```
# Generate local ssh key
Joses-MacBook-Pro$ ssh-keygen
Generating public/private rsa key pair.
Joses-MacBook-Pro$ ssh azadmin@20.213.127.123
The authenticity of host '20.213.127.123 (20.213.127.123)' can't be established.
ECDSA key fingerprint is SHA256:PZ2NPjxb1JQnL23GA6jhj06WRO3fobmytSZCbO62ZAo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.213.127.123' (ECDSA) to the list of known hosts.
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 23:54:57 UTC 2022

  System load:  0.08              Processes:             106
  Usage of /:   4.8% of 28.90GB   Users logged in:       0
  Memory usage: 25%               IPv4 address for eth0: 10.0.0.5
  Swap usage:   0%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azadmin@JumpBoxProvisioner:~$ sudo -l
Matching Defaults entries for azadmin on JumpBoxProvisioner:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b
in

User azadmin may run the following commands on JumpBoxProvisioner:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether 00:0d:3a:6b:0d:49 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.5/24 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20d:3aff:fe6b:d49/64 scope link
       valid_lft forever preferred_lft forever
azadmin@JumpBoxProvisioner:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]

Reading state information... Done
15 packages can be upgraded. Run 'apt list --upgradable' to see them.
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
.
Processing triggers for systemd (245.4-4ubuntu3.16) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for dbus (1.12.16-2ubuntu2.1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.7) ...
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker pull cyberxsecurity/ubuntu:bionic
bionic: Pulling from cyberxsecurity/ubuntu
5bed26d33875: Pull complete
f11b29a9c730: Pull complete
930bda195c84: Pull complete
78bf9a5ad49e: Pull complete
Digest: sha256:e5dd9dbb37df5b731a6688fa49f4003359f6f126958c9c928f937bec69836320
Status: Downloaded newer image for cyberxsecurity/ubuntu:bionic
docker.io/cyberxsecurity/ubuntu:bionic
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker run -ti cyberxsecurity/ubuntu:bionic bash
root@32dfe6bd7804:/#
root@32dfe6bd7804:/#
root@32dfe6bd7804:/# id
uid=0(root) gid=0(root) groups=0(root)
root@32dfe6bd7804:/# hostname
32dfe6bd7804
root@32dfe6bd7804:/#
root@32dfe6bd7804:/# exit
exit
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset:
enabled)
     Active: active (running) since Fri 2022-05-06 00:17:20 UTC; 27min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 14380 (dockerd)
      Tasks: 9
     Memory: 131.1M
     CGroup: /system.slice/docker.service
             └─14380 /usr/bin/dockerd -H fd:// --
containerd=/run/containerd/containerd.sock
```

```
May 06 00:17:19 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:19.882225378Z" level=warning msg="Your kernel does not suppor
May 06 00:17:19 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:19.882465981Z" level=info msg="Loading containers: start."
May 06 00:17:20 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:20.418103961Z" level=info msg="Default bridge (docker0) is as
May 06 00:17:20 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:20.500448545Z" level=info msg="Loading containers: done."
May 06 00:17:20 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:20.571050960Z" level=warning msg="Not using native diff for o
May 06 00:17:20 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:20.571554363Z" level=info msg="Docker daemon" commit="20.10.1
May 06 00:17:20 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:20.571798464Z" level=info msg="Daemon has completed initializ
May 06 00:17:20 JumpBoxProvisioner systemd[1]: Started Docker Application Container
Engine.
May 06 00:17:20 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:17:20.606516669Z" level=info msg="API listen on /run/docker.sock"
May 06 00:22:19 JumpBoxProvisioner dockerd[14380]: time="2022-05-
06T00:22:19.182679594Z" level=info msg="ignoring event" container=32df


azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker pull cyberxsecurity/ansible
Using default tag: latest
latest: Pulling from cyberxsecurity/ansible
345e3491a907: Pull complete
57671312ef6f: Pull complete
5e9250ddb7d0: Pull complete
06c2579b8983: Pull complete
Digest: sha256:1e59530cfc0fb86b8fefdc2c7b0666e053c9f53a339639fb34e99ffee9812730
Status: Downloaded newer image for cyberxsecurity/ansible:latest
docker.io/cyberxsecurity/ansible:latest
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker run -ti cyberxsecurity/ansible:latest bash
root@ca6d91c736bc:~#
root@ca6d91c736bc:~# ls -l
total 0
root@ca6d91c736bc:~# ls /
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  packer-files
proc  root  run  sbin  srv  sys  tmp  usr  var
root@ca6d91c736bc:~#
root@ca6d91c736bc:~# exit
exit
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker images
REPOSITORY               TAG       IMAGE ID       CREATED         SIZE
cyberxsecurity/ansible   latest    7d2d9fa20ccf   11 months ago   754MB
cyberxsecurity/ubuntu    bionic    4e5021d210f6   2 years ago     64.2MB
azadmin@JumpBoxProvisioner:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether 00:0d:3a:6b:0d:49 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.5/24 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20d:3aff:fe6b:d49/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
group default
    link/ether 02:42:93:9c:1b:f3 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:93ff:fe9c:1bf3/64 scope link
       valid_lft forever preferred_lft forever
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                            COMMAND                  CREATED
STATUS                         PORTS     NAMES
ca6d91c736bc   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   40 minutes ago
Exited (0) 40 minutes ago                relaxed_mclean
32dfe6bd7804   cyberxsecurity/ubuntu:bionic    "bash"                   About an hour
ago   Exited (0) About an hour ago             crazy_liskov
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker start relaxed_mclean
relaxed_mclean
azadmin@JumpBoxProvisioner:~$ sudo docker ps
CONTAINER ID   IMAGE                            COMMAND                  CREATED
STATUS          PORTS     NAMES
ca6d91c736bc   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   44 minutes ago
Up 42 seconds             relaxed_mclean
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker attach relaxed_mclean
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~# ssh-keygen
Generating public/private rsa key pair.
root@ca6d91c736bc:~# ssh sysadmin@10.0.0.6
The authenticity of host '10.0.0.6 (10.0.0.6)' can't be established.
ECDSA key fingerprint is SHA256:BhD6YkqlDeoABZjZUaGFYMQOS4smURxg7VLPbndcCzQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.6' (ECDSA) to the list of known hosts.
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 Fri May  6 01:45:27 UTC 2022

  System load:  0.0               Processes:             106
  Usage of /:   4.9% of 28.90GB   Users logged in:       0
  Memory usage: 12%               IPv4 address for eth0: 10.0.0.6
  Swap usage:   0%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

sysadmin@Web-1:~$
sysadmin@Web-1:~$ ls
sysadmin@Web-1:~$ ls -l
total 0
sysadmin@Web-1:~$ exit
logout
Connection to 10.0.0.6 closed.
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~# cd /etc/ansible
root@ca6d91c736bc:/etc/ansible# ls
ansible.cfg  hosts
root@ca6d91c736bc:/etc/ansible# nano ansible.cfg
root@ca6d91c736bc:/etc/ansible#
root@ca6d91c736bc:/etc/ansible# nano hosts
root@ca6d91c736bc:/etc/ansible#
root@ca6d91c736bc:/etc/ansible# ansible webservers -m ping
10.0.0.6 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.0.8 | UNREACHABLE! => {
    "changed": false,
    "msg": "Failed to connect to the host via ssh: sysadmin@10.0.0.8: Permission
denied (publickey).",
    "unreachable": true
}
root@ca6d91c736bc:/etc/ansible# ssh sysadmin@10.0.0.8
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 Fri May  6 02:06:17 UTC 2022

  System load:  0.0               Processes:             106
  Usage of /:   4.9% of 28.90GB   Users logged in:       0
  Memory usage: 12%               IPv4 address for eth0: 10.0.0.8
  Swap usage:   0%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
```

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

sysadmin@Web-2:~$
sysadmin@Web-2:~$ exit
logout
Connection to 10.0.0.8 closed.
root@ca6d91c736bc:/etc/ansible# ansible webservers -m ping
10.0.0.6 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.0.8 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
root@ca6d91c736bc:/etc/ansible# ansible webservers -m ping
10.0.0.6 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.0.8 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
root@ca6d91c736bc:/etc/ansible# exit
exit
azadmin@JumpBoxProvisioner:~$ exit
logout
Connection to 20.213.127.123 closed.
Joses-MacBook-Pro$ ssh azadmin@20.213.127.123
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 Sat May  7 14:02:37 UTC 2022

  System load:  0.01              Processes:                117
  Usage of /:   9.8% of 28.90GB   Users logged in:          0
  Memory usage: 35%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.0.0.5


14 updates can be applied immediately.
13 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Thu May  5 23:55:00 2022 from 75.40.54.33
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker images
REPOSITORY               TAG       IMAGE ID       CREATED         SIZE
cyberxsecurity/ansible   latest    7d2d9fa20ccf   11 months ago   754MB
cyberxsecurity/ubuntu    bionic    4e5021d210f6   2 years ago     64.2MB
```

```
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                           COMMAND                  CREATED
STATUS                     PORTS     NAMES
ca6d91c736bc   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   37 hours ago
Exited (0) 36 hours ago             relaxed_mclean
32dfe6bd7804   cyberxsecurity/ubuntu:bionic    "bash"                   38 hours ago
Exited (0) 38 hours ago             crazy_liskov
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker start relaxed_mclean
relaxed_mclean
azadmin@JumpBoxProvisioner:~$ sudo docker ps
CONTAINER ID   IMAGE                           COMMAND                  CREATED
STATUS          PORTS     NAMES
ca6d91c736bc   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   37 hours ago
Up 16 seconds             relaxed_mclean
azadmin@JumpBoxProvisioner:~$
azadmin@JumpBoxProvisioner:~$ sudo docker attach relaxed_mclean
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~# ansible webservers -m ping
10.0.0.8 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.0.6 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
root@ca6d91c736bc:~#
root@ca6d91c736bc:~#
root@ca6d91c736bc:~# cd /etc/andsible
bash: cd: /etc/andsible: No such file or directory
root@ca6d91c736bc:~# cd /etc/ansible
root@ca6d91c736bc:/etc/ansible# ls
ansible.cfg  hosts
root@ca6d91c736bc:/etc/ansible#
root@ca6d91c736bc:/etc/ansible# nano pentest.yml
root@ca6d91c736bc:/etc/ansible# ls
ansible.cfg  hosts  pentest.yml
root@ca6d91c736bc:/etc/ansible# nano pentest.yml
root@ca6d91c736bc:/etc/ansible# ls
ansible.cfg  hosts  pentest.yml
root@ca6d91c736bc:/etc/ansible# nano pentest.yml
root@ca6d91c736bc:/etc/ansible# nano pentest.yml
root@ca6d91c736bc:/etc/ansible#
root@ca6d91c736bc:/etc/ansible# ansible-playbook pentest.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may
result in incorrectly calculated text widths that can cause Display to print incorrect
line lengths

PLAY [Config Web VM with Docker]
**************************************************************************************
***************************************************

TASK [Gathering Facts]
**************************************************************************************
*************************************************************
ok: [10.0.0.6]
ok: [10.0.0.8]
```

```
TASK [docker.io]
***************************************************************************************
********************************************************************
changed: [10.0.0.8]
changed: [10.0.0.6]

TASK [Install pip3]
***************************************************************************************
*****************************************************************
changed: [10.0.0.8]
changed: [10.0.0.6]

TASK [Install Docker pyhton module]
***************************************************************************************
*************************************************
changed: [10.0.0.8]
changed: [10.0.0.6]

TASK [download and launch a docker web container]
***************************************************************************************
***********************************
[DEPRECATION WARNING]: The container_default_behavior option will change its default
value from "compatibility" to "no_defaults" in community.docker 2.0.0. To remove
this warning, please specify an explicit value for it now. This feature will be
removed from community.docker in version 2.0.0. Deprecation warnings can be disabled
by
setting deprecation_warnings=False in ansible.cfg.
changed: [10.0.0.8]
changed: [10.0.0.6]

TASK [enable docker service]
***************************************************************************************
********************************************************
ok: [10.0.0.8]
ok: [10.0.0.6]

PLAY RECAP
***************************************************************************************
**************************************************************************
10.0.0.6                   : ok=6    changed=4    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0
10.0.0.8                   : ok=6    changed=4    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0

root@ca6d91c736bc:/etc/ansible#
root@ca6d91c736bc:/etc/ansible# nano pentest.yml
root@ca6d91c736bc:/etc/ansible#
root@ca6d91c736bc:/etc/ansible# ssh sysadmin@10.0.0.6
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 Sat May  7 15:20:02 UTC 2022

  System load:  0.0               Processes:                122
  Usage of /:   11.1% of 28.90GB  Users logged in:          0
  Memory usage: 28%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.0.0.6
 * 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.
13 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Sat May  7 15:01:43 2022 from 10.0.0.5
sysadmin@Web-1:~$
sysadmin@Web-1:~$
sysadmin@Web-1:~$ curl localhost/setup.php
<!DOCTYPE html>

root@1170f08f2e53:~#
root@1170f08f2e53:~#
root@1170f08f2e53:~#
root@1170f08f2e53:~# nano /etc/ansible/install-elk.yml
root@1170f08f2e53:~# ansible-playbook /etc/ansible/install-elk.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may
result in incorrectly calculated text widths that can cause Display to
print incorrect line lengths

PLAY [Config Elk-Server]
**************************************************************************************
******************************************

TASK [Gathering Facts]
**************************************************************************************
********************************************
ok: [10.1.0.4]

TASK [docker.io]
**************************************************************************************
**************************************************
changed: [10.1.0.4]

TASK [Install pip3]
**************************************************************************************
***********************************************
changed: [10.1.0.4]

TASK [Install Docker python module]
**************************************************************************************
*******************************
changed: [10.1.0.4]

TASK [Increase virtual memory]
**************************************************************************************
************************************
changed: [10.1.0.4]

TASK [Use more memory]
**************************************************************************************
********************************************
changed: [10.1.0.4]
```

```
TASK [download and launch a docker elk container]
**************************************************************************************
*****************
[DEPRECATION WARNING]: The container_default_behavior option will change its default
value from "compatibility" to "no_defaults" in community.docker
2.0.0. To remove this warning, please specify an explicit value for it now. This
feature will be removed from community.docker in version 2.0.0.
Deprecation warnings can be disabled by setting deprecation_warnings=False in
ansible.cfg.
changed: [10.1.0.4]

TASK [Enable docker service]
**************************************************************************************
**************************************
ok: [10.1.0.4]

PLAY RECAP
**************************************************************************************
********************************************************
10.1.0.4                   : ok=8    changed=6    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0

root@1170f08f2e53:~#
root@1170f08f2e53:~# ssh sysadmin@10.1.0.4
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 2.0


10 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Fri May 13 00:44:51 2022 from 10.0.0.4
sysadmin@ELK-Server:~$ docker ps
Got permission denied while trying to connect to the Docker daemon socket at
unix:///var/run/docker.sock: Get
"http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json": dial unix
/var/run/docker.sock: connect: permission denied
sysadmin@ELK-Server:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED              STATUS
PORTS
NAMES
827668caee67   sebp/elk:761   "/usr/local/bin/star…"   About a minute ago   Up About a
minute   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp,
9300/tcp   elk
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ curl localhost:5601/app/kibana
<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><meta http-equiv="X-UA-
 class="kibanaWelcomeText">This Kibana installation has strict security requirements
enabled that your current browser does not meet.</div></div><script>
            // Since this is an unsafe inline script, this code will not run
            // in browsers that support content security policy(CSP). This is
            // intentional as we check for the existence of __kbnCspNotEnforced__ in
            // bootstrap.
            window.__kbnCspNotEnforced__ = true;
          </script><script
src="/bundles/app/kibana/bootstrap.js"></script></body></html>sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ ping
ping: usage error: Destination address required
sysadmin@ELK-Server:~$ 20.190.96.123
20.190.96.123: command not found
sysadmin@ELK-Server:~$ ping 20.190.96.123
PING 20.190.96.123 (20.190.96.123) 56(84) bytes of data.
^C
--- 20.190.96.123 ping statistics ---
22 packets transmitted, 0 received, 100% packet loss, time 21503ms

sysadmin@ELK-Server:~$ ping 75.40.54.33
PING 75.40.54.33 (75.40.54.33) 56(84) bytes of data.
^C
--- 75.40.54.33 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8200ms

sysadmin@ELK-Server:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED          STATUS
PORTS
NAMES
827668caee67   sebp/elk:761   "/usr/local/bin/star…"   29 minutes ago   Up 29 minutes
0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
sysadmin@ELK-Server:~$ sudo netstat -antpl
sudo: netstat: command not found
sysadmin@ELK-Server:~$ sudo apt install netstat
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package netstat
sysadmin@ELK-Server:~$ netstat

Command 'netstat' not found, but can be installed with:

sudo apt install net-tools

sysadmin@ELK-Server:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 10 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64
1.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 0s (1579 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 64420 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ sudo netstat -antpl
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:5044            0.0.0.0:*               LISTEN
10417/docker-proxy
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
567/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1038/sshd: /usr/sbi
tcp        0      0 127.0.0.1:43095         0.0.0.0:*               LISTEN
2813/containerd
tcp        0      0 0.0.0.0:5601            0.0.0.0:*               LISTEN
10403/docker-proxy
tcp        0      0 0.0.0.0:9200            0.0.0.0:*               LISTEN
10390/docker-proxy
tcp        0      0 10.1.0.4:53000          23.101.248.31:80        TIME_WAIT   -
tcp        0    196 10.1.0.4:22             10.0.0.4:37524          ESTABLISHED
10783/sshd: sysadmi
tcp6       0      0 :::22                   :::*                    LISTEN
1038/sshd: /usr/sbi
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ exit
logout
Connection to 10.1.0.4 closed.
root@1170f08f2e53:~#
root@1170f08f2e53:~# ssh sysadmin@10.1.0.4
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri May 13 01:44:30 UTC 2022

  System load:  0.0                Processes:                128
  Usage of /:   16.2% of 28.90GB   Users logged in:          0
  Memory usage: 73%                IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                 IPv4 address for eth0:    10.1.0.4


10 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Fri May 13 00:45:23 2022 from 10.0.0.4
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ exit
logout
Connection to 10.1.0.4 closed.
root@1170f08f2e53:~# ssh sysadmin@10.1.0.4
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri May 13 01:45:51 UTC 2022
  System load:  0.0               Processes:                128
  Usage of /:   16.2% of 28.90GB   Users logged in:          0
  Memory usage: 73%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.1.0.4


10 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Fri May 13 01:44:31 2022 from 10.0.0.4
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED             STATUS
PORTS
NAMES
827668caee67   sebp/elk:761   "/usr/local/bin/star…"   About an hour ago   Up About an
hour   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp,
9300/tcp   elk
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ exit
logout
Connection to 10.1.0.4 closed.
root@1170f08f2e53:~# ls -l
total 0
root@1170f08f2e53:~# nano /etc/ansible/install-elk.yml
root@1170f08f2e53:~#
root@1170f08f2e53:~# ssh sysadmin@10.1.0.4
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri May 13 02:27:43 UTC 2022

  System load:  0.0               Processes:                128
  Usage of /:   16.2% of 28.90GB   Users logged in:          0
  Memory usage: 73%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.1.0.4


10 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Fri May 13 01:45:52 2022 from 10.0.0.4
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ sudo netstat -antpl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:5044            0.0.0.0:*               LISTEN
10417/docker-proxy
```

```
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
567/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1038/sshd: /usr/sbi
tcp        0      0 127.0.0.1:43095         0.0.0.0:*               LISTEN
2813/containerd
tcp        0      0 0.0.0.0:5601            0.0.0.0:*               LISTEN
10403/docker-proxy
tcp        0      0 0.0.0.0:9200            0.0.0.0:*               LISTEN
10390/docker-proxy
tcp        0    196 10.1.0.4:22             10.0.0.4:37530          ESTABLISHED
11975/sshd: sysadmi
tcp6       0      0 :::22                   :::*                    LISTEN
1038/sshd: /usr/sbi
sysadmin@ELK-Server:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED       STATUS
PORTS
NAMES
827668caee67   sebp/elk:761   "/usr/local/bin/star…"   2 hours ago   Up 2 hours
0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$
sysadmin@ELK-Server:~$ sudo netstat -antpl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:5044            0.0.0.0:*               LISTEN
10417/docker-proxy
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
567/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1038/sshd: /usr/sbi
tcp        0      0 127.0.0.1:43095         0.0.0.0:*               LISTEN
2813/containerd
tcp        0      0 0.0.0.0:5601            0.0.0.0:*               LISTEN
10403/docker-proxy
tcp        0      0 0.0.0.0:9200            0.0.0.0:*               LISTEN
10390/docker-proxy
tcp        0    196 10.1.0.4:22             10.0.0.4:37530          ESTABLISHED
11975/sshd: sysadmi
tcp6       0      0 :::22                   :::*                    LISTEN
1038/sshd: /usr/sbi
sysadmin@ELK-Server:~$ sudo netstat -antpl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:5044            0.0.0.0:*               LISTEN
10417/docker-proxy
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
567/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1038/sshd: /usr/sbi
tcp        0      0 127.0.0.1:43095         0.0.0.0:*               LISTEN
2813/containerd
tcp        0      0 0.0.0.0:5601            0.0.0.0:*               LISTEN
10403/docker-proxy
tcp        0      0 0.0.0.0:9200            0.0.0.0:*               LISTEN
10390/docker-proxy
tcp        0    196 10.1.0.4:22             10.0.0.4:37530          ESTABLISHED
11975/sshd: sysadmi
```

```
tcp6       0      0 :::22                   :::*                    LISTEN
1038/sshd: /usr/sbi
sysadmin@ELK-Server:~$ Connection to 10.1.0.4 closed by remote host.
Connection to 10.1.0.4 closed.
root@1170f08f2e53:~# Connection to 20.248.195.51 closed by remote host.
Connection to 20.248.195.51 closed.
Joses-MacBook-Pro:~ yennicastilloespinosa$ ssh sysadmin@20.213.85.255
The authenticity of host '20.213.85.255 (20.213.85.255)' can't be established.
ECDSA key fingerprint is SHA256:t68KFCLyMcWUSSWQcTNseF0olfeDf22+42XjnXm+dJI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.213.85.255' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat May 14 14:06:01 UTC 2022

  System load:  0.0                Processes:                108
  Usage of /:   10.7% of 28.90GB   Users logged in:          0
  Memory usage: 35%                IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                 IPv4 address for eth0:    10.0.0.4

 * 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

9 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Thu May 12 23:40:21 2022 from 75.40.54.33
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset:
enabled)
     Active: active (running) since Sat 2022-05-14 13:57:34 UTC; 9min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 968 (dockerd)
      Tasks: 8
     Memory: 118.2M
     CGroup: /system.slice/docker.service
             └─968 /usr/bin/dockerd -H fd:// --
containerd=/run/containerd/containerd.sock

May 14 13:57:32 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:32.316143967Z" level=warning msg="Your kernel does n
May 14 13:57:32 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:32.316150567Z" level=warning msg="Your kernel does n
May 14 13:57:32 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:32.316871981Z" level=info msg="Loading containers: s
May 14 13:57:33 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:33.157401946Z" level=info msg="Default bridge (docke
May 14 13:57:33 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:33.323810527Z" level=info msg="Loading containers: d
```

```
May 14 13:57:33 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:33.924378849Z" level=warning msg="Not using native d
May 14 13:57:33 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:33.924702855Z" level=info msg="Docker daemon" commit
May 14 13:57:33 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:33.936820879Z" level=info msg="Daemon has completed
May 14 13:57:34 Jump-Box-Provisioner systemd[1]: Started Docker Application Container
Engine.
May 14 13:57:34 Jump-Box-Provisioner dockerd[968]: time="2022-05-
14T13:57:34.131981693Z" level=info msg="API listen on /run/do


sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker images
REPOSITORY              TAG       IMAGE ID       CREATED         SIZE
cyberxsecurity/ansible   latest    7d2d9fa20ccf   11 months ago   754MB
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                           COMMAND                  CREATED
STATUS                       PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible          "/bin/sh -c /bin/bas…"   3 days ago
Exited (137) 35 hours ago              sweet_robinson
7f81a2eaa9ac   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   3 days ago
Exited (0) 3 days ago                  gracious_chandrasekhar
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker start sweet_robinson
sweet_robinson
sysadmin@Jump-Box-Provisioner:~$ sudo docker attach sweet_robinson
root@1170f08f2e53:~#
root@1170f08f2e53:~# ls -l
total 0
root@1170f08f2e53:~# cd /etc/ansible
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  hosts  install-elk.yml  pentest.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# curl
https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b7
2586fbe148c11f9c87bf96a63cb25760/Filebeat >> /etc/ansible/filebeat-config.yml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 73112  100 73112    0     0   463k      0 --:--:-- --:--:-- --:--:--  463k
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  hosts  install-elk.yml  pentest.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# touch filebeat-playbook.yml
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
pentest.yml
root@1170f08f2e53:/etc/ansible# nano filebeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/# ansible-playbook filebeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may
result in incorrectly calculated text widths that can cause Display to print incorrect
line lengths

PLAY [Installing and Launch Filebeat]
**************************************************************************************
**************************************************************************************
**
```

```
TASK [Gathering Facts]
***************************************************************************************
***************************************************************************************
*****************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Download filebeat .deb file]
***************************************************************************************
***************************************************************************************
*****
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Install filebeat .deb]
***************************************************************************************
***************************************************************************************
***********
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Drop in filebeat.yml]
***************************************************************************************
***************************************************************************************
************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [Enable and Configure System Module]
***************************************************************************************
*************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Setup filebeat]
***************************************************************************************
***************************************************************************************
******************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Start filebeat service]
***************************************************************************************
***************************************************************************************
**********
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Enable service filebeat on boot]
***************************************************************************************
***************************************************************************************
*
changed: [10.0.0.5]
changed: [10.0.0.6]

PLAY RECAP
***************************************************************************************
***************************************************************************************
*****************************
10.0.0.5                   : ok=8    changed=7    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0
```

```
10.0.0.6                   : ok=8    changed=7    unreachable=0    failed=0    
skipped=0    rescued=0    ignored=0   

root@1170f08f2e53:/# 
root@1170f08f2e53:/# nano filebeat-playbook.yml 
root@1170f08f2e53:/# 
root@1170f08f2e53:/# ls -l /etc/ansible
total 108
-rw-r--r-- 1 root root 19988 May 11 00:07 ansible.cfg
-rw-r--r-- 1 root root 73111 May 14 14:46 filebeat-config.yml
-rw-r--r-- 1 root root   936 May 14 15:18 filebeat-playbook.yml
-rw-r--r-- 1 root root  1147 May 13 00:06 hosts
-rw-r--r-- 1 root root   951 May 13 00:41 install-elk.yml
-rw-r--r-- 1 root root   687 May 11 00:28 pentest.yml
root@1170f08f2e53:/# touch /etc/ansible/metricbeat-playbook.yml
root@1170f08f2e53:/# ls -l /etc/ansible
total 108
-rw-r--r-- 1 root root 19988 May 11 00:07 ansible.cfg
-rw-r--r-- 1 root root 73111 May 14 14:46 filebeat-config.yml
-rw-r--r-- 1 root root   936 May 14 15:18 filebeat-playbook.yml
-rw-r--r-- 1 root root  1147 May 13 00:06 hosts
-rw-r--r-- 1 root root   951 May 13 00:41 install-elk.yml
-rw-r--r-- 1 root root     0 May 14 16:12 metricbeat-playbook.yml
-rw-r--r-- 1 root root   687 May 11 00:28 pentest.yml
root@1170f08f2e53:/# ls
bin  boot  dev  etc  filebeat-playbook.yml  home  lib  lib32  lib64  libx32  media
mnt  opt  packer-files  proc  root  run  sbin  srv  sys  tmp  usr  var
root@1170f08f2e53:/# ls -l /etc/ansible
total 108
-rw-r--r-- 1 root root 19988 May 11 00:07 ansible.cfg
-rw-r--r-- 1 root root 73111 May 14 14:46 filebeat-config.yml
-rw-r--r-- 1 root root   936 May 14 15:18 filebeat-playbook.yml
-rw-r--r-- 1 root root  1147 May 13 00:06 hosts
-rw-r--r-- 1 root root   951 May 13 00:41 install-elk.yml
-rw-r--r-- 1 root root     0 May 14 16:12 metricbeat-playbook.yml
-rw-r--r-- 1 root root   687 May 11 00:28 pentest.yml
root@1170f08f2e53:/# nano /etc/ansible/metricbeat-playbook.yml 
root@1170f08f2e53:/# cd /etc/ansible
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metricbeat-playbook.yml  pentest.yml
root@1170f08f2e53:/etc/ansible# curl https://gt.bootcampcontent.com/GT-Coding-Boot-
Camp/GT-VIRT-CYBER-PT-02-2022-U-LOL/-/blob/main/1-Lesson-Plans/13-Elk-Stack-
Project/Activities/Stu_Day_2/Solved/config_files/metricbeat-configuration.yml
<html><body>You are being <a
href="https://gt.bootcampcontent.com/users/sign_in">redirected</a>.</body></html>root@
1170f08f2e53:/etc/ansible# 
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metricbeat-playbook.yml  pentest.yml
root@1170f08f2e53:/etc/ansible# curl
https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e7
44c54513616966affb5e9d96f5e12f73/metricbeat
###################### Metricbeat Configuration Example #######################

# This file is an example configuration file highlighting only the most common
# options. The metricbeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
#migration.6_to_7.enabled: trueroot@1170f08f2e53:/etc/ansible# ls
```

```
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metricbeat-playbook.yml  pentest.yml
root@1170f08f2e53:/etc/ansible# curl
https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e7
44c54513616966affb5e9d96f5e12f73/metricbeat >> /etc/ansible/metric-configuration.yml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6188  100  6188    0     0  52888      0 --:--:-- --:--:-- --:--:-- 52440
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-playbook.yml  pentest.yml
root@1170f08f2e53:/etc/ansible# nano metricbeat-configuration.yml
root@1170f08f2e53:/etc/ansible# nano metricbeat-config.yml
root@1170f08f2e53:/etc/ansible# curl
https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e7
44c54513616966affb5e9d96f5e12f73/metricbeat >> /etc/ansible/metricbeat-
configuration.yml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6188  100  6188    0     0  15665      0 --:--:-- --:--:-- --:--:-- 15626
root@1170f08f2e53:/etc/ansible# nano metricbeat-configuration.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible# ansible-playbook metricbeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may
result in incorrectly calculated text widths that can cause Display to print incorrect
line lengths

PLAY [Install metric beat]
**************************************************************************************
**************************************************************************************
*************

TASK [Gathering Facts]
**************************************************************************************
**************************************************************************************
*****************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Download metricbeat]
**************************************************************************************
**************************************************************************************
*************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [install metricbeat]
**************************************************************************************
**************************************************************************************
**************
changed: [10.0.0.5]
changed: [10.0.0.6]
```

```
TASK [drop in metricbeat config]
**************************************************************************************
**************************************************************************************
*******
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [enable and configure docker module for metric beat]
**************************************************************************************
********************************************************************

changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [setup metric beat]
**************************************************************************************
**************************************************************************************
***************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [start metric beat]
**************************************************************************************
**************************************************************************************
***************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Enable service metricbeat on boot]
**************************************************************************************
*************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

PLAY RECAP
**************************************************************************************
**************************************************************************************
*****************************
10.0.0.5                   : ok=8    changed=7    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=8    changed=7    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0

root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible# cat filebeat-playbook.yml
---
- name: Installing and Launch Filebeat
  hosts: webservers
  become: yes
  tasks:
    # Use command module
  - name: Download filebeat .deb file
    command: curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

    # Use command module
  - name: Install filebeat .deb
    command: dpkg -i filebeat-7.4.0-amd64.deb
    # Use copy module
  - name: Drop in filebeat.yml
    copy:
      src: /etc/ansible/filebeat-config.yml
      dest: /etc/filebeat/filebeat.yml
      remote_src: yes

    # Use command module
  - name: Enable and Configure System Module
    command: filebeat modules enable system

    # Use command module
  - name: Setup filebeat
    command: filebeat setup

    # Use command module
  - name: Start filebeat service
    command: service filebeat start

    # Use systemd module
  - name: Enable service filebeat on boot
    systemd:
      name: filebeat
      enabled: yes

root@1170f08f2e53:/etc/ansible# rm filebeat-playbook.yml
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  hosts  install-elk.yml  metric-configuration.yml
metricbeat-configuration.yml  metricbeat-playbook.yml  pentest.yml
root@1170f08f2e53:/etc/ansible# cd ..
root@1170f08f2e53:/etc# cd ,,
bash: cd: ,,: No such file or directory
root@1170f08f2e53:/etc# cd
root@1170f08f2e53:~# ls
root@1170f08f2e53:~# ls -l
total 0
root@1170f08f2e53:~#
root@1170f08f2e53:~# ls
root@1170f08f2e53:~# ls
root@1170f08f2e53:~# ls -a
.  ..  .ansible  .bashrc  .cache  .local  .profile  .ssh
root@1170f08f2e53:~# cd /etc/ansible
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  hosts  install-elk.yml  metric-configuration.yml
metricbeat-configuration.yml  metricbeat-playbook.yml  pentest.yml
root@1170f08f2e53:/etc/ansible# touch filebeat-playbook.yml
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible# nano filebeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible# nano filebeat-playbook.yml
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# Connection to 20.213.85.255 closed by remote host.
```

```
Connection to 20.213.85.255 closed.
Joses-MacBook-Pro$ ssh sysadmin@20.248.200.164
The authenticity of host '20.248.200.164 (20.248.200.164)' can't be established.
ECDSA key fingerprint is SHA256:t68KFCLyMcWUSSWQcTNseF0olfeDf22+42XjnXm+dJI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.248.200.164' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 16 17:50:20 UTC 2022

  System load:  0.0                Processes:                108
  Usage of /:   10.7% 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:    10.0.0.4

 * 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

9 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Sat May 14 14:06:03 2022 from 75.40.54.33
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                            COMMAND                  CREATED
STATUS                     PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible           "/bin/sh -c /bin/bas…"   5 days ago
Exited (137) 2 days ago              sweet_robinson
7f81a2eaa9ac   cyberxsecurity/ansible:latest    "/bin/sh -c /bin/bas…"   5 days ago
Exited (0) 5 days ago                gracious_chandrasekhar
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker start sweet_robinson
sweet_robinson
sysadmin@Jump-Box-Provisioner:~$ sudo docker attach sweet_robinson
root@1170f08f2e53:~#
root@1170f08f2e53:~#
root@1170f08f2e53:~# cd /etc/ansible
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# sudo nano metricbeat-playbook.yml
bash: sudo: command not found
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ansible-playbook metricbeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may
result in incorrectly calculated text widths that can cause Display to print incorrect
line lengths

PLAY [Install metric beat]
**************************************************************************************
```

```
**************************************************************************************
*************

TASK [Gathering Facts]
**************************************************************************************
**************************************************************************************
*****************
ok: [10.0.0.6]
ok: [10.0.0.5]

TASK [Download metricbeat]
**************************************************************************************
**************************************************************************************
*************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [install metricbeat]
**************************************************************************************
**************************************************************************************
**************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [drop in metricbeat config]
**************************************************************************************
**************************************************************************************
*******
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [enable and configure docker module for metric beat]
**************************************************************************************
********************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [setup metric beat]
**************************************************************************************
**************************************************************************************
***************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [start metric beat]
**************************************************************************************
**************************************************************************************
***************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [Enable service metricbeat on boot]
**************************************************************************************
*************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

PLAY RECAP
**************************************************************************************
**************************************************************************************
*****************************
```

```
10.0.0.5                   : ok=8    changed=5    unreachable=0    failed=0    
skipped=0    rescued=0    ignored=0   
10.0.0.6                   : ok=8    changed=5    unreachable=0    failed=0    
skipped=0    rescued=0    ignored=0   

root@1170f08f2e53:/etc/ansible# 
root@1170f08f2e53:/etc/ansible# ssh sysadmin@10.0.0.5
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 16 17:58:57 UTC 2022

  System load:  0.0               Processes:                124
  Usage of /:   13.0% of 28.90GB   Users logged in:          0
  Memory usage: 28%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.0.0.5

 * 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

17 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Mon May 16 17:55:38 2022 from 10.0.0.4
sysadmin@Web-1:~$ 
sysadmin@Web-1:~$ cd /etc
sysadmin@Web-1:/etc$ cd metricbeat
sysadmin@Web-1:/etc/metricbeat$ 
sysadmin@Web-1:/etc/metricbeat$ ls
fields.yml  metricbeat.reference.yml  metricbeat.yml  modules.d
sysadmin@Web-1:/etc/metricbeat$ 
sysadmin@Web-1:/etc/metricbeat$ nano metricbeat.yml
sysadmin@Web-1:/etc/metricbeat$ sudo nano metricbeat.yml
sysadmin@Web-1:/etc/metricbeat$ sudo nano metricbeat.reference.yml
sysadmin@Web-1:/etc/metricbeat$ cd ..
sysadmin@Web-1:/etc$ cd ..
sysadmin@Web-1:/$ 
sysadmin@Web-1:/$ sudo systemctl status metricbeat
● metricbeat.service - Metricbeat is a lightweight shipper for metrics.
     Loaded: loaded (/lib/systemd/system/metricbeat.service; enabled; vendor preset: 
enabled)
     Active: active (running) since Mon 2022-05-16 17:40:07 UTC; 26min ago
       Docs: https://www.elastic.co/products/beats/metricbeat
   Main PID: 707 (metricbeat)
      Tasks: 8 (limit: 2289)
     Memory: 86.1M
     CGroup: /system.slice/metricbeat.service
             └─707 /usr/share/metricbeat/bin/metricbeat -e -c 
/etc/metricbeat/metricbeat.yml -path.home /usr/share/metricbeat -path.config 
/etc/metricbeat -path.data /var/lib/metricbeat -path.logs /var/log/metri

May 16 18:02:12 Web-1 metricbeat[707]: 2022-05-16T18:02:12.567Z        INFO    
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s    
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
```

```
May 16 18:02:42 Web-1 metricbeat[707]: 2022-05-16T18:02:42.566Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:03:12 Web-1 metricbeat[707]: 2022-05-16T18:03:12.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:03:42 Web-1 metricbeat[707]: 2022-05-16T18:03:42.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:04:12 Web-1 metricbeat[707]: 2022-05-16T18:04:12.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:04:42 Web-1 metricbeat[707]: 2022-05-16T18:04:42.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:05:12 Web-1 metricbeat[707]: 2022-05-16T18:05:12.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:05:42 Web-1 metricbeat[707]: 2022-05-16T18:05:42.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:06:12 Web-1 metricbeat[707]: 2022-05-16T18:06:12.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy
May 16 18:06:42 Web-1 metricbeat[707]: 2022-05-16T18:06:42.567Z        INFO
[monitoring]        log/log.go:145        Non-zero metrics in the last 30s
{"monitoring": {"metrics": {"beat":{"cpu":{"sy


sysadmin@Web-1:/etc$ cd metricbeat
sysadmin@Web-1:/etc/metricbeat$ ls
fields.yml  metricbeat.reference.yml  metricbeat.yml  modules.d
sysadmin@Web-1:/etc/metricbeat/modules.d$ cd ..
sysadmin@Web-1:/etc/metricbeat$ cd ..
sysadmin@Web-1:/etc$ cd ..
sysadmin@Web-1:/$ exit
logout
Connection to 10.0.0.5 closed.
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ssh sysadmin@10.0.0.5
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 16 19:08:36 UTC 2022

  System load:  0.0               Processes:                123
  Usage of /:   13.0% of 28.90GB   Users logged in:          0
  Memory usage: 28%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.0.0.5

 * 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

17 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Mon May 16 17:58:58 2022 from 10.0.0.4
sysadmin@Web-1:~$ cd /etc/metricbeat/modules.d
sysadmin@Web-1:/etc/metricbeat/modules.d$ sudo nano kibana.yml
sysadmin@Web-1:/etc/metricbeat/modules.d$ sudo nano kibana.yml.disabled
sysadmin@Web-1:/etc/metricbeat/modules.d$ client_loop: send disconnect: Broken pipe
Joses-MacBook-Pro$ ssh sysadmin@52.147.62.243
The authenticity of host '52.147.62.243 (52.147.62.243)' can't be established.
ECDSA key fingerprint is SHA256:OXO5VbUpE4IXVMcbFf39HDOvX0QVYEx8aHgLQ0kMWJ0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '52.147.62.243' (ECDSA) to the list of known hosts.
sysadmin@52.147.62.243: Permission denied (publickey).
Joses-MacBook-Pro:~ yennicastilloespinosa$ ssh sysadmin@20.248.200.164
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 16 20:46:23 UTC 2022

  System load:  0.0               Processes:                112
  Usage of /:   10.8% of 28.90GB  Users logged in:          0
  Memory usage: 37%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.0.0.4

 * 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

17 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Mon May 16 17:50:21 2022 from 75.40.54.33
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                          COMMAND                  CREATED
STATUS                  PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible          "/bin/sh -c /bin/bas…"   5 days ago
Up 3 hours                        sweet_robinson
7f81a2eaa9ac   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   5 days ago
Exited (0) 5 days ago             gracious_chandrasekhar
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker ps
CONTAINER ID   IMAGE                    COMMAND                  CREATED      STATUS
PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible   "/bin/sh -c /bin/bas…"   5 days ago   Up 3
hours             sweet_robinson
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker attach sweet_robinson
sysadmin@Web-1:/etc/metricbeat/modules.d$
```

```
sysadmin@Web-1:/etc/metricbeat/modules.d$
sysadmin@Web-1:/etc/metricbeat/modules.d$
sysadmin@Web-1:/etc/metricbeat/modules.d$ exit
logout
Connection to 10.0.0.5 closed.
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# Connection to 20.248.200.164 closed by remote host.
Connection to 20.248.200.164 closed.
Joses-MacBook-Pro:~ yennicastilloespinosa$ ssh sysadmin@
^C
Joses-MacBook-Pro:~ yennicastilloespinosa$ ssh sysadmin@20.211.188.223
The authenticity of host '20.211.188.223 (20.211.188.223)' can't be established.
ECDSA key fingerprint is SHA256:t68KFCLyMcWUSSWQcTNseF0olfeDf22+42XjnXm+dJI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.211.188.223' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue May 17 00:46:54 UTC 2022

  System load:  0.11               Processes:                113
  Usage of /:   10.9% of 28.90GB   Users logged in:          0
  Memory usage: 32%                IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                 IPv4 address for eth0:    10.0.0.4

 * 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

17 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Mon May 16 20:46:24 2022 from 75.40.54.33
sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                          COMMAND                  CREATED
STATUS                      PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible         "/bin/sh -c /bin/bas…"   6 days ago
Exited (137) 3 hours ago              sweet_robinson
7f81a2eaa9ac   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   6 days ago
Exited (0) 6 days ago                 gracious_chandrasekhar
sysadmin@Jump-Box-Provisioner:~$ sudo docker start sweet_robinson
sweet_robinson
sysadmin@Jump-Box-Provisioner:~$ sudo docker attach sweet_robinson
root@1170f08f2e53:~#
root@1170f08f2e53:~# cd etc/ansible
bash: cd: etc/ansible: No such file or directory
root@1170f08f2e53:~# cd /etc/ansible
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible# sudo nano metricbeat-configuration.yml
bash: sudo: command not found
```

```
root@1170f08f2e53:/etc/ansible# nano metricbeat-configuration.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ansible-playbook metricbeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may
result in incorrectly calculated text widths that can cause Display to print incorrect
line lengths

PLAY [Install metric beat]
**************************************************************************************
**************************************************************************************
*************

TASK [Gathering Facts]
**************************************************************************************
**************************************************************************************
*****************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Download metricbeat]
**************************************************************************************
**************************************************************************************
*************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [install metricbeat]
**************************************************************************************
**************************************************************************************
**************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [drop in metricbeat config]
**************************************************************************************
**************************************************************************************
*******
ok: [10.0.0.6]
ok: [10.0.0.5]

TASK [enable and configure docker module for metric beat]
**************************************************************************************
********************************************************************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [setup metric beat]
**************************************************************************************
**************************************************************************************
***************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [start metric beat]
**************************************************************************************
**************************************************************************************
***************
changed: [10.0.0.5]
changed: [10.0.0.6]
```

```
TASK [Enable service metricbeat on boot]
*************************************************************************************
************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

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

root@1170f08f2e53:/etc/ansible# nano metricbeat-playbook.yml
root@1170f08f2e53:/etc/ansible# client_loop: send disconnect: Broken pipe
Joses-MacBook-Pro$ ssh sysadmin@20.213.127.129
The authenticity of host '20.213.127.129 (20.213.127.129)' can't be established.
ECDSA key fingerprint is SHA256:t68KFCLyMcWUSSWQcTNseF0olfeDf22+42XjnXm+dJI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.213.127.129' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue May 17 19:22:12 UTC 2022

  System load:  0.1               Processes:                113
  Usage of /:   10.9% of 28.90GB  Users logged in:          0
  Memory usage: 32%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.0.0.4

 * 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

17 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Tue May 17 00:46:56 2022 from 75.40.54.33

sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                          COMMAND                  CREATED
STATUS                     PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible          "/bin/sh -c /bin/bas…"   6 days ago
Exited (137) 18 hours ago            sweet_robinson
7f81a2eaa9ac   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   6 days ago
Exited (0) 6 days ago                gracious_chandrasekhar
sysadmin@Jump-Box-Provisioner:~$ sudo docker start sweet_robinson
sweet_robinson
sysadmin@Jump-Box-Provisioner:~$ sudo docker attach sweet_robinson
root@1170f08f2e53:~#
root@1170f08f2e53:~# cd /etc/ansible
root@1170f08f2e53:/etc/ansible# ls
```

```
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
root@1170f08f2e53:/etc/ansible# nano pentest.yml
root@1170f08f2e53:/etc/ansible#
Joses-MacBook-Pro$ ssh sysadmin@20.211.3.206
The authenticity of host '20.211.3.206 (20.211.3.206)' can't be established.
ECDSA key fingerprint is SHA256:t68KFCLyMcWUSSWQcTNseF0olfeDf22+42XjnXm+dJI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.211.3.206' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1023-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat May 21 23:14:13 UTC 2022

  System load:  0.0                Processes:                108
  Usage of /:   10.9% 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:    10.0.0.4

 * 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

21 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Tue May 17 19:22:13 2022 from 75.40.54.33
sysadmin@Jump-Box-Provisioner:~$
sysadmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID   IMAGE                            COMMAND                  CREATED
STATUS                    PORTS     NAMES
1170f08f2e53   cyberxsecurity/ansible           "/bin/sh -c /bin/bas…"   10 days ago
Exited (137) 4 days ago             sweet_robinson
7f81a2eaa9ac   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   10 days ago
Exited (0) 10 days ago              gracious_chandrasekhar
sysadmin@Jump-Box-Provisioner:~$ sudo docker start sweet_robinson
sweet_robinson
sysadmin@Jump-Box-Provisioner:~$ sudo docker attach sweet_robinson
root@1170f08f2e53:~#
root@1170f08f2e53:~# cd /etc/ansible
root@1170f08f2e53:/etc/ansible#
root@1170f08f2e53:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  filebeat-playbook.yml  hosts  install-elk.yml
metric-configuration.yml  metricbeat-configuration.yml  metricbeat-playbook.yml
pentest.yml
```