Alcance (Scope)

El alcance (scope) define los permisos que una aplicación solicita de un usuario para acceder a sus recursos protegidos. Es un concepto fundamental en OAuth 2.0 y OIDC (OpenID Connect) que controla el nivel de acceso que una aplicación puede tener a los datos de un usuario.

¿Qué es un alcance (scope)?

En los protocolos OAuth 2.0 y OpenID Connect (OIDC) , un **alcance (scope)** es un mecanismo para limitar el acceso que una aplicación tiene a los recursos de un usuario. Define los permisos que la aplicación está solicitando del usuario.

Los alcances se representan como cadenas de texto que son definidas por el servidor de autorización (authorization server). Cuando una aplicación solicita acceso a los recursos de un usuario, especifica los alcances que necesita en la solicitud de autorización (authorization request). Luego se le pide al usuario que otorgue o niegue estos permisos durante el proceso de autorización.

¿Por qué usar alcances?

- **Control de acceso (access control) granular**: Los alcances permiten a las aplicaciones solicitar solo los permisos que necesitan para realizar acciones específicas, reduciendo el riesgo de acceso no autorizado.
- **Consentimiento del usuario**: Los alcances ayudan a los usuarios a entender qué datos la aplicación accederá y por qué.
- **Seguridad**: Los alcances ayudan a prevenir que las aplicaciones sobrepasen sus permisos de acceso, mejorando la seguridad de los datos del usuario.

¿Cómo funciona el alcance (scope)?

Cuando una aplicación inicia el proceso de autorización (authorization) de OAuth 2.0 / OIDC, incluye una lista de alcances en la solicitud de autorización (authorization request). El servidor de autorización (authorization server) presenta al usuario una pantalla de consentimiento que lista los alcances solicitados. El usuario puede elegir otorgar o negar acceso a cada alcance. Este proceso se utiliza típicamente cuando la aplicación es una aplicación de terceros que requiere acceso a los recursos del usuario.

Alternativamente, si la aplicación es de confianza para el servidor de autorización (authorization server), es posible que no se le pida al usuario el consentimiento, sino que se realice un consentimiento automático y se otorguen todos los alcances solicitados.

Definición de alcances

Los alcances son típicamente definidos por el proveedor de API. Pueden ser:

- **Alcances estándar**: Alcances comúnmente utilizados definidos por la especificación de OAuth 2.0, compartidos por diferentes aplicaciones y servicios. Por ejemplo `openid`, `profile`, `email`.
- **Alcances personalizados**: Específicos para una aplicación o servicio, adaptados a sus requisitos únicos. Por ejemplo `read:orders`, `write:comments`.

¿Dónde se pueden utilizar los alcances en OIDC y gestión de identidades?

Los alcances pueden utilizarse en varios aspectos de OIDC, incluyendo pero no limitándose a:

- **Autenticación (Authentication)**: Los alcances pueden utilizarse para solicitar información específica del usuario durante el proceso de autenticación (authentication). Por ejemplo `profile`, `email`.
- **Autorización (Authorization)**: Los alcances pueden utilizarse para solicitar acceso a recursos específicos o realizar acciones específicas. Por ejemplo `read:orders`, `write:comments`.
- **Consentimiento**: Los alcances se presentan al usuario durante la pantalla de consentimiento para informarles de los permisos solicitados por la aplicación.
- **Emisión de tokens**: Los alcances se incluyen en la respuesta del token para indicar los permisos otorgados a la aplicación.
- **Validación de tokens**: Los alcances pueden utilizarse para validar los derechos de acceso de la aplicación cuando presenta el token para acceder a recursos protegidos.
- **Servidor de recursos (Resource server)**: Los alcances pueden ser utilizados por el servidor de recursos para aplicar políticas de control de acceso (access control) basadas en los permisos otorgados a la aplicación.
- **Perfil del usuario**: Los alcances pueden utilizarse para solicitar información adicional del perfil del usuario más allá de los claims básicos.

Mejores prácticas

- **Solicitar alcances mínimos**: Siempre solicita el conjunto mínimo de alcances necesario para el funcionamiento de tu aplicación. Esto minimiza el riesgo de sobre-permiso y mejora la confianza del usuario.
- **Explicar el uso de alcances**: Explica claramente a los usuarios por qué se necesita cada alcance. La transparencia ayuda a obtener el consentimiento del usuario.
- **Utilizar alcances estándar cuando sea posible**: Aprovecha los alcances estándar para asegurar la compatibilidad y reducir la complejidad.