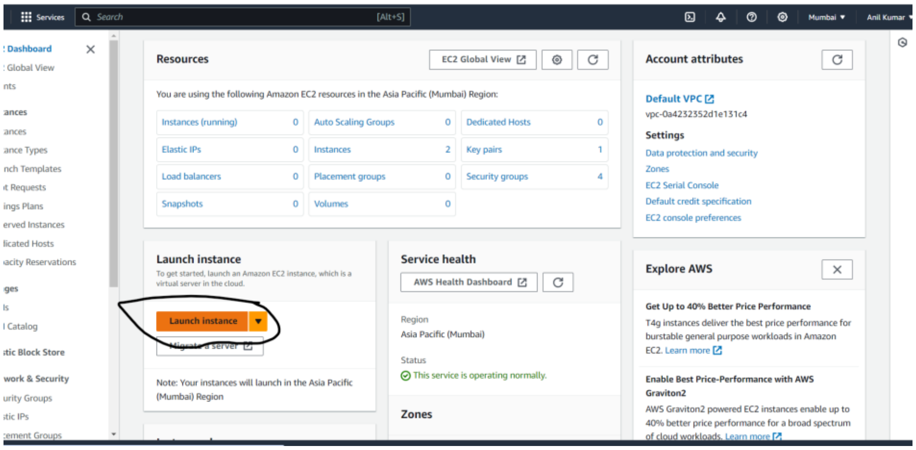
1. L1 - Demonstrate the AWS EC2 Ubuntu Instance Creation steps and connect to EC2 Instance using Mobaxterm/putty agent
Ans:- Steps to create EC2 instance are

First of all login the aws console.

Step1:- Type EC2- in search box of console of accunt and then click on launch ec2



You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	2	Key pairs	1
Load balancers	0	Placement groups	0	Security groups	4
Snapshots	0	Volumes	0		

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Region
Asia Pacific (Mumbai)

Status
This service is operating normally.

Default VPC
vpc-0a4232352d1e131c4

Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences

Get Up to 40% Better Price Performance
T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more

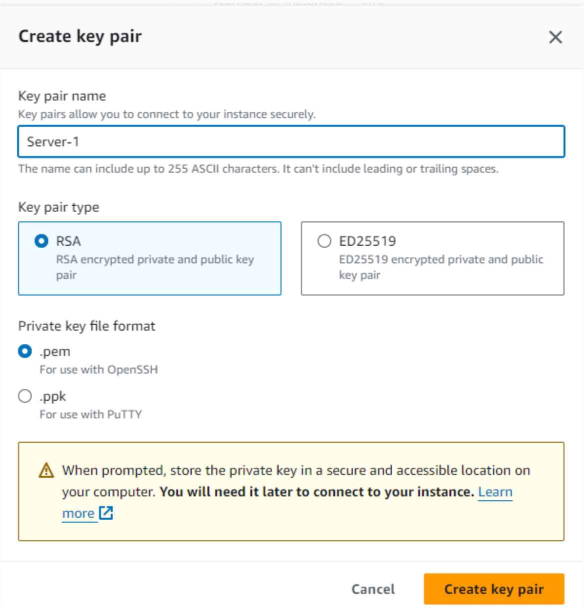
Enable Best Price-Performance with AWS Graviton2
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Configure the server specification

Server Name =Server1 → Application and OS Images (Amazon Machine Image)= Ubuntu server 2023 free tier → instance type = T2 micro

Key pair (login)

reate new key pair→ Key pair name=server-1 → Key pair type=RSA → .pem → Create new keypair



Key pair name
Key pairs allow you to connect to your instance securely.
Server-1
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

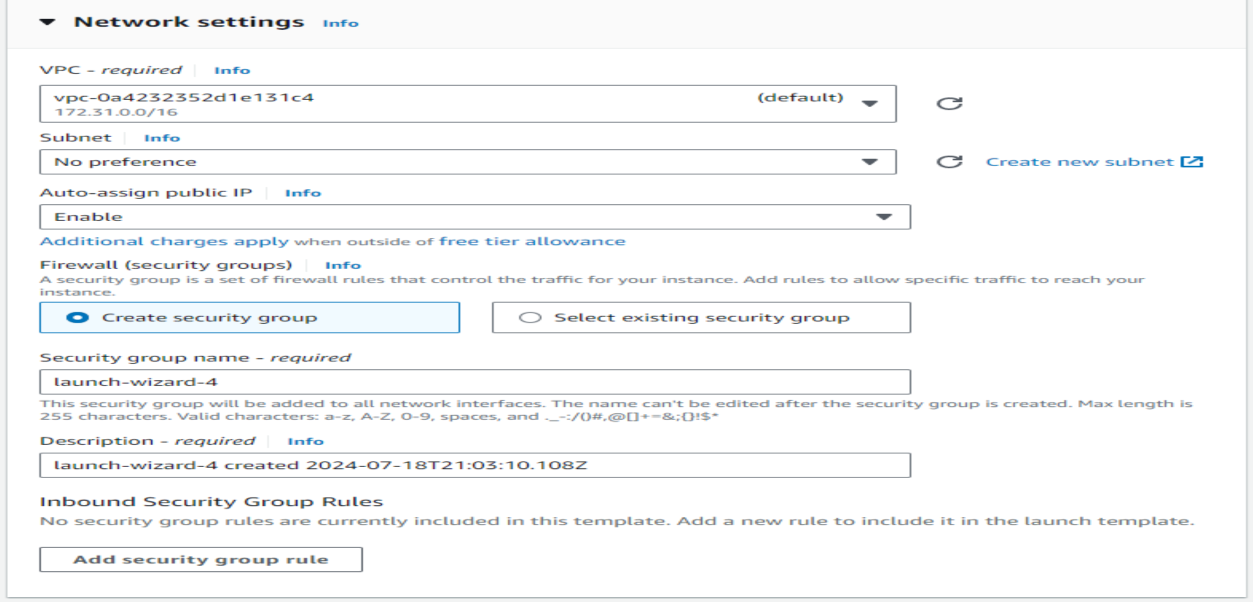
Key pair type
● RSA
RSA encrypted private and public key pair
○ ED25519
ED25519 encrypted private and public key pair

Private key file format
● .pem
For use with OpenSSH
○ .ppk
For use with PuTTY

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

Network settings➔

Edit → Auto-assign public IP=Enable→ Firewall (security groups)= Create Security group→ Inbound Security Group Rules=SSH enable



▼ Network settings Info

VPC - *required* | Info

vpc-0a4232352d1e131c4 (default)
172.31.0.0/16

Subnet | Info

No preference

Create new subnet

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

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*

launch-wizard-4

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

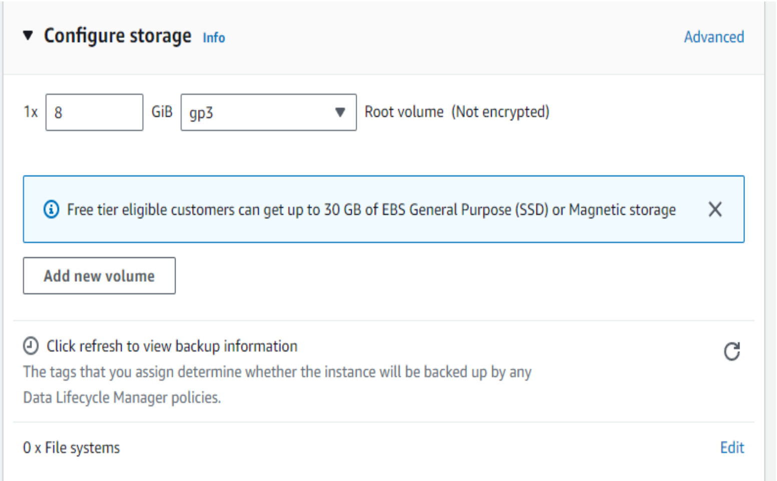
launch-wizard-4 created 2024-07-18T21:03:10.108Z

Inbound Security Group Rules

No security group rules are currently included in this template. Add a new rule to include it in the launch template.

Add security group rule

Configure Storage



▼ Configure storage Info Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information

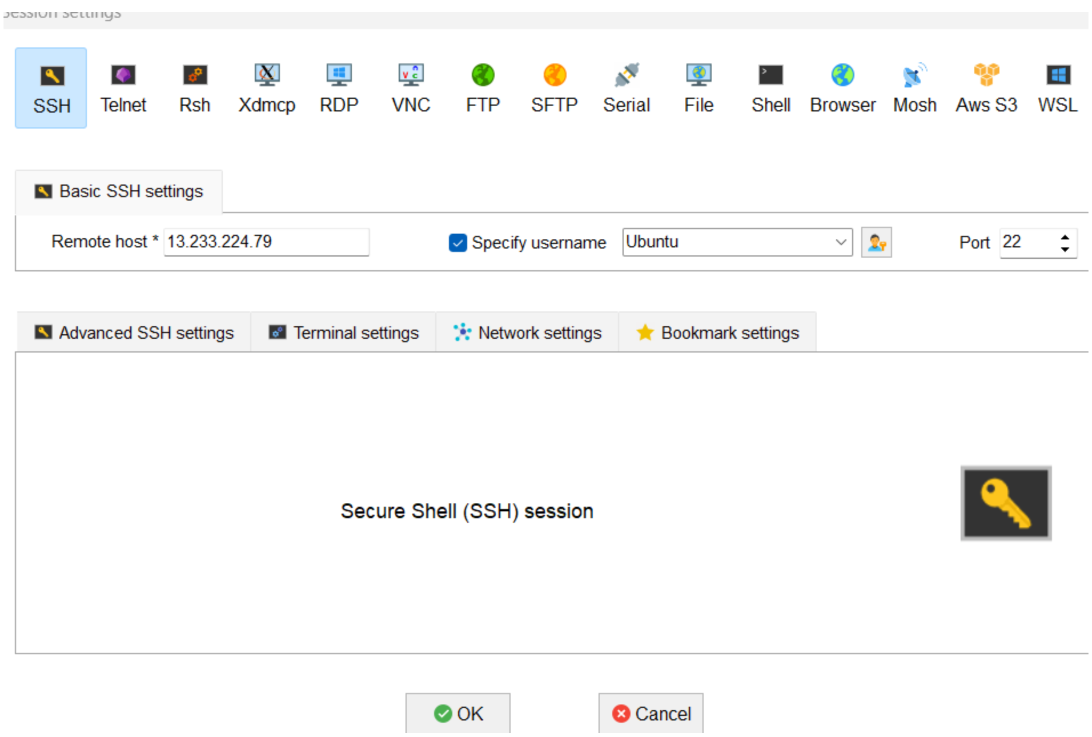
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

Then Launch Instance

Step2 : Connect to mobaxterm

Copy the public ip of instance and open the mobaxterm and click the the SSH



Remote host * 13.233.224.79

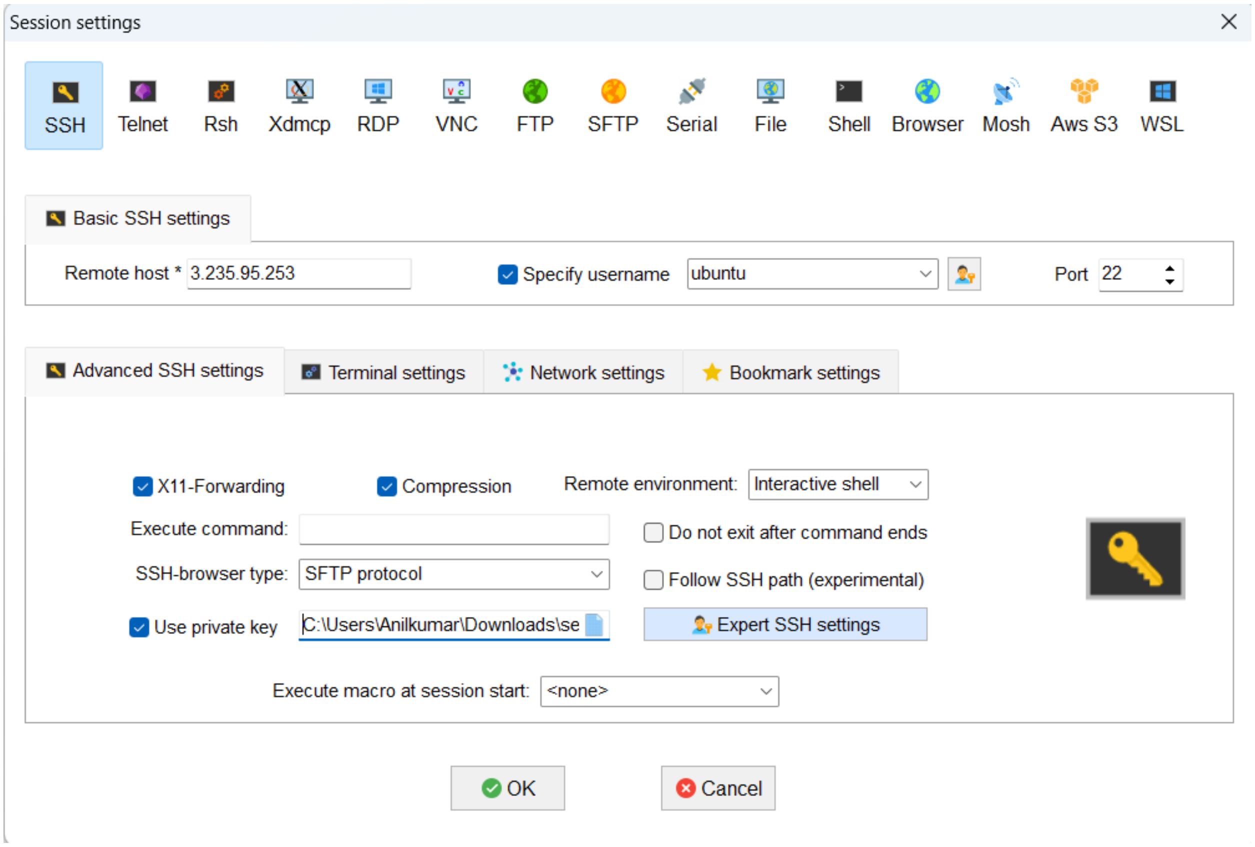
☑ Specify username Ubuntu

Port 22

Secure Shell (SSH) session

Then check on specify username click on box and type = “Ubuntu” →

Advance SSH Setting → check on use private key → select the public key → ok → accept



Remote host * 3.235.95.253

☑ Specify username ubuntu

Port 22

☑ X11-Forwarding

☑ Compression

Remote environment: Interactive shell

Execute command:

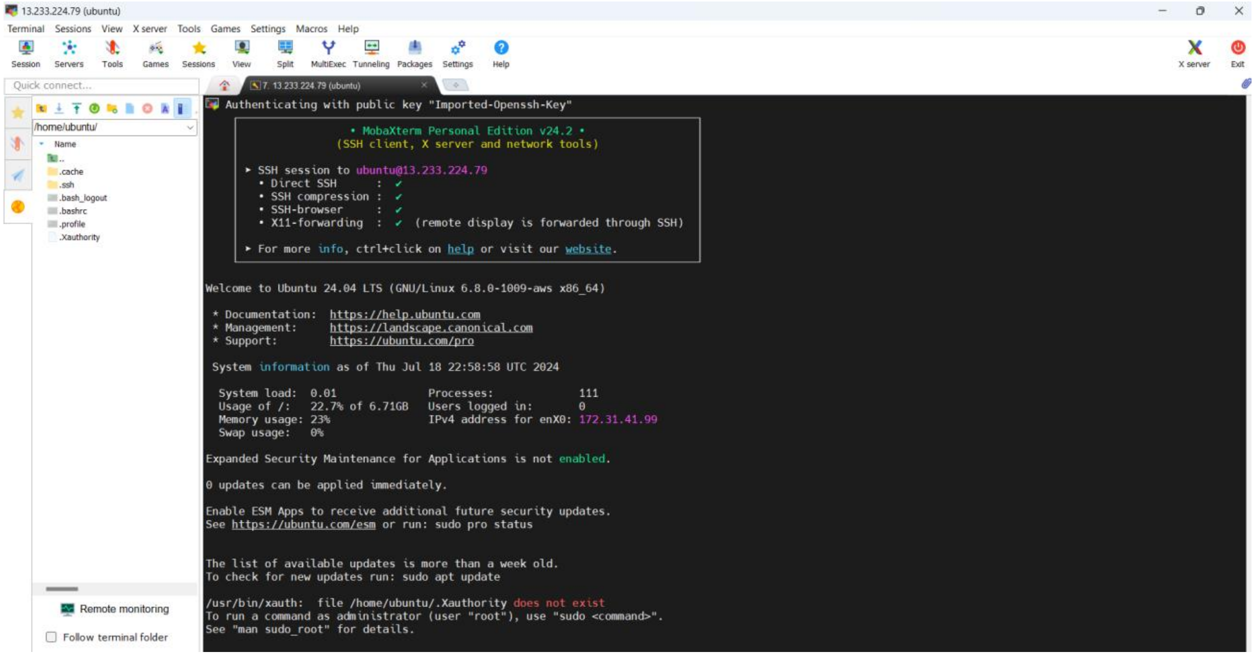
□ Do not exit after command ends

SSH-browser type: SFTP protocol

□ Follow SSH path (experimental)

☑ Use private key C:\Users\Anilkumar\Downloads\se

Execute macro at session start: <none>



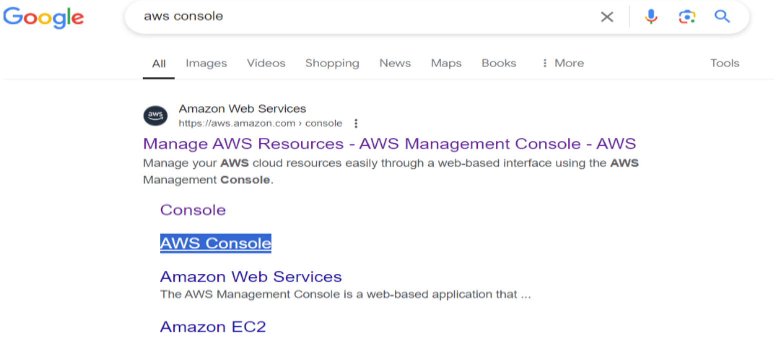
/home/ubuntu/

Name
..
.cache
.ssh
.bash_logout
.bashrc
.profile
.Xauthority

```
Authenticating with public key "Imported-Openssh-Key"

                  • MobaXterm Personal Edition v24.2 •
                (SSH client, X server and network tools)

    ➤ SSH session to ubuntu@13.233.224.79
      • Direct SSH      :  ✓
      • SSH compression :  ✓
      • SSH-browser     :  ✓
      • X11-forwarding  :  ✓  (remote display is forwarded through SSH)

    ➤ For more info, ctrl+click on help or visit our website.

Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

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

 System information as of Thu Jul 18 22:58:58 UTC 2024

  System load:  0.01              Processes:             111
  Usage of /:   22.7% of 6.71GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for enX0: 172.31.41.99
  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

/usr/bin/xauth:  file /home/ubuntu/.Xauthority does not exist
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

2. L2 - Login to AWS Console and Create IAM User, Role, and Group

Ans-first of all open chrome browser and search AWS console and click on it.



Amazon Web Services
https://aws.amazon.com › console

Manage AWS Resources - AWS Management Console - AWS

Manage your **AWS** cloud resources easily through a web-based interface using the **AWS** Management **Console**.

Console

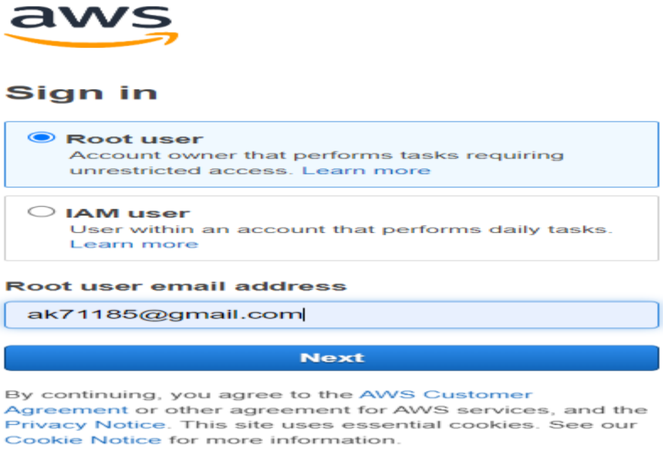
AWS Console

Amazon Web Services

The AWS Management Console is a web-based application that ...

Amazon EC2

Step 1:- Login your credential of AWS account

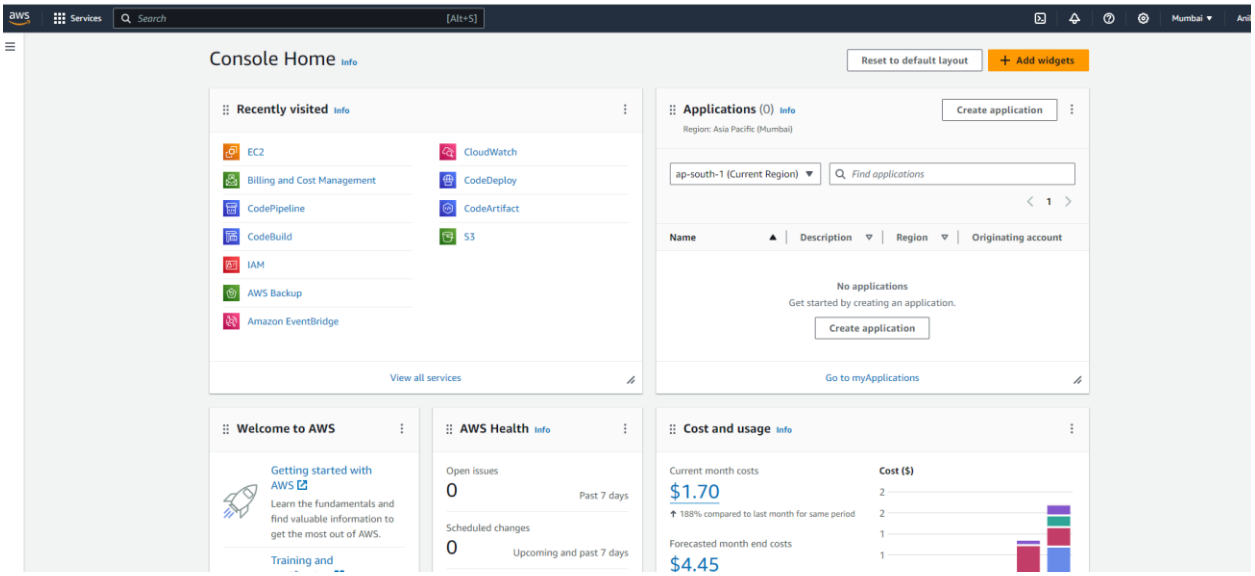


● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address: ak71185@gmail.com

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.



Console Home Info

Reset to default layout | + Add widgets

Recently visited Info

- EC2
- Billing and Cost Management
- CodePipeline
- CodeBuild
- IAM
- AWS Backup
- Amazon EventBridge
- CloudWatch
- CodeDeploy
- CodeArtifact
- S3

View all services

Applications (0) Info

Region: Asia Pacific (Mumbai)

Create application

ap-south-1 (Current Region) ▾ | Find applications

Name ▲	Description ▽	Region ▽	Originating account

No applications

Get started by creating an application.

Create application

Go to myApplications

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and

AWS Health Info

Open issues

0 Past 7 days

Scheduled changes

0 Upcoming and past 7 days

Cost and usage Info

Current month costs

$1.70

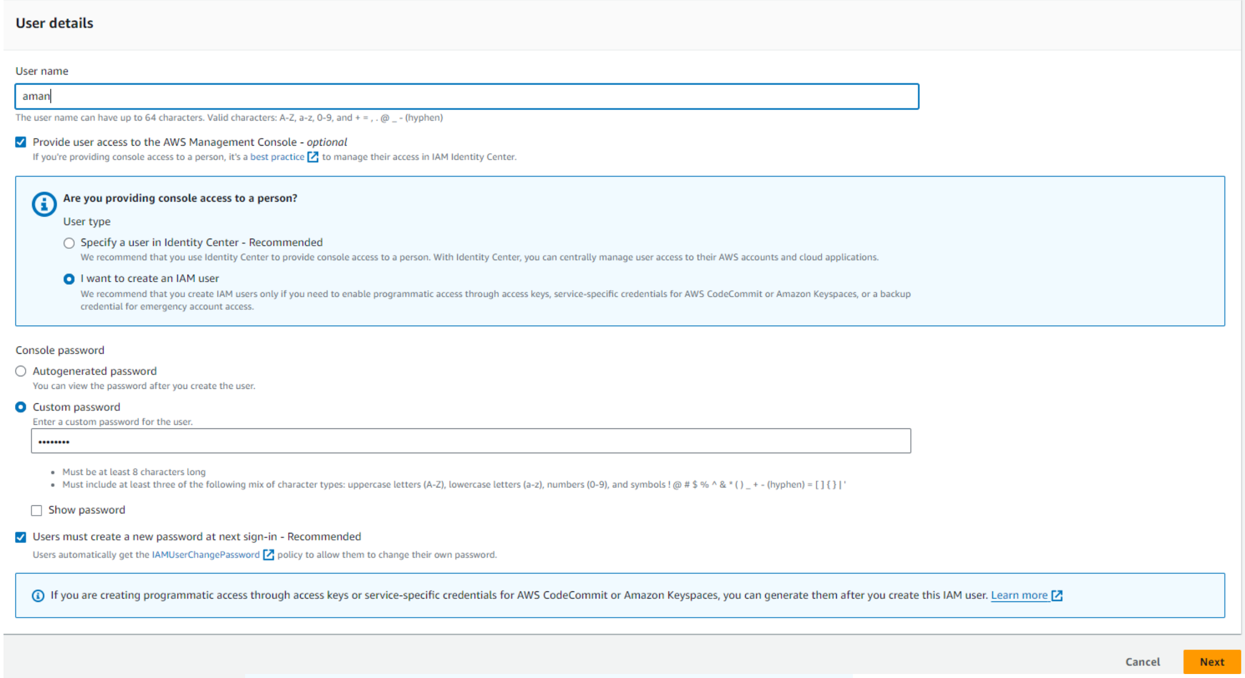
↑ 188% compared to last month for same period

Forecasted month end costs

$4.45

Step 2:- IAM User creation

Type IAM in Search box → click on IAM → Access management → click on user → Create User → User name = Aman → click on check box **Provide user access to the AWS Management Console -** ***optional*** → click on **I want to create an IAM user** → Console password → Custom password = xxxxxx → next



User details

User name

aman

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password

You can view the password after you create the user.

● Custom password

Enter a custom password for the user.

••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

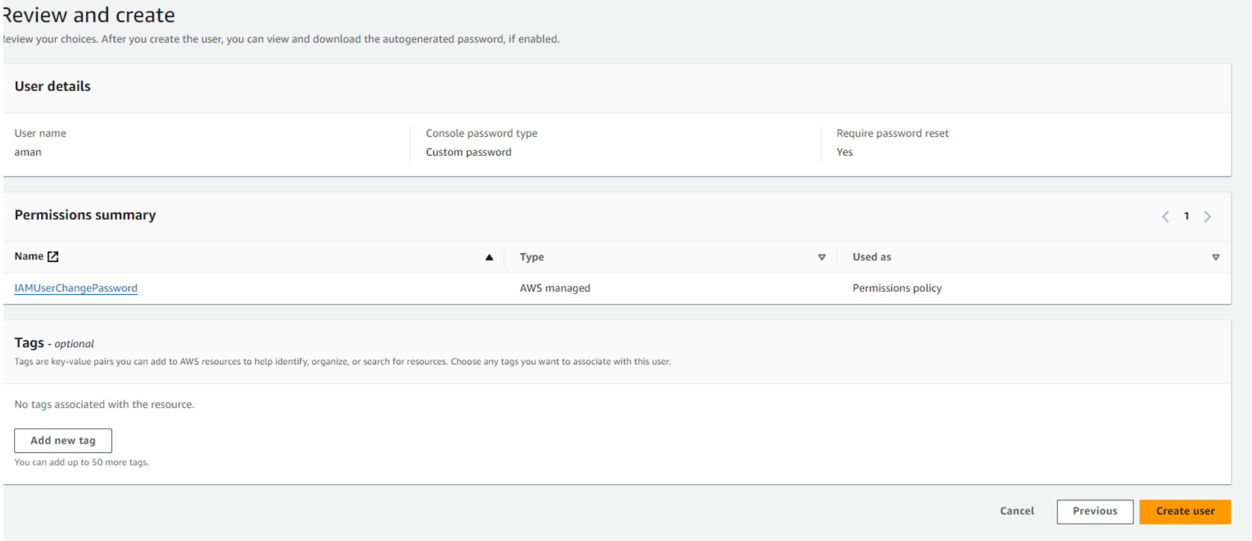
□ Show password

☑ Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Set permissions → Add user to group→ Next → click on create user



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
aman	Custom password	Yes

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - *optional*

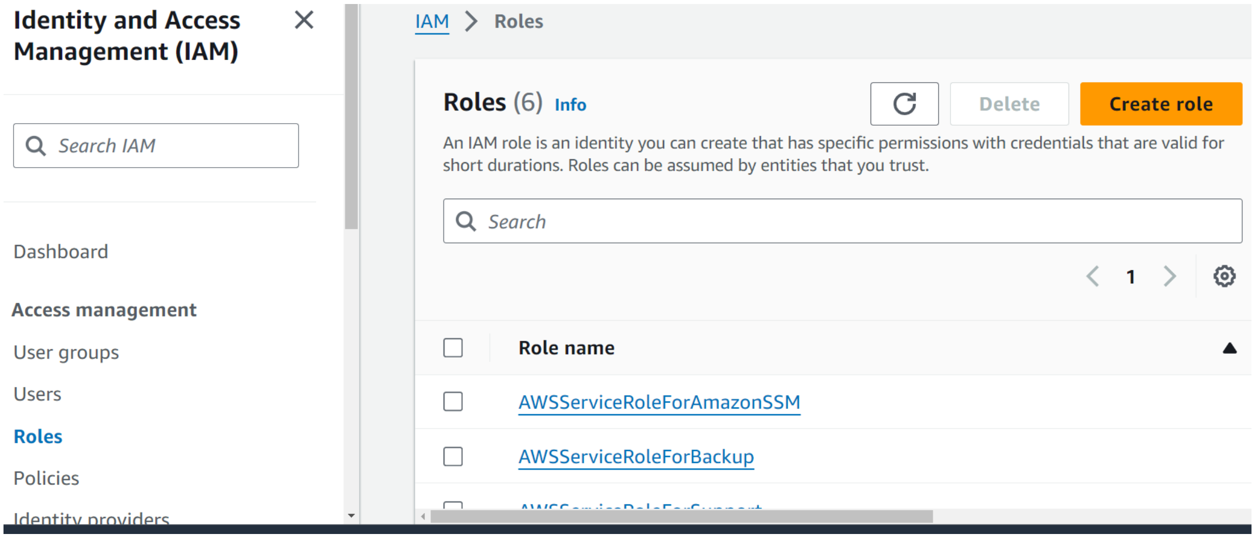
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.

Step 3:- Role creation

Type IAM in Search box → click on IAM → Access management → click on Roles

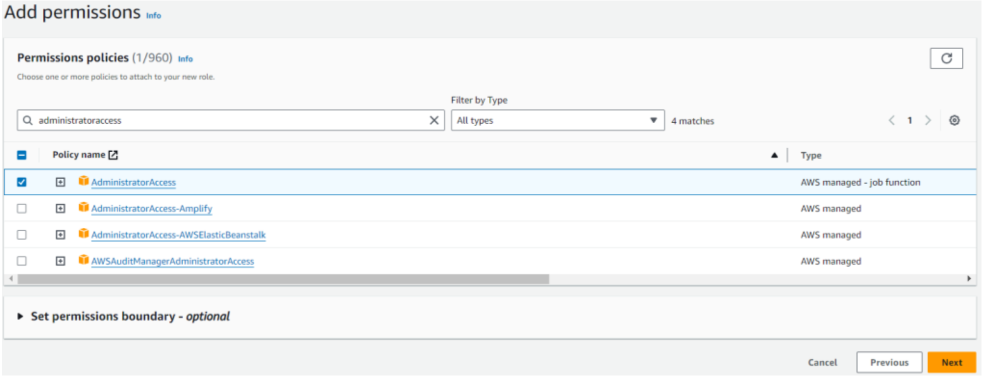


Roles (6) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name
AWSServiceRoleForAmazonSSM
AWSServiceRoleForBackup
AWSServiceRoleForSupport

Trusted entity type = AWS Services → Service or use case = EC2→ Next → Add permissions= Adminstrator access → Next



Add permissions Info

Permissions policies (1/960) Info

Choose one or more policies to attach to your new role.

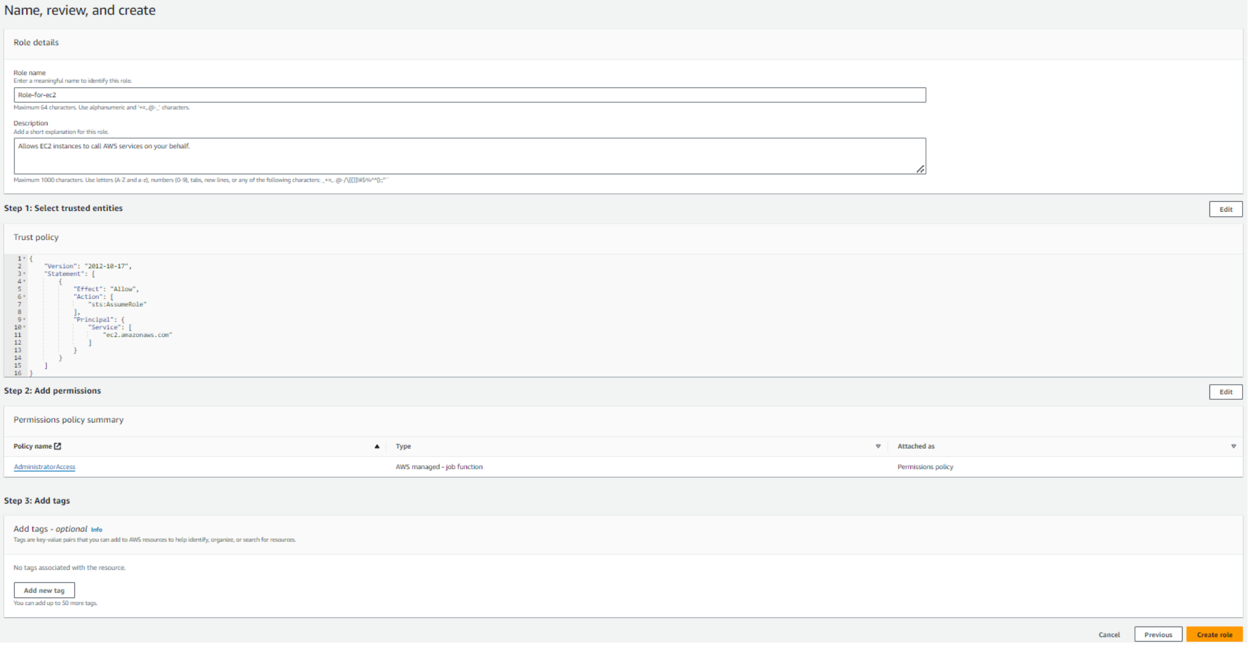
Search: administratoraccess

Filter by Type: All types

4 matches

	Policy name	Type
☑	AdministratorAccess	AWS managed - job function
□	AdministratorAccess-Amplify	AWS managed
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed
□	AWSAuditManagerAdministratorAccess	AWS managed

Role name= Role-for-ec2 → Create Role



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
Role-for-ec2
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,.@-/\[{]}!#$%^*();"'`

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AdministratorAccess	AWS managed - job function	Permissions policy

Step 3: Add tags

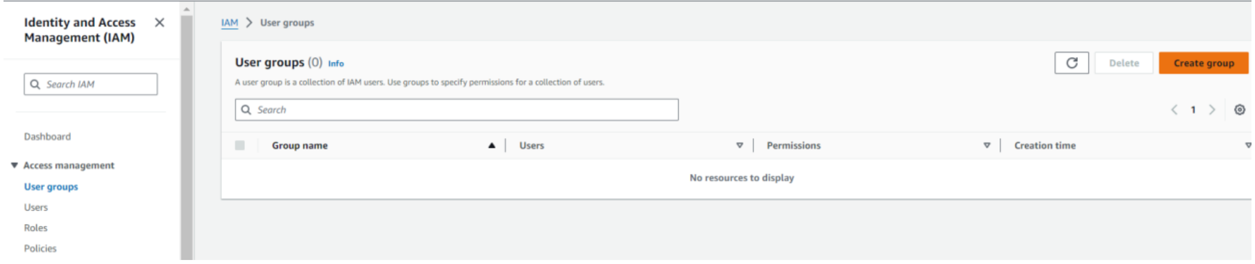
Add tags - *optional* Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Step 4:- Group creation

Type IAM in Search box → click on IAM → Access management → click on User Groups →Click on Create Group →

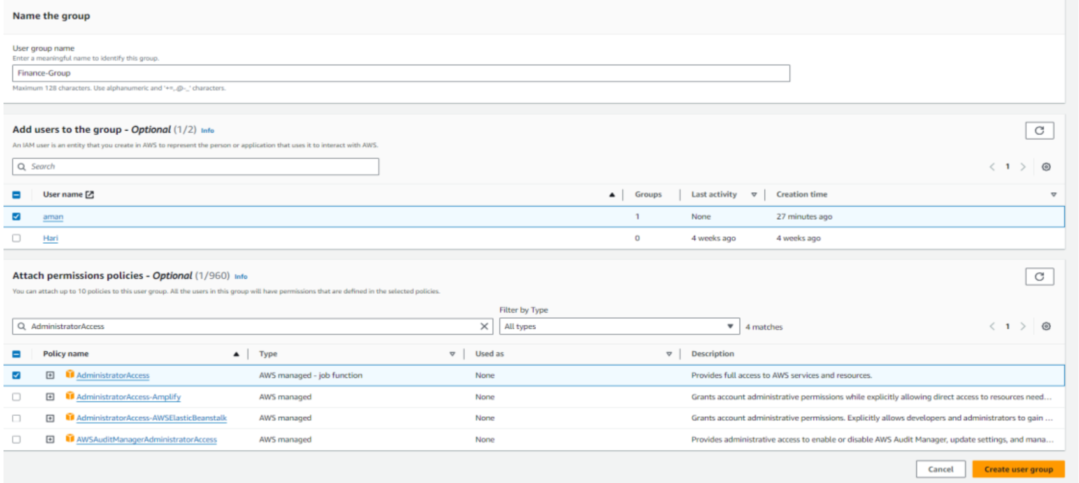


User groups (0) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time

No resources to display

Name the group = Finance-Group → Add users to the group → check on finance group user to add on finance group → Attach permissions policies → administrator access → click on create user and group



Name the group

User group name
Enter a meaningful name to identify this group.
Finance-Group
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1/2) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

	User name	Groups	Last activity	Creation time
☑	aman	1	None	27 minutes ago
□	Hari	0	4 weeks ago	4 weeks ago

Attach permissions policies - *Optional* (1/960) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

AdministratorAccess
Filter by Type: All types
4 matches

	Policy name	Type	Used as	Description
☑	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services and resources.
□	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources need…
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to gain …
□	AWSAuditManagerAdministratorAccess	AWS managed	None	Provides administrative access to enable or disable AWS Audit Manager, update settings, and mana…