



AWS: La nube de Amazon

IAM: Identity and Access Management

Programa de Tecnología en Cómputo

Instructores:

Samuel Arturo Garrido Sánchez
Héctor Mauricio García Serrano

IAM: “Que no te pase compa, que un empleado enojado borre todo” ★



- AWS Identity and Access Management (IAM) proporciona un control de acceso detallado en todo AWS. Con IAM, puede especificar quién puede acceder a qué servicios y recursos, y en qué condiciones. Con las políticas de IAM, administre los permisos de su personal y sus sistemas para garantizar los permisos de privilegios necesarios.
- En pocas palabras, es un servicio para administrar quién entra a la nube y qué tiene permitido hacer.



Conceptos fundamentales

- **Usuarios:** Un usuario de IAM es una identidad con credenciales a largo plazo que se utiliza para interactuar con AWS en una cuenta.
- **Grupos:** Un grupo de usuarios es una colección de usuarios de IAM. Use grupos para especificar permisos para una colección de usuarios.
- **Roles:** Un rol de IAM es una identidad que puede crear que tiene permisos específicos con credenciales que son válidas por períodos breves. Los roles pueden ser asumidos por entidades en las que confíe.



Conceptos fundamentales

- **Políticas:** Una política es un objeto en AWS que define permisos.
- Puede administrar el acceso en AWS creando políticas y asignándoselas a identidades de IAM (usuarios, grupos de usuarios o roles) o a recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal de IAM (usuario o rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega.
- **MAYORMENTE SE MANEJA EN JSON**



Funcionamiento 🙄

Con IAM, usted define quién puede acceder a qué al especificar permisos detallados. Luego, IAM aplica esos permisos para cada solicitud. El acceso se niega de forma predeterminada y se concede solo cuando los permisos especifican “Permitir”.



Símbolos usados en la arquitectura

Íconos de recursos

ícono del servicio



Amazon IAM



Add-on



Permissions



MFA token



AWS STS



AWS STS alternate



Long-term security credential



Encrypted data



Data encryption key



Temporary security credential



Role



AWS IAM Access Analyzer

Tablero inicial IAM

En el tablero inicial tendremos estadísticas de nuestra consola AWS como los grupos de usuarios, la cantidad de usuarios, roles que hemos asignado y las políticas aplicadas. **De preferencia hacer caso a las recomendaciones de seguridad como añadir una autenticación múltiple o MFA en entornos reales.**

IAM dashboard

Security recommendations 1



Add MFA for root user

Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA



Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

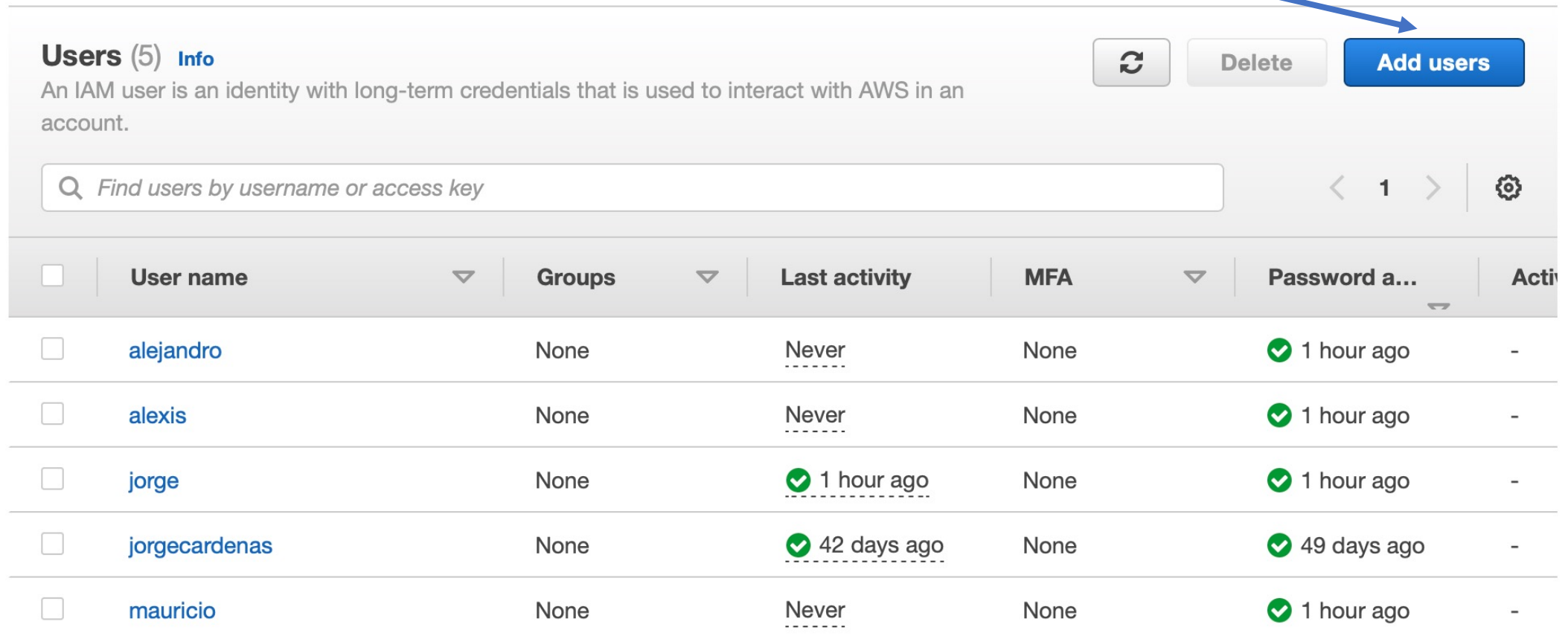
IAM resources



User groups	Users	Roles	Policies	Identity providers
2	5	10	3	0

Crear usuarios 🐶

Dentro de usuarios podemos crear unos en el botón de “Add users”



Users (5) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Refresh](#) [Delete](#) [Add users](#)

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password a...	Activ...
<input type="checkbox"/>	alejandro	None	Never	None	✓ 1 hour ago	-
<input type="checkbox"/>	alexis	None	Never	None	✓ 1 hour ago	-
<input type="checkbox"/>	jorge	None	✓ 1 hour ago	None	✓ 1 hour ago	-
<input type="checkbox"/>	jorgecardenas	None	✓ 42 days ago	None	✓ 49 days ago	-
<input type="checkbox"/>	mauricio	None	Never	None	✓ 1 hour ago	-

Crear usuarios

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*



[+ Add another user](#)

Añadimos username al usuario y si queremos añadir más de un jalón, hacemos click en “add another user”

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☐

Access key - Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐

Password - AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

Si queremos que el usuario IAM acceda por llave o por contraseña habrá que seleccionarlo

Crear usuarios

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☐

Access key - Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒

Password - AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

Seleccionamos la opción password

Console password*

☐

Autogenerated password

☒

Custom password

proteco+123

☒

Show password

Creamos una contraseña con al menos un símbolo para el/los usuarios a crear.

Require password reset

☒

User must create a new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Para mayor seguridad habilitamos la opción que una vez ingresados por primera vez, le pida cambiar la clave.

* Required

Cancel


Next: Permissions


Asignar políticas (permisos)


Add user

- 1
- 2
- 3
- 4
- 5


Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Create policy








Puede añadirse por grupos ya asignados, por copia de políticas de otro usuario existente o en caliente agregarle políticas

Filter policies

Search

Showing 730 results

	Policy name	Type	Used as
<input type="checkbox"/>	 AdministratorAccess	Job function	None
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS managed	None
<input type="checkbox"/>	 AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
<input type="checkbox"/>	 AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	 AlexaForBusinessFullAccess	AWS managed	None

Buscamos la política que se ajuste a dicho usuario.

Si es de poca confianza buscar de readonly

Confirmación de usuarios

✓ **Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at <https://514760535364.signin.aws.amazon.com/console>

Download .csv

	User	Email login instructions
▶ ✓	ejemplo	Send email

Una vez que hemos creados los usuarios con el link descrito aquí o con el ID que se puede ver en el link, ingresaremos estos usuarios a través de AMI al inicio de sesión de AWS.

También se puede descargar un CSV con la información de cada uno de los usuarios creados y enviar correo.