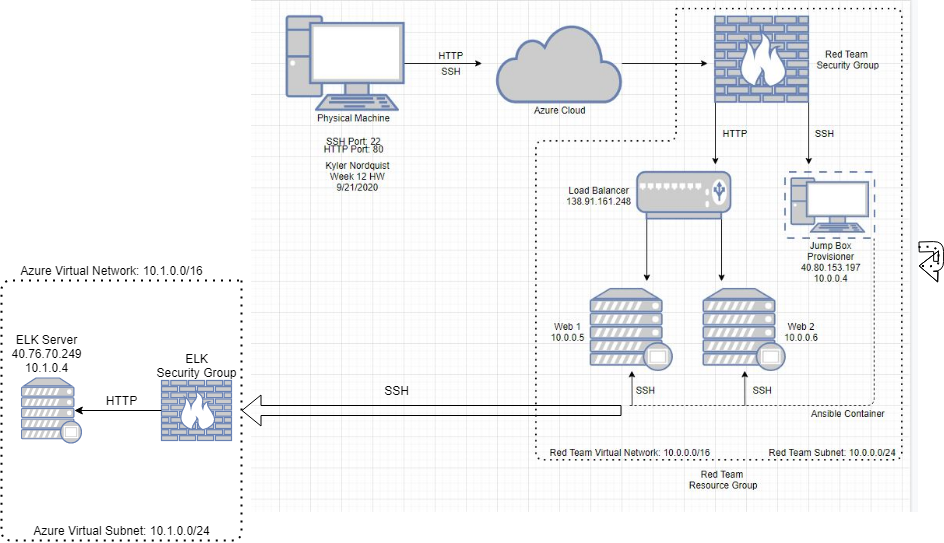
## Automated ELK Stack Deployment

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

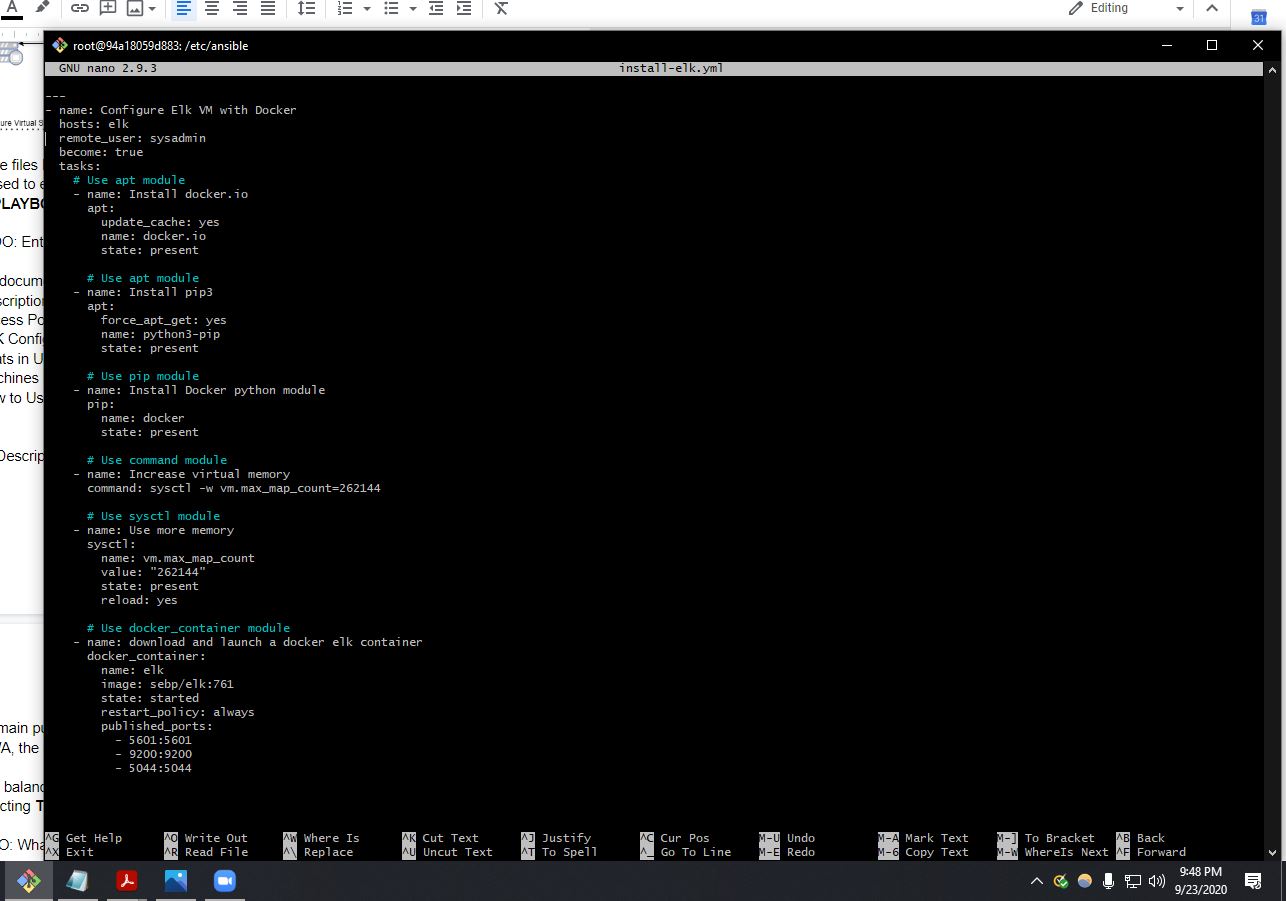
TODO: Update the path with the name of your diagram](Images/diagram\_filename.png)

**Apologies for sloppiness - original network diagram didn’t save.**



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.

TODO: Enter the playbook file.



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 **FUNCTIONAL**, in addition to restricting **TRAFFIC** to the network.

TODO: What aspect of security do load balancers protect? What is the advantage of a jump box?

**Load balancers protect against attacks like DDoS, as they distribute traffic to several different servers that it overlooks and is assigned to. The advantage of having a jump box is that it requires a secured login (user/pass/ip) before any administrative tasks can be performed on the servers.**

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

TODO: What does Filebeat watch for?

**Filebeat watches for SSH connections, uses of administrative privileges and commands.**

TODO: What does Metricbeat record?

**Metricbeat watches and records different metric outputs such as CPU usage, Memory usage, and statistics about the open containers.**

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 | Server | 10.0.0.5 | Linux |

| Web 2 | Server 2 | 10.0.0.6 | Linux |

| ELKSERVER | Network Overview | 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:

TODO: Add whitelisted IP addresses\_

**My physical machine's IP? Ya right... ;)**

Machines within the network can only be accessed by **SSH CONNECTION**.

TODO: Which machine did you allow to access your ELK VM? What was its IP address?\_

**JumpBox (13.64.233.231) -> Elk Server (40.76.70.249)**

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | No | Physical Machine |

| Web 1 | No | 10.0.0.4 |

| Web 2 | No | 10.0.0.4 |

| Elk Server | No | 10.0.0.4 |

### 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?\_

**Everything is written into a playbook, which is a single file that you can copy and deploy to 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.\_

**1) Build and connect to Jump Box Provisioner Container**

**2) Check for and start/attach Jump Box Provisioner Container**

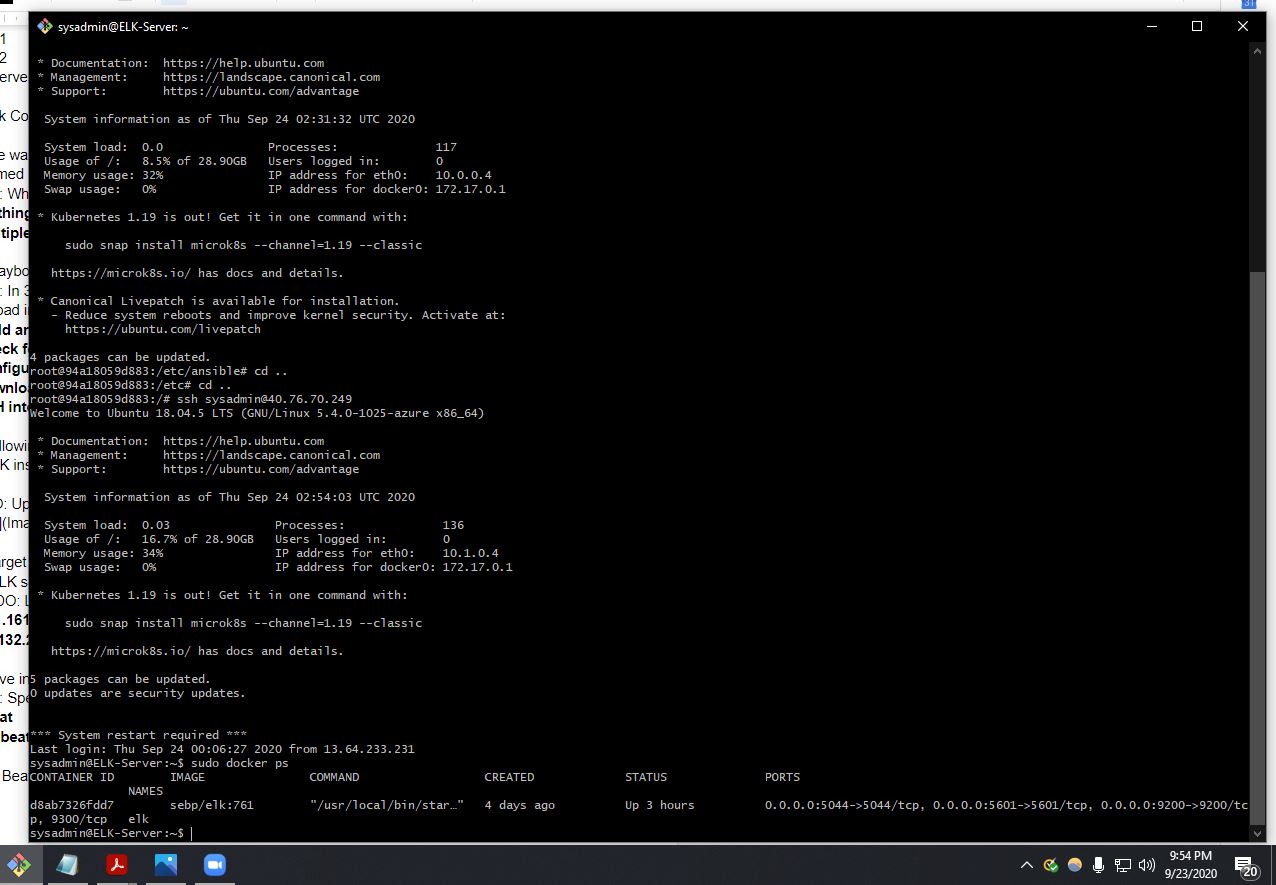
**3) Configure new VM using new SSH Key (Add VM to Ansible Hosts file)**

**4) Download image and search for ELK Docker**

**5) SSH into ELK VM and make sure everything is started and running**

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]



### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- \_TODO: List the IP addresses of the machines you are monitoring\_

**138.91.161.248**

**49.11.132.249**

We have installed the following Beats on these machines:

TODO: Specify which Beats you successfully installed:

**Filebeat**

**Metricbeat**

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.

**Filebeat - watches for SSH connections, uses of administrative privileges and commands.**

**Metricbeat - watches and records different metric outputs such as CPU usage, Memory usage, and statistics about the open containers.**

### 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 **PLAYBOOK** file to **/etc/ansible** .

- Update the **PLAYBOOK** file to include...

- Run the playbook, and navigate to **ELK CONTAINER** 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? **YML, /etc/ansible**

- 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? **Playbook.yml, Jump Box container = playbook to download docker and update ELK Server, install Filebeat on ELK Server since it overlooks servers**

- Which URL do you navigate to in order to check that the ELK server is running? **http://your.VM.IP:5601/app/kibana**

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

**nano elk-installation.yml**

**ansible-playbook elk-installation.yml**