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)

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 .yml file may be used to install only certain pieces of it, such as Filebeat.

Below are a list of the yml file playbooks

- My First Playbook

- Install ELK

- Filebeat

- Metricbeat

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 available, in addition to restricting access to the network. The load balancer's main purpose is distribution of incoming data creating a security barrier. A jump box provides additional protection from the outside access to the network.

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

- Filebeat watches for log files by location or directly specified log file/files.

- Metricbeat records metrics from the system to help you monitor your servers.

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

|---------------|----------------------------------|----------------|--------------------------|

| Jump Box Provisioner | Gateway | 10.0.0.4 | Linux |

| Web-1 | Server Running Docker | 10.0.0.5 | Linux |

| Web-2 | Server Running Docker | 10.0.0.6 | Linux |

| Web-3 | Server Running Docker | 10.0.0.9 | Linux |

| Elk-Server | Logging Server | 10.2.0.4 | Linux |

Access Policies

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

Only the Jump Box Provisioner machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- PERSONAL IP ADDRESS

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

Jump Box Provisioner allowed access to ELK with PERSONAL IP ADDRESS through the allowed 5601 port.

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

| Name | Publicly Accessible | Allowed IP Addresses |

|-------------------------------|---------------------------|-------------------------------------|

| Jump Box Provisioner | Yes | PERSONAL IP ADDRESS |

| Load Balancer | Yes | 40.85.164.183 |

| Web-1 | No | 10.0.0.5 |

| Web-2 | No | 10.0.0.6 |

| Web-3 | No | 10.0.0.9 |

| Elk-Server | Yes | 40.86.177.11 |

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because the process of the installation or updating can be replicated across multiple machines.

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.

![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:

- Web-1 10.0.0.5

- Web-2 10.0.0.6

- Web-3 10.0.0.9

We have installed the following Beats on these machines:

- Filebeat

- Metricbeat

These Beats allow us to collect the following information from each machine:

- Filebeat is made up of inputs and harvesters. Both of these items work together to look at files that were specified by the user and records event data. It logs files that have changed and when. Example would be monitoring apache servers and MySQL databas logs.

- Metricbeat collects metrics from your systems and services. Examples would be CPU and memory usage.

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 config file to the ansible containers on the webserver VM’s.

- Update the ansible hosts file to include the correct IP addresses of the webservers and Elk Stack.

- Run the playbook, and navigate to [http://[your.VM.IP]:5601/app/kibana](about:blank) to check that the installation worked as expected.

- Which file is the playbook? filebeat-config.yml

- Where do you copy it? cp /etc/ansible/filebeat-config.yml to /etc/ansible/files/filebeat-config.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? To update you would want to run filebeat-config.yml. To target a specific machine you would need to navigate to the /etc/ansible/hosts and edit the file to add the new IP address for the new webserver or elk server.

(Images/docker\_ps\_output.png)

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

[http://[your.VM.IP]:5601/app/kibana](about:blank)

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

- SSH into the jumpbox : example ssh azdmin@10.0.0.0

- sudo apt update

- sudo apt install docker.io

- sudo docker pull cyberxsecurity/ubuntu:bionic

- sudo docker run -ti cyberxsecurity/ansible bash

- sudo docker container list -a

- (Find the correct docker - goofy\_cannon)

- sudo docker start goofy\_cannon

- sudo docker attach goofy\_cannon

To install a playbook (ansible-playbook (name of playbook).yml