

SYSTEM ADMINISTRATION (CIT6314)

PROJECT (30%)

Student Name : Maab Abdalla Awadalla

TASK A: LINUX SERVER SELECTION, INSTALLATION & CONFIGURATION

1. Linux Distribution Selection and Justification

1.1 Selected Distribution

Distribution Name: Rocky Linux v.10.1

1.2 Justification for Selection

System Stability:

- compatible with red hat enterprise binary which make it more reliable in regard of distribution performance(RESF, 2024).
- It offers long term support and maintance(RESF, 2024).
- Rocky Linux has been tested and validated and is used in real world systems, which ensure its reliability(Red Hat, 2023).

Package Management:

- Rocky Linux uses DNF (Dandified YUM) package manager which has strong dependency resolution (Fedora Project, 2023).
- The available access to large software packages which work perfectly with RHEL(Red Hat, 2023).
- Modular repositories which allow different versions of the same software within the same reposistory(Red Hat, 2023).

Security Features:

- In Rocky Linux SELinux (Security-Enhanced Linux) is enabled by default which provide Mandatory Access Control (National Security Agency [NSA] & Red Hat, 2022).
- Security updates are aligned with the RHEL release schedule (Red Hat, 2023).
- It has built in firewalld for network security management (Red Hat, 2023).

Community Support:

- Rocky Linux has strong community support as a successor to CentOS (RESF, 2024).
- Available developer resources including active forums and documentation and others (RESF, 2024).
- Enterprise-level support available through ecosystem partners (RESF, 2024).
- Compatibility with RHEL documentation and ecosystem tools (Red Hat, 2023).

2. Server Installation Process

2.1 Virtual Machine Creation

- **Hypervisor:** VMware Workstation
- **Allocated Resources:**
 - CPU: 2 cores
 - RAM: GB
 - Storage: 20 GB
 - Network Adapter: NAT

New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

Installer disc:
No drives available

Installer disc image file (iso):
C:\Users\maaba\Downloads\Rocky-10.1-x86_64-minim Browse...

Rocky Linux 64-bit detected.
To use Easy Install, insert the first disc of the set.

I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

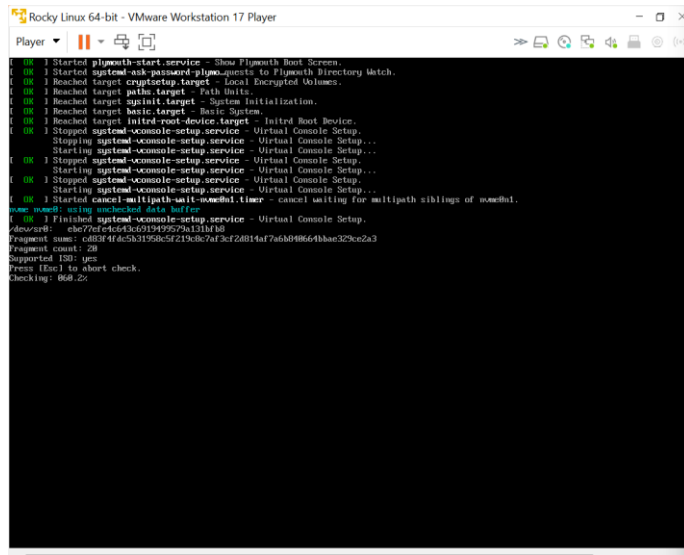
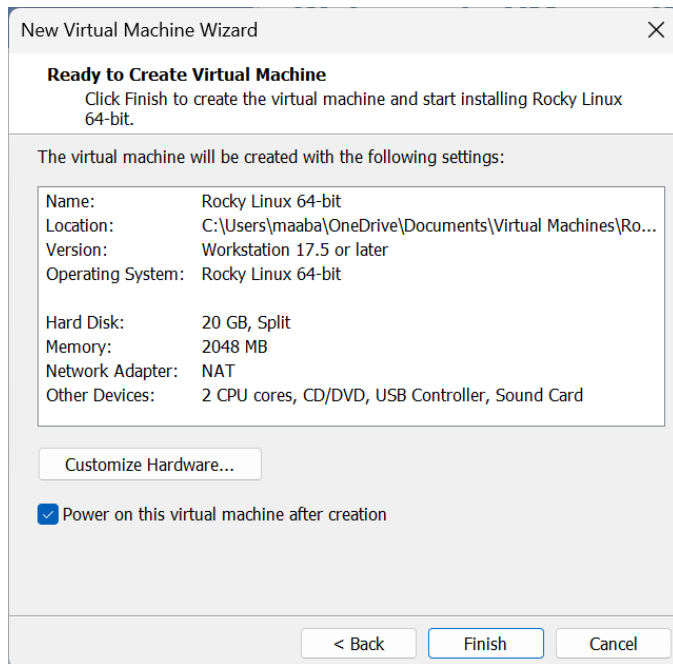
Maximum disk size (GB): 20.0

Recommended size for Rocky Linux 64-bit: 20 GB

Store virtual disk as a single file

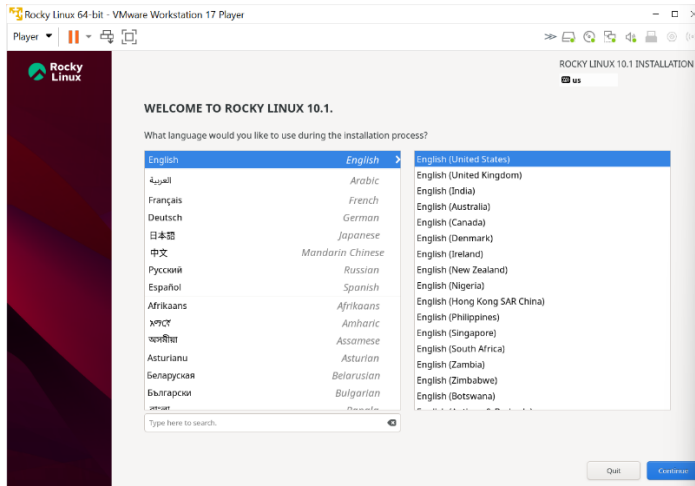
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back Next > Cancel

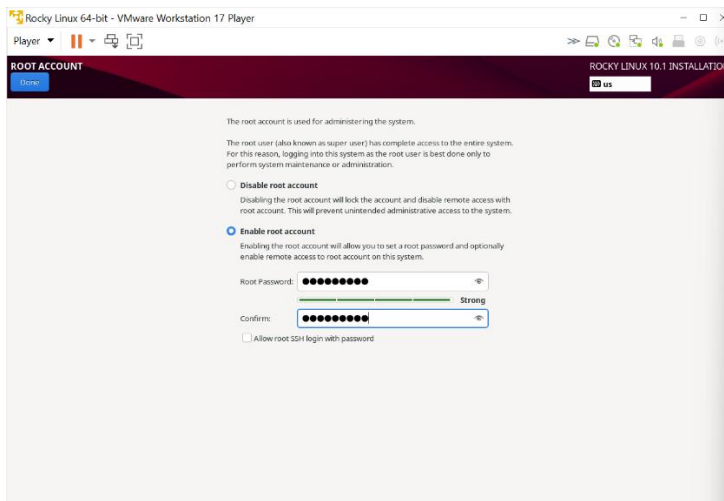
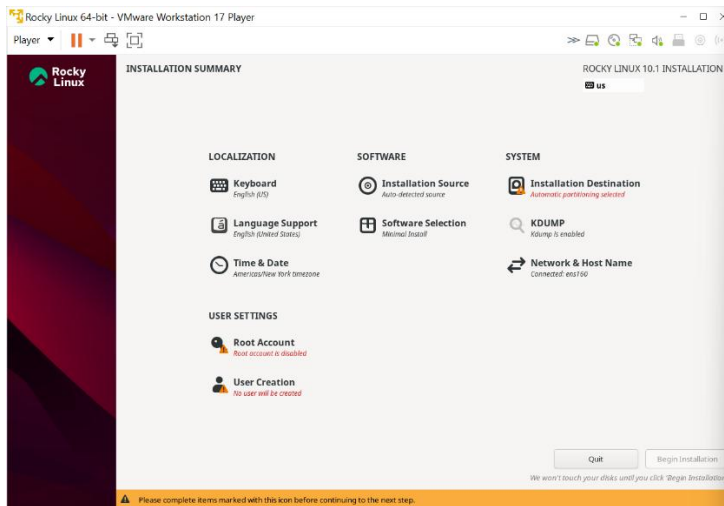


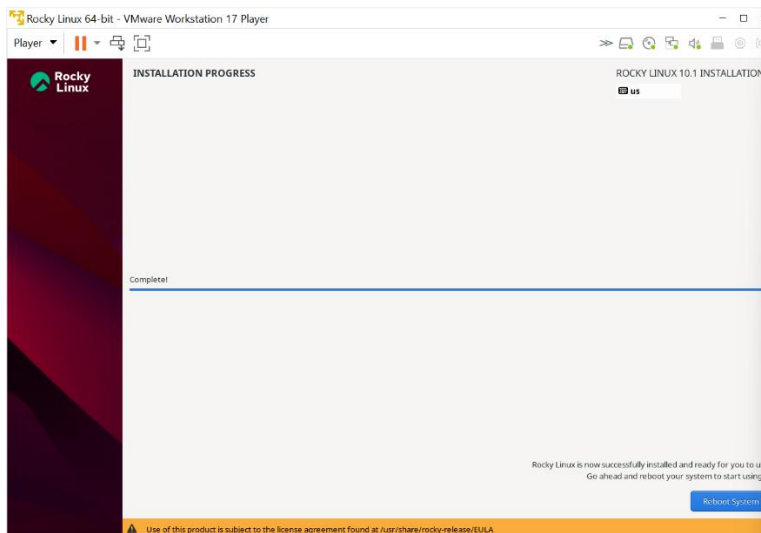
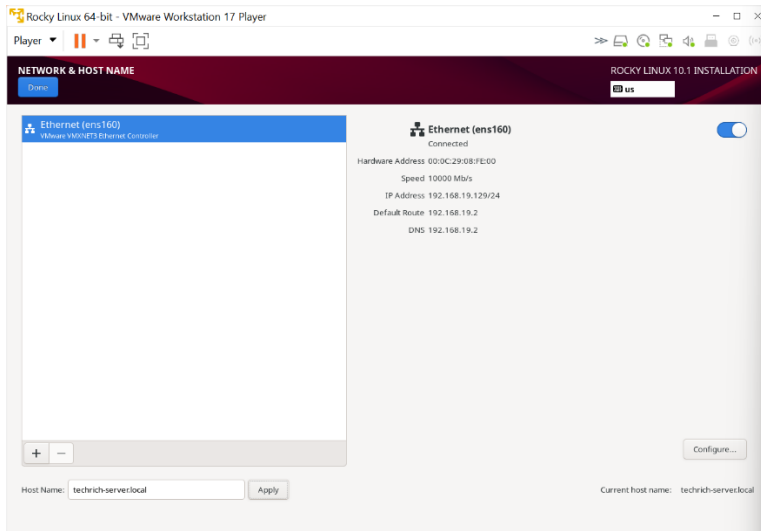
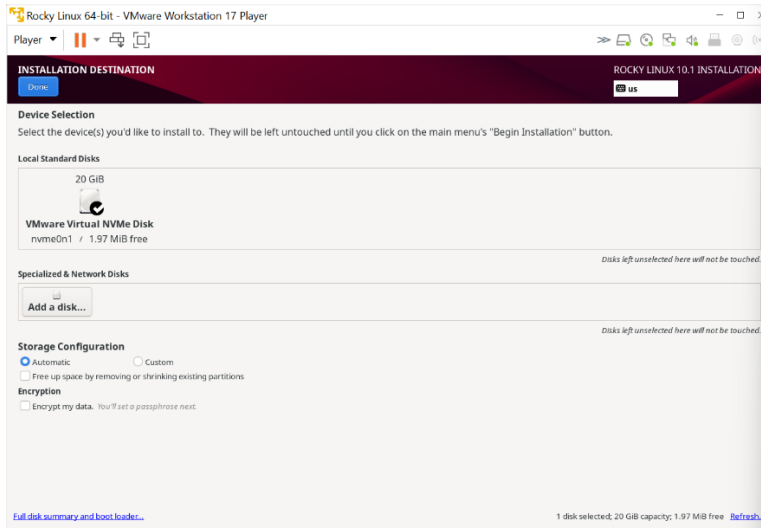
2.1 Installation Process

Selecting language: English US



Configuring installation destination, root account and hostname

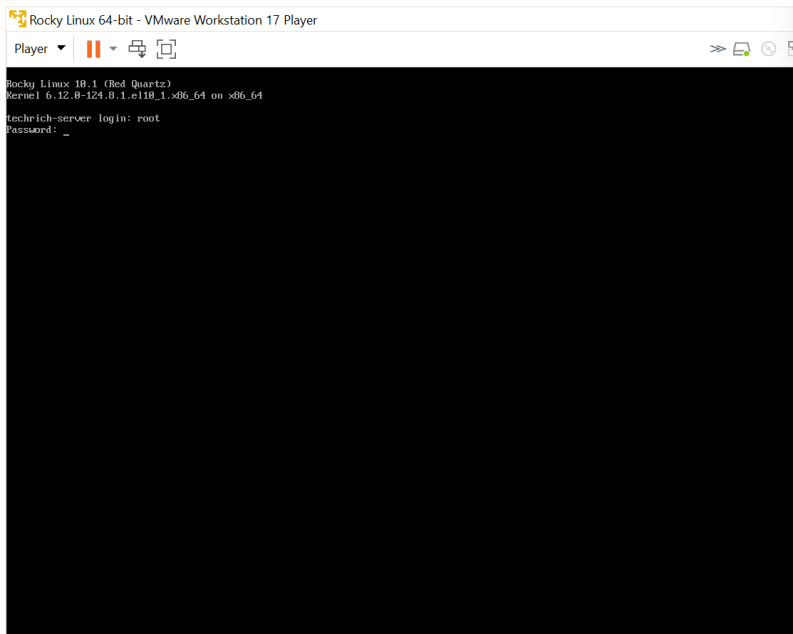




3. Initial System Configuration

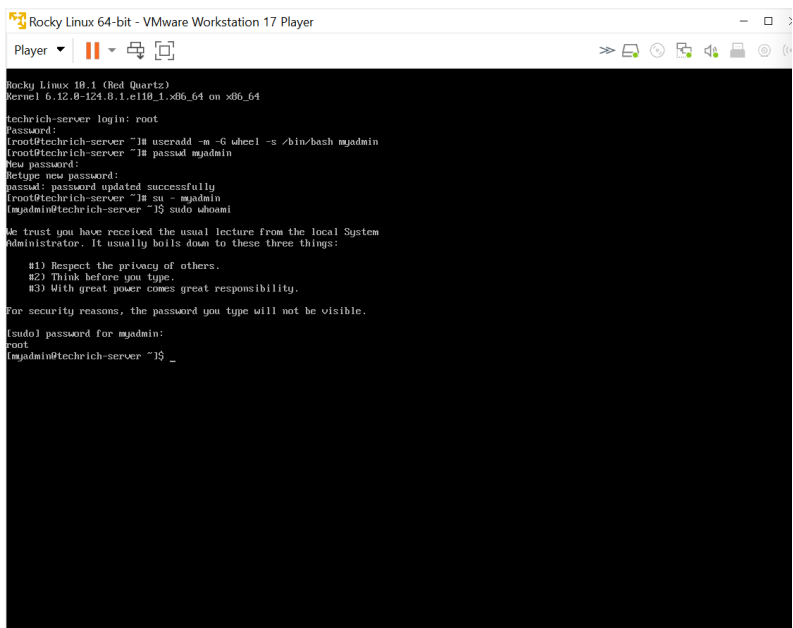
3.1 Post-Installation Updates

Login as root



```
Rocky Linux 64-bit - VMware Workstation 17 Player
Player
Rocky Linux 10.1 (Red Quartz)
Kernel 6.12.0-124.0.1.el10_1.x86_64 on x86_64
techrich-server login: root
Password: _
```

Add user myadmin and give it sudo credentials



```
Rocky Linux 64-bit - VMware Workstation 17 Player
Player
Rocky Linux 10.1 (Red Quartz)
Kernel 6.12.0-124.0.1.el10_1.x86_64
techrich-server login: root
Password:
[root@techrich-server ~]# useradd -m -s /bin/bash myadmin
[root@techrich-server ~]# passwd myadmin
New password:
Retype new password:
passwd: password updated successfully
[root@techrich-server ~]# su - myadmin
(myadmin@techrich-server ~) $ sudo whoami
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

 #1) Respect the privacy of others.
 #2) Think before you type.
 #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.
(sudo) password for myadmin:
root
(myadmin@techrich-server ~) $ _
```

```
Rocky Linux 64-bit - VMware Workstation 17 Player
Player
[admin@techrich-server ~]$ hostnamectl
Failed to query product UUID, ignoring: Access denied
Failed to query hardware serial, ignoring: Access denied
  Static hostname: techrich-server.local
    Icon name: computer-vm
  Chassis: vm
  Machine ID: 692f9124312e4c769f744bfc37558248
  Boot ID: 71f326e472041ceb91476b04cb09ff
  AF USUCK CID: 10f522649
  Virtualization: vmware
  Operating System: Rocky Linux 8.1 (Red Quartz)
  OS Name: cpe:/o:redhat:rocky:8:-baseos
  OS Support End: Thu 2035-05-31
  OS Support Remaining: 9y 4month
  Kernel: Linux 6.12.0-124.8.1.el10_1.x86_64
  Architecture: x86_64
  Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
  Firmware Version: 6.00
  Firmware Date: Thu 2020-11-12
  Firmware Age: 5y 2month 2w 1d
[admin@techrich-server ~]$
```

```
nmcli device status
[admin@techrich-server ~]$ nmcli device status
DEVICE  TYPE  STATE  CONNECTION
ens160  ethernet  connected  ens160
lo      loopback  connected (externally)  lo
[admin@techrich-server ~]$ ip route show
default via 192.168.19.2 dev ens160 proto dhcp src 192.168.19.129 metric 100
192.168.19.0/24 dev ens160 proto kernel scope link src 192.168.19.129 metric 100
[admin@techrich-server ~]$ nmcli connection modify "$INTERFACE" \_
valid_lft forever preferred_lft forever
[admin@techrich-server ~]$ nmcli device status
DEVICE  TYPE  STATE  CONNECTION
ens160  ethernet  connected  ens160
lo      loopback  connected (externally)  lo
[admin@techrich-server ~]$ ip route show
default via 192.168.19.2 dev ens160 proto dhcp src 192.168.19.129 metric 100
192.168.19.0/24 dev ens160 proto kernel scope link src 192.168.19.129 metric 100
[admin@techrich-server ~]$ nmcli connection modify "$INTERFACE" \_
valid_lft forever preferred_lft forever
```

Setting network configurations

```
Rocky Linux 64-bit - VMware Workstation 17 Player
Player
[sudo] password for admin:
[admin@techrich-server ~]$ sudo nmcli connection down "$INTERFACE"
sudo: nmcli: command not found
[admin@techrich-server ~]$ sudo nmcli connection down "$INTERFACE"
Connection 'ens160' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
[admin@techrich-server ~]$ sudo nmcli connection up "$INTERFACE"
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
[admin@techrich-server ~]$ ip addr show "$INTERFACE"
2: ens160: <BRIDGEPORT,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:80:fe:80 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens30
    inet 192.168.19.129/24 brd 192.168.19.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::2980:fe80::64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@techrich-server ~]$ ping -c 4 google.com
ping: google.com: Name or service not known
[admin@techrich-server ~]$ ping -c 4 0.0.0.0
PING 0.0.0.0 (0.0.0.0) 56(84) bytes of data:
From 192.168.19.129 icmp_seq=1 Destination Host Unreachable
From 192.168.19.129 icmp_seq=2 Destination Host Unreachable
From 192.168.19.129 icmp_seq=3 Destination Host Unreachable
From 192.168.19.129 icmp_seq=4 Destination Host Unreachable

--- 0.0.0.0 ping statistics ---
 4 packets transmitted, 0 received, 100% packet loss, time 300ms
pipe 3
[admin@techrich-server ~]$ ping -c 4 google.com
PING google.com (172.217.27.14) 56(84) bytes of data:
64 bytes from sin1s82-in-f14.1e100.net (172.217.27.14): icmp_seq=1 ttl=120 time=14.2 ms
64 bytes from sin1s82-in-f14.1e100.net (172.217.27.14): icmp_seq=2 ttl=120 time=32.6 ms
64 bytes from sin1s82-in-f14.1e100.net (172.217.27.14): icmp_seq=3 ttl=120 time=14.1 ms
64 bytes from sin1s82-in-f14.1e100.net (172.217.27.14): icmp_seq=4 ttl=120 time=15.4 ms

--- google.com ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 300ms
rtt min/avg/max/mdev = 14.113/19.881/32.591/7.817 ms
[admin@techrich-server ~]$ ping -c 4 0.0.0.0
PING 0.0.0.0 (0.0.0.0) 56(84) bytes of data:
64 bytes from 0.0.0.0: icmp_seq=1 ttl=120 time=7.71 ms
64 bytes from 0.0.0.0: icmp_seq=2 ttl=120 time=6.90 ms
64 bytes from 0.0.0.0: icmp_seq=3 ttl=120 time=6.62 ms
64 bytes from 0.0.0.0: icmp_seq=4 ttl=120 time=6.72 ms

--- 0.0.0.0 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 300ms
rtt min/avg/max/mdev = 6.722/7.407/8.622/0.752 ms
[admin@techrich-server ~]$
```

Installing GUI for Rocky Linux

```

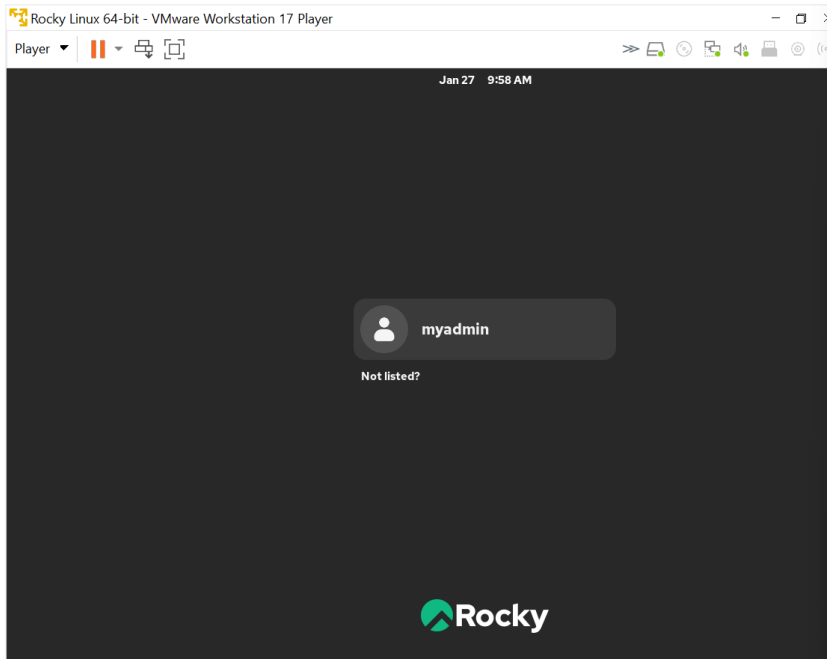
Rocky Linux 64-bit - VMware Workstation 17 Player
Player
[myadmin@techrich-server ~]$ sudo dnf groupinstall "Server with GUI" -y

Rocky Linux 64-bit - VMware Workstation 17 Player
Player
Total download size: 1.0 G
Downloading Packages:
(1/983): NetworkManager-ads1-1.54.0-2.el10_1.x86_64.rpm          193 kB/s |
(2/983): NetworkManager-glib-1.22.0-7.el10.x86_64.rpm          1.5 MB/s |
(3/983): NetworkManager-bluetooth-1.54.0-2.el10_1.x86_64.rpm   779 kB/s |
(4/983): NetworkManager-config-server-1.54.0-2.el10_1.noarch.rpm 182 kB/s |
(5/983): NetworkManager-wifi-1.54.0-2.el10_1.x86_64.rpm         1.1 MB/s |
(6/983): NetworkManager-wan-1.54.0-2.el10_1.x86_64.rpm         1.1 MB/s |
(7/983): ac1-2.3.2-4.el10.x86_64.rpm                            689 kB/s |
(8/983): adcli-0.9.2-9.el10.x86_64.rpm                          1.2 MB/s |
(9/983): NetworkManager-1.22.0-7.el10.x86_64.rpm               2.6 MB/s |
(10/983): at-3.2.5-14.el10.x86_64.rpm                           1.1 MB/s |
(11/983): avahi-0.9.7rc2-2.el10_0.x86_64.rpm                   2.4 MB/s |
(12/983): bc-1.07.1-23.el10.x86_64.rpm                          698 kB/s |
(13/983): bash-completions-2.11-16.el10.noarch.rpm             1.9 MB/s |
(14/983): bluez-libs-5.03-2.el10.x86_64.rpm                    425 kB/s |
(15/983): bolt-0.9.0-3.el10.x86_64.rpm                         887 kB/s |
(16/983): bluez-5.03-2.el10.x86_64.rpm                          4.2 MB/s |
(17/983): bubblewrap-0.10.0-3.el10.x86_64.rpm                  816 kB/s |
(18/983): bz2-1.0.8-25.el10.x86_64.rpm                          815 kB/s |
(19/983): cockpit-344-1.el10.rocky.0.1.x86_64.rpm              711 kB/s |
(20/983): chromium-1.6.1-2.el10.x86_64.rpm                     2.9 MB/s |
(21/983): cockpit-bridge-344-1.el10.rocky.0.1.noarch.rpm        1.1 MB/s |
(22/983): cockpit-ws-selinux-344-1.el10.rocky.0.1.x86_64.rpm    365 kB/s |
(23/983): cryptsetup-2.7.5-2.el10.x86_64.rpm                   515 kB/s |
(24/983): cockpit-system-344-1.el10.rocky.0.1.noarch.rpm        5.5 MB/s |
(25/983): cockpit-ws-344-1.el10.rocky.0.1.x86_64.rpm            1.1 MB/s |
(26/983): cups-filesystem-2.4.10-12.el10_1.2.x86_64.rpm         169 kB/s |
(27/983): cups-libs-2.4.10-12.el10_1.2.x86_64.rpm               3.5 MB/s |
(28/983): cups-sasl-plugin-2.1.20-29.el10.x86_64.rpm            348 kB/s |
(29/983): dbus-tools-1.14.10-5.el10.x86_64.rpm                  771 kB/s |
(30/983): default-fonts-core-mono-4.1-3.el10.noarch.rpm         151 kB/s |
(31/983): default-fonts-core-sans-4.1-3.el10.noarch.rpm         513 kB/s |
(32/983): default-fonts-core-serif-4.1-3.el10.noarch.rpm       169 kB/s |
(33/983): dejavu-sans-fonts-2.37-25.el10.noarch.rpm             6.2 MB/s |
(34/983): dejavu-sans-mono-fonts-2.37-25.el10.noarch.rpm        1.8 MB/s |
(35/983): dejavu-serif-fonts-2.37-25.el10.noarch.rpm            2.7 MB/s |
(36/983): device-mapper-multipath-0.9.9-12.el10.x86_64.rpm      646 kB/s |
(37/983): device-mapper-multipath-libs-0.9.9-12.el10.x86_64.rpm 864 kB/s |
(38/983): dmidecode-3.6-3.el10.x86_64.rpm                       324 kB/s |
(39/983): dos2unix-7.5.2-3.el10.x86_64.rpm                      1.2 MB/s |
(40/983): dosfstools-4.2-12.el10.x86_64.rpm                     687 kB/s |
(41/983): duktape-2.7.0-10.el10.x86_64.rpm                      855 kB/s |
(42/983): ed-1.20-5.el10.x86_64.rpm                              475 kB/s |
(43/983): fonts-filesystem-2.0.5-10.el10.noarch.rpm             249 kB/s |
(44/983): exfatprogs-1.2.0-1.el10.x86_64.rpm                    1.4 MB/s |
(45/983): fuse-common-3.16.2-5.el10.x86_64.rpm                  184 kB/s |
(46/983): freetype-2.13.2-0.el10.x86_64.rpm                     4.4 MB/s |
(47/983): fuse3-3.16.2-5.el10.x86_64.rpm                        1.8 MB/s |
(48/49/983): fusermount-1.9.11-1.el10.x86_64.rpm                 1x | =
xdg-user-dirs-gtk-0.11-6.el10.x86_64.rpm                        1 2.0 MB/s |
xkbcomp-1.4.7-3.el10.x86_64.rpm
xmail-common-0.6.3-65.el10.noarch
xmailsec1-openssl-1.1.2.39-3.el10.x86_64
xprop-1.2.7-3.el10.x86_64
xsel-1.20.10-1.el10.x86_64
xorg-x11-server-Xwayland-24.1.5-5.el10_0.x86_64
xosd-2.9.1.003-6.el10.x86_64
xorg-x11-xkb-1.3.0-10.el10.noarch
xorg-x11-xkb-1.3.0-10.el10.noarch
zip-3.0-45.el10.x86_64

Complete!
[myadmin@techrich-server ~]$ sudo systemctl set-default graphical.target
[sudo] password for myadmin:
Removed '/etc/systemd/system/default.target'.
Created symlink '/etc/systemd/system/default.target' → '/usr/lib/systemd/system/graphical.target'.
l 0702.0166861 systemd-rc-local-generator[22635]: /etc/rc.d/rc.local is not marked executable, skipping.
[myadmin@techrich-server ~]$

```

GUI Installed



Part B

User & Group Creation

Create 5 groups for the 5 department (developers, testers, HR, IT, management)

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo groupadd developers  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo groupadd developers  
groupadd: group 'developers' already exists  
myadmin@techrich-server:~$ sudo groupadd testers  
myadmin@techrich-server:~$ sudo groupadd hr  
myadmin@techrich-server:~$ sudo groupadd it  
myadmin@techrich-server:~$ management  
bash: management: command not found...  
myadmin@techrich-server:~$ sudo groupadd management  
myadmin@techrich-server:~$ getent group | grep -E 'developers|testers|hr|it|management'  
polkitd:x:114:  
rtkit:x:172:  
gnome-initial-setup:x:986:  
chrony:x:983:  
developers:x:1001:  
testers:x:1002:  
hr:x:1003:  
it:x:1004:  
management:x:1005:  
myadmin@techrich-server:~$
```

Add 10 users to each group and verify user creation, with setting default password for each user to “TechRich2026!”

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ for user in dev{01..10}; do  
  sudo useradd -m -G developers -s /bin/bash -c "Developer" $user  
  echo "TechRich2026!" | sudo passwd --stdin $user  
done  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(dev)[0-9]{2}$'  
dev01  
dev02  
dev03  
dev04  
dev05  
dev06  
dev07  
dev08  
dev09  
dev10  
myadmin@techrich-server:~$ getent group developers  
developers:x:1001:dev01,dev02,dev03,dev04,dev05,dev06,dev07,dev08,dev09,dev10  
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ for user in test{01..10}; do  
    sudo userdel -r -f $user  
done  
[sudo] password for myadmin:  
myadmin@techrich-server:~$  
myadmin@techrich-server:~$ for user in test{01..10}; do  
    sudo useradd -m -G testers -s /bin/bash -c "Tester" $user  
    echo "TechRich2026!" | sudo passwd --stdin $user  
done  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(test)[0-9]{2}$'  
test01  
test02  
test03  
test04  
test05  
test06  
test07  
test08  
test09  
test10  
myadmin@techrich-server:~$ getent group testers  
testers:x:1002:test01,test02,test03,test04,test05,test06,test07,test08,test09,test10  
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ for user in hr{01..10}; do  
    sudo useradd -m -G hr -s /bin/bash -c "HR Employee" $user  
    echo "TechRich2026!" | sudo passwd --stdin $user  
done  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(hr)[0-9]{2}$'  
hr01  
hr02  
hr03  
hr04  
hr05  
hr06  
hr07  
hr08  
hr09  
hr10  
myadmin@techrich-server:~$ getent group hr  
hr:x:1003:hr01,hr02,hr03,hr04,hr05,hr06,hr07,hr08,hr09,hr10  
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ for user in it{01..10}; do  
    sudo useradd -m -G it -s /bin/bash -c "IT Staff" $user  
    echo "TechRich2026!" | sudo passwd --stdin $user  
done  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(it)[0-9]{2}$'  
it01  
it02  
it03  
it04  
it05  
it06  
it07  
it08  
it09  
it10  
myadmin@techrich-server:~$ getent group it  
it:x:1004:it01,it02,it03,it04,it05,it06,it07,it08,it09,it10  
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ for user in mgmt{01..10}; do  
    sudo useradd -m -G management -s /bin/bash -c "Manager" $user  
    echo "TechRich2026!" | sudo passwd --stdin $user  
done  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(\management)[0-9]{2}$'  
myadmin@techrich-server:~$ getent group management  
management:x:1005:mgmt01,mgmt02,mgmt03,mgmt04,mgmt05,mgmt06,mgmt07,mgmt08,mgmt09,mgmt10  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(\management)[0-9]{2}$'  
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(\mgmt)[0-9]{2}$'  
mgmt01  
mgmt02  
mgmt03  
mgmt04  
mgmt05  
mgmt06  
mgmt07  
mgmt08  
mgmt09  
mgmt10  
myadmin@techrich-server:~$
```

Role-Based Access Control

Create group admins and add two IT admins to it, give the admins sudors credentials, the reason why creating 2 admins instead of 1 is to prevent single point of failure.

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo groupadd admins  
myadmin@techrich-server:~$ sudo usermod -aG wheel,admins it01  
myadmin@techrich-server:~$ sudo usermod -aG wheel,admins it02  
myadmin@techrich-server:~$ sudo tee /etc/sudoers.d/techrich-admins > /dev/null << 'EOF'  
it01    ALL=(ALL)    ALL  
it02    ALL=(ALL)    ALL  
EOF  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo chmod 440 /etc/sudoers.d/techrich-admins  
myadmin@techrich-server:~$ sudo visudo -c  
/etc/sudoers: parsed OK  
/etc/sudoers.d/techrich-admins: parsed OK  
myadmin@techrich-server:~$ sudo -l -U it01  
Matching Defaults entries for it01 on techrich-server:  
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,  
env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME  
LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",  
env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE  
LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin  
  
User it01 may run the following commands on techrich-server:  
(ALL) ALL  
(ALL) ALL  
myadmin@techrich-server:~$ sudo -l -U it02  
Matching Defaults entries for it02 on techrich-server:  
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,  
env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME  
LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",  
env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE
```

File & Directory Permissions

Create a shared file directory with separate subdirectories for

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo mkdir -p /shared  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo mkdir -p /shared/developers  
myadmin@techrich-server:~$ sudo mkdir -p /shared/testers  
myadmin@techrich-server:~$ sudo mkdir -p /shared/hr  
myadmin@techrich-server:~$ sudo mkdir -p /shared/it  
myadmin@techrich-server:~$ sudo mkdir -p /shared/management  
myadmin@techrich-server:~$ sudo mkdir -p /shared/common  
myadmin@techrich-server:~$ sudo mkdir -p /shared/developers  
myadmin@techrich-server:~$ ls -la /shared/  
total 0  
drwxr-xr-x. 8 root root 91 Jan 31 08:54 .  
dr-xr-xr-x. 19 root root 249 Jan 31 08:51 ..  
drwxr-xr-x. 2 root root 6 Jan 31 08:54 common  
drwxr-xr-x. 2 root root 6 Jan 31 08:52 developers  
drwxr-xr-x. 2 root root 6 Jan 31 08:52 hr  
drwxr-xr-x. 2 root root 6 Jan 31 08:52 it  
drwxr-xr-x. 2 root root 6 Jan 31 08:52 management  
drwxr-xr-x. 2 root root 6 Jan 31 08:52 testers  
myadmin@techrich-server:~$
```

change the ownership of each directory to its group

```
myadmin@techrich-server:~$ sudo chown root:developers /shared/developers  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo chown root:testers /shared/testers  
myadmin@techrich-server:~$ sudo chown root:testers /shared/testers  
myadmin@techrich-server:~$ sudo chown root:hr /shared/hr  
myadmin@techrich-server:~$ sudo chown root:it /shared/it  
myadmin@techrich-server:~$ sudo chown root:management /shared/management  
myadmin@techrich-server:~$ sudo chown root:root /shared/common  
myadmin@techrich-server:~$ ls -l /shared/  
total 0  
drwxr-xr-x. 2 root root 6 Jan 31 08:54 common  
drwxr-xr-x. 2 root developers 6 Jan 31 08:52 developers  
drwxr-xr-x. 2 root hr 6 Jan 31 08:52 hr  
drwxr-xr-x. 2 root it 6 Jan 31 08:52 it  
drwxr-xr-x. 2 root management 6 Jan 31 08:52 management  
drwxr-xr-x. 2 root testers 6 Jan 31 08:52 testers  
myadmin@techrich-server:~$
```

change the permission of each group directory to ensure that each file created in the directory inherit the group ownership and only the group

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo chmod 2770 /shared/developers  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo chmod 2770 /shared/testers  
myadmin@techrich-server:~$ sudo chmod 2770 /shared/hr  
myadmin@techrich-server:~$ sudo chmod 2770 /shared/it  
myadmin@techrich-server:~$ sudo chmod 2770 /shared/management  
myadmin@techrich-server:~$ ls -la /shared/  
total 0  
drwxr-xr-x.  8 root root    91 Jan 31 08:54 .  
dr-xr-xr-x. 19 root root   249 Jan 31 08:51 ..  
drwxr-xr-x.  2 root root    6 Jan 31 08:54 common  
drwxrws---.  2 root developers 6 Jan 31 08:52 developers  
drwxrws---.  2 root hr         6 Jan 31 08:52 hr  
drwxrws---.  2 root it         6 Jan 31 08:52 it  
drwxrws---.  2 root management 6 Jan 31 08:52 management  
drwxrws---.  2 root testers   6 Jan 31 08:52 testers  
myadmin@techrich-server:~$
```

create sample files in each department directory

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo su - dev01 << 'EOF'  
touch /shared/developers/project_alpha.txt  
touch /shared/developers/code_review.md  
touch /shared/developers/sprint_plan.doc  
touch /shared/developers/bug_tracker.xlsx  
touch /shared/developers/meeting_notes.pdf  
echo "Project Alpha - Main Development Branch" > /shared/developers/project_alpha.txt  
EOF  
myadmin@techrich-server:~$ sudo su - test01 << 'EOF'  
touch /shared/testers/test_cases.xlsx  
touch /shared/testers/bug_reports.txt  
touch /shared/testers/qa_checklist.md  
touch /shared/testers/automation_scripts.sh  
touch /shared/testers/test_results.log  
echo "QA Test Cases - Sprint 24" > /shared/testers/test_cases.xlsx  
EOF  
myadmin@techrich-server:~$ sudo su - hr01 << 'EOF'  
touch /shared/hr/employee_handbook.pdf  
touch /shared/hr/leave_requests.xlsx  
touch /shared/hr/performance_reviews.doc  
touch /shared/hr/recruitment_plan.txt  
touch /shared/hr/training_schedule.md  
echo "Employee Handbook 2024" > /shared/hr/employee_handbook.pdf  
EOF  
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo su - it01 << 'EOF'  
touch /shared/it/server_inventory.xlsx  
touch /shared/it/backup_procedures.md  
touch /shared/it/security_policies.pdf  
touch /shared/it/network_diagram.png  
touch /shared/it/incident_log.txt  
echo "IT Infrastructure Documentation" > /shared/it/server_inventory.xlsx  
EOF  
Last login: Sat Jan 31 08:13:32 EST 2026 on pts/0  
myadmin@techrich-server:~$ sudo su - mgmt01 << 'EOF'  
touch /shared/management/quarterly_report.pdf  
touch /shared/management/budget_2024.xlsx  
touch /shared/management/strategic_plan.doc  
touch /shared/management/board_minutes.txt  
touch /shared/management/company_policies.md  
echo "Q1 2024 Financial Report" > /shared/management/quarterly_report.pdf  
EOF  
myadmin@techrich-server:~$
```

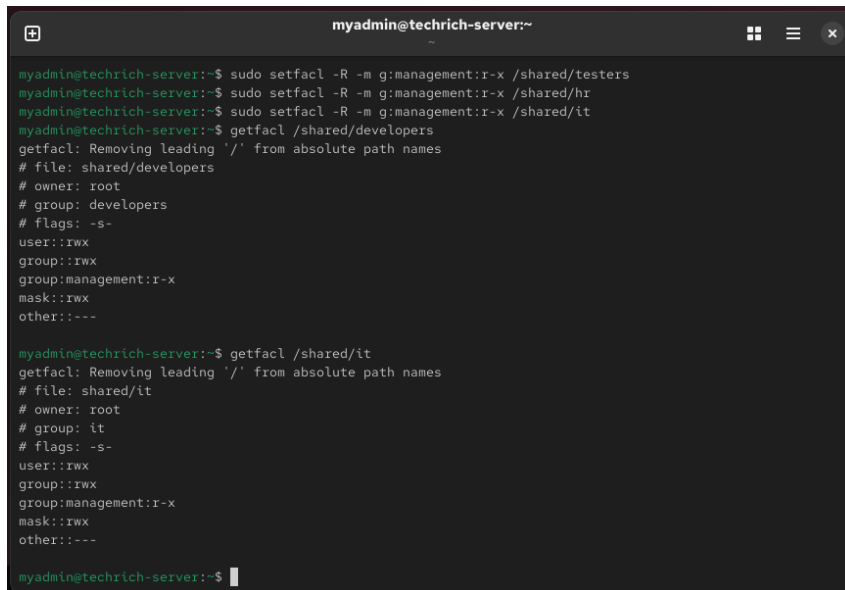
verifying department files, by listing all the files with ownership and permissions

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ # Check all departments  
for dept in developers testers hr it management; do  
  echo "=== $dept ==="  
  sudo ls -lh /shared/$dept/  
  echo ""  
done  
=== developers ===  
total 4.0K  
-rw-r--r--. 1 dev01 developers 0 Jan 31 10:24 bug_tracker.xlsx  
-rw-r--r--. 1 dev01 developers 0 Jan 31 10:24 code_review.md  
-rw-r--r--. 1 dev01 developers 0 Jan 31 10:24 meeting_notes.pdf  
-rw-r--r--. 1 dev01 developers 40 Jan 31 10:24 project_alpha.txt  
-rw-r--r--. 1 dev01 developers 0 Jan 31 10:24 sprint_plan.doc  
  
=== testers ===  
total 4.0K  
-rw-r--r--. 1 test01 testers 0 Jan 31 10:26 automation_scripts.sh  
-rw-r--r--. 1 test01 testers 0 Jan 31 10:26 bug_reports.txt  
-rw-r--r--. 1 test01 testers 0 Jan 31 10:26 qa_checklist.md  
-rw-r--r--. 1 test01 testers 26 Jan 31 10:26 test_cases.xlsx  
-rw-r--r--. 1 test01 testers 0 Jan 31 10:26 test_results.log  
  
=== hr ===  
total 4.0K  
-rw-r--r--. 1 hr01 hr 23 Jan 31 10:26 employee_handbook.pdf  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 leave_requests.xlsx  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 performance_reviews.doc  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 recruitment_plan.txt
```

```
myadmin@techrich-server:~  
-rw-r--r--. 1 test01 testers 0 Jan 31 10:26 test_results.log  
  
=== hr ===  
total 4.0K  
-rw-r--r--. 1 hr01 hr 23 Jan 31 10:26 employee_handbook.pdf  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 leave_requests.xlsx  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 performance_reviews.doc  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 recruitment_plan.txt  
-rw-r--r--. 1 hr01 hr 0 Jan 31 10:26 training_schedule.md  
  
=== it ===  
total 4.0K  
-rw-r--r--. 1 it01 it 0 Jan 31 10:27 backup_procedures.md  
-rw-r--r--. 1 it01 it 0 Jan 31 10:27 incident_log.txt  
-rw-r--r--. 1 it01 it 0 Jan 31 10:27 network_diagram.png  
-rw-r--r--. 1 it01 it 0 Jan 31 10:27 security_policies.pdf  
-rw-r--r--. 1 it01 it 32 Jan 31 10:27 server_inventory.xlsx  
  
=== management ===  
total 4.0K  
-rw-r--r--. 1 mgmt01 management 0 Jan 31 10:28 board_minutes.txt  
-rw-r--r--. 1 mgmt01 management 0 Jan 31 10:28 budget_2024.xlsx  
-rw-r--r--. 1 mgmt01 management 0 Jan 31 10:28 company_policies.md  
-rw-r--r--. 1 mgmt01 management 25 Jan 31 10:28 quarterly_report.pdf  
-rw-r--r--. 1 mgmt01 management 0 Jan 31 10:28 strategic_plan.doc  
  
myadmin@techrich-server:~$
```

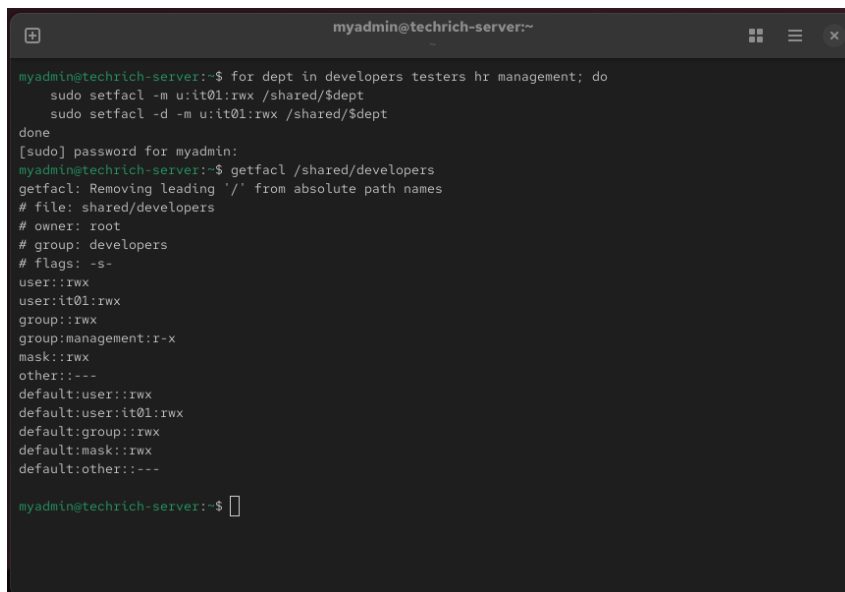
ACL Implementation

applying read and execute ACLs for the management group on all the directories and verify it with getfacl, to ensure smooth flow of the business process and the managerial tasks.



```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo setfacl -R -m g:management:r-x /shared/testers  
myadmin@techrich-server:~$ sudo setfacl -R -m g:management:r-x /shared/hr  
myadmin@techrich-server:~$ sudo setfacl -R -m g:management:r-x /shared/it  
myadmin@techrich-server:~$ getfacl /shared/developers  
getfacl: Removing leading '/' from absolute path names  
# file: shared/developers  
# owner: root  
# group: developers  
# flags: -s-  
user::rwx  
group::rwx  
group:management:r-x  
mask::rwx  
other:---  
  
myadmin@techrich-server:~$ getfacl /shared/it  
getfacl: Removing leading '/' from absolute path names  
# file: shared/it  
# owner: root  
# group: it  
# flags: -s-  
user::rwx  
group::rwx  
group:management:r-x  
mask::rwx  
other:---  
  
myadmin@techrich-server:~$
```

Set read and write ACLs for IT admins for all the directories



```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ for dept in developers testers hr management; do  
    sudo setfacl -m u:it01:rwx /shared/$dept  
    sudo setfacl -d -m u:it01:rwx /shared/$dept  
done  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ getfacl /shared/developers  
getfacl: Removing leading '/' from absolute path names  
# file: shared/developers  
# owner: root  
# group: developers  
# flags: -s-  
user::rwx  
user:it01:rwx  
group::rwx  
group:management:r-x  
mask::rwx  
other:---  
default:user::rwx  
default:user:it01:rwx  
default:group::rwx  
default:mask::rwx  
default:other:---  
  
myadmin@techrich-server:~$
```

Security Explanation

Linux permissions control what actions (read, write, execute) a user can perform on files and folders (Stallings, 2022). Group ownership allows access to be assigned by role. ACLs add extra access rules for specific users when the basic permissions and groups aren't enough (SUSE, 2023). Together, they enforce least privilege, meaning each user only gets access to what they need for their role. This limits damage if an account is compromised, keeps departments separate, and makes access easy to manage as the organisation grows (Stallings, 2022).

Task C

Start and enable SSH service

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo systemctl start sshd  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo systemctl enable sshd  
myadmin@techrich-server:~$ sudo systemctl status sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)  
   Active: active (running) since Fri 2026-01-30 10:36:21 EST; 1 day 2h ago  
  Invocation: a6beb18a0fa34914bf2f07c82f38b58d  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Main PID: 1200 (sshd)  
    Tasks: 1 (limit: 10341)  
  Memory: 100K (peak: 2.5M, swap: 1.1M, swap peak: 1.1M)  
     CPU: 34ms  
  CGroup: /system.slice/sshd.service  
          └─1200 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Jan 30 10:36:20 techrich-server.local systemd[1]: Starting sshd.service - OpenSSH server daemon...  
Jan 30 10:36:21 techrich-server.local sshd[1200]: Server listening on 0.0.0.0 port 22.  
Jan 30 10:36:21 techrich-server.local systemd[1]: Started sshd.service - OpenSSH server daemon.  
Jan 30 10:36:21 techrich-server.local sshd[1200]: Server listening on :: port 22.  
myadmin@techrich-server:~$ sudo ss -tlnp | grep :22  
[sudo] password for myadmin:  
Sorry, try again.  
[sudo] password for myadmin:  
LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users:(("sshd",pid=1200,fd=7))  
LISTEN 0      128          [::]:22        [::]:*         users:(("sshd",pid=1200,fd=8))  
myadmin@techrich-server:~$
```

Configure SSH firewall

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo firewall-cmd --state  
[sudo] password for myadmin:  
running  
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=ssh  
Warning: ALREADY_ENABLED: ssh  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --reload  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --list-services  
cockpit dhcpv6-client ssh  
myadmin@techrich-server:~$
```

Backing up the original sshd configuration before editing

```
myadmin@techrich-server:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
[sudo] password for myadmin:
myadmin@techrich-server:~$ sudo nano /etc/ssh/sshd_config
myadmin@techrich-server:~$
```

Editing sshd configuration and confirming security hardening (disable root login, enable key authentication, ... etc).

```
myadmin@techrich-server:~ - sudo nano /etc/ssh/sshd_config
GNU nano 8.1 /etc/ssh/sshd_config Modified
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
# X11Forwarding no
# AllowTcpForwarding no
# PermitTTY no
# ForceCommand cvs serve
# Change or add these settings:
PermitRootLogin no # Disable root login
PasswordAuthentication yes # Keep enabled for now, will disable later
PubkeyAuthentication yes # Enable key-based authentication
Port 22 # Default port (can change for security)
Protocol 2 # Use SSH protocol 2 only
MaxAuthTries 3 # Limit authentication attempts
LoginGraceTime 60 # Timeout for login
ClientAliveInterval 300 # Keep-alive messages every 5 minutes
ClientAliveCountMax 2 # Disconnect after 2 missed keep-alives

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^G Location M-U Undo
^X Exit ^R Read File ^N Replace ^V Paste ^J Justify ^Y Go To Line M-E Redo
```

Restart SSH and confirming it's enabled

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo nano /etc/ssh/sshd_config  
myadmin@techrich-server:~$ sudo sshd -t  
[sudo] password for myadmin:  
MaabSorry, try again.  
[sudo] password for myadmin:  
myadmin@techrich-server:~$ sudo systemctl restart sshd  
myadmin@techrich-server:~$ sudo systemctl status sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2026-01-31 13:36:57 EST; 14s ago  
  Invocation: 22c5bd9680c04939869143447e3e3ed8  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
    Main PID: 25457 (sshd)  
      Tasks: 1 (limit: 10341)  
     Memory: 4M (peak: 4.1M)  
        CPU: 44ms  
    CGroup: /system.slice/ssh.service  
           └─25457 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Jan 31 13:36:57 techrich-server.local systemd[1]: Starting sshd.service - OpenSSH server daemon...  
Jan 31 13:36:57 techrich-server.local sshd[25457]: Server listening on 0.0.0.0 port 22.  
Jan 31 13:36:57 techrich-server.local sshd[25457]: Server listening on :: port 22.  
Jan 31 13:36:57 techrich-server.local systemd[1]: Started sshd.service - OpenSSH server daemon.  
myadmin@techrich-server:~$
```

Create SSH key pair for admin it01

```
it01@techrich-server:~$ sudo su - it01  
myadmin@techrich-server:~$  
myadmin@techrich-server:~$ sudo su - it01  
Last login: Sat Jan 31 10:27:48 EST 2026  
it01@techrich-server:~$ ssh-keygen -t rsa -b 4096 -C "it01@techrich-server"  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/it01/.ssh/id_rsa):  
Created directory '/home/it01/.ssh'.  
Enter passphrase for '/home/it01/.ssh/id_rsa' (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/it01/.ssh/id_rsa  
Your public key has been saved in /home/it01/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:CE4MHdIeWy8dy+Vniu5mSLcuQ/9YBG4l66/kCwZjd8M it01@techrich-server  
The key's randomart image is:  
+---[RSA 4096]-----+  
| oo.. |  
| ++ . . . |  
| .+ +o= |  
| oo..+== o |  
| = o.E..+ |  
| . +o+oo |  
| oo=oo.. |  
| .+*+ |  
| BB+o |  
+---[SHA256]-----+  
it01@techrich-server:~$ ls -la ~/.ssh/  
total 8  
drwxr-xr-x 2 it01 it01 20 Jan 31 12:42 .
```

```
it01@techrich-server:~ - sudo su - it01

The key's randomart image is:
+---[RSA 4096]-----+
| oo.. |
| ++. . . |
| .+ +o= |
| oo..+=. o |
| = o.E..+ |
| . +o+oo. |
| oo=0.. |
| .+*+ |
| BB+o |
+---[SHA256]-----+
it01@techrich-server:~$ ls -la ~/.ssh/
total 8
drwx----- 2 it01 it01 38 Jan 31 13:42 .
drwx----- 5 it01 it01 104 Jan 31 13:42 ..
-rw----- 1 it01 it01 3389 Jan 31 13:42 id_rsa
-rw-r--r-- 1 it01 it01 746 Jan 31 13:42 id_rsa.pub
it01@techrich-server:~$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACb0NzI9kJCTJKmiju6gjmTqGJ4it3eWcgWDzop/MEIVErT3DCuuDpz01Dz+LJEofD6
3ykSSTZaM1LBgGd1uDFshvDyHHstrmTio491XHLClqLzEGVjwmG5FSyzqdRy0ZViDDtgy3XVT/2+YR68ZhSap4GgkP5Pbyk+p74nG22x0
kE1/Gv90CP8Pw0NEP7KGVeKoo0Js2PUgrAUraeQs+D5wmi1uOm7zEVb0izpHIT8kFhmSSuM1JyUEDTWKbaAFftkJ7U/fTHTANUELMgS
xRTYcgk9/EO4xZ4kSav8ezaMph/6WpodYPgscM6r/w8W01HMotsPuVIkEDN5c5Hs5V84VM17es1xVUN1Iyzqg6p2g3nqNVGexMRJp7unH
K+jxp9B4e6FOXSM30n6HKy1Hsn6CZB/SAmJp8JoEtawNixzk461TRMJR31Tc/ETpEwkbDSYX4kkjB97KS0y6xqFmUcyiBq4/dY8dq69
CZFB5G95V0LX4PzTUgDmvVf7cTz+T09qTcnI03zBYH3/8+WkiUW8WCJ70L57dAAjgtkjtirvAC+Y6jZ/9LkWB0W0QfbNbrwZy+X/76tgK
+P7JbcX59IVikzGMhDFKI0mME7dJZaKMaGI1dHvBBp/9pYx+rbd175DibiaInNqELh385DLk1Trd/t3I5G409160H3i0== it01@techr
ich-server
it01@techrich-server:~$
```

Copy it01 public key and setting the permissions

```
myadmin@techrich-server:~

it01@techrich-server:~$ mkdir -p ~/.ssh
it01@techrich-server:~$ chmod 700 ~/.ssh
it01@techrich-server:~$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
it01@techrich-server:~$ chmod 600 ~/.ssh/authorized_keys
it01@techrich-server:~$ exit
logout
myadmin@techrich-server:~$
```

Create SSH key pair for it02 admin

```
myadmin@techrich-server:~  
logout  
myadmin@techrich-server:~$ sudo bash << 'EOF'  
for user in it01 it02; do  
  echo "Generating SSH keys for $user..."  
  su - $user -c "ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa -N '' -C '$user@techrich-server'"  
  su - $user -c "cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys"  
  su - $user -c "chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys"  
done  
EOF  
[sudo] password for myadmin:  
Sorry, try again.  
[sudo] password for myadmin:  
Generating SSH keys for it01...  
Generating public/private rsa key pair.  
/home/it01/.ssh/id_rsa already exists.  
Overwrite (y/n)? Generating SSH keys for it02...  
Generating public/private rsa key pair.  
Created directory '/home/it02/.ssh'.  
Your identification has been saved in /home/it02/.ssh/id_rsa  
Your public key has been saved in /home/it02/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:9hXlnbtLykPvuopQ0U+vgXYkdi2yeb1HhuAxLfctU04 it02@techrich-server  
The key's randomart image is:  
+--[RSA 4096]----+  
|  
| . o o |  
| . = @ * . |  
| o & % B . |  
|-----+-----+  
S B P F
```

Test SSH login as it01 and it02 and ensure that the key based authentication is successful for both

```
it01@techrich-server:~ -- ssh it01@localhost  
myadmin@techrich-server:~$ ssh it01@localhost  
it01@localhost's password:  
Web console: https://techrich-server.local:9090/ or https://192.168.19.129:9090/  
  
Last failed login: Sat Jan 31 14:40:19 EST 2026 from ::1 on ssh:notty  
There were 4 failed login attempts since the last successful login.  
Last login: Sat Jan 31 13:50:16 2026  
it01@techrich-server:~$ ls -la ~/.ssh/  
total 12  
drwx----- 2 it01 it01 61 Jan 31 13:46 .  
drwx----- 5 it01 it01 125 Jan 31 13:47 ..  
-rw----- 1 it01 it01 1492 Jan 31 13:50 authorized_keys  
-rw----- 1 it01 it01 3389 Jan 31 13:42 id_rsa  
-rw-r--r-- 1 it01 it01 746 Jan 31 13:42 id_rsa.pub  
it01@techrich-server:~$ ssh it01@localhost  
The authenticity of host 'localhost (::1)' can't be established.  
ED25519 key fingerprint is SHA256:SaouK5xRDPB4LR7rx2go7cS5o88S1XWD5IG5WygqX6o.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.  
ssh_dispatch_run_fatal: Connection to ::1 port 22: Broken pipe  
it01@techrich-server:~$ ssh it01@localhost  
Web console: https://techrich-server.local:9090/ or https://192.168.19.129:9090/  
  
Last login: Sat Jan 31 18:12:35 2026 from ::1  
it01@techrich-server:~$
```

```
it02@techrich-server:~ - ssh it01@localhost
it01@techrich-server:~$ sudo su - it02
Last login: Sat Jan 31 18:21:36 EST 2026 on pts/3
it02@techrich-server:~$ ssh it02@localhost
Web console: https://techrich-server.local:9090/ or https://192.168.19.129:9090/
Last login: Sat Jan 31 18:26:16 2026
it02@techrich-server:~$
```

Install Apache (httpd) and confirming the installation

```
myadmin@techrich-server:~ - ssh it01@localhost
myadmin@techrich-server:~$ sudo dnf install httpd -y
[sudo] password for myadmin:
Rocky Linux 10 - BaseOS                2.9 kB/s | 4.3 kB    00:01
Rocky Linux 10 - AppStream              2.9 kB/s | 4.3 kB    00:01
Rocky Linux 10 - Extras                 2.2 kB/s | 3.1 kB    00:01
Dependencies resolved.
=====
Package                Architecture  Version           Repository        Size
=====
Installing:
httpd                  x86_64        2.4.63-4.el10_1.3  appstream         52 k
Installing dependencies:
apr                    x86_64        1.7.5-2.el10      appstream         128 k
apr-util               x86_64        1.6.3-21.el10     appstream         98 k
apr-util-ldap          x86_64        1.6.3-21.el10     appstream         14 k
httpd-core             x86_64        2.4.63-4.el10_1.3 appstream         1.5 M
httpd-filesystem       noarch        2.4.63-4.el10_1.3 appstream         14 k
httpd-tools            x86_64        2.4.63-4.el10_1.3 appstream         81 k
rocky-logos-httpd     noarch        100.4-7.el10      appstream         24 k
Installing weak dependencies:
apr-util-openssl      x86_64        1.6.3-21.el10     appstream         16 k
mod_http2              x86_64        2.0.29-3.el10     appstream         164 k
mod_lua                x86_64        2.4.63-4.el10_1.3 appstream         59 k
Transaction Summary
=====
```

```
myadmin@techrich-server:~ -- ssh it01@localhost
Preparing      :                               1/11
Installing     : apr-1.7.5-2.el10.x86_64      1/11
Installing     : apr-util-lmdb-1.6.3-21.el10.x86_64 2/11
Installing     : apr-util-openssl-1.6.3-21.el10.x86_64 3/11
Installing     : apr-util-1.6.3-21.el10.x86_64    4/11
Installing     : httpd-tools-2.4.63-4.el10_1.3.x86_64 5/11
Installing     : rocky-logos-httpd-100.4-7.el10.noarch 6/11
Running scriptlet: httpd-filesystem-2.4.63-4.el10_1.3.noarch 7/11
Installing     : httpd-filesystem-2.4.63-4.el10_1.3.noarch 7/11
Installing     : httpd-core-2.4.63-4.el10_1.3.x86_64 8/11
Installing     : mod_http2-2.0.29-3.el10.x86_64   9/11
Installing     : mod_lua-2.4.63-4.el10_1.3.x86_64 10/11
Installing     : httpd-2.4.63-4.el10_1.3.x86_64  11/11
Running scriptlet: httpd-2.4.63-4.el10_1.3.x86_64 11/11

Installed:
apr-1.7.5-2.el10.x86_64          apr-util-1.6.3-21.el10.x86_64
apr-util-lmdb-1.6.3-21.el10.x86_64  apr-util-openssl-1.6.3-21.el10.x86_64
httpd-2.4.63-4.el10_1.3.x86_64    httpd-core-2.4.63-4.el10_1.3.x86_64
httpd-filesystem-2.4.63-4.el10_1.3.noarch  httpd-tools-2.4.63-4.el10_1.3.x86_64
mod_http2-2.0.29-3.el10.x86_64    mod_lua-2.4.63-4.el10_1.3.x86_64
rocky-logos-httpd-100.4-7.el10.noarch

Complete!
myadmin@techrich-server:~$ httpd -v
Server version: Apache/2.4.63 (Rocky Linux)
Server built:   Dec 10 2025 00:00:00
myadmin@techrich-server:~$
```

Configuring HTTP/HTTPS firewalls

```
myadmin@techrich-server:~ -- ssh it01@localhost
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=http
[sudo] password for myadmin:
success
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=https
success
myadmin@techrich-server:~$ sudo firewall-cmd --reload
success
myadmin@techrich-server:~$ sudo firewall-cmd --list-services
cockpit dhcpv6-client http https ssh
myadmin@techrich-server:~$
```

Confirming port 80 is listening and retrieve the default html test page

```
myadmin@techrich-server:~ - ssh it01@localhost
myadmin@techrich-server:~$ sudo ss -tlnp | grep :80
[sudo] password for myadmin:
LISTEN 0      511          *:80          *: * users:(("httpd",pid=30695,fd=4),("httpd",pid=30687,fd=4),("httpd",pid=30684,fd=4),("httpd",pid=30682,fd=4))
myadmin@techrich-server:~$ curl http://localhost
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /*![CDATA[*/

      html {
        height: 100%;
        width: 100%;
      }
      body {
        background: rgb(69,23,32);
        background: -moz-linear-gradient(180deg, rgba(69,23,32,1) 30%, rgba(0,0,0,1) 90%) ;
        background: -webkit-linear-gradient(180deg, rgba(69,23,32,1) 30%, rgba(0,0,0,1) 90%) ;
        background: linear-gradient(180deg, rgba(69,23,32,1) 30%, rgba(0,0,0,1) 90%);
        background-repeat: no-repeat;
        background-attachment: fixed;
        filter: progid:DXImageTransform.Microsoft.gradient(startColorstr="#b43c56",endColorstr="#b43c56",Gradie
```

Verify the server ip address with ip addr show

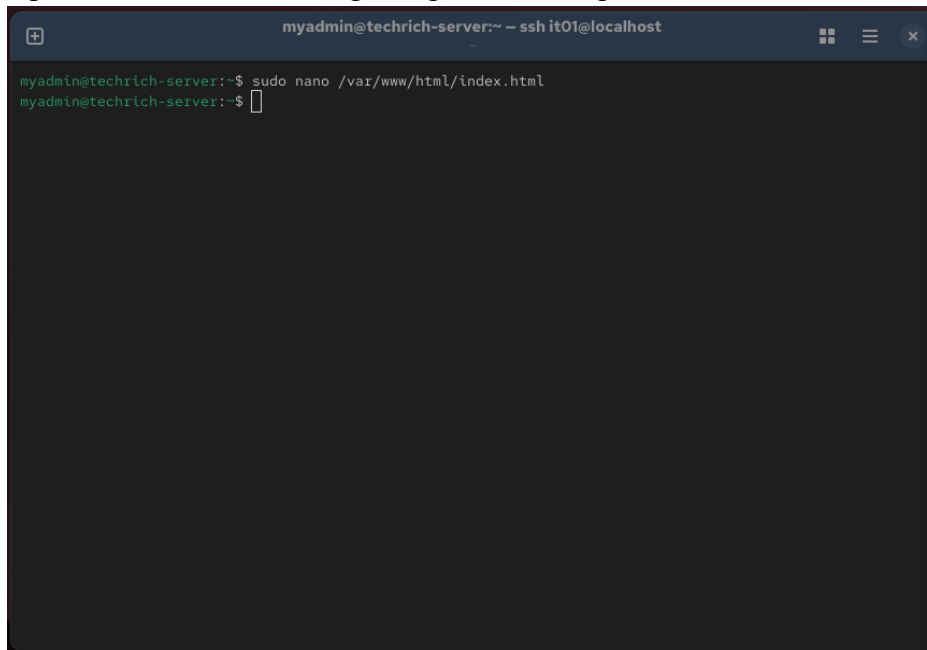
```
myadmin@techrich-server:~ - ssh it01@localhost
<a href="https://nginx.org">Nginx</strong></a>:
You can add your content in a location of your
choice and edit the <code>root</code> configuration directive
in <code>/etc/nginx/nginx.conf</code>.</p>

<div id="logos">
  <a href="https://rockylinux.org/" id="rocky-poweredby"></a> <!-- Rocky -->
   <!-- webserver -->
</div>
</div>
</div>

<footer class="col-sm-12">
  <a href="https://apache.org">Apache</a> is a registered trademark of <a href="https://apache
.org">the Apache Software Foundation</a> in the United States and/or other countries.<br />
  <a href="https://nginx.org">NGINX</a> is a registered trademark of <a href="https://">F5 Net
works, Inc.</a>.
</footer>

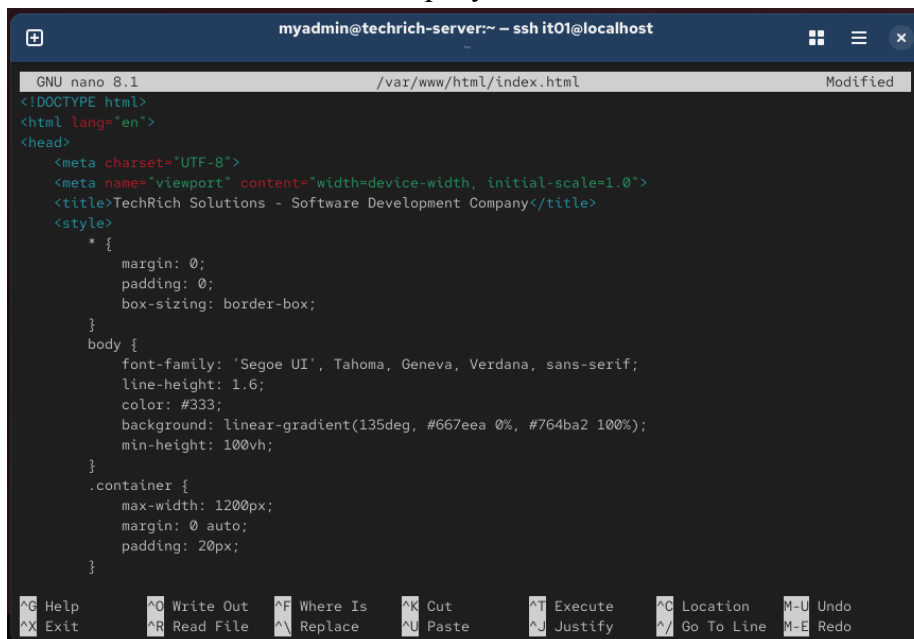
</body>
</html>
myadmin@techrich-server:~$ ip addr show | grep inet
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host noprefixroute
inet 192.168.19.129/24 brd 192.168.19.255 scope global noprefixroute ens160
inet6 fe80::20c:29ff:fe08:fe00/64 scope link noprefixroute
myadmin@techrich-server:~$
```

Open index.html for editing using nano and replace the default file



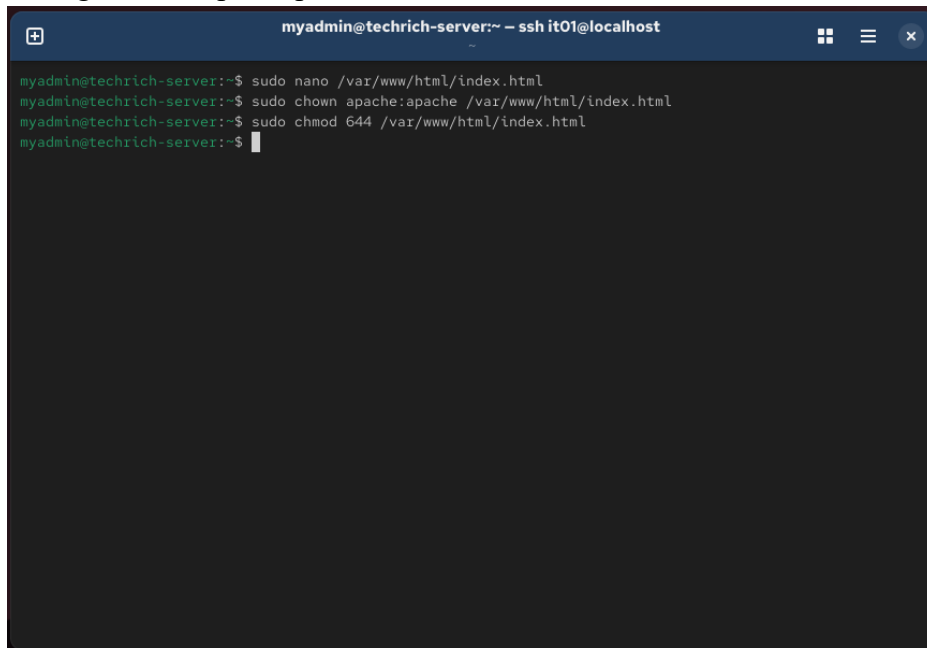
```
myadmin@techrich-server:~ - ssh it01@localhost
myadmin@techrich-server:~$ sudo nano /var/www/html/index.html
myadmin@techrich-server:~$
```

Edit on the file to create the company website



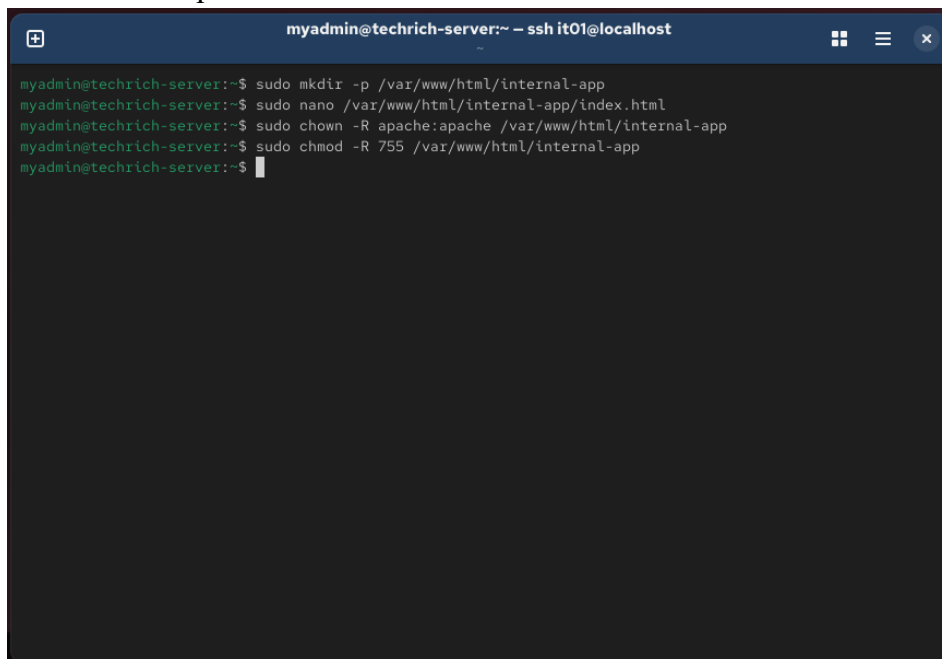
```
GNU nano 8.1 /var/www/html/index.html Modified
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>TechRich Solutions - Software Development Company</title>
  <style>
    * {
      margin: 0;
      padding: 0;
      box-sizing: border-box;
    }
    body {
      font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
      line-height: 1.6;
      color: #333;
      background: linear-gradient(135deg, #667eea 0%, #764ba2 100%);
      min-height: 100vh;
    }
    .container {
      max-width: 1200px;
      margin: 0 auto;
      padding: 20px;
    }
  }
}
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

setting ownership and permissions



```
myadmin@techrich-server:~ - ssh it01@localhost
myadmin@techrich-server:~$ sudo nano /var/www/html/index.html
myadmin@techrich-server:~$ sudo chown apache:apache /var/www/html/index.html
myadmin@techrich-server:~$ sudo chmod 644 /var/www/html/index.html
myadmin@techrich-server:~$
```

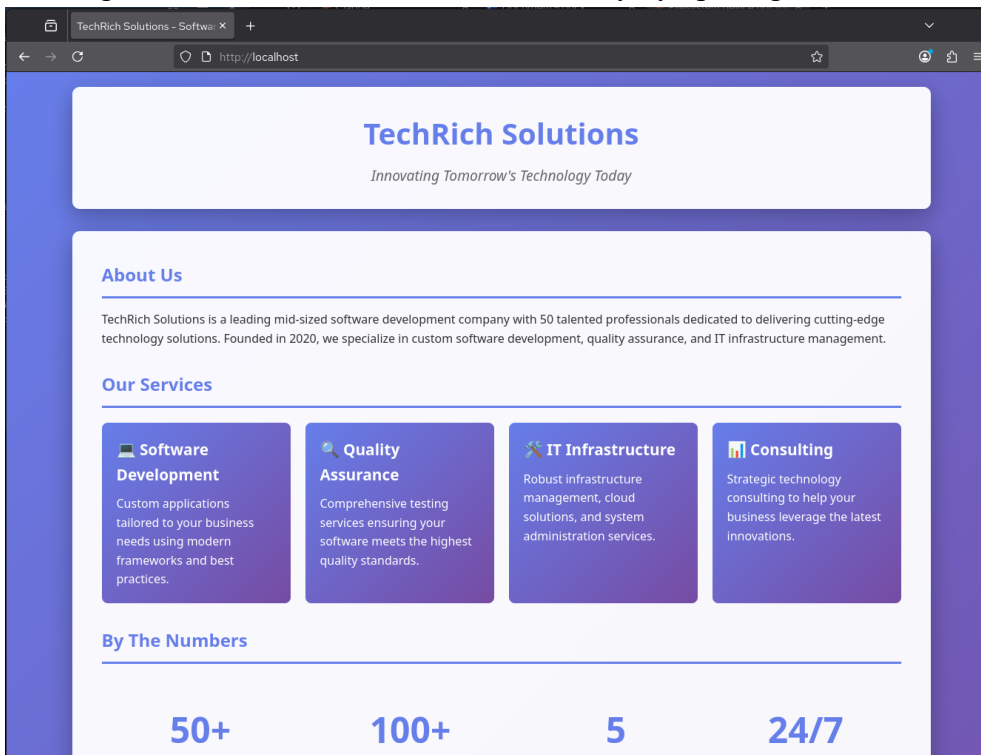
create internal portal website

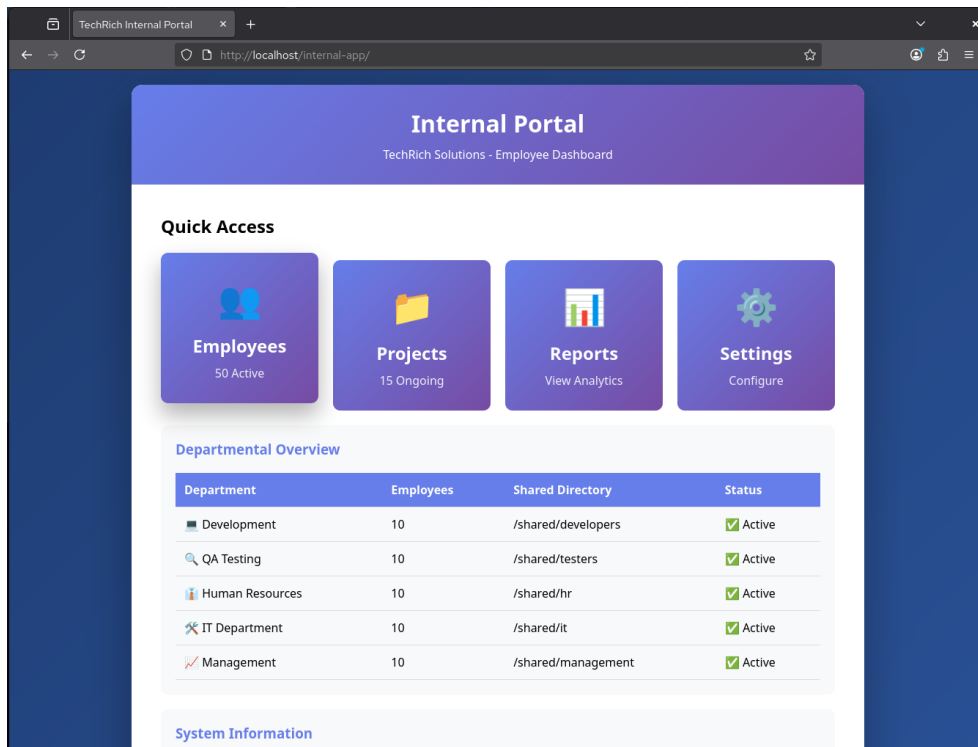


```
myadmin@techrich-server:~ - ssh it01@localhost
myadmin@techrich-server:~$ sudo mkdir -p /var/www/html/internal-app
myadmin@techrich-server:~$ sudo nano /var/www/html/internal-app/index.html
myadmin@techrich-server:~$ sudo chown -R apache:apache /var/www/html/internal-app
myadmin@techrich-server:~$ sudo chmod -R 755 /var/www/html/internal-app
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~ -- ssh it01@localhost
GNU nano 8.1 /var/www/html/internal-app/index.html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>TechRich Internal Portal</title>
  <style>
    * {
      margin: 0;
      padding: 0;
      box-sizing: border-box;
    }
    body {
      font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
      background: linear-gradient(135deg, #1e3c72 0%, #2a5298 100%);
      min-height: 100vh;
      display: flex;
      justify-content: center;
      align-items: center;
      padding: 20px;
    }
    .container {
      background: white;
      border-radius: 15px;
    }
  </style>
</head>
<body>
  <div class="container">
    <div class="header">
      <h1>TechRich Solutions</h1>
      <p>Innovating Tomorrow's Technology Today</p>
    </div>
    <div class="content">
      <h2>About Us</h2>
      <p>TechRich Solutions is a leading mid-sized software development company with 50 talented professionals dedicated to delivering cutting-edge technology solutions. Founded in 2020, we specialize in custom software development, quality assurance, and IT infrastructure management.</p>
      <h2>Our Services</h2>
      <div class="services">
        <div class="service">
          <h3>Software Development</h3>
          <p>Custom applications tailored to your business needs using modern frameworks and best practices.</p>
        </div>
        <div class="service">
          <h3>Quality Assurance</h3>
          <p>Comprehensive testing services ensuring your software meets the highest quality standards.</p>
        </div>
        <div class="service">
          <h3>IT Infrastructure</h3>
          <p>Robust infrastructure management, cloud solutions, and system administration services.</p>
        </div>
        <div class="service">
          <h3>Consulting</h3>
          <p>Strategic technology consulting to help your business leverage the latest innovations.</p>
        </div>
      </div>
      <h2>By The Numbers</h2>
      <div class="stats">
        <div class="stat">50+</div>
        <div class="stat">100+</div>
        <div class="stat">5</div>
        <div class="stat">24/7</div>
      </div>
    </div>
  </div>
</body>
</html>
```

ensuring both websites were created successfully by opening both in the browser





NFS

Installing NFS service and starting and enabling it

```
myadmin@techrich-server:~ - ssh it01@localhost

myadmin@techrich-server:~$
myadmin@techrich-server:~$ sudo dnf install nfs-utils -y
Last metadata expiration check: 0:29:48 ago on Sat 31 Jan 2026 10:10:11 PM EST.
Dependencies resolved.
=====
Package                Architecture    Version          Repository      Size
=====
Installing:
nfs-utils              x86_64         1:2.8.3-0.el10  baseos         475 k
Installing dependencies:
gssproxy               x86_64         0.9.2-10.el10  baseos         111 k
libev                  x86_64         4.33-14.el10   baseos         52 k
libnfsidmap            x86_64         1:2.8.3-0.el10  baseos         61 k
libverto-libev        x86_64         0.3.2-10.el10  baseos         13 k
rpcbind                x86_64         1.2.7-3.el10   baseos         57 k
sssd-nfs-idmap        x86_64         2.11.1-2.el10_1.1 baseos         36 k

Transaction Summary
=====
Install 7 Packages

Total download size: 805 k
Installed size: 2.0 M
Downloading Packages:
(1/7): libnfsidmap-2.8.3-0.el10.x86_64.rpm 514 kB/s | 61 kB 00:00
(2/7): libev-4.33-14.el10.x86_64.rpm      388 kB/s | 52 kB 00:00
(3/7): gssproxy-0.9.2-10.el10.x86_64.rpm  723 kB/s | 111 kB 00:00
(4/7): libverto-libev-0.3.2-10.el10.x86_64.rpm 360 kB/s | 13 kB 00:00
(5/7): rpcbind-1.2.7-3.el10.x86_64.rpm    1.2 MB/s | 57 kB 00:00
(6/7): sssd-nfs-idmap-2.11.1-2.el10_1.1.x86_64.rpm 1.2 MB/s | 36 kB 00:00
(7/7): nfs-utils-1:2.8.3-0.el10.x86_64.rpm 1.2 MB/s | 475 kB 00:00
```

Baking up the original nfs /etc/exports before editing it

```
myadmin@techrich-server:~$ sudo cp /etc/exports /etc/exports.backup
[sudo] password for myadmin:
myadmin@techrich-server:~$ sudo nano /etc/exports
myadmin@techrich-server:~$
```

Configuring 6 nfs shares for all departments

```
myadmin@techrich-server:~ -- sudo nano /etc/exports
GNU nano 8.1 /etc/exports Modified
# Departmental Shares - Accessible within local network
/shared/developers 192.168.19.0/24(rw,sync,no_root_squash,no_all_squash)
/shared/testers    192.168.19.0/24(rw,sync,no_root_squash,no_all_squash)
/shared/hr         192.168.19.0/24(rw,sync,no_root_squash,no_all_squash)
/shared/it         192.168.19.0/24(rw,sync,no_root_squash,no_all_squash)
/shared/management 192.168.19.0/24(rw,sync,no_root_squash,no_all_squash)
/shared/common     192.168.19.0/24(rw,sync,no_root_squash,no_all_squash)

# Options explained:
# rw           - Read and write access
# sync        - Synchronous writes (more stable, slightly slower)
# no_root_squash - Root on client has root privileges on share
# no_all_squash - Preserve user IDs

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

Exporting nfs shares using exportfs to activate all the 6 shares

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo exportfs -arv  
exporting 192.168.19.0/24:/shared/common  
exporting 192.168.19.0/24:/shared/management  
exporting 192.168.19.0/24:/shared/it  
exporting 192.168.19.0/24:/shared/hr  
exporting 192.168.19.0/24:/shared/testers  
exporting 192.168.19.0/24:/shared/developers  
myadmin@techrich-server:~$ sudo exportfs -v  
/shared/developers  
192.168.19.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all  
_squash)  
/shared/testers  
192.168.19.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all  
_squash)  
/shared/hr  
192.168.19.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all  
_squash)  
/shared/it  
192.168.19.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all  
_squash)  
/shared/management  
192.168.19.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all  
_squash)  
/shared/common 192.168.19.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all  
_squash)  
myadmin@techrich-server:~$ sudo showmount -e localhost  
Export list for localhost:  
/shared/common 192.168.19.0/24  
/shared/management 192.168.19.0/24  
/shared/it 192.168.19.0/24  
/shared/hr 192.168.19.0/24
```

Configuring nfs firewall adding services: nfs, rpc-bind, mountd, reloading and ensuring that the services were allowed

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=nfs  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=rpc-bind  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=rpc-mountd  
Error: INVALID_SERVICE: Zone 'public': 'rpc-mountd' not among existing services  
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-service=mountd  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --reload  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --list-services  
cockpit dhcpv6-client http https mountd nfs rpc-bind ssh  
myadmin@techrich-server:~$
```

Verification

Ensuring that all the services are enabled

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo systemctl is-enabled sshd  
enabled  
myadmin@techrich-server:~$ sudo systemctl is-enabled httpd  
enabled  
myadmin@techrich-server:~$ sudo systemctl is-enabled nfs-server  
enabled  
myadmin@techrich-server:~$ sudo systemctl is-enabled rpcbind  
enabled  
myadmin@techrich-server:~$
```

Ensuring that all the services are running

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ services=("sshd" "httpd" "nfs-server" "rpcbind")  
  
for service in "${services[@]}; do  
    echo "Checking $service..."  
    if sudo systemctl is-active --quiet $service; then  
        echo "$service is running"  
    else  
        echo "$service is NOT running"  
    fi  
    echo ""  
done  
Checking sshd...  
sshd is running  
  
Checking httpd...  
httpd is running  
  
Checking nfs-server...  
nfs-server is running  
  
Checking rpcbind...  
rpcbind is running  
  
myadmin@techrich-server:~$
```

SSH (Secure Shell)

SSH provides secure remote access to the server, allowing IT administrators to manage the system from anywhere without physically being there (Stallings, 2022). Its main vulnerability is brute force attacks, attackers repeatedly guess passwords to break in (Singh et al., 2024). This was mitigated by disabling root login, limiting login attempts to three, and switching to key-based authentication (Stallings, 2022). For performance, SSH is lightweight and adds

minimal load to the server, so it requires little optimization beyond keeping the software updated.

Apache (Web Server)

Apache hosts the company website and the internal employee portal, making information accessible to customers and staff. It is vulnerable to attacks like DDoS (flooding the server with traffic) and directory traversal — accessing files you shouldn't (OWASP Foundation, 2023). To reduce risk, the server version should be hidden, directory listing should be turned off, and HTTPS should be enabled (Apache Software Foundation, 2024). For performance, enabling compression and browser caching reduces page load times and server load, which becomes important as more users access the site simultaneously (Apache Software Foundation, 2024).

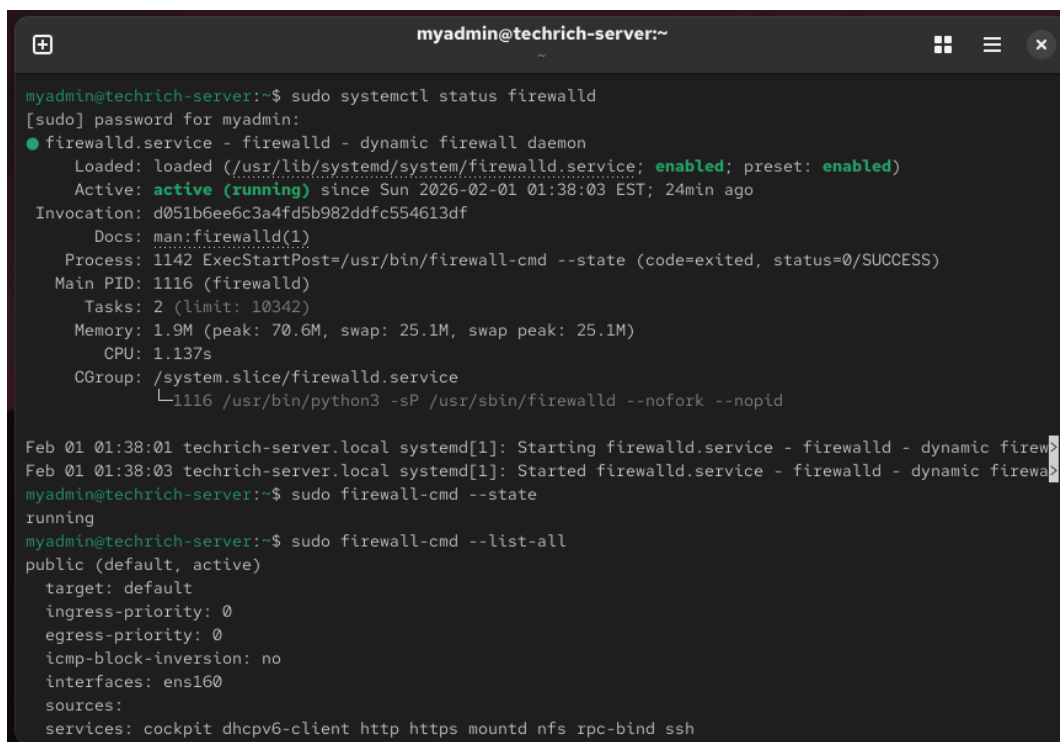
NFS (Network File System)

NFS allows employees to access shared departmental folders from their workstations instead of copying files back and forth. Its biggest vulnerability is that it does not encrypt data by default, meaning files could be intercepted if someone monitors the network traffic. Access is currently restricted to the local network only, but upgrading to NFSv4 with Kerberos encryption would significantly improve security. For performance, NFS works well on a fast local network but slows down over longer distances. Using synchronous writes keeps data safe but is slightly slower; switching to asynchronous writes for non-critical folders could improve speed (Pratt, 2019).

Task D

Firewall

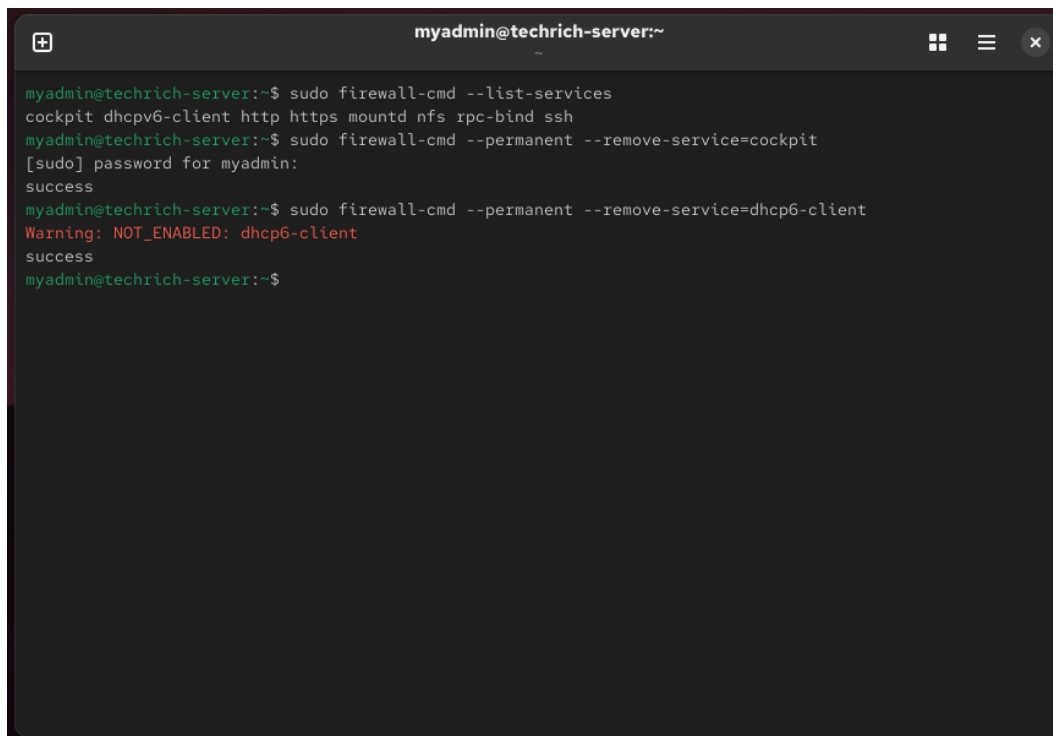
Ensure firewalld is enableed and running



```
myadmin@techrich-server:~$ sudo systemctl status firewalld
[sudo] password for myadmin:
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: active (running) since Sun 2026-02-01 01:38:03 EST; 24min ago
     Invocation: d051b6ee6c3a4fd5b982ddfc554613df
       Docs: man:firewalld(1)
    Process: 1142 ExecStartPost=/usr/bin/firewall-cmd --state (code=exited, status=0/SUCCESS)
   Main PID: 1116 (firewalld)
      Tasks: 2 (limit: 10342)
     Memory: 1.9M (peak: 70.6M, swap: 25.1M, swap peak: 25.1M)
        CPU: 1.137s
    CGroup: /system.slice/firewalld.service
            └─1116 /usr/bin/python3 -sP /usr/sbin/firewalld --nofork --nopid

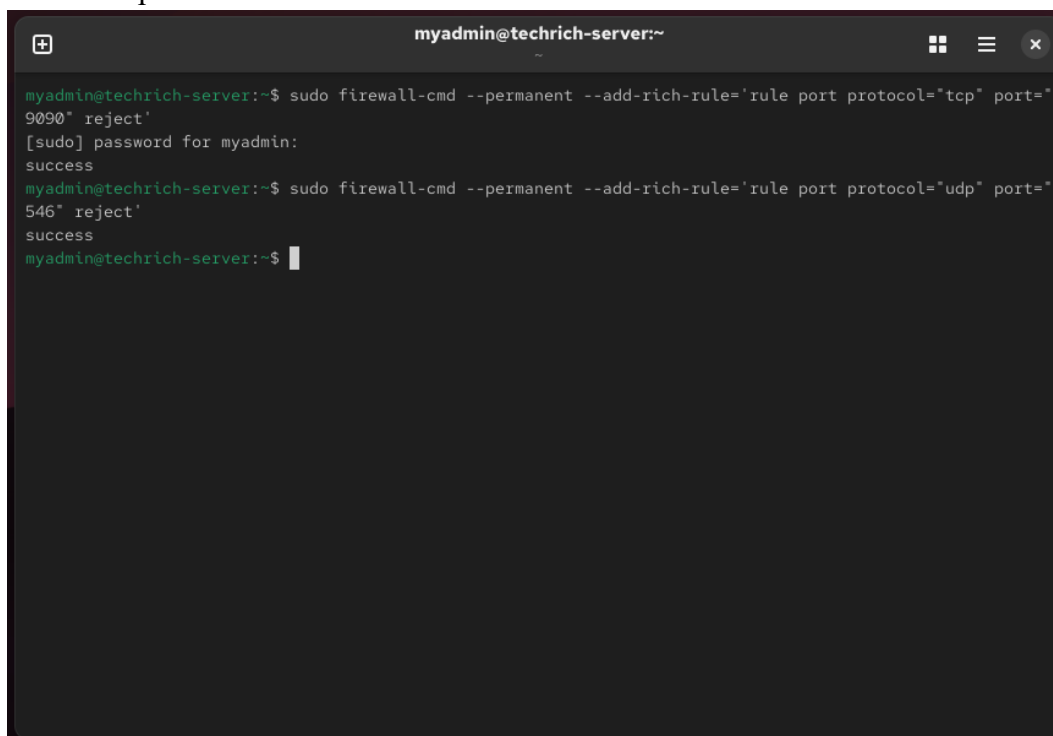
Feb 01 01:38:01 techrich-server.local systemd[1]: Starting firewalld.service - firewalld - dynamic firewa
Feb 01 01:38:03 techrich-server.local systemd[1]: Started firewalld.service - firewalld - dynamic firewa
myadmin@techrich-server:~$ sudo firewall-cmd --state
running
myadmin@techrich-server:~$ sudo firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client http https mountd nfs rpc-bind ssh
```

List the currently allowed services and block the non-essential services (cockpit, dhcpv6-client)

A terminal window titled 'myadmin@techrich-server:~' with standard window controls. The terminal shows the following commands and output:

```
myadmin@techrich-server:~$ sudo firewall-cmd --list-services
cockpit dhcpv6-client http https mountd nfs rpc-bind ssh
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --remove-service=cockpit
[sudo] password for myadmin:
success
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --remove-service=dhcpv6-client
Warning: NOT_ENABLED: dhcpv6-client
success
myadmin@techrich-server:~$
```

Block the ports of the non-essential services

A terminal window titled 'myadmin@techrich-server:~' with standard window controls. The terminal shows the following commands and output:

```
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-rich-rule='rule port protocol="tcp" port="
9090" reject'
[sudo] password for myadmin:
success
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-rich-rule='rule port protocol="udp" port="
546" reject'
success
myadmin@techrich-server:~$
```

Limit ssh connection to 3 attempts per minute per ip

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo firewall-cmd --permanent --add-rich-rule='rule service name="ssh" audit limit value="3/m" accept'  
[sudo] password for myadmin:  
success  
myadmin@techrich-server:~$ sudo firewall-cmd --reload  
success  
myadmin@techrich-server:~$
```

Final verification : verify allowed services, allowed ports and rich rules

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo firewall-cmd --list-all  
public (default, active)  
  target: default  
  ingress-priority: 0  
  egress-priority: 0  
  icmp-block-inversion: no  
  interfaces: ens160  
  sources:  
  services: dhcpv6-client http https mountd nfs rpc-bind ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
    rule service name="ssh" audit limit value="3/m" accept  
    rule port port="546" protocol="udp" reject  
    rule port port="9090" protocol="tcp" reject  
myadmin@techrich-server:~$
```

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ echo "=== Allowed Services ==="  
sudo firewall-cmd --list-services  
=== Allowed Services ===  
dhcpv6-client http https mountd nfs rpc-bind ssh  
myadmin@techrich-server:~$ echo "=== Rich Rules ==="  
sudo firewall-cmd --list-rich-rules  
=== Rich Rules ===  
rule service name="ssh" audit limit value="3/m" accept  
rule port port="546" protocol="udp" reject  
rule port port="9090" protocol="tcp" reject  
myadmin@techrich-server:~$
```

SSH Hardening

Edit sshd config file and test and restart sshd

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo nano /etc/ssh/sshd_config  
myadmin@techrich-server:~$ sudo sshd -t  
myadmin@techrich-server:~$ sudo systemctl restart sshd  
myadmin@techrich-server:~$ sudo systemctl status sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)  
   Active: active (running) since Sun 2026-02-01 03:13:29 EST; 21s ago  
     Invocation: 49e09d5afaaa4e09a69b386e197a735d  
       Docs: man:sshd(8)  
             man:sshd_config(5)  
    Main PID: 7830 (sshd)  
      Tasks: 1 (limit: 10342)  
     Memory: 1.3M (peak: 1.6M)  
        CPU: 33ms  
    CGroup: /system.slice/sshd.service  
            └─7830 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Feb 01 03:13:28 techrich-server.local systemd[1]: Starting sshd.service - OpenSSH server daemon...  
Feb 01 03:13:29 techrich-server.local sshd[7830]: Server listening on 0.0.0.0 port 22.  
Feb 01 03:13:29 techrich-server.local sshd[7830]: Server listening on :: port 22.  
Feb 01 03:13:29 techrich-server.local systemd[1]: Started sshd.service - OpenSSH server daemon.  
myadmin@techrich-server:~$
```

Ensure that sshd hardening is successful (root login is disabled, key-based auth is enabled, it01 and it02 are in the AllowUsers)

```
myadmin@techrich-server:~  
myadmin@techrich-server:~$ sudo grep "^PermitRootLogin" /etc/ssh/sshd_config  
PermitRootLogin no # Disable root login  
myadmin@techrich-server:~$ sudo grep "^PubkeyAuthentication" /etc/ssh/sshd_config  
PubkeyAuthentication yes # Enable key-based authentication  
myadmin@techrich-server:~$ sudo grep "^PasswordAuthentication" /etc/ssh/sshd_config  
PasswordAuthentication no # Disabled  
myadmin@techrich-server:~$ sudo grep "^AllowUsers" /etc/ssh/sshd_config  
AllowUsers it01 it02  
myadmin@techrich-server:~$ ssh root@localhost  
root@localhost's password:  
Permission denied, please try again.  
root@localhost's password:  
Permission denied, please try again.  
root@localhost's password:  
Received disconnect from ::1 port 22:2: Too many authentication failures  
Disconnected from ::1 port 22  
myadmin@techrich-server:~$
```

Ensure that the SSH keys generated earlier for it01 and it02 are working (passwordless connection for it01 and it02, and root login is disabled)

```
myadmin@techrich-server:~ - sudo su - it01  
myadmin@techrich-server:~$ sudo su - it01  
Last login: Sun Feb 1 04:00:29 EST 2026 from ::1 on pts/3  
it01@techrich-server:~$ ssh localhost  
Web console: https://techrich-server.local:9090/ or https://192.168.19.129:9090/  
  
Last login: Sun Feb 1 04:01:22 2026  
it01@techrich-server:~$ exit  
logout  
Connection to localhost closed.  
it01@techrich-server:~$ exit  
logout  
myadmin@techrich-server:~$ sudo su - it02  
Last login: Sun Feb 1 03:33:30 EST 2026 on pts/3  
it02@techrich-server:~$ ssh localhost  
Web console: https://techrich-server.local:9090/ or https://192.168.19.129:9090/  
  
Last login: Sun Feb 1 04:01:53 2026  
it02@techrich-server:~$ exit  
logout  
Connection to localhost closed.  
it02@techrich-server:~$ exit  
logout  
myadmin@techrich-server:~$ ssh root@localhost  
root@localhost: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
myadmin@techrich-server:~$
```

Set password policy by editing the pwquality.conf file

```
myadmin@techrich-server:~ -- sudo su - it01

myadmin@techrich-server:~$ sudo dnf search pwquality
Last metadata expiration check: 2:18:48 ago on Sun 01 Feb 2026 01:59:21 AM EST.
===== Name & Summary Matched: pwquality =====
python3-pwquality.x86_64 : Python bindings for the libpwquality library
===== Name Matched: pwquality =====
libpwquality.x86_64 : A library for password generation and password quality checking
myadmin@techrich-server:~$ sudo dnf install libpwquality -y
Last metadata expiration check: 2:19:13 ago on Sun 01 Feb 2026 01:59:21 AM EST.
Package libpwquality-1.4.5-12.el10.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
myadmin@techrich-server:~$ sudo dnf install libpwquality -y
Last metadata expiration check: 2:19:37 ago on Sun 01 Feb 2026 01:59:21 AM EST.
Package libpwquality-1.4.5-12.el10.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
myadmin@techrich-server:~$ sudo nano /etc/security/pwquality.conf
myadmin@techrich-server:~$
```

```
GNU nano 8.1 /etc/security/pwquality.conf Modified
# Skip testing the password quality for users that are not present in the
# /etc/passwd file.
# Enabled if the option is present.
# local_users_only
# Minimum password length
minlen = 8

# Require at least 1 uppercase letter
dcredit = -1

# Require at least 1 lowercase letter
lcredit = -1

# Require at least 1 number
dcredit = -1

# Require at least 1 special character
ocredit = -1

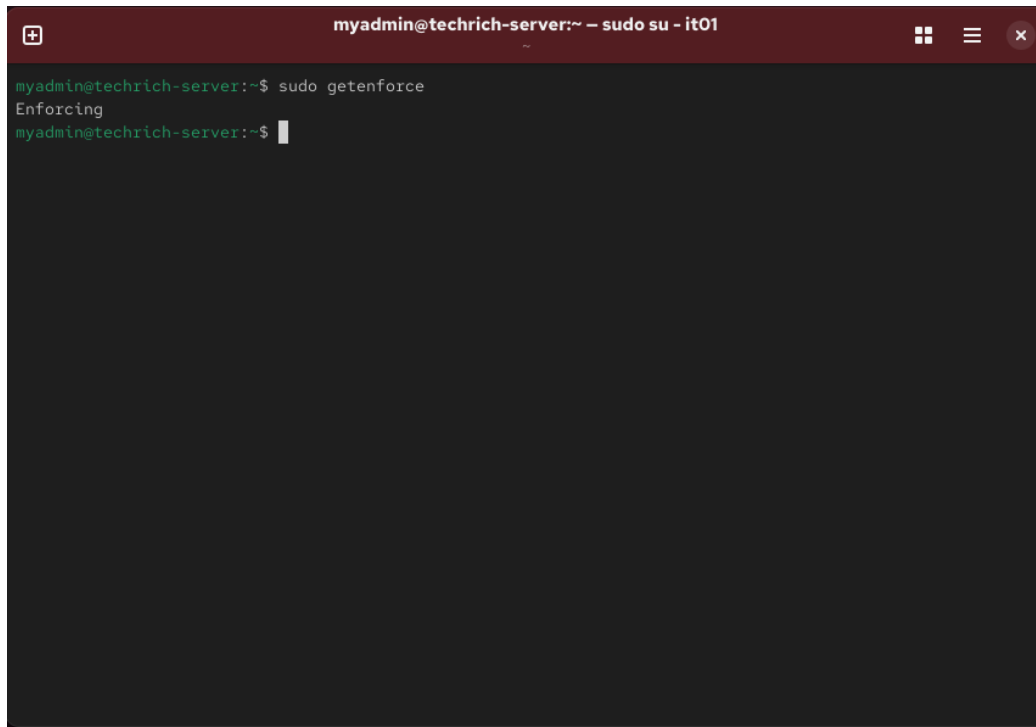
# Minimum number of different character classes
minclass = 3

# Maximum number of repeated characters
maxrepeat = 3

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_/ Go To Line  M-E Redo
```

SSELinux

Ensure that SELinux is enabled

A terminal window with a dark red title bar containing the text 'myadmin@techrich-server:~ - sudo su - it01'. The terminal content shows the command 'sudo getenforce' being executed, resulting in the output 'Enforcing'. The prompt 'myadmin@techrich-server:~\$' is visible at the end of the line.

```
myadmin@techrich-server:~$ sudo getenforce
Enforcing
myadmin@techrich-server:~$
```

Explain the importance of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) in enterprise computing environments.

Firewalls filter network traffic to block unauthorized access while allowing legitimate traffic through based on predefined rules. IDS monitors network activity for suspicious behaviour and alerts administrators, functioning like a security camera that observes but does not act (Stallings, 2022). IPS goes further by automatically blocking detected threats in real time, acting as a security guard that stops threats before damage occurs (Cole, 2011). Together, these three technologies create a layered defence: firewalls prevent unauthorized entry, IDS detects threats that penetrate defences, and IPS stops those threats, protecting the organisation at multiple levels (Stallings, 2022).

Task E

System monitoring

Install monitoring tools (htop, iotop, net-tools), and verify successful installation

```
myadmin@techrich-server:~ - sudo su - it01
Complete!
myadmin@techrich-server:~$
myadmin@techrich-server:~$ sudo dnf install htop -y
Extra Packages for Enterprise Linux 10 - x86_64 3.7 MB/s | 5.6 MB 00:01
Last metadata expiration check: 0:00:01 ago on Sun 01 Feb 2026 04:45:52 AM EST.
Dependencies resolved.
=====
Package Architecture Version Repository Size
=====
Installing:
htop x86_64 3.3.0-5.el10_0 epel 196 k
Installing dependencies:
hwloc-libs x86_64 2.11.1-3.el10 baseos 2.1 M
ocl-icd x86_64 2.3.2-8.el10 baseos 66 k
Transaction Summary
=====
Install 3 Packages

Total download size: 2.3 M
Installed size: 3.5 M
Downloading Packages:
(1/3): ocl-icd-2.3.2-8.el10.x86_64.rpm 244 kB/s | 66 kB 00:00
(2/3): htop-3.3.0-5.el10_0.x86_64.rpm 704 kB/s | 196 kB 00:00
(3/3): hwloc-libs-2.11.1-3.el10.x86_64.rpm 2.3 MB/s | 2.1 MB 00:00
-----
Total 549 kB/s | 2.3 MB 00:04
Extra Packages for Enterprise Linux 10 - x86_64 1.6 MB/s | 1.6 kB 00:00
-----
```

```
myadmin@techrich-server:~ -- sudo su - it01
Complete!
myadmin@techrich-server:~$ sudo dnf install iotop -y
[sudo] password for myadmin:
Last metadata expiration check: 0:07:19 ago on Sun 01 Feb 2026 04:45:52 AM EST.
Dependencies resolved.
=====
Package                Architecture    Version         Repository      Size
=====
Installing:
iotop-c                 x86_64         1.26-4.el10    baseos          68 k
=====
Transaction Summary
=====
Install 1 Package

Total download size: 68 k
Installed size: 139 k
Downloading Packages:
iotop-c-1.26-4.el10.x86_64.rpm                443 kB/s | 68 kB    00:00
-----
Total                                          48 kB/s | 68 kB    00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : iotop-c-1.26-4.el10.x86_64    1/1
=====
```

```
myadmin@techrich-server:~ -- sudo su - it01
iotop-c-1.26-4.el10.x86_64.rpm                443 kB/s | 68 kB    00:00
-----
Total                                          48 kB/s | 68 kB    00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : iotop-c-1.26-4.el10.x86_64    1/1
  Running scriptlet: iotop-c-1.26-4.el10.x86_64  1/1
=====
Installed:
  iotop-c-1.26-4.el10.x86_64

Complete!
myadmin@techrich-server:~$ sudo dnf install net-tools -y
Last metadata expiration check: 0:08:22 ago on Sun 01 Feb 2026 04:45:52 AM EST.
Package net-tools-2.0-0.73.20160912git.el10.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
myadmin@techrich-server:~$ which htop iotop netstat top
/usr/bin/htop
/usr/sbin/iotop
/usr/bin/netstat
/usr/bin/top
myadmin@techrich-server:~$
```

CPU Monitoring

Monitor CPU performance using top

```
myadmin@techrich-server:~ - sudo su - it01
myadmin@techrich-server:~$ top -b -n 1
top - 04:56:54 up 3:03, 4 users, load average: 0.88, 0.81, 0.93
Tasks: 326 total, 1 running, 325 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 4.5 sy, 0.0 ni, 95.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 2697.7 total, 132.7 free, 2365.7 used, 446.3 buff/cache
MiB Swap: 2048.0 total, 1015.7 free, 1032.3 used, 332.0 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
13339 myadmin   20   0 231580 5020 2924 R  9.1   0.2   0:00.02 top
   1 root      20   0  50180 9584 6196 S  0.0   0.3   0:13.30 systemd
   2 root      20   0   0      0   0 S  0.0   0.0   0:00.06 kthreadd
   3 root      20   0   0      0   0 S  0.0   0.0   0:00.00 pool_workqueue_release
   4 root      0 -20   0      0   0 I  0.0   0.0   0:00.00 kworker/R-rcu_gp
   5 root      0 -20   0      0   0 I  0.0   0.0   0:00.00 kworker/R-sync_wq
   6 root      0 -20   0      0   0 I  0.0   0.0   0:00.00 kworker/R-slub_flushwq
   7 root      0 -20   0      0   0 I  0.0   0.0   0:00.00 kworker/R-netns
  10 root      0 -20   0      0   0 I  0.0   0.0   0:00.00 kworker/0:0H-events_highpri
  11 root      20   0   0      0   0 I  0.0   0.0   0:00.00 kworker/u512:0-ipv6_addrconf
  12 root      0 -20   0      0   0 I  0.0   0.0   0:00.00 kworker/R-mm_percpu_wq
  13 root      20   0   0      0   0 I  0.0   0.0   0:00.35 kworker/u512:1-netns
  14 root      20   0   0      0   0 I  0.0   0.0   0:00.00 rcu_tasks_kthread
  15 root      20   0   0      0   0 I  0.0   0.0   0:00.00 rcu_tasks_rude_kthread
  16 root      20   0   0      0   0 I  0.0   0.0   0:00.00 rcu_tasks_trace_kthread
  17 root      20   0   0      0   0 S  0.0   0.0   0:01.06 ksoftirqd/0
  18 root      20   0   0      0   0 I  0.0   0.0   0:09.43 rcu_preempt
  19 root      20   0   0      0   0 S  0.0   0.0   0:00.00 rcu_exp_par_gp_kthread_worker/1
  20 root      20   0   0      0   0 S  0.0   0.0   0:00.02 rcu_exp_gp_kthread_worker
  21 root      rt   0   0      0   0 S  0.0   0.0   0:00.10 migration/0
```

Monitor CPU using htop

```
myadmin@techrich-server:~ - sudo su - it01
0% [|||||] 14.3% Tasks: 153, 776 thr, 175 kthr; 0 running
1% [|||||] 100.0% Load average: 0.85 0.81 0.92
Mem [|||||] 2.03G/2.63G Uptime: 03:05:03
Swp [|||||] 916M/2.00G

Main I/O
  PID USER      PRI  NI  VIRT  RES  SHR S CPU%MEM%  TIME+  Command
13363 myadmin   20   0 227M 6372 4256 R 57.1 0.2 0:00.26 htop -n 1
   1 root      20   0  50180 9584 6196 S  0.0  0.3 0:13.30 /usr/lib/systemd/systemd --switched-ro
  885 root      20   0 34488 4348 3708 S  0.0  0.2 0:02.86 /usr/lib/systemd/systemd-journald
  926 root      20   0 15864 1696 1580 S  0.0  0.1 0:00.20 /usr/lib/systemd/systemd-userdbd
  937 root      20   0 37784 2860 2756 S  0.0  0.1 0:00.67 /usr/lib/systemd/systemd-udev
 1006 rpc      20   0 12628 160 136 S  0.0  0.0 0:00.06 /usr/bin/rpcbind -w -f
 1009 root      16  -4 94392 1288 1064 S  0.0  0.0 0:00.42 /usr/sbin/auditd
 1010 root      16  -4 94392 1288 1064 S  0.0  0.0 0:00.03 /usr/sbin/auditd
 1011 root      16  -4 6164 856 712 S  0.0  0.0 0:00.15 /usr/sbin/sedispach
 1012 root      16  -4 94392 1288 1064 S  0.0  0.0 0:00.11 /usr/sbin/auditd
 1016 root      20   0  5364 12 8 S  0.0  0.0 0:00.00 /usr/sbin/nfsdclld
 1022 dbus     20   0  9036 1548 1372 S  0.0  0.1 0:00.14 /usr/bin/dbus-broker-launch --scope sy
 1033 dbus     20   0  8464 2456 1232 S  0.0  0.1 0:03.20 dbus-broker --log 4 --controller 9 --m
 1039 avahi    20   0  6152 1372 1228 S  0.0  0.0 0:00.31 avahi-daemon: running [techrich-server
 1042 root      20   0 80540 1596 1416 S  0.0  0.1 0:01.25 /usr/sbin/irqbalance
 1043 libstorage 20   0  2504 256 220 S  0.0  0.0 0:00.09 /usr/bin/lsm
 1044 root      20   0  2580 12 8 S  0.0  0.0 0:00.01 /usr/sbin/mcelog --daemon --foreground
 1045 polkitd 20   0  592M 4172 3704 S  0.0  0.2 0:01.15 /usr/lib/polkit-1/polkitd --no-debug -
 1046 rtkit    21   1 21316 2000 1868 S  0.0  0.1 0:00.26 /usr/libexec/rtkit-daemon
myadmin@techrich-server:~$
```

Check CPU usage details

```
myadmin@techrich-server:~ -- sudo su - it01
myadmin@techrich-server:~$ cat /proc/cpuinfo
processor       : 0
vendor_id     : GenuineIntel
cpu family    : 6
model        : 186
model name    : 13th Gen Intel(R) Core(TM) i5-1340P
stepping     : 2
microcode    : 0xffffffff
cpu MHz      : 2188.798
cache size   : 12288 KB
physical id  : 0
siblings    : 1
core id     : 0
cpu cores   : 1
apicid     : 0
initial apicid : 0
fpu        : yes
fpu_exception : yes
cpuid level : 32
wp         : yes
flags      : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr
sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon rep_good nopl xtopology tsc_reliable
nonstop_tsc cpuid tsc_known_freq pni pclmulqdq sse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes
xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust
bmi1 avx2 smep bmi2 erms invpcid rdseed adx smap clflushopt clwb sha_ni xsaveopt xsavec xgetbv1 xsaves av
x_vnni arat umip gfni vaes vpclmulqdq rdpid movdiri movdir64b fsrm md_clear serialize flush_l1d arch_capa
bilities
bugs       : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs retbleed rfds bhi
spectre_v2 user_its
```

Check CPU load average

```
myadmin@techrich-server:~ -- sudo su - it01
myadmin@techrich-server:~$ uptime
 04:59:39 up 3:06, 4 users, load average: 1.30, 0.97, 0.97
myadmin@techrich-server:~$ nproc
2
myadmin@techrich-server:~$
```

RAM monitoring

Memory overview and detailed memory info

```
myadmin@techrich-server:~ - sudo su - it01

myadmin@techrich-server:~$ free -h
              total        used         free   shared  buff/cache   available
Mem:           2.6Gi         2.1Gi         351Mi       30Mi        415Mi        512Mi
Swap:          2.0Gi          979Mi         1.0Gi

myadmin@techrich-server:~$ cat /proc/meminfo
MemTotal:        2762396 kB
MemFree:          360000 kB
MemAvailable:    525504 kB
Buffers:           0 kB
Cached:          375332 kB
SwapCached:      134788 kB
Active:          1240708 kB
Inactive:        435308 kB
Active(anon):    1055176 kB
Inactive(anon):  274716 kB
Active(file):    185532 kB
Inactive(file):  160592 kB
Unevictable:     0 kB
Mlocked:         0 kB
SwapTotal:       2097148 kB
SwapFree:        1094008 kB
Zswap:           0 kB
Zswapped:        0 kB
Dirty:           656 kB
Writeback:       0 kB
AnonPages:      1271036 kB
```

Disk Monitoring

Overall disk usage and detailed disk usage for specific directories

```
myadmin@techrich-server:~ - sudo su - it01

myadmin@techrich-server:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/rl-root 17G  5.1G  12G  30% /
devtmpfs        809M   0  809M   0% /dev
tmpfs           837M   84K  837M   1% /dev/shm
tmpfs           335M   8.6M  327M   3% /run
tmpfs           1.0M   0  1.0M   0% /run/credentials/systemd-journald.service
/dev/nvme0n1p2  960M  275M  686M  29% /boot
tmpfs           168M  140K  168M   1% /run/user/1000
/dev/sr0        1.5G  1.5G   0 100% /run/media/myadmin/Rocky-10-1-x86_64-dvd
tmpfs           168M   56K  168M   1% /run/user/0

myadmin@techrich-server:~$ du -sh /shared/
du: cannot read directory '/shared/developers': Permission denied
du: cannot read directory '/shared/testers': Permission denied
du: cannot read directory '/shared/hr': Permission denied
du: cannot read directory '/shared/it': Permission denied
du: cannot read directory '/shared/management': Permission denied
16K    /shared/

myadmin@techrich-server:~$ sudo du -sh /shared/
[sudo] password for myadmin:
40K    /shared/

myadmin@techrich-server:~$ sudo du -sh /var/log
15M    /var/log

myadmin@techrich-server:~$ sudo du -sh /home
695M   /home

myadmin@techrich-server:~$
```

Disk I/O Monitoring

Monitoring disk I/O using iostat and iotop

```

myadmin@techrich-server:~$ sudo su - it01
myadmin@techrich-server:~$ iostat -x 1 3
Linux 6.12.0-124.8.1.el10_1.x86_64 (techrich-server.local)    02/01/2026    _x86_64_    (2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           13.83    0.01  10.04   5.58    0.00   70.53

Device            r/s    kB/s    rrqm/s  %rrqm r_await rareq-sz    w/s    kB/s    wrqm/s  %wrqm w_await
t wareq-sz    d/s    dkB/s    drqm/s  %drqm d_await dareq-sz    f/s f_await  aqu-sz  %util
dm-0              264.49 17607.91    0.00  0.00    0.63   66.57    3.68   83.61    0.00  0.00    3.3
8 22.70      0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00    0.18   4.46
dm-1             878.84 3515.52    0.00  0.00    0.37    4.00  993.88 3983.87    0.00  0.00   12.0
3 4.01      0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00   12.28  15.66
nvme0n1          1037.94 21129.67  105.48   9.22    0.44   20.36  276.45 4067.67  721.14  72.29  20.0
5 14.71      0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00    6.00  13.75
sr0              0.01    0.27    0.00  0.00   16.57   26.55    0.00    0.00    0.00  0.00    0.0
0 0.00      0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00    0.00  0.02

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           5.50    0.00   5.00   2.50    0.00   87.00

Device            r/s    kB/s    rrqm/s  %rrqm r_await rareq-sz    w/s    kB/s    wrqm/s  %wrqm w_await
t wareq-sz    d/s    dkB/s    drqm/s  %drqm d_await dareq-sz    f/s f_await  aqu-sz  %util
dm-0              0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00    0.00    0.00  0.0
0 0.00      0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00    0.00  0.0
dm-1             15.00   60.00    0.00  0.00    0.73    4.00    0.00    0.00    0.00  0.00  0.0
0 0.00      0.00    0.00    0.00  0.00    0.00    0.00    0.00    0.00    0.01  0.80
nvme0n1          15.00   60.00    0.00  0.00    0.60    4.00    0.00    0.00    0.00  0.00  0.0

```

```

myadmin@techrich-server:~$ sudo su - it01
Total DISK READ: 3.59 K/s ... | Total DISK WRITE: 14.38 K/s ...
Current DISK READ: 3.59 K/s ... | Current DISK WRITE: 32.35 K/s ...
TID  PRIO USER    DISK READ  DISK WRITE  GRAPH[R+W]  COMMAND
3502 !be/4 myadmin  3.59 K/s   0.00 B/s   ... | ptyxis
3503 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3504 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3505 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3506 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3507 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3549 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3550 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3551 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3552 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3553 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
3554 be/7 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
13769 be/4 myadmin  0.00 B/s   0.00 B/s   ... | ptyxis
11997 !be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12129 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12262 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12017 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12018 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12019 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12021 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12022 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12024 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12025 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12027 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox
12028 be/4 myadmin  0.00 B/s   0.00 B/s   ... | firefox

```

Network Monitoring

Monitoring network interface status

```
myadmin@techrich-server:~ - sudo su - it01

myadmin@techrich-server:~$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:08:fe:00 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname enx000c2908fe00
    inet 192.168.19.129/24 brd 192.168.19.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe08:fe00/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
myadmin@techrich-server:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:08:fe:00 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname enx000c2908fe00
myadmin@techrich-server:~$ ip route show
default via 192.168.19.2 dev ens160 proto static metric 100
192.168.19.0/24 dev ens160 proto kernel scope link src 192.168.19.129 metric 100
myadmin@techrich-server:~$
```

Monitoring network connection and ports using ss -tn

```
myadmin@techrich-server:~ - sudo su - it01

192.168.19.0/24 dev ens160 proto kernel scope link src 192.168.19.129 metric 100
myadmin@techrich-server:~$

myadmin@techrich-server:~$ ss -tn
State      Recv-Q    Send-Q      Local Address:Port      Peer Address:Port
ESTAB      0          0           192.168.19.129:44504    20.189.173.26:443
ESTAB      0          0           192.168.19.129:48632    18.97.36.58:443
ESTAB      0          0           192.168.19.129:48674    34.107.243.93:443
ESTAB      0          0           192.168.19.129:48314    52.108.9.12:443
ESTAB      0          0           192.168.19.129:54734    52.111.240.2:443
ESTAB      0          0           192.168.19.129:39334    52.108.36.35:443
ESTAB      0          0           192.168.19.129:44514    20.189.173.26:443
ESTAB      0          0           192.168.19.129:52416    52.108.68.0:443
myadmin@techrich-server:~$ ss -tlnp
State      Recv-Q    Send-Q      Local Address:Port      Peer Address:Port      Process
LISTEN     0          4096       0.0.0.0:20048            0.0.0.0:*
LISTEN     0          4096       0.0.0.0:57231            0.0.0.0:*
LISTEN     0          4096       0.0.0.0:40879            0.0.0.0:*
LISTEN     0          4096       127.0.0.1:631            0.0.0.0:*
LISTEN     0          4096       0.0.0.0:111              0.0.0.0:*
LISTEN     0          4096       0.0.0.0:2049            0.0.0.0:*
LISTEN     0          128        0.0.0.0:22               0.0.0.0:*
LISTEN     0          4096       [::]:20048               [::]:*
LISTEN     0          4096       *:9090                   *:
LISTEN     0          4096       [::]:59313               [::]:*
LISTEN     0          4096       [::]:39123               [::]:*
LISTEN     0          511        *:80                      *:
LISTEN     0          4096       [::]:111                 [::]:*
LISTEN     0          4096       [::]:2049                [::]:*
```

```
myadmin@techrich-server:~ -- sudo su - it01

myadmin@techrich-server:~$ ss -tn state established
Recv-Q          Send-Q          Local Address:Port      Peer Address:Port
0               0              192.168.19.129:44504    20.189.173.26:443
0               0              192.168.19.129:54390    34.107.243.93:443
0               0              192.168.19.129:48632    18.97.36.58:443
0               0              192.168.19.129:54380    34.107.243.93:443
0               0              192.168.19.129:48314    52.108.9.12:443
0               0              192.168.19.129:54734    52.111.240.2:443
0               0              192.168.19.129:39334    52.108.36.35:443
0               0              192.168.19.129:44514    20.189.173.26:443
0               0              192.168.19.129:52416    52.108.68.0:443
myadmin@techrich-server:~$
```

Log Analysis

Analyzing Using journalctl

Verify all system logs

```
myadmin@techrich-server:~ -- sudo su - it01

myadmin@techrich-server:~$ sudo journalctl
[sudo] password for myadmin:
Feb 01 01:37:49 techrich-server.local kernel: Linux version 6.12.0-124.8.1.el10_1.x86_64 (mockbuild@iad1)
Feb 01 01:37:49 techrich-server.local kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.8.1
Feb 01 01:37:49 techrich-server.local kernel: BIOS-provided physical RAM map:
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000098bfff] usa>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x00000000000098c000-0x0000000000009fffff] res>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x000000000000dc0000-0x000000000000ffffff] res>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x000000000001000000-0x000000000007fedfffff] usa>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x000000000007fee00000-0x000000000007fefeffff] ACP>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x000000000007feff0000-0x000000000007feffffff] ACP>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x000000000007fff00000-0x000000000007ffffffffff] usa>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x00000000000f00000000-0x00000000000f7ffffffffff] res>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x0000000000fec0000000-0x0000000000fec0fffff] res>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x0000000000fee0000000-0x0000000000fee00ffff] res>
Feb 01 01:37:49 techrich-server.local kernel: BIOS-e820: [mem 0x0000000000ffe0000000-0x0000000000ffffffffff] res>
Feb 01 01:37:49 techrich-server.local kernel: NX (Execute Disable) protection: active
Feb 01 01:37:49 techrich-server.local kernel: APIC: Static calls initialized
Feb 01 01:37:49 techrich-server.local kernel: SMBIOS 2.7 present.
Feb 01 01:37:49 techrich-server.local kernel: DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Re
Feb 01 01:37:49 techrich-server.local kernel: DMI: Memory slots populated: 1/128
Feb 01 01:37:49 techrich-server.local kernel: vmware: hypercall mode: 0x02
Feb 01 01:37:49 techrich-server.local kernel: Hypervisor detected: VMware
Feb 01 01:37:49 techrich-server.local kernel: vmware: TSC freq read from hypervisor : 2188.798 MHz
Feb 01 01:37:49 techrich-server.local kernel: vmware: Host bus clock speed read from hypervisor : 6600000
Feb 01 01:37:49 techrich-server.local kernel: vmware: using clock offset of 6794067790 ns
Feb 01 01:37:49 techrich-server.local kernel: tsc: Detected 2188.798 MHz processor
```

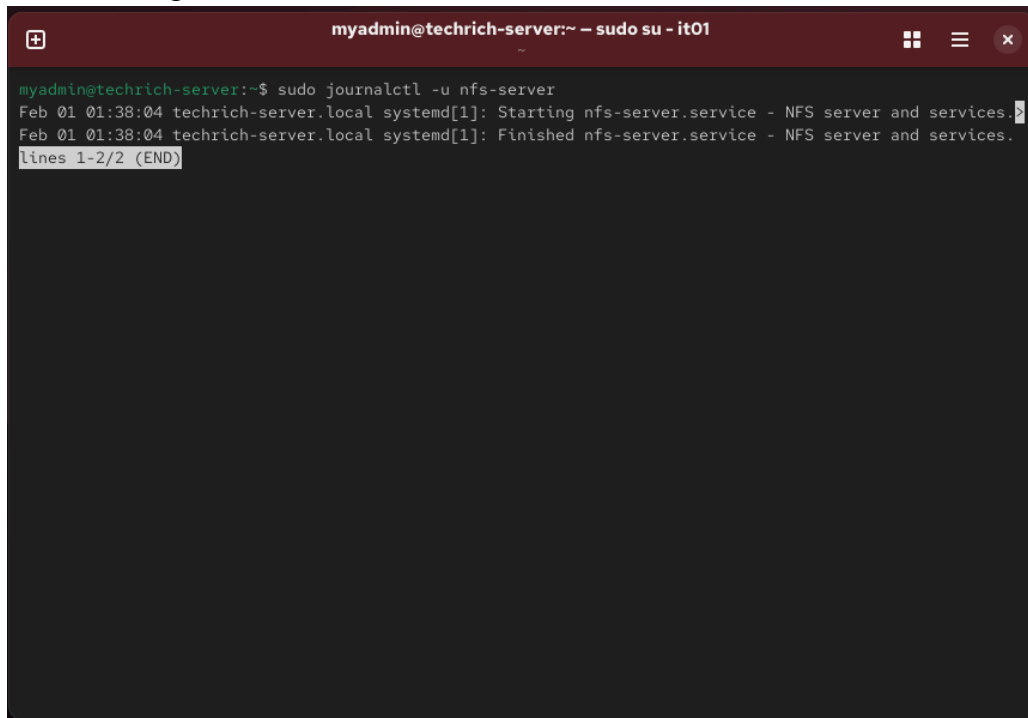
Check sshd logs

```
myadmin@techrich-server:~ - sudo su - it01
Feb 01 01:37:49 techrich-server.local kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserv
Feb 01 01:37:49 techrich-server.local kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
myadmin@techrich-server:~$
myadmin@techrich-server:~$ sudo journalctl -u sshd
Feb 01 01:38:03 techrich-server.local systemd[1]: Starting sshd.service - OpenSSH server daemon...
Feb 01 01:38:03 techrich-server.local sshd[1185]: Server listening on 0.0.0.0 port 22.
Feb 01 01:38:03 techrich-server.local sshd[1185]: Server listening on :: port 22.
Feb 01 01:38:03 techrich-server.local systemd[1]: Started sshd.service - OpenSSH server daemon.
Feb 01 03:13:28 techrich-server.local systemd[1]: Stopping sshd.service - OpenSSH server daemon...
Feb 01 03:13:28 techrich-server.local sshd[1185]: Received signal 15; terminating.
Feb 01 03:13:28 techrich-server.local systemd[1]: sshd.service: Deactivated successfully.
Feb 01 03:13:28 techrich-server.local systemd[1]: Stopped sshd.service - OpenSSH server daemon.
Feb 01 03:13:28 techrich-server.local systemd[1]: Starting sshd.service - OpenSSH server daemon...
Feb 01 03:13:29 techrich-server.local sshd[7830]: Server listening on 0.0.0.0 port 22.
Feb 01 03:13:29 techrich-server.local sshd[7830]: Server listening on :: port 22.
Feb 01 03:13:29 techrich-server.local systemd[1]: Started sshd.service - OpenSSH server daemon.
Feb 01 03:20:09 techrich-server.local sshd-session[8237]: User root from ::1 not allowed because not lis
Feb 01 03:20:22 techrich-server.local sshd-session[8237]: pam_unix(sshd:auth): authentication failure; l
Feb 01 03:20:24 techrich-server.local sshd-session[8237]: Failed password for invalid user root from ::1
Feb 01 03:20:37 techrich-server.local sshd-session[8237]: Failed password for invalid user root from ::1
Feb 01 03:20:55 techrich-server.local sshd-session[8237]: Failed password for invalid user root from ::1
Feb 01 03:20:56 techrich-server.local sshd-session[8237]: error: maximum authentication attempts exceede
Feb 01 03:20:56 techrich-server.local sshd-session[8237]: Disconnecting invalid user root ::1 port 37522
Feb 01 03:20:56 techrich-server.local sshd-session[8237]: PAM 2 more authentication failures; logname= u
Feb 01 03:24:41 techrich-server.local sshd-session[8405]: pam_unix(sshd:auth): authentication failure; l
Feb 01 03:24:43 techrich-server.local sshd-session[8405]: Failed password for it01 from ::1 port 52898 s
Feb 01 03:24:52 techrich-server.local sshd-session[8405]: Failed password for it01 from ::1 port 52898 s
Feb 01 03:24:56 techrich-server.local sshd-session[8405]: Failed password for it01 from ::1 port 52898 s
Feb 01 03:24:57 techrich-server.local sshd-session[8405]: error: maximum authentication attempts exceede
```

Check httpd logs

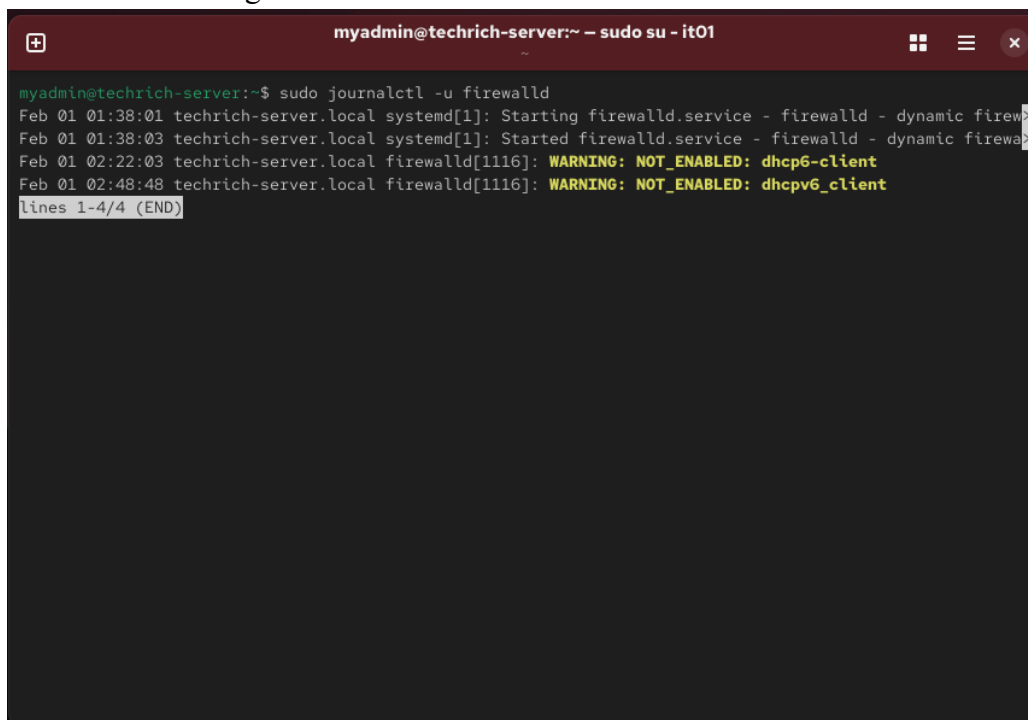
```
myadmin@techrich-server:~ - sudo su - it01
myadmin@techrich-server:~$ sudo journalctl -u httpd
Feb 01 01:38:03 techrich-server.local systemd[1]: Starting httpd.service - The Apache HTTP Server...
Feb 01 01:38:03 techrich-server.local (httpd)[1209]: httpd.service: Referenced but unset environment var
Feb 01 01:38:04 techrich-server.local httpd[1209]: Server configured, listening on: port 80
Feb 01 01:38:04 techrich-server.local systemd[1]: Started httpd.service - The Apache HTTP Server.
lines 1-4/4 (END)
```

Check nfs logs



```
myadmin@techrich-server:~ - sudo su - it01
myadmin@techrich-server:~$ sudo journalctl -u nfs-server
Feb 01 01:38:04 techrich-server.local systemd[1]: Starting nfs-server.service - NFS server and services.
Feb 01 01:38:04 techrich-server.local systemd[1]: Finished nfs-server.service - NFS server and services.
lines 1-2/2 (END)
```

Check firewalld logs



```
myadmin@techrich-server:~ - sudo su - it01
myadmin@techrich-server:~$ sudo journalctl -u firewalld
Feb 01 01:38:01 techrich-server.local systemd[1]: Starting firewalld.service - firewalld - dynamic firewa
Feb 01 01:38:03 techrich-server.local systemd[1]: Started firewalld.service - firewalld - dynamic firewa
Feb 01 02:22:03 techrich-server.local firewalld[1116]: WARNING: NOT_ENABLED: dhcp6-client
Feb 01 02:48:48 techrich-server.local firewalld[1116]: WARNING: NOT_ENABLED: dhcpv6_client
lines 1-4/4 (END)
```

Analyzing /var/log files

analyze ssh authentication logs

```
myadmin@techrich-server:~ - sudo su - it01

myadmin@techrich-server:~$
myadmin@techrich-server:~$ sudo cat /var/log/secure
Feb 1 00:32:36 techrich-server gdm-password[35917]: gkr-pam: unlocked login keyring
Feb 1 00:52:45 techrich-server sudo[36542]: pam_unix(sudo:auth): authentication failure; logname=it02 uid=1000 euid=0 tty=/dev/pts/4 ruser=myadmin rhost= user=myadmin
Feb 1 00:53:07 techrich-server sudo[36542]: myadmin : TTY=pts/4 ; PWD=/home/myadmin ; USER=root ; COMMAND=/bin/systemctl start nfs-server
Feb 1 00:53:07 techrich-server sudo[36542]: pam_unix(sudo:session): session opened for user root(uid=0) by it02(uid=1000)
Feb 1 00:53:08 techrich-server sudo[36542]: pam_unix(sudo:session): session closed for user root
Feb 1 00:53:30 techrich-server sudo[36639]: myadmin : TTY=pts/4 ; PWD=/home/myadmin ; USER=root ; COMMAND=/bin/systemctl enable nfs-server
Feb 1 00:53:30 techrich-server sudo[36639]: pam_unix(sudo:session): session opened for user root(uid=0) by it02(uid=1000)
Feb 1 00:53:31 techrich-server sudo[36639]: pam_unix(sudo:session): session closed for user root
Feb 1 00:53:45 techrich-server sudo[36799]: myadmin : TTY=pts/4 ; PWD=/home/myadmin ; USER=root ; COMMAND=/bin/systemctl start rpcbind
Feb 1 00:53:45 techrich-server sudo[36799]: pam_unix(sudo:session): session opened for user root(uid=0) by it02(uid=1000)
Feb 1 00:53:45 techrich-server sudo[36799]: pam_unix(sudo:session): session closed for user root
Feb 1 00:53:56 techrich-server sudo[36807]: myadmin : TTY=pts/4 ; PWD=/home/myadmin ; USER=root ; COMMAND=/bin/systemctl enable rpcbind
Feb 1 00:53:56 techrich-server sudo[36807]: pam_unix(sudo:session): session opened for user root(uid=0) by it02(uid=1000)
Feb 1 00:53:57 techrich-server sudo[36807]: pam_unix(sudo:session): session closed for user root
Feb 1 00:54:06 techrich-server sudo[36955]: myadmin : TTY=pts/4 ; PWD=/home/myadmin ; USER=root ; COMMAND=/bin/systemctl status nfs-server
Feb 1 00:54:06 techrich-server sudo[36955]: pam_unix(sudo:session): session opened for user root(uid=0)
```

Analyzing system messages

```
myadmin@techrich-server:~ - sudo su - it01

myadmin@techrich-server:~$ sudo tail -50 /var/log/messages
[sudo] password for myadmin:
Sorry, try again.
[sudo] password for myadmin:
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:18 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:33 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:33 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:33 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:48 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:48 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:40:48 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:41:03 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:41:03 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:41:03 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:41:03 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:42:34 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:42:34 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
Feb 1 05:42:34 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
```

Analyzing Apache access log

```
myadmin@techrich-server:~  
myadmin@techrich-server:~ - sudo su - it01  
myadmin@techrich-server:~$ sudo tail -50 /var/log/httpd/access_log  
:::1 - - [31/Jan/2026:21:48:23 -0500] "GET / HTTP/1.1" 403 7620 "-" "curl/8.12.1"  
192.168.19.129 - - [31/Jan/2026:21:50:27 -0500] "GET / HTTP/1.1" 403 7620 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
192.168.19.129 - - [31/Jan/2026:21:50:28 -0500] "GET /icons/poweredby.png HTTP/1.1" 200 15443 "http://192.168.19.129/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
192.168.19.129 - - [31/Jan/2026:21:50:28 -0500] "GET /poweredby.png HTTP/1.1" 200 5714 "http://192.168.19.129/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
192.168.19.129 - - [31/Jan/2026:21:50:28 -0500] "GET /favicon.ico HTTP/1.1" 404 196 "http://192.168.19.129/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
:::1 - - [31/Jan/2026:22:31:19 -0500] "GET / HTTP/1.1" 200 7938 "-" "curl/8.12.1"  
127.0.0.1 - - [31/Jan/2026:22:31:46 -0500] "GET / HTTP/1.1" 200 7938 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
127.0.0.1 - - [31/Jan/2026:22:31:47 -0500] "GET /favicon.ico HTTP/1.1" 404 196 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
127.0.0.1 - - [31/Jan/2026:22:32:15 -0500] "GET / HTTP/1.1" 200 7938 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
127.0.0.1 - - [31/Jan/2026:22:33:53 -0500] "GET / HTTP/1.1" 200 7934 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
127.0.0.1 - - [31/Jan/2026:22:33:53 -0500] "GET /favicon.ico HTTP/1.1" 404 196 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
127.0.0.1 - - [31/Jan/2026:22:36:33 -0500] "GET /internal-app/ HTTP/1.1" 200 6632 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"  
myadmin@techrich-server:~$
```

Analyzing Apache error logs

```
myadmin@techrich-server:~  
myadmin@techrich-server:~ - sudo su - it01  
myadmin@techrich-server:~$ sudo tail -50 /var/log/httpd/error_log  
[Sat Jan 31 18:52:44.407781 2026] [suexec:notice] [pid 30682:tid 30682] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Sat Jan 31 18:52:44.490394 2026] [lbmethod_heartbeat:notice] [pid 30682:tid 30682] AH02282: No slotmem from mod_heartbeat  
[Sat Jan 31 18:52:44.492444 2026] [systemd:notice] [pid 30682:tid 30682] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Sat Jan 31 18:52:44.512903 2026] [mpm_event:notice] [pid 30682:tid 30682] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations  
[Sat Jan 31 18:52:44.512989 2026] [core:notice] [pid 30682:tid 30682] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'  
[Sat Jan 31 21:48:23.672239 2026] [autoindex:error] [pid 30695:tid 30792] [client ::1:51348] AH01276: Cannot serve directory /var/www/html/: No matching DirectoryIndex (index.html) found, and server-generated directory index forbidden by Options directive  
[Sat Jan 31 21:50:27.369673 2026] [autoindex:error] [pid 30687:tid 30819] [client 192.168.19.129:60700] AH01276: Cannot serve directory /var/www/html/: No matching DirectoryIndex (index.html) found, and server-generated directory index forbidden by Options directive  
[Sat Jan 31 22:30:24.795417 2026] [mpm_event:notice] [pid 30682:tid 30682] AH00492: caught SIGWINCH, shutting down gracefully  
[Sat Jan 31 22:30:26.231783 2026] [suexec:notice] [pid 34318:tid 34318] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Sat Jan 31 22:30:26.323441 2026] [lbmethod_heartbeat:notice] [pid 34318:tid 34318] AH02282: No slotmem from mod_heartbeat  
[Sat Jan 31 22:30:26.324898 2026] [systemd:notice] [pid 34318:tid 34318] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Sat Jan 31 22:30:26.338173 2026] [mpm_event:notice] [pid 34318:tid 34318] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
```

Analyzing boot messages

```
myadmin@techrich-server:~$ sudo dmesg | tail -50
[10078.340292] [ 3452] 0 3452 161285 100 32 68 0 204800 1312
0 fwupd
[10078.340293] [ 3502] 1000 3502 436684 27 11 16 0 827392 19360
200 ptyxis
[10078.340315] [ 3509] 1000 3509 94442 13 0 13 0 102400 224
200 ptyxis-agent
[10078.340317] [ 3525] 1000 3525 244 16 0 16 0 40960 0
200 catatonit
[10078.340319] [ 3558] 1000 3558 57541 61 32 29 0 69632 480
200 bash
[10078.340321] [ 4031] 1000 4031 189241 34 0 34 0 159744 320
200 gvfsd-trash
[10078.340322] [ 4046] 1000 4046 170892 29 0 29 0 147456 352
200 gvfsd-network
[10078.340324] [ 4052] 1000 4052 152960 54 32 22 0 143360 288
200 gvfsd-dnssd
[10078.340326] [ 4058] 1000 4058 170754 13 0 13 0 143360 320
200 gvfsd-wsdd
[10078.340328] [ 4064] 1000 4064 65038 74 58 16 0 143360 4704
200 wsdd
[10078.340330] [ 7599] 998 7599 60972 80 64 16 0 106496 288
0 sssd_kcm
[10078.340332] [ 8244] 1000 8244 2222 51 32 19 0 65536 224
0 ssh-agent
[10078.340334] [ 8530] 1000 8530 59909 16 0 16 0 94208 352
200 sudo
[10078.340346] [ 8534] 0 8534 5624 76 32 44 0 86016 832
100 systemd
```

Analyzing cron job logs

```
myadmin@techrich-server:~$ sudo cat /var/log/cron
[11719.344035] systemd-rc-local-generator[13971]: /etc/rc.d/rc.local is not marked executable, skipping.
myadmin@techrich-server:~$
myadmin@techrich-server:~$ sudo cat /var/log/cron
Feb 1 01:01:01 techrich-server CROND[37075]: (root) CMD (run-parts /etc/cron.hourly)
Feb 1 01:01:01 techrich-server run-parts[37078]: (/etc/cron.hourly) starting 0anacron
Feb 1 01:01:01 techrich-server anacron[37088]: Anacron started on 2026-02-01
Feb 1 01:01:01 techrich-server anacron[37088]: Normal exit (0 jobs run)
Feb 1 01:01:01 techrich-server run-parts[37090]: (/etc/cron.hourly) finished 0anacron
Feb 1 01:01:01 techrich-server CROND[37074]: (root) CMDEND (run-parts /etc/cron.hourly)
Feb 1 01:38:03 techrich-server crond[1233]: (CRON) STARTUP (1.7.0)
Feb 1 01:38:03 techrich-server crond[1233]: (CRON) INFO (Syslog will be used instead of sendmail.)
Feb 1 01:38:03 techrich-server crond[1233]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 48% if used.)
Feb 1 01:38:03 techrich-server crond[1233]: (CRON) INFO (running with inotify support)
Feb 1 02:01:01 techrich-server CROND[4825]: (root) CMD (run-parts /etc/cron.hourly)
Feb 1 02:01:01 techrich-server run-parts[4828]: (/etc/cron.hourly) starting 0anacron
Feb 1 02:01:01 techrich-server anacron[4838]: Anacron started on 2026-02-01
Feb 1 02:01:01 techrich-server anacron[4838]: Normal exit (0 jobs run)
Feb 1 02:01:01 techrich-server run-parts[4840]: (/etc/cron.hourly) finished 0anacron
Feb 1 02:01:01 techrich-server CROND[4824]: (root) CMDEND (run-parts /etc/cron.hourly)
Feb 1 04:01:01 techrich-server CROND[10079]: (root) CMD (run-parts /etc/cron.hourly)
Feb 1 04:01:01 techrich-server run-parts[10082]: (/etc/cron.hourly) starting 0anacron
Feb 1 04:01:01 techrich-server anacron[10092]: Anacron started on 2026-02-01
Feb 1 04:01:01 techrich-server anacron[10092]: Will run job `cron.daily' in 5 min.
Feb 1 04:01:01 techrich-server anacron[10092]: Jobs will be executed sequentially
Feb 1 04:01:01 techrich-server run-parts[10094]: (/etc/cron.hourly) finished 0anacron
Feb 1 04:01:01 techrich-server CROND[10078]: (root) CMDEND (run-parts /etc/cron.hourly)
Feb 1 04:06:01 techrich-server anacron[10092]: Job `cron.daily' started
```

Analyzing NFS logs

```
myadmin@techrich-server:~  
myadmin@techrich-server:~ - sudo su - it01  
Feb 1 05:01:01 techrich-server CROND[13482]: (root) CMDEND (run-parts /etc/cron.hourly)  
myadmin@techrich-server:~$  
myadmin@techrich-server:~$ sudo cat /var/log/messages | grep nfs  
Feb 1 00:53:07 techrich-server systemd[1]: Mounting proc-fs-nfsd.mount - NFSD configuration filesystem..  
..  
Feb 1 00:53:07 techrich-server systemd[1]: Mounting var-lib-nfs-rpc_pipefs.mount - RPC Pipe File System..  
..  
Feb 1 00:53:07 techrich-server systemd[1]: Mounted var-lib-nfs-rpc_pipefs.mount - RPC Pipe File System..  
Feb 1 00:53:07 techrich-server systemd[1]: Starting nfs-idmapd.service - NFSv4 ID-name mapping service..  
..  
Feb 1 00:53:08 techrich-server systemd[1]: Started nfs-idmapd.service - NFSv4 ID-name mapping service..  
Feb 1 00:53:08 techrich-server systemd[1]: Mounted proc-fs-nfsd.mount - NFSD configuration filesystem..  
Feb 1 00:53:08 techrich-server systemd[1]: Starting nfs-mountd.service - NFS Mount Daemon..  
Feb 1 00:53:08 techrich-server systemd[1]: Starting nfsdclld.service - NFSv4 Client Tracking Daemon..  
Feb 1 00:53:08 techrich-server systemd[1]: Started nfsdclld.service - NFSv4 Client Tracking Daemon..  
Feb 1 00:53:08 techrich-server systemd[1]: Started nfs-mountd.service - NFS Mount Daemon..  
Feb 1 00:53:08 techrich-server systemd[1]: Starting nfs-server.service - NFS server and services..  
Feb 1 00:53:08 techrich-server kernel: NFSD: Using nfsdclld client tracking operations..  
Feb 1 00:53:08 techrich-server systemd[1]: Finished nfs-server.service - NFS server and services..  
Feb 1 01:16:18 techrich-server systemd[1]: Stopping nfs-server.service - NFS server and services..  
Feb 1 01:16:18 techrich-server systemd[1]: nfs-server.service: Deactivated successfully..  
Feb 1 01:16:18 techrich-server systemd[1]: Stopped nfs-server.service - NFS server and services..  
Feb 1 01:16:18 techrich-server systemd[1]: Stopping nfs-idmapd.service - NFSv4 ID-name mapping service..  
..  
Feb 1 01:16:18 techrich-server systemd[1]: Stopping nfs-mountd.service - NFS Mount Daemon..  
Feb 1 01:16:18 techrich-server systemd[1]: nfs-idmapd.service: Deactivated successfully..  
Feb 1 01:16:18 techrich-server systemd[1]: Stopped nfs-idmapd.service - NFSv4 ID-name mapping service..  
Feb 1 01:16:18 techrich-server systemd[1]: Starting nfs-idmapd.service - NFSv4 ID-name mapping service..
```

Explain how system monitoring and log analysis support proactive maintenance, troubleshooting, and security incident response.

System monitoring tracks real-time performance of CPU, memory, and disk usage which help administrators to detect problems before they lead to system failures (Stallings, 2022). Log analysis reviews records to determine what happened, why a failure occurred or if a security breach happened (National Institute of Standards and Technology [NIST], 2006). All together, they enable proactive maintenance by identifying issues before they escalate, speed up troubleshooting by providing an audit trail of system activity, and support security incident response by revealing suspicious behavior such as repeated failed login attempts or unauthorized access (NIST, 2012).

References

- Fedora Project. (2023). DNF package manager documentation. <https://dnf.readthedocs.io>
- National Security Agency & Red Hat. (2022). Security-Enhanced Linux (SELinux). <https://selinuxproject.org>
- Red Hat. (2023). Red Hat Enterprise Linux documentation. <https://access.redhat.com/documentation>
- Rocky Enterprise Software Foundation. (2024). Rocky Linux documentation. <https://docs.rockylinux.org>
- VMware. (2023). VMware Workstation documentation. <https://docs.vmware.com>
- Apache Software Foundation. (2024). Security tips. Apache HTTP Server Project. https://httpd.apache.org/docs/trunk/misc/security_tips.html
- Cole, E. (2011). Advanced persistent threat: Understanding the danger and how to fight it. Syngress.
- The Linux Foundation. (2022). Classic SysAdmin: Understanding Linux file permissions. The Linux Foundation Blog. <https://www.linuxfoundation.org/blog/blog/classic-sysadmin-understanding-linux-file-permissions>
- National Institute of Standards and Technology. (2011). Guidelines on firewalls and firewall policy (NIST Special Publication 800-41 Rev. 1). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf>
- National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- OWASP Foundation. (2023). Path traversal. https://owasp.org/www-community/attacks/Path_Traversal
- Pratt, M. (2019). Encrypting NFSv4 with stunnel TLS. Linux Journal. <https://www.linuxjournal.com/content/encrypting-nfsv4-stunnel-tls>
- Singh, S., Kamkar, M., Kalbarczyk, Z., & Iyer, R. K. (2024). Brute-force SSH attacks in the wild and how to stop them. In Proceedings of the 21st USENIX Conference on Networked Systems Design and Implementation (NSDI '24). USENIX Association. <https://www.usenix.org/system/files/nsdi24-singh-sachin.pdf>
- Stallings, W. (2022). Cryptography and network security: Principles and practices (8th ed.). Pearson Education.
- SUSE. (2023). Access control lists in Linux. In Security and hardening guide (SLES 12 SP5). <https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-security-acls.html>

National Institute of Standards and Technology. (2006). Guide to computer security log management (NIST Special Publication 800-92). U.S. Department of Commerce.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>

National Institute of Standards and Technology. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). U.S. Department of Commerce.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Appendix

Reflective Report:

A. Challenges encountered:

Setting Passwords did not work

When creating users accounts I set the password to "TechRich2026!", however Linux treated the exclamation as a special character so the password was never saved. No error message appeared and I didn't know it failed until I tried to log in later.

3.2 Could Not Log In via SSH

After setting up SSH, I tried logging in as IT admin "it01" but kept getting "Permission denied". This was probably because of the password problem.

File sharing was not working

When I tried to set up NFS, the firewall was blocking it because I used the wrong name for one of the firewall rules, also I forgot that NFS needs rpcbind to be running first. Once I fixed the rule names and started rpcbind, file sharing worked.

B. Troubleshooting

Issue 1: Passwords Were Not Being Saved

What Happened

Password for the 50 users was not saved because it contained exclamation mark and linux misread it

How I Checked

Tool I Used	What It Told Me
passwd -S username	It showed whether the password was set, locked, or missing for that user.
getent shadow username	Check the password entry to see if really no password was saved
ssh user@localhost	Tested if I can log in with the password.

How I Fixed It

Used chpasswd, which doesn't have problems with special characters. I ran it for all 50 users:

```
echo "username:TechRich2026!" | sudo chpasswd
```

After that passwords were saved and SSH logins worked correctly.

4.2 Issue 2: SSH Login Kept Failing

What Happened

I was not able to login after setting SSH. The system kept saying "Permission denied". The reasons of this error were: the passwords were not set (from Issue 1), and SSH was set to only allow specific users to log in.

How I Checked

Tool I Used	What It Told Me
sudo sshd -t	Check if SSH settings file had any mistakes but it was clean.
grep AllowUsers in the SSH config	Check which users were allowed to log in via SSH.
sudo systemctl status sshd	Confirm SSH was running.
Checking /var/log/secure	Check the login failure messages to see exactly why access was denied.

How I Fixed It

First, I fixed the passwords using `chpasswd` (as in Issue 1). Then made sure that SSH settings were correct, only the two IT admin accounts (`it01` and `it02`) were allowed to log in via SSH, then I tested it for each of them it worked for both.

Issue 3: File Sharing Was Blocked

What Happened

I set up NFS, but clients could not access the shared folders, because the firewall was blocking the connection and `rpcbind` service was not running

How I Checked

Tool I Used	What It Told Me
<code>firewall-cmd --list-services</code>	To check which services are allowed through the firewall.
<code>systemctl status nfs-server</code>	Told me the NFS server was not running properly.
<code>systemctl status rpcbind</code>	Checked the status of <code>rpcbind</code> and I found it was not running.
<code>exportfs -v</code>	To check which folders were being shared but I found not folders were shared yet.
<code>showmount -e localhost</code>	Checked what shared folders were visible from the local machine.

How I Fixed It

Changed the names of the firewall rules to ones that are recognized by the system: "`nfs`", "`rpc-bind`", and "`mountd`", then started `rpcbind` and reload the firewall. After restarting the NFS server, I checked the shared folders again and this time all five department folders were accessible.

C. Skills Gained

1. Managing a Linux Server

How to install Linux, create user accounts, set permissions, and keep services running which are the basics that every system administrator needs to know.

2. Keeping Systems Secure

By turning off unnecessary services, blocking ports that are not needed, setting strong password policies and using SSH for admins login.

3. Finding and Fixing Problems

I learned how to inspect what is issue when a some error happen systematically by using specific tools and not just guessing and fixing randomly.

4. Understanding How Services Work Together

I learned that services are not independent, but they work together for example NFS need rpcbind to work and firewalls needs the correct rules to be set to allow the traffic through.

Connection to Computer Science Principles

Principle	How I Saw It in This Project
Access Control	Setting up rules for who can access which files and folders
Security in Layers	Security was considered in many ways: firewalls, SSH login, password policy
Breaking Things Into Smaller Parts	Setting each service separately (SSH, Apache, firewalld,...etc) and testing each alone, which made it easier to configure and test.
Debugging Step by Step	If some error occur, I check first what's the issue using the appropriate tools instead of just fixing things randomly
How Networked Systems Work	I learned that for NFS to work it requires right firewalls rules to be set, helper services and right configurations on the server.
Watching and Logging	Using monitoring tools and reviewing log files to check system performance and detect any issues in the system.