# elkstackproject

#

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.

Diagram

Description automatically generated

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.

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 available in addition to preventing unwanted access to the network through use of a security-group-controlled Jump Box and load balancer.

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

The configuration details of each machine may be found below.

Note: Use the Markdown Table Generator to add/remove values from the table.

Name

Function: The purpose of our setup is to have two network security groups. The first is to protect the public IP address and to provide limited connectivity between virtual machines by limiting port access.

Operating System

Jump Box:

52.149.151.87 (public)

Gateway

10.0.0.4 (internal)

Web-1:

10.0.0.5 (internal)

Web-2:

10.0.0.6 (internal)

Web-3:

10.0.0.7 (internal)

Load Balancer:

40.117.127.52

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:

Policy 1 - You will want to set up the network security group inbound rules to set it to allow SSH access between the Jump Box and Web-1, Web-2, and Web-3. This will allow it to make changes to the other machines remotely.

A screenshot of a cell phone

Description automatically generated

Machines within the network can only be accessed by ssh from the Jumpbox (52.149.151.87).

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

Allowed IP Addresses

|  |  |  |
| --- | --- | --- |
| Name | Publicly Accessibly | Allowed IP |
| Jump Box | Yes | Variable Personal IP |
| Web-1 | No | 10.0.0.5 |
| Web-2 | No | 10.0.0.6 |
| Web-3 | No | 10.0.0.7 |
| Elk-VM | Yes | Variable Personal IP |
| Load Balancer | No | All internal IP addresses |

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because automating Ansible setup prevents installation errors and simplifies installation and container configuration. Automating setup means that each one is set up the same way should one need to be recreated as well.

The playbook implements the following tasks:

* installs elk
* installs docker.io
* installs python3-pip
* installs docker
* sets sysctl memory limitation
* creates elk container and provides port access for our VMs to 5601, 9200, 5044

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:

VM – Web 1: 10.0.0.5

VM – Web 2: 10.0.0.6

VM – Web 3: 10.0.0.7

* For security reasons, these do not have a public IP address
* The security group intercepts all traffic before it gets to the “jump box” or assigned by the load balancer

We have installed the following Beats on these machines:

* Filebeat

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

* Filebeat forwards log data located in the registry. it can collect a variety of log events which can be tailored to preferred specifications. There is a filebeat input file that determines which

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.

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:

(in our case, we connect to the control node from the Jump Box)

1. create the directory “files”
2. Copy the “install-elk.yml file” to the directory “/etc/ansible”.

3. Update the hosts file to include...

[webservers]

## alpha.example.org

## beta.example.org

## 192.168.1.100

## 192.168.1.110

10.0.0.5 ansible\_python\_interpreter=/usr/bin/python3

10.0.0.6 ansible\_python\_interpreter=/usr/bin/python3

10.0.0.7 ansible\_python\_interpreter=/usr/bin/python3

[elk]

10.2.0.4 ansible\_python\_interpreter=/usr/bin/python3

4. Navigate to /etc/ansible/roles

* Run the playbook, and navigate to /etc/ansible/files to check that the installation worked as expected.
* there will be a filebeat configuration file generated if it has run correctly

URL to check ELK Server

<http://13.64.155.154:5601/app/kibana#/home?_g=()>

* the IP address listed here is the external IP address of the ELK VM
* if this does not work, please check the NSG rules to ensure that your personal IP address has been given access to the machine