



Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation
Ecole Nationale des Sciences Appliquées de Marrakech - Université Caddi Ayyad
Génie Cyber-Défense et Systèmes de Télécommunications Embarqués



Introduction à la Virtualisation

**Module M45 – Virtualisation, Cloud Computing,
SDN et sécurité**

Prof. Omar ACHBAROU

2023/2024

©Achbarou

o.achbarou@uca.ma



PLAN

01 Architectures classiques

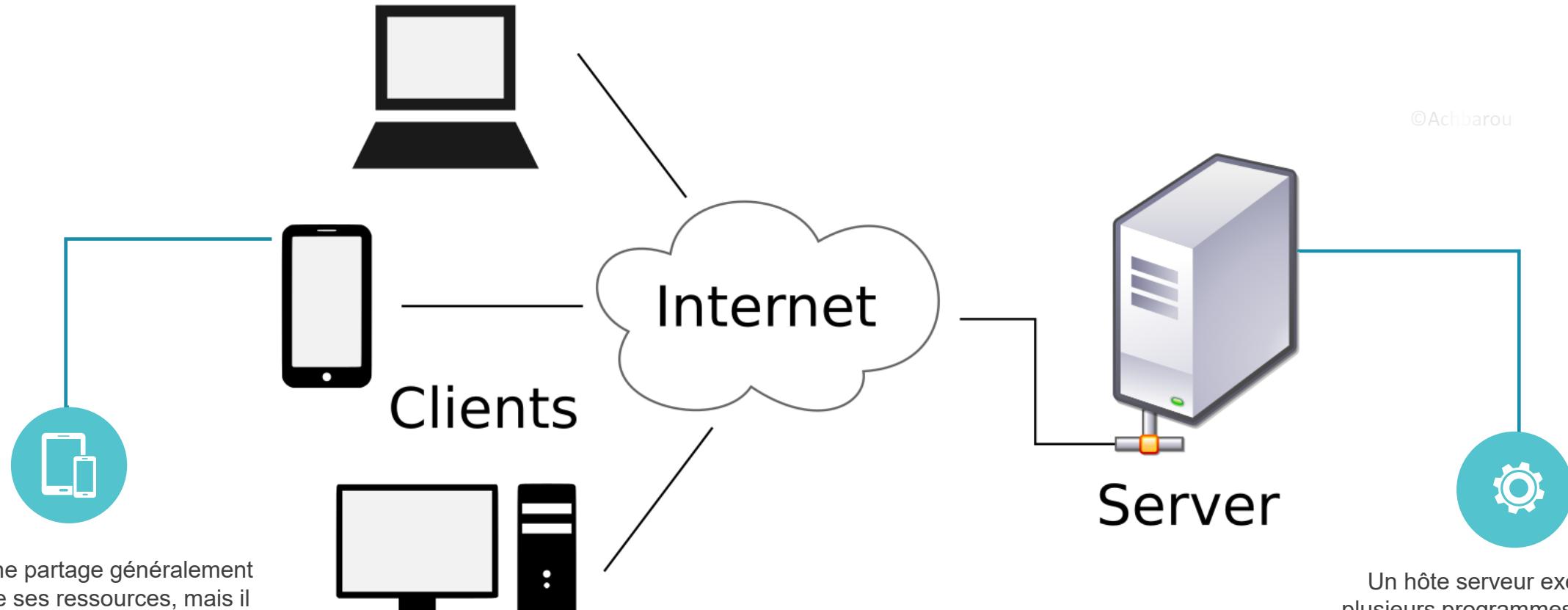
02 Virtualisation

03 Hyperviseurs

04 Types de Virtualisation

05 Virtualisation et Sécurité

Architecture Classique (client / serveur)

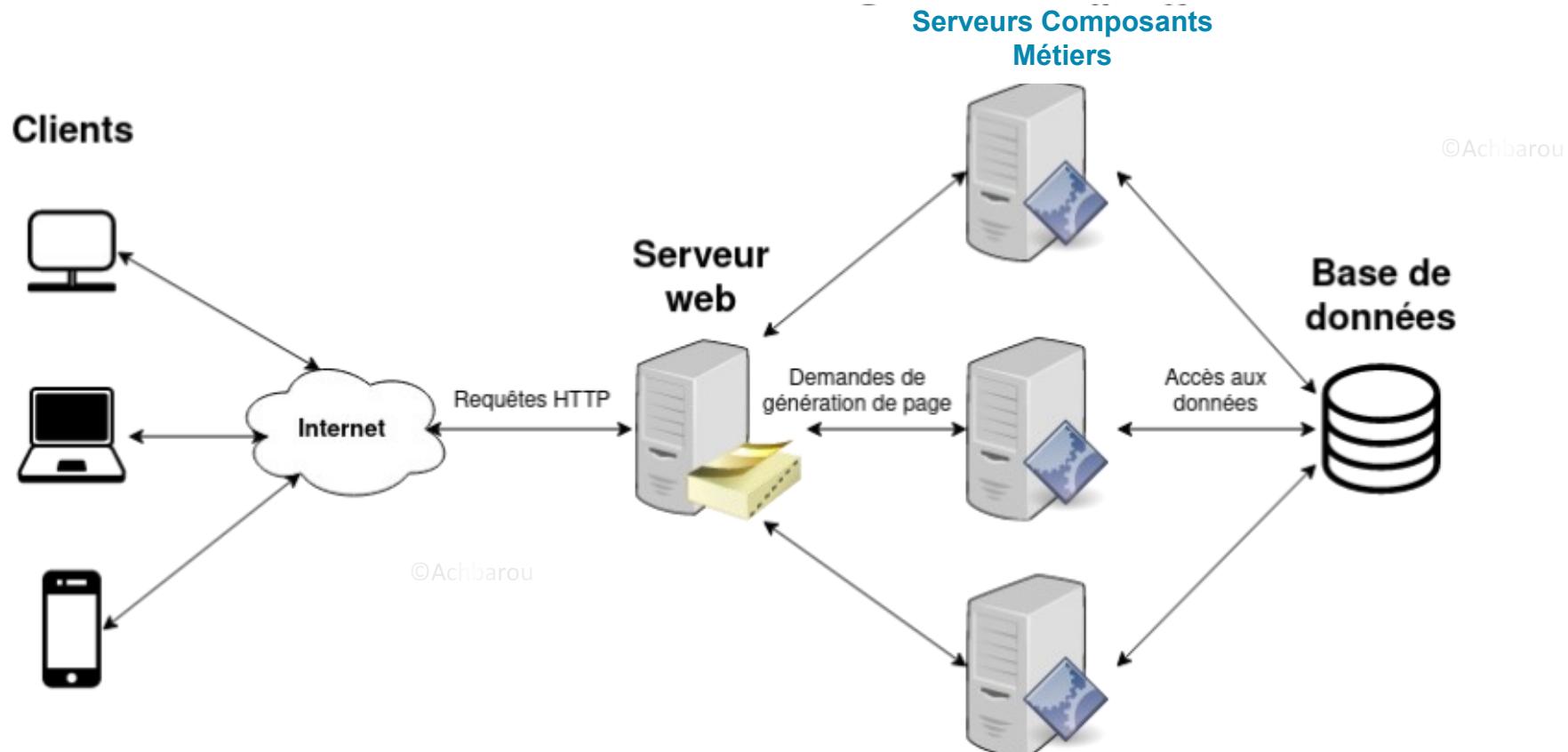


Un client ne partage généralement aucune de ses ressources, mais il demande un contenu ou un service à un serveur.

Un hôte serveur exécute un ou plusieurs programmes serveurs, qui partagent leurs ressources avec les clients.

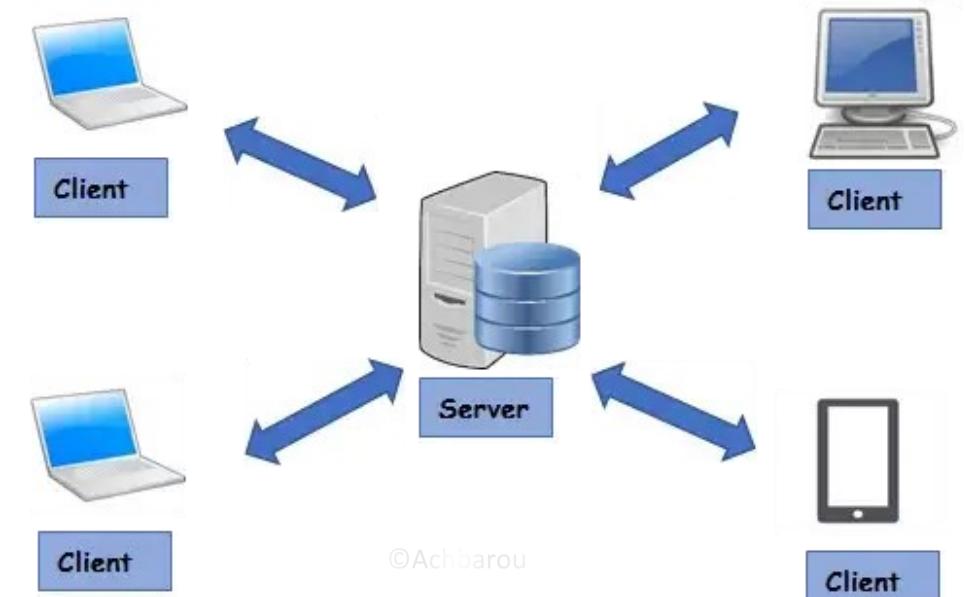
Architecture classique N-tiers

L'architecture N-tier ou encore: étage, niveau est une [architecture client-serveur](#) dans appelée multi-tier, est une architecture client-serveur dans laquelle une application est exécutée par plusieurs laquelle une application est exécutée par plusieurs composants logiciels distincts



Inconvénient des architectures classiques

- Coût
- L'application dépend du matériel
- Un seul OS par serveur
- Une application par OS
- Gaspillage des ressources serveur
- L'arrêt d'un service engendre un blocage du système
- Pas de reprise instantanée en cas d'arrêt du service
- La maintenance du système ou d'application engendre un arrêt complet du service



©Achbarou



Altérer la Sûreté de fonctionnement de l'application

La nouvelle conception architectural

La **virtualisation** utilise un logiciel pour créer sur le matériel informatique une couche d'abstraction qui permet de **diviser** les éléments matériels d'un même ordinateur - processeurs, mémoire, stockage et autres - en plusieurs **ordinateurs virtuels**, communément appelés **machines virtuelles** (**VM**). Chaque VM exécute son propre OS et se comporte comme un ordinateur indépendant, même si elle ne fonctionne que sur une partie du matériel informatique sous-jacent.



La virtualisation

- La **virtualisation** est une technologie qui permet de fonctionner sur un seul serveur plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des **ordinateurs physiques** distincts.

©Achbarou

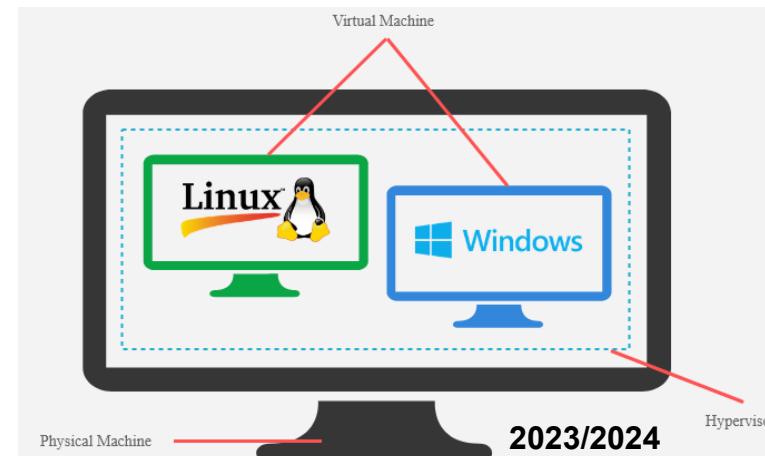
- L'exécution de **plusieurs systèmes d'exploitation** avec plusieurs **applications exécutées** sur un même serveur en même temps tout en augmentant **l'utilisation et la flexibilité du matériel**.

©Achbarou

©Achbarou

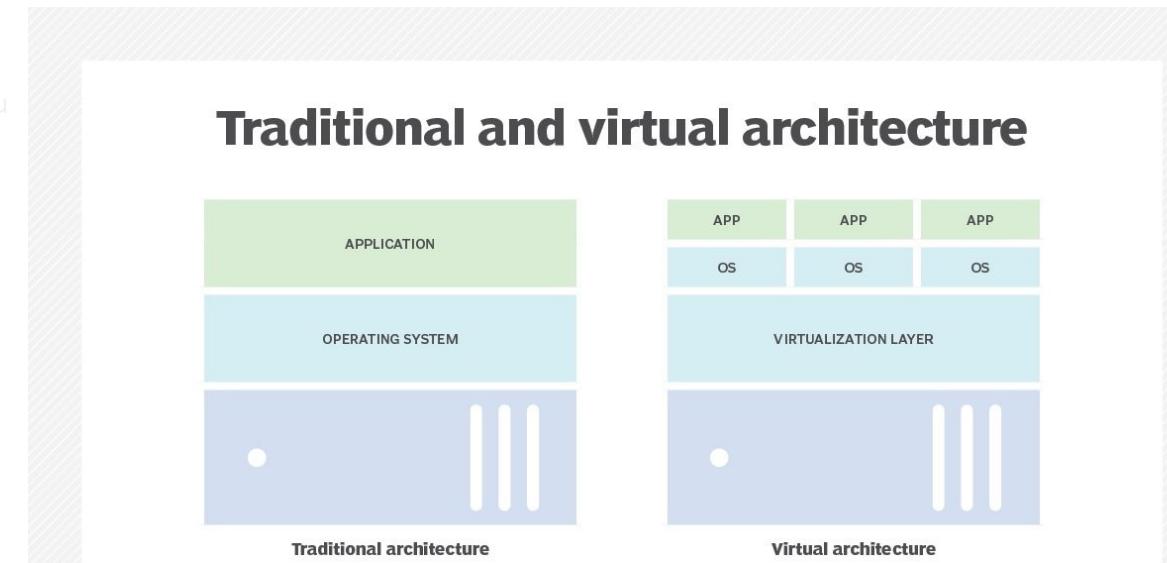
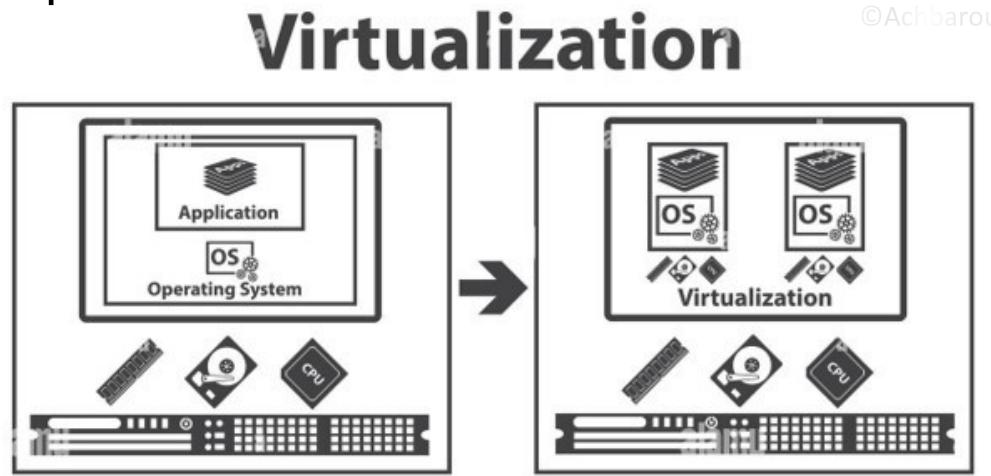
- La virtualisation est une technologie qui permet une **gestion optimisée des ressources matérielles** en disposant de plusieurs machines virtuelles sur une seule machine physique.

©Achbarou



L'architecture de virtualisation

- L'architecture de virtualisation est une **représentation visuelle** de virtualisation. Elle cartographie et décrit les différents éléments virtuels de l'écosystème.
- Une machine virtuelle (VM) est un **environnement d'exécution isolé** (système d'exploitation invité et applications).
- Plusieurs systèmes virtuels (VM) peuvent fonctionner sur un seul système physique.



L'architecture de virtualisation

- **Partitionnement**

- Différents OS peuvent **être partagés** sur les différents machines virtuelles
- Les ressources de matériels peuvent **être partagées** sur les différents VMs

- **Isolation**

©Achbarou

- **Niveau de sécurité** au niveau d'architecture
- Contrôle de ressources pour un niveau de **performance constant**.

- **Encapsulation**

- Toute la machine virtuelle est stockée dans des **fichiers isolés**
- Toutes les opérations usuelles de gestion des fichiers sont applicables sur les VM de **manière isolée**.



©Achbarou

Avantages de la virtualisation

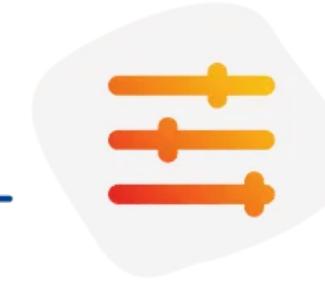
- La virtualisation permet donc une utilisation plus **efficace du matériel** informatique physique et offre un meilleur retour sur **l'investissement matériel** d'une organisation tout en augmentant l'**utilisation** et la **flexibilité** du matériel.
- La virtualisation peut accroître l'**agilité**, la **flexibilité** et l'**évolutivité** de l'informatique tout en permettant de réaliser d'**importantes économies**.
- Une plus grande **mobilité** des charges de travail, des **performances** et une **disponibilité** accrues des ressources, des **opérations automatisées** - ce sont tous des avantages de la virtualisation qui rendent l'informatique **plus simple** à gérer et **moins coûteuse** à posséder et à exploiter.

@Achbarou



Cost Saving

+



High Flexibility And Scalability

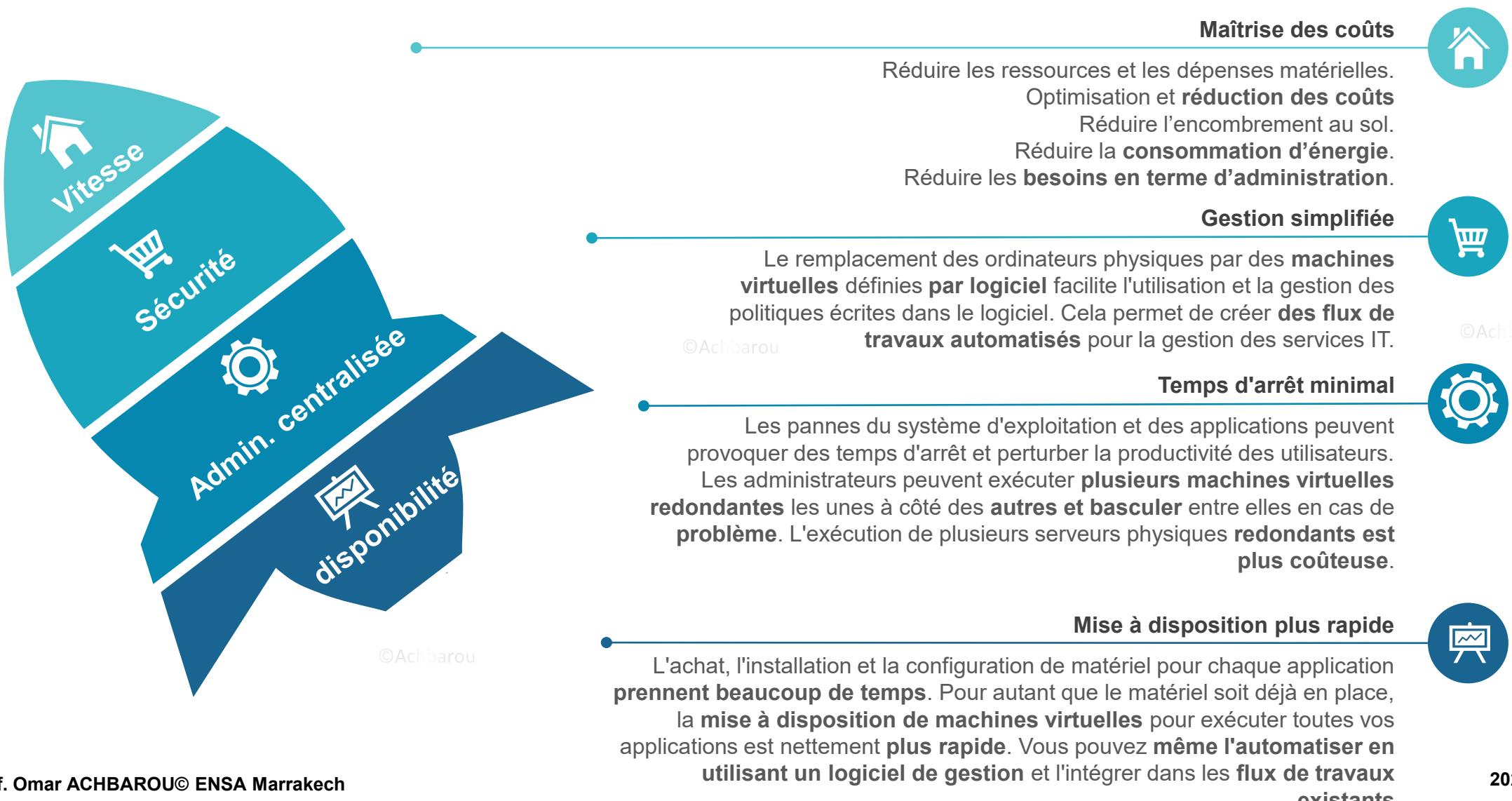
+



Enhanced Security

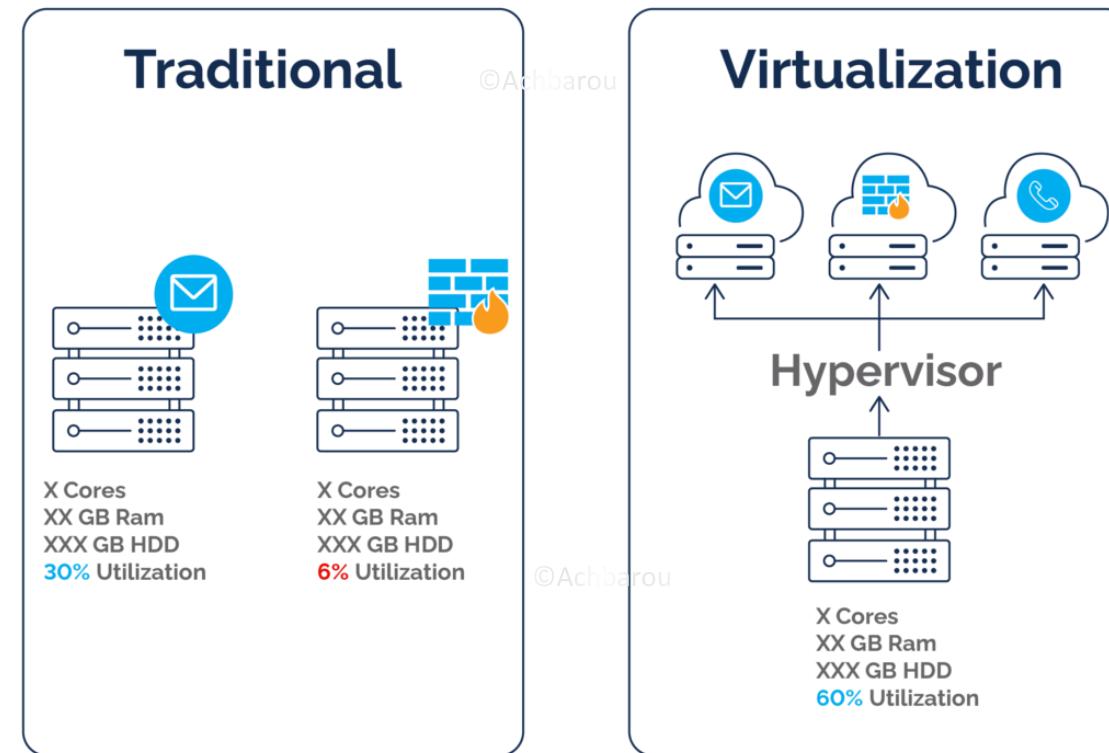
@Achbarou

Avantages de la virtualisation



hyperviseurs

- La **gestion** et l'**ordonnancement** des machines virtuelles sont effectués par une plate-forme qui vient se placer entre la couche matérielle et les machines virtuelles : **Virtual Machine Monitor (VMM)** ou le gestionnaire de machines virtuelles, également connu sous le nom d'**hyperviseur**.



Pourquoi l'hyperviseurs

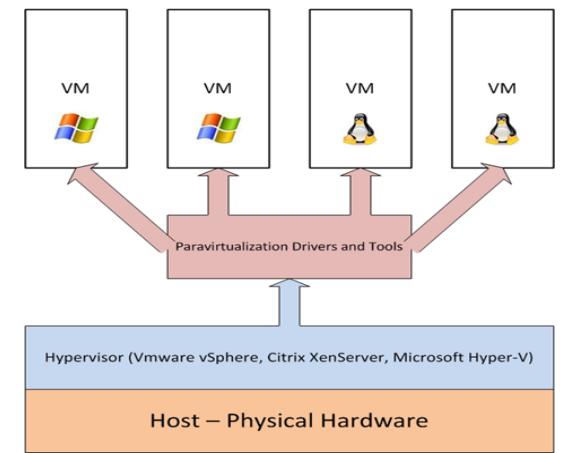
- Il permet à un ordinateur hôte de prendre en charge plusieurs VM clientes en partageant **virtuellement ses ressources**, en d'autres termes, gère les ressources physiques, telles que le CPU, la mémoire et le stockage, qui exécutent des fonctions dans les **environnements VM**.

©Achbarou

- Les hyperviseurs permettent de mieux exploiter les ressources disponibles d'un système et de procurer une plus **grande mobilité** informatique, puisque les VM clientes sont indépendantes du matériel de l'hôte. Autrement dit, elles peuvent facilement être **déplacées entre différents serveurs**.

©Achbarou

©Achbarou



Caractéristiques d'hyperviseur

01 Consolidation des serveurs

Hyper offre un tableau de bord, qui centralise la gestion des serveurs sur plusieurs VM, qui peuvent exécuter différents OS. Les admins peuvent interagir avec de nombreuses VMs par le biais de l'hyperviseur, comme s'il s'agissait d'une **seule vitre**.



02 RéPLICATION des données

Les VM sont difficiles à répliquer à l'aide des méthodes traditionnelles. Il est nécessaire de répliquer le volume entier de la VM et, souvent, toutes les VM d'un serveur particulier. **Vous pouvez sélectionner les VM et les parties de ces VM à répliquer**, ce qui constitue une nette amélioration.

03 Optimisation des ressources

Les hypers aident les entreprises à utiliser plus l'équipement physique sous-jacent. La virtualisation a considérablement augmenté les taux d'utilisation des serveurs.

En distribuant également le **réseau et la bande passante de manière de plus en plus intelligente**, les hyperviseurs peuvent vous aider à **tirer le meilleur parti** de toutes sortes de ressources.

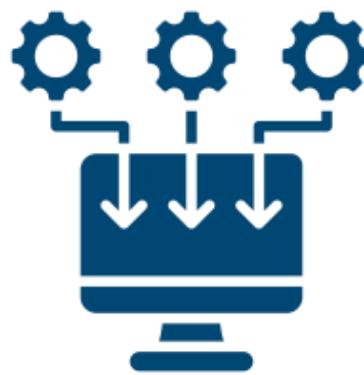
04 Mise en miroir de l'environnement bureau

Vous pouvez utiliser un hyperviseur pour héberger facilement un bureau virtuel sur un serveur (**Virtual desktop integration (VDI)**). Ce VDI sera la **réplique exacte du bureau physique** d'un utilisateur. Cela permettra à vos employés de travailler à distance, où qu'ils soient, puisqu'ils pourront accéder à **leur PC** par Internet ou par un **client léger**.

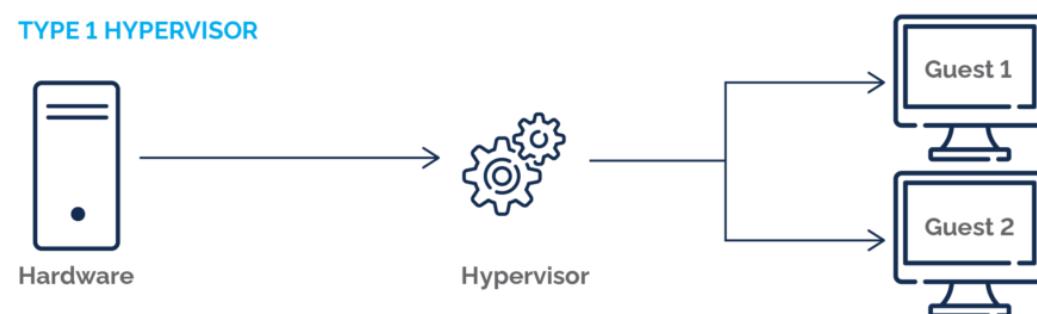
Types d'hyperviseurs

- Il existe deux principaux types d'hyperviseurs utilisés par les administrateurs système et les développeurs de logiciels.
- Ces types d'hyperviseurs présentent des avantages uniques pour différentes fonctions professionnelles.

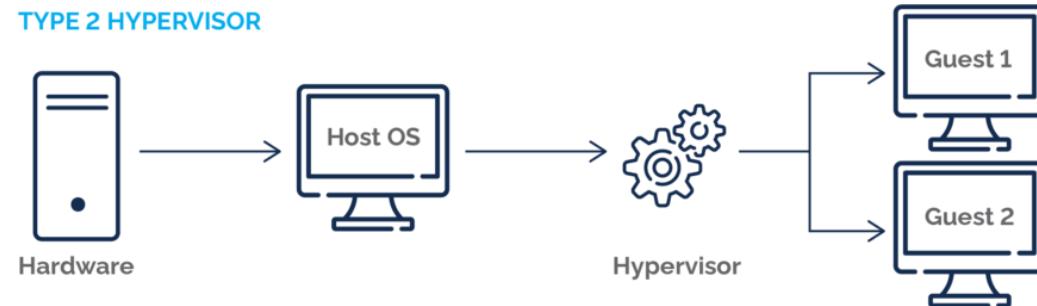
HYPervisor TYPES



TYPE 1 HYPERVISOR



TYPE 2 HYPERVISOR

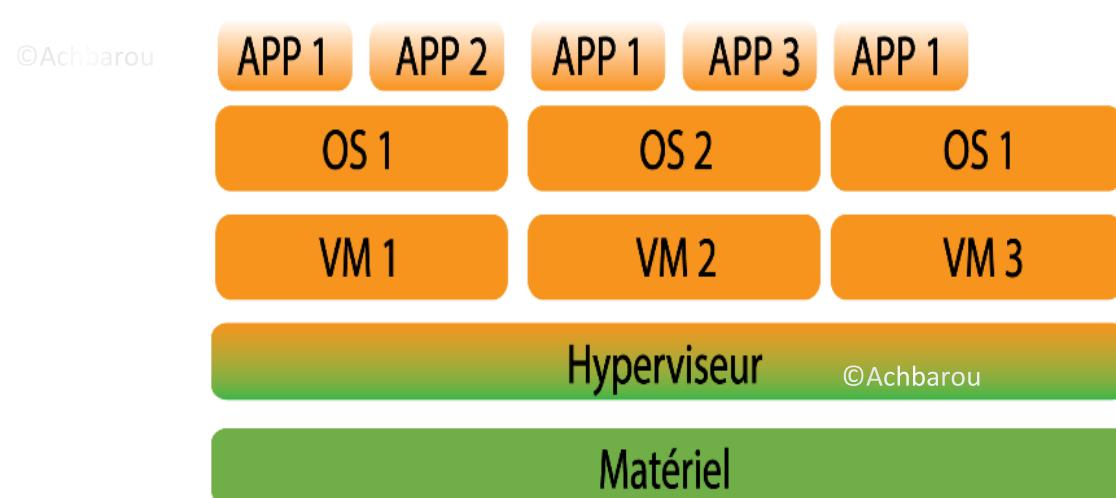


Types d'hyperviseurs – type 1

- Un hyperviseur de type 1 (natif) est une plate-forme qui fonctionne directement sur la **couche matérielle** du serveur.
- Plus courant dans les centres de données d'entreprise, un hyperviseur de type 1 **remplace le système d'exploitation** de l'hôte et se trouve juste au-dessus du matériel.
- Pour cette raison, les hyperviseurs de type 1 sont également appelés hyperviseurs **bare metal** ou **natif** (Bare metal or native hypervisors).

Exemple

- VMware hypervisors like vSphere, ESXi and ESX
- Microsoft Hyper-V
- Oracle VM Server
- Citrix Hypervisor
- Proxmox
- Xen



Types d'hyperviseurs – type 2

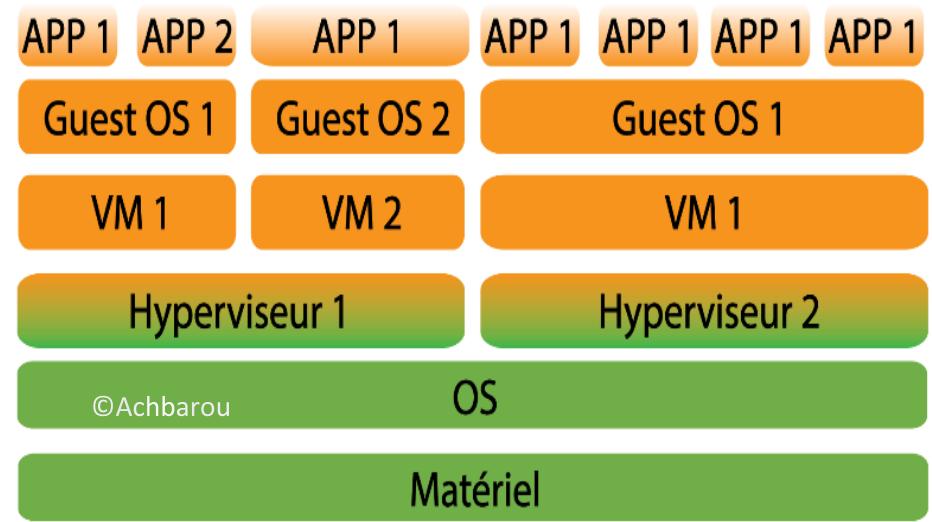
- Un hyperviseur de type 2 (Hosted or embedded hypervisors) qui s'installe et s'exécute sur un système d'exploitation standard. L'intérêt de ce type est le fait de pouvoir **exécuter plusieurs hyperviseurs** simultanément qu'ils ne sont pas liés à la couche matérielle.
- Il est hébergé et **fonctionné en tant que logiciel** sur le OS qui, à son tour, fonctionne sur le matériel physique. Cette forme d'hyperviseur est généralement utilisée pour exécuter **plusieurs OS sur un ordinateur personnel**, par exemple pour permettre à l'utilisateur de démarrer sur Windows ou Linux.

@Achbarou

Exemple

- VMware Workstation
- VMware Fusion
- Oracle VirtualBox
- Oracle Solaris Zones
- Oracle VM Server for x86

@Achbarou



Hyperviseurs - la sécurité

- Une VM fournit un **environnement isolé** du reste du système, donc il ne peut y avoir aucune **interférence** entre les programmes exécutés au sein d'une machine virtuelle et sur le matériel physique.
- Ainsi, si l'une d'entre elles (VM) est compromise, cela ne devrait pas avoir d'effet sur le reste du système.
- En revanche, si l'hyperviseur **est piraté**, toutes les machines virtuelles qu'il gère, et toutes les données qu'elles contiennent, se **retrouvent exposées**.
- Les protocoles et les exigences de **sécurité peuvent varier** selon le type d'hyperviseur.

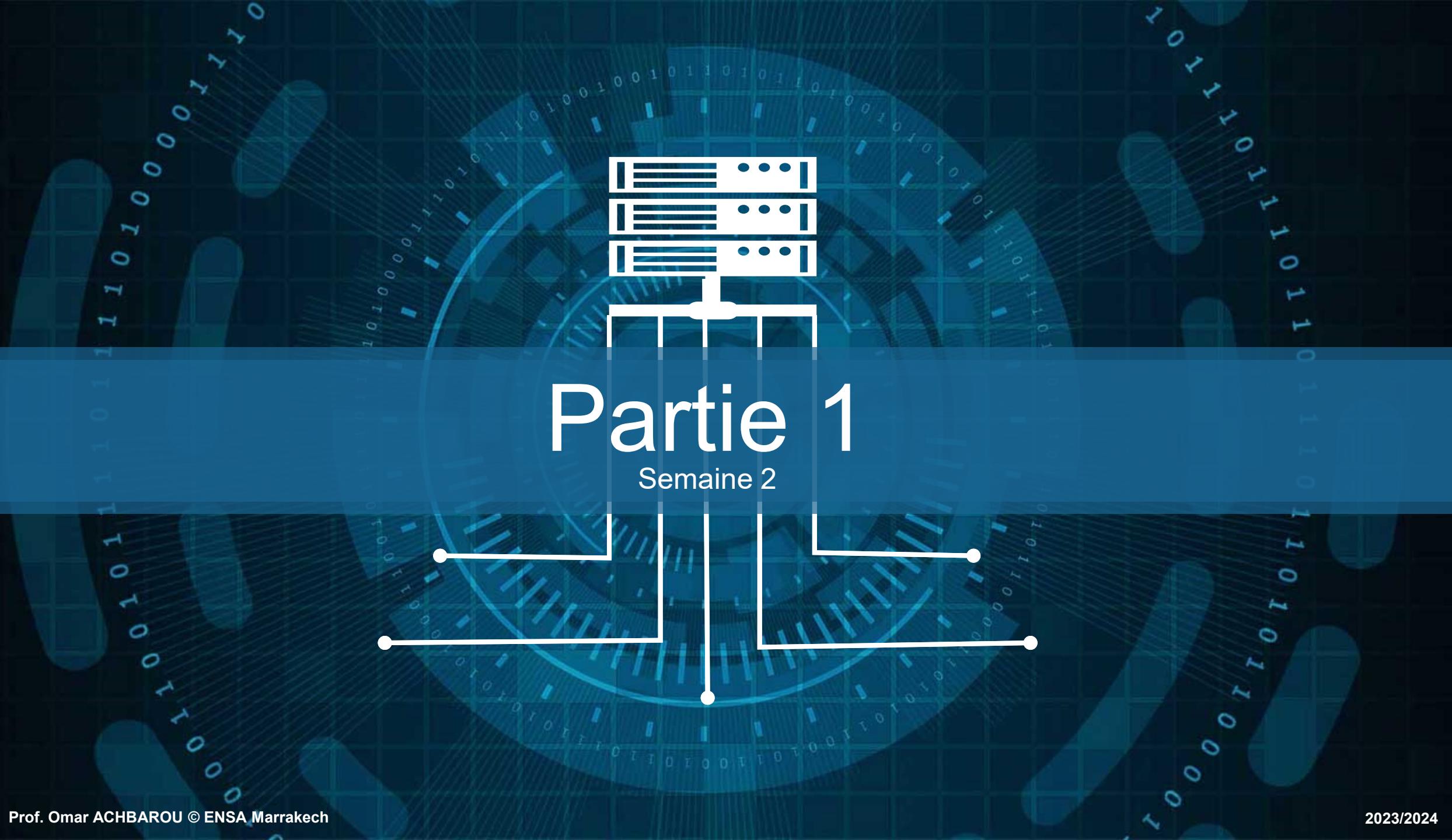
©Achbarou

©Achbarou



Partie 1

Semaine 2



Types de virtualisation

virtualization architecture



Types de virtualisation

- Virtualisation de postes
- Virtualisation du réseau
- Virtualisation du stockage
- Virtualisation d'applications
- Virtualisation des données
- Virtualisation du centre de données
- Virtualisation des unités centrales (UC)
- Virtualisation des processeurs graphiques (GPU)
- Virtualisation Linux
- Virtualisation du cloud

©Achbarou

©Achbarou

Types Of Virtualization



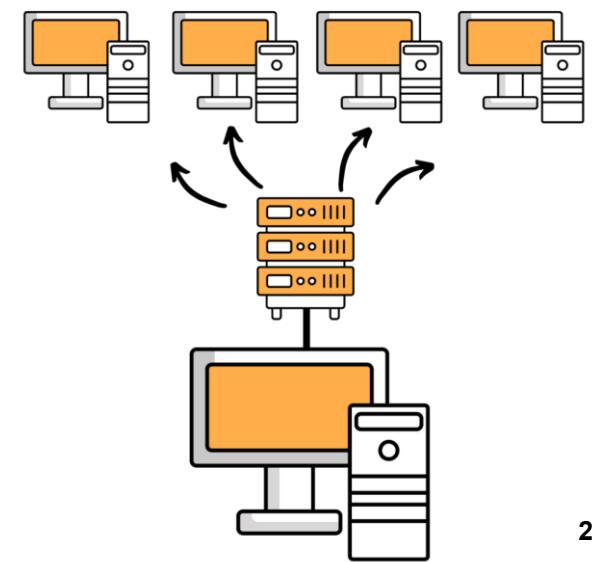
www.educba.com

Virtualisation de postes

- La virtualisation de postes est une méthode de simulation d'une station de travail d'un utilisateur accessible depuis un **terminal connecté à distance**.
- Les entreprises peuvent permettre aux utilisateurs de travailler pratiquement partout avec une connexion réseau, en utilisant n'importe quel ordinateur **portable**, **tablette** ou **smartphone** pour accéder aux **ressources de l'entreprise** quels que soient le terminal (passif) ou le système d'exploitation de l'utilisateur distant.
- Il existe deux types de virtualisation de postes :
 - L'infrastructure de bureau virtuel (VDI)
 - La virtualisation de poste local

@Achbarou

@Achbarou



@Achbarou

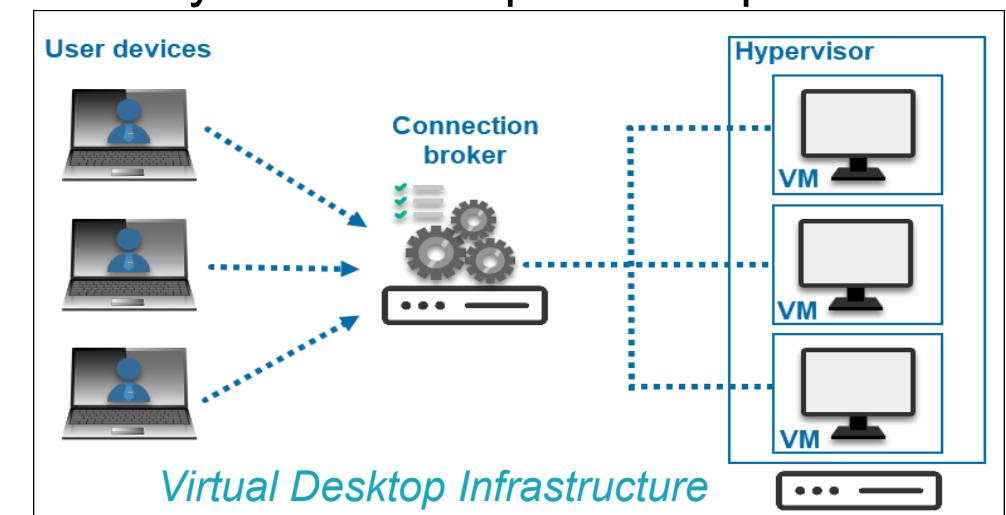
L'infrastructure de bureau virtuel - VDI

- Les hyper de type 1 peuvent virtualiser plus que les systèmes d'exploitation des serveurs. Ils peuvent également virtualiser les **systèmes d'exploitation des postes de travail** pour les entreprises qui souhaitent gérer de **manière centralisée** les ressources informatiques **à la demande** des utilisateurs finaux.
- Intégration du bureau virtuel (VDI) permet aux utilisateurs de travailler sur des postes de travail fonctionnant à l'intérieur de machines virtuelles sur un serveur central, ce qui **facilite l'administration** et la **maintenance** des systèmes d'exploitation par le personnel informatique.

©Achbarou

©Achbarou

©Achbarou



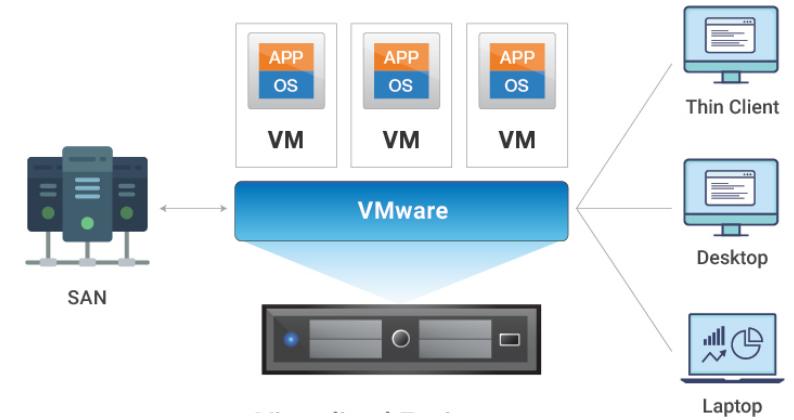
L'infrastructure de bureau virtuel - VDI

- Dans la VDI, un hyperviseur segmente les serveurs en machines virtuelles qui, à leur tour, hébergent des **bureaux virtuels** auxquels les utilisateurs accèdent à distance depuis leurs appareils.
- Les utilisateurs peuvent accéder à ces **postes de travail virtuels** à partir de n'importe quel appareil ou emplacement, et tout le traitement est effectué sur le serveur hôte.
- Les utilisateurs se connectent à leurs instances de bureau par l'intermédiaire d'un courtier de connexion, qui est une **passerelle logicielle** servant d'intermédiaire entre l'utilisateur et le serveur

©Achbarou

©Achbarou

©Achbarou



Virtualisation de poste local

- La **virtualisation de poste local** exécute un **hyperviseur sur un ordinateur local**, ce qui permet à l'utilisateur d'exécuter un ou plusieurs systèmes d'exploitation supplémentaires sur cet ordinateur et de passer d'un système d'exploitation à un autre selon les besoins, sans rien changer au système d'exploitation principal.
- Dans le contexte du Cloud Computing, on parle de "**Desktop-as-a-Service (DaaS)**"

©Achbarou

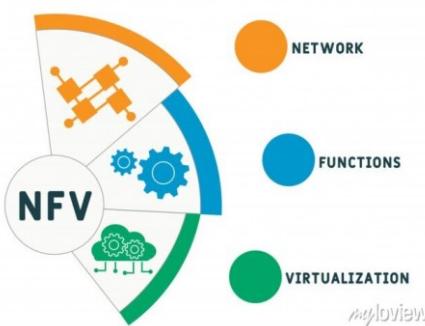
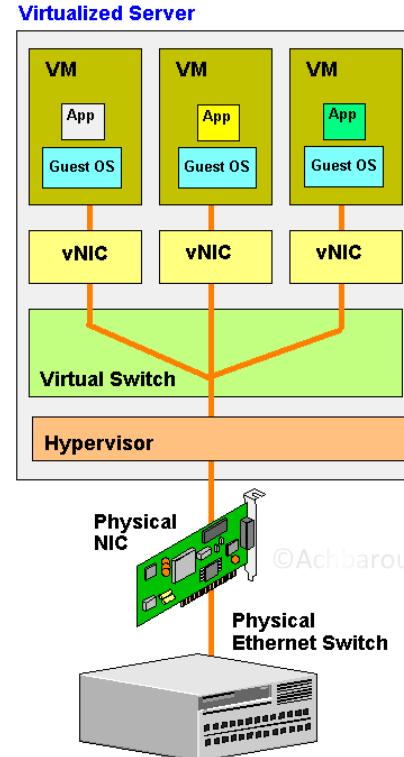


Virtualisation du réseau

- La virtualisation des réseaux (NV) fait référence à **l'abstraction des ressources** de réseau qui étaient traditionnellement fournies sous forme de matériel pour **les transformer en logiciel**. La NV peut combiner plusieurs réseaux physiques en un seul **réseau virtuel basé sur un logiciel**, ou elle peut diviser un réseau physique en **réseaux virtuels séparés** et indépendants (VLAN).
- Le logiciel de virtualisation de réseau permet aux administrateurs de réseau de déplacer des VM dans différents domaines sans **reconfigurer le réseau**. Le logiciel crée une superposition de réseaux qui peut exécuter des couches de réseaux virtuels distincts au-dessus de la même structure de réseau physique.
- Exemple : **mise en réseau définie par logiciel (SDN)**, et la **virtualisation de la fonction réseau (NFV)**, Les **LAN virtuels (VLAN)**, **VMware NSX Data Center**

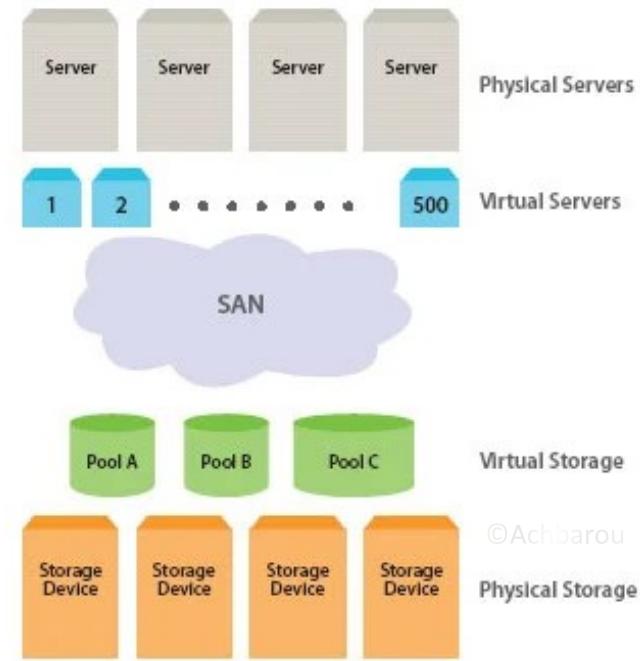
©Achbarou

©Achbarou



Virtualisation du stockage

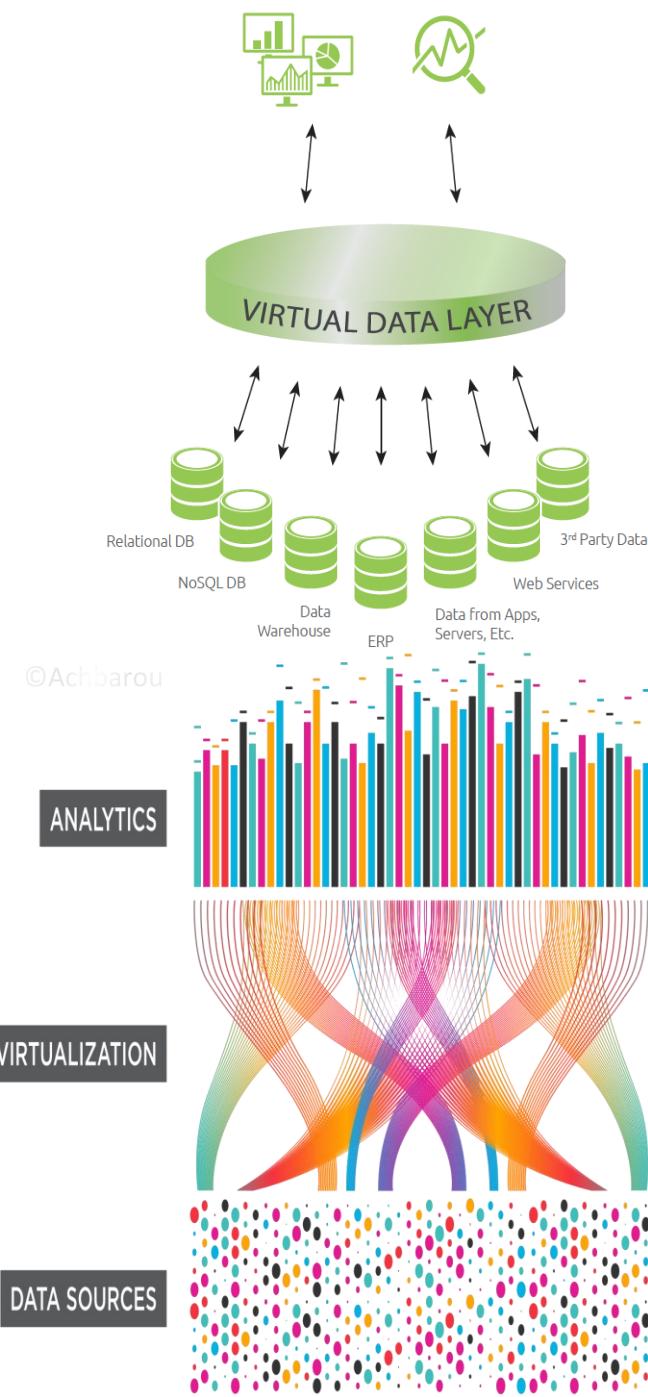
- La virtualisation du stockage (parfois appelée **Software-Defined Storage** ou **SAN** virtuel) consiste à regrouper en **pool plusieurs baies de stockage physique** des réseaux SAN et à les faire apparaître comme un **seul dispositif de stockage virtuel**. Le pool peut **intégrer des matériels de stockage différents**, provenant de différents **réseaux, fournisseurs** ou **datacenters**, dans une seule vue logique et les gérer à partir d'une interface unique.
- De plus, elle permet de **virtualiser le matériel de stockage** (baies et disques) sous forme de pools de stockage virtuel de la même manière que la virtualisation du calcul (VMWare ESX ou Hyper-V) virtualise le matériel de calcul (serveurs) en instances de machines virtuelles (VM).



Virtualisation des données

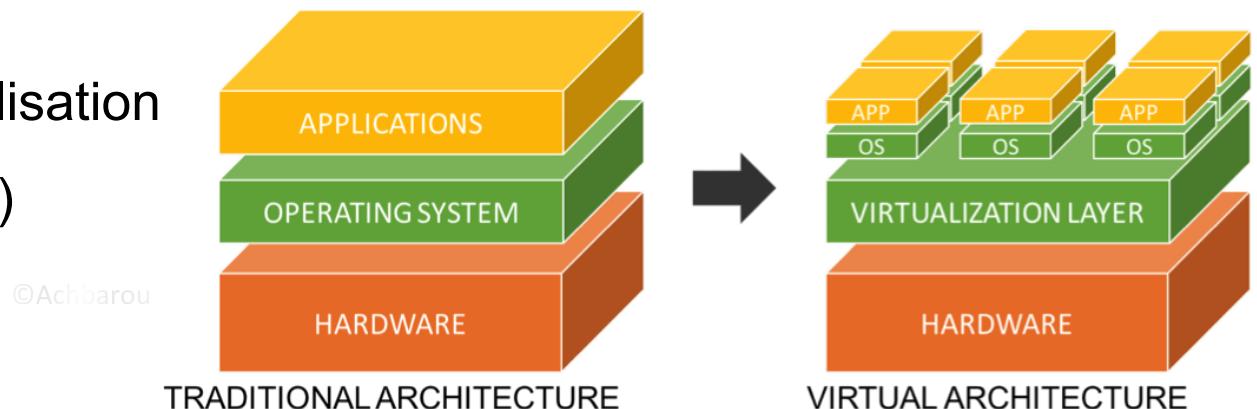
- La **Data Virtualization** ou virtualisation de données permet d'intégrer des données en provenance de **sources diverses** et quels que soient **leur format ou leur emplacement**. Cette technique simplifie l'accès aux données et leur analyse. Elle permet de manipuler les données et de les retrouver **même sans savoir où elles sont stockées** où dans quel format.
- Virtualiser les données** consiste à fournir une abstraction (ou une interface) qui masque les détails techniques liés à la donnée, tels que sa localisation sur le disque dur ou dans la base de données, sa structure de stockage, les API d'accès, le langage de requête,...etc
- Exemple : **IBM Cloud Pak for Data**, **Datameer Spotlight**, **Data Virtuality**, **Denodo Platform**

@Achbarou



Virtualisation d'applications

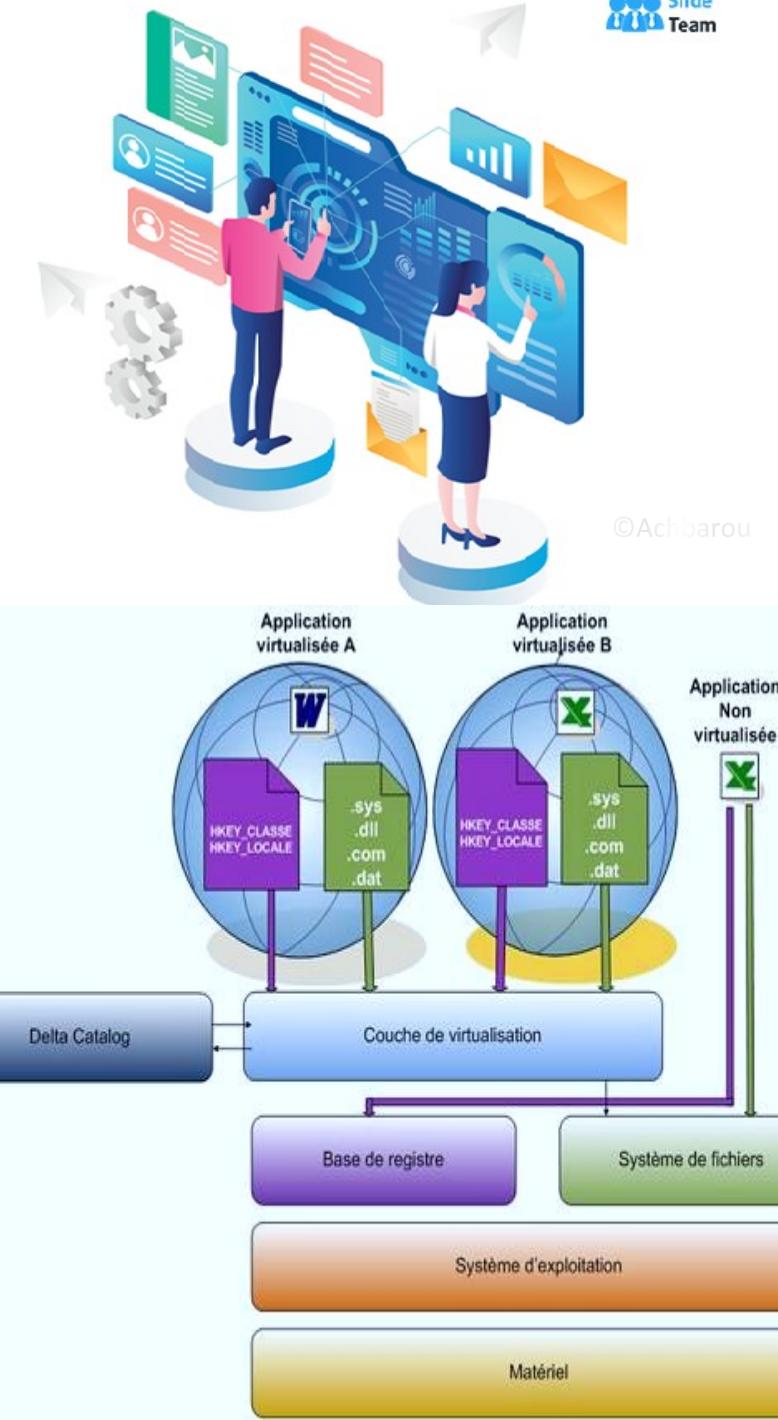
- Elle permet d'exécuter des **logiciels d'application** sans les installer directement sur le système d'exploitation de l'utilisateur.
- Cela fait référence à l'exécution d'une application sur un **client léger**; un terminal ou un poste de travail réseau avec peu de programmes résidents et accédant à la plupart des programmes résidant sur un **serveur connecté**. Le client léger s'exécute dans un environnement distinct, parfois appelé **encapsulé**, du système d'exploitation où se trouve l'application.
- Cette méthode diffère de la virtualisation complète du poste de travail (VDI)



Virtualisation d'applications

Il existe trois types de virtualisation d'applications :

- **Virtualisation d'application locale** : L'ensemble de l'application s'exécute sur le périphérique d'extrémité, mais dans un environnement d'exécution plutôt que sur le matériel natif.
- **Diffusion d'application en continu** : L'application réside sur un serveur qui envoie de petits composants du logiciel à exécuter sur l'appareil de l'utilisateur final lorsque cela est nécessaire.
- **Virtualisation d'application basée sur un serveur** : L'application s'exécute entièrement sur un serveur qui n'envoie que son interface utilisateur à l'appareil client.



Virtualisation des processeurs graphiques

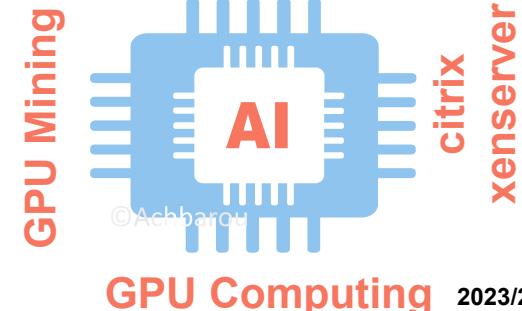
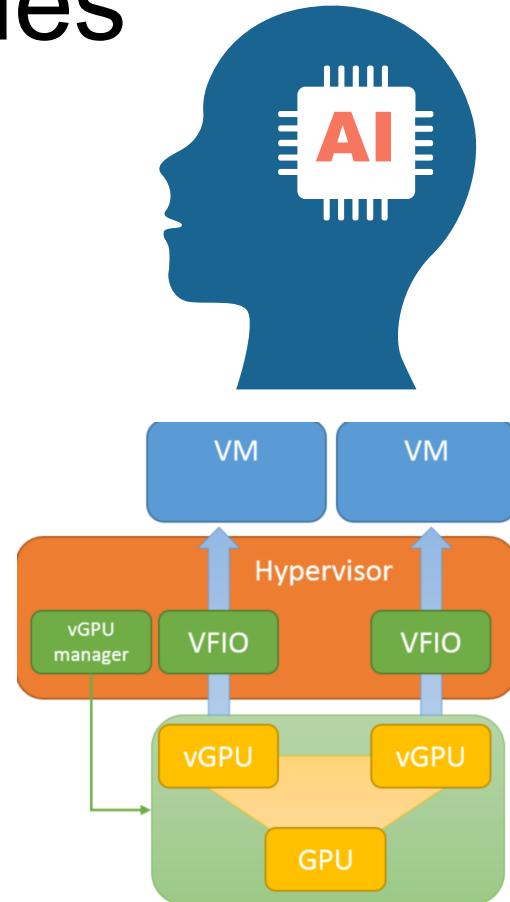
- Une **unité de traitement graphique** (ou processeur graphique, **GPU**) est un processeur multicœur spécifique qui améliore les **performances informatiques** globales en prenant en charge le **traitement graphique** ou **mathématique lourd**.

©Achbarou

- La virtualisation des processeurs graphiques permet à plusieurs machines virtuelles d'utiliser tout ou partie de la **puissance de traitement** d'un GPU pour **accélérer la vidéo, l'intelligence artificielle (IA)** et d'autres applications à forte **intensité graphique** ou mathématique.

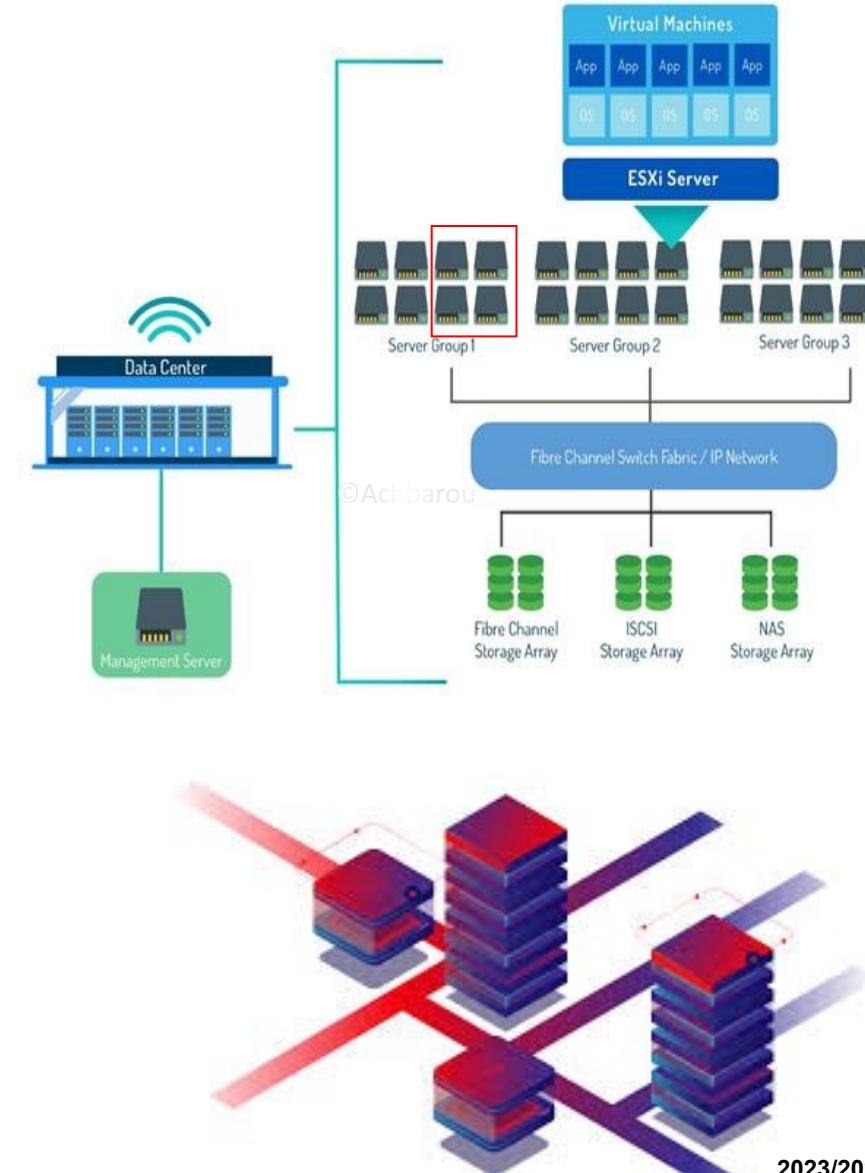
©Achbarou

- Les **GPU de type Pass-through** (à accès direct) mettent l'ensemble du GPU à la disposition d'un seul système d'exploitation invité.
- Les **GPU virtuels (vGPU) partagés** divisent les coeurs du GPU physique entre plusieurs GPU virtuels (vGPU) destinés à être utilisés par des machines virtuelles basées sur un serveur.



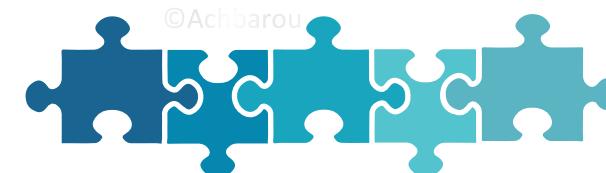
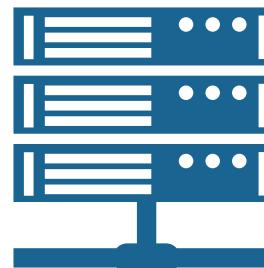
Virtualisation du centre de données (Datacenter)

- La virtualisation des centres de données est le processus de création d'un centre de **données moderne, hautement évolutif, disponible et sécurisé**.
- La virtualisation du centre de données transforme la majeure partie du matériel d'un **centre de données en logiciel**, ce qui permet à un administrateur de **diviser** un centre de données **physique unique** en **plusieurs centres de données virtuels** pour différents clients.
- Chaque client peut accéder à **sa propre infrastructure** sous forme de service (**IaaS**), qui fonctionne sur le même matériel physique sous-jacent.



Virtualisation des unités centrales

- Elle est la technologie fondamentale qui rend possible les **hyperviseurs**, les machines virtuelles et les systèmes d'exploitation comme une infrastructure virtuelle. Elle permet de **diviser** une unité centrale en plusieurs unités centrales virtuelles qui peuvent être utilisées par plusieurs machines virtuelles.
- Au début, la virtualisation des unités centrales était entièrement définie **par logiciel**, mais la plupart des processeurs actuels incluent des **jeux d'instructions étendus** qui prennent **en charge la virtualisation des unités centrales**, ce qui améliore les **performances des machines virtuelles**.



Virtualisation Linux

- KVM (Kernel-based Virtual Machine) est une technologie de virtualisation Open Source intégrée à Linux®. Avec KVM, vous pouvez transformer Linux en un **hyperviseur** qui permet à une machine hôte d'exécuter plusieurs environnements virtuels isolés.
- KVM convertit Linux en un **hyperviseur de type 1** (bare metal). Pour exécuter des machines virtuelles, tous les hyperviseurs ont besoin de certains composants au niveau du système d'exploitation : gestionnaire de mémoire, ordonnanceur, pile d'entrées/sorties (E/S), pilotes de périphériques, **gestionnaire de la sécurité**, pile réseau, etc

©Achbarou

©Achbarou



Prof. Omar ACHBAROU © ENSA Marrakech



2023/2024

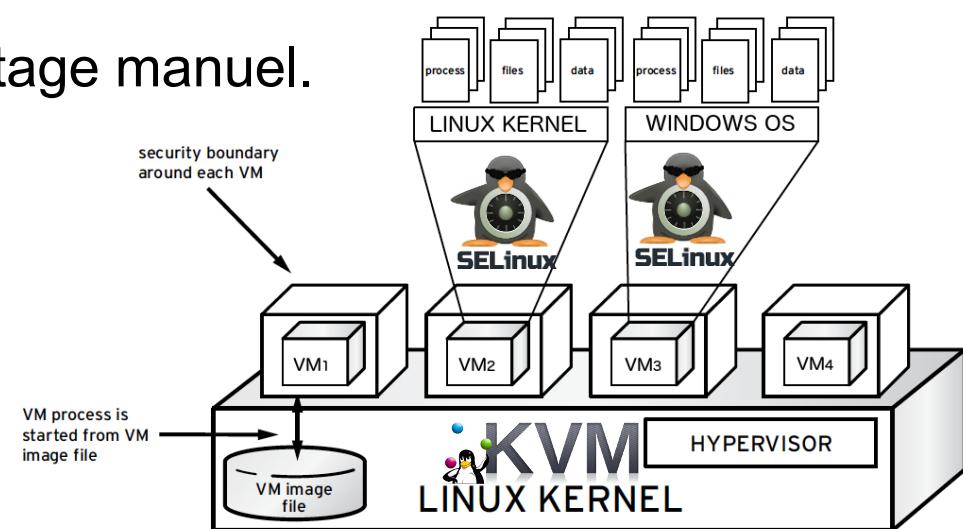
Virtualisation Linux : KVM et Sécurité

- KVM combine la technologie **SELinux (Security-Enhanced Linux)** et la **virtualisation sécurisée (sVirt)** pour renforcer la sécurité et l'isolement des machines virtuelles.
- **SELinux** établit des barrières de sécurité autour des machines virtuelles. La technologie **sVirt** étend quant à elle les capacités de SELinux, en vous permettant d'appliquer le mécanisme de **contrôle d'accès obligatoire (MAC)** aux machines virtuelles invitées et en évitant les erreurs d'étiquetage manuel.

©Achbarou

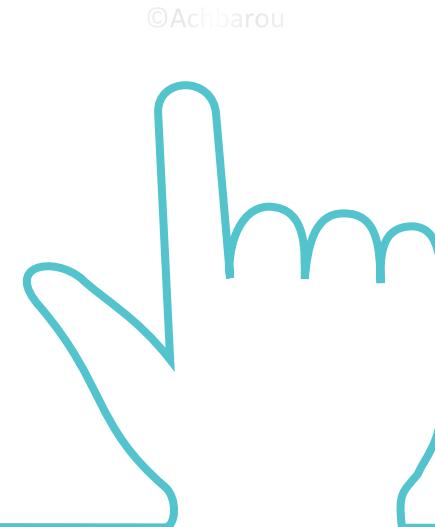
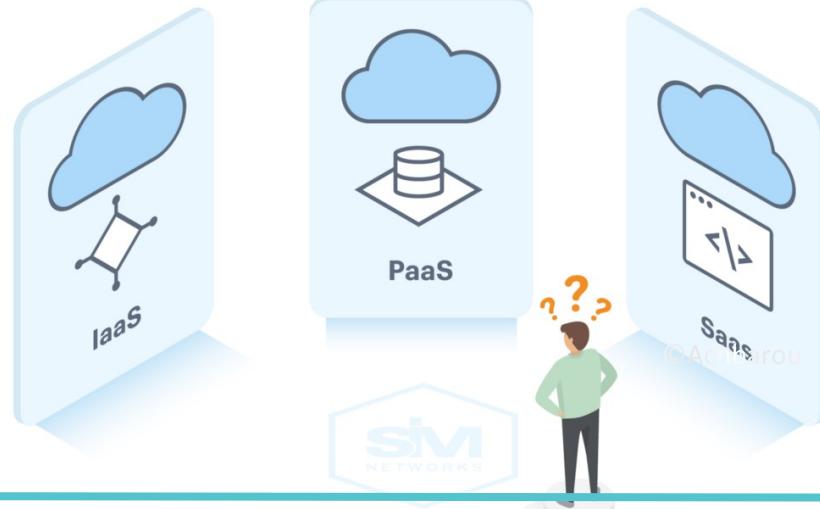
©Achbarou

©Achbarou



Virtualisation du cloud

- La **virtualisation** et le **Cloud Computing** sont deux technologies à ne pas confondre
- La plateforme de **cloud computing** repose sur la virtualisation.
- En virtualisant les **serveurs**, le **stockage** et d'autres **ressources physiques** du **centre de données**, les fournisseurs de cloud computing peuvent offrir toute un **modèle de services** aux clients **à la demande**.



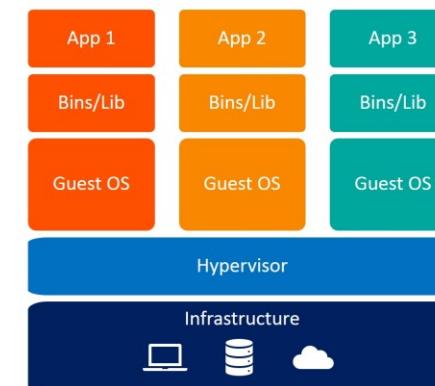
Virtualisation vs Conteneurs

- La notion de **conteneur** est aussi souvent rapprochée de celle de virtualisation. mais comme son nom l'indique, une **machine virtuelle** est l'imitation virtuelle d'un appareil informatique créée, dans le cadre de la virtualisation, à l'aide d'un logiciel **hyperviseur**, et doté d'un système d'exploitation (ou OS) complet.
- La virtualisation **par conteneurisation**, quant à elle, consiste à cloisonner directement au niveau du système d'exploitation. Ainsi, chaque conteneur exécute son environnement, mais partage le même OS hôte. C'est pour cette raison que les conteneurs servent généralement à la **virtualisation d'un programme**, et non d'un serveur dans son **intégralité**.

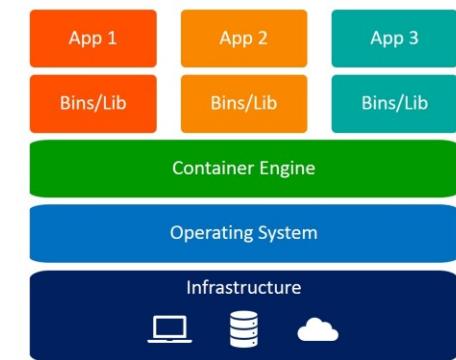
@Achbarou

@Achbarou

@Achbarou



Virtual Machines



Containers

Virtualisation et Sécurité

virtualization architecture & Security



Virtualisation et sécurité

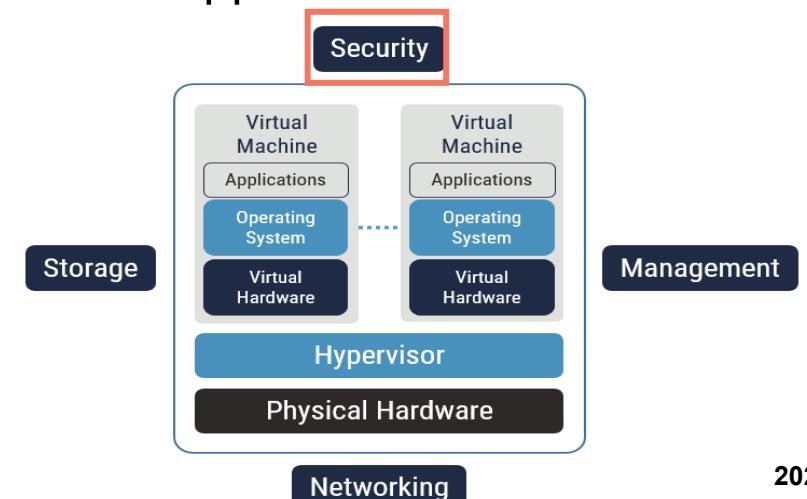
- La **sécurité virtualisée**, ou **virtualisation de la sécurité**, désigne les solutions de sécurité qui sont basées sur des logiciels et conçues pour fonctionner dans un environnement **informatique virtualisé**. Elle diffère de la sécurité réseau traditionnelle, basée sur le matériel, qui est statique et fonctionne sur des dispositifs tels que **les pare-feu, routeurs et commutateurs traditionnels**.

©Achbarou

- La **virtualisation** et la **sécurité** vont de pair, car la virtualisation présente des avantages inhérents en **matière de sécurité**. Par exemple, la virtualisation permet de stocker les données dans un **emplacement centralisé** plutôt que sur des appareils d'utilisateurs finaux **non approuvés** ou **non sécurisés**.

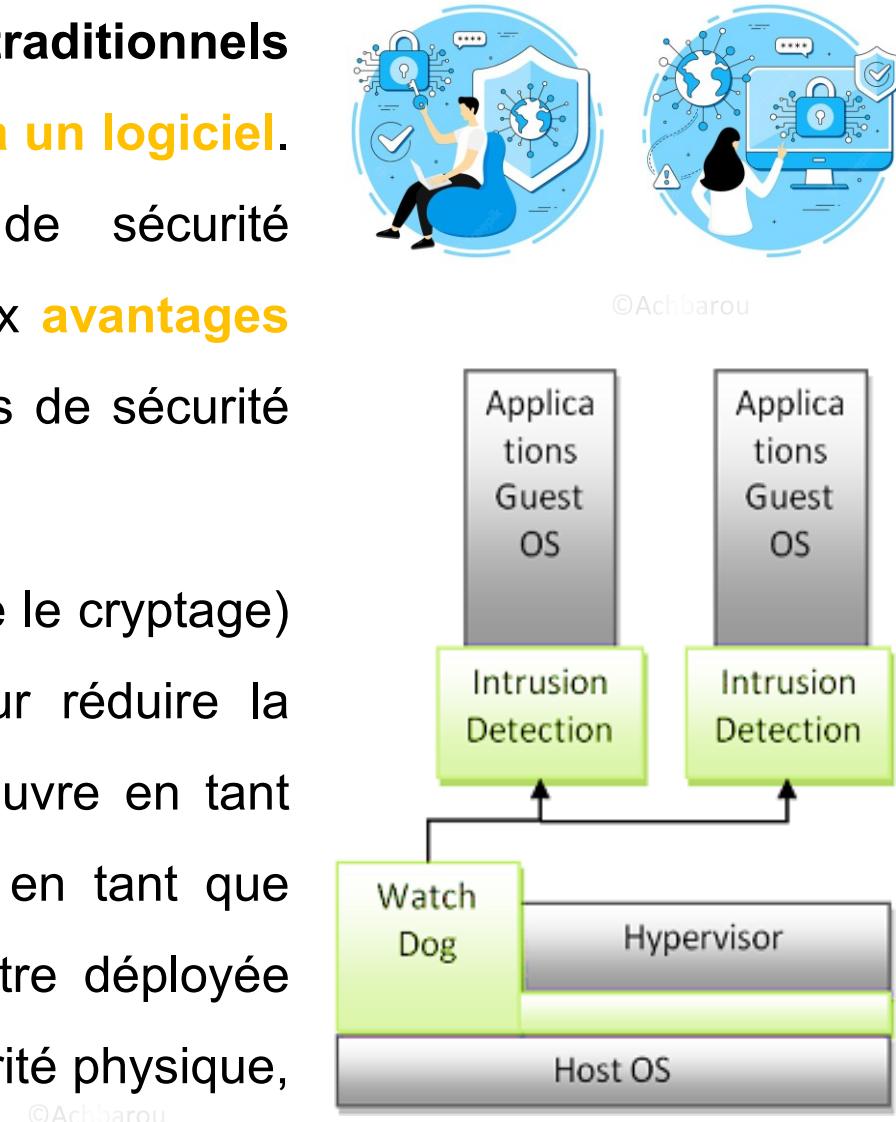
©Achbarou

©Achbarou



Virtualisation et sécurité

- La sécurité virtualisée peut prendre les composants de **sécurité traditionnels** (tels que les pare-feu et la protection antivirus) et les **déployer via un logiciel**. En outre, elle peut également exécuter des fonctions de sécurité supplémentaires. Ces fonctions ne sont possibles que grâce aux **avantages de la virtualisation**, et sont conçues pour répondre aux besoins de sécurité spécifiques d'un **environnement virtualisé**.
- Par exemple, on peut insérer des **contrôles de sécurité** (tels que le cryptage) entre la couche applicative et l'infrastructure sous-jacente pour réduire la **surface d'attaque**. La sécurité virtualisée peut être mise en œuvre en tant qu'application directement sur un **hyperviseur bare metal** ou en tant que **service hébergé** sur une VM. Dans les deux cas, elle peut être déployée **rapidement** là où elle est la plus efficace, contrairement à la sécurité physique, qui est liée à un dispositif spécifique.



Virtualisation et sécurité

- Les autres effets **positifs de la sécurité** de la virtualisation sont les suivants :
 - **Contrôle d'accès granulaire (Granular Access Control)**: Les équipes informatiques et les administrateurs ont beaucoup plus de contrôle sur l'accès au réseau qu'avec une infrastructure matérielle traditionnelle. Les équipes peuvent utiliser des **techniques de micro-segmentation** pour **accorder aux utilisateurs l'accès à des applications** ou des ressources spécifiques au niveau de la charge de travail.
 - **Isolation des applications** : le fait d'isoler les applications les unes des autres sur le réseau. **L'isolement des applications** permet de protéger les données **contre le partage** entre elles ou contre les **logiciels malveillants** ou les **virus** qui pourraient avoir infecté d'autres parties du système. L'isolation est souvent réalisée par la **Conteneurisation** et le **Sandboxing**.



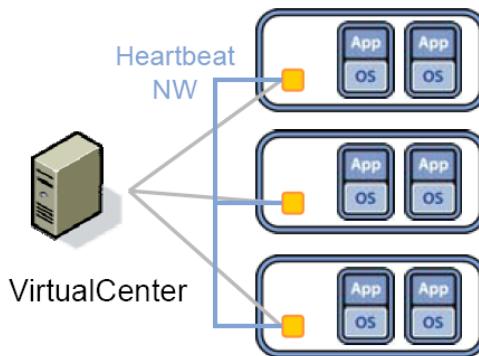
©Achbarou



©Achbarou

Virtualisation et sécurité

- Les autres effets positifs de la sécurité de la virtualisation sont les suivants :
 - **Isolation des machines virtuelles (VM)** : L'exécution de plusieurs machines virtuelles sur un seul serveur permet **un haut niveau d'isolation**. Si la sécurité est compromise dans un serveur, cette séparation assure la protection des autres serveurs virtuels.
 - **Isolation et segmentation du réseau** : Les charges de travail ou les applications indépendantes sur un réseau peuvent être divisées et partagées sur des réseaux virtuels **segmentés** qui sont **isolés** les uns des autres. Cela garantit que les informations et l'accès ne sont pas partagés sur l'ensemble du réseau.
 - **Maintenance des hyperviseurs** : Les hyperviseurs qui créent et exécutent les VM nécessitent généralement **moins de ressources** que les solutions matérielles, ce qui **réduit leur surface d'attaque**. De plus, les **hyperviseurs se mettent généralement à jour automatiquement**.



Les risques de la sécurité virtualisée ?

- Si la virtualisation présente plusieurs avantages en matière de sécurité, il existe également quelques problèmes de sécurité inhérents à la virtualisation dont vous devez être conscient :
 - **Vulnérabilités des réseaux locaux virtuels (VLAN)** : Lors de l'utilisation de VLAN, le trafic réseau est acheminé du tuyau vers un pare-feu, ce qui peut entraîner une latence du réseau. En outre, la communication entre plusieurs VM sur un VLAN ne peut pas être **inspectée**, ce qui la rend peu sûre.
 - **La prolifération des VM (VM Sprawl)** : se produit lorsqu'il y a des **VM inutilisées** et non comptabilisées présentes dans votre système. Les VM étant **très faciles à déployer**, de nombreuses équipes informatiques en créent un trop grand nombre, souvent à des fins de test, et **ne les suppriment pas** lorsqu'elles ne sont plus nécessaires. Les VM **inutilisées** sont souvent ignorées et **ne reçoivent pas de mises à jour de sécurité**, ce qui les laisse sans correctif et **vulnérables aux attaques**.

les risques de la sécurité virtualisée ?

- La **complexité accrue** de la sécurité virtualisée peut constituer un **défi** pour le service informatique, ce qui entraîne une **augmentation des risques**. Dans un environnement virtualisé, il est plus difficile de suivre les charges de travail et les applications qui migrent d'un serveur à l'autre, ce qui complique la surveillance **des politiques et des configurations de sécurité**.
©Achbarou
- De plus, la **facilité** avec laquelle on peut faire **tourner des machines virtuelles** peut également contribuer à **créer des failles de sécurité**.
- Cependant, que **nombre de ces risques** sont déjà présents dans un environnement virtualisé, que les services de sécurité **soient virtualisés ou non**. Le **respect des meilleures pratiques de sécurité** de l'entreprise (**Normes et Standards**) peut contribuer à atténuer ces risques.
©Achbarou

Les risques de la sécurité virtualisée ?

- **Attaques DDoS** : Indépendamment de leur isolement, les VM fonctionnant sur le même serveur **partagent les ressources** de ce serveur (par exemple, CPU, RAM et mémoire). Si une attaque DDoS inonde une machine virtuelle de trafic malveillant pour compromettre ses performances, les **autres machines virtuelles** du serveur en **ressentiront les effets**.
©Achbarou
- **Attaques d'hyperviseurs** : Si les **hyperviseurs** ont des **surfaces d'attaque** relativement réduites, ils peuvent néanmoins être compromis. Si un **hyperviseur** est **attaqué avec succès**, toutes les VM fonctionnant sur le même serveur sont en danger. Cela donne aux attaquants un point **d'accès centralisé à cibler**. En outre, les administrateurs d'hyperviseurs supervisent leurs informations **d'identification de sécurité**, ce qui signifie qu'un initié malveillant pourrait **partager ces informations d'identification** avec n'importe qui.
©Achbarou

References Bibliographies

References

1. <https://www.techno-science.net/glossaire-definition/Virtualisation.html>
2. <https://www.alamyimages.fr/photos-images/virtualization-vector-vectors.html?sortBy=relevant>
3. <https://www.ibm.com/fr-fr/cloud/learn/virtualization-a-complete-guide>
4. <https://www.vmware.com/solutions/virtualization.html>
5. <https://www.parkplacetechologies.com/blog/what-is-hypervisor-types-benefits/>
6. <https://www.vmware.com/fr/topics/glossary/content/hypervisor.html>
7. <https://www.pluralsight.com/blog/it-ops/what-is-hypervisor>
8. <https://www.vmware.com/fr/topics/glossary/content/hypervisor.html>
9. <https://www.ibm.com/topics/hypervisors>
10. <https://www.vmware.com/fr/topics/glossary/content/desktop-virtualization.html>
11. <https://www.vmware.com/topics/glossary/content/network-virtualization.html>
12. <https://www.datacore.com/fr/storage-virtualization/>
<https://www.lebigdata.fr/data-virtualization>
13. <https://www.redhat.com/fr/topics/virtualization/what-is-KVM>
14. <https://www.fosslinux.com/48755/top-opensource-virtualization-software-for-linux.htm>
15. <https://www.quadbridge.com/knowledge-center-fr/en-quoi-consiste-la-virtualisation-dun-centre-de-donnees>
16. <https://www.appvizer.fr/magazine/services-informatiques/virtualisation/type-virtualisation>
17. <https://www.liquidweb.com/blog/virtualization-security/>



THANK YOU





Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation
Ecole Nationale des Sciences Appliquées de Marrakech - Université Caddi Ayyad
Génie Cyber-Défense et Systèmes de Télécommunications Embarqués



Introduction à la Virtualisation

**Module M45 – Virtualisation, Cloud Computing,
SDN et sécurité**

Prof. Omar ACHBAROU

2023/2024

o.achbarou@uca.ma