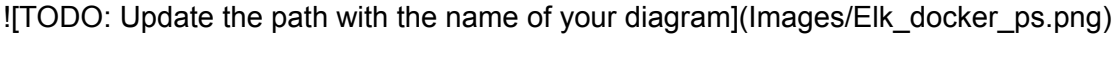
Automated ELK Stack Deployment

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.

- _TODO: Enter the playbook file._

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 access to the network.

Load balancing will protect from the denial of service attack as it will help to divert the traffic and to distribute the load. Moreover, It helps with the intrusion prevention by restricting access to the servers holding the application.

A jump box provides a controlled access to the servers/VMs holding the applications and helps with the management of these hosts.

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

What does Filebeat watch for?

Filebeat watches are for changs in the files in the locations that we specify or the log files. Then collects and send the date to lostash/elasticsearch.

What does Metricbeat record?

Metricbeat collets the metric data from the services and the operating system and sends it to logstash/elasticsearch.

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	Publicly Accessible	Allowed IP Addresses
Jump Box	Yes	10.0.0.1 10.0.0.2	Personal
Load Balancer	Yes	Open
Web 1	No	10.0.0.5
Web 2	NO	10.0.0.6
ELK Server	Yes	Personal

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because services running can be limited, system installation and update can be streamlined and processes become more replicable.

The playbook implements the following tasks:

- Install s docker.io, pip3, and the docker module

```
# Use apt module
  - name: Install docker.io
    apt:
      update_cache: yes
      name: docker.io
      state: present

# Use apt module
  - name: Install pip3
    apt:
      force_apt_get: yes
      name: python3-pip
      state: present
```

```
  # Use pip module
    - name: Install Docker python module
      pip:
        name: docker
        state: present
```

- Increase the virtual memory

```
# Use command module
    - name: Increase virtual memory
      command: sysctl -w vm.max_map_count=262144
```

- Uses sysctl module

```
      # Use sysctl module
        - name: Use more memory
          sysctl:
            name: vm.max_map_count
            value: "262144"
            state: present
            reload: yes
```

- Downloads and launches the docker container for ELK server

```
# 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
        published_ports:
          - 5601:5601
          - 9200:9200
          - 5044:5044
```

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 - 10.0.0.5
Web 2 - 10.0.0.6

We have installed the following Beats on these machines:
- Filebeat
- Metric Beat
-

These Beats allow us to collect the following information from each machine:
- Filebeat is a log data shipper for local files. Installed as an agent on your servers, Filebeat monitors the log directories or specific log files, tails the files, and forwards them either to Elasticsearch or Logstash for indexing. An examle of such are the logs produced from the MySQL database supporting our application.
- Metricbeat collects metrics and statistics on the system. An example of such is cpu usage, which can be used to monitor the system health.

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 configuration file from your Ansible container to your Web VM's.
- Update the /etc/ansible/hosts file to include the IP address of the Elk Server VM and web servers.
- Run the playbook, and navigate to http://[Elk_VM_Public_IP]:5601/app/kibana to check that the installation worked as expected.

- Which file is the playbook? The Filebeat-configuration
- Where do you copy it? copy /etc/ansible/files/filebeat-config.yml to /etc/filebeat/filebeat.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?

update filebeat-config.yml -- specify which machine to install by updating the host files with ip addresses of web/elk servers and selecting which group to run on in ansible

- Which URL do you navigate to in order to check that the ELK server is running?
  http://[your.ELK-VM.External.IP]:5601/app/kibana

Filebeats

```
- name: Installing and Launch Filebeat
  hosts: webservers
  become: yes
  tasks:
    # Use command module
  - name: Download filebeat .deb file
    command: curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

    # Use command module
  - name: Install filebeat .deb
    command: dpkg -i filebeat-7.4.0-amd64.deb

    # Use copy module
  - name: Drop in filebeat.yml
    copy:
      src: /etc/ansible/files/filebeat-config.yml
      dest: /etc/filebeat/filebeat.yml

    # Use command module
  - name: Enable and Configure System Module
    command: filebeat modules enable system

    # Use command module
  - name: Setup filebeat
    command: filebeat setup

    # Use command module
  - name: Start filebeat service
    command: service filebeat start
```

Metricbeats

```
- name: Install metric beat
  hosts: webservers
  become: true
  tasks:
```

```
    # Use command module
  - name: Download metricbeat
    command: curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.4.0-amd64.deb

    # Use command module
  - name: install metricbeat
    command: dpkg -i metricbeat-7.4.0-amd64.deb

    # Use copy module
  - name: drop in metricbeat config
    copy:
      src: /etc/ansible/files/metricbeat-config.yml
      dest: /etc/metricbeat/metricbeat.yml

    # Use command module
  - name: enable and configure docker module for metric beat
    command: metricbeat modules enable docker

    # Use command module
  - name: setup metric beat
    command: metricbeat setup

    # Use command module
  - name: start metric beat
    command: service metricbeat start
```