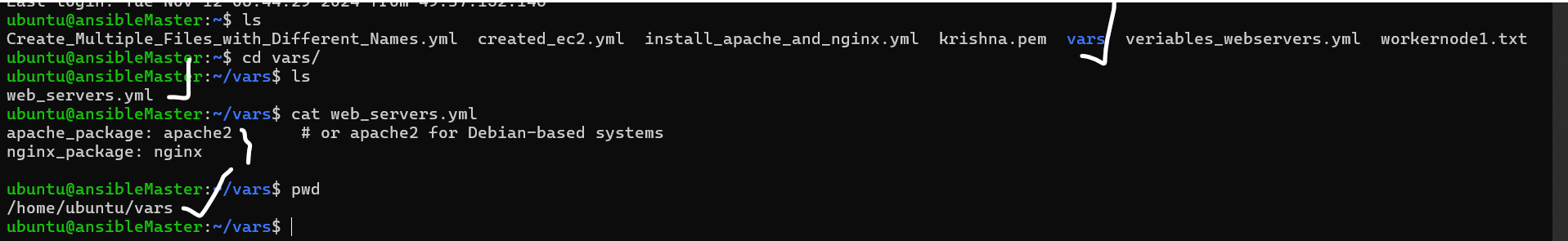
1) Write a single ansible playbook which will install apache and nginx.

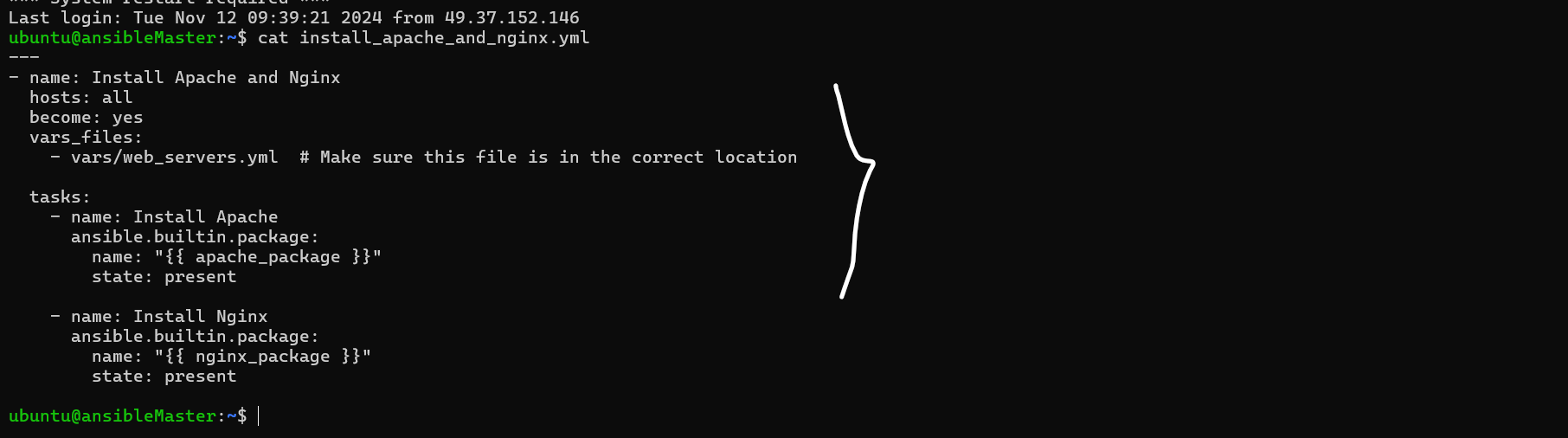
Note: Playbook should not be hardcoded and pass the variables from different file.

So here I am created one folder --- vars

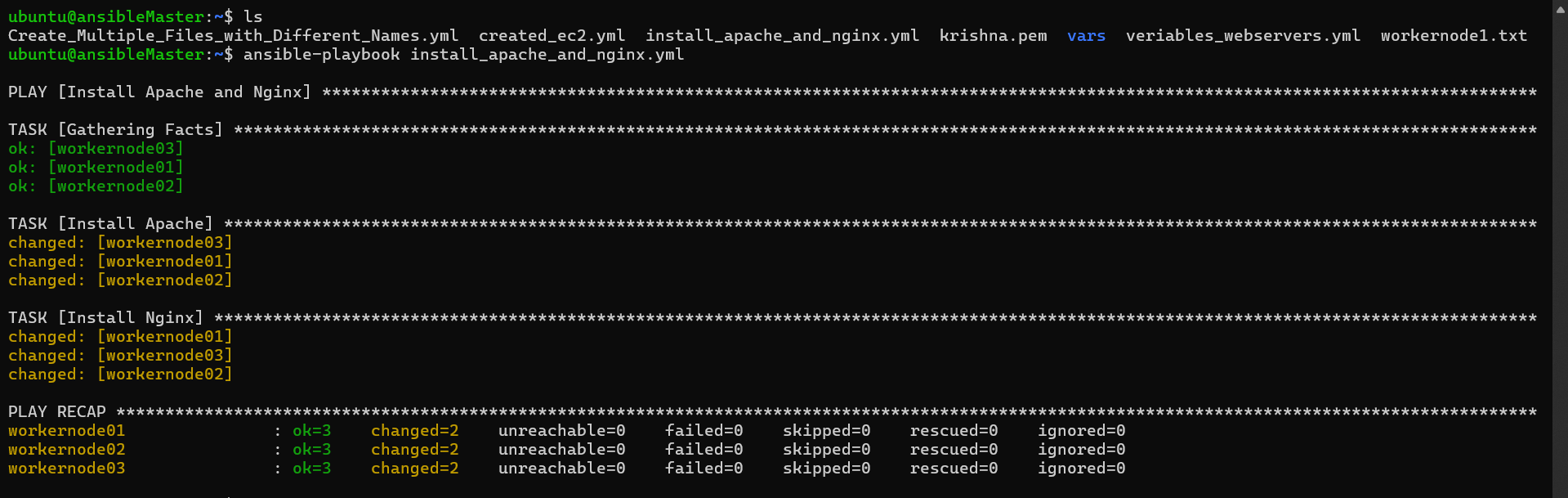
Within the folder I am created one web\_servers.yml



After that I am came again back there I am created one .yml file.



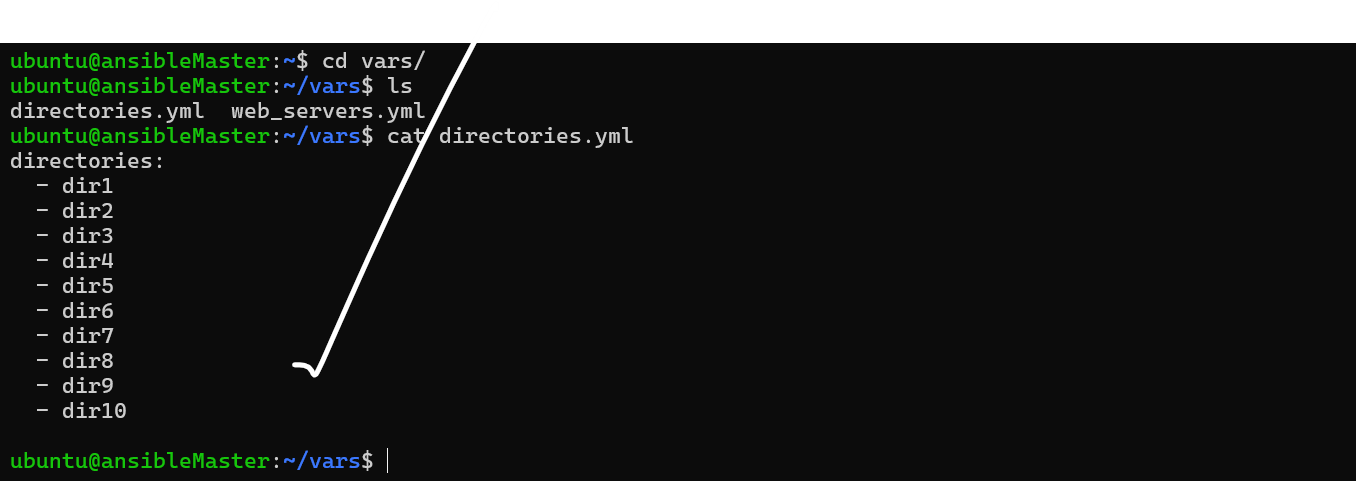
Now I am run the playbook.



Now I want to check in all workernodes.

2) Ansible playbook to create 10 different directories with minimal code and directory names should be passed as variables.

I am created one file in in vars directory with name directories.yml



I am created the one file name create\_directories.yml



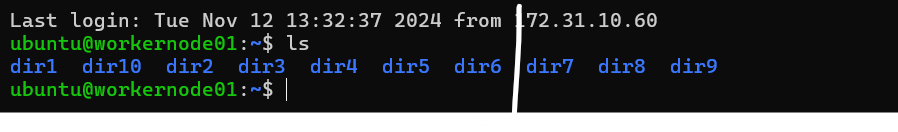
Now I want to run this playbook using the below command.



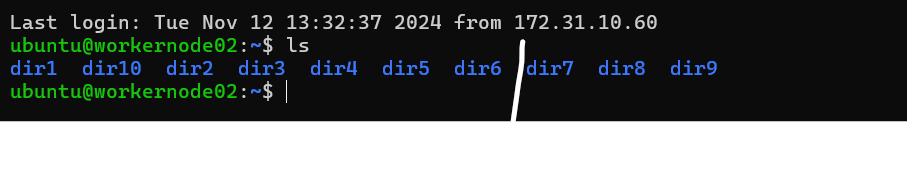


Now I have check the all worker nodes the directories are created or not like these.

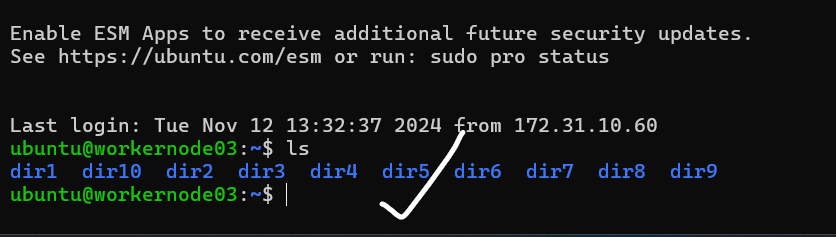
This workernode\_01



This workernode\_02



This workernode\_03



This task is Done!

3) Ansible playbook to copy ssh-keygen from master to worker nodes.

Note:

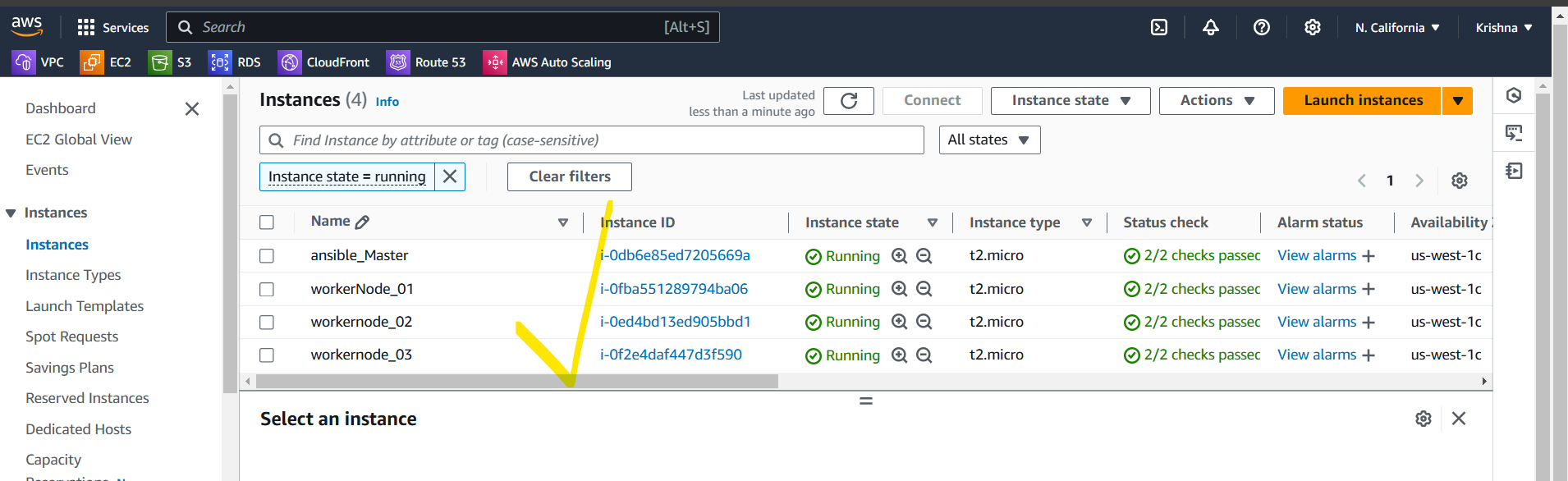
a)Provision new 3 ec2 machines, one master and two worker nodes.

b)Create common user called ansadm and provide sudo priviliges on 3 ec2 instances.

c)Create ssh-keygen in master and you playbook should copy the keygen making it password less

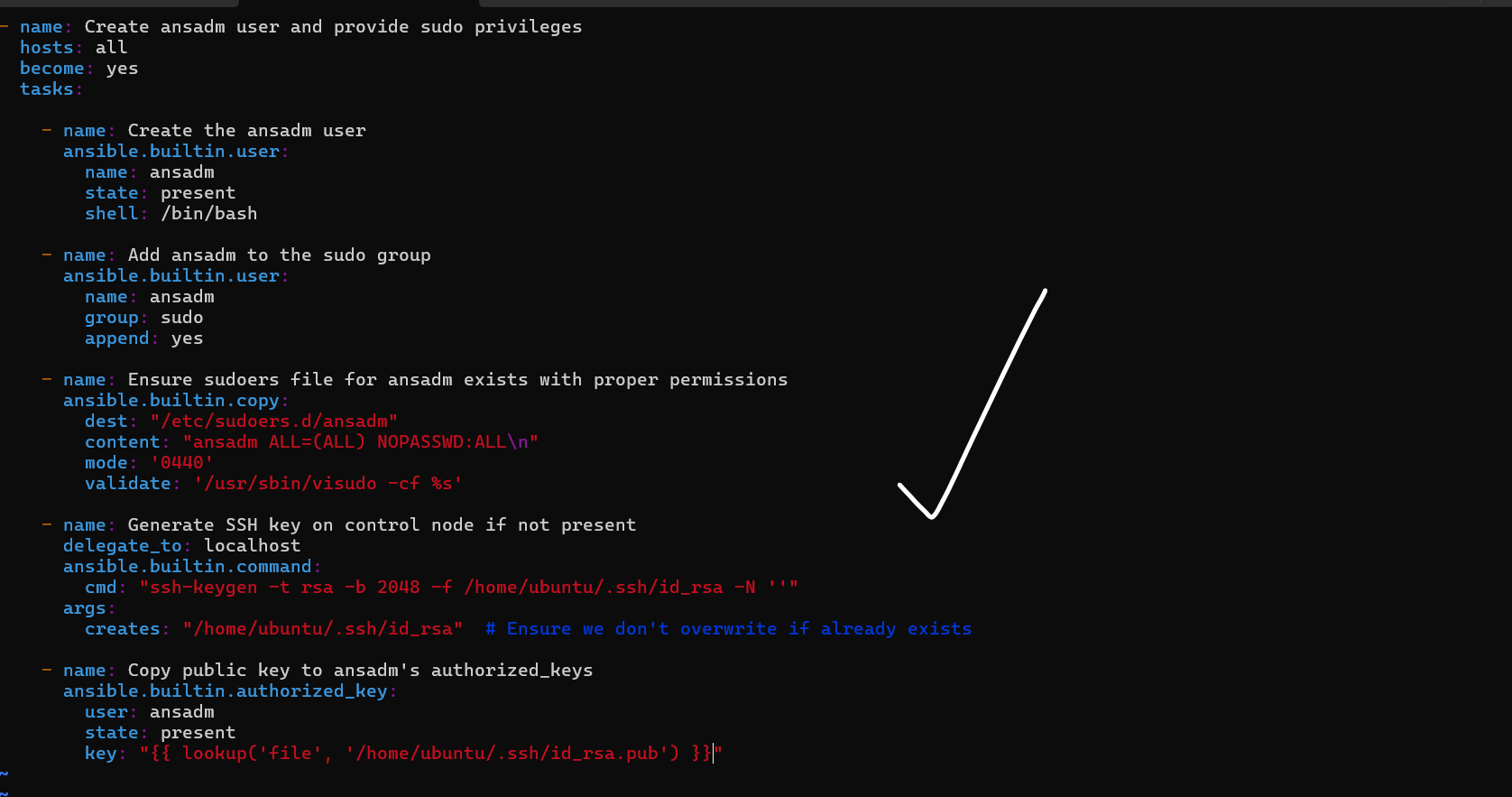
authentication.

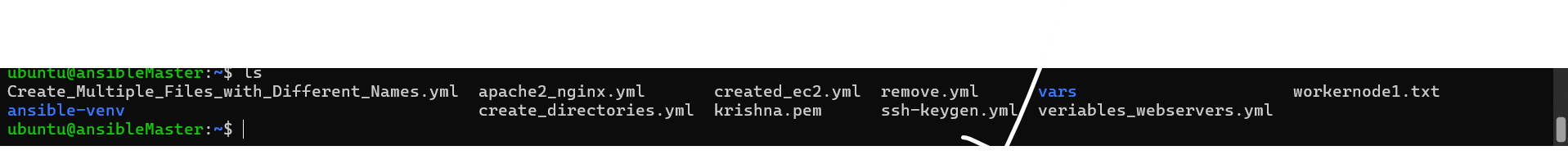
Here my ansible\_master server and worker nodes are available.



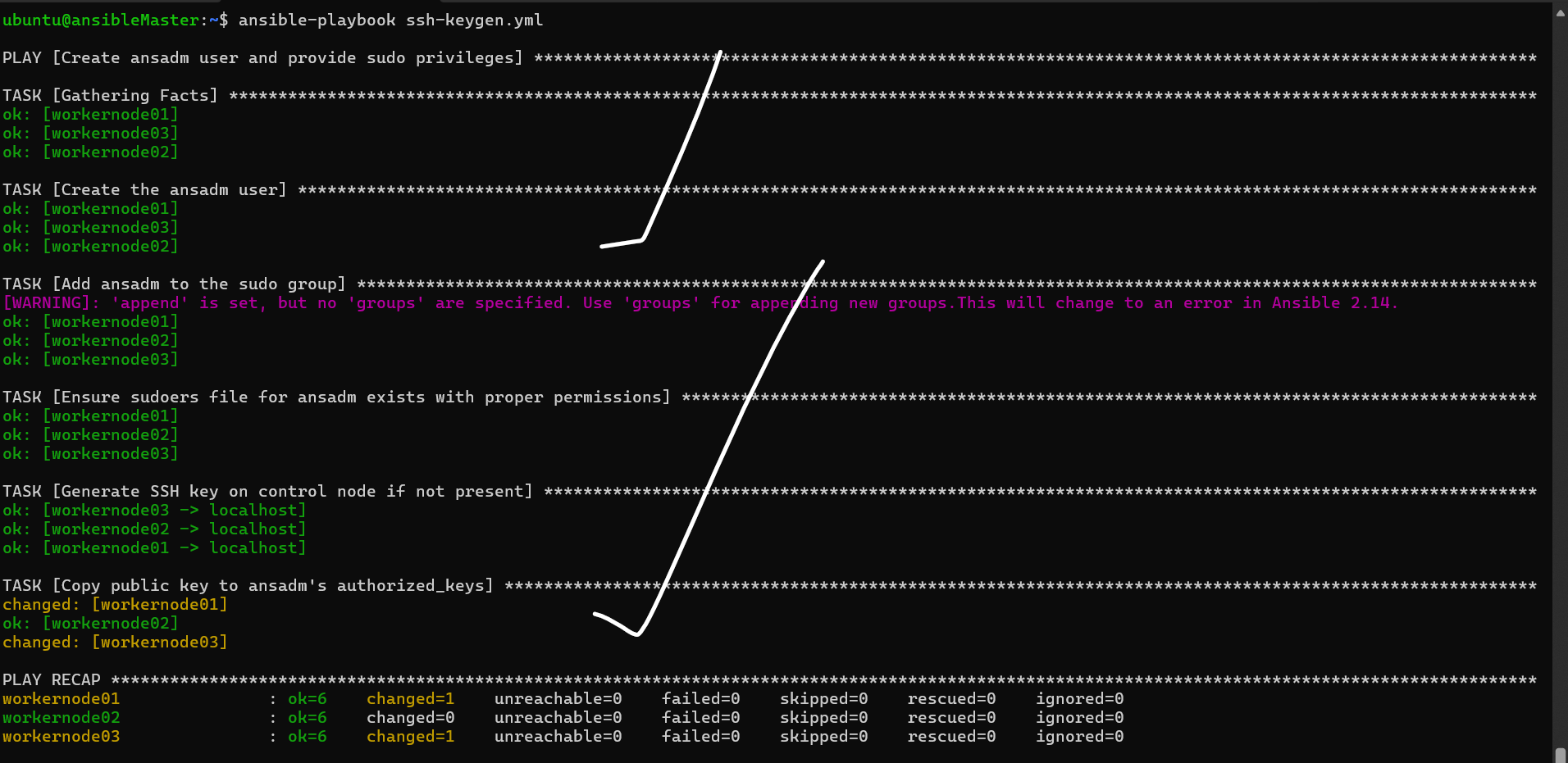
So I am configure in hosts file my all worker nodes.



Now I am created one ssh-keygen.yml file.



Now I want to run the playbook.



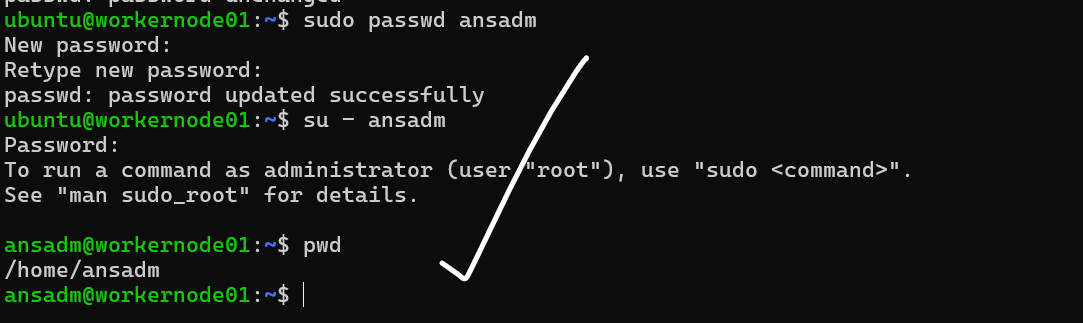
The playbook is successful.

Now I want to check the user is created or not and check the permissions.



Here I want to switch the user ansadm.

Here first I changes the password and switched to this user.



Like this check the all servers.

This workernode2 here also I am changed as ansadm user.

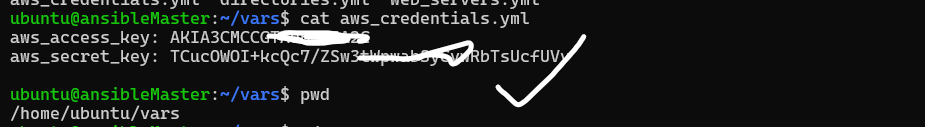


Now this task is successful.

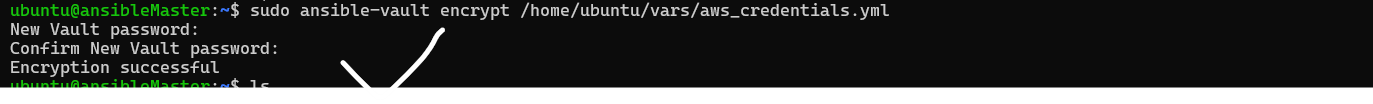
4) Ansible playbook to inject ansible vault variables.

**Ansible Vault** is a feature of Ansible that allows you to encrypt sensitive data, such as passwords, keys, or any other secrets, within playbooks and variables. This data is stored in a secure, encrypted format and can be decrypted only when needed, using a Vault password or key.

The aws\_credentials.yml file contains sensitive information, such as the access key and secret key. To protect this data, it is important to encrypt the file before use.

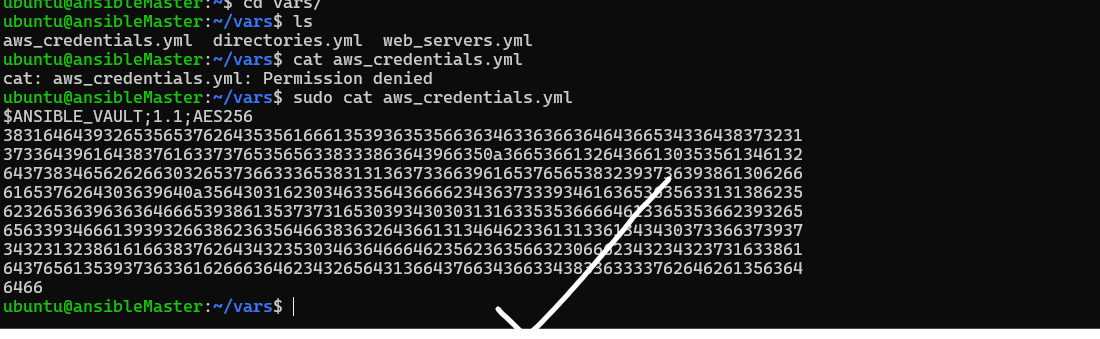


The command sudo ansible-vault encrypt /home/ubuntu/vars/aws\_credentials.yml encrypts the aws\_credentials.yml file to protect its sensitive data using Ansible Vault.

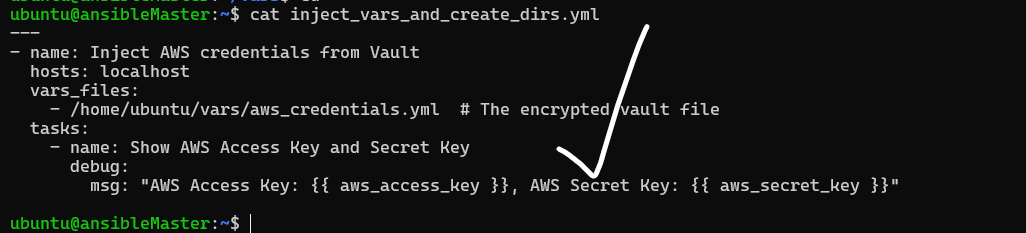


Then comeback /home/ubuntu/vars/ this location.

See here we unable to see the credentials.



To see the see password I am created one playbook.



When I run the playbook to see the credentials.

