REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Relizane

Faculté des Sciences et Technologie

Département d'Informatique

جامعة غليزان
RELIZANE UNIVERSITY

POLYCOPIE DE COURS CLOUD COMPUTING

(2017/2023)

Présenté par :

DR Yachba khadidja : Maitre de conférences classe A, Université de Relizane

Année Universitaire : 2022/ 2023

Préface

Le Cloud Computing est une technologie qui a révolutionné l'industrie informatique en permettant aux entreprises et aux organisations de disposer de ressources informatiques évolutives et flexibles, sans avoir à investir dans une infrastructure matérielle et logicielle coûteuse. Le Cloud Computing offre un accès à la demande à des ressources informatiques telles que le stockage, le calcul, les bases de données et les services d'applications, en les hébergeant sur des serveurs distants accessibles via Internet.

Ce polycopié sur le Cloud Computing est destiné aux étudiants de Master 1 en informatique option Réseaux et Systèmes Distribués a pour objectif de fournir une introduction à cette technologie, ainsi qu'une compréhension de ses principes fondamentaux et de ses applications.

Le polycopié couvre les principes fondamentaux du Cloud Computing, les différents types de Cloud Computing, les avantages et inconvénients du Cloud Computing, la virtualisation en Cloud Computing, les cas d'utilisation du Cloud Computing, les problèmes de sécurité et les outils de sécurité disponibles.

Ojectifs visés

Le module Cloud Computing peut être très important pour les étudiants en Master Réseaux et Systèmes Distribués, car il permet de comprendre les concepts clés et les technologies associées au stockage, à la gestion et à la fourniture de services dans le cloud. Voici quelques-unes des

raisons pour lesquelles le module Cloud Computing peut être important pour les étudiants en Master Réseaux et Systèmes Distribués :

- Comprendre les concepts de base : Les étudiants apprendront les concepts de base du cloud computing, notamment la virtualisation, la mise en réseau, la sécurité et la gestion de données. Ces concepts sont essentiels pour comprendre comment le cloud fonctionne et comment il peut être utilisé pour fournir des services.
- Comprendre les différentes architectures cloud : Les étudiants apprendront les différentes architectures cloud, telles que les clouds publics, privés et hybrides, et comment elles peuvent être utilisées pour fournir des services en fonction des besoins de l'entreprise.
- Apprendre les technologies clés : Les étudiants apprendront les technologies clés utilisées dans le cloud computing, telles que les services d'infrastructure (IaaS), les plates-formes de développement (PaaS) et les services de logiciels (SaaS). Ils comprendront également les technologies de virtualisation, telles que la virtualisation des serveurs et la virtualisation du stockage.
- Comprendre les défis et les opportunités du cloud computing : Les étudiants apprendront les défis et les opportunités associés au cloud computing, notamment les questions de sécurité, de conformité et de confidentialité des données, ainsi que les avantages potentiels de l'utilisation du cloud, tels que l'évolutivité, la flexibilité et les économies de coûts.

En résumé, le module Cloud Computing peut aider les étudiants en Master Réseaux et Systèmes Distribués à comprendre comment les services informatiques peuvent être fournis dans le cloud, ce qui est de plus en plus important dans un monde où les entreprises et les organisations cherchent à utiliser de plus en plus les technologies du cloud.

L'auteur peut être contacté par courrier électronique à l'adresse suivante:

yachba.khadidja@univ-relizane.dz

FICHE MATIERE

Objectifs	Ce cours permettra à l'étudiant d'assimiler les concepts fondamentaux du Cloud, d'acquérir des connaissances solides de son écosystème. L'étudiant se familiarisera avec les différents modèles du Cloud ainsi que les plateformes les plus utilisées. Il prendra connaissance des enjeux sécuritaires et des bonnes stratégies de migration vers le Cloud.
Connaissances préalables recommandées	Connaissances acquises durant le cursus de formation de la licence : Systèmes informatiques (SI) ou Ingénierie des Systèmes d'Information et du Logiciel (ISIL)
Volume horaire	45H : (1H30 Cours +1H30 TP par semaine)
Moyens Pédagogiques	• Tableaux , data show • Salle de cours • Salle de TP • Polycopiés de cours • Fiches de TP
Evaluation	• Crédits : 3 • Coefficients : 1 • Mode d'évaluation : Contrôle continu, examen écrit final

Carte mentale

La structure de la représentation visuelle de ce document pédagogique est construite en trois sections distinctes, suivies d'une synthèse globale portant sur le domaine du cloud computing. La première section aborde les principes essentiels du cloud computing, la seconde approfondit sur les étapes de la migration vers ce modèle, tandis que la troisième explore les aspects liés à la sécurité dans le domaine du cloud computing.

Figure 1 : Carte mentale

Sommaire

PARTIE I :

Génialité sur le Cloud Computing

I.1 Introduction

La demande croissante pour de nouveaux services informatiques plus économiques a permis l'émergence d'une nouvelle architecture : le Cloud Computing.

Le Cloud Computing représente la cinquième génération de l'informatique après les mainframes, les ordinateurs personnels, le paradigme client/serveur et le web (World Wide Web). Il désigne un modèle dans lequel les ressources telles que la puissance de calcul, le stockage ou encore la bande passante sont fournies comme des services qui peuvent être loués par des utilisateurs via Internet à la demande.

Figure 2: Le Cloud Computing

I.2 Définition du cloud computing

Le cloud computing, également connu sous le nom d'informatique en nuage, est un modèle de prestation de services informatiques sur Internet. Au lieu de stocker et de gérer des données et des applications sur des ordinateurs locaux ou des serveurs physiques, le cloud computing permet d'accéder à ces ressources à partir de n'importe quel endroit et à tout moment, en utilisant une connexion Internet.

En d'autres termes, le cloud computing permet aux utilisateurs d'utiliser des ressources informatiques, telles que des serveurs, des applications, des bases de données et du stockage, sans avoir à les posséder physiquement ou à les gérer eux-mêmes. Les fournisseurs de services cloud fournissent ces ressources via des serveurs distants et les utilisateurs peuvent y accéder en utilisant un navigateur web ou une application spécifique.

Le cloud computing est devenu de plus en plus populaire ces dernières années car il offre une grande souplesse, une évolutivité élevée et des économies de coûts pour les entreprises et les particuliers. Les fournisseurs de services cloud les plus connus sont Amazon Web Services (AWS), Microsoft Azure, Google Cloud et IBM Cloud.

Figure 3 : Le Cloud Computing : Aperçu

I.3 Les principes fondamentaux du Cloud Computing

Les principes fondamentaux du Cloud Computing sont les suivants :

- Accès à la demande : Les ressources informatiques sont disponibles à la demande et sont provisionnées rapidement. Les utilisateurs peuvent accéder aux ressources de manière flexible et en fonction de leurs besoins, sans avoir à se soucier de la configuration ou de la gestion des ressources sous-jacentes.
- Ressources partagées : Les ressources informatiques sont partagées entre plusieurs utilisateurs et applications. Les utilisateurs peuvent accéder aux mêmes ressources sans être limités par des contraintes physiques, telles que la capacité de stockage ou la puissance de traitement.
- Elasticité : Les ressources informatiques peuvent être augmentées ou réduites automatiquement en fonction de la demande. Les utilisateurs ne paient que pour les ressources qu'ils utilisent réellement, ce qui permet de réduire les coûts d'infrastructure.

- Service mesurable : Les ressources informatiques sont mesurées et facturées en fonction de l'utilisation réelle. Les utilisateurs peuvent suivre et contrôler leur utilisation des ressources, ce qui leur permet de gérer les coûts.
- Accès réseau ubiquitaire : Les utilisateurs peuvent accéder aux ressources informatiques depuis n'importe où via Internet. Les utilisateurs peuvent accéder aux ressources depuis n'importe quel appareil connecté à Internet, ce qui offre une grande flexibilité et une mobilité accrue.
- Service géré : Les ressources informatiques sont gérées par le fournisseur de services Cloud. Le fournisseur de services Cloud est responsable de la maintenance, de la mise à niveau et de la sécurité des ressources, ce qui permet aux utilisateurs de se concentrer sur leurs activités principales.

Le Cloud Computing offre une infrastructure informatique flexible, évolutive et gérée par un tiers, ce qui permet aux utilisateurs d'accéder à des ressources informatiques à la demande sans avoir à gérer l'infrastructure sous-jacente.

I.4 Evolution du Cloud Computing

Le cloud computing a connu une évolution rapide et continue depuis sa première apparition. Voici quelques étapes clés de son évolution :

- Début des années 2000 : Les premiers services de cloud computing ont commencé à apparaître, tels que Amazon Web Services (AWS), qui a lancé en 2002 son service de stockage en ligne S3.

- Milieu des années 2000 : Des entreprises telles que Salesforce ont commencé à proposer des logiciels en tant que service (SaaS) pour les entreprises.
- Début des années 2010 : Les plateformes en tant que service (PaaS) ont commencé à gagner en popularité, permettant aux développeurs de créer et de déployer des applications sans avoir à gérer l'infrastructure sous-jacente.
- Milieu des années 2010 : L'infrastructure en tant que service (IaaS) est devenue plus mature, offrant des capacités de stockage et de calcul à grande échelle pour les entreprises.
- 2020 et au-delà : Le cloud hybride, qui combine les services cloud publics et privés, est devenu de plus en plus populaire pour les entreprises souhaitant une flexibilité et un contrôle accrus. L'intelligence artificielle et l'apprentissage automatique ont également commencé à être intégrés dans les services cloud, offrant de nouvelles opportunités pour les entreprises.

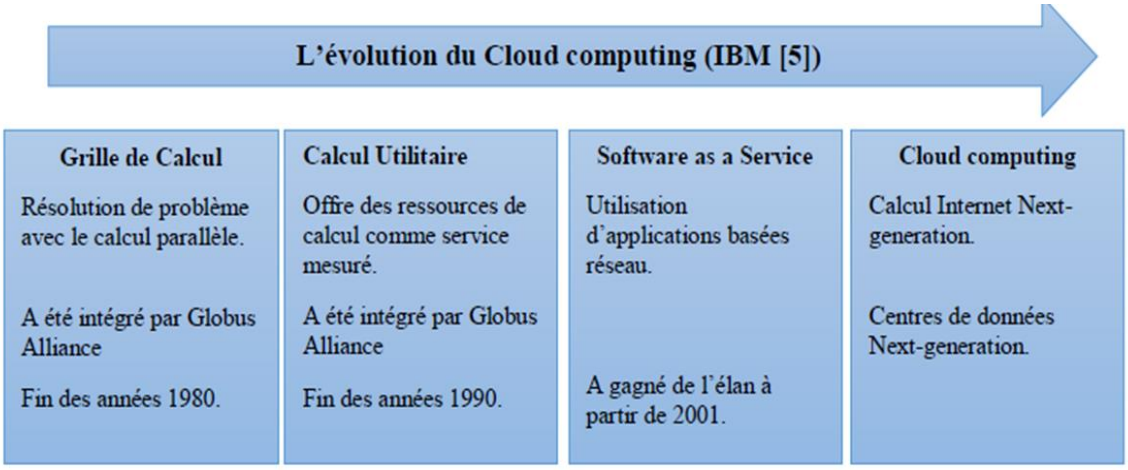

Figure 4 : Evolution du Cloud Computing

L'évolution du cloud computing a été marquée par l'apparition de nouveaux services et technologies, ainsi que par une adoption croissante par les entreprises et les particuliers en raison de ses avantages en termes de flexibilité, de scalabilité et de coûts réduits.

I.5 Les types de cloud computing

Il existe plusieurs types de Cloud Computing, qui se différencient par le type de services fournis, le modèle de déploiement et le type de Cloud utilisé. Voici les principaux types de Cloud Computing :

- Infrastructure-as-a-Service (IaaS) : l'IaaS fournit des ressources informatiques telles que des serveurs, des machines virtuelles, des réseaux et des capacités de stockage à la demande. Les entreprises peuvent utiliser ces ressources pour déployer et exécuter des applications et des services personnalisés.
- Platform-as-a-Service (PaaS) : le PaaS fournit un environnement de développement et de déploiement pour les applications. Les entreprises peuvent utiliser le PaaS pour créer, tester et déployer des applications sans avoir à gérer l'infrastructure sous-jacente.
- Software-as-a-Service (SaaS) : le SaaS fournit des applications et des services à la demande. Les entreprises peuvent accéder à ces applications et services via Internet, sans avoir à les installer localement.

Figure 5 : Les types du Cloud Computing

Le tableau 1 présente des exemples des services selon le type du cloud

Infrastructure as a Service (IaaS)	**Plateforme as a Service (PaaS)**	**Software as a Service (SaaS)**
Amazon Web Services (AWS) : AWS est le fournisseur IaaS le plus populaire et propose une large gamme de services de calcul, de stockage, de base de données et de réseau, ainsi que des outils de gestion et de sécurité.	**Salesforce App Cloud :** Salesforce App Cloud est une plateforme de développement et de déploiement d'applications PaaS qui prend en charge la création d'applications sur mesure pour Salesforce CRM.	**Salesforce :** Salesforce est un fournisseur SaaS populaire qui fournit des solutions de gestion de la relation client (CRM) pour les entreprises, avec des fonctionnalités de vente, de marketing et de service client.
Microsoft Azure : Azure est un service cloud de Microsoft qui offre des services de calcul, de stockage,	**AWS Elastic Beanstalk** : AWS Elastic Beanstalk est une plateforme de développement et	**Zoom :** Zoom est un fournisseur SaaS qui fournit des services de vidéoconférence

de base de données et de réseau, ainsi que des fonctionnalités de machine learning et d'analyse de données.	de déploiement d'applications PaaS qui prend en charge plusieurs langages de programmation, tels que Java, .NET, PHP, Python, Node.js, Ruby, Go, etc.	pour les entreprises, avec des fonctionnalités de collaboration et de partage d'écran.
Google Cloud Platform : Google Cloud Platform propose une infrastructure de cloud computing pour la création, le déploiement et la gestion d'applications et de services, avec des services de calcul, de stockage, de base de données, de réseau et d'analyse de données.	**Microsoft Azure** : Azure offre une plateforme de développement d'applications PaaS qui prend en charge plusieurs langages de programmation, tels que .NET, Java, Python, Node.js, etc. Elle fournit des outils pour le développement, le déploiement, la gestion et la surveillance des applications.	**Dropbox :** Dropbox est un fournisseur SaaS qui fournit un stockage en ligne et une collaboration de fichiers pour les entreprises, avec des fonctionnalités de partage, de synchronisation et de sauvegarde.

Tableau 1 : Exemples des services selon le type du cloud

Exemples :

La figure suivante illustre des exemples de modèles de services dans le cloud computing.

Modèle de service	Outils d'accès et de gestion	Services offerts
SaaS 	Navigateur Web	Réseaux sociaux, suites bureautiques, CRM, traitement vidéo.
PaaS 	Environnement de développement	Langages de programmation, systèmes, gestionnaire de données structurés.
IaaS 	Gestionnaire d'infrastructure virtuelle	Serveurs de calcul, stockage de données, Pare-feu.

Figure 6 : Exemples de services du Cloud Computing

I.6 Modèles de déploiement

Il existe plusieurs modèles de déploiement du cloud computing, qui définissent comment les services cloud sont mis à disposition des utilisateurs. Voici les trois principaux modèles de déploiement du cloud computing :

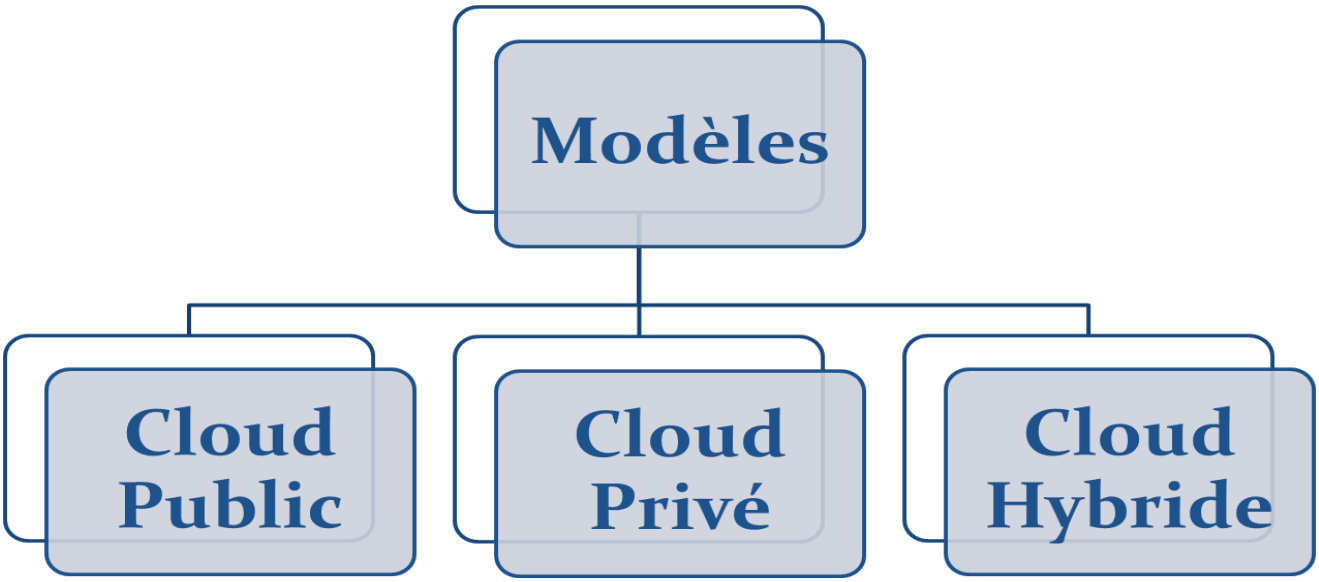

Figure 7 : Modèles de déploiement du Cloud Computing

- Cloud privé : le Cloud privé est un modèle de déploiement dans lequel les ressources informatiques sont dédiées à une seule entreprise ou organisation. Le Cloud privé peut être géré en interne ou par un fournisseur de services Cloud.
- Cloud hybride : le Cloud hybride est un modèle de déploiement dans lequel une entreprise utilise à la fois un Cloud public et un Cloud privé pour répondre à ses besoins en matière de ressources informatiques. Les entreprises peuvent utiliser le Cloud public pour les charges de travail qui nécessitent une évolutivité rapide et le Cloud privé pour les charges de travail sensibles.
- Cloud public : le Cloud public est un modèle de déploiement dans lequel les ressources informatiques sont fournies par des fournisseurs tiers et partagées entre plusieurs clients. Les clients peuvent accéder aux ressources à la demande et ne paient que pour ce qu'ils utilisent.

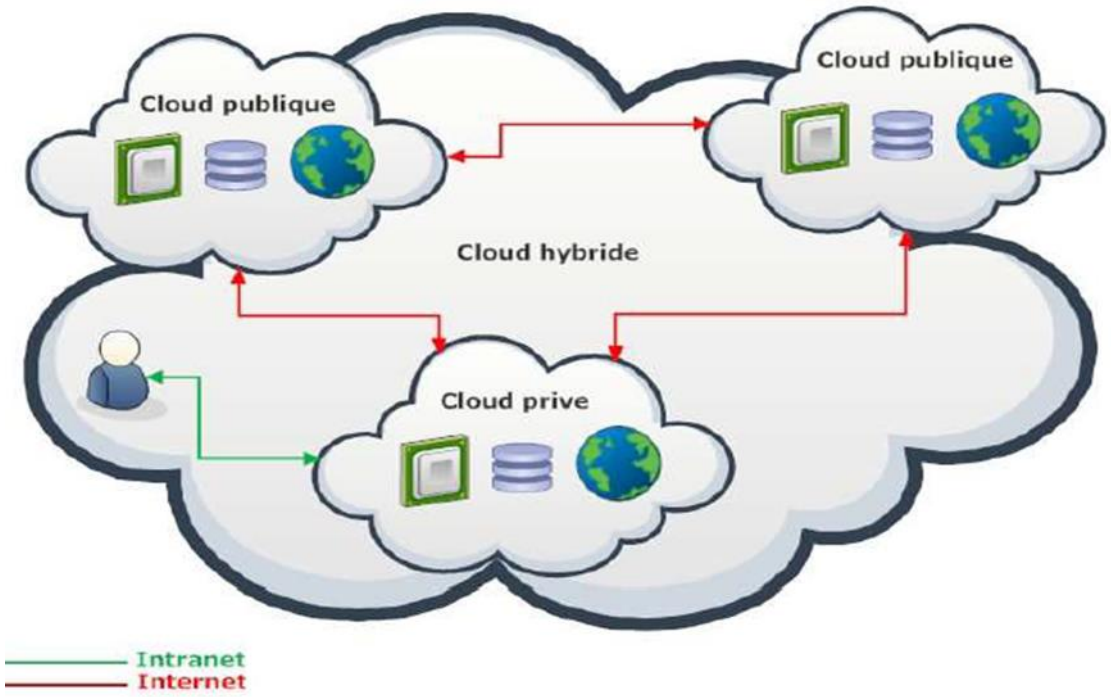

Figure 8 : Modèles de Déploiement du Cloud Computing

Chaque type de Cloud Computing a ses avantages et ses inconvénients, et les entreprises doivent choisir le type de Cloud qui convient le mieux à leurs besoins en matière de ressources informatiques et de sécurité des données.

I.7 Comparaison entre le Cloud public et le Cloud privé

En raison des spécificités des clouds privés et publics, il est essentiel de clarifier les distinctions fondamentales entre ces deux catégories de services cloud. Le tableau ci-dessous présent la solution jugée la plus avantageuse selon divers critères.

	Cloud Privé	**Cloud Public**
Haute Sécurité	✓	
Personnalisation	✓	

Réduction des Coûts		✓
Haute Évolutivité et Flexibilité		✓
Faible Latence	✓	
Gestion Facile		✓
Haute Concurrence		✓
Mesures de Protection des Lois et Règlements	✓	

Tableau 2 : Comparaison entre le cloud public et privé

Les informations mentionnées ci-dessus mettent en lumière de manière évidente que les deux modèles d'informatique en cloud présentent des avantages et des inconvénients distincts. Le cloud public offre des services hautement flexibles et évolutifs à un coût relativement bas, tandis que le cloud privé propose des services personnalisés avec un niveau de sécurité élevé. Les entreprises ont également la possibilité d'adopter une approche intermédiaire, connue sous le nom de "cloud hybride", qui combine des services de cloud privé et public tout en permettant le partage de données et d'applications entre les deux.

Il est vrai que le modèle de cloud hybride présente certaines limitations. Par exemple, sa complexité croissante rend sa maintenance et sa protection plus difficiles. De plus, l'intégration de différentes plateformes, données et applications dans le cloud peut s'avérer être un défi important. De surcroît, la compatibilité de l'infrastructure doit être prise en considération lors du déploiement d'un cloud hybride.

Cependant, les avantages de ce modèle ne sont pas négligeables. Il offre aux utilisateurs la possibilité d'exploiter au mieux les atouts du cloud privé et du cloud public. Par exemple, les entreprises peuvent utiliser des environnements de cloud privé pour leurs charges de travail informatiques tout en complétant leur infrastructure avec des ressources provenant du cloud public.

I.8 Cas d'utilisation du Cloud Computing

Le Cloud Computing est une technologie qui permet aux entreprises de disposer de ressources informatiques flexibles et évolutives sans avoir à investir dans l'infrastructure matérielle et logicielle. Les applications du Cloud Computing sont nombreuses et peuvent être utilisées dans de nombreux secteurs d'activité. Voici quelques exemples de cas d'utilisation du Cloud Computing :

- Stockage et sauvegarde de données : Les services de stockage en nuage tels que Amazon S3, Google Drive, Dropbox et OneDrive offrent une solution économique pour stocker des fichiers, des documents, des images et des vidéos en ligne. Les services de sauvegarde en nuage tels que Backblaze et Carbonite offrent une solution pour sauvegarder les données sur un serveur distant.
- Calcul haute performance : Les entreprises peuvent utiliser les services de calcul en nuage pour exécuter des calculs complexes et gourmands en ressources, tels que l'analyse de données, la modélisation de simulations et la création d'applications. Les

services de calcul en nuage tels qu'Amazon EC2 et Microsoft Azure offrent des instances de calcul haute performance pour répondre à ces besoins.

- Développement d'applications : Les services de développement en nuage tels que Microsoft Azure et Google App Engine offrent une plateforme de développement pour les développeurs qui souhaitent créer des applications en nuage.
- Internet des objets (IoT) : Le Cloud Computing offre une plateforme pour stocker et traiter les données générées par les appareils IoT tels que les capteurs, les caméras et les machines. Les services IoT tels que AWS IoT et Microsoft Azure IoT offrent des solutions de traitement des données IoT en nuage.
- Services Web : Les services de Web en nuage tels que Amazon Web Services (AWS) et Microsoft Azure offrent des plateformes pour les développeurs qui souhaitent créer et déployer des applications Web évolutives.
- Analyse de données : Les services d'analyse de données en nuage tels que Amazon Redshift et Microsoft Azure SQL Data Warehouse permettent aux entreprises de stocker, de traiter et d'analyser des données volumineuses en utilisant des algorithmes d'apprentissage automatique et des outils d'analyse de données.
- Collaboration : Les services de collaboration en nuage tels que Microsoft Teams et Slack offrent une plateforme pour les équipes de travail qui souhaitent communiquer, partager des fichiers et collaborer sur des projets.

Ces exemples montrent la variété des applications du Cloud Computing et les avantages qu'ils peuvent offrir aux entreprises. Les avantages clés sont l'évolutivité, la flexibilité, la réduction des coûts et la disponibilité à la demande des ressources informatiques.

I.9 Succés du cloud computing

Le cloud computing a connu un immense succès au cours des dernières années, avec une adoption croissante dans de nombreux secteurs et industries.

Voici quelques raisons qui ont contribué à ce succès :

Économies d'échelle : le cloud computing permet aux entreprises de réduire les coûts en utilisant des ressources informatiques partagées et en évitant les investissements initiaux élevés associés à la création et à la maintenance de leur propre infrastructure informatique.

Évolutivité : Les services cloud sont hautement évolutifs, ce qui signifie que les entreprises peuvent facilement augmenter ou réduire leur utilisation de ressources informatiques en fonction de leurs besoins en temps réel.

Accès à distance : le cloud computing permet aux utilisateurs d'accéder à leurs applications et données de n'importe où et à tout moment, tant qu'ils ont une connexion Internet.

Flexibilité : le cloud computing offre une grande flexibilité aux entreprises en leur permettant de choisir les services dont elles ont besoin, tels que le stockage de données, les services de calcul, les services de base de données, etc.

Sécurité : Les fournisseurs de services cloud mettent en place des mesures de sécurité avancées pour protéger les données de leurs clients, notamment des contrôles d'accès, des pare-feu, des systèmes de détection d'intrusion, etc.

Le cloud computing a connu un succès phénoménal en raison de ses avantages économiques, de son évolutivité, de sa flexibilité et de sa sécurité accrue.

1.10 Avantages du cloud compuing

Le cloud computing présente plusieurs avantages, notamment :

- Accès à distance : Le cloud computing permet d'accéder à des applications et des données à partir de n'importe quel endroit et à tout moment, tant qu'une connexion Internet est disponible.
- Économies de coûts : Les entreprises peuvent économiser de l'argent en utilisant le cloud computing car elles n'ont pas à acheter et à gérer leur propre infrastructure informatique. Les coûts d'exploitation, de maintenance et de mise à niveau sont également réduits.
- Flexibilité : Le cloud computing permet aux entreprises de s'adapter rapidement à l'évolution des besoins de leur activité en ajoutant ou en supprimant des ressources informatiques selon les besoins.
- Évolutivité : Le cloud computing permet de facilement et rapidement augmenter ou diminuer la capacité de stockage et de traitement, selon les besoins de l'entreprise.

- Sécurité : Les fournisseurs de services cloud ont généralement des mesures de sécurité en place pour protéger les données de leurs clients. Les entreprises peuvent également prendre des mesures supplémentaires pour renforcer la sécurité de leurs données dans le cloud.
- Collaboration : Le cloud computing permet aux employés de travailler ensemble sur des projets en temps réel, peu importe où ils se trouvent.

En somme, le cloud computing offre une grande souplesse et une évolutivité élevée, ainsi que des économies de coûts et une meilleure sécurité pour les entreprises.

I.11 Inconvénients du cloud computing

Bien que le Cloud Computing présente de nombreux avantages, il comporte également des inconvénients. Voici quelques-uns des principaux inconvénients associés au Cloud Computing :

- Sécurité des données : La sécurité des données est l'un des principaux inconvénients du Cloud Computing. Les entreprises doivent faire confiance à des tiers pour stocker et protéger leurs données sensibles, ce qui peut entraîner des risques de violation de la sécurité et de confidentialité des données.
- Dépendance à l'égard du fournisseur de services Cloud : Les entreprises qui utilisent le Cloud Computing sont dépendantes des fournisseurs de services Cloud pour la disponibilité, la sécurité et les performances de leurs applications et de leurs données.

Si le fournisseur rencontre des problèmes, cela peut affecter la disponibilité et la qualité des services.

- Coûts : Bien que le Cloud Computing puisse offrir des économies de coûts, les coûts peuvent augmenter rapidement si les entreprises ne surveillent pas leur utilisation de manière proactive. Les entreprises peuvent également être confrontées à des coûts imprévus pour des services supplémentaires, tels que la migration des données vers le Cloud.
- Performance : La performance des applications peut être affectée par la latence du réseau et la qualité de la connexion Internet. Les entreprises doivent veiller à ce que leurs connexions Internet soient suffisamment rapides et fiables pour prendre en charge les exigences de performance de leurs applications.
- Conformité réglementaire : Les entreprises doivent s'assurer que leurs données sont conformes aux réglementations en matière de sécurité et de confidentialité des données, telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne. Les fournisseurs de services Cloud peuvent être situés dans différents pays, ce qui peut rendre difficile la conformité à certaines réglementations.

Bien que le Cloud Computing présente de nombreux avantages, les entreprises doivent prendre en compte les inconvénients associés à cette technologie avant de décider de migrer leurs ressources informatiques vers le Cloud. Les entreprises doivent comprendre les risques et les

coûts associés à l'utilisation du Cloud Computing et prendre des mesures pour atténuer ces risques.

I.12 Le cloud et la virtualisation

Le Cloud Computing et la virtualisation sont deux technologies étroitement liées. La virtualisation permet de créer plusieurs machines virtuelles sur une seule machine physique, tandis que le Cloud Computing permet d'accéder à des ressources informatiques à la demande via Internet. Voici comment la virtualisation et le Cloud Computing sont liés :

- La virtualisation est souvent utilisée dans les infrastructures de Cloud Computing pour fournir des machines virtuelles à la demande. Les fournisseurs de services Cloud peuvent utiliser la virtualisation pour diviser les ressources informatiques de leurs serveurs physiques en plusieurs machines virtuelles, qui peuvent être utilisées par plusieurs clients.
- La virtualisation peut aider à maximiser l'utilisation des ressources dans les centres de données en permettant à plusieurs machines virtuelles de s'exécuter sur une seule machine physique. Cela peut réduire le nombre de serveurs physiques nécessaires, ce qui peut réduire les coûts et la consommation d'énergie.
- Le Cloud Computing peut utiliser des technologies de virtualisation pour fournir des ressources informatiques à la demande. Les fournisseurs de services Cloud peuvent créer des instances de machines virtuelles à la demande, permettant aux clients d'obtenir rapidement des ressources informatiques sans avoir à gérer l'infrastructure sous-jacente.

- La virtualisation peut également aider à la flexibilité des charges de travail dans le Cloud Computing. Les fournisseurs de services Cloud peuvent utiliser des technologies de virtualisation pour allouer rapidement des ressources supplémentaires aux clients qui en ont besoin, puis les réduire lorsque la charge diminue.

La virtualisation est un élément clé de l'infrastructure de Cloud Computing, permettant aux fournisseurs de services Cloud de fournir des ressources informatiques à la demande de manière flexible et rentable.

I.12.1 Cloud computing et virtualisation: les différences

Alors que les données informatiques augmentent de façon exponentielle, et que les entreprises font de plus en plus appel aux processus informatiques pour gagner en productivité et en compétitivité, la possibilité de réduction des coûts de gestion des infrastructures informatiques est une des principales priorités des entreprises.

Ces dernières années, plusieurs moyens sont apparus pour aborder cette réduction des coûts, parmi lesquels, la virtualisation, et le Cloud Computing.

La virtualisation et le Cloud Computing sont deux concepts différents, mais pourtant complémentaires.

La virtualisation est une technique pour l'exécution de plusieurs systèmes d'exploitation indépendants de façon virtuelle sur une seule machine physique. Ce terme fut utilisé pour la première fois vers les années 1960 en référence à une machine virtuelle (parfois appelée pseudo machine).

La virtualisation des ressources est au cœur de la plupart des architectures Cloud. Le concept de la virtualisation permet une vue logique abstraite sur les ressources physiques et serveurs, les bases de données, les réseaux et les logiciels.

L'idée de base est de mettre en commun les ressources physiques et les gérer comme un tout. Les demandes individuelles peuvent ensuite être servies selon les besoins de ces pools de ressources.

I.12.2 Types de virtualisation en cloud computing

Il existe plusieurs types de virtualisation qui peuvent être utilisés dans le Cloud Computing. Voici les principaux types de virtualisation :

- La virtualisation de serveur : la virtualisation de serveur permet de créer plusieurs machines virtuelles sur un seul serveur physique. Les fournisseurs de services Cloud peuvent utiliser la virtualisation de serveur pour créer des instances de machines virtuelles à la demande, permettant aux clients d'obtenir rapidement des ressources informatiques.

D'après VMWare, la majeure partie des serveurs opèrent à moins de 15 % de leurs capacités effectives, ce qui donne lieu à une prolifération excessive et à une complexité accrue. La virtualisation des serveurs résout ces problèmes d'efficacité en autorisant l'exécution de multiples systèmes d'exploitation sur un unique serveur physique.

Un autre point clé en faveur de cette forme de virtualisation réside dans sa capacité à générer des économies substantielles sans générer de modifications majeures au sein du département informatique. En effet, quelques instances d'hyperviseurs ainsi qu'une interface

de gestion prennent le relais en remplacement de dizaines, voire de centaines de serveurs physiques.

De manière concrète, cette approche simule effectivement les serveurs physiques en altérant leurs caractéristiques telles que leur identité, leurs numéros, leurs processeurs et leurs systèmes d'exploitation. Cette démarche libère l'utilisateur de la charge constante liée à la gestion de ressources serveur complexes.

- La virtualisation de bureau : la virtualisation de bureau permet de créer des environnements de bureau virtuels pour les utilisateurs finaux. Les utilisateurs peuvent accéder à leur bureau virtuel depuis n'importe quel appareil connecté à Internet, ce qui peut être pratique pour les entreprises ayant des travailleurs distants.
- La virtualisation de stockage : la virtualisation de stockage permet de regrouper plusieurs ressources de stockage physiques en une seule ressource de stockage virtuelle. Les utilisateurs peuvent accéder à cette ressource de stockage virtuelle depuis n'importe quel emplacement, ce qui peut simplifier la gestion des données.

La virtualisation du stockage englobe une approche qui rassemble l'espace de stockage matériel provenant de divers périphériques de stockage interconnectés pour former une entité simulée unique, administrée à partir d'une console de commande centralisée. Cette méthode de gestion du stockage dans le cloud se révèle particulièrement bénéfique pour des tâches telles que la sauvegarde, l'archivage et la récupération de données, en masquant la complexité inhérente à l'architecture de stockage réelle et physique.

Cette stratégie de stockage trouve fréquemment son utilisation au sein des réseaux de stockage. Elle offre un éventail d'avantages, tels que la réduction des temps d'indisponibilité, l'amélioration de la vitesse et des performances.

- La virtualisation de réseau : la virtualisation de réseau permet de créer plusieurs réseaux virtuels sur une seule infrastructure physique. Les utilisateurs peuvent gérer ces réseaux virtuels de manière indépendante, ce qui peut offrir plus de flexibilité et de sécurité.

La virtualisation du réseau implique une récréation complète d'un réseau physique à l'aide de composants logiciels. Cette approche consiste à agréger les ressources disponibles au sein d'un réseau en divisant la bande passante totale en canaux distincts et isolés.

L'essence de cette technique réside dans sa capacité à simplifier la complexité sous-jacente du réseau en le fragmentant en éléments gérables. Cette technologie facilite la surveillance, tout en améliorant la visibilité de l'utilisation des données. Par ailleurs, elle contribue à renforcer la sécurité en restreignant les mouvements de fichiers entre plusieurs réseaux.

- La virtualisation d'application : la virtualisation d'application permet de créer des environnements d'exécution d'applications isolés les uns des autres. Cela peut aider à éviter les conflits entre les applications et à maximiser l'utilisation des ressources.

La virtualisation d'application représente une avancée significative dans la manière dont les applications sont exécutées et gérées au sein d'un environnement informatique. Cette approche

novatrice permet de créer des environnements d'exécution isolés pour chaque application, ce qui se traduit par une série d'avantages et de bénéfices concrets.

Lorsque nous parlons d'environnements d'exécution isolés, il s'agit de créer des "conteneurs" ou des "bulles" virtuelles autour de chaque application. Chaque application fonctionne comme si elle était installée sur son propre système dédié, avec ses propres dépendances logicielles et ses bibliothèques spécifiques. Cette isolation évite les conflits potentiels qui pourraient survenir entre différentes applications qui partagent le même environnement d'exécution. Par exemple, une application qui nécessite une version spécifique d'une bibliothèque ne perturbera pas d'autres applications qui utilisent une version différente de cette bibliothèque.

L'un des avantages majeurs de la virtualisation d'application est sa capacité à optimiser l'utilisation des ressources. En isolant les applications les unes des autres, les ressources du système, telles que le processeur, la mémoire et le stockage, peuvent être allouées de manière plus efficace et équilibrée. Les applications n'ont pas besoin de rivaliser pour les ressources, ce qui peut entraîner une augmentation des performances globales du système. De plus, en optimisant l'utilisation des ressources, la virtualisation d'application peut contribuer à prolonger la durée de vie des infrastructures existantes, en retardant potentiellement la nécessité d'investir dans de nouveaux matériels.

En outre, la virtualisation d'application simplifie également le déploiement et la gestion des applications. Les environnements d'exécution virtuels peuvent être créés rapidement et reproduits facilement sur différents systèmes. Cela facilite le déploiement cohérent et

reproductible des applications, que ce soit sur des serveurs locaux, dans le cloud ou sur des appareils clients.

En résumé, les différentes formes de virtualisation peuvent être utilisées dans le Cloud Computing pour créer des environnements informatiques virtuels qui peuvent être gérés de manière flexible et rentable.

I.12.3 Consolidation, orchestration et mutualisation en cloud compuing

La consolidation, l'orchestration et la mutualisation sont des concepts importants en matière de Cloud Computing. Voici une explication de chacun de ces termes :

Consolidation : la consolidation consiste à regrouper plusieurs machines virtuelles sur une seule machine physique. La consolidation peut aider à maximiser l'utilisation des ressources informatiques, car elle permet de réduire le nombre de machines physiques nécessaires.

Orchestration : l'orchestration consiste à coordonner l'utilisation de plusieurs machines virtuelles afin de fournir un service informatique cohérent. L'orchestration peut inclure la gestion des ressources informatiques, la répartition de la charge de travail et la coordination des opérations entre les machines virtuelles.

Mutualisation : la mutualisation consiste à partager les ressources informatiques entre plusieurs utilisateurs ou applications. La mutualisation peut aider à réduire les coûts et à améliorer l'utilisation des ressources, car elle permet à plusieurs utilisateurs de partager les mêmes ressources informatiques.

En combinant ces trois concepts, les fournisseurs de services Cloud peuvent créer des environnements informatiques rentables et flexibles. Par exemple, en utilisant la consolidation, les fournisseurs de services Cloud peuvent réduire le nombre de machines physiques nécessaires, ce qui peut réduire les coûts. En utilisant l'orchestration, les fournisseurs de services Cloud peuvent coordonner l'utilisation de plusieurs machines virtuelles pour fournir des services cohérents et fiables. En utilisant la mutualisation, les fournisseurs de services Cloud peuvent partager les ressources informatiques entre plusieurs utilisateurs ou applications, ce qui peut aider à maximiser l'utilisation des ressources et à réduire les coûts.

I.12.4 Virtual Machine Manager (VMM) / Hyperviseur

La mise en place d'une machine virtuelle (également appelée VM pour Virtual Machine) requiert l'intégration d'une couche logicielle supplémentaire sur la machine physique. Cette couche d'abstraction est positionnée entre le matériel physique et le système d'exploitation, et est désignée sous le nom d'hyperviseur ou de moniteur de machine virtuelle (VMM).

L'hyperviseur assume le rôle d'un médiateur entre les systèmes invités : il alloue des intervalles de temps du processeur ainsi que des ressources à chacun d'eux, achemine les demandes d'entrées-sorties vers les ressources matérielles réelles, et garantit l'isolation des invités dans leurs propres environnements distincts.

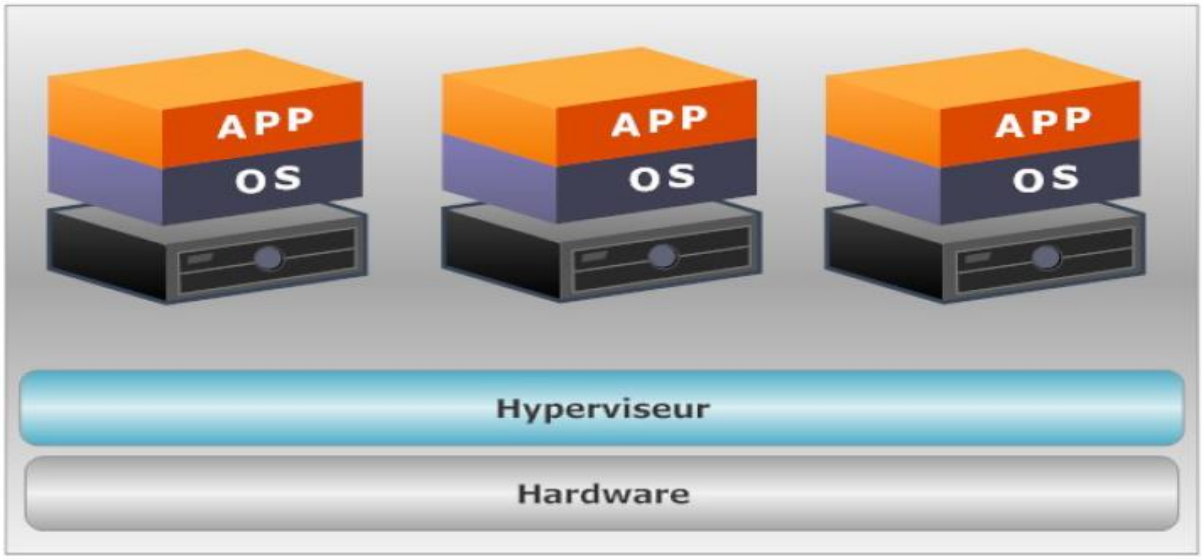

Figure 9: Hyperviseur

La création et le fonctionnement d'une machine virtuelle (VM), également connue sous l'acronyme VM pour "Virtual Machine", englobent une étape cruciale qui implique l'ajout d'une strate logicielle supplémentaire au sein de la machine physique sous-jacente. Cette strate logicielle, qui agit comme une sorte de médiateur entre le matériel physique et le système d'exploitation, est désignée sous le terme "hyperviseur" ou "moniteur de machine virtuelle" (VMM).

L'hyperviseur, en tant qu'entité de contrôle essentielle, assume un rôle fondamental dans le déploiement et la gestion des machines virtuelles. Il agit comme un arbitre au sein de l'environnement virtualisé, orchestrant les interactions entre les différentes entités en présence. Concrètement, il répartit le temps de traitement du processeur entre les diverses VMs, veillant ainsi à équilibrer les ressources disponibles et à empêcher qu'une VM ne monopolise l'ensemble des capacités de calcul.

De plus, l'hyperviseur joue un rôle critique dans la gestion des opérations d'entrées-sorties. Il canalise et redirige les demandes d'entrées-sorties émanant des machines virtuelles vers les ressources matérielles réelles, tout en s'assurant que ces interactions se déroulent de manière ordonnée et efficace. Cela garantit une allocation appropriée des ressources et contribue à maintenir des performances fluides et stables.

Un autre aspect essentiel de la fonction de l'hyperviseur est de maintenir l'isolation entre les différentes machines virtuelles présentes sur la même machine physique. Cette séparation stricte prévient tout conflit potentiel entre les systèmes invités et permet à chaque VM de fonctionner de manière autonome dans son propre environnement virtuel. Ainsi, même si une VM rencontre des problèmes ou subit des pannes, les autres machines virtuelles ne sont pas directement affectées, préservant ainsi l'intégrité globale du système.

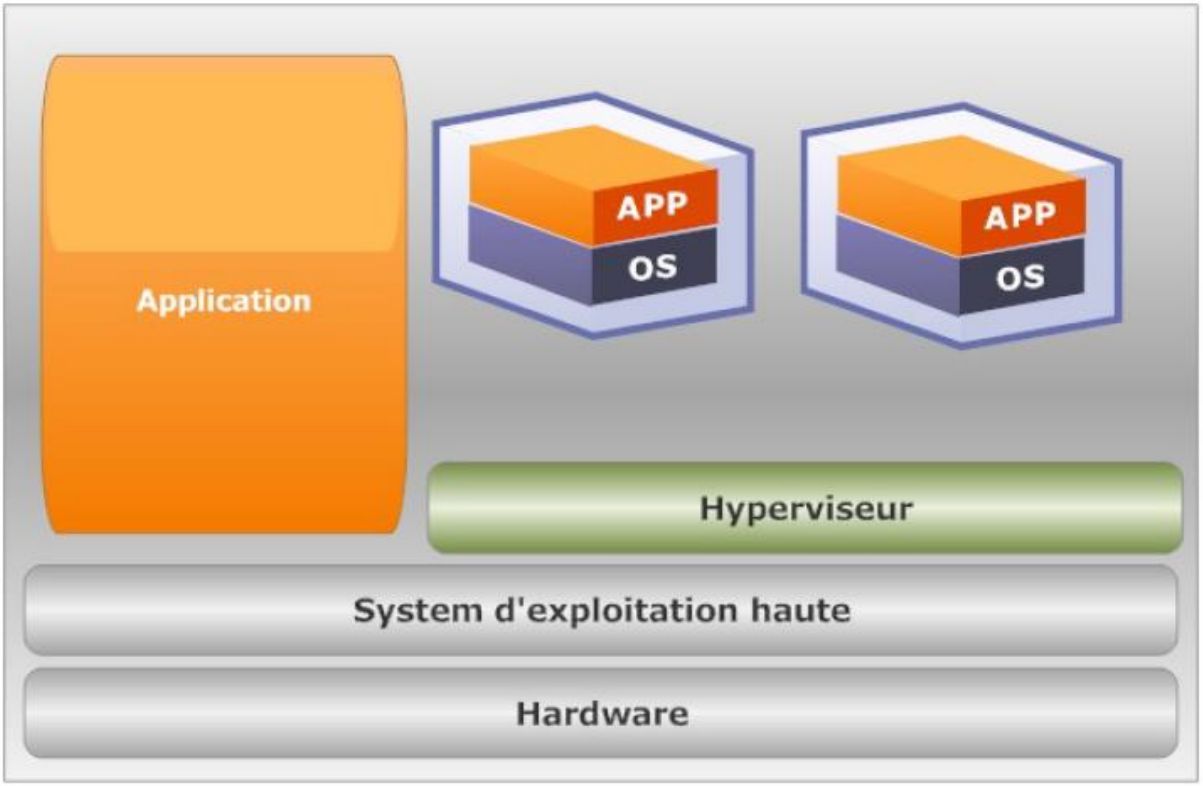

Figure 10 : Architecture d'un environnement vituel

I.12.5 Virtual Machine Manager (VMM) / Hyperviseur

La comparaison entre une architecture physique et une architecture virtualisée se fait sur plusieurs aspects. Voici quelques points clés pour illustrer les différences entre les deux :

- **Nature de l'Infrastructure** :

Physique : Utilisation de matériel physique dédié, y compris des serveurs, des disques durs, et des composants matériels spécifiques.

Virtualisée : Utilisation de logiciels de virtualisation pour créer des machines virtuelles (VM) sur une seule infrastructure physique. Ces VM partagent les ressources matérielles de la machine hôte.

- **Flexibilité et Évolutivité :**

Physique : Moins flexible, car chaque serveur est généralement dédié à une tâche spécifique.

Virtualisée : Plus flexible, permettant la création, la modification et la suppression rapides de VM en fonction des besoins. Cela facilite également l'évolutivité en ajoutant ou en retirant des ressources virtuelles.

- **Utilisation des Ressources :**

Physique : Utilisation moins efficace des ressources, car chaque serveur a ses propres ressources dédiées.

Virtualisée : Une utilisation plus efficace des ressources, car plusieurs VM peuvent partager les ressources d'une seule machine physique.

- **Isolation des Applications :**

Physique : Une application s'exécute sur un serveur physique dédié sans interférence directe avec d'autres applications.

Virtualisée : Les VM sont isolées les unes des autres, ce qui permet l'exécution d'applications différentes sur une même machine physique sans interférence directe.

- **Redondance et Disponibilité :**

Physique : La redondance nécessite souvent du matériel supplémentaire et peut être coûteuse.

Virtualisée : La redondance peut être mise en œuvre plus facilement à travers des VM dupliquées ou des solutions de haute disponibilité.

- **Gestion et Maintenance :**

Physique : La gestion et la maintenance nécessitent des interventions physiques sur chaque serveur.

Virtualisée : La gestion est centralisée, ce qui facilite les mises à jour, la sauvegarde et la restauration des VM.

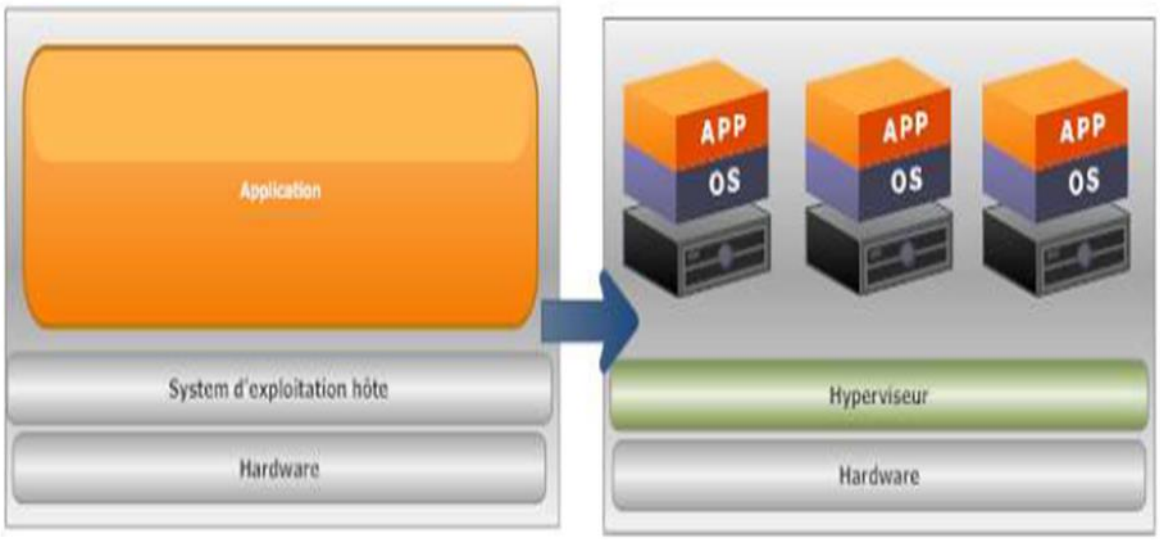

Figure 11 : Comparaison entre architecture physique et virtualisée

L'architecture physique est plus traditionnelle et utilise des serveurs dédiés, tandis que l'architecture virtualisée offre une flexibilité accrue en permettant l'exécution de plusieurs systèmes d'exploitation et applications sur une seule machine physique. Le choix entre les deux dépend des besoins spécifiques de l'entreprise en termes de performances, d'évolutivité et de gestion des ressources.

I.13 Sécurité, disponibilité, SLA dans le cloud compuing

La sécurité, la disponibilité et les accords de niveau de service (SLA) sont des considérations importantes pour toute entreprise qui envisage d'utiliser le Cloud Computing. Voici un aperçu de ces aspects :

- Sécurité : Le Cloud Computing peut offrir un niveau de sécurité élevé pour les données et les applications, mais cela dépend en grande partie de la manière dont la sécurité est

mise en œuvre et gérée. Il est important de comprendre les politiques de sécurité du fournisseur de Cloud, de vérifier la conformité réglementaire, d'appliquer des mesures de sécurité supplémentaires et de gérer l'authentification et l'autorisation des utilisateurs.

- Disponibilité : La disponibilité est cruciale pour les entreprises qui ont besoin d'un accès constant à leurs applications et à leurs données. Les fournisseurs de Cloud Computing offrent généralement des garanties de disponibilité dans leurs accords de niveau de service (SLA), qui spécifient les temps d'arrêt autorisés et les dédommagements prévus en cas d'interruption de service.
- Accords de niveau de service (SLA) : Les SLA définissent les engagements contractuels du fournisseur de Cloud en matière de disponibilité, de performance, de temps de réponse, de sécurité, de sauvegarde, de restauration de données, etc. Il est important de comprendre les SLA du fournisseur de Cloud, de vérifier leur conformité avec les besoins de l'entreprise, et de s'assurer que les SLA sont régulièrement surveillés et respectés.

Il est également important de noter que la sécurité, la disponibilité et les SLA sont interdépendants et qu'une approche holistique est nécessaire pour garantir la réussite de l'utilisation du Cloud Computing. Les entreprises doivent évaluer les risques, élaborer une stratégie de sécurité claire, mettre en place des processus de surveillance et de conformité et travailler en étroite collaboration avec leurs fournisseurs de Cloud pour garantir la sécurité et la disponibilité de leurs données et applications dans le Cloud.

I.14 Conclusion sur la partie I

Un cloud (« nuage ») est un ensemble de matériels, de raccordements réseau et de logiciels qui fournit des services que les individus et les collectivités peuvent exploiter à volonté depuis n'importe où dans le monde . Le cloud computing est un basculement de tendance : au lieu d'obtenir de la puissance de calcul par acquisition de matériel et de logiciel, le consommateur se sert de puissance mise à sa disposition par un fournisseur via Internet .

Les caractéristiques essentielles d'un nuage sont la disponibilité mondiale en libre-service, l'élasticité, l'ouverture, la mutualisation et le paiement à l'usage.

En conclusion, le cloud computing et la virtualisation sont deux concepts interconnectés qui ont profondément transformé le paysage informatique. La virtualisation a ouvert la voie en permettant la création de machines virtuelles sur une infrastructure physique, tandis que le cloud computing a étendu cette idée en fournissant des services informatiques à la demande via Internet.

Le cloud computing offre une agilité accrue, une élasticité et une scalabilité, permettant aux entreprises de provisionner et de gérer rapidement des ressources sans avoir à investir massivement dans une infrastructure physique. Il offre des modèles de service tels que l'Infrastructure en tant que Service (IaaS), la Plateforme en tant que Service (PaaS) et le Logiciel en tant que Service (SaaS), offrant une variété d'options aux utilisateurs.

La virtualisation reste un élément fondamental du cloud computing, permettant l'optimisation des ressources, la consolidation des serveurs, et une meilleure gestion des charges de travail. Elle contribue à l'efficacité opérationnelle en permettant la création, la migration et la gestion agiles des machines virtuelles.

En combinant la virtualisation et le cloud computing, les organisations peuvent bénéficier d'une infrastructure informatique plus flexible, rentable et facile à gérer. Ces technologies continuent d'évoluer, apportant des innovations constantes pour répondre aux besoins changeants des entreprises dans un monde de plus en plus axé sur la connectivité, la mobilité et l'évolutivité.

PARTIE II :

La Migration vers

Le Cloud Computing

II.1 Migration le cloud computing

La migration vers le Cloud Computing est une décision importante pour toute entreprise qui souhaite améliorer son infrastructure informatique. Voici quelques éléments à considérer lors de la migration vers le Cloud Computing :

- Choix de la plateforme Cloud : il existe plusieurs fournisseurs de services Cloud, chacun ayant ses propres avantages et inconvénients. Il est important de choisir une plateforme Cloud qui répond aux besoins spécifiques de l'entreprise.
- Évaluation des coûts : la migration vers le Cloud Computing peut impliquer des coûts initiaux élevés. Il est important de prendre en compte les coûts de migration, les coûts de formation et les coûts d'utilisation de la plateforme Cloud.
- Sécurité et conformité : la migration vers le Cloud Computing peut soulever des préoccupations en matière de sécurité et de conformité. Il est important de s'assurer que la plateforme Cloud choisie répond aux normes de sécurité et de conformité de l'entreprise.
- Gestion du changement : la migration vers le Cloud Computing peut impliquer un changement significatif dans la façon dont les employés travaillent. Il est important de

prévoir une formation adéquate pour les employés afin qu'ils puissent travailler efficacement dans un environnement Cloud.

- Évaluation des avantages : la migration vers le Cloud Computing peut offrir de nombreux avantages, tels que la réduction des coûts informatiques, l'amélioration de la flexibilité et de la scalabilité, et l'amélioration de l'efficacité opérationnelle. Il est important de déterminer quels avantages sont les plus importants pour l'entreprise et comment ils peuvent être réalisés grâce à la migration vers le Cloud Computing.

En résumé, la migration vers le Cloud Computing est une décision importante qui doit être prise en considérant plusieurs facteurs, notamment le choix de la plateforme Cloud, l'évaluation des coûts, la sécurité et la conformité, la gestion du changement et l'évaluation des avantages. Il est important de travailler avec des professionnels expérimentés pour faciliter la migration et s'assurer que l'entreprise tire le meilleur parti du Cloud Computing.

II.2 Types de migration vers le cloud

Il existe plusieurs types de migration vers le Cloud Computing, chacun ayant ses propres avantages et inconvénients. Voici les principaux types de migration vers le Cloud Computing :

- Migration complète : la migration complète consiste à transférer toutes les applications et données de l'entreprise vers le Cloud. Cela peut prendre du temps et être coûteux, mais cela peut offrir des avantages significatifs en matière de coûts et de flexibilité.

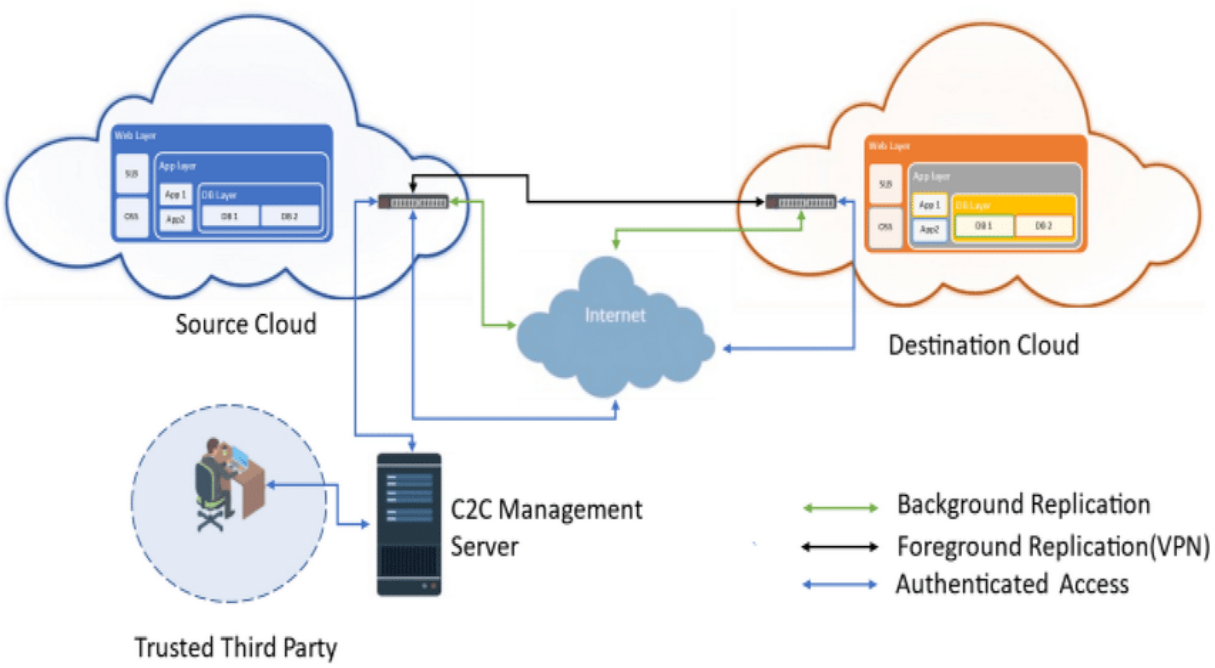

Figure 12 : Schéma de la Migration complète

- Migration partielle : la migration partielle consiste à transférer certaines applications et données vers le Cloud, tout en conservant d'autres applications et données sur site. Cela peut offrir une transition plus douce vers le Cloud et permettre à l'entreprise de conserver certains systèmes existants.

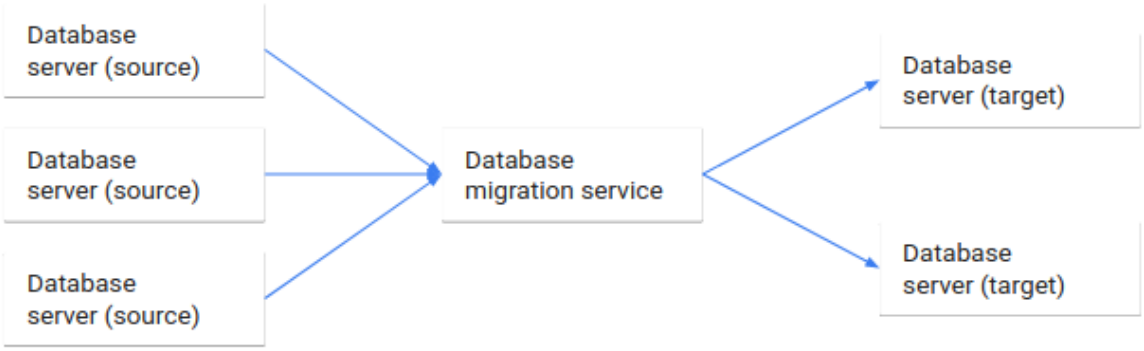

Figure 13 : Exemple de Migration partielle

Le schéma précédant illustre ce processus de migration de base de données. La migration de base de données implique le transfert de données depuis une ou plusieurs

bases de données sources vers une ou plusieurs bases de données cibles, en utilisant un service dédié de migration. Une fois cette opération achevée, l'intégralité des données initialement présentes dans les bases sources se trouve désormais dans les bases cibles, éventuellement restructurées. Les utilisateurs accédant aux bases sources sont ensuite redirigés vers les bases de données cibles, et les bases sources sont ensuite désactivées.

- Migration hybride : la migration hybride consiste à utiliser une combinaison de Cloud public et privé. Cela peut offrir plus de flexibilité et de sécurité pour certaines applications et données tout en permettant à l'entreprise de conserver le contrôle sur certaines applications et données.

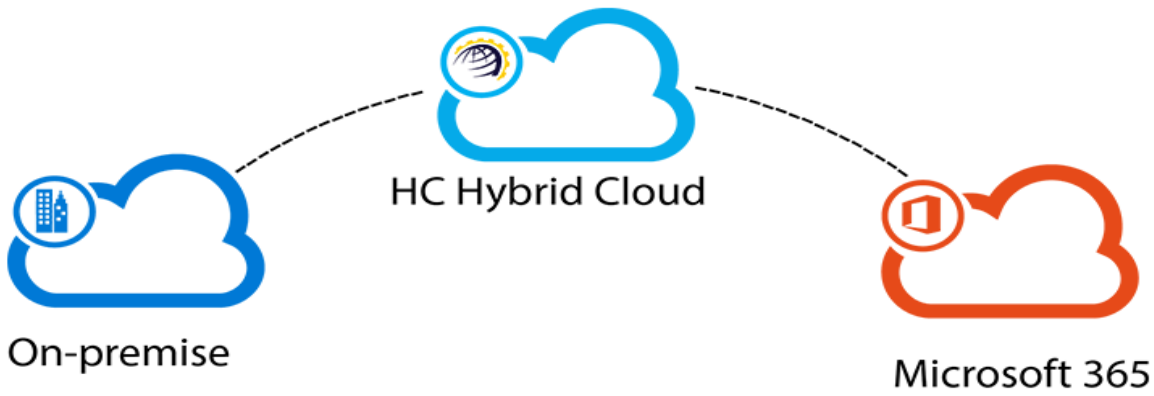

Figure 14 : Exemple de Migration hybride vers Microsoft Office 365

La figure 14 illustre un exemple de migration hybride vers Microsoft Office 365. La migration hybride vers Microsoft Office 365 est un processus qui permet de déplacer progressivement des services et des données depuis un environnement sur site (sur les

serveurs locaux d'une entreprise) vers le service cloud Office 365 de Microsoft. Cette approche offre une transition en douceur, permettant aux entreprises de conserver une partie de leurs services localement tout en exploitant les avantages du cloud.

- Migration en nuage parallèle : la migration en nuage parallèle consiste à migrer des applications et des données vers le Cloud tout en conservant des systèmes existants sur site. Cela permet à l'entreprise de tester les nouvelles applications et données sur le Cloud tout en conservant la continuité des opérations sur site.

Figure 15: Exemple de Migration parallèle

La migration parallèle est une approche où les deux environnements (ancien et nouveau) coexistent simultanément pendant une période définie, ce qui permet une transition progressive sans interruption majeure des services.

Imaginons une entreprise qui souhaite migrer son système de messagerie vers une nouvelle plateforme tout en minimisant l'impact sur la productivité des utilisateurs.

- **Configuration initiale :**

Ancien Système : L'entreprise utilise actuellement un serveur de messagerie local, par exemple Microsoft Exchange 2010.

Nouveau Système : La décision est prise de migrer vers Microsoft Office 365.

- **Configuration de la migration parallèle :**

Un environnement hybride est mis en place, permettant la coexistence des deux systèmes. Cela implique une connexion entre le serveur Exchange local et les services cloud d'Office 365.

Les utilisateurs continuent d'utiliser leur boîte aux lettres sur l'ancien système tout en ayant une nouvelle boîte aux lettres créée sur Office 365.

- **Migration progressive des boîtes aux lettres :**

Les boîtes aux lettres des utilisateurs sont migrées progressivement de l'ancien serveur Exchange vers Office 365.

Pendant la migration, les utilisateurs ont accès à leurs boîtes aux lettres sur les deux environnements, ce qui permet une transition transparente.

- **Synchronisation d'annuaires :**

Une synchronisation d'annuaires est établie pour maintenir la cohérence des informations sur les utilisateurs entre les deux environnements.

Tests et Validation :

Les équipes informatiques effectuent des tests approfondis pour s'assurer que la migration se déroule sans problème.

Les utilisateurs continuent d'accéder à leurs boîtes aux lettres sur l'ancien système et la nouvelle plateforme pendant les tests.

- **Finalisation de la migration :**

Une fois que toutes les boîtes aux lettres ont été migrées avec succès et que les tests ont été validés, la migration est finalisée.

Les utilisateurs sont complètement basculés vers Office 365, et l'ancien serveur Exchange est désactivé.

Formation des utilisateurs :

Si nécessaire, des sessions de formation peuvent être organisées pour aider les utilisateurs à s'adapter à l'interface et aux fonctionnalités de la nouvelle plateforme.

La migration parallèle offre l'avantage d'une transition en douceur sans perturbation majeure des services, ce qui est crucial pour les entreprises cherchant à minimiser l'impact sur la productivité pendant le processus de migration.

Chaque type de migration a ses propres avantages et inconvénients, et il est important de prendre en compte les besoins spécifiques de l'entreprise avant de décider du type de migration à entreprendre. Il est également important de travailler avec des professionnels expérimentés pour faciliter la migration et s'assurer que l'entreprise tire le meilleur parti du Cloud Computing.

II.3 Méthodologie de migration

La migration vers le Cloud Computing peut être un processus complexe, mais en suivant une méthodologie de migration bien définie, l'entreprise peut minimiser les risques et les perturbations. Voici une méthodologie de migration typique :

- Évaluation de l'environnement existant : il est important d'effectuer une évaluation complète de l'environnement informatique existant, y compris les applications, les données, les serveurs et les réseaux. Cette évaluation aidera à identifier les applications et les données qui sont les plus adaptées à la migration vers le Cloud, ainsi que les contraintes et les problèmes potentiels.
- Planification de la migration : une fois que l'évaluation de l'environnement existant est terminée, il est temps de planifier la migration. Cela comprend la sélection de la plateforme Cloud, la définition des objectifs de migration, l'évaluation des coûts et des délais, et la définition des tâches et des ressources nécessaires.
- Préparation pour la migration : la préparation pour la migration implique la configuration de la plateforme Cloud, la migration des données et des applications vers la plateforme Cloud, la vérification de la compatibilité des applications et la préparation des employés pour la migration.
- Migration : la migration elle-même consiste à transférer les applications et les données vers la plateforme Cloud. Cela peut être réalisé par étapes, en commençant par les applications et les données les plus critiques.

- Tests et vérification : une fois que la migration est terminée, il est important de tester et de vérifier les applications et les données pour s'assurer qu'elles fonctionnent correctement sur la plateforme Cloud.
- Formation et support : une fois que la migration est terminée, il est important de fournir une formation et un support adéquats aux employés pour qu'ils puissent travailler efficacement dans l'environnement Cloud.
- Surveillance et maintenance : enfin, il est important de surveiller et de maintenir régulièrement l'environnement Cloud pour s'assurer qu'il fonctionne de manière optimale et qu'il répond aux besoins de l'entreprise.

En suivant une méthodologie de migration bien définie, l'entreprise peut minimiser les risques et les perturbations associés à la migration vers le Cloud Computing, tout en maximisant les avantages potentiels tels que la réduction des coûts informatiques, l'amélioration de la flexibilité et de la scalabilité, et l'amélioration de l'efficacité opérationnelle.

II.4 Outils de migration vers le cloud

Il existe de nombreux outils de migration disponibles pour aider les entreprises à migrer leurs applications et leurs données vers le Cloud Computing. Voici quelques exemples d'outils couramment utilisés :

- AWS Migration Hub : cet outil fourni par Amazon Web Services (AWS) permet de suivre les migrations d'applications vers AWS et de centraliser les informations sur les applications migrées.
- Azure Migrate : cet outil fourni par Microsoft Azure permet de migrer des applications vers Azure et fournit des évaluations pré-migration, des recommandations de dimensionnement et des rapports de migration.
- Google Cloud Migrate : cet outil fourni par Google Cloud Platform (GCP) permet de migrer des applications vers GCP et fournit des outils d'évaluation et de planification de la migration, ainsi que des outils de migration automatisés.
- CloudEndure : cet outil permet de migrer des charges de travail vers le Cloud avec une interruption minimale et fournit une réplication continue des données.
- VMware Cloud on AWS : cet outil permet de migrer des charges de travail vers AWS tout en conservant les mêmes outils de gestion et de sécurité que sur site.
- Carbonite Migrate : cet outil permet de migrer des charges de travail physiques, virtuelles et de Cloud à Cloud et offre des options de migration automatisées.

Ces outils peuvent aider les entreprises à simplifier et à accélérer le processus de migration vers le Cloud Computing en fournissant des évaluations, des recommandations, des outils de migration automatisés et des fonctionnalités de suivi pour garantir une migration réussie. Cependant, il est important de noter que le choix de l'outil dépendra des besoins et des exigences

spécifiques de l'entreprise, et il est conseillé de consulter des experts en migration pour choisir le meilleur outil pour votre cas d'utilisation spécifique.

II.5 Avantages de migration vers le cloud computing

La migration vers le Cloud Computing offre de nombreux avantages pour les entreprises, voici les principaux :

- Réduction des coûts : La migration vers le Cloud permet aux entreprises de réduire leurs coûts d'infrastructure informatique, en évitant l'achat et la maintenance de serveurs physiques, de stockage et de réseaux coûteux. Les entreprises ne paient que pour les services dont elles ont besoin, ce qui peut réduire les coûts opérationnels et les coûts d'investissement.
- Évolutivité : Le Cloud Computing permet aux entreprises de répondre rapidement aux changements dans leur environnement commercial en ajustant leur utilisation des services Cloud. Les entreprises peuvent facilement augmenter ou réduire leur utilisation des ressources Cloud en fonction de la demande, ce qui peut aider à éviter les problèmes de capacité et de surutilisation.
- Accès facile aux données : Les données stockées dans le Cloud sont facilement accessibles de n'importe où, ce qui permet aux employés de travailler de manière plus flexible et de collaborer plus facilement. Les données peuvent être partagées entre les

employés et les sites distants en temps réel, ce qui peut améliorer la productivité et la communication.

- Sécurité : Les fournisseurs de services Cloud ont des mécanismes de sécurité sophistiqués pour protéger les données de leurs clients contre les menaces externes et internes. Les données sont souvent sauvegardées régulièrement et les fournisseurs de services Cloud disposent généralement de plans de reprise après sinistre pour garantir la continuité des activités en cas de catastrophe.
- Innovation : Le Cloud Computing peut aider les entreprises à innover plus rapidement en leur permettant de tester rapidement de nouvelles idées et de nouvelles applications sans investir dans une infrastructure coûteuse. Les entreprises peuvent développer, tester et déployer rapidement des applications sur le Cloud, ce qui peut réduire le temps nécessaire pour lancer de nouveaux produits ou services.

En conclusion, la migration vers le Cloud Computing peut offrir de nombreux avantages aux entreprises, notamment des économies de coûts, une évolutivité facile, un accès facile aux données, une sécurité améliorée et la possibilité d'innover plus rapidement. Cependant, les entreprises doivent également prendre en compte les difficultés et les défis potentiels pour garantir une migration réussie.

II.6 Etapes de migration vers le cloud

Suivre une approche stratégique et déterminée pour une migration vers le cloud peut éviter de nombreux tracas technologiques. En suivant ces cinq étapes, l’entreprise pourra mener à bien sa transition.

- **Étape 1 : pourquoi migrer ?**

Les entreprises se dirigent vers le cloud pour toute sorte de raisons, mais s'intéresser à ce qui pousse les organisations à migrer vers le cloud est extrêmement révélateur de leurs motivations centrales. Le mouvement vers l'utilisation du cloud pour une gestion et un stockage solides des données, sans parler des systèmes analytiques, montre le degré de maturité du secteur.

Les e-mails, les messageries, la collaboration et le partage de fichiers représentent des solutions à rendement immédiat du cloud et dominent le marché depuis longtemps. Les entreprises dépassent actuellement cette phase initiale de déploiement pour s'enfoncer davantage dans le cloud.

À mesure qu'elles le font, elles délaissent de plus en plus les modèles d'adoption du cloud classiques basés sur les coûts associés. Même si le cloud peut offrir des tarifs inférieurs aux systèmes classiques, ce qui est le cas pour un niveau de base, les entreprises prennent conscience que les frais associés au cloud suivent un modèle complexe et demandent une gestion attentive.

La transition vers des systèmes de cloud plus sophistiqués, et donc potentiellement plus coûteux, montre que les attentes des entreprises en matière de migration vers le cloud vont au-delà d'une réduction des dépenses.

POURQUOI L' ENTREPRISE PASSE-T-ELLE AU CLOUD ? C'est la première question que les responsables de l'entreprise doivent poser avant toute migration vers le cloud. Le monde des affaires a des préoccupations qui dépassent la réduction des dépenses. Les entreprises doivent donc aller au-delà des offres de base et examiner leurs propres motivations pour passer au cloud. **Parmi les questions à prendre en compte :**

- ✓ Quels sont les problèmes technologiques que l'entreprise souhaite résoudre avec le cloud ?

- ✓ Comment le cloud soutiendra-t-il les objectifs commerciaux à court et long terme fixés par l'entreprise ?
- ✓ Comment le passage au cloud affectera-t-il la compétitivité de l'entreprise sur le marché ?
- ✓ Quels changements au niveau opérationnel et dans la culture d'entreprise souhaite l'entrepsise soutenir en passant au cloud ?

Environ 64 % des entreprises se préoccupent d'obtenir une Visibilité totale sur leur configuration en cloud. Et 63 % déclarent oeuvrer pour prévoir les frais liés au Cloud computing. De plus, les plans pour le cloud ont tellement évolué que de nombreuses entreprises ne comprennent plus la portée complète de leur configuration7. Pour éviter ce genre d'étalement du cloud, il convient d'avoir une intention claire et manifeste derrière chaque phase de sa migration vers le cloud.

En considérant les raisons qui poussent l'entreprise à passer au cloud, il faut éviter d'effectuer cette migration par réaction.

Répondre aux exigences du marché est essentiel, mais simplement réagir à quelques événements marquants peut conduire à une migration cloud trop rapide, à laquelle l'entreprise n'est pas préparée.

Prendre le temps de déterminer tous les facteurs motivant de migration vers le cloud, au lieu de céder aux pressions pour la commencer.

Il est crucial de bien comprendre les problèmes de l'organisation à l'origine du passage au cloud pour tirer le maximum de valeur de la technologie. Sinon, les entreprises risquent de résoudre des problèmes isolés sans obtenir d'avantages opérationnels majeurs.

Faire preuve de discernement peut éviter à l'organisation une migration hâtive vers le cloud qui ne donnera pas les résultats escomptés.

Une fois que les motivations de passage au cloud sont fixées, l'entreprise doit réfléchir à la façon dont elle va le faire. Considérez en particulier :

- Les applications et les services existants qui ne pourront pas fonctionner correctement dans un environnement cloud.
- La façon dont l'entreprise sépare les différents types de données après la migration entre les environnements du cloud et internes.
- Les formations que les employés devront suivre pour être à l'aise avec de nouveaux services et applications.
- L'impact du passage au cloud sur le comportement du réseau.

Toutes ces questions sont directement liées aux problèmes globaux.

- Si le plan de l'entreprise pour le cloud favorise les systèmes côté client, elle n'aura quasiment pas à actualiser son réseau WAN.
- L'entreprise doit toutefois former ses représentants du service client pour qu'ils soient prêts à dépanner ses clients durant la transition.
- Il est crucial de prendre en compte ces questions techniques centrales quand on se demande si on doit ou non migrer vers le cloud.

- **Etape 2 : évaluer l'environnement et choisir les charges de travail**

L'effort introspectif ne s'arrête pas une fois que les motivations de la migration vers le cloud ont été fixées. Une fois que les objectifs sont clairs, la configuration actuelle doit être examinée avec un nouveau regard. Pour ce faire, il faut une analyse poussée de tout l'environnement applicatif, ainsi que des systèmes sous-jacents à ces applications. Une fois ces processus accomplis, il ne faut pas négliger l'impact qu'aura le passage au cloud sur les comportements des utilisateurs. Il faut Veiller à prendre ces changements en compte quand l'entreprise planifie la migration.

- Les flux de tâches qui croisent les différents services et applications sont critiques pour les performances de l'entreprise.
- Si certaines des applications sont des goulets d'étranglement, elles peuvent faire rapidement dérailler les opérations. Ceci s'applique particulièrement dans le cas où ces applications recourent à d'anciennes méthodologies pouvant créer un délai de traitement dans la gestion et la maintenance.
- Une compréhension précise des interactions des applications et de leur interdépendance permettra de guider la mise en oeuvre du cloud en donnant une visibilité.
- Les sites pouvant nécessiter une mise à niveau du réseau

  Les applications à traiter en priorité pendant la transition.

  Les indicateurs de performance nécessaires pour évaluer les solutions cloud visant à résoudre les problèmes actuels.

- Ne passez pas au cloud sans tout d'abord comprendre les nuances de l’environnement applicatif actuel.
- Sinon, des limitations ou problèmes préexistants peuvent entraver la transition.

Chaque application aura un comportement légèrement différent dans différentes configurations IT. Il faut également déterminer les charges susceptibles de migrer facilement vers le cloud. Parmi les éléments à prendre en compte à propos des applications :

- Leur interaction avec des données considérées comme trop sensibles pour le cloud public.
- •Leur traitement de données réglementées au point que le recours à un prestataire de service tiers est impossible.
- Leur teneur en architectures ou en code de programmation qui fonctionnent mal dans un environnement virtuel.
- Leur dépendance à des sources si diverses que leur déplacement hors du site produirait une latence excessive lors de leur accès aux bases de données.

Les performances en environnements virtuels peuvent considérablement varier selon les architectures spécifiques mises en oeuvre dans les machines virtuelles. Cela donne au processus de migration vers le cloud une part d'incertitude. Parallèlement, l'acheminement des données sur Internet vers des applications du cloud ajoute une certaine latence aux délais potentiels dus à la virtualité du système.

C'est pourquoi les entreprises doivent effectuer le monitoring des performances applicatives dans leur configuration existante. Puis elles doivent déterminer le niveau acceptable de perturbation sur

les solutions sensibles à ces performances. Enfin, elles doivent envisager une migration stratégique de ces solutions.

L'évolutivité du cloud peut être idéale à certains services et applications ayant beaucoup de contenu. Toutefois, négliger les évaluations de performance peut conduire les organisations à faire des compromis que leurs clients ne peuvent pas se permettre.

Même si les questions techniques sont au coeur de la réussite d'une migration vers le cloud, il ne faut pas négliger la manière dont les utilisateurs interagissent avec les systèmes quand l'entreprise élabore ses plans. Parmi les principaux points à prendre en compte :

• La diversité des appareils utilisés pour accéder aux applications.

• La diversité accrue des sources internes et externes vers lesquelles les données sont acheminées.

La dépendance croissante des réseaux sans fil avec des utilisateurs qui accèdent aux applications du cloud à l'aide de leurs appareils mobiles.

Les performances des applications du cloud dépendent considérablement du réseau sous-jacent et des systèmes de partage des données. Il est ainsi essentiel de prendre en compte les différents moyens d'accès des utilisateurs à un service pour préparer votre configuration de déplacement.

Étape 3: durée de migration

Une fois la migration vers le cloud en menant des analyses en interne a été préparée . Le moment est maintenant venu de sauter le pas et de mettre en oeuvre les nouveaux services dans le cloud.

En général, ce processus peut se résumer à quatre étapes :

• Choisir les prestataires de services.

• Identifier les responsabilités dans la relation avec eux.

• Ajuster la configuration en interne autour des services cloud.

• Susciter l'adhésion des utilisateurs.

Choisir le prestataire de services adapté aux besoins de l'entreprise est la première étape essentielle du processus. Il s'agit aussi d'un domaine où les entreprises ont plus d'options qu'auparavant.

Même si les géants du cloud que sont Amazon Web Services (AWS), Google Cloud Platform et Microsoft Azure se partagent toujours la part du lion, des prestataires de services régionaux offrant des solutions spécialisées gagnent des parts de marché.

L'ensemble du secteur lié au cloud public progresse selon un taux de croissance annuel composé de 22 %. Même les méga-fournisseurs ne peuvent suivre ce rythme d'expansion.

Le cloud computing peut rendre floues les limites de la responsabilité dans la relation. Il faut définir avec le prestataire de services les responsabilités respectives. Il est, par exemple, essentiel de savoir quel niveau de contrôle que l'entreprise garde sur ses applications dans l'environnement du cloud.

Les différents prestataires de cloud proposent des niveaux variés de personnalisation et de responsabilité pour le client. De plus, les besoins peuvent varier d'une application à l'autre.

Le cloud computing a souvent des effets secondaires intéressants sur les attentes vis-à-vis des services IT. Les utilisateurs étant habitués à pouvoir accéder aux services et aux données partout et à tout moment, ils attendent la même chose des applications internes.

De plus, la rationalisation de l'intégration et du partage des données dans le cloud incite les entreprises à faire monter en puissance des processus similaires en interne. Le besoin d'emprunter des ressources de gestion pour régir les systèmes dans le cloud vient se rajouter à l'équation. Le résultat : les organisations doivent revoir leurs méthodes de gestion des configurations classiques en même temps que celles du cloud.

Toutes les percées techniques du monde n'auront aucun impact tant que les employés ne seront pas à l'aise avec la technologie et tant qu'ils n'adopteront pas le changement.

Environ 12 % des responsables it ont mentionné que la plus grande difficulté rencontrée pendant leur migration vers le cloud était une mauvaise formation des employés. Cela fait de la formation la difficulté la plus fréquemment citée devant, notamment :

• Une mauvaise intégration (10 %).

• Une assistance technique médiocre (9 %).

• Des paramètres de sécurité erronés (5 %).

Les obstacles techniques à la réussite de la migration vers le cloud sont importants,

Il faut Prendre le temps de former les utilisateurs professionnels et IT sur l'impact que le cloud aura sur eux. Ils seront ainsi prêts pour le jour J.

Étape 4 : évaluer la réussite

Le temps où les opérations IT résidaient en arrière-plan et soutenaient les entreprises comme des gouffres financiers est révolu.

À la place, les services IT sont confrontés à un nouveau climat opérationnel. D'un côté, ils peuvent prétendre à des budgets plus importants auprès de la direction car la technologie est un outil déterminant. De l'autre, l'accent mis sur la technologie impose de faire la preuve du retour sur investissement.

Les responsables IT ne peuvent pas se permettre de simplement migrer vers le cloud en espérant que cela sera rentable. Au contraire, ils doivent mesurer et évaluer constamment les performances afin de prouver que leurs efforts et les investissements consentis se traduisent en valeur directe pour l'entreprise. considérable.

Le cloud computing apporte uniquement de la valeur à la mesure de l'engagement de l'entreprise. Déplacer quelques applications vers le cloud n'apporte pas beaucoup de retour sur investissement. Toutefois, une transition à grande échelle peut dégager une valeur.

Étape 5 : ne pas oublier les plans futurs

Une transition vers le cloud peut intervenir à un moment charnière. Pour certaines entreprises, il s'agit d'une décision pour déplacer une charge de travail cruciale vers le cloud public. Pour d'autres, il peut s'agir d'une première étape visant à tout déplacer à terme dans le cloud.

Quel que soit le type de processus migratoire vers le cloud (et même si l’entreprise vise à devenir une entreprise 100 % dans le cloud), ce n'est pas parce que les nouveaux services fonctionnent que la transition s'achève.

Les principaux avantages du cloud dérivent de sa flexibilité et de son évolutivité. C'est pourquoi la réussite d'une migration dépend d'une culture d'entreprise bien établie visant une amélioration continue et en phase avec les futures stratégies de l'entreprise.

Une exécution réussie des stratégies du cloud à long terme s'appuie sur une connaissance constante des performances des services et des applications. Mesurer les résultats initiaux d'une migration et s'arrêter là ne suffit pas.

Il est essentiel que les responsables IT et les dirigeants de l'entreprise s'accordent sur les futures stratégies pour établir la réussite à long terme après une migration vers le cloud. Établir un partenariat interne efficace facilite l'adhésion de tous aux priorités et à la définition des feuilles de route pour les services afin de rester en phase avec lesexigences du marché.

II.7 Migration vers le Cloud : difficultés rencontrées

La migration vers le Cloud Computing peut être une entreprise complexe et difficile pour les entreprises, et il y a plusieurs défis et difficultés à prendre en compte. Voici quelques-unes des difficultés les plus courantes rencontrées lors de la migration vers le Cloud :

- Complexité de l'infrastructure existante : La plupart des entreprises ont des infrastructures informatiques complexes et hétérogènes qui peuvent rendre la migration vers le Cloud difficile. Les applications et les données peuvent être dispersées sur des serveurs physiques et virtuels, des centres de données locaux et distants, ce qui peut rendre la migration complexe.
- Sécurité et conformité : La sécurité et la conformité sont des préoccupations majeures pour les entreprises lors de la migration vers le Cloud. Les entreprises doivent s'assurer que leurs données sont protégées contre les menaces internes et externes, qu'elles

respectent les réglementations en matière de confidentialité des données et qu'elles peuvent répondre aux exigences en matière d'audit.

- Interopérabilité et intégration : Les entreprises doivent être en mesure d'intégrer leurs applications et leurs données avec d'autres applications et services dans le Cloud et sur site. Cela peut être difficile car les différentes plateformes et technologies peuvent ne pas être compatibles.
- Coûts : La migration vers le Cloud peut être coûteuse, notamment en termes de coûts de transition et de coûts d'abonnement. Les entreprises doivent évaluer soigneusement les coûts et les avantages de la migration pour déterminer si elle est rentable.
- Compétences et formation : Les entreprises doivent disposer des compétences nécessaires pour gérer leur environnement Cloud. Cela peut nécessiter une formation et un développement de compétences supplémentaires pour les employés de l'entreprise.
- Risque de perte de données : Les entreprises doivent être conscientes du risque de perte de données lors de la migration vers le Cloud. Elles doivent s'assurer que leurs données sont sauvegardées régulièrement et qu'elles disposent d'un plan de récupération de données en cas de perte de données.

II.8 Migration Prématurée vers le cloud

La migration vers le cloud peut être une étape importante et stratégique pour une entreprise, mais cela ne doit pas être fait de manière précipitée ou prématurée. Voici quelques raisons pour lesquelles une migration prématurée vers le cloud peut poser des problèmes :

Manque de préparation : Si une entreprise ne se prépare pas correctement avant de migrer vers le cloud, elle risque de rencontrer des problèmes de compatibilité, de performances et de sécurité qui pourraient entraîner une interruption de ses activités.

Coûts élevés : Si une entreprise migre trop tôt vers le cloud, elle peut se retrouver à payer des coûts élevés pour des services dont elle n'a pas besoin ou qui ne conviennent pas à ses besoins spécifiques.

Risques de sécurité : Si une entreprise migre vers le cloud sans avoir pris en compte les mesures de sécurité nécessaires, elle risque de compromettre la sécurité de ses données et de ses applications.

Perte de contrôle : Si une entreprise migre vers le cloud sans avoir une bonne compréhension de la manière dont elle utilisera les services cloud, elle risque de perdre le contrôle sur ses données et ses applications.

Conflits internes : Si une entreprise migre vers le cloud sans impliquer les parties prenantes clés ou les équipes de développement, cela peut entraîner des conflits internes qui peuvent compromettre le succès de la migration.

En conclusion, une migration prématurée vers le cloud peut entraîner des problèmes de sécurité, de performances, de coûts et de perte de contrôle. Il est donc important pour une entreprise de se préparer adéquatement avant de prendre cette décision.

La migration vers le Cloud peut offrir de nombreux avantages, mais il est important de prendre en compte les difficultés et les défis potentiels pour garantir une migration réussie. Les entreprises doivent s'assurer qu'elles ont les compétences et les ressources nécessaires pour gérer leur environnement Cloud et qu'elles sont en mesure de répondre aux exigences en matière de sécurité, de conformité et de coûts.

II.9 Conclusion sur la partie II

La migration vers le cloud a émergé comme une transformation fondamentale pour de nombreuses organisations, apportant des avantages significatifs tout en introduisant de nouveaux défis. La migration vers le cloud représente une étape stratégique pour de nombreuses entreprises cherchant à rester compétitives dans un environnement numérique en constante évolution. Cependant, une planification minutieuse, une gestion efficace des risques et une collaboration étroite avec les parties prenantes sont essentielles pour garantir le succès de ce processus de transformation.

PARTIE III :

Panorama des solutions de sécurité mises en place pour le Cloud Computing

III.1 Introduction

L'introduction au panorama des solutions de sécurité pour le Cloud Computing s'inscrit dans un contexte où la migration vers des environnements cloud devient la norme pour de nombreuses entreprises, offrant agilité, flexibilité et économies d'échelle. Cependant, cette transition vers le cloud s'accompagne de défis de sécurité uniques, nécessitant une approche stratégique et robuste pour garantir la protection des données, la confidentialité des informations et la continuité des opérations. Dans cette perspective, les fournisseurs de services cloud et les entreprises adoptent des solutions de sécurité diversifiées, allant du chiffrement des données aux contrôles d'accès avancés, pour faire face à un paysage de menaces en constante évolution. Cette introduction explore l'écosystème complexe de la sécurité en cloud computing et souligne l'importance cruciale de ces solutions pour assurer une utilisation sécurisée et efficiente des services cloud.

III.2 Panorama des solutions de sécurité mises en place pour le Cloud Computing

Le Cloud Computing présente des défis uniques en matière de sécurité, car les données et les applications sont stockées et accessibles à distance. Les fournisseurs de services Cloud ont mis en place des solutions de sécurité pour protéger les données de leurs clients contre les menaces externes et internes. Voici un panorama des solutions de sécurité mises en place pour le Cloud Computing :

- Chiffrement des données : Les données stockées dans le Cloud sont souvent chiffrées pour protéger les données contre les vols et les fuites de données. Les données peuvent être chiffrées à la fois en transit et au repos.

Exemple : Un exemple courant de chiffrement des données dans le cloud est l'utilisation de services de stockage cloud tels que AWS S3 (Amazon Simple Storage Service) avec le chiffrement côté serveur. Voici comment cela fonctionne :

1. **Configuration du Chiffrement Côté Serveur :**

Lorsque vous créez un compartiment (bucket) sur Amazon S3, vous avez l'option de configurer le chiffrement côté serveur.

Vous pouvez choisir d'utiliser le chiffrement AWS Key Management Service (KMS) ou le chiffrement géré par le service S3 lui-même.

2. **Chiffrement des Objets :**

Une fois le chiffrement côté serveur activé, tous les objets (fichiers, données, etc.) que vous téléchargez dans ce compartiment sont automatiquement chiffrés.

AWS S3 gère le processus de chiffrement et de déchiffrement de manière transparente pour l'utilisateur.

3. **Gestion des Clés :**

Si vous utilisez AWS KMS, vous avez la possibilité de gérer les clés de chiffrement. AWS KMS vous permet de créer, importer et gérer vos propres clés de chiffrement maître.

4. **Contrôle d'Accès :**

Vous pouvez définir des politiques d'accès pour contrôler qui a la permission de lire ou de déchiffrer les données dans le compartiment S3.

Les politiques d'accès peuvent être configurées pour travailler de concert avec les services de sécurité d'AWS.

Avantages du Chiffrement Côté Serveur :

Le chiffrement côté serveur offre une sécurité renforcée, car il garantit que les données sont chiffrées dès qu'elles sont stockées dans le cloud.

Il simplifie également la gestion des clés, offrant une solution centralisée pour la gestion des clés de chiffrement.

- **Chiffrement en Transit :**

En complément du chiffrement côté serveur, il est également essentiel de chiffrer les données lors de leur transit entre votre système local et le cloud. Cela peut être réalisé en utilisant des protocoles sécurisés tels que HTTPS.

- **Conformité et Normes :**

Cette approche répond souvent aux exigences de conformité en matière de sécurité des données, car le chiffrement côté serveur est une mesure robuste pour protéger la confidentialité des informations.

Le chiffrement des données dans le cloud, illustré ici par le chiffrement côté serveur sur AWS S3, est une pratique clé pour garantir la confidentialité et la sécurité des données stockées dans des services cloud. Il offre une couche de protection supplémentaire, même en cas d'accès non autorisé aux données stockées.

- Contrôle d'accès : Les fournisseurs de services Cloud mettent en place des mécanismes de contrôle d'accès pour s'assurer que seuls les utilisateurs autorisés ont accès aux données et aux applications.

  Exemple :

  Le contrôle d'accès dans le cloud computing est crucial pour garantir que seules les personnes autorisées ont accès aux ressources et aux données sensibles. Un exemple de contrôle d'accès dans le cloud peut être illustré par l'utilisation d'AWS Identity and Access Management (IAM) d'Amazon Web Services.

  Voici comment cela fonctionne :

  1. **Création de Politiques IAM :**

     AWS IAM permet la création de politiques qui définissent les autorisations pour les utilisateurs, groupes ou rôles. Ces politiques spécifient quelles actions peuvent être effectuées sur quelles ressources.

  2. **Attribution de Politiques aux Utilisateurs :**

     Chaque utilisateur, groupe ou rôle dans AWS IAM peut se voir attribuer des politiques spécifiques déterminant les actions qu'ils sont autorisés à effectuer.

Par exemple, un administrateur peut avoir une politique offrant des autorisations étendues, tandis qu'un utilisateur standard peut avoir une politique limitant ses actions à des opérations spécifiques.

3. Utilisation de Groupes IAM :

Pour simplifier la gestion des autorisations, les utilisateurs peuvent être regroupés dans des groupes IAM. Les politiques attribuées à un groupe s'appliquent à tous les membres de ce groupe.

Cela facilite la gestion des autorisations pour des ensembles d'utilisateurs similaires.

4. Attribution de Rôles IAM :

Les rôles IAM sont utilisés pour accorder temporairement des autorisations à des entités, telles que des applications ou des services, plutôt qu'à des utilisateurs individuels.

Par exemple, un rôle IAM peut être créé pour permettre à un service AWS de lire des données depuis un compartiment S3 spécifique.

5. Utilisation de Conditions :

Les politiques IAM peuvent inclure des conditions pour définir des circonstances sous lesquelles les autorisations sont accordées. Par exemple, une condition peut être définie pour autoriser l'accès uniquement depuis certaines adresses IP.

6. Audit des Accès :

AWS IAM offre des outils de journalisation qui permettent de suivre qui a accédé à quelles ressources et quelles actions ont été effectuées.

Les journaux d'audit facilitent la détection d'activités suspectes et la conformité aux réglementations.

7. Intégration avec d'Autres Services :

Les solutions de contrôle d'accès IAM d'AWS peuvent être intégrées à d'autres services de sécurité, tels que AWS Key Management Service (KMS) pour la gestion des clés de chiffrement.

Le contrôle d'accès dans le cloud, illustré ici par AWS IAM, offre un moyen puissant de gérer les autorisations et de garantir la sécurité des ressources cloud. Il permet une granularité fine dans la définition des autorisations et offre des fonctionnalités avancées pour répondre aux besoins spécifiques des organisations en matière de sécurité.

- Pare-feu : Les pare-feu sont utilisés pour protéger les réseaux Cloud contre les attaques malveillantes et les menaces externes.

Exemple :

En cloud computing, les pare-feu sont des éléments essentiels pour sécuriser les infrastructures en ligne. Un exemple notable de pare-feu dans le cloud est le service AWS WAF (Web Application Firewall) d'Amazon Web Services. Voici comment cela fonctionne :

1. AWS WAF - Protection des Applications Web :

AWS WAF est un pare-feu applicatif web qui protège les applications en ligne contre les attaques web courantes, telles que les injections SQL, les attaques par injection de scripts, les attaques par déni de service distribué (DDoS), etc.

2. Configuration des Règles de Sécurité :

Les administrateurs peuvent configurer des règles de sécurité dans AWS WAF pour définir les comportements autorisés ou bloqués. Par exemple, ils peuvent créer des règles pour bloquer l'accès à des URL spécifiques ou pour détecter des schémas de requêtes malveillantes.

3. Filtrage de Contenu Malicieux :

AWS WAF permet de filtrer le trafic entrant en fonction de plusieurs critères, notamment les adresses IP, les en-têtes HTTP, les chaînes de requêtes, etc. Cela permet de bloquer le trafic malveillant avant qu'il n'atteigne l'application.

4. Protection contre les DDoS :

AWS WAF peut être associé aux services AWS Shield pour fournir une protection avancée contre les attaques par déni de service distribué (DDoS). Cela aide à maintenir la disponibilité des applications même pendant des attaques volumétriques importantes.

5. Intégration avec AWS CloudFront :

AWS WAF peut être intégré avec le service AWS CloudFront, un service de distribution de contenu (CDN). Cette intégration permet d'appliquer des règles de sécurité aux distributions CloudFront, offrant une protection sur le réseau de distribution mondial.

6. **Gestion des Accès :**

Les administrateurs peuvent définir des règles pour gérer l'accès aux ressources en fonction des adresses IP, des en-têtes HTTP, des chaînes de requêtes, etc.

Cela permet de restreindre l'accès aux ressources sensibles et de prévenir les attaques ciblées.

7. **Journalisation et Analyse :**

AWS WAF fournit des journaux détaillés qui permettent aux administrateurs de surveiller les activités, de détecter les incidents de sécurité et de répondre aux menaces de manière proactive.

8. **Mises à Jour Automatiques :**

AWS WAF est continuellement mis à jour pour inclure de nouvelles règles de sécurité et pour contrer les dernières menaces en ligne.

AWS WAF est un exemple de pare-feu dans le cloud qui offre une protection robuste pour les applications web en filtrant le trafic et en détectant et bloquant les menaces courantes. Il peut être intégré facilement avec d'autres services AWS pour créer une solution de sécurité complète dans le cloud.

- Surveillance et détection d'intrusions : Les fournisseurs de services Cloud surveillent constamment les activités sur leur plateforme pour détecter les comportements malveillants et les intrusions.

Exemple :

La surveillance et la détection d'intrusions sont des aspects essentiels de la sécurité en cloud computing. Un exemple notable est le service AWS GuardDuty d'Amazon Web Services, qui est conçu pour surveiller en continu les activités malveillantes et les comportements suspects dans le cloud. Voici comment cela fonctionne :

1. **AWS GuardDuty - Surveillance Continue :**

AWS GuardDuty analyse en continu les logs et les données de trafic dans un environnement AWS afin de détecter des activités malveillantes.

2. **Analyse des Logs CloudTrail, VPC Flow, et DNS :**

GuardDuty examine les logs de services clés tels que AWS CloudTrail (qui enregistre les activités API), les logs de flux VPC (Virtual Private Cloud) pour surveiller le trafic réseau, et les logs DNS pour détecter des activités malveillantes liées aux noms de domaine.

3. **Machine Learning pour la Détection :**

Le service utilise des techniques avancées de machine learning pour analyser les modèles de comportement et détecter les anomalies. Il peut identifier des schémas qui pourraient indiquer des attaques ou des tentatives d'intrusion.

4. **Détection de Comportements Anormaux :**

AWS GuardDuty est capable de détecter des comportements anormaux tels que des tentatives de compromission de compte, des attaques de force brute, des changements de configuration inhabituels, etc.

5. **Intégration avec AWS CloudWatch :**

GuardDuty peut envoyer des alertes à AWS CloudWatch, permettant aux administrateurs de mettre en place des réponses automatisées ou de recevoir des notifications en cas de détection d'une activité suspecte.

6. **Alertes et Notifications :**

Lorsqu'une activité malveillante est détectée, AWS GuardDuty génère des alertes détaillées, y compris des informations sur la nature de l'activité suspecte et les ressources impliquées.

7. **Corrélation d'Événements :**

Le service est capable de corréler plusieurs événements pour fournir une vue d'ensemble cohérente des activités malveillantes potentielles.

8. **Intégration avec AWS Security Hub :**

AWS GuardDuty est intégré à AWS Security Hub, fournissant une interface centralisée pour la gestion des alertes de sécurité et la prise de décisions.

9. **Gestion des Menaces Connu :**

AWS GuardDuty utilise des listes de menaces connues et des bases de données d'indicateurs de compromission (IOC) pour améliorer la détection des activités malveillantes.

AWS GuardDuty est un exemple de solution de surveillance et de détection d'intrusions en cloud computing qui utilise des techniques avancées telles que le machine learning

pour identifier les comportements malveillants et protéger les environnements cloud contre les menaces.

- Gestion des identités et des accès : Les fournisseurs de services Cloud ont des systèmes de gestion des identités et des accès pour s'assurer que seuls les utilisateurs autorisés ont accès aux données et aux applications.

Exemple :

Un exemple notable de service de gestion des identités et des accès en cloud computing est Azure Active Directory (Azure AD) de Microsoft. Voici comment cela fonctionne :

1. **Création d'Utilisateurs dans Azure AD :**

Les administrateurs peuvent créer des utilisateurs dans Azure AD, attribuer des identifiants uniques à chaque utilisateur et définir des informations d'identification telles que le mot de passe.

2. **Attribution de Rôles et de Groupes :**

Azure AD permet d'attribuer des rôles et des groupes aux utilisateurs. Les rôles définissent les autorisations spécifiques pour les actions dans Azure, et les groupes simplifient la gestion en permettant d'appliquer des autorisations à plusieurs utilisateurs.

3. **Authentification Multifacteur (MFA) :**

Azure AD prend en charge l'authentification multifacteur (MFA) pour renforcer la sécurité. Les utilisateurs doivent fournir une preuve supplémentaire d'identité, telle qu'un code généré par une application mobile.

4. **Fédération d'Identités avec Azure AD :**

Azure AD prend en charge la fédération d'identités, permettant aux utilisateurs de se connecter à divers services cloud et applications avec leurs identifiants d'entreprise existants.

5. **Application Proxy :**

Azure AD Application Proxy permet de publier en toute sécurité des applications locales pour un accès distant, offrant une gestion des identités et un contrôle d'accès centralisés.

6. **Contrôle d'Accès Conditionnel :**

Azure AD propose des politiques de contrôle d'accès conditionnel qui permettent de définir des règles basées sur des conditions telles que l'emplacement de l'utilisateur, le type d'appareil utilisé, etc.

7. **Gestion des Accès Privilégiés (PIM) :**

Azure AD Privileged Identity Management (PIM) permet de gérer, surveiller et auditer les accès à des rôles privilégiés. Les utilisateurs n'ont des droits élevés que lorsqu'ils en ont besoin, minimisant ainsi les risques.

8. **Surveillance des Identités et des Accès :**

Azure AD offre des fonctionnalités de journalisation et de surveillance pour suivre les activités liées aux identités et aux accès, permettant la détection des comportements anormaux.

9. **Intégration avec d'Autres Services Azure :**

Azure AD est étroitement intégré avec d'autres services Azure, offrant une gestion des identités et des accès qui s'étend à l'ensemble de l'écosystème Azure.

Azure Active Directory est un exemple de solution de gestion des identités et des accès en cloud computing proposée par Microsoft. Il offre une gamme étendue de fonctionnalités pour sécuriser les identités, gérer les autorisations et permettre une collaboration sécurisée dans des environnements cloud.

- Tests de pénétration : Les fournisseurs de services Cloud effectuent régulièrement des tests de pénétration pour détecter les vulnérabilités de leur système et les corriger avant qu'elles ne soient exploitées.

  Exemple :

  Les tests de pénétration, ou tests d'intrusion, sont essentiels pour évaluer la sécurité d'une infrastructure en cloud computing. Voici un exemple de scénario de test de pénétration en cloud computing :

  Scénario de Test de Pénétration :

  Objectif : Évaluer la robustesse de la sécurité d'une application web hébergée sur une plateforme cloud (par exemple, AWS, Azure, Google Cloud).

  1. Reconnaissance :

  Identifier les informations sur l'application web, telles que les adresses IP, les noms de domaine, les services utilisés, etc.

Utiliser des techniques telles que la collecte d'informations publiques, le scanning de ports, etc.

2. Analyse de Vulnérabilités :

Utiliser des outils automatisés pour scanner l'application à la recherche de vulnérabilités connues, telles que des failles de sécurité dans les bibliothèques, des injections SQL, des vulnérabilités XSS, etc.

3. Tests d'Authentification :

Tenter de contourner l'authentification de l'application en utilisant des attaques de force brute, des attaques par injection, ou en exploitant des faiblesses dans le mécanisme d'authentification.

4. Tests d'Autorisation :

Vérifier si les mécanismes d'autorisation sont correctement configurés en essayant d'accéder à des ressources pour lesquelles l'utilisateur n'est pas autorisé.

5. Injection de Code :

Tester la résistance de l'application aux attaques d'injection de code, telles que les injections SQL, en essayant d'injecter du code malveillant pour manipuler la base de données.

6. Attaques XSS (Cross-Site Scripting) :

Tester la sécurité contre les attaques XSS en injectant du code JavaScript malveillant dans les champs de formulaire et en vérifiant si le code est exécuté côté client.

7. Attaques CSRF (Cross-Site Request Forgery) :

Vérifier si l'application est vulnérable aux attaques CSRF en essayant d'envoyer des requêtes non autorisées depuis un site tiers.

8. Tests de Sécurité des API :

Vérifier la sécurité des API utilisées par l'application en examinant les autorisations, en effectuant des tests d'intrusion sur les points d'extrémité, et en s'assurant que les données sensibles sont correctement protégées.

9. Analyse de la Sécurité du Réseau :

Tester la configuration du réseau cloud pour détecter d'éventuelles vulnérabilités, telles que des règles de pare-feu inappropriées, des erreurs de configuration de réseau virtuel, etc.

10. Rapport et Recommandations :

Compiler les résultats du test de pénétration dans un rapport détaillé, y compris les vulnérabilités découvertes, les risques associés et des recommandations pour les atténuer.

11. Collaboration avec le Client :

Travailler en étroite collaboration avec le client pour discuter des résultats, partager des recommandations et aider à mettre en œuvre des correctifs de sécurité.

Cet exemple de scénario de test de pénétration en cloud computing met en lumière la nécessité de tester la sécurité à différents niveaux, de l'infrastructure réseau à l'application elle-même, pour identifier et remédier aux vulnérabilités potentielles.

- Plans de reprise après sinistre : Les fournisseurs de services Cloud ont des plans de reprise après sinistre pour garantir la continuité des activités en cas de catastrophe.

Exemple :

Les plans de reprise après sinistre (PRAS) en cloud computing visent à assurer la continuité des opérations et la récupération rapide des services en cas d'incident majeur. Voici un exemple de plan de reprise après sinistre en cloud computing :

Plan de Reprise Après Sinistre en Cloud Computing :

Objectif : Garantir la disponibilité continue des services critiques et la récupération rapide en cas de sinistre affectant l'infrastructure cloud.

1. Évaluation des Risques :

Identifier les risques potentiels et évaluer leur impact sur l'infrastructure cloud.

Classer les services en fonction de leur importance stratégique et de leur impact sur les opérations.

2. Définition des Objectifs de Reprise (RTO et RPO) :

Établir les objectifs de temps de reprise (Recovery Time Objective - RTO) et de point de reprise (Recovery Point Objective - RPO) pour chaque service critique.

Le RTO définit la durée maximale acceptable de temps d'inactivité, tandis que le RPO détermine la perte maximale de données tolérée.

3. Sauvegarde Régulière des Données :

Mettre en place des procédures de sauvegarde régulières pour garantir la disponibilité des données et minimiser la perte de données en cas de sinistre.

4. Stratégies de Redondance :

Utiliser des stratégies de redondance pour les services critiques, telles que la réplication des données sur des zones géographiques distinctes ou l'utilisation de services de basculement automatique.

5. Infrastructure en Mode Multi-Région :

Si possible, déployer des composants clés de l'infrastructure cloud dans plusieurs régions pour garantir une disponibilité continue en cas d'indisponibilité dans une région spécifique.

6. Documentation Détaillée :

Élaborer une documentation détaillée du plan de reprise après sinistre, y compris les responsabilités spécifiques, les procédures de récupération, les contacts d'urgence, etc.

7. Tests Réguliers du Plan de Reprise :

Conduire régulièrement des exercices de simulation pour tester l'efficacité du plan de reprise après sinistre.

Identifier les lacunes potentielles et apporter des ajustements au plan en conséquence.

8. Notification d'Incident et Activation du Plan :

Mettre en place des procédures claires de notification d'incident pour alerter rapidement les équipes en cas de sinistre.

Activer le plan de reprise après sinistre dès qu'un incident est confirmé.

9. Coordination et Communication :

Établir des canaux de communication clairs pour coordonner les efforts de récupération entre les équipes internes et, le cas échéant, avec les fournisseurs de services cloud.

10. Évaluation Post-Sinistre :

Après la récupération, mener une évaluation post-sinistre pour analyser la performance du plan, identifier les opportunités d'amélioration et ajuster le plan en conséquence.

11. Formation du Personnel :

Assurer une formation régulière du personnel pour s'assurer qu'ils comprennent les procédures de récupération après sinistre et soient prêts à agir efficacement en cas d'incident.

Ce plan de reprise après sinistre en cloud computing met l'accent sur la préparation proactive, la documentation claire, les tests réguliers et l'amélioration continue pour assurer une réponse efficace en cas d'incident.

- Conformité réglementaire : Les fournisseurs de services Cloud sont tenus de se conformer à des normes de sécurité et de confidentialité strictes pour protéger les données de leurs clients.

Exemple :

La conformité réglementaire en cloud computing est cruciale pour s'assurer que les services cloud respectent les lois et régulations spécifiques à chaque secteur. Un exemple concret concerne la conformité avec le Règlement général sur la protection des données (RGPD) de l'Union européenne. Voici comment un fournisseur de services cloud pourrait assurer la conformité avec le RGPD :

Conformité avec le RGPD en Cloud Computing :

1. **Collecte et Traitement des Données :**

Le fournisseur de services cloud doit s'assurer que la collecte et le traitement des données personnelles sont conformes aux principes du RGPD, tels que la légitimité, la limitation de la finalité et la minimisation des données.

2. **Sécurité des Données :**

Mettre en place des mesures de sécurité robustes pour protéger les données personnelles contre tout accès non autorisé, la perte ou la destruction. Cela peut inclure le chiffrement des données, la gestion des accès et des identités, ainsi que des audits de sécurité réguliers.

3. **Transparence et Consentement :**

Informer clairement les utilisateurs finaux sur la manière dont leurs données seront utilisées, stockées et traitées. Obtenez leur consentement explicite là où c'est nécessaire.

4. **Droit à l'Oubli et Portabilité des Données :**

Permettre aux utilisateurs de supprimer leurs données personnelles lorsque cela est demandé (droit à l'oubli) et de transférer leurs données vers un autre service (portabilité des données).

5. **Responsabilité Partagée :**

Clarifier les rôles et responsabilités entre le fournisseur de services cloud et le client en ce qui concerne la conformité au RGPD. Par exemple, le client peut être responsable de la conformité de ses propres applications, tandis que le fournisseur de services cloud peut être responsable de la sécurité de l'infrastructure sous-jacente.

6. **Accès aux Données par les Autorités de Contrôle :**

Faciliter l'accès aux données pour les autorités de contrôle compétentes conformément aux exigences du RGPD.

7. **Notification des Violations de Données :**

Mettre en place des procédures pour détecter et notifier les violations de données dans les délais prescrits par le RGPD.

8. **Documentation et Tenue de Registres :**

Maintenir une documentation détaillée sur les processus de traitement des données, les évaluations d'impact sur la protection des données, et d'autres aspects pertinents pour démontrer la conformité.

9. Formation du Personnel :

Assurer que le personnel du fournisseur de services cloud est formé sur les principes et les exigences du RGPD, notamment en ce qui concerne le traitement des données personnelles.

10. Évaluation d'Impact sur la Protection des Données (EIPD) :

Effectuer des évaluations d'impact sur la protection des données lorsque cela est nécessaire, en particulier lors de la mise en œuvre de nouveaux traitements de données susceptibles d'entraîner un risque élevé pour les droits et libertés des personnes concernées.

En respectant ces mesures, un fournisseur de services cloud peut démontrer son engagement envers la conformité au RGPD, ce qui est crucial pour les clients traitant des données personnelles dans l'environnement cloud.

En conclusion, les fournisseurs de services Cloud ont mis en place des solutions de sécurité sophistiquées pour protéger les données de leurs clients contre les menaces externes et internes. Les entreprises doivent s'assurer que leur fournisseur de services Cloud dispose de mesures de sécurité adéquates avant de migrer leurs données et leurs applications vers le Cloud.

III.3 Comment sécuriser le cloud compuing

La sécurité dans le Cloud Computing est une préoccupation importante pour les entreprises qui stockent leurs données et applications dans le Cloud. Voici quelques mesures que les entreprises peuvent prendre pour sécuriser leurs données et applications dans le Cloud :

Chiffrement des données : Les données stockées dans le Cloud doivent être chiffrées pour protéger les données contre les vols et les fuites de données. Les données doivent être chiffrées à la fois en transit et au repos.

- Contrôle d'accès : Les entreprises doivent mettre en place des mécanismes de contrôle d'accès pour s'assurer que seuls les utilisateurs autorisés ont accès aux données et aux applications.
- Gestion des identités et des accès : Les entreprises doivent avoir des systèmes de gestion des identités et des accès pour s'assurer que seuls les utilisateurs autorisés ont accès aux données et aux applications.
- Surveillance et détection d'intrusions : Les entreprises doivent surveiller constamment les activités sur leur plateforme Cloud pour détecter les comportements malveillants et les intrusions.
- Formation des utilisateurs : Les entreprises doivent former leurs utilisateurs sur les bonnes pratiques de sécurité et les sensibiliser aux risques de sécurité associés à l'utilisation du Cloud.

- Tests de pénétration : Les entreprises doivent effectuer régulièrement des tests de pénétration pour détecter les vulnérabilités de leur système et les corriger avant qu'elles ne soient exploitées.
- Plans de reprise après sinistre : Les entreprises doivent avoir des plans de reprise après sinistre pour garantir la continuité des activités en cas de catastrophe.
- Choix du fournisseur Cloud : Les entreprises doivent choisir un fournisseur de services Cloud qui dispose de mesures de sécurité adéquates et qui est conforme aux normes de sécurité et de confidentialité.

En conclusion, la sécurité dans le Cloud Computing est une responsabilité partagée entre le fournisseur de services Cloud et l'entreprise. Les entreprises doivent mettre en place des mesures de sécurité pour protéger leurs données et applications dans le Cloud, et choisir un fournisseur de services Cloud qui dispose de mesures de sécurité adéquates.

III.4 Comment choisir un fournisseur cloud ?

Le choix d'un fournisseur de services cloud est une décision importante pour toute entreprise. Voici quelques éléments clés à prendre en compte pour choisir le fournisseur cloud qui convient le mieux aux besoins d'une entreprise :

- Compatibilité : l'entreprise doit s'assurer que le fournisseur de services cloud qu'elle envisage de choisir est compatible avec les technologies et les applications existantes. Il est important de choisir un fournisseur de services cloud qui peut s'intégrer facilement à l'infrastructure informatique existante.

- Niveau de service : l’entreprise doit vérifier le niveau de service offert par le fournisseur de services cloud. L’entreprise doit Assurer que le fournisseur offre des niveaux de service élevés et des garanties de disponibilité qui répondent à ses besoins.
- Coûts : l’entreprise doit évaluer les coûts des différents fournisseurs de services cloud. Il est important de comprendre les différents coûts associés à l'utilisation des services cloud, tels que les coûts de stockage, les frais d'utilisation, etc.
- Sécurité : l’entreprise doit s’assurer que le fournisseur de services cloud qu’elle envisage de choisir offre des mesures de sécurité de haut niveau pour protéger les données. Elle doit vérifier que le fournisseur utilise des pratiques de sécurité éprouvées, telles que le cryptage de données, la gestion des accès, la surveillance des menaces et la conformité aux normes de sécurité.
- Évolutivité : l’entreprise doit Vérifier que le fournisseur de services cloud peut s'adapter aux besoins d'évolutivité à mesure que l’entreprise se développe. Il est important de choisir un fournisseur de services cloud qui peut offrir des capacités d'évolutivité et de flexibilité pour répondre aux besoins de l’entreprise en constante évolution.

Le choix d'un fournisseur de services cloud est une décision importante qui doit être prise après une évaluation minutieuse des différents fournisseurs. Il est important de prendre en compte les facteurs clés tels que la compatibilité, le niveau de service, les coûts, la sécurité et l'évolutivité pour prendre la bonne décision.

III.5 Statistiques sur les fournisseurs cloud les plus réputés au monde

Les principaux fournisseurs de services cloud :

Amazon Web Services (AWS) :

AWS est l'un des fournisseurs de cloud les plus importants et a longtemps dominé le marché.

En 2021, AWS détenait une part de marché d'environ 32%, selon diverses estimations.

Microsoft Azure :

Azure de Microsoft est un concurrent majeur d'AWS.

En 2021, Azure détenait une part de marché d'environ 20%, faisant de lui le deuxième plus grand fournisseur de services cloud.

Google Cloud Platform (GCP) :

GCP est en troisième position, mais il a gagné en popularité au fil des ans.

En 2021, la part de marché de GCP était d'environ 9%.

Alibaba Cloud :

Alibaba Cloud est le principal fournisseur de services cloud en Chine et connaît une expansion internationale.

En 2021, Alibaba Cloud détenait une part de marché d'environ 6%.

Autres Fournisseurs :

Il existe de nombreux autres fournisseurs de services cloud, tels qu'IBM Cloud, Oracle Cloud, et d'autres acteurs régionaux.

La part de marché des autres fournisseurs combinés était d'environ 33% en 2021.

Tendances Clés :

Le marché du cloud computing continue de croître rapidement, alimenté par la demande croissante de services cloud dans divers secteurs.

Les fournisseurs de cloud élargissent constamment leur gamme de services, y compris l'intelligence artificielle, l'Internet des objets, l'analyse de données, etc.

La concurrence entre les principaux fournisseurs reste intense, avec des avantages concurrentiels se déplaçant d'un domaine de service à un autre.

Il est important de noter que ces chiffres sont basés sur des estimations et peuvent varier en fonction des sources. La part de marché peut également évoluer au fil du temps en fonction des stratégies des fournisseurs et des évolutions du marché. Pour les données les plus récentes, je vous recommande de consulter des rapports et analyses actualisés du marché du cloud computing.

III.6 Applications courantes du cloud computing

Le cloud computing offre une multitude d'applications pour les entreprises et les particuliers. Voici quelques exemples d'applications courantes du cloud computing :

Stockage de données : Les services cloud de stockage de données tels que Dropbox, Google Drive et Microsoft OneDrive permettent aux utilisateurs de stocker et de partager des fichiers en ligne.

Applications web : Les applications web sont des applications qui sont hébergées sur le cloud et qui peuvent être accédées depuis n'importe quel navigateur web. Des exemples d'applications web populaires sont les services de messagerie électronique tels que Gmail, les applications de productivité telles que Google Docs, et les plateformes de réseaux sociaux tels que Facebook et Twitter.

Le cloud computing offre une variété d'applications pour les entreprises et les particuliers, allant du stockage de données à l'infrastructure, en passant par les applications web, les plateformes et les logiciels en tant que service. Les avantages du cloud computing, tels que la flexibilité, la scalabilité et l'accessibilité, ont permis à de nombreuses entreprises de développer de nouveaux produits et services et de gérer leurs opérations plus efficacement.

III.7 Les fournisseurs du cloud computing les plus connus

Il existe de nombreux fournisseurs cloud connus, mais voici une liste des principaux fournisseurs cloud du marché :

- Amazon Web Services (AWS) : AWS est le fournisseur de services cloud le plus populaire et le plus utilisé dans le monde. Il offre une large gamme de services cloud tels que le stockage, le calcul, l'intelligence artificielle, l'apprentissage machine, la sécurité, la gestion de bases de données et bien plus encore.
- Microsoft Azure : Azure est la plateforme cloud de Microsoft qui offre une gamme complète de services cloud tels que l'hébergement de sites Web, le stockage de données, les services de calcul, l'analyse, l'Internet des objets (IoT), la sécurité et plus encore.

- Google Cloud Platform (GCP) : GCP est la plateforme cloud de Google qui offre une gamme complète de services cloud tels que le stockage, le calcul, les bases de données, l'analyse, l'apprentissage machine, l'intelligence artificielle et plus encore.
- IBM Cloud : IBM Cloud est une plateforme cloud de bout en bout qui offre une gamme complète de services cloud tels que l'hébergement de sites Web, le stockage de données, les services de calcul, l'analyse, l'Internet des objets (IoT), la sécurité et plus encore.
- Oracle Cloud : Oracle Cloud est une plateforme cloud qui offre une gamme complète de services cloud tels que le stockage, le calcul, les bases de données, l'analyse, l'apprentissage machine, l'intelligence artificielle, la sécurité et plus encore.

Il existe également d'autres fournisseurs de cloud notables tels que Alibaba Cloud, DigitalOcean, VMware, Red Hat OpenShift et bien plus encore.

III.8 Quels sont les clouds publics les plus utilisés au sein du secteur des technologies ?

Dans le secteur des technologies, plusieurs clouds publics sont largement utilisés en raison de leur robustesse, de leurs fonctionnalités étendues et de leur réputation. Les trois principaux clouds publics les plus utilisés dans ce secteur sont : Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

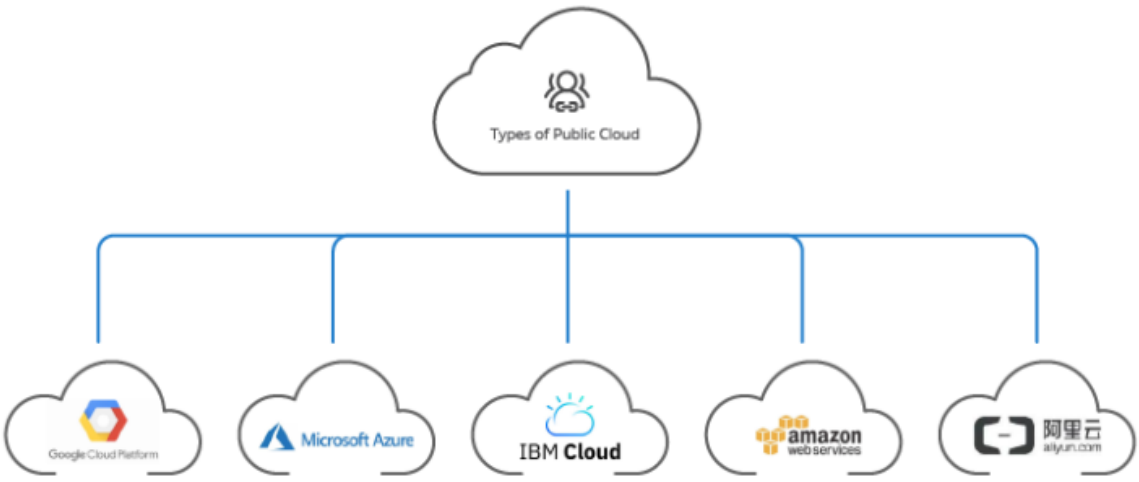

Figure 16 : Les clouds publics les plus utilisés au sein du secteur des technologies

III.9 Quels sont les clouds privés les plus utilisés au sein du secteur des technologies ?

La Figure suivante illustre quelques fournisseurs de clouds privés les plus utilisés dans le secteur des technologies.

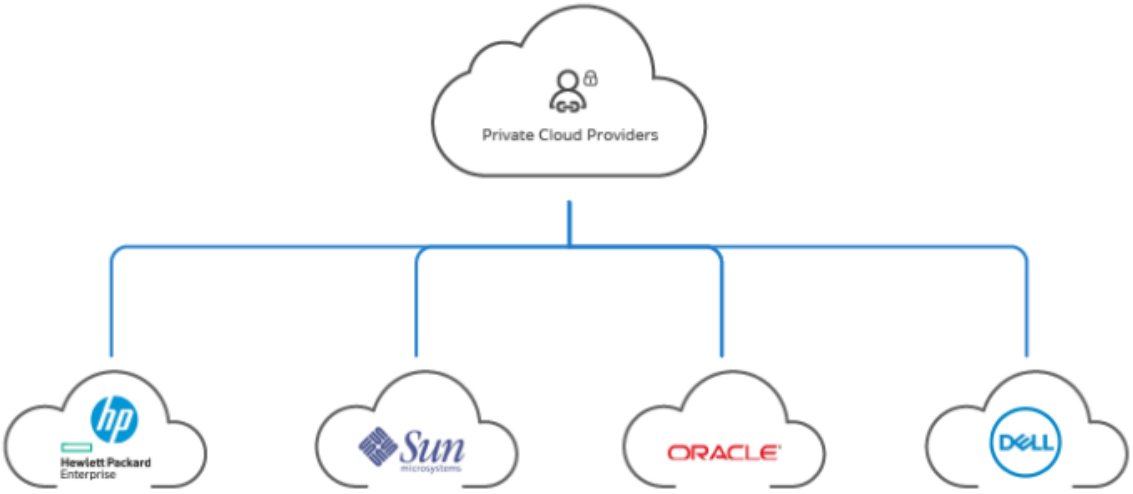

Figure 17 : Les clouds publics les plus utilisés au sein du secteur des technologies

III.10 Conclusion sur la 3 ime partie

En conclusion, le panorama des solutions de sécurité déployées pour le cloud computing reflète une approche proactive et diversifiée visant à garantir la protection des données, la confidentialité des informations et la disponibilité des services. Les fournisseurs de services cloud, ainsi que les entreprises utilisant ces services, ont mis en œuvre une gamme variée de technologies et de pratiques de sécurité pour faire face aux défis spécifiques liés à l'environnement cloud. Parmi les solutions clés, on trouve le chiffrement des données, les contrôles d'accès avancés, la surveillance continue, les tests de pénétration, la gestion des identités et des accès, ainsi que la conformité réglementaire.

L'évolution constante des menaces et des vulnérabilités exige une vigilance continue et une adaptation des stratégies de sécurité. Les solutions émergentes intègrent de plus en plus l'intelligence artificielle et l'apprentissage automatique pour détecter et répondre aux menaces de manière proactive. La gestion des identités et des accès joue un rôle crucial dans la sécurisation des environnements cloud, offrant une granularité fine dans le contrôle des autorisations.

L'importance de la conformité réglementaire, notamment dans le contexte du règlement général sur la protection des données (RGPD) et d'autres normes sectorielles, a conduit à des efforts significatifs pour garantir que les services cloud respectent les exigences légales.

En fin de compte, le panorama de la sécurité en cloud computing évolue rapidement pour répondre aux exigences croissantes de confidentialité, d'intégrité et de disponibilité des données. Les organisations doivent adopter une approche holistique de la sécurité, intégrant des solutions technologiques, des politiques de conformité et une culture de la sécurité au sein de leurs équipes pour tirer pleinement parti des avantages du cloud tout en atténuant les risques potentiels.

III.11 Conclusion générale

Le Cloud Computing est une technologie qui a révolutionné la manière dont les entreprises utilisent les ressources informatiques. Il permet aux entreprises de disposer de ressources informatiques flexibles et évolutives sans avoir à investir dans l'infrastructure matérielle et logicielle. Cette technologie a changé la façon dont les entreprises conçoivent, déploient et gèrent leur infrastructure informatique.

Ce polycopié a été préparé dans le but d'atteindre plusieurs objectifs essentiels, permettant ainsi de fournir une compréhension approfondie et pratique de ce domaine en pleine expansion. Ce support peut être utile pour :

- Éducation et Sensibilisation : Le polycopié a pour mission d'éduquer les étudiants, les professionnels de l'informatique et toute personne intéressée aux concepts fondamentaux, aux technologies et aux enjeux du cloud computing. Il offre une opportunité d'apprentissage structuré et approfondi.
- Compréhension des Concepts : Le polycopié vise à expliquer de manière claire et approfondie les principes sous-jacents du cloud computing, tels que la virtualisation, les modèles de service (IaaS, PaaS, SaaS), les modèles de déploiement (cloud public, privé, hybride) et les avantages inhérents.
- Formation Pratique : En fournissant des exemples concrets, des études de cas et des exercices pratiques, le polycopié permet aux apprenants de mettre en œuvre leurs

connaissances théoriques dans des scénarios réels, ce qui favorise une compréhension pratique et applicable.

- Développement de Compétences Techniques : Le contenu du polycopié vise à développer les compétences nécessaires pour déployer, gérer et optimiser des solutions cloud. Il couvre les compétences techniques telles que la gestion des ressources, la sécurité, l'évolutivité et la gestion des données.
- Adaptation aux Tendances du Marché : Le polycopié permet aux apprenants de rester au fait des dernières évolutions technologiques et des tendances du marché dans le domaine du cloud computing, ce qui est essentiel pour rester compétitif dans le secteur de l'informatique.
- Préparation à la Certification : De nombreux polycopiés de cours sur le cloud computing sont conçus pour préparer les individus à passer des certifications professionnelles dans ce domaine, ce qui peut renforcer leurs perspectives de carrière et leur crédibilité.
- Encouragement de l'Innovation : En comprenant les opportunités et les défis du cloud computing, les apprenants sont mieux préparés à explorer de nouvelles idées et à innover dans le développement de solutions cloud pour des besoins spécifiques.
- Sensibilisation aux Enjeux : Le polycopié peut également aborder les aspects éthiques, légaux et de sécurité liés au cloud computing, sensibilisant ainsi les apprenants aux préoccupations et aux responsabilités liées à l'utilisation et à la gestion des ressources cloud.

En conclusion, la création d'un polycopié de cours sur le cloud computing vise à offrir une base solide de connaissances théoriques et pratiques, à préparer les individus aux défis du monde moderne de l'informatique et à les positionner en tant que professionnels compétents et informés dans le domaine du cloud computing.

Références

- Li, X., Xia, Q., Zhang, L., Wang, R., & Liu, Y. (2021). A survey of machine learning in cloud computing. Journal of Parallel and Distributed Computing, 148, 1-18.
- Michael Armbrust, Armando Fox, Rean Gri_th, Anthony D Joseph, RandyKatz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM,53(4):50-58, 2010.
- Rodrigues, B., & de Oliveira, R. A. R. (2020). A survey on resource allocation techniques in cloud computing. Journal of Parallel and Distributed Computing, 144, 111-137.
- Subashini Subashini and Veeraruna Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1):1-11, 2011.

- Wang, D., Duan, Y., & Wu, H. (2021). Cloud computing-based artificial intelligence: A survey. Journal of Parallel and Distributed Computing, 149, 107-117.
- Wang, X., Ren, H., & Sun, Y. (2022). Energy-efficient cloud computing systems: A survey. Journal of Parallel and Distributed Computing, 160, 140-151.
- Zhang, Q., Cheng, L., & Boutaba, R. (2018). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 9(1), 1-42.
- Zhou, M., Cao, J., & Yang, Y. (2021). Edge computing in the era of 5G and beyond: a survey. Journal of Parallel and Distributed Computing, 152, 249-267.
- Zhang, L., Liu, S., Liu, Z., & Sun, G. (2022). A survey on cloud-based big data processing platforms. Journal of Parallel and Distributed Computing, 161, 34-45. http://www.nebula-project.eu/fr/.