

Cloud Foundation - Lab - 1 (Introduction to AWS IAM)

Resumen del Lab: Introducción a AWS IAM

Objetivo del lab

Este laboratorio introduce los conceptos básicos de AWS Identity and Access Management (IAM) , una herramienta para gestionar usuarios, roles y permisos en AWS. Aprenderás cómo:

- Crear y administrar usuarios y grupos .
- Asignar políticas de permisos a usuarios y grupos.
- Probar cómo las políticas afectan el acceso a servicios como Amazon S3 y Amazon EC2 .

Conceptos clave

1. IAM (Identity and Access Management):
 - Permite gestionar quién puede hacer qué en tu cuenta de AWS.
 - Se basa en políticas que definen permisos específicos.
2. Políticas (Policies):
 - Son documentos JSON que especifican qué acciones están permitidas o denegadas.

Estructura básica:

```
{  
  "Effect": "Allow/Deny",  
  "Action": ["service:action"],  
  "Resource": "arn:aws:service:region:account:resource"  
}
```

Ejemplo:

- Una política puede permitir (Allow) listar buckets de S3 (s3:ListBucket) pero denegar (Deny) eliminarlos.
3. Grupos (Groups):
 - Colecciones de usuarios que comparten permisos.
 - Ejemplo: Un grupo llamado S3-Support puede tener permisos de solo lectura para S3.
 4. Roles (Roles):
 - Identidades temporales que pueden ser asumidas por usuarios, aplicaciones o servicios.
 5. Federación de usuarios:
 - Permite a usuarios externos (como empleados de una empresa) acceder a AWS sin crear cuentas IAM individuales.

Detalles relevantes en el lab

Explorar usuarios y grupos precreados

Usuarios creados previamente:

- user-1, user-2, user-3.

Grupos creados previamente:

- EC2-Admin: Permite iniciar y detener instancias EC2.
- EC2-Support: Permite solo leer información de EC2 (permisos de solo lectura).
- S3-Support: Permite solo leer información de S3.

Cómo explorar:

- En la consola de AWS, navega a IAM > Users o IAM > User Groups .
- Revisa las políticas adjuntas a cada grupo usando el botón Permissions .

Agregar usuarios a grupos

Asignación de roles según el escenario empresarial:

user-1 → Grupo S3-Support (permisos de solo lectura para S3).

user-2 → Grupo EC2-Support (permisos de solo lectura para EC2).

user-3 → Grupo EC2-Admin (permisos para iniciar/detener instancias EC2).

Pasos para agregar usuarios:

Ve a IAM > User Groups .

Selecciona el grupo correspondiente.

Haz clic en Add users y selecciona el usuario user-1.

Probar permisos de usuarios

user-1



[AmazonS3ReadOnlyAccess](#)

AWS managed

AmazonS3ReadOnlyAccess

Provides read only access to all buckets via the AWS Management Console.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "s3:Get*",  
8         "s3:List*",  
9         "s3:Describe*",  
10        "s3-object-lambda:Get*",  
11        "s3-object-lambda:List*",  
12      ],  
13      "Resource": "*"   
14    }  
15  ]  
16 }
```

Solo puede leer S3

Instantánea de la cuenta: actualizada cada 24 horas [Todas las regiones de AWS](#) [Ver panel de Storage Lens](#)

Storage Lens permite visualizar el uso del almacenamiento y las tendencias de la actividad. Las métricas no incluyen los buckets de directorio. [Más información](#)

Buckets de uso general [Información](#) [Todas las regiones de AWS](#) [Copiar ARN](#) [Vaciar](#) [Eliminar](#) [Crear bucket](#)

Los buckets son contenedores de datos almacenados en S3.

Buscar buckets por nombre

Nombre	Región de AWS	Analizador de acceso de IAM	Fecha de creación
samplebucket--ce6c7830	EE.UU. Este (Norte de Virginia) us-east-1	Ver analizador para us-east-1	21 Apr 2025 9:07:09 PM CEST

Configuración de bloqueo de

No puedo ver ec2..

Instancias [información](#) Última actualización Hace less than a minute [Conectar](#) [Estado de la instancia](#) [Acciones](#) [Lanzar instancias](#)

Buscar Instancia por atributo o etiqueta (case-sensitive) Todos los ...

Estado de la instancia = running [Quitar los filtros](#)

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la i...	Zona de dispon...	DNS de IPv...
<div><div><div></div><div>You are not authorized to perform this operation. User: arn:aws:iam::217985108518:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action</div><div>Retry</div></div></div>							

Europa (Estocolmo) ▼ | user-1 @ 2179-8510-8518 ▲

ID de cuenta
2179-8510-8518

Usuario de IAM
user-1

Cuenta

Organización

Service Quotas

Administración de facturación y costos

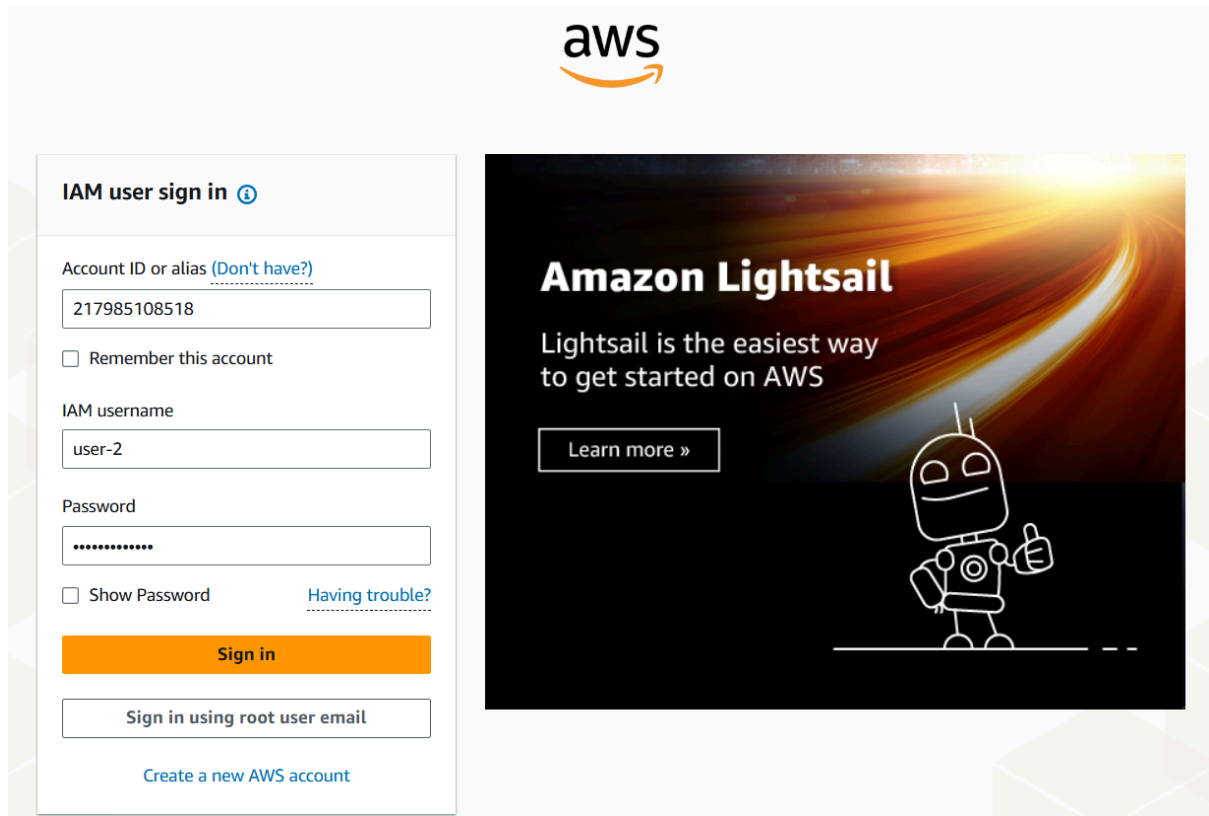
Credenciales de seguridad

Activar compatibilidad con varias sesiones

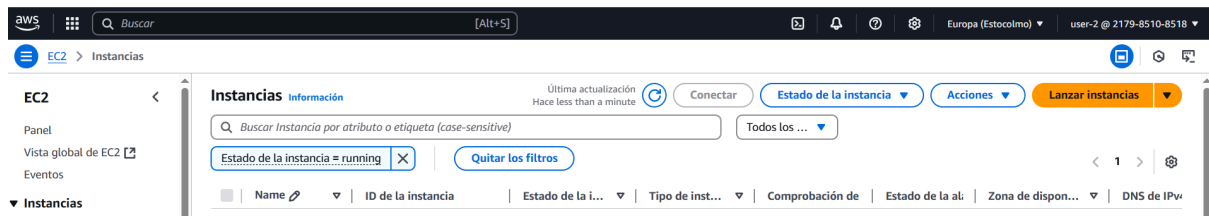
Cambiar el rol

Cerrar sesión

Cerrar sesión



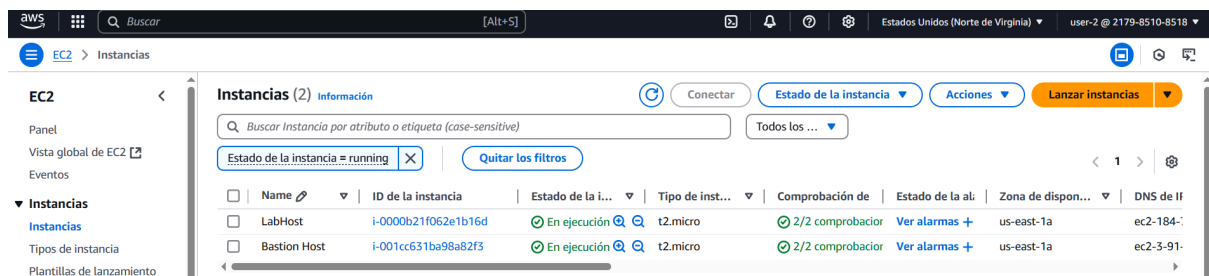
user-2





No veo nada porque estoy en la región equivocada.

Nos vamos a us-east-1

Ahora si podemos ver



 [AmazonEC2ReadOnlyAccess](#)

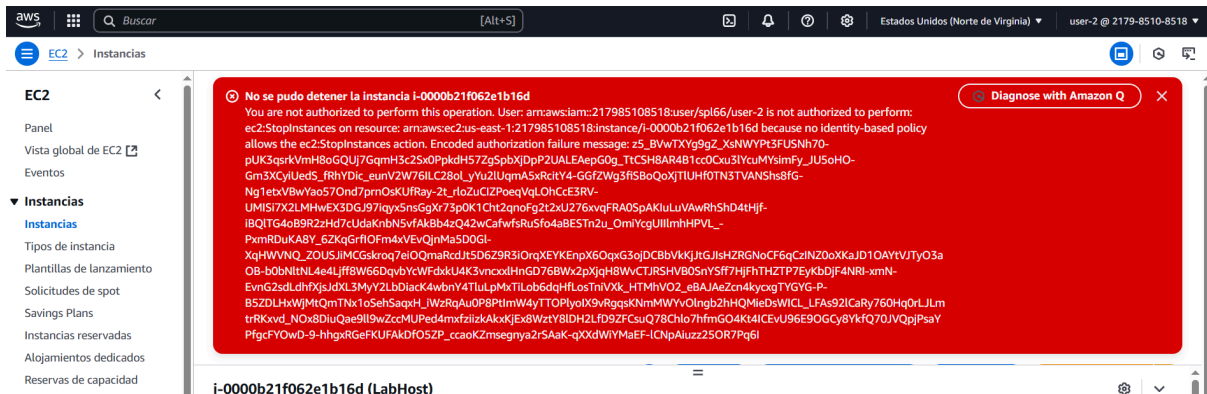
AWS managed

AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Console.

```
12 {
13     "Effect": "Allow",
14     "Action": "elasticloadbalancing:Describe*",
15     "Resource": "*"
16 },
17 {
18     "Effect": "Allow",
19     "Action": [
20         "cloudwatch:ListMetrics",
21         "cloudwatch:GetMetricStatistics",
22         "cloudwatch:Describe*"
23     ],
24     "Resource": "*"
25 },
26 {
27     "Effect": "Allow",
28     "Action": "autoscaling:Describe*",
29     "Resource": "*"
30 }
31 ]
```

Como observamos solo tiene permisos para ver y no puede hacer mas.



Ahora verificamos el s3:

The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open to 'Amazon S3' > 'Buckets'. The main content area shows the 'Buckets de uso general' tab. At the top, there's a message about the account dashboard being updated every 24 hours. Below that, there's a section for 'Buckets de uso general (0)'. A search bar is present. Below the search bar, there's a table with columns: 'Nombre', 'Región de AWS', 'Analizador de acceso de IAM', and 'Fecha de creación'. The table is currently empty. Below the table, there's a red error message: 'Error: Acceso denegado'. To the right of the error message is a button that says 'Diagnose with Amazon Q'. At the top right of the console, there's a user profile dropdown showing 'user-2 @ 2179-8510-8518'.

Y como podemos ver no tiene acceso.

The screenshot shows the AWS IAM user sign-in page. The page has the AWS logo at the top. On the left, there's a sign-in form with the following fields: 'Account ID or alias (Don't have?)' with the value '217985108518', 'Remember this account' (unchecked), 'IAM username' with the value 'user-3', and 'Password' (masked with dots). There are links for 'Having trouble?' and 'Sign in using root user email'. At the bottom, there's a link to 'Create a new AWS account'. On the right, there's an advertisement for Amazon Lightsail, featuring a robot character and the text 'Amazon Lightsail' and 'Lightsail is the easiest way to get started on AWS'. There's a 'Learn more »' button in the advertisement.

user-3

☐ Policy name

☐ [EC2-Admin-Policy](#) Customer inline

EC2-Admin-Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": [  
6         "ec2:Describe*",  
7         "ec2:StartInstances",  
8         "ec2:StopInstances"  
9       ],  
10      "Resource": [  
11        "*" ]  
12      },  
13      "Effect": "Allow"  
14    ]  
15  }  
16 }
```

El user-3 tiene permisos para ec2 para start y stop las instancias.

Puede hacerlo.

Resultados esperados

user-1: Solo puede acceder a S3.

user-2: Solo puede ver información de EC2, pero no modificarla.

user-3: Puede iniciar/detener instancias EC2.

Error → Solución

No tuve problemas.

Conclusión

- Cómo usar IAM para gestionar usuarios, grupos y permisos.
- Cómo asignar políticas predefinidas (managed policies) o personalizadas (inline policies).

- Cómo probar los efectos de las políticas en el acceso a servicios como S3 y EC2 .

Este conocimiento es fundamental para asegurar nuestra infraestructura en AWS y garantizar que cada usuario tenga solo los permisos necesarios para su rol.

Submit del lab

01:15 ▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Details ✕

Submit Submission Report Grades

Total score	40/40
TASK 2a - Added user-1 to S3-Support group	5/5
TASK 2b - Added user-2 to EC2-Support group	5/5
TASK 2c - Added user-3 to EC2-Admin group	5/5
TASK 3a - user-1 logged in	5/5
TASK 3b - user-2 logged in	5/5
TASK 3c - user-2 ec2 stop instance attempt	5/5
TASK 3d - user-3 logged in	5/5
TASK 3e - user-3 EC2 stop instance attempt	5/5