



## 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	5
<b>Credenciales requeridas</b>	<b>5</b>
Autenticación	5
Autorización (Oauth2)	9
Gobierno activo	11
<b>Emulación SSO vía Oauth2</b>	<b>11</b>

## Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	22/11/2023	Anjana Producto	Anjana Producto	Creación del documento. Compatibilidad con la v4.5 de todos los módulos de Anjana

# 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` se configuran los distintos proveedores de autenticación que se utilizan.

En el caso de AWS es necesario configurar las siguientes propiedades:

```
security:
  authentication:
    oidc:
      providers:
        aws:
          name: Anjana AWS
          authorize-url:
            https://${security.authentication.oidc.providers.aws.domain}.auth.${security.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.aws.redirect-uri}&state=STATE&scope=${security.authentication.oidc.providers.aws.scopes}
          authorize-url-portuno:
            https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/login?response_type=code&client_id=${security.authentication.oidc.providers.aws.client-id}&redirect_uri=${security.authentication.oidc.providers.aws.redirect-uri-portuno}&state=STATE&scope=${security.authentication.oidc.providers.aws.scopes}
          token-url:
            https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth2/token
          scopes: openid+profile
          client-id: <client-id>
          client-secret: <client-secret>
          client-authentication-method: GET
          redirect-uri: https://url.anjanadata.com/anjana/authorized
```

```

  redirect-uri-portuno:
https://url.anjanadata.com/admin/authorized
  username-claim: cognito:username
  workflowType: AUTHORIZATION_CODE
  authorizeServer:
https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth2/userInfo
  userNameProperty: username
  type: AWS
  region: eu-web-1
  domain: anjana-app-desarrollo

```

## Configuración de autorización

En la propiedad `security.authorization` se configuran los distintos proveedores de autorización que se utilizan.

En el caso de AWS es necesario configurar las siguientes propiedades:

```

security:
  authorization:
    oidc:
      providers:
        aws:
          providers:
            anjana-dev-app:
              poolID: eu-central-1_5oDfN6Jvv
              region: eu-central-1
              accessKey: <accessKey>
              secretKey: <secretKey>
              groupOrgUnitSeparator: "/"
              roleOrgUnitSeparator: "-"
              groupPrefix: "prefix-"

```

- `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<sup>1</sup>.

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.

---

<sup>1</sup> Independientemente de los separadores usados en los repositorios de identidades el producto normalizará al formato estándar, por lo que en la configuración del producto ha de usarse siempre los separadores ‘/’ y ‘-’ para conformar el alias, por ejemplo “UO/UO..../UO-role”.

A screenshot of the AWS Cognito service page. At the top, there is a navigation bar with the AWS logo, a search bar, and links for "Servicios", "Irlanda", and "Soporte". The main title "Amazon Cognito" is centered above a purple circular icon. Below the title, a descriptive text block explains the service's purpose: "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." Two blue buttons are visible: "Administrar grupos de usuarios" and "Administrar grupos de identidades", with the latter being highlighted. Below these buttons are two sections: one showing a user icon with a plus sign and the text "Añadir la funcionalidad de inscripción e inicio de sesión", and another showing a computer monitor with a lock icon and the text "Conceda acceso a sus usuarios a los servicios de AWS". Each section includes a small explanatory text at the bottom.

En el apartado “Clientes de aplicación” se obtienen las credenciales que más tarde hay que indicar en la configuración de Zeus.

aws Servicios ▼ Buscar servicios, características, productos del [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
- Cuentas 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 cuentas 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.

anjana-app-desarrollo

**ID de cuenta de aplicación**

66 [REDACTED]

**Clave secreta de cuenta de aplicación**

if8 [REDACTED]

**Actualizar el vencimiento del token**

30 días y 0 minutos

Deben estar comprendidos entre 60 minutos y 3650 días

**Vencimiento del token de acceso**

0 días y 60 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 sensitivity 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 sensitivity 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](#).

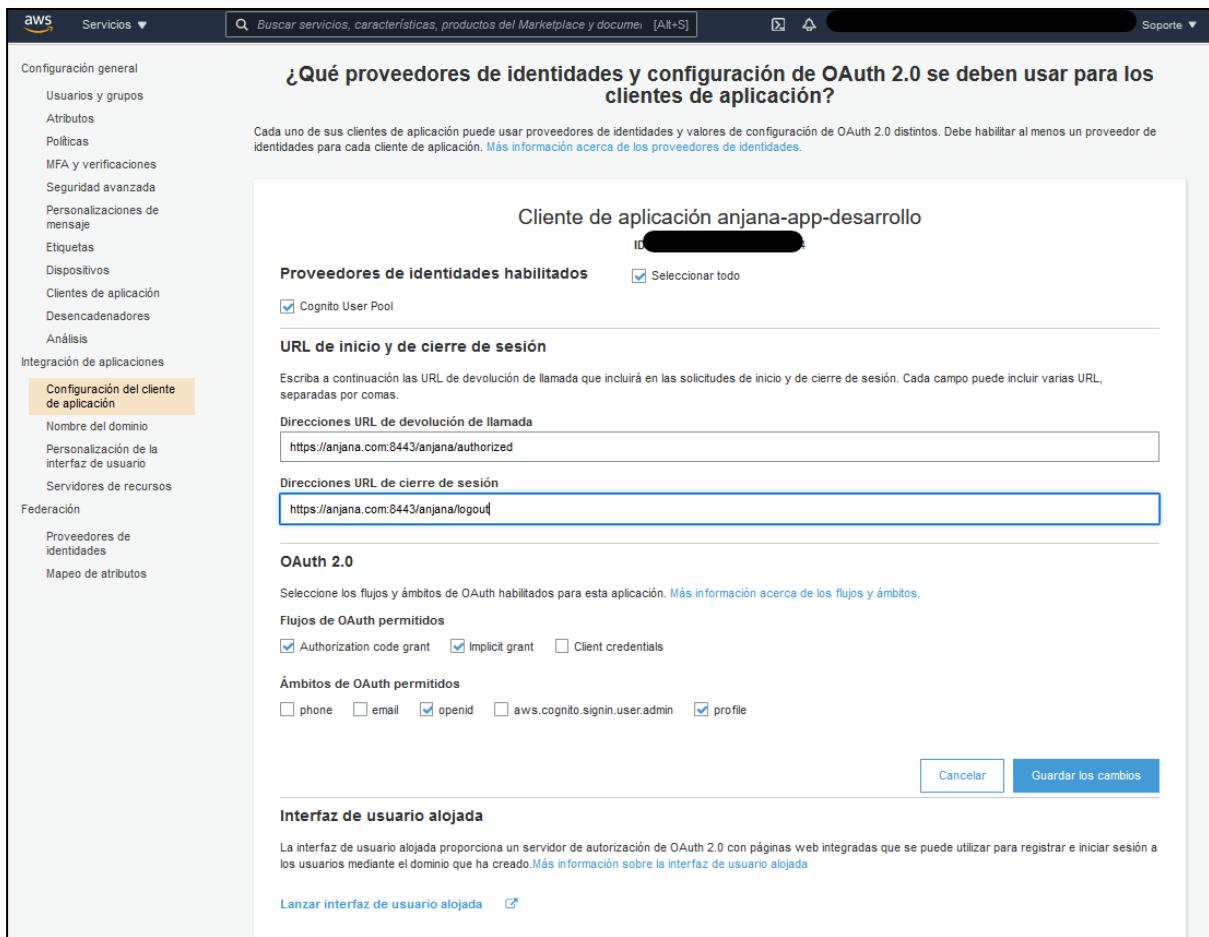
Required	Attribute	Required	Attribute
<input type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	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” se configuran las url acorde al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta:

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

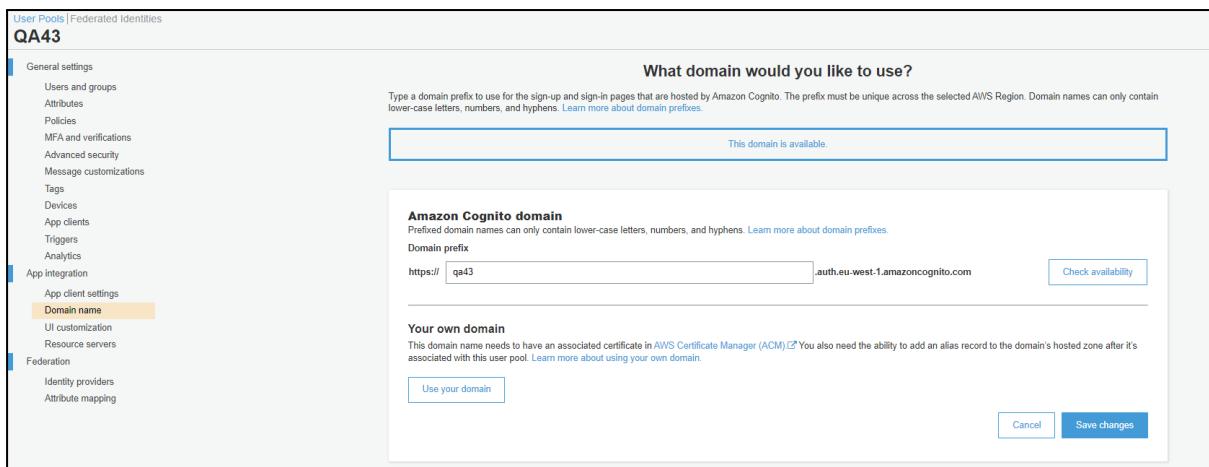


The screenshot shows the AWS Cognito User Pools configuration page for a client application named "Cliente de aplicación anjana-app-desarrollo". The left sidebar shows the navigation menu with "Configuración del cliente de aplicación" selected. The main content area is titled "¿Qué proveedores de identidades y configuración de OAuth 2.0 se deben usar para los clientes de aplicación?" and contains the following sections:

- Proveedores de identidades habilitados:** Shows "Cognito User Pool" selected. There is a checkbox for "Seleccionar todo".
- URL de inicio y de cierre de sesión:** Contains fields for "Direcciones URL de devolución de llamada" (https://anjana.com:8443/anjana/authorized) and "Direcciones URL de cierre de sesión" (https://anjana.com:8443/anjana/logout).
- OAuth 2.0:** Contains sections for "Flujos de OAuth permitidos" (Authorization code grant, Implicit grant, Client credentials selected) and "Ámbitos de OAuth permitidos" (phone, email, openid, aws.cognito.signin.user.admin, profile selected).
- Interfaz de usuario alojada:** Provides information about the hosted UI and a "Lanzar interfaz de usuario alojada" button.

At the bottom are "Cancelar" and "Guardar los cambios" buttons.

También, en el apartado de nombre del dominio se debe rellenar el nombre del pool, en minúsculas.



The screenshot shows the AWS Cognito User Pools configuration page for a domain name. The left sidebar shows the navigation menu with "Domain name" selected. The main content area is titled "What domain would you like to use?" and contains the following sections:

- Amazon Cognito domain:** A text input field with "https://qa43.auth.eu-west-1.amazoncognito.com" and a "Check availability" button.
- Your own domain:** A text input field with "https://qa43" and a "Use your domain" button.

At the bottom are "Cancel" and "Save changes" buttons.

## 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 son necesarios los siguientes permisos AdminListGroupForUser, Admin GetUser, ListUsers, listGroups y ListUsersInGroup.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "VisualEditor0",  
            "Effect": "Allow",  
            "Action": [  
                "cognito-idp>ListUsersInGroup",  
                "cognito-idp>ListGroups",  
                "cognito-idp:AdminListGroupForUser",  
                "cognito-idp:Admin GetUser",  
                "cognito-idp>ListUsers"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

En la configuración de Zeus para autorización se indican las credenciales creadas en el apartado de “Credenciales de seguridad” de la ficha del usuario.



Identity and Access Management (IAM)

Panel

Administración del acceso

Grupos de usuarios

**Usuarios**

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

Informes de acceso

Analizador de acceso

Reglas de archivo

Analizadores

Configuración

Informe de credenciales

Actividad de la organización

Políticas de control de servicios (SCP)

Buscar en IAM

ID de la cuenta de AWS:  
467370864902

Usuarios > anjana-app-desarrollo-user

## Resumen

ARN de usuario: arn:aws:iam:█████████████████████:user/anjana-app-desarrollo-user

Ruta: /

Hora de creación: 2021-10-27 12:00 UTC+0200

Permisos Grupos (1) Etiquetas Credenciales de seguridad Access Advisor

### Credenciales de inicio de sesión

Resumen: El usuario no tiene acceso de administración de la consola

Contraseña de la consola: Deshabilitada | Administración

Dispositivo MFA asignado: Sin asignar | Administración

Certificados de firma: Ninguna

### Claves de acceso

Utilice las claves de acceso para realizar llamadas mediante programación a AWS desde la CLI de AWS, las herramientas para PowerShell, los SDK de AWS o llamadas directas a la API de AWS. Puede tener un máximo de dos claves de acceso (activas o inactivas) a la vez.

Para su protección, no comparta nunca las claves secretas. Como práctica recomendada, sugerimos un cambio frecuente de las claves.

**La clave secreta solo se puede ver o descargar durante el proceso de creación. Cree una nueva clave de acceso si ha perdido la ya existente.** [Más información](#)

Crear una clave de acceso

ID de clave de acceso	Creado	Último uso	Estado
AKIAWZUL█████████████████████	2021-10-27 12:00 UTC+0200	N/D	Activa   Desactivar

### Claves de SSH para AWS CodeCommit

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

El valor poolID se puede encontrar en el grupo de usuarios creado en Amazon Cognito.

aws Servicios ▾ Buscar servicios, características, productos del Marketplace y documentación [Alt+S] Irlanda

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

**Id de grupo** eu-west-1\_FO [REDACTED]

**ARN de grupo** arn:aws:cognito-idp:eu-west-1:4[REDACTED]userpool/eu-west-1\_FO [REDACTED]

**Número estimado de usuarios** 1

**Atributos obligatorios** name, email

**Atributos de alias** ninguna

**Atributos de nombre de usuario** ninguna

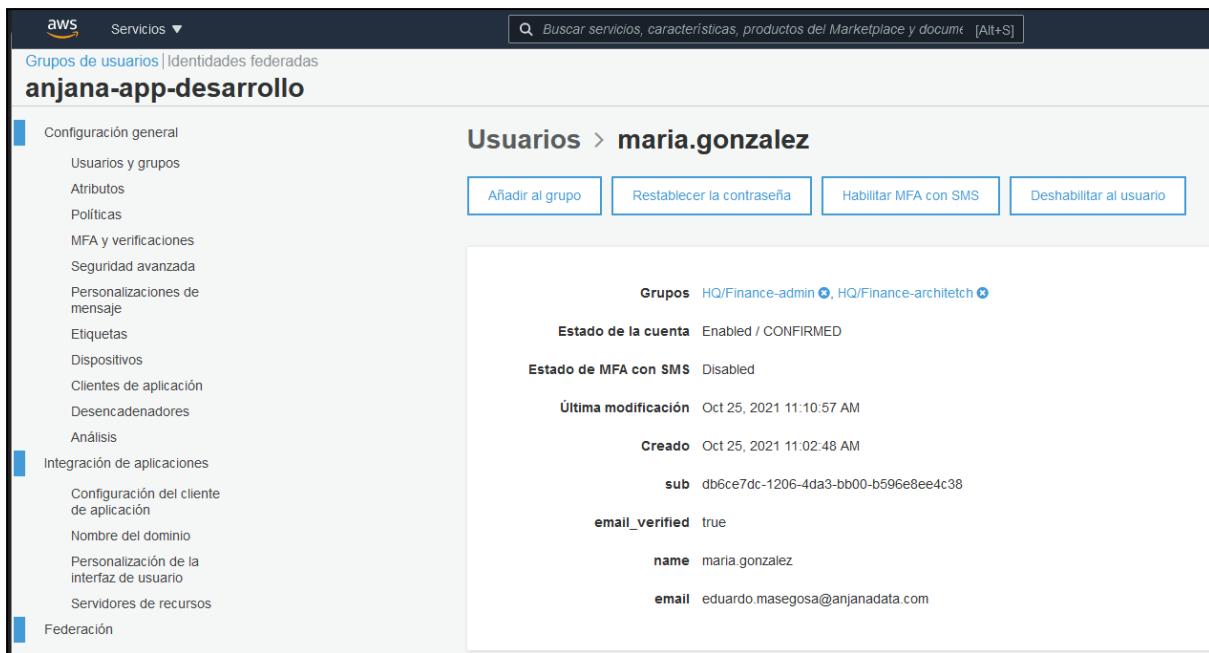
**¿Desea habilitar la indistinción de mayúsculas y minúsculas?** Si

**Atributos personalizados** Elegir atributos personalizados...

**Longitud mínima de la contraseña** 6

**Política de contraseñas** sin requisitos

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



The screenshot shows the AWS IAM User Details page for the user 'maria.gonzalez'. The left sidebar lists navigation options: 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, and Federación. The main content area displays the user's attributes:

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

At the top of the main content area, there are four buttons: 'Añadir al grupo', 'Restablecer la contraseña', 'Habilitar MFA con SMS', and 'Deshabilitar al usuario'.

## 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.