

Résumé module 4 - GC Infrastructure: Foundation

Introduction aux services

- **IaaS** (Infrastructure as a Service) : On gère les ressources de base comme les CPUs, mémoire, disques, etc.
- **PaaS** (Platform as a Service) : On gère les serveurs et clusters
- **SaaS** (Software as a Service) : Solutions serverless qui s'adaptent automatiquement

Principaux services

Compute Engine permet de créer des machines virtuelles quand on en a besoin. C'est la solution IaaS de base pour contrôler complètement l'infrastructure.

Google Kubernetes Engine (GKE) aide à faire tourner des applications conteneurisées dans un environnement que Google gère mais qu'on contrôle.

App Engine est une plateforme entièrement gérée (PaaS) qui permet de faire tourner du code sans se préoccuper de l'infrastructure.

Cloud Functions offre un environnement complètement serverless pour exécuter du code quand des événements se produisent.

Cloud Run permet de faire tourner des conteneurs stateless via des requêtes web ou des événements Pub/Sub, avec un scaling automatique très rapide.

Interaction avec Google Cloud

Il y a quatre façons d'interagir avec Google Cloud :

- Console web Google Cloud
- Cloud Shell et CLI
- API REST
- Application mobile

Le **Cloud Shell** donne un accès en ligne de commande à une VM temporaire avec 5GB de stockage persistant et une autorisation intégrée.

Réseaux virtuels (VPC)

Structure des réseaux

Les **projets** lient les objets aux facturations et peuvent contenir jusqu'à 15 réseaux. Les **réseaux** sont globaux et couvrent toutes les régions disponibles. Ils contiennent des **sous-réseaux** qui marchent à l'échelle régionale.

Et il existe trois types de réseaux :

- **Default** : Un sous-réseau par région avec règles de firewall par défaut
- **Auto Mode** : Allocation IP automatique avec masque /20 par région, qu'on peut étendre jusqu'à /16
- **Custom Mode** : Contrôle total des plages IP donc pas de sous-réseaux créés par défaut

Adresses IP

Les **adresses IP internes** sont données par DHCP avec un bail renouvelé toutes les 24h. Les **adresses IP externes** peuvent être temporaires (depuis un pool) ou fixes (réservées).

La résolution DNS interne utilise le format : *[hostname].[zone].c.[project-id].internal*

Routes et Firewall

Les **routes** font correspondre des plages IP vers des destinations. Les **règles de firewall** protègent les instances des connexions non autorisées. Elles s'appliquent au niveau du réseau mais agissent au niveau des instances. Par défaut, tout le trafic entrant est bloqué et tout le trafic sortant est autorisé.

Machines virtuelles

Options

Les types de machines sont organisés en familles :

- **General-purpose** : E2 (coût optimisé), N2/N2D/N1 (équilibré), Tau T2D/T2A (mise à l'échelle optimisée)
- **Compute-optimized** : C2/C2D/H3 pour les charges haute performance
- **Memory-optimized** : M1/M2 pour les bases de données en mémoire
- **Accelerator-optimized** : A2/G2 pour le ML et la visualisation

Tarification

La facturation se fait à la seconde avec un minimum d'une minute. Les remises incluent :

- Utilisation soutenue (automatique)
- Engagement d'utilisation
- Instances préemptibles (jusqu'à 91% de réduction)

Configurations spéciales

Les **instances préemptibles** offrent des prix réduits mais peuvent être interrompues à tout moment avec 24h maximum d'exécution.

Les **Shielded VMs** offrent une intégrité vérifiable avec Secure Boot et monitoring d'intégrité.

Les **Confidential VMs** chiffrent les données pendant leur traitement.

Stockage

Disques persistants

Ils sont attachés via l'interface réseau et survivent à l'arrêt de la VM. Ils offrent des snapshots incrémentaux et peuvent être redimensionnés même en cours d'exécution.

Disques SSD locaux

Attachés physiquement à la VM, ils offrent de meilleures performances mais les données sont perdues à l'arrêt de l'instance.

Snapshots

Ils permettent de sauvegarder les données importantes dans Cloud Storage de manière incrémentale. On peut les utiliser pour migrer des données entre zones ou améliorer les performances en passant d'un HDD à un SSD.