## Automated ELK Stack Deployment

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

A picture containing 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 configuration file may be used to install only certain pieces of it, such as Filebeat.

### 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 secure, in addition to restricting access to the network.

* Load balancers add resiliency by rerouting live traffic from one server to another if a server falls prey to a DDoS attack or otherwise becomes unavailable.
* A Jump Box Provisioner is also important as it prevents Azure VMs from being exposed via a public IP Address. This allows us to do monitoring and logging on a single box. We can also restrict the IP addresses able to communicate with the Jump Box, as we've done here.

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

* Filebeat collects data about the file system.
* Metricbeat collects machine metrics such as uptime.

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-wb1 | Azure vm | 10.0.0.5 | linix |
| DVWA-wb2 | Azure vm | 10.0.0.6 | linix |
| Elk-server | Analytics platform | 10.1.0.4 | linix |

### Access Policies

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

Only the jump box provisioner machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

Machines within the network can only be accessed by home ip address.

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

|  |  |  |
| --- | --- | --- |
| Name | Publicly | Allowed ip addresses |
| Jump box | yes | 97.93.xx.xxx |
| DVWA-wb1 | no | 10.0.0.5 |
| DVWA-wb2 | no | 10.0.0.6 |

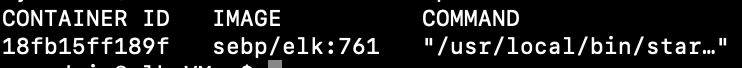
### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because.it allows for setup in minute using openSSH without installing anything on the server also makes life dramatically easier.

The playbook implements the following tasks:

* Install Docker.io
* Install Python-pip
* Increase Virtual Memory
* Download and Launch ELK Docker Container (image sebp/elk)
* Published ports 5044, 5601 and 9200 were made available

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



### Target Machines & Beats

This ELK server is configured to monitor the following machines:

* DVWA-wb1 10.0.0.8
* DVWA-wb2 10.0.0.10

We have installed the following Beats on these machines:

* Metricbeat
* Filebeat

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

* Filebeat will be used to collect log files from very specific files such as Apache, Azure tools and web servers.
* Metericbeat will be used to monitor VM stats, per CPU core stats, per filesystem stats, memory stats and network stats.

### 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 filebeat-config file to Elk VM .

- Update the hosts file to include webservers 10.0.0.5 – 10.0.0.6 ,10.1.0.4

- Run the playbook, and navigate to ( your ip address):5601 from your browser to check that the installation worked as expected.

* Open your ELK server homepage
* Click on Add Log Data.
* Click on the DEB tab under Getting Started to view the correct Linux Filebeat installation instructions.
* Choose System Logs.
* Copy the filebeat-playbook.yml file to /etc/ansible/roles

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated with medium confidence