#### **SSH Key-based authentication :**

## **Steps to Create a New Sudo User :**

## Log in to your server as the root user.

Use the adduser command to add a new user to your system.

#adduser username

Password : \*\*\*\*\*\*

Re-Password : \*\*\*\*\*\*

Follow the prompts to set the new user's information. It is fine to accept the defaults to leave all of this information blank.

User information prompts:

Changing the user information for username

Enter the new value, or press ENTER for the default

Full Name []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n]

## **Editing Sudoers**

To open up the /etc/sudoers file for editing with visudo simply run sudo visudo.

Before making any edits it's a good idea to check the existing configuration, and understand what everything means. One line you'll definitely encounter is this:

root ALL=(ALL:ALL) ALL

username ALL=(ALL:ALL) ALL OR NOPASSWD:ALL

Open the SSH configuration file /etc/ssh/sshd\_config, search for the following directives and modify as it follows:

/etc/ssh/sshd\_config

PasswordAuthentication no

ChallengeResponseAuthentication no

UsePAM no

Once you are done save the file and restart the SSH service.

On Ubuntu or Debian servers, run the following command:

sudo systemctl restart ssh

Copy

On CentOS or Fedora servers, run the following command:

sudo systemctl restart sshd

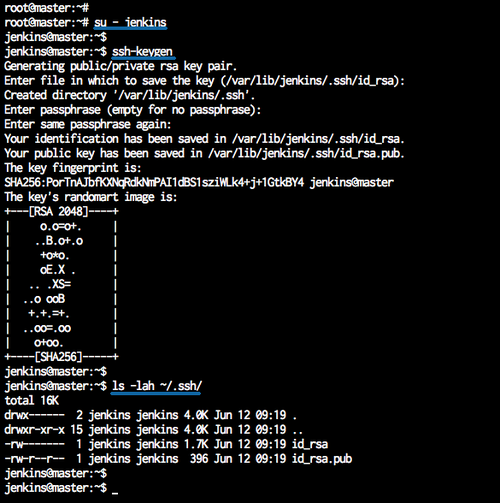
**Generate SSH Key :**

We will be using the ssh key authentication to setup our agent nodes, so we need to generate the ssh key for the Jenkins user and then upload the key to each server node manually using 'ssh-copy-id'.

On the Jenkins master server, login to the Jenkins user and generate the ssh key.

*su - jenkins  
ssh-keygen*

And you will get the 'id\_rsa' private and 'id\_rsa.pub' public key in the '.ssh' directory.



*ssh-copy-id jenkins@10.0.15.21*