

Paso 1

Acceder a la consola de AWS mediante el siguiente link:

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

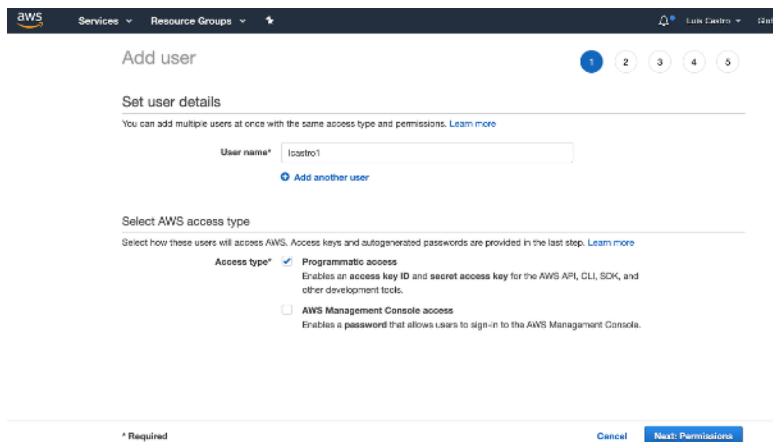
Paso 2

Ingresar al servicio de **Identity Access Management** y escoger **Users>Create New Users**

Crear un usuario con el mismo nombre de usuario agregando el numero 1

- Ej: lcastro1

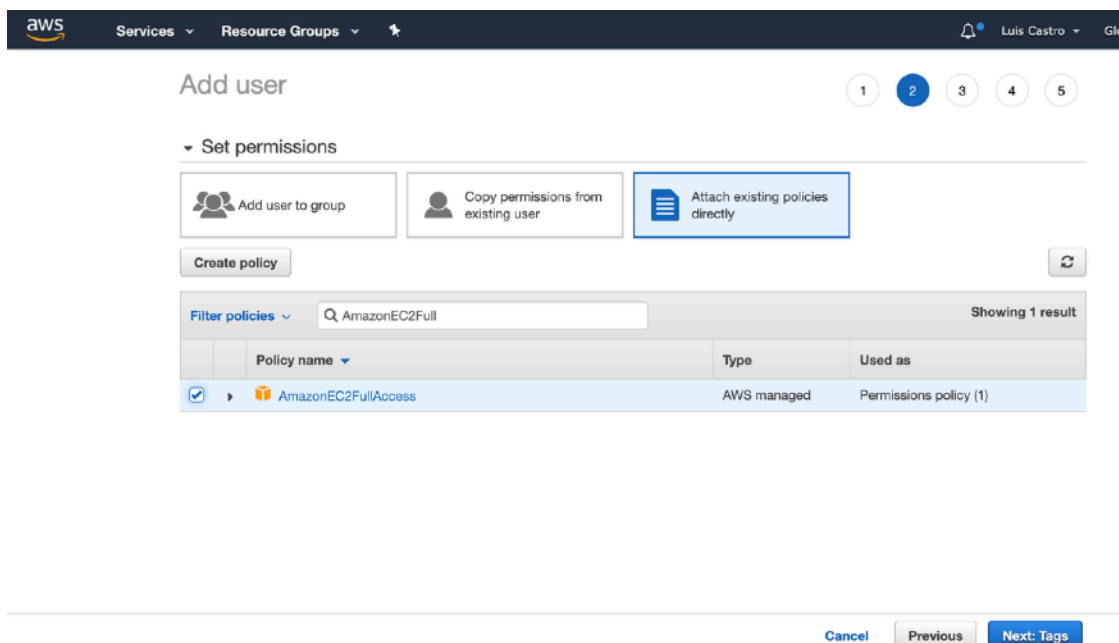
Marcar **Programmatic Access**



The screenshot shows the 'Add user' page in the AWS IAM console. The 'Set user details' section is active, showing the 'User name' as 'lcastro1'. Below this, the 'Select AWS access type' section shows 'Programmatic access' selected, which enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools. The 'AWS Management Console access' option is unselected. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

Paso 3

Set Permissions y hacer click en **Attach existing policies directly** y buscar la política **AmazonEC2FullAccess**



The screenshot shows the 'Add user' page in the AWS IAM console, now at the 'Set permissions' step. The 'Attach existing policies directly' option is selected. Below this, there is a search bar with 'AmazonEC2Full' entered, and a table showing the search results. The table has columns for 'Policy name', 'Type', and 'Used as'. The result shown is 'AmazonEC2FullAccess', which is an 'AWS managed' policy used as a 'Permissions policy (1)'. At the bottom, there are 'Cancel', 'Previous', and 'Next: Tags' buttons.

Policy name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy (1)

Paso 4

Create User

Services

Resource Groups

★

🔔

Luis Castro

G

Add user

1

2

3

4

5

Review

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

User details

User name

lcastro1

AWS access type

Programmatic access - with an access key

Permissions boundary

Permissions boundary is not set

Permissions summary

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

Type	Name
Managed policy	AmazonEC2FullAccess

Tags

No tags were added.

Cancel

Previous

Create user

Paso 5

Download Access Key

Add user

1

2

3

4

5

✓

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://lcastro1e.signin.aws.amazon.com/console>

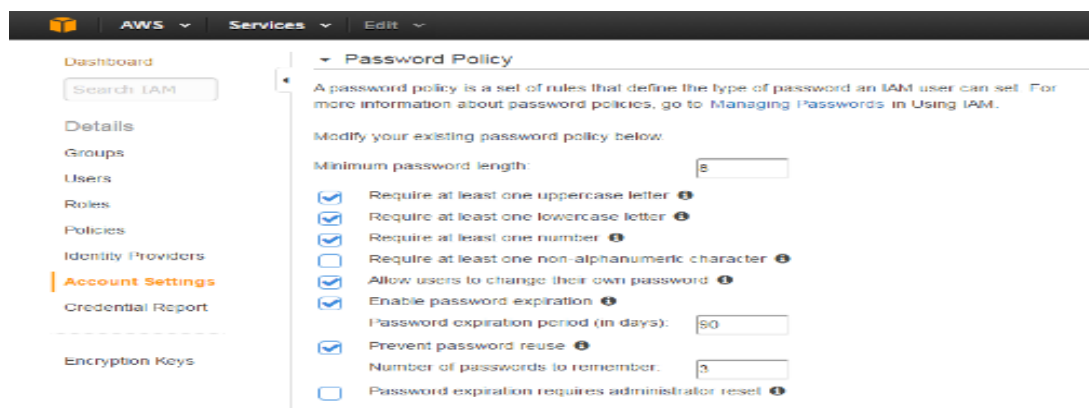
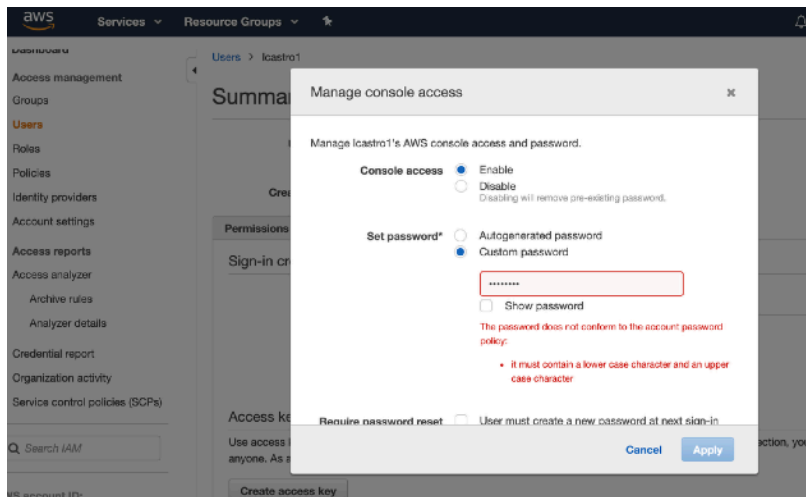
Download .csv

User	Access key ID	Secret access key
▶ ✓ lcastro1	AKIARYHDXUF35JP63XDZ	***** Show

Paso 5

Marcar el usuario creado en el panel principal y hacer click en **Users>Security Credentials>Console Password>Manage**

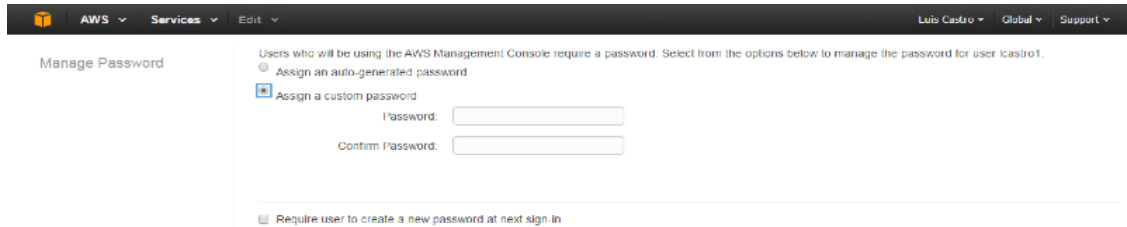
- **Enable Access**
- **Custom password**
 - Utilice primeramente el siguiente password
 - 12345678
 - Verifique el mensaje de error
 - Vaya al menú principal en **Account Settings** y valide las políticas de Password



Paso 6

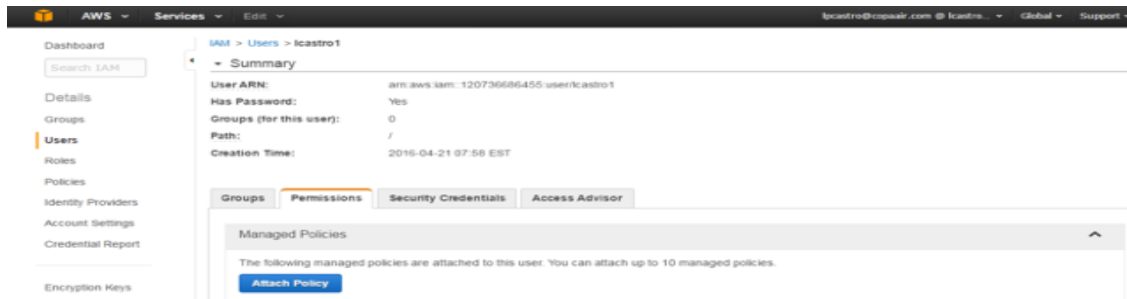
Vuelva nuevamente a **Users>Security Credentials>Console Password>Manage**

- Cree un password de su conveniencia siguiendo los lineamientos de password definidos
- Deje sin marcar
 - **Require user to create a new password at Next sign-in**



Paso 7

Marcar el usuario creado en el panel principal y hacer click en el tab de **Permissions>Attach Policy**



- Buscar la política **AmazonEC2FullAccess**



- Seguidamente marque **Simulate Policy**
 - Marque su usuario y la política creada (En caso que no lo tome automáticamente)

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

Has Password: Yes

Groups (for this user): 0

Path: /

Creation Time: 2016-04-21 07:58:58

Groups Permissions Security Credentials Access Advisor


Managed Policies

The following managed policies are attached to this user. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AmazonEC2FullAccess	Show Policy Detach Policy Simulate Policy

- Se abrirá un nuevo Browser, selecciones los siguientes servicios uno a uno, **Select All** y dele click en Run Simulation :
 - **S3, VPC, Route53 y Cloudfront**
 - Valide que las acciones son negadas


IAM Policy Simulator

Mode : Listing Policies -
ipcastro@copart.com -

Policies

Editing policy: **AmazonEC2FullAccess**

AWS Managed Policy

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "ec2:*",
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "elasticloadbalancing:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow"
    }
  ]
}

```

Policy Simulator


AWS CloudFor... 20 Action(s) sel... Select All Deselect All Reset Contexts Clear Results Run Simulation

Global Settings ⓘ

Action Settings and Results (20 actions selected, 0 actions not simulated, 0 actions allowed, 20 actions denied.)

Service	Action	Resource Type	Simulation Resource	Permission
AWS CloudFormation	CancelUpdateStack	stack	*	denied implicitly denied (no matc...
AWS CloudFormation	CreateStack	stack	*	denied implicitly denied (no matc...
AWS CloudFormation	CreateOrUpdateStack	not required	*	denied implicitly denied (no matc...
AWS CloudFormation	DeleteStack	stack	*	denied implicitly denied (no matc...
AWS CloudFormation	DescribeAccountLimits	not required	*	denied implicitly denied (no matc...
AWS CloudFormation	DescribeStackEvents	stack	*	denied implicitly denied (no matc...
AWS CloudFormation	DescribeStackResource	stack	*	denied implicitly denied (no matc...
AWS CloudFormation	DescribeStackResources	stack	*	denied implicitly denied (no matc...
AWS CloudFormation	DescribeStacks	stack	*	denied implicitly denied (no matc...

- Haga click en **Deselect All** y escoja el servicio de **EC2** y **Select All, Run Simulator**
- Valide que las acciones son permitidas


IAM Policy Simulator

Mode: Loading Policies -
ipcsato@openpan.com -

Policies
Back

Editing policy: **AmazonEC2FullAccess**
 AWS Managed Policy

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "ec2:*",
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "elasticloadbalancing:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow"
    }
  ]
}

```

Policy Simulator

Amazon EC2
196 Action(s) selected
Select All
Deselect All
Reset Contexts
Clear Results
Run Simulation

Global Settings


Action Settings and Results [207 actions selected 0 actions not simulated 196 actions allowed 11 actions denied]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	AcceptVpcPeeringConnec...	vpc-peering-conne...	*	allowed 1 matching statements.
Amazon EC2	ActivateLicense	not required	*	allowed 1 matching statements.
Amazon EC2	AllocateAddress	not required	*	allowed 1 matching statements.
Amazon EC2	AssignPrivateIpAddresses	not required	*	allowed 1 matching statements.
Amazon EC2	AssociateAddress	not required	*	allowed 1 matching statements.
Amazon EC2	AssociateDhcpOptions	not required	*	allowed 1 matching statements.
Amazon EC2	AssociateRouteTable	not required	*	allowed 1 matching statements.
Amazon EC2	AttachClassicLinkVpc	Instance.security-g...	*	allowed 1 matching statements.

Paso 8

Haga click en Dashboard en el menú principal de AIM y utilice el **IAM users sign-in link** para probar el acceso del nuevo usuario:

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



Account:

User Name:

Password:

MFA users, enter your code on the next screen.

- Haga click en el servicio de AWS RDS y valide si tiene permisos para acceder a las configuraciones



- Seguidamente entre a los servicios de **VPC, CloudFormation y Cloudfront** y debería de comportarse de la misma manera
- Entre al servicio de **EC2** y cree una nueva instancia **t2.micro** con valores **default**