

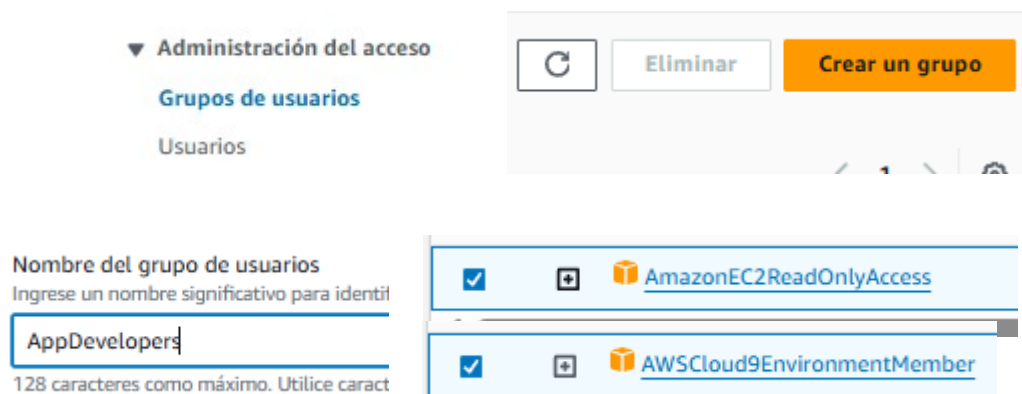
# Laboratorio de desafíos: Control del acceso a las cuentas de AWS mediante IAM

En el caso de que trabajemos en equipo y tengamos a varios compañeros en el equipo, es necesario crear reglas que permitan o denieguen el acceso a según que servicios. En este laboratorio vamos a crear 2 cuentas nuevas: una AppDevelopers que tendrá acceso a la instancia EC2 mediante conexión Cloud y acceso de solo lectura a la EC2, y otra DBAdministrators con acceso completo tanto a la base de datos RDS y al AWS System Manager.

## Una solicitud empresarial: Configurar el acceso a la cuenta de AWS para los desarrolladores de aplicaciones (Desafío n.º 1)

### Tarea 1: Configuración de un grupo de IAM con políticas y un usuario de IAM

Para empezar, debemos irnos a la consola de IAM y darle a crear un nuevo grupo. Le ponemos un nombre y le asignamos las siguientes políticas:



▼ Administración del acceso

Grupos de usuarios

Usuarios

Crear un grupo

Nombre del grupo de usuarios

Ingrese un nombre significativo para identificarlo

AppDeveloper

128 caracteres como máximo. Utilice caracteres

☒ ☐ ☐ AmazonEC2ReadOnlyAccess

☒ ☐ ☐ AWSCloud9EnvironmentMember



Estas políticas hacen que los usuarios solo puedan: tener acceso de solo lectura a la instancia EC2 y poder acceder a la instancia mediante Cloud9, es decir, pueden ver como está hecha la instancia por fuera, pero solo modificarla por dentro.

Ahora crearemos un usuario para meterlo en el grupo. El usuario deberá tener los siguientes datos:

▼ **Administración del acceso**

Grupos de usuarios

**Usuarios**


  

---

### Detalles del usuario

Nombre de usuario

El nombre de usuario puede tener un máximo de 64 caracteres. Caracteres válidos: A-Z, a-z, 0-9, and + = , . @ \_ - (guion)

☒ **Proporcione acceso de usuario a la consola de administración de AWS: *opcional***  
Si proporciona acceso a la consola a una persona, se trata de un [práctica recomendada](#)  para administrar su acceso Center.


Contraseña de la consola

☐ Contraseña generada automáticamente  
Puede ver la contraseña después de crear el usuario.


☒ **Contraseña personalizada**  
Ingrese una contraseña personalizada para el usuario.

- Debe tener como mínimo 8 caracteres
- Debe incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas (A-Z), letras minúsculas (a-z), n {} | ' "

☒ **Mostrar contraseña**

☐ **Los usuarios deben crear una nueva contraseña en el siguiente inicio de sesión (recomendado).**  
Los usuarios obtienen automáticamente la [IAMUserChangePassword](#)  política para poder cambiar su propia contraseña.

En la siguiente pestaña, añadimos el usuario al grupo que creamos antes:

Grupos de usuarios (1/1)		
<input type="text" value="Buscar"/>		
<input checked="" type="checkbox"/>	Nombre del grupo 	Usuarios
<input checked="" type="checkbox"/>	<a href="#">AppDevelopers</a>	0

Le damos a crear y si queremos podemos descargarnos las credenciales del usuario.

Vamos a configurar la app desde el IDE Cloud9, para ello entramos al servicio y en **DEV CafeServer** le damos a abrir IDE:

	Nombre ▲	Cloud9 IDE 	Tipo de entorno
<input type="radio"/>	<a href="#">DEV CafeServer</a>	<a href="#">Abrir</a>	Instancia de EC2

Una vez dentro, debemos poner estos 3 comandos

- `wget https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod8-challenge/install-cafe-app.sh`
- `chmod +x install-cafe-app.sh`
- `./install-cafe-app.sh`

```
voclabs:~/environment $ wget https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod8-challenge/install-cafe-app.sh
--2024-06-02 14:03:22-- https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod8-challenge/install-cafe-app.sh
Resolving aws-tc-largeobjects.s3-us-west-2.amazonaws.com (aws-tc-largeobjects.s3-us-west-2.amazonaws.com).
Connecting to aws-tc-largeobjects.s3-us-west-2.amazonaws.com (aws-tc-largeobjects.s3-us-west-2.amazonaws.com).
HTTP request sent, awaiting response... 200 OK
Length: 3911 (3.8K) [application/x-sh]
Saving to: 'install-cafe-app.sh'

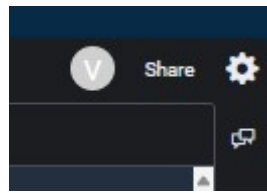
100%[=====] 3.8K 168 MB/s in 0.02s (3911/3911)

2024-06-02 14:03:22 (168 MB/s) - 'install-cafe-app.sh' saved [3911/3911]

voclabs:~/environment $ chmod +x install-cafe-app.sh
voclabs:~/environment $ ./install-cafe-app.sh
```

El primero nos descargará un script de bash de un bucket s3, el segundo lo hará ejecutable y el tercero lo ejecutará.

Mientras el script termina, vamos a compartir el entorno con el usuario que creamos antes. En el IDE Cloud9, pulsamos compartir arriba a la derecha:



Nos saldrá este formulario:

**Share this environment**

**Links to share**

Environment:

Application:

To make your application accessible from the internet, please follow [our documentation](#).

**Who has access**

▼ ReadWrite

● You (online) RW

☐ Don't allow members to save their tab state

**Invite Members**

R RW Invite

Invite an existing IAM user or [create a new user](#).

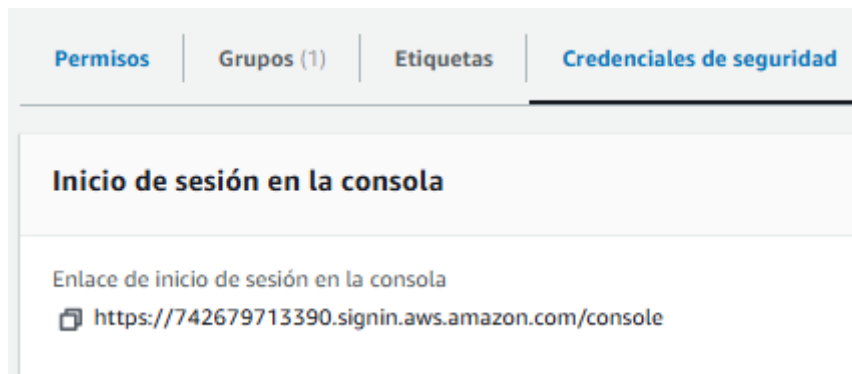
Done

En “Invite Members”, debemos poner el nombre del usuario que creamos anteriormente: Nikhil, y le damos a “Invite”. Nos saldrá una advertencia de seguridad, le damos que OK y listo.

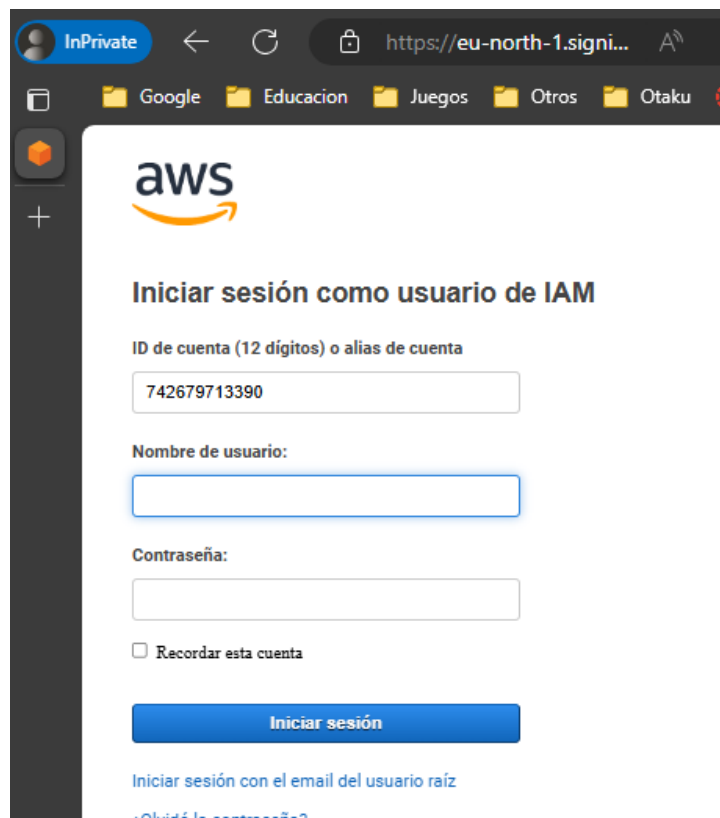
Ahora podremos cerrar algunas pestañas del navegador, pero debemos dejar al menos 1 con el usuario Sofía.

## Tarea 2: Inicio de sesión como Nikhil y prueba del acceso

Para esta tarea, debemos iniciar sesión como Nikhil, para ello, con el usuario principal, nos vamos a los usuario IAM y elegimos Nikhil, y copiamos ese enlace:



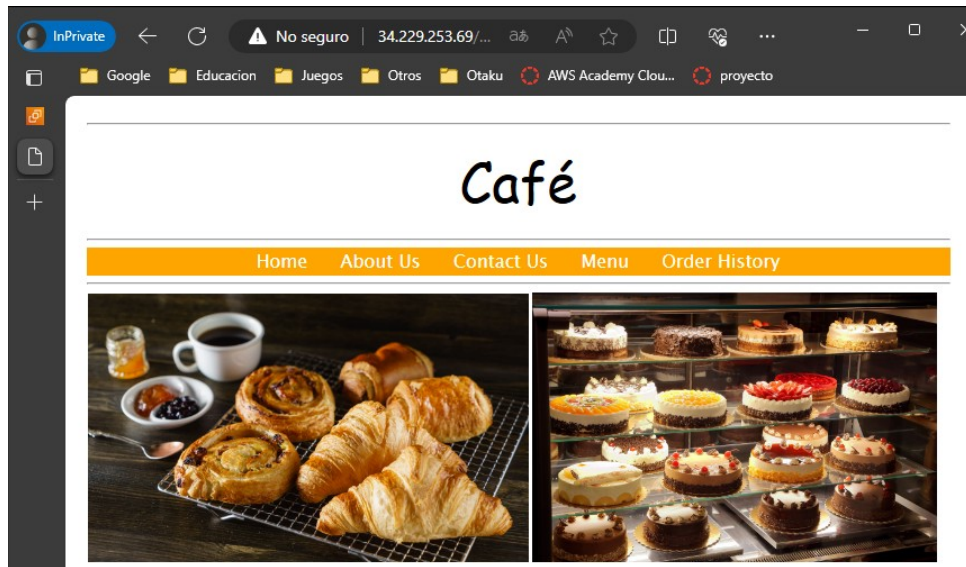
Este enlace nos permitirá logearnos como Nikhil desde el navegador privado(puede ser una pestaña privada u otro navegador, lo importante es que no tenga la sesión principal).



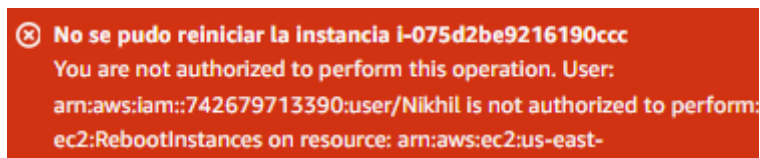
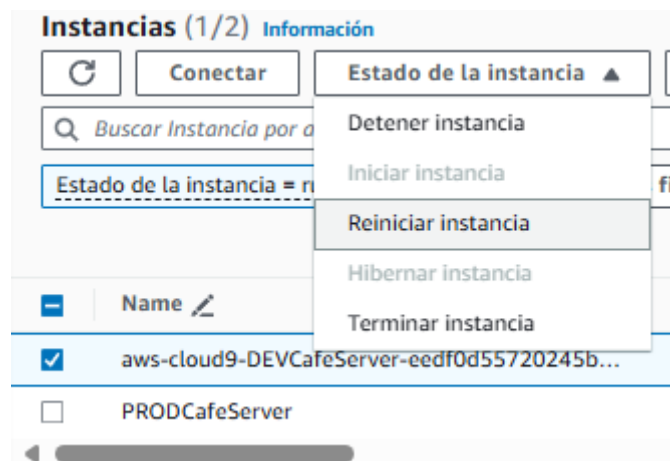
Ponemos los datos necesarios: Nikhil y @ppD3veloper2020!

Una vez dentro, nos vamos al servicio EC2 y copiamos la dirección IPv4 de la instancia aws-cloud... y la ponemos en el navegador(privado):

Deberíamos ver perfectamente la app:



Por ultimo vamos a probar a reiniciar la instancia:

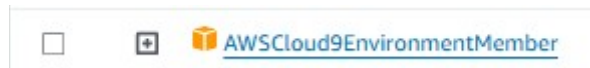


Antes de continuar, vamos a resolver unas preguntas:

**¿Qué ocurrió cuando Nikhil intentó reiniciar la instancia de EC2?**

Como vimos antes, nos salió un error de permisos debido al rol IAM

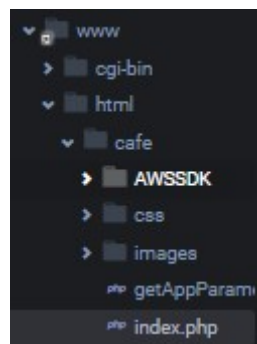
**¿Qué política de IAM permitió a Nikhil acceder al entorno de AWS Cloud9?**



Volvamos con el laboratorio, vamos a conectarnos al IDE cloud9 con el usuario Nikhil. Para ello, nos vamos al servicio Cloud9, y en entornos debemos especificar que son entornos compartidos:



Así nos aparecerá y podremos conectarnos a él. Ahora que estamos dentro vamos a comprobar si podemos realizar algún cambio en la app. Nos vamos a la siguiente carpeta:



En index php, cambiamos la línea 13 y ponemos lo siguiente:

```
<div class="center">Café; DEV Site</div>
```

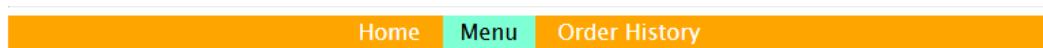
Guardamos el archivo y volvemos a copiar la IP:



Vemos que el cambio se ha producido.

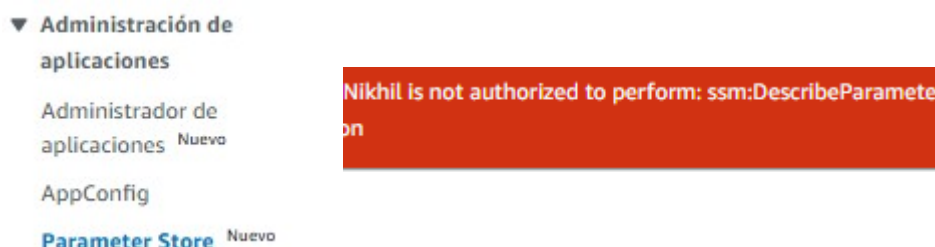
Vamos a contestar alguna preguntas antes de continuar:

**¿Qué mensaje se muestra en la página Menu (Menú) de la instancia de desarrollo del sitio web de la cafetería?**



No me aparece ninguno, pero en internet pone que debería salir un mensaje de conexión perdida con el servidor.

Con el usuario Nikhil entramos al servicio **Systems Manager** y en **Parameter Store**:

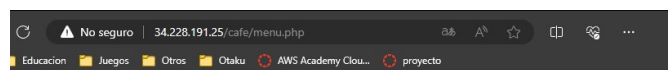
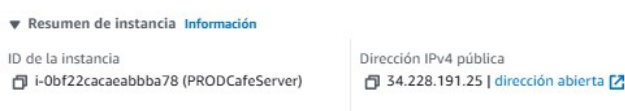


Mismo error de antes, no podemos entrar debido a los permisos.

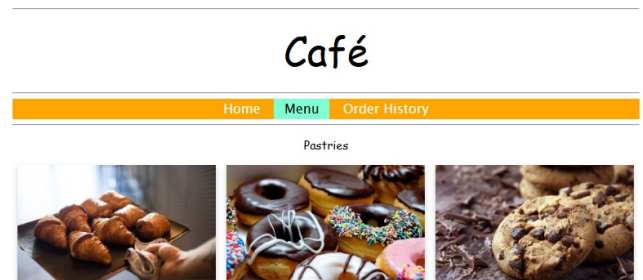
**¿Qué mensaje se mostró cuando Nikhil abrió la página Almacén de parámetros de Systems Manager en la consola?**

Resumiendolo, ninguna poñíta basada en identidad permite la acción ssm, osea, no podemos entrar debido a los permisos del grupo IAM.

Copiamos ahora la IPv4 de la otra instancia y comprobemos que pasa ahora en el menú:



Esta funciona perfectamente. Básicamente, son 2 instancias diferentes pero iguales, una la ve el público y la otra sirve para los desarrolladores





# Nuevo requisito empresarial: Configuración del acceso a la cuenta de AWS para administradores de bases de datos (Desafío n.º 2)

## Tarea 3: Configuración de IAM para el acceso de usuarios administradores de bases de datos

En esta tarea vamos a hacer lo mismo que en la tarea 1 pero con nuevos permisos y usuario. Nos vamos al servicio IAM y creamos un nuevo grupo:

Nombre del grupo de usuarios  
Ingrese un nombre significativo para identificar a este grupo.

DBAdministrators  
128 caracteres como máximo. Utilice caracteres alfabéticos y números.

☒ ☐ [AmazonRDSReadOnlyAccess](#)

☒ ☐ [AmazonSSMFullAccess](#)

Permite el acceso de solo lectura a la RDS a través de la consola de administración.

Permite acceso total a Amazon ssm.

Ahora creamos al usuario Olivia:

Nombre de usuario  
El nombre de usuario puede tener un máximo de 64 caracteres. Caracteres permitidos: letras, números, guiones bajos y guiones.

Olivia

☒ Proporcione acceso de usuario a la consola de administración  
Si proporciona acceso a la consola a una persona, se trata de un usuario de la consola.

Contraseña de la consola

☐ Contraseña generada automáticamente  
Puede ver la contraseña después de crear el usuario.

☒ Contraseña personalizada  
Ingrese una contraseña personalizada para el usuario.

Db@dministrat0r2020!  
Debe tener como mínimo 8 caracteres.  
Debe incluir al menos tres de los siguientes tipos de caracteres: mayúsculas, minúsculas, números y caracteres especiales.

☒ Mostrar contraseña

Grupos de usuarios (1/2)

Buscar

☒ Nombre del grupo

☐ [AppDevelopers](#)

☒ [DBAdministrators](#)

Tarea 4: Inicio de sesión como administrador de la base de datos y resolución del problema de conectividad de la base de datos

En este punto, no necesitaremos más a Nikhil, por lo que podremos cerrar sesión con esta y abrirla con Olivia. Copiamos el enlace de sesión se Olivia y ponemos sus credenciales.

Una vez dentro, comprobemos que la base de datos funcione perfectamente:

Identificador de base de datos	Estado	Rol	Motor	Región
<a href="#">c115383a2736372l6445569t1w74267971339-cafedatabase-vjkbvt8h01rx</a>	Disponible	Instancia	MariaDB	us-east

Vemos que está todo correcto(Comprobad que la región es la misma que la de Sofía)

Abrimos ahora la consola EC2 y vemos las instancias en ejecución.

Una pregunta:

¿Por qué Olivia no puede acceder a los detalles de la instancia de EC2?

No puede porque su rol IAM no lo permite.

You are not authorized to perform this operation. User: arn:aws:iam::742679713390:user/Olivia is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

Olivía necesita poder acceder las instancias en ejecución para solucionar el problema, vamos a darle los permisos necesarios para ello. Nos vamos al grupo DBAdministrator y adjuntamos las siguientes políticas:

<input type="checkbox"/>			<a href="#">AmazonEC2ReadOnlyAccess</a>
<input type="checkbox"/>			<a href="#">AmazonRDSReadOnlyAccess</a>
<input type="checkbox"/>			<a href="#">AmazonSSMFullAccess</a>
<input type="checkbox"/>			<a href="#">IAMReadOnlyAccess</a>

En la consola IAM, usuario Sofía pestaña **Access Advisor**, podemos ver los servicios que intentó abrir Sofía:

<a href="#">Amazon EC2</a>	<a href="#">AmazonRDSReadOnlyAccess y 2 más</a>	Hoy
<a href="#">Amazon CloudWatch</a>	<a href="#">AmazonRDSReadOnlyAccess y 2 más</a>	Hoy
<a href="#">Amazon RDS</a>	<a href="#">AmazonRDSReadOnlyAccess</a>	Hoy
<a href="#">Elastic Load Balancing</a>	<a href="#">AmazonEC2ReadOnlyAccess</a>	Hoy
<a href="#">Amazon EC2 Auto Scaling</a>	<a href="#">AmazonEC2ReadOnlyAccess</a>	Hoy

Esto es más como un dato por si necesitamos añadir x permisos.

Volviendo con Olivía, veremos que ahora si podemos acceder a la consola EC2:

<input type="checkbox"/>	Name	ID de la instancia	Estado de la i...	Tipo de inst...
<input type="checkbox"/>	aws-cloud...	i-075d2be9216190ccc	En ejecución	t2.micro
<input type="checkbox"/>	PRODCafeServer	i-0bf22cacaeabbba78	En ejecución	t2.micro

Como sabemos por Olivia, algo de la instancia aws-cloud está mal y en la PROD está bien. Vamos a ver el Rol IAM CafeRole de la instancia aws-cloud:

Fijémonos en **AmazonSSMManagedInstanceCore** y observemos el JSON.

**Nombre dos acciones específicas en la política que permiten a la aplicación web de la cafetería en esta instancia acceder a las credenciales de la base de datos en el Almacén de parámetros.**

Las acciones son:

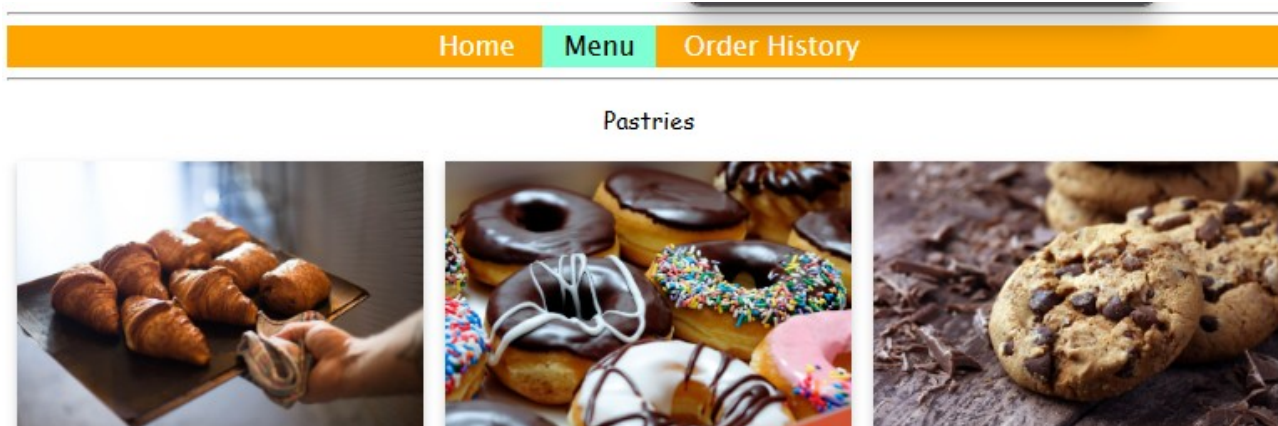
"ssm:GetParameter",  
"ssm:GetParameters",

Podemos ver que los permisos no son, ya que son correctos.

Por aquí comentan que antiguamente la base de datos estaba en local y luego se pasó a RDS, a lo mejor, los datos en System Manager no se cambiaron correctamente. Como Olivía, vamos a cambiar esos datos, nos han chivado que es el nombre de usuario:

Valor  
root

En realidad, debería ser **dbUser**, lo cambiamos y comprobamos, copiamos la IPv4 de la instancia aws-cloud... e intentamos entrar al menú:



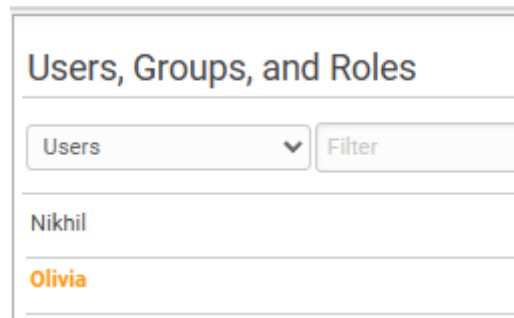
## Nuevo requisito empresarial: Perfeccionamiento del acceso del usuario de IAM (Desafío n.º 3)

### Tarea 5: Uso del Simulador de políticas de IAM y creación de una política de IAM personalizada con el editor visual

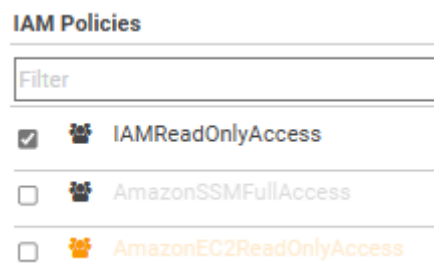
En el navegador donde se encuentra la sesión de Sofía pondremos la siguiente URL:

<https://policysim.aws.amazon.com/>

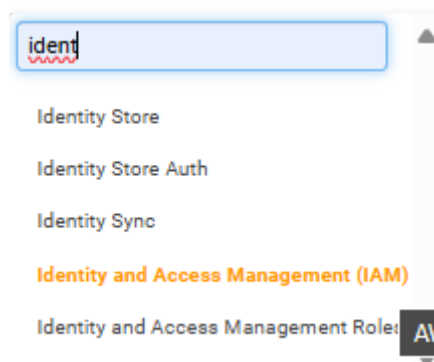
Esto es un simulador de políticas de IAM. Seleccionamos al usuario Olivia:



Y en la lista de políticas, nos aseguramos de que **IAMReadOnlyAccess** esté marcado, y desmarcamos las casillas de verificación de las demás políticas:



En la parte del simulador, le damos a seleccionar servicios y seleccionamos el siguiente:



Le damos a select all y Run Simulation

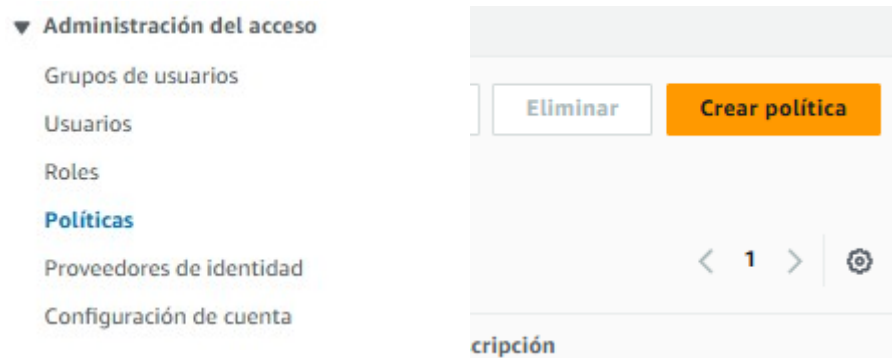
---

**Action Settings and Results** [171 actions selected. 0 actions not simulated. 69 actions allowed. 102 actions denied. ]

---

Este es el resultado, Olivia con ese permiso puede realizar 69 acciones en total.

En este punto recordamos que le hemos dado permisos de más al grupo de bases de datos, vamos a crear una política un poco más restrictiva, volvemos a trabajar con Sofía y en la consola de IAM le damos a crear una política:



Ponemos lo siguiente:



Abajo le damos a añadir un permiso adicional y ponemos lo siguiente:

#### Leer









- |                                                                                            |                                                                                                  |                                                                                               |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <input type="checkbox"/> <a href="#">GetAccessKeyLastUsed</a>   Información                | <input type="checkbox"/> <a href="#">GetAccountAuthorizationDetails</a>   Información            | <input type="checkbox"/> <a href="#">GetAccountEmailAddress</a>   Información                 |
| <input type="checkbox"/> <a href="#">GetAccountName</a>   Información                      | <input type="checkbox"/> <a href="#">GetAccountPasswordPolicy</a>   Información                  | <input type="checkbox"/> <a href="#">GetCloudFrontPublicKey</a>   Información                 |
| <input type="checkbox"/> <a href="#">GetContextKeysForCustomPolicy</a>   Información       | <input type="checkbox"/> <a href="#">GetContextKeysForPrincipalPolicy</a>   Información          | <input type="checkbox"/> <a href="#">GetCredentialReport</a>   Información                    |
| <input type="checkbox"/> <a href="#">GetGroup</a>   Información                            | <input type="checkbox"/> <a href="#">GetGroupPolicy</a>   Información                            | <input checked="" type="checkbox"/> <a href="#">GetInstanceProfile</a>   Información          |
| <input type="checkbox"/> <a href="#">GetMFADevice</a>   Información                        | <input type="checkbox"/> <a href="#">GetOpenIDConnectProvider</a>   Información                  | <input type="checkbox"/> <a href="#">GetOrganizationsAccessReport</a>   Información           |
| <input type="checkbox"/> <a href="#">GetPolicy</a>   Información                           | <input checked="" type="checkbox"/> <a href="#">GetPolicyVersion</a>   Información               | <input checked="" type="checkbox"/> <a href="#">GetRole</a>   Información                     |
| <input checked="" type="checkbox"/> <a href="#">GetRolePolicy</a>   Información            | <input type="checkbox"/> <a href="#">GetSAMLProvider</a>   Información                           | <input type="checkbox"/> <a href="#">GetServerCertificate</a>   Información                   |
| <input type="checkbox"/> <a href="#">GetServiceLastAccessedDetails</a>   Información       | <input type="checkbox"/> <a href="#">GetServiceLastAccessedDetailsWithEntities</a>   Información | <input type="checkbox"/> <a href="#">GetServiceLinkedRoleDeletionStatus</a>   Información     |
| <input type="checkbox"/> <a href="#">GetSSHPublicKey</a>   Información                     | <input type="checkbox"/> <a href="#">GetUser</a>   Información                                   | <input type="checkbox"/> <a href="#">GetUserPolicy</a>   Información                          |
|                                                                                            |                                                                                                  |                                                                                               |
| <input type="checkbox"/> <a href="#">ListAccessKeys</a>   Información                      | <input type="checkbox"/> <a href="#">ListAccountAliases</a>   Información                        | <input type="checkbox"/> <a href="#">ListAttachedGroupPolicies</a>   Información              |
| <input checked="" type="checkbox"/> <a href="#">ListAttachedRolePolicies</a>   Información | <input type="checkbox"/> <a href="#">ListAttachedUserPolicies</a>   Información                  | <input type="checkbox"/> <a href="#">ListCloudFrontPublicKeys</a>   Información               |
| <input type="checkbox"/> <a href="#">ListEntitiesForPolicy</a>   Información               | <input type="checkbox"/> <a href="#">ListGroupPolicies</a>   Información                         | <input type="checkbox"/> <a href="#">ListGroups</a>   Información                             |
| <input type="checkbox"/> <a href="#">ListGroupsForUser</a>   Información                   | <input checked="" type="checkbox"/> <a href="#">ListInstanceProfiles</a>   Información           | <input checked="" type="checkbox"/> <a href="#">ListInstanceProfilesForRole</a>   Información |
| <input type="checkbox"/> <a href="#">ListInstanceProfileTags</a>   Información             | <input type="checkbox"/> <a href="#">ListMFADevices</a>   Información                            | <input type="checkbox"/> <a href="#">ListMFADeviceTags</a>   Información                      |
| <input type="checkbox"/> <a href="#">ListOpenIDConnectProviders</a>   Información          | <input type="checkbox"/> <a href="#">ListOpenIDConnectProviderTags</a>   Información             | <input checked="" type="checkbox"/> <a href="#">ListPolicies</a>   Información                |
| <input type="checkbox"/> <a href="#">ListPoliciesGrantingServiceAccess</a>   Información   | <input type="checkbox"/> <a href="#">ListPolicyTags</a>   Información                            | <input type="checkbox"/> <a href="#">ListPolicyVersions</a>   Información                     |
| <input checked="" type="checkbox"/> <a href="#">ListRolePolicies</a>   Información         | <input checked="" type="checkbox"/> <a href="#">ListRoles</a>   Información                      | <input type="checkbox"/> <a href="#">ListRoleTags</a>   Información                           |

En la pestaña de recursos, seleccionamos **Any in this account** para los 3 recursos. Antes de acabar, vamos a ver las opciones que hemos añadido en formato JSON para verlo mejor:

```
"Statement": [
  {
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "iam:ListPolicies",
      "ec2:DescribeIamInstanceProfileAssociations",
      "iam:ListRoles",
      "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
  },
  {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
      "iam:GetRole",
      "iam:ListInstanceProfilesForRole",
      "iam:GetPolicyVersion",
      "iam:GetInstanceProfile",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:GetRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::742679713390:policy/*",
      "arn:aws:iam::742679713390:instance-profile/*",
      "arn:aws:iam::742679713390:role/*"
    ]
  }
]
```

Le ponemos un nombre y le damos a crear política. Esto mismo se hizo con mi cuenta, por lo que en realidad, no puedo crear políticas de IAM XD, salimos y le damos a cancelar. Sin embargo se creó una política para que nosotros la pudiéramos usar en el Laboratorio: **LimitedIamPolicy**

Vamos a editar al grupo **DBAdministrators**, añadirle esta política y a borrarle **IAMReadOnlyAccess**:

<input type="checkbox"/>	Nombre de la política 
<input type="checkbox"/>	  <a href="#">AmazonEC2ReadOnlyAccess</a>
<input type="checkbox"/>	  <a href="#">AmazonRDSReadOnlyAccess</a>
<input type="checkbox"/>	  <a href="#">AmazonSSMFullAccess</a>
<input type="checkbox"/>	 <a href="#">LimitedIamPolicy</a>

Si lo comprobamos, podremos ver que Olivia aún puede ver los detalles de las instancias EC2, lo que hemos hecho es limitarle un poco para que no pueda cambiar nada.

Si algún punto no ha salido correctamente, no es para alarmarse, este laboratorio solo está para ver y demostrar los permisos IAM y las cuentas de usuario.