



Launching EC2 Instance in VPC

1. Now navigate to EC2 and click on launch instance.
2. Then give your instance a name.

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

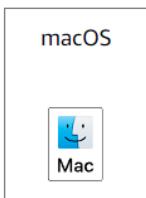
Name

[Add additional tags](#)

3. Then select your OS as ubuntu.

▼ 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

[Recents](#)[Quick Start](#)[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-03f4878755434977f (64-bit (x86)) / ami-077885f59ecb77b84 (64-bit (Arm))

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

Free tier eligible

4. Select the instance type as t2.micro because it is free tier eligible.

▼ 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: 0.0724 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](#)

5. Then select your key pair.

▼ 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*

linuxweb-key

[!\[\]\(e3275251d0893157c3584e20c81dc3ba_img.jpg\) Create new key pair](#)

6. Now for the network settings choose the VPC that you created.

7. Then choose the web subnet for it. And enable auto assign public IP.

▼ Network settings [Info](#)

VPC - *required* | [Info](#)

vpc-0592817f98a3df74e (app-vpc)
10.0.0.0/16



Subnet | [Info](#)

subnet-0eb211eabd0433b62 web-subnet
VPC: vpc-0592817f98a3df74e Owner: 878893308172
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.0.0/24



[!\[\]\(a8ff699ced33317c53c86f9bf3171905_img.jpg\) Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable



8. For the security groups create a new group. Name your security group if you want to.

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*

web-security-group

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](#)

web-security-group

9. The for the inbound security group rules, add HTTP with port 80 and allow traffic from everywhere by selecting CIDR block as 0.0.0.0/0

Inbound Security Group Rules

<p>▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)</p>	<p>Remove</p>
<p>Type Info</p>	<p>Protocol Info</p>
<p>ssh</p>	<p>TCP</p>
<p>Source type Info</p>	<p>Port range Info</p>
<p>Anywhere</p>	<p>22</p>
<p>Source Info</p>	<p>Description - <i>optional</i> Info</p>
<p><input type="text"/> Add CIDR, prefix list or security</p>	<p>e.g. SSH for admin desktop</p>
<p><input type="text"/> 0.0.0.0/0 </p>	
<p>▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)</p>	<p>Remove</p>
<p>Type Info</p>	<p>Protocol Info</p>
<p>HTTP</p>	<p>TCP</p>
<p>Source type Info</p>	<p>Port range Info</p>
<p>Custom</p>	<p>80</p>
<p>Source Info</p>	<p>Description - <i>optional</i> Info</p>
<p><input type="text"/> Add CIDR, prefix list or security</p>	<p>e.g. SSH for admin desktop</p>
<p><input type="text"/> 0.0.0.0/0 </p>	

10. After that launch your instance.

11. Once you instance is launched, now click on connect

Instances (1/1) Info		 Connect	Instance state	Actions	Launch instances
<input type="text"/> Find Instance by attribute or tag (case-sensitive)					
<input checked="" type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check
<input checked="" type="checkbox"/>	web-instance	i-0efdc51e642cd75aa	 Running	 t2.micro	 2/2 checks passed View alarms

12. Connect by using EC2 instance connect. You can also use Putty app to connect your instance.

It totally depends on your choice which medium you want to connect with your instance.

13. Now click on connect.

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID
 i-0efdc51e642cd75aa (web-instance)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
 35.154.38.225

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.

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

14. A new page will open in the new tab it will say that your instance has established the connection successfully.

```
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

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

System information as of Tue Jan 16 19:11:52 UTC 2024

System load:  0.0          Processes:            96
Usage of /:   20.6% of 7.57GB  Users logged in:    0
Memory usage: 21%           IPv4 address for eth0: 10.0.0.33
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-10-0-0-33:~$
```

15. Now you need to run two commands one is for updating your instance and the other is for installing nginx webserver on your instance.
sudo apt-get update
sudo apt-get install nginx
16. Once both the commands have run successfully now you need to copy the public IP address of your instance and paste it in a new tab.
17. You will see that nginx webserver is up and running successfully.

