Laboratorio del módulo 7: Introducción a IAM

Información general sobre el laboratorio

En este laboratorio, explorarás los usuarios, los grupos y las políticas del servicio AWS Identity and Access Management (IAM).

Duración

El tiempo estimado para completar este laboratorio es de **40 minutos**.

Acceso a la consola de administración de AWS

1. Para comenzar la sesión de laboratorio, selecciona **Start Lab** (Iniciar laboratorio) en la esquina superior derecha de la página.
    - Comienza la sesión del laboratorio.
    - En la esquina superior derecha de esta página aparece un temporizador que muestra el tiempo que queda de la sesión.

      Sugerencia: Para actualizar la duración de la sesión en cualquier momento, vuelve a seleccionar **Start Lab** (Iniciar laboratorio) antes de que el temporizador llegue a 0:00.
2. Antes de continuar, espera hasta que el entorno de laboratorio esté listo. El entorno está listo cuando aparecen los detalles del laboratorio en el lado derecho de la página y el icono del círculo junto al enlace de **AWS** en la esquina superior izquierda pasa a ser verde.
3. Para volver a estas instrucciones, selecciona el enlace **Readme** (Léeme) en la esquina superior derecha.
4. Para conectarte a la consola de administración de AWS, selecciona el enlace de **AWS** en la esquina superior izquierda, encima de la ventana del terminal.

Se abre una nueva pestaña del navegador que te conecta a la consola de administración de AWS.

Sugerencia: Si no se abre una pestaña nueva del navegador, generalmente aparece un banner o un icono en la parte superior de este, el cual indica que el navegador no permite que se abran ventanas emergentes en el sitio. Elige el banner o el icono y, a continuación, selecciona **Permitir elementos emergentes**.

Nota: Vas a utilizar la consola en el entorno de laboratorio, por lo que no incurrirás en ningún gasto real. Sin embargo, en el mundo real, cuando se utiliza una cuenta personal o de empresa para acceder a la consola, los usuarios incurren en gastos por el uso de servicios específicos de AWS.

Tarea 1. Explorar usuarios y grupos

En esta tarea, explorarás los usuarios y los grupos que ya se han creado para ti en IAM.

4. En primer lugar, toma nota de la región en la que te encuentras; por ejemplo, **N. Virginia**. La región se muestra en la esquina superior derecha de la página de la consola.

   Es posible que necesites esta información más adelante en el laboratorio.

5. Selecciona el menú **Servicios**, localiza los servicios de **Seguridad, identidad y conformidad** y selecciona **IAM**.

6. En el panel de navegación de la izquierda, elige **Usuarios**.

   Ya Se han creado los siguientes usuarios de IAM:

   - user-1
   - user-2
   - user-3

7. Selecciona el nombre **user-1**.

   - Se abrirá una página de resumen de user-1. Aparecerá la pestaña **Permisos**.
   - Observa que user-1 no tiene permisos.

8. Selecciona la pestaña **Grupos**.

   Observa que user-1 tampoco es miembro de ningún grupo.

9. Selecciona la pestaña **Credenciales de seguridad**.

   Observa que a user-1 se le asignado una **Contraseña de la consola**. Esto permite al usuario acceder a la consola de administración de AWS.

10. En el panel de navegación de la izquierda, selecciona **Grupos de usuarios**.

    Ya se han creado los siguientes grupos:

    - EC2-Admin
    - EC2-Support
    - S3-Support

11. Selecciona el nombre del grupo **EC2-Support**.

    Esto le lleva a la página de resumen del grupo **EC2-Support**.

12. Selecciona la pestaña **Permisos**.

    Este grupo está asociado a una política administrada denominada **AmazonEC2ReadOnlyAccess**. Las políticas administradas son políticas prediseñadas (que crearon AWS o sus administradores) que se pueden adjuntar a grupos o usuarios de IAM. Cuando la política se actualiza, los cambios se implementan inmediatamente en los usuarios y grupos adjuntos a ella.

13. En **Nombre de la política**, elige el enlace de la política **AmazonEC2ReadOnlyAccess**.

14. Selecciona la pestaña **{} JSON**.

    - Una política define qué acciones están permitidas o denegadas para recursos concretos de AWS. Esta política concede permiso para *Enumerar* y *Describir* (ver) información sobre Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch y Amazon EC2 Auto Scaling. Esta capacidad para ver recursos, pero no modificarlos, resulta idónea para asignar un rol de soporte.
    - Los enunciados de una política de IAM tienen la siguiente estructura básica:
      - **Efecto** nos indica si *Permitir* o *Denegar* los permisos.
      - **Acción** especifica las llamadas a la API que se pueden realizar desde un servicio de AWS (por ejemplo, *cloudwatch:ListMetrics*).

- **Recurso** define el alcance de las entidades cubiertas por la regla de la política (por ejemplo, un bucket de Amazon Simple Storage Service [Amazon S3] o una instancia de Amazon EC2 específicos; un asterisco [*] significa *cualquier recurso*).

15. En el panel de navegación de la izquierda, selecciona **Grupos de usuarios**.
16. Elige el nombre del grupo **S3-Support**.
17. Selecciona la pestaña **Permisos**.

    El grupo S3-Support tiene la política **AmazonS3ReadOnlyAccess** asociada.

18. En **Nombre de la política**, elige el enlace de la política **AmazonS3ReadOnlyAccess**.
19. Selecciona la pestaña **{} JSON**.

    Esta política tiene permisos para *obtener* y *enumerar todos* los recursos en Amazon S3.

20. En el panel de navegación de la izquierda, selecciona **Grupos de usuarios**.
21. Elige el nombre del grupo **EC2-Admin**.
22. Selecciona la pestaña **Permisos**.

    Este grupo es diferente de los otros dos. En lugar de una política administrada, el grupo tiene una *política insertada*, que es una política asignada a un solo usuario o grupo. Las políticas insertadas, generalmente, se usan para asignar permisos en situaciones específicas.

23. En **Nombre de la política**, elige el nombre de la política **EC2-Admin-Policy**.
24. Selecciona la pestaña **JSON**.

    Esta política concede permiso para *Describir* información acerca de instancias de Amazon EC2 y también la capacidad de *Iniciar* y *Detener* instancias.

25. En la parte inferior de la pantalla, selecciona **Cancelar** para cerrar la política.

Escenario empresarial

Durante el resto del laboratorio, trabajaremos con estos usuarios y grupos para habilitar los permisos compatibles con la siguiente situación empresarial.

Tu empresa utiliza los servicios de AWS cada vez más, y utiliza muchas instancias de Amazon EC2 y buckets de Amazon S3. Quieres dar acceso al nuevo personal según su función laboral, como se indica en la siguiente tabla:

Usuario	En el grupo	Permisos
user-1	S3-Support	Acceso de solo lectura a Amazon S3
user-2	EC2-Support	Acceso de solo lectura a Amazon EC2
user-3	EC2-Admin	Ver, iniciar y detener instancias de Amazon EC2

Tarea 2. Añadir usuarios a grupos

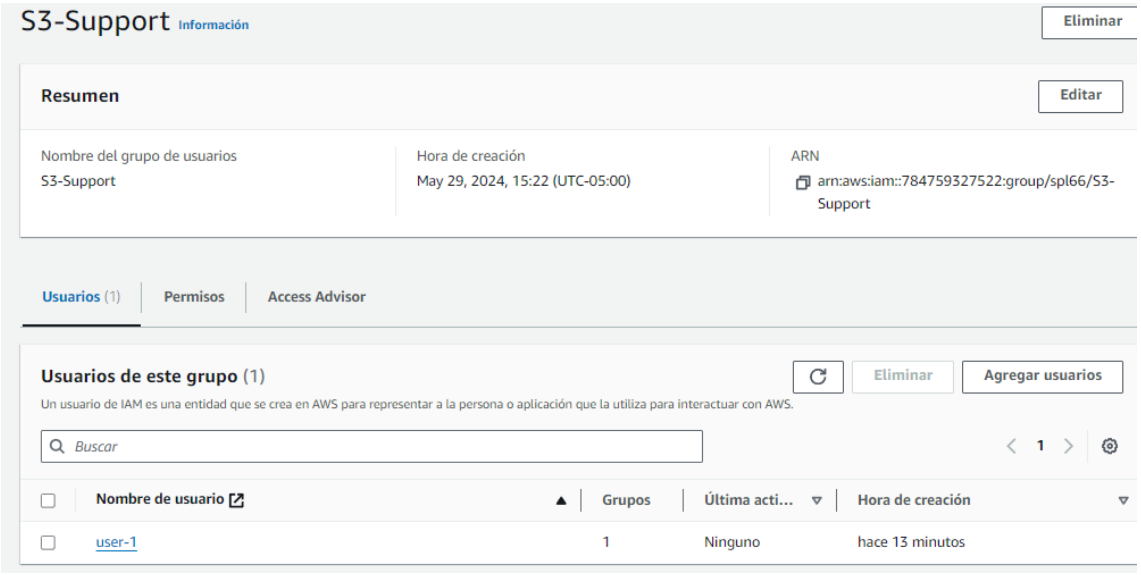
Recientemente, has contratado al *user-1* para un rol en el que presta soporte a Amazon S3. Añadirás a este usuario al grupo *S3-Support* para que herede los permisos necesarios mediante la política *AmazonS3ReadOnlyAccess* asociada.

Haz caso omiso de los errores de tipo "no autorizado" que aparezcan durante esta tarea. Se deben a que la cuenta del laboratorio tiene permisos limitados, pero no afectarán a tu capacidad para completar el laboratorio.

Añadir a user-1 al grupo S3-Support

26. En el panel de navegación izquierdo, selecciona **Grupos de usuarios**.
27. Elige el nombre del grupo **S3-Support**.
28. En la pestaña **Usuarios**, elige **Añadir usuarios**.
29. Selecciona **user-1** y después **Añadir usuarios**.

    En la pestaña **Usuarios**, observa que *user-1* se ha añadido al grupo.

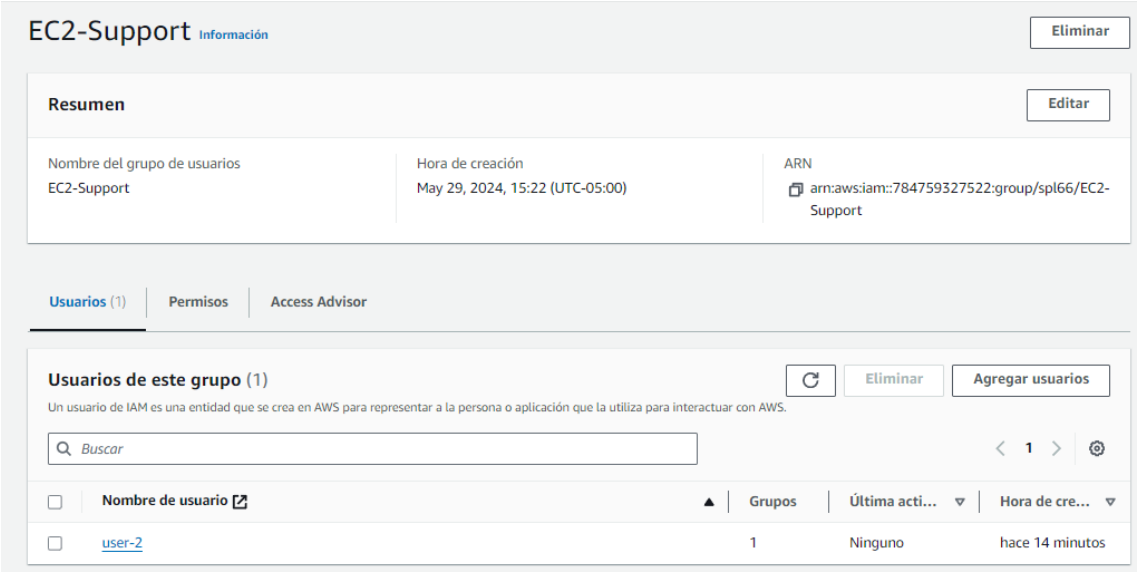


Añadir a user-2 al grupo EC2-Support

Has contratado a *user-2* para un rol en el que presta soporte a Amazon EC2. Lo añadirás al grupo *EC2-Support* para que pueda heredar los permisos necesarios mediante la política *AmazonEC2ReadOnlyAccess* adjunta.

30. Utiliza lo aprendido de los pasos anteriores para añadir a *user-2* al grupo *EC2-Support*.

    Ahora, *user-2* debería formar parte del grupo *EC2-Support*.



Añadir a user-3 al grupo EC2-Admin

Has contratado a *user-3* como administrador de Amazon EC2 para que administre las instancias de EC2. Lo añadirás al grupo *EC2-Admin* para que

pueda heredar los permisos necesarios mediante la política *EC2-Admin-Policy* adjunta.

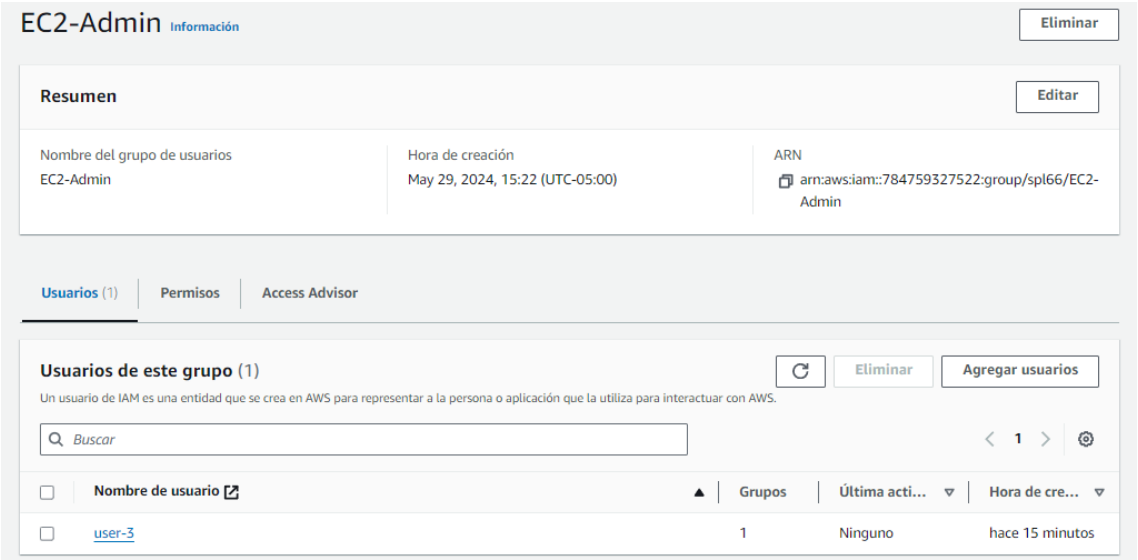
31. Utiliza lo aprendido de los pasos anteriores para añadir a *user-3* al grupo *EC2-Admin*.

    Ahora, *user-3* debería formar parte del grupo *EC2-Admin*.

32. En el panel de navegación de la izquierda, selecciona **Grupos de usuarios**.

    Cada grupo debe tener un **1** en la columna **Usuarios**. Indica el número de usuarios de cada grupo.

    Si no ves un **1** en la columna **Usuarios** de un grupo, repasa los pasos anteriores para asegurarte de que cada usuario se ha asignado a un grupo, como se muestra en la tabla de la sección **Situación empresarial**.



Tarea 3. Iniciar sesión y probar usuarios

En esta tarea, probarás los permisos de cada usuario de IAM en la consola.

Obtener la URL de inicio de sesión de la consola

33. En el panel de navegación de la izquierda, selecciona **Panel**.

    Observa la sección **URL de inicio de sesión para los usuarios de IAM** de esta cuenta en la parte superior de la página. La URL de inicio

de sesión tiene un aspecto similar al siguiente: **https://123456789012.signin.aws.amazon.com/console**

Este enlace se puede utilizar para iniciar sesión en la cuenta de AWS que utilizas actualmente.

34. Copia el enlace de inicio de sesión en un editor de texto.

Probar permisos de user-1

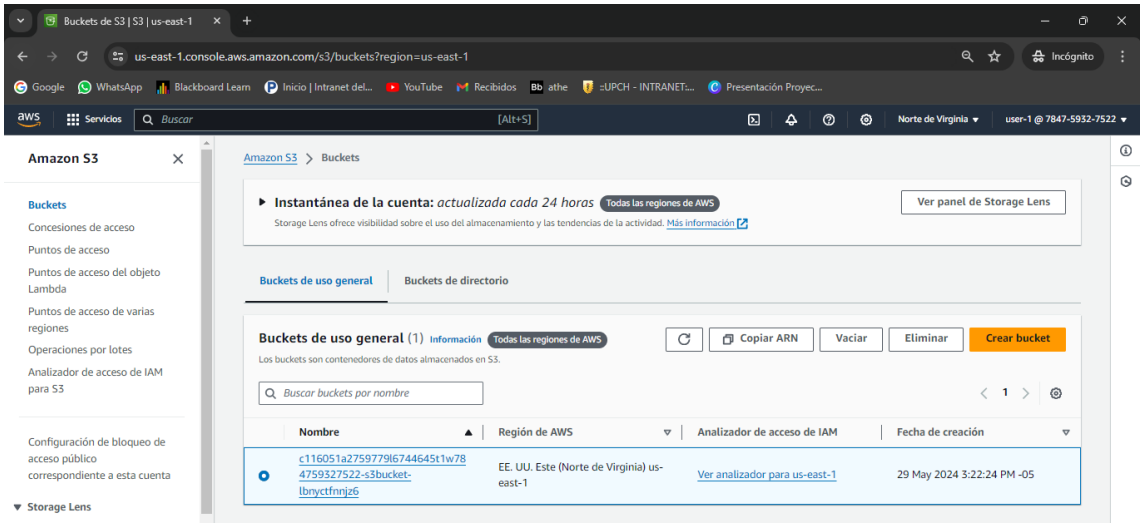
35. Abre una ventana privada o de incógnito en el navegador.
36. Pega el enlace de inicio de sesión en el navegador privado y pulsa INTRO.

    Ahora iniciarás sesión como *user-1*, que ha sido contratado como personal de apoyo de almacenamiento de Amazon S3.

37. Inicia sesión con las siguientes credenciales:
    - **Nombre de usuario de IAM:** `user-1`
    - **Contraseña:** `Lab-Password1`
38. Selecciona el menú **Servicios** y luego **S3**.
39. Elige el nombre de uno de los buckets y explora el contenido.

    Dado que este usuario forma parte del grupo *S3-Support* de IAM, tiene permiso para ver una lista de los buckets de Amazon S3 y su contenido.

    Ahora, verifica si el usuario tiene acceso a Amazon EC2.

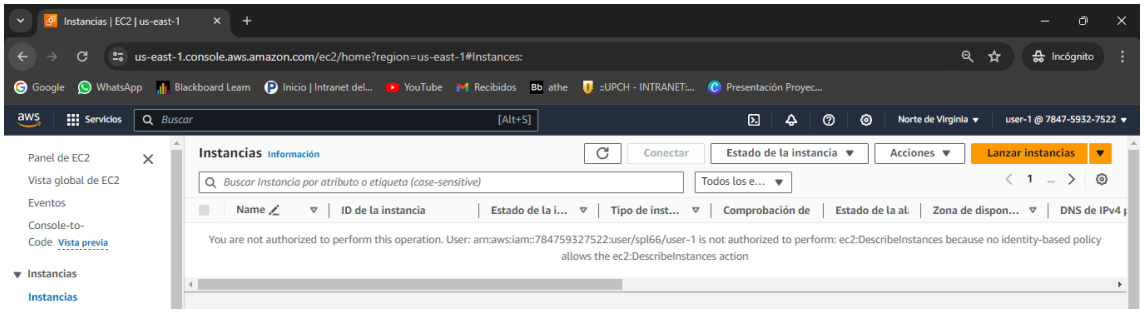


40. Selecciona el menú **Servicios** y después **EC2**.

41. En el panel de navegación izquierdo, selecciona **Instancias**.

    No aparece ninguna instancia. En cambio, aparece un mensaje que dice que *no estás autorizado a realizar esta operación*. A este usuario no se le ha asignado ningún permiso de uso de Amazon EC2.

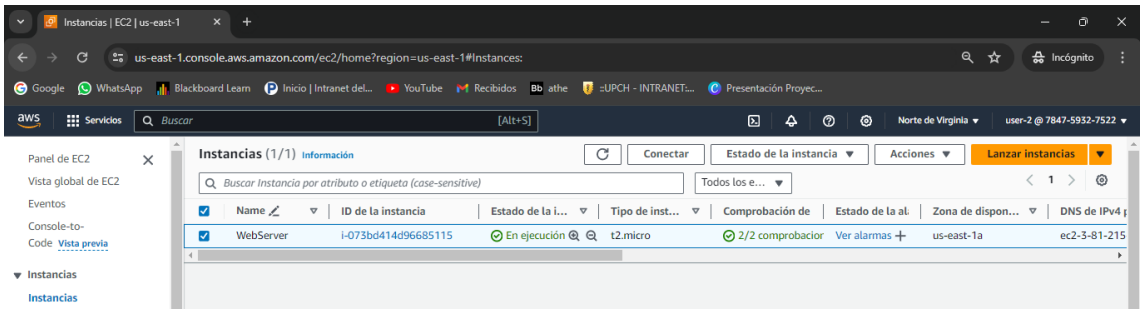
    Ahora, iniciarás sesión como *user-2*, al que se ha contratado como personal de soporte de Amazon EC2.



42. En primer lugar, cierra la sesión de *user-1* en la consola:
    - En la esquina superior derecha de la página, selecciona **user-1**.
    - Selecciona **Cerrar sesión**.

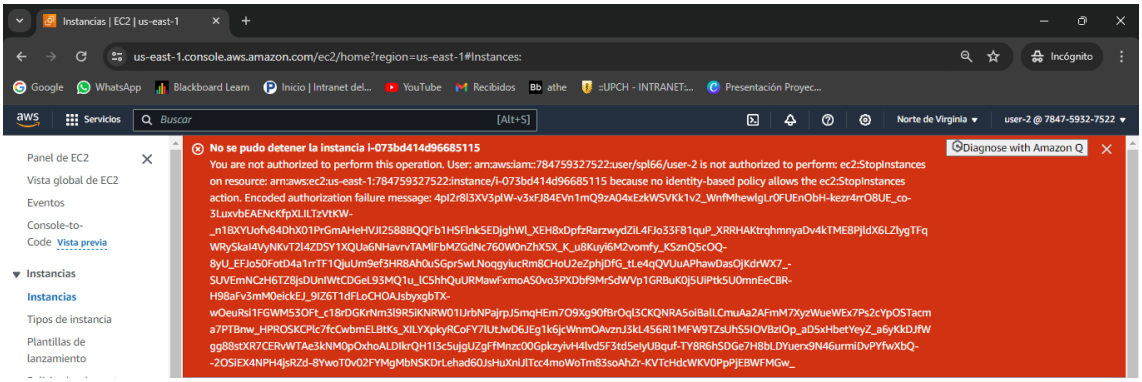
Probar permisos de user-2

43. Vuelve a pegar el enlace de inicio de sesión en el navegador privado y pulsa INTRO.
44. Inicia sesión con las siguientes credenciales:
    - **Nombre de usuario de IAM:** `user-2`
    - **Contraseña:** `Lab-Password2`
45. Selecciona el menú **Servicios** y después **EC2**.
46. En el panel de navegación de la izquierda, selecciona **Instancias**.
    - Ahora puedes ver una instancia de EC2. Sin embargo, no puedes realizar ningún cambio en los recursos de Amazon EC2 porque tienes permisos de solo lectura.
    - Si no ves una instancia de EC2, es posible que la región sea incorrecta. En la esquina superior derecha de la página, elige el nombre de la región y, a continuación, elige la región en la que te encontrabas al principio del laboratorio (por ejemplo, **N. Virginia**).



47. Selecciona la instancia de EC2.

48. Selecciona el menú **Estado de la instancia** y, a continuación, selecciona **Detener instancia**.



49. Para confirmar que quieres detener la instancia, selecciona **Detener**.

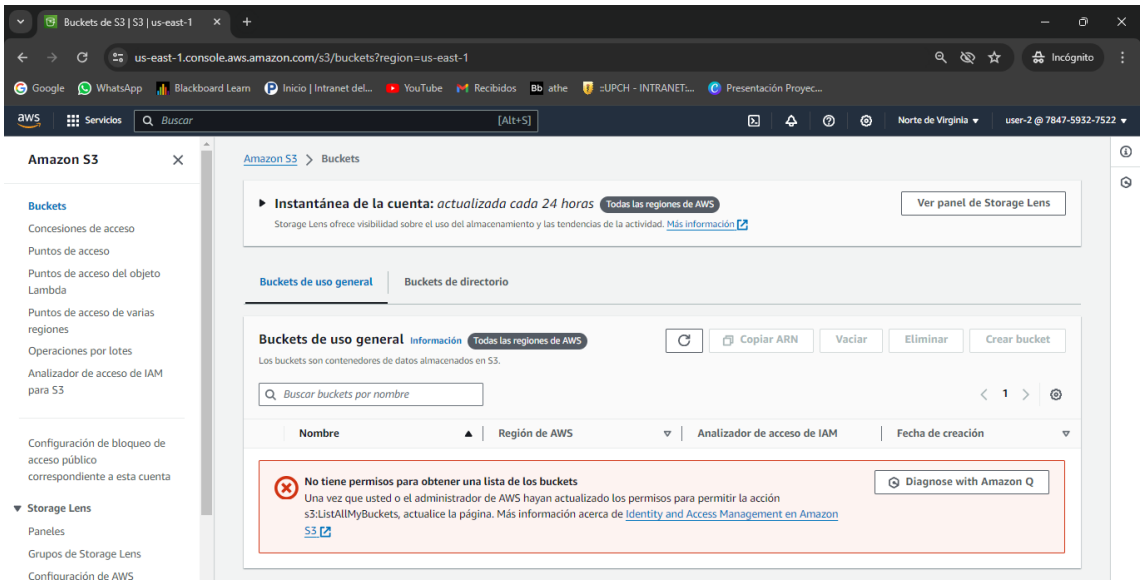
    Aparece un mensaje de error que indica que *no estás autorizado a realizar esta operación*. Esto demuestra que la política solo te permite ver información sin realizar cambios.

    A continuación, verifica si *user-2* puede acceder a Amazon S3.

50. Selecciona el menú **Servicios** y luego **S3**.

    Un mensaje de error indica que *no tienes permisos para enumerar buckets* porque *user-2* no tiene permiso para usar Amazon S3.

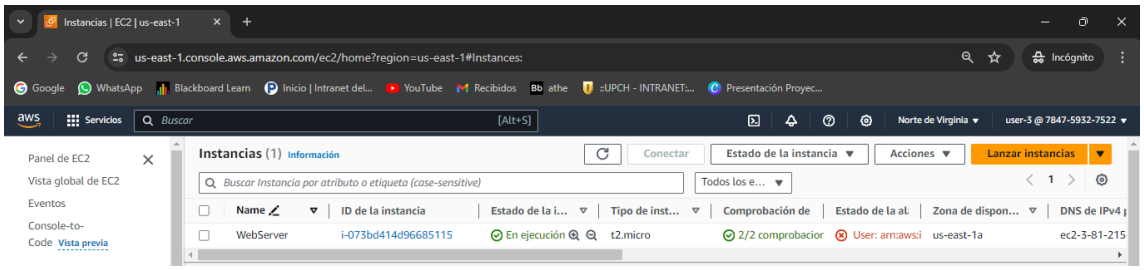
    Ahora, iniciarás sesión como *user-3*, al que se ha contratado como administrador de Amazon EC2.



51. En primer lugar, cierra la sesión de *user-2* en la consola:
    - En la esquina superior derecha de la página, selecciona **user-2**.
    - Selecciona **Cerrar sesión**.

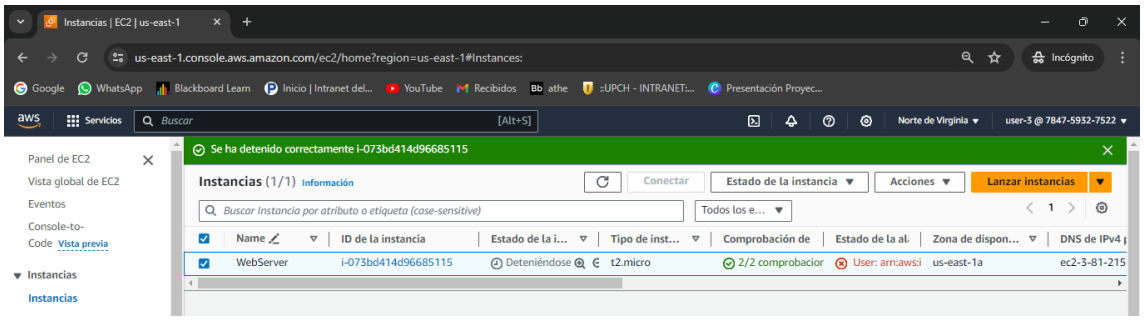
Probar permisos de user-3

52. Vuelve a pegar el enlace de inicio de sesión en el navegador privado y pulsa INTRO.
53. Inicia sesión con las siguientes credenciales:
    - **Nombre de usuario de IAM:** `user-3`
    - **Contraseña:** `Lab-Password3`
54. Selecciona el menú **Servicios** y después **EC2**.
55. En el panel de navegación de la izquierda, selecciona **Instancias**.
    - Se muestra una instancia de EC2. Como administrador de Amazon EC2, este usuario debe tener permisos para *Detener* la instancia de EC2.
    - Si no ves una instancia de EC2, es posible que la región sea incorrecta. En la esquina superior derecha de la página, elige el nombre de la región y, a continuación, elige la región en la que te encontrabas al principio del laboratorio (por ejemplo, **N. Virginia**).



56. Selecciona la instancia de EC2.
57. Selecciona el menú **Estado de la instancia** y, a continuación, selecciona **Detener instancia**.
58. Para confirmar que quieres detener la instancia, selecciona **Detener**.

    Esta vez, la acción se realiza correctamente porque *user-3* tiene permiso para detener instancias de EC2. El **Estado de la instancia** cambia a *Deteniéndose* y empieza a apagarse.



59. Cierra la ventana del navegador privado.

Laboratorio completado

¡Enhorabuena! Has completado el laboratorio.

60. Cierra la sesión de la consola de administración de AWS.
    - En la esquina superior derecha de la página, elige tu nombre de usuario. Tu nombre de usuario comienza por **voclabs/user**.
    - Selecciona **Cerrar sesión**.
61. Selecciona **Finalizar laboratorio** en la parte superior de esta página y, a continuación, selecciona Sí para confirmar que quieres dar por concluido el laboratorio.