13.3 ELK STACK project completed project

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 Load balancing can do more than just act as a network traffic cop. Software load balancers provide benefits like predictive analytics that determine traffic bottlenecks before they happen. As a result, the software load balancer gives an organization actionable insights. These are key to automation and can help drive business decisions.

The load balancer helps servers move data efficiently, optimizes the use of **application delivery resources** and **prevents server overloads**. Load balancers conduct continuous health checks on servers to ensure they can handle requests. **The load balancer removes unhealthy servers from the pool until they are restored. Some load balancers even trigger the creation of new virtualized application servers to cope with increased demand.**

In the seven-layer Open System Interconnection (OSI) model, network firewalls are at levels one to three (L1-Physical Wiring, L2-Data Link and L3-Network). Meanwhile, load balancing happens between layers four to seven (L4-Transport, L5-Session, L6-Presentation and L7-Application).

Load balancers have different capabilities, which include:

What aspect of security do load balancers protect?

- **L4 — directs traffic based on data from network and transport layer protocols, such as IP address and TCP port.**

- L7 — adds content switching to load balancing. This allows routing decisions based on attributes like HTTP header, uniform resource identifier, SSL session ID and HTML form data.
- GSLB — Global Server Load Balancing extends L4 and L7 capabilities to servers in different geographic locations.

_____ to the network. Answer continued: 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?*
- *Answer: The jump boxes use your IP address there for you are able to ssh to my jump box using my ip address only. Keeps it safe*

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

- *What does Filebeat watch for?*
-
- *Answer: Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.*
- *What does Metricbeat record?*
-
- *Answer: Metricbeat takes the metrics and statistics that it collects and ships them to the output that you specify, such as Elasticsearch or Logstash.*
-

Metricbeat helps you monitor your servers by collecting metrics from the system and services running on the server, such as:

- *Apache*
- *HAProxy*
- *MongoDB*
- *MySQL*
- *Nginx*
- *PostgreSQL*
- *Redis*

- *System*
- *Zookeeper*
-

The configuration details of each machine may be found below. *Note: Use the [Markdown Table Generator](#) add/remove values from the table.*

Name	Function	IP Address	Operating System
Jump Box	Gateway	10.0.0.1	Linux
ELK	**Google Cloud Platform**	52.184.147.235 Public 10.0.0.4 Private IP	**Linux**
DVWA WEB-1	web application,	40.88.139.223 Public IP 10.1.0.5 Private IP	**Linux**
DVWA WEB-2	web application,	10.1.0.8 Private IP	**Linux**

Access Policies

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

Only the __owner of___ machine can accept connections from the Internet. Access to this machine is only allowed from the private IP addresses:

Add whitelisted IP addresses?

Answer: is a security feature often used for limiting and controlling access only to trusted users. IP whitelisting allow you to create lists of trusted IP address or IP ranges from which your users can access your domain,

Machines within the network can only be accessed by?

Answer: The only access allowed on virtual machines the service from specific IP addresses.. At the same time , it blocks access for computers attempting unauthorized access from all unspecified IP addresses.

TODO: Which machine did you allow to access your ELK VM?

What was its IP address?

Answer: 10.1.0.8

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

Name	**Publicly Accessible**	**Allowed IP Addresses**
Jump Box	**Yes**	**10.1.0.4 private IP** 13.68.185.62 Public which you connect to

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 _name of file to _the container____.**
- **Update the_ansible__ file to include...**
- **Run the playbook, and navigate to sudo docker ps -a to check that the installation worked as expected.**

Answer the following questions to fill in the blanks:

- ***Which file is the playbook?***
- ***Answer: Ansible***
-
- ***Where do you copy it?***
- ***Answer: Jumpbox***
-

- ***Which file do you update to make Ansible run the playbook on a specific machine?***
- ***Answer: first_playbook.yml Ansible is to use an inventory file to organize your managed nodes into groups with information like the*** `ansible_network_os` ***and the SSH user.***
    - ***Next Previous***
-
-
- ***How do I specify which machine to install the ELK server on versus which to install Filebeat on?***
- ***Answer: All the web servers, and ELK or just use the name of the Website via encryption of IPv4 and install on only these machines.***
-
- **_Which URL do you navigate to in order to check that the ELK server is running?**
- **Answer: Your web site. Off your web server**

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?

Answer: Ansible Playbook to accomplish the task of setting up and configuring ELK; which is reusable.

- *ansible-playbook install_elk.yml elk. This runs the install_elk.yml playbook on the elk host. No configuration was performed manually.*
- Very simple to set up and use: No special coding skills are necessary to use **Ansible's** playbooks (more on playbooks later). Powerful: **Ansible** lets you model even highly complex IT workflows. Flexible

The playbook implements the following tasks: (playbook fie)

- *In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.*
- *Answer: 1. ELK Stack (Elasticsearch, Logstash & Kibana) offers Azure users with all the key ingredients required for monitoring*

their applications — Elasticsearch for scalable and centralized data storage, Logstash for aggregation and processing, Kibana for visualization and analysis, and Beats for collection of different types of data and forwarding it into the stack.

- *2. The ELK Stack can be deployed in a variety of ways and in different environments*

- *3. a Network Security Group configured to allow incoming traffic to Elasticsearch and Kibana from the outside.*

- The ELK VM exposes an Elastic Stack instance. **Docker** is used to download and manage an ELK container.

```
●  * Install docker.io
●              - name: Install docker.io
●                   apt:
●                   update_cache: yes
●                   name: docker.io
●                   state: present
●         * Install Python-pip
●              - name: Install pip3
●                   apt:
●                   force_apt_get: yes
●                   name: python3-pip
●                   state: present
●     * Install: docker
●              - name: Install Docker python module
●                   pip:
●                   name: docker
●                   state: present
●     * Command: sysctl -w vm.max_map_count=262144
●         - Launch docker container: elk
●              - 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
-
- Update the path with the name of your screenshot of docker ps output](Diagrams/docker_ps_output.png) root@Jump-Box-Provisioner:/home/azadmin# docker ps -a
-
- ### Target Machines & Beats
- **This ELK server is configured to monitor the following machines: All web activity**
-
- - _Which file is the playbook?
- **$Answer:** `cd /etc/ansible`
- `$ ansible-playbook install_elk.yml elk`
- `$ ansible-playbook install_filebeat.yml webservers`
- `$ ansible-playbook install_metricbeat.yml webservers` Ansible-playbook
-
- Where do you copy it?
- **Answer: nano and place script in the ansible container**
- **Next, you must create a** `hosts` **file to specify which VMs to run each playbook on. Run the commands below:**
- **Answer:** `$ cd /etc/ansible`
- `$ cat > hosts <<EOF`
- `[webservers]`
- `10.0.0.5`
- `10.0.0.6`
-
- `[elk]`

- `10.0.0.8`
- `EOF`
-
- **/etc/ansible/file/filebeat-configuration.yml**
-
- - _Which file do you update to make Ansible run the playbook on a specific machine?
- **Answer:** `$ cd /etc/ansible`
- **`$ ansible-playbook install_elk.yml elk`**
- **`$ ansible-playbook install_filebeat.yml webservers`**
- **`$ ansible-playbook install_metricbeat.yml webservers`**
-
- How do I specify which machine to install the ELK server on versus which to install Filebeat on?
- **Answer: Directed by the script it specifies . You must put the Filebeat on every server you're able to collect log…**
-
- Edit the /etc/ansible/host file to add webserver/elkserver ip addresses
-
- - _Which URL do you navigate to in order to check that the ELK server is running?
- **Answer: http://20.44.106.36:5601/app/kibana**
-

Load balancing ensures that the application will be highly **availability,** in addition to restricting **IP addresses** to the network.

- What aspect of security do load balancers protect?
- Answers: **Load balancers protect** the system from DDoS attacks by shifting attack traffic.
-
- What is the advantage of a jump box?
- Answer: The **advantage of a jump box** is to give access to the user from a single node that can be secured and monitored.

The following screenshot displays the result of running docker ps after successfully configuring the ELK instance. (these images or screen shots are on the GitHub repository)

```
 azadmin@ELK:~$ sudo docker ps -a

CONTAINER ID       IMAGE              COMMAND                  CREATED             STATUS
PORTS

b52c3740e92a       sebp/elk:761       "/usr/local/bin/star…"   3 days ago          Up 4 minutes
0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:

azadmin@ELK:~$ sudo docker start elk

elk
```

? Update the image file path with the name of your screenshot of docker ps output:

```
root@Jump-Box-Provisioner:/home/azadmin# docker ps -a

CONTAINER ID       IMAGE                    COMMAND            CREATED             STATUS
PORTS              NAMES

32dfa58246fa       cyberxsecurity/ansible   "bash"             10 days ago         Exited (127) 2
minutes ago                     frosty_villani
```

Exploring_Kibana unsolved.md

Instructions

Add the sample web log data to Kibana. (included in images / snap_shots) in the repository.

Answer the following questions:

- In the last 7 days, how many unique visitors were located in India?
- **Answer: 228 unique visitors**
-
- In the last 24 hours, of the visitors from China, how many were using Mac OSX?
- **Answer: 68 visitors used MAC OSX**
-
- In the last 2 days, what percentage of visitors received 404 errors?
  Answer: 5.376%
-
- How about 503 errors?
- **Answer: 3.226%**

-
- In the last 7 days, what country produced the majority of the traffic on the website?
- **Answer: China 331**
-
- Of the traffic that's coming from that country, what time of day had the highest amount of activity?
- **Answer: 9am , 12. , 1300**
-
- List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).
- **Answer: html, .gz, .css located in HTML, on a webpage. .zip, deb Debian Linux software packages using apt. And .rpm file formats are Read Hat Software Packaged files**
- **AnsibleRoles.md, File beat-config.yml, filebeatg-playbook.yml, metricbeat-config.yml, metricbeat-playbook.yml, these are the file types used .**

Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.

- Locate the time frame in the last 7 days with the most amount of bytes (activity).?
- **Answer: 10,735,667 ave bytes**
-
- In your own words, is there anything that seems potentially strange about this activity?
- **Answer: Only 3 users were using an extreme amount of bytes 3=count users and copying the data from the cookies to retrieve personal info informing the users of personal interest, taste, and needs to direct to web sites.**

Filter the data by this event.

- What is the timestamp for this event?
- **Answer: March 21, 2021**

-
- What kind of file was downloaded?
- **Answer: Rpm** response 200 HTTP
-
- From what country did this activity originate?
- **Answer: India**
-
- What HTTP response codes were encountered by this visitor?
- **Answer: 200 tag success ,**

Switch to the Kibana Discover page to see more details about this activity.

- What is the source IP address of this activity?
- **Answer: 35.143.166.159**
-
-
- What are the geo coordinates of this activity?
- **Answer: { "lat": 43.34121, "lon": -73.6103075 }**
-
- What OS was the source machine running?
- **Answer:064 machine.os:win**
-
- What is the full URL that was accessed?
- **Answer: Artifacts.elastic.co**
-
- **From what website did the visitor's traffic originate?** **Answer: Facebook**

Finish your investigation with a short overview of your insights.

- What do you think the user was doing?
- **Answer: Delivering Packages**
-
- Was the file they downloaded malicious?
- Answer: **No**

- Is there anything that seems suspicious about this activity?
- **Answer: He was able to download cookies during the session to steal the information**
- **downloaded all the information off the session on facebook**

- Is any of the traffic you inspected potentially outside of compliance guidelines?
- **Answer: It is not compliant with post package links on facebook.**

○

○