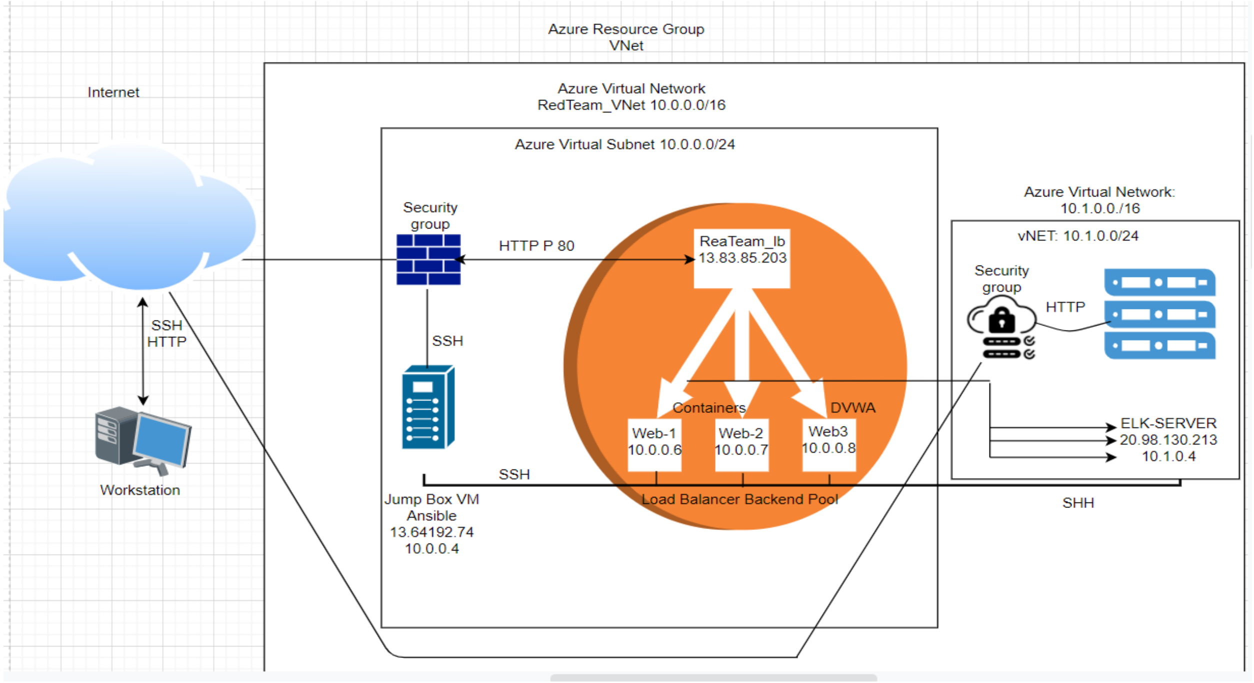
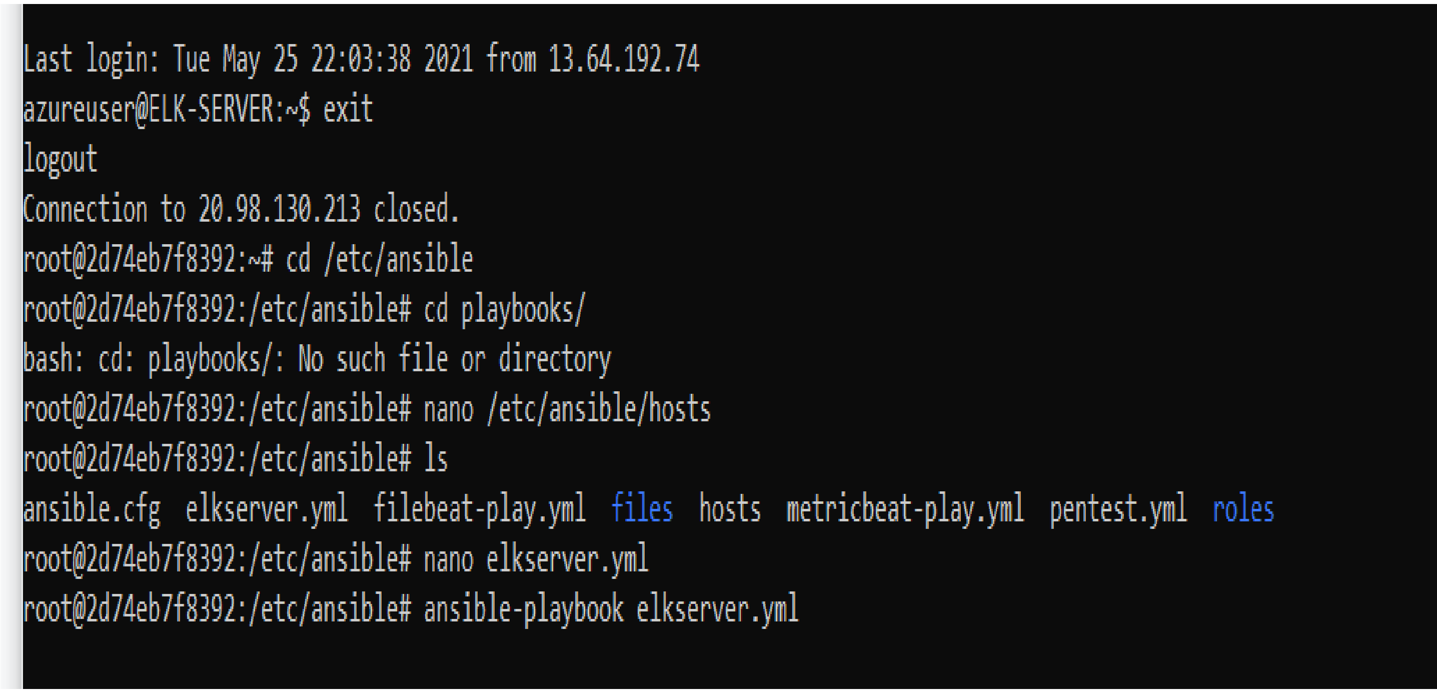
PROJECT I

Cloud security diagram



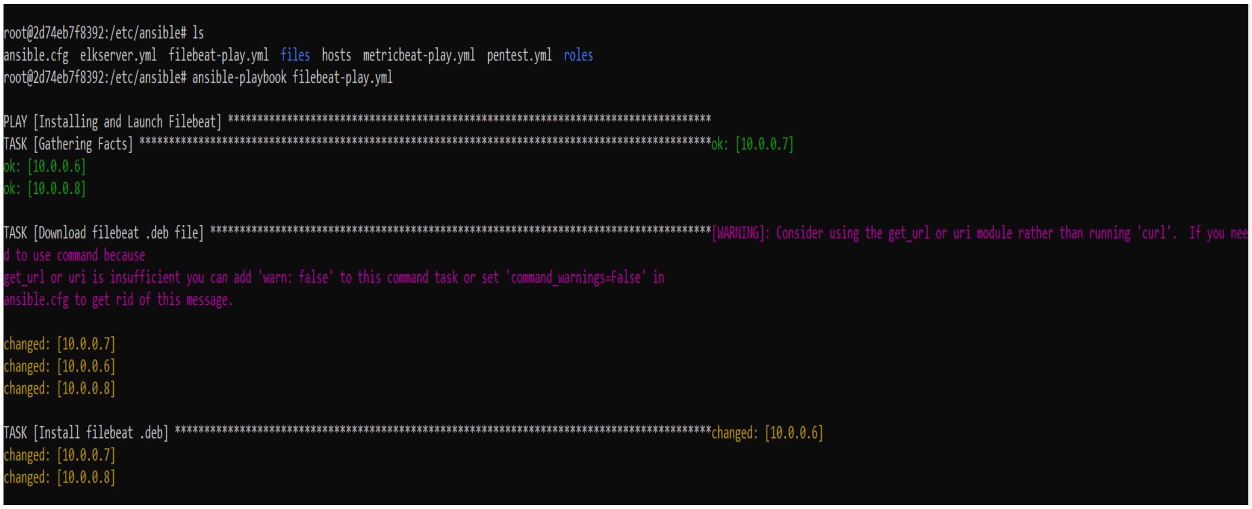
3 PLAYBOOKS AND CONFIGURED FILES

COULD RUN THE ANSIBLE-PLAYBOOK ELKSERVER.YML

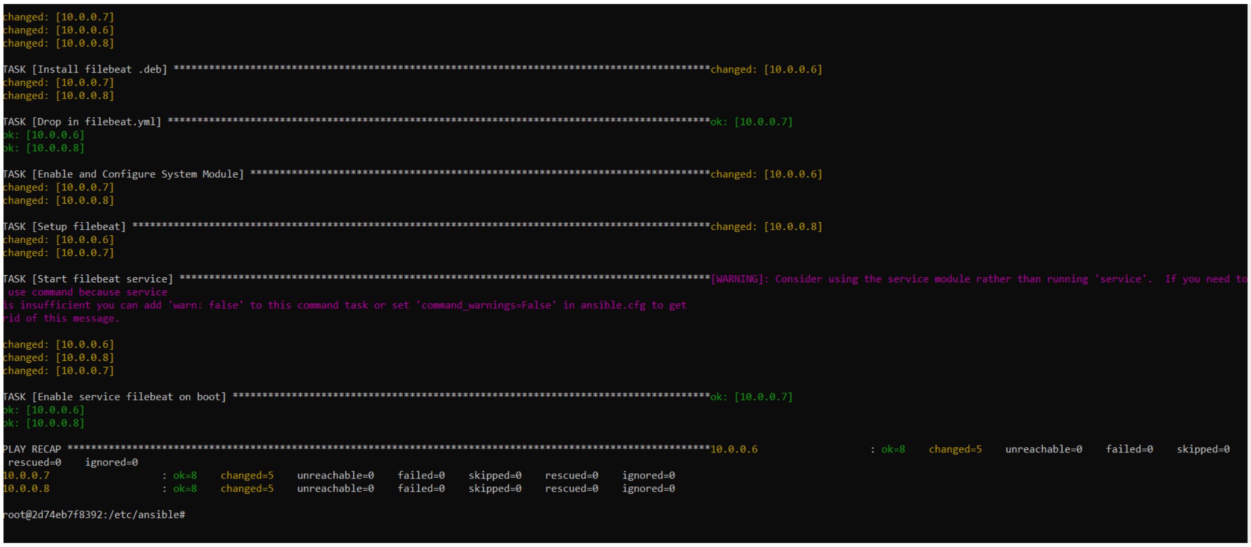


```
Last login: Tue May 25 22:03:38 2021 from 13.64.192.74
azureuser@ELK-SERVER:~$ exit
logout
Connection to 20.98.130.213 closed.
root@2d74eb7f8392:~# cd /etc/ansible
root@2d74eb7f8392:/etc/ansible# cd playbooks/
bash: cd: playbooks/: No such file or directory
root@2d74eb7f8392:/etc/ansible# nano /etc/ansible/hosts
root@2d74eb7f8392:/etc/ansible# ls
ansible.cfg  elkserver.yml  filebeat-play.yml  files  hosts  metricbeat-play.yml  pentest.yml  roles
root@2d74eb7f8392:/etc/ansible# nano elkserver.yml
root@2d74eb7f8392:/etc/ansible# ansible-playbook elkserver.yml
```

ANSIBLE-PLABOOK FILEBEAT-PLAY.YML

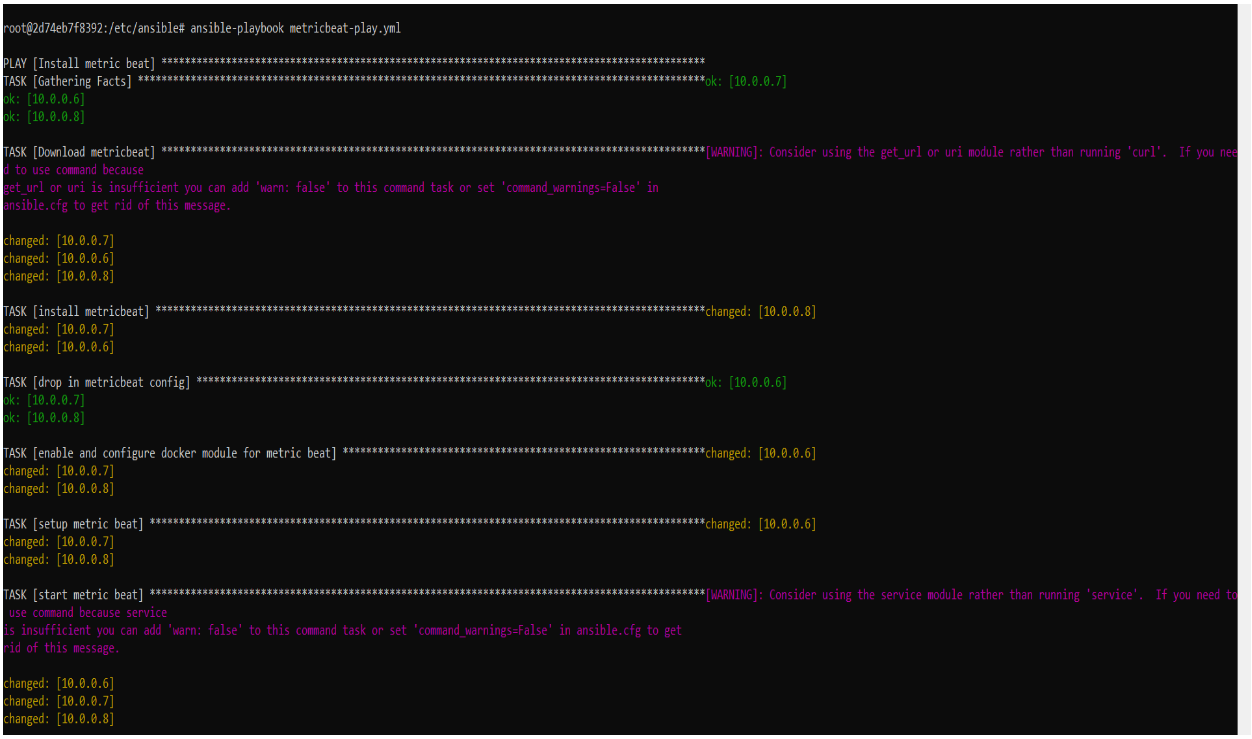


```
root@2d74eb7f8392:/etc/ansible# ls
ansible.cfg  elkserver.yml  filebeat-play.yml  files  hosts  metricbeat-play.yml  pentest.yml  roles
root@2d74eb7f8392:/etc/ansible# ansible-playbook filebeat-play.yml

PLAY [Installing and Launch Filebeat] ********************************************************************************
TASK [Gathering Facts] ***********************************************************************************************ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.8]

TASK [Download filebeat .deb file] ***********************************************************************************[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you nee
d to use command because
get_url or uri is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in
ansible.cfg to get rid of this message.

changed: [10.0.0.7]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [Install filebeat .deb] *****************************************************************************************changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.8]
```

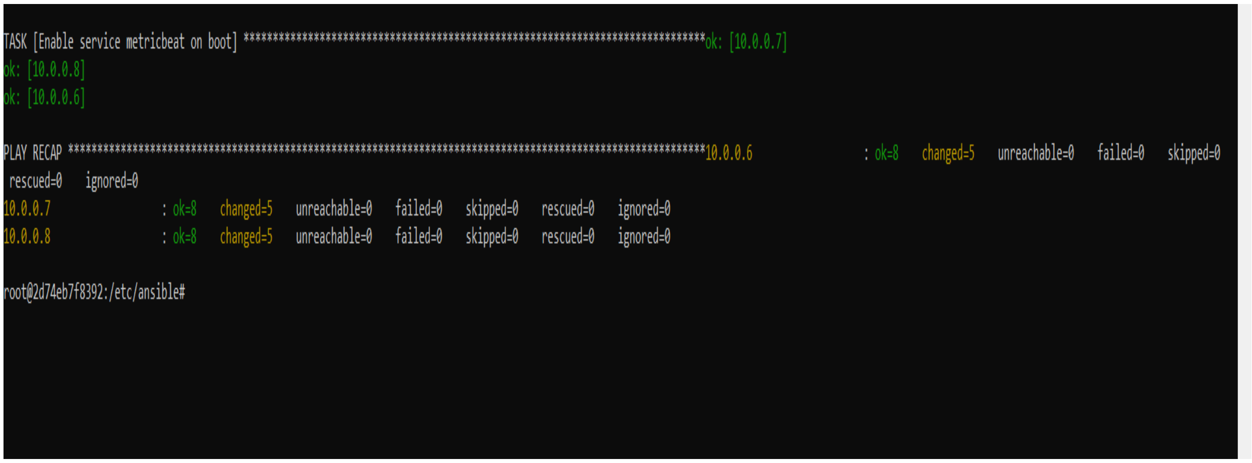


```
changed: [10.0.0.7]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [Install filebeat .deb] *****************************************************************************************changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.8]

TASK [Drop in filebeat.yml] ******************************************************************************************ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.8]

TASK [Enable and Configure System Module] ****************************************************************************changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.8]

TASK [Setup filebeat] ************************************************************************************************changed: [10.0.0.8]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [Start filebeat service] ****************************************************************************************[WARNING]: Consider using the service module rather than running 'service'.  If you need to
 use command because service
is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get
rid of this message.

changed: [10.0.0.6]
changed: [10.0.0.8]
changed: [10.0.0.7]

TASK [Enable service filebeat on boot] *******************************************************************************ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.8]

PLAY RECAP ***********************************************************************************************************10.0.0.6                  : ok=8    changed=5    unreachable=0    failed=0    skipped=0
 rescued=0    ignored=0
10.0.0.7                  : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.8                  : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@2d74eb7f8392:/etc/ansible#
```

ANSIBLE-PLAYBOOK METRICBEAT-PLAY.YML



```
root@2d74eb7f8392:/etc/ansible# ansible-playbook metricbeat-play.yml

PLAY [Install metric beat] *********************************************************************************************
TASK [Gathering Facts] *************************************************************************************************ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.8]

TASK [Download metricbeat] *********************************************************************************************[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you nee
d to use command because
get_url or uri is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in
ansible.cfg to get rid of this message.

changed: [10.0.0.7]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [install metricbeat] **********************************************************************************************changed: [10.0.0.8]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [drop in metricbeat config] ***************************************************************************************ok: [10.0.0.6]
ok: [10.0.0.7]
ok: [10.0.0.8]

TASK [enable and configure docker module for metric beat] **************************************************************changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.8]

TASK [setup metric beat] ***********************************************************************************************changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.8]

TASK [start metric beat] ***********************************************************************************************[WARNING]: Consider using the service module rather than running 'service'.  If you need to
 use command because service
is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get
rid of this message.

changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.8]
```



```
TASK [Enable service metricbeat on boot] *******************************************************************************ok: [10.0.0.7]
ok: [10.0.0.8]
ok: [10.0.0.6]

PLAY RECAP *************************************************************************************************************10.0.0.6                   : ok=8    changed=5    unreachable=0    failed=0    skipped=0
 rescued=0    ignored=0
10.0.0.7                   : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.8                   : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@2d74eb7f8392:/etc/ansible#
```