**ELK Stack Deployment**

**Timeline

Description automatically generated**

These following files have been used to generate an ELK Stack Deployment. These files can be used to recreate the Network Diagram (shown in the Network Diagram above) or used to install specific portions of the network diagram.

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansible.cfg.TXT

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansibleinstall-elk.yml.TXT

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/metricbeat-playbook.TXT

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/filebeat-playbook.yml.TXT

**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.

* The load balancer was used to ensure that the application would be available.
* Integrating the ELK server allowed users to monitor the VMs for changes to files and logs.
* The Filebeat was used for data collection within the file system
* The Metricbeat was used to analyze the operational state of the computer machines.

The configuration details of each machine may be found below:

| **Name** | **Function** | **IP Address** | **Operating System** |
| --- | --- | --- | --- |
| JumpBox | Gateway | 10.0.0.1 | Linux UBUNTU 18.4 |
| WEB1 | DVWA | 10.0.0.5 | Linux UBUNTU 18.4 |
| WEB2 | DVWA | 10.0.0.7 | Linux UBUNTU 18.4 |
| ELKVM | ELK Stack | 10.2.0.4 | Linux UBUNTU 18.4 |

**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:

Workstation with PERSONAL IP Address through SSH Port 22.

Machines within this network can only be accessed by jump box

* Which machine did you allow to access your ELK VM?
  + Jump Box; IP Address 10.0.0.1

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

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| --- | --- | --- |
| Jump Box | Yes | SSH via Admin's IP |
| WEB1 | No | 10.0.0.5 |
| WEB2 | No | 10.0.0.7 |
| ELK | No | 10.2.0.4 |

**Elk Configuration**

Ansible was used to make the configuration on the ELK machine. No configuration was performed manually, which will decrease the chances of mistakes.

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansible.yml.TXT

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/ansibleinstall-elk.yml.TXT

The following are benefits to using ansible:

* Ansible is relatively inexpensive
* Ansible is simple to set up
* Ansible can easily be used to automate complex task.
* Ansible is good for quickly creating IT infrastructure

The playbook implements the following tasks:

Install Docker, which intern facilitates installation of containers Install Python-pip Install Docker Python Module Increases Virtual Memory Downloads and launches a docker ELK container with the ports 5601, 9200, 5044

[Docker PS](https://github.com/liltran615/Azure-Project-1/blob/main/Pictures/sudo%20docker%20ps.png)

**Target Machines & Beats**

The following machines were monitored by the ELK Server:

* Web-1: 10.0.0.5
* Web-2: 10.0.0.7

The following File Beats were installed on the machine:

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/filebeat-playbook.yml.TXT

[Graphical user interface, text, application, chat or text message

Description automatically generated](https://github.com/liltran615/Azure-Project-1/blob/main/Pictures/file%20beat%20status.png)

https://github.com/marklollis1/Mark\_Lollis\_Repo/blob/main/Ansible%20YAML/metricbeat-playbook.TXT

[Graphical user interface, text, application, chat or text message

Description automatically generated](https://github.com/liltran615/Azure-Project-1/blob/main/Pictures/metric%20beat%20status.png)

This allows us to collect the following information:

* Log files from applications such as Microsoft Azure and MySQL
* CPU, VM and Network statistics

**Using the Playbook**

The following are steps needed to use the playbook:

* Copy the configuration file to the ansible container.
* Update the configuration file to include hosts: IP address of the ELK server ["10.2.0.4"]
* Run the playbook and navigate to http://(vm ip):5601/app/kibana. This will allow you to make sure the installation worked correctly.