## 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)

* Elk- stack server

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 Balancing plays an important security role as computing moves evermore to the cloud. The off-loading function of a load balancer defends an organization against distributed denial-of-service (DDoS) attacks.
* It does this by shifting attack traffic from the corporate load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent users) and reliability of applicationsserver to a public cloud provider.
* jumpbox is a (special-purpose) computer on a network typically used to access devices in a separate security zone. ... This could be accessing your home network from remote location. Access internet from your mobile device in public locations via VPN and so on.

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 monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexin.

- \_TODO: What does Metricbeat record?\_

* Metricbeat takes the metrics and statistics 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 | 10.0.0.1 | Linux |

Jump-box provisioner|20.190.44.30 |10.0.0.4|Linux Ubuntu 18.04|

| Wab-1 | | 10.0.0.6 | Linux Ubutun 18.04

| Web-2 | | 10.0.0.7 | Linux Ubuntu 18.04

Pangie -VM | | 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?\_

* Pangie-VM :13.66.18.34

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 |

| Jump-Box provisioner | Yes |10.0.0.4,20.190.44.30|

|Pangie-VM| Yes |, 13.66.18.34|

### 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?\_

* Ansible uses a simple syntax written in YAML called playbooks.
* help deliver more value to the business by spending time on more important tasks.

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.\_

* Elk docker configure
* Install dockr.io
* Install python3-pip
* Install docker module
* Icrease virtual memory

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\_

* Wab-1 :10.0.0.6
* Wab-2 :10.0.0.7

We have installed the following Beats on these machines:

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

* Metricbeat
* 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.\_

* Metricbeat: Redisbeat is used as a redis monitoring.
* Filebeat: syslog is used to collect various device logs from several different machines in a centrai location for monitoring and review.

### 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 thou copy e following questions to fill in the blanks:\_

-Which file is the playbook? : Playbooks are the files where Ansible code is written

. Where do copy it?

* etc/ansible/# ansible-playbook filebeat-playbook.yml
* etc/ansible/# ansible-playbook metricbeat-playbook.yml
* etc/ansible/# ansible-playbook elk-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/ansible# ansible-playbook elk
* etc/ansible/# ansible-playbook filebeat-playbook.yml
* etc/ansible/# ansible-playbook metricbeat-playbook.yml

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

* http:// [your.VM.IP] :5601 HTTP:// 13.66.18.34:5601

\_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"