Configure Secure Key-Based SSH Access Between Root Users on Ubuntu and OpenSUSE 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.

Introduction

- Why this task?
  - Secure server-to-server communication is critical in system administration.
  - Password-based SSH is less secure and inconvenient.
- What we are doing?
  - Configuring SSH key-based authentication between:
    - ubuntu.example.com (root) → opensuse.example.com (root)
    - opensuse.example.com (root) → ubuntu.example.com (root)
- Benefits of key-based SSH:
  - Eliminates the need to type passwords.
  - Stronger security compared to password-based login.
  - Faster and more reliable access between servers.
  - Reduces risk of brute-force attacks.
- End Goal:
  - Enable secure, passwordless SSH communication between the two servers for root users.

UBUNTU

Step 1. Update package repository

```
root@ubuntu:~# apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
378 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ubuntu:~#
```

📌 This refreshes the package index to ensure you get the latest available versions.

Step 2. Install OpenSSH Server

```
root@ubuntu:~# apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.2p1-4ubuntu0.13).
0 upgraded, 0 newly installed, 0 to remove and 378 not upgraded.
root@ubuntu:~#
```

- Installs the SSH server package which allows remote login over SSH.
- In the screenshot, it shows that the latest version was already installed.

Step 3. Start SSH service Enable SSH service

```
root@ubuntu:~# systemctl start ssh
root@ubuntu:~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@ubuntu:~#
```

- Starts the SSH service immediately so that it begins accepting connections.
- Configures the SSH service to start automatically every time the system boots.

Step 4. Check SSH service status

```
root@ubuntu:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-08-22 09:38:36 IST; 4min 3s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 2220 (sshd)
      Tasks: 1 (limit: 3448)
     Memory: 4.9M
     CGroup: /system.slice/ssh.service
             └─2220 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 22 09:38:59 ubuntu.example.com sshd[2222]: Accepted password for uddhav from 192.168.50.87 port 57540 ssh2
Aug 22 09:38:59 ubuntu.example.com sshd[2222]: pam_unix(sshd:session): session opened for user uddhav by (uid=>
Aug 22 09:39:17 ubuntu.example.com sshd[2420]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eui>
Aug 22 09:39:20 ubuntu.example.com sshd[2420]: Failed password for root from 192.168.50.68 port 60611 ssh2
Aug 22 09:39:23 ubuntu.example.com sshd[2420]: error: Received disconnect from 192.168.50.68 port 60611:13: Un>
Aug 22 09:39:23 ubuntu.example.com sshd[2420]: Disconnected from authenticating user root 192.168.50.68 port 6>
Aug 22 09:39:27 ubuntu.example.com sshd[2422]: Accepted password for uddhav from 192.168.50.68 port 60612 ssh2
Aug 22 09:39:27 ubuntu.example.com sshd[2422]: pam_unix(sshd:session): session opened for user uddhav by (uid=>
Aug 22 09:39:28 ubuntu.example.com sshd[2424]: Accepted password for uddhav from 192.168.50.68 port 60613 ssh2
Aug 22 09:39:28 ubuntu.example.com sshd[2424]: pam_unix(sshd:session): session opened for user uddhav by (uid=>
lines 1-21/21 (END)
```

📌 Verifies if the OpenSSH service is active and running.

📌 The screenshot confirms the service is enabled and active.

Step 5. Attempt SSH login to remote machine

```
root@ubuntu:~# ssh uddhav@192.168.50.196
The authenticity of host '192.168.50.196 (192.168.50.196)' can't be established.
ECDSA key fingerprint is SHA256:mxcWTQvwxlnizMuIlR1a/+IgckmQNCQageLOtLWIbPE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.196' (ECDSA) to the list of known hosts.
Password:
```

- Tries to connect to the remote host (192.168.50.196) using user uddhav.
- On first connection, it asks to trust the remote host's fingerprint.
- After accepting (yes), it saves the host in the known_hosts file.
- The connection proceeds, but it requires a password since key-based authentication is not yet configured.

Step 6. Generate SSH key pair

```
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:x5yuDz0pKvmk4/w2mFlcU9vqVXnt+af29mzwAMFfHeE root@ubuntu.example.com
The key's randomart image is:
+---[RSA 3072]----+
|           .   o+|
|          . o . o|
|         . o o E.|
|        oo..o + o|
|     . .S.=. o o.|
|      o  +... o..|
|     *. o.=.   +.|
|   .Boo. +..  ..*|
|   .+*+....  ..=*|
+----[SHA256]-----+
root@ubuntu:~#
```

- Creates a public/private RSA key pair (/root/.ssh/id_rsa and /root/.ssh/id_rsa.pub).
- The user can set a passphrase (optional, can press Enter for none).
- This private key will be used to authenticate securely without passwords.

Step 7. Copy the public key to the remote server

```
root@ubuntu:~# ssh-copy-id uddhav@192.168.50.196
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already instal
led
/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
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'uddhav@192.168.50.196'"
and check to make sure that only the key(s) you wanted were added.
```

- Transfers the generated public key (id_rsa.pub) to the remote host's ~/.ssh/authorized_keys.
- Once added, the remote host recognizes this key for authentication.
- After this step, you can log in without typing the password.

Step 8. SSH into Remote Host (openSUSE)

```
root@ubuntu:~# ssh uddhav@192.168.50.196
Have a lot of fun...
Last login: Fri Aug 22 09:44:26 2025 from 192.168.50.87
uddhav@opensuse:~>
```

- Successfully connects from Ubuntu to openSUSE without a password (thanks to key-based authentication).
- The login banner (Have a lot of fun...) confirms entry into the openSUSE system.

Step 9. Verify Current Working Directory, Current User, Host Details

```
uddhav@opensuse:~> pwd
/home/uddhav
uddhav@opensuse:~> whoami
uddhav
uddhav@opensuse:~> hostnamectl
   Static hostname: opensuse.example.com
Transient hostname: opensuse
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 2371e01d885b4db586c6520f60acc8a4
           Boot ID: 8924ce081b8746648bf9b6916b5ab55d
    Virtualization: oracle
  Operating System: openSUSE Leap 15.6
       CPE OS Name: cpe:/o:opensuse:leap:15.6
            Kernel: Linux 6.4.0-150600.23.60-default
      Architecture: x86-64
   Hardware Vendor: innotek GmbH
    Hardware Model: VirtualBox
  Firmware Version: VirtualBox
     Firmware Date: Fri 2006-12-01
      Firmware Age: 18y 8month 3w
uddhav@opensuse:~>
```

📌 Displays detailed system information about the openSUSE server, such as:

- Hostname (opensuse.example.com)
- OS version (openSUSE Leap 15.6)
- Virtualization platform (VirtualBox)
- Kernel version
- Architecture (x86-64)

Step 10. Edit the Hosts File (openSUSE side)

```
root@ubuntu:~# vi /etc/hosts
root@ubuntu:~#
```

- Maps the local system IP to hostname for easy identification.
- Example entry added:

```
127.0.0.1       localhost
192.168.50.196  opensuse.example.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
```

- /etc/hosts entry is used for local DNS resolution. It maps a hostname to its IP address, enabling systems to communicate using easy-to-remember names instead of numeric IPs.`

OpenSUSE

Step 11. Install OpenSSH package

```
opensuse:~ # zypper install openssh
Looking for gpg keys in repository Update repository of openSUSE Backports.
  gpgkey=http://download.opensuse.org/update/leap/15.6/backports/repodata/repomd.xml.key
Retrieving repository 'Update repository of openSUSE Backports' metadata .....
Building repository 'Update repository of openSUSE Backports' cache .....
Building repository 'Non-OSS Repository' cache .....
Retrieving repository 'Open H.264 Codec (openSUSE Leap)' metadata .....
Building repository 'Open H.264 Codec (openSUSE Leap)' cache .....
Building repository 'Main Repository' cache .....[done]
Looking for gpg keys in repository Update repository with updates from SUSE Linux Enterprise 15.
  gpgkey=http://download.opensuse.org/update/leap/15.6/sle/repodata/repomd.xml.key
```

Step 12. Enable and start the SSH service and Check SSH service status

```
opensuse:~ # systemctl start sshd
opensuse:~ # systemctl enable sshd
opensuse:~ # systemctl status sshd
● sshd.service - OpenSSH Daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-08-22 12:36:20 IST; 2min 12s ago
   Main PID: 1782 (sshd)
      Tasks: 1
        CPU: 220ms
     CGroup: /system.slice/sshd.service
             └─1782 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 12:36:20 opensuse systemd[1]: Starting OpenSSH Daemon...
Aug 22 12:36:20 opensuse sshd-gen-keys-start[1769]: Checking for missing server keys in /etc/ssh
Aug 22 12:36:20 opensuse sshd[1782]: Server listening on 0.0.0.0 port 22.
Aug 22 12:36:20 opensuse sshd[1782]: Server listening on :: port 22.
Aug 22 12:36:20 opensuse systemd[1]: Started OpenSSH Daemon.
Aug 22 12:36:57 opensuse sshd[14177]: Accepted keyboard-interactive/pam for root from 192.168.50.68 port 63274 ssh2
Aug 22 12:36:58 opensuse sshd[14177]: pam_unix(sshd:session): session opened for user root by (uid=0)
Aug 22 12:36:58 opensuse sshd[14182]: Accepted password for root from 192.168.50.68 port 63275 ssh2
Aug 22 12:36:58 opensuse sshd[14182]: pam_unix(sshd:session): session opened for user root by (uid=0)
opensuse:~ #
```

📌 Confirms that the **sshd service** is running.

- Shows log entries for successful SSH connections.

Step 13. Allow SSH through the firewall

```
opensuse:~ # sudo firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
opensuse:~ # firewall-cmd --reload
success
opensuse:~ #
```

- --permanent ensures the rule is saved permanently.
- firewall-cmd --reload reloads the firewall rules.

Step 14. (Optional) Edit the hosts file

```
opensuse:~ # vi /etc/hosts
opensuse:~ #
```

📌 This step is used to configure hostname-to-IP mappings if needed.

```
192.168.50.87   ubuntu.example.com

127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
```

Step 15. Generate SSH Key Pair on openSUSE

```
opensuse:~ # ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
/root/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:p8MbRqjkff6YKLY2ILCE5udlVEuvAQGUYfWvvaKj7oA root@opensuse
The key's randomart image is:
+--[ED25519 256]--+
|   .==o.         |
|  .. ..o         |
|.     +.o        |
|oo   . +..       |
|=.  o . S..      |
|+..+ = +oo       |
|Eoo.= ..B.       |
|  ..=. * *.      |
|  o*o=+ *o.      |
+----[SHA256]-----+
opensuse:~ #
```

- Generates a public/private key pair (id_ed25519 by default).
- Press **Enter** to accept defaults.
- Optionally set a passphrase (or leave empty for no passphrase).

Step 16. Copy Public Key to Remote Machine (Ubuntu)

```
opensuse:~ # ssh-copy-id uddhav@192.168.50.87
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already instal
led
/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
uddhav@192.168.50.87's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'uddhav@192.168.50.87'"
and check to make sure that only the key(s) you wanted were added.
```

- Installs your **public key** into the remote user's ~/.ssh/authorized_keys.
- Requires the remote user password **only once**.
- After success, the key-based login will be enabled.

Step 17. Verify SSH Login Without Password

```
opensuse:~ # ssh uddhav@192.168.50.87
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

 * 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 Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra 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 '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Aug 22 09:39:30 2025 from 192.168.50.68
uddhav@ubuntu:~$
```

📌 You should now log in directly **without being prompted for a password**.

Conclusion

- Passwordless SSH access was successfully configured between Ubuntu and openSUSE.
- This enhances **security** by reducing dependency on password authentication.
- It improves **efficiency** for remote administration and system management.
- Provides a **reliable and secure communication channel** between servers.