Rest API with nodeJs

1. What is a restful API
2. C’est quoi un rest api

Un REST API (ou RESTful API) est un type d'API (Application Programming Interface) qui suit les principes et les contraintes de l'architecture REST (Representational State Transfer).

L'architecture REST est une approche standardisée pour la conception de systèmes distribués et de services web qui permettent aux clients de communiquer avec des serveurs via des requêtes HTTP (Hypertext Transfer Protocol) en utilisant des méthodes standardisées telles que GET, POST, PUT, DELETE, etc.

Un REST API permet donc aux clients de communiquer avec un serveur web en utilisant des requêtes HTTP, en envoyant et en recevant des données dans un format standardisé tel que JSON ou XML. Les ressources sont identifiées par des URI (Uniform Resource Identifiers) et manipulées via les méthodes standardisées.

Les API RESTful sont largement utilisées pour fournir des services web tels que des interfaces de programmation pour les applications mobiles, les sites web, les services cloud, etc. Ils offrent une interface simple, cohérente et facile à utiliser pour les développeurs de clients et de serveurs.

1. Les contraintes d’un rest api

Un RESTful API (Application Programming Interface) est un ensemble de contraintes qui définissent les normes pour la création de services web. Les contraintes qui s'appliquent à un RESTful API sont les suivantes :

1. Architecture client-serveur : Les clients et les serveurs sont des entités distinctes qui communiquent via une interface uniforme.
2. Stateless : Le serveur ne conserve pas l'état de la session client entre les requêtes. Chaque requête doit contenir toutes les informations nécessaires pour être traitée.
3. Interface uniforme : Les ressources sont identifiées par des URI (Uniform Resource Identifiers) et manipulées via un ensemble d'opérations standard (GET, POST, PUT, DELETE, etc.).
4. Système de mise en cache : Les réponses doivent être marquées comme cacheables ou non-cacheables pour éviter les requêtes inutiles.
5. Couche de présentation : Les données retournées par le serveur doivent être dans un format standard (JSON, XML, etc.) afin de pouvoir être facilement interprétées par les clients.
6. Code à la demande (optionnel) : Le serveur peut transmettre du code exécutable au client pour étendre ses fonctionnalités.

En respectant ces contraintes, un RESTful API peut offrir une interface simple, cohérente et facile à utiliser pour les développeurs de clients et de serveurs.

1. difference entre rest et restful api

La différence entre REST et RESTful API est souvent une source de confusion, car les termes sont souvent utilisés de manière interchangeable. Cependant, voici une explication de la différence entre les deux :

* REST (Representational State Transfer) est un style architectural qui définit un ensemble de contraintes pour la conception de systèmes distribués, tels que les services web. Il s'agit d'une approche standardisée pour la conception de systèmes distribués qui permet aux clients de communiquer avec des serveurs via des requêtes HTTP en utilisant des méthodes standardisées telles que GET, POST, PUT, DELETE, etc.
* RESTful API, quant à lui, est un terme utilisé pour décrire une API (Application Programming Interface) qui suit les principes et les contraintes de l'architecture REST. Une API RESTful fournit donc une interface web qui permet aux clients de communiquer avec un serveur web en utilisant des requêtes HTTP et en utilisant des ressources identifiées par des URI (Uniform Resource Identifiers) et manipulées via des méthodes standardisées.

En résumé, REST est une architecture de conception de systèmes distribués, tandis qu'une API RESTful est une implémentation d'une interface web qui suit les principes de cette architecture.

Une image contenant texte, Visage humain, personne, capture d’écran

Description générée automatiquement

1. Planting and first steps

Une image contenant texte, Visage humain, capture d’écran, homme

Description générée automatiquement

For this project we have /products to have a product resource it support get request to get a list of product we have ,post request to add new products

/prodect/{id} individual product by id get ,patch to change it and update it ,delete that product

Etc ………….

We will add authenfication to make sure that sume of these routes of these endpoints are protected so that only logged in users can acees them

1. Adding more routes

**You can see branch 2**

**We will use express.router**

**express.Router()** et **app.use()** sont deux fonctions clés d'Express.js qui permettent de définir des routes et de gérer les middlewares dans une application.

**express.Router()** permet de créer des instances de routeurs qui peuvent être utilisées pour définir des routes de manière modulaire. Les routeurs peuvent être montés dans une application principale ou utilisés comme des applications autonomes. Les routeurs peuvent également avoir leurs propres middlewares, qui seront exécutés avant ou après les middlewares définis dans l'application principale.

Par exemple, si vous avez un ensemble de routes qui gèrent les produits dans votre application, vous pouvez les encapsuler dans un routeur et les monter dans votre application principale en utilisant la méthode **app.use()** :

const express = require('express');

const app = express();

// Créer un routeur pour les routes relatives aux produits

const productsRouter = express.Router();

productsRouter.get('/', (req, res) => {

  // Logique pour la page d'accueil des produits

});

productsRouter.get('/:id', (req, res) => {

  // Logique pour afficher un produit spécifique

});

// Monter le routeur dans l'application principale

app.use('/products', productsRouter);

Dans cet exemple, nous créons un routeur **productsRouter** qui gère les routes relatives aux produits. Nous définissons deux routes pour afficher la page d'accueil des produits et un produit spécifique. Enfin, nous utilisons **app.use()** pour monter le routeur dans l'application principale en spécifiant le chemin de base **/products**. Toutes les routes définies dans le routeur seront préfixées avec **/products**.

1. Handling Errors & improving the project setup
2. **Project setup** 
   1. Nodemon

We will install nodemon **npm i --save-dev nodemon**

Nodemon est un outil de développement pour les applications Node.js qui surveille les modifications des fichiers du projet et redémarre automatiquement l'application à chaque fois qu'un changement est détecté.

"scripts": {

    "start": "nodemon server",

    "test": "echo \"Error: no test specified\" && exit 1"

  },

* 1. Morgan

**npm i morgan**

Lorsque vous utilisez Morgan dans votre application, il enregistre automatiquement des informations sur chaque requête HTTP entrante, telles que l'adresse IP de l'utilisateur, la méthode HTTP utilisée (GET, POST, etc.), l'URL demandée, le code de statut HTTP de la réponse, le temps de réponse, etc. Ces informations sont ensuite écrites dans la console, dans un fichier de journal ou envoyées à un service de journalisation tiers.

Ensuite, vous pouvez utiliser la fonction **morgan()** pour ajouter le middleware à votre application. Voici un exemple de code pour enregistrer les informations de journalisation dans la console :

const app = express();

app.use(morgan('dev'));

app.get('/', (req, res) => {

  res.send('Hello World!');

});

app.listen(3000, () => {

  console.log('Server started on port 3000');

});

Dans cet exemple, nous ajoutons le middleware Morgan à notre application Express en utilisant **app.use()**. Nous passons le format **'dev'** à **morgan()** pour spécifier le format de journalisation à utiliser. Le format **'dev'** est un format de journalisation prédéfini qui enregistre des informations de base sur chaque requête HTTP entrante dans la console.

Lorsque nous accédons à l'URL **http://localhost:3000/** dans notre navigateur, les informations de journalisation de la requête HTTP sont automatiquement enregistrées dans la console :

Une image contenant texte, capture d’écran, Police, affichage

Description générée automatiquement

1. Handling Errors

app.use((req, res, next) => {

  const error = new Error("Not found");

  error.status = 404;

  next(error);

});

app.use((error, req, res, next) => {

  res.status(error.status || 500);

  res.json({

    error: {

      message: error.message,

    },

  });

});

With this setup errors thrown from anywhere else in this application ,this shouldn’t really be able to happen yet but later if we add a db for example when we have operations doing work on the db these operations could fail and we then want to return a 500 error ,now if these operation fail they will directly throw an error so we don’t make it into the first middleware but since they throw an erroe the second middlware would triggered and it would handle or get this error

1. Parsing the body & handling the cors
2. Parsing the body with (body-parser)

**body-parser** est un middleware populaire pour Node.js qui permet de traiter les données envoyées dans une requête HTTP POST ou PUT et de les rendre disponibles sous forme d'objet JavaScript facilement exploitable.

Lorsqu'un client envoie des données à un serveur Node.js via une requête HTTP POST ou PUT, les données sont envoyées dans le corps de la requête HTTP. Cependant, le corps de la requête n'est pas automatiquement analysé et transformé en un objet JavaScript exploitable. C'est là que **body-parser** entre en jeu.

**body-parser** analyse le corps de la requête HTTP et le transforme en un objet JavaScript qui peut être utilisé dans le code de l'application. Cela facilite grandement le traitement des données envoyées par les clients et simplifie la gestion des requêtes HTTP.

Voici un exemple de code pour utiliser **body-parser** dans une application Express.js :

const express = require('express');

const bodyParser = require('body-parser');

const app = express();

app.use(bodyParser.urlencoded({ extended: false }));

app.use(bodyParser.json());

app.post('/submit', (req, res) => {

  const name = req.body.name;

  const email = req.body.email;

  res.send(`Merci pour votre envoi, ${name} (${email})`);

});

app.listen(3000, () => {

  console.log('Server started on port 3000');

});

Dans cet exemple, nous utilisons **body-parser** pour analyser les données envoyées dans le corps d'une requête HTTP POST envoyée à l'URL **/submit**. Nous utilisons **app.use()** pour ajouter les middleware **bodyParser.urlencoded()** et **bodyParser.json()** à notre application Express. **bodyParser.urlencoded()** analyse les données envoyées en tant que paramètres de requête HTML et **bodyParser.json()** analyse les données envoyées en tant que JSON.

Nous pouvons ensuite accéder aux données envoyées dans la requête HTTP POST via **req.body**. Dans cet exemple, nous utilisons **req.body.name** et **req.body.email** pour accéder aux valeurs envoyées dans les champs de formulaire HTML. Enfin, nous renvoyons une réponse HTTP avec un message de remerciement qui utilise les valeurs envoyées par le client.

1. Fixing cors errors

Une image contenant texte, capture d’écran

Description générée automatiquement

Une erreur de CORS (Cross-Origin Resource Sharing) se produit lorsqu'une requête HTTP émanant d'un navigateur web tente d'accéder à une ressource située sur un autre domaine que celui qui a émis la requête.

Les navigateurs web imposent une politique de sécurité Same-Origin, qui interdit à une page web d'accéder à des ressources sur un autre domaine que celui à partir duquel elle a été chargée. Cette politique est mise en place pour empêcher les attaques par injection de code malveillant et autres formes de piratage.

Cependant, il peut y avoir des cas où une application web doit accéder à des ressources situées sur un autre domaine, par exemple lorsque l'application web doit récupérer des données depuis une API distante. C'est là qu'intervient CORS.

CORS est un mécanisme qui permet aux serveurs web de spécifier les domaines à partir desquels les requêtes HTTP sont autorisées à accéder à leurs ressources. Pour permettre une requête HTTP à traverser les limites de domaine, le serveur doit ajouter les entêtes appropriés dans la réponse HTTP. Ces entêtes permettent au navigateur de savoir si la ressource demandée peut être accédée ou non.

Si le serveur ne fournit pas les en-têtes appropriés, le navigateur empêchera l'accès à la ressource et générera une erreur de CORS. Cette erreur peut être visible dans la console du navigateur ou renvoyée au client sous forme de message d'erreur.

Pour résoudre une erreur de CORS, le serveur doit envoyer les entêtes CORS appropriés dans la réponse HTTP. Cela peut inclure l'ajout de l'en-tête **Access-Control-Allow-Origin** pour spécifier les domaines autorisés à accéder à la ressource, ou l'utilisation de middleware dans le cas d'une application Node.js, comme **cors** ou en configurant manuellement les en-têtes nécessaires.

Haut du formulaire

Pour résoudre une erreur de CORS dans une application Node.js, il est nécessaire d'ajouter les en-têtes CORS appropriés dans les réponses HTTP. Il existe plusieurs façons de le faire, mais voici deux méthodes couramment utilisées :

**Méthode 1 : Utiliser le module cors**

Le module **cors** est un middleware pour Express.js qui permet de gérer les requêtes CORS. Voici un exemple d'utilisation :

const express = require('express');

const cors = require('cors');

const app = express();

app.use(cors());

// définir les routes de l'application ici

Cette utilisation simple de **cors** autorisera toutes les requêtes provenant de n'importe quel domaine à accéder aux ressources de votre application. Vous pouvez également spécifier des options pour restreindre l'accès à certaines origines en utilisant la méthode **cors(options)**. Voir la documentation du module **cors** pour plus de détails.

### Méthode 2 : Ajouter manuellement les en-têtes CORS

Si vous ne voulez pas utiliser de middleware, vous pouvez également ajouter manuellement les en-têtes CORS dans votre application Express.js en utilisant un middleware personnalisé. Voici un exemple de middleware qui ajoute les en-têtes CORS nécessaires pour autoriser les requêtes de tous les domaines :

app.use((req, res, next) => {

  res.setHeader('Access-Control-Allow-Origin', '\*');

  res.setHeader('Access-Control-Allow-Methods', 'GET, POST, PUT, DELETE');

  res.setHeader('Access-Control-Allow-Headers', 'Content-Type, Authorization');

  next();

});

Ce middleware ajoute les en-têtes CORS suivants :

* **Access-Control-Allow-Origin** : Autorise les requêtes de tous les domaines en utilisant l'astérisque **\***. Vous pouvez spécifier des domaines spécifiques si vous le souhaitez.
* **Access-Control-Allow-Methods** : Spécifie les méthodes HTTP autorisées pour accéder à la ressource. Dans cet exemple, toutes les méthodes HTTP (GET, POST, PUT, DELETE) sont autorisées.
* **Access-Control-Allow-Headers** : Spécifie les en-têtes HTTP autorisés dans la requête. Dans cet exemple, le type de contenu (**Content-Type**) et l'autorisation (**Authorization**) sont autorisés.

Ces en-têtes peuvent être personnalisés en fonction de vos besoins. Il est important de noter que l'ajout de ces en-têtes peut constituer une vulnérabilité de sécurité si elles sont configurées de manière incorrecte. Il est donc important de prendre les mesures de sécurité nécessaires.

**In my example :**

app.use((req, res, next) => {

  res.header("Access-Control-Allow-Origin", "\*");

  res.header(

    "Access-Control-Allow-headers",

    "Origin,X-Requested-With,Content-Type,Accept,Authorization"

  );

  if (req.method === "OPTIONS") {

    res.header("Access-Control-Allow-Methods", "PUT,POST,PATCH,DELETE");

    return res.status(200).json({});

  }

  next();

});