## Automated ELK Stack Deployment

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

Update the path with the name of your diagram]

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.

*elk\_playbook.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 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 functional, in addition to restricting access to the network.

Load balancers can help mitigate against DDos attacks by redirecting traffic.

A jump box provides administrators with the ability manage and deploy servers while also automating tasks that would have otherwise been time consuming.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the servers and system network

* Filebeat watches for log data.
* Metricbeat records CPU data and metrics of the operating system

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

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

| Jump Box | Gateway | 10.1.0.5 | Linux |

| Web1 | Server | 10.1.0.8 | Linux |

| Web2 | Server | 10.1.0.9 | Linux |

| Elk |ElkServer | 10.4.0.4 | 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:

Add whitelisted IP addresses:

* 40.118.151.111 (Which is the public IP of the JumpBox VM

Machines within the network can only be accessed by those specified within Network Security group

Which machine did you allow to access your ELK VM? What was its IP address?\_Jumpbox VM Public IP: 40.118.151.111 Private IP:(10.1.0.5)

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 70.48.184.183 |

| Web-1 VM | No | 10.1.0.8 |

| Web-2 VM | No | 10.1.0.9 |

| Elk-VM. | No | 10.4.0.4 |

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because automating configuration with ansible saves administrators time and effort from having to manually configure each component. This also allows for synchronized configuration across all available machines. This ultimately allows more time to be spent on other important aspects

Playbook Installation Components:

- Install docker.io

- Install python3.pip

- Install docker python module

- Launch the docker container

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

Graphical user interface, text, application

Description automatically generated

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- Web Server 1: 10.1.0.8

- Web Server 2: 10.1.0.9

We have installed the following Beats on these machines:

- FileBeat

- MetricBeat

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

- Filebeat collects information related to log files and events that keeps track of events that occur. Winlogbeat collects Windows logs, which is used to track user logon events, etc.

- Metricbeat is used to obtain metrics and statistics on the specified servers and records that information

### 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 install\_elk.yml file to ansible directory.

- Update the hosts file to include...the IP addresses of both the elk andwebservers 1 & 2

- Run the playbook and navigate to Elk machine to check that the installation worked as expected.

- Filebeat-playbook.ymlis copied to the etc/ansible directory

- The hosts file will need to be updated in order to make ansible run the playbook on a specific machine. You would also need to specify the IP of the machines you want installed by modifying the host file

- Once the previous steps have been completed, navigate to this website listed to ensure ELK server is running **http://<(ELKVMPublicIP)>:5601/app/kibana**

Commands Guide:

The following commands detailed below were used to download the playbook:

* Command to ssh into the environment: ssh azadmin@(JumpBoxPublicIP)
* Command to run playbook file: ansible-playbook (example-file.yml)
* Command to update/configure file: nano (example-file)
* Command to see list of containers available: sudo docker container list -a
* Command to attach container to Virtual Machine: sudo docker attach (container I.D.)
* Command to navigate to various directories: **cd** /etc/ansible/roles (just an illustration)
* Command to list files within specific directory: /etc/ansible **ls**