TASK – 3

DEVOPS

ASSIGNMENT – 2

BY

TEAM – 9

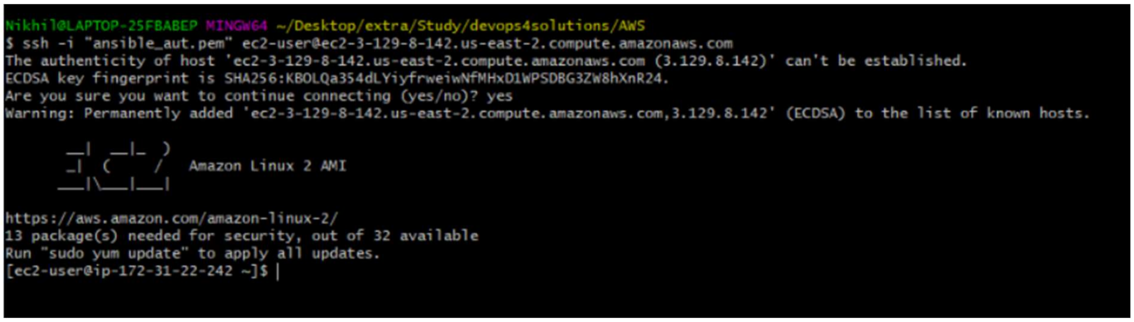
Setup SSH between two AWS EC2 instances using Ansible

- We will create an ansible playbook which will setup a user
- We will use the .pem file which we have associated while launching the instances to connect to the server initially.

Steps

1. Create and Setup AWS EC2 instances
2. SSH to the Ansible master node
3. Setup a new user devops on the Ansible master node manually
4. Run the playbook to setup a devops user on all other nodes
5. If you do not want to create a new user and use the default user like ec2-user,ubuntu then you can skip the creation of user.

Connect to Ansible Master Node using SSH



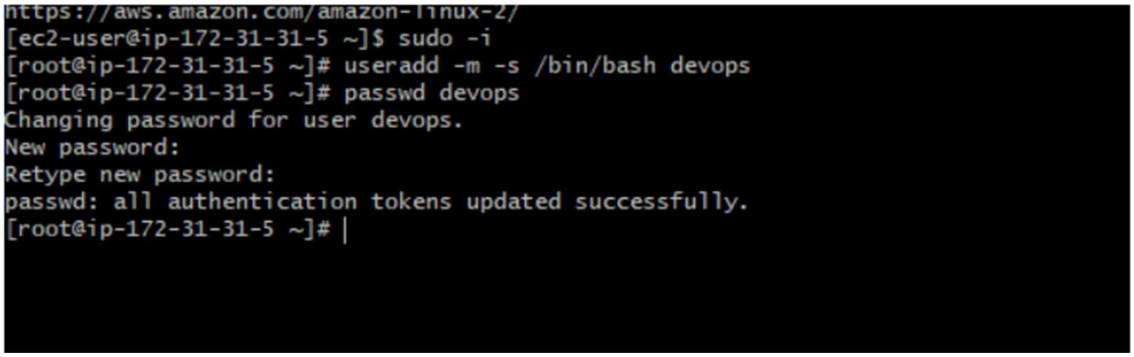
```
Nikhil@LAPTOP-25FBABEP MINGW64 ~/Desktop/extra/Study/devops4solutions/AWS
$ ssh -i "ansible_aut.pem" ec2-user@ec2-3-129-8-142.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-3-129-8-142.us-east-2.compute.amazonaws.com (3.129.8.142)' can't be established.
ECDSA key fingerprint is SHA256:KBOLQa354dLYiyfrweiwNfMHxD1WPSDBG3ZW8hXnR24.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-3-129-8-142.us-east-2.compute.amazonaws.com,3.129.8.142' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 32 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-22-242 ~]$ |
```

Then update it using yum cmd

Then install ansible by the following cmd

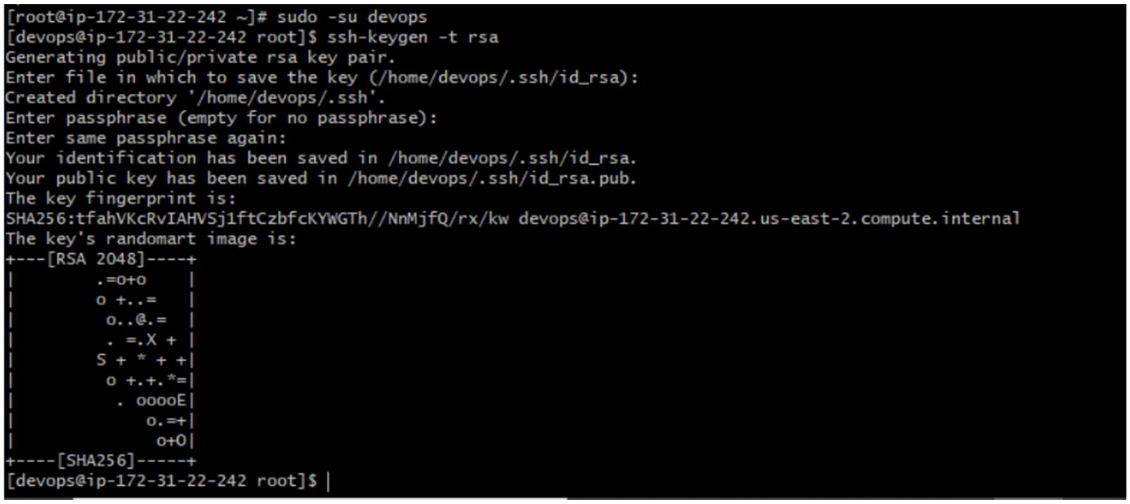
```
sudo amazon-linux-extras install ansible2
```

Setup a devops user on Master Node



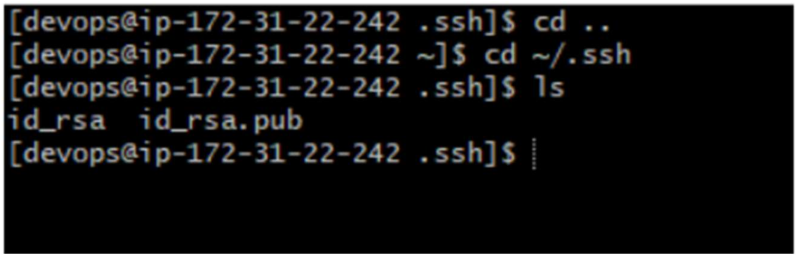
```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-31-5 ~]$ sudo -i
[root@ip-172-31-31-5 ~]# useradd -m -s /bin/bash devops
[root@ip-172-31-31-5 ~]# passwd devops
Changing password for user devops.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-31-5 ~]# |
```

Generate a SSH Key



```
[root@ip-172-31-22-242 ~]# sudo -su devops
[devops@ip-172-31-22-242 root]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/devops/.ssh/id_rsa):
Created directory '/home/devops/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/devops/.ssh/id_rsa.
Your public key has been saved in /home/devops/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:tfahVKcRvIAHVSj1ftCzbfcKYWGTh//NnMjfQ/rx/kw devops@ip-172-31-22-242.us-east-2.compute.internal
The key's randomart image is:
+---[RSA 2048]----+
|        .=o+o    |
|        o +..=   |
|         o..@.=  |
|         . =.X + |
|        S + * + +|
|         o +.+.*=|
|          . ooooE|
|             o.=+|
|              o+O|
+----[SHA256]-----+
[devops@ip-172-31-22-242 root]$ |
```

Now we have to add this public key to all the remote hosts.



```
[devops@ip-172-31-22-242 .ssh]$ cd ..
[devops@ip-172-31-22-242 ~]$ cd ~/.ssh
[devops@ip-172-31-22-242 .ssh]$ ls
id_rsa  id_rsa.pub
[devops@ip-172-31-22-242 .ssh]$
```

Install git and clone the git repo

- Write a playbook to create a new user, set a password, add it to the sudoers file.
- lookup command will try to find the .pub file on the master ansible node for devops user and put that public key in the authorized_keys on the

remote servers. Put the .pub file either on your git repo or anywhere on the master node

```
- name: Add a new user named devops
     user:
          name=devops
          password={{ devops_password }}

   - name: Add devops user to the sudoers
     copy:
          dest: "/etc/sudoers.d/devops"
          content: "devops  ALL=(ALL)  NOPASSWD: ALL"

   - name: Deploy SSH Key
     authorized_key: user=devops
                     key="{{ lookup('file', 'devops_id_rsa.pub') }}"
                     state=present
```

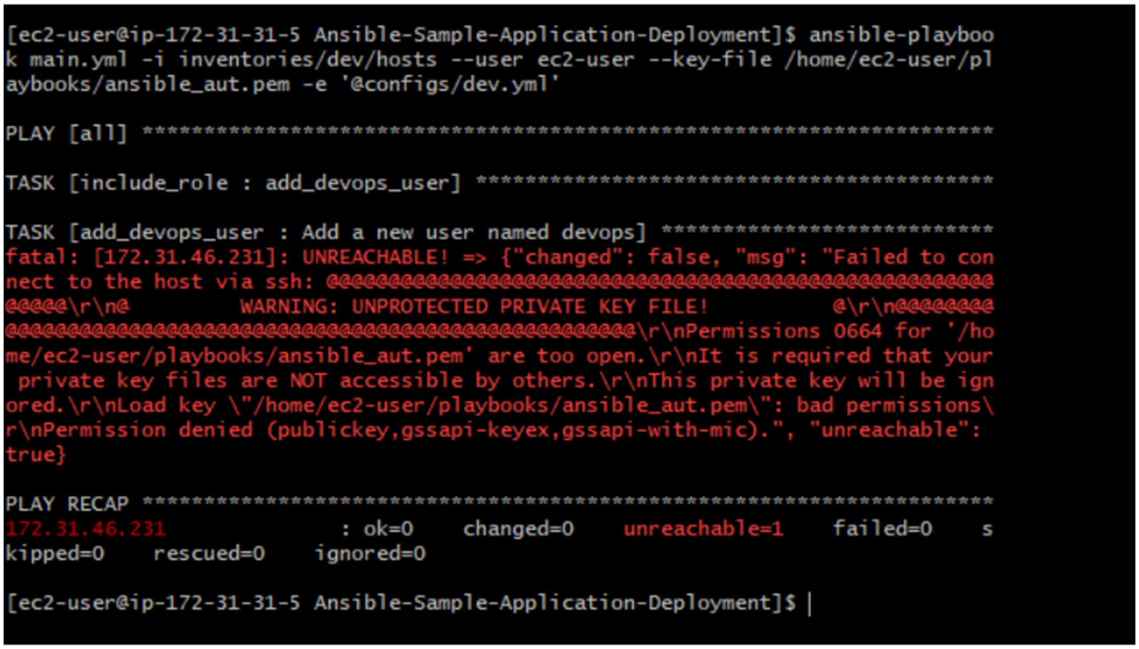
- Playbook to call the above role

```
- hosts: all
  become: true
  become_user: root
  gather_facts: false
  tasks:
    - include_role:
        name: add_devops_user
        tasks_from: add_user.yml
```

How to run the playbook

- You need to provide the user ec2-user and the key to connect to the remote host.
- I am assuming all the remote hosts have same keys
- You need to use the .pem file to connect initially
- PEM file need to have specific permission before you can use it directly. If the permission is not set properly you will see the error “It is required that your private key files are NOT accessible by others. This private key will be ignored.”

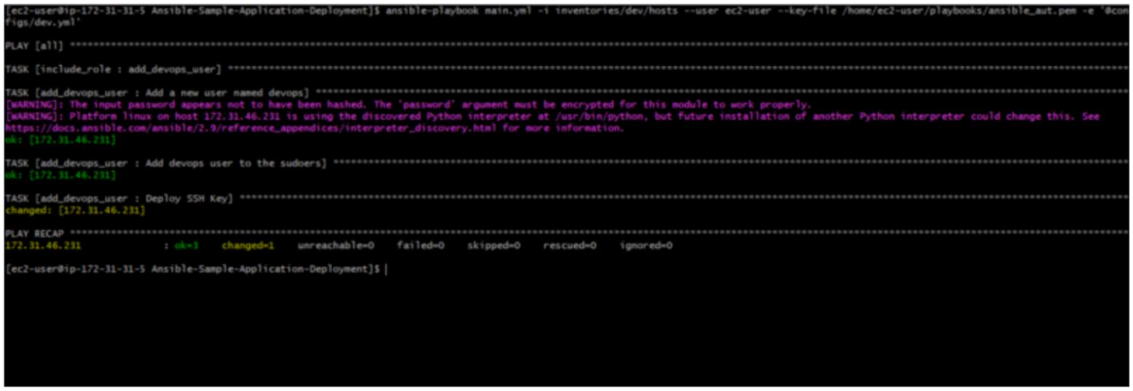
- ansible-playbook main.yml -i inventories/dev/hosts --user ec2-user --key-file ansible_aut.pem -e '@configs/dev.yml'



```
[ec2-user@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ ansible-playboo
k main.yml -i inventories/dev/hosts --user ec2-user --key-file /home/ec2-user/pl
aybooks/ansible_aut.pem -e '@configs/dev.yml'

PLAY [all] *********************************************************************

TASK [include_role : add_devops_user] ******************************************

TASK [add_devops_user : Add a new user named devops] ***************************
fatal: [172.31.46.231]: UNREACHABLE! => {"changed": false, "msg": "Failed to con
nect to the host via ssh: @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@\r\n@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @\r\n@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@\r\nPermissions 0664 for '/ho
me/ec2-user/playbooks/ansible_aut.pem' are too open.\r\nIt is required that your
 private key files are NOT accessible by others.\r\nThis private key will be ign
ored.\r\nLoad key \"/home/ec2-user/playbooks/ansible_aut.pem\": bad permissions\
r\nPermission denied (publickey,gssapi-keyex,gssapi-with-mic).", "unreachable":
true}

PLAY RECAP *********************************************************************
172.31.46.231              : ok=0    changed=0    unreachable=1    failed=0    s
kipped=0    rescued=0    ignored=0

[ec2-user@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ |
```

Now change the permission of the pem file and then re-run the playbook

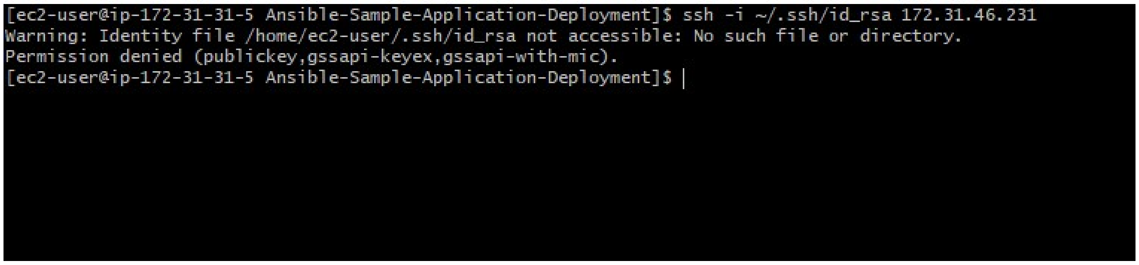
```
sudo chmod 600 ansible_aut.pem
```



```
[ec2-user@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ ansible-playbook main.yml -i inventories/dev/hosts --user ec2-user --key-file /home/ec2-user/playbooks/ansible_aut.pem -e '@con
figs/dev.yml'

PLAY [all] *******************************************************************************************************************************************************************************

TASK [include_role : add_devops_user] ****************************************************************************************************************************************************

TASK [add_devops_user : Add a new user named devops] *************************************************************************************************************************************
[WARNING]: The input password appears not to have been hashed. The 'password' argument must be encrypted for this module to work properly.
[WARNING]: Platform linux on host 172.31.46.231 is using the discovered Python interpreter at /usr/bin/python, but future installation of another Python interpreter could change this. See
https://docs.ansible.com/ansible/2.9/reference_appendices/interpreter_discovery.html for more information.
ok: [172.31.46.231]

TASK [add_devops_user : Add devops user to the sudoers] **********************************************************************************************************************************
ok: [172.31.46.231]

TASK [add_devops_user : Deploy SSH Key] **************************************************************************************************************************************************
changed: [172.31.46.231]

PLAY RECAP *******************************************************************************************************************************************************************************
172.31.46.231              : ok=3    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

[ec2-user@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ |
```

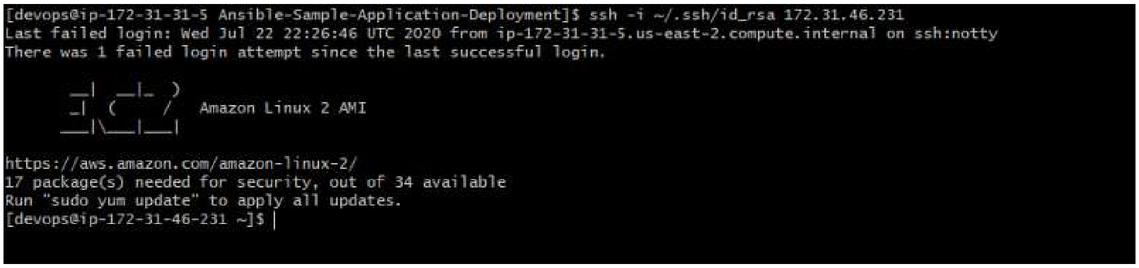
devops user has created successfully and the public key also get copied to the remote servers

- Now try to do the ssh using ec2-user you will still see the “Permission Denied” error, because we have set the devopsuser for ssh connectivity



```
[ec2-user@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ ssh -i ~/.ssh/id_rsa 172.31.46.231
Warning: Identity file /home/ec2-user/.ssh/id_rsa not accessible: No such file or directory.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ |
```

- Now try to ssh using devopsuser



```
[devops@ip-172-31-31-5 Ansible-Sample-Application-Deployment]$ ssh -i ~/.ssh/id_rsa 172.31.46.231
Last failed login: Wed Jul 22 22:26:46 UTC 2020 from ip-172-31-31-5.us-east-2.compute.internal on ssh:notty
There was 1 failed login attempt since the last successful login.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
17 package(s) needed for security, out of 34 available
Run "sudo yum update" to apply all updates.
[devops@ip-172-31-46-231 ~]$ |
```

You have successfully setup the ssh key between two servers.

- Once you setup the devops user then you can use the devops key and run the playbook using devops user