## **Automated ELK Stack Deployment**

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

**Note**: The following image link needs to be updated. Replace diagram\_filename.png with the name of your diagram image file.

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.*
* filebeat.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 \_monitored\_\_\_\_, 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?*

1. Load balancers protect network security

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*  collects data about the file system

* *TODO: What does Metricbeat record?*

Collects machine metric

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 |
| DVWA-VM1 | Azure vm | 10.1.0.5 | linux |
| DVWA-VM2 | Azure vm | 10.1.0.6 | linux |
| ELK-SERVER | Azure vm | 10.2.0.7 | linux |

### **Access Policies**

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

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

* *TODO: Add whitelisted IP addresses*

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

* *TODO: Which machine did you allow to access your ELK VM? What was its IP address?*

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

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box    DVWAV1  DVMAV2 | YES  NO  NO | 51.143.1.111  10.1.0.5  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...

* *TODO: What is the main advantage of automating configuration with Ansible?*
* It allows setup very quickly using ssh

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.*
* ...
* ...

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

**Note**: The following image link needs to be updated. Replace docker\_ps\_output.png with the name of your screenshot image file.

### **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* *TODO: List the IP addresses of the machines you are monitoring*
* 10.1.0.5
* 10.1.0.6

We have installed the following Beats on these machines:

* *TODO: Specify which Beats you successfully installed*

Filebeat

Metric beat

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 will be monitoring virtual machines stats
* Filebeat will be used to gather primarily log files from webservers, apache, azure

**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 \_\_\_yml\_\_ file to \_\_jumbox\_\_\_.
* Update the \_\_\_\_hosts\_ file to include. Ip of your vm..
* Run the playbook, and navigate to \_vm\_\_\_ 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?*

*ELK install .yml , in the ansible*

* *Which file do you update to make Ansible run the playbook on a specific machine?*

*Hosts file*

* *How do I specify which machine to install the ELK server on versus which to install Filebeat on?*

By putting the IP of the ELK VM IN THE HOST FILE AND FILEBEAT CONFIG*.*

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

The IP of the ELK : 5601

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