

Paso 1

Acceder a la consola de AWS mediante el siguiente link:

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

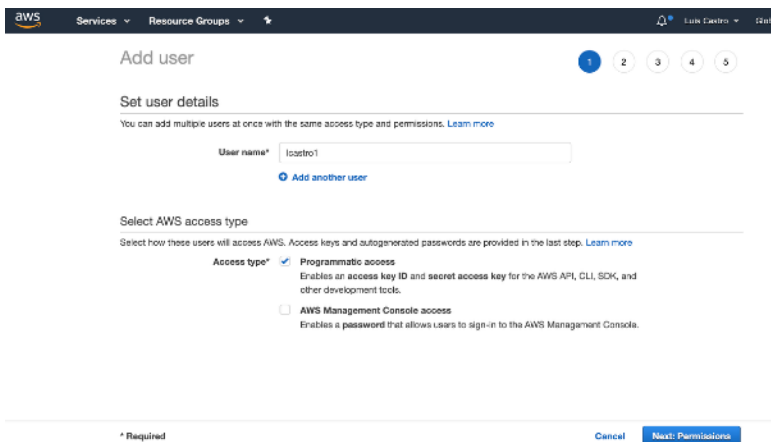
Paso 2

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

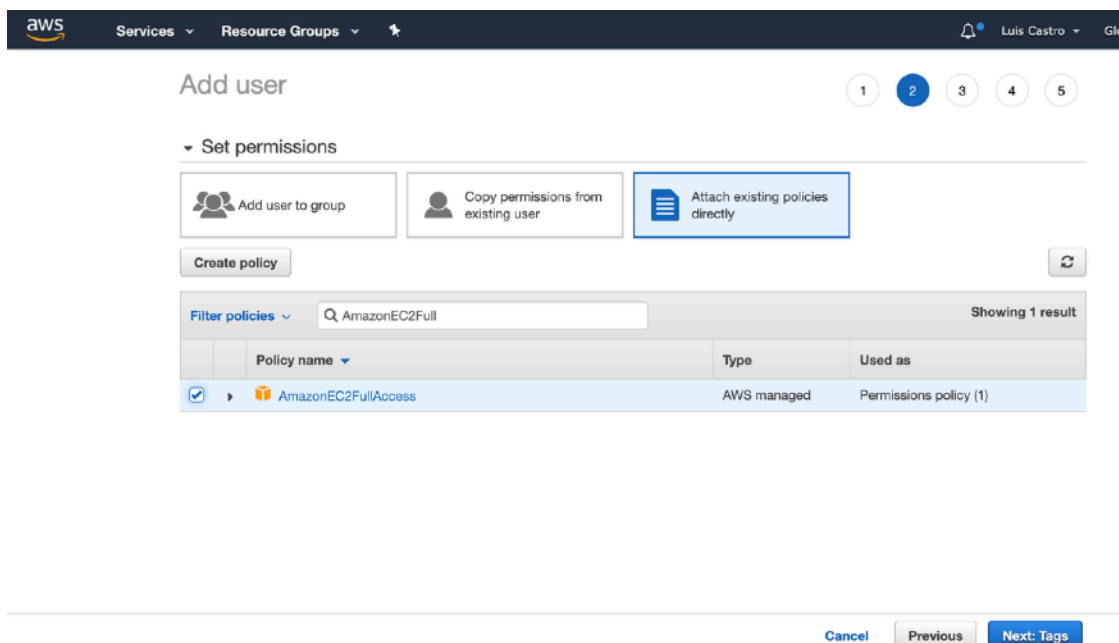
Marcar **Programmatic Access**



The screenshot shows the 'Add user' wizard in the AWS IAM console. Step 1 of 5 is 'Set user details'. The 'User name' field contains 'lcastro1'. Under 'Select AWS access type', 'Programmatic access' is selected, which enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools. 'AWS Management Console access' is not selected. 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' wizard in the AWS IAM console, step 2 of 5: 'Set permissions'. Three options are available: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly' (which is selected). Below these options is a 'Create policy' button. A search bar contains 'AmazonEC2Full'. The results table shows one result: '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://lcastro1.signin.aws.amazon.com/console>

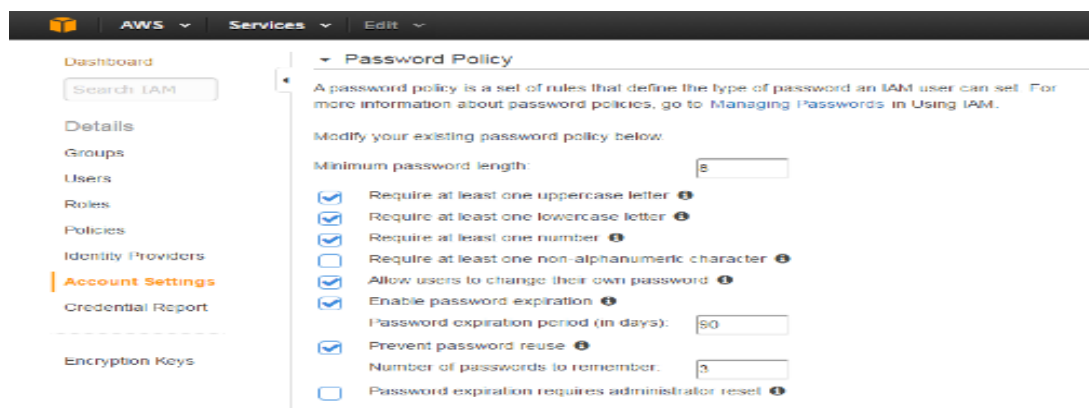
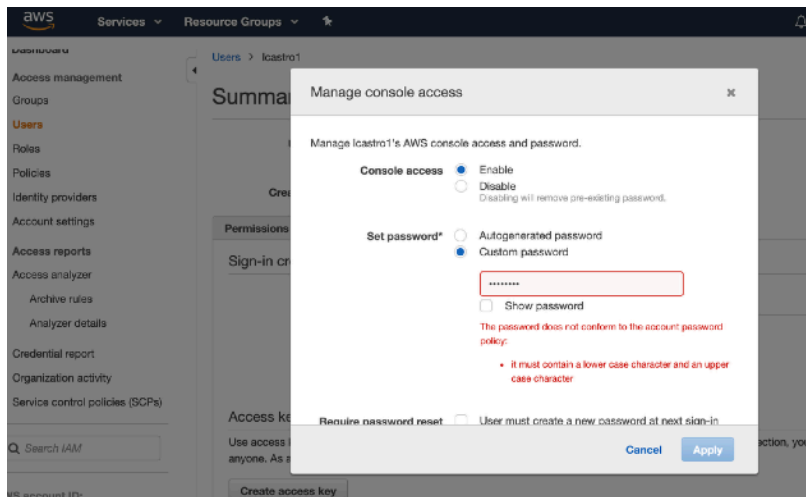
Download .csv

| 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**

AWS

Services

▼

Edit

▼

Luis Castro

▼

Global

▼

Support

▼

Manage Password

Users who will be using the AWS Management Console require a password. Select from the options below to manage the password for user lcastro1.

☐ Assign an auto-generated password

☒ Assign a custom password

Password:

Confirm Password:

☐ 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**

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Search IAM, Details, Groups, Users (highlighted), Roles, Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The main content area shows the 'Users' page for 'icastro1'. The 'Summary' tab is active, displaying the following information:

- User ARN: arn:aws:iam::120736686455:user/icastro1
- Has Password: Yes
- Groups (for this user): 0
- Path: /
- Creation Time: 2016-04-21 07:58 EST

Below the summary, there are four tabs: Groups, Permissions (selected), Security Credentials, and Access Advisor. Under the 'Permissions' tab, there is a section titled 'Managed Policies' with an upward arrow icon. A message states: 'The following managed policies are attached to this user. You can attach up to 10 managed policies.' Below this message is a blue button labeled 'Attach Policy'.

- Buscar la política **AmazonEC2FullAccess**

AWS

Services

Edit

ipcastro@copair.com

ipcastro...

Global

Support

Attach Policy

Attach Policy

Select one or more policies to attach. Each user can have up to 10 policies attached.

Filter: Policy Type

Q/T filter

Showing 107 results

| | Policy Name | Attached Entities | Creation Time | Edited Time |
|--|---------------------|-------------------|----------------------|----------------------|
| | AmazonEC2FullAccess | 4 | 2015-02-06 13:40 EST | 2015-02-06 13:40 EST |

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

Services

Edit

ipad.rupkoppesit.com @ kaskr...

Global

Support

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 EST

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 |
|---------------------|---|
| Amazon.C2F ulAccess | 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, Route53 y Cloudfront**
 - Valide que las acciones son negadas


IAM Policy Simulator

Mode : Listing Policies >
ipcasto@copium.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",
      "Action": "iam:*",
      "Resource": "*"
    }
  ]
}

```

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 | 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 -
ipcast@ipcast.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 ⓘ

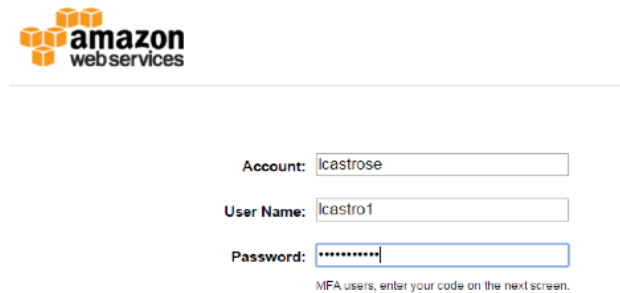
Action Settings and Results [202 actions selected 0 actions not simulated 196 actions allowed 6 actions denied]

| 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>



amazon
webservices

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**