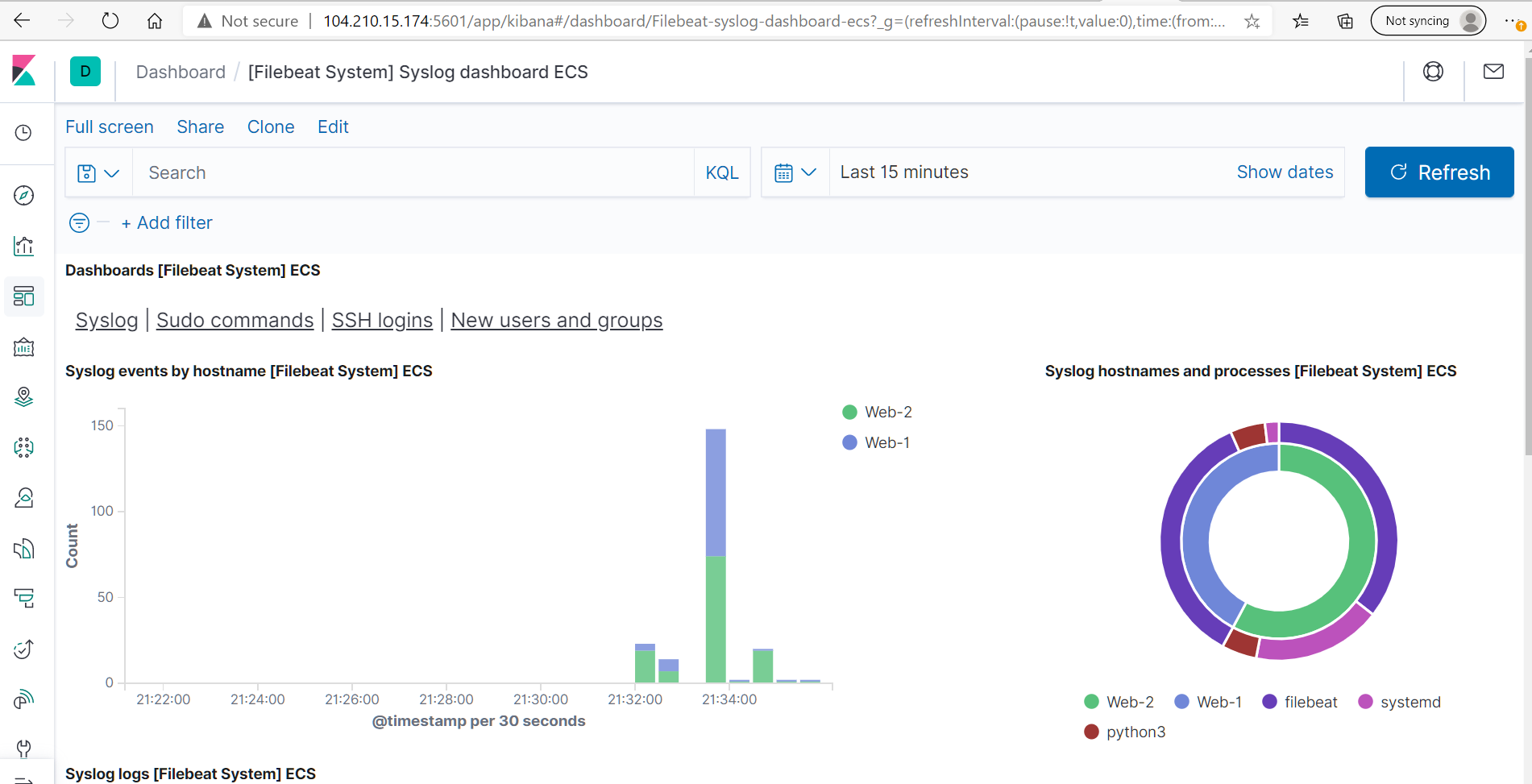
## Execute filebeat playbook on Ansible Container

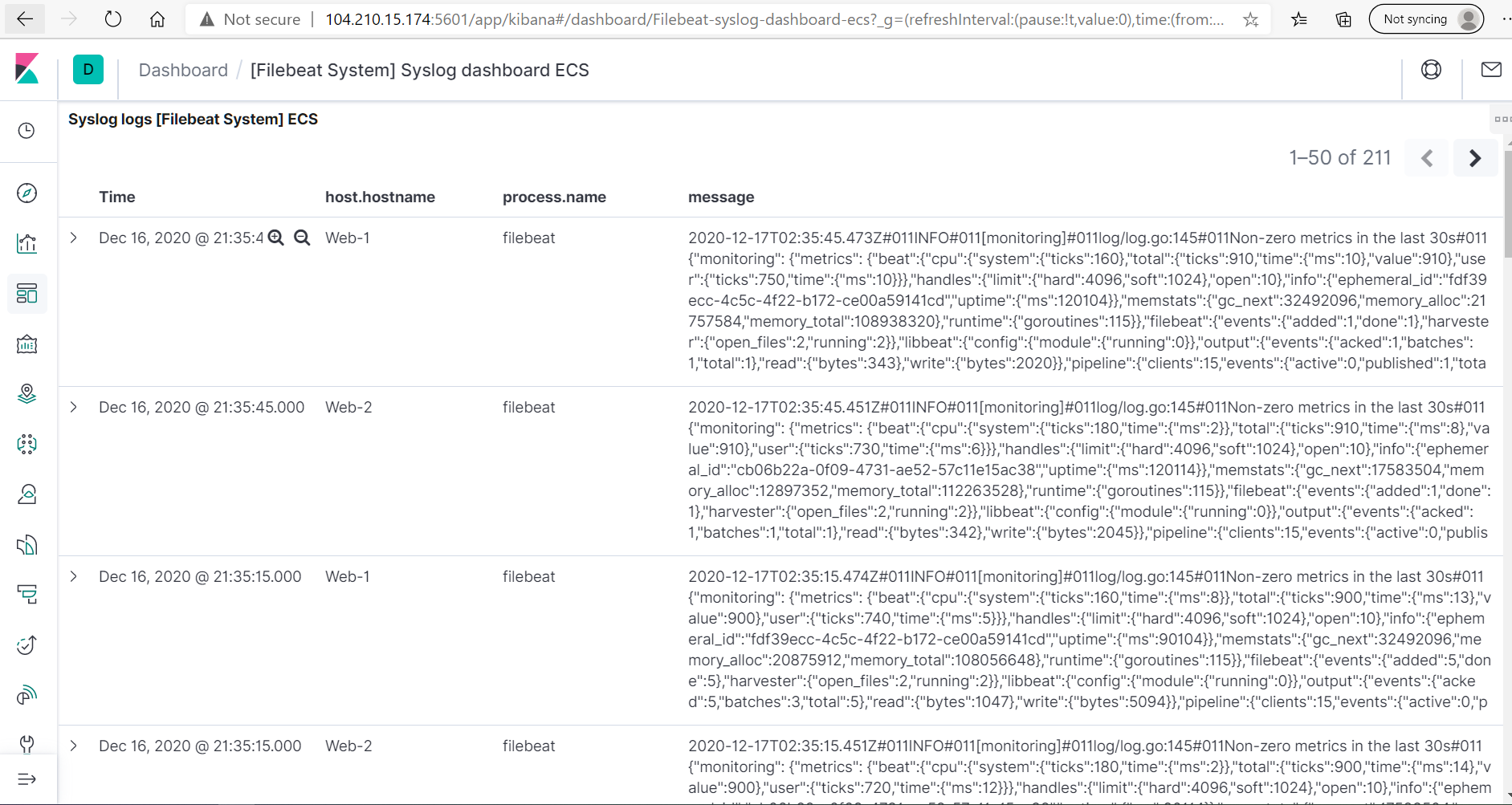


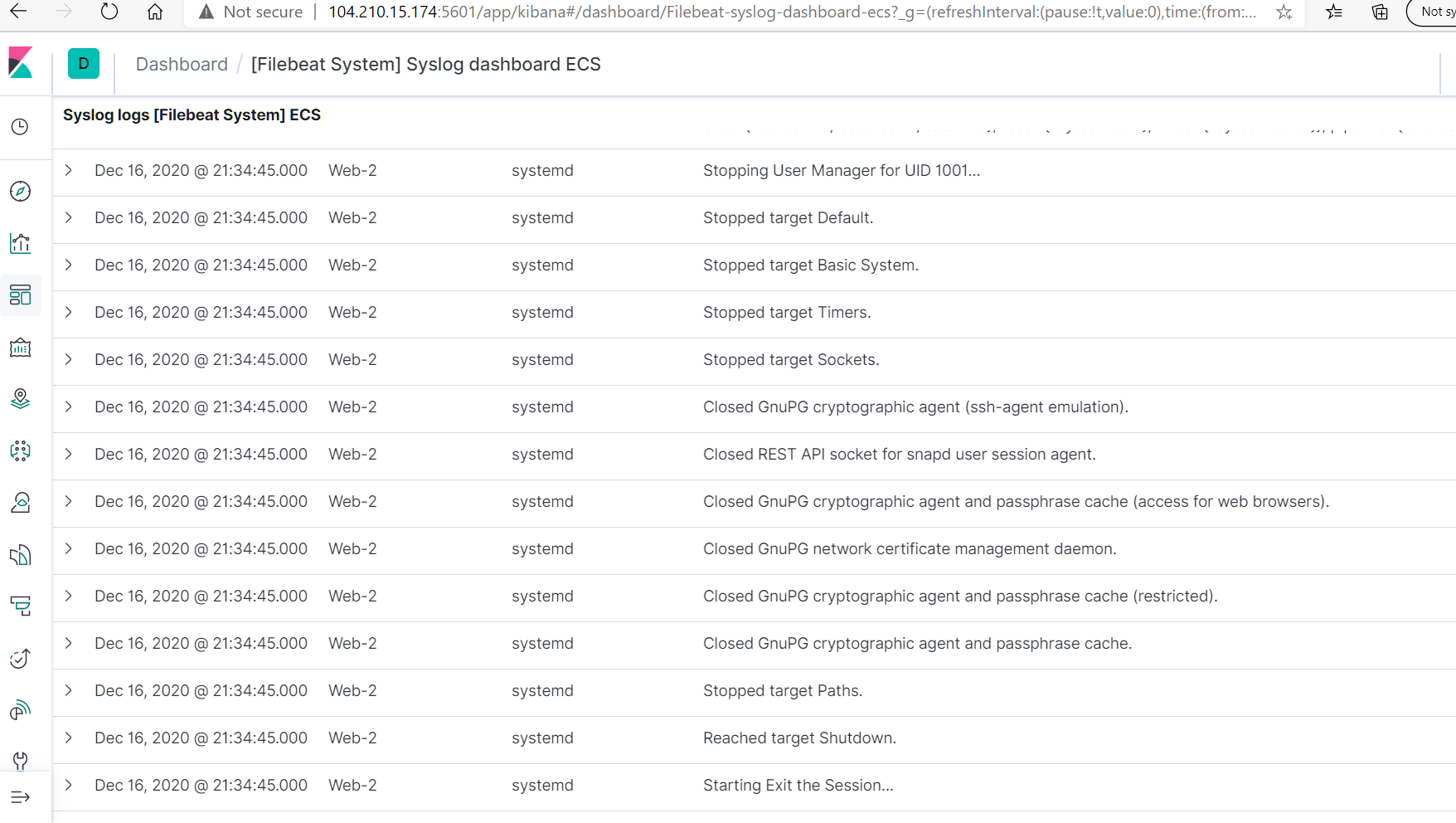
## Verify that filebeat is functional on the Web VM running the DVWA Container

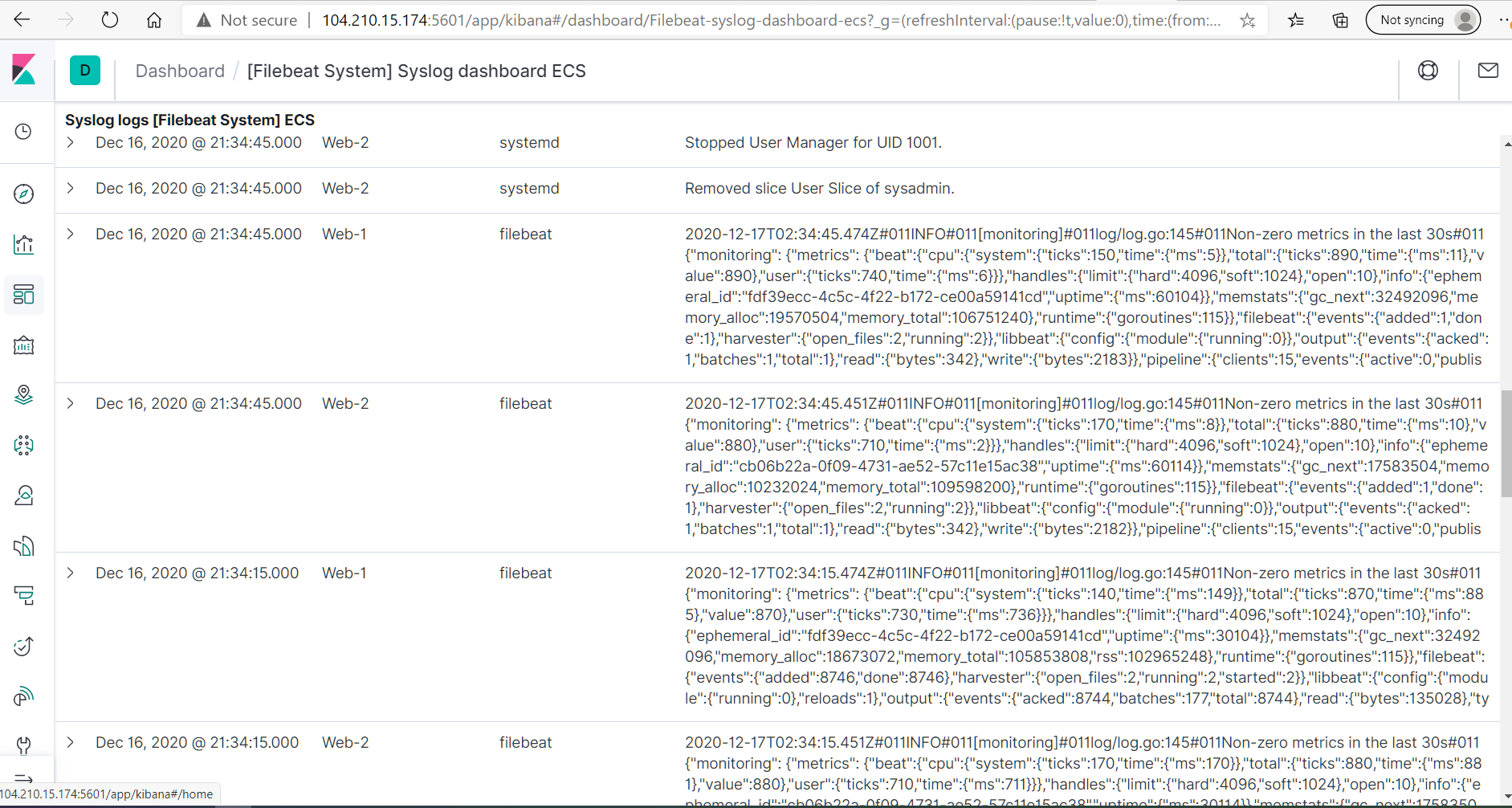


## Check if Data is received on the ELK Server



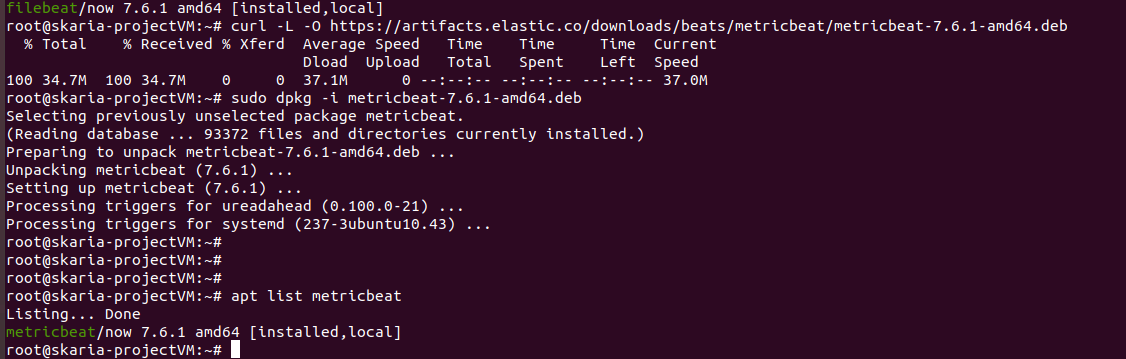


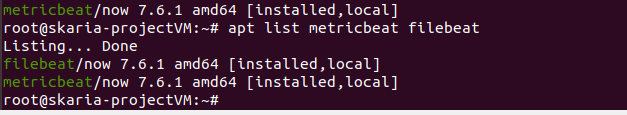




# **Part 6: Installing Metricbeat on the Web VM’s running the DVWA Container**

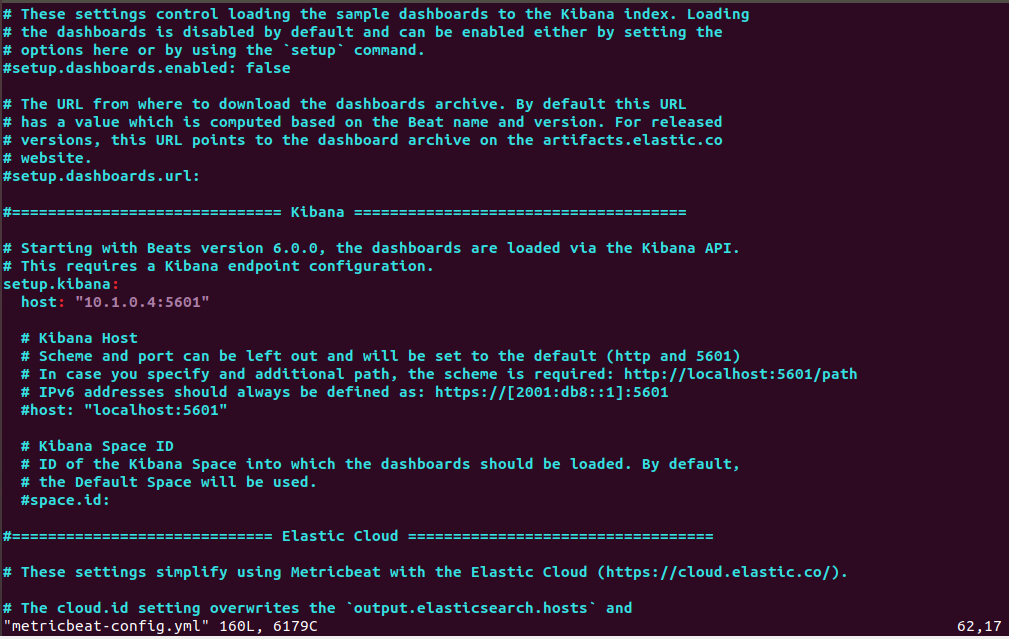
## Downlaod metricbeat and verify if ELK container is running on docker on ELK VM



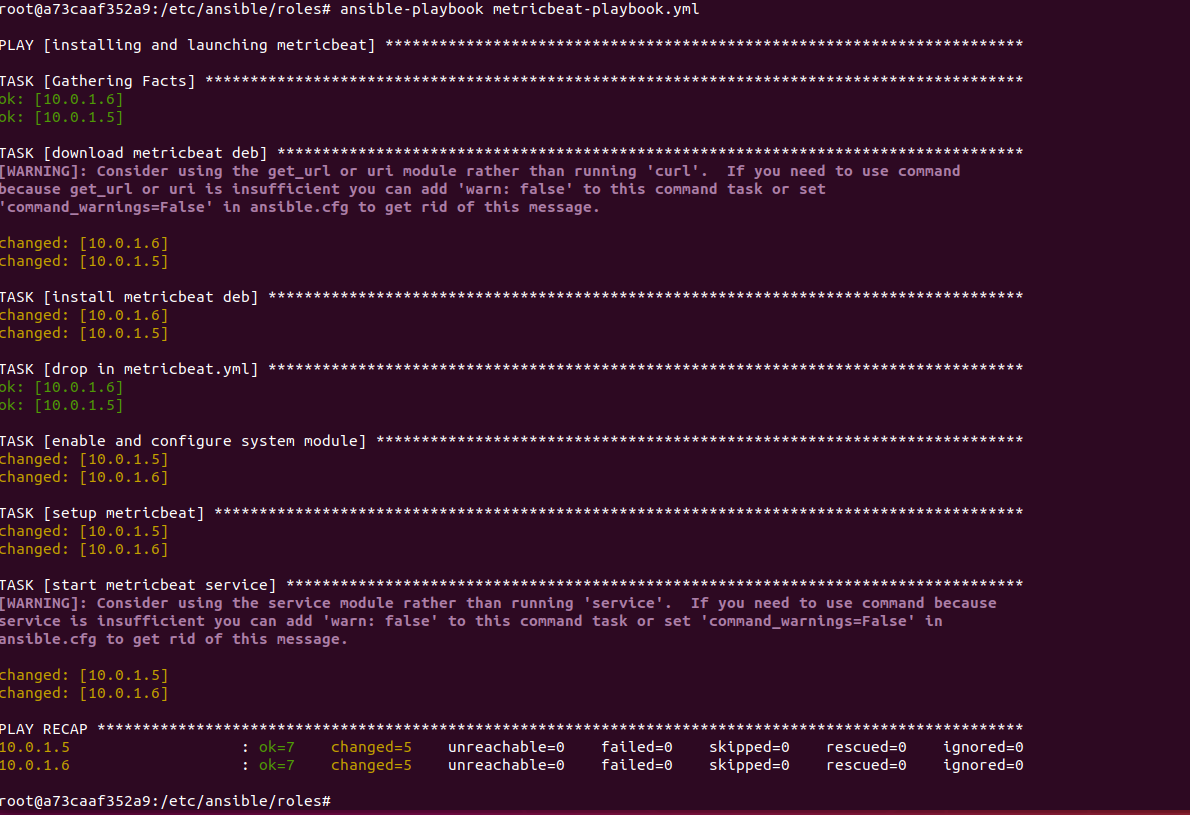


## Update the metricbeat.yml configuration file

### Ensure to update host IP to the ELK Server VM IP 10.1.0.4



## Execute metricbeat playbook on Ansible Container



## Verify that filebeat is functional on the Web VM running the DVWA Container

