INTRODUCTION TO VIRTUALIZATION AND CLOUD COMPUTING

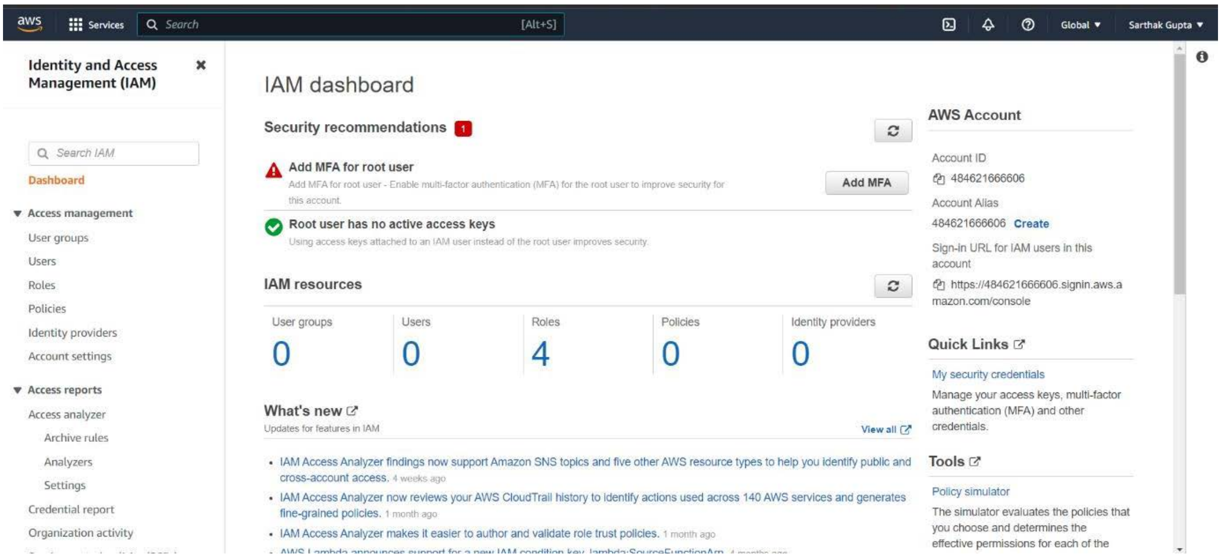
NAME- Shubhi Dixit

BATCH- 05

SAP ID- 500094571

Identity Access Management (IAM) in AWS

Creating a User



IAM dashboard

Security recommendations 1

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.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	4	0	0

What's new

Updates for features in IAM

- IAM Access Analyzer findings now support Amazon SNS topics and five other AWS resource types to help you identify public and cross-account access. 4 weeks ago
- IAM Access Analyzer now reviews your AWS CloudTrail history to identify actions used across 140 AWS services and generates fine-grained policies. 1 month ago
- IAM Access Analyzer makes it easier to author and validate role trust policies. 1 month ago
- AWS Lambda announces support for a new IAM condition key, lambda:SourceFunctionArn. 4 months ago

AWS Account

Account ID

484621666606

Account Alias

484621666606

Sign-in URL for IAM users in this account

https://484621666606.signin.aws.amazon.com/console

Quick Links

My security credentials

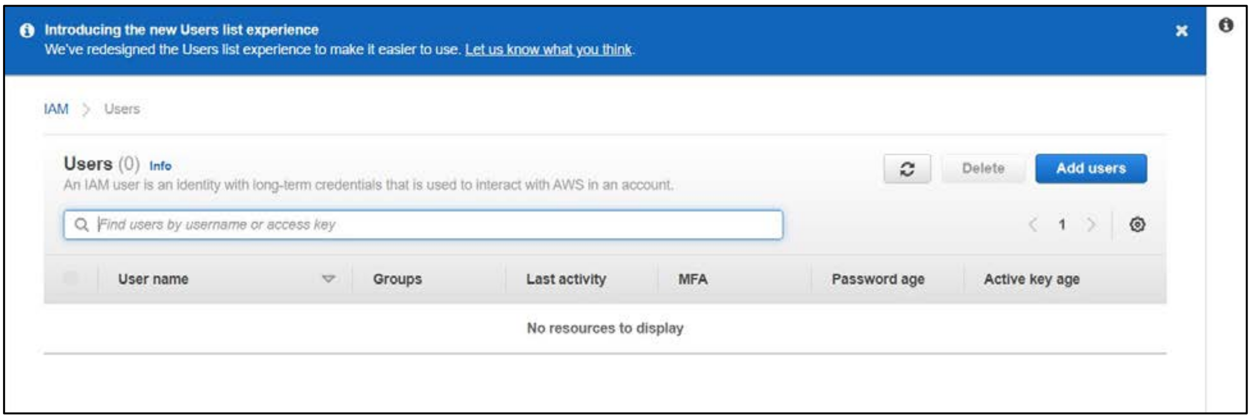
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the

Step 1: In the Dashboard of IAM select ‘Users’ from the left panel and go to ‘ADD USER’



Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. Let us know what you think.

IAM > Users

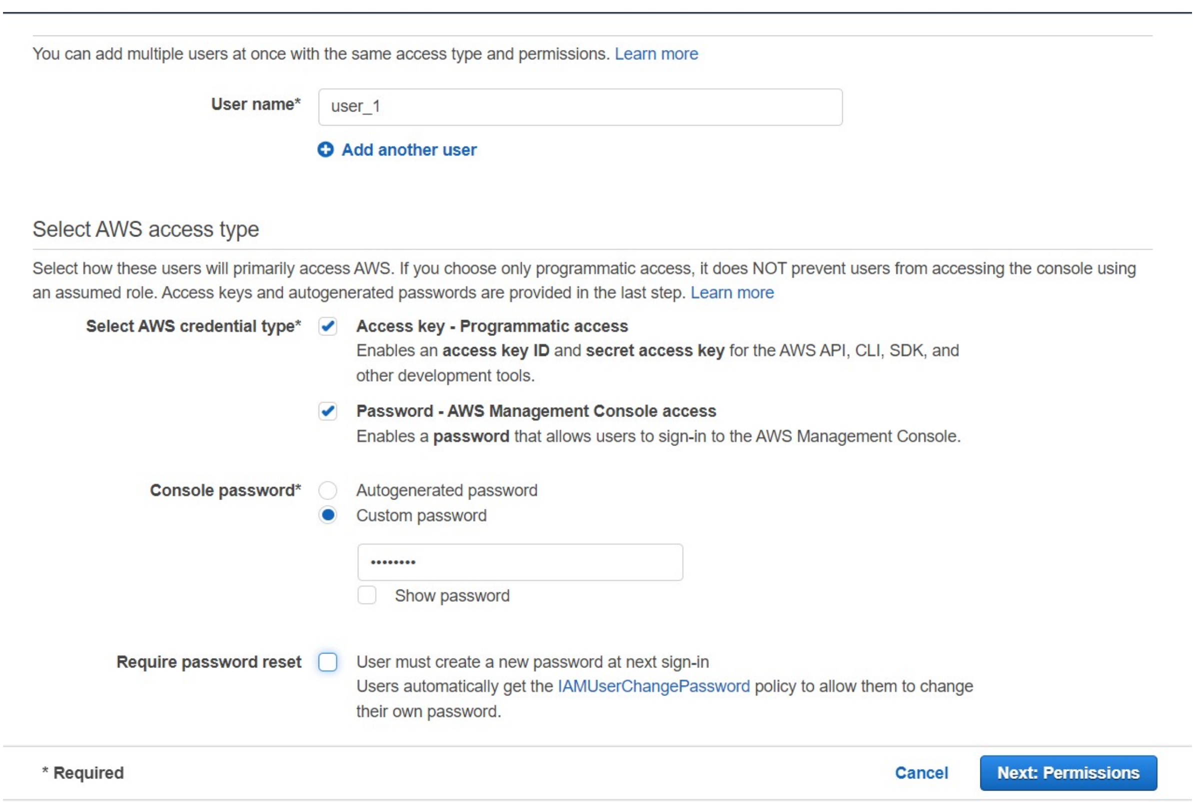
Users (0) Info

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

User name	Groups	Last activity	MFA	Password age	Active key age

No resources to display

Step 2: Type the name, check the below options and create a custom password. Then click next.



You can add multiple users at once with the same access type and permissions. Learn more

User name* user_1

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.

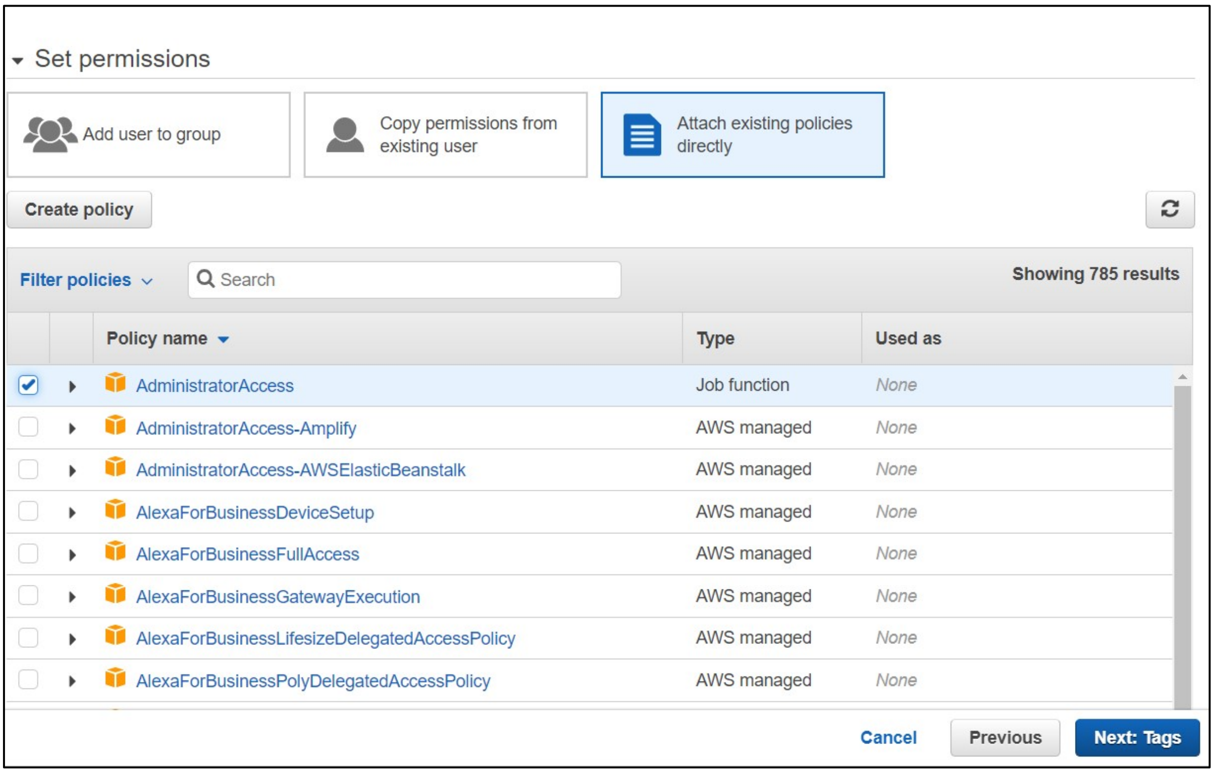
Console password* ○ Autogenerated password
● Custom password

••••••••

□ Show password

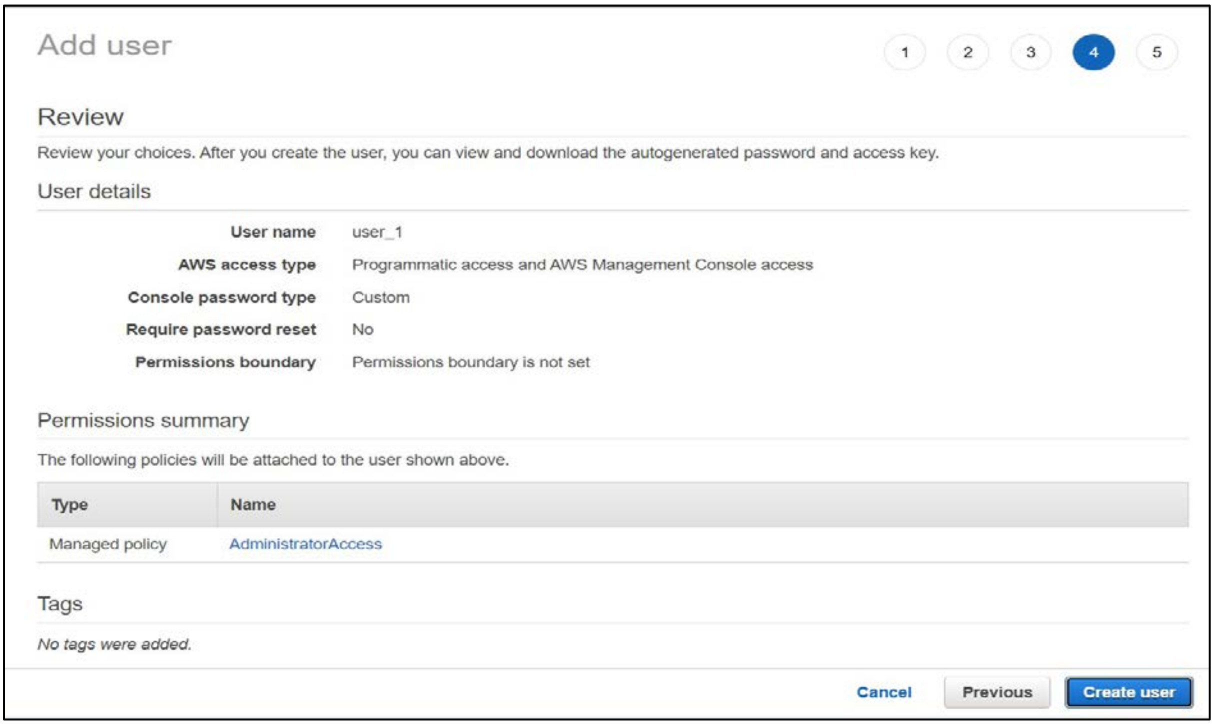
Require password reset □ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required



	Policy name	Type	Used as
☑	AdministratorAccess	Job function	None
□	AdministratorAccess-Amplify	AWS managed	None
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
□	AlexaForBusinessDeviceSetup	AWS managed	None
□	AlexaForBusinessFullAccess	AWS managed	None
□	AlexaForBusinessGatewayExecution	AWS managed	None
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None

Click on create user



Review

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

User details

User name	user_1
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

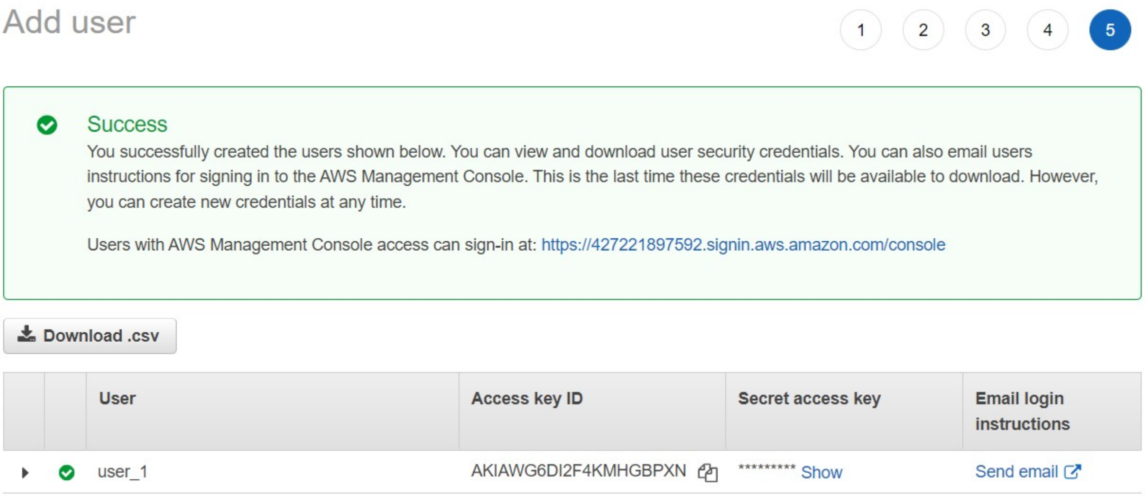
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess

Tags

No tags were added.

Step 4: Copy the Access Key ID and Secret Access Key and save it as it appears only once.



Add user

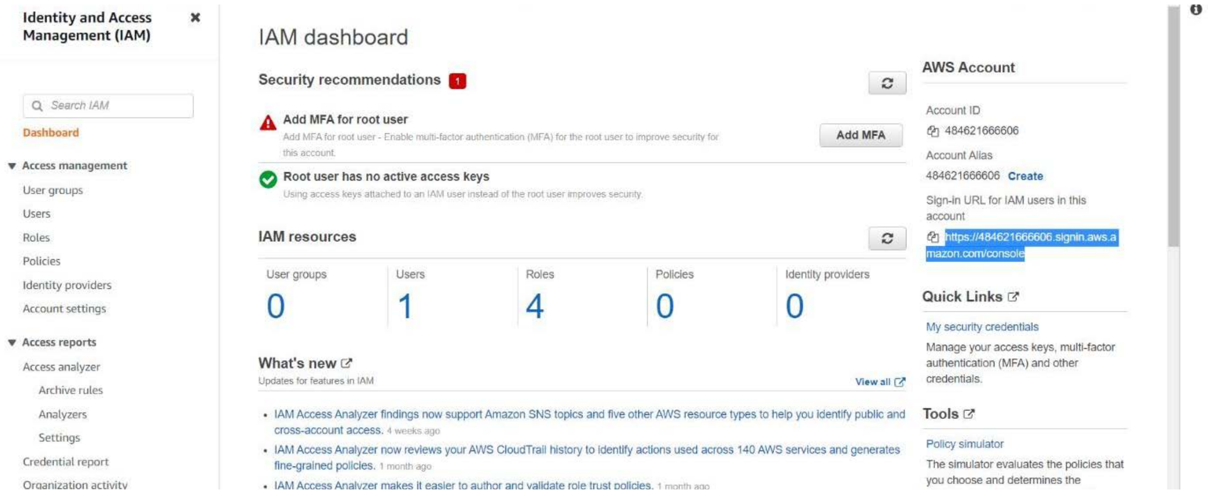
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://427221897592.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions
▸	✓	user_1	AKIAWG6DI2F4KMHGBPXN	********* Show	Send email

Step 5: Copy the selected URL from the dashboard and login as the created user.



IAM dashboard

Security recommendations 1

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.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	1	4	0	0

What's new

Updates for features in IAM

- IAM Access Analyzer findings now support Amazon SNS topics and five other AWS resource types to help you identify public and cross-account access. 4 weeks ago
- IAM Access Analyzer now reviews your AWS CloudTrail history to identify actions used across 140 AWS services and generates fine-grained policies. 1 month ago
- IAM Access Analyzer makes it easier to author and validate role trust policies. 1 month ago

AWS Account

Account ID: 484621666606

Account Alias: 484621666606 Create

Sign-in URL for IAM users in this account: https://484621666606.signin.aws.amazon.com/console

Quick Links

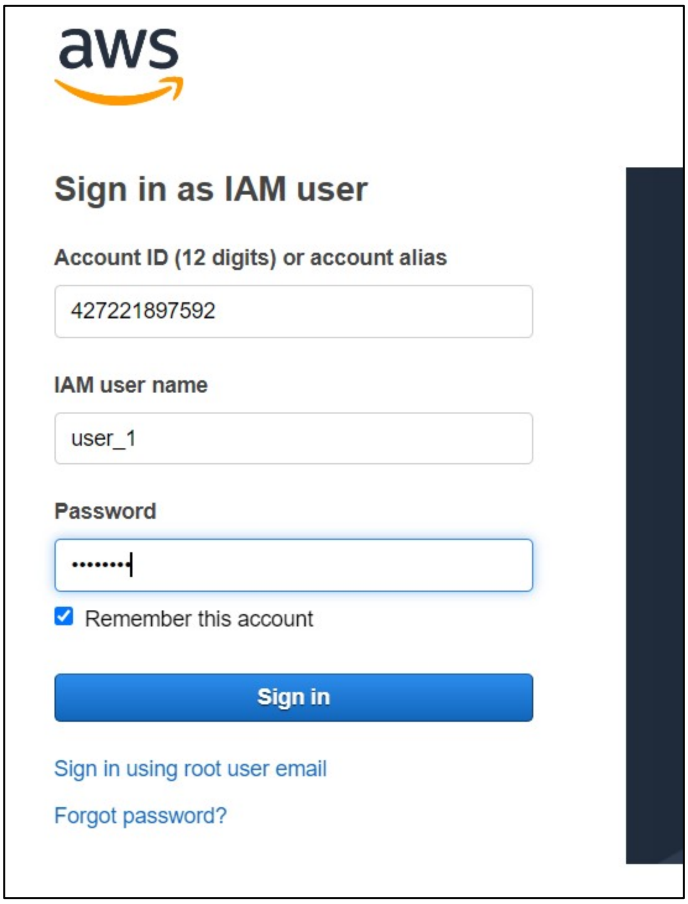
My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the



Sign in as IAM user

Account ID (12 digits) or account alias

427221897592

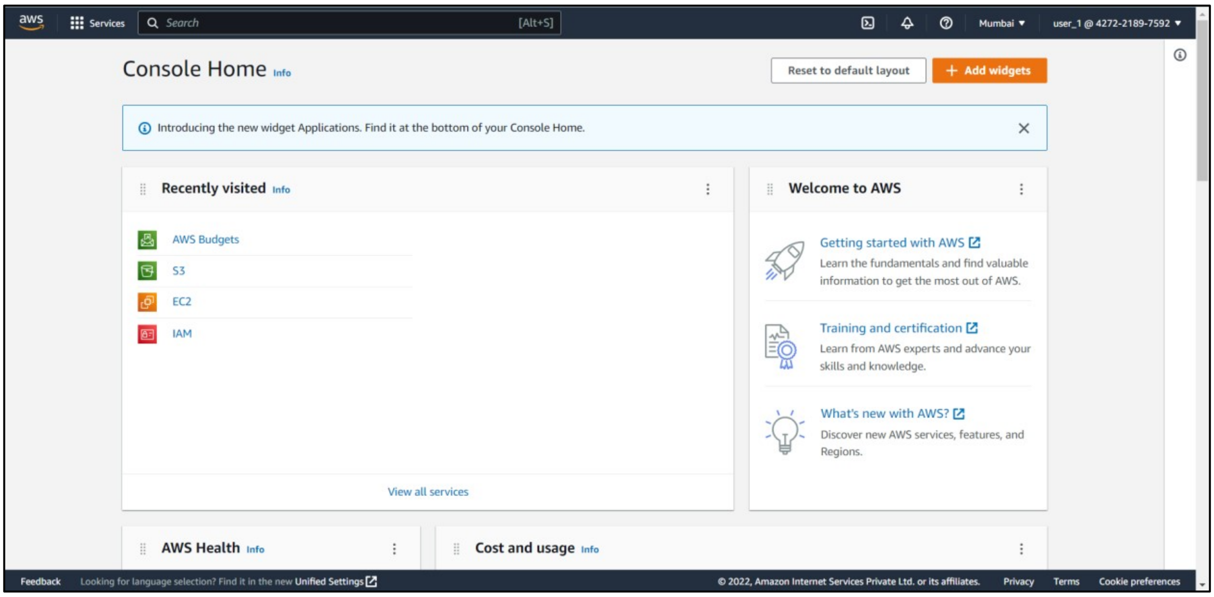
IAM user name

user_1

Password

••••••••

☑ Remember this account



Console Home Info

Introducing the new widget Applications. Find it at the bottom of your Console Home.

Recently visited Info

- AWS Budgets
- S3
- EC2
- IAM

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.

AWS Health Info

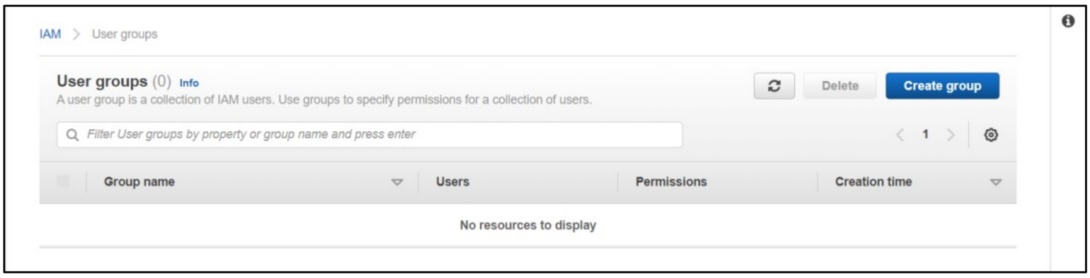
Cost and usage Info

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Creating a Group

Step 1: In the Dashboard of IAM select ‘User groups’ from the leftpanel and go to ‘Create group’.



IAM > User groups

User groups (0) Info

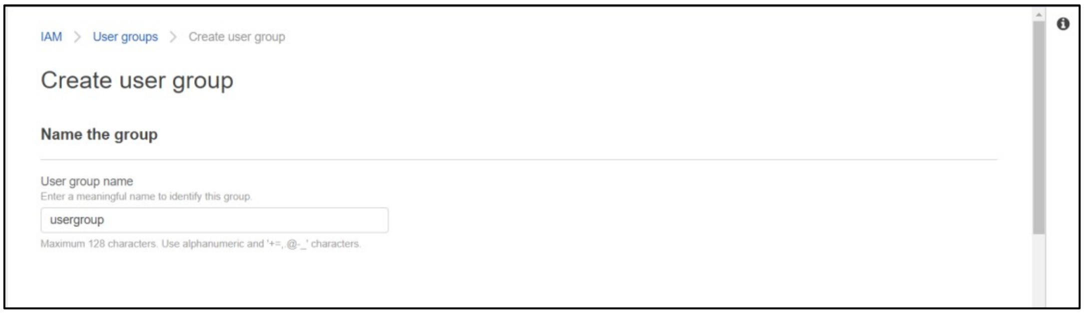
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Delete
Create group
Filter User groups by property or group name and press enter
1

Group name	Users	Permissions	Creation time

No resources to display

Step 2: Type a group name and choose a policy you want to attach and click on create group.



IAM > User groups > Create user group

Create user group

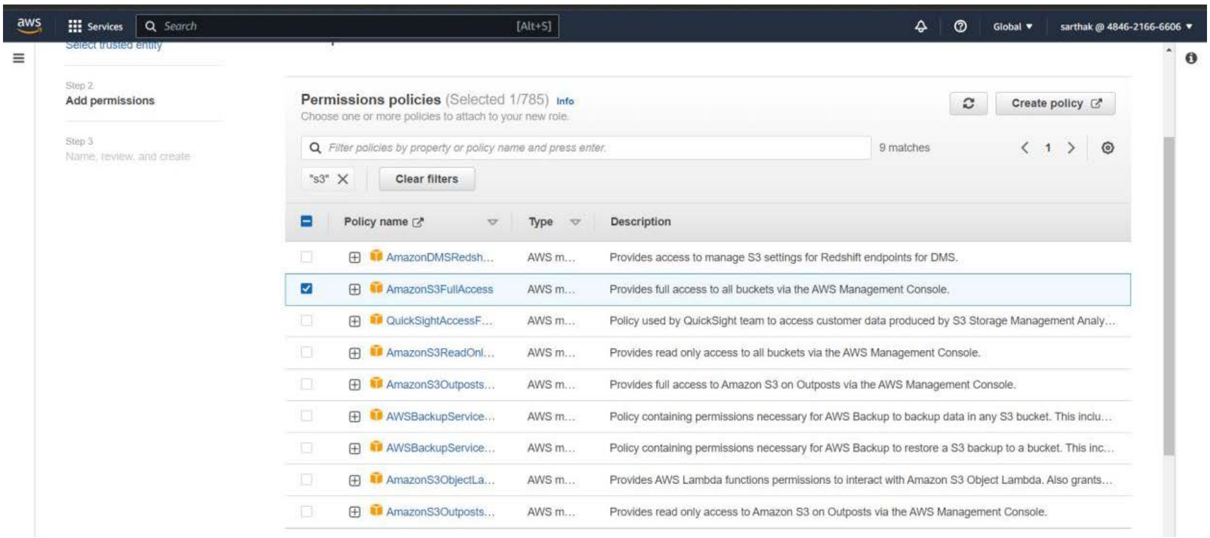
Name the group

User group name

Enter a meaningful name to identify this group.

usergroup

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



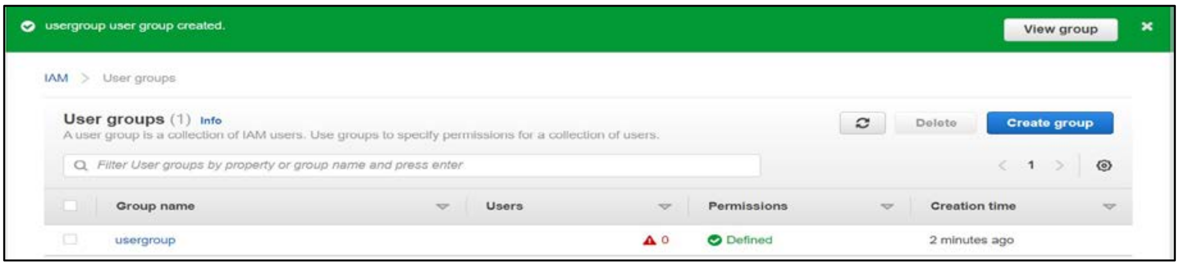
Permissions policies (Selected 1/785) Info

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

Filter policies by property or policy name and press enter.   9 matches

"s3" ✕   Clear filters

▬	Policy name	Type	Description
□	AmazonDMSRedsh...	AWS m...	Provides access to manage S3 settings for Redshift endpoints for DMS.
☑	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the AWS Management Console.
□	QuickSightAccessF...	AWS m...	Policy used by QuickSight team to access customer data produced by S3 Storage Management Analy...
□	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets via the AWS Management Console.
□	AmazonS3Outposts...	AWS m...	Provides full access to Amazon S3 on Outposts via the AWS Management Console.
□	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This inclu...
□	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to restore a S3 backup to a bucket. This inc...
□	AmazonS3ObjectLa...	AWS m...	Provides AWS Lambda functions permissions to interact with Amazon S3 Object Lambda. Also grants...
□	AmazonS3Outposts...	AWS m...	Provides read only access to Amazon S3 on Outposts via the AWS Management Console.



usergroup user group created.

IAM > User groups

User groups (1) Info

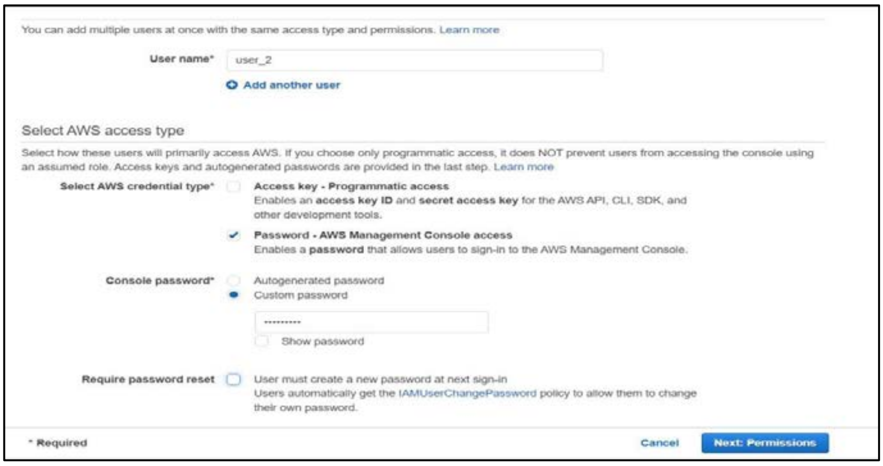
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Delete
Create group
Filter User groups by property or group name and press enter
< 1 >

□	Group name	Users	Permissions	Creation time
□	usergroup	⚠ 0	✓ Defined	2 minutes ago

User group is created successfully

Step 3: Now go to users again and create another user.



You can add multiple users at once with the same access type and permissions. Learn more

User name* user_2

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

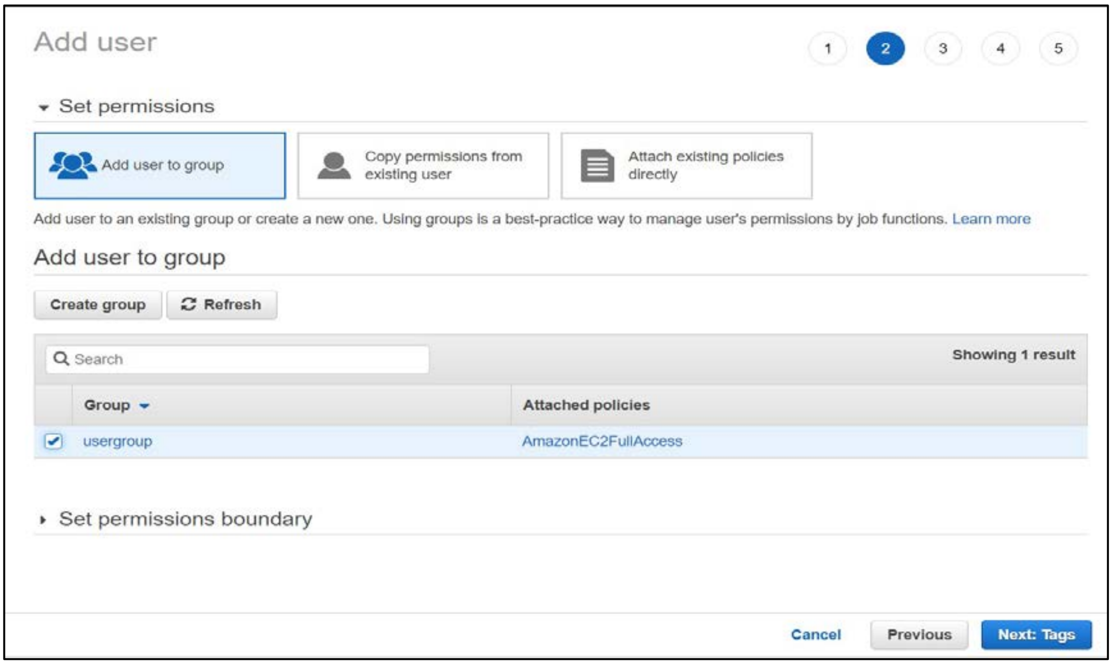
  ••••••••••

  □ 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

Step 4: Click on add user to group in permissions window. Select the user you want to add to the group.



Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

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

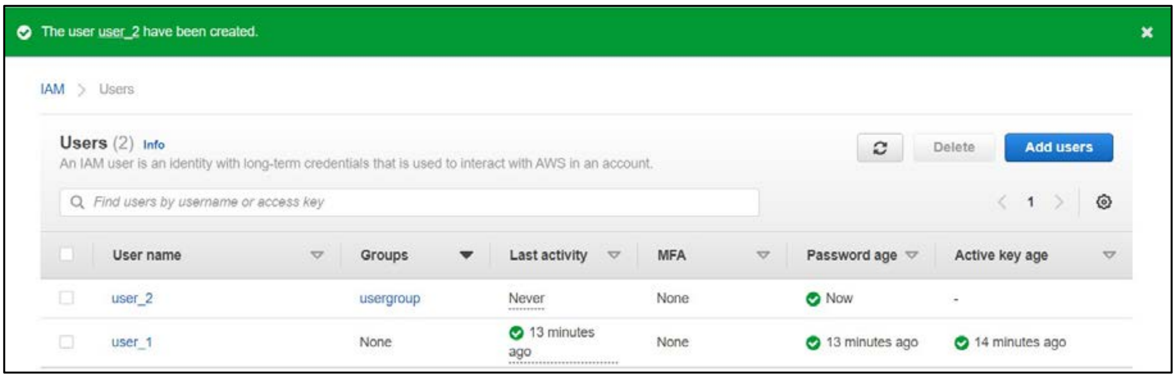
Add user to group

Showing 1 result

	Group	Attached policies
☑	usergroup	AmazonEC2FullAccess

Set permissions boundary

Second User has been successfully created



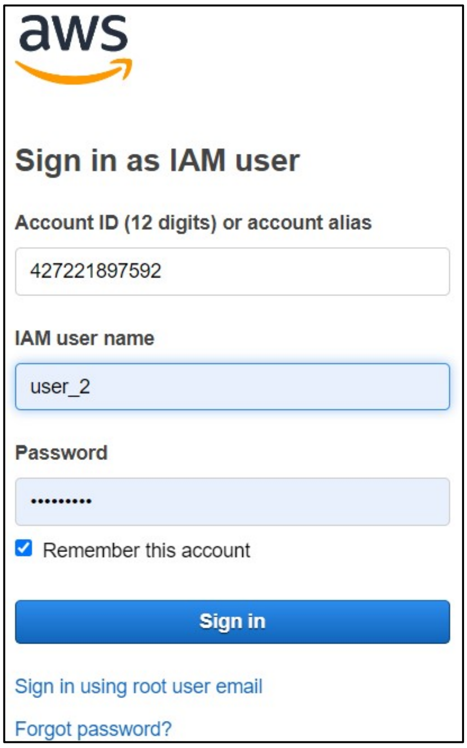
The user user_2 have been created.

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	Groups	Last activity	MFA	Password age	Active key age
□	user_2	usergroup	Never	None	✓ Now	-
□	user_1	None	✓ 13 minutes ago	None	✓ 13 minutes ago	✓ 14 minutes ago

Step 5: Login as a user who is in the group **[Do not login as the user who has administrator access].**



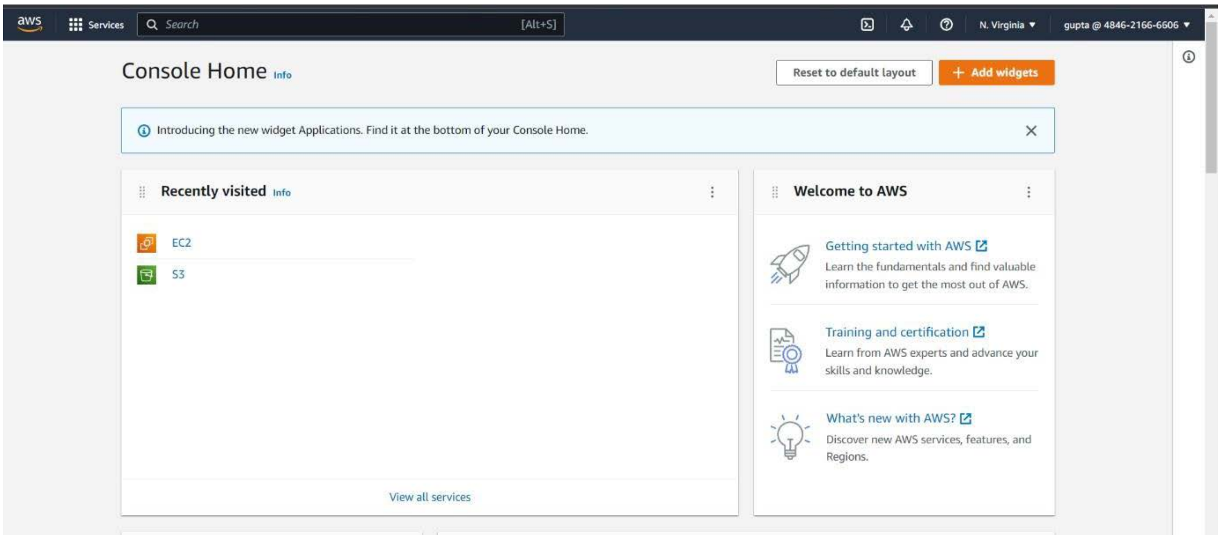
Sign in as IAM user

Account ID (12 digits) or account alias: 427221897592

IAM user name: user_2

Password: •••••••••

☑ Remember this account



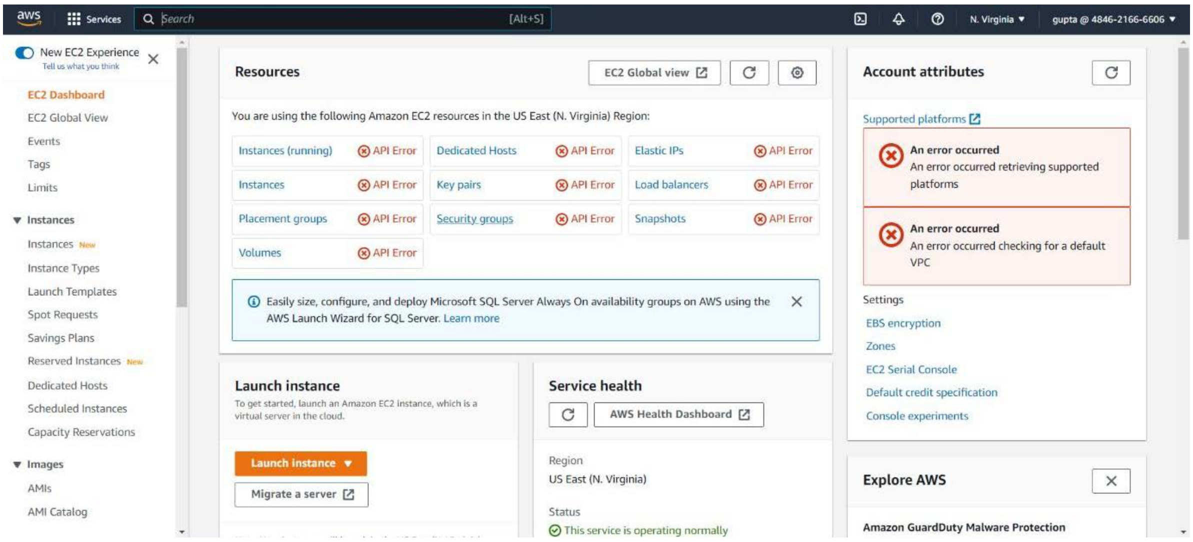
Introducing the new widget Applications. Find it at the bottom of your Console Home.

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.

The user will not be able to access services other than AWS S3



You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	⊗ API Error	Dedicated Hosts	⊗ API Error	Elastic IPs	⊗ API Error
Instances	⊗ API Error	Key pairs	⊗ API Error	Load balancers	⊗ API Error
Placement groups	⊗ API Error	Security groups	⊗ API Error	Snapshots	⊗ API Error
Volumes	⊗ API Error				

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

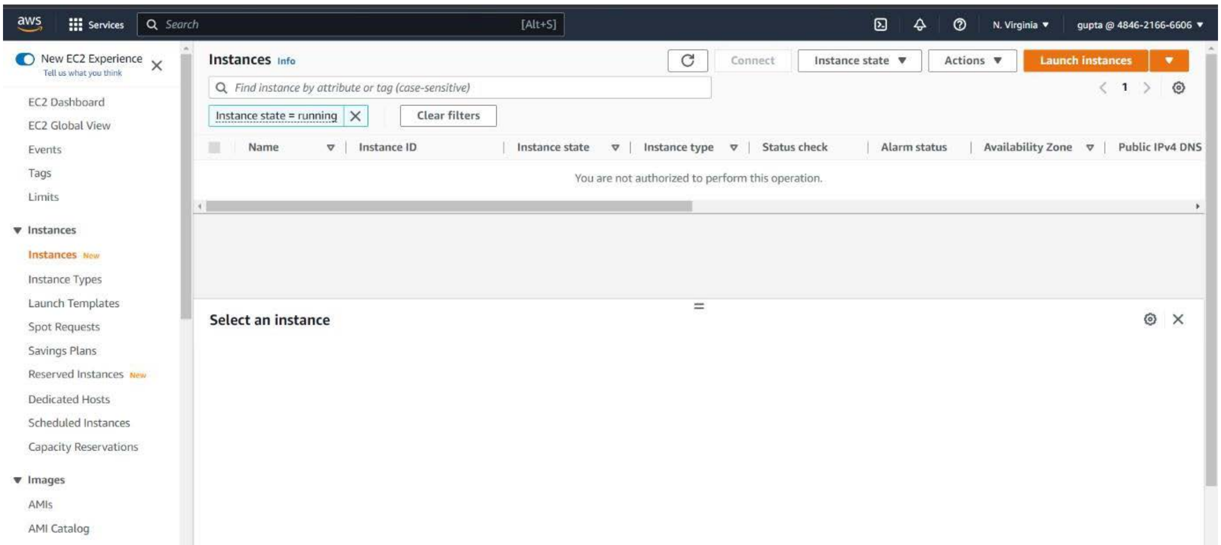
An error occurred
An error occurred retrieving supported platforms

An error occurred
An error occurred checking for a default VPC

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

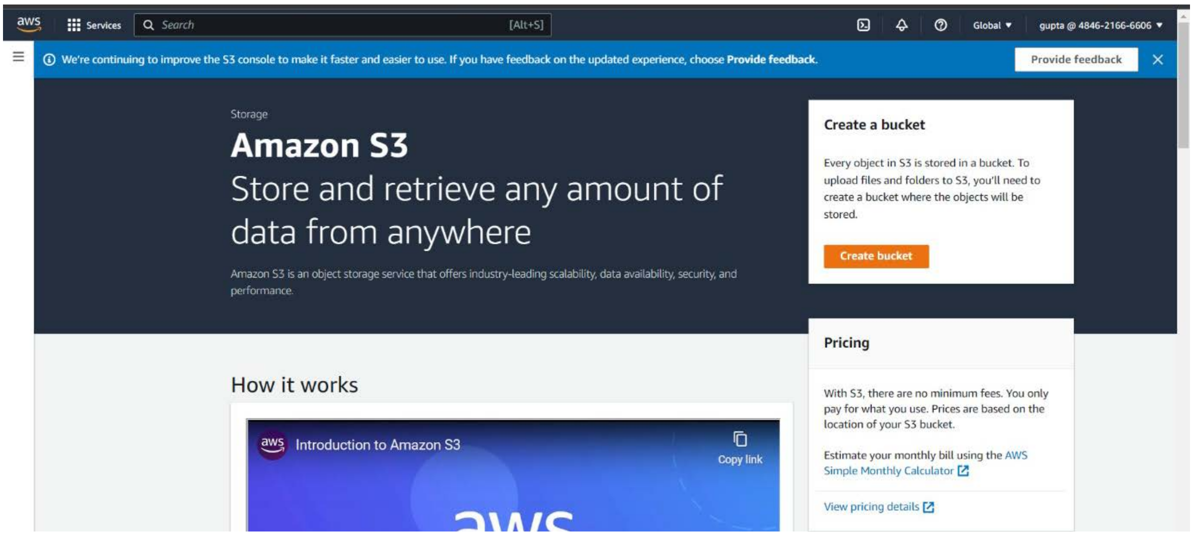
Region
US East (N. Virginia)

Status
This service is operating normally



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS

You are not authorized to perform this operation.



We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose **Provide feedback**.

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Pricing

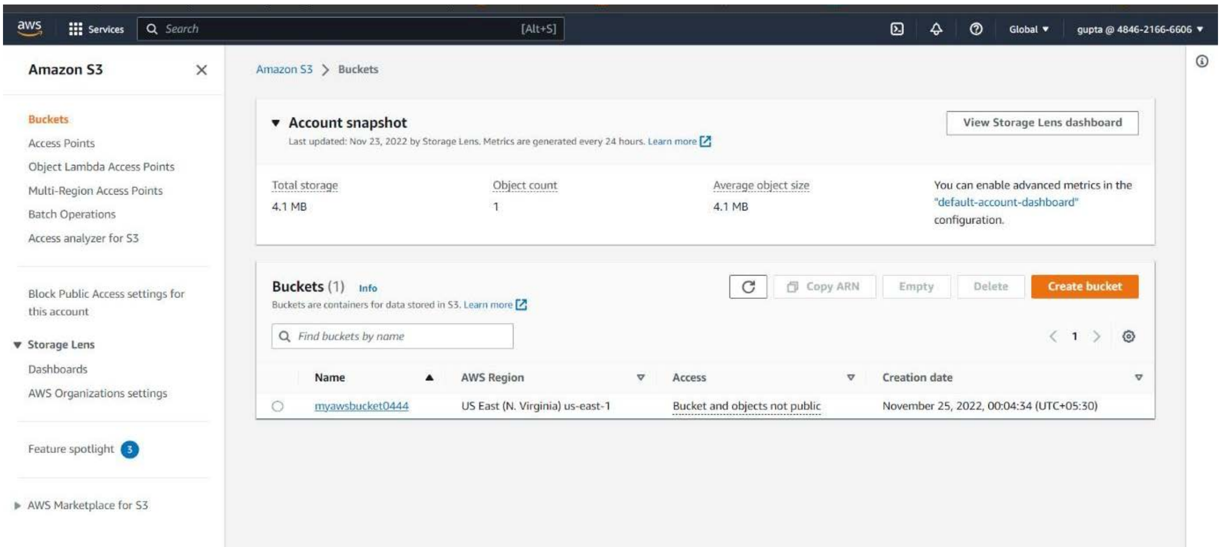
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

How it works

Introduction to Amazon S3



Account snapshot

Last updated: Nov 23, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more

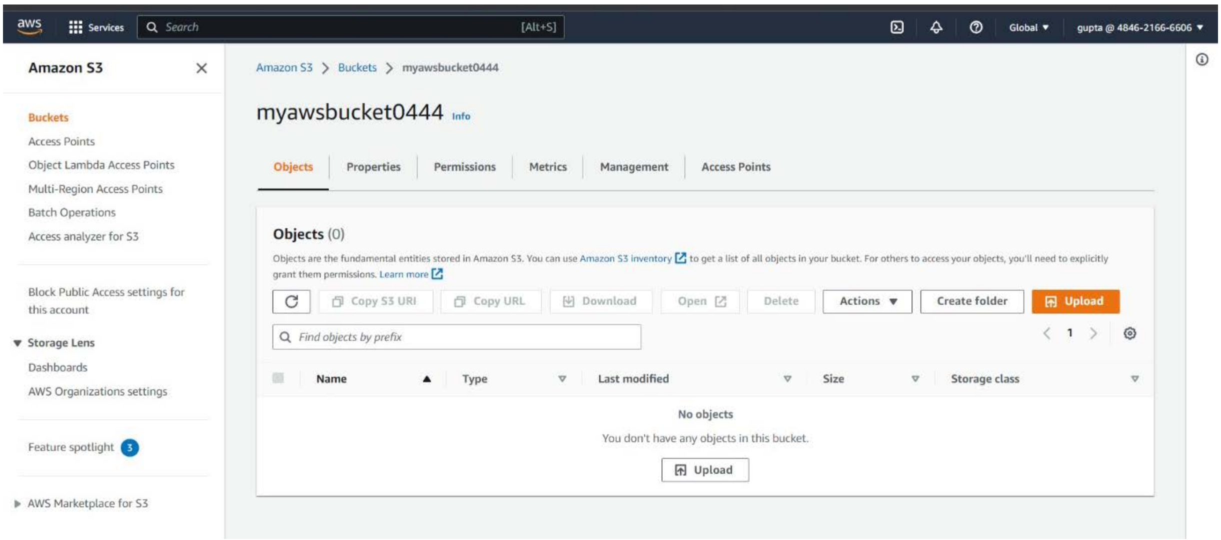
Total storage	Object count	Average object size
4.1 MB	1	4.1 MB

You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	myawsbucket0444	US East (N. Virginia) us-east-1	Bucket and objects not public	November 25, 2022, 00:04:34 (UTC+05:30)



myawsbucket0444 Info

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

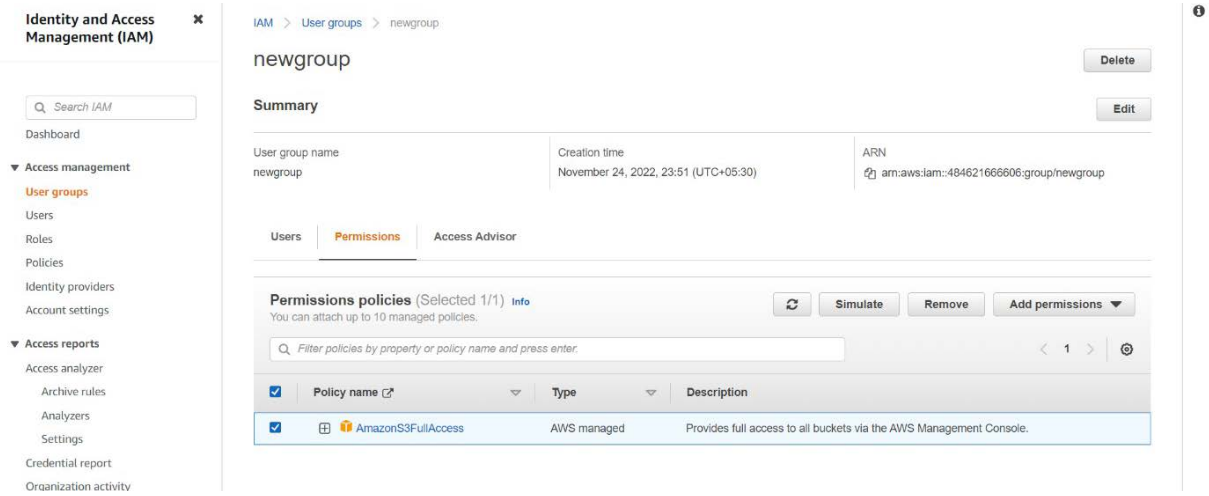
Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Upload

Now remove the 'AWSS3FullAccess' permission now.



newgroup

Summary

User group name
newgroup

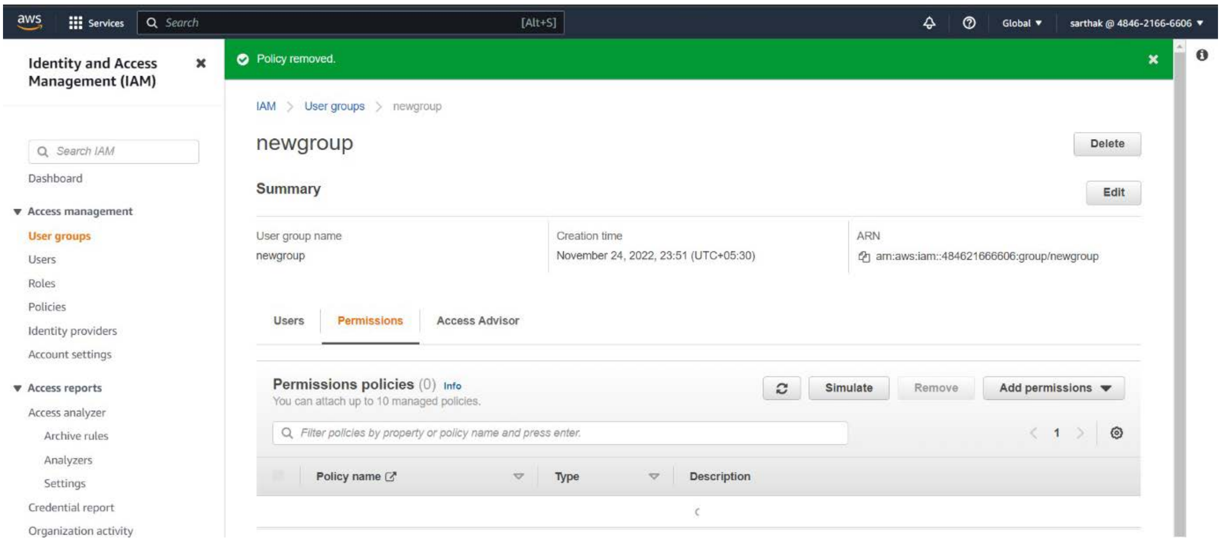
Creation time
November 24, 2022, 23:51 (UTC+05:30)

ARN
arn:aws:iam::484621666606:group/newgroup

Permissions policies (Selected 1/1) Info

You can attach up to 10 managed policies.

☑	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.



Policy removed.

newgroup

Summary

User group name
newgroup

Creation time
November 24, 2022, 23:51 (UTC+05:30)

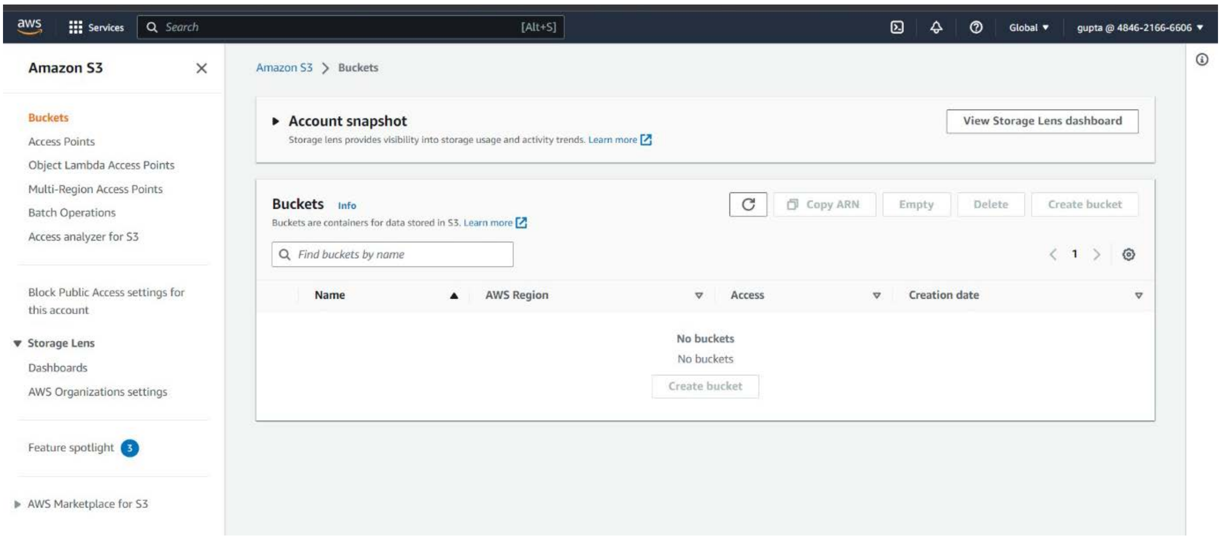
ARN
arn:aws:iam::484621666606:group/newgroup

Permissions policies (0) Info

You can attach up to 10 managed policies.

□	Policy name	Type	Description

Now, the user won't be able to access the AWS S3 services.



Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date

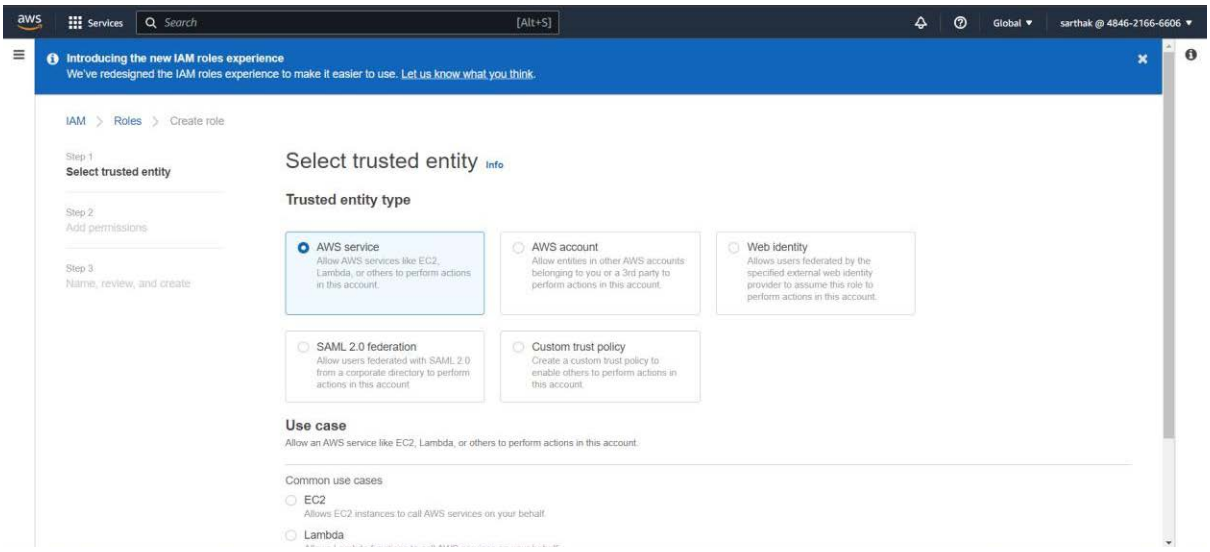
No buckets

No buckets

Create bucket

Creating and adding a role.

STEP 1: In the Dashboard of IAM select 'Roles' from the left panel andgo to 'Create role'.



Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

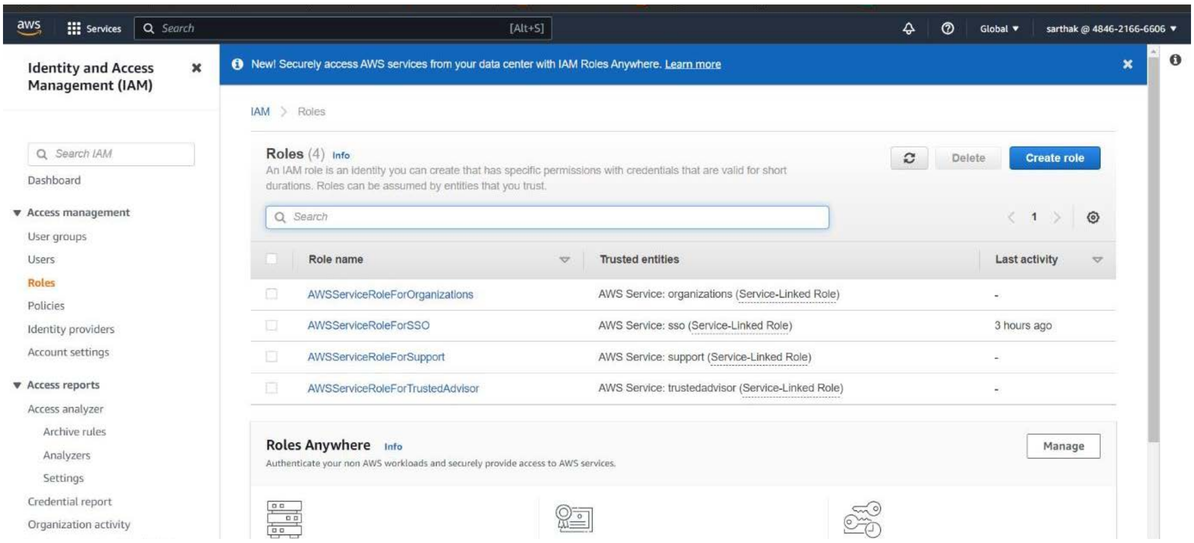
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

○ EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda

STEP 2: Select 'AWS Service' then add 'AWSS3FullAccess' Policy. Assign a name for the created role



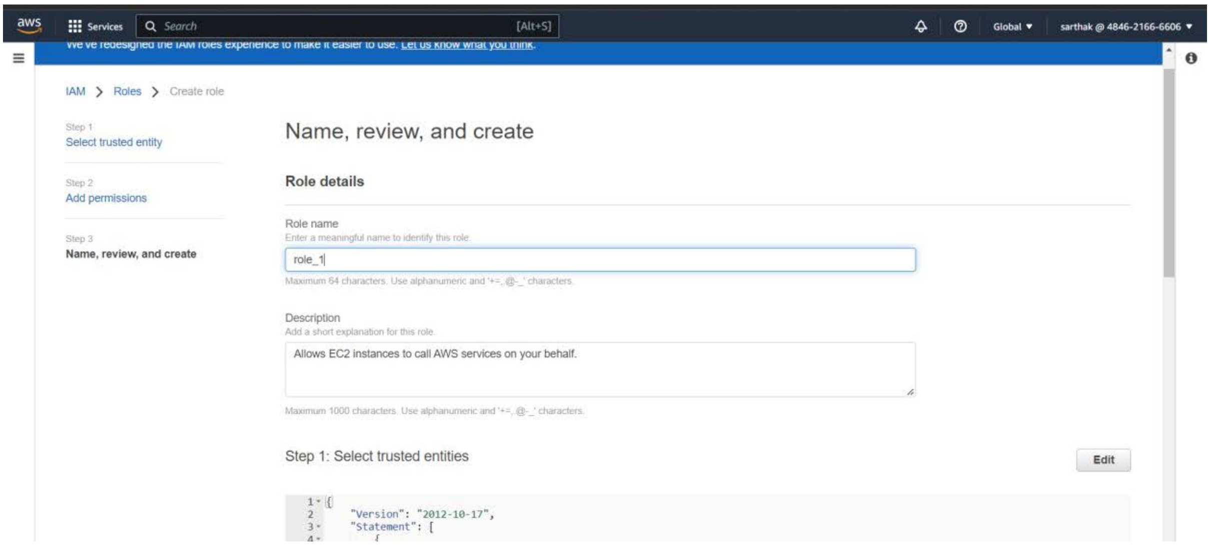
New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more

IAM > Roles

Roles (4) 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	Trusted entities	Last activity
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	-
AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Role)	3 hours ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Roles Anywhere Info
Authenticate your non AWS workloads and securely provide access to AWS services.



We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

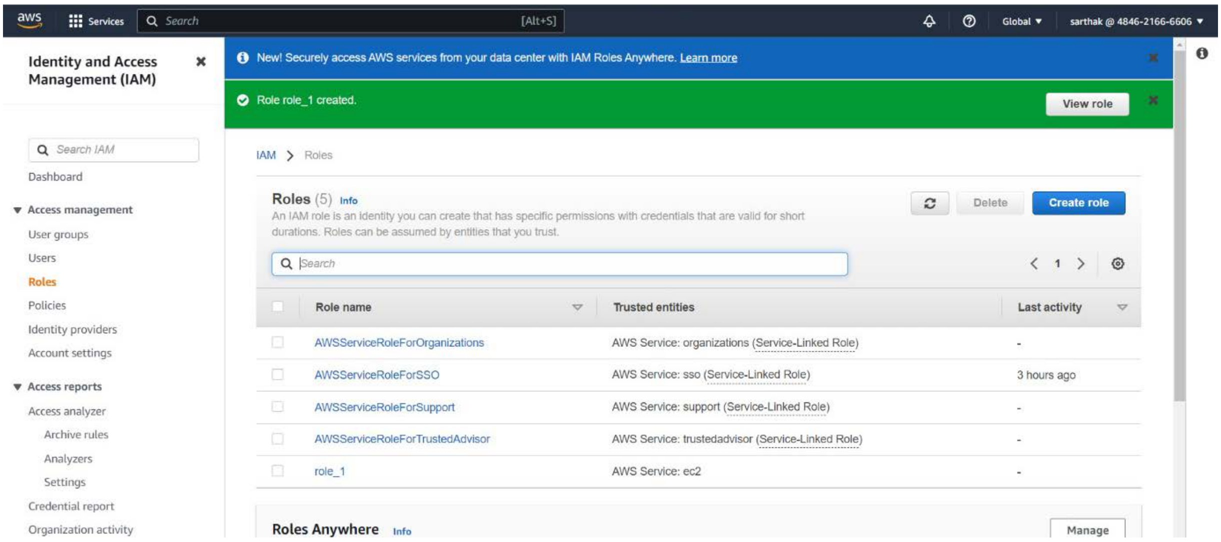
Role details

Role name
Enter a meaningful name to identify this role
role_1
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 alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```



New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more

Role role_1 created.

IAM > Roles

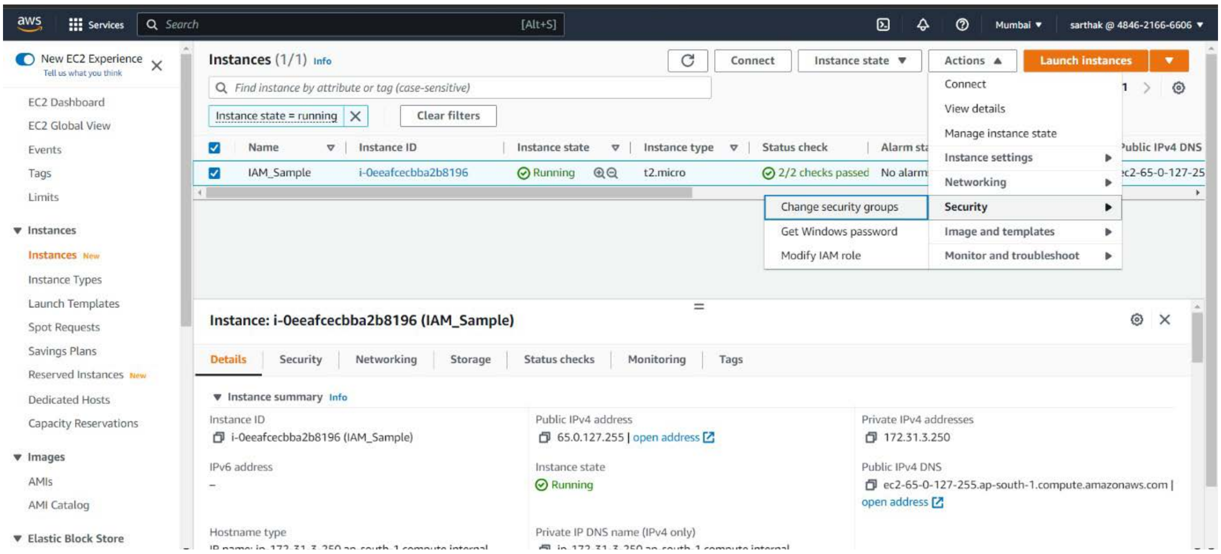
Roles (5) Info

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	Trusted entities	Last activity
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	-
□	AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Role)	3 hours ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	role_1	AWS Service: ec2	-

Roles Anywhere Info

STEP 3: Now go to the service dashboard and select EC2, Create a sample instance to add a role from INSTANCES->ACTIONS- >SECURITY->MODIFY IAM ROLE.



Instances (1/1) Info

Instance state = running

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm sta	Public IPv4 DNS
☑	IAM_Sample	i-0eeafcecbba2b8196	Running	t2.micro	2/2 checks passed	No alarm	ec2-65-0-127-25

Instance: i-0eeafcecbba2b8196 (IAM_Sample)

▾ Instance summary Info

Instance ID: i-0eeafcecbba2b8196 (IAM_Sample)

Public IPv4 address: 65.0.127.255 | open address

Private IPv4 addresses: 172.31.3.250

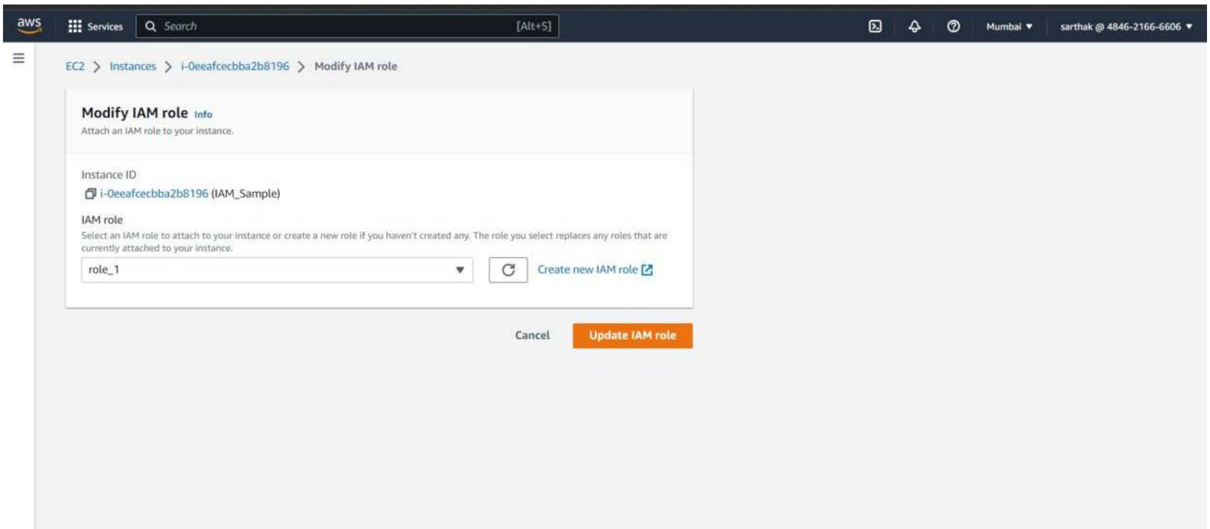
IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-65-0-127-255.ap-south-1.compute.amazonaws.com | open address

Hostname type

Private IP DNS name (IPv4 only)


aws
Services
Search [Alt+S]
Mumbai ▾
sarthak @ 4846-2166-6606 ▾
EC2 > Instances > i-0eeafcecbba2b8196 > Modify IAM role
Create new IAM role
Cancel
Update IAM role

Modify IAM role Info

Attach an IAM role to your instance.

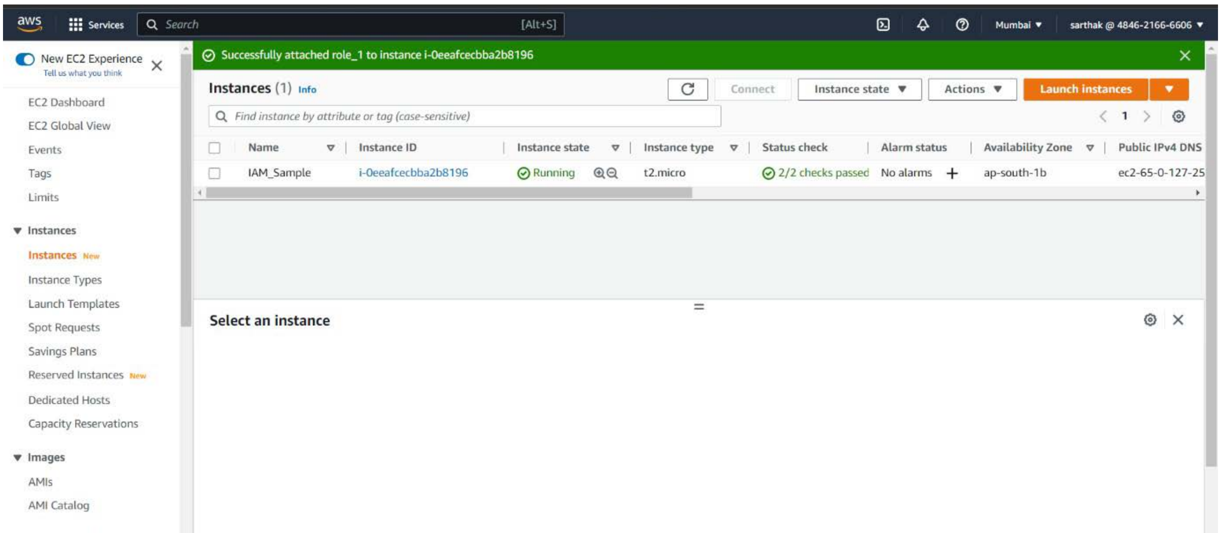
Instance ID

i-0eeafcecbba2b8196 (IAM_Sample)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

role_1



Successfully attached role_1 to instance i-0eeafcecbba2b8196

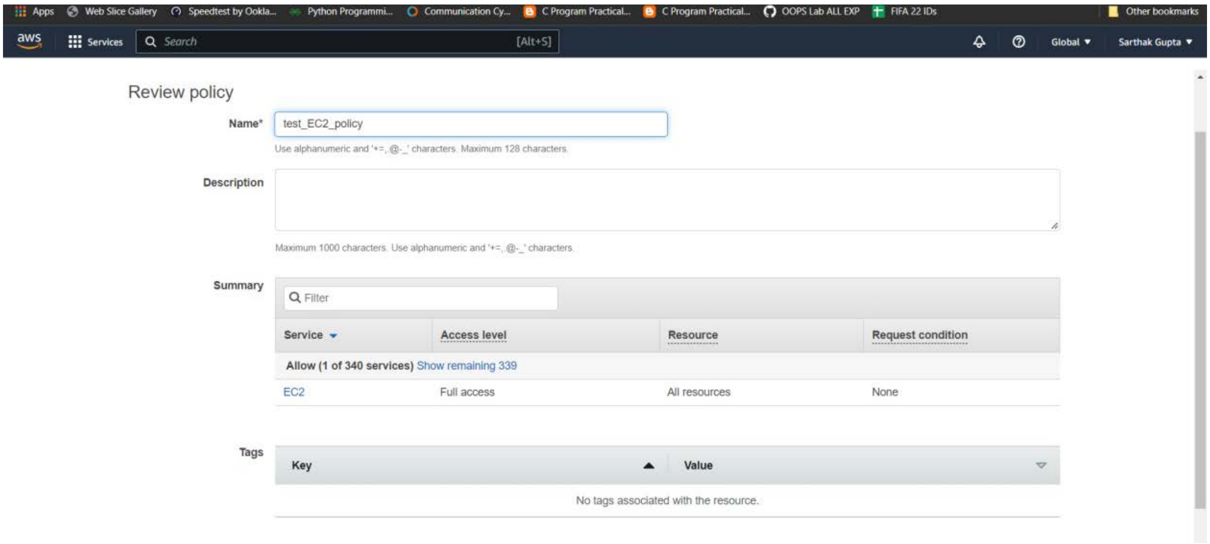
Instances (1) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	IAM_Sample	i-0eeafcecbba2b8196	Running	t2.micro	2/2 checks passed	No alarms +	ap-south-1b	ec2-65-0-127-25

Select an instance

Creating a policy

Step 1: In the Dashboard of IAM select ‘Policies’ from the left paneland go to ‘Create policy’ and do the following settings.



Review policy

Name* test_EC2_policy

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

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

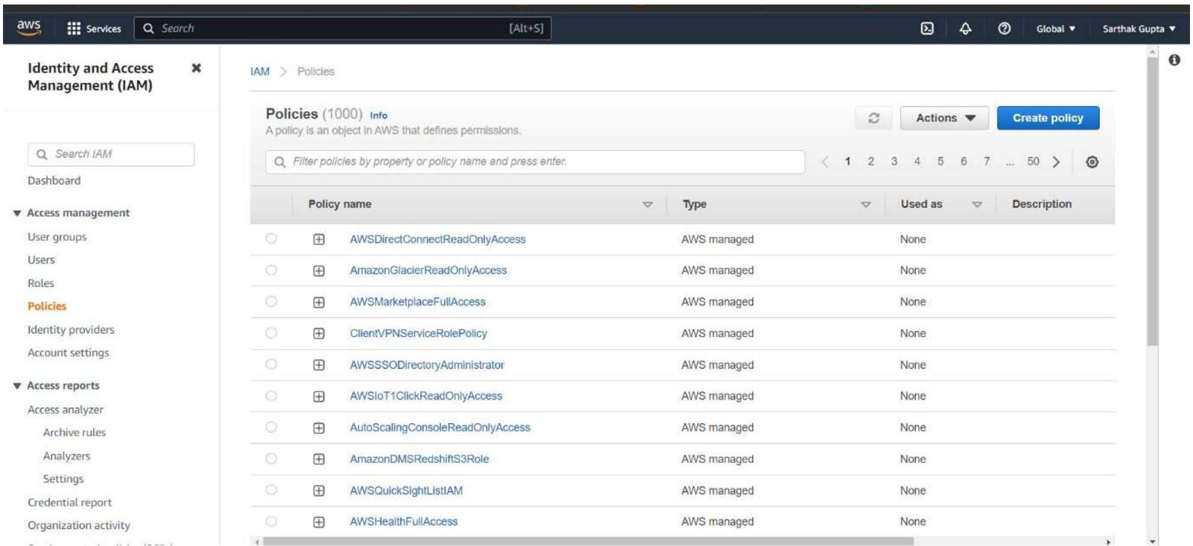
Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 340 services) Show remaining 339			
EC2	Full access	All resources	None

Tags

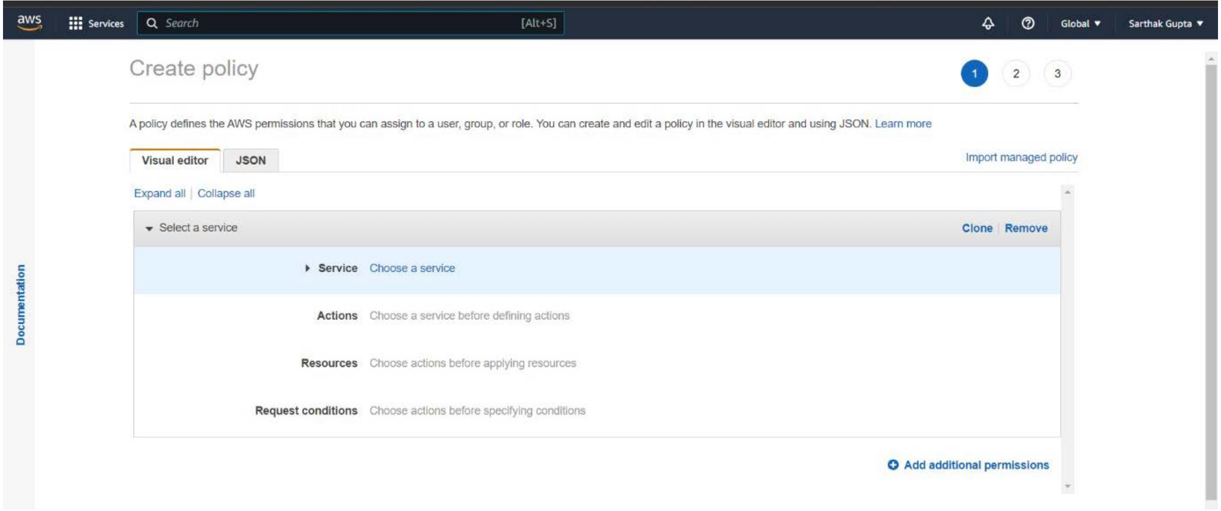
Key	Value
No tags associated with the resource.	



Policies (1000) Info

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
AWSDirectConnectReadOnlyAccess	AWS managed	None	
AmazonGlacierReadOnlyAccess	AWS managed	None	
AWSMarketplaceFullAccess	AWS managed	None	
ClientVPNServiceRolePolicy	AWS managed	None	
AWSSSODirectoryAdministrator	AWS managed	None	
AWSIoT1ClickReadOnlyAccess	AWS managed	None	
AutoScalingConsoleReadOnlyAccess	AWS managed	None	
AmazonDMSRedshiftS3Role	AWS managed	None	
AWSQuickSightListIAM	AWS managed	None	
AWSHealthFullAccess	AWS managed	None	



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Select a service

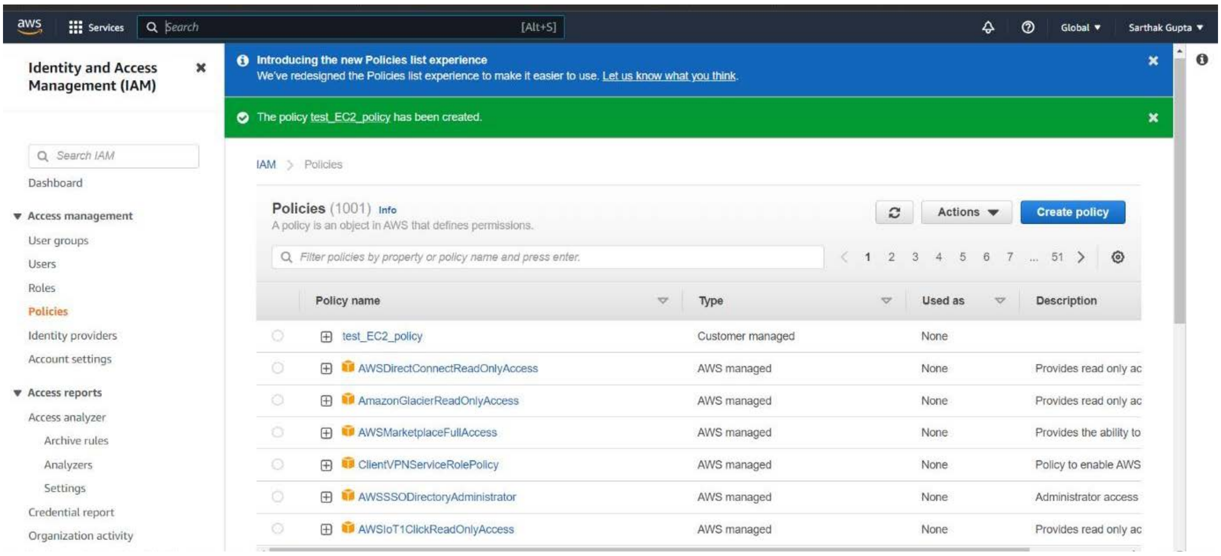
Service: Choose a service

Actions: Choose a service before defining actions

Resources: Choose actions before applying resources

Request conditions: Choose actions before specifying conditions

Now, A policy has been created



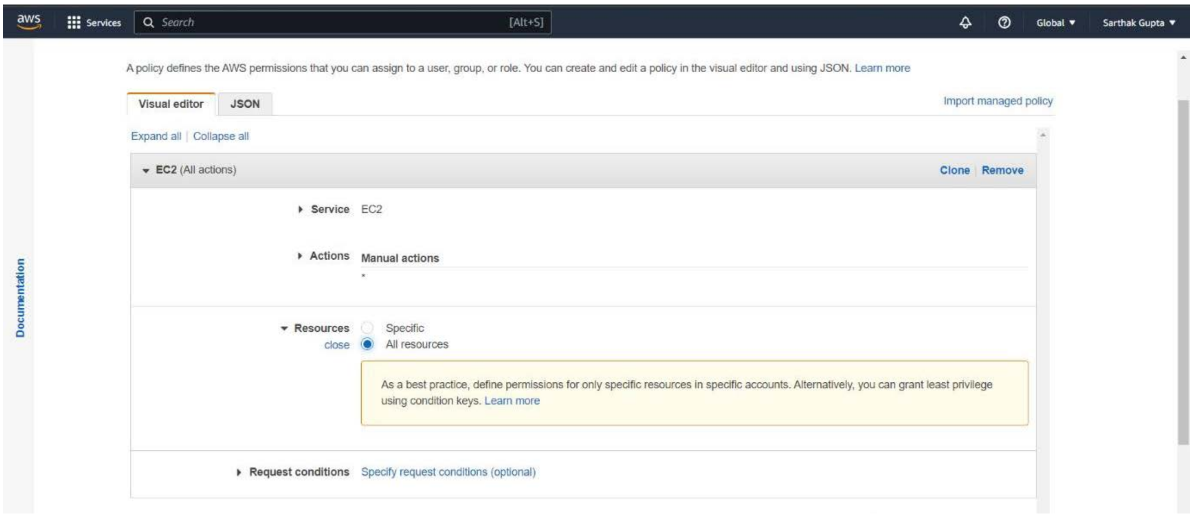
Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy test_EC2_policy has been created.

Policies (1001) Info
A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter.

Policy name	Type	Used as	Description
test_EC2_policy	Customer managed	None	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only ac
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only ac
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to
ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable AWS
AWSSSODirectoryAdministrator	AWS managed	None	Administrator access
AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only ac



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

EC2 (All actions)

Service: EC2

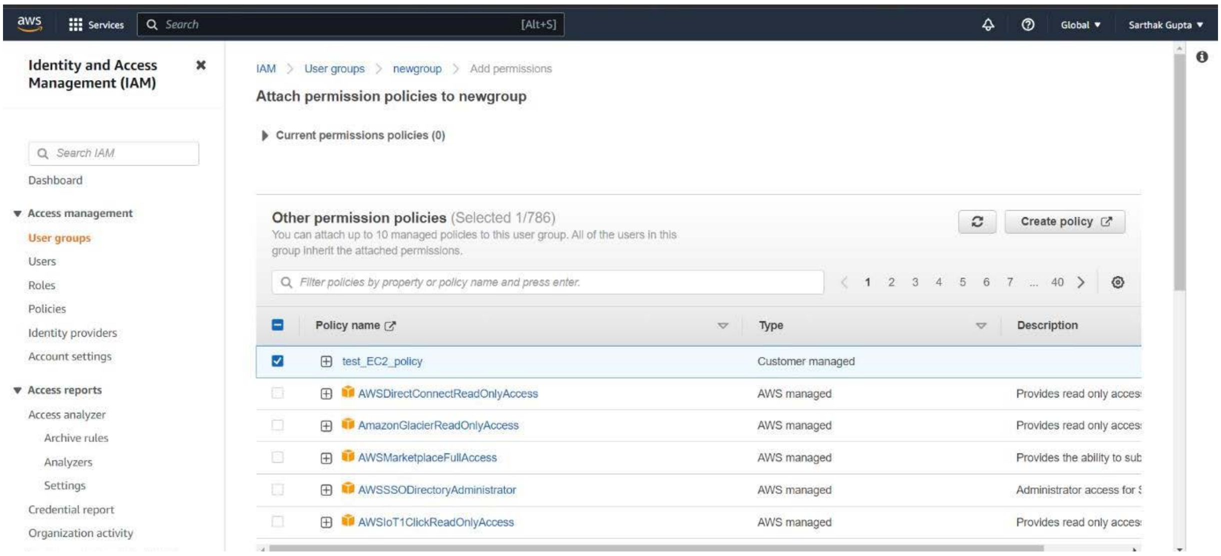
Actions: Manual actions
*

Resources close
○ Specific
● All resources

As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

Request conditions: Specify request conditions (optional)

Step 2: Attach the created policy to the previously created group.



Attach permission policies to newgroup

Current permissions policies (0)

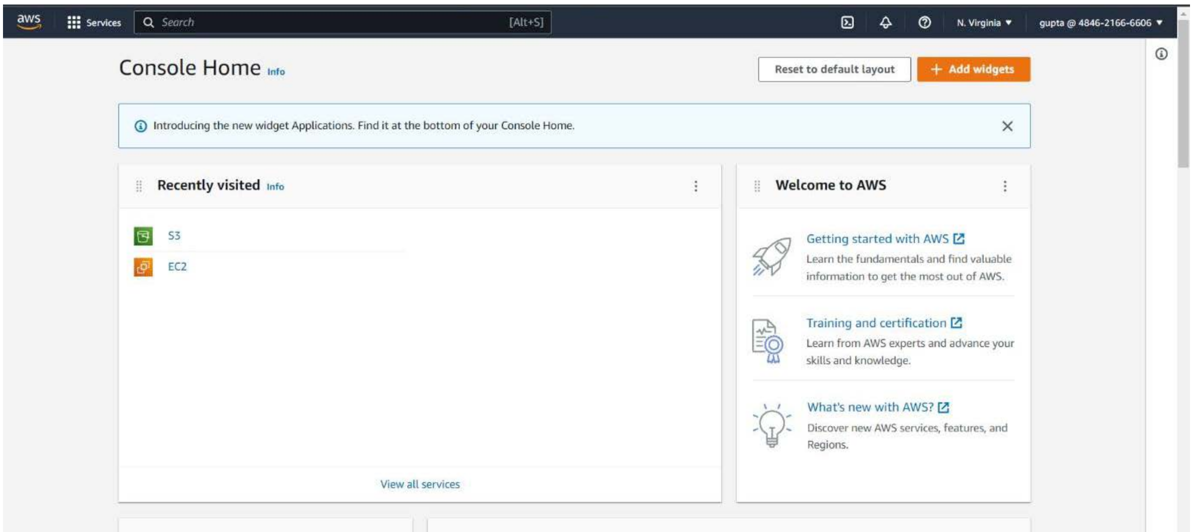
Other permission policies (Selected 1/786)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter policies by property or policy name and press enter.

	Policy name	Type	Description
☑	test_EC2_policy	Customer managed	
□	AWSDirectConnectReadOnlyAccess	AWS managed	Provides read only acces
□	AmazonGlacierReadOnlyAccess	AWS managed	Provides read only acces
□	AWSMarketplaceFullAccess	AWS managed	Provides the ability to sub
□	AWSSSODirectoryAdministrator	AWS managed	Administrator access for S
□	AWSIoT1ClickReadOnlyAccess	AWS managed	Provides read only acces

Step 3: Now log in as the created user without administrator access, and try using EC2 services.



Introducing the new widget Applications. Find it at the bottom of your Console Home.

Getting started with AWS

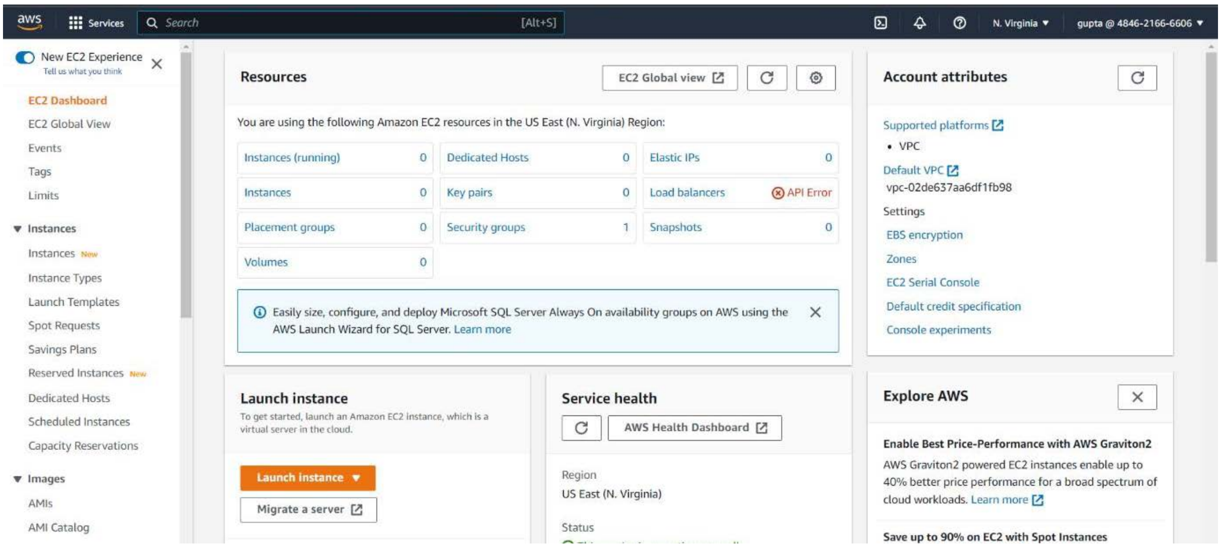
Learn the fundamentals and find valuable information to get the most out of AWS.

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.



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	0	Key pairs	0	Load balancers	⊗ API Error
Placement groups	0	Security groups	1	Snapshots	0
Volumes	0				

ⓘ Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Account attributes

Supported platforms
- VPC

Default VPC
vpc-02de637aa6df1fb98

Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments

Launch instance

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

Service health

Region
US East (N. Virginia)

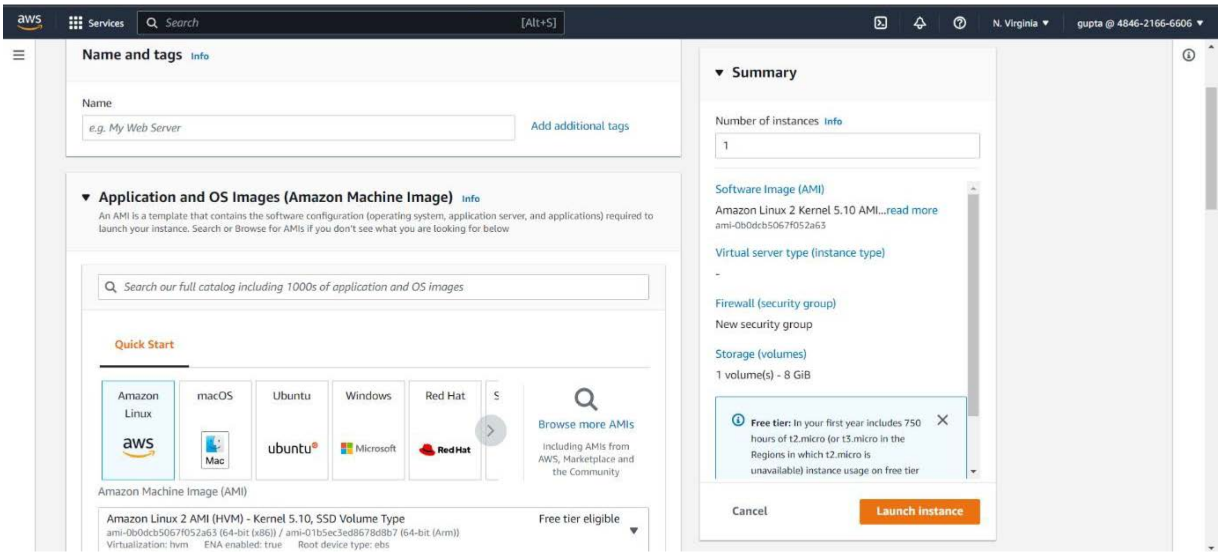
Status

Explore AWS

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

Save up to 90% on EC2 with Spot Instances



Name and tags

Name: e.g. My Web Server

▼ Application and OS Images (Amazon Machine Image)

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

Search our full catalog including 1000s of application and OS images

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible
ami-0b0dcb5067f052a63 (64-bit (x86)) / ami-01b5ec3ed8678d8b7 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

▼ Summary

Number of instances: 1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0b0dcb5067f052a63

Virtual server type (instance type)
-

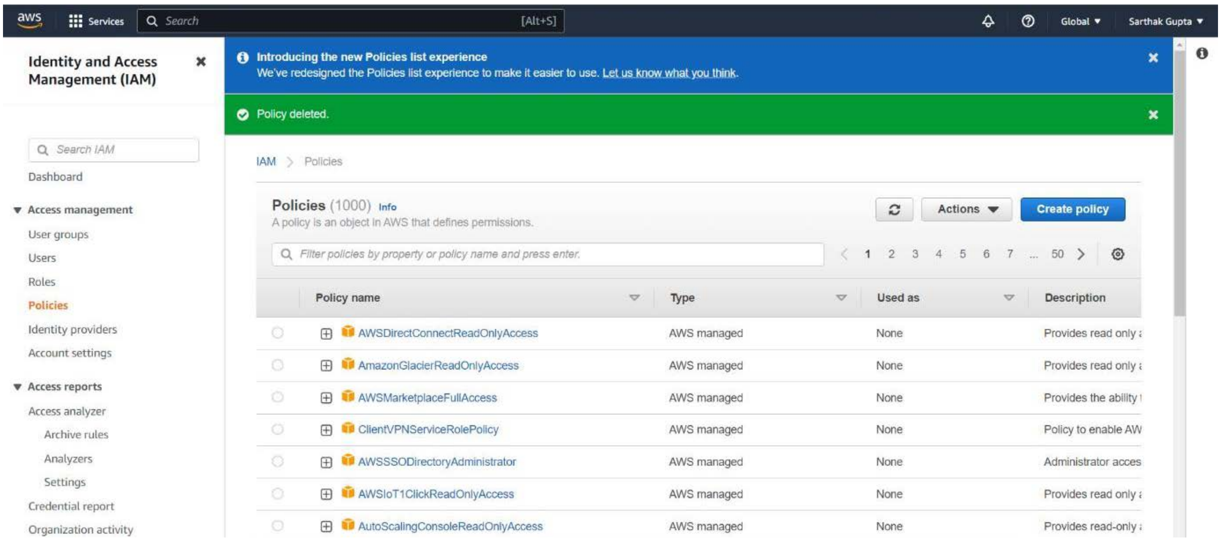
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

ⓘ Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

As seen above the user is able to use the EC2 services.

Step 4: Now, delete the previous policy and create a new policy but this time in Actions choose ‘Switch to deny permissions’ option or editthe policy. This will deny the user from using the selected services.



Identity and Access Management (IAM)

Search IAM

- Dashboard
- ▾ Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- ▾ Access reports
  - Access analyzer
    - Archive rules
    - Analyzers
    - Settings
  - Credential report
  - Organization activity

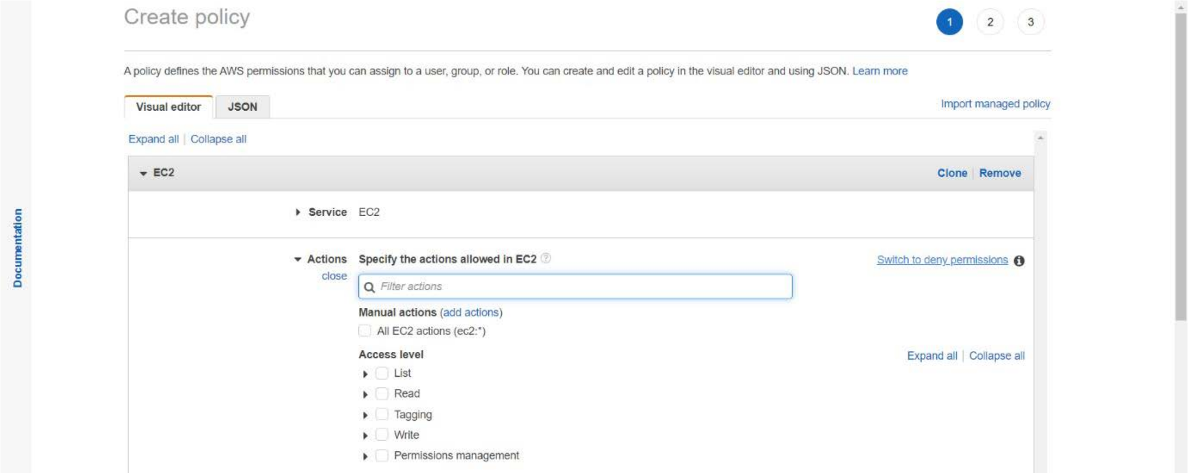
Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

Policy deleted.

IAM > Policies

Policies (1000) Info
A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	⊞ AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only a
○	⊞ AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only a
○	⊞ AWSMarketplaceFullAccess	AWS managed	None	Provides the ability t
○	⊞ ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable AW
○	⊞ AWSSSODirectoryAdministrator	AWS managed	None	Administrator acces
○	⊞ AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only a
○	⊞ AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only a



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

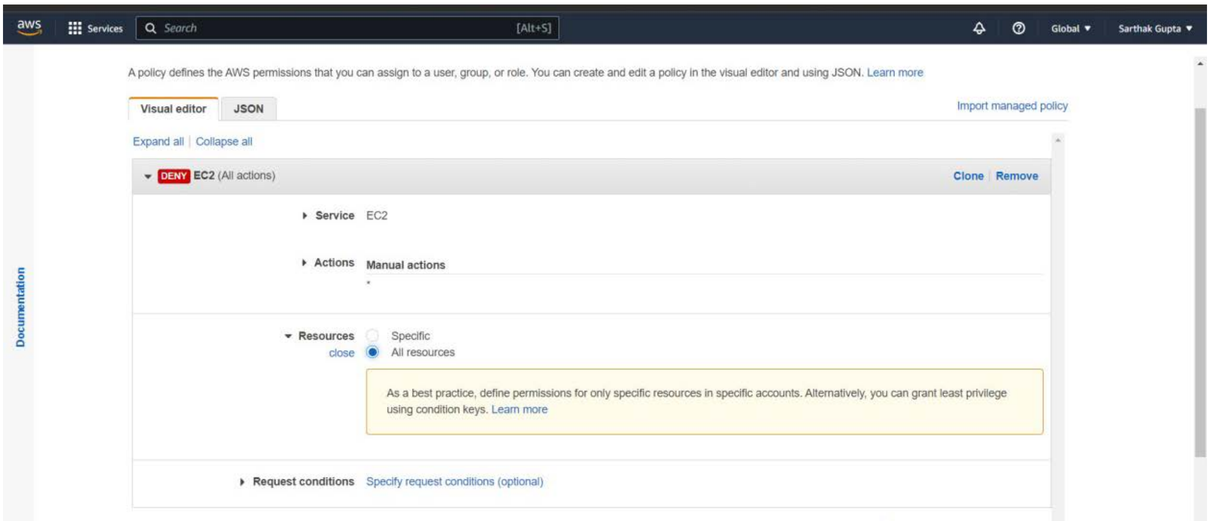
▾ EC2

▸ Service EC2

▾ Actions close — Specify the actions allowed in EC2

Manual actions (add actions)
□ All EC2 actions (ec2:*)

Access level — Expand all | Collapse all
- ▸ □ List
- ▸ □ Read
- ▸ □ Tagging
- ▸ □ Write
- ▸ □ Permissions management



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

▾ DENY EC2 (All actions)

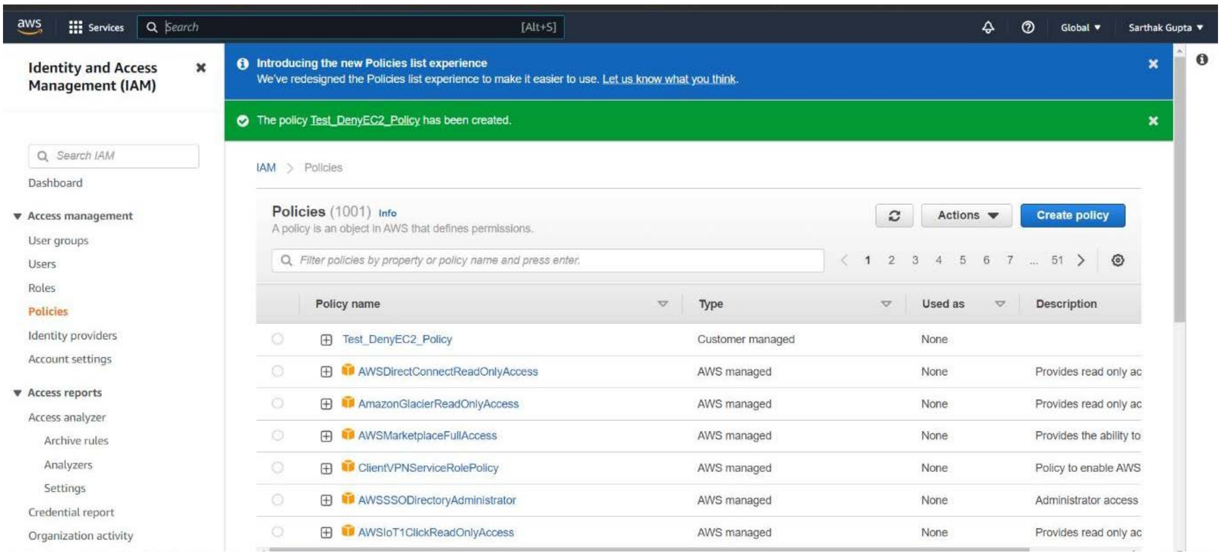
▸ Service EC2

▸ Actions Manual actions
*

▾ Resources close
○ Specific
● All resources

As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

▸ Request conditions Specify request conditions (optional)



Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy Test_DenyEC2_Policy has been created.

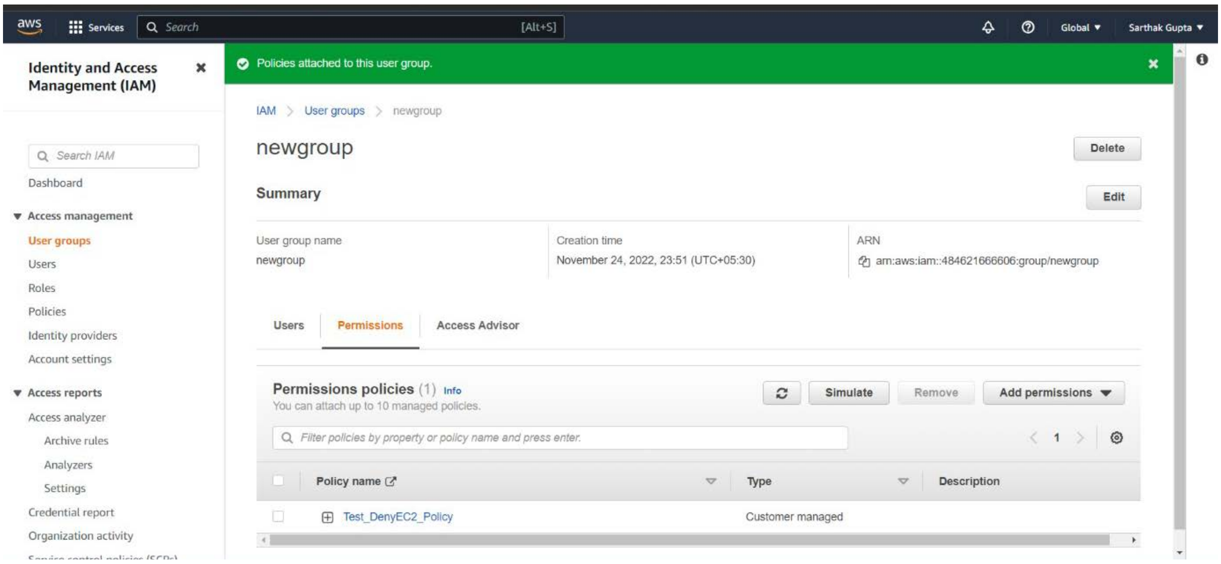
IAM > Policies

Policies (1001) Info
A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter.

Policy name	Type	Used as	Description
Test_DenyEC2_Policy	Customer managed	None	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only ac
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only ac
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to
ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable AWS
AWSSSODirectoryAdministrator	AWS managed	None	Administrator access
AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only ac

Step 5: Attach this created policy to the previously created group.



Policies attached to this user group.

IAM > User groups > newgroup

newgroup

Summary

User group name	Creation time	ARN
newgroup	November 24, 2022, 23:51 (UTC+05:30)	arn:aws:iam::484621666606:group/newgroup

Permissions policies (1) Info
You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name	Type	Description
Test_DenyEC2_Policy	Customer managed	

Step 6: Now try access the EC2 services again but this time the access will be denied.

What is IAM?

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With AWS IAM, you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.

Components of IAM are:

USERS: An IAM user is an identity with an associated credential and permissions attached to it. This could be an actual person who is a user, or it could be an application that is a user. With IAM, you can securely manage access to AWS services by creating an IAM user name for each employee in your organization. Each IAM user is associated with only one AWS account.

USER GROUPS: A collection of IAM users is an IAM group. You can use IAM groups to specify permissions for multiple users so that any permissions applied to the group are applied to the individual users in that group as well. Managing groups is quite easy. You set permissions for the group, and those permissions are automatically applied to all the users in the group. If you add another user to the group, the new user will automatically inherit all the policies and the permissions already assigned to that group.

POLICIES: An IAM policy sets permission and controls access to AWS resources. Policies are stored in AWS as JSON documents. Permissions specify who has access to the resources and what actions they can perform. For example, a policy could allow an IAM user to access one of the buckets in Amazon S3. The policy would contain the following information:

1. Who can access it
2. What actions that user can take
3. Which AWS resources that user can access
4. When they can be accessed

ROLES: An IAM role is a set of permissions that define what actions are allowed and denied by an entity in the AWS console. It is similar to a user in that it can be accessed by any type of entity (an individual or AWS service). Role permissions are temporary credentials.

The difference between IAM roles and policies in AWS is that a role is a type of IAM identity that can be authenticated and authorized to utilize an AWS resource, whereas a policy defines the permissions of the IAM identity.