

LABORATORIO 6

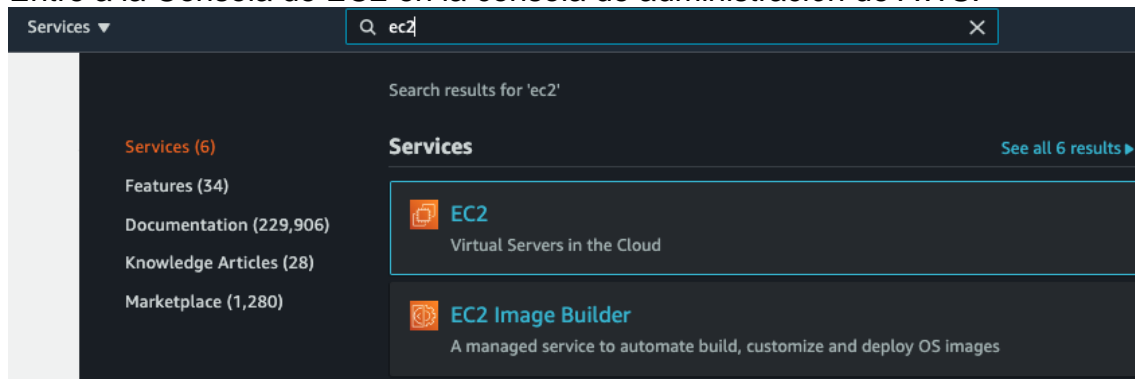
Este laboratorio práctico se divide en las siguientes partes:

1. Lanzar instancias de EC2 con etiquetas
2. Crear identidades de AWS IAM
3. Probar el acceso a los recursos
4. Asignar el rol de IAM para la instancia de EC2 y probar el acceso

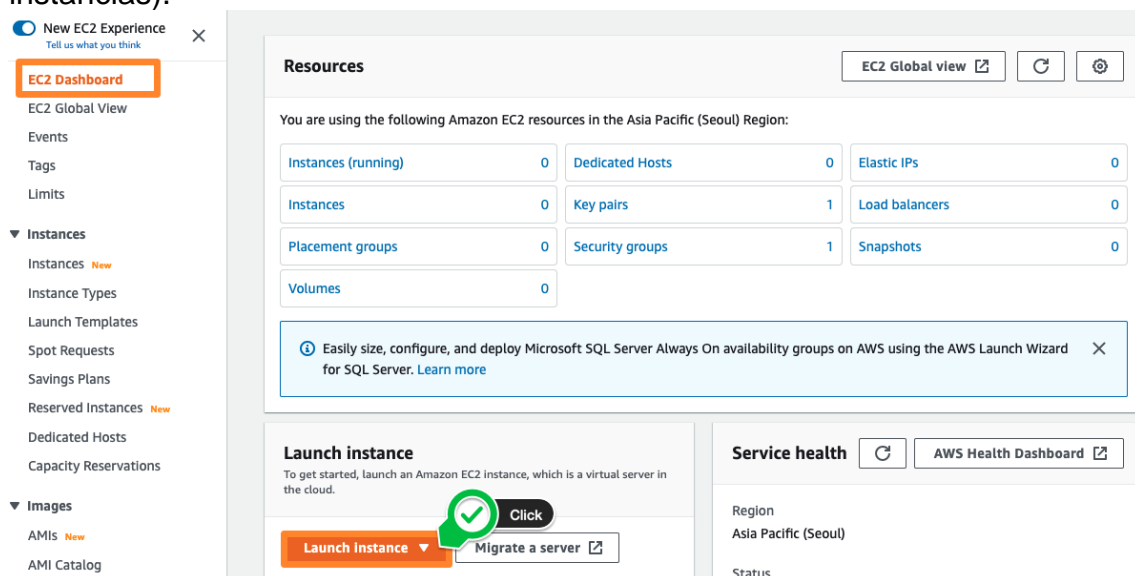
Lanzar instancias EC2 con etiquetas

En este laboratorio, lanzaremos dos instancias de Amazon Linux 2. Supongamos que una es una instancia de EC2 que se usa en un entorno de desarrollo y la otra se usa en un entorno de producción. Usaremos **etiquetas** para distinguir estas dos instancias.

Entre a la Consola de EC2 en la consola de administración de AWS.



Haga clic en **EC2 Dashboard** (Panel de EC2) cerca de la parte superior del menú de la izquierda. Luego, haga clic en **Launch instances** (Lanzar instancias).



En **Name** (Nombre), ingrese el valor **prod-instance**. Y haga clic en **Add additional tags** (Agregar etiquetas adicionales).

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

Haga clic en **Add tag** (Agregar etiqueta), luego en **Key** (Clave) e ingrese **Env** (Entorno), y en **Value** (Valor) ingrese **prod** (producción).

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

▼ **Name and tags** [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

48 remaining (Up to 50 tags maximum)

Compruebe la configuración predeterminada de imagen de máquina de Amazon y seleccione **t2.micro** en Instance Type (Tipo de instancia).

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux
aws

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0022f774911c1d690 (64-bit (x86)) / ami-0e449176cecc3e577 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220426.0 x86_64 HVM gp2

Architecture

AMI ID

64-bit (x86) ▼

ami-0022f774911c1d690

▼ Instance type [Info](#)

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible ▼

[Compare instance types](#)

En **Key pair (login)** (Par de claves [inicio de sesión]), seleccione **Proceed without a key pair** (Continuar sin un par de claves). Luego, haga clic en **Launch instance** (Lanzar instancia).

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Proceed without a key pair (Not recommended) Default value ▼

Create new key pair

Regions in which t2.micro is unavailable)
instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet

Cancel

Launch instance

Ha lanzado una instancia de EC2 para el entorno de producción. Ahora tiene que crear **una instancia de EC2 más para el entorno de desarrollo**. Repita las instrucciones anteriores (comience por el n.º 1 y siga hasta el n.º 5), pero con una etiqueta de Name (Nombre) y de Env (Entorno) diferentes en el paso n.º 2 y el paso n.º 3 de la siguiente manera.

CLAVE	VALOR
-------	-------

Name (Nombre)	dev-instance
---------------	--------------

Env (Entorno)	dev
---------------	-----

▼ Name and tags [Info](#)

Key Info	Value Info	Resource types Info
<input type="text" value="Name"/>	<input type="text" value="dev-instance"/>	<input type="text" value="Select resource types"/>
<input type="button" value="X"/>	<input type="button" value="X"/>	<input type="button" value="Instances"/>

Key Info	Value Info	Resource types Info
<input type="text" value="Env"/>	<input type="text" value="dev"/>	<input type="text" value="Select resource types"/>
<input type="button" value="X"/>	<input type="button" value="X"/>	<input type="button" value="Instances"/>

48 remaining (Up to 50 tags maximum)

Después de lanzar las dos instancias, puede encontrarlas en el menú de instancias de la barra lateral. Haga clic en la casilla de verificación de prod-instance y haga clic en la pestaña **Tags** (Etiquetas) en la parte inferior de la página. Puede ver detalles sobre la información de las etiquetas de esta instancia de EC2.

Instances (1/2) Info

1. Click

	Instance ID	Instance state	Instance type	Status check
<input checked="" type="checkbox"/> prod-instance	i-0e0218d4da46f0767	Running	t2.micro	Initializing
<input type="checkbox"/> dev-instance	i-0fdcb8a9f7e28c41e	Running	t2.micro	-

Instance: i-0e0218d4da46f0767 (prod-instance)

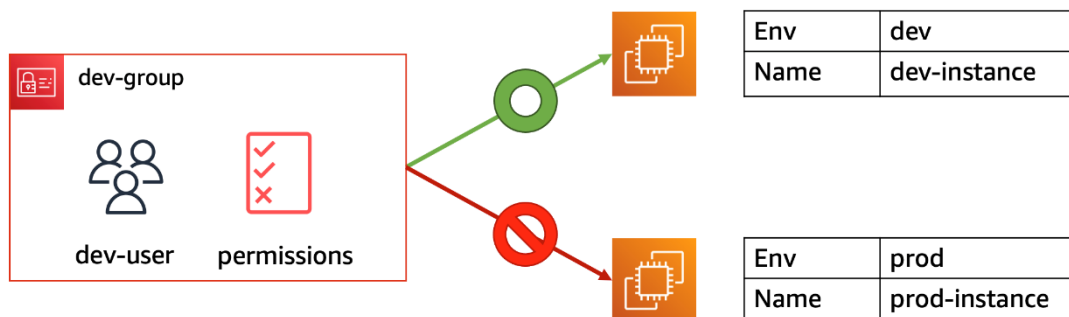
2. Click

Tags

Key	Value
Env	prod
Name	prod-instance

Crear identidades de IAM de AWS

En este capítulo, trabajaremos en la creación de **identidades de AWS IAM**. Una entidad de AWS IAM incluye usuarios de IAM, grupos de usuarios de IAM y roles de IAM. Además, trabajaremos en la creación de una **política de IAM**, un objeto en AWS que, cuando se asocia a una identidad o un recurso, define sus permisos.



Este capítulo consta de los siguientes pasos.

- Creación de una **política de IAM** para anexarla al grupo de usuarios de IAM.
- Creación de un **grupo de usuarios de IAM** denominado dev-group.
- Creación de un **usuario de IAM** cuyo nombre sea dev-user colocado en dev-group.

Inicie sesión en la consola de IAM . Para generar una **URL de inicio de sesión** en la consola, haga clic en el botón **customize** (personalizar) como se muestra a continuación.

IAM dashboard

Security recommendations 1

Add MFA for root user
Enable multi-factor authentication (MFA) for the root user to improve security for this account.

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	2	16	4	0

AWS Account

Account ID
233219696677

Account Alias
233219696677 Create

Sign-in URL for IAM users in this account
<https://233219696677.signin.aws.amazon.com/console>

Ingrese el alias de cuenta. Para este laboratorio, escriba `aws-login-user_name` y haga clic en el botón **create alias** (crear alias).

Create alias for AWS account 233219696677 ✕

Preferred alias

aws-login-joozero aws-login-[name]

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL
`https://aws-login-joozero.signin.aws.amazon.com/console`

i IAM users will still be able to use the default URL containing the AWS account ID.

Click
Cancel
Save changes

Haga clic en **Políticas** (Políticas) en el lado izquierdo de la consola de IAM y, a continuación, haga clic en el botón **Create Policy** (Crear política) situado en la parte superior de la esquina derecha.

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Políticas** 1. Click
 - Identity providers
 - Account settings

Policies (834) Info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter < 1 2 3 4 5 6 7 ... 42 >

Policy Name	Type	Used as	Description
0d8fd6bfe6d74be58e0135dd7e51bb6e-policy	Customer managed	Permissions policy ...	Team Policy
ops-default-policy	Customer managed	Permissions policy ...	ops role default policy
team-default-policy	Customer managed	Permissions policy ...	team default policy

2. Click Create Policy

Al definir la política para los permisos de AWS, puede crear y editar en el editor visual o JSON. En esta práctica de laboratorio, utilizaremos el método **JSON**. Describa brevemente el permiso a continuación, esta política permite todas las acciones de **EC2 etiquetadas como Env-dev**. Además, **permite describir las acciones relacionadas** con todas las instancias de EC2. Sin embargo,

deniega la acción de crear y eliminar etiquetas para evitar que los usuarios las modifiquen arbitrariamente. Tenga en cuenta que el efecto Deny (Denegar) tiene prioridad sobre el efecto Allow (Permitir).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "dev"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    }
  ]
}
```

Haga clic en la pestaña JSON, pegue la política anterior y haga clic en el botón **Next: Tags** (Siguiente: Etiquetas).

Create policy

1 2 3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

1. Click

Import managed policy

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": "ec2:*",
7-       "Resource": "*",
8-       "Condition": {
9-         "StringEquals": {
10-          "ec2:ResourceTag/Env": "dev"
11-        }
12-      },
13-     },
14-     {
15-       "Effect": "Allow",
16-       "Action": "ec2:Describe*",
17-       "Resource": "*"
18-     },
19-     {
20-       "Effect": "Deny",
21-       "Action": [
22-         "ec2:DeleteTags",
23-         "ec2:CreateTags"
24-       ],
25-       "Resource": "*"
26-     }
27-   ]
28- }
```

2. Paste policy

Estructura de políticas JSON

- Version (Versión): utilice la última versión del 17/10/2012.
- Statement (Declaración): puede incluir más de una declaración en una política.
- Sid(optional) (Sid [opcional]): un ID de declaración opcional.
- Effect (Efecto): utilice **Allow** (Permitir) o **Deny** (Denegar) para indicar que la política permite o deniega el acceso. **Deny** (Denegar) tiene prioridad.
- Principal (Entidad principal): si crea una política basada en recursos, debe indicar la cuenta, el usuario, el rol o el usuario federado al que desea permitir o denegar el acceso. Si va a crear una política de permisos de IAM para anexarla a un usuario o rol, no puede incluir este elemento. La entidad principal está implícita como ese usuario o rol.
- Action (Acción): una lista de acciones que la política permite o deniega.
- Resource (Recurso): si crea una política de permisos de IAM, debe especificar una lista de recursos a los que se aplican las acciones. Si crea una política basada en recursos, este elemento es opcional. Si no incluye este elemento, el recurso al que se aplica la acción es el recurso al que se anexa la política.
- Condition Block(optional) (Bloque de condiciones [opcional]): especifique las circunstancias en las que la política concede permiso.

Mantenga la configuración predeterminada en el siguiente paso, haga clic en el botón **Next: Review** (Siguiente: Revisar). Escriba DevPolicy en la sección de nombres y escriba la descripción de esta política. A continuación, haga clic en el botón Create policy (Crear política).

Create policy

1 2 3

Review policy

Name* DevPolicy 1. DevPolicy
Use alphanumeric and '+=,@-.' characters. Maximum 128 characters.

Description IAM Policy for Dev Group 2. Input description
Maximum 1000 characters. Use alphanumeric and '+=,@-.' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Explicit deny (1 of 285 services)			
EC2	Full: Tagging	All resources	None
Allow (1 of 285 services) Show remaining 284			
EC2	Full: List, Read, Write, Permissions management	All resources	ec2:ResourceTag/Env = dev

Tags

Key	Value
No tags associated with the resource.	

* Required

3. Click

Cancel Previous Create policy

CLAVE

VALOR

Name (Nombre) DevPolicy

Descripción IAM Policy for Dev Group (Política de IAM para Dev Group)

Haga clic en **User groups** (Grupos de usuarios) en el lado izquierdo de la consola de IAM y, a continuación, haga clic en el botón **Create group** (Crear grupo) situado en la parte superior de la esquina derecha.

Identity and Access Management (IAM)

Dashboard

Access management

User groups 1. Click

Users

Roles

Policies

Identity providers

IAM > User groups

User groups (1) Info

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

Filter User groups by property or group name and press enter

Group name	Users	Permissions
AdminGroup	1	Defined

2. Click

Create group

Escriba dev-group en **User group name** (Nombre del grupo de usuarios) y seleccione DevPolicy en la sección **Attach permissions policies - Optional** (Anexar políticas de permisos - Opcional).

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

dev-group



1. dev-group

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

Add users to the group - *Optional* (1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

<input type="checkbox"/>	User name ↗	Groups	Last activity	Creation time
<input type="checkbox"/>	EEOverlord	0	None	24 hours ago

Attach permissions policies - *Optional* (Selected 1/672) [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.

<input type="checkbox"/>	Policy Name ↗	Type	Description
<input type="checkbox"/>	0d8fd6bfe6d... ↗	Customer managed	Team Policy
<input checked="" type="checkbox"/>	DevPolicy	Customer managed	IAM Policy for Dev Group

CLAVE

VALOR

User group name (Nombre del grupo de usuarios) dev-group

Haga clic en **Users** (Usuarios) en la parte izquierda de la página y, a continuación, haga clic en el botón **Add users** (Agregar usuarios).

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users** [↗](#) 1. Click
 - Roles
 - Policies
 - Identity providers
 - Account settings

IAM > Users

Users (1) [Info](#)

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

[↻](#) [Delete](#) [Add users](#) 2. Click

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age
<input type="checkbox"/>	EEOverlord	None	Never	None	None

Escriba dev-user en **User name** (Nombre de usuario) y permita tanto el acceso mediante programación como el acceso a la consola de administración de AWS. Y, a continuación, seleccione **Custom password** (Contraseña personalizada) y escriba la contraseña que desee. Por último, desmarque

Require password reset function (Requerir función de restablecimiento de contraseña) para una acción rápida. En el mundo real, se recomienda activar el restablecimiento de la contraseña. Haga clic en el botón **Next: Permissions** (Siguiente: Permisos).

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* 1. dev-user
[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☒ **Programmatic access** 2. Click
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **AWS Management Console access** 3. Click
Enables a **password** that allows users to sign in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ **Custom password** 4. Custom password
..... 5. Input password
☐ Show password

Require password reset ☐ **User must create a new password at next sign-in** 6. Uncheck
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

Seleccione el dev-group que creamos justo antes y haga clic en el botón **Next: Tags** (Siguiente: Etiquetas). Omita la página Add user (Agregar usuario) y vaya al siguiente paso.

Add user

1 2 3 4 5

Set permissions

☒ **Add user to group** ☐ Copy permissions from existing user ☐ Attach existing policies directly

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](#)

Add user to group

Create group Refresh

Q Search Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> dev-group Select	DevPolicy

Set permissions boundary

Haga clic en el botón **Create user** (Crear usuario) para agregar dev-user.

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

dev-user

AWS access type

Programmatic access and AWS Management Console access

Console password type

Custom

Require password reset

No

Permissions boundary

Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	dev-group

Tags

No tags were added.

Descargue el archivo .csv para obtener el ID de clave de acceso y la clave de acceso secreta. Además, puede enviar instrucciones para el inicio de sesión.

Haga clic en **Sign-in URL** (URL de inicio de sesión) para iniciar sesión como dev-user.

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://aws-login-joozero.signin.aws.amazon.com/console> 

Download .csv

	User	Access key ID	Secret access key	Email login instructions
▼	dev-user		***** Show	Send email 

Created user dev-user

Added user dev-user to group dev-group

Created access key for user dev-user

Created login profile for user dev-user

Escriba el **IAM user name** (Nombre de usuario de IAM) y la **Password** (Contraseña) para ingresar e iniciar sesión para entrar en la consola de administración de AWS.



Sign in as IAM user

Account ID (12 digits) or account alias

aws-login-joozero

IAM user name

dev-user

dev-user

Password

.....

Type password

Sign in

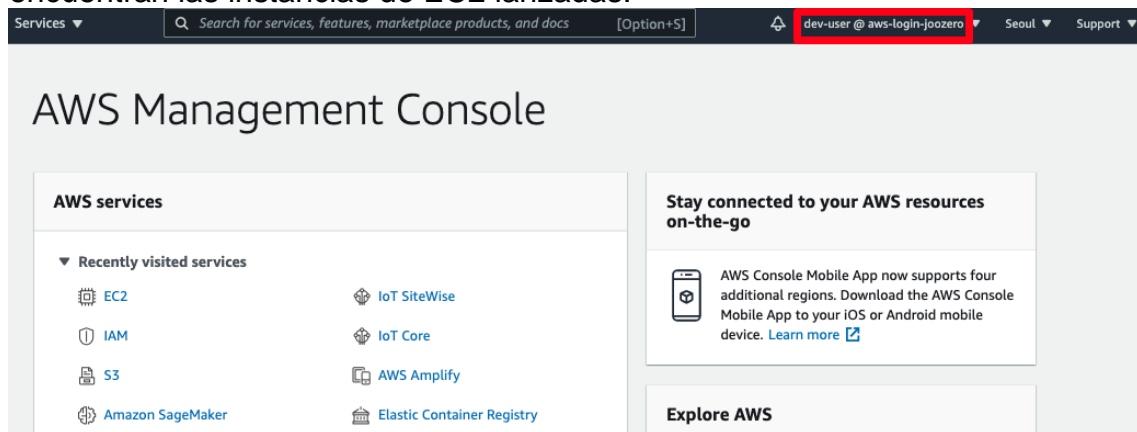
[Sign in using root user email](#)

[Forgot password?](#)

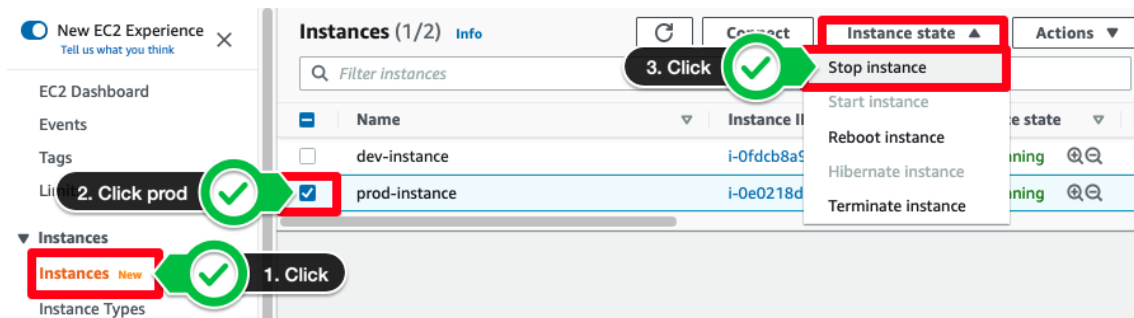


Probar el acceso a los recursos

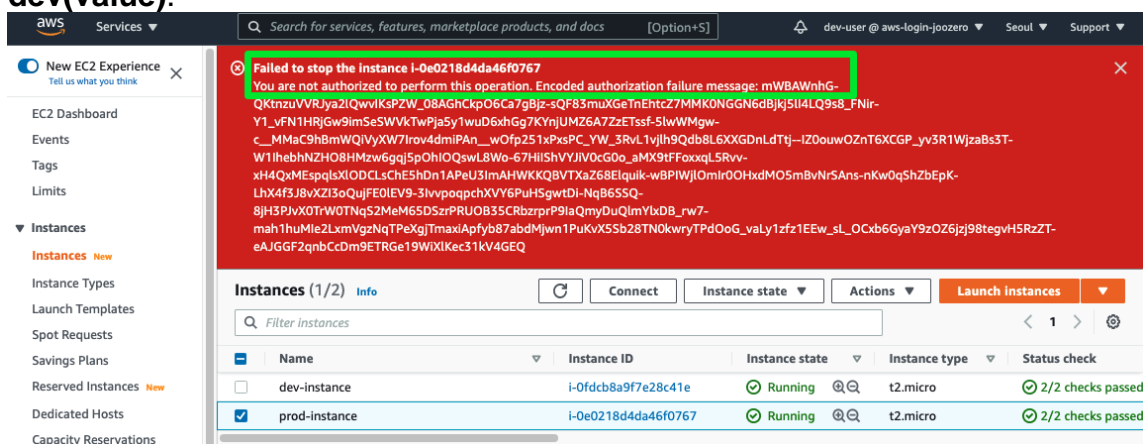
Inicie sesión en la consola de AWS y compruebe el alias de cuenta y el **usuario de IAM**. Además, compruebe la **región de AWS** en la que se encuentran las instancias de EC2 lanzadas.



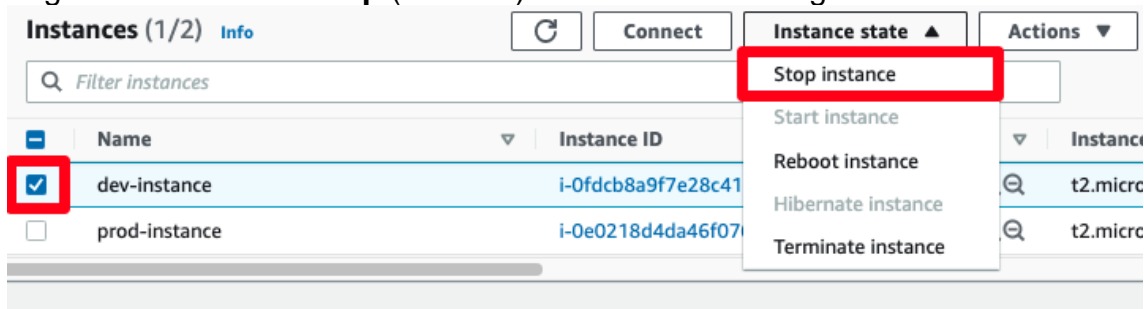
Vaya a la **consola de EC2** y haga clic en el menú **Instances** (Instancias). Seleccione la instancia llamada prod-instance y haga clic en el botón **Instance state** (Estado de instancia) y en el botón **Stop instance** (Detener instancia). Y haga clic en el botón **Stop** (Detener) en la ventana emergente.



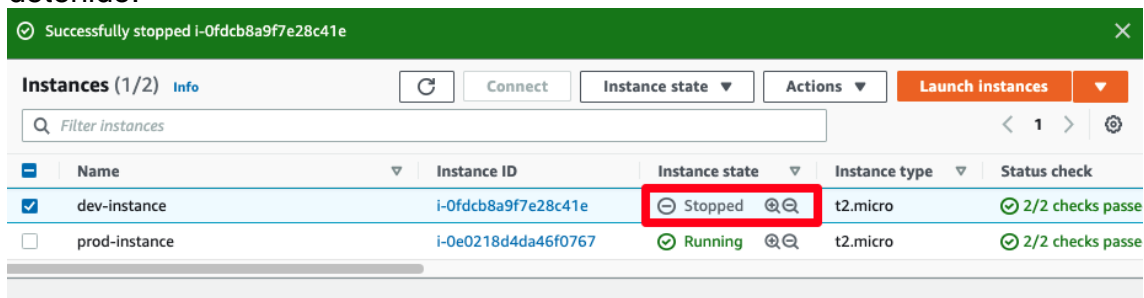
Aparece una señal de advertencia de que el dev-user no tiene permisos para realizar la operación de detención de la instancia de EC2. Esto se debe a que el laboratorio práctico anterior solo permitía al **dev-user** realizar la acción de detención en las instancias de EC2 con la etiqueta de recurso **Env (key)-dev(value)**.



Seleccione la instancia llamada dev-instance y haga clic en el botón **Instance State** (Estado de instancia) y en el botón **Stop instance** (Detener instancia). Y haga clic en el botón **Stop** (Detener) en la ventana emergente.



Después de unos segundos, puede ver que la instancia dev-instance se ha detenido.

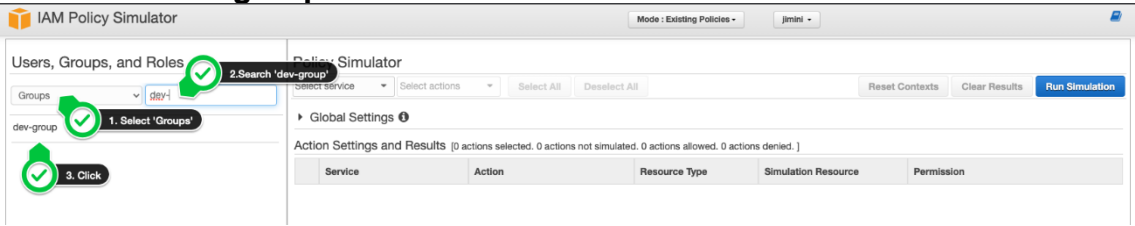


En el mundo real, es posible que no quiera cerrar la instancia de EC2 para probar la política de IAM personalizada. El simulador de políticas es una herramienta que le permite examinar y validar los permisos que establecen sus políticas. En este paso, probaremos el permiso de **dev-group** simulando las acciones **DeleteTags** y **StopInstances** mediante el simulador de política de IAM. Saltarse este paso no afecta a sus próximas prácticas de laboratorio.

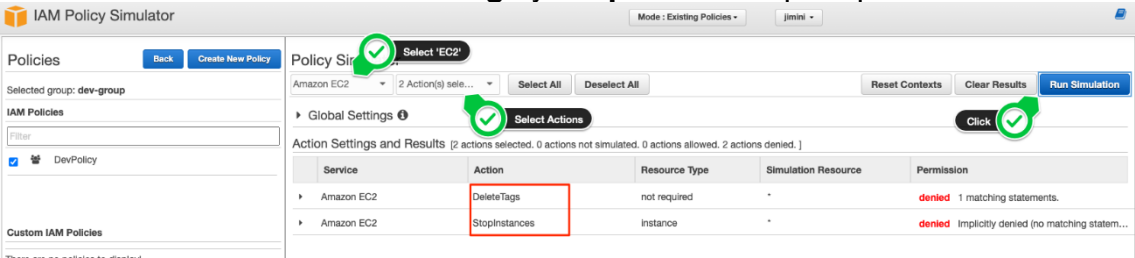
El **dev-user** que estaba utilizando no tiene acceso al **IAM Policy Simulator** (Simulador de política de IAM). Inicie sesión como **Administrador**.

Vaya al IAM Policy simulator (Simulador de política de IAM).

Seleccione **dev-group**.



Seleccione las acciones **DeleteTags** y **StopInstances** para probarlas.



Puede ver que ambas acciones están denegadas, pero por diferentes motivos. Se denegó **DeleteTags** debido a **** matching statement**** (1 instrucción coincidente) y **StopInstances** se denegó con el mensaje **Implicitly denied (no matching statements)** (Denegado implícitamente [sin instrucciones coincidentes]).

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	DeleteTags	not required	*	denied 1 matching statements.
Amazon EC2	StopInstances	instance	*	denied Implicitly denied (no matching statem...

Expanda **DeleteTags** y haga clic en **Show statement** (Mostrar instrucción) en **DevPolicy (IAM Policy)** (DevPolicy [Política de IAM]). Resalta automáticamente qué instrucción coincide de forma exacta con la acción simulada.

IAM Policy Simulator

Mode: Existing Policies | jmini

Policies | [Back](#)

Editing policy: DevPolicy

Customer Managed Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/env": "dev"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "ec2:DeleteTags",
      "Resource": "*"
    }
  ]
}
```

Policy Simulator

Amazon EC2 | 2 Action(s) sele... | [Select All](#) | [Deselect All](#) | [Reset Contexts](#) | [Clear Results](#) | [Run Simulation](#)

Global Settings ⓘ

Action Settings and Results [2 actions selected. 0 actions not simulated. 0 actions allowed. 2 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	DeleteTags	not required	*	denied 1 matching statements.
Show statement in DevPolicy (IAM Policy)				
Resource You can specify the resource and context keys used to simulate this action. By default the simulation resource is '*'.				
Add Resource				
Amazon EC2	StopInstances	instance	*	denied Implicitly denied (no matching statem...
Resource You can specify the resource and context keys used to simulate this action. By default the simulation resource is '*'.				
Instance				
ec2:resourcetag/env Leave blank to ignore key.				

Expanda StopInstances. Se denegó la acción *porque el recurso de simulación es "*"*. Tenga en cuenta que **dev-group** solo puede detener las instancias de EC2 que tengan las etiquetas **dev**.

Resource You can specify the resource and context keys used to simulate this action. By default the simulation resource is '*'.

Instance *

ec2:resourcetag/env [Leave blank to ignore key.](#)

Ahora probaremos la política después de agregar la etiqueta **dev** para validar la política de forma correcta.

Policy Simulator

Amazon EC2 | 2 Action(s) sele... | [Select All](#) | [Deselect All](#) | [Reset Contexts](#) | [Clear Results](#) | [Run Simulation](#)

Global Settings ⓘ

2. Run simulation ✓

Action Settings and Results [2 actions selected. 0 actions not simulated. 1 actions allowed. 1 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	DeleteTags	not required	*	denied 1 matching statements.
Amazon EC2	StopInstances	instance	*	allowed 1 matching statements.

[Show statement in DevPolicy \(IAM Policy\)](#)

Resource You can specify the resource and context keys used to simulate this action. By default the simulation resource is '*'.

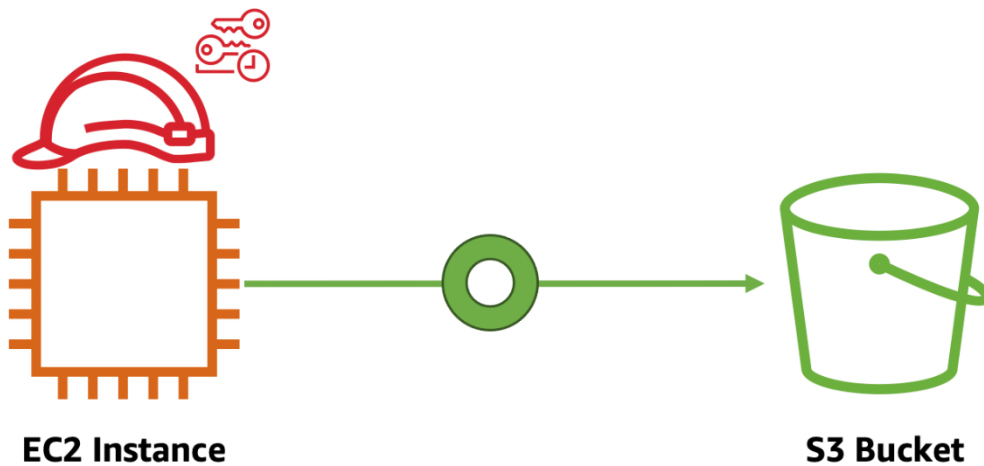
Instance *

ec2:resourcetag/env **dev** 1. Add 'dev' tag ✓

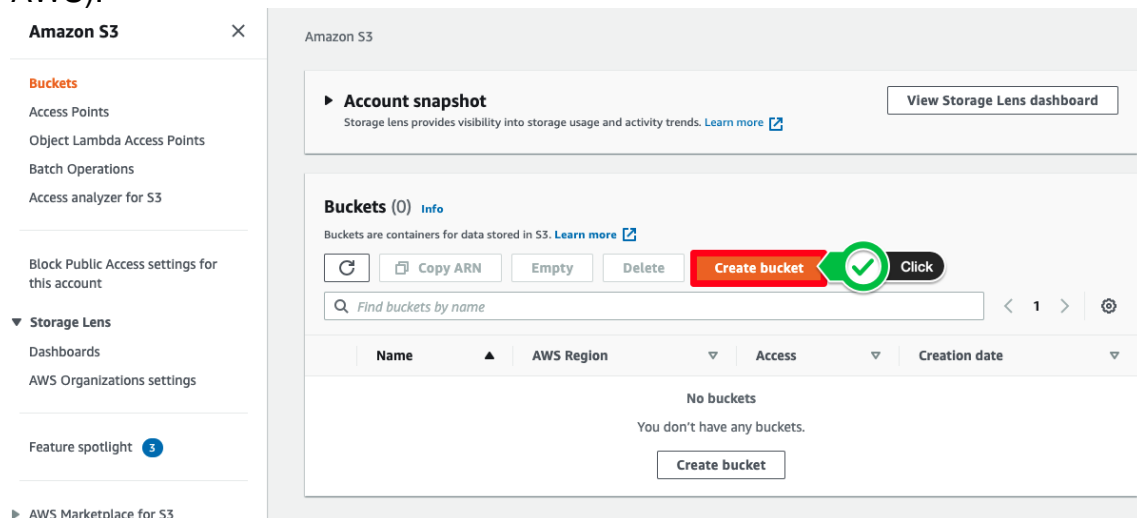
3. Allowed ✓

Asigne el rol de IAM para la instancia EC2 y pruebe el acceso

Vuelva a iniciar sesión en la **cuenta de AWS con el rol de administrador** al principio del laboratorio práctico, no como dev-user antes de continuar con este capítulo.



Para crear un bucket de S3, ingrese a la **consola de S3** . Luego, haga clic en el botón **Create bucket** (Crear bucket). Para obtener información detallada sobre Amazon S3, consulte el capítulo Storage on AWS (Almacenamiento en AWS).



Ingresa un nombre único en el campo **Bucket name** (Nombre del bucket). En este laboratorio, escriba iam-test-user_name. Todos los nombres de bucket de Amazon S3 tienen que ser únicos y no se pueden repetir. Haga clic en el botón

Create bucket (Crear bucket) y no modifique la configuración restante.

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

iam-test-joozero

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Seoul) ap-northeast-2

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

☒ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cargue cualquier archivo en el bucket de S3.

Amazon S3 > iam-test-joozero > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 33.9 KB) Remove Add files Add folder

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name ▲	Folder ▼	Type ▼	Size ▼
<input type="checkbox"/>	aws-logo-sample.jpg	-	image/jpeg	33.9 KB

Destination

Destination
[s3://iam-test-joozero](#)

► **Destination details**
Bucket settings that impact new objects stored in the specified destination.

► **Permissions**
Grant public access and access to other AWS accounts.

► **Properties**
Specify storage class, encryption settings, tags, and more.

Cancel Upload

Cree otro bucket más llamado iam-test-other-user_name. Cargue cualquier archivo en el bucket de S3.

Diríjase a la **consola de IAM**

para crear el rol de IAM para la instancia de EC2. Haga clic en **Roles** (Roles) en el lado izquierdo de la consola de IAM y haga clic en el botón **Create role** (Crear rol). En el paso 1, elija **EC2** para la entidad de confianza y haga clic en **Next: Permissions** (Siguiente: Permisos). El rol de IAM se puede aplicar a muchos servicios de AWS, incluidos EC2 y Lambda, así como a otras cuentas de AWS, identidades web y federación SAML 2.0.

Create role


1


2


3


4

Select type of trusted entity

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

**SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

 Click

Lambda
Allows Lambda functions to call AWS services on your behalf.

En el paso 2, haga clic en **Create policy** (Crear política) para crear una política que se asocie al rol de la instancia de EC2. En la pestaña **JSON**, pegue la política que aparece a continuación y haga clic en **Next: Tags** (Siguiente: Etiquetas).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": [
        "arn:aws:s3:::iam-test-user_name/*",
        "arn:aws:s3:::iam-test-user_name"
      ]
    }
  ]
}
```

Create policy

1 2 3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
6-       "Effect": "Allow",
7-       "Resource": ["arn:aws:s3:*"]
8-     },
9-     {
10-      "Effect": "Allow",
11-      "Action": [
12-        "s3:Get*",
13-        "s3:List*"
14-      ],
15-      "Resource": [
16-        "arn:aws:s3::iam-test-joozero/*",
17-        "arn:aws:s3::iam-test-joozero"
18-      ]
19-    }
20-   ]
21- }
22-
```

En el archivo JSON anterior, asegúrese de cambiar el valor de **Resource** (Recurso) por **el nombre del bucket de S3 que creó**.

Para omitir la operación de agregar etiquetas, haga clic en **** Next: Review**** (Siguiendo: Revisar) y escriba **IAMBucketTestPolicy** en el cuadro de entrada **Name** (Nombre). Haga clic en **Create policy** (Crear política) para asociarla al rol de IAM.

Create policy

Review policy

Name*

IAMBucketTestPolicy

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

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Vuelva a la página en la que estaba creando el rol de IAM, pulse el botón **Actualizar** en la esquina derecha y escriba **IAMBucketTestPolicy**. Si ve la política que acaba de crear en la lista a continuación, selecciónela y diríjase al siguiente paso.

Create role

1

2

▼ Attach permissions policies

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

Create policy

Filter policies ▼ Type policy name

Policy name ▼	Used as
<input checked="" type="checkbox"/> IAMBucketTestPolicy	None

Click

En el paso 4, escriba IAMBucketTestRole y cree el rol.

Create role

1

2

3

4

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies [IAMBucketTestPolicy](#)

Permissions boundary Permissions boundary is not set

No tags were added.

Diríjase a la consola de EC2

para asociar el rol de IAM en la instancia de EC2. En este momento, si no tiene instancias de EC2 creadas en el laboratorio anterior, verifique la parte superior derecha para ver si la región de AWS está configurada correctamente.

Seleccione prod-instance y, luego, haga clic en el botón **Connect** (Conectar).

New EC2 Experience

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Connect

Name	Instance ID	Instance state
<input type="checkbox"/> dev-instance	i-0d908f5eb3f3dc42e	Running
<input checked="" type="checkbox"/> prod-instance	i-08149a613a6ed1070	Running

Conéctese a la instancia mediante la opción EC2 Instance Connect (Conexión de la instancia de EC2) y haga clic en el botón **Connect** (Conectar). Luego, el terminal saldrá como se muestra a continuación. Escriba `aws s3 ls` y verá que

```

      #
    _\#####_
--  \#####\
--   \###|
--   \#/
--   v-'-'>
--
--  .
--  /
-- /m/'

```

Amazon Linux 2023

<https://aws.amazon.com/linux/amazon-linux-2023>

Last login: Fri May 26 06:02:30 2023 from 13.209.1.59

[ec2-user@ip-172-31-8-179 ~]\$ aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied

[ec2-user@ip-172-31-8-179 ~]\$

Modify IAM role (Modificar rol de IAM).

EC2 > Instances > i-0e0218d4da46f0767 > Modify IAM role

Modify IAM role

Info

Attach an IAM role to your instance.

Instance ID

i-0e0218d4da46f0767 (prod-instance)

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

Q |

No IAM Role

Choose this option to detach an IAM role

IAMBucketTestRole

arn:aws:iam::[REDACTED]:instance-profile/IAMBucketTestRole

TeamRoleInstanceProfile

arn:aws:iam::[REDACTED]:instance-profile/TeamRoleInstanceProfile

Create new IAM role

Are you sure you want to detach the IAM role from this instance? The instance will be removed. Are you

Cancel

Save

Conéctese nuevamente a la instancia de EC2 y vuelva a escribir `aws s3 ls`. Ahora podrá ver las listas de buckets de S3. Además, podrá ver la lista de

objetos ubicada en iam-test-user_name, pero no en iam-test-other-user_name, porque no tiene una política de IAM para este bucket.

```
[ec2-user@ip-172-31-4-64 ~]$ aws s3 ls
2021-07-31 15:30:58 iam-test-joozero
2021-07-31 16:20:04 iam-test-other-joozero
[ec2-user@ip-172-31-4-64 ~]$ aws s3 ls iam-test-joozero
2021-07-31 17:19:30      34664 aws-logo-sample.jpg
[ec2-user@ip-172-31-4-64 ~]$ aws s3 ls iam-test-other-joozero

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
[ec2-user@ip-172-31-4-64 ~]$
```

aws s3 ls

aws s3 ls iam-test-user_name

aws s3 ls iam-test-other-user_name