Résumé Module 5 - GC Infrastructure: Core Services

IAM (Identity and Access Management)

Principe de base

IAM permet de définir qui peut faire quoi sur quelles ressources dans Google Cloud. C'est le système central de sécurité qui contrôle tous les accès.

Hiérarchie des ressources

L'organisation suit une structure en arbre :

- **Organization** : Le niveau racine qui représente la société
- **Folders** : Souvent utilisés pour les départements (chaque dept. un dossier)
- **Projects** : Regroupent les ressources qui partagent la même confiance
- **Resources** : Les services concrets comme Compute Engine, Cloud Storage

Types de rôles

Il existe trois catégories de rôles :

- **Basic roles** : Owner, Editor, Viewer et Billing Administrator
- **Predefined roles** : Ce sont des rôle spécifiques à chaque service Google Cloud
- **Custom roles** : Permettent de définir des permissions précises (plus fines)

Service Accounts

Ces comptes permettent aux applications d'accéder aux ressources Google Cloud sans intervention humaine. Ils sont identifiés par une adresse email et permettent l'authentification service-à-service.

Services de stockage et bases de données

Cloud Storage

Service de stockage pour les fichiers binaires comme les images, vidéos, sauvegardes. Il propose quatre storage classes :

- **Standard** : Accès fréquent, pas de durée minimum
- **Nearline** : Accès mensuel, 30 jours minimum
- **Coldline** : Accès trimestriel, 90 jours minimum
- **Archive** : Accès annuel, 365 jours minimum

Services de bases de données

- **Cloud SQL** : Base de données relationnelle managée (MySQL, PostgreSQL, SQL Server)
- **Spanner** : Base de données relationnelle distribuée avec cohérence forte
- **AlloyDB** : PostgreSQL optimisé pour les workloads hybrides transactionnels/analytiques
- **Firestore** : Base NoSQL pour applications mobiles et web
- **Bigtable** : Base NoSQL pour gros volumes avec latence sub-millisecondes
- **Memorystore** : Service Redis/Memcached en mémoire

Resource Management

Quotas

Les quotas limitent la consommation des ressources pour éviter les coûts imprévus et forcer une réflexion sur le dimensionnement. Ils s'appliquent par project, par région et définissent des limites sur le nombre de ressources et la vitesse des requêtes API.

Labels et billing

Les labels permettent d'organiser les ressources par équipe, environnement ou centre de coût. Ils sont essentiels pour optimiser les coûts en exportant les données de billing vers BigQuery pour analyse.

Budgets et alertes

On peut configurer des budgets avec des alertes email quand les dépenses approchent certains seuils. Les données peuvent être analysées avec Looker Studio pour créer des dashboards.

Monitoring et observabilité

Google Cloud Observability

C’est une plateforme intégrée qui combine logging, monitoring, error reporting, tracing et profiling. Elle fonctionne avec Google Cloud mais aussi AWS et les environnements on-premise.

Monitoring

Il permet de surveiller les metrics des plateformes, systèmes et applications. On peut créer des custom dashboards et des alerting policies. Les uptime checks testent la disponibilité des services publics.

Quelques autres outils

- **Logging** : Collecte et analyse des logs avec rétention 30 jours
- **Error Reporting** : Agrège et affiche les erreurs des services
- **Tracing** : Système de tracing distribué pour analyser la latence
- **Profiling** : Analyse les performances des fonctions CPU/mémoire intensives