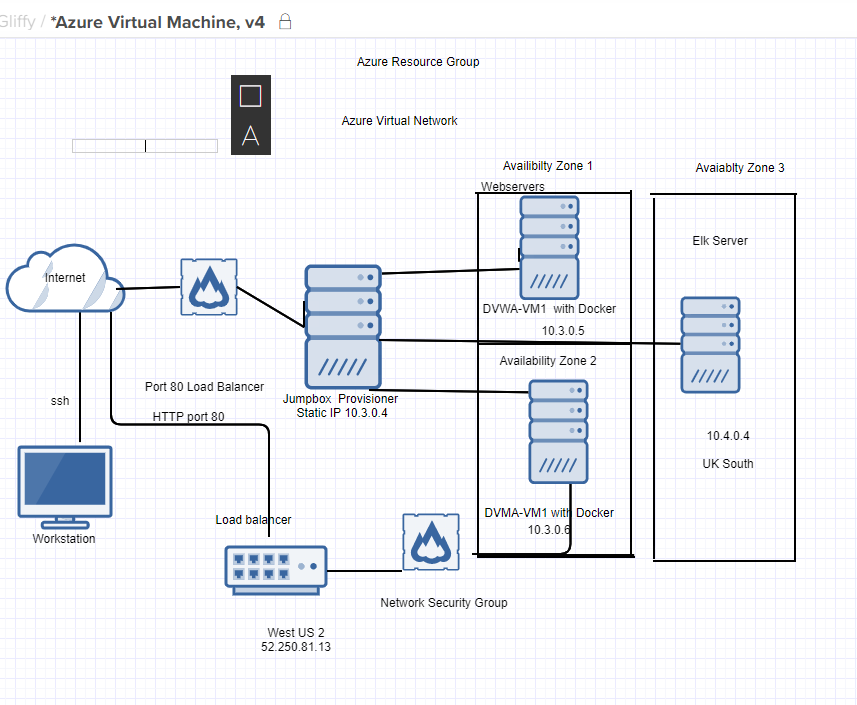
Erika Perry



Jump box

* + region: West US
  + private IP: 10.3.0.4
  + public IP (static): 52.183.62.233
* DVWA-VM1
  + region: West US 2
  + availability zone: 1
  + private IP: 10.3.0.5
* DVWA-VM2
  + region: West US 2
  + availability zone: 2
  + private IP: 10.3.0.6

Elk Server

* + region: West US 2
  + availability zone: 3
  + private IP: 10.4.0.4
* Firewall
  + I added whitelist of IPs
  + Setup inbound rules to only allow the IP’s in the whitelist access the jump-box from my external network
* **Load balancer**
  + Fronted IP Configuration: 52.250.81.13
  + Backend pools: DVWA-VM1 and DVWA-VM2
  + Health probes: setup for load balancing rule and detect the failure of an application on a backend endpoint BT-LB WVS2-Pool
  + Load balancing rules: The open port 80 for HTTP

**Load balancing ensures that the application will be highly available in addition to restricting traffic to the network.**

* The load balancers protect an organization against distributed denial-of-service (DDoS) attack. It reverses network traffic across a server
* The advantage of a jump box is to provide and to prevent the Azure VM's from being expose to the public. The jumpbox is the entry point.

**Integrating an ELK server allows users to easily monitor the vulnerable Virtual Machine’s for changes to the infrastructure and system logs.**

* Filebeat is watch for collecting and shipping log files.
* Metricbeat collects ships various system-level metrics to a specified destination

The configuration details of each machine may be found below.

| **Name** | **Function** | **IP Address** | **Operating System** |
| --- | --- | --- | --- |
| Jump Box | Gateway | 10.3.0.4 | Linux |
| DVWA-VM1 | Webserver | 10.3.0.5 | Linux |
| DVWA-VM2 | Webserver | 10.3.0.6 | Linux |
| DVWA-VM3 | ELK Server | 10.4.0.4 | Linux |

The files and Ips have been tested

* **Tested and configure the jump box to run my Docker containers and to install a container**
* **Tested and used to generate webserver containers, a live ELK deployment and loadbalancer on the Azure. All my YML and Filebeat work please see my diagram I design in Gliffy**

**I used two different regions and I had to peer them**

**Access Policies**

The machines on the internal network are not exposed to the public Internet.

Only the **Jump-box** machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* *Add whitelisted IP addresses into the firewall rules to allow the inbound access,*

*--- I added the IP address of my local machine from chicken IP I gathered*

Machines within the network can only be accessed by the Jump-box machine and other machines in the network.

* Only my local machine which is in the whitelisted machine added into the firewall rules I went to [www.ipchicken.com](http://www.ipchicken.com) from Internet can access the ELK server

A summary of the access policies in place can be found in the table below.

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes | IP-in-whitelist my own machine |
| DVWA-VM1 | Yes | Any |
| DVWA-VM2 | Yes | Any |
| Elk Server | Yes | 10.4.0.4 |

Elk Configuration

What is the main advantage of automating configuration with ansible?

The ability to automate all your IT landscape for your organization from one single tool

Elk Installation:

PLAY [Configure Elk VM with Docker] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.4.0.4]

TASK [Install docker.io] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[WARNING]: Updating cache and auto-installing missing dependency: python-apt

changed: [10.4.0.4]

TASK [Install python-pip] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

TASK [Install Docker module] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

TASK [Increase virtual memory] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

TASK [download and launch a docker elk container] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.4.0.4 : ok=6 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@9ce0421357ab:/etc/ansible/roles# exit

exit

blueadmin@Jump-Box-Provisioner:~$ /etc/ansible

-bash: /etc/ansible: No such file or directory

blueadmin@Jump-Box-Provisioner:~$ sudo docker container list -a

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

9ce0421357ab cyberxsecurity/ansible:latest "bash" 3 hours ago Exited (0) 6 minutes ago nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker start nice\_tu

nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach

"docker attach" requires exactly 1 argument.

See 'docker attach --help'.

Usage: docker attach [OPTIONS] CONTAINER

Attach local standard input, output, and error streams to a running container

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach contanier

Error: No such container: contanier

blueadmin@Jump-Box-Provisioner:~$ exit

logout

There are stopped jobs.

blueadmin@Jump-Box-Provisioner:~$ exit

logout

Connection to 52.183.62.233 closed.

sysadmin@ubuntu-vm:~/.ssh$ ssh blueadmin@52.183.62.233

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 20:15:47 UTC 2020

System load: 0.08 Processes: 112

Usage of /: 7.1% of 28.90GB Users logged in: 0

Memory usage: 42% IP address for eth0: 10.3.0.4

Swap usage: 0% IP address for docker0: 172.17.0.1

22 packages can be updated.

4 updates are security updates.

Last login: Fri Jun 5 16:57:16 2020 from 73.82.221.157

blueadmin@Jump-Box-Provisioner:~$ sudo docker container list -a

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

9ce0421357ab cyberxsecurity/ansible:latest "bash" 3 hours ago Up 8 minutes nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker start nice\_tu

nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach nice\_tu

root@9ce0421357ab:~# ssh blueadmin@10.4.0.4

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 20:20:10 UTC 2020

System load: 0.06 Processes: 129

Usage of /: 17.0% of 28.90GB Users logged in: 0

Memory usage: 41% IP address for eth0: 10.4.0.4

Swap usage: 0% IP address for docker0: 172.17.0.1

22 packages can be updated.

4 updates are security updates.

Last login: Fri Jun 5 19:54:05 2020 from 10.3.0.4

blueadmin@Elk-Server:~$ sudo docker ps

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

3546ff11486b sebp/elk "/usr/local/bin/star…" 22 minutes ago Up 22 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

blueadmin@Elk-Server:~$ exit

logout

Connection to 10.4.0.4 closed.

root@9ce0421357ab:~# cd /etc/ansible/

root@9ce0421357ab:/etc/ansible# ls

ansible.cfg hosts roles

**Target Machines Beats**

blueadmin@Jump-Box-Provisioner:~$ sudo apt install docker.io

Reading package lists... Done

Building dependency tree

Reading state information... Done

E: Unable to locate package docker.io

E: Couldn't find any package by glob 'docker.io'

E: Couldn't find any package by regex 'docker.io'

blueadmin@Jump-Box-Provisioner:~$ sudo apt-get update

Hit:1 http://azure.archive.ubuntu.com/ubuntu bionic InRelease

Get:2 http://azure.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]

Get:3 http://azure.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]

Get:4 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]

Get:5 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]

Get:6 http://azure.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]

Get:7 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]

Get:8 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]

Get:9 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [951 kB]

Get:10 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [324 kB]

Get:11 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1077 kB]

Get:12 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [335 kB]

Get:13 http://azure.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [15.7 kB]

Get:14 http://azure.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation-en [6384 B]

Get:15 http://azure.archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [7516 B]

Get:16 http://azure.archive.ubuntu.com/ubuntu bionic-backports/main Translation-en [4764 B]

Get:17 http://azure.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [7484 B]

Get:18 http://azure.archive.ubuntu.com/ubuntu bionic-backports/universe Translation-en [4436 B]

Get:19 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [727 kB]

Get:20 http://security.ubuntu.com/ubuntu bionic-security/main Translation-en [230 kB]

Get:21 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [669 kB]

Get:22 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en [222 kB]

Get:23 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [7596 B]

Get:24 http://security.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [2824 B]

Fetched 18.6 MB in 4s (4536 kB/s)

Reading package lists... Done

blueadmin@Jump-Box-Provisioner:~$ sudo apt install docker.io

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following packages were automatically installed and are no longer required:

grub-pc-bin linux-headers-4.15.0-101

Use 'sudo apt autoremove' to remove them.

The following additional packages will be installed:

bridge-utils cgroupfs-mount containerd pigz runc ubuntu-fan

Suggested packages:

ifupdown aufs-tools debootstrap docker-doc rinse zfs-fuse | zfsutils

The following NEW packages will be installed:

bridge-utils cgroupfs-mount containerd docker.io pigz runc ubuntu-fan

0 upgraded, 7 newly installed, 0 to remove and 22 not upgraded.

Need to get 63.8 MB of archives.

After this operation, 319 MB of additional disk space will be used.

Do you want to continue? [Y/n] y

Get:1 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 pigz amd64 2.4-1 [57.4 kB]

Get:2 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 bridge-utils amd64 1.5-15ubuntu1 [30.1 kB]

Get:3 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 cgroupfs-mount all 1.4 [6320 B]

Get:4 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 runc amd64 1.0.0~rc10-0ubuntu1~18.04.2 [2000 kB]

Get:5 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 containerd amd64 1.3.3-0ubuntu1~18.04.2 [21.7 MB]

Get:6 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 docker.io amd64 19.03.6-0ubuntu1~18.04.1 [39.9 MB]

Get:7 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 ubuntu-fan all 0.12.10 [34.7 kB]

Fetched 63.8 MB in 2s (32.6 MB/s)

Preconfiguring packages ...

Selecting previously unselected package pigz.

(Reading database ... 76606 files and directories currently installed.)

Preparing to unpack .../0-pigz\_2.4-1\_amd64.deb ...

Unpacking pigz (2.4-1) ...

Selecting previously unselected package bridge-utils.

Preparing to unpack .../1-bridge-utils\_1.5-15ubuntu1\_amd64.deb ...

Unpacking bridge-utils (1.5-15ubuntu1) ...

Selecting previously unselected package cgroupfs-mount.

Preparing to unpack .../2-cgroupfs-mount\_1.4\_all.deb ...

Unpacking cgroupfs-mount (1.4) ...

Selecting previously unselected package runc.

Preparing to unpack .../3-runc\_1.0.0~rc10-0ubuntu1~18.04.2\_amd64.deb ...

Unpacking runc (1.0.0~rc10-0ubuntu1~18.04.2) ...

Selecting previously unselected package containerd.

Preparing to unpack .../4-containerd\_1.3.3-0ubuntu1~18.04.2\_amd64.deb ...

Unpacking containerd (1.3.3-0ubuntu1~18.04.2) ...

Selecting previously unselected package docker.io.

Preparing to unpack .../5-docker.io\_19.03.6-0ubuntu1~18.04.1\_amd64.deb ...

Unpacking docker.io (19.03.6-0ubuntu1~18.04.1) ...

Selecting previously unselected package ubuntu-fan.

Preparing to unpack .../6-ubuntu-fan\_0.12.10\_all.deb ...

Unpacking ubuntu-fan (0.12.10) ...

Setting up runc (1.0.0~rc10-0ubuntu1~18.04.2) ...

Setting up cgroupfs-mount (1.4) ...

Setting up containerd (1.3.3-0ubuntu1~18.04.2) ...

Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.service.

Setting up bridge-utils (1.5-15ubuntu1) ...

Setting up ubuntu-fan (0.12.10) ...

Created symlink /etc/systemd/system/multi-user.target.wants/ubuntu-fan.service → /lib/systemd/system/ubuntu-fan.service.

Setting up pigz (2.4-1) ...

Setting up docker.io (19.03.6-0ubuntu1~18.04.1) ...

Adding group `docker' (GID 116) ...

Done.

Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.

docker.service is a disabled or a static unit, not starting it.

Processing triggers for systemd (237-3ubuntu10.40) ...

Processing triggers for man-db (2.8.3-2ubuntu0.1) ...

Processing triggers for ureadahead (0.100.0-21) ...

blueadmin@Jump-Box-Provisioner:~$ systemctl service docker

Unknown operation service.

blueadmin@Jump-Box-Provisioner:~$ sudo systemctl service docker

Unknown operation service.

blueadmin@Jump-Box-Provisioner:~$ sudo systemctl docker status

Unknown operation docker.

blueadmin@Jump-Box-Provisioner:~$ sudo systemctl docker.io status

Unknown operation docker.io.

blueadmin@Jump-Box-Provisioner:~$ sudo systemctl start docker

blueadmin@Jump-Box-Provisioner:~$ sudo systemctl service docker

Unknown operation service.

blueadmin@Jump-Box-Provisioner:~$ sudo status docker

sudo: status: command not found

blueadmin@Jump-Box-Provisioner:~$ sudo service docker status

● docker.service - Docker Application Container Engine

Loaded: loaded (/lib/systemd/system/docker.service; disabled; vendor preset:

Active: active (running) since Fri 2020-06-05 17:03:50 UTC; 1min 42s ago

Docs: https://docs.docker.com

Main PID: 16303 (dockerd)

Tasks: 8

CGroup: /system.slice/docker.service

└─16303 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/contai

Jun 05 17:03:49 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:49.3

Jun 05 17:03:49 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:49.3

Jun 05 17:03:49 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:49.3

Jun 05 17:03:49 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:49.6

Jun 05 17:03:49 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:49.7

Jun 05 17:03:50 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:50.1

Jun 05 17:03:50 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:50.1

Jun 05 17:03:50 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:50.1

Jun 05 17:03:50 Jump-Box-Provisioner systemd[1]: Started Docker Application Cont

Jun 05 17:03:50 Jump-Box-Provisioner dockerd[16303]: time="2020-06-05T17:03:50.2

lines 1-19/19 (END)

[1]+ Stopped sudo service docker status

^C^C

blueadmin@Jump-Box-Provisioner:~$ sudo docker pull cyberxsecurity/ansible

Using default tag: latest

latest: Pulling from cyberxsecurity/ansible

7ddbc47eeb70: Pull complete

c1bbdc448b72: Pull complete

8c3b70e39044: Pull complete

45d437916d57: Pull complete

78440e84779a: Pull complete

b6f0115afe25: Pull complete

blueadmin@Jump-Box-Provisioner:~$ sudo docker run -ti cyberxsecurity/ansible:latest bash

root@9ce0421357ab:~# exit

exit

blueadmin@Jump-Box-Provisioner:~$ sudo docker container list -a

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

9ce0421357ab cyberxsecurity/ansible:latest "bash" About a minute ago Exited (0) 59 seconds ago nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker start

"docker start" requires at least 1 argument.

See 'docker start --help'.

Usage: docker start [OPTIONS] CONTAINER [CONTAINER...]

Start one or more stopped containers

blueadmin@Jump-Box-Provisioner:~$ sudo docker start nice\_tu

nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach nice\_tu

root@9ce0421357ab:~# ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

Created directory '/root/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa.

Your public key has been saved in /root/.ssh/id\_rsa.pub.

The key fingerprint is:

SHA256:FSjvbg8+Dc17UVYcGltkgyD0NlJ6KZJig+EcYyNnnkA root@9ce0421357ab

The key's randomart image is:

+---[RSA 2048]----+

|.E O .+.o..oB.|

| X B . o =...\* +|

| \* + = +.\* o . |

| . o o.= . o |

| .So o |

| o o . |

| ..o . . |

| .+.o . |

| ..o.. |

+----[SHA256]-----+

root@9ce0421357ab:~# cat .ssh/id\_rsa.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDNtnGG5043zWZ0Syr0UkvvSGum8/G8YIWKfhkmnLuljBpVOUBLKsO7EElWreX+d9fARWcrrwz/wtb1Uw6CBWkzCqj0R8hIPc6PBiYIu7B9aOZ5je03zrogKXtlqAmsg9YEkr7H4nL+g6b1lqE4sfgnewYBSHDrV8hNM1qQi9W/7282cc5X4xUMszaAb+5VgfPpoYqSW4eoqhBn3B9mwMG4pTjbRGvwDDrtzMf8uMNDwRtRuxnRBjEYupJluz9YBp8/IntOB6iVr/Z0Ldo0N83pf1o4rrfLZzbV/xAJH6kFBZSNnzu+NMA7Y4rZWdNeot3uuPOr+RDwgdydyzdixEQX root@9ce0421357ab

root@9ce0421357ab:~# ssh blueadmin@10.3.0.5

The authenticity of host '10.3.0.5 (10.3.0.5)' can't be established.

ECDSA key fingerprint is SHA256:auzzUqi9BD+s18FZpEZpHxBxjOl4btOnfl2plcYMSHI.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.3.0.5' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 17:28:55 UTC 2020

System load: 0.09 Processes: 116

Usage of /: 4.3% of 28.90GB Users logged in: 0

Memory usage: 30% IP address for eth0: 10.3.0.5

Swap usage: 0%

0 packages can be updated.

0 updates are security updates.

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.

blueadmin@DVWA-VM1:~$ exit

logout

Connection to 10.3.0.5 closed.

root@9ce0421357ab:~# ssh blueadmin@10.3.0.5

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 17:41:09 UTC 2020

System load: 0.02 Processes: 109

Usage of /: 4.3% of 28.90GB Users logged in: 0

Memory usage: 30% IP address for eth0: 10.3.0.5

Swap usage: 0%

0 packages can be updated.

0 updates are security updates.

Last login: Fri Jun 5 17:28:57 2020 from 10.3.0.4

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo\_root" for details.

blueadmin@DVWA-VM1:~$ ssh blueadmin@10.3.0.6

The authenticity of host '10.3.0.6 (10.3.0.6)' can't be established.

ECDSA key fingerprint is SHA256:jdBBStLxmwa5nrXr8aNrzepXwPs9w2vFNKY/ewKAwck.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.3.0.6' (ECDSA) to the list of known hosts.

blueadmin@10.3.0.6: Permission denied (publickey).

blueadmin@DVWA-VM1:~$ cat .ssh/id\_rsa.pub

cat: .ssh/id\_rsa.pub: No such file or directory

blueadmin@DVWA-VM1:~$ exit

logout

Connection to 10.3.0.5 closed.

root@9ce0421357ab:~# ssh blueadmin@10.3.0.6

The authenticity of host '10.3.0.6 (10.3.0.6)' can't be established.

ECDSA key fingerprint is SHA256:jdBBStLxmwa5nrXr8aNrzepXwPs9w2vFNKY/ewKAwck.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.3.0.6' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 17:43:54 UTC 2020

System load: 0.18 Processes: 109

Usage of /: 4.3% of 28.90GB Users logged in: 0

Memory usage: 30% IP address for eth0: 10.3.0.6

Swap usage: 0%

0 packages can be updated.

0 updates are security updates.

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.

blueadmin@DVWA-VM2:~$ exit

logout

Connection to 10.3.0.6 closed.

root@9ce0421357ab:~# cd /etc/ansible/

root@9ce0421357ab:/etc/ansible# ls

ansible.cfg hosts roles

root@9ce0421357ab:/etc/ansible# nano ansible.cfg

root@9ce0421357ab:/etc/ansible# nano host

root@9ce0421357ab:/etc/ansible# nano hosts

root@9ce0421357ab:/etc/ansible# ansible -m ping webservers

[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 10.3.0.5 should use

/usr/bin/python3, but is using /usr/bin/python for backward compatibility with prior Ansible

releases. A future Ansible release will default to using the discovered platform python for

this host. See

https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more

information. This feature will be removed in version 2.12. Deprecation warnings can be

disabled by setting deprecation\_warnings=False in ansible.cfg.

10.3.0.5 | SUCCESS => {

"ansible\_facts": {

"discovered\_interpreter\_python": "/usr/bin/python"

},

"changed": false,

"ping": "pong"

}

[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 10.3.0.6 should use

/usr/bin/python3, but is using /usr/bin/python for backward compatibility with prior Ansible

releases. A future Ansible release will default to using the discovered platform python for

this host. See

https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more

information. This feature will be removed in version 2.12. Deprecation warnings can be

disabled by setting deprecation\_warnings=False in ansible.cfg.

10.3.0.6 | SUCCESS => {

"ansible\_facts": {

"discovered\_interpreter\_python": "/usr/bin/python"

},

"changed": false,

"ping": "pong"

}

root@9ce0421357ab:/etc/ansible# cd roles

root@9ce0421357ab:/etc/ansible/roles# nano dvwa-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# ansible-playbook dvwa-playbook.yml

PLAY [DVWA Playbook] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.3.0.6]

ok: [10.3.0.5]

TASK [Install docker.io] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[WARNING]: Updating cache and auto-installing missing dependency: python-apt

changed: [10.3.0.6]

changed: [10.3.0.5]

TASK [Install python-pip] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.6]

changed: [10.3.0.5]

TASK [Install Docker] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

changed: [10.3.0.6]

TASK [download and launch a docker web container] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.6]

changed: [10.3.0.5]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.3.0.5 : ok=5 changed=4 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

10.3.0.6 : ok=5 changed=4 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@9ce0421357ab:/etc/ansible/roles# ssh blueadmin@10.3.0.5

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-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 1.0

20 packages can be updated.

4 updates are security updates.

Last login: Fri Jun 5 18:16:55 2020 from 10.3.0.4

blueadmin@DVWA-VM1:~$ curl localhost/setup.php

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Setup :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</title>

<link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

<link rel="icon" type="\image/ico" href="favicon.ico" />

<script type="text/javascript" src="dvwa/js/dvwaPage.js"></script>

</head>

<body class="home">

<div id="container">

<div id="header">

<img src="dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

</div>

<div id="main\_menu">

<div id="main\_menu\_padded">

<ul class="menuBlocks"><li class="selected"><a href="setup.php">Setup DVWA</a></li>

<li class=""><a href="instructions.php">Instructions</a></li>

</ul><ul class="menuBlocks"><li class=""><a href="about.php">About</a></li>

</ul>

</div>

</div>

<div id="main\_body">

<div class="body\_padded">

<h1>Database Setup <img src="dvwa/images/spanner.png" /></h1>

<p>Click on the 'Create / Reset Database' button below to create or reset your database.<br />

If you get an error make sure you have the correct user credentials in: <em>/var/www/html/config/config.inc.php</em></p>

<p>If the database already exists, <em>it will be cleared and the data will be reset</em>.<br />

You can also use this to reset the administrator credentials ("<em>admin</em> // <em>password</em>") at any stage.</p>

<hr />

<br />

<h2>Setup Check</h2>

Operating system: <em>\*nix</em><br />

Backend database: <em>MySQL</em><br />

PHP version: <em>7.0.30-0+deb9u1</em><br />

<br />

Web Server SERVER\_NAME: <em>localhost</em><br />

<br />

PHP function display\_errors: <em>Disabled</em><br />

PHP function safe\_mode: <span class="success">Disabled</span><br/ >

PHP function allow\_url\_include: <span class="success">Enabled</span><br/ >

PHP function allow\_url\_fopen: <span class="success">Enabled</span><br />

PHP function magic\_quotes\_gpc: <span class="success">Disabled</span><br />

PHP module gd: <span class="success">Installed</span><br />

PHP module mysql: <span class="success">Installed</span><br />

PHP module pdo\_mysql: <span class="success">Installed</span><br />

<br />

MySQL username: <em>app</em><br />

MySQL password: <em>\*\*\*\*\*\*</em><br />

MySQL database: <em>dvwa</em><br />

MySQL host: <em>127.0.0.1</em><br />

<br />

reCAPTCHA key: <span class="failure">Missing</span><br />

<br />

[User: www-data] Writable folder /var/www/html/hackable/uploads/: <span class="success">Yes</span><br />

[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: <span class="success">Yes</span><br />

<br />

<br />

[User: www-data] Writable folder /var/www/html/config: <span class="success">Yes</span>

<br />

<i><span class="failure">Status in red</span>, indicate there will be an issue when trying to complete some modules.</i><br />

<br />

If you see disabled on either <i>allow\_url\_fopen</i> or <i>allow\_url\_include</i>, set the following in your php.ini file and restart Apache.<br />

<pre><code>allow\_url\_fopen = On

allow\_url\_include = On</code></pre>

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

<br /><br /><br />

<!-- Create db button -->

<form action="#" method="post">

<input name="create\_db" type="submit" value="Create / Reset Database">

<input type='hidden' name='user\_token' value='0b2565e835d314ef5622278a54d1fa80' />

</form>

<br />

<hr />

</div>

<br /><br />

</div>

<div class="clear">

</div>

<div id="system\_info">

</div>

<div id="footer">

<p>Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</p>

<script src='/dvwa/js/add\_event\_listeners.js'></script>

</div>

</div>

</body>

</html>blueadmin@DVWA-VM1:~$ exit

logout

Connection to 10.3.0.5 closed.

root@9ce0421357ab:/etc/ansible/roles# ssh blueadmin@10.3.0.6

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 18:20:04 UTC 2020

System load: 0.56 Processes: 123

Usage of /: 10.5% of 28.90GB Users logged in: 0

Memory usage: 54% IP address for eth0: 10.3.0.6

Swap usage: 0% IP address for docker0: 172.17.0.1

20 packages can be updated.

4 updates are security updates.

Last login: Fri Jun 5 18:16:55 2020 from 10.3.0.4

blueadmin@DVWA-VM2:~$ curl localhost/setup.php

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Setup :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</title>

<link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

<link rel="icon" type="\image/ico" href="favicon.ico" />

<script type="text/javascript" src="dvwa/js/dvwaPage.js"></script>

</head>

<body class="home">

<div id="container">

<div id="header">

<img src="dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

</div>

<div id="main\_menu">

<div id="main\_menu\_padded">

<ul class="menuBlocks"><li class="selected"><a href="setup.php">Setup DVWA</a></li>

<li class=""><a href="instructions.php">Instructions</a></li>

</ul><ul class="menuBlocks"><li class=""><a href="about.php">About</a></li>

</ul>

</div>

</div>

<div id="main\_body">

<div class="body\_padded">

<h1>Database Setup <img src="dvwa/images/spanner.png" /></h1>

<p>Click on the 'Create / Reset Database' button below to create or reset your database.<br />

If you get an error make sure you have the correct user credentials in: <em>/var/www/html/config/config.inc.php</em></p>

<p>If the database already exists, <em>it will be cleared and the data will be reset</em>.<br />

You can also use this to reset the administrator credentials ("<em>admin</em> // <em>password</em>") at any stage.</p>

<hr />

<br />

<h2>Setup Check</h2>

Operating system: <em>\*nix</em><br />

Backend database: <em>MySQL</em><br />

PHP version: <em>7.0.30-0+deb9u1</em><br />

<br />

Web Server SERVER\_NAME: <em>localhost</em><br />

<br />

PHP function display\_errors: <em>Disabled</em><br />

PHP function safe\_mode: <span class="success">Disabled</span><br/ >

PHP function allow\_url\_include: <span class="success">Enabled</span><br/ >

PHP function allow\_url\_fopen: <span class="success">Enabled</span><br />

PHP function magic\_quotes\_gpc: <span class="success">Disabled</span><br />

PHP module gd: <span class="success">Installed</span><br />

PHP module mysql: <span class="success">Installed</span><br />

PHP module pdo\_mysql: <span class="success">Installed</span><br />

<br />

MySQL username: <em>app</em><br />

MySQL password: <em>\*\*\*\*\*\*</em><br />

MySQL database: <em>dvwa</em><br />

MySQL host: <em>127.0.0.1</em><br />

<br />

reCAPTCHA key: <span class="failure">Missing</span><br />

<br />

[User: www-data] Writable folder /var/www/html/hackable/uploads/: <span class="success">Yes</span><br />

[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: <span class="success">Yes</span><br />

<br />

<br />

[User: www-data] Writable folder /var/www/html/config: <span class="success">Yes</span>

<br />

<i><span class="failure">Status in red</span>, indicate there will be an issue when trying to complete some modules.</i><br />

<br />

If you see disabled on either <i>allow\_url\_fopen</i> or <i>allow\_url\_include</i>, set the following in your php.ini file and restart Apache.<br />

<pre><code>allow\_url\_fopen = On

allow\_url\_include = On</code></pre>

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

<br /><br /><br />

<!-- Create db button -->

<form action="#" method="post">

<input name="create\_db" type="submit" value="Create / Reset Database">

<input type='hidden' name='user\_token' value='c4b3aaf6ba5c10f176a0d13cb19a363d' />

</form>

<br />

<hr />

</div>

<br /><br />

</div>

<div class="clear">

</div>

<div id="system\_info">

</div>

<div id="footer">

<p>Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</p>

<script src='/dvwa/js/add\_event\_listeners.js'></script>

</div>

</div>

</body>

</html>blueadmin@DVWA-VM2:~$

blueadmin@DVWA-VM2:~$ exit

logout

Connection to 10.3.0.6 closed.

root@9ce0421357ab:/etc/ansible/roles# cd ..

root@9ce0421357ab:/etc/ansible# nano hosts

root@9ce0421357ab:/etc/ansible# ansible -m ping elkservers

10.4.0.4 | UNREACHABLE! => {

"changed": false,

"msg": "Failed to connect to the host via ssh: ssh: connect to host 10.4.0.4 port 22: Connection timed out",

"unreachable": true

}

root@9ce0421357ab:/etc/ansible# ssh blueadmin@10.4.0.4

ssh: connect to host 10.4.0.4 port 22: Connection timed out

root@9ce0421357ab:/etc/ansible# ping 10.4.0.4

PING 10.4.0.4 (10.4.0.4) 56(84) bytes of data.

64 bytes from 10.4.0.4: icmp\_seq=1 ttl=63 time=134 ms

64 bytes from 10.4.0.4: icmp\_seq=2 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=3 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=4 ttl=63 time=130 ms

64 bytes from 10.4.0.4: icmp\_seq=5 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=6 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=7 ttl=63 time=130 ms

64 bytes from 10.4.0.4: icmp\_seq=8 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=9 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=10 ttl=63 time=131 ms

64 bytes from 10.4.0.4: icmp\_seq=11 ttl=63 time=131 ms

^C

--- 10.4.0.4 ping statistics ---

11 packets transmitted, 11 received, 0% packet loss, time 10013ms

rtt min/avg/max/mdev = 130.781/131.474/134.112/0.903 ms

root@9ce0421357ab:/etc/ansible# ssh blueadmin@10.4.0.4

The authenticity of host '10.4.0.4 (10.4.0.4)' can't be established.

ECDSA key fingerprint is SHA256:rV6t4G8sYWaUi0P+uYVv7BmcC78ZCAgpYl6vz0wjiMQ.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.4.0.4' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 19:30:22 UTC 2020

System load: 0.0 Processes: 117

Usage of /: 4.3% of 28.90GB Users logged in: 0

Memory usage: 3% IP address for eth0: 10.4.0.4

Swap usage: 0%

0 packages can be updated.

0 updates are security updates.

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.

blueadmin@Elk-Server:~$ exit

logout

Connection to 10.4.0.4 closed.

root@9ce0421357ab:/etc/ansible# cd roles

root@9ce0421357ab:/etc/ansible/roles# nano elk-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# nano elk-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# ansible-playbook elk-playbook.yml

PLAY [Configure Elk VM with Docker] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.4.0.4]

TASK [Install docker.io] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[WARNING]: Updating cache and auto-installing missing dependency: python-apt

changed: [10.4.0.4]

TASK [Install python-pip] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

TASK [Install Docker module] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

TASK [Increase virtual memory] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

TASK [download and launch a docker elk container] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.4.0.4]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.4.0.4 : ok=6 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@9ce0421357ab:/etc/ansible/roles# exit

exit

blueadmin@Jump-Box-Provisioner:~$ /etc/ansible

-bash: /etc/ansible: No such file or directory

blueadmin@Jump-Box-Provisioner:~$ sudo docker container list -a

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

9ce0421357ab cyberxsecurity/ansible:latest "bash" 3 hours ago Exited (0) 6 minutes ago nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker start nice\_tu

nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach

"docker attach" requires exactly 1 argument.

See 'docker attach --help'.

Usage: docker attach [OPTIONS] CONTAINER

Attach local standard input, output, and error streams to a running container

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach contanier

Error: No such container: contanier

blueadmin@Jump-Box-Provisioner:~$ exit

logout

There are stopped jobs.

blueadmin@Jump-Box-Provisioner:~$ exit

logout

Connection to 52.183.62.233 closed.

sysadmin@ubuntu-vm:~/.ssh$ ssh blueadmin@52.183.62.233

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 20:15:47 UTC 2020

System load: 0.08 Processes: 112

Usage of /: 7.1% of 28.90GB Users logged in: 0

Memory usage: 42% IP address for eth0: 10.3.0.4

Swap usage: 0% IP address for docker0: 172.17.0.1

22 packages can be updated.

4 updates are security updates.

Last login: Fri Jun 5 16:57:16 2020 from 73.82.221.157

blueadmin@Jump-Box-Provisioner:~$ sudo docker container list -a

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

9ce0421357ab cyberxsecurity/ansible:latest "bash" 3 hours ago Up 8 minutes nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker start nice\_tu

nice\_tu

blueadmin@Jump-Box-Provisioner:~$ sudo docker attach nice\_tu

root@9ce0421357ab:~# ssh blueadmin@10.4.0.4

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1022-azure x86\_64)

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

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

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

System information as of Fri Jun 5 20:20:10 UTC 2020

System load: 0.06 Processes: 129

Usage of /: 17.0% of 28.90GB Users logged in: 0

Memory usage: 41% IP address for eth0: 10.4.0.4

Swap usage: 0% IP address for docker0: 172.17.0.1

22 packages can be updated.

4 updates are security updates.

Last login: Fri Jun 5 19:54:05 2020 from 10.3.0.4

blueadmin@Elk-Server:~$ sudo docker ps

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

3546ff11486b sebp/elk "/usr/local/bin/star…" 22 minutes ago Up 22 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

blueadmin@Elk-Server:~$ exit

logout

Connection to 10.4.0.4 closed.

root@9ce0421357ab:~# cd /etc/ansible/

root@9ce0421357ab:/etc/ansible# ls

ansible.cfg hosts roles

root@9ce0421357ab:/etc/ansible# cd roles

root@9ce0421357ab:/etc/ansible/roles# touch filebeat-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# mkdir files

root@9ce0421357ab:/etc/ansible/roles# nano filebeat-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# cd roles

bash: cd: roles: No such file or directory

root@9ce0421357ab:/etc/ansible/roles# cd files

root@9ce0421357ab:/etc/ansible/roles/files# ls

root@9ce0421357ab:/etc/ansible/roles/files# touch filebeat.yml

root@9ce0421357ab:/etc/ansible/roles/files# nano filebeat.yml

root@9ce0421357ab:/etc/ansible/roles/files# nano filebeat.yml

root@9ce0421357ab:/etc/ansible/roles/files# nano filebeat.yml

root@9ce0421357ab:/etc/ansible/roles/files# apt-get upgrade --yes

Reading package lists... Done

Building dependency tree

Reading state information... Done

Calculating upgrade... Done

0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

root@9ce0421357ab:/etc/ansible/roles/files# apt-get update

Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]

Get:2 http://ppa.launchpad.net/ansible/ansible/ubuntu bionic InRelease [15.9 kB]

Get:3 http://archive.ubuntu.com/ubuntu bionic InRelease [242 kB]

Get:4 http://ppa.launchpad.net/ansible/ansible/ubuntu bionic/main amd64 Packages [622 B]

Get:5 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [856 kB]

Get:6 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]

Get:7 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]

Get:8 http://archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [186 kB]

Get:9 http://archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages [13.5 kB]

Get:10 http://archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [11.3 MB]

Get:11 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [933 kB]

Get:12 http://security.ubuntu.com/ubuntu bionic-security/restricted amd64 Packages [59.3 kB]

Get:13 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [8815 B]

Get:14 http://archive.ubuntu.com/ubuntu bionic/main amd64 Packages [1344 kB]

Get:15 http://archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [73.6 kB]

Get:16 http://archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [20.1 kB]

Get:17 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1387 kB]

Get:18 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [1230 kB]

Get:19 http://archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [8286 B]

Get:20 http://archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [8158 B]

Fetched 18.0 MB in 4s (4151 kB/s)

Reading package lists... Done

root@9ce0421357ab:/etc/ansible/roles/files# apt-get upgrade --yes

Reading package lists... Done

Building dependency tree

Reading state information... Done

Calculating upgrade... Done

The following packages will be upgraded:

ansible apt base-files bsdutils ca-certificates distro-info-data e2fsprogs fdisk gcc-8-base libapt-inst2.0 libapt-pkg5.0 libblkid1 libbsd0

libcom-err2 libext2fs2 libfdisk1 libgcc1 libgcrypt20 libglib2.0-0 libgnutls30 libldap-2.4-2 libldap-common libmount1 libpython2.7-minimal

libpython2.7-stdlib libpython3.6 libpython3.6-minimal libpython3.6-stdlib libsasl2-2 libsasl2-modules-db libsmartcols1 libsqlite3-0 libss2

libssl1.1 libstdc++6 libsystemd0 libudev1 libuuid1 mount openssl python-apt-common python2.7 python2.7-minimal python3-apt

python3-software-properties python3.6 python3.6-minimal software-properties-common util-linux vim vim-common vim-runtime xxd

53 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 32.2 MB of archives.

After this operation, 124 kB of additional disk space will be used.

Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 base-files amd64 10.1ubuntu2.8 [59.9 kB]

Get:2 http://ppa.launchpad.net/ansible/ansible/ubuntu bionic/main amd64 ansible all 2.9.9-1ppa~bionic [5790 kB]

Get:3 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 bsdutils amd64 1:2.31.1-0.4ubuntu3.6 [60.3 kB]

Get:4 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libext2fs2 amd64 1.44.1-1ubuntu1.3 [157 kB]

Get:5 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 e2fsprogs amd64 1.44.1-1ubuntu1.3 [391 kB]

Get:6 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libuuid1 amd64 2.31.1-0.4ubuntu3.6 [20.1 kB]

Get:7 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libblkid1 amd64 2.31.1-0.4ubuntu3.6 [124 kB]

Get:8 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libfdisk1 amd64 2.31.1-0.4ubuntu3.6 [164 kB]

Get:9 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libmount1 amd64 2.31.1-0.4ubuntu3.6 [136 kB]

Get:10 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libsmartcols1 amd64 2.31.1-0.4ubuntu3.6 [83.7 kB]

Get:11 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 fdisk amd64 2.31.1-0.4ubuntu3.6 [108 kB]

Get:12 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 util-linux amd64 2.31.1-0.4ubuntu3.6 [903 kB]

Get:13 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 gcc-8-base amd64 8.4.0-1ubuntu1~18.04 [18.7 kB]

Get:14 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libgcc1 amd64 1:8.4.0-1ubuntu1~18.04 [40.6 kB]

Get:15 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libstdc++6 amd64 8.4.0-1ubuntu1~18.04 [400 kB]

Get:16 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libsystemd0 amd64 237-3ubuntu10.41 [207 kB]

Get:17 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libudev1 amd64 237-3ubuntu10.41 [56.8 kB]

Get:18 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libapt-pkg5.0 amd64 1.6.12ubuntu0.1 [807 kB]

Get:19 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libgnutls30 amd64 3.5.18-1ubuntu1.3 [646 kB]

Get:20 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 apt amd64 1.6.12ubuntu0.1 [1201 kB]

Get:21 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 mount amd64 2.31.1-0.4ubuntu3.6 [107 kB]

Get:22 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython3.6 amd64 3.6.9-1~18.04ubuntu1 [1414 kB]

Get:23 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libssl1.1 amd64 1.1.1-1ubuntu2.1~18.04.6 [1301 kB]

Get:24 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3.6 amd64 3.6.9-1~18.04ubuntu1 [203 kB]

Get:25 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython3.6-stdlib amd64 3.6.9-1~18.04ubuntu1 [1710 kB]

Get:26 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3.6-minimal amd64 3.6.9-1~18.04ubuntu1 [1609 kB]

Get:27 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython3.6-minimal amd64 3.6.9-1~18.04ubuntu1 [533 kB]

Get:28 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libsqlite3-0 amd64 3.22.0-1ubuntu0.3 [498 kB]

Get:29 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python2.7 amd64 2.7.17-1~18.04ubuntu1 [248 kB]

Get:30 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython2.7-stdlib amd64 2.7.17-1~18.04ubuntu1 [1915 kB]

Get:31 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python2.7-minimal amd64 2.7.17-1~18.04ubuntu1 [1294 kB]

Get:32 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython2.7-minimal amd64 2.7.17-1~18.04ubuntu1 [335 kB]

Get:33 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libcom-err2 amd64 1.44.1-1ubuntu1.3 [8848 B]

Get:34 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libgcrypt20 amd64 1.8.1-4ubuntu1.2 [417 kB]

Get:35 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libss2 amd64 1.44.1-1ubuntu1.3 [11.1 kB]

Get:36 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssl amd64 1.1.1-1ubuntu2.1~18.04.6 [614 kB]

Get:37 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 ca-certificates all 20190110~18.04.1 [146 kB]

Get:38 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 distro-info-data all 0.37ubuntu0.7 [4676 B]

Get:39 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libapt-inst2.0 amd64 1.6.12ubuntu0.1 [54.4 kB]

Get:40 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libbsd0 amd64 0.8.7-1ubuntu0.1 [41.6 kB]

Get:41 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libglib2.0-0 amd64 2.56.4-0ubuntu0.18.04.6 [1171 kB]

Get:42 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 vim amd64 2:8.0.1453-1ubuntu1.3 [1153 kB]

Get:43 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 vim-runtime all 2:8.0.1453-1ubuntu1.3 [5436 kB]

Get:44 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 xxd amd64 2:8.0.1453-1ubuntu1.3 [49.4 kB]

Get:45 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 vim-common all 2:8.0.1453-1ubuntu1.3 [70.6 kB]

Get:46 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python-apt-common all 1.6.5ubuntu0.3 [16.8 kB]

Get:47 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-apt amd64 1.6.5ubuntu0.3 [149 kB]

Get:48 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libsasl2-modules-db amd64 2.1.27~101-g0780600+dfsg-3ubuntu2.1 [14.8 kB]

Get:49 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libsasl2-2 amd64 2.1.27~101-g0780600+dfsg-3ubuntu2.1 [49.2 kB]

Get:50 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libldap-common all 2.4.45+dfsg-1ubuntu1.5 [16.9 kB]

Get:51 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libldap-2.4-2 amd64 2.4.45+dfsg-1ubuntu1.5 [155 kB]

Get:52 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 software-properties-common all 0.96.24.32.13 [10.0 kB]

Get:53 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-software-properties all 0.96.24.32.13 [23.8 kB]

Fetched 32.2 MB in 3s (10.9 MB/s)

debconf: delaying package configuration, since apt-utils is not installed

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../base-files\_10.1ubuntu2.8\_amd64.deb ...

Unpacking base-files (10.1ubuntu2.8) over (10.1ubuntu2.7) ...

Setting up base-files (10.1ubuntu2.8) ...

Installing new version of config file /etc/issue ...

Installing new version of config file /etc/issue.net ...

Installing new version of config file /etc/lsb-release ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../bsdutils\_1%3a2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking bsdutils (1:2.31.1-0.4ubuntu3.6) over (1:2.31.1-0.4ubuntu3.4) ...

Setting up bsdutils (1:2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libext2fs2\_1.44.1-1ubuntu1.3\_amd64.deb ...

Unpacking libext2fs2:amd64 (1.44.1-1ubuntu1.3) over (1.44.1-1ubuntu1.2) ...

Setting up libext2fs2:amd64 (1.44.1-1ubuntu1.3) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../e2fsprogs\_1.44.1-1ubuntu1.3\_amd64.deb ...

Unpacking e2fsprogs (1.44.1-1ubuntu1.3) over (1.44.1-1ubuntu1.2) ...

Setting up e2fsprogs (1.44.1-1ubuntu1.3) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libuuid1\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking libuuid1:amd64 (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up libuuid1:amd64 (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libblkid1\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking libblkid1:amd64 (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up libblkid1:amd64 (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libfdisk1\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking libfdisk1:amd64 (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up libfdisk1:amd64 (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libmount1\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking libmount1:amd64 (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up libmount1:amd64 (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libsmartcols1\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking libsmartcols1:amd64 (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up libsmartcols1:amd64 (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../fdisk\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking fdisk (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up fdisk (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../util-linux\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking util-linux (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Setting up util-linux (2.31.1-0.4ubuntu3.6) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../gcc-8-base\_8.4.0-1ubuntu1~18.04\_amd64.deb ...

Unpacking gcc-8-base:amd64 (8.4.0-1ubuntu1~18.04) over (8.3.0-6ubuntu1~18.04.1) ...

Setting up gcc-8-base:amd64 (8.4.0-1ubuntu1~18.04) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libgcc1\_1%3a8.4.0-1ubuntu1~18.04\_amd64.deb ...

Unpacking libgcc1:amd64 (1:8.4.0-1ubuntu1~18.04) over (1:8.3.0-6ubuntu1~18.04.1) ...

Setting up libgcc1:amd64 (1:8.4.0-1ubuntu1~18.04) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libstdc++6\_8.4.0-1ubuntu1~18.04\_amd64.deb ...

Unpacking libstdc++6:amd64 (8.4.0-1ubuntu1~18.04) over (8.3.0-6ubuntu1~18.04.1) ...

Setting up libstdc++6:amd64 (8.4.0-1ubuntu1~18.04) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libsystemd0\_237-3ubuntu10.41\_amd64.deb ...

Unpacking libsystemd0:amd64 (237-3ubuntu10.41) over (237-3ubuntu10.31) ...

Setting up libsystemd0:amd64 (237-3ubuntu10.41) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libudev1\_237-3ubuntu10.41\_amd64.deb ...

Unpacking libudev1:amd64 (237-3ubuntu10.41) over (237-3ubuntu10.31) ...

Setting up libudev1:amd64 (237-3ubuntu10.41) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libapt-pkg5.0\_1.6.12ubuntu0.1\_amd64.deb ...

Unpacking libapt-pkg5.0:amd64 (1.6.12ubuntu0.1) over (1.6.12) ...

Setting up libapt-pkg5.0:amd64 (1.6.12ubuntu0.1) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libgnutls30\_3.5.18-1ubuntu1.3\_amd64.deb ...

Unpacking libgnutls30:amd64 (3.5.18-1ubuntu1.3) over (3.5.18-1ubuntu1.1) ...

Setting up libgnutls30:amd64 (3.5.18-1ubuntu1.3) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../apt\_1.6.12ubuntu0.1\_amd64.deb ...

Unpacking apt (1.6.12ubuntu0.1) over (1.6.12) ...

Setting up apt (1.6.12ubuntu0.1) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../00-mount\_2.31.1-0.4ubuntu3.6\_amd64.deb ...

Unpacking mount (2.31.1-0.4ubuntu3.6) over (2.31.1-0.4ubuntu3.4) ...

Preparing to unpack .../01-libpython3.6\_3.6.9-1~18.04ubuntu1\_amd64.deb ...

Unpacking libpython3.6:amd64 (3.6.9-1~18.04ubuntu1) over (3.6.9-1~18.04) ...

Preparing to unpack .../02-libssl1.1\_1.1.1-1ubuntu2.1~18.04.6\_amd64.deb ...

Unpacking libssl1.1:amd64 (1.1.1-1ubuntu2.1~18.04.6) over (1.1.1-1ubuntu2.1~18.04.5) ...

Preparing to unpack .../03-python3.6\_3.6.9-1~18.04ubuntu1\_amd64.deb ...

Unpacking python3.6 (3.6.9-1~18.04ubuntu1) over (3.6.9-1~18.04) ...

Preparing to unpack .../04-libpython3.6-stdlib\_3.6.9-1~18.04ubuntu1\_amd64.deb ...

Unpacking libpython3.6-stdlib:amd64 (3.6.9-1~18.04ubuntu1) over (3.6.9-1~18.04) ...

Preparing to unpack .../05-python3.6-minimal\_3.6.9-1~18.04ubuntu1\_amd64.deb ...

Unpacking python3.6-minimal (3.6.9-1~18.04ubuntu1) over (3.6.9-1~18.04) ...

Preparing to unpack .../06-libpython3.6-minimal\_3.6.9-1~18.04ubuntu1\_amd64.deb ...

Unpacking libpython3.6-minimal:amd64 (3.6.9-1~18.04ubuntu1) over (3.6.9-1~18.04) ...

Preparing to unpack .../07-libsqlite3-0\_3.22.0-1ubuntu0.3\_amd64.deb ...

Unpacking libsqlite3-0:amd64 (3.22.0-1ubuntu0.3) over (3.22.0-1ubuntu0.2) ...

Preparing to unpack .../08-python2.7\_2.7.17-1~18.04ubuntu1\_amd64.deb ...

Unpacking python2.7 (2.7.17-1~18.04ubuntu1) over (2.7.15-4ubuntu4~18.04.2) ...

Preparing to unpack .../09-libpython2.7-stdlib\_2.7.17-1~18.04ubuntu1\_amd64.deb ...

Unpacking libpython2.7-stdlib:amd64 (2.7.17-1~18.04ubuntu1) over (2.7.15-4ubuntu4~18.04.2) ...

Preparing to unpack .../10-python2.7-minimal\_2.7.17-1~18.04ubuntu1\_amd64.deb ...

Unpacking python2.7-minimal (2.7.17-1~18.04ubuntu1) over (2.7.15-4ubuntu4~18.04.2) ...

Preparing to unpack .../11-libpython2.7-minimal\_2.7.17-1~18.04ubuntu1\_amd64.deb ...

Unpacking libpython2.7-minimal:amd64 (2.7.17-1~18.04ubuntu1) over (2.7.15-4ubuntu4~18.04.2) ...

Preparing to unpack .../12-libcom-err2\_1.44.1-1ubuntu1.3\_amd64.deb ...

Unpacking libcom-err2:amd64 (1.44.1-1ubuntu1.3) over (1.44.1-1ubuntu1.2) ...

Setting up libcom-err2:amd64 (1.44.1-1ubuntu1.3) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libgcrypt20\_1.8.1-4ubuntu1.2\_amd64.deb ...

Unpacking libgcrypt20:amd64 (1.8.1-4ubuntu1.2) over (1.8.1-4ubuntu1.1) ...

Setting up libgcrypt20:amd64 (1.8.1-4ubuntu1.2) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../libss2\_1.44.1-1ubuntu1.3\_amd64.deb ...

Unpacking libss2:amd64 (1.44.1-1ubuntu1.3) over (1.44.1-1ubuntu1.2) ...

Setting up libss2:amd64 (1.44.1-1ubuntu1.3) ...

(Reading database ... 16471 files and directories currently installed.)

Preparing to unpack .../00-openssl\_1.1.1-1ubuntu2.1~18.04.6\_amd64.deb ...

Unpacking openssl (1.1.1-1ubuntu2.1~18.04.6) over (1.1.1-1ubuntu2.1~18.04.5) ...

Preparing to unpack .../01-ca-certificates\_20190110~18.04.1\_all.deb ...

Unpacking ca-certificates (20190110~18.04.1) over (20180409) ...

Preparing to unpack .../02-distro-info-data\_0.37ubuntu0.7\_all.deb ...

Unpacking distro-info-data (0.37ubuntu0.7) over (0.37ubuntu0.6) ...

Preparing to unpack .../03-libapt-inst2.0\_1.6.12ubuntu0.1\_amd64.deb ...

Unpacking libapt-inst2.0:amd64 (1.6.12ubuntu0.1) over (1.6.12) ...

Preparing to unpack .../04-libbsd0\_0.8.7-1ubuntu0.1\_amd64.deb ...

Unpacking libbsd0:amd64 (0.8.7-1ubuntu0.1) over (0.8.7-1) ...

Preparing to unpack .../05-libglib2.0-0\_2.56.4-0ubuntu0.18.04.6\_amd64.deb ...

Unpacking libglib2.0-0:amd64 (2.56.4-0ubuntu0.18.04.6) over (2.56.4-0ubuntu0.18.04.4) ...

Preparing to unpack .../06-vim\_2%3a8.0.1453-1ubuntu1.3\_amd64.deb ...

Unpacking vim (2:8.0.1453-1ubuntu1.3) over (2:8.0.1453-1ubuntu1.1) ...

Preparing to unpack .../07-vim-runtime\_2%3a8.0.1453-1ubuntu1.3\_all.deb ...

Unpacking vim-runtime (2:8.0.1453-1ubuntu1.3) over (2:8.0.1453-1ubuntu1.1) ...

Preparing to unpack .../08-xxd\_2%3a8.0.1453-1ubuntu1.3\_amd64.deb ...

Unpacking xxd (2:8.0.1453-1ubuntu1.3) over (2:8.0.1453-1ubuntu1.1) ...

Preparing to unpack .../09-vim-common\_2%3a8.0.1453-1ubuntu1.3\_all.deb ...

Unpacking vim-common (2:8.0.1453-1ubuntu1.3) over (2:8.0.1453-1ubuntu1.1) ...

Preparing to unpack .../10-python-apt-common\_1.6.5ubuntu0.3\_all.deb ...

Unpacking python-apt-common (1.6.5ubuntu0.3) over (1.6.4) ...

Preparing to unpack .../11-python3-apt\_1.6.5ubuntu0.3\_amd64.deb ...

Unpacking python3-apt (1.6.5ubuntu0.3) over (1.6.4) ...

Preparing to unpack .../12-ansible\_2.9.9-1ppa~bionic\_all.deb ...

Unpacking ansible (2.9.9-1ppa~bionic) over (2.9.2-1ppa~bionic) ...

Preparing to unpack .../13-libsasl2-modules-db\_2.1.27~101-g0780600+dfsg-3ubuntu2.1\_amd64.deb ...

Unpacking libsasl2-modules-db:amd64 (2.1.27~101-g0780600+dfsg-3ubuntu2.1) over (2.1.27~101-g0780600+dfsg-3ubuntu2) ...

Preparing to unpack .../14-libsasl2-2\_2.1.27~101-g0780600+dfsg-3ubuntu2.1\_amd64.deb ...

Unpacking libsasl2-2:amd64 (2.1.27~101-g0780600+dfsg-3ubuntu2.1) over (2.1.27~101-g0780600+dfsg-3ubuntu2) ...

Preparing to unpack .../15-libldap-common\_2.4.45+dfsg-1ubuntu1.5\_all.deb ...

Unpacking libldap-common (2.4.45+dfsg-1ubuntu1.5) over (2.4.45+dfsg-1ubuntu1.4) ...

Preparing to unpack .../16-libldap-2.4-2\_2.4.45+dfsg-1ubuntu1.5\_amd64.deb ...

Unpacking libldap-2.4-2:amd64 (2.4.45+dfsg-1ubuntu1.5) over (2.4.45+dfsg-1ubuntu1.4) ...

Preparing to unpack .../17-software-properties-common\_0.96.24.32.13\_all.deb ...

Unpacking software-properties-common (0.96.24.32.13) over (0.96.24.32.11) ...

Preparing to unpack .../18-python3-software-properties\_0.96.24.32.13\_all.deb ...

Unpacking python3-software-properties (0.96.24.32.13) over (0.96.24.32.11) ...

Setting up python-apt-common (1.6.5ubuntu0.3) ...

Setting up libapt-inst2.0:amd64 (1.6.12ubuntu0.1) ...

Setting up python3-apt (1.6.5ubuntu0.3) ...

Setting up xxd (2:8.0.1453-1ubuntu1.3) ...

Setting up libldap-common (2.4.45+dfsg-1ubuntu1.5) ...

Setting up libglib2.0-0:amd64 (2.56.4-0ubuntu0.18.04.6) ...

No schema files found: doing nothing.

Setting up libsasl2-modules-db:amd64 (2.1.27~101-g0780600+dfsg-3ubuntu2.1) ...

Setting up mount (2.31.1-0.4ubuntu3.6) ...

Setting up libsasl2-2:amd64 (2.1.27~101-g0780600+dfsg-3ubuntu2.1) ...

Setting up distro-info-data (0.37ubuntu0.7) ...

Setting up libbsd0:amd64 (0.8.7-1ubuntu0.1) ...

Setting up ansible (2.9.9-1ppa~bionic) ...

Setting up libldap-2.4-2:amd64 (2.4.45+dfsg-1ubuntu1.5) ...

Setting up libssl1.1:amd64 (1.1.1-1ubuntu2.1~18.04.6) ...

debconf: unable to initialize frontend: Dialog

debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 76.)

debconf: falling back to frontend: Readline

debconf: unable to initialize frontend: Readline

debconf: (Can't locate Term/ReadLine.pm in @INC (you may need to install the Term::ReadLine module) (@INC contains: /etc/perl /usr/local/lib/x86\_64-linux-gnu/perl/5.26.1 /usr/local/share/perl/5.26.1 /usr/lib/x86\_64-linux-gnu/perl5/5.26 /usr/share/perl5 /usr/lib/x86\_64-linux-gnu/perl/5.26 /usr/share/perl/5.26 /usr/local/lib/site\_perl /usr/lib/x86\_64-linux-gnu/perl-base) at /usr/share/perl5/Debconf/FrontEnd/Readline.pm line 7.)

debconf: falling back to frontend: Teletype

Setting up openssl (1.1.1-1ubuntu2.1~18.04.6) ...

Setting up vim-common (2:8.0.1453-1ubuntu1.3) ...

Setting up libsqlite3-0:amd64 (3.22.0-1ubuntu0.3) ...

Setting up python3-software-properties (0.96.24.32.13) ...

Setting up vim-runtime (2:8.0.1453-1ubuntu1.3) ...

Setting up libpython2.7-minimal:amd64 (2.7.17-1~18.04ubuntu1) ...

Setting up ca-certificates (20190110~18.04.1) ...

debconf: unable to initialize frontend: Dialog

debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 76.)

debconf: falling back to frontend: Readline

debconf: unable to initialize frontend: Readline

debconf: (Can't locate Term/ReadLine.pm in @INC (you may need to install the Term::ReadLine module) (@INC contains: /etc/perl /usr/local/lib/x86\_64-linux-gnu/perl/5.26.1 /usr/local/share/perl/5.26.1 /usr/lib/x86\_64-linux-gnu/perl5/5.26 /usr/share/perl5 /usr/lib/x86\_64-linux-gnu/perl/5.26 /usr/share/perl/5.26 /usr/local/lib/site\_perl /usr/lib/x86\_64-linux-gnu/perl-base) at /usr/share/perl5/Debconf/FrontEnd/Readline.pm line 7.)

debconf: falling back to frontend: Teletype

Updating certificates in /etc/ssl/certs...

2 added, 8 removed; done.

Setting up libpython2.7-stdlib:amd64 (2.7.17-1~18.04ubuntu1) ...

Setting up python2.7-minimal (2.7.17-1~18.04ubuntu1) ...

Setting up software-properties-common (0.96.24.32.13) ...

Setting up python2.7 (2.7.17-1~18.04ubuntu1) ...

Setting up libpython3.6-minimal:amd64 (3.6.9-1~18.04ubuntu1) ...

Setting up libpython3.6-stdlib:amd64 (3.6.9-1~18.04ubuntu1) ...

Setting up python3.6-minimal (3.6.9-1~18.04ubuntu1) ...

Setting up libpython3.6:amd64 (3.6.9-1~18.04ubuntu1) ...

Setting up python3.6 (3.6.9-1~18.04ubuntu1) ...

Setting up vim (2:8.0.1453-1ubuntu1.3) ...

Processing triggers for mime-support (3.60ubuntu1) ...

Processing triggers for libc-bin (2.27-3ubuntu1) ...

Processing triggers for ca-certificates (20190110~18.04.1) ...

Updating certificates in /etc/ssl/certs...

0 added, 0 removed; done.

Running hooks in /etc/ca-certificates/update.d...

done.

root@9ce0421357ab:/etc/ansible/roles/files# nano filebeat.yml

root@9ce0421357ab:/etc/ansible/roles/files# ls

filebeat.yml

root@9ce0421357ab:/etc/ansible/roles/files# cd ..

root@9ce0421357ab:/etc/ansible/roles# ls

dvwa-playbook.yml elk-playbook.yml filebeat-playbook.yml files

root@9ce0421357ab:/etc/ansible/roles# nano filebeat-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# ansible-playbook filebeat-playbook.yml

PLAY [installing and launching filebeat] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

fatal: [10.3.0.5]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ssh: connect to host 10.3.0.5 port 22: Connection timed out", "unreachable": true}

fatal: [10.3.0.6]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ssh: connect to host 10.3.0.6 port 22: Connection timed out", "unreachable": true}

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.3.0.5 : ok=0 changed=0 unreachable=1 failed=0 skipped=0 rescued=0 ignored=0

10.3.0.6 : ok=0 changed=0 unreachable=1 failed=0 skipped=0 rescued=0 ignored=0

root@9ce0421357ab:/etc/ansible/roles# ansible-playbook filebeat-playbook.yml

PLAY [installing and launching filebeat] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 10.3.0.5 should use /usr/bin/python3, but is using /usr/bin/python for backward compatibility

with prior Ansible releases. A future Ansible release will default to using the discovered platform python for this host. See

https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information. This feature will be removed in version

2.12. Deprecation warnings can be disabled by setting deprecation\_warnings=False in ansible.cfg.

ok: [10.3.0.5]

fatal: [10.3.0.6]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ssh: connect to host 10.3.0.6 port 22: Connection timed out", "unreachable": true}

TASK [download filebeat deb] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[WARNING]: Consider using the get\_url or uri module rather than running 'curl'. If you need 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: [10.3.0.5]

TASK [install filebeat deb] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

TASK [drop in filebeat.yml] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

TASK [enable and configure system module] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

TASK [setup filebeat] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

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: [10.3.0.5]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.3.0.5 : ok=7 changed=6 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

10.3.0.6 : ok=0 changed=0 unreachable=1 failed=0 skipped=0 rescued=0 ignored=0

root@9ce0421357ab:/etc/ansible/roles# ansible-playbook filebeat-playbook.yml

PLAY [installing and launching filebeat] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 10.3.0.5 should use /usr/bin/python3, but is using /usr/bin/python for backward compatibility

with prior Ansible releases. A future Ansible release will default to using the discovered platform python for this host. See

https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information. This feature will be removed in version

2.12. Deprecation warnings can be disabled by setting deprecation\_warnings=False in ansible.cfg.

ok: [10.3.0.5]

[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 10.3.0.6 should use /usr/bin/python3, but is using /usr/bin/python for backward compatibility

with prior Ansible releases. A future Ansible release will default to using the discovered platform python for this host. See

https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information. This feature will be removed in version

2.12. Deprecation warnings can be disabled by setting deprecation\_warnings=False in ansible.cfg.

ok: [10.3.0.6]

TASK [download filebeat deb] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[WARNING]: Consider using the get\_url or uri module rather than running 'curl'. If you need 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: [10.3.0.6]

changed: [10.3.0.5]

TASK [install filebeat deb] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

changed: [10.3.0.6]

TASK [drop in filebeat.yml] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.3.0.5]

changed: [10.3.0.6]

TASK [enable and configure system module] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

changed: [10.3.0.6]

TASK [setup filebeat] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.3.0.5]

changed: [10.3.0.6]

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: [10.3.0.5]

changed: [10.3.0.6]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.3.0.5 : ok=7 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

10.3.0.6 : ok=7 changed=6 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@9ce0421357ab:/etc/ansible/roles# ls

dvwa-playbook.yml elk-playbook.yml filebeat-playbook.yml files

root@9ce0421357ab:/etc/ansible/roles# touch metricbeat-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# ls

dvwa-playbook.yml elk-playbook.yml filebeat-playbook.yml files metricbeat-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# nano metricbeat-playbook.yml

root@9ce0421357ab:/etc/ansible/roles# nano filebeat-playbook.yml

root@9ce0421357