



## 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

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
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://${security.authentication.oidc.providers.aws.domain}.auth.${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=${security.authentication.oidc.providers.aws.scopes}
          token-url:
            https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth2/token
          scopes: openid+profile
          client-id: asdfasdfasdfsdfasdfasdf
          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_F0xxxxx
      region: eu-west-1
      accessKey: AAAAAAAAAAAAAAAA
      secretKey: aaaaaaaaaaaaaabbffffbbbbbcccccccccc
```

- `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.

A screenshot of the AWS Cognito service page. The top navigation bar shows the AWS logo, a search bar, and various service links. The main heading is "Amazon Cognito" with a purple hexagon icon. Below the heading is a descriptive text block: "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 are two blue buttons: "Administrar grupos de usuarios" and "Administrar grupos de identidades". The bottom section is divided into two main sections: "Añadir la funcionalidad de inscripción e inicio de sesión" (with an icon of a user profile and a plus sign) and "Conceda acceso a sus usuarios a los servicios de AWS" (with an icon of a computer monitor and a lock). Each section has a brief description and a note at the bottom.

En el apartado “Cientes de aplicación” obtendremos las credenciales que más tarde habrá 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
- 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**  
66 [REDACTED]

**Clave secreta de cliente 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 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](#).

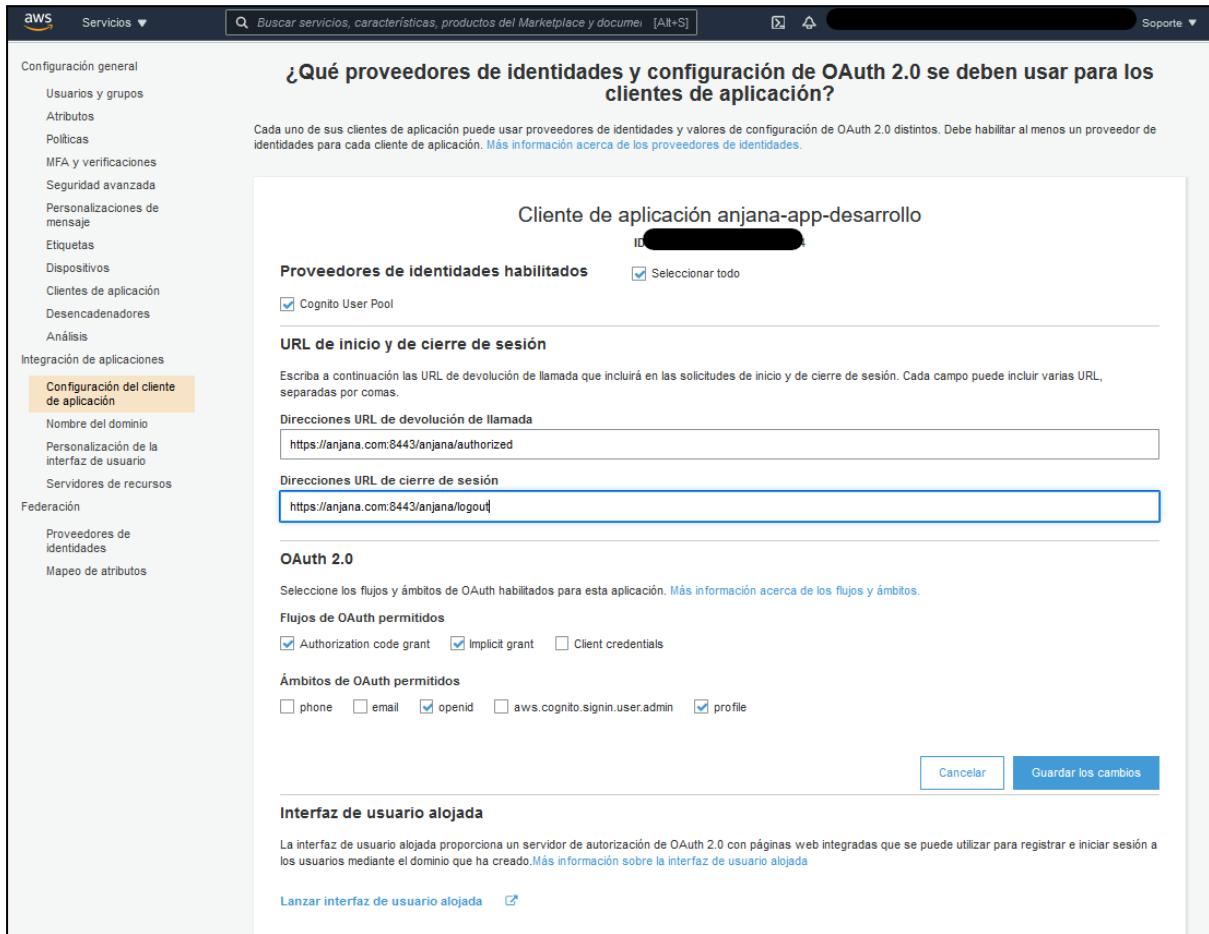
Required	Attribute	Required	Attribute
<input type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	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.

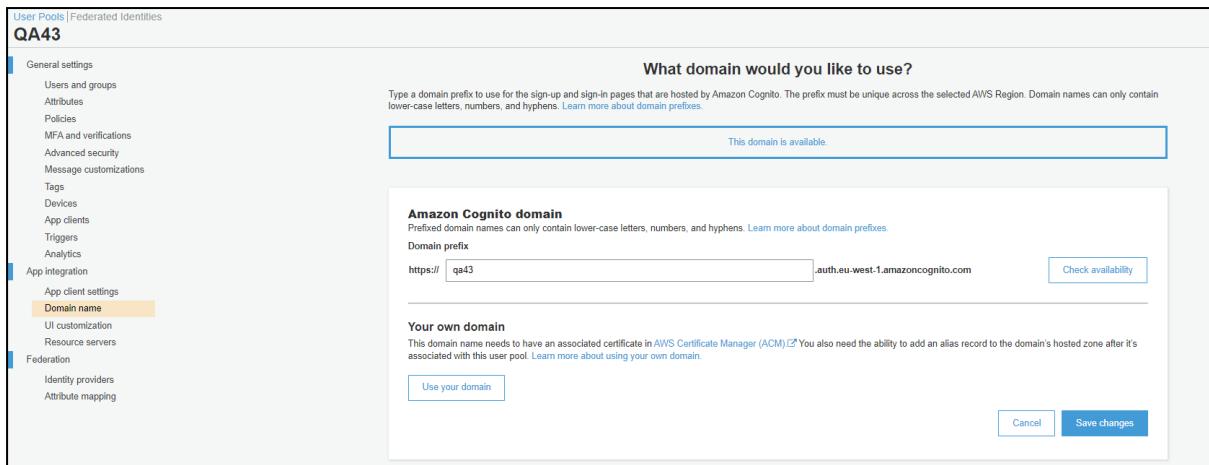
En el apartado “Configuración del cliente de aplicación” configuraremos las url acordes al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta dos, más la de log out:

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



The screenshot shows the 'Client de aplicación anjana-app-desarrollo' configuration page. The left sidebar is titled 'Configuración del cliente de aplicación' and includes options like 'Nombre del dominio', 'Personalización de la interfaz de usuario', and 'Servidores de recursos'. The main content area has a heading '¿Qué proveedores de identidades y configuración de OAuth 2.0 se deben usar para los clientes de aplicación?' and a note about enabling providers for each client. It shows 'Proveedores de identidades habilitados' (Cognito User Pool selected), 'URL de inicio y de cierre de sesión' (URLs for 'https://anjana.com:8443/anjana/authorized' and 'https://anjana.com:8443/anjana/logout'), and 'OAuth 2.0' settings (Authorization code grant, Implicit grant selected). At the bottom are 'Cancelar' and 'Guardar los cambios' buttons.

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

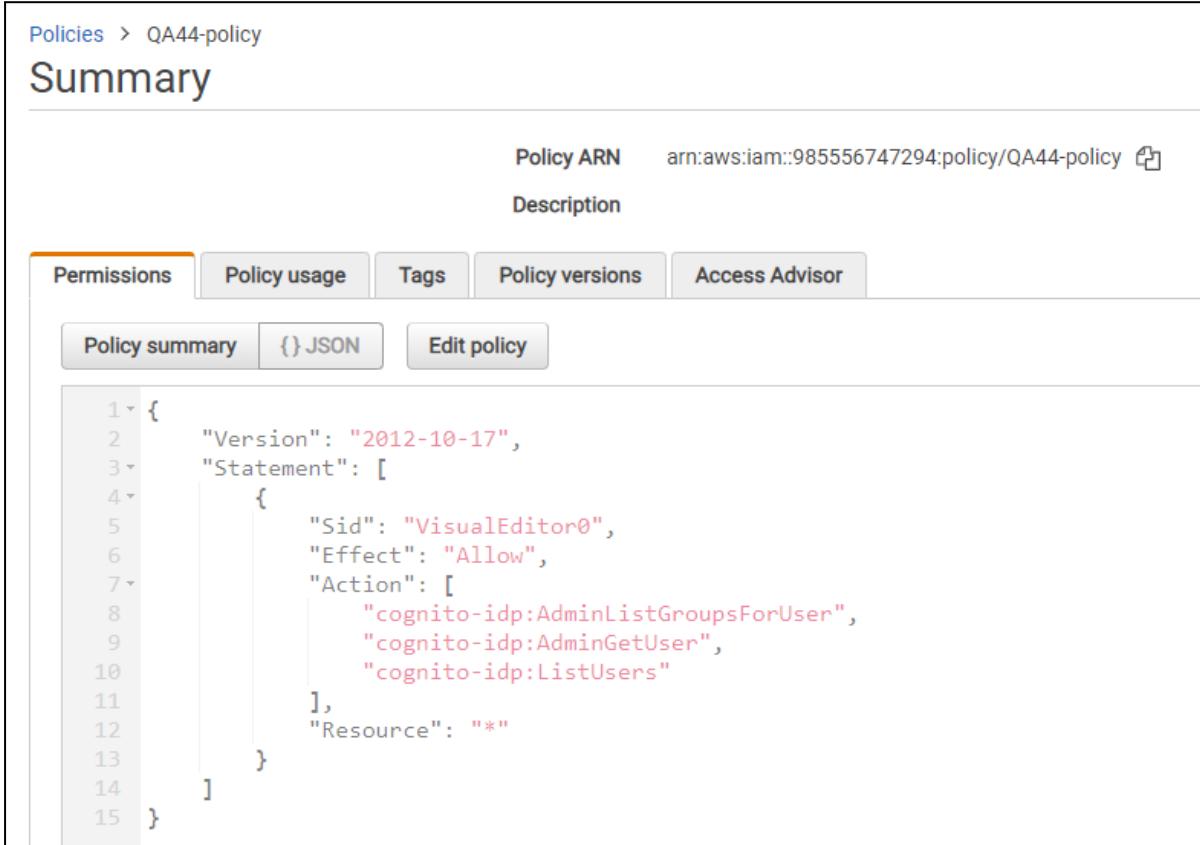


The screenshot shows the 'Domain name' configuration page for 'User Pools | Federated Identities' under 'QA43'. The left sidebar includes 'General settings' (Users and groups, Attributes, Policies, MFA and verifications, Advanced security, Message customizations, Tags, Devices, App clients, Triggers, Analytics), 'App integration' (App client settings, Domain name selected), and 'Identity providers' (Federation, Attribute mapping). The main content area asks 'What domain would you like to use?' and shows a 'Domain name is available' message for 'qa43'. It also shows the 'Amazon Cognito domain' section with the URL 'https://qa43.auth.eu-west-1.amazoncognito.com' and a 'Check availability' 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 el servicio AdminListGroupsForUser, Admin GetUser y ListUsers.



The screenshot shows the AWS IAM 'Policies > QA44-policy' page. The 'Summary' section displays the Policy ARN (arn:aws:iam::985556747294:policy/QA44-policy) and a 'Description' field. Below the summary, there are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is selected, showing a 'Policy summary' and a 'JSON' button. The JSON code is as follows:

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "VisualEditor0",
6              "Effect": "Allow",
7              "Action": [
8                  "cognito-idp:AdminListGroupsForUser",
9                  "cognito-idp:Admin GetUser",
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

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 lo podemos 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\_FG [REDACTED]

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

**Número estimado de usuarios** 1

**Atributos obligatorios** name, email

**Atributos de alias** ninguna

**Atributos de nombre de usuario** ninguna

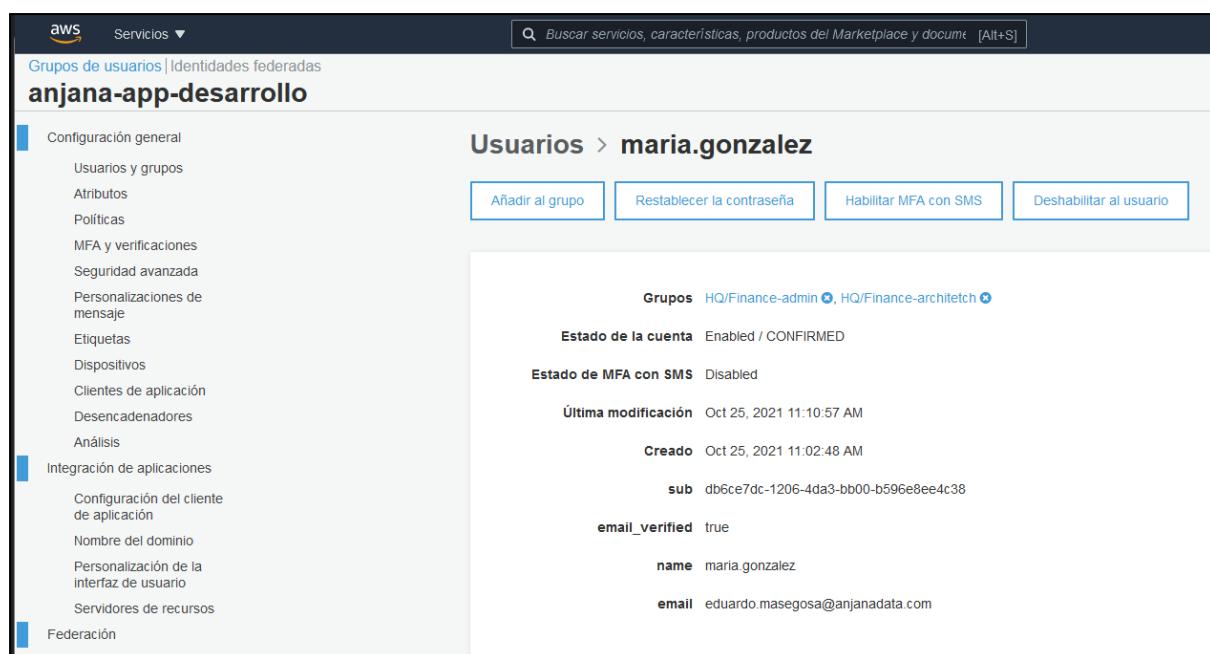
**¿Desea habilitar la indistinción de mayúsculas y minúsculas?** Sí

**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.



## 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.