Automated ELK Stack Deployment

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

https://drive.google.com/file/d/1y4rfK6ZueKpf5Shd6JEknWtindc4NFdS/view?usp=sharing

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

- _TODO: Enter the playbook file._

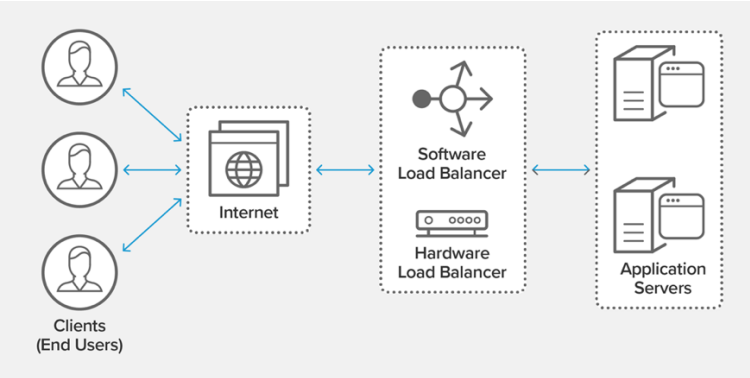
This document contains the following details:
- Description of the Topology
- Access Policies
- ELK Configuration
  - Beats in Use
  - Machines Being Monitored
- How to Use the Ansible Build

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.

jump box is a system on a network used to access and manage devices in a separate security zone. A **jump** server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them.

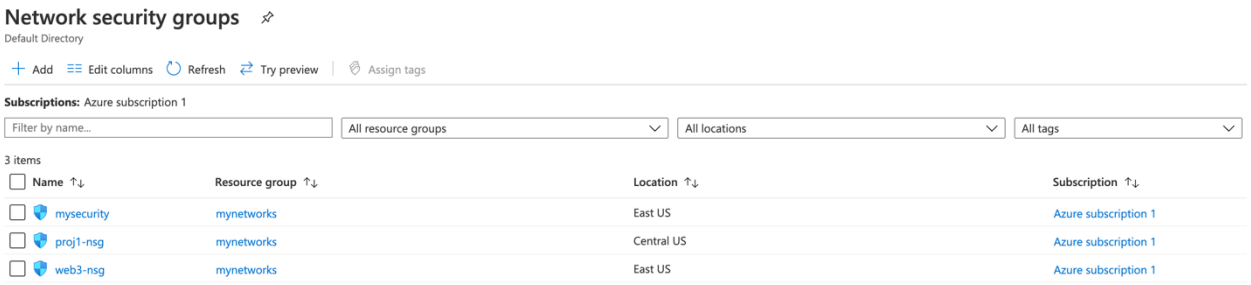
Load balancing ensures that the application will be highly available, in addition to restricting traffic to the network.
A **load balancer** is a device that acts as a reverse proxy and distributes **network** or application traffic across a number of servers. **Load balancers** are used to increase capacity (concurrent users) and reliability of applications.

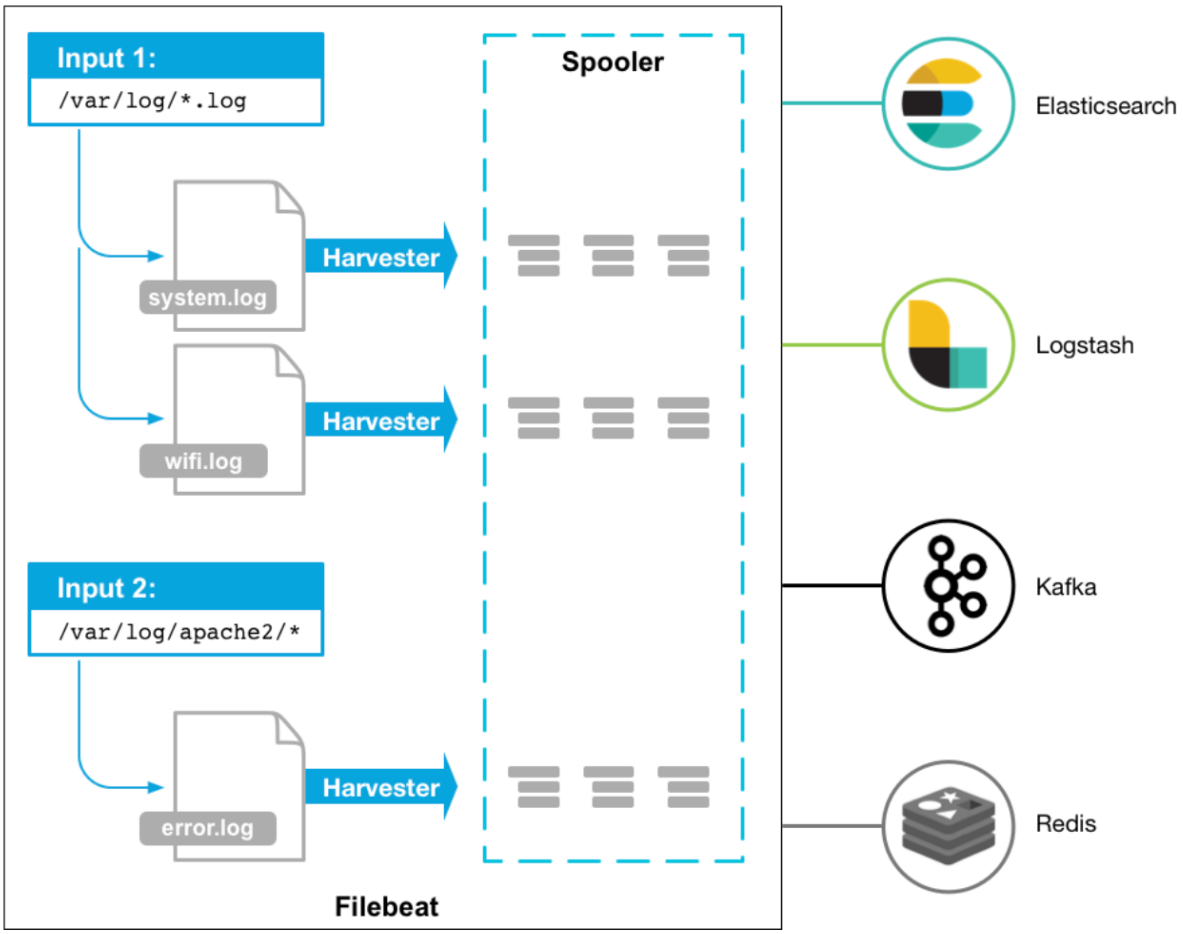


Load Balancing plays an important security role as computing moves evermore to the cloud. The off-loading function of a load balancer defends an organization against distributed **denial**-of-service (DDoS) attacks. It does this by shifting attack traffic from the corporate server to a public cloud provider.

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

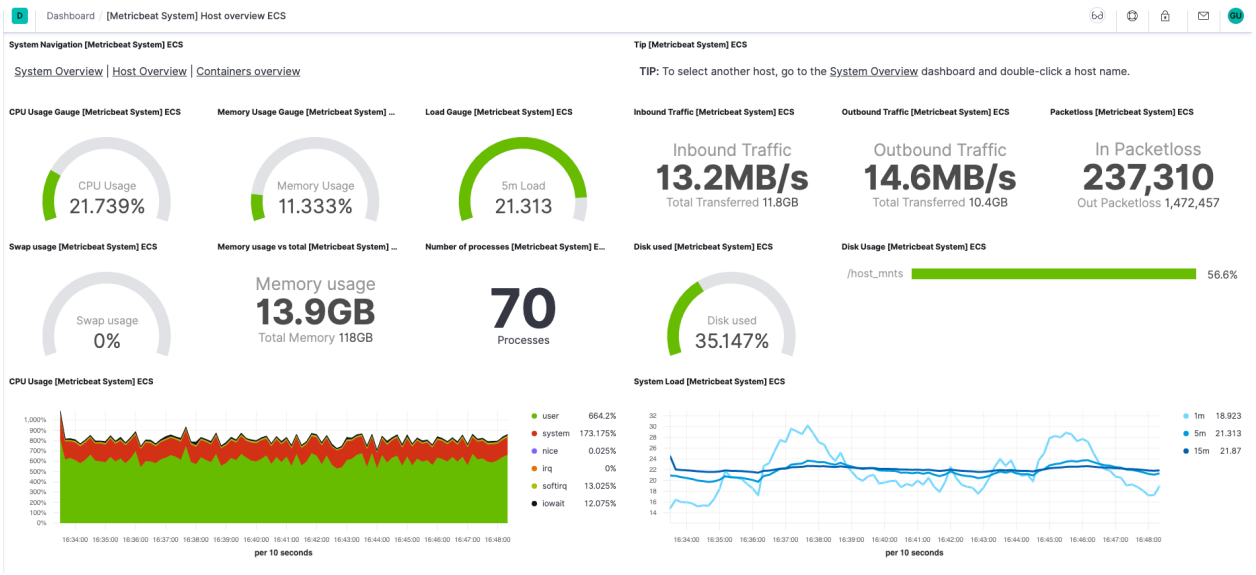
Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.





Metricbeat is a lightweight shipper that you can install on your servers to periodically collect metrics from the operating system and from services running on the server. 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:



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	10.0.0.6	Linux
Web 1	Webserver	10.0.0.7	Linux
Web 2	Webserver	10.0.0.8	Linux
Web 3	Webserver	10.0.0.10	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:
- _TODO: Add whitelisted IP addresses_

Machines within the network can only be accessed by ssh.
Which machine did you allow to access your ELK VM? What was its IP 13.92.154.17
Elk was accessed from the Jump Box ansible container

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

Name	Publicly Accessible	Allowed IP Addresses
Jump Box	Yes/No	10.0.0.6 13.92.154.17

Inbound access is limited to port 22 and the ip of my local computer

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?_You can create and maintain multiple servers.

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._
- ...
- ...

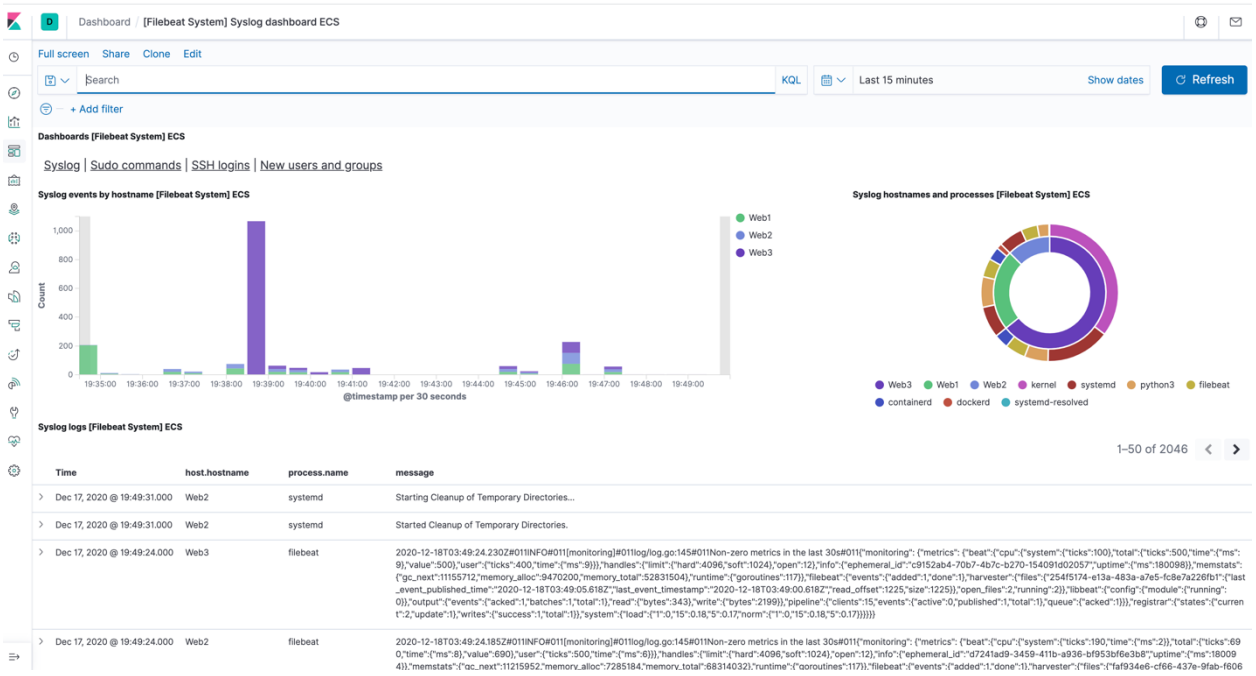
The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

```
TASK [use more memory] *********************************************************************************************************************************
changed: [10.1.0.4]

TASK [download and launch a docker elk container] ******************************************************************************************************
changed: [10.1.0.4]

PLAY RECAP *********************************************************************************************************************************************
10.1.0.4                   : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@96fa14d8abbb:/etc/ansible# ssh azuser@10.1.0.4
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1031-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Dec 16 04:17:48 UTC 2020

  System load:  0.46              Processes:             133
  Usage of /:   16.0% of 28.90GB  Users logged in:       0
  Memory usage: 37%               IP address for eth0:   10.1.0.4
  Swap usage:   0%                IP address for docker0: 172.17.0.1


16 packages can be updated.
16 updates are security updates.

New release '20.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Dec 16 04:11:08 2020 from 10.0.0.6
azuser@proj1:~$ sudo dockerps
sudo: dockerps: command not found
azuser@proj1:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
                                                NAMES
3bf365c3c483        sebp/elk:761        "/usr/local/bin/star…"   4 minutes ago       Up 4 minutes        0.0.0.0:5044->5044/tcp, 0.0.
:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
azuser@proj1:~$
```

Target Machines & Beats
This ELK server is configured to monitor the following machines:
List the IP addresses of the machines you are monitoring_
10.0.0.7
10.0.0.8
10.0.0.10

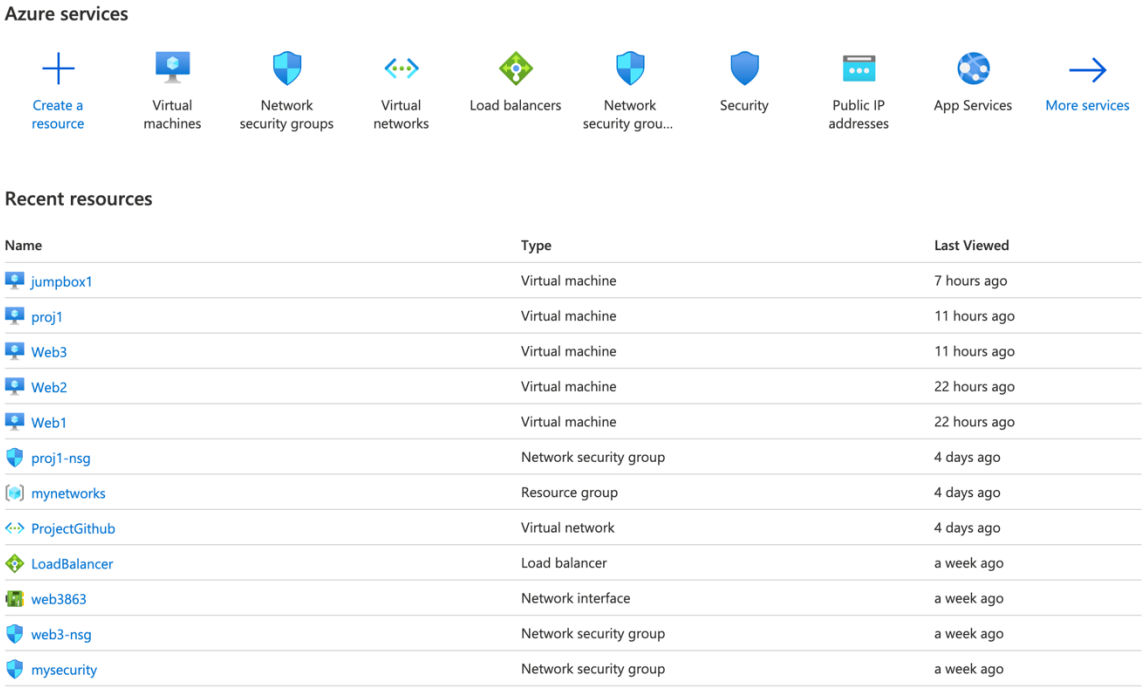
We have installed the following Beats on these machines:
Web 1, Web 2, Web 3

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



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 _____ file to _____.
- Update the hosts file to include the ip address of the machine being updated
- Run the playbook, and navigate to elk server to check that the installation worked as expected.



TODO: Answer the following questions to fill in the blanks:
- _Which file is the playbook? Where do you copy it? Install-elk.yml – jumpbox container
- _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?_The playbook and the hosts file.
- _Which URL do you navigate to in order to check that the ELK server is running? http://40.122.24.253:5601/app/kibana#/discover

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