REVATURE

Project

“Web and File Server Configuration for Managing Departmental Users and Groups in a Large Network Environment Using YUM Server"

Prepred by
Karan Verma
Tushar More
Nikita Bacha
Shruti Jagtap
Pratiksha Deshmukh
Nandkumar Chavan
Vaskar Paul

Guided by
Zakir Hussain

Table of Contents

YUM SERVER ,WEB SERVER AND FILE SERVER ADMINISTRATION

Project Overview

In this project,We will act as the system administrator for a mid- sized company that relies on CentOS 7.1 to manage its internal software repositories and file server needs. The primary focus is to set up and maintain a YUM server to streamline package management for internal systems, while also configuring a File Server that allows secure storage and sharing of documents among employees. We'll also ensure system security, service uptime, and handle user accounts effectively.

Real-Life Scenario

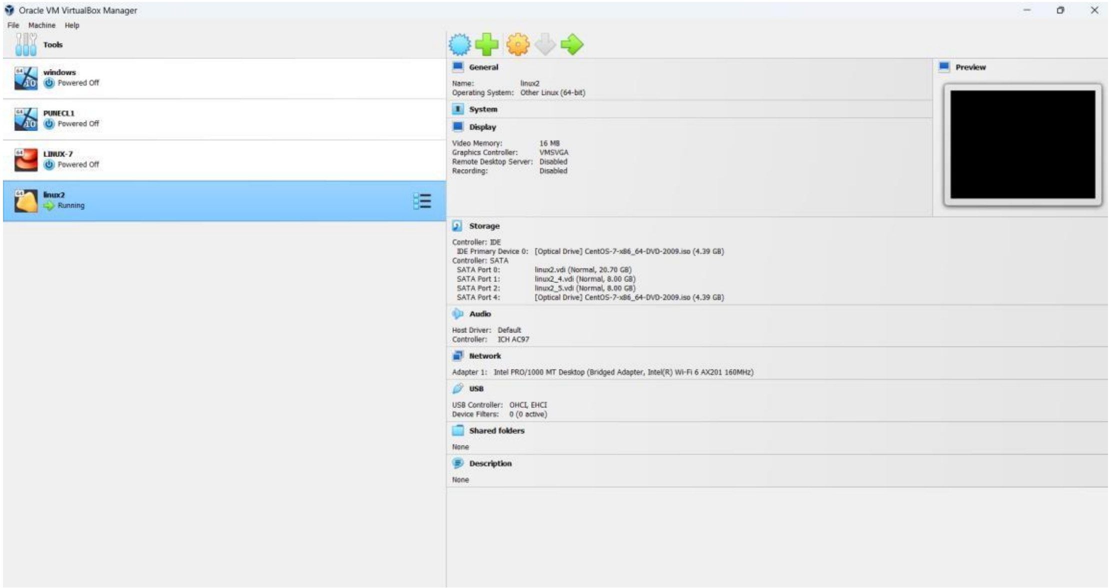
Our organization manages over 100 Linux-based systems, and to reduce dependency on external repositories, we've been tasked with setting up a **local YUM server**. In addition, the company requires a **centralized file server** where employees can securely upload and access shared documents. The servers must remain secure, automated for backups, and accessible via a properly configured network with minimal downtime.

Project Objectives

- Set up and configure a **YUM server** to host packages locally.
- Configure a **File Server** using NFS or FTP for sharing files across the network.
- Set up user accounts and manage permissions to control access to the file server.
- Ensure **network security** by configuring a firewall and SSH.
- Automate backup and update tasks using shell scripts .
- Troubleshoot issues through logs and system tools like topand htop.

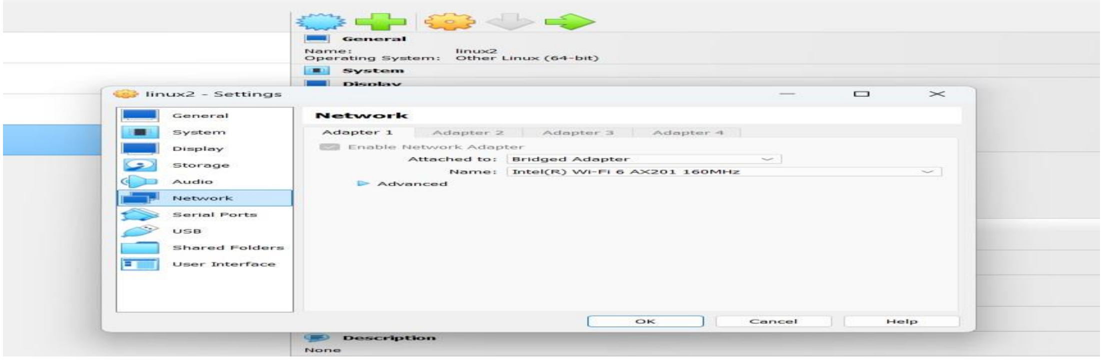
Detailed Tasks & Steps

1 Centos : CentOS is an open-source Linux operating system distribution based on Red Hat Enterprise Linux. It is designed to provide a stable and reliable platform for servers and workstations. It is a popular choice for businesses and organizations that need a robust and secure operating system.



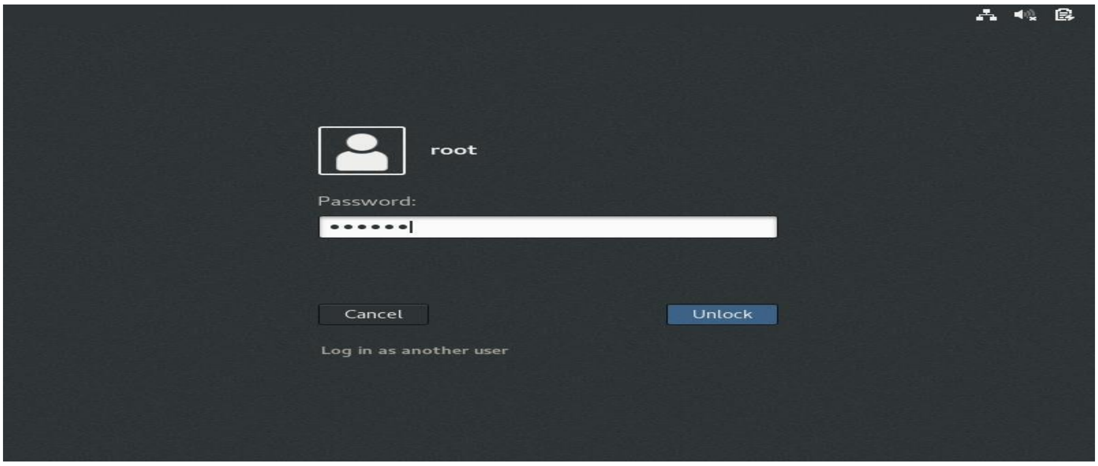
```
General
Name:               linux2
Operating System:   Other Linux (64-bit)
System
Display
Video Memory:             16 MB
Graphics Controller:      VMSVGA
Remote Desktop Server:    Disabled
Recording:                Disabled
Storage
Controller: IDE
  IDE Primary Device 0:  [Optical Drive] CentOS-7-x86_64-DVD-2009.iso (4.39 GB)
Controller: SATA
  SATA Port 0:           linux2.vdi (Normal, 20.70 GB)
  SATA Port 1:           linux2_4.vdi (Normal, 8.00 GB)
  SATA Port 2:           linux2_5.vdi (Normal, 8.00 GB)
  SATA Port 4:           [Optical Drive] CentOS-7-x86_64-DVD-2009.iso (4.39 GB)
Audio
Host Driver:   Default
Controller:    ICH AC97
Network
Adapter 1:  Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Wi-Fi 6 AX201 160MHz)
USB
USB Controller:   OHCI, EHCI
Device Filters:   0 (0 active)
Shared folders
None
Description
None
```

Network Setting :

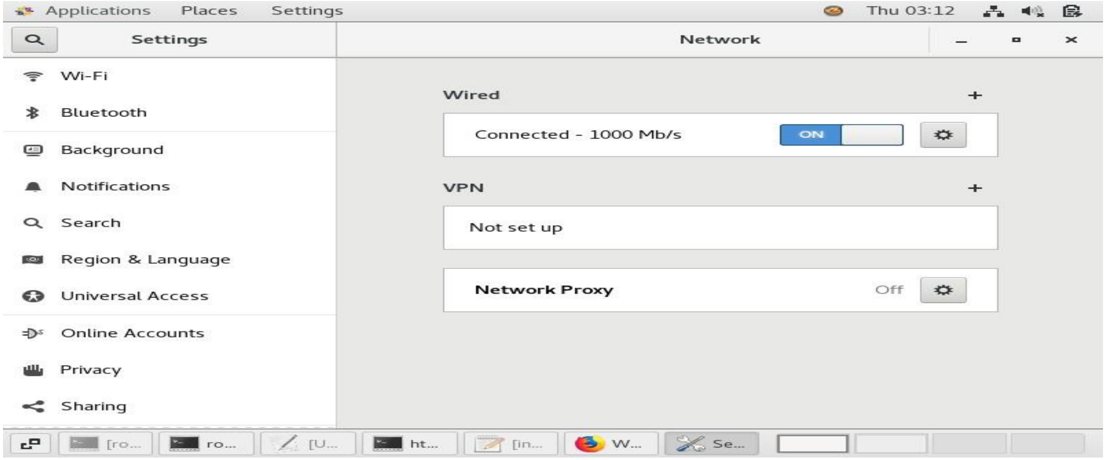


```
General
Name:                linux2
Operating System:    Other Linux (64-bit)
System
Display

Network
Adapter 1
☑ Enable Network Adapter
        Attached to:  Bridged Adapter
               Name:  Intel(R) Wi-Fi 6 AX201 160MHz

Description
None
```

Logging in with the root account on CentOS allows you to have full administrative privileges on the system. However, it is recommended to use the root account only when necessary, as using it for regular tasks can pose security risks. It is a good practice to create a separate user account with limited permissions for everyday use on CentOS.



Checking Network Connection :



Wired

Connected - 1000 Mb/s ON

VPN

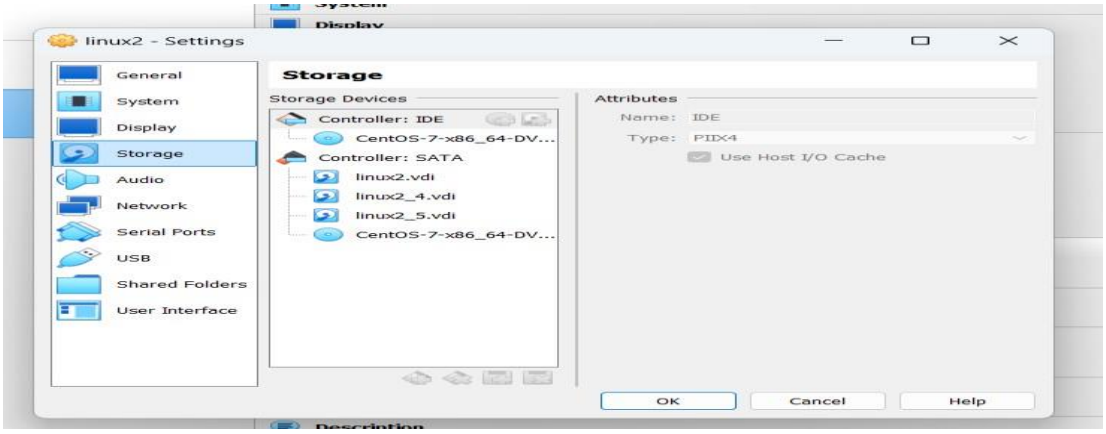
Not set up

Network Proxy Off

Steps to configure web server :

Insert ISO in VirtualBox DVD Drive

1. **Open VirtualBox**.
2. Go to **Settings** of your VM.
3. Click on **Storage**.
4. Under **Controller: IDE**, click the **Empty** disk icon.
5. Click the disk icon on the right and choose **a disk file**.
6. Select the CentOS ISO file you have downloaded.
7. Start the VM.



Storage

Storage Devices

- Controller: IDE
  - CentOS-7-x86_64-DV...
- Controller: SATA
  - linux2.vdi
  - linux2_4.vdi
  - linux2_5.vdi
  - CentOS-7-x86_64-DV...

Attributes

Name: IDE

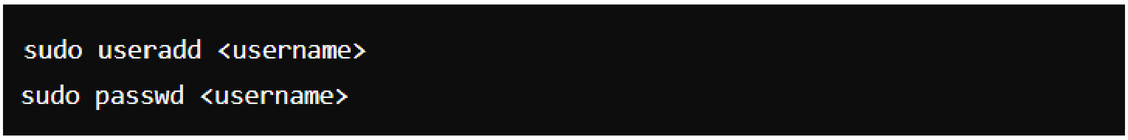
Type: PIIX4

☑ Use Host I/O Cache

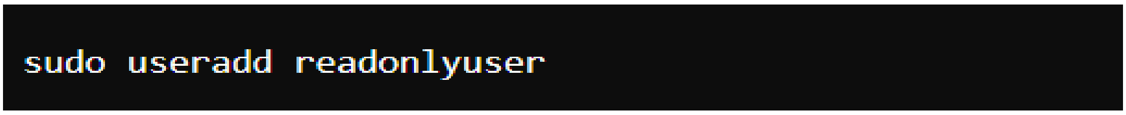
STEP 1 : User Account Management

Objective: Create and manage user accounts with appropriate permissions for accessing the file server.

1 Create user accounts:

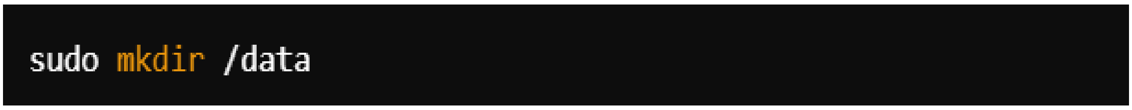


```
sudo useradd <username>
sudo passwd <username>
```



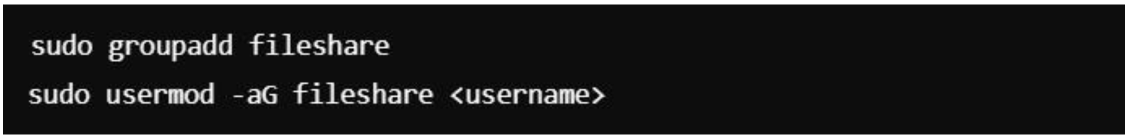
```
sudo useradd readonlyuser
```

2.Create a Directory for the User



```
sudo mkdir /data
```

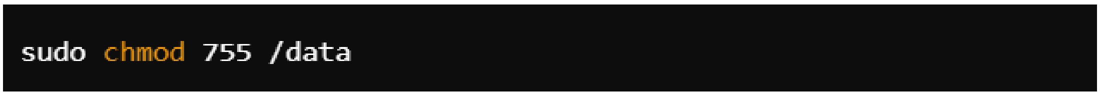
3 Assign users to groups (for managing file access):



```
sudo groupadd fileshare
sudo usermod -aG fileshare <username>
```

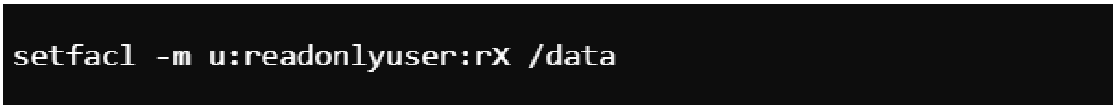
4 Manage permissions using chmod, chown, and chgrp

: Set Read-Only Permission Using chmod



```
sudo chmod 755 /data
```

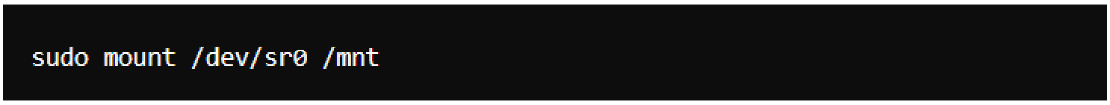
Grant Read Permission Using setfacl.



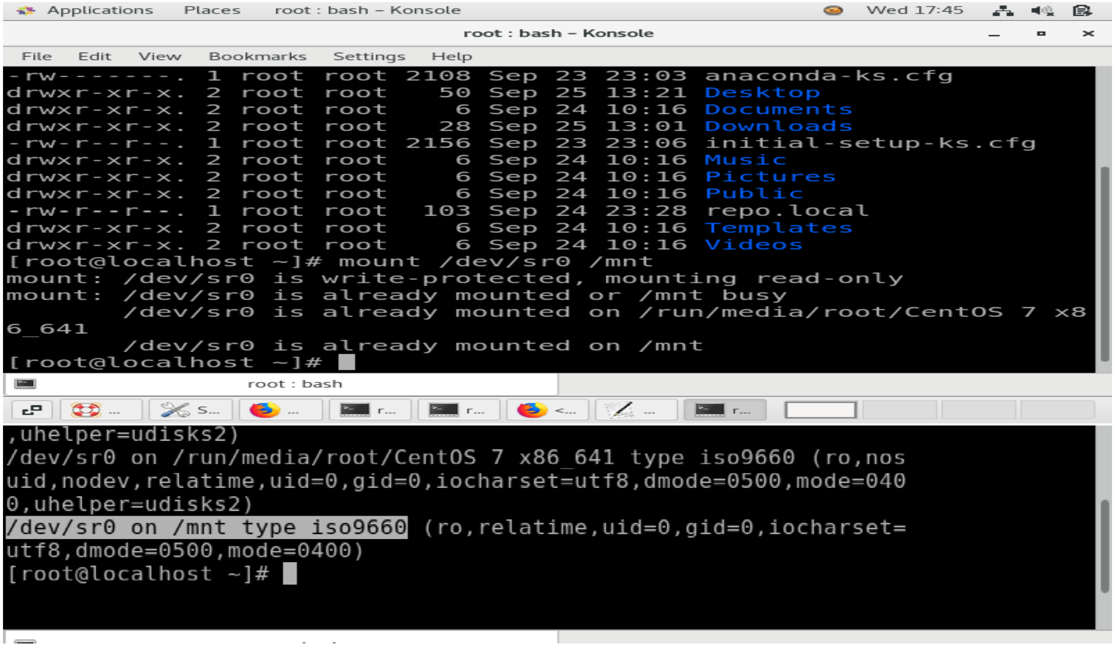
```
setfacl -m u:readonlyuser:rX /data
```

STEP 2. Mount the ISO to /mnt

Once your VM has booted, open a terminal and mount the ISO:



```
sudo mount /dev/sr0 /mnt
```

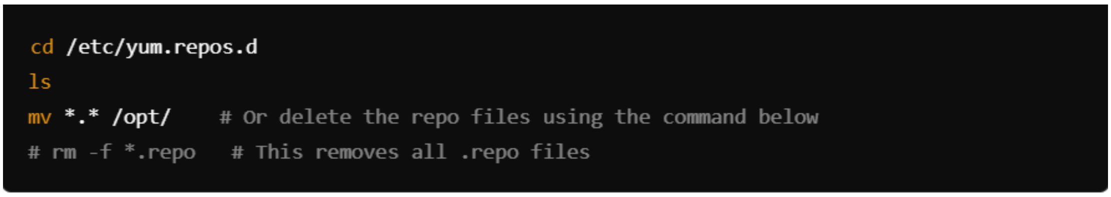


```
-rw-------. 1 root root 2108 Sep 23 23:03 anaconda-ks.cfg
drwxr-xr-x. 2 root root   50 Sep 25 13:21 Desktop
drwxr-xr-x. 2 root root    6 Sep 24 10:16 Documents
drwxr-xr-x. 2 root root   28 Sep 25 13:01 Downloads
-rw-r--r--. 1 root root 2156 Sep 23 23:06 initial-setup-ks.cfg
drwxr-xr-x. 2 root root    6 Sep 24 10:16 Music
drwxr-xr-x. 2 root root    6 Sep 24 10:16 Pictures
drwxr-xr-x. 2 root root    6 Sep 24 10:16 Public
-rw-r--r--. 1 root root  103 Sep 24 23:28 repo.local
drwxr-xr-x. 2 root root    6 Sep 24 10:16 Templates
drwxr-xr-x. 2 root root    6 Sep 24 10:16 Videos
[root@localhost ~]# mount /dev/sr0 /mnt
mount: /dev/sr0 is write-protected, mounting read-only
mount: /dev/sr0 is already mounted or /mnt busy
       /dev/sr0 is already mounted on /run/media/root/CentOS 7 x8
6_641
       /dev/sr0 is already mounted on /mnt
[root@localhost ~]# 
```

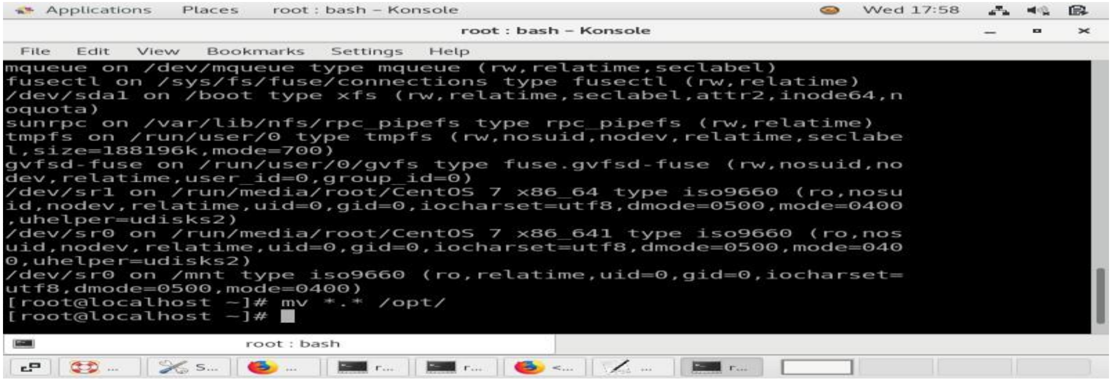
```
,uhelper=udisks2)
/dev/sr0 on /run/media/root/CentOS 7 x86_641 type iso9660 (ro,nos
uid,nodev,relatime,uid=0,gid=0,iocharset=utf8,dmode=0500,mode=040
0,uhelper=udisks2)
/dev/sr0 on /mnt type iso9660 (ro,relatime,uid=0,gid=0,iocharset=
utf8,dmode=0500,mode=0400)
[root@localhost ~]# 
```

STEP 3. Remove Existing Repos :

To remove or move the existing YUM repository files:



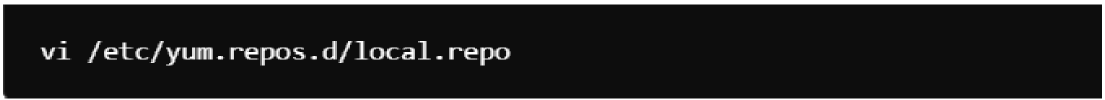
```
cd /etc/yum.repos.d
ls
mv *.* /opt/    # Or delete the repo files using the command below
# rm -f *.repo   # This removes all .repo files
```



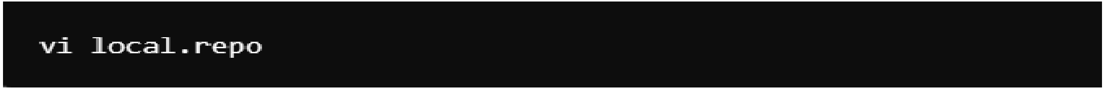
```
mqueue on /dev/mqueue type mqueue (rw,relatime,seclabel)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/sda1 on /boot type xfs (rw,relatime,seclabel,attr2,inode64,n
oquota)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,seclabe
l,size=188196k,mode=700)
gvfsd-fuse on /run/user/0/gvfs type fuse.gvfsd-fuse (rw,nosuid,no
dev,relatime,user_id=0,group_id=0)
/dev/sr1 on /run/media/root/CentOS 7 x86_64 type iso9660 (ro,nosu
id,nodev,relatime,uid=0,gid=0,iocharset=utf8,dmode=0500,mode=0400
,uhelper=udisks2)
/dev/sr0 on /run/media/root/CentOS 7 x86_641 type iso9660 (ro,nos
uid,nodev,relatime,uid=0,gid=0,iocharset=utf8,dmode=0500,mode=040
0,uhelper=udisks2)
/dev/sr0 on /mnt type iso9660 (ro,relatime,uid=0,gid=0,iocharset=
utf8,dmode=0500,mode=0400)
[root@localhost ~]# mv *.* /opt/
[root@localhost ~]# 
```

STEP 4. Create a Local Repository File

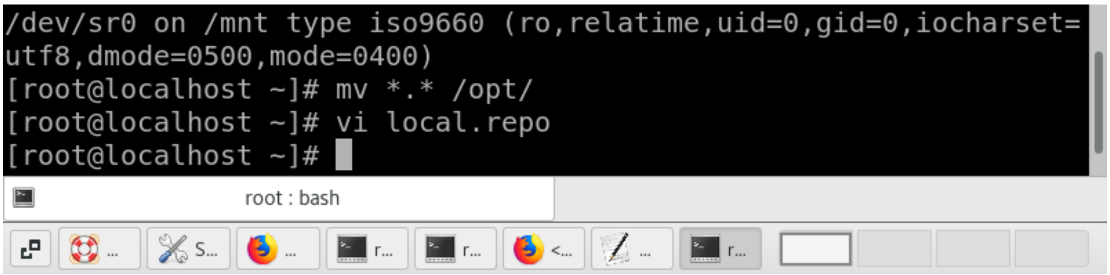
Now,creating a repository file for the local ISO:



```
vi /etc/yum.repos.d/local.repo
```

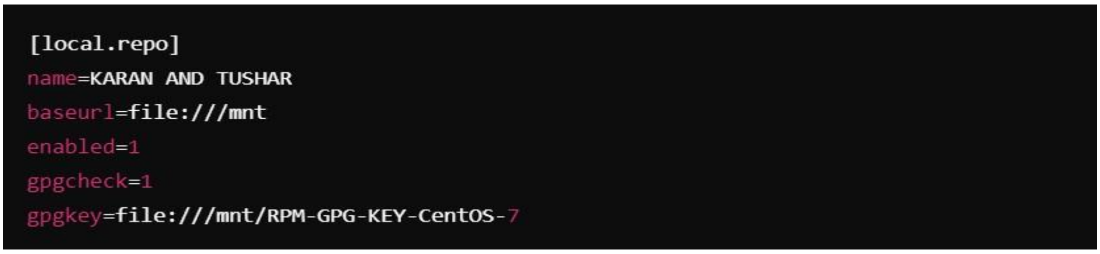


```
vi local.repo
```

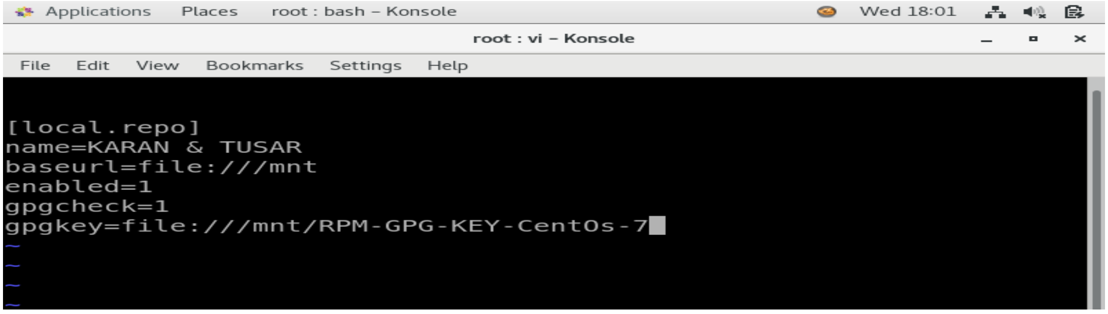


```
/dev/sr0 on /mnt type iso9660 (ro,relatime,uid=0,gid=0,iocharset=
utf8,dmode=0500,mode=0400)
[root@localhost ~]# mv *.* /opt/
[root@localhost ~]# vi local.repo
[root@localhost ~]#
```

Add the following lines to the file:

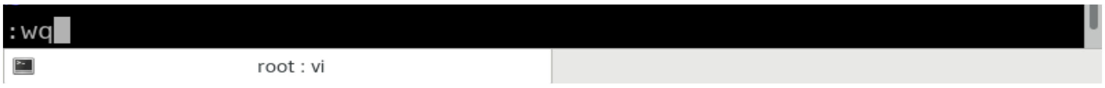


```
[local.repo]
name=KARAN AND TUSHAR
baseurl=file:///mnt
enabled=1
gpgcheck=1
gpgkey=file:///mnt/RPM-GPG-KEY-CentOS-7
```



```
[local.repo]
name=KARAN & TUSAR
baseurl=file:///mnt
enabled=1
gpgcheck=1
gpgkey=file:///mnt/RPM-GPG-KEY-CentOs-7
~
~
~
~
```

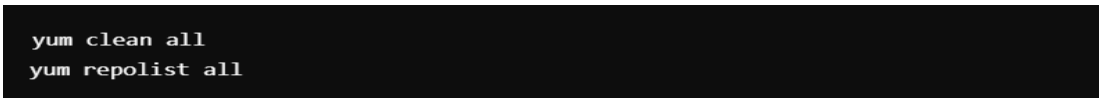
Save and close the file by typing :wq.



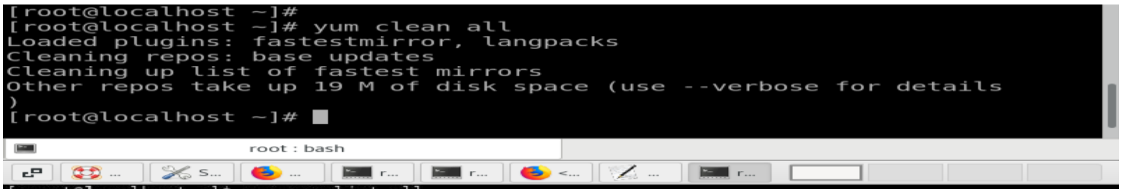
```
:wq
```

STEP 5. Clean YUM Cache and List Repositories

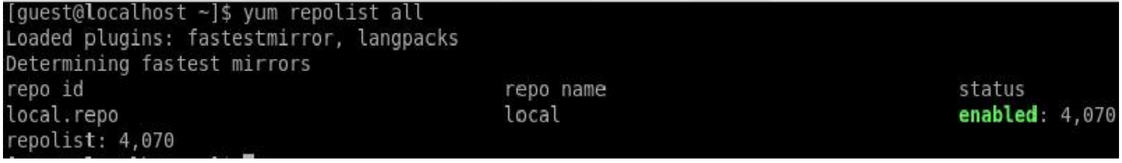
Clean the YUM cache and verify if the repository is properly configured:



```
yum clean all
yum repolist all
```



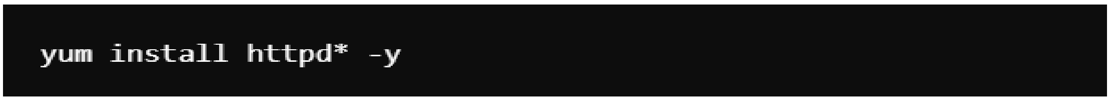
```
[root@localhost ~]#
[root@localhost ~]# yum clean all
Loaded plugins: fastestmirror, langpacks
Cleaning repos: base updates
Cleaning up list of fastest mirrors
Other repos take up 19 M of disk space (use --verbose for details
)
[root@localhost ~]# █
```



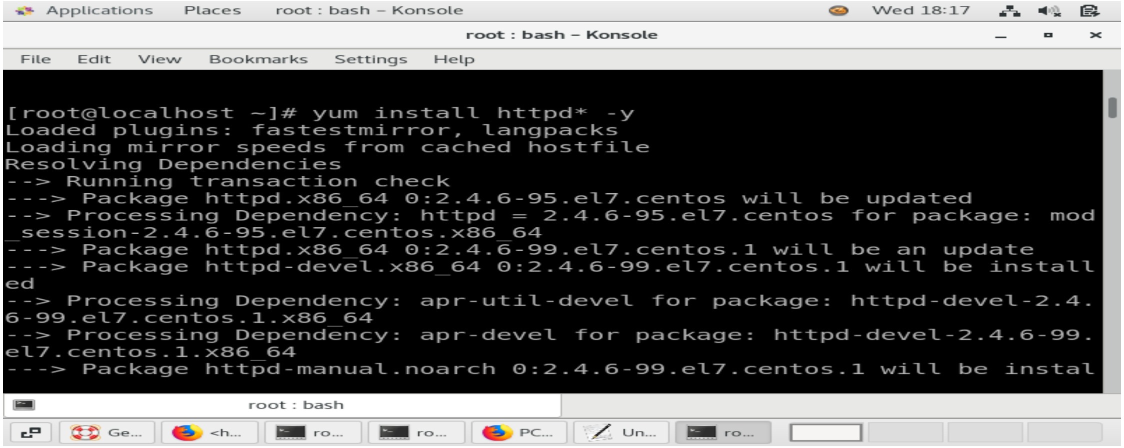
```
[guest@localhost ~]$ yum repolist all
Loaded plugins: fastestmirror, langpacks
Determining fastest mirrors
repo id                              repo name                         status
local.repo                           local                             enabled: 4,070
repolist: 4,070
```

STEP 6. Install Apache Web Server

To install Apache (httpd), run:

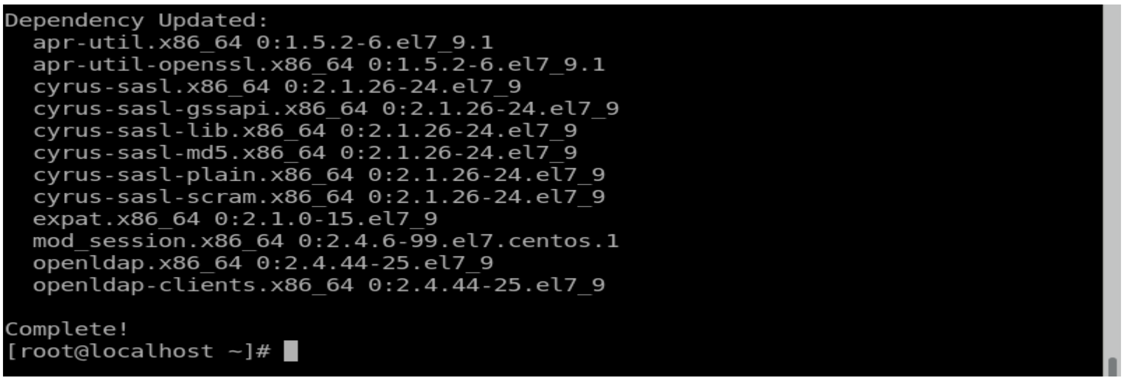


```
yum install httpd* -y
```



```
[root@localhost ~]# yum install httpd* -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.6-95.el7.centos will be updated
--> Processing Dependency: httpd = 2.4.6-95.el7.centos for package: mod
_session-2.4.6-95.el7.centos.x86_64
---> Package httpd.x86_64 0:2.4.6-99.el7.centos.1 will be an update
---> Package httpd-devel.x86_64 0:2.4.6-99.el7.centos.1 will be install
ed
--> Processing Dependency: apr-util-devel for package: httpd-devel-2.4.
6-99.el7.centos.1.x86_64
--> Processing Dependency: apr-devel for package: httpd-devel-2.4.6-99.
el7.centos.1.x86_64
---> Package httpd-manual.noarch 0:2.4.6-99.el7.centos.1 will be instal
```

This will install the Apache web server and all its dependencies.

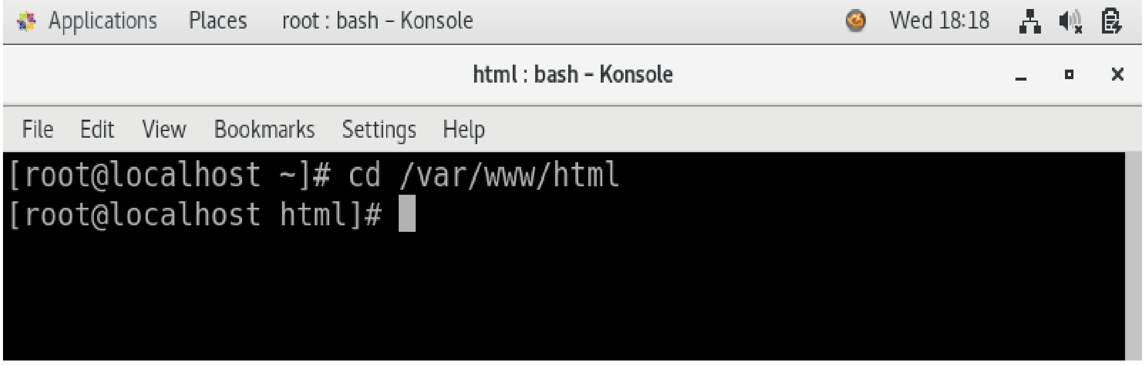


```
Dependency Updated:
  apr-util.x86_64 0:1.5.2-6.el7_9.1
  apr-util-openssl.x86_64 0:1.5.2-6.el7_9.1
  cyrus-sasl.x86_64 0:2.1.26-24.el7_9
  cyrus-sasl-gssapi.x86_64 0:2.1.26-24.el7_9
  cyrus-sasl-lib.x86_64 0:2.1.26-24.el7_9
  cyrus-sasl-md5.x86_64 0:2.1.26-24.el7_9
  cyrus-sasl-plain.x86_64 0:2.1.26-24.el7_9
  cyrus-sasl-scram.x86_64 0:2.1.26-24.el7_9
  expat.x86_64 0:2.1.0-15.el7_9
  mod_session.x86_64 0:2.4.6-99.el7.centos.1
  openldap.x86_64 0:2.4.44-25.el7_9
  openldap-clients.x86_64 0:2.4.44-25.el7_9

Complete!
[root@localhost ~]# █
```

STEP 7. Verify Apache Installation

To verify if Apache is installed, navigate to its web root directory:

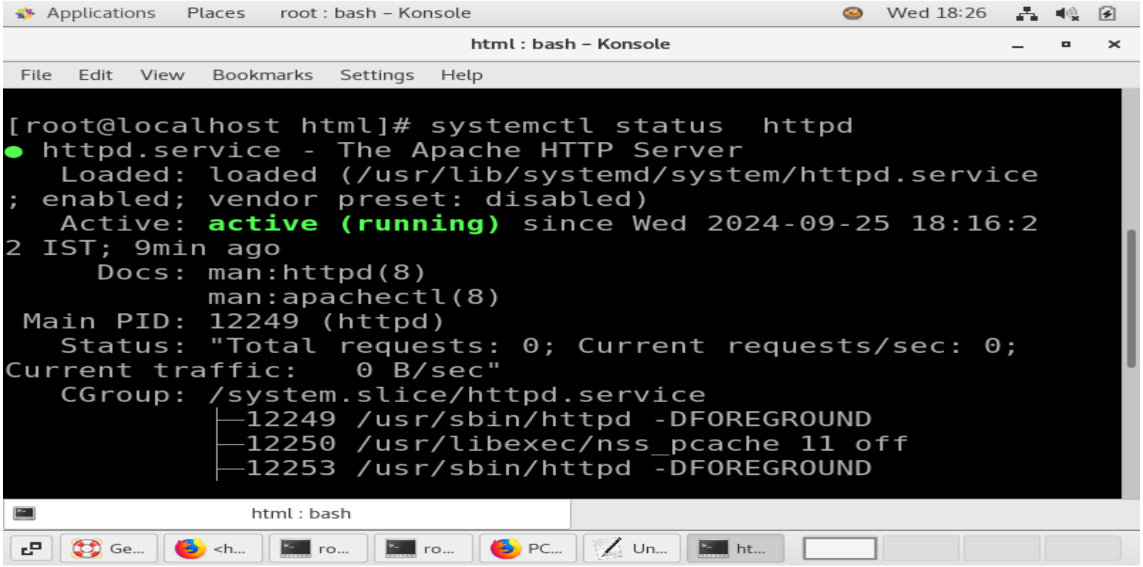
```
cd /var/www/html/
```



```
[root@localhost ~]# cd /var/www/html
[root@localhost html]# 
```

checking the status of the Apache service:

```
systemctl status httpd
```

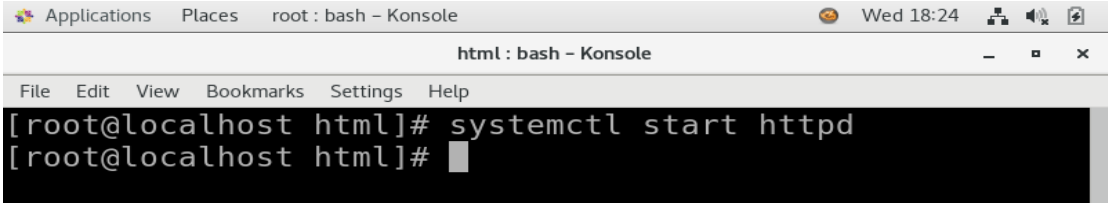


```
[root@localhost html]# systemctl status  httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service
; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-09-25 18:16:2
2 IST; 9min ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 12249 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0;
Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─12249 /usr/sbin/httpd -DFOREGROUND
           ├─12250 /usr/libexec/nss_pcache 11 off
           └─12253 /usr/sbin/httpd -DFOREGROUND
```

STEP 8. Start and Enable Apache

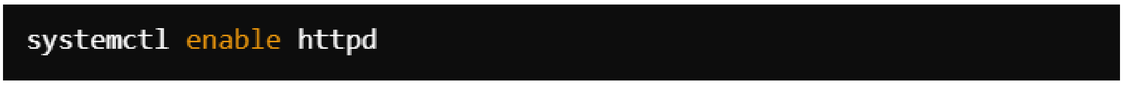
1 To start the Apache service:

```
systemctl start httpd
```

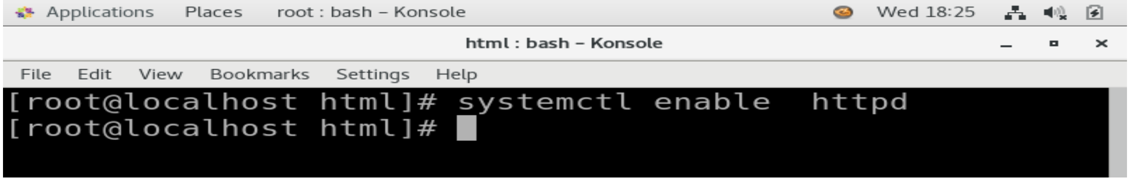


```
[root@localhost html]# systemctl start httpd
[root@localhost html]# 
```

2 To enable the Apache service to start at boot:



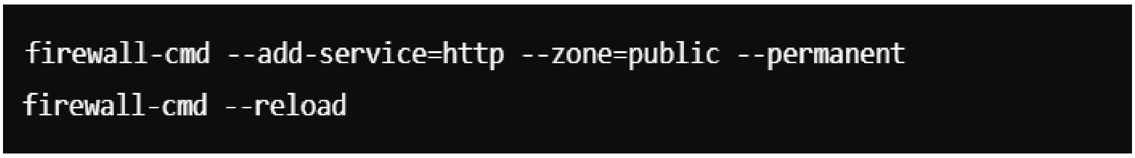
```
systemctl enable httpd
```



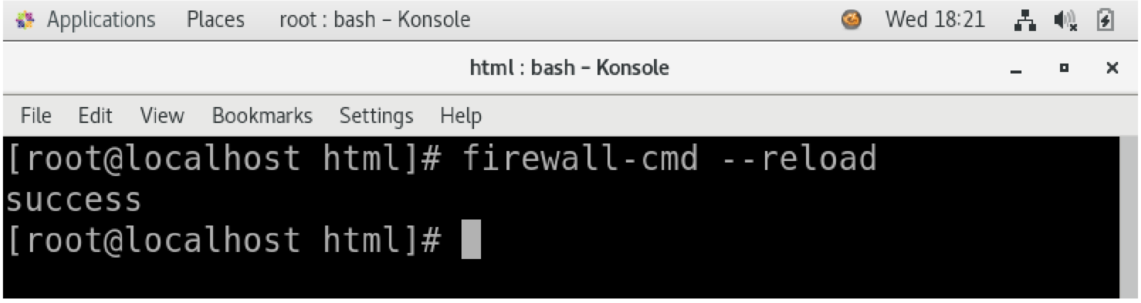
```
[root@localhost html]# systemctl enable  httpd
[root@localhost html]# 
```

STEP 9. Configure Firewall to Allow HTTP Traffic

Allow the HTTP service through the firewall using the following command:

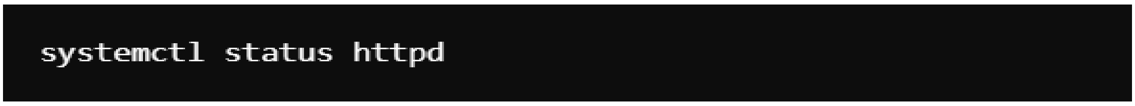


```
firewall-cmd --add-service=http --zone=public --permanent
firewall-cmd --reload
```

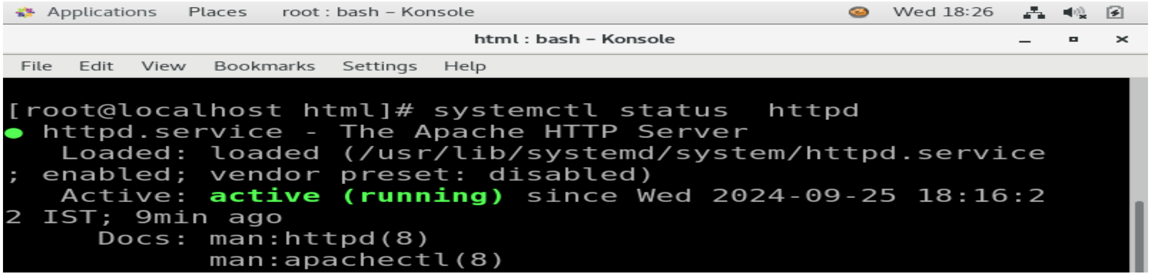


```
[root@localhost html]# firewall-cmd --reload
success
[root@localhost html]# 
```

STEP 10. Verify Apache is Running



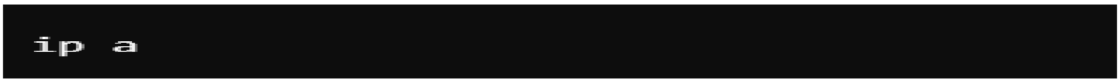
```
systemctl status httpd
```



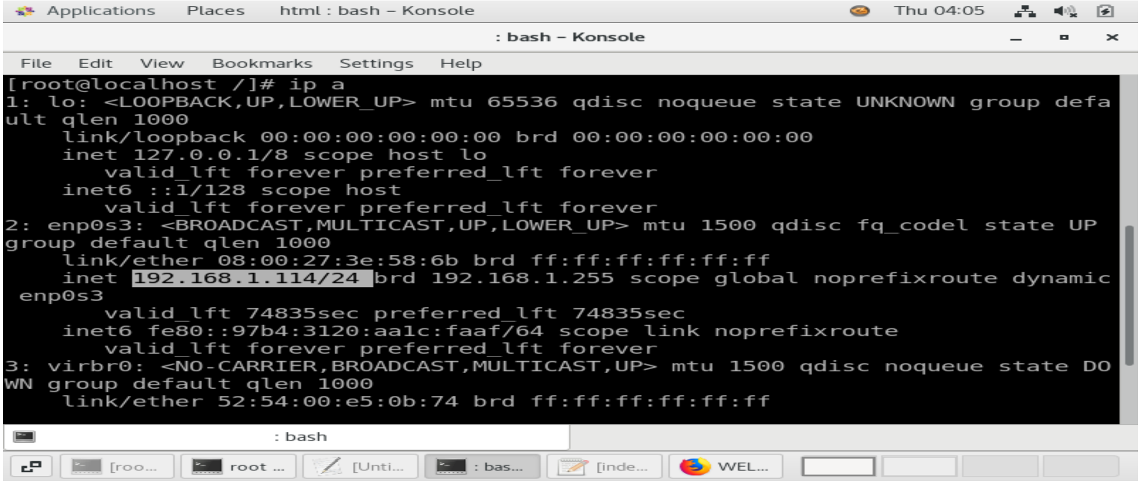
```
[root@localhost html]# systemctl status  httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service
; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-09-25 18:16:2
2 IST; 9min ago
     Docs: man:httpd(8)
           man:apachectl(8)
```

Make sure it shows active (running).

STEP 11. Test Apache in Browser

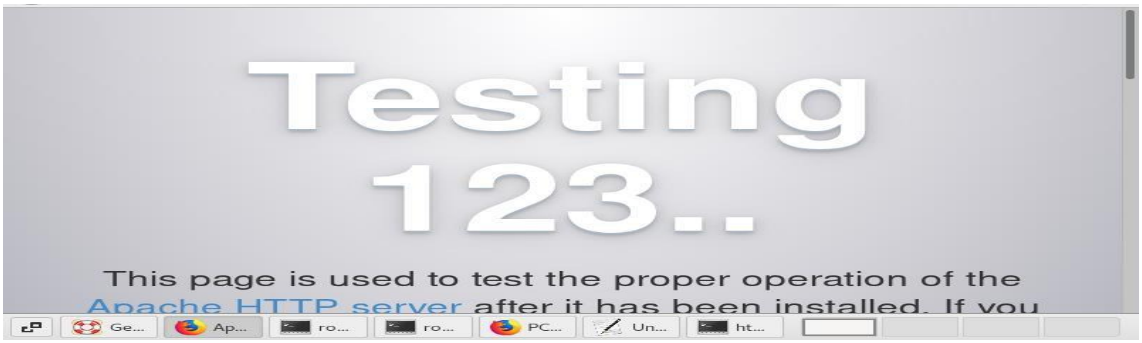


```
ip a
```



```
[root@localhost /]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult 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 08:00:27:3e:58:6b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.114/24 brd 192.168.1.255 scope global noprefixroute dynamic
 enp0s3
       valid_lft 74835sec preferred_lft 74835sec
    inet6 fe80::97b4:3120:aa1c:faaf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DO
WN group default qlen 1000
    link/ether 52:54:00:e5:0b:74 brd ff:ff:ff:ff:ff:ff
```

Open a browser and type the IP address of your virtual machine :



Testing 123..

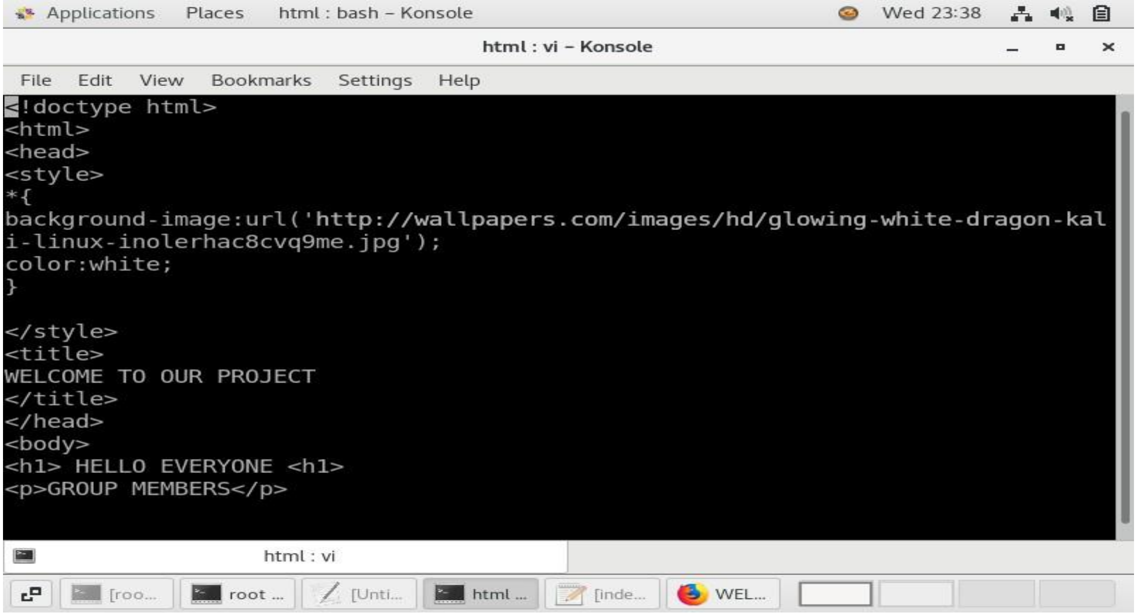
This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you

STEP 10. Steps to Edit index.html in vi

1 Open the file:

```
vi index.html
```

2 **Press** ito enter "Insert" mode. **Type or paste your HTML content**. For example,a basic HTML structure might look like this:



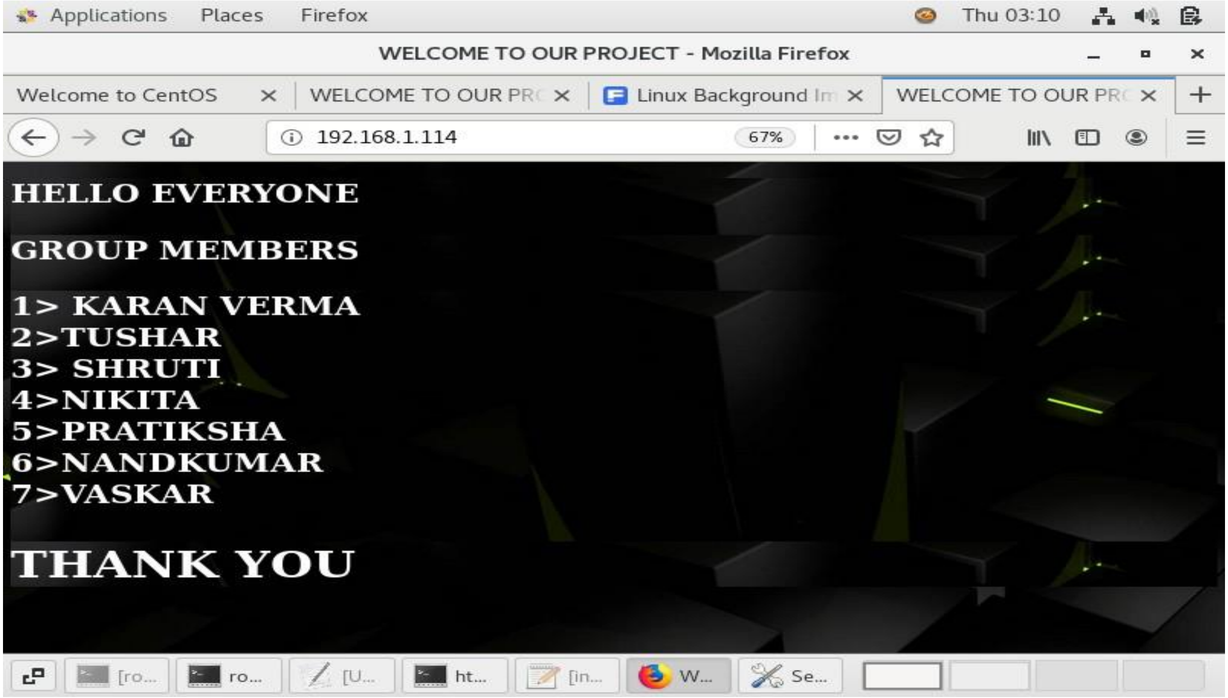
Applications Places html : bash – Konsole Wed 23:38
html : vi – Konsole
File Edit View Bookmarks Settings Help

```
<!doctype html>
<html>
<head>
<style>
*{
background-image:url('http://wallpapers.com/images/hd/glowing-white-dragon-kal
i-linux-inolerhac8cvq9me.jpg');
color:white;
}

</style>
<title>
WELCOME TO OUR PROJECT
</title>
</head>
<body>
<h1> HELLO EVERYONE <h1>
<p>GROUP MEMBERS</p>
```

3 **Press** Escto exit "Insert" mode.

4 **Type** :wqand press Enterto save and exit the file.

STEP 11 : browse your server's IP address in a browser :



HELLO EVERYONE

GROUP MEMBERS

1> KARAN VERMA
2>TUSHAR
3> SHRUTI
4>NIKITA
5>PRATIKSHA
6>NANDKUMAR
7>VASKAR

THANK YOU

FTP Server Administrator

Configuring an FTP server allows you to transfer files between a server and a client over a network using the FTP protocol. Here's an overview of the essential concepts, components, and steps involved in setting up an FTP server, typically using vsftpd (Very Secure FTP Daemon) on Linux.

1.FTP (File Transfer Protocol) Overview

FTP is a standard network protocol used for transferring files between a client and server over a TCP-based network, such as the Internet or an intranet. FTP follows a client-server model where the server hosts files and the client can upload or download files.

- **Key Features**:
  - File Upload and Download: Transfer files in both directions.
  - User Authentication: Authenticate users with username and password.
  - Anonymous Access (optional): Allows public access to download files without requiring login credentials.

2. vsftpd (Very Secure FTP Daemon)

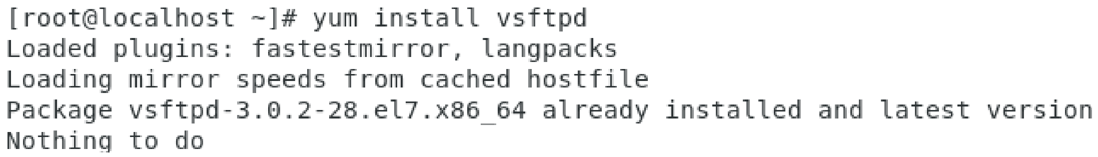
vsftpd is one of the most widely used and secure FTP server applications for Linux distributions such as CentOS, Ubuntu, and Fedora. It is known for its performance, security, and ease of configuration.

- **Key Features**:
  - Support for local users and anonymous FTP.
  - Enforces security policies (e.g., chroot jail for users).
  - Built-in options for file access control.
  - Passive and active mode support for network communication.

Step 1: FTP Server Configuration on CentOS 7

1. Install vsftpd

This installs the vsftpd (Very Secure FTP Daemon) package on CentOS, a commonly used FTP server. The yum install command fetches the software from the default CentOS repository.



```
[root@localhost ~]# yum install vsftpd
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
Package vsftpd-3.0.2-28.el7.x86_64 already installed and latest version
Nothing to do
```

2. Start and enable vsftpd service

The systemctl commands start the FTP service and enable it to run automatically on system boot.

- **sudo systemctl start vsftpd**

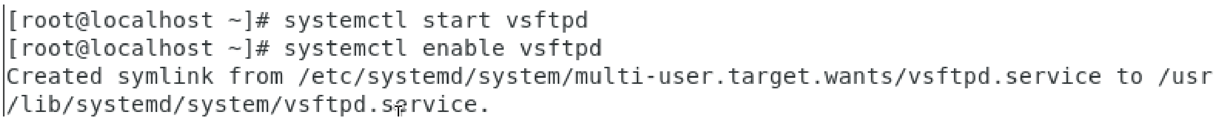
  This command starts the vsftpd service immediately, allowing the FTP server to run and begin accepting connections. If the service is not already running, this will activate it without needing a reboot.

- **sudo systemctl enable vsftpd**

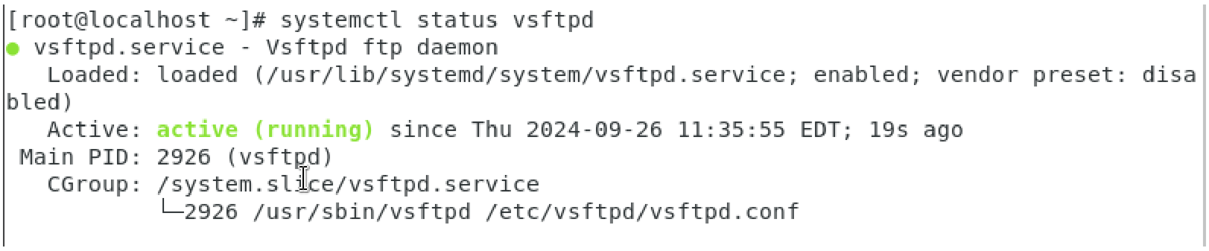
This command ensures that the vsftpd service starts automatically at boot. By enabling it, the service will launch each time the system is restarted, ensuring continuous availability of the FTP server.

- **sudo systemctl status vsftpd**

  This command checks the current status of the vsftpd service. It displays whether the service is active (running), inactive (stopped), or failed, along with additional information such as the process ID, uptime, and recent log messages.



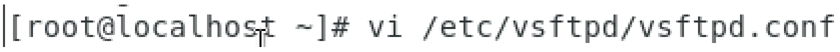
```
[root@localhost ~]# systemctl start vsftpd
[root@localhost ~]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service to /usr
/lib/systemd/system/vsftpd.service.
```



```
[root@localhost ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disa
bled)
   Active: active (running) since Thu 2024-09-26 11:35:55 EDT; 19s ago
 Main PID: 2926 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─2926 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
```

3. Configure vsftpd

Edit the configuration file to allow local users, enable file uploads, and restrict users to their home directories. These settings secure the FTP environment and customize behavior.



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

Make sure the following settings are adjusted according to your needs :

Enable local user login:

local_enable=YES

Enable file upload and modification:

write_enable=YES

Restrict users to their home directory:

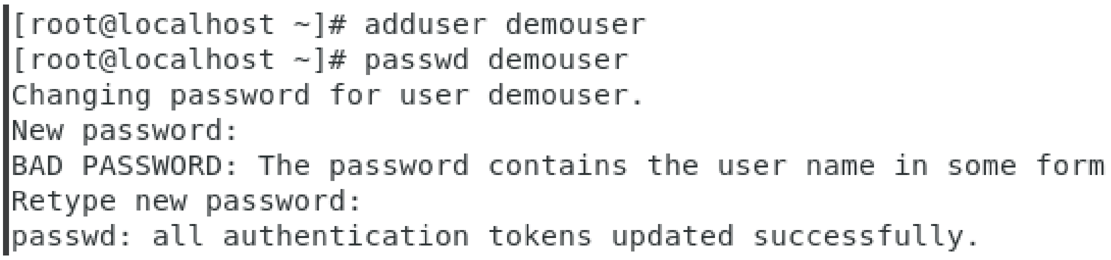
chroot_local_user=YES

Allow anonymous access (not recommended for file sharing):

anonymous_enable=NO

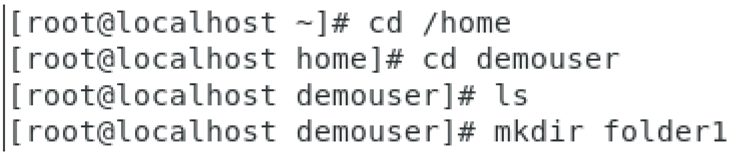
4. Add FTP users

The useradd command creates a new system user (in this case, demouser), and passwd sets the password for that user.

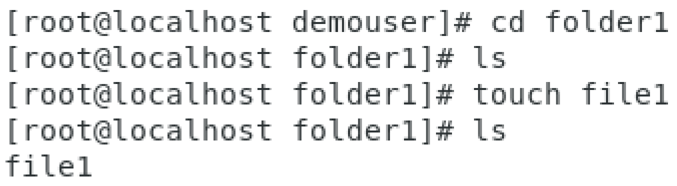


```
[root@localhost ~]# adduser demouser
[root@localhost ~]# passwd demouser
Changing password for user demouser.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
```

Optionally, create a shared directory for all users :



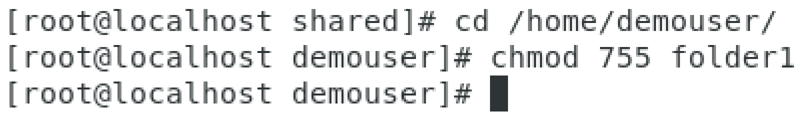
```
[root@localhost ~]# cd /home
[root@localhost home]# cd demouser
[root@localhost demouser]# ls
[root@localhost demouser]# mkdir folder1
```



```
[root@localhost demouser]# cd folder1
[root@localhost folder1]# ls
[root@localhost folder1]# touch file1
[root@localhost folder1]# ls
file1
```

5. Set permissions for FTP directories

This ensures that the ftpuser can write and access files in the designated shared directory. The chmod 755 command allows the owner to write, while others can read and execute.



```
[root@localhost shared]# cd /home/demouser/
[root@localhost demouser]# chmod 755 folder1
[root@localhost demouser]#
```

6. Adjust the firewall

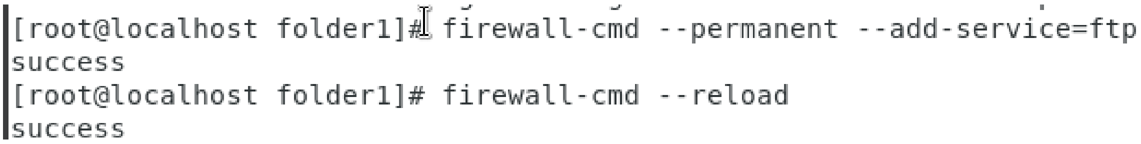
The firewall-cmd commands open FTP (port 21) in the firewall to allow incoming FTP connections. Reloading applies the changes.

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 :

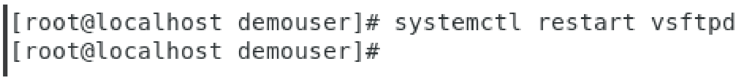
This command reloads the firewall configuration to apply any new changes made (such as allowing FTP service). It activates the updated rules without needing a system reboot.



```
[root@localhost folder1]# firewall-cmd --permanent --add-service=ftp
success
[root@localhost folder1]# firewall-cmd --reload
success
```

7. Restart the FTP server

After making changes to the configuration file, restart the vsftpd service to apply them.



```
[root@localhost demouser]# systemctl restart vsftpd
[root@localhost demouser]#
```

Step 2: FTP Client Configuration

1. Connect to the FTP server

ftp <server_ip_or_domain>
The ftp command initiates a connection from the client to the specified FTP server using its IP address or domain. This opens a session, and you will be prompted to log in with your FTP credentials.
Example:
ftp 192.168.122.1

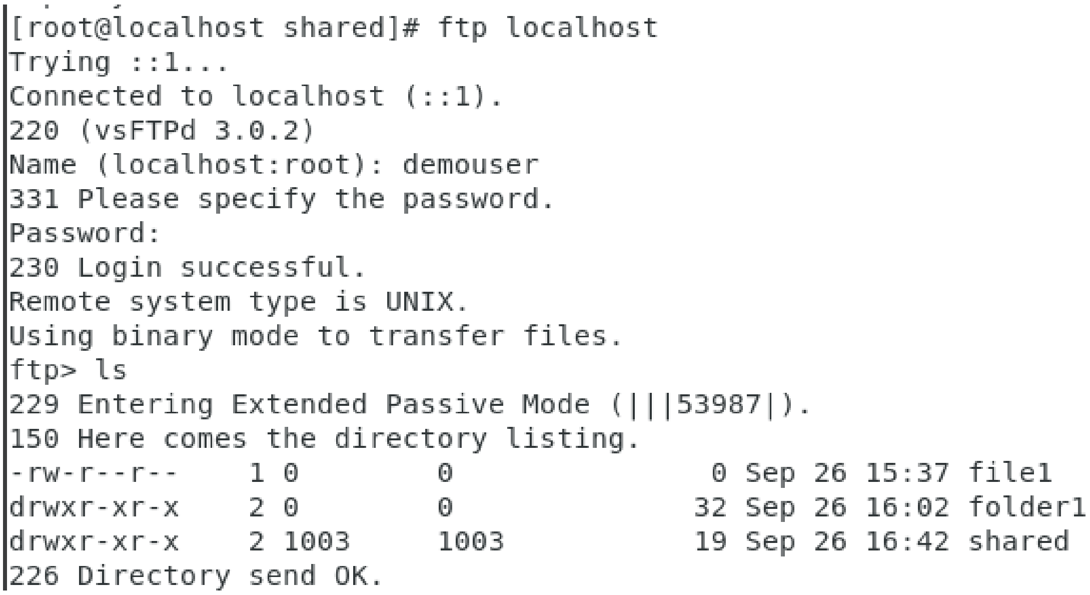
2. Login with your FTP username and password

After entering the ftp command, the system prompts for a Username and Password. These are the credentials created for the FTP server.

Once the credentials are verified, you’ll have access to the files and directories available to the FTP user.

3. View files on the server

The ls command lists the contents (files and directories) of the current directory on the remote FTP server. It shows what’s available for the connected user to download or manage.



```
[root@localhost shared]# ftp localhost
Trying ::1...
Connected to localhost (::1).
220 (vsFTPd 3.0.2)
Name (localhost:root): demouser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53987|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0               0 Sep 26 15:37 file1
drwxr-xr-x    2 0        0              32 Sep 26 16:02 folder1
drwxr-xr-x    2 1003     1003           19 Sep 26 16:42 shared
226 Directory send OK.
```