Elk-Stack-server

Martha Sarfo Gyimah

## 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)

Project 1-Elk-Stack-Server\images\ELK-Stack-Server.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: Enter the playbook file.\_

Ansible-playbook elk-playbook.yml

Ansible-playbook filebeat-playbook.yml

Ansible-playbook metricbeat-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 \_\_\_\_\_, in addition to restricting \_\_\_\_\_ to the network.

- \_TODO: What aspect of security do load balancers protect? What is the advantage of a jump box?\_

* Load balancer offers defends for organization against distributed denial-of-service (DDoS) attacks. It shifts the attack traffic from organization’s server to a public cloud provider.
* Jump box bridges two different security zones and offers controlled access between them

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

- \_TODO: What does Filebeat watch for?\_

* Filebeat watches the log files or the specified locations, collects events and forward them to either Elasticsearch or Logstash for indexing

- \_TODO: What does Metricbeat record?\_

* Metricbeat collects data of metrics and statistics and forward them to the output specified 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 | 10.0.0.1 | Linux |

| Golden Jump Box | 52.137.79.40 | 10.0.0.4 | Linux Ubuntu 18.04

| Web1 | | 10.0.0.5 | Linux Ubuntu 18.04

| Web2 | | 10.0.0.6 | Linux Ubuntu 18.04

| Flagship | 13.84.39.51 | 10.1.0.4 | Linux Ubuntu 18.04

### Access Policies

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

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

- \_TODO: Add whitelisted IP addresses\_

-5601:5601

-9200:9200

-5044:5044

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

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

-Flagship-VM IP: 13.84.39.51

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes/No | 10.0.0.1 10.0.0.2 |

| Golden Jump Box| Yes | 10.0.0.4 73.153.161.4|

| Flagship | yes | 73.153.161.4 |

### 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 is simple to use and it saves time.

The playbook implements the following tasks:

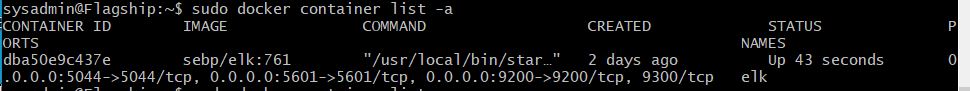
- \_TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.\_

* Configure Elk VM with docker: This has the name, the hosts and remote user
* Install docker.io: This installs the docker
* Install python3-pip:This is the script interpreter
* Install docker module
* Download and launch a docker elk container

- ...

- ...

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\_

-Web1: 10.0.0.5

-Web2: 10.0.0.6

We have installed the following Beats on these machines:

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

-Filebeat

-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.\_.

-Filebeat: Syslog sends event data logs to a central location for storage

-Metricbeat: Redisbeat exports general 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 \_\_\_\_\_ file to \_\_\_\_\_.

- Update the \_\_\_\_\_ 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?

Playbooks are files where ansible codes are written.

-Playbook\_example.yml

Copy from:

- /etc/ansibe# ansible-playbook elk-playbook.yml

-/etc/ansible# ansible-playbook filebeat-playbook.yml

-/etc/ansible# ansible-playbook 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?\_

-elk-playbook.yml

- /etc/ansibe# ansible-playbook elk-playbook.yml

-/etc/ansible# ansible-playbook filebeat-playbook.yml

- \_Which URL do you navigate to in order to check that the ELK server is running?

-http:// [your.VM.IP] : 5601 <http://13.137.79.40:5601>

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

-sudo apt-get update

-sudo apt-get upgrade -y