

How to Enable SSH on Ubuntu 18.04

Updated Aug 2, 2019 • 5 min read

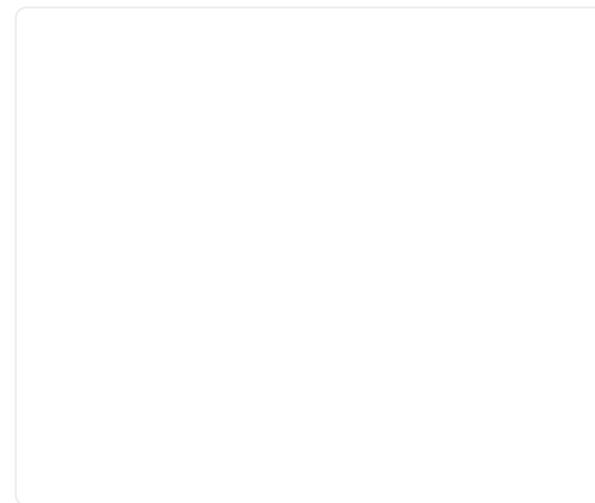


Secure Shell (SSH) is a cryptographic network protocol used for a secure connection between a client and a server.

In this tutorial, we'll show you how to enable SSH on an Ubuntu Desktop machine. Enabling SSH will allow you to remotely connect to your Ubuntu machine and securely transfer files or perform administrative tasks.

Prerequisites

Before continuing with this tutorial, make sure you are logged in as a [user with sudo privileges](#).



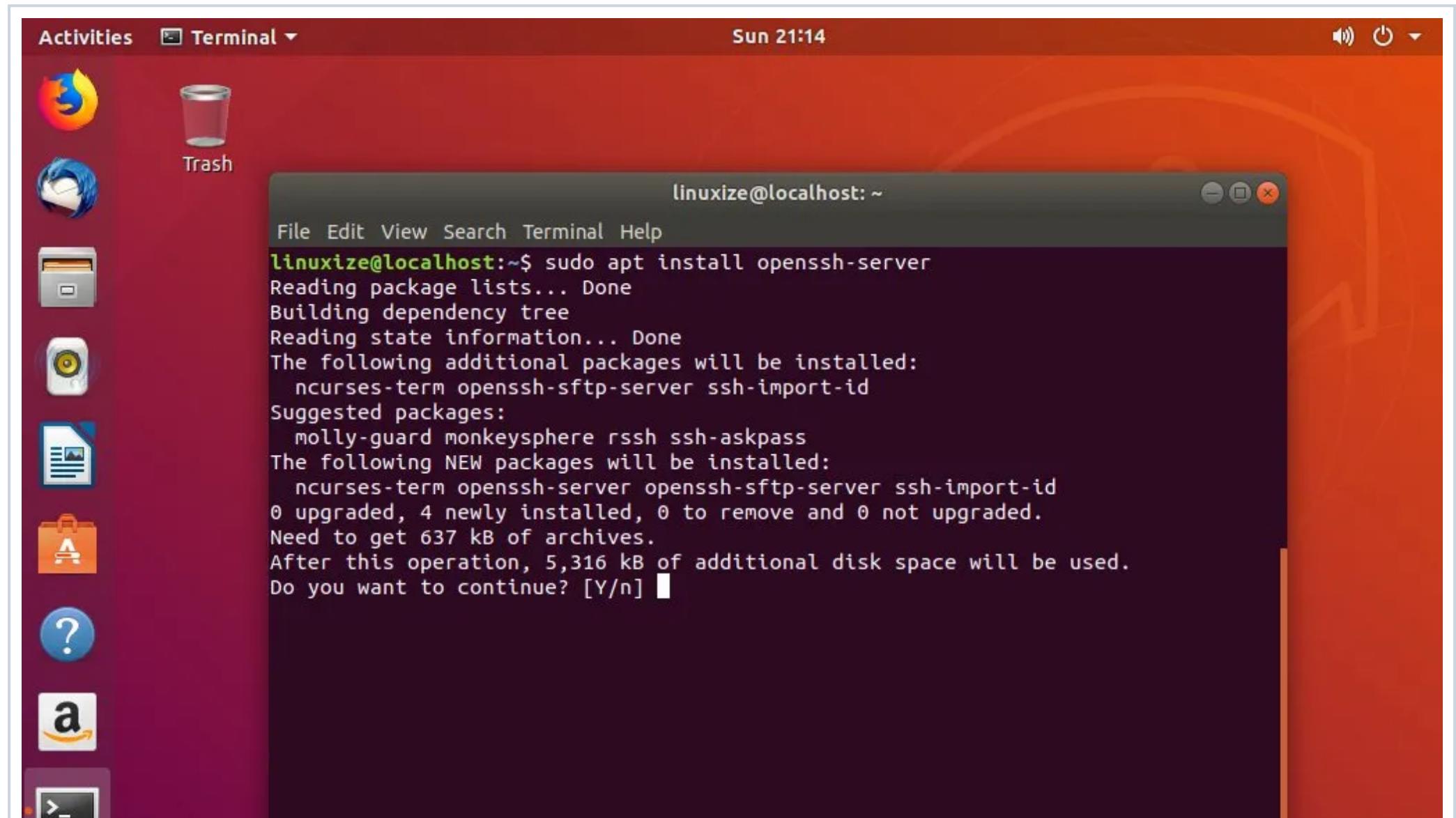
Enabling SSH on Ubuntu

The SSH server is not installed by default on Ubuntu desktop systems but it can be easily installed from the standard Ubuntu repositories.

To install and enable SSH on your Ubuntu system complete the following steps:

```
$ sudo apt update  
$ sudo apt install openssh-server
```

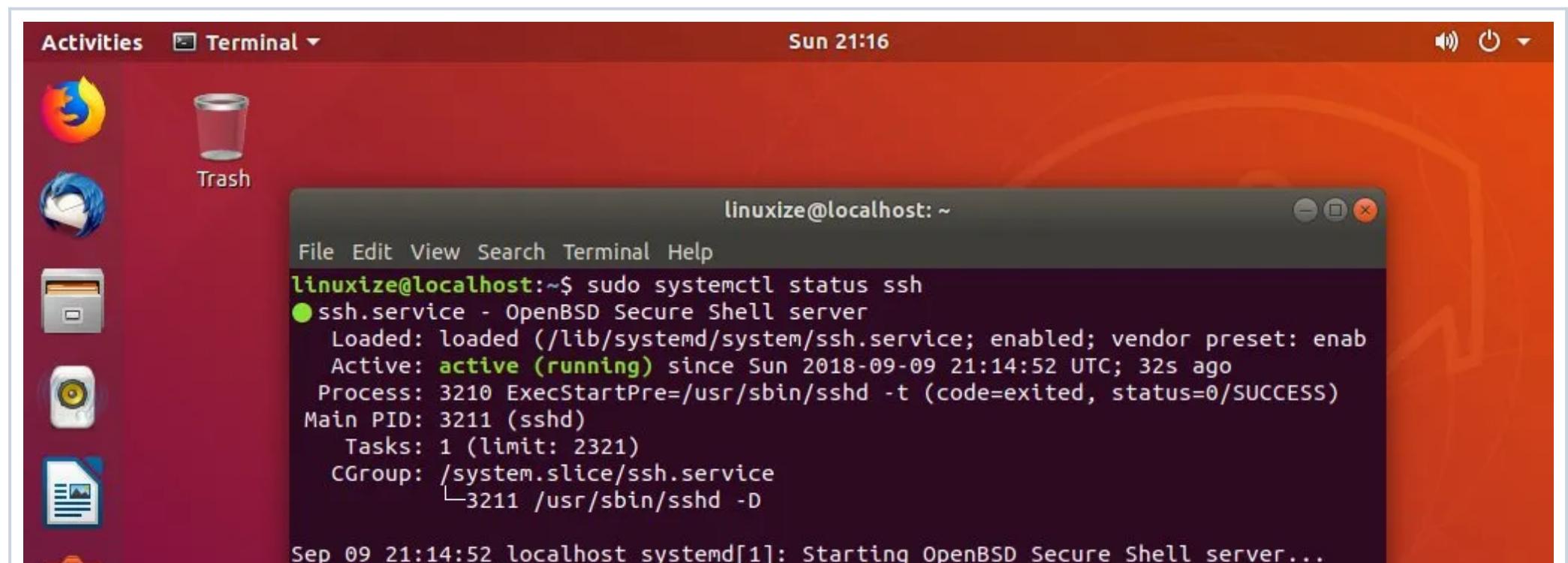
Enter the password when prompted and enter Y to continue with the installation.



02 . Once the installation is completed, the SSH service will start automatically. To verify that the installation was successful and SSH service is running type the following command which will print the SSH server status:

```
$ sudo systemctl status ssh
```

You should see something like Active: active (running) :

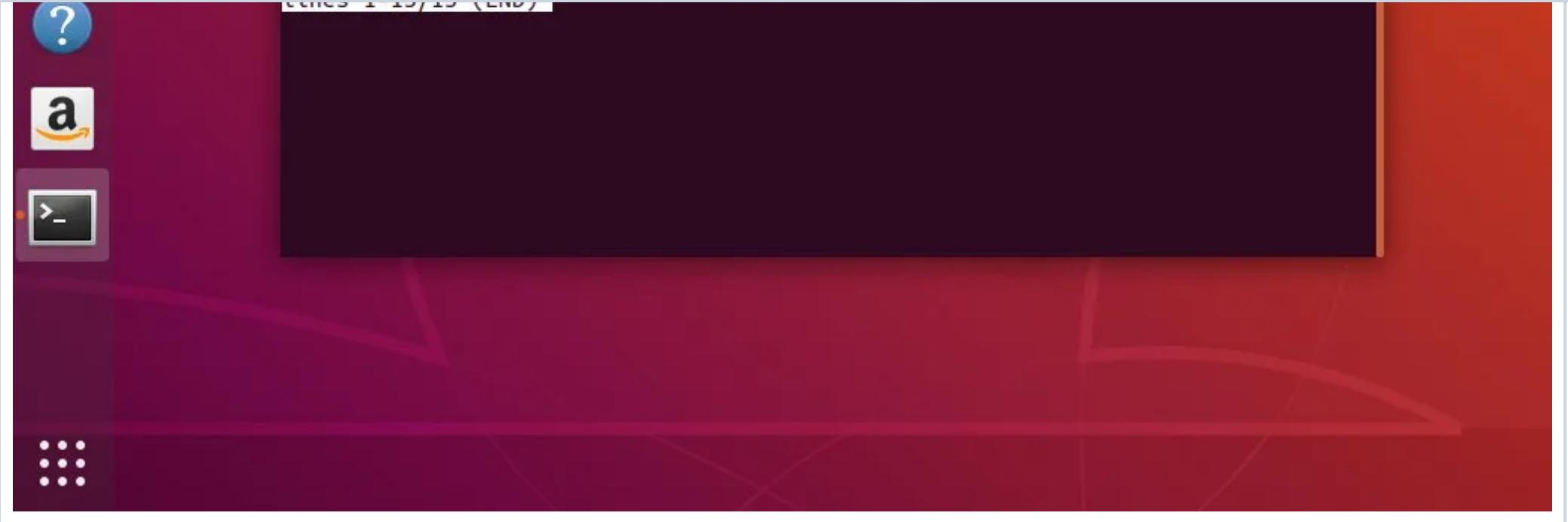


The image shows a screenshot of an Ubuntu desktop environment. On the left, there's a dock with icons for the Dash, Home, Applications, and Dash to Dock. The main desktop has a red-orange gradient background. A terminal window is open in the center, titled "linuxize@localhost: ~". The window contains the following text:

```
File Edit View Search Terminal Help
linuxize@localhost:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2018-09-09 21:14:52 UTC; 32s ago
    Process: 3210 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3211 (sshd)
     Tasks: 1 (limit: 2321)
    CGroup: /system.slice/ssh.service
            └─3211 /usr/sbin/sshd -D

Sep 09 21:14:52 localhost systemd[1]: Starting OpenBSD Secure Shell server...
```

At the bottom of the terminal window, there's a status message: "Sep 09 21:14:52 localhost systemd[1]: Starting OpenBSD Secure Shell server...". The top bar shows the date and time as "Sun 21:16".



Press `q` to get back to the command line prompt.

03. Ubuntu comes with a firewall configuration tool called UFW. If the firewall is enabled on your system, make sure to open the SSH port:

```
$ sudo ufw allow ssh
```

Now that SSH is installed and running on your Ubuntu system you can connect to it via SSH from any remote machine. Linux and macOS systems have SSH clients installed by default. If you want to connect from a Windows machine then you can use an SSH client such as [PUTTY](#).

Connecting to SSH Over LAN

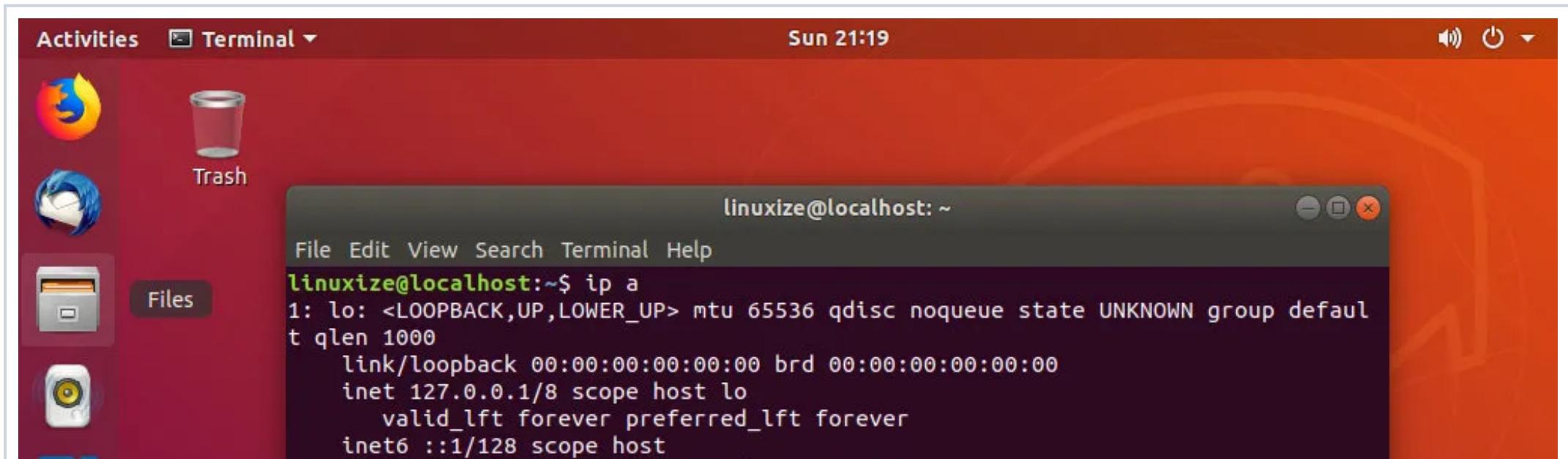


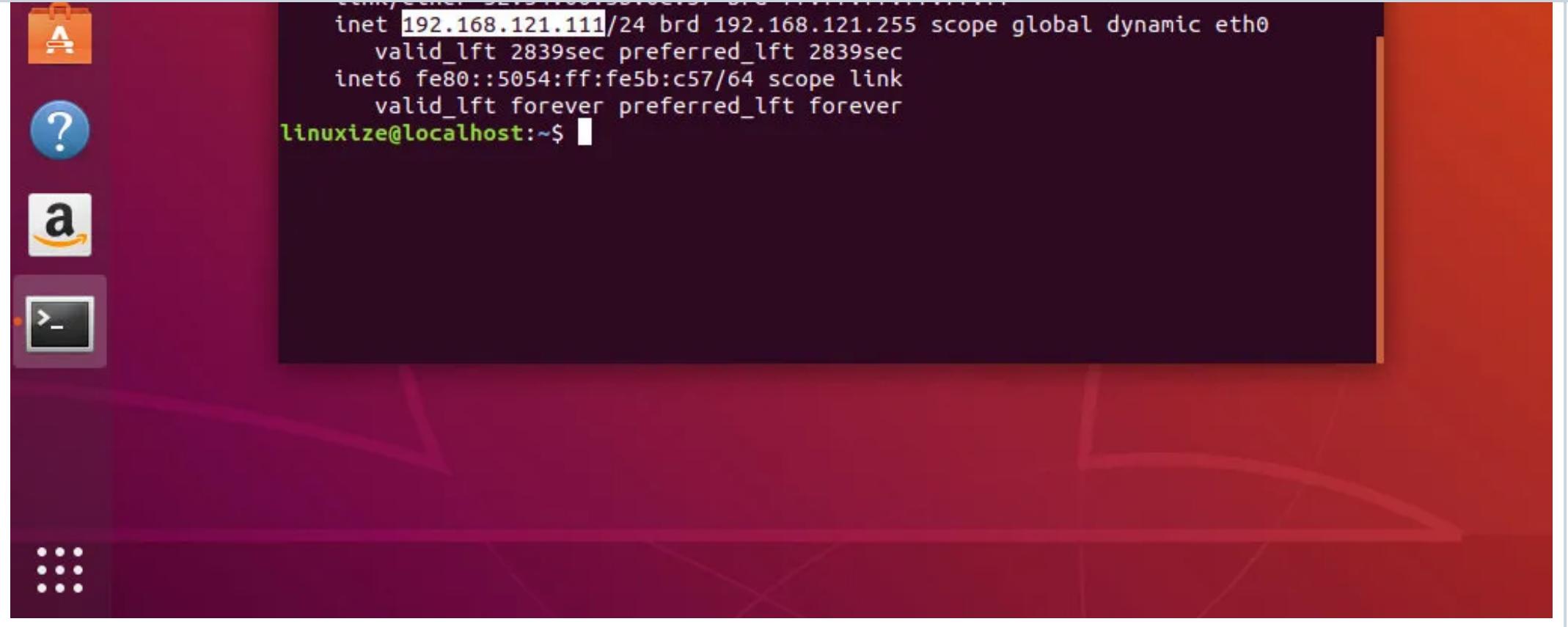
```
$ ssh username@ip_address
```

Change the `username` with the actual user name and `ip_address` with the IP Address of the Ubuntu machine where you installed SSH.

If you don't know your IP address you can easily find it using the [ip command](#):

```
$ ip a
```





As you can see from the output, the system IP address is 192.168.121.111.

Once you've found the IP address, login to remote machine by running the following [ssh](#) command:

```
$ ssh linuxize@192.168.121.111
```

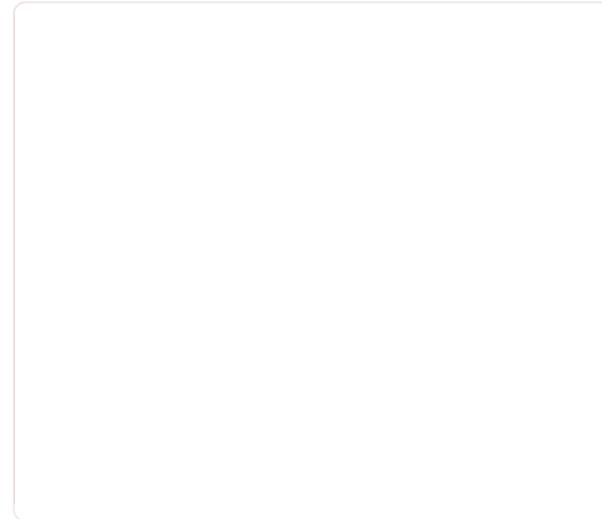
When you connect through SSH for the first time, you will see a message looking something like this:

Output

The authenticity of host '192.168.121.111 (192.168.121.111)' can't be established.



Type yes and you'll be prompted to enter your password.



Output

```
Warning: Permanently added '192.168.121.111' (ECDSA) to the list of known hosts.  
linuxize@192.168.121.111's password:
```

Once you enter the password you will be greeted with a message similar to the one below.

Output

```
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-33-generic x86_64)
```

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

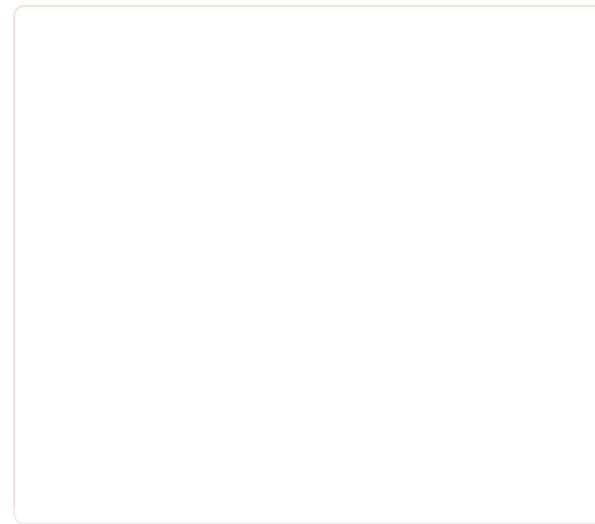
...



Connecting to SSH Over Internet

To connect to your Ubuntu machine over the Internet you will need to know your public IP Address and to configure your router to accept data on port 22 and send it to the Ubuntu machine where the SSH is running.

To determine the public IP address of the machine you're trying to SSH to, simply visit the following URL: <https://api.ipify.org>.



When it comes to setting up [port forwarding](#) each router has a different way to setup port forwarding. You should consult your router documentation about how to set up port forwarding. In short, you need to enter the port number where requests will be made (Default SSH port is 22) and the private IP address you found earlier (using the `ip` a command) of the machine where the SSH is running.

Once you've found the IP address, and configured your router you can log in by typing:

```
$ ssh username@public_ip_address
```



You can also [set up an SSH key-based authentication](#) and connect to your Ubuntu machine without entering a password.

Disabling SSH on Ubuntu

If for some reason you want to disable SSH on your Ubuntu machine you can simply stop the SSH service by running:

```
$ sudo systemctl stop ssh
```

To start it again run:

```
$ sudo systemctl start ssh
```

To disable the SSH service to start during system boot run:

```
$ sudo systemctl disable ssh
```

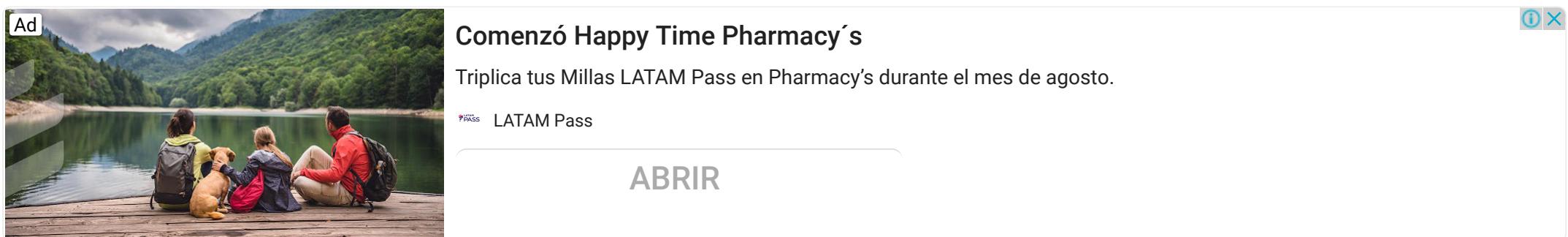


```
$ sudo systemctl enable ssh
```

Conclusion

You have learned how to install and enable SSH on your Ubuntu 18.04. You can now login to your machine and perform common sysadmin tasks through the command prompt.

By default, SSH listens on port 22. [Changing the default SSH port](#) adds an extra layer of security to your server by reducing the risk of automated attacks.



If you are managing multiple systems, you can simplify your workflow by defining all of your connections in the [SSH config file](#).

For more information, about how to configure your SSH server read the Ubuntu's [SSH/OpenSSH/Configuring](#) guide and the [official SSH manual](#) page.

If you have any questions, please leave a comment below.

ssh ubuntu



[Linuxize](#) [Ubuntu](#) [Centos](#) [Debian](#) [Commands](#) [Series](#) [Donate](#)



If you like our content, please consider buying us a coffee.

Thank you for your support!



BUY ME A COFFEE

Sign up to our newsletter and get our latest tutorials and news straight to your mailbox.

Your email...

Subscribe

We'll never share your email address or spam you.

Related Articles

SEP 22, 2018

How to Set Up SSH Keys on Ubuntu 18.04

JUL 27, 2020

How to Set Up SSH Keys on Ubuntu 20.04

JUN 1, 2020

How to Enable SSH on Ubuntu 20.04



Linuxize

Ubuntu

Centos

Debian

Commands

Series

Donate



Show comments (9)

© 2020 Linuxize.com

[Privacy Policy](#) [Terms](#) [Contact](#)

