



***Step by step guidance to  
create a Linux EC2 instance  
and connect to it from a Mac  
operating system***

**-BY**

**SOWBARNICKA G K**

To create a Linux EC2 instance and connect to it from a Mac operating system, follow this simple steps:

**Step 1: Enter the instance name:**

In the "Name and tags" section, type the desired name for your instance, like "KPR-LINUX". This helps you identify your instance easily later on.

[EC2](#) > ... > [Launch an instance](#)

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags** [Info](#)

Name

[Add additional tags](#)

**▼ Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

**Step2:**Select an **Amazon Machine Image (AMI)** :

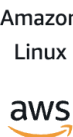
- Choose the operating system and configuration you want for your instance.

For example, you can select "**Ubuntu Server 24.04 LTS**" from the list of available AMIs


- Choose architecture as "**64-bit (x86)**".

Below


**Quick Start**




Amazon Linux




macOS




Ubuntu




Windows



Red Hat



SUSE Linux



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

**Amazon Machine Image (AMI)**

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

Free tier eligible ▼

ami-0dee22c13ea7a9a67 (64-bit (x86)) / ami-0c8eea98010057bd0 (64-bit (Arm))

Virtualization: hvm   ENA enabled: true   Root device type: ebs

**Description**

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture


64-bit (x86) ▼

AMI ID

ami-0dee22c13ea7a9a67

Username

ubuntu



Verified provider

### Step 3: Select the instance type:

- Choose "t2.micro" from the list of instance types.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Linux base pricing: 0.0124 USD per Hour  
On-Demand Windows base pricing: 0.017 USD per Hour  
On-Demand RHEL base pricing: 0.0268 USD per Hour  
On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

☒ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

This type is "**Free tier eligible**" and provides 1 vCPU and 1 GiB of memory, making it a cost-effective option for small workloads.

### Step 4: Create a key pair:

- Enter a name for your key pair.
- Select the key pair type (RSA or ED25519).
- Choose the private key file format (.pem for OpenSSH or .ppk for PuTTY).

This key pair will be used to securely connect to your instance.

## Create key pair



### Key pair name

Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

### Key pair type

☒ RSA

RSA encrypted private and public key pair

☐ ED25519

ED25519 encrypted private and public key pair

### Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY



When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Cancel

Create key pair

Better to choose `".pem"` as private key file format for use with OpenSSH

### Step 5: Configure the key pair and network settings:

- Select an existing key pair or create a new one for secure access.
- Then, choose the VPC and subnet for your instance and enable the option to auto-assign a public IP.

#### ▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

kplinux ▼

↻ [Create new key pair](#)

#### ▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0be03f8df40a75130  
172.31.0.0/16

(default) ▼



Subnet [Info](#)

subnet-0e2752dd7596745b2

VPC: vpc-0be03f8df40a75130   Owner: 038462791702  
Availability Zone: ap-south-1a   Zone type: Availability Zone  
IP addresses available: 4091   CIDR: 172.31.32.0/20



↻ [Create new subnet](#) [↗](#)

Auto-assign public IP [Info](#)

Enable ▼

[Additional charges apply](#) when outside of [free tier allowance](#)

## Step6:To create a security group:

- Name the security group.
- Add a description, and define inbound and outbound rules to control traffic to your instance.

### Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

#### Security group name - *required*

kprlinux-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . \_ - / ( ) # , @ [ ] + = & ; ! \$ \*

#### Description - *required* [Info](#)

kprlinux-sg

### Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

#### Type [Info](#)

ssh ▼

#### Protocol [Info](#)

TCP

#### Port range [Info](#)

22

#### Source type [Info](#)

Anywhere ▼

#### Source [Info](#)

🔍 Add CIDR, prefix list or security

0.0.0.0/0 ✕

#### Description - *optional* [Info](#)

e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Add security group rule

**Step 7:** To configure storage, set the size (**e.g., 8 GiB**), choose the type (**e.g., gp3**), and add any additional volumes if needed.

▼ **Configure storage** [Info](#)

Advanced

1x  GiB  ▼ Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

×

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

🕒 Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

↻

0 x File systems [Edit](#)

**Step 8:** To connect to your AWS EC2 instance:

- Use an SSH client with the provided private key file and the instance's public DNS.



[EC2](#) > [Instances](#) > [i-0e8d94803fb9080d9](#) > [Connect to instance](#)

## Connect to instance [Info](#)

Connect to your instance i-0e8d94803fb9080d9 (KPR-LINUX) using any of these options

EC2 Instance Connect



Session Manager

**SSH client**


EC2 serial console


Instance ID

 **i-0e8d94803fb9080d9** (KPR-LINUX)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is `kprlinux.pem`
3. Run this command, if necessary, to ensure your key is not publicly viewable.  
 `chmod 400 "kprlinux.pem"`
4. Connect to your instance using its Public DNS:  
 `ec2-13-232-94-122.ap-south-1.compute.amazonaws.com`

Example:

 `ssh -i "kprlinux.pem" ubuntu@ec2-13-232-94-122.ap-south-1.compute.amazonaws.com`

 **Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

**Step 9:** Change the permissions of your private key file to 400 using `chmod 400 kprlinux.pem` before connecting via SSH.

```
-rw-r--r--@ 1 mahendranelvakumar staff 165 7 Oct 09:36 ~$AWS Presentation by Mahe.pptx
mahendranelvakumar@Mahendranelvakumar-MBP Downloads % ssh -i "kprlinux.pem" ubuntu@ec2-13-232-94-122.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-232-94-122.ap-south-1.compute.amazonaws.com (13.232.94.122)' can't be established.
ED25519 key fingerprint is SHA256:6Gg/aLoR7WKZGKsZaNRnpDztRn2LZV6Tua+yDAiXso.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-232-94-122.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'kprlinux.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "kprlinux.pem": bad permissions
ubuntu@ec2-13-232-94-122.ap-south-1.compute.amazonaws.com: Permission denied (publickey).
```

**Step 10:** Use `chmod 400 kprlinux.pem` to secure your private key file before connecting via SSH.

```
mahendranelvakumar@Mahendrants-MBP Downloads % chmod 400 "kprlinux.pem"
mahendranelvakumar@Mahendrants-MBP Downloads % ls -la
```

**Step 11:** To check system info, disk usage, and directory contents on Linux, use:

- **uname -a** for system info
- **df -h** for disk usage
- **ls -l** for directory contents

```
mahendranelvakumar@Mahendrants-MBP Downloads % ssh -i "kprlinux.pem" ubuntu@ec2-13-232-94-122.ap-south-1.compute.amazonaws.com
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Mon Oct  7 10:28:30 UTC 2024

System load:  0.0               Processes:    104
Usage of /:   22.8% of 6.71GB   Users logged in:  0
Memory usage: 19%              IPv4 address for enX0: 172.31.42.222
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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-42-222:~$ ls
ubuntu@ip-172-31-42-222:~$ ls -la
total 28
drwxr-x--- 4 ubuntu ubuntu 4096 Oct  7 10:28 .
drwxr-xr-x 3 root   root   4096 Oct  7 10:16 ..
-rw-r--r-- 1 ubuntu ubuntu  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Mar 31  2024 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Oct  7 10:28 .cache
-rw-r--r-- 1 ubuntu ubuntu  807 Mar 31  2024 .profile
drwx----- 2 ubuntu ubuntu 4096 Oct  7 10:16 .ssh
ubuntu@ip-172-31-42-222:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-42-222:~$
```