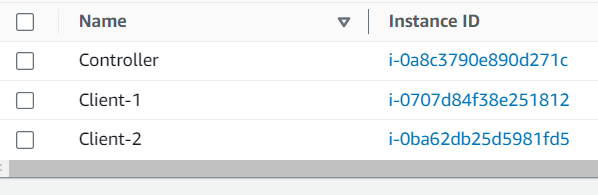
**PASSWORDLESS AUTHENTICATION**

This project helps to eliminate the use of passwords by entering them manually. Instead, we can use the public & private keys for authentication. Following are the steps used to setup password less authentication. All the steps on the server should be performed as a root user only to avoid access issues. This can be very useful when we are working with configuration management tools like ansible/chef/puppet.

1. As a pre-requisite we must have RHEL instances up & running in AWS console.



1. Second step, create a new user & setup a password for the user. If you wish to use same user set the password, by the below command. Repeat this step on controller & clients as well.

Adduser <username>

Sudo passwd <username>

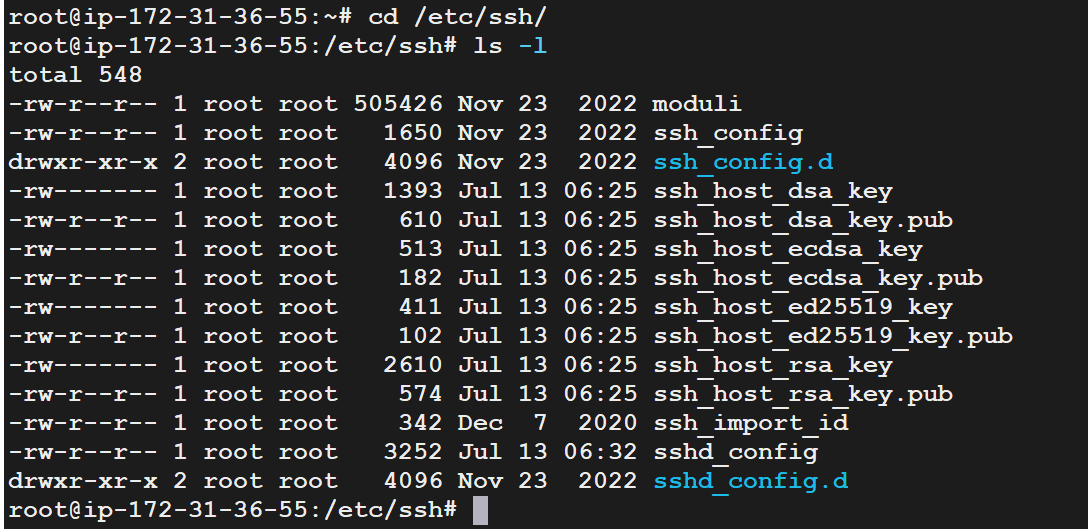
1. Go to the sudo’ers file & add the user. Repeat these steps for controller & clients as well.

visudo

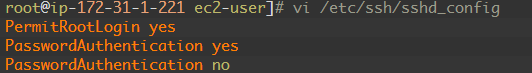


Add the username with ALL=(ALL) & NOPASSWD: ALL for the same.

1. Next step, go to the /etc/ssh directory & edit the sshd\_config file.



Do a vi sshd\_config and edit the below parameters,



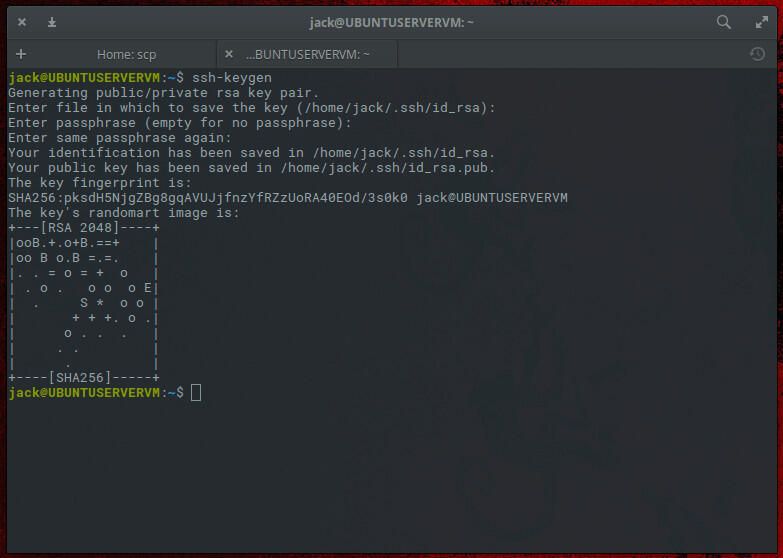
1. After changing the sshd\_config file you have to restart the sshd service by the below command.

Service sshd restart

FOLLOW THE BELOW STEPS ON THE CONTROL NODE

1. Creation of ssh keypair has to be done by the below command. Make sure to use same newly created user to run this command.

Ssh-keygen -t rsa



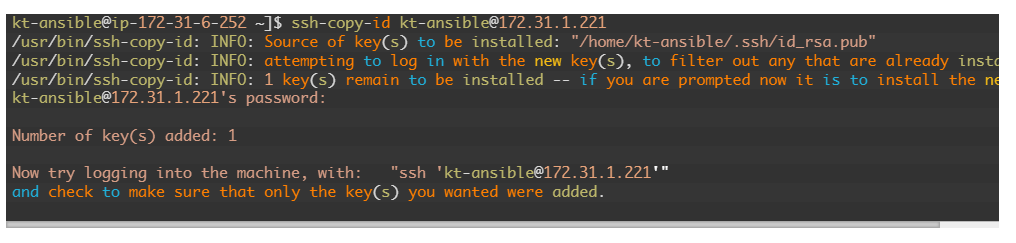
1. Ensure that .ssh/ directories & it’s files are having proper permissions. Private file id\_rsa should have 600 as an octal permission whereas id\_rsa.pub should have 777 as an octal permission.

chmod 600 id\_rsa

chmod 777 id\_rsa.pub

1. Copy the files to the remote nodes by the below commands.

Ssh-copy-id <user-name>@<server-public-ip-address>



1. Please check if the authorized keys are present on the below servers. Switch to the user & then go to .ssh/ folder where you can see authorized keys file.

