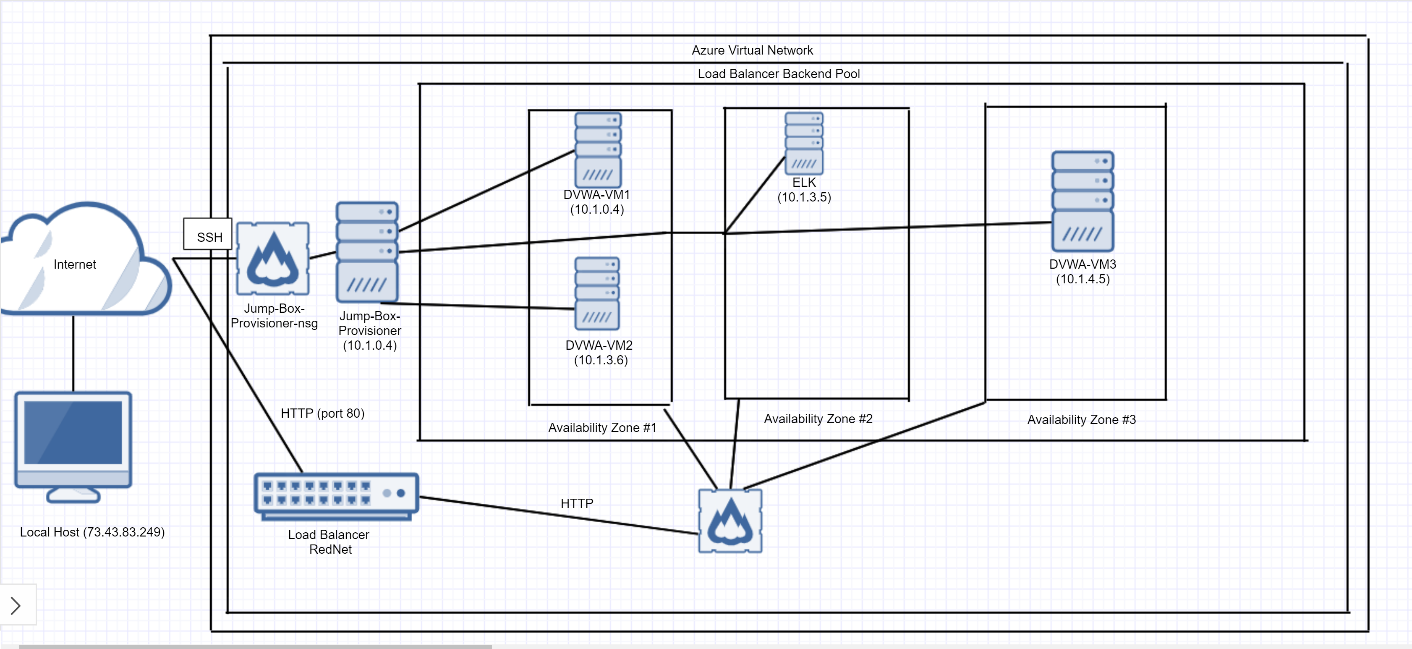
## Automated ELK Stack Deployment

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



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 **Project 1 - Elk Stack Diagram** file may be used to install only certain pieces of it, such as Filebeat.

* **Filebeat-playbook.yml**
* **Filebeat-configuration.yml**

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 **DoS attacks** to the network.

- What aspect of security do load balancers protect? What is the advantage of a jump box? **The advantage of a jump box is that it prevents all VMs on Azure from being exposed to the general public.**

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

- What does Filebeat watch for? **Filebeat watches for log files and/or locations that are specified, and as it collects log events, it is forwarded to either Elasticsearch or Logstash for indexing.**

- What does Metricbeat record? **Metricbeat records metrics from the operating system and metrics from services that are 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 | 10.1.0.4 | Linux |

| DVWA-VM1 | Server | 10.1.3.6 | Linux |

| DVWA-VM2 | Server | 10.1.4.4 | Linux |

| DVWA-VM | Server | 10.1.4.5 | Linux |

| ELK-VM | Server | 10.1.3.5 | 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:

**73.43.83.249 (IP address of the local host)**

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

- Which machine did you allow to access your ELK VM? What was its IP address? **I used the Jump-Box-Provisioner to access my ELK VM. The IP address of the ELK VM is 10.1.0.4.**

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | 73.43.83.249 |

| DVWA-VM1 | No | 10.1.0.4 |

| DVWA-VM2 | No | 10.1.0.4 |

| DVWA-VM3 | No | 10.1.0.4 |

| 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

- What is the main advantage of automating configuration with Ansible?

**The main advantage is that the Ansible playbooks are written in YAML, which makes it primed for management configuration.**

The playbook implements the following tasks:

- In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.\_

**- ssh into the New-Jump-Box-Provisioner from the localhost machine**

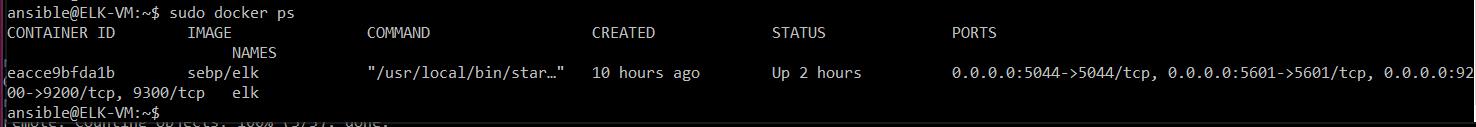
- **Start and attach the ansible docker container. My ansible docker container was called “unruffled\_montalcini.” As a result, I first ran “sudo docker start unruffled\_montalcini”, and then I ran “sudo docker attach unruffled\_montalcini”.**

- **Once I accessed the root, I change directories into the /etc/ansible/roles and create the ELK playbook (elk-playbook.yml).**

- **Run the elk-playbook.yml by typing “ansible-playbook elk-playbook.yml”.**

- **ssh into the ELK-VM to verify that the ELK-VM has been configured.**

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



### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- List the IP addresses of the machines you are monitoring:

- **10.1.3.6 (DVWA-VM1)**

**- 10.1.4.4 (DVWA-VM2)**

**- 10.1.4.5 (DVWA-VM3)**

We have installed the following Beats on these machines:

- **The beats that were installed in this project were Filebeat and Metricbeat.**

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

- 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.\_

**Metricbeat collects the statistics from your web activity and ships it to either Elasticsearch or Logstash. Filebeat monitors the locations or log files that are specified by the user, and after it collects log events, the data is forwarded to either Elasticsearch or Logstash for indexing.**

### 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-configuration.yml** file to **/etc/ansible/roles/files**.

- Update the **filebeat-configuration.yml** file to include **ELK Private IP in lines 1106 and 1806.**

- Run the playbook and navigate to **http://20.49.1.209:5601** to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

- Which file is the playbook? Where do you copy it? **The playbook is filebeat-playbook.yml and copy it to /etc/ansible/roles.**

- Which file do you update to make Ansible run the playbook on a specific machine? **The filepath to run the ansible playbook on a specific machine is /etc/ansible/hosts file.**

- How do I specify which machine to install the ELK server on versus which to install Filebeat on? **I had to define two different groups in the /etc/ansible/hosts file (webservers and elkservers). For the webservers group, I had to specify the private IPs of the VMs that needed Filebeat installed. For the elkservers group, I had to include the IP of the VM that needed ELK installed.**

- Which URL do you navigate to in order to check that the ELK server is running? <http://40.76.104.255:5601/>

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

**To create the filebeat-configuration.yml file: nano filebeat-configuration.yml.**