Name: ESCOSIA, JERICO JAMES	Date Performed: 9/15/24
Course/Section: CPE212- CPE31S21	Date Submitted:9/15/24
Instructor: Sir Valenzuela	Semester and SY: 2024-2025

Activity 3: Install SSH server on CentOS or RHEL 8

1. **Objectives:**

1.1 Install Community Enterprise OS or Red Hat Linux OS

1.2 Configure remote SSH connection from remote computer to CentOS/RHEL-8

2. **Discussion:**

CentOS vs. Debian: Overview

CentOS and Debian are Linux distributions that spawn from opposite ends of the candle.

CentOS is a free downstream rebuild of the commercial Red Hat Enterprise Linux distribution where, in contrast, Debian is the free upstream distribution that is the base for other distributions, including the Ubuntu Linux distribution.

As with many Linux distributions, CentOS and Debian are generally more alike than different; it isn't until we dig a little deeper that we find where they branch.

CentOS vs. Debian: Architecture

The available supported architectures can be the determining factor as to whether a distro is a viable option or not. Debian and CentOS are both very popular for x86_64/AMD64, but what other archs are supported by each?

Both Debian and CentOS support AArch64/ARM64, armhf/armhfp , i386 , ppc64el/ppc64le. (Note: armhf/armhfp and i386 are supported in CentOS 7 only.)

CentOS 7 additionally supports POWER9 while Debian and CentOS 8 do not. CentOS 7 focuses on the x86_64/AMD64 architecture with the other archs released through the AltArch SIG (Alternate Architecture Special Interest Group) with CentOS 8 supporting x86_64/AMD64, AArch64 and ppc64le equally.

Debian supports MIPSel, MIPS64el and s390x while CentOS does not. Much like CentOS 8, Debian does not favor one arch over another —all supported architectures are supported equally.

CentOS vs. Debian: Package Management

Most Linux distributions have some form of package manager nowadays, with some more complex and feature-rich than others.

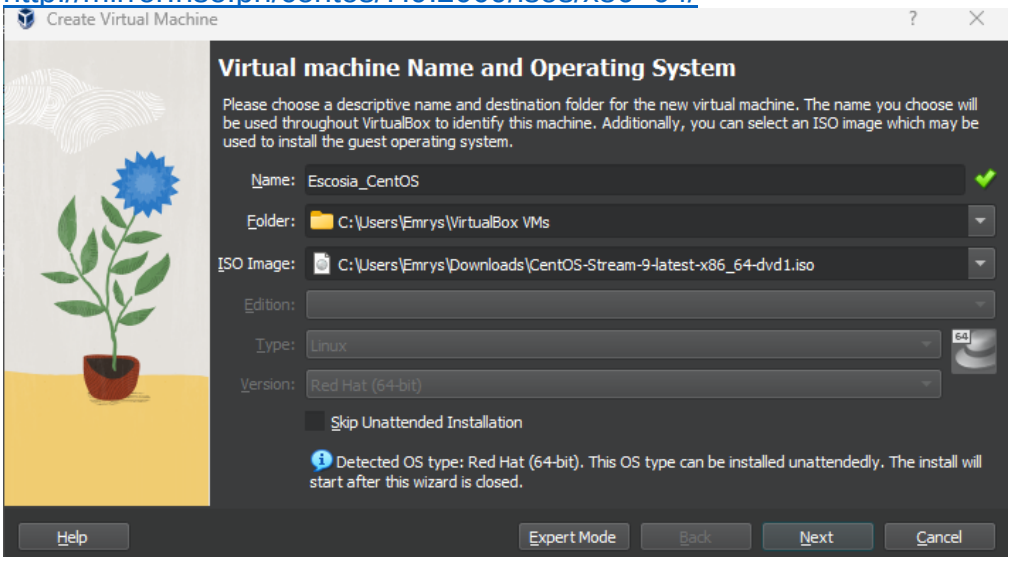
CentOS uses the RPM package format and YUM/DNF as the package manager.

Debian uses the DEB package format and dpkg/APT as the package manager.

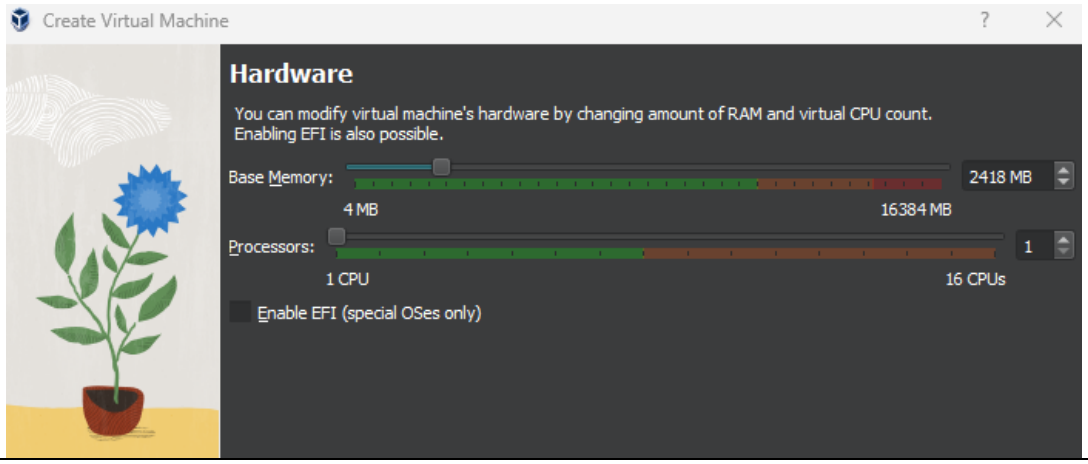
Both offer full-feature package management with network-based repository support, dependency checking and resolution, etc.. If you're familiar with one but not the other, you may have a little trouble switching over, but they're not overwhelmingly different. They both have similar features, just available through a different interface.

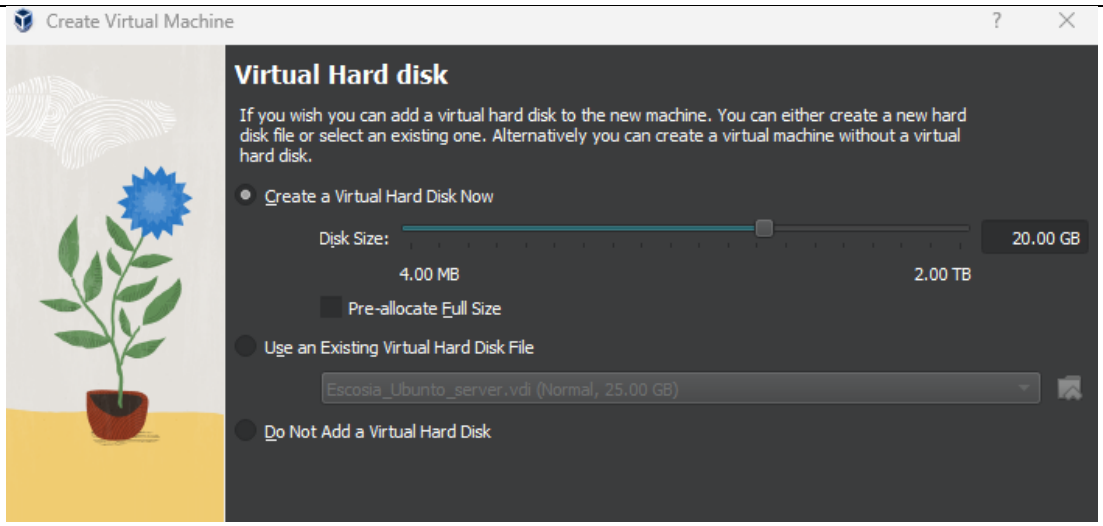
Task 1: Download the CentOS or RHEL-8 image (Create screenshots of the following)

1. Download the image of the CentOS here: http://mirror.rise.ph/centos/7.9.2009/isos/x86_64/

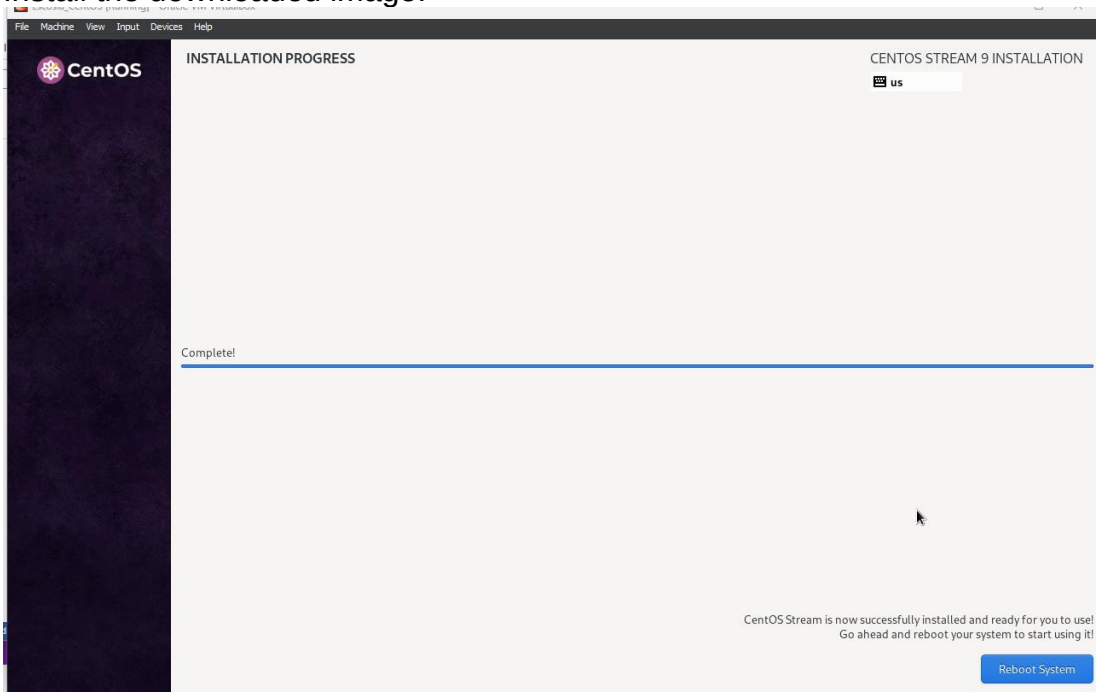


2. Create a VM machine with 2 Gb RAM and 20 Gb HD.

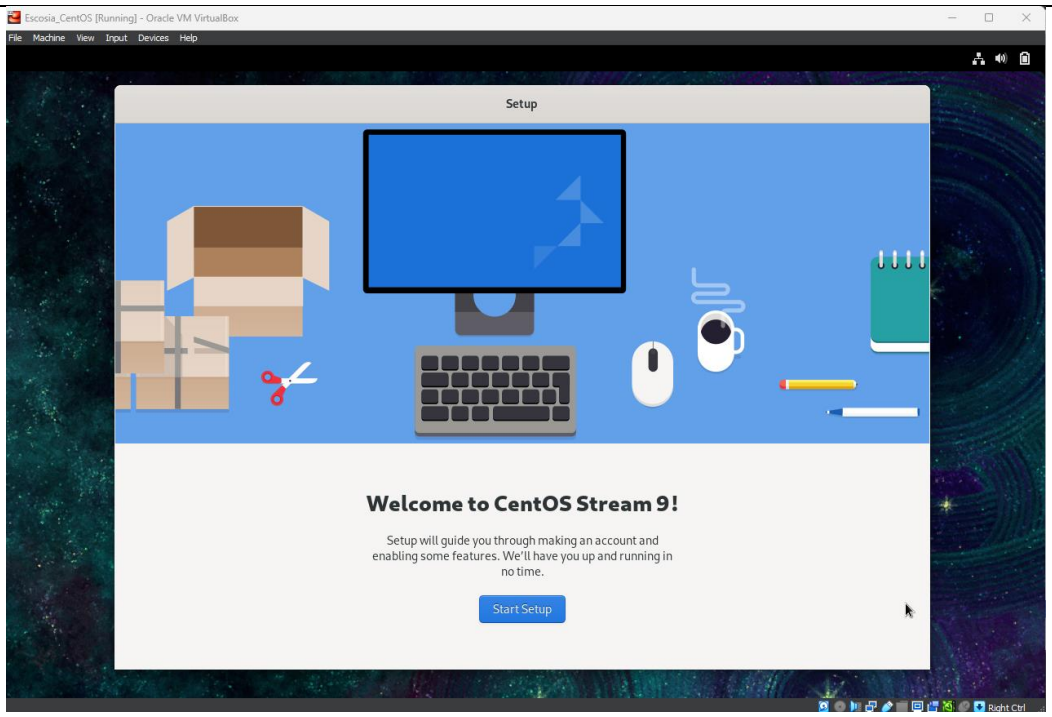




3. Install the downloaded image.



4. Show evidence that the OS was installed already.



Task 2: Install the SSH server package *openssh*

1. Install the ssh server package *openssh* by using the *dnf* command:
   $ dnf install openssh-server

```
[root@localhost qjjescosia]# dnf install openssh-server
Updating Subscription Management repositories.
Unable to read consumer identity

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

Last metadata expiration check: 0:56:46 ago on Fri 06 Sep 2024 09:54:39 AM PST.
Package openssh-server-8.7p1-43.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

2. Start the *sshd* daemon and set to start after reboot:
   $ systemctl start sshd
   $ systemctl enable sshd

```
[root@localhost qjjescosia]# systemctl start sshd
[root@localhost qjjescosia]# systemctl enable sshd
[root@localhost qjjescosia]# systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: ena>
     Active: active (running) since Fri 2024-09-06 09:27:46 PST; 1h 29min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 925 (sshd)
      Tasks: 1 (limit: 13256)
     Memory: 2.3M
        CPU: 14ms
     CGroup: /system.slice/sshd.service
             └─925 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

3. Confirm that the sshd daemon is up and running:
   $ systemctl status sshd

```
[root@localhost qjjescosia]# systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: ena>
     Active: active (running) since Fri 2024-09-06 09:27:46 PST; 1h 29min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 925 (sshd)
      Tasks: 1 (limit: 13256)
     Memory: 2.3M
        CPU: 14ms
     CGroup: /system.slice/sshd.service
             └─925 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

4. Open the SSH port 22 to allow incoming traffic:
   $ firewall-cmd --zone=public --permanent --add-service=ssh
   $ firewall-cmd –reload

```
[root@localhost qjjescosia]# firewall-cmd --zone=public --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
[root@localhost qjjescosia]# firewall-cmd --reload
success
[root@localhost qjjescosia]#
```

5. Locate the ssh server man config file /*etc/ssh/sshd_config* and perform custom configuration. Every time you make any change to the /*etc/ssh/sshd-config* configuration file reload the *sshd* service to apply changes:
   $ systemctl reload sshd

```
[root@localhost qjjescosia]# sudo cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a  *.conf  file under
#  /etc/ssh/sshd_config.d/  which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

Task 3: Copy the Public Key to CentOS

1. Make sure that *ssh* is installed on the local machine.
2. Using the command *ssh-copy-id*, connect your local machine to CentOS.

```
[root@localhost centos1]# ssh-keycopy centos1@192.168.56.106
bash: ssh-keycopy: command not found...
[root@localhost centos1]# ssh-copy-id centos1@192.168.56.106
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.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 prompted now it is to install
the new keys
centos1@192.168.56.106's password:
```

3. On CentOS, verify that you have the *authorized_keys*.

```
[root@centos1 .ssh]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCya52l/Qopxcss5CGkb+ZmJ+vIThanbX3TxNbA8BH1J1dn1THKOm
fGVkyy34kqBFIpIIHtsd9D29Lr2l882TO2d3paUD/K3UEh1FRlj7KqilWxdUkH9khdxb8mS1uPHitP/Wpb/oCAhdaP
NSgi1ZhDjMg6Hn+07K5MEJQSVDcNVttb+E2K1NSnwuVcwDZSKrF3tNPYd5xZawJF5p2LLQqjUVxXYcTQb3S2rvzUno
SA9VOozTlEZ5Tp9dksd7HY0HWVl7tRXz9QkeK0yZgJA0Si80gGOp/q948SJjkfnN2Wfe1zW2f/8atB+Pz4SZg5xwSv
7700nA7MgJOdvenfASmJYnxA/ZbcPf2MFL6USv0/9666OeITYRPYsBYI4mydSUqqlMCzRQCyYPKPYbaMYt/MHq+lrA
DDpTU87bh6ukNFEL34N/brabpkHPnSxdJN2HyxdkzAujdpTc6h8bg1zI0uCeCYQbfxxAFyoBbKSnGYk78U4ivZS9zl
m1ahsYeAme1FTP/aHZNGfgDJuXu99dNv+3Kgrq7+ByryisuibnRdzO/rsFHdQwa3ry1T6qI2ngaqTGVr4k0K325xUW
Gz9uQSNI11pIjV2DgkCfMviy8duxNDzLmpeFCHVj5LJEXlWtYfzbhJFWxLgRxTIav2I4qmchseOeH9U+fj29DmPT/U
3w== root@centos1
```

Task 4: Verify ssh remote connection

1. Using your local machine, connect to CentOS using ssh.
2. Show evidence that you are connected.

```
root@workstation:/home/workstation# ssh workstation@192.168.56.113
The authenticity of host '192.168.56.113 (192.168.56.113)' can't be established.
ED25519 key fingerprint is SHA256:1GeTjfxcz15dHZzasXhX+A+Ou0WM8uKJBAHNXVoDp/E.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.113' (ED25519) to the list of known hosts.
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

0 updates can be applied immediately.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Sep 15 15:49:38 2024 from 192.168.56.106
workstation@centos1:~$
```

Reflections:

Answer the following:

1. What do you think we should look for in choosing the best distribution between Debian and Red Hat Linux distributions?

   -In looking for the best linux distribution you should choose one on what you need it for, if you want a cost-effective and more community base, Debian is the best one. Red Hat on the other hand is for commercial support and predictable updates caters to mostly enterprises.

2. What are the main diffence between Debian and Red Hat Linux distributions?

   -Debian and Red Hat handle package management differently. Debian, known for its stability, uses apt and dpkg for managing packages. In contrast, Red Hat provides commercial support through a subscription model and ensures a predictable release schedule with long-term support, using rpm and yum/dnf for package management. In short, Red Hat focuses on stability and expert support, while Debian is better suited for more varied environments.