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

- \_TODO: Enter the playbook file.\_

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.

- \_TODO: What aspect of security do load balancers protect? What is the advantage of a jump box?

Load balancers protect availability. A jump box allows for a secure way to work on the network from a single endpoint impoving security.

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

- \_TODO: What does Filebeat watch for?Logs and File changes

- \_TODO: What does Metricbeat record?System Metrics

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 | Entry point | 10.0.0.5 | Linux |

| Web 1 |Web Server| 10.0.0.6 | Linux |

| Web 2 |Web Server| 10.0.0.7 | Linux |

| Elk |Elk Server|20.109.182.136| Linux |

### Access Policies

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

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

- \_TODO: Add whitelisted IP addresses Home Ip-71.33.134.71

Machines within the network can only be accessed by SSH with key.

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address? Ansible Container on JumpBox 127.17.0.2

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

|  |  |  |
| --- | --- | --- |
| Name | Publicly Accessible | Allowed IP |
| Jump Box | Yes | 71.33.134.71 |
| Web 1 | No |  |
| Web 2 | No |  |
| Web 3 | No |  |
| Load Balancer | Yes | 71.33.134.71 |
| Elk | Yes | 71.33.134.71 |

### Elk Configuration

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

- \_TODO: What is the main advantage of automating configuration with Ansible? automated configuration is going to be consistent across all machines and can be scaled up to do many machines in a short time.

The playbook implements the following tasks:

- \_TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.

Install Docker

Pull ansible container

Update ansible config file

Update hosts file

Write and execute your play with metric/file beats install package

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)

Graphical user interface, text

Description automatically generated

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- \_TODO: List the IP addresses of the machines you are monitoring

10.0.0.6, 10.0.0.7, 10.0.0.10

We have installed the following Beats on these machines:

- \_TODO: Specify which Beats you successfully installed

Metricbeats and Filebeats

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

- \_TODO: In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.\_

Filebeat collects log data related to file changes and log ons

Metricbeat collects system log data related to the machines syustem performance

### 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 playbook file to /etc/ansible/hosts.

- Update thehosts file to include groups (webservers) and (elk) with corresponding Ips so that when you run the play it targets the correct machines.

- Run the playbook, and navigate to kibana to check that the installation worked as expected.

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

- \_Which file is the playbook? Where do you copy it?\_

- \_Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

- \_Which URL do you navigate to in order to check that the ELK server is running?

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