Securing Your Server

Add a Limited User Account

Accessing your server as the *root* user will have unlimited privileges and can execute *any* command–even one that could accidentally disrupt your server. We advise you to create limited user accounts and using them to access your server. Administrative tasks will be done using *sudo* to temporarily elevate your limited user's privileges to super user.

Create user

```
adduser example_user
adduser example_user sudo
```

Switch to user account and create the authorized key file (this file should be populated with the public ssh key with which the user can log in into the server). Be very careful to verify your public key is properly copied in authorized keys file. After this process if the key is not properly copied you will loose access to the server.

```
su example_user
cd ~
mkdir -p ~/.ssh && sudo chmod -R 700 ~/.ssh/ && cd .ssh/ && vim authorized_keys
```

Make the root account not accessible for direct login and make the server accessible only through ssh key

```
sudo vim /etc/ssh/sshd_config

PermitRootLogin no
PasswordAuthentication no
```

Remove Password as a requirement to run sudo commands

```
sudo visudo
%sudo        ALL=(ALL) NOPASSWD:ALL
or
example_user    ALL=NOPASSWD: ALL
```

Restart the ssh service for the changes to take affect

```
sudo service ssh restart
```

Checking Config errors in Nginx

```
nginx -t -c /etc/nginx/nginx.conf
```