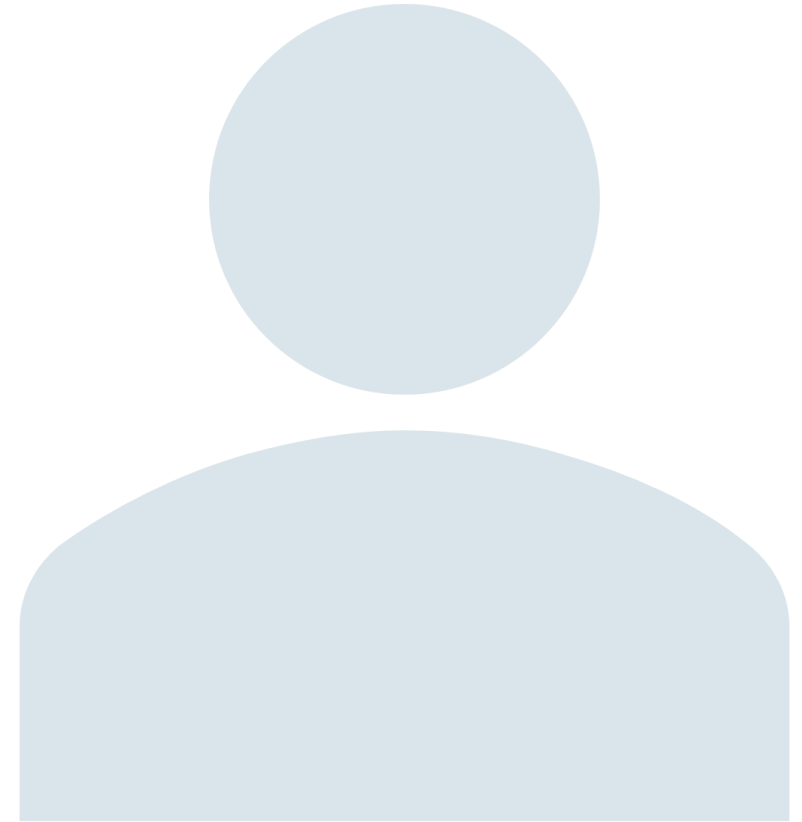


IAM (Identity and Access Management)

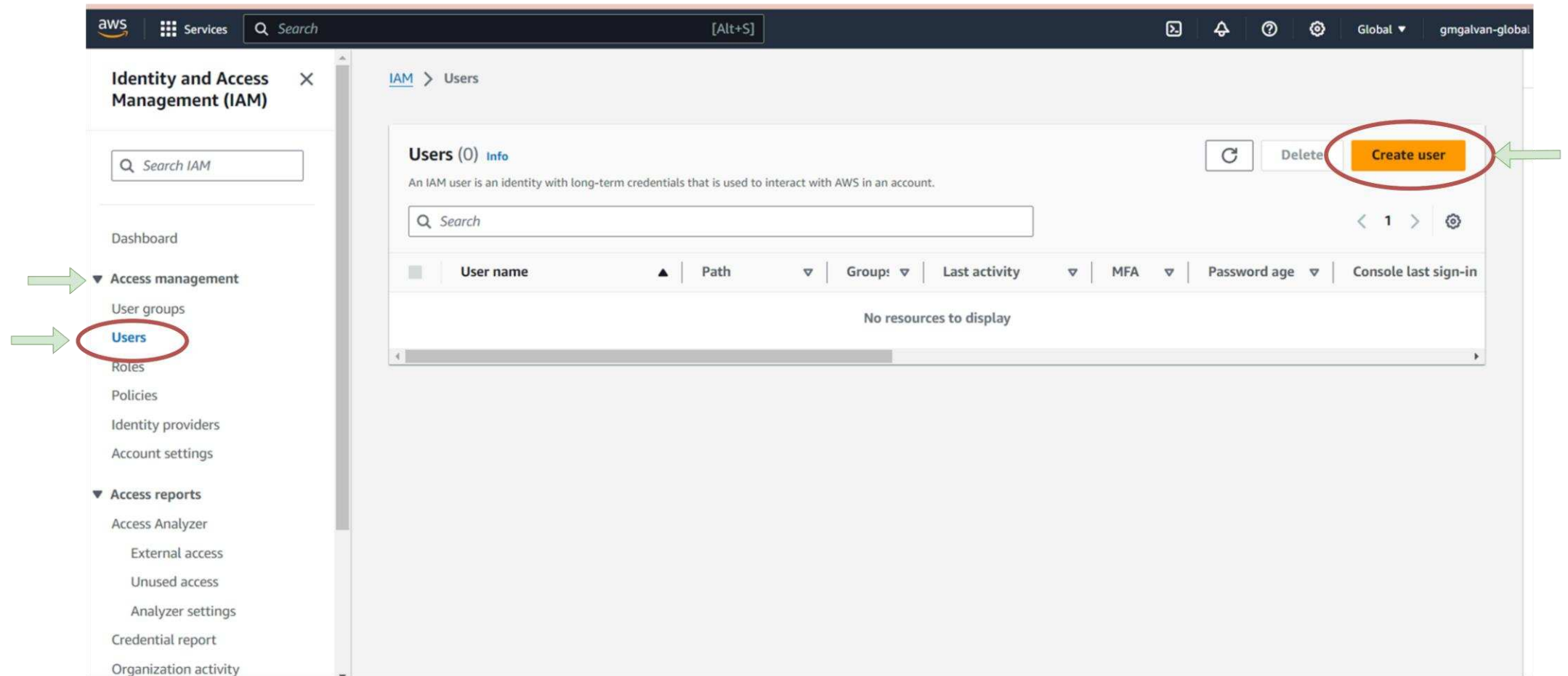


Usuarios, Grupos, Roles y Políticas



Crear
Usuario





Ir a sección de creación de usuarios

aws Services Search [Alt+S] Global gmgalvan-global

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

User name

student

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

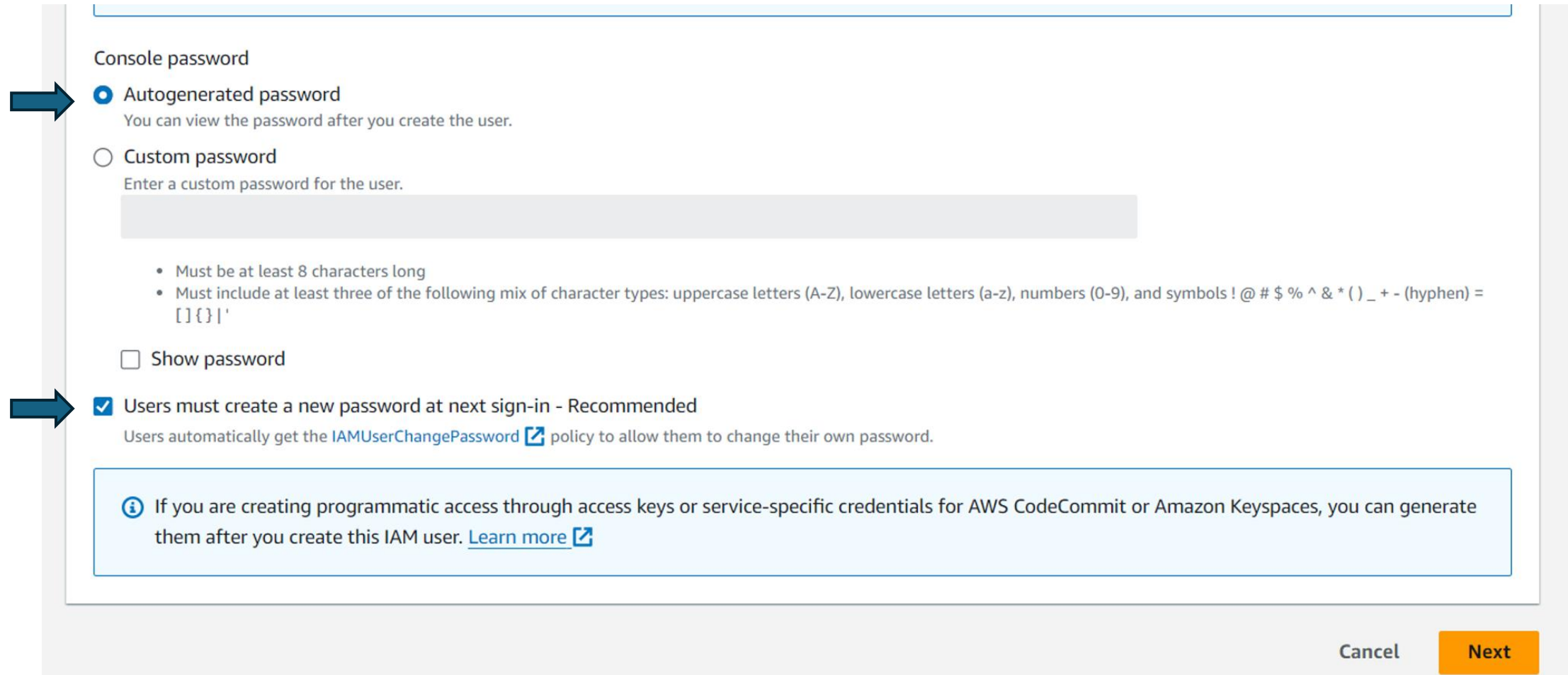
Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Especificación de detalles del usuario Parte 1



Console password

☒ Autogenerated password
You can view the password after you create the user.

☐ Custom password
Enter a custom password for the user.

☐ Show password

☒ Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Info If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

Especificación de detalles del usuario Parte 2

aws Services Search [Alt+S]

global

IAM > Users > Create user

Step 1
[Specify user details](#)

Step 2
[Set permissions](#)

Step 3
Review and create

Step 4
Retrieve password

Review and create


Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name student	Console password type Autogenerated	Require password reset Yes
----------------------	--	-------------------------------

Permissions summary

< 1 >

Name 	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Revisar y crear usuario Parte 1

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

aws Services Search [Alt+S]

Step 2
[Set permissions](#)

Step 3
Review and create

Step 4
Retrieve password

User details

User name student	Console password type Autogenerated	Require password reset Yes
----------------------	--	-------------------------------

Permissions summary

< 1 >

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key	Value - optional	
project	aws-course	Remove

[Add new tag](#)

You can add up to 49 more tags.

Cancel Previous **Create user**

Revisar y crear usuario Parte 2

aws Services Search [Alt+S] Global 1-global

User created successfully View user X

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[IAM](#) > [Users](#) > Create user

Step 1
[Specify user details](#)

Step 2
[Set permissions](#)

Step 3
[Review and create](#)

Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

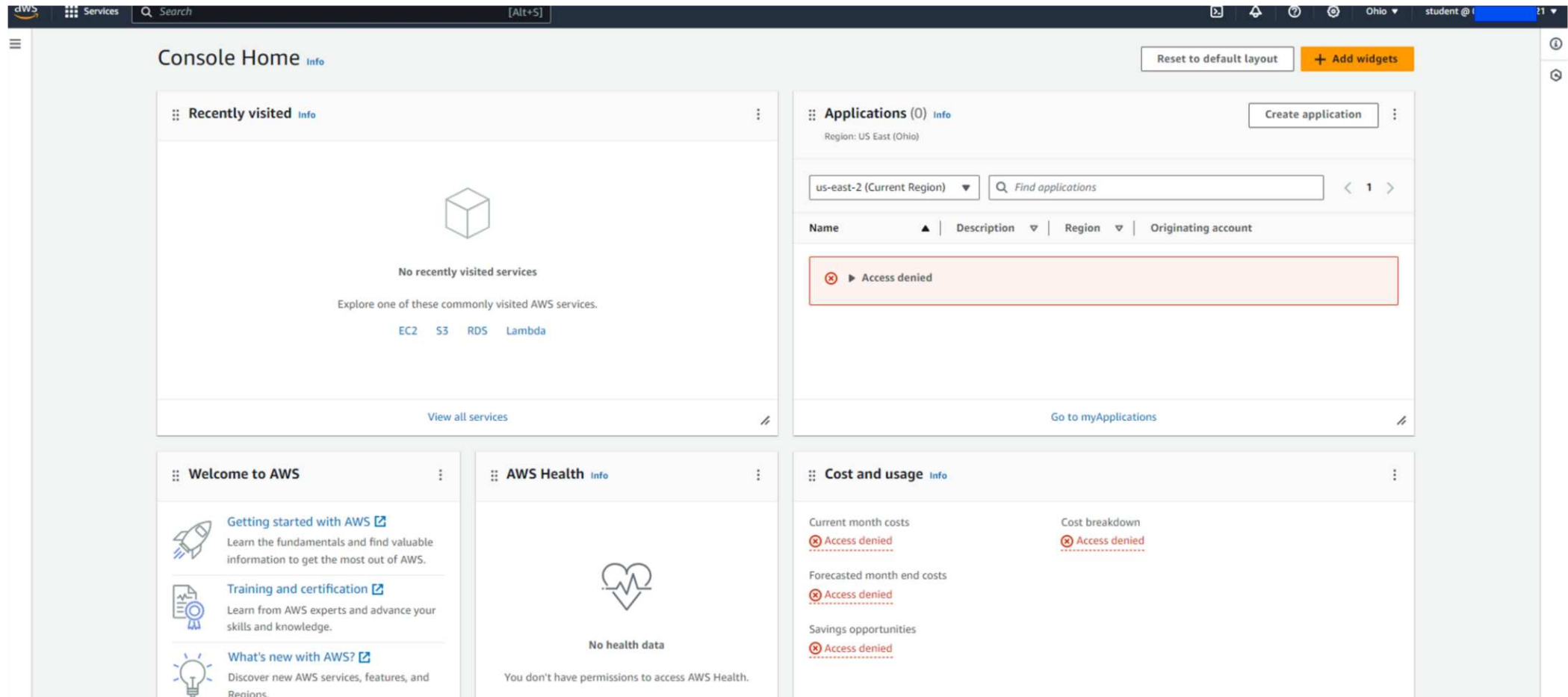
Console sign-in URL
https://02[redacted].signin.aws.amazon.com/console

User name
student

Console password
***** Show

Cancel Download .csv file Return to users list

Descargar CSV y obtener
credenciales



Entrar a la cuenta de usuario creado

CREAR GRUPO DE USUARIO



Admins

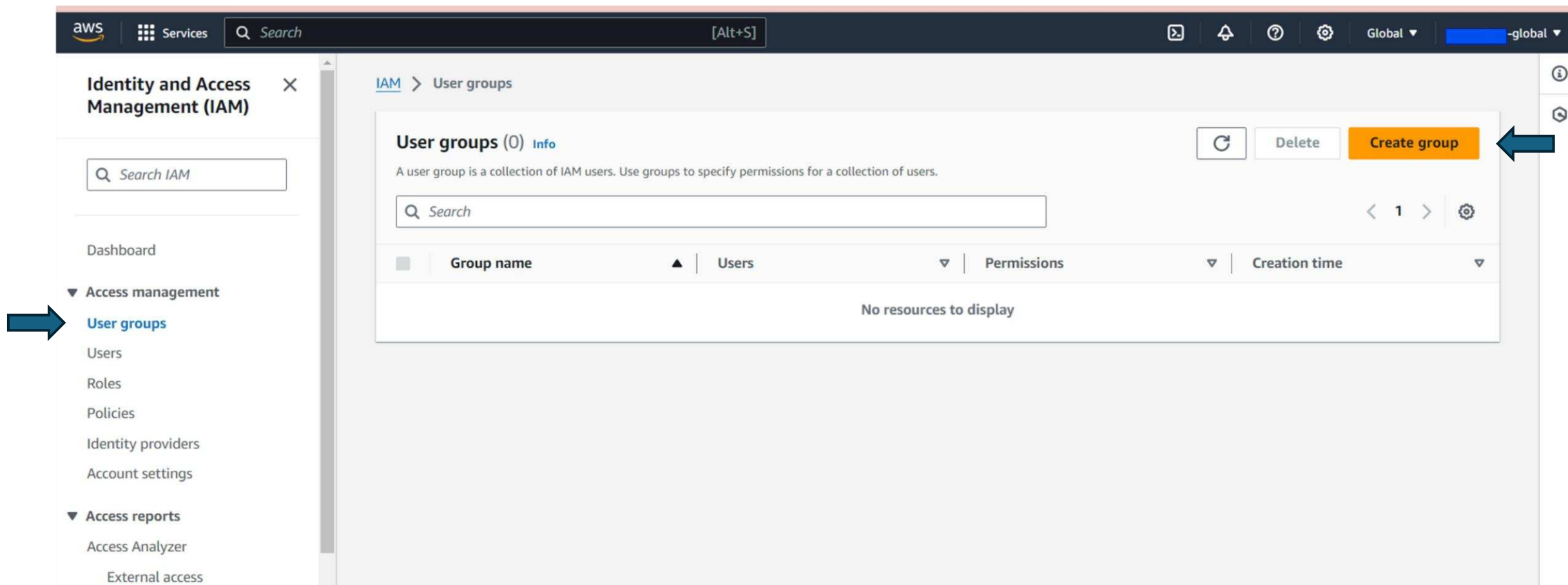


Data Scientists



Developers





Ir a sección de creación de grupos

The screenshot shows the AWS IAM console interface for creating a new user group. The left sidebar contains the navigation menu with sections for Identity and Access Management (IAM), Access management, and Access reports. The main content area is titled 'Create user group' and includes a breadcrumb trail: IAM > User groups > Create user group.

Name the group

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Add users to the group - Optional (1/1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

<input checked="" type="checkbox"/>	User name ?	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	student	0	None	12 minutes ago

Asignar nombre y usuario

aws

Services

Search

[Alt+S]

Global

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Attach permissions policies - Optional (945) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Search

All types

< 1 2 3 4 5 6 7 ... 48 >

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="checkbox"/>	AdministratorAccess-...	AWS managed	None	Grants account administrative permissi...
<input type="checkbox"/>	AdministratorAccess-...	AWS managed	None	Grants account administrative permissi...
<input type="checkbox"/>	AlexaForBusinessDevi...	AWS managed	None	Provide device setup access to AlexaFo...
<input type="checkbox"/>	AlexaForBusinessDevi...	AWS managed	None	Grants full access to AlexaForBusiness...

Dejar permisos y crear grupo

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
 - External access
 - Unused access
 - Analyzer settings

StudentCloudUsers user group created. View group

IAM > User groups > StudentCloudUsers

StudentCloudUsers Info

Delete

Summary Edit

User group name	Creation time	ARN
StudentCloudUsers	Aug [redacted]:00)	arn:aws:iam::0[redacted]:group/StudentCloudUsers

Users (1) Permissions Access Advisor

Users in this group (1)

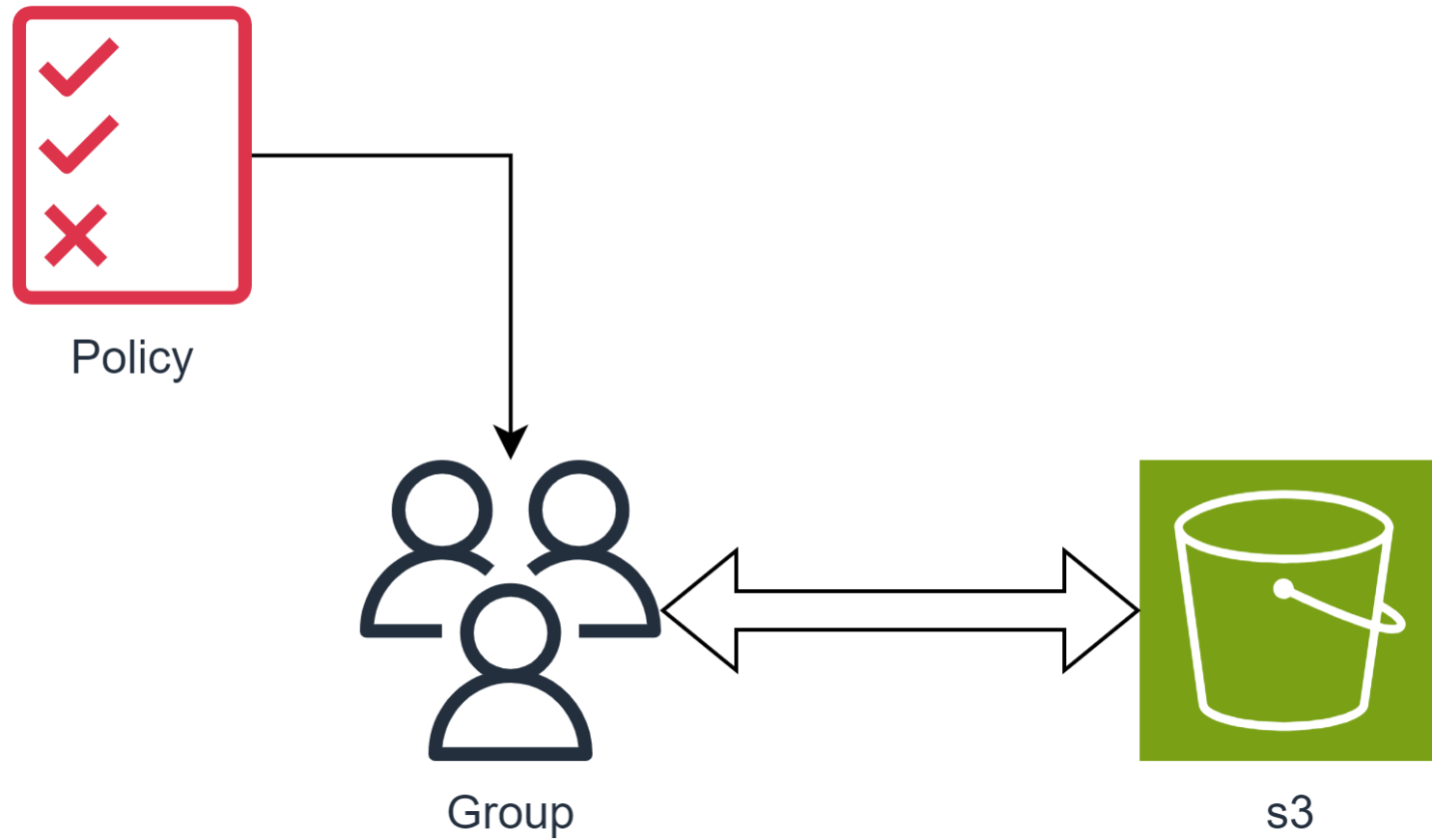
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

Remove Add users

< 1 > ⚙


Validar grupo es creado




Política para grupo de usuarios
hacia s3

The screenshot displays the AWS IAM console interface. On the left, the navigation menu is visible under the 'Identity and Access Management (IAM)' header. The 'Policies' link is highlighted with a blue arrow. The main content area shows the 'Policies (1221)' page. At the top right of this area, there are buttons for 'Create policy' (highlighted with a blue arrow), 'Delete', and 'Actions'. Below these buttons is a search bar and a 'Filter by Type' dropdown menu. A table lists various AWS managed policies, including 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayExecution', 'AlexaForBusinessLifesizeDelegatedAccessPolicy', 'AlexaForBusinessNetworkProfileServicePolicy', and 'AlexaForBusinessPolyDelegatedAccessPolicy'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

Ir a crear nueva política

 Services [Alt+S]

 IAM > Policies > Create policy


Step 1
Specify permissions

Step 2
Review and create

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

▼ Select a service

Specify what actions can be performed on specific resources in a service.

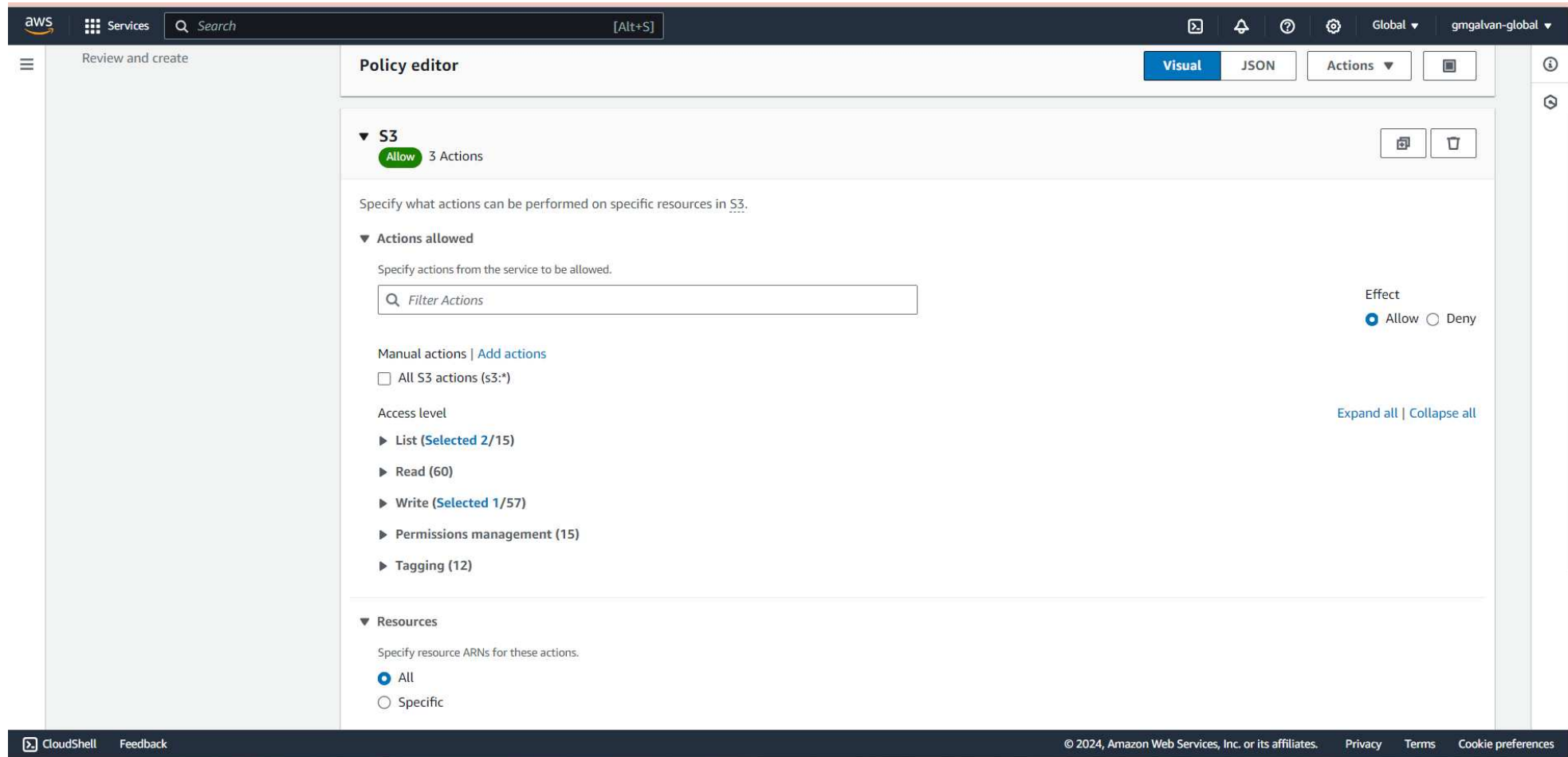
Service

Choose a service ▼

+ Add more permissions

CancelNext

Seleccionar permisos hacia S3



Agregar permisos: ListBucket,
ListAllMyBuckets, CreateBucket y
Resources All

Review and create [info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and "+,=,_,@,-" characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+,=,_,@,-" characters.

Permissions defined in this policy [info](#) [Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 420 services) [Show remaining 419 services](#)

Service	Access level	Resource	Request condition
S3	Limited: List, Write	All resources	None

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+,=,_,@,-" characters.

Permissions defined in this policy [info](#) [Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 420 services) [Show remaining 419 services](#)

Service	Access level	Resource	Request condition
S3	Limited: List, Write	All resources	None

Add tags - optional [info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create policy](#)

Nombrar y seguir

The screenshot displays the AWS IAM console interface. On the left, the navigation pane shows 'Identity and Access Management (IAM)' with a search bar and a list of options including 'Access management', 'Users', 'Roles', 'Policies', and 'Access reports'. The main content area shows the 'StudentCloudUsers' user group details. The 'Permissions' tab is selected, showing 'Permissions policies (0)'. The 'Add permissions' dropdown menu is open, with 'Attach policies' highlighted. Blue arrows indicate the path: from 'User groups' in the breadcrumb, to the 'Permissions' tab, and finally to the 'Attach policies' option in the dropdown menu.

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

StudentCloudUsers Info

Summary

User group name: StudentCloudUsers

Creation time: August 04, 2024, 12:15 (UTC-06:00)

ARN: arn:aws:iam::021891591921:group/StudentCloudUsers

Users (1) | **Permissions** | Access Advisor

Permissions policies (0) Info

You can attach up to 10 managed policies.

Search

Filter by Type: All types

Refresh Simulate Remove Add permissions ▲

Attach policies

Create inline policy

Policy name Type Attached entities

No resources to display

Agregar política a grupo


aws Services Q iam X

Global gmgalvan-global

IAM > User groups > StudentCloudUsers > Add permissions


Attach permission policies to StudentCloudUsers


► Current permissions policies (0)

Other permission policies (1/948) 

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

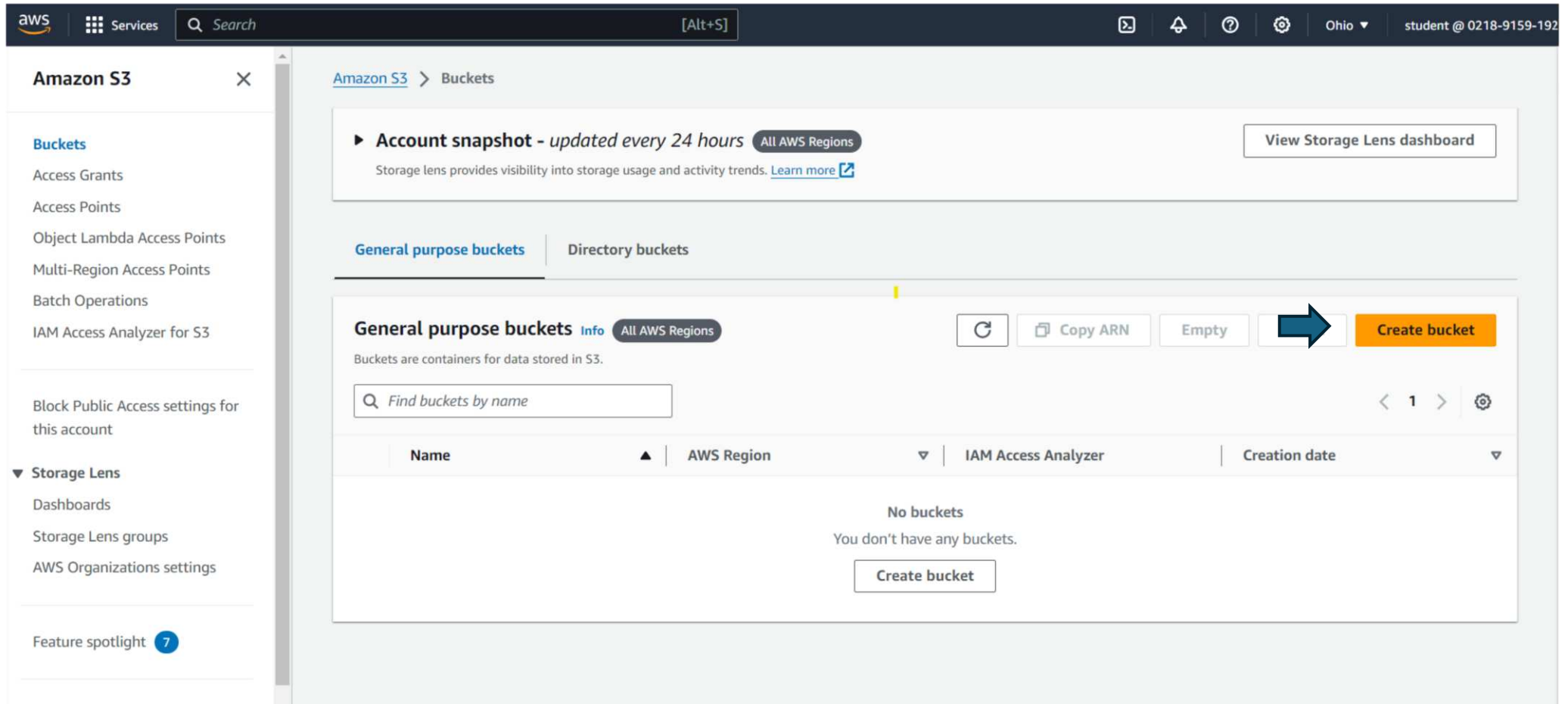
Filter by Type

Q S3CustomPolicy X All types 1 match < 1 > 

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	 S3CustomPolicy	Customer managed	None	-

Cancel Attach policies

Buscar y agregar política recién creada



Ir a S3 y verificar se puede lista ry
crear un bucket

aws Services Search [Alt+S] Ohio student @ 0218-9159-1921

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (Ohio) us-east-2

Bucket name [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

aws Services Search [Alt+S] Ohio student @ 0218-9159-1921

Successfully created bucket "bucket-example-20240805"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Insufficient permissions to apply Default Encryption
You need the s3:PutEncryptionConfiguration permission to apply Default Encryption on this bucket. After you or your AWS admin has updated your IAM permissions to allow s3:PutEncryptionConfiguration, go to [edit Default Encryption](#).

Amazon S3 > Buckets

Account snapshot - updated every 24 hours [All AWS Regions](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	bucket-example-20240805	US East (Ohio) us-east-2	View analyzer for us-east-2	August 5, 2024, 11:43:14 (UTC-06:00)

Crear S3 con configuraciones por default y verificar bucket es creado