¿Qué es el análisis de token (token introspection)?

El análisis de token (Token introspection) es una extensión de OAuth 2.0 definida en RFC 7662 que permite a los clientes consultar el Servidor de autorización (Authorization server) para validar los tokens de acceso (access tokens) y recuperar metadatos sobre ellos. Esta extensión es útil cuando:

- El cliente quiere verificar la validez de un token de acceso (access token) en tiempo real.
- El token de acceso (access token) es opaco (no autónomo) y requiere que el servidor de autorización lo valide.

¿Cómo funciona el análisis de token (token introspection)?

Aquí hay un ejemplo no normativo de una solicitud de análisis de token (token introspection):

```
POST /introspect HTTP/1.1
Host: authorization-server.example.com
Content-Type: application/x-www-form-urlencoded

token=random-token-value
  &token_type_hint=access_token
```

El parámetro `token_type_hint` es opcional y debe establecerse en el tipo de token que se está analizando. Si el token de acceso (access token) es válido, el servidor de autorización responde con los metadatos del token:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "active": true,
  "scope": "read write",
```

```
  "client_id": "client-id",
  "username": "johndoe",
  "token_type": "Bearer",
  "exp": 1634020800,
  "iat": 1634017200
}
```

Vale la pena señalar que no todos los servidores de autorización (authorization servers) admiten el análisis de token (token introspection) y no todos los tokens son susceptibles de análisis. El Servidor de autorización (Authorization server) puede limitar el uso del análisis de token (token introspection) basándose en varios factores, por ejemplo, algunos servidores de autorización pueden no admitir el análisis de JWTs .

Parámetros clave en una solicitud de análisis de token (token introspection)

Estos son dos parámetros clave en una solicitud de análisis de token (token introspection):

- **`token`**: El token a analizar.
- **`token_type_hint`**: El tipo de token que se está analizando. Puede ser `access_token` o `refresh_token`.

Revisión #2
Creado 2024-11-11 17:56:32 UTC por Marluan Espiritusanto
Actualizado 2024-11-13 14:02:03 UTC por Marluan Espiritusanto