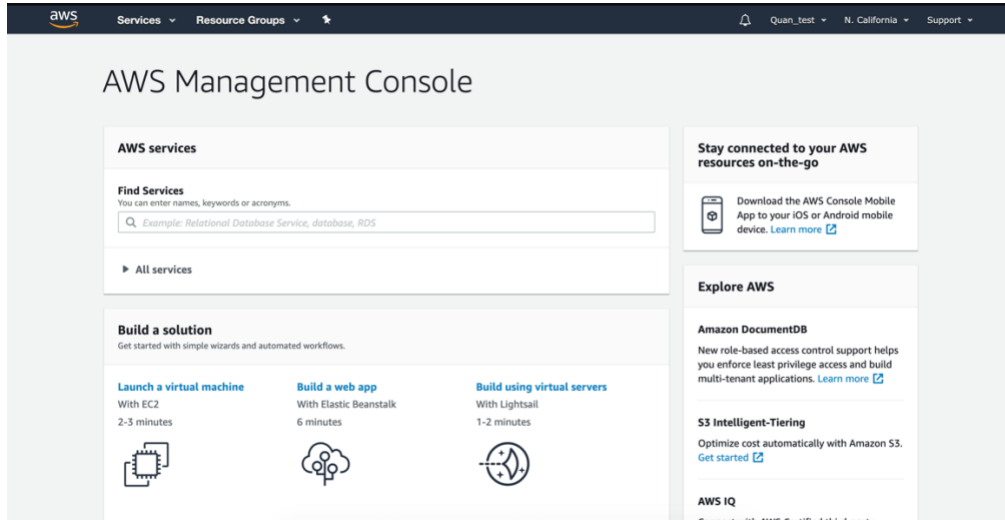
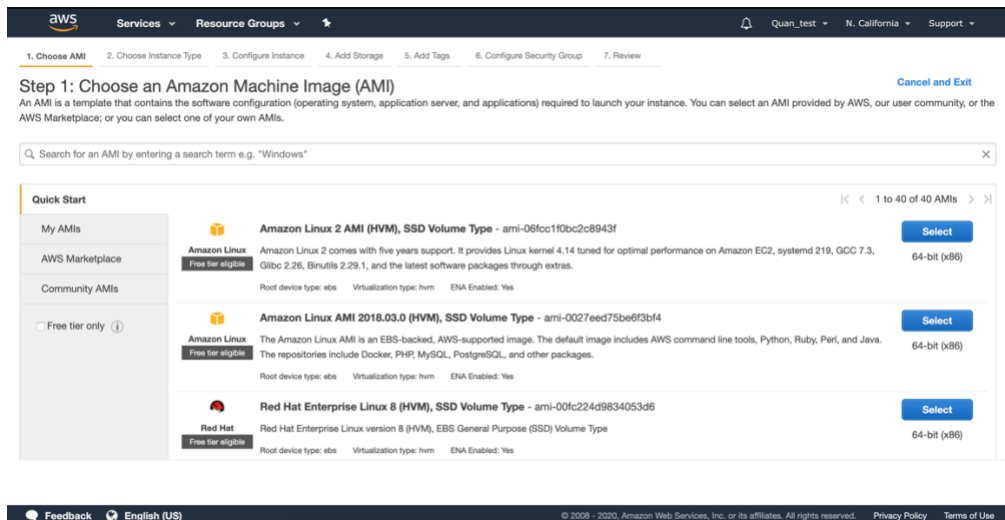


This document is about how-to setup and start an Instance on Amazon Web Service (AWS)

1. Go to [AWS website](https://aws.amazon.com/) and create a root account
2. Log in to AWS and you should see something like this:



3. Click **Launch a virtual machine**, and it will take you to this page,



- I am going to use Amazon Linux 2 AMI for development environment, so click the select button, and go to next page:

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance types** **Current generation** [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

- Click on **Next: Configure Instance Details**, and go to the next page

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-a6bb53c0 (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open [Create new Capacity Reservation](#)

IAM role: None [Create new IAM role](#)

Shutdown behavior: Stop

Stop - Hibernate behavior: ☐ Enable hibernation as an additional stop behavior

Enable termination protection: ☐ Protect against accidental termination

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

6. Click **Create new IAM role**, and it will take you to another page, and click **Create Role**,

The screenshot shows the 'Create role' page in the AWS IAM console. The page has a dark header with the AWS logo and navigation links. The main content area is titled 'Create role' and has a progress indicator with four steps: 1 (selected), 2, 3, and 4. The first step is 'Select type of trusted entity'. Below this, there are four options: 'AWS service' (selected), 'Another AWS account', 'Web identity', and 'SAML 2.0 federation'. The 'AWS service' option is highlighted with a blue border. Below the options, there is a section 'Choose a use case' with 'Common use cases' and 'Or select a service to view its use cases'. Under 'Common use cases', 'EC2' is selected, with the description 'Allows EC2 instances to call AWS services on your behalf.' Below this, there is a grid of services: API Gateway, CodeDeploy, EMR, KMS, RoboMaker, AWS Backup, CodeGuru, ElasticCache, Kinesis, S3, AWS Chatbot, CodeStar Notifications, Elastic Beanstalk, Lambda, SMS, AWS Support, Comprehend, Elastic Container Service, Lex, and SNS. At the bottom, there are buttons for 'Cancel' and 'Next: Permissions'.

7. Choose **AWS service** and **EC2** on this page and click **Next: Permissions**,
8. Click **Next: Tags**
9. Click **Next: Review**
10. On next page, choose a name for the role name, I choose MyRole

The screenshot shows the 'Create role' page in the AWS IAM console, step 4: Review. The page has a dark header with the AWS logo and navigation links. The main content area is titled 'Create role' and has a progress indicator with four steps: 1, 2, 3, and 4 (selected). The fourth step is 'Review'. Below this, there is a section 'Provide the required information below and review this role before you create it.' The 'Role name' field is filled with 'MyRole'. The 'Role description' field is filled with 'Allows EC2 instances to call AWS services on your behalf.' The 'Trusted entities' field is filled with 'AWS service: ec2.amazonaws.com'. The 'Policies' field is filled with 'Policies not attached'. The 'Permissions boundary' field is filled with 'Permissions boundary is not set'. At the bottom, there are buttons for 'Cancel', 'Previous', and 'Create role'.

11. Click **Create role**

12. Go back to the previous page of creating the instance, and click the **refresh button** next to the dropdown of **IAM role** and choose the role name you just created (In my case, I choose MyRole)

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation [Create new Capacity Reservation](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

13. Click **Next: Add Storage**

14. Click **Next: Add Tags**

15. Click **Add Tags** and type value for key and value, in my case, I choose key=Name and Value=Value, click **Next Configure Security Group**

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 (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	Value	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

16. Click **Add Rule**, and add rules as show in the screenshot, and click **Review and Launch**

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:

Description:

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
Custom TCP	TCP	8443	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](#)

17. click **Launch** and you should see this,

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 instances may be accessible from any IP address. You can also open additional ports in your security groups.

AMI Details
Amazon Linux 2 AMI (HVM), SSD Volume Type
Free tier eligible
Root Device Type: ebs Virtualization type: hvm

Instance Type
Instance Type: t2.micro ECU: Variable vCPU: 1

Security Groups

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:


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](#)


18. choose **Create a New Key Pair** in the dropdown list and give it a name and click **Download Key Pair**, and save this **** .pem file in a place that you can remember**


19. Click **Launch Instance**, and you have created your first EC2 instance, Cheers!

 Services ▾ Resource Groups ▾ ★

Quan_test ▾ N. California ▾ Support ▾

Launch Status

 **Your instances are now launching**
The following instance launches have been initiated: i-030acb3ecc2423429 [View launch log](#)

 **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](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [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](#)

 Feedback  English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

20. Go and proceed to the next step.