

# Criação do usuário IAM na AWS

Para a criação dos recursos na AWS através do AWS CDK na máquina de desenvolvimento, é necessário criar um usuário na conta da AWS, com permissões de administrador, como será detalhado nos passos a seguir.

## 1) Criação do usuário no IAM

Para utilizar o AWS CLI e fazer o deployment da infraestrutura criada com o projeto do AWS CDK, é necessário primeiro criar um usuário no AWS IAM com permissões específicas. As credenciais desse usuário serão utilizadas no tópico seguinte. Para começar, abra o console da AWS e vá até o serviço IAM.

Dentro desse console, clique no menu lateral esquerdo, na opção `Access Management -> Users`, como na figura a seguir:

### Identity and Access Management (IAM) ✕

Dashboard

#### ▼ Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Nessa tela, clique no botão `Add user`, no canto superior direito da página.

Na primeira tela de criação do usuário, digite um nome que você desejar e **DEIXE DESMARCAD**A a opção `Enable console access`, como na figura a seguir:

# Specify user details

User details

User name

aws\_cdk

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

☐ Enable console access - optional

Enables a password that allows users to sign in to the AWS Management Console.

For programmatic access, you can generate access keys after you create the user. [Learn more](#)

Em seguida clique em `Next`. Nessa tela, selecione a opção `Attach policies directly` e escolha a política de nome `Administrator 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 (1/1085)

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

Filter distributions by text, property or value

< 1 2 3 4 5 6 7 ... 55 >

	Policy name	Type	Attached entities
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	AWS managed	0
<input checked="" type="checkbox"/>	AdministratorAccess	AWS managed - job function	3

Create policy



Continue clicando no botão `Next`, até a última tela para a criação efetiva do usuário. Nessa tela, clique no botão `Create user`. Após a criação do usuário, você verá a lista de todos os usuários do IAM que você possui, como no exemplo a seguir:

<b>Users (2)</b> <a href="#">Info</a> An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.				
<input type="text"/> Find users by username or access key				
<input type="checkbox"/>	User name	Groups	Last activity	MFA
<input type="checkbox"/>	amplify	None	✓ 9 days ago	None
<input type="checkbox"/>	aws_cdk	None	Never	None

Na lista onde seu recém criado usuário aparece, clique no nome dele para ser redirecionado para a página com as credenciais de acesso:

[IAM](#) > [Users](#) > [aws\\_cdk](#)

## aws\_cdk

<b>Summary</b>	
ARN  arn:aws:iam::946835467386:user/aws_cdk	Console access Disabled
Created February 13, 2023, 10:10 (UTC-03:00)	Last console sign-in -
<div> <a href="#">Permissions</a> <a href="#">Groups</a> <a href="#">Tags</a> <a href="#">Security credentials</a> <a href="#">Access Advisor</a> </div>	
<b>Console sign-in</b>	
Console sign-in link  https://946835467386.signin.aws.amazon.com/console	Console password Not enabled

Nessa tela, clique na aba `Security credentials` e vá até a sessão `Access keys`:

## Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls.

Create access key

## No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools v

Create access key

Nessa sessão, clique no botão `Create access key`. Na tela seguinte, selecione a opção `Command Line Interface (CLI)`, como mostra a figura a seguir:

## Access key best practices & alternatives

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

### ☒ Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

Nessa tela, clique no botão `Next` e em seguida no botão `Create access key`.

A tela seguinte exibirá a chave de acesso que foi criada para esse usuário. Copie os valores de `Access key` e `Secret access key`. Essa credencial será utilizada no tópico seguinte.

## 2) Configuração do AWS CLI com as credenciais do usuário criado no IAM

Para configurar o AWS CLI da sua máquina de desenvolvimento, é necessário fornecer as credenciais do usuário criado no IAM no tópico anterior. Para isso, abra um terminal e digite o seguinte comando:

```
aws configure
```

No primeiro parâmetro solicitado, informe a `Access Key ID` do usuário criado no IAM. Em seguida, forneça a `Secret Access Key`. O terceiro parâmetro é a região desejada, que deve ser `us-east-1`. O último parâmetro é o formato da saída dos comandos, que pode ser configurado como `json`.

Todos os recursos que forem criados com o AWS CDK, durante esse curso, serão criados em nome desse usuário.



[siecola.com.br](http://siecola.com.br)