Ansible Container.

Edit ansible.cfg to set remote user

```
root@0ee040206a9f:/etc/ansible# ls
ansible.cfg  filebeat-7.6.1-amd64.deb  filebeat-7.6.2-amd64.deb  files  hosts  install-elk.yml  metricbeat-7.6.1-amd64.deb  pentest.yml  roles
root@0ee040206a9f:/etc/ansible# nano ansible.cfg
```

Set Remote User in ansible.cfg

```
root@0ee040206a9f: /etc/ansible
  GNU nano 4.8                                                    ansible.cfg
# default user to use for playbooks if user is not specified
# (/usr/bin/ansible will use current user as default)
remote_user = azadmin
```

Edit Ansible Hosts to Add the IP Addresses

1) **Webservers**
2) **Elk Server**

```
root@0ee040206a9f: /etc/ansible
  GNU nano 4.8                                                          hosts
# This is the default ansible 'hosts' file
# It should live in /etc/ansible/hosts
#
#   - Comments begin with the '#' character
#   - Blank lines are ignored
#   - Groups of hosts are delimited by [header] elements
#   - You can enter hostnames or ip addresses
#   - A hostname/ip can be a member of multiple groups

# Ex 1: Ungrouped hosts, specify before any group headers.

#green.example.com
#blue.example.com
#192.168.100.1
#192.168.100.10

# Ex 2: A collection of hosts belonging to the 'webservers' group

[webservers]
10.0.0.6 ansible_python_interpreter=/usr/bin/python3
10.0.0.5 ansible_python_interpreter=/usr/bin/python3


[elk]
10.1.0.4 ansible_python_interpreter=/usr/bin/python3

#[dbservers]
#
#db01.intranet.mydomain.net
#db02.intranet.mydomain.net
#10.25.1.56
#10.25.1.57

# Here's another example of host ranges, this time there are no
# leading 0s:

#db-[99:101]-node.example.com
```

Configure Elk VM with Docker (install-elk.yml)

```
---
- name: Configure Elk VM with Docker
  hosts: elk
  remote_user: azadmin
  become: true
  tasks:
    # Use apt module
    - name: Install docker.io
      apt:
        update_cache: yes
        name: docker.io
        state: present

    # Use apt module
    - name: Install pip3
      apt:
        force_apt_get: yes
        name: python3-pip
        state: present

    # Use pip module
    - name: Install Docker python module
      pip:
        name: docker
        state: present

    # Use sysctl module
    - name: Use more memory
      sysctl:
        name: vm.max_map_count
        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
        published_ports:
          - 5601:5601
          - 9200:9200
          - 5044:5044

    # Use systemd module
```

```
- name: Enable service docker on boot
  systemd:
    name: docker
    enabled: yes
```