

# GLG105: Génie logiciel

November 24, 2025  
Jacopo Bufalino (CNAM)

# Introduction



# Contenu du module

Ce module se concentrera sur les aspects **réseau et sécurité** du cloud computing (principalement) du point de vue de l'utilisateur cloud :

- Sécurité et réseau Linux
- Virtualisation et conteneurisation
- Réseau cloud
- Chaîne d'approvisionnement logicielle

# Objectifs d'apprentissage

- Comprendre les principaux concepts du cloud computing
- Déployer des applications sur le cloud
- Comprendre les concepts clés de la sécurité de la chaîne d'approvisionnement
- Travailler avec les pipelines CI/CD

# Prérequis

Connaissances de base de :

- Linux et son noyau
- Réseau
- Git et contrôle de version

**Nous couvrirons quand même les bases dans ce cours**

# Organisation du cours

## Informations pratiques

Nous aurons une session de TP par leçon. Il y aura un mélange de tutoriels et d'exercices notés.

Les TPs seront disponibles à: <https://glg105.jackops.dev>

Les diapositives de cours et les annonces seront publiées sur Moodle.

La date limite de chaque TP sera annoncée après la date de publication (généralement une semaine).

# Le cloud



# Définitions

**Il y a beaucoup de sites web et d'applications fonctionnant dans le cloud. Mais qu'est-ce que c'est exactement ?**

- Logiciels, infrastructures et plateformes fonctionnant à la demande
- Instances et services gérés
- Provisionnement, mise à l'échelle et réplication automatiques
- L'ordinateur de quelqu'un d'autre

**Il existe différents types de cloud**

- Cloud public : Services fournis par des fournisseurs tiers
- Cloud privé : Infrastructure cloud auto-hébergée
- Cloud hybride : Combinaison de cloud public et privé



# Pourquoi choisir le cloud ?

- **Évolutivité** : Mise à l'échelle automatique des ressources.
- **Efficacité des coûts** : Payer uniquement pour ce que vous utilisez.
- **Accessibilité** : Accéder aux services et données depuis n'importe où.
- **Maintenance** : Les fournisseurs cloud gèrent la maintenance.
- **Reprise après sinistre** : Options de redondance et de sauvegarde intégrées pour la protection des données.
- **API First** : La communication avec le cloud est possible via des API, ce qui facilite la gestion des ressources.

## Les startups et petites entreprises bénéficient aussi du cloud

La maintenance et les connaissances du domaine permettent aux petites équipes de développement de déployer et gérer facilement des applications complexes.

# Différents paradigmes de cloud computing

- **Infrastructure as a Service (IaaS) :**
  - ▶ Fournit des ressources informatiques virtualisées via Internet.
  - ▶ Les utilisateurs gèrent les systèmes d'exploitation, les applications et les données.
- **Platform as a Service (PaaS) :**
  - ▶ Fournit une plateforme permettant aux clients de développer, exécuter et gérer des applications.
  - ▶ Les utilisateurs gèrent les applications et les données, tandis que le fournisseur gère l'infrastructure.
- **Software as a Service (SaaS) :**
  - ▶ Fournit des applications logicielles via Internet sur la base d'un abonnement.
  - ▶ Les utilisateurs accèdent au logiciel via un navigateur web, le fournisseur gérant l'infrastructure et la plateforme.

# Exemples de paradigmes de cloud computing



# Réplication et virtualisation



# Régions et zones de disponibilité

- **Régions** : Zones géographiques contenant plusieurs zones de disponibilité. Chaque région est isolée pour garantir la souveraineté et la conformité des données. Il existe plusieurs régions en Europe.
- **Zones de disponibilité (AZ)** : Groupes de centres de données physiquement séparés au sein d'une région.

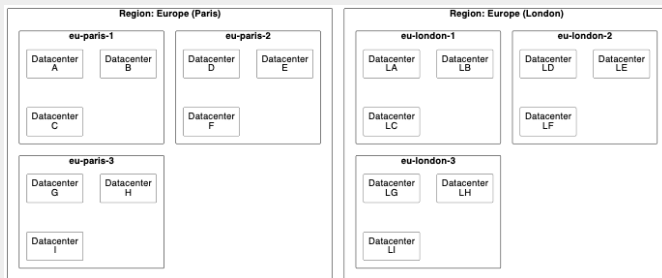


Figure: Régions et zones de disponibilité

# Importance des régions et zones de disponibilité

- **Haute disponibilité** : Garantit que les applications restent disponibles même si une zone tombe en panne.
- **Reprise après sinistre** : Fournit un mécanisme pour récupérer après des catastrophes naturelles ou techniques en répliquant les données entre les zones.
- **Faible latence** : Améliore les performances en permettant aux utilisateurs de se connecter à la région la plus proche.
- **Conformité** : Aide à respecter les exigences réglementaires en stockant les données dans des emplacements géographiques spécifiques (HIPAA, RGPD)

## Il suffit généralement de répliquer sur différentes AZ

Les logiciels critiques peuvent également être répliqués entre régions (plus coûteux)

## Les applications et services cloud fonctionnent dans des environnements virtualisés

- Machines virtuelles (VM)
  - ▶ Virtualisation complète du système d'exploitation
  - ▶ Noyau individuel
- Conteneurs :
  - ▶ Processus isolés légers
  - ▶ Même architecture que l'hôte
  - ▶ Même noyau que l'hôte
  - ▶ Plus faciles à gérer que les VM

# Virtualisation

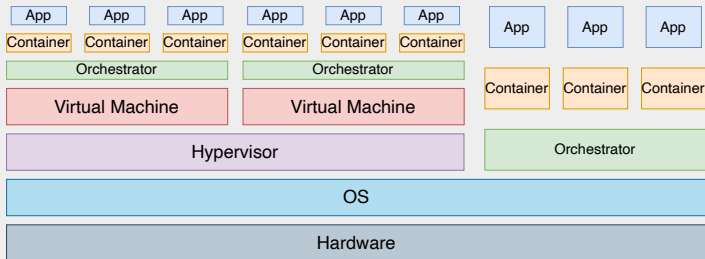


Figure: Pile de virtualisation



# Sécurité cloud - introduction



# Sécurité cloud

## La sécurité est une préoccupation majeure dans le cloud

- 81% des organisations ont connu un incident de sécurité lié au cloud en 2023
- 52% des organisations ont subi une perte de données dans le cloud en raison d'une mauvaise configuration en 2021
- Les incidents de sécurité cloud ont entraîné une perte financière moyenne de 263 000 \$ par incident

## La surface d'attaque du cloud est importante

- Nombreuses couches de virtualisation
  - ▶ Chaque couche peut être ciblée par les attaquants
- Composants en interaction
- Responsabilité peu claire

# Sécurité cloud - aperçu

Il existe de nombreux types de contrôles de sécurité dans le cloud.



IAM



Logs



Firewall



System  
security



PKI



Incident  
Response



IDS

**Pas seulement la sécurité, la conformité est également importante**

# Modèle de responsabilité partagée

Le fournisseur cloud et l'utilisateur partagent la responsabilité de la sécurité. **Dépend des paradigmes de cloud computing (Orange est la responsabilité du cloud)**

