

## 2.6

# Capa de gestión usuarios IAM

[https://docs.aws.amazon.com/es\\_es/IAM/latest/UserGuide/introduction.html](https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html)

## 2.6 Capa de gestión usuarios IAM

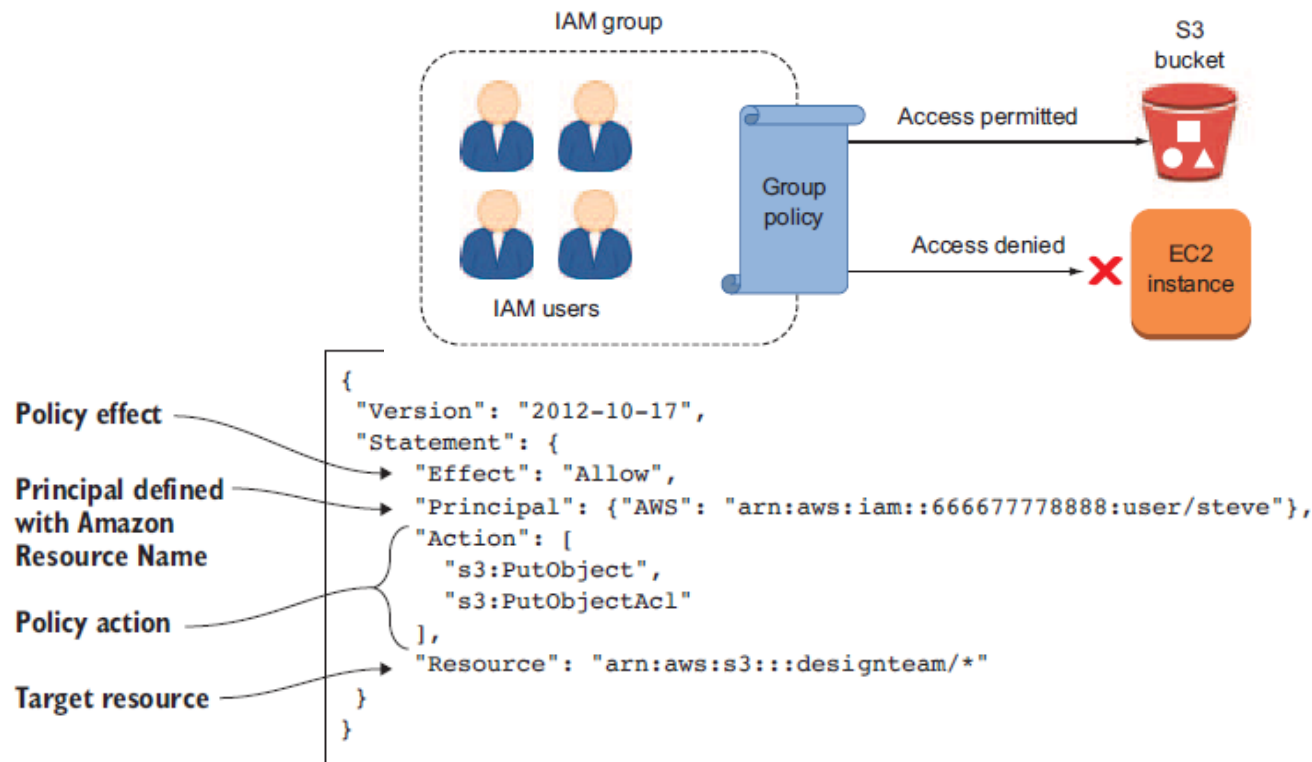
- En proyectos donde el grupo de desarrolladores es amplio se requiere de una configuración de uso de los recursos CLOUD detallado
- Servicio IAM
  - Permite gestionar el control de acceso a usuarios basandose en sus credenciales de autenticación



[https://docs.aws.amazon.com/es\\_es/IAM/latest/UserGuide/id\\_roles\\_common-scenarios.html](https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/id_roles_common-scenarios.html)

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Políticas
    - Definen que acciones se pueden realizar sobre que recursos
  - Roles
    - Son una agrupación de políticas asignables a los recursos , por ejemplo un servidor EC2 que requiere acceso a un bucket S3
  - Usuarios
    - Se les asocian políticas y credenciales de acceso sobre una cuenta
  - Grupos
    - Se les asocian políticas y los usuarios son parte

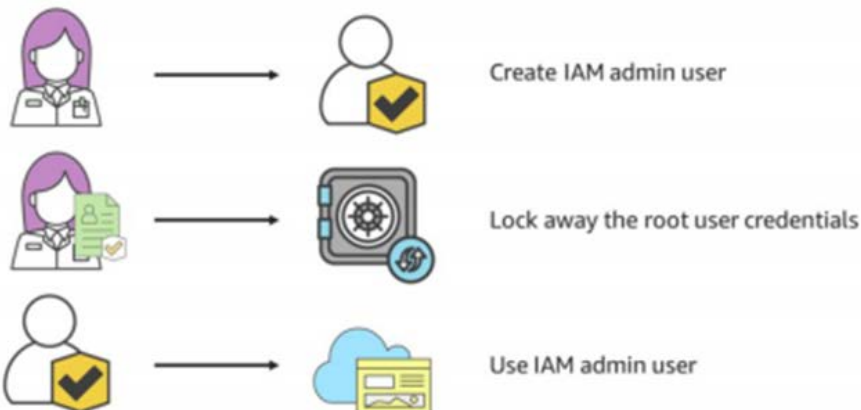


## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Cuenta Raíz
    - La cuenta raíz contiene todos los permisos
    - Se recomienda no utilizar la cuenta raíz
      - Crear otra cuenta con ligeras modificaciones,
      - por ejemplo tema de Billing

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Buenas prácticas
    - Cerrar el acceso a la cuenta root
    - Activar autenticación multifactor
      - Password + Código enviado al usuario
    - Crear una política de password IAM que asegura la calidad de los passwords
    - Claves de acceso
      - Normalmente para facilitar el acceso programático



### Credentials

#### AWS Access

Session started at: 2020-11-22T10:11:45-0800  
Session to end at: 2020-11-22T13:11:45-0800  
Remaining session time: 2h55m37s

Term: 80 days 13:50:22

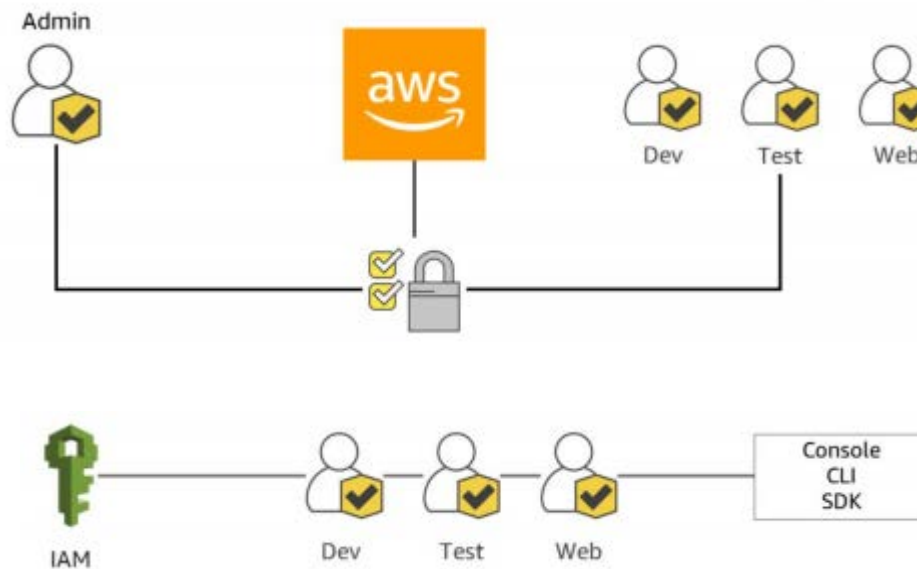
#### AWS CLI:

Copy and paste the following into ~/.aws/credentials

```
[default]
aws_access_key_id=[REDACTED]
aws_secret_access_key=[REDACTED]
aws_session_token=[REDACTED]
```

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Restringir el acceso de forma granular



## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Acceso via Consola y via CLI

### Identity and Access Management (IAM)

#### ▼ AWS Account (420693608596)

Panel

Grupos

**Usuarios**

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

Informe de credenciales

Q Buscar en IAM

#### ▼ AWS Organizations

Organization activity

Service control policies (SCPs)

hora de creación 2019-02-08 14:34 UTC+0100

Permisos Grupos (1) Etiquetas **Credenciales de seguridad** Access Advisor

Credenciales de inicio de sesión

**Resumen**

- Enlace de inicio de sesión de la consola: <https://420693608596.signin.aws.amazon.com/console>

**Contraseña de la consola** Habilitada (último inicio de sesión Hoy) | [Administración](#)

**Dispositivo MFA asignado** Sin asignar | [Administración](#)

**Certificados de firma** Ninguna

Claves de acceso

Utilice las claves de acceso para realizar solicitudes seguras de protocolos Query HTTP o REST a las API de servicio de AWS. Para su protección, no comparta nunca las claves frecuente. [Más información](#)

**Crear una clave de acceso**

ID de clave de acceso	Creado	Último uso
AKIAWD42LBCKA5LCKE55	2019-10-15 09:53 UTC+0100	2019-10-18 17:15 UTC+0100 con ec2 en eu-west-1

Claves de SSH para AWS CodeCommit

Utilice las claves públicas de SSH para autenticar el acceso a los repositorios de AWS CodeCommit. [Más información](#)

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Acceso CLI AWS Credentials

Crear una clave de acceso



**Correcto**

Esta es la **solo** vez que se pueden ver o descargar las claves de acceso secretas. No puede recuperarlas más adelante. Sin embargo, puede crear nuevas claves de acceso en cualquier momento.



Descargar archivo .csv

ID de clave de acceso

Clave de acceso secreta

AKIAQJDKHE7K362

JY31RIHHmTY10CtP/lye

[Ocultar](#)



## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Permisos



## 2.6 Capa de gestión usuarios IAM

### • Servicio IAM

- Acceso vía Consola y via CLI
- Ejemplo Educate Classroom

#### • Are Service Linked Roles supported?

Yes, you can use Service Linked roles for every service that is supported with your Classroom Account.

#### • I can't start any resources. What happened?

#### • Can I create users within my Classroom Account for others to access?

No, you cannot create users or groups within your Classroom Account.

#### • Can I create my own IAM policy within Starter Account or Classroom?

No, however you are free to use any AWS Managed Policy in your Classroom Account.

#### • How can I use IAM roles within AWS services?

You can use IAM by creating an execution role within the IAM console and referencing it within the service you are using, rather than creating an execution role within a service directly. For example, it is not possible to create lambda execution role directly from lambda console; instead create the lambda execution role from the IAM console and reference it from the lambda console when using it.

#### • Are there any restrictions on AWS services in my Classroom Account?

Yes, Classroom Accounts come with following restrictions on services:

- IAM: IAM support is limited. You cannot create policies or additional users. Additionally you cannot create federated users, or use switch roles to switch between different accounts.
- EC2: Creation of VPN gateways, VPN links, NAT gateways and Inspector is not permitted.
- EC2 and RDS: Reserved Instance Purchases are not permitted.
- EC2 supported instances types - "t2.small", "t2.micro", "t2.nano", "m4.large", "c4.large", "c5.large", "m5.large", "t2.medium", "m4.xlarge", "t2.nano", "c4.xlarge", "c5.xlarge", "t2.2xlarge", "m5.2xlarge"
- RDS: All instances supported EXCEPT: db.x1.\*, "db.x1e.\*", "db.r3.8xlarge", "db.r3.4xlarge", "db.r4.16xlarge", "db.r4.8xlarge", "db.r4.4xlarge", "db.m4.2xlarge", "db.m4.10xlarge", "db.m4.4xlarge", "db.m4.8xlarge", "db.m4.4xlarge", "db.m4.2xlarge"
- Route53: Domain name registration not supported.

#### • My cloudformation scripts are failing. Why?

Don't forget to logout once you are done with your work!

#### Credentials

##### AWS Access

Session started at: 2019-11-07T06:52:17-0800

Session to end at: 2019-11-07T09:52:17-0800

Remaining session time: 2h59m53s

Term: 52 days 19:26:51

##### AWS CLI:

Copy and paste the following into ~/.aws/credentials

```
[default]
aws_access_key_id=ASIATPWA...
aws_secret_access_key=...
aws_session_token=FwoGZXIvYXZlEIj//////////...
95IUP8aoXpI2Ni+I4NT5wS+zhDYoZ4tZrg4bGhy...
```

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Permisos



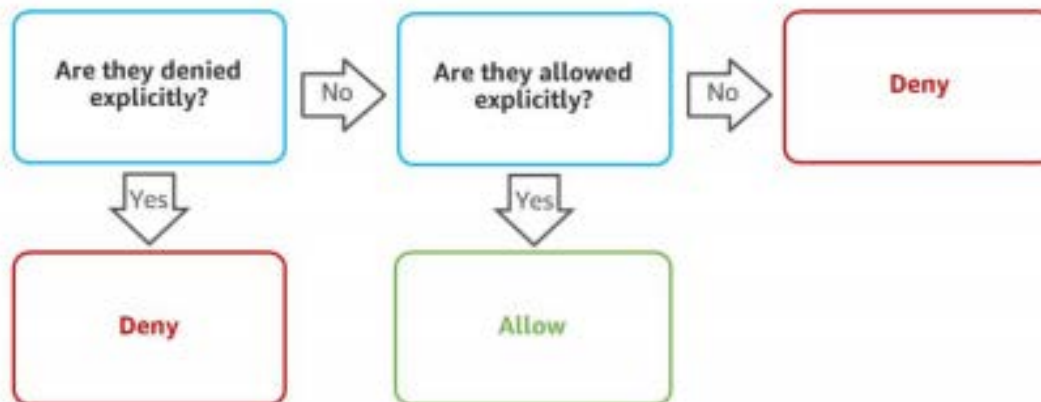
## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Permisos



Policy

- A formal declaration of **one or more permissions**
- Evaluated at the **time of request**
- IAM policies ONLY control access to **AWS services**
- IAM has **no visibility** above the hypervisor



## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Permisos



- Resource-Based – Attached to an **AWS resource**
- Identity-Based – Attached to an **IAM principal**



### Attached to:

- User
- Group
- Role

### Control:

- Actions performed
- Which resources
- What conditions are required

### Types of Policies:

- AWS-managed
- Customer-managed
- Inline



### Attached to:

- AWS resources such as Amazon S3, Amazon Glacier, and AWS KMS

### Control:

- Actions allowed by specific principal
- What conditions are required
- Are always inline policies
- No AWS-managed resource-based policies

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Permisos

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["dynamodb:*", "s3:*"],
    "Resource": ["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
    "arn:aws:s3:::bucket-name",
    "arn:aws:s3:::bucket-name/*"]
  },
  {
    "Effect": "Deny",
    "Action": ["dynamodb:*", "s3:*"],
    "NotResource": ["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
    "arn:aws:s3:::bucket-name",
    "arn:aws:s3:::bucket-name/*"]
  }
]
}
```

Gives users access to a specific DynamoDB table and...

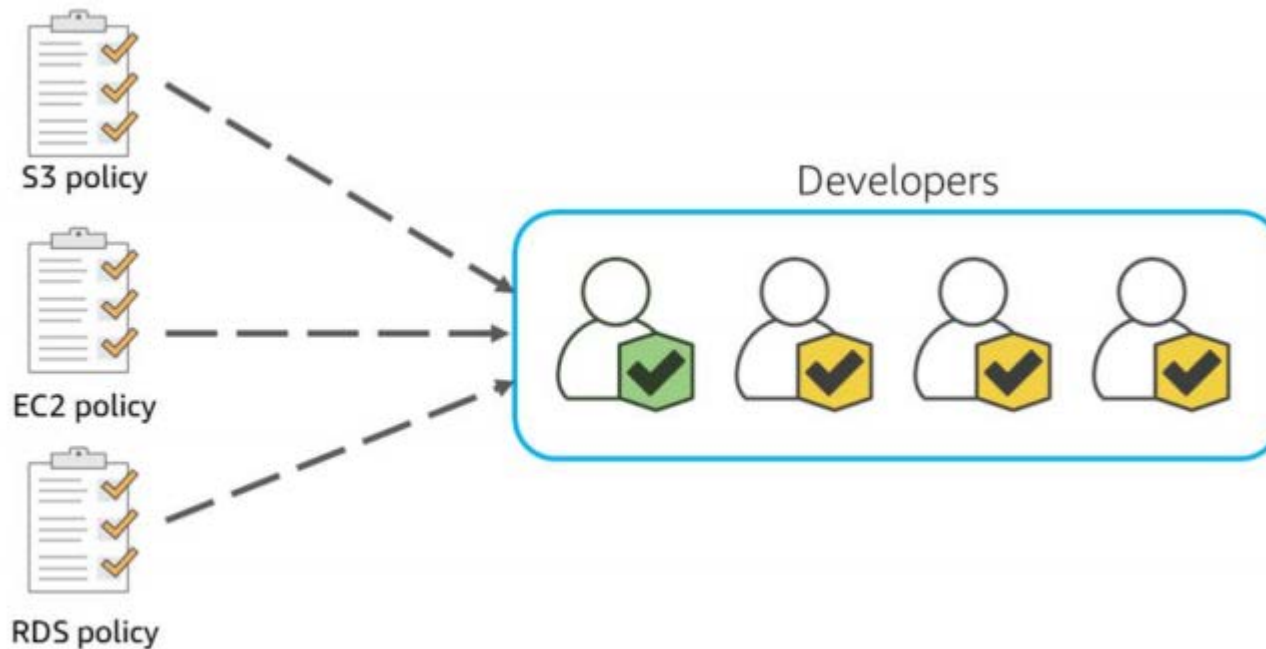
...a specific Amazon S3 bucket and its contents

An explicit deny statement ensures that principals cannot use any AWS actions or resources other than the specified table and bucket

An explicit deny statement takes precedence over an allow statement

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Organizando usuarios



## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Multiple cuentas

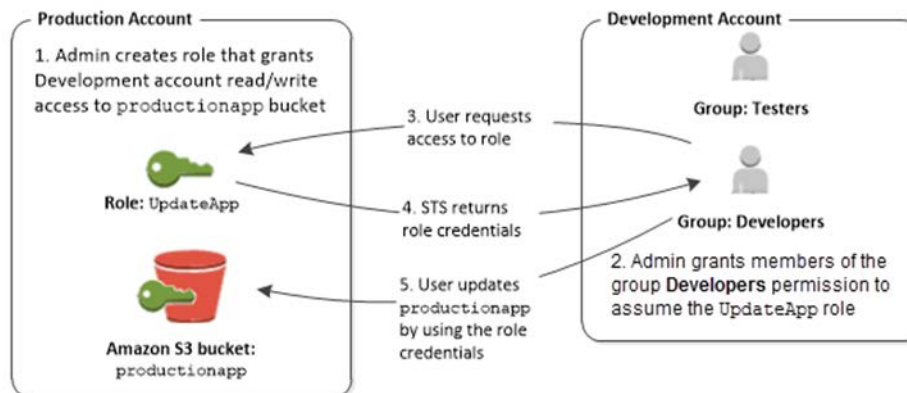




## 2.6 Capa de gestión usuarios IAM

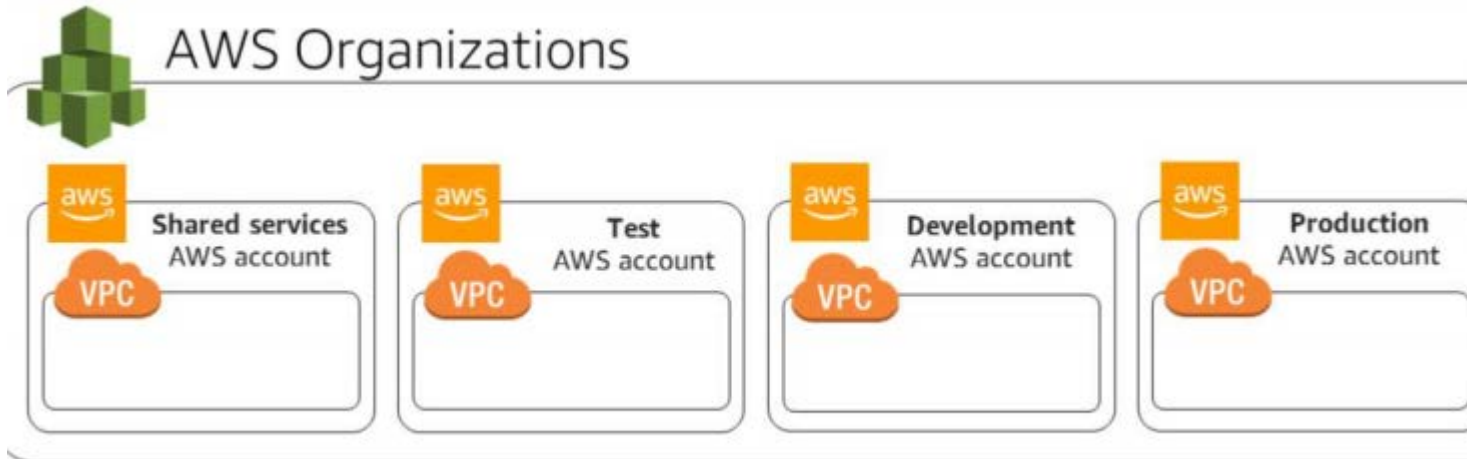
- Servicio IAM
  - Multiple cuentas

Centralized security management	Single AWS account
Separation of production, development, and testing environments	Three AWS accounts
Multiple autonomous departments	Multiple AWS accounts
Centralized security management with multiple autonomous independent projects	Multiple AWS accounts



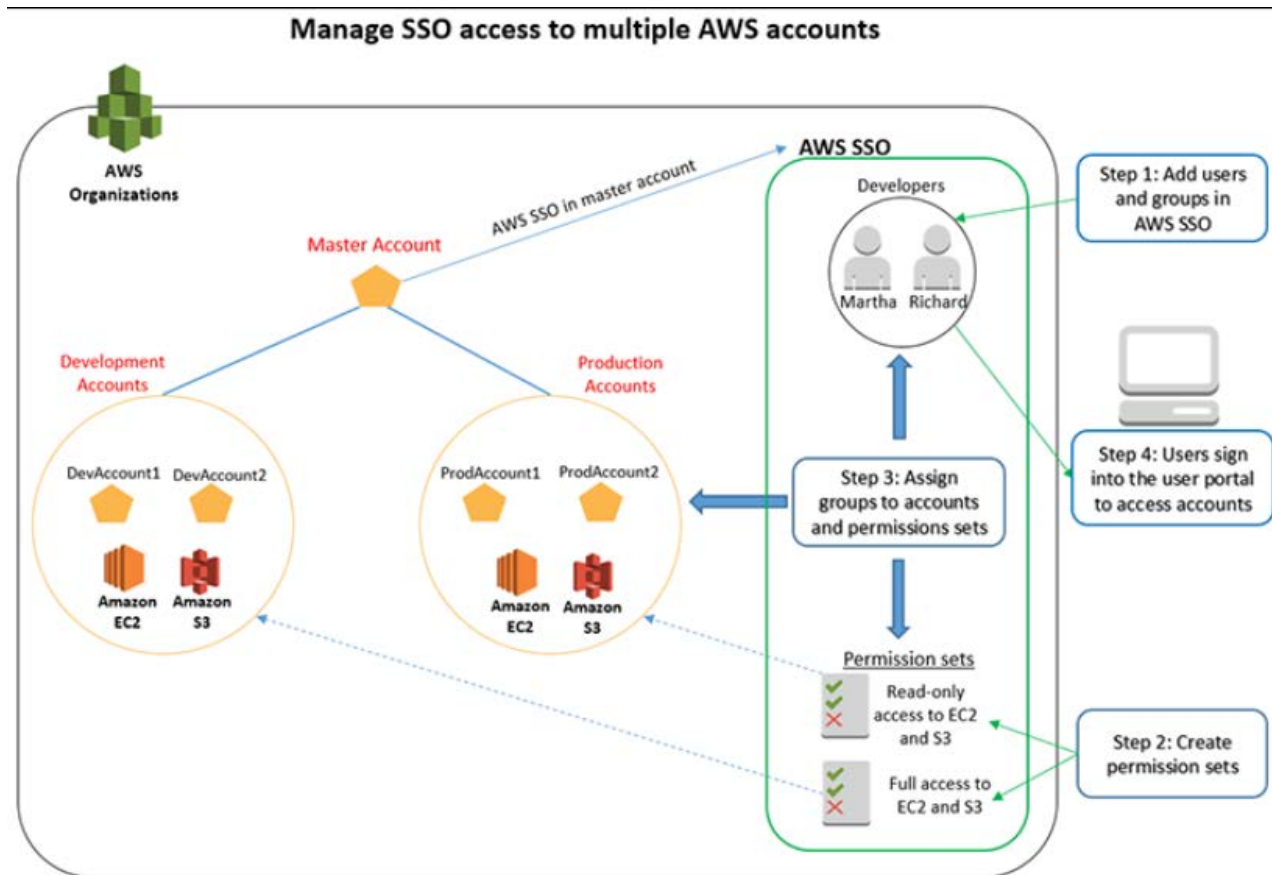
## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - AWS organizations
    - Es un servicio para gestión de cuentas



## 2.6 Capa de gestión usuarios IAM

- Servicio SSO
- Portal de Usuarios y Login



## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Roles
    - Permisos asociados a roles
    - Casos de uso
      - Recursos AWS que acceden a otros recursos
      - Ofrecer acceso a usuarios autenticados externamente
      - Ofrecer acceso a terceros
      - Cambiar de roles de un usuario par acceder distintos recursos

Crear un rol



Seleccionar el tipo de entidad de confianza

 <b>Servicio de AWS</b> EC2, Lambda y otros	 <b>Otra cuenta de AWS</b> Pertenciente a usted o a un tercero	 <b>Identidad web</b> Cognito o cualquier proveedor de OpenID	 <b>Federación SAML 2.0</b> Su directorio corporativo
--	---	--	--

Permite a las entidades de otras cuentas realizar acciones en esta. [Más información](#)

Especificar las cuentas que pueden utilizar este rol

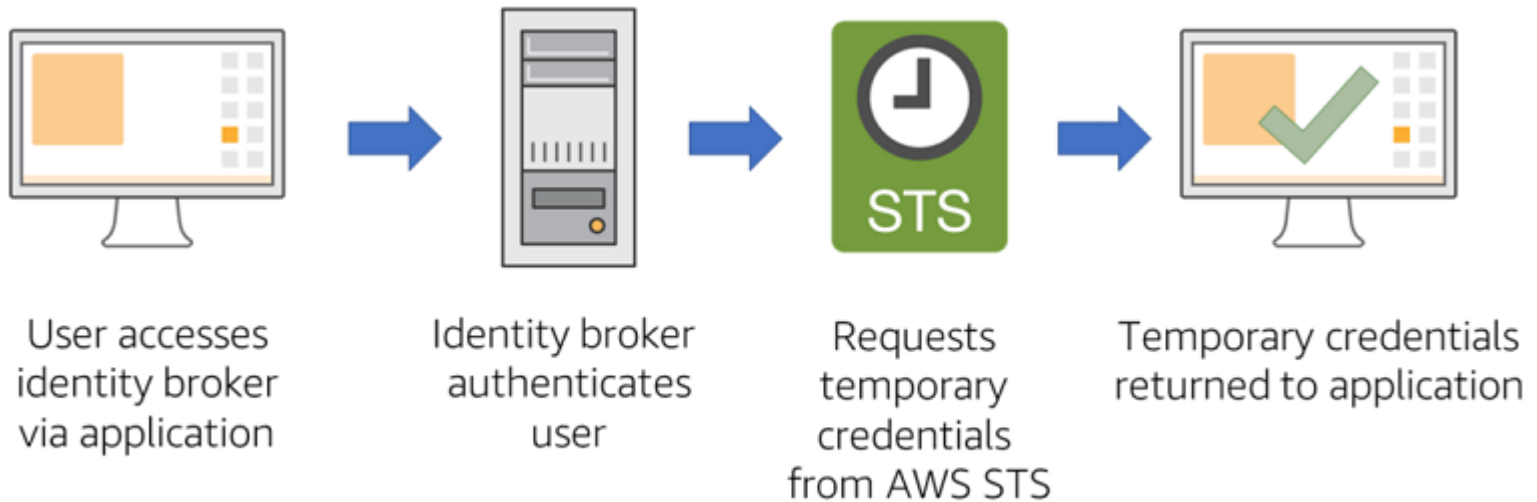
ID de cuenta\*

Este campo es obligatorio.

- Opciones
- ☐ Requerir un ID externo (practica recomendada si un tercero va a adoptar este rol)
  - ☐ Require MFA (Requerir MFA)

## 2.6 Capa de gestión usuarios IAM

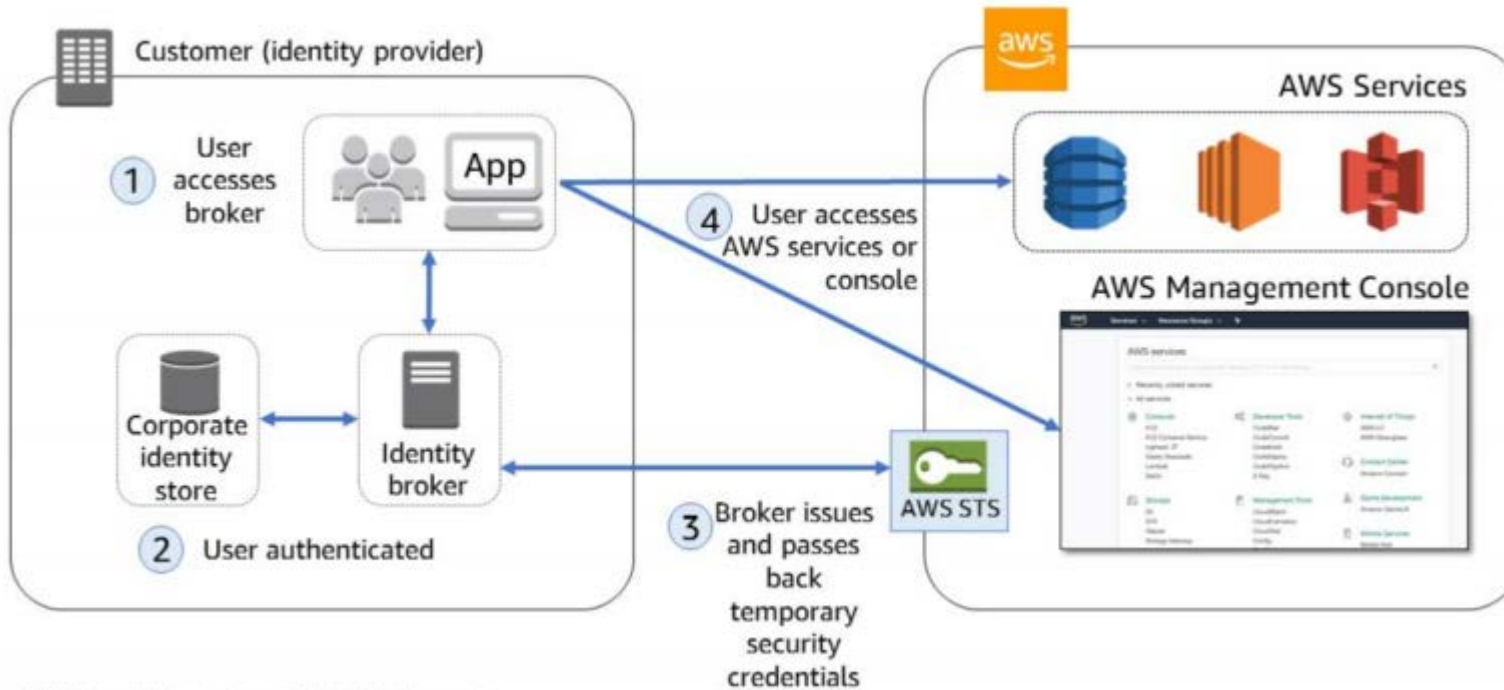
- Servicio IAM
  - Crear credenciales temporales a terceros
    - STS identity Broker -> SAML (Empresa ), OIDC (Aplicación WEB)



[https://docs.aws.amazon.com/es\\_es/IAM/latest/UserGuide/id\\_credentials\\_temp.html](https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/id_credentials_temp.html)

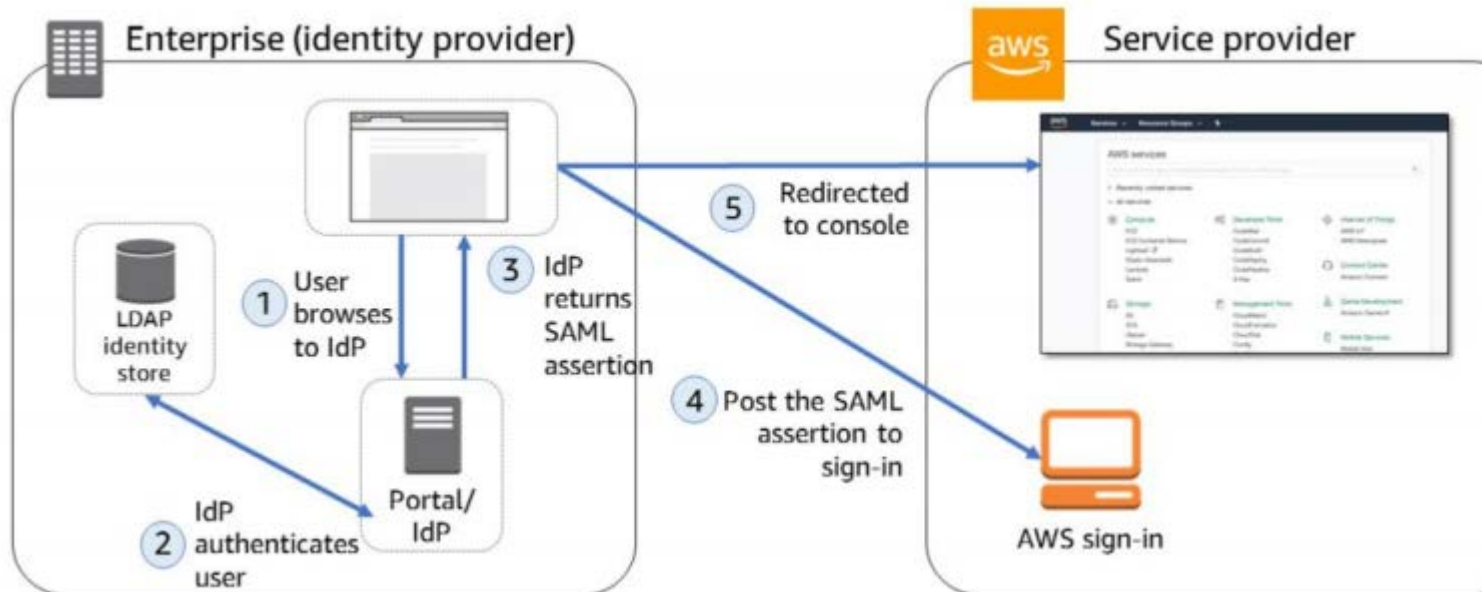
## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Crear credenciales temporales a terceros
    - STS identity Broker



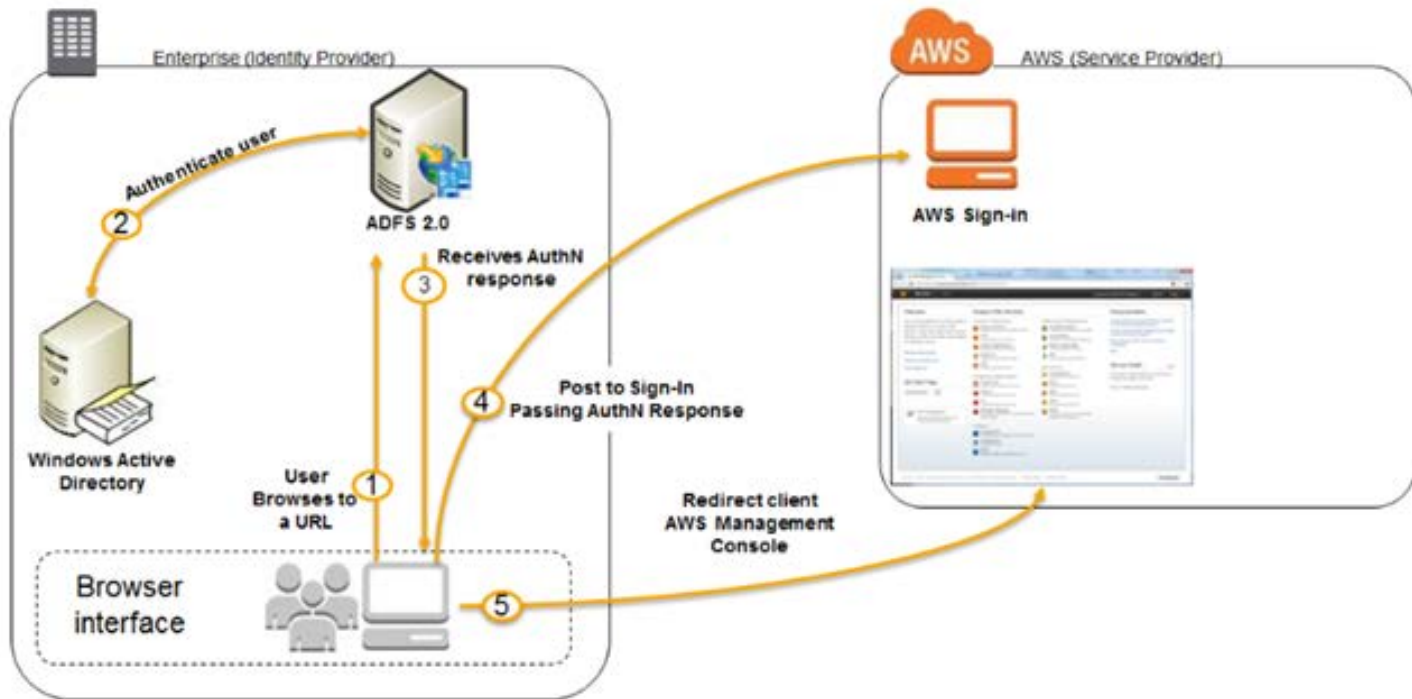
## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - SAML: Utilizar login empresarial



## 2.6 Capa de gestión usuarios IAM

- Servicio IAM
  - Ejemplo Single Sign-On (SSO) with SAML y Windows Active Directory + ADFS y AWS IAM Identity Provider

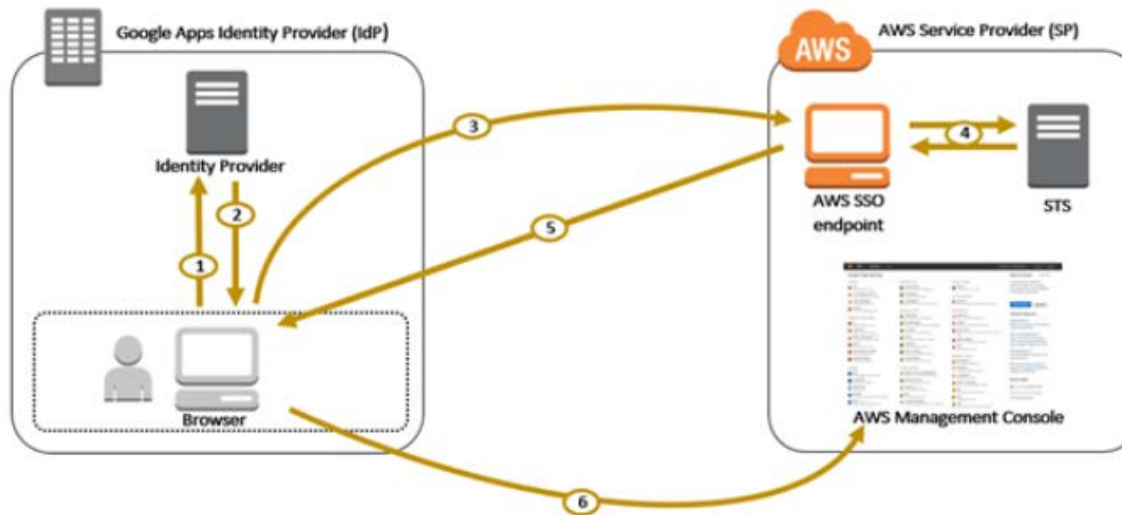


<https://aws.amazon.com/es/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/>



## 2.6 Capa de gestión usuarios IAM

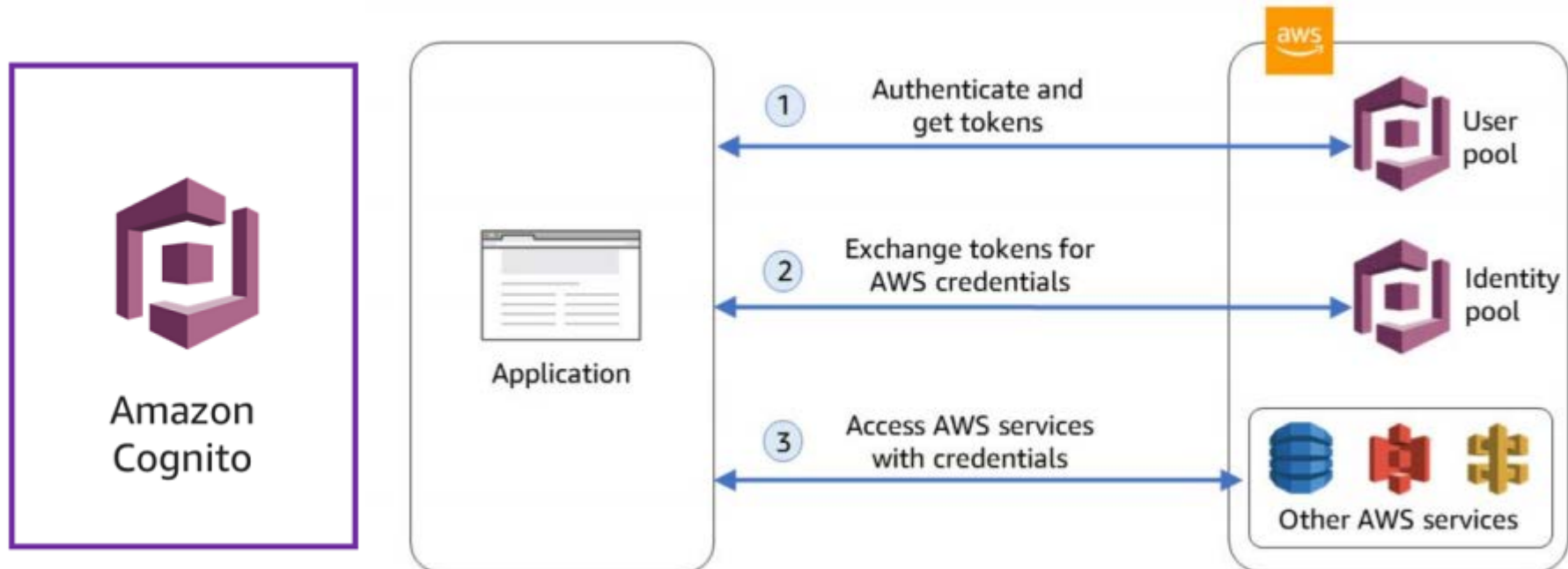
- Servicio IAM
  - Ejemplo Single Sign-On (SSO) with SAML y Google



<https://aws.amazon.com/es/blogs/security/how-to-set-up-federated-single-sign-on-to-aws-using-google-apps/>

## 2.6 Capa de gestión usuarios IAM

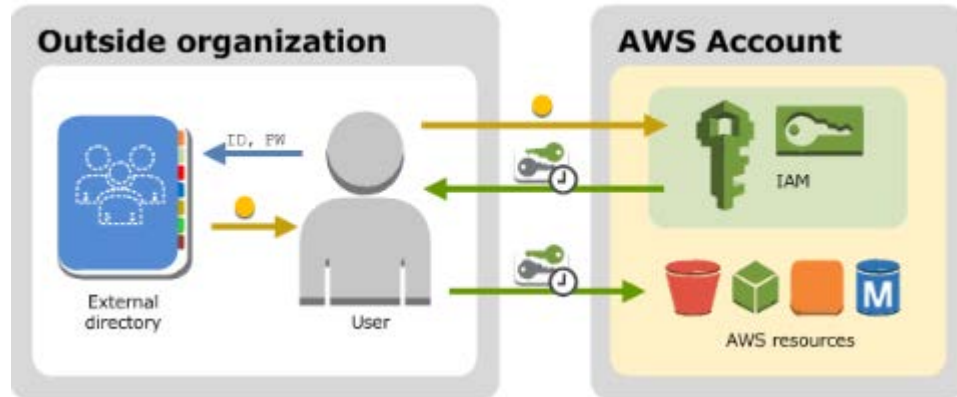
- Servicio IAM
  - Cognito
    - Servicio de autenticación para aplicaciones web y móviles
    - Permite logearse con username/password , o con credenciales de google, Facebook, ....
    - Permite asignar acceso a servicios AWS a lo usuarios



<https://aws.amazon.com/es/blogs/mobile/building-fine-grained-authorization-using-amazon-cognito-user-pools-groups/>

## 2.6 Capa de gestión usuarios IAM

- Usuarios IAM en una cuenta vs Federación de usuarios



SAML, Custom App, AWS Directory  
Service, OIDC -> Cognito

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - <https://awseducate.qwiklabs.com>

### Introduction to AWS Identity and Access Management (IAM)

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 Amazon EC2 instances

End Lab

00:42:58

Open Console

**Caution:** When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more.](#)

InstanceId

i-0f4d1e425ac150902

aws

Servicios ▾ Grupos de recursos ▾

jaagirre @ 7238-2637-0237 ▾

Consola de administración de AWS

Servicios de AWS

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM: Tags
- <https://aws.amazon.com/es/blogs/security/add-tags-to-manage-your-aws-iam-users-and-roles/>

Let's say I want to apply the same tags to all new IAM users so that I can track them consistently along with my other AWS resources. Now, when you [create a user](#), you can also pass in one or more tags. Let's say I want to ensure that all the administrators on my team apply a `CostCenter` tag. I create an IAM policy that includes the actions required to create and tag users. I also use the `Condition` element to list the tags required to be added to each new user during creation. If an administrator forgets to add a tag, the administrator's attempt to create the user fails.

**Note:** These actions are creating new users by using the AWS CLI.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ThisRequiresSpecificTagsWhenYouCreateANewUsers",
      "Effect": "Allow",
      "Action": [
        "iam:CreateUser",
        "iam:TagUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/CostCenter": "*"
        }
      }
    }
  ]
}
```

## 2.6 Capa de gestión usuarios IAM

- Servicio IAM: Tags

The preceding policy grants `iam:CreateUser` and `iam:TagUser` to allow creating and tagging IAM users in the AWS CLI. The `Condition` element that specifies the `CostCenter` tag is required during creation by using the condition key `aws:RequestTag`.

```
"Statement": [  
  {  
    "Sid": "ThisRequiresSpecificTagsWhenYouCreateANewUsers",  
    "Effect": "Allow",  
    "Action": [  
      "iam:CreateUser",  
      "iam:TagUser"  
    ],  
    "Resource": "*",  
    "Condition": {  
      "StringLike": {  
        "aws:RequestTag/CostCenter": "*" }  
    }  
  }  
]
```

## 2.6 Capa de gestión usuarios IAM

- Creación de un grupo con políticas concretas
  - Modificar política EC2Full para únicamente poder crear instancias t2.micro en la región Irlanda

```
{
  "Effect": "Deny",
  "Action": "ec2:*",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringNotEquals": {
      "ec2:InstanceType": [
        "t1.micro",
        "t2.micro"
      ]
    }
  }
}

{
  "Effect": "Deny",
  "Action": "ec2:*",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringNotEquals": {
      "aws:RequestedRegion": [
        "eu-central-1",
        "eu-west-1"
      ]
    }
  }
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - ¿Qué grupos y usuarios existen en el lab?

<input type="checkbox"/>	Nombre de grupo ↕	Usuarios	Política insertada
<input type="checkbox"/>	EC2-Admin	0	✓
<input type="checkbox"/>	EC2-Support	0	
<input type="checkbox"/>	S3-Support	0	

<input type="text" value="Buscar por nombre de usuario o clave de acceso"/>	
<input type="checkbox"/>	Nombre de usuario ▼ Grupos
<input type="checkbox"/>	awsstudent
<input type="checkbox"/>	root-qwkl
<input type="checkbox"/>	user-1 Ninguna
<input type="checkbox"/>	user-2 Ninguna
<input type="checkbox"/>	user-3 Ninguna



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - ¿Qué grupos y usuarios existen en el lab?
  - ¿Qué permisos tienen?

<input type="checkbox"/>	Nombre de grupo ↕	Usuarios	Política insertada
<input type="checkbox"/>	EC2-Admin	0	✓
<input type="checkbox"/>	EC2-Support	0	
<input type="checkbox"/>	S3-Support	0	

Q Buscar por nombre de usuario o clave de acceso	
<input type="checkbox"/>	Nombre de usuario ▼ Grupos
<input type="checkbox"/>	awsstudent
<input type="checkbox"/>	root-qwkl
<input type="checkbox"/>	user-1 Ninguna
<input type="checkbox"/>	user-2 Ninguna
<input type="checkbox"/>	user-3 Ninguna

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - Grupo EC2-support

IAM > Grupos > EC2-Support

### ▼ Resumen

**ARN del grupo:** arn:aws:iam::723826370:  
Support 

**Usuarios (en este grupo):** 0

**Ruta:** /spl66/

**Hora de creación:** 2019-09-25 15:46 UTC+

Usuarios

Permisos

Access Advisor

⚠ Este grupo no contiene ningún usuario.

Añadir usuarios al grupo


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "elasticloadbalancing:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "autoscaling:Describe*",
      "Resource": "*"
    }
  ]
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - Grupo EC2-admin

IAM > Grupos > EC2-Admin

### ▼ Resumen

**ARN del grupo:** arn:aws:iam::723826370237:group/spl66/EC2-Admin   
**Usuarios (en este grupo):** 0  
**Ruta:** /spl66/  
**Hora de creación:** 2019-09-25 15:46 UTC+0200

Usuarios

Permisos

Access Advisor

⚠ Este grupo no contiene ningún usuario.

[Añadir usuarios al grupo](#)


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:Describe*",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - Grupo EC2-admin

IAM > Grupos > EC2-Admin

### ▼ Resumen

**ARN del grupo:** arn:aws:iam::723826370237:group/spl66/EC2-Admin   
**Usuarios (en este grupo):** 0  
**Ruta:** /spl66/  
**Hora de creación:** 2019-09-25 15:46 UTC+0200

Usuarios

Permisos

Access Advisor

⚠ Este grupo no contiene ningún usuario.

[Añadir usuarios al grupo](#)


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:Describe*",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : AWS Educate Lab
  - Grupo EC2-support

IAM > Grupos > S3-Support

▼ Resumen

ARN del grupo:	arn:aws:iam::723826 Support 
Usuarios (en este grupo):	0
Ruta:	/spl66/
Hora de creación:	2019-09-25 15:46 UT

Usuarios

Permisos

Access Advice

⚠ Este grupo no contiene ningún usuario

Añadir usuarios al grupo

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Agregar los usuarios en los grupos correspondientes

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 Amazon EC2 instances

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Probar la accesibilidad
  - Copiar URL de login del usuario y abrir navegación incógnita

Usuarios > user-3

### Resumen

Elim

N de usuario arn:aws:iam::723826370237:user/spl66/user-3

Ruta /spl66/

de creación 2019-09-25 15:46 UTC+0200

Permisos

Grupos (1)

Etiquetas

Credenciales de seguridad

Acce

### Credenciales de inicio de sesión

Resumen

- Enlace de inicio de sesión de la consola:  
<https://723826370237.signin.aws.amazon.com/console>

Contraseña de la consola

Habilitada (nunca ha iniciado sesión) | Administración

- IAM user name: user-3
- Password: lab-password

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Probar la accesibilidad
  - Tratar de ver las instancias EC2 con user-1

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, 'Servicios', 'Grupos de recursos', a user profile 'user-1 @ 7238-2637-0237', and the region 'Ohio'. The left sidebar contains navigation links: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (expanded), Instances (selected), Launch Templates, and Spot Requests. The main content area displays the 'Launch Instance' button, a 'Connect' button, and an 'Actions' dropdown. Below these is a search bar 'Filter by tags and attributes or search by keyword' and a table header with columns: Name, Instance ID, Instance Type, Availability Zone, and Instance State. A yellow highlight is drawn around the error message: 'An error occurred fetching instance data: You are not authorized to perform this operation.'



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Probar la accesibilidad
  - Tratar de ver las instancias EC2 con user-2
  - Y tratar de parar la instancia

Are you sure you want to stop these instances?

i-0f4d1e425ac150902



**Note that when your instances are stopped:**

Any data on the ephemeral storage of your instances will be lost.



### Error stopping instances

You are not authorized to perform this operation. Encoded authorization token: 4c3He\_TzAO7tz2RDeLQtaSnEZHFVRVHowFjGFO9WuTNTP3voC-y7feeNwuAKLmcapljiliCst94zZmMKfNTZeNcPFmk4YIqwf6D8:ptw9HOcRlg3przJguRGfCPWiks9BsWy2IWR3leFaBZ-GruIWFLcK6g\_MrSsGY6oV9i0y7tF-CwrTaLMj7lxe74w1TVdd4ShcLR0wYSzxnigNdrFLgzJODnIn1Vutk82dYrTqwJxwqLyn2XNJbiuwGxJlcPTyfmIGv9qNznIraE\_cSI1g6TZX\_x6VA268vu6\_fgkCVPv6Gmo\_lxX

os ▾ Grupos de recursos ▾ ⚡ 🔔 user-2 @ 7238-2637-0237 ▾ Oregón

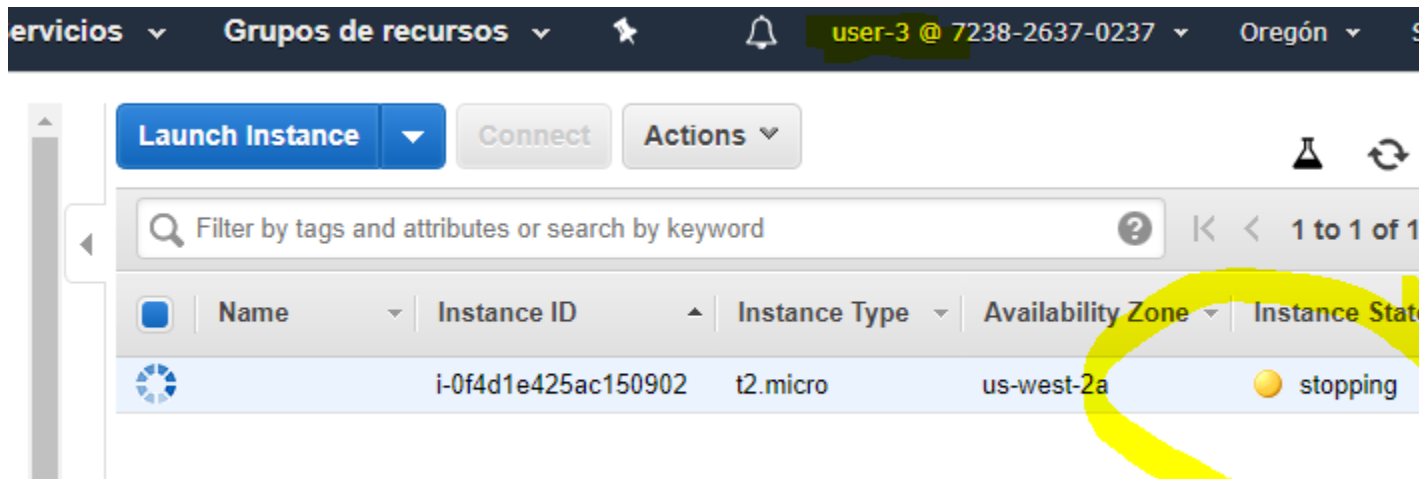
Launch Instance ▾ Connect Actions ▾

Filter by tags and attributes or search by keyword ? |< < 1

<input type="checkbox"/>	Name ▾	Instance ID ▴	Instance Type ▾	Availability Zone ▾	Insta
<input type="checkbox"/>		i-0f4d1e425ac150902	t2.micro	us-west-2a	● ru

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Probar la accesibilidad
  - Tratar de ver las instancias EC2 con user-3
  - Y tratar de parar la instancia



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM
  - Para esta práctica es necesario una cuenta con acceso al IAM
    - El starter account y los classrooms no permiten trabajar con el servicio IAM!!!!!!
  - Crear usuario para tareas de administración
  - Bloquear la cuenta raíz
  - Creación de un grupo con políticas concretas



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Crear un grupo para tareas de administración

### Establecer el nombre de grupo

Especifique un nombre de grupo. Los nombres de grupos se p

**Nombre de grupo:**

Ejemplo: Desarrolladores o Proyecto  
128 caracteres como máximo

**Filtro:** Tipo de política ▼

		Nombre de la política ↕	Entidades asociadas
<input checked="" type="checkbox"/>		AdministratorAccess	2

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Crear un usuario y agregarlo al nuevo grupo de “*admins*”

### Establecer los detalles del usuario

Puede añadir varios usuarios a la vez con los mismos permisos y el mismo tipo de acceso. [Más inf](#)

Nombre de usuario\* admin  
[+ Añadir otro usuario](#)

Los usuarios con acceso a la consola de administración de AWS pueden iniciar sesión en:  
<https://420693608596.signin.aws.amazon.com/console>

[Descargar .csv](#)

### Seleccionar el tipo de acceso de AWS

Seleccione la forma en que estos usuarios accederán a AWS. Las claves de acceso se generan en el último paso. [Más información](#)

	Usuario	ID de clave de acceso	Clave de acceso secreta	Contraseña	Enviar instrucciones
	admin2	AKIAWD42LBCKLBYUKTV2	***** <a href="#">Mostrar</a>	***** <a href="#">Mostrar</a>	<a href="#">Enviar correo electrónico</a>

- Tipo de acceso\* ☒ **Acceso mediante programación**  
Habilita una **ID de clave de acceso** y una **clave de acceso** para la CLI y la API de AWS, además de otras herramientas de línea de comandos.
- ☒ **Acceso a la consola de administración de AWS**  
Habilita una **contraseña** que permite a los usuarios iniciar sesión en la consola de administración de AWS.

Contraseña de la consola\* ☐ Contraseña generada automáticamente  
☒ Contraseña personalizada

.....

☐ Mostrar contraseña

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Cuenta Root con login MFA

Factores de forma de MFA

	Dispositivo MFA virtual	Llave de seguridad Universal 2nd Factor (U2F)	Dispositivo MFA de llave única de hardware	Dispositivo MFA de tarjeta gráfica de hardware	Dispositivo MFA con SMS (vista previa)	Llave única de hardware Dispositivo MFA para AWS GovCloud (EE.UU.)
Dispositivo	Consulte la tabla que aparece a continuación.	Comprar.	Comprar.	Comprar.	Utilice su dispositivo móvil.	Comprar.
Factor de forma físico	Utilice su smartphone o tablet y ejecute cualquier aplicación que admita el estándar abierto <a href="#">TOTP</a> .	Llave de seguridad de hardware duradera, impermeable y resistente a golpes YubiKey, suministrada por el proveedor externo Yubico.	Dispositivo de llave única de hardware con precinto de seguridad, suministrado por el proveedor externo Gemalto.	Dispositivo con tarjeta gráfica de hardware con precinto de seguridad, suministrado por el proveedor externo Gemalto.	Cualquier dispositivo móvil que pueda recibir mensajes SMS (Servicio de mensajes cortos).	Dispositivo de llave única de hardware con precinto de seguridad, suministrado por el proveedor externo SurePassID.
Precio	Gratis	40,00 USD	12,99 USD	19,99 USD	Es posible que se apliquen cargos por SMS o datos.	15,95 USD
Características	Compatible con varios tokens en un solo dispositivo.	Compatible con varias cuentas raíz o usuarios de IAM mediante una única llave de seguridad.	El mismo tipo de dispositivo que utilizan muchos servicios financieros y empresariales.	Similar a los dispositivos de llave única, pero con un factor de forma que le permite transportarlo en la cartera.	Opción familiar con reducidos costos de configuración.	Un dispositivo de llave única exclusivamente para uso con cuentas <a href="#">AWS GovCloud</a> .

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Cuenta Root con login MFA

### Aplicaciones MFA virtuales

Las aplicaciones de su smartphone se pueden instalar desde la tienda de aplicaciones correspondiente a su tipo de teléfono. E especifican algunas aplicaciones para distintos tipos de smartphone.

Android

Google Authenticator; autenticación de 2 factores de Authy

iPhone

Google Authenticator; autenticación de 2 factores de Authy

Windows Phone

Authenticator

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Cuenta Root con login MFA
  - Una vez instalada la aplicación en el móvil
  - Activar MFA en la cuenta RAIZ

**Identity and Access Management (IAM)**

▼ AWS Account (420693608596)

Panel

Grupos

Usuarios

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

Informe de credenciales

Q Buscar en IAM

▼ AWS Organizations

Organization activity

Service control policies (SCPs)

### Le damos la bienvenida a Identity and Access Management (IAM)

Enlace de inicio de sesión de los usuarios de IAM:

<https://420693608596.signin.aws.amazon.com/console> | Personaliz

### Recursos de IAM

Usuarios: 7 Roles: 9

Grupos: 4 Proveedores de identidad: 0

Políticas administradas por el cliente: 1

Estado de seguridad 4 de 5 completado

- ✓ Eliminar las claves de acceso raíz
- ✓ Activar MFA en la cuenta raíz
- Administrar MFA
- ✓ Crear usuarios de IAM individuales
- ✓ Utilizar grupos para asignar permisos
- ⚠ Aplicar una política de contraseñas de IAM

Active la autenticación multifactor (MFA) en su cuenta raíz de AWS para añadir una capa de protección adicional que le ayude a mantener la seguridad de la cuenta. [Más información](#)



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Cuenta Root con login MFA
  - Una vez instalada la aplicación en el móvil
  - Activar MFA en la cuenta RAIZ



**Identity and Access Management (IAM)**

- ▼ AWS Account (420693608596)
  - Panel
  - Grupos
  - Usuarios
  - Roles
  - Políticas
  - Proveedores de identidad
  - Configuración de cuenta
  - Informe de credenciales

Q Buscar en IAM

### Sus credenciales de seguridad

Utilice esta página para administrar las credenciales de su cuenta de AWS. Para administrar Management (IAM), utilice una lista [Consola de IAM](#).

Para obtener más información sobre los tipos de credenciales de AWS y cómo utilizarlas de AWS.

▲ Contraseña

▼ Multi-Factor Authentication (MFA)

Utilice MFA para aumentar la seguridad de los entornos de AWS. Para iniciar sesión contraseña y código de autenticación de un dispositivo MFA.

Tipo de dispositivo	Número de serie
Virtual	arn:aws:iam::420693608596:mfa/root-account-mfa-device

1. Instale una aplicación compatible en el equipo o dispositivo móvil

Consulte la información de [lista de aplicaciones compatibles](#)

2. Utilice la aplicación de MFA virtual y la cámara del dispositivo para escanear el código QR



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Cuenta Root con login MFA
  - Una vez instalada la aplicación en el móvil
  - Activar MFA en la cuenta RAIZ
  - escanear qr con el móvil
  - E insertar los dos códigos de MFA en la consola de AWS

### Configurar un dispositivo MFA virtual

1. Instale una aplicación compatible en el equipo o dispositivo móvil

Consulte la información de [lista de aplicaciones compatibles](#)

2. Utilice la aplicación de MFA virtual y la cámara del dispositivo para escanear el código QR



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM : Bloquear la cuenta raíz
  - Eliminar todas las claves de acceso
- Ahora solo se puede acceder a la cuenta con el password y el móvil
  - Que pasa si se pierde el móvil???

### Solución de problemas con el dispositivo de autenticación

#### Volver a sincronizar con los servidores de AWS

Si su dispositivo con autenticación multifactor (MFA) parece estar funcionando correctamente y, sin embargo, no puede iniciar sesión, es posible que el dispositivo esté desincronizado.

[Volver a sincronizar el dispositivo de MFA](#)

#### Iniciar sesión con otros factores de autenticación

Si su dispositivo de autenticación multifactor (MFA) se ha perdido, está averiado o no funciona, puede iniciar sesión con otros factores de autenticación. Debe verificar su identidad utilizando el correo electrónico y teléfono que están registrados en esta cuenta.

[Iniciar sesión con otros factores](#)

#### Póngase en contacto con el servicio de atención al cliente

Si no puede iniciar sesión en su cuenta con el dispositivo de MFA u otros factores de autenticación, póngase en contacto con el servicio de atención al cliente. Un representante del servicio de atención al cliente podrá comprobar la propiedad de su cuenta y desactivar la configuración de MFA.

[Póngase en contacto con el servicio de atención al cliente](#)

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM :Crear Política de passwords

### ▼ Política de contraseñas

Una política de contraseñas es un conjunto de reglas que puede establecer. [Más información](#)

#### Política de contraseñas

Esta cuenta de AWS no tiene una política de contraseñas

**Establecer la política de contraseñas**

### ▼ Security Token Service (STS)

### Establecer la política de contraseñas

La política de contraseñas es un conjunto de reglas que definen los requisitos de complejidad y los periodos de rotación obligatorios para las contraseñas de los usuarios de IAM. [Más información](#)

Seleccione los requisitos de la política de contraseñas de su cuenta:

☒ Establecer la longitud mínima de la contraseña

caracteres

☐ Exigir al menos un carácter en mayúscula del alfabeto latino (A-Z)

☐ Exigir al menos un carácter en minúscula del alfabeto latino (a-z)

☐ Require at least one number

☐ Require at least one non-alphanumeric character (!@#\$%^&\*()\_+=[]{}|')

☐ Enable password expiration

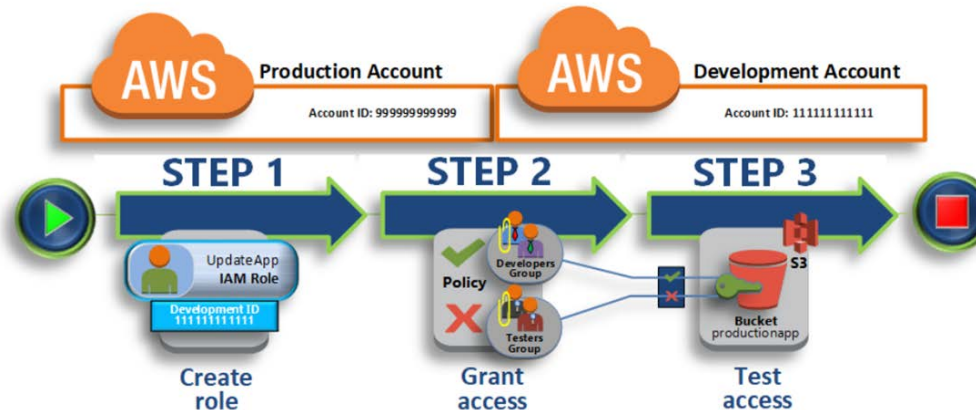
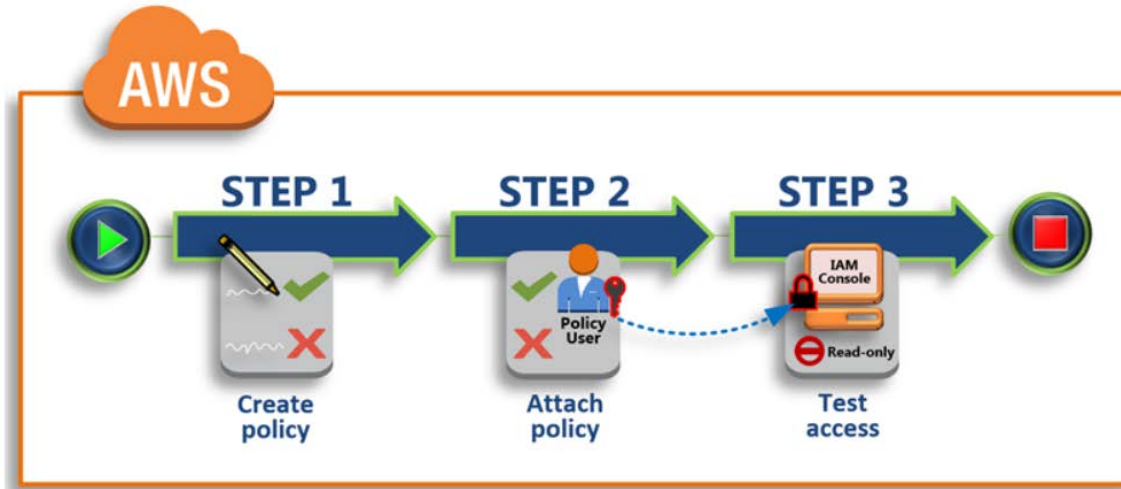
☐ Password expiration requires administrator reset

☐ Allow users to change their own password

☐ Prevent password reuse

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas

- Vamos a crear un grupo de desarrolladores
  - SOLO PODRAN CREAR MAQUINAS EC2 MINIMAS Y EN IRLANDA

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:Describe*",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:GetConsole*"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "arn:aws:ec2:us-east-1:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceType": [
            "t1.micro",
            "t2.micro"
          ]
        }
      }
    }
  ]
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Crear grupo dev y usuario dev1
    - Crear inicialmente el grupo dev con permisos EC2Full

[Descargar .csv](#)

	Usuario	ID de clave de acceso	Clave de acceso secreta	Contraseña
▶ ✓	dev1	AKIAWD42LBCKPSPVLV6K	***** <a href="#">Mostrar</a>	***** <a href="#">Mostrar</a>

Usuarios

Permisos

Access Advisor

Políticas administradas

Las siguientes políticas administradas se han asociado a este grupo de políticas administradas.

[Asociar la política](#)

Nombre de la política	Acciones
 AmazonEC2FullAccess	<a href="#">Mostrar la política</a>   <a href="#">Desasociar</a>

## 2.6 Capa de gestión usuarios IAM

- **Práctica: Configuración básica IAM:**  
Creación de un grupo con políticas concretas

- Modificar política grupo dev
  - Partir de la política EC2Full

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "ec2:*",
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "elasticloadbalancing:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "autoscaling:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Modificar política EC2Full para únicamente poder crear instancias t2.micro en la región Irlanda

Usuarios Permisos Access Advisor

Políticas administradas

No hay ninguna política administrada asociada a este grupo.

[Asociar la política](#)

Políticas insertadas

No hay políticas insertadas para mostrar. Para crear una, [haga clic aquí](#).

Políticas del servicio de grupo de usuarios

☐ Generador de políticas

☒ Política personalizada

Utilice el editor de políticas para personalizar su propio conjunto de permisos.

[Seleccionar](#)

## 2.6 Capa de gestión usuarios IAM

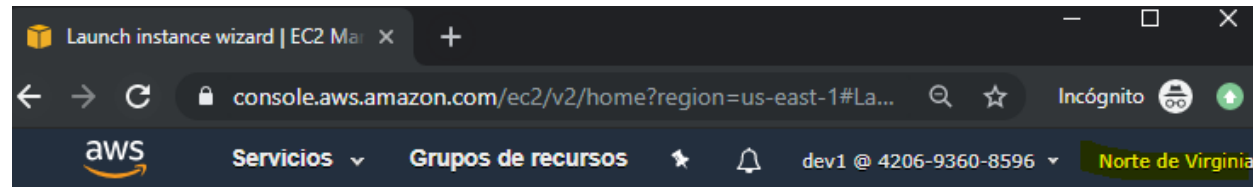
- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Modificar política EC2Full para únicamente poder crear instancias t2.micro en la región Irlanda

```
{
  "Effect": "Deny",
  "Action": "ec2:*",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringNotEquals": {
      "ec2:InstanceType": [
        "t1.micro",
        "t2.micro"
      ]
    }
  }
}

{
  "Effect": "Deny",
  "Action": "ec2:*",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringNotEquals": {
      "aws:RequestedRegion": [
        "eu-central-1",
        "eu-west-1"
      ]
    }
  }
}
```

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Validar nueva regla : Crear instancia t2.micro en EEUU



### Launch Status

**! Launch Failed**

You are not authorized to perform this operation. Encoded authorization failure message: eUm-l2JhgXTYQB4QmQGQTySGklQkAMIDuA8xrWYJSouAJhSnjloNJMFYfpQzv7HzqUQc4fcey9m8BghfNGXTxbBli7lUw3MfIYbojmg\_CPHoF4Z5ARVJPkQ675bmUzJ7hWvUMqrZslr\_eFVGRqKmwakDH0MiLK9ke0fgZyX5nlMwf6H94CyOssSVmgSjVWeoOOxqOoHRsGzxpAii36odTy34WJQVAlvPt3wWYJUR8uvjR2laEyEdNdTZF-rFnhWuzzhsW-l-tMSBuud87hsUC7XXTum4HSOTs-vW\_f96DtiCJoYEz16aOv4-9adUMv-zucsc-NYu5CRm0CcHtMeRy0Jvs8DBCf1jQPSgy8qnbCx1LgyY8A7GS8XqB\_urQUBrfJ8X6HX7OjxpgFE1Ocp-1vh4bl0KuSNd\_J3OeApfPBJTZi08EJXqPWAVdTmT-NJt8TG5-SdglX7CsA-58wvG0DhiTlsfdtrh8cbjJOH\_5hKgx7fhYtU2Ny-JtEr1xIIWOFA0YT3T635vhJRWZ7b96xlnDmk85V9cnrDQhOYrVCHRTqk2fK3a-8D6sm\_mY6gCx-YQNyphH\_QHnMWWuAYCqU6R5RuVBRakJs89eHeaebDNmjnCMm8M6EBQwim-mxsRxtM9vLK-0HipeHHz6UXrzyruikjGSTKEAoChog1A6HbaIC6ls-IG\_Wc2kOu74HiUMB76jDOPI-sIIlSBOc32FsqhF1fclPnDFDcexWKISpni1B6qcG7UvYKT\_Pbx8RygL5erJRzlx3cJDFeQEfvMaereCmbe

[View launch log](#)

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Validar nueva regla : Crear instancia t2.micro en Europa

Launch Status

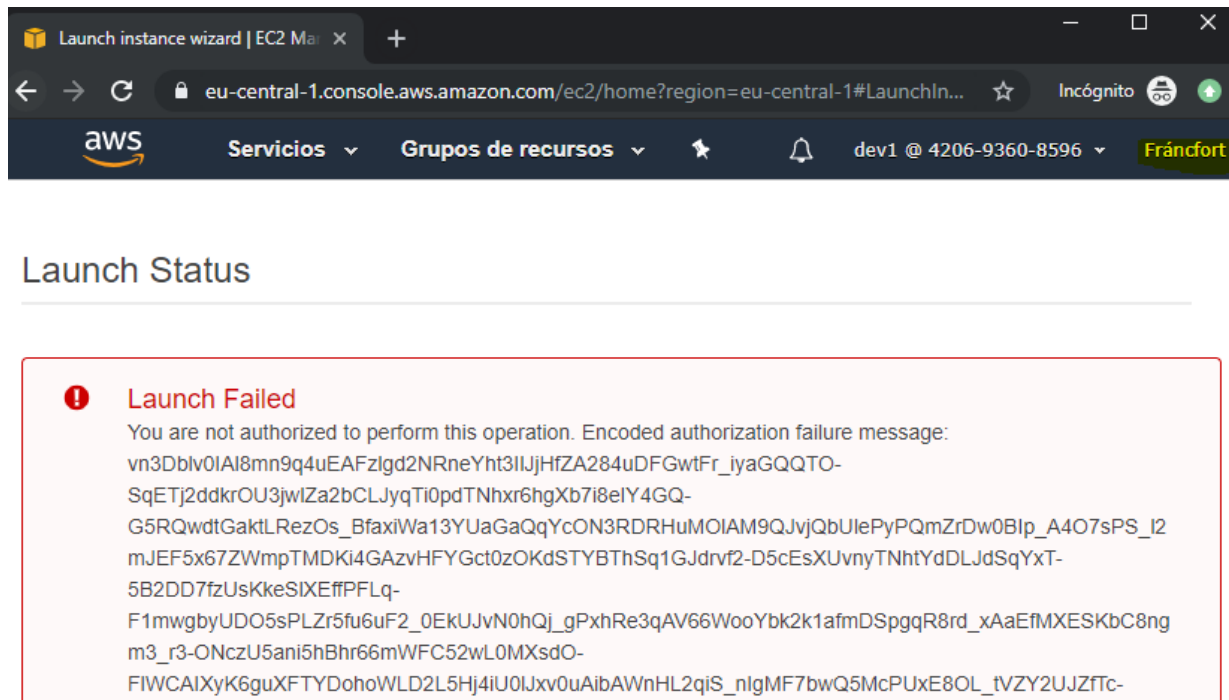
✓ Your instances are now launching  
The following instance launches have been initiated: i-0889650495c932e52 [View launch log](#)

ℹ Get notified of estimated charges  
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

	Name	Instance ID	Instance Type	Availability Zone	Insta
<input checked="" type="checkbox"/>		i-0889650495c932e52	t2.micro	eu-central-1b	ru

## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Validar nueva regla : Crear instancia t2.medium en Europa



## 2.6 Capa de gestión usuarios IAM

- Práctica: Configuración básica IAM: Creación de un grupo con políticas concretas
  - Y durante un tiempo concreto

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "service-prefix:action-name",
    "Resource": "*",
    "Condition": {
      "DateGreaterThan": {"aws:CurrentTime": "2017-07-01T00:00:00Z"},
      "DateLessThan": {"aws:CurrentTime": "2017-12-31T23:59:59Z"}
    }
  }
}
```

## 2.6 Capa de gestión usuarios IAM

- Recursos : Definición de políticas
  - Buenas prácticas
    - [https://github.com/awsdocs/iam-user-guide/blob/master/doc\\_source/best-practices.md](https://github.com/awsdocs/iam-user-guide/blob/master/doc_source/best-practices.md)
  - Ejemplos de políticas
    - [https://github.com/awsdocs/iam-user-guide/blob/master/doc\\_source/access\\_policies.md](https://github.com/awsdocs/iam-user-guide/blob/master/doc_source/access_policies.md)
  - Operadores de condiciones
    - [https://docs.aws.amazon.com/es\\_es/IAM/latest/UserGuide/reference\\_policies\\_elements\\_condition\\_operators.html](https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html)
    - [https://docs.aws.amazon.com/es\\_es/IAM/latest/UserGuide/reference\\_policies\\_multi-value-conditions.html](https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/reference_policies_multi-value-conditions.html)