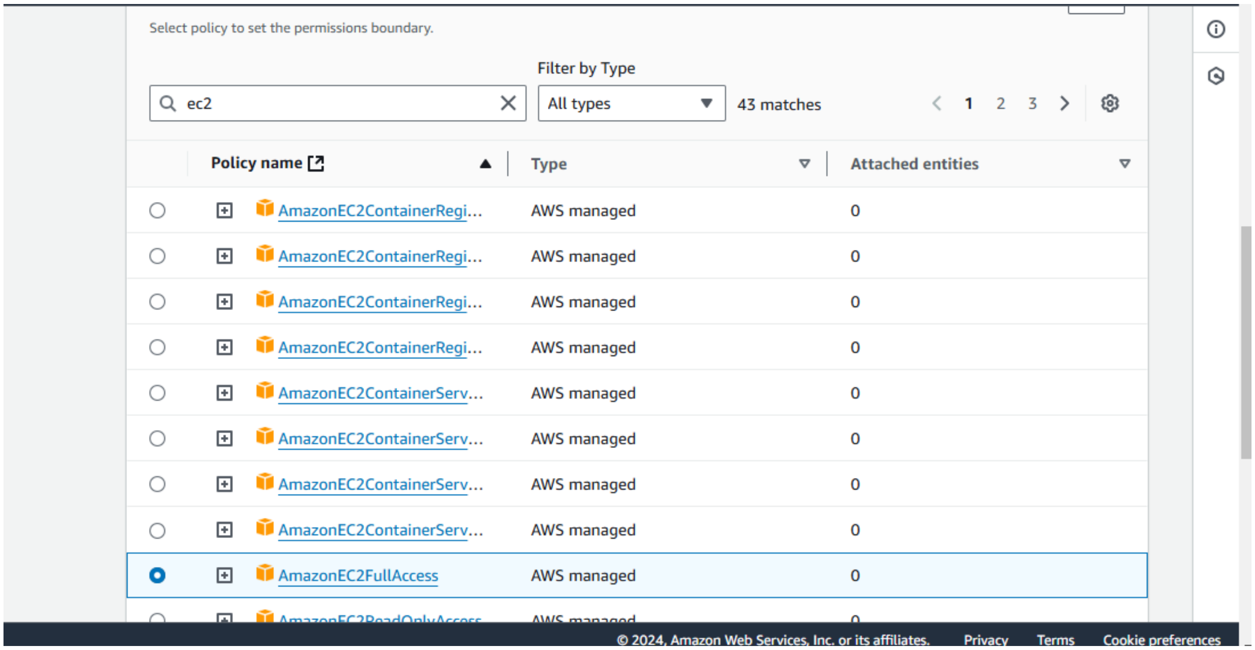
IAM TASKS

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

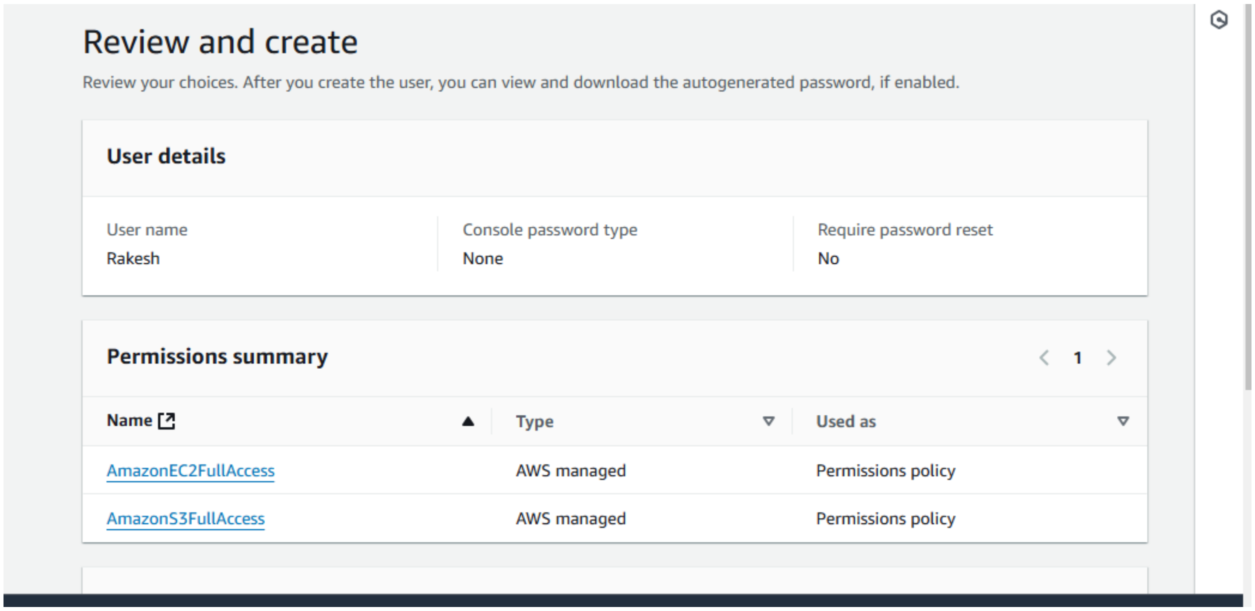


Select policy to set the permissions boundary.

Filter by Type

ec2 | All types | 43 matches

	Policy name	Type	Attached entities
○	AmazonEC2ContainerRegi...	AWS managed	0
○	AmazonEC2ContainerRegi...	AWS managed	0
○	AmazonEC2ContainerRegi...	AWS managed	0
○	AmazonEC2ContainerRegi...	AWS managed	0
○	AmazonEC2ContainerServ...	AWS managed	0
○	AmazonEC2ContainerServ...	AWS managed	0
○	AmazonEC2ContainerServ...	AWS managed	0
○	AmazonEC2ContainerServ...	AWS managed	0
●	AmazonEC2FullAccess	AWS managed	0
○	AmazonEC2ReadOnlyAccess	AWS managed	0



Review and create

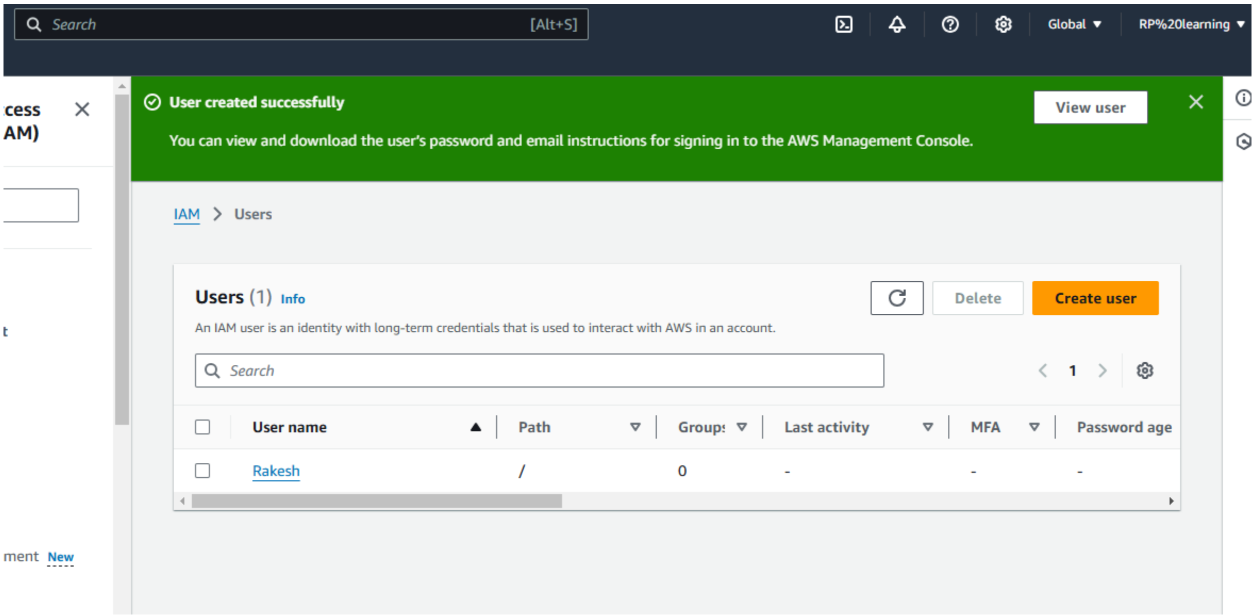
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
Rakesh	None	No

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy



User created successfully

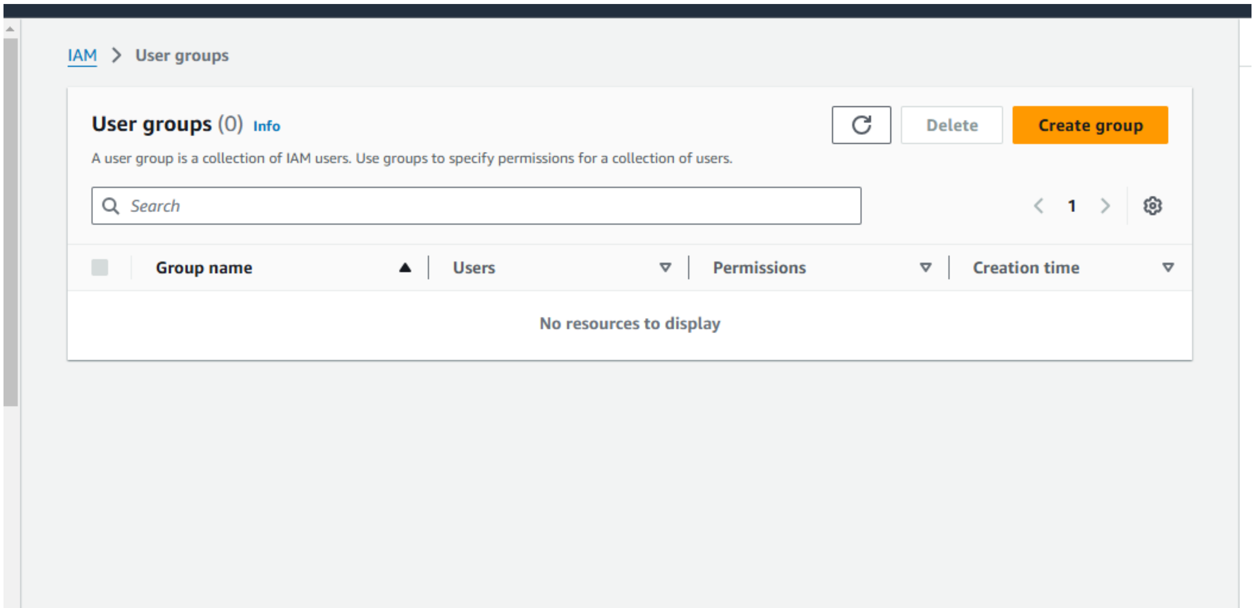
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (1)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path	Groups	Last activity	MFA	Password age
□	Rakesh	/	0	-	-	-

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

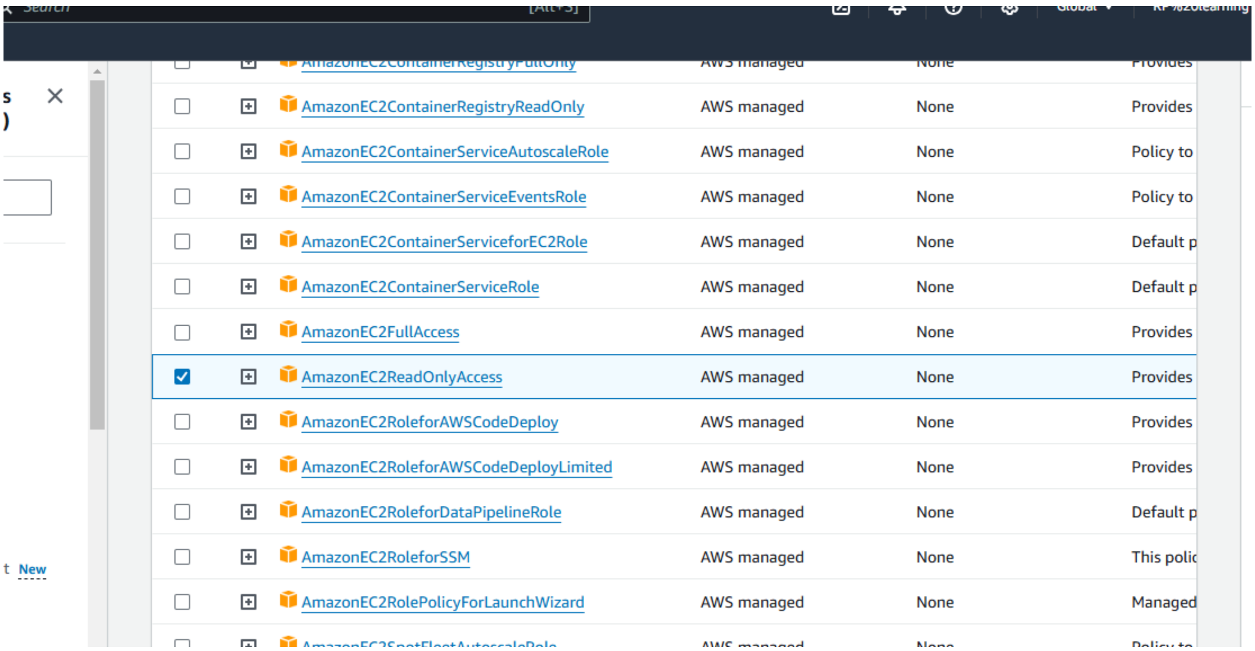


IAM > User groups

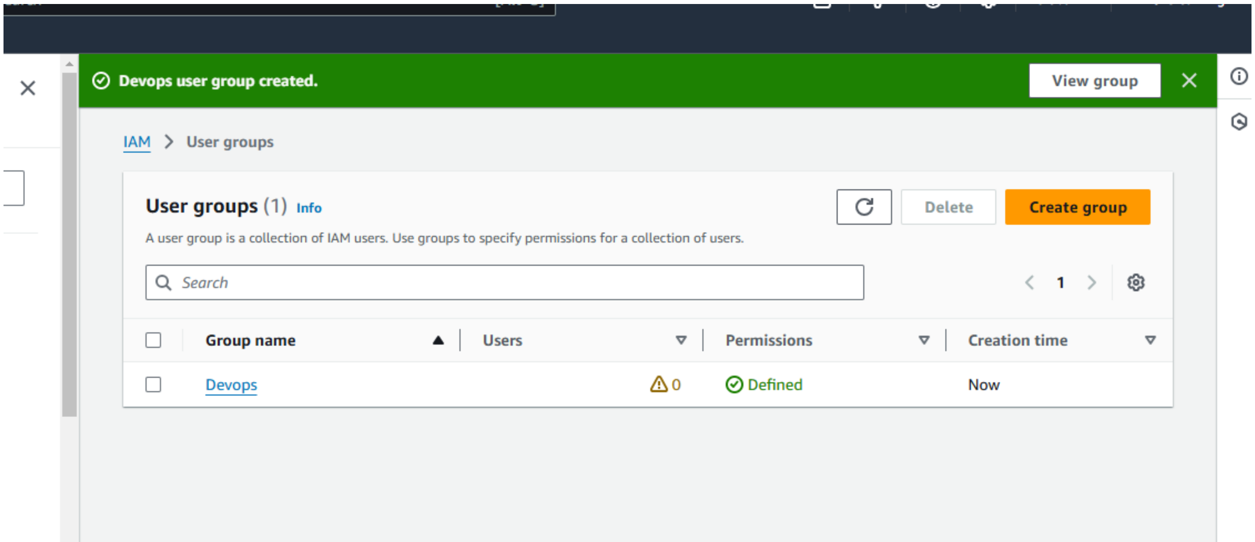
User groups (0) Info

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				



□	⊞	AmazonEC2ContainerRegistryPullOnly	AWS managed	None	Provides
□	⊞	AmazonEC2ContainerRegistryReadOnly	AWS managed	None	Provides
□	⊞	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	None	Policy to
□	⊞	AmazonEC2ContainerServiceEventsRole	AWS managed	None	Policy to
□	⊞	AmazonEC2ContainerServiceforEC2Role	AWS managed	None	Default p
□	⊞	AmazonEC2ContainerServiceRole	AWS managed	None	Default p
□	⊞	AmazonEC2FullAccess	AWS managed	None	Provides
☑	⊞	AmazonEC2ReadOnlyAccess	AWS managed	None	Provides
□	⊞	AmazonEC2RoleforAWSCodeDeploy	AWS managed	None	Provides
□	⊞	AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	None	Provides
□	⊞	AmazonEC2RoleforDataPipelineRole	AWS managed	None	Default p
□	⊞	AmazonEC2RoleforSSM	AWS managed	None	This polic
□	⊞	AmazonEC2RolePolicyForLaunchWizard	AWS managed	None	Managed
□	⊞	AmazonEC2SpotFleetAutoscaleRole	AWS managed	None	Policy to



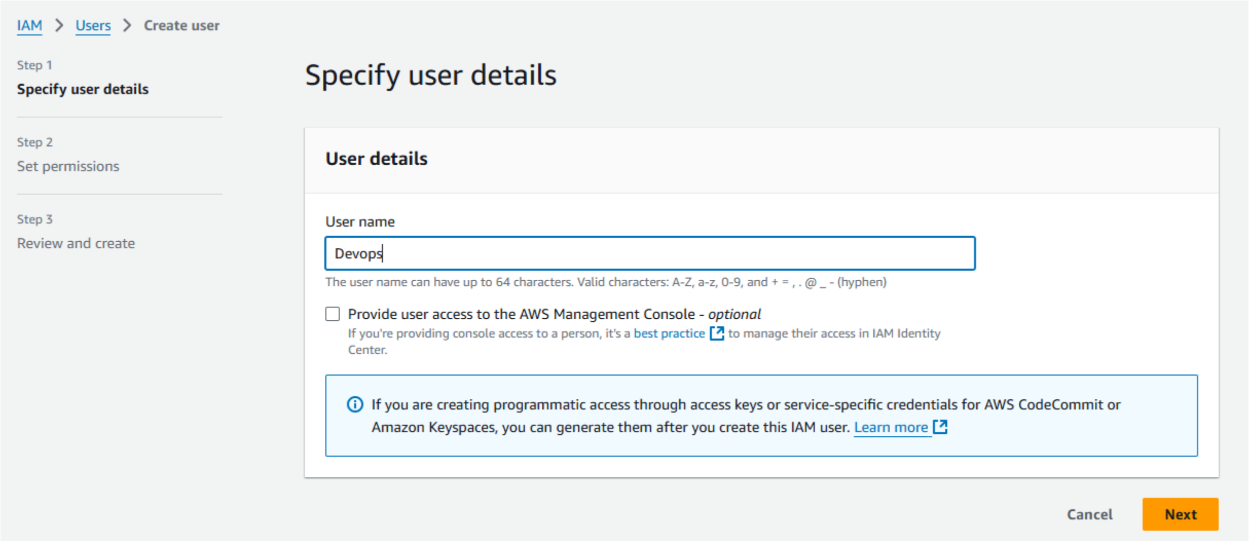
Devops user group created.

User groups (1)

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
□	Devops	⚠ 0	✓ Defined	Now

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



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

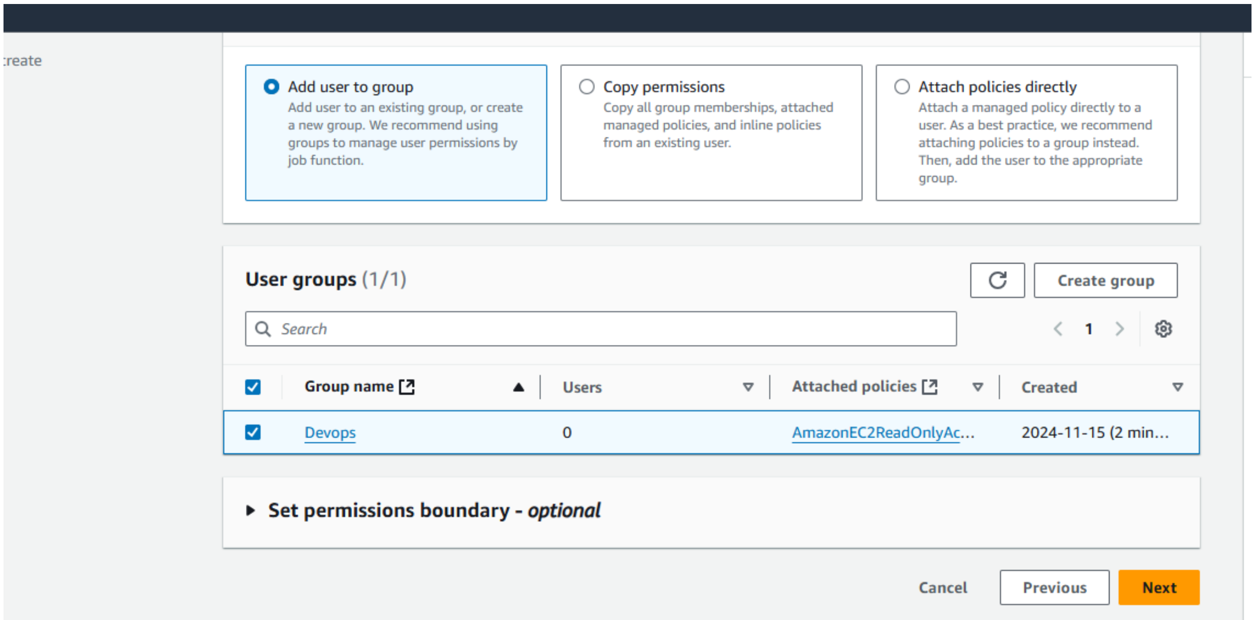
User name

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.

ⓘ 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



reate

● 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.

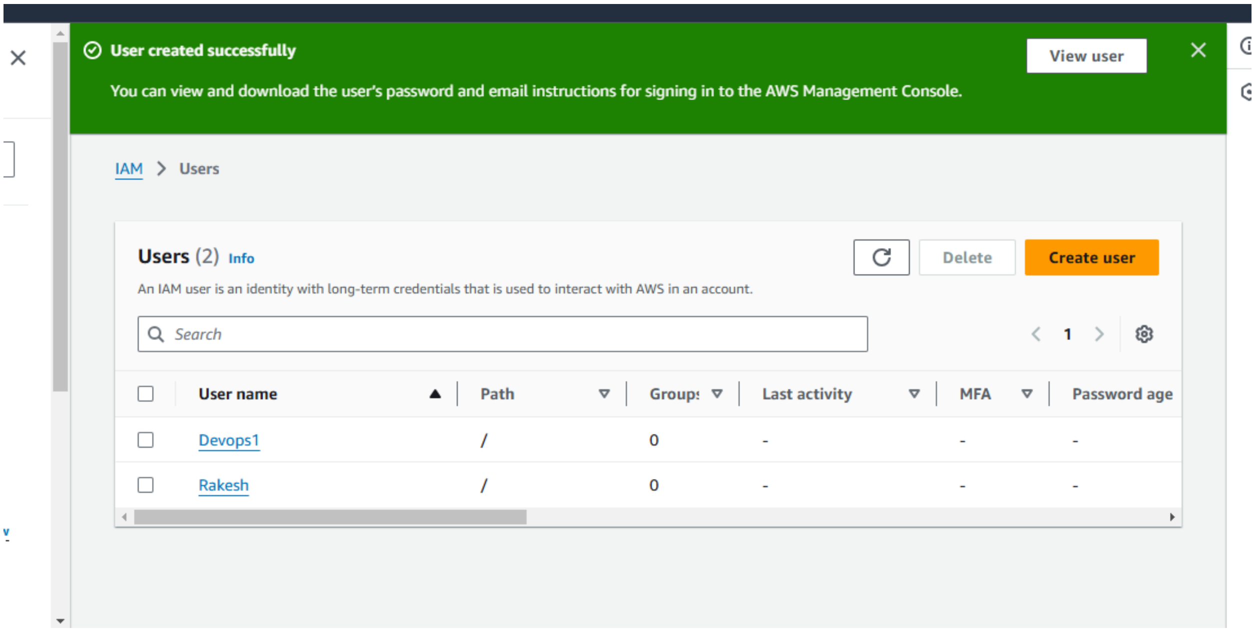
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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 (1/1)

☑	Group name	Users	Attached policies	Created
☑	Devops	0	AmazonEC2ReadOnlyAc...	2024-11-15 (2 min...

▸ **Set permissions boundary - *optional***



User created successfully

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

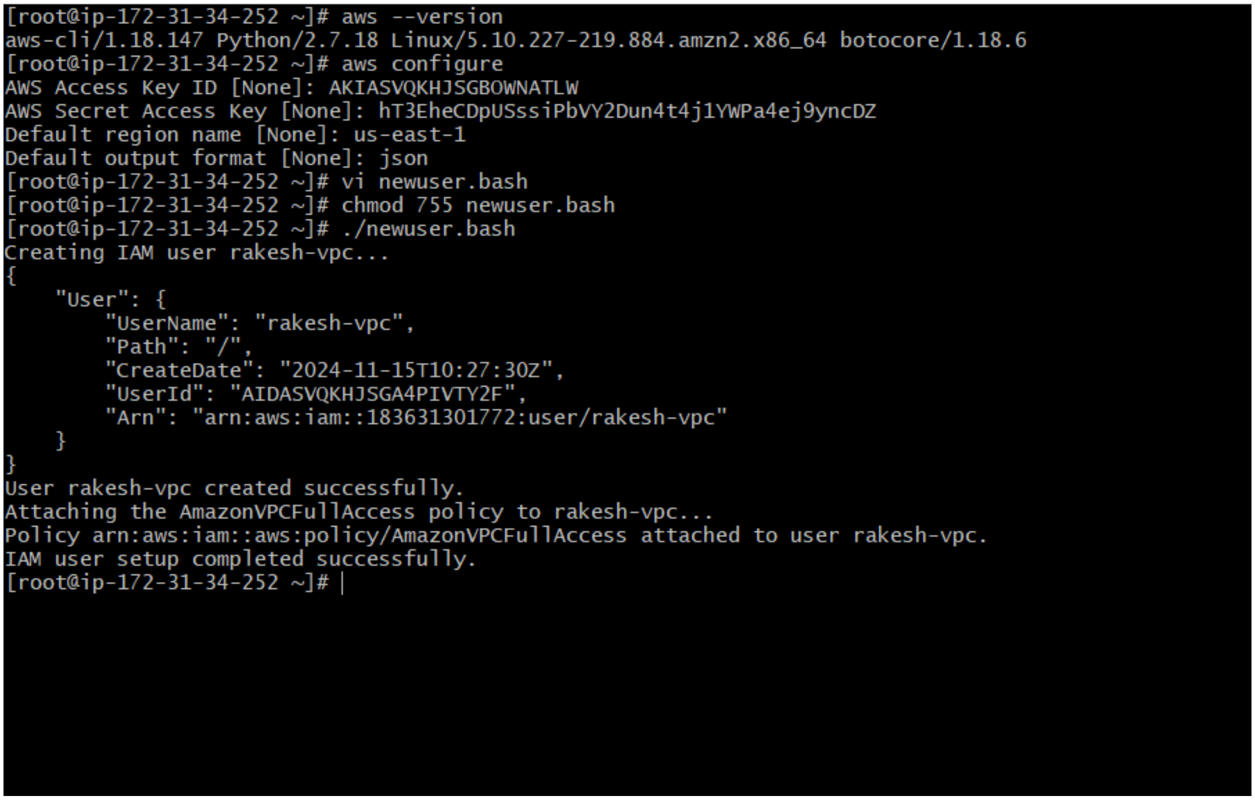
IAM > Users

Users (2) Info

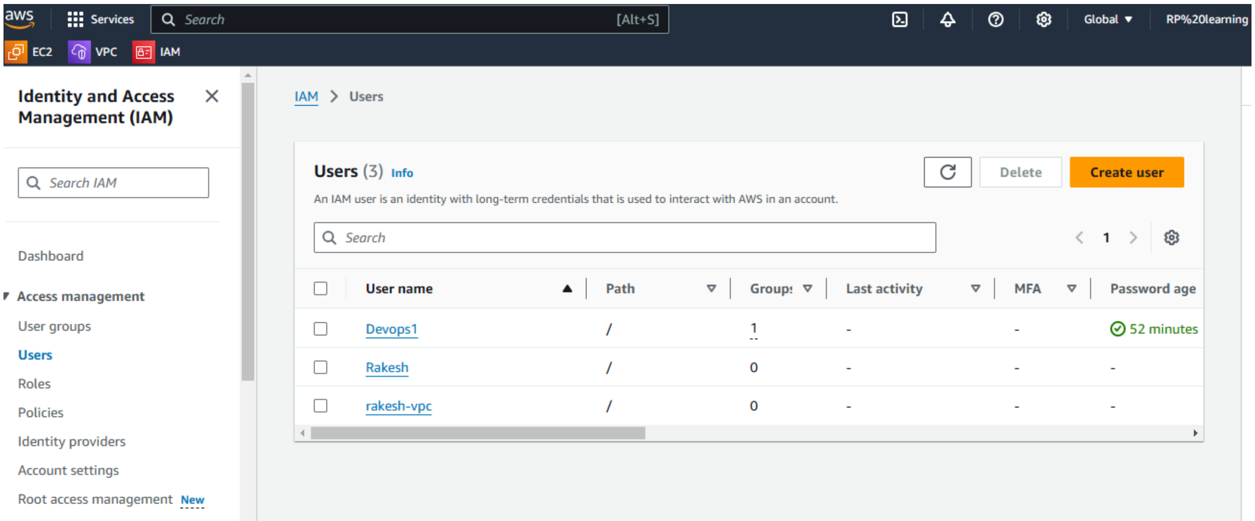
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Groups	Last activity	MFA	Password age
□	Devops1	/	0	-	-	-
□	Rakesh	/	0	-	-	-

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



```
[root@ip-172-31-34-252 ~]# aws --version
aws-cli/1.18.147 Python/2.7.18 Linux/5.10.227-219.884.amzn2.x86_64 botocore/1.18.6
[root@ip-172-31-34-252 ~]# aws configure
AWS Access Key ID [None]: AKIASVQKHJSGBOWNATLW
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
[root@ip-172-31-34-252 ~]# vi newuser.bash
[root@ip-172-31-34-252 ~]# chmod 755 newuser.bash
[root@ip-172-31-34-252 ~]# ./newuser.bash
Creating IAM user rakesh-vpc...
{
    "User": {
        "UserName": "rakesh-vpc",
        "Path": "/",
        "CreateDate": "2024-11-15T10:27:30Z",
        "UserId": "AIDASVQKHJSGA4PIVTY2F",
        "Arn": "arn:aws:iam::183631301772:user/rakesh-vpc"
    }
}
User rakesh-vpc created successfully.
Attaching the AmazonVPCFullAccess policy to rakesh-vpc...
Policy arn:aws:iam::aws:policy/AmazonVPCFullAccess attached to user rakesh-vpc.
IAM user setup completed successfully.
[root@ip-172-31-34-252 ~]# |
```

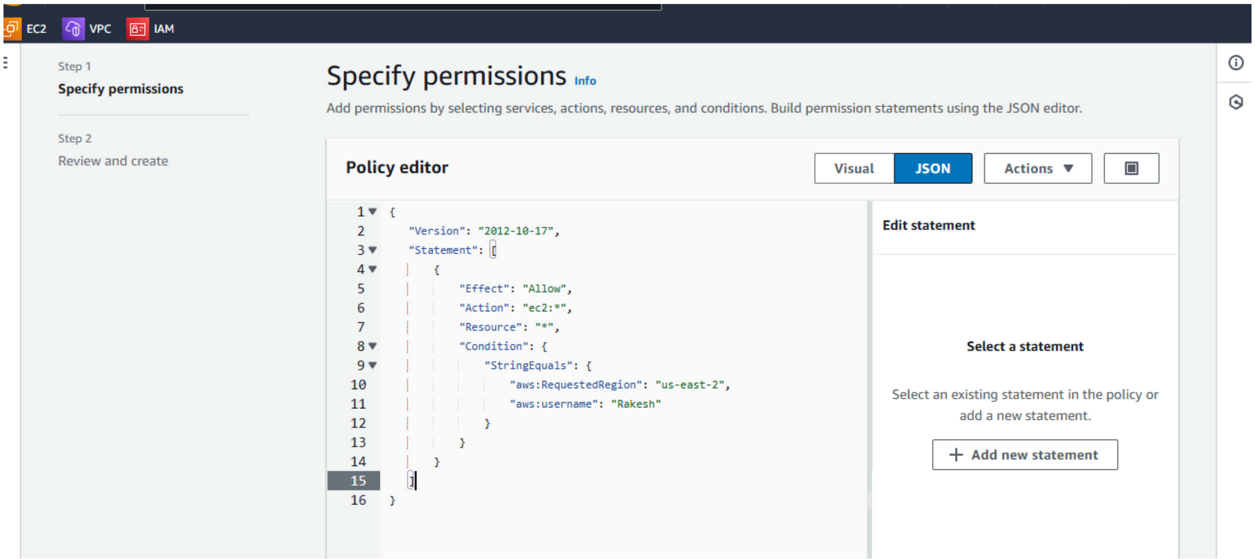


Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path	Groups	Last activity	MFA	Password age
□	Devops1	/	1	-	-	✓ 52 minutes
□	Rakesh	/	0	-	-	-
□	rakesh-vpc	/	0	-	-	-

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



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

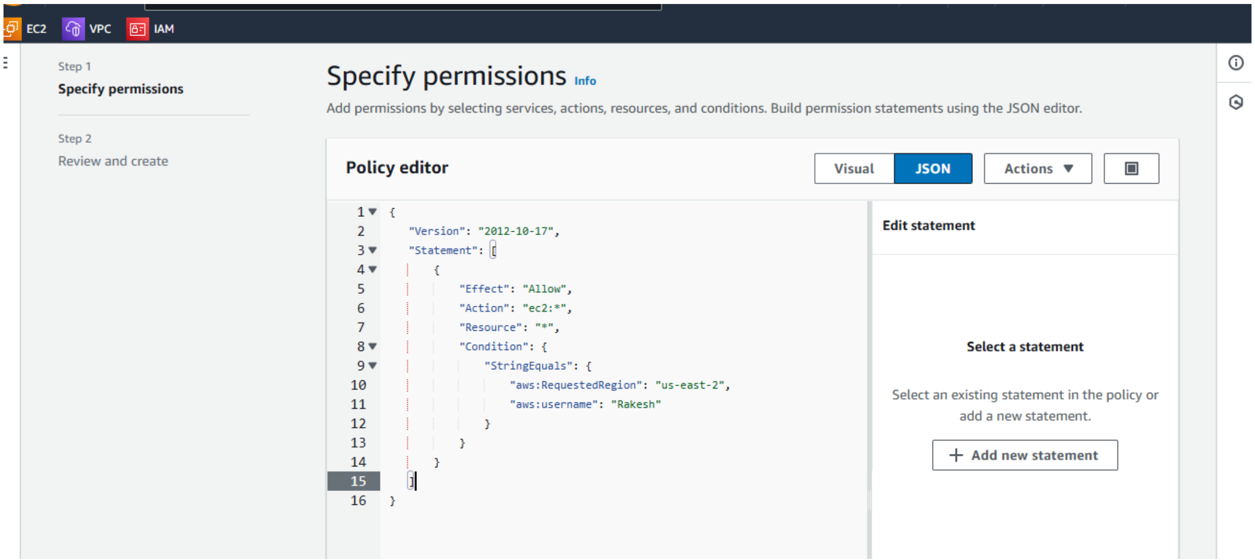
Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": "us-east-2",
                    "aws:username": "Rakesh"
                }
            }
        }
    ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.


EC2
VPC
IAM
Step 1
Specify permissions
Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual
JSON
Actions ▼

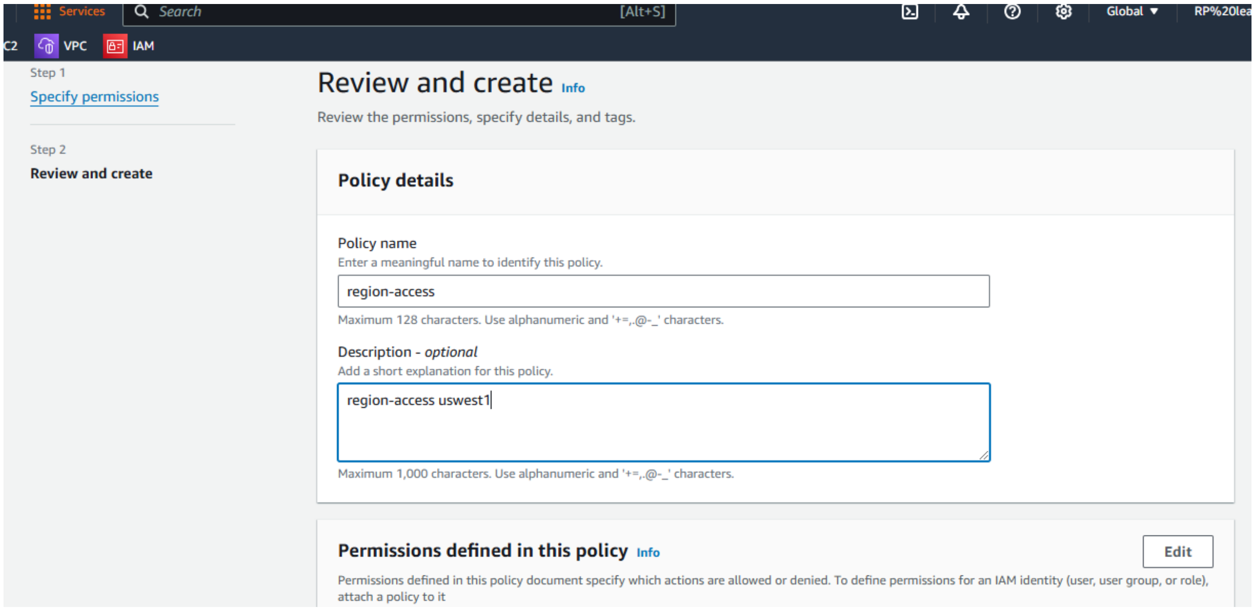
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": "us-east-2",
                    "aws:username": "Rakesh"
                }
            }
        }
    ]
}

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

region-access

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

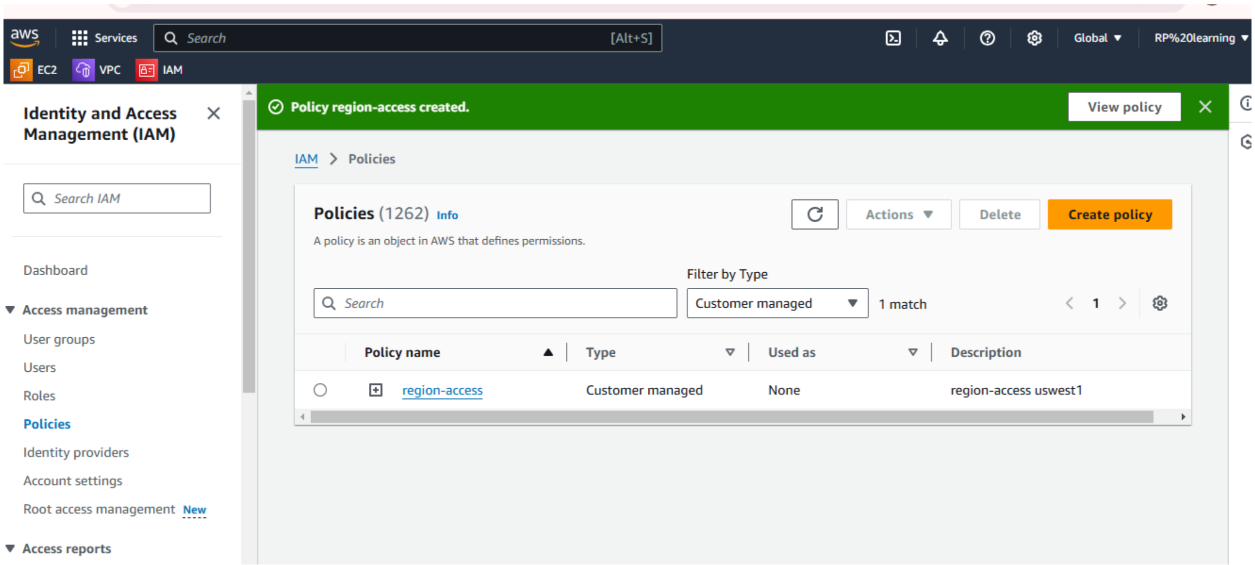
Add a short explanation for this policy.

region-access uswest1

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

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



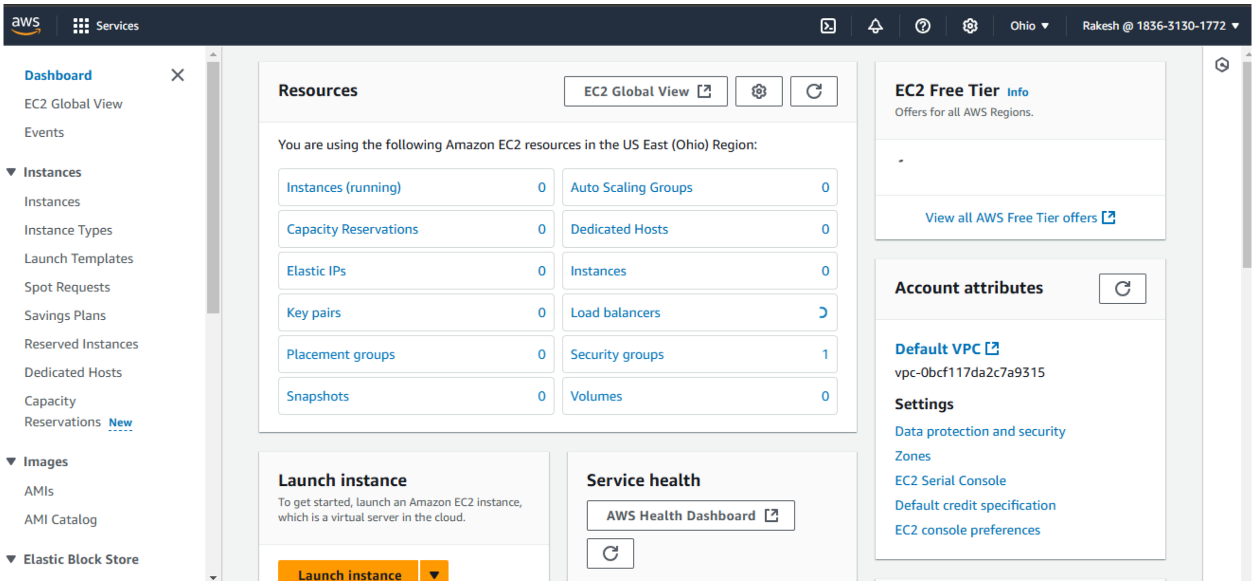
Policy region-access created.

Policies (1262)

A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed ▼ — 1 match

Policy name	Type	Used as	Description
○ region-access	Customer managed	None	region-access uswest1



Resources

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

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

EC2 Free Tier

Offers for all AWS Regions.

Account attributes

Default VPC

vpc-0bcf117da2c7a9315

Settings

Data protection and security

Zones

EC2 Serial Console

Default credit specification

EC2 console preferences

Launch instance

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

Service health

6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B.