Autorización (Authorization)

La autorización es el proceso de determinar qué acciones puede realizar una identidad en un recurso. Es un mecanismo de seguridad fundamental para definir y hacer cumplir políticas de acceso.

¿Qué es la autorización (Authorization)?

> **TL;DR**: La autorización (Authorization) responde a la pregunta “¿Qué puedes hacer?”

La autorización (Authorization) es un proceso de toma de decisiones que determina si una identidad (usuario, servicio o dispositivo) tiene los permisos necesarios para realizar una acción específica en un recurso. Veamos algunos ejemplos:

- En un editor de documentos en línea, un usuario puede compartir un documento con otros.
- En un servicio de almacenamiento en la nube, un servicio puede leer y escribir archivos en una carpeta específica.
- En un sistema de hogar inteligente, un dispositivo puede encender las luces en la sala de estar.

Todos estos ejemplos implican una identidad (sujeto) realizando una acción en un recurso. Por supuesto, la autorización (Authorization) también puede fallar, como cuando un usuario intenta eliminar un archivo al que no tiene permiso para acceder.

El modelo básico para la autorización (Authorization) es simple: Si **identidad** realiza **acción** en **recurso**, entonces **aceptar** o **denegar**.

Diferencia entre autenticación (Authentication) y autorización (Authorization)

La autenticación (authentication) y la autorización (Authorization) a menudo se confunden, pero son fundamentalmente diferentes: Autenticación (Authentication) responde a la pregunta “¿Qué identidad posees?”. Además, en la mayoría de los casos, la autorización (Authorization) ocurre después de la autenticación (authentication) porque el sistema necesita conocer la identidad antes

de tomar decisiones de acceso.

Diferencia entre autorización (Authorization) y control de acceso (Access control)

La autorización (Authorization) es un subconjunto del control de acceso (Access control). El control de acceso es el concepto más amplio que incluye la autorización (Authorization) y otras restricciones en la gestión de acceso. En otras palabras, el control de acceso (Access control) es un término general que describe la restricción selectiva del acceso a los recursos, mientras que la autorización (Authorization) se refiere específicamente al proceso de toma de decisiones.

¿Cómo funciona la autorización (Authorization)?

La autorización (Authorization) normalmente se implementa utilizando Modelos de control de acceso (Access control) . Estos definen cómo se asignan y aplican los permisos en un sistema.

Marcos de trabajo (protocolos) de autorización (Authorization)

Mientras que OAuth 2.0 es un marco muy popular para la autorización (Authorization), vale la pena mencionar que OAuth 2.0 no define qué modelo de control de acceso (Access control) usar. En su lugar, se enfoca en la delegación de la autorización (Authorization) y la emisión de tokens de acceso (access tokens).

Dicho esto, OAuth 2.0 es adecuado para escenarios de autorización de terceros donde un usuario otorga permiso a un cliente para acceder a sus recursos. Por ejemplo, cuando inicias sesión en un sitio web usando tu cuenta de Google, estás autorizando al sitio web para que acceda a tu perfil de Google.

Si estás tratando con autorización de primera parte (por ejemplo, dentro de tu aplicación u organización), es posible que necesites implementar un modelo de control de acceso (Access control) como Control de acceso basado en roles (Role-based access control, RBAC) o Control de

acceso basado en atributos (Attribute-based access control, ABAC) . La combinación de OpenID Connect (OIDC) y modelos de control de acceso (Access control) puede proporcionar una base sólida tanto para la autenticación (authentication) como para la autorización (Authorization).

En lugar de construir un sistema de autorización (Authorization) propio, se recomienda utilizar un Proveedor de identidad (Identity provider, IdP) que ofrezca capacidades de autenticación (authentication) y autorización (Authorization). Un buen proveedor de identidad (identity provider) manejará la complejidad del control de acceso (Access control) y proporcionará una solución segura y escalable para tus aplicaciones.