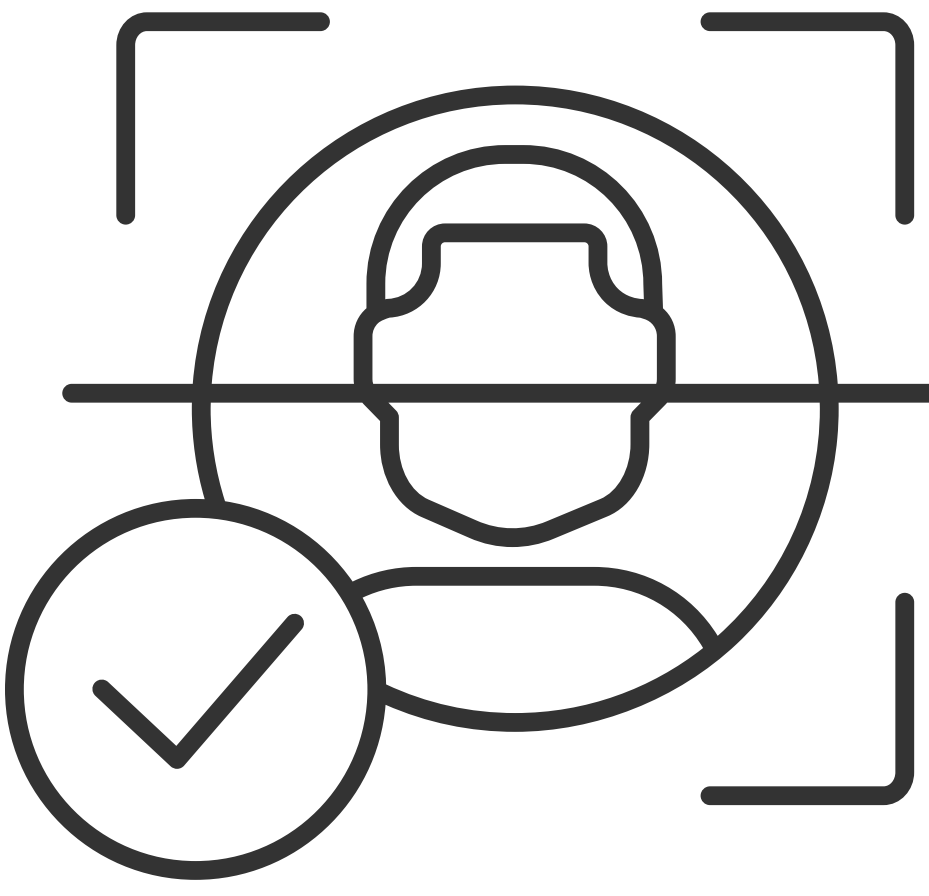
26°

Lab - AWS re/Start

Introducción a la Gestión de Identidades



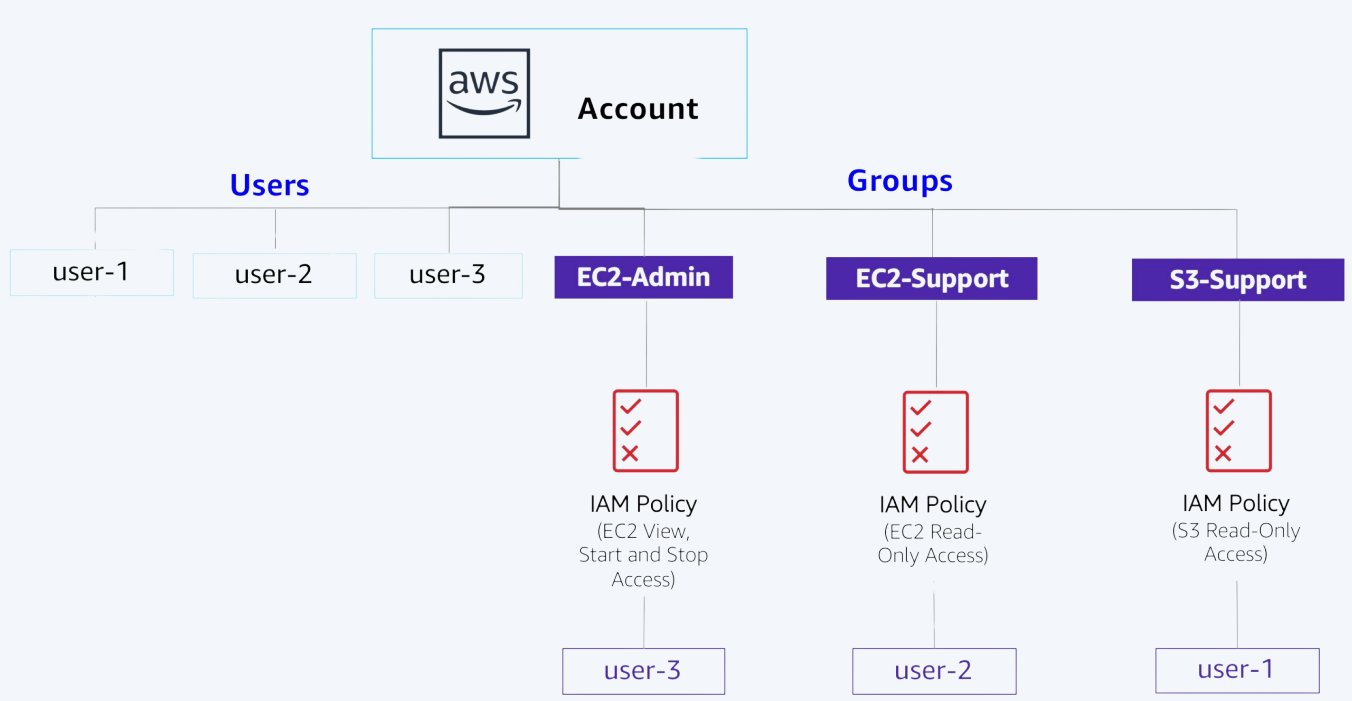
SWIPE

Tarea 01

Gestionado user, grps y roles con AWS IAM

A continuación, se muestra los objetivos del laboratorio:

- 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



SWIPE

Tarea 01

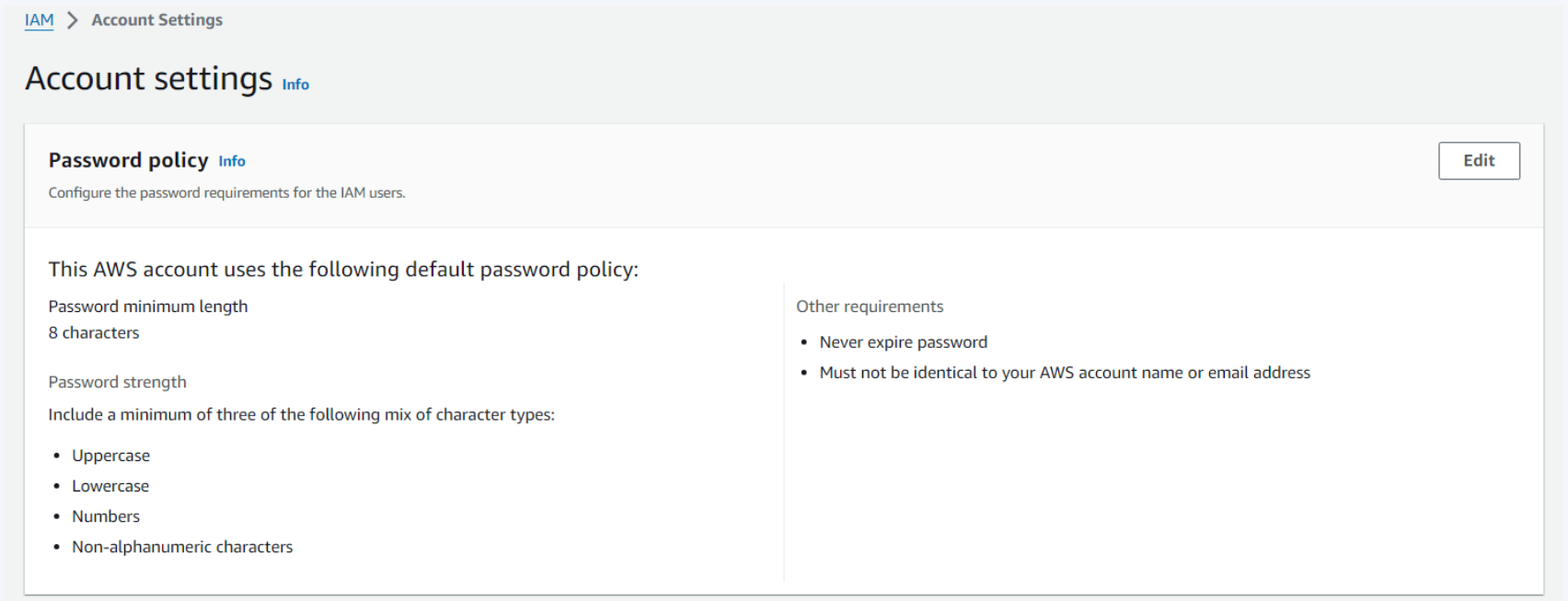
Es conveniente tener un repaso de lo que es AWS IAM (Identity and Access Management), este servicio se puede usar para lo siguiente:

- **Administrar usuarios de IAM y su acceso**: puede crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos con Multi-Factor Authentication). Puede administrar los permisos para controlar qué operaciones puede realizar cada usuario.
- **Administrar roles de IAM y sus permisos**: un rol de IAM es similar a un usuario, ya que un rol es una identidad de AWS con políticas de permisos que establecen qué puede hacer o no la identidad en Amazon Web Services (AWS). Sin embargo, en lugar de estar asociado únicamente a una persona, el objetivo es que cualquiera que necesite el rol pueda asumirlo (incluso un servicio)

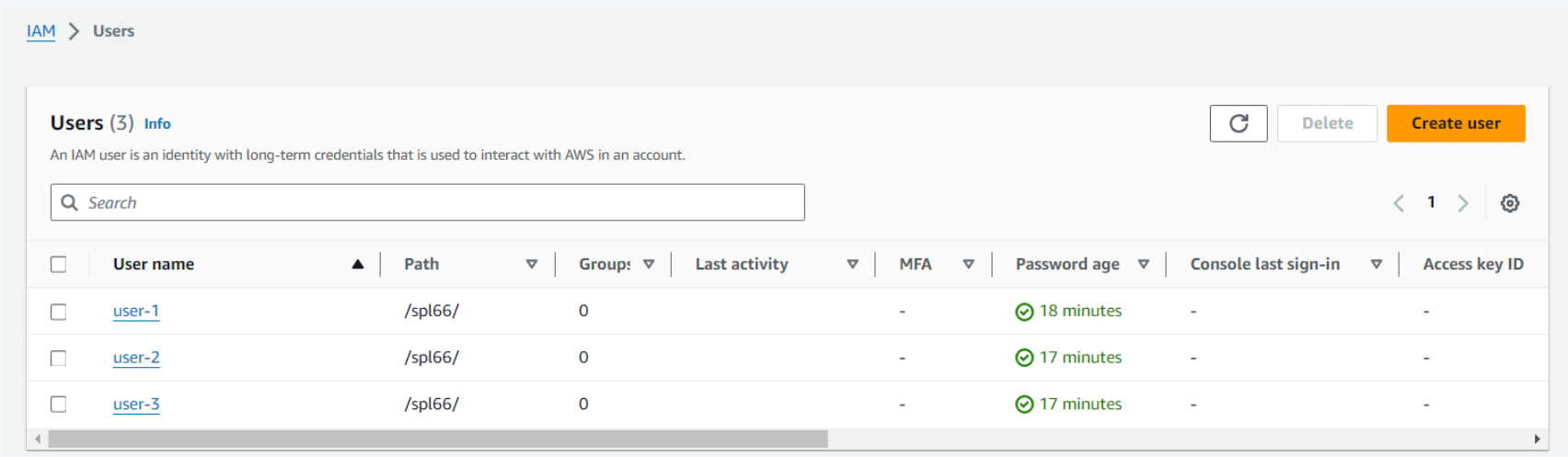
SWIPE

Tarea 01

Empezamos inspeccionando una política para la contraseña de la cuenta AWS. Esta política afecta a todos los usuarios asociados a esta cuenta. Acá notamos la política que se encuentra de manera predeterminada:



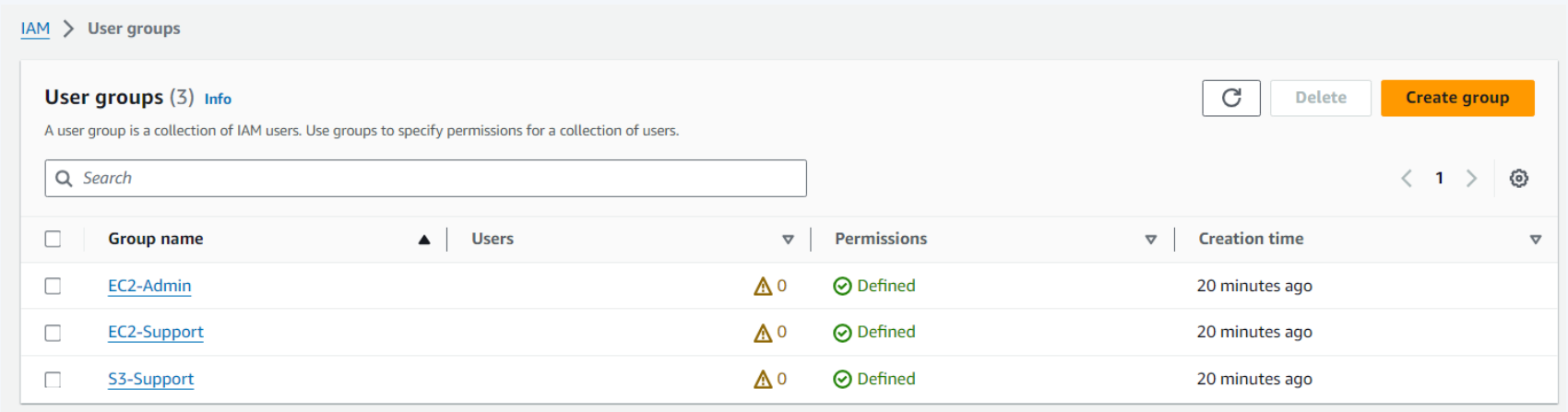
Ahora, procedemos a explorar los usuarios y grupos. A continuación se muestran los usuarios vinculados a la cuenta



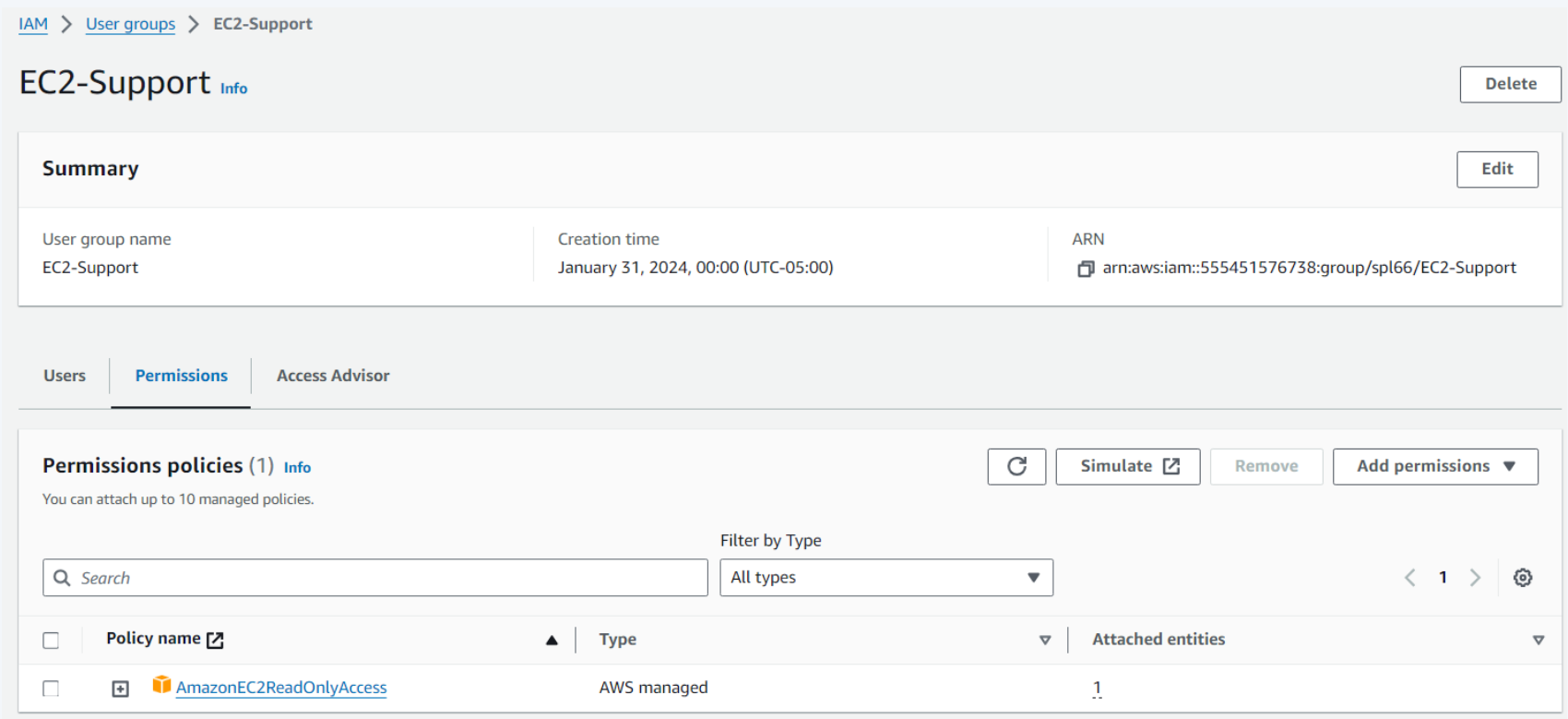
SWIPE

Tarea 01

Mientras que los grupos de usuarios:



Y podemos ver los permisos asignados al grupo EC2-Support

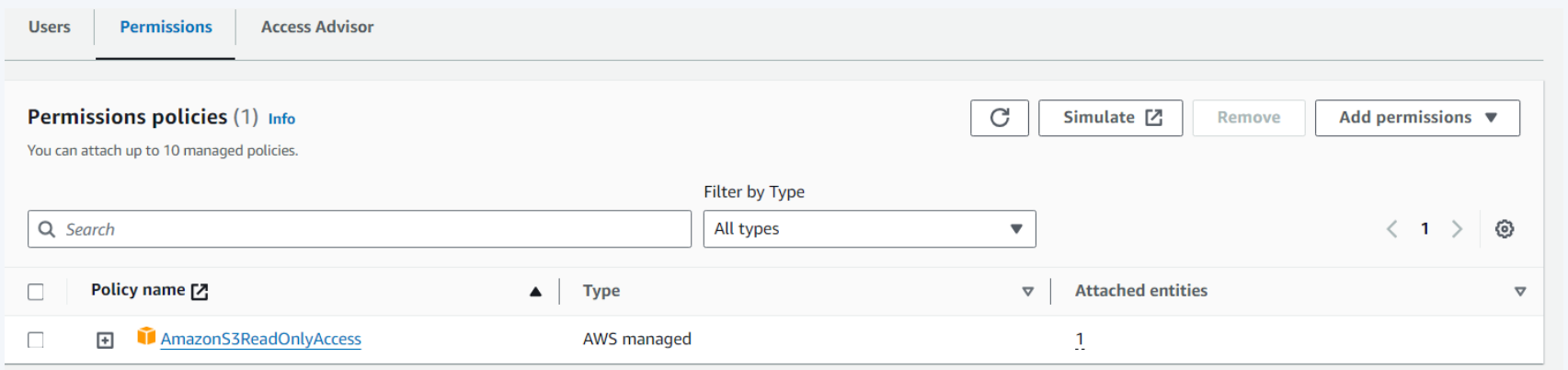


Donde **Effect** indica si tenemos *permitido* o *denegado* hacer alguna **Action** (eg: CloudWatch:ListMetrics). Y **Resource** puede ser eg: un bucket específico de S3, una instancia de EC2 o * que significa **cualquier recurso**.

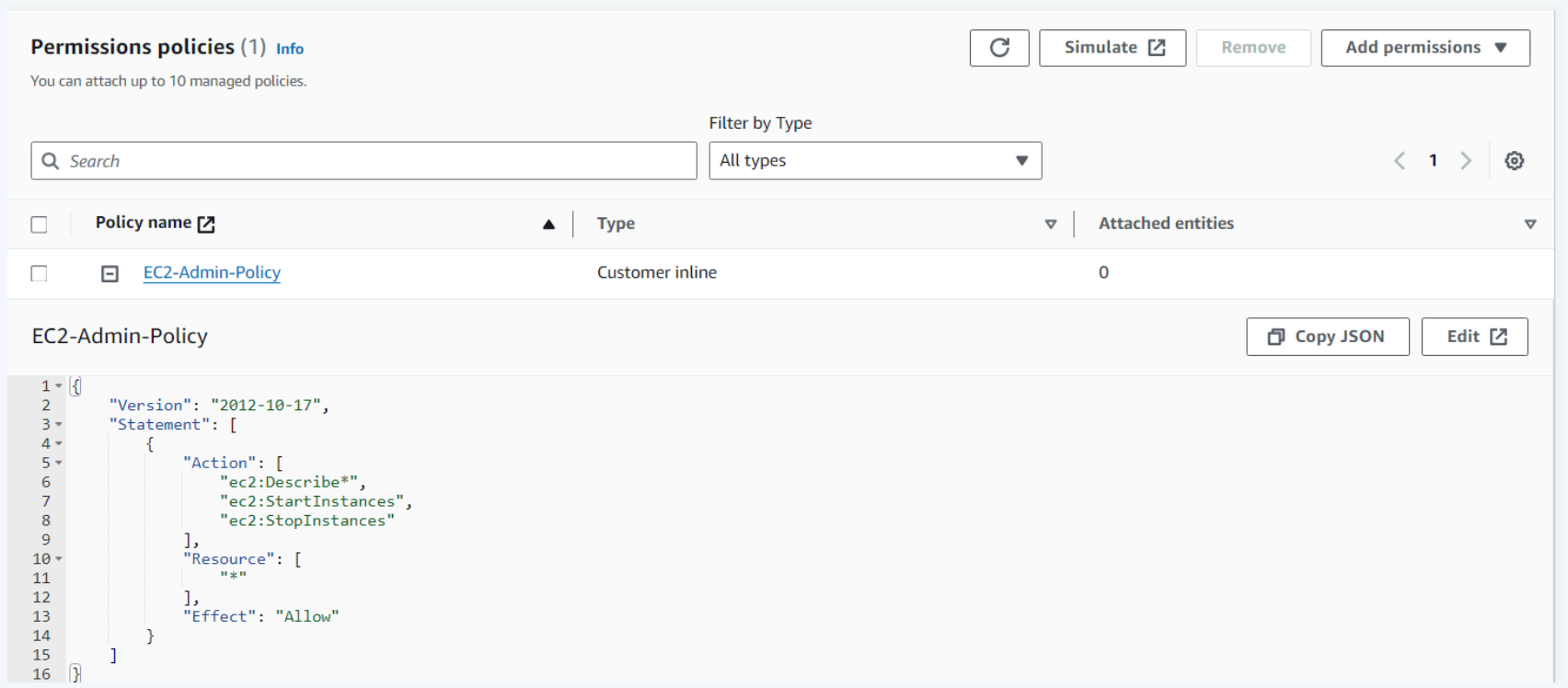
SWIPE

Tarea 01

Así, tenemos los permisos asignado al grupo S3-Support



Y al grupo EC2-Admin, cuya política es *Customer inline*, la cual es asignada únicamente a un único usuario o grupo



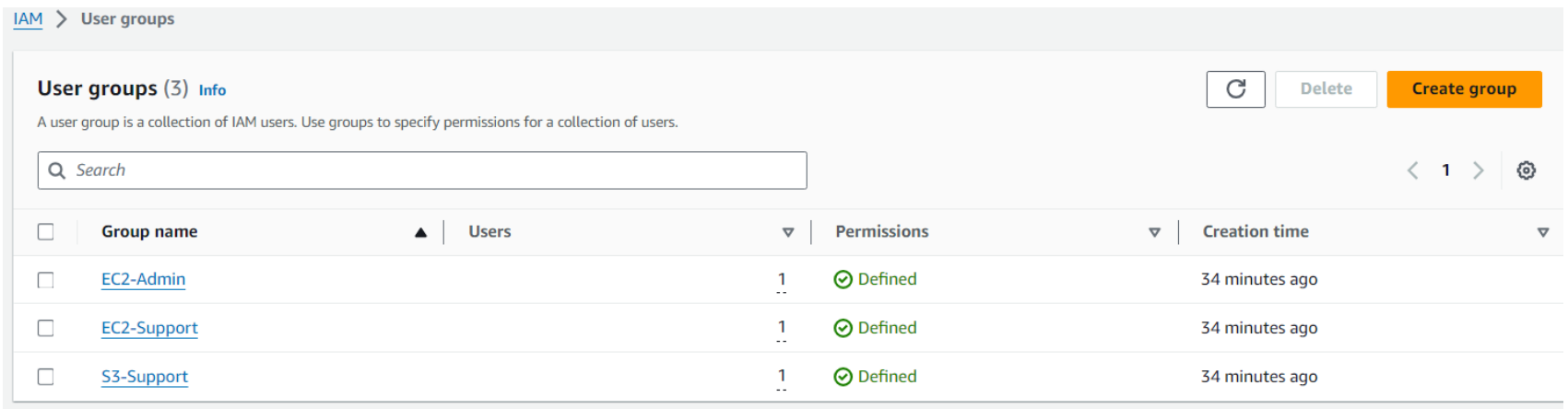
Como caso de negocio, debemos vincular estos usuarios

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

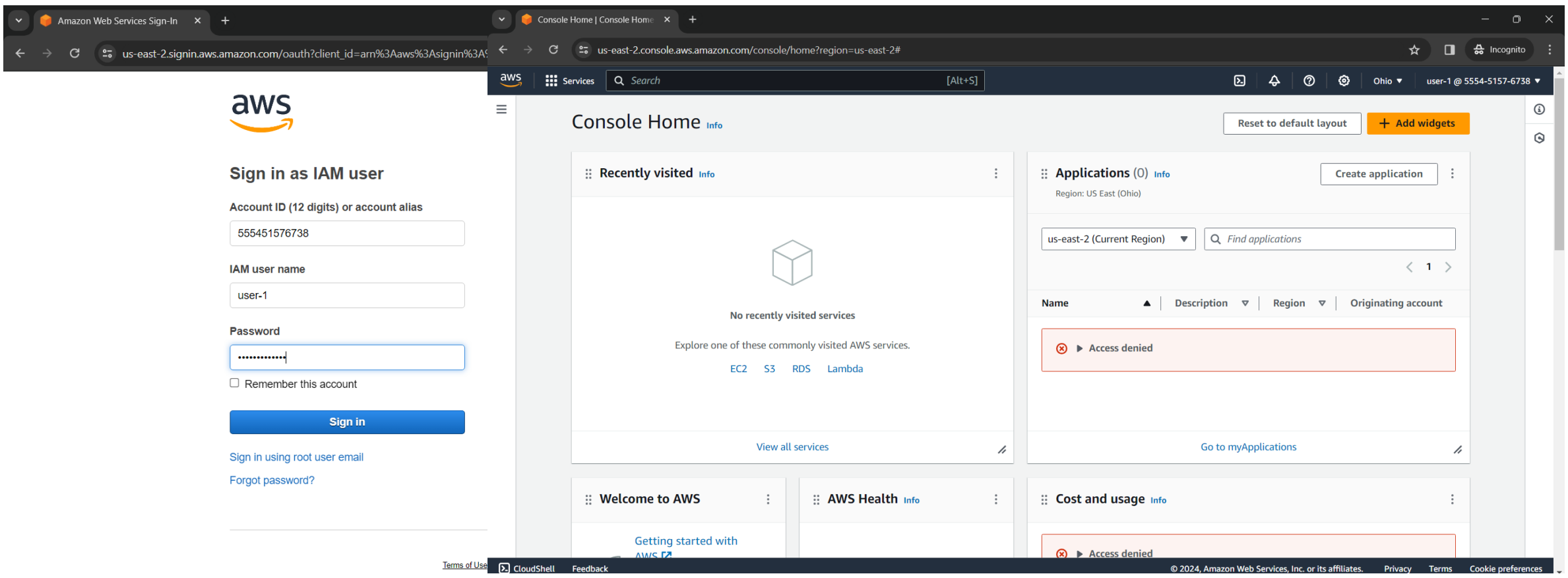
SWIPE

Tarea 01

Ahora, procederemos a añadir usuarios a sus respectivos grupos de usuarios:



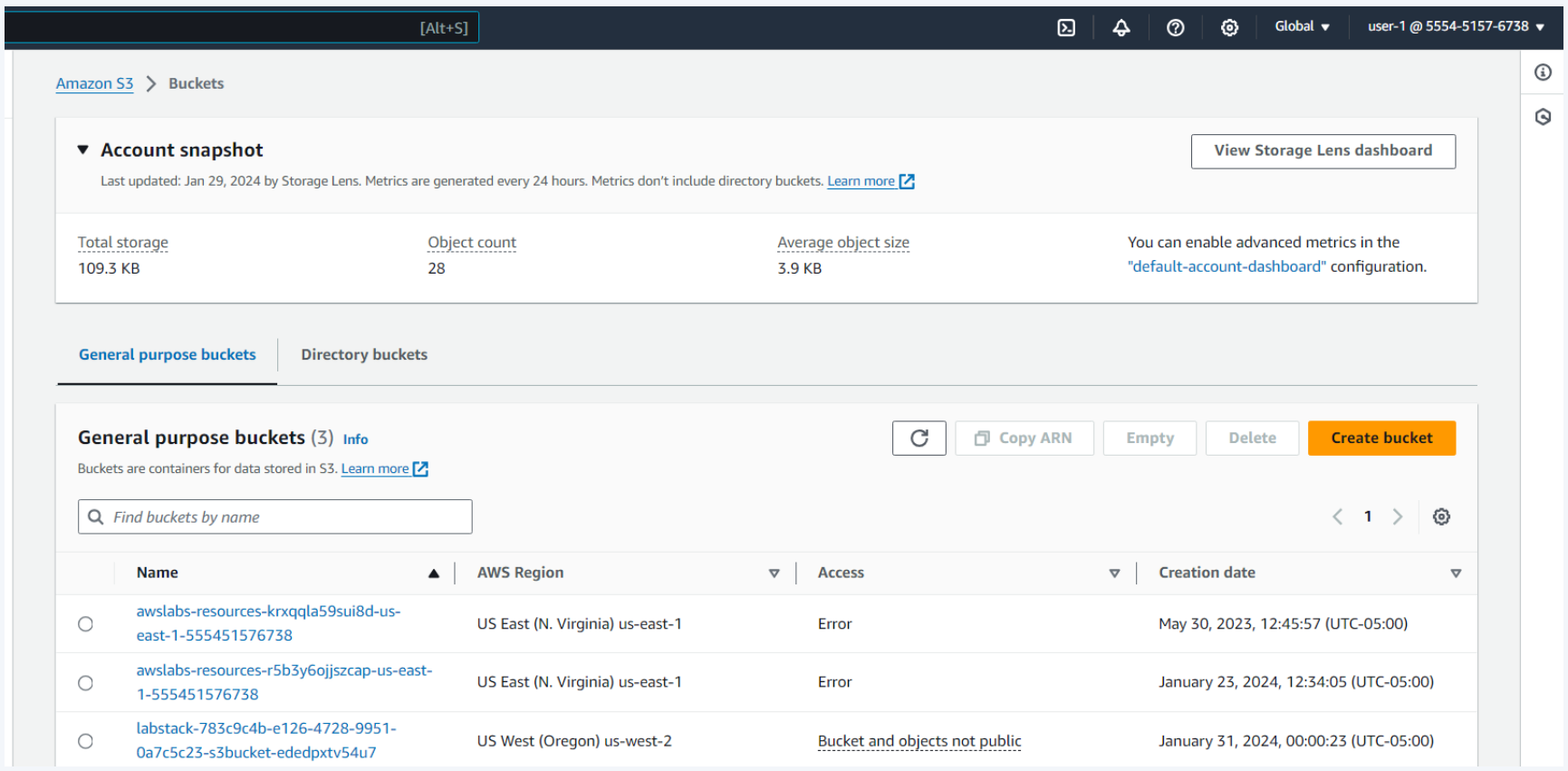
Esto nos permitirá testear los permisos asignados a partir del grupo vinculado de cada usuario. Pero, primero, comprobaremos el inicio de sesión usando el link para los usuarios IAM vinculados a esta cuenta. Pudimos ingresar con la clave del user-1 de manera exitosa



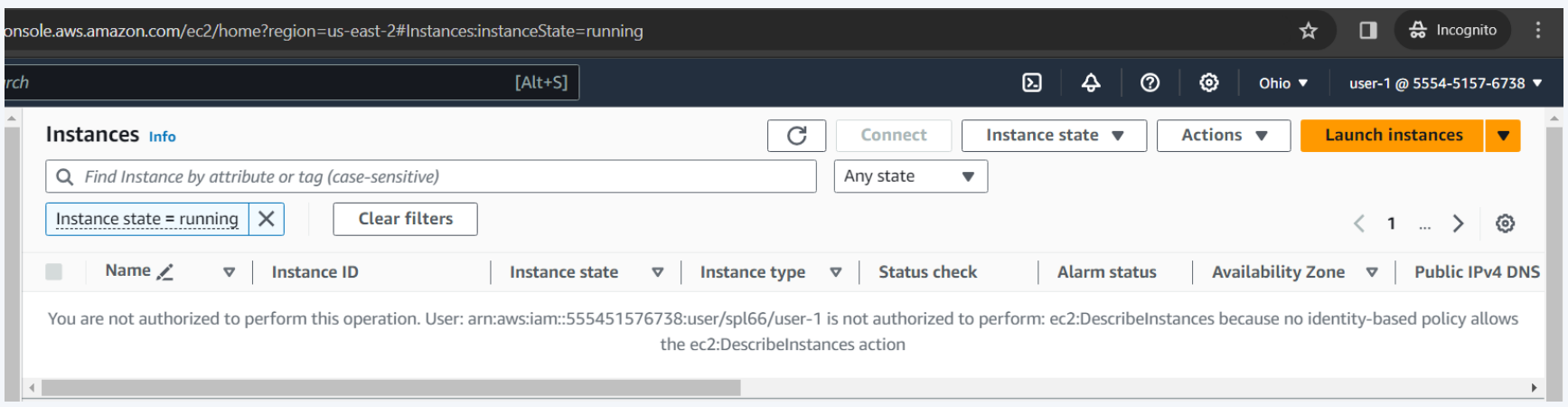
SWIPE

Tarea 01

Y podemos ver la lista de buckets de S3, lo cual va acorde al permiso asignado en el grupo S3-Support:



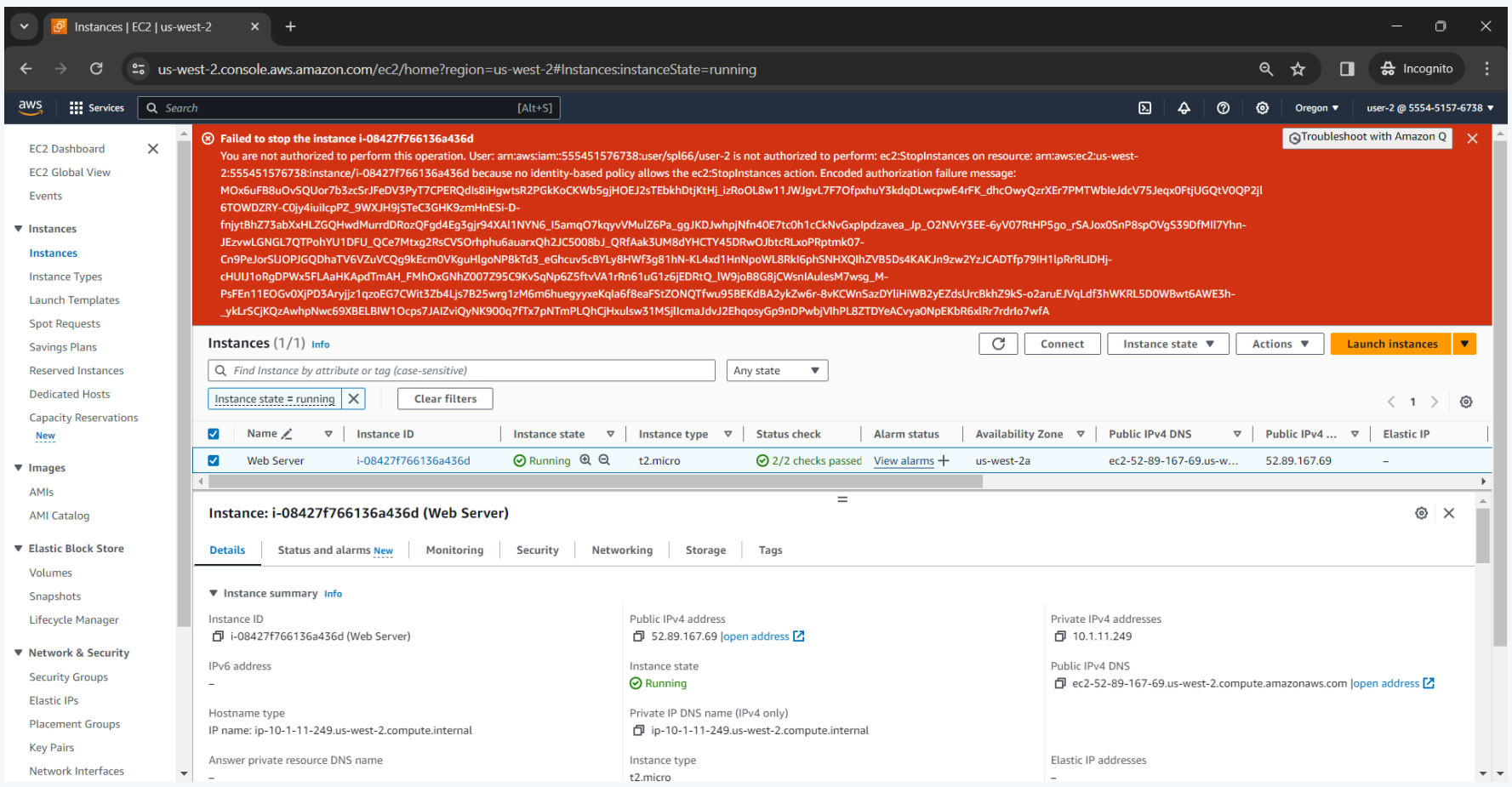
Y como no estamos autorizados para visualizar las instancias de EC2



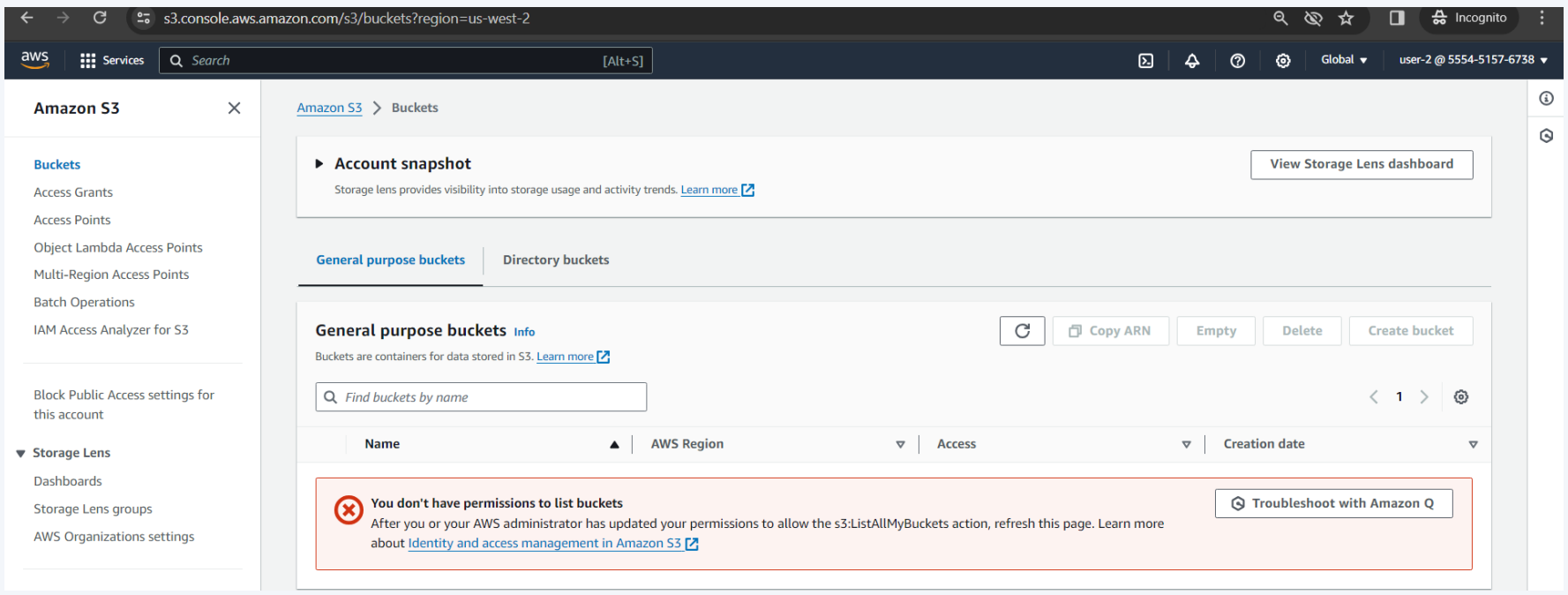
SWIPE

Tarea 01

Ahora ingresamos como user-2, y al tratar de detener una instancia de EC2 nos salta el mensaje de que no estamos autorizados. Esto solo lo puedo hacer el user-3, que pertenece al grupo EC2-Admin



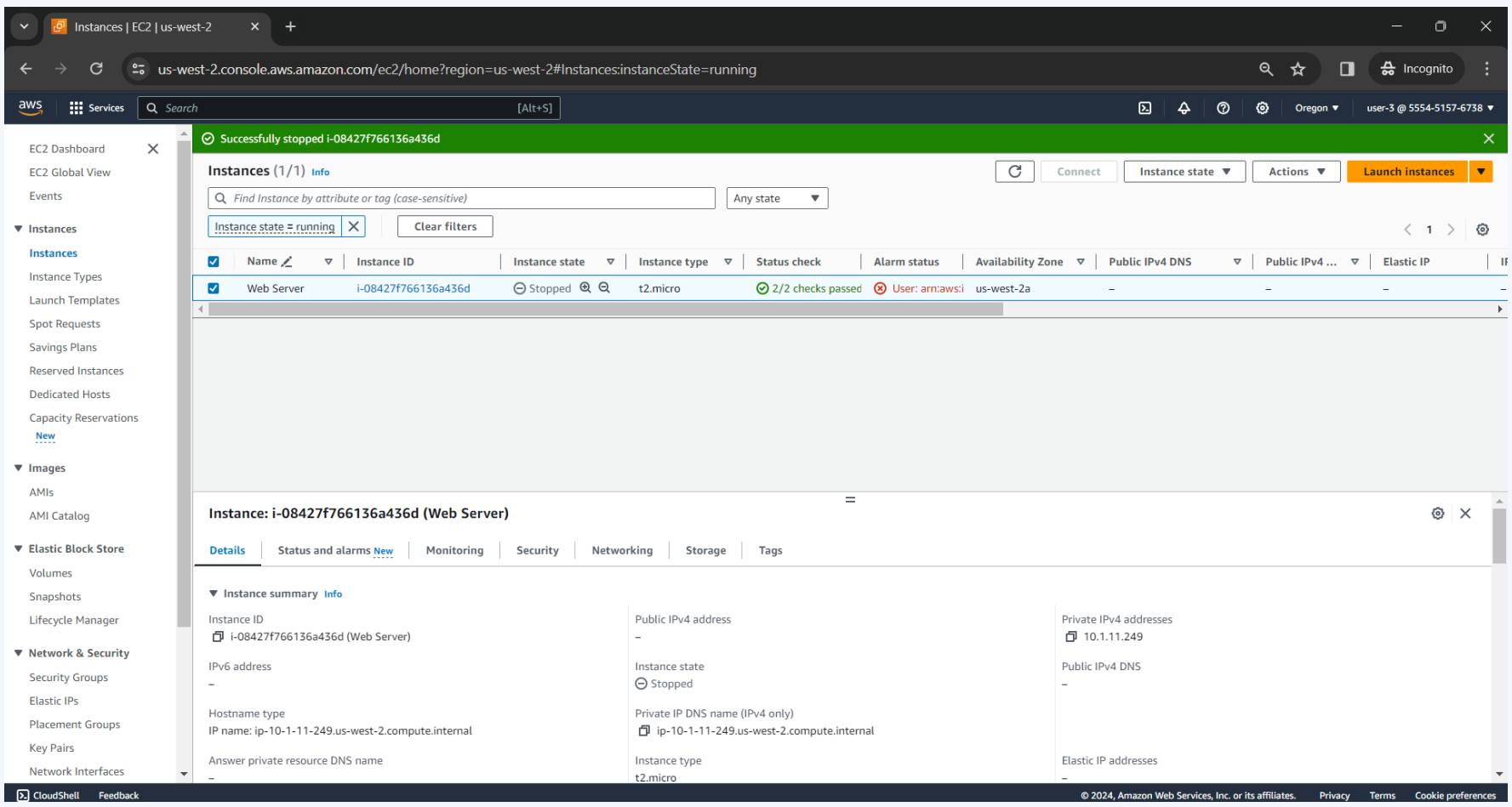
Y tampoco podemos ver la lista de buckets de S3



SWIPE

Tarea 01

Y como había mencionado, al logearme como user-3, ya puedo detener una instancia EC2, puesto que el grupo al que pertenece dicho usuario tiene el permiso **EC2-Admin-Policy** que te permite iniciar y detener instancias de EC2



SWIPE