## **Automated ELK Stack Deployment**

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

**Note**: The following image link needs to be updated. Replace diagram\_filename.png with the name of your diagram image file.

<https://drive.google.com/file/d/1oxZc93JeMGpbNmax0AS7543aor_13wIB/view>

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 “ansible playbook elk.yml” file may be used to install only certain pieces of it, such as Filebeat.

* *TODO:*

*---*

*- name: Config elk VM with Docker*

*hosts: elk*

*become: True*

*tasks:*

*- name: Set the vm.max\_map\_count to 262144 in sysctl*

*sysctl: name={{ item.key }} value={{ item.value }}*

*with\_items:*

*- { key: "vm.max\_map\_count", value: "262144" }*

*- name: docker.io*

*apt:*

*force\_apt\_get: yes*

*update\_cache: yes*

*name: docker.io*

*state: present*

*- name: Install pip3*

*apt:*

*force\_apt\_get: yes*

*name: python3-pip*

*state: present*

*- name: Install Docker python module*

*pip:*

*name: docker*

*state: present*

*- name: download and launch a docker web container*

*docker\_container:*

*name: elk*

*image: sebp/elk:761*

*state: started*

*restart\_policy: always*

*published\_ports:*

*- 5601:5601*

*- 9200:9200*

*- 5044:5044*

*- name: Enable docker service*

*systemd:*

*name: docker*

*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 \_\_responsive\_\_\_, in addition to restricting traffic to the network.

* *TODO: What aspect of security do load balancers protect? The off-loading function of a* ***load balancer*** *defends an organization against distributed denial-of-service (DDoS) attacks. It* ***does*** *this by shifting attack traffic from the corporate server to a public cloud provider.*
* *What is the advantage of a jump box? When a* ***jump box*** *is used, its hidden* ***benefit*** *is that any tools in place for the SAN system are maintained on that single system. Therefore, when an update to the SAN management software is available, only a single system requires the update.*

*https://www.techrepublic.com/blog/data-center/jump-boxes-vs-firewalls/*

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

* *TODO: What does Filebeat watch for?- log files/locations and collects log events.*
* *TODO: What does Metricbeat record?* ***Metricbeat*** *takes the metrics and statistics that it collects and ships them to the output that you specify, 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 | Gateway | 10.0.0.1 | Linux |
| Web-1 | Server | 10.0.0.5 | linux |
| Web-2 | Server | 10.0.0.6 | linux |
| ElkProject | Server | 10.1.0.4 | linux |

### **Access Policies**

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

Only the \_\_\_\_whitelisted IP VM\_+   
Elk VM machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* *TODO:*

*96.255.46.155 and*

*157.55.198.166*

Machines within the network can only be accessed by \_\_\_single server/ ssh\_\_.

* *TODO: Which machine did you allow to access your ELK VM? Jumpbox*
* *What was its IP address? 10.0.0.4*

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  Web-2 no 10.0.04  ElkProject no 10.0.0.4 | 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...

* *TODO: What is the main advantage of automating configuration with Ansible?*
* *The* ***primary benefit*** *of* ***Ansible*** *is it allows IT administrators* ***to automate*** *away the drudgery from their daily tasks. That frees them to focus on efforts that help deliver more value to the business by spending time on more important tasks.*

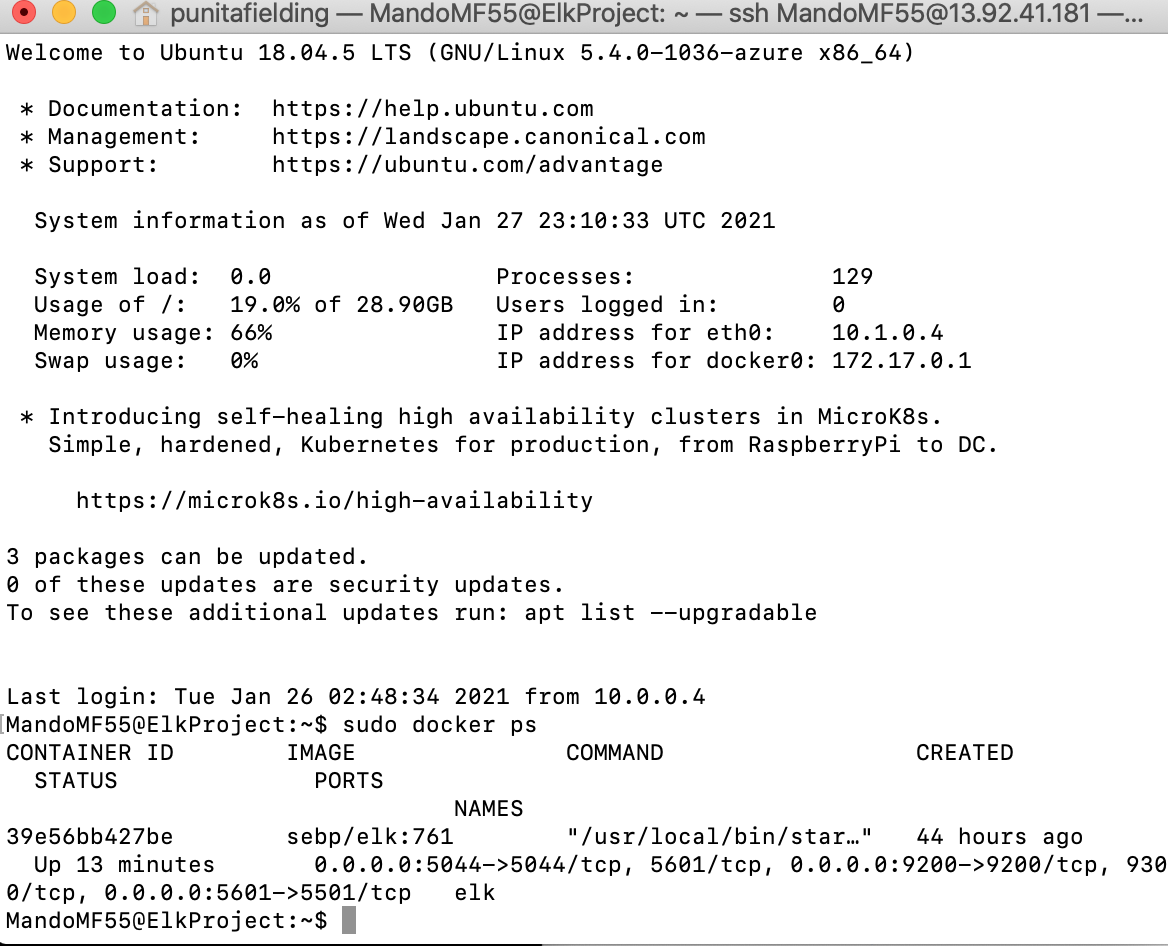
*https://wtop.com/open-first/2017/05/5-primary-reasons-for-the-popularity-of-ansible/#:~:text=The%20primary%20benefit%20of%20Ansible,time%20on%20more%20important%20tasks.*

The playbook implements the following tasks:

* *TODO: In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.*
* Install Docker.io
* Start and attach docker
* Install Python\_pip
* Download image
* Install Docker
* Modify config file
* Command: sysctl -w vm.max\_map\_count=262144
* Write yml file
* Enable docker +launch docker container:elk

...

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



**Note**: The following image link needs to be updated. Replace docker\_ps\_output.png with the name of your screenshot image file.

### **Target Machines & Beats**

This ELK server is configured to monitor the following machines:

* *TODO: List the IP addresses of the machines you are monitoring: Jumpbox VM 10.0.0.4*

We have installed the following Beats on these machines:

* *TODO: Specify which Beats you successfully installed- Filebeat, Metric Beat*

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

* *TODO: 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 collects the changes done (screenshot: Images/Filebeat) Metric beat collects metrics and statistics screenshot: Images/Metricbeat)*

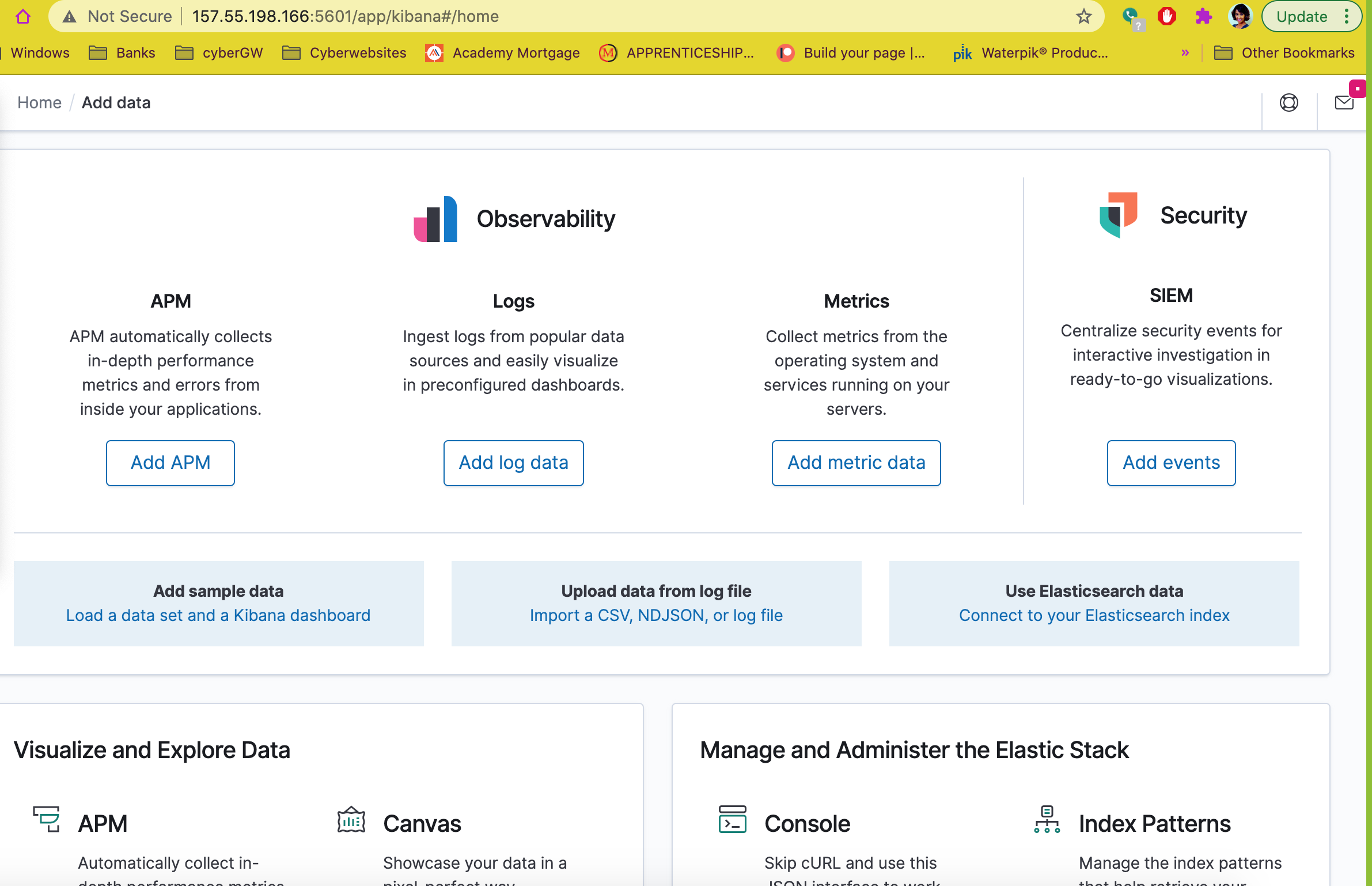
### **Using the Playbook**

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 \_\_\_filebeak configuration file to \_\_\_\_\_/etc/ansible/roles.
* Update the \_\_\_filebeat\_config.yml\_\_ file to include...elk webserver
* Run the playbook, and navigate to \_kibana\_\_\_ to check that the installation worked as expected.

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

* *Which file is the playbook? Filebeat.yml Where do you copy it? roles*
* *Which file do you update to make Ansible run the playbook on a specific machine? filebeat\_config.yml*
* *How do I specify which machine to install the ELK server on versus which to install Filebeat on? Elk Webserver with IP was added*
* \_Which URL do you navigate to in order to check that the ELK server is running? http://<publicIP>:5601/app/kibana
* 

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

*Nano filebeat-playbook.yml*

*Ansible-playbook filebeat.yml*