## Automated ELK Stack Deployment

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

![TODO: Update the path with the name of your diagram](Images/diagram\_filename.png)

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

- filebeat-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 available, in addition to restricting access to the network.

- Load balancers provide protection against Denial of Service attacks by distributing incoming traffic amongst multiple servers.

- The advantage of a jump box is that it forces all traffic through a single node, which makes it easier to secure and monitor virtual machines that sit behind it.\_

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the logs and system traffic.

- Filebeat monitors log files and collects log events and sends them to Elasticsearch or Logstash for indexing.

- Metricbeat monitors metrics and statistics that it collects and sends the data to Elasticsearch or Logstash.

The configuration details of each machine may be found below.

\_Note: Use the [Markdown Table Generator](http://www.tablesgenerator.com/markdown\_tables) to add/remove values from the table\_.

| Name | Function | IP Address | Operating System |

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

| Jump Box | Gateway | 40.83.177.96 10.0.0.4 | LinuxUbunto 20.04 |

| Web-1 | Web Server | 10.0.0.5 | LinuxUbunto 20.04 |

| Web-2 | Web Server | 10.0.0.6 | LinuxUbunto 20.04 |

| Web-3 | Web Server | 10.0.0.7 | LinuxUbunto 20.04 |

| Elk | Elk Server | 52.149.182.103 10.1.0.4 | LinuxUbunto 20.04 |

| Red-Team-LB | Load Balancer | 13.83.216.144 | LinuxUbunto 20.04 |

### 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:

- 73.13.116.239

Machines within the network can only be accessed by the Jump Box using SSH.

- The Jump Box has access to the ELK VM and its IP address is 10.0.0.4.

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

| Name | Publicly Accessible | AllowedIP Address |

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

| Jump Box | No | 73.13.116.239 |

| Web-1 | Yes | 13.83.216.144 |

| Web-2 | Yes | 13.83.216.144 |

| Web-3 | Yes | 13.83.216.144 |

| Elk | No | 10.0.0.4 |

### Elk Configuration

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

- \_Automated configuration is more efficient and allows for replication across multiple containers and reduces errors.

The playbook implements the following tasks:

- Install modules

- Increase virtual memory of containers

- Download and configure Elk container

- set ports

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

![TODO: Update the path with the name of your screenshot of docker ps output](Images/docker\_ps\_output.png)

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- Web-1 10.0.0.5

- Web-2 10.0.0.6

- Web-3 10.0.0.7

We have installed the following Beats on these machines:

- Filebeat was successfully installed on these machines.

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

- Filebeat monitors changes to files and their locations. These changes are logged and sent to Elasticsearch and Logstash 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 filebeat-config.yml file to etc/ansible/files.

- Update the hosts file to include the ip address of the Elk server.

- Run the playbook, and navigate to http://52.149.182.103:5601/app/kibana to check that the installation worked as expected.

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

- Which file is the playbook? Filebeat-config.yml

Where do you copy it? /etc/ansible/files/filebeat-config.yml to etc/filebeat/filebeat.yml

- Which file do you update to make Ansible run the playbook on a specific machine? **Hosts inventory file**

- How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_Add the ip address under the elk or web server section in the host file.

- \_Which URL do you navigate to in order to check that the ELK server is running? http://52.149.182.103:5601/app/kibana

\_As a \*\*Bonus\*\*, provide the specific commands the user will need to run to download the playbook, update the files, etc.\_

* ssh [azadmin@52.149.182.103](mailto:azadmin@52.149.182.103)
* sudo docker container list -all
* sudo docker start
* cd /etc/ansible
* ansible-playbook install-elk.yml to install and configure the ELK Server
* cd /etc/ansible/roles
* ansible-playbook filebeat-playbook.yml to install and configure Filebeats
* Open a browser and navigate to http:// 52.149.182.103:5601/app/kibana to interact with the Kibana website.