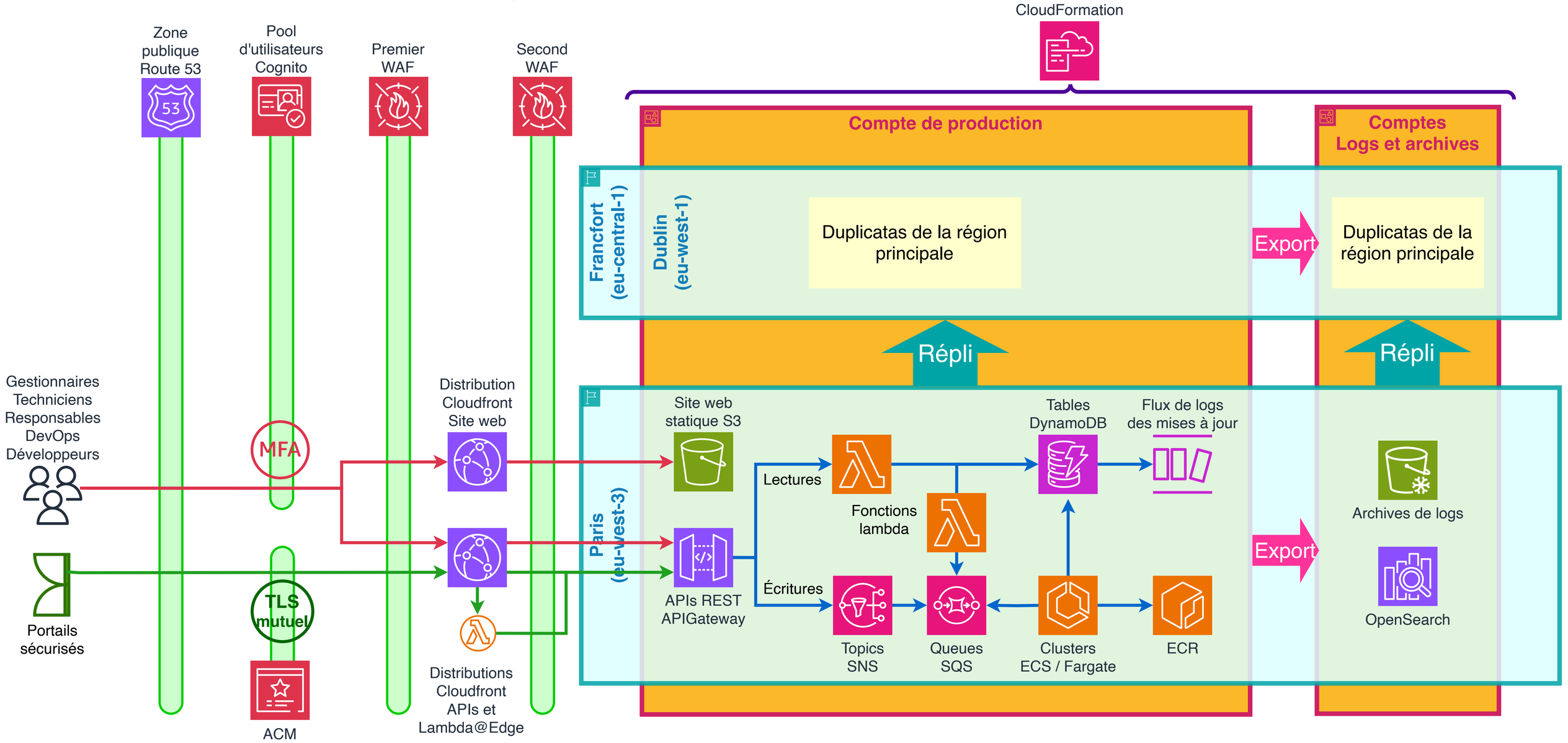
AccessGranted

Sécurise les accès à votre domicile

Présentation générale

- J’ai imaginé un projet que j’ai nommé « AccessGranted » pour une société du type PME et qui porte le même nom.
- AccessGranted permet un accès sécurisé et exclusif aux parkings des résidents d’immeubles.
- Pour pouvoir établir un cadre bien architecturé qui répond aux besoin du client (imaginé), je me suis basée prioritairement sur les piliers **Security** et **Reliability**.
- Les **services serverless** d’AWS y ont été privilégiés, ainsi réduisant les coûts opérationnels et optimisant les frais de maintenance.
- L’architecture reste valide en cas d’expansion du business.

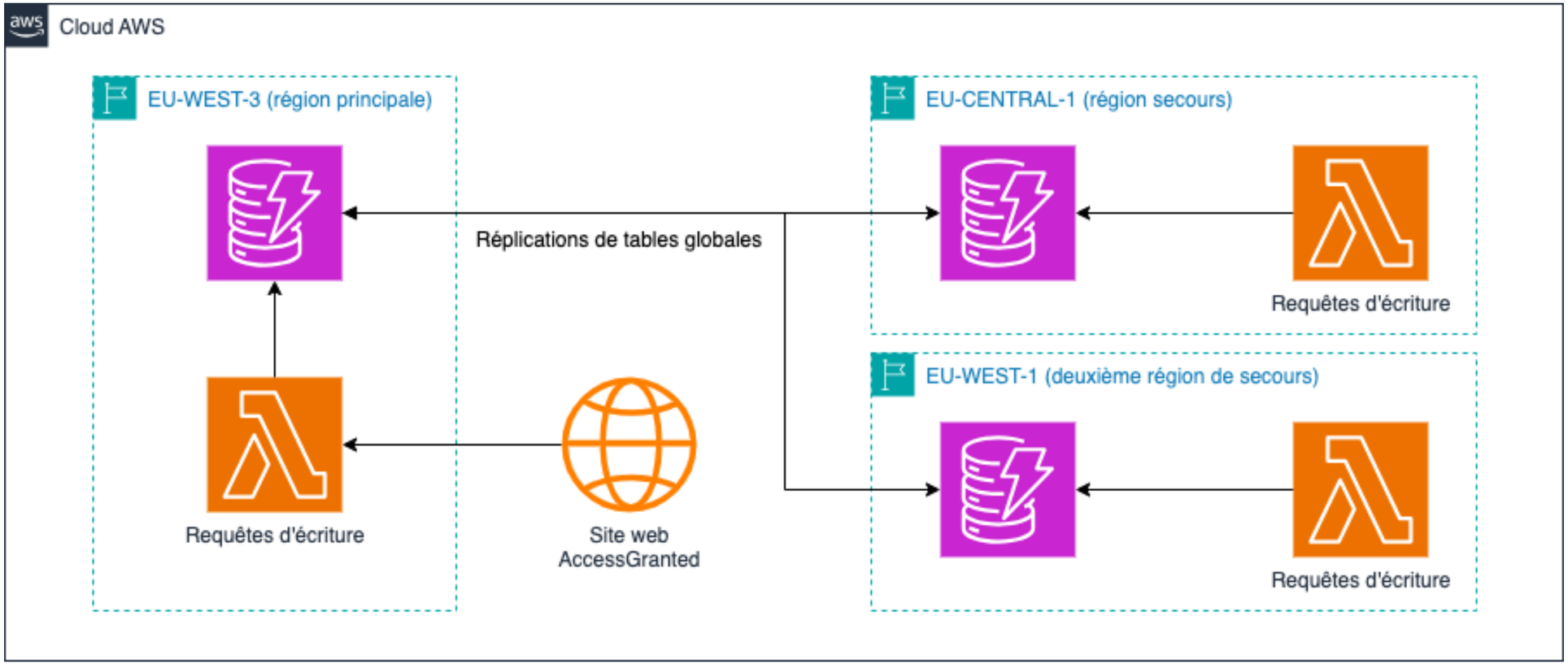
Présentation générale



Haute Disponibilité

DynamoDB

Réplication active active sur 3 régions



DynamoDB

Tables globales

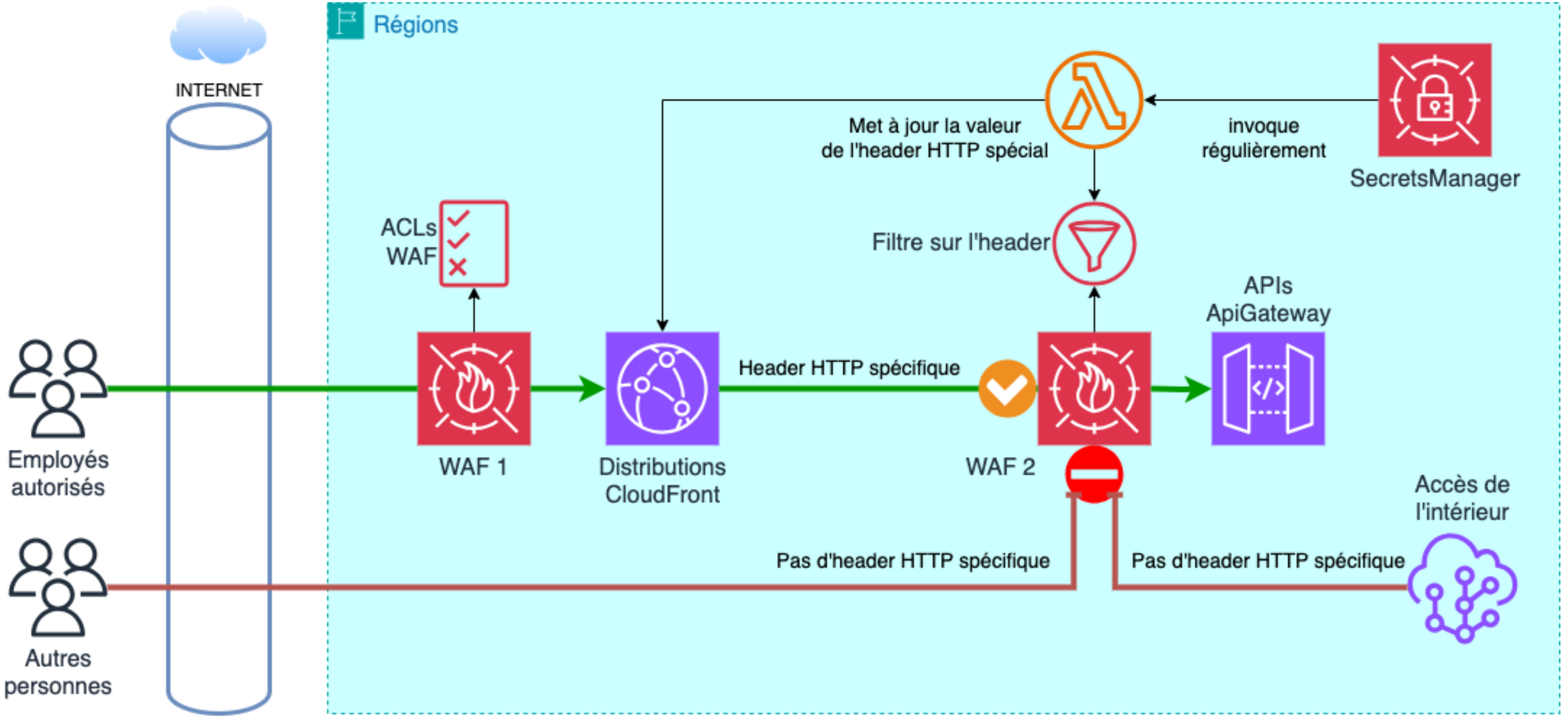
- Lorsque les utilisateurs changent les données (ex. l'enregistrement d'une nouvelle télécommande), ces modifications sont répliquées automatiquement en temps réel dans les régions de secours.
- La distribution globale de cette base de données (table globale) à travers plusieurs régions permet non seulement la réplication multi-active (évoquée plus haut), mais aussi la tolérance aux pannes régionales.
- Pour accessgranted.com, en cas de sinistre, elle redevient disponible pratiquement instantanément (haute dispo à 99.999%).

Sécurité renforcée

Securité renforcée pour les requêtes web

Double WAF combiné avec Secrets Manager

- Avant d'arriver aux APIs AccessGranted, les requêtes doivent passer par deux WAFs.
  - Le premier WAF (déployé sur CloudFront) place un entête HTTP spécifique avec une valeur secrète.
  - Le deuxième WAF (déployé sur API Gateway) n'autorise l'accès que s'il y a l'entête du premier WAF avec la valeur secrète.
- Secrets Manager est mis en place avec une fonction Lambda qui change la valeur secrète de l'entête HTTP spécifique périodiquement.
- Il est impossible d'accéder aux APIs sans passer par le premier WAF, qu'on essaie d'Internet ou d'AWS.


Régions
INTERNET
Met à jour la valeur
de l'header HTTP spécial
invoque
régulièrement
SecretsManager
ACLs
WAF
Filtre sur l'header
APIs
ApiGateway
Header HTTP spécifique
Employés
autorisés
WAF 1
Distributions
CloudFront
WAF 2
Accès de
l'intérieur
Pas d'header HTTP spécifique
Pas d'header HTTP spécifique
Autres
personnes

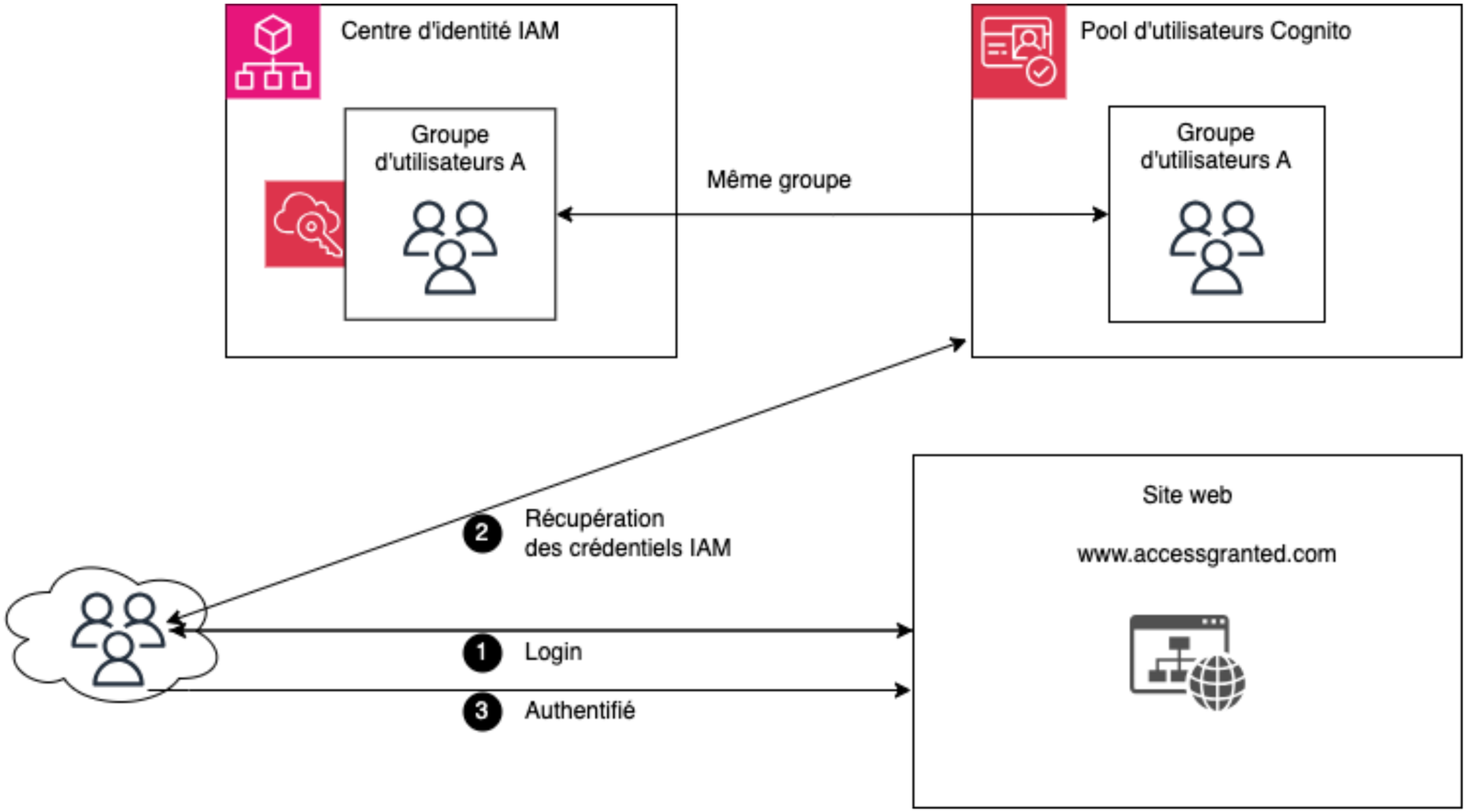
Securité renforcée de l’API d’AccessGranted

Authentification avec AWS Cognito (avec MFA)

- Les utilisateurs qui peuvent être autorisés pour accéder au site sont les employés de la société AccessGranted.
- Lorsque les utilisateurs se connectent au site, leur authentification passe par AWS Cognito (avec MFA) qui agit en tant que fournisseur d’identité.
- Le token (temporaire) émis par AWS Cognito permet l’autorisation d’accès au site de l’appli. Il contient aussi leurs identifiants enregistrés dans le Centre d’Identité IAM qui, lui, agit en tant que source d’identité.
- Les utilisateurs sont autorisés à accéder au site accessgranted.com et s’y retrouvent avec leurs permissions « Least Privilege » définies auparavant dans le Centre d’Identité IAM.

Securité renforcée de l’API d’AccessGranted

Cognito et centre d’identité IAM



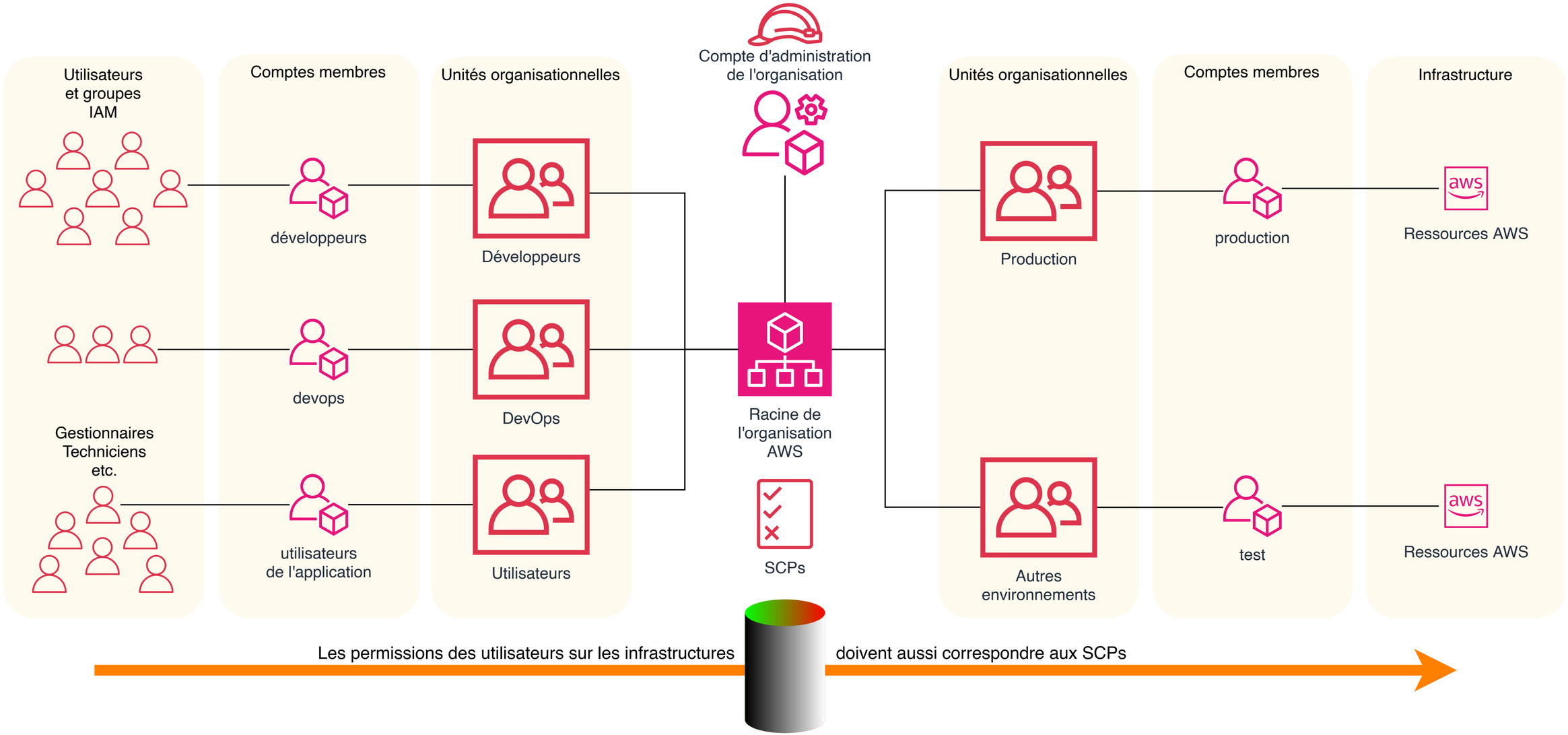
Securité renforcée de l’API d’AccessGranted

Authentification des portails par TLS mutuel

- Chaque portail a son certificat émis par AWS ACM.
- Une fonction Lambda@Edge est utilisée pour requêter une API avec le mTLS activé pour que seuls les certificats enregistrés soient autorisés.
- Les certificats ont une durée de vie très limitée et les portails en reçoivent un nouveau tous les mois.

AWS Organisations

ORGANISATIONS



ORGANISATIONS

- La solution AccessGranted utilise à la base **aws organizations**, service clé pour la gestion des accès aux différents environnements de l'infrastructure (dev, test, prod, gestion etc.) où le principe "least privilege" est appliqué.

- La gestion centralisée de l'infrastructure est constituée de différentes unités organisationnelles (les OU), comptes des employés aux rôles et permissions différents et CloudFormation StackSets.

- Le déploiement des ressources se fait d'une manière sécurisé (grâce aux polices basées sur l'identité, SCP, IAM Roles, tags, etc.), ainsi que leurs accès à d'autres services aws. Le principe "least privilege" y est fortement recommandé pour ne donner aux utilisateurs IAM (les développeurs, gestionnaires, techniciens) que les droits nécessaires pour accomplir leurs tâches.

ORGANISATIONS

Optimisation des coûts

- Partage des ressources à travers les comptes via RAM (Resource Access Manager)
- Une seule facture pour les dépenses effectuées (**consolidated billing**).
- D’autres tâches administratives (ex.création et gestion d’autre comptes membres) se font à partir du compte de gestion de l’unité organisationnelle racine.
- Surveillance et seuils budgétaires / des coûts avec AWS Budgets, Cost Explorer, AWS Compute Optimizer.

Plan de reprise d’activité

PRA Pilot Light

RPO - en-dessous d’une minute, RTO - minutes

- Comme les tables globales DynamoDB sont conçues pour se remettre automatiquement (réplication multi-active et tolérance aux pannes multi-régionales inclues), il n’y a besoin d’aucune configuration.
- Dans les régions de secours, via CloudFormation, un cluster ECS est créé avec ses tâches et définitions de services réduites à 0 et les autres ressources nécessaires comme le réseau.
- Des réplications cross-région sont en place pour les données statiques et les logs. Les données répliquées sont chiffrées en transit et au repos.
- Les environnement de secours sont testés régulièrement pour leur assurer les dernières mises à jour et améliorations pour une bascule douce en cas d’incident.