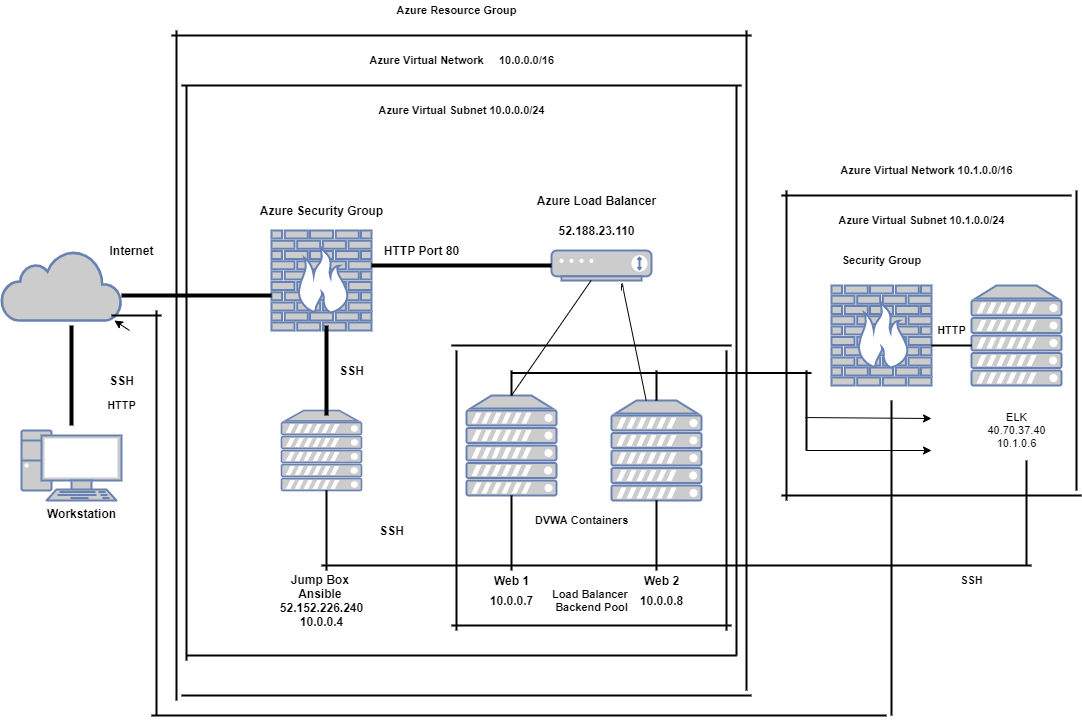
**Automated ELK Stack Deployment**

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

* /etc/ansible/install-elk.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.

*The load balancer has a health probe that monitors the machines and if there is a problem it reroutes the traffic IE: DDoS attack*

* *What is the advantage of a jump box? It gives users a single node of access that can be secured and monitored*

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the Files and system Logs.

* *TODO: What does Filebeat watch for?*

Organizes and logs files and keeps track of the changing of files and the time they were changed

* *TODO: What does Metricbeat record?*

*It collects stats and metrics that it sends to 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 | | DVWA Web-1 | Server | 10.0.0.7 | Linux | | DVWA Web-2 | Server | 10.0.0.8 | Linux | | ELK | Server | 10.1.0.6 | Linux | |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Access Policies**

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

Only the Load Balancer machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* *10.0.0.7 ,10.0.0.8*

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

Jump Box 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 | Public |
| DVWA Web-1 | No | 10.0.0.4 |
| DVWA Web-2 | No | 10.0.0.4 |
| ELK Server | No | 10.0.0.4 |

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes/No | 10.0.0.1 10.0.0.2 |
|  |  |  |
|  |  |  |

**Elk Configuration**

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

* *It can be easily used to configure multiple machines and editing is simple*

The playbook implements the following tasks

* *Configure ELK VM with Docker*
* *Ist module is Install docker.io*
* *Next module Install pip3*
* *Next module Install Docker python module*
* *Next sysctl module Use more memory vm.max\_map\_count 262144*
* download and launch a docker elk container sebp/elk:761 Publish ports
* Last module Enable service docker on boot

The following screenshot displays the result of running docker ps after successfully configuring the ELK instance. Graphical user interface, text

Description automatically generated

**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: DVWA Web-1 10.0.0.7 & DVWA Web-2 10.0.0.8

We have installed the following Beats on these machines: Filebeat

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

Filebeat collects log files for each machine and forwards them for indexing or processing

* Graphical user interface, text, application, email

  Description automatically generated

**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 \_\_\_\_\_ file to \_\_\_\_\_.
* Update the \_\_\_\_\_ file to include...
* Run the playbook, and navigate to \_\_\_\_ to check that the installation worked as expected.

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

* *Which file is the playbook? Where do you copy it?*
* 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/
* copy it to /etc/ansible/files/filebeat-config.yml
* You update the /etc/ansible/hosts file to specify what machine to run the playbook on by adding the IP address to the Ansible inventory groups webservers and create a elk group for the ELK server

http:// http://20.62.106.35:5601/app/kibana