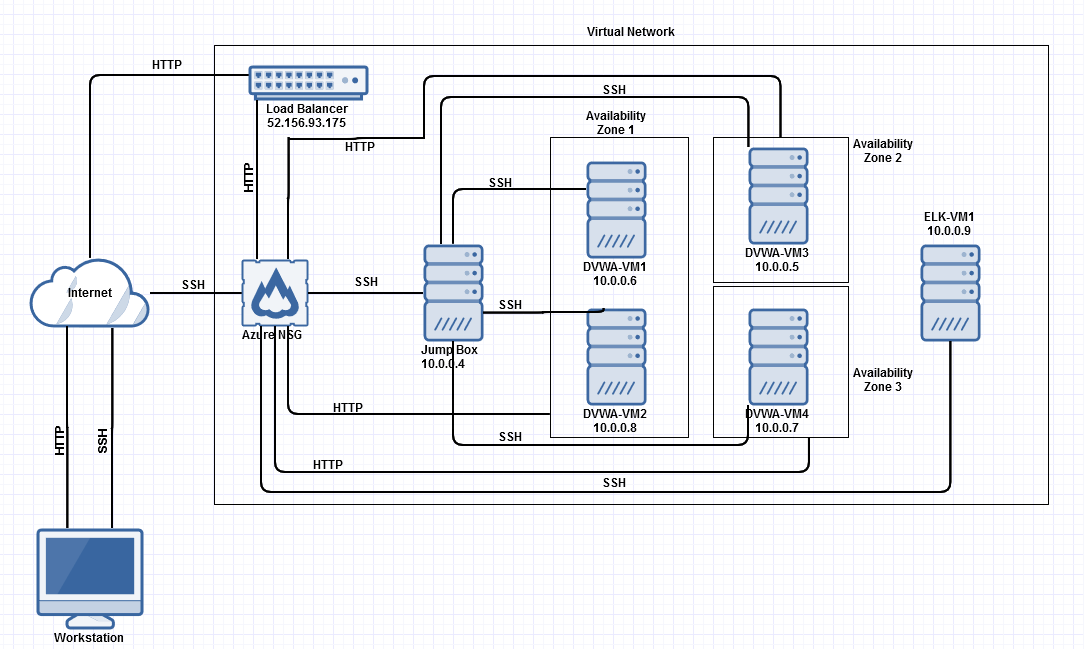
## Automated ELK Stack Deployment  
  
The files in this repository were used to configure the network depicted below.

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

---

- name: Config Web VM with Docker

hosts: webservers

become: true

tasks:

- name: Uninstall apache2

apt:

name: apache2

state: absent

- name: docker.io

apt:

name: docker.io

state: present

- name: Install pip

apt:

name: python-pip

state: present

- name: Install Docker python module

pip:

name: docker

state: present

- name: download and launch a docker web container

docker\_container:

name: dvwa

image: cyberxsecurity/dvwa

state: started

published\_ports: 80:80

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 traffic to the network.  
- **Load balancers protect from DoS attacks. Jump boxes are advantageous because it keeps much of the network from being accessible directly by the user. It provides a layer of separation from critical systems and a potential attacker.**  
image1.png  
The configuration details of each machine may be found below.  
  
|Name | Function | IP Address | Operating System |  
|------------------|------------------|---------------|-----------------------|  
|Jump Box |Gateway | 10.0.0.4 | Linux |  
|DVWA-VM1 |Web server | 10.0.0.6 | Linux |  
|DVWA-VM2 |Web server | 10.0.0.8 | Linux |  
|DVWA-VM3 |Web server | 10.0.0.5 | Linux |  
|DVWA-VM4 |Web server | 10.0.0.7 | Linux |  
|ELK-VM1 |Log server | 10.0.0.9 | Linux |  
  
### 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:  
- 136.49.34.233  
  
Machines within the network can only be accessed by SSH.  
- The local workstation was able to access the ELK VM. The IP was 136.49.34.233   
  
A summary of the access policies in place can be found in the table below.  
  
| Name | Publicly Accessible | Allowed IP Addresses |  
|--------------|-------------------------|----------------------------|  
| Jump Box | No | 136.49.34.233 |  
| ELK | No | 136.49.34.233 |  
| VNet | Yes | All |  
  
### Elk Configuration  
  
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...  
-**Ansible is advantageous because updates to the configuration can be made remotely without any downtime.**  
  
The playbook implements the following tasks:  
- **Install Docker**  
- **Increase Memory**  
- **Download and launch ELK container**  
  
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:  
- **10.0.0.5, 10.0.0.6, 10.0.0.7, 10.0.0.8**  
  
We have installed the following Beats on these machines:  
- **Filebeat**  
  
These Beats allow us to collect the following information from each machine:  
- **Filebeat monitors the log files, collects events, and then forwards them to Elasticsearch for review.**

### 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 **hosts** file to include **IP addresses of Web servers and ELK server**.  
- Which file do you update to make Ansible run the playbook on a specific machine? **Hosts**

- Which URL do you navigate to in order to check that the ELK server is running? **10.0.0.9:5601**