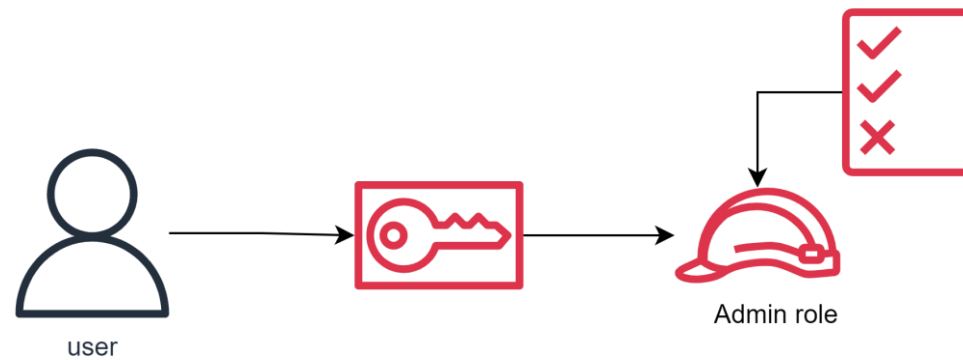


# Creción de Rol de Administrador y Asumirlo



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

### 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

IAM > Roles

**Roles (2)** Info Refresh Delete Create role


An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linker)	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service)	-


**Roles Anywhere** Info Manage

Authenticate your non AWS workloads and securely provide access to AWS services.




**Access AWS from your non AWS workloads**

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.



**X.509 Standard**

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.



**Temporary credentials**

Use temporary credentials with ease and benefit from the enhanced security they provide.

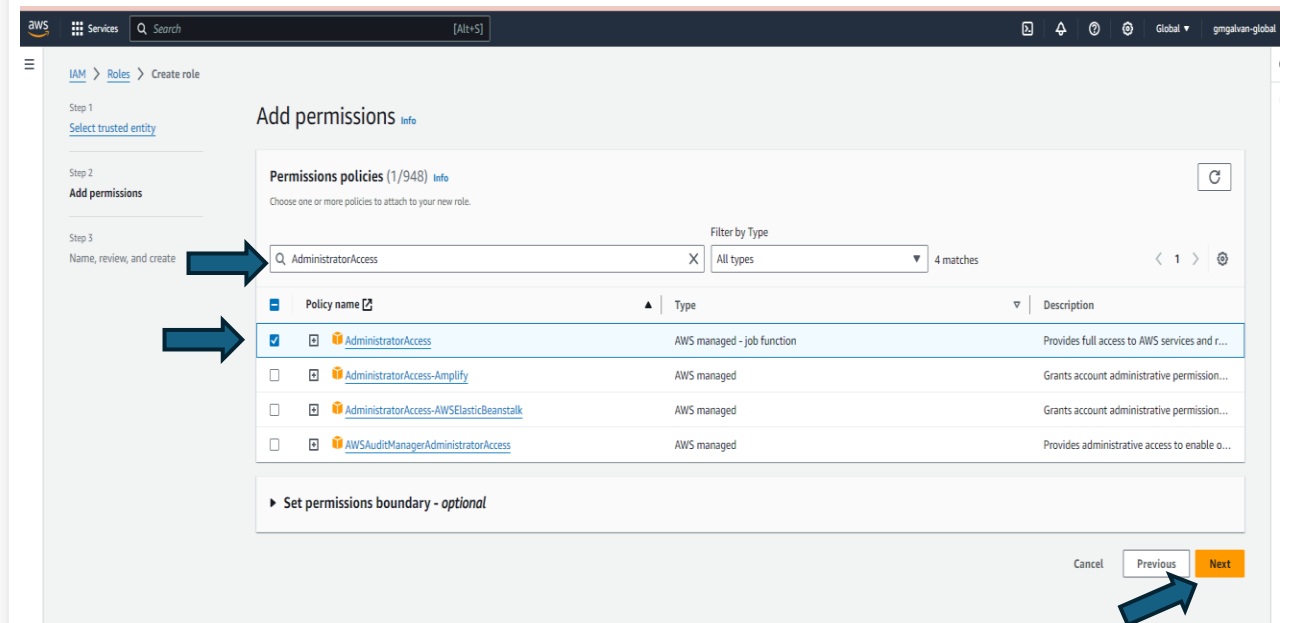
Acceder a  
roles y  
crear uno  
nuevo

- Seleccionar AWS Account
- En AWS account seleccionar esta cuenta
- Dar clic en Next

The screenshot shows the AWS IAM console 'Create role' wizard, Step 1: Select trusted entity. The interface is as follows:

- Trusted entity type:** Five options are listed in a grid:
  - ☐ AWS service: Allow AWS services like EC2, Lambda, or others to perform actions in this account.
  - ☒ AWS account: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account. (Indicated by a blue arrow)
  - ☐ Web identity: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
  - ☐ SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
  - ☐ Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.
- An AWS account:** Two options are listed:
  - ☒ This account (021891591921): Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account. (Indicated by a blue arrow)
  - ☐ Another AWS account
- Options:** Two checkboxes are present:
  - ☐ Require external ID (Best practice when a third party will assume this role)
  - ☐ Require MFA: Requires that the assuming entity use multi-factor authentication.
- Navigation:** At the bottom right, there are 'Cancel' and 'Next' buttons. A blue arrow points to the 'Next' button.

- Busca AdministratorAccess en los permisos existente
- Continúa en el siguiente paso



**Name, review, and create**

**Role details**

**Role name**  
Enter a meaningful name to identify this role.  
  
Maximum 64 characters. Use alphanumeric and \*+,:@\_- characters.

**Description**  
Add a short explanation for this role.  
  
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: \_+,:@\_-/[]!#\$%^&'()\*~=->|;:{}. Do not use spaces or the following characters: < > , " / \ : ; ' . , < > , " / \ : ; ' .

**Step 1: Select trusted entities** Edit

**Trust policy**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "021801591921"
9       },
10      "Condition": {}
11    }
12  ]
13 }
```

**Step 2: Add permissions** Edit

**Permissions policy summary**

Policy name	Type	Attached as
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy

**Step 3: Add tags**

**Add tags - optional** [Info](#)

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

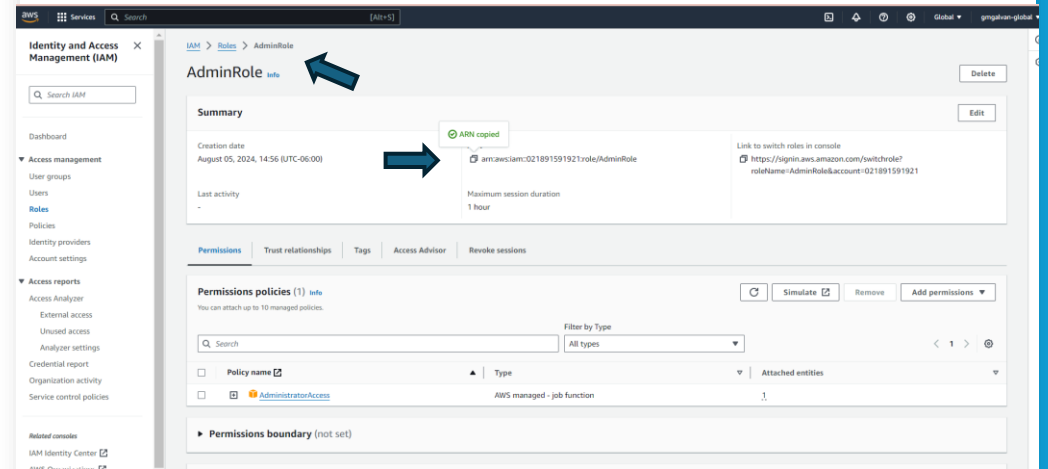
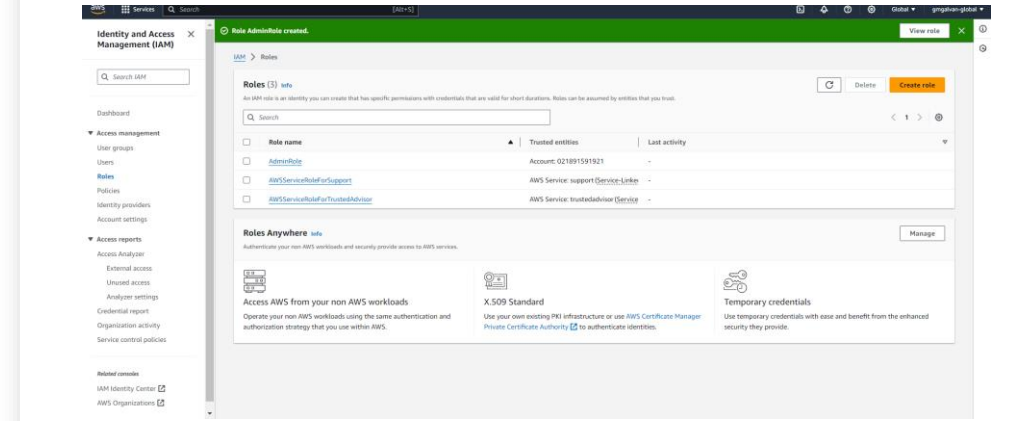
No tags associated with the resource.

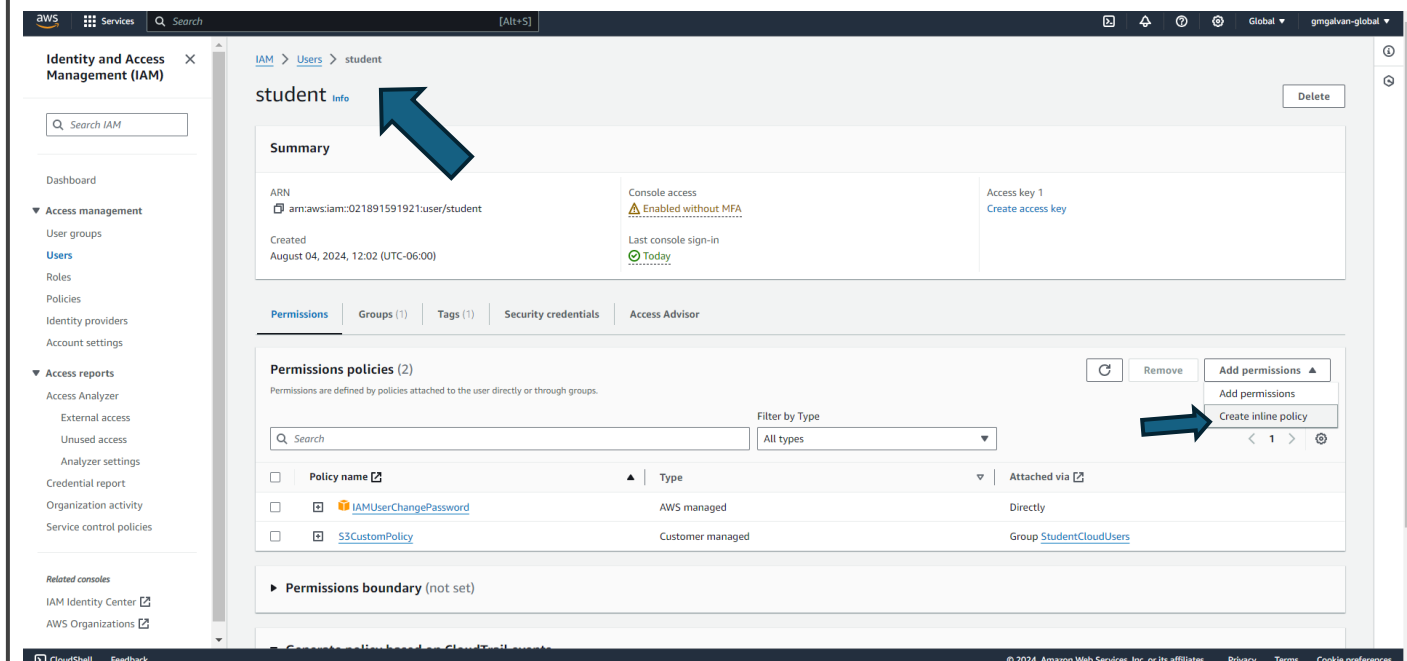
Add new tag  
You can add up to 50 more tags.

Cancel Previous Create role

- Nombrar el rol
- Revisar la información
- Continuar

Rol creado con éxito, copia el arn del rol para usarlo después.





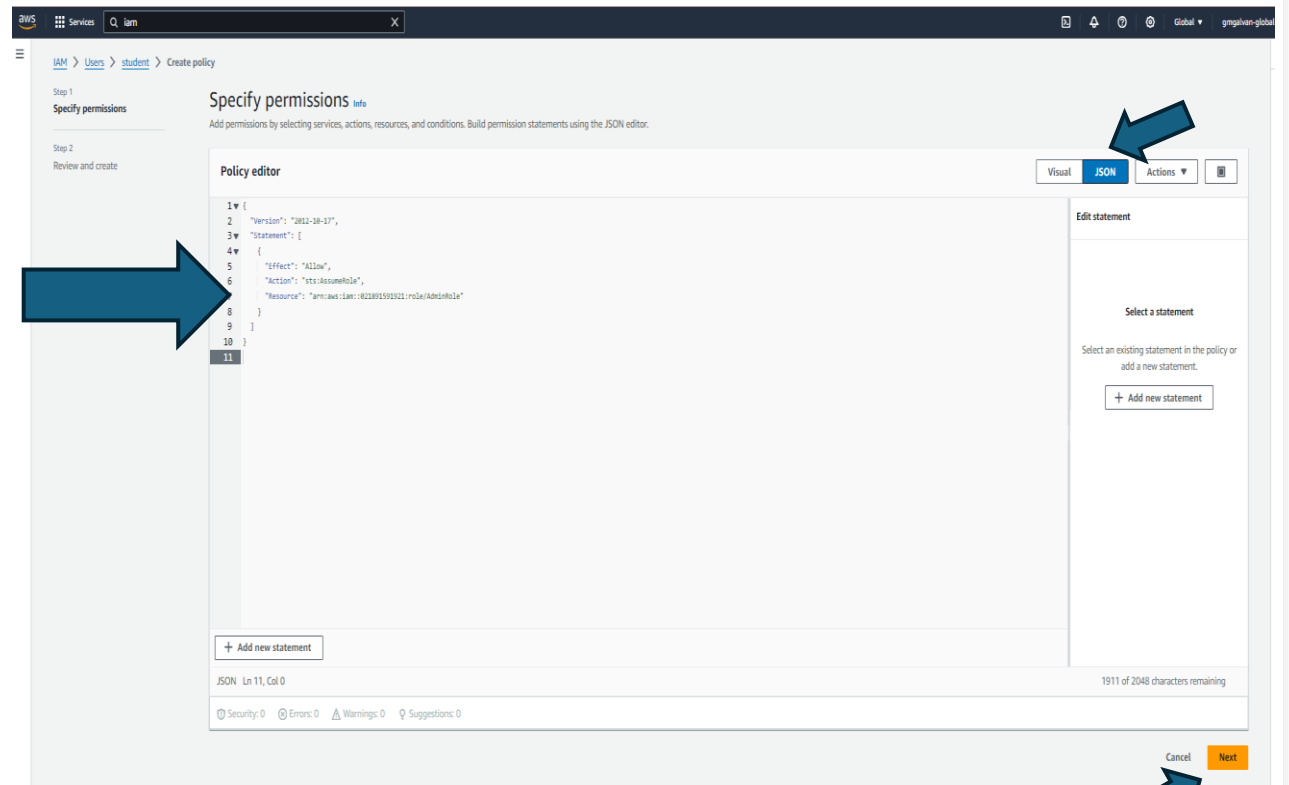
# Pasos asumir Rol

Ir hacia el usuario e  
ir a crear una  
politica en línea

- Ir al editor JSON y agregar el siguiente JSON :

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Resource": "arn:aws:iam::<your-account-number>:role/AdminRole"  
    }  
  ]  
}
```

- Remplaza el recurso con el arn del rol recién creado.
- Continua





# Revisar y crear

aws Services  X

Step 1  
[Specify permissions](#)

Step 2  
**Review and create**

## 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.

### Permissions defined in this policy [Info](#)

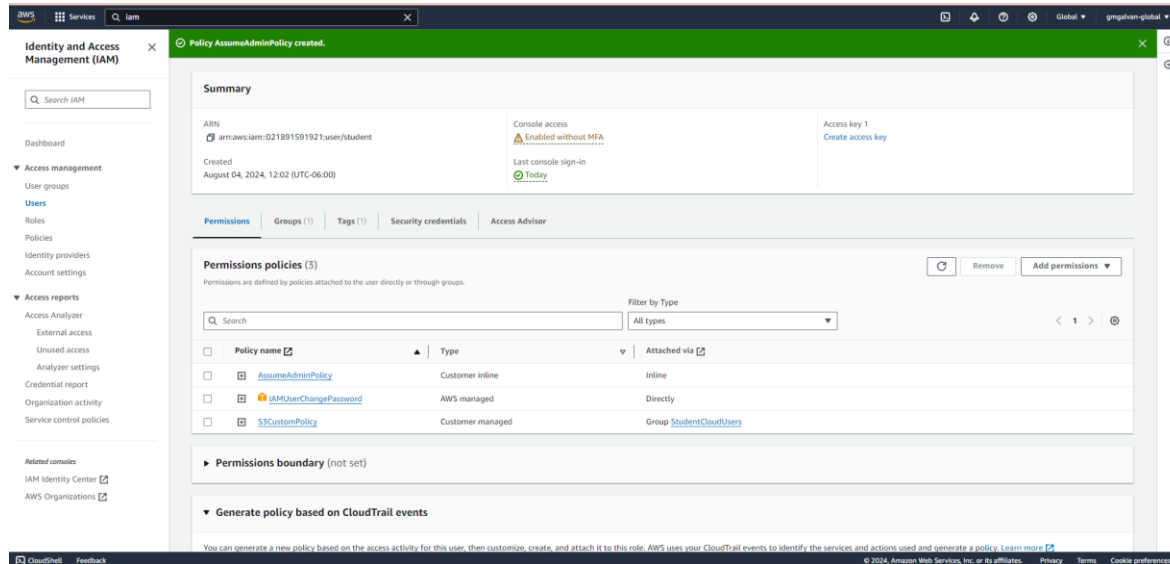
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 420 services) ☐ Show remaining 419 services

Service	Access level	Resource	Request condition
<a href="#">STS</a>	Limited: Write	RoleName  string like  AdminRole	None

Cancel Previous **Create policy**


# Rol asigando con éxito



The screenshot shows the AWS Management Console interface for the Amazon S3 Buckets page. The top navigation bar includes the AWS logo, a search bar, and the current region 'Ohio' with the user 'student @ 0218-9159-1921'. The left sidebar shows the 'Amazon S3' menu with options like 'Buckets', 'Access Grants', 'Access Points', etc. The main content area displays 'General purpose buckets' and a table with one bucket: 'bucket-example-20240805' in the 'US East (Ohio) us-east-2' region. A dropdown menu is open on the right, showing options like 'Account', 'Organization', 'Service Quotas', 'Billing and Cost Management', and 'Security credentials'. A blue arrow points to the 'Switch role' button in the dropdown.

## Validar Admin rol asignado a usuario

- Cambiaremos de cuenta e iniciamos el login en el usuario creado
- Ir a Switch role o cambiar de rol

English

### Switch Role

Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. [Learn more](#)

Account ID

The 12-digit account number or the alias of the account in which the role exists.

1921

IAM role name

The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the **TestRole** role name from the following role ARN: `arn:aws:iam::123456789012:role/TestRole`.

AdminRole

Display name - *optional*

This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.

Display color - *optional*

The selected color displays in the console navigation when this role is active

None

Cancel

Switch Role

- Agregar el id de la cuenta donde hacemos el cambio de rol y agregamos el nombre del rol.



**EC2 Dashboard**

EC2 Global View

Events

▼ **Instances**

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations

▼ **Images**

- AMIs
- AMI Catalog

▼ **Elastic Block Store**

- Volumes
- Snapshots
- Lifecycle Manager

**Resources**

EC2 Global View

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	0
Load balancers	0	Placement groups	0	Security groups	1
Snapshots	0	Volumes	0		

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#)

[Migrate a server](#)

Note: Your instances will launch in the US East (Ohio) Region

**Service health**

[AWS Health Dashboard](#)

Region  
US East (Ohio)

Status  
✔ This service is operating normally.

**Zones**

**EC2 Free Tier**

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast  
⚠ 0 offers forecasted to exceed free tier limit.

Exceeds free tier  
⚠ 0 offers exceeded and is now pay-as-you-go pricing.

[View Global EC2 resources](#)

[View all AWS Free Tier offers](#)

**Account attributes**

[Default VPC](#)  
vpc-06bd7cae1d7bfbcc9

**Settings**  
[Data protection and security](#)

AdminRole @

## Validación del rol asumido

- Validamos que tenemos acceso Administrativo
- Ir a EC2 y no debe de existir ningún error de permisos