



Curso Symphony 4 - Clase 4

¿Qué es una API Rest?

Antes de introducir el concepto de Rest API o API Rest, es necesario explicar qué es una API (Interfaz de programación de aplicaciones). Es un conjunto de peticiones que permite la comunicación de datos entre aplicaciones.

Para eso, la API utiliza peticiones HTTP que son responsables de las operaciones básicas necesarias para la manipulación de datos.

Las principales solicitudes son:

- POST: crea datos en el servidor;
- GET: lectura de datos en el host;
- DELETE: borra la información;
- PUT: registro de actualizaciones.

(Estos son los métodos HTTP más utilizados en las API Rest)

Rest, que es la abreviación de Representational State Transfer, es un conjunto de restricciones que se utilizan para que **las solicitudes HTTP cumplan con las directrices definidas en la arquitectura.**

Básicamente, las restricciones determinadas por la arquitectura Rest son:

- **Cliente-servidor:** las aplicaciones existentes en el servidor y el cliente deben estar separadas.
- **Sin estado:** las requisiciones se realizan de forma independiente, es decir, cada una ejecuta sólo una determinada acción.
- **Caché:** la API debe utilizar la caché para evitar llamadas recurrentes al servidor.
- **Interfaz uniforme:** agrupa otros cuatro conceptos en los que se determina que los recursos deben ser identificados, la manipulación de los recursos debe ser a través de la representación, con mensajes autodescriptivos y utilizando enlaces para navegar por la aplicación.

Luego, cuando se habla de Rest API, significa utilizar una API para acceder a aplicaciones back-end, de manera que **esa comunicación se realice con los estándares definidos por el estilo de arquitectura Rest.**

Las api Rest suelen programarse o diseñarse indiferentemente del front-end. Lo que quiere decir que se toma como un sistema aparte o único. En algunos casos suele verse que el front y el back (La api en este caso) están en la misma estructura de código. Esta solución no es la mejor pero dado algunos requerimientos específicos puede llegar a utilizarse.

Operaciones de ABM:

Las operaciones de ABM o Alta - Baja - Modificación, son las operaciones más comunes que podemos encontrar en una API Rest, son utilizadas para mantener un crud común entre todos los objetos o entidades del sistema o proyecto.

JWT:

JWT (JSON Web Token) es un estándar que está dentro del documento RFC 7519.

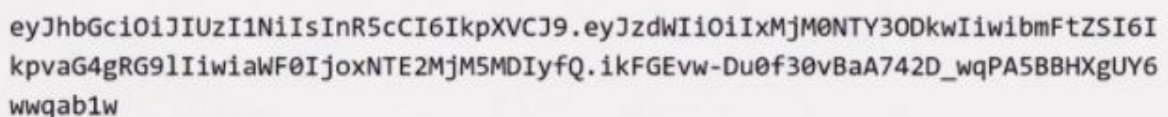
En el mismo se define un mecanismo para poder propagar entre dos partes, y de forma segura, la identidad de un determinado usuario, además con una serie de claims o privilegios.

Estos privilegios están codificados en objetos de tipo JSON, que se incrustan dentro de del payload o cuerpo de un mensaje que va firmado digitalmente.

Token JWT:

En la práctica, se trata de una cadena de texto que tiene tres partes codificadas en Base64, cada una de ellas separadas por un punto, como la que vemos en la imagen siguiente:

- **Encabezamiento**
- **Carga útil**
- **Firma**



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.ikFGEvw-Du0f30vBaA742D_wqPA5BBHXgUY6wwqab1w
```

¿Cuándo debería utilizar JSON Web Tokens?

A continuación, se muestran algunos escenarios en los que los tokens web JSON son útiles:

- **Autorización** : este es el escenario más común para usar JWT. Una vez que el usuario haya iniciado sesión, cada solicitud incluirá el JWT, lo que permitirá

al usuario acceder a rutas, servicios y recursos que están permitidos con ese token. El inicio de sesión único es una función que utiliza ampliamente JWT en la actualidad, debido a su pequeña sobrecarga y su capacidad para usarse fácilmente en diferentes dominios.

- **Intercambio de información** : los tokens web JSON son una buena forma de transmitir información de forma segura entre las partes. Debido a que los JWT se pueden firmar, por ejemplo, utilizando pares de claves públicas / privadas, puede estar seguro de que los remitentes son quienes dicen ser. Además, como la firma se calcula utilizando el encabezado y la carga útil, también puede verificar que el contenido no haya sido manipulado.

En Symfony contamos con varias librerías para manejar el uso de JWT por lo que el desarrollo será más sencillo.

