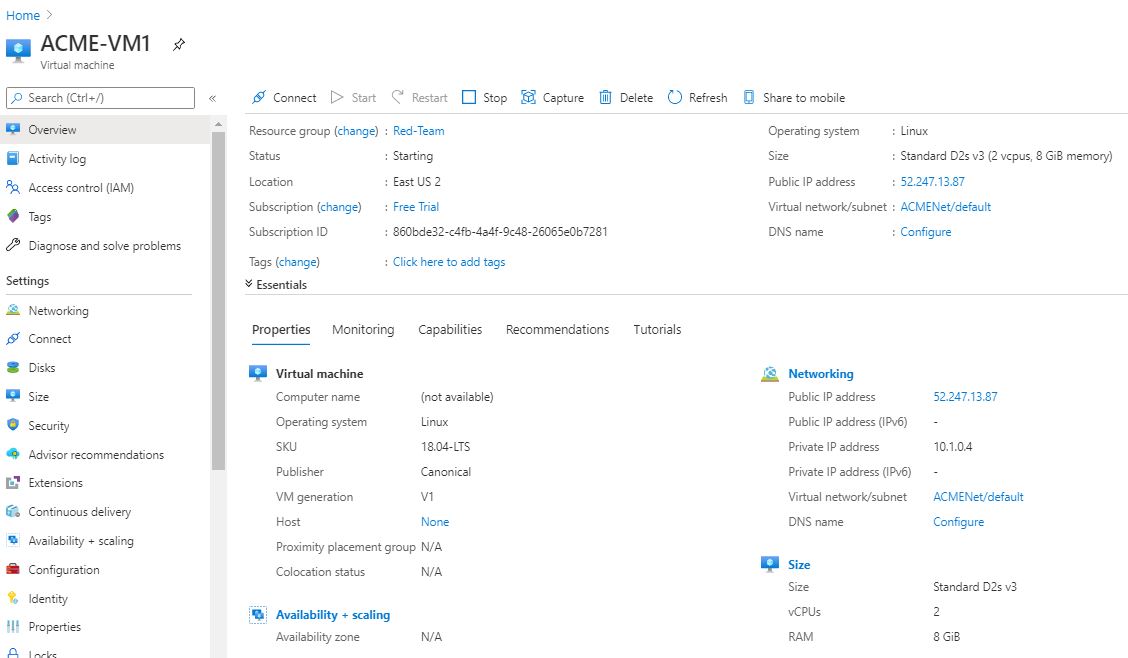
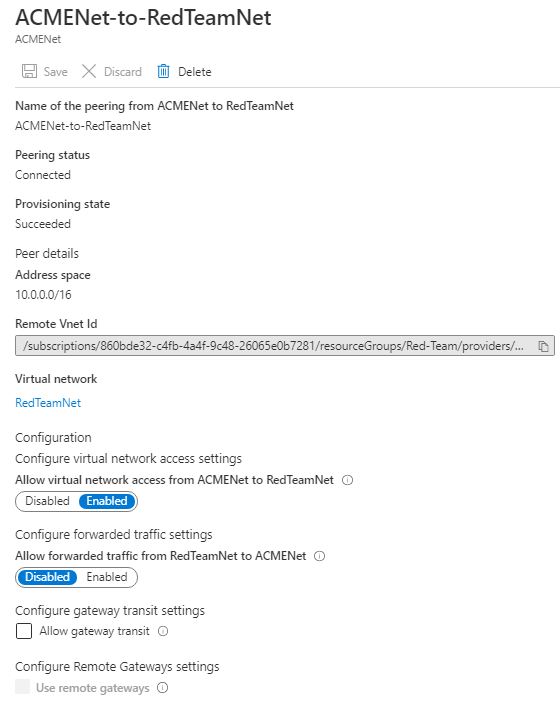
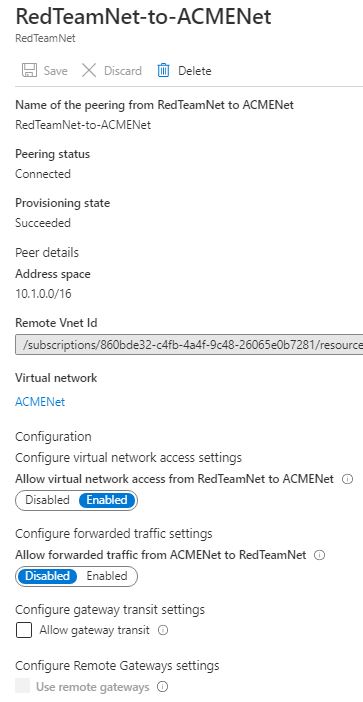
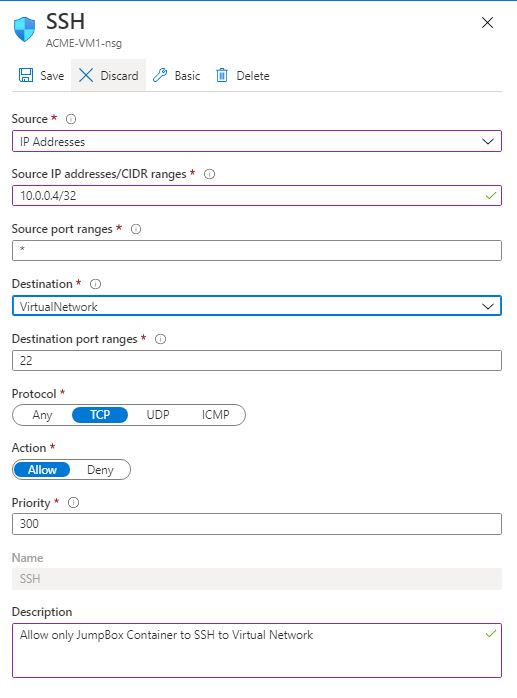
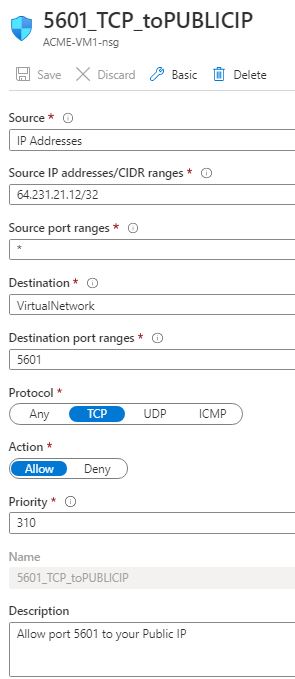
ELK VM Properties.



Peering : ACMENET to REDTEAMNET (Vise Versa)

Firewalls: ACME-VM1-nsg



etc/ansible/hosts

Ansible root : nano /etc/ansible/hosts

[webservers]

## alpha.example.org

## beta.example.org

## 192.168.1.100

## 192.168.1.110

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

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

# If you have multiple hosts following a pattern you can specify

# them like this:

[elk]

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

ELK Installation yml file:

Ansible root# : touch /etc/ansible/install-elk.yml

---  
- name: Configure Elk VM with Docker  
 hosts: elk  
 remote\_user: sysadmin  
 become: true  
 tasks:  
 # Use apt module  
 - name: Install docker.io  
 apt:  
 update\_cache: yes  
 name: docker.io  
 state: present # Use apt module  
 - name: Install pip3  
 apt:  
 force\_apt\_get: yes  
 name: python3-pip  
 state: present # Use pip module  
 - name: Install Docker python module  
 pip:  
 name: docker  
 state: present # Use command module  
 - name: Increase virtual memory  
 command: sysctl -w vm.max\_map\_count=262144 # Use sysctl module  
 - name: Use more memory  
 sysctl:  
 name: vm.max\_map\_count  
 value: "262144"  
 state: present  
 reload: yes # Use docker\_container module  
 - name: download and launch a docker elk container  
 docker\_container:  
 name: elk  
 image: sebp/elk:761  
 state: started  
 restart\_policy: always  
 published\_ports:  
 - 5601:5601  
 - 9200:9200  
 - 5044:5044

To manually start elk, it is needed to login to ansible first then to elk.

Access Jumpbox : ssh -i id\_rsa [sysadmin@52.242.18.55](mailto:sysadmin@52.242.18.55)

Check status of Docker Service: systemctl status docker

Start the Docker Service: sudo service docker start

List Ansible files : sudo docker ps -a

Start the image Ansible : sudo docker start <image-name>

Access the Ansible in Jumpbox in root: sudo docker attach <image-name>

Ansible Image : c1e0a059c0b0

root#: ssh [sysadmin@10.1.0.4](mailto:sysadmin@10.1.0.4)

sudo docker start elk

or sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk:761

Test Kibana on web : <http://[your.ELK-VM.External.IP]:5601/app/kibana>

Public IP : 52.247.13.87

Test Kibana on localhost: sysadmin@10.1.0.4: curl localhost:5601/app/kibana