**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.

- filebeat-playbook.yml, metricbeat-playbook.yml

- name: Installing and launching filebeat

hosts: elk

become: yes

tasks:

**# Use command module**

- name: Download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

**# Use command module**

- name: Install filebeat deb

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

**# Use copy module**

- name: Drop in filebeat.yml

copy:

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

dest: /etc/filebeat/filebeat.yml

**# Use command module**

- name: Enable and configure system module

command: filebeat modules enable logstash

**# Use command module**

- name: Setup filebeat

command: filebeat setup

**# Use command module**

- name: Start filebeat service

command: sudo service filebeat startThis 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

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 available, in addition to restricting traffic to the network.

- What aspect of security do load balancers protect? Availability What is the advantage of a jump box? They allow multiple operating systems environments to exsist simultaneously on the same machine.

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

- What does Filebeat watch for? Filebeat is a lightweight shipper for forwarding and centralizing log data.Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events,and forwards them either to Elasticsearch or Logstash for indexing

- What does Metricbeat record? Metricbeat is a lightweight shipper that you can install on your servers to periodicallycollect metrics from the operating system and from services running on the server. Metricbeat takes the metrics andstatistics that it collects and ships them to the output that you specify, such as 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 | 10.0.0.4 | Linux |

| Web1 | Ubuntu | 10.1.0.5 | Linux |

| Web2 | Ubuntu | 10.1.0.6 | Linux |

| ElkVM | Gateway | 10.2.0.4 | Linux |

**### Access Policies**

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

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

- 52.183.5.158

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

- Jump Box, the IP address was 10.0.0.4

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 52.183.5.158 |

| Web 1 | No | 10.1.0.5 |

| Web 2 | 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 advantage to using ansible playbooks is that you can send commands to mutiple servers/jumpboxes at once

The playbook implements the following tasks:

- Install Docker

Run Docker and download file ex.(angry\_moser)

SSH into Elk

create docker and start docker container

Configure ansible files and the create a playbook

run playbook

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

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

d79b9b3faafa sebp/elk:761 "/usr/local/bin/star…" 3 days ago Up Less than a second 0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp elk

**### Target Machines & Beats**

This ELK server is configured to monitor the following machines:

- Elk 10.2.0.4

Web-1 10.1.0.5

Web-2 10.1.0.6

We have installed the following Beats on these machines:

File Beats

Metric Beats

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

- \_Filebeats monitors the log files or location that I specify, and metricbeats takes the metrics and statistics that it collects. Both go to Elasticsearch or Logstash. Winlogbeat collects windows log that can be tracked and recorded.

**### 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 curl file to playbook.

- Update the config file to include...

- 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:\_*

- root@062eccb1c80d://etc/ansible/roles# ls

filebeat-playbook.yml metricbeat-playbook.yml

- \_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?\_\_update IP address on host file

- \_Which URL do you navigate to in order to check that the ELK server is running?http://157.55.80.118:5601/app/kibana#/home

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