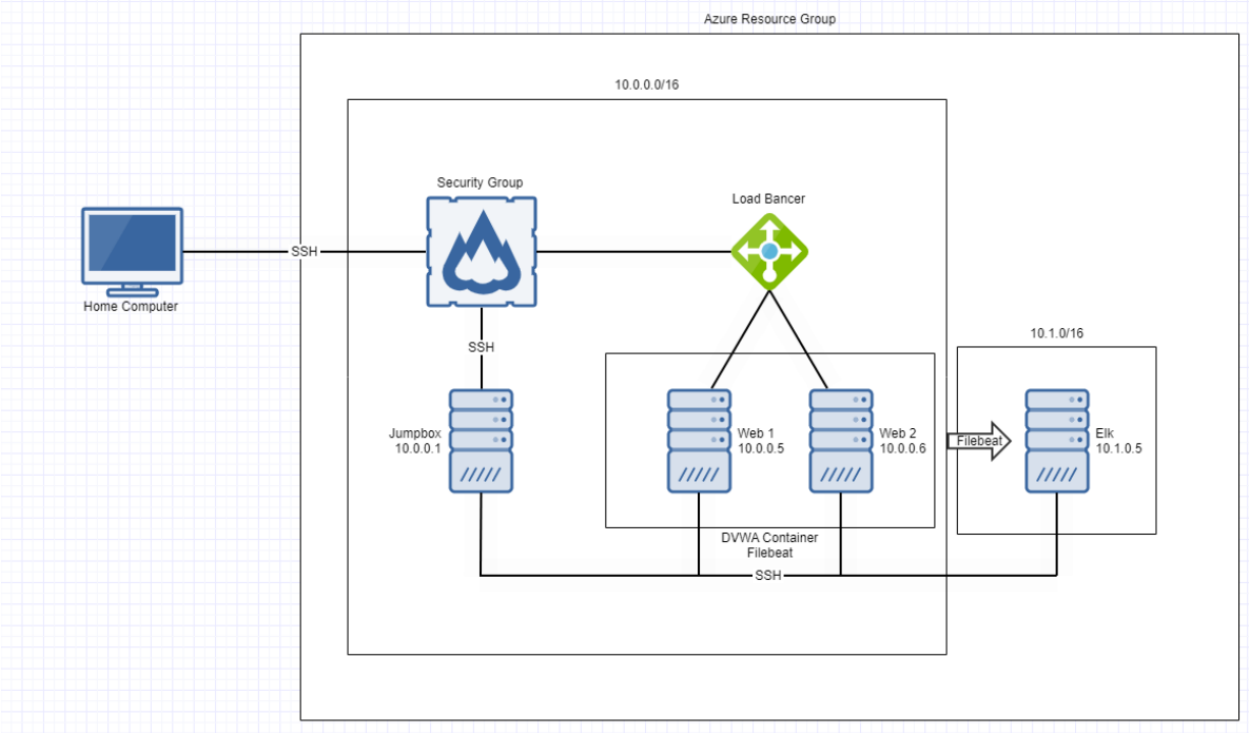
Automated ELK Stack Deployment

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



This file was tested to install a live, load-balanced instance of ELK on a container.

/etc/ansible/install-elk.yml

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 purpose of this network is to create a load balanced DVWA server that is actively monitored. Load balancers are useful because they ensure that no machine is overtaxed. They are also useful to protect against DDoS attacks. A jumpbox was used to provide security by ensuring there is only one entrance to the network. Filebeat was installed to monitor the file system and Metricbeat was installed to record system metrics such as uptime, CPU usage etc.

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.0.0.1	Linux
Web1	Host DVWA	10.0.0.5	Linux
Web2	Host DVWA	10.0.0.6	Linux
ELK	Host ELK	10.1.0.5	Linux
Docker	Container	172.17.0.3	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:
66.60.96.133

Machines within the network can only be accessed by container VMs and jumpbox.

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

Name	Function	Allowed IP Addresses
Jump Box	Yes	66.60.96.133
Docker	No	10.0.01
Web1	No	172.17.0.3
Web2	No	172.17.0.3
ELK	No	172.17.0.3

ELK Configuration

Ansible was used to automate the ELK installation. Ansible is helpful because it can be used to make deployment fast and simple. It also allows the installation to be quickly replicated on other machines.

Basic Overview of ELK installation

- Install docker.io
- Install python3-pip
- Install Docker module
- Increase virtual memory
- Download and launch an ELK container

Target Machines & Beats

This ELK server is configured to monitor the following machines:

- Web 1 and 2 10.0.0.5 and 10.0.0.6

We have installed the following Beats on these machines:

- Installed Filebeat on the docker container VM

These Beats allow us to collect Windows logs, which we use to track user logon events, etc. Filebeat monitors changes in any of the specified log files. Log files contain information about system boots, messages, logons, etc. This data is forwarded to the GUI for the ELK server.

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 configuration file to the /etc/ansible/files
- Update the configuration file to include the ip address of the ELK machine
- Run the playbook, and navigate to ELK server GUI and verify incoming data