



AWS Cloud Practice - Part 1

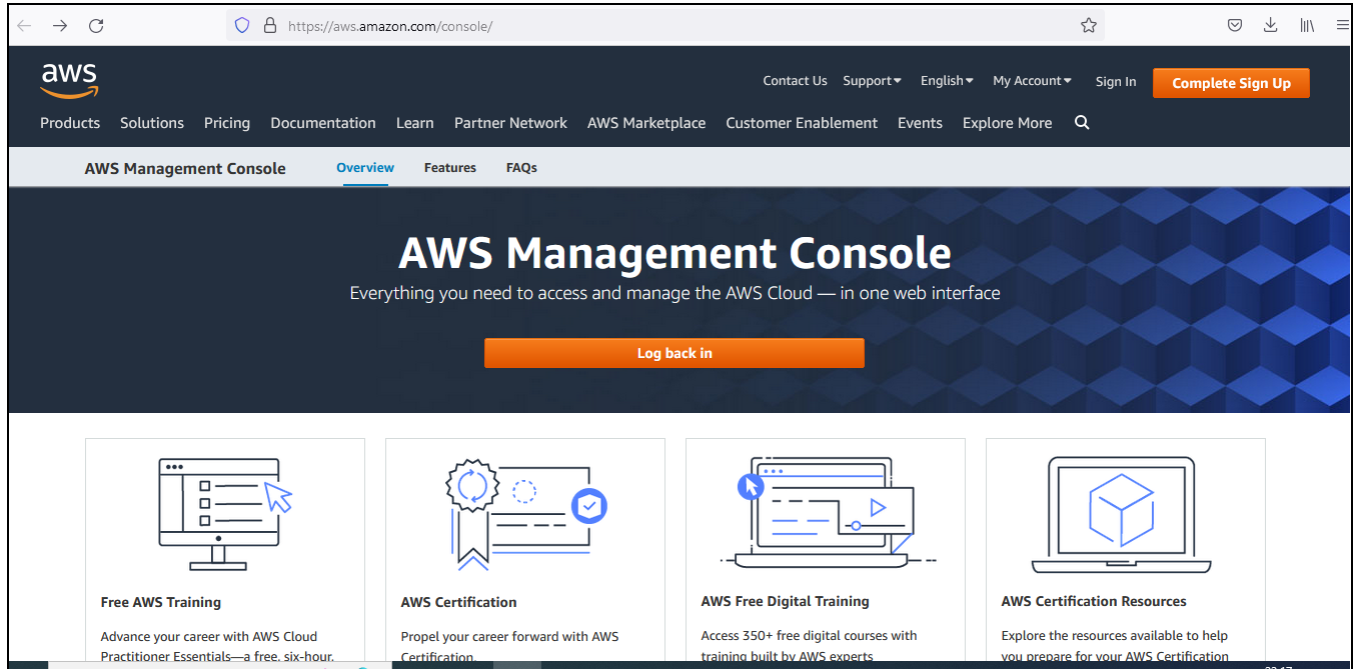
CLOUD COMPUTING TEAM
CDAC
CHENNAI

Table of Contents

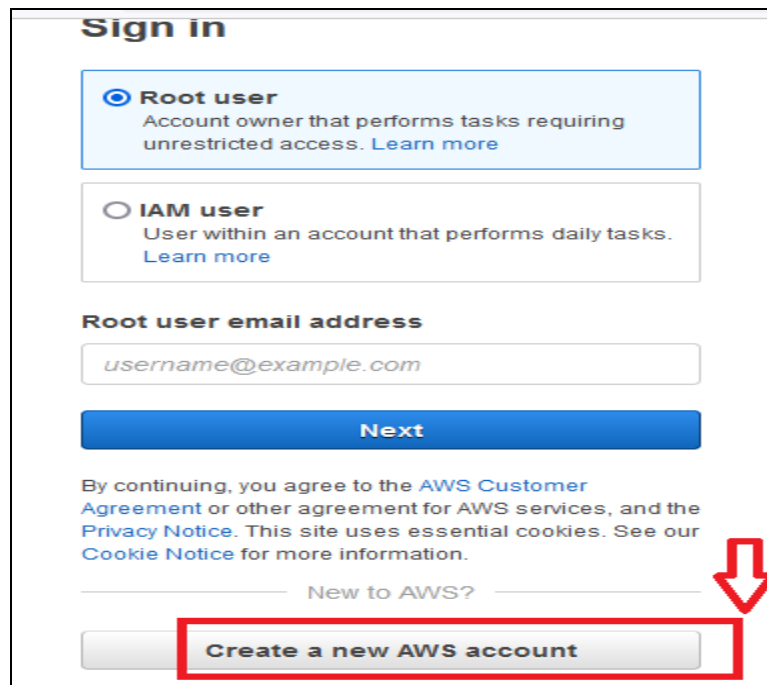
- Free tier Account Creation in AWS
- Identity and Access Management (IAM)
- Multi-factor Authentication creation
- Launch first EC2 instance
- Launch Windows instance

AWS Management Console

Step:1 Login to the Console : <https://aws.amazon.com/console> Click Sign In to the Console



Step2: Sign Up as the first time user by clicking the **Create a new AWS account**.



Step 3: Verify email address



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.



Sign up for AWS

Root user email address

Used for account recovery and some administrative functions

prabhav@cdac.in

AWS account name

Choose a name for your account. You can change this name in your account settings after you sign up.

Prabhasathesh

Verify email address

OR

Sign in to an existing AWS account



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.



Sign up for AWS

Confirm you are you

Making sure you are secure -- it's what we do.

We sent an email with a verification code to **maruthicarstudio@gmail.com**. (not you?)

Enter it below to confirm your email.

Verification code

361421

Verify

Resend code

Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.



Always free
Never expires



12 months free
Start from initial sign-up date



Trials
Start from service activation date

Sign up for AWS

Contact Information

How do you plan to use AWS?

- ☐ Business - for your work, school, or organization
- ☒ Personal - for your own projects

Who should we contact about this account?

Full Name

Sathesh

Phone Number

Enter your country code and your phone number.

91-9999999999

Country or Region

India ▼

City

Chennai

State, Province, or Region

TamilNadu

Postal Code


600100

Customers with an Indian contract address are served by Amazon Internet Services Private Ltd. (AISPL). AISPL is the local seller for AWS services in India.


☐ I have read and agree to the terms of the [AWS Customer Agreement](#).


Continue (step 2 of 5)

Step 4: Give the credit card details correctly, Card Number, Expiry Date and Card Holder Name. Click on Secure Submit



Secure verification




 We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to \$1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.



Sign up for AWS

Billing Information

Credit or Debit card number

AWS accepts all major credit and debit cards. To learn more about payment options, review our [FAQ](#)

Expiration date


Month ▼

Year ▼

Cardholder's name

CVV

Verified by VISA



Merchant details

Merchant Name:	AMAZON
Date:	Jun 06, 2022
Card Number:	4639 XXXX XXXX 1361
Total Charge:	Rs. 2.00

Authenticate Transaction

OTP

Successfully sent the One Time Password to your Registered Mobile Number 99**2***51.

Enter OTP

[Resend OTP](#)

CANCEL

SUBMIT

Note- Please ensure that your latest mobile number/ email id is updated in the Bank records. Visit nearest Branch or call Customer Care for the same.

This page will automatically time out after **02:54** seconds

Step 5: After successful verification, Select the Support plan as Basic Plan (Free)



Select a Support Plan

AWS offers a selection of support plans to meet your needs. Choose the support plan that best aligns with your AWS usage. [Learn more](#)

Basic Plan	Developer Plan	Business Plan
Free	From \$29/month	From \$100/month
<ul style="list-style-type: none"> Included with all accounts 24/7 self-service access to forums and resources Best practice checks to help improve security and performance Access to health status and notifications 	<ul style="list-style-type: none"> For early adoption, testing and development Email access to AWS Support during business hours 1 primary contact can open an unlimited number of support cases 12-hour response time for nonproduction systems 	<ul style="list-style-type: none"> For production workloads & business-critical dependencies 24/7 chat, phone, and email access to AWS Support Unlimited contacts can open an unlimited number of support cases 1-hour response time for production systems

Need Enterprise level support?
Contact your account manager for additional information on running business and mission critical-workloads on AWS (starting at \$15,000/month). [Learn more](#)

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.
[Privacy Policy](#) [Terms of Use](#) [Sign Out](#)

Step 6: Once account is created, login using the credentials



The image shows the AWS Root user sign-in page. At the top is the AWS logo. Below it is the heading "Root user sign in" with an information icon. The email field is pre-filled with "prabhav@cdac.in". The password field is masked with dots. There is a "Forgot password?" link next to the password field. A blue "Sign in" button is at the bottom. Below the button are two links: "Sign in to a different account" and "Create a new AWS account".

aws

Root user sign in ⓘ

Email: prabhav@cdac.in

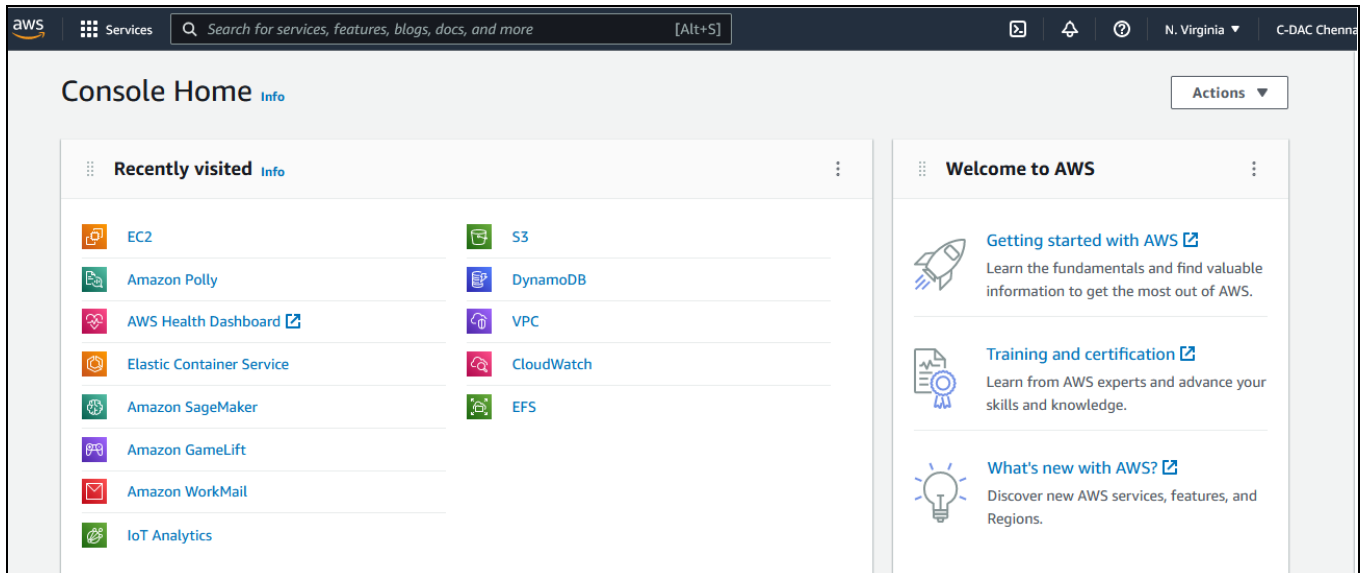
Password [Forgot password?](#)

.....|

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)



The image shows the AWS Console Home dashboard. The top navigation bar includes the AWS logo, "Services", a search bar, and a language selector "[Alt+S]". The right side of the header shows the region "N. Virginia" and the account type "C-DAC Chennai". The main content area is titled "Console Home" and includes an "Actions" dropdown. The dashboard is divided into two main sections: "Recently visited" and "Welcome to AWS".

Recently visited ⓘ

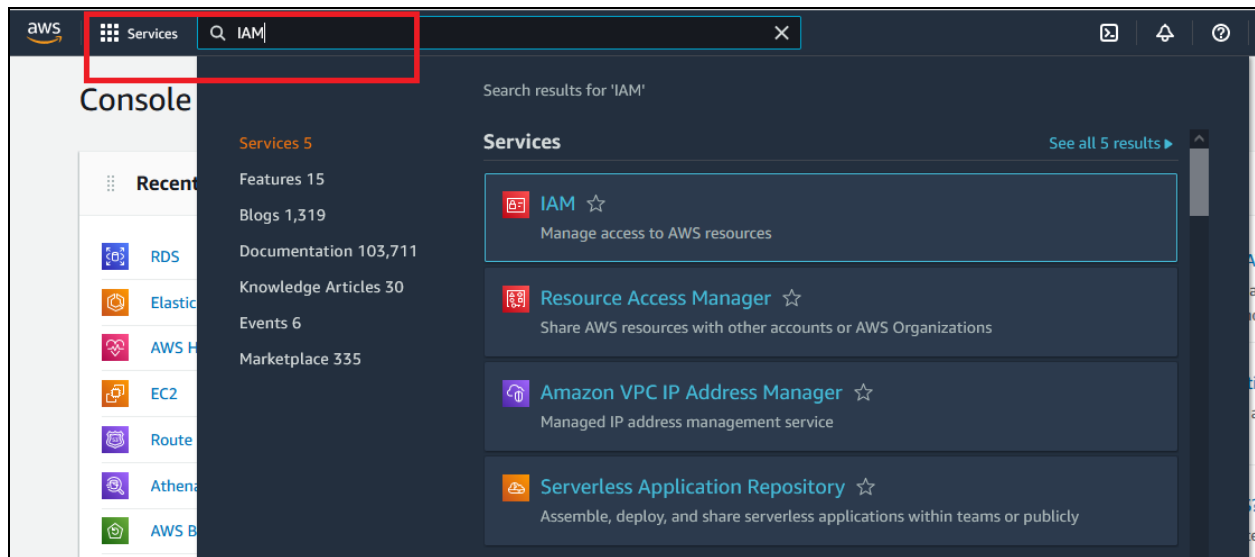
- EC2
- Amazon Polly
- AWS Health Dashboard ⓘ
- Elastic Container Service
- Amazon SageMaker
- Amazon GameLift
- Amazon WorkMail
- IoT Analytics
- S3
- DynamoDB
- VPC
- CloudWatch
- EFS

Welcome to AWS

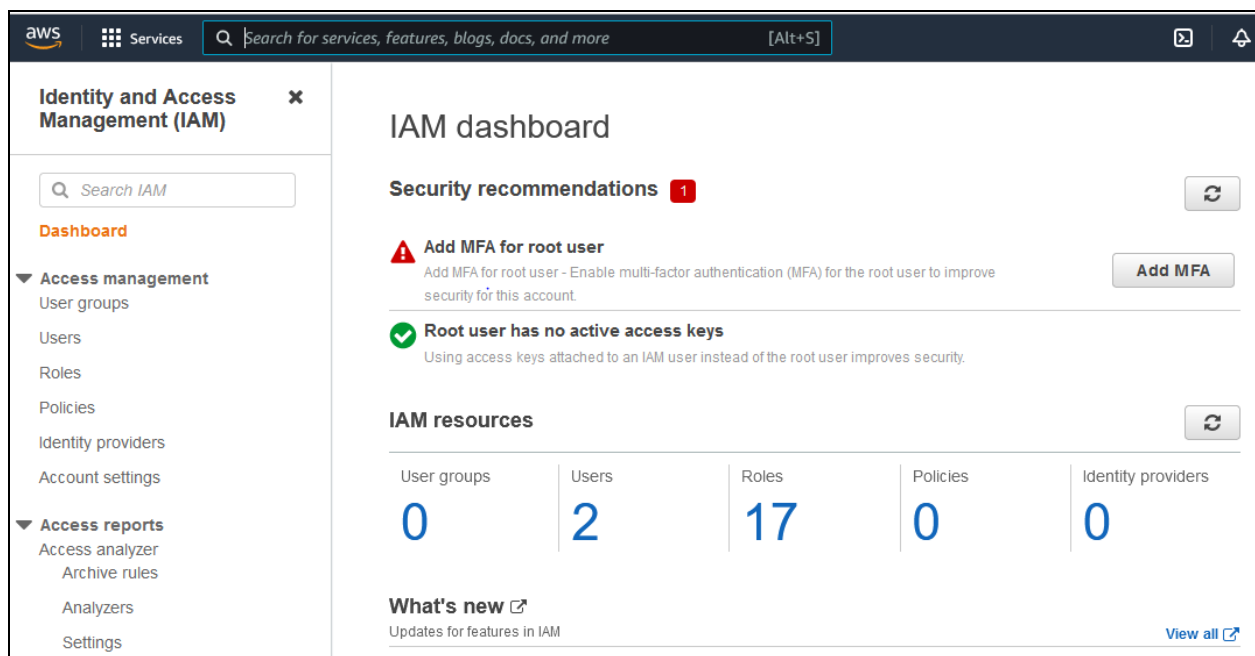
- Getting started with AWS** ⓘ
Learn the fundamentals and find valuable information to get the most out of AWS.
- Training and certification** ⓘ
Learn from AWS experts and advance your skills and knowledge.
- What's new with AWS?** ⓘ
Discover new AWS services, features, and Regions.

Identity and Access Management (IAM)

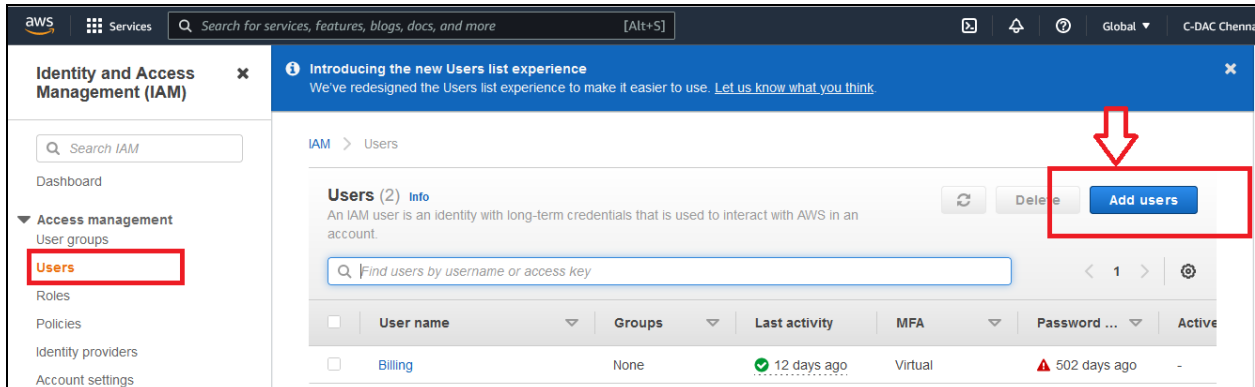
Step 7 - Search IAM in Services



Step 8 - Create Users, Roles and Policies using IAM dashboard



Step 9: To create new user- Select Users → Add users



The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Users' selected under 'Access management'. The main content area shows the 'Users (2)' page. A red box highlights the 'Add users' button in the top right corner of the main content area, with a red arrow pointing to it.

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

- ☐ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

*** Required** [Cancel](#) [Next: Permissions](#)

Step 10: Select AWS credential type as Password and create a custom password

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☐ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

☐ Autogenerated password

☒ Custom password

••••••••

☐ Show password

Require password reset

☐ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

Cancel **Next: Permissions**

Step 11: Attach policy to the newly created user

Add user

1 2 3 4 5

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

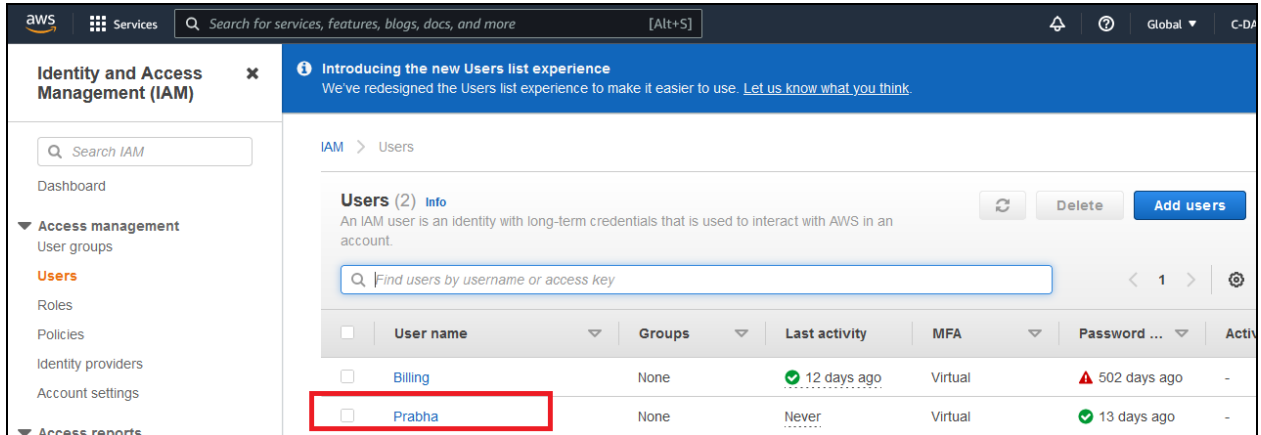
Create policy

Filter policies ▼ Showing 754 results

	Policy name ▼	Type	Used as
<input type="checkbox"/>	AdministratorAccess	Job function	None
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None

Cancel Previous **Next: Tags**

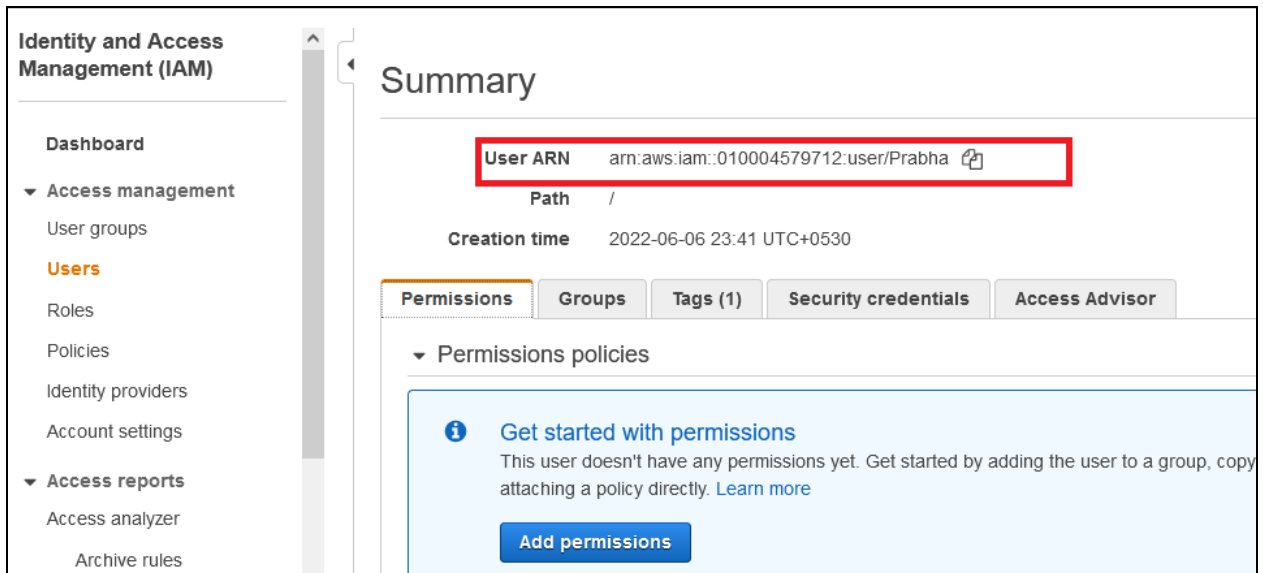
Step 12: View the newly created user



The screenshot shows the AWS IAM console 'Users' page. A table lists the users, with 'Prabha' highlighted by a red box. The table columns are: User name, Groups, Last activity, MFA, Password, and Actions.

User name	Groups	Last activity	MFA	Password	Actions
Billing	None	12 days ago	Virtual	502 days ago	-
Prabha	None	Never	Virtual	13 days ago	-

User creation has been completed successfully now you will get an access URL with your account number. Note the URL for access



The screenshot shows the 'Summary' page for the user 'Prabha'. The 'User ARN' is highlighted with a red box. The page also shows the 'Creation time' and a 'Permissions policies' section with a 'Get started with permissions' message and an 'Add permissions' button.

User ARN `arn:aws:iam::010004579712:user/Prabha`

Path /

Creation time 2022-06-06 23:41 UTC+0530

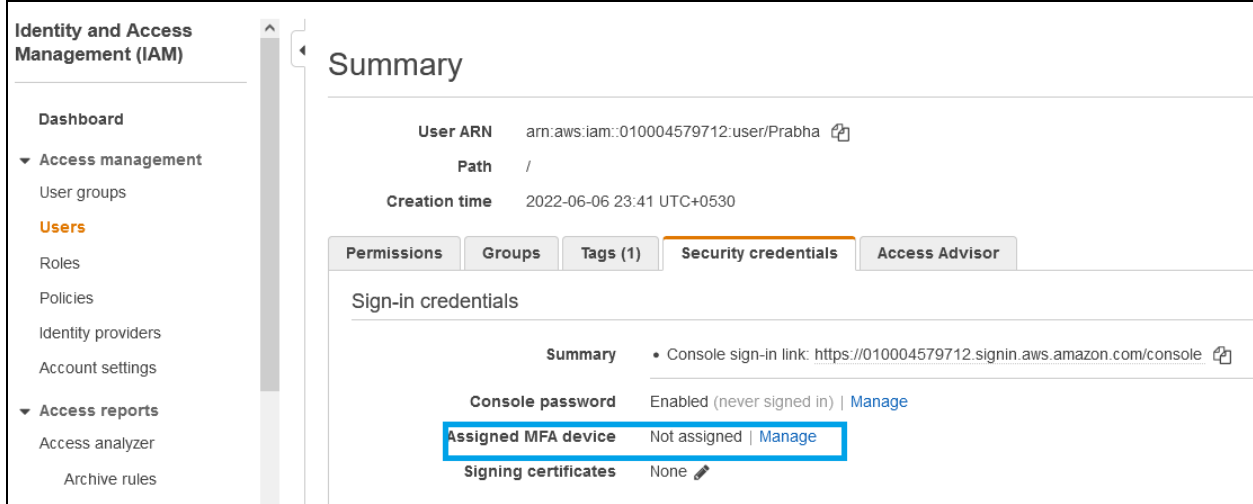
Permissions policies

Get started with permissions
This user doesn't have any permissions yet. Get started by adding the user to a group, copy attaching a policy directly. [Learn more](#)

Add permissions

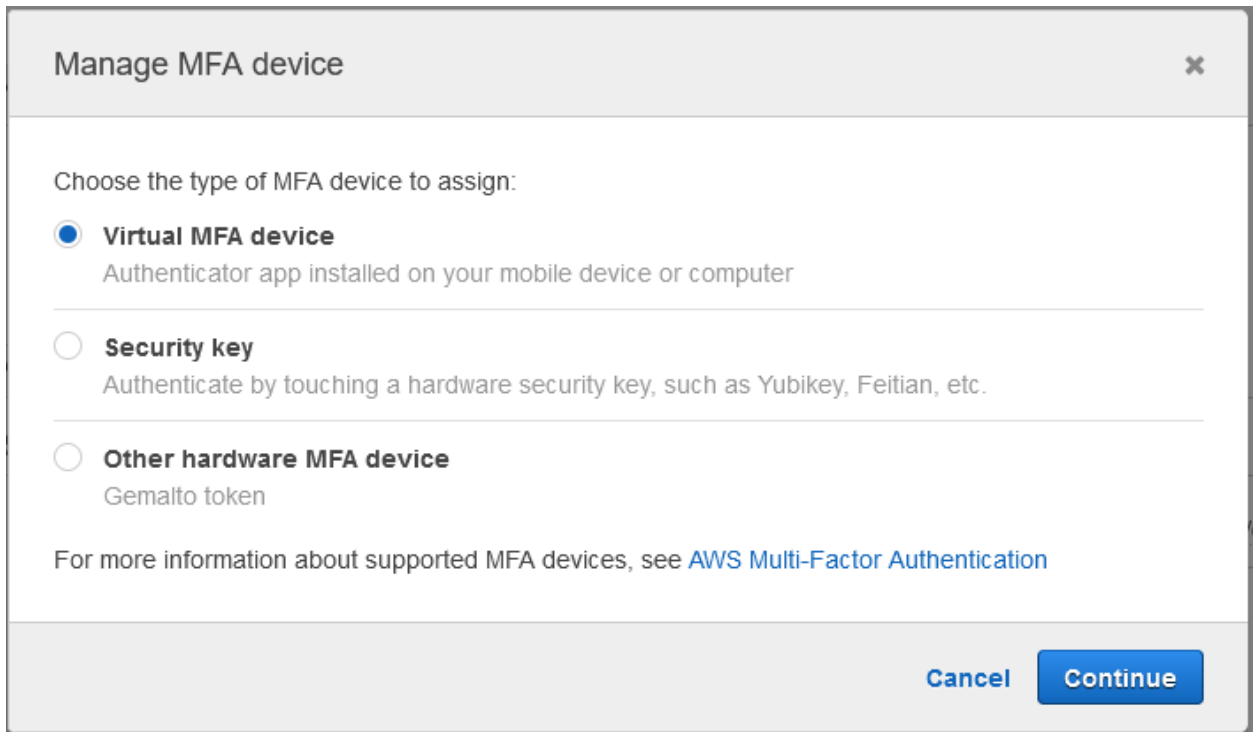
Multi-factor Authentication creation

Step 13: View the newly created user



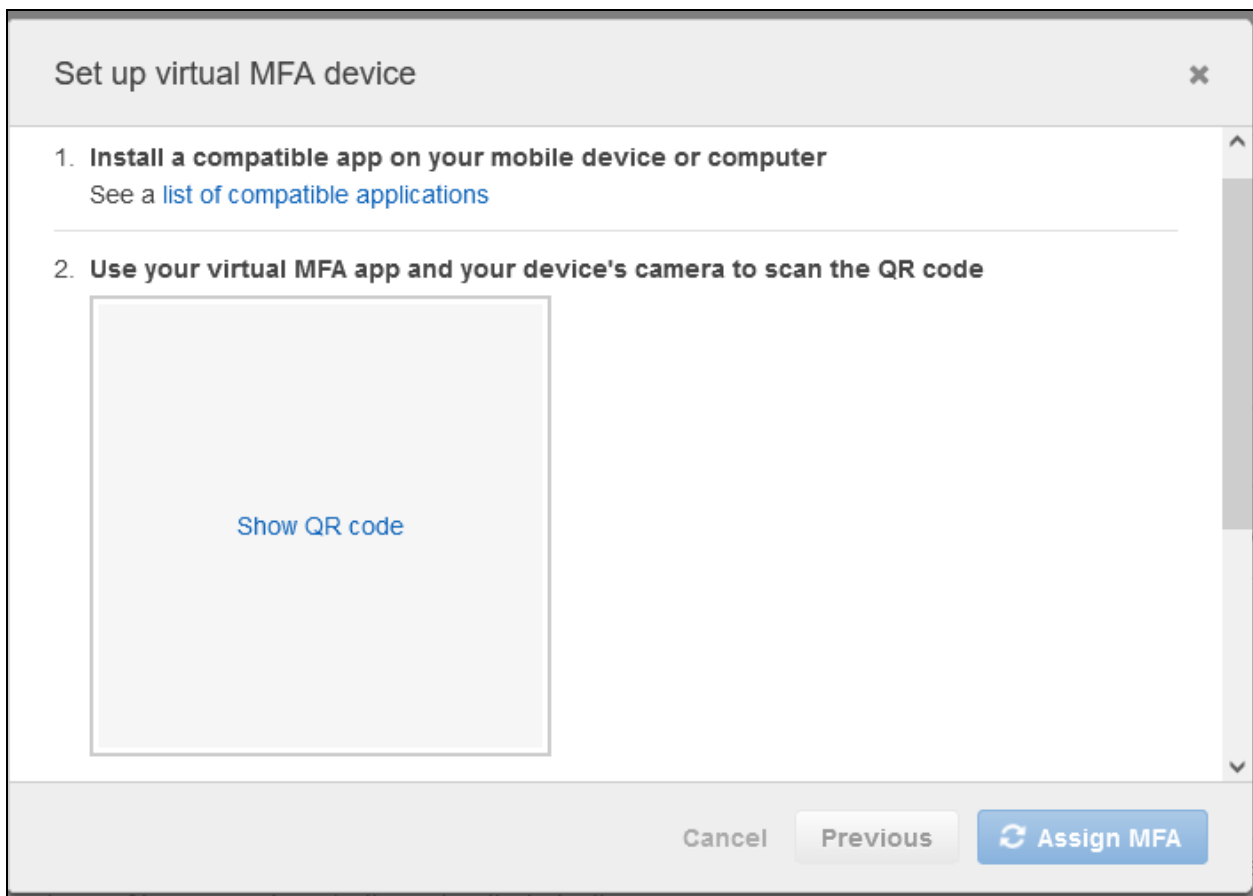
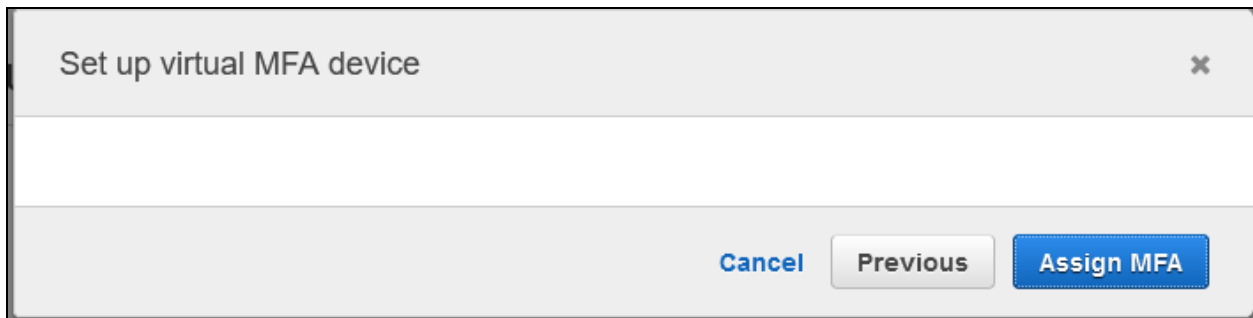
The screenshot shows the AWS Identity and Access Management (IAM) console. On the left is a navigation menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, and Archive rules. The main area displays the 'Summary' tab for a user. Key details include: User ARN (arn:aws:iam::010004579712:user/Prabha), Path (/), and Creation time (2022-06-06 23:41 UTC+0530). Below these are tabs for Permissions, Groups, Tags (1), Security credentials, and Access Advisor. The 'Security credentials' tab is active, showing 'Sign-in credentials'. It includes a 'Summary' section with a console sign-in link, a 'Console password' section (Enabled, never signed in), and an 'Assigned MFA device' section (Not assigned). The 'Assigned MFA device' section is highlighted with a blue box. There is also a 'Signing certificates' section showing 'None'.

Step 14: Install Google Authenticator in smart phone and ready to pair. Click Continue in Manage MFA device



The screenshot shows the 'Manage MFA device' dialog box. It has a title bar with a close button (X). The main content area asks the user to 'Choose the type of MFA device to assign:'. There are three radio button options: 'Virtual MFA device' (selected), 'Security key', and 'Other hardware MFA device'. Each option has a brief description: 'Authenticator app installed on your mobile device or computer' for Virtual, 'Authenticate by touching a hardware security key, such as Yubikey, Feitian, etc.' for Security key, and 'Gemalto token' for Other hardware. At the bottom, there is a link to 'AWS Multi-Factor Authentication' for more information. The dialog box has 'Cancel' and 'Continue' buttons at the bottom right.

Step 15: Click Assign MFA in Setup Virtual MFA device



Step 16: Click in Show QR Code and scan the same code from your Google authenticator App. It will generate six digit codes enter one code in first MFA code 1 wait 1 minute and second code in MFA Code 2 Click on Assign MFA

That's it, now you successfully enabled MFA (Multi-Factor Authentication).

Hereafter if you want to login, you have to enter credentials and MFA code to Login.

Set up virtual MFA device

✓

You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.

Close

Sign-in credentials

Summary

- Console sign-in link: <https://010004579712.signin.aws.amazon.com/console>
- MFA is required when signing in. [Learn more](#)


Console password

Enabled (never signed in) | [Manage](#)

Assigned MFA device

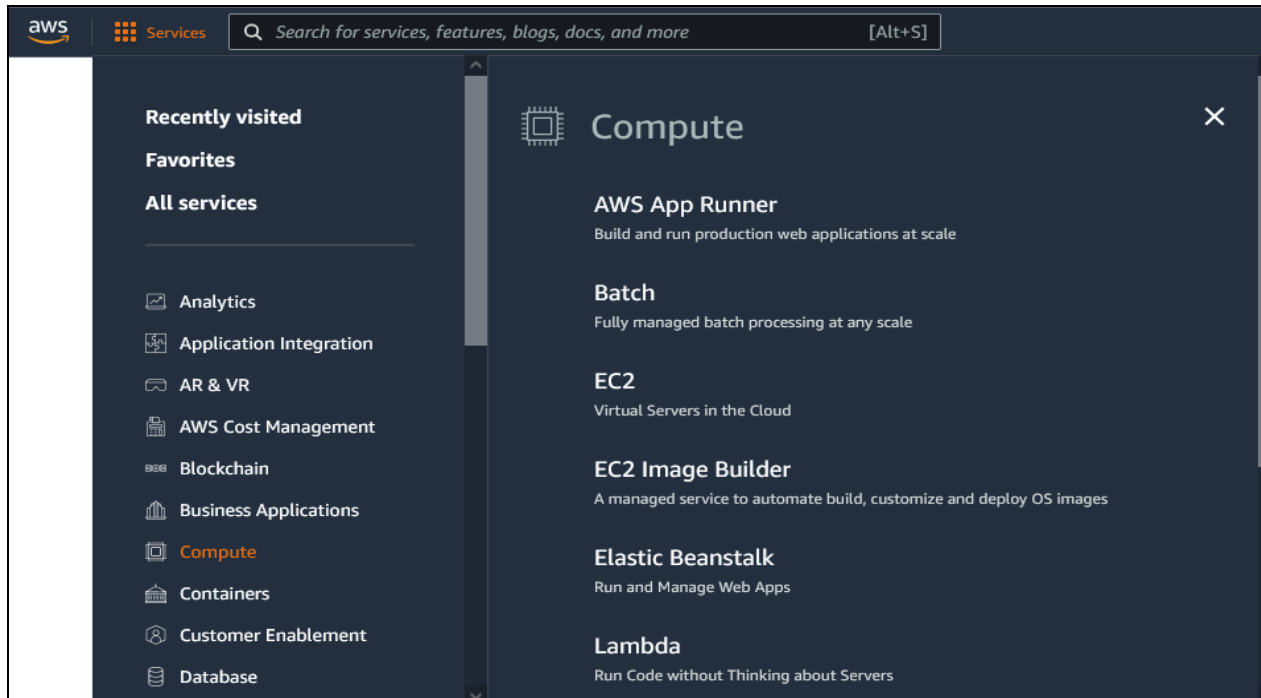
arn:aws:iam::010004579712:mfa/Prabha (Virtual) | [Manage](#)

Signing certificates

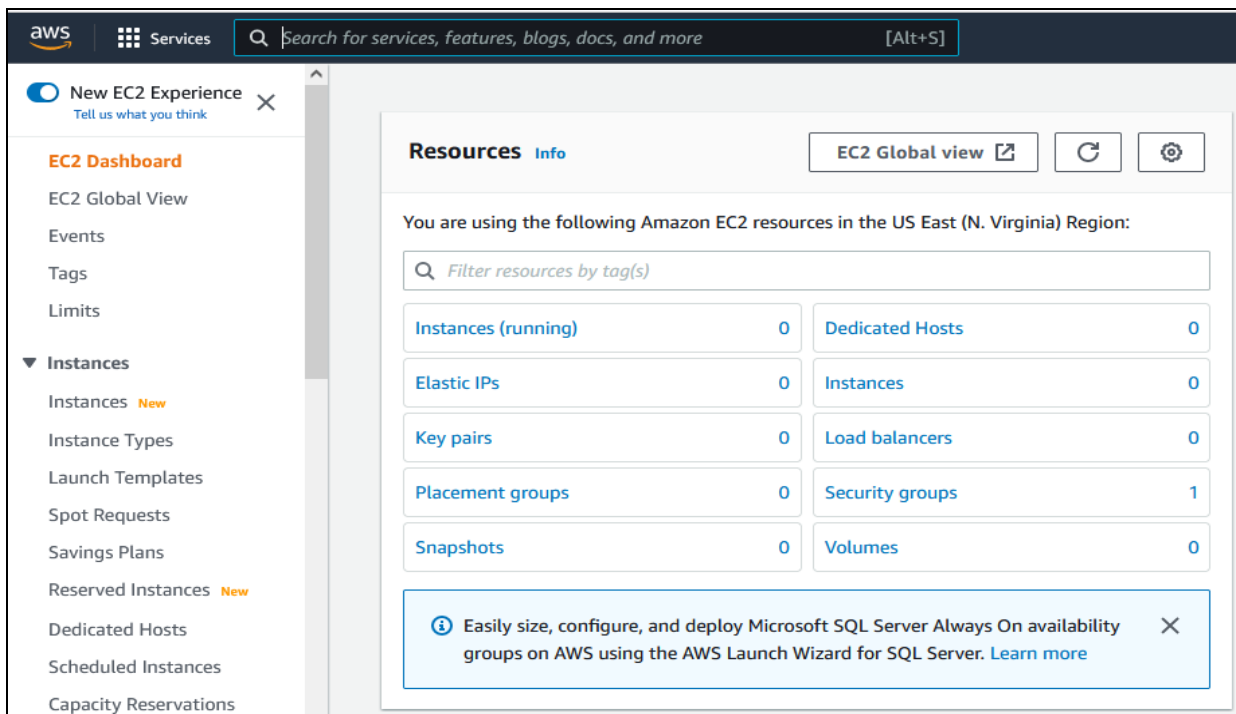
None 

Launching of first EC2 instance

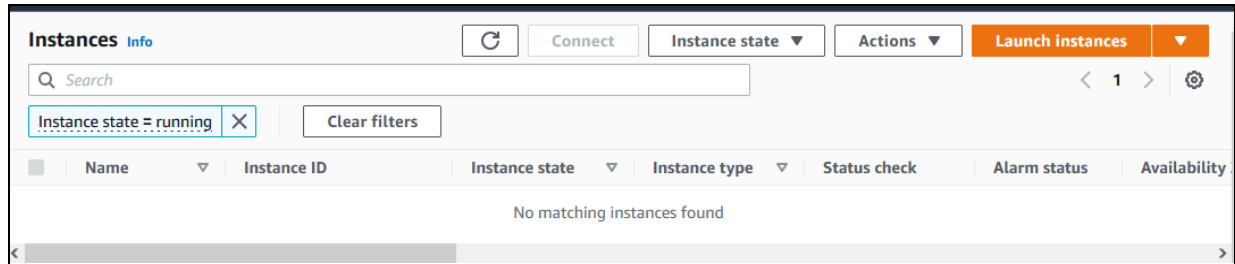
Step 17: Go to Services drop down click on Compute → EC2



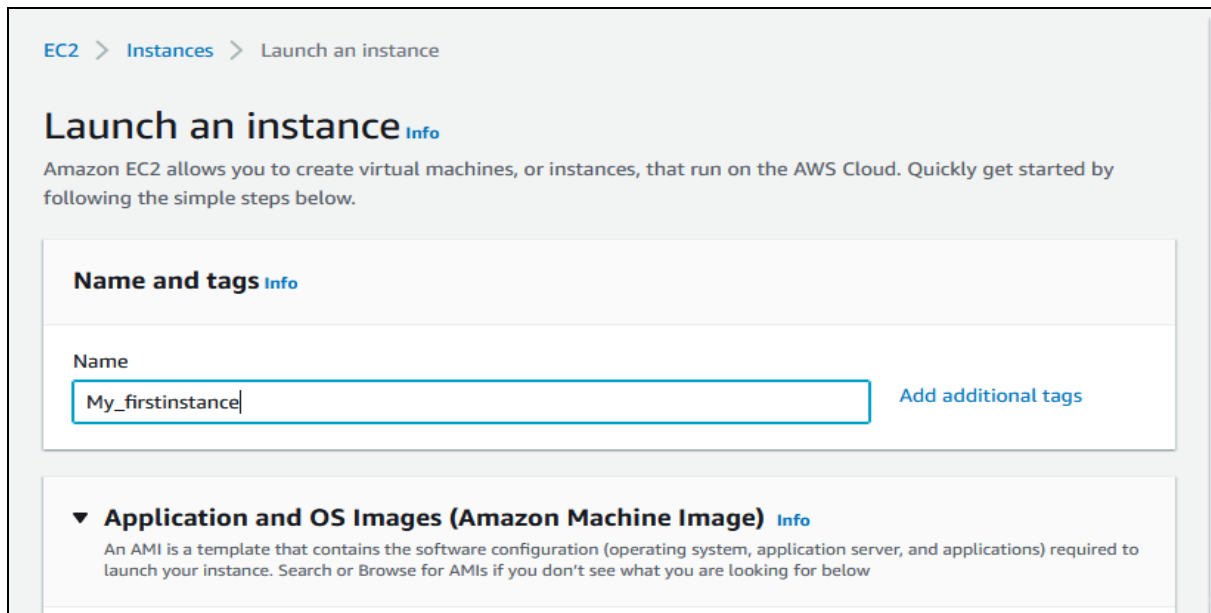
Step 18: Resource provides an overview of the Compute → EC2



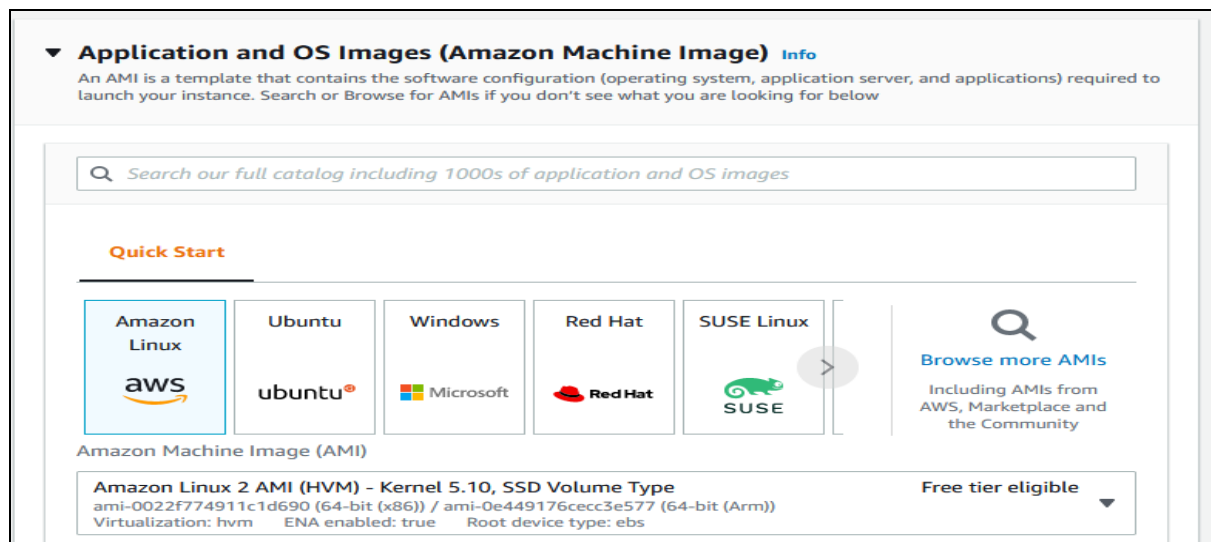
Step 19: Go to Instances → Launch Instances



Step 20: Provide a Name to the instance



Step 21: Select the Image from the List



Step 22: Select the AMI Flavors (free tier) that suits the requirement

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type ami-0022f774911c1d690 (64-bit (x86)) / ami-0e449176cecc3e577 (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible
Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type ami-06eecef118bbf9259 (64-bit (x86)) / ami-090230ed0c6b13c74 (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible
Deep Learning AMI GPU PyTorch 1.11.0 (Amazon Linux 2) 20220526 ami-00ab1614b421d5575 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Deep Learning AMI (Amazon Linux 2) Version 61.3 ami-0ac44af394b7d6689 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Deep Learning AMI GPU TensorFlow 2.7.0 (Amazon Linux 2) 20220526 ami-04ff3b97e4a48d8e0 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Deep Learning Base AMI (Amazon Linux 2) Version 53.1 ami-082ef5337e086ab05 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Amazon Linux 2 LTS with SQL Server 2017 Standard ami-02160391b456f1164 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Amazon Linux 2 with .NET 6, PowerShell, Mono, and MATE Desktop Environment ami-0728c171aa8e41159 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	
Amazon Linux 2 LTS with SQL Server 2019 Standard ami-0874d82d2138e9fd1 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs	

Step 23: Select the Amazon Linux Image with Free tier eligible

Recents

Quick Start

Amazon Linux

aws

Ubuntu

ubuntu®

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Search

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-0022f774911c1d690 (64-bit (x86)) / ami-0e449176cecc3e577 (64-bit (Arm))

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

Free tier eligible

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220426.0 x86_64 HVM gp2

Architecture

AMI ID

64-bit (x86)

ami-0022f774911c1d690

Step 24 : Select the Instance Flavor in free tier eligible

▼ Instance type Info

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible

Compare instance types

Step 25 : Select the Key pair (already existing) to login the instances using the SSH key pair. If no existing key pair Click on Create new 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

Select

Create new key pair

Step 26 : Create a Key pair name with preferred type as RSA(RSA private key cryptographic algorithm) and Private key file format as .pem.

Note : Download the private key file (demo.pem) and keep it safe. If the key is lost, then the VM becomes inaccessible.

Create key pair

×

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. 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](#)

Key pair name

The name can include upto 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 (Not supported for Windows instances)

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

Cancel

Create key pair

Step 27 : Use the created 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*

▼

↻

Create new key pair

Step 28: A default VPC Network is created. Create Security Groups for Firewall policies that create inbound and outbound connections

▼ Network settings
Edit

Network

vpc-96d840eb

Subnet

No preference (Default subnet in any availability zone)

Auto-assign public IP

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

Step 29: Additional EBS storage volumes can be created and attached to the instance.

▼ Configure storage [Info](#)
Advanced

1x 8 GiB gp2 Root volume

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

0 x File systems
Edit

▼ **Configure storage** [Info](#)

Advanced

1x 8 GiB gp2 Root volume

1x 8 GiB gp3 EBS volume

Remove

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

0 x File systems

Edit

Step 30 : Summary of the Instance

▼ **Summary**

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)

ami-09d56f8956ab235b3

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group


Storage (volumes)

2 volume(s) - 16 GiB

Cancel

Launch instance

EC2 > Instances > Launch an instance


Success
 Successfully initiated launch of instance (i-06b0dea5fa14b97b0)

▼ Launch log

Initializing requests	Succeeded
Creating security groups	Succeeded
Creating security group rules	Succeeded
Launch initiation	Succeeded

Step 31: Dashboard view of the instance

Instances (1/2) Info Refresh Connect Instance state Actions Launch instances

Search

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input type="checkbox"/>	My_firstinstance	i-06b0dea5fa14b97b0	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c
<input checked="" type="checkbox"/>	Demo_instance	i-0dad2336b7da4fdbba	Running	t2.micro	–	No alarms	us-east-1c

Instance: i-0dad2336b7da4fdbba (Demo_instance)

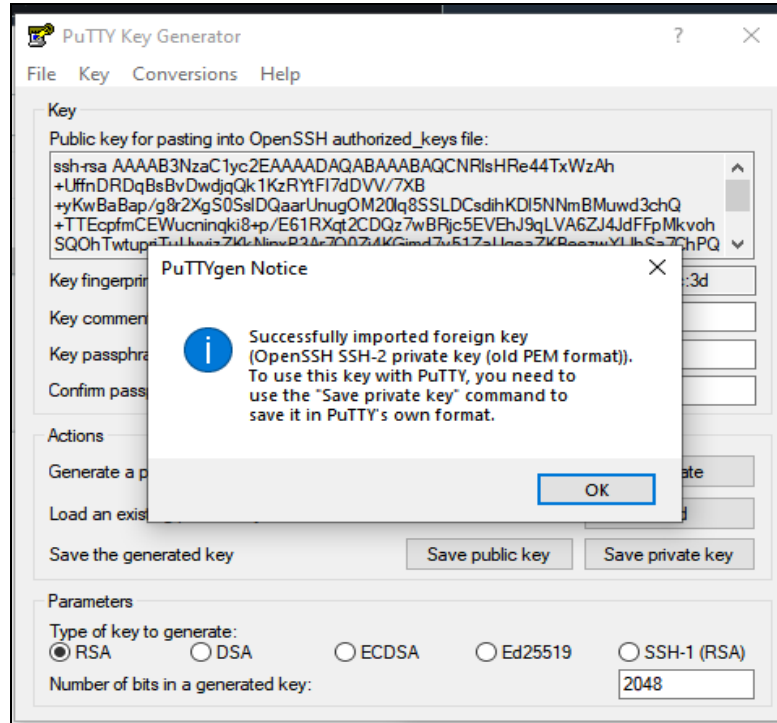
Details Security Networking Storage Status checks Monitoring Tags

▼ Instance summary Info

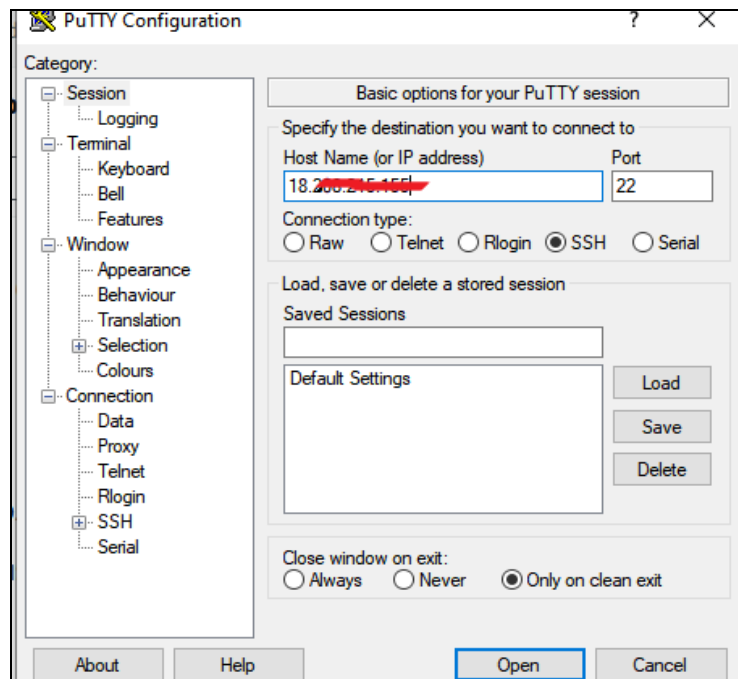
Instance ID i-0dad2336b7da4fdbba (Demo_instance)	Public IPv4 address 18 [redacted] open address	Private IPv4 addresses 172.31.16.22
IPv6 address –	Instance state Running	Public IPv4 DNS ec2-18-[redacted].1.amazonaws.com open address

Step 32: Install putty msi installer you will get PuttyGen and Putty for accessing Linux VM. Open PuttyGen and load the demo.pem file downloaded from Step 26.

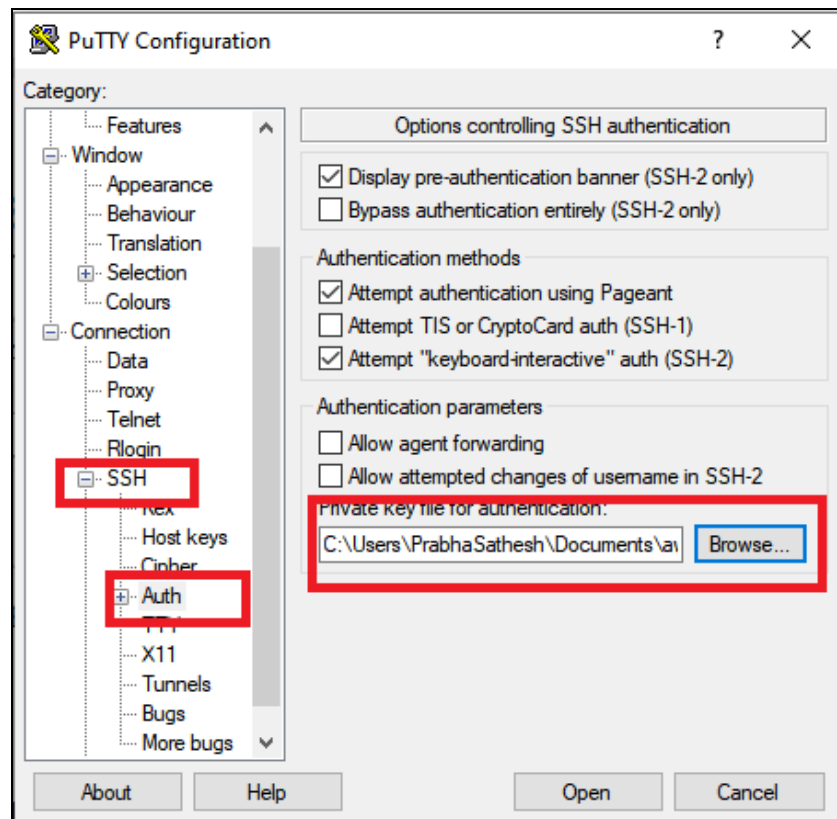
Click OK and save the Private key.(demo.ppk)



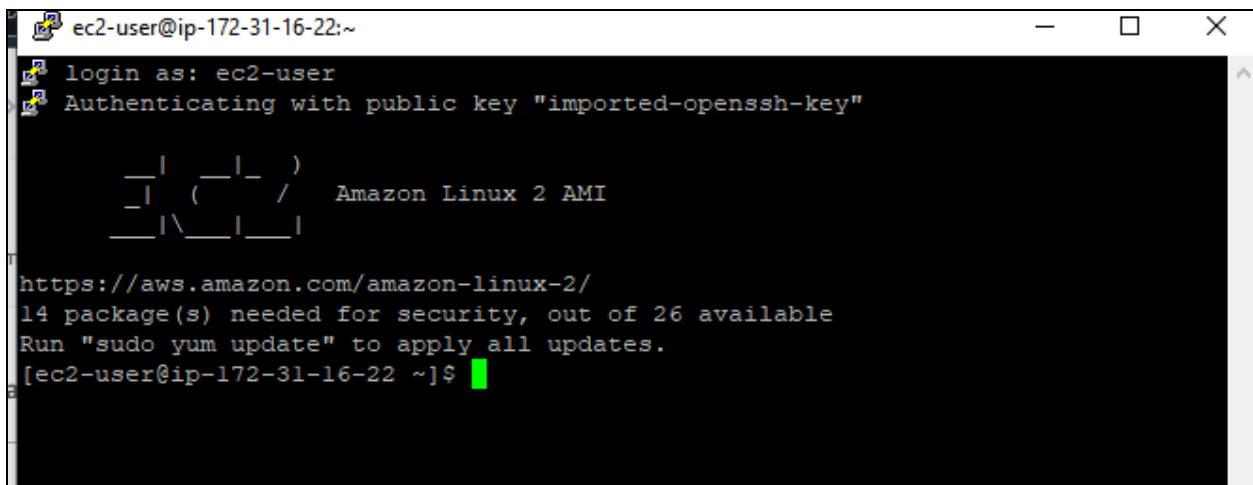
Step 33: Enter the public IP address of the VM in Putty.



Expand SSH Click on Auth Browse and attach demo.ppk file downloaded from Step 32



Step 34: Now we have successfully logged inside the VM



Step 35: Another method to connect to EC2 instance is using EC2 Instance Connect

Connect to instance [Info](#)

Connect to your instance i-0dad2336b7da4fdbba (Demo_instance) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 Serial Console

Instance ID
i-0dad2336b7da4fdbba (Demo_instance)

Public IP address
18.232.173.212

User name

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

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

Cancel

Connect

```
last login: Wed Jun 8 07:07:23 2022 from 106.198.4.169
 _ | _ | _ |
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
14 package(s) needed for security, out of 26 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-16-22 ~]$
```

i-0dad2336b7da4fdbba (Demo_instance)

Public IPs: 18.232.173.212 Private IPs: 172.31.16.22

Step 36: Creating a Web server inside the Virtual Machine.Update the repository using yum update.

```
[ec2-user@ip-172-31-16-22 ~]$ sudo yum update -y;
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                               | 3.7 kB      00:00
Resolving Dependencies
--> Running transaction check
---> Package curl.x86_64 0:7.79.1-1.amzn2.0.1 will be updated
---> Package curl.x86_64 0:7.79.1-2.amzn2.0.1 will be an update
---> Package dracut.x86_64 0:033-535.amzn2.1.5 will be updated
---> Package dracut.x86_64 0:033-535.amzn2.1.6 will be an update
---> Package dracut-config-generic.x86_64 0:033-535.amzn2.1.5 will be updated
---> Package dracut-config-generic.x86_64 0:033-535.amzn2.1.6 will be an update
---> Package iproute.x86_64 0:5.10.0-2.amzn2.0.1 will be updated
---> Package iproute.x86_64 0:5.10.0-2.amzn2.0.2 will be an update
---> Package kernel.x86_64 0:5.10.112-108.499.amzn2 will be installed
---> Package kernel-tools.x86_64 0:5.10.109-104.500.amzn2 will be updated
```

```
ec2-user@ip-172-31-16-22:~
Installed:
  kernel.x86_64 0:5.10.112-108.499.amzn2

Updated:
  curl.x86_64 0:7.79.1-2.amzn2.0.1
  dracut.x86_64 0:033-535.amzn2.1.6
  dracut-config-generic.x86_64 0:033-535.amzn2.1.6
  iproute.x86_64 0:5.10.0-2.amzn2.0.2
  kernel-tools.x86_64 0:5.10.112-108.499.amzn2
  libcurl.x86_64 0:7.79.1-2.amzn2.0.1
  libgcc.x86_64 0:7.3.1-15.amzn2
  libgomp.x86_64 0:7.3.1-15.amzn2
  libstdc++.x86_64 0:7.3.1-15.amzn2
  libtiff.x86_64 0:4.0.3-35.amzn2.0.2
  microcode_ctl.x86_64 2:2.1-47.amzn2.0.12
  openldap.x86_64 0:2.4.44-23.amzn2.0.4
  openssl.x86_64 1:1.0.2k-24.amzn2.0.3
  openssl-libs.x86_64 1:1.0.2k-24.amzn2.0.3
  python.x86_64 0:2.7.18-1.amzn2.0.5
  python-devel.x86_64 0:2.7.18-1.amzn2.0.5
  python-libs.x86_64 0:2.7.18-1.amzn2.0.5
  systemd.x86_64 0:219-78.amzn2.0.18
  systemd-libs.x86_64 0:219-78.amzn2.0.18
  systemd-sysv.x86_64 0:219-78.amzn2.0.18
  vim-common.x86_64 2:8.2.4857-1.amzn2.0.1
  vim-data.noarch 2:8.2.4857-1.amzn2.0.1
  vim-enhanced.x86_64 2:8.2.4857-1.amzn2.0.1
  vim-filesystem.noarch 2:8.2.4857-1.amzn2.0.1
  vim-minimal.x86_64 2:8.2.4857-1.amzn2.0.1

Complete!
```

Step 37: Install Apache http server

```
[ec2-user@ip-172-31-16-22 ~]$ sudo yum install httpd -y;
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
--> Package httpd.x86_64 0:2.4.53-1.amzn2 will be installed
--> Processing Dependency: httpd-tools = 2.4.53-1.amzn2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: httpd filesystem = 2.4.53-1.amzn2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: system-logos-httpd for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: mod_http2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: httpd filesystem for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.53-1.amzn2.x86_64
```

```
Installed:
  httpd.x86_64 0:2.4.53-1.amzn2

Dependency Installed:
  apr.x86_64 0:1.7.0-9.amzn2          apr-util.x86_64 0:1.6.1-5.amzn2.0.2
  apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2  generic-logos-httpd.noarch 0:18.0.0-4.amzn2
  httpd filesystem.noarch 0:2.4.53-1.amzn2  httpd-tools.x86_64 0:2.4.53-1.amzn2
  mailcap.noarch 0:2.1.41-2.amzn2          mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
```

```
ec2-user@ip-172-31-16-22-
[ec2-user@ip-172-31-16-22 ~]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
[ec2-user@ip-172-31-16-22 ~]$ sudo service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-06-08 07:20:39 UTC; 13s ago
     Docs: man:httpd.service(8)
  Main PID: 10440 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    CGroup: /system.slice/httpd.service
            └─10440 /usr/sbin/httpd -DFOREGROUND
              └─10441 /usr/sbin/httpd -DFOREGROUND
                └─10442 /usr/sbin/httpd -DFOREGROUND
                  └─10443 /usr/sbin/httpd -DFOREGROUND
                    └─10444 /usr/sbin/httpd -DFOREGROUND
                      └─10445 /usr/sbin/httpd -DFOREGROUND

Jun 08 07:20:39 ip-172-31-16-22.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Jun 08 07:20:39 ip-172-31-16-22.ec2.internal systemd[1]: Started The Apache HTTP Server.
[ec2-user@ip-172-31-16-22 ~]$ sudo chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
```

Step 38: Now go back to EC2 Security Groups and Click Edit inbound rules

EC2 > Security Groups > sg-Offb8110891861383 - launch-wizard-2

sg-Offb8110891861383 - launch-wizard-2

Details

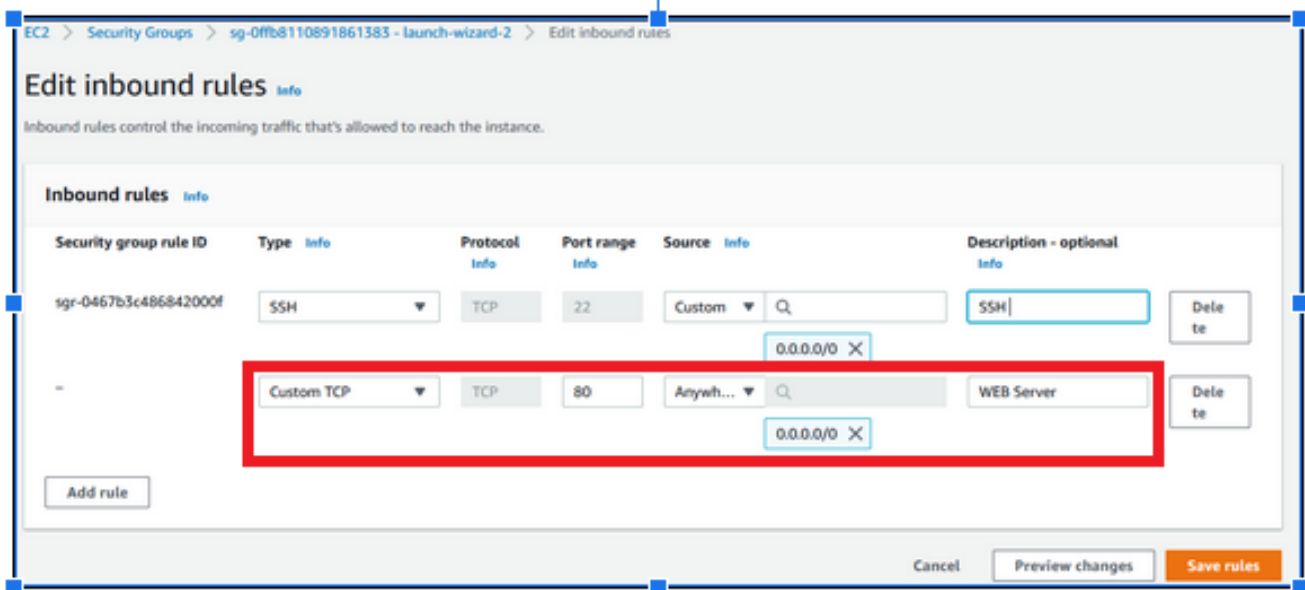
Security group name launch-wizard-2	Security group ID sg-Offb8110891861383	Description launch-wizard created 2022-06-08T07:01:39.176Z	VPC ID vpc-96d840eb
Owner 010004579712	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (1/1)

Manage tags | **Edit inbound rules**

Step 39: Add 80 port as custom TCP protocol



EC2 > Security Groups > sg-0ffb8110891861383 - launch-wizard-2 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

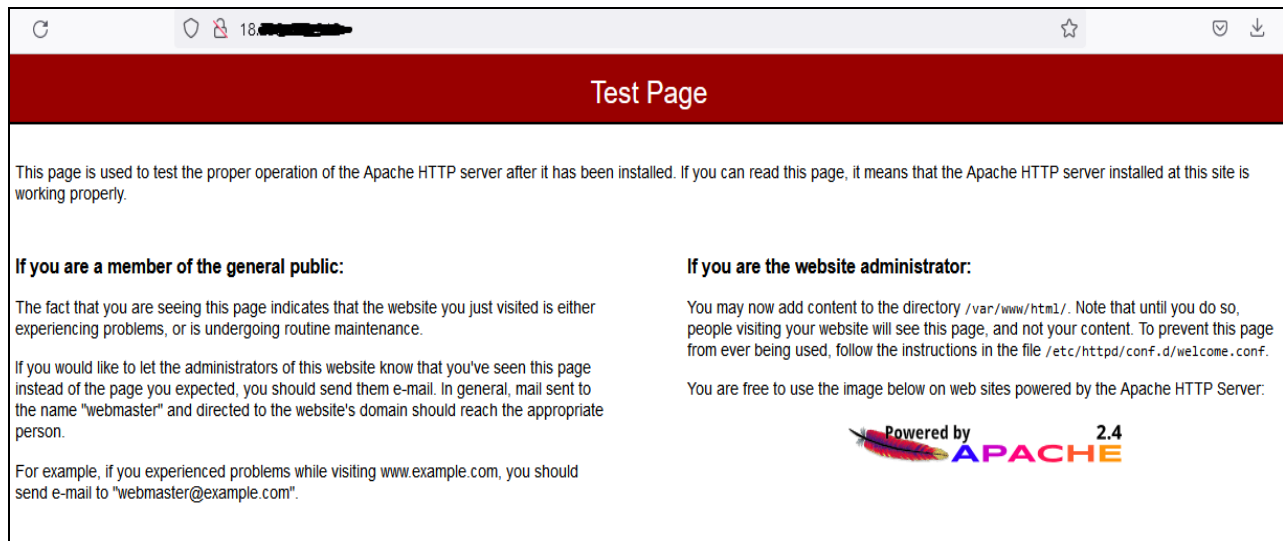
Inbound rules Info

Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
sg-0467b3c486842000f	SSH	TCP	22	Custom	SSH	Delete
-	Custom TCP	TCP	80	Anywh...	WEB Server	Delete

Add rule

Cancel Preview changes Save rules

Step 40: Access the web server using Public IP



18.██████████

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".

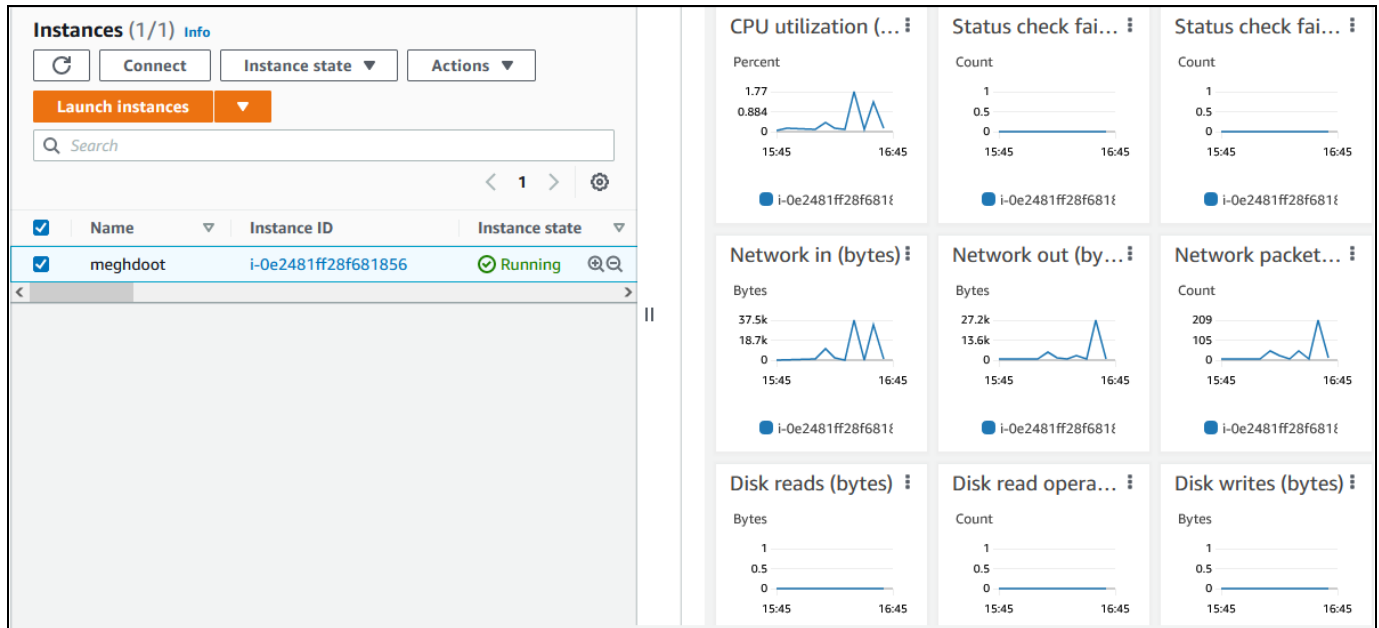
If you are the website administrator:

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`.

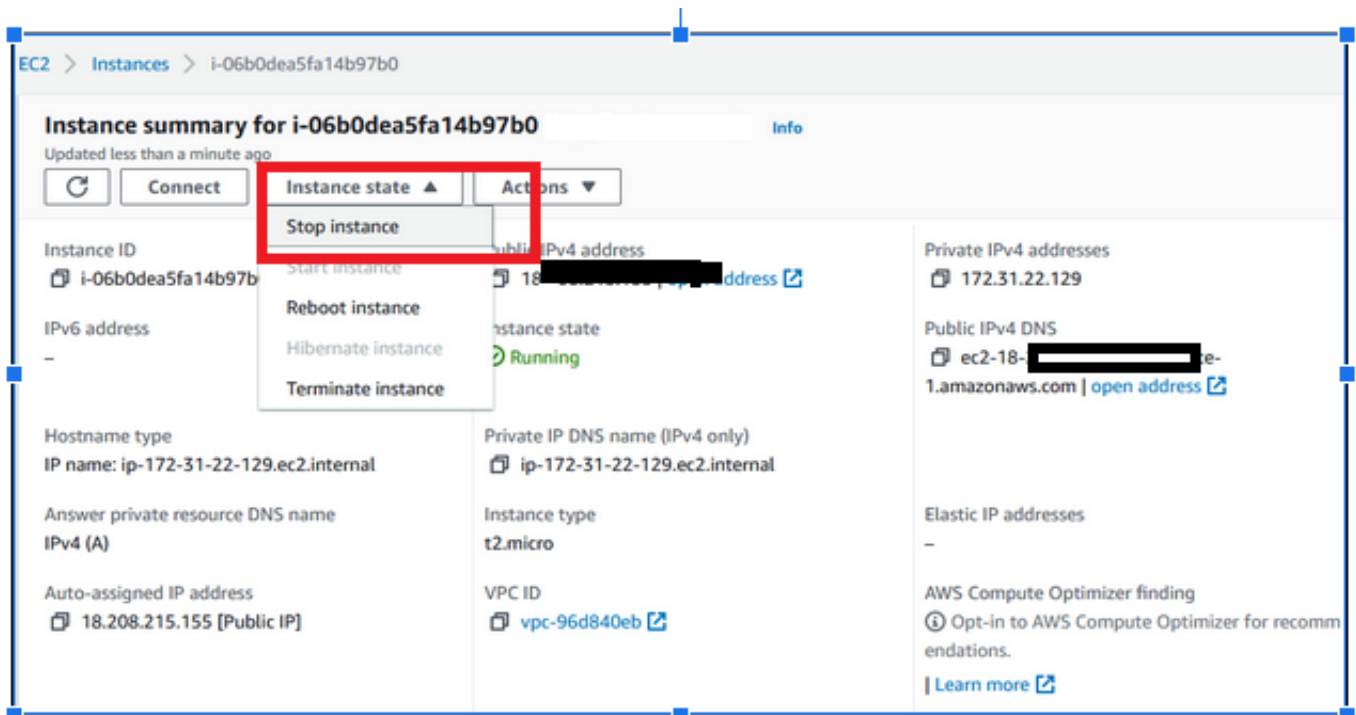
You are free to use the image below on web sites powered by the Apache HTTP Server:

Powered by **APACHE** 2.4

Step 41: EC2 instance Monitoring



Step 42: To Stop/Terminate an instance



The screenshot shows the 'Instance summary' page for EC2 instance 'i-06b0dea5fa14b97b0'. The instance is in a 'Running' state. The 'Instance state' dropdown menu is open, highlighting the 'Stop instance' option. The summary page includes the following details:

- Instance ID:** i-06b0dea5fa14b97b0
- Public IPv4 address:** 18.208.215.155
- Private IPv4 addresses:** 172.31.22.129
- Public IPv4 DNS:** ec2-18-208-215-155.compute-1.amazonaws.com
- Private IP DNS name (IPv4 only):** ip-172-31-22-129.ec2.internal
- Instance type:** t2.micro
- VPC ID:** vpc-96d840eb
- Auto-assigned IP address:** 18.208.215.155 [Public IP]

Launch Windows Instances

Step 43 : Select Launch instance and assign a name to the instance and select Windows AMI(free tier eligible)

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

[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

Recents

My AMIs

Quick Start

Amazon Linux

aws

Ubuntu

ubuntu[®]

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Quickstart AMIs (19)
Commonly used AMIs

My AMIs (0)
Created by me

AWS Marketplace AMIs (968)
AWS & trusted third-party AMIs

Community AMIs (500)
Published by anyone

Refine results

☐ Free tier only Info

▼ OS category

☐ All Linux/Unix
 ☐ All Windows

▼ Architecture

☐ 64-bit (Arm)
 ☐ 32-bit (x86)
 ☐ 64-bit (x86)
 ☐ 64-bit (Mac)

windows (19 filtered, 19 unfiltered)

< 1 >

<div>Microsoft</div> <div>Windows</div> <div>Free tier eligible</div>	Microsoft Windows Server 2019 Base ami-041306c411c38a789 (64-bit (x86)) Microsoft Windows 2019 Datacenter edition. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<input type="button" value="Select"/>
<div>Microsoft</div> <div>Windows</div> <div>Free tier eligible</div>	Microsoft Windows Server 2019 Base with Containers ami-08bcca76f90fdddc4 (64-bit (x86)) Microsoft Windows 2019 Datacenter edition with Containers. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<input type="button" value="Select"/>
<div>Microsoft</div> <div>Windows</div>	Microsoft Windows Server 2019 with SQL Server 2017 Standard ami-05025ffb60d04baf2 (64-bit (x86)) Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2017 Standard. [English] Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes	<input type="button" value="Select"/>

Step 44 : Confirmation to the changes of the existing policy of Security Groups and Volumes

Some of your current settings will be changed or removed if you proceed

Changing your AMI will result in some of your current settings being overridden. You will require permission for your changes to succeed. [Find out more.](#)

Changes

- Your security group rules will be overridden.

▼ Volumes details

The difference from your previous volume configuration will be as follows:

Show custom volumes that will be deleted and volumes that can't... ▼

Cancel
Confirm Changes

Step 45: Select the VPC, subnet and Security Groups (new or existing .pem file)

▼ Network settings
Edit

Network

vpc-96d840eb

Subnet

No preference (Default subnet in any availability zone)

Auto-assign public IP

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-4' with the following rules:

☒ Allow RDP 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

Step 46: Connect to the Windows Instance and select the RDP client

Instances (1/3) [Info](#)

Search

	Name	Instance ID	Instance state	Instance type	Status check	Alarm
<input type="checkbox"/>	meghdoot	i-0e2481ff28f681856	Running	t2.micro	2/2 checks passed	No alarm
<input checked="" type="checkbox"/>	Windows	i-056e1d6244a556470	Running	t2.micro	2/2 checks passed	No alarm
<input type="checkbox"/>	Windows	i-0f27d484cc8cae12f	Terminated	t2.micro	-	No alarm

Actions

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

Launch instances

Public IPv4

ec2-3-229-2

ec2-34-239

-


EC2 > Instances > i-056e1d6244a556470 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-056e1d6244a556470 (Windows) using any of these options

Session Manager | **RDP client** | EC2 serial console

Instance ID


 i-056e1d6244a556470 (Windows)

Connection Type

☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.

☐ **Connect using Fleet Manager**
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

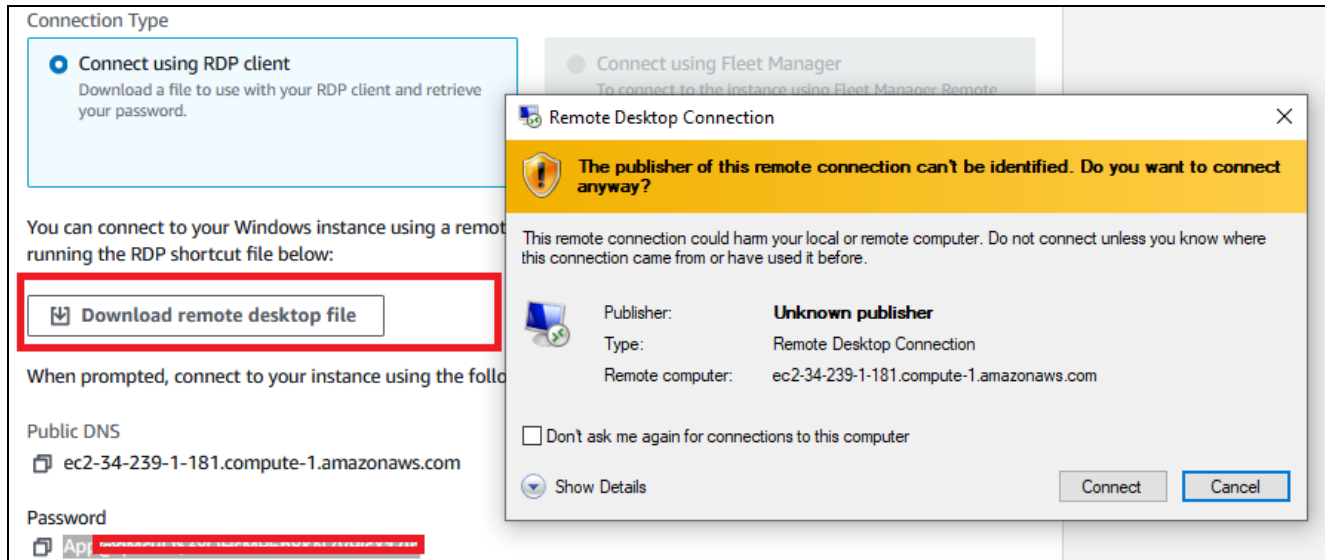
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

 **Download remote desktop file**

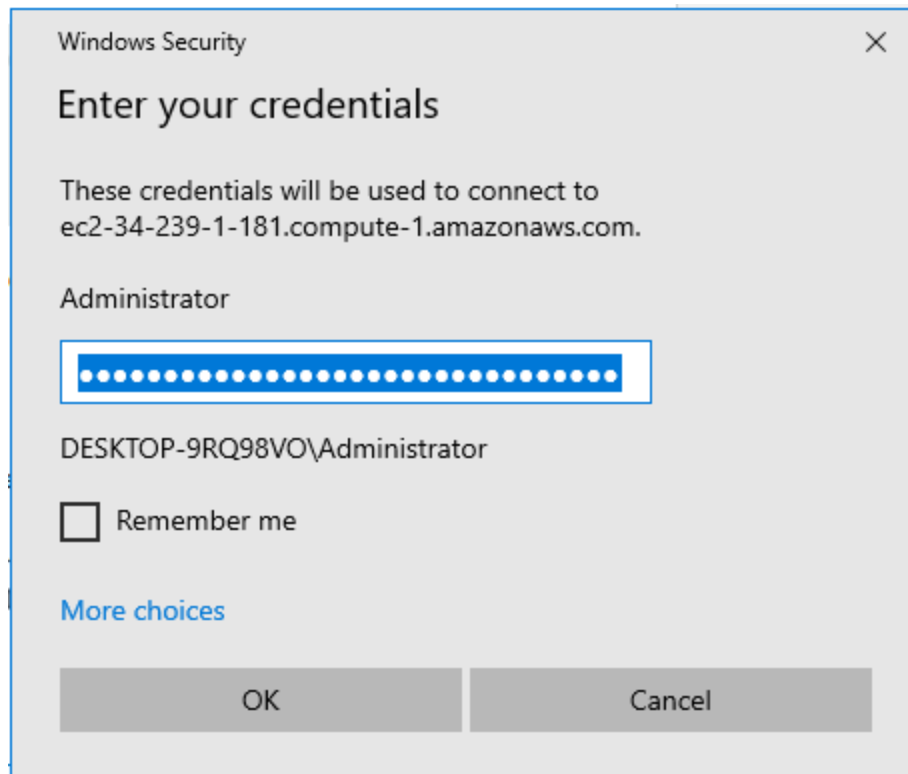
When prompted, connect to your instance using the following details:

App@ [REDACTED]

Step 49: Click Download remote desktop file and Windows.rdp client file would be downloaded. Click on the Windows.rdp file



Step 50 : Enter the password which is copied from the previous step



Finally, the Windows instance is accessible

