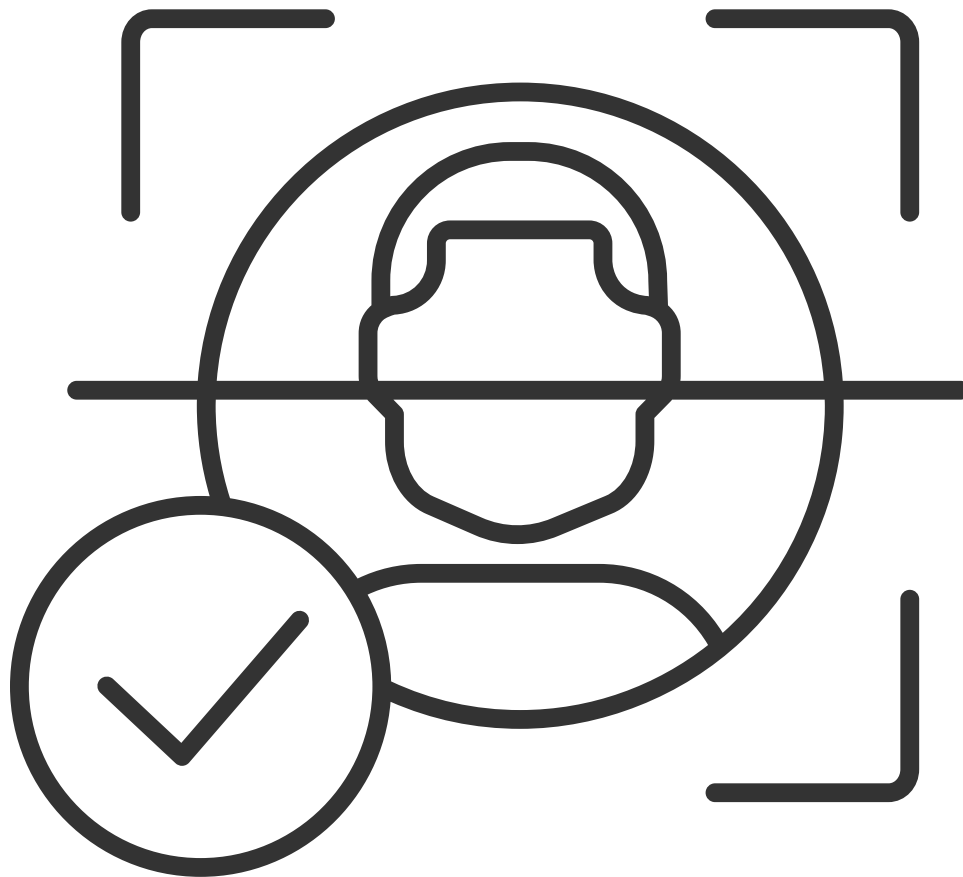




26°

Lab - AWS re/Start

Introducción a la Gestión de Identidades



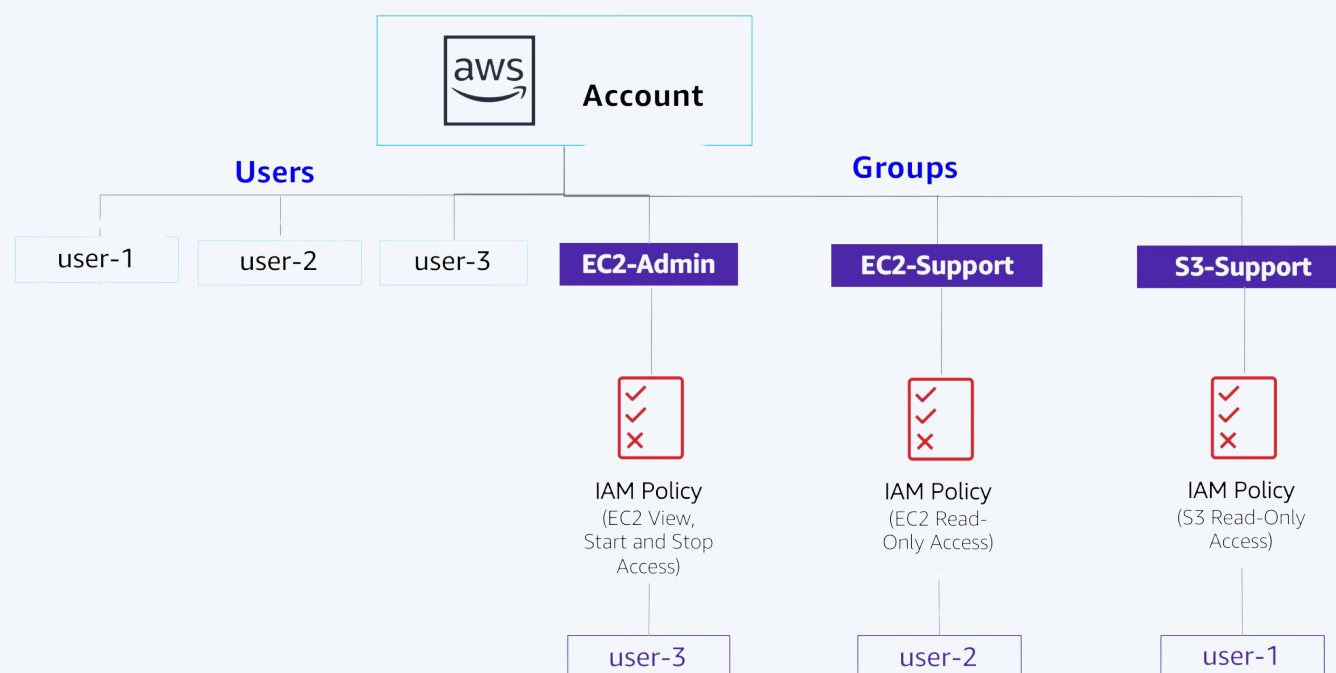
Tarea 01



Gestionado user, grps y roles con **AWS IAM**

A continuación, se muestra los objetivos del laboratorio:

- Crear y aplicar una política de contraseñas de IAM
- Analizar usuarios y grupos de usuarios de IAM creados previamente
- Inspeccionar políticas de IAM según se apliquen a los grupos de usuarios creados previamente
- Agregar usuarios a grupos de usuario con capacidades específicas activas
- Ubicar y usar la URL de inicio de sesión de la IAM
- Probar los efectos de las políticas en el acceso a los servicios



Tarea 01



Es conveniente tener un repaso de lo que es AWS IAM (Identity and Access Management), este servicio se puede usar para lo siguiente:

- **Administrar usuarios de IAM y su acceso:** puede crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos con Multi-Factor Authentication). Puede administrar los permisos para controlar qué operaciones puede realizar cada usuario.
- **Administrar roles de IAM y sus permisos:** un rol de IAM es similar a un usuario, ya que un rol es una identidad de AWS con políticas de permisos que establecen qué puede hacer o no la identidad en Amazon Web Services (AWS). Sin embargo, en lugar de estar asociado únicamente a una persona, el objetivo es que cualquiera que necesite el rol pueda asumirlo (incluso un servicio)

Tarea 01



Empezamos inspeccionando una política para la contraseña de la cuenta AWS. Esta política afecta a todos los usuarios asociados a esta cuenta. Acá notamos la política que se encuentra de manera predeterminada:

IAM > Account Settings

Account settings [Info](#)

Password policy [Info](#)

Configure the password requirements for the IAM users.

This AWS account uses the following default password policy:

Password minimum length

8 characters

Password strength

Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

Edit

Ahora, procedemos a explorar los usuarios y grupos. A continuación se muestran los usuarios vinculados a la cuenta

IAM > Users

Users (3) [Info](#)

Refresh

Delete

Create user

Search

< 1 > ⚙

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
<input type="checkbox"/>	user-1	/spl66/	0		-	✓ 18 minutes	-	-
<input type="checkbox"/>	user-2	/spl66/	0		-	✓ 17 minutes	-	-
<input type="checkbox"/>	user-3	/spl66/	0		-	✓ 17 minutes	-	-

< SWIPE ≡

Tarea 01



Mientras que los grupos de usuarios:

IAM > User groups				
User groups (3) Info				
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.				
<input type="text" value="Search"/>				
<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin	0	Defined	20 minutes ago
<input type="checkbox"/>	EC2-Support	0	Defined	20 minutes ago
<input type="checkbox"/>	S3-Support	0	Defined	20 minutes ago

Y podemos ver los permisos asignados al grupo EC2-Support

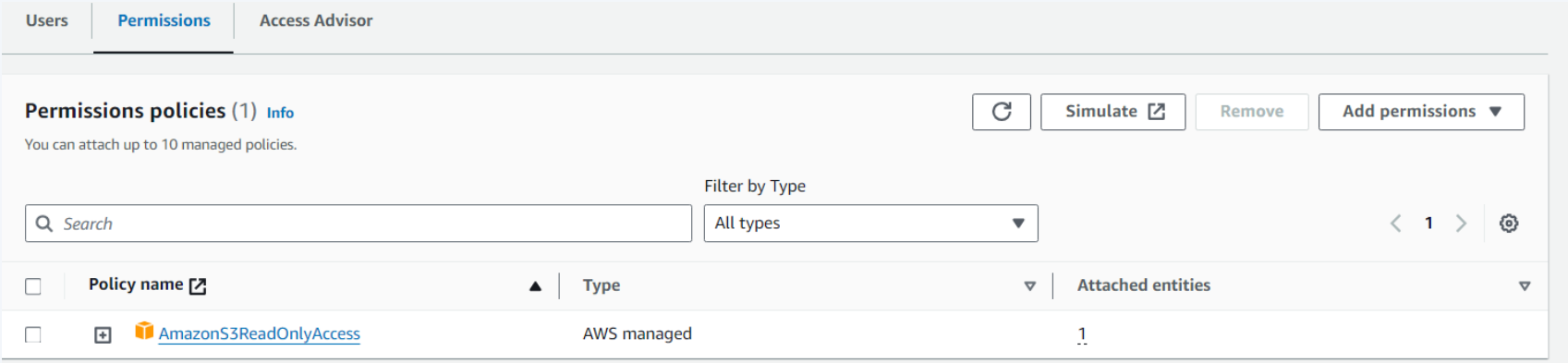
IAM > User groups > EC2-Support		
EC2-Support Info		
Delete		
Summary		
Edit		
User group name	Creation time	ARN
EC2-Support	January 31, 2024, 00:00 (UTC-05:00)	arn:aws:iam::555451576738:group/spl66/EC2-Support
Users	Permissions	Access Advisor
Permissions policies (1) Info		
You can attach up to 10 managed policies.		
<input type="text" value="Search"/>		
Filter by Type		
All types		
<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed

Donde **Effect** indica si tenemos *permitido* o *denegado* hacer alguna **Action** (eg: CloudWatch:ListMetrics). Y **Resource** puede ser eg: un bucket específico de S3, una instancia de EC2 o * que significa **cualquier recurso**.

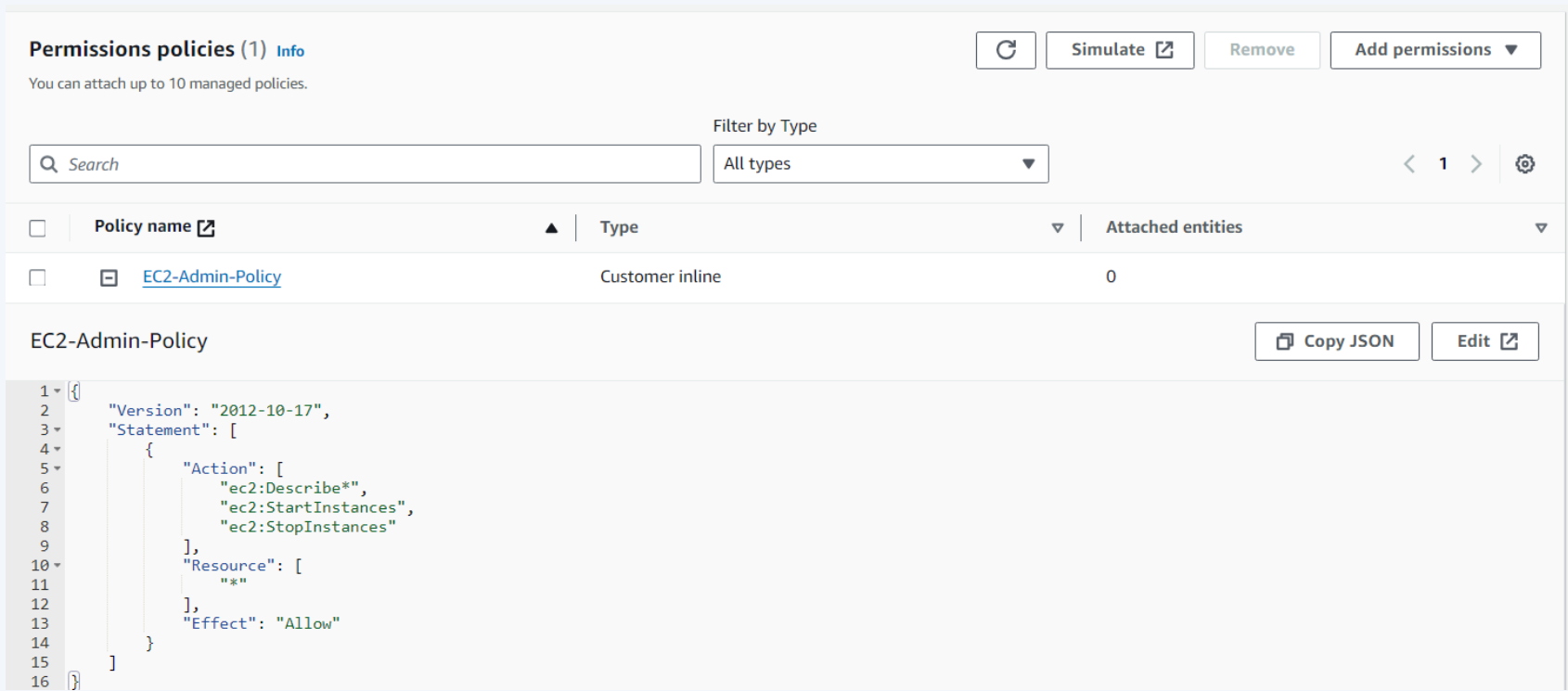
Tarea 01



Así, tenemos los permisos asignado al grupo S3-Support



Y al grupo EC2-Admin, cuya política es *Customer inline*, la cual es asignada únicamente a un único usuario o grupo



Como caso de negocio, debemos vincular estos usuarios

User	In Group	Permissions
user-1	S3-Support	Read-only access to Amazon S3
user-2	EC2-Support	Read-only access to Amazon EC2
user-3	EC2-Admin	View, start, and stop EC2 instances

Tarea 01



Ahora, procederemos a añadir usuarios a sus respectivos grupos de usuarios:

IAM > User groups

User groups (3) Info Refresh Delete Create group

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

Search

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin	1	Defined	34 minutes ago
<input type="checkbox"/>	EC2-Support	1	Defined	34 minutes ago
<input type="checkbox"/>	S3-Support	1	Defined	34 minutes ago

Esto nos permitirá testear los permisos asignados a partir del grupo vinculado de cada usuario. Pero, primero, comprobaremos el inicio de sesión usando el link para los usuarios IAM vinculados a esta cuenta. Pudimos ingresar con la clave del user-1 de manera exitosa

The screenshot shows the AWS IAM console with the 'Sign in as IAM user' page on the left and the 'Console Home' dashboard on the right. The sign-in page has fields for Account ID (555451576738), IAM user name (user-1), and Password. The 'Sign in' button is highlighted. The 'Console Home' dashboard shows 'Recently visited' services (EC2, S3, RDS, Lambda), 'Applications' (0), and 'Cost and usage' sections. A red 'Access denied' message is visible in the 'Applications' section.

Tarea 01



Y podemos ver la lista de buckets de S3, lo cual va acorde al permiso asignado en el grupo S3-Support:

[Alt+S]

Global

user-1 @ 5554-5157-6738

Amazon S3 > Buckets

▼ Account snapshot

View Storage Lens dashboard

Last updated: Jan 29, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. [Learn more](#)

Total storage

Object count

Average object size

You can enable advanced metrics in the "default-account-dashboard" configuration.

109.3 KB

28

3.9 KB

General purpose buckets

Directory buckets

General purpose buckets (3) Info

Refresh

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

< 1 >

Settings

Name	AWS Region	Access	Creation date
<input type="radio"/> awslabs-resources-krxqqla59sui8d-us-east-1-555451576738	US East (N. Virginia) us-east-1	Error	May 30, 2023, 12:45:57 (UTC-05:00)
<input type="radio"/> awslabs-resources-r5b3y6ojjszcap-us-east-1-555451576738	US East (N. Virginia) us-east-1	Error	January 23, 2024, 12:34:05 (UTC-05:00)
<input type="radio"/> labstack-783c9c4b-e126-4728-9951-0a7c5c23-s3bucket-ededpxtv54u7	US West (Oregon) us-west-2	Bucket and objects not public	January 31, 2024, 00:00:23 (UTC-05:00)

Y como no estamos autorizados para visualizar las instancias de EC2

onsole.aws.amazon.com/ec2/home?region=us-east-2#Instances:instanceState=running

Ohio

user-1 @ 5554-5157-6738

Instances Info

Refresh

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

Any state

Instance state = running

Clear filters

< 1 ... >

Settings

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
You are not authorized to perform this operation. User: arn:aws:iam::555451576738:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action							

Tarea 01



Ahora ingresamos como user-2, y al tratar de detener una instancia de EC2 nos salta el mensaje de que no estamos autorizados. Esto solo lo puedo hacer el user-3, que pertenece al grupo EC2-Admin

Failed to stop the instance i-08427f766136a436d

You are not authorized to perform this operation. User: arn:aws:iam::555451576738:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-west-2:555451576738:instance/i-08427f766136a436d because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: MOx6uFB8uOv5QUor7b3zc5rJFeDV3PyT7CPERQds8IHgwisR2PGkKoCKWb5gJHOEJ2sTEbkhdJkHj_LzRoOL8w11JWJgyl7F7OfpxhuY3kdqDLwcpwE4rFK_dhcOwyQzrXEr7PMTWbleJdcV75Jeqx0fjUGQv0QP2jI6TOWDZRY-C0jy4iulcpP2_9WXJH9jStEC3GHK9zmHnESI-D-fnjyBhZ73abXxHLZGQHwdMurrDDrozQFgd4Eg3gjr94XAl1NYN6_I5amqO7kqyvVMuL26Pa_ggJKDjwhpjNfn40E7tc0h1cCkNvGxpIpdzavea_Jp_O2NvY3EE-6yv07RtHP5go_rSAJox0SnP8spOVgS39DFmII7Yhn-JEzvwLGNGL7QTPohYU1DFU_QCe7Mtxp2RsCV5Orhphu6auarxQH2JC5008bJ_QRfAak3UM8dYHCTY45DRwOJbtCRLxoPRptmk07-Cn9PeJorSIUOPiGQDhaTV6VZuVCQg9kEcm0VKguHlgeNP8kTd3_eGhcuV5c8Vly8HWF3g81hN-KL4xd1HnNpoWL8Rkl6phSNHXQlhZVB5Ds4KAKJn9zw2YzJCADTFp79IH1pRrRLIDHj-cHUIJ1oRgDPWx5FLAaHKApdTmAH_FMH0xGNhZ007295C9Kv5qNp6Z5fvvVATrRn61uG1z6jEDRtQ_IW9joB8G8jCWsnIAulesM7wsg_M-PsFEn11EOGv0XjPD3Anyjz1qzoEG7CWit3Zb4Ljs7B25wrg1zM6m6huegyyxeKqla6f8eaFStZONQTFwu95BEKdBAzyk2w6r-8vKCWnSazDYIIHIBW2yEZdsUrcBkhZ9k5-o2aruEJVqlDf3hWKRLSDOWBwt6AWESh-_yLr5CjKQzAwHpNwc69XBELBIW1Ocps7JAIZviQyNK900q7FTx7pNTmPLQHjHxulsw31MSjllcmajdvJ2EhqosyGp9nDPwbjVihPL8ZTDYAcVyaONpEKbR6xlRr7rdrio7wfa

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive) Any state

Instance state = running X Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/>	Web Server	i-08427f766136a436d	Running	t2.micro	2/2 checks passed	View alarms	us-west-2a	ec2-52-89-167-69.us-w...	52.89.167.69	-

Instance: i-08427f766136a436d (Web Server)

Details Status and alarms New Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID
i-08427f766136a436d (Web Server)

Public IPv4 address
52.89.167.69 [open address](#)

Instance state
Running

Private IP DNS name (IPv4 only)
ip-10-1-11-249.us-west-2.compute.internal

Instance type
t2.micro

Private IPv4 addresses
10.1.11.249

Public IPv4 DNS
ec2-52-89-167-69.us-west-2.compute.amazonaws.com [open address](#)

Elastic IP addresses
-

Y tampoco podemos ver la lista de buckets de S3

Amazon S3

Buckets

Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards
Storage Lens groups
AWS Organizations settings

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets Directory buckets

General purpose buckets Info

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name **AWS Region** **Access** **Creation date**

You don't have permissions to list buckets

After you or your AWS administrator has updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. [Learn more about Identity and access management in Amazon S3](#)

[Troubleshoot with Amazon Q](#)

Tarea 01



Y como había mencionado, al logearme como user-3, ya puedo detener una instancia EC2, puesto que el grupo al que pertenece dicho usuario tiene el permiso **EC2-Admin-Policy** que te permite iniciar y detener instancias de EC2

The screenshot displays the AWS Management Console for the 'us-west-2' region. A green notification banner at the top states 'Successfully stopped i-08427f766136a436d'. The 'Instances' page shows a table with one instance, 'Web Server', which is in a 'Stopped' state. The instance details panel below the table provides further information about the instance, including its ID, IP addresses, and DNS names.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
Web Server	i-08427f766136a436d	Stopped	t2.micro	2/2 checks passed	User: amawsil	us-west-2a	-	-	-

Instance: i-08427f766136a436d (Web Server)

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-08427f766136a436d (Web Server)	-	10.1.11.249
IPv6 address	Instance state	Public IPv4 DNS
-	Stopped	-
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-1-11-249.us-west-2.compute.internal	ip-10-1-11-249.us-west-2.compute.internal	-
Answer private resource DNS name	Instance type	
-	t2.micro	