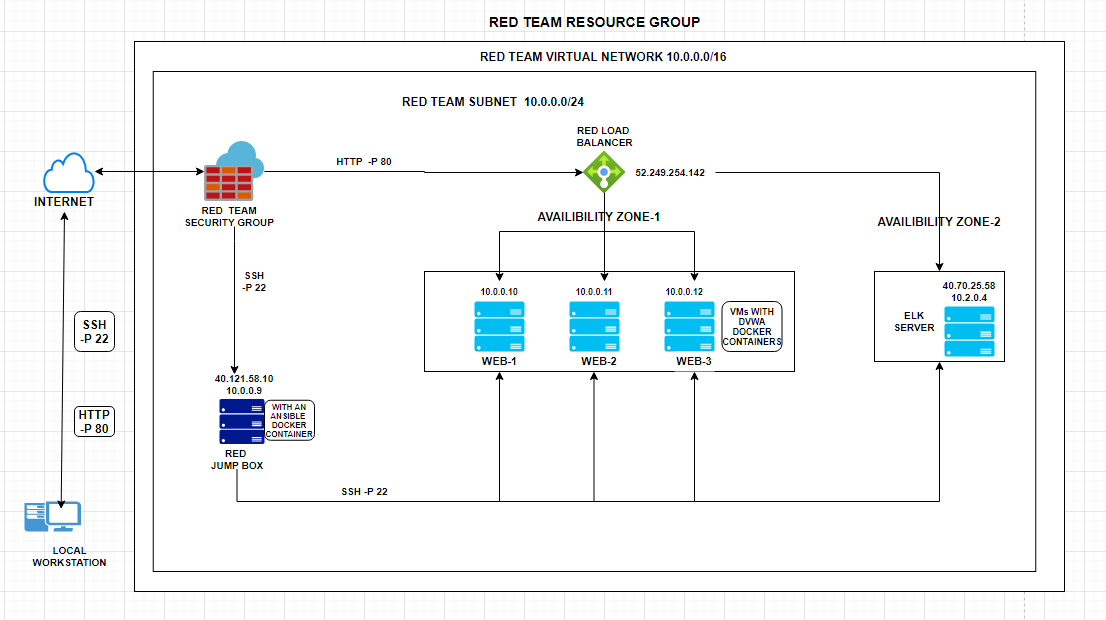
## **Automated ELK Stack Deployment**

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

**Note**: The following image link needs to be updated. Replace diagram\_filename.png with the name of your diagram image file.



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.yml files may be used to install only certain pieces of it, such as Filebeat.

* filebeat-playbook.yml
* filebeat-config.yml

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 enables an application to be highly functional by distributing and also restricting unusual high-traffic to the network.

* *What aspect of security do load balancers protect?*

Prevents overloading of servers and maximizes their uptime.

* *What is the advantage of a jump box?*

Jump Box acts as a Gateway, avoids redundancy and provides a single point secured access to the network

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

* *What does Filebeat watch for?*

It watches and monitors the specified log files/events and enables them for indexing.

* *What does Metricbeat record?*

It records statistics and metric data of the operating system and the services 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 | 10.0.0.9  40.121,58.10 | Linux |
| DVWA-VM1 | webserver | 10.0.0.10 | Linux |
| DVWA-VM2 | webserver | 10.0.0.11 | Linux |
| DVWA-VM3 | webserver | 10.0.0.12 | Linux |
| ELK Server | Elkserver | 10.2.0.4  40.70.25.58 | 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:

* Personal IP Address

Machines within the network can only be accessed by \_\_\_\_

* The ELK-VM is accessible by SSH from the JumpBox which is accessed via web from Personal IP Address

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Address** |  |
| Jump Box | Yes/No | 40.121,58.10 - Public IP Address  10.0.0.9 - Private IP Address |  |
| DVWA-VM1 | No | 10.0.0.10 |  |
| DVWA-VM2 | No | 10.0.0.11 |  |
| DVWA-VM3 | No | 10.0.0.12 |  |
| ELK Server | No | 10.2.0.4 |  |

### **Elk Configuration**

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

* Using playbooks multiple machines can be configured with a single command

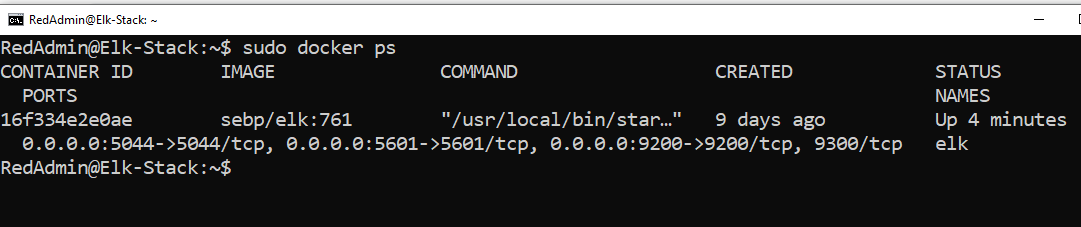
The playbook implements the following tasks:

In 3-5 bullets, explain the steps of the ELK installation

* SSH into the Jump-Box-Provisioner
* Start and attach the ansible docker
* Created the playbook.yml in the /etc/ansible/roles directory
* Ran the Playbook.yml in that same directory
* Verified that the server is up by SSH into the ELK-VM

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:

* DVMA-VM1 - 10.0.0.10
* DVMA-VM2 - 10.0.0.11
* DVMA-VM3 - 10.0.0.12

We have installed the following Beats on these machines:

* Filebeat
* Metricbeat

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

* Filebeat monitor log files and collect log events
* Metricbeats provides the machine metrics

### **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:

For Filebeat:-

* Copy the filebeat-config.yml file to /etc/ansible/roles
* Update to include the correct ELK-VM private IP in the filebeat-config.yml file
* Run the playbook, and navigate to ELK-VM Public IP Address to check the installation

For Metricbeat:-

* Copy the metricbeat-config.yml file to /etc/ansible/roles/
* Update to include the the correct ELK private IP in the metricbeat-config.yml file
* Run the playbook, and navigate to ELK-VM public IP to check the installation

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

Filebeat Installation file with commands

---

- name: installing and launching filebeat

hosts: webservers

become: yes

tasks:

- name: download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-amd64.deb

- name: install filebeat deb

command: dpkg -i filebeat-7.6.2-amd64.deb

- name: drop in filebeat.yml

copy:

src: /etc/ansible/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

- name: enable and configure system module

command: filebeat modules enable system

- name: setup filebeat

command: filebeat setup

- name: start filebeat service

command: service filebeat start

- name: enable service filebeat on boot

systemd:

name: filebeat

enabled: yes

Metricbeat Installation file with commands

---

- name: Install metric beat

hosts: webservers

become: true

tasks:

# Use command module

- name: Download metricbeat

command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.2-amd64.deb

# Use command module

- name: install metricbeat

command: sudo dpkg -i metricbeat-7.6.2-amd64.deb

# Use copy module

- name: drop in metricbeat config

copy:

src: /etc/ansible/metricbeat-config.yml

dest: /etc/metricbeat/metricbeat.yml

# Use command module

- name: enable and configure docker module for metric beat

command: metricbeat modules enable docker

# Use command module

- name: setup metric beat

command: metricbeat setup

# Use command module

- name: start metric beat

command: service metricbeat start

# Use systemd module

- name: enable service metricbeat on boot

systemd:

name: metricbeat

enabled: yes