ELK Stack, Filebeat, and Metricbeat

Setup Walkthrough

By: Walter T. Pan

Contents

[Create a new virtual network for ELK Stack. 2](#_Toc67842581)

[Set up ELK-Server VM 5](#_Toc67842582)

[Create a new ELK-VM 6](#_Toc67842583)

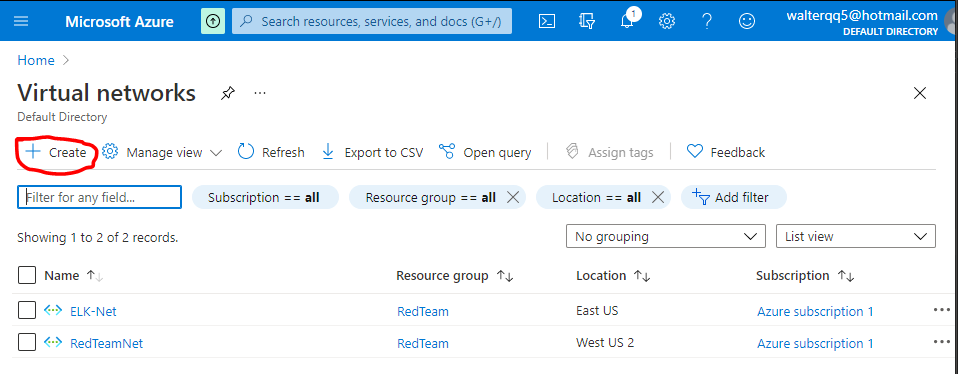
[Setting up FileBeats 13](#_Toc67842584)

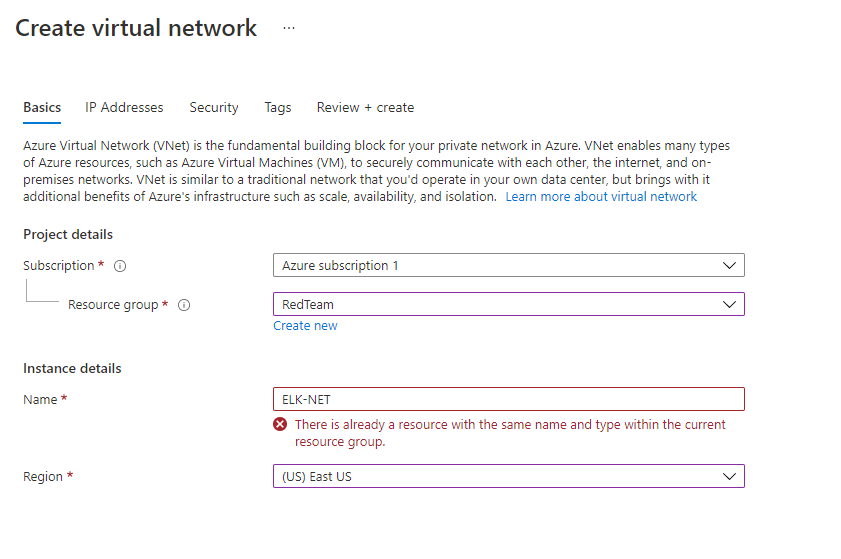
[Setting up Metricbeats 15](#_Toc67842585)

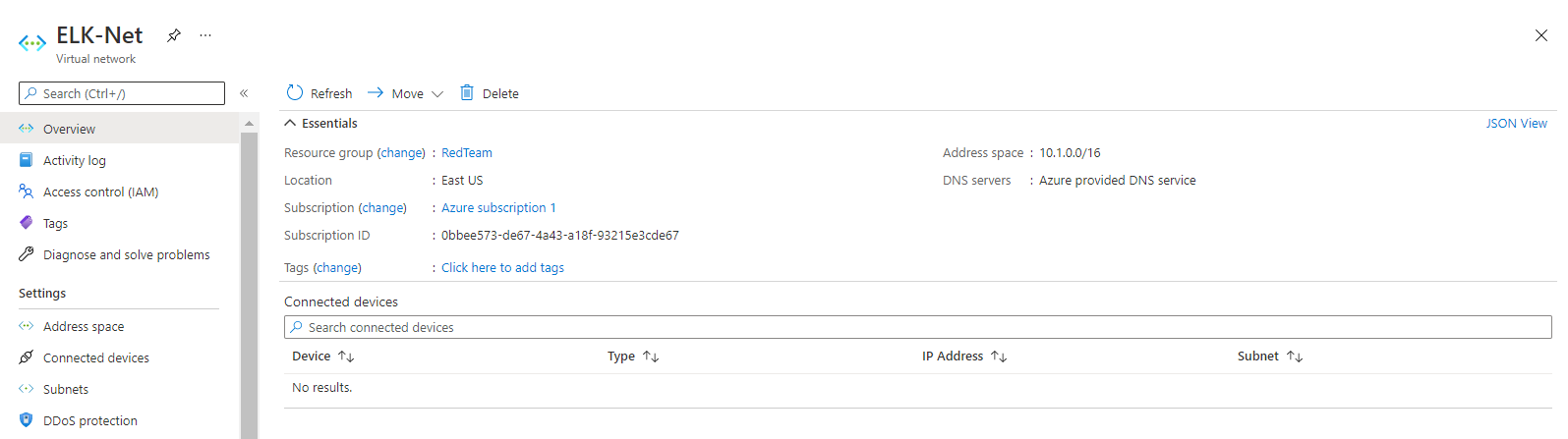
# Create a new virtual network for ELK Stack.

Navigate the Azure portal/Virtual Networks

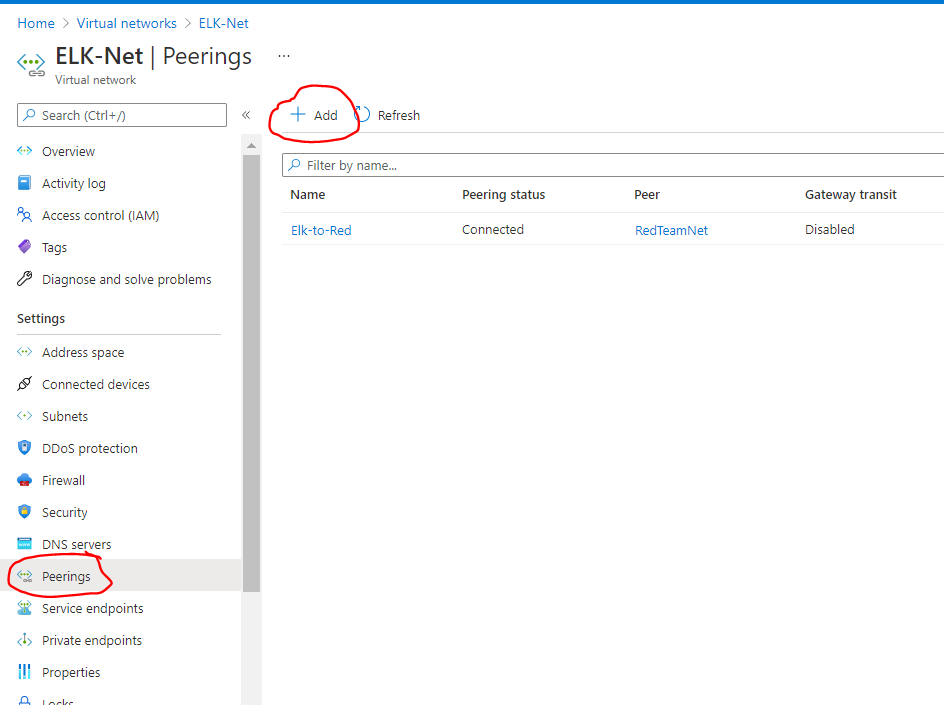
Select create.



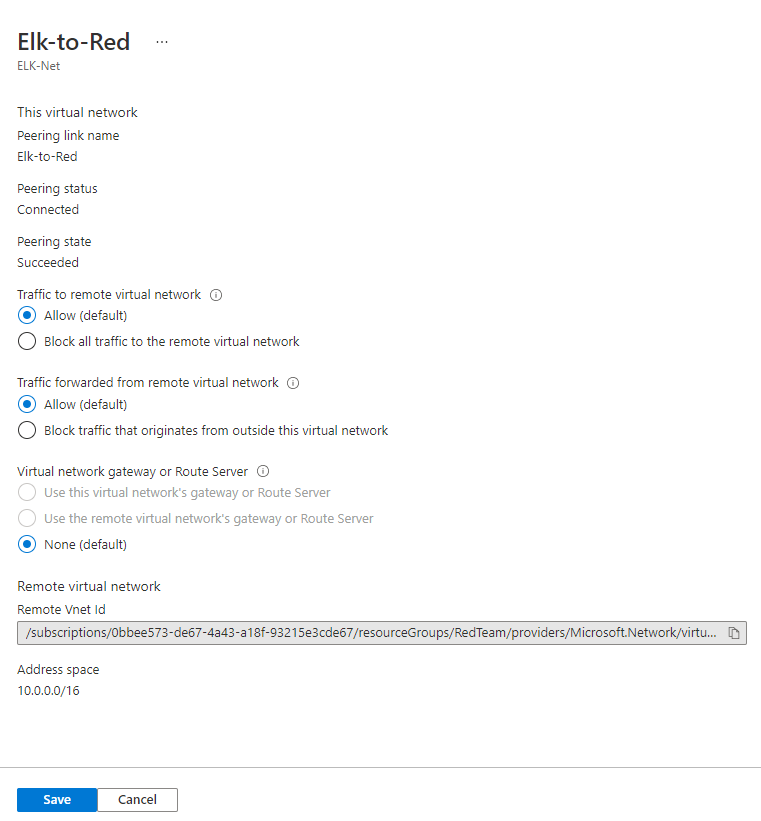
Input the settings above and leave the rest of the settings at default.



Create a Peer connection between the virtual networks, by going to peering and adding a new peering.

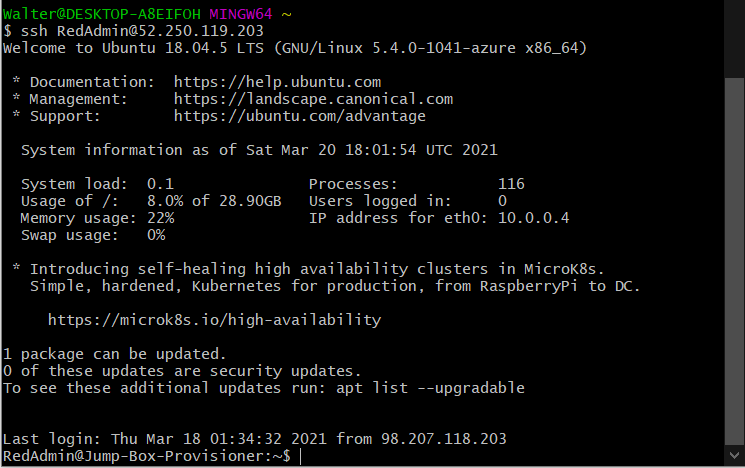


Select the following settings.



# Set up ELK-Server VM

Navigate to GitBash and SSH into Jump Box.

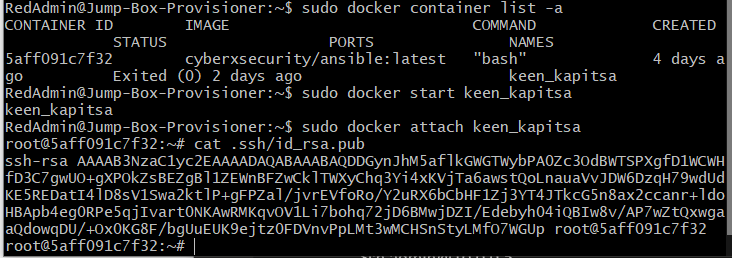


Check and locate an Ansible container.

Start the container.

Connect to the container.

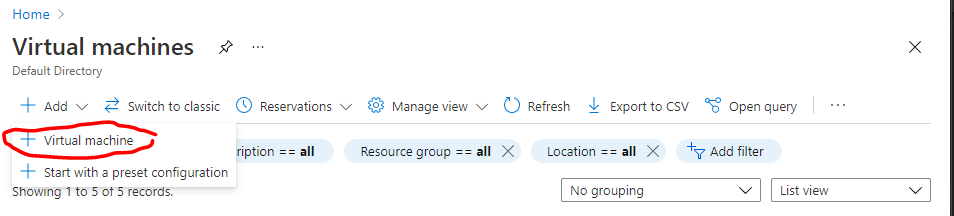
Copy the SSH key from the Ansible container on your Jump Box.



# Create a new ELK-VM

Navigate to virtual machines.

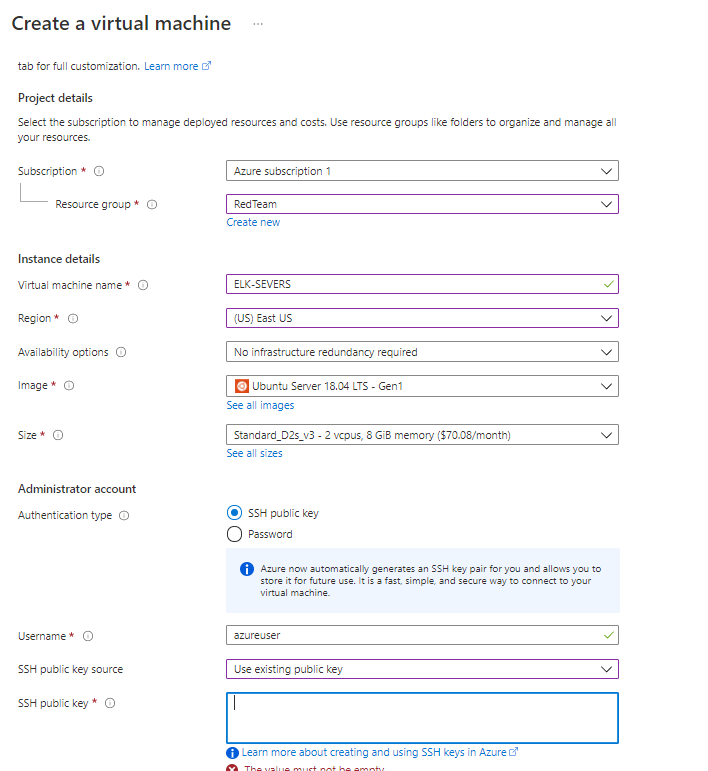
Add new virtual machine.

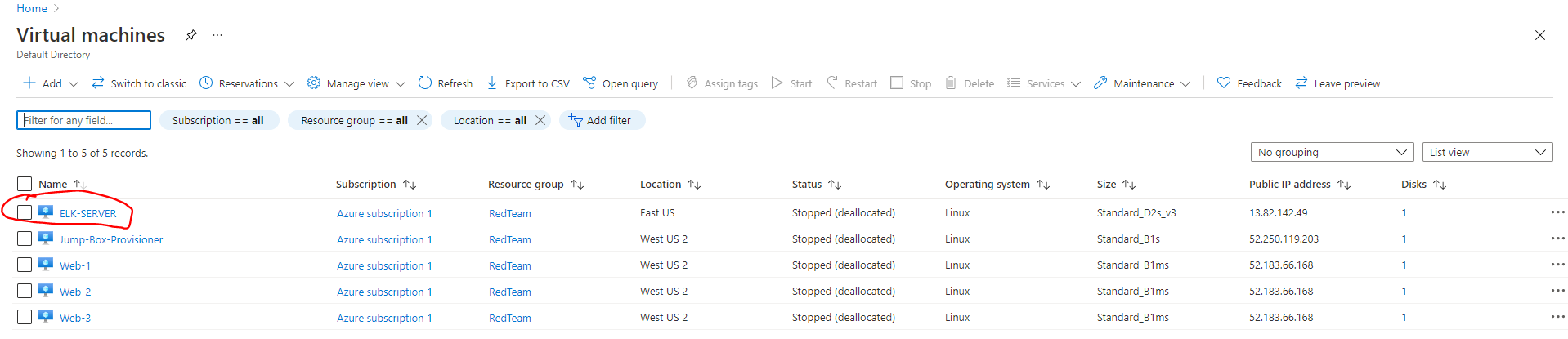


Memory: At least 4 GB of RAM

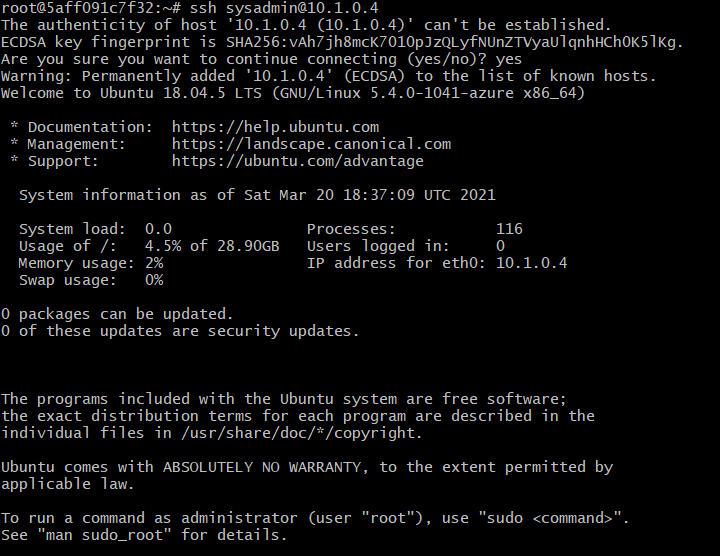
Public IP address

Add the ELK VM to a new security group.

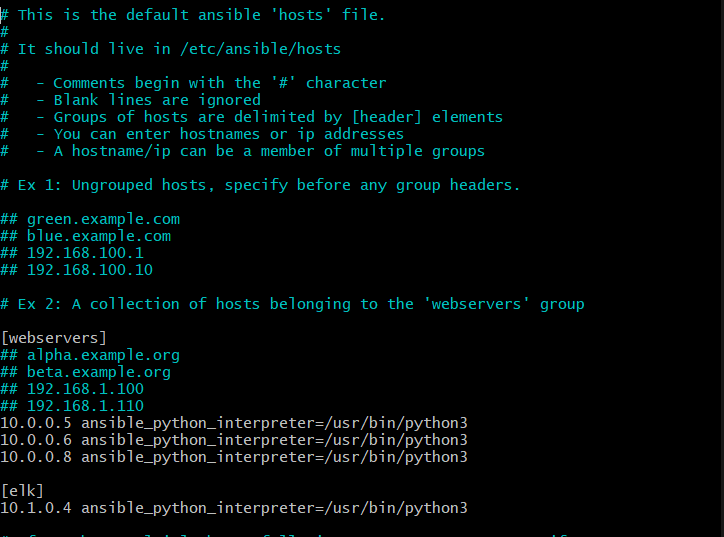




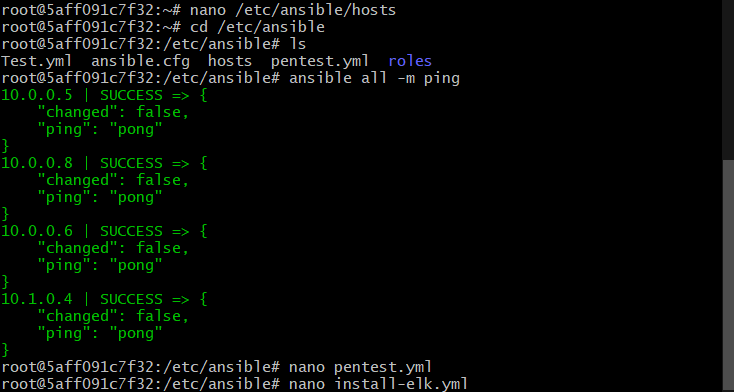
Test the new virtual machine with SSH.



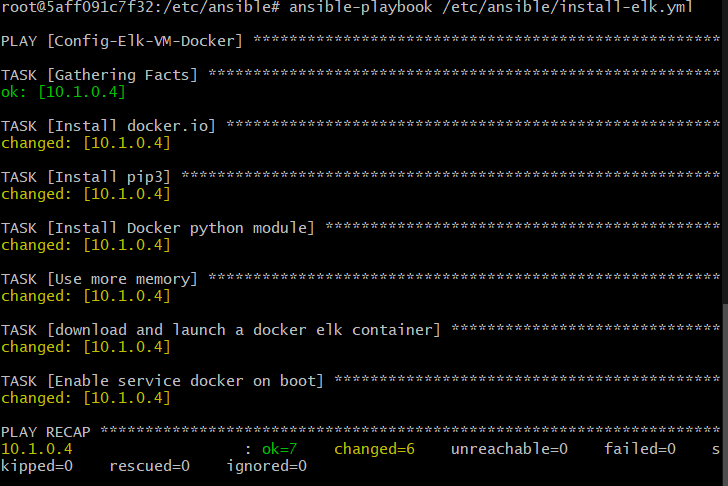
Add the ELK VM to the ansible Host file at /etc/host.

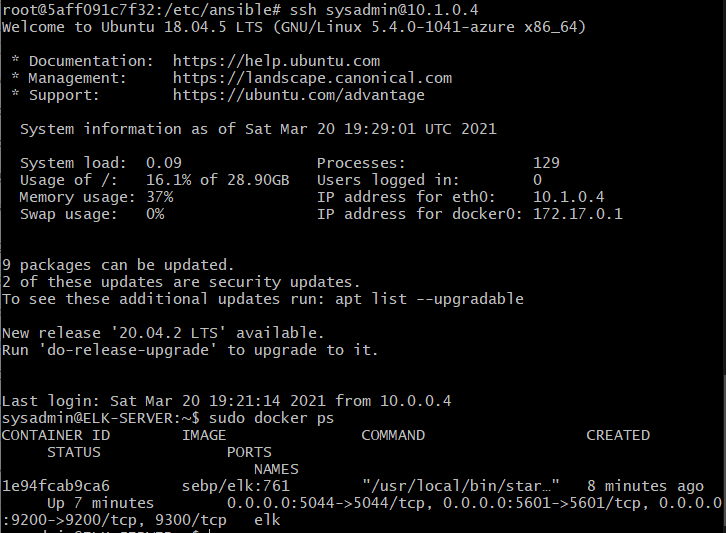


Test connection to the VMs.

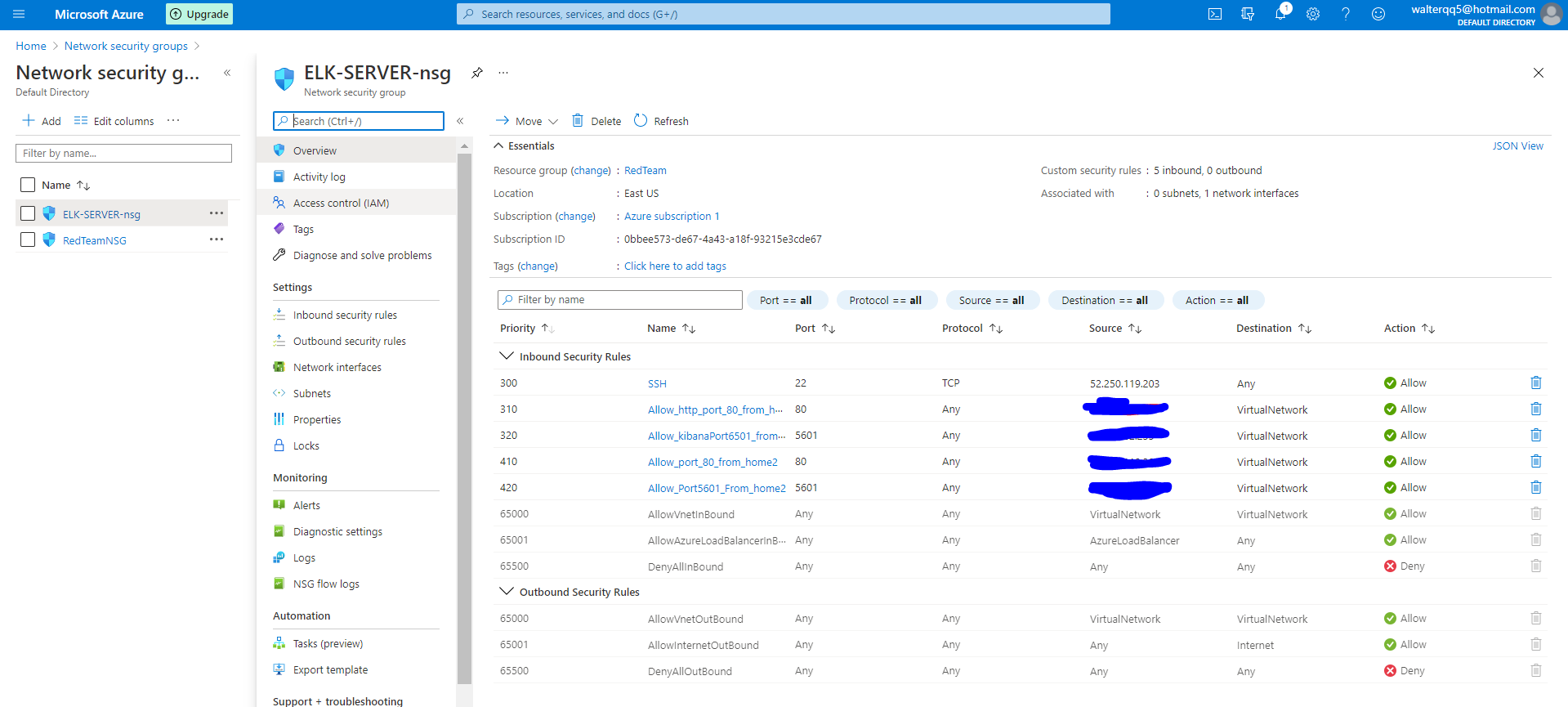


Run ansible-playbook install-elk.yml



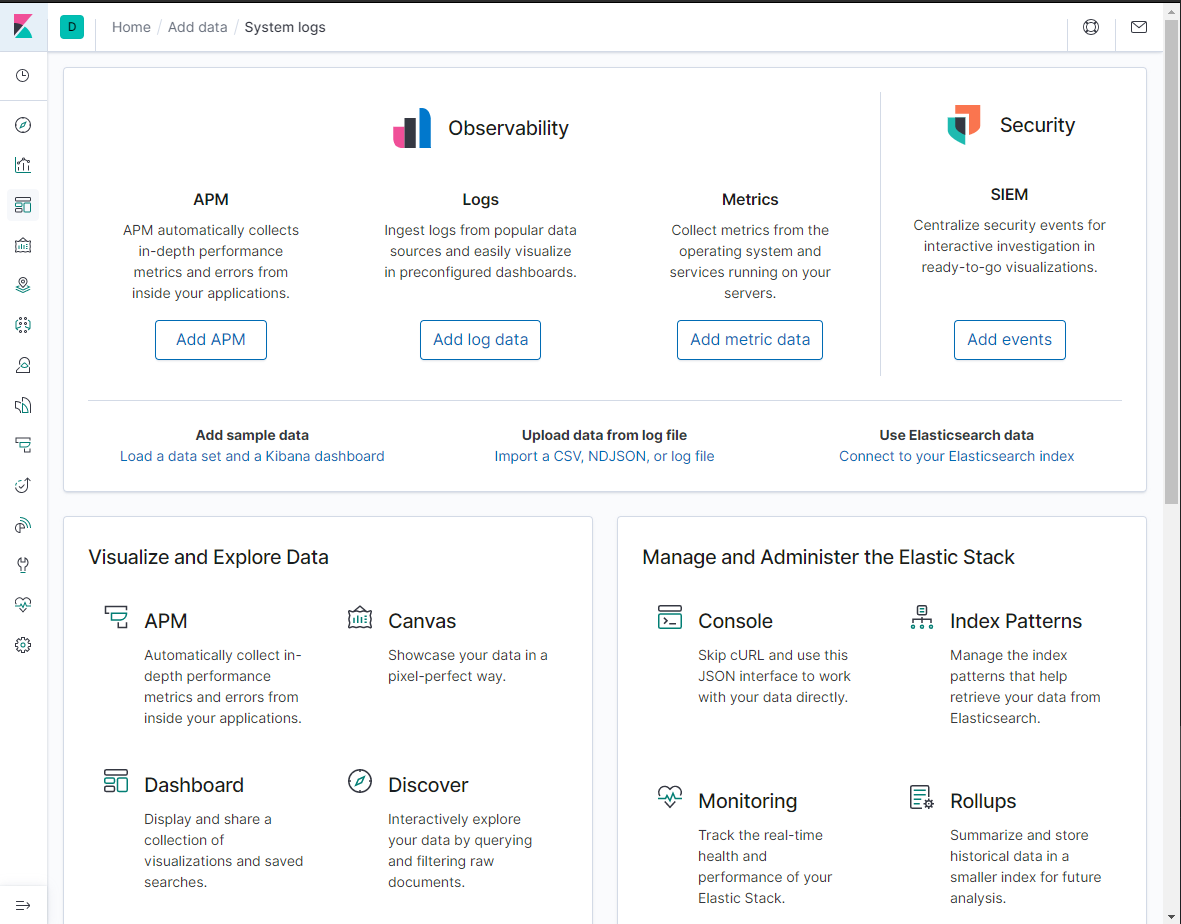
SSH into the ELK-Server VM and check ELK-Server VM sudo docker ps

Add security rules to allow connect to the ELK-Server VM



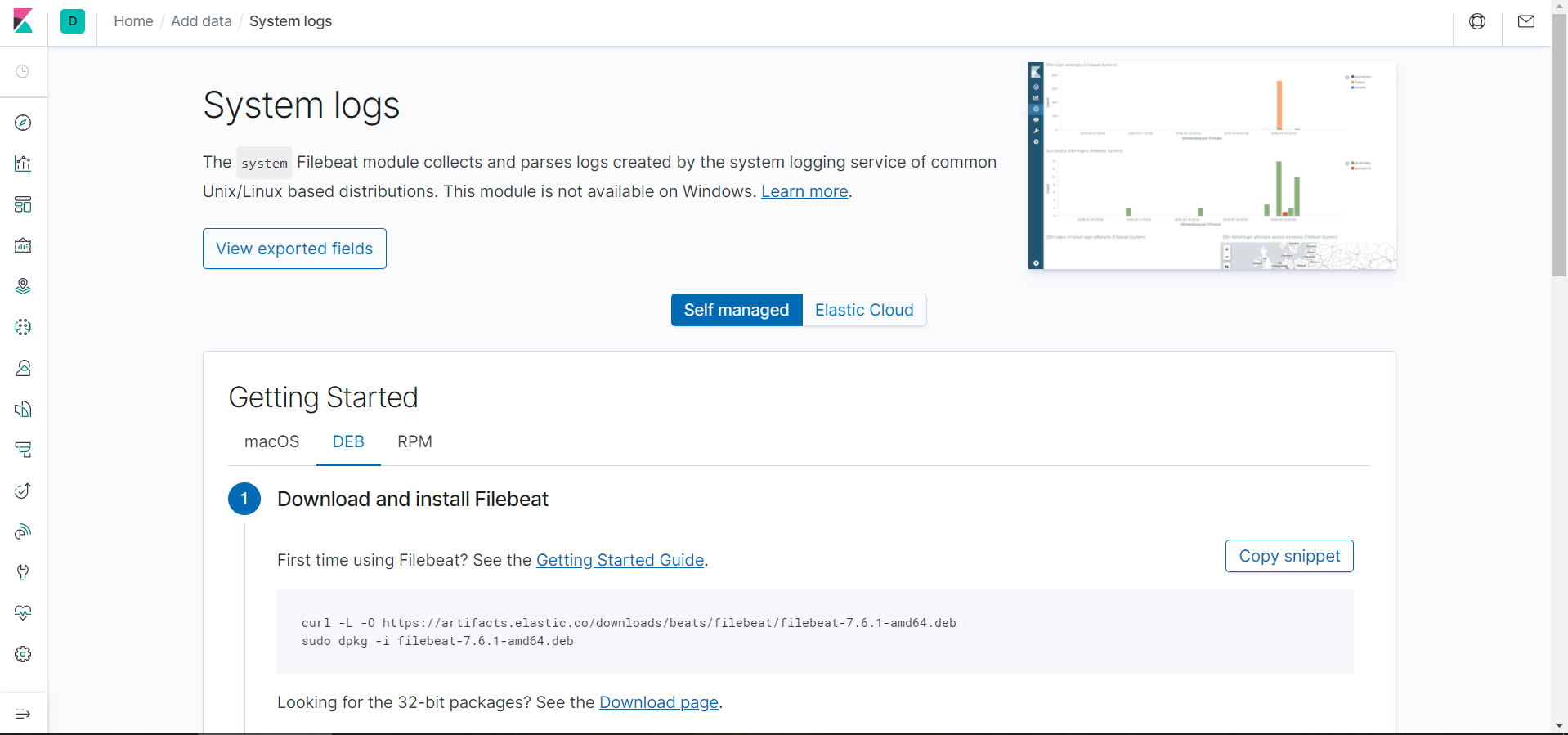
Launch the Kibana webpage from the follow address:

<http://13.82.142.49:5601/app/kibana>



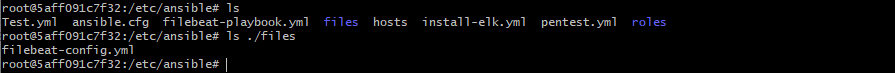
# Setting up FileBeats

In the Kibana webpage, navigate to Home/Add data/ System Logs.



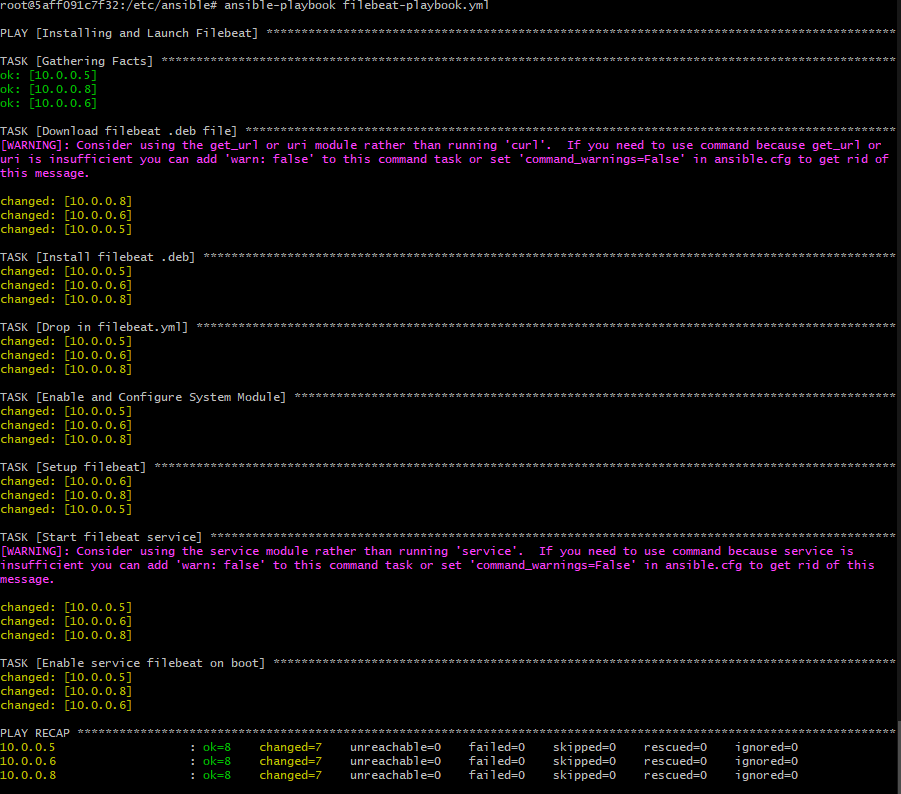
Copy the file filebeat-config.yml to /etc/ansible/files.



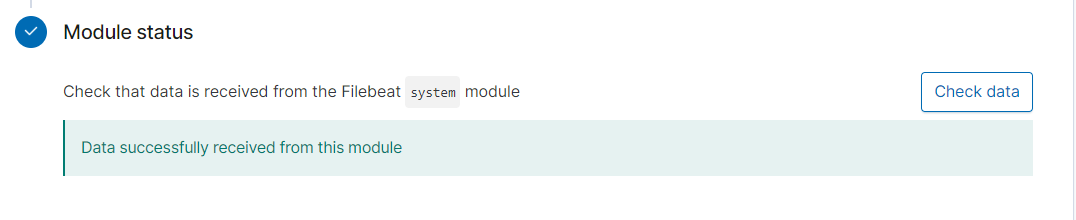


Copy the filebeat-playbook.yml file to /etc/ansible.

Run the filebeat-playbook.yml playbook.



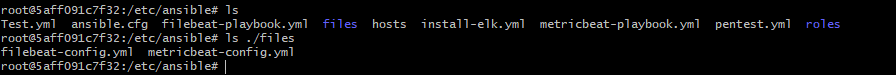
- Check on Kibana that logs are being received from module status.



# Setting up Metricbeats

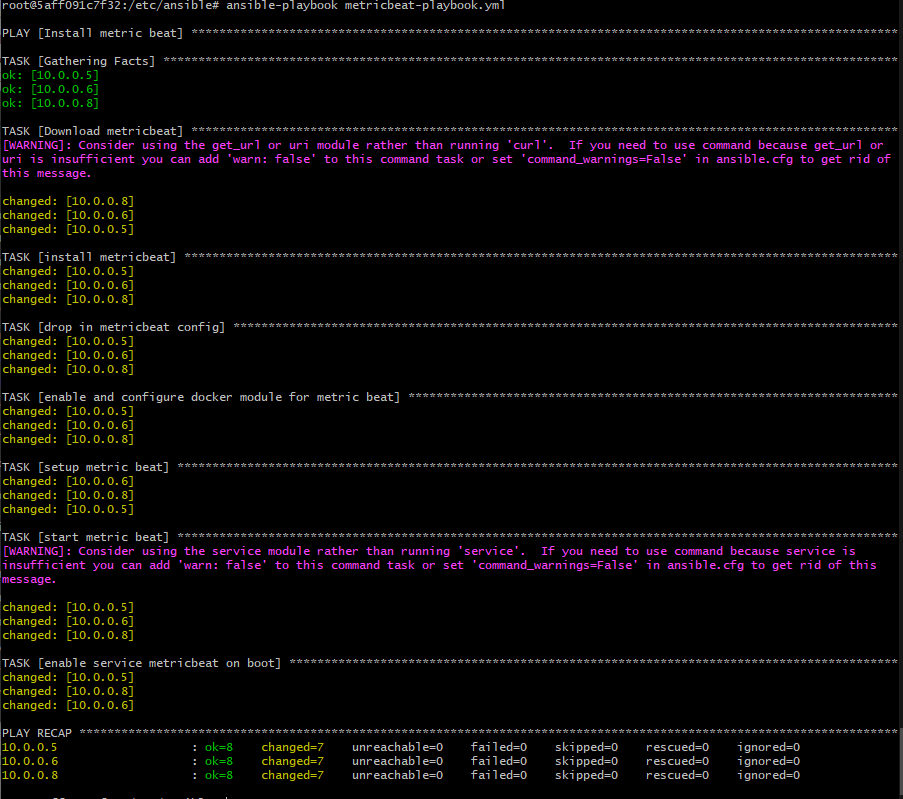
In the Kibana webpage, navigate to Home/Add data/ System Logs.

Copy the file metricbeat-config.yml to /etc/ansible/files.



Copy the metricbeat-playbook.yml file to /etc/ansible.

Run the metricbeat-playbook.yml playbook.



Check on Kibana that logs are being received.