

STEAL DEALS: [\\$13/YEAR 128MB XEN PV VP...](#) | [\\$25/YEAR 1GB RAM DDOS-PR...](#) |

[\\$9.87/YEAR 1GB RAM SSD V...](#) | [\\$25/YEAR 2.5GB RAM VPS @...](#)

ServerMom

[HOW TO ▾](#)
[TOPICS : ▾](#)
[NEWS](#)
[ABOUT](#)
[SITEMAP](#)
[WRITE FOR US](#)


VPS hosting providers.

HOW TO PASSWORDLESS SSH LOGIN

[Sawiyati](#) | [June 6th, 2014](#) | [How To](#) | [3 Comments](#)



Dedicated Servers \$99

24Shells Dedicated Servers Special Black Friday Promotion ads by BSA

In this guide I'll show you how to use key-based SSH login to your server / vps instead of using username and password. The [tutorial](#) covers Linux to Linux and Windows (PuTTY) to Linux. This adds more security to your server. As usual, this article includes some pictures (screenshot pics) to make everything as clear as crystal.



But first, meet **SSH Key Pairs**! Secure SHell (aka SSH) is not as secure as its name. Crackers who know your server's IP can simply use advanced brute force tool to try login to your server using any possible password combination. I explained [how to change](#) your default username, password and SSH port (*either for [Ubuntu](#) and [CentOS](#)*) as part of basic and common security setup. But now you can bring that basic level to one level up by switching to **passwordless SSH login using key pairs**. Shortly, it is a method to access your server via SSH without entering any password. The advantage, you don't have to remember long yet complicated password plus avoiding brute force attack (even you can still use [Fail2ban](#)).

HOW DOES PASSWORD-LESS SSH LOGIN WORK?

It works by simply comparing public key you share to and stored in remote server **with** private key stored in your local computer or another server you want to connect from. If the keys match, the SSH connection will be established without having to enter password. Obviously you have to firstly generate those private and public keys. This guide is about how to do that.



p.s: Just click on image to see its larger version in case it's not displayed clearly.

PASSWORD-LESS LOGIN: LINUX TO LINUX

This section is aimed for Linux (and Mac) users that need no PuTTY to connect to a server / vps. Or, you may need this just in case if you want to allow login from one of your Linux VPS to another, e.g: to setup rsync to run automatically via cron job.

In this tutorial I use **server 1** to connect it to **server 2** (remote server). Server 1 doesn't have to be a server, it can also be a local computer running your favorite Linux Distro.



HOW TO ADD NEW WEBSITE ON VESTA CP

73 Comments



HOW TO ADD NEW SITE INTO YOUR APACHE-BASED CENTOS SERVER

62 Comments



BASIC CENTOS SETUP BEFORE BUILDING A WORKING

SERVER

59 Comments



HOW TO BUILD OPENVPN SERVER ON

CENTOS 6.X

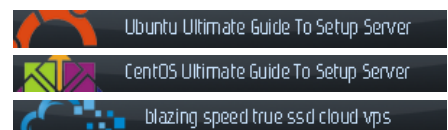
55 Comments



INSTALL VARNISH 3 TO RUN WITH


APACHE 2 ON CENTOS SERVER

45 Comments



Step 1 – Login to server 1 as your favorite username. My server 1 is a playground vps hosted by [Digital Ocean](#) and in this example I login as root so all commands have no *sudo* prefix.

```
login as: root
Access denied
root@1[redacted] 7's password:
[root@play ~]#
```




Step 2 – Now lets generate a pair of public keys using following command:

```
ssh-keygen -t rsa
```

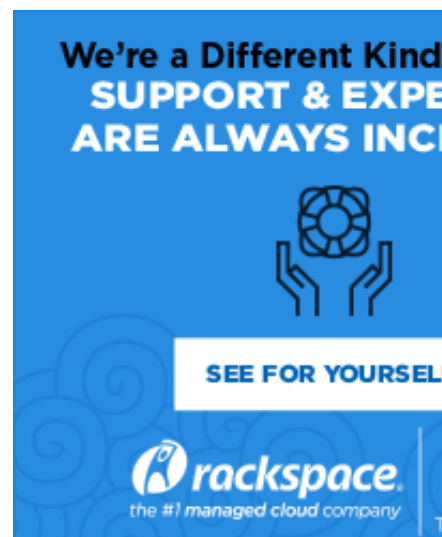
pic:

```
[root@play ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
9b:7c:c0:e2:62:74:bf:6b:85:4f:61:8f:d3:10:ef:b7 root@play.servermom.org
The key's randomart image is:
+--[ RSA 2048 ]-----+
|           .           |
|            o          |
|       .   +   .       |
|    . o So B          |
|   . o +. += + .      |
|  . o . =+ . . .      |
| . . . o.   E         |
|   . o.              |
+-----+
[root@play ~]#
```



As you may see above, simply leave all questions empty. Just hit Enter button on your keyboard several times till you see the key's random art image.

Step 3 – Now login to server 2 (*the remote server you want to password-less SSH login to*) from inside server 1. You can login as a user or as root. In this example I'll login as user called servermom. Use this command:



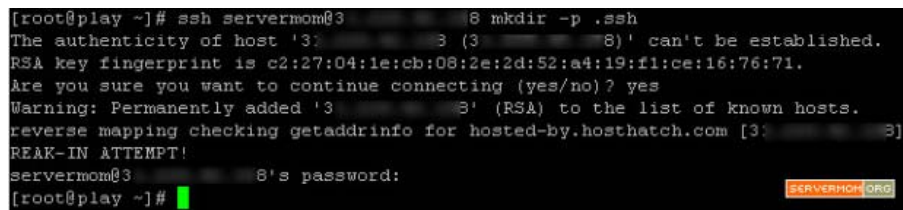
```
ssh username@xxx.xxx.xxx.xxx mkdir -p .ssh
```

or, if you've configured SSH to [run on](#) non default / standard port (other than 22) then use this instead:

```
ssh -p 21000 username@xxx.xxx.xxx.xxx mkdir -p .ssh
```

replace xxx.xxx.xxx.xxx with actual IP address of your server 2 and replace username with actual username. Also replace 21000 with actual port number of your SSH configuration.

pic:



```
[root@play ~]# ssh servermom03 8 mkdir -p .ssh
The authenticity of host '3: 3 (3 8)' can't be established.
RSA key fingerprint is c2:27:04:1e:cb:08:2e:2d:52:a4:19:f1:ce:16:76:71.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '3 3' (RSA) to the list of known hosts.
reverse mapping checking getaddrinfo for hosted-by.hosthatch.com [3: 3]
REAK-IN ATTEMPT!
servermom03 8's password:
[root@play ~]#
```

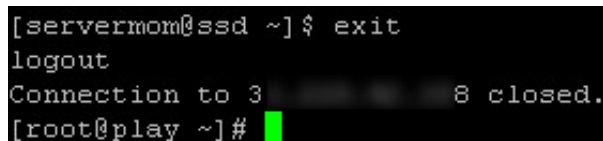
What the command does is logging in plus creating new directory called **.ssh** in server 2. If asked (first time), type **yes** hit Enter and type in your password.

p.s: My server 2 here is hosted by [HostHatch](#).

Step 4 – Next, exit from server 2 and back to server 1. Type:

```
exit
```

pic:



```
[servermom03sd ~]$ exit
logout
Connection to 3 8 closed.
[root@play ~]#
```

Step 5- Now issue this command to copy generated public key to server 2.

```
cat .ssh/id_rsa.pub | ssh username@xxx.xxx.xxx.xxx 'cat >> .ssh/
```

example:

```
[root@play ~]# cat .ssh/id_rsa.pub | ssh servermom@3 'cat >> .ssh/authorized_keys'
reverse mapping checking getaddrinfo for hosted-by.hosthatch.com [31.220.42.158] failed - POSSIBLE
REAK-IN ATTEMPT!
servermom@3: 8's password:
[servermom@3 ~]#
```

do not forget to enter you password and replace username and xxx.xxx.xxx.xxx with actual ones.

Step 6 – Do not also forget to set permissions on .ssh directory and authorized_keys file stored in server 2.

```
ssh username@xxx.xxx.xxx.xxx "chmod 700 .ssh; chmod 640 .ssh/authorized_keys"
```

in my case it's seen like this:

```
[root@play ~]# ssh servermom@3 'chmod 700 .ssh; chmod 640 .ssh/authorized_keys'
reverse mapping checking getaddrinfo for hosted-by.hosthatch.com [31.220.42.158] failed - POSSIBLE
REAK-IN ATTEMPT!
servermom@3: 8's password:
[servermom@3 ~]#
```

That's all. You can now try SSH-ing to server 2 (remote vps) from server 1 (local computer or another vps).

```
ssh username@xxx.xxx.xxx.xxx
```

pic:

```
[root@play ~]# ssh servermom@3
reverse mapping checking getaddrinfo for hosted-by.hosthatch.com [31.220.42.158] failed - POSSIBLE
REAK-IN ATTEMPT!
Last login: Fri Jun  6 20:01:42 2014 from 162.245.216.87
[servermom@ssd ~]$ uptime
 20:20:27 up 127 days,  2:19,  1 user,  load average: 0.00, 0.00, 0.00
[servermom@ssd ~]$
```

This time you won't be asked to enter password.

PASSWORD-LESS LOGIN: WINDOWS (VIA PUTTY) TO LINUX

This guide will make use of Putty to reach your Linux server / vps via SSH. First time using Putty? Read my previous article on [where to download and how to use Putty](#).

Step 1 – Download additional software called PuTTYgen a.k.a PuTTY key generator from its [official page here](#) or from link below:

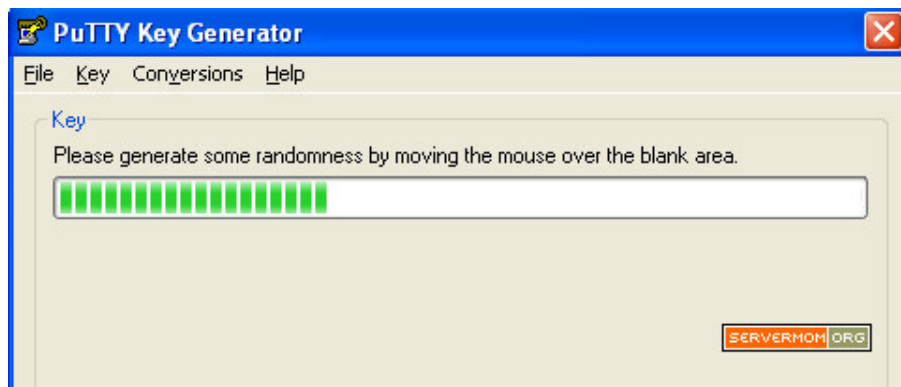
<https://app.box.com/s/rvqly0vIr9gxtzie2g1t>

Step 2 – Launch up Puttygen tool up. If you are on Windows 7 or upper version, right-click on it and select Run as Administrator.



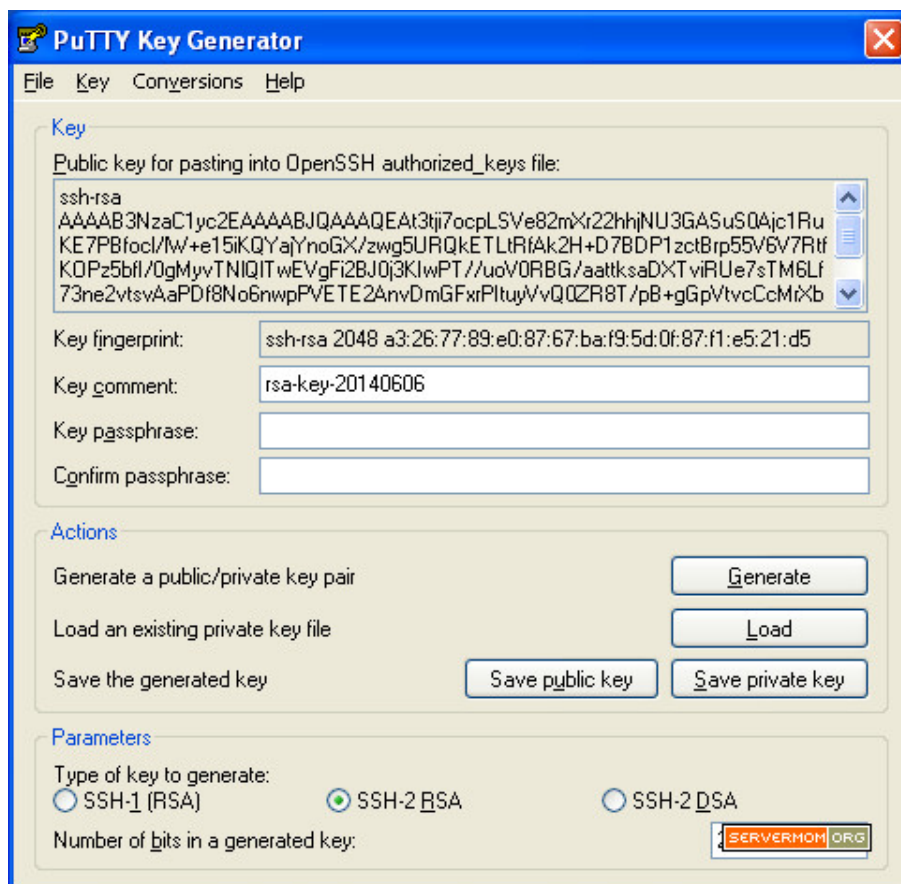
Step 3 – Normally, to create a new key, you have to select the parameters at the bottom that match your requirements. But however the default values will work great so for this example leave it as it is. The key point is make sure you select **SSH-2 RSA** because it is better and more secure than **SSH-1** and **SSH-2 DSA**. You can also increase the value in “*Number of bits in a generated key*” from 2048 to 4096 for stronger key – make it harder to crack.

Now hit the **Generate** button.



When the progress is the phase like pic above, make sure you move your mouse over and over again to boost the generator.

Step 4 – Once done, you'll see something like this:



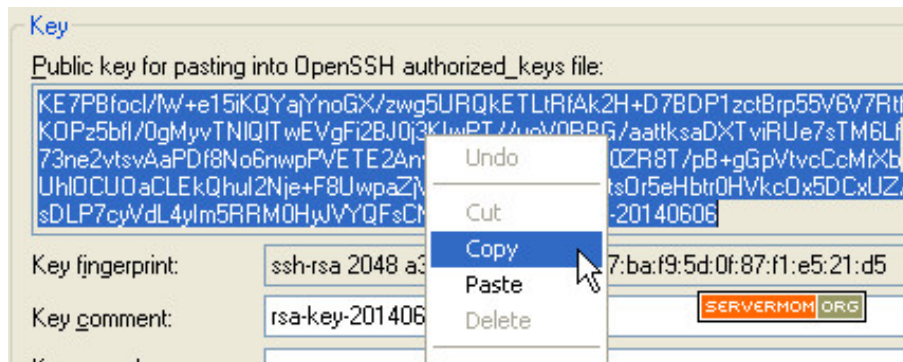
Step 5 – Login back to your server 2 (remote server / vps) and issue following lines of command:

```
mkdir -p .ssh
chmod 700 .ssh
nano .ssh/authorized_keys
```

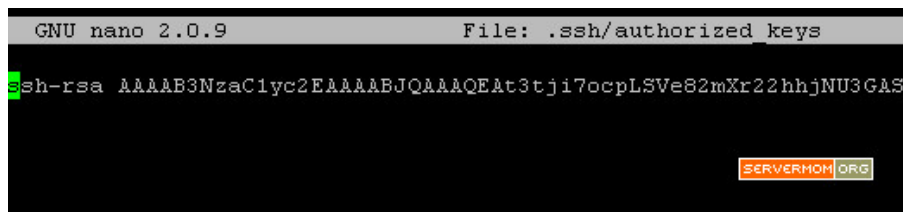

pic:

```
login as: servermom
Access denied
servermom@1:~$ 7's password:
[servermom@play ~]$ mkdir -p .ssh
[servermom@play ~]$ chmod 700 .ssh
[servermom@play ~]$ nano .ssh/authorized_keys
```

then copy the generated public key in PuttyGen:



and paste it in Nano editor:



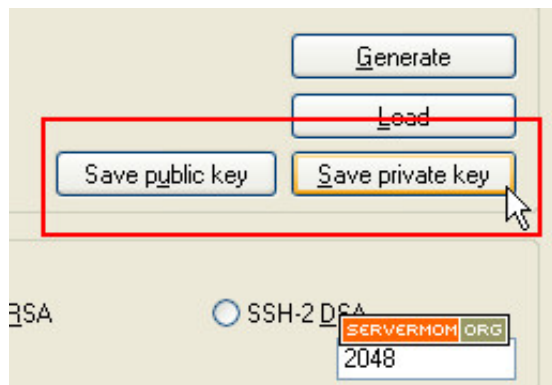
Save and exit Nano by hitting Control+O then Control+X on your keyboard. Next, change its permission to 644:

```
chmod 644 .ssh/authorized_keys
```

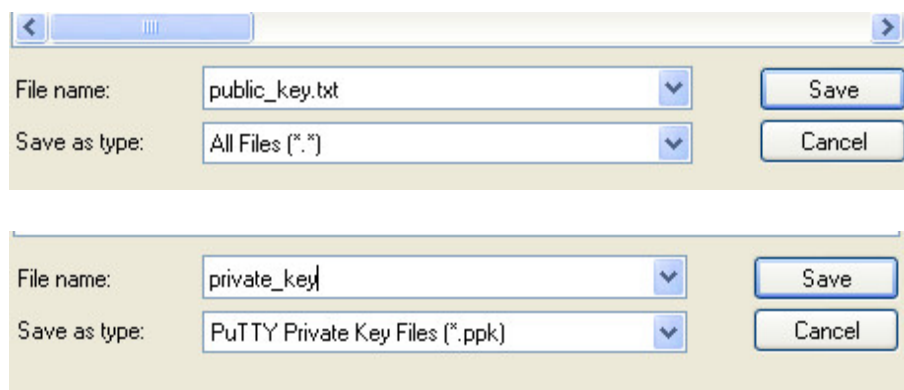
pic:

```
[servermom@play ~]$ mkdir -p .ssh
[servermom@play ~]$ chmod 700 .ssh
[servermom@play ~]$ nano .ssh/authorized_keys
[servermom@play ~]$ nano .ssh/authorized_keys
[servermom@play ~]$ chmod 644 .ssh/authorized_keys
[servermom@play ~]$
[servermom@play ~]$
```


Step 6 – Now exit and go back to Puttygen. Next, you'll need to save the Private Key and Public Key (to use later). Simply hit the appropriate buttons.

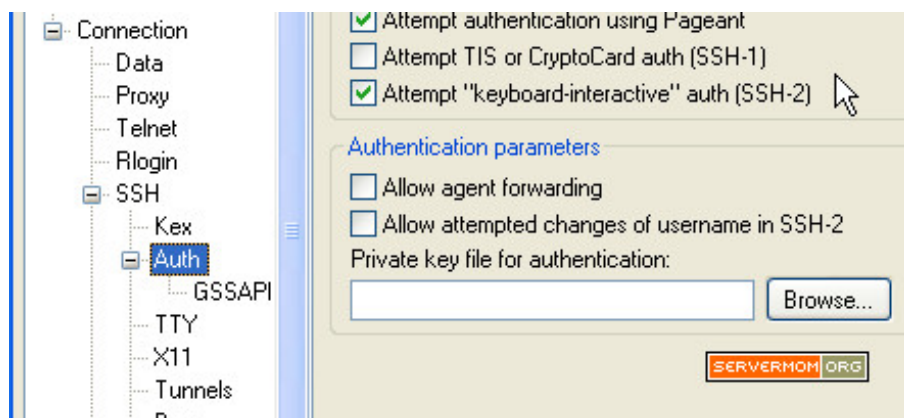


Make sure you save Public Key as **.txt** while Private Key as **.ppk**.



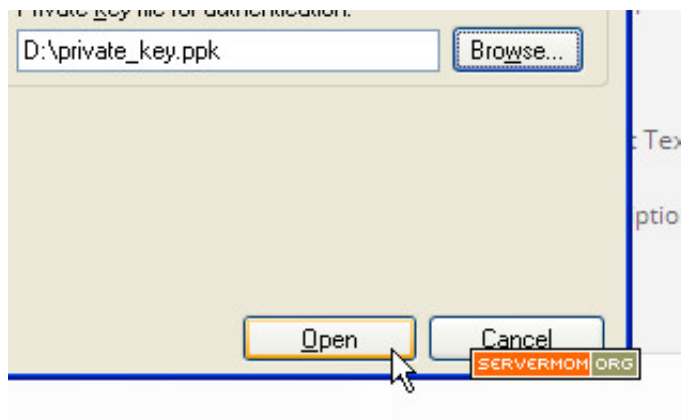
When saving Private key you'll be asked to confirm saving without Passphrase, chose **No**.

Step 6 – Let's configure Putty to use that newly generated key. So open it up and go to **Connection > SSH > Auth**.

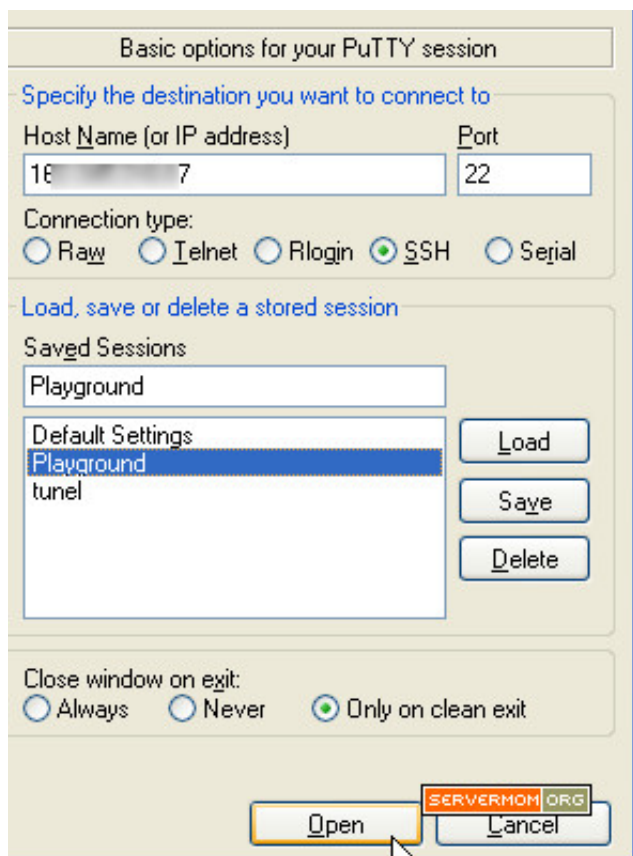


Step 7 – Click the **Browse** button and locate the private key (.ppk)

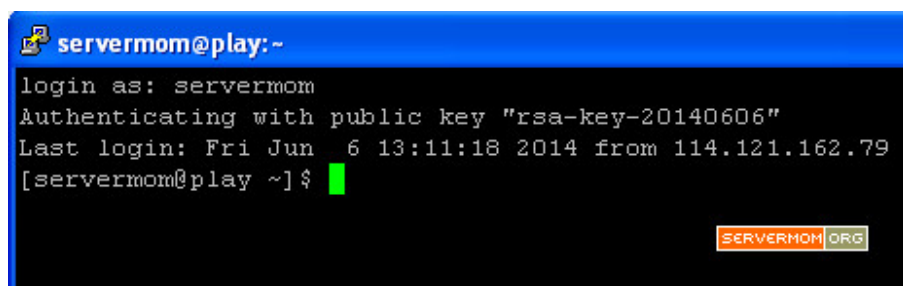
you've just saved.



Step 8 – Now go back to main page on Putty and login as usual:



Step 9 – That's it. Upon clicking the Open button Putty will logging you in without asking for password:



OPTIONAL – BUT IMPORTANT

Once you've followed steps above, you'll be able to login either by using password **or** using ssh keys. However, you can also choose only 1 login method which in this case is SSH key-based login.

Follow steps below to **disable password-based SSH login**:

Step 1 – Edit sshd config file using your favorite text editor:

```
nano /etc/ssh/sshd_config
```

Step 2 – Now look for this line:

```
#PermitRootLogin yes
```

or,

```
PermitRootLogin no
```

Step 3 – Change that to:

```
PermitRootLogin without-password
```

Step 4 – Save that file and exit (in Nano: Control+O, then Control+X).

That's it.

Do not forget to follow me on twitter [@servermomdotcom](#) [or download](#) my [official Android app](#) to get faster update.

SHARE THIS:



Facebook 12



Twitter 1



Google+



Reddit

RELATED POSTS



HOW TO BUILD WORKING CENTOS SERVER WITH

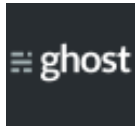
LIGHTTPD AND PHP5 (PART 4)

4 Comments | May 18, 2013



HOW TO ADD NEW WEBSITE ON VESTA CP

73 Comments | Dec 31, 2013



HOW TO RUN GHOST WITH VARNISH CACHE

2 Comments | Jan 27, 2014



HOW TO INSTALL FAIL2BAN TO PROTECT SERVER FROM BRUTE FORCE SSH LOGIN ATTEMPTS (UBUNTU)

7 Comments | Mar 8, 2013

ABOUT THE AUTHOR



Sawiyati

Hi! I'm Sawiyati, a mom with passion about blogging, programming and everything techy. Having no offline job, so I decided to start blogging while

learning what I love for. You can find me at Google+ [here](#).

3 COMMENTS



Dhavid Claudius Gunawan | June 8, 2014

[Reply](#)

artikelnya mirip2 sama yang saya buat, cuma lebih detail



Greg | June 16, 2014

[Reply](#)

Is it safe to use the root user with SSH Key Pairs? Or is it safer to create a new user?

If you are using passwordless SSH login, I also think it is a good idea to prevent login with passwords by changing
`/etc/ssh/sshd_config`

PermitRootLogin without-password



davies | October 22, 2014

[Reply](#)

You rock ! Servermom. Linux is easier with you.

ADD A COMMENT

Your email address will not be published. Required fields are marked *

Name: *

Email Address: *

Website:

Comment: *

ADD COMMENT

Notify me of follow-up comments by email. ☐

Notify me of new posts by email. ☐

REVIEW



5+ FREE SELF-HOSTED SERVER MONITORING TOOLS



15+ LOW END CLOUD SERVER PROVIDERS



USEFUL FREE UPTIME MONITORING SERVICES FOR YOUR SERVER



RECOMMENDED VPS #3: CRISSIC



LIST OF FREE DNS HOSTING PROVIDERS FOR POINTING DOMAIN TO YOUR VPS



RECOMMENDED VPS #4: INIZ

ServerMom

COPYRIGHT © 2014 [SERVERMOM](http://www.servermom.org).

[CONTACT US](#)

[PARTNER US](#)

[PRIVACY POLICY](#)

[DISCLAIMER](#)

