

## Automated ELK Stack Deployment

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

### [Red-Team Network Diagram](#)

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 Project 1 Red Team Network Diagram file may be used to install only certain pieces of it, such as Filebeat.

*install-elk.yml*

*filebeat-playbook.yml*

*filebeat-config.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.

**What aspect of security do load balancers protect?** *It helps prevent overloading servers as well as optimizes productivity and maximizing uptime. It is also a resilient system by rerouting traffic from one server to another which helps mitigate DoS attacks.*

### **What is the advantage of a jump box?**

*It offers security for admins. It's a simple system that can run as a single operating system that can connect to two networks.*

*Jumpbox sits in front of other machines that are not exposed to the public internet. It controls access to the other machines by allowing connections from specific IP addresses. This decreases chances of hackers and malware.*

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?** *It monitors the log files or locations that users specify, it collects log events and forwards them to either a Elasticsearch or Logstash for indexing.*

**What does Metricbeat record?** *It records metrics/statics such CPU, hosts, inbound/outbound traffic then transports them to an output the user specifies through Elasticsearch/Logstash.*

The configuration details of each machine may be found below.

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.0.0.4/40.117.150.166	Linux
Web-1	DVWA/Server	10.0.0.5/20.102.127.226	Linux
Web-2	DVWA/Server	10.0.0.7/20.102.127.226	Linux
Web-3 Elk	ELK	10.1.0.4/40.83.192.102	Linux

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: 172.17.0.1?**

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

**Which machine did you allow to access your ELK VM?** *Jump-Box-Provisioner*

**What was its IP address?** *10.0.0.4 Private*

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

Name	Publicly Accessible	Allowed IP Addresses
Jump-Box	Yes	40.117.150.166/99.167.227.23
Web-1	No	10.0.0.4
Web-2	No	10.0.0.4
Web-3 Elk	No	10.0.0.4

## 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?

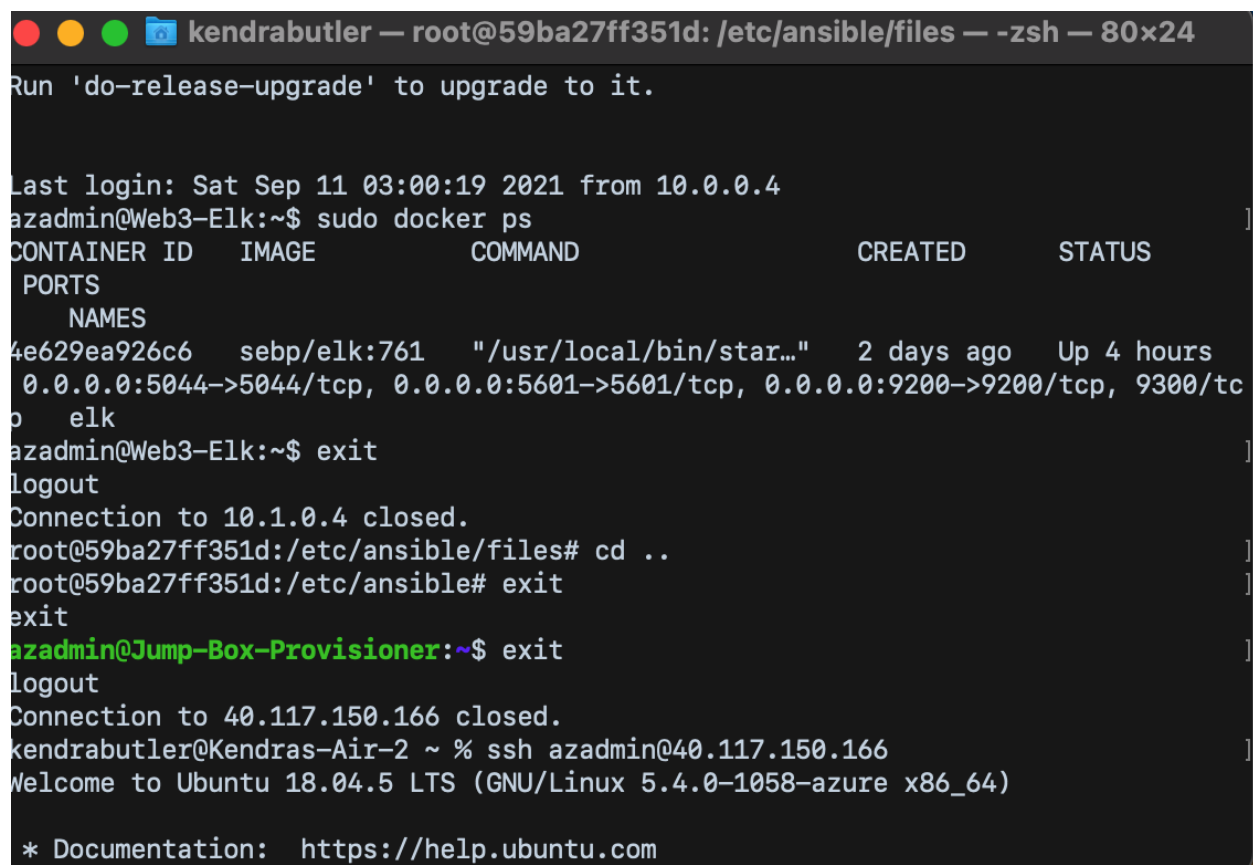
*It allows IT administrators to automate away the work from their daily tasks. Not to mention the YAML playbooks are an effective way to configure and automate. Ansible is open-source tool*

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 Jump-Box-Provisioner SSH azadmin@40.117.140.166
- List Containers, Start, and Attach to eloquent\_morse
- Cd /etc/ansible/roles directory and created playbooks
- Ran the ansible-playbook in the same directory
- SSH into ELK-VM to verify server is up and running

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



```
kendrabutler — root@59ba27ff351d: /etc/ansible/files — -zsh — 80x24

Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Sep 11 03:00:19 2021 from 10.0.0.4
azadmin@Web3-Elk:~$ sudo docker ps
CONTAINER ID   IMAGE             COMMAND                  CREATED        STATUS
PORTS
NAMES
4e629ea926c6   sebp/elk:761      "/usr/local/bin/star...  2 days ago    Up 4 hours
0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tc
o   elk
azadmin@Web3-Elk:~$ exit
logout
Connection to 10.1.0.4 closed.
root@59ba27ff351d:/etc/ansible/files# cd ..
root@59ba27ff351d:/etc/ansible# exit
exit
azadmin@Jump-Box-Provisioner:~$ exit
logout
Connection to 40.117.150.166 closed.
kendrabutler@Kendras-Air-2 ~ % ssh azadmin@40.117.150.166
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1058-azure x86_64)

* Documentation:  https://help.ubuntu.com
```

## Target Machines & Beats

This ELK server is configured to monitor the following machines:

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

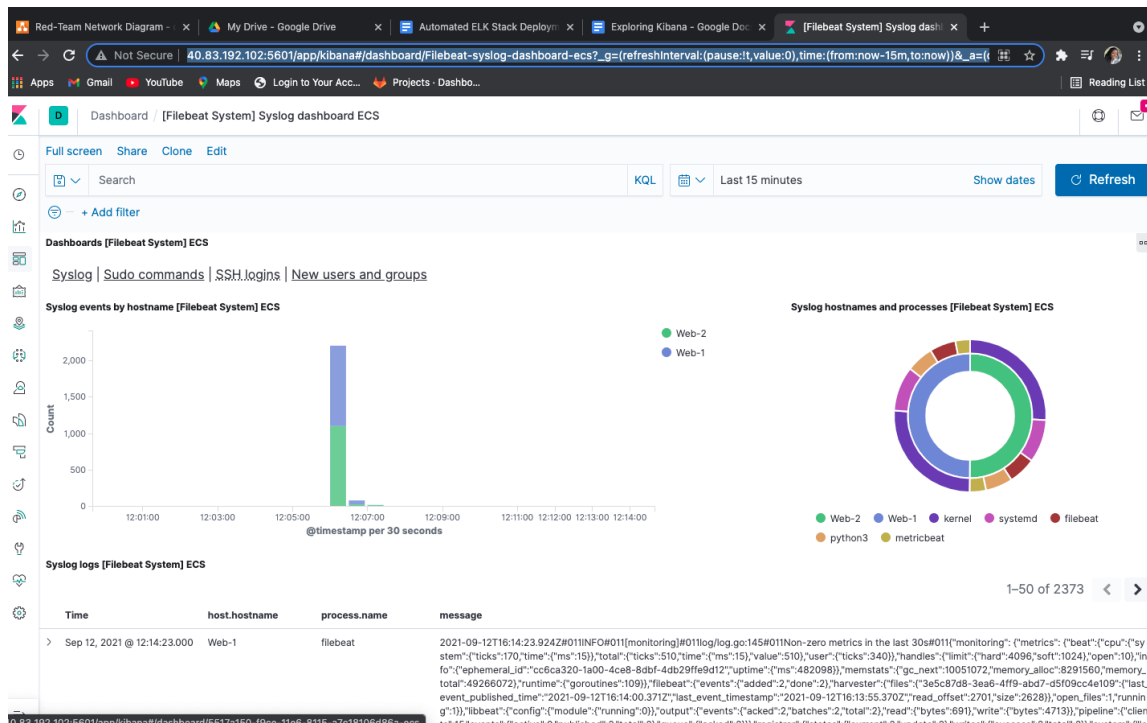
*Private IP addresses of Web1- 10.0.0.5 and Web2- 10.0.0.7*

We have installed the following Beats on these machines:

### Specify which Beats you successfully installed

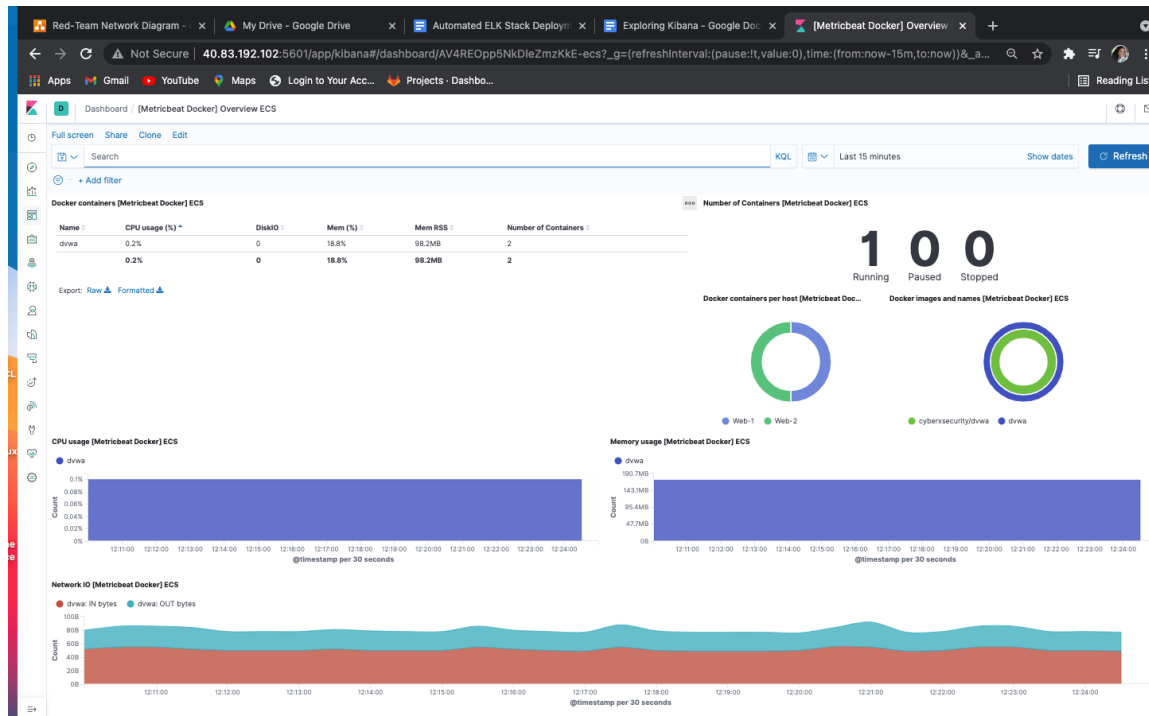
Filebeat system

<http://40.83.192.102:5601/app/kibana>



Metricbeat Docker

<http://40.83.192.102:5601/app/kibana>



These Beats allow us to collect the following information from each machine: 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 is used to collect log files from specific files on remote machines. Files that can be generated by Apache, Microsoft Azure tools, the Nginx web server and MySQL.*

## 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

- **Copy the filebeat-configuration file to /etc/ansible/roles/files.**
- **Update the filebeat-configuration file to include the EIK Private IP in lines #1106 and #1806**
- **Run the playbook, and navigate to to check that the <http://40.83.192.102:5601/app/kibana> installation worked as expected.**

### Metricbeat

- **Copy the metricbeat-configuration.yml file to /etc/ansible/roles/files**

- **Update the metricbeat-configuration file to include the Elk private IP in lines 62 and 96.**
- **Run the playbook and navigate to <http://40.83.192.102:5601/app/kibana>**

Answer the following questions to fill in the blanks:

**\* Which file is the playbook?** *Filebeat-playbook.yml*

**\*Where do you copy it?** */etc/ansible/roles*

**\* Which file do you update to make Ansible run the playbook on a specific machine?**  
*/etc/ansible/hosts file (IP of Virtual Machines).*

**How do I specify which machine to install the ELK server on versus which to install Filebeat on?** *Separate the groups in the etc/ansible/hosts file. One of the groups will be webserver which have the ips of the VMs that will install Filebeat. The other group name is elk which will have the IP of the VM that will install ELK to.*

**\* Which URL do you navigate to in order to check that the ELK server is running?**  
*http://13.64.169.101:5601/app/kibana*

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

*Sudo apt-get update*  
*Sudo docker install*  
*Sudo docker run ti*  
*Sudo docker start container name*  
*Sudo docker ps*  
*Sudo ansible-playbook (.yml file to run)*  
*Systemctl status docker*  
*Ssh-keygen*

**\*\*\***I didn't put them in order, just listed as many as I could.