Last login: Sat Apr 23 18:21:10 on ttys001

Myrons-MacBook-Air-3:~ myronlewisiii$ ssh azureuser@20.213.92.185

Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1022-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Sun Apr 24 23:12:14 UTC 2022

System load: 0.21 Processes: 115

Usage of /: 11.3% of 28.90GB Users logged in: 0

Memory usage: 34% IPv4 address for docker0: 172.17.0.1

Swap usage: 0% IPv4 address for eth0: 10.1.0.4

\* Super-optimized for small spaces - read how we shrank the memory

footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

Last login: Sat Apr 23 22:21:18 2022 from 76.97.131.141

**azureuser@Jumpbox**:**~**$ ssh azureuser@10.1.0.4

azureuser@10.1.0.4: Permission denied (publickey).

**azureuser@Jumpbox**:**~**$ sudo docker start confident\_black

confident\_black

**azureuser@Jumpbox**:**~**$ sudo docker attach confident\_black

root@af014afa16f8:~# ls

filebeat-playbook.yml

root@af014afa16f8:~# cd /etc/ansible/

root@af014afa16f8:/etc/ansible# ls

ansible.cfg **files** hosts install-elk.yml pentest.yml **roles**

root@af014afa16f8:/etc/ansible# cd roles

root@af014afa16f8:/etc/ansible/roles# ls

filebeat-playbook.yml metricbeat-playbook.yml

root@af014afa16f8:/etc/ansible/roles# cd file

bash: cd: file: No such file or directory

root@af014afa16f8:/etc/ansible/roles# cd files

bash: cd: files: No such file or directory

root@af014afa16f8:/etc/ansible/roles# cd ..

root@af014afa16f8:/etc/ansible# cd files

root@af014afa16f8:/etc/ansible/files# ls

filebeat-config.yml metricbeat-config.yml

root@af014afa16f8:/etc/ansible/files# nano filebeat-config.yml

root@af014afa16f8:/etc/ansible/files# cd ..

root@af014afa16f8:/etc/ansible# cd roles

root@af014afa16f8:/etc/ansible/roles# ls

filebeat-playbook.yml metricbeat-playbook.yml

root@af014afa16f8:/etc/ansible/roles# nano filebeat-playbook.yml

root@af014afa16f8:/etc/ansible/roles# cd files

bash: cd: files: No such file or directory

root@af014afa16f8:/etc/ansible/roles# cd ..

root@af014afa16f8:/etc/ansible# cd fikes

bash: cd: fikes: No such file or directory

root@af014afa16f8:/etc/ansible# cd files

root@af014afa16f8:/etc/ansible/files# ls

filebeat-config.yml metricbeat-config.yml

root@af014afa16f8:/etc/ansible/files# nano filebeat-config.yml

root@af014afa16f8:/etc/ansible/files# cd ..

root@af014afa16f8:/etc/ansible# ls

ansible.cfg **files** hosts install-elk.yml pentest.yml **roles**

root@af014afa16f8:/etc/ansible# cd hosts

bash: cd: hosts: Not a directory

root@af014afa16f8:/etc/ansible# nano hosts

root@af014afa16f8:/etc/ansible# cd files

root@af014afa16f8:/etc/ansible/files# ls

filebeat-config.yml metricbeat-config.yml

root@af014afa16f8:/etc/ansible/files# nano filebeat-config.yml

root@af014afa16f8:/etc/ansible/files# Connection to 20.213.92.185 closed by remote host.

Connection to 20.213.92.185 closed.

Myrons-MacBook-Air-3:~ myronlewisiii$

[Restored May 5, 2022 at 2:43:05 PM]

Last login: Sun Apr 24 19:11:48 on ttys002

Myrons-Air-3:~ myronlewisiii$ ssh azureuser@20.213.92.185

ssh: connect to host 20.213.92.185 port 22: Operation timed out

Myrons-Air-3:~ myronlewisiii$ ssh azureuser@20.213.92.185

ssh: connect to host 20.213.92.185 port 22: Operation timed out

Myrons-Air-3:~ myronlewisiii$ ssh azureuser@20.213.92.185

Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1022-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Thu May 5 22:52:56 UTC 2022

System load: 0.03 Processes: 109

Usage of /: 11.6% of 28.90GB Users logged in: 0

Memory usage: 36% IPv4 address for docker0: 172.17.0.1

Swap usage: 0% IPv4 address for eth0: 10.1.0.4

\* Super-optimized for small spaces - read how we shrank the memory

footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

15 updates can be applied immediately.

11 of these updates are standard security updates.

To see these additional updates run: apt list --upgradable

Last login: Tue Apr 26 23:27:02 2022 from 76.97.131.141

**azureuser@Jumpbox**:**~**$ sudo docker start confident\_black

confident\_black

**azureuser@Jumpbox**:**~**$ sudo docker attach confident\_black

root@af014afa16f8:~# cd /etc/

root@af014afa16f8:/etc# ls

adduser.conf fstab **ld.so.conf.d** **os-release** **rmt**

**alternatives** gai.conf **ldap** pam.conf **security**

**ansible** group legal **pam.d** **selinux**

**apt** group- libaudit.conf passwd shadow

bash.bashrc gshadow login.defs profile shells

bindresvport.blacklist gshadow- **logrotate.d** **profile.d** **skel**

**ca-certificates** **gss** lsb-release **python3** **ssh**

ca-certificates.conf host.conf machine-id **python3.8** **ssl**

**cron.d** hostname mailcap **rc0.d** subgid

**cron.daily** hosts mailcap.order **rc1.d** subuid

debconf.conf **init.d** mime.types **rc2.d** sysctl.conf

debian\_version inputrc mke2fs.conf **rc3.d** **sysctl.d**

**default** issue **mtab** **rc4.d** **systemd**

deluser.conf issue.net nanorc **rc5.d** **terminfo**

**dpkg** **kernel** networks **rc6.d** **update-motd.d**

e2scrub.conf ld.so.cache nsswitch.conf **rcS.d** **vim**

environment ld.so.conf **opt** resolv.conf xattr.conf

root@af014afa16f8:/etc# cd /ansible/

bash: cd: /ansible/: No such file or directory

root@af014afa16f8:/etc# cd /etc/ansible/

root@af014afa16f8:/etc/ansible# ls

ansible.cfg **files** hosts install-elk.yml pentest.yml **roles**

root@af014afa16f8:/etc/ansible# nano ansible.cfg

root@af014afa16f8:/etc/ansible# nano install-elk.yml

GNU nano 4.8 install-elk.yml

---

- name: Configure Elk VM with Docker

hosts: elk

remote\_user: azureuser

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: 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 (It will default to pip3)

- 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

# Please list the ports that ELK runs on

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

# Use systemd module

- name: Enable service docker on boot

systemd:

name: docker

enabled: yes