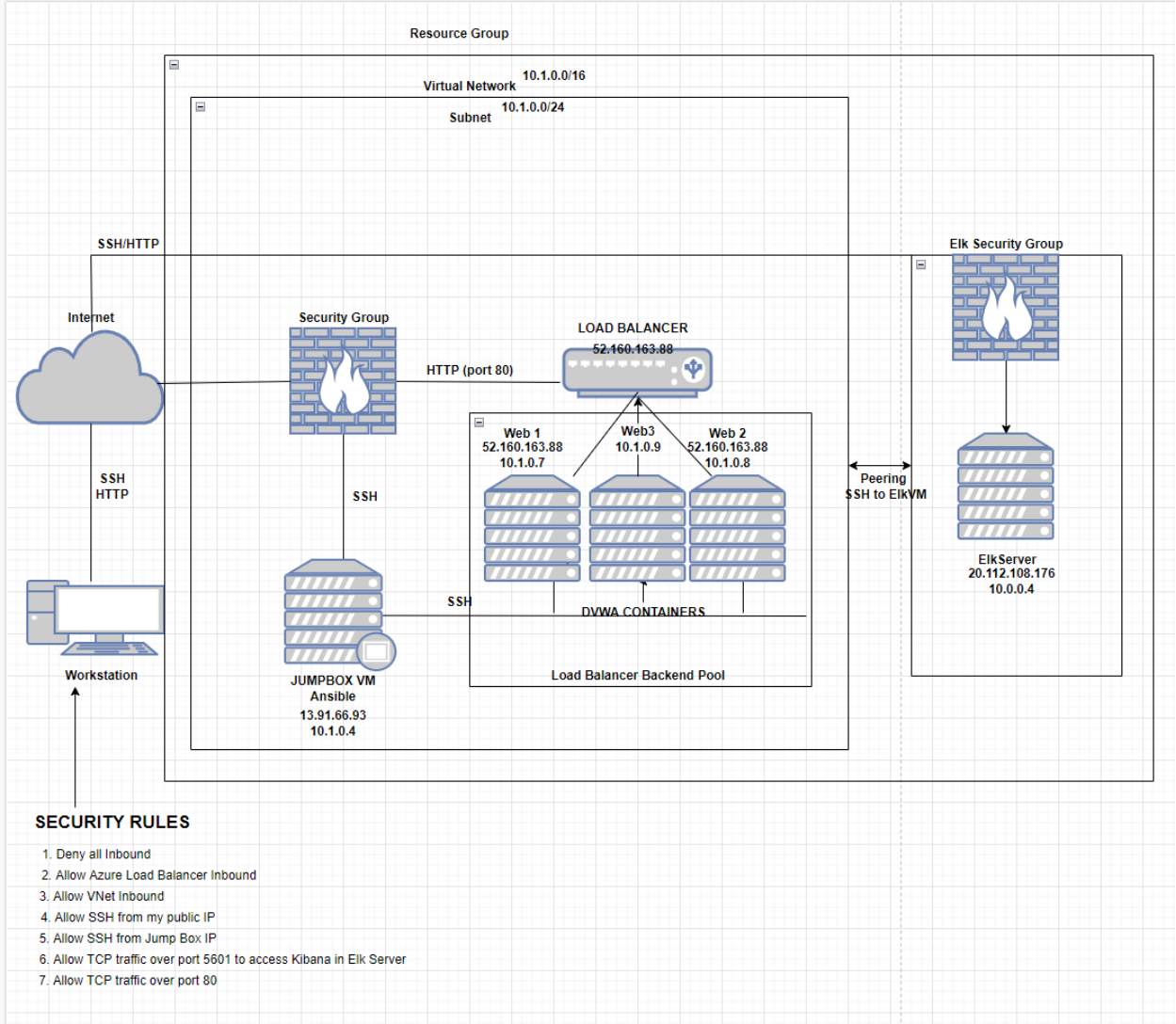
Automated ELK Stack Deployment

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 playbook file may be used to install only certain pieces of it, such as Filebeat.

This document contains the following details:

- Description of the Topology
- Access Policies
- ELK Configuration
    - Beats in Use
    - 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.

The off-loading function of a load balancer defends an organization against distributed denial-of-service (DDoS) attacks by shifting attack traffic. It does this by shifting attack traffic from the corporate server to a public cloud provider.

A jump box can give access to the user from a single node that can be secured and monitored. No hardware cost, access, and ease to setup.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the logs and system traffic.

Filebeat watches for any information in the file system which has been changed and when.

Merticbeat takes the metrics and statistics that it collects and ships them to the output that you specify. Metricbeat helps you monitor your servers by collecting metrics from the system and services running on the server.

The configuration details of each machine may be found below. *Note: Use the Markdown Table Generator to add/remove values from the table*.

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.1.0.4	Linux
Web-1	DVWA	10.1.0.7	Linux
Web-2	DVWA	10.1.0.8	Linux
Web-3	DVWA	10.1.0.9	Linux
ELK	Elk	10.0.0.4	Linux

Access Policies

The machines on the internal network are not exposed to the public Internet. Only the Jumpbox machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

My home IP address

Machines within the network can only be accessed by SSH.

Which machine did you allow to access your ELK VM? What was its IP address?

I allowed the JumpBox VM, and its private IP address-10.1.0.4

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

Name	Publicly Accessible	Allowed IP Addresses
JumpBox VM	Yes	13.91.66.93
Web-1	No	10.1.0.7
Web-2	No	10.1.0.8
Web-3	No	10.1.0.9
ELK	No	20.112.108.176, 10.0.0.4

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because the main advantage is that you can put commands into multiple servers from a single playbook, like how I combined Filebeat and Metricbeat.

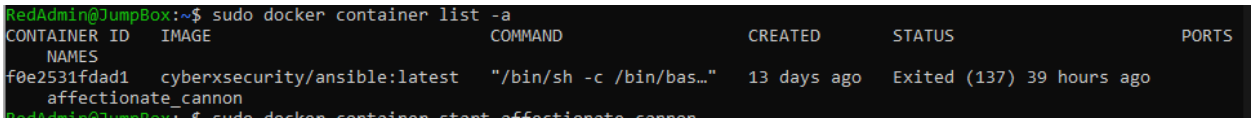
The playbook implements the following tasks:

- Install docker.io
    - name: Install docker.io apt: update_cache: yes name: docker.io state: present
- Install Python-pip
    - name: Install pip3 apt: force_apt_get: yes name: python3-pip state: present

- Install: docker
    - name: Install Docker python module pip: name: docker state: present
- Command: sysctl -w vm.max_map_count=262144

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

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



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 (10.1.0.7), Web-2 (10.1.0.8), Web-3 (10.1.0.9)

We have installed the following Beats on these machines:

- Specify which Beats you successfully installed:

  I installed Filebeat and Metricbeat

These Beats allow us to collect the following information from each machine:

Filebeat is a lightweight shipper for forwarding and centralizing log data. It monitors the log files or locations that one specifies and forwards them to Elasticsearch or Logstash.

Metricbeat is a lightweight shipper that you can install on your servers to collect metrics from the OS and from services running on the server. Metricbeat takes the metrics and statistics that it collects and sends them to either Elasticsearch or Logstash, An example of metricbeat is the measurement of memory usage of your operating system.

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:

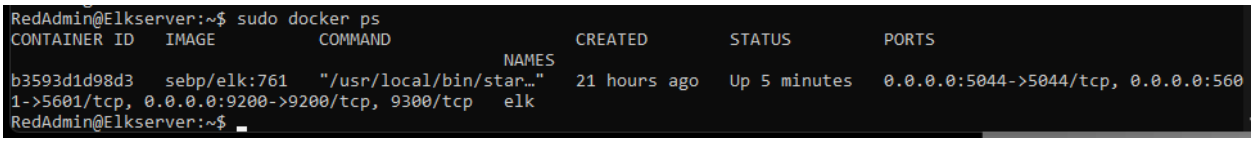
SSH into the control node and follow the steps below:

- Copy the playbook file to /etc/ansible .
- Update the host file to your private IP
- Run the playbook and navigate to Jump Box to check that the installation worked as expected.

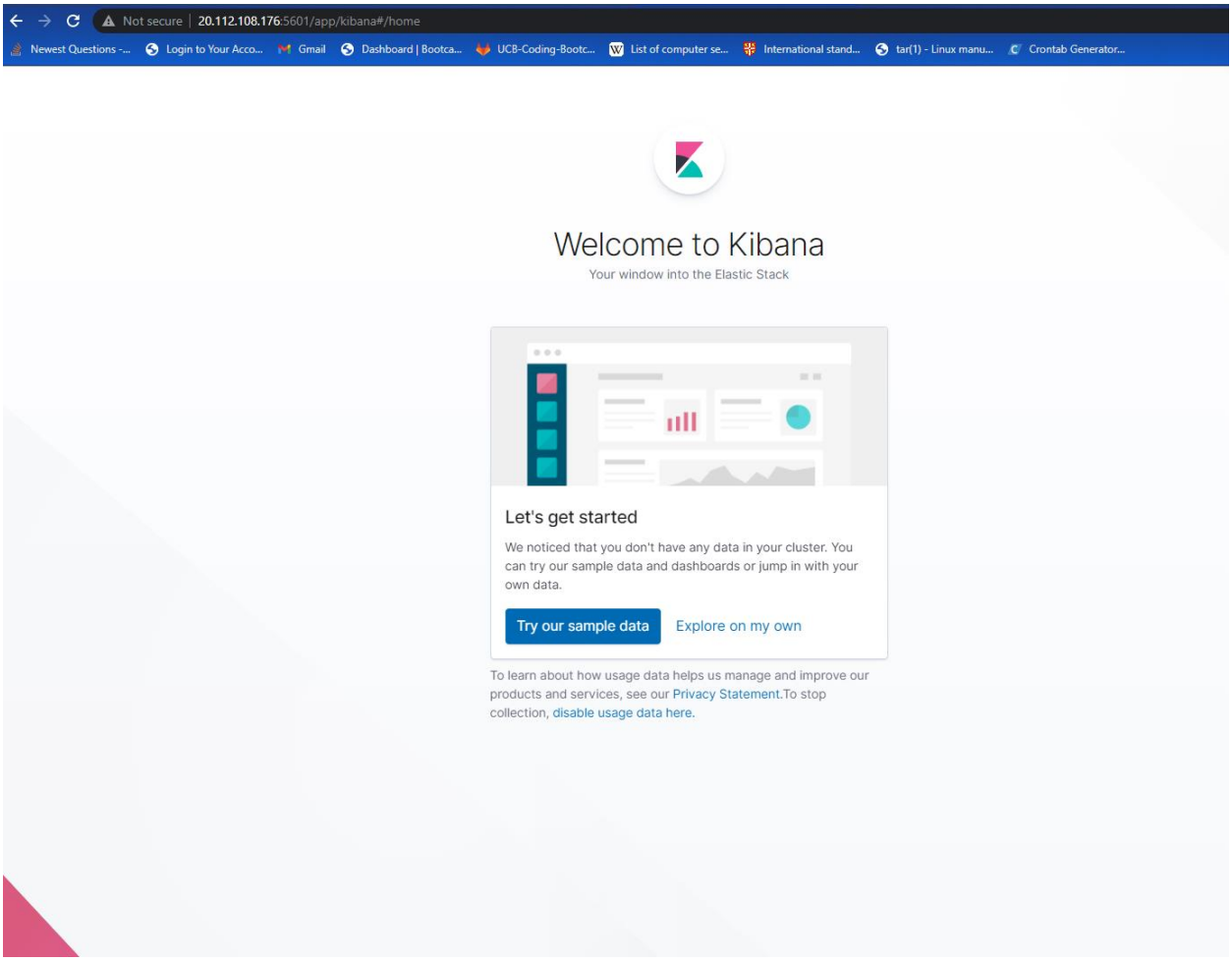
You would need to edit the /etc/ansible/host file to add webserver/elks IP addresses

```
[webservers]
#alpha.example.org
#beta.example.org
#192.168.1.100
#192.168.1.110
10.1.0.7 ansible_python_interpreter=/usr/bin/python3
10.1.0.8 ansible_python_interpreter=/usr/bin/python3
10.1.0.9 ansible_python_interpreter=/usr/bin/python3

[Elk]
10.0.0.4 ansible_python_interpreter=/usr/bin/python3

# If you have multiple hosts following a pattern you can specify
# them like this:

#www[001:006].example.com

# Ex 3: A collection of database servers in the 'dbservers' group
```

Run the playbook, and SSH into the Elk vm, then run docker ps to check that the installation worked as expected.



Navigate to http://[your.ELK-VM.External.IP]:5601/app/kibana to confirm ELK and kibana are running. You may need to try from multiple web browsers Click 'Explore On Your Own' and you should see the following:



Answer the following questions to fill in the blanks:

- Which file is the playbook? Where do you copy it?

  /etc/ansible/file/filebeat-config.yml

- Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on?_

  edit the /etc/ansible/hosts file to add webserver/elkserver ip addresses

- Which URL do you navigate to in order to check that the ELK server is running?
  http://[your.ELK-VM.External.IP]:5601/app/kibana

  Copy the filebeat.yml file to the /etc/ansible/files/ directory.

- Update the configuration file to include the Private IP of the Elk-Server to the ElasticSearch and Kibana sections of the configuration file.

- Create a new playbook in the /etc/ansible/roles/ directory that will install, drop in the updated configuration file, enable and configure system module, run the filebeat setup, and start the filebeat service.

- Create a new playbook in the /etc/ansible/roles/ directory that will install, drop in the updated configuration file, enable and configure system module, run the metricbeat setup, and start the metricbeat service.

- Run the playbooks, and navigate back to the installation page on the ELk-Server GUI, click the check data on the Module Status

- Click the verfiy incoming Data to check and see the receiving logs from the DVWA machines.