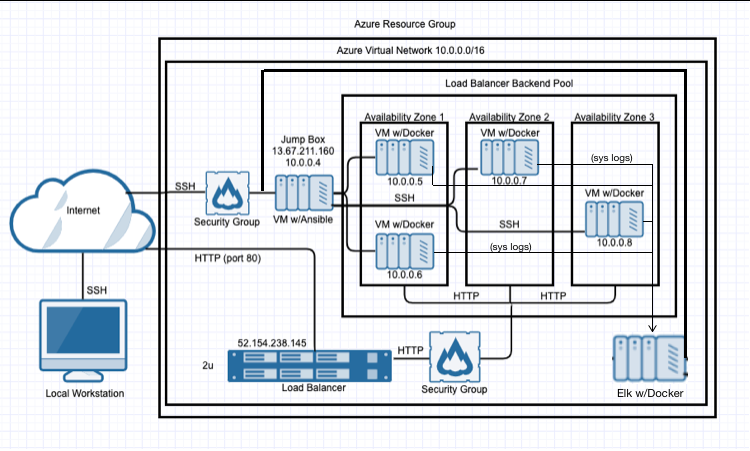
**## Automated ELK Stack Deployment**

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 **install-elk.yml** 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 *\_\_*\_\_\_, in addition to restricting \_\_\_\_\_ to the network.

- *Load balancers protect against DDoS attacks by dropping the traffic before it gets to your website. The machines with issues ar reported.*

- *The advantage of a jump box is that the VM is separated from public internet and is thus less vulnerable to attacks.*

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the *\_\_*\_\_\_ and system \_\_\_\_\_.

- *Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.*

- along with standard cpu/mem/disk/network metrics, you can also monitor Apache, Docker, etc. as well as create your own collector in the Go language.

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

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

| Jump Box | Gateway | 10.0.0.1 | Linux |

| DVWA-VM1 | VM | 10.0.0.5 | Linux |

| Elk-Server| VM | 10.0.0.6 | 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:

- *10.0.0.1, 10.0.0.5, 10.0.0.6, 10.0.0.8*

Machines within the network can only be accessed by Ansible Container.

- *Ansible Container – 10.0.0.8*

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes/No | 10.0.0.1 10.0.0.2 |

| | | |

| | | |

**### Elk Configuration**

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

- *You are able to configure a number of VMs at the same time using automation*

The playbook implements the following tasks:

- *install docker*

- *install pip*

- Install Docker python module

- Increase virtual memory

- download and launch a docker elk container

**### Target Machines & Beats**

This ELK server is configured to monitor the following machines:

- *10.0.0.1, 10.0.0.2*

We have installed the following Beats on these machines:

Winlogbeat

Logz.io

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

*Winlogbeat collects Windows logs, which we use to track user logon events, etc.*

*Logz.io*

**### 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 *\_\_*\_\_\_ file to \_\_\_\_\_.

- Update the \_\_\_\_\_ file to include...

- Run the playbook, and navigate to *\_\_*\_\_ to check that the installation worked as expected.

*\_TODO: Answer the following questions to fill in the blanks:\_*

- *filebeat-playbook.yml is copies to the ansible container*

- *You update the yml file*

- *Since Filebeat is built to collect data about specific files on remote machines, it must be installed on the VMs that you want to monitor.*