

Steps to Configure SSH Key-Based Authentication

Step 1:- Logged in to Server A and created ssh key

```
root@ServerA:~# 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:ezuCEqTScAhR+AQ8F+7tHT07h6vyUgtETsorrsmT2R0 root@ServerA
The key's randomart image is:
+----[RSA 3072]-----+
|oo ..|
|.o+. o|
|++o=|
|. =o+o .|
|+ *o. .So|
|o.o.oE....+|
|..= .o+oo+..|
|.* ..+....=|
|+.. .+o.o..|
+----[SHA256]-----+
root@ServerA:~#
```

Step 2:- We need to copy the Public Key from server A

```
root@ServerA:/home/ubuntu# cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCiZ9TbFag16PJE/8JySVLN1MK2yzmrdEdQ6X33MY9yMgBGQb0ZpdXhIX9UAX5NAzL3VwVxFoQ/NBK8C
53PYkzEpVxE3N7S1eq0AwV/Ik+EE1wD6k8wYtCSKMP13ThMU8yRzZ0BkMH3yfTgVRbZk3vu4e/zq6j6rJRuax00/BUXgVJDPdKijjBBJmmwPTARIFxJH0m
+q7E1R0KHYNzBGnSZPI7SIXa6kRn3LLw4o3r9P0hz9LFC1s5tkNohNjA1vuKjRy3jlnyXZU5MZ89Jc4RpmkX7qxaMIwN8AczX7+/n8iwLeZeTbgWz6t70V
Bfh8BfgGukgrXnJn6jSrVKzMJvRFeRLJ3sXrva7AQXlowWgDctBsp1mPbhJFEDBwhaRC0H76LD6GMnLZ6sa8qB1JxKFzDve8NtCtK0h0ttqoGqaDlqwgA+
o3jLtxQnMdrM4w17o0jJlq6dkL6kLwDE+TQ8xiJH28N8Qy2m4RH7+vr1AP0BG5bwc481X12gLAyKE9s= root@ServerA
root@ServerA:/home/ubuntu#
```

Step 3 :- We need to create /.ssh file in server B and need to give 700 file permission to the same file

```
ubuntu@ip-172-31-7-250:~$ mkdir -p ~/.ssh && \
chmod 700 ~/.ssh
```

Step 4:-Take Server B access and write below commands

echo "(paste_the Server A_public_key_here)" >> ~/.ssh/authorized_keys and give below permission to file :- ~/.ssh/authorized_keys

chmod 600 ~/.ssh/authorized_keys

```
ubuntu@ip-172-31-7-250:~$ mkdir -p ~/.ssh && \
chmod 700 ~/.ssh
ubuntu@ip-172-31-7-250:~$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCiZ9TbFAG16PJE/8JySVLNl1MK2yzmrdEdQ6X33MY9yMgBGQ
b0ZpdXhIX9UAX5NAzL3VwVxFoQ/NBK8C53PYkzEpVxE3N7S1eq0AwV/Ik+EE1WD6k8wYtCSKMPL3ThMU8yRzZ0BkMH3yFTgVRbZKw3vu4e/zq6j6rJRuax
00/BUXgVJDPdKijjBBJmWPTARIFxJH0m+q7E1R0KHYNZBGnSZPI7SIxa6kRn3LLw4o3r9P0hz9LFC1s5tkNohNjA1vuKjRy3jlnyXZU5MZ89Jc4RpmkX7q
xaMIwN8AczX7+/n8iwLeZeTbgWz6t70VBfh8BfgGukgrXnJn6jsrVKzMJvRFeRlJsXrva7AQXlowNWgDctBspLmPbhJFEDBwhaRC0H76LD6GMnLZ6sa8qB
1JxKFzDve8NTCTk0h0ttqoGqaDlqwgA+o3jLtxQnMdrM4w17oOjJlq6dkL6kLwDE+TQ8xiJH28N8Qy2m4RH7+vr1APOBG5bwc48LXL2gLAyKE9s= root@
ServerA" >> ~/.ssh/authorized_keys && \
chmod 600 ~/.ssh/authorized_keys
ubuntu@ip-172-31-7-250:~$
```

Step 5 :- Try to access ServerB from ServerA

```
root@ServerA:/home/ubuntu# ssh ubuntu@ip-172-31-7-250
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1015-aws x86_64)

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

System information as of Tue Jan 14 08:16:17 UTC 2025

System load:  0.0          Processes:      105
Usage of /:   21.5% of 7.57GB Users logged in:  1
Memory usage: 20%          IPv4 address for eth0: 172.31.7.250
Swap usage:   0%

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 '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 14 08:10:35 2025 from 172.31.0.42
ubuntu@ServerB:~$
```

Note :- 1) We can access Server B from Server A, but not vice versa

2) We need to copy the Public keys for connection not an Private