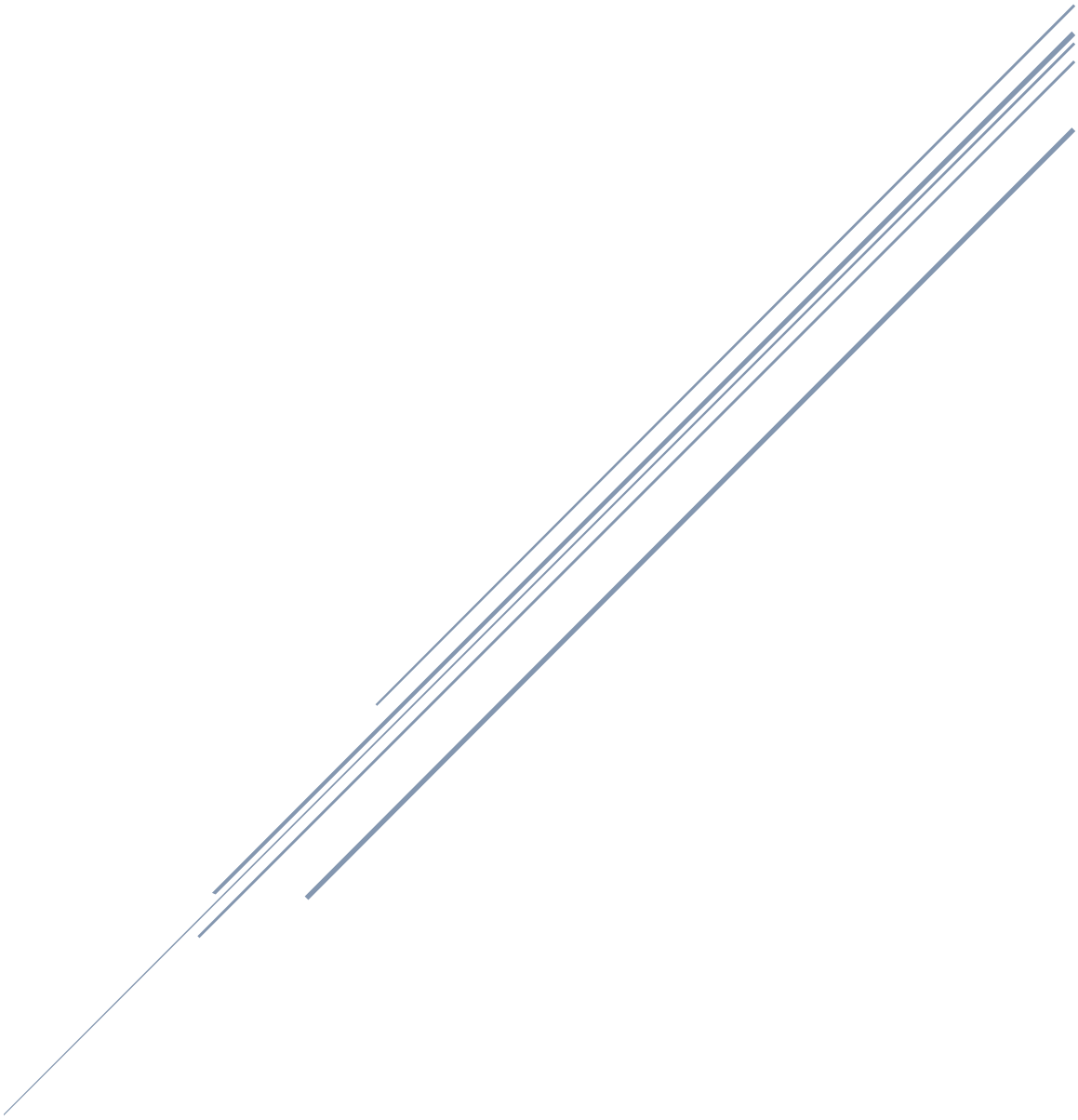
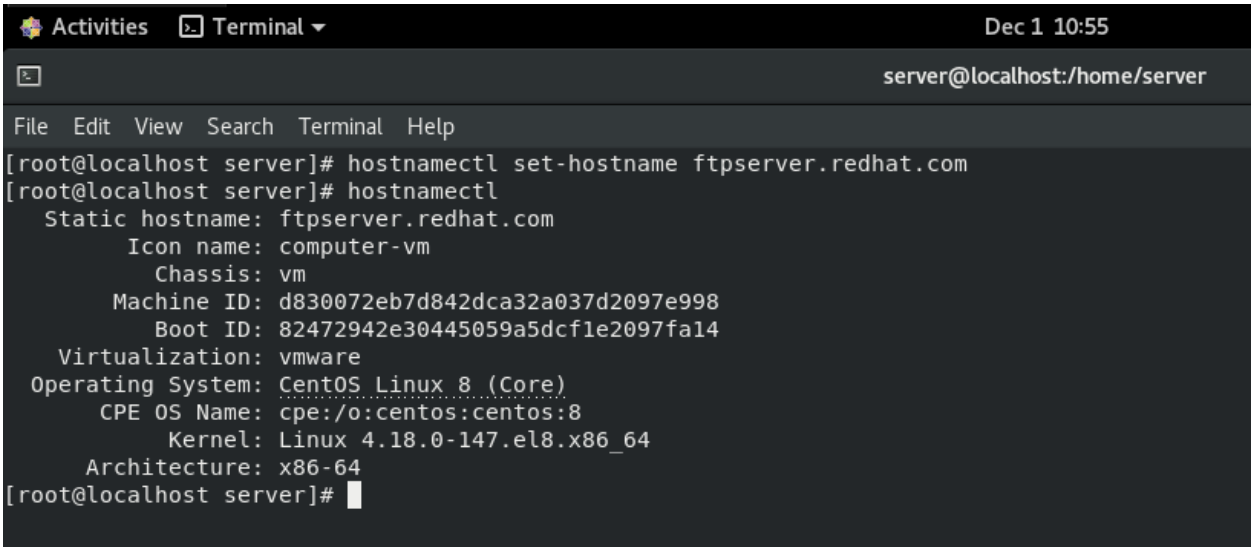
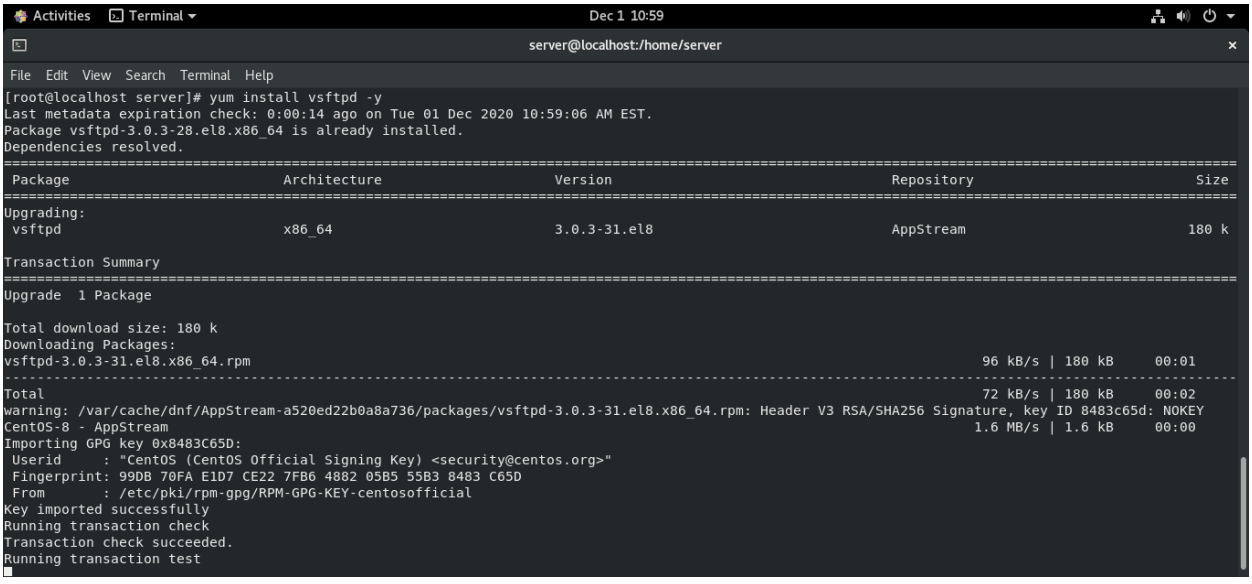
FTP – INSTALL,CONFIG AND SECURE

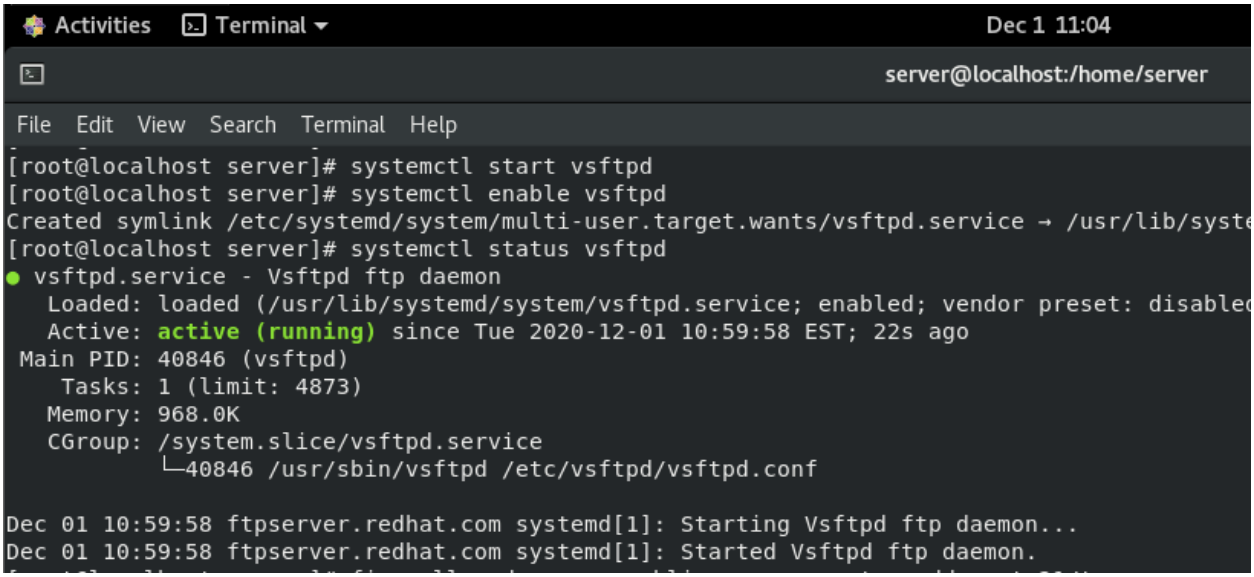


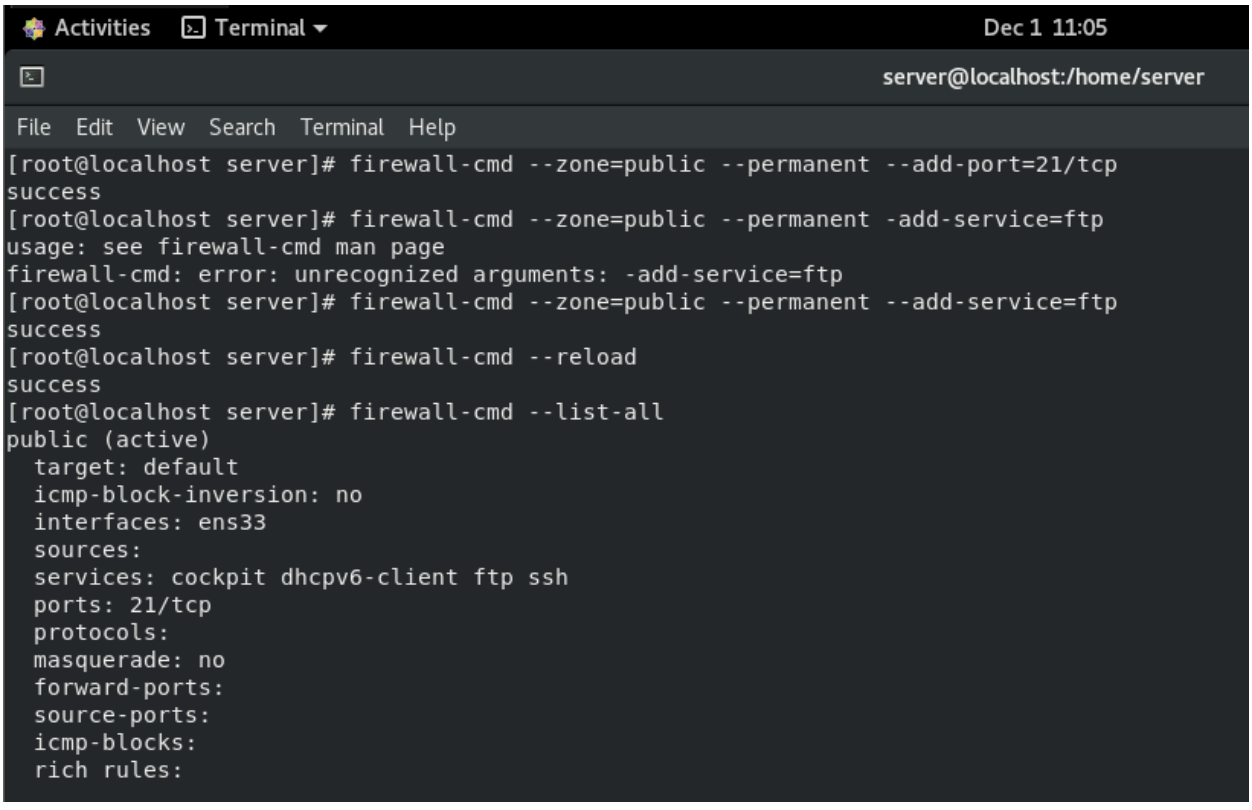
Jadhusan. M. S

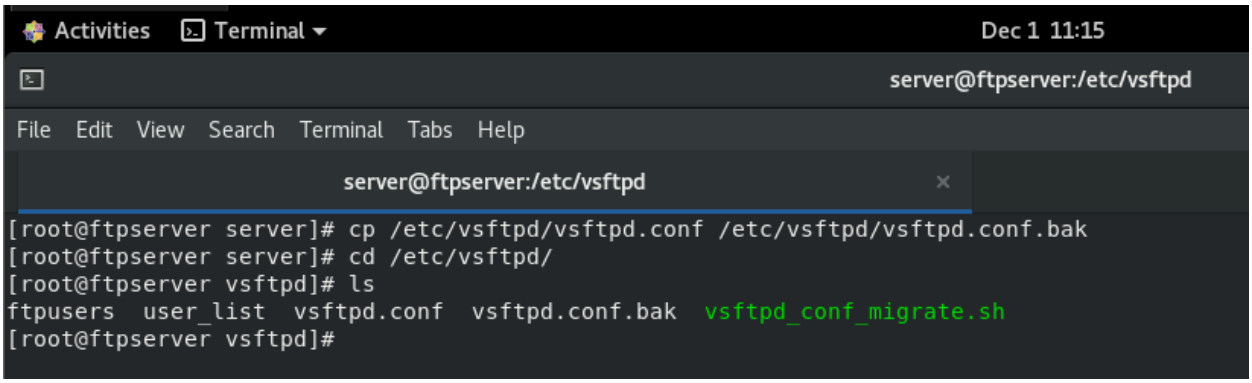
VSFTP CONFIGURATION






Activities
Terminal
Dec 1 11:04
server@localhost:/home/server
File Edit View Search Terminal Help
[root@localhost server]# systemctl start vsftpd
[root@localhost server]# systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/syste
[root@localhost server]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disable
Active: active (running) since Tue 2020-12-01 10:59:58 EST; 22s ago
Main PID: 40846 (vsftpd)
Tasks: 1 (limit: 4873)
Memory: 968.0K
CGroup: /system.slice/vsftpd.service
└─40846 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
Dec 01 10:59:58 ftpserver.redhat.com systemd[1]: Starting Vsftpd ftp daemon...
Dec 01 10:59:58 ftpserver.redhat.com systemd[1]: Started Vsftpd ftp daemon.


Activities
Terminal
Dec 1 11:05
server@localhost:/home/server
File Edit View Search Terminal Help
[root@localhost server]# firewall-cmd --zone=public --permanent --add-port=21/tcp
success
[root@localhost server]# firewall-cmd --zone=public --permanent -add-service=ftp
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: -add-service=ftp
[root@localhost server]# firewall-cmd --zone=public --permanent --add-service=ftp
success
[root@localhost server]# firewall-cmd --reload
success
[root@localhost server]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: ens33
sources:
services: cockpit dhcpv6-client ftp ssh
ports: 21/tcp
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:



Now add these two following options to restrict FTP users to their Home directories.

chroot_local_user=YES
allow_writeable_chroot=YES

chroot_local_user=YES means local users will be placed in a chroot jail, their home directory after login by default settings.

And also by default, vsftpd does not allow the chroot jail directory to be writable for security reasons, however, we can use the option allow_writeable_chroot=YES to override this setting.

Set the SELinux boolean below to allow FTP to read files in a user's home directory. Note that this was initially done using the the command:

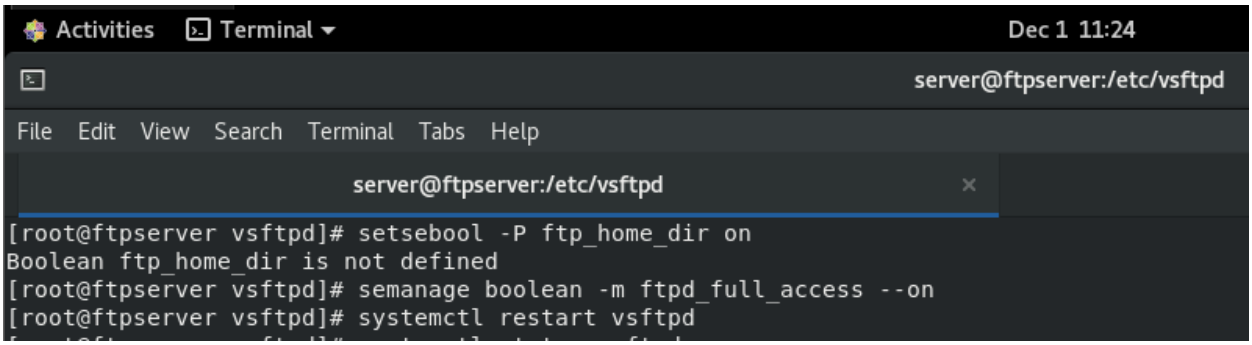
setsebool -P ftp_home_dir on

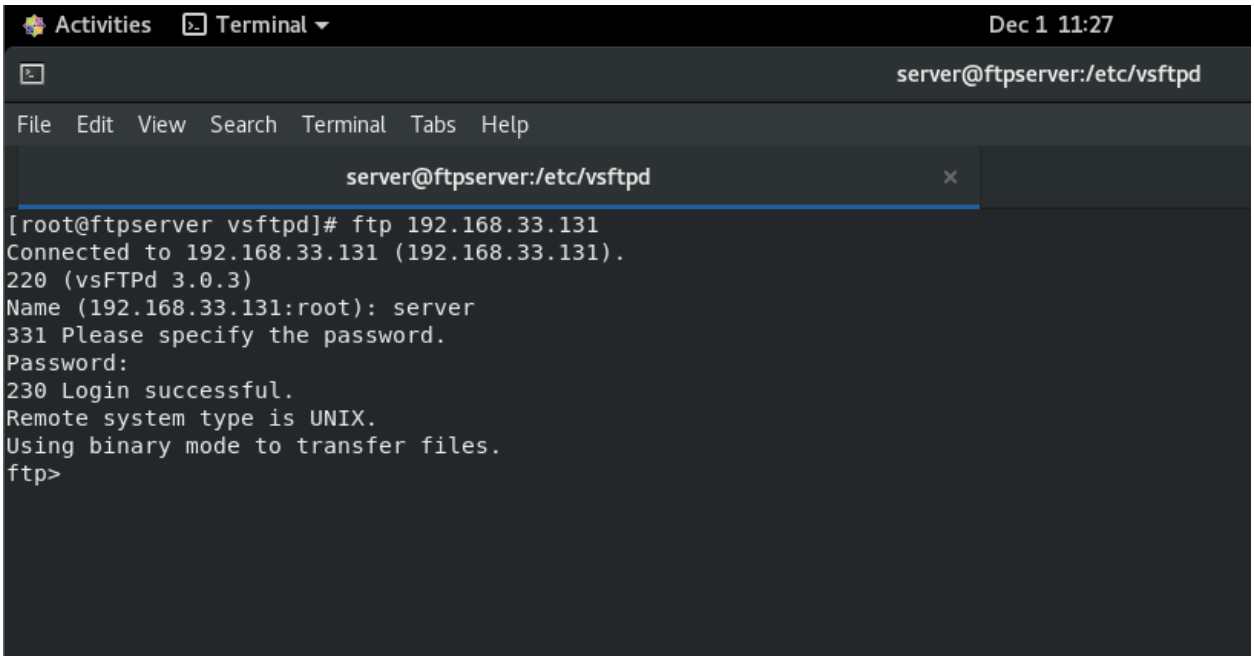
semanage command to set SELinux rule to allow FTP to read/write user's home directory

semanage boolean -m ftpd_full_access –on

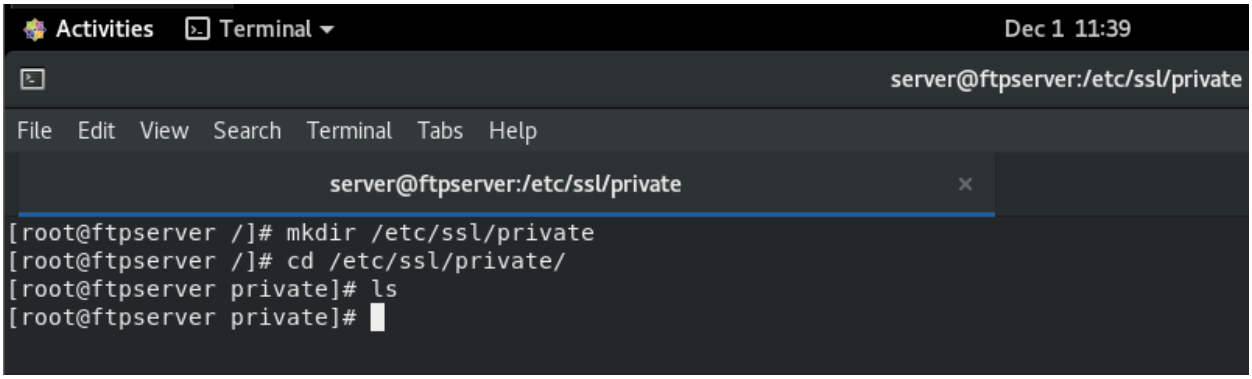
We have to restart vsftpd to effect all the changes we made so far above:

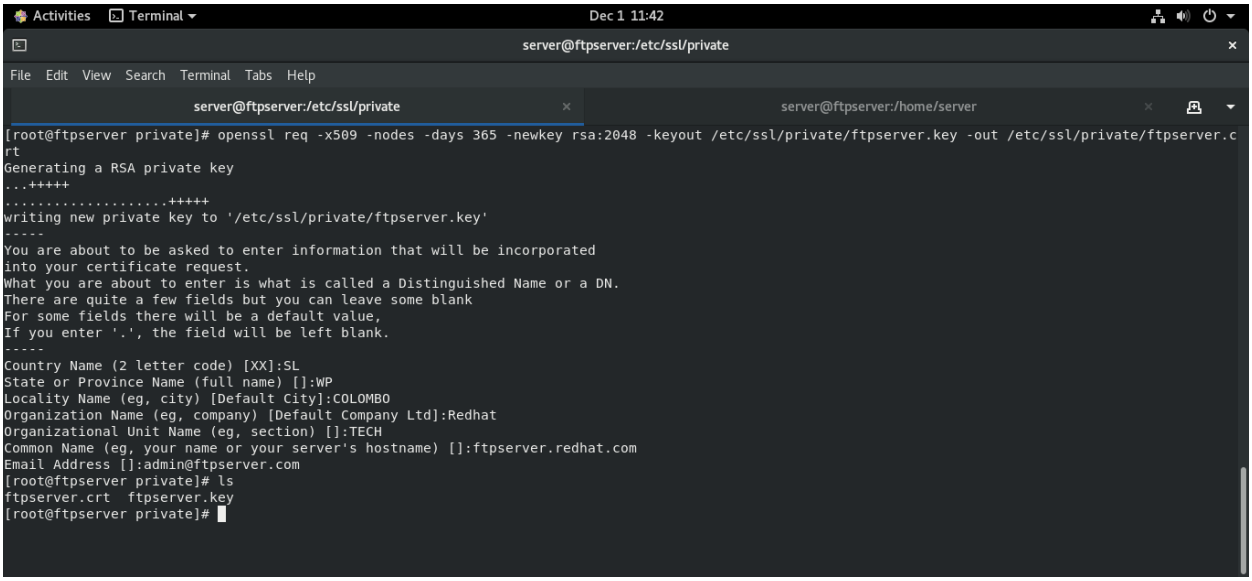
systemctl restart vsftpd

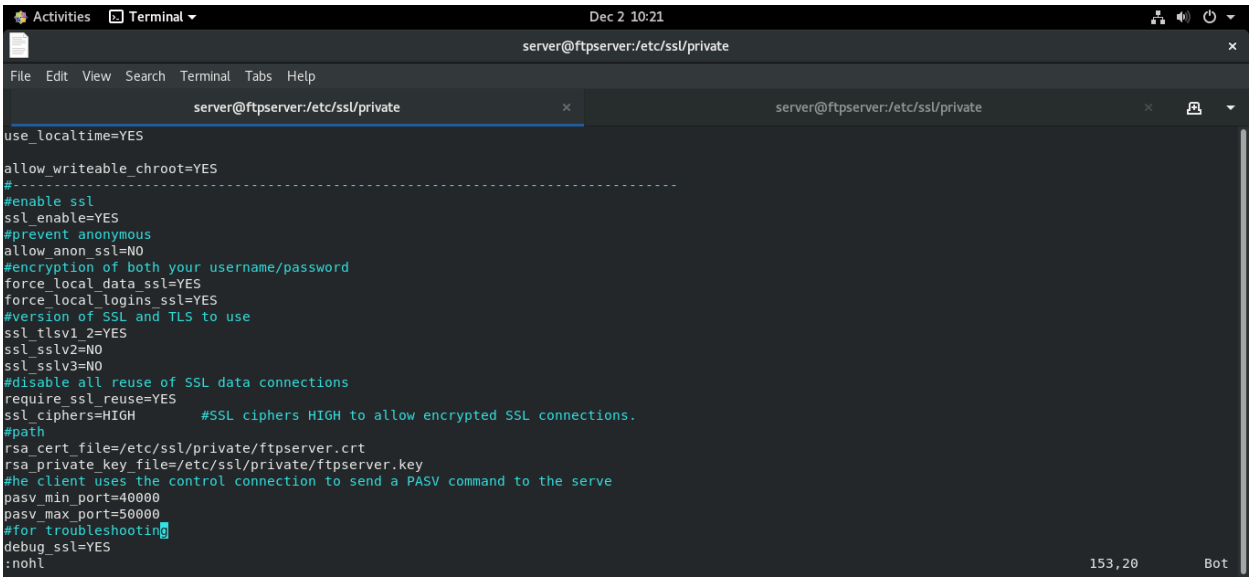

Activities
Terminal
Dec 1 11:24
server@ftpserver:/etc/vsftpd
File Edit View Search Terminal Tabs Help
server@ftpserver:/etc/vsftpd
[root@ftpserver vsftpd]# setsebool -P ftp_home_dir on
Boolean ftp_home_dir is not defined
[root@ftpserver vsftpd]# semanage boolean -m ftpd_full_access --on
[root@ftpserver vsftpd]# systemctl restart vsftpd

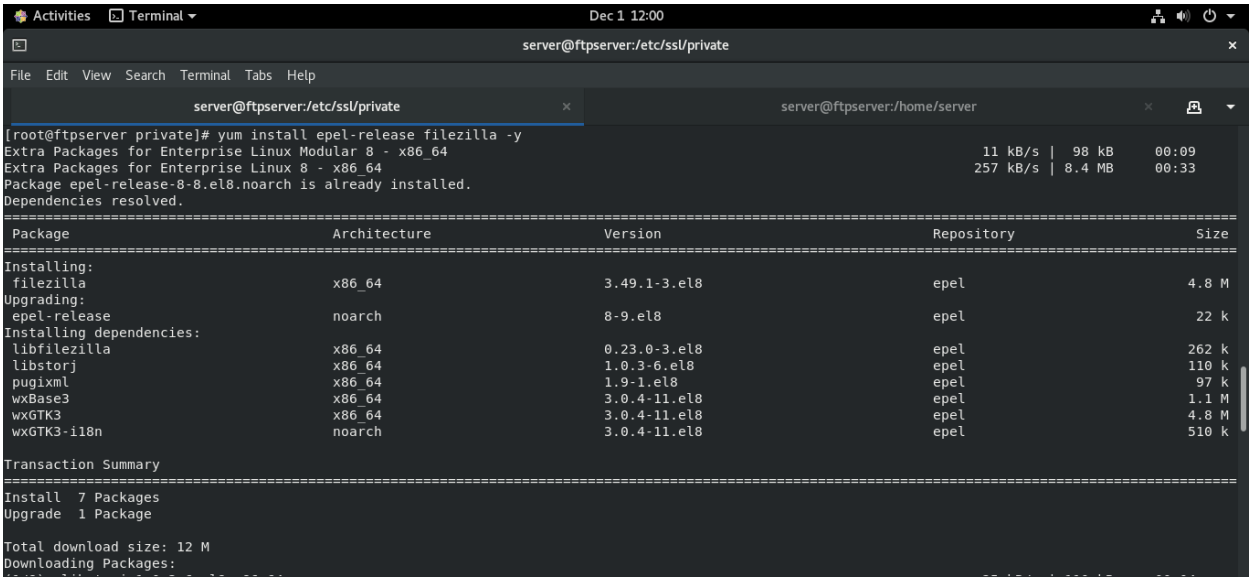

Activities
Terminal
Dec 1 11:27
server@ftpserver:/etc/vsftpd
File Edit View Search Terminal Tabs Help
server@ftpserver:/etc/vsftpd
[root@ftpserver vsftpd]# ftp 192.168.33.131
Connected to 192.168.33.131 (192.168.33.131).
220 (vsFTPd 3.0.3)
Name (192.168.33.131:root): server
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

SSL CONFIGURATION

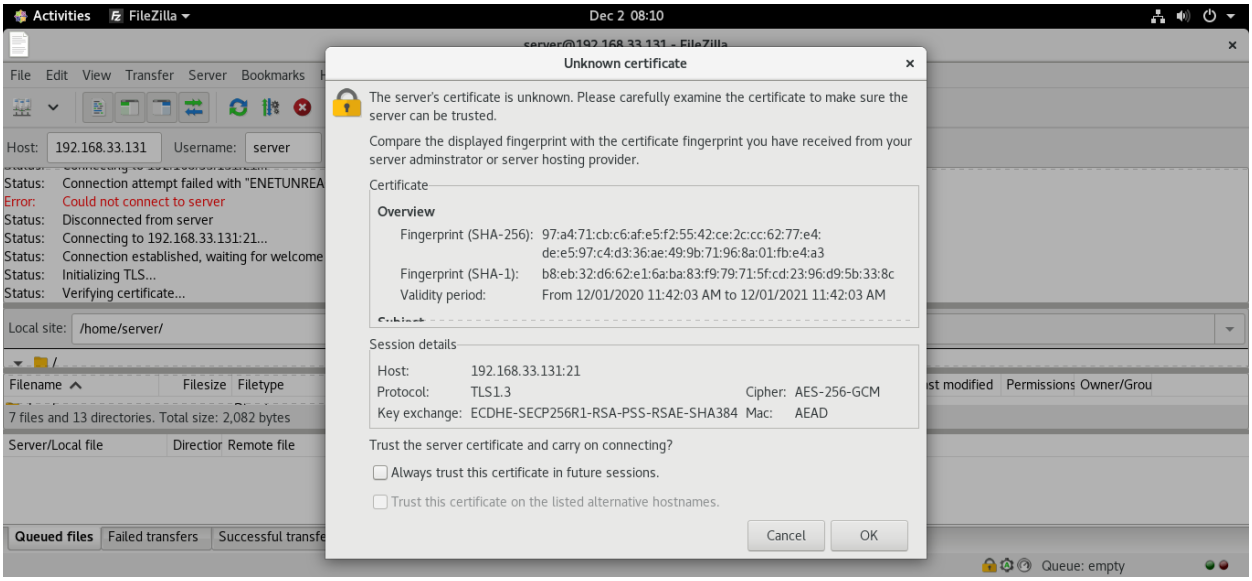


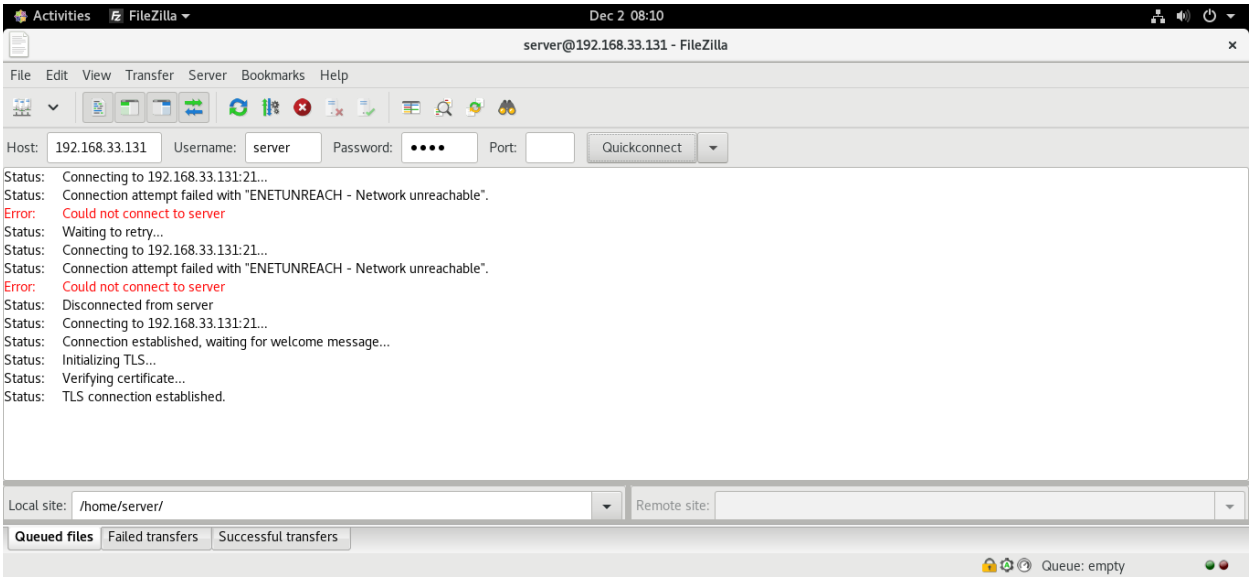



Activities
Terminal
Dec 2 10:21
server@ftpserver:/etc/ssl/private
File Edit View Search Terminal Tabs Help
server@ftpserver:/etc/ssl/private
server@ftpserver:/etc/ssl/private
use_localtime=YES
allow_writeable_chroot=YES
#--
#enable ssl
ssl_enable=YES
#prevent anonymous
allow_anon_ssl=NO
#encryption of both your username/password
force_local_data_ssl=YES
force_local_logins_ssl=YES
#version of SSL and TLS to use
ssl_tlsv1_2=YES
ssl_sslv2=NO
ssl_sslv3=NO
#disable all reuse of SSL data connections
require_ssl_reuse=YES
ssl_ciphers=HIGH #SSL ciphers HIGH to allow encrypted SSL connections.
#path
rsa_cert_file=/etc/ssl/private/ftpserver.crt
rsa_private_key_file=/etc/ssl/private/ftpserver.key
#he client uses the control connection to send a PASV command to the serve
pasv_min_port=40000
pasv_max_port=50000
#for troubleshooting
debug_ssl=YES
:nohl
153,20 Bot


Activities
Terminal
Dec 1 12:00
server@ftpserver:/etc/ssl/private
File Edit View Search Terminal Tabs Help
server@ftpserver:/etc/ssl/private
server@ftpserver:/home/server
[root@ftpserver private]# yum install epel-release filezilla -y
Extra Packages for Enterprise Linux Modular 8 - x86_64 11 kB/s | 98 kB 00:09
Extra Packages for Enterprise Linux 8 - x86_64 257 kB/s | 8.4 MB 00:33
Package epel-release-8-8.el8.noarch is already installed.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
filezilla x86_64 3.49.1-3.el8 epel 4.8 M
Upgrading:
epel-release noarch 8-9.el8 epel 22 k
Installing dependencies:
libfilezilla x86_64 0.23.0-3.el8 epel 262 k
libstorj x86_64 1.0.3-6.el8 epel 110 k
pugixml x86_64 1.9-1.el8 epel 97 k
wxBase3 x86_64 3.0.4-11.el8 epel 1.1 M
wxGTK3 x86_64 3.0.4-11.el8 epel 4.8 M
wxGTK3-i18n noarch 3.0.4-11.el8 epel 510 k
Transaction Summary
Install 7 Packages
Upgrade 1 Package
Total download size: 12 M
Downloading Packages:

CONNECTION


Activities
FileZilla
Dec 2 08:10
File Edit View Transfer Server Bookmarks
Host: 192.168.33.131 Username: server
Status: Connection attempt failed with "ENETUNREA
Error: Could not connect to server
Status: Disconnected from server
Status: Connecting to 192.168.33.131:21...
Status: Connection established, waiting for welcome
Status: Initializing TLS...
Status: Verifying certificate...
Local site: /home/server/
Filename Filesize Filetype
7 files and 13 directories. Total size: 2,082 bytes
Server/Local file Direction Remote file
Queued files Failed transfers
Queue: empty
Unknown certificate
The server's certificate is unknown. Please carefully examine the certificate to make sure the server can be trusted.
Compare the displayed fingerprint with the certificate fingerprint you have received from your server adminstrator or server hosting provider.
Certificate
Overview
Fingerprint (SHA-256): 97:a4:71:cb:c6:af:e5:f2:55:42:ce:2c:cc:62:77:e4:de:e5:97:c4:d3:36:ae:49:9b:71:96:8a:01:fb:e4:a3
Fingerprint (SHA-1): b8:eb:32:d6:62:e1:6a:ba:83:f9:79:71:5f:cd:23:96:d9:5b:33:8c
Validity period: From 12/01/2020 11:42:03 AM to 12/01/2021 11:42:03 AM
Session details
Host: 192.168.33.131:21
Protocol: TLS1.3
Cipher: AES-256-GCM
Key exchange: ECDHE-SECP256R1-RSA-PSS-RSAE-SHA384
Mac: AEAD
Trust the server certificate and carry on connecting?
Always trust this certificate in future sessions.
Trust this certificate on the listed alternative hostnames.
Cancel
OK


Activities
FileZilla
Dec 2 08:10
server@192.168.33.131 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: 192.168.33.131 Username: server Password: •••• Port: Quickconnect
Status: Connecting to 192.168.33.131:21...
Status: Connection attempt failed with "ENETUNREACH - Network unreachable".
Error: Could not connect to server
Status: Waiting to retry...
Status: Connecting to 192.168.33.131:21...
Status: Connection attempt failed with "ENETUNREACH - Network unreachable".
Error: Could not connect to server
Status: Disconnected from server
Status: Connecting to 192.168.33.131:21...
Status: Connection established, waiting for welcome message...
Status: Initializing TLS...
Status: Verifying certificate...
Status: TLS connection established.
Local site: /home/server/
Remote site:
Queued files Failed transfers Successful transfers
Queue: empty