.1.1.1

Idearium
Consultores

Guía

MODIFICACIÓN DE GEOSERVER PARA LA UTILIZACIÓN DE CONTROL DE ACCESOS MEDIANTE UN LDAP EXTERNO

.1.1.2

ÍNDICE

Idearium
Consultores

CONTROL DE ACCESOS EN GEOSERVER

En este documento se recogen los pasos para implementar un control de accesos en geoserver que utilice un LDAP externo para la autenticación y una base de datos para la gestión de roles. Los pasos se realizan sobre un geoserver versión 2.16 con todas sus opciones por defecto.

.2. Seguridad en geoserver

Geoserver utiliza un sistema de seguridad basado en Spring Security. De forma simplificada existen:

- Usuarios: Entidad para identificar a una persona. Cada usuario tiene asignado un conjunto de roles.
- Roles: Definen lo que un usuario puede o no puede hacer
- Reglas: Se aplican sobre espacios de trabajo o capas individuales y definen los permisos de uno o más roles sobre ese objeto.

En Geoserver la autenticación tiene dos partes:

- Filter chain: Se encarga de obtener las credenciales del usuario. Existen duna serie de mecanismos de autenticación que se ejecutan en orden y si uno falla se prueba con el siguiente.
- Provider chain: Se encarga de realizar la autenticación del usuario. Puede configurarse para que se realice sobre un documento XML, un LDAP, una base de datos o de varias formas a la vez.

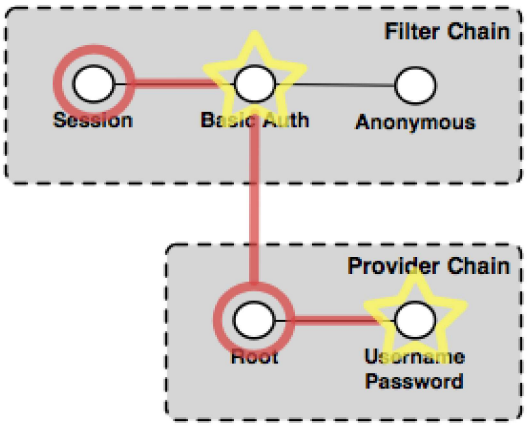

Figura 1: OWS service authentication chain

.3. Protección de una capa o espacio de trabajo

Desde la interfaz de administración de Geoserver en la pestaña previsualización de capas podemos ver todas las capas de prueba que vienen con geoserver. Estas capas son accesibles por defecto por usuarios anonimos.

Para obtener la dirección del servicio ows que se quiere proteger hay que seleccionar un formato específico.

En la pestaña seguridad de los datos se muestra el listado de todas las reglas del sistema. Si una capa está protegida y se intenta acceder a ella sin permiso se devuelve un error 404. Si se prefiere devolver un 401 hay que cambiar catalog mode a "desafio". Para crear una nueva regla sobre un espacio

de trabajo o capa hay que pulsar en “Agregar nueva capa”. Rellenar cómo se indica en la figura y pulsar a guardar.

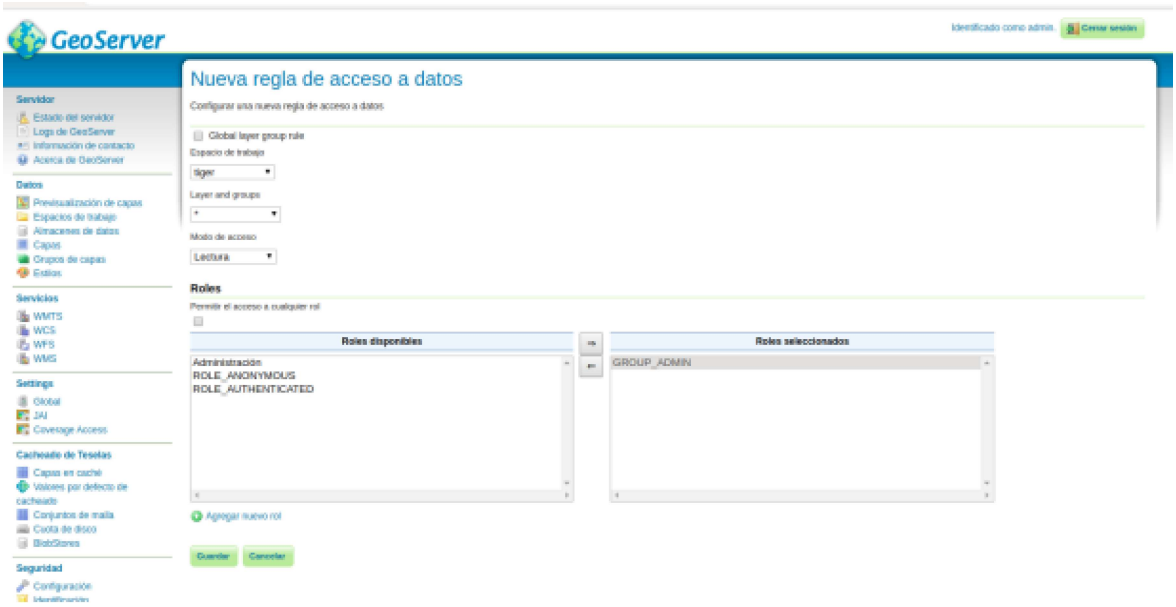

Figura 2: Crear nueva regla

En este punto, las capas del espacio de trabajo “tiger” solo son accesibles para usuarios logueados como administrador.

.4. Integración con un LDAP externo

En la pestaña “identificación” en el apartado “proveedores de identificación”, seleccionar en “Agregar nuevo” e introducir los datos de la figura. En este ejemplo se ha introducido un LDAP de prueba con algunos usuarios en donde todas las contraseñas son “password”

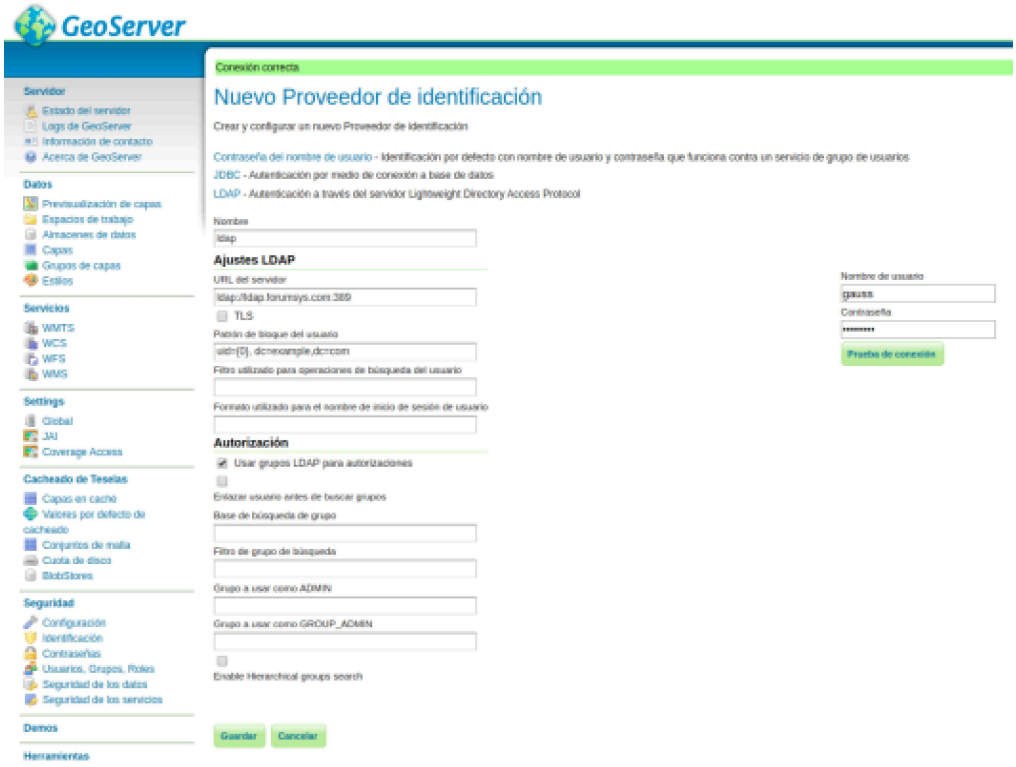

Figura 4: Nuevo proveedor LDAP

Una vez creado el proveedor hay que seleccionarlo en el apartado cadena de proveedores.

En este punto ya es posible autenticarse como un usuario del LDAP, pero no hay ningun rol asignado a esos usuarios.

.5. Asignación de roles

En la pestaña “Usuarios, Grupos, Roles” en el apartado “user group services” seleccionar “Agregar nuevo” y rellenar como aparece en la figura. En este caso se ha utilizado una base de datos postgresql local como ejemplo.

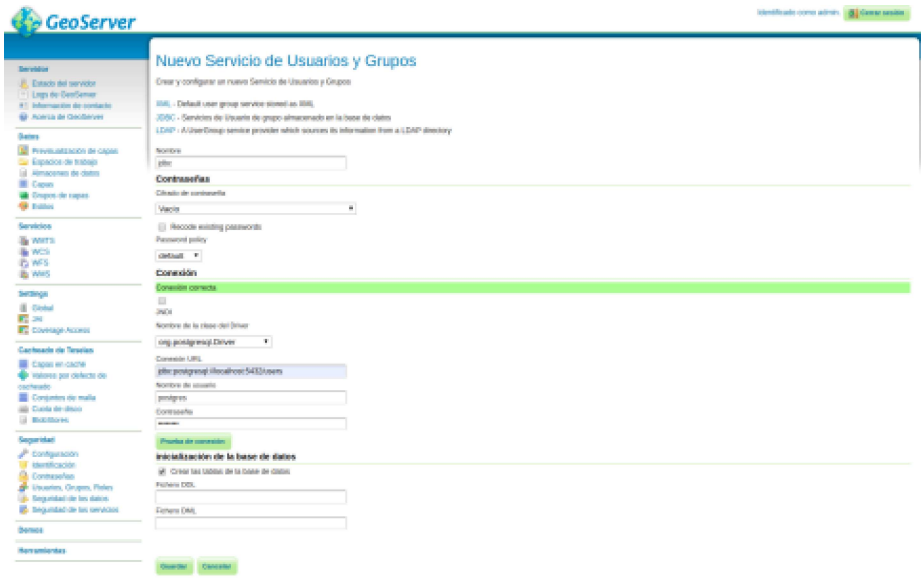

Figura 5: Nuevo User group service con jdbc

En este punto ya se ha conectado a la base de datos con los usuarios autorizados y ha creado las tablas necesarias que se muestran en la figura inferior. Para introducir los usuarios autorizados desde geoserver, hay que pulsar en el group service recién creado, pulsar en la pestaña usuarios y pulsar en "Agregar nuevo usuario". Rellenar como se indica en la figura.

```
postgres@jorge-HP:~$ psql users
psql (10.12 (Ubuntu 10.12-0ubuntu0.18.04.1))
Type "help" for help.

users=# \dt
              List of relations
 Schema |      Name       | Type  |  Owner
--------+-----------------+-------+----------
 public | group_members   | table | postgres
 public | group_roles     | table | postgres
 public | groups          | table | postgres
 public | role_props      | table | postgres
 public | roles           | table | postgres
 public | user_props      | table | postgres
 public | user_roles      | table | postgres
 public | users           | table | postgres
(8 rows)
```

Figura 6: Tablas generadas por geoserver

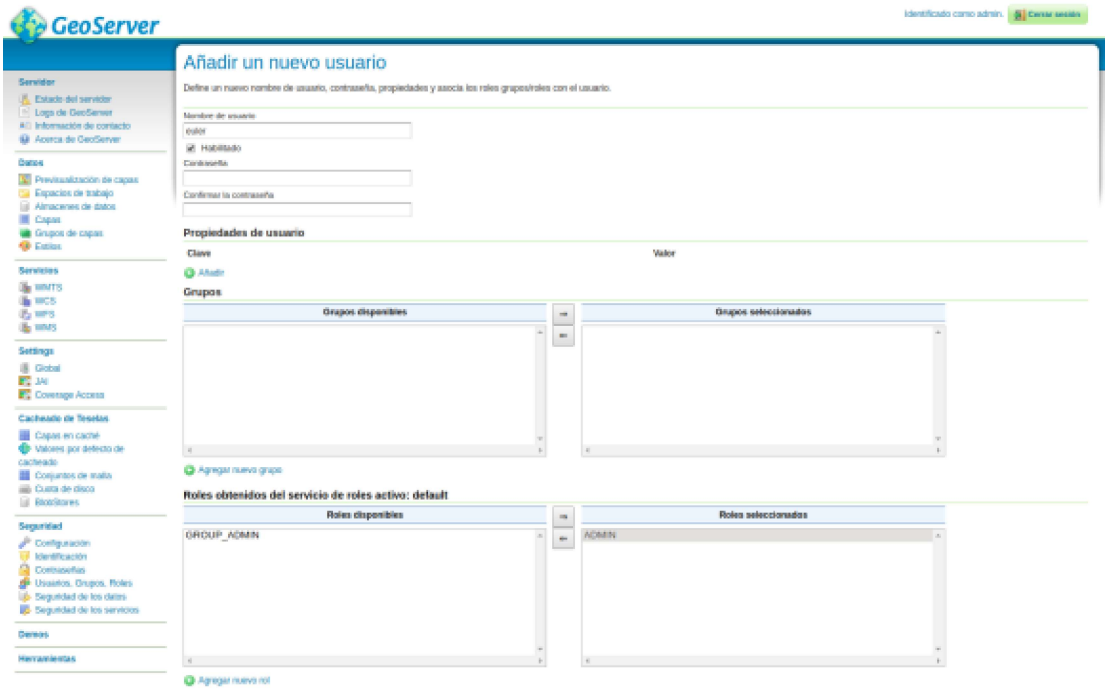

Figura 7: Nuevo usuario en el group service

Para terminar hay que pulsar de nuevo en la pestaña "identificación" se leccionar ldap creado anteriormente y modificarlo como se indica en la figura.

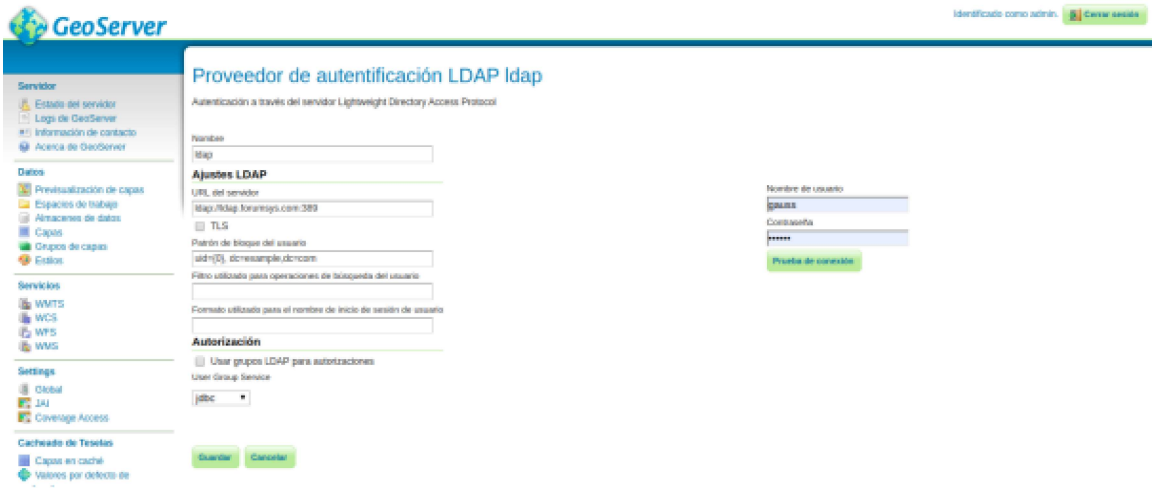

Figura 8: Autorización mediante el group service jdbc

.6. Peticiones servicios ows

Durante las pruebas se ha utilizado Postman para realizar las peticiones al servidor. Para poder mostrarlo en este documento se han exportado las peticiones realizadas a código curl.

La petición de abajo se utiliza para iniciar sesión. Si se han seguido los pasos de la giía y se introduce un usuario del ldap, debería responder con un mensaje de bienvenida y una cookie llamada JSESSIONID.

```
Curl --location --request POST 'http://localhost:8080/geoserver/j_spring_security_check' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'username=gauss' \
--data-urlencode 'password=password'
```

A modo de prueba, se ha utilizado una petición para obtener una imágen png de una de las capas protegidas. Solo con la cookie del apartado anterior, el servidor debería permitir el acceso y devolver un código 200 junto con una imágen.

```
curl --location --request POST 'http://localhost:8080/geoserver/tiger/wms?service=WMS&version=1.1.0&request=GetMap&layers=tiger%3Apoi&bbox=-74.0118315772888%2C40.70754683896324%2C-74.00153046439813%2C40.719885123828675&width=641&height=768&srs=EPSG%3A4326&format=image%2Fpng' \
--header 'Cookie: JSESSIONID=node013qodqrgvcxebkcon62fsjzu01.node0'
```