



Install and configure OpenSSH

SSH (Secure Shell) is a cryptographic network protocol for secure data communication, to remotely login through command-line, execute command remotely, and other secure network services between two networked computers.

SSH is not enabled by default in Ubuntu, but you could enable this service via OpenSSH, a free version of the SSH connectivity tools developed by the OpenBSD Project.

Task 1: Install openssh-server.

Step 1: Logon your workstation/server.

Step 2: Open Terminal if you are using Workstation edition.

Step 3: Write the command: **sudo apt-get update**, click Enter. Give in your root password, click Enter.

```
administrator@administrator-Virtual-Machine: ~
administrator@administrator-Virtual-Machine:~$ sudo apt-get install openssh-server
Läser paketlistor... Färdig
Bygger beroendeträd
Läser tillståndsinformation... Färdig
Följande ytterligare paket kommer att installeras:
 libck-connector0 ncurses-term openssh-sftp-server ssh-import-id
Föreslagna paket:
 rssh molly-guard monkeysphere
Följande NYA paket kommer att installeras:
 libck-connector0 ncurses-term openssh-server openssh-sftp-server
 ssh-import-id
0 att uppgradera, 5 att nyinstallera, 0 att ta bort och 74 att inte uppgradera.
Behöver hämta 618 kB arkiv.
Efter denna åtgärd kommer ytterligare 3 424 kB utrymme användas på disken.
Vill du fortsätta? [Y/n]
```

Step 4: Write in the command: **sudo apt-get install openssh-server**, click Enter.

Step 5: Write a Y, and press Enter to continue with your installation.

Task 2: To configure openssh-server to allow root to login.



Step 1: Edit `/etc/ssh/sshd_config` with your favorite editor, I will open config file with nano, my command: **sudo nano /etc/ssh/sshd_config**, then press Enter.

```
administrator@administrator-Virtual-Machine: ~
GNU nano 2.2.6      Fil: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
[ Läste 88 rader ]
^G Få hjälp  ^O Spara    ^R Läs fil  ^Y Föreg sid ^K Klipp ut  ^C Akt. pos
^X Avsluta  ^J Justera  ^W Var finns ^V Nästa sid ^U Angra kopi ^T Stavkontr.
```

Step 2: Locate `PermitRootLogin withoutpassword`, to **PermitRootLogin yes**.

Step 3: Write the file to filesystem, and then close the editor.

```
administrator@administrator-Virtual-Machine: ~
administrator@administrator-Virtual-Machine:~$ sudo service ssh restart
ssh stop/waiting
ssh start/running, process 3982
administrator@administrator-Virtual-Machine:~$
```

Task 3: Restart the openssh service.

Step 1: Write the command: **sudo service ssh restart**, click Enter.