**Automated ELK Stack Deployment**

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

A close up of a map

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.

ansible-playbook docker\_elk.yml

- name: Install / Configure Docker Repository

hosts: elkservers

become: true

tasks:

- name: Make sure the Docker repo key is installed

apt\_key:

id: 9DC858229FC7DD38854AE2D88D81803C0EBFCD88

url: https://download.docker.com/linux/ubuntu/gpg

state: present

- name: Make sure Docker repo is installed

apt\_repository:

repo: deb [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable

state: present

- name: docker-ce

apt:

update\_cache: yes

name: docker-ce

state: present

- name: docker-ce-cli

apt:

update\_cache: yes

name: docker-ce-cli

state: present

- name: containerd.io

apt:

update\_cache: yes

name: containerd.io

state: present*.*

ansible-playbook install-elk.yml

- name: Configure Elk VM with Docker

hosts: elkservers

remote\_user: jzinn

become: true

tasks:

# Use apt module

- name: Install pip3

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module

- name: Install Docker python module

pip:

name: docker

state: present

# Use command module

- name: Increase virtual memory

command: sysctl -w vm.max\_map\_count=262144

# Use shell module

- name: Increase virtual memory on restart

shell: echo "vm.max\_map\_count=262144" >> /etc/sysctl.conf

# Use docker\_container module

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

This document contains the following details:

* Description of the Topology
* 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 responsive, 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?*
* *Answer: Load balancers off-loading function defends an organization from DDoS (distributed denial-of-service) attacks by shifting attack traffic from the corporate server to a public cloud provider. The advantage of a jump box is that it protects against attacks and to not expose internal resources (Web 1 and 2) to the internet.*

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

* *TODO: What does Filebeat watch for?*
* *Answer: Filebeat monitors log files that you specify, collects log events, and forwards them either to Elasticsearch or logstash for indexing.*
* *TODO: What does Metricbeat record?*
* *Answer: Metricbeat records metrics and statistics from the system and services running on the server.*

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 | | 52.191.128.174 | Linux |
| Web 1 | | Web Server | | 10.0.0.8 | Linux |
| Web 2 | | Web Server | | 10.0.0.7 | Linux |
| Elk-VM | | Elastic Stack | | 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:

* Home IP address which is dynamic: 73.14.227.51

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

* *Jump Box Provisioner 52.191.128.174*

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

| **Name** | **Publicly Accessible** | | **Allowed IP Addresses** | |
| --- | --- | --- | --- | --- |
| Jump Box | No | | 52.191.128.174 | |
| Web 1 | No | | 10.0.0.8 | |
| Web 2 | No | | 10.0.0.7 | |
| Elk-VM | No | | 10.1.0.4 | |
|  |  | |  | |
|  |  |  | |
|  |  |  | |

**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?*
* *Answer: The main advantage is the ability to automate application deployment to multiple systems within a network.*

The playbook implements the following tasks:

* *Install docker.io, a container that packages and runs an application in an isolated environment.*
* Install pip3, an installer for python3.
* Install docker python module.
* Increase virtual memory.
* Download and launch docker ELK container which includes image sebp/elk: 761, the state as started, and published ports: 5601, 9200, and 5044.

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

A screenshot of a cell phone

Description automatically generated

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* *Web 1: 10.0.0.8, and Web 2: 10.0.0.7*

We have installed the following Beats on these machines:

* *Filebeat successfully, Metricbeat successfully.*
* A screenshot of a computer

  Description automatically generated

A screenshot of a cell phone

Description automatically generated

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.*
* *Answer: Filebeat is used for monitoring log files, forwarding and centralizing log data to Elasticsearch or Logstash for indexing. Metricbeat periodically collects metrics from the operating system and from services running on the server.*

**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?*
* *Answer: The playbook is the file ending with the extension .yml. You copy it to the Elk-VM.*
* *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?*
* *Answer: You would update the configuration file, then the playbook file. Installing it to your private IP. The public one might give you issues in terms of trying to make changes to it and also it's more secure to install things within the internal network.*
* Which URL do you navigate to in order to check that the ELK server is running?
* *Answer: The ELK-VM’s public IP address. In my case: http://40.124.5.54:5601/app/kibana#/home*

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