Initial Server Setup with Debian 7

Authored by: ***ASPHostServer Administrator*** *[asphostserver@gmail.com]*
Saved From: *http://faq.asphosthelpdesk.com/article.php?id=199*

The Basics

After you have deployed your new server instance, it is important to create a new user and provide it with root privileges. This not only makes your virtual server more secure, but also prevents any drastic system damage/change that can happen when operating as root.

1) Root Login

Once you know your IP address, login as the "root" user from the command line.

```
ssh root@xxx.xxx.xx.xx
```

Prompt: Are you sure you want to continue connecting (yes/no)?
Go ahead and type yes.

Potential Warning

If you happen to receive a "man in the middle" warning, this is most likely because another fingerprint is associated with the virtual server's IP. To fix this, simply remove the files in the **.ssh/known_hosts** directory by utilizing the "remove" command:

```
rm .ssh/known_hosts
```

Retry logging in as the root user.

2) Change Your Password

Currently, you do not have a root password with your freshly registered server instance . The next step is to change it to one of your choice from the command line:

```
passwd
```

It will ask you to type and confirm a password of your choice.

3) Create a New User

In this step, we will make a new user and give them all of the root capabilities.

You can make your username whatever you wish. Here, we'll be using "demo"-- simply replace it with your chosen username when applicable.

```
adduser demo
```

After you set the password, you do not need to enter any further information about the new user. You can leave all the following lines blank if you wish.

4) Root Privileges

As of yet, only root has all of the administrative capabilities. We are going to give the new user the root privileges.

When you perform any root tasks with the new user, you will need to use the phrase "sudoâ€• before the command. This is a helpful command for a few reasons, primarily in that it prevents the user from making any system-destroying mistakes and stores all the commands run with sudo to the file "/var/log/secure' (which can be reviewed later if needed).

Let"s go ahead and edit the sudo configuration. This can be done by using a text editor:

```
visudo
```

Find the section called user privilege specification. It will look like this:

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
```

Add the following line right below the root privilege specification, granting all the permissions to your new user:

```
demo    ALL=(ALL:ALL) ALL
```

Type "cntrl x" then 'y' to save and exit the file. Hit 'enter' to return to the command line.

5) SSH as New User

At the moment, you are still logged into the root directory. In the future, login to your server directly with your newly setup username:

```
ssh demo@xxx.xxx.xx.xx
```

However, since you are already logged into your server as root, you can save time by using the sudo command to change over to your new user.

```
su demo
```

Remember, although you are now logged into your new username, you are still operating in the root directory. Simply use the **cd** command in order to switch over to your username's home directory.

Now you're all set!