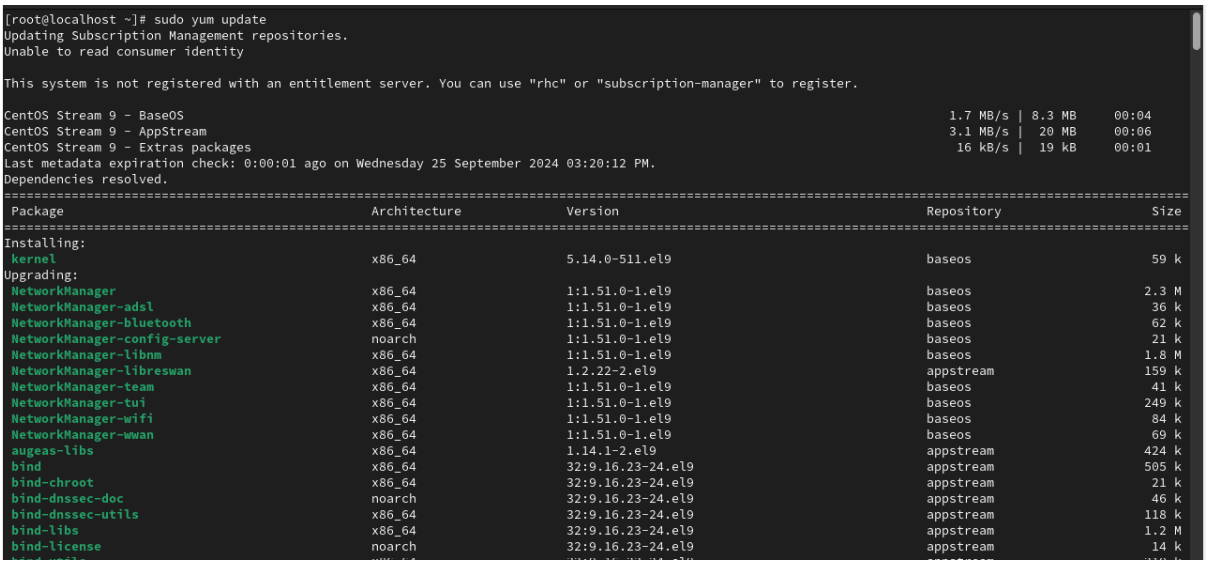
Name: Rachana Mangalaram

Topic: Configuration of FTP Server

sudo yum update

The sudo yum update command updates all installed packages on Red Hat-based systems like CentOS or Amazon Linux. It checks for the latest versions of packages and installs them, ensuring your system is up-to-date with the latest security patches and features.



```
[root@localhost ~]# sudo yum update
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

CentOS Stream 9 - BaseOS                                        1.7 MB/s | 8.3 MB     00:04
CentOS Stream 9 - AppStream                                     3.1 MB/s |  20 MB     00:06
CentOS Stream 9 - Extras packages                                16 kB/s |  19 kB     00:01
Last metadata expiration check: 0:00:01 ago on Wednesday 25 September 2024 03:20:12 PM.
Dependencies resolved.
================================================================================
 Package                 Architecture            Version                 Repository                Size
================================================================================
Installing:
 kernel                  x86_64                  5.14.0-511.el9          baseos                    59 k
Upgrading:
 NetworkManager          x86_64                  1:1.51.0-1.el9          baseos                   2.3 M
 NetworkManager-adsl     x86_64                  1:1.51.0-1.el9          baseos                    36 k
 NetworkManager-bluetooth x86_64                 1:1.51.0-1.el9          baseos                    62 k
 NetworkManager-config-server noarch             1:1.51.0-1.el9          baseos                    21 k
 NetworkManager-libnm    x86_64                  1:1.51.0-1.el9          baseos                   1.8 M
 NetworkManager-libreswan x86_64                 1.2.22-2.el9            appstream                159 k
 NetworkManager-team     x86_64                  1:1.51.0-1.el9          baseos                    41 k
 NetworkManager-tui      x86_64                  1:1.51.0-1.el9          baseos                   249 k
 NetworkManager-wifi     x86_64                  1:1.51.0-1.el9          baseos                    84 k
 NetworkManager-wwan     x86_64                  1:1.51.0-1.el9          baseos                    69 k
 augeas-libs             x86_64                  1.14.1-2.el9            appstream                424 k
 bind                    x86_64                  32:9.16.23-24.el9       appstream                505 k
 bind-chroot             x86_64                  32:9.16.23-24.el9       appstream                 21 k
 bind-dnssec-doc         noarch                  32:9.16.23-24.el9       appstream                 46 k
 bind-dnssec-utils       x86_64                  32:9.16.23-24.el9       appstream                118 k
 bind-libs               x86_64                  32:9.16.23-24.el9       appstream                1.2 M
 bind-license            noarch                  32:9.16.23-24.el9       appstream                 14 k
```

sudo yum install vsftpd

The command sudo yum install vsftpd is used to install the vsftpd (Very Secure File Transfer Protocol Daemon) package on Red Hat-based Linux distributions like CentOS or Amazon Linux. This software allows you to set up and manage an FTP server, enabling users to transfer files to and from the server securely. Running this command will download and install the vsftpd package and its dependencies from the repository

sudo systemctl enable vsftpd

The command sudo systemctl enable vsftpd enables the vsftpd service to start automatically at boot on systems using systemd (like CentOS, RHEL, or Amazon Linux 2). This ensures that the FTP server starts whenever the system is rebooted or powered on, without needing to manually start it each time. It does not start the service immediately but sets it to start on future boots.

sudo systemctl start vsftpd

The command sudo systemctl start vsftpd is used to start the vsftpd (FTP server) service immediately on a system running systemd. After executing this, the FTP server will be running, allowing users to transfer files to and from the server. To ensure the service starts automatically at boot, you would pair this command with sudo systemctl enable vsftpd.

```
[root@localhost ~]# sudo yum install vsftpd
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

Last metadata expiration check: 1:14:16 ago on Wednesday 25 September 2024 03:20:12 PM.
Package vsftpd-3.0.5-6.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost ~]# sudo systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@localhost ~]# sudo systemctl start vsftpd
```

vi etc/vsftpd/vsftpd.conf

The command vi /etc/vsftpd/vsftpd.conf opens the configuration file for vsftpd (Very Secure FTP Daemon) using the vi text editor. This file contains the settings for the FTP server, such as access permissions, security options, anonymous login, and FTP-related parameters.

By editing this file, we can customize the behavior of your FTP server to suit your needs.

sudo systemctl restart vsftpd

It is used to restart the vsftpd service. It stops the currently running FTP service and starts it again, applying any new changes made to the configuration file or clearing any issues that may have occurred. This is commonly used after modifying the /etc/vsftpd/vsftpd.conf file to ensure the changes take effect.

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
[root@localhost ~]# sudo systemctl restart vsftpd
```

sudo firewall-cmd --zone=public --add-service=ftp --permanent

It allows FTP traffic through the firewall in the public zone, ensuring the FTP service can be accessed from external networks. The --permanent flag makes this rule persistent across reboots.

sudo firewall-cmd –reload

This command reloads the firewall configuration to apply any new changes made (such as allowing FTP service). It activates the updated rules without needing a system reboot.

sudo adduser ftpuser

This command creates a new user named ftpuser on the system. This user can be given access to the FTP server for file transfers.

sudo passwd ftpuser

This command sets or changes the password for the ftpuser account. The user will need this password to log in to the FTP server.

ip addr show

This command displays the IP addresses and network interfaces of the system. It's useful for identifying the server's IP address that FTP clients will connect to.

systemctl status vsftpd.service

This command checks the status of the vsftpd service, showing whether it is running, stopped, or experiencing any issues. It also provides logs and details about the service’s current state.

```
[root@localhost ~]# sudo firewall-cmd --zone=public --add-service=ftp --permanent
success
[root@localhost ~]# sudo firewall-cmd --reload
success
[root@localhost ~]# sudo adduser ftpuser
[root@localhost ~]# sudo passwd ftpuser
Changing password for user ftpuser.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:28:7d:9e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 83331sec preferred_lft 83331sec
    inet6 fe80::a00:27ff:fe28:7d9e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]# systemctl status vsftpd.service
● vsftpd.service - Vsftpd ftp daemon
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
     Active: active (running) since Wed 2024-09-25 16:42:29 IST; 4min 37s ago
```

chmod a-w /home/ftpuser

This command removes write permissions from the /home/ftpuser directory, ensuring that the FTP user cannot upload or modify files within their home directory. It's often done to secure FTP accounts.

vi /etc/vsftpd/vsftpd.conf

This command opens the vsftpd configuration file for editing using the vi editor. You can make changes to customize FTP settings such as anonymous access, local user permissions, or security options.

sudo systemctl restart vsftpd

ftp localhost

This command initiates an FTP session with the local machine (localhost). It is typically used to test the FTP server by connecting to it from the same server it's running on.

```
[root@localhost ~]# chmod a-w /home/ftpuser
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
[root@localhost ~]# sudo systemctl restart vsftpd
[root@localhost ~]# ftp localhost
Trying ::1...
ftp: connect to address ::1Connection refused
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.5)
Name (localhost:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,211,165).
150 Here comes the directory listing.
226 Directory send OK.
ftp> bye
421 Timeout.
```

Lets check the contents present in vsftpd.conf :

cat /etc/vsftpd/vsftpd.conf

```
[root@localhost ~]# cat /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
# When SELinux is enforcing check for SE bool allow_ftpd_anon_write, allow_ftpd_full_access
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
```

```
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode. The vsftpd.conf(5) man page explains
# the behaviour when these options are disabled.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
```

```
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
user_sub_token=$USER
local_root=/home/$USER
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=NO

pam_service_name=vsftpd
userlist_enable=YES

[root@localhost ~]#
```

Using filezilla client: