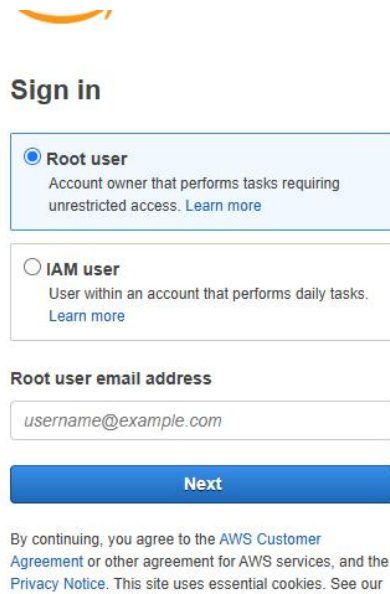


AWS IAM (Identity & Access Management)

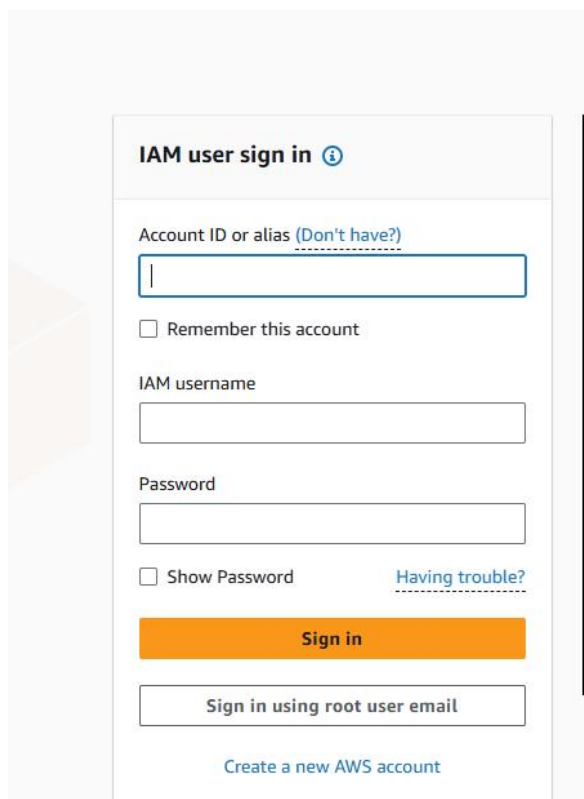
We are able to log into AWS cloud and use services -> two types of accounts -->
Root account and IAM account

Root is like the super user and no limitations. It is the most powerful account with no restrictions
If you want to place restrictions on user accounts, then we need IAM user. I can decide which user
should have what access



The image shows the AWS IAM 'Sign in' page. At the top is the AWS logo. Below it is the heading 'Sign in'. There are two radio button options: 'Root user' (selected) and 'IAM user'. The 'Root user' option has a description: 'Account owner that performs tasks requiring unrestricted access. [Learn more](#)'. The 'IAM user' option has a description: 'User within an account that performs daily tasks. [Learn more](#)'. Below these options is a text input field for 'Root user email address' with the placeholder text 'username@example.com'. A blue 'Next' button is below the email field. At the bottom, there is a disclaimer: 'By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Privacy Notice](#).'

Sign into AWS console, that's what we usually see



The image shows the AWS IAM 'IAM user sign in' screen. The title is 'IAM user sign in' with an information icon. Below the title is a text input field for 'Account ID or alias' with a link '(Don't have?)'. There is a checkbox for 'Remember this account'. Below that is a text input field for 'IAM username'. Then a text input field for 'Password'. There is a checkbox for 'Show Password' and a link 'Having trouble?'. A large orange 'Sign in' button is below the password field. Below the 'Sign in' button is a button that says 'Sign in using root user email'. At the bottom is a link 'Create a new AWS account'.

It is used to manage users, groups, policies and roles. IAM is a free service

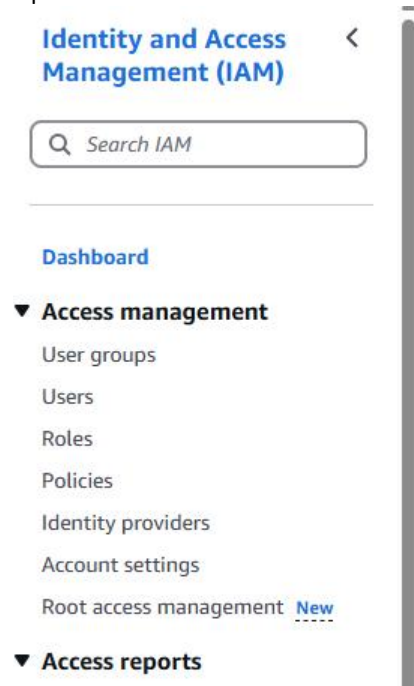
Root account is very powerful with no restrictions and we can access everything in AWS cloud

Key points to be considered for the root account:

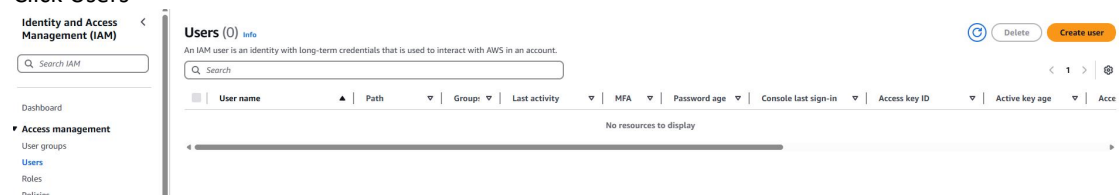
We should not use root account for daily task also we should not share root account credentials with anyone (it is also highly-recommended to enable high security by enabling Multi-Factor Authentication MFA for root users)

As a part of a project or team, we will not be getting root account credentials rather we will get IAM account credentials with specific access

Open IAM



Click Users



Create user

Specify user details

User details

User name

test_user

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 Key Management Service, you must provide a backup credential for emergency account access. [Learn more](#)

If you don't click 'Provide user access to the AWS management console - optional' then user cannot access AWS console through browser

User details

User name

test_user

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 applications.
☐ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Key Management Service, you must provide a backup credential for emergency account access. [Learn more](#)

Apart from browser access, AWS console can be accessed via AWS CLI, Terraform, Software Development Kit (SDK). Using Security key or Access key only we can access AWS console

Lets use the second option

☒ 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 applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ Autogenerated password
You can view the password after you create the user.

☐ 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 ! @

☒ 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

[Learn more](#)

‘Attach policies directly’ means what the user can access

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 (1335) [Create policy](#)

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

Search Filter by Type

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	AWS managed	0
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	0
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
<input type="checkbox"/>	AIOpsAssistantPolicy	AWS managed	0
<input type="checkbox"/>	AIOpsConsoleAdminPolicy	AWS managed	0
<input type="checkbox"/>	AIOpsOperatorAccess	AWS managed	0

I want to give only EC2 access

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

Filter by Type
All types

<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerRegistryPullOnly	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerRegistryReadOnly	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceAutoscaleRole	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceEventsRole	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	AWS managed
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeploy	AWS managed

In total, we can give 1335 permission policies to your user ---> AWS managed policies

Permissions policies (1/1335)

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

User details

User name test_user	Console password type Autogenerated	Require password reset No
------------------------	--	------------------------------

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel
Previous
Create user

Click Create user
Sign out of account

IAM user sign in ⓘ

Account ID or alias ([Don't have?](#))

☐ Remember this account

IAM username

Password

☐ Show Password [Having trouble?](#)

Sign in

Sign in using root user email

[Create a new AWS account](#)

IAM username

Password

☐ Show Password [Having trouble?](#)

Sign in

Sign in using root user email

[Create a new AWS account](#)

For example, Cost and usage is access denied

Canada (Central)test_user @ 5776-3838-6543

Reset to default layout

Add widgets

Applications (0) Info

Create application

Region: Canada (Central)

ca-central-1 (Current Region)

Find applications

< 1 >

Name

Description

Region

Originati

★ ▲

Access denied to servicecatalog:ListApplications

Diagnose with Amazon Q

Go to myApplications

Cost and usage Info

Current month costs

Access denied

Cost breakdown

Access denied

Forecasted month end costs

Access denied

Savings opportunities

Access denied

Only EC2 access is there for this user

Access denied when trying to create S3 bucket with the test_user

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Failed to create bucket

To create a bucket, the s3:CreateBucket permission is required.

View your permissions in the [IAM console](#) or [Identity and Access Management in Amazon S3](#)

API response

Cancel

Create bucket

Failed to create bucket

To create a bucket, the s3:CreateBucket permission is required.

View your permissions in the [IAM console](#) or [Identity and Access Management in Amazon S3](#)

API response

Login as root user

Users (1) [Info](#)

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

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password
<input type="checkbox"/>	test_user	/	0	25 minutes ago	-	29 minutes ago

Later also I can modify Permissions policies

Permissions policies (1) Remove Add permissions

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

		Filter by Type	
<input type="text" value="Search"/>		All types	< 1 >
<input type="checkbox"/> Policy name	Type		Attached via
<input type="checkbox"/> AmazonEC2FullAccess	AWS managed		Directly

▶ Permissions boundary (not set)

User groups are also there

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
--	---	---

No resources to display

I add users to user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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

Add users to the group - *Optional* (2/2) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application.

☒ | **User name** [?](#)

☒ [test_user](#)

☒ [test_user2](#)

Attach permissions policies - *Optional* (1/1038) [Info](#)

I add permissions to the user group

☒ | **User name** [?](#)

☒ [test_user](#)

☒ [test_user2](#)

Attach permissions policies - *Optional* (1/1038) [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](#)
All types

<input type="checkbox"/>	<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3FullAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3TablesFullAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3TablesReadOnlyAccess	AWS managed

User group is created

✔ AWSDevOpsGrp user group created.

User groups (1) [Info](#)

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

<input type="checkbox"/>	Group name	▲ Users	▼ Permissions
<input type="checkbox"/>	AWSDevOpsGrp	2	✔ Defined

Policies

AWS managed policies

Policies (1335) [Info](#)

A policy is an object in AWS that defines permissions.

Filter by Type

All types

	Policy name	▲ Type	▼ Usr
<input type="radio"/>	AccessAnalyzerServiceRolePolicy	AWS managed	No
<input type="radio"/>	AdministratorAccess	AWS managed - job function	No
<input type="radio"/>	AdministratorAccess-Amplify	AWS managed	No
<input type="radio"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	No
<input type="radio"/>	AIOpsAssistantPolicy	AWS managed	No
<input type="radio"/>	AIOpsConsoleAdminPolicy	AWS managed	No
<input type="radio"/>	AIOpsOperatorAccess	AWS managed	No
<input type="radio"/>	AIOpsReadOnlyAccess	AWS managed	No
<input type="radio"/>	AlexaForBusinessDeviceSetup	AWS managed	No

How to create my own policy?

Click Create policy

Specify permissions [Info](#)

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

Policy editor

▼ EC2

Set permissions for EC2.

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

▼ Actions allowed

Specify actions from the service to be allowed.

► Resources

Specify resource ARNs for these actions.

► Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

[+ Add more permissions](#)

I can select whatever policies I want to include

▼ S3

[Allow](#) 6 Actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Manual actions | [Add actions](#)

☐ All S3 actions (s3:*)

Access level

► List (16)

▼ Read (Selected 6/61)

☐ All read actions

☐ DescribeJob [Info](#)

☐ GetAccessGrant [Info](#)

☐ GetAccessGrantsInstanceResourcePolicy [Info](#)

☐ GetAccessPointConfigurationForObjectLambda [Info](#)

☐ GetAccessPointPolicyForObjectLambda [Info](#)

☐ GetAccountPublicAccessBlock [Info](#)

☐ GetBucketCORS [Info](#)

☐ GetBucketMetadataTableConfiguration [Info](#)

☐ DescribeMultiRegionAccessPointOperation

☐ GetAccessGrantsInstance [Info](#)

☐ GetAccessGrantsLocation [Info](#)

☐ GetAccessPointForObjectLambda [Info](#)

☐ GetAccessPointPolicyStatus [Info](#)

☐ GetAnalyticsConfiguration [Info](#)

☐ GetBucketLocation [Info](#)

☐ GetBucketNotification [Info](#)

I have created the custom policy

My_Policy

Info

Policy details

Type

Customer managed

Creation time

March 17, 2025, 00:48 (UTC-04:00)

Edited time

March 17, 2025, 00:48 (UTC-04:00)

Permissions

Entities attached

Tags

Policy versions

Last Accessed

Policy versions

(1)

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, role), you must specify the actions that the identity is allowed or denied to perform on the resource.

Search

Allow (2 of 440 services)

Service	Access level	Resource	Request condition
EC2	Limited: Read	All resources	None
S3	Limited: Read	All resources	None

I have got an extra option here: Custom managed

Policies (1336)

Info

A policy is an object in AWS that defines permissions.

Filter by Type

Customer managed

1 match

Search

Policy name	Type	Used as
<div><div></div><div>My_Policy</div></div>	Customer managed	None

We have two policies for this user group
One is AWS managed and other is Customer managed

AWSDevOpsGrp [Info](#)

Summary

User group name
AWSDevOpsGrp

Creation time
March 17, 2025, 00:34 (UTC-04:00)

Users
(2)

Permissions

Access Advisor

Permissions policies (2) [Info](#)

You can attach up to 10 managed policies.

Search		Filter by Type
<input type="text"/>		All types
<input type="checkbox"/>	Policy name ↗	Type
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed
<input type="checkbox"/>	My_Policy	Customer managed

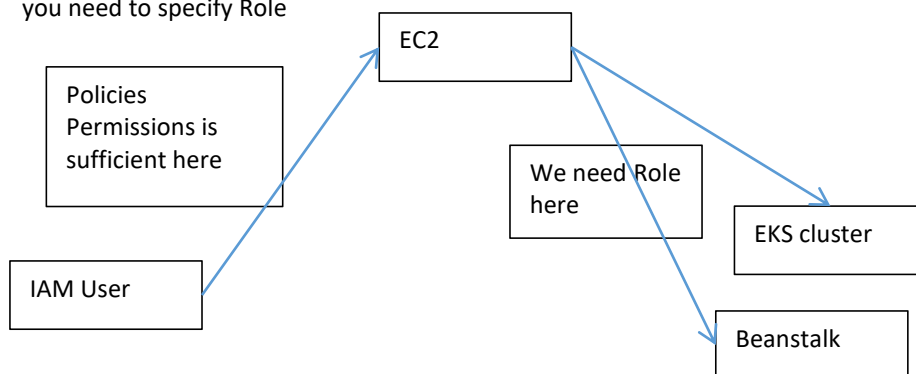
Roles

Roles (6) [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.

Search		
<input type="checkbox"/>	Role name	Trusted entities

IAM Roles: Inside AWS cloud we have a service EC2, say if the root user has given you (IAM User) a policy to access EC2. can you access EC2? Yes. From EC2, IAM user is accessing EKS, Beanstalk then you need to specify Role



We (IAM users) need 'Role' to access one service from another service.

Which Role you want to create?

> Create role

identity

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 with web identity providers 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.

Service or use case

Use case

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

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.










☐ **EC2 - Spot Fleet Tagging**

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ **EC2 - Spot Instances**

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ **EC2 - Spot Fleet**

<input type="checkbox"/>		AWSManagedEC2RoleCWL	AWS managed
<input type="checkbox"/>		AWSElasticBeanstalkRoleCWL	AWS managed
<input type="checkbox"/>		AWSElasticBeanstalkRoleECS	AWS managed
<input type="checkbox"/>		AWSElasticBeanstalkRoleRDS	AWS managed
<input type="checkbox"/>		AWSElasticBeanstalkRoleSNS	AWS managed
<input type="checkbox"/>		AWSElasticBeanstalkRoleWorkerTier	AWS managed
<input type="checkbox"/>		AWSElasticBeanstalkService	AWS managed
<input checked="" type="checkbox"/>		AWSElasticBeanstalkWebTier	AWS managed
<input checked="" type="checkbox"/>		AWSElasticBeanstalkWorkerTier	AWS managed

> Set permissions boundaries (optional)

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,., @-/ \[{}]!#\$%^&*()';:~`

My_Role is added to the list of Roles

Roles (7) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short duration

<input type="checkbox"/>	Role name	Trusted entities
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	AWS Service: autosca
<input type="checkbox"/>	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticl
<input type="checkbox"/>	AWSServiceRoleForRDS	AWS Service: rds (Ser
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: suppor
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trusted
<input type="checkbox"/>	My_Role	AWS Service: ec2
<input type="checkbox"/>	rds-monitoring-role	AWS Service: monito

Role demo:

Now I got into EC2 and create an instance

EC2

<

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Instances (2) [Info](#)

<input type="checkbox"/>	Name ✎	Instance ID	Instance state ▼	Instance type
<input type="checkbox"/>	DevOpsCourse...	i-0f87d8181852ad376	⏸ Stopped ⚙ 🔍	t2.micro
<input type="checkbox"/>	TestEC2_Role	i-0352efdaf5910d18f	🟢 Running ⚙ 🔍	t2.micro

Click on Actions ---> Security ---> Modify IAM role

⌂

Connect

Instance state [▼](#)

Actions [▲](#)

Launch instances

Availability Zone [▼](#)

Public IPv4 DNS

ca-central-1b

ca-central-1b

ec2-99-79-59-242.ca-c

Connect

View details

Manage instance state

Instance settings [▶](#)

Networking [▶](#)

Security [▶](#)

Image and templates [▶](#)

Monitor and troubleshoot [▶](#)

Change security groups

Get Windows password

Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

 i-0352efdaf5910d18f (TestEC2_Role)

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.

Choose IAM role



Create new IAM role [↗](#)



If you choose **No IAM Role**, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?

I select My_Role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

 i-0352efdaf5910d18f (TestEC2_Role)

IAM role

Select an IAM role to attach to your instance or

My_Role

Click Modify IAM Role

Now can you access Elastic BeanStalk from this EC2? YES

Role provide Service to Service access


I create another User

Now, Create access key

test_user [Info](#)

Summary

ARN

 arn:aws:iam::577638386543:user/test_user

Created

March 17, 2025, 01:29 (UTC-04:00)

Console access

Disabled

Last console sign-in

-

Access key 1

[Create access key](#)

Permissions

Groups

Tags

Security credentials

Last Accessed

Console sign-in

Console sign-in link

 <https://577638386543.signin.aws.amazon.com/console>

Console password

Not enabled

Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

☐ **Command Line Interface (CLI)**
You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**
You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

☐ **Other**
Your use case is not listed here.

Application running outside AWS means SDK

CLI

☒ **Command Line Interface (CLI)**
You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**
You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

☐ **Other**
Your use case is not listed here.

⚠ Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

Confirmation
☒ I understand the above recommendation and want to proceed to create an access key.

[Cancel](#) [Next](#)

We need both Security access key and Access key for CLI access

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

Access key

Secret access key



AKIAYM7POJNXRPKLJ3RF



***** [Show](#)

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

We have understood about User, UserGroups, Policies --> AWS managed policies, Customer managed policies, Roles -->