

UD.1 Practica 2. AWS IAM

1

1.	<u>Introducción.....</u>	<u>3</u>
2.	<u>Explorar los usuarios y los grupos de IAM.....</u>	<u>4</u>
3.	<u>Añadir los usuarios a sus grupos.....</u>	<u>5</u>
4.	<u>Probar los permisos asignados a cada usuario.....</u>	<u>7</u>

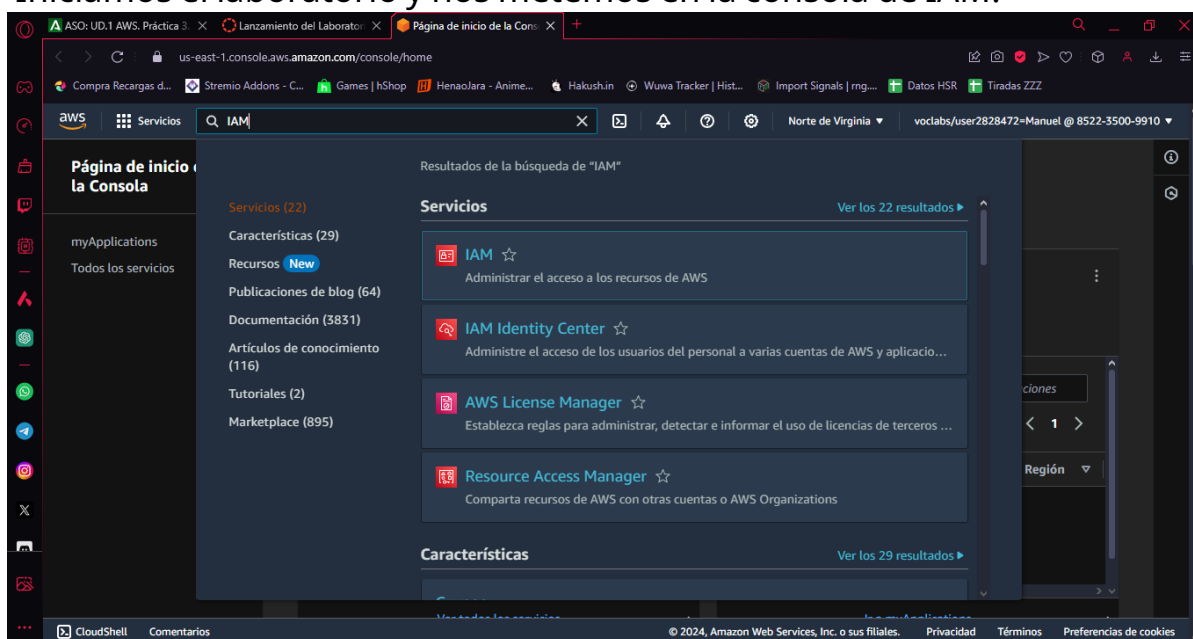
1. Introducción

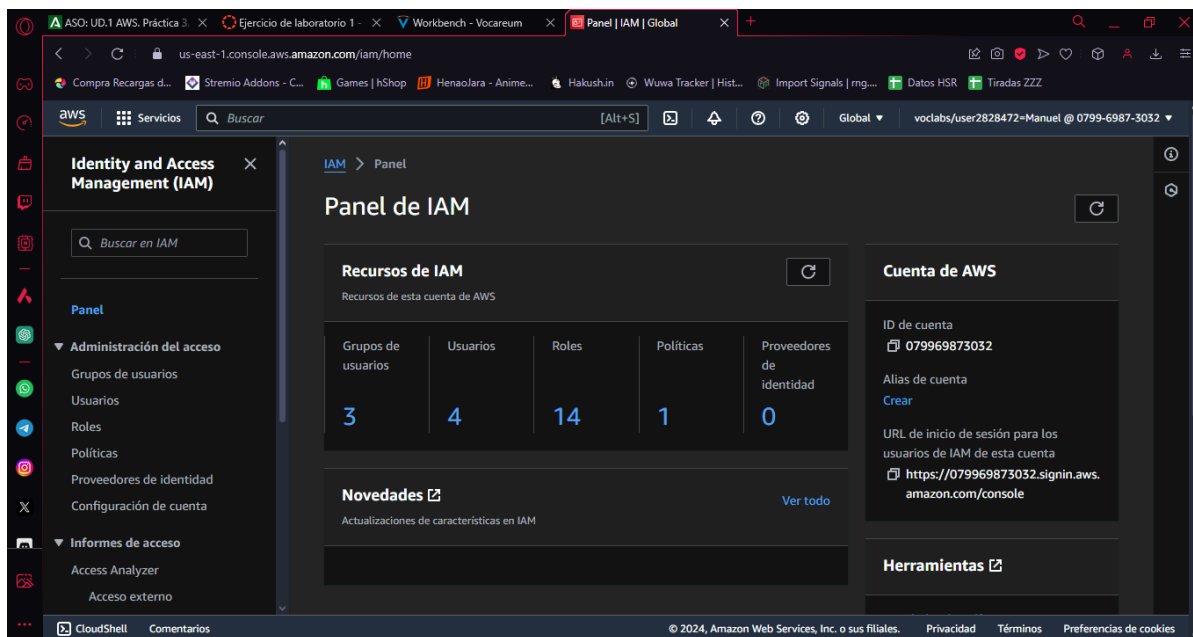
Para acceder a la consola de admon de AWS con un usuario de IAM, el usuario debe proporcionar el ID de cuenta de 12 dígitos o el alias de cuenta correspondiente. Con MFA, los usuarios y los sistemas deben proporcionar un token de MFA (además de las credenciales de inicio de sesión habituales) para poder obtener acceso a los servicios y recursos de AWS.

Esta practica es el laboratorio num.1 mod.4 del curso Cloud Foundation. Arranca el laboratorio correspondiente.

Las políticas administradas son aquellas diseñadas con anterioridad (creadas por sus administradores o por AWS) que se pueden asociar a grupos y a usuarios de IAM. Cuando la política se actualiza, los cambios se implementan inmediatamente en todos los usuarios y los grupos que tiene asociados.

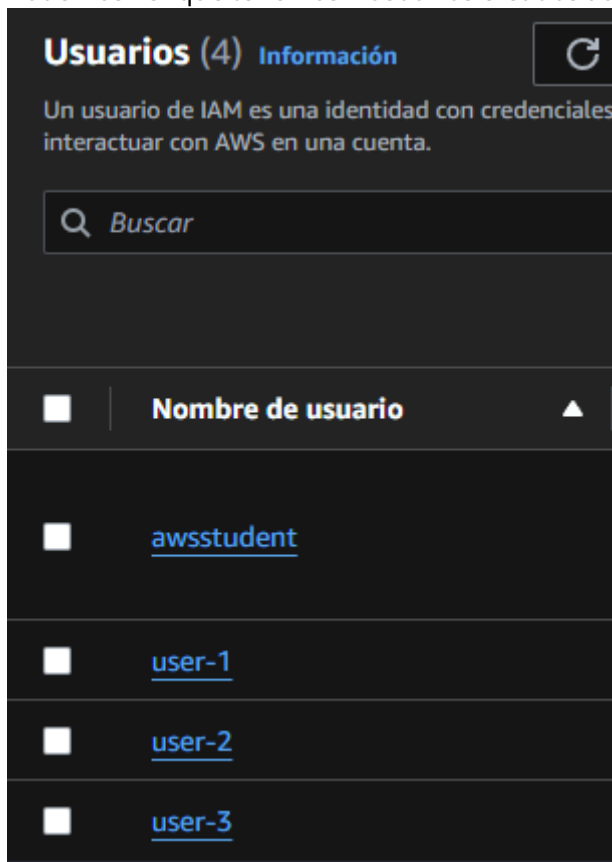
Iniciamos el laboratorio y nos metemos en la consola de IAM.





2. Explorar los usuarios y los grupos de IAM

Podemos ver que tenemos 4 usuarios creados automáticamente. Entraremos en el user-1.



Aquí podemos ver que no tiene ningún permiso otorgado. Ni pertenece a un grupo.

En Credenciales de seguridad, vemos que se le ha asignado una contraseña de la consola.

IAM

...

user-1

Nunca

Crear clave de acceso

Permisos

Grupos


Etiquetas (1)

Credenciales de seguridad

Inicio de sesión en la consola

Administrar el acceso a la consola


Enlace de inicio de sesión en la consola

 <https://079969873032.signin.aws.amazon.com/console>

Contraseña de la consola

Actualizado hace 10 minutos (2024-09-29 19:54 GMT+2)

Último inicio de sesión en la consola

 Nunca

► Límite de permisos (no establecido)


Eliminar

Agregar el usuario a los grupos

Un grupo de usuarios es un conjunto de usuarios de IAM. Los grupos se utilizan para especificar permisos que se aplican a un conjunto de usuarios. Un usuario puede ser miembro de hasta 10 grupos a la vez.

Nombre del grupo

▲

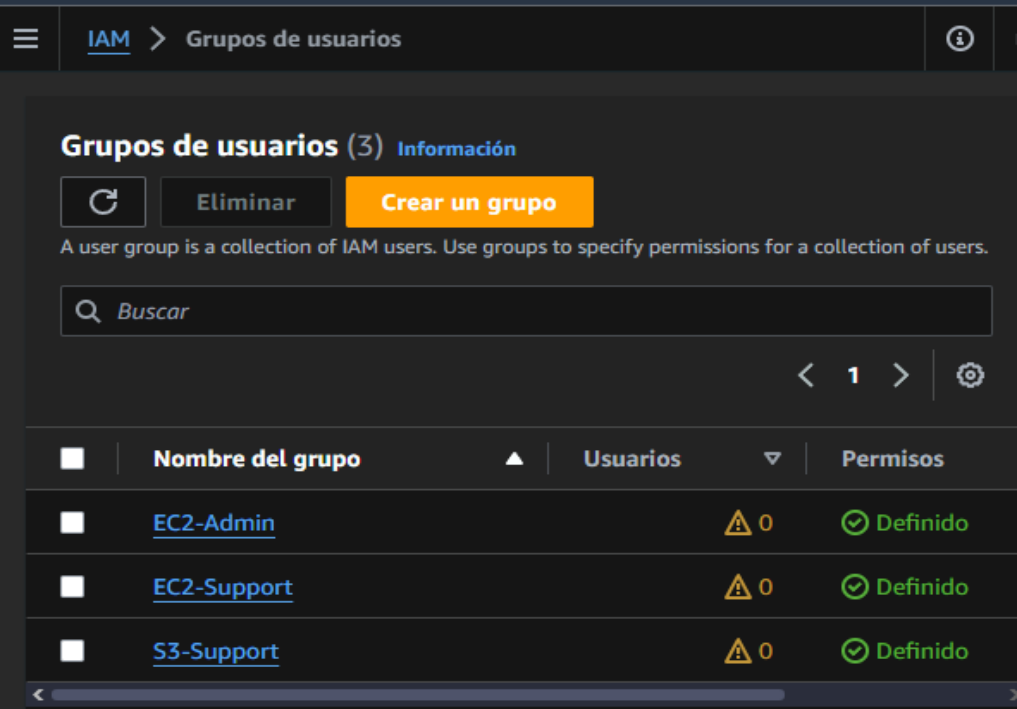
Políticas adjuntas 

▼

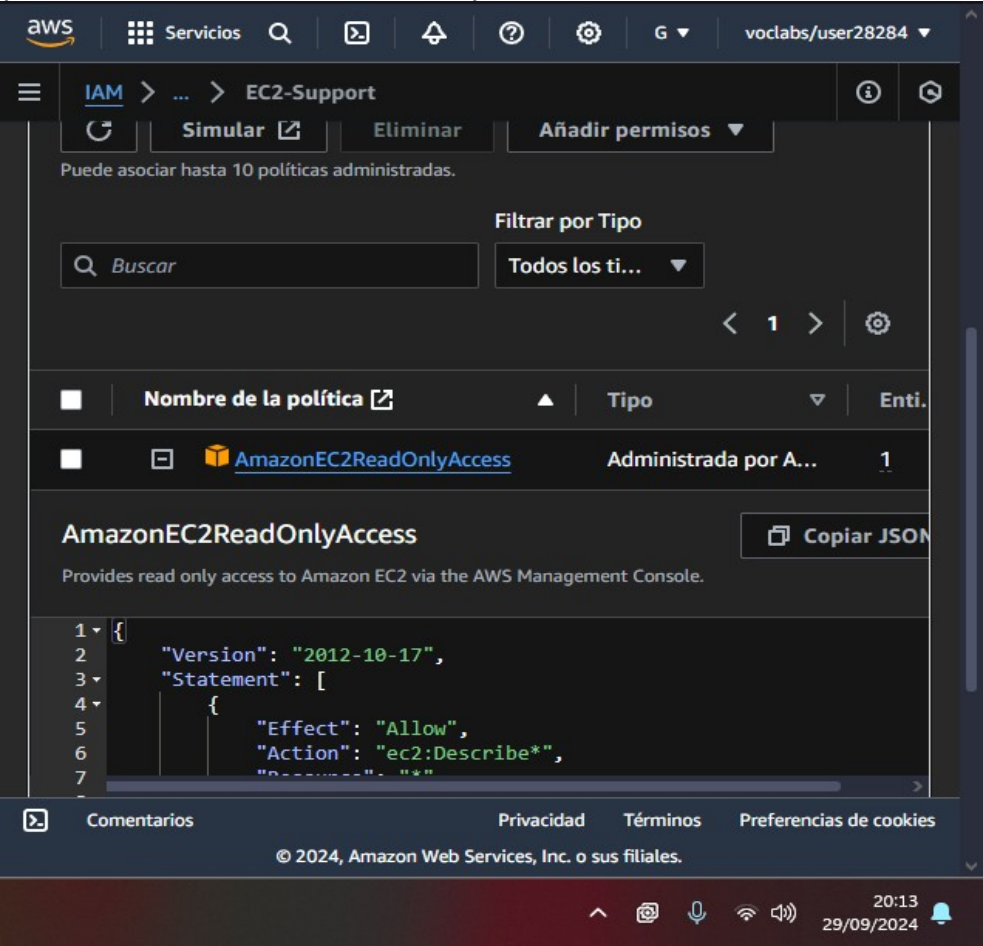
Sin recursos

Este usuario no pertenece a ningún grupo.

Ahora, entramos en grupos de usuarios y vemos que se han creado tres grupos. Entraremos en el grupo EC2-Support



Ahora entramos en Permisos, y observamos que unicamente hay una política prediseñada por AWS, y modificarla o actualizarla implica cambiar todos los usuarios y grupos en los que está activa. Si pulsamos en el + a la izquierda de la política, podremos ver los detalles de la política.

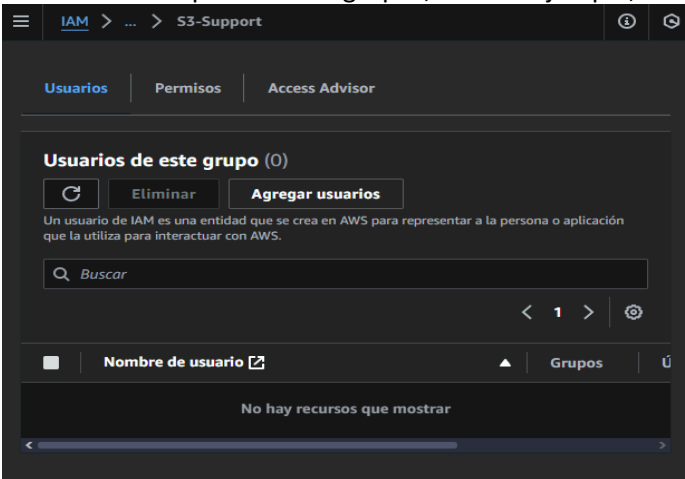


En el grupo S3-Support, tambien hay una unica politica, pero el grupo EC2-Admin es distinto, ya que la política que tiene no es administrada, como las otras, sino que esta es insertada, es decir, que solo se le asigna a un usuario/grupo, por lo que sirven para situaciones aisladas.

3. Añadir los usuarios a sus grupos:

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 Amazon EC2 instances

Ahora, entramos a los grupos de usuarios, y añadimos al usuario requerido de la siguiente manera: Metete en cualquiera de los grupos, en este ejemplo, entraré en S3-Support.

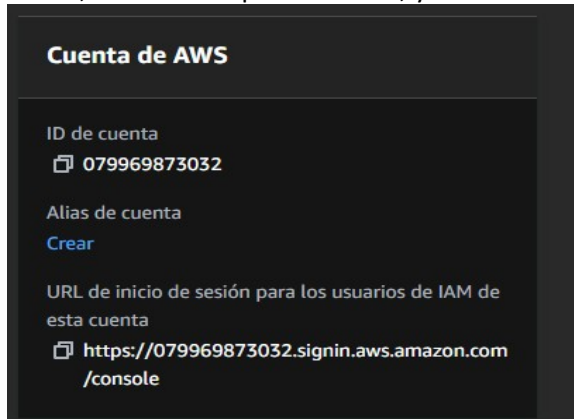


En la ventana que nos aparece, le damos el tick al usuario que queremos meter al grupo, en este caso es user-1. Ahora, repetimos este simple proceso con los otros usuarios. Aqui vemos que cada grupo tiene un usuario asignado.

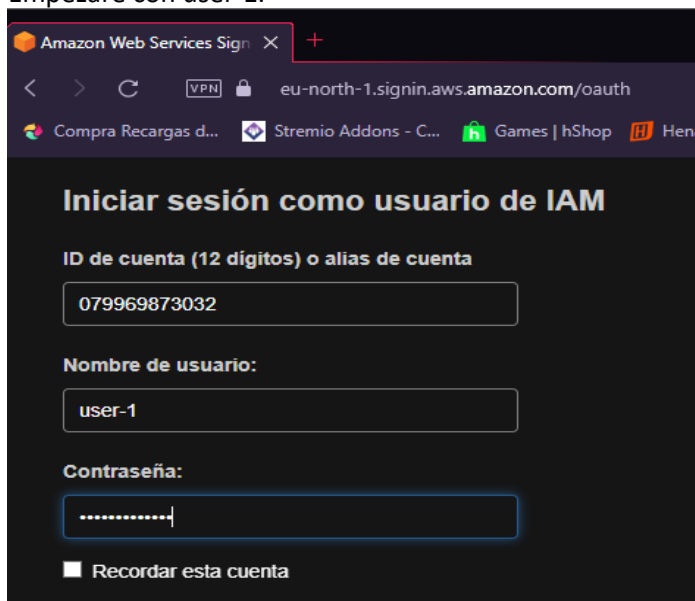
<input type="checkbox"/>	Nombre del grupo	Usuarios
<input type="checkbox"/>	EC2-Admin	1
<input type="checkbox"/>	EC2-Support	1
<input type="checkbox"/>	S3-Support	1

4. Probar los permisos asignados a cada usuario

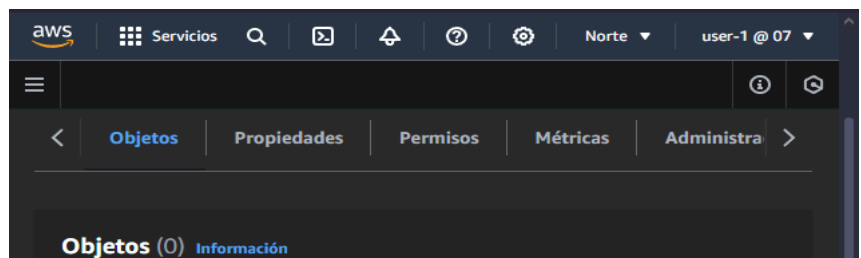
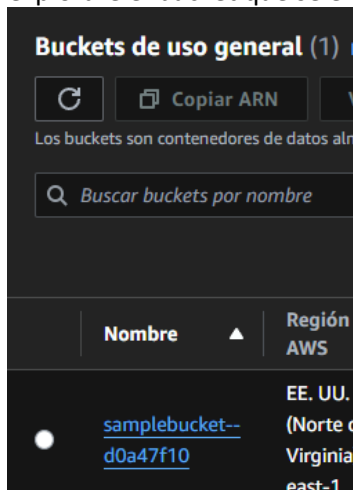
Ahora, volvemos al panel de IAM, y en la derecha podemos observar que hay una URL.



Ahora, con ese enlace, abriré una ventana de incógnito en el navegador, e iniciaré sesión con los usuarios Empezaré con user-1.

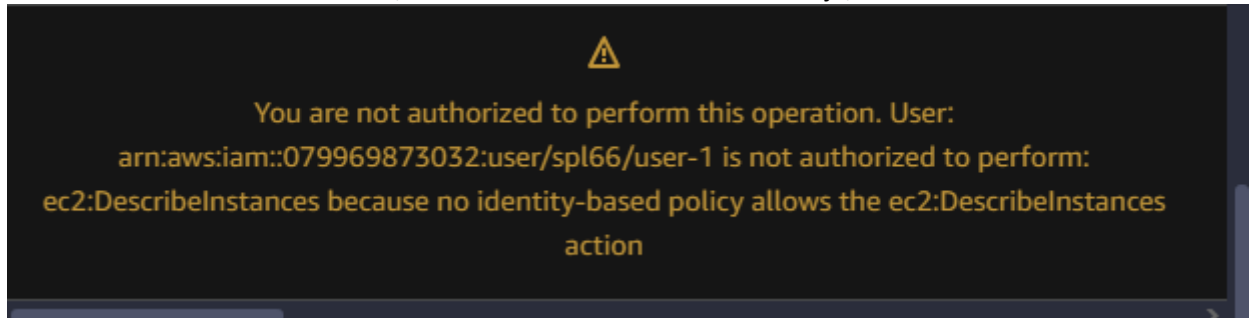


Las credenciales son user-1 como nombre de usuario y Lab-Password1. Una vez dentro, entraré a S3 y exploraré el bucket que se encuentra allí. Está vacío, ya que solo es un ejemplo.



Ahora, intentaremos acceder a EC2 con el user-1.

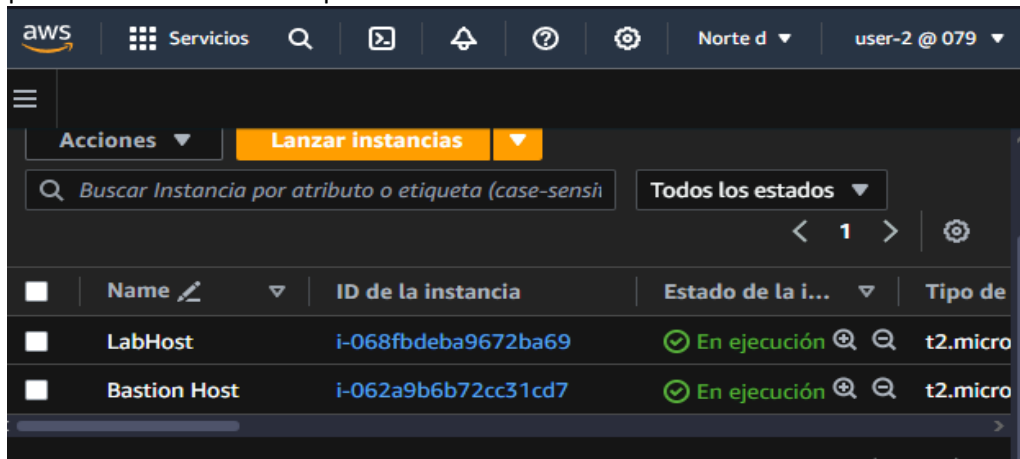
Cuando entramos a las instancias, nos encontraremos con este mensaje,



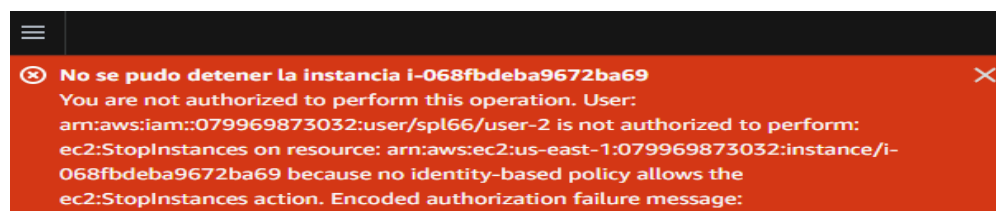
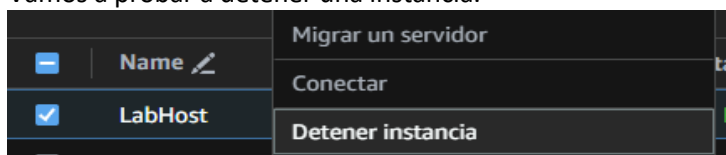
Ahora, comprobemos que podemos hacer con el user-2, así que cerramos sesión con user-1 e iniciamos con user-2. Las credenciales son las mismas que con user-1, solo que cambiando el 1 del final por un 2.

A screenshot of the AWS IAM login page. The title is "Iniciar sesión como usuario de IAM". It has three input fields: "ID de cuenta (12 dígitos) o alias de cuenta" with the value "079969873032", "Nombre de usuario:" with the value "user-2", and "Contraseña:" with masked dots. There is a checkbox labeled "Recordar esta cuenta".

Ahora, entramos a EC2, y vemos que en las instancias, si podemos ver sin problemas lo que hay, aunque no podemos hacer nada más que verlas con este usuario.

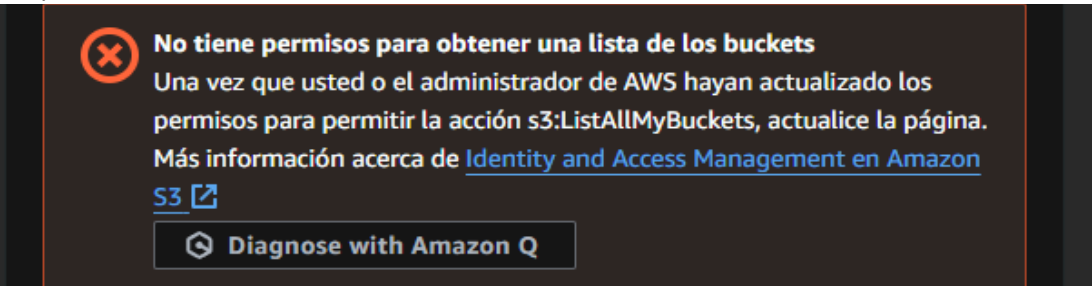


Vamos a probar a detener una instancia.

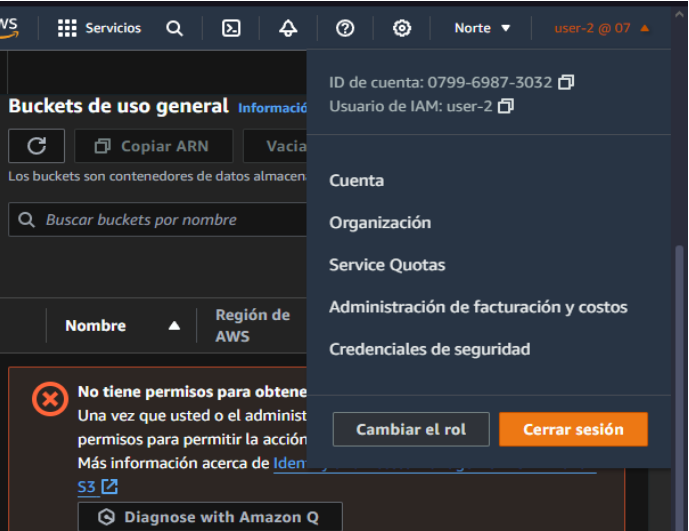


No contamos con permisos para detener la instancia. Ahora vamos a entrar en S3 con este usuario.

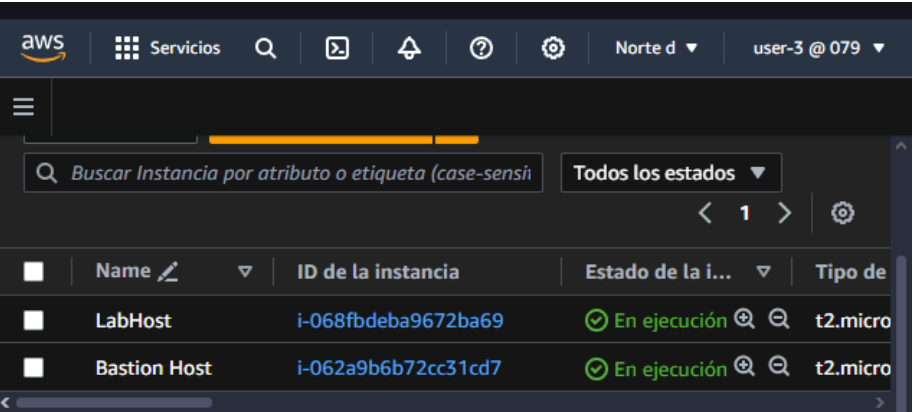
No podemos ver nada.



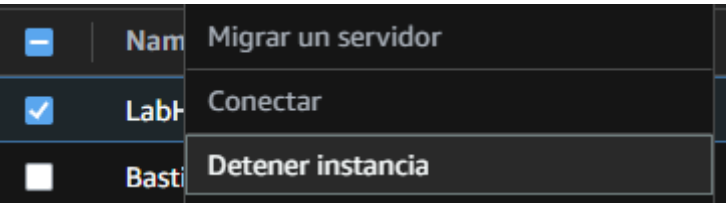
Cerraremos sesión, y ahora probamos con el user-3. Las credenciales cambian de igual manera.



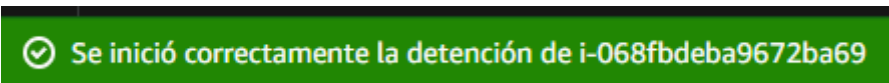
Estamos con user-3, y podemos ver sin problemas las instancias.



Vamos a detener la instancia



Podemos ejecutar la operación



Con esto, hemos finalizado la práctica.