Exercise 1 – Installing and Configuring the SSH Server and Client

Verification of the installation and functionality of the OpenSSH server

Exercise 1.1: Tasks to Perform on AlmaLinux:

1. Verify that the **OpenSSH server** is installed and started on the **AlmaLinux server.**

   dnf list openssh-server

```
[mperez@server1 ~]$ dnf list openssh-server
AlmaLinux 9 - AppStream                                          36 MB/s |  15 MB     00:00
AlmaLinux 9 - BaseOS                                             41 MB/s |  17 MB     00:00
AlmaLinux 9 - Extras                                            104 kB/s |  13 kB     00:00
Extra Packages for Enterprise Linux 9 - x86_64                   13 MB/s |  23 MB     00:01
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64  5.1 kB/s | 2.5 kB     00:00
Installed Packages
openssh-server.x86_64                    8.7p1-43.el9.alma.2                                  @baseos
[mperez@server1 ~]$
```

Installed package openssh-server.x86_64 being listed as installed with version 8.7p1-43.el9.alma.2.

systemctl status sshd

used to check the status of the OpenSSH server daemon (`sshd`)

```
openssh-server.x86_64
[mperez@server1 ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-27 22:32:22 EDT; 3 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 996 (sshd)
      Tasks: 1 (limit: 22829)
     Memory: 2.7M
        CPU: 11ms
     CGroup: /system.slice/sshd.service
             └─996 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 27 22:32:22 server1 systemd[1]: Starting OpenSSH server daemon...
Mar 27 22:32:22 server1 sshd[996]: Server listening on 0.0.0.0 port 22.
Mar 27 22:32:22 server1 sshd[996]: Server listening on :: port 22.
Mar 27 22:32:22 server1 systemd[1]: Started OpenSSH server daemon.
[mperez@server1 ~]$
```

2. Identify the folder that contains the SSH daemon **(sshd)** configuration files.

   The SSH daemon configuration files are located in:

   cd /etc/sshd

   ll -a

```
[mperez@server1 ssh]$ ll -a
total 616
drwxr-xr-x.   4 root root       4096 Mar  1 03:47 .
drwxr-xr-x. 139 root root       8192 Mar 30 23:17 ..
-rw-r--r--.   1 root root     578094 Mar  1 03:46 moduli
-rw-r--r--.   1 root root       1921 Mar  1 03:46 ssh_config
drwxr-xr-x.   2 root root         28 Mar  1 03:47 ssh_config.d
-rw-------.   1 root root       3667 Mar  1 03:46 sshd_config
drwx------.   2 root root         28 Mar  1 03:47 sshd_config.d
-rw-r-----.   1 root ssh_keys    480 Mar 24 14:21 ssh_host_ecdsa_key
-rw-r--r--.   1 root root        162 Mar 24 14:21 ssh_host_ecdsa_key.pub
-rw-r-----.   1 root ssh_keys    387 Mar 24 14:21 ssh_host_ed25519_key
-rw-r--r--.   1 root root         82 Mar 24 14:21 ssh_host_ed25519_key.pub
-rw-r-----.   1 root ssh_keys   2578 Mar 24 14:21 ssh_host_rsa_key
-rw-r--r--.   1 root root        554 Mar 24 14:21 ssh_host_rsa_key.pub
[mperez@server1 ssh]$ ll
total 600
```

3. What is the name of the **main configuration file used** by the sshd server?

   /etc/ssh/sshd_config

```
mperez@server1 ssh]$ sudo cat sshd_config | more
[sudo] password for mperez:
#       $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

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile    .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnablek5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

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

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
[mperez@server1 ssh]$
```

4. How many **public/private keys** does this server have?

   ll /etc/ssh/ssh_host_*

```
[mperez@server1 ssh]$ ll /etc/ssh/ssh_host_*
-rw-r-----. 1 root ssh_keys  480 Mar 24 14:21 /etc/ssh/ssh_host_ecdsa_key
-rw-r--r--. 1 root root      162 Mar 24 14:21 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r-----. 1 root ssh_keys  387 Mar 24 14:21 /etc/ssh/ssh_host_ed25519_key
-rw-r--r--. 1 root root       82 Mar 24 14:21 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r-----. 1 root ssh_keys 2578 Mar 24 14:21 /etc/ssh/ssh_host_rsa_key
-rw-r--r--. 1 root root      554 Mar 24 14:21 /etc/ssh/ssh_host_rsa_key.pub
[mperez@server1 ssh]$
```

Three pairs of public/private keys, corresponding to different cryptographic algorithms:

a. ECDSA (Elliptic Curve Digital Signature Algorithm)
- Private Key: `/etc/ssh/ssh_host_ecdsa_key`
- Public Key: `/etc/ssh/ssh_host_ecdsa_key.pub`

b. Ed25519 (Edwards-curve Digital Signature Algorithm)
- Private Key: `/etc/ssh/ssh_host_ed25519_key`
- Public Key: `/etc/ssh/ssh_host_ed25519_key.pub`

c. RSA (Rivest-Shamir-Adleman Algorithm)
- Private Key: `/etc/ssh/ssh_host_rsa_key`
- Public Key: `/etc/ssh/ssh_host_rsa_key.pub`

5. Type the following command and leave it listening:
   sudo tcpdump -i *ens192* -XX -s 0 tcp port 22 *(where **ens192** is the name of the interface connected to the Ubuntu machine)*

```
[mperez@server1 ~]$ sudo tcpdump -i ens192 -XX -s 0 tcp port 22 -w tcpdump_ssh.pcap
dropped privs to tcpdump
tcpdump: listening on ens192, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Get the IP for LAN1 and interface name

```
bash: alma: command not found...
[mperez@server1 ssh]$ nmcli
ens160: connected to ens160
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:0C:29:E7:F8:DA, hw, mtu 1500
        ip4 default
        inet4 192.168.204.128/24
        route4 192.168.204.0/24 metric 100
        route4 default via 192.168.204.2 metric 100
        inet6 fe80::20c:29ff:fee7:f8da/64
        route6 fe80::/64 metric 1024

ens192: connected to LAN1
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:0C:29:E7:F8:E4, hw, mtu 1500
        inet4 192.168.50.10/24
        route4 192.168.50.0/24 metric 101
        route4 default via 192.168.50.1 metric 101
        inet6 fe80::3e70:81df:4f1a:15be/64
        route6 fe80::/64 metric 1024

lo: connected (externally) to lo
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536
        inet4 127.0.0.1/8
        inet6 ::1/128

DNS configuration:
        servers: 192.168.204.2
        domains: localdomain
        interface: ens160

        servers: 8.8.8.8
        interface: ens192

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(7) manual pages for complete usage details.
[mperez@server1 ssh]$
```

6. Leave the **AlmaLinux** session open and switch to the **Ubuntu** machine.

Verification of the installation and functionality of the OpenSSH client

Exercise 1.2: Tasks to Perform on Ubuntu and AlmaLinux:

1. Verify that the **OpenSSH client** is installed on the **Ubuntu** system.

   sudo apt list openssh-client

```
mperez@client1:~$ sudo apt list openss
openssh-client        openssh-known-hosts  openssh-sftp-server  openssl              openssn-data
openssh-client-ssh1   openssh-server       openssh-tests        openssn
mperez@client1:~$ sudo apt list openssh-client
[sudo] password for mperez:
Listing... Done
openssh-client/jammy-updates,jammy-security,now 1:8.9p1-3ubuntu0.11 amd64 [installed]
openssh-client/jammy-updates,jammy-security 1:8.9p1-3ubuntu0.11 i386
mperez@client1:~$
```

openssh-client` package is installed on Ubuntu system with version 1:8.9p1-3ubuntu0.11

2. From the **Ubuntu** client, use the **ssh** command to connect remotely to the **AlmaLinux** server remotely with your **AlmaLinux user account.**

   ssh mperez@192,168,50.10

3. Were you successful? What happened when you attempted to connect to the AlmaLinux server using the ssh command? It was sucessful
4. Run the command: **cat /etc/*-release**. If the connection is successful, the AlmaLinux version should be displayed.

```
mperez@client1:~$ ssh mperez@192.168.50.10
mperez@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 17:27:11 2025 from 192.168.50.20
[mperez@server1 ~]$ cat /etc/*release
AlmaLinux release 9.5 (Teal Serval)
NAME="AlmaLinux"
VERSION="9.5 (Teal Serval)"
ID="almalinux"
ID_LIKE="rhel centos fedora"
VERSION_ID="9.5"
PLATFORM_ID="platform:el9"
PRETTY_NAME="AlmaLinux 9.5 (Teal Serval)"
ANSI_COLOR="0;34"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:almalinux:almalinux:9::baseos"
HOME_URL="https://almalinux.org/"
DOCUMENTATION_URL="https://wiki.almalinux.org/"
BUG_REPORT_URL="https://bugs.almalinux.org/"

ALMALINUX_MANTISBT_PROJECT="AlmaLinux-9"
ALMALINUX_MANTISBT_PROJECT_VERSION="9.5"
REDHAT_SUPPORT_PRODUCT="AlmaLinux"
REDHAT_SUPPORT_PRODUCT_VERSION="9.5"
SUPPORT_END=2032-06-01
AlmaLinux release 9.5 (Teal Serval)
AlmaLinux release 9.5 (Teal Serval)
[mperez@server1 ~]$ exit
logout
Connection to 192.168.50.10 closed.
mperez@client1:~$
```

5. Leave the session open on **Ubuntu** and go back to the **AlmaLinux** server to review the output of the **tcpdump** command.

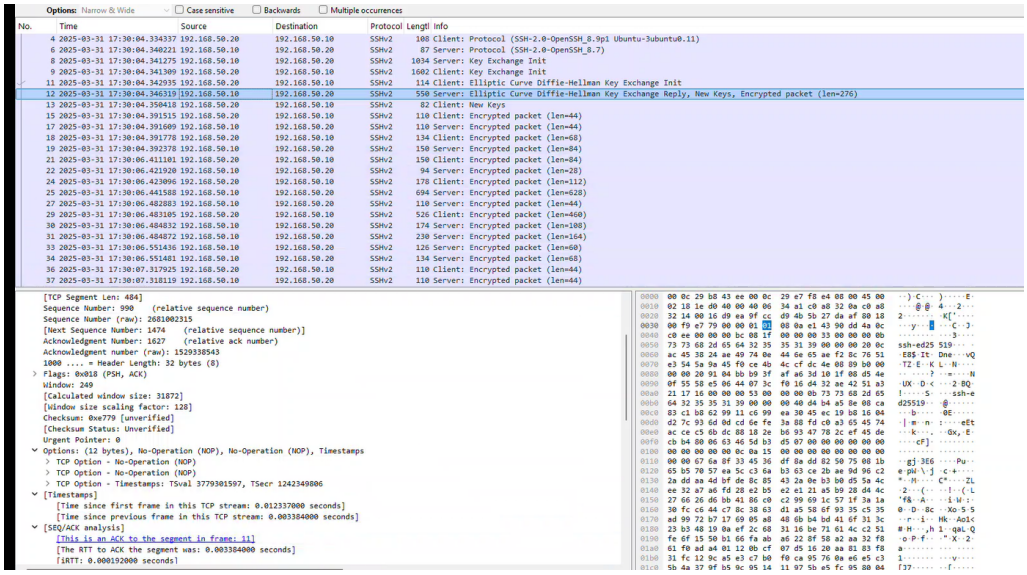
Get the pcap file and analyze in wireshark

```
C:\Users\2498056>
C:\Users\2498056>
C:\Users\2498056>sftp mperez@192.168.204.128
mperez@192.168.204.128's password:
Connected to 192.168.204.128.
sftp> dir
10.164.1.4          192.168.204.128     Desktop             Documents           Downloads           Music

Pictures            Public              Templates           Videos              tcpdump_ssh.pcap    volume

sftp> get tcpdump_ssh.pcap
Fetching /home/mperez/tcpdump_ssh.pcap to tcpdump_ssh.pcap
tcpdump_ssh.pcap                                                                      100%   15KB   7.2MB/s   00:00
sftp> exit
```

```
C:\Users\2498056>dir
 Volume in drive C has no label.
 Volume Serial Number is 7AB1-EC7B

 Directory of C:\Users\2498056

2025-03-31  05:34 PM    <DIR>          .
2025-03-16  02:22 PM    <DIR>          ..
2025-01-17  09:00 AM    <DIR>          .ms-ad
2025-03-21  12:29 AM               180 .packettracer
2025-03-31  05:15 PM    <DIR>          .ssh
2025-03-19  12:41 PM                 0 .uc-55b5a86b38d5d5c971f9bcc00b06044a.2498056.jac-2kww7v3.tmp
2025-03-21  12:30 AM    <DIR>          Cisco Packet Tracer 8.2.1
2025-01-16  09:52 AM    <DIR>          Contacts
2025-01-18  02:08 PM    <DIR>          Documents
2025-03-24  12:44 PM    <DIR>          Downloads
2025-01-16  09:52 AM    <DIR>          Favorites
2025-01-29  11:39 PM    <DIR>          GNS3
2025-01-16  09:52 AM    <DIR>          Links
2025-01-16  09:52 AM    <DIR>          Music
2024-06-11  05:53 PM    <DIR>          OneDrive
2025-03-28  04:57 PM    <DIR>          OneDrive - John Abbott College
2025-01-16  09:55 AM    <DIR>          PSAppDeployToolkit
2025-01-16  09:52 AM    <DIR>          Saved Games
2025-01-16  09:52 AM    <DIR>          Searches
2025-03-31  05:20 PM            14,399 ssh_port_LAN1.pcap
2025-03-31  05:34 PM            15,113 tcpdump_ssh.pcap
2025-01-16  09:52 AM    <DIR>          Videos
               4 File(s)         29,692 bytes
```

6. Can you see your username and password? Why or why not?

No password is not visible password is encrypted.



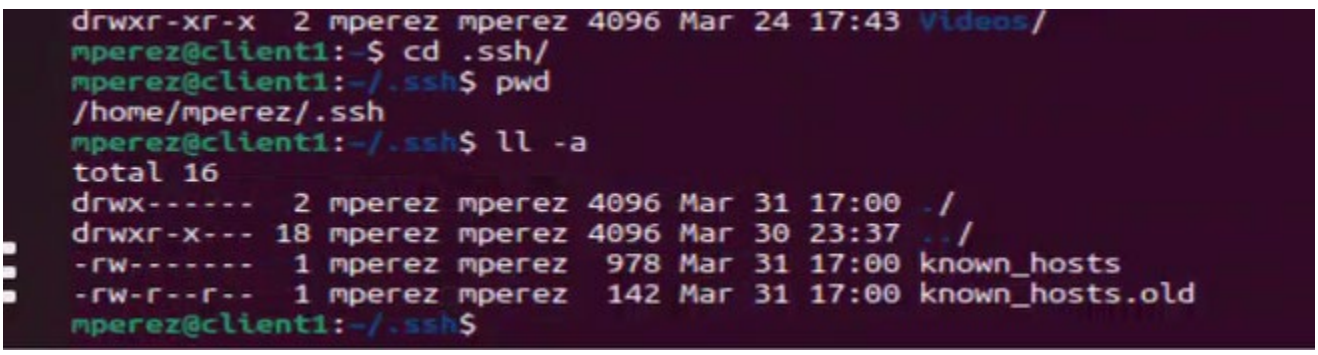
7. Stop the **tcpdump** command on **AlmaLinux** and return to the **Ubuntu** client.

8. Log out from the **sshd server.**

9. Open the user's **.ssh** directory and list its contents.

   cd /home/mperez/.ssh

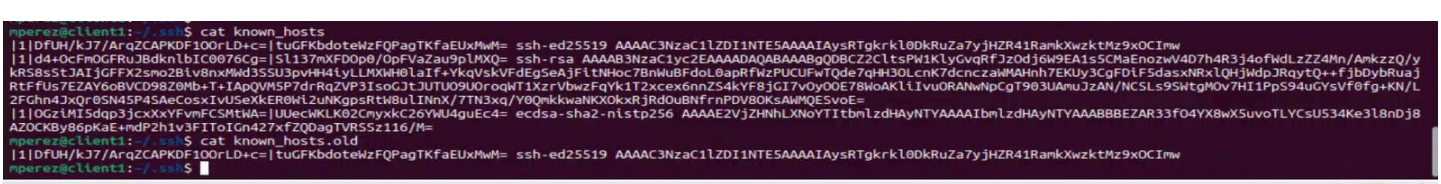
   ll -a



10. Does it contain files? If yes, what is the name of this file and what does it contain?

Contents of the `.ssh` Directory:

- Two files are present:
  - `known_hosts`: This file stores the fingerprints of previously connected SSH servers.
  - `known_hosts.old`: A backup of the `known_hosts` file, likely containing older host fingerprints.



Generation of Public/Private keys on the SSH client

Exercise 1.3: Tasks to Perform on Ubuntu:

1. From the **Ubuntu** client, connect to the **AlmaLinux** server again using **ssh** with your **AlmaLinux user account.**

```
mperez@client1:~/.ssh$ ssh mperez@192.168.50.10
mperez@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 17:30:06 2025 from 192.168.50.20
[mperez@server1 ~]$
```

2. Were you able to log in without entering a password? Yes

3. **Close the SSH connection using the exit command.**

You will now generate a public/private key pair on the client and copy the public key to the server in order to enable passwordless SSH authentication using the authorized_keys mechanism.

4. On the **Ubuntu** client, generate a public/private key pair using the **RSA** algorithm.

ssh-keygen -t rsa -b 4096

```
mperez@client1:~/.ssh$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mperez/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mperez/.ssh/id_rsa
Your public key has been saved in /home/mperez/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:mNGrV5lXS8og+ZwuiBDYNZ2oHjpD6ZjJGvfMh3q61qk mperez@client1
The key's randomart image is:
+---[RSA 4096]----+
|     oo .         |
| o ...o. .        |
|. +.  . + .   o   |
| oo.   + = * + .  |
|==..  o S B + .   |
|Ooo. . o o .      |
|.= =.oo o .       |
|. . O .. .        |
| .E* .            |
+----[SHA256]-----+
mperez@client1:~/.ssh$
```

Keys are generated

```
mperez@client1:~/.ssh$
mperez@client1:~/.ssh$ pwd
/home/mperez/.ssh
mperez@client1:~/.ssh$ ll -a
total 24
drwx------  2 mperez mperez 4096 Mar 31 18:07 ./
drwxr-x--- 18 mperez mperez 4096 Mar 30 23:37 ../
-rw-------  1 mperez mperez 3381 Mar 31 18:07 id_rsa
-rw-r--r--  1 mperez mperez  740 Mar 31 18:07 id_rsa.pub
-rw-------  1 mperez mperez  978 Mar 31 17:00 known_hosts
-rw-r--r--  1 mperez mperez  142 Mar 31 17:00 known_hosts.old
mperez@client1:~/.ssh$
```

5. Use an SSH tool to copy the client's public key to the server.

   ssh-copy-id mperez@192.168.50.10

```
mperez@client1:~/.ssh$
mperez@client1:~/.ssh$ ssh-copy-id mperez@192.168.50.10
/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
mperez@192.168.50.10's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'mperez@192.168.50.10'"
and check to make sure that only the key(s) you wanted were added.

mperez@client1:~/.ssh$
```

cat .ssh/authorzed_keys

```
[mperez@server1 ~]$ cat .ssh//authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCx5ZXJrG8Z1r3PD3zKowMkEyEPEwFES5Egv/IrMT3VvbQStkBNLRZWZl84UOm4UUusvYaAzd8pqZcaZ5r0ClXB/qIB1l4/1g9/junSYZZE/5gsSh94t709DqSMfCvChqdftndXTmkPXG71rXv0uwpEOMjUft3jQIbWy7H8Dr5V+5ULPT1Frbqqg+zKGDEov81wXRzPw
c9gMmkz/LJ+RG6VA/4d0TUKr4CUdd6Qx4kp/Qi5opyXc7xfIUIFLzGzF7t0R5DmJgo3b4GR8PNUYVOpwC5+ai7IpYKd1jvvih5vnKedlb0CN9EuhjSHDbhweYyq6ULSDTpKgd6chiMltJ97LWtxGDonPX/eEJjYLQgofoDzBkUIHCLAIlk3Ja58in5WYRHlvmHta7KwTo81caKEs66jHWSoLL3odSPhHG9JJ6ZdhXFysN
gS2Z6EIf+qjdWw48jIln0fjyMeJF9bOXvF01qDzSwaisglPFZU0zlG3aQyl+NXUg4FhrN3iPzMtoQflc4iS0q4UpcUaexpsB/f3AeoG7lrpOizQrxz0ojAEaUQwAOX3QTRiH5D7E+cZUpaRb7hBxhf6ND5kfnJdNHKyXWNda8YDjliNGHi9qhvlH4OirFgpd0ieiiFow2b46ik0y8A0MWPBbYjd4L3UCmlG07amcEwB/z
c6vsvJ2WACQ== mperez@client1
[mperez@server1 ~]$
```

```
[mperez@server1 ~]$ cat .ssh//authorized_keys
ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAACAQCx5ZXJrG8Z1r3PD3zKowMkEyEPEwFES5Egv/IrMT3VvbQStkBNLRZWZl84UOm4
    UUusvYaAzd8pqZcaZ5r0ClXB/qIB1l4/1g9/junSYZZE/5gsSh94t709DqSMfCvChqdftndXTmkPXG71rXv0uwpEOMjUft3jQIbW
    y7H8Dr5V+5ULPT1Frbqqg+zKGDEov81wXRzPwc9gMmkz/LJ+RG6VA/4d0TUKr4CUdd6Qx4kp/Qi5opyXc7xfIUIFLzGzF7t0R5
    DmJgo3b4GR8PNUYVOpwC5+ai7IpYKd1jvvih5vnKedlb0CN9EuhjSHDbhweYyq6ULSDTpKgd6chiMltJ97LWtxGDonPX/eEJjY
    LQgofoDzBkUIHCLAIlk3Ja58in5WYRHlvmHta7KwTo81caKEs66jHWSoLL3odSPhHG9JJ6ZdhXFysNgS2Z6EIf+qjdWw48jIln0fj
    yMeJF9bOXvF01qDzSwaisglPFZU0zlG3aQyl+NXUg4FhrN3iPzMtoQflc4iS0q4UpcUaexpsB/f3AeoG7lrpOizQrxz0ojAEaUQw
    AOX3QTRiH5D7E+cZUpaRb7hBxhf6ND5kfnJdNHKyXWNda8YDjliNGHi9qhvlH4OirFgpd0ieiiFow2b46ik0y8A0MWPBbYjd4L
    3UCmlG07amcEwB/zc6vsvJ2WACQ== mperez@client1

[mperez@server1 ~]$
```

6. Try connecting to the remote SSH server again.
7. You should now be able to log in without a password. If not, review the previous steps to ensure everything was completed correctly.

8. **Close the SSH connection using the exit command.**

Password less connection is possible.

```
mperez@client1:~/.ssh$ ssh mperez@192.168.50.10
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 18:05:32 2025 from 192.168.50.20
[mperez@server1 ~]$ exit
logout
Connection to 192.168.50.10 closed.
mperez@client1:~/.ssh$
```

Modification of the OpenSSH server configuration

Exercise 1.4: Tasks to Perform on AlmaLinux and Ubuntu:

1. From the **Ubuntu** client, try to connect to the **AlmaLinux** server using **SSH** with the **root** account? Are you able to connect? No

   By default, root login is typically disabled for security reasons, so you'll likely receive a "Permission denied" error.

```
Connection to 192.168.50.10 closed.
mperez@client1:~/.ssh$ ssh root@192.168.50.10
root@192.168.50.10's password:
Permission denied, please try again.
root@192.168.50.10's password:
Permission denied, please try again.
root@192.168.50.10's password:

mperez@client1:~/.ssh$
```

2. On the **AlmaLinux** server, open the **OpenSSH server configuration file** and modify a **keyword** that allows the **root** user to connect to the sshd server.

   sudo cat /etc/ssh/sshd_config | grep 'Permit'

```
[sudo] password for mperez:
[mperez@server1 ~]$ sudo cat /etc/ssh/sshd_config | grep 'Permit'
[sudo] password for mperez:
#PermitRootLogin prohibit-password
#PermitEmptyPasswords no
# the setting of "PermitRootLogin without-password".
#PermitTTY yes
#PermitUserEnvironment no
#PermitTunnel no
#       PermitTTY no
[mperez@server1 ~]$
```

Home | Ubuntu 64-bit | AlmaLinux 64-bit

mperez@server1:~ — sudo vim /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

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
"/etc/ssh/sshd_config" 131L, 3687B
```

NOTE

```
[mperez@server1 ~]$ sudo cat /etc/ssh/sshd_config | grep 'Permit'
#PermitRootLogin prohibit-password
PermitRootLogin yes
#PermitEmptyPasswords no
# the setting of "PermitRootLogin without-password".
#PermitTTY yes
#PermitUserEnvironment no
#PermitTunnel no
#       PermitTTY no
```

3. Reload the **SSH service** to apply the new configuration.

```
[mperez@server1 ~]$
[mperez@server1 ~]$ sudo systemctl reload sshd
[mperez@server1 ~]$ sudo systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-27 22:32:22 EDT; 3 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 15627 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
   Main PID: 996 (sshd)
      Tasks: 1 (limit: 22829)
     Memory: 2.8M
        CPU: 340ms
     CGroup: /system.slice/sshd.service
             └─996 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 31 18:15:35 server1 sshd[15387]: Failed password for root from 192.168.50.20 port 49190 ssh2
Mar 31 18:15:40 server1 unix_chkpwd[15390]: password check failed for user (root)
Mar 31 18:15:43 server1 sshd[15387]: Failed password for root from 192.168.50.20 port 49190 ssh2
Mar 31 18:15:54 server1 sshd[15387]: Connection closed by authenticating user root 192.168.50.20 port 49190 [preauth]
Mar 31 18:15:54 server1 sshd[15387]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.20  user=root
Mar 31 18:40:37 server1 systemd[1]: Reloading OpenSSH server daemon...
Mar 31 18:40:37 server1 sshd[996]: Received SIGHUP; restarting.
Mar 31 18:40:37 server1 systemd[1]: Reloaded OpenSSH server daemon.
Mar 31 18:40:37 server1 sshd[996]: Server listening on 0.0.0.0 port 22.
Mar 31 18:40:37 server1 sshd[996]: Server listening on :: port 22.
[mperez@server1 ~]$
```

4. Type the following command, to **audit** the connection between client and server:

   tail -f /var/log/audit/audit.log

```
[mperez@server1 ~]$ sudo tail -f /var/log/audit/audit.log
```

5. Switch back to **Ubuntu** and try connecting again as **root** via SSH.

6. If your configuration was correctly updated, you **should be able to log in with the root account.**

```
mperez@client1:~/.ssh$ ssh root@192.168.50.10
root@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Mon Mar 31 18:15:43 EDT 2025 from 192.168.50.20 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Thu Mar 27 11:41:59 2025
[root@server1 ~]# exit
logout
Connection to 192.168.50.10 closed.
mperez@client1:~/.ssh$
```

7. Go back to the **AlmaLinux** server and examine the output in **audit.log.**

```
[mperez@server1 ~]$ sudo tail -f /var/log/audit/audit.log
```

```
type=USER_ACCT msg=audit(1743460847.064:1807): pid=15632 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting
grantors=pam_unix,pam_localuser acct="mperez" exe="/usr/bin/sudo" hostname=?
addr=? terminal=/dev/pts/1 res=success'UID="mperez" AUID="mperez"
type=USER_CMD msg=audit(1743460847.064:1808): pid=15632 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/mperez"
cmd=73797374656D63746C2073746174757320737368 64 exe="/usr/bin/sudo" terminal=pts/1
res=success'UID="mperez" AUID="mperez"
type=CRED_REFR msg=audit(1743460847.064:1809): pid=15632 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=?
terminal=/dev/pts/1 res=success'UID="mperez" AUID="mperez"
type=USER_START msg=audit(1743460847.066:1810): pid=15632 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix
acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/1
res=success'UID="mperez" AUID="mperez"
type=USER_END msg=audit(1743460847.076:1811): pid=15632 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=PAM:session_close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix
acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/1
res=success'UID="mperez" AUID="mperez"
type=CRED_DISP msg=audit(1743460847.077:1812): pid=15632 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=?
terminal=/dev/pts/1 res=success'UID="mperez" AUID="mperez"
type=USER_ACCT msg=audit(1743460917.866:1813): pid=15659 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting
grantors=pam_unix,pam_localuser acct="mperez" exe="/usr/bin/sudo" hostname=?
addr=? terminal=/dev/pts/1 res=success'UID="mperez" AUID="mperez"
type=USER_CMD msg=audit(1743460917.867:1814): pid=15659 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/mperez"
cmd=7461696C202D66202F7661722F6C6F672F61756469742F61756469742E6C6F67
exe="/usr/bin/sudo" terminal=pts/1 res=success'UID="mperez" AUID="mperez"
type=CRED_REFR msg=audit(1743460917.867:1815): pid=15659 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=?
terminal=/dev/pts/1 res=success'UID="mperez" AUID="mperez"
type=USER_START msg=audit(1743460917.868:1816): pid=15659 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix
acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/1
res=success'UID="mperez" AUID="mperez"
type=CRYPTO_KEY_USER msg=audit(1743460936.647:1817): pid=15663 uid=0
auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
msg='op=destroy kind=server
fp=SHA256:a4:48:7a:9b:d6:6c:7a:9f:51:bc:07:19:be:e5:ab:4d:58:b5:f6:9c:f3:03:7e:01:
c0:d6:ef:b5:f3:eb:cf:17 direction=? spid=15663 suid=0  exe="/usr/sbin/sshd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="unset" SUID="root"
type=CRYPTO_SESSION msg=audit(1743460936.648:1818): pid=15662 uid=0
auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
msg='op=start direction=from-server cipher=chacha20-poly1305@openssh.com ksize=512
mac=<implicit> pfs=curve25519-sha256 spid=15663 suid=74 rport=59530
laddr=192.168.50.10 lport=22  exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20
terminal=? res=success'UID="root" AUID="unset" SUID="sshd"
type=CRYPTO_SESSION msg=audit(1743460936.648:1819): pid=15662 uid=0
auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
msg='op=start direction=from-client cipher=chacha20-poly1305@openssh.com ksize=512
mac=<implicit> pfs=curve25519-sha256 spid=15663 suid=74 rport=59530
laddr=192.168.50.10 lport=22  exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20
```

```
terminal=? res=success'UID="root" AUID="unset" SUID="sshd"
type=USER_AUTH msg=audit(1743460936.719:1820): pid=15662 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=pubkey
acct="root" exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=ssh
res=failed'UID="root" AUID="unset"
```

```
type=USER_AUTH msg=audit(1743460941.544:1821): pid=15662 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
msg='op=PAM:authentication grantors=pam_unix acct="root" exe="/usr/sbin/sshd"
hostname=192.168.50.20 addr=192.168.50.20 terminal=ssh res=success'UID="root"
AUID="unset"
```

```
type=USER_ACCT msg=audit(1743460941.550:1822): pid=15662 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:accounting
grantors=pam_unix,pam_localuser acct="root" exe="/usr/sbin/sshd"
hostname=192.168.50.20 addr=192.168.50.20 terminal=ssh res=success'UID="root"
AUID="unset"
```

```
type=CRYPTO_KEY_USER msg=audit(1743460941.568:1823): pid=15662 uid=0
auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
msg='op=destroy kind=session fp=? direction=both spid=15663 suid=74 rport=59530
laddr=192.168.50.10 lport=22  exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20
terminal=? res=success'UID="root" AUID="unset" SUID="sshd"
```

```
type=CRED_ACQ msg=audit(1743460941.568:1824): pid=15662 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_unix acct="root" exe="/usr/sbin/sshd" hostname=192.168.50.20
addr=192.168.50.20 terminal=ssh res=success'UID="root" AUID="unset"
```

```
type=LOGIN msg=audit(1743460941.568:1825): pid=15662 uid=0
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none)
old-ses=4294967295 ses=15 res=1UID="root" OLD-AUID="unset" AUID="root"
```

```
type=SYSCALL msg=audit(1743460941.568:1825): arch=c000003e syscall=1 success=yes
exit=1 a0=3 a1=7ffe057e2080 a2=1 a3=0 items=0 ppid=996 pid=15662 auid=0 uid=0
gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=15 comm="sshd"
exe="/usr/sbin/sshd" subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
key=(null)ARCH=x86_64 SYSCALL=write AUID="root" UID="root" GID="root" EUID="root"
SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1743460941.568:1825):
proctitle=737368643A20726F6F74205B707269765D
type=USER_ROLE_CHANGE msg=audit(1743460941.569:1826): pid=15662 uid=0 auid=0
ses=15 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=pam_selinux default-
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 selected-
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/sbin/sshd"
hostname=192.168.50.20 addr=192.168.50.20 terminal=ssh res=success'UID="root"
AUID="root"
type=SERVICE_START msg=audit(1743460941.594:1827): pid=1 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=user-runtime-dir@0
comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=success'UID="root" AUID="unset"
type=USER_ACCT msg=audit(1743460941.608:1828): pid=15667 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='op=PAM:accounting
grantors=pam_unix acct="root" exe="/usr/lib/systemd/systemd" hostname=? addr=?
terminal=? res=success'UID="root" AUID="unset"
type=CRED_ACQ msg=audit(1743460941.608:1829): pid=15667 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='op=PAM:setcred grantors=?
acct="root" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=failed'UID="root" AUID="unset"
type=USER_ROLE_CHANGE msg=audit(1743460941.608:1830): pid=15667 uid=0
auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='op=pam_selinux default-context=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 selected-context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
```

```
type=LOGIN msg=audit(1743460941.608:1831): pid=15667 uid=0
subj=system_u:system_r:init_t:s0 old-auid=4294967295 auid=0 tty=(none) old-
ses=4294967295 ses=16 res=1UID="root" OLD-AUID="unset" AUID="root"
type=SYSCALL msg=audit(1743460941.608:1831): arch=c000003e syscall=1 success=yes
exit=1 a0=7 a1=7ffe57708040 a2=1 a3=0 items=0 ppid=1 pid=15667 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=16 comm="(systemd)"
exe="/usr/lib/systemd/systemd" subj=system_u:system_r:init_t:s0
key=(null)ARCH=x86_64 SYSCALL=write AUID="root" UID="root" GID="root" EUID="root"
SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1743460941.608:1831): proctitle="(systemd)"
type=USER_START msg=audit(1743460941.610:1832): pid=15667 uid=0 auid=0 ses=16
subj=system_u:system_r:init_t:s0 msg='op=PAM:session_open
grantors=pam_selinux,pam_selinux,pam_loginuid,pam_keyinit,pam_umask,pam_namespace,
pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root"
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="root"
type=BPF msg=audit(1743460941.623:1833): prog-id=100 op=LOAD
type=SYSCALL msg=audit(1743460941.623:1833): arch=c000003e syscall=321 success=yes
exit=8 a0=5 a1=7fff82df6d10 a2=90 a3=0 items=0 ppid=1 pid=15667 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=16 comm="systemd"
exe="/usr/lib/systemd/systemd" subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key=(null)ARCH=x86_64 SYSCALL=bpf AUID="root" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1743460941.623:1833): proctitle="(systemd)"
type=BPF msg=audit(1743460941.624:1834): prog-id=100 op=UNLOAD
type=SYSCALL msg=audit(1743460941.624:1834): arch=c000003e syscall=3 success=yes
exit=0 a0=8 a1=7fff82df6df0 a2=90 a3=200000008 items=0 ppid=1 pid=15667 auid=0
uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=16
comm="systemd" exe="/usr/lib/systemd/systemd"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)ARCH=x86_64
SYSCALL=close AUID="root" UID="root" GID="root" EUID="root" SUID="root"
FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1743460941.624:1834): proctitle="(systemd)"
type=BPF msg=audit(1743460941.624:1835): prog-id=101 op=LOAD
type=SYSCALL msg=audit(1743460941.624:1835): arch=c000003e syscall=321 success=yes
exit=8 a0=5 a1=7fff82df6db0 a2=90 a3=4 items=0 ppid=1 pid=15667 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=16 comm="systemd"
exe="/usr/lib/systemd/systemd" subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key=(null)ARCH=x86_64 SYSCALL=bpf AUID="root" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1743460941.624:1835): proctitle="(systemd)"
type=BPF msg=audit(1743460941.624:1836): prog-id=101 op=UNLOAD
type=SYSCALL msg=audit(1743460941.624:1836): arch=c000003e syscall=3 success=yes
exit=0 a0=8 a1=7fff82df6db0 a2=90 a3=4 items=0 ppid=1 pid=15667 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=16 comm="systemd"
exe="/usr/lib/systemd/systemd" subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key=(null)ARCH=x86_64 SYSCALL=close AUID="root" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1743460941.624:1836): proctitle="(systemd)"
type=SERVICE_START msg=audit(1743460941.699:1837): pid=1 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=user@0 comm="systemd"
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=USER_START msg=audit(1743460941.711:1838): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyini
t,pam_limits,pam_systemd,pam_unix,pam_umask,pam_lastlog acct="root"
exe="/usr/sbin/sshd" hostname=192.168.50.20 addr=192.168.50.20 terminal=ssh
res=success'UID="root" AUID="root"
type=CRYPTO_KEY_USER msg=audit(1743460941.711:1839): pid=15684 uid=0 auid=0 ses=15
```

```
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server
fp=SHA256:a4:48:7a:9b:d6:6c:7a:9f:51:bc:07:19:be:e5:ab:4d:58:b5:f6:9c:f3:03:7e:01:
c0:d6:ef:b5:f3:eb:cf:17 direction=? spid=15684 suid=0  exe="/usr/sbin/sshd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="root" SUID="root"
type=CRED_ACQ msg=audit(1743460941.712:1840): pid=15684 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix
acct="root" exe="/usr/sbin/sshd" hostname=192.168.50.20 addr=192.168.50.20
terminal=ssh res=success'UID="root" AUID="root"
type=USER_LOGIN msg=audit(1743460941.756:1841): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0
exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/0
res=success'UID="root" AUID="root" ID="root"
type=USER_START msg=audit(1743460941.756:1842): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0
exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/0
res=success'UID="root" AUID="root" ID="root"
type=CRYPTO_KEY_USER msg=audit(1743460941.760:1843): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server
fp=SHA256:a4:48:7a:9b:d6:6c:7a:9f:51:bc:07:19:be:e5:ab:4d:58:b5:f6:9c:f3:03:7e:01:
c0:d6:ef:b5:f3:eb:cf:17 direction=? spid=15685 suid=0  exe="/usr/sbin/sshd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="root" SUID="root"
type=BPF msg=audit(1743460941.766:1844): prog-id=102 op=LOAD
type=BPF msg=audit(1743460941.766:1845): prog-id=103 op=LOAD
type=SERVICE_START msg=audit(1743460941.808:1846): pid=1 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed
comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=success'UID="root" AUID="unset"
type=USER_END msg=audit(1743460960.116:1847): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0
exe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="root"
AUID="root" ID="root"
type=USER_LOGOUT msg=audit(1743460960.116:1848): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0
exe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="root"
AUID="root" ID="root"
type=CRYPTO_KEY_USER msg=audit(1743460960.118:1849): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=session fp=?
direction=both spid=15684 suid=0 rport=59530 laddr=192.168.50.10 lport=22
exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=?
res=success'UID="root" AUID="root" SUID="root"
type=CRYPTO_KEY_USER msg=audit(1743460960.118:1850): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server
fp=SHA256:a4:48:7a:9b:d6:6c:7a:9f:51:bc:07:19:be:e5:ab:4d:58:b5:f6:9c:f3:03:7e:01:
c0:d6:ef:b5:f3:eb:cf:17 direction=? spid=15684 suid=0  exe="/usr/sbin/sshd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="root" SUID="root"
type=USER_END msg=audit(1743460960.119:1851): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_close
grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyini
t,pam_limits,pam_systemd,pam_unix,pam_umask,pam_lastlog acct="root"
exe="/usr/sbin/sshd" hostname=192.168.50.20 addr=192.168.50.20 terminal=ssh
res=success'UID="root" AUID="root"
type=CRED_DISP msg=audit(1743460960.119:1852): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix
acct="root" exe="/usr/sbin/sshd" hostname=192.168.50.20 addr=192.168.50.20
terminal=ssh res=success'UID="root" AUID="root"
type=CRYPTO_KEY_USER msg=audit(1743460960.119:1853): pid=15662 uid=0 auid=0 ses=15
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server
fp=SHA256:a4:48:7a:9b:d6:6c:7a:9f:51:bc:07:19:be:e5:ab:4d:58:b5:f6:9c:f3:03:7e:01:
c0:d6:ef:b5:f3:eb:cf:17 direction=? spid=15662 suid=0  exe="/usr/sbin/sshd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="root" SUID="root"
```

```
type=CRED_DISP msg=audit(1743460970.295:1854): pid=15669 uid=0 auid=0 ses=16
subj=system_u:system_r:init_t:s0 msg='op=PAM:setcred grantors=? acct="root"
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root"
AUID="root"
type=SERVICE_STOP msg=audit(1743460970.297:1855): pid=1 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=user@0 comm="systemd"
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=SERVICE_STOP msg=audit(1743460970.308:1856): pid=1 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=user-runtime-dir@0
comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1743460971.827:1857): pid=1 uid=0 auid=4294967295
ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed
comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=success'UID="root" AUID="unset"
type=BPF msg=audit(1743460971.864:1858): prog-id=103 op=UNLOAD
type=BPF msg=audit(1743460971.864:1859): prog-id=102 op=UNLOAD
^C
[mperez@server1 ~]$
```

8. Which log message indicates a successful login by the root user?

```
type=LOGIN msg=audit(1743460941.568:1825): pid=15662 uid=0
    subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none)
    old-ses=4294967295 ses=15 res=1UID="root" OLD-AUID="unset" AUID="root"
```

- **Type**: `LOGIN` - Specifies that this message pertains to a login event.
- **Audit ID (AUID)**: The `old-auid=4294967295` (unset) transitioned to `auid=0` (root), indicating the root user successfully authenticated.
- **Result**: `res=1` confirms the login was successful.
- **Session ID**: `ses=15` identifies the session associated with this login.
- **Process ID**: `pid=15662` refers to the process managing the login, in this case, the SSH daemon (`sshd`).

This log clearly indicates the authentication and login process for the root user succeeded.

9. Stop the **tail** command on the **AlmaLinux** server by pressing **Ctrl+C.**

10. . Return to **Ubuntu** and disconnect the root session from the SSH server.

X11 FORWARDING

Exercise 1.5: Tasks to Perform on Ubuntu:

1. From ubuntu, start an SSH session with X11 forwarding enabled:

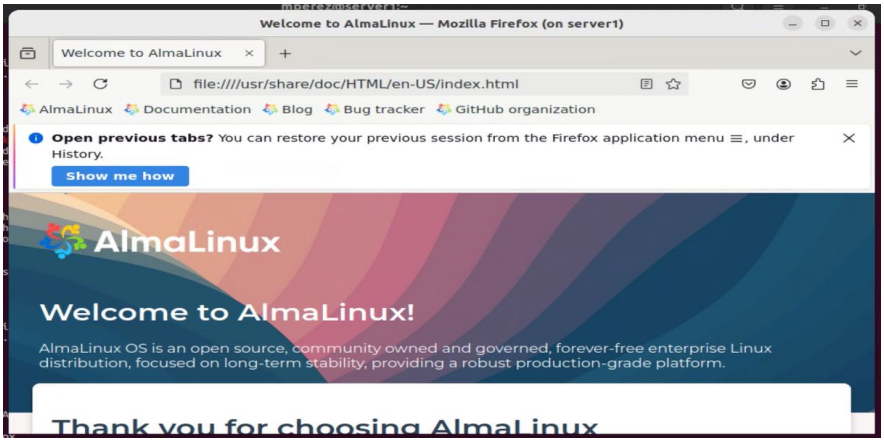
   sudo nano /etc/ssh/sshd_config.d/50-redhat.conf

```
^C
[mperez@server1 ~]$ sudo cat /etc/ssh/ssh_config.d/50-redhat.conf | grep 'X11'
[sudo] password for mperez:
# If this option is set to yes then remote X11 clients will have full access
# to the original X11 display. As virtually no X11 client supports the untrusted
        ForwardX11Trusted yes
[mperez@server1 ~]$ sudo cat /etc/ssh/ssh_config.d/50-redhat.conf
# The options here are in the "Match final block" to be applied as the last
# options and could be potentially overwritten by the user configuration
Match final all
        # Follow system-wide Crypto Policy, if defined:
        Include /etc/crypto-policies/back-ends/openssh.config

        GSSAPIAuthentication yes

# If this option is set to yes then remote X11 clients will have full access
# to the original X11 display. As virtually no X11 client supports the untrusted
# mode correctly we set this to yes.
        ForwardX11Trusted yes

# Uncomment this if you want to use .local domain
# Host *.local
[mperez@server1 ~]$ sudo nano /etc/ssh/ssh_config.d/50-redhat.conf
[mperez@server1 ~]$ sudo cat /etc/ssh/ssh_config.d/50-redhat.conf
# The options here are in the "Match final block" to be applied as the last
# options and could be potentially overwritten by the user configuration
Match final all
        # Follow system-wide Crypto Policy, if defined:
        Include /etc/crypto-policies/back-ends/openssh.config

        GSSAPIAuthentication yes

# If this option is set to yes then remote X11 clients will have full access
# to the original X11 display. As virtually no X11 client supports the untrusted
# mode correctly we set this to yes.
        ForwardX11Trusted yes
        X11Forwarding yes
# Uncomment this if you want to use .local domain
# Host *.local
[mperez@server1 ~]$
```

2. Once connected, type the following command to launch Firefox: **firefox &**

```
Connection to 192.168.50.10 closed.
mperez@client1:~/.ssh$ ssh -X mperez@192.168.50.10
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Apr  1 00:52:39 2025 from 192.168.50.20
[mperez@server1 ~]$ firefox&
[1] 18102
[mperez@server1 ~]$
```

3. If the **Firefox** browser opens and displays the AlmaLinux website, **X11 forwarding** is working correctly.



4. Go back to the AlmaLinux server and verify if the **firefox process** is running.

Process 1802 corresponds to process running when firefox is started in client (Ubuntu)

```
Connection to 192.168.50.10 closed.
mperez@client1:~/.ssh$ ssh -X mperez@192.168.50.10
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Apr  1 00:52:39 2025 from 192.168.50.20
[mperez@server1 ~]$ firefox&
[1] 18102
[mperez@server1 ~]$
```

```
[mperez@server1 ~]$ ps -aux | grep firefox
mperez     18102  3.9  9.4 3190976 351372 pts/0   Sl   01:04   0:06 /usr/lib64/firefox/firefox
mperez     18170  0.0  1.4 268112 52992 pts/0    Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -parentBuildID 20250310042414 -prefsLen 24539 -prefMapSize 248932 -appDir /usr/lib64/firefox/browser {546f7023-fcb0-4ed1-a317-56cc
769832e8} 18102 socket
mperez     18194  0.6  3.8 2717992 142996 pts/0  Sl   01:04   0:01 /usr/lib64/firefox/firefox -contentproc -childID 1 -isForBrowser -prefsLen 24680 -prefMapSize 248932 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/f
irefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {764acadf-3aba-4d98-a400-2a3eff05dad7} 18102 tab
mperez     18233  0.2  3.2 2704424 120408 pts/0  Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -childID 2 -isForBrowser -prefsLen 30451 -prefMapSize 248932 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/f
irefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {cf714820-6bb3-4271-abf8-561323eecabf} 18102 tab
mperez     18258  0.1  3.0 2697548 111576 pts/0  Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -childID 3 -isForBrowser -prefsLen 30451 -prefMapSize 248932 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/f
irefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {417bcea9-ee14-4333-99c7-1ab69af8d23f} 18102 tab
mperez     18307  0.0  1.3 265112 48272 pts/0    Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -parentBuildID 20250310042414 -sandboxingKind 0 -prefsLen 30615 -prefMapSize 248932 -appDir /usr/lib64/firefox/browser {5e0fa461-2
911-48e9-b1f3-2e5d351abe7c} 18102 utility
mperez     18312  0.0  2.4 2666988 90272 pts/0   Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -childID 4 -isForBrowser -prefsLen 28251 -prefMapSize 248932 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/f
irefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {ee6c87c9-a90e-46f8-9b9b-b791ef97022c} 18102 tab
mperez     18313  0.0  2.4 2666988 90408 pts/0   Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -childID 5 -isForBrowser -prefsLen 28251 -prefMapSize 248932 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/f
irefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {f176abac-495f-4eab-90d3-adb000294f46} 18102 tab
mperez     18339  0.0  2.4 2666992 90312 pts/0   Sl   01:04   0:00 /usr/lib64/firefox/firefox -contentproc -childID 6 -isForBrowser -prefsLen 28251 -prefMapSize 248932 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/f
irefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {481d4957-bf88-4aa2-a9e3-db72569d40ec} 18102 tab
mperez     18475  0.0  0.0 221660  2176 pts/1    S+   01:06   0:00 grep --color=auto firefox
[mperez@server1 ~]$ ps -aux | grep firefox
```

5. Return to **Ubuntu** and close the **Firefox** application.

```
mperez     18475  0.0  0.0 221660  2176 pts/1    S+   01:06   0:00 grep --color=auto firefox
[mperez@server1 ~]$ ps -aux | grep firefox
mperez     18521  0.0  0.0 221660  2176 pts/1    R+   01:07   0:00 grep --color=auto firefox
[mperez@server1 ~]$
```

6. Log out of the ssh session.

```
[1] 18102
[mperez@server1 ~]$ exit
logout
Connection to 192.168.50.10 closed.
mperez@client1:~/.ssh$
```