## Automated ELK Stack Deployment

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

- \_TODO: Images/Diagram2\_final.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 filebeat-playbook.yml file may be used to install only certain pieces of it, such as Filebeat.

- \_TODO: elk.yml

This document contains the following details:

- Description of the Topology

Provisioner (Jump-Box) has Ansible, there are YAML config files for 3 VM web servers and ELK server

- Access Policies

Jump-Box has SSH access from outside, WEB server are set into availability set and are behind load balancer with HTTP (port 80). Elk server has access from outside from specific sources only

- ELK Configuration

- Beats in Use: filebeat and mericbeat

- Machines Being Monitored: WEB VMs 1, 2 and 3

- How to Use the Ansible Build: There are 2 directories under etc/ansible. Directory “roles” contains playbooks elk.yml filebeat-playbook.yml, metricbeat-playbook.yml. First run elk.yml to run/configure prerequisites on elk server. Under “files” directory are the config files with modified IP addresses for elk server config files for filebeat and metricbeat. Next step is to run files under “roles” directory: filebeat-playbook.yml, metricbeat-playbook.yml

### Description of the Topology

There are 2 network security groups. One group has 10.0.0.0/16 subnet, another 10.1.0.0/16. These groups are peered, so traffic is allowed between the hosts. Each group has its own network security group.

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?\_

Load balancers are the front end and do not expose the actual servers, plus they distribute the traffic between the back end server to make sure the service is available.

Jump box is the only machine that can access the rest of the network nodes ( asymmetric ssh key access ). Plus there is access control to a jump box too: IP source and ssh keys.

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

- \_TODO: What does Filebeat watch for?\_ changes in log files

- \_TODO: What does Metricbeat record? Monitors CPU, memory, network, disk, plus apps like apache, docker , etc. In other words data from operating system and services.

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 |

| WEB-1 | DWVA | 10.0.0.10 | Linux |

| WEB-2 |DWVA | 10.0.0.11 | Linux |

| WEB-3 | DWVA |10.0.0.13 | Linux |

### Access Policies

Jump-Box has ssh access to WEB servers. Load Balancer provides distributed/even access to the resources on web servers over HTTP.

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

Only the Jump-Box and ELK machines can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses: 76.102.188.228,174.194.192.151,70.35.42.0/24

- \_TODO: 76.102.188.228,174.194.192.151,70.35.42.0/24

Machines within the network can only be accessed by Jump-Box(Provisioner).

- \_TODO: Which machine did you allow to access your ELK VM? What was its IP address? 76.102.188.228,174.194.192.151,70.35.42.0/24

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 | 76.102.188.228,174.194.192.151,70.35.42.0/24 |

|ELK-server| YES | 76.102.188.228,174.194.192.151,70.35.42.0/24|

| | | |

### 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?\_

ELK server can be replaced/configure/built with minimum down time

The playbook implements the following tasks( the beaty of it – minimum downtime) :

- Increases/allocates memory for necessary services to perform

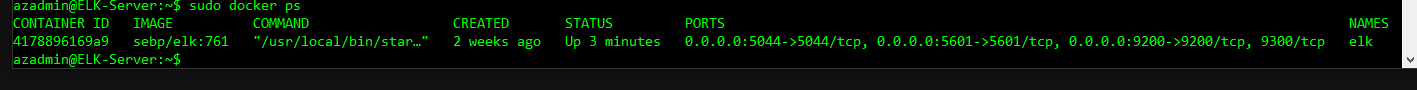
- installs docker app

- installs python

- downloads elk container

- allocates/presets access ports

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\_

10.0.0.10

10.0.0.11

10.0.0.13

We have installed the following Beats on these machines:

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

Filebeat and 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 is a logging agent that collect the log data and forwards to Elastic or Logstash for indexing.

Metricbeat collects data about the host system like CPU, memory disk usage even the application/services usage of the system resources and sends data to Elastic/Logstash for indexing and monitoring.

### 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 and metricbeat-config.yml files to /etc/ansible/files.

- Update the filebea-config.yml and metric-config.yml files to include ip address 10.1.0.4 of ELK server

- Run the playbook, and navigate to http://10.1.0.4:5601 to check that the installation worked as expected.

\_TODO: Answer the following questions to fill in the blanks:\_

- \_Which file is the playbook? \*-playbook.yml Where do you copy it?\_ /etc/ansible/roles

- \_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?\_/etc/ansible/hosts file

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

<http://10.1.0.4:5601>

<http://40.75.5.137:5601> ( access allowed to specific sources )

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