**Automated ELK Stack Deployment**

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

Diagram, schematic

Description automatically generated

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.

Install-elk.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.

* Load balancers distribute network traffic across several servers. Load balancers are used to prevent overloading servers and protect against attacks like DoS. Jump box gives access to the user from a single node and the advantage of that is that it is secured and monitored.

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

* What does Filebeat watch for? Log files
* What does Metricbeat record? Performance Metrics

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 | Web server | 10.0.0.5 | Linux |
| Web-2 | Web server | 10.0.0.8 | Linux |
| Web-3 | Web server | 10.0.0.10 | Linux |
| ELK-Project-VM | Monitoring | 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:

* My IPv4

Machines within the network can only be accessed by port 22.

* Jump Box has access to the ELK VM. Private IP address 10.0.0.4 A summary of the access policies in place can be found in the table below.

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes | My IPv4 |
| Web-1 | No | 10.0.0.4 |
| Web-2 | No | 10.0.0.4 |
| Web-3 | No | 10.0.0.4 |
| ELK-Project-VM | Yes | My IPv4 (port 5601),10.0.0.4(P22) |

**Elk Configuration**

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because

* Automating configuration with Ansible saves a lot of time TO DO

The playbook implements the following tasks:

* Install python3-pip
* Install Docker python module
* Install docker.IO
* Install docker elk container
* Set the vm.max\_map\_count to 262144

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

[Text

Description automatically generated](https://github.com/WassimDjida/Project-1/blob/main/diagrams/DockerPS.PNG)

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* Web-1 10.0.0.5
* Web-2 10.0.0.8
* Web-3 10.0.0.10

We have installed the following Beats on these machines:

* Filebeat
* Metricbeat These Beats allow us to collect the following information from each machine:
* Filebeats is used to monitor log events and send server log files to kibana.
* Metricbeat collect metric data from your target servers and it can also be used to monitor other beats and ELK stack itself.

**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-playbook.yml file to /etc/ansible/roles.
* Update the /etc/ansible/hosts file to include

[webservers]

* 10.0.0.5 ansible\_python\_interpreter=/usr/bin/python3
* 10.0.0.8 ansible\_python\_interpreter=/usr/bin/python3
* 10.0.0.10 ansible\_python\_interpreter=/usr/bin/python3

[elk]

* 10.1.0.4 ansible\_python\_interpreter=/usr/bin/python3
* Run the playbook, and navigate to <http://40.79.18.114/app/kibana#/home> to check that the installation worked as expected.

**Answer the following questions to fill in the blanks:**

* Which file is the playbook? Install-elk.yml’ Where do you copy it?\_/etc/ansible
* Which file do you update to make Ansible run the playbook on a specific machine? /etc/ansible/hosts
* How do I specify which machine to install the ELK server on versus which to install Filebeat on? In the hosts file with the heading [webservers] & [ek]
* Which URL do you navigate to in order to check that the ELK server is running? <http://40.79.18.114/app/kibana#/home>

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

* Ansible-playbook /etc/ansible install-elk.yml