**Automated ELK Stack Deployment**

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

Diagram

Description automatically generated

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

* [Filebeat Playbook](https://docs.google.com/document/d/1S2LgjGciTTl0bK_UiOZvN9lrxe_xjGEiNXbkhwpDAl0/edit?usp=sharing)

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 Vulnerable Web Application.

Load balancing ensures that the application will be highly reliable, in addition to restricting access to the network.

* Load Balancers protect against DoS attacks. The advantage of the jump box is that it restricts access to one administrator. Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the actual machines and system logs.
* Filebeat helps generate and organize log files to send to Logstash and Elasticsearch. Specifically, it logs information about the file system, including which files have changed and when.
* Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics from the operating system and from services running on the server. Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or 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 |

| Web-1 | DVWA Containers | 10.0.0.5 | Linux |

| Web-2 | DVWA Containers | 10.0.0.6 | Linux |

| Web-3 | DVWA Containers | 10.0.0.7 | Linux |

| ELK | Configuration VM | 10.1.0.8 | Linux |

| Applications Used | Versions |

|-------------------|--------------------------------------|

| Docker | version 19.03.6 |

| filebeat | version 7.4.0 (amd64), flibbeat 7.4.0 |

| metricbeat | version 7.4.0 (amd64), flibbeat 7.4.0 |

**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:

* 76.171.145.84 - my personal machine.

Machines within the network can only be accessed by accessing the DVWA container in the Jump Box VM.

* The only machines that can access the ELK server are 76.171.145.84 - my personal machine, and the Jump Box VM at IP 10.0.0.7 through a peering connection.

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

| Name | Publicly Accessible | Allowed IP Address |

|----------------------|---------------------|-------------------------|

| Jump-Box-Provisioner | Yes | 10.0.0.7, 76.171.145.84 |

| Web-1 | No | 10.0.0.1-254 |

| Web-2 | No | 10.0.0.1-254 |

| Web-3 | No | 10.0.0.1-254 |

| ELK | No | 10.0.0.7, 76.171.145.84 |

**ELK Configuration**

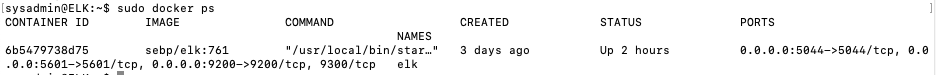
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

* You don’t need to install any other software or firewall ports on the client systems you want to automate. You also don’t have to set up a separate management structure.

The playbook implements the following tasks:

* Install Docker
* Download Image
* Configure container
* Create playbook to install container with docker and Filebeat and Metricbeat.
* Run playbook to launch the container

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

[](https://github.com/criscollazos/cybersecurity-project-1/blob/master/images/sudo_docker_elk_server.png)

**Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* 10.0.0.5 - Web-1
* 10.0.0.6 - Web-2
* 10.0.0.7 - Web-3

We have installed the following Beats on these machines:

* Filebeat
* Metricbeat

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

* **Filebeat** monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing. When Filebeat starts logging, it will represent data such as system log events in a dashboard: [Graphical user interface, text, application, email

  Description automatically generated](https://github.com/criscollazos/cybersecurity-project-1/blob/master/images/kibana_1.png) [Text, letter

  Description automatically generated](https://github.com/criscollazos/cybersecurity-project-1/blob/master/images/kibana_2.png)
* **Metricbeat** periodically collect metrics from the operating system and from services running on the server. Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash. Metricbeat will display information such as container CPU usage as follows: [Graphical user interface

  Description automatically generated with medium confidence](https://github.com/criscollazos/cybersecurity-project-1/blob/master/images/Kibana_3.png) [Graphical user interface, text, application

  Description automatically generated with medium confidence](https://github.com/criscollazos/cybersecurity-project-1/blob/master/images/kibana_4.png)

**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:

* Go to /etc/ansible/files and use the curl command to add the config file:

curl https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/files/filebeat-config.yml

* Copy the filebeat-playbook.yml file to /etc/ansible/roles.
* Update the filebeat-config.yml file to include the ELK server private IP in lines 1106 and 1806.
* Run the filebeat-playbook.yml playbook, and navigate to the Kibana page at [ELK public IP]/app/Kibana to check that the installation worked as expected.