IAM TASKS

1) Create one IAM user and assign ec2,s3 full access role.

In the AWS Console, search for and click IAM in the search bar.

1. In the left sidebar, click Users.
2. Click the “Add users” button.

Add User Details

1. User name: Enter a name (e.g., ec2-s3-user).
2. Access type:
    - Check “Programmatic access” if the user needs API/CLI access.
    - Check “AWS Management Console access” if the user will use the web console.

Click Next: Permissions.

Set Permissions

1. Choose “Attach policies directly”.
2. In the search bar, find and check these policies:
    - AmazonEC2FullAccess
    - AmazonS3FullAccess

Click Next: Tags.

Step 5: Add Tags (Optional)

You can add tags like:

- Key: Purpose, Value: EC2 and S3 access

Click Next: Review.

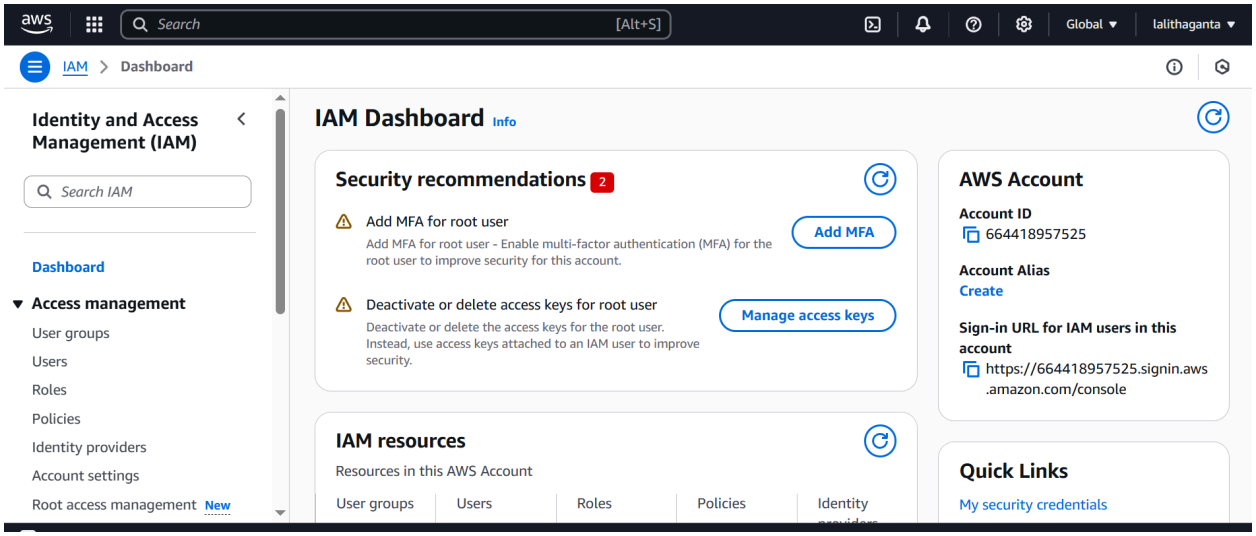
Step 6: Review and Create

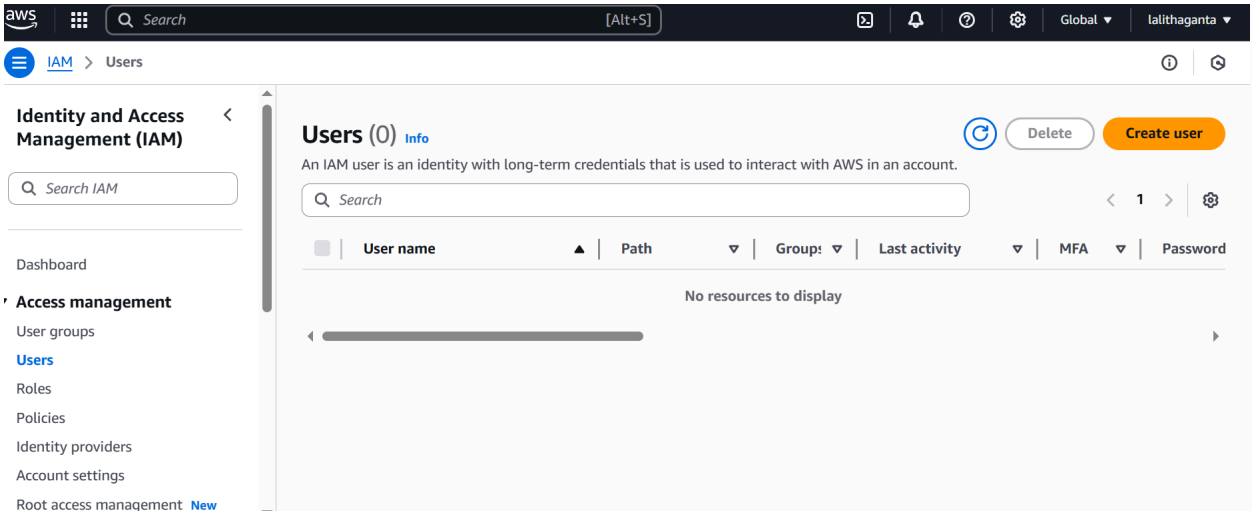
1. Review the user information.
2. Click “Create user”.

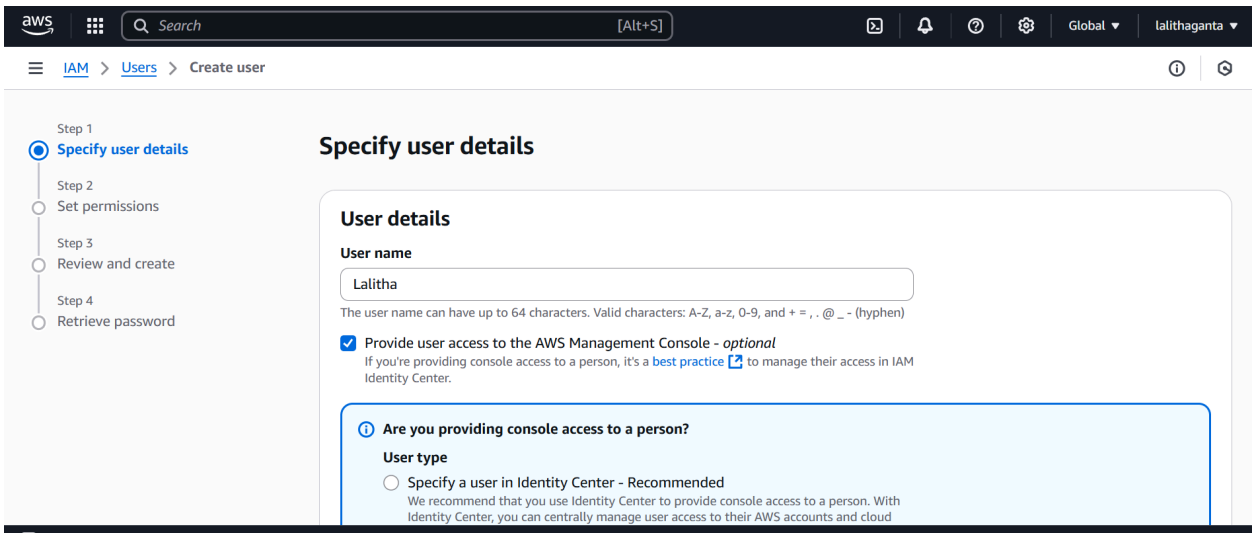
Step 7: Save Credentials

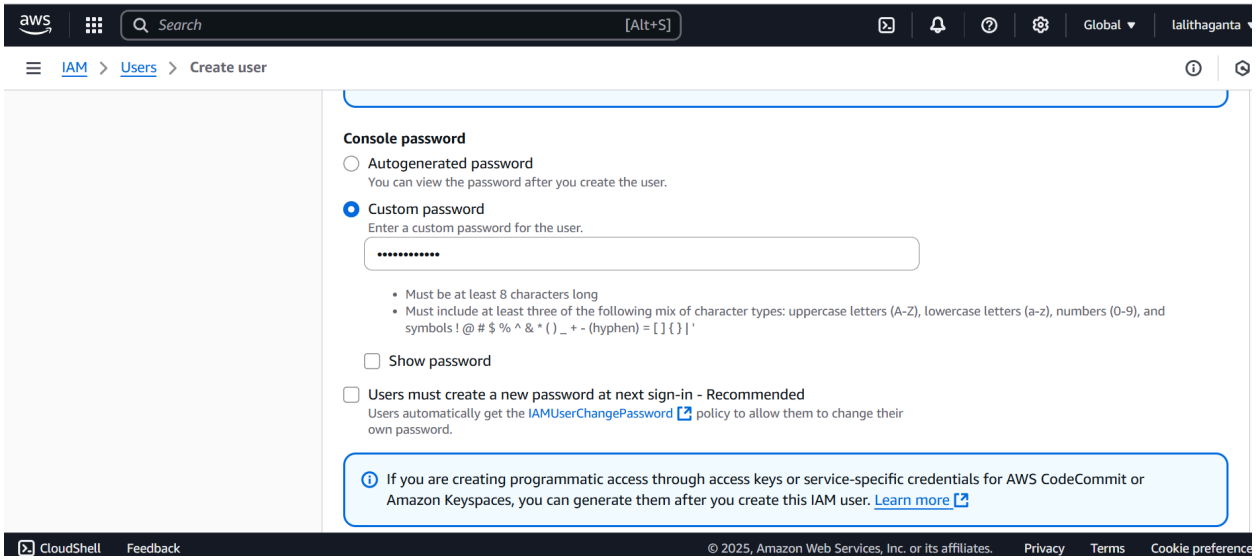
Once the user is created:

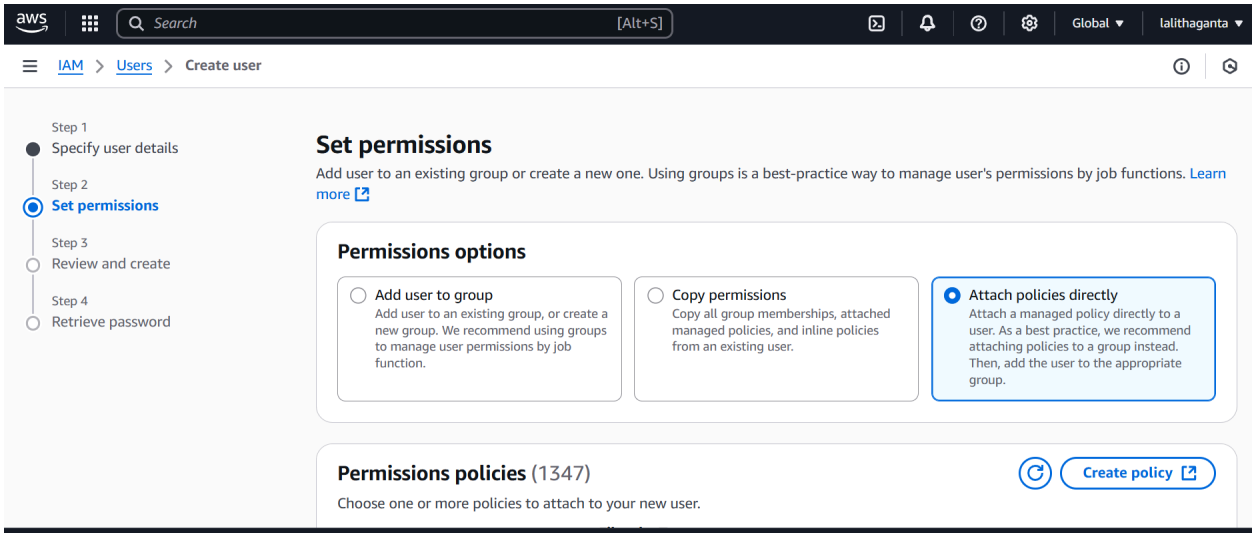
- You’ll see the Access Key ID and Secret Access Key (if you enabled programmatic access).

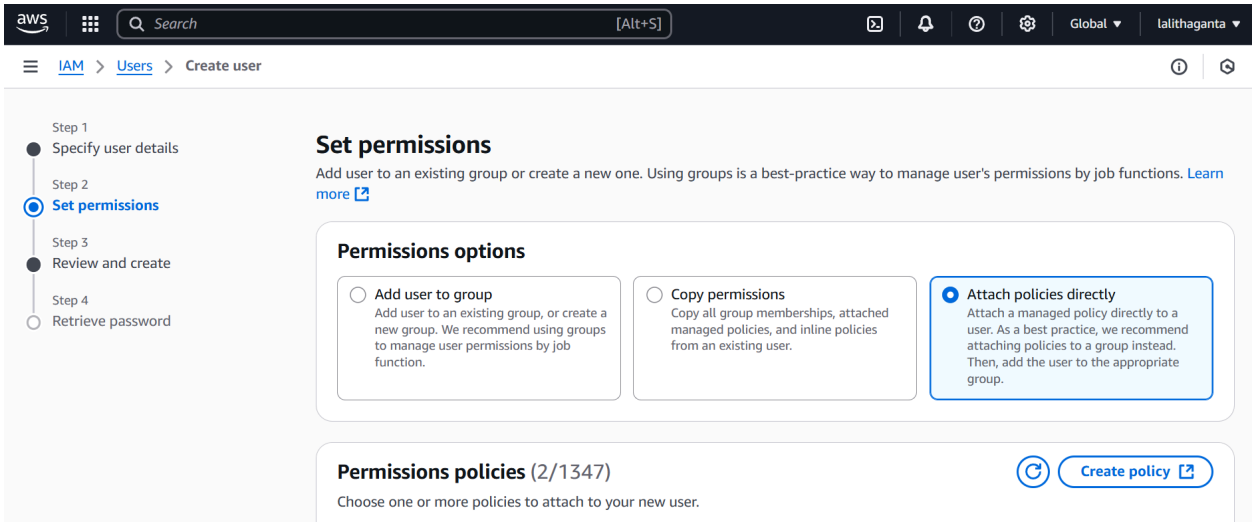

Search [Alt+S]
Global
lalithaganta
IAM > Dashboard
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
IAM Dashboard Info
Security recommendations 2
Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
Add MFA
Deactivate or delete access keys for root user
Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.
Manage access keys
IAM resources
Resources in this AWS Account
User groups
Users
Roles
Policies
Identity
AWS Account
Account ID
664418957525
Account Alias
Create
Sign-in URL for IAM users in this account
https://664418957525.signin.aws.amazon.com/console
Quick Links
My security credentials

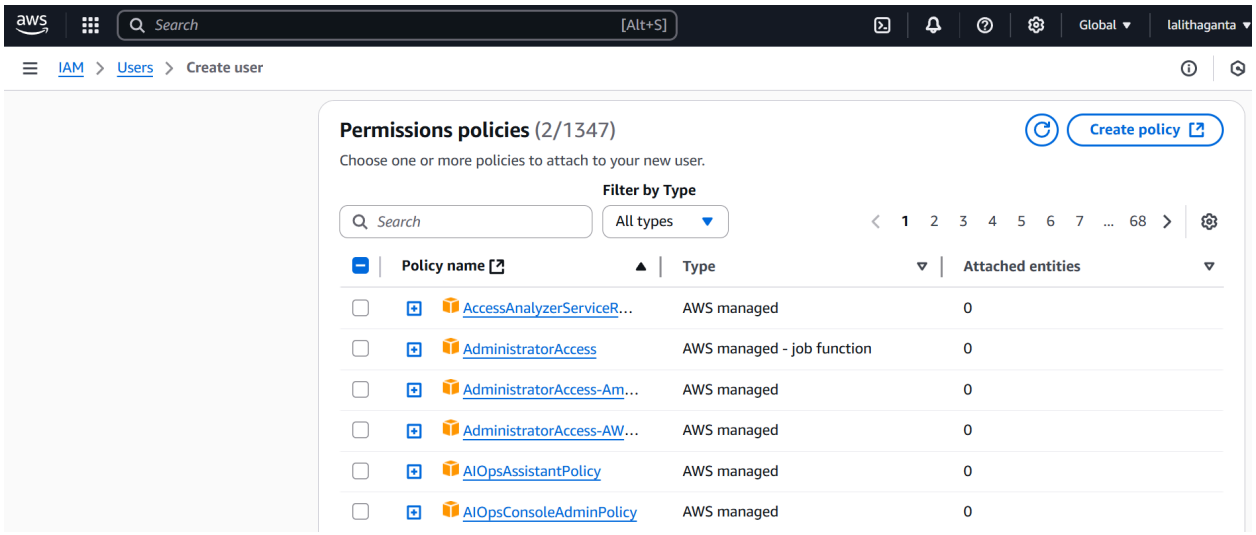

Search [Alt+S]
Global
lalithaganta
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Users (0) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Path
Groups
Last activity
MFA
Password
No resources to display

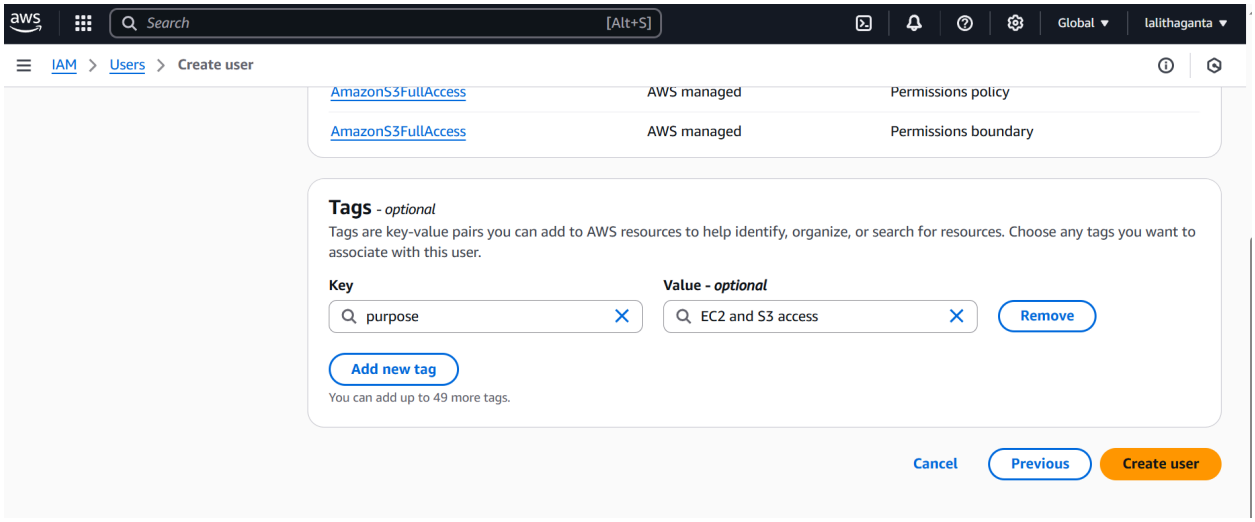

Search [Alt+S]
Global
lalithaganta
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Lalitha
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (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

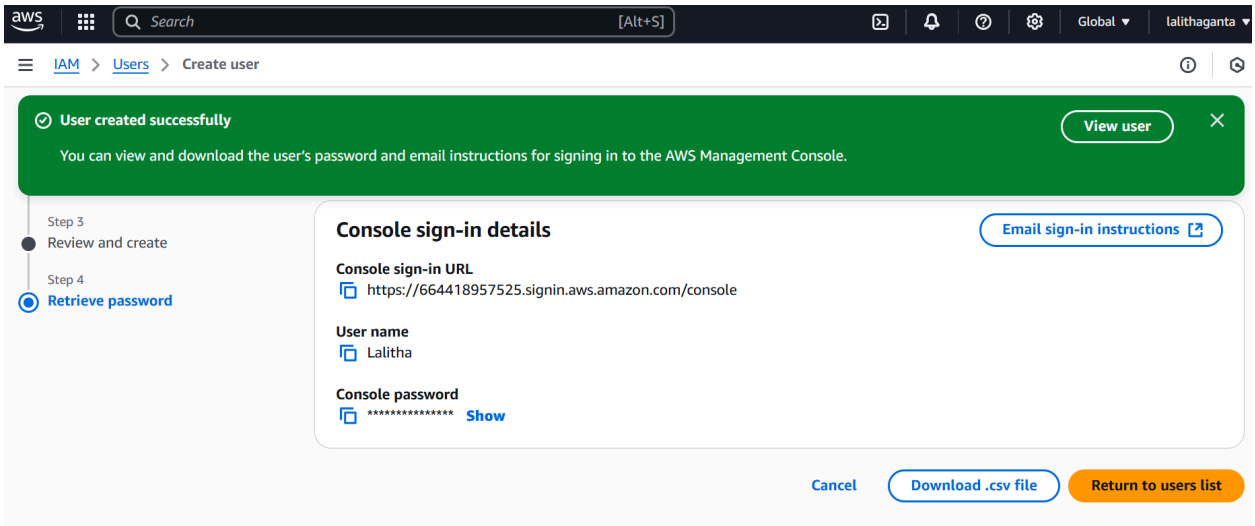

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
••••••••••••
Must be at least 8 characters long
Must include at least three of the following 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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preference

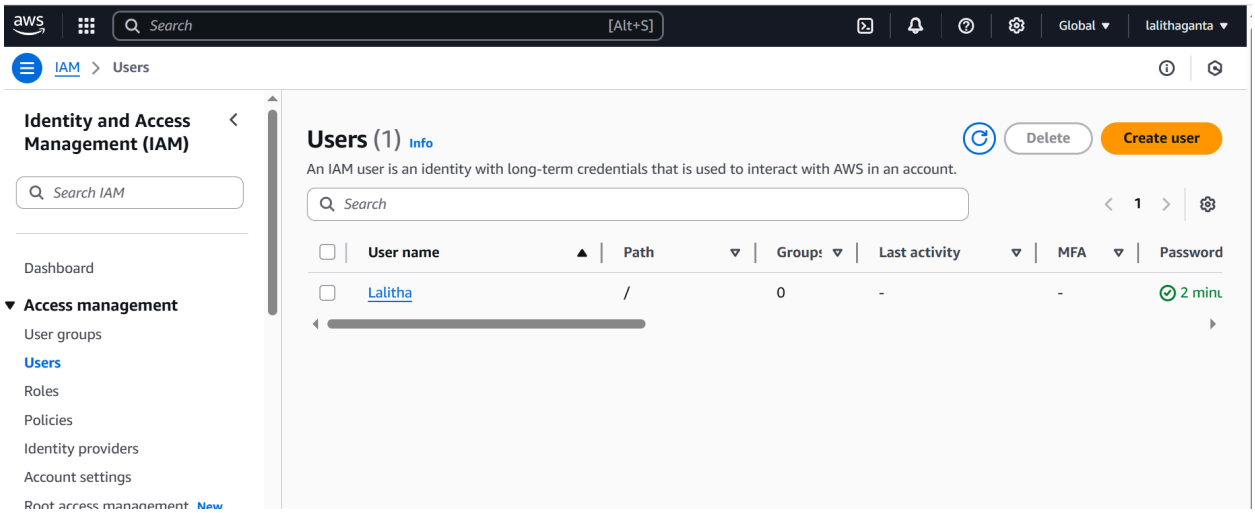

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
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.
Permissions policies (1347)
Create policy
Choose one or more policies to attach to your new user.

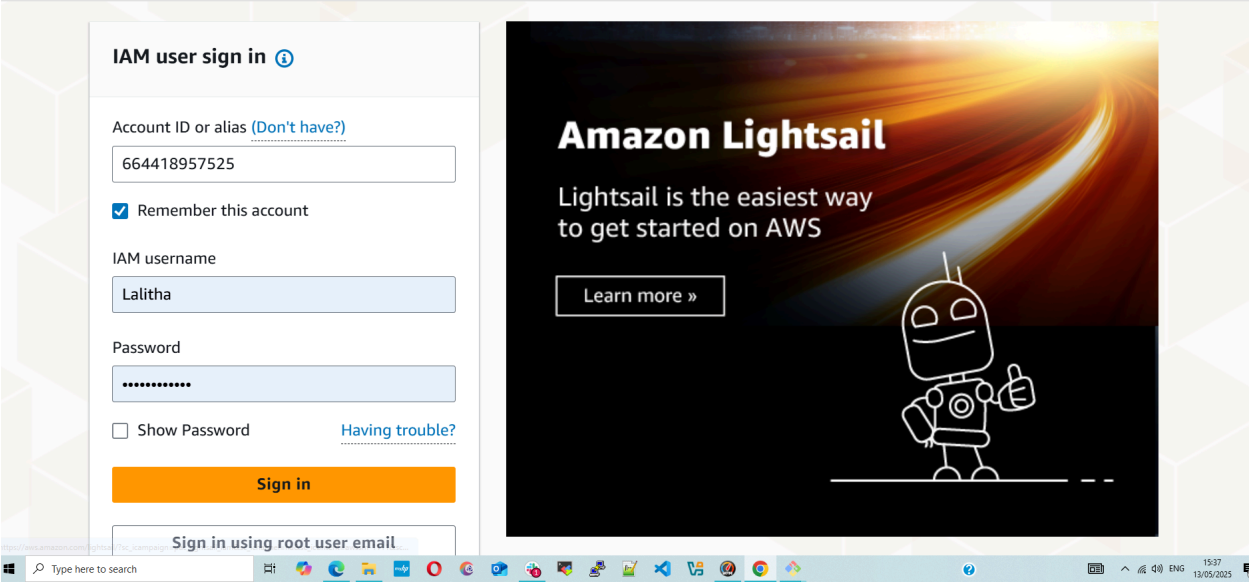

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
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.
Permissions policies (2/1347)
Choose one or more policies to attach to your new user.
Create policy

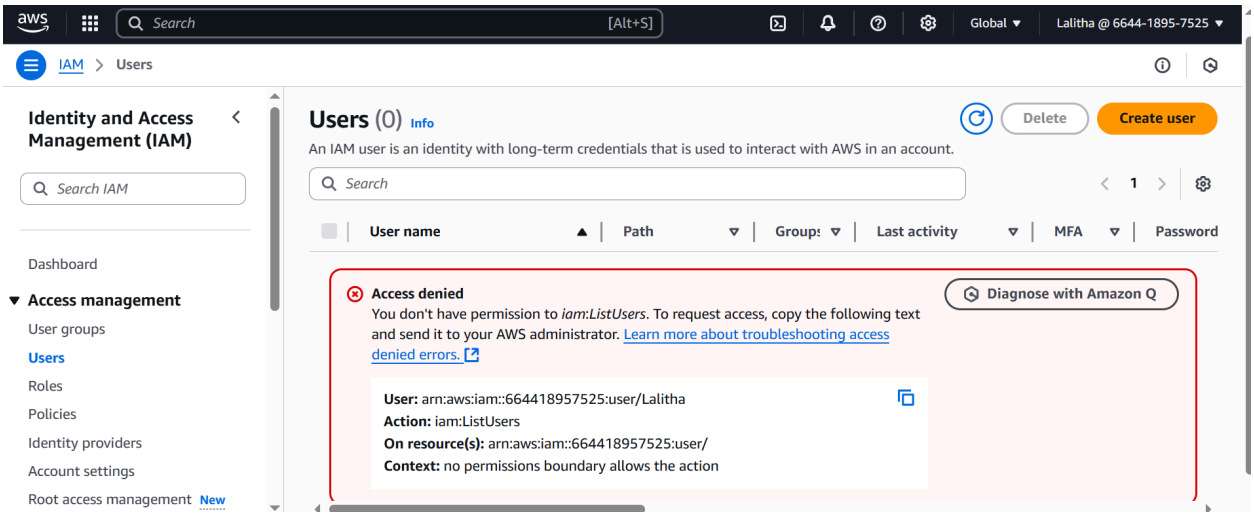

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
Permissions policies (2/1347)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 68
Policy name
Type
Attached entities
AccessAnalyzerServiceR... AWS managed 0
AdministratorAccess AWS managed - job function 0
AdministratorAccess-Am... AWS managed 0
AdministratorAccess-AW... AWS managed 0
AIOpsAssistantPolicy AWS managed 0
AIOpsConsoleAdminPolicy AWS managed 0


Search [Alt+S]
Global
lalithaganta
IAM > Users > Create user
AmazonS3FullAccess AWS managed Permissions policy
AmazonS3FullAccess AWS managed Permissions boundary
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.
Key
Value - optional
purpose
EC2 and S3 access
Remove
Add new tag
You can add up to 49 more tags.
Cancel
Previous
Create user


Search [Alt+S]
Global
lalithaganta
IAM > Users > Create user
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.
Step 3
Review and create
Step 4
Retrieve password
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://664418957525.signin.aws.amazon.com/console
User name
Lalitha
Console password
********** Show
Cancel
Download .csv file
Return to users list


Search [Alt+S]
Global
lalithaganta
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Users (1) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
1
User name
Path
Groups
Last activity
MFA
Password
Lalitha
/
0
-
-
2 minu





2) Create one Group in IAM and Assign Read access for ec2.

Open IAM Service

1. In the top search bar, type “IAM” and open the IAM service.
2. From the left panel, click on “User groups”.
3. Click the “Create group” button.

Set Group Name

1. Enter a group name, such as: EC2ReadOnlyGroup.

Attach Permissions to the Group

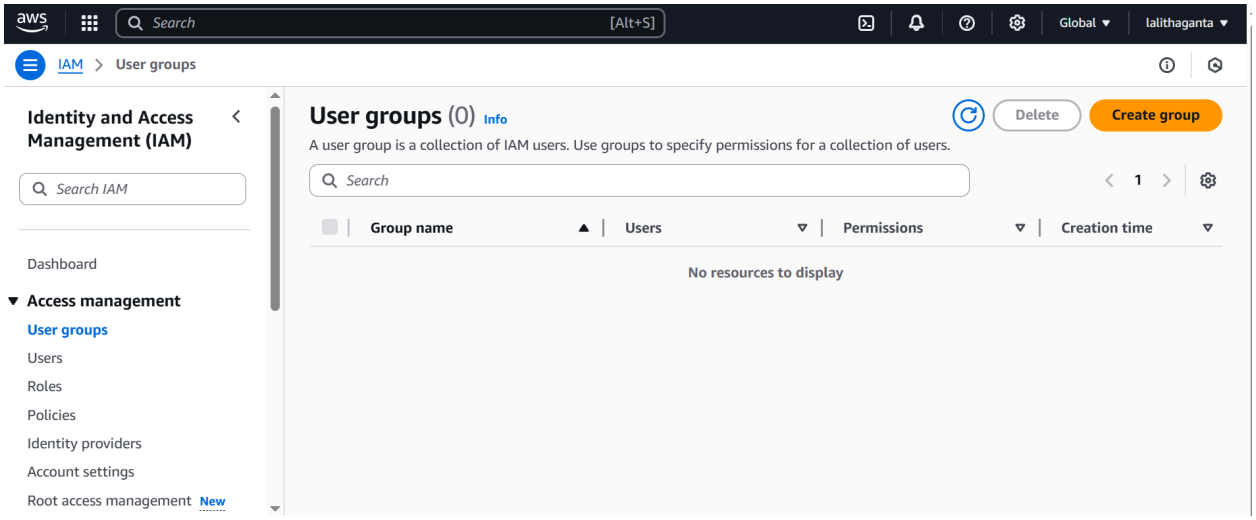
In the permissions policy list, search for:

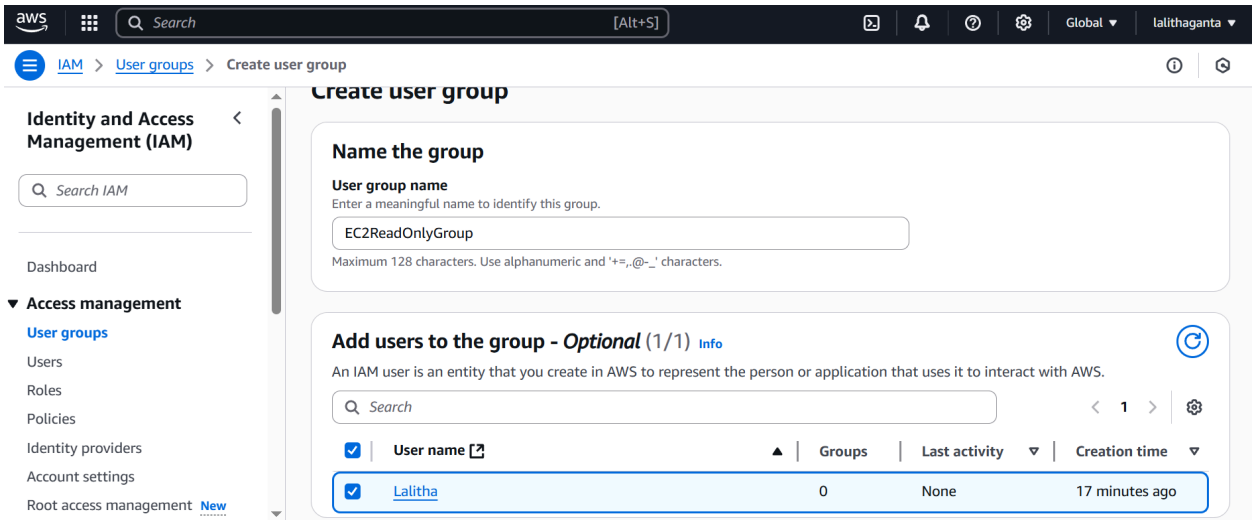
AmazonEC2ReadOnlyAccess

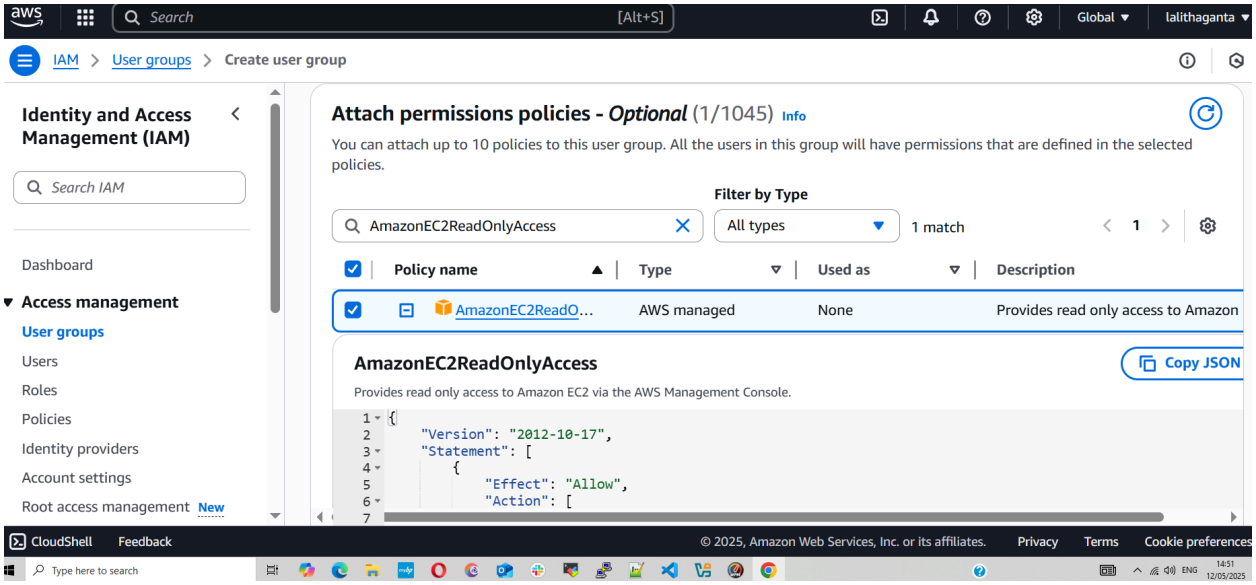
Click Next.

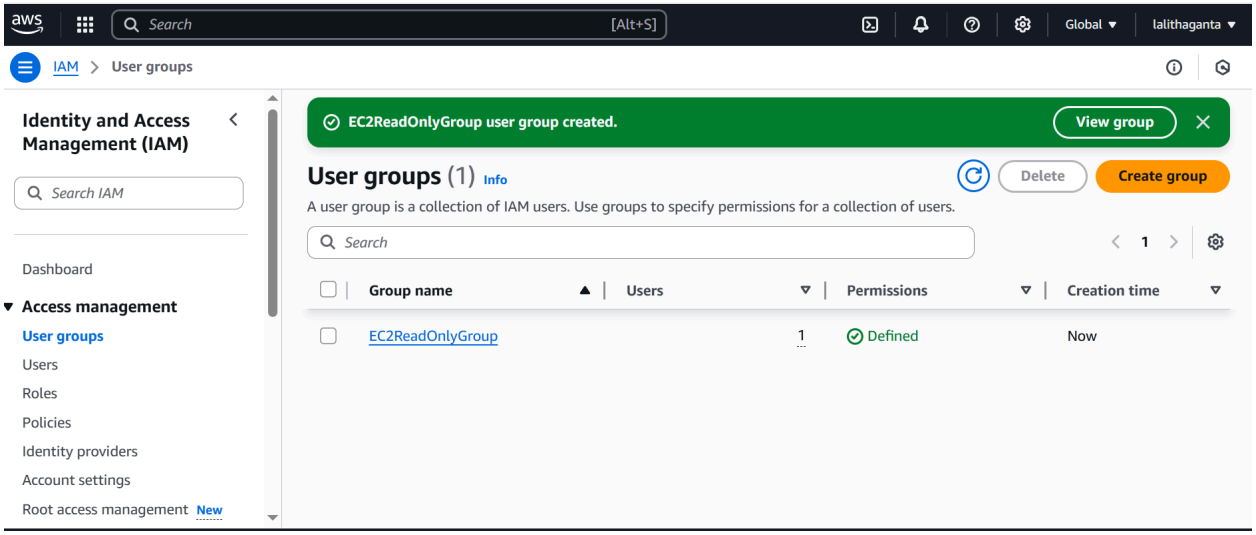
Step 5: Review and Create

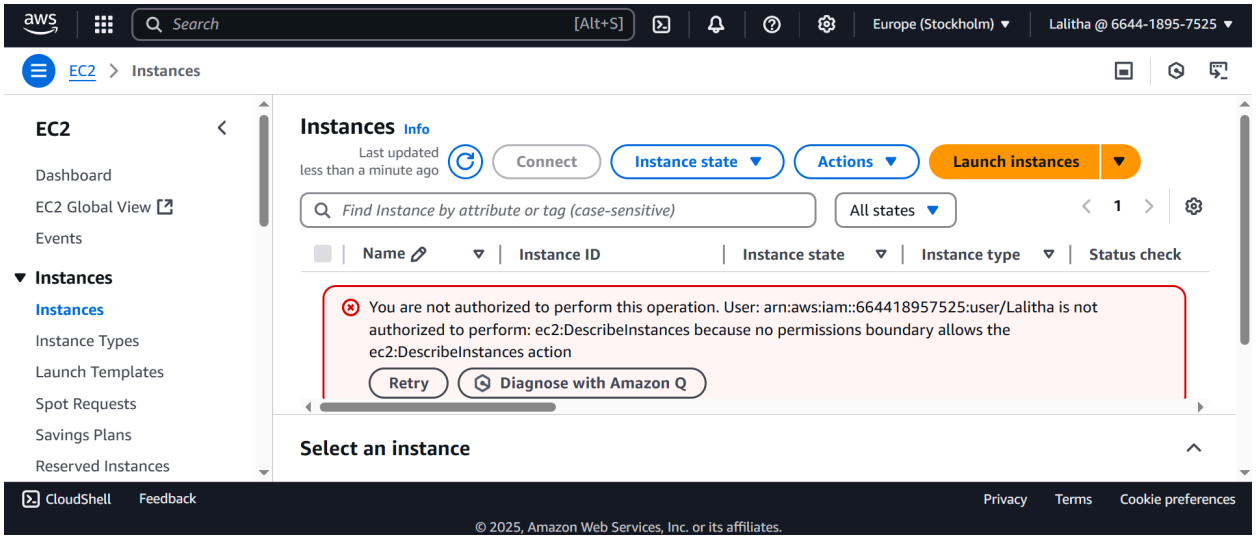
1. Review the group name and attached policy.
2. Click “Create group”.


Search [Alt+S]
Global
lalithaganta
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
User groups (0) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
No resources to display


Search [Alt+S]
Global
lalithaganta
IAM > User groups > Create user group
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
EC2ReadOnlyGroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (1/1) 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.
Search
User name
Groups
Last activity
Creation time
Lalitha
0
None
17 minutes ago


Search [Alt+S]
Global
lalithaganta
IAM > User groups > Create user group
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Attach permissions policies - Optional (1/1045) 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.
Filter by Type
AmazonEC2ReadOnlyAccess
All types
1 match
Policy name
Type
Used as
Description
AmazonEC2ReadO...
AWS managed
None
Provides read only access to Amazon
AmazonEC2ReadOnlyAccess
Copy JSON
Provides read only access to Amazon EC2 via the AWS Management Console.
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search





3) Create a new user with name Devops and add to the group created in task2.

Step 1: Open AWS Console and Go to IAM

1. Sign in to the [AWS Management Console](#).

2. Search for and open IAM.

Step 2: Add New User

1. In the left sidebar, click "Users".
2. Click the "Add users" button.

Step 3: Enter User Details

- User name: **Devops**
- Access type (choose as needed):

Programmatic access (for CLI/API)

AWS Management Console access (for web access)

Set a password if enabling console access.

Click Next: Groups.

Step 4: Add User to Group

From the list of groups, find and check the box for:

EC2ReadOnlyGroup

1. This will assign the permissions attached to that group (EC2 read-only).

Click Next: Tags.

Step 5: (Optional) Add Tags

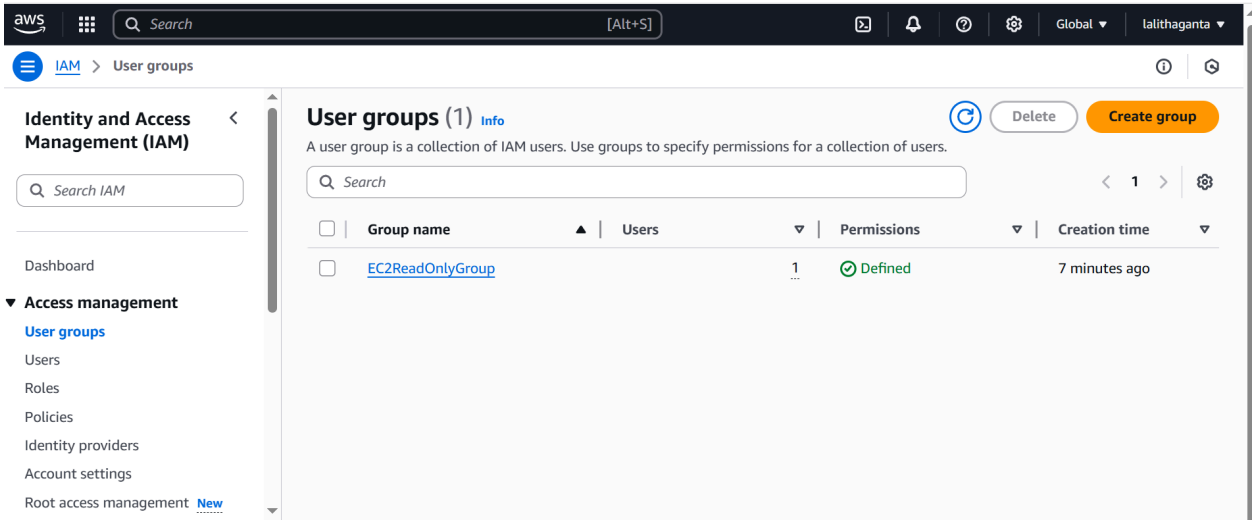
Example:

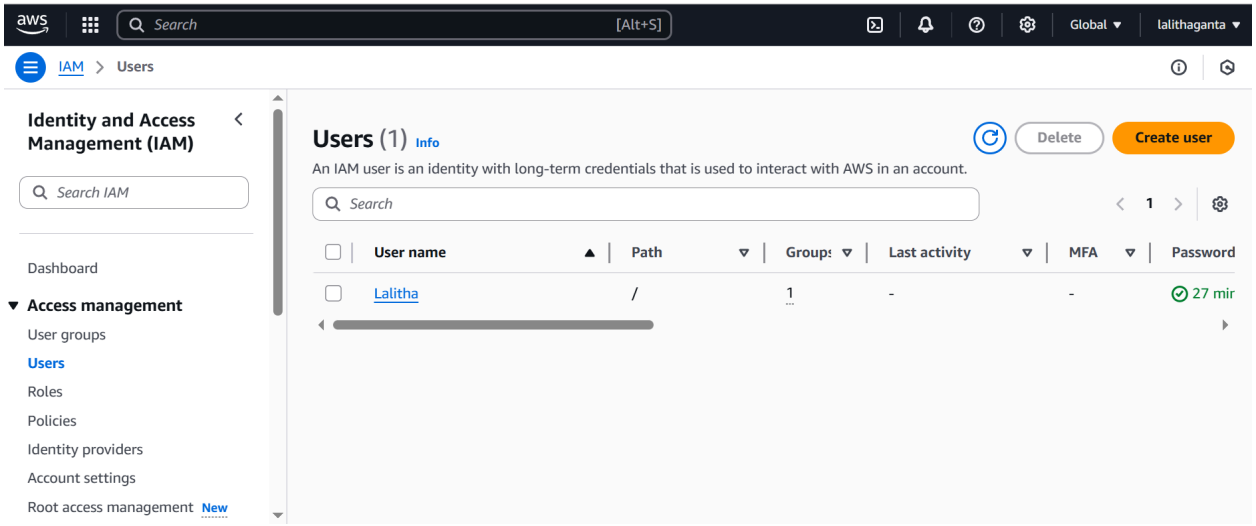
- Key: Department, Value: DevOps

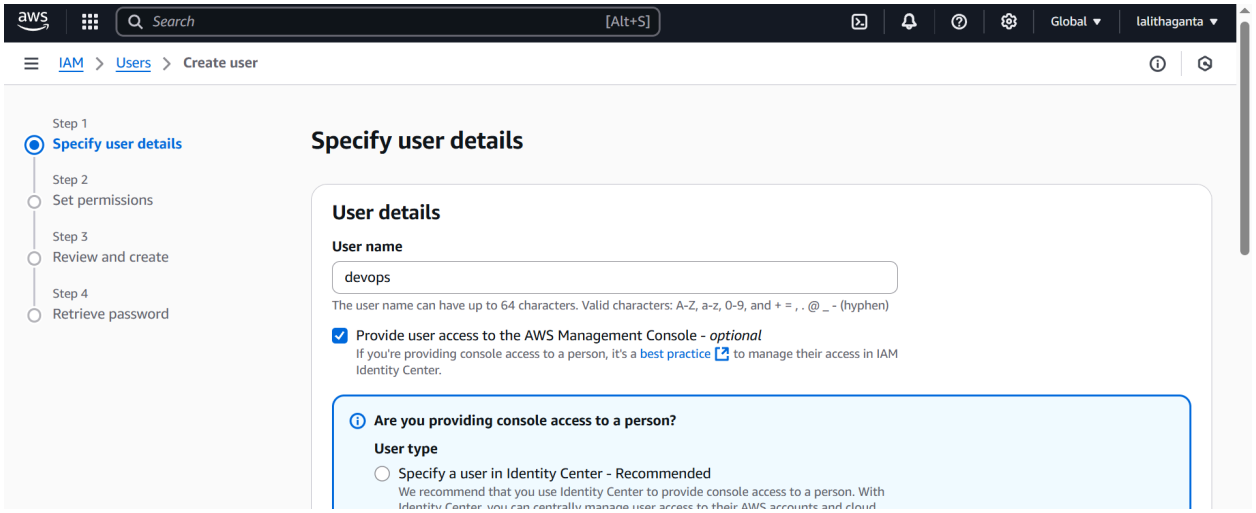
Click Next: Review.

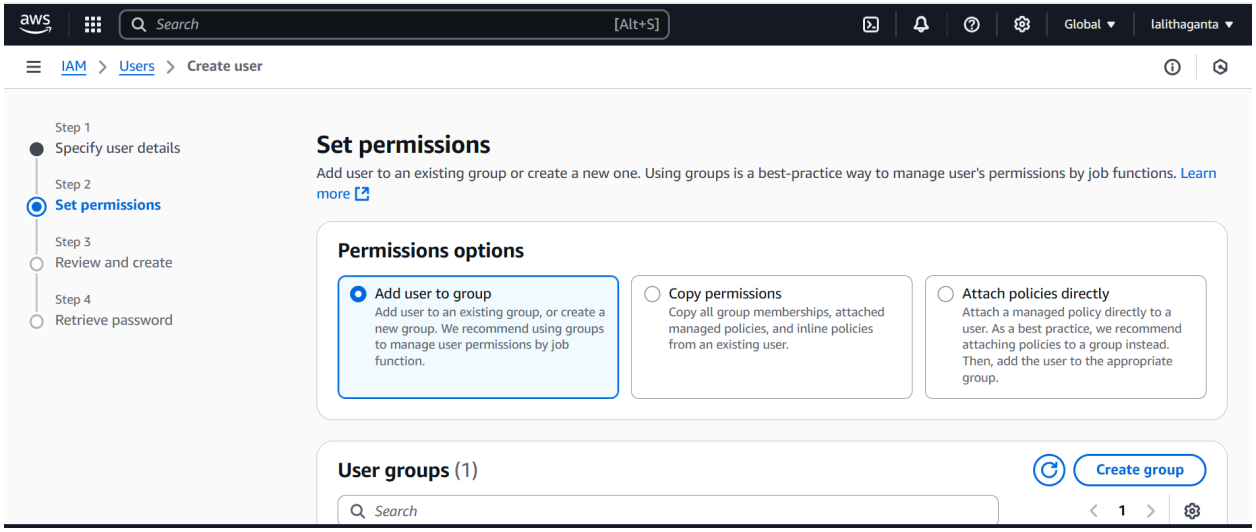
Step 6: Review and Create

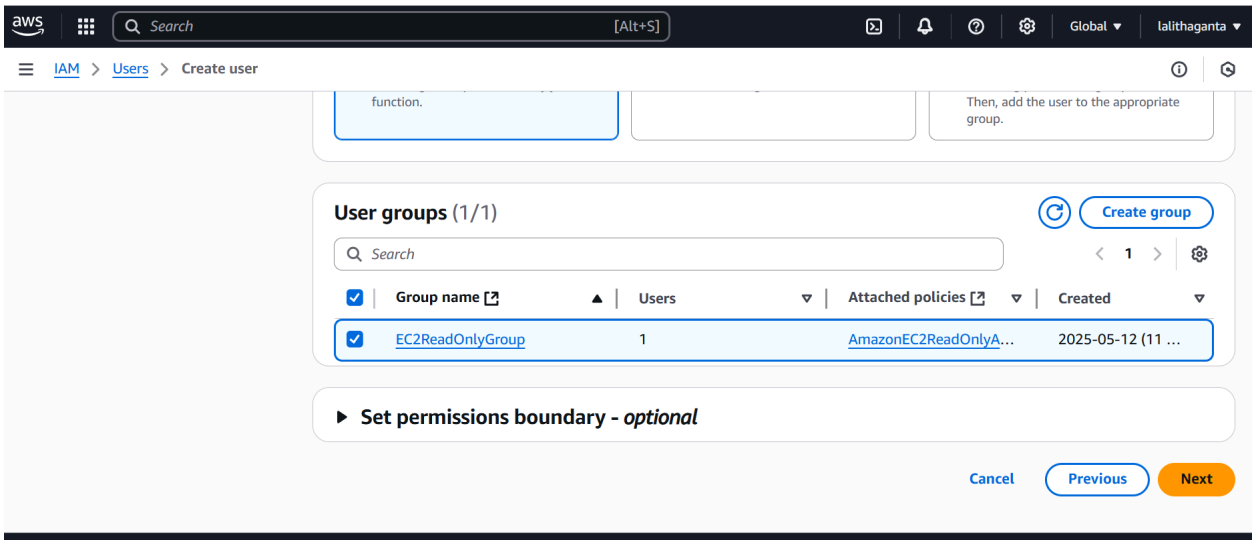
1. Verify:
    - Username: Devops
    - Group: EC2ReadOnlyGroup
    - Permissions: AmazonEC2ReadOnlyAccess (via group)
2. Click Create user.

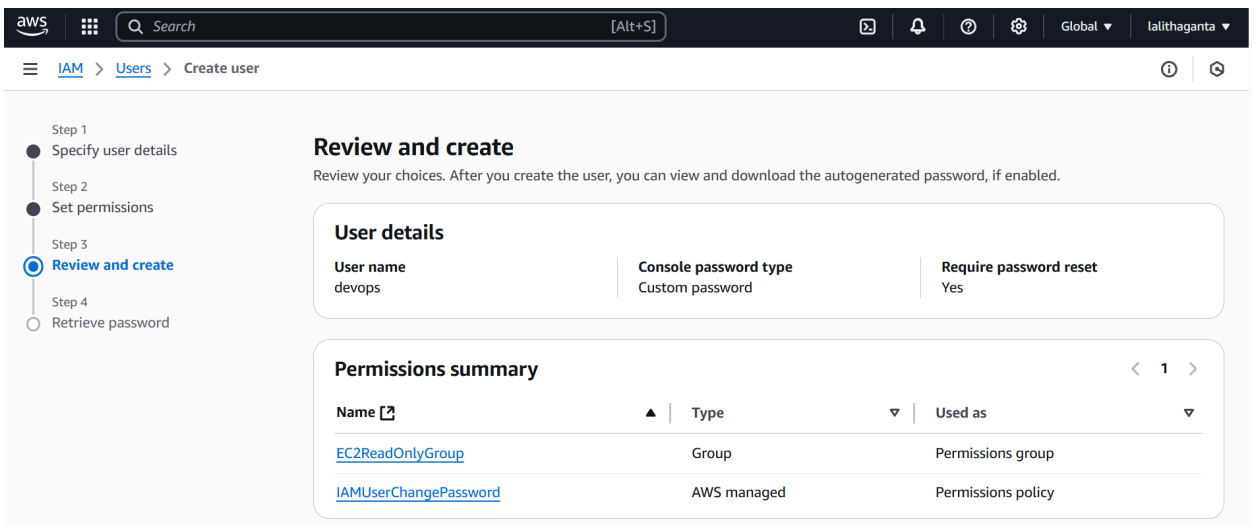

Search [Alt+S]
Global
lalithaganta
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
EC2ReadOnlyGroup
1
Defined
7 minutes ago

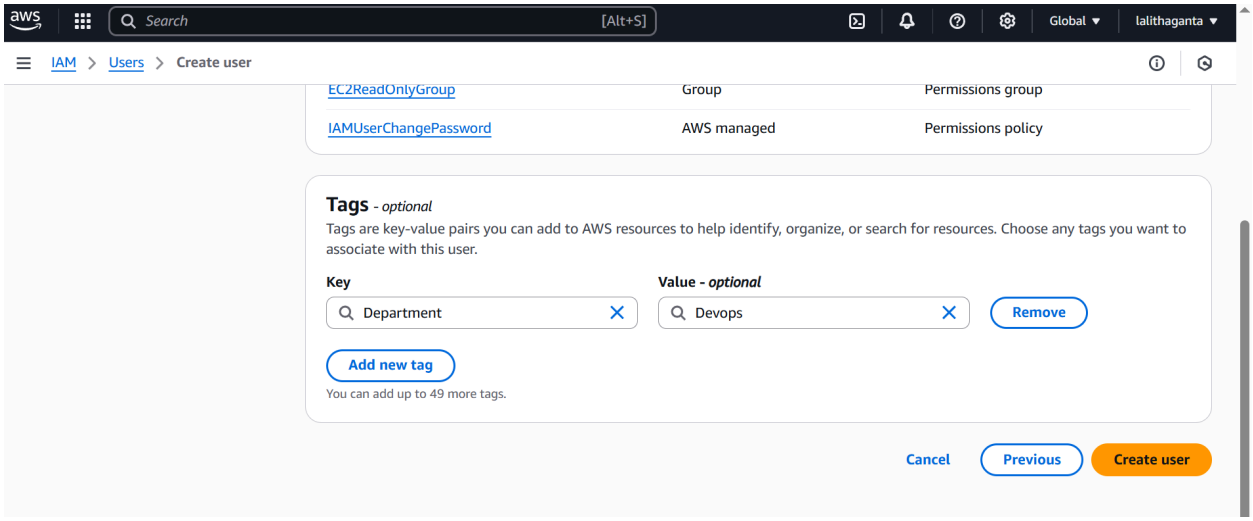

Search [Alt+S]
Global
lalithaganta
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password
Lalitha
/
1
-
-
27 mir

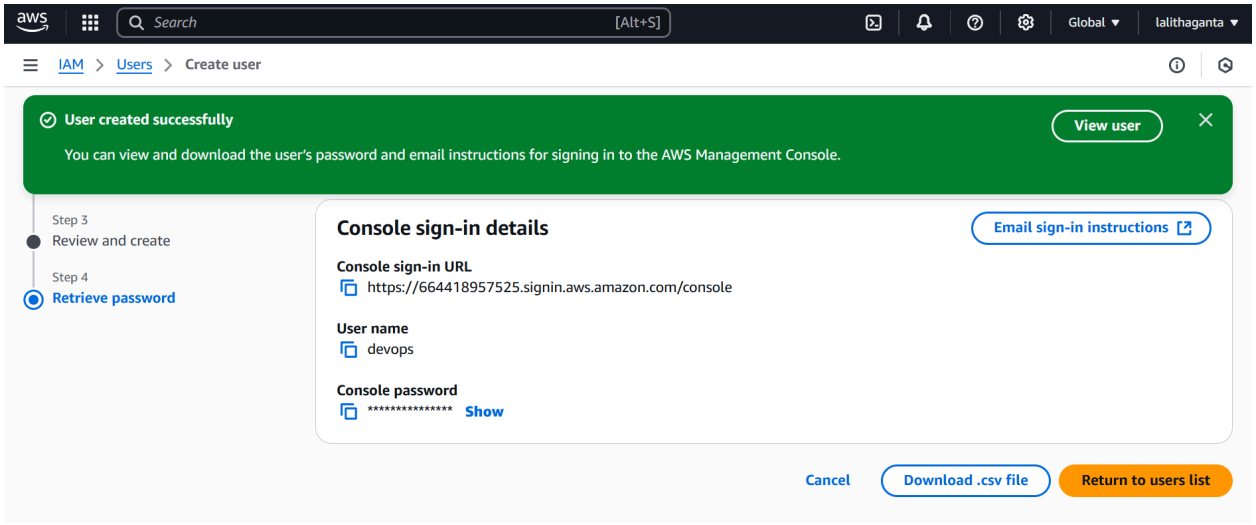

Search [Alt+S]
Global
lalithaganta
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
devops
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (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

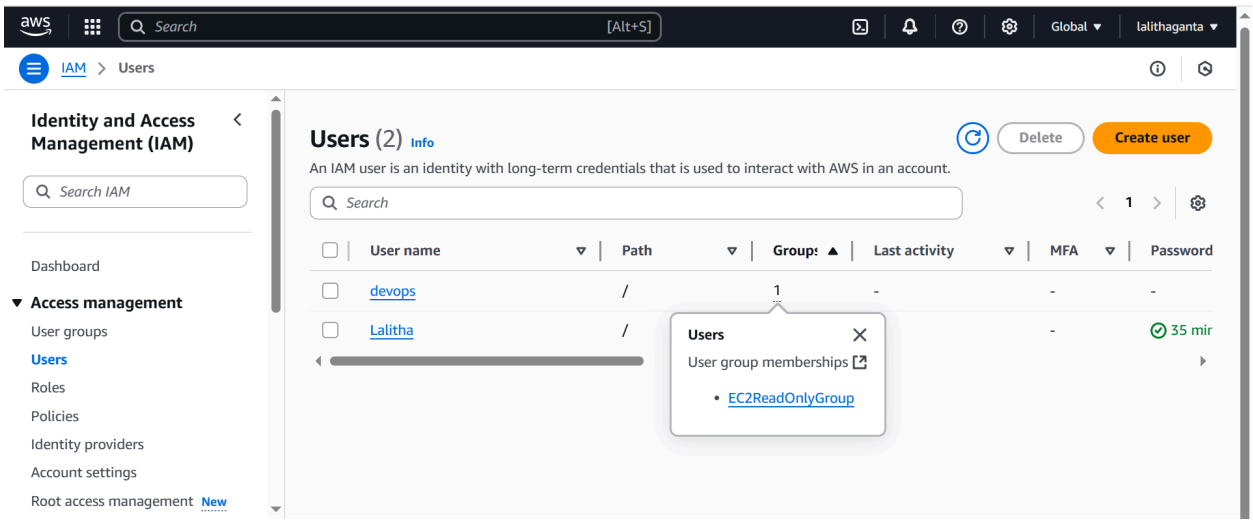

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
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)
Create group
Search
1


aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
function.
Then, add the user to the appropriate group.
User groups (1/1)
Create group
Search
1
Group name
Users
Attached policies
Created
EC2ReadOnlyGroup
1
AmazonEC2ReadOnlyA...
2025-05-12 (11 ...
Set permissions boundary - optional
Cancel
Previous
Next


aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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
devops
Console password type
Custom password
Require password reset
Yes
Permissions summary
1
Name
Type
Used as
EC2ReadOnlyGroup
Group
Permissions group
IAMUserChangePassword
AWS managed
Permissions policy


aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
EC2ReadOnlyGroup
Group
Permissions group
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.
Key
Value - optional
Department
Devops
Remove
Add new tag
You can add up to 49 more tags.
Cancel
Previous
Create user


aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users > Create user
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 3
Review and create
Step 4
Retrieve password
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://664418957525.signin.aws.amazon.com/console
User name
devops
Console password
********** Show
Cancel
Download .csv file
Return to users list


aws
Search
[Alt+S]
Global
lalithaganta
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Users (2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Group:
Last activity
MFA
Password
devops
/
1
-
-
-
Lalitha
/
-
35 mir
Users
User group memberships
EC2ReadOnlyGroup

4) Write a bash script to create a IAM user with VPC full access.

AWS CLI is installed.

```
aws --version
```

AWS CLI is configured with admin credentials:

```
aws configure
```

You have permission to create IAM users and attach policies.

Create a new file: `nano create-vpc-user.sh`

Paste the following script:

bash

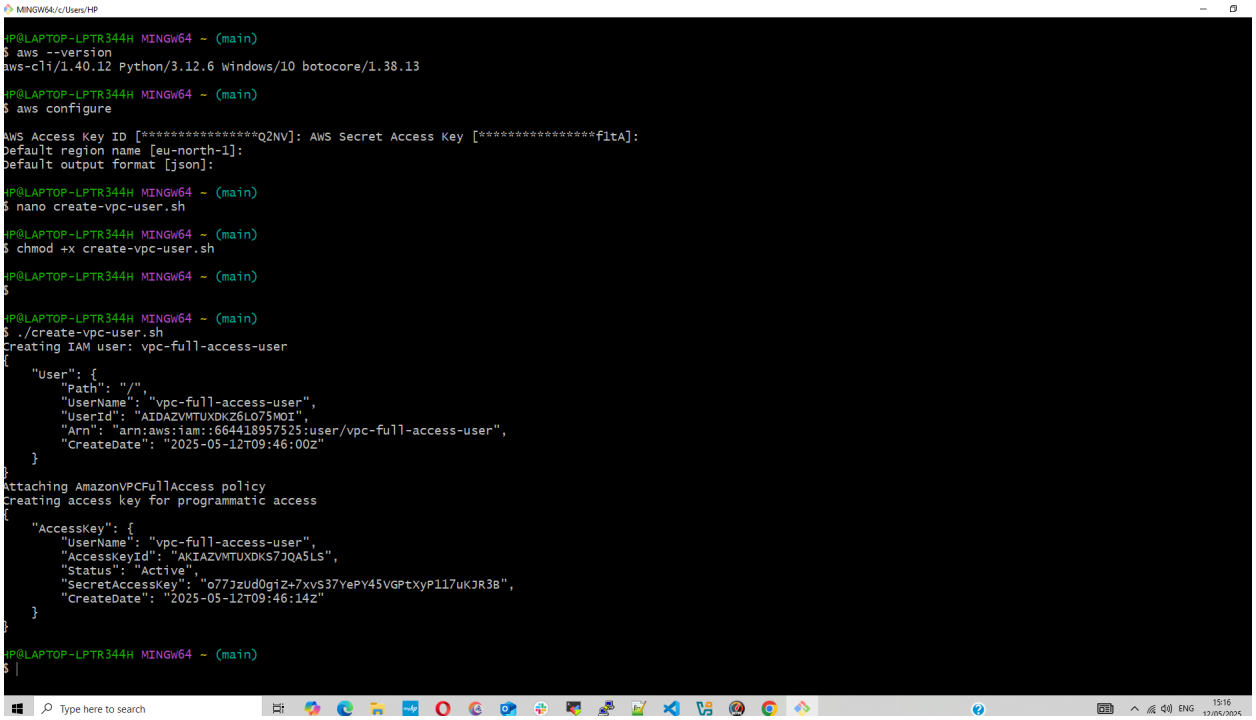
```
#!/bin/bash

# Variables
IAM_USER="vpc-full-access-user"
POLICY_ARN="arn:aws:iam::aws:policy/AmazonVPCFullAccess
"

echo "Creating IAM user: $IAM_USER"
aws iam create-user --user-name "$IAM_USER"

echo "Attaching AmazonVPCFullAccess policy"
aws iam attach-user-policy --user-name "$IAM_USER"
--policy-arn "$POLICY_ARN"

echo "Creating access key for programmatic access"
aws iam create-access-key --user-name "$IAM_USER"
```

Step 2: Make the Script Executable

```
chmod +x create-vpc-user.sh
```

Step 3: Run the Script

```
./create-vpc-user.sh
```



HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$ ./create-vpc-user.sh
Creating IAM user: vpc-full-access-user
{
"User": {
"Path": "/",
"UserName": "vpc-full-access-user",
"UserId": "AIDAZVMTUXDKZ6LO75MOI",
"Arn": "arn:aws:iam::664418957525:user/vpc-full-access-user",
"CreateDate": "2025-05-12T09:46:00Z"
}
}
Attaching AmazonVPCFullAccess policy
Creating access key for programmatic access
{
"AccessKey": {
"UserName": "vpc-full-access-user",
"AccessKeyId": "AKIAZVMTUXDKS7JQA5LS",
"Status": "Active",
"SecretAccessKey": "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",
"CreateDate": "2025-05-12T09:46:14Z"
}
}
HP@LAPTOP-LPTR344H MINGW64 ~ (main)
$
Type here to search

5) Create a IAM policy to access ec2 for a specific user in specific regions only.

Navigate to IAM > Policies

1. **In the AWS Console, go to IAM**
2. **In the left panel, click Policies**
3. **Click "Create policy"**

Step 3: Create Custom Policy JSON

1. **Click the JSON tab**
2. **Paste the following policy:**

json
CopyEdit

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2RegionRestrictedAccess",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "us-east-1",
            "us-west-2"
          ]
```

```
        }
      }
    }
  ]
}
```

Name and Create the Policy

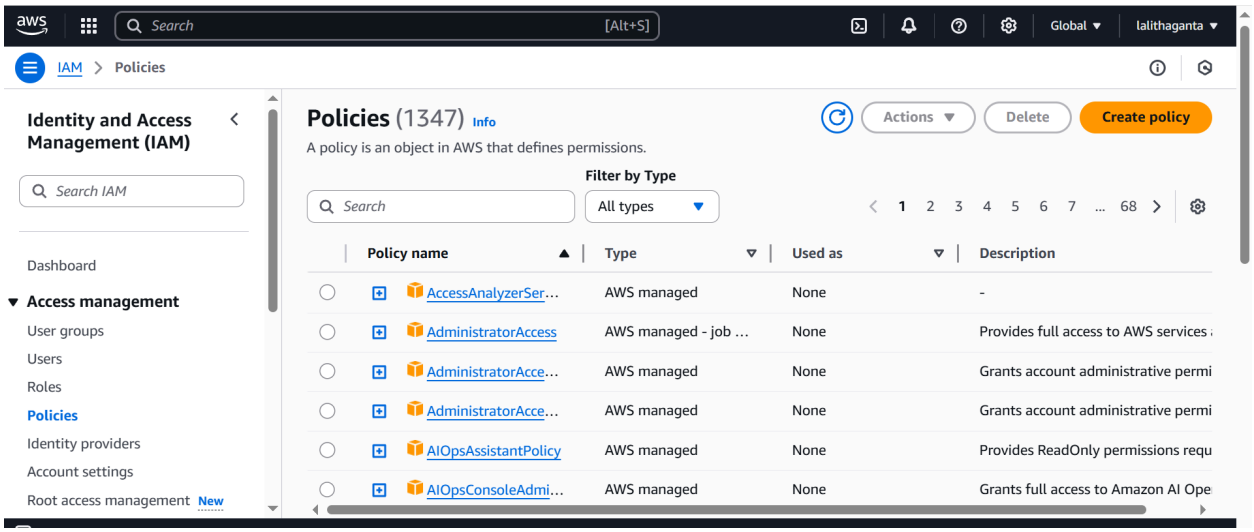
1. Click Next: Tags (optional)
2. Click Next: Review
3. Set:
    - Name: `EC2SpecificRegionsPolicy`
    - Description: `Allows EC2 access only in us-east-1 and us-west-2`
4. Click Create policy

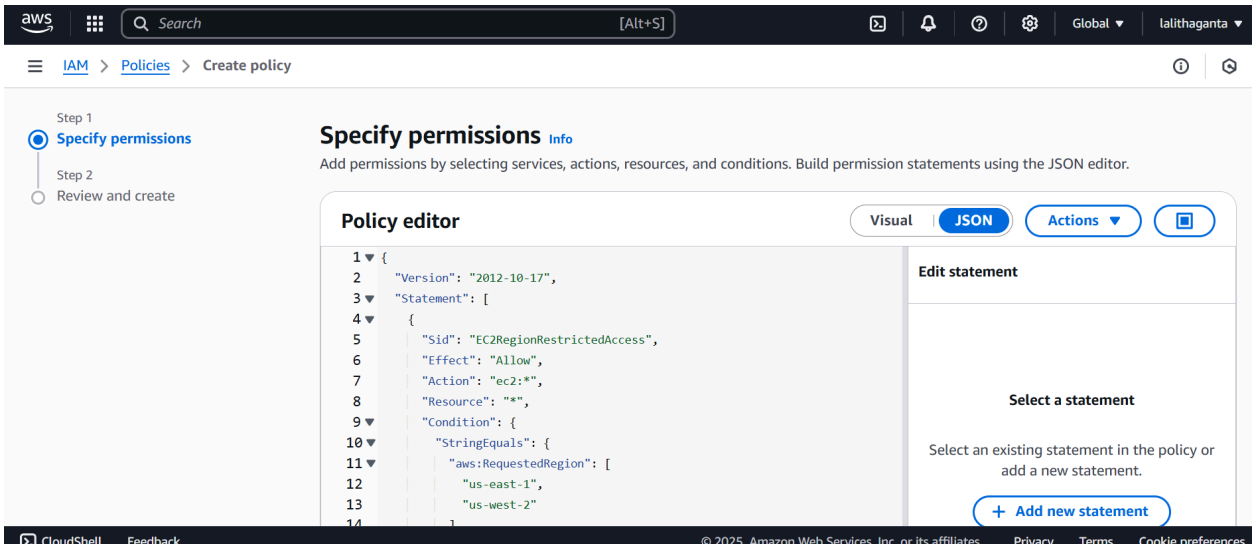
Attach Policy to a Specific User

1. In the IAM console, go to Users
2. Click on the user you want to assign the policy to (e.g., `DevopsUser`)
3. Go to Permissions > Add permissions
4. Choose Attach policies directly

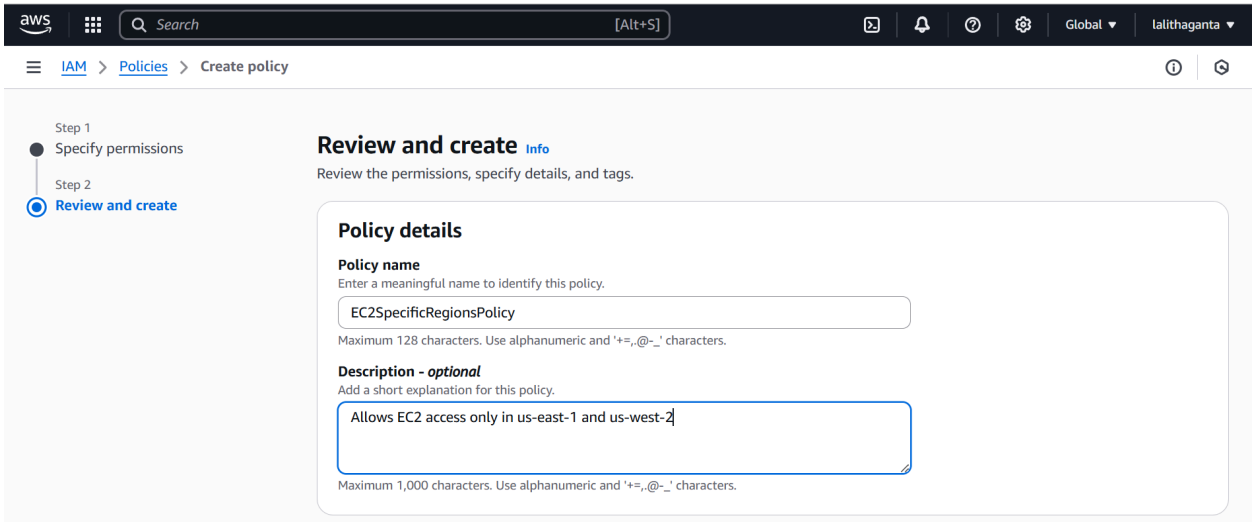
5. Search for and select **EC2SpecificRegionsPolicy**

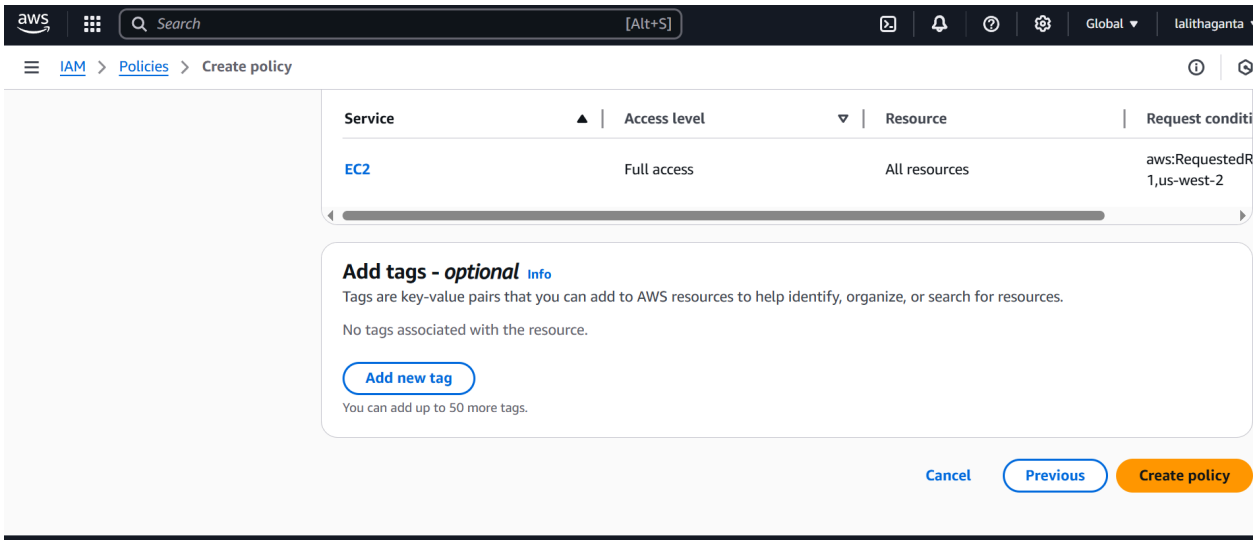
6. Click **Next > Review > Add permissions**

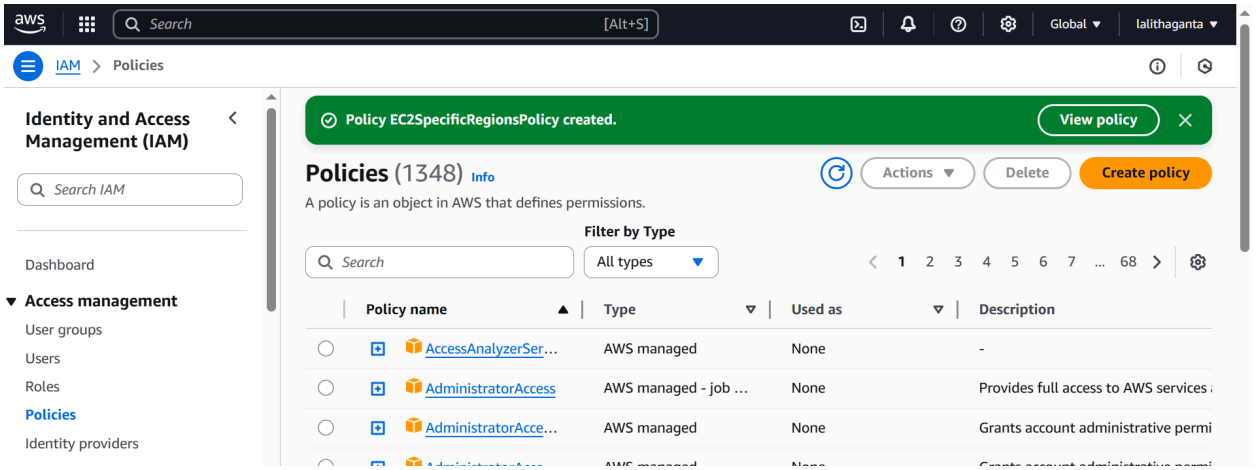


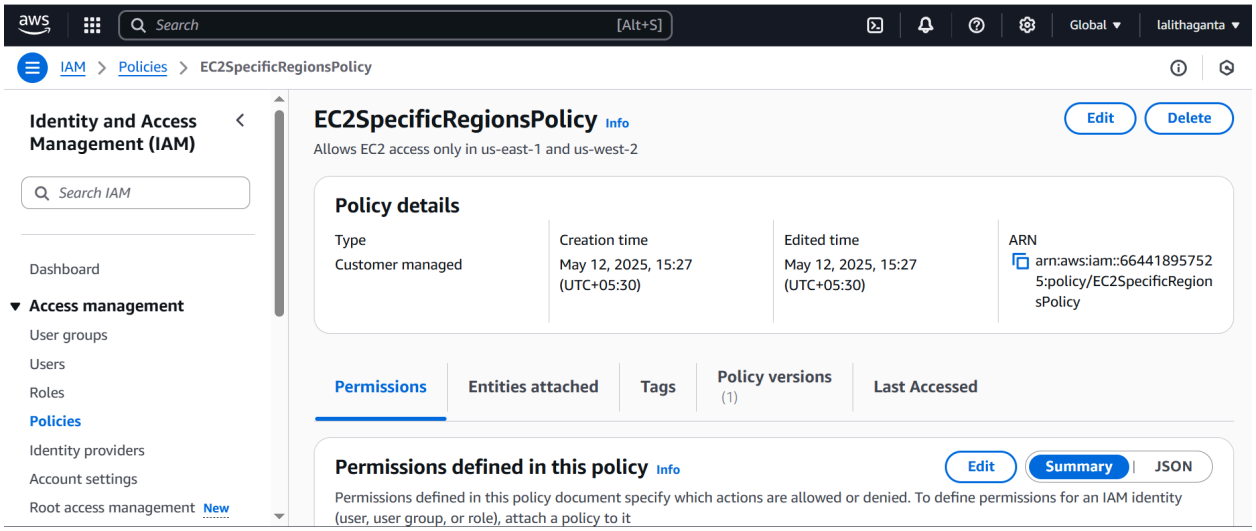


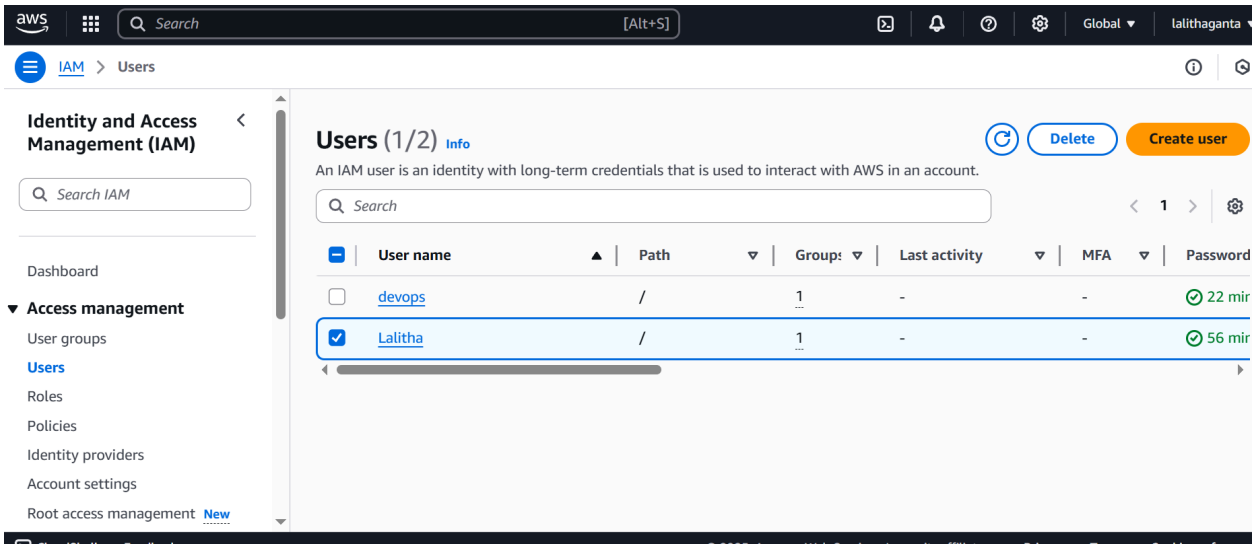

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Policies > Create policy
7 "Action": "ec2:*",
8 "Resource": "*",
9 "Condition": {
10 "StringEquals": {
11 "aws:RequestedRegion": [
12 "us-east-1",
13 "us-west-2"
14]
15 }
16 }
17 }
18]
19 }
20
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement

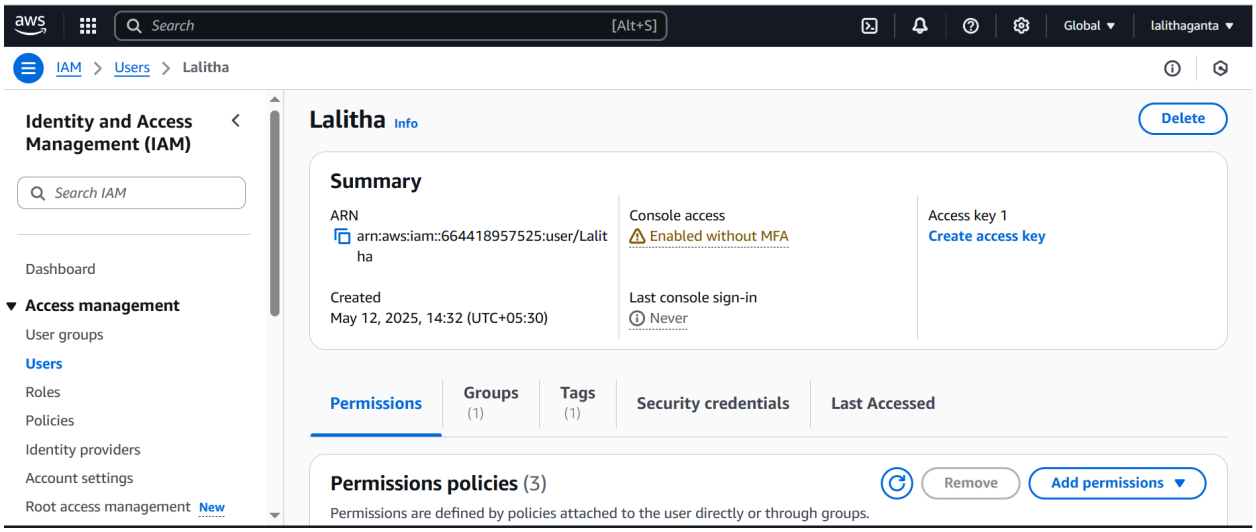

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
EC2SpecificRegionsPolicy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Allows EC2 access only in us-east-1 and us-west-2
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

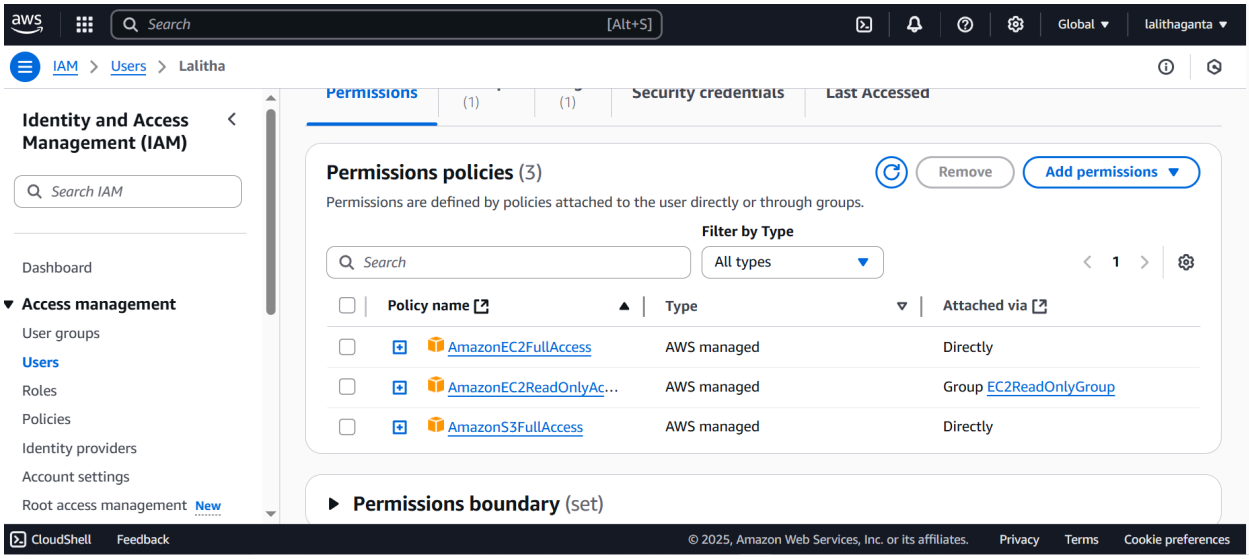

aws
Search
[Alt+S]
Global
lalithaganta
IAM > Policies > Create policy
Service
Access level
Resource
Request conditi
EC2
Full access
All resources
aws:RequestedR
1,us-west-2
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create policy

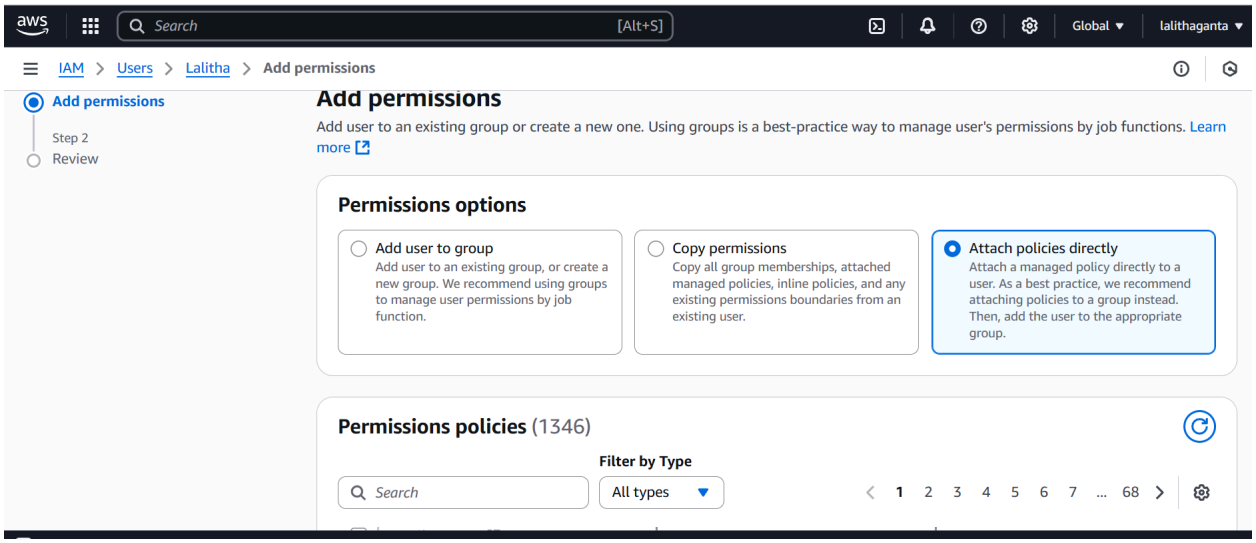

Search [Alt+S]
Global
lalithaganta
IAM > Policies
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Policy EC2SpecificRegionsPolicy created.
View policy
Policies (1348) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 68
Policy name
Type
Used as
Description
AccessAnalyzerSer...
AWS managed
None
-
AdministratorAccess
AWS managed - job ...
None
Provides full access to AWS services
AdministratorAcce...
AWS managed
None
Grants account administrative permi

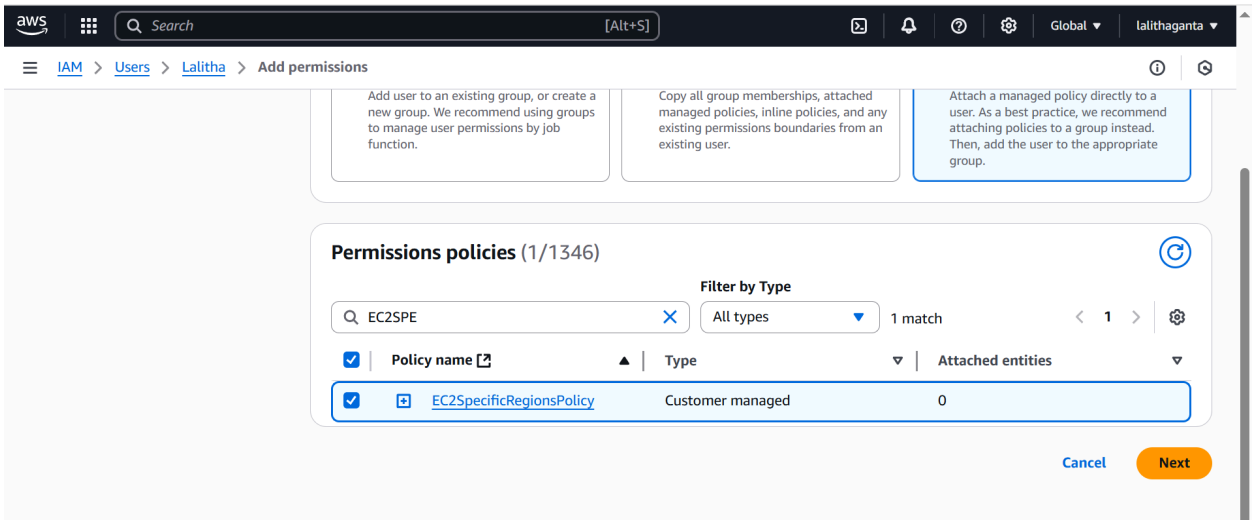

Search [Alt+S]
Global
lalithaganta
IAM > Policies > EC2SpecificRegionsPolicy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
EC2SpecificRegionsPolicy Info
Allows EC2 access only in us-east-1 and us-west-2
Edit
Delete
Policy details
Type
Customer managed
Creation time
May 12, 2025, 15:27 (UTC+05:30)
Edited time
May 12, 2025, 15:27 (UTC+05:30)
ARN
arn:aws:iam::664418957525:policy/EC2SpecificRegionsPolicy
Permissions
Entities attached
Tags
Policy versions (1)
Last Accessed
Permissions defined in this policy Info
Edit
Summary
JSON
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

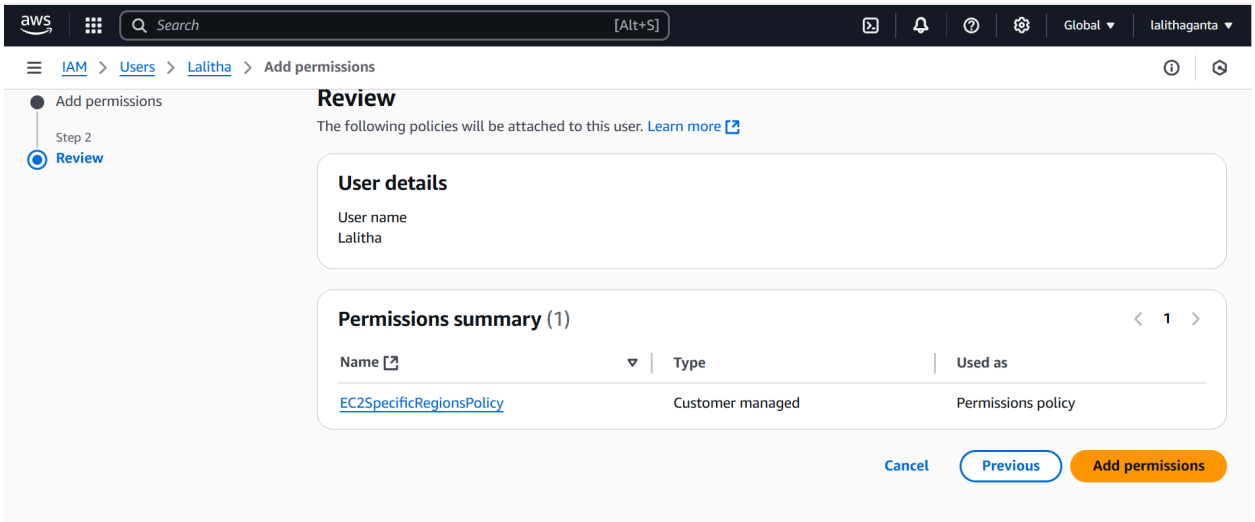

Search [Alt+S]
Global
lalithaganta
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Users (1/2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
1
User name
Path
Groups
Last activity
MFA
Password
devops
/
1
-
-
22 mir
Lalitha
/
1
-
-
56 mir

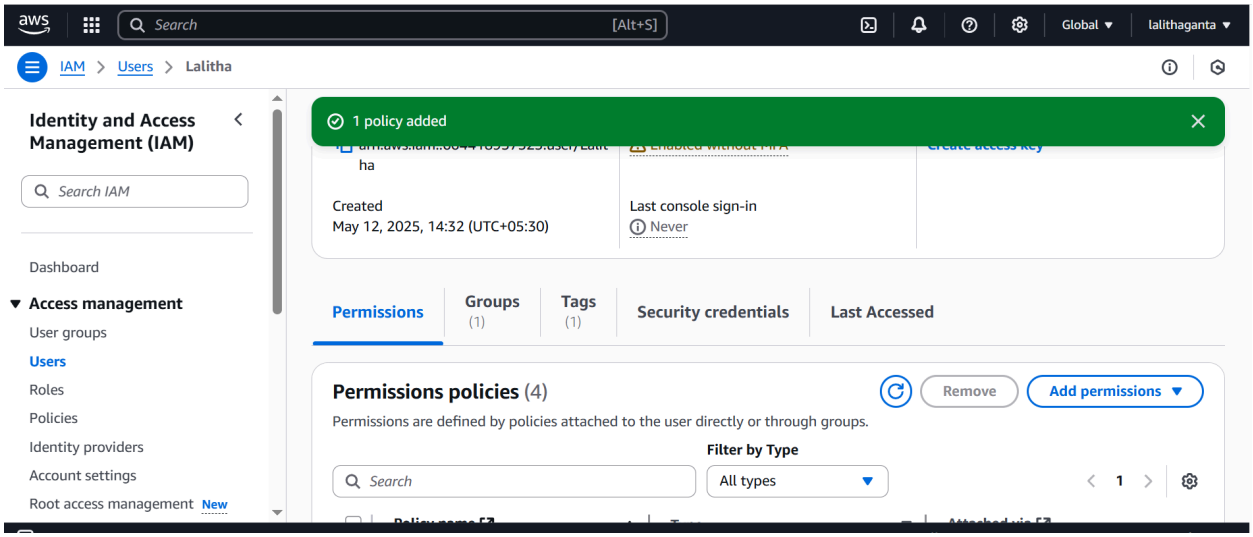

Search [Alt+S]
Global
lalithaganta
IAM > Users > Lalitha
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Lalitha Info
Delete
Summary
ARN
arn:aws:iam::664418957525:user/Lalitha
Console access
Enabled without MFA
Access key 1
Create access key
Created
May 12, 2025, 14:32 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags (1)
Security credentials
Last Accessed
Permissions policies (3)
Remove
Add permissions
Permissions are defined by policies attached to the user directly or through groups.

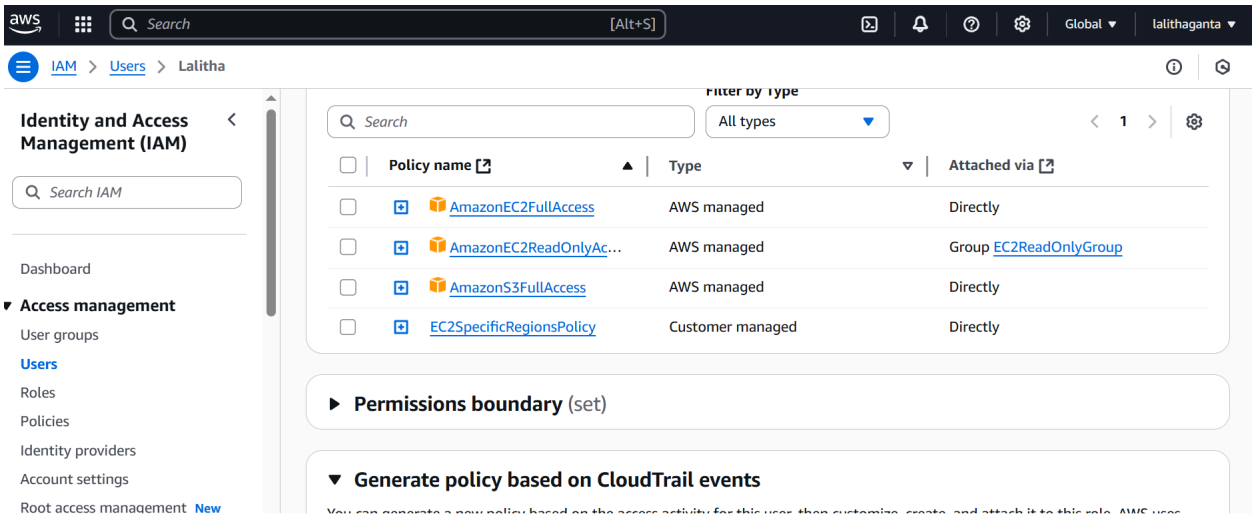

Search [Alt+S]
Global
lalithaganta
IAM > Users > Lalitha
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Permissions (1) (1) Security credentials Last Accessed
Permissions policies (3)
Remove
Add permissions
Permissions are defined by policies attached to the user directly or through groups.
Filter by Type
Search
All types
1
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
AmazonEC2ReadOnlyAc...
AWS managed
Group EC2ReadOnlyGroup
AmazonS3FullAccess
AWS managed
Directly
Permissions boundary (set)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
lalithaganta
IAM > Users > Lalitha > Add permissions
Add permissions
Step 2
Review
Add 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
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
Attach policies directly
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.
Permissions policies (1346)
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 68


Search [Alt+S]
Global
lalithaganta
IAM > Users > Lalitha > Add permissions
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, inline policies, and any existing permissions boundaries 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.
Permissions policies (1/1346)
Filter by Type
EC2SPE
All types
1 match
1
Policy name
Type
Attached entities
EC2SpecificRegionsPolicy
Customer managed
0
Cancel
Next


Search [Alt+S]
Global
lalithaganta
IAM > Users > Lalitha > Add permissions
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
Lalitha
Permissions summary (1)
1
Name
Type
Used as
EC2SpecificRegionsPolicy
Customer managed
Permissions policy
Cancel
Previous
Add permissions


Search [Alt+S]
Global
lalithaganta
IAM > Users > Lalitha
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
1 policy added
ha
Created
May 12, 2025, 14:32 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups (1)
Tags (1)
Security credentials
Last Accessed
Permissions policies (4)
Remove
Add permissions
Permissions are defined by policies attached to the user directly or through groups.
Filter by Type
Search
All types
1



6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B. (Collaborate with team member and execute this.Mostly asked in every interview)

STEP 1 : Create IAM user in account A And S3 bucket in account B

STEP 2 : The created user gives awsfullaccess to the S3 bucket and provide permission to the below policy

The below Inline policy :

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
   ],
   "Resource": [
    "arn:aws:s3:::<>bucketname",
    "arn:aws:s3:::<bucketname>/*"
```

```
  ]
 }
]
}
```

STEP 4 : Create a S3 bucket in Account B and give the below policy to the S3 Bucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS":
"arn:aws:iam::750471539774:user/crossregion-IAM"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
 "Resource": [
"arn:aws:s3:::task-s3bucket-29",
        "arn:aws:s3:::task-s3bucket-29/*"
      ]
    }
```

]

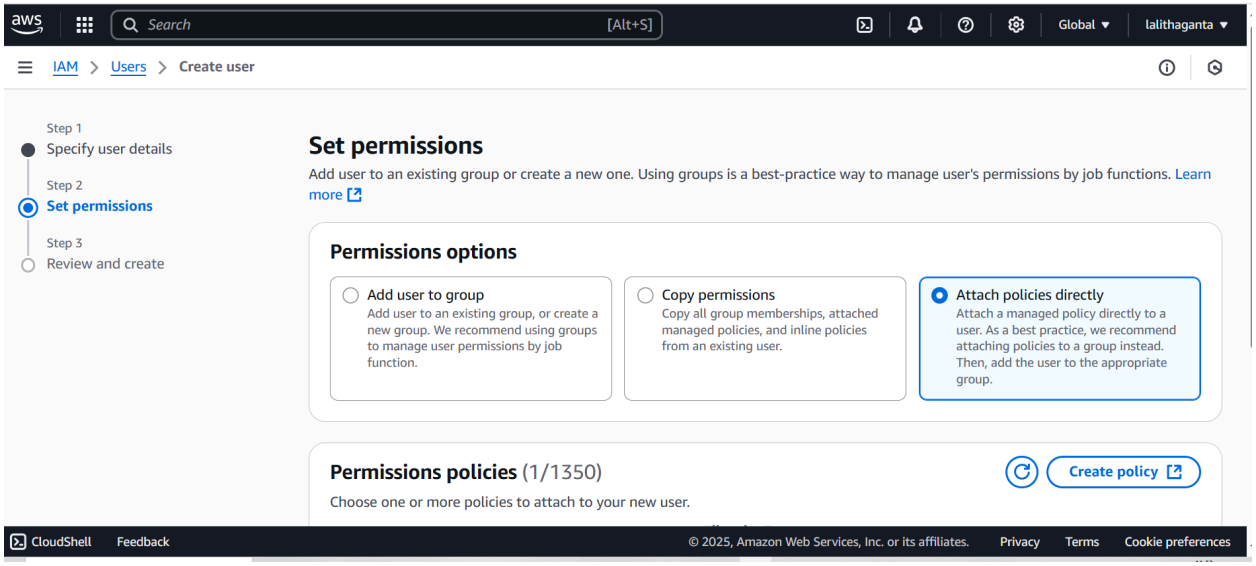
}

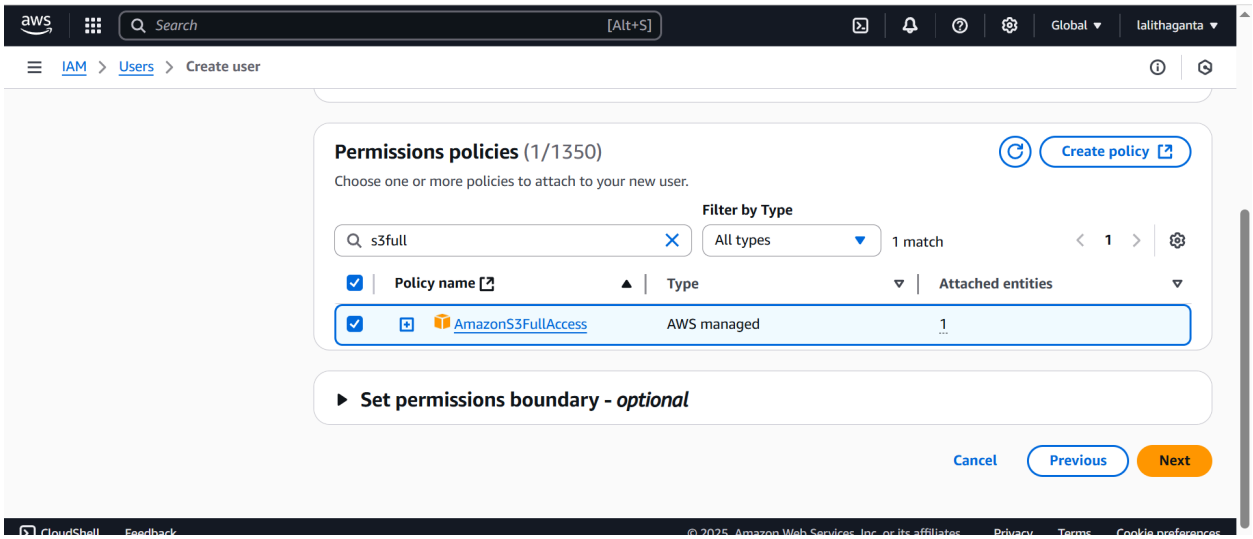
Then save all the changes

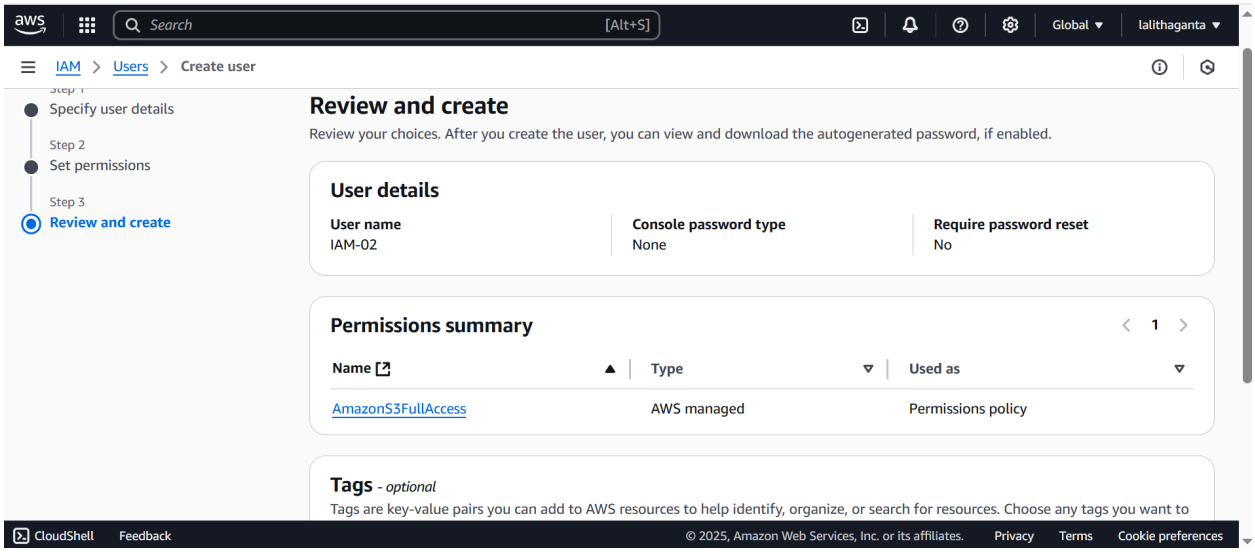
Open git bash and run the below commands

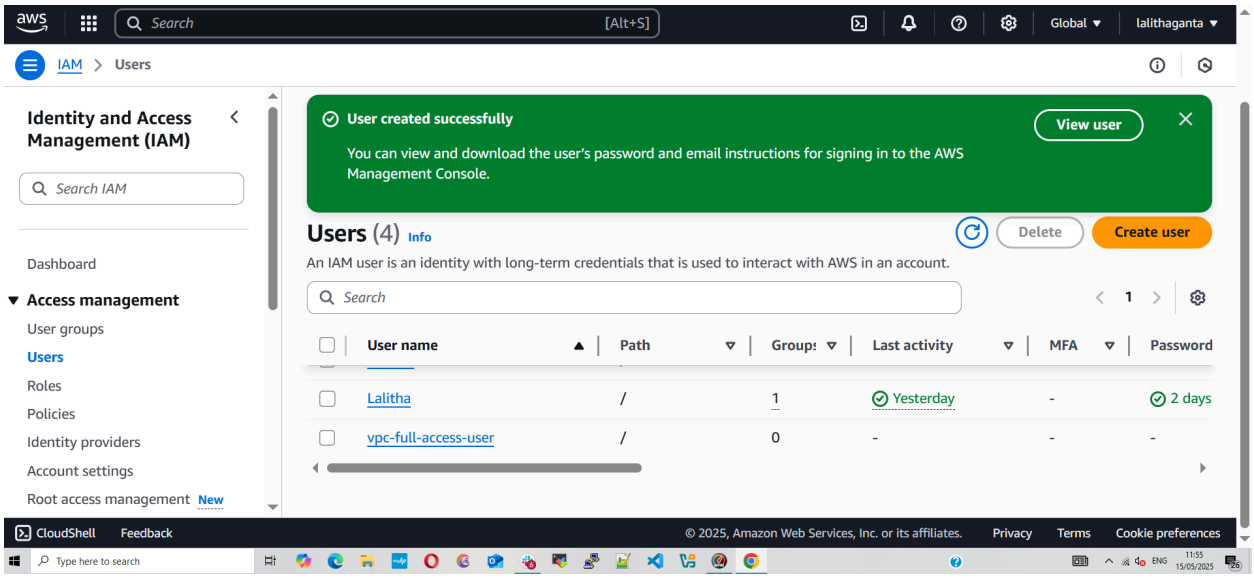
aws configure --profile crossregion-IAM

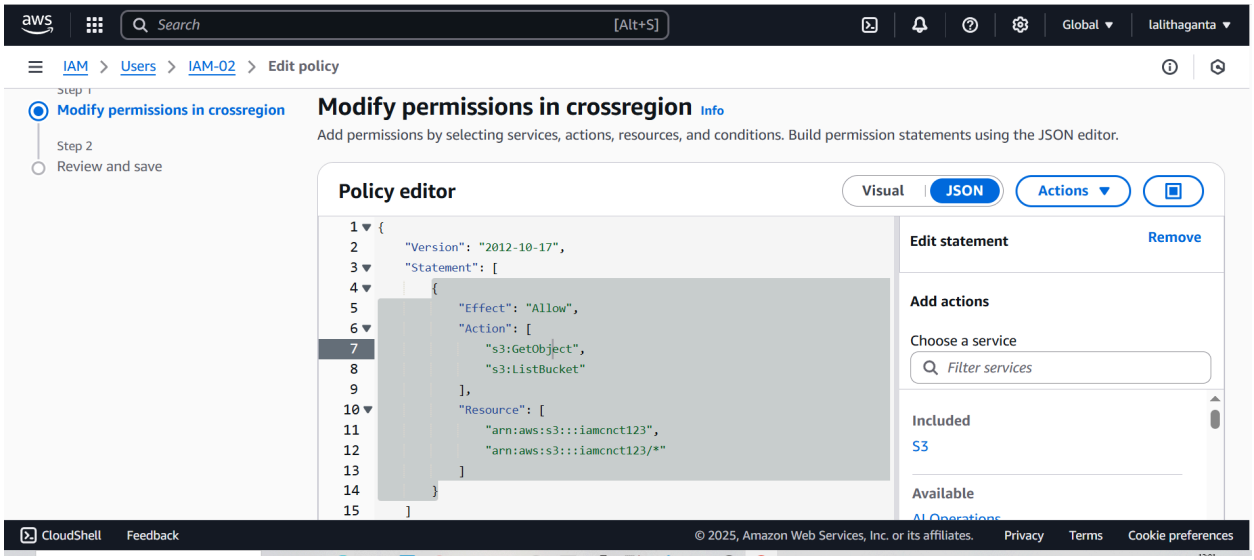
Provide access key and security key

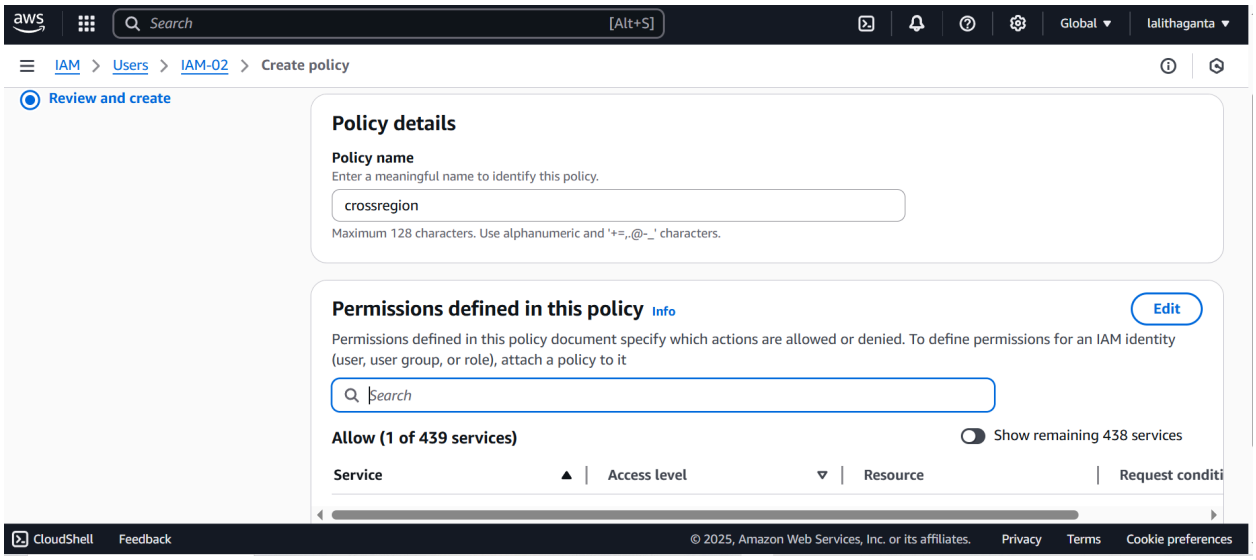


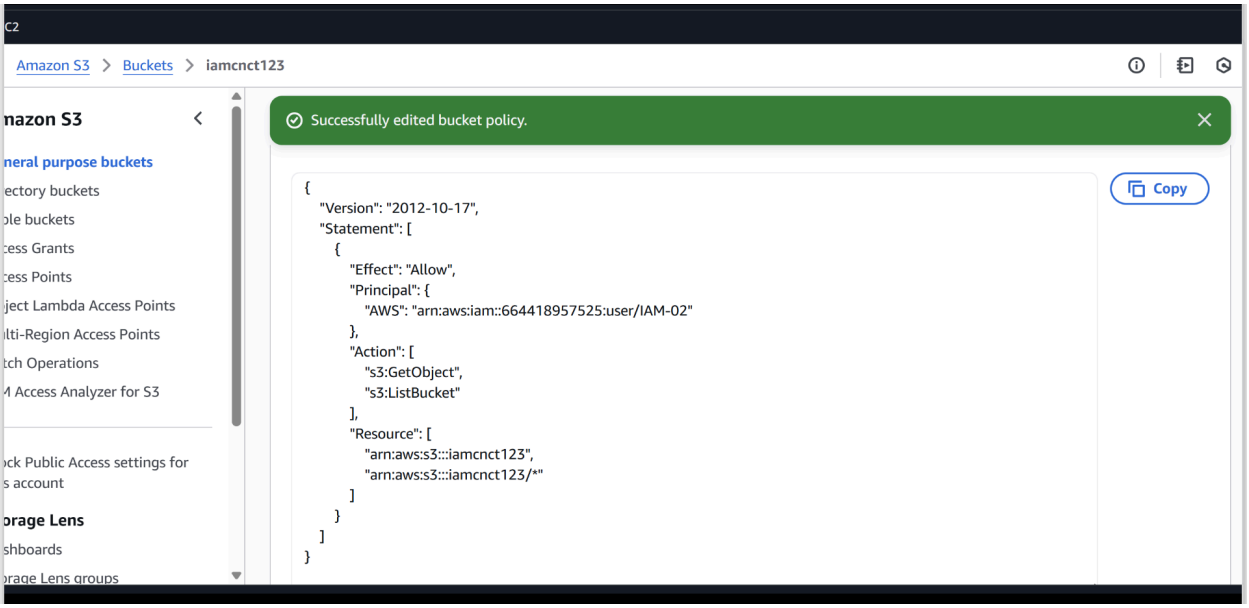


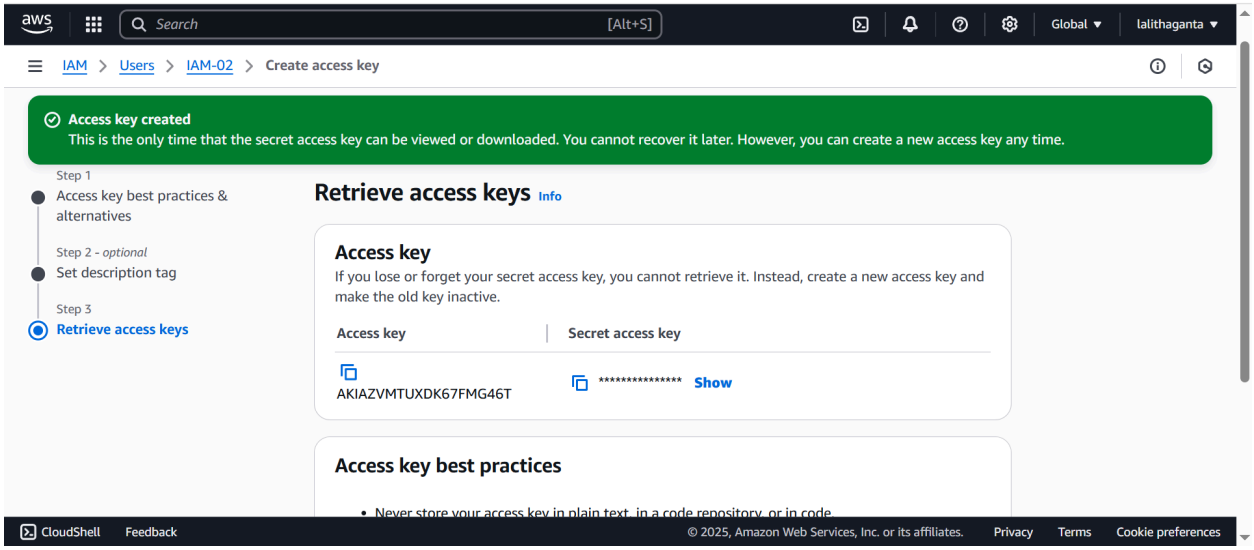

Search [Alt+S]
Global
lalithaganta
IAM > Users > Create user
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
IAM-02
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonS3FullAccess
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

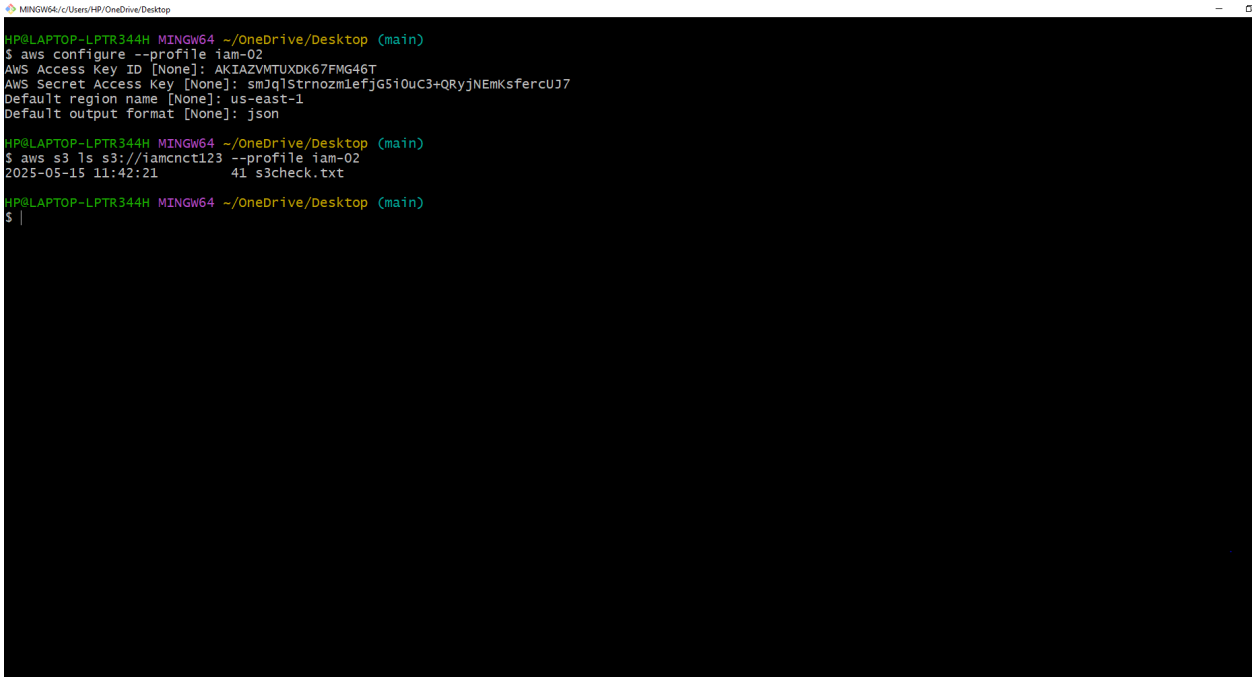

Search [Alt+S]
Global
lalithaganta
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
User created successfully
View user
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
Users (4) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Path
Groups
Last activity
MFA
Password
Lalitha
/
1
Yesterday
-
2 days
vpc-full-access-user
/
0
-
-
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search


Search
[Alt+S]
Global
lalithaganta
IAM > Users > IAM-02 > Edit policy
Modify permissions in crossregion
Step 2
Review and save
Modify permissions in crossregion Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::iamcnct123",
"arn:aws:s3:::iamcnct123/*"
]
}
]
Edit statement
Remove
Add actions
Choose a service
Filter services
Included
S3
Available
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Global
lalithaganta
IAM > Users > IAM-02 > Create policy
Review and create
Policy details
Policy name
Enter a meaningful name to identify this policy.
crossregion
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 439 services)
Show remaining 438 services
Service
Access level
Resource
Request conditi
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon S3 > Buckets > iamcnct123
Successfully edited bucket policy.
Copy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::664418957525:user/IAM-02"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::iamcnct123",
"arn:aws:s3:::iamcnct123/*"
]
}
]
}


Search
[Alt+S]
Global
lalithaganta
IAM > Users > IAM-02 > Create access key
Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Retrieve access keys Info
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
AKIAZVMTUXDK67FMG46T
********** Show
Access key best practices
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


MINGW64:/c/Users/HP/OneDrive/Desktop
HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ aws configure --profile iam-02
AWS Access Key ID [None]: AKIAZVMTUXDK67FMG46T
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$ aws s3 ls s3://iamcnct123 --profile iam-02
2025-05-15 11:42:21 41 s3check.txt
HP@LAPTOP-LPTR344H MINGW64 ~/OneDrive/Desktop (main)
$