
Connectivity using ssh, rsync & vsftpd

A Presentation for the 2005 Linux Server Boot Camp
by David Brown

David has 15 years of systems development experience with EDS, and has been writing Linux-based real-time data acquisition systems for Rolls-Royce in Indianapolis since 1999. He has been a member of the CINLUG Board of Directors for the past 2 years.

What is OpenSSH?

- OpenSSH is a FREE version of the SSH (Secure Shell) suite of network connectivity tools that increasing numbers of people on the Internet are coming to rely on.
- Many users of telnet, rsh, rlogin, ftp, and other such programs might not realize that their password is transmitted across the Internet unencrypted, but it is. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

Installing/Starting OpenSSH

- `apt-get install ssh`
(Installs ssh, rssh and openssh-server.)
- `update-rc.d -f ssh defaults 20`
(Sets up the server to run at default run levels.)
- `/etc/init.d/ssh`
(Use start, stop, or restart to control the server.)
- `pgrep sshd`
(Check to see if the server is running.)
- Don't forget to uninstall telnetd or turn it off if it is on.

Using SSH to remote login

- `ssh -l <user> <host>`
- `ssh <user>@<host>`
- `ssh <host>`

The first time you login, a warning will appear and if you type “yes” then the host key which is in `/etc/ssh/ssh_host_rsa_key.pub` will be added to your `~/.ssh/known_hosts` file. The warning will not appear on next login.

If a warning appears that WON'T let you login, it may be that ssh has been reinstalled or the hardware has changed. Removing the line corresponding to the remote server from `~/.ssh/known_hosts` will fix the problem.

Using SSH to run remote commands

- `ssh <host> “uptime”`
- `ssh <user>@<host> “ls -al”`
- `ssh root@<host> “shutdown -r now”`

(Be careful however! To disable root logins edit the `/etc/ssh/sshd_config` file and set `PermitRootLogin` to “no” and restart `sshd`.)

Using scp and sftp

An alternative to rcp and ftp is to use secure copy (scp) and secure ftp (sftp)

- `scp /etc/hosts root@<host>:/tmp`
(Copies local hosts file to remote /tmp folder.)
- `scp root@<host>:/etc/hosts /tmp`
(Copies remote hosts file to local /tmp folder.)
- `sftp <host>`
help, ls, put, get, quit, etc.

Using SSH to login without passwords

- `ssh-keygen -t rsa`
(Generates a public RSA key in file `~/.ssh/id_rsa.pub` on the local host.)
- `ssh-copy-id -i ~/.ssh/id_rsa.pub <user>@<host>`
(Adds a line to `~/.ssh/authorized_keys` file on the remote host.)
- Be sure `RSAAuthentication` & `PubkeyAuthentication` are set to “yes” in `/etc/ssh/sshd_config`. Now you can freely move about without typing your password.

X11 forwarding with SSH

- Server-side: The file `/etc/ssh/sshd_config` must have `X11Forwarding` set to “yes.”
- Client-side: To make it the default for all users, `/etc/ssh/ssh_config` must have `X11Forward` set to “yes.”
- Only use X11 forwarding on trusted systems otherwise turn it off and invoke it manually:

```
ssh -X <user>@<host>
```
- It isn't necessary to set `DISPLAY`, “echo `$DISPLAY`” to see something like: `localhost:10.0`

What is rsync?

- rsync is a replacement for rcp that has many more features and can be used in conjunction with ssh.
- rsync uses an algorithm which provides a very fast method of synchronizing remote files. It does this by only sending the differences in the files across the link!
- rsync can update entire directory trees and filesystems while preserving ownership, permissions, times, links, and devices!

Installing rsync

- apt-get install rsync
(Installed by default with ubuntu-standard package.)
- rsyncd doesn't have to be running to use rsync via ssh
(See /usr/share/doc/rsync/examples/rsyncd.conf, & in /etc/default/rsync set `RSYNC_ENABLE=true`.)
- Ubuntu rsync is compiled to use ssh by default, on some systems you must use the `--rsh=ssh` option.

-a (archive) -z (compress) -v (verbose) -n (dryrun)

Using rsync with SSH

- `rsync -avz <host>:/var/log /log`
(All files on remote host `/var/log` sync'd to `/log/log`.)
- `rsync -avz /var/log/ <host>:/log`
(All files in `/var/log` sync'd to remote host `/log`.)
- `rsync -avz <host>:/home/<user> /backup`
(`<user>` files on `<host>` sync'd to local `/backup/<user>`.)
- `rsync -avz --exclude="*[cC]ache*" <host>:/home/<user> /backup`
(Same as above but cache files are excluded.)

What is vsftpd?

- vsftp is the Very Secure FTP Daemon.
- It is a lightweight, efficient FTP server written with security in mind.
- vsftp supports both authenticated and anonymous FTP, PAM authentication, bandwidth limiting, and SSL encryption support.
- If sftp and ssh are not enough for your system, then consider using vsftpd.

Authenticated and Anonymous FTP

- **Authenticated FTP**

Users with IDs on the system can use this method to send and retrieve files from the system after providing username and password. vsftpd can be configured to allow all or only groups of privileged users to use FTP.

- **Anonymous FTP**

Anonymous FTP allows users to login as username “anonymous” with an email address as a password. This way, the public can download (and upload if configured) files to the default /home/ftp directory.

Installing vsftpd

- vi /etc/apt/sources.list to include Ubuntu Internet sources in addition to the default CDROM sources.
- apt-get install vsftpd
- The scripts will setup vsftpd to run and it will be by default an anonymous FTP server with no uploading.
- pgrep ftp
(Check to see if vsftpd is running.)
- /etc/init.d/vsftpd
(Use stop, start, or restart to control the server.)

Configure vsftpd via /etc/vsftpd.conf

- `anonymous_enable=no` (disables anonymous logins.)
- `local_enable=yes` (enables local users to login and use FTP.)
- `write_enable=yes` AND `anon_upload_enable=yes` (enables anonymous uploads, but also a location must be created: `mkdir /home/ftp/pub/upload;`
`chmod 722 /home/ftp/pub/upload.`)
- `anon_mkdir_write_enable` (enables anonymous directory creation.)
- Default log file may be changed from `/var/log/vsftpd.log` (`xferlog_file`)
- Default banner may be changed (`ftpd_banner`)
- After any changes use `/etc/init.d/vsftpd` script to restart the server.
- `max_clients`, `max_per_ip`, `anon_max_rate`, `local_max_rate` tunes server limits for max clients, max connections per IP, and transfer rates.

Restrict users via /etc/ftpusers

- By default root users are not allowed to login. Unless you are on a very secure local network with no connection to the outside, “root” should remain in the /etc/ftpusers file. Commenting root out of the file will allow root users to use FTP.
- This should be avoided! Use scp and sftp instead!

Windows/Linux Connectivity

- Cygwin (Free Linux BASH shell for Windows as well as ssh, rsync, ftp, sftp and a very good Cygwin/X Windows server.)

WWW.CYGWIN.COM

- PuTTY (A free Telnet/SSH client for windows.)

WWW.PUTTY.NL

- Filezilla (A free FTP/SFTP GUI client for windows.)

FILEZILLA.SOURCEFORGE.NET

References and Links

- OpenSSH (www.openssh.com)
- rsync (samba.anu.edu.au/rsync)
- vsftpd (vsftpd.beasts.org)
- Ubuntu Linux (www.ubuntulinux.org)
- Linux Home Networking
(www.linuxhomenetworking.com)
- TheOpenCD (www.theopencd.org)