Launching an EC2 instance

We are going to launch an EC2 instance. An EC2 instance is just a virtual computer in AWS's data center. While launching the instance I am going to discuss each step in detail.

To follow along, login to your AWS account and select EC2 from the services section.

Let's Get Started

The price of instances varies in different regions and some instances are only available in certain regions.

In this case, I will be using the **Asia Pacific (Mumbai)** region, you may also choose this one or select US East (N. Virginia) region. You can change your region at the top right corner of the page.

Now click on **Launch Instance** button.

A. The first step is to choose the Amazon Machine Image (AMI) that will be used to launch our instance. It is like a configurable ISO file of your Operating System.

You have the option of selecting AMIs provided by AWS, AWS community AMIs, AWS marketplace or your own AMIs.

Here I am going to select the first one i.e. Amazon Linux AMI.

B. The second step is to choose an Instance Type. AWS provides a large number of instances to choose from depending on your use case. You can scroll down and see instances optimized for compute, graphics,

memory and storage.

Each instance has a fixed number of virtual CPUs and RAM. The larger the size, more is the computing power and memory size.

I am going to select the **t2.micro** here since its available in the free tier.

Note -If you select any instance other than t2.micro you will charged.

After selecting the instance of your choice click on the **Next: Configure Instance Details** button.

C. Now it's time to configure our instance details. You can hover over the info button after each option to learn more about that option.

1. **Number of Instances** —The total number of instances you want to launch.
2. **Purchasing Option** —You can check this checkbox to launch spot instances.
3. **Network** —You can select the VPC in which to launch this instance.
4. **Subnet** —You can specify the preferred subnet (availability zone) in which to launch this instance.
5. **Auto-assign Public IP** —When this option is enabled your EC2 instance gets a public IP. You can then host a website on this server and access it via instance's public IP.
6. **Placement Group** —**You can add this instance to a placement group by selecting this option.
7. **Capacity Reservation** —**Using this option you can reserve capacity of your instance in an availability zone. Leave this option as default.
8. **IAM role** —You can assign an IAM role to this instance to allow it to access other AWS services without storing access keys on the instance.

9. **Shutdown behavior**—You can stop or terminate an instance when an OS-level shutdown is performed.
10. **Enable Termination Protection**—Selecting this option will prevent you from accidentally terminating your instances. You will have to disable this option to terminate an instance.
11. **Monitoring**—Checking this option will enable Cloudwatch detailed monitoring. Detailed monitoring logs your instance's performance metrics every 1 minute as opposed to 5 minutes for basic monitoring. Additional charges will be applied if you select this option.
12. **Tenancy**—By default your instances are hosted on a shared host. You can select dedicated instance or dedicated host to comply with your license but you will have to pay additional charges. Leave this option as shared.
13. **T2 Unlimited**—Allows your instance to burst CPU utilization in case of high traffic. Additional charges may apply when you select this option.

Under the Advanced Details section at the bottom of the page you have a **User data** text field. You can use it to run configuration scripts or commands to configure your instance.

These scripts or commands will run as soon as your instance starts the first time.

Now click **Next: Add Storage** button.

D. It's time to add some storage to our instance. The first volume that will be attached to your instance will be a **Root volume.** You can set its size (default is 8 GB) and it's volume type.

You can select whether to delete this volume when an instance is terminated. By default root volumes are deleted on termination and cannot be encrypted.

You can add additional volumes using the **Add New Volume** button. Additional volumes can be encrypted and are not deleted on termination

by default.

For the root volume you have three options for Volume type -

1. General Purpose SSD (gp2)
2. Provisioned IOPS SSD (io1)
3. Magnetic (standard)

For other volumes you have two additional options along with the above three-

1. Throughput Optimized HDD (st1)
2. Cold HDD (sc1)

Usually SSD type volumes are faster and expensive than HDD type volumes.

I am not going to make any changes here so click **Next: Add Tags** button.

1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances ⓘ	Volumes ⓘ	
Name	My First Instance	☑	☑	✕

Add another tag   (Up to 50 tags maximum)

Cancel   Previous   **Review and Launch**   Next: Configure Security Group

E. Here we can add tags to our instance. A tag are just key-value pair.

Tags can be used to group instances by departments and teams. They can be used to search for resources across an AWS account.

They can also help in managing costs of resources.

Here I am adding a single tag with Key of "Name" and Value as "My First Instance".

Now click on **Next: Configure Security Group.**

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ⦿ Create a **new** security group

◯ Select an **existing** security group

Security group name: My SG

Description: My SG

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ		Description ⓘ	
SSH ⬍	TCP	22	Custom ⬍	0.0.0.0/0	e.g. SSH for Admin Desktop	✕
HTTP ⬍	TCP	80	Custom ⬍	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop	✕
HTTPS ⬍	TCP	443	Custom ⬍	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop	✕

Add Rule

⚠ **Warning**

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.

Cancel   Previous   **Review and Launch**

F. Now we are going to configure our security group. A security group acts as a firewall for our instances. We can use it to open different ports for different applications.

Here I am opening the SSH port since we will be logging in to our instance once it is running.

HTTP and HTTPS ports are opened since we are going to install an apache server on our instance once it's running.

In the source tab you can see that we have entered **0.0.0.0/0** to allow our instance to accept traffic from anywhere on the internet. This is the reason why we are seeing the warning on the screen.

For our personal case this won't be an issue but for a company you will want the source for SSH to be your company's static IPs.

Now click on **Review and Launch.**

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ **Improve your instances' security. Your security group, My SG, is open to the world.**
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

▼ AMI Details   Edit AMI

📦 **Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0912f71e06545ad88**

[Free tier eligible] The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs   Virtualization type: hvm

▼ Instance Type   Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▼ Security Groups   Edit security groups

Security group name My SG
Description My SG

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	
HTTP	TCP	80	0.0.0.0/0	

Cancel Previous Launch

G. You can review the instance details now. Next click on
Launchbutton.

Select an existing key pair or create a new key pair   ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair ⌄
Key pair name
ec2keypair

Download Key Pair

💬 You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel **Launch Instances**

H. Now you will see a pop up for selecting a key pair.

Select **Create a new key pair** option and enter a key pair name and
click on **Download Key Pair.**

After downloading the key pair file click on **Launch Instances**
button.

Launch Status

✅ **Your instances are now launching**
The following instance launches have been initiated: i-086900233100edb86   View launch log

ℹ️ **Get notified of estimated charges**
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

▼ Here are some helpful resources to get you started
- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)

Create and attach additional EBS volumes (Additional charges may apply)

Manage security groups

View Instances

We can see that our instance is now launching, click on **View Instances** and wait a few minutes until the instance is running.

Congratulations, You have just launched your first EC2 instance!

You can now see that our instance has a public DNS and a Public IP address. We will use this IP address to SSH into our instance.

SSH into EC2 instance

If you are using Linux or MacOS open your **terminal**, if you are using Windows, download **git bash** to continue.

1. In terminal or git bash, navigate to the folder where you have saved

the key pair file and type the following command to change the file permissions.

For Linux and Mac users— `sudo chmod 600 ec2keypair.pem`
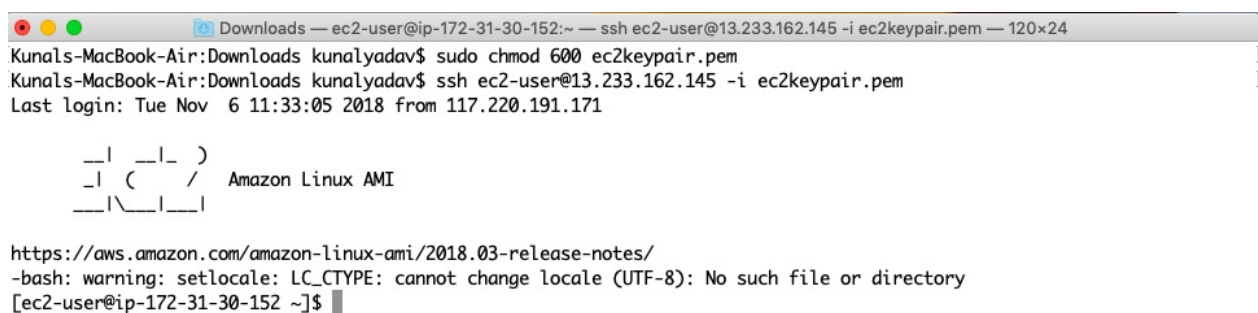
For Windows users— `chmod 600 ec2keypair.pem`

In place of ec2keypair.pem enter the name of your key pair file.

2. Now, to log in to your ec2 instance type the following command.

`ssh ec2-user@public-ip-address -i ec2keypair.pem`

If you are prompted to type yes or no, type yes.

The above commands looks like the following on my terminal.

```
●●● 		🔵 Downloads — ec2-user@ip-172-31-30-152:~ — ssh ec2-user@13.233.162.145 -i ec2keypair.pem — 120×24
Kunals-MacBook-Air:Downloads kunalyadav$ sudo chmod 600 ec2keypair.pem
Kunals-MacBook-Air:Downloads kunalyadav$ ssh ec2-user@13.233.162.145 -i ec2keypair.pem
Last login: Tue Nov  6 11:33:05 2018 from 117.220.191.171

      __|  __|_  )
      _|  (     /   Amazon Linux AMI
     ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory
[ec2-user@ip-172-31-30-152 ~]$ ▌
```

Now type the following commands in the terminal to start an apache server.

```
sudo yum update -y
sudo yum install -y httpd
sudo service httpd start
sudo chkconfig httpd on
```

Once the following commands are completed. Enter your IP in a web browser and press enter.

You will see a page similar to this.

Amazon Linux AMI **Test Page**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Amazon Linux AMI , please visit the Amazon AWS website.

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:

Congratulations, you have just installed an apache server on your EC2 instance.

Now you can terminate the instance from the EC2 dashboard using the Actions tab in the navigation.