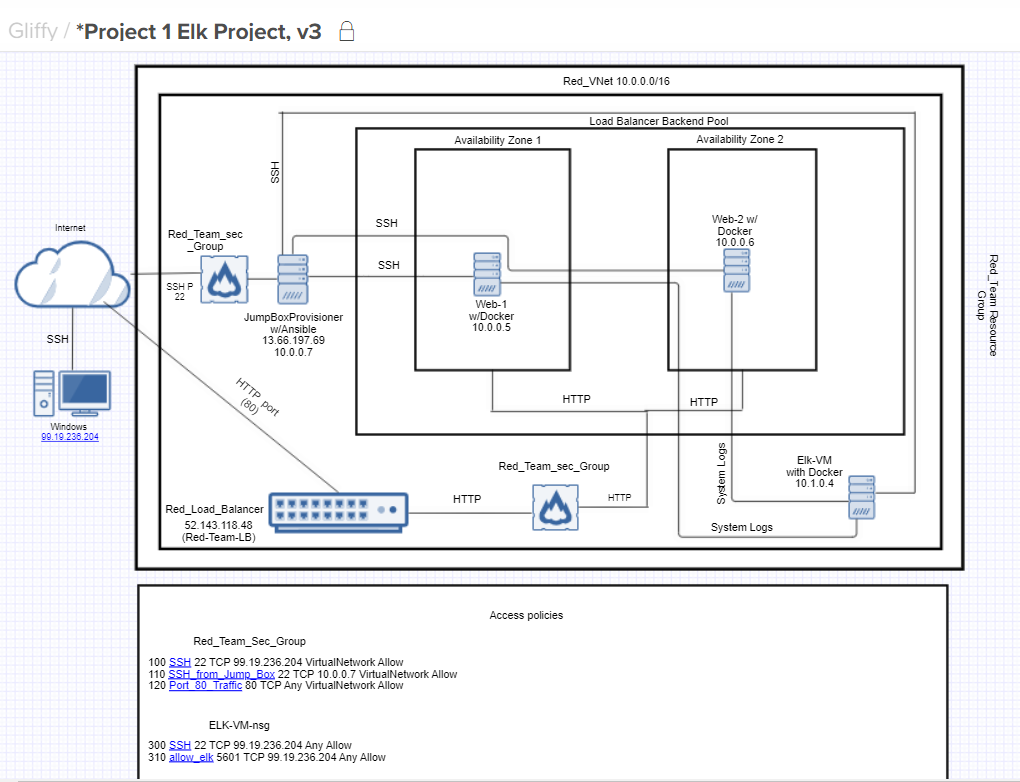
**## Automated ELK Stack Deployment**

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.

- ---

- name: installing and launching filebeat

hosts: webservers

become: yes

tasks:

- name: download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

- name: install filebeat deb

command: dpkg -i filebeat-7.4.0-amd64.deb

- name: drop in filebeat.yml

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

- name: enable and configure system module

command: filebeat modules enable system

- name: setup filebeat

command: filebeat setup

- name: start filebeat service

command: service filebeat start

- name: enable service filebeat on boot

systemd:

name: filebeat

enabled: yes

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 access to the network.

- Load Balancers are useful in case an attacker sends multiple requests to create a Denial of Service attack since it will redirect the traffic to the second web server when the first one fails or vice versa. The jump box works as a gateway in from the public. Only the user can SSH through the Jump Box if configured correctly using an NSG.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the log files and system performance.

- Filebeat collects logs and sends them to you to get analyzed. Its used to track any suspicious log ins or attempted breaches.

- Metric beat is installed in your servers in your created environment and monitors their performance such as CPU usage for any suspicious activity

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

|----------|----------|------------|------------------|

| JumpBoxProvisioner | Gateway | 10.0.0.7 | Linux ubuntu 18.04 |

| Web-1 | VM | 10.0.0.5 | Linux ubuntu 18.04 |

| Web-2 | VM | 10.0.06 | Linux ubuntu 18.04 |

| ELK-VM | VM | 10.0.1.4 | Linux ubuntu 18.04 |

**### Access Policies**

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

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

- 99.19.236.204

Machines within the network can only be accessed by using Port 22.

- I allowed my JumpBoxProvisioner to be the gateway using my IP address to be allowed to SSH into ELK

10.0.0.7

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

| Name | Publicly Accessible | Allowed IP Addresses |

|----------|---------------------|----------------------|

| JumpBox Provisioner | No | 99.19.236.20 |

| Web 1-2 | No | 10.0.0.7 |

| ELK-VM | No | 10.0.0.7 |

### Elk Configuration

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

- Ansible is used to configure all the VMs with the same configuring scriptswithout having to do it manually in each individual one.

The playbook implements the following tasks:

- Changes the memory that is able to get used on the ELK-VM

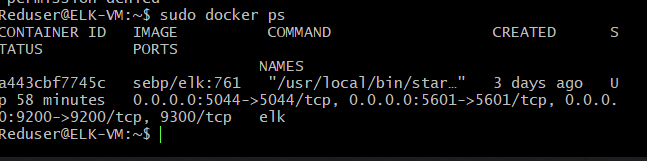
- It installs docker.io

- It installs python-pip

- It Installs docker python module

- Downloads and launches a docker ELK stack

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:

* 10.1.0.4
* 10.0.0.7
* 10.0.0.5
* 10.0.0.6

We have installed the following Beats on these machines:

- filebeat-7.4.0-amd64.deb

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

- File beats is used to log activity in your VMs to your Kibana webserver. One type of log that is sent is a audit log. It records any event in any monitored system and it documents any resources accessed and includes destination and source addresses.

**### 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 filebeat-config.yml file to the ELK-VM.

- Update the host file to include 10.1.0.4, 10.0.0.7, 10.0.0.5, 10.0.0.6

- Run the playbook, and head to the Kibana website to check that the installation worked .

- To Run Playbook: ansible-playbook filebeat-playbook.yml

- To allow Ansible to know which VMs to be configured filebeat-config.yml

- http:/20.150.140.167/:5601/app/kibana

\_ ansible-playbook filebeat-playbook.yml