



## Integración AWS

<b>Control de versiones</b>	<b>2</b>
<b>Modelo de integración</b>	<b>3</b>
Autenticación y autorización (Oauth2)	3
Configuración de autenticación	3
Configuración de autorización	4
Gobierno activo	4
Nomenclatura de los grupos	4
<b>Credenciales requeridas</b>	<b>5</b>
Autenticación	5
Autorización (Oauth2)	8
Gobierno activo	10
<b>Emulación SSO vía Oauth2</b>	<b>10</b>

## Control de versiones

<b>Versión</b>	<b>Fecha de modificación</b>	<b>Responsable</b>	<b>Aprobador</b>	<b>Resumen de cambios</b>
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento

# Modelo de integración

## Autenticación y autorización (Oauth2)

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

### Configuración de autenticación

En la propiedad `security.authentication.oidc.providers` colgarán los distintos proveedores de autenticación que tengamos. En el caso de AWS debemos poner las siguientes propiedades:

```
security:
  ...
  authentication:
    oidc:
      providers:
        aws:
          name: Anjana AWS IAM
          authorize-url:
https://${security.authentication.oidc.providers.aws.domain}.auth.${sec
urity.authentication.oidc.providers.aws.region}.amazoncognito.com/login
?response_type=code&client_id=${security.authentication.oidc.providers.
aws.client-id}&redirect_uri=${security.authentication.oidc.providers.aw
s.redirect-uri}&state=STATE&scope=${security.authentication.oidc.provid
ers.aws.scopes}
          token-url:
https://${security.authentication.oidc.providers.aws.domain}.auth.${sec
urity.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth
2/token
          scopes: openid+profile
          client-id: asdfasdfasdfasdfasdfasdf
          client-secret: a8sdfasd6as7d68f8sd6f78a6ds76d8qaasd6
          client-authentication-method: GET
          redirect-uri: https://localhost:8443/anjana/authorized
          username-claim: cognito:username
          type: AWS
          region: eu-west-1
          domain: anjana-app-desarrollo
```

## Configuración de autorización

En la propiedad `security.authorization` colgarán los distintos proveedores de autenticación que tengamos. En el caso de AWS debemos poner sus propiedades:

```
aws:
  providers:
    anjana-dev-app:
      poolID: eu-west-1_FOxxxxx
      region: eu-west-1
      accessKey: AAAAAAAAAAAAAAAAAA
      secretKey: aaaaaaaaaaaaabbbbbbbbbbbbbbcccccccccccccc
```

- `groupOrgUnitSeparator`: separador de partes de unidad organizativa en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida) (En caso de configurar un separador distinto a '/', en el provider las OUs no se puede usar '/' como parte de un nombre de OU)
- `roleOrgUnitSeparator`: separador del rol del resto de la cadena en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)
- `groupPrefix`: prefijo que contengan los grupos (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)

## Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre AWS es "Tot plugin AWS IAM".

## Nomenclatura de los grupos

El nombre del grupo debe contener el alias de la unidad organizativa y el rol que aplica a dicha unidad organizativa.

Un ejemplo de un nombre de un grupo sería : HQ/Legal-architect , donde HQ/Legal es el alias de la unidad organizativa y architect el rol.

Como se puede observar hay dos separadores:

-El separador de jerarquía de la unidad organizativa → '/', cuyo valor es configurable gracias a la propiedad del yml: `roles.separator-organizational-unit`.

-El separador de la unidad organizativa y el rol → '-', cuyo valor es configurable gracias a la propiedad del yml: `roles.separator-role`.

## Credenciales requeridas

La credencial puede ser única aglutinando los permisos de ambas, pero se recomienda mantenerlas por separado de cara a facilitar la monitorización y auditoría de la actividad ejercida por las mismas.

## Autenticación

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

Es necesario registrar un grupo de usuarios en el servicio Amazon Cognito con las siguientes propiedades.



The screenshot shows the Amazon Cognito console page. At the top, there is a navigation bar with the AWS logo, a search bar, and a dropdown menu for 'Servicios'. The main content area features the Amazon Cognito logo and the text: 'Amazon Cognito ofrece grupos de usuarios y de identidades. Los grupos de usuarios son directorios de usuarios que proporcionan a los usuarios de las aplicaciones opciones para inscribirse e iniciar sesión. Los grupos de identidades proporcionan las credenciales de AWS para conceder a los usuarios acceso a otros servicios de AWS.' Below this text are two buttons: 'Administrar grupos de usuarios' and 'Administrar grupos de identidades'. At the bottom, there are two columns of information. The left column is titled 'Añadir la funcionalidad de inscripción e inicio de sesión' and includes the text: 'Los grupos de usuarios de Cognito le permiten añadir de forma fácil y segura la funcionalidad de inscripción e inicio de sesión a sus'. The right column is titled 'Conceda acceso a sus usuarios a los servicios de AWS' and includes the text: 'Los grupos de identidades de Cognito permiten que su aplicación obtenga credenciales temporales para que usuarios invitados anónimo'.

En el apartado “Clientes de aplicación” obtendremos las credenciales que más tarde habrá que indicar en la configuración de Zeus.

aws Servicios  [Alt+S] Soporte

Grupos de usuarios | Identidades federadas

## anjana-app-desarrollo

Configuración general

- Usuarios y grupos
- Atributos
- Políticas
- MFA y verificaciones
- Seguridad avanzada
- Personalizaciones de mensaje
- Etiquetas
- Dispositivos
- Clientes de aplicación
- Desencadenadores
- Análisis

Integración de aplicaciones

- Configuración del cliente de aplicación
- Nombre del dominio
- Personalización de la interfaz de usuario
- Servidores de recursos

Federación

- Proveedores de identidades
- Mapeo de atributos

### ¿Qué clientes de aplicación tendrán acceso a este grupo de usuarios?

Los clientes de aplicación que añada recibirán un ID único y una clave secreta opcional para obtener acceso a este grupo de usuarios.

**ID de cliente de aplicación**

**Clave secreta de cliente de aplicación**

**Actualizar el vencimiento del token**

días y  minutos

*Deben estar comprendidos entre 60 minutos y 3650 días*

**Vencimiento del token de acceso**

días y  minutos

*Deben estar comprendidos entre 5 minutos y 1 día. No pueden ser mayores que el vencimiento del token de actualización.*

### How do you want your end users to sign in?

You can choose to have users sign in with an email address, phone number, username or preferred username plus their password. [Learn more.](#)

**Username** - Users can use a username and optionally multiple alternatives to sign up and sign in.

- Also allow sign in with verified email address
- Also allow sign in with verified phone number
- Also allow sign in with preferred username (a username that your users can change)

**Email address or phone number** - Users can use an email address or phone number as their "username" to sign up and sign in.

- Allow email addresses
- Allow phone numbers
- Allow both email addresses and phone numbers (users can choose one)

You can choose to enable case insensitivity on the username input for the selected sign-in option. For example, when this option is selected, the users can sign in using either "username" or "Username".

(Recommended) Enable case insensitivity for username input

### Which standard attributes do you want to require?

All of the standard attributes can be used for user profiles, but the attributes you select will be required for sign up. You will not be able to change these requirements after the pool is created. If you select an attribute to be an alias, users will be able to sign-in using that value or their username. [Learn more about attributes.](#)

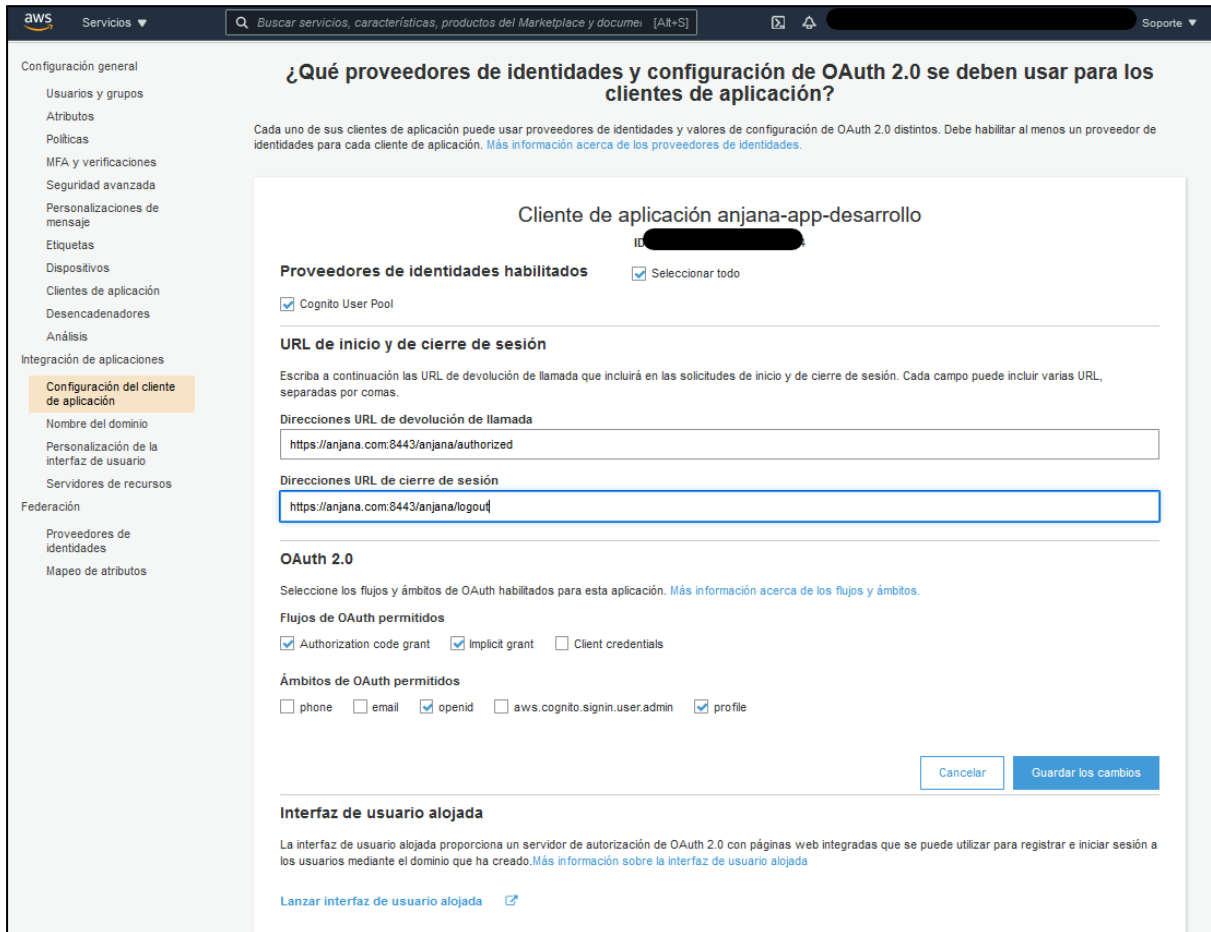
Required	Attribute	Required	Attribute
<input type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username
<input type="checkbox"/>	gender	<input type="checkbox"/>	profile
<input type="checkbox"/>	given name	<input type="checkbox"/>	zoneinfo
<input type="checkbox"/>	locale	<input type="checkbox"/>	updated at
<input type="checkbox"/>	middle name	<input type="checkbox"/>	website
<input type="checkbox"/>	name		

### Do you want to add custom attributes?

Enter the name and select the type and settings for custom attributes.

En el apartado “Configuración del cliente de aplicación” configuraremos las url acordes al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta dos, más la de log out:

- <https://<host>:<port>/anjana/authorized>
- <https://<host>:<port>/anjana/logout>



The screenshot shows the AWS IAM console page for configuring an application client. The title is "¿Qué proveedores de identidades y configuración de OAuth 2.0 se deben usar para los clientes de aplicación?". The client name is "Cliente de aplicación anjana-app-desarrollo".

**Proveedores de identidades habilitados:**  Selecionar todo,  Cognito User Pool.

**URL de inicio y de cierre de sesión:**

- Direcciones URL de devolución de llamada:
- Direcciones URL de cierre de sesión:

**OAuth 2.0:**

- Flujos de OAuth permitidos:  Authorization code grant,  Implicit grant,  Client credentials.
- Ámbitos de OAuth permitidos:  phone,  email,  openid,  aws.cognito.signin.user.admin,  profile.

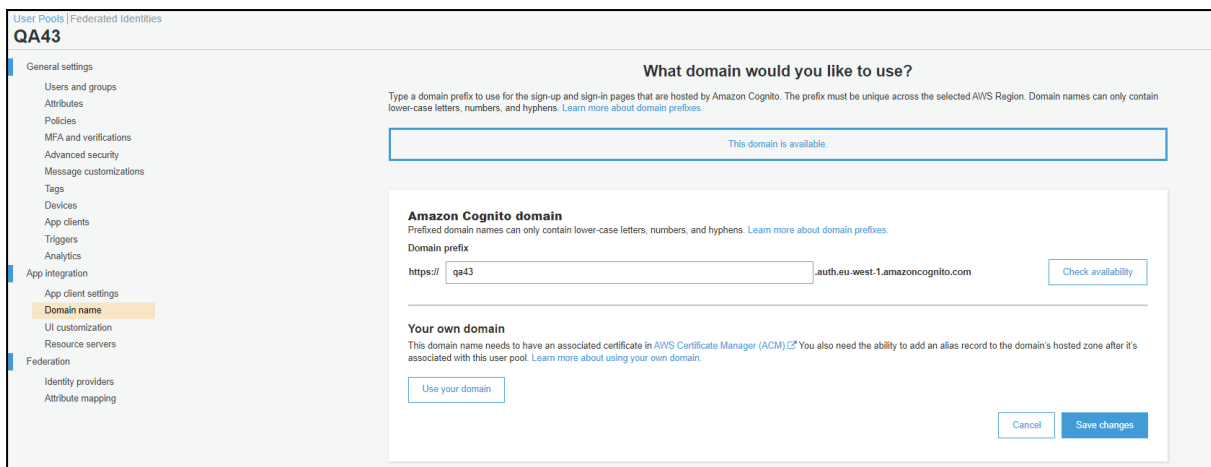
Buttons: "Cancelar", "Guardar los cambios".

**Interfaz de usuario alojada:**

La interfaz de usuario alojada proporciona un servidor de autorización de OAuth 2.0 con páginas web integradas que se puede utilizar para registrar e iniciar sesión a los usuarios mediante el dominio que ha creado. [Más información sobre la interfaz de usuario alojada](#)

[Lanzar interfaz de usuario alojada](#)

También entramos al apartado de nombre del dominio, que está justo abajo. Ahí debemos de poner el nombre del pool, en minúsculas.



The screenshot shows the "What domain would you like to use?" page in the AWS IAM console. The title is "What domain would you like to use?".

Text: "Type a domain prefix to use for the sign-up and sign-in pages that are hosted by Amazon Cognito. The prefix must be unique across the selected AWS Region. Domain names can only contain lower-case letters, numbers, and hyphens. [Learn more about domain prefixes.](#)"

Input field:  This domain is available

**Amazon Cognito domain:**

Prefixed domain names can only contain lower-case letters, numbers, and hyphens. [Learn more about domain prefixes.](#)

Domain prefix:  .auth.eu-west-1.amazoncognito.com

**Your own domain:**

This domain name needs to have an associated certificate in [AWS Certificate Manager \(ACM\)](#). You also need the ability to add an alias record to the domain's hosted zone after it's associated with this user pool. [Learn more about using your own domain.](#)

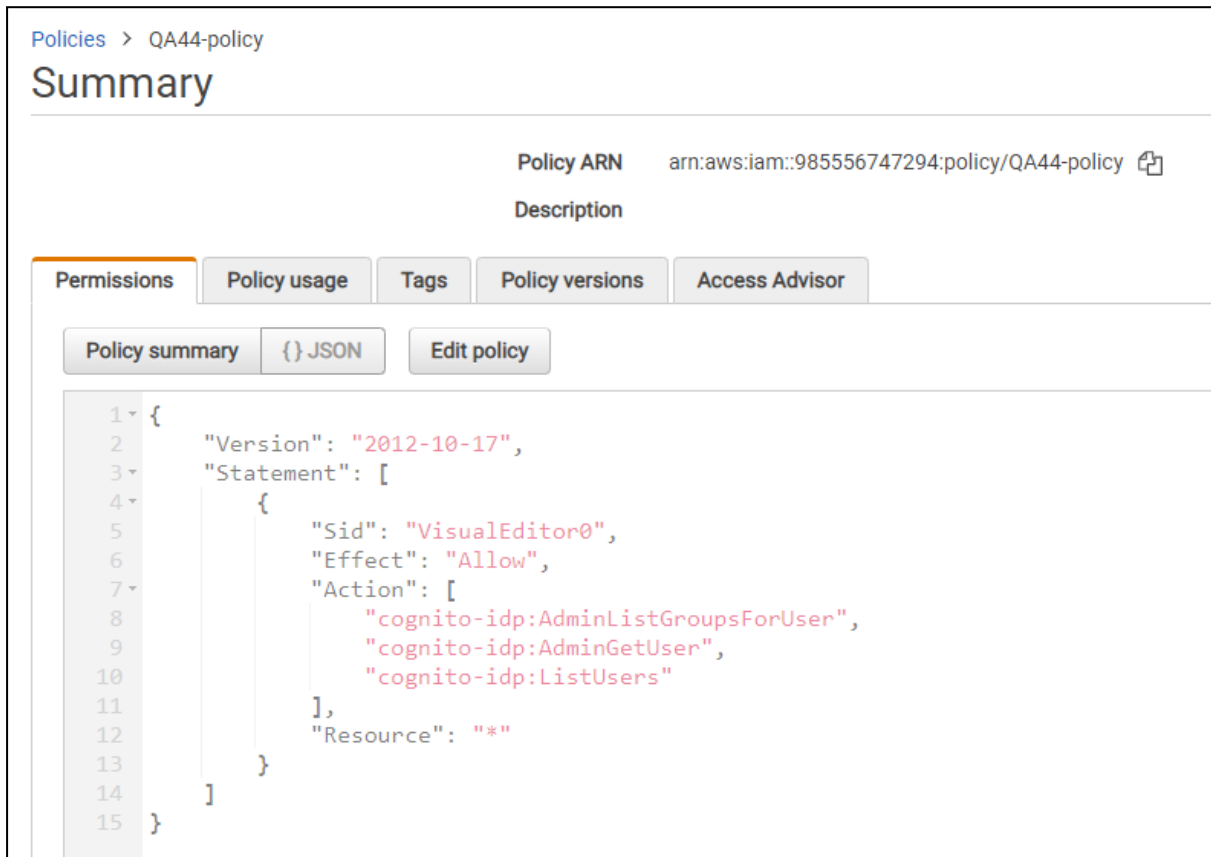
Buttons: "Cancel", "Save changes".



## Autorización (Oauth2)

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

En el servicio de Cognito User Pools de Amazon el servicio AdminListGroupsForUser, AdminGetUser y ListUsers.



Policies > QA44-policy

### Summary

Policy ARN: `arn:aws:iam::985556747294:policy/QA44-policy`

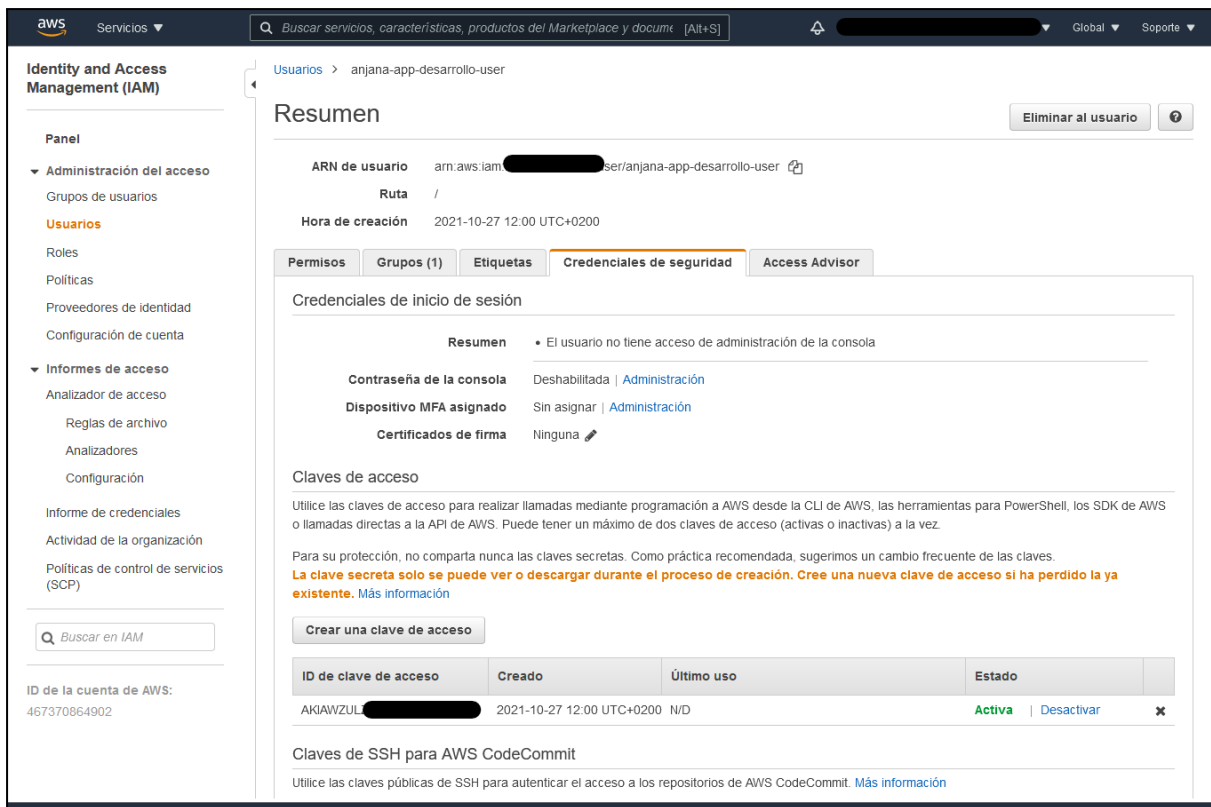
Description

Permissions | Policy usage | Tags | Policy versions | Access Advisor

Policy summary | {} JSON | Edit policy

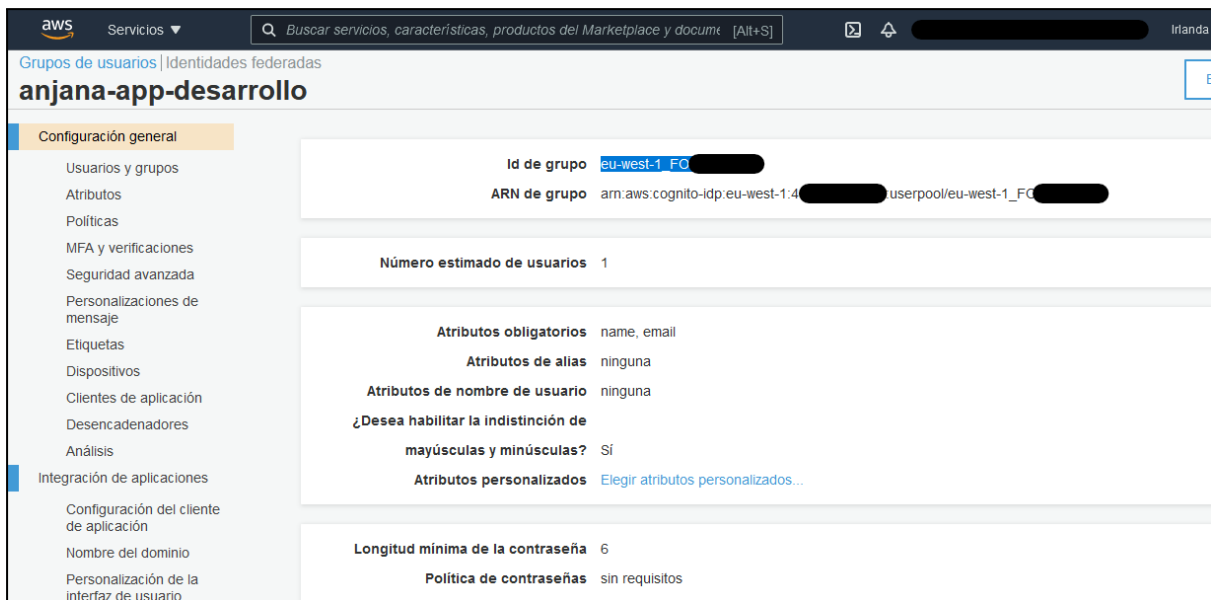
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "cognito-idp:AdminListGroupsForUser",
9         "cognito-idp:AdminGetUser",
10        "cognito-idp:ListUsers"
11      ],
12      "Resource": "*"
13    }
14  ]
15 }
```

En la configuración de Zeus configuraremos unas credenciales creadas en el apartado de “Credenciales de seguridad” de la ficha del usuario. Estos valores irán en el apartado Authorization de la configuración de Zeus



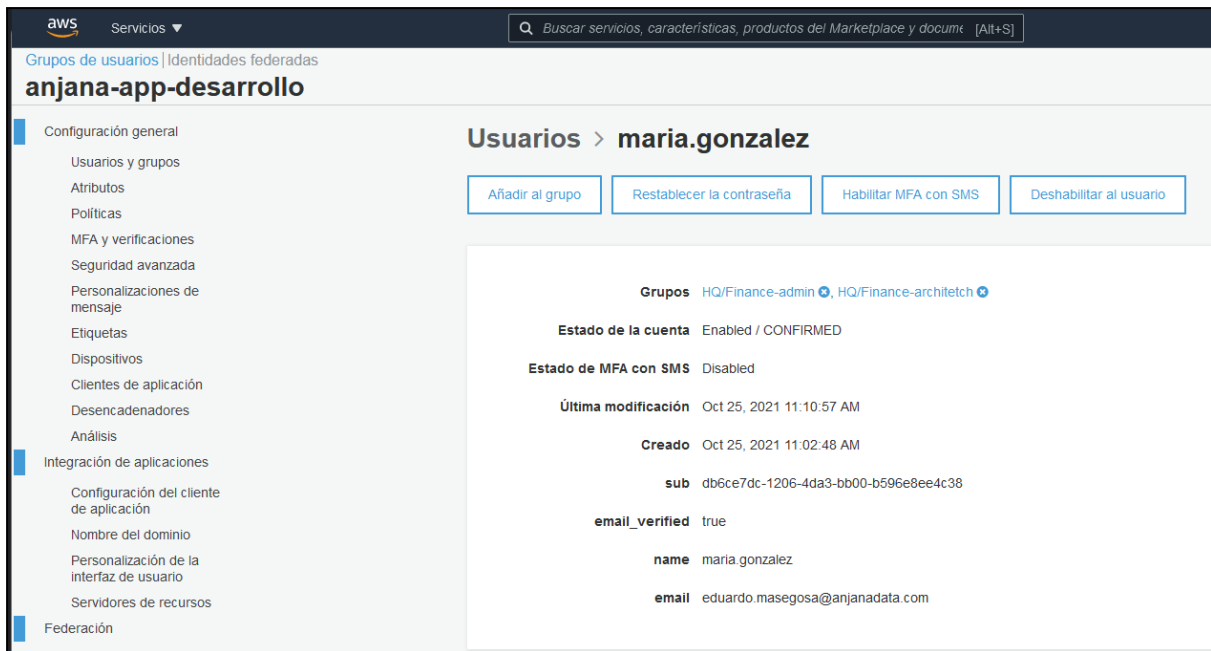
The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options for Identity and Access Management (IAM), including 'Administración del acceso', 'Usuarios', 'Roles', 'Políticas', and 'Informes de acceso'. The main content area displays the 'Resumen' (Summary) for the user 'anjana-app-desarrollo-user'. Key details include the ARN of the user, the creation time (2021-10-27 12:00 UTC+0200), and a list of security credentials. The 'Credenciales de inicio de sesión' (Login credentials) section shows that the console password is disabled, MFA is not assigned, and no certificates are present. A table below lists the access keys, with one active key shown. The 'Claves de SSH para AWS CodeCommit' section is also visible at the bottom.

El valor poolID lo podemos encontrar en el grupo de usuarios creado en Amazon Cognito.



The screenshot shows the AWS Cognito console configuration page for the user pool 'anjana-app-desarrollo'. The left sidebar lists various configuration options such as 'Configuración general', 'Usuarios y grupos', 'Atributos', and 'Integración de aplicaciones'. The main content area displays the 'Configuración general' (General configuration) for the user pool. Key details include the group ID ('eu-west-1\_FC...'), the group ARN, the estimated number of users (1), and the list of required attributes (name, email). It also shows settings for password policies, such as the minimum password length (6) and whether to require uppercase and lowercase letters (Yes).

El usuario y sus membresías deben darse en el grupo de usuarios creado en cognito.



The screenshot shows the AWS IAM console interface. At the top, there's a search bar and the text "Grupos de usuarios | Identidades federadas". Below that, the page title is "anjana-app-desarrollo". On the left, there's a navigation menu with categories like "Configuración general", "Integración de aplicaciones", and "Federación". The main content area is titled "Usuarios > maria.gonzalez" and contains several action buttons: "Añadir al grupo", "Restablecer la contraseña", "Habilitar MFA con SMS", and "Deshabilitar al usuario". Below these buttons, the user's details are displayed in a structured format:

<b>Grupos</b>	HQ/Finance-admin, HQ/Finance-architect
<b>Estado de la cuenta</b>	Enabled / CONFIRMED
<b>Estado de MFA con SMS</b>	Disabled
<b>Última modificación</b>	Oct 25, 2021 11:10:57 AM
<b>Creado</b>	Oct 25, 2021 11:02:48 AM
<b>sub</b>	db6ce7dc-1206-4da3-bb00-b596e8ee4c38
<b>email_verified</b>	true
<b>name</b>	maria.gonzalez
<b>email</b>	eduardo.masegosa@anjanadata.com

## Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre AWS es "Tot plugin AWS IAM", en su documentación queda descrita la credencial requerida.

## Emulación SSO vía Oauth2

El protocolo Oauth2 observa la autenticación transparente en caso de que sea posible, para lo cual solo es necesario redirigir al usuario a <https://<host>/anjana/login?provider=<identificador de provider en zeus>>, si el usuario ya está logado en dicho provider y las políticas configuradas en dicho provider hacen que no se requiera validar nuevamente la credencial, el usuario será autenticado en Anjana Data de forma totalmente transparente.