



## 279-[SF]-Lab - Introducción a IAM

### Datos Generales:

**Nombre:** Tomás Alfredo Villaseca Constantinescu

**País:** Chile

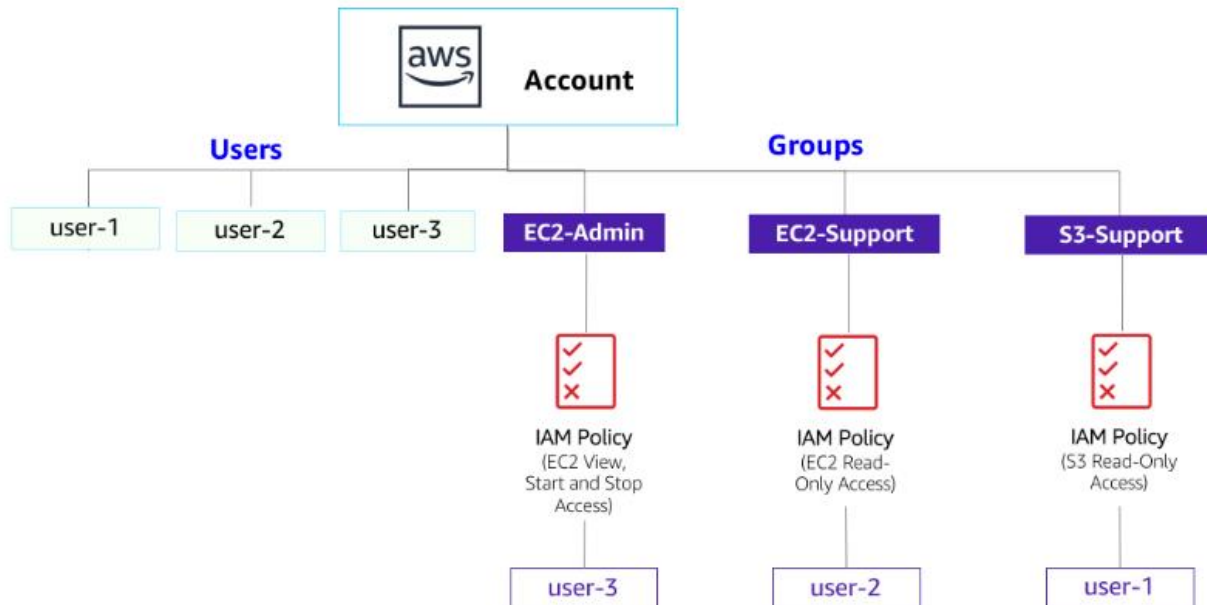
**Fecha:** 23/09/2023

**Contacto:** [tomas.villaseca.c@gmail.com](mailto:tomas.villaseca.c@gmail.com)

Después de completar este laboratorio, podrá realizar lo siguiente:

- Crear y aplicar una política de contraseñas de IAM
- Analizar usuarios y grupos de usuarios de IAM creados previamente
- Inspeccionar políticas de IAM según se apliquen a los grupos de usuarios creados previamente
- Agregar usuarios a grupos de usuario con capacidades específicas activas
- Ubicar y usar la URL de inicio de sesión de la IAM
- Probar los efectos de las políticas en el acceso a los servicios

## Diagrama del entorno del laboratorio:



**AWS IAM** = Servicio que le permite administrar el acceso a los servicios y recursos de AWS de forma segura.



AWS IAM

- Flexibilidad para configurar el acceso en función de las necesidades operativas y de seguridad específicas de su empresa.

**Usuario IAM** = Entidad que se crea en AWS y que representa a la persona o aplicación que interactúa con los servicios y recursos de AWS.

- Por defecto (Cuando creas un nuevo Usuario IAM) ☐ Sin permisos
- Se deben conceder permisos para que el Usuario IAM pueda realizar acciones específicas en AWS.

**Grupo IAM** = Colección de usuarios IAM.

- Cuando se asigna una política IAM a un grupo, todos los usuarios del grupo reciben los permisos especificados por la política.

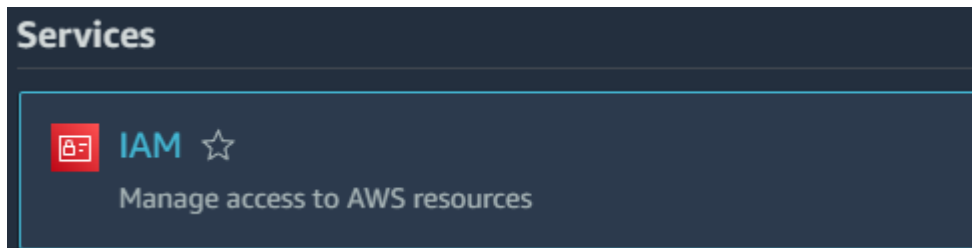
**Políticas de IAM** = Documento que permite o denega permisos a los servicios y recursos de AWS.

- Permite personalizar el nivel de acceso de los usuarios a los recursos.
- Principio de mínimo privilegio = a un usuario se le concede acceso solo a lo que necesita.
- Documento de políticas IAM → Formato tipo JSON

# Tarea 1: Crear una política de contraseña de cuenta

En esta tarea, se crea una política de contraseñas personalizada para la cuenta de AWS. Esta política afecta a todos los usuarios asociados a la cuenta.

**Paso 1:** Amazon Management Console → Search → IAM



**Paso 2:** IAM → Panel de navegación → Account Settings

- Se puede visualizar la política de contraseña predeterminada actualmente en efecto.

Account settings [Info](#)

**Password policy** [Info](#)  
Configure the password requirements for the IAM users.

This AWS account uses the following default password policy:

Password minimum length  
8 characters

Password strength  
Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

**Paso 3:** Change Password Policy (Edit) → Configurar → Save Changes

- Enforce minimum password length → 10 characters
- Seleccionar todas las casillas excepto "Password expiration requires administrator reset".
- Enable password expiration → 90 days
- Prevent password reuse → 5 passwords

# Edit password policy [Info](#)

## Password policy

☐ IAM default  
Apply default password requirements.

☒ Custom  
Apply customized password requirements.

### Password minimum length.

Enforce a minimum length of characters.

characters

Needs to be between 6 and 128.

### Password strength

- ☒ Require at least one uppercase letter from the Latin alphabet (A-Z)
- ☒ Require at least one lowercase letter from the Latin alphabet (a-z)
- ☒ Require at least one number
- ☒ Require at least one non-alphanumeric character (! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } | ' )

### Other requirements

- ☒ Turn on password expiration

Expire password in  day(s)

Needs to be between 1 and 1095 days.

- ☐ Password expiration requires administrator reset

- ☒ Allow users to change their own password
- ☒ Prevent password reuse

Remember  password(s)

Needs to be between 1 and 24.

Estos cambios en la política de contraseñas tiene efecto a nivel de cuenta de AWS y se aplica a todos los usuarios de la cuenta.

Se reforzaron los requisitos de contraseña creando una política de contraseñas personalizada. Las distintas opciones de contraseña que se seleccionaron han hecho que las contraseñas que crean los usuarios sean mucho más difíciles de descifrar.

## Tarea 2: Analizar los usuarios y los grupos de usuarios

En esta tarea, explorará los usuarios y grupos de usuarios que ya han sido creados para usted en IAM.

### Paso 1: IAM → Panel de navegación → Users

**Users (3)** [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	▼	Groups	▼
<input type="checkbox"/>	<a href="#">user-1</a>		/spl66/		0	
<input type="checkbox"/>	<a href="#">user-2</a>		/spl66/		0	
<input type="checkbox"/>	<a href="#">user-3</a>		/spl66/		0	

### Paso 2: Users → user-1 → Summary → Permissions

- Se puede ver que user-1 no tiene permisos.

**user-1** [Info](#)

**Summary**



ARN  <code>arn:aws:iam::970885214660:user/spl66/user-1</code>	Console access  <b>Enabled without MFA</b>	Access key 1 <a href="#">Create access key</a>
Created September 23, 2023, 20:24 (UTC-03:00)	Last console sign-in  <b>Never</b>	

[Permissions](#) | [Groups](#) | [Tags \(2\)](#) | [Security credentials](#) | [Access Advisor](#)

**Permissions policies (0)**

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

Filter by Type All types ▼

<input type="checkbox"/>	Policy name 	▲	Type	▼	Attached via 
No resources to display					

Paso 3: Users → user-1 → Summary → Groups

- Se puede ver que user-1 no es miembro de ningún grupo.

Permissions

Groups

Tags (2)

Security credentials

Access Advisor

User groups membership (0)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name

Attached policies

This user does not belong to any groups.

Paso 4: Users → user-1 → Summary → Security credentials

- Se puede ver que user-1 tiene asignada una contraseña de consola.

Permissions

Groups

Tags (2)

Security credentials

Access Advisor

Console sign-in

Console sign-in link

https://970885214660.signin.aws.amazon.com/console

Console password

Updated 6 minutes ago (2023-09-23 20:25 GMT-3)

Last console sign-in

Never

Paso 5: IAM → Panel de navegación → User groups

User groups (3) Info

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

Search

Group name

Users

Permissions

EC2-Admin

0

Defined

EC2-Support

0

Defined

S3-Support

0

Defined

**Paso 6:** User groups → EC2-Support → Summary → Permissions

- Tiene la política **AmazonEC2ReadOnlyAccess** adjuntada.

### EC2-Support Info

#### Summary

User group name EC2-Support	Creation time September 23, 2023, 20:24 (UTC-03:00)	ARN arn:aws:iam::97086
--------------------------------	--	---------------------------

Users

Permissions

Access Advisor

#### Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type  
All types

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	<a href="#">AmazonEC2ReadOnlyAccess</a>	AWS managed	1

**Paso 7:** Desplegar la política **AmazonEC2ReadOnlyAccess** → Marcar la X para desplegar

Estructura de un documento de políticas de IAM (formato JSON):

- Effect = indica si permitir o denegar permisos
- Action = especifica el API Call que se puede realizar en un servicio de AWS.
- Resource = define el alcance de las entidades cubiertas por la regla de la política.

☒

Policy name

▲

Type

☒

[AmazonEC2ReadOnlyAccess](#)

AWS managed

#### AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Console.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:Describe*",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "elasticloadbalancing:Describe*",
12      "Resource": "*"
13    },
14    {
15      "Effect": "Allow",
16      "Action": [
17        "cloudwatch:ListMetrics",
18        "cloudwatch:GetMetricStatistics",
19        "cloudwatch:Describe*"
20      ]
21    }
22  ]
23 }
```

**Paso 8:** User groups → S3-Support → Summary → Permissions

- Tiene la política **AmazonS3ReadOnlyAccess** adjuntada.

S3-Support

Summary

User group name

S3-Support

Creation time

September 23, 2023, 20:24 (UTC-03:00)

ARN

arn:aws:iam::9708

Users

Permissions

Access Advisor


Permissions policies (1)

You can attach up to 10 managed policies.

Search

Filter by Type

All types

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	 <a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	1

**Paso 9:** Desplegar la política **AmazonS3ReadOnlyAccess** → Marcar la X para desplegar


- La política tiene permisos para GET, LIST y DESCRIBE recursos en S3.

☒

Policy name

Type

☒

 [AmazonS3ReadOnlyAccess](#)

AWS managed

AmazonS3ReadOnlyAccess

Provides read only access to all buckets via the AWS Management Console.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*",
9         "s3:Describe*",
10        "s3-object-lambda:Get*",
11        "s3-object-lambda:List*"
12      ],
13       "Resource": "*"
14     }
15   ]
16 }
```



**Paso 10:** User groups → EC2-Admin → Summary → Permissions

- Tiene la política **EC2-Admin-Policy** adjuntada.

## EC2-Admin [Info](#)

### Summary

User group name EC2-Admin	Creation time September 23, 2023, 20:24 (UTC-03:00)	ARN arn:aws:iam::9708
------------------------------	--	--------------------------

Users

**Permissions**

Access Advisor

### Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

Filter by Type  
All types

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Attached entities
<input type="checkbox"/>	<a href="#">EC2-Admin-Policy</a>	Customer inline	0

**Paso 11:** Desplegar la política **EC2-Admin-Policy** → Marcar la X para desplegar

- La política tiene permisos para ver (describir) información sobre EC2s y también la capacidad para iniciar y detener instancias.

☒

Policy name [↗](#)

▲

Type

☒

[EC2-Admin-Policy](#)

Customer inline

### EC2-Admin-Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "ec2:Describe*",
7         "ec2:StartInstances",
8         "ec2:StopInstances"
9       ],
10      "Resource": [
11        "*"
12      ],
13      "Effect": "Allow"
14    }
15  ]
16 }
```

## Tarea 3: Agregar usuarios a los grupos de usuarios

En esta tarea se visualizaron los usuarios y grupos pre-creados. También se pudo visualizar las políticas IAM adjuntadas a los grupos y los permisos que estas entregan.

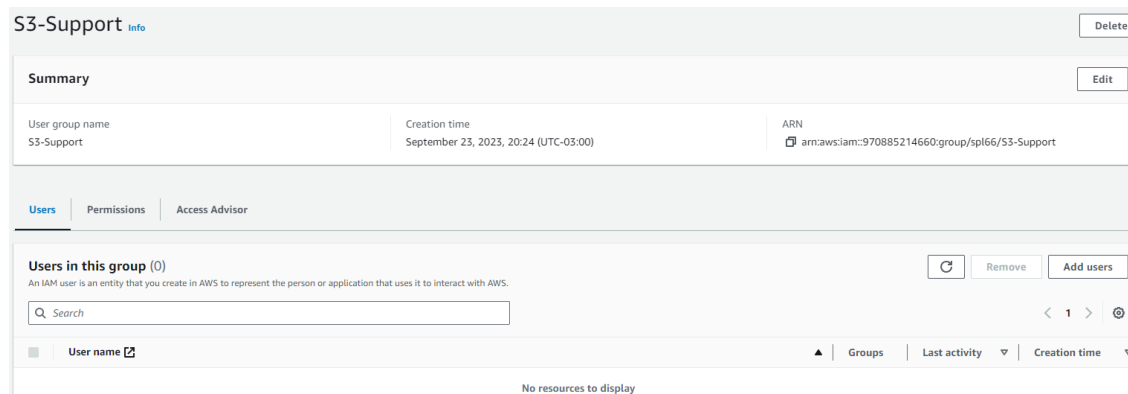
### Escenario Empresarial:

Agregar a todos los usuarios asociados al grupo respectivo.

User	In Group	Permissions
user-1	S3-Support	Read-only access to Amazon S3
user-2	EC2-Support	Read-only access to Amazon EC2
user-3	EC2-Admin	View, start, and stop EC2 instances

### Tarea 3.1 – Agregar al user-1 al grupo S3-Support

**Paso 1:** IAM → Panel de navegación → User Groups → S3-Support



S3-Support [Info](#) [Delete](#)

**Summary** [Edit](#)

User group name S3-Support	Creation time September 23, 2023, 20:24 (UTC-03:00)	ARN <a href="#">arn:aws:iam::970885214660:group/spl66/S3-Support</a>
-------------------------------	--	---

[Users](#) | [Permissions](#) | [Access Advisor](#)

**Users in this group (0)** [Refresh](#) [Remove](#) [Add users](#)

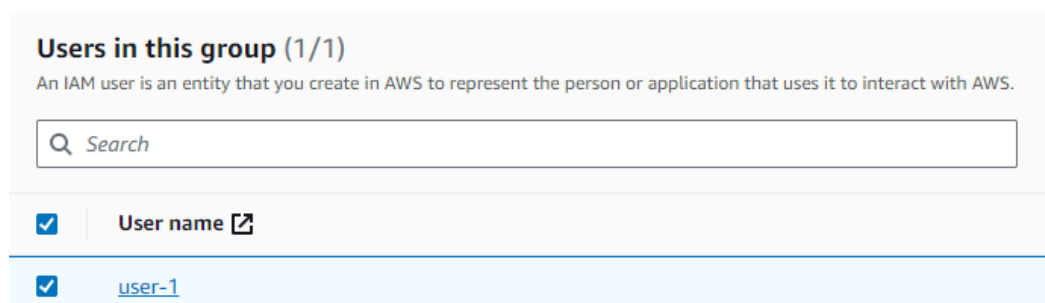
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☐ [User name](#) [Groups](#) [Last activity](#) [Creation time](#)

No resources to display

**Paso 2:** Users → Add users

- Seleccionar la casilla para “user-1”



**Users in this group (1/1)**

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

☒ [User name](#) [Groups](#) [Last activity](#) [Creation time](#)

<input checked="" type="checkbox"/> <a href="#">user-1</a>
--

# Tarea 3.2 – Agregar al user-2 al grupo EC2-Support

Paso 1: IAM → Panel de navegación → User Groups → EC2-Support

EC2-Support

Info

Delete

Summary

Edit

User group name

EC2-Support

Creation time

September 23, 2023, 20:24 (UTC-03:00)

ARN

arn:aws:iam::970885214660:group/spl66/EC2-Support

Users

Permissions

Access Advisor

Users in this group (0)

Remove

Add users

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

Search

< 1 >

⚙

User name

Groups

Last activity

Creation time

No resources to display

Paso 2: Users → Add users

- Seleccionar la casilla para “user-2”

Users in this group (1/1)

Remove

Add users

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

Search

< 1 >

⚙

✓

User name

✓

user-2

### Tarea 3.3 – Agregar al user-3 al grupo EC2-Admin

Paso 1: IAM → Panel de navegación → User Groups → EC2-Admin

EC2-Admin [Info](#) Delete

Summary Edit

User group name

EC2-Admin

Creation time

September 23, 2023, 20:24 (UTC-03:00)

ARN

arn:aws:iam::970885214660:group/spl66/EC2-Admin

Users

Permissions

Access Advisor

Users in this group (0)

Refresh Remove Add users

Q Search

< 1 >

☐ User name

Groups | Last activity | Creation time

No resources to display

Paso 2: Users → Add users

- Seleccionar la casilla para “user-3”

Users in this group (1/1)

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

Q Search

☒ User name

☒ [user-3](#)

Se verifica que todos los grupos quedaron con 1 usuario:



<input type="checkbox"/>	Group name		Users		Permissions
<input type="checkbox"/>	<a href="#">EC2-Admin</a>		1	..	Defined
<input type="checkbox"/>	<a href="#">EC2-Support</a>		1	..	Defined
<input type="checkbox"/>	<a href="#">S3-Support</a>		1	..	Defined

## Tarea 4: Iniciar sesión y probar permisos de usuarios

En esta tarea, se prueban los permisos de cada usuario IAM.

### Paso 1: IAM → Panel de navegación → Dashboard

- Sección AWS Account → Sign-in URL for IAM users in this account (Link)
- Se puede utilizar el link para iniciar sesión.
- Link → <https://970885214660.signin.aws.amazon.com/console>

IAM Dashboard	AWS Account
	<p>Account ID</p> <p> 970885214660</p> <p>Account Alias</p> <p><a href="#">Create</a></p> <p>Sign-in URL for IAM users in this account</p> <p> <a href="https://970885214660.signin.aws.amazon.com/console">https://970885214660.signin.aws.amazon.com/console</a></p>

### Paso 2: Abrir una ventana incognito en un navegador.

- Pegar el **Link** en la ventana incognito del navegador.
- Iniciar sesión con user-1
- IAM username = user-1
- Password = Lab-password1

#### Iniciar sesión como usuario de IAM

ID de cuenta (12 dígitos) o alias de cuenta

Nombre de usuario:

Contraseña:

☐ Recordar esta cuenta

Iniciar sesión

### Paso 3: AWS Management Console → Services → S3

- Seleccionar uno de los S3 y revisar contenido.
- Permisos de S3-Support permiten ver el contenido de los S3.

**Buckets (1)** [Información](#)  
Los buckets son contenedores de datos almacenados en S3. [Más información](#)

	Nombre	Región de AWS
	c89400a1935447l4819972t1w970885214660-s3bucket-1fck08dz9v5pj	EE. UU. Oeste (Oregón) us-west-2

Objetos

Propiedades

Permisos

Métricas

Administración

Puntos de acceso

**Objetos (0)**  
Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan una lista de forma explícita, [Más información](#)

Copiar URI de S3 Copiar URL Descargar Abrir Eliminar Acciones Crear carpeta Cargar

	Nombre	Tipo	Última modificación	Tamaño
No hay objetos				

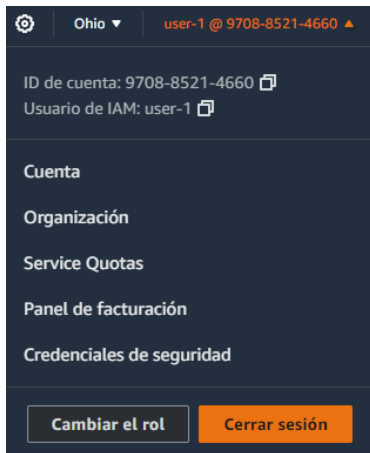
### Paso 4: AWS Management Console → Services → EC2 → Instances

- No se pueden visualizar las instancias EC2.
- Permisos de S3-Support no permiten visualizar las instancias EC2.

**Instancias** [Información](#)

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zo
You are not authorized to perform this operation.							

## Paso 5: Cerrar sesión de cuenta user-1



## Paso 6: Abrir una ventana incognito en un navegador.

- Pegar el **Link** en la ventana incognito del navegador.
- Iniciar sesión con user-2
- IAM username = user-2
- Password = Lab-password2

ID de cuenta (12 dígitos) o alias de cuenta

Nombre de usuario:

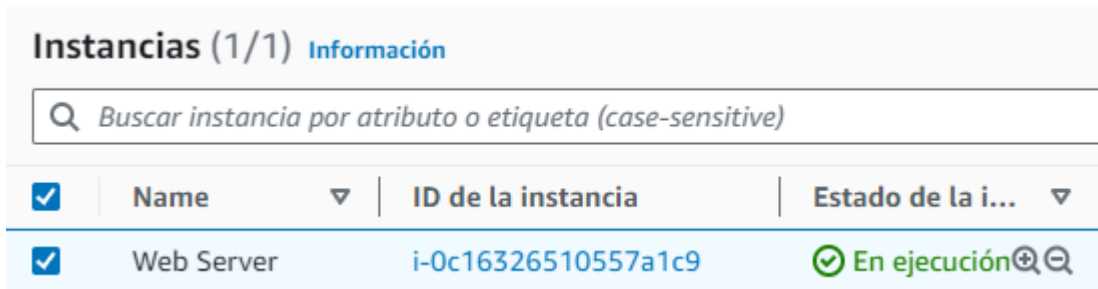
Contraseña:

☐ Recordar esta cuenta

Iniciar sesión


## Paso 7: AWS Management Console → Services → EC2 → Instances

- Puede visualizar las instancias EC2.
- Permisos de EC2-Support permiten visualizar las instancias EC2.






**Paso 8:** EC2 → Instances → Seleccionar una instancia → Instance State → Stop Instance

- Usuario no tiene permisos para detener instancias.
- Permisos de EC2-Support no permiten detener instancias.


 **No se pudo detener la instancia i-0c16326510557a1c9**  
You are not authorized to perform this operation. Encoded authorization failure message: b2UQBsQs4\_CXP9dw73YC8IH\_UGw6vG4DLWUpp0V8qBTc-Jv10mYzWNcMMEBCWjANq6a6MINZrtq165SrtIYk6SFCIMQ4a9axNVB1CwZybEqiUOCj8tiIGf-ARIlv5UeImPFmfj4fJDUeo8\_swBx-NotyF1pDJWB2tF7bKFFHjvj6PfZAN8jAqshshaj2xsZFqqTrV0-CZ-ChaWXW1Hi82JL\_4lwR-LCvfFrz8QYqf-qRJEOSiW9L23W-ykGqVdmRJOZcd9aGT3NmswXCqkV1MWyw2S9pnDaScVPuXACuAlfuWiF7B8Y7HBISzSudgxHvSe93a2Jo

**Instancias (1/1)** [Información](#)  


<input checked="" type="checkbox"/>	Name	ID de la instancia	Estado de la i...
<input checked="" type="checkbox"/>	Web Server	i-0c16326510557a1c9	 En ejecución  

**Paso 9:** AWS Management Console → Services → S3

- No se pueden visualizar los contenidos de los S3.
- Permisos de EC2-Support no permiten ver el contenido de los S3.

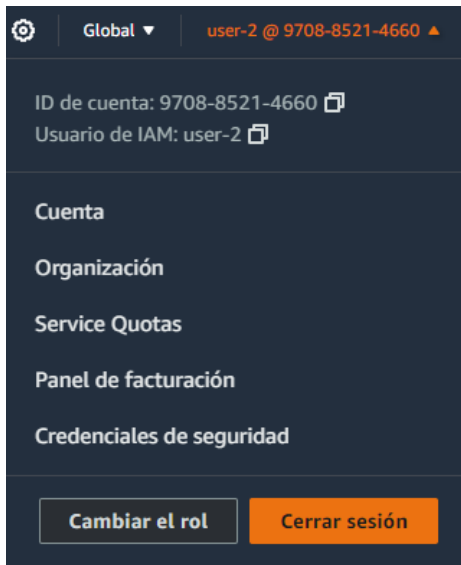
**Buckets** [Información](#)  
Los buckets son contenedores de datos almacenados en S3. [Más información](#) 

Nombre	Región de AWS
--------	---------------

 **No tiene permisos para obtener una lista de los buckets**  
Una vez que usted o el administrador de AWS hayan actualizado los permisos



## Paso 10: Cerrar sesión de cuenta user-2



## Paso 11: Abrir una ventana incognito en un navegador.

- Pegar el **Link** en la ventana incognito del navegador.
- Iniciar sesión con user-3
- IAM username = user-3
- Password = Lab-password3

ID de cuenta (12 dígitos) o alias de cuenta

970885214660

Nombre de usuario:

user-3

Contraseña:

.....

☐ Recordar esta cuenta

Iniciar sesión

**Paso 12:** EC2 → Instances → Seleccionar una instancia → Instance State → Stop Instance

- Usuario tiene permisos para detener instancias.
- Permisos de EC2-Support permiten detener instancias.

**Instancias (1/1)** Información

Q Buscar instancia por atributo o etiqueta (case-sensitive)

<input checked="" type="checkbox"/>	Name ▾	ID de la instancia	Estado de la i... ▾
<input checked="" type="checkbox"/>	Web Server	i-0c16326510557a1c9	En ejecución 🔍

✔ Se ha detenido correctamente i-0c16326510557a1c9

**Instancias (1/1)** Información

Q Buscar instancia por atributo o etiqueta (case-sensitive)

<input checked="" type="checkbox"/>	Name ▾	ID de la instancia	Estado de la i... ▾
<input checked="" type="checkbox"/>	Web Server	i-0c16326510557a1c9	Deteniéndose 🔍

En esta tarea, pudo iniciar sesión como los tres usuarios. Verificó que el user-1 podía ver los S3 Buckets pero no podía ver las instancias de EC2.

Inició sesión como usuario-2 y verificó que podía ver las instancias EC2, pero no podía realizar la acción de detener instancia. el usuario-2 tampoco podía ver los S3 Buckets.

Inició sesión como usuario-3 y verificó que pudo ver las instancias EC2 y realizar la acción de detener instancia.

Laboratorio Completado

