Identity and Access Management (IAM) ✕

✓ **User created successfully**
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

🔍 Search IAM

Dashboard

▼ **Access management**

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ **Access reports**

Access analyzer

IAM dashboard

Security recommendations 2

🔄

⚠️ **Add MFA for root user**
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

✓ **Root user has no active access keys**
Using access keys attached to an IAM user instead of the root user improves security.

⚠️ **Update your access permissions for AWS Billing, Cost Management, and Account consoles**
We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: aws-portal:ViewBilling, aws-portal:ModifyBilling, aws-portal:ViewAccount, aws-portal:ModifyAccount, aws-portal:ViewPaymentMethods, aws-portal:ModifyPaymentMethods, aws-portal:ViewUsage, purchase-orders:ViewPurchaseOrders, and purchase-orders:ModifyPurchaseOrders. To ensure you

View affected policies

✓ Engineers user group created.

View group ✕

IAM ⟩ User groups

User groups (2) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

🔄 Delete **Create group**

🔍 Filter User groups by property or group name and press enter

‹ 1 › ⚙️

	Group name	Users	Permissions	Creation time
☐	Developer	1	✓ Defined	8 minutes ago
☐	Engineers	⚠️ 0	✓ Defined	Now

⦙⦙⦙ Services 🔍 Search

FAIR=57 🖥️ ⌃ ? Global ▼ Subhi Pande

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name

prachi

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?**

○ 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.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more 🗗

Permissions options

⦿ Add user to group	◯ Copy permissions	◯ Attach policies directly
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.	Copy all group memberships, attached managed policies, and inline policies from an existing user.	Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/2)   ↻   Create group

🔍 Search groups   ‹ 1 › ⚙

☐	Group name 🗗 ▲	Users ▽	Attached policies 🗗 ▽	Created ▽
☐	Developer	1	AmazonEC2FullAccess	2023-03-09 (9 minutes a...

⊘ **User created successfully** | View user | ✕
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users > **Create user**

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details | Email sign-in instructions 🗗 |

Console sign-in URL
🗐 https://839626613242.signin.aws.amazon.com/console

User name
🗐 prachi

Console password
🗐 ************** Show

EC2 > Instances > **Launch an instance**

⊘ **Success**
Successfully initiated launch of instance (i-00882d314e1ce3f71)

▶ Launch log

Next Steps

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

| Create billing alerts 🗗 |

Connect to your instance

Once your instance is running, log into it from your local computer.
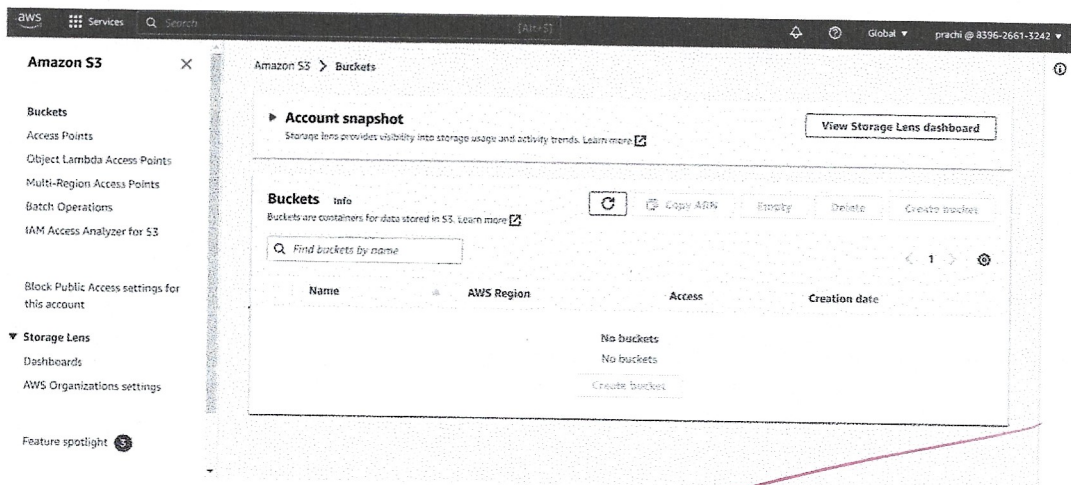
| Connect to instance 🗗 |

Learn more 🗗

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

| Connect an RDS database 🗗 |

Create a new RDS database 🗗

28

Amazon S3 ✕

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens
Dashboards
AWS Organizations settings

Feature spotlight ③

Amazon S3 > Buckets

▶ **Account snapshot**
Storage Lens provides visibility into storage usage and activity trends. Learn more ↗

View Storage Lens dashboard

Buckets Info
Buckets are containers for data stored in S3. Learn more ↗

[C] Copy ARN Empty Delete Create bucket

🔍 Find buckets by name

< 1 > ⚙

Name	AWS Region	Access	Creation date
	No buckets		
	No buckets		

Create bucket

Pati
16/03/23