

# PRÁCTICAS DE AWS

## *SESIÓN 1: SEGURIDAD EN LA NUBE (IAM)*

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



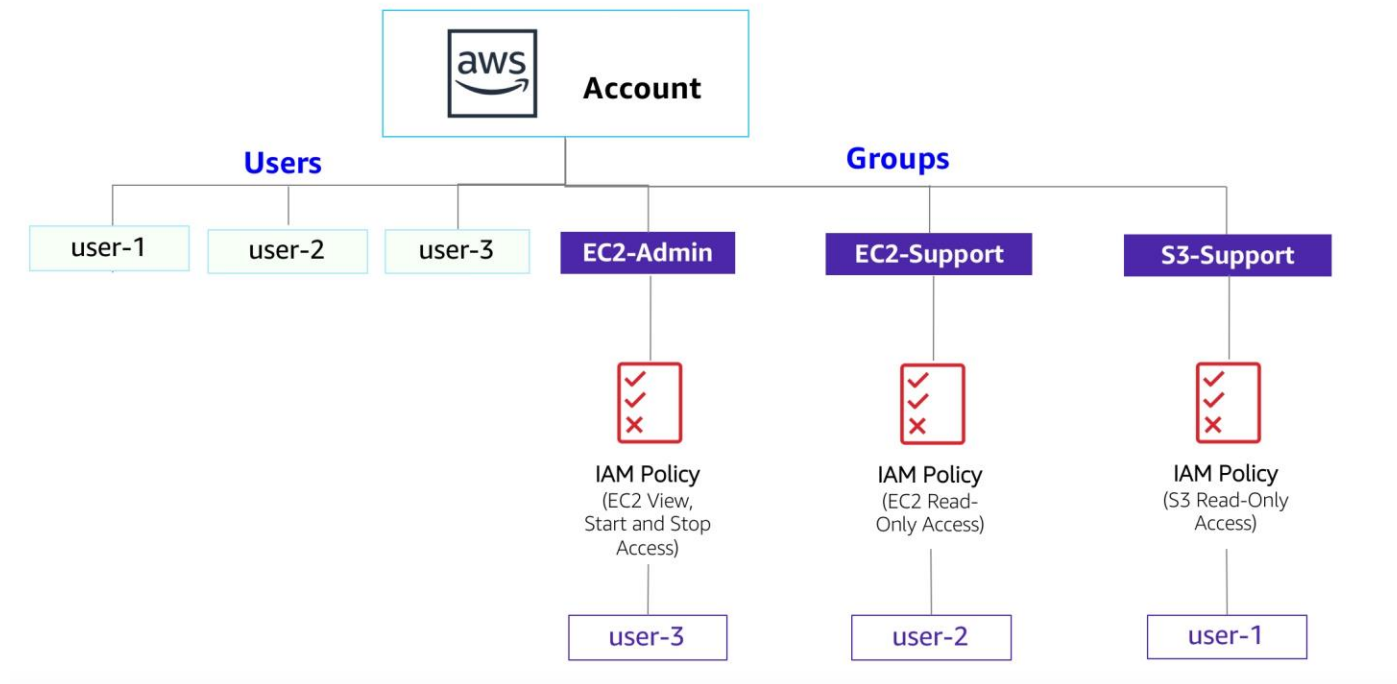
- **AWS IAM** es un servicio que permite a los clientes de AWS **administrar** de forma **centralizada** los usuarios, grupos y sus permisos
  - ▣ **Administrar usuarios de IAM y su acceso:** permite crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos 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



- ❑ 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



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





- **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"**



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

aws Servicios [Alt+S] Global voclabs/user1669733=Roberto\_Rey\_Exp\_\_sito @ 3683-3624-2271

Identity and Access Management (IAM)

Buscar en IAM

Panel

Administración del acceso

Grupos de usuarios

Usuarios

Roles

Políticas

Proveedores de Identidad

Configuración de cuenta

IAM > Grupos de usuarios

Grupos de usuarios (3) Información

Un grupo de usuarios es una colección de usuarios de IAM. Utilice los grupos para especificar los permisos de un conjunto de usuarios.

Filtre los grupos de usuarios por propiedad o nombre de grupo y pulse Intro

<input type="checkbox"/>	Nombre del grupo	Usuarios	Permisos	Hora de creación
<input type="checkbox"/>	EC2-Admin	0	Definido	hace 3 minutos
<input type="checkbox"/>	EC2-Support	0	Definido	hace 3 minutos
<input type="checkbox"/>	S3-Support	0	Definido	hace 3 minutos

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



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

aws Servicios [Alt+S] Global user-1 @ 3683-3624-2271

## Amazon S3

- Buckets
- Puntos de acceso
- Puntos de acceso del objeto Lambda
- Puntos de acceso de varias regiones
- Operaciones por lotes
- Analizador de acceso de IAM para S3
- Configuración de bloqueo de acceso público correspondiente a esta cuenta

### Instantánea de la cuenta

Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de la actividad. [Más información](#)

[Ver panel de Storage Lens](#)

### Buckets (1) Información

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

[Buscar buckets por nombre](#)

[Copiar contenido](#) [Vaciar](#) [Eliminar](#) [Crear bucket](#)

Nombre	Región de AWS	Acceso	Fecha de creación
<a href="#">samplebucket--3b2162a0</a>	EE. UU. Este (Norte de Virginia) us-east-1	<a href="#">Bucket y objetos que no son públicos</a>	21 Aug 2023 11:08:08 AM CEST

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



aws Servicios [Alt+S] Norte de Virginia user-2 @ 3683-3624-2271

**No se pudo detener la instancia i-0bd778572dd63ab43**

You are not authorized to perform this operation. Encoded authorization failure message:  
ATW99RESqdOk2BI5m\_ykXGpHAGDoVxuyT4jOgQ6TXJwAEVPVQsuW6\_lIH5mmGbsu2Gpcjo11aLBkw7OD1P114jElmsEW3kxs5UZB9Fr-Chi9eF73bw5GhcH9BzTc69n3w-JQFNDWkaUsgl2g4eta6Wi4HYT-2wxnITZasibSxMI6Urx3JIKP19\_gT2uozGQYmFa8rlGm9z1dKc\_GKNclE3tqG19F-Lecnymn2PT4JWaoSdJRvpJ8XKtK6Uy48Y0938CZWswHGHAmbCpty1Jm37BILZFmoheAR\_xWXTJWkjSlyzsg9MsboeRS\_X8jltXOV2-Tkbt-suj2dBAJcGwu8dxZILmXz7TE7ahHYkeR5u60xoktwbB83nAL6N44jMwb7\_JrNsnFfZ1bSPJy0yfcNh9Mlqv7cwL3COpilf6b6VcWziNuDDI5Eupko7K-mPtV9PDC7y\_FQ\_\_bXWm\_by-ttLmGqzEzsw-rnvuTdYFec\_fhF1KrZba0DhGqIG\_RYQfvUnbCTaRmpZzu1ppV9rlhqbK48SHIVIOtMvkX4fgs\_en3KWzPqLELSMpXNYI5oPxmVxQnKyzDSqgp6JuzClb5I7\_wAtrpvkAW1wfpqMQc4rsplc4YS2oF26GH7JL5swpU7euSGCnOYckRkA7X5nU-0U9PfcRhXk-NcD9wY6K2Or4gdsfcxQvWF6XJcYx9Z9uXPRnFMGeW5V9Jpe671f7l9bM1eSnJQyCwRRgM1ZgUb6ctPgU41JmN0qY6dkWBOa1RSNg7M0\_tA7lMkaJNR9GinQ9eHZd0cSDbd1bT4uSKHbUDI2HqTIUI2TVgKITNAqZ1a4gXD2ENPa0WrvRVz3nFDp1Xof9Q7F9dP6NlSk1EjOHFRRA\_dv8Hc7DUEpY11bPeWu6ErTd7y912Rh5ZkvC3H1UuqGktQ8o1D\_76A-Za1E6U1S3av5OAyWVZSVhZyg5OJ2j4yeSkuiSyjx7HFJIAfkpiSwTxv9NKPqk2g

**Instancias (1/2) Información**

Buscar instancia por atributo o etiqueta (case-sensitive)

Estado de la instancia = running Quitar los filtros

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zona de dispon...	DNS de IPv4 pública
<input type="checkbox"/>	Bastion Host	i-0b1542d8dea07d61a	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-1a	ec2-3-89-145-78.comp...
<input checked="" type="checkbox"/>	LabHost	i-0bd778572dd63ab43	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-1a	ec2-3-85-49-34.comput...

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





aws Servicios [Alt+S] Global user-2 @ 3683-3624-2271

Amazon S3 Buckets

**Instantánea de la cuenta**  
Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de la actividad. [Más Información](#) [Ver panel de Storage Lens](#)

**Buckets** [Información](#)  
Los buckets son contenedores de datos almacenados en S3. [Más Información](#)

Buscar buckets por nombre

Nombre ▲ Región de AWS ▼ Acceso ▼ Fecha de creación ▼

**No tiene permisos para obtener una lista de los buckets**  
Una vez que usted o el administrador de AWS hayan actualizado los permisos para permitir la acción s3:ListAllMyBuckets, actualice la página. [Más información acerca de Identity and Access Management en Amazon S3](#)

Ver panel de Storage Lens

Copiar contenido Vaciar Eliminar Crear bucket

Storage Lens

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



aws Servicios [Al+S] Norte de Virginia user-3 @ 3683-3624-2271

Se ha detenido correctamente i-0bd778572dd63ab43

Instancias (1/2) Información

Buscar instancia por atributo o etiqueta (case-sensitive)

Estado de la instancia = running Quitar los filtros

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zona de dispon...	DNS de IPv4 pública
<input type="checkbox"/>	Bastion Host	i-0b1542d8dea07d61a	En ejecución	t2.micro	2/2 comprobaci...	User: arn:aws:i	us-east-1a	ec2-3-89-145-78.comp...
<input checked="" type="checkbox"/>	LabHost	i-0bd778572dd63ab43	Detenida	t2.micro	2/2 comprobaci...	User: arn:aws:i	us-east-1a	-

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