ESN.81
Ecole Supérieure du Numérique du Tarn

ÉTUDE DE CAS

Refonte sécurité et scalabilité d'un site e-commerce mondial

Par

Ronald PINA GUILLEN & Nicolas REDON

SOMMAIRE

Contexte

Globalshop

site e-commerce international

Elle réalise 200 000 visites / jour
pics à 2 millions durant les ventes flash
L’infrastructure actuelle AWS est mal architecturée.

Modelé de cloud

Cloud public

Services concernés

EC2 pour le front-end, sans Auto Scaling
RDS MySQL en instance unique
S3 avec un bucket devenu public par erreur

Données manipulées

Fiches produits, données clients/fournisseurs
données bancaires

Contraintes

RGPD

GlobalShop

Historique

- des pannes fréquentes
- un manque de scalabilité
- une fuite S3 médiatisée l’année dernière

GlobalShop

Infrastructure existante

EC2 front-end :sans Auto Scaling
RDS MySQL : en instance unique
S3 : bucket public
CloudFront : partiellement configuré
WAF : inexistant
IAM : comptes admin partagés
Github : secrets stockés dans les fichiers .env
CloudTrail,GuardDuty : désactivés
VPC : peu segmentée

GlobalShop

Architecture envisagée

1. **CloudFront (CDN mondial)**
2. **Application Load Balancer**
3. **Auto Scaling Group EC2 ou ECS Fargate**
4. **RDS Aurora MySQL (multi-AZ)**
5. **ElastiCache Redis**
6. **S3 privé + URL signées**
7. **Secrets Manager**
8. **VPC 3-tiers (public / private / database)**
9. **GuardDuty + Security Hub**
10. **CI/CD GitHub → CodeBuild → CodeDeploy**

GlobalShop

Contraintes de sécurité / performance

1. **Site monétisé → indisponibilité = pertes financières majeures**
2. **Données personnelles (RGPD)**
3. **Historique de fuite → risque réputationnel**
4. **Traçabilité obligatoire**
5. **Attaques DDoS fréquentes**
6. **Délai maximum d’interruption très faible**

Risques et niveau de criticité

Analyse des risques

Catégories	Risques	Description
Confidentialité	S3 avec un bucket devenu public par erreur, Secrets stockés dans les fichiers .env	configuration des permissions et mauvaise pratique de la gestion des fichiers importants
Disponibilité	pannes fréquentes	modele de déploiement non adaptés, diversification des modeles
Intégrité	Aucun WAF	aucune protection des API
Performance	manque de scalabilité	site e-commerce international , modele de déploiement mal adapté : des pics (ventes flash) , 200 000 ventes/jour.
IAM	comptes admin partagés	mauvaise configuration des permissions & rôles
Coûts(FinOps)	explosion des coûts AWS	Dépendance du fournisseur du service, obligation de s'adapter
Conformité	RGPD, fuite de données hors UE, fuites fréquentes	localisation des serveurs hors UE, non conformité RGPD

Niveau criticité

Proabability/ Menace	Faible	Moyen	Fort	Catastrophique
Tres probable		pannes fréquentes		
Probable			explosion des coûts	
Possible			manque de scalabilité, fuite données	stockage fichiers .env public aucun waf
Peu probable				S3 public par erreur, compte admin partagés
Improbable				

Proposition de mesures

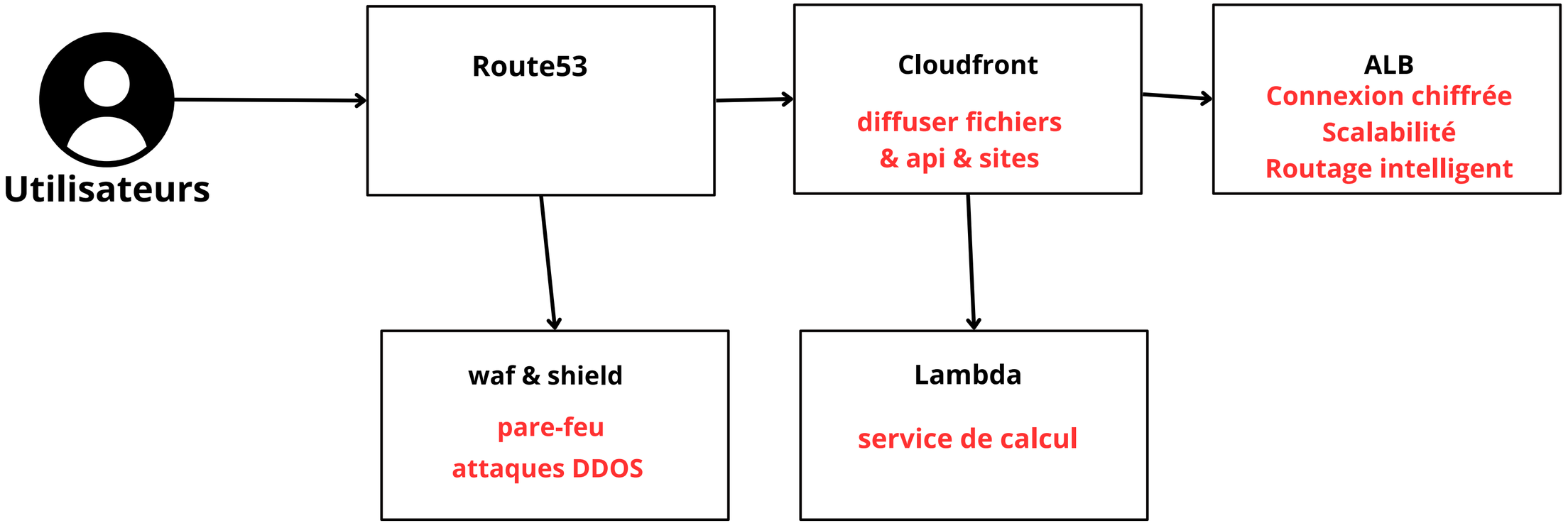
Mesures de préventive

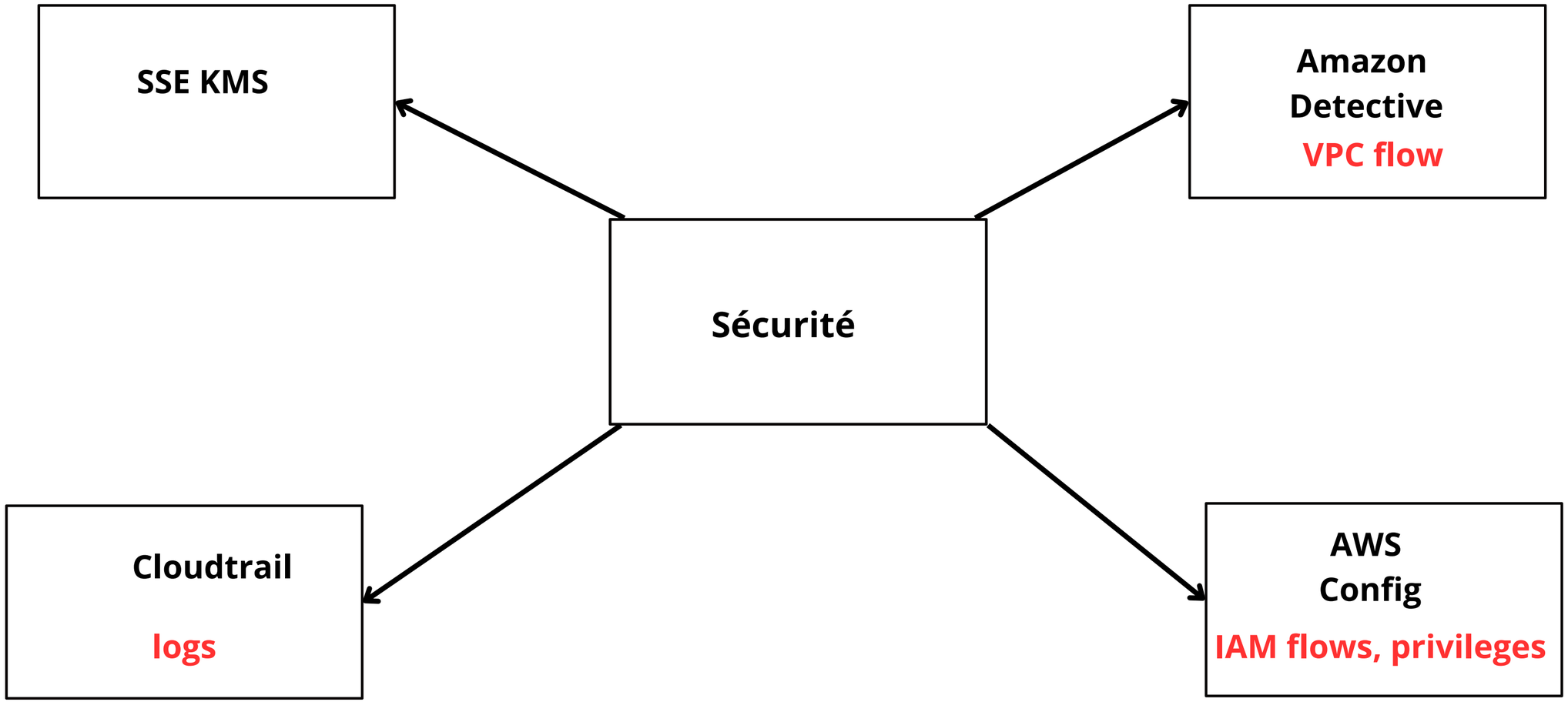
Risque	Mesure de prévention
S3 (Bucket) devenu public par erreur	- Activer Block Public Access au niveau du compte et des buckets
Secrets stockes dans les fichiers .env	- Stocker dans AWS Sectres Manager
Pannes frèquentes	- Auto Scaling - Health checks ALB
Aucun WAF	- Déployer le WAF sur CloudFront
Manque de scalabilité	- Utiliser du ECS (Elastic Container Service) Fargate ou EC2 - Utiliser du ElasticCache
Comptes admin partagés	- Suppression des comptes partagés - Utiliser IAM avec MFA
Explosion des coût AWS	- Analyser les coût + budget - Empêcher l'utilisation de services non utilisés
Fuite de données hors UE	- Configurer les services au régions EU
Fuites frèquentes	- CloudTrail + VPC Flow Logs centralises

Mesures de détection

Objectif	Mesure de détection
Détecter les accès suspects ou non autorisés	• AWS CloudTrail activé en multi-région • Alertes CloudWatch (API sensibles, IAM changes)
Identifier les comportements réseau anormaux	• VPC Flow Logs (trafic accept/refusé) • GuardDuty (détection IP malveillantes, port scans)
Détecter les fuites de données ou accès à des données sensibles	• Alertes sur accès anormal à des buckets S3 • WAF logs (extraction de données)
Surveiller la santé et les erreurs des applications	• Logs applicatifs dans CloudWatch • Dashboards + alarms
Détecter les dérives de configuration ou mauvaises pratiques	• AWS Config + Security Hub
Traçabilité obligatoire RGPD	• CloudTrail immuable dans S3 (Object Lock)• Centralisation logs dans un “Log Account”

Schéma archi AWS


Utilisateurs
Route53
Cloudfront
diffuser fichiers
& api & sites
ALB
Connexion chiffrée
Scalabilité
Routage intelligent
waf & shield
pare-feu
attaques DDOS
Lambda
service de calcul


SSE KMS
Amazon
Detective
VPC flow
Sécurité
Cloudtrail
logs
AWS
Config
IAM flows, privileges

Stratégie IAM Zero

Stratégies	Explications
Donner le minimum de permissions	Chaque utilisateur n’a que les accès nécessaires, pas plus.
Utiliser des rôles IAM (pas des utilisateurs)	Privilégier des identifiants temporaires au lieu de clés fixes.
Activer la MFA partout	MFA obligatoire pour tous les comptes, surtout administrateurs.
Séparer les rôles (Dev / Ops / Sec)	Éviter un super-admin ; chacun a son rôle séparé.
Ne jamais faire confiance par défaut	Toute action doit être explicitement autorisée.
Utiliser des conditions d’accès	Ex : accès seulement avec MFA, IP spécifique, appareil répondant aux règles.
Supprimer/mettre à jour les permissions inutilisées	Nettoyer régulièrement, tourner les clés si nécessaire.
Surveiller l’activité IAM	CloudTrail + IAM Access Analyzer pour détecter anomalies et permissions risquées.
Protéger le compte root	À n’utiliser presque jamais. Toujours MFA et mot de passe très fort.

Plan DevSecOps

Catégorie	Mesures DevSecOps
1. Sécurité intégrée au CI/CD	- Scans automatiques à chaque commit - Pipelines GitHub, CodeBuild avec étapes sécurité intégrées
2. Scans Automatisés – Code & Dépendances	**- SAST** : scan du code (GitHub Security) **- SCA** : scan des dépendances (CVE critiques)
3. Sécurité AWS Continue	- IAM Access Analyzer : permissions trop larges - GuardDuty : détection IP malveillantes / anomalies - CloudTrail activé en continu
4. Alertes & Monitoring	- Alertes CloudWatch : accès suspects, erreurs applicatives
5. Automatisation des corrections	- Patching automatique via AWS Systems Manager - Dependabot / Renovate pour libs vulnérables - Remédiation auto (ex : S3 public → privé)
6. Tests de sécurité	- Pentests réguliers - Tests de charge et résilience
7. Culture DevSecOps	- Formations régulières - Revues de code sécurité - Checklists sécurité avant déploiement

RTO & RPO

RTO (Temps de Reprise)

L'objectif doit être de reprendre l'activité avant même que l'utilisateur ne se rende compte de la panne.
Cible : 0 à 5 minutes

RPO (Point de Reprise)

Chaque panne est une opportunité de perdre des commandes ou des données client.
Cible : 0 à 10 secondes

ANALYSE :

se rapprocher de 0

fréquentes pannes **=> affecte l’image, médiatisation**
coûts importants essentiels vu le nombre de ventes réalisées (CA 200k/jour)

réponse à incident en cas de nouvelle fuite S3 (procédure attendue).

Phase	Objectif	Actions
Identification et recherche de la fuite	**Détecter et comprendre la fuite.**	Analyse de journaux des logs (S3, CloudTrail) : Identifier la source, l'utilisateur et le périmètre des données touchées.
Isolation	**Arrêter immédiatement la fuite.**	Révoquer les accès compromis, désactiver les clés
Suppression	**Supprimer la cause racine.**	Mettre à jour les systèmes, corriger la mauvaise configuration, éliminer les portes dérobées.
Rétablissement	**Retour à la normale en toute sécurité.**	Vérifier la fonctionnalité, s'assurer que la vulnérabilité a disparu, renforcer la surveillance.
Communication	**Informer les parties prenantes.**	Communiquer en interne une fois l'incident identifié. Notifier les autorités (ex. CNIL) si des données personnelles

Conclusion

La refonte de l’architecture AWS de GlobalShop, combinée à une approche DevSecOps et une stratégie IAM Zero Trust, une optimisation des coût,renforcer la sécurité afin d'éviter une nouvelle fuite, permet de répondre à tous les enjeux critiques de l’entreprise :

- Haute disponibilité et scalabilité grâce à CloudFront, ALB et les service de scaling comme ElasticCache.
- Sécurité renforcée : S3 privé, gestion centralisée des secrets, WAF et GuardDuty.
- Traçabilité et conformité RGPD via CloudTrail, VPC Flow Logs et centralisation des logs.
- Détection et prévention des incidents automatisées avec alertes CloudWatch et remédiation automatique.
- Culture DevSecOps intégrée au cycle CI/CD avec scans, tests et formation continue.
- Optimisation des coûts (FinOps) grâce à des bonnes pratiques sur le scaling, S3, NAT Gateway et Reserved Instances.

Annexes

DevSecOps : Anchore, About.gitlab, OpsMx