

Creación de Grupos y Usuarios en AWS IAM

Introducción

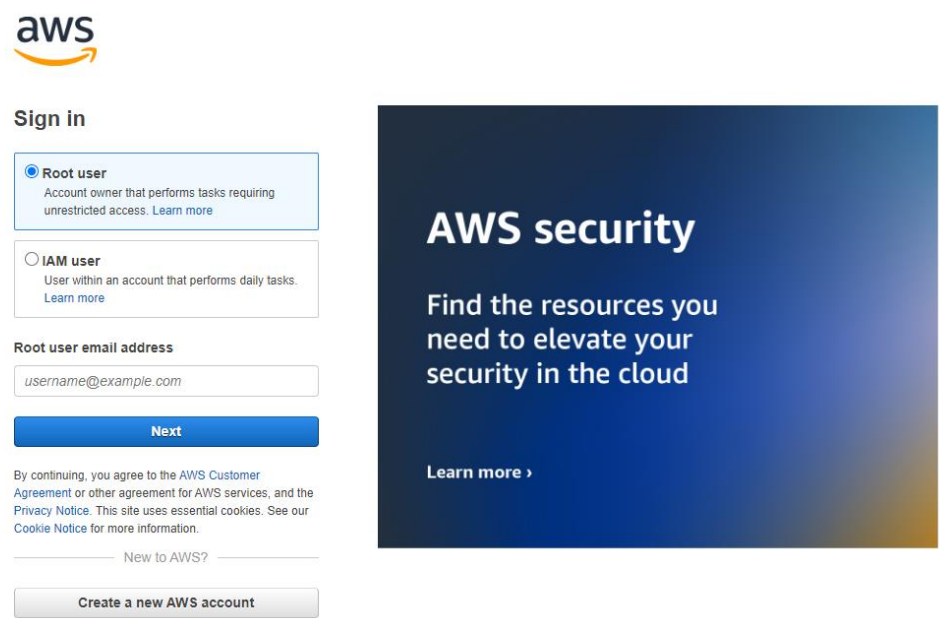
Este documento detalla los pasos necesarios para la creación de dos grupos en AWS IAM, llamados *bigdata-admin* y *bigdata-read*, asignando políticas específicas y creando usuarios para cada grupo.

Contenido

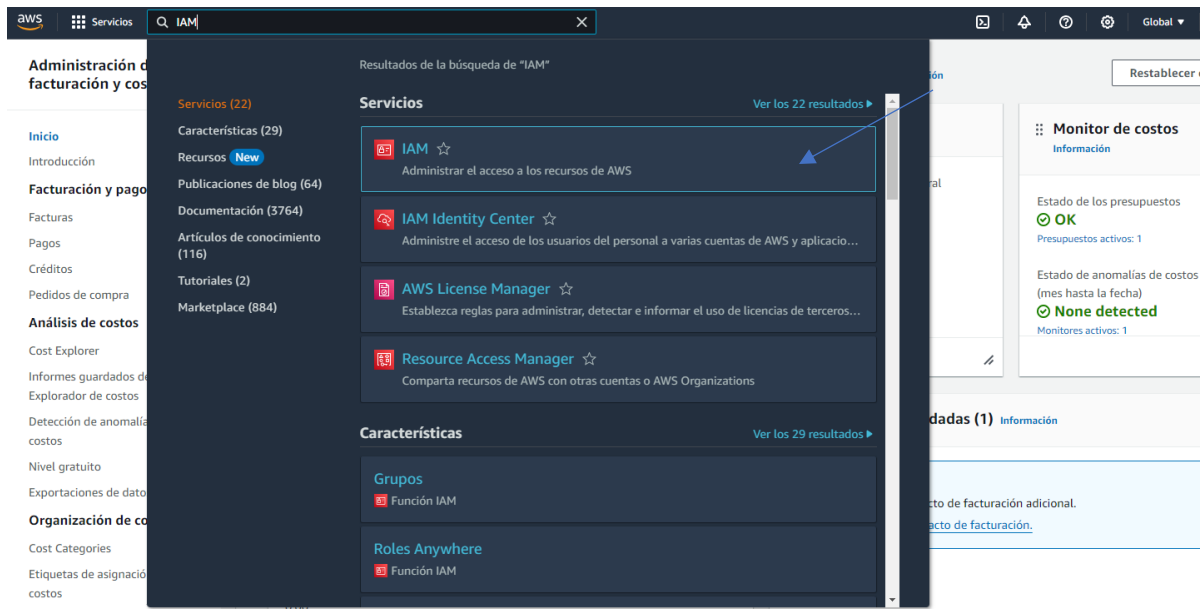
Introducción.....	1
1. Acceso a la Consola de AWS IAM.....	1
2. Creación del Grupo bigdata-admin.....	2
3. Creación del Grupo bigdata-read.....	4
4. Creación de Usuarios BD-admin y Asignación a Grupo.....	5
5. Creación de Usuarios BD-S3read y Asignación a Grupo.....	8
6. Revisión y Finalización.....	11
Conclusión	12

1. Acceso a la Consola de AWS IAM

1. Inicia sesión en la consola de administración de AWS como usuario Root.

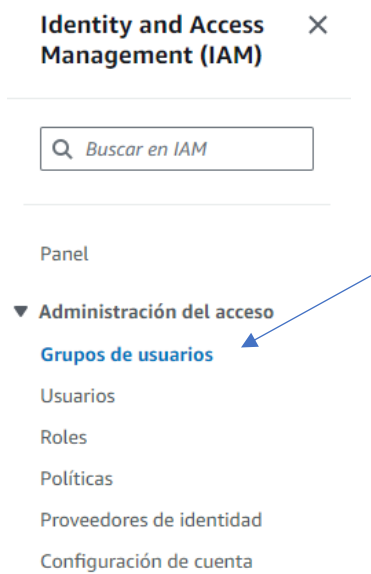


2. En la barra de búsqueda, escribe "IAM" y selecciona el servicio de **Identity and Access Management (IAM)**.

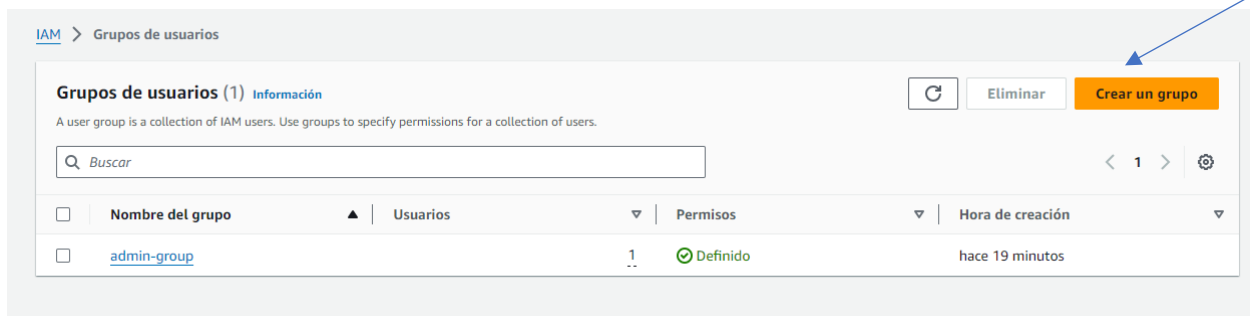


2. Creación del Grupo bigdata-admin

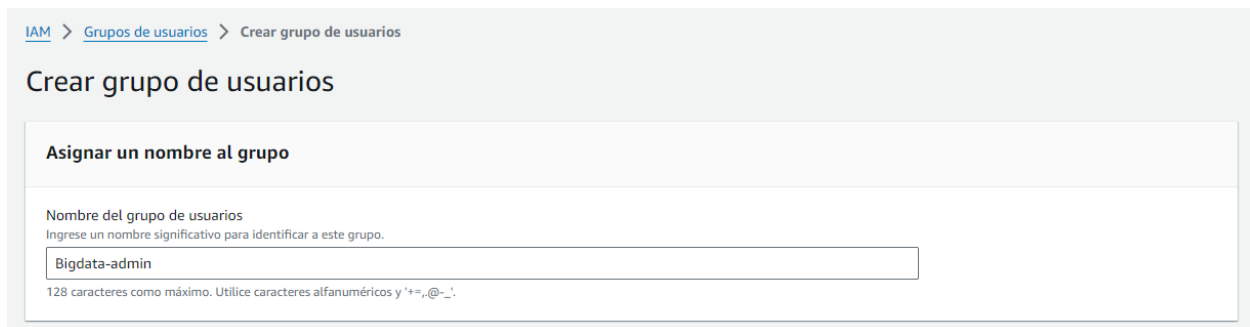
1. En el menú lateral izquierdo, selecciona **Grupos de usuarios**.



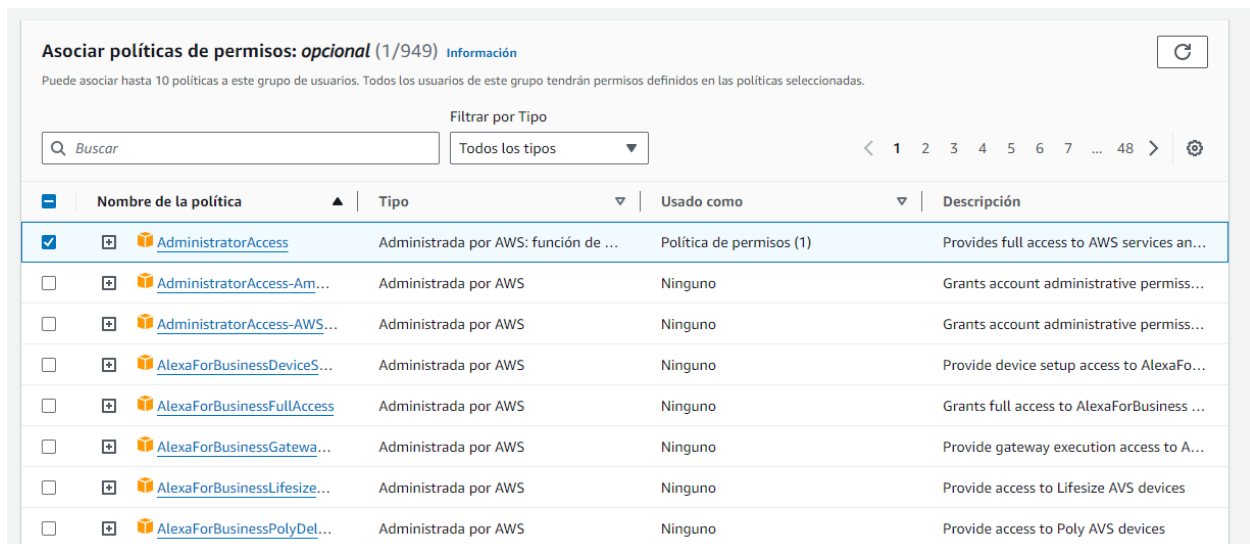
2. Haz clic en **Crear grupo**.



3. En el campo de nombre, ingresa *bigdata-admin*.



4. En la sección de políticas, busca y selecciona la política **AdministratorAccess**.



5. Haz clic en **Crear grupo de usuarios**.

<input type="checkbox"/>		Policy Name	Administrada por	Acción	Descripción
<input type="checkbox"/>		AmazonAPIGatewayPush...	Administrada por AWS	Ninguno	Allows API Gateway to push logs to us...
<input type="checkbox"/>		AmazonAppFlowFullAccess	Administrada por AWS	Ninguno	Provides full access to Amazon AppFlo...
<input type="checkbox"/>		AmazonAppFlowReadOnl...	Administrada por AWS	Ninguno	Provides read only access to Amazon A...
<input type="checkbox"/>		AmazonAppStreamFullAc...	Administrada por AWS	Ninguno	Provides full access to Amazon AppStr...
<input type="checkbox"/>		AmazonAppStreamPCAA...	Administrada por AWS	Ninguno	Amazon AppStream 2.0 access to AWS...
<input type="checkbox"/>		AmazonAppStreamRead...	Administrada por AWS	Ninguno	Provides read only access to Amazon A...
<input type="checkbox"/>		AmazonAppStreamServic...	Administrada por AWS	Ninguno	Default policy for Amazon AppStream ...
<input type="checkbox"/>		AmazonAthenaFullAccess	Administrada por AWS	Ninguno	Provide full access to Amazon Athena ...
<input type="checkbox"/>		AmazonAugmentedAIFull...	Administrada por AWS	Ninguno	Provides access to perform all operati...

3. Creación del Grupo bigdata-read

1. Una vez finalizados los pasos anteriores, aparecerá la confirmación del primer grupo creado. Ahora repite el proceso anterior, pero esta vez llama al grupo *bigdata-read*.

Grupo de usuarios Bigdata-admin creado.

IAM > Grupos de usuarios

Grupos de usuarios (2) Información

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Buscar

<input type="checkbox"/>	Nombre del grupo	Usuarios	Permisos	Hora de creación
<input type="checkbox"/>	admin-group	1	Definido	hace 24 minutos
<input type="checkbox"/>	Bigdata-admin	0	Definido	Ahora

IAM > Grupos de usuarios > Crear grupo de usuarios

Crear grupo de usuarios

Asignar un nombre al grupo

Nombre del grupo de usuarios

Ingrese un nombre significativo para identificar a este grupo.

Bigdata-read

128 caracteres como máximo. Utilice caracteres alfanuméricos y '+', '@', '-', '_'.

2. Busca en las políticas el servicio AmazonS3 y elegimos **AmazonS3ReadOnlyAccess**, luego haz clic en el botón **Crear grupo de usuarios**

The screenshot shows the 'Asociar políticas de permisos' (Associate permissions policies) page in the AWS IAM console. The search bar contains 'amazons3' and the filter is set to 'Todos los tipos' (All types), showing 5 results. The table lists several AWS managed policies, with 'AmazonS3ReadOnlyAccess' selected. A blue arrow points to the search bar, and another points to the 'AmazonS3ReadOnlyAccess' row. At the bottom right, there are 'Cancelar' (Cancel) and 'Crear grupo de usuarios' (Create user group) buttons.

	Nombre de la política	Tipo	Usado como	Descripción
<input type="checkbox"/>	AmazonS3FullAccess	Administrada por AWS	Ninguno	Provides full access to all buckets via t...
<input type="checkbox"/>	AmazonS3ObjectLambda...	Administrada por AWS	Ninguno	Provides AWS Lambda functions permi...
<input type="checkbox"/>	AmazonS3OutpostsFullA...	Administrada por AWS	Ninguno	Provides full access to Amazon S3 on ...
<input type="checkbox"/>	AmazonS3OutpostsRead...	Administrada por AWS	Ninguno	Provides read only access to Amazon S...
<input checked="" type="checkbox"/>	AmazonS3ReadOnlyAccess	Administrada por AWS	Ninguno	Provides read only access to all bucket...

4. Creación de Usuarios BD-admin y Asignación a Grupo

1. En el menú lateral izquierdo, selecciona **Usuarios**.

The screenshot shows the 'Identity and Access Management (IAM)' console. In the left-hand navigation menu, under 'Administración del acceso' (Access administration), the 'Usuarios' (Users) option is highlighted with a blue arrow. The main content area shows a search bar labeled 'Buscar en IAM' (Search in IAM).

2. Haz clic en **Agregar usuario**.



3. Ingresa el nombre de usuario para el primer usuario que será asignado al grupo *bigdata-admin* (en nuestro caso, *BD-admin*), tilda la opción **Proporcione acceso a usuario a la consola de administración de AWS**, y elije la opción **Quiero crear un usuario de IAM**.

Especificar los detalles del usuario

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 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. Es recomendable crear una contraseña personalizada, como opcional puedes tildar la opción de crear nueva contraseña en el siguiente inicio de sesión, para que cada usuario pueda personalizarla, luego presiona el botón **Siguiente**.

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), números (0-9) y símbolos ! @ # \$ % ^ & * () _ + - (guion) = [] { } | ' "

☒ **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.

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. En la sección de permisos, selecciona la opción **Agregar usuario a un grupo** y elige el grupo *bigdata-admin*, luego presiona en **Siguiente**.

Establecer permisos

Agregue un usuario a un grupo existente o cree uno nuevo. El uso de grupos es una práctica recomendada para administrar los permisos de usuario según las funciones laborales. [Más información](#)

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, le sugerimos, en cambio, adjuntar políticas a un grupo. A continuación, agregue el usuario al grupo adecuado.

Grupos de usuarios (1/3)

Q Buscar

< 1 > ⚙

	Nombre del grupo	Usuarios	Políticas adjuntas	Creado
<input type="checkbox"/>	admin-group	1	AdministratorAccess	2024-09-18 (hace 33 minutos)
<input checked="" type="checkbox"/>	Bigdata-admin	0	AdministratorAccess	2024-09-18 (hace 9 minutos)
<input type="checkbox"/>	Bigdata-read	0	AmazonS3ReadOnlyAccess	2024-09-18 (hace 5 minutos)

► Establecer límite de permisos: *opcional*

Cancelar Anterior **Siguiente**

6. Chequea si la información es correcta, y presiona el botón **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 BD-admin	Tipo de contraseña de consola Custom password	Exigir el restablecimiento de la contraseña No
-------------------------------	--	---

Resumen de permisos

< 1 >

Nombre	Tipo	Usado como
Bigdata-admin	Grupo	Grupo de permisos

Etiquetas : *opcional*

Las etiquetas son pares clave-valor que puede agregar a los recursos de AWS para ayudar a identificar, organizar o buscar recursos. Elija las etiquetas que desee asociar a este usuario.

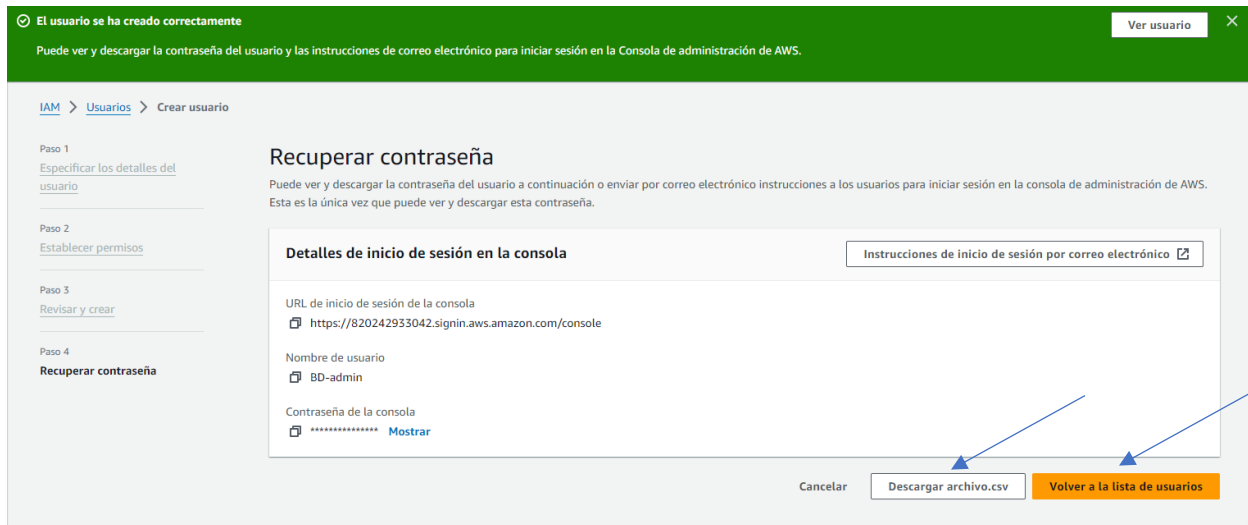
No hay etiquetas asociadas al recurso.

Agregar nueva etiqueta

Puede agregar hasta 50 etiqueta más.

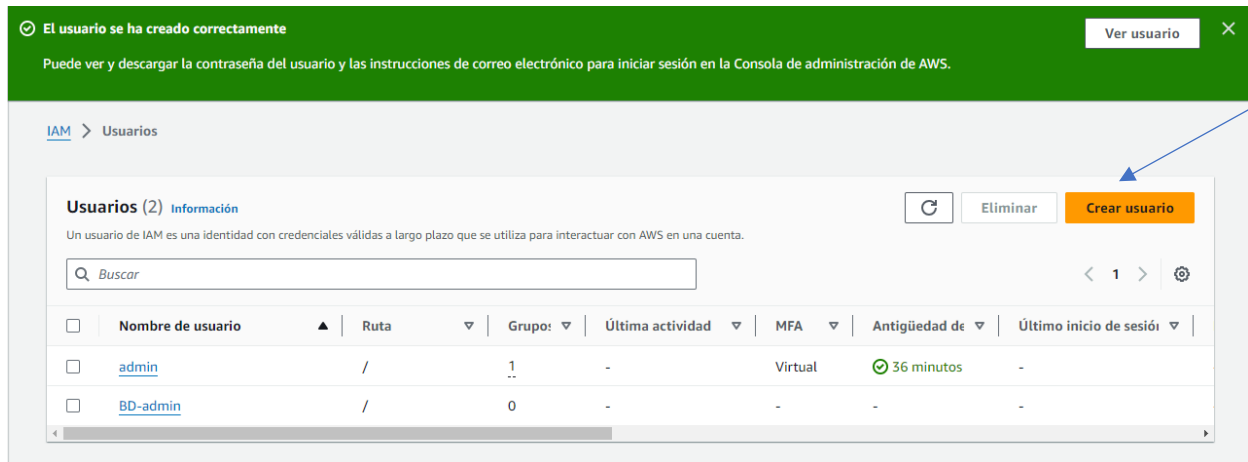
Cancelar Anterior **Crear usuario**

7. Aparecerá un cartel de confirmación de usuario creado, opcional puedes descargar el archivo csv con la información del usuario creado, para volver a la pantalla principal presiona **Volver a la lista de usuarios**.



5. Creación de Usuarios BD-S3read y Asignación a Grupo

1. Repite el proceso para el segundo usuario, que será asignado al grupo *bigdata-read* (en nuestro caso, *BD-S3read*)



Especificar los detalles del usuario

Detalles del usuario

Nombre de usuario

BD-S3read

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.

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), números (0-9) y símbolos ! @ # \$ % ^ & * () _ + - (guion) = [] { } ' "

☒ **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.

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

2. Selecciona en este caso el grupo Bigdata-read

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, le sugerimos, en cambio, adjuntar políticas a un grupo. A continuación, agregue el usuario al grupo adecuado.

Grupos de usuarios (1/3)

Buscar

< 1 > ⚙

	Nombre del grupo	Usuarios	Políticas adjuntas	Creado
<input type="checkbox"/>	admin-group	1	AdministratorAccess	2024-09-18 (hace 42 minutos)
<input type="checkbox"/>	Bigdata-admin	0	AdministratorAccess	2024-09-18 (hace 18 minutos)
<input checked="" type="checkbox"/>	Bigdata-read	0	AmazonS3ReadOnlyAccess	2024-09-18 (hace 14 minutos)

► Establecer límite de permisos: *opcional*

Cancelar

Anterior

Siguiente

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 BD-S3read	Tipo de contraseña de consola Custom password	Exigir el restablecimiento de la contraseña No
--------------------------------	--	---

Resumen de permisos < 1 >

Nombre	Tipo	Usado como
Bigdata-read	Grupo	Grupo de permisos

Etiquetas : opcional
Las etiquetas son pares clave-valor que puede agregar a los recursos de AWS para ayudar a identificar, organizar o buscar recursos. Elija las etiquetas que desee asociar a este usuario.

No hay etiquetas asociadas al recurso.

Agregar nueva etiqueta

Puede agregar hasta 50 etiqueta más.

Cancelar Anterior **Crear usuario**

El usuario se ha creado correctamente Ver usuario X
Puede ver y descargar la contraseña del usuario y las instrucciones de correo electrónico para iniciar sesión en la Consola de administración de AWS.

[IAM](#) > [Usuarios](#) > Crear usuario

Paso 1
[Especificar los detalles del usuario](#)

Paso 2
[Establecer permisos](#)

Paso 3
[Revisar y crear](#)

Paso 4
Recuperar contraseña

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 Instrucciones de inicio de sesión por correo electrónico

URL de inicio de sesión de la consola
 <https://820242933042.signin.aws.amazon.com/console>

Nombre de usuario
 BD-S3read

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

Cancelar Descargar archivo.csv **Volver a la lista de usuarios**

6. Revisión y Finalización

1. Revisa la configuración de cada usuario y asignaciones de políticas, para eso haz clic en el nombre de usuario.

El usuario se ha creado correctamente

Ver usuario

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

IAM > Usuarios

Usuarios (3) Información

Eliminar

Crear usuario

Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.

Buscar

< 1 >

<input type="checkbox"/>	Nombre de usuario	Ruta	Grupo	Última actividad	MFA	Antigüedad de	Último inicio de sesión
<input type="checkbox"/>	admin	/	1	-	Virtual	42 minutos	-
<input type="checkbox"/>	BD-admin	/	1	-	-	-	-
<input type="checkbox"/>	BD-S3read	/	0	-	-	-	-

IAM > Usuarios > BD-admin

BD-admin Información

Eliminar

Resumen

ARN
arn:aws:iam::820242933042:user/BD-admin

Acceso a la consola
Habilitado sin MFA

Clave de acceso 1
Crear clave de acceso

Creado
September 18, 2024, 21:50 (UTC-03:00)

Último inicio de sesión en la consola
Nunca

Permisos

Grupos (1)

Etiquetas

Credenciales de seguridad

Access Advisor

Políticas de permisos (1)

Eliminar

Agregar permisos

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

Buscar

Filtrar por Tipo
Todos los tipos

< 1 >

<input type="checkbox"/>	Nombre de la política	Tipo	Adjuntado a través de
<input type="checkbox"/>	AdministratorAccess	Administrada por AWS: función de trabajo	Grupo Bigdata-admin

IAM > Usuarios > BD-S3read

BD-S3read Información

Eliminar

Resumen

ARN
arn:aws:iam::820242933042:user/BD-S3read

Acceso a la consola
Habilitado sin MFA

Clave de acceso 1
Crear clave de acceso

Creado
September 18, 2024, 21:58 (UTC-03:00)

Último inicio de sesión en la consola
Nunca

Permisos

Grupos (1)

Etiquetas

Credenciales de seguridad

Access Advisor

Políticas de permisos (1)

Eliminar

Agregar permisos

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

Buscar

Filtrar por Tipo
Todos los tipos

< 1 >

<input type="checkbox"/>	Nombre de la política	Tipo	Adjuntado a través de
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	Administrada por AWS	Grupo Bigdata-read

2. Se recomienda realizar un MFA (Autenticación multifactor) para cada usuario, para eso aprieta en el botón de advertencia que dice Habilitado sin MFA, ingresa luego el nombre del dispositivo, y elije alguna de las opciones que más se ajuste a tu dispositivo.

Seleccionar el dispositivo MFA [Info](#)

MFA device name

Nombre del dispositivo
Este nombre se utilizará en el ARN de identificación de este dispositivo.

Máximo de 64 caracteres. Utilice caracteres alfanuméricos y "+", ".", "@", "-", "_".

MFA device

Opciones de dispositivo
Además del nombre de usuario y la contraseña, utilizará este dispositivo para autenticarse en la cuenta.

☐**Clave de paso o clave de seguridad**
Autentíquese mediante la huella digital, el rostro o el bloqueo de pantalla. Cree una clave de paso en este dispositivo o use otro dispositivo, como una clave de seguridad FIDO2.

☒**Aplicación del autenticador**
Autenticarse mediante un código generado por una aplicación instalada en el dispositivo móvil o la computadora.

☐**Token de contraseña temporal de un solo uso (TOTP) de hardware**
Autentíquese mediante un código generado por el token de TOTP de hardware u otros dispositivos de hardware.

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

Conclusión

En este informe hemos descrito el proceso para crear dos grupos en AWS IAM con permisos diferenciados y asignar usuarios a dichos grupos. Estos pasos aseguran la gestión adecuada de permisos en un entorno de Big Data.

Martin Carlos Carchano Vargas

12