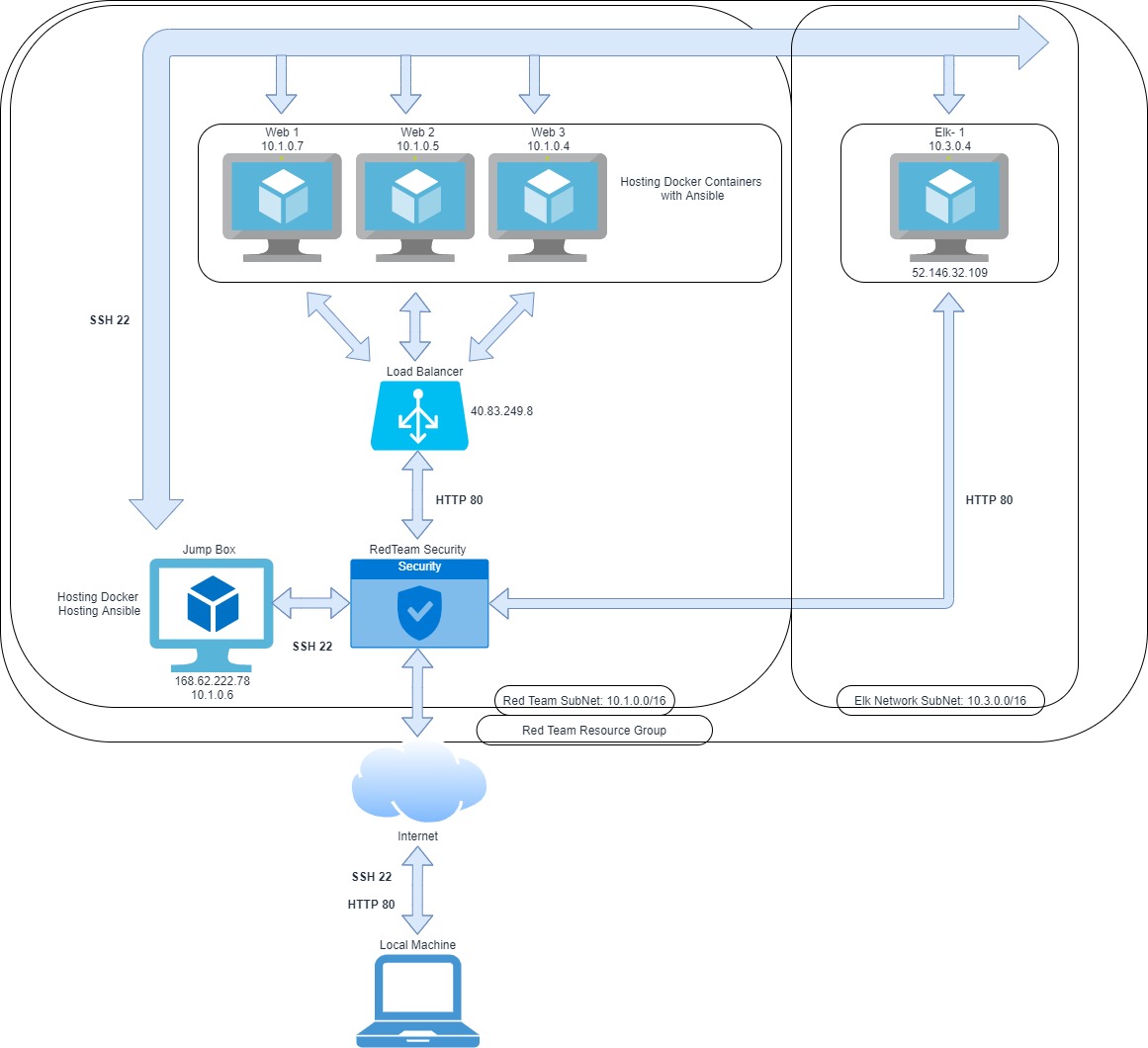
## Automated ELK Stack Deployment

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



(Images/ELK Diagram.PDF)

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

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 to authorized access, in addition to restricting unauthorized access to the network.

What aspect of security do load balancers protect?

* Load balancers protect from incoming traffic and malicious activity by spreading it across servers.

What is the advantage of a jump box?

* Jumpbox allows users to change or access multiple machines from one central hub.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the Event Logs and files and system Metrics.

- File beats watches for log files

-Metricbeat watches system metrics

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

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

| Jump Box |Gateway | 10.1.0.6 | Linux |

| Web 1 |Server | 10.1.0.7 | Linux |

| Web 2 |Server | 10.1.0.5 | Linux |

| web 3 |Server | 10.1.0.4 | Linux |

| Elk 1 |Loging | 10.3.0.4 | Linux |

### Access Policies

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

Only the Jumpbox and Elk-1 machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

Local 64.252.58.123

Machines within the network can only be accessed by SSH from Jumpbox.

ELK-1 can use Port 5601

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 64.252.58.123 |

| Web 1 | No | 10.1.0.6 |

| Web 2 | No | 10.1.0.6 |

| Web 3 | No | 10.1.0.6 |

| Elk 1 | No | 10.1.0.6 |

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because The administrator can configure multiple devices at once and all configurations are identical. If there are errors they only need to be fixed at the original location.

The playbook implements the following tasks:

Configure Elk VM with Docker

1.Install docker.io

2. Install python3-pip

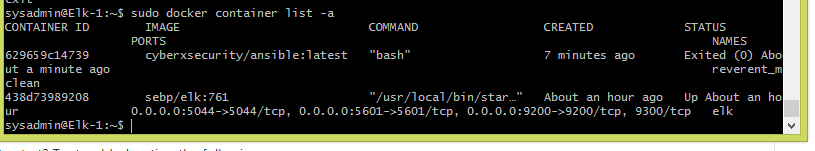
3. Install Docker module

4. Increase virtual memory to 262144and use more memory

5. Download and launch a docker elk container sebp/elk:761

6. Enable service docker on boot

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



### Target Machines & Beats

This ELK server is configured to monitor the following machines:

Jump Box 10.1.0.6

Web-1 10.1.0.7

Web-2 10.1.0.5

Web-3 10.1.0.4

We have installed the following Beats on these machines:

Filebeat

Metricbeats

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

-Filebeats collects and monitors log files, locations and events.

-Metricbeats collects and monitors data from operating systems and services. Provides specific information on metric data and statistics.

### 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 file to Elk-1.

- Update the Hosts file to include Ip addresses for the VM that are monitored

Jump Box 10.1.0.6

Web-1 10.1.0.7

Web-2 10.1.0.5

Web-3 10.1.0.4

- Run the playbook, and navigate to

[http://[104.41.137.229:5601/app/kibana](about:blank). to check that the installation worked as expected.

/etc/ansible/roles# nano Filebeat-Playbook.yml

---

- name: filebeat installer

hosts: webservers

become: true

tasks:

- name: download filebeat

shell: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/$

- name: install filebeat

shell: dpkg -i filebeat-7.6.1-amd64.deb

- name: Copy filebeat configuration

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

owner: root

group: root

mode: '0600'

backup: yes

- name: restart filebeat

shell: filebeat modules enable system

- name: filebeat setup

shell: filebeat setup

- name: filebeat -e

shell: filebeat -e &

- name: Start filebeat service

command: service filebeat start

Change the filebeat or metricbeat configuration file to send data to the Elk server’s Ip address. The elk server is the machine the logs are being sent to and the filebeat are the machines that are being logged.

[http://[your.VM.IP]:5601/app/kibana](about:blank). Will show if the server is running and logging files