**API de données.**

#### **Architecture de l'API**

L'API expose des données relatives aux émissions de CO2 par état, secteur et type de carburant. L'architecture est basée sur FastAPI, une bibliothèque pour la création d'API web en Python. L'API est sécurisée à l'aide de OAuth2 avec le schéma de mot de passe.

##### **Composants Principaux**

1. FastAPI : Cadre principal pour créer l'API.
2. OAuth2PasswordBearer : Pour gérer l'authentification des utilisateurs.
3. SQLite3 : Base de données pour stocker les données d'émissions.
4. Pandas : Pour manipuler et interroger les données.
5. Pydantic : Pour la validation des données.

#### **Points de Terminaisons (Endpoints)**

L'API REST, créée à l'aide de FastAPI, expose les données relatives aux émissions de gaz à effet de serre. Voici les détails des points de terminaisons disponibles :

POST /token

* Description : Authentifie l'utilisateur et retourne un jeton d'accès.
* Paramètres de Requête :
  + username (string) : Nom d'utilisateur.
  + password (string) : Mot de passe.
* Réponse : Jeton d'accès (type Bearer).
* Exemple de Requête :

curl -X POST "http://127.0.0.1:8000/token" -d "username=admin&password=secret"

* Exemple de Réponse :

{

"access\_token": "secrettoken",

"token\_type": "bearer"

}

GET /emissions

* Description : Récupère les données d'émissions selon les filtres spécifiés.
* Paramètres de Requête :
  + year (Optionnel, string) : Année des données. Par défaut 'any'.
  + state\_name (Optionnel, string) : Nom de l'état. Par défaut 'any'.
  + sector\_name (Optionnel, string) : Nom du secteur. Par défaut 'any'.
  + fuel\_name (Optionnel, string) : Nom du carburant. Par défaut 'any'.
* Authentification : Nécessite un jeton d'accès (Bearer Token).
* Réponse : Liste des enregistrements correspondant aux critères de recherche.
* Exemple de Requête :

curl -X GET "http://127.0.0.1:8000/emissions?year=2020&state\_name=California&sector\_name=Transportation&fuel\_name=Gasoline" -H "Authorization: Bearer secrettoken"

* Exemple de Réponse :

[

{

"year": 2020,

"state\_name": "California",

"sector\_name": "Transportation",

"fuel\_name": "Gasoline",

"value": 12345.67,

"latitude": 34.0522,

"longitude": -118.2437

},

...

]

#### **Règles d'Authentification et/ou d'Autorisation**

L'API utilise OAuth2 avec le schéma Password pour l'authentification. Voici les règles d'authentification et d'autorisation :

1. Authentification :
   * Les utilisateurs doivent s'authentifier en envoyant leurs identifiants (nom d'utilisateur et mot de passe) au point de terminaison /token.
   * Si les identifiants sont corrects, un jeton d'accès (Bearer Token) est retourné, qui doit être utilisé pour accéder aux points de terminaison protégés.
2. Autorisation :
   * Le jeton d'accès doit être inclus dans le header Authorization pour accéder aux points de terminaison protégés, comme /emissions.
   * Le jeton est vérifié par la fonction authenticate\_token. Si le jeton est invalide, une réponse 401 Unauthorized est retournée.

#### Respect des Standards du Modèle REST

L'API respecte les standards REST suivants :

* Statelessness : Chaque requête contient toutes les informations nécessaires pour être traitée, sans dépendance à des états antérieurs.
* Clarity : Les points de terminaison sont clairs et suivent des conventions de dénomination cohérentes.
* HTTP Verbs : Utilisation appropriée des verbes HTTP (POST pour créer des jetons et GET pour récupérer des données).
* Authentication : Utilisation de OAuth2 pour sécuriser les points de terminaison protégés.