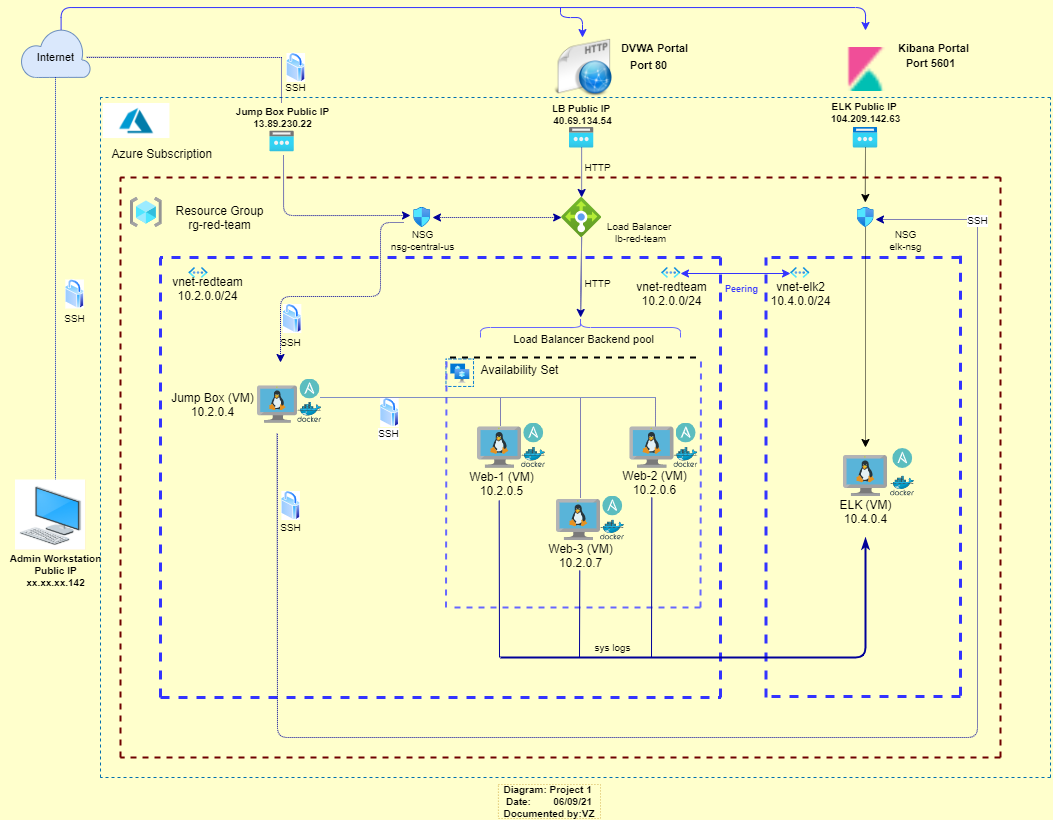
**Automated ELK Stack Deployment**

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

* TODO: Update the path with the name of your diagram: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/images/Project1-Network-Diagram.png>

[](https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/images/Project1-Network-Diagram.png)

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

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

**Jump Box Ansible file configuration details:**

The ansible container should be started the on the Jump box in order to access configuration file.

Configuration files are located under **/etc/ansible** folder:

./hosts

./ansible.cfg

./elk.yml

./pentest.yml

./roles (folder)

./roles/filebeat-playbook.yml

./roles/metricbeat-playbook.yml

./files (folder)

./files/metricbeat-config.yml

./files/filebeat-config.yml

**File Details:**

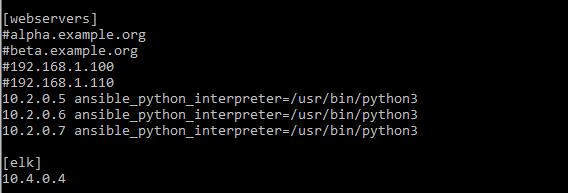
* Ansible **hosts** file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/hosts>

The following [webservers] and [elk] sections were added to the ansible **hosts** file:

**[webservers]**

**[elk]**

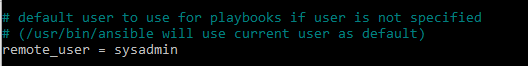
Each section includes web and elk server IP addresses, listed under relevant section:



Adding “ansible\_python\_interpreter=/usr/bin/python3” section next to IP address is required for Ubuntu 18.04 (Web). That option is not required VM running Ubuntu 20.4 (Elk).

* Ansible.cfg file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/ansible.cfg>

In the ansible configuration file the **remote\_user** line was uncommented, and **root** account was replaced with **sysadmin** as listed below:



* Ansible **pentest.yml** playbook file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/pentest.yml>

**Elk Stack playbook and configuration files:**

* Ansible **elk.yml** playbook file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/elk.yml>

View the file for additional details.

**Filebeat Service playbook and configuration files:**

* + **filebeat-config.yml** Filebeat Configuration file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/files/filebeat-config.yml>
  + **filebeat-playbook.yml** Filebeat Playbook file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/roles/filebeat-playbook.yml>

**Metricbeat Service playbook and configuration files:**

* + **metricbeat-config.yml** Metricbeat Configuration file: https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/files/metricbeat-config.yml
  + **metrickbeat-playbook.yml** Metricbeat Playbook file: <https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/ansible/roles/metricbeat-playbook.yml>

**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/traffic** to the network.

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

Load balancer protects from the potential distributed denial-of-service (DDoS) attacks. Jump box prevents all Azure VM's to be exposed by only allowing VM infrastructure access via dedicated static IP address assigned to the jump box, using secured SSH connection from authorized IPs and Public key encryption.

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

* TODO: 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. Ref: <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html>
* TODO: What does Metricbeat record? Metricbeat collects and ships various system and service metrics to a specified output destination. Ref: <https://logz.io/blog/metricbeat-tutorial/>

**The configuration details of each machine may be found in the tables below:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NAME | LOCATION | OS | PRIVATE IP | PUBLIC IP | VIRTUAL NETWORK |
| vm-elk-server | East US 2 | Ubuntu 20.04 | 10.4.0.4 | 104.209.142.63 | vnet-elk2 |
| vm-jump-box-provisioner | Central US | Ubuntu 18.04 | 10.2.0.4 | 13.89.230.22 | vnet-redteam |
| Web-1 | Central US | Ubuntu 18.04 | 10.2.0.5 | 40.69.134.54 | vnet-redteam |
| Web-2 | Central US | Ubuntu 18.04 | 10.2.0.6 | 40.69.134.54 | vnet-redteam |
| Web-3 | Central US | Ubuntu 18.04 | 10.2.0.7 | 40.69.134.54 | vnet-redteam |

**VM Size and OS:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| NAME | OS | SIZE | vCPU | RAM (GiB) | LOCATION | PRIVATE IP | PUBLIC IP |
| vm-elk-server | Ubuntu 20.04 | Standard\_B2s | 2 | 4 | East US 2 | 10.4.0.4 | 104.209.142.63 |
| vm-jump-box-provisioner | Ubuntu 18.04 | Standard\_B1s | 1 | 1 | Central US | 10.2.0.4 | 13.89.230.22 |
| Web-1 | Ubuntu 18.04 | Standard\_B1ms | 1 | 2 | Central US | 10.2.0.5 | 40.69.134.54 |
| Web-2 | Ubuntu 18.04 | Standard\_B1ms | 1 | 2 | Central US | 10.2.0.6 | 40.69.134.54 |
| Web-3 | Ubuntu 18.04 | Standard\_B1ms | 1 | 2 | Central US | 10.2.0.7 | 40.69.134.54 |

**Custom Access Policies**

* The following VM Web Servers on the internal network are not directly exposed to the public Internet:
  + Web-1
  + Web-2
  + Web-3

They are assigned to load balancer backend pool. The Web application installed on these servers can be accessed via public IP address 40.69.134.54 that is assigned to the load balancer, on port 80.

* Only the **vm-jump-box-provisioner** virtual machine can accept connections from the Internet. Access to this machine is only allowed via SSH protocol on port 22, from the following IP address: xxx.xxx.xxx.142 (the actual public IP address of the admin workstation is masked for security purpose).
* Machines within the network can only be accessed by **vm-jump-box-provisioner** (10.2.0.4).
* TODO: Which machine did you allow to access your ELK VM? What was its IP address?\_

ELK VM console can only be accessed from Jump Box VM 10.2.0.4 on port 22 via SSH protocol. Externally facing ELK portal can be accessed by public IP address of the Admin Computer xxx.xxx.xxx.142

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Vnet | Network Security Group | Inbound Rules | Port(s) | Action | Source(s) | Destination |
| vnet-redteam | nsg-central-us | Allow-SSH | 22 | Allow | Admin WS Public IP, 10.2.0.4 | Virtual Network (10.2.0.0./24) |
| vnet-redteam | nsg-central-us | Port-80 | 80 | Allow | Admin WS Public IP, 10.2.0.4 | Virtual Network (10.2.0.0./24) |
| vnet-elk2 | elk-nsg | Allow-SSH | 22 | Allow | 10.2.0.4 | 10.4.0.4 |
| vnet-elk2 | elk-nsg | Port\_5601 | 5601, 5044, 9200, 9300 | Allow | Admin WS Public IP | Virtual Network (10.2.0.0./24) |

Network traffic that does not meet above polices will be denied.

**Elk Configuration**

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

* TODO: What is the main advantage of automating configuration with Ansible?\_

Ansible is an open-source automation engine that uses code, where you can describe configuration, deployment, provisioning that can used for process automation. It uses YAML language playbook to describe automation task.

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.\_
* Add your new ELK ip address to the Ansible hosts file.
* Create a new Ansible playbook to use for your new ELK virtual machine. The elk.yml playbook file includes the following tasks:
* to use more memory:

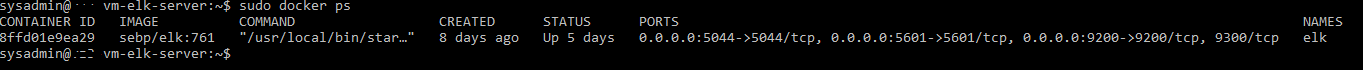
name: vm.max\_map\_count

value: '262144'

* Install the following services: docker.io, python3-pip, docker
* Configure the following published ports: 5601, 9200, 5044
* Run the ansible playbook to launch the container using the following command: ansible-playbook elk.yml
* Navigate to <http://104.209.142.63:5601/app/kibana> URL to verify that Elk stack server portal can be loaded.

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

<https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/images/elk-docker-ps.png>

[](https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/images/elk-docker-ps.png)

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* TODO: List the IP addresses of the machines you are monitoring:

10.2.0.5

10.2.0.6

10.2.0.7

We have installed the following Beats on these machines:

* TODO: Specify which Beats you successfully installed:
  + Filebeat module
  + Metricbeat module

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

* TODO: In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.
  + Filebeat module monitors, collects and parse various predefined log files and forwards them to Logstash or Elasticsearch.
  + Metricbeat module collect metrics from OS and services and forwards them to Logstash or Elasticsearch.

**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?\_

The **filebeat-playbook.yml** and **metricbeat-playbook.yml** are the playbook files. The files should be copied into **/etc/ansible/roles** folder of the container running on the Jump Box.

The **filebeat-config.yml** and **metricbeat-config.yml** configuration filesshould be placed into **/etc/ansible/files** folder

- \_Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

First, we modify **hosts** file of the ansible container on the Jump Box provisioner to include special sections [webservers] and [elk] with IP addresses of the target machine.

Then in the filebeat-playbook.yml, or metricbeat-playbook.yml we identify target machines in the **hosts** statement. For example:

- name: Config elk VM with Docker

hosts: **elk**

- \_Which URL do you navigate to in order to check that the ELK server is running?

Navigate to <http://104.209.142.63:5601/app/kibana> URL to verify that Elk stack server portal can be loaded

[Graphical user interface

Description automatically generated with medium confidence](https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/images/Kibana-dashboard.png)

<https://github.com/vz-cyber/Cyber-Security-Project-1/blob/main/images/Kibana-dashboard.png>

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

|  |  |
| --- | --- |
| Command | Description |
| ansible webservers -m ping | to verify that group of servers are accessible |
| sudo docker container ls -a | to list docker containers |
| sudo docker container start <container name> | to start the container |
| sudo docker ps | to validate if container is running. The uptime will be indicated under STATUS column |
| sudo docker container attach <container name> | to log in to the container |