**ELK Installation**

**elk-install.yml**

---

- name: Configure Elk VM with Docker

hosts: ELK-Server

remote\_user: RedAdmin1

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker

state: present

# Use apt module

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

# Use command module

- name: Increase virtual memory

command: sysctl -w vm.max\_map\_count=262144

# Use sysctl module

- name: Use more memory

sysctl:

name: vm.max\_map\_count=262144

value: ‘262144’

state: present

reload: yes

# Use docker\_container module

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

# Please list the ports that ELK runs on

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

# Use systemd module

- name: Enable service docker on boot

systemd:

name: docker

enabled: yes