

INTRODUCCIÓN A AWS IDENTITY AND ACCESS MANAGEMENT (IAM)

Laboratorio 279

Participantes: Felipe Barceló, Balter Velázquez, Michelle Devera,
Ignacio Suarez, Agustín Esteche y Juan Sanserro.

OBJETIVOS:

- 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

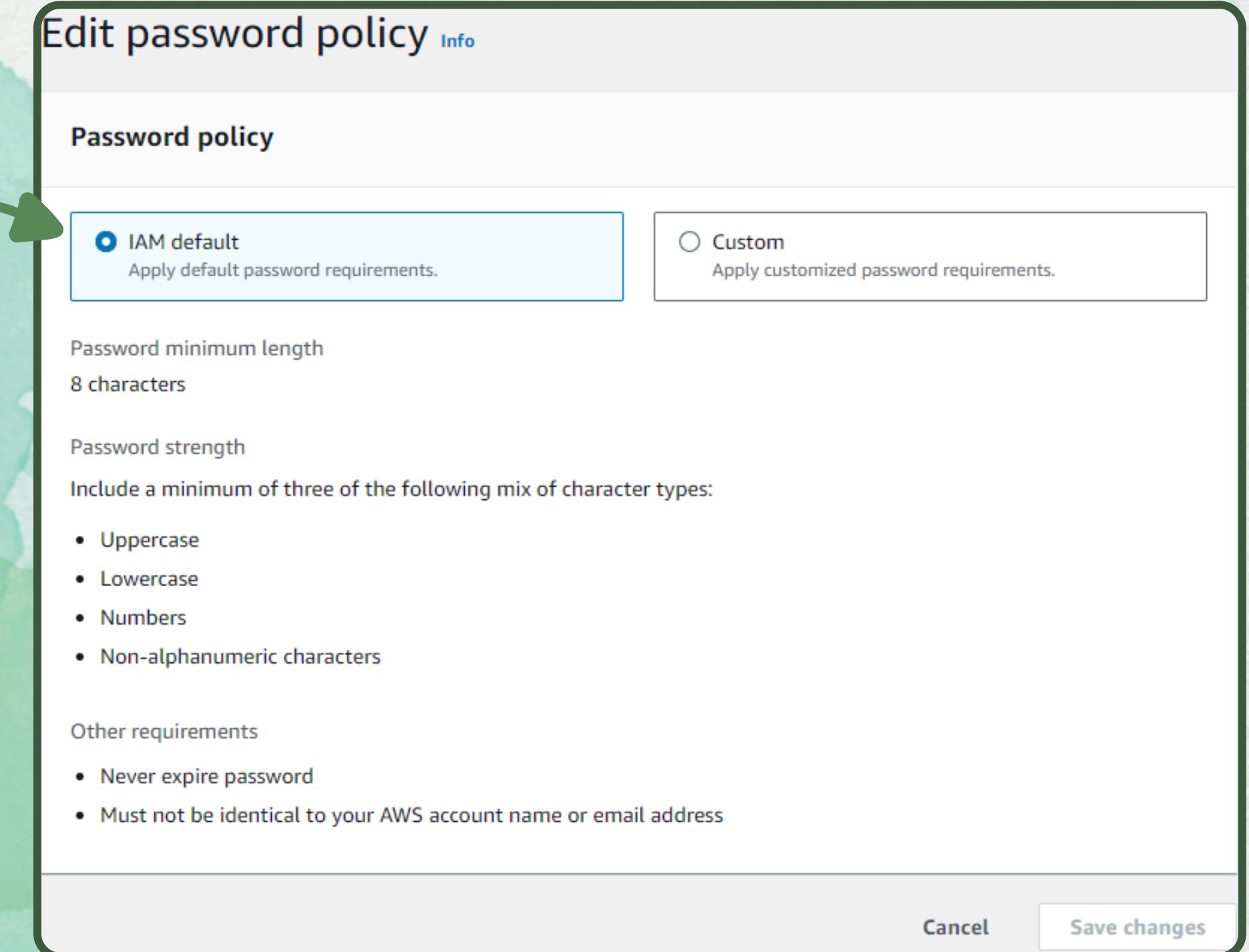
TAREA 1: CREAR UNA POLÍTICA DE CONTRASEÑA DE CUENTA

- En esta tarea crearemos una política de contraseña personalizada para la cuenta de AWS.
- Esta política afecta a todos los usuarios asociados con esa cuenta.

Aquí ingresamos a la consola de administración de AWS, en el cuadro de búsqueda , ingrese IAM y selecciónelo.

En el panel de navegación, elija Account settings (Configuración de la aplicación).

Seleccione Change password policy (Cambiar política de contraseñas).



En Select your account password policy requirements (Seleccionar los requisitos de políticas de contraseñas de su cuenta), configure las siguientes opciones:

Password policy

IAM default
Apply default password requirements.

Custom
Apply customized password requirements.

Password minimum length.
Inforce a minimum length of characters.
10 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 **90** 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 **5** password(s)
Needs to be between 1 and 24.

TAREA 2: ANALIZAR LOS USUARIOS y LOS GRUPOS DE USUARIOS

- En esta tarea exploraremos los usuarios y grupos que ya han sido creados para nosotros en AWS IAM.
- Aprendimos acerca de las políticas de asociación de los grupos de usuarios y cuales son las diferencias entre los diferentes permisos de los grupos.

En el panel de navegación, haga clic en Users (Usuarios). Podemos ver que hay algunos usuarios de IAM creados

Elegiremos **user-1**

The screenshot shows the 'User groups' page with three entries:

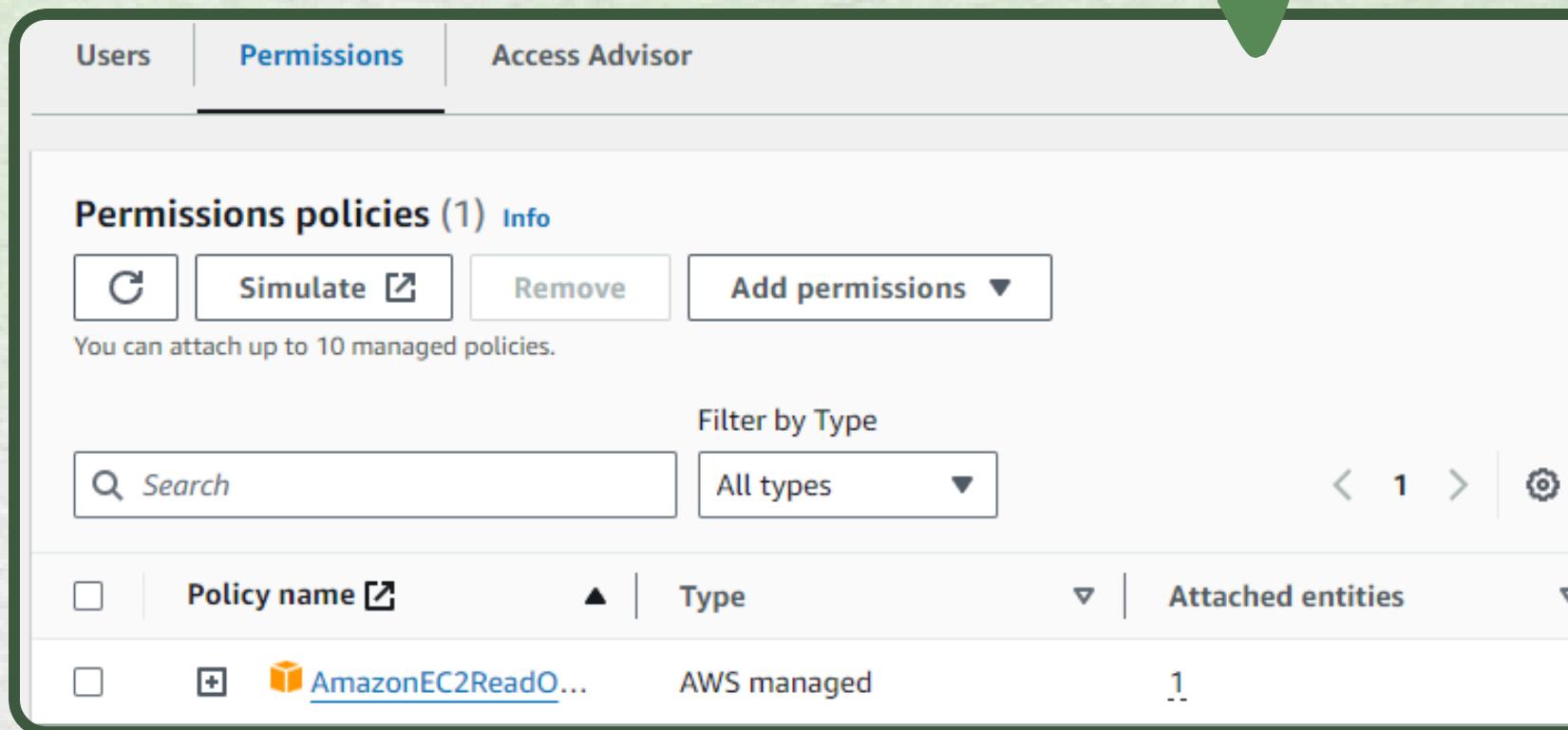
Group name	Users	Permissions	Creation time
EC2-Admin	⚠ 0	Defined	14 minutes ago
EC2-Support	⚠ 0	Defined	14 minutes ago
S3-Support	⚠ 0	Defined	14 minutes ago

The screenshot shows the 'Users' page with three entries:

User name	Path	Group	Last activity
user-1	/spl66/	0	
user-2	/spl66/	0	
user-3	/spl66/	0	

Iremos hasta la pestaña Groups y luego Security credentials elija User groups (Grupos de usuarios). Allí veremos los siguientes usuarios. Elegiremos el grupo EC2-Support.

Seleccione la pestaña Permissions (Permisos).
Junto a la política AmazonEC2ReadOnlyAccess, seleccione el signo más para mostrar la política.



La política tiene permisos para obtener y hacer una lista de recursos en Amazon S3.

This screenshot shows the 'Permissions policies' page with one policy listed: 'AmazonS3ReadOnlyAccess'. A green arrow points from the text above to this policy. The policy is described as providing 'read only access to all buckets via the AWS Management Console'. Below the description is a JSON representation of the policy:

```
1 { "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:Get*", "s3>List*", "s3:Describe*", "s3-object-lambda:Get*", "s3-object-lambda>List*" ], "Resource": "*" } ] }
```

Permissions policies (1) [Info](#)

[Copy](#) [Simulate](#) [Remove](#) [Add permissions](#) ▾

You can attach up to 10 managed policies.

Filter by Type

[All types](#) ▾

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

AmazonEC2ReadOnlyAccess

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

[Copy JSON](#)

```
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}
```

Este usuario tiene una política insertada de cliente, que es una política asignada a un único usuario o grupo. Las políticas insertadas, generalmente, se usan para asignar permisos a situaciones aisladas.

La política de este usuario concede permiso para ver, iniciar o detener instancias de EC2.

Permissions policies (1) Info			
	Simulate	Remove	Add permissions ▾
You can attach up to 10 managed policies.			
Filter by Type			
	<input type="text"/> Search	All types ▾	« 1 » ⚙️
<input type="checkbox"/>	Policy name 🔗	Type	Attached entities
<input type="checkbox"/>	EC2-Admin-Policy	Customer inline	0
EC2-Admin-Policy		Copy JSON	Edit 🔗
<pre>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 }</pre>			

TAREA 3: AGREGAR USUARIOS A LOS GRUPOS DE USUARIOS

- Problema: Recientemente contratamos a tres personas que realizarán diferentes tareas.
 - user-1 al grupo S3-Support
 - user-2 al grupo EC2-Support
 - user-3 al grupo EC2-Admin
- En esta tarea deberemos de añadir a todos los usuarios a su grupo correspondiente.

AGREGAR A USER-1 AL GRUPO S3-SUPPORT.

- En la ventana Add users to S3-Support (Aregar usuarios a S3-Support), configure las siguientes opciones:
 - Seleccione la casilla que corresponde a user-1.
 - Seleccione Add users (Aregar usuarios).
 - En la pestaña Users (Usuarios), verá que user-1 se agregó al grupo.

The image contains two screenshots of the AWS IAM console. The top screenshot shows the 'Add users to S3-Support' window. It has a search bar at the top followed by a table titled 'Other users in this account (1/3)'. The table lists three users: 'user-1' (selected with a checked checkbox), 'user-2', and 'user-3'. Each row includes columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. A green curved arrow points from the text 'user-1' in the first bullet point to the 'user-1' entry in the table. The bottom screenshot shows the 'Users in this group' list for the 'S3-Support' group. It has a search bar at the top followed by a table. The table lists one user, 'user-1', with a checked checkbox next to it. The table includes columns for 'User name' and 'Groups'.

Other users in this account (1/3)

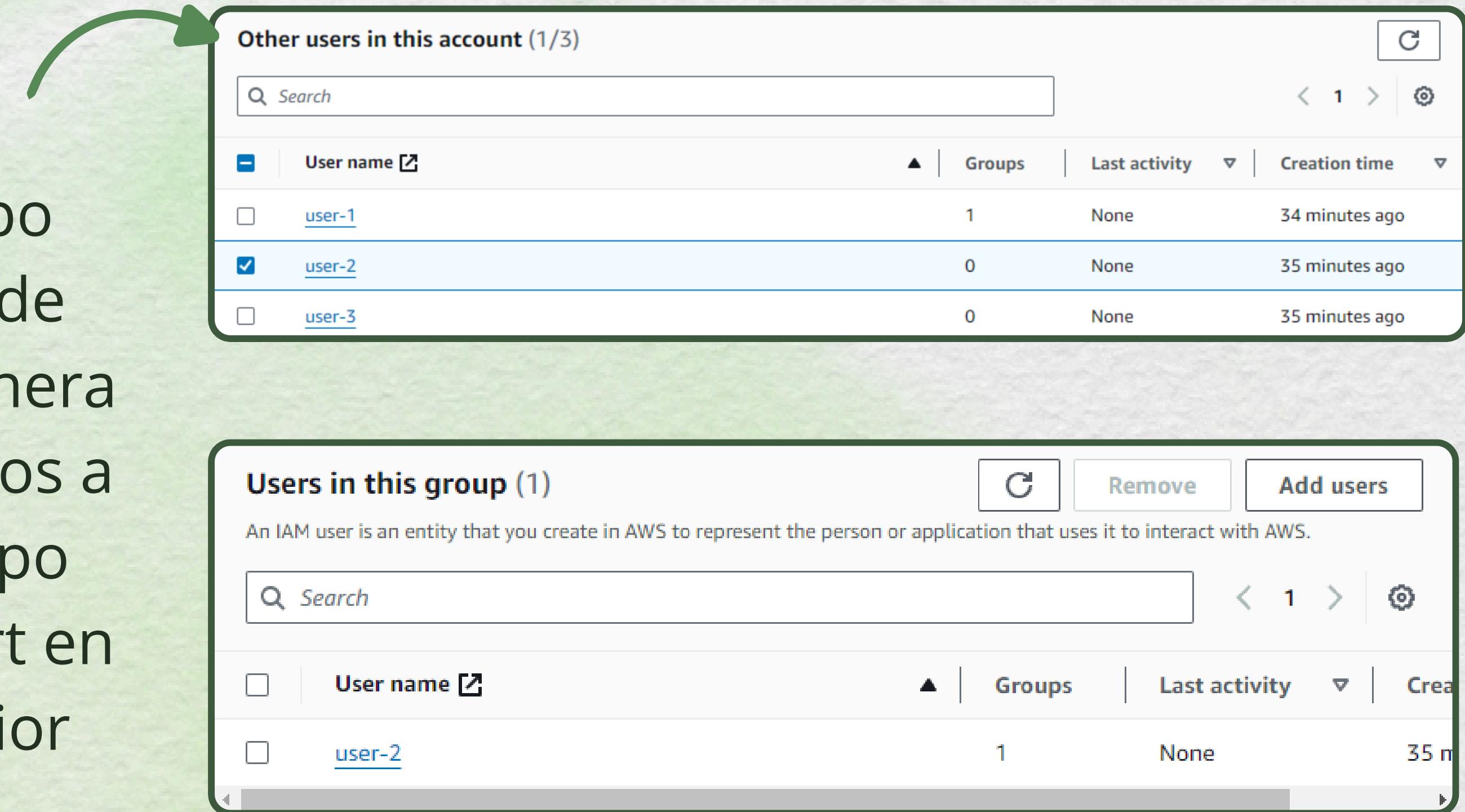
User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/> user-1	0	None	32 minutes ago
<input type="checkbox"/> user-2	0	None	32 minutes ago
<input type="checkbox"/> user-3	0	None	32 minutes ago

Users in this group (1)

User name	Groups
<input type="checkbox"/> user-1	1

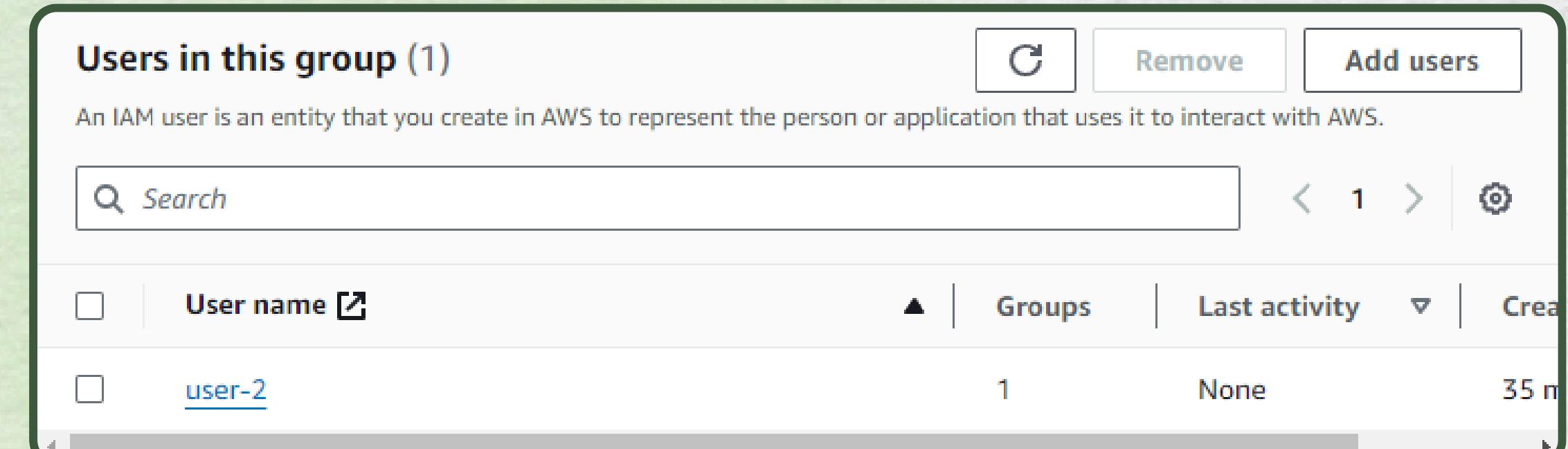
AGREGAR A USER-2 AL GRUPO EC2-SUPPORT.

- Y ahora agregamos a user-2 al grupo EC2-Support de la misma manera que agregamos a user- 1 al grupo de S3-Support en el paso anterior



The screenshot shows the 'Other users in this account (1/3)' list. It includes a search bar, a header with columns for User name, Groups, Last activity, and Creation time, and three rows of data:

User name	Groups	Last activity	Creation time
user-1	1	None	34 minutes ago
user-2	0	None	35 minutes ago
user-3	0	None	35 minutes ago



The screenshot shows the 'Users in this group (1)' list for the EC2-Support group. It includes a search bar and one row of data:

User name	Groups	Last activity	Creation time
user-2	1	None	35 m

AGREGAR A USER-3 AL GRUPO EC2-ADMIN

- Y ahora agregamos a user-3 al grupo EC2-Admin de la misma manera que agregamos a los dos otros usuarios a sus respectivos grupos.

The screenshot shows two panels of the AWS IAM Groups interface. The top panel, titled 'Other users in this account (1/3)', lists three users: user-1, user-2, and user-3. user-3 is selected, indicated by a checked checkbox. The bottom panel, titled 'Users in this group (1)', shows the single user user-3 listed under the EC2-Admin group. A green arrow points from the text in the slide to the 'user-3' row in the top panel.

User name	Groups	Last activity	Creation time
user-1	1	None	36 minutes ago
user-2	1	None	37 minutes ago
<input checked="" type="checkbox"/> user-3	0	None	37 minutes ago

User name	Groups	Last activity	Creation time
<input type="checkbox"/> user-3	1	None	37 m

CONTRATÓ A USER-3 COMO ADMINISTRADOR DE AWS EC2 PARA QUE
ADMINISTRE SUS INSTANCIAS EC2.

TAREA 4: INICIAR SESIÓN Y PROBAR PERMISOS DE USUARIOS

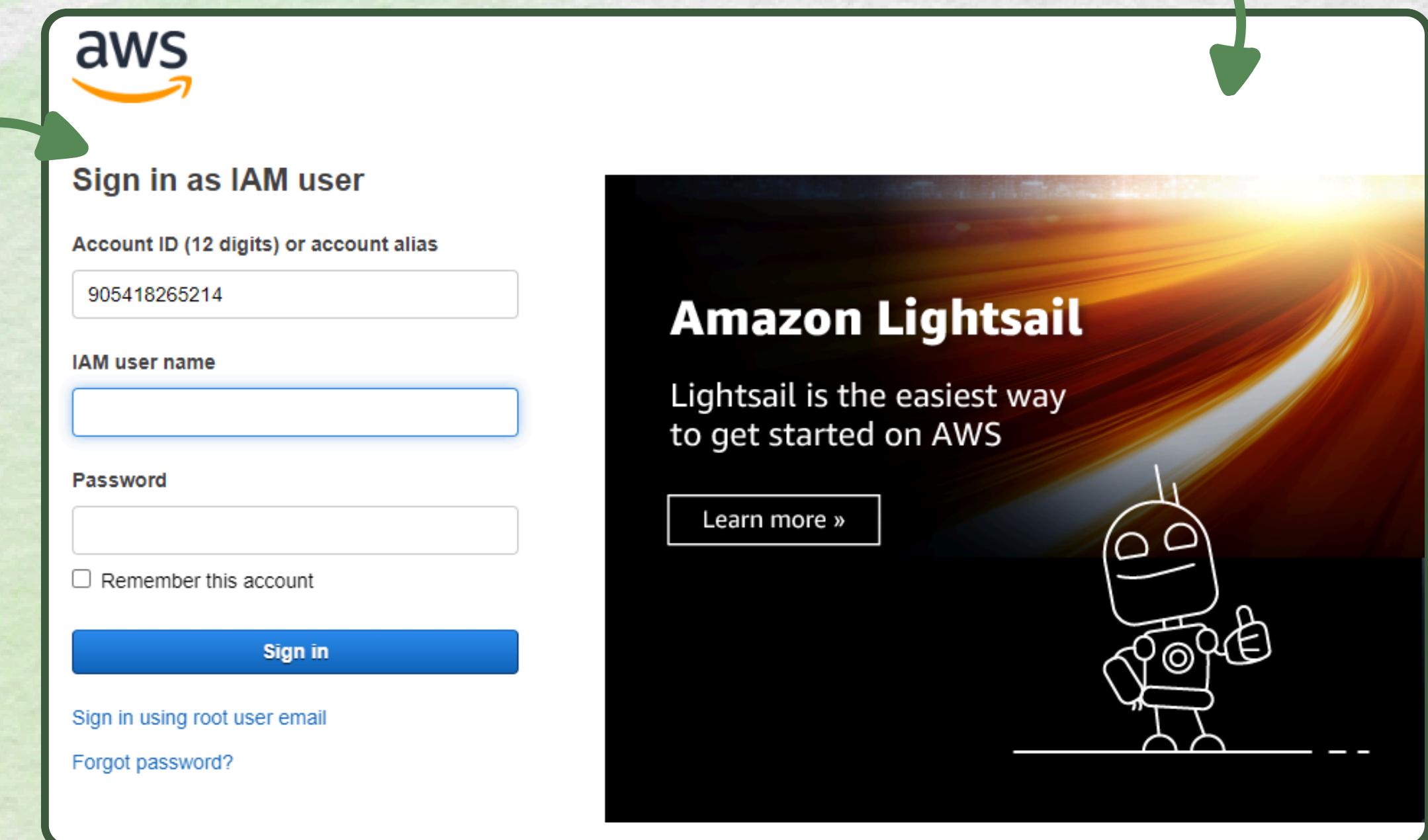
- En esta tarea probaremos los permisos para cada uno de los usuarios.
- Verificaremos que el user-1 puede ver los S3 buckets pero no las instancias EC2.
- Verificaremos que el user-2 puede ver las instancias EC2 pero no puede detenerlas ni ver los S3 buckets.
- Verificaremos que el user-3, puede ver y detener las instancias EC2.

En el panel de navegación izquierdo, seleccione Dashboard (Panel). La sección AWS Account (Cuenta de AWS) incluye una URL de inicio de sesión para los usuarios de IAM en esta cuenta. En nuestro caso es:

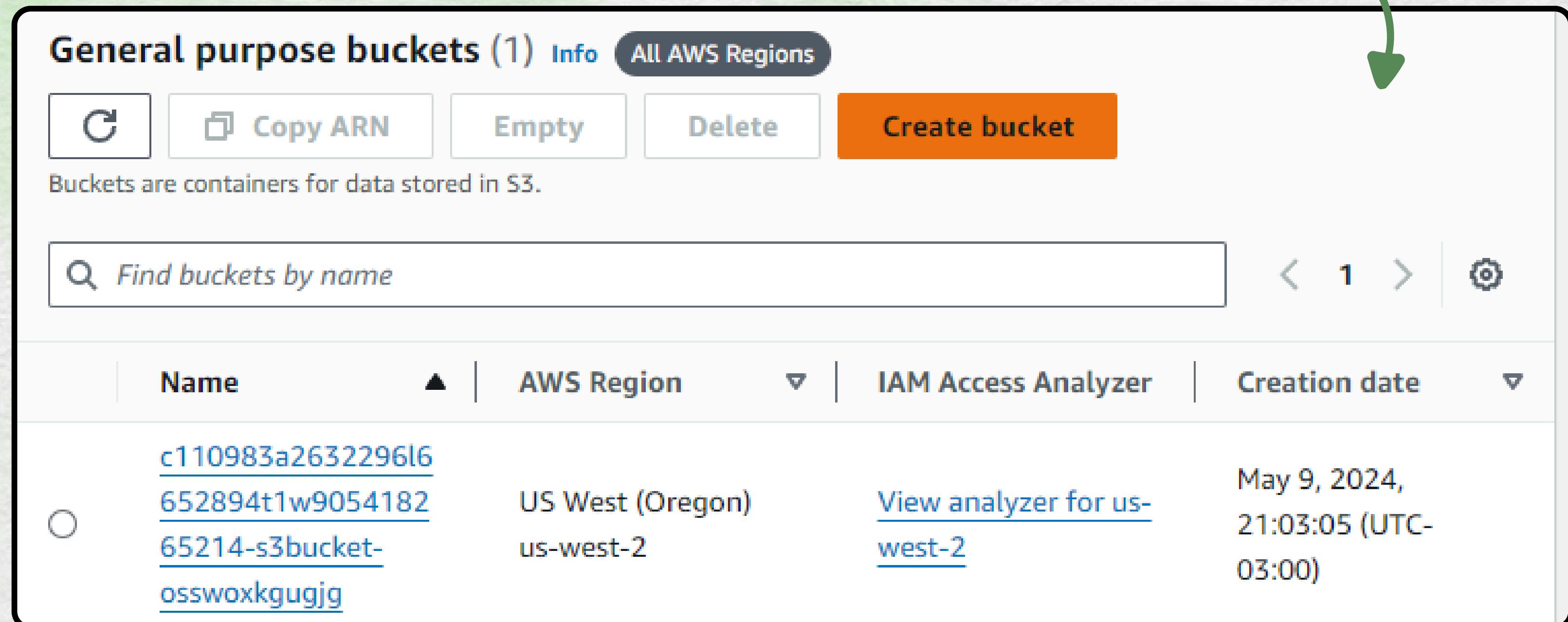
<https://905418265214.signin.aws.amazon.com/console>

Inicie sesión con las siguientes credenciales:

- IAM user name (Nombre de usuario AIM): Ingrese user-1
- Password (Contraseña): Ingrese Lab-Password1



- Haga clic en el nombre de uno de los buckets y busque el contenido.
- Debido a que el usuario forma parte del grupo S3-Support en IAM, tiene permiso para ver una lista de buckets de S3 y su contenido.



General purpose buckets (1) [Info](#) [All AWS Regions](#)

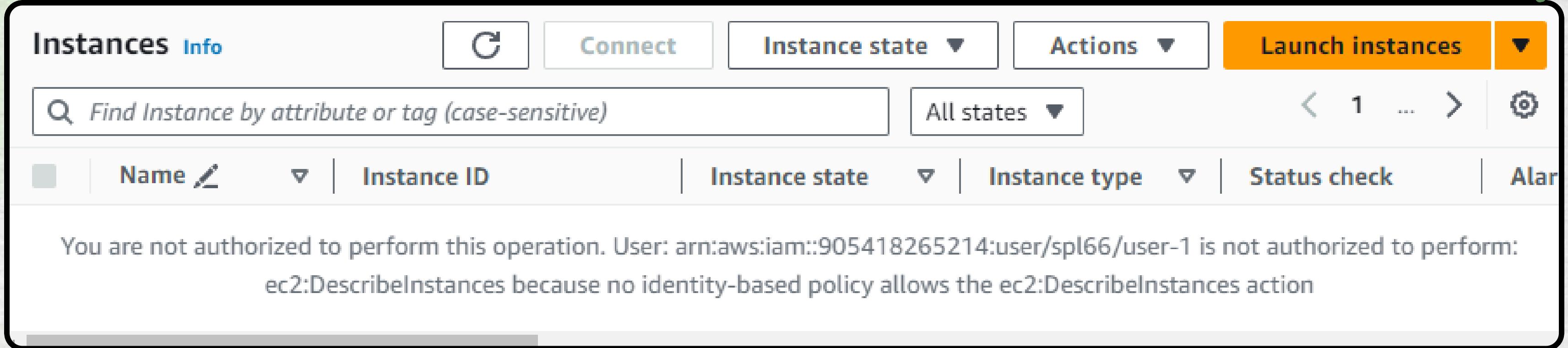
[**C**](#) [!\[\]\(81312b19ca3202a7c3e2f42667ac19f0_img.jpg\) Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

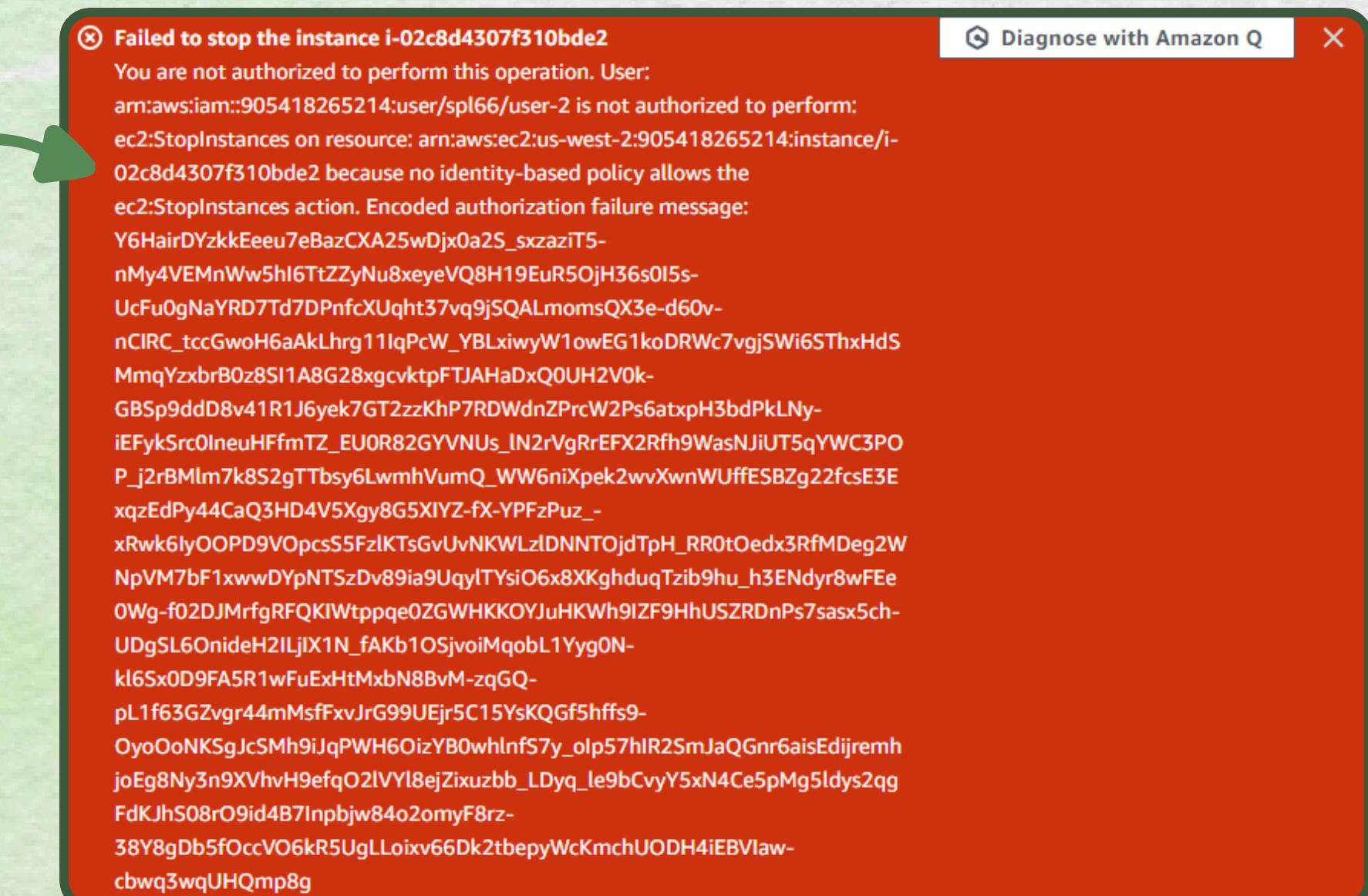
 [Find buckets by name](#) [<<](#) [1](#) [>](#) 

Name	AWS Region	IAM Access Analyzer	Creation date
c110983a2632296l6	US West (Oregon)	View analyzer for us-west-2	May 9, 2024, 21:03:05 (UTC-03:00)
652894t1w9054182	us-west-2		
65214-s3bucket-osswoxkgugjg			

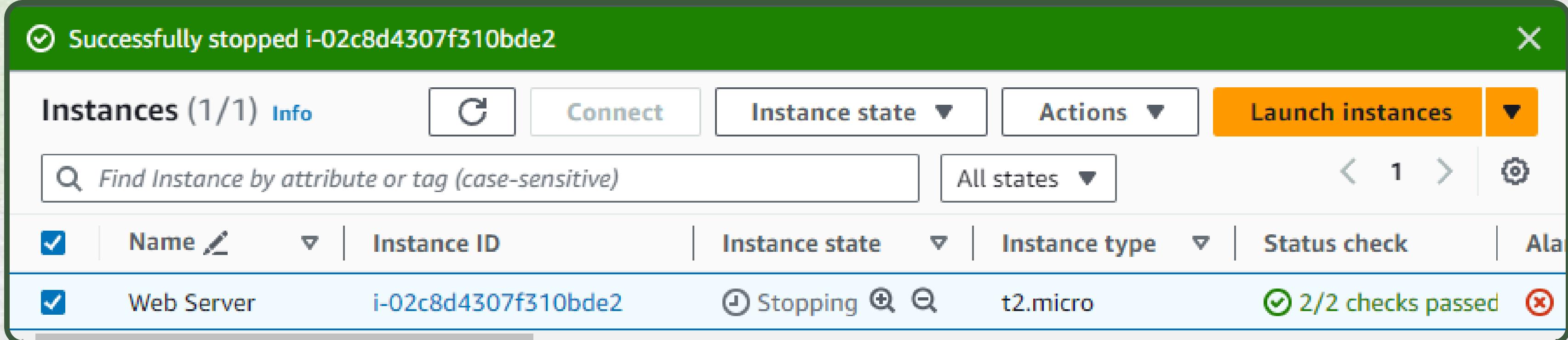
- Ahora, pruebe si tienen acceso a Amazon EC2.
- En el panel de navegación, elija Instances (Instancias).
- No puede ver ninguna instancia. En su lugar, verá el siguiente mensaje. Este mensaje aparece ya que el usuario no tiene ningún permiso para utilizar Amazon EC2.



- Cierre la sesión de user-1 en la Consola de administración de AWS
 - Ahora, iniciará sesión como user-2, a quien se contrató como personal de soporte para Amazon EC2.
 - Ahora puede ver una instancia de EC2 porque tiene permisos de solo lectura. Sin embargo, no podrá realizar ninguna modificación en los recursos de Amazon EC2.
-
- Desde la lista desplegable Instance state, seleccione Stop instance (Detener instancia).
 - En la ventana Stop instance (Detener instancia), elija Stop (Detener).
 - Recibirá el siguiente mensaje ya que la política le otorga el permiso solo para ver información y no para realizar cambios.



- Cierre la sesión de user-2 en la Consola de administración de AWS
- Ahora, iniciará sesión como user-3, a quien se contrató como personal administrador para Amazon EC2.
- En el panel de navegación, elija Instances (Instancias).
- En la ventana Stop instance (Detener instancia), elija Stop (Detener).
- Ahora la instancia si se debería de detener ya que el user-3 tiene los permisos necesarios.



CONCLUSIONES:

- Creamos y aplicamos una política de contraseñas en IAM.
- Exploramos usuarios y grupos de IAM ya creados.
- Inspeccionar políticas de IAM aplicadas a los grupos ya creados.
- Agregamos usuarios a grupos con capacidades específicas activas.
- Localizamos y utilizamos el URL para iniciar sesión en IAM.
- Experimentamos con el efecto de las políticas en nuestros servicios.

¡GRACIAS POR SU ATENCIÓN!