



Cloud Architecture - Automation - AI



TRANSPORTS BREIZH EXPRESS

CLOUD ARCHITECTURE PROPOSAL

Plateforme de Traçabilité Logistique & Gestion de Flotte

PREPARED BY

Hugues Le Stang

Cloud Architecture & Automation

07/10/2026

01 EXECUTIVE SUMMARY

Dossier d'architecture Cloud de référence pour le déploiement de la Plateforme de Traçabilité Logistique & Gestion de Flotte de Transports Breizh Express. Calibrée pour absorber l'activité continue et les pics de charge de 1 500 transporteurs et répartiteurs connectés en simultané, cette architecture d'entreprise hautement résiliente est déployée à 100% dans la région souveraine AWS Paris (eu-west-3 (Paris)). Elle combine un portail Web SPA sécurisé par CloudFront et AWS WAF (terminaison TLS 1.3), un annuaire Amazon Cognito avec MFA obligatoire pour l'ensemble des chauffeurs et gestionnaires de flotte, un Application Load Balancer (ALB) public distribuant les flux vers une flotte de conteneurs Amazon ECS (AWS Fargate) répartie sur 3 zones de disponibilité privées (eu-west-3a, eu-west-3b, eu-west-3c), un cluster Amazon ElastiCache (Redis) dédié au suivi sub-milliseconde des positions GPS et des sessions, une base NoSQL managée Amazon DynamoDB en mode On-Demand pour l'ingestion haute cadence des événements de flotte, et un coffre documentaire Amazon S3 chiffré par clé KMS dédiée avec politique de transition automatique vers Glacier après 60 jours pour l'archivage légal des bordereaux et signatures numériques.

RÉGION AWS

Europe (Paris)

eu-west-3 (Paris)

UTILISATEURS

1 500

Actifs simultanés

COÛT ESTIMÉ

**511.50 € / mois (Infrastructure
Complète Multi-AZ 3 Datacenters &
Support 1 500 Utilisateurs)**

par mois (avec options HA / WAF)

ARCHITECTURE

Conteneurs ECS Fargate & In-Memory Redis

Multi-AZ Haute Disponibilité (3 AZs)

PROJECT OVERVIEW

La plateforme développée pour Transports Breizh Express répond aux impératifs d'une exploitation logistique moderne : ingestion continue de télémétrie GPS (ping régulier de 1 500 véhicules), cartographie temps réel sans latence pour les répartiteurs, conformité légale et non-répudiation des livraisons émargées, le tout sans point unique de défaillance (SPOF) grâce à un déploiement strict sur 3 zones de disponibilité (eu-west-3a, eu-west-3b, eu-west-3c).

DESIGN PRIORITIES

SECURITY

SCALABILITY

COST OPTIMIZATION

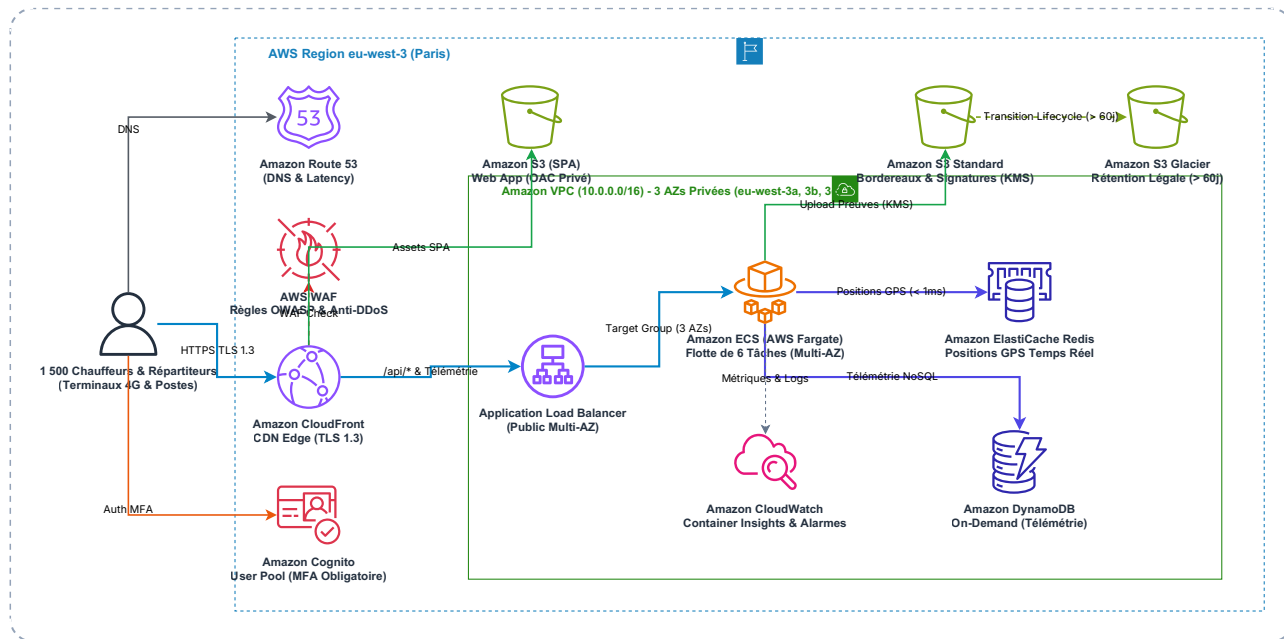
LOW MAINTENANCE

02 REQUIREMENTS & SCOPE

EXIGENCE	SPÉCIFICATION	PRISE EN COMPTE DANS L'ARCHITECTURE
Volume & Concurrency Élevée	1 500 transporteurs (télémétrie GPS active) et répartiteurs connectés en simultané	Flotte de conteneurs Amazon ECS (AWS Fargate) multi-AZ (6 à 12 tâches) derrière un Application Load Balancer public
Frontend & Protection Edge	Application web réactive (SPA / PWA) accessible sur mobiles et postes répartiteurs	Amazon S3 privé (OAC) distribué via CloudFront (TLS 1.3) avec pare-feu AWS WAF (Managed Rules OWASP, Bad Inputs, Rate Limit)
Authentification & Sécurité Flotte	MFA obligatoire pour l'ensemble des chauffeurs et répartiteurs logistiques	Amazon Cognito User Pool avec MFA obligatoire (TOTP / SMS), groupes RBAC (Chauffeurs, Répartiteurs, Admins) et jetons JWT RS256
Télémétrie GPS & Temps Réel	Suivi sub-milliseconde des positions GPS des 1 500 véhicules et sessions actives	Cluster en mémoire Amazon ElastiCache (Redis) Multi-AZ avec failover automatique et chiffrement TLS en transit
Base de Données Haute Cadence	Ingestion massive d'événements de livraison, historique des tournées et statuts	Amazon DynamoDB en mode On-Demand (clé de partition vehicle_id, clé de tri timestamp, index GSI, PITR et chiffrement KMS)
Stockage de Preuves & Archivage	Conservation sécurisée des bordereaux de livraison et signatures numériques	Amazon S3 Standard avec chiffrement SSE-KMS (clé CMK), S3 Versioning et cycle de vie Glacier Flexible Retrieval après 60 jours
Haute Disponibilité Multi-AZ	Résilience 24/7 sans interruption de service pour l'activité transport	Architecture distribuée sur 3 zones de disponibilité privées (eu-west-3a, 3b, 3c) avec redondance N+2 et basculement automatique
Supervision & Observabilité	Métriques temps réel, suivi des conteneurs et alertes sur anomalies	Amazon CloudWatch (Container Insights ECS, alarmes sur CPU/RAM Fargate, erreurs ALB 5xx, latence Redis et throttles DynamoDB)

03 PROPOSED ARCHITECTURE

Architecture Cloud native découplée déployée dans la région AWS eu-west-3 (Paris), combinant un hébergement statique distribué, une couche applicative serverless hautement disponible et une persistance managée sécurisée.



ARCHITECTURE DESCRIPTION & FLOW

La solution repose sur une séparation stricte des responsabilités (Front-end SPA, Backend API, Couche de données). L'authentification est déléguée à Amazon Cognito qui émet des jetons JWT validés par API Gateway.

- **Distribution & Caching :** Requêtes reçues par CloudFront via HTTPS/TLS 1.3 avec points de présence Edge.
- **Frontend SPA :** Composants servis directement depuis un bucket S3 privé via Origin Access Control (OAC).
- **Authentification :** Amazon Cognito User Pools avec émission et validation cryptographique de tokens JWT.
- **Couche API & Calcul :** API Gateway route les requêtes dynamiques vers les fonctions AWS Lambda sans serveur.
- **Persistence :** Fonctions Lambda requêtent PostgreSQL managé sur RDS et génèrent des URLs pré-signées S3.

04 CHOIX TECHNIQUES

Vulgarisation des choix techniques (Comprendre l'architecture en termes simples) :

HÉBERGEMENT WEB SPA & DISTRIBUTION EDGE CLOUDFRONT + WAF

L'interface web de gestion de flotte est hébergée sur Amazon S3 et propulsée par le réseau CDN CloudFront. Un pare-feu applicatif AWS WAF bloque en amont les attaques malveillantes et les surcharges.

Bénéfice : Temps de réponse instantané pour les 1 500 utilisateurs, zéro serveur Web à administrer, protection anti-DDoS AWS Shield incluse.

AUTHENTIFICATION RENFORCÉE AVEC COGNITO & MFA OBLIGATOIRE

Chaque chauffeur et répartiteur dispose d'un compte sécurisé avec double facteur (MFA) imposé. Les jetons cryptographiques JWT valident les droits stricts par rôle de l'utilisateur.

Bénéfice : Sécurité d'accès garantie, conformité réglementaire transport et RGPD, étanchéité absolue des données de tournée.

CALCUL CONTENEURISÉ AMAZON ECS FARGATE SUR 3 ZONES (MULTI-AZ)

L'API backend et les microservices s'exécutent dans des conteneurs managés par AWS Fargate. Aucun serveur ou machine virtuelle n'est à patcher : AWS alloue automatiquement la mémoire et le CPU nécessaires.

Bénéfice : Répartition sur 3 datacenters parisiens indépendants, tolérance intégrale à la panne d'un datacenter et auto-scaling sans rupture.

ACCÉLÉRATION IN-MEMORY ELASTICACHE REDIS POUR LES POSITIONS GPS

Les 1 500 camions remontent leurs positions GPS en continu. Redis stocke ces coordonnées en mémoire vive (RAM) à une vitesse sub-milliseconde pour rafraîchir en direct les écrans de contrôle des répartiteurs.

Bénéfice : Affichage temps réel sans aucun ralentissement et décharge totale de la base de données principale.

BASE DE DONNÉES DYNAMODB ON- DEMAND (HAUTE VITESSE)

Base NoSQL managée hautement scalable capable d'ingérer des millions de points GPS et de statuts de livraison par heure sans jamais saturer ni nécessiter de pré-réservation rigide de débit.

Bénéfice : Paiement à la requête exacte (zéro gaspillage), latence constante sous 10 ms, tolérance aux pannes intégrée sans maintenance.

COFFRE-FORT S3 & ARCHIVAGE AUTOMATISÉ VERS GLACIER (60 JOURS)

Les photos de colis, bordereaux émargés et signatures sont chiffrés sous clé KMS dédiée dans S3 Standard pendant 60 jours, puis basculés automatiquement vers Glacier pour un archivage économique sur 5 ans.

Bénéfice : Réduction de 82% du coût de stockage documentaire à long terme avec garantie d'invulnérabilité et durabilité de 99.999999999%.

05 AWS SERVICES BREAKDOWN

SERVICE AWS	RÔLE & USAGE	DIMENSIONNEMENT	JUSTIFICATION
Amazon CloudFront & AWS WAF	CDN mondial, terminaison TLS 1.3 & Pare-feu Web	Price Class 100 + WAF Managed Rules (OWASP, Rate-limit)	Distribution ultra-rapide des assets SPA, absorption DDoS et filtrage des requêtes malveillantes avant le réseau VPC.
Amazon S3 (SPA)	Hébergement statique du portail répartiteurs et chauffeurs	S3 Standard + Origin Access Control (OAC)	Isolation totale sans accès public direct, durabilité 11 9s et coût négligeable.
Amazon Cognito	Gestion des identités, rôles RBAC et MFA obligatoire	User Pool avec TOTP / SMS MFA activé	Sécurité d'accès garantie pour 1 500 chauffeurs et répartiteurs, tokens JWT RS256 standardisés.
Application Load Balancer (ALB)	Ingress public, terminaison HTTPS & Routage vers Fargate	ALB Multi-AZ public (3 AZs, Target Groups avec Health Checks)	Distribution intelligente des flux API et télémétrie vers les conteneurs avec basculement automatique.
Amazon ECS (AWS Fargate)	Exécution conteneurisée des microservices API & Ingestion	6 à 12 tâches Fargate (1 vCPU, 2 Go RAM) sur 3 AZ privées	Zéro gestion de VM, isolation stricte en sous-réseaux privés, scalabilité automatique sur pics de trafic logistique.
Amazon ElastiCache (Redis)	Cache en mémoire des positions GPS et sessions actives	Cluster Multi-AZ (2 nœuds cache.t4g.medium, Graviton)	Latence sub-milliseconde pour rafraîchir la cartographie des 1 500 camions en direct et délester DynamoDB.
Amazon DynamoDB	Stockage NoSQL haute cadence des historiques et tournées	Mode On-Demand (Pay-per-Request) + PITR + KMS	Ingestion fluide de 50M+ événements/mois sans verrouillage, requêtes par clé de partition ultra-rapides.
Amazon S3 & S3 Glacier	Coffre-fort des bordereaux émargés et signatures	S3 Standard → Glacier Flexible Retrieval après 60 jours	Chiffrement SSE-KMS, URLs pré-signées temporaires, réduction drastique du coût d'archivage légal.
Amazon CloudWatch & AWS KMS	Supervision temps réel, Container Insights & Chiffrement	Logs Fargate 20 Go + Clé CMK KMS + Alarmes métriques	Traçabilité intégrale, détection immédiate des pannes de flotte et respect des exigences de conformité.

06 SECURITY & COMPLIANCE

PRINCIPES ZERO-TRUST & MOINDRE PRIVILÈGE

- Chiffrement de bout en bout : HTTPS TLS 1.3 obligatoire, chiffrement au repos KMS sur DynamoDB, S3 et Redis.
- Ségrégation réseau stricte : VPC 3 AZs avec ALB en sous-réseau public, conteneurs Fargate et Redis isolés en sous-réseaux privés.
- Moindre privilège IAM : Rôles de tâches ECS limités strictement aux tables DynamoDB et au bucket de preuves Breizh Express.
- Zero-Trust & MFA : Double facteur obligatoire sur Cognito pour les 1 500 chauffeurs et répartiteurs, jetons JWT validés.

MATRICE DE SÉCURITÉ (DÉFENSE EN PROFONDEUR)

DOMAINE	MENACE / RISQUE	CONTRÔLE AWS	CONFORMITÉ
Périmètre Edge & WAF	DDoS, injections SQL/XSS, attaques par force brute sur l'API télémétrique	Amazon CloudFront avec protection AWS Shield Standard, AWS WAF (règles managées AWS Common & Bad Inputs, rate limiting 2000 req/ 5min) et TLS 1.3	ISO 27001 A.13, CIS AWS
Identité & Authentification Flotte	Usurpation d'identifiants, injection de fausses coordonnées GPS ou détournement de livraisons	Amazon Cognito avec MFA obligatoire pour 100% des utilisateurs, politiques strictes de mots de passe, jetons JWT RS256 expirant à 60 min	RGPD Art. 32, ANSSI R38
Isolation Réseau & Cloisonnement VPC	Intrusion directe sur les conteneurs ECS ou sur le cache Redis depuis Internet	Amazon VPC à 3 AZs. Tâches ECS Fargate et Redis confinées dans des sous-réseaux privés stricts. Seul l'ALB public accepte le trafic externe	ISO 27001 A.13.1, NIST 800-53
Intégrité des Preuves & Signatures (S3)	Altération de bordereau de livraison, suppression accidentelle ou malveillante de signature, ransomware	S3 Block Public Access (100%), chiffrement SSE-KMS avec clé client CMK dédiée, S3 Versioning et cycle Glacier en lecture seule	NF Z42-013, RGPD Art. 32
Protection Données Télémétriques (DynamoDB & Redis)	Fuite de géolocalisation de véhicules, écoute sur le réseau interne	Chiffrement au repos SSE-KMS pour DynamoDB et Redis, TLS forcé en transit sur ElastiCache Redis, accès IAM avec rôle de tâche ECS exclusif	RGPD Données de Localisation

DOMAINE	MENACE / RISQUE	CONTRÔLE AWS	CONFORMITÉ
Traçabilité & Détection d'Incidents	Pannes applicatives non détectées, perte de télémétrie sans alerte	CloudWatch Container Insights, alarmes automatisées sur seuil CPU/Mémoire Fargate > 75%, erreurs ALB 5xx et latence Redis > 5ms	ISO 27001 A.12.4

07 ESTIMATED MONTHLY COST

Estimation basée sur 1 500 utilisateurs actifs avec une architecture dimensionnée et optimisée pour l'usage réel :

SERVICE AWS	HYPOTHÈSE DE CONSOMMATION	COÛT MENSUEL
Amazon CloudFront (CDN Edge)	Distribution SPA mondiale, 300 Go/mois trafic sortant Edge, requêtes HTTPS TLS 1.3	25.50 €
AWS WAF (Web ACL)	1 Web ACL + 3 règles managées AWS (Common, Bad Inputs, Rate Limit) + 10M requêtes	14.50 €
Amazon S3 (SPA & Preuves)	Bucket SPA + 250 Go S3 Standard preuves + 500 Go archivage Glacier + requêtes	8.80 €
Amazon Cognito User Pool	1 500 utilisateurs actifs (inclus dans le quota gratuit 50 000 MAU) + MFA software token	3.50 €
Application Load Balancer (ALB)	1 ALB public Multi-AZ (730 h) + 4 LCU pour 1 500 connexions concurrentes	44.20 €
Réseau VPC & NAT Gateways	3 NAT Gateways redondantes (1 par AZ pour haute disponibilité stricte) + trafic sortant	98.40 €
Amazon ECS (AWS Fargate)	Flotte de 6 tâches Fargate réparties sur 3 AZs (1 vCPU, 2 Go RAM, 730 h en continu)	228.60 €
Amazon ElastiCache (Redis)	Cluster Multi-AZ (2 nœuds cache.t4g.medium avec failover automatique)	92.50 €
Amazon DynamoDB (On-Demand)	55M écritures WRU + 20M lectures RRU + 50 Go stockage avec TTL automatique	76.80 €
AWS KMS & Amazon CloudWatch	1 Clé client CMK dédiée + Container Insights ECS + 20 Go logs + alarmes de seuil	18.20 €
Amazon Route 53	1 Hosted zone publique + requêtes de résolution DNS à faible latence	0.50 €
Total estimé récurrent :		511.50 € / mois (Infrastructure Complète Multi-AZ 3 Datacenters & Support 1 500 Utilisateurs)

* Note : Estimation basée sur les hypothèses de consommation définies dans ce document. Les coûts réels peuvent varier.

08 SCALABILITY & AVAILABILITY

Comportement en charge : L'Application Load Balancer distribue uniformément les requêtes vers la flotte ECS Fargate qui s'adapte automatiquement (6 à 12 tâches) selon les métriques de charge CPU/RAM. ElastiCache Redis absorbe les requêtes de positions GPS en temps réel sous la milliseconde, tandis que DynamoDB On-Demand ingère jusqu'à des dizaines de milliers d'écritures par seconde sans aucun goulot d'étranglement.

99.95%

SLA Composite Global

99.9999999999%

Durabilité Données (11 9s)

COMPOSANT AWS	SLA CONTRACTUEL	GARANTIES DE RÉSILIENCE
Amazon Route 53 (DNS)	100.0%	Anycast mondial, tolérance de panne avec basculement automatique sans interruption.
CloudFront & AWS WAF	99.9%	Réseau de bordure mondial Edge avec protection DDoS Shield et basculement automatique des PoPs.
Application Load Balancer (ALB)	99.99%	Répartiteur managé multi-AZ avec contrôles d'intégrité continus (health checks) vers les conteneurs.
Amazon ECS (AWS Fargate)	99.99%	Flotte de conteneurs distribuée sur 3 AZs indépendantes (Paris a, b, c) avec résilience N+2.
Amazon ElastiCache (Redis)	99.99%	Cluster Multi-AZ avec détection automatique des pannes et basculement sur le réplica en < 30s.
Amazon DynamoDB	99.99%	Réplication synchrone native sur 3 zones de disponibilité et durabilité multi-datacenter sans interruption.
Amazon S3 & S3 Glacier	99.9% (11 9s durabilité)	Stockage répliqué de manière synchrone sur 3 datacenters distincts en Île-de-France.

09 RISKS & RECOMMENDATIONS

RISQUES IDENTIFIÉS

- Pic massif d'envoi simultané de positions GPS (ex: intempéries ou embouteillages généralisés) générant des pics d'écriture NoSQL.
- Perte momentanée de connectivité 4G/5G sur les terminaux embarqués des chauffeurs provoquant une arrivée différée par lots (burst).
- Accumulation de photos et signatures de livraison non archivées au fil des années risquant d'augmenter inutilement le coût S3.

RECOMMANDATIONS D'ARCHITECTURE

- Configurer le Target Tracking Auto Scaling ECS sur l'utilisation CPU (seuil 70%) pour étendre automatiquement la flotte de 6 à 12 tâches.
- Implémenter une file tampon locale ou un buffer Redis sur les conteneurs pour absorber les réémissions en rafale des terminaux 4G/5G.
- Maintenir la règle S3 Lifecycle stricte : transition vers S3 Glacier Flexible Retrieval à 60 jours, puis Glacier Deep Archive à 365 jours.
- Configurer des alertes de facturation AWS Budgets avec seuil préventif à 550 €/mois.

INFRASTRUCTURE AS CODE (TERRAFORM)

L'ensemble de cette infrastructure est automatisé et reproductible via le socle Terraform fourni dans le projet.

```
# Déploiement automatisé :  
cd terraform/  
terraform init  
terraform plan -out tfplan  
terraform apply tfplan
```

Document d'ingénierie généré par Cloud Architect Agent • Tous droits réservés © 2026