IAAS

Fondations

Loïc Rouquette
EPITA - Laboratoire de Recherche de l'EPITA (LRE)
22 mars 2026

Sommaire

Organisation

Répartition des heures

- CM : 2 × 3h + 2h
- TP : 4 × 3h

Objectifs de la séance

- **Distinguer** les caractéristiques fondamentales d'une solution d'hébergement locale (on-premises) et d'une solution mutualisée (cloud) (AAV 4).
- **Différencier** les principaux modèles de service cloud : IaaS, PaaS (Platform as a Service) et SaaS (Software as a Service).
- **Identifier** et décrire les rôles des composants majeurs d'une infrastructure IaaS : machines virtuelles (VM), stockage (Bloc et Objet), réseau virtuel et mécanismes de sécurité de base (AAV 1).
- **Comprendre** les principes fondamentaux de l'estimation des besoins en ressources pour un service (AAV 2).
- **Connaître** l'environnement technique qui sera utilisé lors des travaux pratiques (TP).

01

Introduction aux modèles d'hébergement

Qu'est ce que l'hebergement d'applications ?

Définition

L'hébergement cloud fournit des ressources sur Internet en utilisant l'infrastructure d'un fournisseur de cloud. Cette infrastructure exploite la virtualisation pour abstraire un serveur physique et répartir les ressources sur un réseau de serveurs virtuels et physiques, ceux-ci étant généralement répartis dans plusieurs datacenters. L'hébergement cloud diffère de l'hébergement traditionnel, dans la mesure où ce dernier repose uniquement sur des machines physiques sur site (ou « on-premises »).
— OVH.com

Qu'est ce que l'hebergement d'applications ?

On-Premises (local)

Propriété et Contrôle Total

- L'entreprise possède matériel (serveurs, réseau...) et licences logicielles.
- Maîtrise complète de la configuration, sécurité, données, technologies.
- Avantage pour secteurs réglementés ou à haute confidentialité.

Qu'est ce que l'hebergement d'applications ?

On-Premises (local)

Propriété et Contrôle Total

- L'entreprise possède matériel (serveurs, réseau...) et licences logicielles.
- Maîtrise complète de la configuration, sécurité, données, technologies.
- Avantage pour secteurs réglementés ou à haute confidentialité.

Responsabilité Totale

- Gestion intégrale : Achat, installation, configuration, maintenance, mises à jour, sécurité, surveillance, alimentation, refroidissement, pannes.
- *Nécessite une expertise technique interne significative.*

Qu'est ce que l'hebergement d'applications ?

On-Premises (local)

Propriété et Contrôle Total

- L'entreprise possède matériel (serveurs, réseau...) et licences logicielles.
- Maîtrise complète de la configuration, sécurité, données, technologies.
- Avantage pour secteurs réglementés ou à haute confidentialité.

Responsabilité Totale

- Gestion intégrale : Achat, installation, configuration, maintenance, mises à jour, sécurité, surveillance, alimentation, refroidissement, pannes.
- *Nécessite une expertise technique interne significative.*

Modèle financier : CapEx dominant

- Fortes dépenses d'investissement initiales (Capital Expenditures).
- Coûts amortis sur plusieurs années.
- OpEx (électricité, personnel) existent mais l'investissement initial prédomine.

Qu'est ce que l'hebergement d'applications ?

On-Premises (local)

Inconvénients Associés

- Manque de Flexibilité / Agilité : Scaling lent (achat/installation de matériel).
- Planification de Capacité Complexe : Risque de sur-provisionnement (coûteux) ou sous-provisionnement (performance dégradée).
- Obsolescence Technologique : Risque à gérer par l'entreprise.
- Coûts Cachés : Pannes, maintenance imprévue, mises à niveau.

Qu'est ce que l'hebergement d'applications ?

Cloud Computing (Mutualisée)

Location de Ressources

- Location de ressources virtualisées (calcul, stockage, réseau...) hébergées dans les datacenters du fournisseur.
- Pas d'achat ni de possession de matériel physique par le client.

Qu'est ce que l'hebergement d'applications ?

Cloud Computing (Mutualisée)

Location de Ressources

- Location de ressources virtualisées (calcul, stockage, réseau…) hébergées dans les datacenters du fournisseur.
- Pas d'achat ni de possession de matériel physique par le client.

Gestion Déléguée de l'Infrastructure Physique

- Le fournisseur cloud gère, maintient et sécurise l'infrastructure physique sous-jacente.
- Le client interagit via des interfaces logicielles (consoles, API).

Qu'est ce que l'hebergement d'applications ?

Cloud Computing (Mutualisée)

Location de Ressources

- Location de ressources virtualisées (calcul, stockage, réseau…) hébergées dans les datacenters du fournisseur.
- Pas d'achat ni de possession de matériel physique par le client.

Gestion Déléguée de l'Infrastructure Physique

- Le fournisseur cloud gère, maintient et sécurise l'infrastructure physique sous-jacente.
- Le client interagit via des interfaces logicielles (consoles, API).

Modèle Financier - OpEx Dominant

- Dépenses d'exploitation basées sur la consommation réelle (« pay-as-you-go ») ou abonnements.
- Élimine ou réduit fortement les investissements initiaux (CapEx).

Qu'est ce que l'hebergement d'applications ?

Cloud Computing (Mutualisée)

Élasticité et Scalabilité Rapides

- Ajustement rapide (souvent en minutes) des ressources (↑↓) pour s'adapter à la demande.
- Possibilité d'auto-scaling pour gérer les pics de charge automatiquement.
- Évite le surprovisionnement.

Qu'est ce que l'hebergement d'applications ?

Cloud Computing (Mutualisée)

Élasticité et Scalabilité Rapides

- Ajustement rapide (souvent en minutes) des ressources (↑↓) pour s'adapter à la demande.
- Possibilité d'auto-scaling pour gérer les pics de charge automatiquement.
- Évite le surprovisionnement.

Accès Réseau Étendu & Self-Service

- Ressources accessibles via le réseau (Internet) depuis n'importe où.
- Provisionnement des ressources par l'utilisateur via consoles web ou API.

Qu'est ce que l'hebergement d'applications ?

Cloud Computing (Mutualisée)

Élasticité et Scalabilité Rapides

- Ajustement rapide (souvent en minutes) des ressources (↑↓) pour s'adapter à la demande.
- Possibilité d'auto-scaling pour gérer les pics de charge automatiquement.
- Évite le surprovisionnement.

Accès Réseau Étendu & Self-Service

- Ressources accessibles via le réseau (Internet) depuis n'importe où.
- Provisionnement des ressources par l'utilisateur via consoles web ou API.

Service Mesuré

- Utilisation des ressources suivie et mesurée précisément.
- Facturation basée sur la consommation réelle.

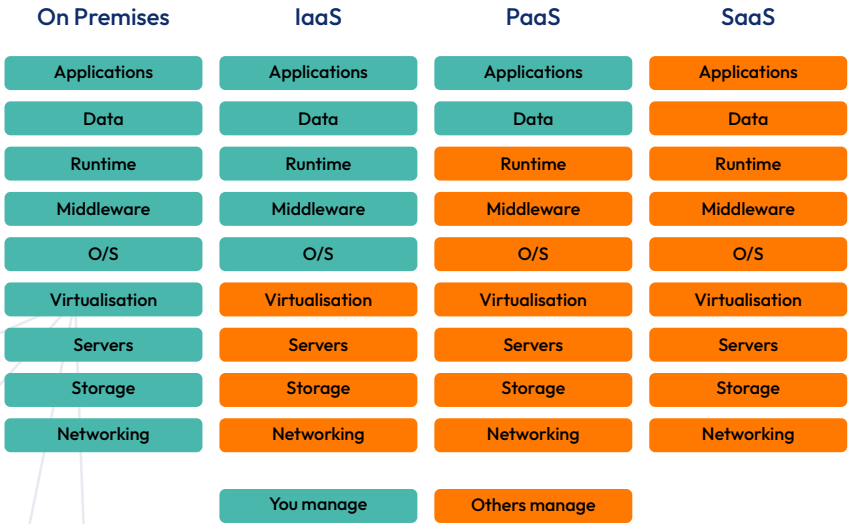
Modèle de Service Cloud : IaaS, PaaS, SaaS

Caractéristique	Infrastructure as a Service	Platform as a Service	Software as a Service
Description	Blocs de construction d'infrastructure IT virtualisée (calcul, stockage, réseau) à la demande.	Plateforme pour développer, déployer et gérer des applications sans gérer l'infrastructure.	Logiciel complet prêt à l'emploi, accessible via Internet sur abonnement.
Ce que vous gérez	Applications, Données, Middleware, Système d'exploitation.	Applications, Données.	Rien
Ce que le fournisseur gère	Virtualisation, Serveurs, Stockage, Réseau, Datacenter physique.	Tout ce que gère l'IaaS + Middleware, Système d'exploitation, Runime	Tout.
Niveau de contrôle	Élevé (sur l'OS et au dessus).	Moyen (sur les applications et les données).	Faible (limité aux fonctionnalités de l'application).

Modèle de Service Cloud : IaaS, PaaS, SaaS

Caractéristique	Infrastructure as a Service	Platform as a Service	Software as a Service
Flexibilité	Trés élevée (contrôle de l'infrastructure).	Moyenne (contraintes liées à la plateforme).	Faible (limité par les fonctionnalités du logiciel)
Cible utilisateur	Administrateurs système, Ingénieurs infrastructure, Architectes Cloud.	Développeurs d'applications, Équipe DevOps	Utilisateurs finaux, Entreprises (pour des fonctions métier spécifiques).
Exemples	AWS EC2, Azure Virtual Machine, Google Compute Engine, OVHcloud Public Cloud.	AWS Elastic Beanstack, Azure App Service, Google App Engine, Heroku.	Microsoft 365, Google Workspace, Salesforce, Slack, Dropbox

Récapitulatif



Pourquoi choisir une infrastructure mutualisée ?

Pourquoi choisir une infrastructure mutualisée ?

Modèle financier OpEx

- Évite les dépenses d'investissement initiales (CapEx).
- Coûts basés sur l'utilisation (dépenses opérationnelles - OpEx).

Pourquoi choisir une infrastructure mutualisée ?

Modèle financier OpEx

- Évite les dépenses d'investissement initiales (CapEx).
- Coûts basés sur l'utilisation (dépenses opérationnelles - OpEx).

Flexibilité et Scalabilité

- Ajustement rapide des ressources (CPU, RAM, stockage) à la hausse ou à la baisse.
- Adapte l'infrastructure aux besoins fluctuants.

Pourquoi choisir une infrastructure mutualisée ?

Modèle financier OpEx

- Évite les dépenses d'investissement initiales (CapEx).
- Coûts basés sur l'utilisation (dépenses opérationnelles - OpEx).

Flexibilité et Scalabilité

- Ajustement rapide des ressources (CPU, RAM, stockage) à la hausse ou à la baisse.
- Adapte l'infrastructure aux besoins fluctuants.

Déploiement rapide

- Provisionnement d'infrastructure en minutes/heures (vs jours/semaines on-premises).
- Accélère la mise sur le marché et l'innovation.

Pourquoi choisir une infrastructure mutualisée ?

Accès à une Infrastructure Globale

- Accès aux datacenters mondiaux du fournisseur.
- Permet de déployer au plus près des utilisateurs (faible latence).

Pourquoi choisir une infrastructure mutualisée ?

Accès à une Infrastructure Globale

- Accès aux datacenters mondiaux du fournisseur.
- Permet de déployer au plus près des utilisateurs (faible latence).

Réduction de la Charge de Maintenance

- Le fournisseur gère le matériel physique, les pannes, les mises à niveau, le datacenter.
- Libère les équipes IT pour des tâches à plus forte valeur ajoutée.

Pourquoi choisir une infrastructure mutualisée ?

Accès à une Infrastructure Globale

- Accès aux datacenters mondiaux du fournisseur.
- Permet de déployer au plus près des utilisateurs (faible latence).

Réduction de la Charge de Maintenance

- Le fournisseur gère le matériel physique, les pannes, les mises à niveau, le datacenter.
- Libère les équipes IT pour des tâches à plus forte valeur ajoutée.

Contrôle sur l'Environnement

- Contrôle direct sur l'OS, les logiciels installés, la configuration réseau.
- Idéal pour applications spécifiques ou migrations « legacy ».

Cas typiques d'utilisation de l'IaaS

- Hébergement de sites web et d'applications ;
- Environnements de Développement et de Test ;
- Stockage, Sauvegarde et Reprise après Sinistre (Disaster Recovery) ;
- Calcul Haute Performance (HPC) ;
- Analyse de Big Data ;
- Migration d'applications existantes ("Lift-and-Shift").

Comparaison Simplifiée : On-Premises vs Cloud

	On-Premises	Cloud IaaS
Avantages	- Contrôle total sur l'infrastructure et les données ; - Sécurité perçue comme maîtrisée (car interne).	- Faibles coûts initiaux (OpEx dominant) ; - Grande flexibilité et scalabilité à la demande ; - Déploiement rapide ; - Réduction de la charge de gestion de l'infra physique.
Inconvénients	- Coûts initiaux (CapEx) très élevés ; - Rigidité et lenteur pour s'adapter aux changements ; - Responsabilité totale de la gestion, maintenance et sécurité, risque de sur/sous-provisionnement.	- Dépendence vis-à-vis du fournisseur et de la connectivité Internet ; - Responsabilité partagée de la sécurité (nécesite une bonne configuration par le client) ; - Potentiels coûts imprévus si la consommation n'est pas maîtrisée, moins de contrôle direct sur le matériel physique.

02

Composants fondamentaux d'IaaS Compute & Storage

Virtualisation

Définition (Virtualisation)

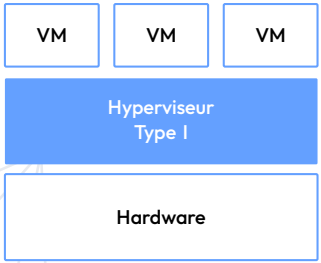
La virtualisation est une technologie permettant de créer des représentations virtuelles de ressources informatiques physiques. Plutôt que d'avoir un système d'exploitation directement installé sur un matériel serveur dédié, la virtualisation permet d'exécuter plusieurs systèmes d'exploitation et applications isolés les uns des autres sur une seule machine physique.

Virtualisation : Rôle de l'Hyperviseur

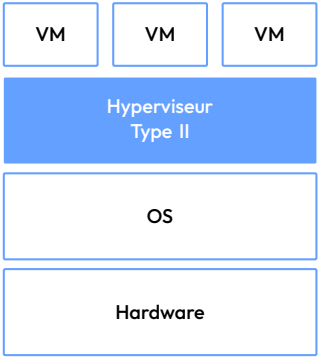
Définition (Hyperviseur)

Au cœur de la virtualisation se trouve l'hyperviseur, également appelé Moniteur de Machine Virtuelle (VMM – Virtual Machine Monitor). Il s'agit d'une couche logicielle (ou parfois matérielle/firmware) qui crée, gère et alloue les ressources matérielles physiques (CPU, mémoire, stockage, réseau) aux différentes machines virtuelles. L'hyperviseur est responsable de l'abstraction du matériel sous-jacent, permettant aux VMs de fonctionner comme si elles disposaient de leur propre matériel dédié.

Les deux types d'Hyperviseur



(a) Hyperviseur de Type I.

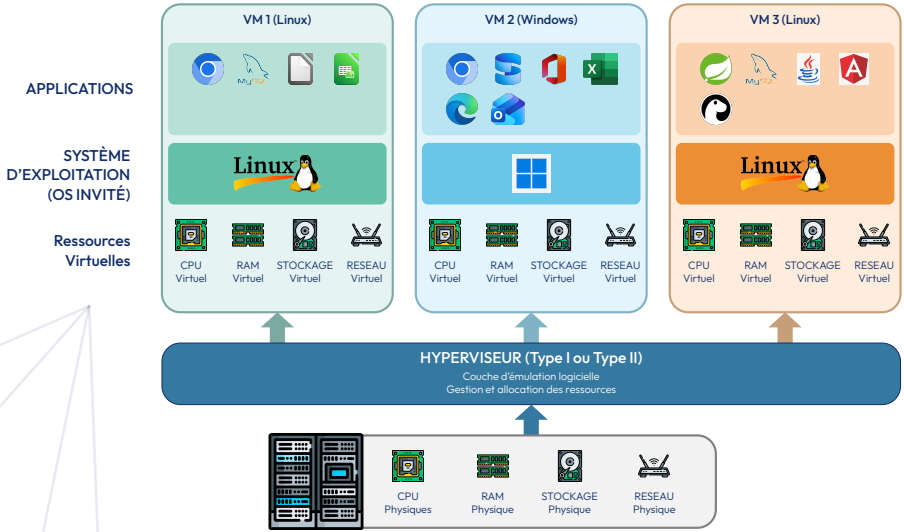


(b) Hyperviseur de Type II.

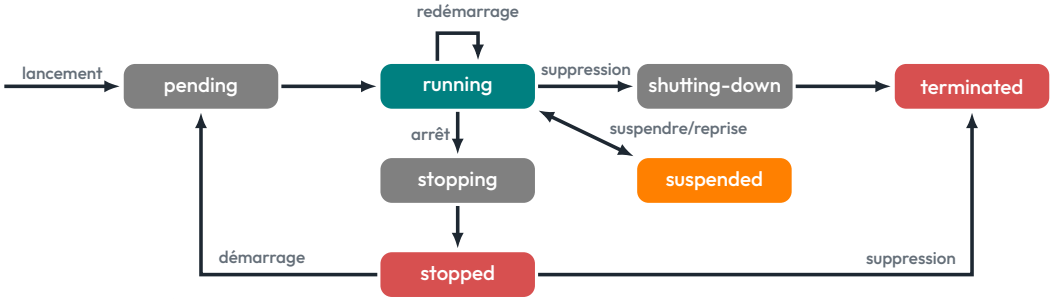
Tableau comparatif : Hyperviseurs de Type I et de Type II

Caractéristique	Hyperviseur de Type I (Baremetal)	Hyperviseur de Type II (Hébergé)
Architecture	S'exécute directement sur le matériel physique	S'exécute sur un système d'exploitation hôte
Performance	Élevée (accès direct au matériel)	Moindre (passe lar l'OS hôte)
Gestion	Complexe (niveau administrateur système requis)	Simple (comme une application standard)
Isolation	Forte (pas de couche OS hôte partagée)	Moins forte (dépendance de l'isolation fournie par l'OS hôte)
Cas d'usage	Datacenters, Cloud, Production, Serveurs critiques	Postes de travail, Développement, Tests, Multi-OS
Exemples	VMware ESXi, Hyper-V, KVM, Xen	Virtual Box, WMware Workstation/Fusion, Parallels

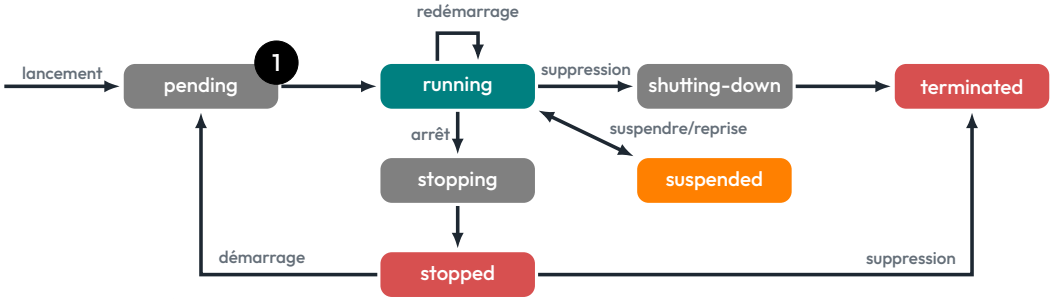
Machine Virtuelles : VMs



Cycle de Vie des VMs



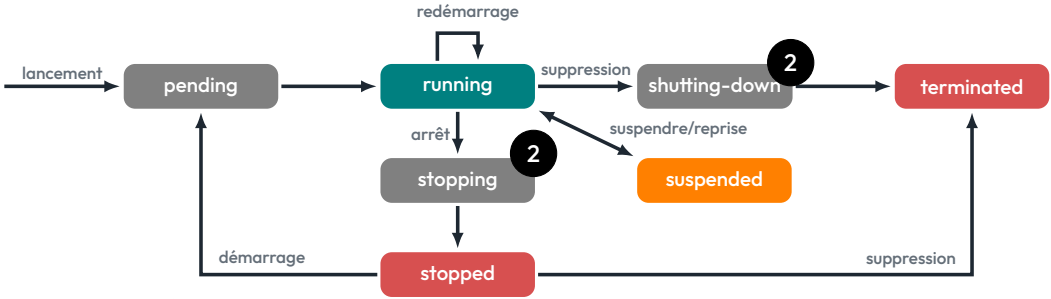
Cycle de Vie des VMs



`pending` (Provisionnement / Préparation)

C'est l'étape où le fournisseur de Cloud (AWS, GCP ou Azure) cherche un serveur physique avec assez de RAM et de CPU pour vous. La VM est « en file d'attente ».

Cycle de Vie des VMs

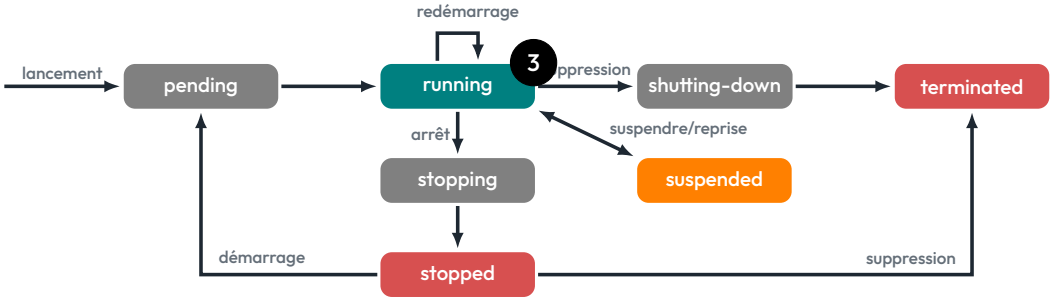


`stopping` / `shutting-down` (En cours d'exécution)

Ce sont les phases où l'OS reçoit le signal d'extinction. Les processus se ferment proprement.

Attention : Dans certains Clouds, la facturation du calcul ne s'arrête qu'une fois ces étapes terminées.

Cycle de Vie des VMs

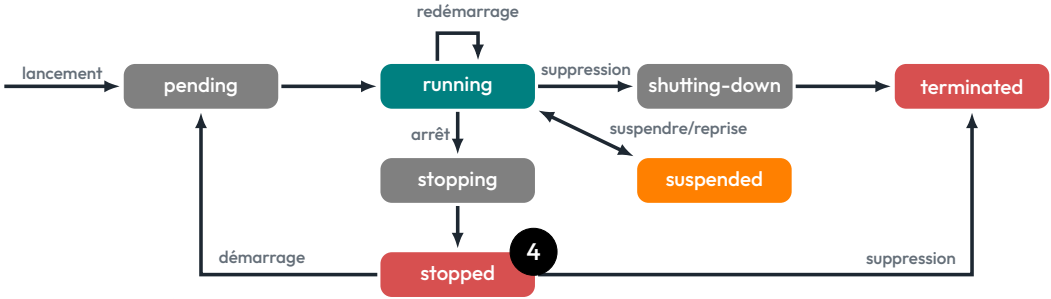


`running` (En cours d'exécution)

C'est le seul état où votre application est accessible.

- Facturation : C'est ici que vous payez le « plein tarif » (CPU + RAM + Disque + IP).
- Action : C'est le point de départ du « redémarrage » (reboot) qui vide la RAM mais garde la VM sur le même hôte physique.

Cycle de Vie des VMs

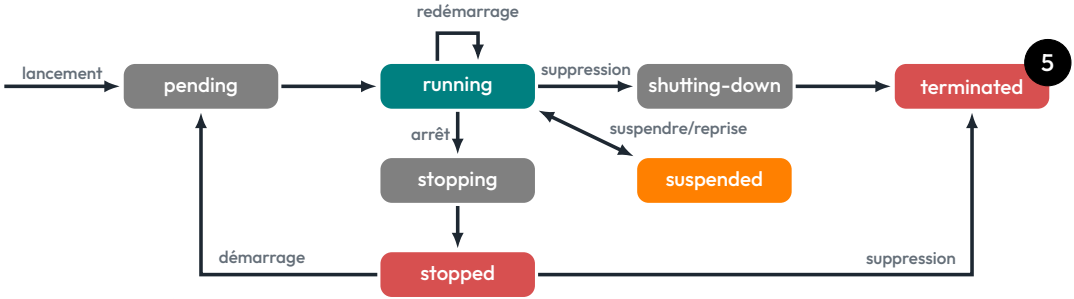


`stopped` (Arrêtée / Deallocated)

La VM est éteinte. Vous ne payez plus pour le CPU ni la RAM.

- Important : Vous continuez à payer pour le stockage (le disque dur ne disparaît pas) et parfois pour l'adresse IP statique si elle est réservée.
- Elle peut repasser à **`pending`** puis **`running`** à tout moment.

Cycle de Vie des VMs



`terminated` (Supprimée)

C'est la fin de vie. Le disque est généralement effacé (sauf option contraire) et la configuration est supprimée de votre console.

Facturation : Tout s'arrête. C'est un état irréversible.

Note sur les spécificités GCP vs AWS

- Sur AWS, **`terminated`** signifie « Supprimée définitivement ».
- Sur GCP, **`terminated`** est souvent utilisé pour dire « Arrêtée » (équivalent au **`stopped`** d'AWS).

États fournisseur

Il existe des états fournisseur spécifique, *e.g.* **`reparairing`** pour GCP : maintenance par le fournisseur.

Images et Templates de Machines Virtuelles

Qu'est ce qu'une image ?

Une **« copie maître »** contenant un OS (et potentiellement des logiciels/paramètres).
Base pour démarrer de nouvelles VMs avec une configuration prédéfinie.

Images et Templates de Machines Virtuelles

Qu'est ce qu'une image ?

Une **« copie maître »** contenant un OS (et potentiellement des logiciels/paramètres).
Base pour démarrer de nouvelles VMs avec une configuration prédéfinie.

Types d'images

Images publiques

- Fournies par le **fournisseur cloud** ou partenaires ;
- **OS populaires** (Linux, Windows Server) avec configuration de base.

Images et Templates de Machines Virtuelles

Qu'est ce qu'une image ?

Une **« copie maître »** contenant un OS (et potentiellement des logiciels/paramètres).
Base pour démarrer de nouvelles VMs avec une configuration prédéfinie.

Types d'images

Images publiques

- Fournies par le **fournisseur cloud** ou partenaires ;
- **OS populaires** (Linux, Windows Server) avec configuration de base.

Images personnalisées

- Créées par **l'utilisateur** à partir d'une **VM configurée** (applis, sécurité, *etc.*) ;
- Nécessite souvent de **« généraliser »** la VM.

Images et Templates de Machines Virtuelles

Avantages des images personnalisées

STANDARDISATION des déploiements.

COHÉRENCE entre environnements (dev, test, prod).

ACCÉLÉRATION de la mise en service de nouvelles instances.

Formats & Fonctionnalités Avancées

- **STANDARDS** comme OVA/OVF pour import/export inter-plateformes.
- **FORMAT SPÉCIFIQUES** *e.g.* GCP Machine Images pour capture multi-disques.

stockage IaaS : Bloc Storage & Object Storage

Après le calcul (VMs), le stockage est l'autre service essentiel de l'IaaS. Les fournisseurs cloud offrent divers types de stockage pour répondre à différents besoins :

- Performance
- Mode d'accès
- Coût
- Cas d'usage

Deux paradigmes principaux : **Bloc Storage** & **Object Storage**.

stockage IaaS : Bloc Storage

Principe

- Fournit des volumes (disques virtuels bruts) attachés à une VM.
- Similaire à un disque dur physique (HDD/SSD) local.
- Données organisées en blocs de taille fixe avec adresses.

Accès

- Volume généralement attaché à une seule VM à la fois.
- L'OS de la VM crée un système de fichiers (NTFS, ext4…) sur le volume.
- Accès via les commandes standards du système de fichiers (comme un disque local).

stockage IaaS : Bloc Storage

Performance

- Optimisé pour faible latence et IOPS (Opérations Entrée/Sortie par seconde) élevés.
- Idéal pour lectures/écritures fréquentes et rapides.
- Varie selon type (SSD > HDD) et options (IOPS garantis).

Cas d'Usage Typiques

- Disques de démarrage (OS) des VMs.
- Bases de données transactionnelles (SQL, NoSQL).
- Applications nécessitant accès via système de fichiers monté.
- Charges de travail exigeant des performances disque élevées.

stockage IaaS : Bloc Storage

Exemples

- AWS EBS, Azure Managed Disks, GCP Persistent Disks.

stockage IaaS : Object Storage

Principe

- Données stockées en « objets » = données + métadonnées + ID unique.
- Structure d'adressage plate dans un « bucket » (ou « conteneur »).
- Pas de hiérarchie de dossiers/fichiers native.

Accès

- Principalement via API RESTful (requêtes HTTP/HTTPS).
- Non monté comme un disque local sur une VM.
- Accessible via réseau (Internet/privé) avec son ID unique (si autorisé).

stockage IaaS : Object Storage

Performance

- Optimisé pour haute durabilité, disponibilité et débit (throughput).
- Scalabilité quasi illimitée (capacité totale, nombre d'objets).
- Latence pour un objet individuel généralement plus élevée que le stockage bloc.

Cas d'Usage Typiques

- Stockage de fichiers statiques volumineux (images, vidéos, docs).
- Sauvegardes et Archivage long terme.
- Logs applicatifs / système.
- Distribution de contenu web statique.
- Data Lakes (Big Data).

stockage IaaS : Object Storage

Exemples

- AWS S3, Azure Blob Storage, Google Cloud Storage (GCS).

Stockage IaaS : Tableau Comparatif

Caractéristiques	Bloc Storage	Object Storage
Unité	Bloc sur volume (disque virtuel)	Objets (données + méta + ID) dans bucket/conteneur
Structure	Hiérarchique (système de fichiers)	Plate (pas de hiérarchie)
Accès	OS (disque local)	API RESTfull (HTTP/HTTPs)
Perf. clé	Faible latence, IOPS élevés	Haut débit / Haute durabilité
Scalabilité	Limitée par taille volume	Quasi illimitée (capacité, nb objets)
Usage	OS, BDD transationnelles, applis	Médias, Backups, Archives, Web, Data Lakes

03

Réseaux IaaS

Réseau IaaS : Le Troisième Pilier

Après le calcul et le stockage, le **réseau** est le pilier essentiel en IaaS.

Les fournisseurs de cloud offrent des capacités de mise en réseau virtualisées pour :

- **Connecter** les ressources (VMs, stockage, etc.) entre elles.
- **Communiquer** avec l'extérieur (Internet, réseaux on-premises).
- Assurer la **sécurité** et l'**isolation** des environnements.

Concepts Clés du Réseau IaaS

- **Réseau Virtuel Privé** (VPC sur AWS/GCP, VNet sur Azure)
- **Sous-réseaux** (Subnets)
- **Adressage IP** (Privé vs Public)
- **Notation CIDR**
- **Passerelles et Routage**
- **Sécurité** (Groupes de sécurité, NSG)

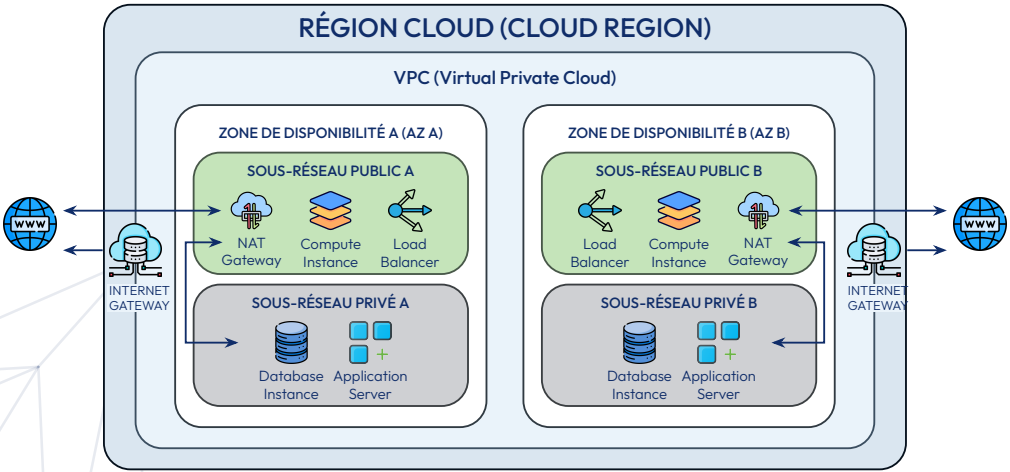
Réseau Privé Virtuel (VPC/VNet)

Qu'est-ce qu'un VPC ?

C'est le cœur de la mise en réseau IaaS : un réseau logique, défini par logiciel, constituant votre "tranche privée" sur le cloud public.

- **Isolation :** Totalement isolé des autres clients sur l'infrastructure partagée (base de la sécurité).
- **Périmètre :** Peut être régional (ex : AWS, Azure) ou global (ex : GCP).
- **Contrôle granulaire :**
  - Définition de l'espace d'adressage IP privé (plage CIDR).
  - Création de sous-réseaux.
  - Configuration du routage et des passerelles.

Réseau Privé Virtuel (VPC/VNet)



Sous-Réseaux (Subnets)

Un VPC est divisé en un ou plusieurs sous-réseaux, chacun représentant une **plage d'adresses IP spécifique**.

- **Organisation logique :** Séparation des ressources (ex : web, app, BDD).
- **Disponibilité et Résilience :**
  - Souvent confinés à une seule Zone de Disponibilité (AZ) (ex : AWS).
  - Répartir les ressources sur plusieurs AZs crée une architecture résiliente.
  - *Exception :* Chez GCP, les sous-réseaux sont régionaux.
- **Types courants :**
  - *Publics :* Possèdent une route directe vers Internet.
  - *Privés :* N'ont pas d'accès direct à Internet.

Adressage IP : Privé vs Public

Adresses IP Privées

- Communication **interne** au VPC.
- Non routables sur l'Internet public.
- Attribuées aux instances lancées dans un sous-réseau.
- Issues des plages RFC 1918 (`10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`).

Adresses IP Publiques

- Communication **avec Internet**.
- Routables publiquement.
- **Dynamiques :** Temporaires, attribuées au lancement.
- **Statiques (Élastiques) :** Fixes, allouées manuellement (idéal pour les serveurs Web).

Adressage IP & Notation CIDR

- **Traduction d'adresses :** Le lien entre IP privée et IP publique est géré par le NAT (Network Address Translation) via la passerelle Internet.
- **Support IPv6 :** De plus en plus courant (adresses globalement uniques).

Notation CIDR (Classless Inter-Domain Routing)

- Exemple : `10.0.0.0/16`
- Définit une plage d'adresses IP et son masque de sous-réseau.
- Le nombre après le / représente le **nombre de bits fixes** alloués à la partie réseau.
- Détermine mathématiquement le nombre d'adresses IP disponibles pour les hôtes.

Conception Initiale du Réseau

La conception réseau est une étape architecturale critique qui impacte la sécurité, la scalabilité et la connectivité.

- **Anticipation :** Choisir judicieusement les plages CIDR pour éviter les chevauchements futurs (ex : lors d'un appairage de VPC).
- **Segmentation :** Diviser en sous-réseaux (par couche applicative, public/privé) est une pratique fondamentale de sécurité.
- **Haute disponibilité :** Répartir stratégiquement les sous-réseaux entre différentes AZs.
- **Sécurité :** L'isolation du VPC est la première barrière, mais elle dépend d'une configuration rigoureuse.

Comment le trafic entre-t-il et sort-il du réseau virtuel ?

Cela repose sur deux composantes clés :

1. La Passerelle Internet (Internet Gateway - IGW)
2. Les Tables de Routage

Passerelle Internet (Internet Gateway - IGW)

- Composant géré par le fournisseur, hautement disponible et scalable.
- **Attachée à un VPC** pour permettre la communication bidirectionnelle entre les sous-réseaux publics et Internet.
- Sans IGW attachée, un VPC reste strictement isolé d'Internet.
- **Fonctionnement :**
  - Sert de cible dans les tables de routage pour le trafic sortant.
  - Effectue le **NAT sortant** pour les instances (utilise leur IP publique).
  - Effectue le **NAT inverse (entrant)** pour le trafic destiné à une IP publique.

Tables de Routage (1/2)

Une table de routage est un ensemble de règles (**routes**) qui déterminent la destination du trafic quittant un sous-réseau ou une passerelle.

- Chaque sous-réseau doit être associé à une table (explicite ou par défaut).
- **Composition typique :**
  - Route locale implicite : Autorise la communication interne au VPC via les IPs privées.
  - Routes explicites : Spécifient une **destination** (plage CIDR) et une **cible** (”next hop”).
- *Exemple :* Destination `0.0.0.0/0` (tout le trafic vers Internet) dirigée vers la cible **IGW** (pour un sous-réseau public).

Tables de Routage (2/2)

- **Règle de priorité :** En cas de conflit, la route la plus spécifique (le masque de sous-réseau le plus long) est prioritaire.
- **Blackhole :** Si aucune route ne correspond, le trafic est silencieusement abandonné.
- **Principe du moindre privilège réseau :** La connectivité n'est jamais automatique. Les tables définissent explicitement les chemins autorisés.
  - Une VM sans route vers une IGW ou une NAT Gateway ne pourra pas joindre Internet.
- **Enjeu :** Le routage est l'outil fondamental pour la segmentation logique et le contrôle précis des flux.

Sécurité : Groupes de Sécurité & Pare-feu

Au-delà du routage, il est impératif de contrôler quel trafic est spécifiquement autorisé à atteindre ou quitter une ressource (comme une VM).

Les Pare-feux virtuels en IaaS

- **Security Groups (SG)** sur AWS et GCP.
- **Network Security Groups (NSG)** sur Azure.

Ils sont généralement associés directement aux **interfaces réseau (NICs)** des VMs, ou au niveau du sous-réseau (dans le cas des NSG Azure).

Fonctionnement des Groupes de Sécurité (SG/NSG)

- **Filtrage granulaire :** N'autorise que les communications *explicitement* permises.
- **Stateful (À état) :**
  - Le pare-feu mémorise les connexions actives.
  - Si une requête sortante est autorisée, le trafic de réponse correspondant (entrant) est automatiquement autorisé à revenir.
  - Cela simplifie grandement la configuration par rapport aux pare-feux "Stateless" (comme les Network ACLs sur AWS où il faut ouvrir les ports de retour).

Règles des Groupes de Sécurité

Tout trafic non autorisé est **refusé par défaut**. Chaque règle d'autorisation doit définir :

- **Direction :** Entrante (Ingress) ou Sortante (Egress).
- **Protocole & Port :** TCP, UDP, ICMP, etc., avec un port ou une plage de ports.
- **Source / Destination :**
  - Une adresse IP spécifique ou une plage CIDR.
  - Un autre groupe de sécurité (très puissant pour lier des architectures applicatives).
- **Action & Priorité :**
  - Généralement "Allow". Azure supporte des "Deny" explicites.
  - Azure utilise un système de priorité. Sur AWS/GCP, une seule règle "Allow" correspondante suffit.

Règles par défaut à surveiller

Généralement, tout le trafic sortant est autorisé, et tout le trafic entrant est refusé. **Il est crucial de les auditer et de les restreindre.**

- **Micro-segmentation :** Isoler les VMs individuellement, même si elles partagent le même sous-réseau.
- **Moindre privilège :** N'autoriser que les flux strictement nécessaires.
  - *Exemple Serveur Web :* Entrant `80/443` depuis `0.0.0.0/0`, et `22/3389` uniquement depuis la plage IP de votre équipe d'administration.
- **Précision :** Soyez aussi spécifique que possible dans vos règles (ports exacts, sources précises).

04

Introduction à la plannification

Comment déterminer les ressources cloud nécessaires ?

Principes d'évaluation des besoins en ressources

Planification de la capacité (Capacity Planning) / Dimensionnement (Sizing)

Déterminer la quantité de ressources (CPU, RAM, Stockage, Réseau) nécessaire au bon fonctionnement d'une application.

Cette évaluation a une **importance double** :

- **Assurer la Performance :** Éviter le sous-dimensionnement qui entraîne des lenteurs ou des pannes.
- **Optimiser les Coûts :** Éviter le surdimensionnement, synonyme de capacité inutilisée et de gaspillage dans un modèle facturé à l'usage (*pay-as-you-go*).

Ressources Clés à Évaluer

CPU (Processeur)

Puissance de calcul. Mesurée en vCPU et fréquence. Dépend de l'intensité de traitement requise.

RAM (Mémoire Vive)

Espace mémoire mesuré en Go. Dépend du volume de données chargées en mémoire, des utilisateurs simultanés et de l'efficacité de l'application.

Ressources Clés à Évaluer

Stockage

- *Capacité :* Quantité totale de données (Go/To).
- *Performance :* Vitesse d'accès (IOPS, débit en Mo/s).
- *Choix technologiques :* Type (Bloc vs Objet) et caractéristiques (SSD vs HDD, IOPS provisionnés).

Réseau (Bande Passante / Débit)

Quantité de données transitant en entrée et en sortie (Mbps/Gbps).

> **Important**
>
> Les coûts de transfert sortant (« egress ») peuvent être importants.

Comment Estimer les Besoins ?

L'estimation repose sur plusieurs méthodes combinées :

- **Analyse Applicative :** Comprendre le fonctionnement, les opérations coûteuses et le profil des utilisateurs.
- **Analyse Historique & Monitoring :** Étudier les données de consommation passées (moyennes et pics) si l'application existe déjà.
- **Benchmarking :** Tester l'application sur différentes configurations en simulant la charge pour établir des *baselines* et identifier les *goulots d'étranglement*.
- **Prévisions de Charge (Forecasting) :** Anticiper l'évolution future (croissance utilisateurs, nouvelles fonctionnalités).
- **Déploiement Pilote :** Valider les hypothèses en environnement réel avec un groupe restreint d'utilisateurs.

Planification dans le Cloud : Itération et Optimisation

La spécificité du cloud : l'élasticité

Contrairement aux infrastructures sur site (on-premises), il est inutile de sur-provisionner massivement à long terme. L'approche est plus **dynamique et itérative**.

- **Démarrage :** Commencer avec une estimation raisonnable.
- **Ajustement continu (« Right-sizing ») :** Monitorer la consommation réelle et ajuster la taille des instances.
- **Auto-scaling :** Utiliser l'automatisation pour adapter la capacité à la demande en temps réel.
- **Objectif :** Trouver en permanence le meilleur équilibre entre la performance applicative et le coût de l'infrastructure.

05

Présentation de l'environnement de TP

Présentation de la plateforme utilisée en TP

- **Plateforme utilisée :** IBM (ou ScaleWay) / Hyperviseur Proxmox
- **Permet de créer et gérer :**
  - Machines Virtuelles (Compute)
  - Réseaux Virtuels (VPC/VNet, Sous-réseaux, Routage, Sécurité)
  - Stockage (Volumes, Buckets)
  - Règles de sécurité (Groupes de Sécurité/NSG)

06

Conclusion & Récapitulation

Conclusion : Fondations IaaS (1/2)

- **Modèles de déploiement :** Contraste On-Premises (propriété, contrôle total, CapEx) vs Cloud Computing (location, gestion déléguée, flexibilité, OpEx).
- **Modèles de service cloud : IaaS**, **PaaS**, **SaaS** (différents niveaux de gestion).
- **Composants fondamentaux de l'IaaS :**
  - **Compute :** Hyperviseur (Type 1), VMs, images/templates.
  - **Stockage :** Bloc (OS, bases de données) vs Objet (fichiers, backups, médias).

Conclusion : Fondations IaaS (2/2)

Le Réseau IaaS

- **VPC/VNet :** Isolation logique.
- **Sous-réseaux :** Organisation et Haute Disponibilité (HA).
- **Adressage IP :** Privé vs Public.
- **Passerelle Internet :** Connectivité externe.
- **Tables de Routage :** Diriger le trafic.
- **Groupes de Sécurité/NSG :** Pare-feux *stateful*, micro-segmentation.

Conclusion : Planification

- Importance de la **planification de la capacité (sizing)** pour équilibrer performance et coût.
- **Ressources clés :** CPU, RAM, Stockage, Réseau.
- **Méthodes d'estimation :** Analyse des exigences/historique, monitoring, benchmarking, prévisions, déploiement pilote.
- **Approche cloud :** Itérative et optimisée grâce à l'élasticité, au monitoring et à l'auto-scaling.

Objectifs atteints

À ce stade, vous devriez être capable de :

- Distinguer les caractéristiques fondamentales d'une infrastructure locale vs cloud.
- Différencier les modèles IaaS, PaaS et SaaS.
- Identifier et décrire les rôles des composants IaaS majeurs (VM, Stockage Bloc/Objet, Réseau Virtuel, Groupe de Sécurité).
- Comprendre les principes de base de l'estimation des besoins en ressources.

Des Questions ?