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.**

```
root@server07 ~ $ dnf list openssh-server
Last metadata expiration check: 20:34:19 ago on Sun 30 Mar 2025 06:40:19 PM.
Installed Packages
openssh-server.x86_64                              8.7p1-43.el9.alma.2                              @baseos
root@server07 ~ $ systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-30 14:41:44 EDT; 24h ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 985 (sshd)
      Tasks: 1 (limit: 22829)
     Memory: 2.7M
        CPU: 10ms
     CGroup: /system.slice/sshd.service
             └─985 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 30 14:41:44 server07 systemd[1]: Starting OpenSSH server daemon...
Mar 30 14:41:44 server07 sshd[985]: Server listening on 0.0.0.0 port 22.
Mar 30 14:41:44 server07 sshd[985]: Server listening on :: port 22.
Mar 30 14:41:44 server07 systemd[1]: Started OpenSSH server daemon.
root@server07 ~ $
```

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

```
root@server07 / $ rpm -ql openssh-server
/etc/pam.d/sshd
/etc/ssh/sshd_config
/etc/ssh/sshd_config.d
/etc/ssh/sshd_config.d/50-redhat.conf
/etc/sysconfig/sshd
/usr/lib/.build-id
/usr/lib/.build-id/a4
/usr/lib/.build-id/a4/db8df4efda8a9c2bc5c1c0ec248b50bbe4815c
/usr/lib/.build-id/f0
/usr/lib/.build-id/f0/4853acb7f1da1987519b49e067bf4d0677c143
/usr/lib/systemd/system/sshd-keygen.target
/usr/lib/systemd/system/sshd-keygen@.service
/usr/lib/systemd/system/sshd.service
/usr/lib/systemd/system/sshd.socket
/usr/lib/systemd/system/sshd@.service
/usr/lib/sysusers.d/openssh-server.conf
/usr/libexec/openssh/sftp-server
/usr/libexec/openssh/sshd-keygen
/usr/sbin/sshd
/usr/share/empty.sshd
/usr/share/man/man5/moduli.5.gz
/usr/share/man/man5/sshd_config.5.gz
/usr/share/man/man8/sftp-server.8.gz
/usr/share/man/man8/sshd.8.gz
root@server07 / $ cd /etc/ssh
root@server07 /etc/ssh $
```

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

```
root@server07 /etc/ssh $ ls
moduli      ssh_config.d  sshd_config.d      ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub  ssh_host_rsa_key.pub
ssh_config  sshd_config   ssh_host_ecdsa_key  ssh_host_ed25519_key    ssh_host_rsa_key
root@server07 /etc/ssh $
```

/etc/ssh/sshd_config

4. How many **public/private keys** does this server have? # 3 Pairs of each for : RSA,ECDSA,ED25519.

```
root@server07 /etc/ssh $ ls -la
total 616
drwxr-xr-x.   4 root root       4096 Mar  1 03:47 .
drwxr-xr-x. 139 root root       8192 Mar 31 14:51 ..
-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    492 Mar 24 14:19 ssh_host_ecdsa_key
-rw-r--r--.   1 root root        162 Mar 24 14:19 ssh_host_ecdsa_key.pub
-rw-r-----.   1 root ssh_keys    387 Mar 24 14:19 ssh_host_ed25519_key
-rw-r--r--.   1 root root         82 Mar 24 14:19 ssh_host_ed25519_key.pub
-rw-r-----.   1 root ssh_keys   2578 Mar 24 14:19 ssh_host_rsa_key
-rw-r--r--.   1 root root        554 Mar 24 14:19 ssh_host_rsa_key.pub
root@server07 /etc/ssh $
```

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)*

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

```
root@server07 /etc/ssh $ tcpdump -i ens192 -XX -s 0 tcp port 22
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

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.

```
gkeymole@client07:~$ apt list openssh-client
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
gkeymole@client07:~$
```

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

```
gkeymole@client07:~$ ssh antoine@192.168.50.10
The authenticity of host '192.168.50.10 (192.168.50.10)' can't be established.
ED25519 key fingerprint is SHA256:MPO3JPZqhEB+kjPz6e1ay/zMXD895wXRUesj/OyRxAo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.10' (ED25519) to the list of known hosts.
antoine@192.168.50.10's password:
Last login: Sat Mar 29 16:29:14 2025
```

```
gkeymole@client07:~$ ssh gkeymole@192.168.50.10
gkeymole@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Mar 30 14:41:55 2025
[gkeymole@server07 ~]$
```

3. Were you successful? What happened when you attempted to connect to the AlmaLinux server using the ssh command?

SSH checked if the AlmaLinux server's key was already known.

Since it was the first connection, SSH showed a key fingerprint warning and asked for confirmation.

After typing yes, the key was added to ~/.ssh/known_hosts on the Ubuntu VM.

```
gkeymole@client07:~$ cat .ssh/known_hosts
|1|Hhbet5k2jDzIucXd8GfYBDeSf4o=|NHblXUEwPNXoZ0CZqirN4L06v/s= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFEakXin+IFSHf2JemIfPyVapniJnAU1Ksk+
KNdYHCB1
|1|ZiwiMM4RjJE1Q5A45AtlirH1ztI=|AjTQvsvm0+YgNk/5vUGJH6fp0OY= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDR1Qt0TTESpA469zPd6gLLvSYSAGfbibR8
8GZI0YTqu8Wd8whuW+Xl9xqIU3XsIg9qF+rMDCiLn9dmnzwAxWjxlFs0yly3PwXNg2clYDSPdng9TpYDf0QNUjJ0D8hvMaCBNq5GNh3kH9sTFQRTcznkku45iJ07577Osb9Q0
dPABVtZMQazRvMkYo0tWu/Wr/MxO+9N2nocp8SgqOOvsodpowCNP7dHQhvBBHG2qTrSMDaZ5EB8ber16Uuew2B0KKppmdVJrZvlxO3UpEiruQJSY2MrUtcsdCCbMcTFtWV1zL
UuU0H1ptWp7W7qHYIJYTptpgvXUxCVzbV6QgKNvdk+LYmdYyBPdYMM9DaFgAr25DqoNIqElnRGIPsH5nk6+39vsCWizuzzXlJjEC8ql2QDuua0GM6P4GzapC9BgvkDWCqq1Mk
6GsDBlhqmniWgJuLsZDZSHPzca5K9H1uXWlk43SXzz3p2GOoqeXJztcRy/8vrgh1Tyh+TuEU7hRd9+d0=
|1|QmVXxq1f0H+o4EbOt3yjkYN4qlQ=|8RVMx3P0DdP9dA52yYHABI3JRws= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABB
BEcn61qhBqS4cAVuCLU9l32re8LQmTLNqIvvvl50ETPz2c9kQwMouFPgHBgYh0J7Mh7jYdezWk+kg5pNKBwZWdI=
gkeymole@client07:~$
```

4. Run the command: **cat /etc/*-release**. If the connection is successful, the AlmaLinux version should be displayed.

```
[antoine@server07 ~]$ 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)
[antoine@server07 ~]$
```

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

```
root@server07 /etc/ssh $ tcpdump -i ens192 -XX -s 0 tcp port 22
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:12:52.586032 IP 192.168.50.20.47184 > server07.ssh: Flags [S], seq 2713502605, win 64240, options [mss 1460,sackOK,
TS val 3431119753 ecr 0,nop,wscale 7], length 0
        0x0000:  000c 2991 682b 000c 293a 9595 0800 4510  ..).h+..):....E.
        0x0010:  003c f218 4000 4006 6324 c0a8 3214 c0a8  .<..@.@.c$..2...
        0x0020:  320a b850 0016 a1bc c38d 0000 0000 a002  2..P............
        0x0030:  faf0 c1e2 0000 0204 05b4 0402 080a cc82  ................
        0x0040:  bb89 0000 0000 0103 0307                 ..........
17:12:52.586135 IP server07.ssh > 192.168.50.20.47184: Flags [S.], seq 1147644349, ack 2713502606, win 31856, options
[mss 1460,sackOK,TS val 1589024217 ecr 3431119753,nop,wscale 7], length 0
        0x0000:  000c 293a 9595 000c 2991 682b 0800 4500  ..):....).h+..E.
        0x0010:  003c 0000 4000 4006 554d c0a8 320a c0a8  .<..@.@.UM..2...
        0x0020:  3214 0016 b850 4467 a9bd a1bc c38e a012  2....PDg........
        0x0030:  7c70 e59d 0000 0204 05b4 0402 080a 5eb6  |p............^.
        0x0040:  95d9 cc82 bb89 0103 0307                 ..........
17:12:52.586237 IP 192.168.50.20.47184 > server07.ssh: Flags [.], ack 1, win 502, options [nop,nop,TS val 3431119753 e
cr 1589024217], length 0
        0x0000:  000c 2991 682b 000c 293a 9595 0800 4510  ..).h+..):....E.
        0x0010:  0034 f219 4000 4006 632b c0a8 3214 c0a8  .4..@.@.c+..2...
        0x0020:  320a b850 0016 a1bc c38e 4467 a9be 8010  2..P......Dg....
        0x0030:  01f6 06e4 0000 0101 080a cc82 bb89 5eb6  ..............^.
        0x0040:  95d9                                     ..
```

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

No, you can't see your username and password in plaintext. That's because SSH encrypts all session data.

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

```
^C
129 packets captured
129 packets received by filter
0 packets dropped by kernel
root@server07 /etc/ssh $
```

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

```
[gkeymole@server07 ~]$ exit
logout
Connection to 192.168.50.10 closed.
gkeymole@client07:~$
```

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

```
gkeymole@client07:~$ cd .ssh/
gkeymole@client07:~/.ssh$ ls -l
total 8
-rw------- 1 gkeymole gkeymole 978 Mar 31 17:13 known_hosts
-rw-r--r-- 1 gkeymole gkeymole 142 Mar 31 17:13 known_hosts.old
gkeymole@client07:~/.ssh$
```

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

Yes, the .ssh directory contains files:

Known_hosts : This file stores the server's public host key / SSH fingerprints of the remote system you have previously connected to (AlmaLinux server). Its used to verify the identity of the server during future connections to prevent cyber security threats.

```
gkeymole@client07:~/.ssh$ cat known_hosts
|1|Hhbet5k2jDzIucXd8GfYBDeSf4o=|NHblXUEwPNXoZ0CZqirN4L06v/s= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFEakXin+IFSHf2JemIfPyVapniJnAU1Ksk+
KNdYHCB1
|1|ZiwiMM4RjJE1Q5A45AtlirH1ztI=|AjTQvsvm0+YgNk/5vUGJH6fp0OY= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDR1Qt0TTESpA469zPd6gLLvSYSAGfbibR8
8GZI0YTqu8Wd8whuW+Xl9xqIU3XsIg9qF+rMDCiLn9dmnzwAxWjxlFs0yly3PwXNg2clYDSPdng9TpYDf0QNUjJ0D8hvMaCBNq5GNh3kH9sTFQRTcznkku45iJ07577Osb9Q0
dPABVtZMQazRvMkYo0tWu/Wr/MxO+9N2nocp8SgqOOvsodpowCNP7dHQhvBBHG2qTrSMDaZ5EB8ber16Uuew2B0KKppmdVJrZvlxO3UpEiruQJSY2MrUtcsdCCbMcTFtWV1zL
UuU0H1ptWp7W7qHYIJYTptpgvXUxCVzbV6QgKNvdk+LYmdYyBPdYMM9DaFgAr25DqoNIqElnRGIPsH5nk6+39vsCWizuzzXlJjEC8ql2QDuua0GM6P4GzapC9BgvkDWCqq1Mk
6GsDBlhqmniWgJuLsZDZSHPzca5K9H1uXWlk43SXzz3p2GOoqeXJztcRy/8vrgh1Tyh+TuEU7hRd9+d0=
|1|QmVXxq1f0H+o4EbOt3yjkYN4qlQ=|8RVMx3P0DdP9dA52yYHABI3JRws= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABB
BEcn61qhBqS4cAVuCLU9l32re8LQmTLNqIvvvl50ETPz2c9kQwMouFPgHBgYh0J7Mh7jYdezWk+kg5pNKBwZWdI=
gkeymole@client07:~/.ssh$
```

Known_hosts.old : This is a backup of the previous known_hosts file, automatically created when a new host key is added or an existing one is modified

```
gkeymole@client07:~/.ssh$ cat known_hosts.old
|1|Hhbet5k2jDzIucXd8GfYBDeSf4o=|NHblXUEwPNXoZ0CZqirN4L06v/s= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFEakXin+IFSHf2JemIfPyVapniJnAU1Ksk+
KNdYHCB1
gkeymole@client07:~/.ssh$
```

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.**

```
gkeymole@client07:~/.ssh$ ssh gkeymole@192.168.50.10
gkeymole@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 17:38:59 2025 from 192.168.50.20
[gkeymole@server07 ~]$
```

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

No because the public key hasn't been copied to the server yet.

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

```
[gkeymole@server07 ~]$ exit
logout
Connection to 192.168.50.10 closed.
gkeymole@client07:~/.ssh$
```

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.

```
gkeymole@client07:~/.ssh$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/gkeymole/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/gkeymole/.ssh/id_rsa
Your public key has been saved in /home/gkeymole/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:ih1m+PdaxEVZr0JhVRaI4b7vygZ0EUywsXWry3ndijo gkeymole@client07
The key's randomart image is:
+---[RSA 3072]----+
|         o+=B=+o+|
|          **oo.o |
|         o .+.  .|
|      .   o.+.  . |
|     . + S +o. .  |
|      * o o. +.. .|
|     . + . o= . ..|
|       . oE.o. . |
|        ..+=+o.  |
+----[SHA256]-----+
gkeymole@client07:~/.ssh$
```

```
gkeymole@client07:~/.ssh$ ll
total 24
drwx------  2 gkeymole gkeymole 4096 Mar 31 18:02 ./
drwxr-x--- 18 gkeymole gkeymole 4096 Mar 30 14:29 ../
-rw-------  1 gkeymole gkeymole 2602 Mar 31 18:02 id_rsa
-rw-r--r--  1 gkeymole gkeymole  571 Mar 31 18:02 id_rsa.pub
-rw-------  1 gkeymole gkeymole  978 Mar 31 17:13 known_hosts
-rw-r--r--  1 gkeymole gkeymole  142 Mar 31 17:13 known_hosts.old
gkeymole@client07:~/.ssh$
```

ssh

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

```
gkeymole@client07:~/.ssh$ ssh-copy-id -i id_rsa.pub gkeymole@192.168.50.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "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
gkeymole@192.168.50.10's password:

Number of key(s) added: 1

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

gkeymole@client07:~/.ssh$
```

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.**

```
gkeymole@client07:~/.ssh$ ssh gkeymole@192.168.50.10
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 17:57:23 2025 from 192.168.50.20
[gkeymole@server07 ~]$ exit
logout
Connection to 192.168.50.10 closed.
gkeymole@client07:~/.ssh$
```

```
[gkeymole@server07 ~]$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCuEZeC+lauLZIUkM3fuwy2jpMNZW+fpHkMany74sQhDQgo6wsmJcR3GPpb5pzuT+ohnuWC6K0vdRYbIvpwO3m1Vlp6AcsR7
GCwmowecgcBtW6GCEgmRI+kh2bEzjc9HbVSo7iDj6TuRgPv8sv9bsce5cetDPvF/vVPkcKUSZ7lpfFUQh3giGVzzmcTAB0FG6l7n1NzC29Z55okxhkNGKQzdXKyzwtKBhHmFL
RJR03f3rsNHfKBg9LoyAwla9ipxOJlr6U5XICnafxNLaVOqPKje66QES6bo/qrKVg/D07FNuxsCmbIUbgq3ePEUvywpi71OHcenjGfv9O/z3EzrX1Jo1MxcCXAYX7wYldYaNM
XcQXHcFPInjlAAV3Y2h6jCXUPwduZyHLCoC43nkQkjwE2NBeHbyoXCdOg4Gr+heeqKsqYT1rzc+59vOL+tlwxr62tyHe5ys6ZIDsnZ3qtZX1b9WwmOOp8ZrnbE2+4fw86DB7/
SJdUX7hfxpGadQouzPc= gkeymole@client07
[gkeymole@server07 ~]$
```

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, permission denied**

```
gkeymole@client07:~/.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:
```

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.

```
root@server07 /etc/ssh $ cd sshd_config.d/
root@server07 /etc/ssh/sshd_config.d $ pwd
/etc/ssh/sshd_config.d
root@server07 /etc/ssh/sshd_config.d $ ll
total 4
-rw-------. 1 root root 719 Mar  1 03:47 50-redhat.conf
root@server07 /etc/ssh/sshd_config.d $ vim 50-redhat.conf
```

```
Include /etc/crypto-policies/back-ends/opensshserver.config

Banner /etc/ssh/banner.txt

PermitRootLogin yes

SyslogFacility AUTHPRIV

ChallengeResponseAuthentication no

GSSAPIAuthentication yes
GSSAPICleanupCredentials no

UsePAM yes

X11Forwarding yes

# It is recommended to use pam_motd in /etc/pam.d/sshd instead of PrintMotd,
# as it is more configurable and versatile than the built-in version.
PrintMotd no

-- INSERT --
```

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

```
root@server07 /etc/ssh/sshd_config.d $ systemctl reload sshd
```

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

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

```
root@server07 /etc/ssh/sshd_config.d $ tail -f /var/log/audit/audit.log
type=SERVICE_START msg=audit(1743462968.495:519): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:in
it_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="
root" AUID="unset"
```

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.**

```
gkeymole@client07:~/.ssh$ ssh root@192.168.50.10
Welcome to AlmaLinux Latino Server
root@192.168.50.10's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Mon Mar 31 19:14:26 EDT 2025 from 192.168.50.20 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Mon Mar 31 15:14:16 2025
root@server07 ~ $
```

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

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

```
type=USER_START msg=audit(1743464313.264:550): pid=4892 uid=0 auid=0 ses=12 subj=system_u:system_r:sshd_t:s0-s0:c0.c10
23 msg='op=PAM:session_open grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_li
mits,pam_systemd,pam_unix,pam_umask,pam_lastlog acct="root" exe="/usr/sbin/sshd" hostname=192.168.50.20 addr=192.168.5
0.20 terminal=ssh res=success'UID="root" AUID="root"
type=CRYPTO_KEY_USER msg=audit(1743464313.264:551): pid=4915 uid=0 auid=0 ses=12 subj=system_u:system_r:sshd_t:s0-s0:c
0.c1023 msg='op=destroy kind=server fp=SHA256:30:f3:b7:24:f6:6a:84:40:7e:92:33:f3:e9:ed:5a:cb:fc:cc:5c:3f:3d:e7:05:d1:
51:eb:23:fc:ec:91:c4:0a direction=? spid=4915 suid=0  exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'UI
D="root" AUID="root" SUID="root"
type=CRED_ACQ msg=audit(1743464313.265:552): pid=4915 uid=0 auid=0 ses=12 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 term
inal=ssh res=success'UID="root" AUID="root"
type=USER_LOGIN msg=audit(1743464313.308:553): pid=4892 uid=0 auid=0 ses=12 subj=system_u:system_r:sshd_t:s0-s0:c0.c10
23 msg='op=login id=0 exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/1 res=success'UID="root" AU
ID="root" ID="root"
type=USER_START msg=audit(1743464313.308:554): pid=4892 uid=0 auid=0 ses=12 subj=system_u:system_r:sshd_t:s0-s0:c0.c10
23 msg='op=login id=0 exe="/usr/sbin/sshd" hostname=? addr=192.168.50.20 terminal=/dev/pts/1 res=success'UID="root" AU
ID="root" ID="root"
```

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

```
type=BPF msg=audit(1743464343.431:560): prog-id=63 op=UNLOAD
type=BPF msg=audit(1743464343.431:561): prog-id=62 op=UNLOAD
^C
root@server07 /etc/ssh/sshd_config.d $
```

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

```
root@server07 ~ $ exit
logout
Connection to 192.168.50.10 closed.
gkeymole@client07:~/.ssh$
```

X11 FORWARDING

Exercise 1.5: Tasks to Perform on Ubuntu:

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

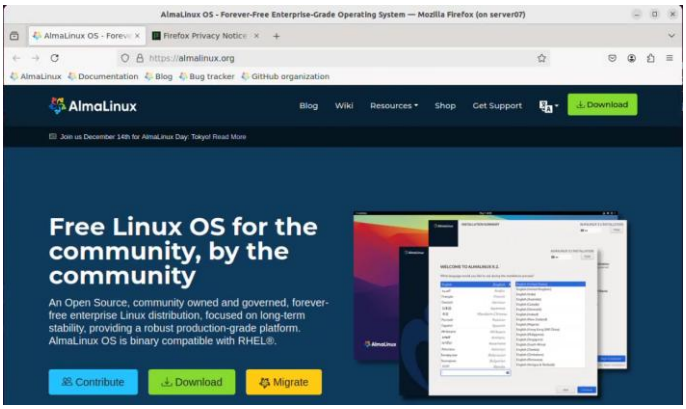
```
gkeymole@client07:~/.ssh$ ssh -X gkeymole@192.168.50.10
Welcome to AlmaLinux Latino Server
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Mar 31 19:14:29 2025 from 192.168.50.20
/usr/bin/xauth:  file /home/gkeymole/.Xauthority does not exist
[gkeymole@server07 ~]$
```

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

```
[gkeymole@server07 ~]$ firefox&
[1] 4988
[gkeymole@server07 ~]$
```

```
[gkeymole@server07 ~]$ firefox&
[1] 5364
```

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.

```
root@server07 /etc/ssh/sshd_config.d $ ps -a | grep firefox
   4988 pts/1    00:00:15 firefox
root@server07 /etc/ssh/sshd_config.d $ ps aux | grep firefox
gkeymole    4988 15.9 11.9 3339880 442652 pts/1  Sl   19:48   0:15 /usr/lib64/firefox/firefox
gkeymole    5042  0.0  1.4 268112 52480 pts/1    Sl   19:48   0:00 /usr/lib64/firefox/firefox -contentproc -parentBuil
dID 20250310042414 -prefsLen 21372 -prefMapSize 246854 -appDir /usr/lib64/firefox/browser {73e51d85-665d-49ec-b9c2-005
563a18166} 4988 socket
gkeymole    5083  0.3  3.1 2708040 117392 pts/1  Sl   19:48   0:00 /usr/lib64/firefox/firefox -contentproc -childID 1
-isForBrowser -prefsLen 23302 -prefMapSize 246854 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/
firefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {b2f8738b-ef0a-4a83-a33
3-e377fc848778} 4988 tab
gkeymole    5109  0.3  3.6 2698344 135232 pts/1  Sl   19:48   0:00 /usr/lib64/firefox/firefox -contentproc -childID 2
-isForBrowser -prefsLen 23730 -prefMapSize 246854 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/
firefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {c3f66734-1684-42d7-82a
1-2de77824ceb3} 4988 tab
gkeymole    5133  0.2  3.6 2716368 135524 pts/1  Sl   19:48   0:00 /usr/lib64/firefox/firefox -contentproc -childID 3
-isForBrowser -prefsLen 24186 -prefMapSize 246854 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/
firefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {9f544bdd-f146-4ef2-8a5
0-71bf6bc4f384} 4988 tab
gkeymole    5151  1.1  4.0 2723560 148920 pts/1  Sl   19:48   0:01 /usr/lib64/firefox/firefox -contentproc -childID 4
-isForBrowser -prefsLen 30548 -prefMapSize 246854 -jsInitLen 234780 -parentBuildID 20250310042414 -greomni /usr/lib64/
firefox/omni.ja -appomni /usr/lib64/firefox/browser/omni.ja -appDir /usr/lib64/firefox/browser {aec242d7-abff-4ed8-a77
d-20a44b4f556c} 4988 tab
gkeymole    5234  0.0  1.2 265112 48128 pts/1    Sl   19:48   0:00 /usr/lib64/firefox/firefox -contentproc -parentBuil
dID 20250310042414 -sandboxingKind 0 -prefsLen 32432 -prefMapSize 246854 -appDir /usr/lib64/firefox/browser {96fd4154-
f23a-4c81-9cb6-f830ac4a8f3a} 4988 utility
gkeymole    5242  0.0  2.4 2665092 91216 pts/1   Sl   19:48   0:00 /usr/lib64/firefox/firefox -contentproc -childID 5
```

```
root@server07 /etc/ssh/sshd_config.d $ netstat -tunap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      985/sshd: /usr/sbin
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      983/cupsd
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      4958/sshd: gkeymole
tcp        0      0 192.168.198.128:57470   142.251.33.163:443      TIME_WAIT   -
```

```
tcp6       0      0 ::1:6010                ::1:55366               ESTABLISHED 4958/sshd: gkeymole
tcp6       0      0 ::1:55366               ::1:6010                ESTABLISHED 5364/firefox
tcp6       0      0 ::1:55368               ::1:6010                TIME_WAIT   -
tcp6       0      0 ::1:55378               ::1:6010                TIME_WAIT   -
tcp6       0      0 ::1:55392               ::1:6010                TIME_WAIT   -
```

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

```
[gkeymole@server07 ~]$ Crash Annotation GraphicsCriticalError: |[0][GFX1-]: RenderCompositorSWGL failed mapping default framebuffer,
no dt (t=268.224) [GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt
^C
[1]+  Done                    firefox
[gkeymole@server07 ~]$
```

6. Log out of the ssh session.

```
[gkeymole@server07 ~]$ exit
logout
Connection to 192.168.50.10 closed.
gkeymole@client07:~/.ssh$
```