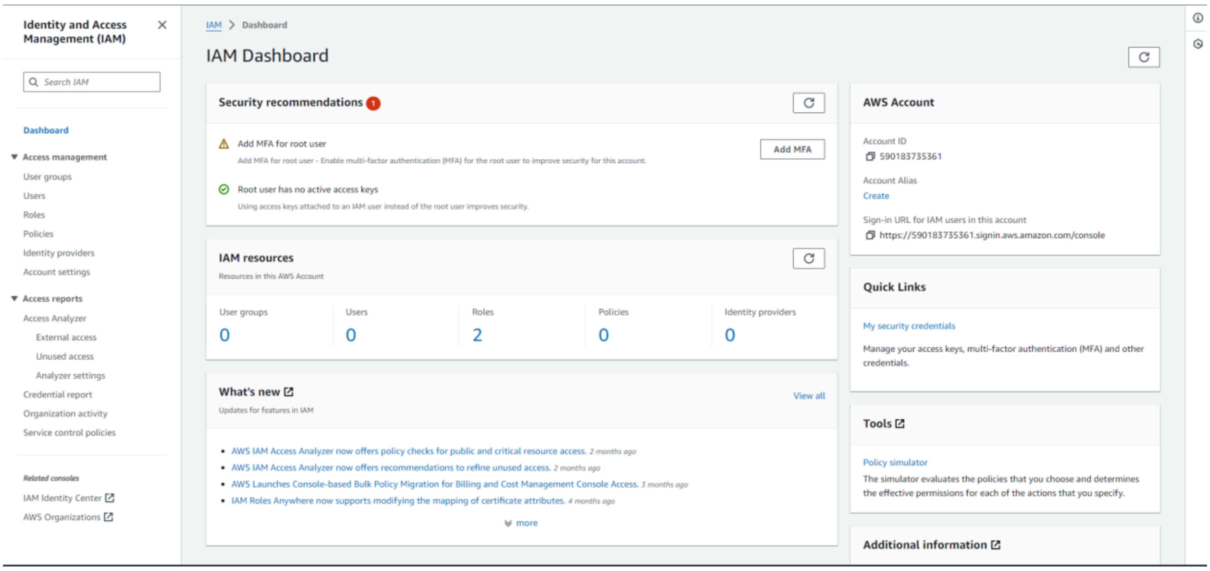
CLOUD COMPUTING

PRACTICAL 3

NAME: BHARVI CHAVDA

ROLL NO. : A006

SAP ID: 86062300028



Identity and Access Management (IAM)

Search IAM

- Dashboard
- ▼ Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- ▼ Access reports
  - Access Analyzer
    - External access
    - Unused access
    - Analyzer settings
  - Credential report
  - Organization activity
  - Service control policies

Related consoles

- IAM Identity Center
- AWS Organizations

IAM > Dashboard

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.

Add MFA

✓ Root user has no active access keys

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

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new

Updates for features in IAM

View all

- AWS IAM Access Analyzer now offers policy checks for public and critical resource access. *2 months ago*
- AWS IAM Access Analyzer now offers recommendations to refine unused access. *2 months ago*
- AWS Launches Console-based Bulk Policy Migration for Billing and Cost Management Console Access. *3 months ago*
- IAM Roles Anywhere now supports modifying the mapping of certificate attributes. *4 months ago*

more

AWS Account

Account ID
590183735361

Account Alias
Create

Sign-in URL for IAM users in this account
https://590183735361.signin.aws.amazon.com/console

Quick Links

My security credentials

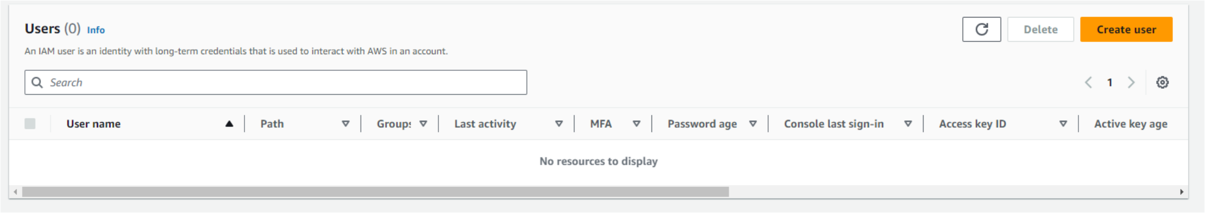
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

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

Additional information



Users (0) Info

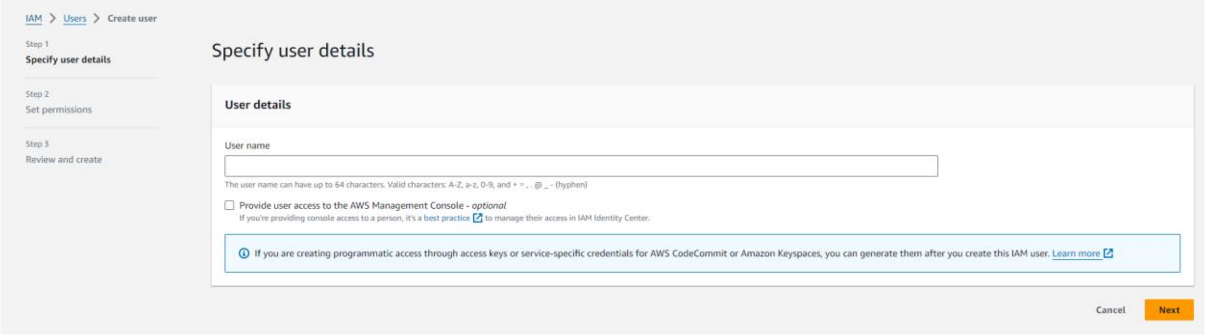
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Delete | Create user

Search

□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age

No resources to display



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

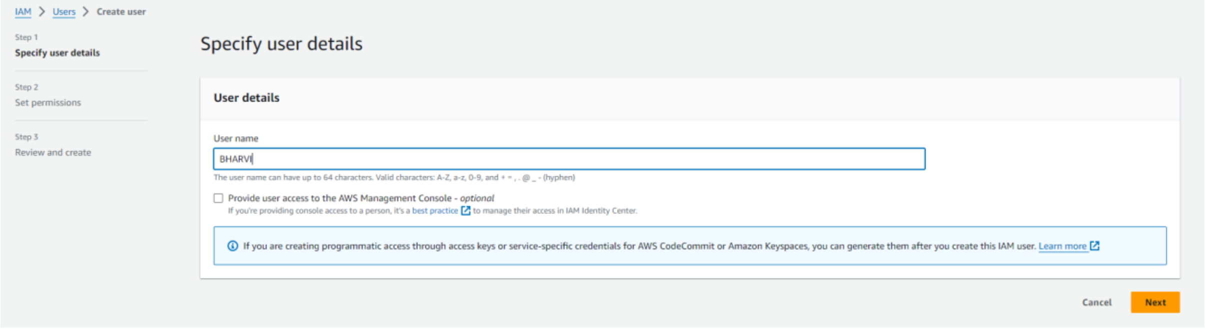
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ 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

Cancel | Next



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
BHARVI

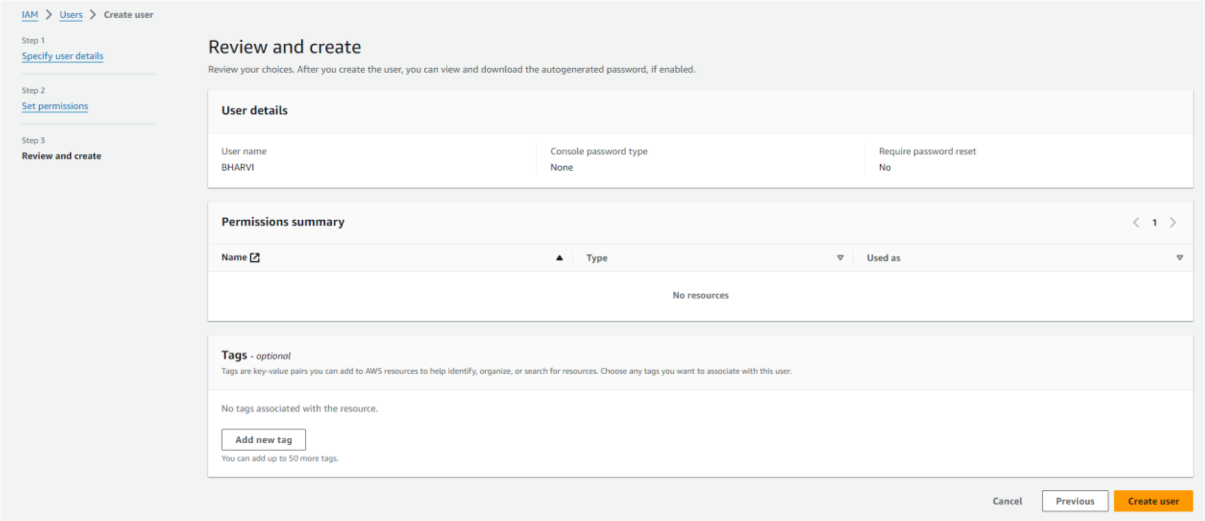
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ 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

Cancel | Next



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
BHARVI	None	No

Permissions summary

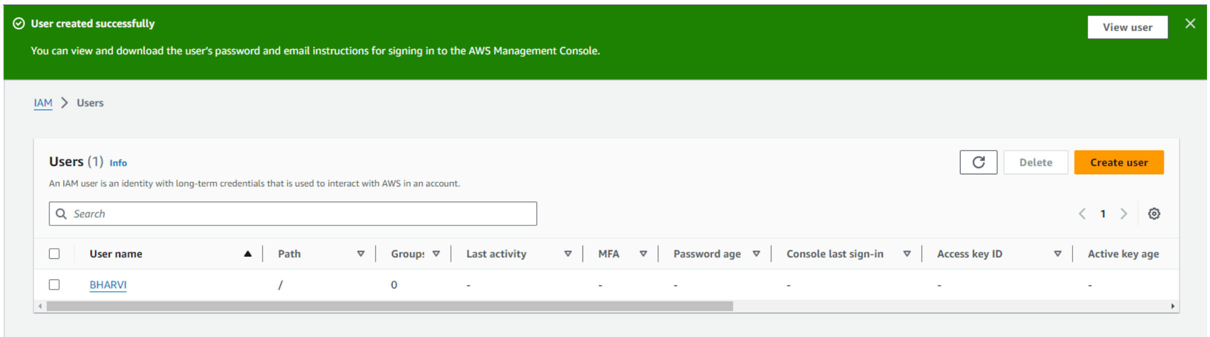
Name	Type	Used as
No resources		

Tags - *optional*

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

No tags associated with the resource.

You can add up to 50 more tags.



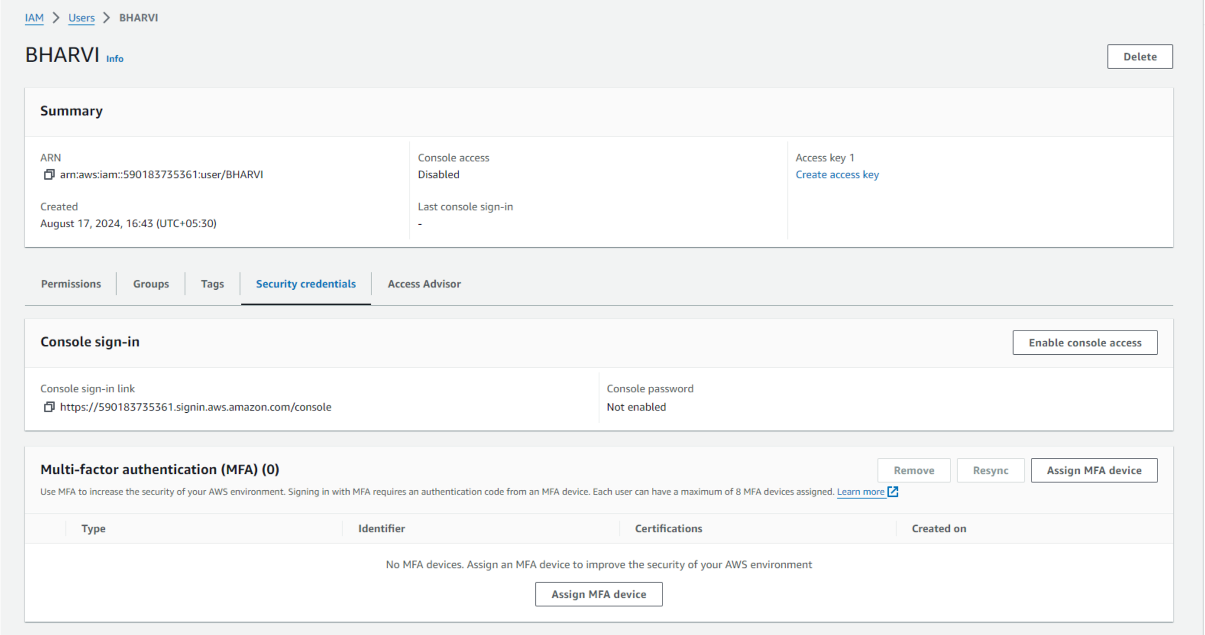
User created successfully

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

Users (1) Info

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

□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
□	BHARVI	/	0	-	-	-	-	-	-



BHARVI Info

Summary

ARN
arn:aws:iam::590183735361:user/BHARVI

Created
August 17, 2024, 16:43 (UTC+05:30)

Console access
Disabled

Last console sign-in
-

Access key 1
Create access key

Console sign-in

Console sign-in link
https://590183735361.signin.aws.amazon.com/console

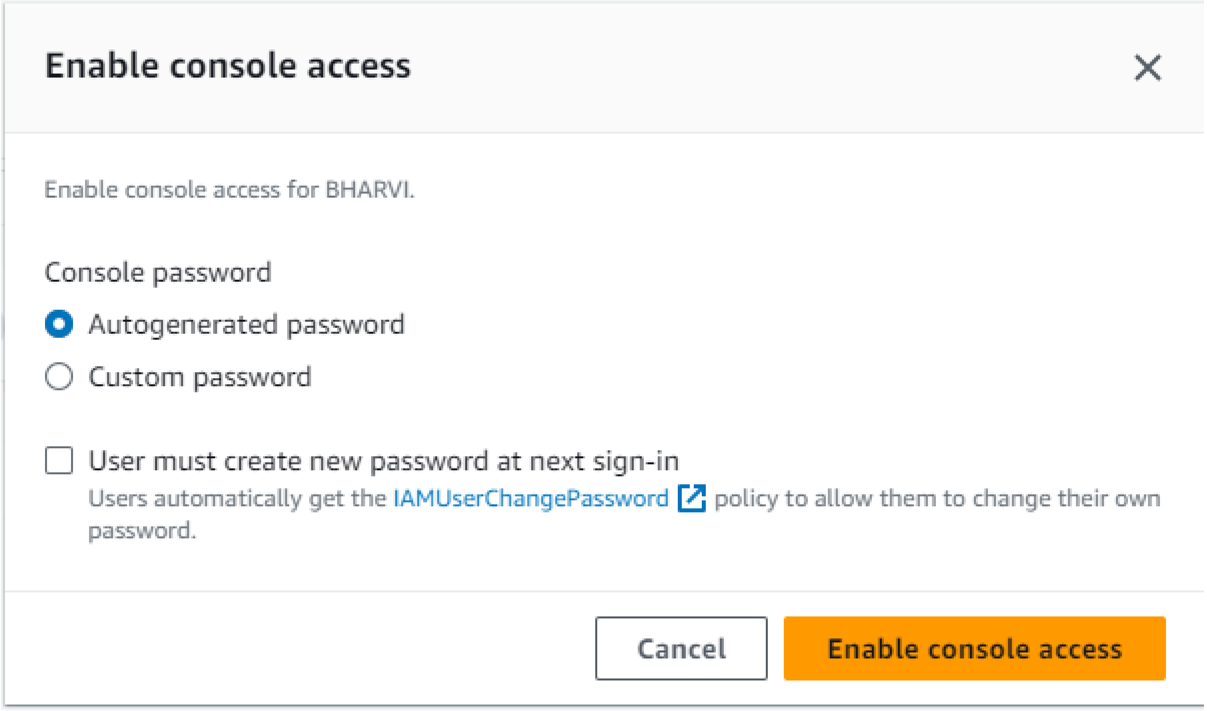
Console password
Not enabled

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment



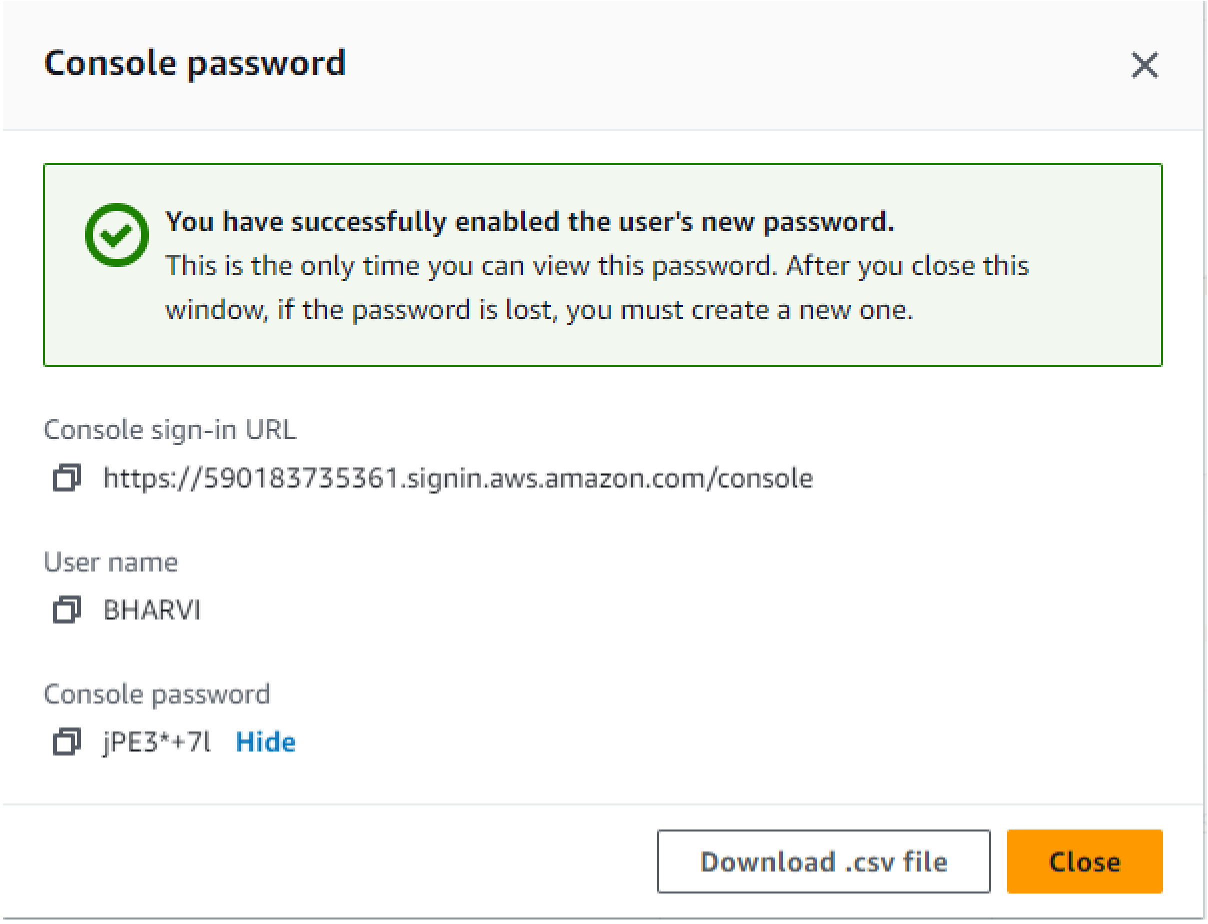
Enable console access for BHARVI.

Console password

● Autogenerated password

○ Custom password

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



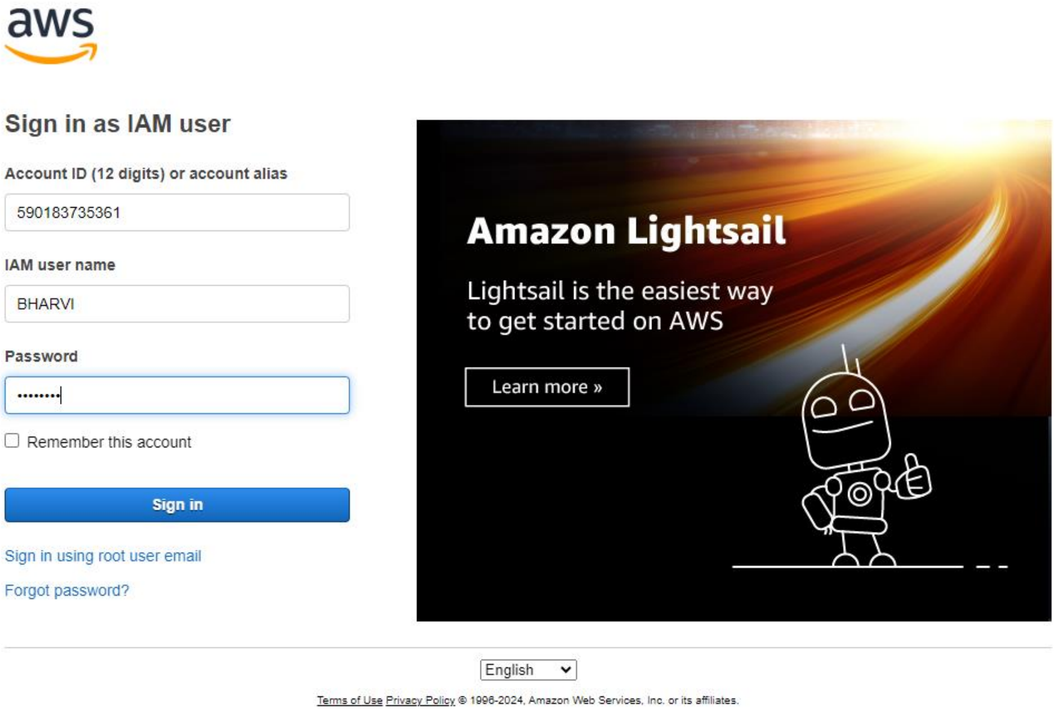
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL
https://590183735361.signin.aws.amazon.com/console

User name
BHARVI

Console password
jPE3*+7l Hide

jPE3*+7l j



Sign in as IAM user

Account ID (12 digits) or account alias

590183735361

IAM user name

BHARVI

Password

••••••••

□ Remember this account

Sign in

Sign in using root user email

Forgot password?

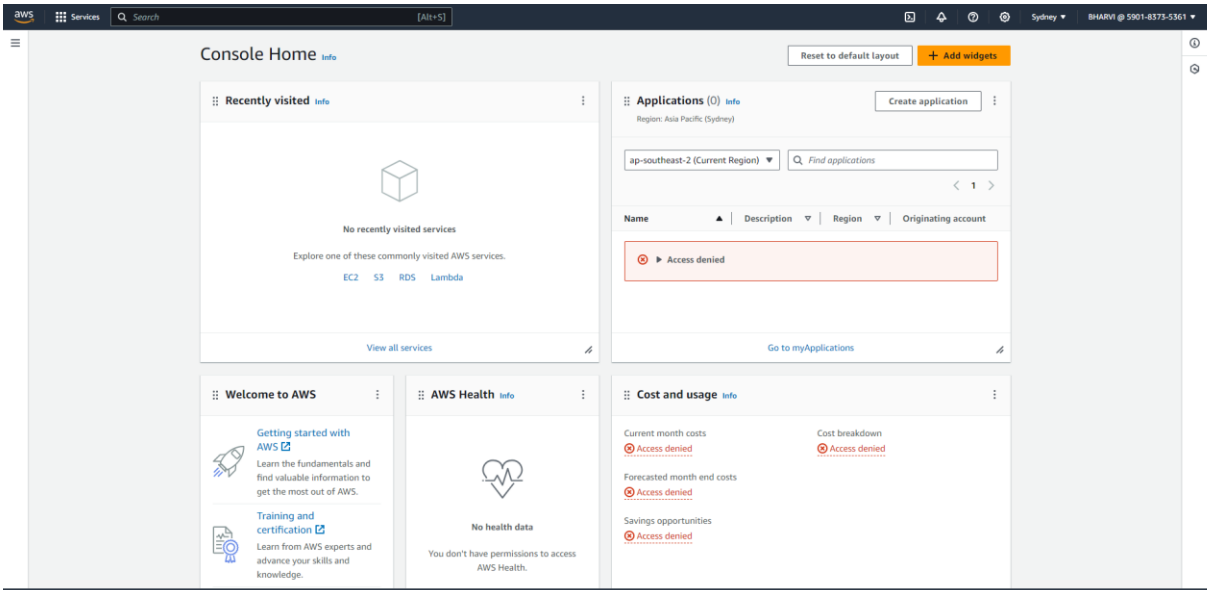
Amazon Lightsail

Lightsail is the easiest way to get started on AWS

Learn more »

English

Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.



Console Home Info

Reset to default layout

+ Add widgets

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

View all services

Applications (0) Info

Region: Asia Pacific (Sydney)

Create application

ap-southeast-2 (Current Region) ▾

Find applications

< 1 >

Name ▲	Description ▽	Region ▽	Originating account
⊗ ▸ Access denied			

Go to myApplications

Welcome to AWS

Getting started with AWS

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

Training and certification

Learn from AWS experts and advance your skills and knowledge.

AWS Health Info

No health data

You don't have permissions to access AWS Health.

Cost and usage Info

Current month costs

⊗ Access denied

Cost breakdown

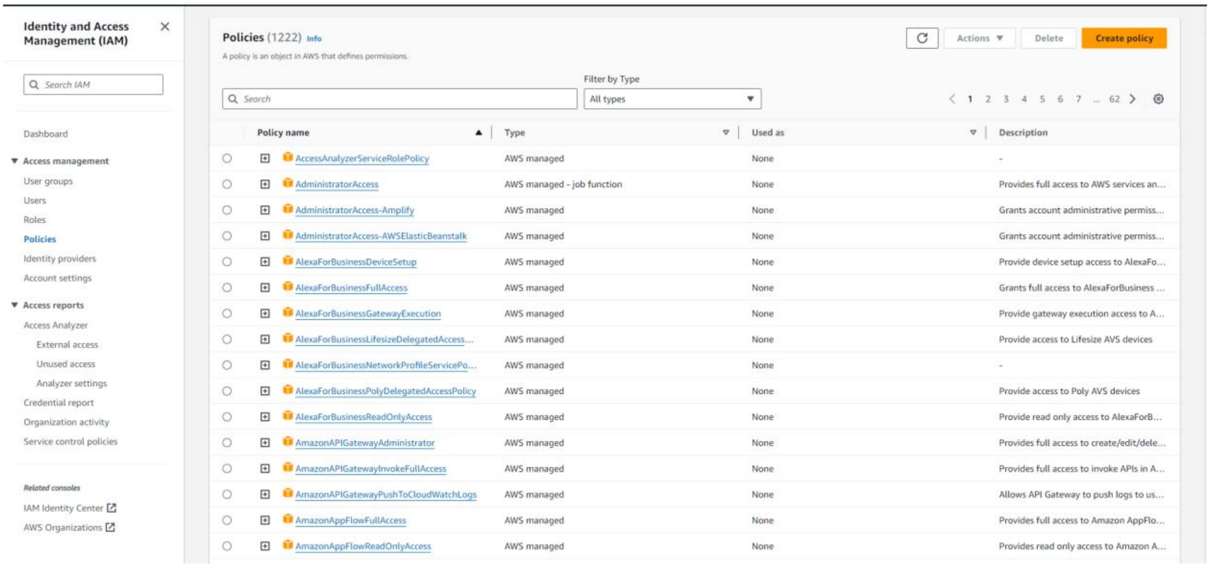
⊗ Access denied

Forecasted month end costs

⊗ Access denied

Savings opportunities

⊗ Access denied

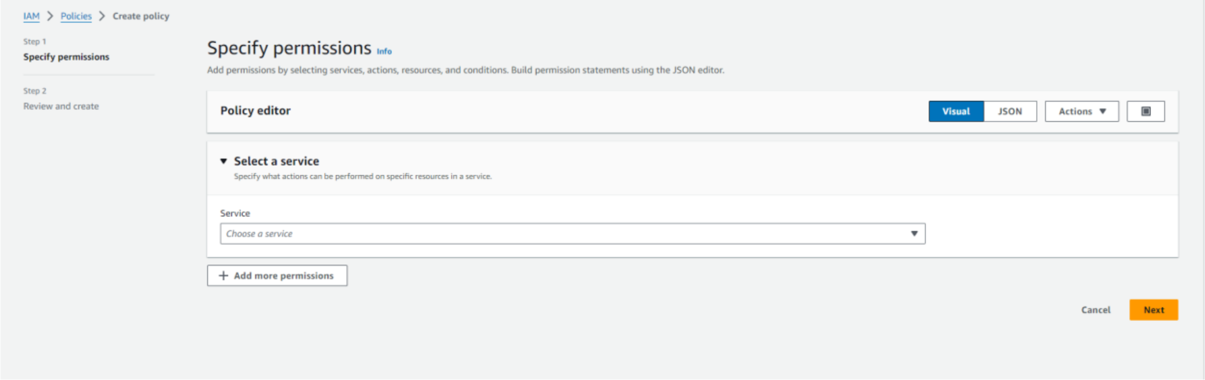


Policies (1222) Info

A policy is an object in AWS that defines permissions.

Filter by Type: All types

	Policy name	Type	Used as	Description
○	AccessAnalyzerServiceRolePolicy	AWS managed	None	-
○	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
○	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
○	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permiss...
○	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
○	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
○	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
○	AlexaForBusinessLifesizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
○	AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
○	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
○	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
○	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...
○	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
○	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to us...
○	AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlo...
○	AmazonAppFlowReadOnlyAccess	AWS managed	None	Provides read only access to Amazon A...



Specify permissions Info

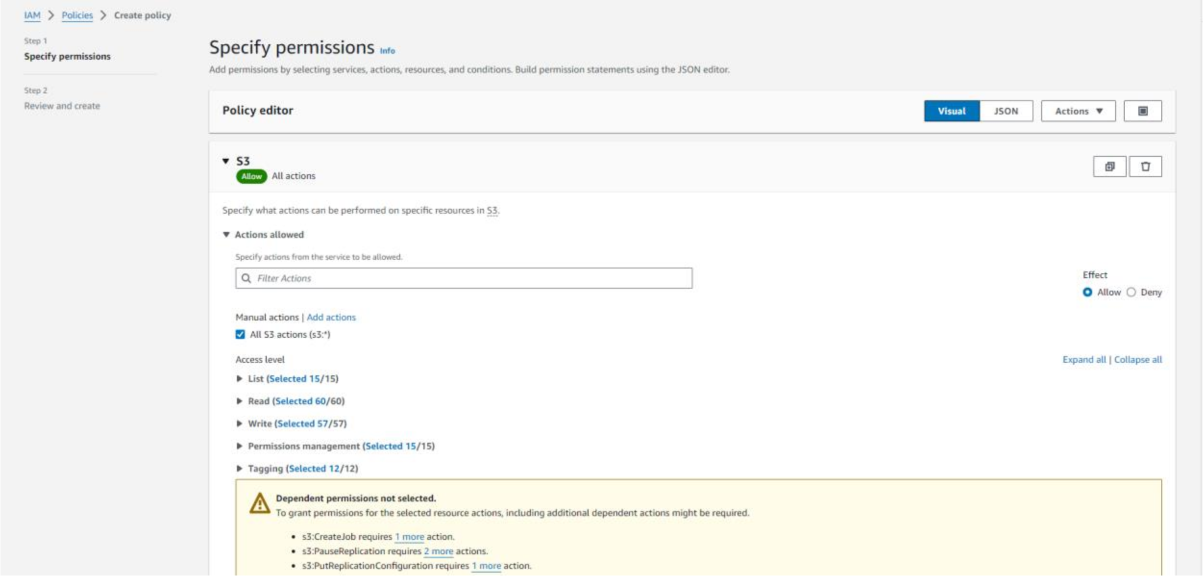
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service



Specify permissions Info

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

Policy editor

S3

Allow All actions

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed.

Effect: ● Allow ○ Deny

Manual actions | Add actions

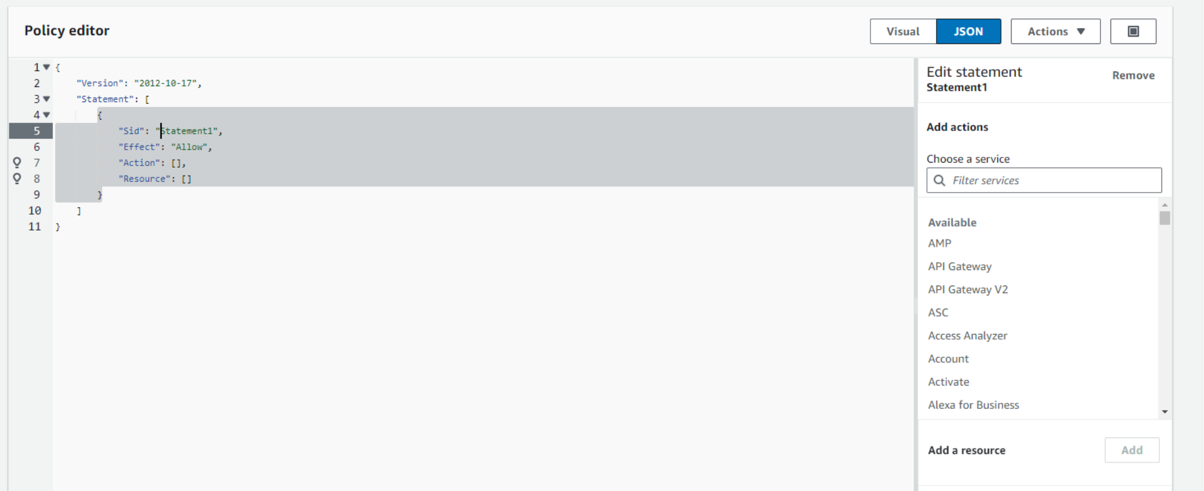
☑ All S3 actions (s3:*)

Access level

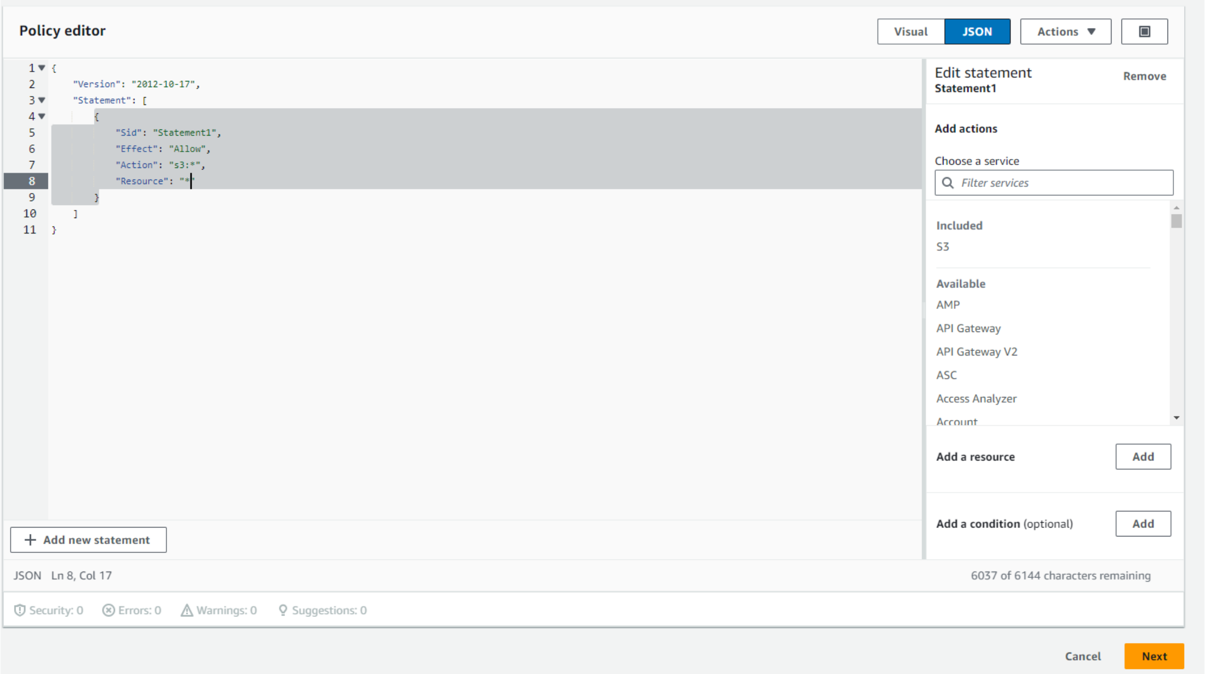
- List (Selected 15/15)
- Read (Selected 60/60)
- Write (Selected 57/57)
- Permissions management (Selected 15/15)
- Tagging (Selected 12/12)

Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.

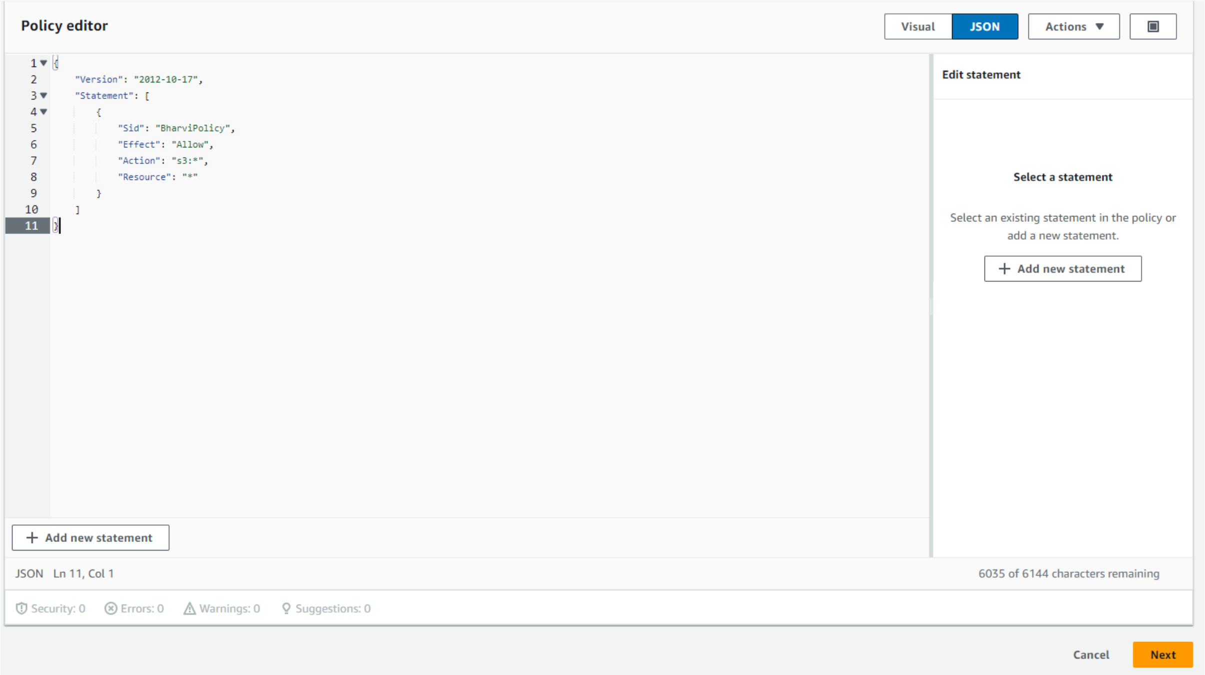
- s3:CreateJob requires 1 more action.
- s3:PauseReplication requires 2 more actions.
- s3:PutReplicationConfiguration requires 1 more action.



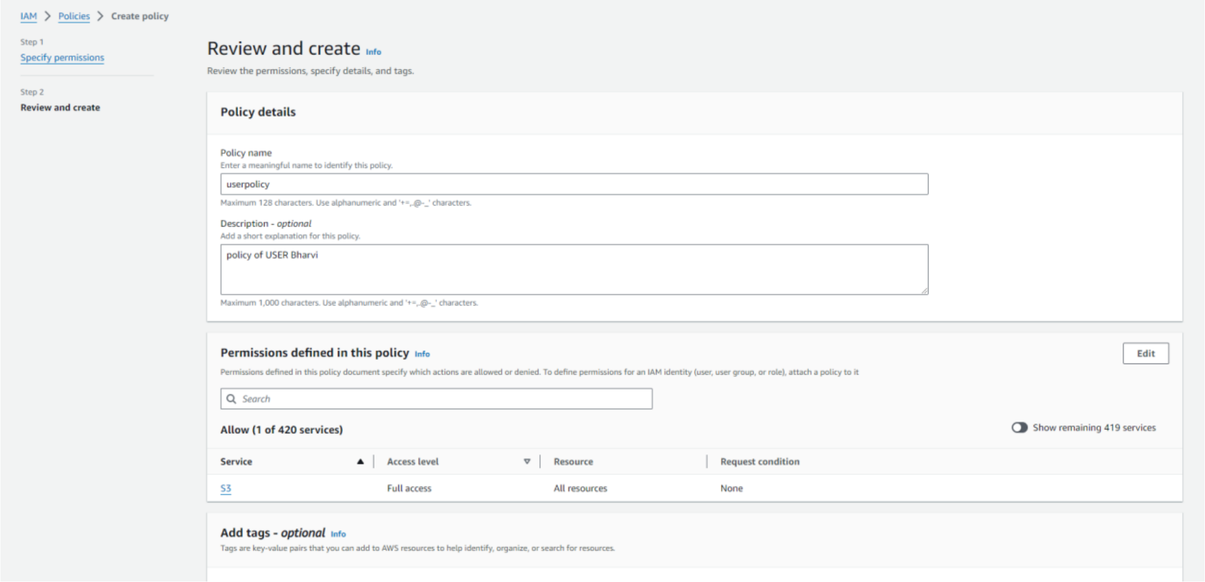
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [],
            "Resource": []
        }
    ]
}
```



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BharviPolicy",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```



Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name: userpolicy

Enter a meaningful name to identify this policy.

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

Description - *optional*: policy of USER Bharvi

Add a short explanation for this policy.

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

Permissions defined in this policy

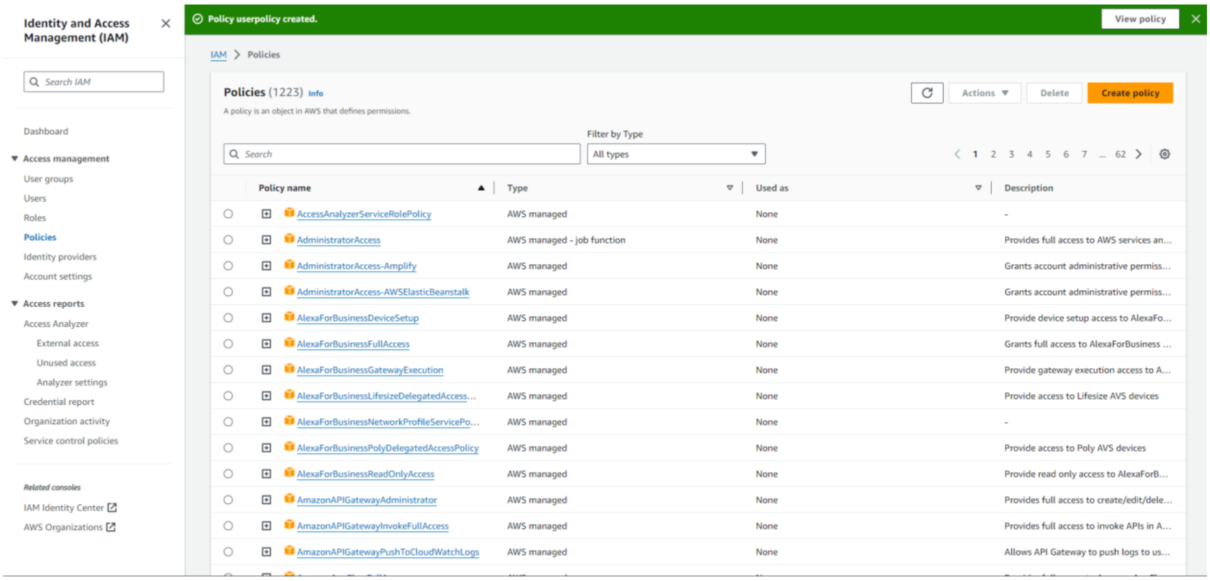
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 420 services)

Service ▲	Access level ▽	Resource	Request condition
S3	Full access	All resources	None

Add tags - *optional*

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



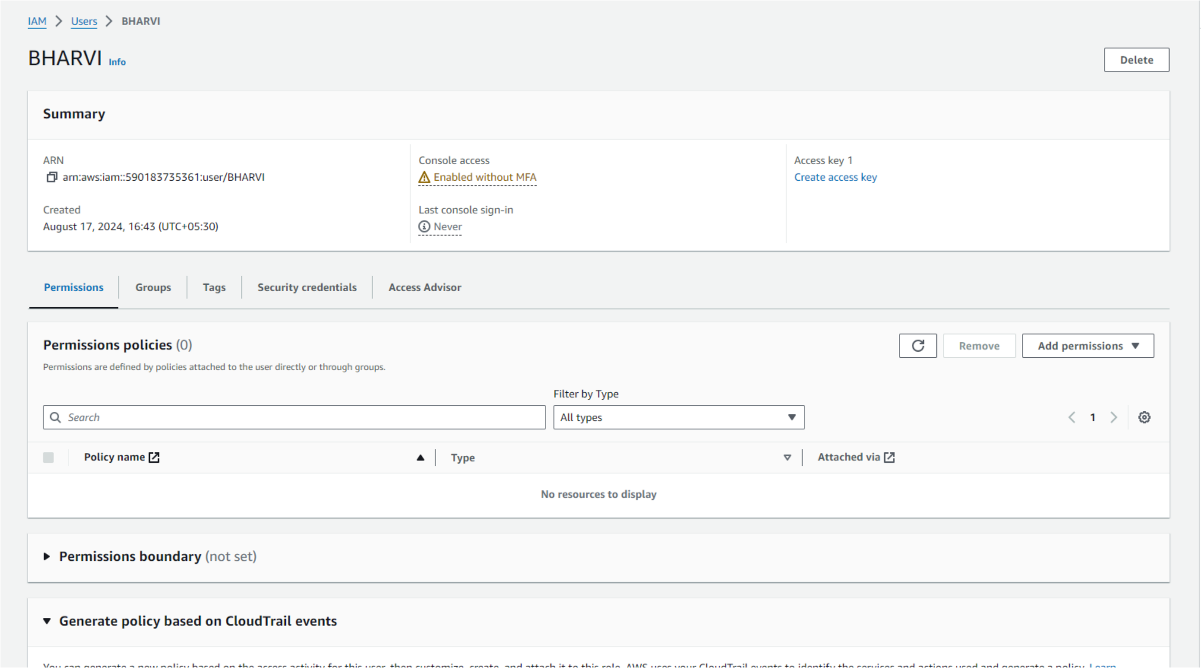
Policy userpolicy created.

Policies (1223)

A policy is an object in AWS that defines permissions.

Filter by Type: All types

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	-
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permiss...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifesizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...
AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to us...



BHARVI

Summary

ARN: arn:aws:iam::590183735361:user/BHARVI

Created: August 17, 2024, 16:43 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Create access key

Permissions policies (0)

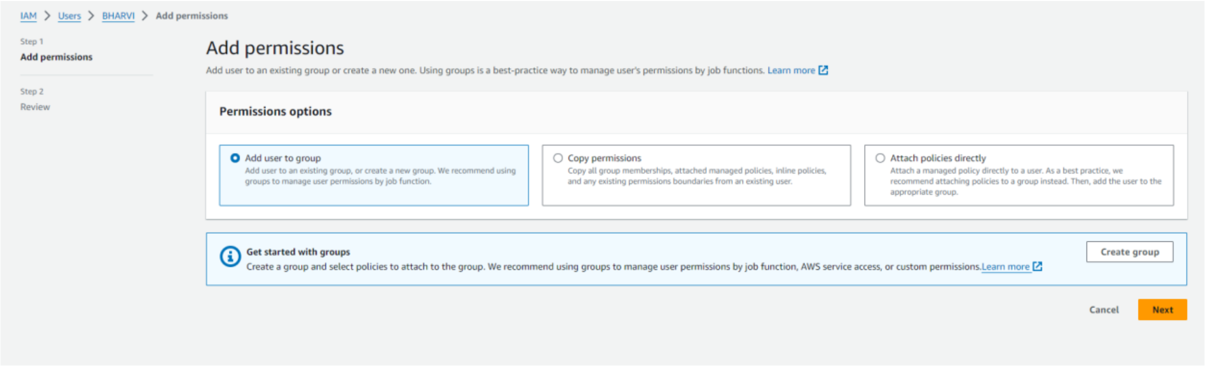
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
No resources to display		

Permissions boundary (not set)

Generate policy based on CloudTrail events



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

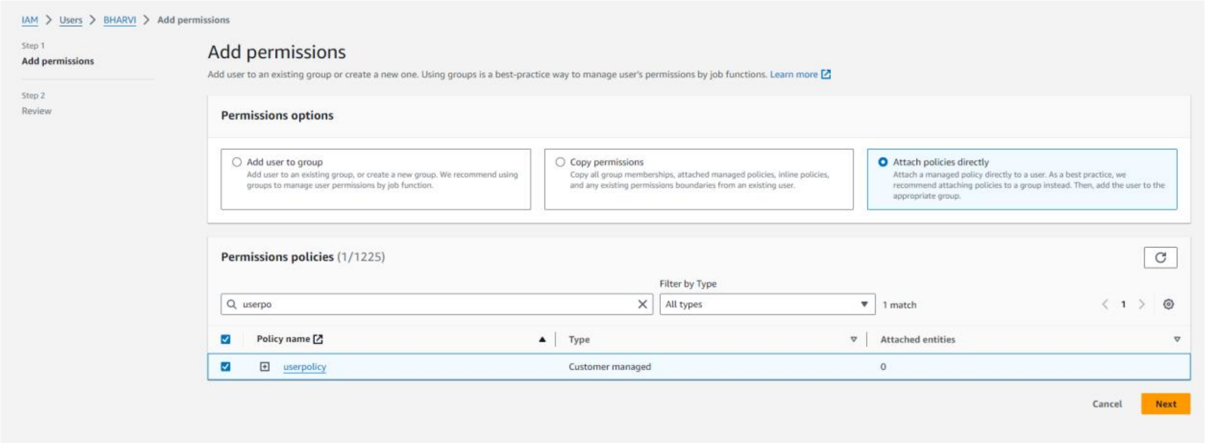
Permissions options

● 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.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.Learn more



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.

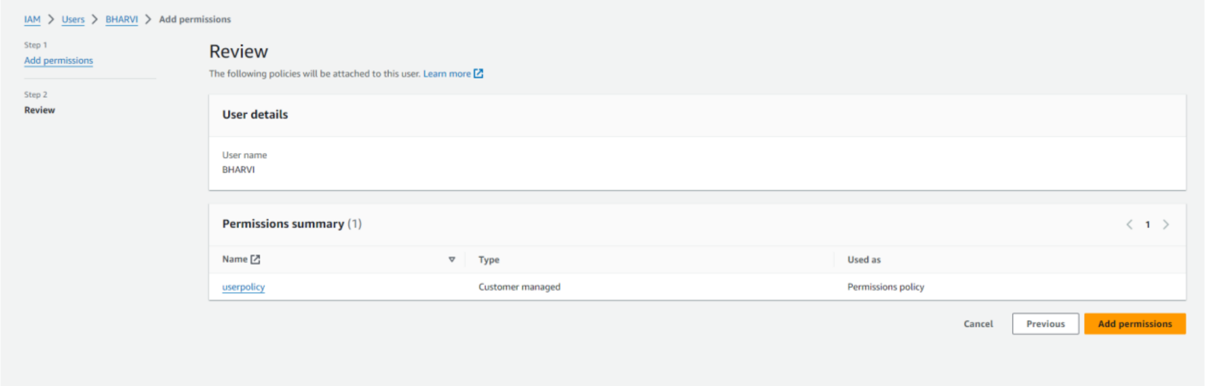
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1225)

Filter by Type

userpo | All types | 1 match

☑	Policy name	Type	Attached entities
☑	userpolicy	Customer managed	0



Review

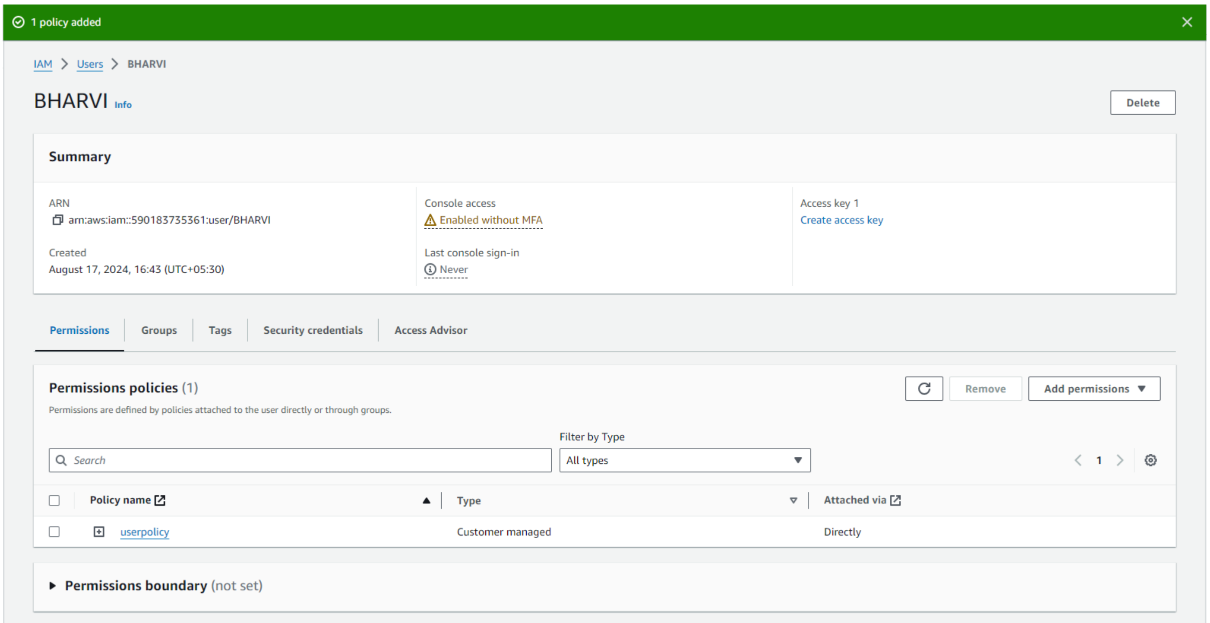
The following policies will be attached to this user. Learn more

User details

User name
BHARVI

Permissions summary (1)

Name	Type	Used as
userpolicy	Customer managed	Permissions policy



1 policy added

BHARVI

Summary

ARN
arn:aws:iam::590183735361:user/BHARVI

Created
August 17, 2024, 16:43 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

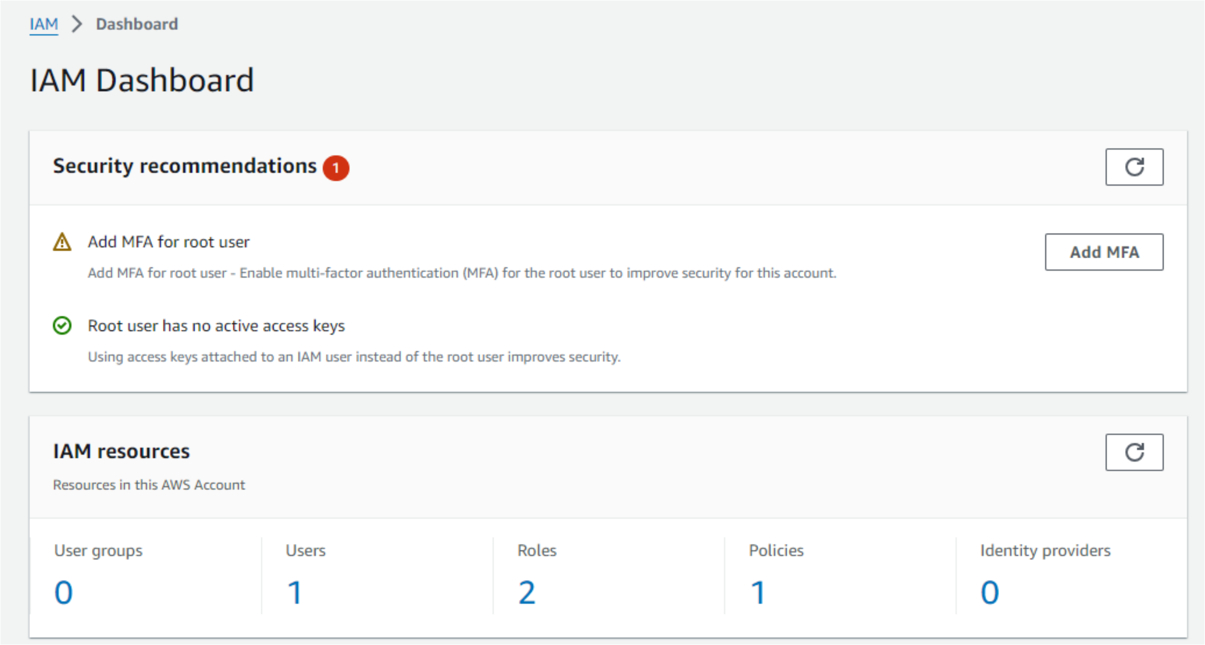
Access key 1
Create access key

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	userpolicy	Customer managed	Directly

▸ Permissions boundary (not set)



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.

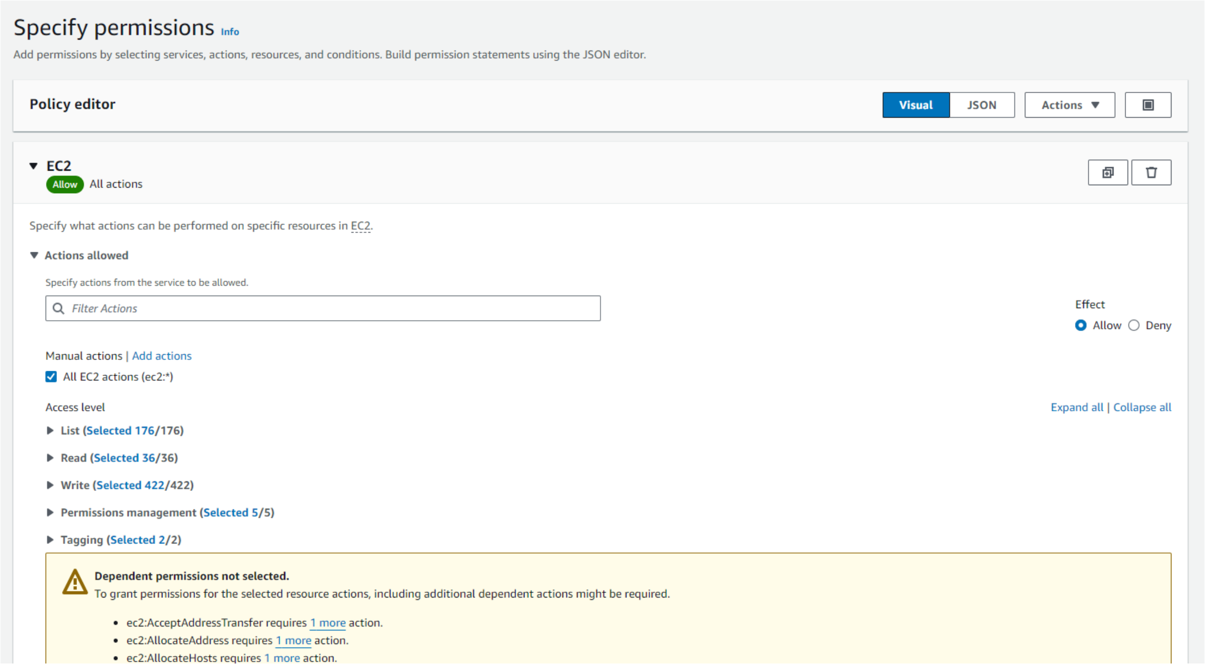
✓ Root user has no active access keys

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

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	1	2	1	0



Specify permissions Info

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

Policy editor

▼ EC2

Allow All actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed

Specify actions from the service to be allowed.

Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All EC2 actions (ec2:*)

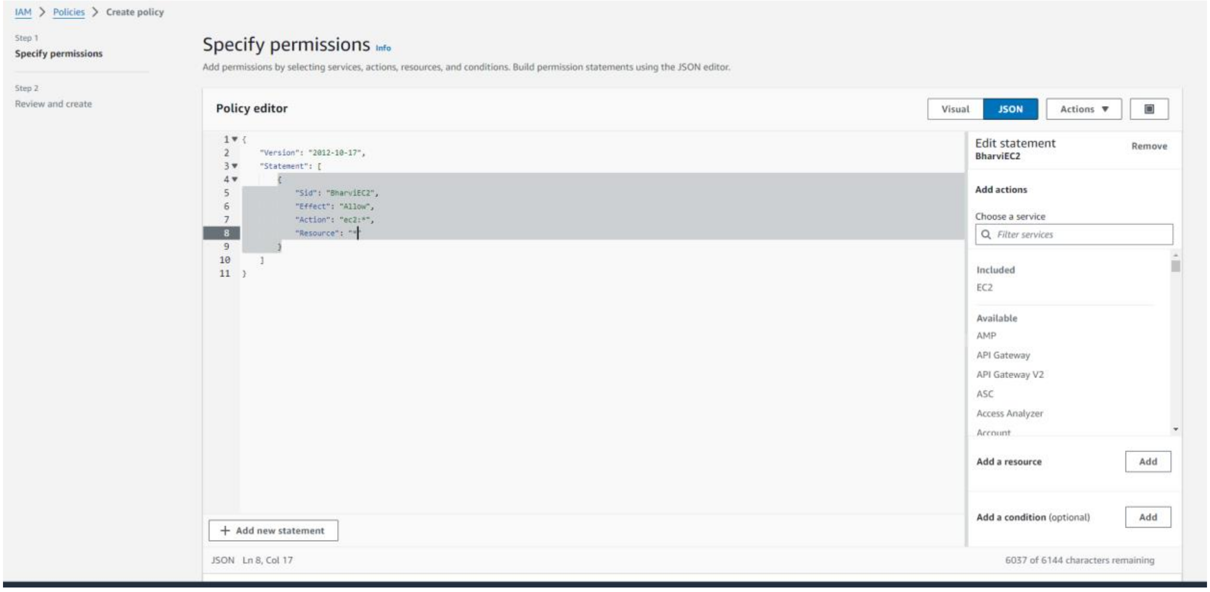
Access level

- ▶ List (Selected 176/176)
- ▶ Read (Selected 36/36)
- ▶ Write (Selected 422/422)
- ▶ Permissions management (Selected 5/5)
- ▶ Tagging (Selected 2/2)

⚠ **Dependent permissions not selected.**

To grant permissions for the selected resource actions, including additional dependent actions might be required.

- ec2:AcceptAddressTransfer requires 1 more action.
- ec2:AllocateAddress requires 1 more action.
- ec2:AllocateHosts requires 1 more action.



IAM > Policies > Create policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BharviEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
}
```

Edit statement
BharviEC2

Add actions

Choose a service

Included
EC2

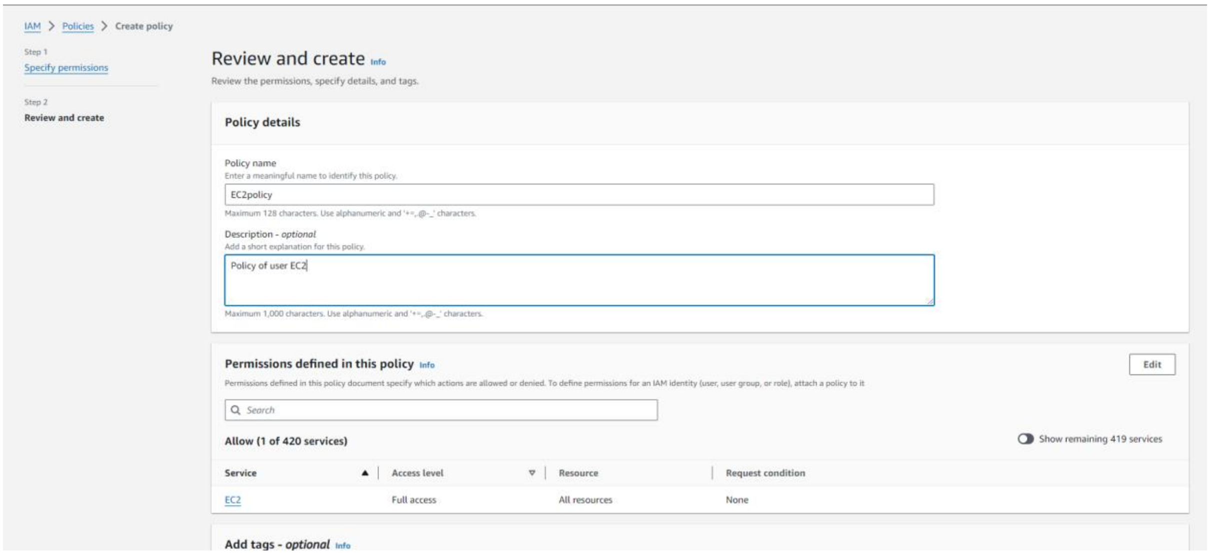
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account

Add a resource

Add a condition (optional)

JSON Ln 8, Col 17

6037 of 6144 characters remaining



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.
EC2policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
Policy of user EC2
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

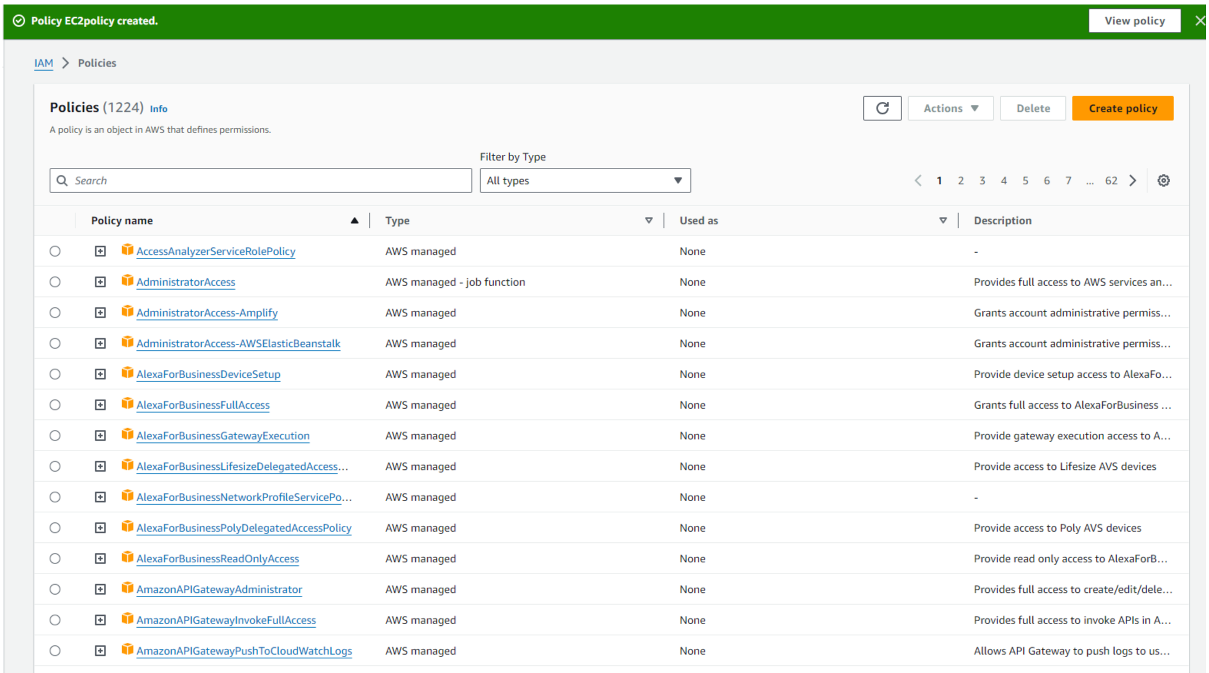
Permissions defined in this policy Info

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

Allow (1 of 420 services)

Service ▲	Access level ▽	Resource	Request condition
EC2	Full access	All resources	None

Add tags - *optional* Info



Policy EC2policy created.

IAM > Policies

Policies (1224) Info

A policy is an object in AWS that defines permissions.

Filter by Type
All types

	Policy name ▲	Type ▽	Used as ▽	Description
○	AccessAnalyzerServiceRolePolicy	AWS managed	None	-
○	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
○	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
○	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permiss...
○	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
○	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
○	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
○	AlexaForBusinessLifesizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
○	AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
○	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
○	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
○	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...
○	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
○	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to us...