# README FILE

## Automated ELK Stack Deployment

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

Images/ELK\_diagram.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 file may be used to install only certain pieces of it, such as Filebeat.

https://gitlab.com/w1810/Ansible/-/tree/9673bbeeaea6ed8b42dadc83aba2ffd066421dc1

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 stable, in addition to restricting unwanted users to the network.

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

- Filebeat: Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

- Metricbeat: Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.

The configuration details of each machine may be found below.

|Name |Function |IP Address |Operating System |

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

|Jump Box |Gateway |10.0.0.5 |Linux |

|Web-1 |DVWA Container |10.0.0.8 |Linux |

|Web-2 |Ansible Container |10.0.0.9 |Linux |

|ELK Stack |ELK Configurations |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 personal IP Address

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

- Jump Box 10.0.0.5

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

|Name |Publicly Accessible |Allowed IP Addresses |

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

|Jump Box |Yes |Personal IP |

|Web-1 |No |10.0.0.5 |

|Web-2 |No |10.0.0.5 |

|ELK Stack |No |10.0.0.9 |

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually. This is advantageous because this saves a tremendous amount of time when recreating setups on new machines.

The playbook implements the following tasks:

- Installs Docker

- Installs Python3

- Increases virtual memory usage

- Downloads and installs Docker Elk container

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

Images/docker\_ps\_output.png

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- 10.0.0.8

- 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 monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

- Metricbeat periodically collects metrics from the operating system and from services running on the server. Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.

### 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 file to /etc/ansible.

- Update the filebeat-config.yml file to include the IP address of your web VM. (For example, my two VMs had the IP addresses of 10.0.0.8 and 10.0.0.9, so I edited the config file to include both.)

- Copy the filebeat-playbook.yml file to /etc/ansible, and run it from that directory by using ansible-playbook filebeat-playbook.yml.

- Navigate to the following address to make sure it was installed correctly: [http://[Public.IP.of.Your.VM]:5601/app/kibana](about:blank)

- To inspect the playbook YAML file, run sudo nano filebeat-playbook.yml. It is possible that you might have to make changes for your specific web VM or to update the link for curl command to download the latest version of Filebeat.

# 

# Interview Question: Cloud Infrastructure as Code

# Cloud Security

**Question 3: Containers**

When is it appropriate to use containers in cloud deployments, and what are the security benefits of doing so?

1. Restate the Problem

Before launching any cloud infrastructure, it is essential to consider the needs and budget of the company or client. If the scale of the project requires containers, then there are many benefits to using them. Containers are cost effective and can be replicated as the client’s needs grow, and they use significantly less resources to run, as opposed to a traditional hardware system, and they can create a very controlled environment for testing purposes.

1. Provide a Concrete Example Scenario

For the first project during boot camp, I was tasked with creating a virtual network that has several virtual machines. More needs were addressed as we progressed through the project such as restricting access, creating containers, and adding ELK configurations and beats to the machines. Of course, not every single measure was taken because this project had very specific needs, much in the same way any organization would.

1. Explain the Solution Requirements

We wanted a totally closed system so that we could test various levels of security controls, including creating a network security group to allow select users, generating public SSH keys, and allowing specific port and IP address access. I also created an ELK stack configuration with Filebeat and Metricbeat with the goal of collecting data about the system and monitoring the machine metrics, respectively.

1. Explain the Solution Details

After installing Docker and the appropriate Ansible container on my machine, I configured my VM settings on Azure by creating a new security rule that allows only my Jump Box to SSH into my Virtual Network. Then, I configured the Ansible host file to allow only the user and IP address of my virtual machines.

1. Identify Advantages/Disadvantages of the Solution

Containers were a great solution for this particular occasion because I was tasked to build an entire virtual network quickly and with a very small budget in mind. They are also very easy to scale up and distribute across several machines and operating systems, as they run uniformly no matter the infrastructure. However, it’s important to keep a limited number of containers to the virtual machines that are compatible with one another and to figure out a more persistent data storage solution.