## Automated ELK Stack Deployment

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

C:\Users\drock\Pictures\Project 1 Diagram.drawio.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 \_playbook\_\_\_\_ file may be used to install only certain pieces of it, such as Filebeat.

- \_TODO: Enter the playbook file.\_

/etc/ansible/roles/filebeat-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 \_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?\_

The aspect of security that load balancers protect is availability. The advantage of using a jump box is that there is much less risk, because it is a secure computer that can be used as a point of origin for other servers or environments.

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

- \_TODO: What does Filebeat watch for?\_ Filebeat monitors the log files that you specify and collets log events, it then forwards it to Elasticsearch or logstash.

- \_TODO: What does Metricbeat record?\_ Metricbeat helps you monitor your servers by collecting different metrics from your system and what is running on the server.

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 |

| Web 1 | DVWA | 10.0.0.5 | Linux |

| Web 2 | DVWA | 10.0.0.6 | Linux |

| Web 3 | DVWA | 10.0.0.8 | Linux |

| Elk |ELK Container| 10.1.0.4| Linux

### Access Policies

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

Only the \_Jump Box\_\_\_\_ machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- \_TODO: Add whitelisted IP addresses\_

73.127.30.244

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

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address?\_ I used the Jump box the IP address is 20.189.162.105.

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | No | my personal IP |

| Web 1 | No | 20.189.162.105 |

| Web 2 | No | 20.189.162.105 |

| Web 3 | No | 20.189.162.105 |

| Elk | Yes | 20.189.162.105 |

### 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?\_ The main advantage of automating the configuration with ansible is that it helps IAC or Infrastructure as Code.

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.\_

- First you install dockder.io using the apt module. When putting in the task make sure you “update\_cache” name “docker.io” and write the “state” as present. While still using the apt module you will also install pip3. For this you will need to “force\_apt\_get” name “python3-pip” and once again state as “present.”

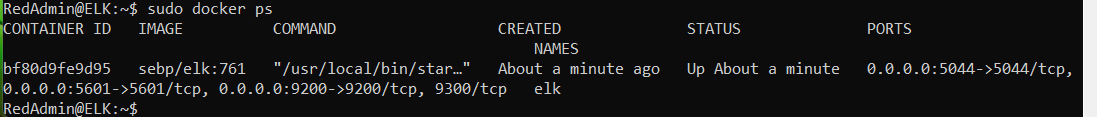
- For the next section you will be using the pip module. We will be installing docker python module in this step. You will need the Name “docker” and the state as “present.”

-For the next step you will be using the sysctl module. In this step we will be seting up the machine to use more memory. In the Name section you will put “vm.max\_map\_count” then in the value section “262144” then state “present”. Then the last part of this task is reload “yes.”

-In this section you download and launch a docker elk container. This will be done in the docker\_container module. In this step you will download the sebp/elk:761 image. You will also put in the published\_ports in this step the ports are 5601, 9200, 5044.

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\_

The IP addresses for the machines I am monitoring are 10.0.0.5, 10.0.0.6, 10.0.0.8.

We have installed the following Beats on these machines:

- \_TODO: Specify which Beats you successfully installed\_

I was successfully able to install filebeat as well as metricbeat.

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.\_

Filebeats collects and files log events. It then forwards them to Elasticsearch for indexing.

Metricbeats collects different metrics on the machines that are running. It shows different graphs and charts to show activity on the network.

### 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 \_all\_playbook\_\_\_ file to \_/etc/ansible/roles\_\_\_\_.

- Update the \_\_filebeatconfig\_and metricbeat config\_\_ file to include the correct IP addresses for the ELK VM.

- Run the playbook, and navigate to kibana and navigate to add log data, and then to system logs and click DEB once finished scroll to the bottom of the page and click check data. You can then navigate to verify incoming data by clicking the link 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?

The URL that you navigate to in order to check that the ELK server is running is http://20.124.15.177:5601/app/kibana.

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

The command you will need to run the playbook is

Ansible-playbook [name of playbook]

The command to download the config files

Curl https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/filebeat-config.yml

The Command to get into the config files to up date them is.

Nano /etc/ansible/files/filebeat-config.yml

Nano /etc/ansible/files/metricbeat-config.yml