

Table Of Contents

Table Of Contents 1

Step # 1: Delete old ssh host keys 2

Step # 2: Reconfigure OpenSSH Server 2

Step # 3: Update all ssh client(s) known_hosts files 2

[Home](#) > [Faq](#) > [Debian / Ubuntu](#)

Ubuntu / Debian Linux Regenerate OpenSSH Host Keys

Posted by [Vivek Gite](#) <vivek@nixcraft.com>

This entry is part 1 of 2 in the series [openssh](#) ^[1]

[openssh](#) ^[1]

- Ubuntu / Debian Linux Regenerate OpenSSH Host Keys
- [Run SSH In The background After Running a GUI Linux Application](#) ^[2]

Q. How do I regenerate OpenSSH sshd server host keys stored in /etc/ssh/ssh_host_* files? Can I safely regenerate ssh host keys using remote ssh session as my existing ssh connections shouldn't be interrupted?

A. To regenerate keys you need to delete old files and reconfigure openssh-server. It is also safe to run following commands **over remote ssh session**. Your **existing session shouldn't be interrupted**.



[3]

Step # 1: Delete old ssh host keys

Login as the root and type the following command:

```
# /bin/rm /etc/ssh/ssh_host_*
```

Step # 2: Reconfigure OpenSSH Server

Now create a new set of keys, enter:

```
# dpkg-reconfigure openssh-server
```

Sample output:

```
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
Restarting OpenBSD Secure Shell server: sshd.
```

Step # 3: Update all ssh client(s) known_hosts files

Finally, you need to update ~/.ssh/known_hosts files, otherwise everyone will see an error message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
f6:67:01:41:e6:20:06:4b:4b:fa:4b:c1:f1:45:45:e0.
Please contact your system administrator.
Add correct host key in /home/vivek/.ssh/known_hosts to get rid of this message.
Offending key in /home/vivek/.ssh/known_hosts:12
RSA host key for 202.54.xx.abc has changed and you have requested strict checking.
Host key verification failed.
```

Either remove [host fingerprint](#) ^[4] or update the file using vi text editor.

Series Navigation

[Run SSH In The background After Running a GUI Linux Application»](#) ^[2]

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/howto-regenerate-openssh-host-keys/>

URLs in this post:

[1] openssh: <http://www.cyberciti.biz/faq/series/openssh/>

[2] Run SSH In The background After Running a GUI Linux Application: <http://www.cyberciti.biz/faq/run-ssh-gui-background-for-unix-x11/>

[3] Image: <http://www.cyberciti.biz/faq/faq/category/debian-ubuntu/>

[4] host fingerprint: <http://www.cyberciti.biz/faq/warning-remote-host-identification-has-changed-error-and-solution/>

Copyright © 2006-2010 [nixCraft](#). All rights reserved. This print / pdf version is for personal non-commercial use only. More details <http://www.cyberciti.biz/tips/copyright>.