Integración AWS

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://${security.authentication.oidc.providers.aws.domain}.auth.${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=${security.authentication.oidc.provid
ers.aws.scopes}
          authorize-url-portuno:
https://${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=${security.authentication.oidc.providers.aw
s.redirect-uri-portuno}&state=STATE&scope=${security.authentication.oid
c.providers.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: <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://${security.authentication.oidc.providers.aws.domain}.auth.${sec
urity.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth
2/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[1].
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.

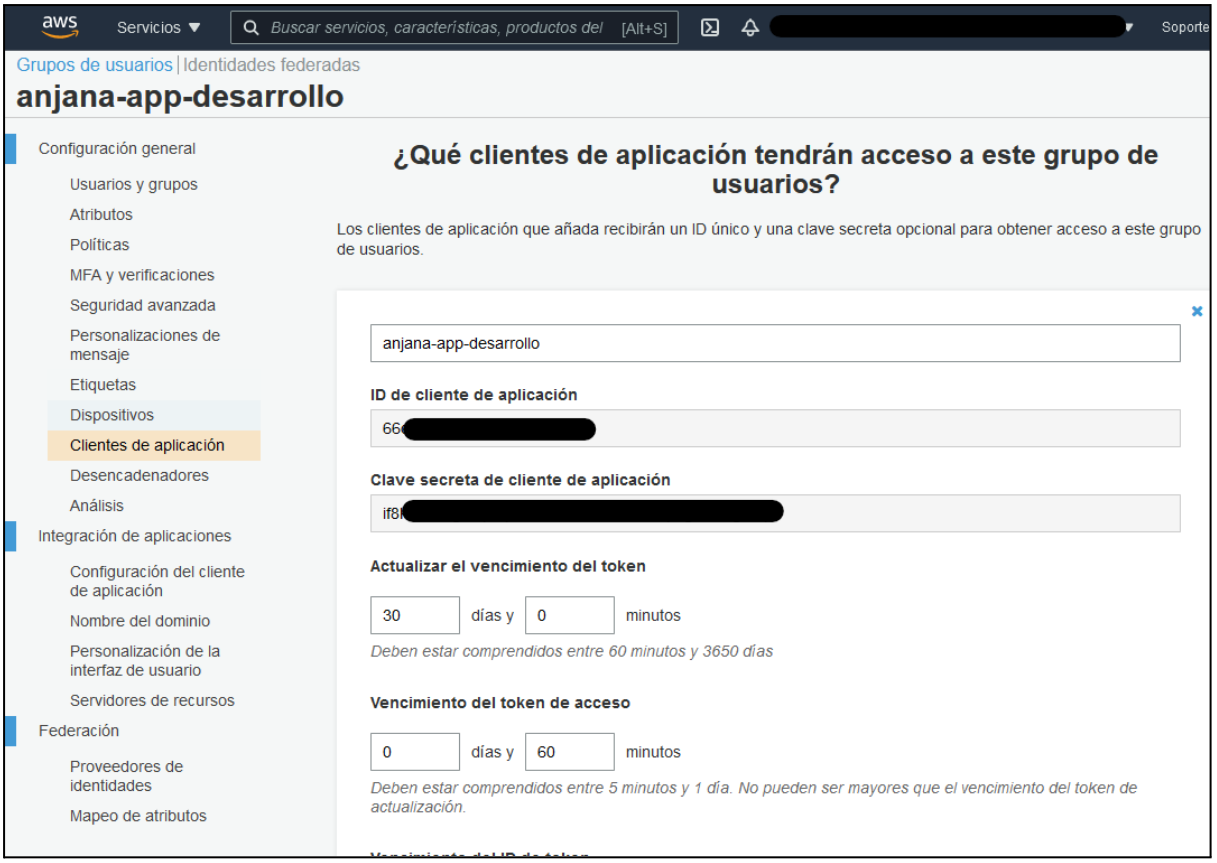
Autenticación

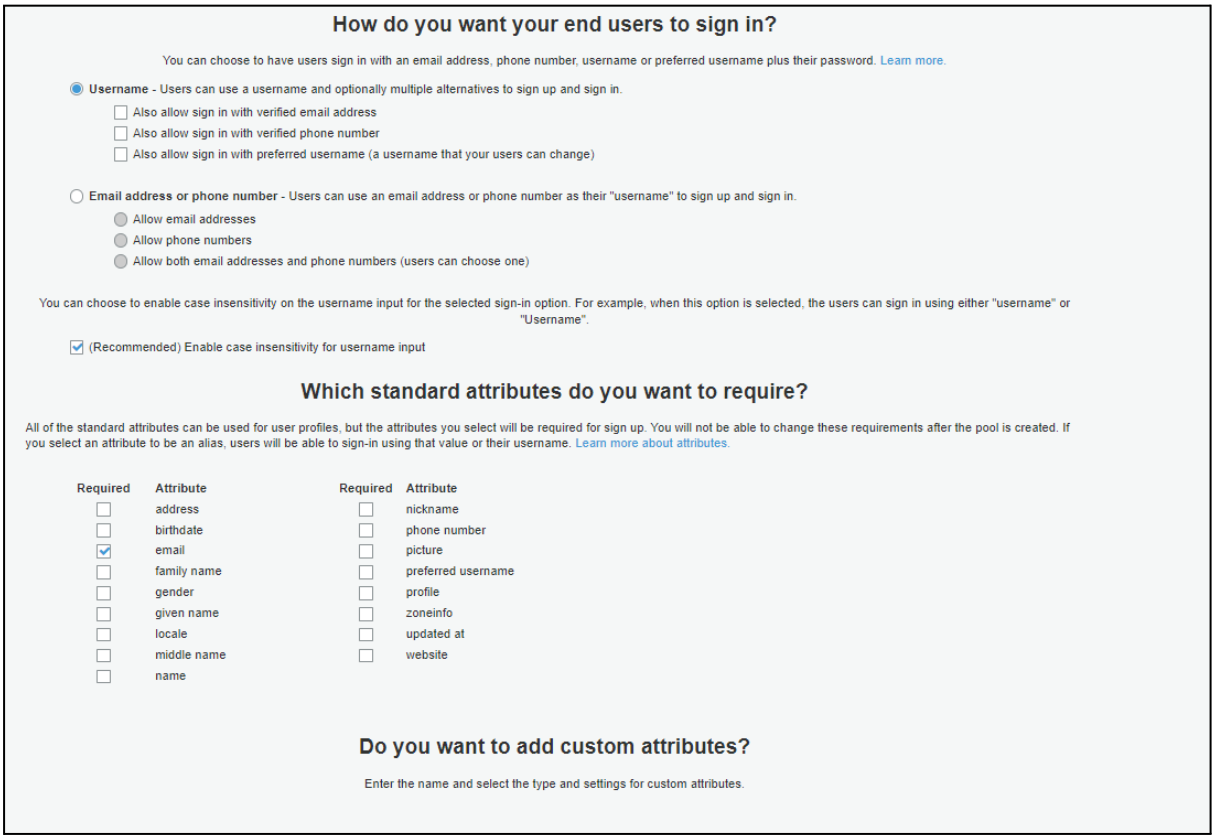
La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

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

[1] 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”.

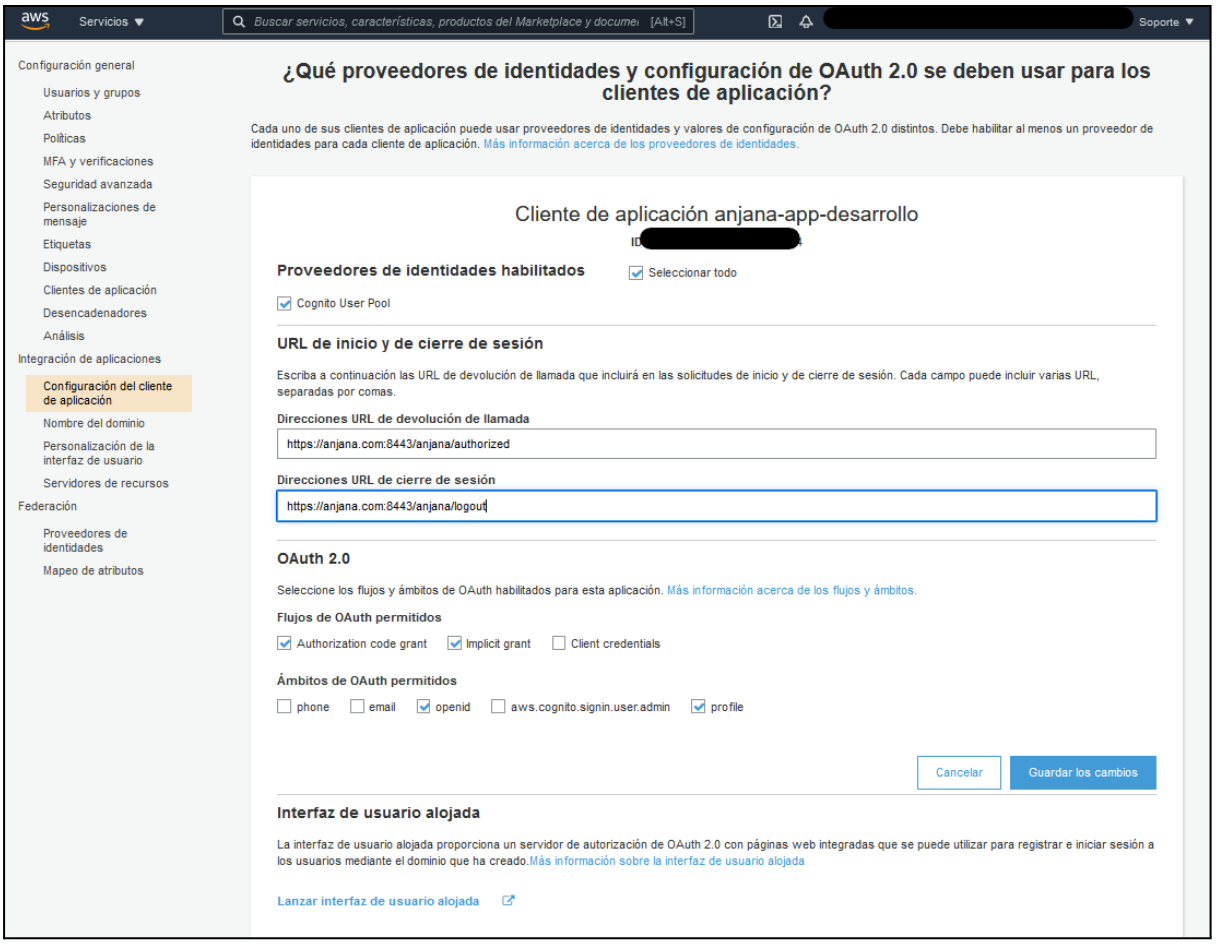
En el apartado “Clientes de aplicación” se obtienen las credenciales que más tarde hay que indicar en la configuración de Zeus.


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
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.
anjana-app-desarrollo
ID de cliente de aplicación
66
Clave secreta de cliente de aplicación
if8
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.

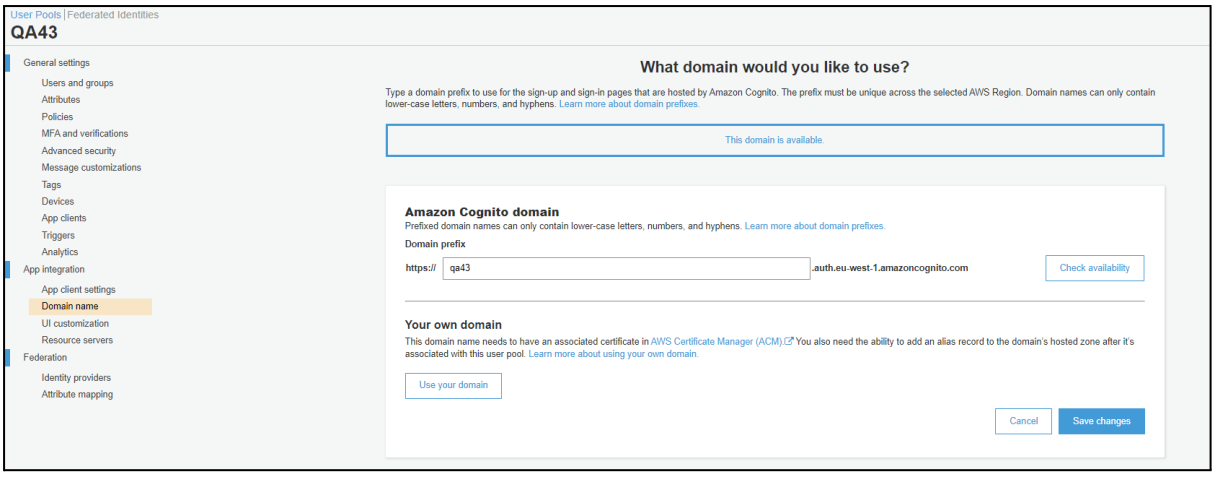

How do you want your end users to sign in?
You can choose to have users sign in with an email address, phone number, username or preferred username plus their password. Learn more.
Username - Users can use a username and optionally multiple alternatives to sign up and sign in.
Also allow sign in with 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
address
birthdate
email
family name
gender
given name
locale
middle name
name
Required
Attribute
nickname
phone number
picture
preferred username
profile
zoneinfo
updated at
website
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



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



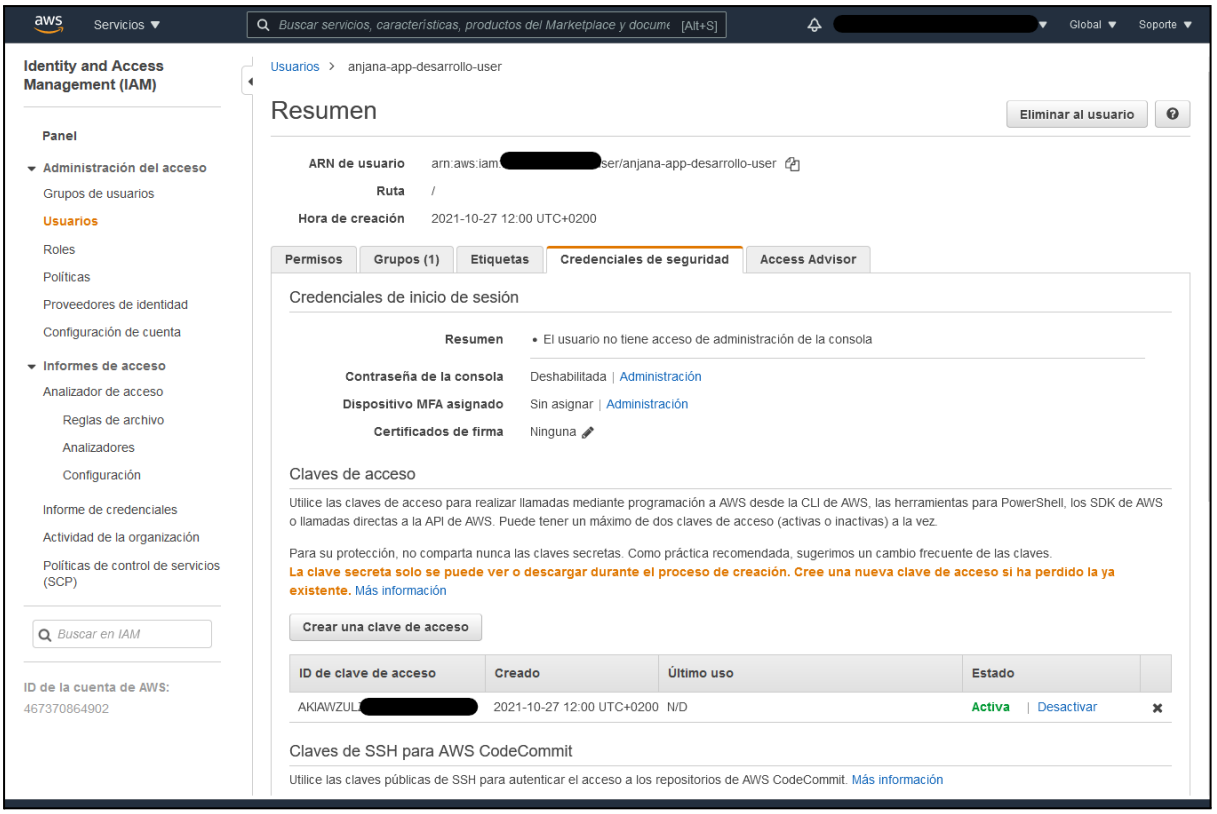
Autorización (Oauth2)

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.

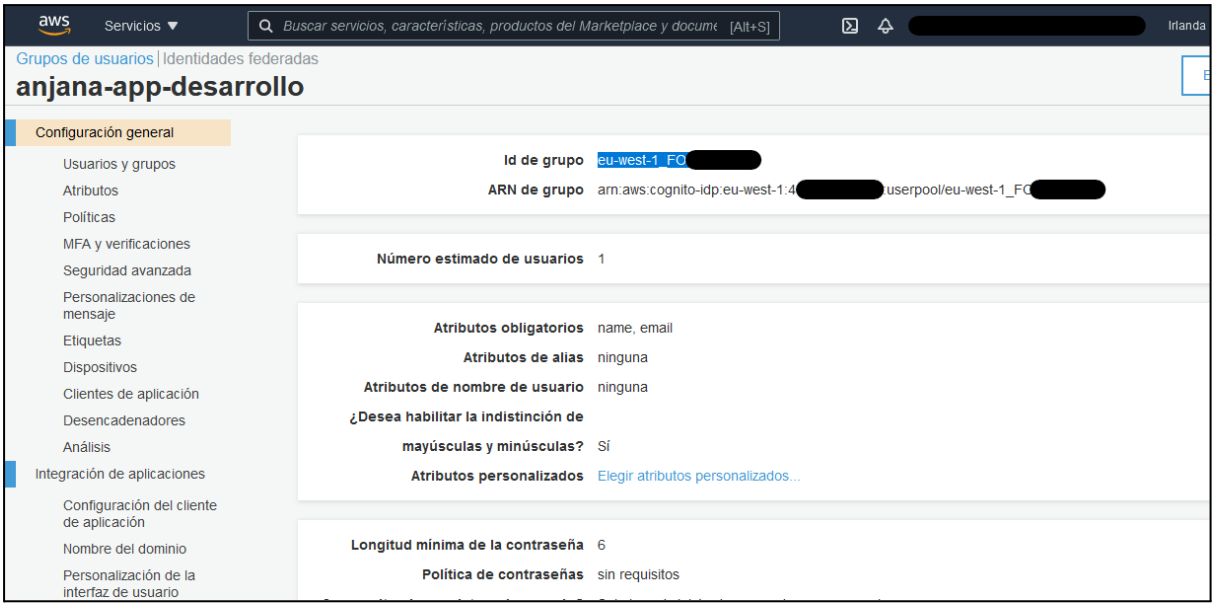
En el servicio de Cognito User Pools de Amazon son necesarios los siguientes permisos AdminListGroupsForUser, AdminGetUser, ListUsers, listGroups y ListUsersInGroup.

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

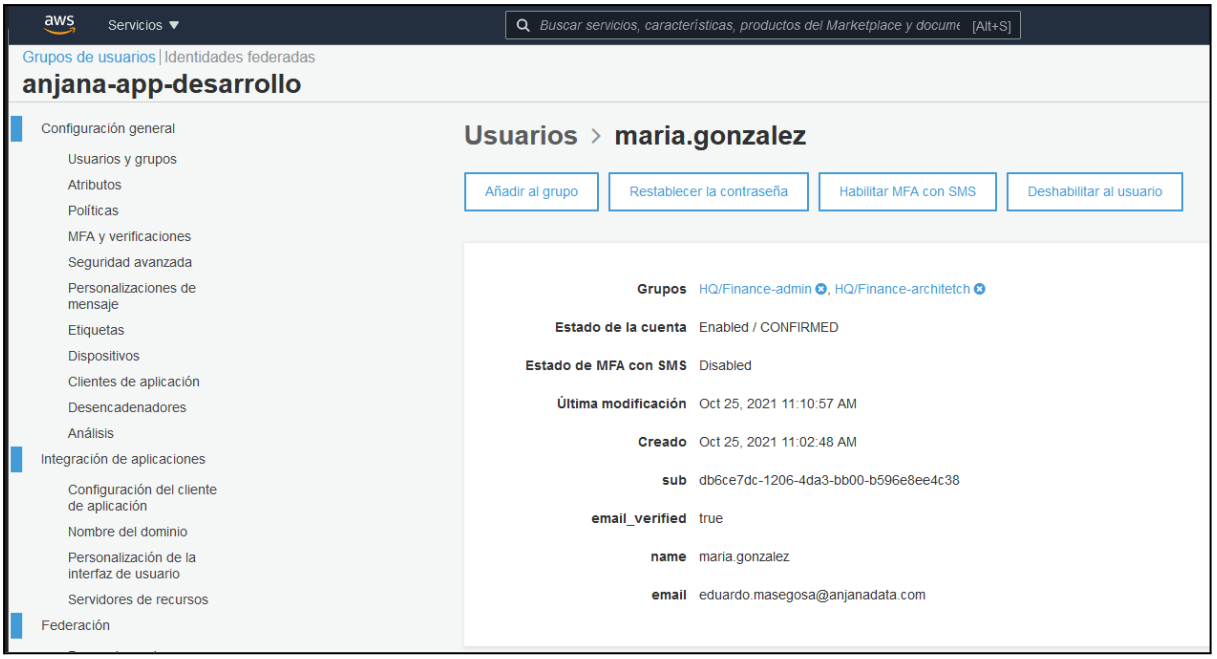
En la configuración de Zeus para autorización se indican las credenciales creadas en el apartado de “Credenciales de seguridad” de la ficha del usuario.



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



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.