**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 **playbook** 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 ***restricting*** access to the network.

* What aspect of security do load balancers protect? What is the advantage of a jump box?
* **Load balancers** protects servers to move data more efficiently and prevents server overloads from DDoS attacks.
* The advantage of a **Jump Box** is to give the user access to connect to other machines outside of their own network that is secured and monitored.

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

* What does Filebeat watch for? Processes data from different servers that is installed on hosts that analyzes, monitors, and ships log files.
* What does Metricbeat record? The metricbeat records and collects a large amount of statistical data from the operating system and ships them to the specified output.

The configuration details of each machine may be found below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Function** | **IP Address** | **Operating System** |
| JumpBox | Gateway | 10.0.0.4 | Linux (ubuntu 20.04) |
| Elk-Server | Elastic-Server | 10.1.0.4 | Linux (ubuntu 20.04) |
| Web-1-DVWA | Load Balancer | 10.0.07 | Linux (ubuntu 20.04) |
| Web-2-DVWA | Load Balancer | 10.0.08 | Linux (ubuntu 20.04) |

**Access Policies**

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

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

* Private IP Address

Machines within the network can only be accessed by the JumpBox-provisioner.

Which machine did you allow to access your ELK VM? What was its IP address?\_

* JumpBox Provisioner: 10.0.0.4

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

|  |  |  |
| --- | --- | --- |
| **Name** | **Publicly Accessible** | **Allowed IP Address** |
| JumpBox | NO | Private IP Address |
| Elk-Server | NO | JumpBox-10.0.0.4 Private IP address |
| Web-1-DVWA | YES | 10.0.07 |
| Web-2-DVWA | YES | 10.0.08 |

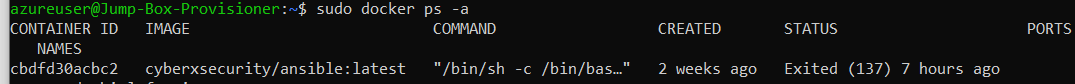
**Elk Configuration**

* Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...
* It allows an automated deployment of workflow that can be added to multiple machines.
* What is the main advantage of automating configuration with Ansible?
* Ansible allows you to control the machines remotely by using SSH, and executing playbooks to configure the virtual machines.

The playbook implements the following tasks:

* Install Docker
* Run container
* Install Filebeat
* Download MetricBeat

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:

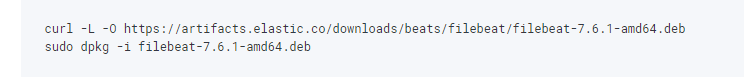
* **10.0.0.7-Web 1**
* **10.0.0.8-Web 2**

We have installed the following Beats on these machines:

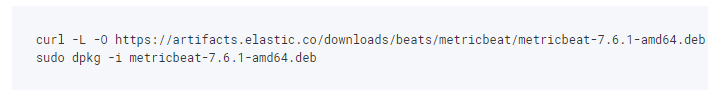
* FileBeat
* MetricBeat

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

* **FileBeat**- Generates logs and stores data when there are multiple machines, servers and containers.



* **MetricBeat**- Monitors system metric data running on the server which includes CPU usage statistics.

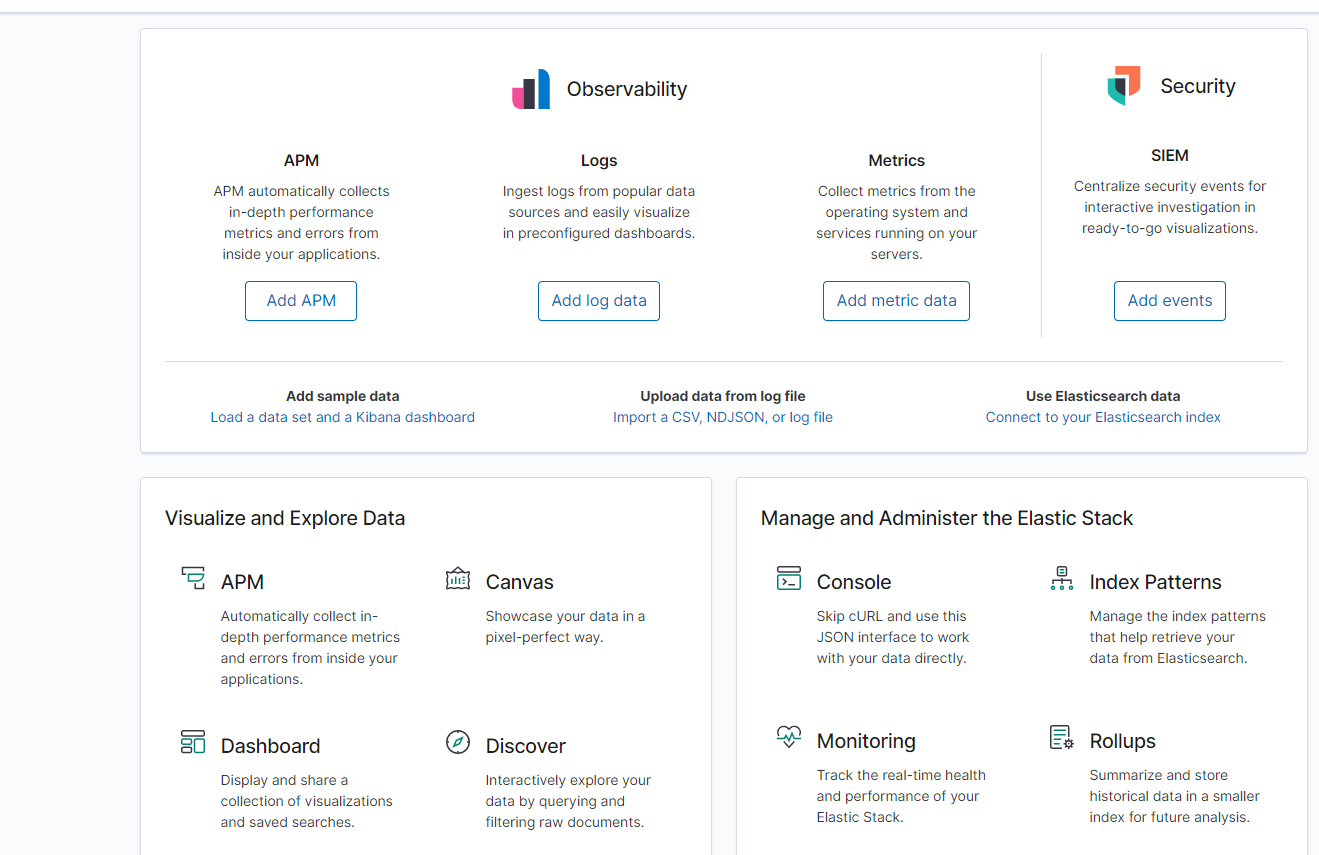


**Using the Playbook**

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 filebeat.yml file to /etc/filebeat directory.
* Update the filebeat-playbook.yml file to include installing the Elk Server
* Run the playbook and navigate to ***Elk Server*** to check that the installation worked as expected.
* Which file is the playbook? Where do you copy it?\_
* Cd /etc/ansible
* 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?\_
* /etc/ansible/hosts
* /etc/ansible/files/filebeat—config.yml
* Which URL do you navigate to in order to check that the ELK server is running?
* **http://40.11\*.174.\*\*\*:5601/app/kibana#/home**



Provide the specific commands the user will need to run to download the playbook, update the files, etc.

* ansible-playbook myplaybook.yml