## Automated ELK Stack Deployment

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

![TODO: Update the path with the name of your diagram](Images/diagram\_filename.png)

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 Cloud security diagram **Cloud security diagram** file may be used to install only certain pieces of it, such as Filebeat.

**Filebeat-playbook.yml**

**Filebeat-configuration.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 **functional**, in addition to restricting **high traffic** to the network.

- \_TODO: What aspect of security do load balancers protect?

* **A load balancer helps prevent network traffic overload and distributes network or application traffic across a number of servers to optimize productivity and maximize uptime.**
* **The off-loading function of a load balancer helps protect organizations against distributed denial-of-service (DDoS) attacks. This is done by redirecting network traffic from one server to another server for example a cloud provider.**

What is the advantage of a jump box?\_

A jump box serves as a secure computer that is connected to before launching any administrative task or used as an origination point to connect to other servers or untrusted environments.

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

What does Filebeat watch for?\_

* **Filebeat is installed as an agent on servers and monitors the log files or locations specified, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.**

What does Metricbeat record?\_

* **Metricbeat helps in the monitoring of servers by recording metrics and statistics and transports them to the output that is specified such as Elasticsearch or Logstash.**

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 Provisioner| Gateway | 10.1.0.4/20.124.192.126 | Linux-Unbuntu LTS 18.04|

| Web-1 |Application Server | 10.1.0.7 | Linux-Unbuntu LTS 18.04|

| Web-2 | Application Server|10.1.0.8 | Linux-Unbuntu LTS 18.04|

| Elk-server | Elk Stack |10.2.0.4/23.100.47.133 | Linux-Unbuntu LTS 18.0|

### Access Policies

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

Only the **JumpBox Provisioner and ELK Stack (kibana)** machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* **My home IP Address**

Machines within the network can only be accessed by JumpBox.

- \_TODO: Which machine did you allow to access your ELK VM?

* **JumpBox Provisioner**

What was its IP address?\_

* **10.1.0.4 (Private)/20.124.192.126 (Public)**

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

| Name | Publicly Accessible | Allowed IP Addresses |

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

| Jump Box | Yes | Home IP Address |

| Web-1 | No |10.1.0.7 |

| Web-2 | No | 10.1.0.8 |

| elk-stack | No | Home IP Address |

### 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?

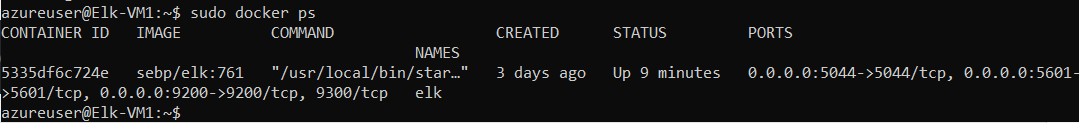
* It allows for a consistent and predictable configuration.
* It is very simple to set up and use and no special coding skills are required to use Ansible's playbooks.
* With an automated setup, the ELK stack can be created and configured very quickly and with minimal or no errors which may be result from human error from manual configuration.

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.\_

* SSH into the Jump-Box-Provisioner (ssh azureuser@JumpBoxpublicIP)
* Open/Start/Attach to the ansible docker (sudo docker start frosty\_newton)/(sudo docker attach frosty\_newton)
* Opened /etc/ansible/roles directory and created the ELK playbook (Elk\_Playbook.yml)
* Ran the Elk\_Playbook.yml in that same directory (ansible-playbook Elk\_Playbook.yml)
* Lastly, I SSH into the ELK-VM (ssh azureuser@elkserverprivateIP) to verify the server is up and running.

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:

* Web-1: 10.1.0.7
* Web-2: 10.1.0.8

We have installed the following Beats on these machines:

* Filebeats
* Metricbeat

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

* Filebeat collects and forwards system logs from the Web VMs to the ELK Stack in an easy to read format.
* Metricbeat reports system metrics about the Web VMs to the ELK stack VM.

### 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:

* Filebeat/Metricbeat
* Copy the filebeat-configuration.yml/metricbeat-configuration.yml file to /etc/ansible/roles/.
* Update the filebeat-configuration.yml/metricbeat configuration files to include the ELK private IP .
* Run the playbook, and navigate to ELK VM Public IP (http://<elk public IP>:5601/app/kibana) to check that the installation worked as expected.

Answer the following questions to fill in the blanks:\_

Which file is the playbook?

* filebeat-playbook.yml

Where do you copy it?

* /etc/ansible/role

Which file do you update to make Ansible run the playbook on a specific machine?

* /etc/ansible/hosts file (IP of the Virtual Machines).

How do I specify which machine to install the ELK server on versus which to install Filebeat on?\_

* Two separate groups in the etc/ansible/hosts file. One of the groups will be webservers which has the IPs of the VMs that I will install Filebeat to. The other group is named elkservers which will have the IP of the VM I will install ELK to.

Which URL do you navigate to in order to check that the ELK server is running?

* http://<elk public IP>:5601/app/kibana

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