

Creación de Política

Buscamos el servicio de IAM

The screenshot shows the AWS IAM service search results in the AWS console. The search bar at the top contains the text "iam". The results are displayed in a dark-themed sidebar on the left and a main content area on the right.

Servicios (20)

- Características (29)
- Recursos **New**
- Blogs (60)
- Documentación (3274)
- Artículos de conocimiento (119)
- Tutoriales (2)
- Marketplace (802)

Resultados de la búsqueda de "iam"

Servicios [Ver los 20 resultados ►](#)

- IAM** ☆
Administrar el acceso a los recursos de AWS
- IAM Identity Center** ☆
Administre el acceso de los usuarios del personal a varias cuentas de AWS y aplicacio...
- AWS License Manager** ☆
Establezca reglas para administrar, detectar e informar el uso de licencias de terceros...
- Resource Access Manager** ☆
Comparta recursos de AWS con otras cuentas o AWS Organizations

Características [Ver los 29 resultados ►](#)

- Grupos**
- Función IAM**

Nos aparecerá la siguiente pantalla y escogeremos la opción de “Políticas”

Identity and Access Management (IAM)

Panel

Administración del acceso

- Grupos de usuarios
- Usuarios
- Roles
- Políticas**
- Proveedores de identidad
- Configuración de cuenta

Panel de IAM

Recomendaciones de seguridad 0

- El usuario raíz tiene MFA
- Cuenta con MFA
- El usuario Backend no tiene claves de acceso activas que no hayan sido utilizadas durante más de un año.

Cuenta de AWS

ID de cuenta

Alias de cuenta

URL de inicio de sesión para los usuarios de IAM de esta cuenta

Le damos Click en “Crear política”

Identity and Access Management (IAM)

Panel

Administración del acceso

- Grupos de usuarios
- Usuarios
- Roles
- Políticas**
- Proveedores de identidad
- Configuración de cuenta

Políticas (1200) Información

Una política es un objeto en AWS que define permisos.

Filtrar por Tipo

Buscar

Todos los tipos

Acciones

Eliminar

Crear política

	Nombre de la política	Tipo	Usado como	Descripción
	AccessAnalyzerService...	Administrada por AWS	Ninguno	-
	AdministratorAccess	Administrada por AWS: función...	Política de permisos (2)	Provides full access to AWS services an...
	AdministratorAccess-...	Administrada por AWS	Ninguno	Grants account administrative permissi...
	AdministratorAccess-...	Administrada por AWS	Ninguno	Grants account administrative permissi...
	AlexaForBusinessDevi...	Administrada por AWS	Ninguno	Provide device setup access to AlexaFo...

Nos aparecerá la siguiente pantalla

[IAM](#) > [Políticas](#) > Crear política


Paso 1
Especificar permisos

Paso 2
Revisar y crear

Especificar permisos [Información](#)

Agregue permisos seleccionando servicios, acciones, recursos y condiciones. Cree instrucciones de permisos con el editor JSON.

Editor de políticas

VisualJSONAcciones 

▼ Seleccionar un servicio

Especifique qué acciones se pueden realizar en recursos específicos de un servicio.

Servicio

Elegir un servicio ▼

+ Agregar más permisos

Cancelar **Siguiente**

Escogemos la opción “Json” y nos mostrará lo siguiente:

Especificar permisos Información

Agregue permisos seleccionando servicios, acciones, recursos y condiciones. Cree instrucciones de permisos con el editor JSON.

Editor de políticas

VisualJSONAcciones ▼

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": [],  
8       "Resource": []  
9     }  
10  ]  
11 }
```

Editar instrucción
Statement1Eliminar

Agregar acciones

Elegir un servicio

Disponible

AMP

API Gateway

API Gateway V2

ASC

Access Analyzer

Account

Activate

Alexa for Business

Amplify

Amplify Admin

En la caja de “Elegir un servicio” escribimos “S3” y nos mostrará la opción del S3

Especificar permisos [Información](#)

Agregue permisos seleccionando servicios, acciones, recursos y condiciones. Cree instrucciones de permisos con el editor JSON.

Editor de políticas

Visual

JSON

Acciones ▼



```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": [],  
8       "Resource": []  
9     }  
10  ]  
11 }
```

Editar instrucción

Eliminar

Agregar acciones

Elegir un servicio

Q s3 X

Disponible

S3

S3 Express

S3 Object Lambda

S3 Outposts

Una vez seleccionado el servicio, buscaremos el permiso de “ListAllMyBuckets”

Especificar permisos [Información](#)

Agregue permisos seleccionando servicios, acciones, recursos y condiciones. Cree instrucciones de permisos con el editor JSON.

Editor de políticas

Visual

JSON

Acciones ▼



```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": [],  
8       "Resource": []  
9     }  
10  ]  
11 }
```

Editar instrucción

Eliminar

Statement1

Agregar acciones

Todos los servicios > S3

🔍 Filtrar acciones

☐ All actions (s3:*)

Nivel de acceso: lista

☐ ListAccessGrants [Información](#)

☐ ListAccessGrantsInstances [Información](#)

☐ ListAccessGrantsLocations [Información](#)

☐ ListAccessPoints [Información](#)

☐ ListAccessPointsForObjectLambda

[Información](#)

☐ ListAllMyBuckets [Información](#)

☐ ListBucket [Información](#)

Veremos que en nuestro Json en el apartado de “Action” ya se agregó el permiso, ahora vamos a agregar nuestro recurso

Especificar permisos [Información](#)

Agregue permisos seleccionando servicios, acciones, recursos y condiciones. Cree instrucciones de permisos con el editor JSON.

Editor de políticas

Visual

JSON

Acciones ▼



```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": [  
8         "s3:ListAllMyBuckets"  
9       ],  
10      "Resource": []  
11    }  
12  ]  
13 }
```

Editar instrucción
Statement1

Eliminar

Agregar acciones

Todos los servicios > S3

listall



Nivel de acceso: lista

☒ ListAllMyBuckets [Información](#)

Nivel de acceso: lectura

Nivel de acceso: lectura o escritura

En la parte inferior le daremos en agregar recurso

The screenshot shows the AWS IAM console's policy editor. The main area displays a JSON policy document being edited. The right-hand pane shows a list of actions available for the selected resource type (s3:*). The action 'ListAllMyBuckets' is selected. At the bottom of the right pane, the 'Agregar un recurso' button is highlighted with a red line. The bottom status bar indicates the policy is in JSON format, at line 7, column 14, and has 6021 of 6144 characters remaining.

```
7  {
8    "Action": [
9      "s3:ListAllMyBuckets"
10   ],
11   "Resource": [ ]
12 }
13 }
```

Filtrar acciones

☐ All actions (s3:*)

Nivel de acceso: lista

☐ ListAccessGrants [Información](#)

☐ ListAccessGrantsInstances [Información](#)

☐ ListAccessGrantsLocations [Información](#)

☐ ListAccessPoints [Información](#)

☐ ListAccessPointsForObjectLambda [Información](#)

☒ ListAllMyBuckets [Información](#)

☐ ListBucket [Información](#)

Agregar un recurso **Agregar**

Agregar una condición (opcional) **Agregar**

+ Agregar nueva instrucción

JSON Ln 7, Col 14 6021 de 6144 caracteres restantes

Escogeremos el “S3”

The screenshot shows the AWS IAM console interface. In the background, a JSON policy is visible with the following content:

```
{
  "Action": [
    "s3:ListAllMyBuckets"
  ],
  "Resource": [
  ]
}
```

Overlaid on this is a modal dialog box titled "Agregar recurso" (Add resource). The dialog contains the following fields:

- Especifique el tipo de recurso y el ARN que desea agregar para el servicio seleccionado.** (Specify the resource type and the ARN you want to add for the selected service.)
- Servicio** (Service): A dropdown menu with "S3" selected.
- Tipo de recurso** (Resource type): A dropdown menu with "All Resources" selected.
- ARN de recurso** (Resource ARN): A text input field containing an asterisk (*).

At the bottom of the dialog are two buttons: "Cancelar" (Cancel) and "Agregar recurso" (Add resource).

Below the dialog, the console status bar shows:

- Seguridad: 0 (Security: 0)
- Errores: 0 (Errors: 0)
- Advertencias: 0 (Warnings: 0)
- Sugerencias: 1 (Suggestions: 1)

Nos va a aparecer de la siguiente forma

Editor de políticas

Visual

JSON

Acciones ▼

1 ▼

{

2

"Version": "2012-10-17",

3 ▼

"Statement": [

4 ▼

{

5

"Sid": "Statement1",

6

"Effect": "Allow",

7 ▼

"Action": [

8

"s3:ListAllMyBuckets"

9

],

10 ▼

"Resource": [

11

"*"

12

]

13

}

14

]

15

}

Editar instrucción

Seleccionar una instrucción

Seleccione una instrucción existente en la política o agregue una nueva instrucción.

+ Agregar nueva instrucción

Vamos a la parte inferior de la página y le damos en “Siguiente”

+ Agregar nueva instrucción

JSON Ln 15, Col 16018 de 6144 caracteres restantes

Seguridad: 0

Errores: 0

Advertencias: 0

Sugerencias: 0

Cancelar

Siguiente

Ahora nos va a pedir los datos para Nombre la Política y alguna descripción

Revisar y crear [Información](#)

Revise los permisos; especifique detalles y etiquetas.

Detalles de la política

Nombre de la política

Ingrese un nombre significativo para identificar a esta política.

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

Descripción: *opcional*

Agregue una breve explicación para esta política.

1000 caracteres como máximo. Utilice caracteres alfanuméricos y "+,=, @-_".

Revisar y crear [Información](#)

Revise los permisos; especifique detalles y etiquetas.

Detalles de la política

Nombre de la política

Ingrese un nombre significativo para identificar a esta política.

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

Descripción: *opcional*

Agregue una breve explicación para esta política.

1000 caracteres como máximo. Utilice caracteres alfanuméricos y '+', '@', '-'.

Nos aparecerá la siguiente pantalla y le damos en “Crear Política”

Permisos definidos en esta política [Información](#)

Editar

Los permisos definidos en este documento de política especifican qué acciones se permiten o deniegan. Para definir permisos para una identidad de IAM (usuario, grupo de usuarios o rol), asóciela a una política

Q

Buscar

Permitir (1 de 415 servicios)

☐ Mostrar los 414 servicios restantes

Servicio	Nivel de acceso	Recurso	Condición de solicitud
S3	Limitado: Enumerar	Todos los recursos	None

Agregar etiquetas - *opcional* [Información](#)

Las etiquetas son pares clave-valor que puede agregar a los recursos de AWS para que sea más fácil identificarlos, organizarlos o buscarlos.

No hay etiquetas asociadas al recurso.

Agregar nueva etiqueta

Puede agregar hasta 50 etiqueta más.

Cancelar

Anterior

Crear política

Nos aparecerá esta pantalla donde nos muestra el mensaje de que la política ya se creó

Se creó la política s3_read_only_list.

Ver la política

Políticas (1201) Información

Una política es un objeto en AWS que define permisos.

Buscar

Filtrar por Tipo

Todos los tipos

< 1 2 3 4 5 6 7 ... 61 >

	Nombre de la política	Tipo	Usado como	Descripción
<input type="radio"/>	AlexaForBusinessRead...	Administrada por AWS	Ninguno	Provide read only access to AlexaForB...
<input type="radio"/>	AmazonAPIGatewayA...	Administrada por AWS	Ninguno	Provides full access to create/edit/dele...
<input type="radio"/>	AmazonAPIGatewayIn...	Administrada por AWS	Ninguno	Provides full access to invoke APIs in A...
<input type="radio"/>	AmazonAPIGatewayP...	Administrada por AWS	Ninguno	Allows API Gateway to push logs to us...
<input type="radio"/>	AmazonAppFlowFullA...	Administrada por AWS	Ninguno	Provides full access to Amazon AppFlo...
<input type="radio"/>	AmazonAppFlowRead...	Administrada por AWS	Ninguno	Provides read only access to Amazon A...
<input type="radio"/>	AmazonAppStreamFu...	Administrada por AWS	Ninguno	Provides full access to Amazon AppStr...
<input type="radio"/>	AmazonAppStreamPC...	Administrada por AWS	Ninguno	Amazon AppStream 2.0 access to AWS...
<input type="radio"/>	AmazonAppStreamRe...	Administrada por AWS	Ninguno	Provides read only access to Amazon A...
<input type="radio"/>	AmazonAppStreamSe...	Administrada por AWS	Ninguno	Default policy for Amazon AppStream ...

Si buscamos la Política ya nos aparecerá

[IAM](#) > Políticas

Políticas (1201) [Información](#)

Acciones ▼

Eliminar

Crear política

Una política es un objeto en AWS que define permisos.

Q s3_ X

Filtrar por Tipo

Todos los tipos ▼

1 coincidencia

< 1 > ⚙

	Nombre de la política ▲	Tipo ▼	Usado como ▼	Descripción
<input type="radio"/>	<div><div>+</div>s3_read_only_list</div>	Administrada por el cliente	Ninguno	Política solo para listar todos los Buck...

Crear Grupo de Usuarios

Buscamos el servicio de IAM

Q iam

×

Resultados de la búsqueda de "iam"

Servicios (20)

Características (29)

Recursos New

Blogs (60)


Documentación (3274)

Artículos de conocimiento (119)

Tutoriales (2)


Marketplace (802)

Servicios Ver los 20 resultados ▶


 IAM ☆

Administrar el acceso a los recursos de AWS


Características principales

 IAM Identity Center ☆

Administre el acceso de los usuarios del personal a varias cuentas de AWS y aplicacio...

 AWS License Manager ☆


Establezca reglas para administrar, detectar e informar el uso de licencias de terceros...

 Resource Access Manager ☆

Comparta recursos de AWS con otras cuentas o AWS Organizations

Características Ver los 29 resultados ▶

Grupos

 Función IAM

Damos click en Grupo de Usuarios

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with a search bar and a navigation menu. The main content area is titled 'Panel de IAM' and contains two panels. The 'Recomendaciones de seguridad' panel on the left lists three security recommendations, all marked with green checkmarks: 'El usuario raíz tiene MFA', 'Cuenta con MFA', and 'El usuario Backend no tiene claves de acceso activas que no hayan sido utilizadas durante más de un año.' The 'Cuenta de AWS' panel on the right displays account details, including the account ID (redacted), account alias, and the login URL (redacted).

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 > Panel

Panel de IAM

Recomendaciones de seguridad 0

El usuario raíz tiene MFA
Al contar con la autenticación multifactor (MFA) para el usuario raíz se mejora la seguridad de esta cuenta.

Cuenta con MFA
Al contar con la autenticación multifactor (MFA) para el usuario de IAM se mejora la seguridad de esta cuenta.

El usuario Backend no tiene claves de acceso activas que no hayan sido utilizadas durante más de un año.
La desactivación o la eliminación de claves de acceso no utilizadas mejora la seguridad.

Cuenta de AWS

ID de cuenta
[Redacted]

Alias de cuenta
Crear

URL de inicio de sesión para los usuarios de IAM de esta cuenta
[Redacted]

Nos aparecerá una ventana en la que pondremos el nombre del grupo de usuarios

The screenshot shows the AWS IAM console interface for creating a new user group. The top navigation bar includes the AWS logo, 'Servicios', a search bar, and a '[Alt+S]' shortcut. The left sidebar shows the 'Identity and Access Management (IAM)' menu with 'Grupos de usuarios' highlighted. The main content area is titled 'Crear grupo de usuarios' and contains a section 'Asignar un nombre al grupo'. This section includes a text input field for the group name, which currently contains 's3_accest_only_list'. Below the input field, a note states: '128 caracteres como máximo. Utilice caracteres alfanuméricos y '+=,.,@-_'.

aws | Servicios | Buscar [Alt+S]

Identity and Access Management (IAM) ×

Buscar en IAM

Panel

Administración del acceso

Grupos de usuarios

Usuarios

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.

s3_accest_only_list

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

Bajamos al final de la página y le damos click en “Crear grupo de usuarios”

▼ Administración del acceso

Grupos de usuarios

Usuarios

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

▼ Informes de acceso

Access Analyzer

Acceso externo

Acceso no utilizado

Configuración del
analizador

Informe de credenciales

<input type="checkbox"/>		AmazonAPIGatewayIn...	Administrada por AWS	Ninguno	Provides full access to invoke APIs in A...
<input type="checkbox"/>		AmazonAPIGatewayP...	Administrada por AWS	Ninguno	Allows API Gateway to push logs to us...
<input type="checkbox"/>		AmazonAppFlowFullA...	Administrada por AWS	Ninguno	Provides full access to Amazon AppFlo...
<input type="checkbox"/>		AmazonAppFlowRead...	Administrada por AWS	Ninguno	Provides read only access to Amazon A...
<input type="checkbox"/>		AmazonAppStreamFu...	Administrada por AWS	Ninguno	Provides full access to Amazon AppStr...
<input type="checkbox"/>		AmazonAppStreamPC...	Administrada por AWS	Ninguno	Amazon AppStream 2.0 access to AWS...
<input type="checkbox"/>		AmazonAppStreamRe...	Administrada por AWS	Ninguno	Provides read only access to Amazon A...
<input type="checkbox"/>		AmazonAppStreamSe...	Administrada por AWS	Ninguno	Default policy for Amazon AppStream ...
<input type="checkbox"/>		AmazonAthenaFullAcc...	Administrada por AWS	Ninguno	Provide full access to Amazon Athena ...
<input type="checkbox"/>		AmazonAugmentedAI...	Administrada por AWS	Ninguno	Provides access to perform all operati...

Cancelar

Crear grupo de usuarios

Y la siguiente pantalla que nos va a aparecer es la lista de Grupos de usuarios donde nos aparecerá nuestro grupo creado

✔ Grupo de usuarios `s3_accest_only_list` creado.

Ver grupo



[IAM](#) > Grupos de usuarios

Grupos de usuarios (1) [Información](#)

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



Eliminar

Crear un grupo

< 1 >

<input type="checkbox"/>	Nombre del grupo ▲	Usuarios ▼	Permisos ▼	Hora de creación ▼
<input type="checkbox"/>	s3_accest_only_list	0	No definido	Ahora

Le damos click al nombre del Grupo de usuarios llamado “s3_accest_only_list” nos va a parecer lo siguiente.

Vamos a la sección de “Permisos”, le daremos click en “Añadir permisos” y después “Asociar Políticas”

s3_accest_only_list

Información

Eliminar

Resumen

Editar

Nombre del grupo de usuarios

s3_accest_only_list

Hora de creación

May 31, 2024, 22:06 (UTC-06:00)

ARN

arn:aws:iam::[redacted]:group/s3_accest_o
nly_list

Usuarios

Permisos

Access Advisor

Políticas de permisos (0)

Información

Actualizar

Simular

Eliminar

Añadir permisos

Asociar políticas

Crear política insertada

Puede asociar hasta 10 políticas administradas.

Filtrar por Tipo

Buscar

Todos los tipos

< 1 >

Configuración

Nombre de la política

Tipo

Entidades asociadas

Buscamos la Política que creamos anteriormente (s3_read_only_list)

IAM > Grupos de usuarios > s3_accest_only_list > Añadir permisos

Asociar políticas de permisos a s3_accest_only_list

► Políticas de permisos actuales (0)

Otra políticas de permisos (930)









Puede asociar hasta 10 políticas administradas a este grupo de usuarios. Todos los usuarios de este grupo heredan los permisos asociados.

Q Buscar

Filtrar por Tipo

Todos los tipos

< 1 2 3 4 5 6 7 ... 47 >

<input type="checkbox"/>	Nombre de la política	Tipo	Usado como	Descripción
<input type="checkbox"/>	<div><div>+</div><div> AdministratorAccess</div></div>	Administrada por AWS: función de trabajo	Política de permisos (2)	Provides full access to AWS services an...
<input type="checkbox"/>	<div><div>+</div><div> AdministratorAccess-Amplify</div></div>	Administrada por AWS	Ninguno	Grants account administrative permissi...
<input type="checkbox"/>	<div><div>+</div><div> AdministratorAccess-AWSElasticBeanstalk</div></div>	Administrada por AWS	Ninguno	Grants account administrative permissi...
<input type="checkbox"/>	<div><div>+</div><div> AlexaForBusinessDeviceSetup</div></div>	Administrada por AWS	Ninguno	Provide device setup access to AlexaFo...
<input type="checkbox"/>	<div><div>+</div><div> AlexaForBusinessFullAccess</div></div>	Administrada por AWS	Ninguno	Grants full access to AlexaForBusiness ...
<input type="checkbox"/>	<div><div>+</div><div> AlexaForBusinessGatewayExecution</div></div>	Administrada por AWS	Ninguno	Provide gateway execution access to A...
<input type="checkbox"/>	<div><div>+</div><div> AlexaForBusinessLifeseDelegatedAccessPo...</div></div>	Administrada por AWS	Ninguno	Provide access to Lifesize AVS devices
<input type="checkbox"/>	<div><div>+</div><div> AlexaForBusinessPolyDelegatedAccessPolicy</div></div>	Administrada por AWS	Ninguno	Provide access to Poly AVS devices

Nos aparecerá la siguiente pantalla

IAM > Grupos de usuarios > s3_accest_only_list

s3_accest_only_list

Información

Eliminar

Resumen

Editar

Nombre del grupo de usuarios

s3_accest_only_list

Hora de creación

May 31, 2024, 22:06 (UTC-06:00)

ARN

arn:aws:iam::s-113364743:group/s3_accest_o

nly_list

Usuarios

Permisos

Access Advisor

Políticas de permisos (1)

Información

Actualizar

Simular

Eliminar

Añadir permisos

Puede asociar hasta 10 políticas administradas.

Filtrar por Tipo

Buscar

Todos los tipos

<

1

>

Configurar

Nombre de la política

Tipo

Entidades asociadas

+

s3_read_only_list

Administrada por el cliente

1

Nos vamos a la parte inferior y le damos click al Botón “Siguiente”

Grupos de usuarios (1/1)

🔄

Crear un grupo

🔍 *Buscar*

< 1 >

⚙️

<input checked="" type="checkbox"/>	Nombre del grupo 🔗	▲	Usuarios	▼	Políticas adjuntas 🔗	▼	Creado	▼
<input checked="" type="checkbox"/>	s3_accest_only_list		0		s3_read_only_list		2024-05-31 (hace 18 minutos)	

▶ Establecer límite de permisos: *opcional*

Cancelar

Anterior

Siguiente

Y nos regresará a esta pantalla y veremos la política de permiso agregada a nuestro grupo de usuarios

IAM > Grupos de usuarios > s3_accest_only_list

s3_accest_only_list

Información

Eliminar

Resumen

Editar


Nombre del grupo de usuarios

s3_accest_only_list

Hora de creación

May 31, 2024, 22:06 (UTC-06:00)

ARN

 arn:aws:iam::304555555555:group/s3_accest_only_list

Usuarios

Permisos

Access Advisor

Políticas de permisos (1)

Información

Recargar

Simular

Eliminar

Añadir permisos


Puede asociar hasta 10 políticas administradas.

Buscar

Filtrar por Tipo

Todos los tipos

< 1 >

<input type="checkbox"/>	Nombre de la política	Tipo	Entidades asociadas
<input type="checkbox"/>	 s3_read_only_list	Administrada por el cliente	1

Agregar un usuario





Buscamos el servicio de IAM

The screenshot shows the AWS IAM service search results page. The search bar at the top contains the text "iam". The left sidebar lists various categories: Servicios (20), Características (29), Recursos (New), Blogs (60), Documentación (3274), Artículos de conocimiento (119), Tutoriales (2), and Marketplace (802). The main content area is titled "Resultados de la búsqueda de 'iam'" and is divided into two sections: "Servicios" and "Características". The "Servicios" section lists four services: IAM, IAM Identity Center, AWS License Manager, and Resource Access Manager. The "IAM" service is highlighted with a red box and a red underline. The "Características" section lists one feature: "Grupos".


Q iam X

Resultados de la búsqueda de "iam"

Servicios Ver los 20 resultados ▶

-  **IAM** ☆
Administrar el acceso a los recursos de AWS
- Características principales**
-  **IAM Identity Center** ☆
Administre el acceso de los usuarios del personal a varias cuentas de AWS y aplicacio...
-  **AWS License Manager** ☆
Establezca reglas para administrar, detectar e informar el uso de licencias de terceros...
-  **Resource Access Manager** ☆
Comparta recursos de AWS con otras cuentas o AWS Organizations

Características Ver los 29 resultados ▶

- Grupos**
-  Función IAM

Se nos va a mostrar la siguiente pantalla y vamos a dar click en “Usuarios” (Marcado con la flecha verde)

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with a search bar and a navigation menu. The 'Panel de IAM' (IAM Dashboard) is the main content area, featuring a 'Recomendaciones de seguridad' (Security Recommendations) section with three items, each marked with a green checkmark. A green arrow points to the 'Usuarios' (Users) link in the left sidebar. On the right, the 'Cuenta de AWS' (AWS Account) section displays account details, including the account ID and a redacted URL for the IAM sign-in page.

Identity and Access Management (IAM)

Panel de IAM

Recomendaciones de seguridad 0

- ✓ El usuario raíz tiene MFA
Al contar con la autenticación multifactor (MFA) para el usuario raíz se mejora la seguridad de esta cuenta.
- ✓ Cuenta con MFA
Al contar con la autenticación multifactor (MFA) para el usuario de IAM se mejora la seguridad de esta cuenta.
- ✓ El usuario Backend no tiene claves de acceso activas que no hayan sido utilizadas durante más de un año.
La desactivación o la eliminación de claves de acceso no utilizadas mejora la seguridad.

Cuenta de AWS

ID de cuenta
[Redacted]

Alias de cuenta
[Crear](#)

URL de inicio de sesión para los usuarios de IAM de esta cuenta
[Redacted]

Vamos a dar click en “Crear Usuario”

The screenshot shows the AWS IAM console 'Usuarios' (Users) page. The page header includes the 'IAM > Usuarios' breadcrumb. Below the header, there is a section titled 'Usuarios' with a sub-header 'Información'. A description states: '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 is located below the description. On the right side of the page, there are three buttons: 'Eliminar', 'Crear usuario', and a settings gear icon. A green arrow points to the 'Crear usuario' button.

IAM > Usuarios

Usuarios Información

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

Buscar

Eliminar Crear usuario

Especificamos el “Nombre de Usuario”, marcamos la acción de acceso de usuario a la consola de administración de AWS, y en la parte inferior le damos click es “Siguiente”

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

Paso 1

Especificar los detalles del usuario

Paso 2

Establecer permisos

Paso 3

Revisar y crear

Paso 4

Recuperar contraseña

Especificar los detalles del usuario

Detalles del usuario

Nombre de usuario


user_s3_access

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.



¿Desea proporcionar acceso a la consola a una persona?
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. Para ello, inicie sesión en la consola con las credenciales de la cuenta de administración en AWS Organizations y, a continuación, habilite Identity Center. Si no es el propietario de la cuenta de administración, póngase en contacto con el propietario para realizar esta tarea.

Contraseña de la consola

☒

Contraseña generada automáticamente

Puede ver la contraseña después de crear el usuario.

En esta sección de permisos asignamos el grupo de usuarios que creamos anteriormente “s3_access_only_test” y en la parte inferior le damos click es “Siguiente”

Paso 1

[Especificar los detalles del usuario](#)

Paso 2

Establecer permisos

Paso 3

Revisar y crear

Paso 4

Recuperar contraseña

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 (1/1)

Buscar

< 1 >

<input checked="" type="checkbox"/>	Nombre del grupo	Usuarios	Políticas adjuntas	Creado
<input checked="" type="checkbox"/>	s3_accest_only_list	0	s3_read_only_list	2024-05-31 (hace 18 minutos)

Revisamos las opciones establecidas para el usuario

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

Paso 2
[Establecer permisos](#)

Paso 3
Revisar y crear

Paso 4
[Recuperar contraseña](#)

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 user_s3_access	Tipo de contraseña de consola Autogenerated	Exigir el restablecimiento de la contraseña Sí
-------------------------------------	--	---

Resumen de permisos

< 1 >

Nombre	Tipo	Usado como
IAMUserChangePassword	Administrada por AWS	Política de permisos
s3_accest_only_list	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

Le damos click en “Crear Usuario”

Nos mostrará la siguiente pantalla donde ya se creó el usuario y la opción de descargar las credenciales

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

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


URL de inicio de sesión de la consola

 [Redacted URL]

Nombre de usuario

 user_s3_access

Contraseña de la consola

 ***** [Mostrar](#)

Instrucciones de inicio de sesión por correo electrónico

Cancelar

Descargar archivo.csv

Volver a la lista de usuarios

Nota, creamos dos usuarios más, pero no se agregan las capturas de su creación, ya que sería repetitivo y solo cambiando el nombre

Asociación de usuarios al Grupo de Usuarios

En esta pantalla de nuestro Grupo de usuarios

IAM > Grupos de usuarios > s3_accest_only_list

s3_accest_only_list Información

[Eliminar](#)

Resumen [Editar](#)

Nombre del grupo de usuarios s3_accest_only_list	Hora de creación May 31, 2024, 22:06 (UTC-06:00)	ARN arn:aws:iam::304555555555:group/s3_accest_only_list
---	---	--

[Usuarios](#) | [Permisos](#) | [Access Advisor](#)

Políticas de permisos (1) Información

Puede asociar hasta 10 políticas administradas.

Filtrar por Tipo Todos los tipos < 1 > ⓘ

<input type="checkbox"/>	Nombre de la política ✕	Tipo	Entidades asociadas
<input type="checkbox"/>	s3_read_only_list	Administrada por el cliente	1

Daremos click en la pestaña de Usuarios

Daremos click en “Agregar Usuarios”



IAM > Grupos de usuarios > s3_accest_only_list

s3_accest_only_list Información

[Eliminar](#)

Resumen [Editar](#)

Nombre del grupo de usuarios: s3_accest_only_list

Hora de creación: May 31, 2024, 22:06 (UTC-06:00)

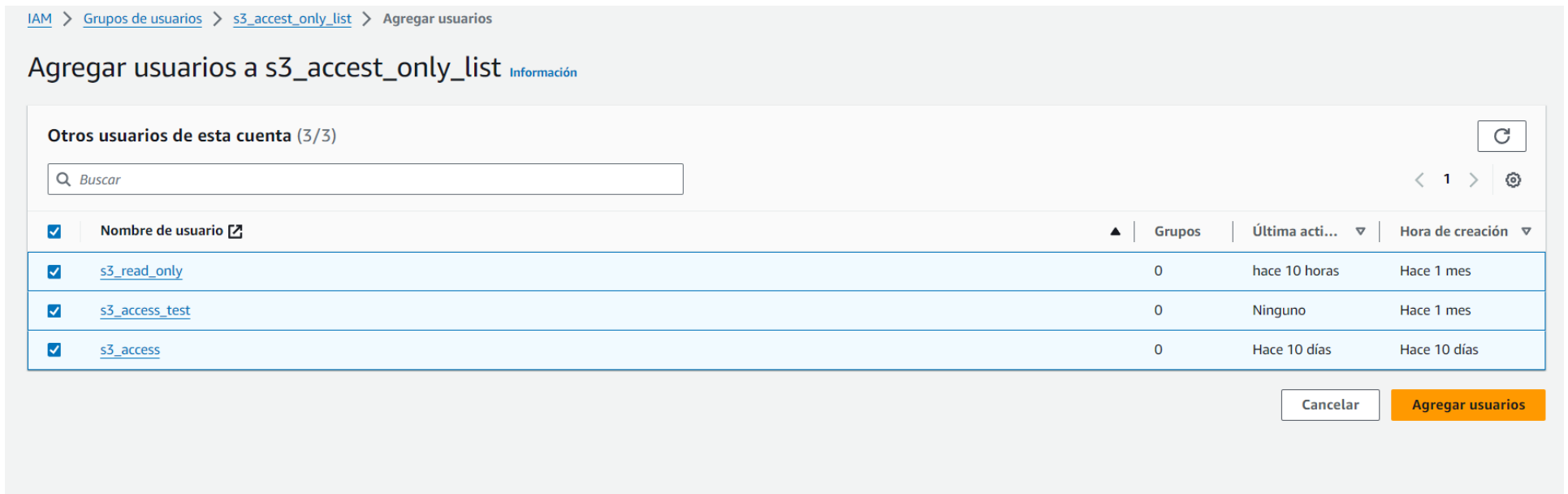
ARN: /s3_accest_only_list

[Usuarios](#) | [Permisos](#) | [Access Advisor](#)

Usuarios de este grupo [Eliminar](#) [Agregar usuarios](#)

Un usuario de IAM es una entidad que se crea en AWS para representar a la persona o aplicación que la utiliza para interactuar con AWS.

Agregaremos los usuarios que creamos anteriormente




IAM > Grupos de usuarios > s3_accest_only_list > Agregar usuarios

Agregar usuarios a s3_accest_only_list Información

Otros usuarios de esta cuenta (3/3)

[Cancelar](#) [Agregar usuarios](#)

<input checked="" type="checkbox"/>	Nombre de usuario 	Grupos	Última acti...	Hora de creación
<input checked="" type="checkbox"/>	s3_read_only	0	hace 10 horas	Hace 1 mes
<input checked="" type="checkbox"/>	s3_access_test	0	Ninguno	Hace 1 mes
<input checked="" type="checkbox"/>	s3_access	0	Hace 10 días	Hace 10 días

Y ahora nos aparecerán nuestros tres usuarios agregados a nuestro Grupo de usuarios

[IAM](#) > [Grupos de usuarios](#) > [s3_accest_only_list](#)

s3_accest_only_list

[Información](#)

Resumen


Nombre del grupo de usuarios

s3_accest_only_list

Hora de creación

May 31, 2024, 22:06 (UTC-06:00)

ARN


 arn:aws:iam:

Usuarios (3)


Permisos



Access Advisor

Usuarios de este grupo (3)



Un usuario de IAM es una entidad que se crea en AWS para representar a la persona o aplicación que la utiliza para interactuar con AWS.

 *Buscar*

<input type="checkbox"/>	Nombre de usuario 	 Grupos
<input type="checkbox"/>	s3_read_only	1
<input type="checkbox"/>	s3_access	1
<input type="checkbox"/>	user_s3_access	1