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).

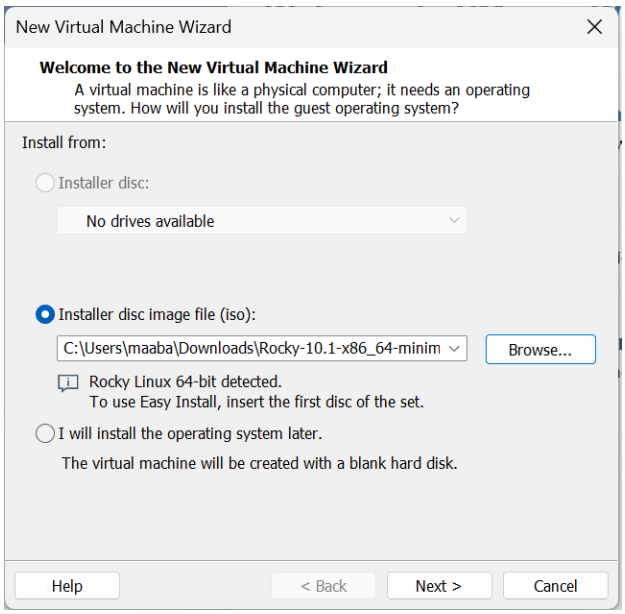
• Enterprise-level support available through ecosystem partners (RESF, 2024).

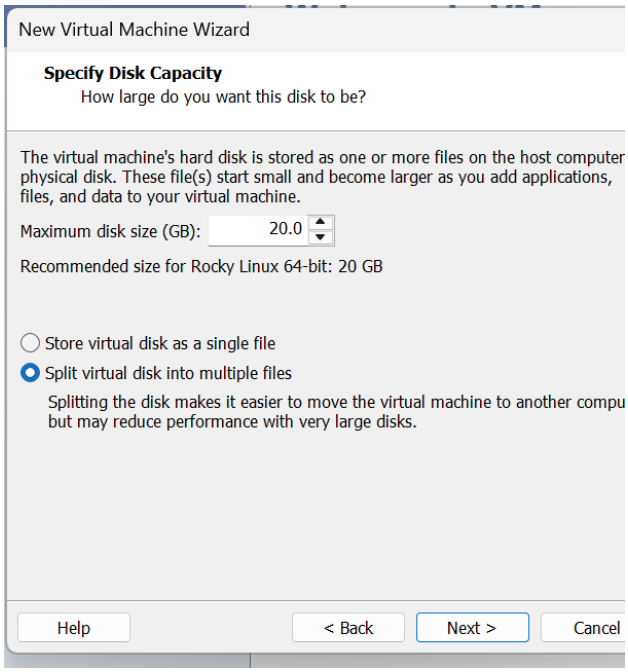
• Compatibility with RHEL documentation and ecosystem tools (Red Hat, 2023).

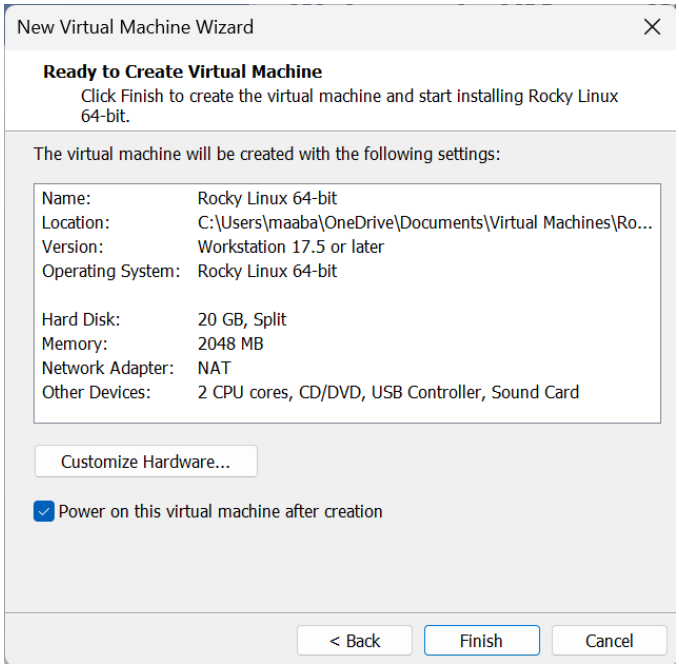
2. Server Installation Process

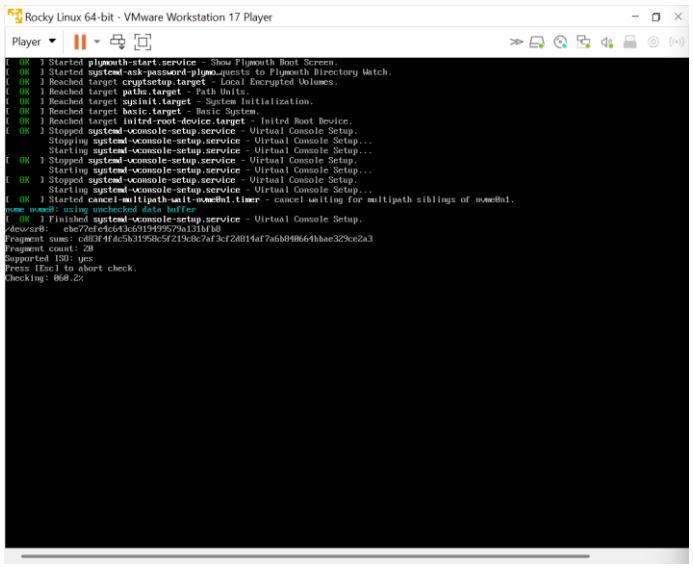
2.1 Virtual Machine Creation

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



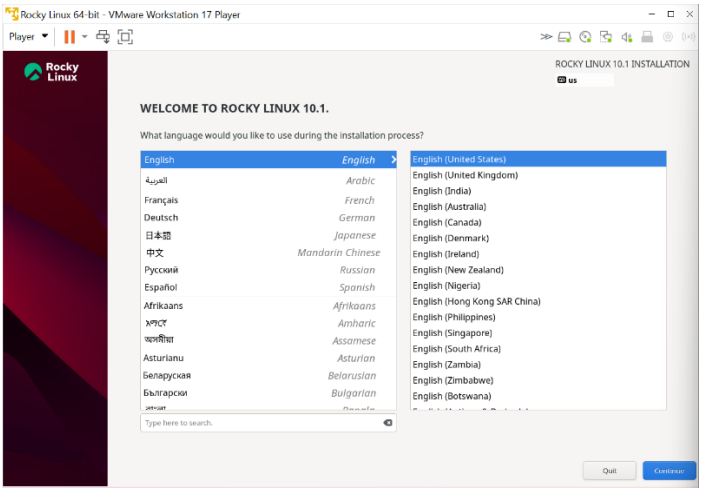




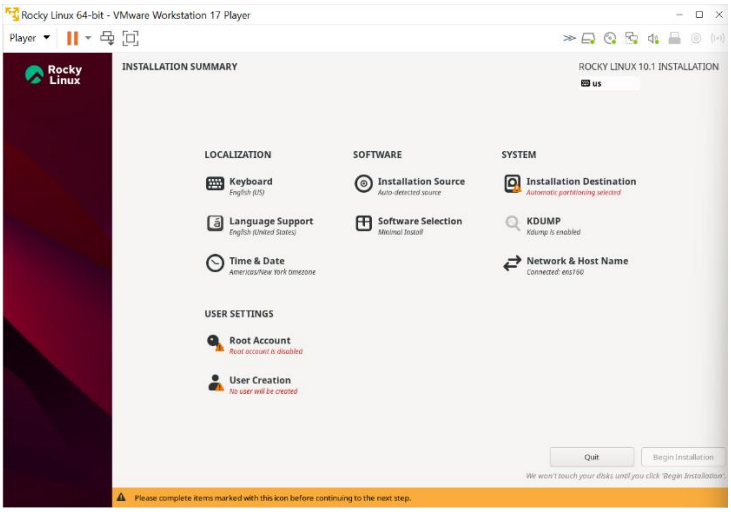


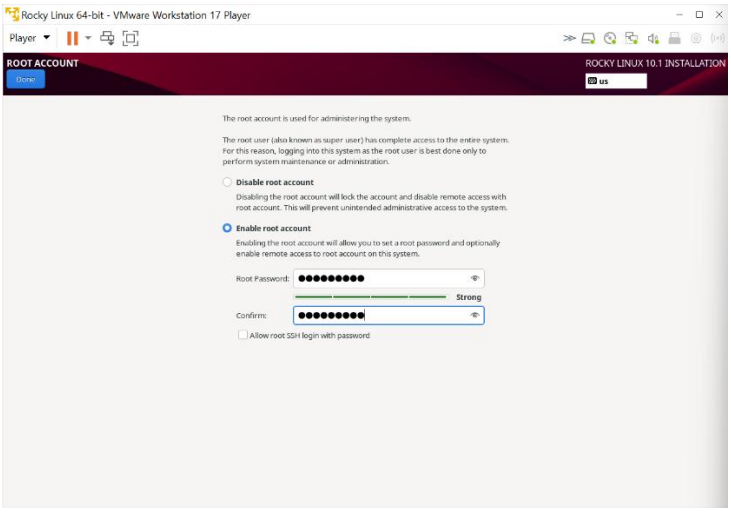
2.1 Installation Process

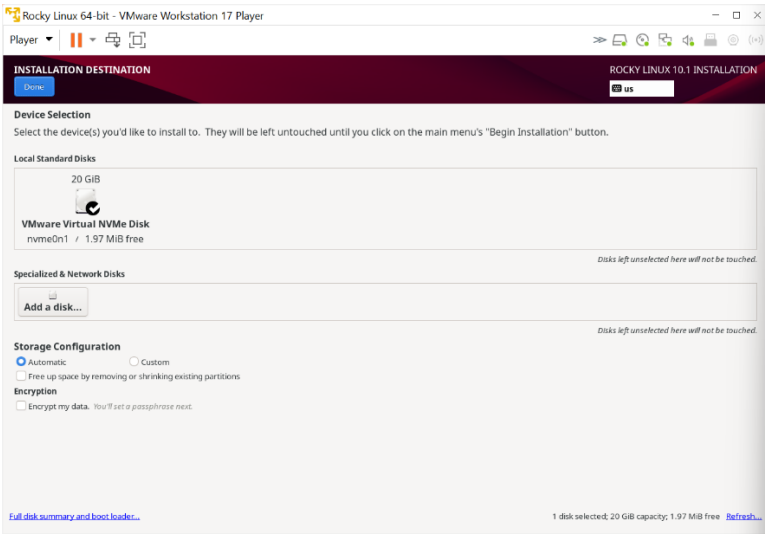
Selecting language: English US

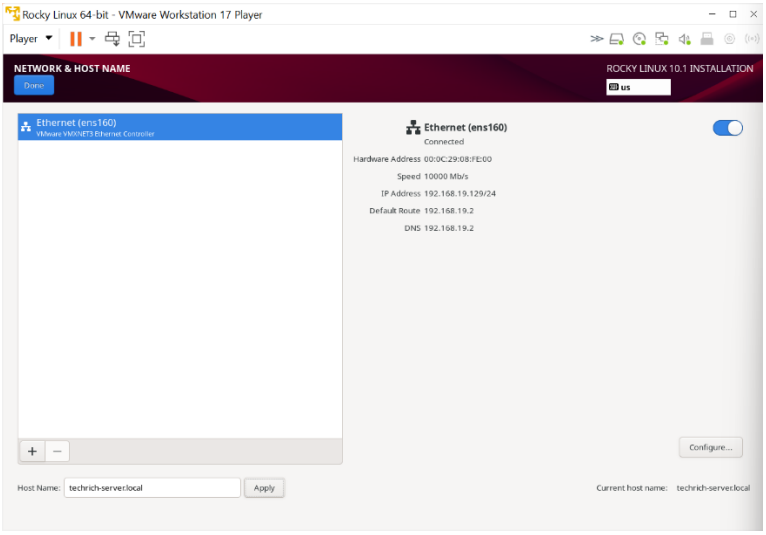


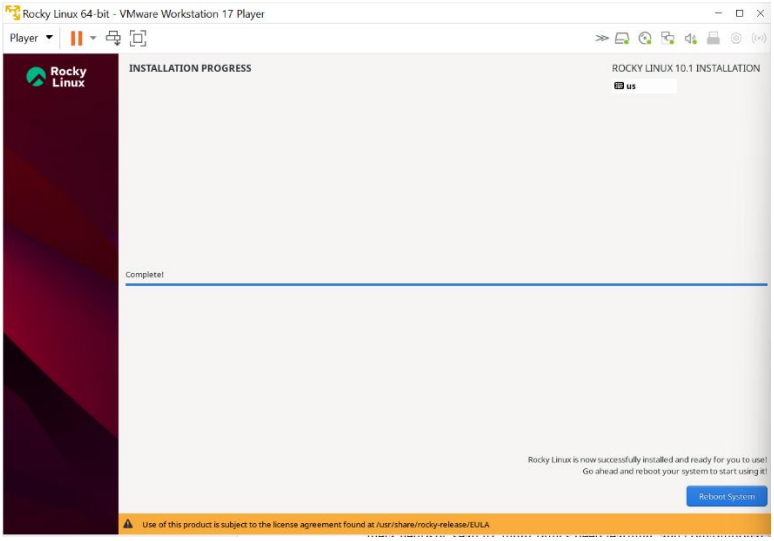
Configuring installation destination, root account and hostname







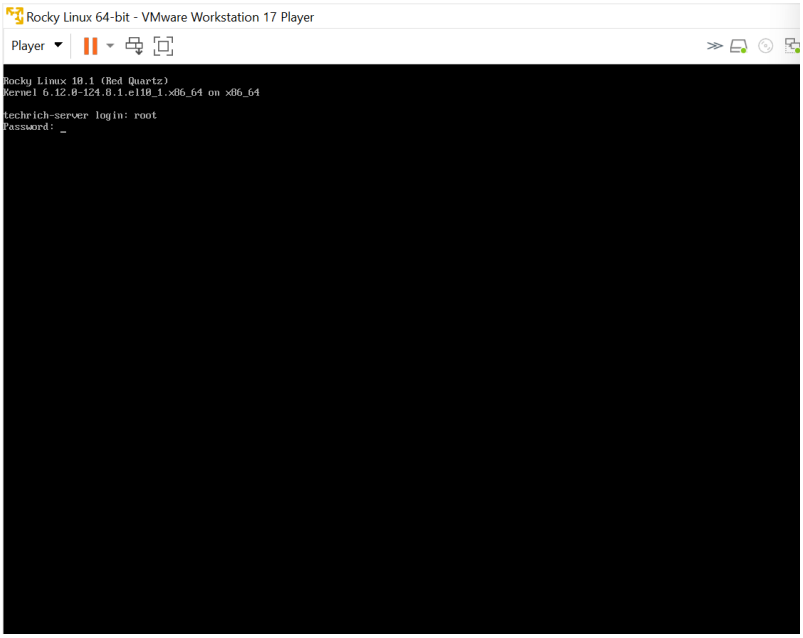




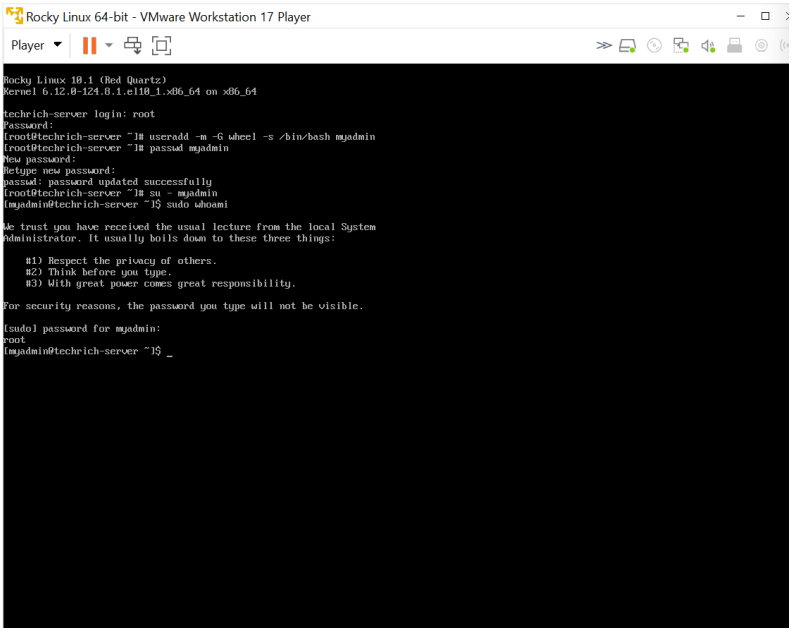
3. Initial System Configuration

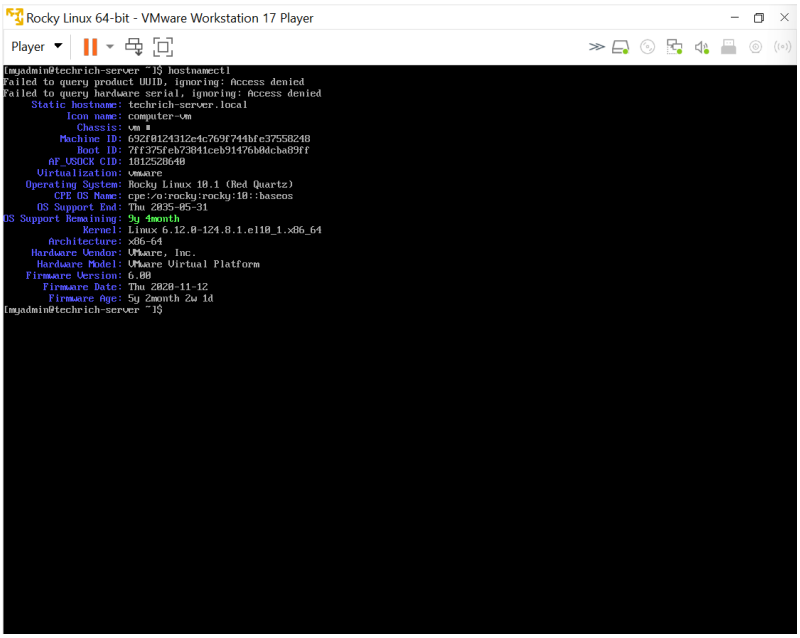
3.1 Post-Installation Updates

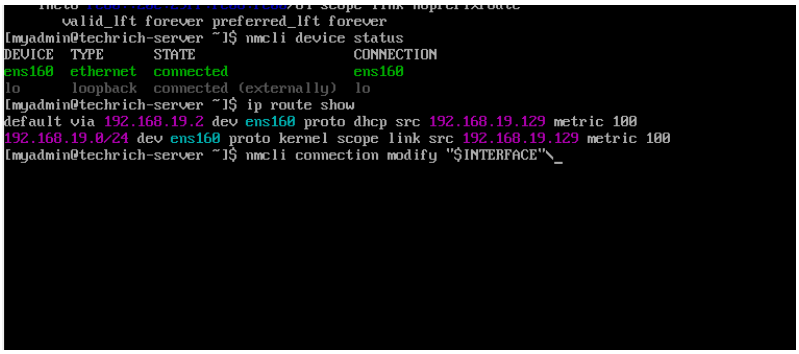
Login as root



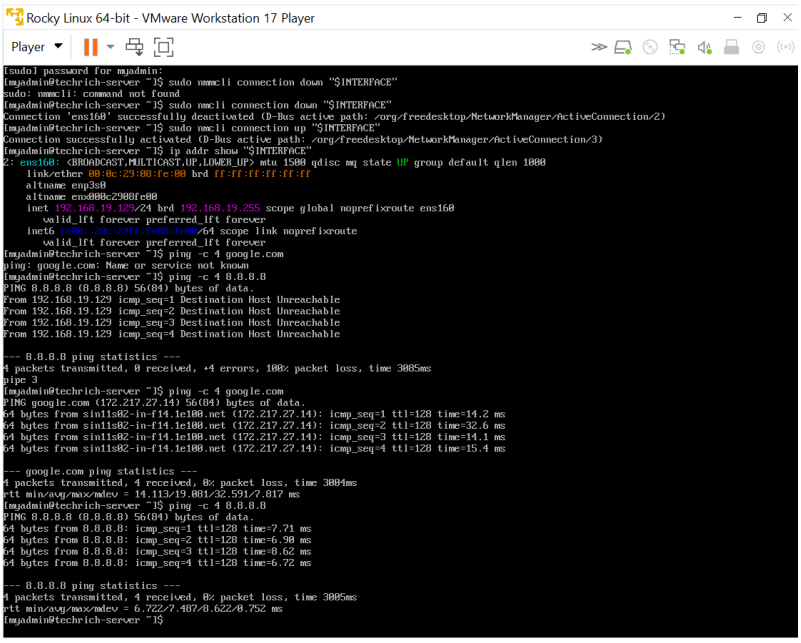
Add user myadmin and give it sudo credentials



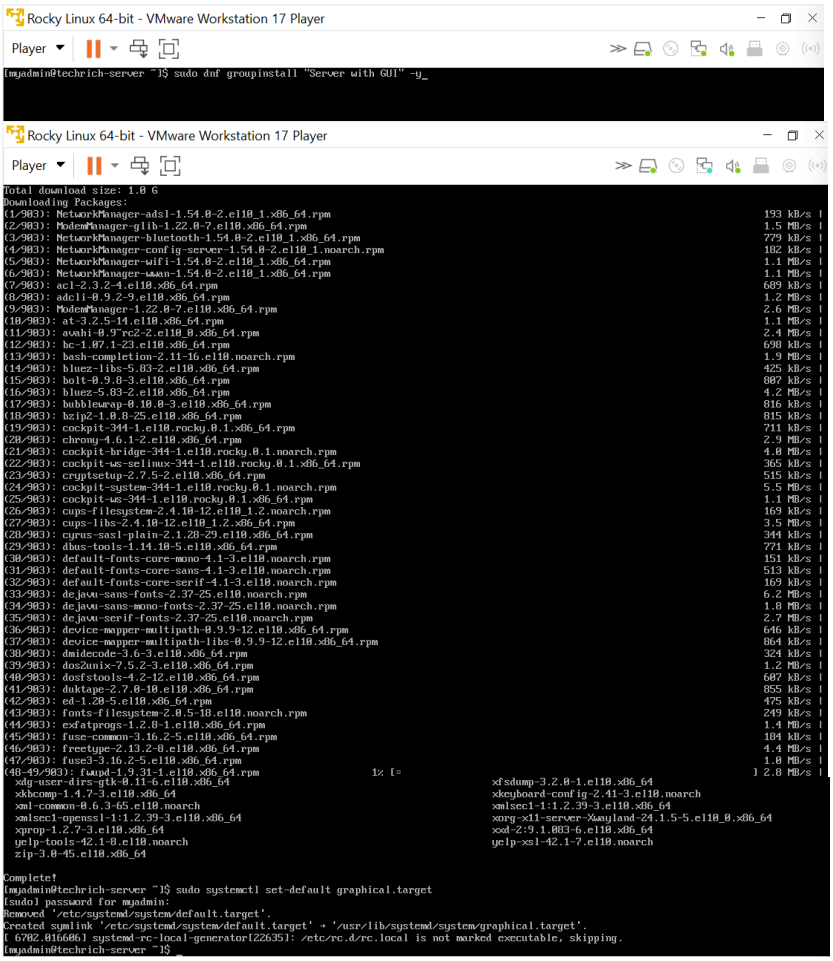




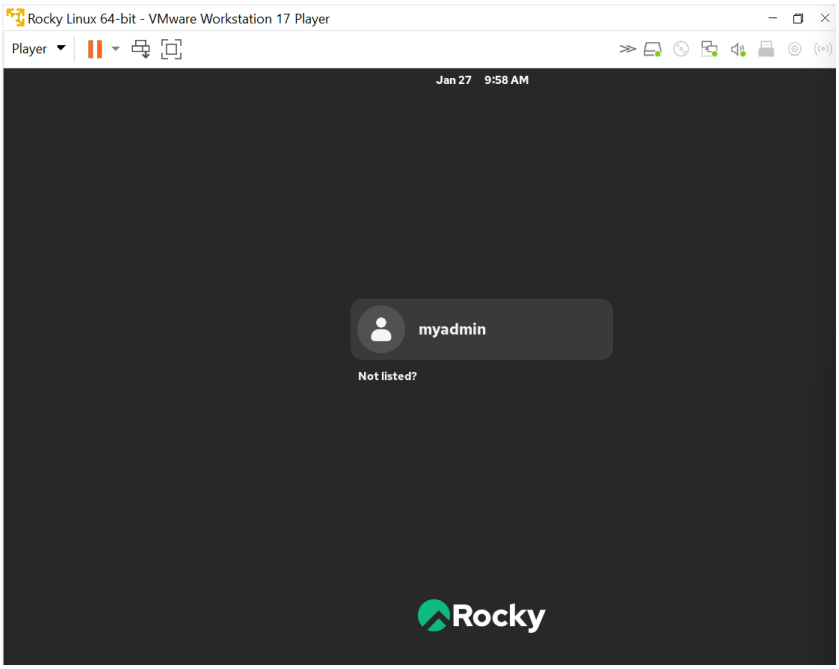
Setting network configurations



Installing GUI for Rocky Linux



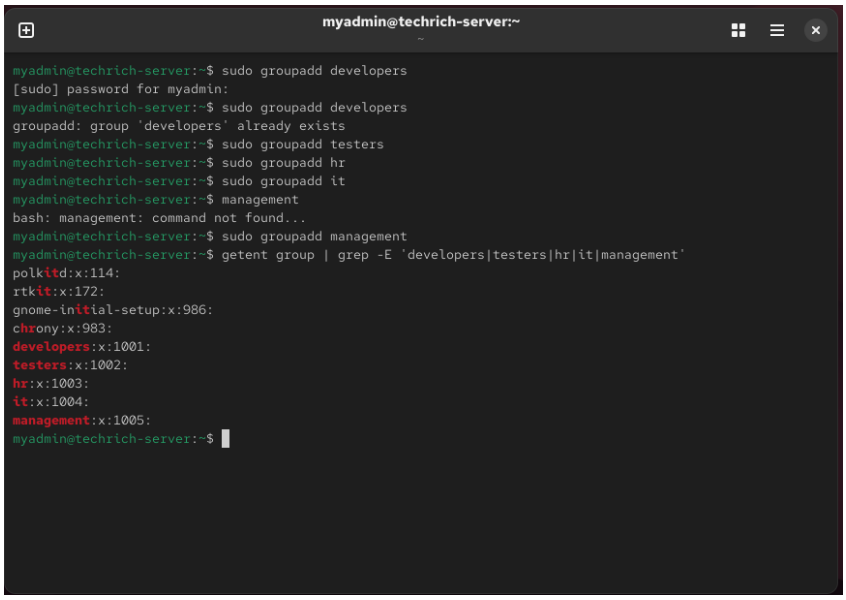
GUI Installed



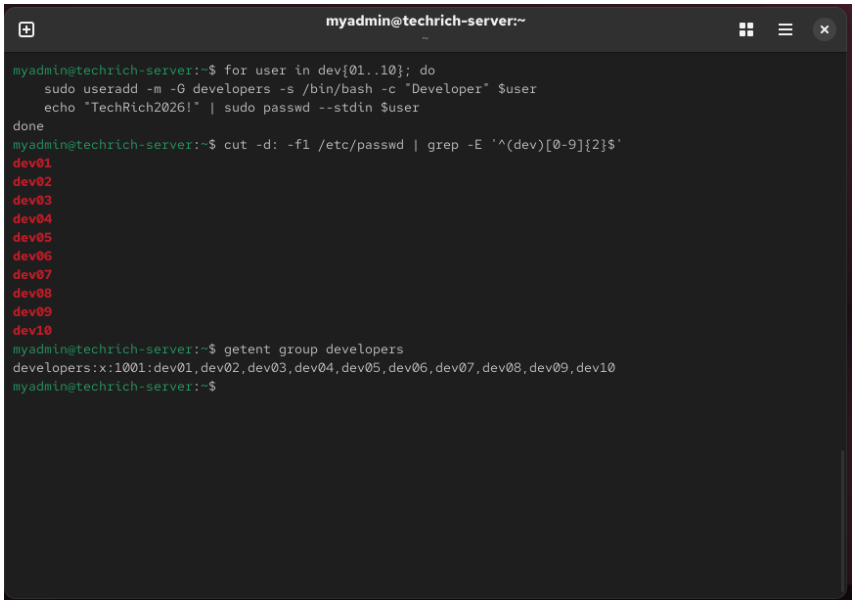
Part B

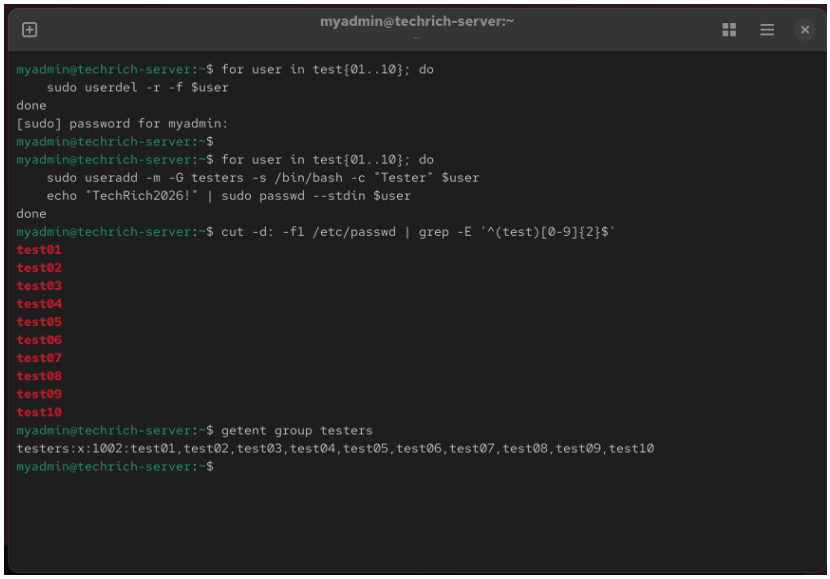
User & Group Creation

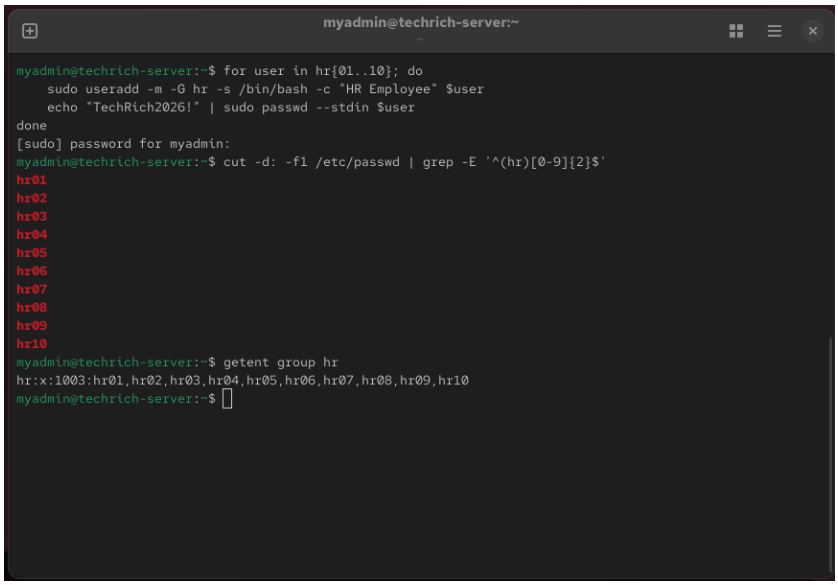
Create 5 groups for the 5 department (developers, testers, HR, IT, management)

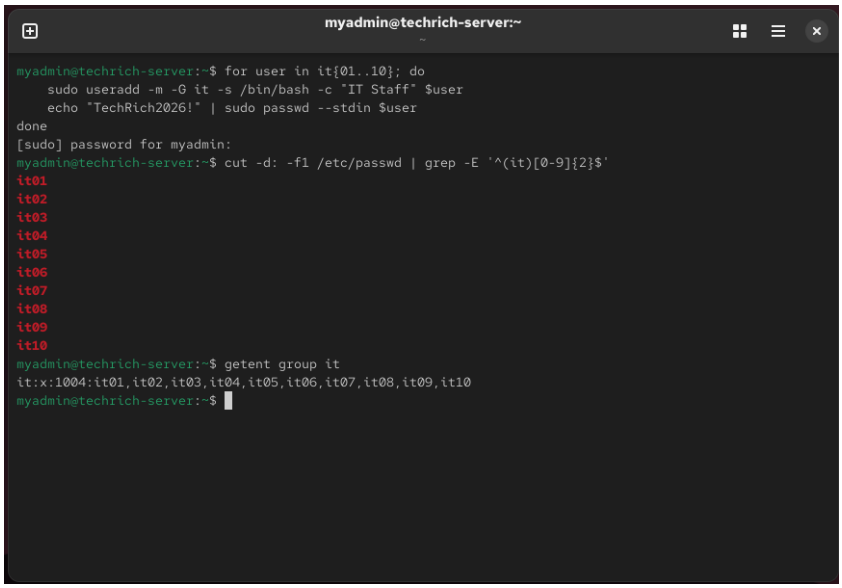


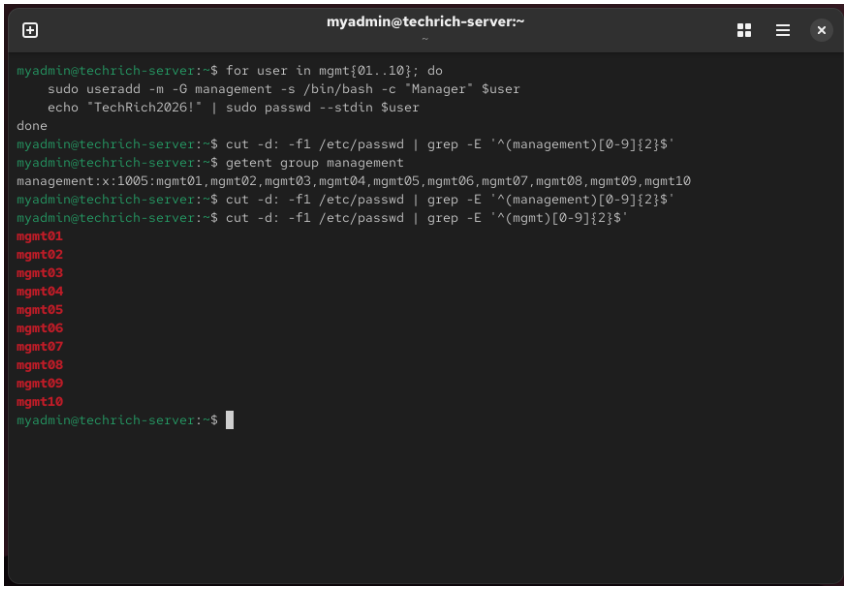
Add 10 users to each group and verify user creation, with setting default password for each user to “TechRich2026!”




myadmin@techrich-server:~
myadmin@techrich-server:~$ for user in 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:~$

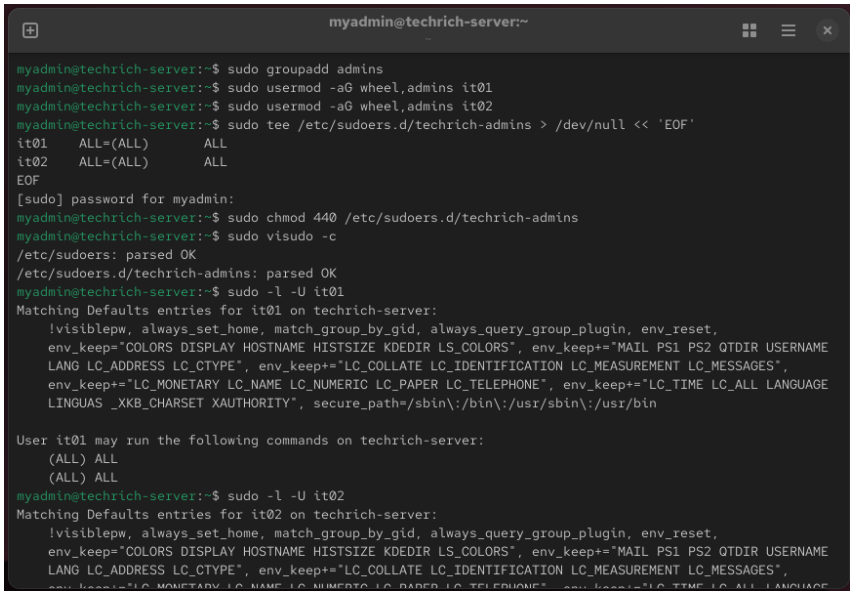

myadmin@techrich-server:~
myadmin@techrich-server:~$ for user in hr{01..10}; do
sudo useradd -m -G hr -s /bin/bash -c "HR Employee" $user
echo "TechRich2026!" | sudo passwd --stdin $user
done
[sudo] password for myadmin:
myadmin@techrich-server:~$ cut -d: -f1 /etc/passwd | grep -E '^(hr)[0-9]{2}$'
hr01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



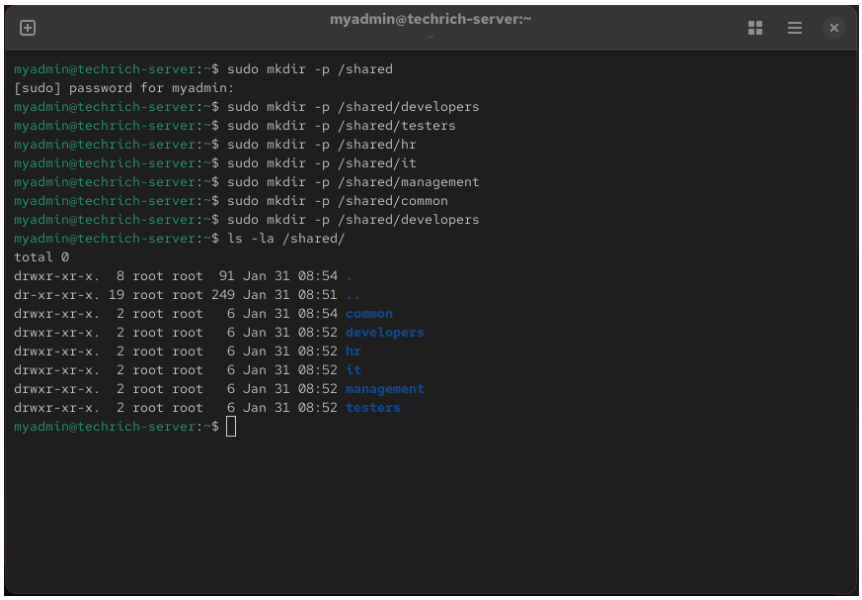
Role-Based Access Control

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.

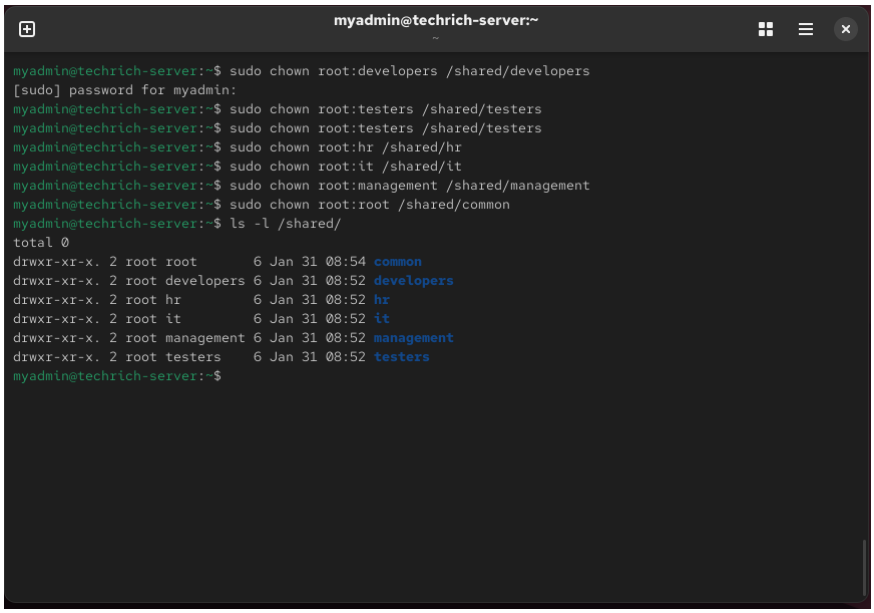


File & Directory Permissions

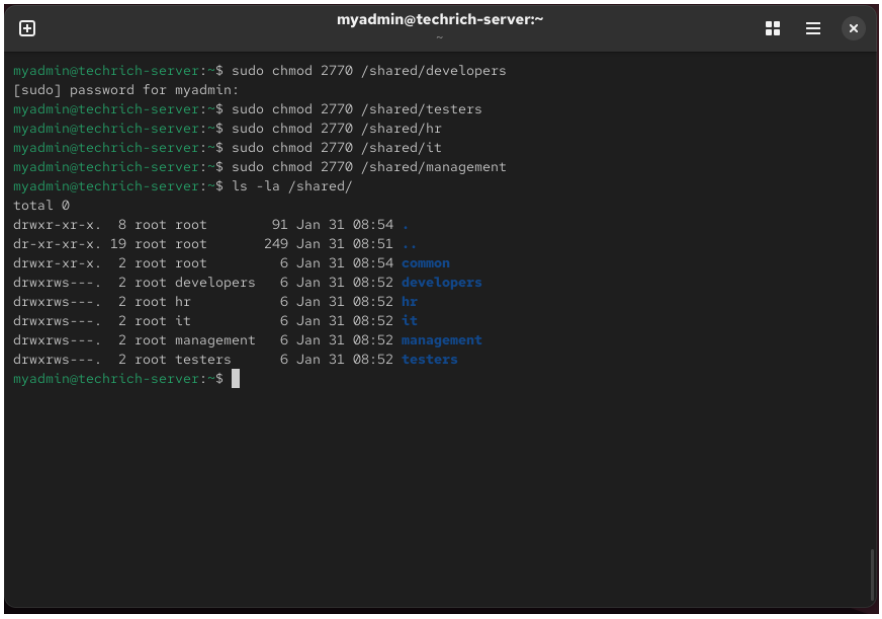
Create a shared file directory with separate subdirectories for



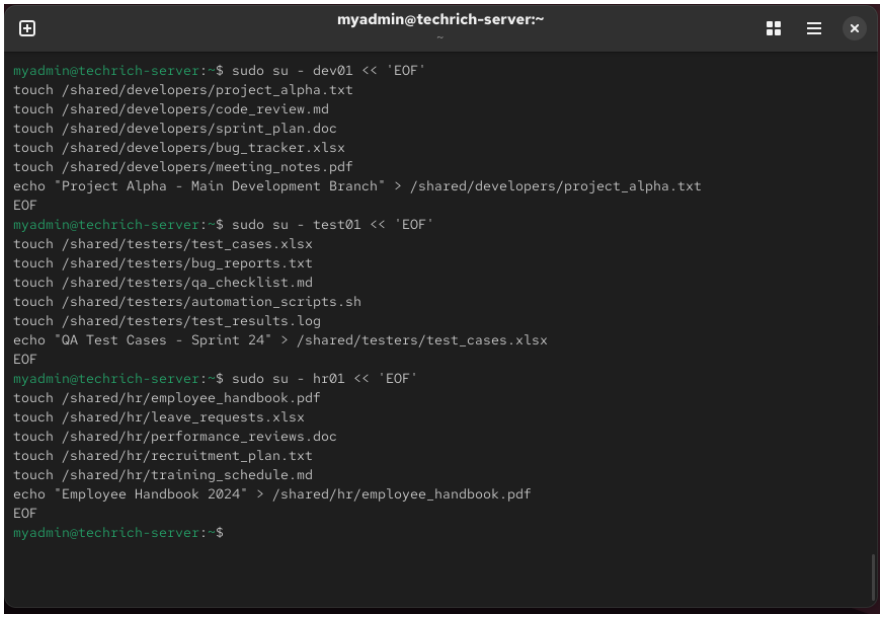
change the ownership of each directory to its group

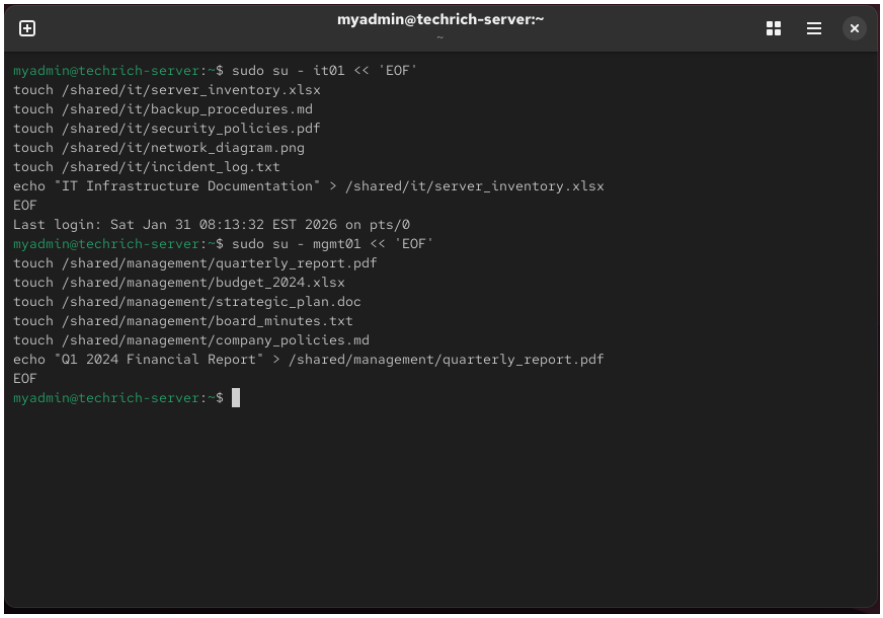


change the permission of each group directory to ensure that each file created in the directory inherit the group ownership and only the group

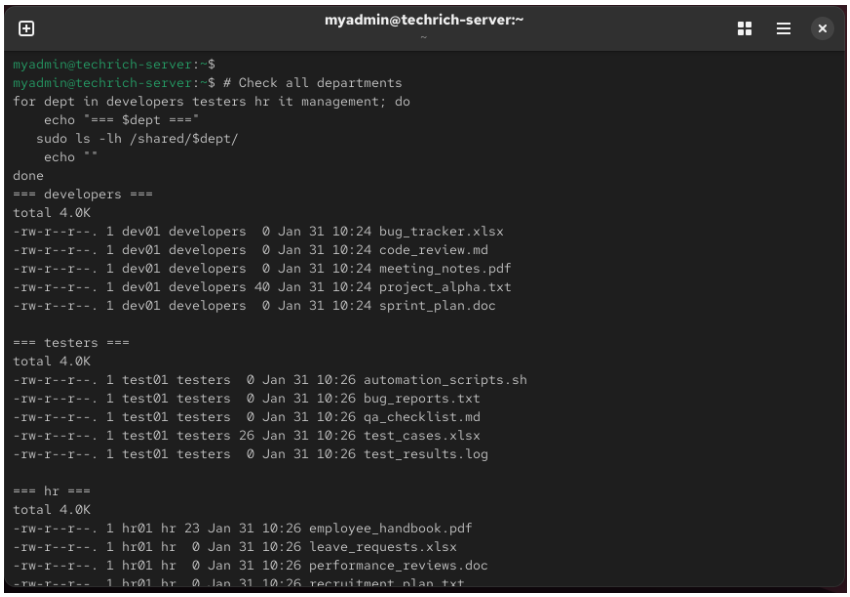


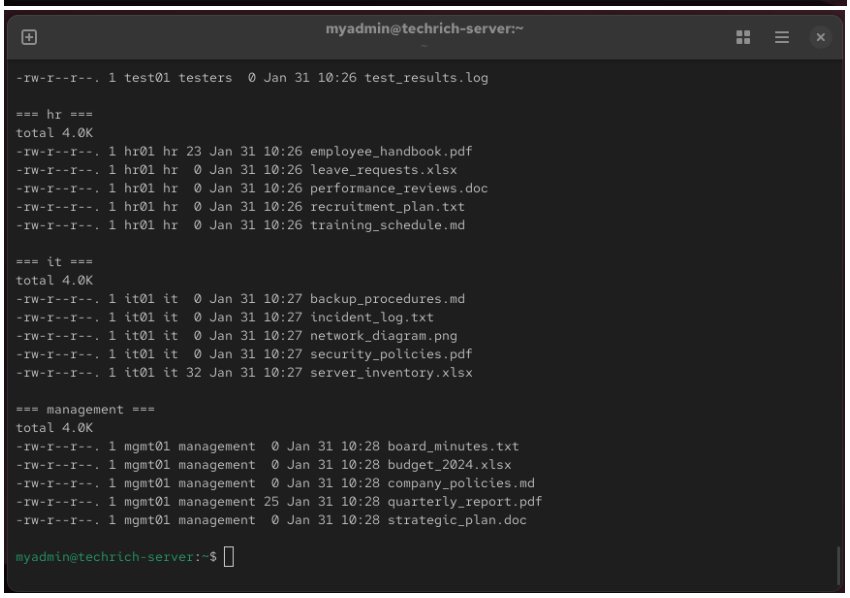
create sample files in each department directory





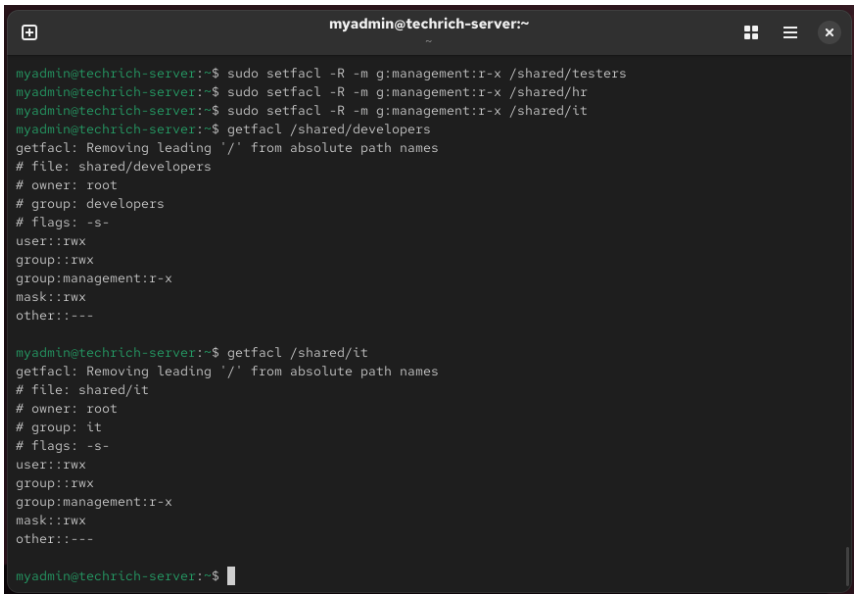
verifying department files, by listing all the files with ownership and permissions



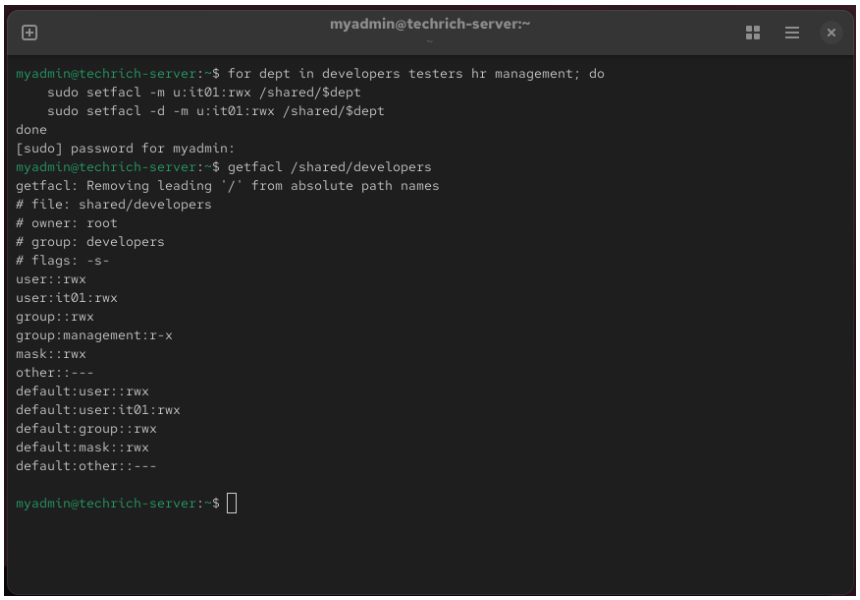


ACL Implementation

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.



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

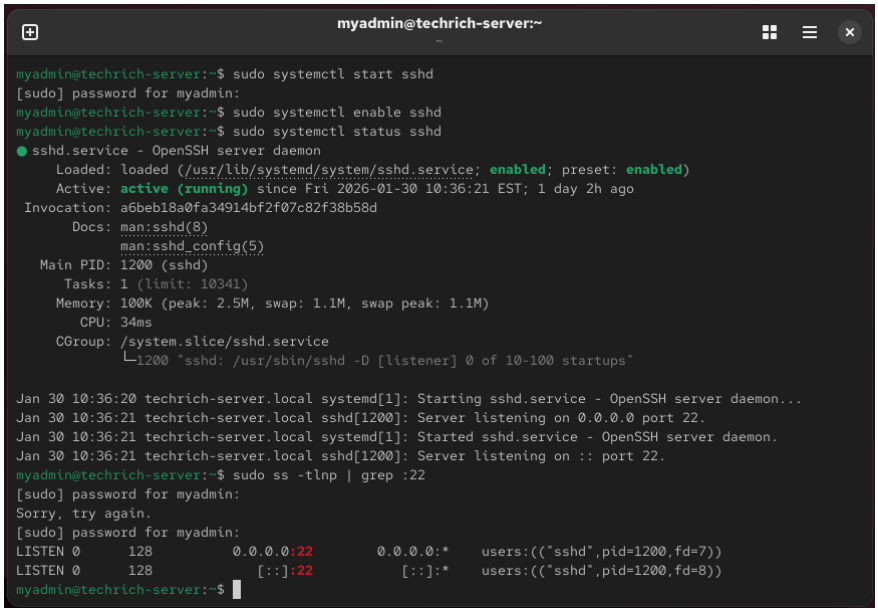


Security Explanation

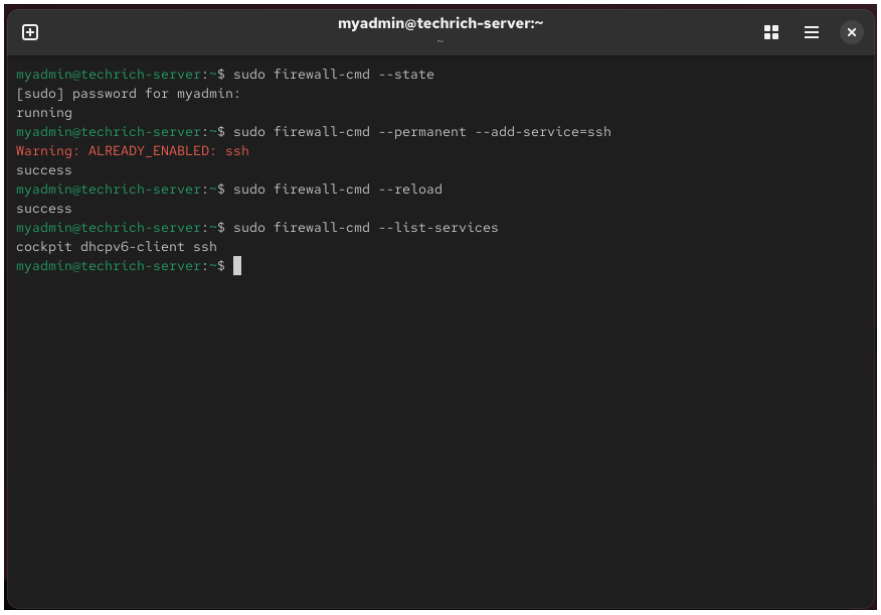
Linux permissions control what actions (read, write, execute) a user can perform on files and folders (Stallings, 2022). Group ownership allows access to be assigned by role. ACLs add extra access rules for specific users when the basic permissions and groups aren't enough (SUSE, 2023). Together, they 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

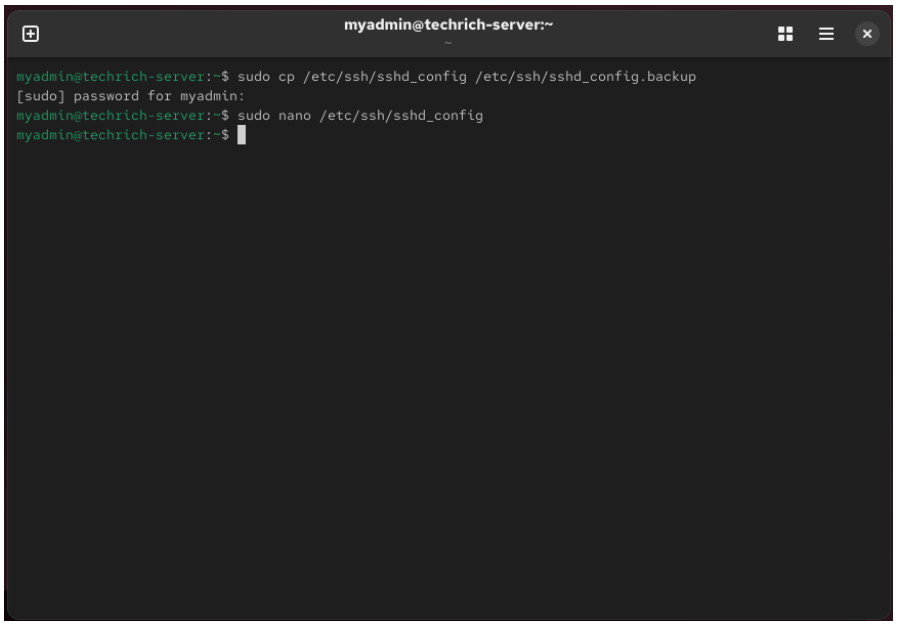
Start and enable SSH service



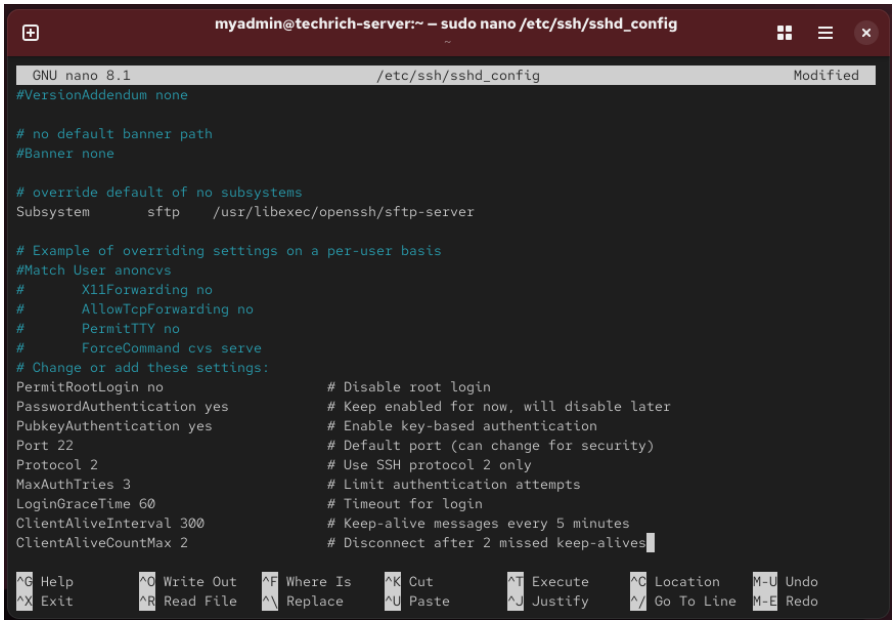
Configure SSH firewall



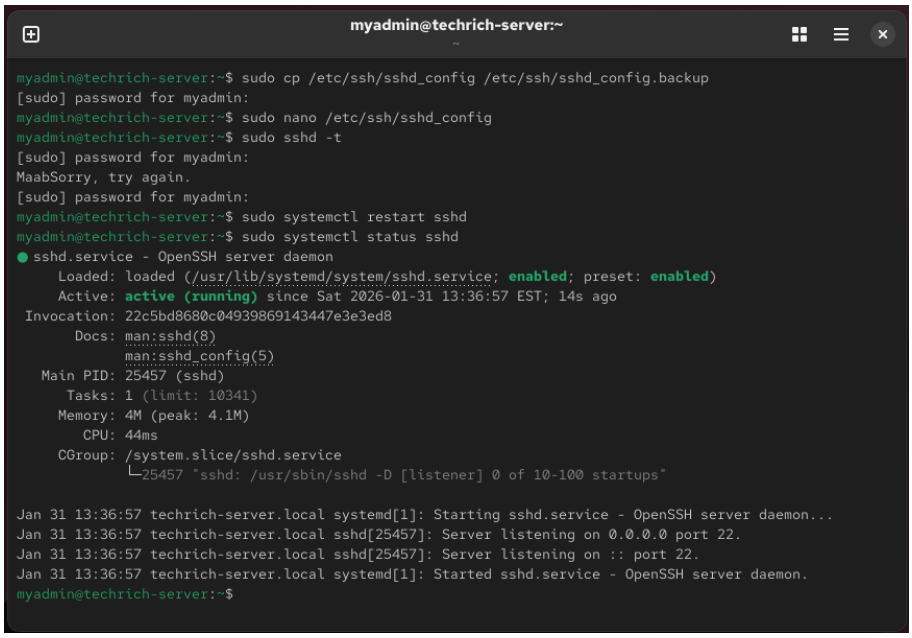
Backing up the original sshd configuration before editting



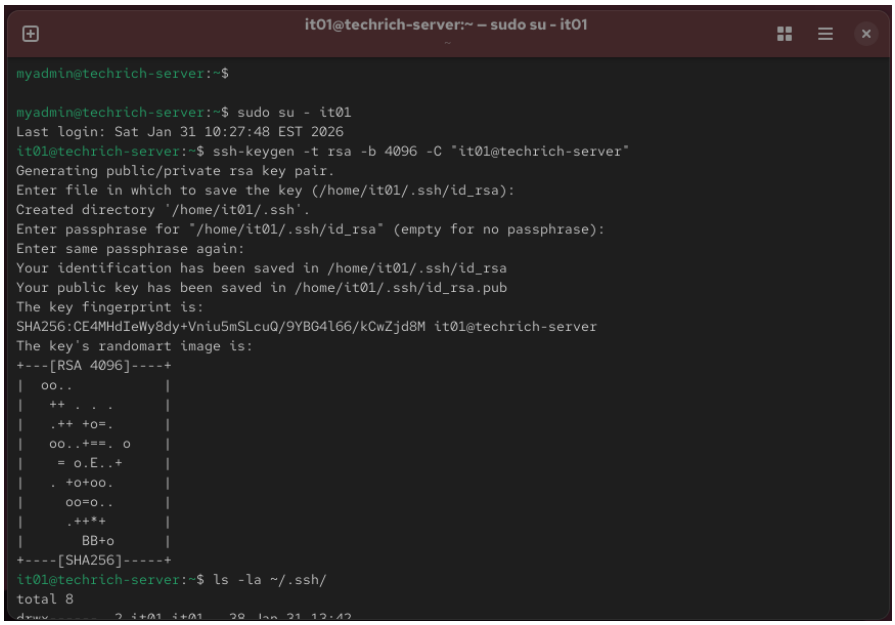
Editing sshd configuration and confirming security hardening (disable root login, enable key authentication, … etc).

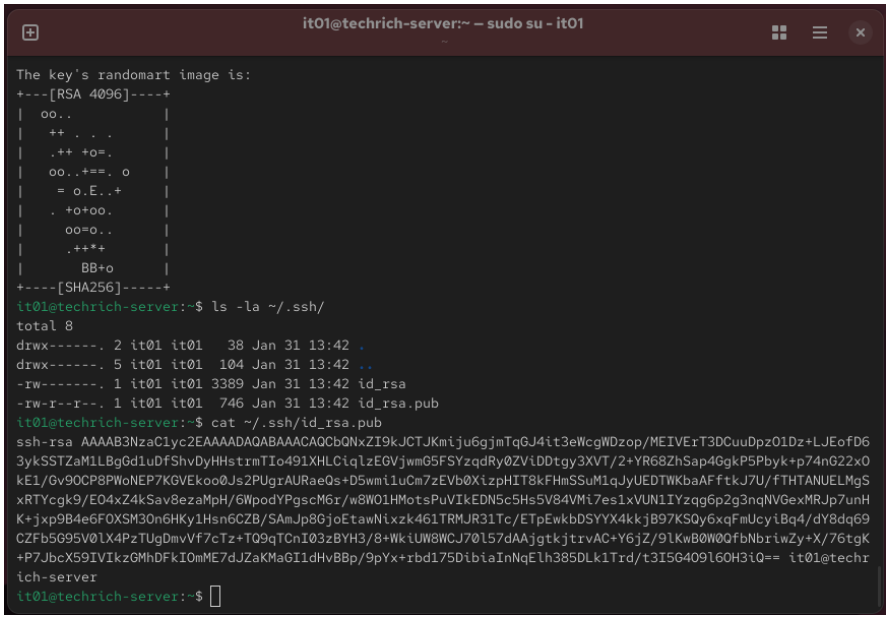


Restart SSH and confirming it’s enabled

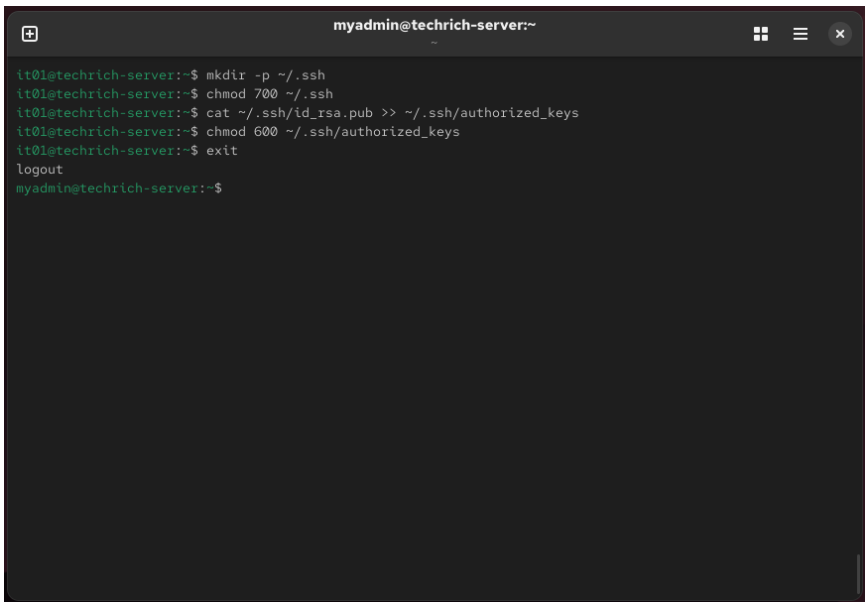


Create SSH key pair for admin it01

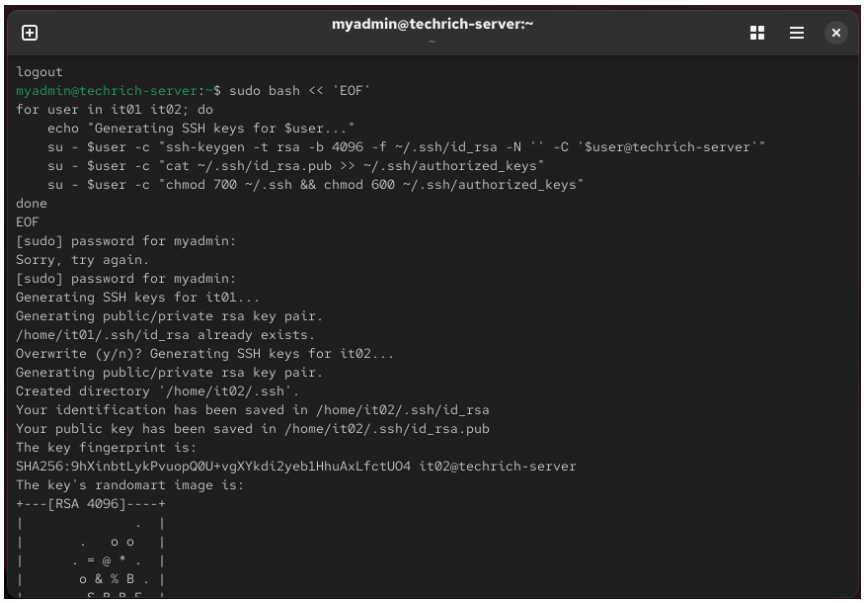




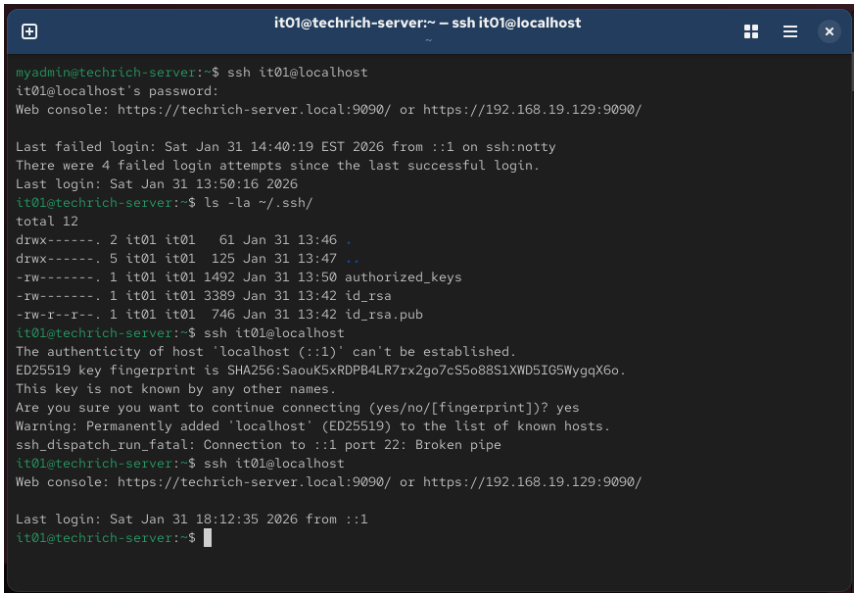
Copy it01 public key and setting the permissions

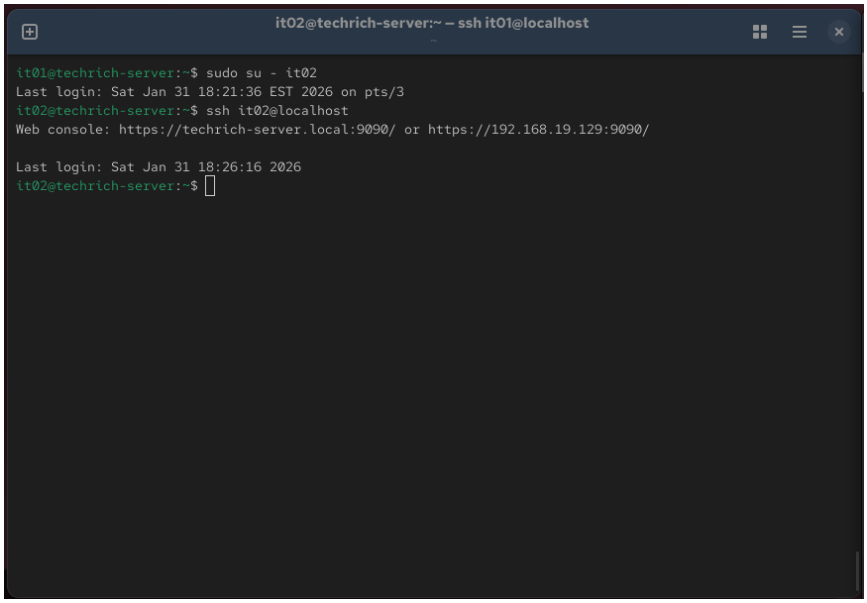


Create SSH key pair for it02 admin

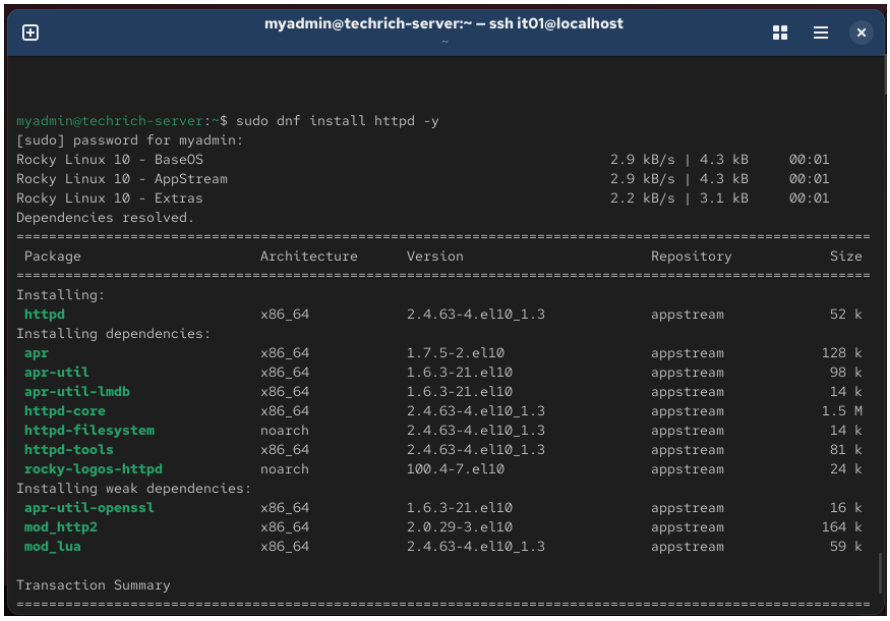


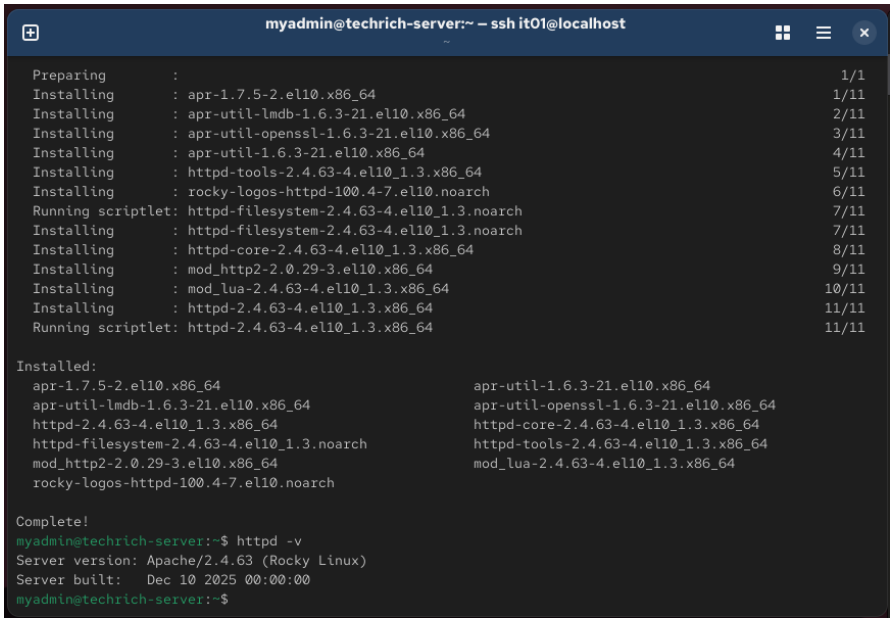
Test SSH login as it01 and it02 and ensure that the key based authentication is successful for both



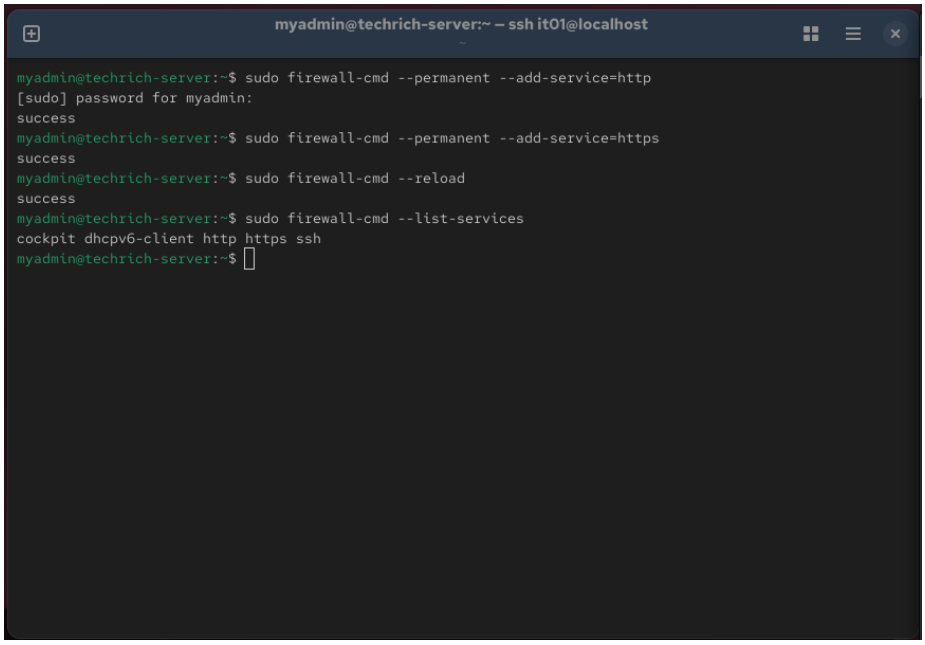


Install Apache (httpd) and confirming the installation

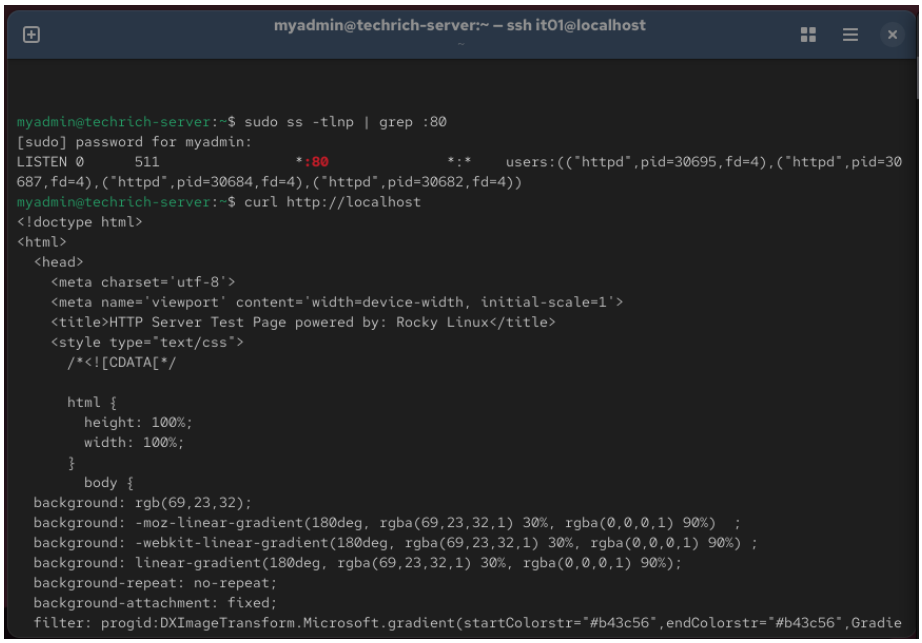




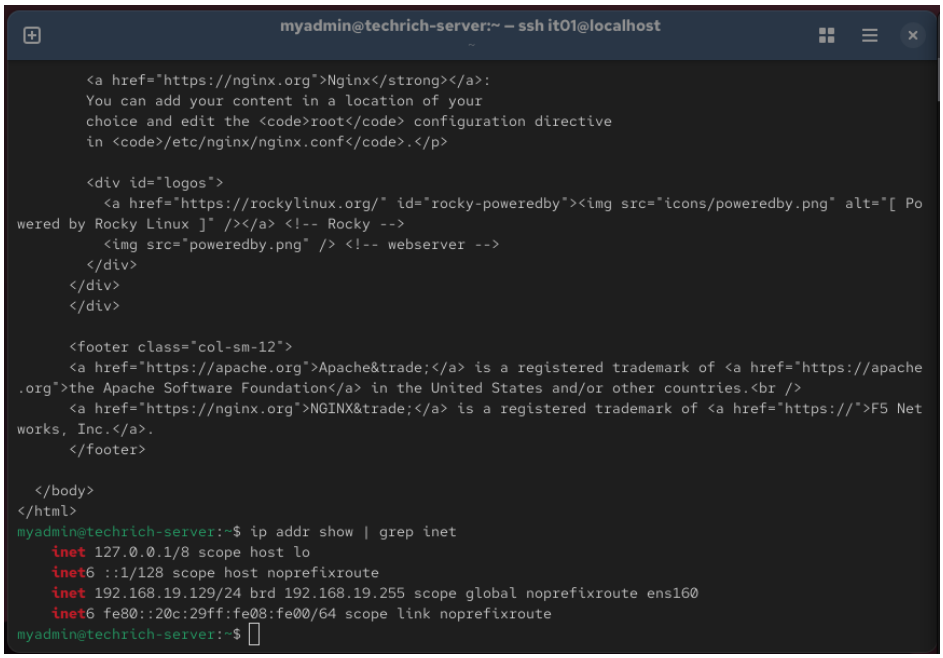
Configuring HTTP/HTTPS firewalls



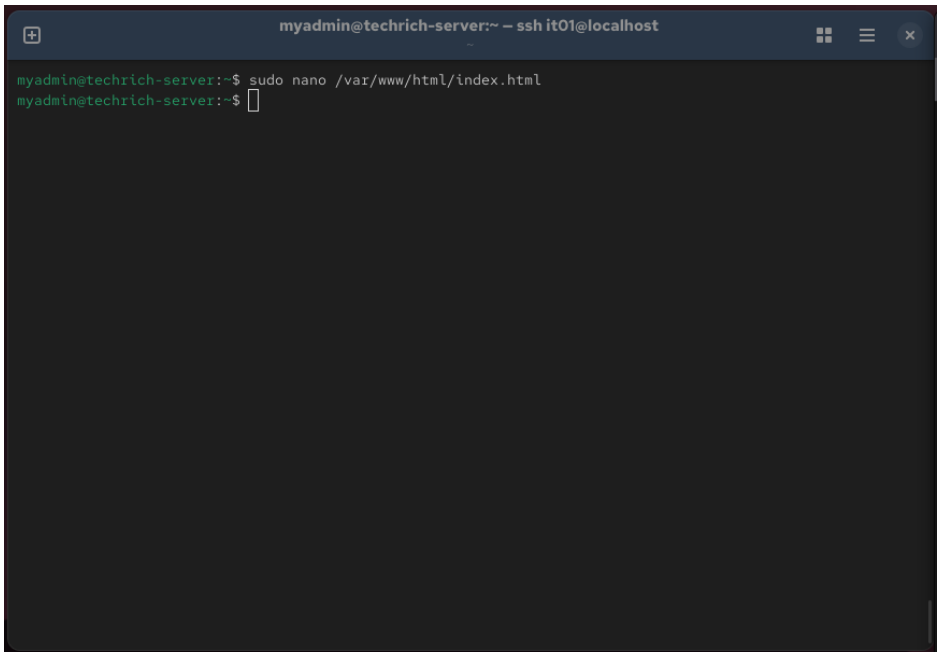
Confirming port 80 is listening and retrieve the default html test page



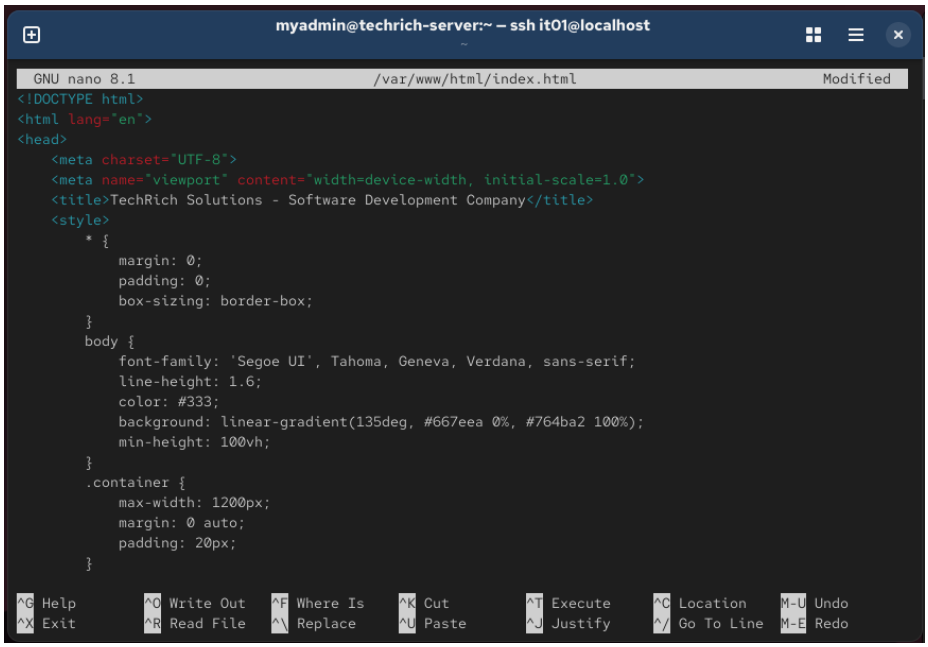
Verify the server ip address with ip addr show



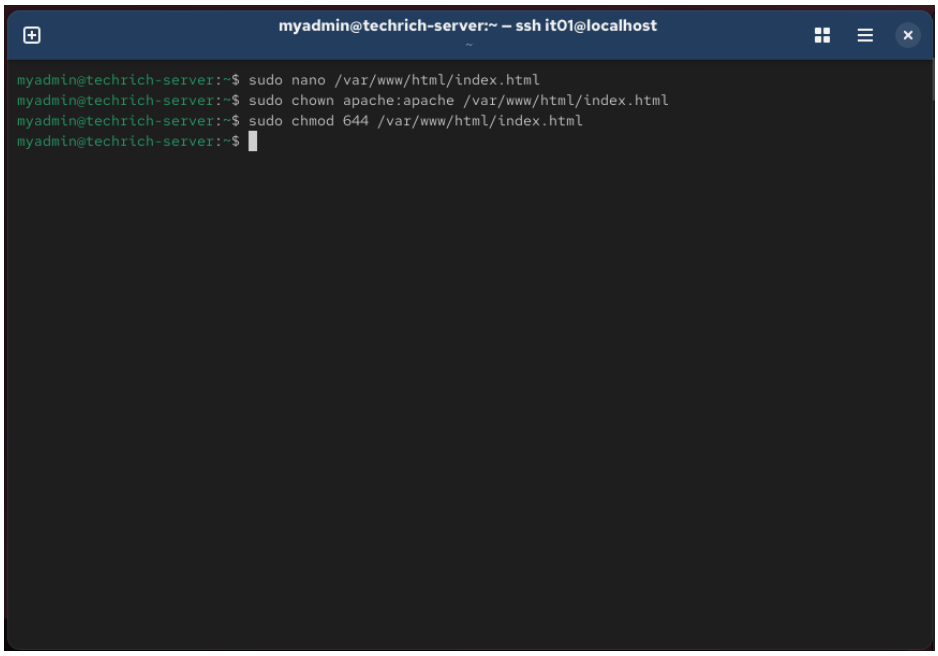
Open index.html for editing using nano and replace the default file



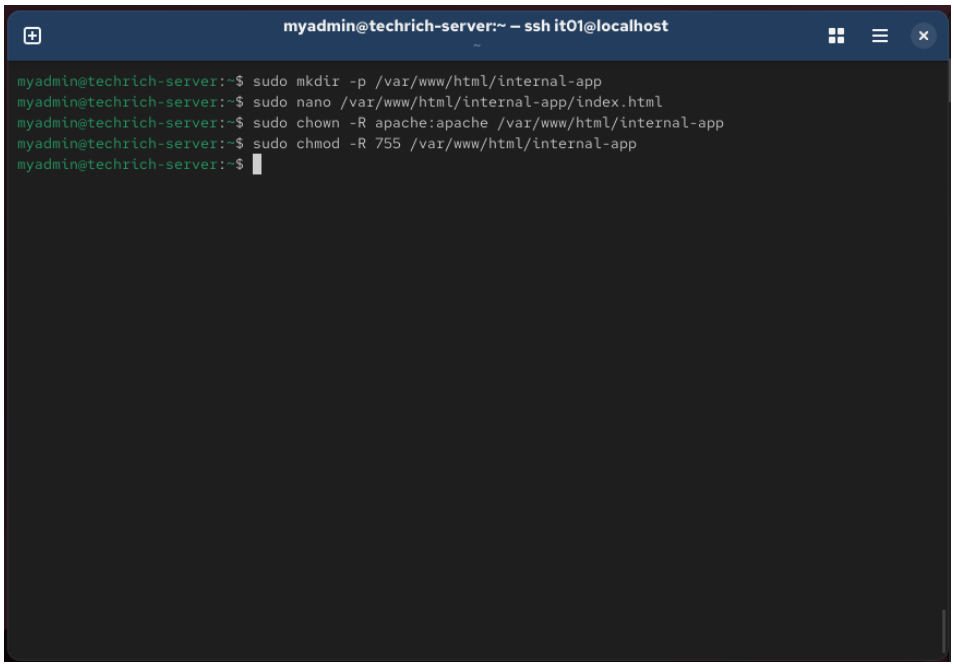
Edit on the file to create the company website

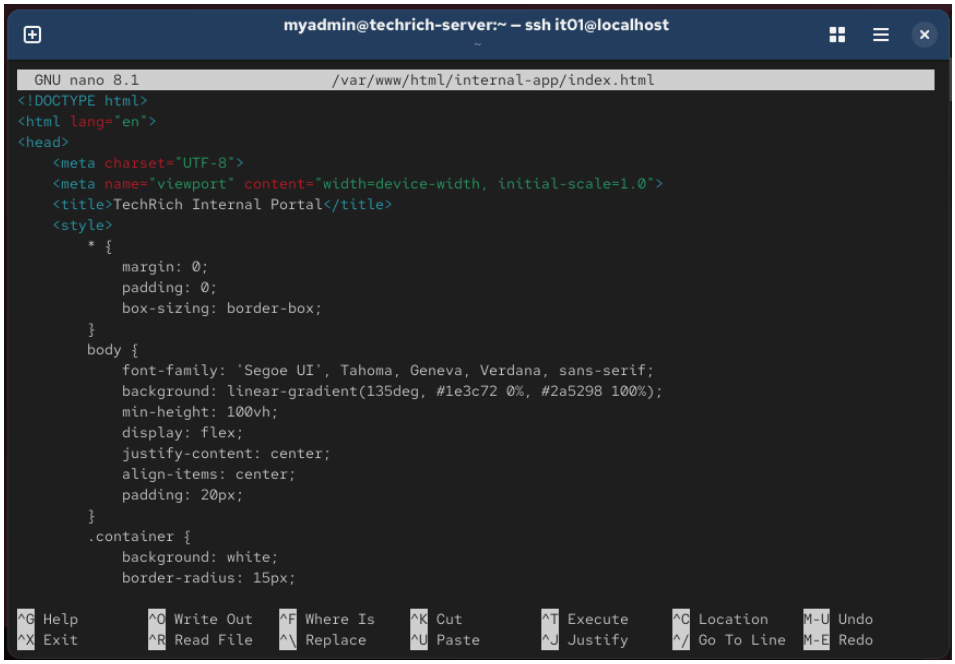


setting ownership and permissions

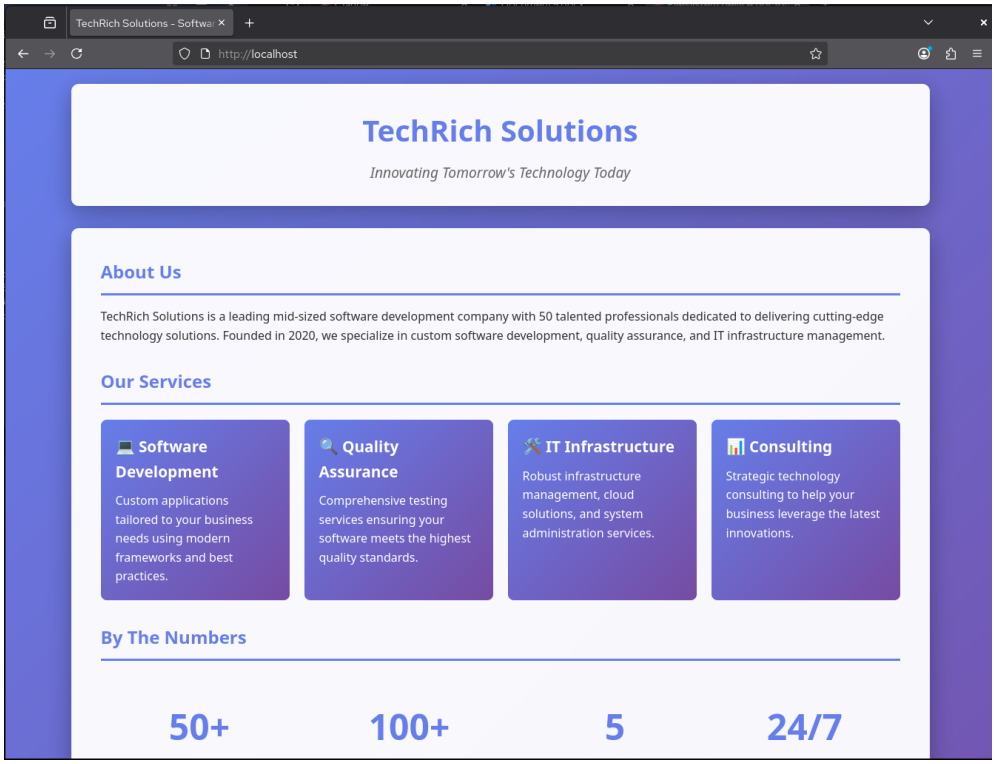


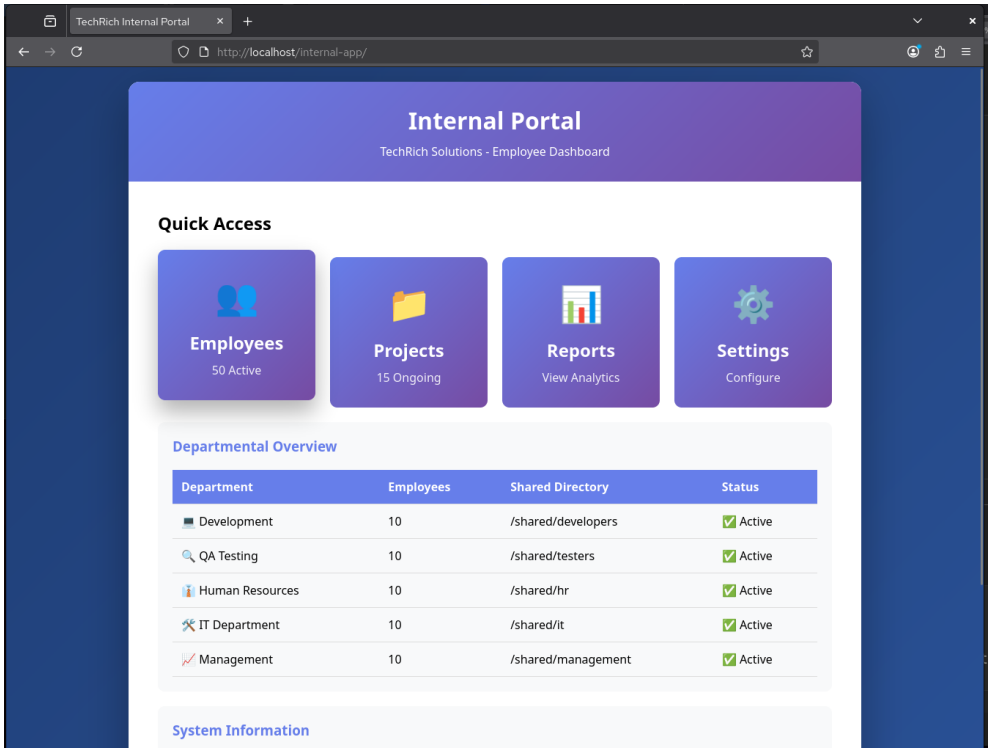
create internal portal website





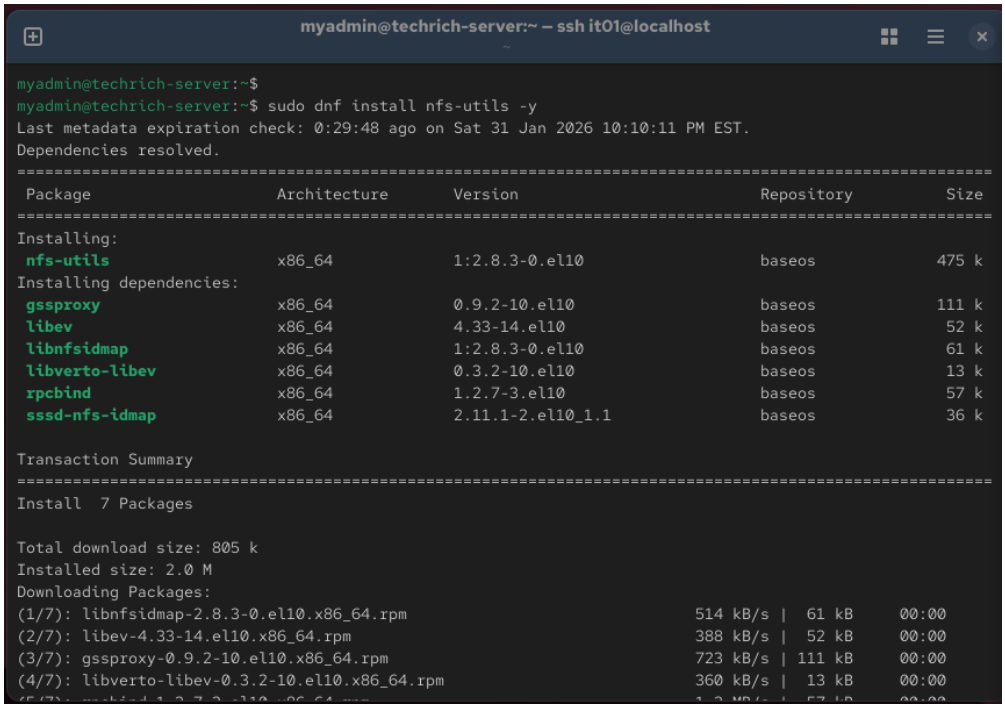
ensuring both websites were created successfully by opening both in the browser



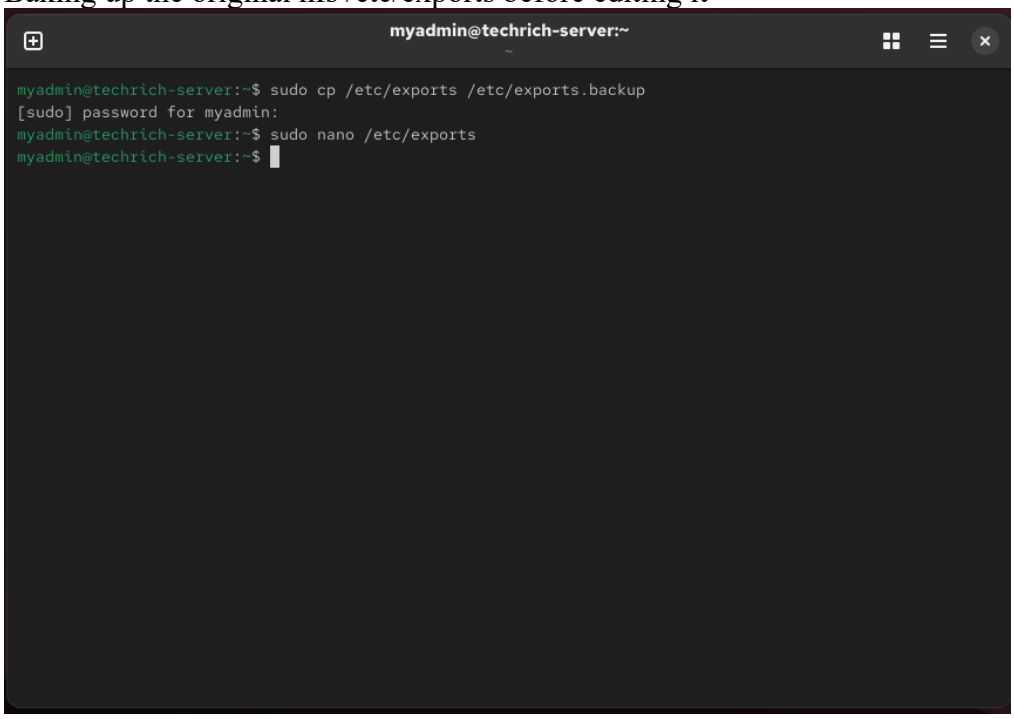


NFS

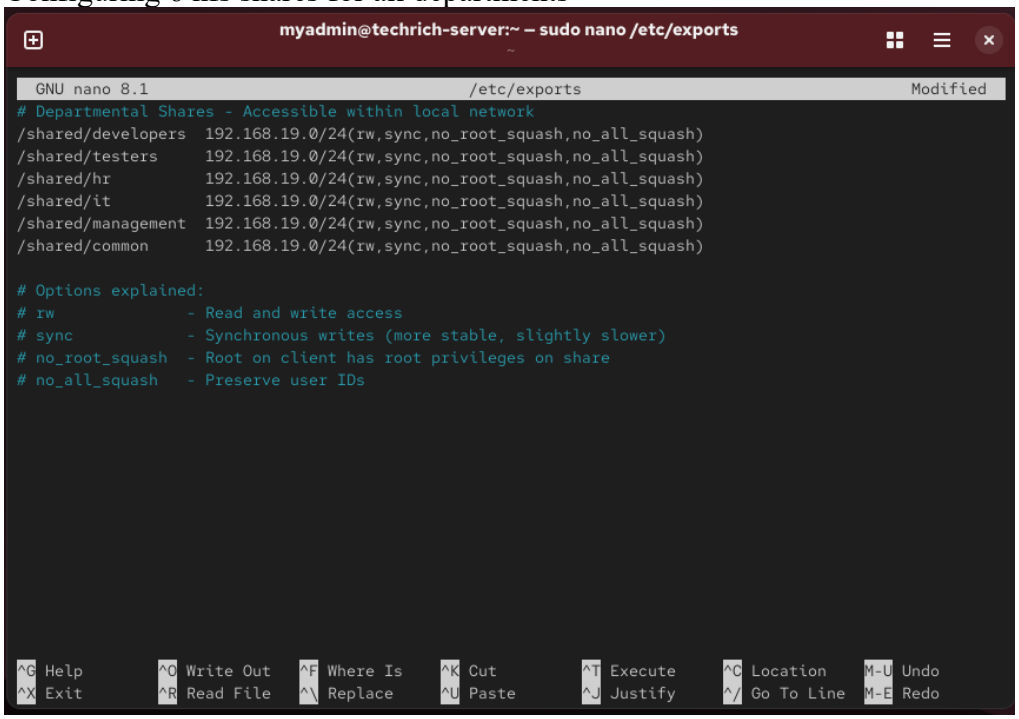
Installing NFS service and starting and enabling it



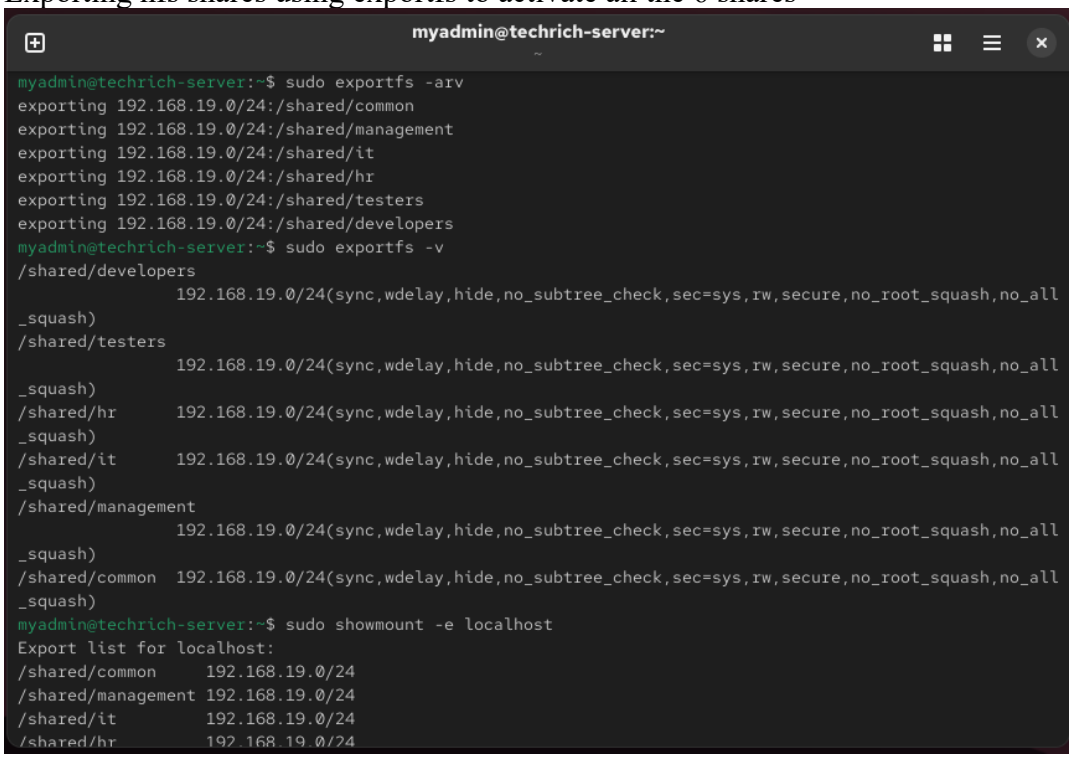
Baking up the original nfs /etc/exports before editing it



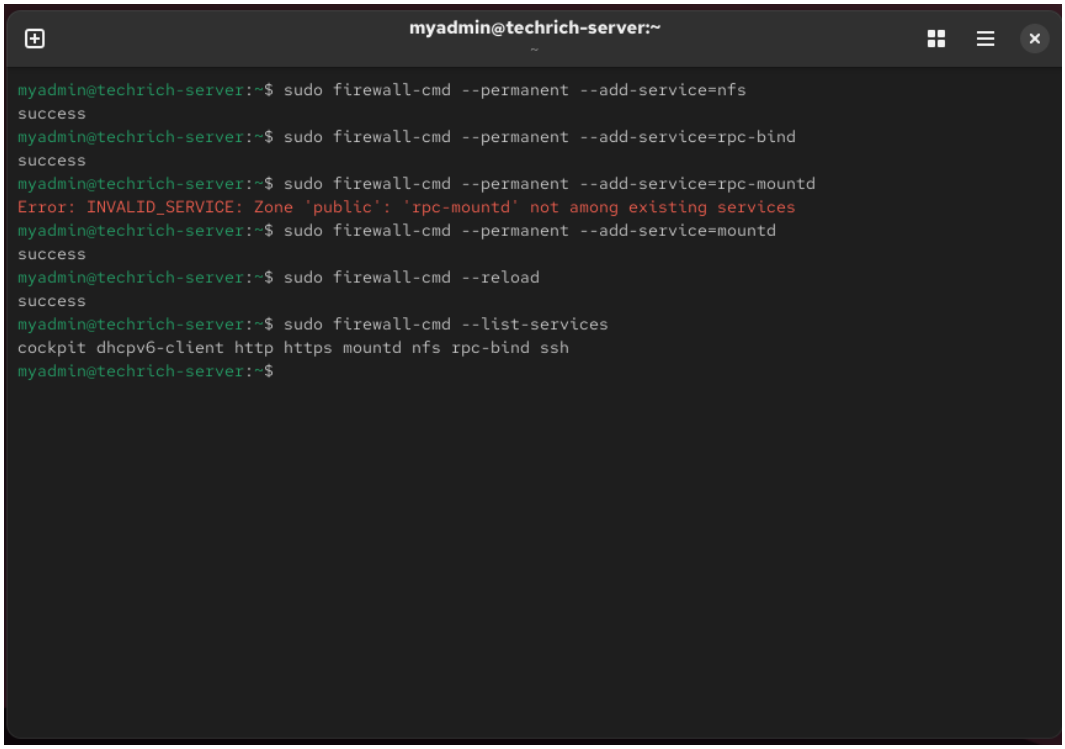
Configuring 6 nfs shares for all departments



Exporting nfs shares using exportfs to activate all the 6 shares

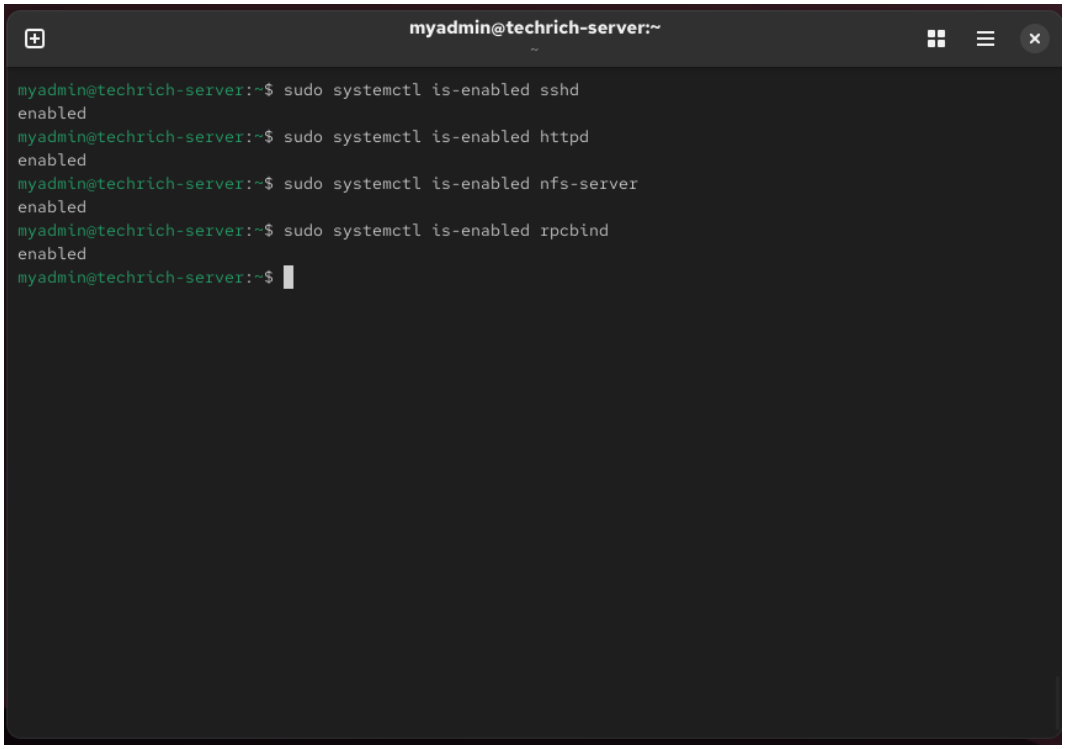


Configuring nfs firewall adding services: nfs, rpc-bind, mountd, reloading and ensuring that the services were allowed

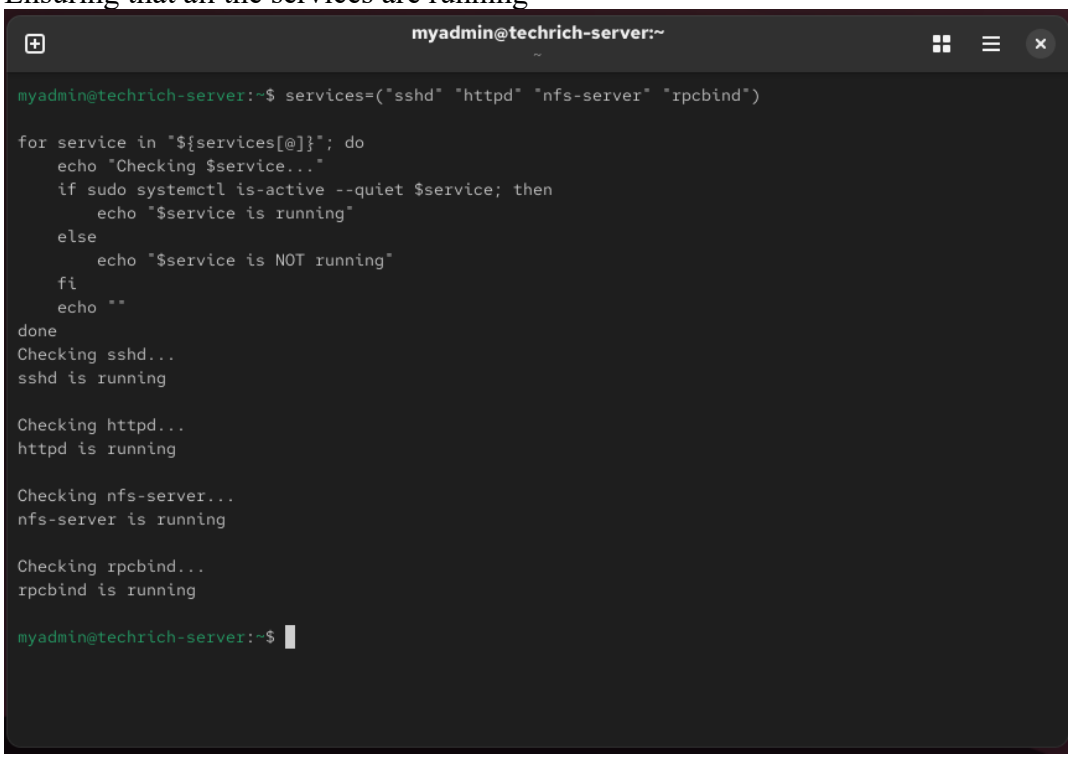


Verification

Ensuring that all the services are enabled



Ensuring that all the services are running



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).

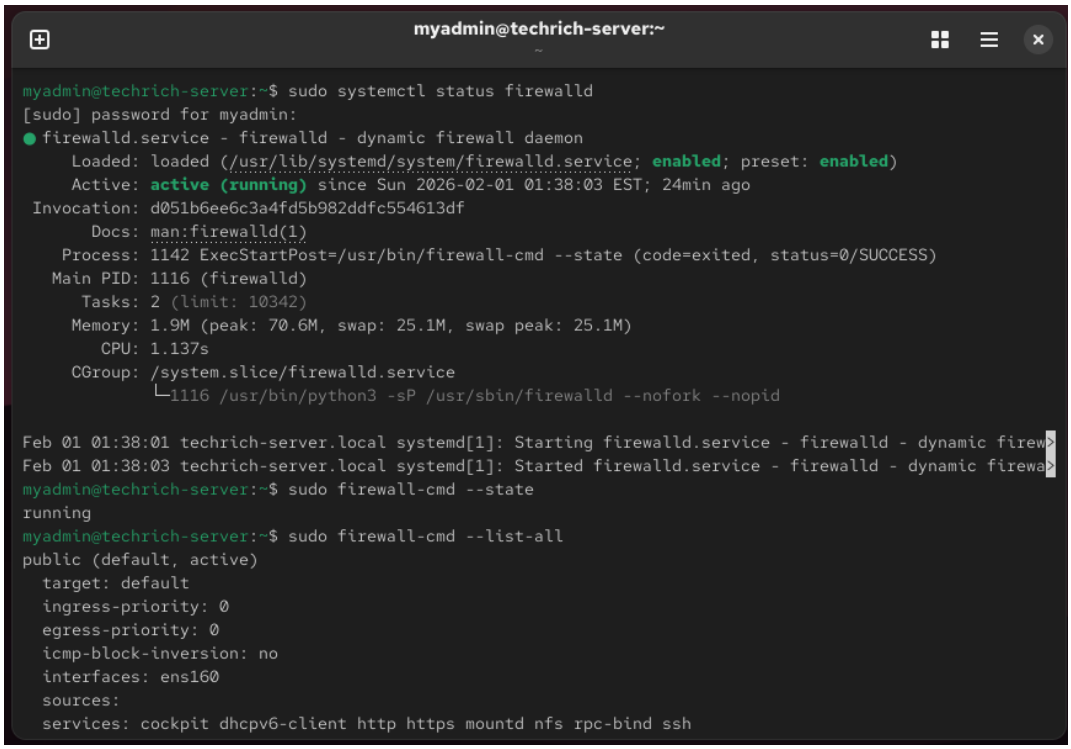
NFS (Network File System)

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).

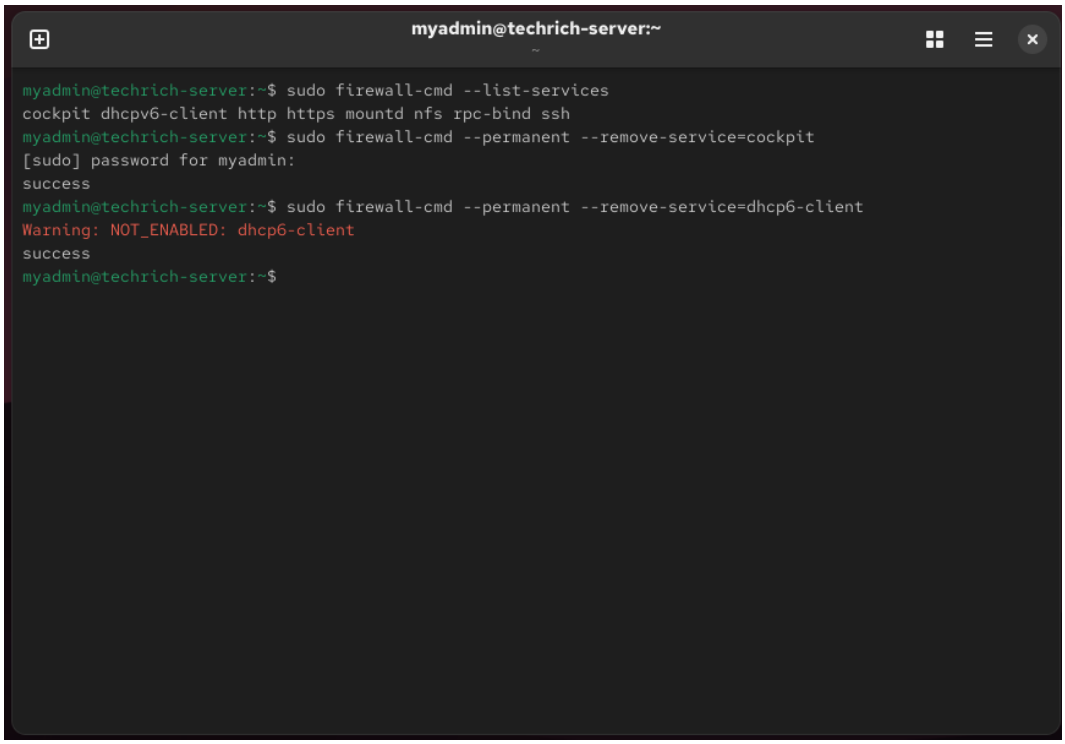
Task D

Firewall

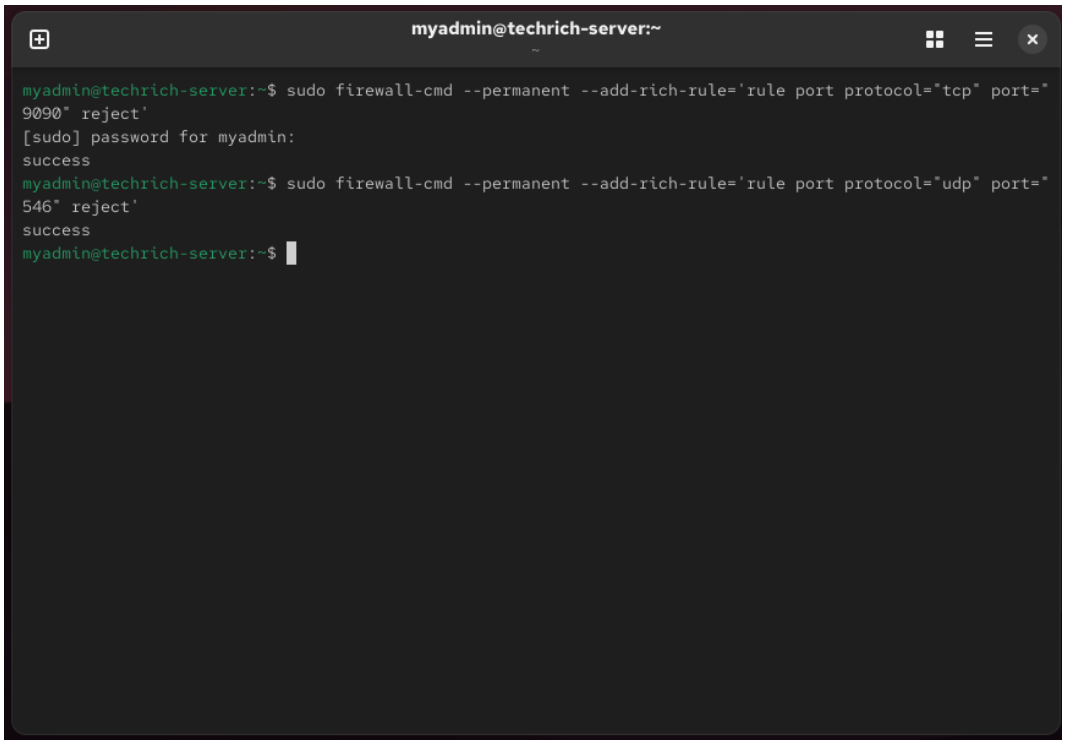
Ensure firewalld is enabeled and running



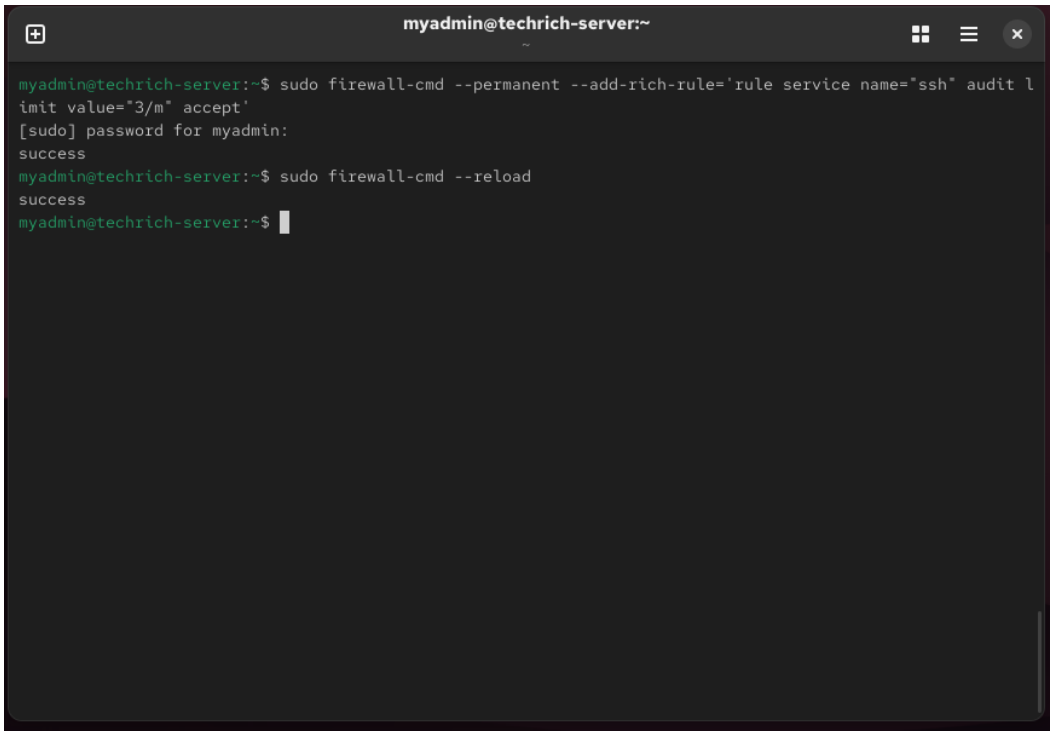
List the currently allowed services and block the non-essential services (cockpit, dhcpv6-client)



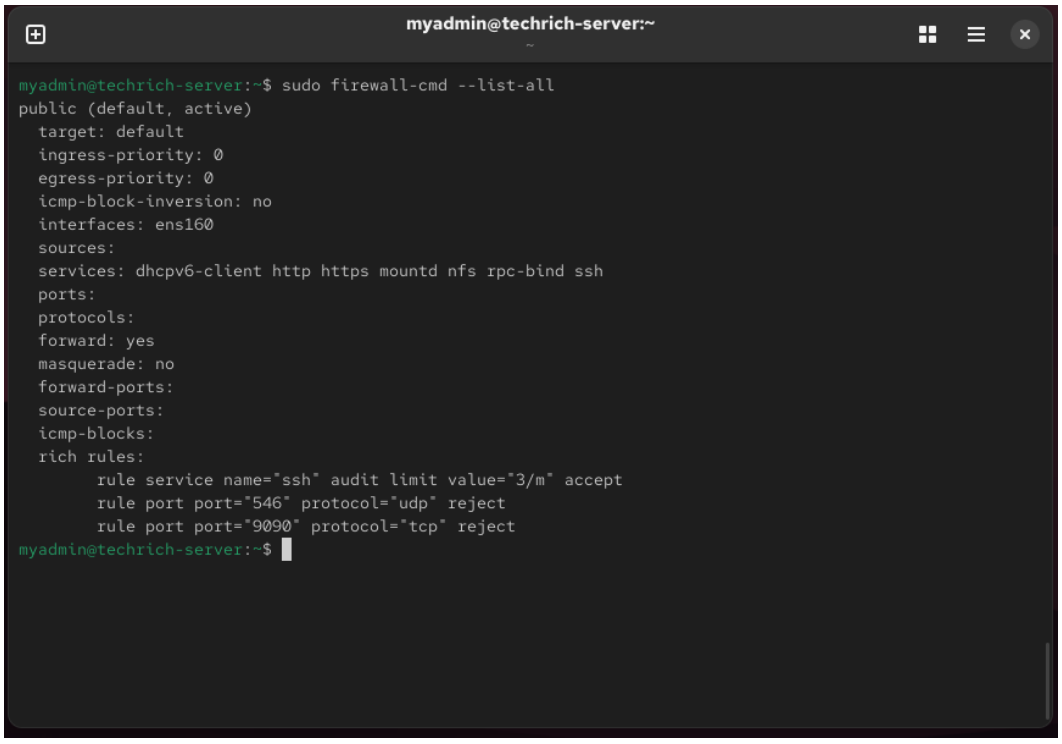
Block the ports of the non-essential services

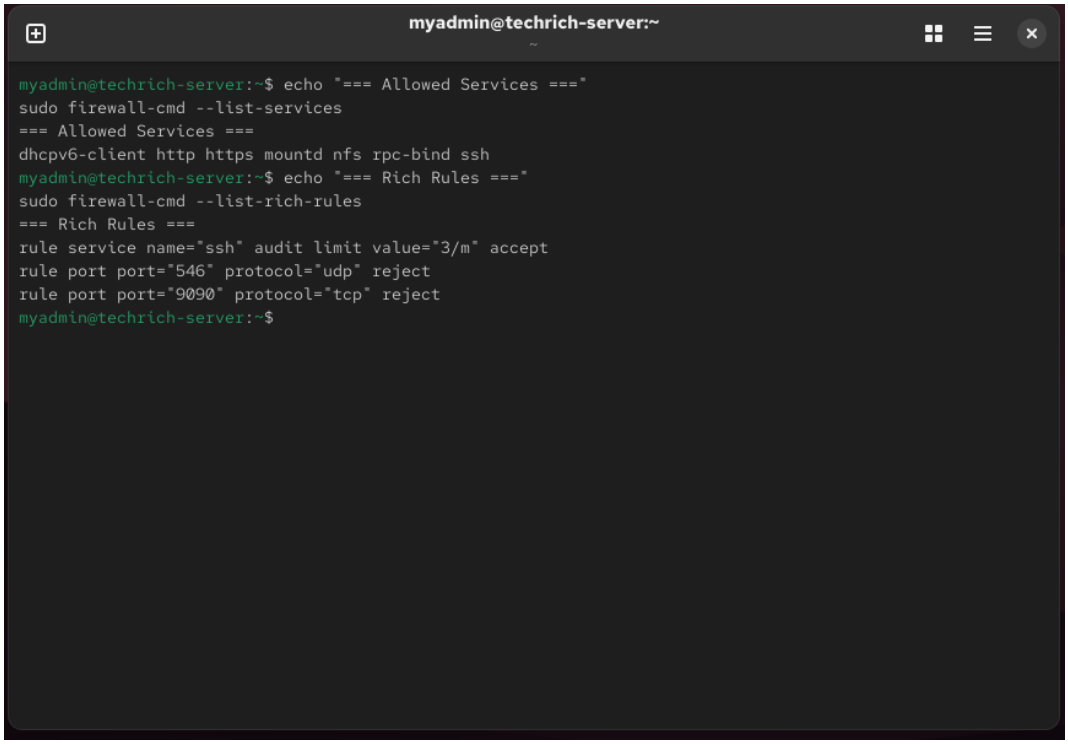


Limit ssh connection to 3 attempts per minute per ip



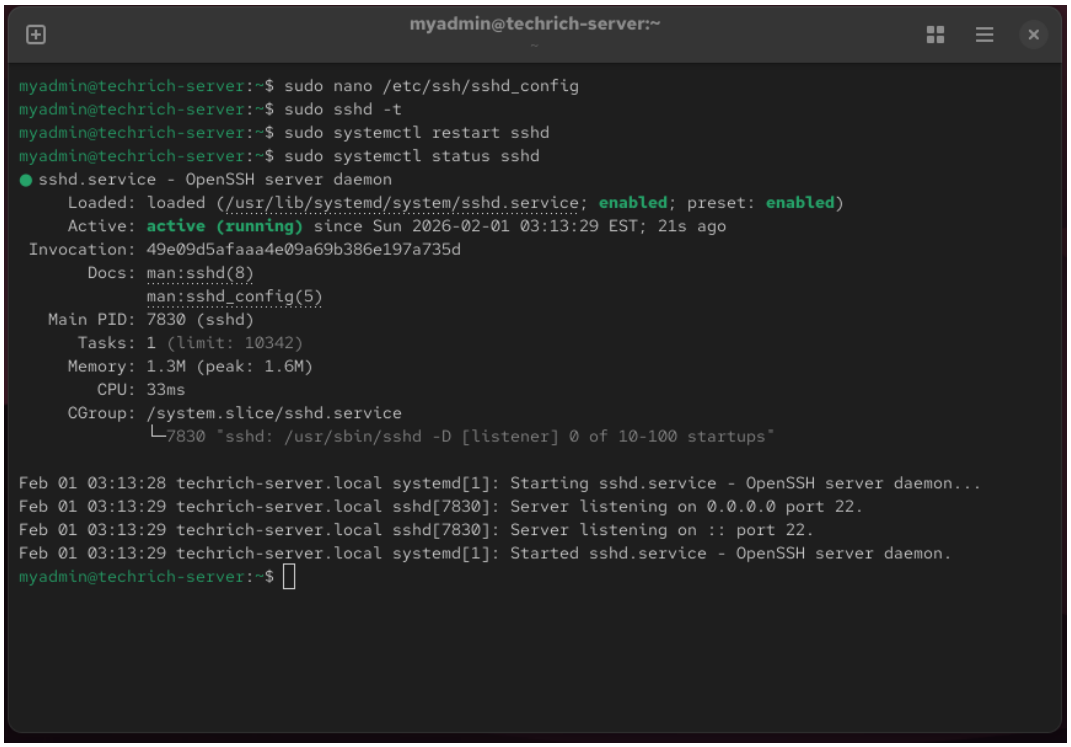
Final verification : verify allowed services, allowed ports and rich rules



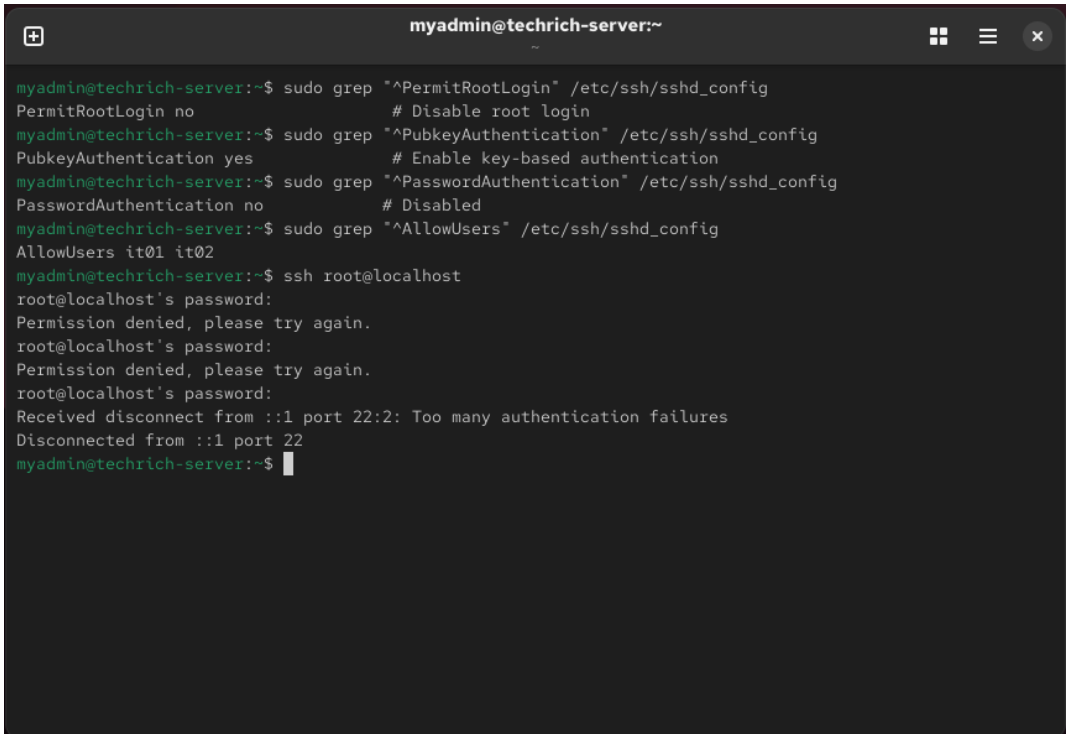


SSH Hardening

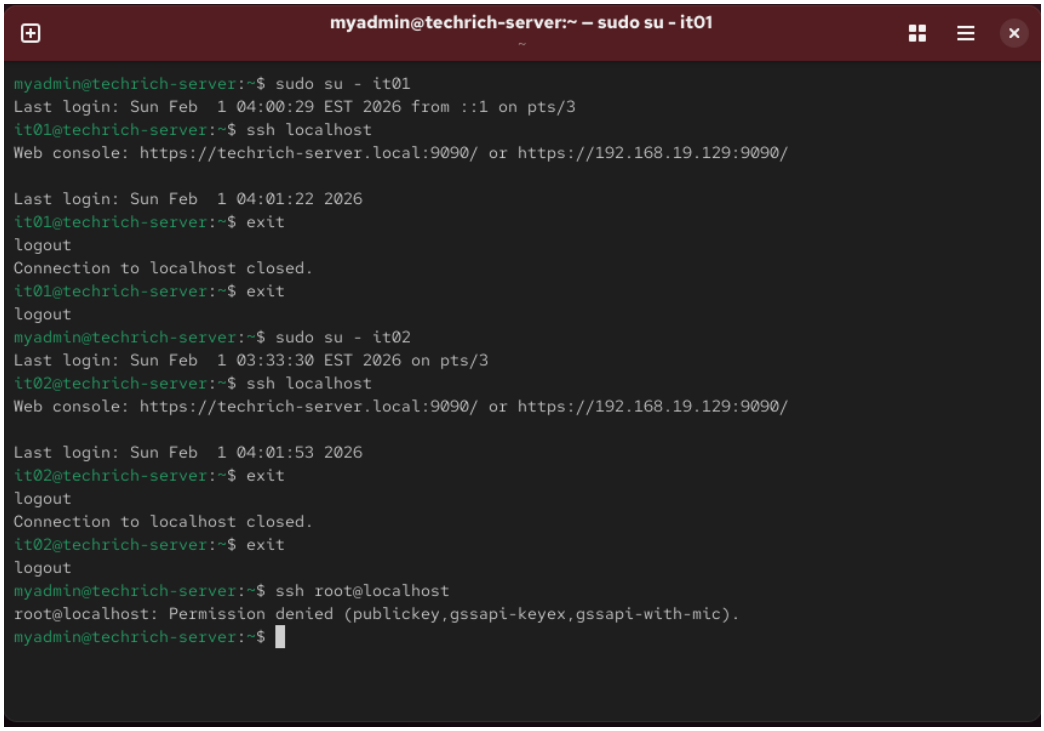
Edit sshd config file and test and restart sshd



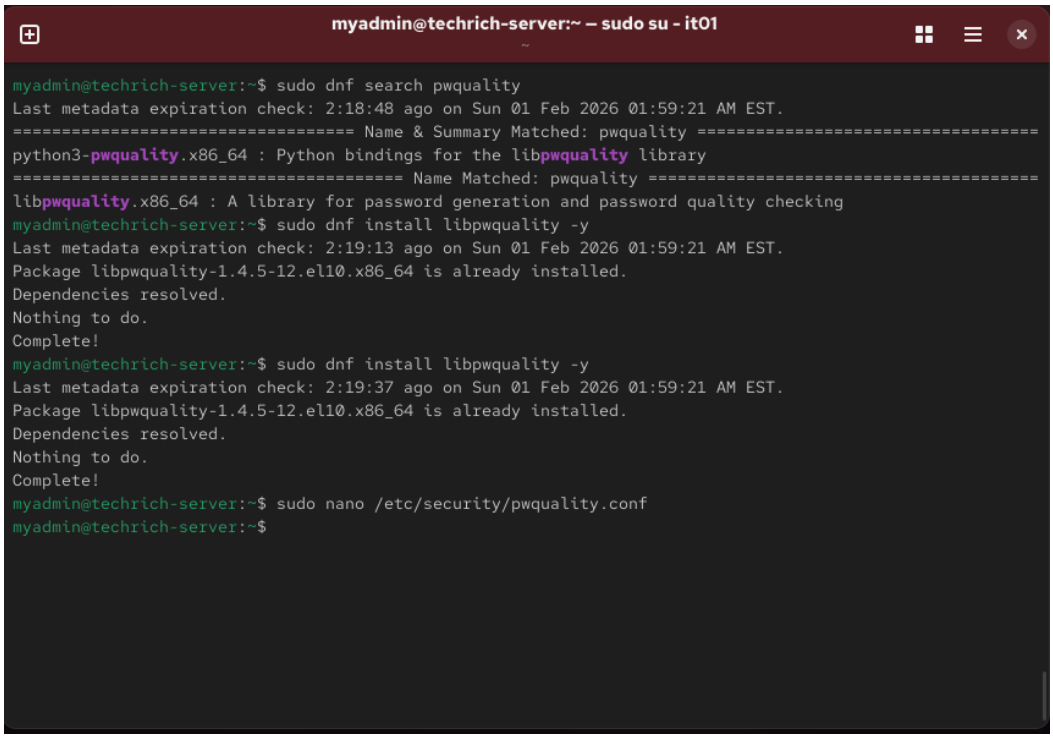
Ensure that sshd hardening is successful (root login is disabled, key-based auth is enabled, it01 and it02 are in the AllowUsers)

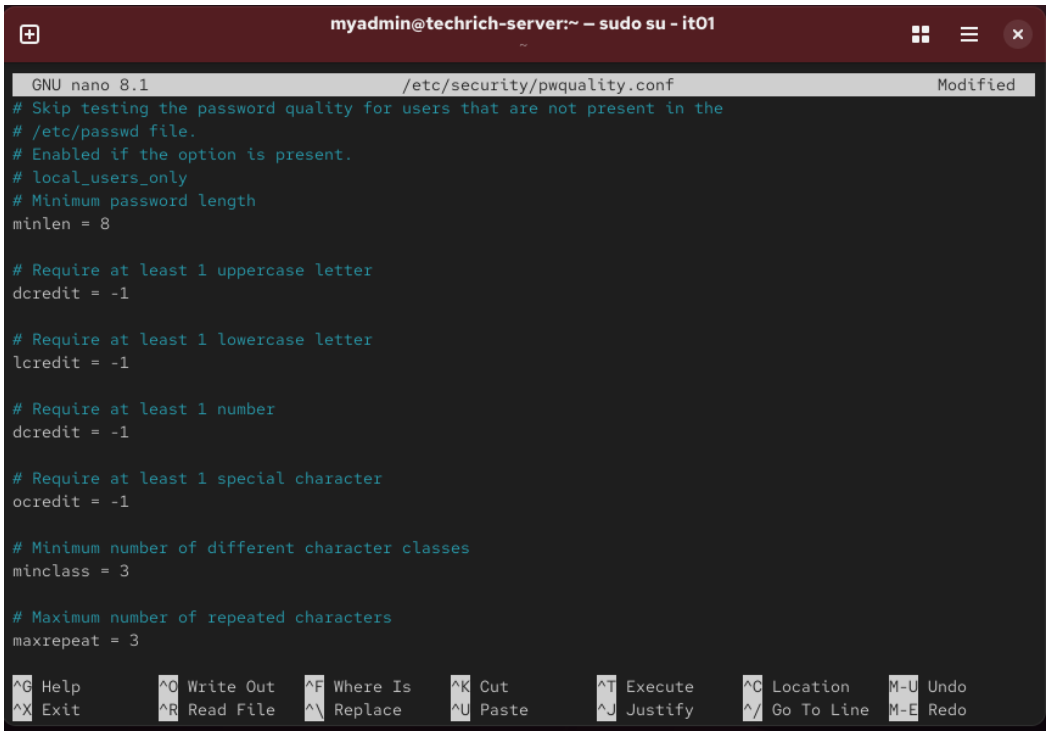


Ensure that the SSH keys generated earlier for it01 and it02 are working (passwordless connection for it01 and it02, and root login is disabled)



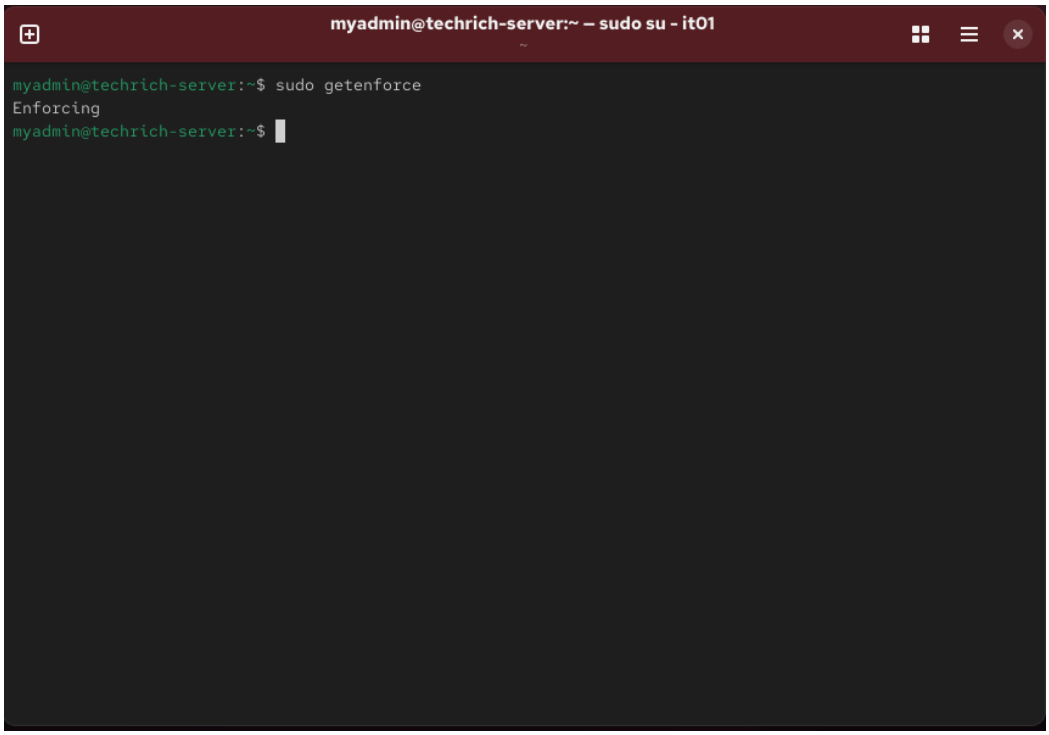
Set password policy by editing the pwquiality.conf file





SSELinux

Ensure that SELinux is enabled



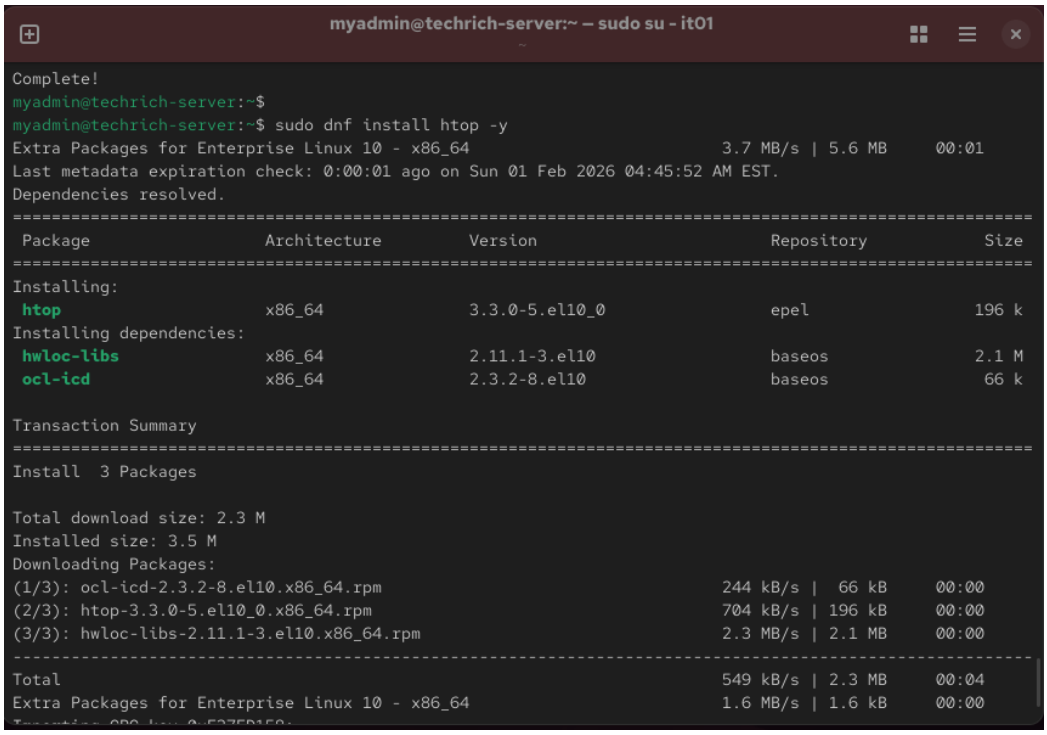
Explain the importance of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) in enterprise computing environments.

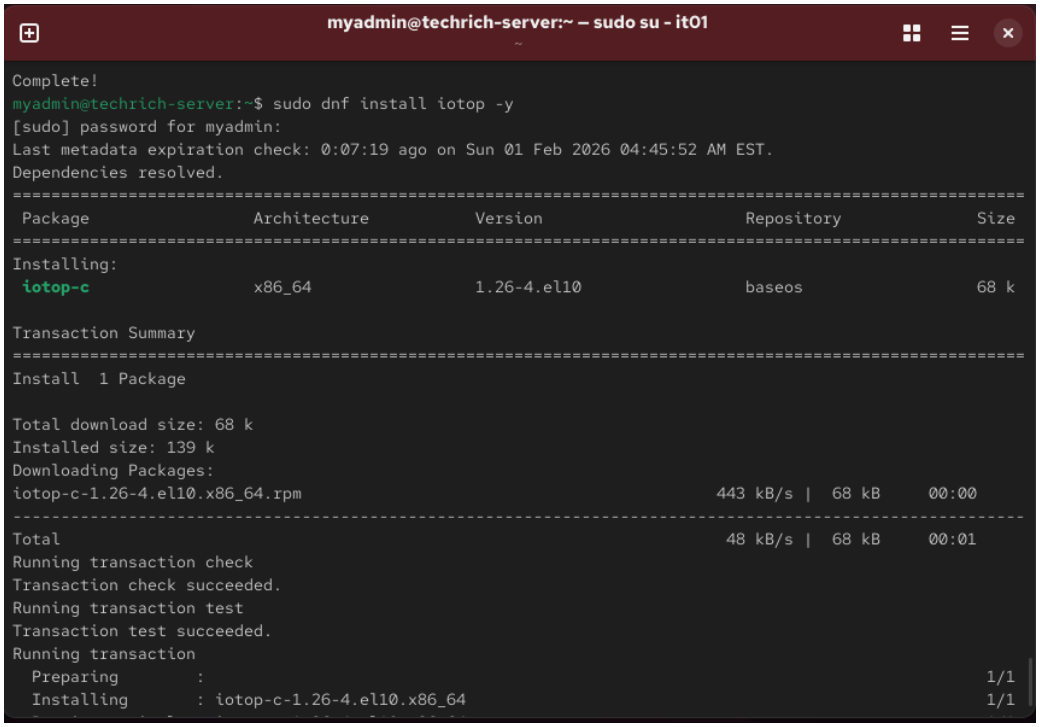
Firewalls filter network traffic to block unauthorized access while allowing legitimate traffic through based on predefined rules. IDS monitors network activity for suspicious behaviour and alerts administrators, functioning like a security camera that observes but does not act (Stallings, 2022). IPS 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).

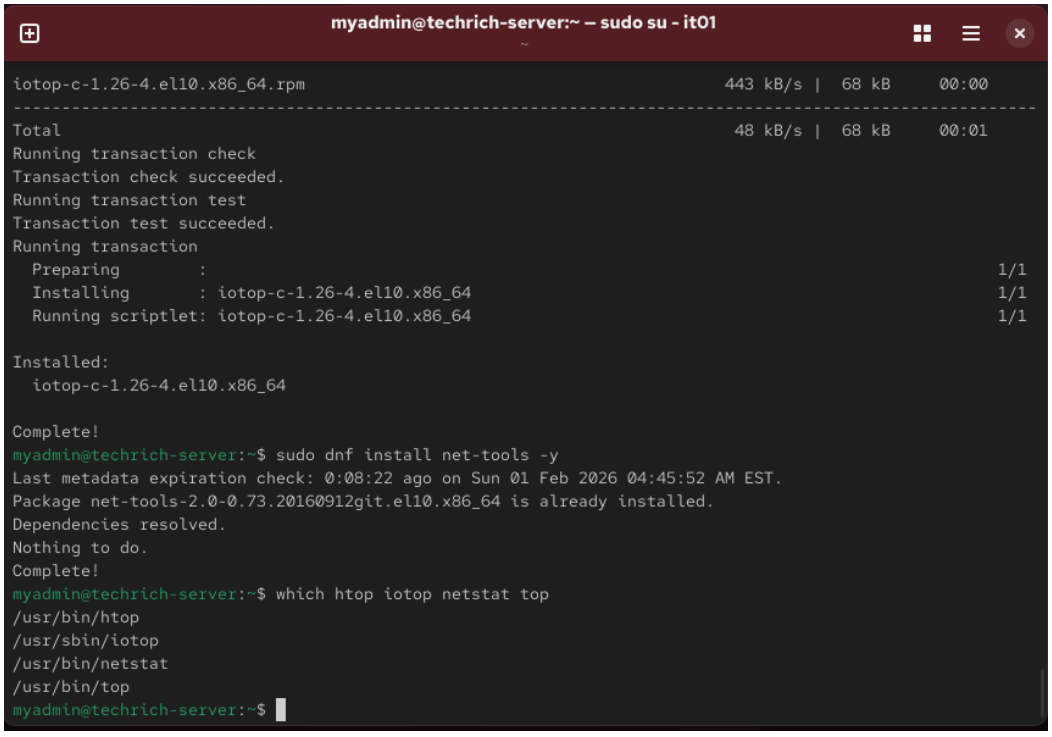
Task E

System monitoring

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

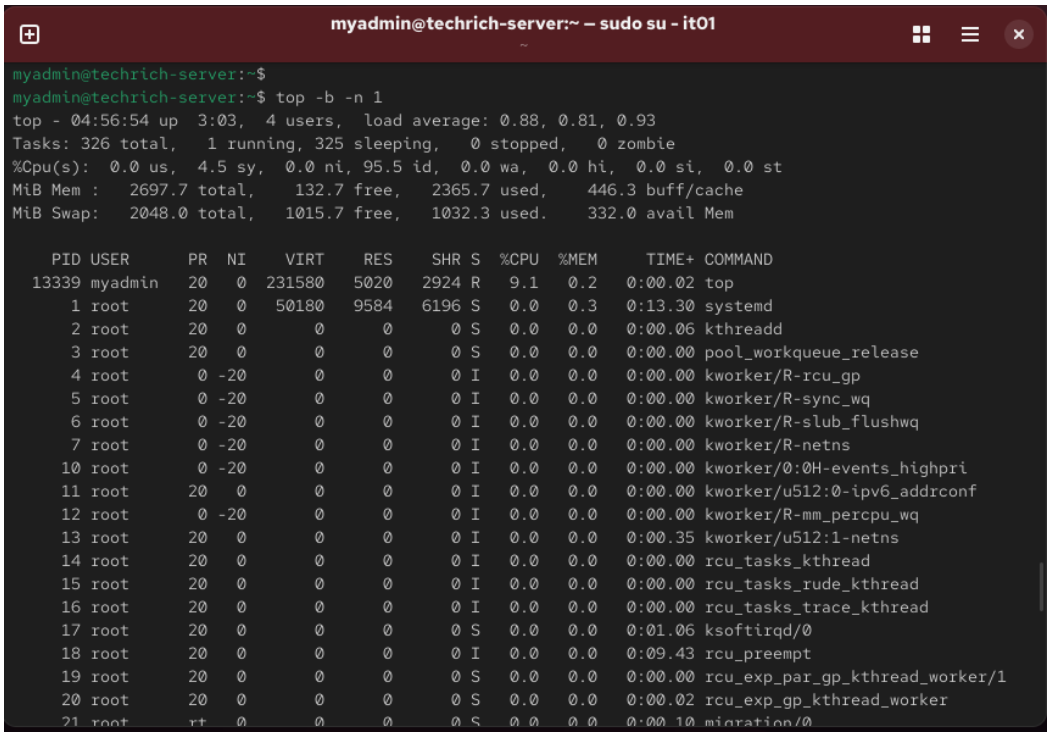




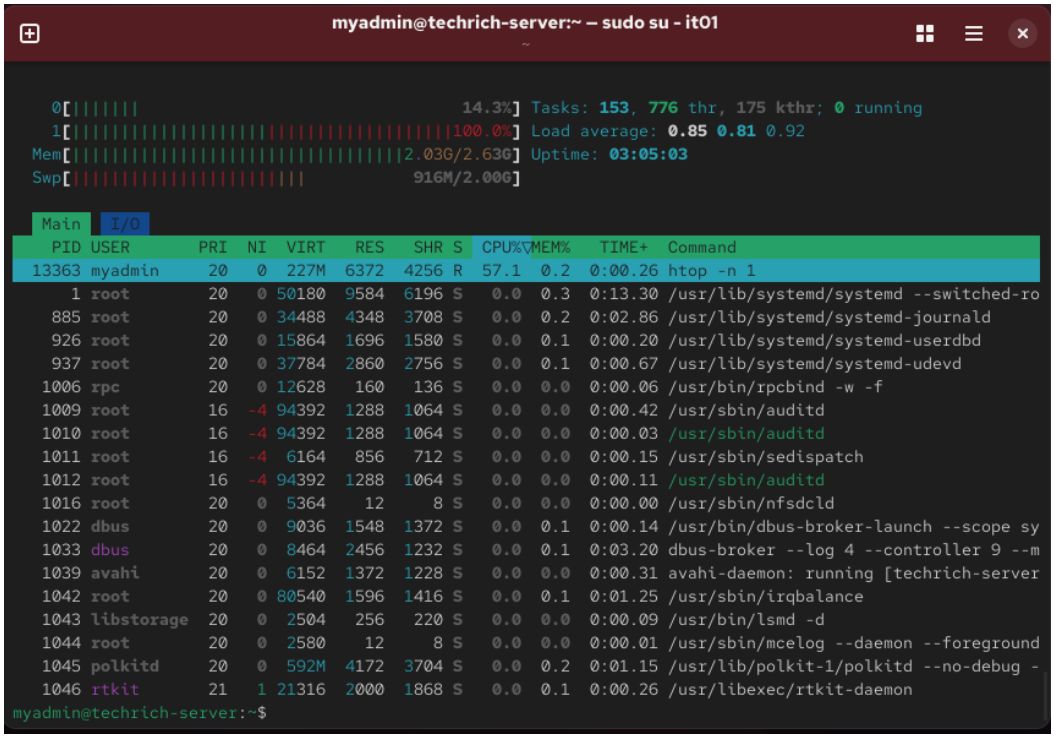


CPU Monitoring

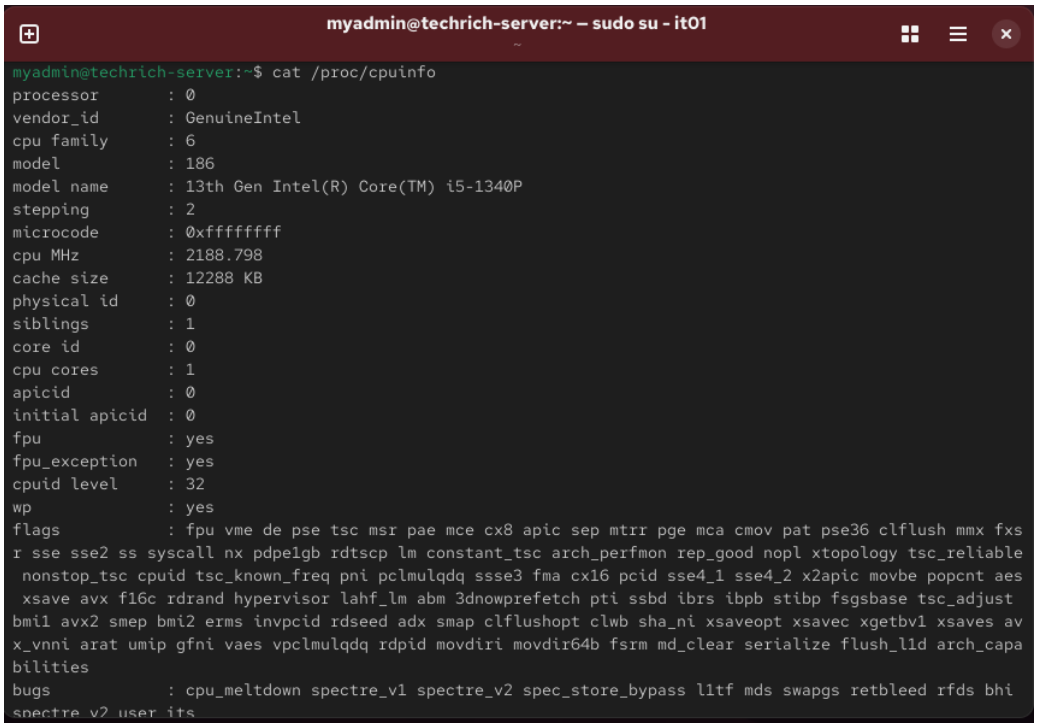
Monitor CPU performance using top



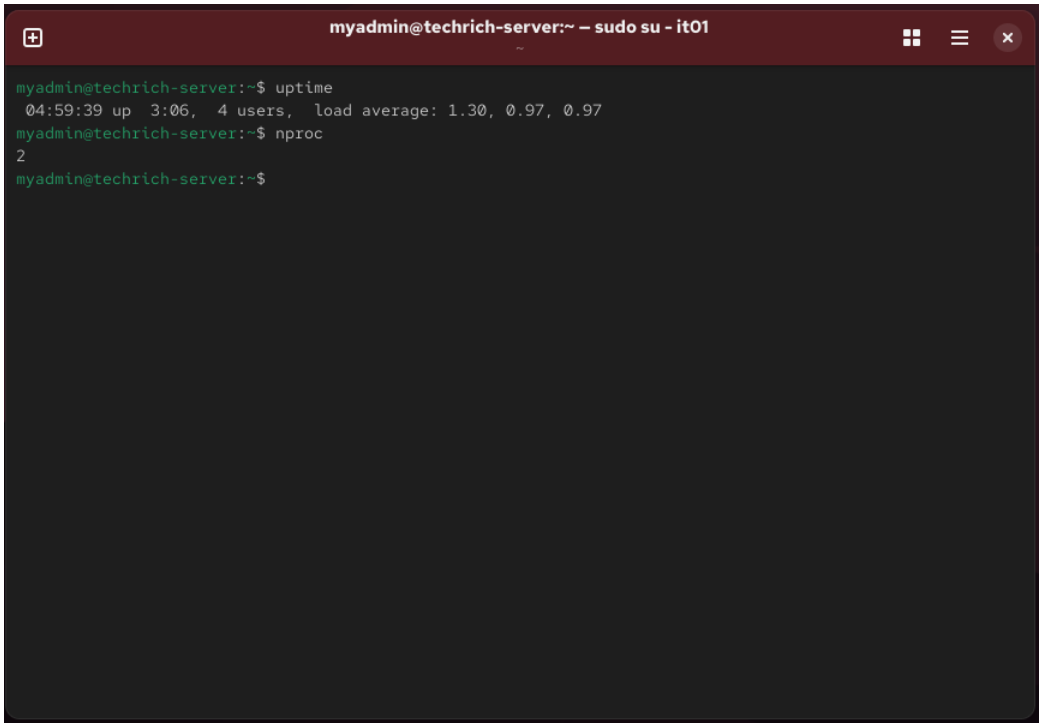
Monitor CPU using htop



Check CPU usage details

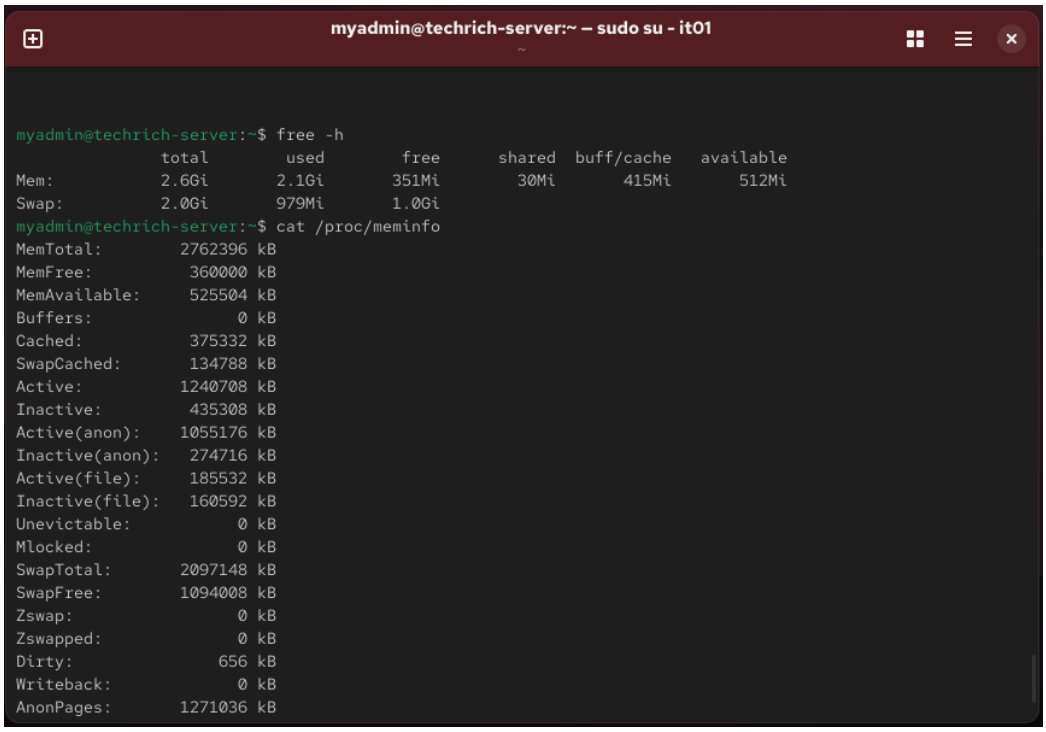


Check CPU load average



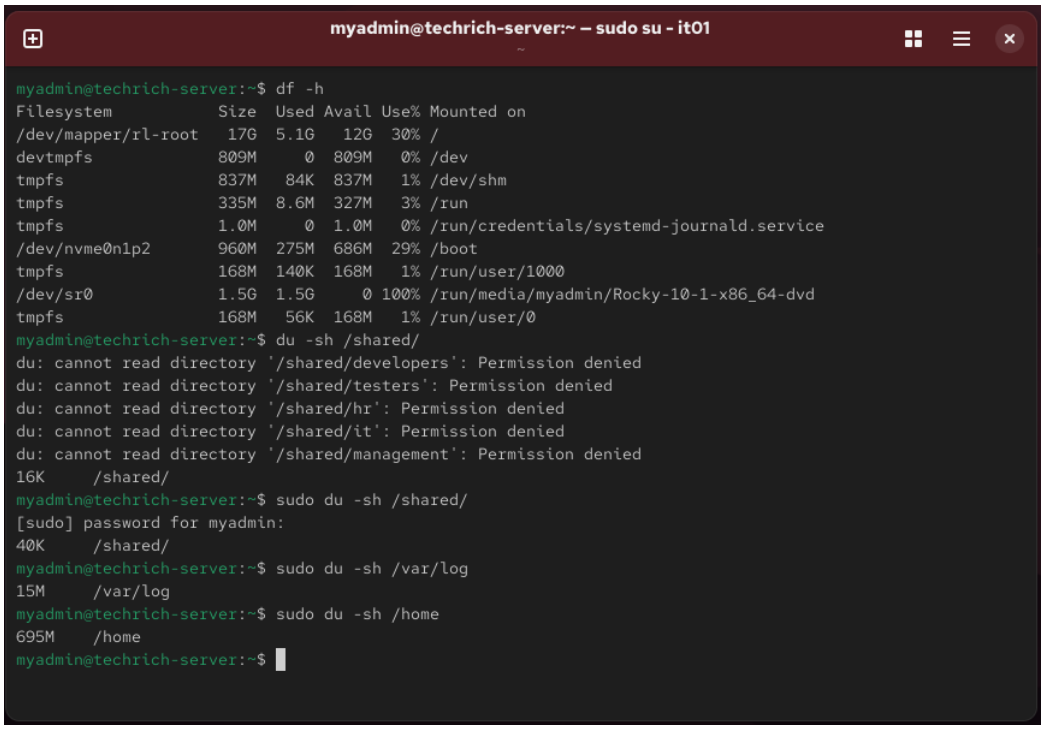
RAM monitoring

Memory overview and detailed memory info



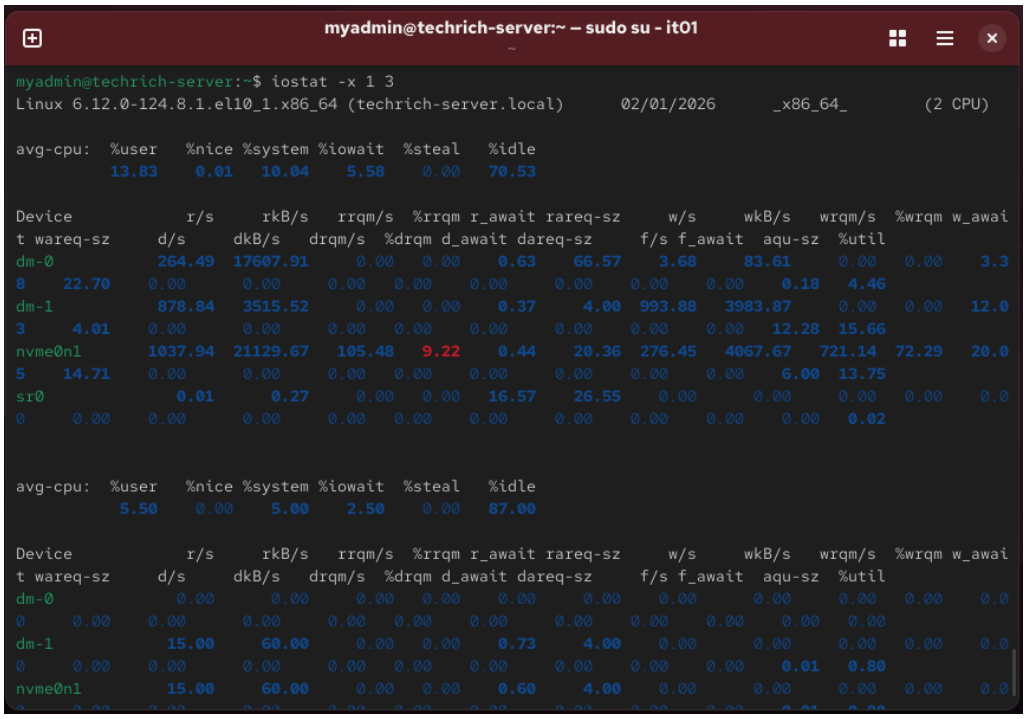
Disk Monitoring

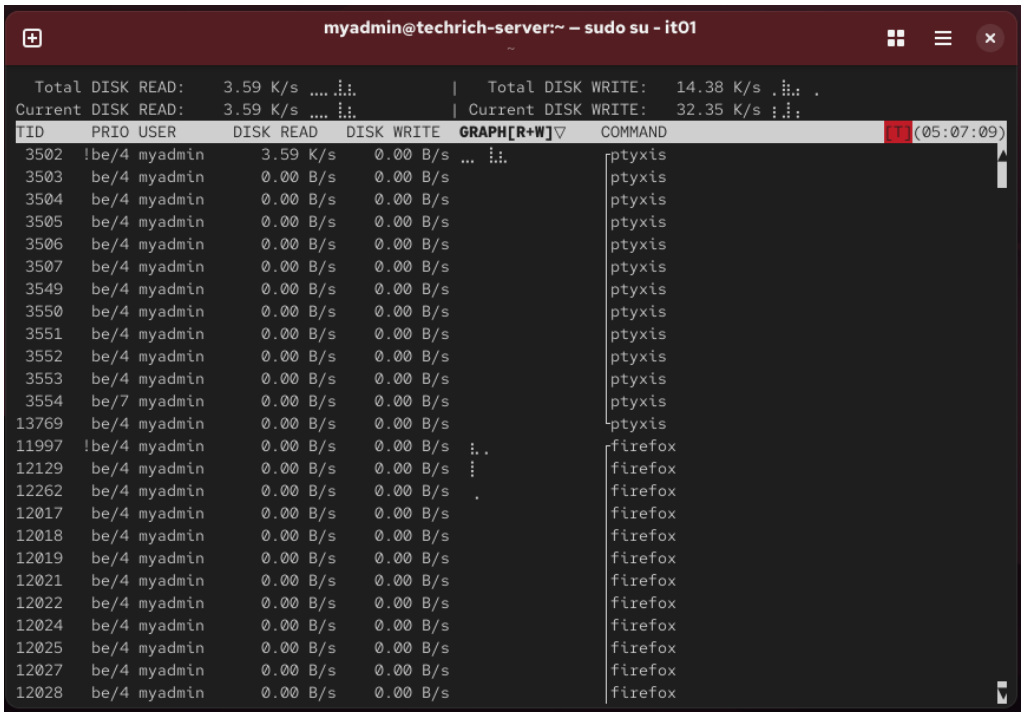
Overall disk usage and detailed disk usage for specific directories



Disk I/O Monitoring

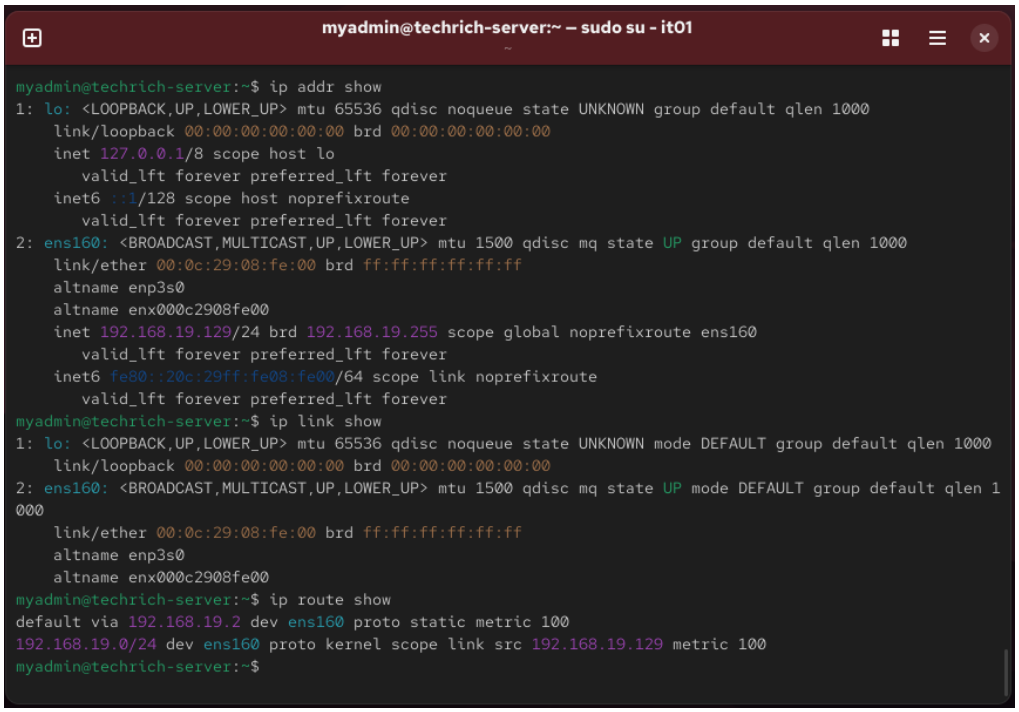
Monitoring disk I/O using iostat and iotop



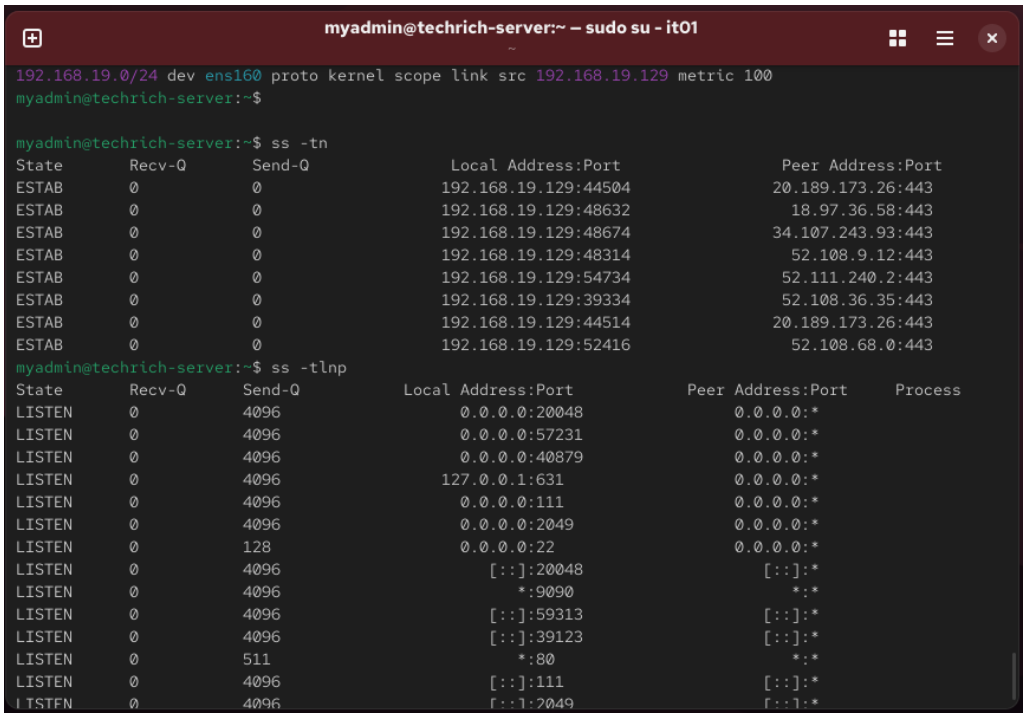


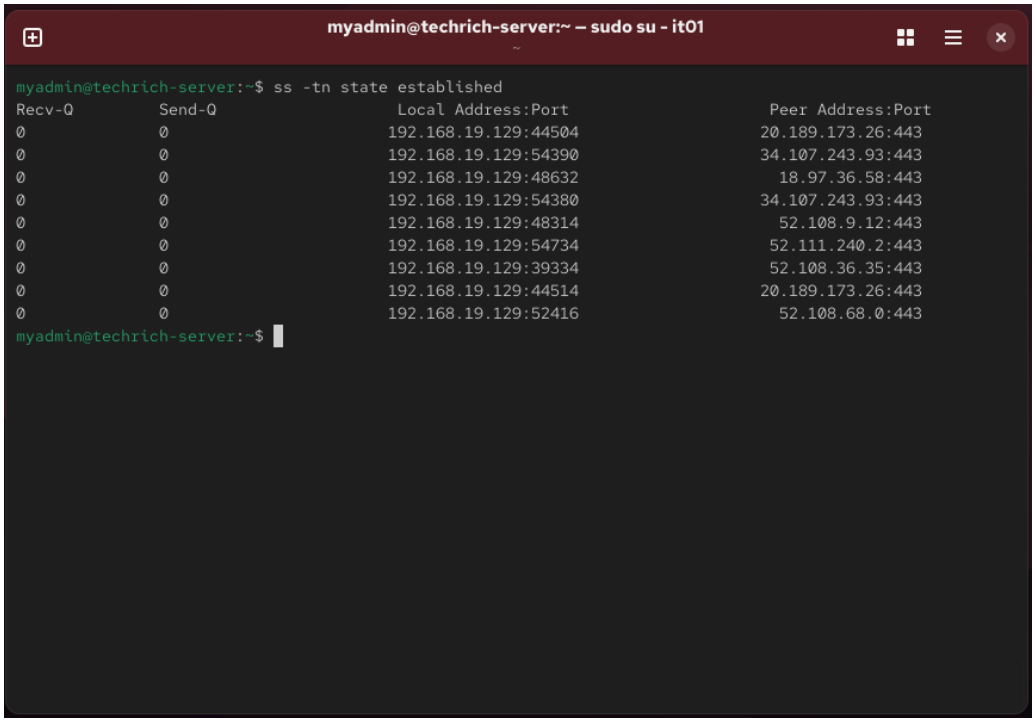
Network Monitoring

Monitoring network interface status



Monitoring network connection and ports using ss -tn

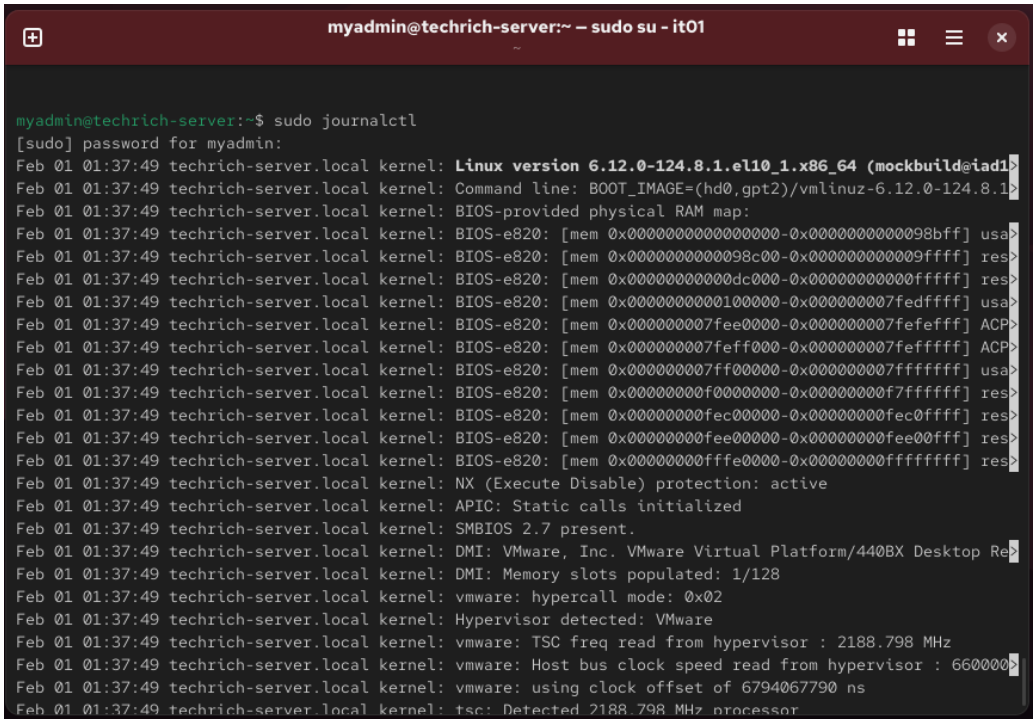




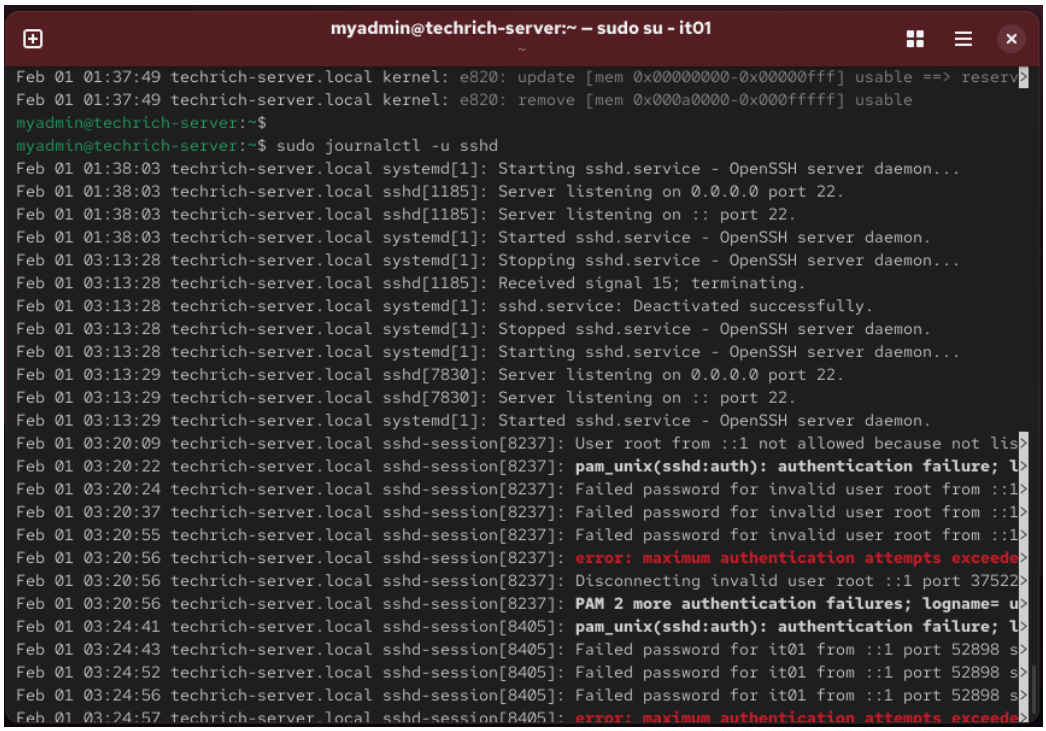
Log Analysis

Analyzing Using journalctl

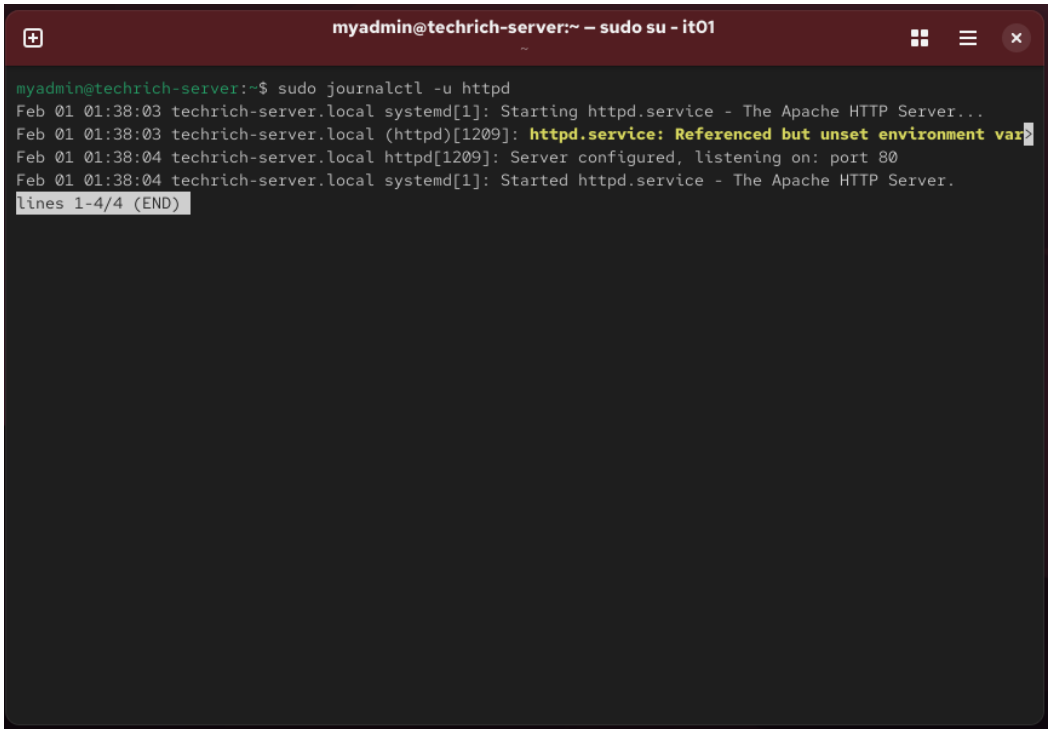
Verify all system logs



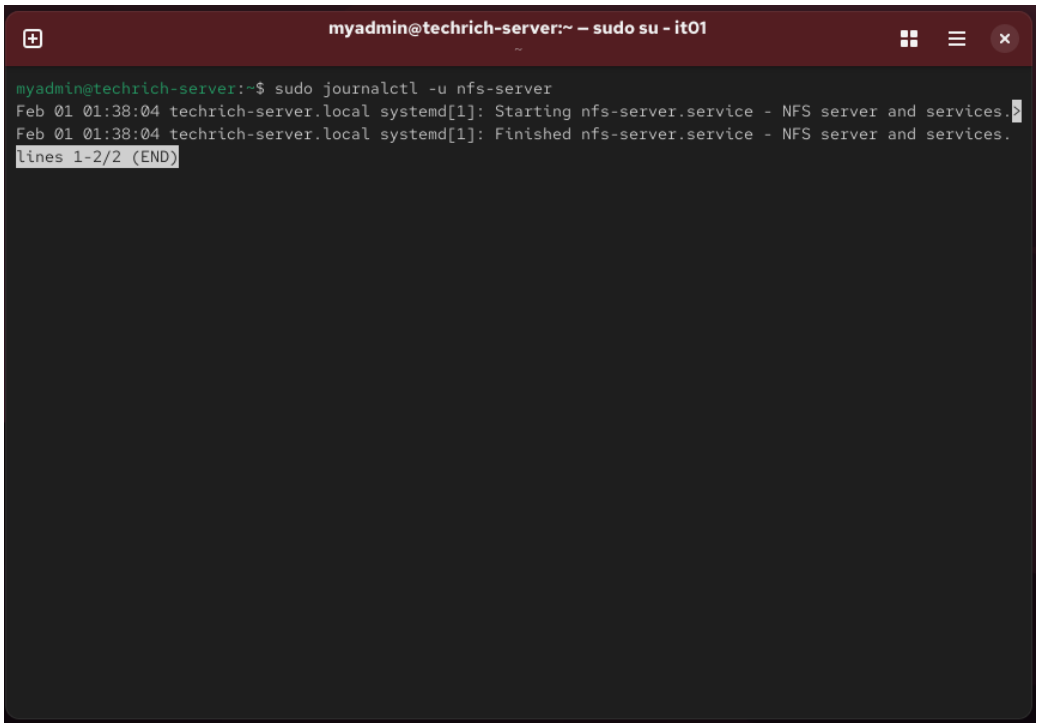
Check sshd logs



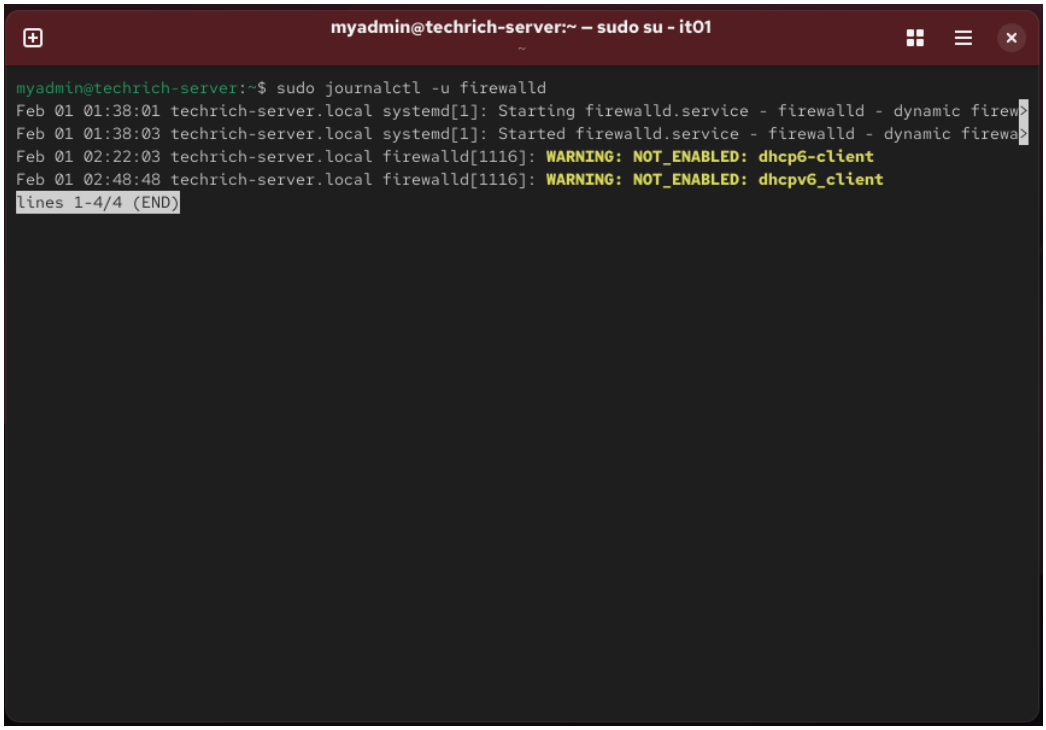
Check httpd logs



Check nfs logs



Check firewalld logs



Analyzing /var/log files

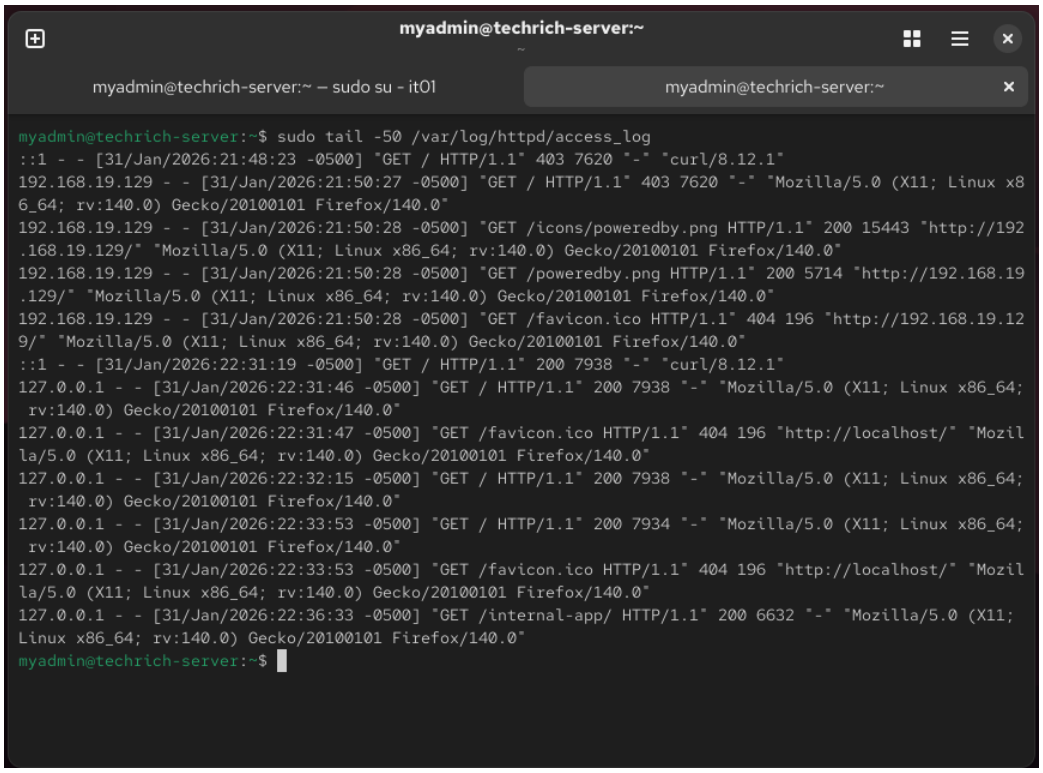
analyze ssh authentication logs

```
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 ui
d=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 ; COMMAN
D=/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 ; COMMAN
D=/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 ; COMMAN
D=/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 ; COMMAN
D=/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 ; COMMAN
D=/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)
```

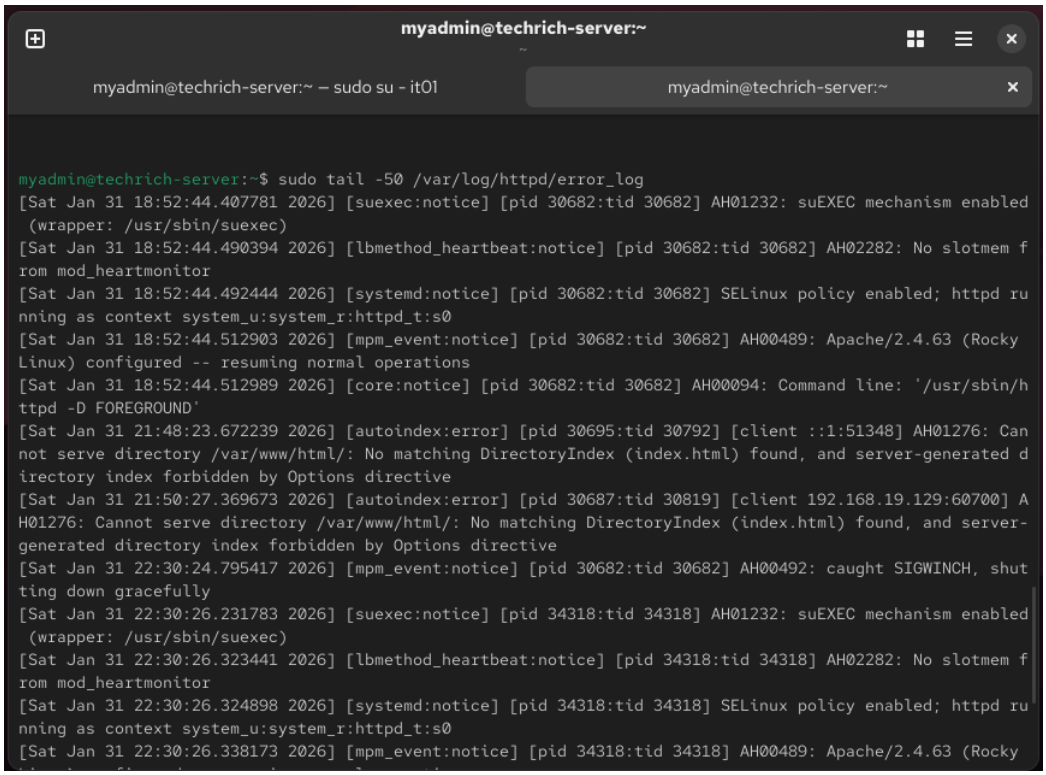
Analyzing system messages

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

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 05:40:18 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 05:40:33 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
Feb  1 05:42:34 techrich-server ptyxis[3502]: context mismatch in svga_surface_destroy
```

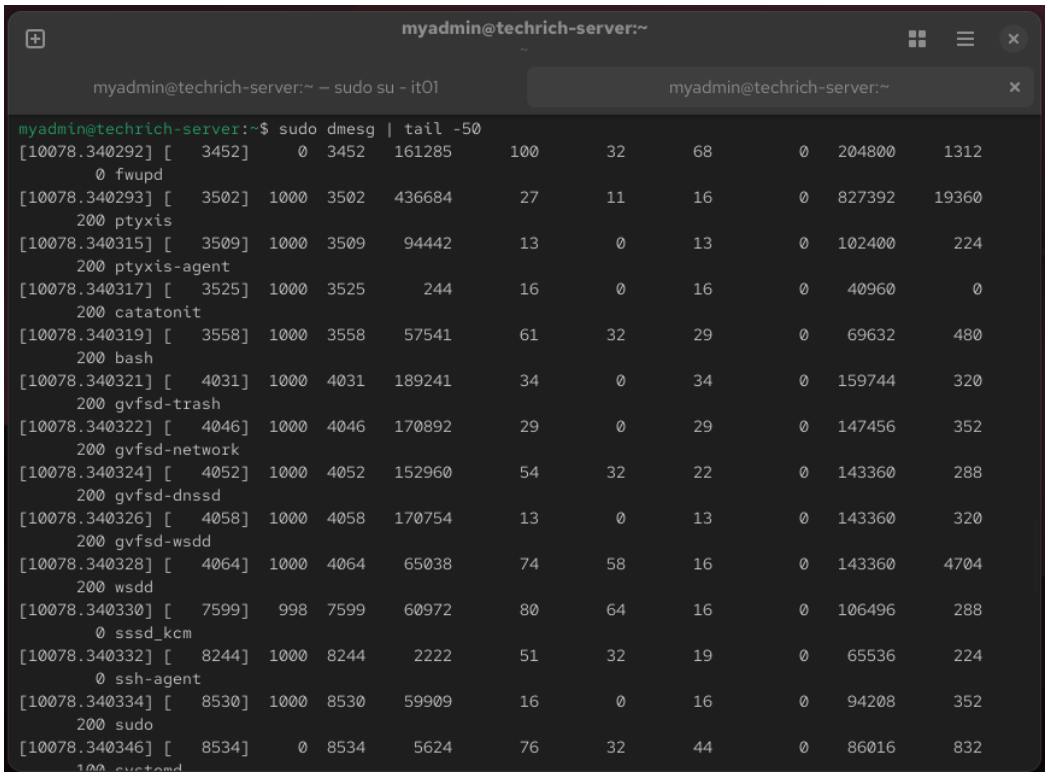
Analyzing Apache access log



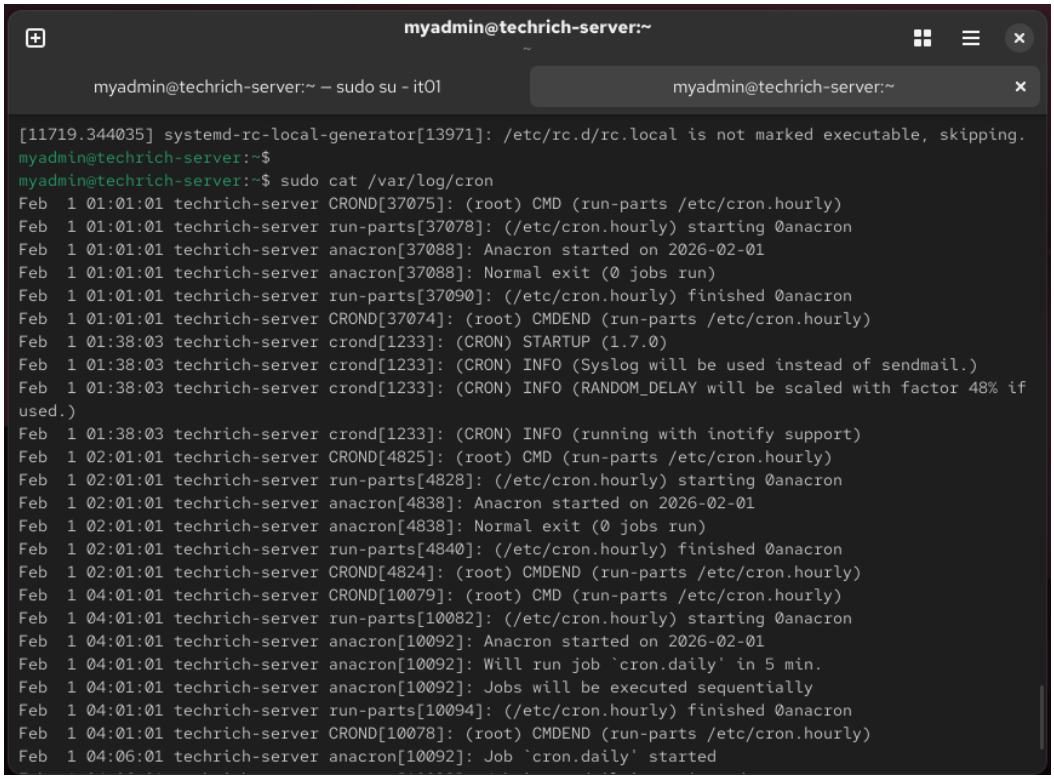
Analyzing Apache error logs



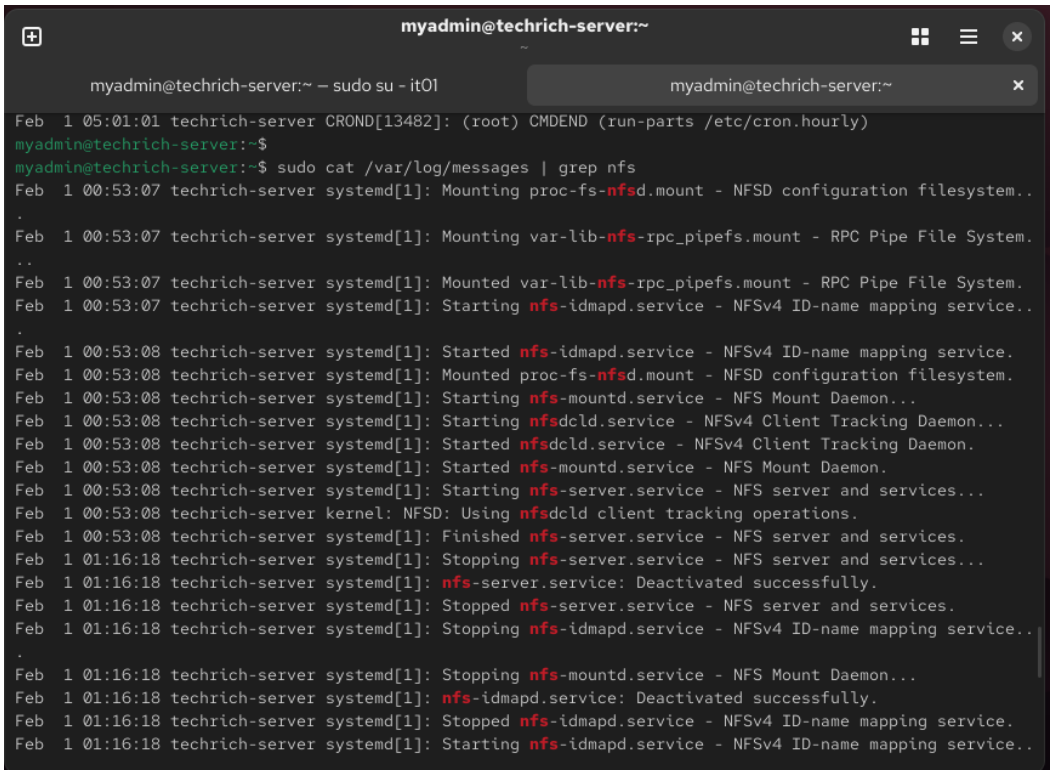
Analyzing boot messages



Analyzing cron job logs



Analyzing NFS logs



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 loging 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 tired 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 entery 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 rcpind service was not running

How I Checked

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