

Document d'architecture — Service d'expédition des commandes (exemple fictif)

Projet : Service d'expédition des commandes (exemple fictif)

Espace : Espace libre-service local (fictif)

Version : V2 — 27 septembre 2026

Conservé par : Client local (fictif)

Statut : Résultat assisté par IA

État de la revue : résultat assisté par IA — proposition, revue critique par un second modèle et contrôles automatiques effectués ; aucune validation professionnelle.

Résultat assisté par IA — proposition, revue critique et contrôles automatiques ; non validé par un professionnel ; ne constitue ni une estimation validée ni une offre de prix

Ce document se lit seul : il reprend le besoin, le périmètre, l'architecture proposée, les décisions justifiées et l'état de la revue, à la version indiquée.

Besoin et objectifs

Construire un nouveau service interne qui orchestre la préparation des expéditions — réception des commandes payées, réservation en entrepôt, demande d'étiquette au transporteur et retour du numéro de suivi — pour réduire le travail manuel actuel, avec une résilience qui couvre toute la chaîne sortante, pas seulement la demande d'étiquette.

Dossier fictif d'exemple public. Une entreprise de vente en ligne automatise aujourd'hui manuellement la préparation de ses expéditions. Le service à construire n'a pas d'écran destiné au client final ; le choix du transporteur et la négociation tarifaire restent de la responsabilité de la direction, hors mandat. Le volume quotidien de commandes n'est pas connu, une croissance forte est annoncée sans chiffre vérifié, et le budget n'a pas été discuté au préalable. La revue a précisé que la reprise après incident (sauvegarde et

restauration testées) fait partie du périmètre retenu, indépendamment de la reprise des demandes d'étiquette, et que la résilience doit aussi couvrir l'accusé de réception à la boutique et la libération d'une réservation en cas d'échec définitif de l'étiquette.

Périmètre inclus

Code	Nature	Élément	État
E-1	Objectif	Automatiser la préparation des expéditions pour réduire le travail manuel	à confirmer
E-2	Exigence	Réception des commandes payées depuis la boutique en ligne par API	à confirmer
E-3	Exigence	Accusé de réception de la commande avant traitement différé	à confirmer
E-4	Exigence	Réservation des articles commandés dans l'entrepôt	à confirmer
E-5	Exigence	Libération de la réservation après échec définitif de l'étiquette	à confirmer
E-6	Exigence	Demande d'étiquette d'expédition au transporteur	à confirmer
E-7	Exigence	Reprise automatique des demandes d'étiquette échouées sans doublon d'expédition	à confirmer
E-8	Exigence	Retour du numéro de suivi à la boutique en ligne	à confirmer
E-9	Exigence	Traitement idempotent d'une commande transmise deux fois par la boutique	à confirmer
E-10	Exigence	Écran de suivi interne pour le personnel de l'entrepôt	à confirmer
E-11	Exigence	Tableaux de bord et rapports sur les expéditions	à confirmer
E-12	Exigence	Conservation des commandes traitées trois ans puis suppression complète	à confirmer
E-13	Contrainte	Trois intégrations externes obligatoires : boutique en ligne, entrepôt, transporteur	à confirmer
E-17	Hypothèse	Volume quotidien de commandes inconnu ; croissance annoncée non chiffrée	à confirmer
E-18	Hypothèse	Budget non discuté au préalable	à confirmer
E-19	Hypothèse	Données traitées limitées à des coordonnées et identifiants clients	à confirmer
E-20	Hypothèse	Les trois systèmes tiers exposent des API exploitables pour l'intégration	à confirmer

Code	Nature	Élément	État
E-21	Hypothèse	Sauvegarde et restauration testées retenues comme acquises	à confirmer
E-22	Hypothèse	Usage de l'étiquette après son obtention à confirmer	à confirmer
E-23	Hypothèse	Niveau ASVS 1 retenu comme base de la revue de sécurité applicative	à confirmer

E-14 figure à la section « Exclusions ».

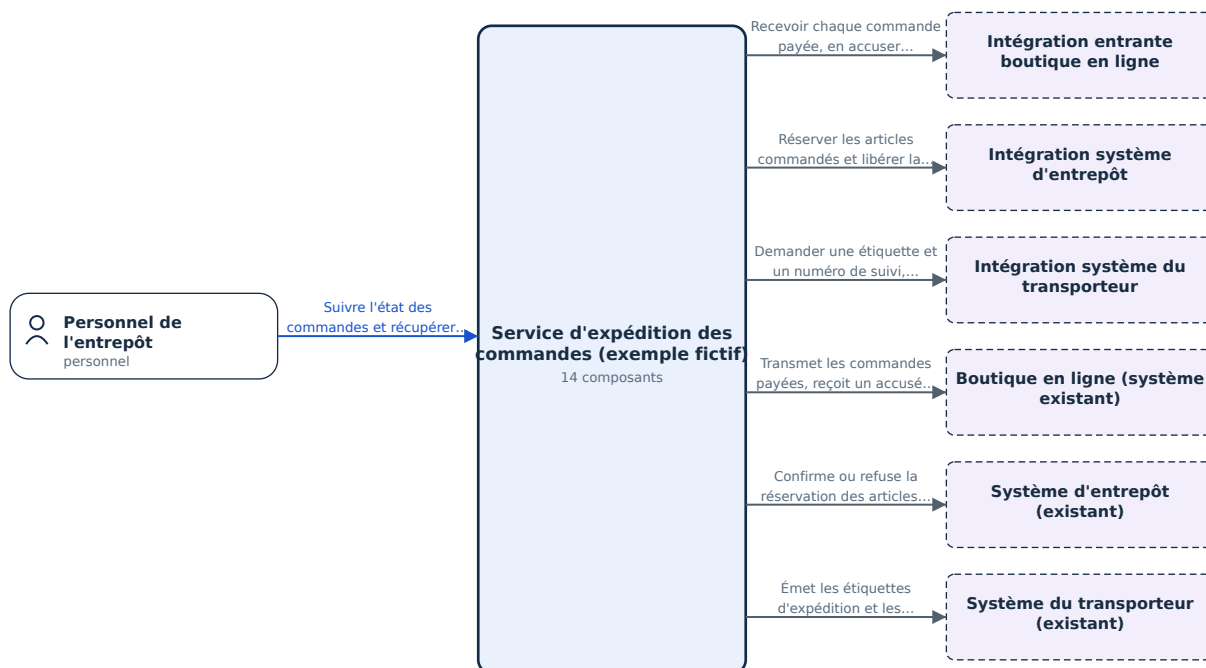
E-15 figure à la section « Exclusions ».

E-16 figure à la section « Exclusions ».

Architecture proposée

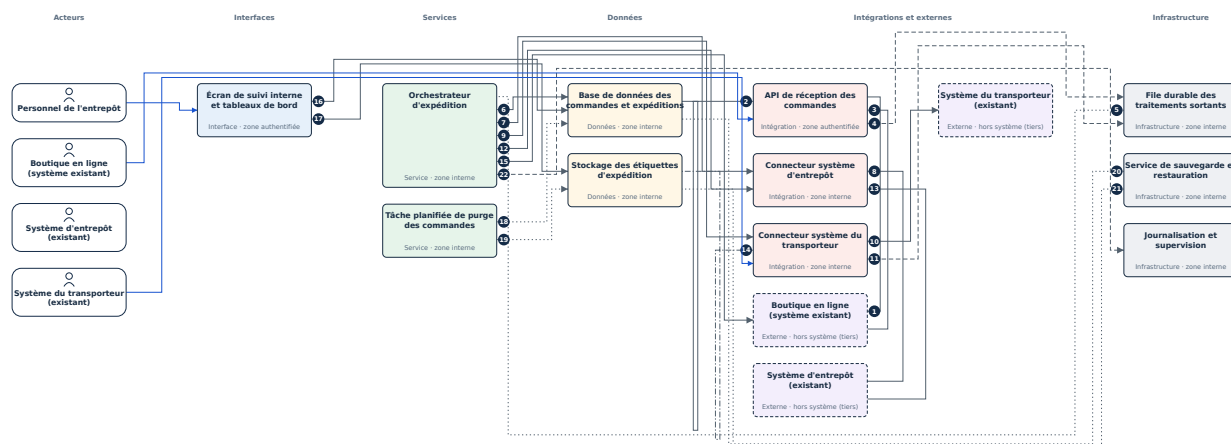
Construire un service back-office léger et sur mesure qui reçoit les commandes payées par API, accuse réception avant tout traitement différé, orchestre la réservation en entrepôt et la demande d'étiquette au transporteur avec une reprise idempotente sur toute la chaîne sortante (réservation, étiquette, retour de suivi), et offre un écran interne de suivi. La sauvegarde et la restauration testées font partie du périmètre retenu, indépendamment de la reprise des appels au transporteur. Les trois systèmes externes restent inchangés : on s'y intègre par leurs interfaces existantes plutôt que de les remplacer.

Vue d'ensemble



Composants et flux

Traits : appel (plein), événement (tirets), traitement planifié (pointillés), fichier (tiret-point), action d'une personne (bleu). Contour épais : zone restreinte ; contour pointillé : hors système.



Composants

Composant	Nature	Responsabilité
API de réception des commandes	Intégration	Reçoit chaque commande payée de la boutique, vérifie sa clé d'idempotence en base, accuse réception immédiatement puis met la commande en file pour un traitement différé (réservation, étiquette, retour de suivi).
File durable des traitements sortants	Infrastructure	Porte chaque étape sortante (réservation entrepôt, demande d'étiquette, retour de suivi) avec reprise automatique et idempotente en cas d'échec transitoire, sans dupliquer une expédition ni perdre un envoi.
Orchestrateur d'expédition	Service	Coordonne le cycle de vie de l'expédition depuis la file : réservation, demande d'étiquette, libération de réservation en cas d'échec définitif, retour de suivi ; tient l'état de la commande sans jamais dupliquer une expédition.
Connecteur système d'entrepôt	Intégration	Traduit vers l'API de l'entrepôt les demandes de réservation et, après un échec définitif de l'étiquette, les demandes de libération des articles réservés.
Connecteur système du transporteur	Intégration	Demande une étiquette au transporteur, reçoit le numéro de suivi, et vérifie l'existence d'une expédition avant toute nouvelle tentative pour éviter un doublon si un délai a été dépassé alors que l'étiquette existait déjà (hypothèse à confirmer avec vous selon les capacités réelles du transporteur).

Composant	Nature	Responsabilité
Base de données des commandes et expéditions	Données	Stocke l'état de chaque commande et expédition, les clés d'idempotence et l'historique des statuts ; applique la conservation de trois ans, distincte de la fenêtre technique de sauvegarde.
Stockage des étiquettes d'expédition	Données	Conserve le fichier d'étiquette obtenu du transporteur, associé à la commande, pour un usage au poste d'emballage encore à confirmer (impression, téléchargement ou transmission à l'entrepôt) ; couvert par la même conservation de trois ans.
Service de sauvegarde et restauration	Infrastructure	Sauvegarde régulièrement la base et le stockage des étiquettes, avec restauration testée, sur une fenêtre technique courte indépendante de la conservation métier de trois ans, retenue comme acquise pour l'exigence de reprise après incident.
Journalisation et supervision	Infrastructure	Centralise les journaux d'étapes, d'erreurs et de tentatives pour le diagnostic et la surveillance, sans y écrire de coordonnées client en clair, avec une rétention courte propre.
Tâche planifiée de purge des commandes	Service	Supprime automatiquement, à échéance des trois ans, les commandes en base et les étiquettes stockées associées ; les sauvegardes et journaux ne survivent pas au-delà grâce à leur propre fenêtre courte.
Écran de suivi interne et tableaux de bord	Interface	Présente au personnel de l'entrepôt la liste des commandes (en attente, expédiées, en erreur), des indicateurs agrégés, et si confirmé, le téléchargement de l'étiquette associée.
Boutique en ligne (système existant)	Externe	Transmet les commandes payées, reçoit un accusé de réception immédiat puis le numéro de suivi ; système existant, non modifié par ce mandat.
Système d'entrepôt (existant)	Externe	Confirme ou refuse la réservation des articles, et traite les demandes de libération ; système existant, non modifié par ce mandat.
Système du transporteur (existant)	Externe	Émet les étiquettes d'expédition et les numéros de suivi ; parfois indisponible ; système existant, non modifié par ce mandat.

Flux

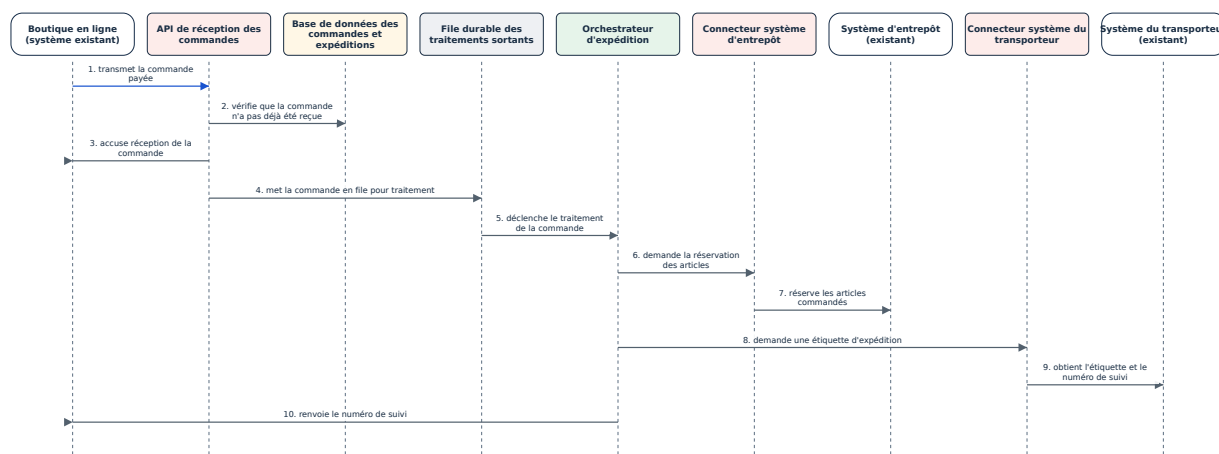
N°	De	Vers	Mode	Échange
1	Boutique en ligne (système existant)	API de réception des commandes	appel	Transmission d'une commande payée avec ses articles et les coordonnées du client
2	API de réception des commandes	Base de données des commandes et expéditions	appel	Vérification de la clé d'idempotence pour détecter une commande déjà reçue
3	API de réception des commandes	Boutique en ligne (système existant)	appel	Accusé de réception immédiat de la commande valide, avant tout traitement différé
4	API de réception des commandes	File durable des traitements sortants	événement	Mise en file de la commande acceptée pour traitement différé (réservation, étiquette, retour de suivi)
5	File durable des traitements sortants	Orchestrateur d'expédition	traitement planifié	Traitement différé et reprise idempotente de chaque étape sortante en échec transitoire
6	Orchestrateur d'expédition	Base de données des commandes et expéditions	appel	Création et mise à jour de l'état de la commande et de l'expédition
7	Orchestrateur d'expédition	Connecteur système d'entrepôt	appel	Demande de réservation des articles commandés
8	Connecteur système d'entrepôt	Système d'entrepôt (existant)	appel	Réservation des articles dans l'entrepôt
9	Orchestrateur d'expédition	Connecteur système du transporteur	appel	Demande d'étiquette d'expédition pour la commande réservée
10	Connecteur système du transporteur	Système du transporteur (existant)	appel	Demande d'étiquette, avec vérification préalable de l'existence d'une expédition avant toute nouvelle tentative
11	Connecteur système du transporteur	File durable des traitements sortants	événement	Remise en file d'une demande d'étiquette en échec transitoire pour nouvelle tentative
12	Orchestrateur d'expédition	Connecteur système d'entrepôt	appel	Libération de la réservation après échec définitif et non récupérable de la demande d'étiquette
13	Connecteur système d'entrepôt	Système d'entrepôt (existant)	appel	Libération des articles précédemment réservés
14	Connecteur système du transporteur	Stockage des étiquettes d'expédition	fichier	Dépôt du fichier d'étiquette obtenu, associé à la commande
15	Orchestrateur d'expédition	Boutique en ligne (système existant)	appel	Retour du numéro de suivi une fois l'étiquette obtenue, avec reprise en cas d'indisponibilité temporaire de la boutique
16	Écran de suivi interne et tableaux de bord	Base de données des commandes et expéditions	appel	Lecture des commandes par statut et des indicateurs agrégés
17	Écran de suivi interne et tableaux de bord	Stockage des étiquettes d'expédition	appel	Téléchargement de l'étiquette associée à une commande (usage à confirmer avec vous)

N°	De	Vers	Mode	Échange
18	Tâche planifiée de purge des commandes	Base de données des commandes et expéditions	traitement planifié	Suppression des commandes et de leur historique dont la conservation de trois ans est échue
19	Tâche planifiée de purge des commandes	Stockage des étiquettes d'expédition	traitement planifié	Suppression des étiquettes associées aux commandes dont la conservation est échue
20	Service de sauvegarde et restauration	Base de données des commandes et expéditions	traitement planifié	Sauvegarde régulière et restauration testée, sur une fenêtre technique courte distincte de la conservation métier
21	Service de sauvegarde et restauration	Stockage des étiquettes d'expédition	traitement planifié	Sauvegarde du stockage des étiquettes, sur la même fenêtre technique courte
22	Orchestrateur d'expédition	Journalisation et supervision	événement	Journalisation des étapes, erreurs et tentatives, sans coordonnées client en clair

Parcours utilisateurs

Expédier automatiquement une commande payée — Boutique en ligne (système existant)

But : Faire réserver les articles, obtenir une étiquette et renvoyer le suivi sans intervention manuelle.



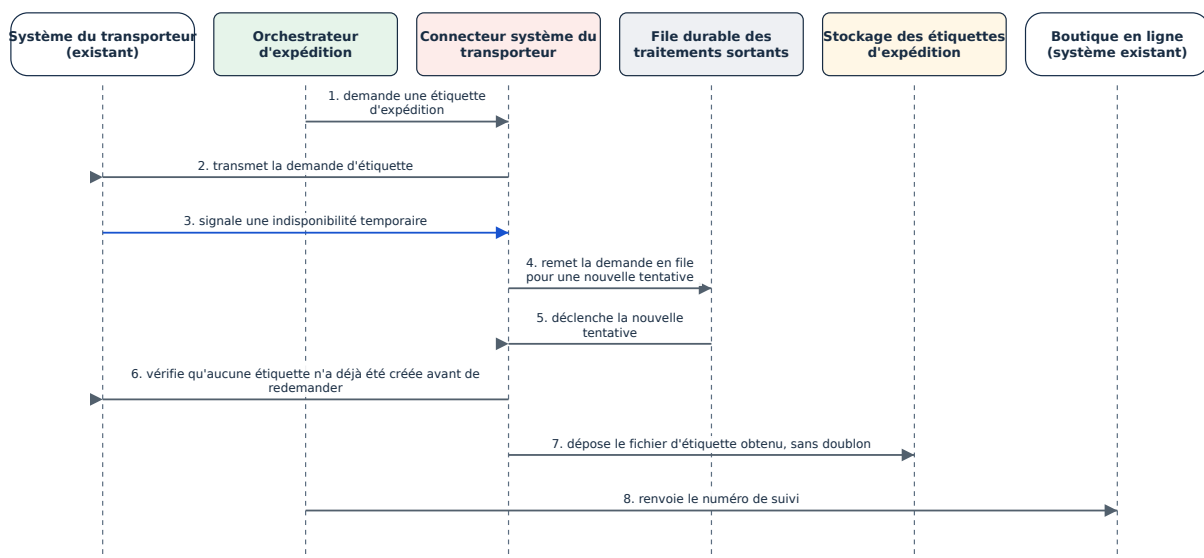
- 1. Boutique en ligne (système existant) → API de réception des commandes : transmet la commande payée
- 2. API de réception des commandes → Base de données des commandes et expéditions : vérifie que la commande n'a pas déjà été reçue
- 3. API de réception des commandes → Boutique en ligne (système existant) : accuse réception de la commande
- 4. API de réception des commandes → File durable des traitements sortants : met la commande en file pour traitement
- 5. File durable des traitements sortants → Orchestrateur d'expédition : déclenche le

traitement de la commande

- 6. Orchestrateur d'expédition → Connecteur système d'entrepôt : demande la réservation des articles
- 7. Connecteur système d'entrepôt → Système d'entrepôt (existant) : réserve les articles commandés
- 8. Orchestrateur d'expédition → Connecteur système du transporteur : demande une étiquette d'expédition
- 9. Connecteur système du transporteur → Système du transporteur (existant) : obtient l'étiquette et le numéro de suivi
- 10. Orchestrateur d'expédition → Boutique en ligne (système existant) : renvoie le numéro de suivi

Reprendre une demande d'étiquette après un échec temporaire du transporteur — Système du transporteur (existant)

But : Obtenir l'étiquette malgré une indisponibilité temporaire, sans créer de double expédition.

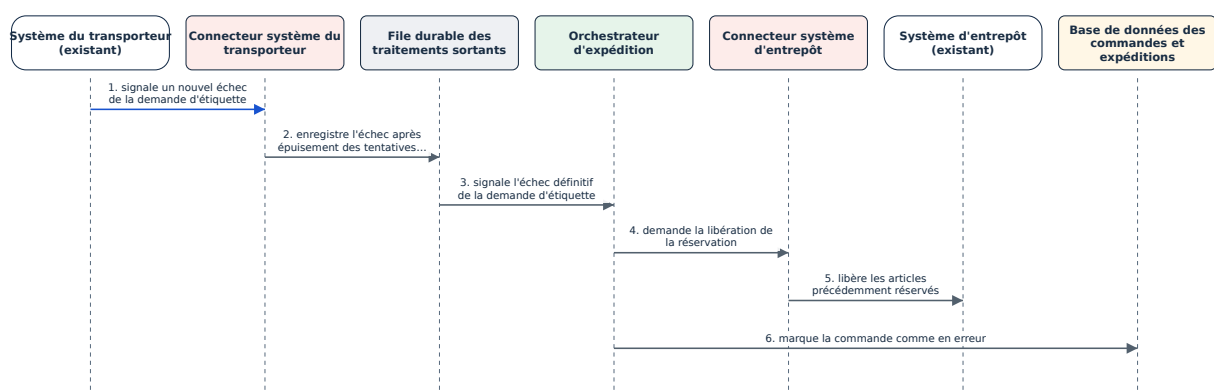


- 1. Orchestrateur d'expédition → Connecteur système du transporteur : demande une étiquette d'expédition
- 2. Connecteur système du transporteur → Système du transporteur (existant) : transmet la demande d'étiquette
- 3. Système du transporteur (existant) → Connecteur système du transporteur : signale une indisponibilité temporaire
- 4. Connecteur système du transporteur → File durable des traitements sortants : remet la demande en file pour une nouvelle tentative
- 5. File durable des traitements sortants → Connecteur système du transporteur : déclenche la nouvelle tentative

- 6. Connecteur système du transporteur → Système du transporteur (existant) : vérifie qu'aucune étiquette n'a déjà été créée avant de redemander
- 7. Connecteur système du transporteur → Stockage des étiquettes d'expédition : dépose le fichier d'étiquette obtenu, sans doublon
- 8. Orchestrateur d'expédition → Boutique en ligne (système existant) : renvoie le numéro de suivi

Libérer les articles réservés après un échec définitif de l'étiquette — Système du transporteur (existant)

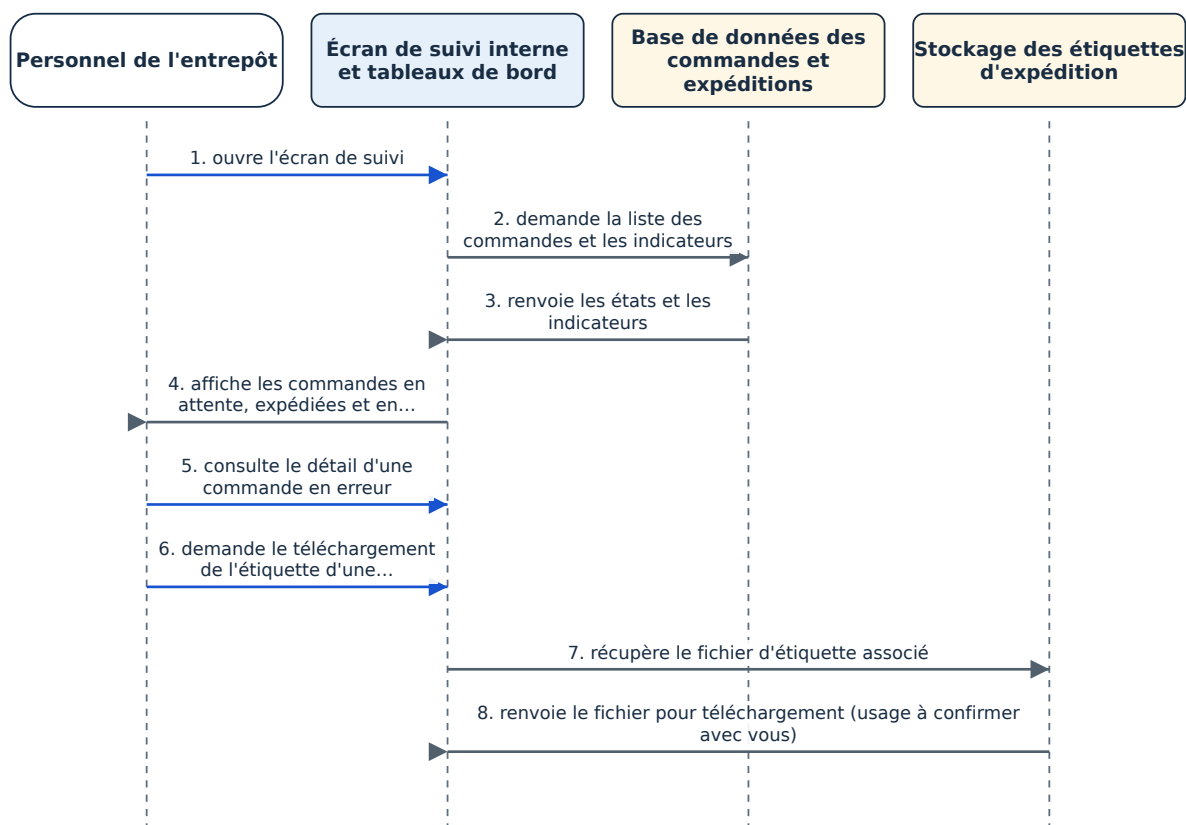
But : Éviter que des articles restent réservés sans être expédiés lorsque le transporteur ne peut jamais fournir d'étiquette.



- 1. Système du transporteur (existant) → Connecteur système du transporteur : signale un nouvel échec de la demande d'étiquette
- 2. Connecteur système du transporteur → File durable des traitements sortants : enregistre l'échec après épuisement des tentatives prévues
- 3. File durable des traitements sortants → Orchestrateur d'expédition : signale l'échec définitif de la demande d'étiquette
- 4. Orchestrateur d'expédition → Connecteur système d'entrepôt : demande la libération de la réservation
- 5. Connecteur système d'entrepôt → Système d'entrepôt (existant) : libère les articles précédemment réservés
- 6. Orchestrateur d'expédition → Base de données des commandes et expéditions : marque la commande comme en erreur

Suivre l'état des commandes et récupérer une étiquette depuis l'entrepôt — Personnel de l'entrepôt

But : Voir en un coup d'œil les commandes en attente, expédiées ou en erreur, et accéder à l'étiquette d'une commande expédiée.



- 1. Personnel de l'entrepôt → Écran de suivi interne et tableaux de bord : ouvre l'écran de suivi
- 2. Écran de suivi interne et tableaux de bord → Base de données des commandes et expéditions : demande la liste des commandes et les indicateurs
- 3. Base de données des commandes et expéditions → Écran de suivi interne et tableaux de bord : renvoie les états et les indicateurs
- 4. Écran de suivi interne et tableaux de bord → Personnel de l'entrepôt : affiche les commandes en attente, expédiées et en erreur
- 5. Personnel de l'entrepôt → Écran de suivi interne et tableaux de bord : consulte le détail d'une commande en erreur
- 6. Personnel de l'entrepôt → Écran de suivi interne et tableaux de bord : demande le téléchargement de l'étiquette d'une commande expédiée
- 7. Écran de suivi interne et tableaux de bord → Stockage des étiquettes d'expédition : récupère le fichier d'étiquette associé
- 8. Stockage des étiquettes d'expédition → Écran de suivi interne et tableaux de bord : renvoie le fichier pour téléchargement (usage à confirmer avec vous)

Données

Composant	Zone	Données conservées
API de réception des commandes	zone authentifiée	Identifiant de commande, Articles commandés, Coordonnées client (nom, courriel, adresse, téléphone)
File durable des traitements sortants	zone interne	Identifiant de commande, Type de tâche sortante, Nombre de tentatives, Dernière erreur reçue
Orchestrateur d'expédition	zone interne	État de la commande (en attente, expédiée, en erreur), Clé d'idempotence de la commande, Historique des tentatives par étape
Connecteur système d'entrepôt	zone interne	Identifiant de commande, Articles à réserver ou libérer, Statut de réservation
Connecteur système du transporteur	zone interne	Identifiant de commande, Données d'expédition (adresse, poids), Étiquette et numéro de suivi
Base de données des commandes et expéditions	zone interne	Commande, Expédition et statut, Coordonnées client, Numéro de suivi, Horodatage de réception et de suppression prévue
Stockage des étiquettes d'expédition	zone interne	Fichier d'étiquette, Identifiant de commande associé, Date d'obtention
Service de sauvegarde et restauration	zone interne	Copies de sauvegarde de la base, Copies de sauvegarde des étiquettes, Journal des restaurations testées
Journalisation et supervision	zone interne	Horodatage et étape, Code d'erreur, Identifiant de commande (référence, sans coordonnées)
Tâche planifiée de purge des commandes	zone interne	Identifiant de commande, Date d'échéance de conservation
Écran de suivi interne et tableaux de bord	zone authentifiée	État des commandes, Indicateurs agrégés (volumes, erreurs, délais)
Boutique en ligne (système existant)	hors système (tiers)	Commande payée, Numéro de suivi
Système d'entrepôt (existant)	hors système (tiers)	Disponibilité des articles, Confirmation de réservation ou de libération
Système du transporteur (existant)	hors système (tiers)	Étiquette d'expédition, Numéro de suivi

Intégrations

Intégration	Objectif
Intégration entrante boutique en ligne	Recevoir chaque commande payée, en accuser réception immédiatement, puis renvoyer le numéro de suivi avec reprise en cas d'indisponibilité de la boutique.
Intégration système d'entrepôt	Réserver les articles commandés et libérer la réservation en cas d'échec définitif de l'étiquette.
Intégration système du transporteur	Demander une étiquette et un numéro de suivi, reprendre automatiquement les échecs transitoires, et vérifier l'existence d'une expédition avant chaque nouvelle tentative.

Contraintes

- Les trois systèmes externes restent inchangés ; le service s'y intègre sans les remplacer ni dupliquer leurs données maîtresses.
- Toute étape sortante (réservation, demande d'étiquette, retour de suivi) passe par la file durable avec reprise idempotente ; aucune répétition ne doit produire deux expéditions ni perdre un numéro de suivi.
- Un échec définitif et non récupérable de la demande d'étiquette libère la réservation correspondante en entrepôt.
- La conservation métier de trois ans s'applique aux commandes, aux étiquettes stockées et à leurs sauvegardes ; la fenêtre de sauvegarde technique reste courte et distincte de cette conservation.
- La journalisation applicative évite toute coordonnée client en clair et suit une rétention courte propre.
- La vérification d'existence d'une expédition avant nouvelle tentative auprès du transporteur reste une hypothèse tant que sa capacité d'idempotence n'est pas confirmée.
- Le dimensionnement de l'infrastructure part d'un volume de commandes hypothétique et modéré, faute de chiffre confirmé par le client.
- Le choix du ou des transporteurs et la négociation tarifaire restent hors architecture ; chaque transporteur additionnel dès le départ requiert un connecteur propre.
- L'API de réception des commandes n'accepte que des appels authentifiés de la boutique en ligne et vérifie l'idempotence avant d'accuser réception ; aucun accès anonyme.
- L'écran de suivi et les tableaux de bord sont réservés au personnel authentifié de l'entrepôt ; aucune interface ni notification par courriel n'est prévue pour le client final.
- Les connecteurs vers l'entrepôt et le transporteur utilisent des identifiants propres à chaque système tiers, distincts des comptes internes ; un connecteur distinct est

prévu par transporteur additionnel.

- La base de données des commandes et expéditions n'est accessible qu'aux composants internes du service, jamais directement de l'extérieur.
- Le stockage des étiquettes n'est accessible qu'aux composants internes et, en lecture, au personnel authentifié via l'écran de suivi, par lien à durée limitée si le téléchargement est confirmé.
- Aucune donnée de paiement n'est reçue ni stockée ; seules les coordonnées nécessaires à l'expédition transitent et sont conservées.
- La journalisation ne conserve pas les coordonnées client en clair et suit sa propre fenêtre de rétention courte, indépendante de la conservation métier de trois ans.

Limites de l'architecture proposée

- 9 décisions d'architecture (DA-1, DA-2, DA-3, DA-4, DA-5, DA-6, DA-7, DA-8, DA-9) : propositions non encore revues (maintenues telles quelles à la revue).

Détails techniques

Avec quoi la solution est construite, et où elle est hébergée. Chaque choix porte son statut : retenu lorsque le dossier l'arrête, hypothèse lorsqu'il a simplement servi au chiffrage, à confirmer lorsqu'il dépend d'une réponse attendue. Un choix marqué hypothèse n'engage personne ; il indique ce qui a été supposé pour produire les chiffres.

Outils de programmation

Couche	Choix	Statut	Pourquoi ce choix pour ce dossier
Langage et exécution	Node.js avec TypeScript (exécution serveur)	hypothèse	Écosystème mature pour API REST et connecteurs HTTP vers trois systèmes tiers ; bon support de traitements asynchrones pour la file de traitements sortants, dont le périmètre couvre désormais l'accusé de réception, la réservation, l'étiquette et le retour de suivi. Hypothèse de chiffrage, proportionnée à une équipe unique et à un monolithe modulaire.
Cadriciel applicatif	Cadriciel web modulaire orienté API et injection de dépendances (ex. NestJS)	hypothèse	Structure en modules alignée sur l'orchestrateur, les connecteurs (boutique, entrepôt, transporteur), la file durable élargie et l'écran de suivi du monolithe modulaire retenu ; frontières claires sans exiger plusieurs équipes.

Couche	Choix	Statut	Pourquoi ce choix pour ce dossier
Interface utilisateur	Application web interne monopage pour l'écran de suivi et les tableaux de bord (ex. React)	hypothèse	Un seul écran interne réservé au personnel de l'entrepôt, sans portail public ; suffit pour lister les commandes par statut, présenter les indicateurs agrégés et, si confirmé, permettre le téléchargement de l'étiquette.
Base de données	Base de données relationnelle gérée (PostgreSQL)	hypothèse	Modèle transactionnel (commandes, statuts, clés d'idempotence sur chaque étape sortante), volumes bornés et rapports attendus : stockage relationnel classique avec sauvegarde et restauration éprouvées.
Stockage de fichiers	Stockage objet compatible S3 pour les étiquettes d'expédition	à confirmer	Utile si le fichier d'étiquette doit être téléchargeable depuis l'écran de suivi ou transmis à l'entrepôt ; dépend directement de la réponse attendue sur l'usage de l'étiquette après son obtention. Couvert par la même conservation de trois ans et la même fenêtre de sauvegarde technique que la base.
File de tâches de fond	File de tâches adossée à la base de données pour l'ensemble des traitements sortants (accusé de réception, réservation, étiquette, retour de suivi)	hypothèse	Le périmètre de la file s'est élargi à toute la chaîne sortante, plus seulement la reprise transporteur ; volume de commandes encore inconnu, donc une file en base suffit au démarrage sans exploitation supplémentaire, migrable vers un courtier dédié si le volume confirmé ou la vérification préalable d'idempotence auprès du transporteur (question Q-7) alourdissent le débit.
Authentification	Authentification par jeton (clé API) pour les appels entrants et sortants ; accès du personnel de l'entrepôt via un fournisseur d'identité	à confirmer	Aucun mécanisme n'est précisé dans le dossier ; le jeton est standard pour des intégrations système à système, et un fournisseur d'identité évite de gérer des mots de passe pour l'écran interne. Dépend de la réponse attendue sur le mécanisme exact par intégration (question Q-4).
Observabilité	Journalisation centralisée et indicateurs de santé applicatifs, sans coordonnées client en clair	hypothèse	La disponibilité exigée et l'élargissement de la reprise à toute la chaîne sortante imposent de détecter rapidement les échecs de réservation, d'étiquette ou de retour de suivi ; les journaux excluent les coordonnées de clients pour ne pas contredire la purge à trois ans, avec une rétention propre et courte.

Couche	Choix	Statut	Pourquoi ce choix pour ce dossier
Intégration continue	Chaîne d'intégration et de déploiement continue (ex. GitHub Actions ou équivalent)	hypothèse	Service déployé d'un bloc (monolithe modulaire) ; une chaîne automatisée limite les erreurs de déploiement manuel et soutient l'excellence opérationnelle attendue pour ce dossier.
Tests	Tests automatisés unitaires et d'intégration couvrant l'idempotence sur toute la chaîne sortante et une revue de sécurité de base au niveau ASVS 1	hypothèse	Les scénarios critiques (commande dupliquée, échec transporteur avec vérification préalable, libération de réservation) exigent des tests reproductibles ; le niveau 1 de l'ASVS 5.0.0 est retenu comme hypothèse de référentiel pour une revue de sécurité applicative, compte tenu des coordonnées de clients traitées.

- Node.js avec TypeScript (exécution serveur) — écarté : Python ; .NET / C# ; Java
- Cadriciel web modulaire orienté API et injection de dépendances (ex. NestJS) — écarté : Cadriciel Python (ex. FastAPI ou Django) ; ASP.NET Core ; Spring Boot
- Application web interne monopage pour l'écran de suivi et les tableaux de bord (ex. React) — écarté : Rendu côté serveur classique ; Vue.js ; Intégration à un outil de tableau de bord existant du client
- Base de données relationnelle gérée (PostgreSQL) — écarté : Base NoSQL orientée documents ; Autre moteur relationnel géré (ex. MySQL)
- Stockage objet compatible S3 pour les étiquettes d'expédition — écarté : Conservation de l'étiquette en base si le fichier est très petit ; Aucun stockage si seul le numéro de suivi est conservé
- File de tâches adossée à la base de données pour l'ensemble des traitements sortants (accusé de réception, réservation, étiquette, retour de suivi) — écarté : Courtier de messages dédié ; Planificateur de tâches simple sans file dédiée
- Authentification par jeton (clé API) pour les appels entrants et sortants ; accès du personnel de l'entrepôt via un fournisseur d'identité — écarté : Authentification mutuelle par certificat (mTLS) ; Réseau privé virtuel dédié par intégration ; Compte applicatif interne sans fournisseur d'identité externe
- Journalisation centralisée et indicateurs de santé applicatifs, sans coordonnées client en clair — écarté : Journalisation locale minimale sans agrégation centralisée ; Outil d'observabilité auto-hébergé
- Chaîne d'intégration et de déploiement continue (ex. GitHub Actions ou équivalent) — écarté : Déploiement manuel scripté ; Autre chaîne d'intégration continue (ex. GitLab CI, Azure DevOps)
- Tests automatisés unitaires et d'intégration couvrant l'idempotence sur toute la chaîne sortante et une revue de sécurité de base au niveau ASVS 1 — écarté : Tests

manuels uniquement ; Tests de contrat automatisés avec chaque système tiers, si un environnement de test tiers est disponible ; Niveau ASVS supérieur si exigé par vous

Hébergement

Modèle d'hébergement : Infonuagique gérée (plateforme) (hypothèse)

Catégorie de fournisseur : Fournisseur d'infonuagique public généraliste offrant calcul applicatif géré, base de données relationnelle gérée, stockage objet et file de messages gérée

Conservation des données : Amérique du Nord (Canada ou États-Unis)

Environnements : Développement · Test et recette (incluant l'accès sandbox aux API de la boutique, de l'entrepôt et du transporteur) · Production

Sauvegardes et rétention : Sauvegarde régulière de la base et réplique du stockage des étiquettes, retenues comme principe indépendant de la reprise des demandes d'étiquette (exigence de reprise après incident déclarée indispensable). La fenêtre technique de rétention des sauvegardes reste courte et distincte de la conservation métier de trois ans, pour ne pas faire survivre des coordonnées de clients au-delà de l'échéance de purge. Cadence exacte et durée de rétention technique à confirmer.

Reprise après incident : Reprise automatique et idempotente sur toute la chaîne sortante (réservation, demande d'étiquette, retour de suivi), avec limite de tentatives et file de rebut ; vérification de l'existence d'une expédition avant chaque nouvelle tentative auprès du transporteur (hypothèse, à confirmer selon ses capacités).
Restauration testée de la base et du stockage des étiquettes à un point dans le temps.
Cibles de délai d'interruption maximal et de perte de données tolérée non chiffrées par le dossier, à établir avec vous.

Services d'hébergement chiffrés

Ces lignes sont celles de l'estimation : elles figurent déjà dans les dépenses du dossier, initiales et récurrentes.

Service	Périodicité	Montant par période
Nom de domaine et certificats TLS	Une fois	0,00 CAD
Frais d'ouverture de l'environnement infonuagique	Une fois	0,00 CAD
Hébergement du service applicatif (API, file, orchestrateur, connecteurs)	Mensuelle	170,00 CAD
Base de données gérée des commandes et expéditions	Mensuelle	190,00 CAD
Stockage objet des fichiers d'étiquettes d'expédition	Mensuelle	8,00 CAD
Surveillance et journalisation centralisée	Mensuelle	45,00 CAD

Service	Périodicité	Montant par période
Sauvegardes régulières et fenêtre de restauration testée (base et étiquettes)	Mensuelle	30,00 CAD
- Aucun outil de programmation ni fournisseur d'hébergement n'est arrêté dans le dossier : l'ensemble de la pile technique est une hypothèse de chiffrage, pas un engagement contractuel. - Les couches paiement, courriel/notifications et recherche ne sont pas retenues : aucune donnée de paiement n'est traitée, aucune notification par courriel n'est demandée et aucune fonction de recherche n'est décrite dans le dossier. - Le périmètre de la file de traitements différés s'est élargi à toutes les étapes sortantes (accusé de réception, réservation, étiquette, retour de suivi) ; le choix entre file en base et courtier dédié dépend du volume réel, encore inconnu. - La sauvegarde et la restauration testées sont retenues comme principe, indépendamment de la reprise des appels au transporteur ; leur cadence et leur fenêtre technique restent à confirmer avec vous, et doivent rester plus courtes que la conservation métier de trois ans. - Aucune exigence de résidence n'est déclarée pour les coordonnées de clients ; l'hébergement en Amérique du Nord est une hypothèse à confirmer, notamment au regard des obligations applicables. - Le stockage objet des étiquettes dépend de la réponse sur l'usage de l'étiquette après son obtention ; il reste à confirmer plutôt que retenu. - Le niveau 1 de l'ASVS 5.0.0 est retenu comme hypothèse de référentiel pour les tests et la revue de sécurité applicative, compte tenu des coordonnées de clients traitées ; à confirmer avec vous avant la mise en production. - La journalisation centralisée exclut les coordonnées de clients en clair et suit sa propre rétention courte, indépendante de la conservation métier de trois ans, pour ne pas contredire la purge.		

Décisions d'architecture et justifications

Aucune décision d'architecture justifiée retenue.

Scénario présenté et alternatives

Scénario présenté : Scénario initial (construire) — scénario exploré, non retenu

État de la revue IA et réserves

État de la revue : résultat assisté par IA — proposition, revue critique par un second modèle et contrôles automatiques effectués ; aucune validation professionnelle.

La revue automatique a porté sur l'intégralité du périmètre présenté (23 éléments).

Aucune réserve non fermée relevée par la revue critique.

Références et versions

Version conservée : V2 — 27 septembre 2026 (2026-09-27T12:50:59-04:00)

Version de présentation : 1.7

Calcul : 23 — moteur 2.3

Gabarit du dossier : 1.7

Ce document se lit hors ligne ; les liens externes éventuels ne servent qu'à approfondir une référence. Il ne remplace pas une validation professionnelle.