

Lire un contrat OpenAPI

Pendant la chasse au trésor, vous avez découvert API-ritif à tâtons, en lisant les réponses une par une. Il existe une méthode plus reposante : lire son **contrat**.

Qu'est-ce qu'un contrat d'API ?

Un contrat décrit **tout** ce qu'une API sait faire, dans un format lisible par les humains et par les machines :

- les routes et les méthodes ;
- les paramètres attendus et leur type ;
- le format des bodies envoyés et reçus ;
- les codes de statut possibles ;
- la méthode d'authentification.

Le standard est **OpenAPI** (anciennement *Swagger*), écrit en YAML ou en JSON. Ce cours utilise la version **3.1**. La 3.2, sortie en 2025, est encore peu supportée par les outils.

Le contrat est la **source de vérité** partagée entre l'équipe front, l'équipe back, les testeurs, les partenaires... et les IA. Quand le code et le contrat ne disent pas la même chose, c'est un bug.

Ouvrir le contrat d'API-ritif

- Téléchargez le contrat : api-ritif.openapi.yaml
- Ouvrez editor.swagger.io.
- Menu **File** → **Import file**, ou copiez-collez le contenu à gauche.

À gauche, le YAML. À droite, la documentation générée.

Swagger Editor sert à **lire et écrire** le contrat. Pour envoyer de vraies requêtes, utilisez la documentation servie par API-ritif elle-même : <http://api-ritif.portlatch.com/docs> (bouton **Try it out**). Depuis editor.swagger.io, les requêtes

seraient bloquées par le navigateur : vous comprendrez pourquoi au chapitre 8 (CORS).

Swagger Editor signale en direct les erreurs de syntaxe : c'est aussi l'outil idéal pour **écrire** un contrat.

Ce qu'on y lit

Un extrait, pour la route qui annule une commande :

```
/orders/{order_id}:
  delete:
    tags: [Commandes]
    operationId: cancelOrder
    summary: Annuler une commande
    description: Possible uniquement tant que la commande est `pending`.
    security:
      - ApiKeyAuth: []
    responses:
      '204':
        description: Commande annulée
      '401':
        $ref: '#/components/responses/Unauthorized'
      '404':
        $ref: '#/components/responses/NotFound'
      '409':
        description: La commande n'est plus annulable
```

Sans même connaître OpenAPI, on comprend : `DELETE /orders/{order_id}`, authentifié par clé d'API, répond `204` en cas de succès et `409` si c'est trop tard. Tout ce que vous avez découvert à la main pendant la chasse au trésor était écrit là.

À vous de chercher

Trouvez dans le contrat la réponse à ces questions :

1. Quelles routes peut-on appeler sans être authentifié ?
2. Combien de caractères peut contenir un `message_to_bartender` ?
3. Combien d'éléments une page contient-elle par défaut ? Et au maximum ?

4. Quels codes de statut `POST /orders` peut-il renvoyer ?
 5. Quels sont les statuts possibles d'une commande ?
 6. Quelles sont les deux façons de s'authentifier ?
-

Revision #4

Created 2 October 2026 20:00:50 by Thibaud FRICHET

Updated 13 October 2026 22:07:03 by Thibaud FRICHET