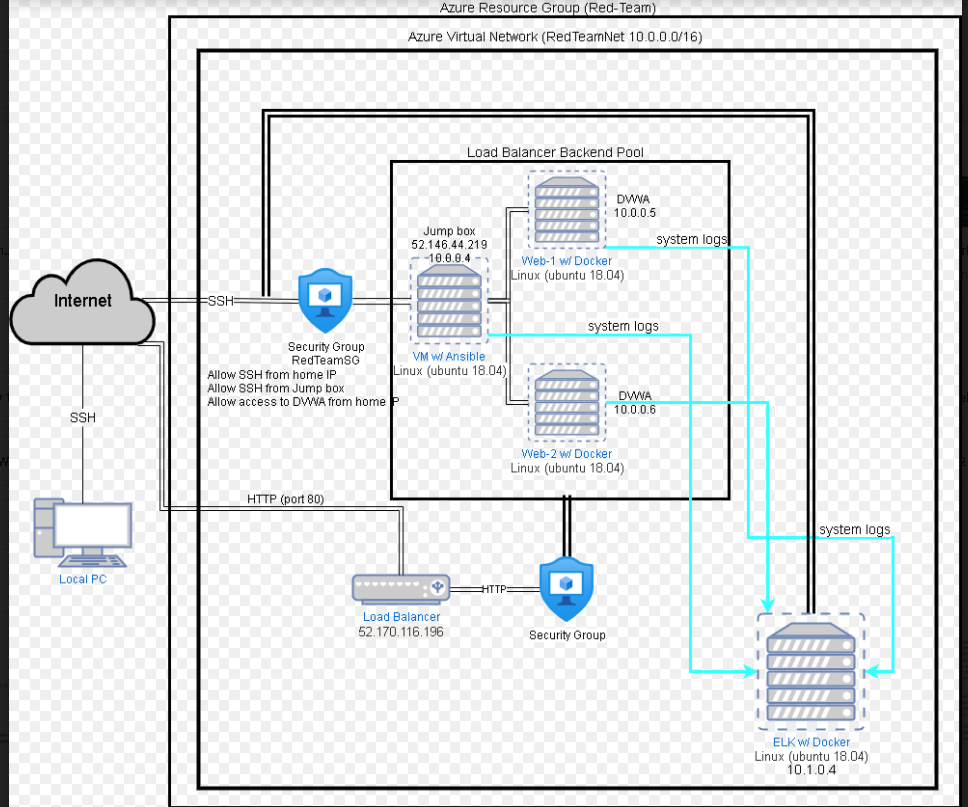
## Automated ELK Stack Deployment

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 \_\_my-elk-playbook.yml\_\_ 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 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 \_\_protective\_\_, in addition to restricting \_\_inbound traffic\_\_ to the network.

* TODO: What aspect of security do load balancers protect? It protects servers form overloading and, possibly, breaking down. The load balancer is there to redirect traffic incase on the servers go down.
* What is the advantage of a jump box? The jump box prevents the VM from being exposed to the public and makes it the point of entry when connecting with a Remote Desktop

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

* TODO: What does Filebeat watch for?
  + Filebeat watches an monitors log files and other locations that the user specifies, it collects log event and forwards them to Elasticsearch or Logstash for indexing
* TODO: What does Metricbeat record?
  + Metricbeat is a shipper that records and collects metrics from the OS and from running services on the server. It takes the metrics and statistics that it collects and ships them to either Elasticsearch or Logstash.

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 | 10.0.0.6 | Linux |
| ELK-SERVER | Monitoring | 10.1.0.4 | 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: 73.12.204.74

* TODO: Add whitelisted IP addresses.

Machines within the network can only be accessed by \_\_Jump Box Provisioner and each other\_\_.

* TODO: Which machine did you allow to access your ELK VM? Jump box Provisioner. 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 | 73.12.204.74 |
| Web-1 | No | 10.0.0.4 |
| We-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... it seals it from any vulnerabilities.

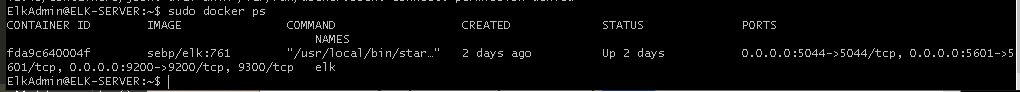
* TODO: What is the main advantage of automating configuration with Ansible?
  + It is an open-source automation tool that can help platform, configuration management and application deployment.

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.
  + Install docker.io
  + Install pip3
  + Install Docker python module
  + Use more memory
  + Download and launch a docker elk container
  + Enable docker service

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

Note: The following image link needs to be updated. Replace docker\_ps\_output.png with the name of your screenshot image file.



### Target Machines & Beats

This ELK server is configured to monitor the following machines:

* 10.0.0.5 and 10.0.0.6

We have installed the following Beats on these machines: Filebeat

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

### Filebeat: detects changes to the filesystem and collects apache logs

* Metricbeat: detects changes in the filesystem metrics such as CPU usage, SSH logins, CPU statistics and failed sudo escalations.

### 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\_\_\_\_ file to \_\_/etc/ansible/roles\_\_\_.
* Update the \_hosts\_\_\_\_ file to include webserver and ELK
* Run the playbook and navigate to \_\_Kibana\_\_ to check that the installation worked as expected.

TODO: Answer the following questions to fill in the blanks:

* Which file is the playbook? Filebeat-playbook.yml and metricbeat-playbook.yml Where do you copy it? To /etc/ansible/roles directory
* Which file do you update to make Ansible run the playbook on a specific machine?
  + You would update the filebeat-config.yml and metricbeat-config.yml to run the ansible-playbook
  + You would also update the hosts file: /etc/ansible/hosts

[webservers]

10.0.0.4 ansible\_python\_interpreter=/usr/bin/python3

10.0.0.5 ansible\_python\_interpreter=/usr/bin/python3

10.0.0.6 ansible\_python\_interpreter=/usr/bin/python3

[elk]

10.1.0.4 ansible\_python\_interpreter=/usr/bin/python3

* How do I specify which machine to install the ELK server on versus which to install Filebeat on?
  + You would need to make a new group [webserver] and include the VM IP’s and [elk] and include the Elk server IP.
* Which URL do you navigate to in order to check that the ELK server is running?
  + You would navigate to the http://[ELK public IP]:5601 (use the ELK server public IP) to access Kibana

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

SSH [RedAdmin@10.0.04](mailto:RedAdmin@10.0.04)

Sudo docker container list -a

Sudo docker start container (container name)

Sudo docker attach container (container name)

Cd /etc/ansible

Nano /etc/ansible/hosts (add webservers and elk groups with the private IP and ansible\_python\_interpreter=/usr/bin/python3 after the IP

Curl <https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat> >> /etc/ansible/filebeat-config.yml

Update file:

```

output.elasticsearch:

Hosts: [“Elk private IP]:9200

Username: “elastic”

Password: “changeme”

```

```

Setup.kibana:

Hosts: “Elk private IP]:5601

```

Curl <https://artiacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.4.0-amd64.deb> >> /etc/ansible/metricbeat-config.yml

Do the same steps as the filebeat when updating the file

Create filebeat-playbook.yml and metricbeat-playbook.yml

Run ansible-playbook filebeat-playbook.yml

Run ansible-playbook metricbeat-playbook.yml

Once you have the “ok” with the from running the playbooks you are ready to navigate to Kibana

In your browser go to <http://(Elk> public IP):5601 and this should bring up the Kibana web portal and you are ready to monitor your VMs