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

- \_TODO: elk-playbook.yml\_

This document contains the following details:

- Description of the Topologu

- 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 \_effective\_\_\_\_, 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?\_

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

- \_TODO: What does Filebeat watch for?- It watches for log files and events as well

- \_TODO: What does Metricbeat record?- it records the metrics from all on going files

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 | 10.0.0.9 | Linux |

| WEB-1 | W-Server | 10.0.0.15 | Linux |

| WEB-2 | W-Server | 10.0.0.16 | Linux |

| elk-1 | W-Server | 10.1.0.4 | Linux |

### Access Policies

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

Only the \_\_\_Virtual machine/jumpbox provisioner\_\_ machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- \_TODO: Add whitelisted IP addresses\_ 10.0.0.9

Machines within the network can only be accessed by \_\_\_jumpbox\_\_.

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address?- 137.135.30.15

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 10.0.0.9 |

| WEB-1 | No | 40.118.186.181 |

| WEB-2 | No | 40.118.186.181 |

| elk-1 | Yes/Http

### 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?-It has flex because it allows changes to be made within any of the Virtual machines linked with it

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.\_

- run Docker start and then attech to the container

- once the container is generated you can then navigate to cd etc/ansible

- once there you will see the ansible playbooks that you can run

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:

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

We have installed the following Beats on these machines:

- \_TODO: Specify which Beats you successfully installed filebeat,

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 monitors the logs locations that you have configured. they can be used to check on system issues, files 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 \_\_playbook file\_\_\_ file to \_\_etc/ansible\_\_\_.

- Update the \_etc/ansible/host\_\_\_\_ file to include...

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

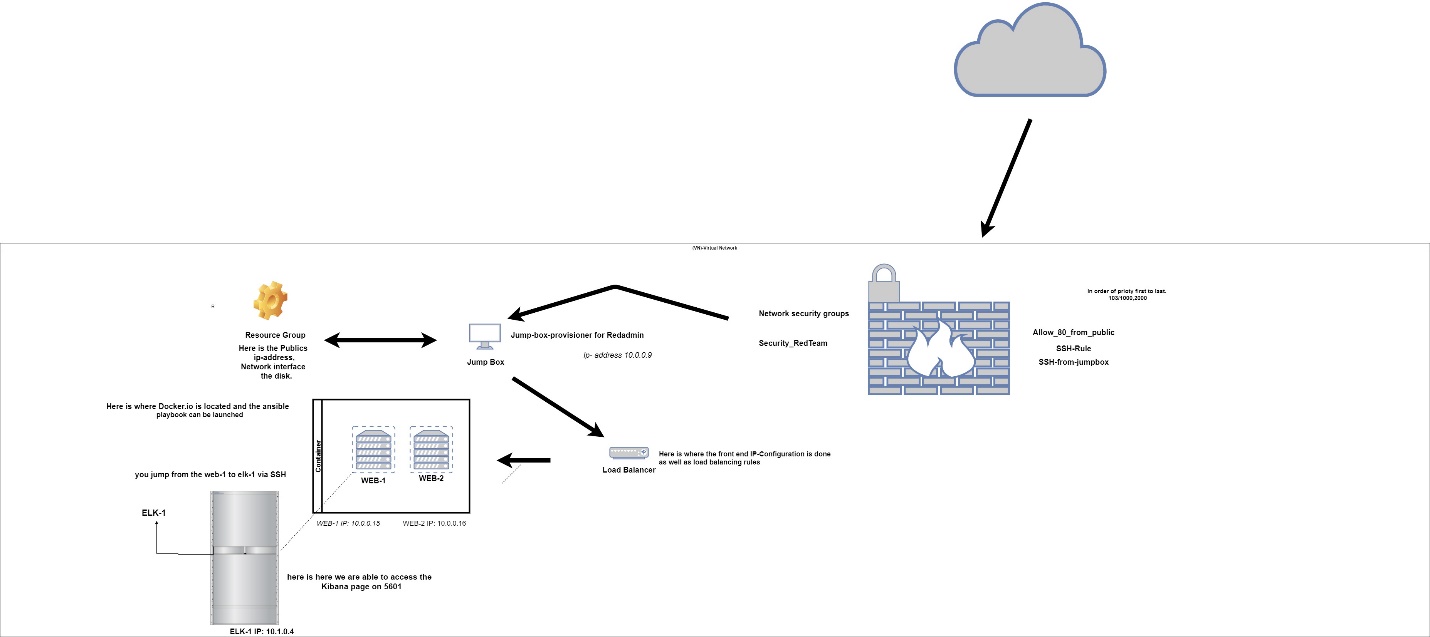
\_TODO: Answer the following questions to fill in the blanks:\_

- \_Which file is the playbook? Where do you copy it?- you copy it in etc/ansible and

- \_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? - http://[your.VM.IP]:5601/app/kibana

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



* Governance, Risk, and Compliance
* Linux and Windows Hardening and Administration
* Archiving and Logging
* Bash Scripting and PowerShell
* Network Security
* Website Security
* Cryptography
* Penetration Testing using Kali Linux
* SIEM Implementation, Alerting, and Reporting
* Forensics
* Red Team vs Blue Team Engagements
* Bug Bounties
* Docker
* Cloud security
* built an elk stack
* splunk
* Kibana
* Wireshark
* Security onion