ANSIBLE 04

1) Create ansible playbook to create ansible vault.

→ ansible playbook to create ansible vault.

```
ubuntu@ip-172-31-15-53: ~
---
- name: Create Ansible Vault
  hosts: all
  gather_facts: no
  become: yes
  tasks:
    - name: Ensure vault directory exists
      file:
        path: "{{ vault_dir }}"
        state: directory
        mode: '0755'

    - name: Create Ansible Vault file
      copy:
        dest: "{{ vault_dir }}/{{ vault_file }}"
        content: "{{ vault_content | default('secret_data') }}"
        mode: '0600'
      no_log: true

    - name: Create vault password file
      copy:
        dest: "{{ vault_password_file }}"
        content: "your_vault_password"
        mode: '0600'
      no_log: true


    - name: Encrypt the vault file
      command: >
        ansible-vault encrypt {{ vault_dir }}/{{ vault_file }} --vault-password-file {{ vault_password_file }}
      args:
        creates: "{{ vault_dir }}/{{ vault_file }}.enc"

  vars:
    vault_dir: "/etc/ansible/vaults"
    vault_file: "secrets.yml"
    vault_password_file: "/etc/ansible/vault_pass.txt"
    vault_content: |
      secret_key: my_secret_value
```

→before run above script install ansible in worker node:

```
ubuntu@ip-172-31-12-185:~$ sudo apt update
```

```
ubuntu@ip-172-31-12-185:~$ sudo apt install ansible -y
```

```
ubuntu@ip-172-31-12-185:~$ ansible --version
ansible [core 2.16.3]
  config file = None
```

→now run the script:

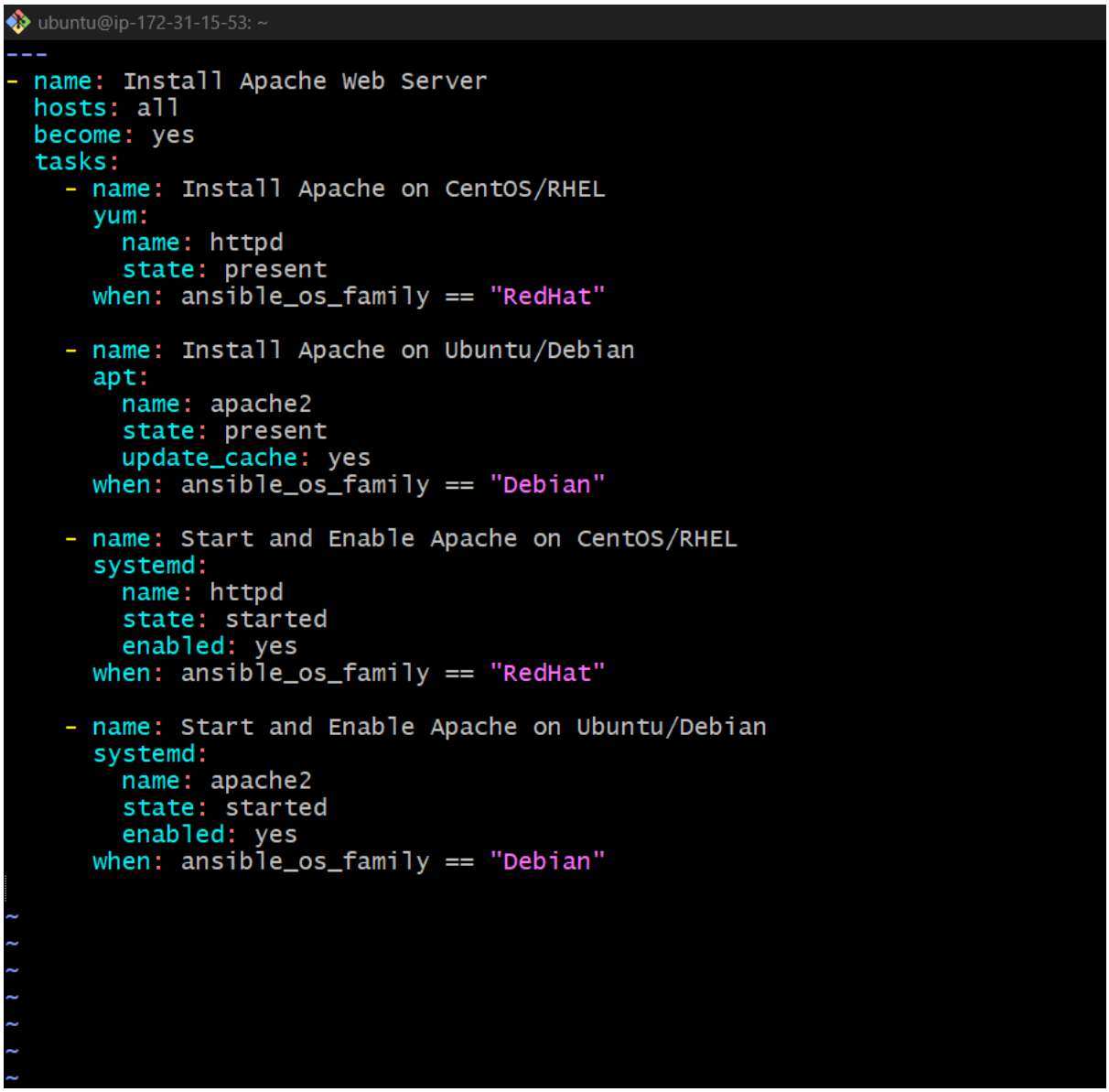
```
ubuntu@ip-172-31-15-53:~$ sudo vi vault1.yml
ubuntu@ip-172-31-15-53:~$ ansible-playbook vault1.yml --ask-become-pass
BECOME password:
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details

PLAY [Create Ansible Vault] ***************************************************************************************************************************************

TASK [Ensure vault directory exists] ******************************************************************************************************************************
[WARNING]: Platform linux on host 172.31.10.100 is using the discovered Python interpreter at /usr/bin/python3.12, but future installation of another Python
interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.17/reference_appendices/interpreter_discovery.html for more
information.
ok: [172.31.10.100]
[WARNING]: Platform linux on host 172.31.12.185 is using the discovered Python interpreter at /usr/bin/python3.12, but future installation of another Python
interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.17/reference_appendices/interpreter_discovery.html for more
information.
ok: [172.31.12.185]

TASK [Create Ansible Vault file] **********************************************************************************************************************************
ok: [172.31.12.185]
ok: [172.31.10.100]

TASK [Create vault password file] *********************************************************************************************************************************
changed: [172.31.12.185]
changed: [172.31.10.100]

TASK [Encrypt the vault file] *************************************************************************************************************************************
changed: [172.31.12.185]
changed: [172.31.10.100]

PLAY RECAP ********************************************************************************************************************************************************
172.31.10.100              : ok=4    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
172.31.12.185              : ok=4    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

→file is encrypted:

```
ubuntu@ip-172-31-12-185:~$ ls -l /etc/ansible/vaults/secrets.yml
-rw------- 1 root root 419 Mar 28 09:28 /etc/ansible/vaults/secrets.yml
ubuntu@ip-172-31-12-185:~$ sudo ansible-vault view /etc/ansible/vaults/secrets.yml --vault-password-file /etc/ansible/vault_pass.txt
secret_key: my_secret_value
ubuntu@ip-172-31-12-185:~$ cat /etc/ansible/vaults/secrets.yml
cat: /etc/ansible/vaults/secrets.yml: Permission denied
ubuntu@ip-172-31-12-185:~$ sudo chown ubuntu:ubuntu /etc/ansible/vaults/secrets.yml
ubuntu@ip-172-31-12-185:~$ cat /etc/ansible/vaults/secrets.yml
$ANSIBLE_VAULT;1.1;AES256
66316332623364303132643636386335366638396630613464656365643430613139306135363535
31323864623031313166343039393230323030623130353370a33633738376133313764623343036
31386435656461333338653837643134626566353132623535396335393863626262376465396462
31396265303732623 10a393431623663653531353335353730313331336431306533636163323836
35623465306261316362363834626534306135393564306465346135636538326361
```

2) Write a ansible playbook to install apache in linux and ubuntu machine by using when condition.

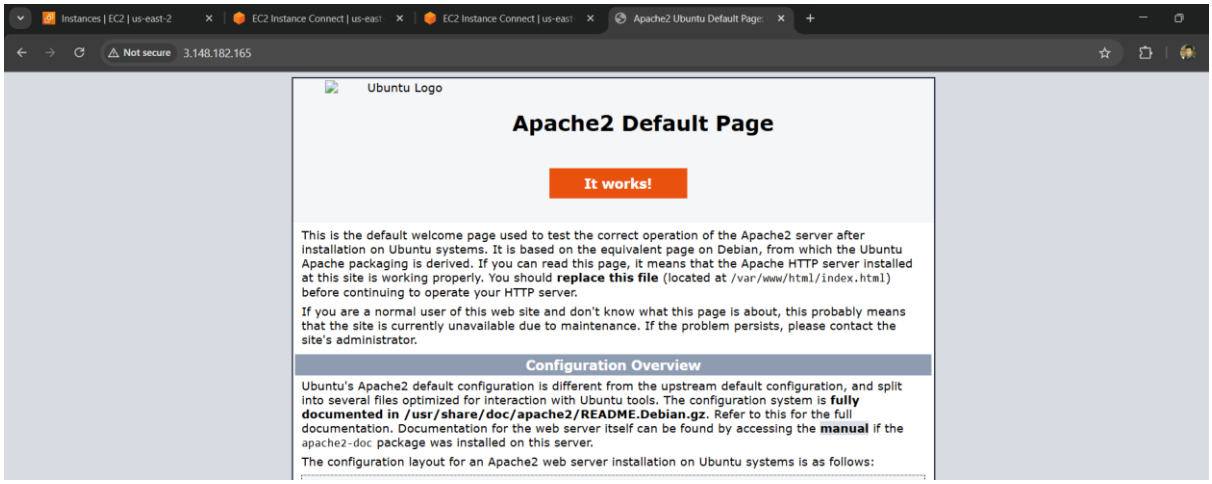
→ ansible playbook to install apache in linux and ubuntu machine by using when condition:



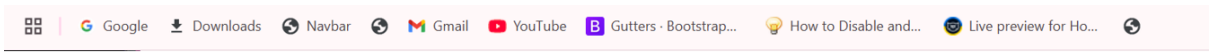
→run the playbook:

```
ubuntu@ip-172-31-15-53:~$ sudo vi webser.yml
ubuntu@ip-172-31-15-53:~$ ansible-playbook webser.yml
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details

PLAY [Install Apache Web Server] ***********************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************
[WARNING]: Platform linux on host 172.31.12.185 is using the discovered Python interpreter at /usr/bin/python3.12, but future installation of another Python
interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.17/reference_appendices/interpreter_discovery.html for more
information.
ok: [172.31.12.185]
[WARNING]: Platform linux on host 172.31.10.100 is using the discovered Python interpreter at /usr/bin/python3.12, but future installation of another Python
interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.17/reference_appendices/interpreter_discovery.html for more
information.
ok: [172.31.10.100]

TASK [Install Apache on CentOS/RHEL] *******************************************************************************************************************************
skipping: [172.31.12.185]
skipping: [172.31.10.100]

TASK [Install Apache on Ubuntu/Debian] *****************************************************************************************************************************
ok: [172.31.10.100]
ok: [172.31.12.185]

TASK [Start and Enable Apache on CentOS/RHEL] **********************************************************************************************************************
skipping: [172.31.12.185]
skipping: [172.31.10.100]

TASK [Start and Enable Apache on Ubuntu/Debian] ********************************************************************************************************************
ok: [172.31.10.100]
ok: [172.31.12.185]

PLAY RECAP *********************************************************************************************************************************************************
172.31.10.100              : ok=3    changed=0    unreachable=0    failed=0    skipped=2    rescued=0    ignored=0
172.31.12.185              : ok=3    changed=0    unreachable=0    failed=0    skipped=2    rescued=0    ignored=0

ubuntu@ip-172-31-15-53:~$
```

→Appache2 running:



→Httpd running on linux server:



It works!

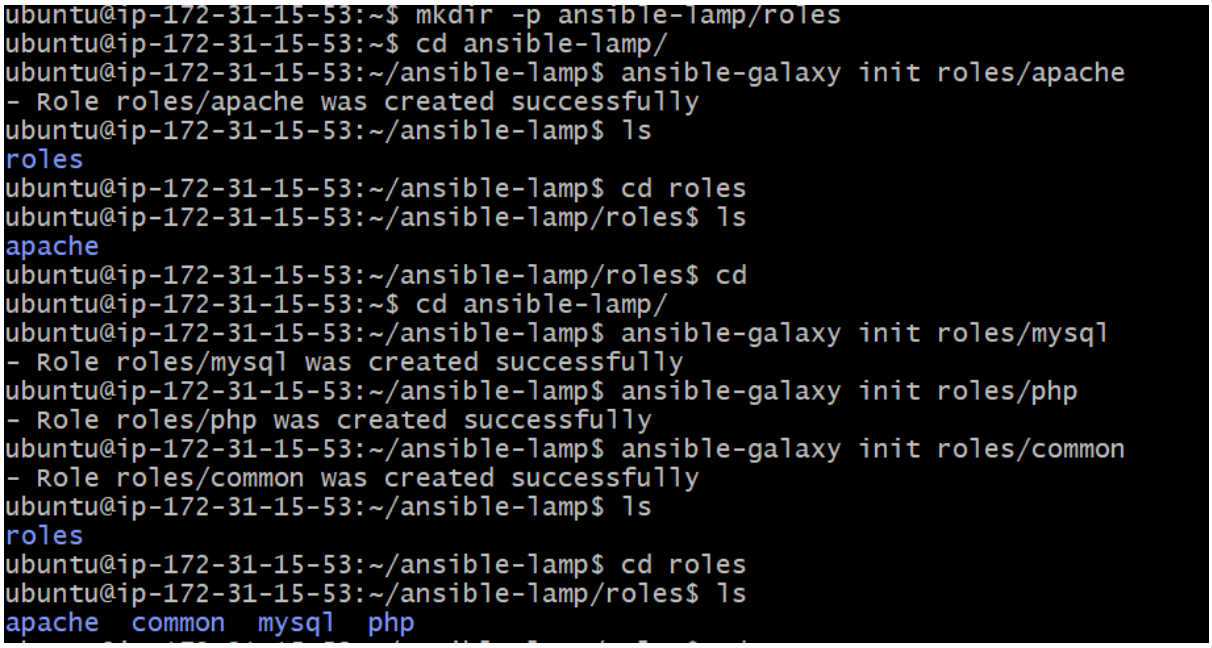
3) Create ansible playbook using roles to configure LAMP stack

→ Create a directory for your Ansible project

mkdir -p ansible-lamp/roles

cd ansible-lamp

→ Generate role structure



→ **Define the playbook (lamp.yml)**

```
---
- name: Configure LAMP Stack using Ansible Roles
  hosts: localhost
  become: yes
  roles:
    - apache
    - mysql
    - php
```

→**Role: apache**

This role installs and configures Apache.

roles/apache/tasks/main.yml

```
- name: Install Apache
  apt:
    name: apache2
    state: present

- name: Start and enable Apache service
  service:
    name: apache2
    state: started
    enabled: yes

- name: Deploy index.php file
  copy:
    dest: /var/www/html/index.php
    content: |
      <?php
      phpinfo();
      ?>
```

→**Role: mysql**

This role installs MySQL and sets up a database.

roles/mysql/tasks/main.yml

yaml

CopyEdit

```yaml
- name: Install MySQL server
  apt:
    name: mysql-server
    state: present

- name: Start and enable MySQL service
  service:
    name: mysql
    state: started
    enabled: yes

- name: Secure MySQL installation (set root password)
  mysql_user:
    name: root
    password: "rootpassword"
    host_all: yes
    state: present
```

→Role: php

This role installs PHP and required extensions.

roles/php/tasks/main.yml

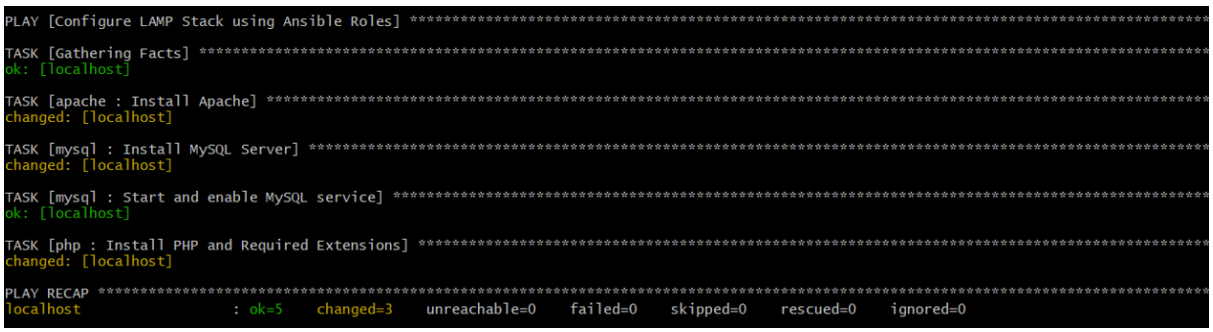
yaml

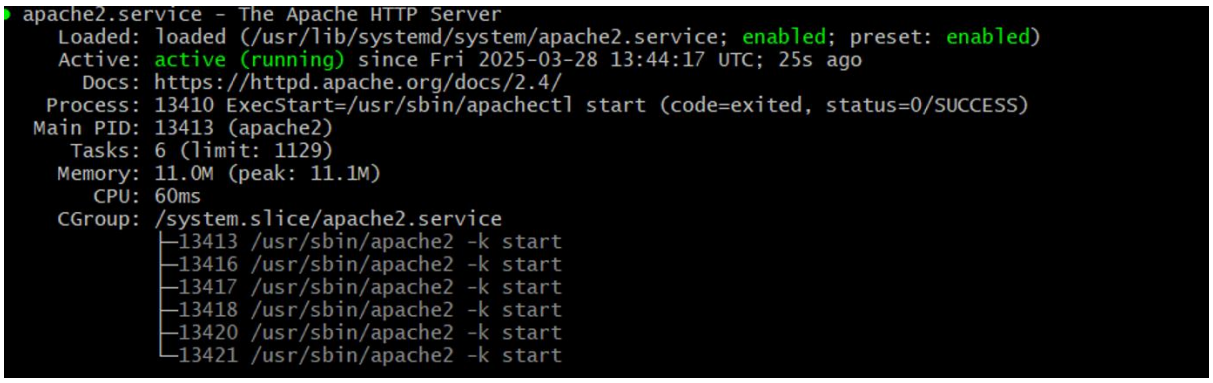
CopyEdit

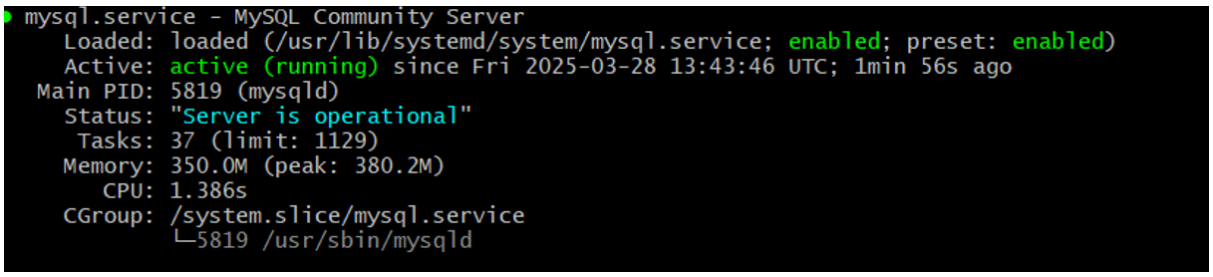
```yaml
- name: Install PHP and extensions
  apt:
    name:
      - php
      - php-mysql
      - libapache2-mod-php
    state: present

- name: Restart Apache
  service:
    name: apache2
    state: restarted
```

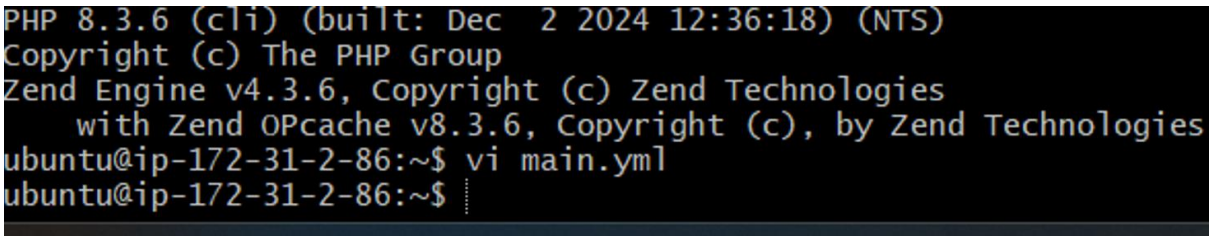
→run the playbook:

ansible-playbook -i lamp.yml









4) Setup ansible AWX and explore the options:

→Following these steps:

1 sudo apt install python-setuptools -y

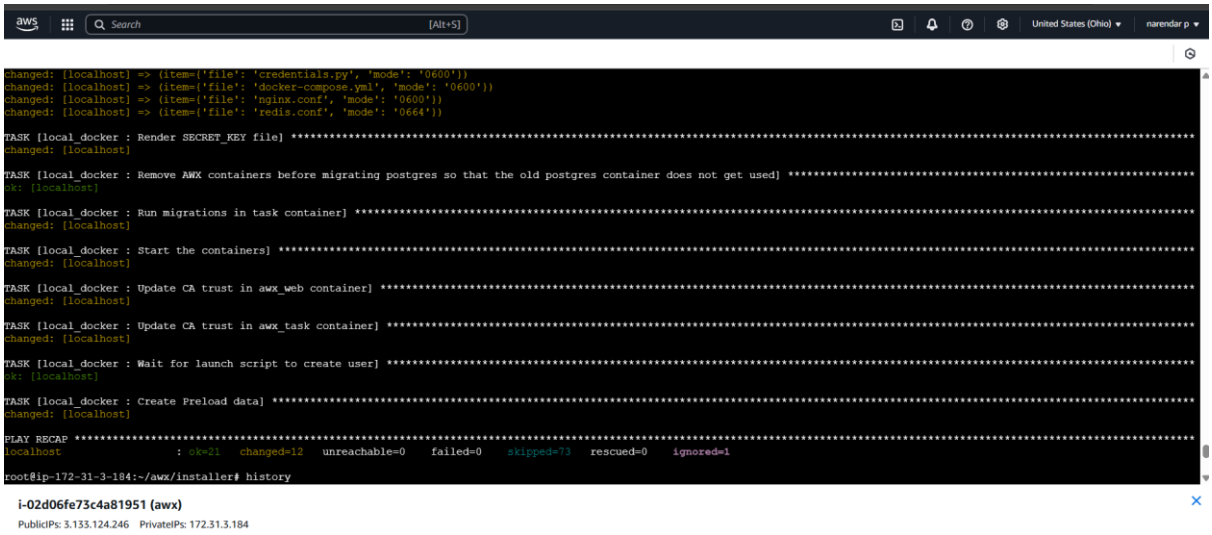
2 sudo apt update -y

3 apt install ansible -y

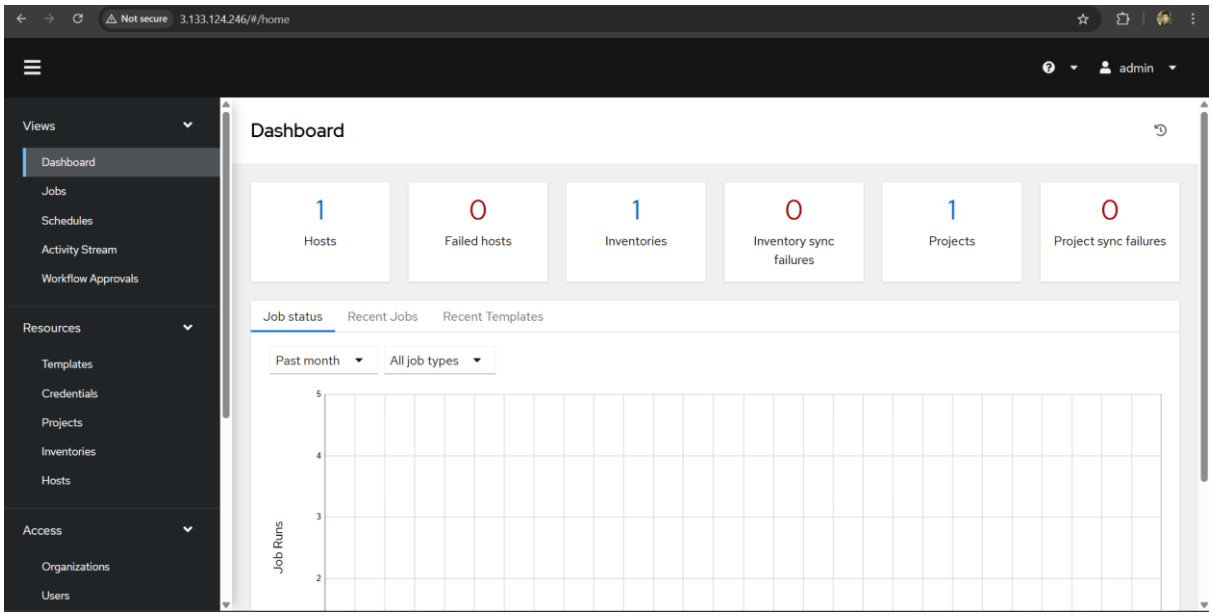
4 sudo apt update && sudo apt install -y ansible

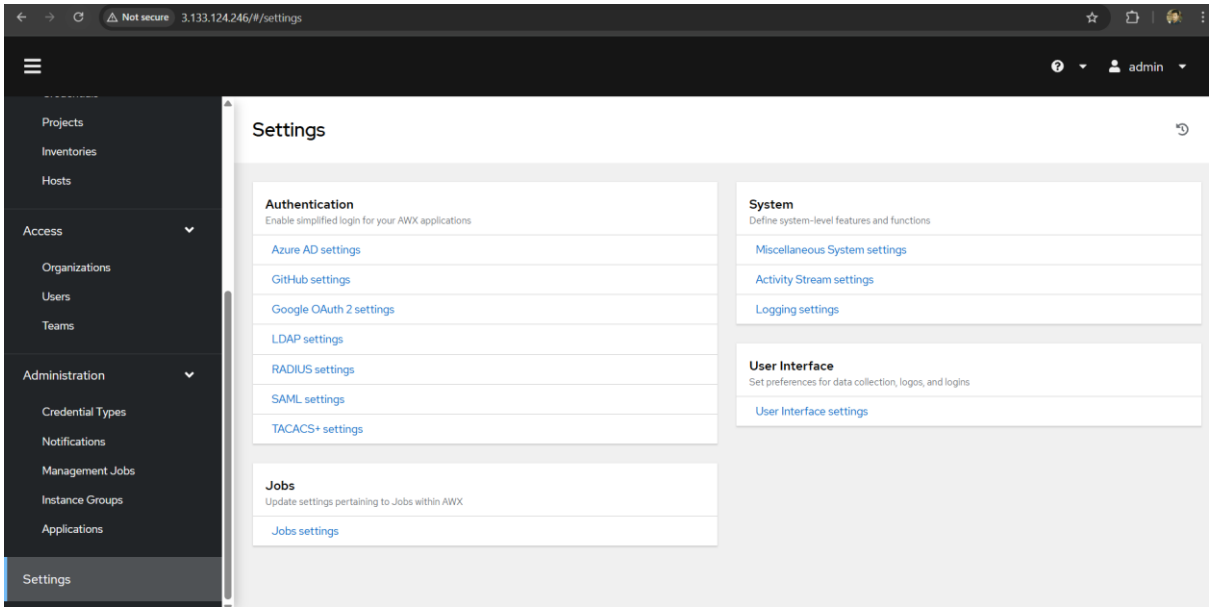
5 which ansible-vault

```
    6  ansible --version
    7  apt install docker
    8  sudo apt remove docker docker-engine docker.io containerd runc
    9  sudo apt update
   10  sudo apt install docker-ce
   11  pip3 install docker==6.1.3
   12  sudo pip3 install docker-compose
   13  sudo apt install apt-transport-https ca-certificates curl software-properties-
common
   14  curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add
-
   15  sudo add-apt-repository "deb [arch=amd64]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
   16  sudo apt update
   17  sudo apt install docker-ce
   18  sudo docker --version
   19  docker ps
   20  systemctl status docker
   21  apt install docker.io
   22  apt install docker-compose
   23  docker-compose version
   24  sudo usermod -aG docker $USER
   25  sudo apt install git vim pwgen -y
   26  sudo git clone https://github.com/ansible/awx.git --branch 17.0.1 --depth 1
   27  cd awx/installer
   28  sudo vi inventory
   29  ansible-playbook -i inventory install.yml
```


changed: [localhost] => (item={'file': 'credentials.py', 'mode': '0600'})
changed: [localhost] => (item={'file': 'docker-compose.yml', 'mode': '0600'})
changed: [localhost] => (item={'file': 'nginx.conf', 'mode': '0600'})
changed: [localhost] => (item={'file': 'redis.conf', 'mode': '0664'})
TASK [local_docker : Render SECRET_KEY file]
changed: [localhost]
TASK [local_docker : Remove AWX containers before migrating postgres so that the old postgres container does not get used]
ok: [localhost]
TASK [local_docker : Run migrations in task container]
changed: [localhost]
TASK [local_docker : Start the containers]
changed: [localhost]
TASK [local_docker : Update CA trust in awx_web container]
changed: [localhost]
TASK [local_docker : Update CA trust in awx_task container]
changed: [localhost]
TASK [local_docker : Wait for launch script to create user]
ok: [localhost]
TASK [local_docker : Create Preload data]
changed: [localhost]
PLAY RECAP
localhost : ok=21 changed=12 unreachable=0 failed=0 skipped=73 rescued=0 ignored=1
root@ip-172-31-3-184:~/awx/installer# history
i-02d06fe73c4a81951 (awx)
PublicIPs: 3.133.124.246 PrivateIPs: 172.31.3.184

→AWS GUI:


Not secure 3.133.124.246/#/home
admin
Views
Dashboard
Jobs
Schedules
Activity Stream
Workflow Approvals
Resources
Templates
Credentials
Projects
Inventories
Hosts
Access
Organizations
Users
Dashboard
1
Hosts
0
Failed hosts
1
Inventories
0
Inventory sync failures
1
Projects
0
Project sync failures
Job status
Recent Jobs
Recent Templates
Past month
All job types
Job Runs
5
4
3
2


Not secure 3.133.124.246/#/settings
admin
Projects
Inventories
Hosts
Access
Organizations
Users
Teams
Administration
Credential Types
Notifications
Management Jobs
Instance Groups
Applications
Settings
Settings
Authentication
Enable simplified login for your AWX applications
Azure AD settings
GitHub settings
Google OAuth 2 settings
LDAP settings
RADIUS settings
SAML settings
TACACS+ settings
Jobs
Update settings pertaining to Jobs within AWX
Jobs settings
System
Define system-level features and functions
Miscellaneous System settings
Activity Stream settings
Logging settings
User Interface
Set preferences for data collection, logos, and logins
User Interface settings