

RE: vsftpd beginner's tutorial?

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2003-10/2741.html>

From: Richardson, Robert (*RRichardson_at_activision.com*)

Date: 10/29/03

To: redhat-list@redhat.com

Date: Wed, 29 Oct 2003 13:20:45 -0800

Hi,

Due to the many requests for my documentation, I am releasing it to the list, as is. It is long, because I try to document as much as possible.

Anyway, I hope that it helps all of you who desire it.

Robert Richardson
Activision Studios

+++++

```
# This file was created to illustrate the steps needed to create a new FTP
Server.
# This server will be configured with Redhat 9.0 and in the vsftpd format.
# Author: Robert Richardson, Activision Studios
# Date: 08/03/2003
# Definition: Create a Very Secure FTP Server.
#
```

SUMMARY OF STEPS

VSFTP Server Configuration steps:

1. System Specifications.
2. Why vsftpd as this FTP Server?
3. Hardware Considerations.
4. Physical disks layout.
5. System kernel upgrade procedures.
6. System software customization considerations.
7. User requirements.
8. User and Group Configuration
9. Creating a chroot (jail) environment.
10. System security requirements.
11. Networking considerations.
12. Configure with postfix.
13. System transition.
14. Windows user connectivity
15. System disk space growth considerations.
16. System recovery requirements.

DETAILS OF STEPS

VSFTP Server Configuration steps:

1. System Specifications.

- A. Disk Space: 104.1 GB
- B. Processor: 731.057 MHz
- C. Memory: 1030988k
- D. CPU: Intel Pentium III (Coppermine)

2. Why vsftpd as this FTP Server? (See <http://vsftpd.beasts.org/>).

A. Security

I. The vsftpd server was design to fix security problems found in other

ftp servers such, BSD-FTP, WU-FTP, and proftp.

II. It solves buffer overflow problems with secure encoding techniques.

III. VSFTPD has the ability to prevent FTP Server saturation by throttling the bandwidth.

IV. All remote network data is done in a process running as an unprivileged user.

V. All operations are handled only in a small privileged parent process.

VI. All requests are distrusted.

VII. After login the privileged parent dynamically calculates what privileges it requires.

VIII. vsftpd does not use an external /bin/lis program because of exploitation risks.

IX. vsftpd avoids using library calls which are also exploitable.

B. Performance

I. 2,500 users were handled concurrently on specific RedHat download servers during a 24 hour period.

II. A more aggressive cache files can be obtained via a small kernel modification.

III. VSFTPD has the ability to prevent FTP Server saturation by throttling the bandwidth.

IV. VSFTPD has been benchmarked over localhost at 70Mbyte/sec.

C. Stability

I. It is used by some well known FTP servers, such as ftp.redhat.com, ftp.suse.com, ftp.gnu.org, and others.

3. Hardware Considerations.

A. Red Hat Hardware Compatibility Listings shows:

- Dell – PowerEdge 4400 x86-based Certified Server Red Hat Linux 9.0 (US)

B. Memory is NOT important for a dedicated FTP server, about 256 MB RAM is sufficient for a very big server, smaller servers can do well with 64 MB RAM.

RedHat: RE: vsftpd beginner's tutorial?

Network connections would still be the most important factor.

4. Physical disks layout.

A. The proposed physical layout is as follows:

I. Configured with Disk Druid as:

I. Configured with Disk Druid as:

```
/dev/sda1 150MB /boot  
/dev/sda2 2000MB swap  
/dev/sda3 500MB /  
/dev/sda4 extended  
/dev/sda5 2500MB /usr  
/dev/sda6 2000MB /tmp  
/dev/sda7 2000MB /home  
/dev/sda8 750MB /var  
/dev/sda9 92500MB /data
```

II. Final layout with "fdisk -l /dev/sda" gives:

```
Device Boot Start End Blocks Id System  
/dev/sda1 * 1 19 152586 83 Linux  
/dev/sda2 20 274 2048287+ 82 Linux swap  
/dev/sda3 275 338 514080 83 Linux  
/dev/sda4 339 13275 103916452+ 5 Extended  
/dev/sda5 339 720 3068383+ 83 Linux  
/dev/sda6 721 975 2048256 83 Linux  
/dev/sda7 976 1230 2048256 83 Linux  
/dev/sda8 1231 1326 771088+ 83 Linux  
/dev/sda9 1327 13275 95980311 83 Linux
```

5. System kernel & software upgrade procedures.

I. Install Redhat 9.0 without X Window System.

6. System software customization considerations.

A. Install without X Window System.

B. VSFTPD FTP Server Software Install.

I. Mount RH 9.0 disk 1.

II. rpm -Uvh /mnt/cdrom/RedHat/RPMS/libcap-1.10-8.i386.rpm

III. Mount RH 9.0 disk 3.

IV. rpm -Uvh /mnt/cdrom/RedHat/RPMS/vsftpd-1.1.3.i386.rpm

V. vi /etc/xinetd.d/vsftpd

```
service ftp  
{  
  disable = no <-- Change from yes to no.  
  socket_type = stream  
  wait = no  
  user = root  
  server = /usr/sbin/vsftpd  
  nice = 10  
  per_source = 5  
  instances = 200  
  banner_fail = /etc/vsftpd.busy_banner  
}
```

VI. vi /etc/vsftpd.conf

```
#anonymous_enable=YES  
ascii_upload_enable=YES  
ascii_download_enable=NO
```

RedHat: RE: vsftpd beginner's tutorial?

```
async_abor_enable=YES
xferlog_file=/var/log/vsftpd.log
xferlog_enable=YES
idle_session_timeout=120 # 2 minutes
data_connection_timeout=300 #5 minutes
#To limits a single client to ~50kbytes / sec download speed.
anon_max_rate=50000
#To disable "ls -R", to prevent it being used as a DoS attack.
ls_recurse_enable=NO
# You may fully customise the login banner string:
ftpd_banner=Welcome to the our FTP server
chroot_list_enable=YES
```

VII. service xinetd restart

VIII. touch /etc/vsftpd.chroot_list <--This file is populated by the account_creation script.

IX. chmod 600 /etc/vsftpd.chroot_list

X. echo "421 Server busy, please try later." >

/etc/vsftpd.busy_banner

C. Invoke software quota on.

I. vi /etc/fstab

```
#Add usrquota after the word defaults
```

```
LABEL=/data /data ext3 defaults,usrquota 1 2
```

II. mount -o remount,usrquota /data

III. quotacheck -c /data #Creates a data file called /data/aquota.user

IV. quotaon /data

V. Get quota information on all accounts using the repquota -a" and format into

the specific quota categories. Eg. quotas_100MB, quotas_256MB, quotas_1GB,

quotas_3GB, and quotas_5GB.

VI. Run the set_quotas.sh script.

VII. OTHER QUOTA COMMANDS:

```
edquota <username> #Edits the quota limits for <username>.
```

```
edquota -p <olduser> <newuser> #Copies the same quotas of <olduser> to <newuser>.
```

```
edquota -t #Edit the soft time limits for each file system.
```

```
repquota -a #To get a formatted quota usage report on all users (good for cron).
```

```
/etc/warnquota.conf #Modify this file to warn users via email, etc.
```

```
quotastats #Displays some stats about quotas.
```

```
"quotacheck -avcugm" #Generates the /home/aquota.usr & /home/aquota.group files
```

D. Fix manpage character caret problem:

I. cd /etc/sysconfig

II. vi i18n

```
LANG="en_US" <--Changed from en_US.UTF-8
```

```
SUPPORTED="en_US.UTF-8:en_US:en"
```

RedHat: RE: vsftpd beginner's tutorial?

7. User service xinetd restart requirements.
 - A. Software Quota on for all FTP user accounts.
 - I. vi /etc/fstab
LABEL=/data /data ext3 defaults,usrquota 1 2
 - B. There is an option for users to get either 100MB, 250MB, 1GB, or 5GB when the account_creation script is executed.
 - C. Quota limits above 250MB for other users are allotted according to specific needs.
8. User and Group Configuration
 - A. Use the "useradd" command to install system administration users (/home), and the fake accounts that will determine the quota for FTP accounts users. The default configuration will be the /etc/default/useradd file.
 - I. Create the system administration user accounts:
 - B. Create the FTP directory.
 - I. mkdir /data/ftp
 - C. Create the ftponly group.
 - I. groupadd -g 5000 ftponly
 - D. Create the 100MB, 250MB, 1GB fake accounts. These accounts will be used to automatically designate new users their quota.
 - I. useradd -d /data/ftp/ftp100 -u 502 -s /bin/bash ftp100
 - II. useradd -d /data/ftp/ftp250 -u 503 -s /bin/bash ftp250
 - III. useradd -d /data/ftp/ftp1GB -u 504 -s /bin/bash ftp1GB
 - IV. useradd -d /data/ftp/ftp3GB -u 506 -s /bin/bash ftp3GB
 - V. useradd -d /data/ftp/ftp5GB -u 505 -s /bin/bash ftp5GB
 - VI. useradd -d /data/ftp/ftp500 -u 507 -s /bin/bash ftp500
 - VII. useradd -d /data/ftp/mondo -u 508 -s /bin/bash mondo
 - VIII. useradd -d /data/ftp/ftp10GB -u 509 -s /bin/bash ftp10GB
 - IX. cd /data/ftp ; chown root:root * ; make sure the ftp### accounts are 700.
 - X. mount -o remount,usrquota /data <--To make sure that quota is turned on.
 - E. Modify the quota for each ftp### account.
 - I. edquota ftp100
Filesystem blocks soft hard inodes soft
hard
/dev/sda9 0 92160 102400 0 0
0
 - II. edquota ftp250
Filesystem blocks soft hard inodes soft
hard
/dev/sda9 0 230400 256000 0 0
0
 - III. edquota ftp1GB
Filesystem blocks soft hard inodes soft
hard
/dev/sda9 0 921600 1024000 0 0
0
 - IV. edquota ftp3GB

RedHat: RE: vsftpd beginner's tutorial?

Filesystem blocks soft hard inodes soft
hard

Filesystem blocks soft hard inodes soft
hard

/dev/sda9 0 2700000 3000000 0 0
0

V. edquota ftp5GB

Filesystem blocks soft hard inodes soft
hard

/dev/sda9 0 4808000 5120000 0 0
0

VI. edquota ftp10GB

Filesystem blocks soft hard inodes soft
hard

/dev/sda9 0 9216000 10240000 0 0
0

F. Create a daily cron report cron job.

I. vi /etc/cron.daily/quotareport.cron

```
#!/bin/sh
#
# The purpose of this cron job is to send a daily reports of
the quota
# status of all user in the /data/ftp filesystem.
#
# Added by Robert Richardson on 03/24/2003.
#
/usr/sbin/repquota -u /data | mail -s "FTP Server Daily Quota
```

Report" root

II. chmod 755 /etc/cron.daily/quotareport.cron

B. Use the "account_creation" script to install ftp users
(/data/ftp/username).

Example 1:

```
./account_creation -c 'admin@mycompany.com' admin
```

9. Creating a chroot (jail) environment (NOT NEEDED ON THIS SYSTEM).

A. Allow for users to only move around in their home directory.

I. vi /etc/vsftpd.conf

```
chroot_list_enable=YES
```

II. Use the account_creation script to append every new user to a
file called

```
/etc/vsftpd.chroot_list
```

III. Make sure that the /data/ftp/<login> has permissions set to
700.

10. System security requirements.

A. Security Level Configuration

Install RedHat 9.0 with security level "No Firewall".

I. The system will only accept connections that are explicitly
defined.

B. Disable the following services:

```
apmd atd autofs gpm ipchains isdn kudzu lpd rhnsd sendmail xfs
```

I. chkconfig --list | grep on

```
crond 0:off 1:off 2:on 3:on 4:on 5:on
```

RedHat: RE: vsftpd beginner's tutorial?

6:off netfs 0:off 1:off 2:on 3:on 4:on 5:on
6:off keytable 0:off 1:on 2:on 3:on 4:on 5:on
6:off network 0:off 1:off 2:on 3:on 4:on 5:on
6:off random 0:off 1:off 2:on 3:on 4:on 5:on
6:off rawdevices 0:off 1:off 2:off 3:on 4:on 5:on
6:off portmap 0:off 1:off 2:on 3:on 4:on 5:on
6:off nfs 0:off 1:off 2:on 3:on 4:on 5:on
6:off nfslock 0:off 1:off 2:on 3:on 4:on 5:on
6:off sshd 0:off 1:off 2:on 3:on 4:on 5:on
6:off syslog 0:off 1:off 2:on 3:on 4:on 5:on
6:off vsftpd :on
6:off xinetd 0:off 1:off 2:on 3:on 4:on 5:on
6:off anacron 0:off 1:off 2:on 3:on 4:on 5:on

C. Configure login messages.

I. vi /etc/issue

Authorized users only. All access are being logged and reported.\n

II. vi /etc/issue.net

Authorized users only.

III. vi /etc/motd

```
#####  
# This system is for the use of authorized users only.  
#  
# Individuals using this computer system without authority, or  
in #  
# excess of their authority, are subject to having all of their  
#  
# activities on this system monitored and recorded by system  
#  
# personnel.  
#
```

```
#####
```

D. Create user chroot environment.

I. Upgrade Secure SSH to version 3.2.5.

RedHat: RE: vsftpd beginner's tutorial?

1. Download version 3.2.5 from ssh.com
 2. tar xvpf ssh-3.2.5.tar
 3. cd ssh-3.2.5
 4. ./configure
 5. make
 6. make install
- II. Replace "r" programs with SSH:
1. cd /usr/bin/
 2. mv ssh orig.ssh
 3. mv ssh-add orig.ssh-add
 4. mv ssh-agent orig.ssh-agent
 5. mv ssh-keygen orig.ssh-keygen
 6. mv ssh-keyscan orig.ssh-keyscan
 7. rm rsh
 8. cp -p /usr/local/bin/ssh2 .
 9. ln -s /usr/bin/ssh2 rsh
 10. rm -f slogin
 11. ln -s /usr/bin/ssh2 slogin
 12. cp -p /usr/local/bin/ssh-agent2 .
 13. ln -s /usr/bin/ssh-agent2 ssh-agent
 14. cp -p /usr/local/bin/ssh-add2 .
 15. ln -s /usr/bin/ssh-add2 ssh-add
 18. cp -p /usr/local/bin/ssh-keygen2 .
 19. ln -s ssh-keygen2 ssh-keygen
 20. cp -p /usr/local/bin/ssh-askpass2 .
 21. ln -s ssh-askpass2 ssh-askpass
 22. cp -p /usr/local/bin/ssh-dummy-shell /bin/.
 23. ln -s /usr/local/bin/sftp-server2 /usr/bin/sftp-server
- III. Restrict users to their chrooted ssh environment (for sftp).
1. vi /etc/ssh2/sshd2_config
ChRootGroups ftponly
subsystem-sftp internal://sftp-server
 2. The users are added via the account_creation script.
 3. service xinetd restart
- E. Restrict access to cron.
- I. vi /etc/cron.allow
root
admin
 - II. "service crond restart" <-- To restart cron.
- F. Configure and start logwatch cron report.
- I. vi /etc/log.d/scripts/logwatch.pl
\$Config{'detail'} = 10;
 - II. vi /etc/log.d/conf/logwatch.conf
Detail = High
- G. Disable useless services.
- I. Files in /etc/rc3.d, such as,
kudzu ipchains netfs apmd atd sendmail gpm anacron inetd
 - II. Disable TELNET remote root logins.
 - III. Restrict TCP connections.
- H. Other hardening steps are:
- I. chmod 700 /var/log

II. vi /etc/profile
TMOUT=1800 <--30 minutes of idle time.
umask 027 <--owner can read, write, and execute, while
members of
the group to which the binary belongs can read
and
execute it, and all others, cannot read,
write, or execute it.

THIS SECTION IS GOOD PRACTISE, BUT NOT USED ON THIS SYSTEM:

I. Allow only certain users to shutdown the system using
[Ctrl]-[Alt]-[Del].
I. Add a -a option to the /etc/inittab line:
ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
II. Create the /etc/shutdown.allow file. It is list of allowed
usernames,
one per line, like the following:
admin
root
J. Disable Console Program Access.
I. To not allow any user at the console to run poweroff, halt, and
reboot

do the following:
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot

11. Networking considerations.
A. vi /etc/sysconfig/network
B. vi /etc/sysconfig/network-scripts/ifcfg-eth0
C. vi /etc/sysconfig/network-scripts/ifcfg-eth1
D. Start routing information.
route add default gw xx.xx.xx.xxx
route add -net xx.xx.xx.xxx netmask 255.0.0.0 gw xx.xx.xx.xxx
D. Create and configure an add gateway init script.
I. vi addgateway
#!/bin/bash

```
*****  
#  
# Purpose: To add and delete the default gateways for eth0 and  
eth1.  
#  
# Name: addgateway  
# Version: 1.0  
# Author: Robert Richardson (Activision Studios)  
# Date: April 4th, 2003.  
#  
# History:  
# 04-APR-03 - Robert Richardson  
# Version: 1.0  
# 1. Created to add and delete the default  
gateways.
```

RedHat: RE: vsftpd beginner's tutorial?

```
#
#
#
# display_gateways --- This function uses netstat to display the
gateways.
display_gateways() { # gateways
    echo " Checking the status of the
gateways"
    echo "
===== "
    echo " "
    /bin/netstat -rn | grep UG
}
#
#
case "$1" in
start)
echo -n "Starting Default Gateway Parameters..."
route add -net xx.xx.xx.x netmask 255.255.0.0 gw xx.xx.xx.x
route add -net 0.0.0.0 netmask 0.0.0.0 gw xx.xx.xx.x
;;
stop)
echo -n "Shutting Down Gateway Parameters..."
route del -net xx.xx.xx.x netmask 255.255.0.0 gw xx.xx.xx.x
route del -net 0.0.0.0 netmask 0.0.0.0 gw xx.xx.xx.x
;;
status)
display_gateways
;;
restart|reload)
$0 stop
$0 start
;;
*)
echo "Usage: gateway {start|stop|status|restart|reload}"
exit 1
esac

exit 0
II. chmod 700 /etc/rc.d/init.d/addgateway
III. chkconfig --add addgateway
IV. chkconfig --level 345 addgateway on
V. Add the addgateway script to the various init directories.
cp -p addgateway /etc/rc.d/init.d/addgateway
cp -p addgateway /etc/rc.d/rc1.d/K91addgateway
cp -p addgateway /etc/rc.d/rc2.d/S11addgateway
cp -p addgateway /etc/rc.d/rc3.d/S11addgateway
cp -p addgateway /etc/rc.d/rc4.d/S11addgateway
```

RedHat: RE: vsftpd beginner's tutorial?

```
cp -p addgateway /etc/rc.d/rc5.d/S11addgateway
cp -p addgateway /etc/rc.d/rc6.d/K91addgateway
```

12. Configure with postfix.

- A. Go to get db*-deve*: ftp ftp.redhat.com
- B. cd pub/redhat/linux/9/RedHat/RPMS
- C. mget db4-*
- D. rpm -qal | grep db4 <---It already exist then do the next steps.
- E. rpm -Uvh db4-devel-4.0.14-20.i386.rpm
- F. rpm -Uvh db4-java-4.0.14-20.i386.rpm
- G. rpm -Uvh db4-utils-4.0.14-20.i386.rpm
- H. useradd -d /home/postfix -u 12345 -s /bin/ssh-dummy-shell postfix
- I. groupadd -g 54321 postdrop
- J. Go to mirror site: <http://mirrors.isc.org/pub/postfix/>
- K. gunzip postfix-2.0.16.tar.gz
- L. tar xpf postfix-2.0.16.tar
- M. cd postfix-2.0.16
- N. cd /home/admin/packages/postfix-2.0.16
- O. make
- P. make install
install_root: [/]
tempdir: [/home/admin/packages/postfix-2.0.16]
config_directory: [/etc/postfix]
daemon_directory: [/usr/libexec/postfix]
command_directory: [/usr/sbin]
queue_directory: [/var/spool/postfix]
sendmail_path: [/usr/sbin/sendmail]
newaliases_path: [/usr/bin/newaliases]
mailq_path: [/usr/bin/mailq]
mail_owner: [postfix]
setgid_group: [postdrop]
manpage_directory: [/usr/local/man]
sample_directory: [/etc/postfix]
readme_directory: [no]
- Q. postfix start
- R. mv /etc/aliases /etc/sendmail.orig.aliases
- S. ln -s /etc/postfix/aliases /etc/aliases
- T. vi /etc/postfix/aliases
root: admin@mycompany.com
postfix: root
- U. newaliases

13. System transition.

14. Windows user connectivity

- A. Instruct Windows users on using secure ftp (sftp) via a pc.
 - I. Go to the website below to get ssh for the pc.
http://geosci.uchicago.edu/computing/windows_ssh.html
 - II. Follow the install instructions.
 - III. Complete all encrypted ftp transactions via sftp.
 - IV. Make these instructions part of the intranet website that has

the rules and

regulations for using this FTP Server.

15. System disk space growth considerations.

RE: vsftpd beginner's tutorial?

16. System recovery requirements.

+++++

--

redhat-list mailing list
unsubscribe <mailto:redhat-list-request@redhat.com?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>