COLLEGE OF APPLIED BUSINESS AND TECHNOLOGY
Chabahil, Gangahity, Kathmandu

Network Security
PRACTICAL EXAM-2081

Submitted by:	**Submitted to:**
Name: AZ Kafle (106)	Indra Chaudhary

College of Applied Business and Technology

B.Sc.CSIT 7th Semester

January, 2025

Table of Contents

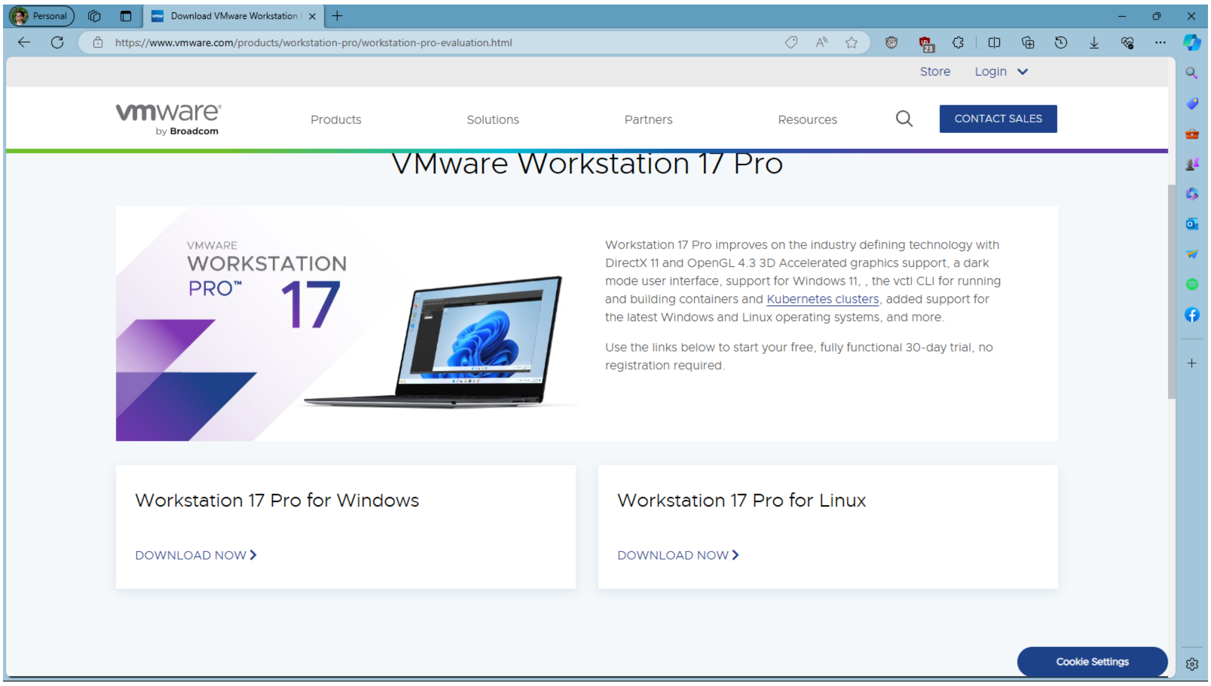
TASK 1

Preparing Lab Environment:

a) Installing VMware Workstation

To install VMware Workstation follow the following steps:

Step1: Go to Download VMware Workstation Pro and download Workstation Pro for Windows or Linux according to the OS you have.


Personal
Download VMware Workstation
https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html
Store
Login
vmware by Broadcom
Products
Solutions
Partners
Resources
CONTACT SALES
VMWARE WORKSTATION PRO™ 17
Cookie Settings

VMware Workstation 17 Pro

Workstation 17 Pro improves on the industry defining technology with DirectX 11 and OpenGL 4.3 3D Accelerated graphics support, a dark mode user interface, support for Windows 11, , the vctl CLI for running and building containers and Kubernetes clusters, added support for the latest Windows and Linux operating systems, and more.

Use the links below to start your free, fully functional 30-day trial, no registration required.

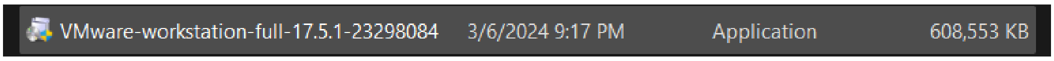
Workstation 17 Pro for Windows

DOWNLOAD NOW ›

Workstation 17 Pro for Linux

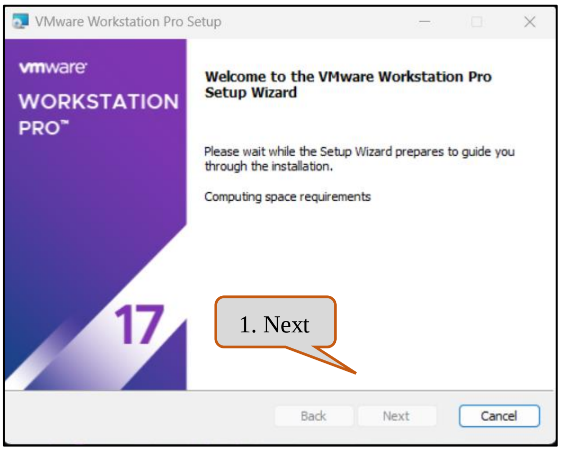
DOWNLOAD NOW ›

Step2: Run the installer as "VMware-workstation-full-16.1.0-17198959.exe".



```
VMware-workstation-full-17.5.1-23298084    3/6/2024 9:17 PM    Application    608,553 KB
```

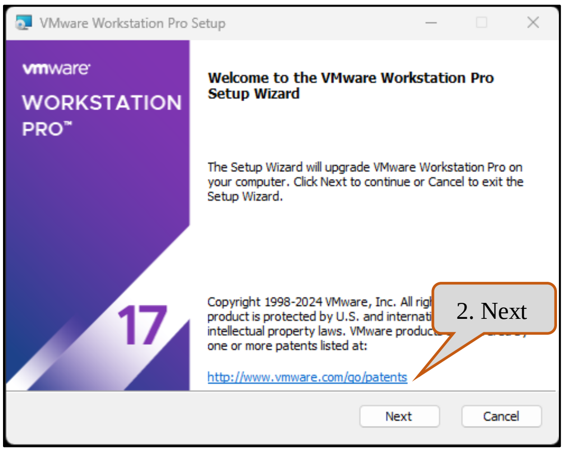
Step3: Follow the steps:



Welcome to the VMware Workstation Pro Setup Wizard

Please wait while the Setup Wizard prepares to guide you through the installation.

Computing space requirements

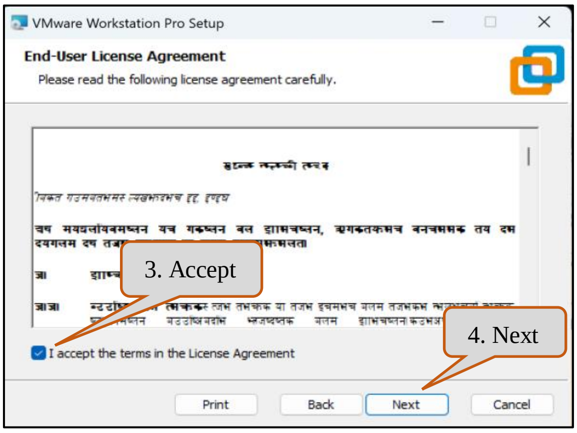


Welcome to the VMware Workstation Pro Setup Wizard

The Setup Wizard will upgrade VMware Workstation Pro on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright 1998-2024 VMware, Inc. All rig
product is protected by U.S. and internati
intellectual property laws. VMware produc
one or more patents listed at:

http://www.vmware.com/go/patents



VMware Workstation Pro Setup

End-User License Agreement

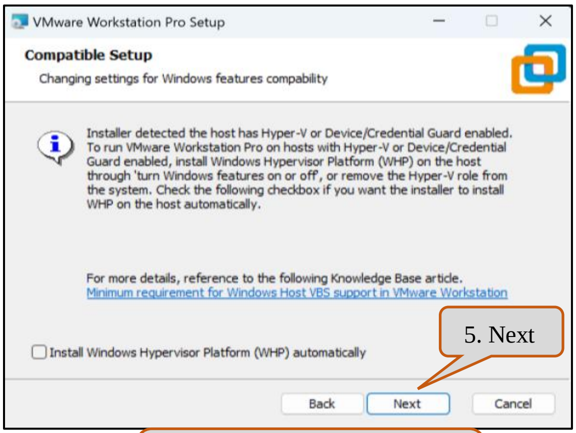
Please read the following license agreement carefully.

[illegible]

☑ I accept the terms in the License Agreement

3. Accept

4. Next



VMware Workstation Pro Setup

Compatible Setup

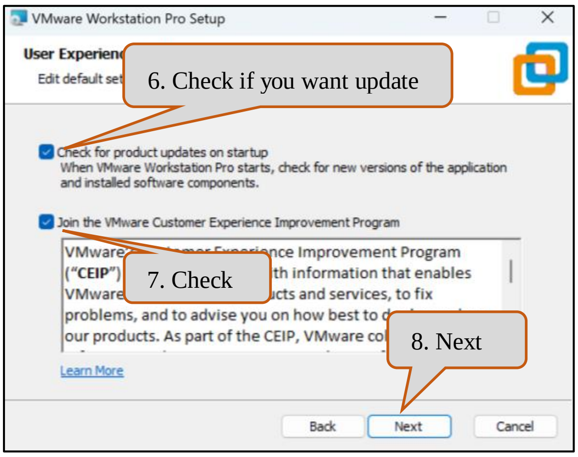
Changing settings for Windows features compability

Installer detected the host has Hyper-V or Device/Credential Guard enabled. To run VMware Workstation Pro on hosts with Hyper-V or Device/Credential Guard enabled, install Windows Hypervisor Platform (WHP) on the host through 'turn Windows features on or off', or remove the Hyper-V role from the system. Check the following checkbox if you want the installer to install WHP on the host automatically.

For more details, reference to the following Knowledge Base article.
Minimum requirement for Windows Host VBS support in VMware Workstation

☐ Install Windows Hypervisor Platform (WHP) automatically

5. Next



VMware Workstation Pro Setup

User Experienc

Edit default set

☑ Check for product updates on startup
When VMware Workstation Pro starts, check for new versions of the application and installed software components.

☑ Join the VMware Customer Experience Improvement Program

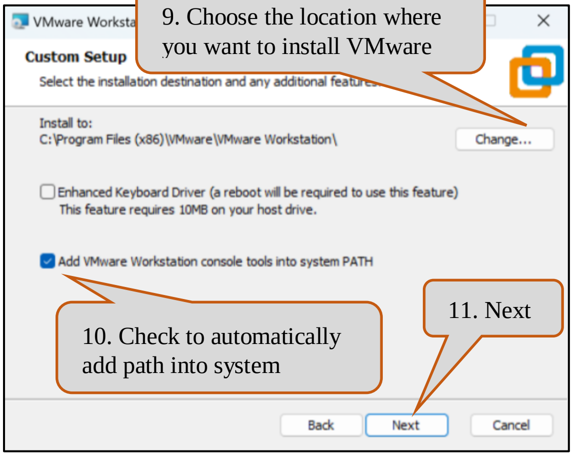
VMware Customer Experience Improvement Program ("CEIP") ... th information that enables VMware ... ucts and services, to fix problems, and to advise you on how best to d... our products. As part of the CEIP, VMware co...

Learn More

6. Check if you want update

7. Check

8. Next



VMware Worksta...

Custom Setup

Select the installation destination and any additional features

Install to:
C:\Program Files (x86)\VMware\VMware Workstation\

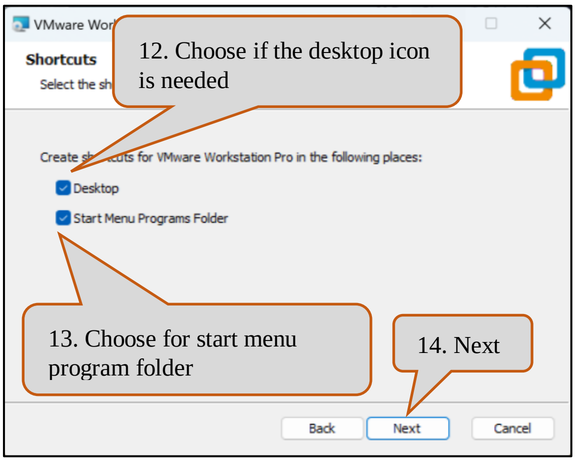
☐ Enhanced Keyboard Driver (a reboot will be required to use this feature)
This feature requires 10MB on your host drive.

☑ Add VMware Workstation console tools into system PATH

9. Choose the location where you want to install VMware

10. Check to automatically add path into system

11. Next



VMware Wor...

Shortcuts

Select the sh...

Create sh...cuts for VMware Workstation Pro in the following places:

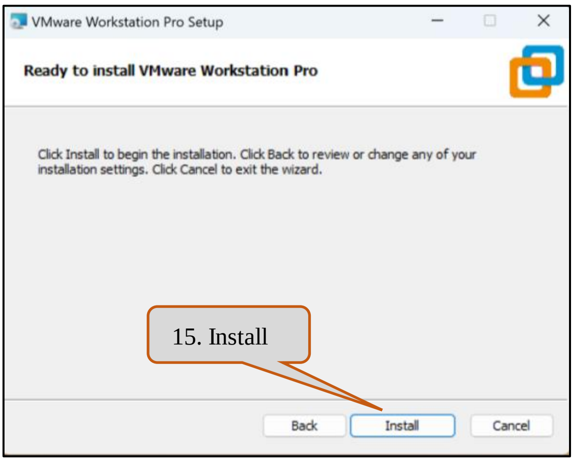
☑ Desktop

☑ Start Menu Programs Folder

12. Choose if the desktop icon is needed

13. Choose for start menu program folder

14. Next

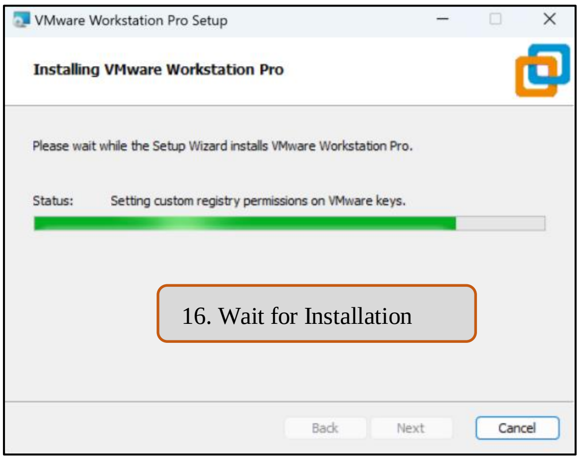


VMware Workstation Pro Setup

Ready to install VMware Workstation Pro

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

15. Install



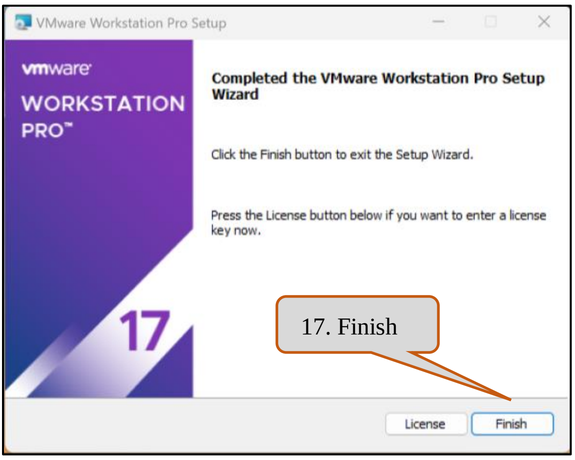
VMware Workstation Pro Setup

Installing VMware Workstation Pro

Please wait while the Setup Wizard installs VMware Workstation Pro.

Status: Setting custom registry permissions on VMware keys.

16. Wait for Installation



VMware Workstation Pro Setup

Completed the VMware Workstation Pro Setup Wizard

Click the Finish button to exit the Setup Wizard.

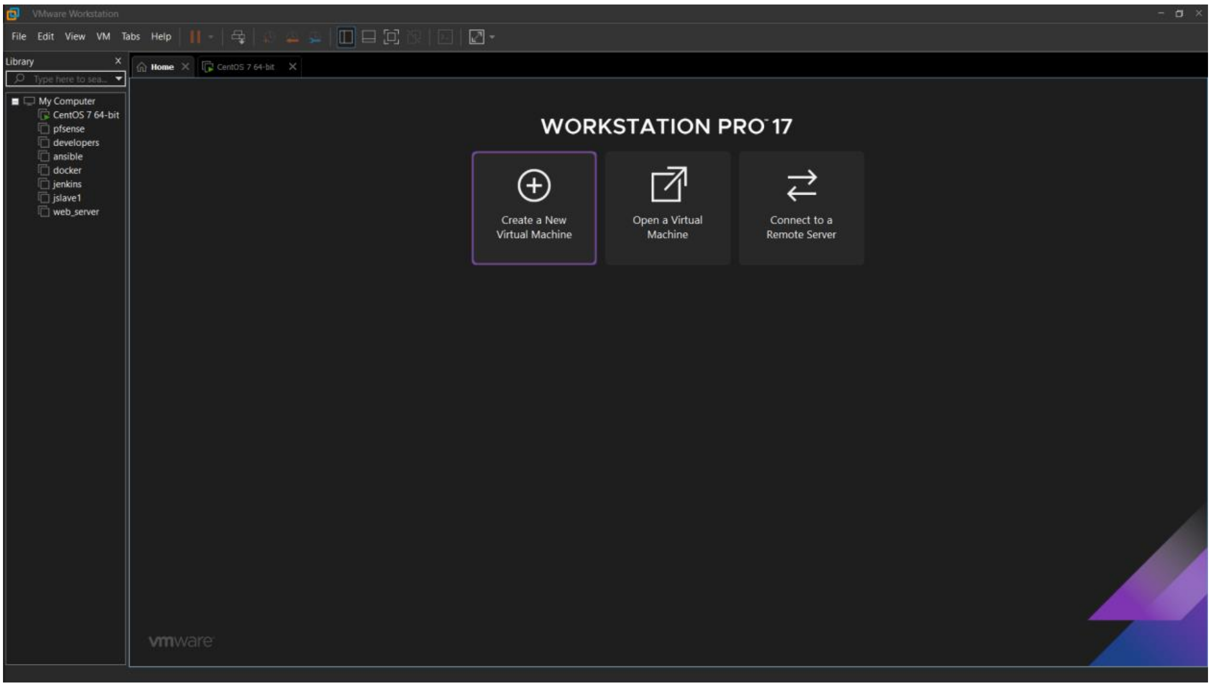
Press the License button below if you want to enter a license key now.

17. Finish

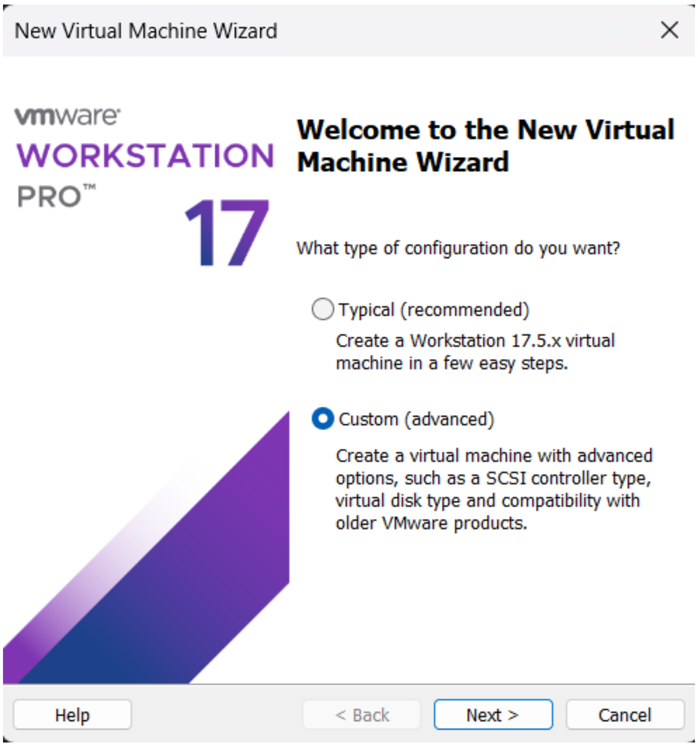
b) Creating Virtual Machine of AlmaLinux9

To create the CentOS & virtual machine follow the following steps:

Step1: Open VMware Workstation, and select **Create a new a Virtual Machine.**



Step2: Choose **Typical (recommended)** then **Next.**



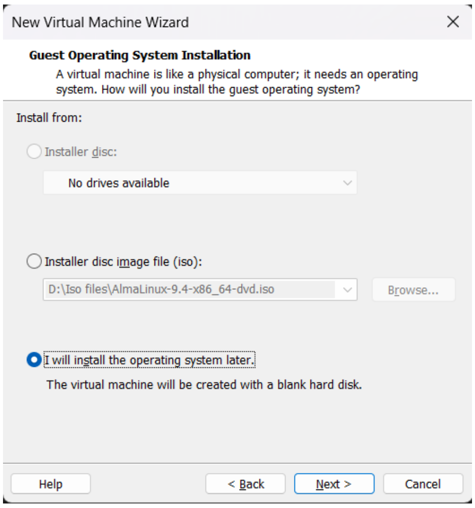
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

○ Typical (recommended)
Create a Workstation 17.5.x virtual machine in a few easy steps.

● Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Step3: Choose **I will install the Operating System later** then **Next .**



New Virtual Machine Wizard

Guest Operating System Installation

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

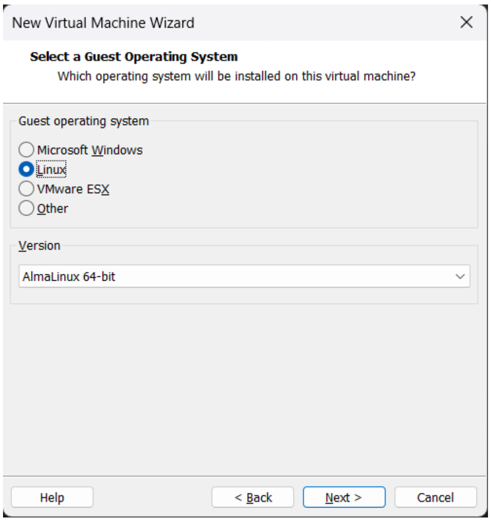
○ Installer disc image file (iso):

D:\Iso files\AlmaLinux-9.4-x86_64-dvd.iso

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.

<u>Step4</u>: Choose **Linux** operating system and **AlmaLinux 64-bit** as version and **Next.**



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

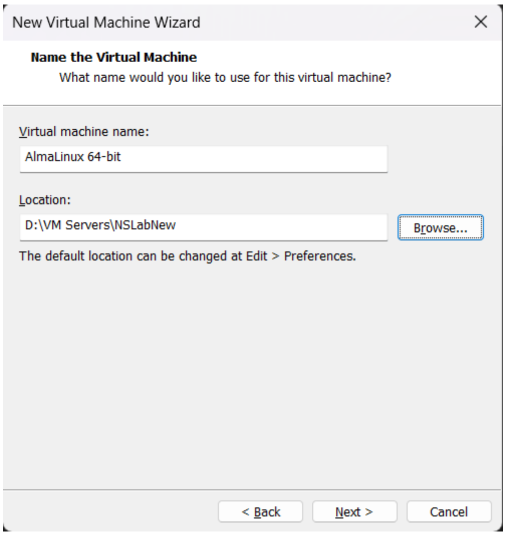
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

AlmaLinux 64-bit

<u>Step5</u>: Add name for virtual machine and choose location for VM**.**



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

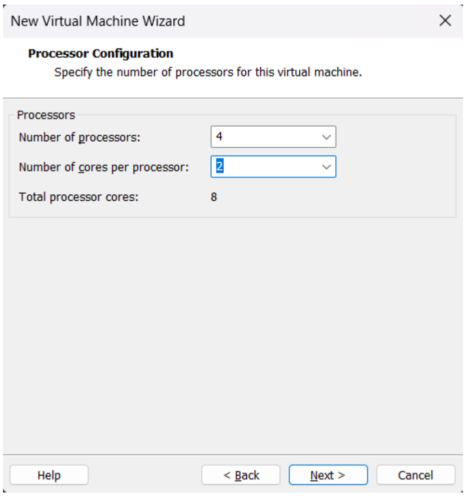
AlmaLinux 64-bit

Location:

D:\VM Servers\NSLabNew

The default location can be changed at Edit > Preferences.

Step6: Specify Processor Configuration and Disk Capacity



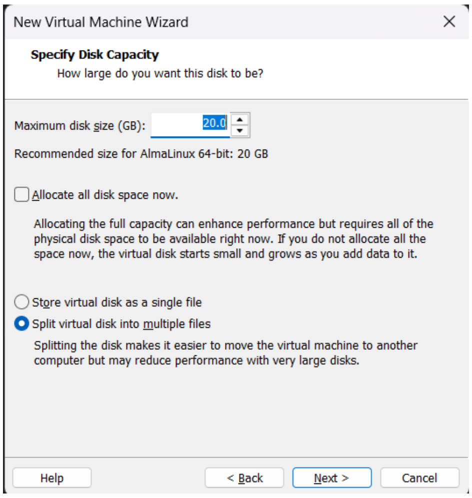
New Virtual Machine Wizard

Processor Configuration

Specify the number of processors for this virtual machine.

Processors

Number of processors:	4
Number of cores per processor:	2
Total processor cores:	8



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 20.0

Recommended size for AlmaLinux 64-bit: 20 GB

□ Allocate all disk space now.

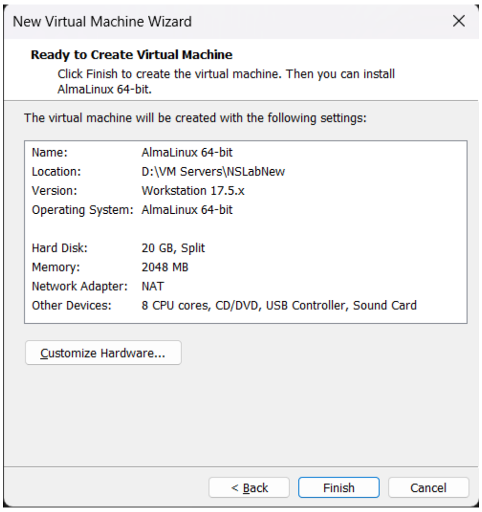
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ 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.

Step7: Customize hardware as per need and finish



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install AlmaLinux 64-bit.

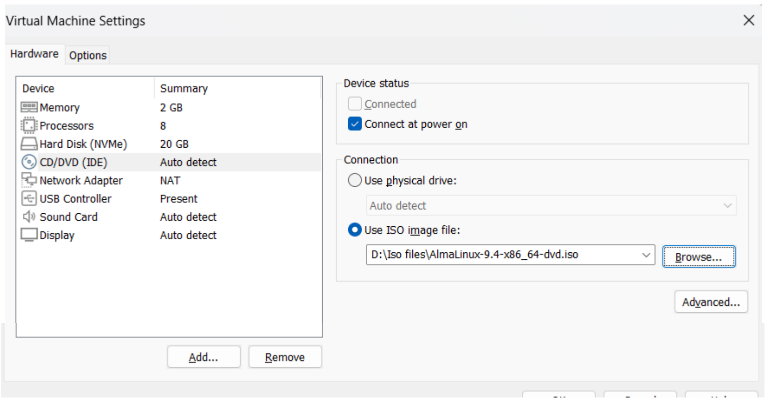
The virtual machine will be created with the following settings:

Name:	AlmaLinux 64-bit
Location:	D:\VM Servers\NSLabNew
Version:	Workstation 17.5.x
Operating System:	AlmaLinux 64-bit
Hard Disk:	20 GB, Split
Memory:	2048 MB
Network Adapter:	NAT
Other Devices:	8 CPU cores, CD/DVD, USB Controller, Sound Card

Step8: Download **AlmaLinux9 iso** file.

Step9: Go to **Edit virtual machine setting**

Step10: Go to CD/DVD ide, check **connect at power on,** and choose **use iso image file** and OK.



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	8
Hard Disk (NVMe)	20 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

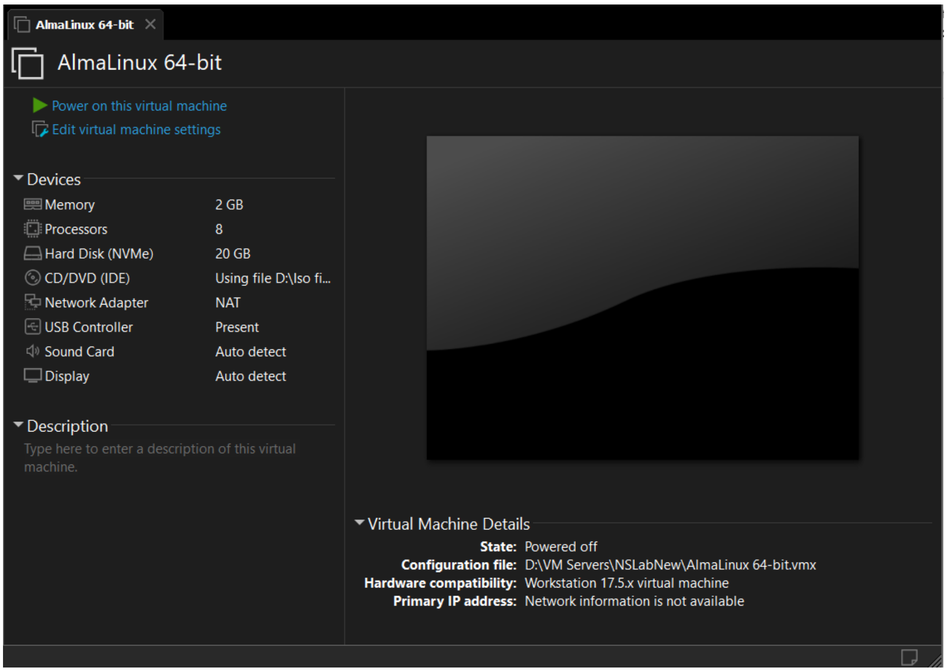
○ Use physical drive:

Auto detect

● Use ISO image file:

D:\Iso files\AlmaLinux-9.4-x86_64-dvd.iso

Step11: Now click **power on this virtual machine**.



Devices

Memory	2 GB
Processors	8
Hard Disk (NVMe)	20 GB
CD/DVD (IDE)	Using file D:\Iso fi...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

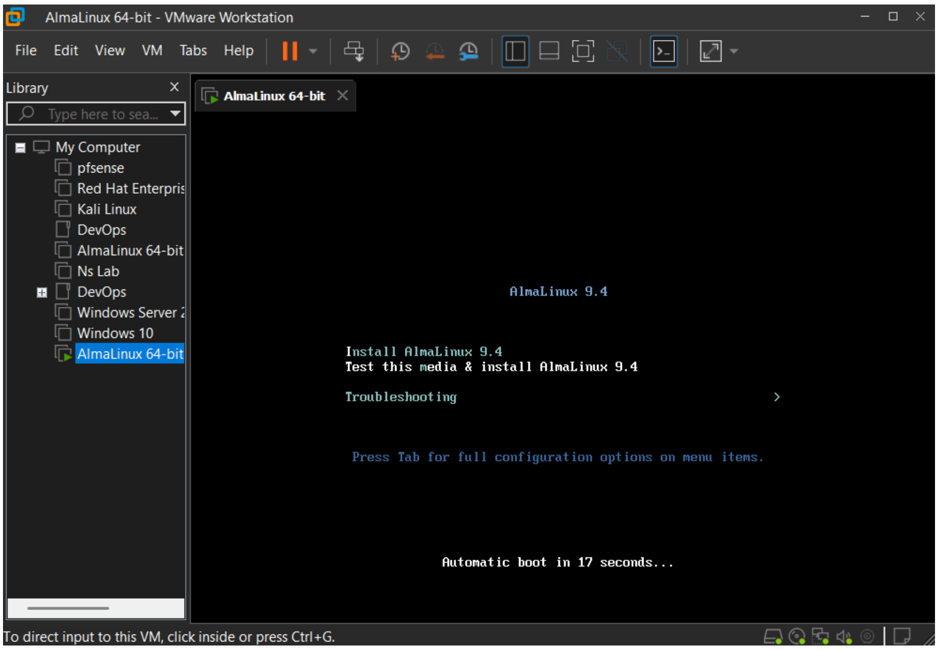
Description

Type here to enter a description of this virtual machine.

Virtual Machine Details

State: Powered off
Configuration file: D:\VM Servers\NSLabNew\AlmaLinux 64-bit.vmx
Hardware compatibility: Workstation 17.5.x virtual machine
Primary IP address: Network information is not available

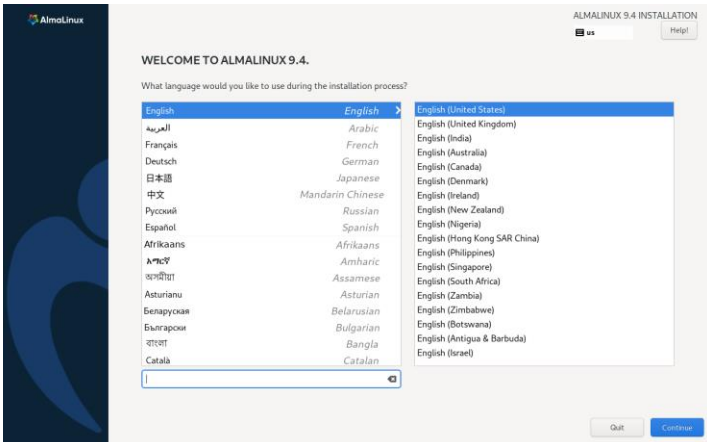
Step12: Select **Install CentOS 7** and press **Enter**.



```
AlmaLinux 9.4

Install AlmaLinux 9.4
Test this media & install AlmaLinux 9.4

Troubleshooting                                          >

 Press Tab for full configuration options on menu items.

Automatic boot in 17 seconds...
```

To direct input to this VM, click inside or press Ctrl+G.

Step13: Select Language you like to use and press **continue**.



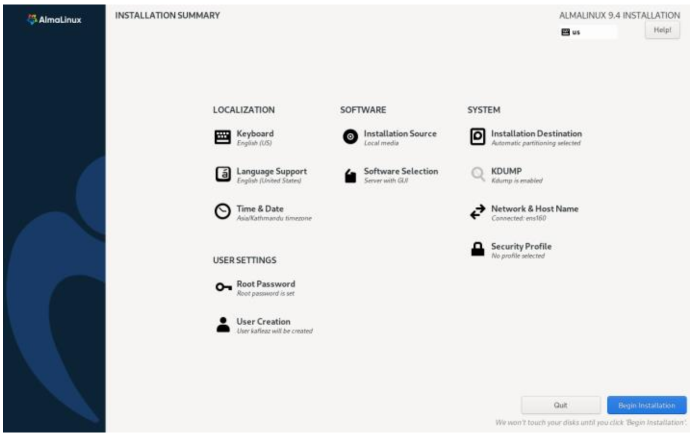
WELCOME TO ALMALINUX 9.4.

What language would you like to use during the installation process?

English	English
العربية	Arabic
Français	French
Deutsch	German
日本語	Japanese
中文	Mandarin Chinese
Русский	Russian
Español	Spanish
Afrikaans	Afrikaans
አማርኛ	Amharic
অসমীয়া	Assamese
Asturianu	Asturian
Беларуская	Belarusian
Български	Bulgarian
বাংলা	Bangla
Català	Catalan

English (United States)
English (United Kingdom)
English (India)
English (Australia)
English (Canada)
English (Denmark)
English (Ireland)
English (New Zealand)
English (Nigeria)
English (Hong Kong SAR China)
English (Philippines)
English (Singapore)
English (South Africa)
English (Zambia)
English (Zimbabwe)
English (Botswana)
English (Antigua & Barbuda)
English (Israel)

Step14:. Configure options Date and time, Language, Keyboard, Network and Hostname.



INSTALLATION SUMMARY

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Asia/Kathmandu timezone

SOFTWARE

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Connected: ens160

Security Profile
No profile selected

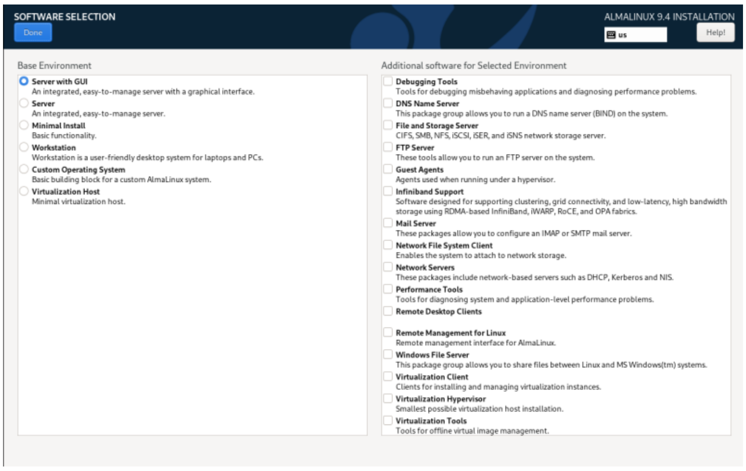
USER SETTINGS

Root Password
Root password is set

User Creation
User kafleaz will be created

We won't touch your disks until you click 'Begin Installation'.

Step15: Choose the software **Software Selection > Server with GUI > Done**.



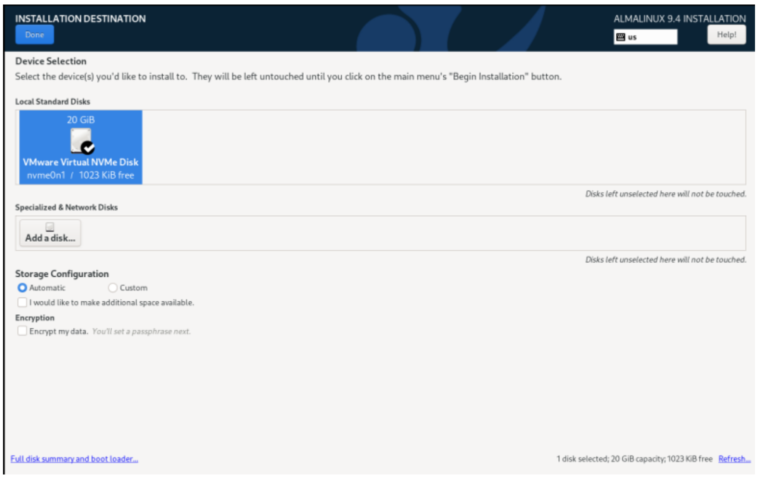
Base Environment

● **Server with GUI**
An integrated, easy-to-manage server with a graphical interface.
○ **Server**
An integrated, easy-to-manage server.
○ **Minimal Install**
Basic functionality.
○ **Workstation**
Workstation is a user-friendly desktop system for laptops and PCs.
○ **Custom Operating System**
Basic building block for a custom AlmaLinux system.
○ **Virtualization Host**
Minimal virtualization host.

Additional software for Selected Environment

□ **Debugging Tools**
Tools for debugging misbehaving applications and diagnosing performance problems.
□ **DNS Name Server**
This package group allows you to run a DNS name server (BIND) on the system.
□ **File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
□ **FTP Server**
These tools allow you to run an FTP server on the system.
□ **Guest Agents**
Agents used when running under a hypervisor.
□ **Infiniband Support**
Software designed for supporting clustering, grid connectivity, and low-latency, high bandwidth storage using RDMA-based InfiniBand, iWARP, RoCE, and OPA fabrics.
□ **Mail Server**
These packages allow you to configure an IMAP or SMTP mail server.
□ **Network File System Client**
Enables the system to attach to network storage.
□ **Network Servers**
These packages include network-based servers such as DHCP, Kerberos and NIS.
□ **Performance Tools**
Tools for diagnosing system and application-level performance problems.
□ **Remote Desktop Clients**
□ **Remote Management for Linux**
Remote management interface for AlmaLinux.
□ **Windows File Server**
This package group allows you to share files between Linux and MS Windows(tm) systems.
□ **Virtualization Client**
Clients for installing and managing virtualization instances.
□ **Virtualization Hypervisor**
Smallest possible virtualization host installation.
□ **Virtualization Tools**
Tools for offline virtual image management.

<u>Step16</u>: Choose **Installation Destination** as default and then **Done**.



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

20 GiB
VMware Virtual NVMe Disk
nvme0n1 / 1023 KiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Add a disk...

Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

□ I would like to make additional space available.

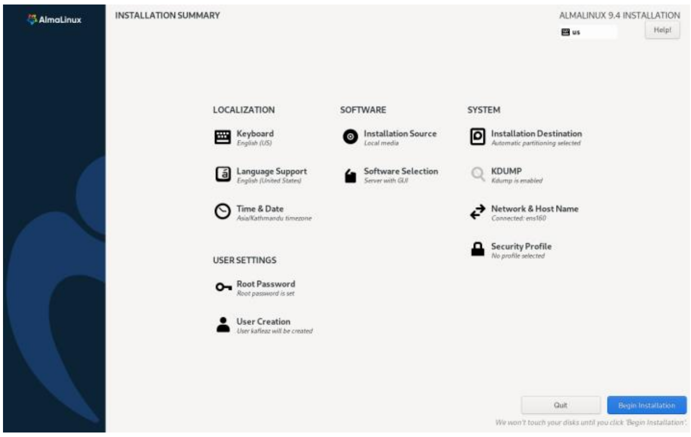
Encryption

□ Encrypt my data. *You'll set a passphrase next.*

Full disk summary and boot loader...

1 disk selected; 20 GiB capacity; 1023 KiB free Refresh...

<u>Step17</u>: Select **Begin Installation**.



LOCALIZATION
- Keyboard — *English (US)*
- Language Support — *English (United States)*
- Time & Date — *Asia/Kathmandu timezone*

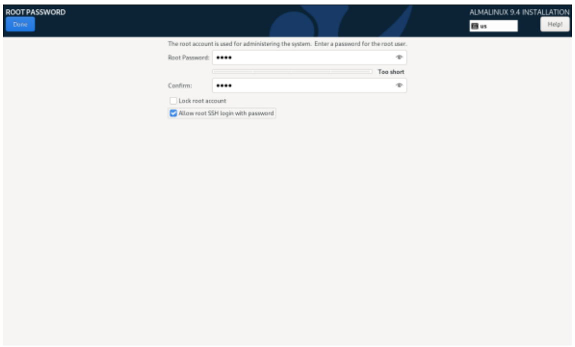
SOFTWARE
- Installation Source — *Local media*
- Software Selection — *Server with GUI*

SYSTEM
- Installation Destination — *Automatic partitioning selected*
- KDUMP — *Kdump is enabled*
- Network & Host Name — *Connected: ens160*
- Security Profile — *No profile selected*

USER SETTINGS
- Root Password — *Root password is set*
- User Creation — *User kafleaz will be created*

We won't touch your disks until you click 'Begin Installation'.

<u>Step18</u>: Set **password** for root and create a **user** and wait for installation.



The root account is used for administering the system. Enter a password for the root user.

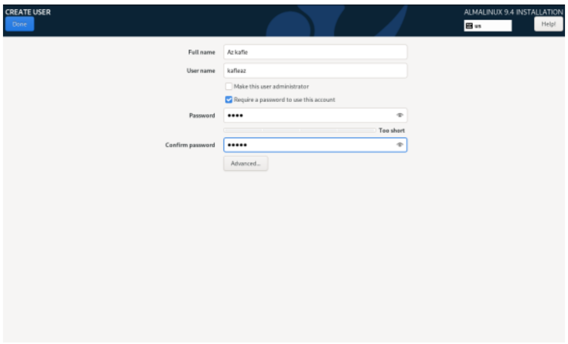
Root Password: ••••

Too short

Confirm: ••••

□ Lock root account

☑ Allow root SSH login with password



Full name: Az kafle

User name: kafleaz

□ Make this user administrator

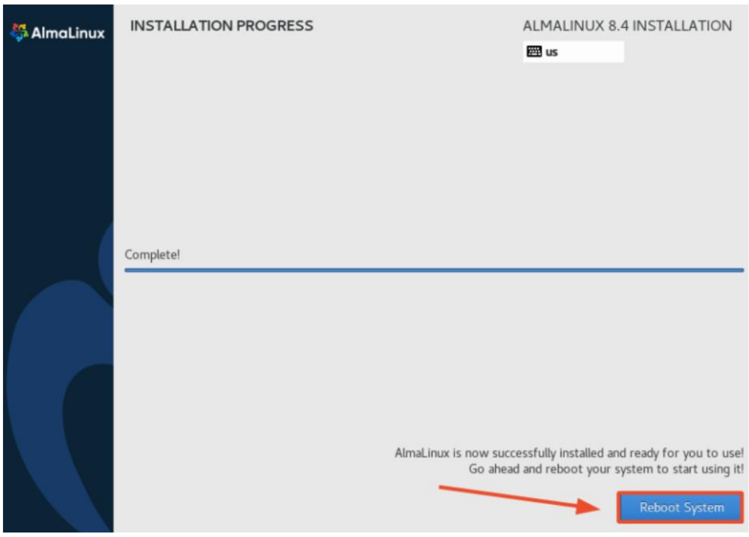
☑ Require a password to use this account

Password: ••••

Too short

Confirm password: •••••

Step19: After completion of installation **Reboot**.

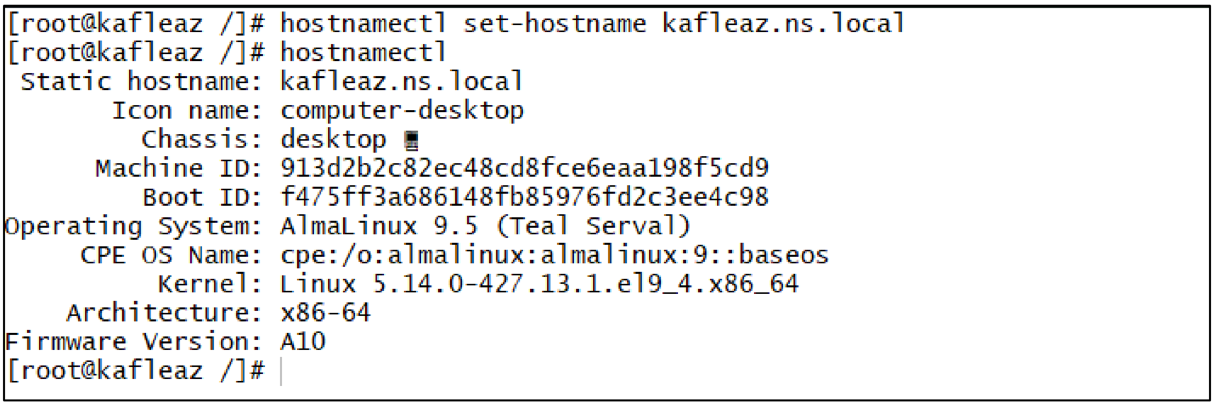


AlmaLinux is now successfully installed and ready for you to use!
Go ahead and reboot your system to start using it!

Step20: After reboot **Accept License agreement > Done**.

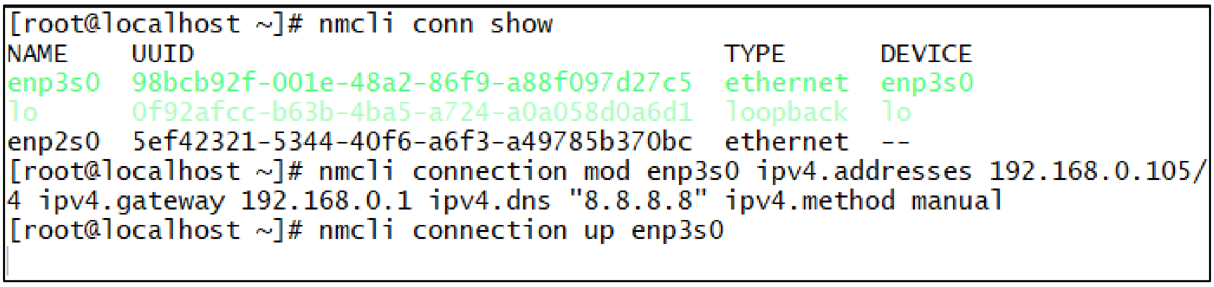
After following all the steps mentioned above our Virtual Machine of AlmaLinux 9 is created successfully.

c) Assign the hostname of Linux machine as <yourname>.ns.local



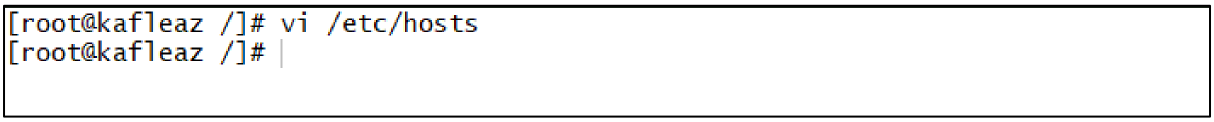
```
[root@kafleaz /]# hostnamectl set-hostname kafleaz.ns.local
[root@kafleaz /]# hostnamectl
 Static hostname: kafleaz.ns.local
       Icon name: computer-desktop
         Chassis: desktop 🖥
      Machine ID: 913d2b2c82ec48cd8fce6eaa198f5cd9
         Boot ID: f475ff3a686148fb85976fd2c3ee4c98
Operating System: AlmaLinux 9.5 (Teal Serval)
     CPE OS Name: cpe:/o:almalinux:almalinux:9::baseos
          Kernel: Linux 5.14.0-427.13.1.el9_4.x86_64
    Architecture: x86-64
Firmware Version: A10
[root@kafleaz /]#
```

d) Configure your network interface with static ip address and start the network service.

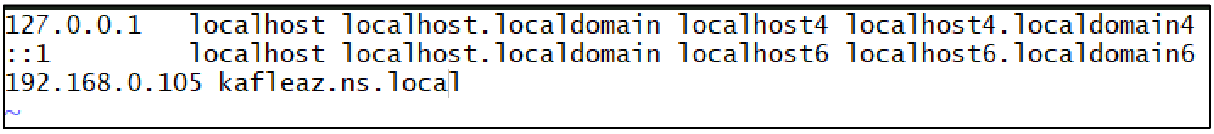


```
[root@localhost ~]# nmcli conn show
NAME    UUID                                  TYPE      DEVICE
enp3s0  98bcb92f-001e-48a2-86f9-a88f097d27c5  ethernet  enp3s0
lo      0f92afcc-b63b-4ba5-a724-a0a058d0a6d1  loopback  lo
enp2s0  5ef42321-5344-40f6-a6f3-a49785b370bc  ethernet  --
[root@localhost ~]# nmcli connection mod enp3s0 ipv4.addresses 192.168.0.105/
4 ipv4.gateway 192.168.0.1 ipv4.dns "8.8.8.8" ipv4.method manual
[root@localhost ~]# nmcli connection up enp3s0
```

e) Map your static ip address to your hosts name in configuration file /etc/hosts



```
[root@kafleaz /]# vi /etc/hosts
[root@kafleaz /]#
```

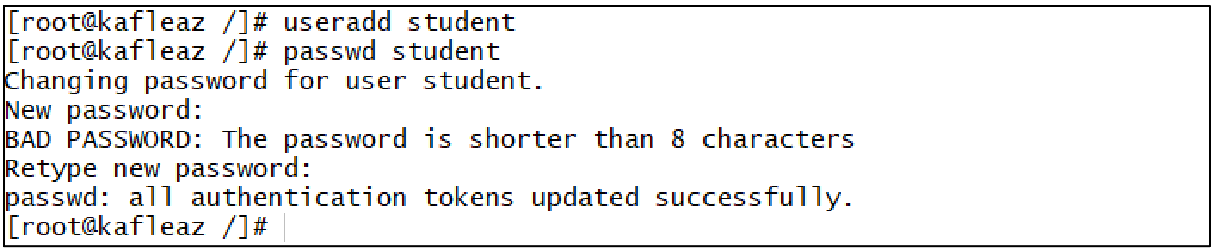


```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.0.105 kafleaz.ns.local
~
```

TASK 2

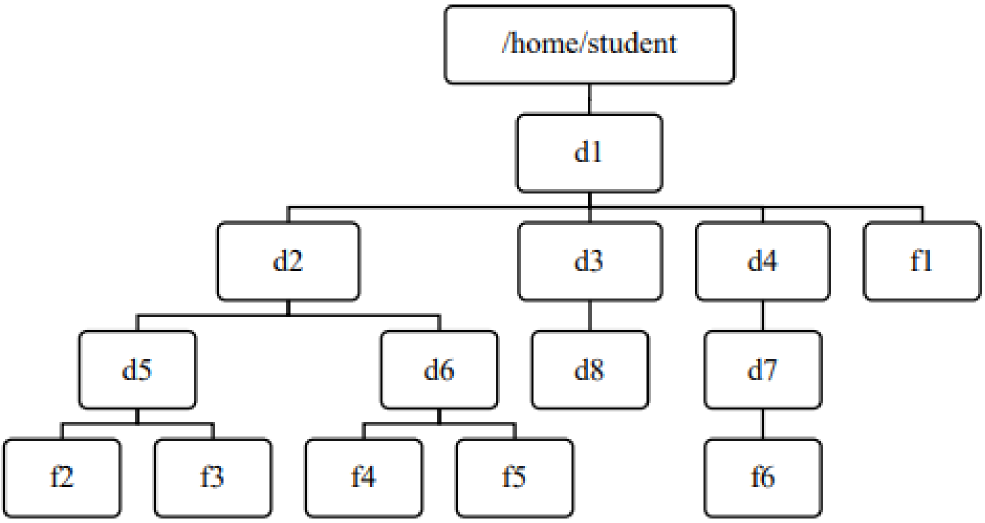
Users, Groups, Permission:

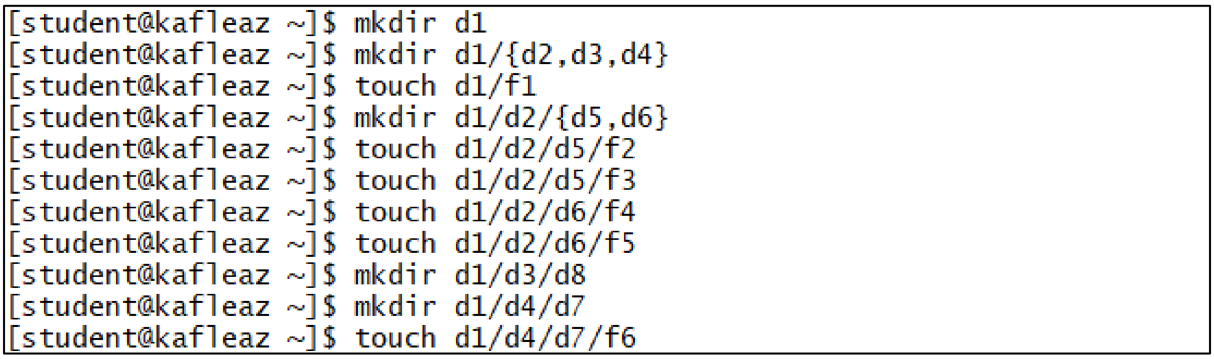
a) Create a user named student.



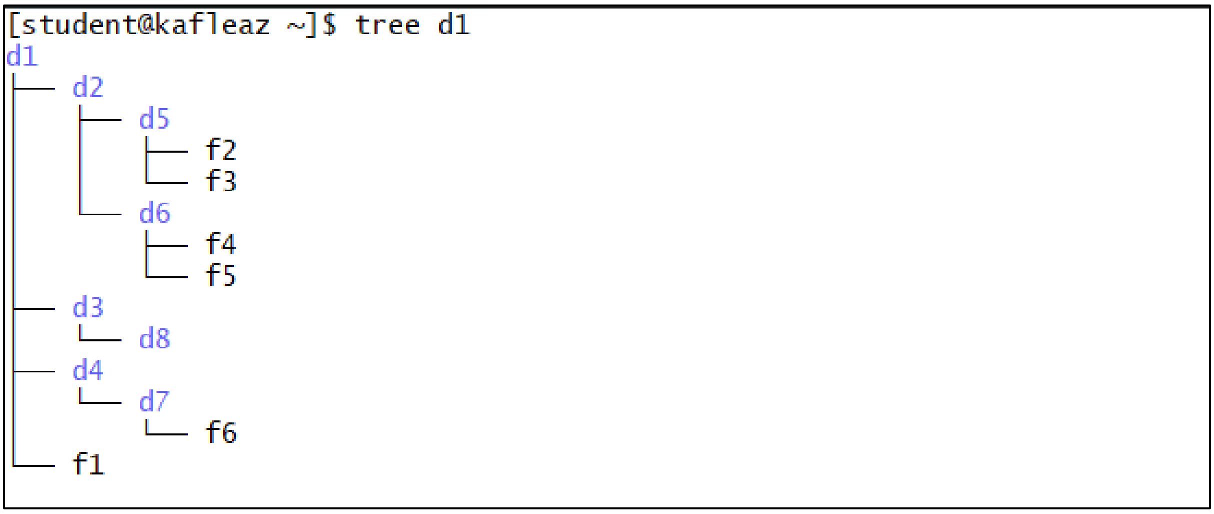
```
[root@kafleaz /]# useradd student
[root@kafleaz /]# passwd student
Changing password for user student.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@kafleaz /]#
```

b) Login from student user then create files and folders according to following tree structure. [where, d→ directory and f→ file]



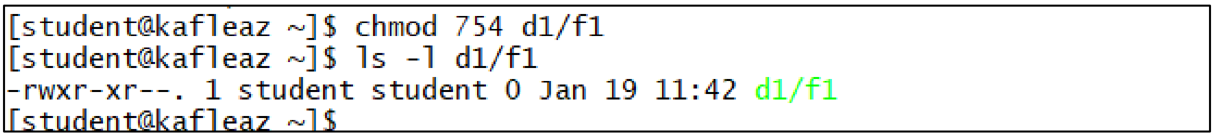


```
[student@kafleaz ~]$ mkdir d1
[student@kafleaz ~]$ mkdir d1/{d2,d3,d4}
[student@kafleaz ~]$ touch d1/f1
[student@kafleaz ~]$ mkdir d1/d2/{d5,d6}
[student@kafleaz ~]$ touch d1/d2/d5/f2
[student@kafleaz ~]$ touch d1/d2/d5/f3
[student@kafleaz ~]$ touch d1/d2/d6/f4
[student@kafleaz ~]$ touch d1/d2/d6/f5
[student@kafleaz ~]$ mkdir d1/d3/d8
[student@kafleaz ~]$ mkdir d1/d4/d7
[student@kafleaz ~]$ touch d1/d4/d7/f6
```



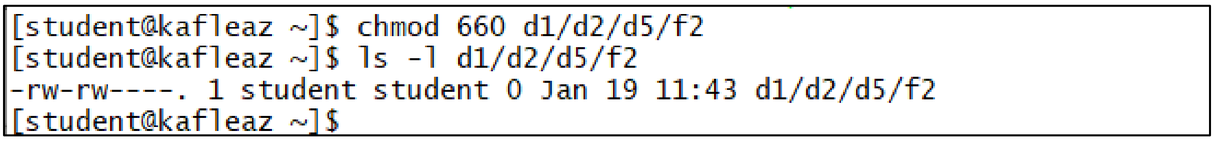
```
[student@kafleaz ~]$ tree d1
d1
├── d2
│   ├── d5
│   │   ├── f2
│   │   └── f3
│   └── d6
│       ├── f4
│       └── f5
├── d3
│   └── d8
├── d4
│   └── d7
│       └── f6
└── f1
```

c) **Change the permission of the file *f1* so that the owner will get full permission, group member will get read and execute permission and others will get read-only permissions.**



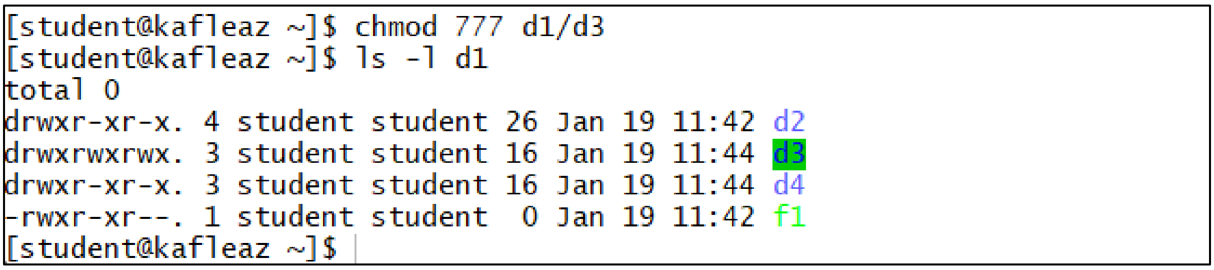
```
[student@kafleaz ~]$ chmod 754 d1/f1
[student@kafleaz ~]$ ls -l d1/f1
-rwxr-xr--. 1 student student 0 Jan 19 11:42 d1/f1
[student@kafleaz ~]$
```

d) **Change permission of the file *f2* such that the owner's and group members will get read and write permission but others will get no permission.**



```
[student@kafleaz ~]$ chmod 660 d1/d2/d5/f2
[student@kafleaz ~]$ ls -l d1/d2/d5/f2
-rw-rw----. 1 student student 0 Jan 19 11:43 d1/d2/d5/f2
[student@kafleaz ~]$
```

e) **Change permission of directory d3 such that all categories of users will get full permissions.**

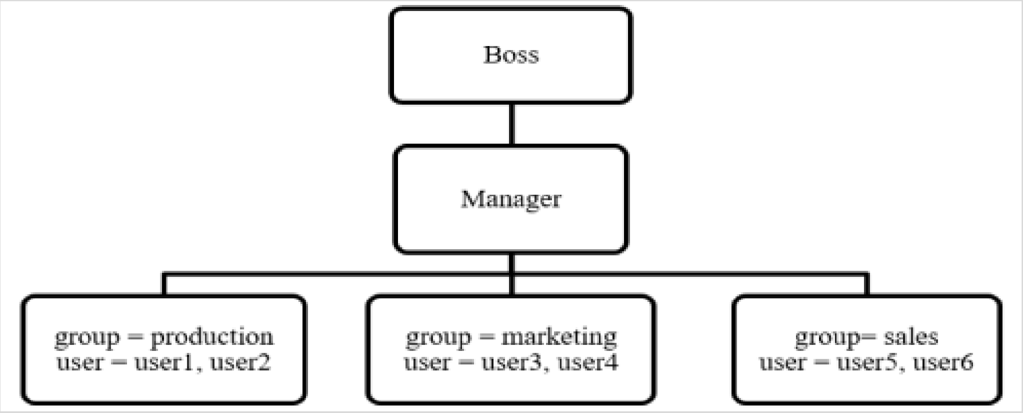


```
[student@kafleaz ~]$ chmod 777 d1/d3
[student@kafleaz ~]$ ls -l d1
total 0
drwxr-xr-x. 4 student student 26 Jan 19 11:42 d2
drwxrwxrwx. 3 student student 16 Jan 19 11:44 d3
drwxr-xr-x. 3 student student 16 Jan 19 11:44 d4
-rwxr-xr--. 1 student student  0 Jan 19 11:42 f1
[student@kafleaz ~]$
```

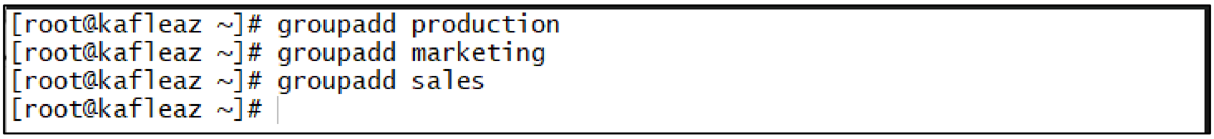
TASK 3

User and Group Administration:

Task below are based on following structure.

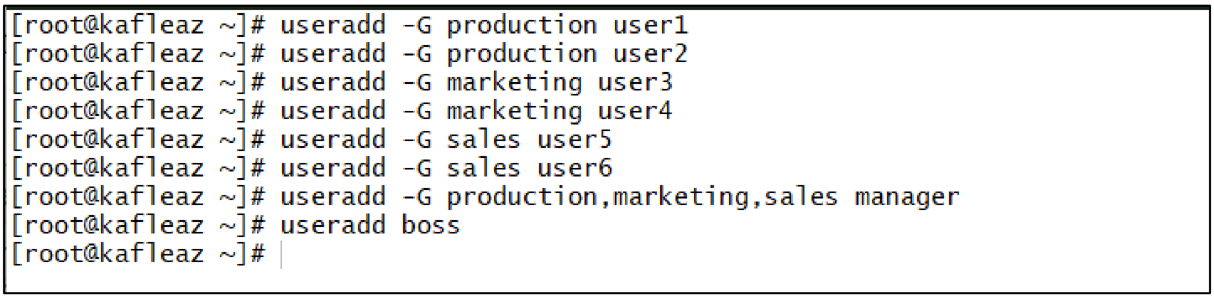


a) **Create group for each department *(production, marketing, sales).***



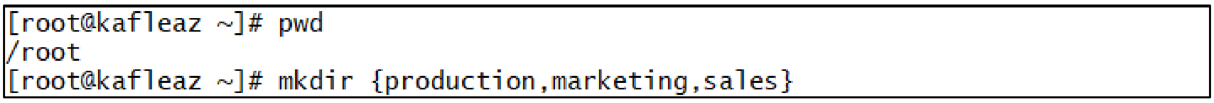
```
[root@kafleaz ~]# groupadd production
[root@kafleaz ~]# groupadd marketing
[root@kafleaz ~]# groupadd sales
[root@kafleaz ~]#
```

b) **Create user account *(user1, user2, user3, user4, user5, user6, manager, boss)* for each employee assigning them respective group.**



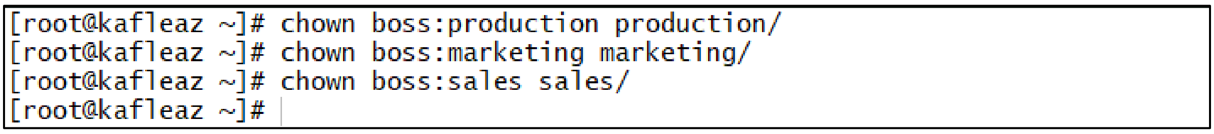
```
[root@kafleaz ~]# useradd -G production user1
[root@kafleaz ~]# useradd -G production user2
[root@kafleaz ~]# useradd -G marketing user3
[root@kafleaz ~]# useradd -G marketing user4
[root@kafleaz ~]# useradd -G sales user5
[root@kafleaz ~]# useradd -G sales user6
[root@kafleaz ~]# useradd -G production,marketing,sales manager
[root@kafleaz ~]# useradd boss
[root@kafleaz ~]#
```

c) **Create common directory (production, marketing and sales) for each department.**



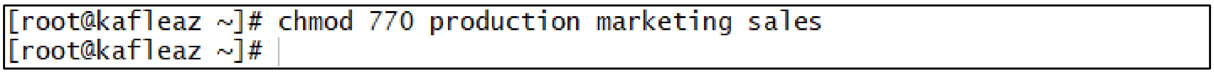
```
[root@kafleaz ~]# pwd
/root
[root@kafleaz ~]# mkdir {production,marketing,sales}
```

d) Change ownership of group directories such that boss will become the owner and the respective groups will be group owner.



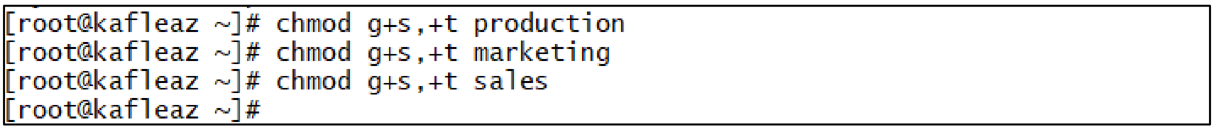
```
[root@kafleaz ~]# chown boss:production production/
[root@kafleaz ~]# chown boss:marketing marketing/
[root@kafleaz ~]# chown boss:sales sales/
[root@kafleaz ~]#
```

e) Change the permission of the group directories such that only the owner and group member will get full permission and other will not get any permission.



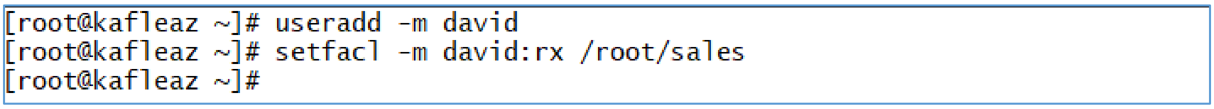
```
[root@kafleaz ~]# chmod 770 production marketing sales
[root@kafleaz ~]#
```

f) Set SGID and sticky bits on the departmental directories.



```
[root@kafleaz ~]# chmod g+s,+t production
[root@kafleaz ~]# chmod g+s,+t marketing
[root@kafleaz ~]# chmod g+s,+t sales
[root@kafleaz ~]#
```

g) Assign special permission (ACL) to anonymous called david such that it can see what’s inside the common directory for sales group i.e., /root/sales..

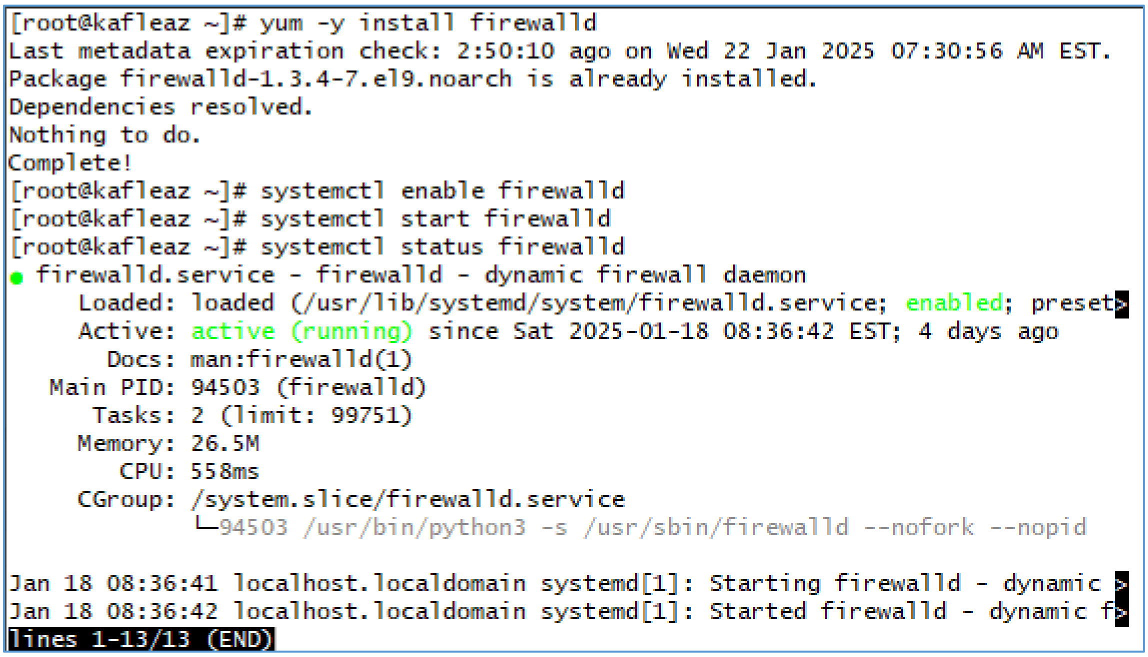


```
[root@kafleaz ~]# useradd -m david
[root@kafleaz ~]# setfacl -m david:rx /root/sales
[root@kafleaz ~]#
```

TASK 4

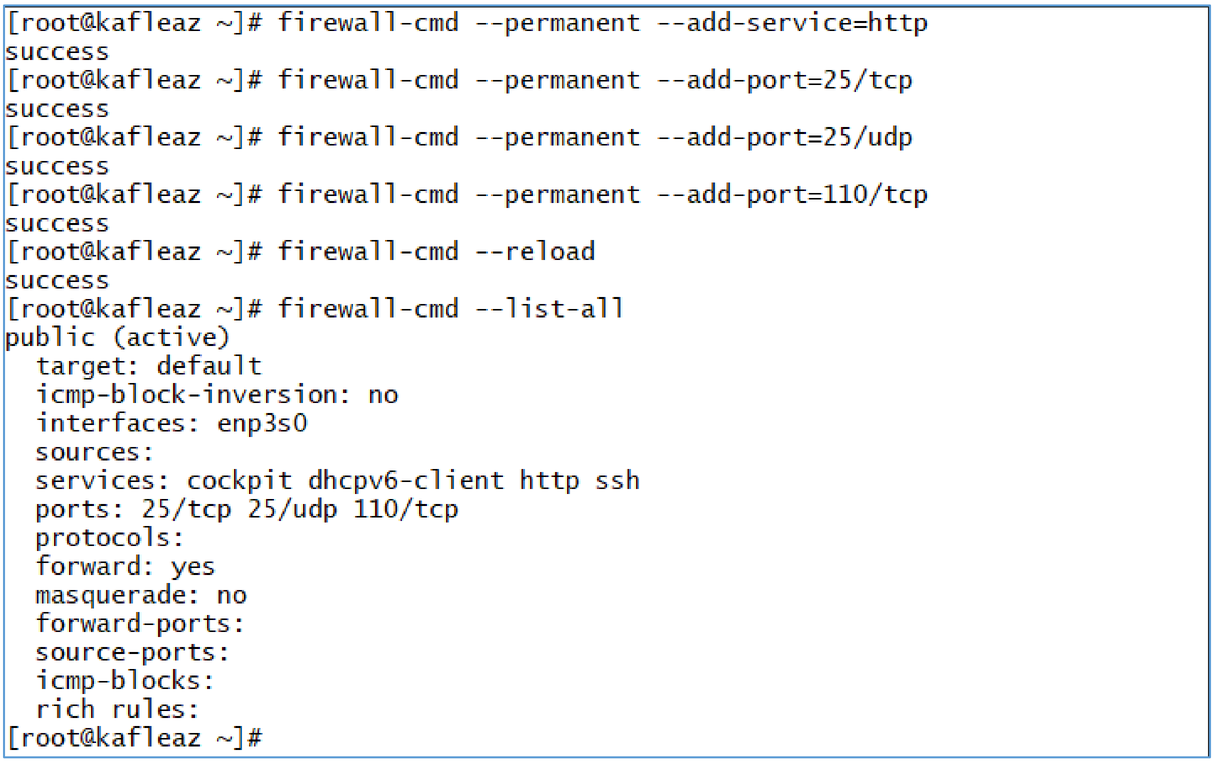
Firewall Configuration in Linux:

a) Install firewalld package as well as start and enable firewall services.



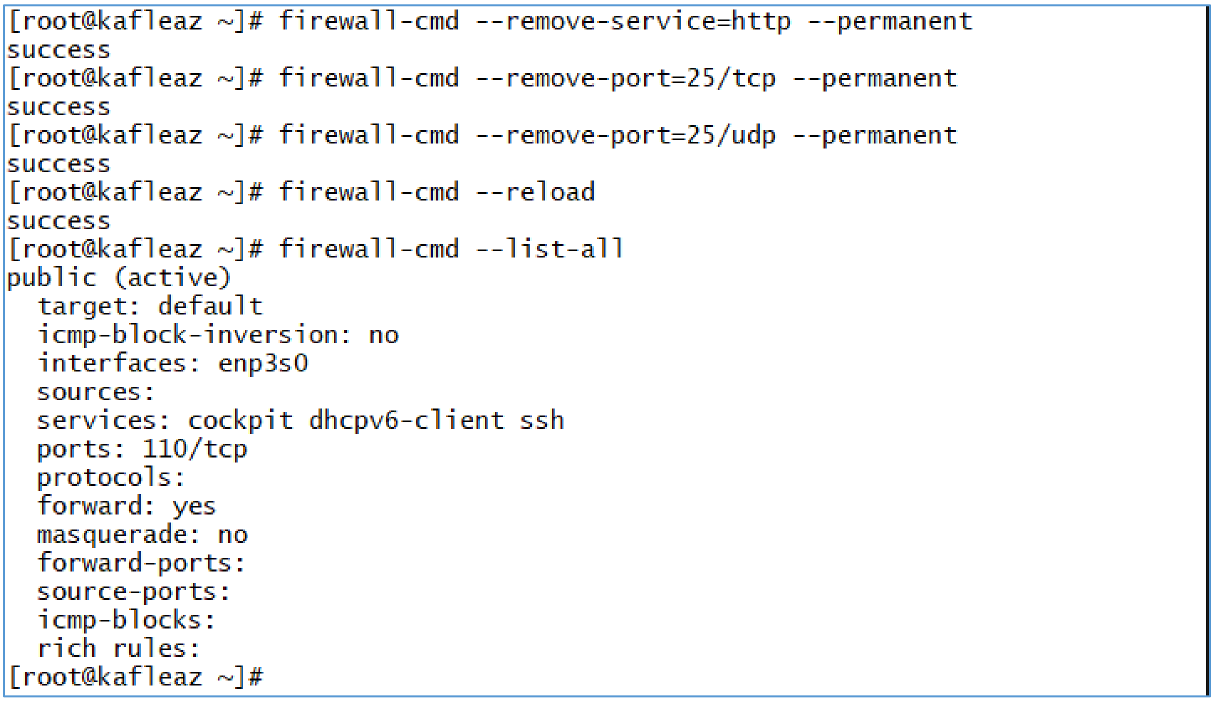
```
[root@kafleaz ~]# yum -y install firewalld
Last metadata expiration check: 2:50:10 ago on Wed 22 Jan 2025 07:30:56 AM EST.
Package firewalld-1.3.4-7.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@kafleaz ~]# systemctl enable firewalld
[root@kafleaz ~]# systemctl start firewalld
[root@kafleaz ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset>
     Active: active (running) since Sat 2025-01-18 08:36:42 EST; 4 days ago
       Docs: man:firewalld(1)
   Main PID: 94503 (firewalld)
      Tasks: 2 (limit: 99751)
     Memory: 26.5M
        CPU: 558ms
     CGroup: /system.slice/firewalld.service
             └─94503 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Jan 18 08:36:41 localhost.localdomain systemd[1]: Starting firewalld - dynamic >
Jan 18 08:36:42 localhost.localdomain systemd[1]: Started firewalld - dynamic f>
lines 1-13/13 (END)
```

b) Add the following services and ports to allow packets through the firewall. [Service = http, smtp port = 25 /tcp, 25/udp, 110/tcp].



```
[root@kafleaz ~]# firewall-cmd --permanent --add-service=http
success
[root@kafleaz ~]# firewall-cmd --permanent --add-port=25/tcp
success
[root@kafleaz ~]# firewall-cmd --permanent --add-port=25/udp
success
[root@kafleaz ~]# firewall-cmd --permanent --add-port=110/tcp
success
[root@kafleaz ~]# firewall-cmd --reload
success
[root@kafleaz ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp3s0
  sources:
  services: cockpit dhcpv6-client http ssh
  ports: 25/tcp 25/udp 110/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@kafleaz ~]#
```

c) Remove the following services and ports to block packets through the firewall. [Service = smtp port = 25 /tcp, 25/udp].

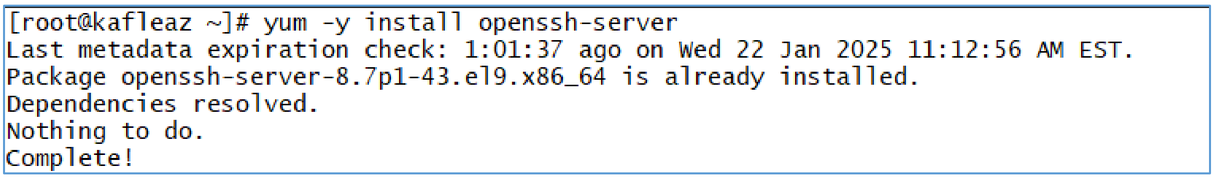


```
[root@kafleaz ~]# firewall-cmd --remove-service=http --permanent
success
[root@kafleaz ~]# firewall-cmd --remove-port=25/tcp --permanent
success
[root@kafleaz ~]# firewall-cmd --remove-port=25/udp --permanent
success
[root@kafleaz ~]# firewall-cmd --reload
success
[root@kafleaz ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp3s0
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 110/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@kafleaz ~]#
```

TASK 5

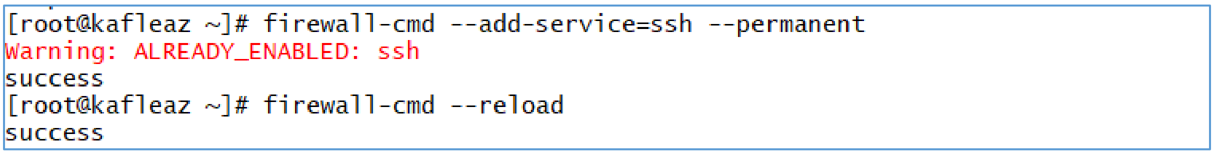
Configuring SSH Server to allow/deny root login and allow/deny users login:

a) Install required package for OpenSSH server.



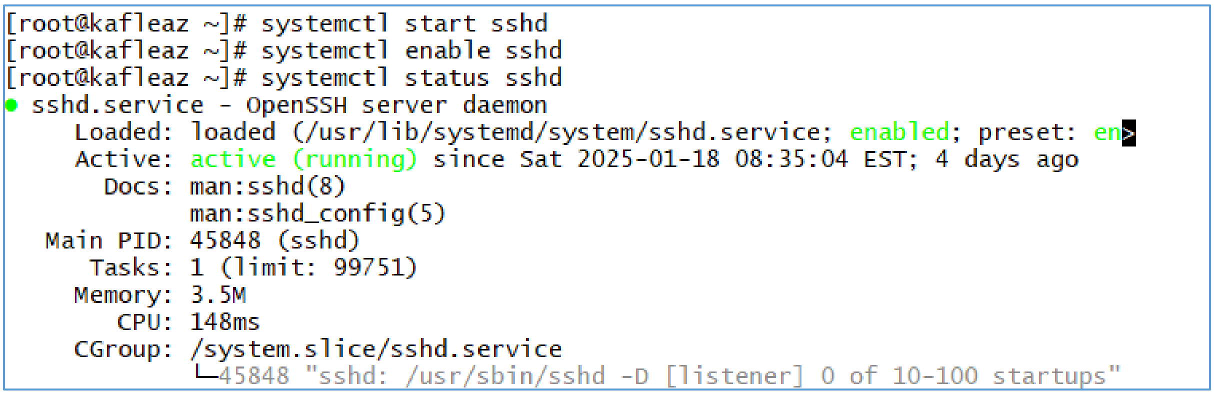
```
[root@kafleaz ~]# yum -y install openssh-server
Last metadata expiration check: 1:01:37 ago on Wed 22 Jan 2025 11:12:56 AM EST.
Package openssh-server-8.7p1-43.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

b) Allow ssh packets to enter through the firewall.



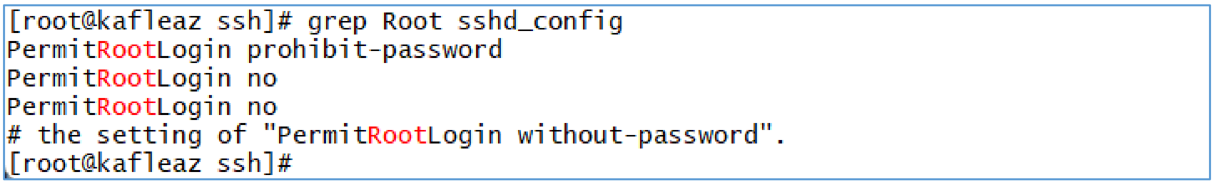
```
[root@kafleaz ~]# firewall-cmd --add-service=ssh --permanent
Warning: ALREADY_ENABLED: ssh
success
[root@kafleaz ~]# firewall-cmd --reload
success
```

c) Start and enable ssh service.

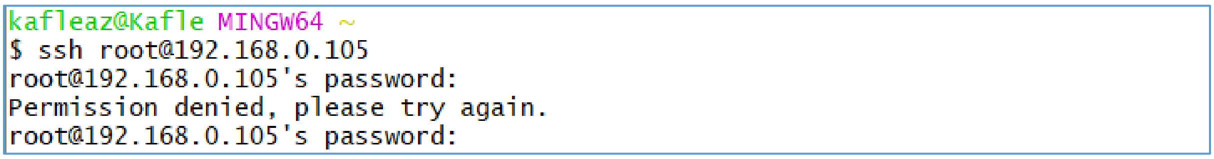


```
[root@kafleaz ~]# systemctl start sshd
[root@kafleaz ~]# systemctl enable sshd
[root@kafleaz ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: en>
     Active: active (running) since Sat 2025-01-18 08:35:04 EST; 4 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 45848 (sshd)
      Tasks: 1 (limit: 99751)
     Memory: 3.5M
        CPU: 148ms
     CGroup: /system.slice/sshd.service
             └─45848 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

d) Configure OpenSSH server to deny direct root login.



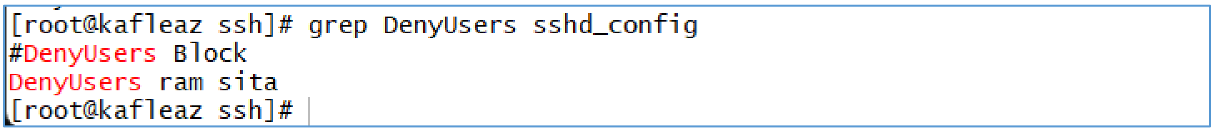
```
[root@kafleaz ssh]# grep Root sshd_config
PermitRootLogin prohibit-password
PermitRootLogin no
PermitRootLogin no
# the setting of "PermitRootLogin without-password".
[root@kafleaz ssh]#
```



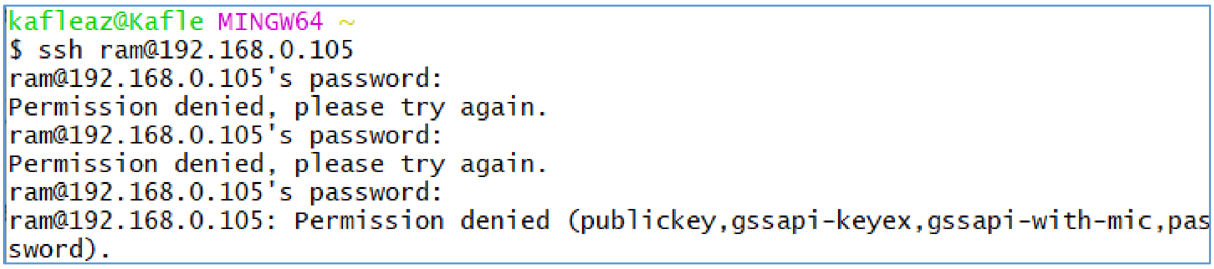
```
kafleaz@Kafle MINGW64 ~
$ ssh root@192.168.0.105
root@192.168.0.105's password:
Permission denied, please try again.
root@192.168.0.105's password:
```

e) Configure OpenSSH Server to block login from users i.e., ram, sita.

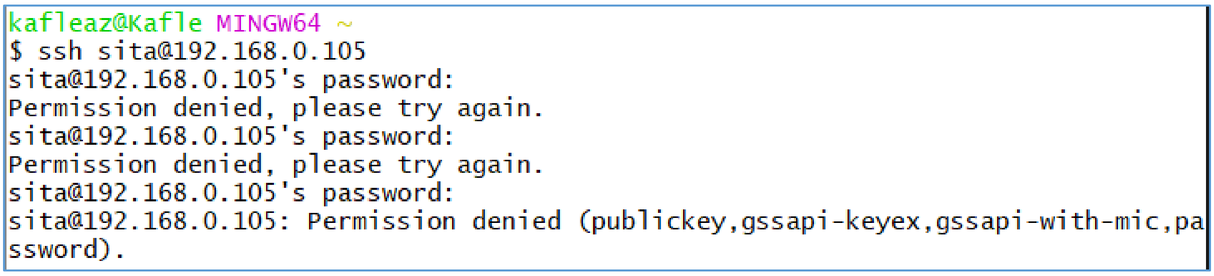
To deny logins from specific user into the server, we can modify the ‘sshd_config’ file to add a block of ‘DenyUsers’ as follows:



```
[root@kafleaz ssh]# grep DenyUsers sshd_config
#DenyUsers Block
DenyUsers ram sita
[root@kafleaz ssh]# 
```



```
kafleaz@Kafle MINGW64 ~
$ ssh ram@192.168.0.105
ram@192.168.0.105's password:
Permission denied, please try again.
ram@192.168.0.105's password:
Permission denied, please try again.
ram@192.168.0.105's password:
ram@192.168.0.105: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,pas
sword).
```



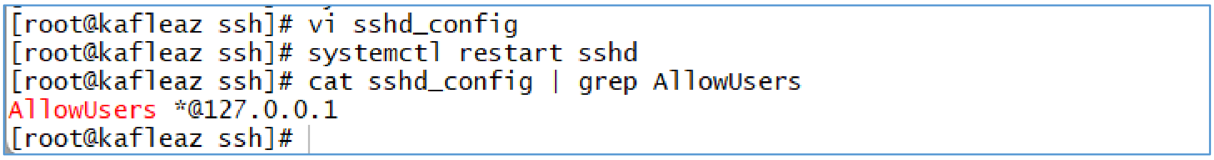
```
kafleaz@Kafle MINGW64 ~
$ ssh sita@192.168.0.105
sita@192.168.0.105's password:
Permission denied, please try again.
sita@192.168.0.105's password:
Permission denied, please try again.
sita@192.168.0.105's password:
sita@192.168.0.105: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,pa
ssword).
```

TASK 6

Configuring SSH Server to allow/deny SSH login from selected hosts only:

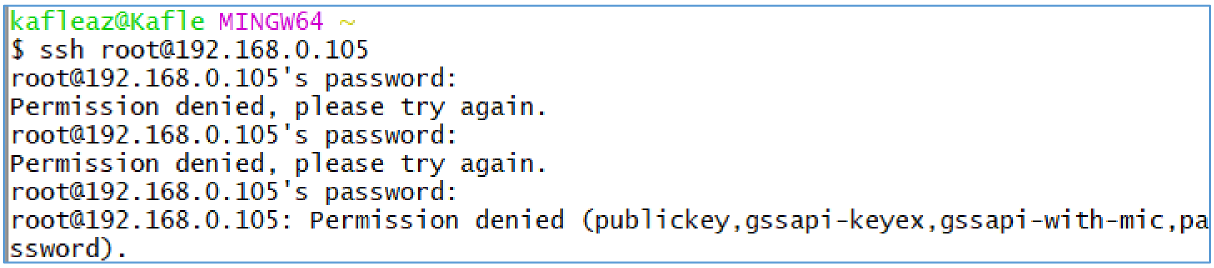
a) **Configure OpenSSH server to deny all hosts except the host (i.e., 192.168.10.10).**

First, we updated the sshd_config file by adding the following entry at the bottom of the file as:



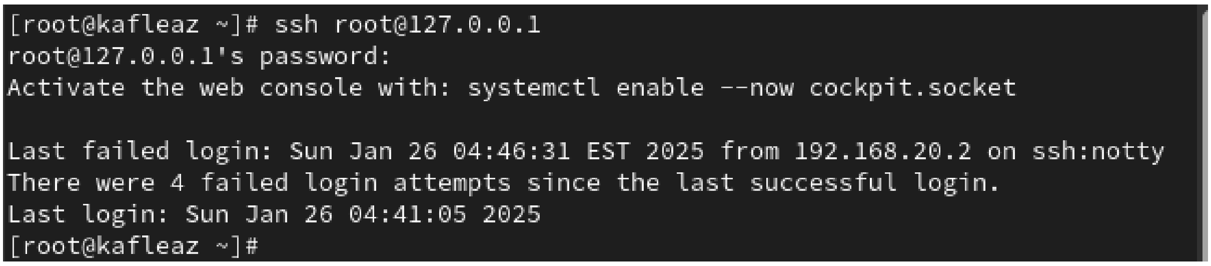
```
[root@kafleaz ssh]# vi sshd_config
[root@kafleaz ssh]# systemctl restart sshd
[root@kafleaz ssh]# cat sshd_config | grep AllowUsers
AllowUsers *@127.0.0.1
[root@kafleaz ssh]#
```

Then, we try to ssh into the machine from the host device itself as:



```
kafleaz@Kafle MINGW64 ~
$ ssh root@192.168.0.105
root@192.168.0.105's password:
Permission denied, please try again.
root@192.168.0.105's password:
Permission denied, please try again.
root@192.168.0.105's password:
root@192.168.0.105: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,pa
ssword).
```

And then, we tried from inside the virtual machine itself:

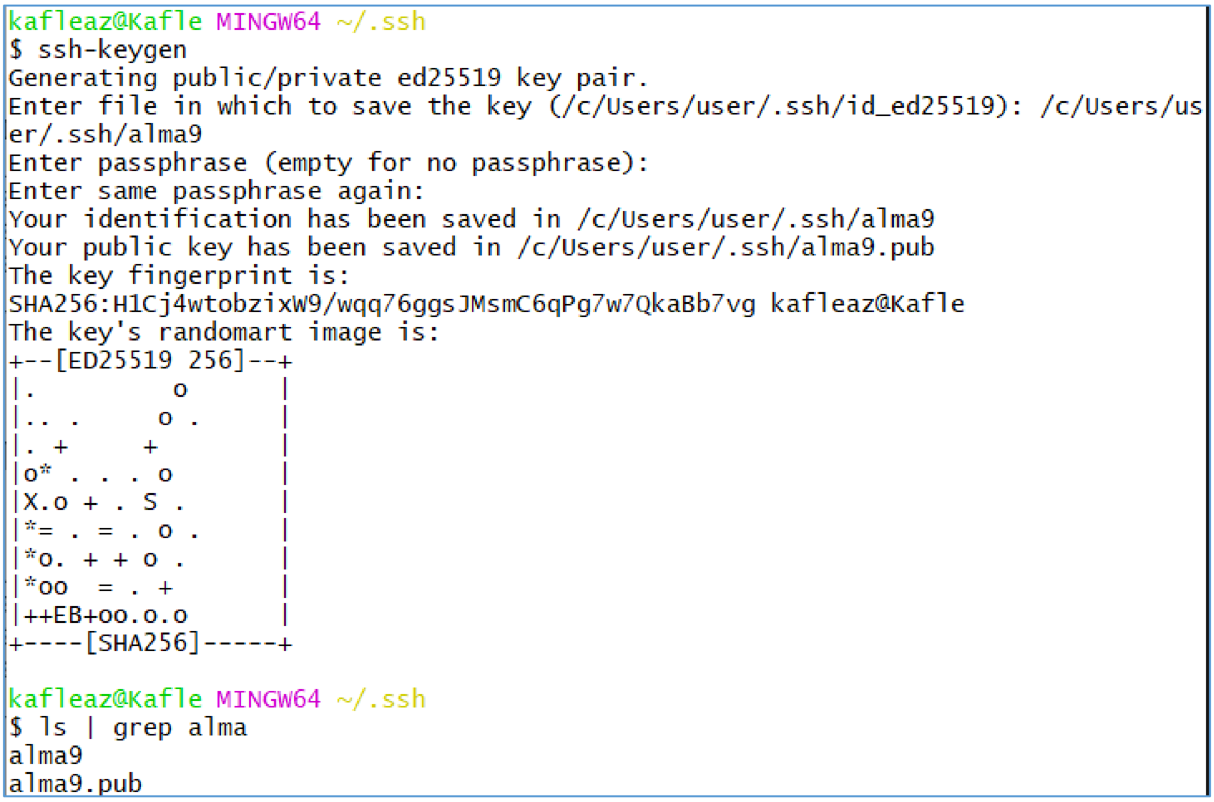


```
[root@kafleaz ~]# ssh root@127.0.0.1
root@127.0.0.1's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sun Jan 26 04:46:31 EST 2025 from 192.168.20.2 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Sun Jan 26 04:41:05 2025
[root@kafleaz ~]#
```

TASK 7

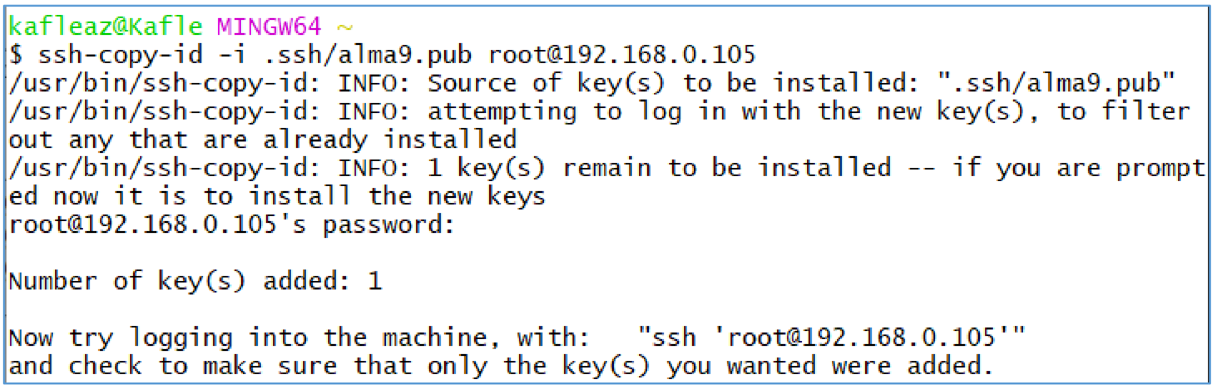
Configuring SSH Server for direct SSH login by generating and publishing private and public key:

a) **Generate SSH key pair (public and private) in local host.**



```
kafleaz@Kafle MINGW64 ~/.ssh
$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/c/Users/user/.ssh/id_ed25519): /c/Users/us
er/.ssh/alma9
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/user/.ssh/alma9
Your public key has been saved in /c/Users/user/.ssh/alma9.pub
The key fingerprint is:
SHA256:H1Cj4wtobzixW9/wqq76ggsJMsmC6qPg7w7QkaBb7vg kafleaz@Kafle
The key's randomart image is:
+--[ED25519 256]--+
|.         o      |
|.. .     o .     |
|. +     +        |
|o* . . . o       |
|X.o + . S .      |
|*= . = . o .     |
|*o. + + o .      |
|*oo  = . +       |
|++EB+oo.o.o      |
+----[SHA256]-----+

kafleaz@Kafle MINGW64 ~/.ssh
$ ls | grep alma
alma9
alma9.pub
```

b) **Send a copy of the public key to the ssh server in which you want to direct login.**



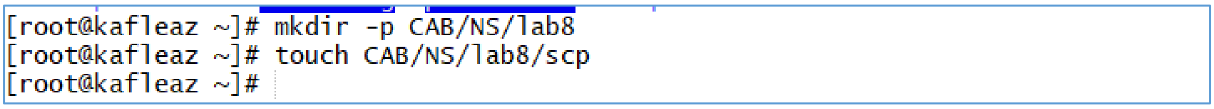
```
kafleaz@Kafle MINGW64 ~
$ ssh-copy-id -i .ssh/alma9.pub root@192.168.0.105
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/alma9.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
root@192.168.0.105's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.0.105'"
and check to make sure that only the key(s) you wanted were added.
```

TASK 8

Secure Network Copy using "SCP":

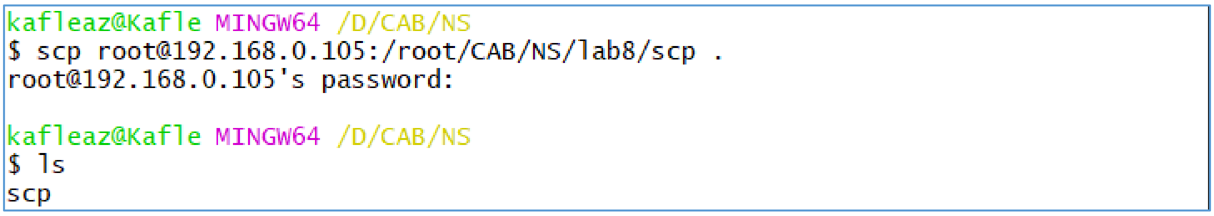
a) Copy remote file into the local system (consider your own example).

A file named "scp" is created in remote server.



```
[root@kafleaz ~]# mkdir -p CAB/NS/lab8
[root@kafleaz ~]# touch CAB/NS/lab8/scp
[root@kafleaz ~]#
```

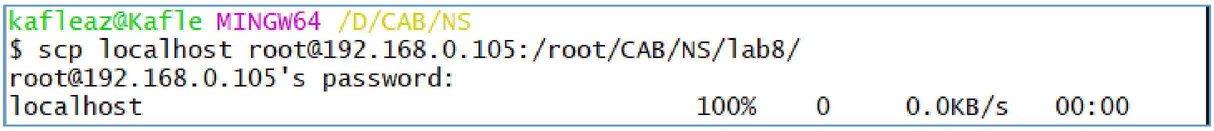
The remote file is copied into my local system using SCP



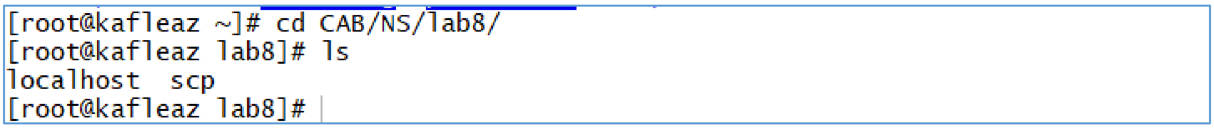
```
kafleaz@Kafle MINGW64 /D/CAB/NS
$ scp root@192.168.0.105:/root/CAB/NS/lab8/scp .
root@192.168.0.105's password:

kafleaz@Kafle MINGW64 /D/CAB/NS
$ ls
scp
```

b) Copy local files to the remote host (consider your won example).

File named "Localhost" is copied to the remote host.



```
kafleaz@Kafle MINGW64 /D/CAB/NS
$ scp localhost root@192.168.0.105:/root/CAB/NS/lab8/
root@192.168.0.105's password:
localhost                                     100%    0     0.0KB/s   00:00
```



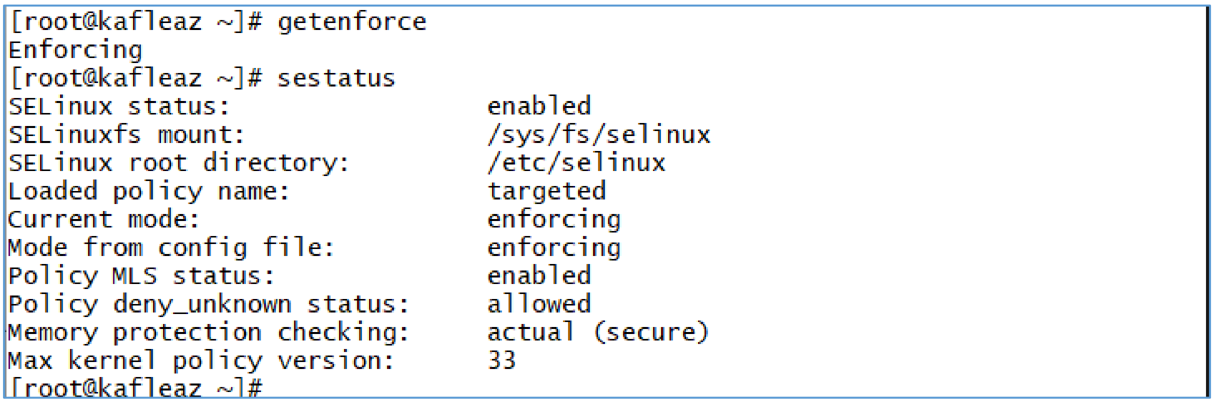
```
[root@kafleaz ~]# cd CAB/NS/lab8/
[root@kafleaz lab8]# ls
localhost  scp
[root@kafleaz lab8]#
```

TASK 9

Security Enhanced Linux (SE Linux):

a) **Check the current status of SE Linux.**

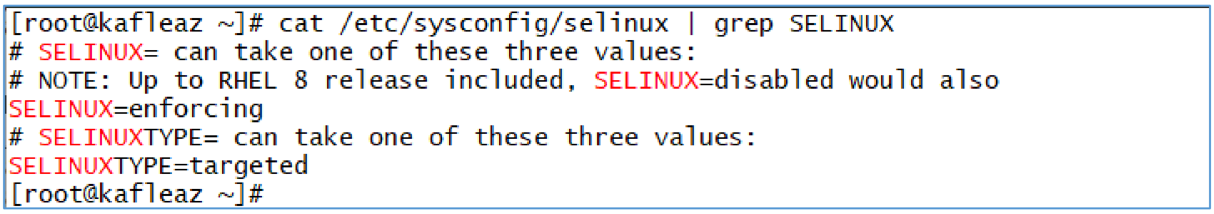
To check the status of SE Linux use can use **getenforce** or **sestatus**



```
[root@kafleaz ~]# getenforce
Enforcing
[root@kafleaz ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[root@kafleaz ~]#
```

b) **Configure the server to enable (enforcing) SE Linux.**

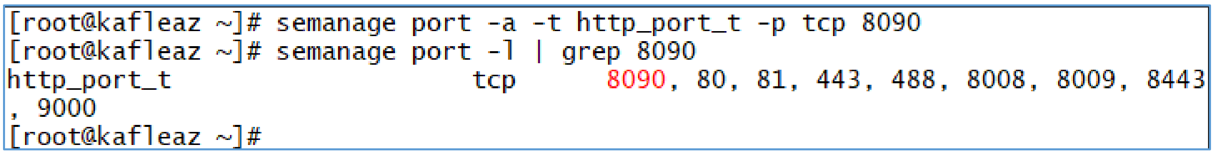
We can enable (enforcing) SE Linux by setting **SELINUX=enforcing** in file /etc/sysconfig/selinux.



```
[root@kafleaz ~]# cat /etc/sysconfig/selinux | grep SELINUX
# SELINUX= can take one of these three values:
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
SELINUXTYPE=targeted
[root@kafleaz ~]#
```

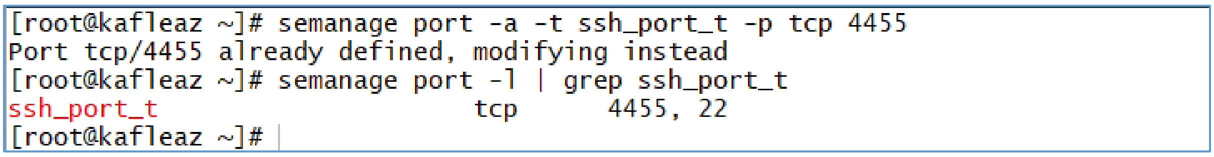
c) **Configure SELinux for a custom HTTP port 8090 and custom SSH port 4455.**

Adding a custom port 8090 for HTTP into SE Linux.



```
[root@kafleaz ~]# semanage port -a -t http_port_t -p tcp 8090
[root@kafleaz ~]# semanage port -l | grep 8090
http_port_t                    tcp      8090, 80, 81, 443, 488, 8008, 8009, 8443
, 9000
[root@kafleaz ~]#
```

Adding a custom port 4455 for custom SSH into SE Linux.

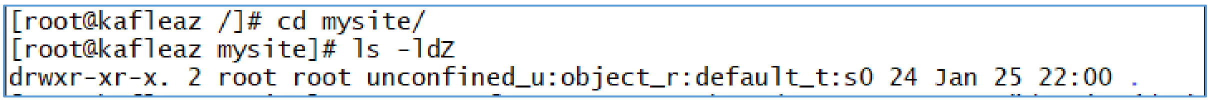


```
[root@kafleaz ~]# semanage port -a -t ssh_port_t -p tcp 4455
Port tcp/4455 already defined, modifying instead
[root@kafleaz ~]# semanage port -l | grep ssh_port_t
ssh_port_t                     tcp      4455, 22
[root@kafleaz ~]#
```

d) Change SELinux context of /mystite1 to httpd_sys_content_t using semanage and chcon respectively.

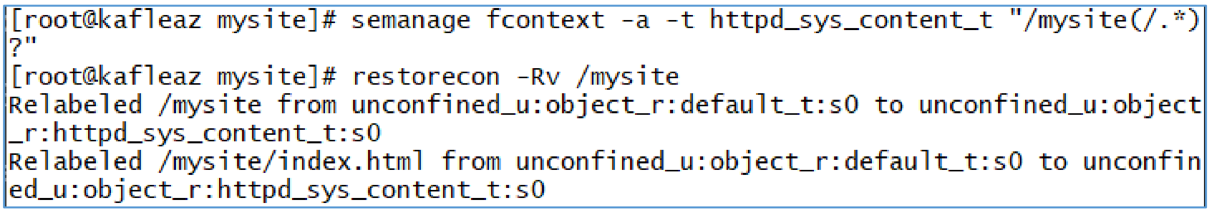
The semanage and chcon commands can be used to modify the SELinux context of files or directories. In this lab, a folder named mysite is created at the root directory (/), and a sample **index.html** file is added to it.

Next, the SELinux context **httpd_sys_content_t** is assigned to the directory, which is the default context for **/var/www/html**, the root directory of the Apache web server. Initially, the directory and its contents are as follows:



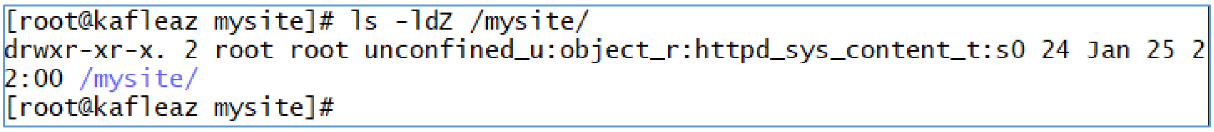
```
[root@kafleaz /]# cd mysite/
[root@kafleaz mysite]# ls -ldZ
drwxr-xr-x. 2 root root unconfined_u:object_r:default_t:s0 24 Jan 25 22:00 .
```

First, the command **semanage fcontext -a -t httpd_sys_content_t "/mysite(/.*)?"** is used to assign the **httpd_sys_content_t** context to the **/mysite** folder and all its contents. Then, the **restorecon -Rv /mysite** command is executed to apply the new context to the directory and its files.



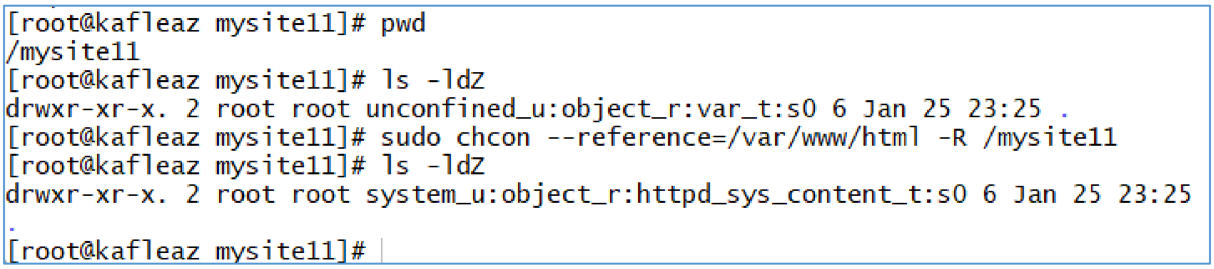
```
[root@kafleaz mysite]# semanage fcontext -a -t httpd_sys_content_t "/mysite(/.*)
?"
[root@kafleaz mysite]# restorecon -Rv /mysite
Relabeled /mysite from unconfined_u:object_r:default_t:s0 to unconfined_u:object
_r:httpd_sys_content_t:s0
Relabeled /mysite/index.html from unconfined_u:object_r:default_t:s0 to unconfin
ed_u:object_r:httpd_sys_content_t:s0
```

We can again test this by running the command **’ls -ldZ’** to check the SE Linux context as:



```
[root@kafleaz mysite]# ls -ldZ /mysite/
drwxr-xr-x. 2 root root unconfined_u:object_r:httpd_sys_content_t:s0 24 Jan 25 2
2:00 /mysite/
[root@kafleaz mysite]#
```

e) Change the SELinux context of /mysite2 using reference context of /var/www/html.

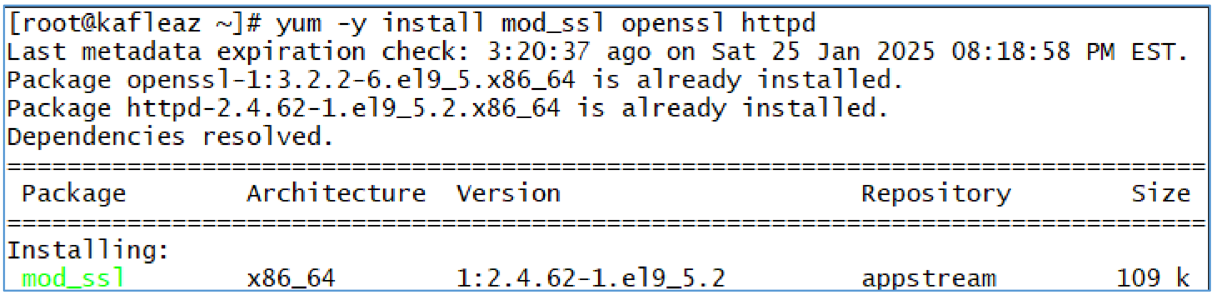


```
[root@kafleaz mysite11]# pwd
/mysite11
[root@kafleaz mysite11]# ls -ldZ
drwxr-xr-x. 2 root root unconfined_u:object_r:var_t:s0 6 Jan 25 23:25 .
[root@kafleaz mysite11]# sudo chcon --reference=/var/www/html -R /mysite11
[root@kafleaz mysite11]# ls -ldZ
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Jan 25 23:25
.
[root@kafleaz mysite11]#
```

TASK 10

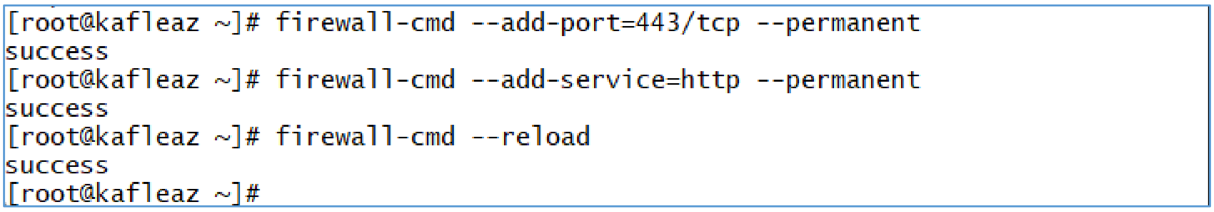
Configuring SSL-Enabled Apache (HTTPS) Server (self-signed):

a) **Install required package for HTTPS server (httpd, mod_ssl). Also, start and enable web service..**



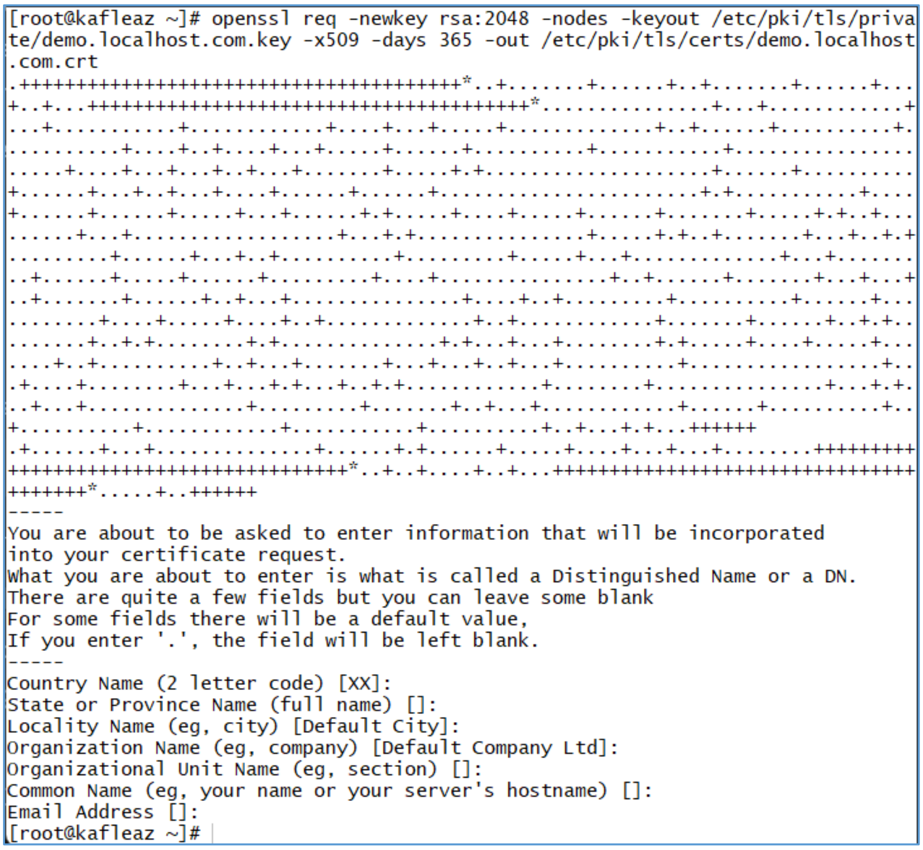
```
[root@kafleaz ~]# yum -y install mod_ssl openssl httpd
Last metadata expiration check: 3:20:37 ago on Sat 25 Jan 2025 08:18:58 PM EST.
Package openssl-1:3.2.2-6.el9_5.x86_64 is already installed.
Package httpd-2.4.62-1.el9_5.2.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package         Architecture  Version                     Repository      Size
================================================================================
Installing:
 mod_ssl         x86_64        1:2.4.62-1.el9_5.2          appstream      109 k
```

b) **Allow https (port 443) packets to enter through the firewall.**



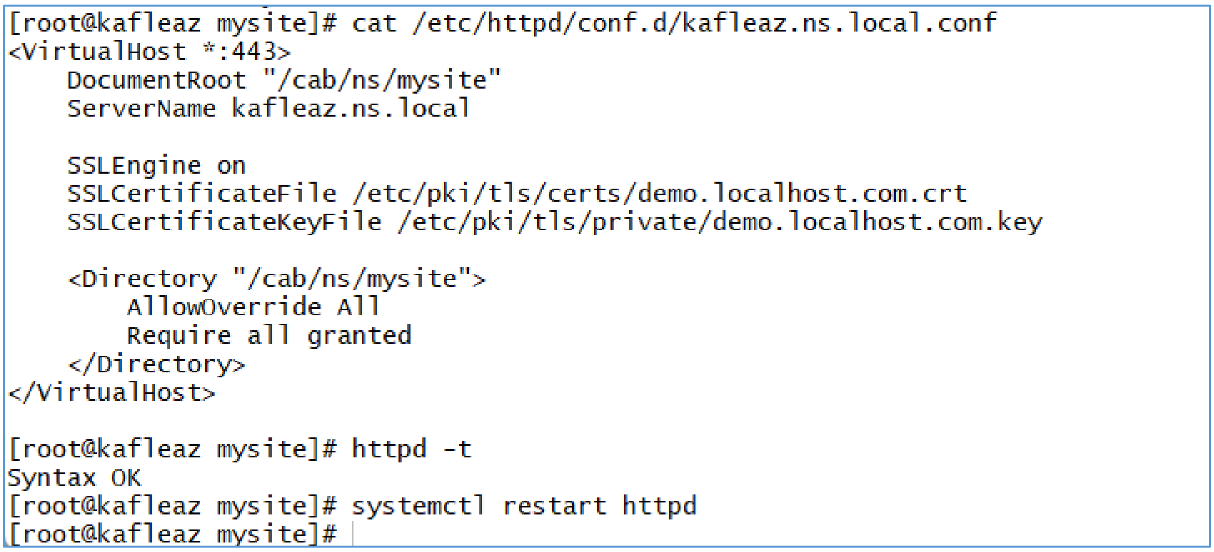
```
[root@kafleaz ~]# firewall-cmd --add-port=443/tcp --permanent
success
[root@kafleaz ~]# firewall-cmd --add-service=http --permanent
success
[root@kafleaz ~]# firewall-cmd --reload
success
[root@kafleaz ~]#
```

c) **Generate self-signed key and cert files using openssl.**

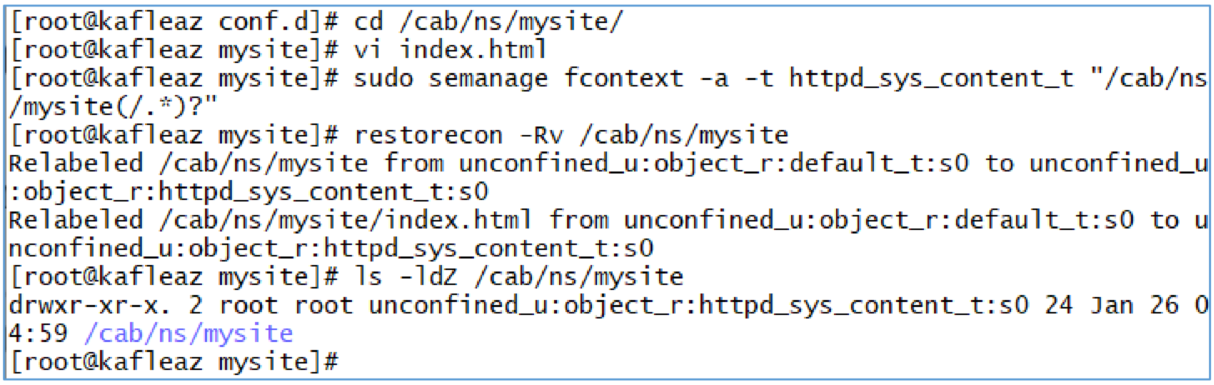


```
[root@kafleaz ~]# openssl req -newkey rsa:2048 -nodes -keyout /etc/pki/tls/priva
te/demo.localhost.com.key -x509 -days 365 -out /etc/pki/tls/certs/demo.localhost
.com.crt
.+++++++++++++++++++++++++++++++++++++++*..+........+......+..+.......+......+...
+..+...+++++++++++++++++++++++++++++++++++++++*...............+...+............+
...+...........+............+....+...+.....+.............+..+......+..........+.
..........+....+..+....+...+.....+......+..........+...........+................
.....+....+...+...+..+...+.......+.....+.+....................+......+..........
+......+...+..+...+....+......+......+.......................+.+...........+....
+......+......+.....+...+......+.+.....+....+.....+......+.......+.....+.+..+...
......+...+..................+...+.+...............+.....+.+..+.......+...+..+.+
.........+......+...+..+..........+.........+.....+...+.............+...+.......
..+......+.....+......+.........+....+...............+..+......+.......+...+...+
..+.......+......+..+...+...............+....+..+.........+..........+......+...
........+....+.....+....+..+.............+..+............+.......+......+..+.+..
.......+..+.+........+.+..............+.+...+...+........+.+.....+....+.....+...
....+..+..........+..+...+.......+...+...+..+...+..........+.................+..
.+....+........+...+...+.+...+..+.+............+........+...............+...+.+.
..+...+..............+.........+.......+..+...+............+......+..........+..
+..........+............+...........+..........+..+...+.+...++++++
.+......+...+..............+......+.+......+.....+....+...+...+........+++++++++
++++++++++++++++++++++++++++++*..+..+....+..+...++++++++++++++++++++++++++++++++
+++++++*.....+..++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
[root@kafleaz ~]#
```

d) **Configure web server to listen from port 443 and set DocumentRoot to “/cab/ns/mystie”, locate the required key and cert files. Include the necessary SELinux configuration.**

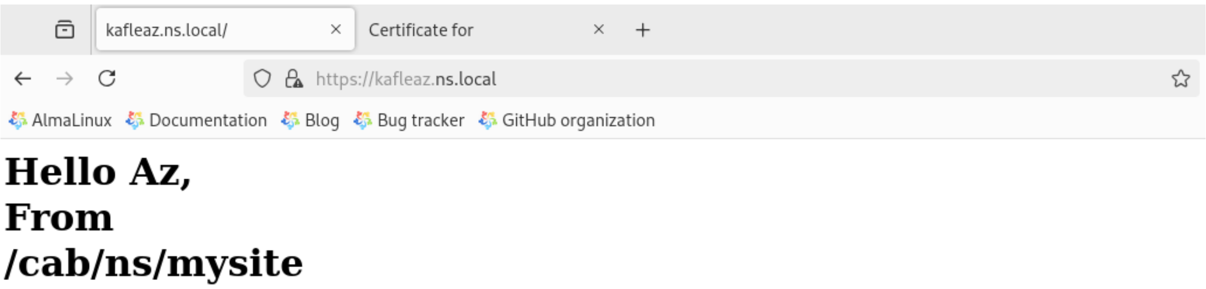


```
[root@kafleaz mysite]# cat /etc/httpd/conf.d/kafleaz.ns.local.conf
<VirtualHost *:443>
    DocumentRoot "/cab/ns/mysite"
    ServerName kafleaz.ns.local

    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/demo.localhost.com.crt
    SSLCertificateKeyFile /etc/pki/tls/private/demo.localhost.com.key

    <Directory "/cab/ns/mysite">
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>

[root@kafleaz mysite]# httpd -t
Syntax OK
[root@kafleaz mysite]# systemctl restart httpd
[root@kafleaz mysite]#
```



```
[root@kafleaz conf.d]# cd /cab/ns/mysite/
[root@kafleaz mysite]# vi index.html
[root@kafleaz mysite]# sudo semanage fcontext -a -t httpd_sys_content_t "/cab/ns
/mysite(/.*)?"
[root@kafleaz mysite]# restorecon -Rv /cab/ns/mysite
Relabeled /cab/ns/mysite from unconfined_u:object_r:default_t:s0 to unconfined_u
:object_r:httpd_sys_content_t:s0
Relabeled /cab/ns/mysite/index.html from unconfined_u:object_r:default_t:s0 to u
nconfined_u:object_r:httpd_sys_content_t:s0
[root@kafleaz mysite]# ls -ldZ /cab/ns/mysite
drwxr-xr-x. 2 root root unconfined_u:object_r:httpd_sys_content_t:s0 24 Jan 26 0
4:59 /cab/ns/mysite
[root@kafleaz mysite]#
```

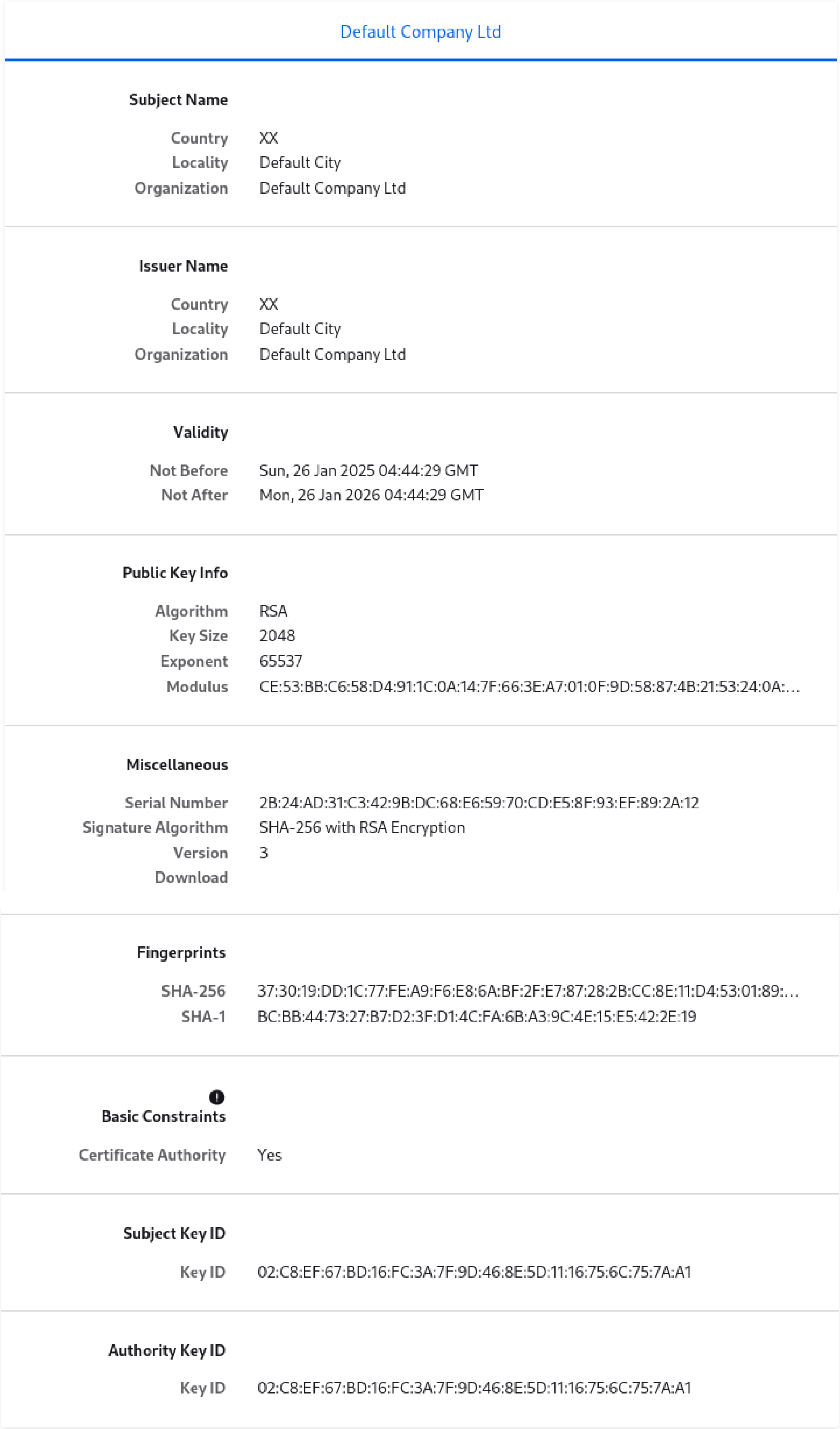
e) **Host a web page called index.html on web server named .ns.local.**



Hello Az,
From
/cab/ns/mysite

Certificate can be further inspect as:

Certificate



Default Company Ltd

Subject Name

Country	XX
Locality	Default City
Organization	Default Company Ltd

Issuer Name

Country	XX
Locality	Default City
Organization	Default Company Ltd

Validity

Not Before	Sun, 26 Jan 2025 04:44:29 GMT
Not After	Mon, 26 Jan 2026 04:44:29 GMT

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CE:53:BB:C6:58:D4:91:1C:0A:14:7F:66:3E:A7:01:0F:9D:58:87:4B:21:53:24:0A:…

Miscellaneous

Serial Number	2B:24:AD:31:C3:42:9B:DC:68:E6:59:70:CD:E5:8F:93:EF:89:2A:12
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	

Fingerprints

SHA-256	37:30:19:DD:1C:77:FE:A9:F6:E8:6A:BF:2F:E7:87:28:2B:CC:8E:11:D4:53:01:89:…
SHA-1	BC:BB:44:73:27:B7:D2:3F:D1:4C:FA:6B:A3:9C:4E:15:E5:42:2E:19

Basic Constraints

Certificate Authority	Yes

Subject Key ID

Key ID	02:C8:EF:67:BD:16:FC:3A:7F:9D:46:8E:5D:11:16:75:6C:75:7A:A1

Authority Key ID

Key ID	02:C8:EF:67:BD:16:FC:3A:7F:9D:46:8E:5D:11:16:75:6C:75:7A:A1