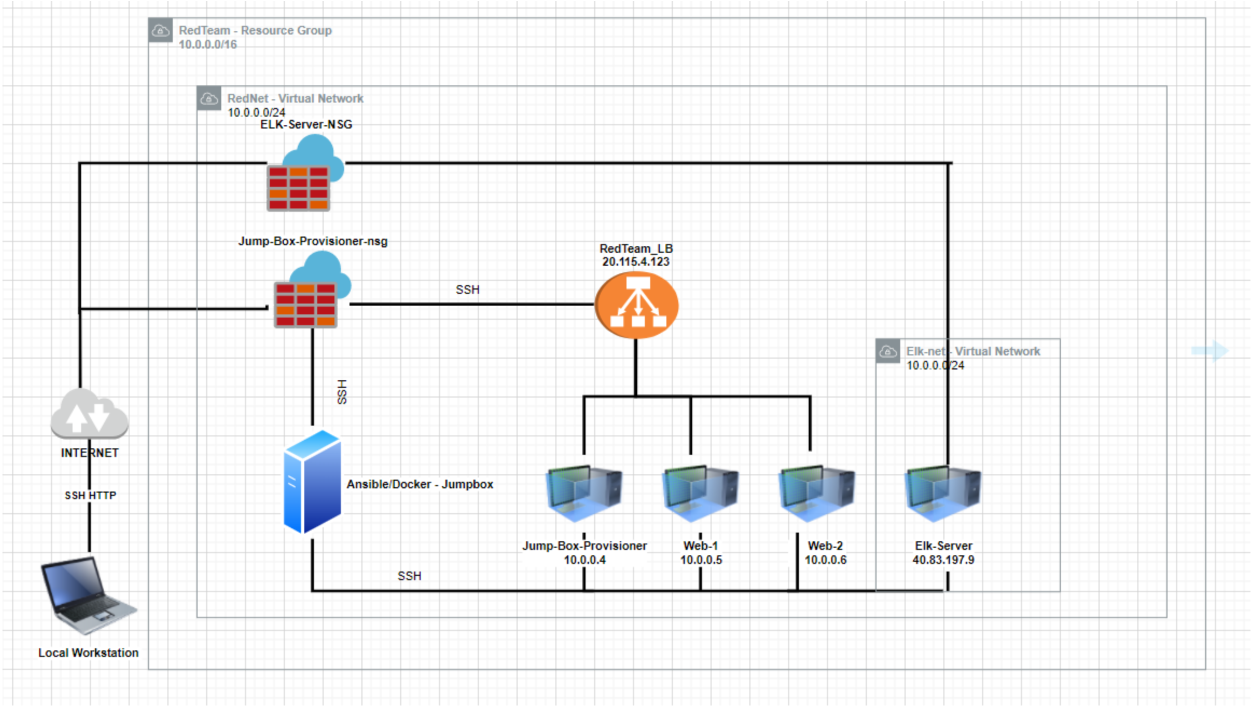
Automated ELK Stack Deployment

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

~/etc/ansible/filebeat-playbook.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 ensures that the application will be highly **available**, in addition to restricting **access** to the network.

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

Load balancers protect against DDos attacks, and many other security threats by distributing network traffic or “loads” across multiple servers. Load balancers protect the availability of cybersecurity because it ensures that no servers are overworked. A jump box serves as a single point of origin for administrators who would like to access multiple servers or unreliable networks. They provide a clear tunnel for administrators to access devices in separate security zones.

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

What does Filebeat watch for?_

Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

What does Metricbeat record?_

Metricbeat records metrics and statistics that it collects from your servers and ships them to the output that you specify.

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
JumpBox	Gateway	10.0.0.4	Linux
Web 1	Web server	10.0.0.5	Linux
Web 2	Web 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 **JumpBox** machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- **20.185.16.253**

Machines within the network can only be accessed by **each other**.

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

My personal workstation or laptop was allowed access to the Elk-server VM.
Workstation IP address: **24.186.69.19**

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

Name	Publicly Accessible	Allowed IP Addresses
JumpBox	Yes	24.186.69.19
Web1	No	10.0.0.0/24
Web2	No	10.0.0.0/24
Elk Server	No	10.0.0.0/24

Elk Configuration

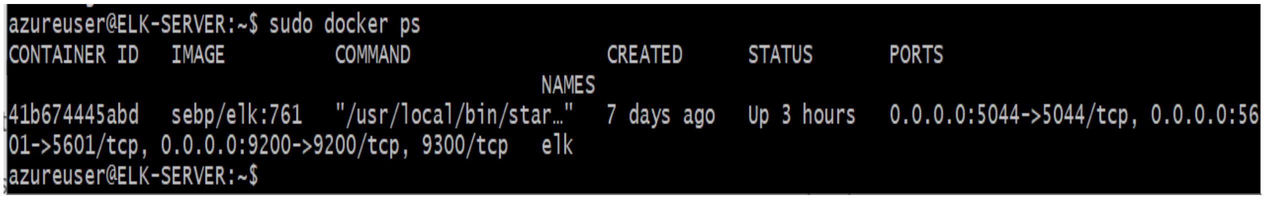
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because ansible is an agentless, open source software that is best used for simplifying and speeding up the production of difficult tasks. It does not rely on the client-server model and therefore speeds up the configuration process.

The playbook implements the following tasks:

- **Install Docker:** docker is installed to the remote server
- **Install Python3_pip:** Pip is installed which allows for additional docker modules to be installed easier

- **Docker Module:** ensures that the pip module installs the necessary docker component modules
- **Increase Memory/Use More Memory:** increasing the memory of the elk docker allows the server to launch
- **Download and Launch ELK Container:** downloads and launch elk container with specified ports

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



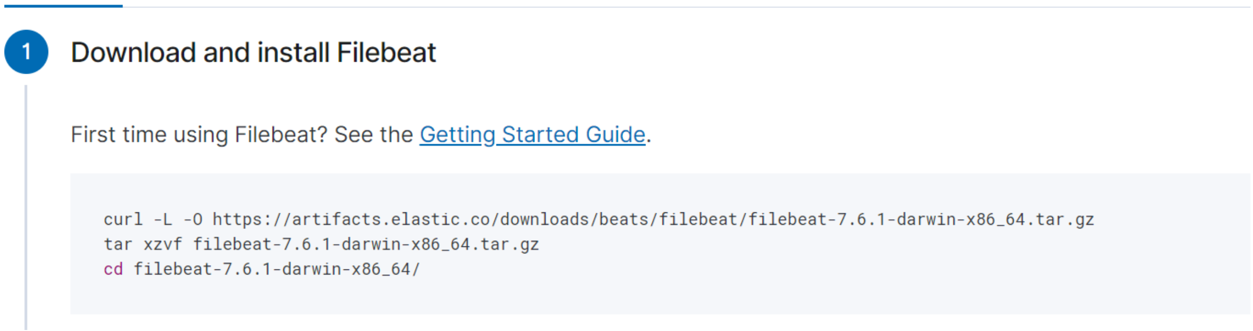
```
azureuser@ELK-SERVER:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED      STATUS       PORTS
                                                 NAMES
41b674445abd   sebp/elk:761   "/usr/local/bin/star…"   7 days ago   Up 3 hours   0.0.0.0:5044->5044/tcp, 0.0.0.0:56
01->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
azureuser@ELK-SERVER:~$
```

Target Machines & Beats

This ELK server is configured to monitor the Web1 and Web2 virtual machines. Their IP addresses are **10.0.0.5** and **10.0.0.6**, respectively.

We have installed the following Beats on these machines:

- Filebeat

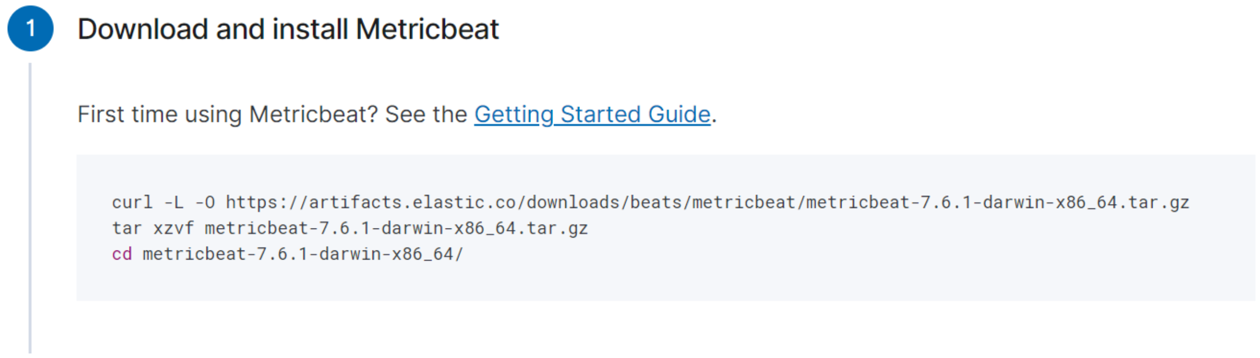


1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-darwin-x86_64.tar.gz
tar xzvf filebeat-7.6.1-darwin-x86_64.tar.gz
cd filebeat-7.6.1-darwin-x86_64/
```

- Metricbeat



Download and install Metricbeat

First time using Metricbeat? See the Getting Started Guide.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-darwin-x86_64.tar.gz
tar xzvf metricbeat-7.6.1-darwin-x86_64.tar.gz
cd metricbeat-7.6.1-darwin-x86_64/
```

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

Filebeat is used to collect log files from specific files on the virtual machines which can be generated by softwares such as Apache or Microsoft Azure tools. Metricbeat collects and analyzes the virtual machine’s metrics such as the CPU usage.

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 **elk_config.yml** file to **filebeat-playbook.yml**.

- Update the **elk_config.yml** file to include virtual machines’ IP addresses as hosts to the playbook.

- Run the playbook, and navigate to **http://40.83.197.9:5601/app/kibana** to check that the installation worked as expected.