## Automated ELK Stack Deployment

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

!(Azure\_ELK\_VNET)

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 filebeat-playbook.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 secure, in addition to restricting DDoS attacks to the network.

-

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

-

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 | 10.0.0.4 | Linux |

| Elk-VM | Elkstack | 10.1.0.5 | Linux |

| Web1-VM | DVWA | 10.0.0.7 | Linux |

| Web2-VM | DVWA | 10.0.0.6 | Linux |

### Access Policies

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

Only the Jumpbox-Provisioner machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- 174.216.2.176 174.215.64.13 (My public IPs)

Machines within the network can only be accessed by the Jumpbox (104.42.107.83).

-

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 174.216.2.176 174.215.64.13 |

| Web1 | No | 104.42.107.83 |

| Web2 | No | 104.42.107.83 |

### Elk Configuration

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

Ansible is free and open source. It is also simple yet powerful by pushing IaC (Infrastructure as code).

The playbook implements the following tasks:

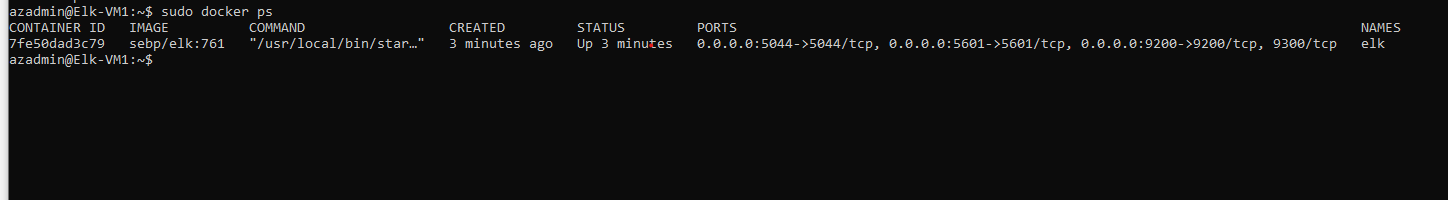
- First the playbook installs docker.io and python3-pip using the apt module.

- Then using the previously downloaded pip module (pip3), It installs the Docker module.

- Increases virtual memory and utilizes that memory through sysctl.

- Downloads the ELK Container and enables it on re-boot.

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

](docker\_ps\_screenshot)

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

Web1-VM: 10.0.0.7

Web2-VM: 10.0.0.8

-

We have installed the following Beats on these machines: Filebeat and Metricbeat

-

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

Filebeat tracks files/logs and will keep the record of last lines sent and will continue reading the files as soon as the output becomes available again.

Metricbeat tracks system performance and monitors external services running on them. (CPU, RAM, etc).

### 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-(filebeat/metricbeat).yml file to the "roles" directory.

- Update the hosts file to include the IP of your ELK server

- Run the playbook, and navigate to http://(public IP of your ELK-VM):5601/app/kibana to check that the installation worked as expected.

\_\*\*\_\*\*

- Once you have the playbook downloaded, you can run the playbook with the <ansible-playbook install-filebeat.yml> command. You must be in your ansible container to do so.

- To update files, you can run <sudo apt update>