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

* **Filebeat-playbook.yml**

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 **efficient**, in addition to restricting **traffic** to the network.

* *It protects availability. Jump-Box provides secure access to web servers .: 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 **data** and system **logs**.

* *Filebeat is for forwarding and centralizing log data, it monitors log files or specified locations: What does Filebeat watch for?*
* *Metricbeat helps you monitor your servers by collections metrics from the system and services running on the server: What does Metricbeat record?*

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 | 10.0.0.1 | Linux |
| **Web1** | **Web server** | **10.0.0.8** | **Linux** |
| **Web2** | **Web server** | **10.0.0.7** | **Linux** |
| **Elk-Net** | **Elk-Net** | **10.1.0.4** | **Linux** |

### 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:

* *My Ip* **24.255.213.180***.*

Machines within the network can only be accessed by the jumpbox.

* *Which machine did you allow to access your ELK VM? What was its IP address?****Jump-box* 52.152.141.95**

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| Jump Box | Yes/No | 10.0.0.1 10.0.0.2 |
| **Jump-Box** | **No** | **52.152.141.95** |
|  |  |  |

### Elk Configuration

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

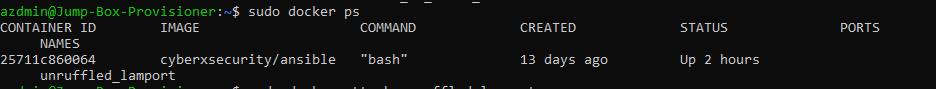
* *What is the main advantage of automating configuration with Ansible?****It allows us to run commands on several machines automatically instead of doing them one by one on each machine:***

The playbook implements the following tasks:

* *In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.*

1. **Install docker**
2. **Create and start container**
3. **Install required program using ansible playbook**
4. **Install filebeat and metricbeat**
5. **Open kibana to upload data**

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:

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

* **Web1 10.0.0.8**
* **Web2 10.0.0.7**

We have installed the following Beats on these machines:

* **Filebeat and Metricbeat: Specify which Beats you successfully installed**

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

* **Filebeat- collets system logs. E.g. error codes, file type scatter**
* **Metricbeat- monitors server. E.g. cpu usage and network traffic**
* **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.**

### 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 **public key** file to **VM password**.
* Update the **hosts** file to include… web server IPs and Elk server IPs
* Run the playbook, and navigate to **Kibana** 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?*

1. **Docker.yml**
2. ***ELK.yml***
3. ***Filebeat-playbook.yml /etc/filebeat***
4. ***Mtericbeat-playbook.yml /etc/metricbeat***

* *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?*

1. **You can change machine in the config files**

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

[**http://**](http://elk)**serverip/app/kibana**

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