

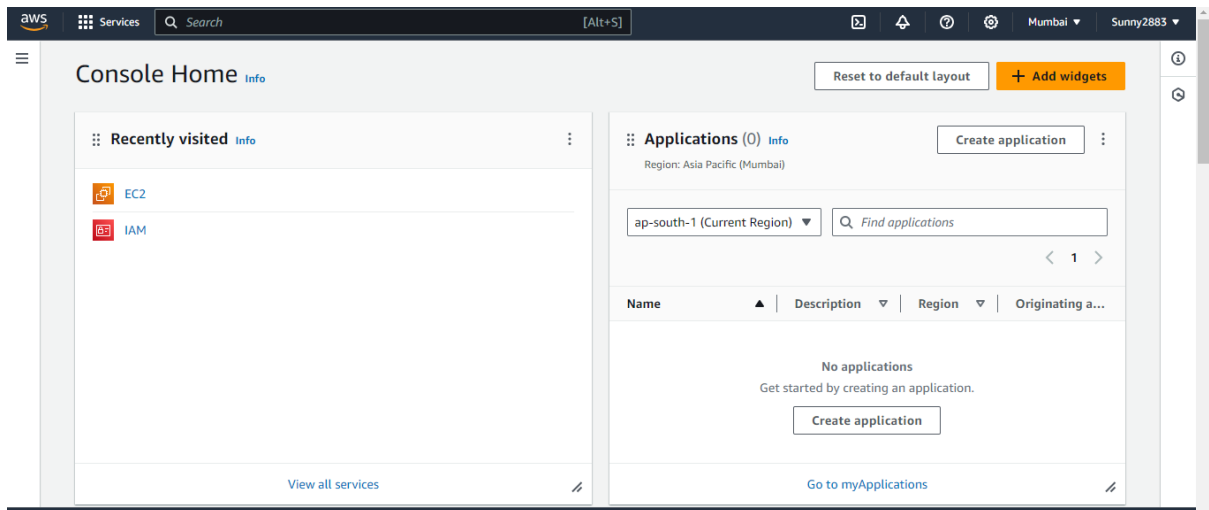
Assignment:2

Task:1

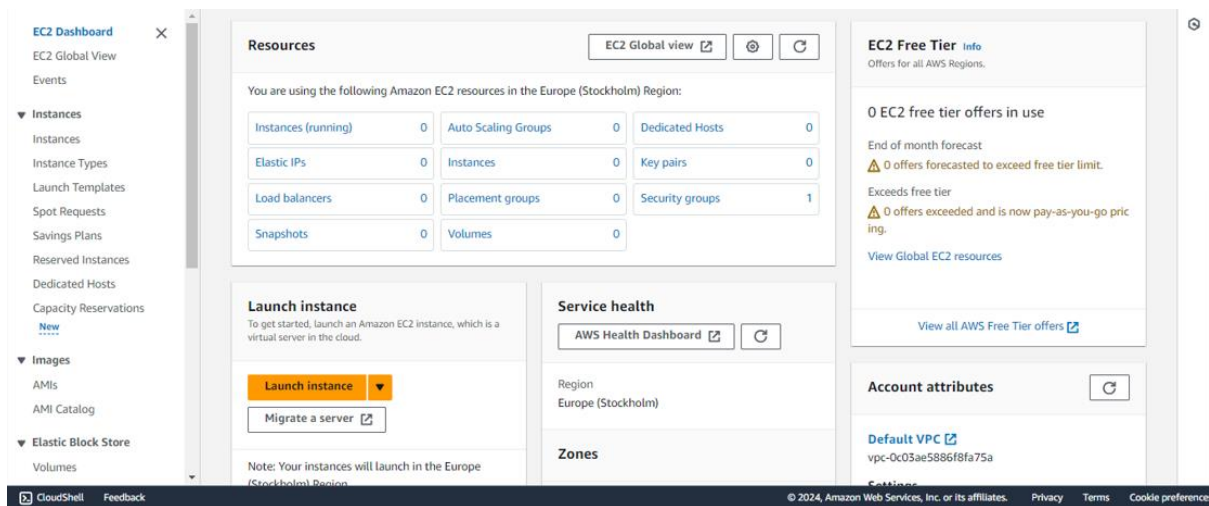
Launch an EC2 Instance:

1. Launch a new EC2 instance using the Amazon Linux 2 AMI using AWS console.

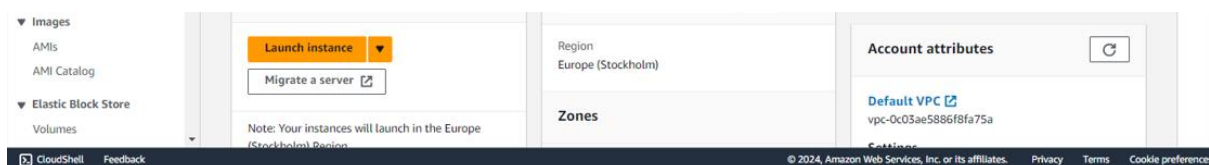
Step1: Access AWS management console .



Step2: navigate to EC2.



Step3: Click on launch instance on the EC2 dashboard.



Step4: Choose an amazon machine image (AMI).

Recents

Quick Start

Amazon Linux
aws


macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUS



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-00952f27cf14db9cd (64-bit (x86), uefi-preferred) / ami-0879d47e9438fb0eb (64-bit (Arm), uefi)

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

Free tier eligible

Step5: Choose an instance type.

▼ 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

Step6: Configure Instance details.

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Amazon Linux 2 AMI (HVM) - Ker...read more

ami-039e1f129f345d75f

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Step7: Configure security group and network setting.

▼ Network settings

Info

Edit

Network

Info

vpc-06988e5057435e138

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

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

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

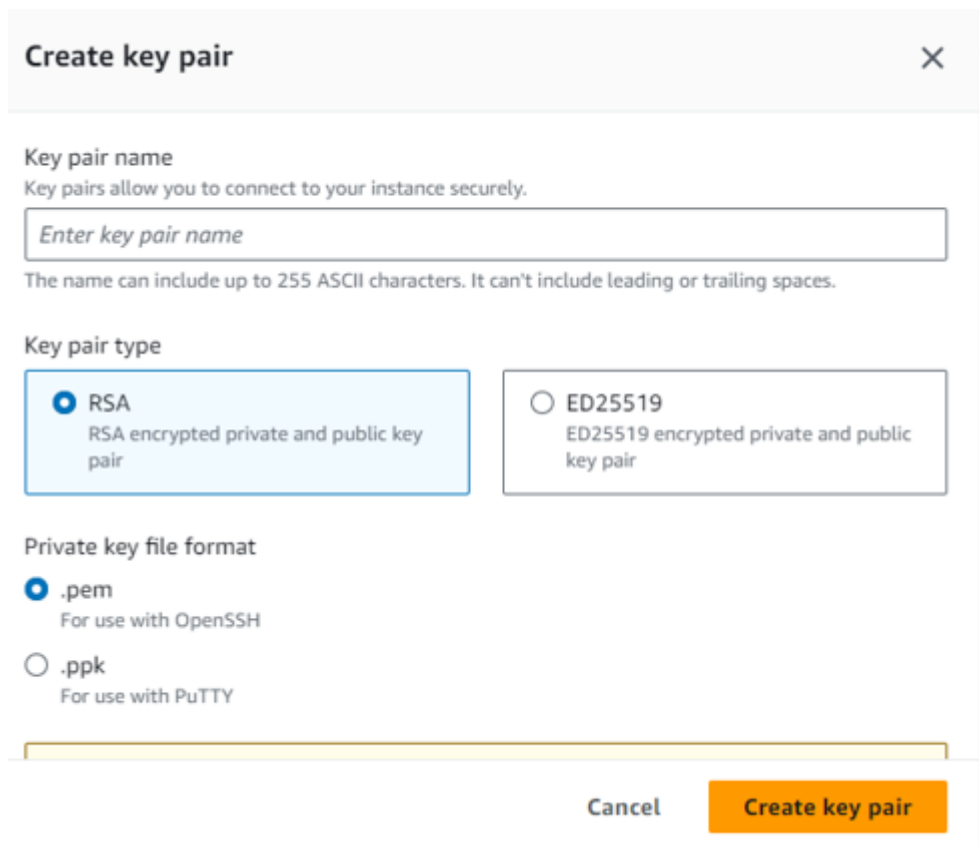
☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

⚠ 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.

×

Step8: Select a create a key pair.



The image shows the 'Create key pair' dialog box in the AWS Management Console. It has a title bar with a close button (X). The main content area is divided into sections: 'Key pair name' with a text input field and a note that the name can include up to 255 ASCII characters; 'Key pair type' with two radio button options: 'RSA' (selected) and 'ED25519'; and 'Private key file format' with two radio button options: '.pem' (selected) and '.ppk'. At the bottom, there are 'Cancel' and 'Create key pair' buttons.

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

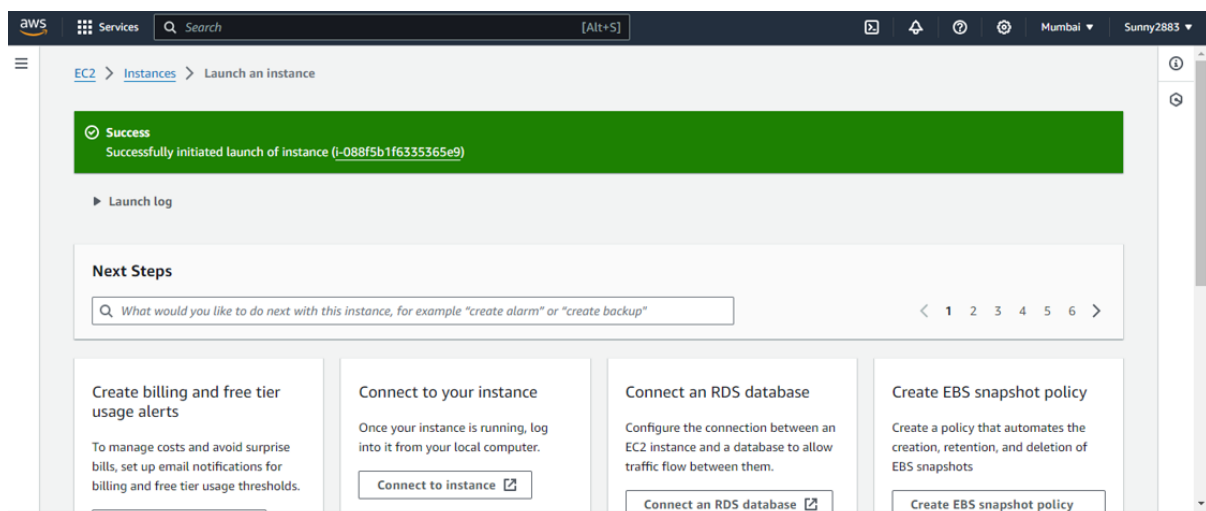
Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

[Cancel](#) [Create key pair](#)

Step9: Launch instance.



2. Configure Security Group:

With 22 and 80 Ports open.

▼ Inbound rules

Filter rules				
Name	Security group rule ID	Port range	Protocol	Source
-	sgr-0f23301ed539394c8	80	TCP	0.0.0.0/0
-	sgr-0efd236374d60357c	22	TCP	0.0.0.0/0



▼ Outbound rules

3. Connect to EC2 Instance:

Connect to the newly launched EC2 instance using SSH.

Step1: Get the public ip of instance.

Public IPv4 address

 43.204.22.221 | [open address](#) 

Step2: Open a terminal or command prompt.

Step3: change key pair permission.

Chmod 400 MyServerKey.pem

Step4: Connect the EC2 instance using SSH.

Ssh -i ./ MyServerKey.pem [ec2@43.204.22.221](#)

```
PS C:\Users\promact\Downloads> ssh -i .\MyServerKey.pem ec2-user@43.204.22.221
The authenticity of host '43.204.22.221 (43.204.22.221)' can't be established.
ED25519 key fingerprint is SHA256:KwaJ2W05ZUja8nUrygNyVGUxPXmMISkfAowIIxhlike.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '43.204.22.221' (ED25519) to the list of known hosts.

#_
~\_ #####_      Amazon Linux 2
~~ \_#####\
~~ \###|         AL2 End of Life is 2025-06-30.
~~ \#/ ---
~~ V~' '--->
    /
  _/ _/
 _/m/'

A newer version of Amazon Linux is available!

Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
```

Step4: We are now connected to the our Ec2 instance.

```
[ec2-user@ip-172-31-45-45 ~]$ whoami
ec2-user
[ec2-user@ip-172-31-45-45 ~]$ |
```