Centos

-You should *yum install* *nano* onto your centos machine, otherwise use *vi*

Create a new user: */usr/sbin/adduser username*

Create a new Password: *passwd username*

**Adding User’s Privileges**

Setup new user with root privileges: */usr/sbin/visudo*

Find This – add your new user in the following format



**Setting up password-less SSH**

First step, generate new keys: *ssh-keygen -t rsa -b 4096*

*Go to the directory: cd ~/.ssh*

To copy your pub key to the other machine use: *ssh-copy-id -i id\_rsa.pub root@address*



You should now be able to connect remotely.

On the host machine, you can disable root login.

**Turning off Root SSH & Allowing User’s to SSH In**

Type: *nano /etc/ssh/sshd\_config*

Hit control+^w and type in #PermitRootLogin

Uncomment and change to no



DNS is on by default and you may also want to turn that off.

Lastly, go to the bottom and add the user you created if you want another way to remote in.



**Generating new keys**

You should always generate new keys when working from a cloned machine.

(**If you want to keep a copy of your old keys** move to a new directory before generating new keys.)

To generate new rsa keys: *ssh-keygen -t rsa -f /etc/ssh/ssh\_host\_rsa\_key*

**Recommended use**: *ssh-keygen -t rsa -b 4096*

**Changing SSH Default Port**

**If you change the default SSH port there is more configuration required \*\*coming soon\*\***

­­­­­­­­­­­­­­­­­­­­­­

Reference Links:

1. <http://www.servermom.org/basic-centos-setup-before-building-a-working-server/414/>