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

-Install-elk.yml:

---

- name: Configure Elk VM with Docker

hosts: elk

remote\_user: azadmin

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker.io

state: present

# Use apt module

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

# Use command module

- name: Increase virtual memory

command: sysctl -w vm.max\_map\_count=262144

# Use sysctl module

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: '262144'

state: present

reload: yes

# Use docker\_container module

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

# Please list the ports that ELK runs on

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

# Use systemd module

- name: Enable service docker on boot

systemd:

name: docker

enabled: yes

- name: installing and launching filebeat

hosts: webservers

become: yes

tasks:

- name: download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

- name: install filebeat deb

command: dpkg -i filebeat-7.4.0-amd64.deb

- name: drop in filebeat.yml

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

- name: enable and configure system module

command: filebeat modules enable system

- name: setup filebeat

command: filebeat setup

- name: start filebeat service

command: service filebeat start

- name: enable service filebeat on boot

systemd:

name: filebeat

enabled: yes

This document contains the following details:

- Description of the Topologu

- 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.

What aspect of security do load balancers protect?

* The load balancer distributes traffic from clients across multiple machines/ servers without the clients having to having to know how many servers are in use or how the configured. The is because the load balancer is in between the clients and the servers allowing it to enhance the user experience by providing additional security performance and stability.

What is the advantage of a jump box?

the jump box is that is gives access to the user from a single node that can be easily secured and monitored.

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

What does Filebeat watch for?

File beat watch for log files and location that have been specified, collects the log event data.

What does Metricbeat record?

Metric beat compares and track the performance metric and stats of the system.

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 |
| web-1 | Web server 1 | 10.0.0.6 | Linux |
| web-2 | Web server 2 | 10.0.0.7 | Linux |
| web-3 | Web server 3 | 10.0.0.8 | linux |
| Elk -server | 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 machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* 5601 port

Machines within the network can only be accessed by jump box provisioner .

Which machine did you allow to access your ELK VM? My machine via ip Address

101.190.211.12

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

|  |  |  |
| --- | --- | --- |
| Name | Publicly accessible | Allowed ip address |
| Jump box | Yes | 101.190.211.12 |
| Web-1 | No | 10.0.0.4 |
| Web-2 | No | 10.0.0.4 |
| Web-3 | No | 10.0.0.4 |
| 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?

* Simple : no coding skills are necessary to use ansible playbooks
* Powerful: allows high level IT workflows
* Efficient: no extra software is needed to operate ansible so there is more space for application and resources on the server
* Open source: ansible is open source so it is free
* Flexible: Customization of ansible playbooks are very flexing tailoring to the need of the server and can be implemented on the entirety of the application

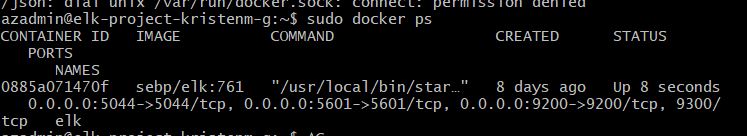
The playbook implements the following tasks:

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

* Install docker.io
* Install pip3
* Install docker python module
* Increase virtual memory
* Download and launch 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:

|  |  |
| --- | --- |
| Name | Ip Addresses |
| Web-1 | 10.0.0.6 |
| Web-2 | 10.0.0.7 |
| Web-3 | 10.0.0.8 |

We have installed the following Beats on these machines:

* Microbeats

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

* Metric beat- collects metrics data such as location and uptime.
* File beat- collects data about file logs and log events

### 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 ansible playbook file to ansible control node.
* Update the hosts file to include:
  + Webservers
  + elk machine
  + edit the hosts file to run on specific machines to install filebeat on the elk server
* Run the playbook and navigate to Kibana (http://[hosts ip]/app/Kibana#/home) to check that the installation worked