Establish Key-Based SSH Access Between servers

Objective:
This task involves setting up secure key-based SSH access for the root user on ubuntu.example.com to access the root user on opensuse.example.com, and vice versa. This will enable secure and passwordless communication between the two servers.

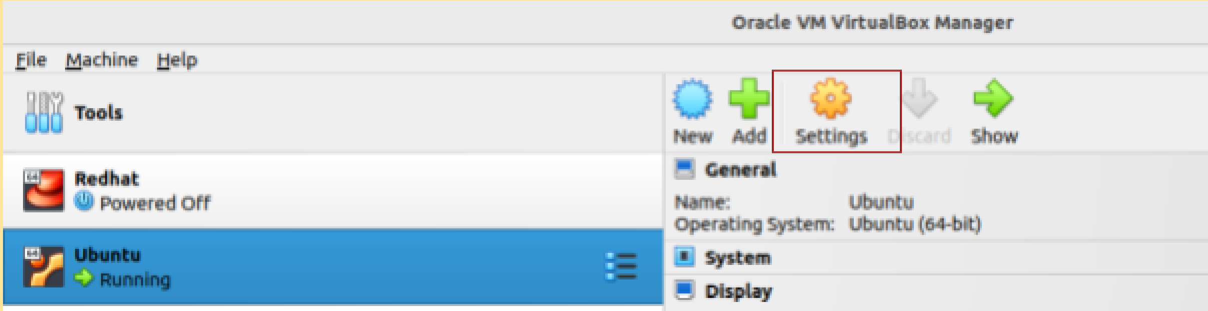
Scenario:
Currently, the root users on both ubuntu.example.com and opensuse.example.com rely on password-based authentication for SSH access. This method is less secure than key-based authentication. You will configure key-based SSH to improve security and streamline access between the servers.

Solution :-

> Simultaneously on both system ubuntu.example.com & opensuse.example.com

Step 1 :- Open VirtualBox and Change Network.

- Click on Ubuntu Vm and Select Settings.



Redhat
Powered Off

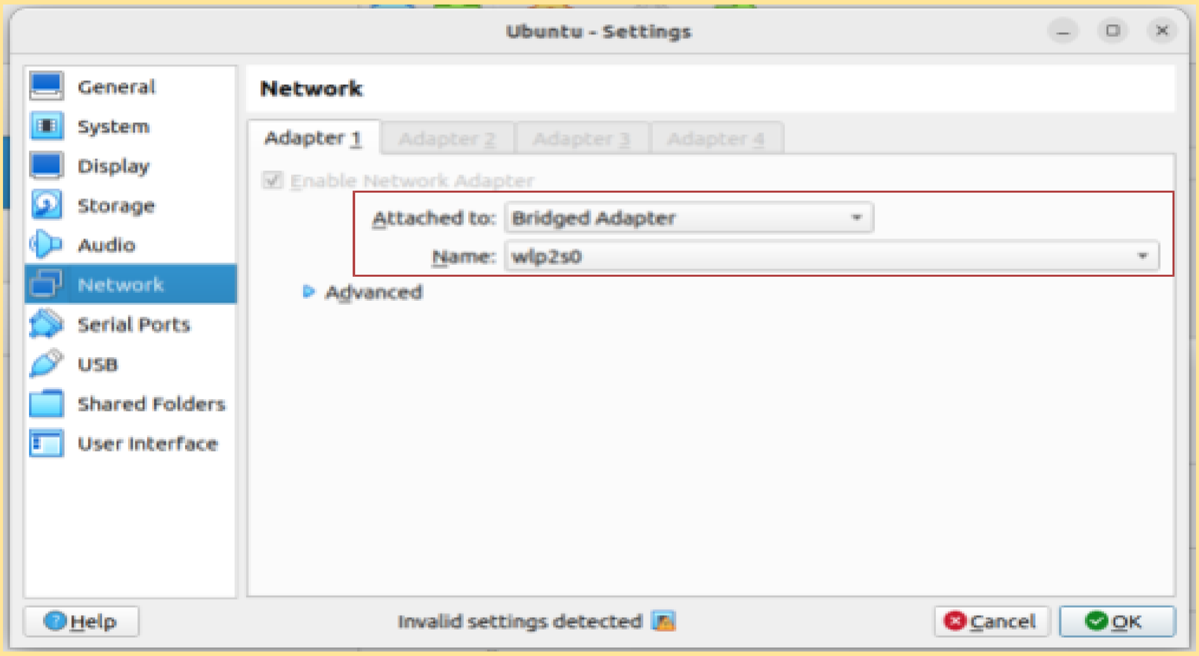
Ubuntu
Running

General
Name: Ubuntu
Operating System: Ubuntu (64-bit)

System

Display

- Select Network Option and Change Attached Network to Bridge Network.



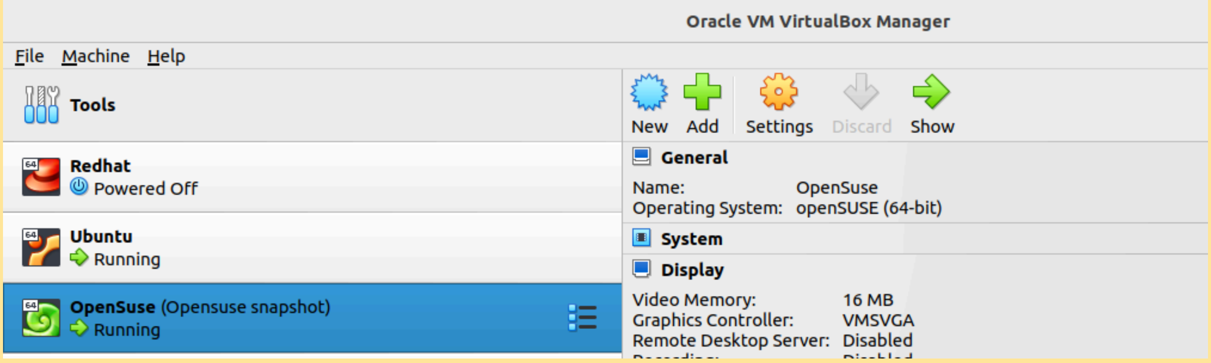
☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: wlp2s0

Invalid settings detected

- Click on OpenSuse Vm and Select Settings.



Redhat
Powered Off

Ubuntu
Running

OpenSuse (Opensuse snapshot)
Running

General

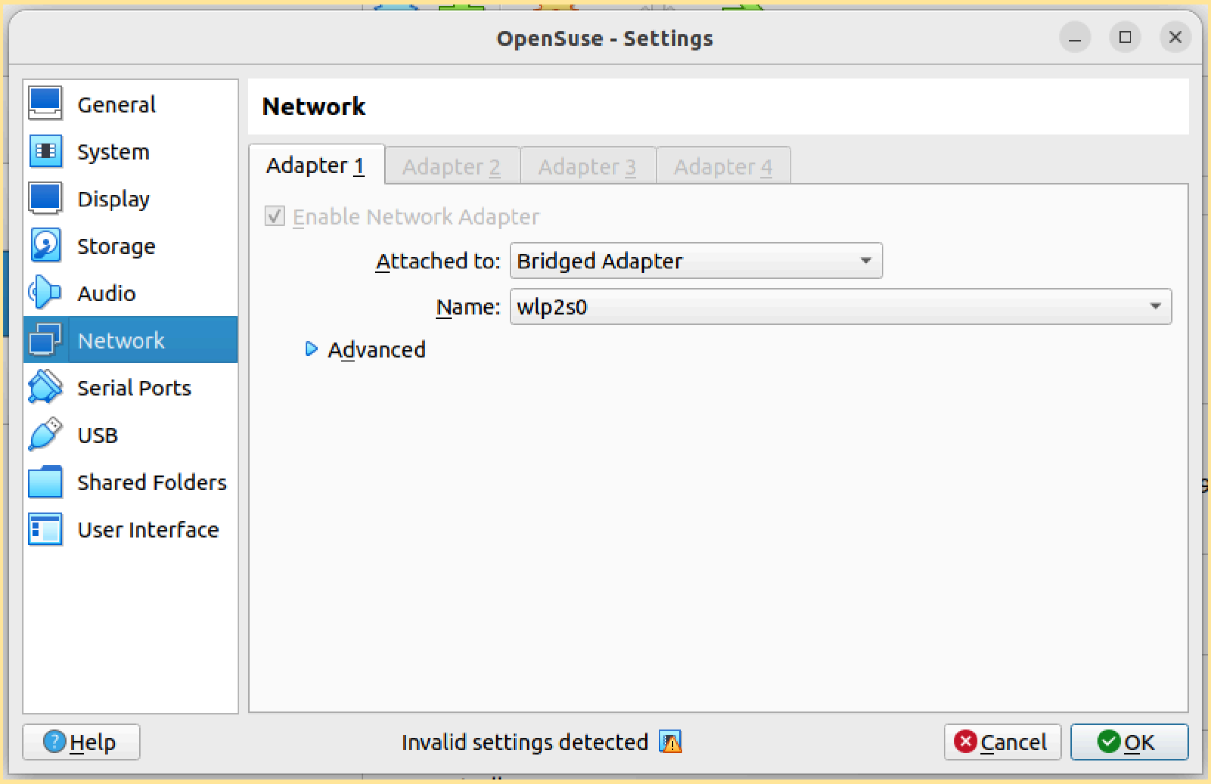
Name: OpenSuse
Operating System: openSUSE (64-bit)

System

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled

- Select Network Option and Change Attached Network to Bridge Network.



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: wlp2s0

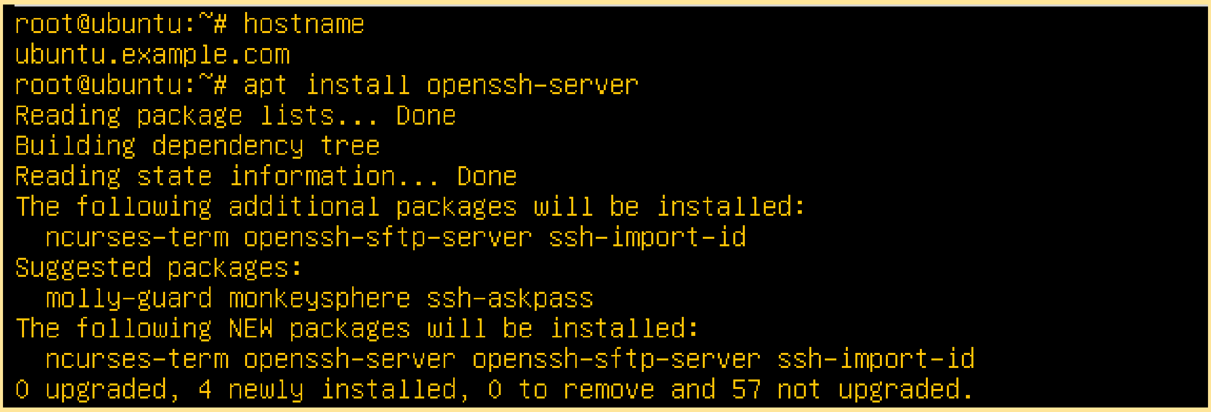
Invalid settings detected

Step 2 :- Start the both VM and login with root user.

- Start the Vm which has hostname ubuntu.example.com and opensuse.example.com

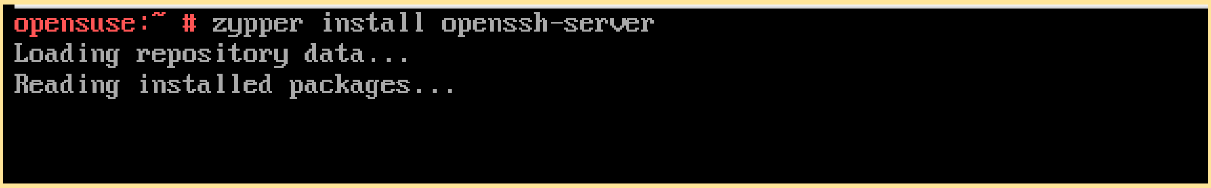
Step 3 :- Install openssh-server package.

- In Ubuntu, execute **apt install openssh-server** command.



```
root@ubuntu:~# hostname
ubuntu.example.com
root@ubuntu:~# apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 57 not upgraded.
```

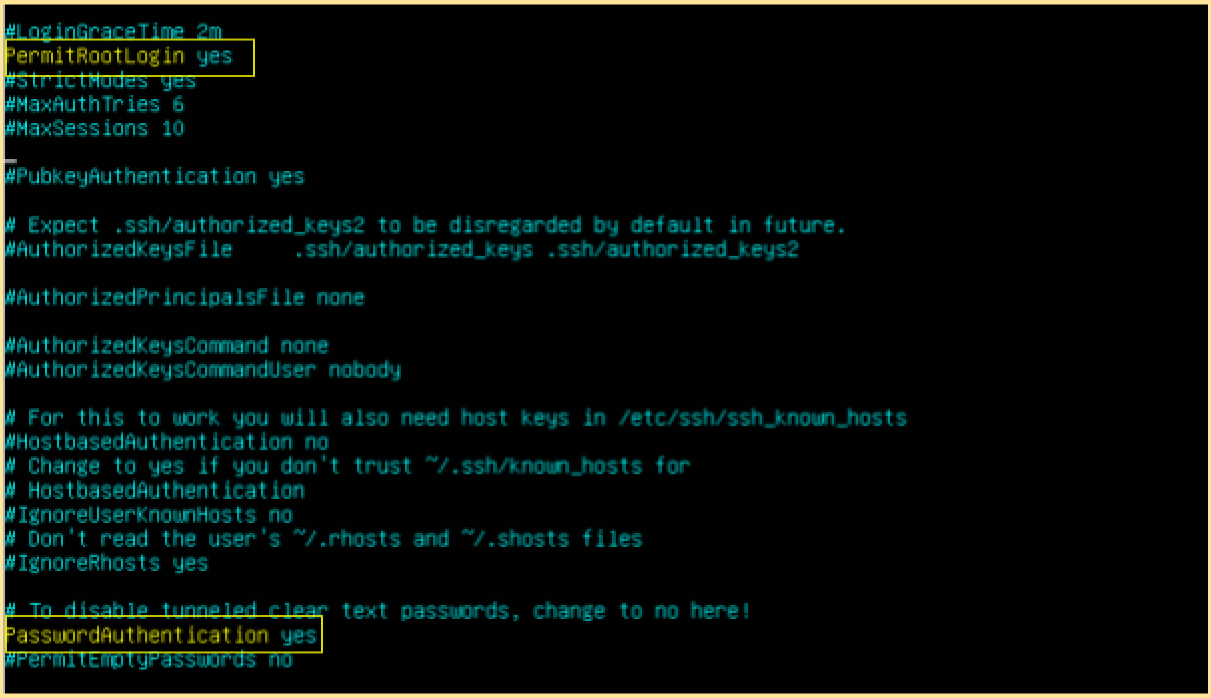
- In Opensuse, execute **zypper install openssh-server** command.



```
opensuse:~ # zypper install openssh-server
Loading repository data...
Reading installed packages...
```

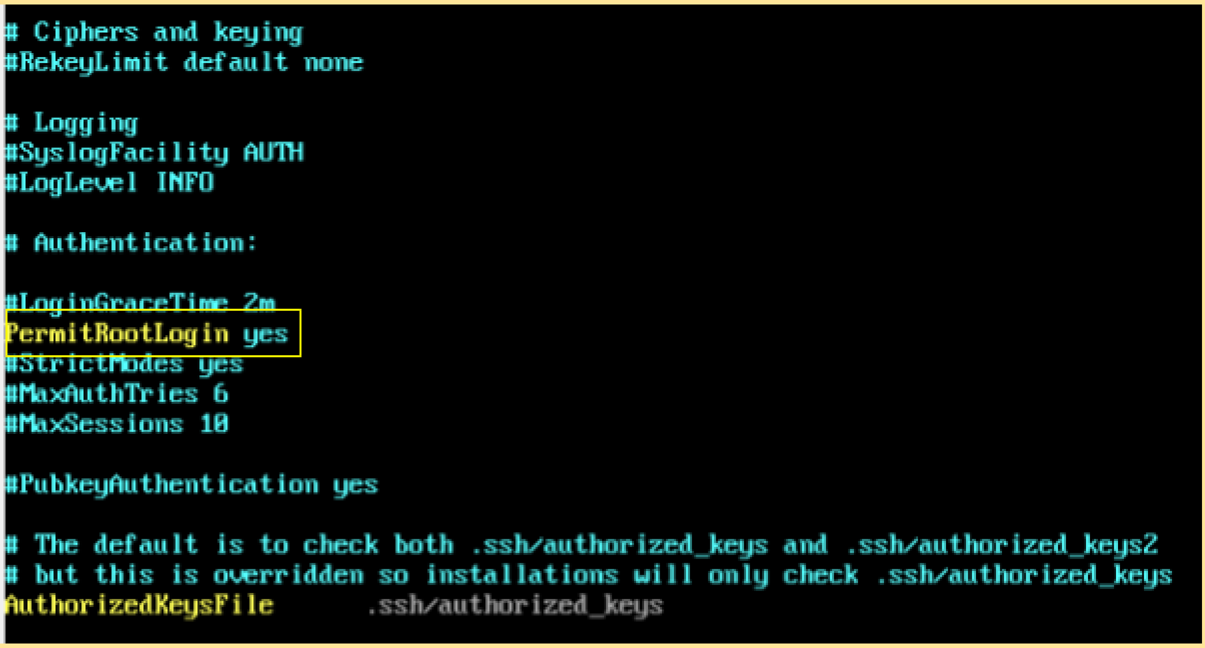
Step :- Change Default settings of /etc/ssh/sshd_config file

- In Ubuntu, execute **vi /etc/ssh/sshd_config** command to open file in vi editor.
- Change **PermitRootLogin** and **PasswordAuthentication** to **yes.**



```
#LoginGraceTime 2m
PermitRootLogin yes
#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
```

- In Opensuse, execute **vi /etc/ssh/sshd_config** command to open file in vi editor.
- Change **PermitRootLogin** to **yes.**



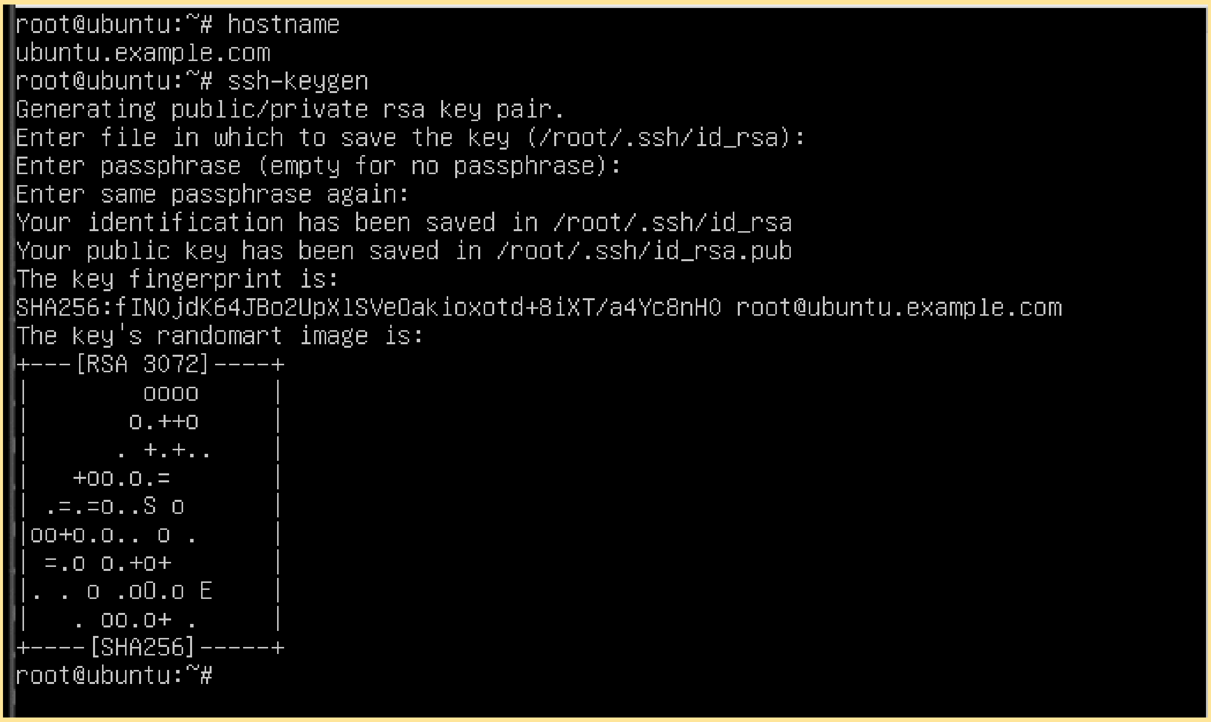
```
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
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
```

In Ubuntu Virtual Machine

To Access Opensuse Virtual Machine From Ubuntu Virtual Machine with ssh

Step 1 :- SSH-KEYGEN

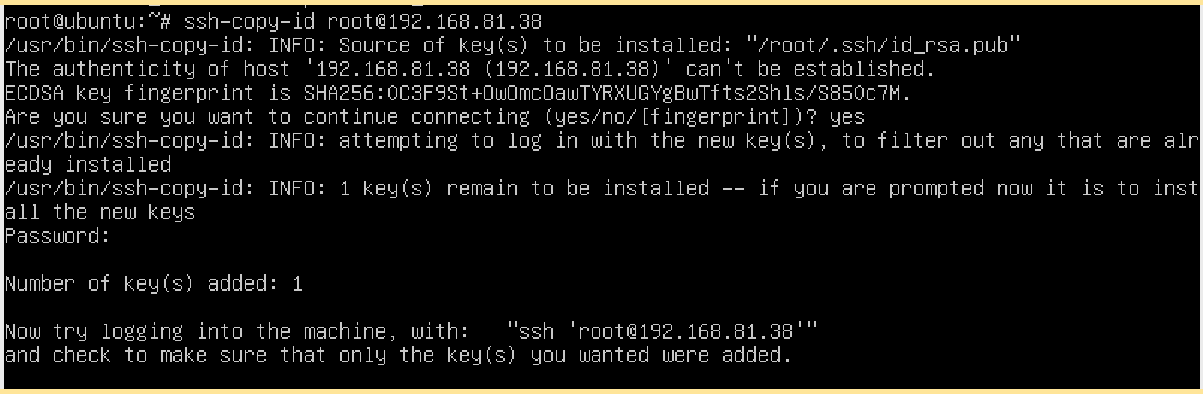
- Execute **ssh-keygen** command in ubuntu..example.com



```
root@ubuntu:~# hostname
ubuntu.example.com
root@ubuntu:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:fINOjdK64JBo2UpXlSVeOakioxotd+8iXT/a4Yc8nHO root@ubuntu.example.com
The key's randomart image is:
+---[RSA 3072]----+
|        oooo     |
|       o.++o     |
|      . +.+..    |
|   +oo.o.=       |
| .=.=o..S o      |
|oo+o.o.. o .     |
| =.o o.+o+       |
|. . o .oO.o E    |
|   . oo.o+ .     |
+----[SHA256]-----+
root@ubuntu:~#
```

Step 2 :- Copy Id of ssh to opensuse.example.com machine

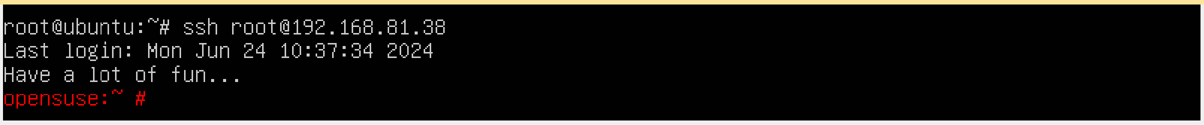
- Check ip of opensuse.example.com
- Execute **ssh-copy-id root@<ip_of_opensuse.example.com>** command.
- Enter password of root user of opensuse.example.com machine for authentication for first time.



```
root@ubuntu:~# ssh-copy-id root@192.168.81.38
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.81.38 (192.168.81.38)' can't be established.
ECDSA key fingerprint is SHA256:OC3F9St+OwOmcOawTYRXUGYgBwTfts2Shls/S85Oc7M.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.81.38'"
and check to make sure that only the key(s) you wanted were added.
```

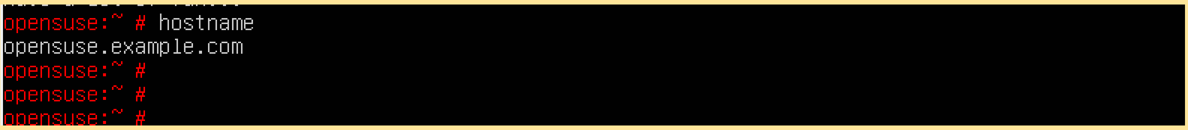
Step 3 :- Access opensuse.example.com via ssh command

- Execute **ssh root@<ip_of_opensuse.example.com>** command.



```
root@ubuntu:~# ssh root@192.168.81.38
Last login: Mon Jun 24 10:37:34 2024
Have a lot of fun...
opensuse:~ #
```

- Check hostname for confirmation.



```
opensuse:~ # hostname
opensuse.example.com
opensuse:~ #
opensuse:~ #
opensuse:~ #
```

Congratulation..!
You Have Successfully Established Connection Between Ubuntu to Opensuse Virtual Machine

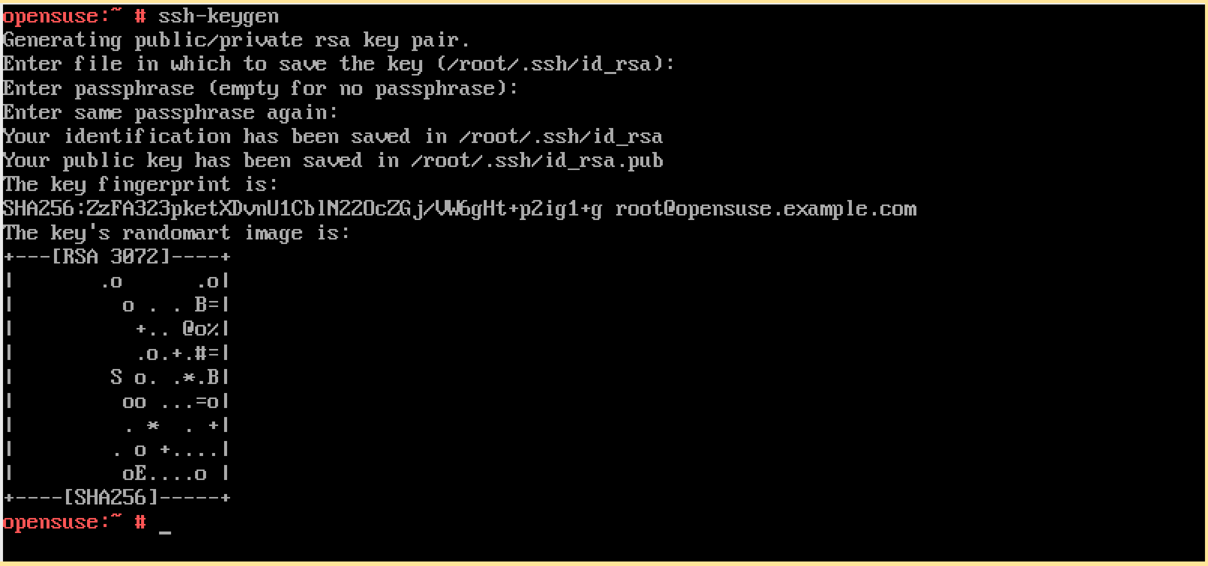
In OpenSuse Virtual Machine

To Access Ubuntu Virtual Machine From OpenSuse Virtual Machine with ssh

Perform the same process which is perform in ubuntu.example.com

Step 1 :- SSH-KEYGEN

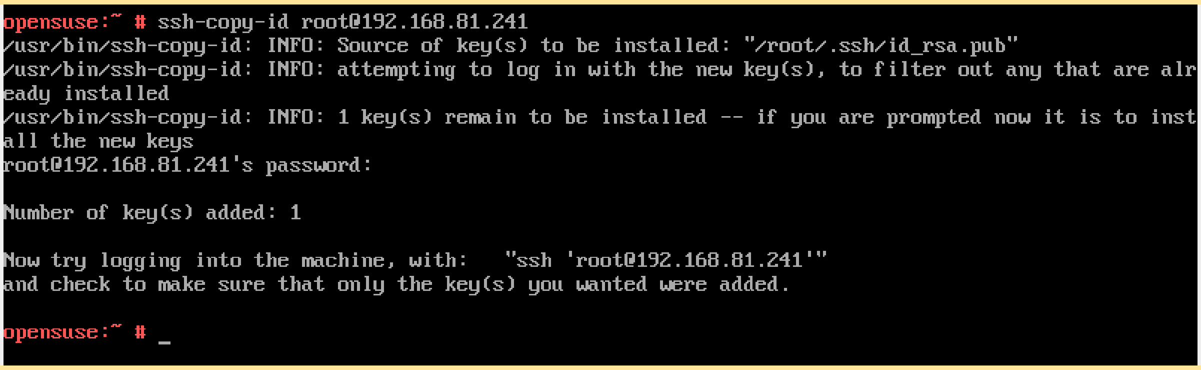
- Execute **ssh-keygen** command in opensuse.example.com



```
opensuse:~ # ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:ZzFA323pketXDvnU1CblN22OcZGj/VW6gHt+p2ig1+g root@opensuse.example.com
The key's randomart image is:
+---[RSA 3072]----+
|       .o      .o|
|         o . . B=|
|          +.. @o%|
|          .o.+.#=|
|        S o. .*.B|
|         oo ...=o|
|         . *  . +|
|        . o +....|
|         oE....o |
+----[SHA256]-----+
opensuse:~ # _
```

Step 2 :- Copy Id of ssh to ubuntu.example.com machine

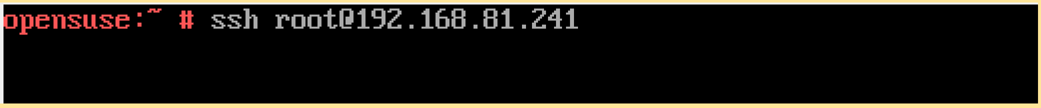
- Check ip of ubuntu.example.com
- Execute **ssh-copy-id root@<ip_of_ubuntu.example.com>** command.
- Enter password of root user of ubuntu.example.com machine for authentication for the first time.



```
opensuse:~ # ssh-copy-id root@192.168.81.241
/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 alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
root@192.168.81.241's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.81.241'"
and check to make sure that only the key(s) you wanted were added.

opensuse:~ # _
```

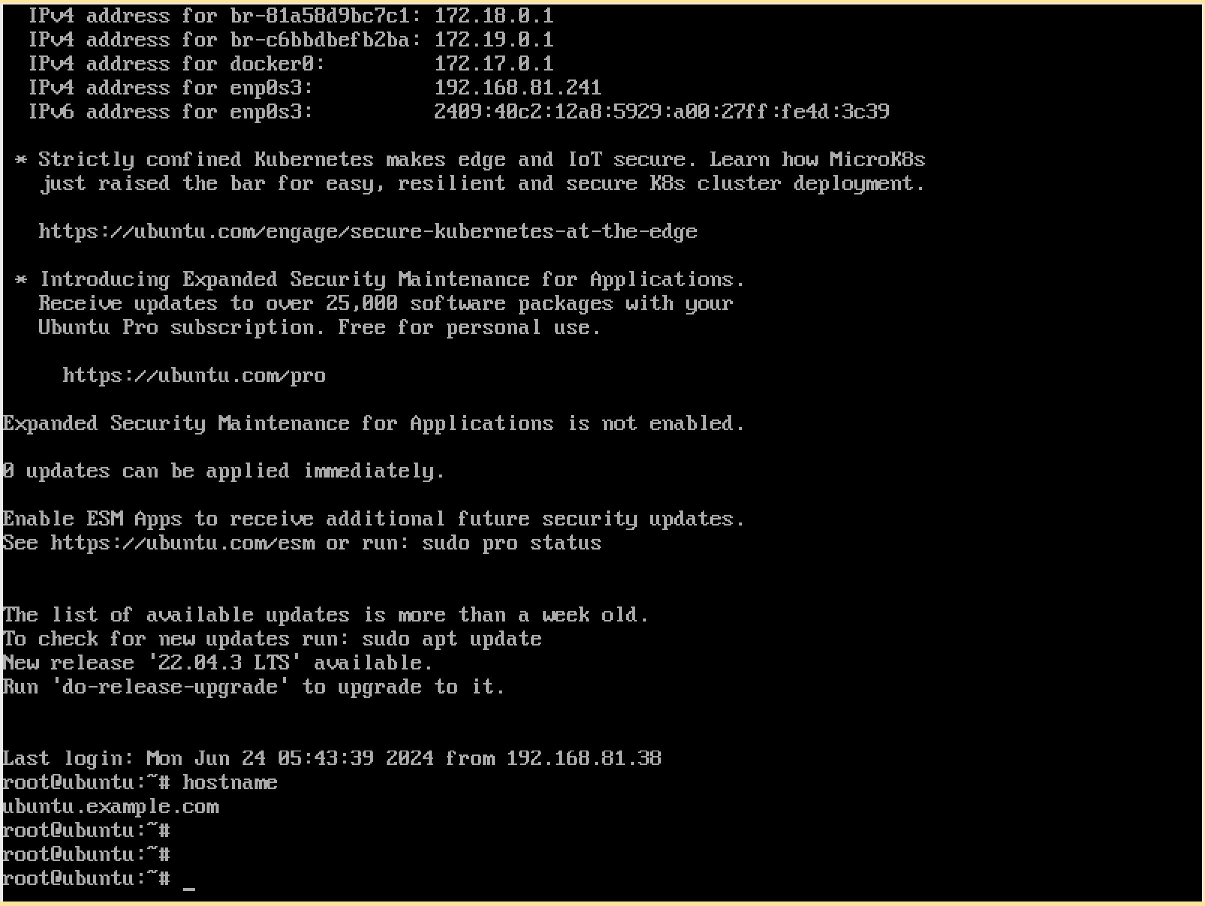
Step 3 :- Access ubuntu.example.com via ssh command

- Execute **ssh root@<ip_of_ubuntu.example.com>** command.



```
opensuse:~ # ssh root@192.168.81.241
```

- Check hostname for confirmation.



```
  IPv4 address for br-81a58d9bc7c1: 172.18.0.1
  IPv4 address for br-c6bbdbefb2ba: 172.19.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for enp0s3:          192.168.81.241
  IPv6 address for enp0s3:          2409:40c2:12a8:5929:a00:27ff:fe4d:3c39

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/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
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Jun 24 05:43:39 2024 from 192.168.81.38
root@ubuntu:~# hostname
ubuntu.example.com
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~# _
```

Congratulation..!
You Have Successfully Established Connection
Between Opensuse to Ubuntu Virtual Machine