## **Automated ELK Stack Deployment**

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

* Enter the playbook file. **This is the first playbook to get things started.**

**---**

**- name: My first playbook**

**hosts: webservers**

**become: true**

**tasks:**

**- name: Install apache httpd (state=present is optional)**

**apt:**

**name: apache2**

**state: present**

**- name: Install docker.io**

**apt:**

**update\_cache: yes**

**name: docker.io**

**state: present**

**- name: Install pip3**

**apt:**

**name: python3-pip**

**state: present**

**- name: Install docker**

**pip:**

**name: docker**

**state: present**

**- name: Install dvwa**

**docker\_container:**

**name: dvwa**

**image: cyberxsecurity/dvwa**

**state: started**

**restart\_policy: always**

**published\_ports: 8080:80**

### **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 **\_resilient\_**, in addition to restricting **\_traffic\_** to the network.

* **What aspect of security do load balancers protect? Load balancers have multiple benefits, one such is the load balancer can request a username/password before granting access to a website to mitigate against unauthorized access.**
* **What is the advantage of a jump box?**

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the **\_logs\_** and system **\_traffiic\_**.

* **What does Filebeat watch for? Filebeat records information about a system, it creates a log of useful information such as if a file or files were changed and when the incident occurred.**
* **What does Metricbeat record?** **Metricbeat is responsible for recording hosts metrics an example being uptime**

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** | **10.0.0.4** | **Linux (Ubuntu 18.04)** |
| **Web-1** | **Web Servers** | **10.0.0.5** | **Linux (Ubuntu 18.04)** |
| **Web-2** | **Web Servers** | **10.0.0.6** | **Linux (Ubuntu 18.04)** |
| **Web-3** | **Web Servers** | **10.0.0.7** | **Linux (Ubuntu 18.04)** |

### 

### **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:

* **The whitelisted IP Address is 24.125.6.250**

Machines within the network can only be accessed by \_**the External Work Station**\_.

* **Which machine did you allow to access your ELK VM? The JumpBox Provisioner has access to the ELK VM.**
* **What was its IP address? 10.0.0.4 or 13.90.156.122**

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
| Jump-Box | Yes | 24.125.6.250 |10.0.0.4 | 13.90.156.122 |
| Web 1 - 3 | No | 10.0.0.4 | 10.0.0.5 | 10.0.0.6 | 10.0.0.7 |
| ELK VM | Yes | 10.0.0.4 | 10.1.0.4 | 52.177.122.201 |

### **Elk Configuration**

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

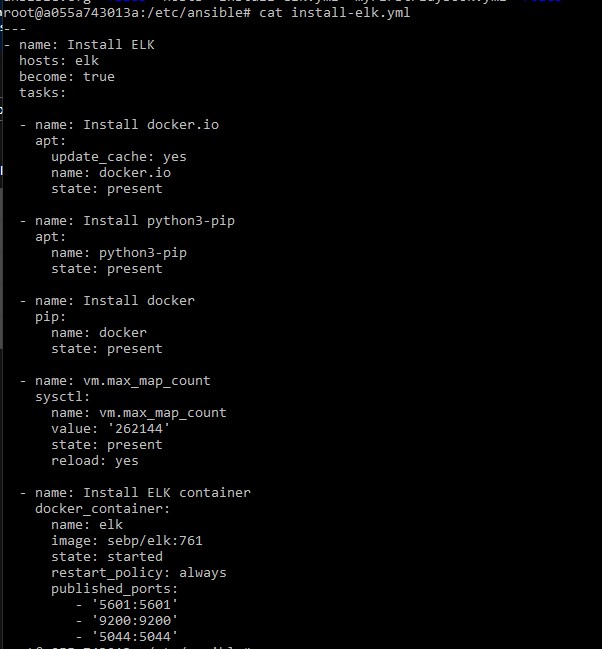
**What is the main advantage of automating configuration with Ansible?**

* **One of the primary advantages for automating with Ansible is that you can push a specific configuration to through hundreds or thousands of computers and the process will remain the same for each and every connection.**

The playbook implements the following tasks:

* **Create a new VM and Increase system memory and the vcpu**
* **Create a yml file**
* **Install docker.io**
* **Install python3**
* **Install docker**
* **Install the elk container and run “ansible-playbook install-elk.yml”**

**Below is a screenshot of how everything should be constructed.**

****

### **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**
* **Web-3: 10.0.0.7**

We have installed the following Beats on these machines:

Specify which Beats you successfully installed

* **Filebeats and Metricbeats were installed on these machines**

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

* **FileBeats: Collects data from the file system: It can aid in locating new additions to recently added files or even inform you if those files have been previously modified.**
* **MetricBeats: Collects metrics about the machine, one primary example being it collects systems and services running on the server. It is really useful information since metricbeats will create an event and inform you of any downtimes/uptimes.**

### **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 \_**playbook.yml\_** file to \_**to roles**\_.
* Update the \_**config.yml**\_ file to include...
* Run the playbook, and navigate to \_the kibana website\_ to check that the installation worked as expected.

TODO: Answer the following questions to fill in the blanks:

* **Which file is the playbook? FileBeat and MetricBeat**
* **Where do you copy it? Under /etc/ansible/roles**
* **Which file do you update to make run the playbook on a specific machine? The Hosts file**
* **How do I specify which machine to install the ELK server on versus which to install Filebeat on? All within the Hosts file. For Web VM 1 - 3 you have to place them under [websevers] and create an independent category for [elk] under all the web servers.**
* **Which URL do you navigate to in order to check that the ELK server is running? In my particular case it would be http://52.177.122.201:5601/app/kibana**

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

**ansible-playbook metricbeat-playbook.yml**

**ansible-playbook filebeat-playbook.yml**

**ansible-playbook install-elk.yml**