Cloud Computing et Virtualisation

Pr. Abdelhadi ZINEDDINE
DUT IDIA, EST, USMS-Béni-Mellal
abdelhadii.zineddine@gmail.com

PLAN

Parties:

- ✓Introduction au Cloud Computing et à la Virtualisation
- ✓Principes de fonctionnement des environnements cloud et des machines virtuelles
- ✓Technologies et plateformes du cloud
- ✓Déploiement et gestion des infrastructures virtuelles
- ✓Pratiques de sécurité pour l'environnement cloud computing
- ✓Méthodes d'optimisation des performances et de la disponibilité dans le cloud

Partie 2: Introduction à la Virtualisation Principe et fonctionnement

Chapitre 1: Introduction à la virtualisation

- Définition & Principe
- Avantages & intérêts
- Formes de la virtualisation

Introduction à la Virtualisation

Définition

“La virtualisation consiste, en informatique, à exécuter sur une machine hôte, dans un environnement isolé, des systèmes d'exploitation — on parle alors de virtualisation système — ou des applications — on parle alors de virtualisation applicative. Ces ordinateurs virtuels sont appelés serveur privé virtuel (Virtual Private Server ou VPS) ou encore environnement virtuel (Virtual Environment ou VE).”

-Wikipedia

Définition

La virtualisation est une technologie qui permet de faire fonctionner plusieurs machines virtuelles sur un seul matériel physique.

Chaque machine virtuel peut avoir son propre système (comme Windows, Linux, etc.) et ses programmes, comme s'il s'agissait d'un vrai ordinateur.

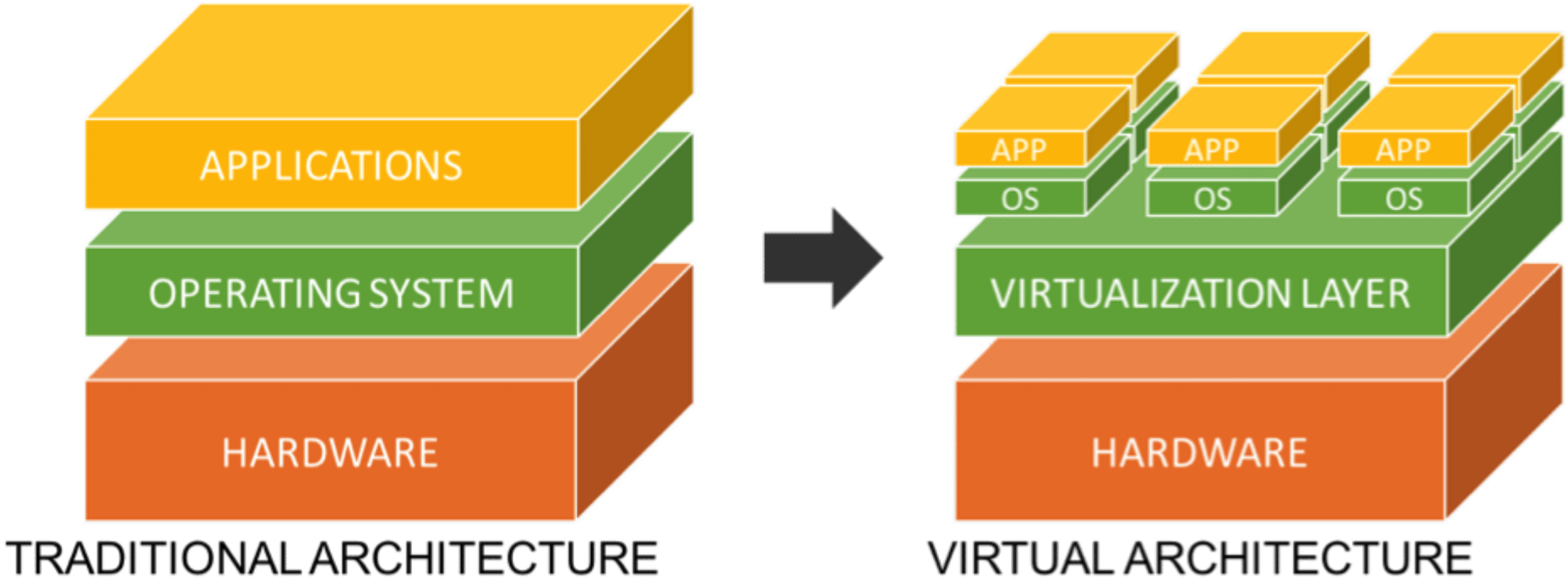
Définition

Exemple :

Sur un seul ordinateur, on peut créer :

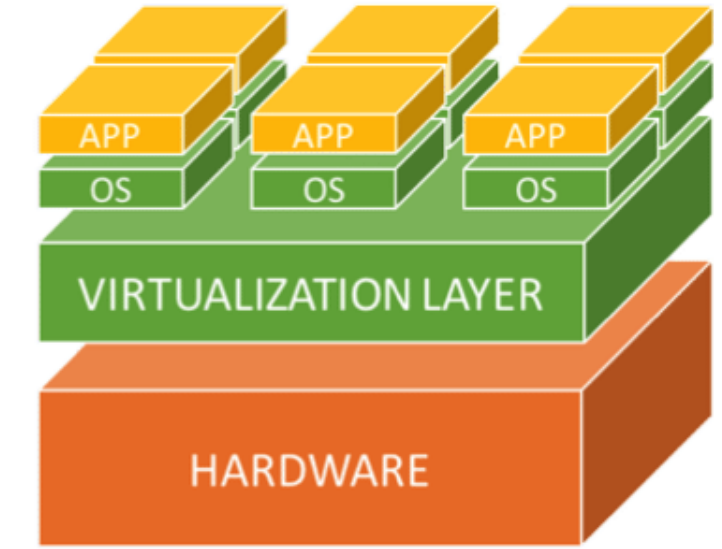
- une machine virtuelle avec Windows,
- une autre avec Linux,
- et une autre avec macOS,
- toutes en même temps, grâce à un logiciel spécial appelé **hyperviseur** (comme VMware ou VirtualBox).

Principe de la virtualisation



la couche de virtualisation (hyperviseur) est le logiciel qui permet de créer et gérer les machines virtuelles. Ex: VMware ou VirtualBox.

Hardware (Matériel): le processeur, la mémoire, le disque dur, la carte réseau, etc**.**



VIRTUAL ARCHITECTURE

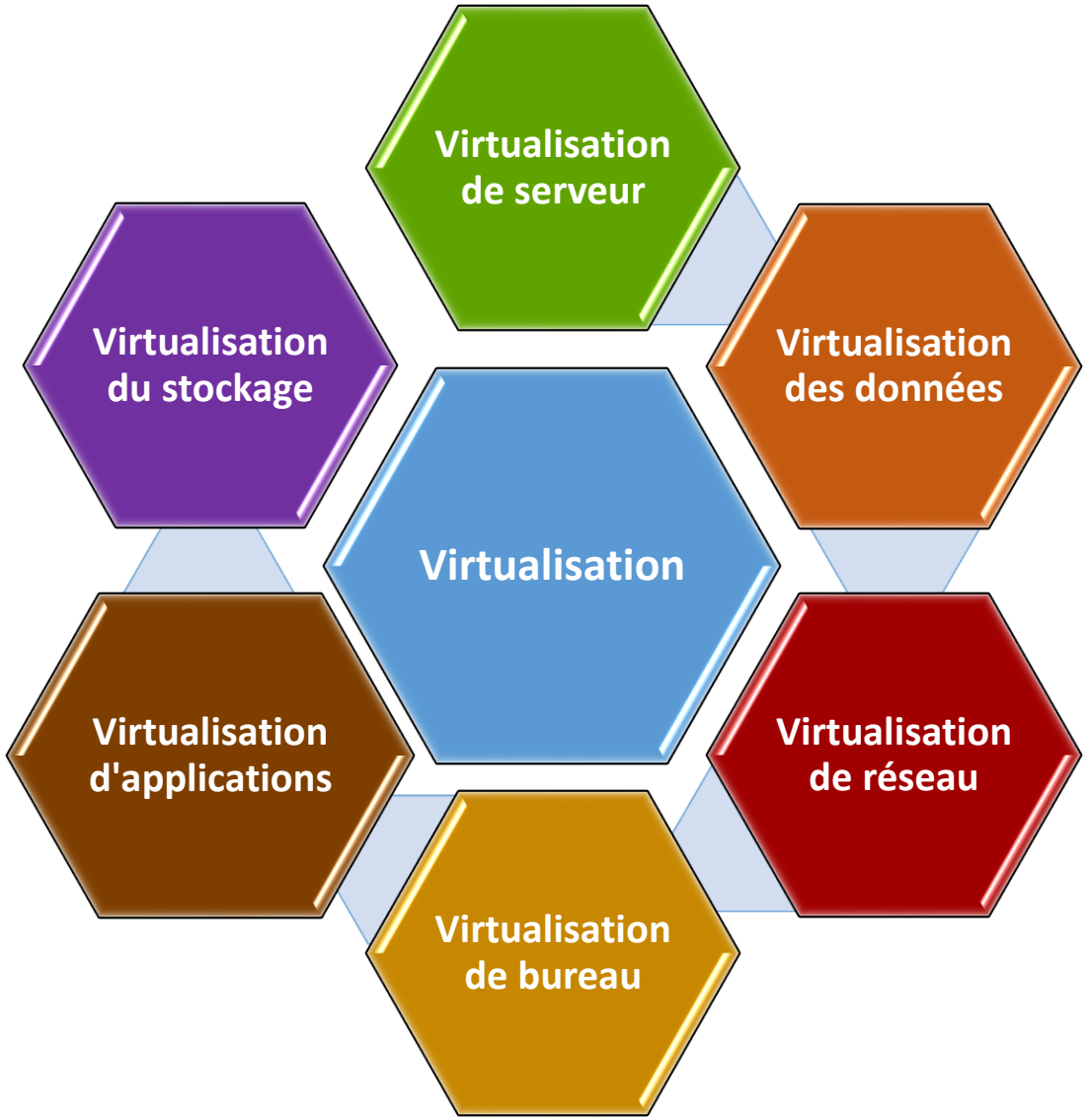
OS ou le système d'exploitation: chaque machine virtuelle possède son propre système d'exploitation (Windows, Linux, etc.).

Cet exemple est la forme de virtualisation la plus connue : **la virtualisation de serveur.**

Les intérêts de la virtualisation

- ✓Moins de serveurs physiques,
- ✓Réduction des coûts,
- ✓Une gestion et une exploitation efficace des ressources,
- ✓Une disponibilité des services optimale,
- ✓Une sécurité renforcée avec les environnements isolés,
- ✓Un gain potentiel sur les coûts de licences.

Les formes de virtualisation



Les formes de virtualisation

- Virtualisation de serveurs : consiste à créer plusieurs machines virtuelles (VM) sur un seul serveur physique. Ex : VirtualBox, VMware, Hyper-V, KVM (Kernel-based Virtual Machine).
- Virtualisation de bureau (postes de travail) : consiste à héberger les ordinateurs des utilisateurs sur un serveur central au lieu de les exécuter directement sur leurs machines locales. Ils se connectent à distance à leur poste de travail virtuel à partir d'un simple ordinateur. Ex: VMware Horizon, Citrix XenDesktop.

Les formes de virtualisation

- Virtualisation des applications: consiste à exécuter une application sans qu'elle soit installée directement sur le système d'exploitation de l'ordinateur de l'utilisateur.
- L'application est isolée du système d'exploitation et fonctionne dans un environnement virtuel qui contient tout ce dont elle a besoin (fichiers, bibliothèques, paramètres…).

- Ex : Microsoft App-V, Citrix XenApp.

Les formes de virtualisation

Virtualisation des applications:

- Exemple concret dans une entreprise :

- Au lieu d’installer Microsoft Office sur 100 ordinateurs, on le virtualise sur un serveur.
- Les employés ouvrent Word ou Excel via une session virtuelle.
- Les mises à jour ou nouvelles versions sont déployées une seule fois sur le serveur.

Les formes de virtualisation

- Virtualisation des réseaux : Cette forme permet de créer des réseaux virtuels indépendants des infrastructures physiques sous-jacentes. Ex : SDN (Software Defined Networking), NFV (Network Functions Virtualization).

Les formes de virtualisation

- Virtualisation des données : Cela permet de centraliser l'accès aux données provenant de plusieurs bases de données ou systèmes de stockage. Cela rend l’accès plus facile ainsi que la manipulation des données. Ex : VMware vSphere, Delphix.
- Virtualisation du stockage : Elle permet de regrouper plusieurs dispositifs de stockage physiques en une seule unité logique qui peut être gérée de manière centralisée. Ex : SAN (Storage Area Networks), NAS (Network-Attached Storage).

Les 3 variantes d’architecture de virtualisation

Les trois principales variantes d'architecture de virtualisation sont :

- la virtualisation complète,
- la paravirtualisation
- et la virtualisation basée sur les conteneurs.

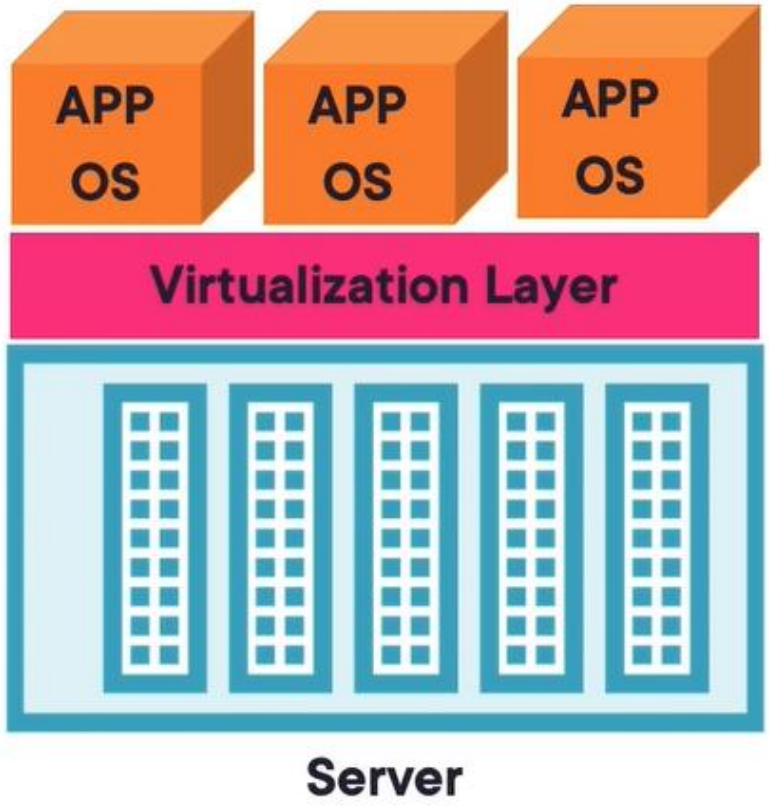
Partie 2: Introduction à la Virtualisation
Principe et fonctionnement

Chapitre 2: Virtualisation des serveurs

- Architecture et fonctionnement (composants)
- Hyperviseur
- Types d'hyperviseur
- VMs et ressources virtuelles
- Avantages et intérêts
- Lab 1: Créer et gérer des VMs sur **VirtualBox**

Virtualisation des serveurs

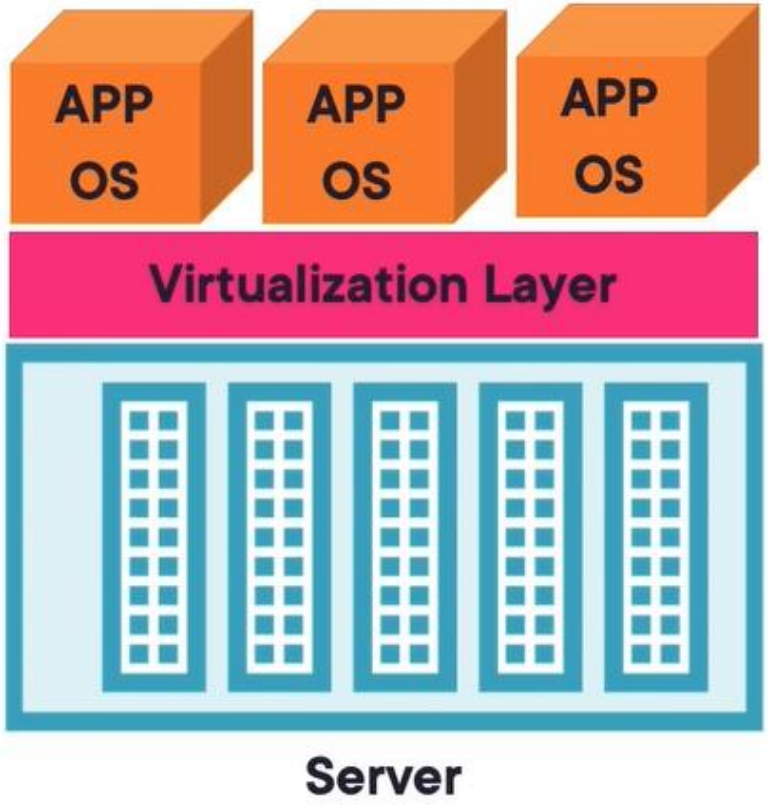
La virtualisation des serveurs consiste à créer plusieurs machines virtuelles (VM) sur un seul serveur physique.



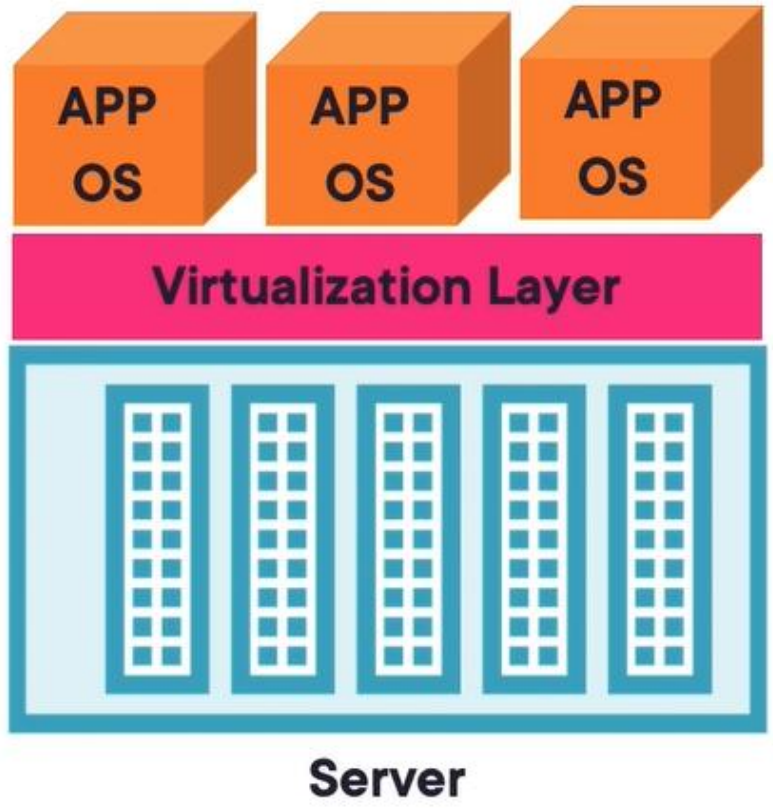
Architecture - Virtualisation des serveurs

Les composants de l'architecture Virtualisation des serveurs :

- Serveur physique,
- Hyperviseur,
- Vms.

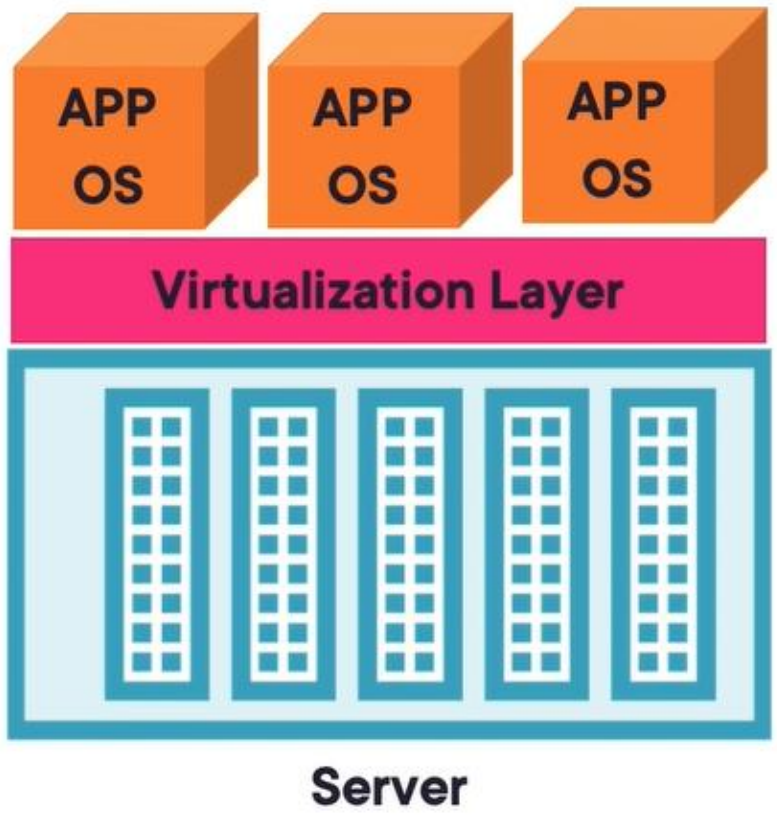


Architecture - Virtualisation des serveurs



Serveur est le matériel physique sur lequel la virtualisation est déployée.
Il fournit les ressources physiques (processeur, mémoire, stockage, etc.) utilisées par les Vms.

Hyperviseur



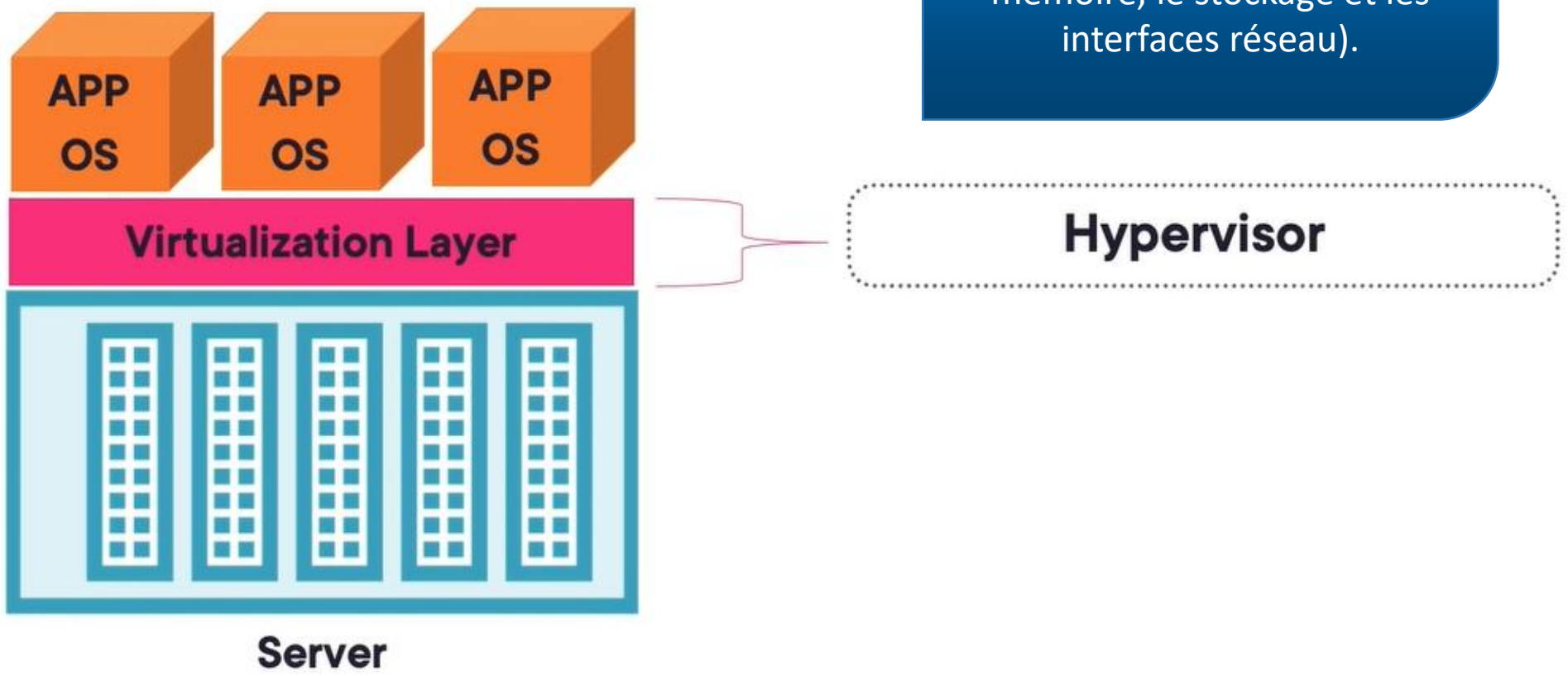
l'hyperviseur est réellement la couche de virtualisation.

Hypervisor

l'hyperviseur est un logiciel qui permet de créer, exécuter et gérer les machines virtuelles (VM).

Hyperviseur

Il permet la création de ressources informatiques virtuelles (le processeur, la mémoire, le stockage et les interfaces réseau).



Types d’Hyperviseurs

Hyperviseur de type 1 (bare-metal)

S'exécute directement sur le matériel de l'hôte, offre les meilleures performances et sécurité et utilisé principalement dans les centres de données (DC), serveurs de virtualisation d’entreprise...

Exemples : VMware ESXi, Microsoft Hyper-V (version serveur), XenServer, KVM.

Hyperviseur de type 2 (hosted)

s'exécute au-dessus d'un système d'exploitation hôte (ex: Linux, Windows ou macOS). Il offre une flexibilité pour les environnements de test, d'apprentissage et de développement.

Exemples : Oracle VirtualBox, VMware Workstation, Parallels Desktop.

Types d’Hyperviseurs

Hyperviseur de type 1 (bare-metal)

VMware vSphere/ESXi : Une solution de virtualisation très populaire, utilisée principalement dans les environnements d'entreprise.

Microsoft Hyper-V : Solution de virtualisation de serveur de Microsoft, intégrée dans les éditions serveur de Windows.

Xen (open-source): Un hyperviseur open-source qui fonctionne également en mode bare-metal.

KVM (Kernel-based Virtual Machine) : Un hyperviseur intégré dans le noyau Linux.

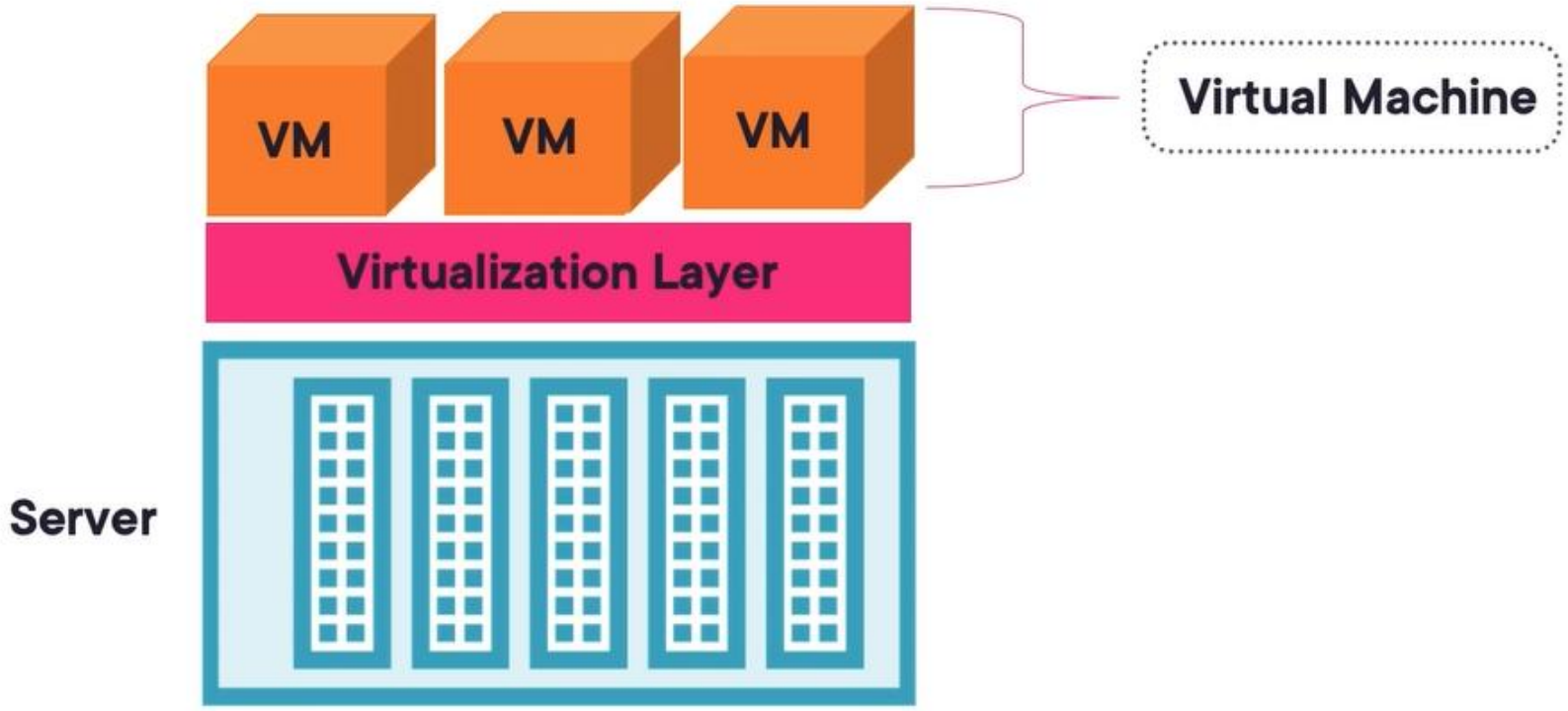
Types d’Hyperviseurs

Hyperviseur de type 2 (hosted)

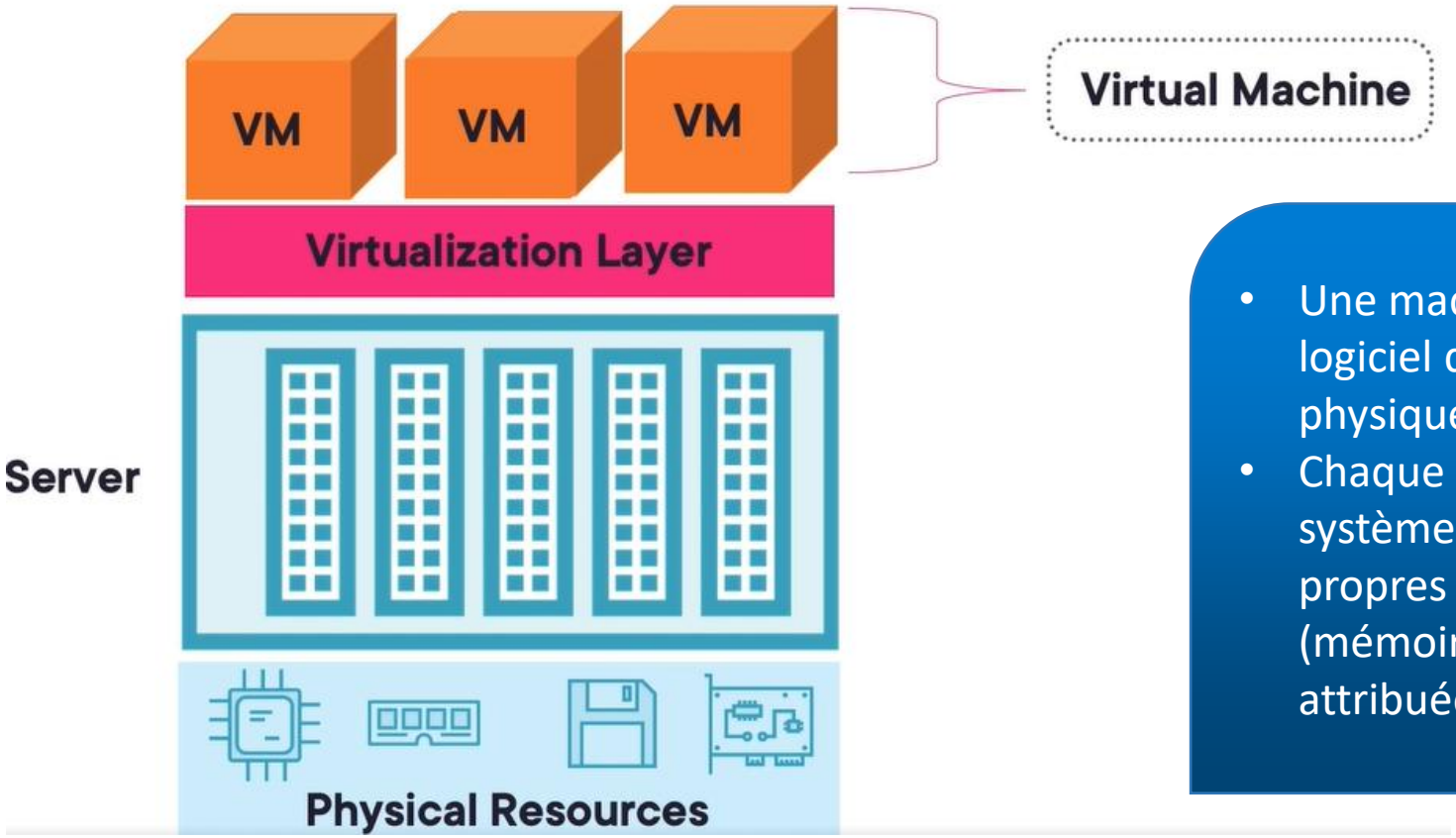
VMware Workstation (propriétaire): Solution de virtualisation pour les postes de travail, utilisée pour créer des VMs locales.

Oracle VirtualBox (open-source): Solution open-source qui permet la création de machines virtuelles sur une machine hôte.

Machine virtuelle et ressources virtuelles

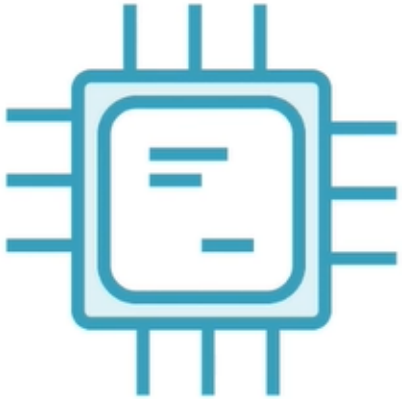


Machine virtuelle et ressources virtuelles



- Une machine virtuelle est un objet logiciel qui simule un serveur physique.
- Chaque Vm dispose de son propre système d'exploitation, de ses propres applications et ressources (mémoire, processeur, disque dur) attribuées par l'hyperviseur.

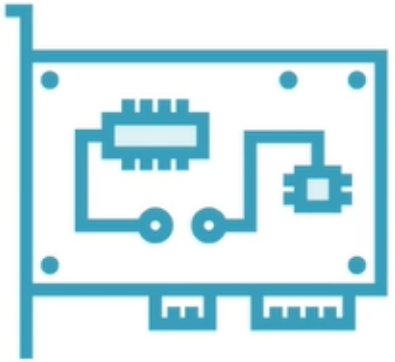
Machine virtuelle et ressources virtuelles



Virtual CPU

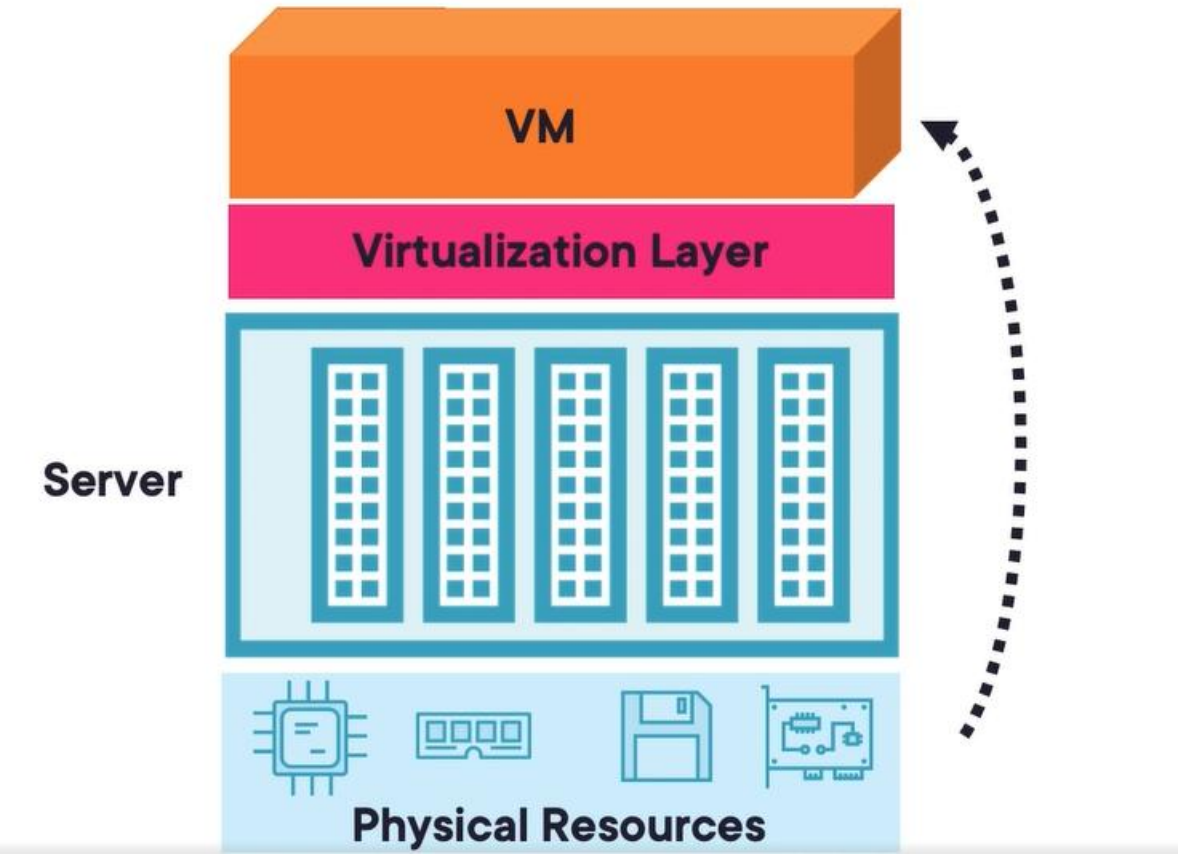
Virtual Memory

Virtual Disk

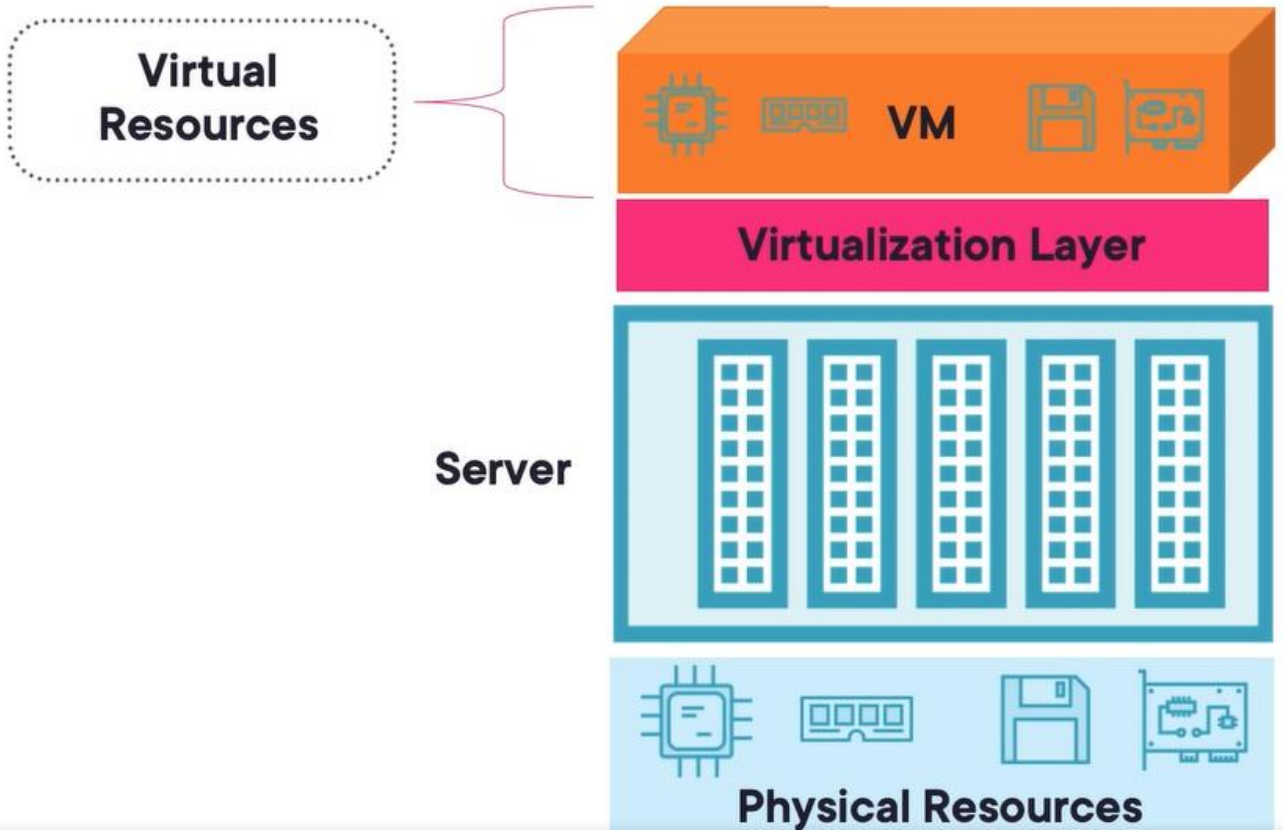


Virtual Network

Machine virtuelle et ressources virtuelles



Machine virtuelle et ressources virtuelles

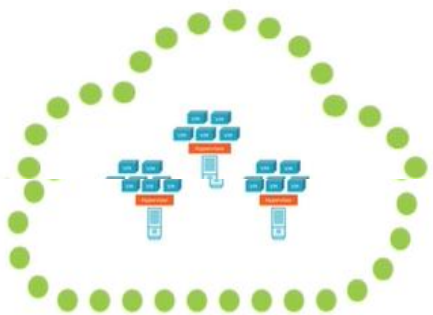


- **Le partage des ressources** permet une utilisation optimale des capacités matérielles, en assurant que plusieurs VMs peuvent fonctionner simultanément sur un serveur physique tout en préservant une certaine isolation.

Les intérêts - Virtualisation des serveurs

- Haute disponibilité et résilience (Migration facile),
- Optimisation des ressources (Meilleure utilisation du matériel),
- Réduction des coûts,
- Flexibilité et agilité (Déploiement rapide),
- Sécurité renforcée (des environnements isolés),...

Cloud-Based Virtualization Labs



VMware Hands-On Labs

https://labs.hol.vmware.com

Lab 1: Créer et gérer des VMs sur VirtualBox/VMware

Les étapes générales que vous pouvez suivre :

- **Étape 1** : Installation du logiciel de virtualisation (VirtualBox ou VMware Workstation) sur votre machine physique.
- **Étape 2** : Création d'une machine (Choisissez le type de système d'exploitation que vous souhaitez installer sur la VM. Configurez les paramètres de la VM, tels que la mémoire RAM, le processeur et le disque dur).
- **Étape 3** : Installation du système d'exploitation (Téléchargez l'image ISO du système d'exploitation choisi et montez-la sur la VM. Démarrez la VM et suivez le processus d'installation du système d'exploitation).
- **Étape 4** : Configuration de la VM (Configurez les paramètres réseau de la VM (par exemple, adresse IP, masque de sous-réseau, passerelle par défaut).
- **Étape 5** : Gestion des VMs (Apprenez à démarrer, arrêter et redémarrer les VMs).
- **Étape 6** : Test et validation (Testez la connectivité réseau entre les VMs et la machine physique. Vérifiez que les VMs fonctionnent correctement et que les applications installées sont accessibles).

Pratiques de sécurité pour l’environnement cloud computing

Cloud Security

- Le Cloud Computing est **un Modèle de fourniture de services informatiques** tels que le stockage de données, les serveurs, les bases de données, les logiciels et d'autres ressources via Internet.

- Cependant, bien que le cloud computing offre des avantages importants, notamment l'élasticité, la flexibilité et la réduction des coûts, mais il introduit aussi des risques spécifiques en matière de sécurité.

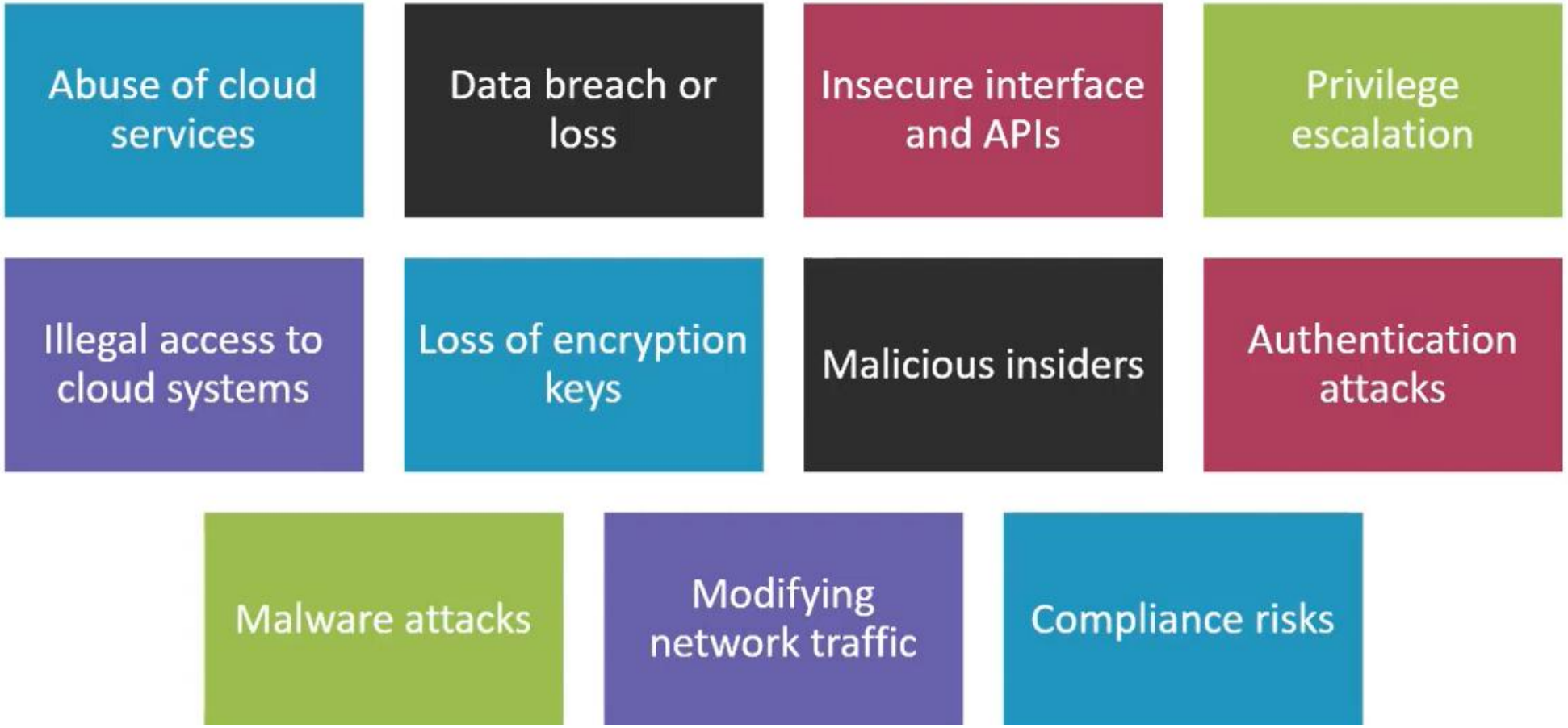
Cloud Security

- C’est pour cela qu’on a introduit la partie sécurité dans notre programme pour savoir un peu les ;
  - Principaux Risques et Menaces,
  - Meilleures Pratiques de Sécurité.

A. Menaces courantes dans le Cloud

- Les menaces sont des risques qui peuvent affecter la sécurité et la confidentialité des données stockées ou traitées dans des environnements Cloud.

A. Menaces courantes dans le Cloud



A. Menaces courantes dans le Cloud

- **Utilisation abusive des ressources (Cloud Resource Abuse):** est une menace courante qui se réfère à la consommation malveillante des ressources cloud, souvent sans autorisation appropriée ou en exploitant les vulnérabilités des systèmes.
  - **Utilisation non autorisée des comptes cloud:** un attaquant peut accéder à un compte cloud via des identifiants volés ou des failles de sécurité. Cela peut entraîner une augmentation des coûts, des violations de données et d'autres impacts.
  - **Cryptomining non autorisé:** consiste à utiliser les serveurs cloud pour miner(extraire) des cryptomonnaies, souvent sans la connaissance des propriétaires des ressources. Cela peut entraîner une surcharge des ressources, une hausse des coûts, une réduction des performances et un gaspillage des capacités informatiques.

A. Menaces courantes dans le Cloud

- **Violation ou Perte de Données:** fait référence à l'accès non autorisé, la divulgation ou la modification de données sensibles, souvent à la suite d'une faille de sécurité.
  - **Accès Non Autorisé (Hacking ou Intrusion) :** Les hackers peuvent exploiter des vulnérabilités dans les systèmes de sécurité, les API mal sécurisées, ou les erreurs de configuration pour accéder illégalement à des données sensibles stockées dans le cloud.
  - **Vulnérabilités dans les Logiciels et Applications Cloud :** Les applications utilisées dans le cloud peuvent contenir des vulnérabilités non corrigées que les attaquants peuvent exploiter pour accéder à des données sensibles.
  - **Attaques par Ransomware :** Les ransomwares sont des logiciels malveillants qui chiffrent les données et demandent une rançon pour les déchiffrer.

A. Menaces courantes dans le Cloud

- **Attaques d'Authentification:** sont des tentatives malveillantes visant à contourner les mécanismes de vérification d'identité utilisés pour accéder aux systèmes cloud ou à des services spécifiques dans le cloud. L'objectif de ces attaques est d'obtenir des privilèges élevés en utilisant des informations d'authentification de manière frauduleuse.
- **Attaque par Force Brute (Brute Force Attack):** Elle consiste à tester toutes les combinaisons possibles de mots de passe ou d'identifiants jusqu'à ce que la bonne combinaison soit trouvée.
- **Attaque par Dictionnaire (Dictionary Attack):** Cette attaque est similaire à l'attaque par force brute, mais au lieu d'essayer toutes les combinaisons possibles, l'attaquant utilise un dictionnaire de mots ou de phrases courantes (des mots de passe populaires ou des combinaisons fréquemment utilisées).
- **Attaque par Rejeu (Replay Attack)**: Elle consiste à capturer et réutiliser des informations d'authentification valides (comme des jetons ou des cookies d'authentification) qui ont été envoyées entre un utilisateur légitime et un service cloud.

A. Menaces courantes dans le Cloud

- **Les interfaces et APIs non sécurisées:**

Les interfaces et APIs sont couramment utilisées dans les environnements cloud pour permettre l'interaction entre les différents services et applications. Cependant, lorsqu'elles ne sont pas correctement sécurisées, elles peuvent devenir des vecteurs d'attaque pour des acteurs malveillants.

  - **API vulnérables à des attaques d'injection :** Certaines APIs sont mal protégées contre des attaques d'injection SQL, de script inter-sites (XSS) ou de commandes à distance, permettant à des attaquants d'injecter des commandes malveillantes ou de manipuler les bases de données sous-jacentes.

B. Meilleures Pratiques de Sécurité

- Pour se protéger contre ces types de menaces dans le cloud, cela nécessite une combinaison de bonnes pratiques, d'outils de sécurité et de stratégies adaptées à l'architecture cloud spécifique de l'entreprise.

B. Meilleures Pratiques de Sécurité

Gestion des identités et des accès (IAM)

- **Contrôle d'accès basé sur les rôles (RBAC - Role-Based Access Control) :** Usage des rôles spécifiques (Administrateur, Manager, Employé) avec des permissions minimales nécessaires pour limiter l'accès aux ressources du cloud.
- **Authentification multifactorielle (MFA) :** Activation de la MFA permet d’ajouter une couche de sécurité supplémentaire lors de l'accès aux systèmes cloud.

B. Meilleures Pratiques de Sécurité

Cryptage des données

- **Cryptage des données en transit :** Utiliser des protocols de chéfrement comme TLS/SSL pour protéger les données pendant leur transfert vers et depuis le cloud.
- **Cryptage des données au repos :** S’assurer que les données stockées dans le cloud sont cryptées pour prévenir l'accès non autorisé en cas de violation de sécurité.

B. Meilleures Pratiques de Sécurité

Surveillance et audit

- **Suivi et surveillance continue :** Utiliser des outils de surveillance pour détecter les activités suspectes et les violations de sécurité dans le cloud.
- **Audits réguliers :** Mettre en place des processus réguliers d'audit et de revue des logs pour identifier des vulnérabilités potentielles.
- **Alertes en temps réel :** Configurez des alertes en temps réel pour des événements de sécurité critiques (tentatives de connexion suspectes, accès non autorisé, etc.).

B. Meilleures Pratiques de Sécurité

Sécurisation des applications

- **Test de sécurité des applications :** Effectuer des tests de sécurité réguliers (par exemple, des tests de pénétration) pour identifier et corriger les vulnérabilités des applications.
- **Mise à jour régulière des logiciels :** Appliquer les patchs de sécurité et les mises à jour logicielles en temps utile pour éviter les attaques utilisant des failles connues.

B. Meilleures Pratiques de Sécurité

Sécurisation du réseau

- **Pare-feu et groupes de sécurité :** Utilisez des pare-feu et des groupes de sécurité pour contrôler le trafic entrant et sortant dans une infrastructure cloud.
- **VPN et tunnels sécurisés :** Pour les connexions privées entre les systèmes locaux et le cloud, utiliser des VPN ou des tunnels chiffrés pour garantir la sécurité des communications.
- **Segmentation du réseau :** Segmenter le réseau dans le cloud pour limiter les risques de propagation en cas de violation de sécurité.

B. Meilleures Pratiques de Sécurité

Sauvegarde et récupération d'urgence

- **Plan de récupération d'urgence :** Développer un plan de reprise après sinistre pour récupérer rapidement vos données et services en cas d’incident.
- **Sauvegarde régulière des données :** Assurer que les données sensibles sont sauvegardées de manière régulière et sécurisée dans le cloud ou hors ligne.

B. Meilleures Pratiques de Sécurité

Sensibilisation et formation des utilisateurs

- **Formation continue :** Une formation continue sur la sécurité à tous les employés afin qu'ils connaissent les bonnes pratiques pour l'utilisation des ressources cloud.
- **Phishing et ingénierie sociale :** Sensibiliser les utilisateurs aux risques d'ingénierie sociale (e.g., phishing attack), qui sont des vecteurs d'attaque courants.

Exemples: Mises à jour de sécurité pour plusieurs produits d'oracle (Réf: DGSSI)

Titre	Mises à jour de sécurité pour plusieurs produits d'oracle
Numéro de Référence	57662210/25
Date de publication	22 octobre 2025
Niveau de Risque	Critique
Niveau d'Impact	Critique

Systèmes affectés:

- Oracle Utilities Network Management System, versions 2.4.0.1.31, 2.5.0.1.15, 2.5.0.2.9, 2.6.0.1.8, 2.6.0.2.3
- Oracle VM VirtualBox, versions 7.1.12, 7.2.2
- Oracle WebCenter Forms Recognition, version 14.1.1.0.0
- Oracle WebCenter Portal, version 12.2.1.4.0
- Oracle WebCenter Sites, version 14.1.2.0.0

Exemples: Mises à jour de sécurité pour plusieurs produits d'oracle (Réf: DGSSI)

Bilan de la vulnérabilité:

L'exploitation de ces vulnérabilités peut permettre à un attaquant distant non authentifié d'exécuter du code arbitraire, d'accéder à des données confidentielles, de contourner des mesures de sécurité ou causer un déni de service (DoS).

Risque:

- Exécution de code arbitraire à distance
- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Déni de service

Solution:

Veuillez se référer au bulletin de sécurité d'Oracle afin **d'installer les nouvelles mises à jour**.

Middleware

Examples of Software Middleware:

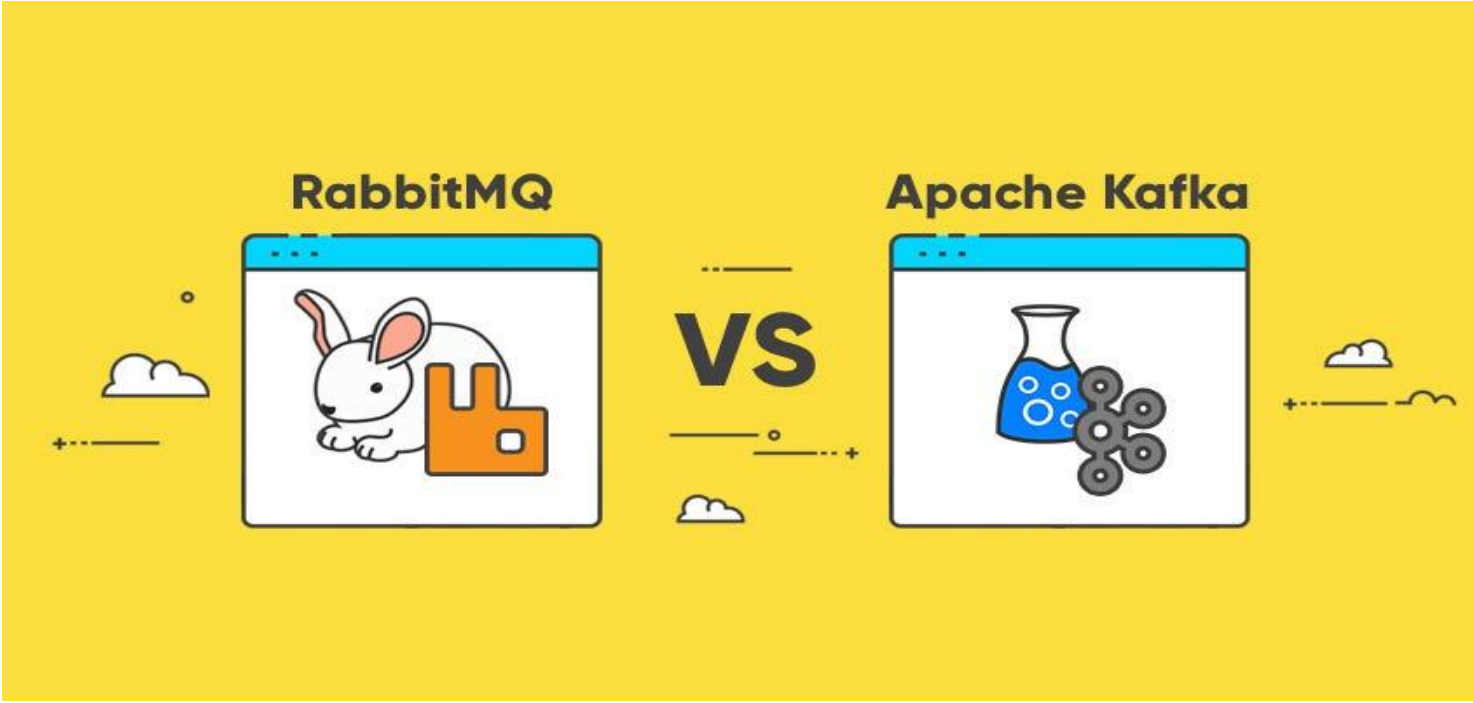
1. Database Middleware

ODBC (Open Database Connectivity) or **JDBC** (Java Database Connectivity), which allow applications to communicate with various database management systems.

Examples of Software Middleware:

2. Message-Oriented Middleware (MOM)

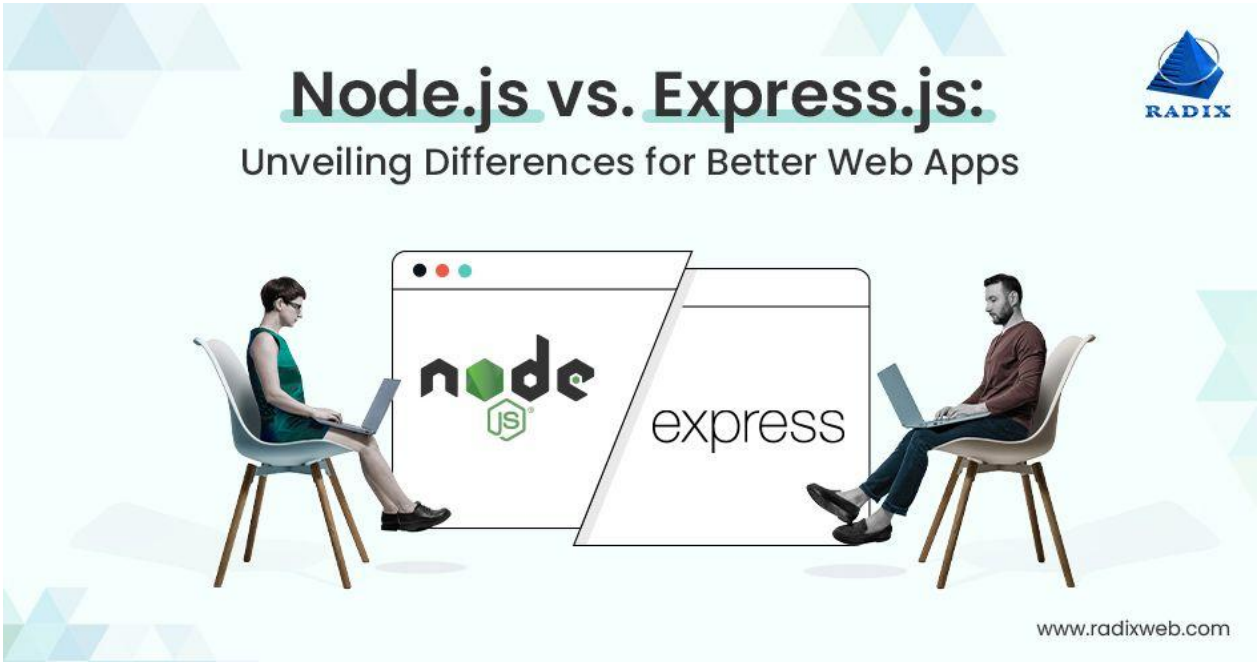
RabbitMQ or **Apache Kafka**, which allow applications to send and receive messages asynchronously.



Examples of Software Middleware:

3. Web Middleware

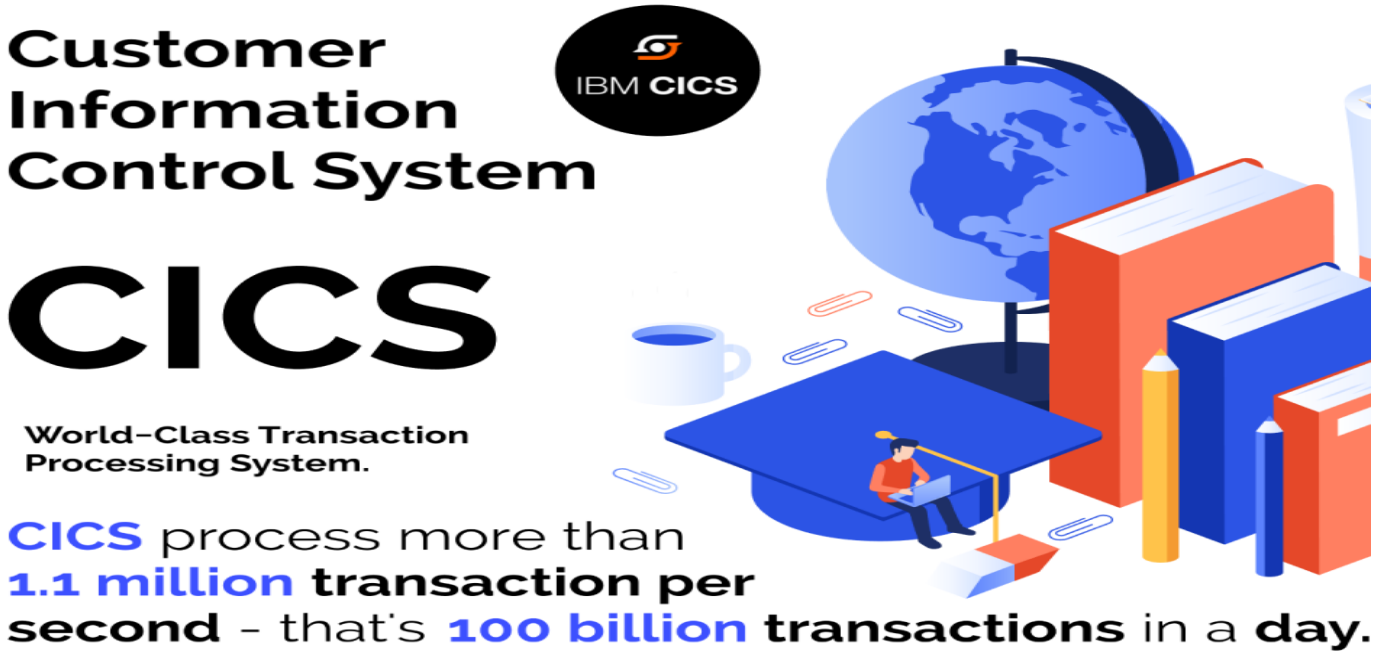
In a web application built with **Node.js** using the **Express.js** framework, **middleware functions** (**express.json(), express.urlencoded(), express-session, …etc**) are used to handle requests and responses (e.g., for authentication, logging, parsing JSON).



Examples of Software Middleware:

4. Transaction Processing Monitors

IBM's CICS, which manage transactions across multiple databases and systems.



Examples of Software Middleware:

5. RPC (Remote Procedure Call) and RMI (Remote Method Invocation)

Mechanisms that allow a program to cause a procedure to execute in another address space (on another computer).