SSH

Experiment: 5

Aim: Installation of Open SSH between two ubuntu machines.

Description:

Remote File Sharing using SSH

OpenSSH is a powerful collection of tools for the remote control of, and transfer of data between, networked computers. You will also learn about some of the configuration settings possible with the OpenSSH server application and how to change them on your Ubuntu system.
OpenSSH is a freely available version of the Secure Shell (SSH) protocol family of tools for remotely controlling, or transferring files between computers. Traditional tools used to accomplish these functions, such as telnet or rcp, are insecure and transmit the user’s password in cleartext when used. OpenSSH provides a server daemon and client tools to facilitate secure, encrypted remote control and file transfer operations, effectively replacing the legacy tools.

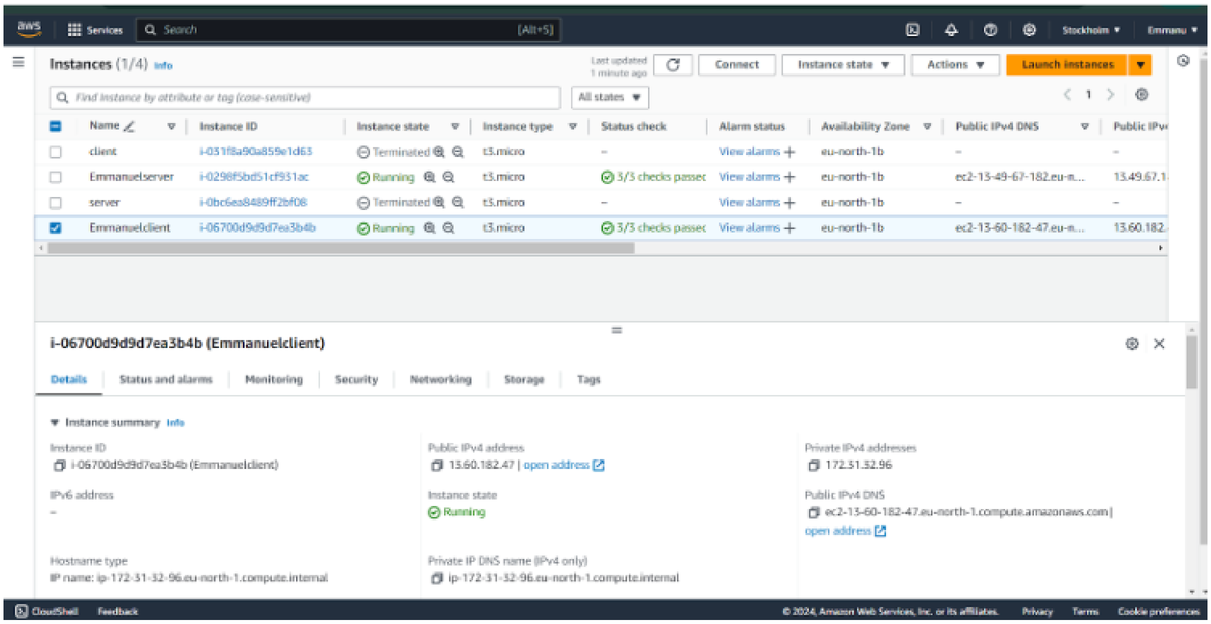
Port No: 22

Package name: openssh-client
Configuration file: /etc/ssh/sshd_config

Procedure:

1. create two EC2 instance of ubuntu ssh client and ssh server
2. Create the password for the instance of ssh server by $sudo passwd ubuntu
3. Now check whether the ssh server is running by the command $sudo servicessh status
4. configure the sshd_config file by the following command $sudo vim /etc/ssh/sshd_config and include the following changes PasswordAuthentication yes , KbdInteractiveAuthenticationno ,KerberosGetAFSToken no
5. Now check the status of the ssh server by the command $sudo service sshstatus
6. Now create a text file by the command $touch text.txt
7. Now log in to the ssh_client and create a ssh_keygen by the command $ssh_keygen
8. Now copy the ssh_keygen form the ssh_client $ssh-copy-id ubuntu@privateip
9. Now restart the client machine
10. Then connect to the ssh_server by ssh_client
11. then type ls you will be prompted with the screen with your text file which you have created

Result:



Instances (1/4) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
□	client	i-031f8a90a859e1d63	Terminated	t3.micro	–	View alarms +	eu-north-1b	–	–
□	Emmanuelserver	i-0298f5bd51cf931ac	Running	t3.micro	3/3 checks passec	View alarms +	eu-north-1b	ec2-13-49-67-182.eu-n...	13.49.67.1
□	server	i-0bc6ea8489ff2bf08	Terminated	t3.micro	–	View alarms +	eu-north-1b	–	–
☑	Emmanuelclient	i-06700d9d9d7ea3b4b	Running	t3.micro	3/3 checks passec	View alarms +	eu-north-1b	ec2-13-60-182-47.eu-n...	13.60.182.

i-06700d9d9d7ea3b4b (Emmanuelclient)

▼ Instance summary Info

Instance ID
i-06700d9d9d7ea3b4b (Emmanuelclient)

Public IPv4 address
13.60.182.47 | open address

Private IPv4 addresses
172.31.32.96

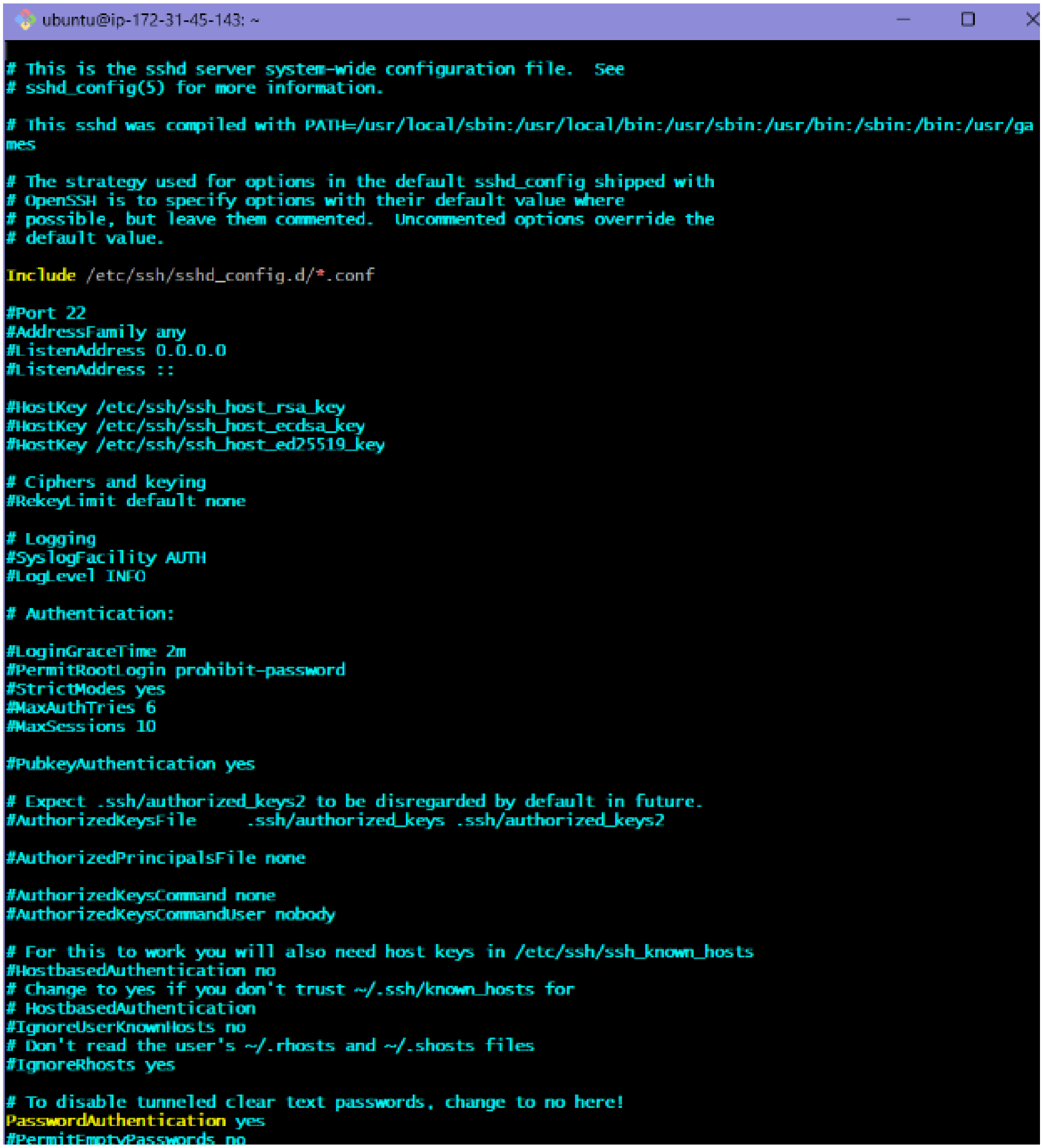
IPv6 address
–

Instance state
Running

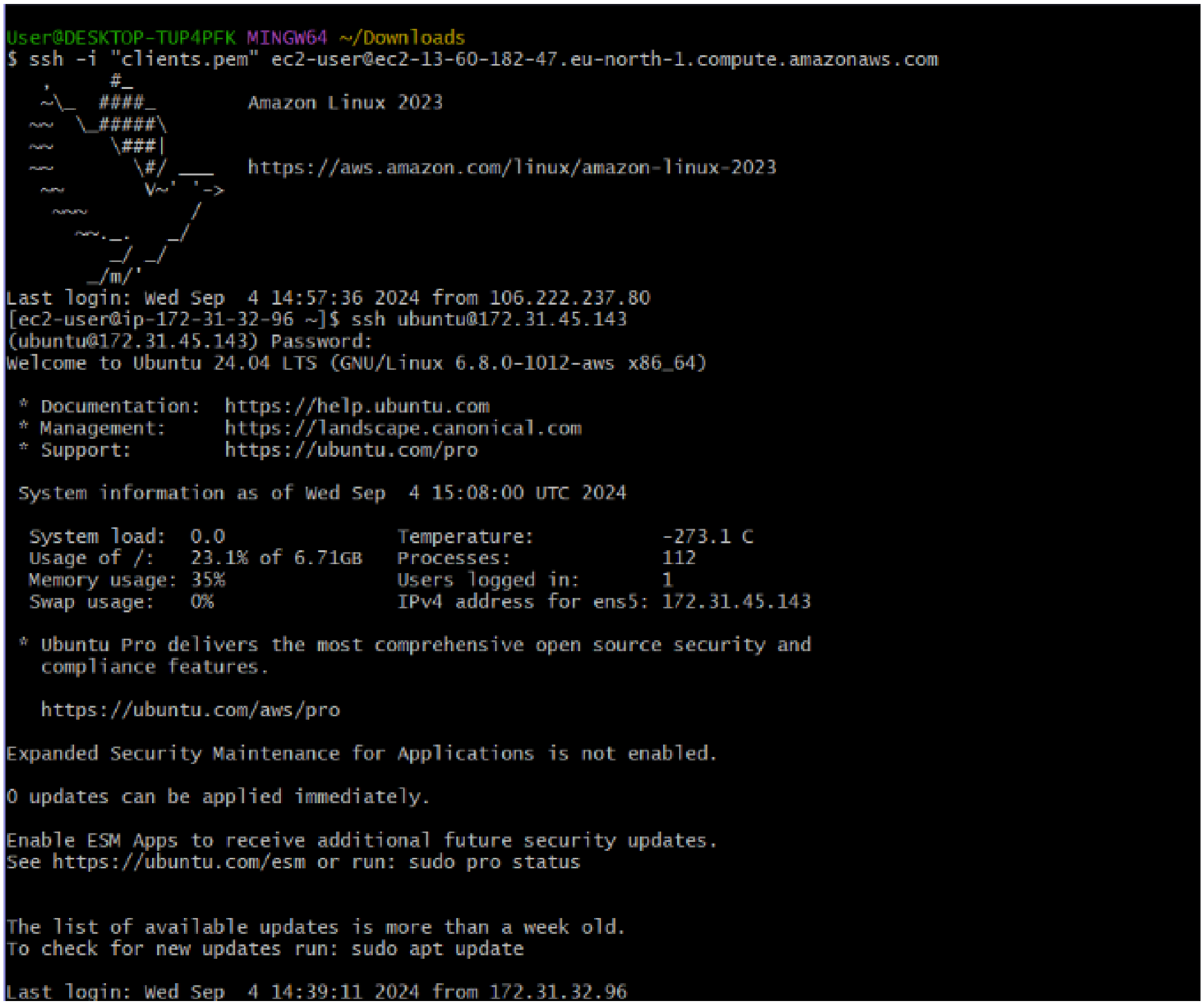
Public IPv4 DNS
ec2-13-60-182-47.eu-north-1.compute.amazonaws.com | open address

Hostname type
IP name: ip-172-31-32-96.eu-north-1.compute.internal

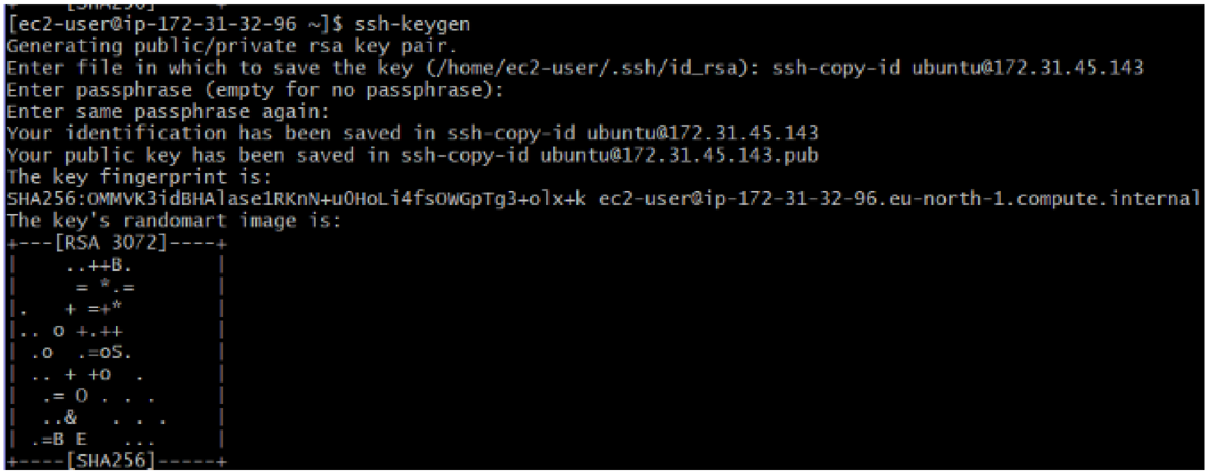
Private IP DNS name (IPv4 only)
ip-172-31-32-96.eu-north-1.compute.internal



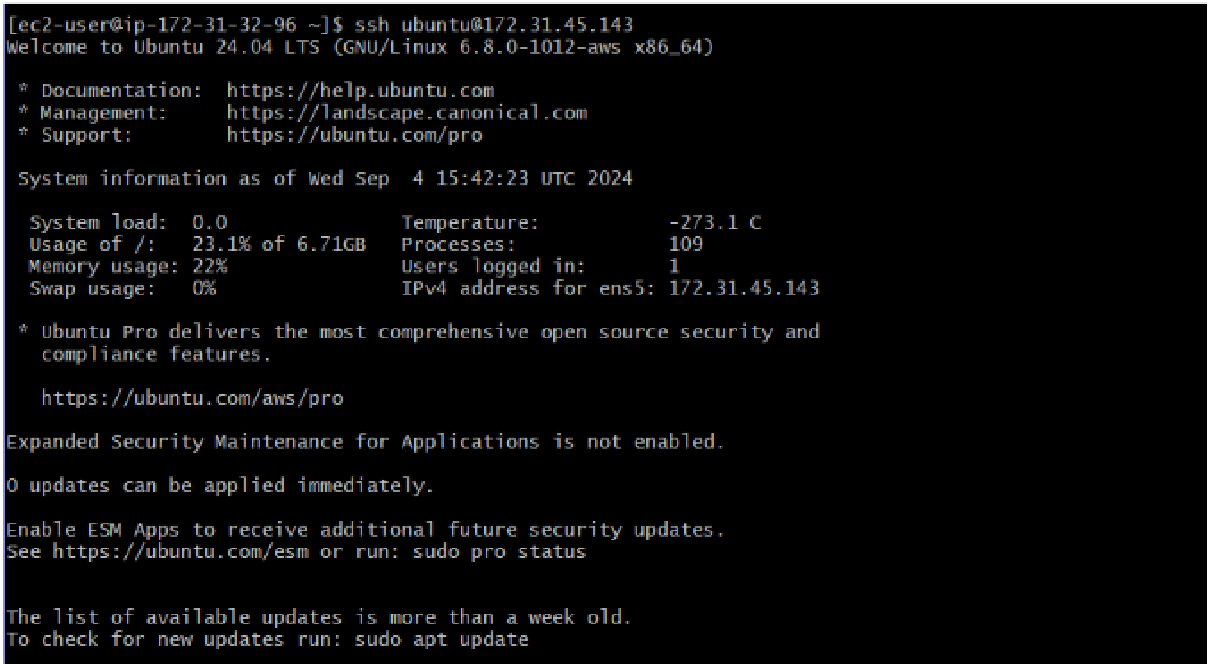
```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

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

# 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.

Include /etc/ssh/sshd_config.d/*.conf

#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

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#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
```



```
User@DESKTOP-TUP4PFK MINGW64 ~/Downloads
$ ssh -i "clients.pem" ec2-user@ec2-13-60-182-47.eu-north-1.compute.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Wed Sep  4 14:57:36 2024 from 106.222.237.80
[ec2-user@ip-172-31-32-96 ~]$ ssh ubuntu@172.31.45.143
(ubuntu@172.31.45.143) Password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

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

 System information as of Wed Sep  4 15:08:00 UTC 2024

  System load:  0.0               Temperature:           -273.1 C
  Usage of /:   23.1% of 6.71GB   Processes:             112
  Memory usage: 35%               Users logged in:       1
  Swap usage:   0%                IPv4 address for ens5: 172.31.45.143

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Sep  4 14:39:11 2024 from 172.31.32.96
```



```
[ec2-user@ip-172-31-32-96 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ec2-user/.ssh/id_rsa): ssh-copy-id ubuntu@172.31.45.143
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ssh-copy-id ubuntu@172.31.45.143
Your public key has been saved in ssh-copy-id ubuntu@172.31.45.143.pub
The key fingerprint is:
SHA256:OMMVK3idBHAlase1RKnN+uOHoLi4fsOWGpTg3+olx+k ec2-user@ip-172-31-32-96.eu-north-1.compute.internal
The key's randomart image is:
+---[RSA 3072]----+
|     ..++B.      |
|      = *.=      |
|.    + =+*       |
|.. o +.++        |
| .o  .=oS.       |
| .. + +o  .      |
|  .= O . . .     |
|  ..&   . . .    |
| .=B E   ...     |
+----[SHA256]-----+
```



```
[ec2-user@ip-172-31-32-96 ~]$ ssh ubuntu@172.31.45.143
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

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

 System information as of Wed Sep  4 15:42:23 UTC 2024

  System load:  0.0               Temperature:           -273.1 C
  Usage of /:   23.1% of 6.71GB   Processes:             109
  Memory usage: 22%               Users logged in:       1
  Swap usage:   0%                IPv4 address for ens5: 172.31.45.143

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

All the commands have been executed and the output has been obtained successfully.