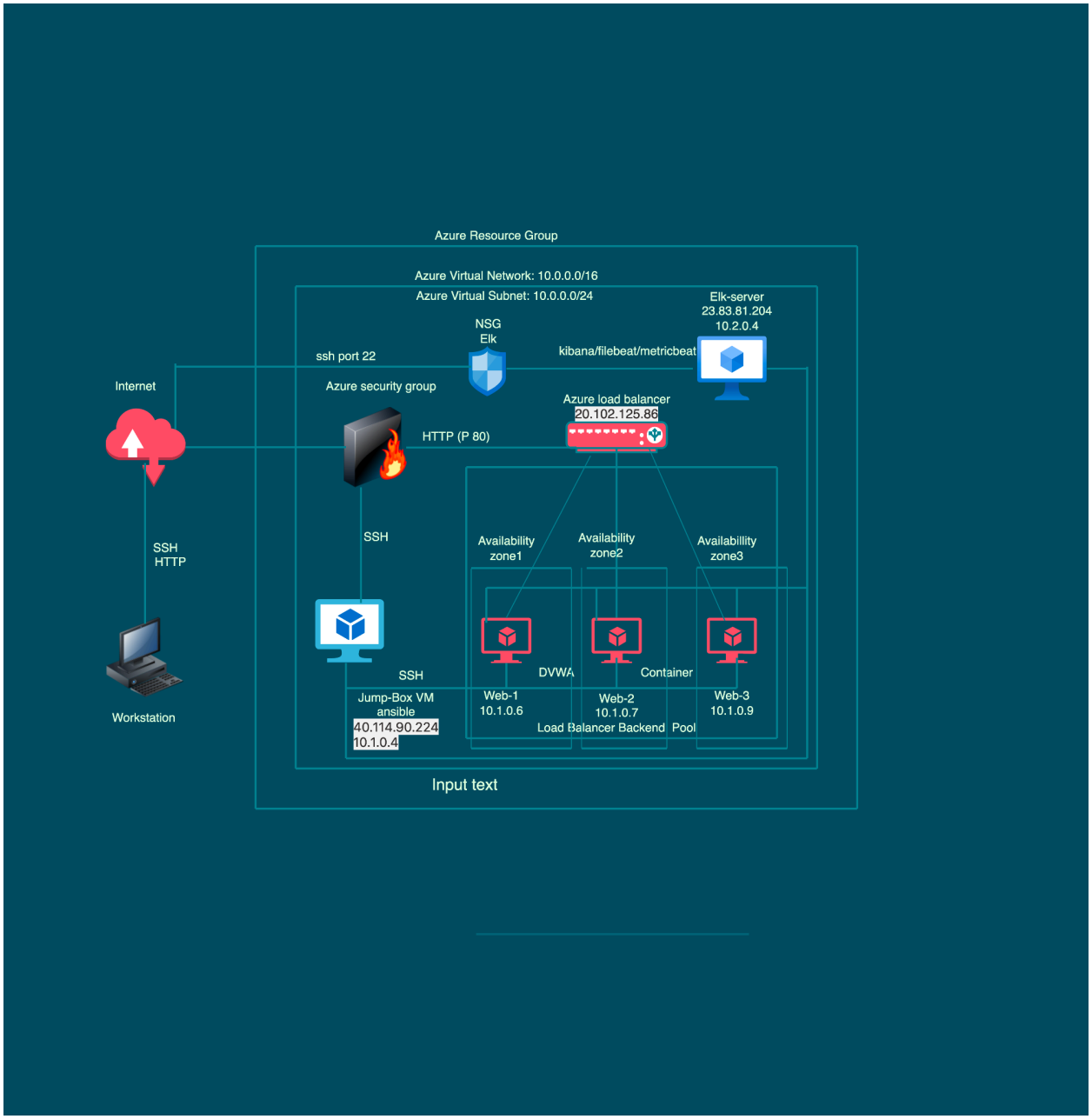
Automated ELK Stack Deployment

The files in this repository were used to configure the network depicted below.



These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the Ansible and YML file may be used to install only certain pieces of it, such as Filebeat.
ELK Installation Playbook
VM with Docker Installation
Filebeats Playbook

Metricbeats Playbook
This document contains the following details:
• Description of the Topology
• Access Policies
• ELK Configuration
 o Beats in Use
 o Machines Being Monitored
• How to Use the Ansible Build

Description of the Topology

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly available,in addition to restricting inbound access to the network.

What aspect of security do load balancers protect?
The load balancer ensures that work to process incoming traffic will be shared by all vulnerable web servers. Access controls will ensure that only authorized users namely, ourselves will be able to connect in the first place.

What is the advantage of a jump box?
The advantage of a jump box is that it allows automation, improves security, audtis traffic of segmented networks, and allows for ease of access control by using a single point to be secured and monitored

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the file systems of the VMs on the network, and system metrics.

What does Filebeat watch for?
Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

What does Metricbeat record?
Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash. Metricbeat helps you monitor your servers by collecting metrics from the system and services running on the server, such as: Apache.

The configuration details of each machine may be found below.

_Note: Use the [Markdown Table Generator](http://www.tablesgenerator.com/markdown_tables) to add/remove values from the table_.

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.1.0.4	Linux
web-1	Server	10.1.0.6	Linux
web-2	Server	10.1.0.7	Linux
web-3	Server	10.1.0.9	Linux
elk	Monitoring	10.2.0.4	Linux
Load Balancer	LB	20.102.125.86	Linux
User	Access Control		

Access Policies

The machines on the internal network are not exposed to the public Internet.
In addition to the above, Azure has provisioned a load balancer in front of all machines except for the jump box. The load balancer's targets are organized into the following availability zones:
* Availability Zone 1: web-1 + web-2 + web-3
* Availability Zone 2: ELK

Only the jump box machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:20.124.115.217

Machines within the network can only be accessed by each other.

- _TODO: Which machine did you allow to access your ELK VM? What was its IP address?_
Jump Box Provisioner Private IP: 10.0.0.4 via ssh port 22 and User Public IP via TCP port 5601.

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

Name	Publicly Accessible	Allowed IP Addresses
Jump Box Provisioner	Yes	20.124.115.217 via ssh port 22
DVWA Web-1	No	10.1.0.6 via ssh port 22
DVWA Web-2	No	10.1.0.7 via ssh port 22
DVWA Web-3	No	10.1.0.9 via ssh port 22
Elk-server	No	10.2.0.4 via ssh TCP port 5601
Load Balancer	NO	20.102.125.86 via HTTP port 80

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

What is the main advantage of automating configuration with Ansible
Ansible automation helps considerably with the representation of Infrastructure as Code (IAC). IAC involves provisioning and management of computing infrastructure and related configuration through machine-processable definition files.

The playbook implements the following tasks:
- TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.

```
- name: Config elk VM with Docker
  hosts: elk
  remote_user: azdmin
  become: true
  tasks:
  # use the apt module to install packages
    - name: Install docker.io
      apt:
        update_cache: yes
        name: docker.io
        state: present

    - name: Install pip3
      apt:
        force_apt_get: yes
        name: python3-pip
        state: present

  # use the pip module to install python
    - name: Install Docker python module
      pip:
        name: docker
        state: present

  # use sysctl to configure the memory
    - name: Use more memory
      sysctl:
        name: vm.max_map_count
        value: '262144'
```

```
    state: present
    reload: yes

# Launch docker elk container
  - name: Download and launch elk container
    docker_container:
        name: elk
        image: sebp/elk:761
        state: started
        restart_policy: always
        published_ports:
          - 5601:5601
          - 9200:9200
          - 5044:5044


# Use systemd to enable docker on boot
  - name: Enable service docker on boot
    systemd:
      name: docker
      enabled: yes
```

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

[TODO: Update the path with the name of your screenshot of docker ps output](Images/docker_ps_output.png)

Elk-server:

```
azdmin@ELK:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED      STATUS
 PORTS
    NAMES
1df32fbf862e   sebp/elk:761   "/usr/local/bin/star…"   8 days 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/tc
p   elk
azdmin@ELK:~$
```

Web-1

```
azdmin@Web-1:~$ sudo docker ps
CONTAINER ID   IMAGE                 COMMAND      CREATED       STATUS       POR
TS                NAMES
3502d6894ae4   cyberxsecurity/dvwa   "/main.sh"   12 days ago   Up 2 hours   0.0
.0.0:80->80/tcp   dvwa
azdmin@Web-1:~$
```

Web-2

```
azdmin@Web-2:~$ sudo docker ps
CONTAINER ID   IMAGE                 COMMAND      CREATED       STATUS       POR
TS                NAMES
3c213ef612df   cyberxsecurity/dvwa   "/main.sh"   12 days ago   Up 3 hours   0.0
.0.0:80->80/tcp   dvwa
azdmin@Web-2:~$
```

Target Machines & Beats

This ELK server is configured to monitor the following machines:
List the IP addresses of the machines you are monitoring:

Web-1 ip:10.1.0.6
Web-2 ip:10.1.0.7
Web-3 ip:10.1.0.9

We have installed the following Beats on these machines:
Elk-server,Web-1 and Web-2
Specify which Beats you successfully installed?
Filebeat and metricbeat

These Beats allow us to collect the following information from each machine:
TODO: In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.:

Filebeat allows us to collect log events.
Ex: Files generated by Apache or MS Azure tools.
Metricbeat allows us to collect the metrics and statistics.
Ex: CPU usage

Using the Playbook

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

SSH into the control node and follow the steps below:
- Copy the Filbeat playbook file to /etc/ansible

- Update the /etc/ansible/hosts file to include Web-1, Web-2 ,Web-3and Elk-server

```
root@fd3e5a63471e:~# cd /etc/ansible
root@fd3e5a63471e:/etc/ansible# ls
ansible.cfg  filebeat-config.yml  files  hosts  playbooks  roles
root@fd3e5a63471e:/etc/ansible#
```

```
# Ex 2: A collection of hosts belonging to the 'webservers' group

[webservers]
10.1.0.7 ansible_python_interpreter=/usr/bin/python3
# 10.1.0.7 = Web-2
10.1.0.6 ansible_python_interpreter=/usr/bin/python3
# 10.1.0.6 = Web-1
10.1.0.9 ansible_python_interpreter=/usr/bin/python3
# 10.1.0.9 = Web-3

#alpha.example.org
#beta.example.org
#192.168.1.100
#192.168.1.110

[elk]
10.2.0.4 ansible_python_interpreter=/usr/bin/python3
# 10.2.0.4 = ELK server
```

- Run the playbook, and navigate to host to check that the installation worked as expected.

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

Copy snippet

```
sudo filebeat setup
sudo service filebeat start
```

Module status

Check that data is received from the Filebeat `system` module

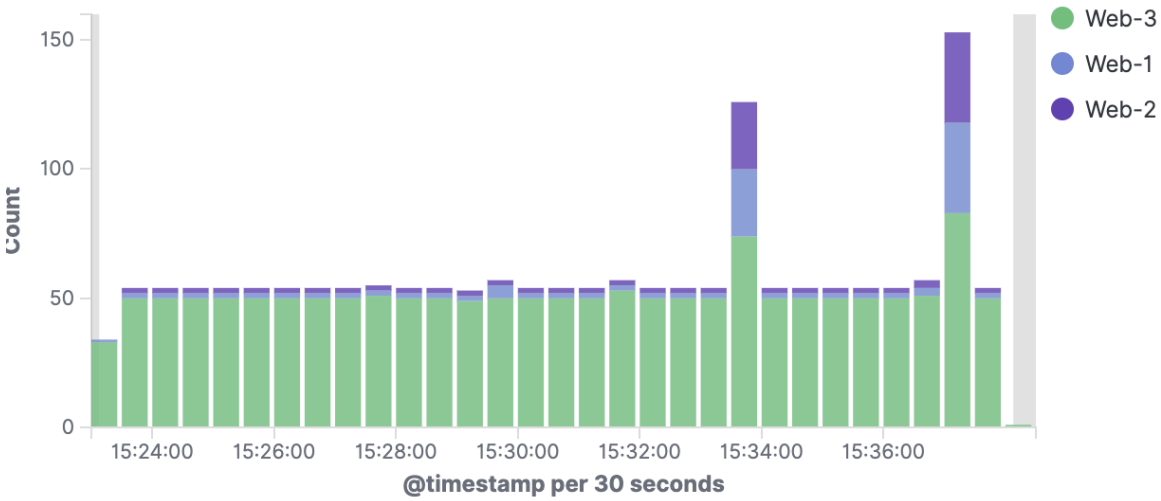
Check data

Data successfully received from this module

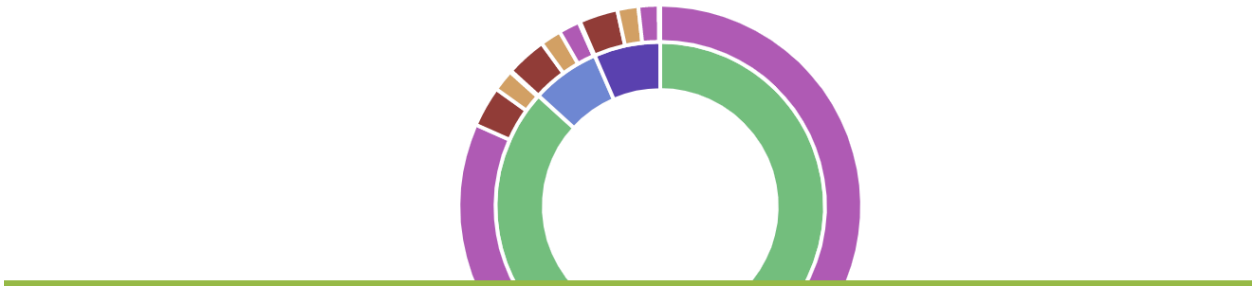
When all steps are complete, you're ready to explore your data.

Syslog | Sudo commands | SSH logins | New users and groups

Syslog events by hostname [Filebeat System] ECS



Syslog hostnames and processes [Filebeat System] ECS



Module status

Check that data is received from the Metricbeat `docker` module

Check data

Data successfully received from this module

Tal

Number of Containers [Metricbeat Docker] ECS

1	0	0
Running	Paused	Stopped

Docker containers per host [Metricbeat Docker] ECS

Docker images and names [Metricbeat Docker] ECS

CPU usage [Metricbeat Docker] ECS

TODO: Answer the following questions to fill in the blanks:
Which file is the playbook?
Filebeat-playbook.yml

Where do you copy it?
Into the /etc/ansbile/files

Which file do you update to make Ansible run the playbook on a specific machine?
/etc/ansible/hosts file and add the IP address of the VM's under [webserver].

How do I specify which machine to install the ELK server on versus which to install Filebeat on?
By specifying two groups in the /etc/ansible/hosts file, labled [webservers] for filebeat, and [ELK] for Elk installation

- Which URL do you navigate to in order to check that the ELK server is running?

http:[Elk.VM.IP]:5601/app/kibana

As a **Bonus**, provide the specific commands the user will need to run to download the playbook, update the files, etc.