**Project-1 Homework Readme**

## Automated ELK Stack Deployment

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

Update the path with the name of your diagram](13\_Homework/Readme/Images/docker ps output.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.

- /etc/ansible

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.

- \_Load Balancers protect against distributed denial of service attacks, and ensure availabilty. The advantage of a jump box is a provide restricted access to your network enviroment.

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

- \_Filebeat monitors file logs, collects log events and forwards them for indexing.

- \_Metricbeat records metrics and statistics from an operating system and services running on a server.

The configuration details of each machine may be found below.

| Name | Function | IP Address | Operating System |

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

| Jump Box | Gateway | 10.0.0.4 | Linux |

| Web-1 | DVWA Container | 10.0.0.9 | Linux |

| Web-2 | DVWA Container | 10.0.0.8 | Linux |

| Web-Elk | Elk/Kibana Server | 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:

- 13.82.180.169

Machines within the network can only be accessed by ssh.

- \_TODO: Which machine did you allow to access your ELK VM? Jump Box

What was its 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 | 13.82.180.169 |

| Web-1 | No | 10.0.0.9 |

| Web-2 | No | 10.0.0.8 |

| Web-Elk | Yes | 104.43..169.70 |

### Elk Configuration

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

- The main advantage of automating configuration with Ansible, is that it allows IT administrators to automate away the drudgery from their daily tasks. That frees them to focus on efforts that help deliver more value to the business by spending time on more important tasks

The playbook implements the following tasks:

- Install Docker.

- Create & Attach a container.

- Create Filebeat on Web Vm's.

- Create Filebeat configuration file.

- Create Filebeat installation play.

- Verify the installation & playbook.

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

Update the path with the name of your screenshot of docker ps

(Images/docker\_ps\_output.png)

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- 10.0.0.9

- 10.0.0.8

- 10.1.0.4

We have installed the following Beats on these machines:

- Filebeats

- Metricbeats

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

- Filebeat monitors file logs, collects log events and forwards them for indexing. E.g auditd module collects and parses logs from the audit daemon.

- Metricbeat records metrics and statistics from an operating system and services running on a server. E.g MongoDB module perodically fetches metries from MongoDB servers.

### 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 Ansible playbook file to /etc/ansible/files.

- Update the filebeat.yml file to include name, image, state and ports.

- Run the playbook, and navigate to the Filebeat installation page on the ELK server GUI to check that the installation worked as expected.

\_ Answer the following questions to fill in the blanks:\_

- Which file is the playbook? filebeat-playbook.yml Where do you copy it? /etc/filebeat/filebeat.yml

- Which file do you update to make Ansible run the playbook on a specific machine? The hosts file. How do I specify which machine to install the ELK server on versus which to install Filebeat on? By specifying the which host group that the various systems belong to

- Which URL do you navigate to in order to check that the ELK server is running? <http://104.43.169.70:5601> .

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

- name: Install curl apt: force\_update\_apt: yes name: curl state: present