UNIVERSITÉ DE JENDOUBA
FACULTÉ DES SCIENCES JURIDIQUES, ÉCONOMIQUES ET DE GESTION
DÉPARTEMENT INFORMATIQUE

Cloud Computing:

Concepts, Technologies et Mise en œuvre

Support de cours

Roukaya Ben Jeddou
FSJEG, Université de Jendouba
CREGO, Université de Bourgogne Europe
rokaya.benjeddou@fsjegj.u-jendouba.tn

Table des matières

Liste des figures

Liste des tableaux

Avant-propos

Le cloud computing est devenu un pilier fondamental de l'infrastructure informatique moderne. Son adoption massive par les entreprises, les administrations et les institutions éducatives transforme profondément la manière dont les services informatiques sont conçus, déployés et consommés.

Ce cours a pour objectif de fournir une compréhension des concepts, des technologies et des pratiques de gouvernance associés au cloud. Il aborde à la fois les aspects techniques, tels que les modèles de services (IaaS, PaaS, SaaS), les architectures de déploiement (privé, public, communautaire, hybride) et la virtualisation, ainsi que les dimensions stratégiques, telles que la migration, la sécurité, la gestion de la conformité.

Ce cours vise à développer les compétences nécessaires pour concevoir, gérer et optimiser des environnements cloud. Il offre également un cadre pour comprendre les bonnes pratiques et les standards internationaux qui guident les choix technologiques et organisationnels dans le cloud.

Chapitre 1

L'Émergence du Cloud Computing

Introduction

Le *cloud computing* s'est imposé comme l'une des évolutions majeures de l'ère numérique, transformant profondément la manière dont les entreprises et les institutions gèrent leurs ressources informatiques. En permettant l'accès à la puissance de calcul, au stockage et aux logiciels à la demande, il marque la transition d'un modèle basé sur la possession d'infrastructures physiques vers un modèle fondé sur la mutualisation et la flexibilité.

Ce chapitre vise à répondre à une question centrale : pourquoi le *cloud* s'est-il imposé aujourd'hui comme une composante incontournable de la stratégie technologique et organisationnelle des entreprises ? Pour y répondre, il convient d'examiner les dimensions économiques, stratégiques et évolutives de ce paradigme technologique.

1.1 Motivation économique

Les entreprises investissent dans des infrastructures informatiques - serveurs, stockage, réseaux - souvent surdimensionnées par rapport à leurs besoins réels. La consommation informatique varie fortement au fil du temps:

- Périodes creuses: les ressources sont sous-utilisées.
- Pics de charge: forte demande temporaire (Black Friday, fin de trimestre...).

Cette variabilité entraîne un gaspillage financier et technique si l'entreprise achète tout le matériel nécessaire pour absorber les pics annuels. C'est le modèle CapEx (dépenses en capital), où l'entreprise paie pour des ressources fixes, qu'elles soient utilisées ou non. Le Cloud Computing permet de payer à l'usage (modèle OpEx), en louant les ressources uniquement quand elles sont nécessaires. Cela offre plusieurs avantages:

- Flexibilité et scalabilité: augmentation ou réduction rapide des ressources selon la demande.
- Réduction des coûts: plus besoin d'acheter et d'entretenir du matériel excédentaire.
- Agilité: déploiement rapide de nouveaux services, sans lourds investissements.

Exemple: Une boutique en ligne doit gérer 10 000 commandes par jour en moyenne, mais 100 000 commandes lors du Black Friday.

> *Sans Cloud:* elle achète 100 serveurs pour absorber ce pic. Pendant 364 jours, ces serveurs restent sous-utilisés $\Rightarrow$ coût élevé et gaspillage.
>
> *Avec Cloud:* elle loue temporairement les 90 serveurs supplémentaires juste pour le Black Friday, payant uniquement pour la durée d'utilisation $\Rightarrow$ économies et flexibilité.

Le Cloud propose un modèle économique innovant:

- passage des dépenses en capital (CapEx) à des dépenses opérationnelles (OpEx);
- paiement uniquement pour les ressources effectivement consommées;
- réduction du besoin d'investissements lourds en matériel.

Modèle économique à l'usage

L'un des bouleversements majeurs introduits par le *cloud computing* réside dans son modèle économique. Le passage d'un modèle de dépenses d'investissement (*CAPEX*) à un

modèle de dépenses d'exploitation (*OPEX*) transforme la manière dont les entreprises conçoivent et financent leurs projets numériques.

Le modèle dit *pay-as-you-go*, comparable à une facturation à la consommation, permet de payer uniquement pour les ressources utilisées.

Table 1.1: Comparaison des approches de prototypage : sur site vs. cloud

Scénario A (Infrastructure sur site)	**Scénario B (Modèle cloud)**
Coût : Achat de serveurs physiques (entre 3 000 et 5 000 $ chacun), ajout des licences logicielles, de la livraison et de l'installation.	**Coût :** Utilisation de ressources virtuelles à 0,50 $ par heure, pour un coût total de quelques dollars.
Délai : Entre 1 et 3 mois pour l'évaluation, l'achat et l'installation du matériel.	**Délai :** Création et test des ressources virtuelles en quelques minutes.
Efficacité : Risque de surinvestissement et de sous-utilisation des ressources physiques.	**Efficacité :** Ajustement instantané des ressources sans gaspillage.

Cette comparaison met en évidence un avantage stratégique majeur : le *cloud* permet une expérimentation rapide, un prototypage agile et une allocation des ressources parfaitement adaptée aux besoins réels. Il offre ainsi une souplesse que les infrastructures traditionnelles ne peuvent égaler.

1.2 Évolution historique

Le *cloud computing* est le résultat d'une évolution technologique progressive plutôt qu'une rupture soudaine. Il représente une synthèse intelligente des modèles informatiques antérieurs.

L'ère des Mainframes

Cette période se caractérisait par une centralisation complète du traitement et des données. Les administrateurs systèmes contrôlaient l'ensemble des ressources informatiques, garantissant une gouvernance stricte, mais limitant la flexibilité et la rapidité d'exécution.

L'ère Client-Serveur

Avec l'apparition des ordinateurs personnels, les charges de travail ont été distribuées, donnant plus d'autonomie aux utilisateurs et aux départements. Toutefois, cette décentralisation a introduit de nouveaux défis liés à la sécurité, à la maintenance et à la cohérence des systèmes d'information.

L'ère d'Internet

L'Internet a marqué un tournant décisif en ouvrant l'entreprise vers l'extérieur. Il a permis l'intégration des fournisseurs et la commercialisation en ligne. Cependant, cette ouverture a accentué les enjeux de sécurité et de complexité.

L'avènement du Cloud

Le *cloud computing* combine les atouts des modèles précédents : le contrôle centralisé du mainframe, la distribution des ressources du client-serveur et la connectivité mondiale d'Internet. Il s'appuie sur une facturation à l'usage et une élasticité sans précédent. Cette évolution représente la convergence logique de plusieurs décennies d'innovations technologiques.

Le *cloud* est désormais une composante standard de l'architecture informatique moderne, adoptée par la majorité des entreprises, administrations et institutions. L'évolution de la sécurité et de la gouvernance a joué un rôle déterminant dans cette maturité. Les premiers obstacles liés à la protection des données ont progressivement été surmontés grâce au développement de standards et de certifications garantissant la conformité et la résilience des infrastructures.

1.3 Définitions

Plusieurs définitions du Cloud Computing coexistent, créant parfois une ambiguïté. Le National Institute of Standards and Technology (NIST) fournit une définition largement

acceptée:

"Le Cloud Computing est un modèle permettant un accès ubiquitaire, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (réseaux, serveurs, stockage, applications et services), qui peuvent être rapidement provisionnées et libérées avec un minimum d'effort de gestion ou d'interaction avec le fournisseur."

Cette définition repose sur:

- cinq caractéristiques essentielles,
- trois modèles de service,
- quatre modèles de déploiement.

1.4 Les caractéristiques et les exigences et du Cloud

Le NIST identifie cinq caractéristiques qui, si elles ne sont pas présentes, signifient que ce n'est pas un véritable service cloud (Figure1.1):

- **Service à la demande (On-demand self-service):** L'utilisateur peut provisionner des ressources informatiques (comme du stockage, des serveurs ou des applications) automatiquement, sans intervention humaine du fournisseur de services.
- **Accès réseau large (Broad network access):** Les ressources sont accessibles via le réseau, à partir de divers types d'appareils (ordinateurs, tablettes, smartphones, etc.), au moyen de mécanismes standard (ex. : navigateur Web).
- **Mutualisation des ressources (Resource pooling):** Les ressources informatiques du fournisseur sont mutualisées pour servir plusieurs clients, avec une séparation logique des données (principe du multitenant).
- **Élasticité et évolutivité rapides (Rapid elasticity):** Les ressources peuvent être augmentées ou réduites rapidement selon la demande. Aux yeux de l'utilisateur, les capacités disponibles semblent illimitées.

- **Service mesuré (Measured service):** Les systèmes de cloud mesurent automatiquement l'utilisation des ressources (CPU, stockage, bande passante, etc.), permettant une facturation transparente et proportionnelle à la consommation réelle.

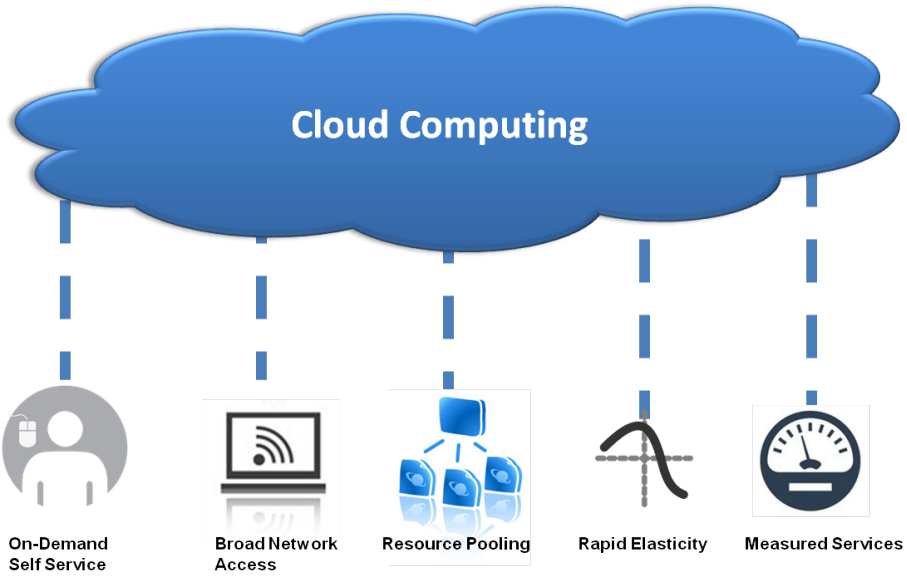

Figure 1.1: Les cinq caractéristiques cloud

Pour être considéré comme véritable service cloud, un fournisseur doit garantir:

- Multitenancy: isolation des utilisateurs tout en partageant les ressources.
- Gestion du cycle de vie des services: démarrage/arrêt automatique, facturation dynamique.
- Sécurité et conformité: protection des données, respect des normes légales (ex.: GDPR).
- Réactivité et fiabilité: disponibilité et reprise rapide en cas d'incident.
- Interopérabilité et portabilité: intégration avec d'autres systèmes et migration possible.
- Traitement des données massives: prise en charge du Big Data et des traitements distribués.

Conclusion

Le *cloud computing* s'impose aujourd'hui comme une infrastructure fondamentale du numérique. Il combine efficacité économique, agilité technologique et alignement stratégique. Cette transformation ne relève pas d'un effet de mode, mais d'un changement structurel et durable dans la manière de concevoir et de gérer les systèmes d'information.

Les bénéfices essentiels sont multiples :

- une flexibilité et une agilité renforcées ;
- une réduction importante des coûts d'investissement ;
- une meilleure réactivité face à la demande ;
- un recentrage sur les compétences métiers essentielles.

Toutefois, la réussite d'une stratégie cloud dépend de la capacité des organisations à aligner les choix technologiques sur leurs objectifs métiers. Les modèles de services - Software as a Service (SaaS), Platform as a Service (PaaS) et Infrastructure as a Service (IaaS) - représentent les trois piliers fondamentaux de cette nouvelle ère, qui feront l'objet du chapitre suivant.

Chapitre 2

Les modèles de service & de déploiement du cloud

Introduction

Le choix du bon modèle de service et de déploiement est l'un des facteurs de succès les plus critiques pour toute solution basée sur le cloud. Cette décision stratégique ne se limite pas à un simple choix technique; elle détermine fondamentalement les responsabilités, le niveau de contrôle et l'agilité future d'une organisation. Le choix du modèle cloud (service & déploiement) influence profondément la manière dont une organisation innove et opère. Un choix éclairé permet de débloquer des gains d'efficacité, tandis qu'une décision mal alignée peut entraîner des coûts imprévus et des limitations techniques.

Pour opérer ce choix stratégique, il est impératif de comprendre en profondeur ce que chaque modèle implique, ainsi que la répartition claire des responsabilités entre le fournisseur de services cloud et le consommateur de ces services. Cette compréhension permet de s'assurer que le modèle sélectionné répond non seulement aux besoins actuels, mais qu'il offre également la flexibilité nécessaire pour évoluer avec l'entreprise. Ce chapitre propose une analyse détaillée des trois modèles de service fondamentaux, ainsi que des modèles de déploiement qui les accompagnent, afin de fournir les connaissances nécessaires pour prendre des décisions architecturales éclairées.

2.1 Les modèles de service

Le cloud computing est structuré en trois modèles de service principaux: l'Infrastructure en tant que Service (*Infrastructure as a service: IaaS*), la Plateforme en tant que Service (*Plateforme as a service: PaaS*) et le Logiciel en tant que Service (*Software as a service: SaaS*) (Figure 2.1). Chacun de ces modèles offre un niveau d'abstraction différent qui réduit l'effort requis par le consommateur pour construire et déployer des systèmes. Plus le niveau d'abstraction est élevé, plus le fournisseur de services gère de composants (Table 2.1), permettant ainsi au consommateur de se concentrer sur des tâches à plus forte valeur ajoutée.

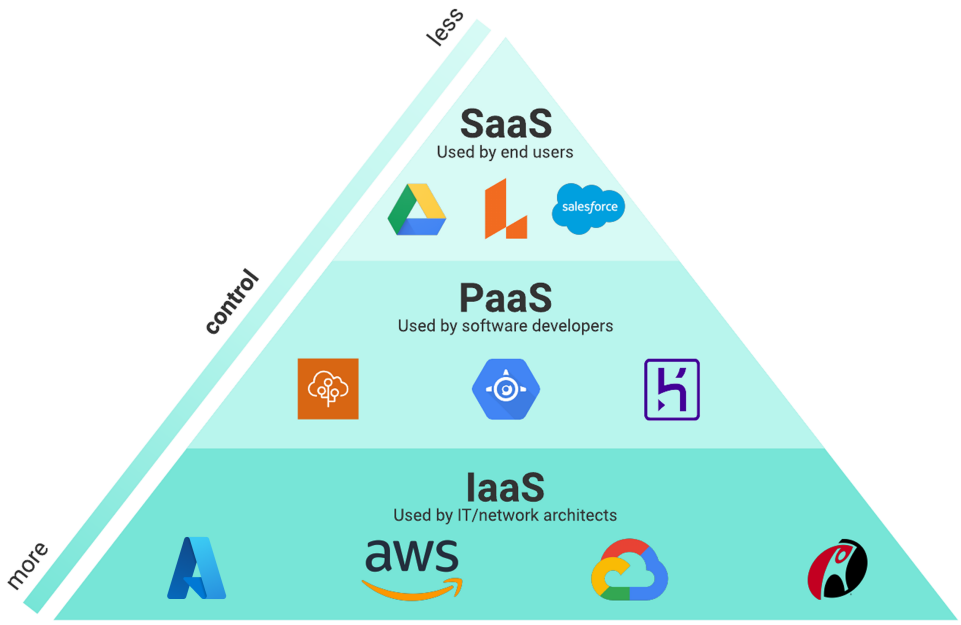

Figure 2.1: Saas, Iaas, Paas

Pour visualiser ces différentes couches d'abstraction et la répartition des responsabilités qui en découle, il est utile de se référer au concept de la *pile cloud* (Cloud Stack). Cette pile illustre comment chaque modèle de service s'appuie sur le précédent, créant une hiérarchie claire des responsabilités entre le fournisseur et le consommateur, un point que nous examinerons en détail pour chaque modèle (Figure 2.2).

Cette répartition des rôles constitue le critère fondamental qui différencie les modèles.

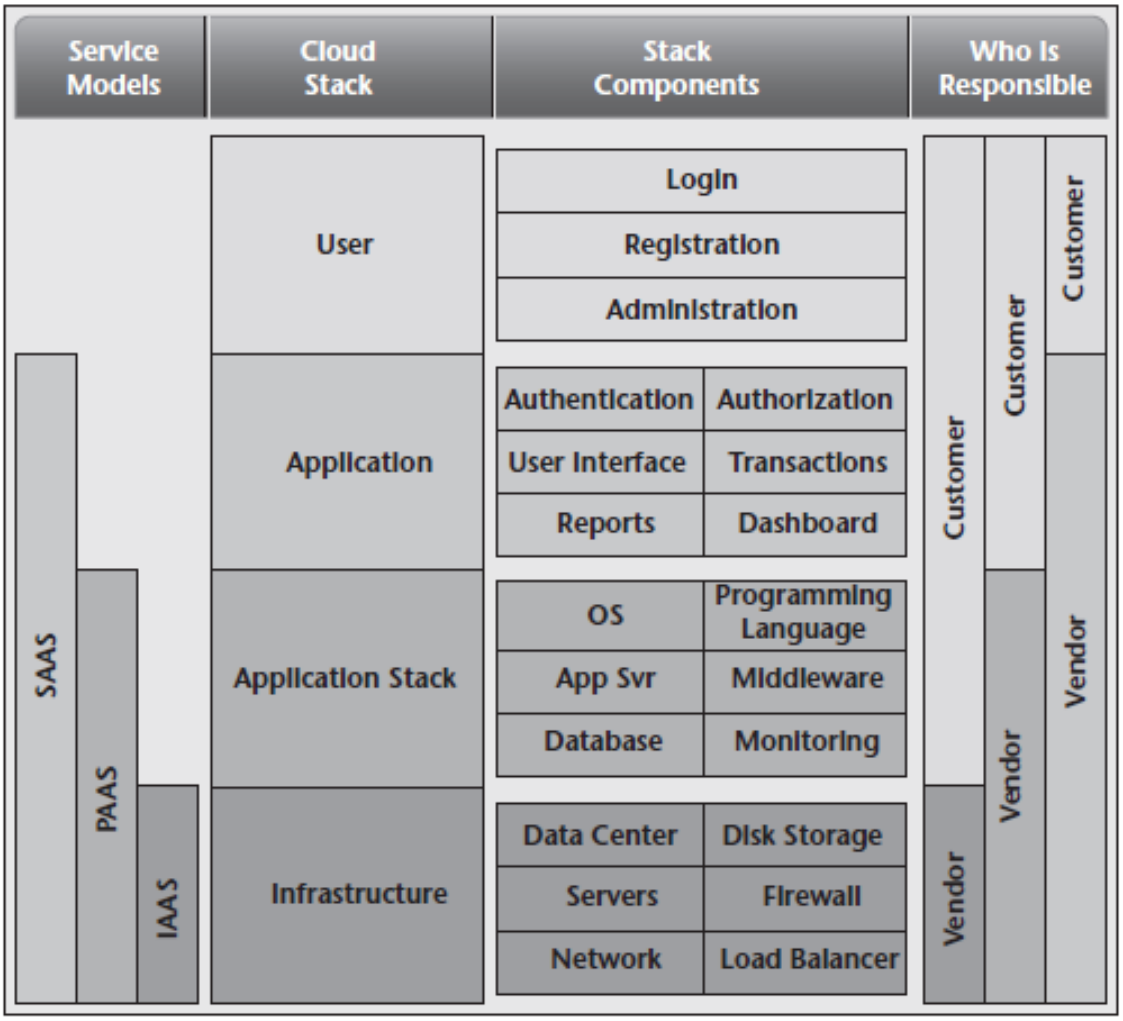

Figure 2.2: Cloud stack

Table 2.1: Tableau comparatif des responsabilités selon le modèle de service

Composant Technologique	**On-Premises**	**IaaS**	**PaaS**	**SaaS**
Réseaux	Client	Fournisseur	Fournisseur	Fournisseur
Stockage	Client	Fournisseur	Fournisseur	Fournisseur
Serveurs (matériel)	Client	Fournisseur	Fournisseur	Fournisseur
Virtualisation	Client	Fournisseur	Fournisseur	Fournisseur
Système d'exploitation	Client	Client	Fournisseur	Fournisseur
Middleware / Runtimes	Client	Client	Fournisseur	Fournisseur
Bases de données	Client	Client	Fournisseur	Fournisseur
Applications	Client	Client	Client	Fournisseur
Gestion des données	Client	Client	Client	Fournisseur

L'analyse du premier niveau, l'IaaS, permettra de comprendre les fondations sur lesquelles reposent les autres services.

Infrastructure as a Service (IaaS)

L'Infrastructure en tant que Service constitue le niveau de base de la pile cloud. Ce modèle offre des capacités de centre de données virtuel, permettant aux entreprises d'externaliser et de provisionner des ressources informatiques fondamentales telles que le calcul, le stockage et les réseaux.

Selon la définition formelle du **NIST**:

> *"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls)."*

La **Cloud Security Alliance (CSA)** complète cette définition en précisant :

> *Delivers computer infrastructure (typically a platform virtualization environment) as a service, along with raw storage and networking. Rather than purchasing servers, software, data center space, or network equipment, clients instead buy those resources as a fully outsourced service.*

Concrètement, l'IaaS abstrait pour le consommateur toute la complexité liée à la gestion d'un centre de données physique: serveurs, stockage, et équipements réseau. Un architecte IT peut ainsi provisionner plusieurs serveurs de tailles différentes et tester de multiples configurations pendant quelques heures pour un coût total de quelques dollars. Dans un modèle traditionnel, cette même tâche aurait nécessité des mois et des milliers de dollars en dépenses d'investissement.

Parmi les fournisseurs pionniers de l'IaaS, on trouve Amazon Web Services (AWS). En parallèle, le projet open source OpenStack permet aux organisations de construire leurs propres capacités IaaS, souvent dans le cadre d'un cloud privé, afin d'éviter la dépendance à un fournisseur unique.

Caractéristiques de l'IaaS: Les fournisseurs d'IaaS mettent à disposition des utilisateurs des ressources informatiques virtualisées, accessibles selon un modèle de facturation à l'usage. En complément des propriétés générales du cloud computing (élasticité, libre-service, accès réseau, mutualisation, mesure des services), l'IaaS présente plusieurs caractéristiques spécifiques.

- Accès aux ressources via Internet: L'IaaS permet aux utilisateurs de provisionner et gérer des ressources (VM, stockage, réseau) à distance, grâce à une interface Web ou une console de gestion. Il suffit d'une connexion Internet pour déployer ou adapter l'infrastructure nécessaire.

- Gestion centralisée: Toutes les ressources, même réparties géographiquement, peuvent être administrées depuis un point unique. Cela facilite le suivi, l'orchestration et l'optimisation de l'utilisation des ressources.

- Élasticité et adaptation automatique: Les ressources peuvent être augmentées ou réduites en fonction de la charge applicative. Ce dimensionnement dynamique assure une utilisation efficace et évite la sur-allocation typique des infrastructures traditionnelles.

- Mutualisation de l'infrastructure: L'IaaS repose généralement sur un modèle multi-tenant: plusieurs clients partagent la même infrastructure physique, tout en bénéficiant d'un isolement grâce à la virtualisation. Chaque organisation dispose ainsi de machines virtuelles indépendantes.

- Machines virtuelles préconfigurées: Les fournisseurs proposent des VM prêtes à l'emploi, intégrant différents systèmes d'exploitation, configurations réseau et images logicielles. Les utilisateurs peuvent ainsi déployer rapidement leurs environnements sans configuration initiale complexe.

- Services mesurés et facturation flexible: La consommation est calculée et facturée selon l'usage réel (CPU, stockage, bande passante). Ce modèle réduit le coût total de possession (Total cost ownership: TCO) et améliore le retour sur investissement

(ROI), notamment pour les structures qui ne peuvent pas immobiliser de capital dans l'achat de matériel.

Cas d'usage recommandés: L'IaaS est particulièrement adapté dans les situations suivantes:

- Variations de charge imprévisibles: idéal lorsque la demande fluctue fortement, rendant difficile le dimensionnement d'une infrastructure interne.
- Contraintes budgétaires: les start-ups et petites structures peuvent bénéficier d'une infrastructure puissante sans investissement initial important.
- Besoins ponctuels en ressources: utile pour des charges saisonnières ou événementielles (ex. pics d'activité lors de fêtes religieuses ou périodes de forte demande).

Situations où l'IaaS peut être déconseillé: L'IaaS peut être déconseillé dans les situations suivantes:

- Contraintes réglementaires strictes: certaines organisations ne peuvent pas héberger leurs données ou applications en dehors de leurs murs.
- Faible besoin en ressources: une infrastructure interne déjà suffisante peut rendre l'IaaS non rentable.
- Nécessité de contrôle physique: l'IaaS ne permet pas de maîtriser le matériel sous-jacent.

Avantages

- Modèle économique flexible: paiement selon l'usage réel, sans investissement initial dans le matériel.
- Évolutivité rapide: augmentation ou réduction des ressources instantanée.
- Réduction du TCO: moins d'investissements matériels, moins de maintenance interne.

- Impact environnemental réduit: la mutualisation améliore l'efficacité énergétique globale.

Limites

- Risques de sécurité: l'usage d'hyperviseurs ouvre la porte à des attaques spécifiques. Une compromission peut potentiellement affecter plusieurs VM.
- Interopérabilité limitée: l'absence de standards stricts rend complexe la migration d'une VM d'un fournisseur à un autre.
- Performance variable: la dépendance au réseau Internet peut entraîner de la latence ou une dégradation de performance.

Platform as a Service (PaaS)

La Plateforme en tant que Service (PaaS) représente le niveau intermédiaire de la pile cloud. Ce modèle va plus loin que l'IaaS en abstrayant non seulement l'infrastructure, mais aussi une grande partie des fonctions standards de la pile applicative (système d'exploitation, middleware, bases de données, etc.). L'objectif est de fournir un environnement complet pour accélérer le développement, le déploiement et la gestion des applications.

Définition du NIST:

> *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*

La CSA décrit le PaaS comme:

> *The delivery of a computing platform and solution stack as a service. PaaS offerings facilitate deployment of applications without the cost and complexity of*

buying and managing the underlying hardware and software and provisioning hosting capabilities.

Le compromis fondamental du PaaS réside dans un échange entre vitesse et contrôle. Les développeurs gagnent en rapidité et peuvent se concentrer sur la logique métier de leurs applications. En contrepartie, ils cèdent le contrôle sur des éléments logiciels de bas niveau comme la mémoire, les threads, ou la configuration système, car ils sont contraints par les outils du fournisseur PaaS.

L'évolution du PaaS illustre une recherche de flexibilité renforcée. Les pionniers comme Force.com, Google App Engine et Microsoft Azure imposaient initialement des environnements spécifiques. Aujourd'hui'hui, des plateformes comme Heroku et Engine Yard offrent plus de liberté, et les géants du secteur prennent désormais en charge plusieurs langages de programmation.

La véritable puissance du PaaS réside dans son aptitude à intégrer des solutions tierces via des plugins, add-ons ou extensions, permettant d'assembler rapidement des solutions complexes à partir de services éprouvés: bases de données, sécurité, mise en cache, etc.

Caractéristiques du PaaS: Le Platform as a Service (PaaS) se distingue des environnements de développement traditionnels en proposant une plateforme complète permettant de concevoir, tester, déployer et maintenir des applications sans gérer l'infrastructure sous-jacente. Les principales caractéristiques sont:

- Environnement intégré de développement: Les fournisseurs PaaS proposent une plateforme unifiée regroupant l'ensemble des services nécessaires au cycle de vie applicatif : développement, tests, déploiement, hébergement et maintenance, souvent accessibles au sein d'un même IDE en ligne.

- Accès via une interface Web: Les outils de développement sont disponibles depuis un navigateur. Les développeurs peuvent ainsi créer, modifier, compiler et déployer leurs applications sans installer d'outils localement.

- Développement hors ligne possible: Certains fournisseurs permettent la synchroni-

sation entre un IDE local et la plateforme cloud. Le développeur peut travailler sans connexion puis publier son application dès qu'Internet est disponible.

- Évolutivité native: Les plateformes PaaS assurent automatiquement la montée ou descente en charge des applications selon l'utilisation. L'élasticité devient alors transparente pour le développeur.

- Plateforme collaborative: Les projets peuvent être développés simultanément par des équipes distribuées géographiquement. Le PaaS favorise la collaboration grâce à des outils partagés, un contrôle de version intégré et des environnements communs.

- Large éventail d'outils: Les services PaaS proposent différents outils pour simplifier le développement : CLI, interfaces Web, API REST, IDE intégrés, etc. Cela permet de s'adapter à différents profils de développeurs.

Cas d'usage recommandés: Le PaaS représente une solution avantageuse pour plusieurs scénarios:

- **Développement collaboratif:** Idéal pour les équipes réparties dans différents lieux travaillant sur un même projet.

- **Automatisation du test et du déploiement:** Les pipelines CI/CD intégrés permettent aux équipes de se concentrer sur la logique métier plutôt que sur la configuration technique.

- **Time-to-market réduit:** Les méthodologies itératives et les outils fournis permettent de lancer rapidement de nouvelles fonctionnalités ou produits.

Situations où le PaaS est moins adapté: Malgré sa popularité, certains contextes limitent l'usage du PaaS:

- **Migrations fréquentes ou multi-cloud :** L'absence de standards et l'utilisation de technologies propriétaires rendent la portabilité difficile.

- **Besoins avancés de personnalisation :** Le contrôle limité de l'infrastructure ne convient pas aux plateformes nécessitant un paramétrage très spécifique.

Avantages

1. **Développement et déploiement accélérés:** Les outils intégrés automatisent une grande partie des opérations, réduisant ainsi les délais de mise en production.
2. **Travail collaboratif facilité:** Les environnements partagés permettent aux équipes d'avancer ensemble, quel que soit leur emplacement.
3. **Réduction des coûts de maintenance:** Les organisations n'ont plus besoin de gérer l'infrastructure ni les couches logicielles associées.

Limites

1. **Dépendance au fournisseur (vendor lock-in):** Les technologies propriétaires compliquent la migration vers un autre service.
2. **Sécurité et confidentialité:** Les données sont hébergées sur des infrastructures tierces, ce qui peut soulever des préoccupations.
3. **Dépendance à la qualité de la connexion Internet:** Une connexion lente peut affecter considérablement l'expérience de développement.

Software as a Service (SaaS)

Le Logiciel en tant que Service (SaaS) se situe au sommet de la pile cloud. Il représente une application complète, prête à l'emploi, livrée comme un service directement à l'utilisateur final via un navigateur ou une API.

Définition du NIST:

> *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser*

> *(e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

Le consommateur ne gère que la configuration et les comptes utilisateurs; tout le reste (infrastructure, application, sécurité, maintenance) relève du fournisseur. Ce modèle est privilégié pour des fonctions métier non stratégiques comme la gestion de la relation client (CRM), la paie ou la comptabilité.

Caractéristiques du SaaS: Le modèle Software as a Service (SaaS) propose des applications entièrement hébergées et accessibles via Internet, ce qui le distingue fondamentalement des logiciels installés localement. Les services SaaS présentent plusieurs caractéristiques essentielles qui expliquent leur adoption massive par les utilisateurs professionnels et particuliers.

- Architecture multi-tenant: Une même instance applicative peut être utilisée simultanément par plusieurs organisations ou utilisateurs, chaque client disposant de son propre espace logique isolé. Ce modèle permet une mutualisation efficace des ressources.

- Accessibilité via le Web: Les applications sont disponibles à travers un navigateur Web, ce qui permet une utilisation depuis n'importe quel lieu, à condition d'avoir une connexion Internet.

- Compatibilité multi-appareils: Les services SaaS peuvent être consultés à partir d'une grande variété de terminaux : ordinateurs fixes, ordinateurs portables, tablettes, smartphones ou clients légers.

- Évolutivité élevée: Puisque les applications SaaS reposent sur des plateformes PaaS et des infrastructures IaaS, elles bénéficient d'une capacité de montée en charge rapide et adaptative.

- Haute disponibilité: Les fournisseurs SaaS garantissent généralement une disponibilité continue (souvent supérieure à 99,9%), grâce à des mécanismes avancés de sauvegarde, réplication et restauration.

- Interopérabilité: Les applications SaaS peuvent s'intégrer avec d'autres services logiciels via des API standard, facilitant les échanges de données et l'automatisation des processus.

Cas d'usage recommandés: Le SaaS constitue une solution pertinente dans plusieurs situations:

- **Applications à la demande:** Idéal pour les organisations souhaitant utiliser un logiciel de manière ponctuelle sans supporter le coût d'une licence permanente.

- **Startups à budget limité:** Le SaaS supprime la nécessité d'investir dans des infrastructures matérielles ou des licences coûteuses.

- **Applications multi-appareils:** Son accessibilité universelle le rend adapté à des environnements où les utilisateurs travaillent sur des terminaux variés.

- **Charges variables:** Grâce à son élasticité, le SaaS permet de gérer efficacement les fluctuations importantes de trafic, comme dans les réseaux sociaux ou les services à forte audience.

Situations où le SaaS est moins adapté: Certains cas d'usage peuvent rendre le SaaS inapproprié:

- **Applications en temps réel sensibles à la latence:** La dépendance à la connexion Internet peut entraîner des performances insuffisantes lorsque le débit est faible.

- **Traitement de données hautement confidentielles:** Les contraintes de sécurité, de conformité ou de gouvernance peuvent limiter l'adoption du SaaS dans certaines organisations.

- **Applications locales déjà adaptées:** Lorsque les solutions internes satisfont pleinement les besoins de l'organisation, la migration vers le SaaS peut ne pas apporter de bénéfices supplémentaires.

Avantages

1. **Aucune installation requise:** Les applications sont opérationnelles immédiatement via un navigateur.
2. **Réduction des coûts:** Le modèle de facturation à l'usage permet de payer uniquement les ressources consommées.
3. **Maintenance réduite:** Les mises à jour, correctifs et opérations de maintenance sont entièrement gérés par le fournisseur.
4. **Accessibilité:** Les services sont disponibles depuis n'importe quel appareil connecté.
5. **Élasticité:** Les applications SaaS peuvent s'adapter automatiquement aux variations de charge.
6. **Reprise après sinistre:** Les mécanismes intégrés de sauvegarde et de réplication assurent une restauration rapide en cas d'incident.
7. **Mutualisation des ressources:** Le modèle multi-tenant optimise les coûts et permet un partage efficace de l'infrastructure.

Limites

1. **Préoccupations de sécurité :** Le stockage des données chez un fournisseur tiers peut créer un risque potentiel de divulgation ou d'accès non autorisé.
2. **Dépendance à la connectivité Internet :** Une connexion instable ou lente réduit fortement la qualité d'utilisation.
3. **Moindre contrôle sur les données :** Les utilisateurs ne disposent pas d'un accès direct à l'infrastructure et doivent se conformer aux politiques du fournisseur.

Choix du modèle de service

Le choix entre IaaS, PaaS et SaaS (Table 2.2) est avant tout stratégique. Il dépend:

- des compétences techniques internes;
- du besoin de contrôle et de personnalisation;
- de la rapidité de mise sur le marché souhaitée.

Table 2.2: Synthèse comparative des modèles de service Cloud

Critère	**IaaS**	**PaaS**	**SaaS**
Niveau de contrôle pour le client	Élevé	Moyen	Faible
Compétences techniques requises	Élevées (gestion de SE, middleware, BD)	Moyennes (développement)	Faibles (utilisation simple)
Rapidité de mise sur le marché	Lente	Rapide	Immédiate
Cas d'usage typique	Hébergement d'infrastructure	Développement d'applications	Utilisation de logiciels métiers

Chaque modèle représente un compromis entre flexibilité, simplicité et contrôle. Le rôle du décideur consiste à aligner le modèle choisi avec les priorités stratégiques et opérationnelles de l'entreprise.

2.2 Les Modèles de Déploiement

Outre le modèle de service, une organisation doit également choisir un modèle de déploiement, qui détermine où et comment les ressources cloud sont provisionnées: cloud privé, public, hybride ou communautaire.

Le Cloud Privé

Selon le NIST:

> *The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned,*

managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Selon le NIST, le cloud privé (Figure 2.3) est une infrastructure destinée à un usage exclusif au sein d'une même organisation. Elle peut être hébergée sur site ou hors site, et être gérée par l'organisation elle-même, par un prestataire externe ou par les deux. Ce modèle est souvent déployé à l'aide de solutions open source telles qu'OpenStack ou Eucalyptus. Le cloud privé est généralement de plus petite taille que les autres modèles et son déploiement, ainsi que sa maintenance, sont directement assurés par l'organisation. Ce modèle offre un contrôle total, adapté aux environnements soumis à des contraintes de conformité. En revanche, l'élasticité et la mutualisation sont réduites, ce qui diminue l'efficacité économique.

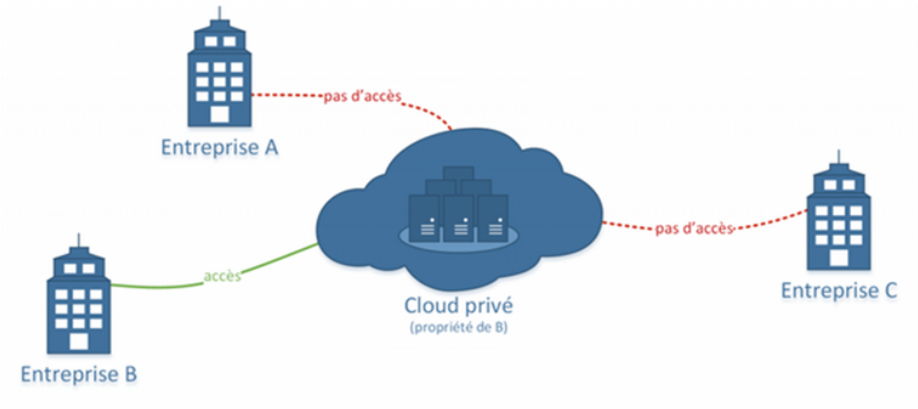

Figure 2.3: Cloud privé

Caractéristiques: Certaines caractéristiques du cloud privé sont les suivantes:

- **Sécurité:** Le cloud privé est sécurisé car il est généralement déployé et géré par l'organisation. Par conséquent, il y a moins de risques de fuite de données hors du cloud. De plus, tous les utilisateurs appartiennent à la même organisation.
- **Contrôle centralisé:** Étant donné que l'organisation a le contrôle total sur le cloud, elle n'a pas besoin de ressources externes pour le gérer.
- **Faible SLA:** Les SLA formels peuvent ne pas exister dans un cloud privé. Lorsqu'ils

existent, ils sont généralement faibles puisqu'ils concernent l'organisation et ses employés. De plus, la qualité de service n'est pas toujours optimale.

Pertinence: La pertinence signifie les conditions et l'environnement les plus appropriés dans lesquels ce modèle de cloud peut être utilisé. Le cloud privé est pertinent lorsque:

- L'organisation dispose des moyens nécessaires (fonds, matériel et locaux) pour le déploiement du cloud.
- L'organisation dispose d'un personnel qualifié pour la gestion et la maintenance du cloud.
- La sécurité des données est considérée comme importante ou critique.
- L'organisation souhaite un contrôle complet sur le cloud.

Le cloud privé n'est pas recommandé dans les cas suivants:

- L'organisation a des contraintes financières.
- L'organisation ne dispose pas de suffisamment de main-d'œuvre pour maintenir et gérer le cloud.
- L'organisation ne possède pas une infrastructure préétablie.

Avantages

- Le cloud est de taille limitée et facile à entretenir.
- Il offre un niveau élevé de sécurité et de confidentialité.
- Il est entièrement contrôlé par l'organisation.

Limites

- Les SLA peuvent ne pas être respectés et le service peut ne pas être optimal.
- Contraintes budgétaires pour les petites entreprises.

Le Cloud Public

Selon le NIST:

> *The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.*

Selon le NIST, le cloud public (Figure 2.4) est une infrastructure ouverte au grand public, pouvant être détenue et exploitée par une entreprise, une institution académique ou un organisme gouvernemental. Elle est hébergée dans les centres de données du fournisseur. Ce modèle permet aux utilisateurs de louer, à la demande et souvent à l'heure, des ressources telles que des serveurs, du stockage, du réseau ou des logiciels. Les fournisseurs traitent généralement toutes les requêtes, donnant ainsi l'impression d'une disponibilité quasi illimitée des ressources. Parmi les principaux fournisseurs de cloud public figurent Amazon AWS et Microsoft Azure.

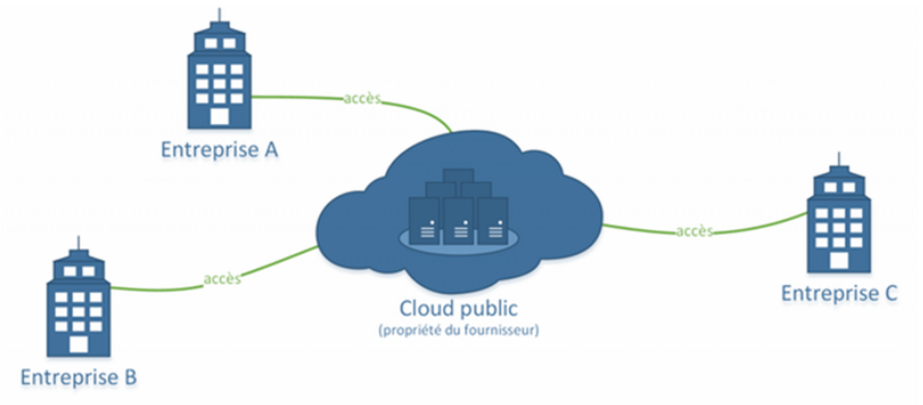

Figure 2.4: Cloud public

Caractéristiques: On peut caractériser le cloud public par:

- **Évolutivité:** Le cloud public est hautement évolutif et l'approvisionnement des ressources passe à l'échelle rapidement. Le fournisseur doit garantir que toutes les demandes des utilisateurs sont satisfaites.

- **Abordable:** Les services du cloud public sont fournis selon le modèle *pay-as-you-go*. L'utilisateur paie uniquement ce qu'il consomme (souvent à l'heure), sans frais liés au déploiement.
- **Moins sécurisé :** Le cloud public est moins sécurisé que les autres modèles, car il est géré par un tiers ayant le contrôle total de l'infrastructure. Malgré les SLA garantissant la confidentialité, le risque de fuite de données demeure plus élevé.
- **Haute disponibilité :** Le cloud public est hautement disponible, car toute personne disposant des autorisations nécessaires peut y accéder depuis n'importe quel endroit, sans contraintes géographiques.
- **SLA strict :** Les fournisseurs de cloud public respectent strictement les SLA, car leur réputation dépend directement de la qualité du service offert.

Pertinence Le cloud public est particulièrement adapté dans les situations suivantes:

- Les besoins en ressources sont importants et variables.
- Aucune infrastructure physique n'est disponible.
- L'entreprise fait face à des contraintes financières.

En revanche, le cloud public n'est pas approprié lorsque :

- La sécurité des données est critique.
- L'organisation souhaite une autonomie totale.
- L'organisation dispose des moyens nécessaires pour mettre en place un cloud privé.

Avantages

- Aucune infrastructure n'a besoin d'être acquise ou installée.
- Pas de maintenance à assurer, celle-ci étant prise en charge par le fournisseur.
- Coût inférieur par rapport aux autres modèles.

- Respect strict des SLA.
- Aucun nombre limite d'utilisateurs.
- Passage à l'échelle rapide.

Les limites

- Problèmes de sécurité plus importants.
- Manque de confidentialité et absence d'autonomie organisationnelle.

Le Cloud communautaire

Selon le NIST, le cloud communautaire (Figure 2.5) est une infrastructure partagée par une communauté spécifique d'organisations ayant des intérêts communs. Il peut être géré par un ou plusieurs membres de la communauté et représente une extension du cloud privé mutualisé entre plusieurs entités.

Son principal avantage réside dans le partage des ressources, permettant aux organisations de bénéficier d'une puissance de calcul supérieure à celle d'un cloud privé, tout en réduisant les coûts. Ce modèle est particulièrement adapté aux organisations qui ne peuvent pas se permettre un cloud privé mais ne souhaitent pas non plus recourir entièrement à un cloud public.

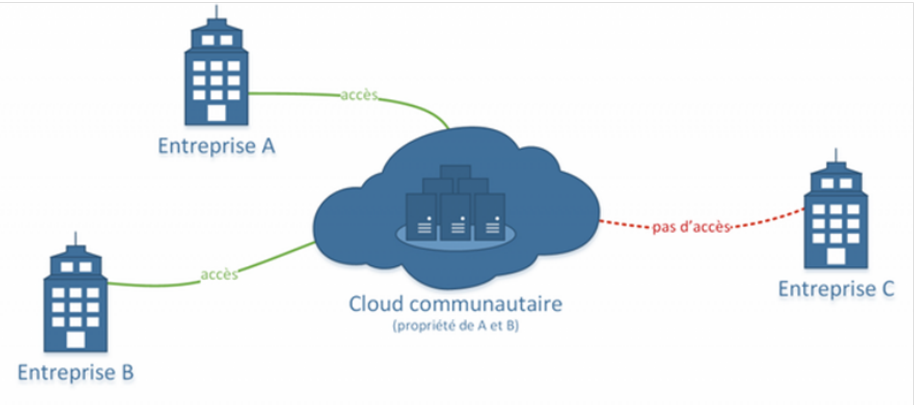

Figure 2.5: Cloud communautaire

Caractéristiques: Le cloud communautaire se distingue par les points suivants:

- **Maintenance collaborative et distribuée:** La gestion du cloud est partagée entre plusieurs organisations, et aucune partie n'a le contrôle total. Une coopération efficace entre les membres améliore la performance et la fiabilité du cloud.
- **Sécurité partielle:** Bien que les données soient protégées contre l'extérieur, le partage entre plusieurs organisations peut présenter un risque de divulgation interne.
- **Rentabilité:** Les coûts et les responsabilités de maintenance sont mutualisés entre les organisations de la communauté, ce qui réduit les dépenses par rapport à un cloud privé individuel.

Pertinence: Le cloud communautaire est adapté aux organisations qui:

- Souhaitent mettre en place un cloud privé mais disposent de contraintes financières.
- Préfèrent ne pas assumer entièrement la maintenance et la gestion.
- Veulent collaborer avec d'autres clouds ou organisations.
- Cherchent une solution plus sécurisée qu'un cloud public.

Il est moins approprié pour les organisations qui:

- Privilégient l'autonomie et le contrôle complet du cloud.
- Ne souhaitent pas collaborer avec d'autres organisations.

Avantages

- Permet de disposer d'un cloud privé à moindre coût.
- Favorise le travail collaboratif entre organisations.
- Mutualise les responsabilités de gestion et de maintenance.
- Offre une sécurité supérieure à celle du cloud public.

Les limites

- L'organisation perd une partie de son autonomie.
- La sécurité n'atteint pas le niveau d'un cloud privé.
- Inefficace si la collaboration n'est pas possible.

Le Cloud Hybride

Le cloud hybride, selon le NIST, est une infrastructure composée de deux ou plusieurs types de clouds distincts (privé, public ou communautaire) interconnectés via des technologies standardisées ou propriétaires pour permettre la portabilité des données et des applications.

Il combine généralement clouds publics et privés afin de tirer parti de la puissance et de l'évolutivité du cloud public tout en conservant le contrôle et la sécurité propres au cloud privé.

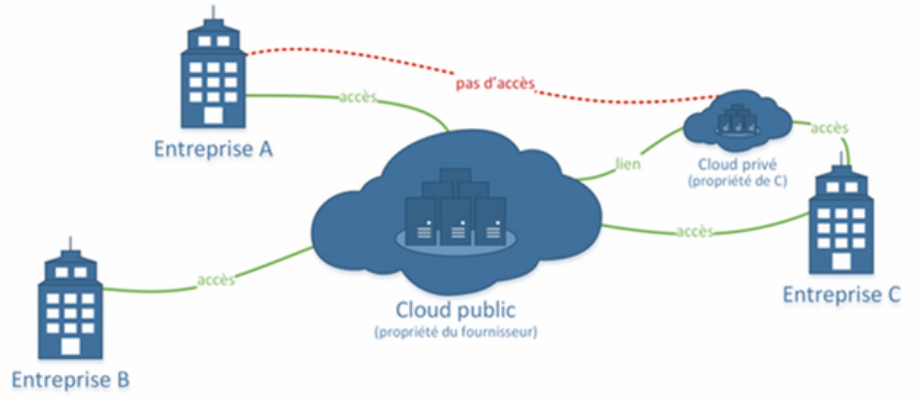

Figure 2.6: Cloud hybride

Caractéristiques: Le cloud hybride présente les caractéristiques suivantes:

- **Évolutivité:** Le cloud hybride tire parti de l'élasticité du cloud public lorsqu'il est intégré à un environnement privé, permettant ainsi d'ajuster les ressources en fonction des besoins.
- **Sécurité partielle:** Étant donné que le cloud hybride fait souvent appel au cloud public, le niveau de sécurité est inférieur à celui d'un cloud privé et ne peut être considéré comme totalement sécurisé.

- **SLA stricts:** L'intervention du cloud public impose le respect rigoureux des SLA afin de garantir la qualité du service.

- **Gestion complexe:** La supervision du cloud hybride est plus difficile en raison de la coexistence de plusieurs modèles de déploiement et du nombre élevé d'utilisateurs.

Pertinence: Le cloud hybride est recommandé pour:

- Les organisations désirant combiner la sécurité d'un cloud privé avec l'évolutivité d'un cloud public.

- Les organisations nécessitant un niveau de sécurité intermédiaire tout en bénéficiant de ressources supplémentaires à la demande.

Il est moins approprié pour:

- Les organisations qui considèrent la sécurité comme une priorité absolue.

- Les structures incapables d'assurer la gestion et la maintenance d'une infrastructure hybride.

Avantages

- Combine les bénéfices du cloud privé et du cloud public.

- Offre une grande évolutivité grâce à l'intégration du cloud public.

Les limites

- La sécurité n'atteint pas le niveau d'un cloud privé.

- La gestion et la maintenance de l'infrastructure hybride sont complexes.

2.3 Accords de niveau de service (SLA)

Un SLA (*Service Level Agreement*) est un contrat formel entre le fournisseur de services cloud et le client, qui définit les niveaux de qualité et de performance attendus pour les services fournis. Il sert de référence pour mesurer la fiabilité et la disponibilité des services cloud.

Objectifs principaux d'un SLA

- **Disponibilité:** Garantir que les services cloud seront accessibles et opérationnels selon un pourcentage défini.
- **Performance:** Définir les temps de réponse et la capacité de traitement que le fournisseur s'engage à respecter.
- **Sécurité et confidentialité:** Spécifier les mesures de protection des données, la gestion des accès et la conformité réglementaire.
- **Support et maintenance:** Préciser les délais d'assistance technique, les procédures de résolution des incidents et la fréquence des mises à jour.
- **Pénalités:** Définir les compensations ou remises appliquées si le fournisseur ne respecte pas les engagements du SLA.

Importance des SLA selon le type de cloud

- **Cloud public:** Les SLA sont généralement stricts, car le fournisseur est responsable devant un grand nombre de clients.
- **Cloud privé:** Les SLA peuvent être moins formalisés et adaptés aux besoins internes de l'organisation.
- **Cloud communautaire:** Les SLA dépendent de la coopération entre les membres et des objectifs partagés.

- **Cloud hybride:** La complexité des SLA augmente en raison de la combinaison de plusieurs modèles de cloud et de fournisseurs.

Bénéfices d'un SLA

- Clarifie les attentes entre le fournisseur et le client.
- Sert de référence pour évaluer la qualité du service.
- Permet de gérer les risques et les responsabilités.
- Facilite la prise de décision lors du choix d'un fournisseur cloud.

Conclusion

Ce chapitre a présenté les principaux modèles de services cloud (IaaS, PaaS, SaaS) ainsi que les modèles de déploiement (privé, public, communautaire et hybride). Chaque modèle présente des caractéristiques propres, des avantages et des limites, qui répondent à différents besoins des organisations en termes de sécurité, flexibilité, coût et évolutivité.

Les SLA jouent un rôle central dans la relation entre les fournisseurs et les utilisateurs, en garantissant la qualité, la disponibilité et la sécurité des services cloud. Leur importance varie selon le type de cloud et la criticité des applications.

LEn effet, le choix du modèle de service et du modèle de déploiement doit être guidé par les besoins spécifiques de l'organisation, la sensibilité des données, les contraintes budgétaires et les objectifs en termes de performance et d'évolutivité. Une bonne compréhension de ces modèles permet aux organisations de tirer pleinement parti des avantages du cloud tout en maîtrisant les risques associés.

Chapitre 3

Architecture et management du Cloud Computing

Introduction

Avec l'adoption croissante du cloud computing à l'échelle mondiale, comprendre son architecture et sa gestion est devenu essentiel pour les organisations. L'architecture cloud définit la structure et le fonctionnement des ressources et services cloud, en précisant la manière dont les utilisateurs finaux accèdent aux services et comment les fournisseurs assurent leur disponibilité et leur performance.

Ce chapitre se concentre sur l'analyse de l'architecture cloud sous forme de couches, en distinguant le front-end et le back-end, et en détaillant les composants clés nécessaires au fonctionnement efficace du cloud. Par ailleurs, il aborde la gestion du cloud, en présentant les stratégies, outils et plateformes utilisés pour superviser les ressources, assurer la qualité de service (QoS), optimiser les performances et garantir la sécurité.

L'objectif est de fournir une vision de l'architecture et de la gestion du cloud, afin de mieux comprendre comment les services cloud sont provisionnés, maintenus et optimisés dans différents environnements.

3.1 Architecture du cloud

L'architecture du cloud décrit le fonctionnement interne du cloud computing. Elle regroupe l'ensemble des composants essentiels assurant la mise à disposition des services cloud aux utilisateurs finaux. Dans cette section, nous étudierons l'architecture en couches, puis nous présenterons les parties front-end et back-end, avant de conclure par différentes formes d'architectures cloud.

Architecture front-end et back-end

De manière simplifiée, on distingue deux extrémités dans l'architecture cloud (Figure 3.1): le front-end (l'interface utilisateur) et le back-end (l'infrastructure du fournisseur). Ces deux extrémités sont reliées par internet, l'élément central du cloud computing. Le schéma ci-dessous illustre cette séparation.

Front-end: Le front-end de l'architecture cloud regroupe les applications et interfaces utilisées pour accéder aux services cloud. Il comprend principalement les équipements matériels connectés à Internet (ordinateurs de bureau, portables, tablettes, smartphones) ainsi que les navigateurs web (par exemple, Microsoft Edge, Google Chrome, Firefox) permettant d'initier l'accès.

Back-end: Le back-end englobe plusieurs composants essentiels:

- **Applications:** ce sont les logiciels ou plateformes que le client utilise via le cloud.
- **Services:** ils fournissent des fonctionnalités comme le stockage, des environnements de développement ou des services web.
- **Stockage:** il héberge et maintient les données clients (fichiers, images, vidéos, etc.). Les services de stockage cloud les plus populaires sont Google Drive, One Drive, Dropbox, etc.

- **Gestion:** elle assure la coordination entre tous les composants de l'environnement cloud.
- **Sécurité:** élément central, elle protège l'ensemble des ressources cloud contre les risques d'attaque ou de fuite.

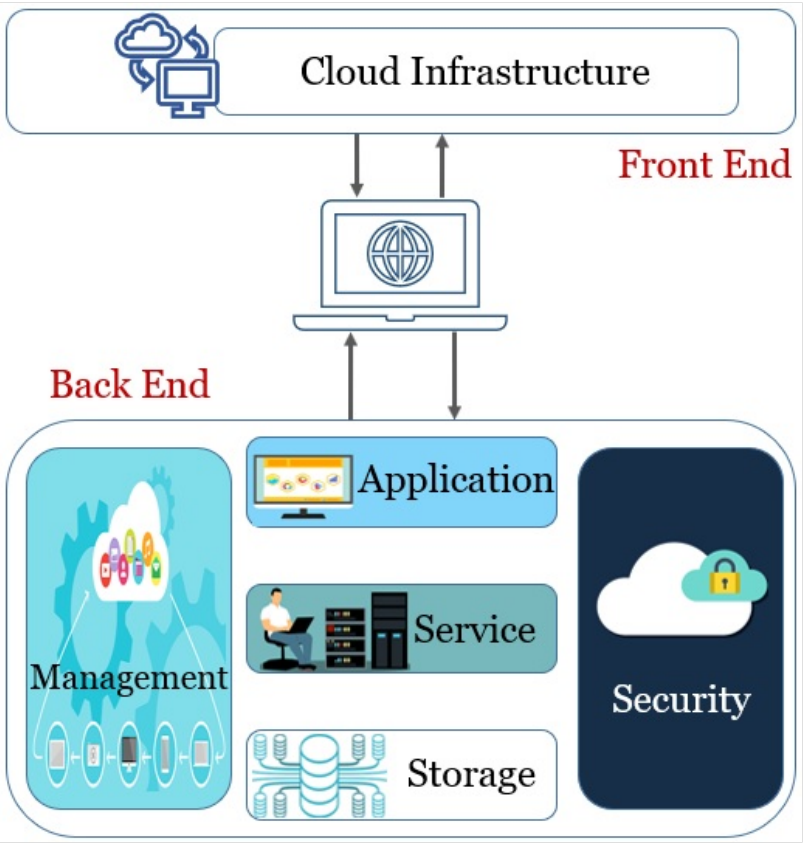

Figure 3.1: L'architecture front-end & back-end du cloud

Architecture en couches

L'architecture du cloud peut être décomposée en couches (Figure 3.2), selon le niveau d'accès et de contrôle:

Couche 1: Couche utilisateur / client

Il s'agit de la couche la plus élevée de l'architecture cloud. Elle regroupe les acteurs finaux: les utilisateurs et les dispositifs clients. Ces dispositifs peuvent être des clients épais - thick client - (ordinateurs dotés d'une capacité de traitement autonome), des clients légers - thin

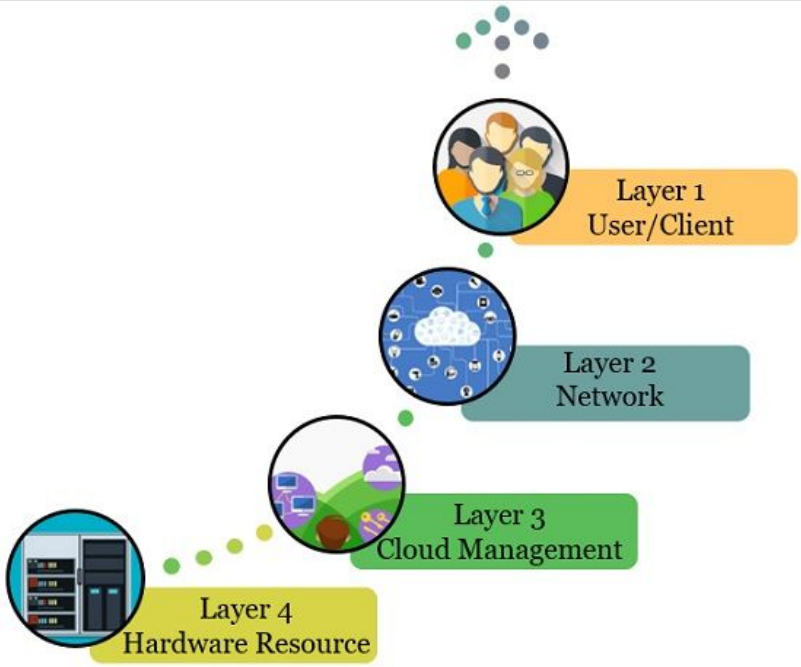

Figure 3.2: L'architecture en couches du cloud

client (terminaux avec peu de capacité de calcul, dépendants d'un serveur) ou des appareils mobiles permettant l'accès à des applications web.

C'est à ce niveau que l'utilisateur ou le client initie la connexion aux services cloud. L'accès aux applications cloud s'apparente à celui des applications web classiques, bien que l'architecture sous-jacente soit différente. L'accès requiert une connexion réseau (Internet ou autre) entre le client et la plateforme cloud. La couche 1 établit donc le point d'entrée entre l'utilisateur et l'ensemble de l'infrastructure cloud.

Couche 2: Couche réseau

La couche réseau assure l'établissement de la connexion entre les utilisateurs et l'infrastructure cloud. Sans cette couche, aucun service ne pourrait être fourni, car l'accès aux ressources dépend entièrement d'un lien de communication opérationnel. Dans le cas d'un cloud public, la connexion s'effectue généralement via Internet, tandis que dans un cloud privé, l'accès repose le plus souvent sur un réseau local (LAN). Dans tous les cas, une bande passante minimale, définie par le fournisseur ou par l'organisation, est nécessaire pour garantir un fonctionnement correct.

Il est important de noter que cette couche n'entre pas dans le périmètre direct de

l'accord de niveau de service (SLA). En effet, le SLA encadre la qualité des services fournis par le cloud, mais ne couvre pas la qualité de la connexion réseau entre l'utilisateur et la plateforme, qui peut varier selon l'environnement et les infrastructures locales.

Couche 3: Couche de gestion du cloud

Cette couche regroupe l'ensemble des logiciels et mécanismes dédiés à l'administration des services cloud. Elle assure la coordination, la supervision et l'optimisation de l'infrastructure sous-jacente. Plusieurs catégories d'outils peuvent intervenir à ce niveau :

- **Systèmes d'exploitation cloud (Cloud OS)** permettant d'établir l'interface entre l'infrastructure et les utilisateurs.
- **Logiciels de gestion des ressources** prenant en charge l'allocation, l'ordonnancement et le provisionnement des services.
- **Outils d'orchestration et de supervision** facilitant la visibilité, le suivi et l'automatisation des opérations cloud.

Les responsabilités principales de cette couche incluent :

- **Gestion des ressources** : planification des tâches, distribution de la charge, allocation dynamique des machines virtuelles et des services.
- **Optimisation de l'infrastructure** :
  - consolidation des serveurs (réduction du nombre de serveurs physiques inutilisés),
  - consolidation des charges de travail (regroupement de plusieurs opérations sur un nombre réduit de plateformes),
  - centralisation du stockage pour accélérer l'accès aux données.
- **Gouvernance interne** : contrôle des politiques internes, administration de la sécurité et conformité aux exigences contractuelles.

Cette couche est étroitement liée aux engagements définis par les *Service Level Agreements* (SLA). Toute défaillance dans la gestion — par exemple un retard dans la mise à disposition d'une ressource ou une mauvaise orchestration — peut entraîner une violation du SLA. Dans ce cas, le fournisseur est tenu d'appliquer les compensations prévues contractuellement.

Couche 4 : Couche des ressources matérielles

Cette couche correspond à l'ensemble des ressources matérielles nécessaires au fonctionnement du cloud. Dans un cloud public, elle prend généralement la forme de vastes centres de données répartis géographiquement. Dans un cloud privé, elle repose plutôt sur une infrastructure matérielle regroupée au sein de l'organisation et interconnectée localement ou via un système informatique de haute performance.

La couche matérielle relève directement des *Service Level Agreements* (SLA), car elle détermine la capacité du fournisseur à fournir les services dans les délais garantis. Une défaillance dans la mise à disposition d'un serveur, d'un stockage ou d'un lien réseau peut entraîner une non-conformité contractuelle et donc des pénalités pour le fournisseur. Pour répondre à ces exigences, un centre de données doit disposer:

- d'une connectivité réseau à très haut débit ;
- de mécanismes d'optimisation permettant un transfert rapide et fiable des données;
- d'algorithmes de gestion performants facilitant;
- la communication entre les ressources matérielles et les couches de gestion.

Un même fournisseur peut exploiter plusieurs centres de données pour un seul cloud, et il est également possible que plusieurs clouds partagent une même infrastructure physique. Bien que la séparation entre la couche de gestion (couche 3) et la couche matérielle puisse varier selon les architectures implémentées, la présence de cette couche matérielle reste indispensable pour garantir les performances attendues et le respect des engagements contractuels.

Cette architecture en couches permet de visualiser clairement comment un service cloud est accessible depuis l'utilisateur (front-end), comment il est géré (couches intermédiaires) et comment il est soutenu par l'infrastructure physique (back-end). Chaque couche joue un rôle essentiel pour garantir la disponibilité, la performance, la sécurité et l'élasticité des services cloud.

3.2 Management du cloud

La gestion du cloud computing désigne l'ensemble des processus qui visent à piloter les ressources cloud afin d'assurer la qualité des services (QoS, *Quality of Service*). Avec l'adoption croissante du cloud à l'échelle mondiale, il devient indispensable de mettre en œuvre une gouvernance adaptée. L'objectif principal est d'assurer un fonctionnement fluide et fiable des services offerts.

La gestion du cloud désigne l'ensemble des outils, processus et stratégies permettant d'administrer, superviser et optimiser les environnements cloud, qu'ils soient publics, privés ou hybrides. Elle vise à garantir la performance, la sécurité, la disponibilité et la conformité des services cloud. Selon le National Institute of Standards and Technology, la gestion du cloud implique le contrôle et l'orchestration des ressources de calcul, de stockage, de réseau et des applications déployées dans le cloud. La gestion du cloud couvre principalement deux dimensions: la *gestion de l'infrastructure* cloud et la *gestion des applications* cloud.

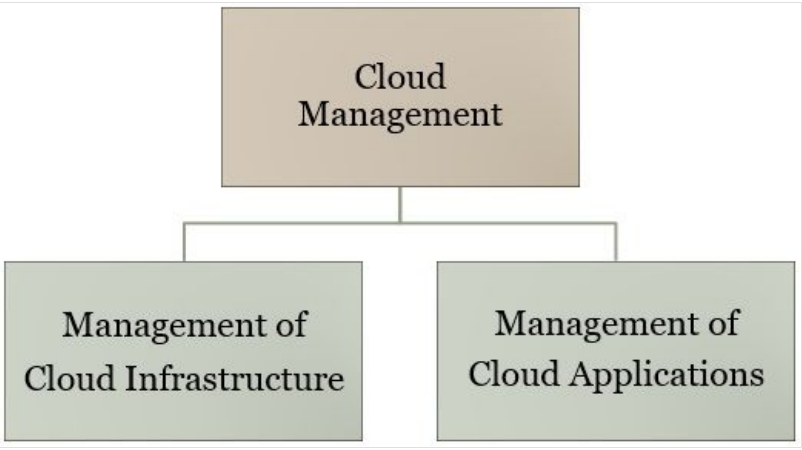

Figure 3.3: La gestion du cloud

Gestion de l'infrastructure Cloud

Toute solution informatique nécessite une infrastructure pour fonctionner. La qualité des services fournis par le cloud dépend directement de la performance et de la bonne gestion de cette infrastructure. Par conséquent, sa gestion devient un élément central pour garantir un niveau de service satisfaisant. Selon le NIST, une infrastructure cloud regroupe un ensemble de ressources de calcul, de stockage et de réseau, dont la gestion conditionne la performance globale du cloud. L'infrastructure cloud est composée d'un grand nombre de ressources interdépendantes, ce qui en fait un système complexe. Les fournisseurs de services cloud ont la responsabilité d'administrer ces ressources, notamment grâce aux systèmes d'exploitation cloud (Cloud OS). Ces derniers assurent la gestion fondamentale des ressources, incluant:

- **l'ordonnancement des ressources** (resource scheduling) ;
- **le provisionnement des ressources** (resource provisioning) ;
- **l'équilibrage de charge** (load balancing).

Ces ressources sont partagées simultanément par un très grand nombre d'utilisateurs à travers le monde. Dès lors, une gestion inadéquate conduirait à :

- une dégradation des performances ;
- un impact négatif sur le fonctionnement des applications ;
- une augmentation des coûts d'exploitation.

Avant l'utilisation des services cloud, un contrat SLA (Service Level Agreement) est établi entre l'utilisateur et le fournisseur. Ce SLA définit les niveaux de performance, de disponibilité et de qualité de service auxquels le fournisseur s'engage. Le respect de ces engagements repose en grande partie sur la bonne gestion de l'infrastructure. Si les fonctionnalités promises ne sont offertes que partiellement, le SLA est considéré comme non respecté.

Enfin, le coût constitue un facteur essentiel dans l'adoption massive du cloud. Les économies réalisées grâce à la mutualisation, l'automatisation et l'évolutivité sont au cœur de son succès mondial. Ainsi, plus les fournisseurs parviennent à réduire les coûts de gestion de l'infrastructure tout en maintenant des performances élevées, plus ils renforcent leur base d'utilisateurs

Gestion des applications Cloud

Un nombre croissant d'entreprises migrent leurs applications vers des plateformes cloud afin d'étendre leur présence à l'échelle mondiale. Toutefois, cette migration introduit une complexité supplémentaire, ce qui rend indispensable la gestion des applications déployées dans le cloud.

La gestion des applications cloud implique plusieurs activités majeures, parmi lesquelles:

- **l'analyse de l'infrastructure d'accueil** afin de vérifier qu'elle répond aux exigences techniques de l'application;
- **l'identification et la supervision des services cloud consommés** (stockage, bases de données, API, environnements d'exécution, etc.);
- **la mise à jour et l'évolution de l'application** pour garantir sa sécurité, sa compatibilité et sa performance.

La gestion des applications doit également s'appuyer sur un ensemble d'outils et de processus permettant d'administrer les environnements connexes qui coexistent avec le cloud (outils de monitoring, systèmes CI/CD, solutions de sécurité, gestion des dépendances). L'objectif est de garantir un fonctionnement optimal, une cohérence entre les versions des composants, ainsi qu'un niveau de service conforme aux attentes des utilisateurs.

Ainsi, la gestion des applications cloud constitue un pilier essentiel du maintien de la qualité de service, du respect des engagements contractuels (SLA) et de la performance globale de l'écosystème cloud.

3.3 Stratégies de gestion du Cloud

La gestion efficace d'un environnement cloud nécessite la mise en place de stratégies adaptées visant à assurer le bon fonctionnement des services et le respect de la qualité de service (QoS). Ces stratégies incluent notamment:

- **Surveillance régulière**: Le personnel informatique doit suivre en permanence le fonctionnement de l'infrastructure cloud. La surveillance peut être effectuée manuellement ou de manière automatisée à l'aide d'outils de monitoring.

- **Audit des services**: Les entreprises procèdent à des audits afin d'évaluer et de documenter la performance de leur fournisseur cloud. Ces audits permettent de vérifier que le prestataire respecte les engagements contractuels et fournit un service optimal. Le *Cloud Security Alliance (CSA)* fournit des guides et des contrôles pour la réalisation de ces audits.

- **Gestion des plans de reprise après sinistre (Disaster Recovery)**: La continuité des services est assurée par des méthodes de prévention et de récupération. Les entreprises mettent en place des systèmes de sauvegarde robustes et utilisent plusieurs serveurs répartis dans différentes régions pour garantir la redondance des données.

Plateformes de gestion cloud: Les *Cloud Management Platforms (CMP)* permettent de superviser et de contrôler toutes les opérations cloud depuis une interface unique. Ces plateformes offrent des fonctionnalités telles que:

- Gouvernance et suivi des ressources,

- Gestion du cycle de vie des services cloud,

- Automatisation de la surveillance et de l'administration des ressources,

- Outils et processus pour interagir avec différents services cloud.

Parmi les solutions CMP les plus reconnues actuellement, on peut citer: BMC Cloud Lifecycle Management, Cisco CloudCenter, Embotics, Flexera RightScale, Hypergrid, Morpheus Data, Red Hat CloudForms, Scalr, et VMware CloudHealth.

Ces stratégies et outils permettent aux entreprises de maintenir un haut niveau de QoS tout en optimisant les ressources cloud et en réduisant les risques opérationnels.

3.4 Migration des applications vers le Cloud

La migration vers le Cloud consiste à transférer une ou plusieurs applications d'une entreprise ainsi que leurs environnements informatiques associés depuis un hébergement traditionnel vers une infrastructure Cloud, qu'elle soit privée, publique ou hybride. Cette démarche permet non seulement de bénéficier de l'élasticité et de l'évolutivité offertes par le Cloud, mais elle contribue également à une réduction significative des coûts liés à l'exploitation et à la maintenance des applications.

Phases de migration

La migration des applications vers le Cloud peut se décomposer en plusieurs phases:

1- Évaluation La première étape consiste à analyser l'environnement existant, y compris les applications, les données et les infrastructures. Il s'agit d'identifier les dépendances, les contraintes techniques et les exigences de performance pour déterminer quelles applications sont adaptées au Cloud. Cette phase inclut également l'analyse des risques liés à la migration et des bénéfices potentiels en termes de coûts, de sécurité et de scalabilité.

2- Stratégie de migration Après l'évaluation, il est nécessaire de définir une stratégie de migration adaptée. Cette stratégie détermine le type de Cloud cible (privé, public ou hybride), le modèle de service à utiliser (IaaS, PaaS ou SaaS), ainsi que les méthodes de migration (réhébergement, refactorisation, replatforming ou remplacement complet). La planification doit inclure les priorités, le calendrier, le budget et les ressources nécessaires.

3- Prototypage Le prototypage consiste à réaliser une migration pilote d'une application ou d'un ensemble limité d'applications. Cette phase permet de tester la faisabilité, d'identifier les problèmes techniques et d'ajuster la stratégie de migration avant un déploiement à grande échelle. Elle permet également d'estimer les performances dans l'environnement Cloud et d'affiner les paramètres de sécurité et de disponibilité.

4- Approvisionnement L'approvisionnement implique la préparation de l'environnement Cloud cible pour accueillir les applications. Cela inclut la configuration des ressources matérielles et logicielles, la mise en place des services nécessaires, la sécurisation des accès et la préparation des outils de gestion et de monitoring. Un approvisionnement adéquat garantit une transition fluide et minimise les interruptions de service.

5- Test La dernière phase consiste à effectuer des tests complets pour s'assurer que les applications migrées fonctionnent correctement dans le nouvel environnement. Les tests incluent la validation des performances, de la sécurité, de la compatibilité et de l'intégrité des données. Cette étape permet également de vérifier le respect des engagements définis dans le SLA et de s'assurer que les utilisateurs finaux disposent de la même qualité de service, voire améliorée, après la migration.

Approche de la migration

Les fournisseurs de services Cloud adoptent généralement plusieurs approches pour migrer des applications vers le Cloud. Ces approches dépendent des objectifs de l'entreprise, de la complexité des applications existantes et des ressources disponibles.

1- Migration des applications existantes: Cette approche consiste à transférer les applications déjà en fonctionnement vers le Cloud en tirant parti des technologies de virtualisation et de conteneurisation. Bien que cette méthode permette d'accélérer la migration, elle nécessite un important travail d'ingénierie pour adapter les applications et développer éventuellement de nouvelles fonctionnalités pour les rendre pleinement compatibles avec l'environnement Cloud.

3.4.0.0.1 2- Développement à partir de zéro: Certaines organisations choisissent de concevoir de nouvelles applications directement pour le Cloud. Avec des environnements de développement avancés et des outils Cloud natifs, il est possible de créer des applications performantes même avec une équipe réduite. Cette approche garantit que l'architecture logicielle est optimisée pour l'élasticité, la scalabilité et la maintenance dans le Cloud.

3.4.0.0.2 3- Création d'une nouvelle entité Cloud: Une autre stratégie consiste à établir une entreprise ou une filiale entièrement nouvelle, distincte de l'organisation existante, avec sa propre marque, sa gestion et ses processus commerciaux. Cette entité fonctionne comme une start-up native du Cloud, ce qui permet d'exploiter pleinement les avantages du Cloud dès la conception, notamment en termes d'innovation, de flexibilité et d'agilité opérationnelle.

Acteurs principaux de la migration vers le Cloud

Plusieurs acteurs interviennent dans le processus de migration vers le Cloud, chacun ayant un rôle précis pour assurer le succès de la transition:

1. **Cloud Service Users (CSUs)**: Client / Utilisateur final consommant les services Cloud. Exemples : individus, entreprises, administrations.

2. **Cloud Service Providers (CSPs)**: fournissent, livrent et maintiennent/ gèrent les services Cloud (ex. : AWS, Azure, Google Cloud).

3. **Cloud Service Partners (CSNs)**: Intégrateurs et partenaires Aidant les entreprises à migrer et gérer leurs solutions Cloud. Par exemple: développeurs d'applications, fournisseurs de contenu, éditeurs de logiciel, fabricants de matériel, intégrateurs de systèmes, auditeurs qui fournissent un support à la création, l'intégration ou l'exploitation des services offerts par un CSP.

4. Autorités de régulation Garantissant la sécurité, la conformité et l'interopérabilité (ex. ISO..)

Conclusion

Ce chapitre a présenté l'architecture et la gestion du cloud computing, en mettant en évidence les différents composants et couches nécessaires au fonctionnement optimal des services cloud. Nous avons détaillé le front-end et le back-end, ainsi que les quatre couches principales: la couche utilisateur, la couche réseau, la couche de gestion du cloud et la couche des ressources matérielles.

Par ailleurs, la gestion du cloud, incluant l'administration des infrastructures et des applications, ainsi que les stratégies de gestion et de migration a également été soulignée pour garantir la qualité de service, l'optimisation des ressources et la sécurité des données.

Chapitre 4

Technologies et architectures supportant le Cloud

Introduction

Le cloud computing repose sur un ensemble de technologies permettant d'abstraire, de partager et de gérer efficacement les ressources informatiques. Parmi ces technologies, la virtualisation occupe une place centrale, car elle permet à une infrastructure physique de fonctionner comme plusieurs infrastructures logiques, optimisant ainsi l'utilisation des ressources et réduisant les coûts. Elle facilite également la flexibilité et la scalabilité des environnements cloud en permettant le déploiement rapide de machines virtuelles et d'applications.

Un aspect clé de la virtualisation dans les environnements cloud est la migration des machines virtuelles (VMs). Cette migration consiste à transférer l'état d'une VM d'un serveur hôte à un autre, permettant ainsi d'équilibrer les charges, d'assurer la continuité des services lors de maintenances, d'améliorer les performances des applications et d'optimiser la consommation énergétique. Ce chapitre présente les concepts de virtualisation, les différents types et technologies de virtualisation, ainsi que les techniques et approches de migration des VMs, en soulignant leurs avantages et limitations dans le contexte du cloud computing.

4.1 SOA et Services Web

L'architecture orientée services (SOA) constitue un modèle d'organisation des systèmes logiciels reposant sur la mise à disposition de services autonomes et accessibles à la demande. Elle définit la manière dont ces services sont publiés, découverts et consommés au sein d'un environnement distribué.

Figure 4.1: Service-Oriented Architecture

Propriétés du SOA

SOA se distingue par plusieurs caractéristiques fondamentales :

- **Composition de services distribués :** le système est constitué d'un ensemble de services déployés sur différents environnements et pouvant être combinés pour former des applications complètes.

- **Interopérabilité :** l'échange d'informations entre des applications provenant de fournisseurs ou de plateformes différentes est assuré sans nécessiter d'adaptation lourde ou de modification du code existant.

- **Indépendance et standardisation :** chaque service possède une interface normalisée et clairement définie, indépendante de son implantation technique.

- **Faible dépendance :** un service ne requiert aucune connaissance préalable du fonctionnement interne de l'application qui l'invoque, et inversement ; seule l'interface rend possible la communication.

Définition 1: *Une architecture orientée services est une architecture informatique permettant de représenter des fonctions logicielles hétérogènes sous forme de services réutilisables, accessibles via des interfaces ouvertes, et indépendants des langages de programmation ou des plateformes techniques.*

Définition 2: *Un service Web est une application logicielle identifiée par un URI, dont l'interface et les points de liaison sont décrits à l'aide de documents XML. Il permet une interaction automatique avec d'autres applications grâce à l'échange de messages XML transportés par des protocoles Internet standard.*

Avantages du SOA

L'approche SOA présente plusieurs bénéfices significatifs pour les entreprises:

- **Réutilisabilité :** un même service peut être sollicité par différentes applications, ce qui diminue les coûts de développement et de maintenance.

- **Flexibilité et agilité :** en s'appuyant sur des standards largement adoptés (notamment les services Web), SOA facilite l'évolution des processus métiers et l'intégration de nouveaux composants.

- **Surveillance et optimisation :** la structure modulaire permet de suivre les performances de chaque service et d'ajuster rapidement les ressources ou les configurations.

- **Collaboration accrue :** SOA favorise l'appel à des services externes ou partagés pour compléter ou enrichir un processus métier, améliorant ainsi l'intégration inter-organisationnelle.

4.2 Technologie multi-cœurs

La technologie multi-cœurs désigne l'intégration, au sein d'une même puce, de plusieurs unités de calcul travaillant en parallèle. Un processeur physique peut ainsi regrouper plusieurs cœurs logiques capables d'exécuter simultanément plusieurs flux d'instructions. Cette organisation peut également s'étendre à plusieurs circuits intégrés (IC) combinés dans un même module (Figure 4.2).

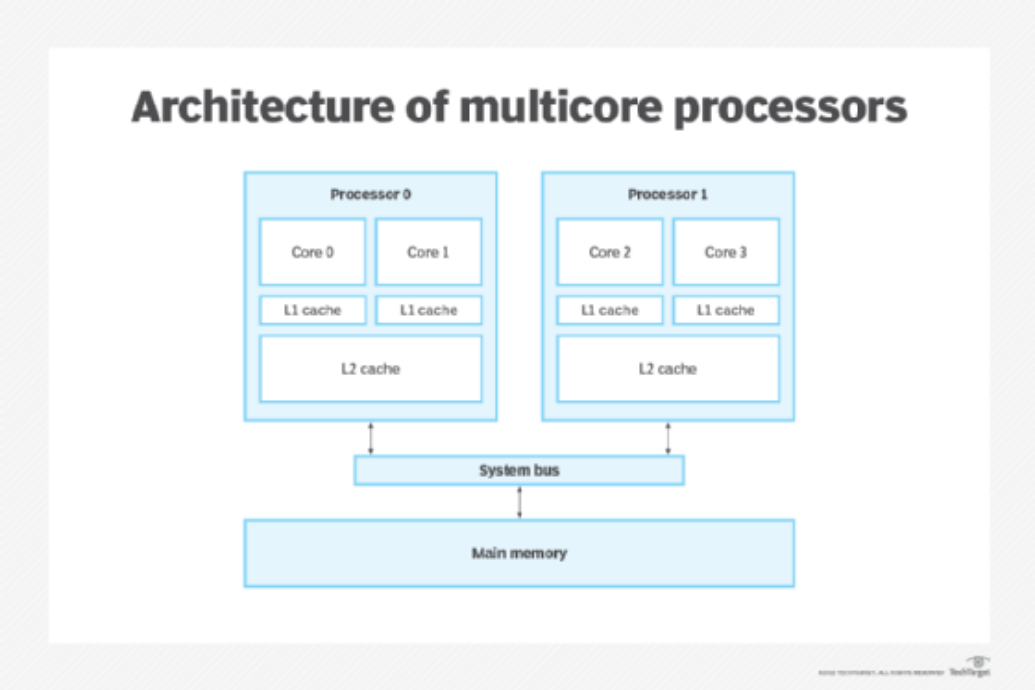

Figure 4.2: Technologie multi-cœurs

L'utilisation de processeurs multi-cœurs présente de nombreux avantages: elle augmente la capacité du système à traiter plusieurs tâches en parallèle, améliore les performances globales et contribue à une meilleure efficacité énergétique. Dans les environnements Cloud, cette technologie est essentielle pour accélérer l'exécution des requêtes, gérer la forte charge des utilisateurs et optimiser les opérations parallèles.

4.3 Technologies de mémoire et de stockage

Les infrastructures Cloud doivent prendre en charge des volumes de données extrêmement variés, provenant de sources multiples. Parmi les types de données rencontrés, on retrouve notamment :

- les images 2D et 3D (médicales, géospatiales, satellitaires, etc.) ;
- les fichiers audio (formats MP3, WMA, WAV, entre autres) ;
- les contenus photographiques ;
- les flux et contenus vidéo en streaming.

Cette diversité nécessite des solutions de stockage capables d'assurer performance, flexibilité et disponibilité.

Exigences du stockage dans le Cloud

Les plateformes de stockage déployées dans les environnements Cloud doivent répondre à un ensemble d'exigences techniques essentielles:

- **Scalabilité:** la capacité de stockage doit pouvoir s'adapter dynamiquement à l'évolution des besoins des utilisateurs et à la croissance des données.
- **Haute disponibilité:** l'accès aux données doit être garanti avec un taux de disponibilité très élevé, indépendamment des défaillances matérielles ou des interruptions de service.
- **Large bande passante:** le système doit être capable de supporter des transferts de données rapides et continus, nécessaires notamment pour le streaming, l'analyse de données ou la réplication.
- **Performances constantes:** le stockage Cloud doit maintenir un niveau de performance stable tout au long de la durée d'utilisation, sans dégradation perceptible liée à la charge ou à l'augmentation du volume de données.

- **Équilibrage de charge :** pour une utilisation optimale des ressources, les solutions de stockage doivent intégrer des mécanismes intelligents répartissant automatiquement la charge entre les différents serveurs et dispositifs.

4.4 Technologies de réseau

Les infrastructures réseau destinées au cloud doivent être conçues pour répondre à un ensemble de contraintes et d'exigences techniques, leur permettant de supporter efficacement les services et applications virtualisés. Parmi ces exigences principales:

- **Consolidation des workflows et fourniture d'IaaS:** La technologie réseau doit permettre de regrouper et d'optimiser les charges de travail des entreprises afin de réduire les coûts de gestion afin d'offrir une plus grande flexibilité et évolutivité pour l'administration des machines virtuelles.

- **Connexion des machines virtuelles aux réseaux physiques et virtuels:** Le système réseau en environnement cloud doit prendre en charge à la fois les réseaux virtuels et physiques, assurer l'application des politiques de sécurité, l'isolement des tenants et le respect des niveaux de service.

- **Connectivité, gestion de la bande passante et optimisation des performances:** Le réseau cloud doit intégrer des mécanismes tels que l'équilibrage de charge et la redondance (fail-over) pour augmenter la bande passante agrégée et garantir la continuité du service. De plus, l'utilisation de technologies à faible latence et de protocoles optimisés pour les data centers contribue à améliorer la performance des applications et des serveurs.

4.5 Virtualisation

La virtualisation constitue la technologie centrale du cloud computing. Elle permet à une infrastructure matérielle unique d'être perçue et utilisée comme plusieurs ressources

logiques indépendantes. Grâce à cette abstraction, l'ensemble des capacités d'une plate-forme physique peut être utilisé au maximum et de manière dynamique.

La virtualisation ne se limite pas au matériel seul; elle peut également s'appliquer à la mémoire, au processeur, aux entrées/sorties, au réseau, aux systèmes d'exploitation, aux données et aux applications. Dans le schéma illustratif (Figure 4.3), plusieurs systèmes d'exploitation et applications coexistent sur une même infrastructure physique virtuelleisée. En mutualisant ainsi les ressources, la virtualisation réduit le besoin d'investissements massifs dans l'acquisition de nouvelles machines et devient un moteur d'innovation dans l'industrie des TI, et particulièrement dans l'univers du cloud computing.

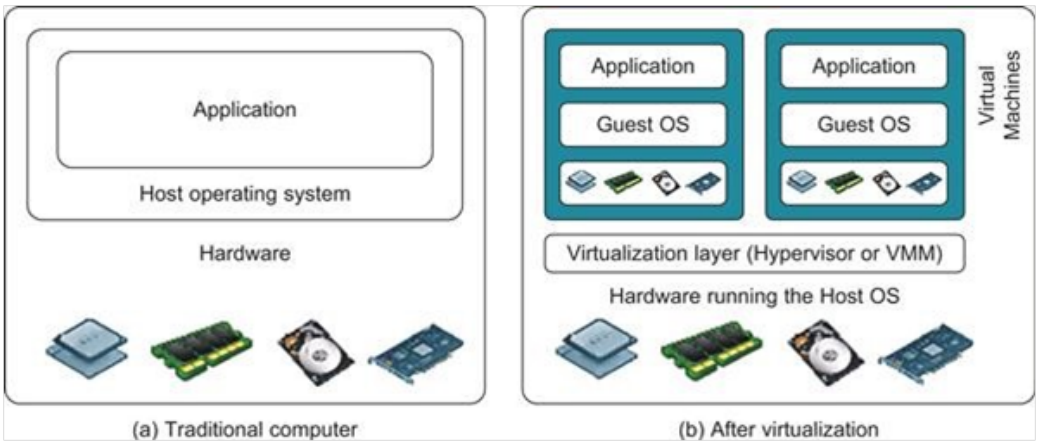

Figure 4.3: Avant et après la virtualisation

Hyperviseurs

De nos jours, les machines virtuelles (VMs) sont largement adoptées dans le secteur informatique industriel, remplaçant de plus en plus les machines physiques. Elles participent à des solutions plus écologiques et plus efficientes. La technologie sous-jacente à ces environnements virtuels suscite évidemment l'intérêt tant dans les milieux industriels qu'académiques.

Cette technologie est incarnée par le logiciel appelé « hyperviseur » (ou « hypervisor »). Il s'agit d'un méta-système d'exploitation minimal placé entre l'infrastructure physique et les VMs. Il permet de fournir à ces dernières une infrastructure virtuelle comprenant notamment : des processeurs virtuels (vCPUs), de la mémoire virtuelle (vRAM), des cartes

réseau virtuelles (vNICs), du stockage virtuel, etc. Les hyperviseurs, parfois désignés VMM (Virtual Machine Monitor), sont le moteur principal de la virtualisation au sein des centres de données.

On distingue deux grandes catégories d'hyperviseurs:

Hyperviseurs de type 1: Ce type s'exécute directement sur le matériel, sans recours à un système d'exploitation hôte intermédiaire (voir la Figure 4.4). Comparativement au type 2, la surcharge liée à la communication avec un OS hôte est supprimée, ce qui améliore l'efficacité, les performances et la sécurité. Ce sont donc ces hyperviseurs qui sont privilégiés pour les serveurs et les infrastructures critiques. Parmi les solutions dominantes : Microsoft Hyper-V, Citrix XenServer, VMware ESXi, Oracle VM (pour SPARC), etc.

Hyperviseurs de type 2: Ce type d'hyperviseur est déployé comme une application sur un système d'exploitation déjà installé (voir par exemple la Figure Figure 4.4). Il dépend donc du bon fonctionnement de l'OS hôte pour accéder aux ressources matérielles. Le point faible majeur est que la défaillance de l'OS hôte entraîne celle de toutes les VMs qu'il héberge. C'est pourquoi les hyperviseurs de type 2 sont plutôt recommandés pour des postes clients ou des environnements à faible criticité. Quelques exemples: VMware Workstation/Player, Oracle VirtualBox, KVM dans certains scénarios.

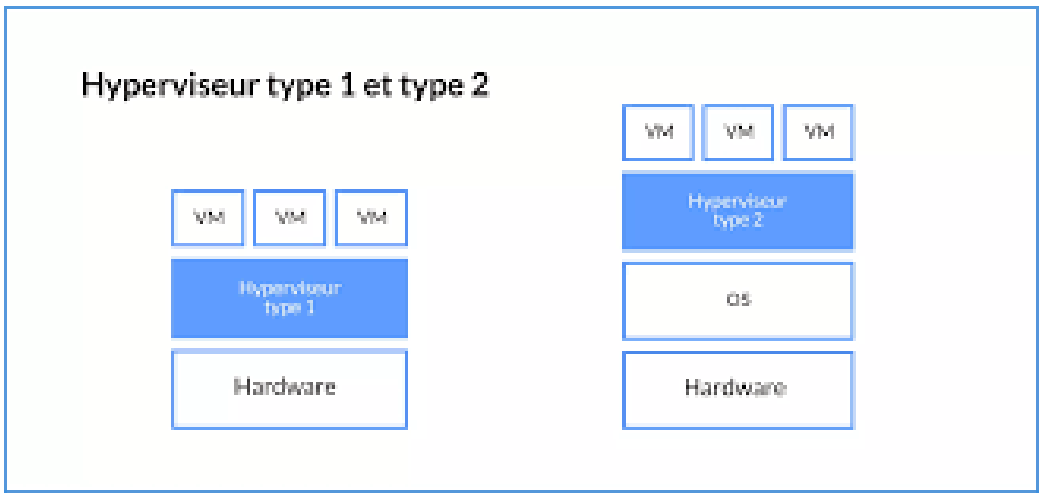

Figure 4.4: Hyperviseur type 1 et 2

Virtualisation des ressources

La virtualisation des ressources désigne le processus d'abstraction des composants physiques d'une infrastructure afin de constituer des pools de ressources virtuelles, mobilisables à la demande par les machines virtuelles (VM). Ces composants peuvent inclure la mémoire, les processeurs, le stockage et le réseau, chacun bénéficiant de technologies dédiées de virtualisation.

1. Virtualisation du processeur: La virtualisation des processeurs permet de diviser un processeur physique en plusieurs unités logiques (vCPUs). Cette partition est orchestrée par l'hyperviseur et chaque VM se voit attribuer une ou plusieurs vCPUs selon ses besoins. Grâce à cette approche, plusieurs environnements virtuels peuvent coexister efficacement sur un même serveur physique.

2. Virtualisation de la mémoire: La virtualisation de la mémoire consiste à représenter la mémoire physique par un espace de mémoire virtuelle partagé entre plusieurs VM. Elle repose notamment sur un mappage entre adresses virtuelles et adresses physiques. Dans les datacenters virtualisés, la mémoire inutilisée de plusieurs serveurs peut être agrégée en un pool virtuel redistribué aux VMs. Cette technique améliore l'utilisation globale de la mémoire matérielle.

3. Virtualisation du stockage: La virtualisation du stockage permet de regrouper plusieurs disques physiques en un ou plusieurs volumes de stockage virtuels destinés aux machines virtuelles. Elle est fréquemment utilisée pour les fonctions de sauvegarde, de réplication ou de haute disponibilité des données. Parmi les technologies courantes on trouve les SAN (Storage Area Network) ou NAS (Network Attached Storage).

4. Virtualisation du réseau: La virtualisation du réseau consiste à abstraire les fonctions réseau pour permettre la création de plusieurs réseaux logiques sur une même infrastructure physique. Par exemple, une seule interface physique peut être partagée entre plusieurs VMs

via des VLANs ou des réseaux virtuels dédiés. Cette virtualisation du réseau offre plusieurs avantages:

- **Transparence:** Les périphériques distribués peuvent être rassemblés au sein d'un unique réseau logique, facilitant la gestion sur plusieurs sites.
- **Sécurité:** Certains systèmes sensibles peuvent être isolés dans un réseau virtuel distinct.

Cependant, l'implémentation des VLANs ou autres formes de virtualisation réseau exige une gestion plus sophistiquée des composants actifs (switchs, routeurs virtuels, etc.).

Types de virtualisation

On distingue principalement trois approches de la virtualisation, chacune ayant ses propres caractéristiques et compromis:

1. Virtualisation complète (Full Virtualization): Dans ce modèle, le système d'exploitation invité (OS Guest) est totalement isolé de la couche matérielle. L'hyperviseur intercepte toutes les instructions sensibles et simule le matériel virtuel, de sorte que l'OS invité fonctionne comme s'il était installé directement sur des ressources physiques. Cette approche ne nécessite aucune modification de l'OS invité.

Avantages

- Isolation forte et bon niveau de sécurité des machines virtuelles.
- Possibilité d'exécuter plusieurs systèmes d'exploitation différents simultanément.
- L'OS invité peut fonctionner sans virtualisation, ce qui garantit une bonne portabilité.
- Pas besoin d'adapter l'OS invité.

Inconvénients

- la traduction binaire des instructions crée un surcoût de traitement, ce qui peut réduire les performances globales.

2. Para-virtualisation: Cette approche, parfois appelée virtualisation partielle, repose sur la collaboration entre l'OS invité et l'hyperviseur : l'OS invité est « conscient » de sa virtualisation et appelle directement l'hyperviseur par le biais de mécanismes dédiés (hypercalls). L'hyperviseur n'a pas besoin d'émuler toutes les instructions, ce qui améliore l'efficacité. Toutefois, l'OS doit être modifié pour fonctionner dans ce cadre.

Avantages

- Suppression de la traduction binaire pour de nombreuses opérations, ce qui améliore les performances.
- Mise en œuvre souvent plus simple que la virtualisation complète.

Inconvénients

- L'OS invité doit être spécifiquement modifié pour cette virtualisation.
- Ces machines virtuelles ne sont pas toujours migrables vers d'autres hôtes non modifiés.
- Moins grande compatibilité avec des OS propriétaires ou peu adaptables.

3. Virtualisation assistée par matériel (Hardware-Assisted Virtualization): Dans cette approche, les processeurs modernes intègrent des extensions matérielles (par exemple Intel VT-x ou AMD-V) pour prendre en charge directement la virtualisation. Cela permet à l'hyperviseur d'exécuter l'OS invité non modifié sans recourir entièrement à l'émulation logicielle.

Avantages

- Réduction du surcoût lié à la traduction ou à la modification de l'OS invité.
- Compatibilité avec des OS non modifiés.

Inconvénients

- Ne fonctionne que sur matériel récent disposant de ces extensions.
- L'augmentation du nombre d'interruptions ou de VM peut entraîner une surcharge processeur et limiter l'évolutivité dans certains scénarios.
- Dans certains cas, les performances peuvent rester légèrement inférieures à celles d'une para-virtualisation optimisée.

Avantages de la virtualisation

L'adoption de la virtualisation présente de nombreux bénéfices pour les fournisseurs de services informatiques. Parmi les avantages les plus significatifs, on peut citer :

- **Consolidation des ressources** : la virtualisation permet d'exécuter plusieurs environnements logiciels sur un même serveur physique. Cette mutualisation réduit le nombre total de serveurs nécessaires et diminue fortement les investissements matériels dans les centres de données.
- **Meilleure utilisation des ressources** : en regroupant plusieurs charges de travail sur une même infrastructure, le taux d'exploitation des serveurs atteint généralement 60 à 80 %, contre seulement 10 à 20 % dans les environnements non virtualisés.
- **Automatisation de la gestion** : la création, la configuration et la mise à disposition des machines virtuelles peuvent être entièrement automatisées, ce qui facilite l'adaptation instantanée aux besoins des utilisateurs.
- **Réduction de la consommation énergétique** : la diminution du nombre de serveurs physiques entraîne une baisse significative des besoins en alimentation électrique et en refroidissement, ce qui réduit les coûts opérationnels.
- **Facilité de déploiement et d'administration** : la virtualisation simplifie l'installation, la sauvegarde, la restauration et la duplication des environnements systèmes et applicatifs. Elle facilite également la migration d'applications vers de nouvelles infrastructures.

- **Sécurité et isolation** : chaque machine virtuelle fonctionne dans un environnement cloisonné, ce qui réduit les risques de propagation d'incidents et améliore la sécurité globale du système.

- **Comportement dynamique** : en cas de surcharge ou de besoin ponctuel en ressources, une machine virtuelle peut recevoir temporairement des ressources supplémentaires (processeur, mémoire, stockage).

- **Optimisation de l'espace physique** : en limitant le nombre de serveurs physiques nécessaires, la virtualisation permet de réduire l'espace occupé dans les salles informatiques, un facteur particulièrement coûteux dans les centres de données.

4.6 Migration des machines virtuelles

La migration des machines virtuelles consiste à transférer l'état d'exécution d'une VM d'un serveur hôte physique à un autre, incluant la mémoire volatile et non volatile, l'état des processeurs virtuels ainsi que les paramètres des interfaces réseau virtuelles et les connexions actives. Les VMs peuvent être migrées pour diverses raisons, notamment pour équilibrer la charge entre serveurs, effectuer la maintenance ou pallier la défaillance d'un hôte, améliorer les performances des applications ou encore optimiser la consommation énergétique et réduire les coûts.

On distingue deux types de migration de machines virtuelles: la migration à froid (*Stop-and-Copy*), la migration à chaud (*Live Migration*).

Migration à froid (Stop-and-Copy)

La migration à froid consiste à :

1. arrêter la VM sur l'hôte source ;

2. transférer l'ensemble de son état vers l'hôte de destination ;

3. relancer la VM sur le serveur cible.

Avantages

- facile à mettre en œuvre ;
- aucune incohérence mémoire possible ;
- l'état de la VM est parfaitement préservé.

Inconvénients

- interruption totale du service durant la migration ;
- surcharge réseau importante lors du transfert complet de la mémoire.

Migration à chaud (Live Migration)

La migration à chaud permet de déplacer une VM en cours d'exécution, avec une interruption minimale du service. Deux approches principales existent :

1. la migration pré-copie (*Pre-copy*) ;
2. la migration post-copie (*Post-copy*);
3. la migration post-copie hybride.

Migration pré-copie: La migration pré-copie s'effectue en plusieurs itérations :

1. transfert de toutes les pages mémoire vers la destination ;
2. transfert des pages modifiées lors des itérations suivantes ;
3. arrêt de la VM lorsque le nombre de pages restantes est inférieur à un seuil ;
4. transfert des dernières pages modifiées ;
5. redémarrage de la VM sur l'hôte cible.

Avantage Assure un temps d'interruption faible et prédictible.

Inconvénient Si la VM modifie trop fréquemment sa mémoire, la migration peut se prolonger indéfiniment.

Migration post-copie: La migration post-copie adopte une stratégie opposée :

1. arrêt immédiat de la VM sur l'hôte source ;
2. transfert des données annexes et de l'état d'exécution ;
3. activation de la VM sur l'hôte de destination ;
4. récupération des pages mémoire manquantes à la demande (*Demand Paging*) ;
5. transfert continu des pages restantes (*Active Push*) ;
6. utilisation possible de la pré-pagination (*Pre-paging*) ;
7. fin de la migration lorsque toutes les pages sont réceptionnées.

Avantage Temps d'interruption très faible, indépendamment de l'activité mémoire.

Inconvénient En cas de défaillance de l'un des hôtes, l'état mémoire peut devenir incohérent.

Migration post-copie hybride: Cette approche combine pré-copie et post-copie :

1. première itération de pré-copie pour transférer toutes les pages utilisées ;
2. arrêt de la VM sur l'hôte source ;
3. transfert des données annexes ;
4. activation de la VM sur l'hôte cible ;
5. récupération à la demande des pages manquantes ;
6. transfert continu des pages modifiées ;
7. répétition jusqu'à réception complète de la mémoire.

Avantages

- temps d'interruption très faible ;
- amélioration des performances de la post-copie classique.

Conclusion

La virtualisation constitue l'un des piliers fondamentaux du cloud computing, offrant la possibilité de transformer une infrastructure physique en un ensemble de ressources logiques flexibles et optimisées. Elle permet non seulement d'améliorer l'utilisation des ressources et de réduire les coûts énergétiques, mais aussi de simplifier le déploiement, la gestion et la sécurisation des environnements cloud.

La migration des machines virtuelles complète ce dispositif en assurant la continuité des services, l'équilibrage des charges et l'optimisation des performances des applications, tout en minimisant les interruptions et les coûts opérationnels. Les différentes techniques de migration, qu'il s'agisse de la migration à froid, à chaud ou hybride, offrent des solutions adaptées aux besoins spécifiques des environnements cloud modernes.

Ainsi, la maîtrise de la virtualisation et des stratégies de migration est essentielle pour garantir un cloud performant, scalable et fiable, capable de répondre aux exigences croissantes des entreprises et des utilisateurs.

Chapitre 5

Gouvernance du Cloud

Introduction

L'adoption du cloud computing transforme profondément la manière dont les organisations gèrent leurs systèmes d'information et leurs ressources technologiques. Si le cloud offre une flexibilité, une évolutivité et une rapidité de déploiement sans précédent, il introduit également de nouveaux défis liés à la sécurité, à la conformité, à la maîtrise des coûts et à la performance opérationnelle.

La gouvernance du cloud constitue un cadre essentiel pour encadrer ces environnements complexes. Elle définit les règles, processus et bonnes pratiques permettant de superviser l'utilisation des ressources cloud, de sécuriser les données sensibles, de contrôler les coûts et d'assurer la cohérence avec les objectifs stratégiques de l'organisation.

Ce chapitre présente les concepts clés de la gouvernance du cloud, ses principes fondamentaux, les composants d'un cadre de gouvernance, ainsi que les modèles et bonnes pratiques existants qui peuvent guider les organisations dans leur adoption et leur gestion du cloud.

5.1 Concepts de la gouvernance du cloud

Avec le cloud, toute équipe d'une organisation peut rapidement déployer ses propres systèmes d'un simple clic. Si cela stimule l'innovation et la productivité, cela peut aussi

générer des problématiques:

- un manque d'intégration entre les solutions cloud, même au sein d'une même entreprise ;
- des redondances inutiles de travail ou de données dans différentes entités ;
- un décalage possible entre les systèmes cloud et les objectifs métiers ;
- des risques nouveaux en matière de sécurité, par exemple le déploiement de services sans contrôle d'accès strict.

Définition: *La gouvernance du cloud désigne l'ensemble des règles, politiques et processus qu'une organisation met en place pour piloter l'exploitation de services cloud. Son objectif est de renforcer la sécurité des données, maîtriser les risques et garantir le bon fonctionnement des systèmes cloud dans le temps.*

La gouvernance du cloud veille donc à ce que le déploiement des ressources, l'intégration des systèmes, la sécurisation des données et tous les aspects de l'informatique en nuage soient planifiés, suivis et contrôlés. Cette gouvernance est particulièrement dynamique, car les environnements cloud peuvent être provisionnés par divers groupes internes ou prestataires externes et sont susceptibles d'évoluer quotidiennement. Les initiatives de gouvernance assurent que ce cadre complexe reste conforme aux politiques de l'organisation, aux bonnes pratiques de sécurité et aux obligations réglementaires.

5.2 L'importance de la gouvernance du cloud

Une gouvernance bien conçue permet notamment à une organisation d'exploiter pleinement les avantages du cloud tout en évitant les pièges classiques : coûts incontrôlés, duplication des ressources, risques de non-conformité ou de failles de sécurité. Elle aide à aligner l'utilisation du cloud avec la stratégie et les objectifs métier, à contrôler les dépenses, et à limiter l'apparition d'îlots technologiques non autorisés ("shadow IT") tout en garantissant la transparence, le contrôle et la traçabilité.

Une gouvernance du cloud bien conçue apporte plusieurs bénéfices essentiels aux organisations qui exploitent des services critiques dans le cloud, tels que :

- **Optimisation de la gestion des ressources cloud :** La gouvernance permet de structurer l'environnement cloud en comptes distincts (départements, projets, centres de coûts), ce qui améliore la visibilité, le contrôle budgétaire et la maîtrise des risques associées aux ressources.

- **Réduction du phénomène de "shadow IT":** Lorsque les employés déploient des systèmes dans le cloud sans passer par le service informatique, les risques et les coûts augmentent. Un cadre de gouvernance permet d'encadrer la demande de ressources cloud, d'appliquer les contrôles nécessaires et de garantir une gestion conforme aux contraintes de l'organisation.

- **Diminution de la charge administrative :** Sans gouvernance, les organisations ont souvent recours à des tableurs ou des processus manuels pour suivre les comptes cloud, les coûts et la conformité. Ces méthodes sont inefficaces et sujettes à erreurs. Une solution de gouvernance permet de centraliser les politiques, d'automatiser la surveillance et de simplifier les réponses aux violations.

- **Renforcement de la sécurité du cloud :** Un modèle de gouvernance instaure une stratégie d'authentification, de contrôle d'accès et de supervision continue. Il garantit que, peu importe l'emplacement des données ou des systèmes critiques, les mesures de sécurité adéquates sont appliquées.

la gouvernance du cloud transforme un environnement potentiellement chaotique - marqué par des déploiements non contrôlés, des coûts imprévus et des risques de sécurité - en un actif stratégique aligné sur les objectifs métier, maîtrisé et sécurisé.

5.3 Principes d'un modèle de gouvernance du cloud

Un modèle de gouvernance du cloud robuste s'appuie sur plusieurs principes fondamentaux qui orientent la gestion des environnements cloud de façon cohérente avec les objectifs

de l'organisation. Voici cinq principes essentiels :

1. **Conformité aux règles et standards :** L'usage du cloud doit respecter les politiques internes, les normes industrielles et les exigences réglementaires propres à l'organisation et à son secteur.

2. **Alignement avec les objectifs métier :** La stratégie cloud doit s'inscrire dans le cadre global des stratégies IT et métier. Tous les systèmes et principes de gouvernance cloud doivent contribuer de manière mesurable aux résultats de l'entreprise.

3. **Collaboration entre parties prenantes :** Un accord clair doit exister entre les propriétaires de l'infrastructure cloud, les utilisateurs et les autres parties prenantes afin d'assurer une utilisation cohérente et bénéfique des ressources cloud.

4. **Gestion des changements :** Toute modification de l'environnement cloud doit être effectuée selon des processus standardisés, contrôlés et traçables, pour garantir l'intégrité et la stabilité des services.

5. **Réactivité dynamique :** Le modèle de gouvernance doit s'appuyer sur des mécanismes de surveillance automatique et d'orchestration afin de réagir rapidement aux événements (changements de charge, incidents, modifications de conformité) dans l'environnement cloud.

5.4 Conception et mise en œuvre d'un cadre de gouvernance du cloud

La mise en place d'un cadre de gouvernance adapté est essentielle pour assurer une gestion efficace des environnements cloud. On y retrouve plusieurs composants clés qui garantissent à la fois contrôle, cohérence et performance (Figure 5.1).

Figure 5.1: Components of a cloud governance framework

Gestion financière du cloud

Dans de nombreuses organisations, les coûts liés au cloud peuvent rapidement devenir incontrôlables. Bien que les services cloud promettent souvent une réduction des coûts informatiques, ceci n'est vrai que si une gestion financière rigoureuse est appliquée. Trois éléments sont fondamentaux:

- **Politiques financières** : elles délimitent clairement comment le cloud doit être utilisé; par exemple, préciser quand recourir à des services managés pour réduire les coûts internes, ou établir une checklist de gestion des coûts avant chaque déploiement.
- **Budgets** : fixer des enveloppes budgétaires assignées à des départements, des projets ou des catégories de services cloud.
- **Rapport des coûts** : la remontée fiable des coûts peut être complexe. Certains services cloud engendrent des frais imprévus. Il est possible d'utiliser les outils de suivi du fournisseur ou des solutions tierces multi-cloud.

Gestion des opérations cloud

La gestion opérationnelle du cloud consiste à définir et superviser les processus de déploiement des services. Ces processus doivent inclure :

- la définition précise des ressources allouées à chaque service dans la durée ;
- des accords de niveau de service (SLA) établissant les performances attendues ;
- une supervision continue pour s'assurer de la conformité aux SLA ;
- des contrôles et procédures avant la mise en production du code ;
- des règles de contrôle d'accès.

Une gouvernance opérationnelle solide aide à limiter la "shadow", contrôle l'usage inutile des ressources cloud et améliore significativement le retour sur investissement à long terme.

Gestion des données cloud

Avec le cloud, il devient plus facile de collecter et d'analyser de grands volumes de données, mais cela introduit aussi des défis majeurs en matière de gestion. La gouvernance des données doit couvrir l'ensemble du cycle de vie dans le cloud :

- mise en place d'une catégorisation des données selon leur sensibilité ;
- chiffrement systématique des données au repos et en transit ;
- contrôle d'accès adapté à chaque catégorie de données ;
- utilisation de techniques comme l'anonymisation ou masquage pour les données utilisées dans les environnements de développement ou de test ;
- stratégie de tiering : migration des données, au fil du temps, d'un stockage à accès rapide et coûteux vers des systèmes archivage moins coûteux ;
- automatisation de la gestion du cycle de vie des données - essentielle dans les déploiements cloud à large échelle.

Gestion de la sécurité et de la conformité

La gouvernance du cloud est responsable de la mise en œuvre des politiques de sécurité et de conformité au sein de l'environnement cloud. Cela implique :

- l'évaluation continue des risques ;
- la gestion des identités et des accès (IAM) ;
- la protection des données et leur chiffrement ;
- la sécurité des applications ;
- la mise en place de plans de reprise après sinistre (Disaster Recovery).

Le cadre de gouvernance doit réussir à concilier les objectifs métier, les risques réels et les exigences des standards de conformité. Il s'appuie sur les politiques existantes en les adaptant au contexte cloud.

5.5 Composants clés de la gouvernance du cloud

Une gouvernance efficace du cloud s'appuie sur plusieurs composantes fondamentales qui permettent d'assurer la sécurité, la conformité, la maîtrise des coûts et la fiabilité des environnements cloud. En particulier, on peut identifier les éléments suivants :

- **Gestion des politiques et des risques :** Définition et application de règles claires concernant l'utilisation des ressources cloud, identification des risques liés aux opérations cloud, et mise en place de mécanismes de contrôle et de remédiation.
- **Gestion des utilisateurs, des identités et des accès (IAM) :** Contrôle de qui peut accéder à quelles ressources cloud, mise en place des principes « least privilege », authentification forte et audit des accès.
- **Sécurité, conformité et protection des données :** Chiffrement des données au repos et en transit, segmentation des réseaux, conformité aux normes et réglementations (ex. : RGPD, ISO 27017) ; surveillance continue pour détecter et corriger les dérives.

- **Gestion des coûts et optimisation financière :** Suivi et contrôle des dépenses cloud, prévention des déploiements non contrôlés, automatisation des ressources inutilisées, alignement des ressources sur les objectifs métier.

- **Gestion opérationnelle et performance :** Suivi de la qualité de service, veille sur les indicateurs de performance (latence, disponibilité), gestion des configurations de l'infrastructure (Infrastructure as Code), garantie de fiabilité et d'efficience.

- **Ressources et configuration :** Allocation rationnelle des ressources, gestion des configurations, standardisation des modèles de déploiement, et indexation ou étiquetage (tagging) pour assurer traçabilité et gouvernance.

Ces composantes sont interconnectées : par exemple, la gestion des politiques conditionne la sécurité, la maîtrise des coûts dépend de l'optimisation opérationnelle, et la conformité repose sur le bon contrôle des accès et des données. En structurant la gouvernance autour de ces piliers, les organisations peuvent mieux exploiter les bénéfices du cloud tout en maîtrisant les risques et en alignant leur usage sur la stratégie métier.

5.6 Meilleures pratiques de gouvernance du cloud

Pour qu'un cadre de gouvernance du cloud soit réellement efficace, il ne suffit pas d'établir des principes et des composants : il importe également d'appliquer des pratiques éprouvées qui permettent d'optimiser l'usage, le contrôle et la conformité des services cloud. Voici quelques-unes des meilleures pratiques que les organisations performantes adoptent.

- **Définir les rôles et responsabilités clairement :** Chaque acteur — sponsor métier, architecte cloud, sécurité, conformité, opération — doit avoir un rôle et une autorité clairement définis, afin d'assurer la coordination et l'application des politiques.

- **Évaluer les obligations de conformité dès le départ :** Comprendre les normes et réglementations applicables (ex. RGPD, HIPAA, ISO 27017) permet de bâtir des contrôles pertinents et de limiter les risques.

- **Utiliser un cadre de gouvernance standardisé :** L'adoption de modèles ou référentiels (COBIT, ISO, NIST, frameworks cloud-adoption des fournisseurs) facilite la création de politiques cohérentes et reconnues.
- **Mettre en œuvre une gestion unifiée des identités et des accès (IAM) :** Le contrôle d'accès granulaire, l'authentification forte et la révision régulière des privilèges sont essentiels pour protéger les ressources cloud.
- **Surveiller en continu et optimiser :** Mettre en place des tableaux de bord, des alertes, des audits réguliers pour suivre la conformité, la performance, les coûts et ajuster les politiques en conséquence.
- **Gouverner dans un environnement multi-cloud ou hybride :** Avec l'usage croissant de plusieurs fournisseurs ou d'architectures hybrides, la gouvernance doit être conçue de façon à couvrir tous les environnements de manière harmonisée.

En intégrant ces pratiques au modèle de gouvernance, il devient possible d'accroître la maturité de la gestion du cloud, d'améliorer l'alignement avec les objectifs de l'entreprise, de réduire les risques, de mieux maîtriser les coûts et de favoriser une dynamique d'amélioration continue.

5.7 Modèles de gouvernance et cadres existants

Pour structurer efficacement la gouvernance du cloud, plusieurs modèles et cadres ont été développés par les fournisseurs de services cloud et par des organismes standards. Ces cadres fournissent des recommandations et des bonnes pratiques pour garantir sécurité, conformité et performance.

Cloud Adoption Framework (CAF)

Le **Cloud Adoption Framework** est un modèle proposé par Microsoft. Il guide les organisations dans leur adoption du cloud en couvrant à la fois les aspects technologiques et organisationnels. Le CAF repose sur plusieurs piliers :

- **Stratégie :** définir les objectifs métiers et les priorités d'adoption du cloud.
- **Planification :** analyser l'infrastructure existante et concevoir la migration vers le cloud.
- **Gouvernance :** établir des politiques, des processus et des outils pour contrôler les ressources cloud.
- **Gestion des ressources et opérations :** définir les rôles, responsabilités et processus opérationnels dans le cloud.
- **Innovation et optimisation :** tirer parti du cloud pour améliorer les services et optimiser les coûts.

Well-Architected Framework (WAF)

Le **Well-Architected Framework**, développé par AWS, est un cadre de bonnes pratiques pour concevoir des architectures cloud robustes et performantes. Il s'appuie sur cinq piliers fondamentaux :

- **Excellence opérationnelle :** automatisation et amélioration continue des processus.
- **Sécurité :** protection des données, gestion des accès et prévention des menaces.
- **Fiabilité :** résilience des systèmes, reprise après incident et haute disponibilité.
- **Efficacité des performances :** optimisation de l'utilisation des ressources et adaptation aux besoins.
- **Optimisation des coûts :** contrôle des dépenses et allocation efficace des ressources.

Autres modèles et cadres

D'autres modèles sont également utilisés pour renforcer la gouvernance du cloud, tels que:

- **Google Cloud Architecture Framework :** similaire au WAF, il met l'accent sur la sécurité, la fiabilité et l'efficacité des architectures cloud.

- **COBIT Cloud :** adaptation du référentiel COBIT pour la gouvernance IT au contexte cloud.
- **ISO/IEC 38500 :** norme internationale pour la gouvernance des technologies de l'information, applicable aux environnements cloud.

Ces cadres permettent aux organisations de disposer d'un référentiel structuré pour gérer la sécurité, la conformité, la performance et les coûts dans leurs environnements cloud.

Conclusion

La gouvernance du cloud s'impose comme un élément stratégique pour toutes les organisations qui exploitent des environnements cloud. Elle permet de structurer l'utilisation des ressources, de sécuriser les données, de maîtriser les coûts et de garantir la conformité aux normes et réglementations.

En appliquant des principes clairs, en mettant en place un cadre de gouvernance robuste et en s'appuyant sur des modèles éprouvés comme le Cloud Adoption Framework ou le Well-Architected Framework, les organisations peuvent transformer le cloud d'un simple outil technologique en un levier stratégique. La gouvernance contribue ainsi à un usage du cloud plus sûr, plus efficace et aligné avec les objectifs métiers, tout en facilitant l'innovation et la flexibilité nécessaires dans un environnement numérique en constante évolution.

Projets Cloud Computing

Enseignante : Rokaya Ben Jeddou

Auditoire : 2MPCM

Date limite de remise des projets : 05/12/2025

Ce chapitre présente une série de projets pratiques visant à renforcer les compétences des étudiants dans le domaine du *Cloud Computing*. Chaque projet est conçu pour explorer un aspect particulier du cloud, de l'hébergement web à l'automatisation d'infrastructure et à l'intelligence artificielle appliquée au cloud.

Projet 1 - Hébergement d'un site web statique sur le Cloud

Objectif : Déployer un site statique sur AWS S3, Azure Blob ou Google Cloud Storage.

Compétences visées : gestion du stockage objet, configuration DNS, HTTPS.

Technologies :

- AWS S3, Azure Blob Storage, Google Cloud Storage (tous disposent d'un *free tier* académique)
- HTML/CSS/JS (open source)

Livrables : URL du site, capture d'écran du tableau de bord cloud, rapport technique.

Source : AWS S3 Static Hosting Guide.

Projet 2 - Création d'une machine virtuelle et serveur web

Objectif : Créer une VM (AWS EC2, Azure VM, GCP Compute Engine) et y déployer un serveur Apache ou Nginx.

Compétences visées : gestion d'instances, SSH, pare-feux.

Technologies :

- AWS EC2 / Azure VM / Google Compute Engine (free tier possible avec une VM légère)
- Apache, Nginx (100% open source)

Livrables : lien d'accès au serveur, capture des configurations réseau.

Source : Azure Virtual Machines Documentation.

Projet 3 - Conteneurisation d'une application avec Docker

Objectif : Créer un conteneur Docker à partir d'une petite application web.

Compétences visées : conception Dockerfile, gestion d'images et volumes.

Technologies :

- Docker Desktop (gratuit pour usage éducatif et personnel)
- Docker Hub (compte gratuit)

Livrables : image Docker, code source, documentation d'exécution.

Source : Docker Get Started.

Projet 4 - Déploiement d'une application conteneurisée sur le Cloud

Objectif : Déployer une application Docker sur AWS ECS, Azure Container Instances ou Google Cloud Run.

Compétences visées : CI/CD, gestion des conteneurs cloud.

Technologies :

- Google Cloud Run, AWS ECS, Azure Container Instances (free tier disponible)
- Docker (open source)

Livrables : URL de l'application, capture du pipeline CI/CD.

Source : Google Cloud Run Quickstart.

Projet 5 - Architecture multi-tier (web + base de données)

Objectif : Déployer une architecture composée d'un frontend web et d'un backend (MySQL, PostgreSQL).

Compétences visées : architecture cloud, sécurité réseau (VPC, groupes de sécurité).

Technologies :

- MySQL, PostgreSQL (open source)
- AWS RDS Free Tier, Azure SQL Free Tier, ou base locale (gratuite)

Livrables : diagramme d'architecture, application fonctionnelle.

Source : AWS Three-tier Architecture.

Projet 6 - Sauvegarde automatisée vers le Cloud

Objectif : Automatiser la sauvegarde de fichiers locaux vers un bucket cloud.

Compétences visées : scripting (Bash/Python), API Cloud, automatisation.

Technologies :

- Python ou Bash (open source)
- API Cloud SDKs : AWS CLI, Azure CLI, GCloud CLI (toutes open source)

Livrables : script, démonstration de sauvegarde, rapport technique.

Source : Google Cloud Storage Libraries.

Projet 7 - Monitoring et optimisation des ressources Cloud

Objectif : Créer un tableau de bord de supervision (Grafana, Prometheus, AWS CloudWatch).

Compétences visées : analyse de performance, visualisation, optimisation.

Technologies :

- Grafana, Prometheus (open source)
- AWS CloudWatch / Azure Monitor (free tier limité)

Livrables : dashboard interactif, rapport d'analyse.

Source : Grafana Cloud Monitoring.

Projet 8 - Infrastructure as Code (IaC) avec Terraform ou Ansible

Objectif : Automatiser le déploiement d'une infrastructure cloud complète.

Compétences visées : IaC, modularité du code, versionnement.

Technologies :

- Terraform (open source, licence MPL 2.0)
- Ansible (open source, licence GPLv3)

Livrables : scripts Terraform/Ansible, démonstration du déploiement.

Source : Terraform Documentation.

Projet 9 - Système IDS basé sur le Cloud

Objectif : Déployer un système de détection d'intrusion (Snort ou Suricata) sur le cloud avec tableau de supervision.

Compétences visées : sécurité réseau, logs, cloud monitoring.

Technologies :

- Snort, Suricata (open source)
- Grafana / Elasticsearch (open source)
- Cloud Free Tier (hébergement ou VM gratuite)

Livrables : démonstration IDS, tableau de bord, rapport complet.

Sources :

- Snort Documentation
- AWS Security Hub

Projet 10 - Plateforme intelligente de détection d'anomalies réseau via Cloud et IA

Objectif : Développer une plateforme cloud combinant collecte de flux réseau et détection d'anomalies par apprentissage automatique.

Compétences visées : cloud computing, IA appliquée, cybersécurité, DevOps.

Technologies :

- Python (open source) + bibliothèques IA : Scikit-learn, TensorFlow, PyTorch
- Cloud AI : Vertex AI, AWS Sagemaker (gratuits dans les limites académiques)

Livrables : prototype fonctionnel, rapport.

Sources :

- Google Vertex AI
- AWS ML Services

Projet 11 - Comparaison des Fournisseurs de Cloud (Multi-Cloud Analysis)

Objectif général : Analyser et comparer plusieurs fournisseurs de cloud selon des critères de performance, sécurité, coût et souveraineté.

Description : Étude documentaire approfondie (analyse d'offres et documentation officielle) et évaluation pratique via les comptes gratuits (*Free Tier*) pour réaliser des tests de performance et de coût.

Critères d'analyse recommandés :

- **Techniques :** disponibilité, latence, évolutivité, support des conteneurs.
- **Sécurité :** chiffrement, conformité, authentification, journalisation.
- **Économiques :** modèle de tarification, coûts cachés, flexibilité.
- **Fonctionnels :** facilité d'usage, documentation, API.
- **Stratégiques :** souveraineté, intégration multi-cloud, réputation.

Exemples de fournisseurs : AWS, Microsoft Azure, Google Cloud Platform, OVHcloud, Oracle Cloud, Scaleway.

Séances applicatives et examens avec correction

Séance Applicative N°1

Objectif : Comprendre les modèles économiques et les principes fondamentaux du Cloud Computing à travers des exercices appliqués.

Exercice 1

1. Pourquoi les entreprises cherchent-elles à passer des dépenses en capital (CapEx) aux dépenses en fonctionnalité (OpEx) dans le contexte du Cloud Computing ?

2. Selon la définition du NIST, quelle est la condition absolue qui, si elle est absente, signifie que le service n'est pas du Cloud Computing ?

Exercice 2

Classez chaque service dans le modèle de service correspondant et justifiez le niveau de contrôle de l'utilisateur :

- Google Docs / Microsoft 365

- Un environnement qui permet à un développeur de déployer son code sans gérer l'OS sous-jacent (ex: Heroku, Google App Engine)

- Location d'une machine virtuelle (VM) sur AWS ou Azure, permettant de choisir l'OS, d'installer ses propres applications, et de définir des topologies réseaux (ex: AWS EC2 / Azure VM)

Exercice 3

Une grande université souhaite moderniser son infrastructure informatique. Choisissez et justifiez le modèle de déploiement approprié pour chaque situation :

1. Trois universités régionales mutualisent leurs ressources pour un Cloud commun.
2. L'université utilise un grand fournisseur commercial pour gérer les e-mails de tous les étudiants et enseignants.
3. L'université crée en interne une infrastructure Cloud pour la recherche sensible.
4. L'université combine son Cloud interne avec un Cloud public pour équilibrer la charge.

Étude de Cas — Service de Streaming Cloud

Une startup lance un service de streaming vidéo basé sur le Cloud. La demande varie de 100 utilisateurs simultanés la nuit à 10 000 pendant un grand événement sportif.

1. Citez les cinq caractéristiques essentielles du Cloud selon le NIST et expliquez comment elles s'appliquent à ce service de streaming.
2. Pourquoi la *multitenancy* (location multiple) est-elle essentielle pour ce type d'architecture Cloud ?
3. Quelles seraient les conséquences si le fournisseur ne garantit pas l'élasticité rapide ?
4. Quelles mesures de sécurité doivent être mises en place pour protéger les données des utilisateurs dans un environnement multitenant ?

Exercice 4

1. Pourquoi le manque de contrôle est-il plus marqué dans le modèle SaaS que dans le modèle IaaS ?

2. Comment une entreprise peut-elle limiter sa dépendance vis-à-vis d'un fournisseur Cloud (*vendor lock-in*) ?

Séance Applicative N°1: Correction

Exercice 1

1. CapEx vs OpEx : Le Cloud supprime l'investissement dans le matériel et transforme les coûts fixes en dépenses variables selon la consommation réelle (pay-as-you-use). L'achat de matériel lourd est éliminé, et l'entreprise passe au modèle paiement à l'utilisation pour les ressources informatiques. Les ressources informatiques ne sont pas toujours exploitées à leur pleine capacité maximale, ce qui justifie ce changement.

2. Condition absolue (NIST) : Si une ou plusieurs des cinq caractéristiques essentielles (accès à la demande, accès réseau large, mutualisation, élasticité rapide, service mesuré) manquent, ce n'est pas un service Cloud.

Exercice 2 — Modèles de Services

Service	**Modèle**	**Justification**
Google Docs / Microsoft 365	SaaS	L'utilisateur utilise l'application via Internet ; il n'a aucun contrôle sur le système d'exploitation ou l'infrastructure sous-jacente.
Heroku / Google App Engine	PaaS	Fournit un environnement de développement sans accès à l'OS ou au matériel, destiné aux développeurs.
AWS EC2 / Azure VM	IaaS	Permet le contrôle sur l'OS, les applications et les topologies réseau.

Exercice 2 — Modèles de Déploiement

Situation	Modèle	Justification
E-mail institutionnel (Google Workspace)	Public	Fournisseur tiers, infrastructure partagée, accessible à tous.
Cloud interne pour la recherche	Privé	Géré par l'université, données et sécurité internes.
Cloud partagé entre universités	Communautaire	Mutualisation entre organisations ayant des besoins communs.
Association Cloud interne et public	Hybride	Combinaison de plusieurs modèles avec portabilité des données.

Étude de Cas

1. Les 5 caractéristiques essentielles (NIST) :

Caractéristique	Application au streaming
Accès à la demande	Allocation automatique des ressources sans intervention.
Accès réseau large	Service accessible sur tout appareil connecté.
Mutualisation	Partage efficace des serveurs entre utilisateurs isolés.
Élasticité rapide	Ajustement dynamique des ressources selon la charge.
Service mesuré	Facturation selon la consommation réelle.

2. Multitenancy : Permet à plusieurs utilisateurs de partager les ressources physiques tout en isolant leurs environnements.

3. Absence d'élasticité : Risque d'instabilité du service lors des pics.

4. Sécurité : chiffrement, isolation des VM, contrôle d'accès, journalisation.

Exercice 4

1. SaaS vs IaaS — Contrôle utilisateur : SaaS : l'utilisateur consomme l'application sans gérer l'infrastructure. IaaS : l'utilisateur contrôle l'OS, le stockage et le réseau.

2. Réduire le vendor lock-in : Utiliser des standards ouverts, des API interopérables, un stockage multi-cloud et des contrats de réversibilité.

Séance Applicative N°2

Partie 1 : L'Écosystème et l'Architecture du Cloud

Le Cloud Computing fonctionne grâce à un écosystème de composants interdépendants qui réalisent, supportent ou consomment les services, structuré sur une architecture hiérarchique en quatre couches.

Exercice 1.1 : Identification des Rôles (Écosystème)

Scénario : Une PME (Petite et Moyenne Entreprise) décide d'utiliser un service de stockage de données en ligne (SaaS) fourni par *TechCloud Inc.*. Pour s'assurer que l'intégration du nouveau service respecte toutes ses réglementations internes de sécurité, la PME fait appel à *SecureIT Consultants* pour un audit et une intégration personnalisée.

Questions :

1. La PME (*Cloud Service User/CSU*, *Cloud Service Provider/CSP*, *Cloud Service Partner/CSN*) ?
2. TechCloud Inc. (*CSU*, *CSP*, *CSN*) ?
3. SecureIT Consultants (*CSU*, *CSP*, *CSN*) ?

Exercice 1.2 : Les Couches Architecturales

Scénario : Un utilisateur accède à sa machine virtuelle hébergée sur un Cloud Public.

1. L'utilisateur utilise son ordinateur portable (un client lourd) pour se connecter au service. À quelle couche architecturale appartient cet appareil, qui est la dernière de l'architecture ?
2. Le Cloud repose sur la Couche Réseau. Dans le cas d'un Cloud Public, quel est le réseau principal utilisé ? Si le service était un Cloud Privé, quel réseau serait utilisé ?

3. Quelle couche est constituée de l'ensemble des logiciels dédiés à la gestion des ressources (ordonnancement, approvisionnement) et joue le rôle d'interface entre le Datacenter (ressources physiques) et le consommateur ?

Partie 2 : Gestion et Contrats (SLA)

La gestion du Cloud vise à gérer les ressources de manière efficace pour atteindre une qualité de service acceptable et respecter les SLAs (Service-Level Agreements).

Exercice 2.1 : SLA et Responsabilité des Couches

1. Quelle couche architecturale est la plus concernée par le SLA et doit être accessible aux utilisateurs dans des délais spécifiques ?

2. Contrairement aux autres couches, la qualité de service de la Couche 2 (Réseau) n'est pas incluse dans le SLA du Cloud. Cependant, si cette couche n'est pas opérationnelle, le Cloud n'est pas utilisable. Que doit supporter le réseau du Datacenter (Couche Physique) pour respecter le SLA concernant le transfert de données ?

Exercice 2.2 : Importance de la Gestion de l'Infrastructure

- Expliquez pourquoi une mauvaise gestion de l'infrastructure est risquée, en vous basant sur les concepts de QoS (Qualité de Service) et de Coût.

Partie 3 : Migration des Applications vers le Cloud

La migration consiste à déplacer une application de son hébergement traditionnel vers le Cloud.

Exercice 3.1 : Caractéristiques et Évolution des Applications

Consigne : Contrastez les principales caractéristiques d'une Application Web et d'une Application Cloud.

Exercice 3.2 : Stratégies et Phases de Migration

La migration vers le Cloud comprend plusieurs phases.

1. Quelle est la première phase de la migration, qui consiste à construire une analyse de rentabilité en examinant l'infrastructure, l'architecture, les risques et les SLAs ?

2. Une entreprise doit migrer une application critique. Cependant, une partie de cette application a des dépendances basées sur des licences existantes et des interconnexions étendues avec d'autres applications. Quelle stratégie de migration est la plus appropriée dans ce cas : *HotPlug* ou *Fusion strategy* ?

3. Une fois les serveurs Cloud configurés et les applications de plateforme déployées, les bases de données et les fichiers sont répliqués. Comment s'appelle cette phase de migration ?

Séance Applicative N°2: Correction

Partie 1 : Écosystème du Cloud

Exercice 1.1 : Identification des Rôles (Écosystème)

Scénario : Une PME (Petite et Moyenne Entreprise) décide d'utiliser un service de stockage de données en ligne (SaaS) fourni par *TechCloud Inc.*. Pour s'assurer que l'intégration du nouveau service respecte toutes ses réglementations internes de sécurité, la PME fait appel à *SecureIT Consultants* pour un audit et une intégration personnalisée.

Questions : Identifiez le rôle de chaque entité dans l'écosystème du Cloud Computing :

1. **La PME (CSU, CSP, CSN) ?**

   → La PME est un **Cloud Service User (CSU)** car elle consomme les services Cloud.

2. **TechCloud Inc. (CSU, CSP, CSN) ?**

   → **TechCloud Inc.** est le **Cloud Service Provider (CSP)** car il fournit, livre et maintient/gère les services Cloud.

3. **SecureIT Consultants (CSU, CSP, CSN) ?**

   → **SecureIT Consultants** est un **Cloud Service Partner (CSN)** car il fournit un support à la création ou à l'intégration d'un service offert par un fournisseur CSP.

Exercice 1.2 : Les Couches Architecturales

Scénario : Un utilisateur accède à sa machine virtuelle hébergée sur un Cloud Public.

1. L'utilisateur utilise son ordinateur portable (un client lourd) pour se connecter au service. À quelle couche architecturale appartient cet appareil, qui est la dernière de l'architecture ?

   → **Couche 1 (Utilisateur/Couche Client)**. Les clients peuvent être des *thin client* ou *thick client*.

2. Le Cloud repose sur la Couche Réseau. Dans le cas d'un Cloud Public, quel est le réseau principal utilisé? Si le service était un Cloud Privé, quel réseau serait utilisé?
   → **Cloud Public :** le réseau Internet.
   → **Cloud Privé :** le réseau local (LAN).

3. Quelle couche est constituée de l'ensemble des logiciels dédiés à la gestion des ressources (ordonnancement, approvisionnement) et joue le rôle d'interface entre le Datacenter (ressources physiques) et le consommateur ?
   → **Couche 3 (Couche de gestion/contrôle)**.

Partie 2 : Gestion et Contrats (SLA)

La gestion du Cloud vise à gérer les ressources de manière efficace pour atteindre une qualité de service acceptable et respecter les *SLAs (Service-Level Agreements)*.

Exercice 2.1 : SLA et Responsabilité des Couches

Le SLA est un engagement officiel entre le fournisseur et le client définissant la qualité du service attendu, incluant des métriques comme la disponibilité et le temps de réponse.

1. Quelle couche architecturale est la plus concernée par le SLA et doit être accessible aux utilisateurs dans des délais spécifiques ?
   → **La Couche 4 (Couche Physique)**, constituée des ressources physiques (Datacenter). Les violations du SLA par cette couche engendrent des pénalités pour le fournisseur du Cloud.

2. Contrairement aux autres couches, la qualité de service de la Couche 2 (Réseau) n'est pas incluse dans le SLA du Cloud. Cependant, si cette couche n'est pas opérationnelle, le Cloud n'est pas utilisable. Que doit supporter le réseau du Datacenter (Couche Physique) pour respecter le SLA concernant le transfert de données ?
   → Il doit supporter le **très haut débit**.

Exercice 2.2 : Importance de la Gestion de l'Infrastructure

Question : Expliquez pourquoi une mauvaise gestion de l'infrastructure est risquée, en vous basant sur les concepts de QoS (Qualité de Service) et de Coût.

→ Une mauvaise gestion de l'infrastructure peut entraîner l'échec du Cloud entier et affecter la **Qualité de Service (QoS)**. De plus, si le coût de gestion des ressources est élevé, cela augmente le prix d'accès aux services Cloud, ce qui peut engendrer une perte de la clientèle.

Partie 3 : Migration des Applications vers le Cloud

La migration consiste à déplacer une application de son hébergement traditionnel vers le Cloud.

Exercice 3.1 : Caractéristiques et Évolution des Applications

Caractéristique	Application Web	Application Cloud
Modèle	Basé sur le modèle client-serveur	Généralement accessible en tant qu'application Web (SaaS)
Élasticité	Non élastique (ne supporte pas de lourdes charges)	Élastique
Multi-tenant	Non multi-tenant	Multi-tenant
Mesure	Ne fournit pas de mesure quantitative des services	Service mesuré

Exercice 3.2 : Stratégies et Phases de Migration

La migration vers le Cloud comprend plusieurs phases.

1. Quelle est la première phase de la migration, qui consiste à construire une analyse

de rentabilité en examinant l'infrastructure, l'architecture, les risques et les SLAs ?

→ **L'Évaluation.**

2. Une entreprise doit migrer une application critique. Cependant, une partie de cette application a des dépendances basées sur des licences existantes et des interconnexions étendues avec d'autres applications. Quelle stratégie de migration est la plus appropriée ?

   → **La Fusion Strategy.** Elle est utilisée lorsque les applications peuvent être partiellement migrées, mais qu'il existe des dépendances complexes.

3. Une fois les serveurs Cloud configurés et les applications de plateforme déployées, les bases de données et les fichiers sont répliqués. Comment s'appelle cette phase de migration ?

   → **L'Approvisionnement.**

Séance Applicative N°3

Exercice 1 : Cloud Computing

1. Citer et commenter deux caractéristiques clés du *Cloud Computing*.

2. Quels sont les éléments d'une architecture orientée services ?

3. Quels sont les quatre modèles de Cloud ? Expliquez-les en illustrant avec des schémas.

4. Qu'est-ce qui peut favoriser le choix de l'un de ces modèles pour une organisation ?

5. Quels sont les différents services fournis par le Cloud selon les couches **SaaS**, **PaaS** et **IaaS** ?

Exercice 2 : Virtualisation

1. La virtualisation est une technologie de plus en plus adoptée par les entreprises aujourd'hui. Donnez trois raisons fondamentales qui poussent à la virtualisation.

2. Pour être utile de manière opérationnelle, la virtualisation doit respecter deux principes fondamentaux. Lesquels ?

3. Citez deux exemples de ressources virtualisables. Laquelle est mise en avant dans la figure suivante ?

4. Les images ci-dessous mettent en avant deux principaux types de virtualisation. Lesquels ? Donnez la différence entre ces deux types de virtualisation du point de vue du fonctionnement.

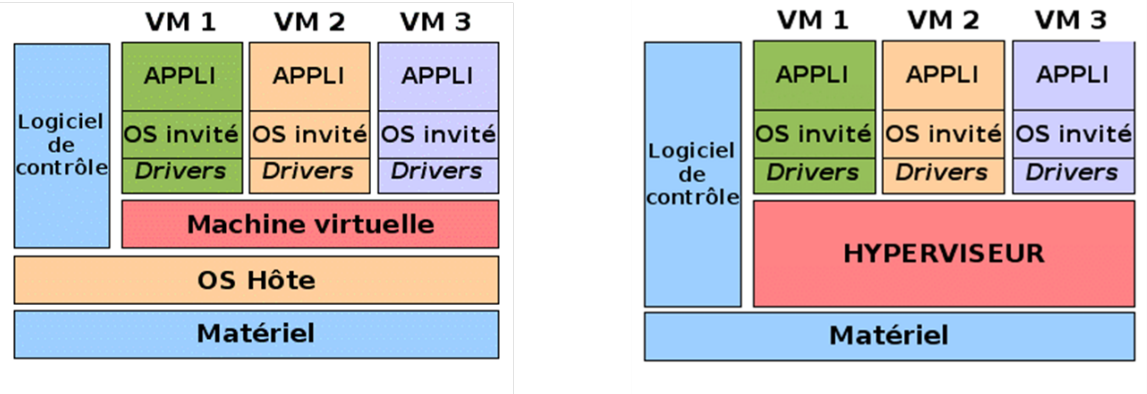

Figure 5.2: Figure A et Figure B : deux principaux types de virtualisation

5. Qu'est-ce qui peut favoriser le choix de l'un de ces modèles pour une organisation ?

6. Quelles sont les différents services fournis par le Cloud selon les couches **SaaS**, **PaaS** et **IaaS** ?

7. Présentez brièvement trois questions de recherche liées à la virtualisation des réseaux.

Séance Applicative N°3: Correction

Exercice 1 : Cloud Computing

1. **Caractéristiques du Cloud Computing :**

   (a) **Libre-service à la demande :** Un consommateur peut fournir unilatéralement des capacités informatiques telles que l'heure du serveur et le stockage en réseau, sans interaction humaine avec le fournisseur.

   (b) **Large accès au réseau :** Les capacités sont disponibles sur le réseau et accessibles via des dispositifs hétérogènes : téléphones, tablettes, PC, etc.

   (c) **Mise en commun des ressources :** Les ressources du fournisseur sont regroupées pour servir plusieurs consommateurs grâce au modèle multi-locataire, avec allocation dynamique.

   (d) **Flexibilité rapide :** Les capacités peuvent être provisionnées rapidement et élastiquement, donnant une impression de ressources illimitées.

   (e) **Service mesuré :** Le système contrôle et optimise l'utilisation des ressources en fonction de métriques adaptées au type de service (stockage, traitement, bande passante, utilisateurs actifs).

2. **Éléments clés d'une SAO (Service Orienté Architecture) :**

   - Un service est autonome et sans état.
   - Un service expose un contrat.
   - Les frontières entre services sont explicites.
   - Les services communiquent par messages.

3. **Modèles de Cloud Computing :**

   (a) **Cloud Hybride :** Combinaison de cloud privé et public pour optimiser sécurité, contrôle et accès à distance.

(b) **Cloud Privé :** Utilisé par une seule organisation, avec contrôle exclusif sur l'infrastructure.

(c) **Cloud Public :** Entièrement fourni par un prestataire externe, infrastructure partagée entre clients.

(d) **Cloud Communautaire :** Partagé par plusieurs organisations avec des besoins communs, géré par les participants ou un fournisseur.

4. **Facteurs favorisant le choix d'un modèle :** Services, sécurité, flexibilité, coût, fiabilité, maintenance facilitée.

5. **Différents services selon les couches :**

   - **SaaS (Software as a Service) :** Accès à un logiciel via interface Web, pas de gestion des mises à jour. Exemples : Google Mail, Dropbox, logiciel comptable en ligne.
   - **IaaS (Infrastructure as a Service) :** Location de machines virtuelles, contrôle complet sur OS et applications, création de réseaux. Exemple : AWS EC2.
   - **PaaS (Platform as a Service) :** Gestion du code applicatif par l'utilisateur, déploiement sur serveurs du prestataire. Exemples : AWS Elastic Beanstalk, Heroku.

6. **Avantages et inconvénients :**

   - **Avantages :** Centralisation des données, réplication, accès simultané, réduction du temps d'administration, scalabilité, archivage.
   - **Inconvénients :** Dépendance à un point central, risques de logiciels malveillants, consommation énergétique, limites du système de fichiers.

Exercice 2 : Virtualisation

1. **Trois raisons de virtualisation :**

   - Mutualisation des capacités des serveurs.

- Réduction du nombre de serveurs.
- Économie des coûts.

2. **Principes fondamentaux de la virtualisation :**
   - **Cloisonnement :** Chaque système invité fonctionne indépendamment et ne peut interférer avec les autres.
   - **Transparence :** Le fonctionnement en mode virtualisé ne change rien pour le SE et les applications.
3. **Ressources virtualisables :**
   - Serveurs
   - Stockage *(mis en avant ici)*
4. **Types de virtualisation :**
   (a) **Virtualisation complète :** Le SE invité n'a pas conscience d'être virtualisé ; émule une machine physique complète.
   (b) **Paravirtualisation :** Fournit une interface aux VMs similaire au matériel sous-jacent ; exemples : Xen, KVM.
5. **Facteurs influençant le choix d'un type de virtualisation :** Sécurité, coût, flexibilité.
6. **Questions de recherche liées à la virtualisation des réseaux :**
   (a) Quels sont les avantages et inconvénients de la virtualisation dans les data centers ?
   (b) Comment la virtualisation des réseaux améliore-t-elle la résilience et la reprise après sinistre ?
   (c) Quelles sont les meilleures pratiques de sécurité pour la virtualisation des réseaux, surtout en environnement multi-locataire ?

Conclusion générale

Le cloud computing représente une transformation majeure dans la manière dont les organisations conçoivent, déploient et gèrent leurs systèmes d'information. Au cours de ce cours, nous avons exploré les concepts fondamentaux du cloud, ses modèles de services (IaaS, PaaS, SaaS), les architectures de déploiement (public, privé, hybride), ainsi que les technologies sous-jacentes telles que la virtualisation, le stockage et la migration des machines virtuelles.

Nous avons également mis en évidence l'importance de la gouvernance du cloud, indispensable pour assurer la sécurité, la conformité, la maîtrise des coûts et la performance des environnements cloud. Les principes, bonnes pratiques et cadres existants permettent aux organisations de gérer efficacement leurs ressources cloud tout en alignant leur exploitation sur les objectifs stratégiques.

Les projets pratiques, séances applicatives et exercices avec corrections ont permis de mettre en œuvre ces notions, afin de renforcer la compréhension technique et organisationnelle du cloud.

Le cloud computing offre de nombreux avantages, tels que la flexibilité, l'évolutivité et la réduction des coûts, mais il exige également une approche structurée pour tirer pleinement parti de son potentiel. La maîtrise des aspects techniques, financiers et organisationnels du cloud constitue donc un facteur clé de réussite pour toute entreprise souhaitant adopter cette technologie de manière sécurisée et fiable.

Bibliographie

Amazon Web Services (2021). Management and governance cloud environment guide. Technical report, Amazon Web Services.

Amazon Web Services (2022). Aws cloud adoption framework: Governance perspective. Technical report, Amazon Web Services.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., and Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4):50–58.

Binary Terms (2022a). What is cloud architecture: Layers and types. https://binaryterms.com/cloud-architecture.html. Consulté en juillet 2025.

Binary Terms (2022b). What is cloud management in cloud computing? working .... https://binaryterms.com/cloud-management.html. Consulté en juillet 2025.

DOIT International (2024). Cloud governance frameworks: A comprehensive guide. https://www.doit.com/blog/cloud-governance-frameworks-a-comprehensive-guide/, consulté en Septembre 2025.

Kavis, M. J. (2014). *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. Wiley CIO Series. John Wiley & Sons, Hoboken, NJ, USA.

LLC, G. (2025). Google cloud documentation. https://docs.cloud.google.com/docs/. Consulté en juillet 2025.

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing. Special publication 800-145, National Institute of Standards and Technology (NIST).

Microsoft Corporation (2025). Microsoft cloud adoption framework. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/. Consulté en juillet 2025.

National Institute of Standards and Technology (NIST) (2011). The nist definition of cloud computing. Special publication 800-145, NIST.