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

* *TODO: Enter the playbook file.*

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 inbound access to the network.

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

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

* *TODO: What does Filebeat watch for? Change to file changes on the machine.*
* *TODO: What does Metricbeat record? Collect metrics from the O/S and from services running on the server.*

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 | 10.0.10.4 | Linux |
| Web-1 | Webserver | 10.0.10.5 | Linux |
| Web-2 | Webserver | 10.0.10.6 | Linux |
| ELK VM | Monitoring | 10.1.0.4 | Linux |

### 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:

* *TODO: Add whitelisted IP addresses 5061 Kibana Port*

Machines within the network can only be accessed by Jump-box Provisioner.

* *TODO: Which machine did you allow to access your ELK VM? What was its IP address?*
* *MY IP address 119.12.214.107*

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

|  |  |  |
| --- | --- | --- |
| Name | Publicly Accessible | Allowed IP Addresses |
| Jump Box | Yes | 52.147.34.245 |
| Web-1 | No | 10.1.0.4 |
| Web-2 | No | 10.1.0.4 |
| ELK-VM | No | 10.1.0.4 |

### Elk Configuration

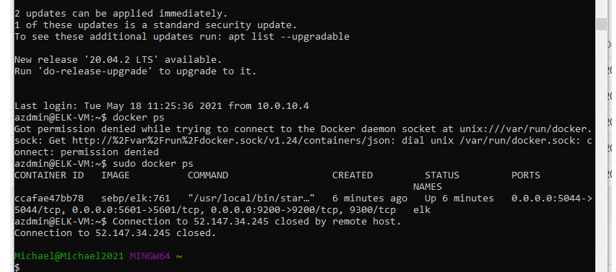
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

* *TODO: What is the main advantage of automating configuration with Ansible?*
* Very easy to use and setup. (No special coding required to create Ansible’s playbooks
* Flexible and you can organise, customize the entire application environment no matter where it is deployed.
* Agentless you do not require to install any other software or firewall ports on the client systems you want to automate. Also do not required to set up a separate management structure.
* Efficient you do not need to install any extra software, therefore more space for application resources on your server.
* And last its free, Ansible is an open-source tool.

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.*
* Step1: Install docker.io,
* Step2 Install pip3,
* Step3 Install docker python module,
* Step4 Download and launch a docker.

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:

* *TODO: List the IP addresses of the machines you are monitoring*
* *Web-1 10.0.1.5* & *Web-2 10.0.1.6*

We have installed the following Beats on these machines:

* *TODO: Specify which Beats you successfully installed “Filebeat & Metricbeat”*

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: Collect the changes done

Graphical user interface

Description automatically generated

* Metricbeat: Collect machine metrics, statistics, such as uptime.

Graphical user interface, application

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 playbook file to Ansible.
* Update the hosts file to include Webserver and Elk, the following host were modify.

Graphical user interface, text

Description automatically generated

* Run the playbook and navigate to Kibana to check that the installation worked as expected.

Graphical user interface, text, application, email

Description automatically generated

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

* *Which file is the playbook? Where do you copy it? “/etc/ansible/file/filebeat-configration.yml”*
* *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?*

You need to edit the host file “etc/ansible/hosts file to add webserver/elkserver ip address

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

<http://20.36.44.120:5601/app/kibana#/home> (Of course using the Public IP of the Azure)

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

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

*curl https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e744c54513616966affb5e9d96f5e12f73/metricbeat > /etc/ansible/files/metricbeat-config.yml*