20/09/2018

Nodejs REST API

JWT (JSON Web Token)

Atención:

La instalación de esta versión requerirá cambios en los requests a la API.

JSON Web Token provee un método sencillo de intercambio de requests con la API una vez efectuado el Log In.

La implementación es un “middleware” que se procesa en cada request.

Mecanismo:

1. El cliente envía un log in (usuario/password) en el “body” de un POST.
2. El server recibe, valida y genera un JWT utilizando un “payload” y la clave “secreta”. Este token será válido por un determinado tiempo, expresado en segundos.
3. El server envía el token al cliente.
4. Para todo request el cliente debe enviar el token recibido en el header de dicho request con key “x-access-token” y value <token>.
5. El server recibe el request, verifica la presencia y validez del JWT y decodifica el “payload”.
6. En caso de ser inválido, el server retorna un código de error (-6002 / -6003).
7. Si es exitoso el middleware inserta el “payload” decodificado en el request y continúa el procesamiento del mismo(next()).

Implementación:

Deberá instalarse los packages:

npm install jsonwebtoken --save

npm install bcrypt --save

Se ha agregado el endpoint http://<miserver>/login para el verbo POST.

El mismo espera un JSON

{

“usuario”: <string>

“pass”: <string>

}

El endpoint valida el contenido contra un arreglos de objetos (usuarios, línea 33) y si el par usuario/password es válido genera un JWT con payload = usuarioId y clave secreta JWTSecret (línea 30), devolviendo al cliente el jwt en el dataset.

Los request sucesivos a cualquier endpoint serán procesados por el “middleware” (rest_token.js). De ser correcto, insertará el valor del payload (usuarioId) en el request y continuará la ejecución de acuerdo a lo programado en cada endpoint.

En este ejemplo se puede ver como, a partir de la validación y del encriptado del payload, puede obtenerse el valor de usuarioId sin necesidad de acceder a la DB.

Mensajes:

Se agregan los siguientes códigos de retorno:

Código	Texto
-6001	Usuario/Password inválido
-6002	Debe proveerse un token
-6003	Token inválido