PRÁCTICAS DE AWS

SESIÓN 1: SEGURIDAD EN LA NUBE (IAM)

Roberto R. Expósito (roberto.rey.exposito@udc.es)
Guillermo L. Taboada (guillermo.lopez.taboada@udc.es)

Informática coma Servizo
Mestrado Universitario en Enxeñaría Informática - UDC

AWS Identity and Access Management (IAM)

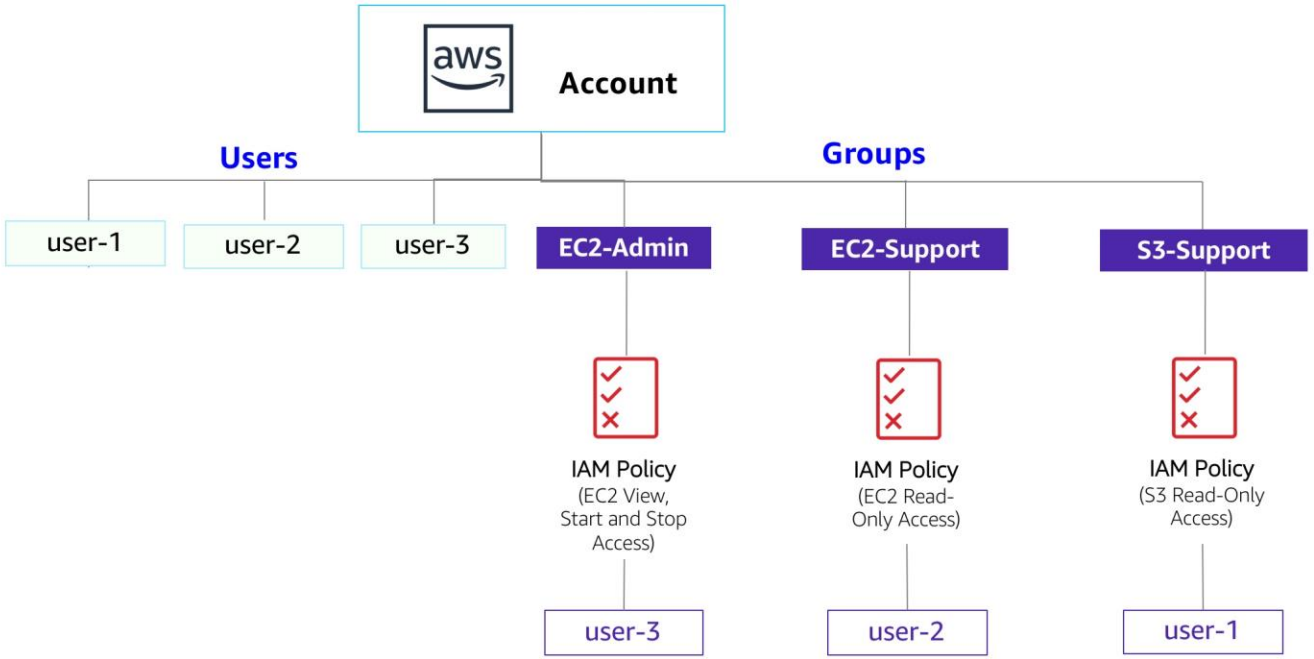
- **AWS IAM** es un servicio que permite a los clientes de AWS **administrar** de forma **centralizada** los usuarios, grupos y sus permisos
  - **Administrar usuarios de IAM y su acceso:** permite crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos de autenticación multifactor)
    - Los permisos permiten 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 es una identidad de AWS con políticas de permisos que establecen qué puede hacer o no la identidad en AWS
    - En lugar de estar asociada únicamente a una persona, el objetivo es que **pueda asignarse** un rol a cualquier persona que lo necesite
  - **Administrar usuarios federados y sus permisos:** puede habilitar la **identidad federada** a fin de permitir que los usuarios existentes en una empresa puedan acceder a la consola de administración de AWS, invocar las APIs de AWS y acceder a los recursos sin necesidad de crear un usuario de IAM para cada identidad

OBJETIVOS

- Completar en AWS Academy el **Laboratorio 1 (Introducción a AWS IAM)** del Módulo 4 (Seguridad en la nube)
  - La duración estimada para completar el laboratorio es de **~25 minutos**
- Prerrequisitos recomendados del módulo 4:
  - Visualizar la Sección 2 (AWS IAM) (~12 minutos)
- Los **objetivos** específicos de este laboratorio son:
  - Analizar los **usuarios y los grupos de IAM** creados previamente
  - Inspeccionar las **políticas de IAM,** según se apliquen a los grupos creados previamente
  - De acuerdo a una **situación real,** agregar usuarios a los grupos con capacidades específicas habilitadas
  - Ubicar y usar la dirección **URL de inicio de sesión de IAM**
  - **Probar** los efectos de las políticas en el acceso a los servicios

TAREAS

- Tarea 1: analizar los usuarios y los grupos
- Tarea 2: agregar usuarios a los grupos
- Tarea 3: iniciar sesión y probar los usuarios



JUSTIFICACIÓN DE LA PRÁCTICA

- **Documento PDF** que incluya **TODAS** las capturas de pantalla mostradas en las siguientes transparencias donde se vea la información solicitada

 **IMPORTANTE** 

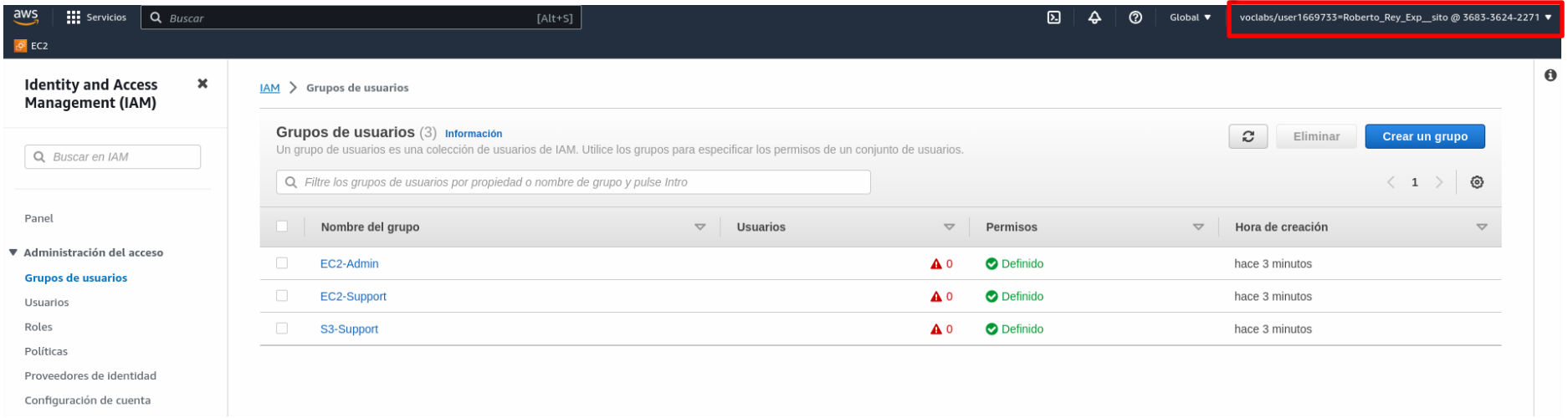
¿Cómo completar los ejercicios de laboratorio en AWS Academy?

Recuerda que hay un **límite de crédito** para cada ejercicio de laboratorio en AWS Academy. Si alcanzas el límite, tu **cuenta temporal es deshabilitada**, y **NO** podrás iniciar el laboratorio de nuevo. Este límite es como mínimo dos veces la cantidad requerida para completar los ejercicios, **pero debes usarlo de forma responsable.** Recuerda **finalizar el laboratorio** cuando termines el ejercicio o no vayas a seguir trabajando en Academy

- **ENTREGA** de la práctica a través de Moodle
- **NO RECORTES** las capturas, **DEBE verse TODA la información** que sea relevante para comprobar el trabajo realizado
- Si no se siguen estas normas **LA PRÁCTICA NO SE CONSIDERARÁ "APTA"**

CAPTURAS (I)

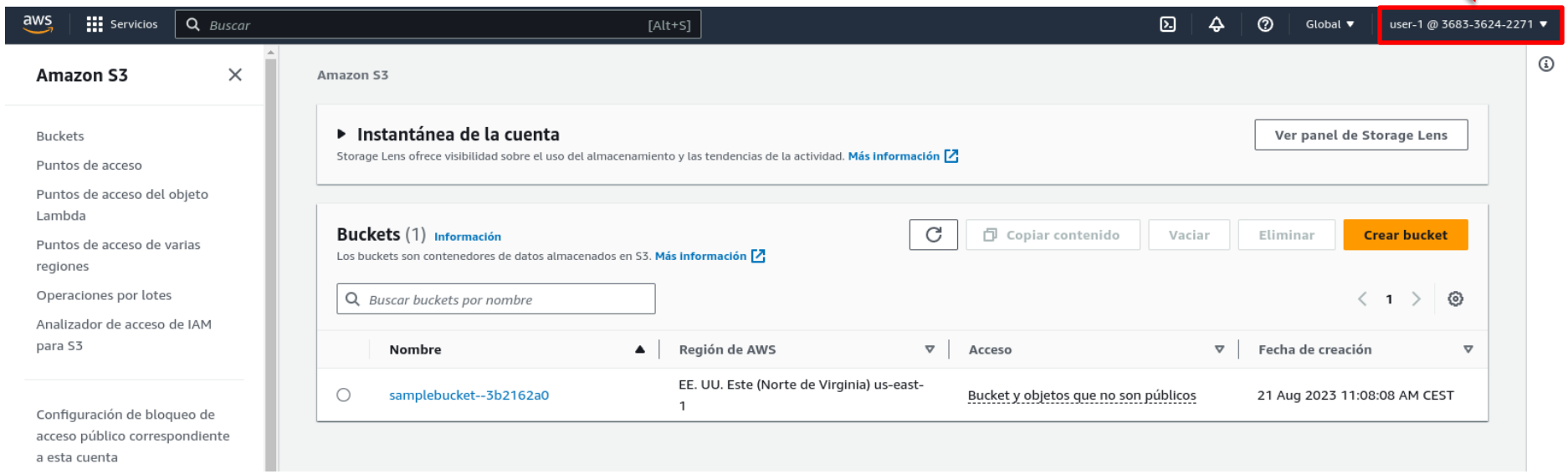
En **TODAS** las capturas de pantalla de la **consola de AWS** debes mostrar la **misma información** que ves en los ejemplos que se incluyen en este enunciado. Especialmente importante es que se vea **SIEMPRE el ID y el nombre de usuario de tu cuenta,** ya que te identifica unívocamente



I) Grupos existentes en IAM sin usuarios asignados inicialmente (Tarea 1)

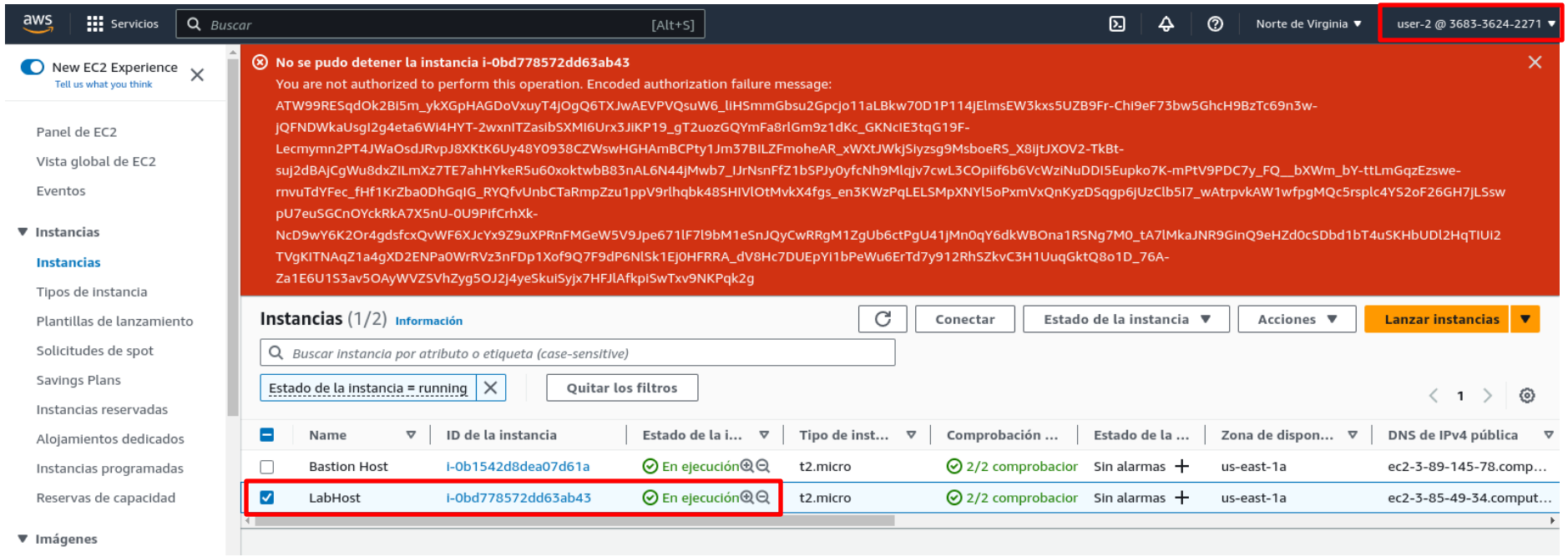
CAPTURAS (II)

DEBE haber correspondencia con el **ID** mostrado en la captura previa



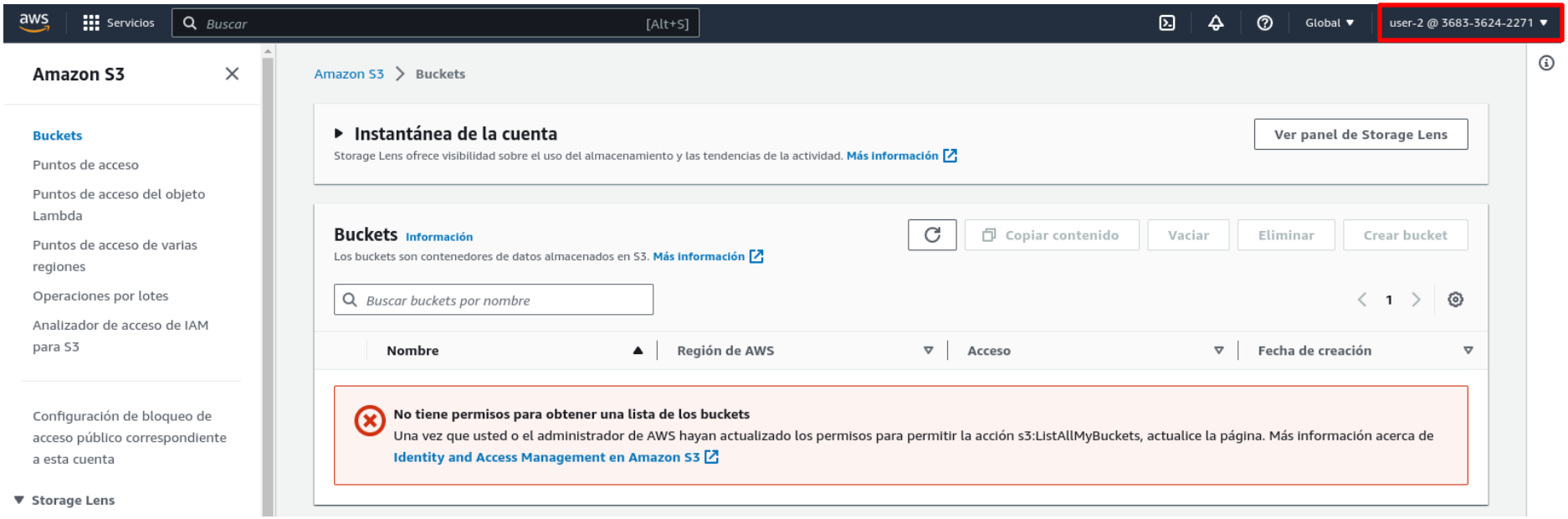
II) Visualización del bucket en S3 logueado como user-1 (Tarea 3)

CAPTURAS (III)



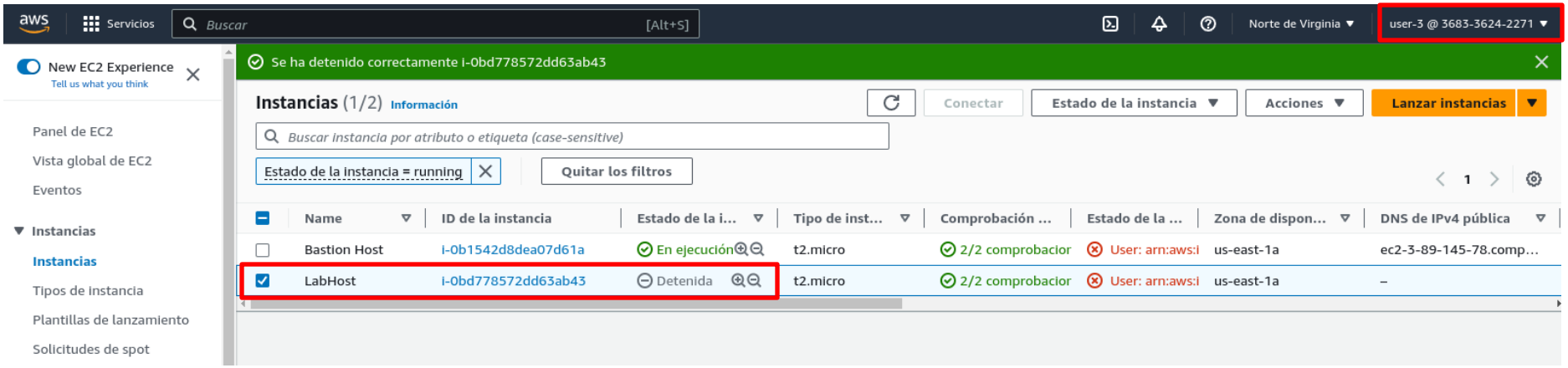
III) user-2 no puede detener la instancia EC2 (Tarea 3)

CAPTURAS (IV)



IV) user-2 no puede ver el bucket S3 (Tarea 3)

CAPTURAS (y V)



V) user-3 puede detener la instancia EC2 (Tarea 3)