

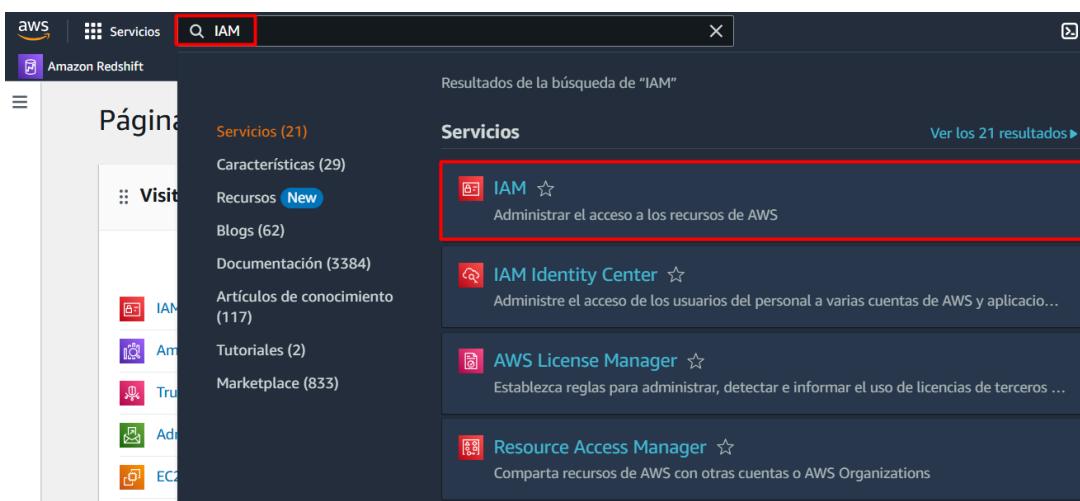
LABORATORIO DE AWS IAM, KMS Y SECRETS MANAGER

En este laboratorio vamos a crear usuarios y grupos, a agregar usuarios a los grupos y a asignar políticas a los usuarios y a los grupos.

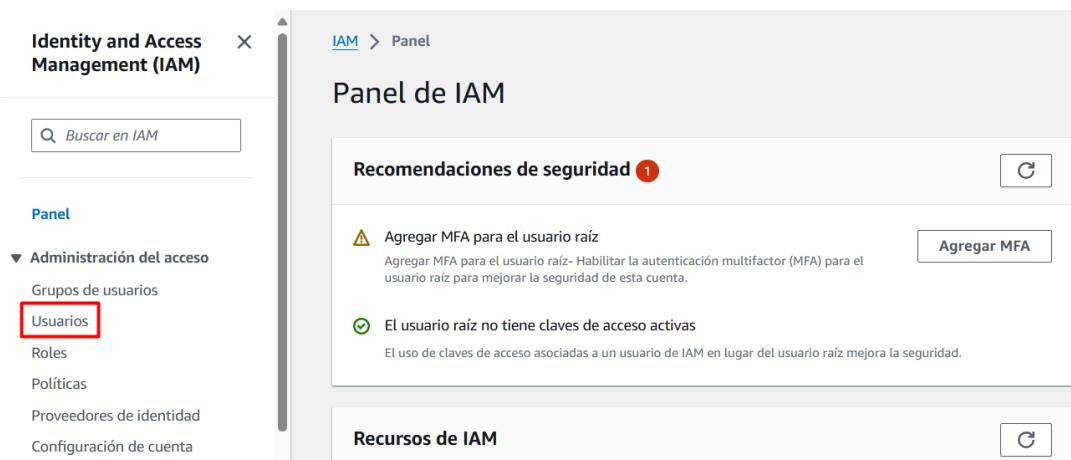
Además, vamos a crear una key con KMS y a proteger secretos con Secrets Manager.

USUARIOS

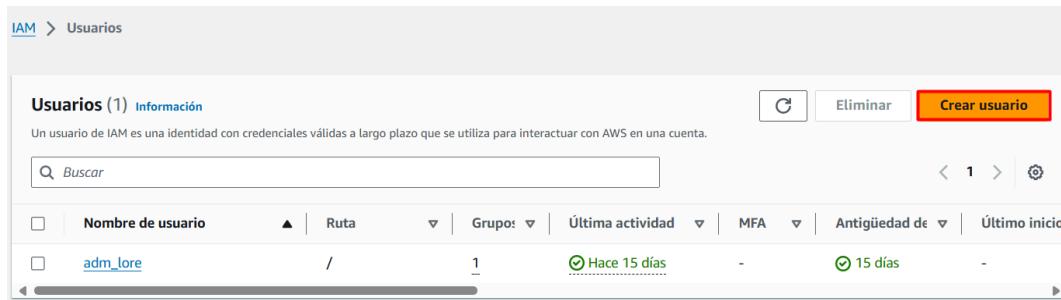
1. Iniciamos sesión en la consola de administración de AWS e ingresamos a la consola de IAM:



2. En el menú lateral, seleccionamos **Usuarios**:



3. Damos clic en **Crear usuario**:



The screenshot shows the AWS IAM 'Users' page. At the top, there is a breadcrumb navigation 'IAM > Usuarios'. Below the header, it says 'Usuarios (1) Información' and provides a brief description: 'Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.' A search bar labeled 'Buscar' is present. On the right side of the header are three buttons: 'Eliminar' (gray), 'Crear usuario' (red), and another gray button. Below the header is a table with the following columns: 'Nombre de usuario', 'Ruta', 'Grupos', 'Última actividad', 'MFA', and 'Antigüedad de'. The table contains one row for the user 'adm_lore', which has a status of 'Hace 15 días' and was created '15 días' ago.

4. Especificar los 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). En este ejemplo usamos **test_betek1**, puedes usar tu nombre si deseas.
- Proporcione acceso de usuario a la consola de administración de AWS: **Check (marcar)**. La consola de administración es la interfaz gráfica de AWS, por la que accedemos a los servicios a través del navegador del web.
- Seleccionar **Quiero crear un usuario de IAM**.
- Cuando vamos a crear la contraseña de la consola, tenemos dos opciones, Contraseña generada automáticamente y Contraseña personalizada. Para este laboratorio vamos seleccionar **Contraseña generada automáticamente**.
- Podemos determinar que los usuarios deban crear una nueva contraseña en el siguiente inicio de sesión, esta es una buena práctica recomendada de seguridad: **Marcar (check)**.
- Clic en **Siguiente**.

Nombre de usuario
 1
 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 en IAM Identity Center.

¿Está proporcionando acceso a la consola a una persona?

Tipo de usuario
 Especificar un usuario en Identity Center: recomendado
 Le recomendamos que utilice Identity Center para proporcionar acceso a la consola a una persona. Con Identity Center, puede administrar de forma centralizada el acceso de los usuarios a sus cuentas de AWS y aplicaciones en la nube.
 Quiero crear un usuario de IAM
 Le recomendamos que cree usuarios de IAM solo si necesita habilitar el acceso mediante programación a través de claves de acceso, credenciales específicas de servicios para AWS CodeCommit o Amazon Keyspaces o una credencial de copia de seguridad para el acceso a la cuenta de emergencia.

4 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.

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.

5 Si está creando acceso mediante programación a través de claves de acceso o credenciales específicas de servicios para AWS CodeCommit o Amazon Keyspaces, puede generarlos después de crear este usuario de IAM. [Más información](#)

[Cancelar](#) [Siguiente](#)

5. Establecer permisos: En este paso vamos a indicar qué acciones podrá realizar este usuario sobre los recursos de AWS:

- Podemos agregar el usuario a un grupo, de esta manera el usuario heredará los permisos del grupo. Se recomienda utilizar grupos para administrar los permisos de usuario según las funciones laborales.
- También podemos copiar los permisos de otro usuario ya existente.
- O adjuntar una política administrada a un usuario de manera directa. Como práctica recomendada, se sugiere adjuntar políticas a un grupo y luego agregar el usuario al grupo adecuado.

Por ahora no le vamos a dar ningún tipo de permiso a este usuario y damos clic en **Siguiente:**

Opciones de permisos

Agregar usuario al grupo
 Agregue el usuario a un grupo existente o cree uno nuevo. Le recomendamos que utilice grupos para administrar los permisos de usuario según las funciones laborales.

Copiar permisos
 Copie todas las suscripciones a grupos, las políticas administradas adjuntas y las políticas insertadas de un usuario existente.

Adjuntar políticas directamente
 Adjunte una política administrada a un usuario de manera directa. Como práctica recomendada, lo sugerimos, en cambio, adjuntar políticas a un grupo. A continuación, agregue el usuario al grupo adecuado.

Grupos de usuarios (1)
[Crear un grupo](#)

Nombre del grupo	Usuarios	Políticas adjuntas	Creado
admin_users	1	AmazonEC2FullAccess, Amaz...	2024-07-07 (Hace 15 días)

Establecer límite de permisos: opcional

[Cancelar](#) [Anterior](#) [Siguiente](#)

6. Revisar y crear: En este paso revisamos la configuración del usuario que vamos a crear, el nombre es **test_betek1**, el tipo de contraseña es autogenerada, si requiere un restablecimiento de la contraseña y, el único permiso que tiene es el de cambiar su propia contraseña, esto es para que él pueda cambiar su contraseña la primera vez que ingrese a AWS.

Después de revisar, damos clic en **Crear usuario**:

Revisar y crear

Revise las opciones seleccionadas. Después de crear el usuario, puede ver y descargar la contraseña autogenerada, si está habilitada.

Detalles del usuario

Nombre de usuario test_betek1	Tipo de contraseña de consola Autogenerated	Exigir el restablecimiento de la contraseña Sí
----------------------------------	--	---

Resumen de permisos

Nombre	Tipo	Usado como
IAMUserChangePassword	Administrada por AWS	Política de permisos

Etiquetas : opcional

No hay etiquetas asociadas al recurso.

Agregar nueva etiqueta

Puede agregar hasta 50 etiquetas más.

Cerrar | Anterior | **Crear usuario**

7. Una vez tengamos el mensaje de que el usuario se creó correctamente, descargamos las credenciales de este nuevo usuario:

El usuario se ha creado correctamente

Puede ver y descargar la contraseña del usuario y las instrucciones de correo electrónico para iniciar sesión en la Consola de administración de AWS.

Ver usuario

Recuperar contraseña

Puede ver y descargar la contraseña del usuario a continuación o enviar por correo electrónico instrucciones a los usuarios para iniciar sesión en la consola de administración de AWS. Esta es la única vez que puede ver y descargar esta contraseña.

Detalles de inicio de sesión en la consola

URL de inicio de sesión de la consola
<https://933028198366.siginin.aws.amazon.com/console>

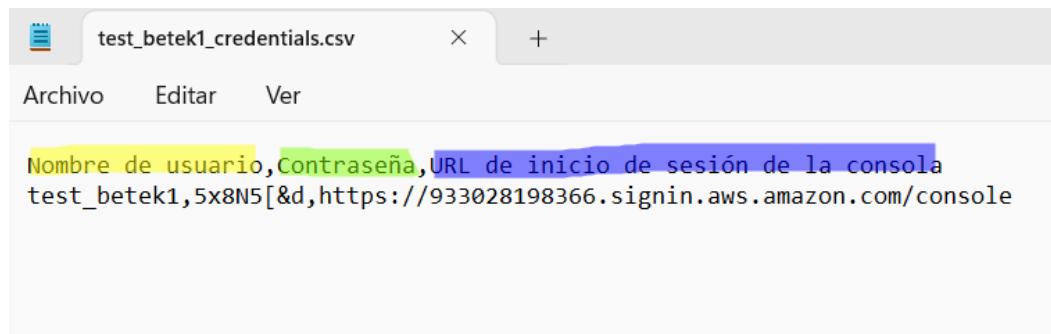
Nombre de usuario
[test_betek1](#)

Contraseña de la consola
***** [Mostrar](#)

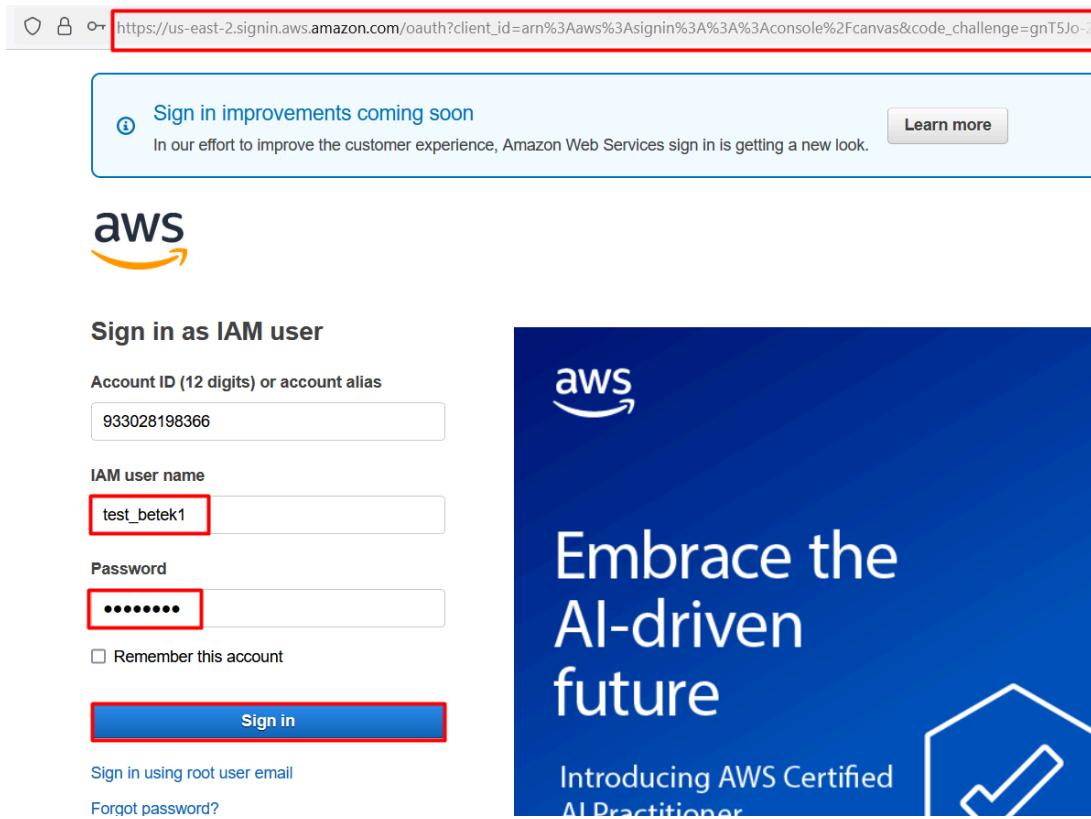
Instrucciones de inicio de sesión por correo electrónico

Cerrar | **Descargar archivo.csv** | Volver a la lista de usuarios

8. El archivo que descargamos, en formato CSV, tiene tres parámetros separados por coma: Nombre de usuario, contraseña y URL del inicio de sesión, con estos tres datos nuestro usuario ya puede ingresar a la consola de AWS:



Para evitar conflictos entre las sesiones, pegamos la URL en otro navegador e ingresamos con los datos del CSV descargado:



Como se lo indicamos en la creación del usuario, nos va a pedir cambio de contraseña, ingresamos la actual (del CSV) y establecemos la nueva:

aws

You must change your password to continue.

AWS account 933028198366

IAM user name test_betek1

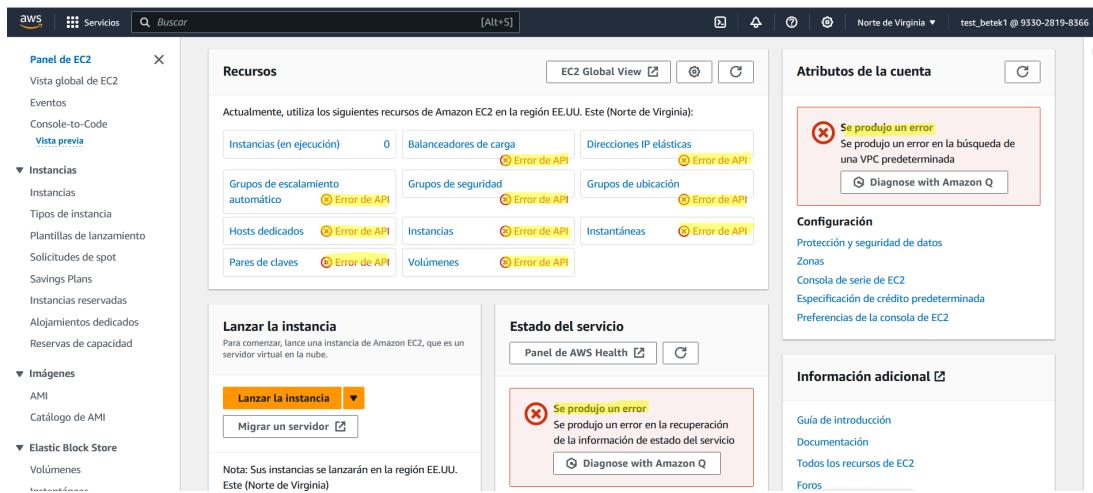
1 Old password

2 New password

3 Retype new password

4 Confirm password change

Si navegamos a la consola de EC2, nos va a salir error, no podemos ver las instancias, los balanceadores de carga, nada:



The screenshot shows the AWS EC2 console interface. On the left, there's a sidebar with navigation links like 'Panel de EC2', 'Instancias', 'Imagenes', and 'Elastic Block Store'. The main content area has several sections: 'Recursos' (Resources) which lists 'Instancias (en ejecución)' (0), 'Balanceadores de carga' (Error de API), 'Direcciones IP elásticas' (Error de API), 'Grupos de escalamiento automático' (Error de API), 'Grupos de seguridad' (Error de API), 'Grupos de ubicación' (Error de API), 'Hosts dedicados' (Error de API), 'Instancias' (Error de API), 'Instantáneas' (Error de API), 'Pares de claves' (Error de API), 'Volumenes' (Error de API); 'Lanzar la instancia' (Launch instance) with 'Lanzar la instancia' and 'Migrar un servidor' buttons; 'Estado del servicio' (Service status) with a note about launching instances in the US East (N. Virginia) region; and 'Atributos de la cuenta' (Account attributes) which shows an error message: 'Se produjo un error: Se produjo un error en la búsqueda de una VPC predeterminada'. Other sections include 'Configuración' (Configuration) and 'Información adicional' (Additional information).

Lo mismo sucede si navegamos en la consola de RDS, o en cualquier otro servicio, no podemos ver nada:

The screenshot shows the AWS RDS console under the 'Bases de datos' section. A red box highlights an error message: 'User: arn:aws:iam::933028198366:user/test_betek1 is not authorized to perform: rds:DescribeDBInstances on resource: arn:aws:rds:us-east-1:933028198366:db-* because no identity-based policy allows the rds:DescribeDBInstances action User: arn:aws:iam::933028198366:user/test_betek1 is not authorized to perform: rds:DescribeDBClusters on resource: arn:aws:rds:us-east-1:933028198366:cluster-* because no identity-based policy allows the rds:DescribeDBClusters action User: arn:aws:iam::933028198366:user/test_betek1 is not authorized to perform: rds:DescribeGlobalClusters on resource: arn:aws:rds:933028198366:global-cluster-* because no identity-based policy allows the rds:DescribeGlobalClusters action'.

A blue box contains a note: 'Considera la posibilidad de crear una implementación azul-verde para minimizar el tiempo de inactividad durante las actualizaciones.' followed by links to the RDS and Aurora user guides.

The main table lists 'Bases de datos (0)' with columns: Identificador de base de datos, Estado, Rol, Motor, Región y AZ, Tamaño, Recomendaciones, and CPU. It shows 'No se encontró ningún tipo de instancias'.

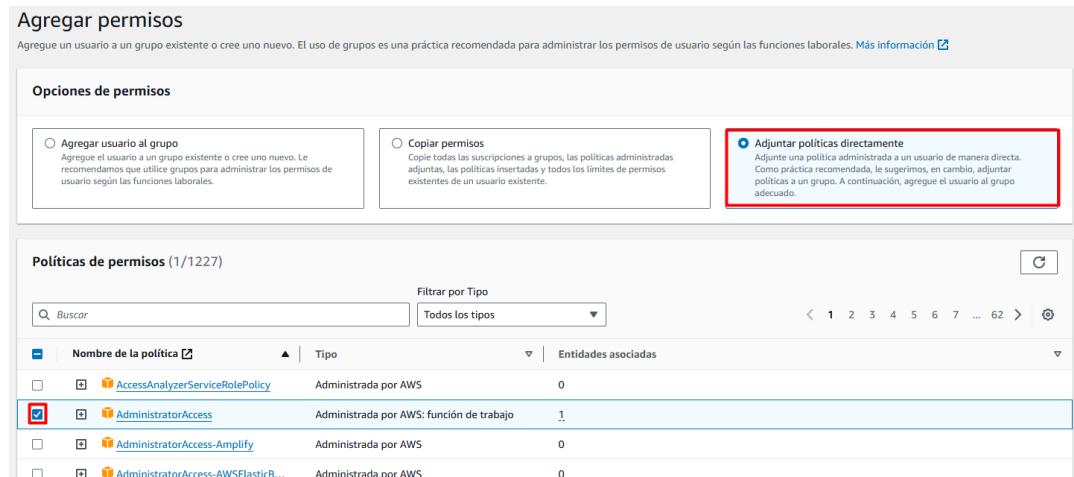
Esto se debe a que el usuario no tiene permiso en EC2, ni en RDS, ni en ningún recurso de AWS, el único permiso que tiene el usuario es el de cambiar su propia contraseña.

Para solucionar esto, debemos ir a la cuenta administradora y agregar los permisos al usuario para poder realizar estas acciones.

9. En la consola del usuario root, vamos al servicio **IAM**, ingresamos a la opción **Usuarios**, buscamos el usuario que creamos (en este ejemplo **test_betek1**), desplegamos el menú Agregar permisos y seleccionamos **Agregar permisos**:

The screenshot shows the IAM 'Users' page with 'test_betek1' selected. The 'Resumen' section displays ARN, Access to the console (Enabled without MFA), and Access key (Access key 1). The 'Permisos' tab is active, showing one policy associated: 'Políticas de permisos (1)'. The 'Agregar permisos' button is highlighted with a red box. Other buttons visible include 'Eliminar', 'Crear clave de acceso', and 'Crear política insertada'.

Vamos a adjuntarle una política que ya existe con los permisos requeridos: Seleccionamos **Adjuntar políticas directamente**, seleccionamos **AdministratorAccess**, esta política le va a dar acceso al usuario a todos los servicios de AWS y va a poder realizar cualquier acción:



Nombre de la política	Tipo	Entidades asociadas
AccessAnalyzerServiceRolePolicy	Administrada por AWS	0
<input checked="" type="checkbox"/> AdministratorAccess	Administrada por AWS: función de trabajo	1
AdministratorAccess-Amplify	Administrada por AWS	0
AdministratorAccess-AWSFleasticR...	Administrada por AWS	0

Al final de la página, damos clic en **Siguiente** y luego en **Agregar permisos**:



Nombre	Tipo	Usado como
AdministratorAccess	Administrada por AWS: función de trabajo	Política de permisos

Ahora vemos que el usuario tiene el permiso FullAccess y el permiso de cambiar su contraseña:

JAM > Usuarios > test_betek1

test_betek1 Información

Resumen

ARN arn:aws:iam::933028198366:user/test_betek1	Acceso a la consola Habilitado sin MFA	Clave de acceso 1 Crear clave de acceso
Creado July 22, 2024, 21:39 (UTC-05:00)	Último inicio de sesión en la consola Hoy	

Permisos | Grupos | Etiquetas | Credenciales de seguridad | Access Advisor

Políticas de permisos (2)

Los permisos se definen mediante políticas asociadas al usuario directamente o a través de grupos.

Nombre de la política	Tipo	Adjuntado a través de
AdministratorAccess	Administrada por AWS: función de trabajo	Directamente
AmazonUserChangePassword	Administrada por AWS	Directamente

10. Regresamos a la sesión del usuario **test_betek1**, damos F5 o refrescamos la página y ahora no tenemos los mensajes de error que teníamos antes de asignar los permisos:

AWS Servicios Buscar [Alt+S] Norte de Virginia test_betek1 @ 9330-2819-8366

Amazon RDS

- Panel
- Bases de datos**
- Editor de consultas
- Información sobre rendimiento
- Instantáneas de
- Exportaciones en Amazon S3
- Copias de seguridad automatizadas
- Instancias reservadas
- Proxies
- Grupos de subredes

RDS > Bases de datos

Consideré la posibilidad de crear una implementación azul-verde para minimizar el tiempo de inactividad durante las actualizaciones. Es posible que desee considerar el uso de las implementaciones azul-verde de Amazon RDS y minimizar el tiempo de inactividad durante las actualizaciones. Una implementación azul-verde proporciona un entorno de ensayo para los cambios en las bases de datos de producción. [Guía del usuario de RDS](#) [Guía del usuario de Aurora](#)

Bases de datos (0) Recursos del grupo | Modificar | Acciones | Restaurar desde S3 | **Crear base de datos**

Filtrar por bases de datos

Identificador de base de datos | Estado | Rol | Motor | Región y AZ | Tamaño | Recomendaciones | CPU

No se encontró ningún tipo de instancias

AWS Servicios Buscar [Alt+S] Norte de Virginia test_betek1 @ 9330-2819-8366

Panel de EC2

- Vista global de EC2
- Eventos
- Console-to-Code
- Vista previa**
- Instancias**
- Tipos de instancia
- Plantillas de lanzamiento
- Solicitudes de spot
- Savings Plans
- Instancias reservadas

Instancias Información Conectar Estado de la instancia | Acciones | **Lanzar instancias**

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

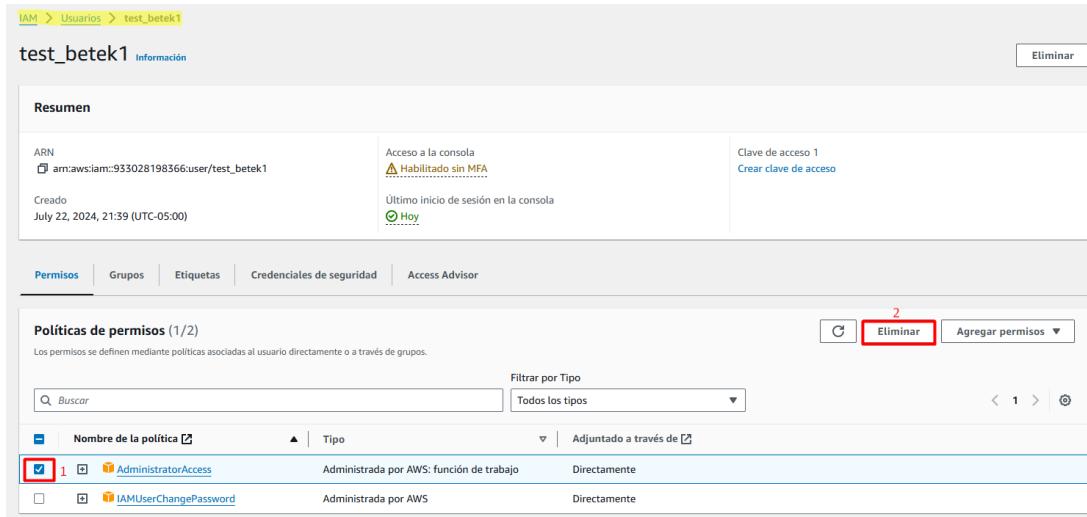
Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al...	Zona de dispon...	DNS de IPv4 públ...
No hay instancias							
No tiene ninguna Instancia en esta región							

Lanzar instancias

Seleccione una instancia

El usuario no ve bases de datos RDS ni instancias EC2 porque aún no ha creado ninguna, pero ya no tiene mensajes de error por falta de permisos, como antes.

11. Ahora vamos a regresar a la cuenta del usuario root y le vamos a quitar los permisos de administrador al usuario **test_betek1**:



Resumen

ARN: arn:aws:iam::933028198366:user/test_betek1
Creado: July 22, 2024, 21:39 (UTC-05:00)

Acceso a la consola: Habilidades sin MFA
Último inicio de sesión en la consola: Hoy

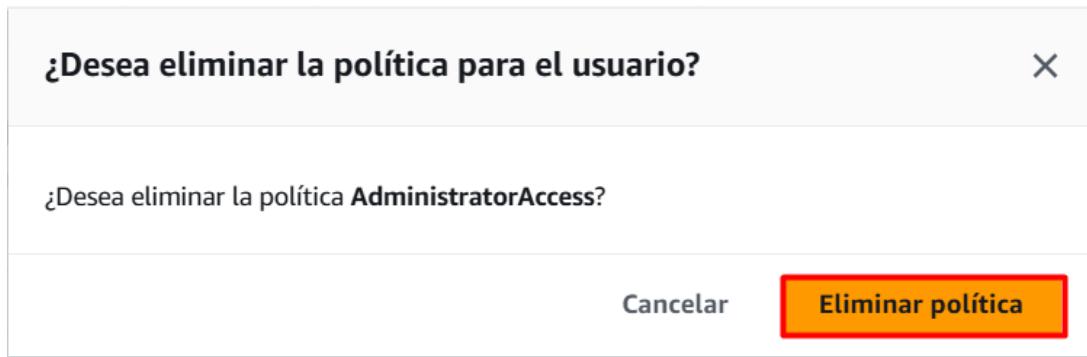
Clave de acceso 1: Crear clave de acceso

Permisos Grupos Etiquetas Credenciales de seguridad Access Advisor

Políticas de permisos (1/2)
Los permisos se definen mediante políticas asociadas al usuario directamente o a través de grupos.

Nombre de la política	Tipo	Adjuntado a través de
<input checked="" type="checkbox"/> AdministratorAccess	Administrada por AWS: función de trabajo	Directamente
<input type="checkbox"/> IAMUserChangePassword	Administrada por AWS	Directamente

Confirmamos que queremos eliminar la política:



12. Si regresamos a la sesión del usuario **test_betek1**, damos F5 o refreshcamos la página ya no debería tener acceso a ver los recursos de EC2, ni de RDS, ni ningún otro recurso:

The screenshot shows the AWS EC2 Global View dashboard. On the left, there's a sidebar with navigation links like 'Panel de EC2', 'Instancias', 'Imagenes', and 'Elastic Block Store'. The main area has sections for 'Recursos' (Resources) and 'Atributos de la cuenta' (Account Attributes). The 'Recursos' section lists various EC2 components with error status indicators. The 'Atributos de la cuenta' section shows an error message about a VPC search. There are also tabs for 'Configuración' (Configuration), 'Información adicional' (Additional Information), and links to 'Guía de introducción' (Getting Started Guide) and 'Documentación' (Documentation).

The screenshot shows the AWS RDS service page under 'Bases de datos'. The sidebar includes links for 'Panel', 'Bases de datos', and 'Grupos de subredes'. The main content displays an error message about a user lacking permissions for RDS actions. Below the message is a table for managing databases, with a prominent orange 'Crear base de datos' (Create database) button.

GRUPOS

Para evitar esto de estar asignando y quitando permisos a los usuarios, lo más recomendable es, primero crear grupos de usuarios y luego agregar los usuarios al grupo que le corresponda, según los permisos que requiera.

En este caso, creamos un grupo de administradores y a todos los usuarios que sean administradores dentro de nuestra empresa, los agregamos a este grupo.

13. En la sesión del usuario root, vamos a la consola de **IAM**, seleccionamos **Grupos de usuarios** y damos clic en **Crear un grupo**:

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, there's a sidebar with 'Identity and Access Management (IAM)' at the top, followed by 'Panel', 'Administración del acceso', and 'Grupos de usuarios' which is highlighted with a red box. Below these are 'Usuarios', 'Roles', and 'Políticas'. The main content area is titled 'Grupos de usuarios (1) Información'. It says 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.' There's a search bar, a delete button ('Eliminar'), and a 'Crear un grupo' button. A table lists one group: 'Nombre del grupo' (admin_users), 'Usuarios' (1), 'Permisos' (Defined), and 'Hora de creación' (Hace 15 días). Navigation icons like back, forward, and refresh are at the bottom.

Asignamos un nombre al grupo de usuarios, en este caso será **admin**, si ya tenemos usuarios creados para agregar al grupo, los seleccionamos, asignamos la política **AdministratorAccesss** y al final de la página damos clic en **Crear grupo de usuarios**:

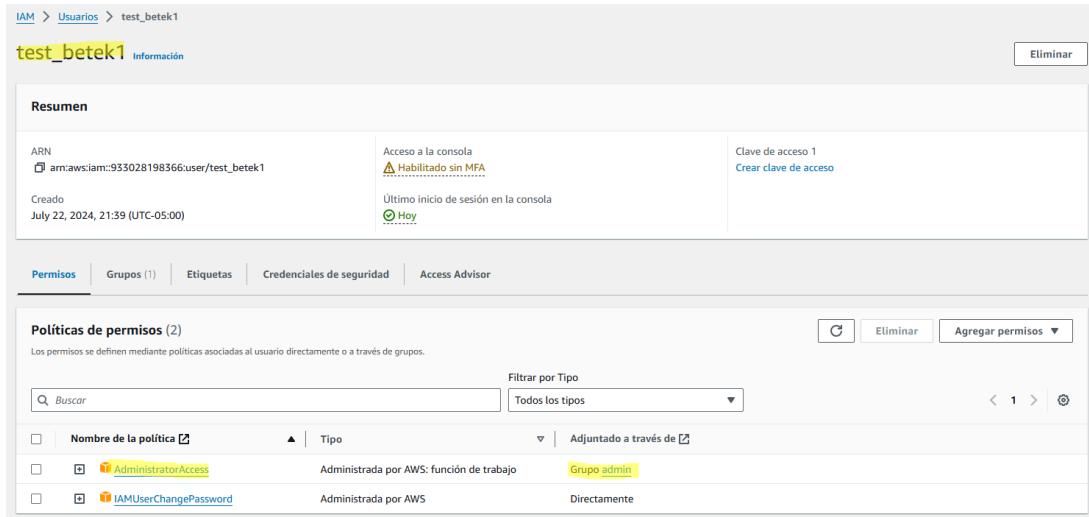
This is a three-step wizard for creating a new IAM group:

- Asignar un nombre al grupo:** The 'Nombre del grupo de usuarios' field contains 'admin' (highlighted with a red box). A note below says '128 caracteres como máximo. Utilice caracteres alfanuméricos y '+-,.,@-_.'
- Agregar usuarios al grupo: opcional (1/2) Información:** Shows a table with two users: 'adm_lore' and 'test_betek1' (highlighted with a red box). The 'test_betek1' row has a checked checkbox.
- Asociar políticas de permisos: opcional (1/950) Información:** Shows a table with two policies: 'AdministratorAccess' (checked and highlighted with a red box) and 'AdministratorAccess-Am...'.

Y así de fácil ya tenemos creado el grupo de administradores, donde tenemos el usuario **test_betek1**:

The screenshot shows the 'Grupos de usuarios' page again. A green banner at the top says 'Grupo de usuarios admin creado.' (Group 'admin' created). The main table now shows two groups: 'admin' (1 user, defined, created now) and 'admin_users' (1 user, defined, created 15 days ago).

14. Regresamos al usuario **test_betek1** y encontramos que nuevamente el usuario tiene la política de administrador, pero esta vez no se le agregó directamente sino a través de un grupo:



Resumen

ARN: arn:aws:iam::933028198366:user/test_betek1
Creado: July 22, 2024, 21:39 (UTC-05:00)

Acceso a la consola: Habilitado sin MFA
Último inicio de sesión en la consola: Hoy

Clave de acceso 1: Crear clave de acceso

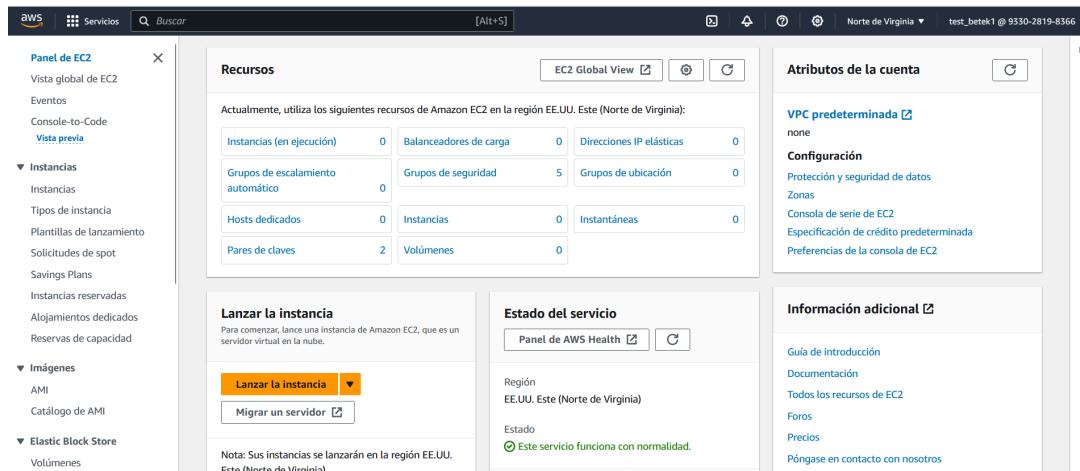
Permisos | Grupos (1) | Etiquetas | Credenciales de seguridad | Access Advisor

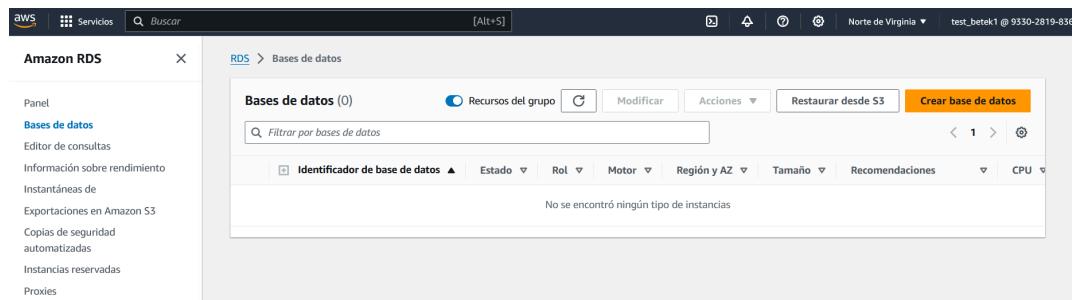
Políticas de permisos (2)

Los permisos se definen mediante políticas asociadas al usuario directamente o a través de grupos.

Nombre de la política	Tipo	Adjuntado a través de
AdministratorAccess	Administrada por AWS: función de trabajo	Grupo admin
AmazonUserChangePassword	Administrada por AWS	Directamente

Si regresamos a la sesión del usuario **test_betek1**, damos F5 y refrescamos la página, vamos a ver cómo este usuario otra vez puede ver todos los recursos (EC2, RDS y demás servicios de AWS) porque nuevamente tiene los permisos para ello:





15. Regresemos a la consola de IAM y vamos a crear otro grupo.

Supongamos que tenemos algunos administradores de bases de datos y queremos crear un grupo para ellos.

El grupo se va a llamar ***dba_admin***, agregamos los usuarios (en este caso no tenemos usuarios para agregar porque el usuario **test_betek1** ya tiene full access y no tiene sentido agregarlo a este grupo), buscamos la política **DatabaseAdministrator**, la seleccionamos y automáticamente se agregan los permisos necesarios para administrar bases de datos en la cuenta de AWS.

Damos clic en **Crear grupo de usuarios**:

The screenshot shows the 'Create New Group' wizard with three steps:

- Step 1: Assign a group name**: The 'Nombre del grupo de usuarios' field contains 'dba_admin'. Step number '1' is highlighted in red in the top-left corner of this section.
- Step 2: Add users to the group (optional)**: Shows a list of users: 'adm_lore' and 'test_betek1'. Step number '2' is highlighted in red in the top-left corner of this section.
- Step 3: Associate permissions (optional)**: Shows a list of policies. The 'DatabaseAdministrator' policy is selected, highlighted with a blue border. Step number '3' is highlighted in red in the top-left corner of this section.

At the bottom right of the third step, there are 'Cancelar' and 'Crear grupo de usuarios' buttons, with 'Crear grupo de usuarios' highlighted by a red rectangle.

CREACIÓN DE KMS KEY

1. Ir la a consola
2. Buscamos KMS en el explorador de la consola:

The screenshot shows the AWS CloudFront console with a search bar at the top containing 'kms'. Below the search bar, there are two main sections: 'Services' and 'Features'. In the 'Services' section, the 'Key Management Service' is listed with a blue icon and the description 'Securely Generate and Manage AWS Encryption Keys'. In the 'Features' section, 'Custom key stores' is listed with a blue icon and the description 'Key Management Service feature'. To the right of these sections, there is a sidebar with a 'Create application' button and a search bar for 'Find applications'. The status bar at the bottom indicates 'United States (N. Virginia)' and 'Entrenamiento (0:40:3:447:0)'.

3. Creamos nuestra primera key

The screenshot shows the 'Configure key' wizard. Step 1: Set Key Type. It has two options: 'Symmetric' (selected) and 'Asymmetric'. Step 2: Set Key Usage. It has two options: 'Encrypt and decrypt' (selected) and 'Generate and verify MAC'. At the bottom, there is a 'Next' button.

4. Nos asignamos como administradores de la key

Define key administrative permissions - *optional*

Key administrators (86)

Select the IAM users and roles authorized to manage this key via the KMS API. These administrators will be added to the key policy under the statement identifier (Sid) 'Allow administration of the key'. Modifying this Sid might impact the console's ability to update the administrator statement in the key policy. [Learn more](#)

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	a.andres1538@gmail.com	/students/	User
<input type="checkbox"/>	alemova.1603@gmail.com	/students/	User
<input type="checkbox"/>	andrea3578@hotmail.com	/students/	User
<input type="checkbox"/>	andresortizbedoya20@gmail.com	/students/	User
<input type="checkbox"/>	anggonpad@gmail.com	/students/	User
<input type="checkbox"/>	adctizahlo6@gmail.com	/students/	User

5. Definimos quién puede usar esa key:

The screenshot shows the 'Key users (86)' section of the AWS IAM console. It lists various IAM users and roles, each with a checkbox, a name, a path, and a type (Role). The users listed include 'GithubActionsAwsOrganizationsCI_CD', 'gluetos5', 'lambda-s3-read-only', 'lambda_function-role-pi9r143a', 'lambda_test-role-zusicaam', and 'OrganizationStack-AWS...'. The table has columns for Name, Path, Type, and a checkbox header.

Desde la consola desde la cloudshell, podemos simular el cifrado.

- Con este comando, solo crea un archivo con un texto:

```
echo -n "PasswordProduccion2026!" > secret.txt
```

- Para cifrar corremos este comando, ajustando el valor al de nuestra llave:

```
aws kms encrypt \  
--key-id alias/app-prod-key \  
--plaintext fileb://secret.txt \  
--query CiphertextBlob \  
--output text > secret.encrypted
```

The screenshot shows the AWS KMS 'Customer managed keys' page. A success message at the top indicates a new key was created with alias 'Key' and key ID '66d16d72-f592-4b8d-934d-ceb8bdb822fc'. Below this, a table lists the customer-managed key 'Key' with its details: Alias 'Key', Key ID '66d16d72-f592-4b8d-934d-ceb8bdb822fc', Status 'Enabled', Key type 'Symmetric', and Key spec 'SYMMETRIC_DEFAULT'. At the bottom, a CloudShell terminal window shows the execution of the AWS CLI command to encrypt the file 'secret.txt' using the specified key alias. The terminal output includes the base64 encoded ciphertext.

Ahora, tenemos un secreto cifrado en base64.

¿Qué ocurrió?

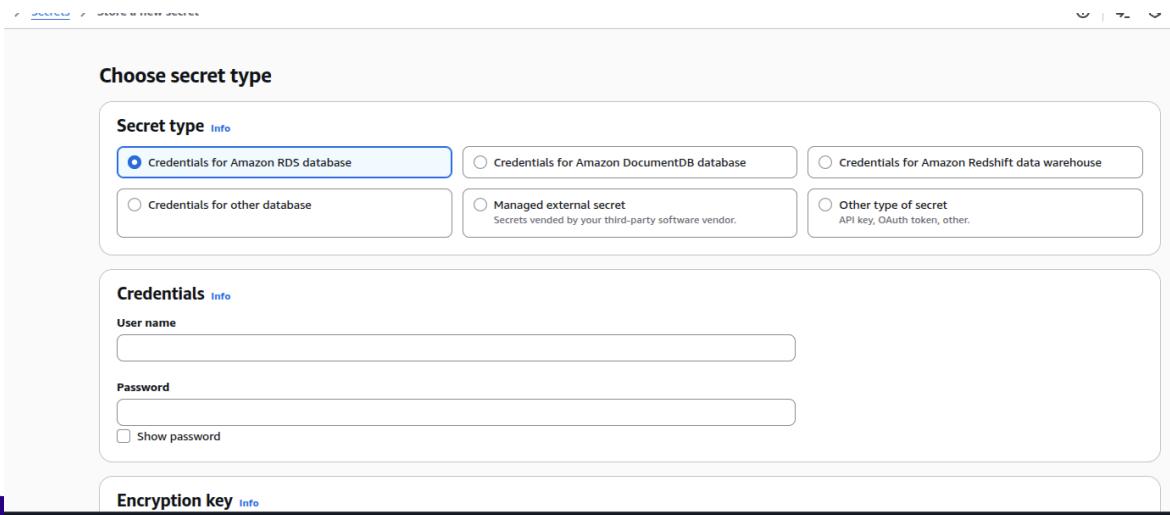
- CLI envió binario
 - KMS generó una data key
 - Cifró el texto
 - Devolvió el blob cifrado
-
- Para desencriptar

```
aws kms decrypt \
--ciphertext-blob fileb://<(base64 -d secret.encrypted) \
--query Plaintext \
--output text | base64 --decode
```

Solo quien tenga permiso **kms :Decrypt** puede hacerlo.

USUARIOS SECRETS MANAGER

1. En la consola, vamos al servicio Secrets Manager y luego a Store new secret



2. Ponemos en texto plano:

```
{  
    "username": "app_user",  
    "password": "PasswordFuerte2026!"  
}
```

3. Necesitamos una política de IAM que permita usar el secreto

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "secretsmanager:GetSecretValue",  
            "Resource":  
                "arn:aws:secretsmanager:us-east-1:654654478122:secret:prod/app/db-credentials-*"  
        }  
    ]  
}
```

4. Para ejemplo práctico crearemos un rol, el cual podrá usar dicho secreto desde una instancia:

- Creamos una instancia
- Asociamos el rol que permite el secreto
- Nos conectamos vía ssh a la ec2
- Ejecutamos:

```
aws secretsmanager get-secret-value \  
    --secret-id prod/app/db-credentials \  
    --query SecretString \  
    --output text
```

- Nos permitirá y devolverá el secreto en formato json

RECUERDA: Eliminar todos los recursos desplegados en esta práctica