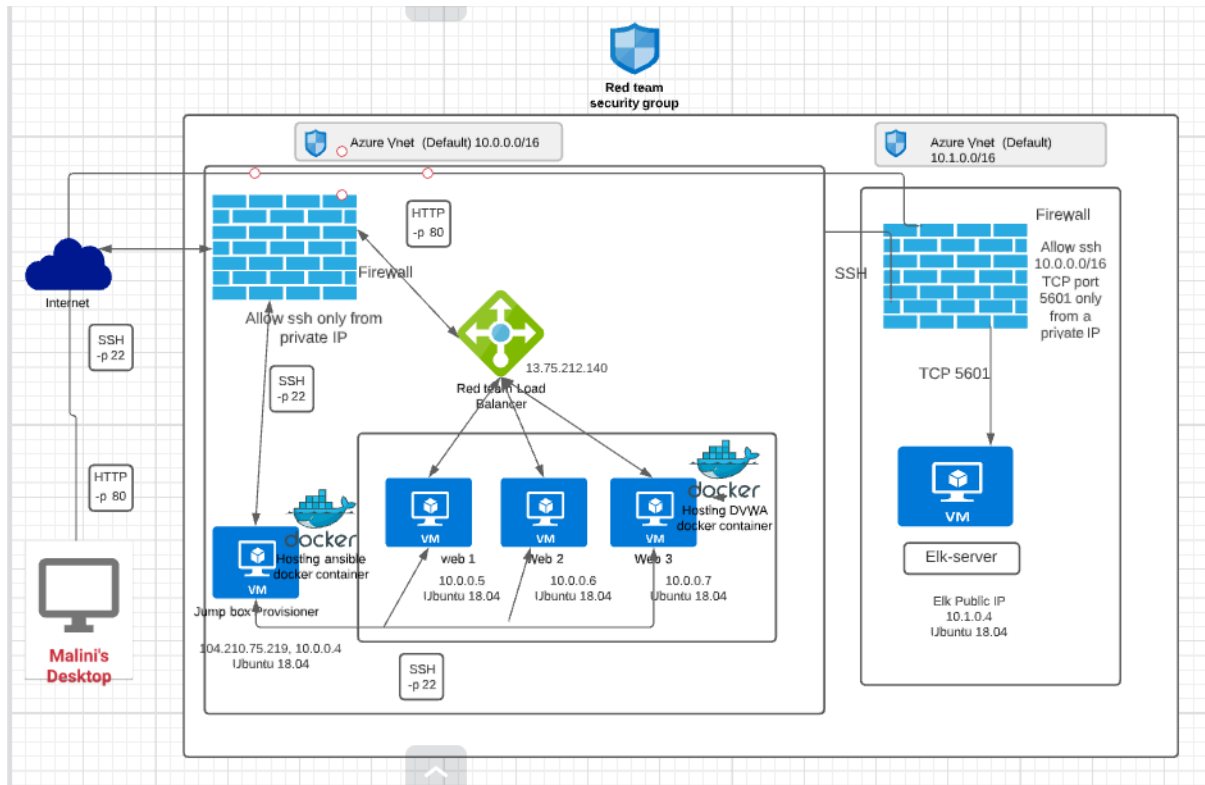


Automated Stack Deployment

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 .yaml file may be used to install only certain pieces of it, such as Filebeat.

- The Ansible playbooks required to recreate the Elk server:
- install-elk.yaml
- filebeat-playbook.yaml

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 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 balancing ensures that the application will be highly functional, in addition to restricting high-traffic to the network.
- What aspect of security do load balancers protect?
 - It helps prevent overloading servers as well as optimizes productivity and maximizes uptime.
 - It also adds resiliency by rerouting live traffic from one server to another causing it to eliminate single points of failure from attacks such as DDoS attack.
- What is the advantage of a jump box?
 - The advantage of having a jump box is being able to use a virtual machine that has hardened security and can manage other systems within your security zone or over all network. Jump-box are highly secured computers that are never used for non-admin tasks.
 - Throughout the years, jump-box has improved into an even more comprehensive/lock-down secure admin workstation to decrease the chances of hackers/malware infection.

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 watch for any information in the file system which has been changed and when it has ,It monitors the log files/locations that you specify and forwards them to Elasticsearch/Logstash for indexing.
- What does Metricbeat record?
 - Metricbeat takes the metrics and statistics that collects and ships them to the output you specify. It records metrics/statistics data and transports them to the output that you specifics thru Elasticsearch/Logstash.

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
Jump-Box-Provisioner	Gateway	10.0.0.4	Linux Ubuntu 18.04
Web-1	Docker-DVWA	10.0.0.5	Linux Ubuntu 18.04
Web-2	Docker-DVWA	10.0.0.6	Linux Ubuntu 18.04
Web-3	Docker-DVWA	10.0.0.7	Linux Ubuntu 18.04
Elk	Elk stack	10.1.0.4	Linux Ubuntu 18.04

Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the Jump-Box-Provisioner box machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- Access to this machine is only allowed from the following IP addresses:
 - LocalHost IP address

Machines within the network can only be accessed by ssh.

- The Elk server can only be reached via ssh @ 10.1.0.4 from the jumpbox on 10.0.0.4 or on TCP port 5601 from a specified IP address

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

Name	Publicly Accessible	Allowed IP Addresses
Jump-Box-Provisioner	No	A Specified IP address Only
Web-1	No	Jumpbox 10.0.0.4 for SSH & A Specified IP address Only for TCP Port 80
Web-2	No	Jumpbox 10.0.0.4 for SSH & A Specified IP address Only for TCP Port 80

Name	Publicly Accessible	Allowed IP Addresses
Web-3	No	Jumpbox 10.0.0.4 for SSH & A Specified IP address Only for TCP Port 80
Elk1	No	Jumpbox 10.0.0.4 for SSH & A Specified IP address Only for TCP Port 5601

Elk Configurations

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

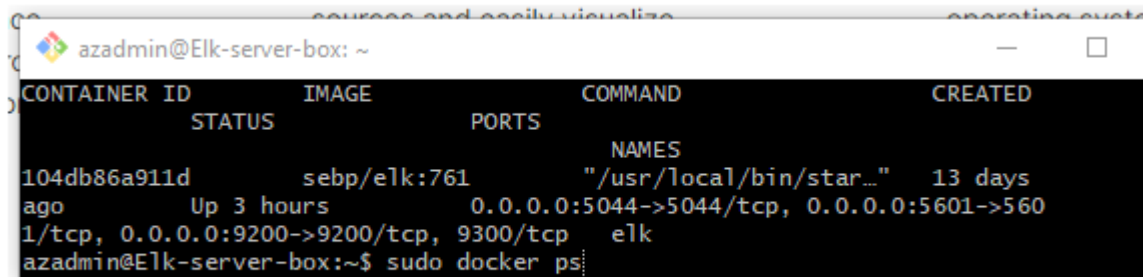
- What is the main advantage of automating configuration with Ansible?

The main advantages of automating configuration through Ansible is the ease of use and an extremely easy learning curve. Through the use of YAML Playbooks you are able to configure multiple Machines through the use of a single command after initial configuration. It makes deployment very easy and scalable, instead of needing to connect and configure each server individually, servers can be configured by one set of scripts running on ansible and deployed to all servers at once.

The playbook implements the following tasks:

- Install docker
- install docker module for pip
- increase the virtual memory
- Download and launcch the elk container
- Enable the docker service on boot
- Create a New VM (should be named something simple "Elk-Server") Keep note of the Private IP (10.1.0.4) and the Public IP (0.0.0.0) you will need the Private IP to SSH into the VM and the Public IP to connect to the Kibana Portal (HTTP Site) to view all Metrics/Syslogs.
- Download and Configure the "elk-docker" container "In the hosts. Then you need to create a new ansible-playbook (install-elk.yml)that will download, install, configures the "Elk-Server" to map the following ports [5601] and starts the container.
- Launch and expose the container "After installing and starting the new container. You can verify that the container is up and running by SSH into the container from your JumpBox Once you are in the [Elk-Server] run the command [sudo docker ps]
- Create new Inbound Security Rules to allow Ports: 5601 "The Inbound Security Rules should allow access from your Personal Network"
- Open a new browser and type in the [Elk-server Public IP:5601] to access the Kibana Portal Site

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



```
azadmin@Elk-server-box: ~  
CONTAINER ID        IMAGE               COMMAND             CREATED  
104db86a911d       sebp/elk:761       "/usr/local/bin/star... 13 days  
ago                Up 3 hours         0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk  
azadmin@Elk-server-box:~$ sudo docker ps
```

Target Machines and Beats

This ELK server is configured to monitor the following machines:

- 10.0.0.5, 10.0.0.6 and 10.0.0.7

We have installed the following Beats on these machines:

- Filebeats and Metricbeat

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

- Filebeat is a lightweight shipper for forwarding and centralizing log data. Filebeat monitors log files in locations you specify, collects log events, and forwards them either to Elasticsearch for indexing.
- Metricbeat collects metrics from the operating system and from services running on the server.

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 `file-config.yml` file to `/etc/ansible/roles/files/`.
- Update the `filebeat-config.yml` to include the Private IP of the Elk-Server to the Elasticsearch and Kibana sections of the configuration file.
- Run the playbook, and navigate to ELk-Server to check that the installation worked as expected.
- Which file is the playbook?
`filebeat-playbook.yml`

- Where do you copy it?
/etc/ansible/roles
- Which file do you update to make Ansible run the playbook on a specific machine?
/etc/ansible/hosts file (IP of the Virtual Machines).
- How do I specify which machine to install the ELK server on versus which to install Filebeat on?
I have to specify two separate groups in the etc/ansible/hosts file. One of the groups will be webserver which has the IPs of the VMs that I will install Filebeat to. The other group is named elkserver which will have the IP of the VM I will install ELK to.
- Which URL do you navigate to in order to check that the ELK server is running?
The URL to use to verify the Elk-Server is running is the Public IP (0.0.0.0:5601)

To install the Elk server, filebeat and metricbeat you will need to perform the following tasks

- SSH to the Jump-Box-Provider
- Sudo docker status
- sudo docker container list -a (to list the containers and to locate the ansible container)
- sudo docker start "container-name"
- sudo docker attach "container-name"
- ensure you have placed your playbooks in /etc/ansible/roles
- edit your /etc/ansible/ansible.cfg as per instructions above
- edit your /etc/ansible/hosts file to include your elk server under the [elk] entries in the hosts file
- edit your /etc/ansible/hosts file to include your web server under the [webserver] entries in the hosts file
- run sudo ansible-playbook /etc/ansible/roles/install-elk.yml and wait a few minutes for the task to complete.
- run sudo ansible-playbook /etc/ansible/roles/filebeat-playbook.yml and wait a few minutes for the task to complete.
- run sudo ansible-playbook /etc/ansible/roles/metricbeat-playbook.yml and wait a few minutes for the task to complete. Open a web browser from the allowed IP address and surf to "Elk Server Public IP":5601 to see the kibana portal pages.
- See below the image of the opened portal

