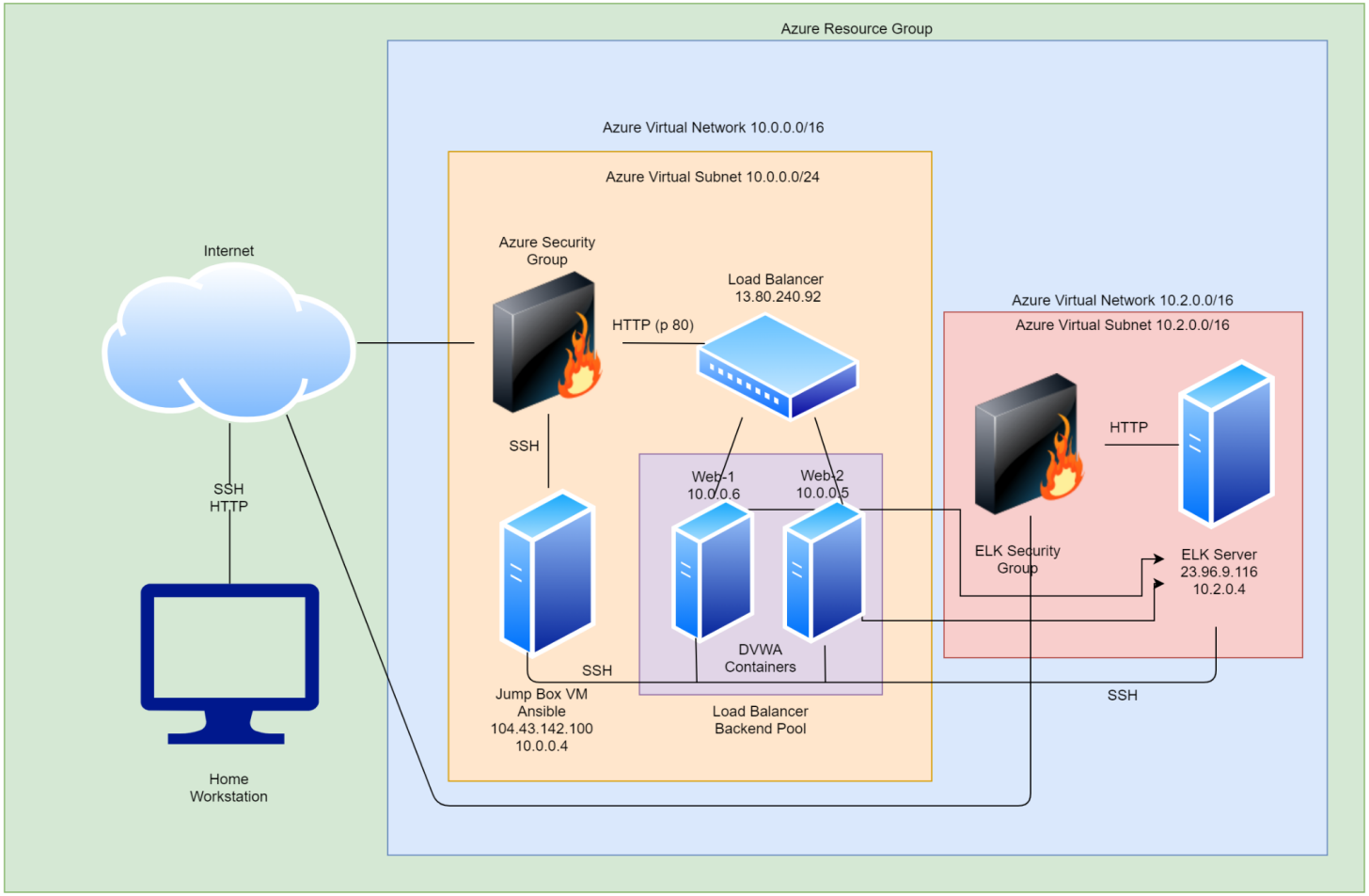
Automated ELK Stack Deployment

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

- /etc/ansible/install-elk.yml

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.

Load balancing ensures that the application will be highly monitored, in addition to restricting access to the network.

Load balancers increase availability. They can protect from DDoS attacks.
The advantage of using a jump box is to have a single location from which you work; in a more secure way that can be monitored.

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

- Filebeat watches for any information watches for changes in the file system.

- Users can use metric beat to output metrics, statistics, and other data to a location that the user specifies.

The configuration details of each machine may be found below.

Name	Function	IP Address	OS
Jump Box	Gateway	10.0.0.4	Linux
Web-1	Server	10.0.0.6	Linux
Web-2	Server	10.0.0.5	Linux
Elk	Server	10.2.0.4	Linux

Access Policies

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

Only the host machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- Personal Public IP from home.

Machines within the network can only be accessed by the Jump Box VM
- Jump Box VM: VNET IP 10.0.0.4

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

Name	**Publically Accessible**	**Allowed IPs**
Jump Box	Yes	Home IP Address
Web-1	No	10.0.0.4
Web-2	No	10.0.0.4
Elk	No	10.0.0.4

Elk Configuration

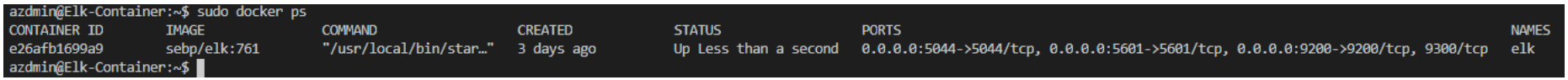
Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because:

- The main advantage of automating configuration with Ansible is that you can deploy these configurations to multiple servers at once from a single playbook.

The playbook implements the following tasks:

- Install: docker.io
- Install: python-pip
- Install: docker
- Command: sysctl -w vm.max_map_count=262144
- Launch docker container: elk

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:

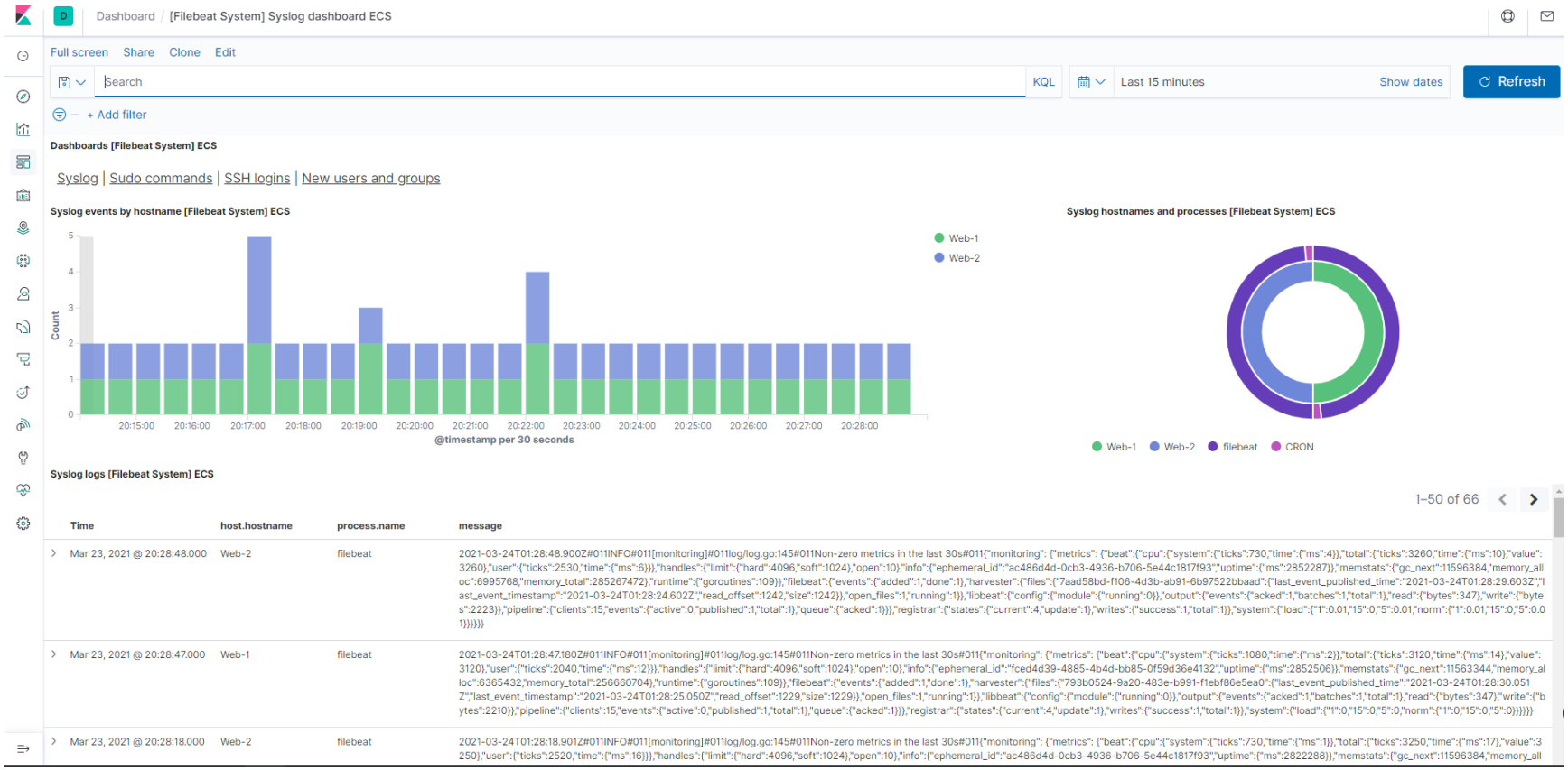
- Web-1: 10.0.0.6
- Web-2: 10.0.0.5

We have installed the following Beats on these machines:

- Filebeat

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

- Filebeat collects the different processes that have run and shows them on a timeline. My system currently is only populated by syslog processes from my Web-1 and Web-2 servers



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 public key file to VM Password.
- Update the hosts file to include...
- Run the playbook, and navigate to Kibana to check that the installation worked as expected.

- Which file is the playbook? Where do you copy it?
    - /etc/ansible/file/filebeat-configuration.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?
    - 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?
        - http://23.96.9.116:5601/app/kibana. This IP is that of my Load Balancer.