

Partie 1 : Virtualisation et Stockage

Yaya DOUMBIA

Consultant supervising associate Cyber Risk & Security

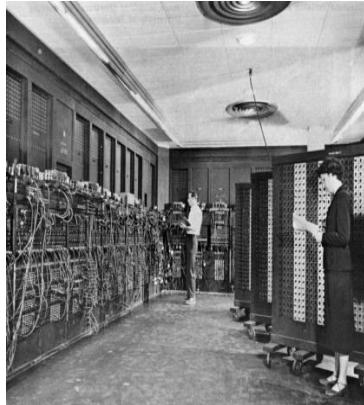
yaya.doumbia@intervenants.efrei.net

Introduction à la virtualisation

Les évolutions de la technologie de l'information

1945-1980

Main frame



Calcul
Numérique

1980-1995

Personal Computer



Traitement de
l'information

1995-2010

Internet



Partage de
l'information

2010-

Cloud Computing

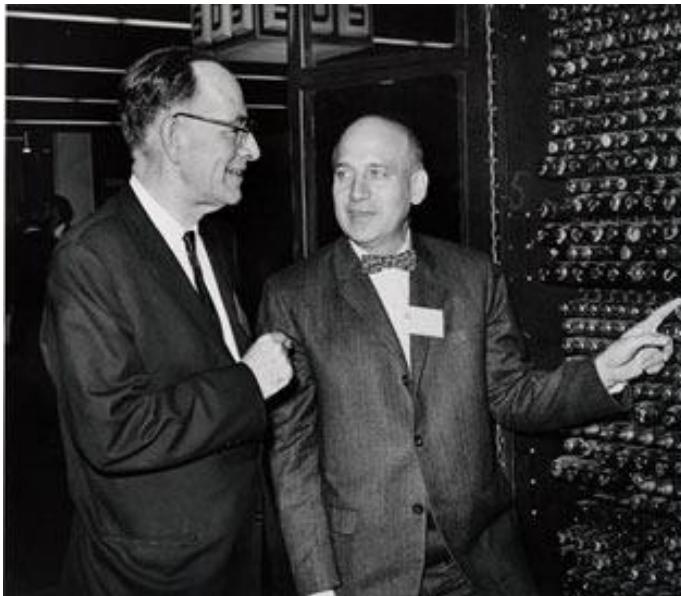


Interaction de
l'information
Mobile Internet
IOT
Big Data

Les évolutions de la technologie de l'information

□ Main Frame

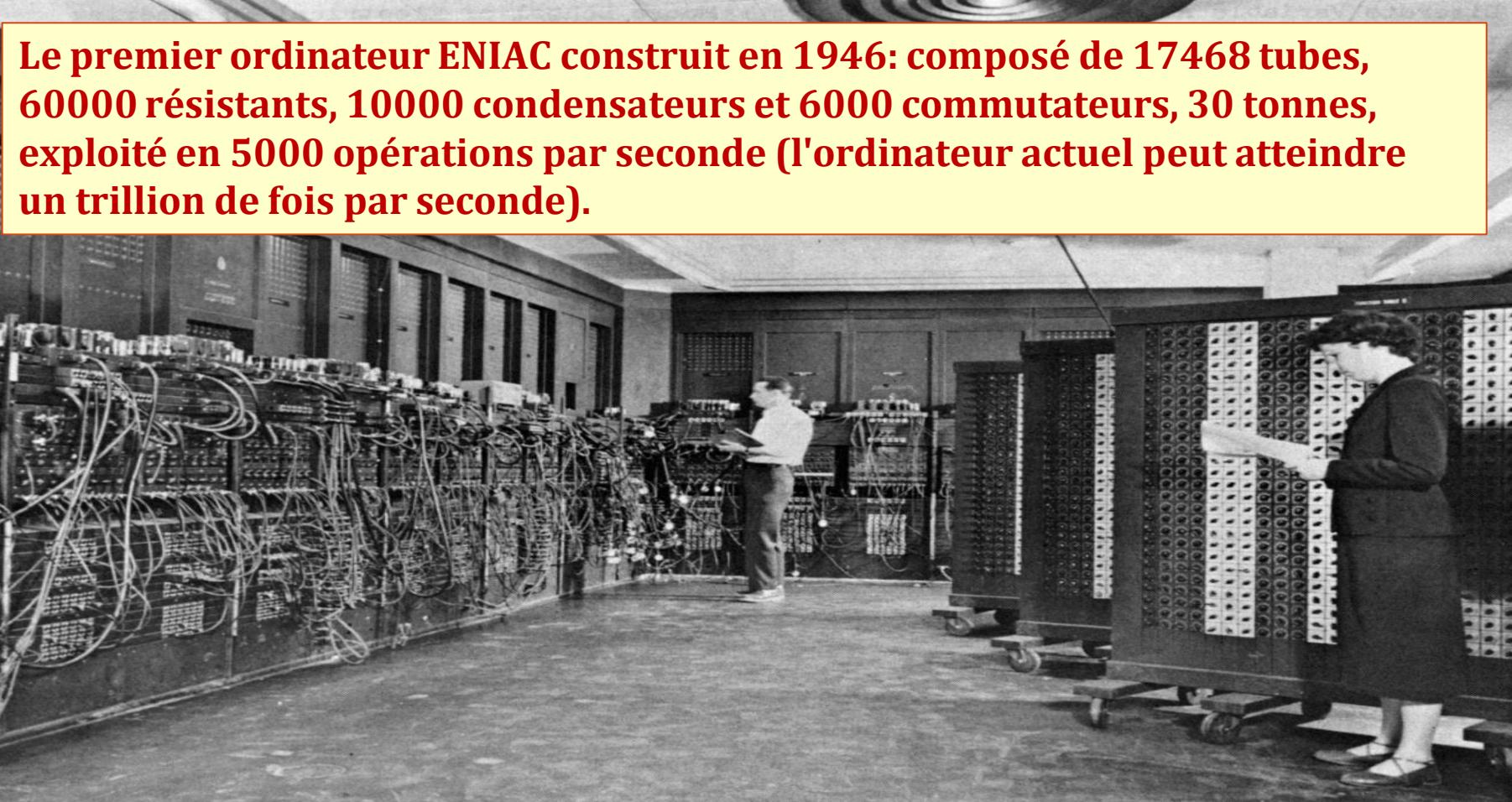
- Au cours de la 2^{ème} guerre mondiale, **Eckert** et **Mauchly** de l'Université de Pennsylvanie ont dirigé une équipe pour produire une machine pour faire le calcul complexe.



John W. Mauchly et
J. Presper Eckert

Les évolutions de la technologie de l'information

□ Main Frame



Le premier ordinateur ENIAC construit en 1946: composé de 17468 tubes, 60000 résistants, 10000 condensateurs et 6000 commutateurs, 30 tonnes, exploité en 5000 opérations par seconde (l'ordinateur actuel peut atteindre un trillion de fois par seconde).

Les évolutions de la technologie de l'information

□ Main Frame

- **Début:**
 - 1946 : le nouvel âge de l'ordinateur
- **Application**
 - Calcul de la recherche et champ de défense

Père de l'ordinateur



John Von Neumann

Les évolutions de la technologie de l'information

□ Personal Computer

- **Début:**
 - 1983 : IBM annonce PC / XT
 - Système Microsoft DOS
 - Inspur produit 0520 PC



Ère de la civilisation Humaine

Les évolutions de la technologie de l'information

□ Internet

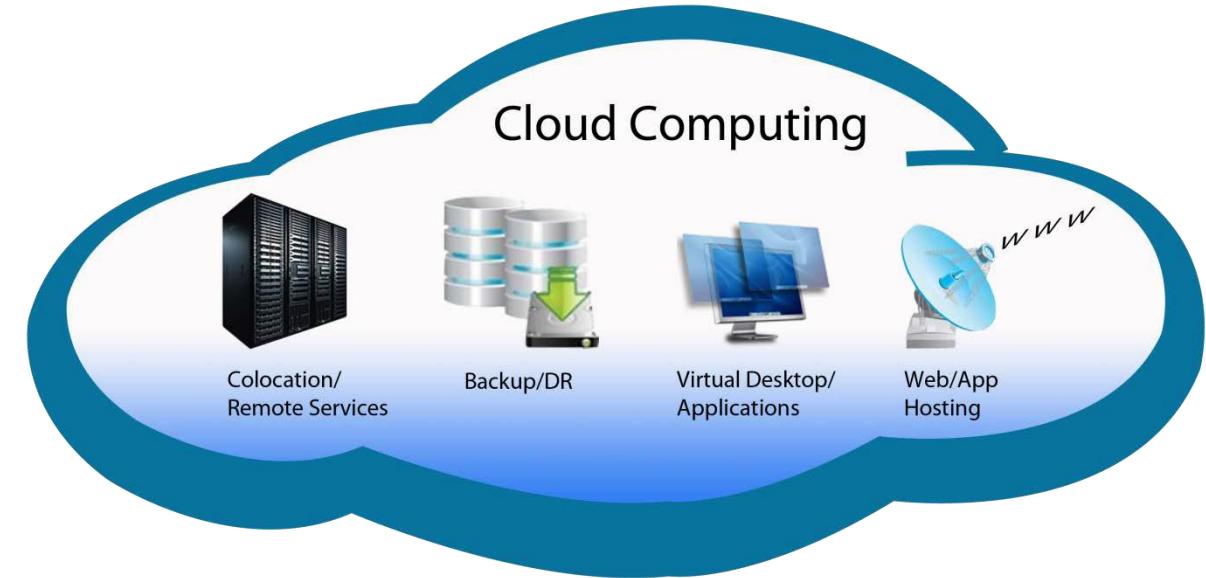
- **Début:**
 - Fin des années 1990
- **Applications:**
 - Email, Gateway Web Page, E-commerce, etc.
 - Démarrage d'une construction à grande échelle



Les évolutions de la technologie de l'information

□ Cloud Computing

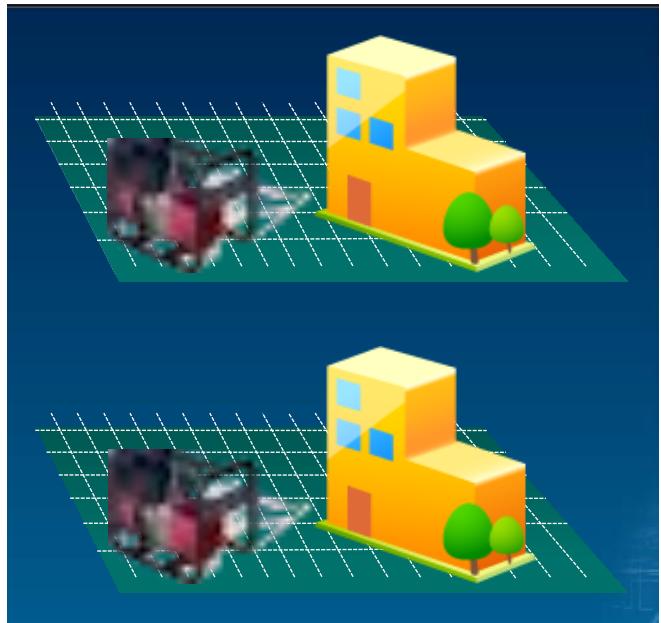
- **Début:**
 - 2010
- **Applications:**
 - Recherche robuste,
 - connectivité sociale,
 - Big Data,
 - IoT,
 - Villes intelligentes (Smart Cities).



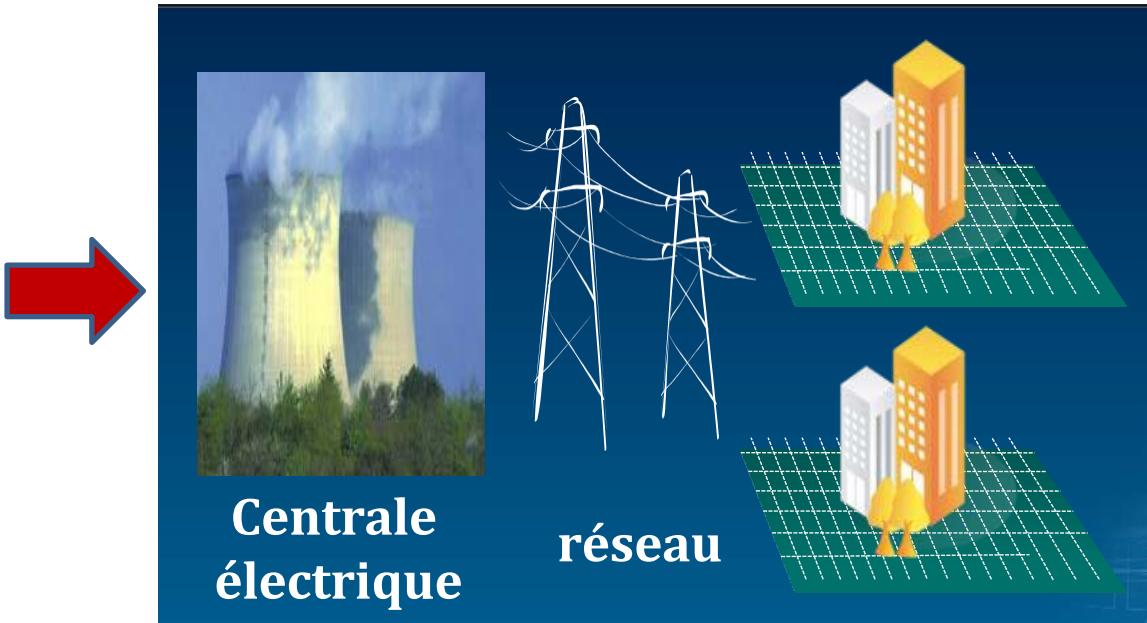
Les évolutions de la technologie de l'information

□ Cloud Computing

Groupe électrogène individuel



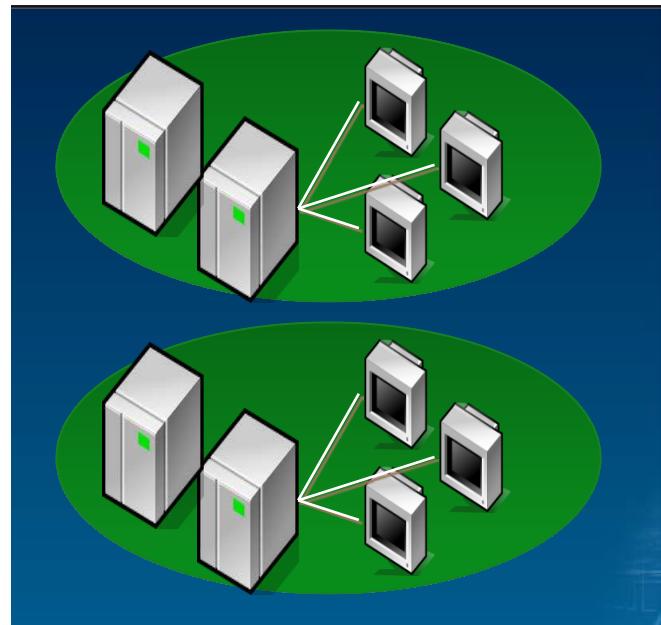
Alimentation centralisée



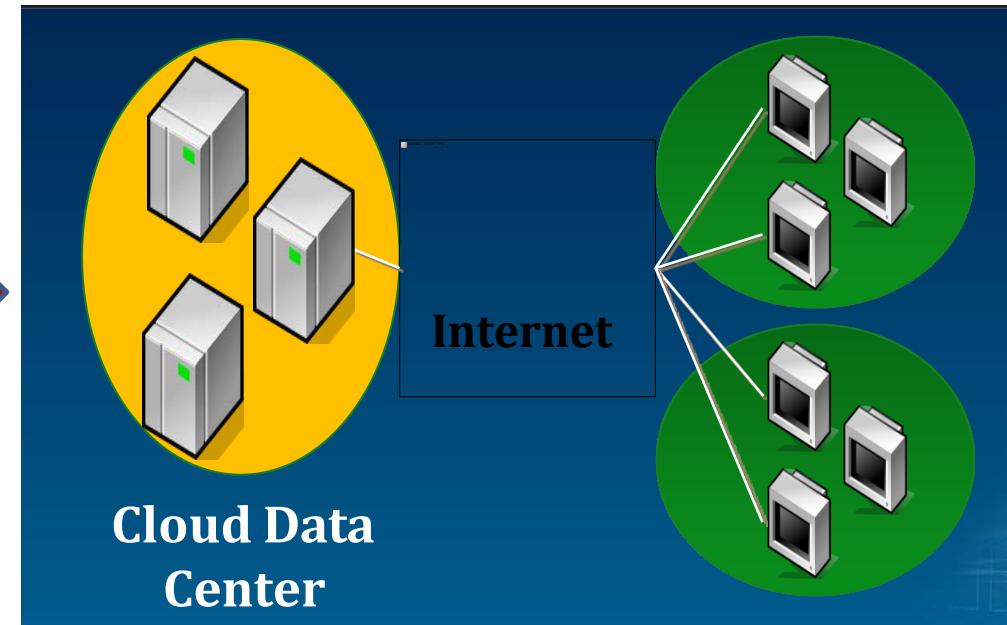
Les évolutions de la technologie de l'information

□ Cloud Computing

Individual
Computing System



Cloud Center Provides Services



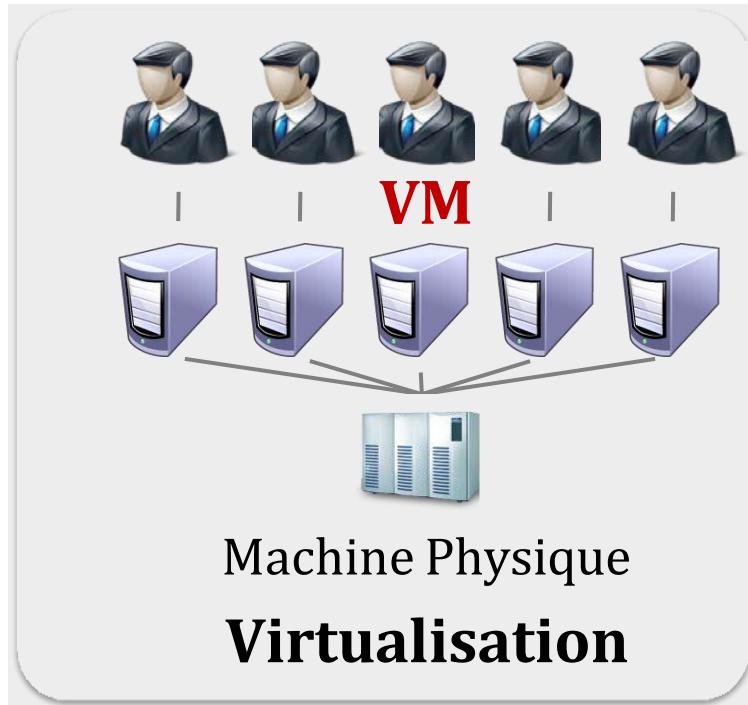
La tendance :

Cloud sera l'infrastructure de base

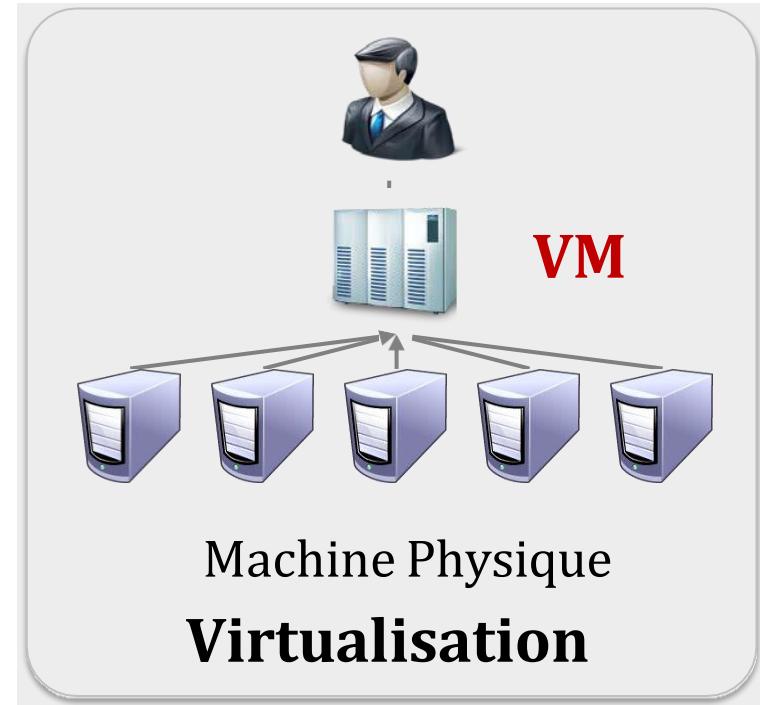
Les évolutions de la technologie de l'information

❑ Technologies clés du cloud computing

Virtualisation- “1 to many”

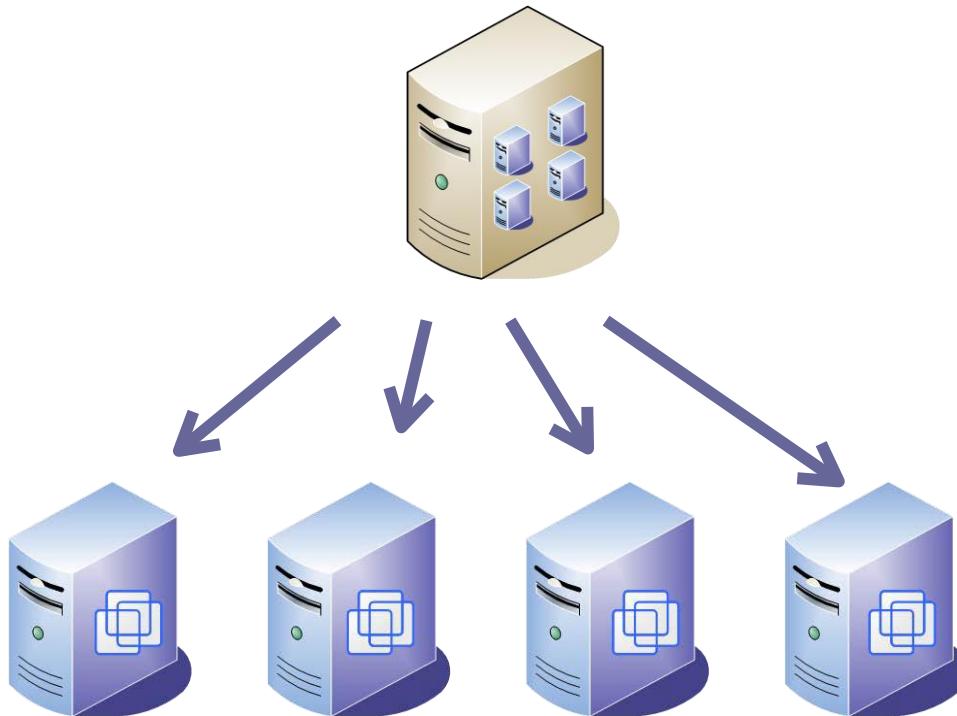


Virtualisation- “many to 1”



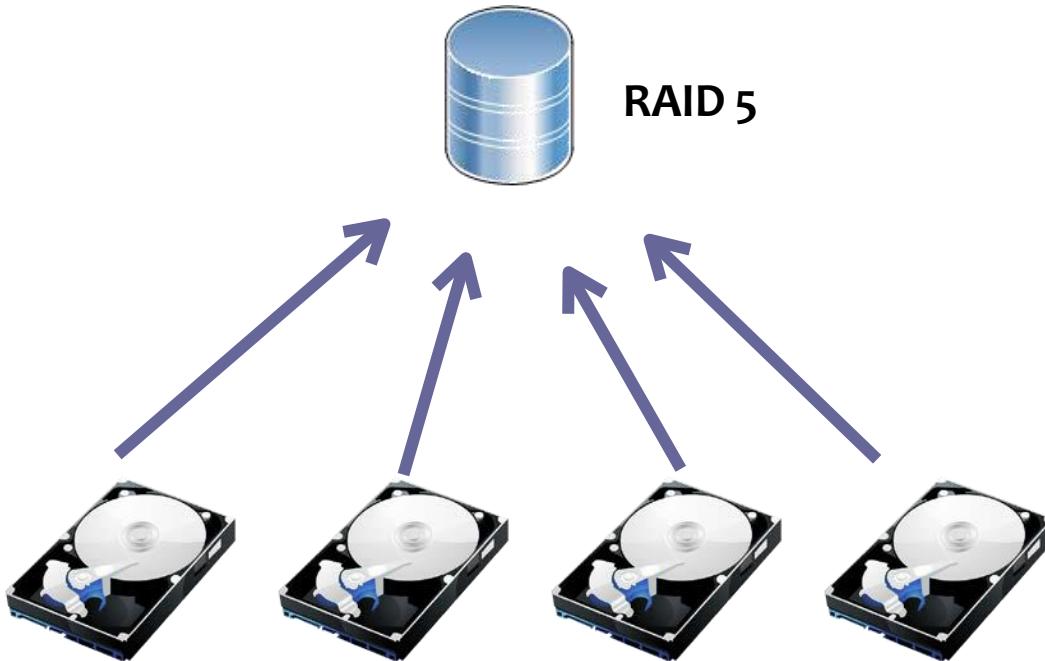
Introduction

Un élément physique, N éléments logiques



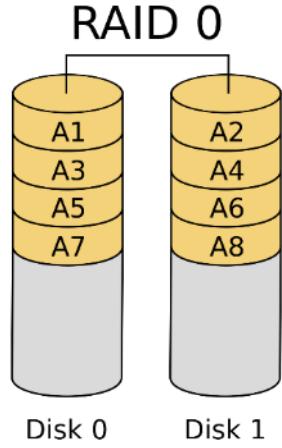
Introduction

□ N éléments physiques, Un élément logique

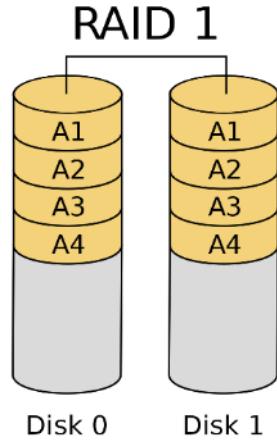


Le **RAID (Redundant Array of Independent Disks)** est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

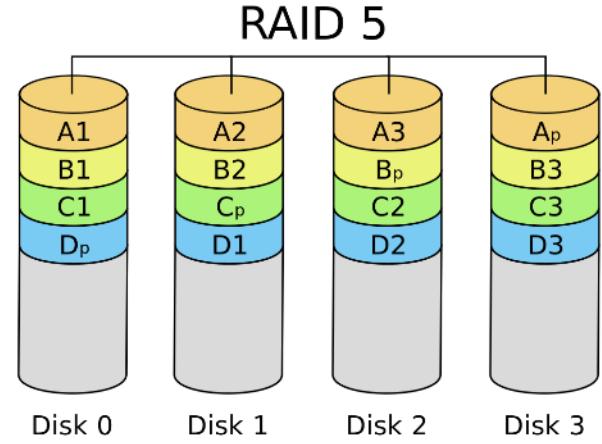
Introduction



Capacité : somme de toute la capacité du disque
Fiabilité : la perte d'un disque entraîne la perte de toutes les données



Capacité : taille du plus petit disque
Fiabilité : les données sont disponibles tant qu'au moins un disque est disponible



Capacité : somme de toute la capacité du disque moins 1
Fiabilité : la perte d'un disque peut être récupérée

Introduction

- **Virtualisation:** terme qui était encore absent du dictionnaire
- **Proposition de définition:**

Abstraction des couches physiques d'un élément de l'infrastructure informatique

- **Un** élément physique apparaît comme **plusieurs** éléments logiques
- **Plusieurs** éléments physiques apparaissent comme **un** élément logique

Définitions

□ Définition (Wikipédia):

*La **virtualisation** est l'ensemble des techniques **matérielles** et **logicielles** permettant de fournir un ensemble ou sous-ensemble de ressources informatiques de manière qu'elles puissent être utilisées, avec avantages, de manière indépendante de la plateforme matérielle (configuration, localisation).*

- L'objectif de la **virtualisation** est de se libérer au maximum de la couche matérielle de l'informatique.
- La **virtualisation** permet de changer exactement l'approche de l'informatique en repoussant les limites du matériel.

Définitions

□ Définition (Redhat):

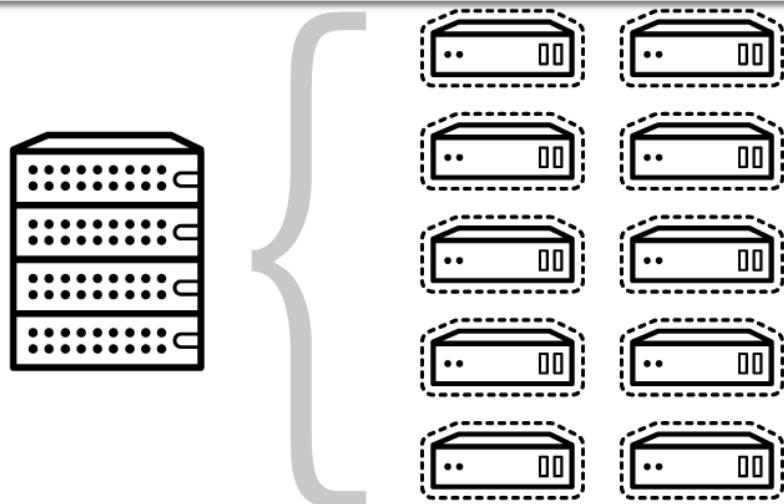
La virtualisation est une technologie qui vous permet de créer plusieurs environnements simulés ou ressources dédiées à partir d'un seul système physique.

- Le logiciel, appelé **hyperviseur**, est directement relié au matériel et permet de fragmenter ce système unique en plusieurs environnements sécurisés distincts.
 - C'est ce que l'on appelle les **machines virtuelles**, ou VM.
- Les VMs reposent sur la capacité de l'**hyperviseur** à émuler les ressources de la machine physique et à les distribuer de manière appropriée.



Définitions

- La machine physique originale équipée de l'hyperviseur s'appelle l'**hôte**, tandis que les nombreuses machines virtuelles qui utilisent ses ressources sont appelées **invités**.
- Les invités traitent les ressources informatiques (CPU, mémoire et stockage) comme un dépôt de ressources qui peuvent facilement être relocalisées.



Virtualisation et stockage

Origines de la virtualisation

- Les premiers serveurs virtualisés (ou plutôt partitionnés) sont les mainframes (Z-series), dans les années 80.
- Le principe d'un Mainframe est de posséder une très grosse capacité de calcul et de la partager.
- La facturation se fait à la consommation de MIPS.
- Le mainframe intègre
 - La gestion de partitions totalement isolées
 - Le load balancing sysplex pour la haute disponibilité
 - Le fail-over, pour les PRA (Plan de Reprise d'Activité)
- La gestion des partitions, le partage des ressources communes, est assurée par le microcode du mainframe

MIPS (Million d'instructions par seconde) : unité de mesure des processeurs



- Z10/Z11
 - 2 tonnes
 - 6 m² x 2m
 - 28KWh
 - Environ 256 CPU x 4 Cores @ 5GHz
 - 100.000 VM0

Origines de la virtualisation

- Le partitionnement s'est poursuivi sur les grands systèmes UNIX comme les P-Series qui ont des centaines de CPU activable sur un même OS ou attribuable à des partitions (LPAR)
- Les partitions sont Logiques et les CPU peuvent être réservés, partagés, priorisés.
- La gestion des **ressources partagées** est, là aussi, appuyé par un sous système intégré à la plateforme, directement dans le hardware.



LPAR (Logical PARtition): ou système de partitionnement logique, est un sous-ensemble des ressources matérielles de l'ordinateur apparaissant comme un serveur distinct. En effet, une machine physique peut être partitionnée en plusieurs LPAR, chacune possédant son propre système d'exploitation.

- Power
 - 70 Kg
 - 17/48/86 cm (4u)
 - 1.6KWh
 - Environ 8 CPU x 8 Cores @ 3.8GHz
 - Environ 300 VM

Origines de la virtualisation

- Enfin, avec la montée en puissance des systèmes X (x86), le besoin de virtualisation est apparu.
- Dans les années 2000 apparaît VMWare aujourd'hui leader dans ce domaine, sur cette plateforme.
- Le principe :
 - Avoir sur un système hôte un programme permettant de **simuler** de **façon logicielle** des systèmes hardware virtuels.
 - **Simule** des processeurs, de la mémoire, des périphériques tels que les disques durs, carte réseau, carte graphique...



- Intel (x86) - Blade
 - Environ 100 Kg
 - Rack 7U
 - 1.4KWh
 - 6 Lames < 4 CPU < 4 Core = 96 Cores
 - 200 VM

Quelle est la différence entre la virtualisation et le cloud computing ?

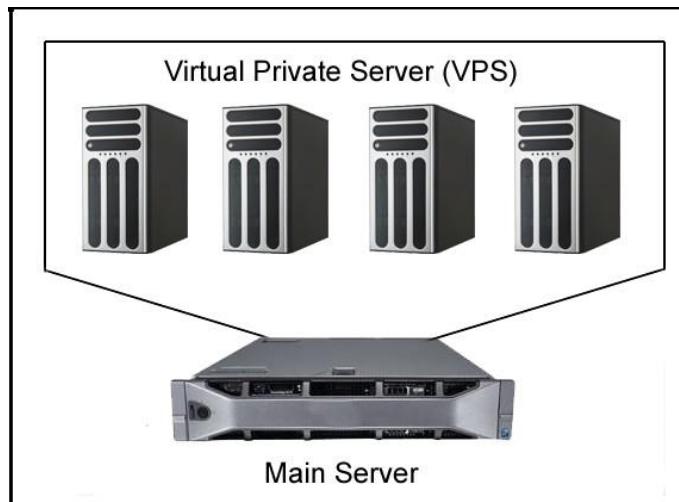
- Il est facile de confondre ces deux concepts, notamment parce qu'ils reposent sur le même principe, à savoir isoler les ressources du matériel afin de créer un environnement optimal.
- Toutefois, il ne s'agit pas de la même chose :
 - La virtualisation est une technologie qui sépare les fonctions du matériel.
 - Le cloud computing s'apparente davantage à une solution qui repose sur cette séparation.
- Bien que la virtualisation contribue à la création de clouds, elle ne peut pas être assimilée au cloud computing.

Quelle est la différence entre la virtualisation et le cloud computing ?

- Le NIST (National Institute of Standards and Technology) définit le cloud computing selon 5 caractéristiques :
 - un réseau,
 - des ressources regroupées en pools,
 - une interface utilisateur,
 - des fonctions d'approvisionnement ainsi que l'allocation
 - et le contrôle automatiques des ressources.
- Même si la virtualisation permet de créer le réseau et de regrouper les ressources dans des pools, des logiciels supplémentaires de gestion et de système d'exploitation sont nécessaires pour créer une interface utilisateur, approvisionner les VM et contrôler ou allouer les ressources.

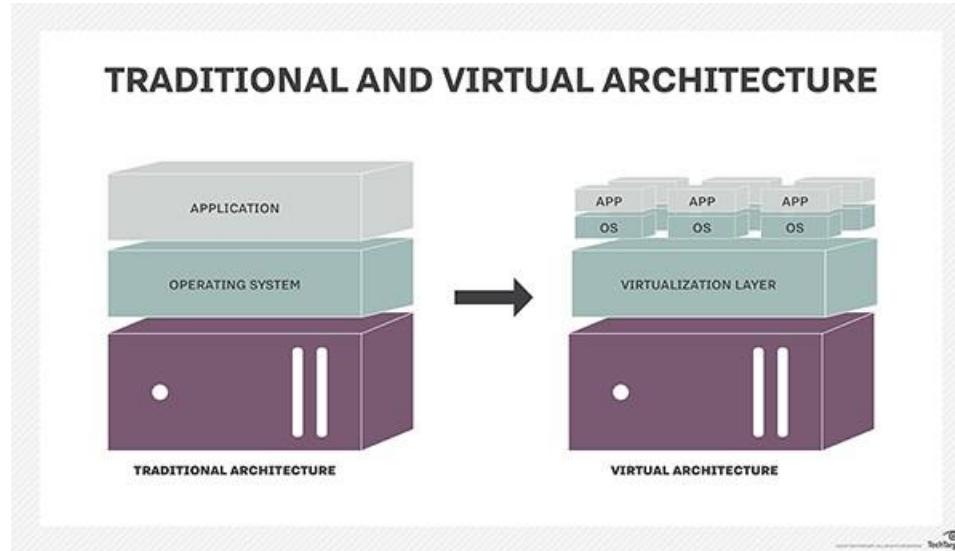
Principe de la virtualisation

- La **virtualisation** est une couche d'abstraction qui découpe le **système d'exploitation** du matériel afin de délivrer une meilleure utilisation et flexibilité des ressources de traitement.
- Les ordinateurs virtuels sont appelés serveur privé virtuel (**Virtual Private Server** ou **VPS**) ou encore environnement virtuel (**Virtual Environment** ou **VE**).



Principe de la virtualisation

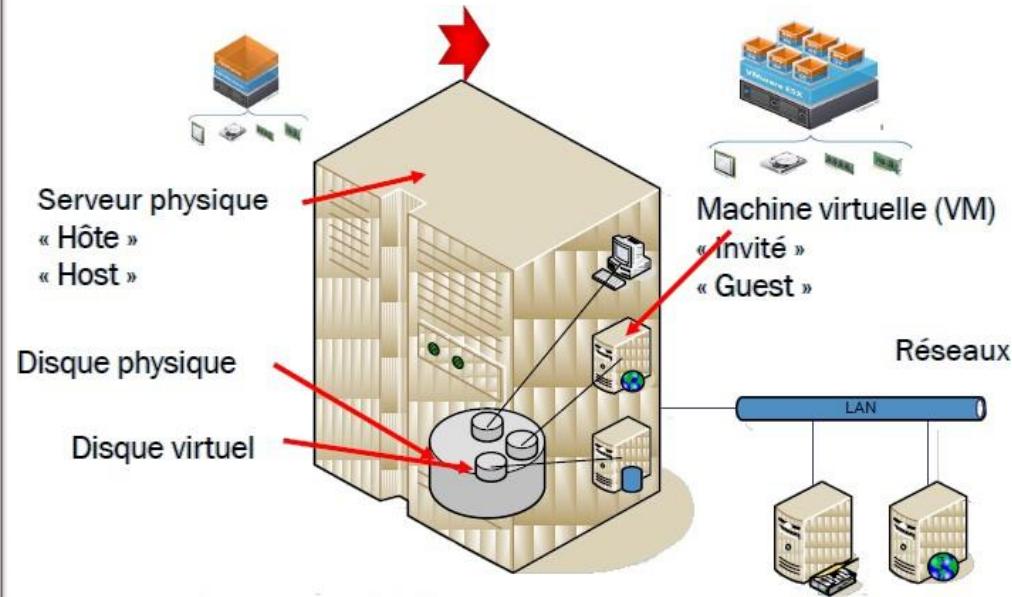
- Une utilisation clé de la technologie de virtualisation est la virtualisation du serveur, qui utilise une couche de logiciel appelée **hyperviseur** pour imiter le matériel sous-jacent.
 - Cela comprend souvent la mémoire de la CPU, les E / S et le trafic réseau.
- L'SE invité, qui interagit normalement avec du matériel réel, le fait maintenant avec une émulation de logiciel de ce matériel et, souvent, le SE invité n'a aucune idée du matériel virtualisé.



Principe de la virtualisation

- La **virtualisation** permet de faire fonctionner plusieurs systèmes d'exploitation et/ou plusieurs applications sur une même machine, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.

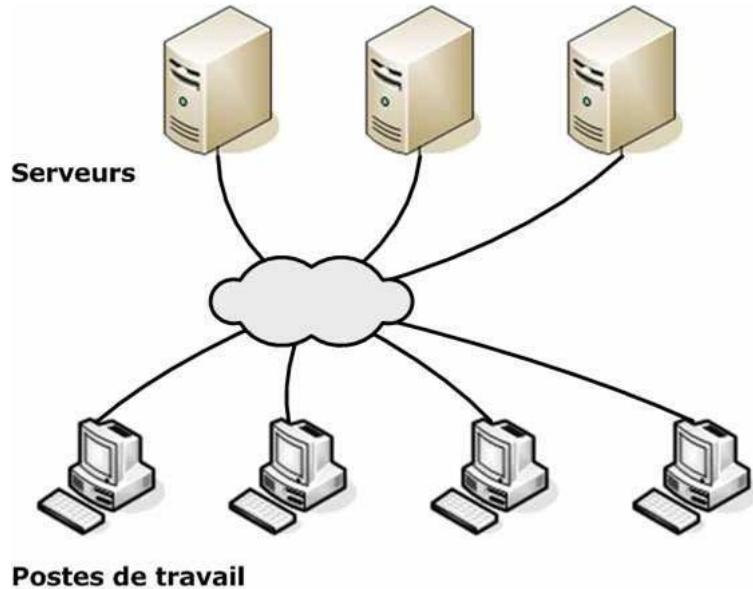
- On parle de :
 - **Machine hôte** : machine exécutant les différents systèmes virtuels
 - **Machine invitée** : machine virtuelle s'exécutant dans l'environnement de virtualisation



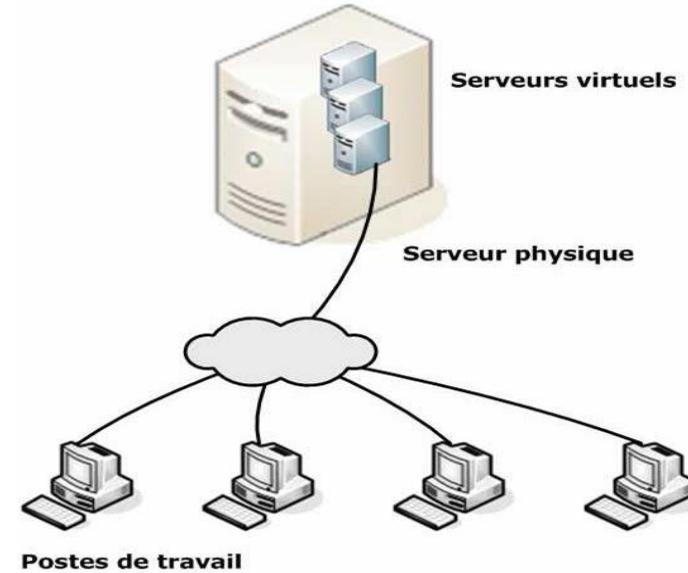
Principe de la virtualisation

- Le **principe** de la virtualisation est donc un principe de **partage** : les différents systèmes d'exploitation se partagent les ressources du serveur.

Architecture traditionnelle



Architecture virtualisée

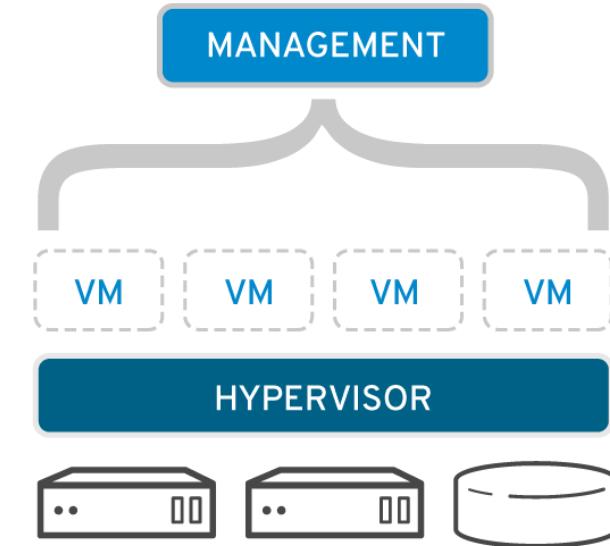


Trois serveurs différents sollicités par un ensemble de postes de travail.

Un Serveur au lieu de trois. L'administration de ces trois serveur est centralisée et l'utilisation des ressources physiques est optimisée

Comment les VMs sont-elles gérées

- Le logiciel de gestion de la virtualisation est conçu pour bien rendre la virtualisation plus facile à gérer.
 - On peut allouer manuellement des ressources dans des VMs, les créer dans des serveurs, les tester et installer des correctifs au besoin. Mais diviser des systèmes individuels en des centaines, il faut multiplier le travail nécessaire pour que ces systèmes soient exécutés, à jour et sécurisés.



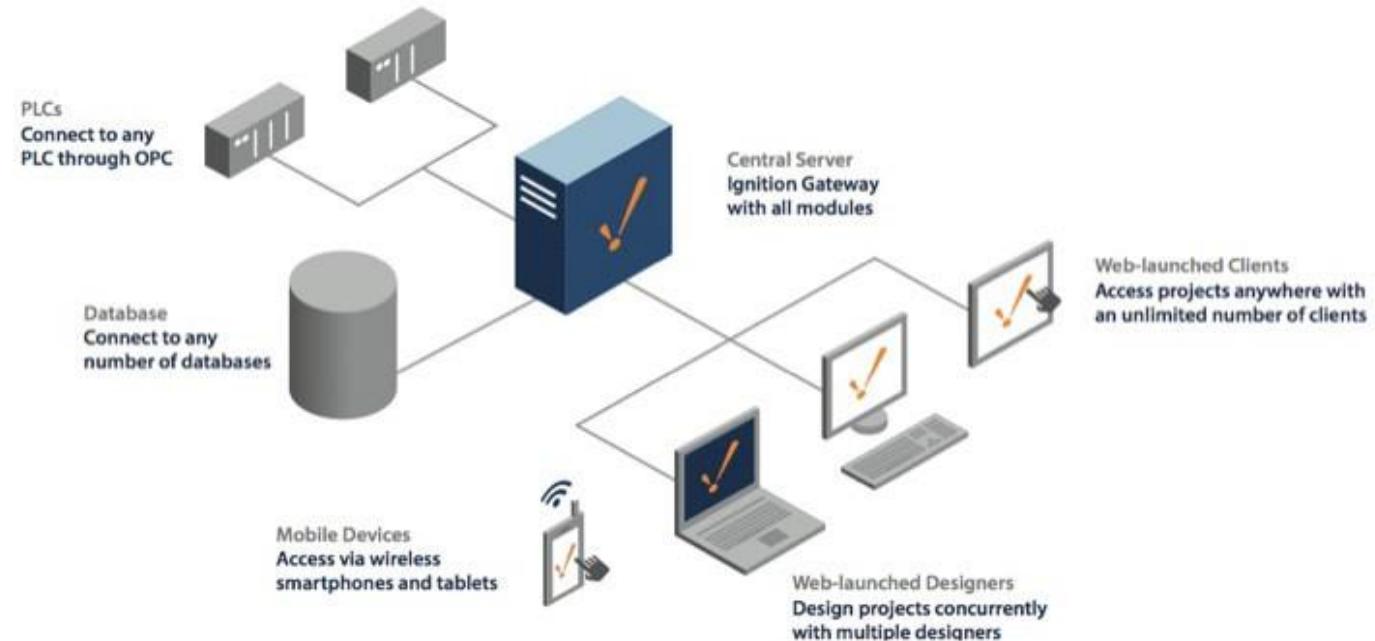
Comment les VMs sont-elles gérées

- Si toutes les machines virtuelles sont liées à un système de surveillance, de provisionnement ou d'outil de gestion, les systèmes peuvent être migrés automatiquement vers un matériel mieux adapté pendant les périodes d'utilisation ou de maintenance maximale.
- Chaque système de gestion de la virtualisation est unique, mais la plupart comportent une interface utilisateur non compliquée, rationalisent le processus de création de la VM, surveillent l'environnement virtuel, allouent des ressources, compilent des rapports et appliquent automatiquement les règles.

Terminologie de base

Qu'est-ce qu'un serveur ?

- Un serveur (au sens logiciel) est un programme informatique qui « *rend service* » à plusieurs ordinateurs en réseau par:
 - le stockage, le partage, l'échange de dossiers, de données ou de ressources comme des imprimantes ou fax par exemple..



Différents rôles serveur

- Un serveur peut avoir plusieurs rôles :
 - Contrôleur de nom de domaine (DNS)
 - Serveur de fichiers - FTP
 - Un serveur DHCP (Dynamics Host Configuration Protocol)
 - Un serveur passerelle (Gateway server)
 - Un serveur d'impression
 - Un serveur Proxy (mandataire d'accès)
 - Un serveur de streaming (diffusion)
 - Un serveur de sauvegarde
 - Un serveur HTTP (Web)
 - Un serveur d'application
 - Un serveur de messagerie (Pop / Imap / Mime / SMTP)

Principe de partage de serveur

- Un serveur est un ordinateur utilisé à distance depuis différents postes de travail, ou autres périphériques.
- Un serveur possède des ressources matérielles, principalement CPU, mémoire, disques et interfaces réseau.
- Les ressources d'un serveur sont utilisées par des applications, non pas de manière directe, mais en s'appuyant sur un système d'exploitation.

- La virtualisation de serveurs est un ensemble de techniques et d'outils permettant de faire tourner plusieurs systèmes d'exploitation sur un même serveur physique.
- Le principe de la virtualisation est donc un principe de ***partage*** : les différents systèmes d'exploitation se partagent les ressources du serveur.

Principe de partage de serveur

- Pour être utile de manière opérationnelle, la virtualisation doit respecter deux principes fondamentaux :
 - **Le cloisonnement (ou l'isolation)** : chaque système d'exploitation a un fonctionnement indépendant, et ne peut interférer avec les autres en aucune manière.
 - **La transparence** : le fait de fonctionner en mode virtualisé ne change rien au fonctionnement du système d'exploitation et à fortiori des applications.

Principe de partage de serveur

- La **transparence** implique la **compatibilité**: toutes les applications peuvent tourner sur un système virtualisé, et leur fonctionnement n'est en rien modifié.
- Pour ce qui est du **cloisonnement**, il existe bien sûr une interférence passive liée à la concurrence dans le partage des ressources.

Qu'est-ce qu'un système d'exploitation ?

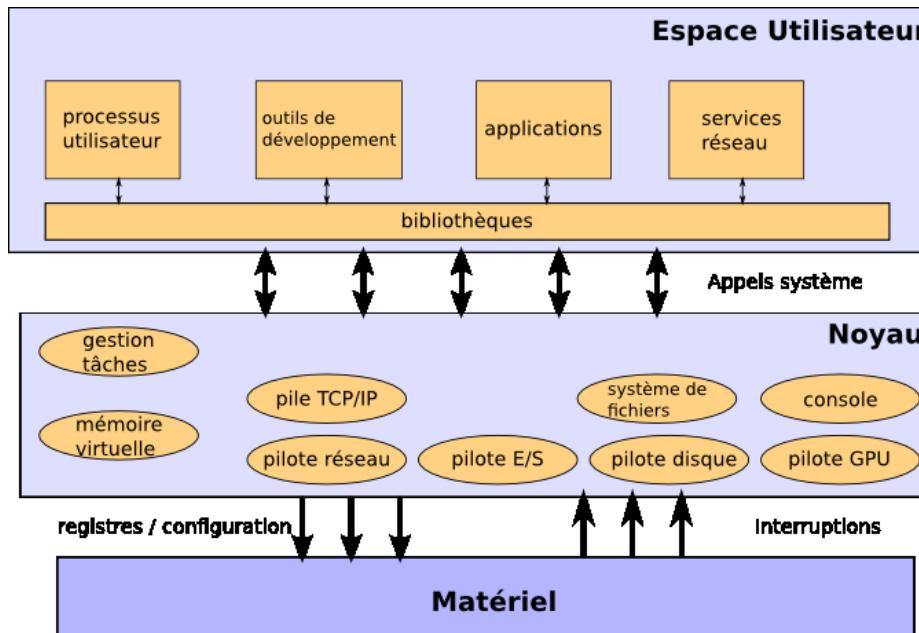
- Le système d'exploitation est chargé d'assurer la liaison entre les ressources matérielles, l'utilisateur et les applications (traitement de texte, jeu vidéo, application...)

- *Lorsqu'un programme désire accéder à une ressource matérielle, il ne lui est pas nécessaire d'envoyer des informations spécifiques au périphérique, il lui suffit d'envoyer les informations au système d'exploitation, qui se charge de les transmettre au périphérique concerné via son pilote...*

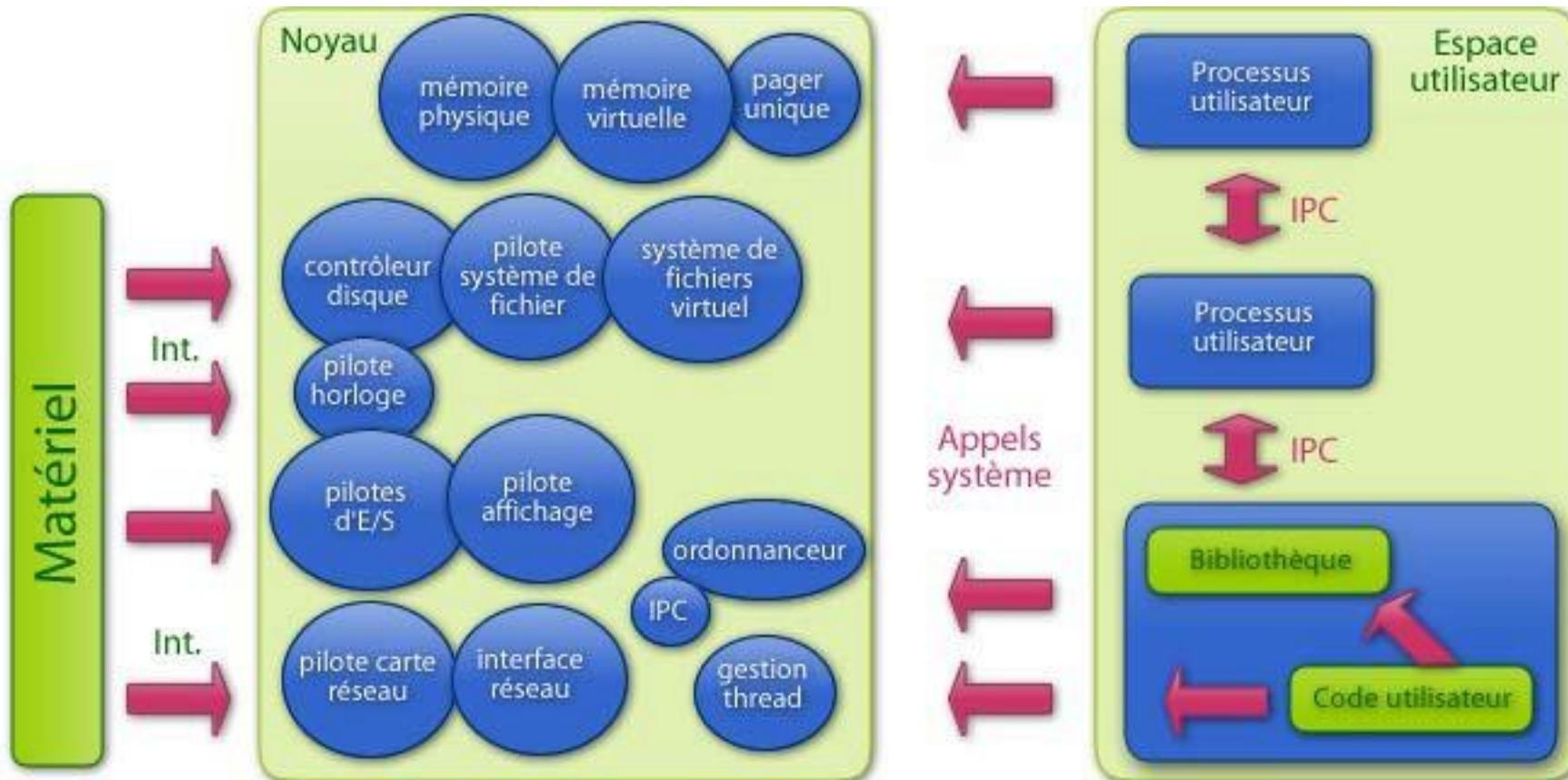


Pourquoi un système d'exploitation ?

- Le système d'exploitation permet ainsi de "dissocier" les programmes et le matériel, afin de faciliter la gestion des ressources et offrir à l'utilisateur une interface homme- machine (IHM) simple pour lui permettre de s'affranchir de la complexité de la machine physique..



Différents rôles d'un système d'exploitation



Différents rôles d'un système d'exploitation

- **Gestion du processeur** : le système d'exploitation est chargé de gérer l'allocation du processeur entre les différents programmes grâce à un algorithme d'ordonnancement.
- **Gestion de la mémoire vive** : le système d'exploitation est chargé de gérer l'espace mémoire alloué à chaque application et, le cas échéant, à chaque usager et la mémoire virtuelle».
- **Gestion des entrées/sorties** : le système d'exploitation permet d'unifier et de contrôler l'accès des programmes aux ressources matérielles par l'intermédiaire des pilotes

Différents rôles d'un système d'exploitation

- **Gestion de l'exécution des applications** : le système d'exploitation est chargé de la bonne exécution des applications en leur affectant les ressources nécessaires à leur bon fonctionnement.
- **Gestion des fichiers** : le système d'exploitation gère la lecture et l'écriture dans le système de fichiers et les droits d'accès aux fichiers par les utilisateurs et les applications.
- **Gestion des informations** : le système d'exploitation fournit un certain nombre d'indicateurs permettant de diagnostiquer le bon fonctionnement de la machine.

Centre de données (data center)



Centre de données (data center)

- Un data center, désigne un lieu physique où sont regroupés différents équipements informatiques, tels que des ordinateurs, des serveurs, etc.
- Sa fonction principale consiste à stocker des informations utiles au bon fonctionnement d'une entreprise.
- Un data center, selon sa taille, la puissance de ses systèmes de stockage, et d'autres caractéristiques, peut en effet conserver des milliards de données sur des clients, des individus, etc.
- Aujourd'hui, une grande partie des data centers de la planète proposés par AWS, Microsoft azure, GCP, Meta, etc., sont consacrés à l'accueil des serveurs utilisés pour la navigation sur Internet.

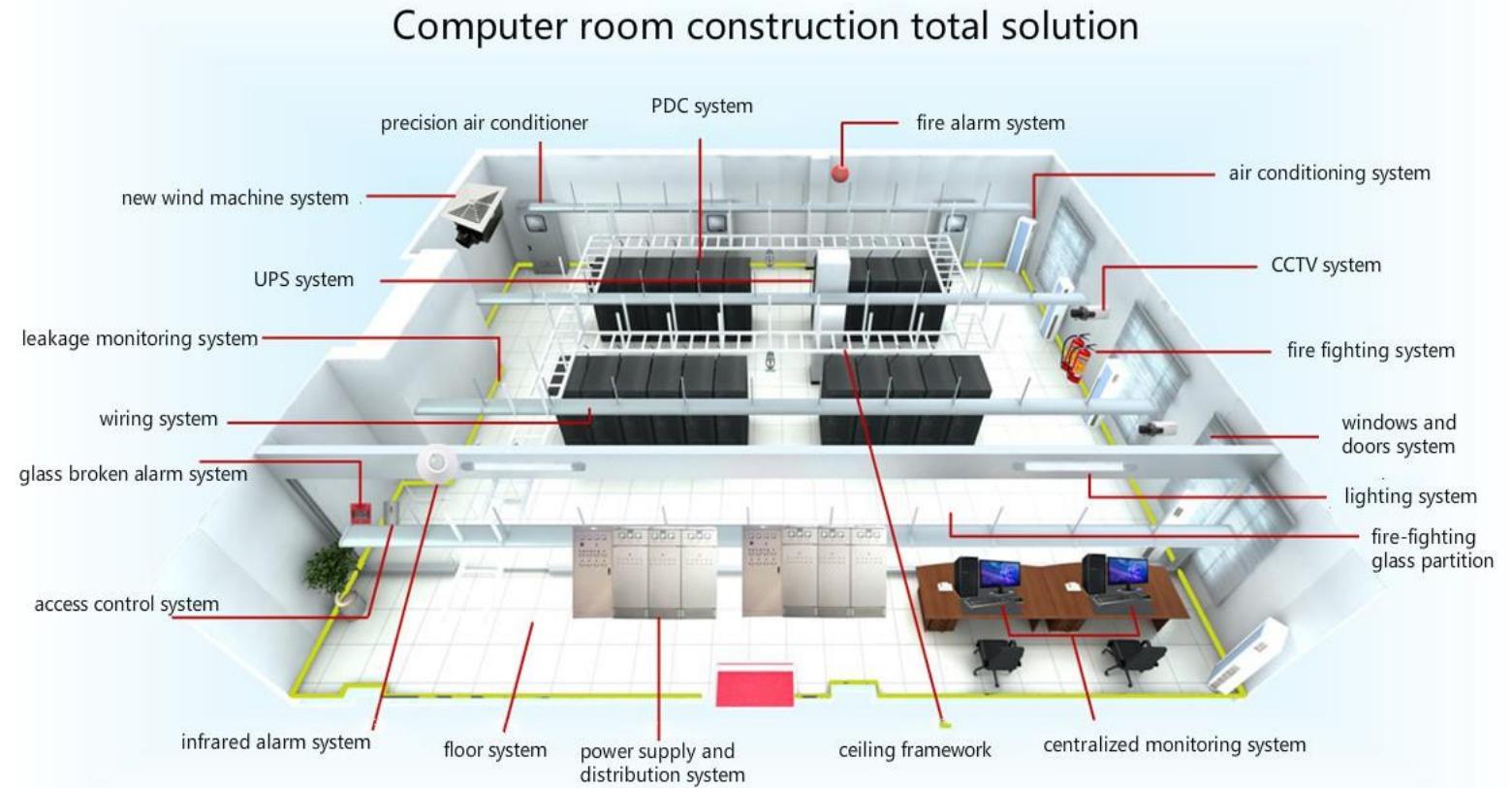
Centre de données (data center)

- Pour qu'un data center puisse fonctionner de façon optimale, certaines conditions doivent être réunies comme:
 - une excellente climatisation,
 - un contrôle de la qualité de l'air (les serveurs informatiques et la poussière ne s'apprécient pas vraiment),
 - une solution d'alimentation électrique d'urgence et de secours,
 - une surveillance 24 h/24 h ,
 - etc.

Centre de données (data center)

- Systèmes intégrés de l'infrastructure d'un DC
 - Distribution d'énergie
 - Générateur
 - Systèmes de batterie
 - Air conditionné
 - Distribution de refroidissement
 - Plancher surélevé
 - Systèmes de détection d'incendie
 - Équipement de détection de fuite
 - CCTV et Systèmes de caméra IP
 - Systèmes de contrôle d'accès
 - Systèmes de surveillance environnementale
 - Racks, armoires et accessoires
 - Câblage structuré

Centre de données (data center)



Centre de données (data center)

- DC peut être une salle de données traditionnelle, une salle de données de conteneurs ou une salle de données modulaire.



DC : Salle de Serveur



DC : Conteneur



DC : Micro-module

Virtualisation et stockage

Centre de données (data center)

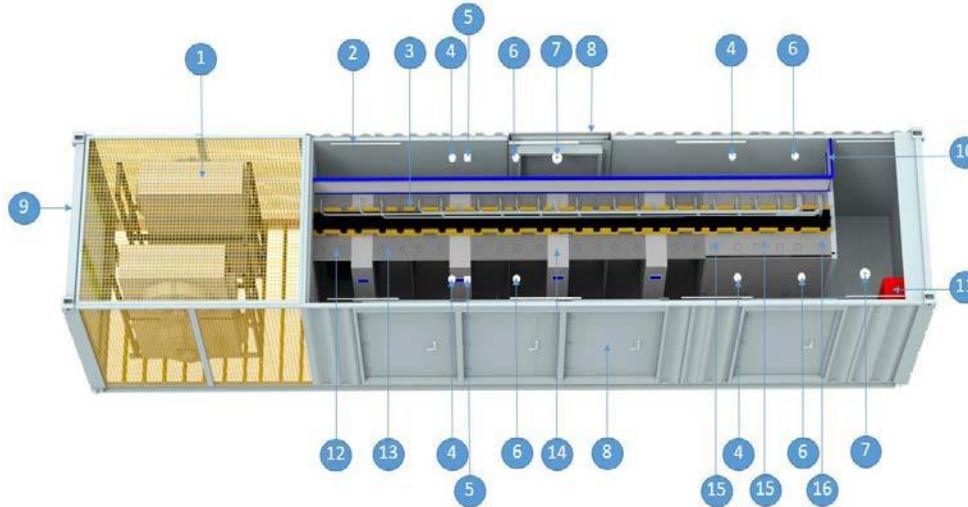
DC : Conteneur



- **Scénarios :**
 - Nécessite un déploiement rapide.
 - Lieu du DC souhaitée non disponible, solution de déploiement à l'extérieur.
 - Une solution parfaite en cas de préparation aux situations d'urgence et de reprise après sinistre.
 - Centre de données de démonstration.

Centre de données (data center)

DC : Conteneur



- **Caractéristiques :**
 - Conception et livraison tout-en-un, intégrant le refroidissement, l'alimentation électrique, la lutte contre l'incendie, la surveillance et d'autres équipements informatiques.
 - Applicable au déploiement rapide et à l'expansion des DC du cloud computing.

Centre de données (data center)



All in one
Rack solution



Micro Modular
DC solution



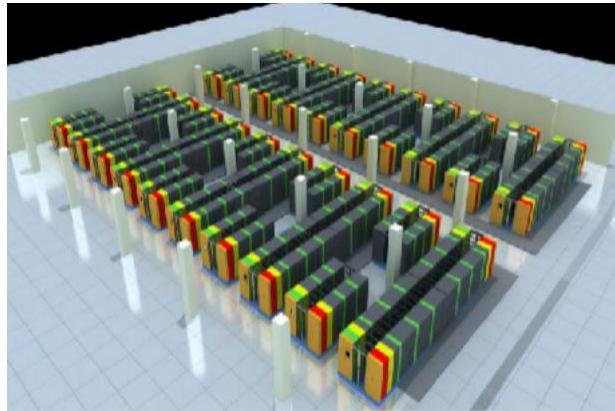
Modular
DC solution

DC Modulaire

- **Valeurs :**
 - Pas besoin d'une grande échelle physique au stade précoce, peut s'étendre en fonction des besoins de l'entreprise.
 - Augmentez l'alimentation et le refroidissement de 25%, réduisez également l'espace occupé de 15%, le coût total réduit de 15%.
 - Assure que la planification de l'infrastructure DC conformément aux exigences garantit l'efficacité du Data Center.

Centre de données (data center)

DC Modulaire

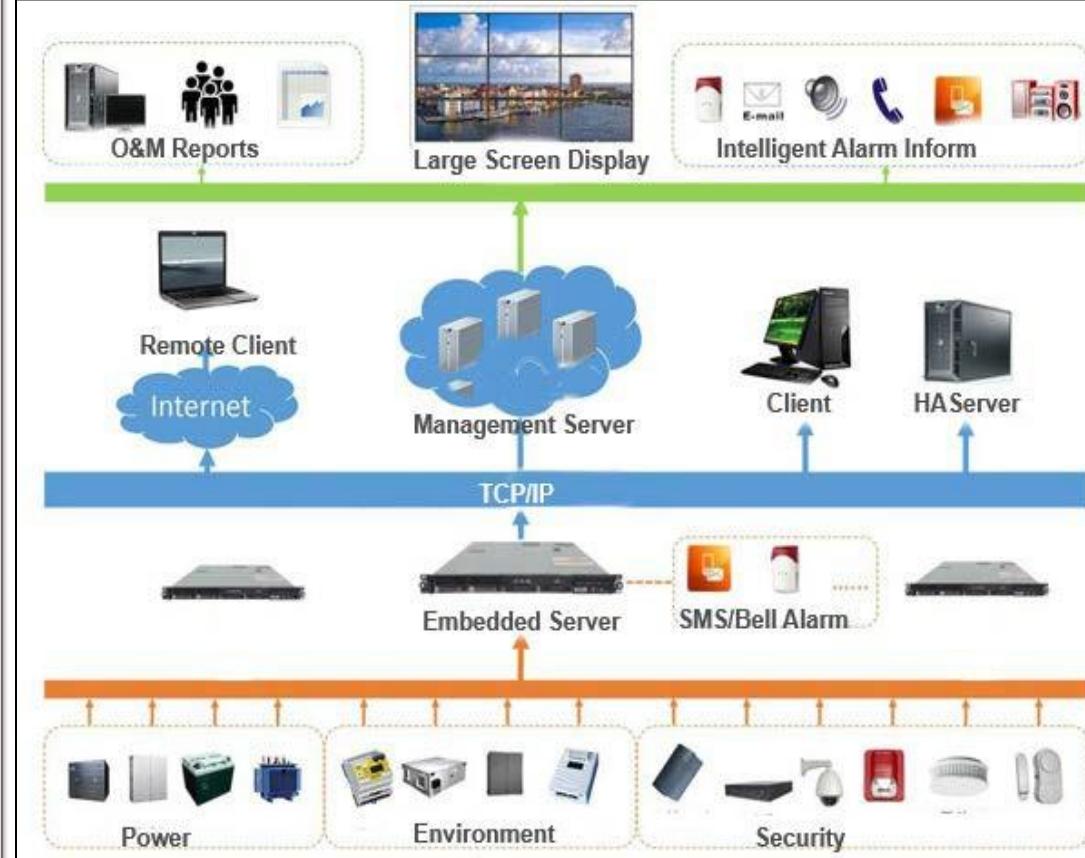


□ Caractéristiques :

- L'ensemble du centre de données est divisé en plusieurs zones indépendantes.
- Chaque module se compose principalement des éléments suivants:
 - Module de système de distribution d'alimentation
 - Module de système de refroidissement
 - module système structurel
 - Module de système de surveillance

Centre de données (data center)

- Le système de surveillance de l'infrastructure du DC comprend l'acquisition de données, le traitement des données, l'analyse et l'affichage, une variété de collecte d'informations sur l'équipement, un avertissement en temps opportun et l'affichage des problèmes et des défauts cachés et génère régulièrement des rapports d'exploitation et de maintenance pour l'exploitation et l'optimisation du centre de données.



Classification des centres de données

- L'organisme Uptime Institute a défini une certification internationalement reconnue des centres de données en quatre catégories, appelées « Tier »:
 - **Tier I (Le Basique)**: Infrastructure non redondante, une seule alimentation électrique, climatisation non redondante.
 - **Tier II (La Redondance)** : Les éléments de production de froid ou d'électricité sont redondants, mais la distribution d'électricité et de froid n'est pas redondante.
 - **Tier III (La Maintenabilité)** : Tous les composants sont maintenables sans arrêt de l'informatique.
 - **Tier IV (La tolérance aux pannes)** : Tolérance aux pannes. Aucune panne n'arrête l'informatique (réponse automatique). Absence de Point de défaillance unique *SPOF* (Single Point of Failure)
- À noter que le niveau « Tier III+ » n'est pas officiel, même si l'usage commercial est parfois rencontré.

Uptime Institute est un consortium d'entreprises créé en 1993 dont l'objectif est de maximiser l'efficacité des centres de traitement de données

Grappe de serveurs

- Grappe de serveurs ou de ferme de calcul (*computer cluster*) désigne les techniques consistant à regrouper plusieurs ordinateurs indépendants appelés nœuds (*node*), afin de permettre une gestion globale et de dépasser les limitations d'un ordinateur pour :
 - augmenter la disponibilité ;
 - faciliter la montée en charge ;
 - permettre une répartition de la charge ;
 - faciliter la gestion des ressources :
 - processeur,
 - mémoire vive,
 - disques dur,
 - bande passante réseau.



Grappe de serveurs

- La création de grappes de serveurs est un procédé peu coûteux, résidant dans la mise en place de plusieurs ordinateurs en réseau qui vont apparaître comme un seul ordinateur ayant plus de performances:
 - puissance du processeur,
 - dimension de l'espace de stockage,
 - quantité de mémoire vive
- Les grappes de serveurs sont particulièrement utilisées pour les calculs parallèles.
- Cet usage optimisé des ressources permet la répartition des traitements sur les différents nœuds.

Grappe de serveurs

□ Utilisation :

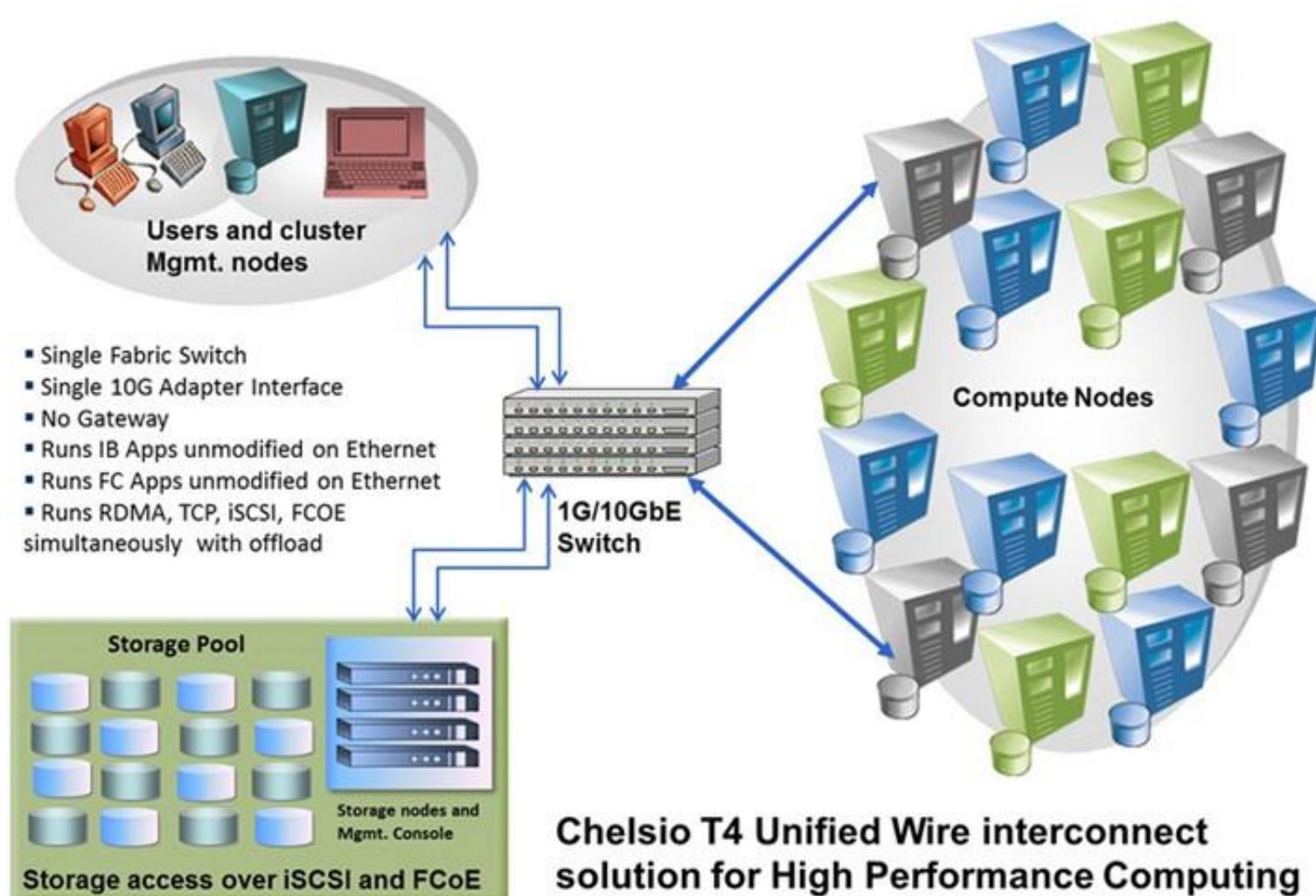
- Leur utilisation est de plus en plus importante dans la communauté scientifique, où les besoins en calculs à haute performance (HPC) sont toujours croissants, ainsi qu'en imagerie numérique notamment pour les images de synthèse au travers des fermes de rendu.
- En Informatique de gestion, les grappes peuvent être utilisées pour minimiser l'impact d'une panne de serveur sur la disponibilité d'une application.
 - Cela nécessite la mise en œuvre de disques partagés, par exemple dans le cadre d'un réseau de stockage SAN.

Grappe de serveurs

□ Bénéfices :

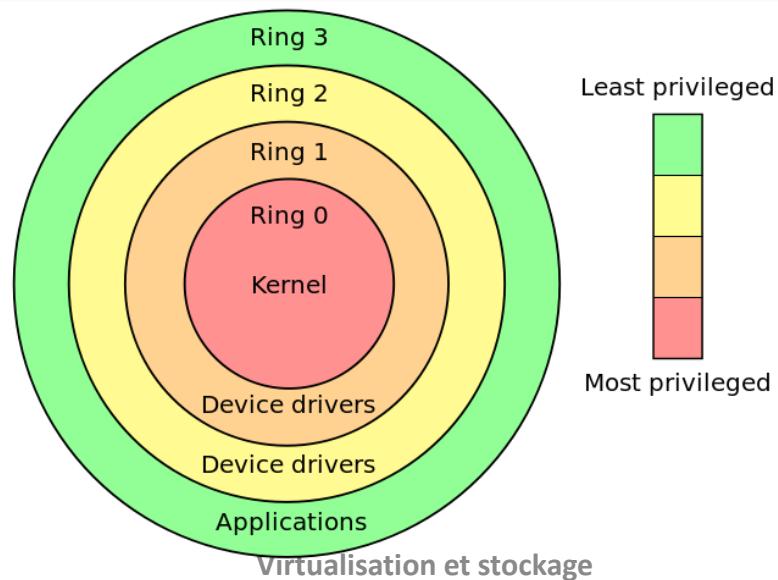
- **Évolutivité ou scalabilité (scalable)** : capacité d'une application à accepter un nombre croissant d'utilisateurs. Reposant sur plusieurs facteurs, notamment le nombre d'utilisateurs pouvant se connecter simultanément à un cluster et le temps nécessaire pour traiter une requête.
- **Disponibilité** : la haute disponibilité peut se définir comme la redondance. Ainsi, si un serveur tombe en panne alors qu'il est en train de traiter des requêtes, d'autres serveurs du cluster doivent pouvoir les traiter d'une manière aussi transparente que possible. Tout serveur défaillant est retiré du cluster dès qu'il tombe en panne de sorte que les requêtes suivantes ne soient plus acheminées vers ce dernier. En matière de reprise à chaud pour les applications d'entreprise, la résilience et la disponibilité revêtent la plus haute importance.

Grappe de serveurs



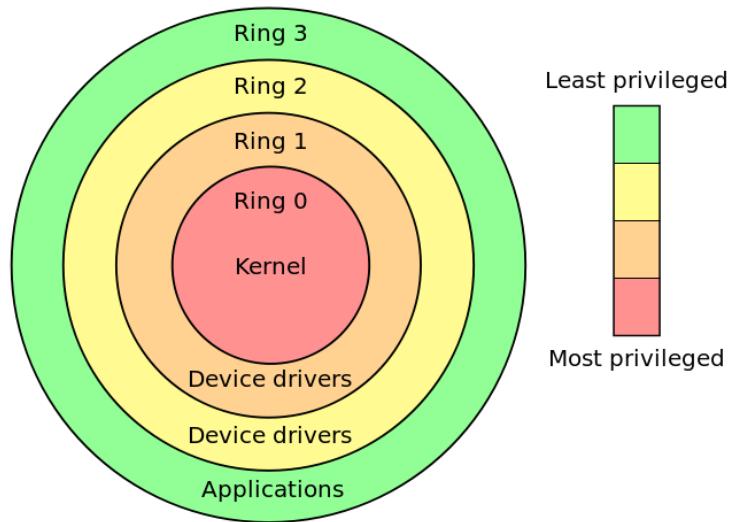
Anneau de protection (RING)

- Un anneau de protection est l'un des niveaux de privilèges imposés par l'architecture d'un processeur.
- De nombreuses architectures modernes de processeurs (architectures parmi lesquelles on trouve le populaire Intel x86) incluent une certaine forme de protection en anneau.
 - Bien que les logiciels d'exploitation ne l'exploitent pas toujours entièrement.



Anneau de protection (RING)

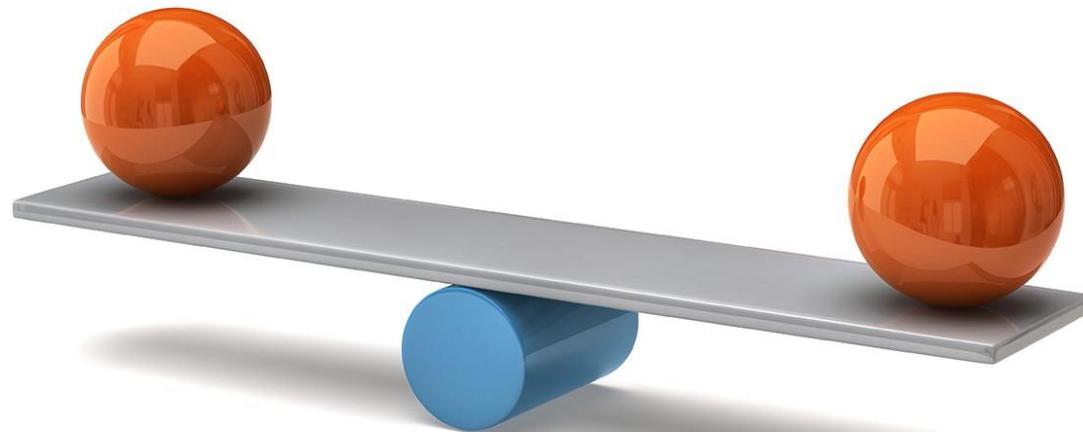
- Les rings étaient parmi les concepts les plus révolutionnaires mis en œuvre par le système d'exploitation Multics (prédecesseur fortement sécurisé de la famille UNIX).
- Les anneaux sont rangés dans une hiérarchie allant du plus privilégié (celui qui est le plus sécurisé, habituellement le numéro zéro dit *Ring0*) au moins privilégié (le moins sécurisé, habituellement l'anneau le plus élevé).



Multics (*MULTIplexed Information and Computing Service*) est le nom d'un système d'exploitation en temps partagé.

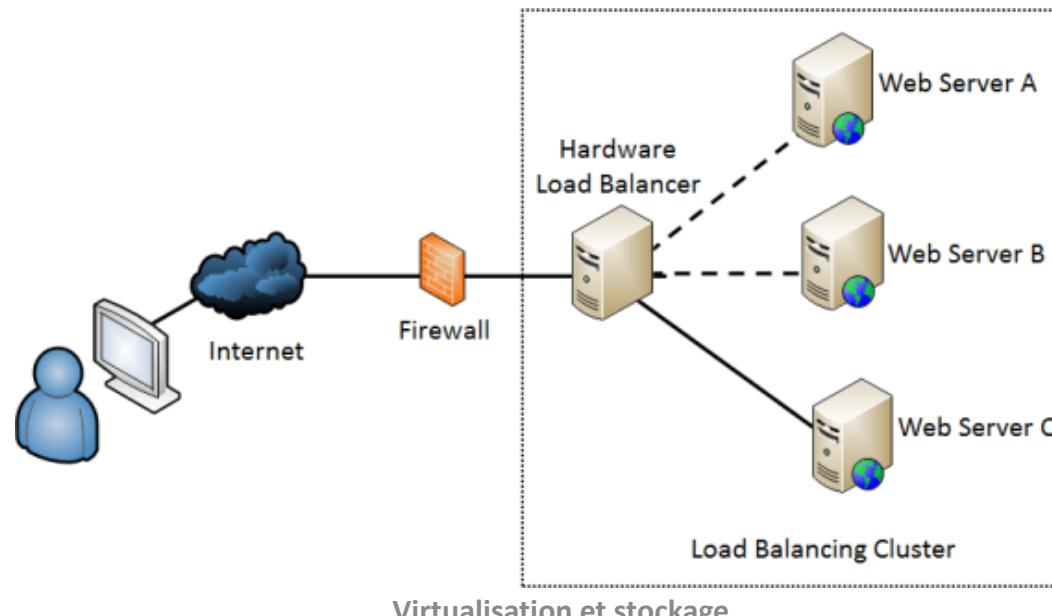
Répartition de charge (load balancing)

- **La répartition de charge** : ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe.
- Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur.



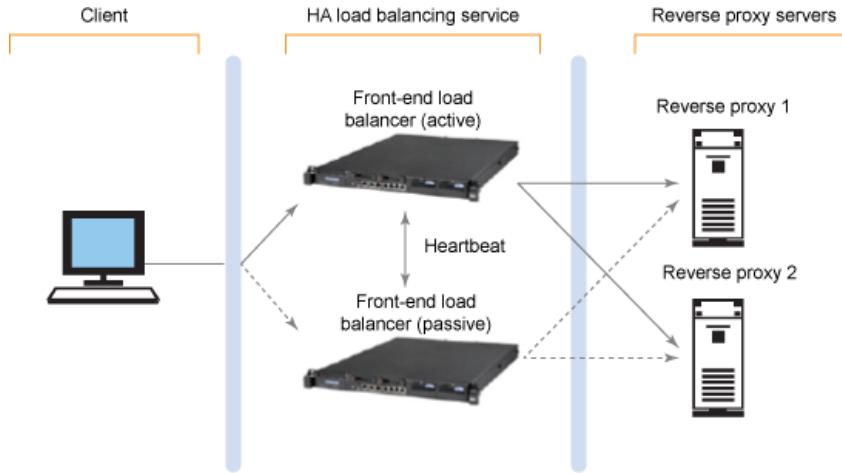
Répartition de charge (load balancing)

- Ces techniques sont par exemple très utilisées dans le domaine des services HTTP où un site à forte audience doit pouvoir gérer des centaines de milliers de requêtes par seconde.
- La répartition de charge est issue de la recherche dans le domaine des ordinateurs parallèles.



Répartition de charge (load balancing)

- L'architecture la plus courante est constituée de plusieurs répartiteurs de charge (routeurs dédiés à cette tâche), un principal, et un ou plusieurs de secours pouvant prendre le relais, et d'une collection d'ordinateurs similaires effectuant les calculs.



- On peut appeler cet ensemble de serveurs une **ferme de serveurs** (*server farm*) ou de façon plus générique, une **grappe de serveurs** (*server cluster*).
- On parle encore de **groupe de serveurs** (*server pool*).

Répartition de charge (load balancing)

- Dans le **domaine de la répartition de charge**, on appelle :
 - **Serveur virtuel** : un pool de serveurs assigné à une tâche, l'adresse et le port utilisés doivent être réglés sur le répartiteur de charge et, selon le mode, sur les serveurs de calcul.
 - **Serveur réel** : un des serveurs dans le pool.

Répartition de charge (load balancing)

- Sur les répartiteurs de charge les plus courants, on peut pondérer la charge de chaque serveur indépendamment.
 - Cela est utile lorsque, par exemple, on veut mettre, à la suite d'un pic ponctuel de charge, un serveur de puissance différente dans la grappe pour alléger sa surcharge.
 - On peut ainsi y ajouter un serveur moins puissant, si cela suffit, ou un serveur plus puissant en adaptant le poids.

Haute disponibilité (High Availability)

- On définit la haute disponibilité comme un système permettant d'assurer une continuité opérationnelle d'un service sur une période donnée.
- Il n'y a pas de norme en ce qui concerne la durée d'une interruption de service : cela dépend du contexte et de la criticité de l'application.
 - **Exemple** : un système de navigation embarqué dans un avion sera conçu pour avoir une période d'indisponibilité de 5 minutes par an, alors que l'application de facturation d'une entreprise sera conçue pour une période d'indisponibilité d'une journée par an.

Haute disponibilité (High Availability)

- Pour mesurer la disponibilité, on utilise une échelle qui est composée de 9 échelons.
- Un service Hautement Disponible est 99% disponible soit moins de 365 jours par an.
- Afin de calculer la disponibilité, les métriques suivantes sont utilisées:
 1. **MTBF** (*Mean Time Between Failure*) : mesure du temps estimé entre 2 défaillances d'un système.
 2. **MTTR** (*Mean Time to Resolution*) : mesure du temps estimé pour restaurer la fonctionnalité.
- La formule de calcul de disponibilité est :

$$\text{Disponibilité} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

Haute disponibilité (High Availability)

- Deux moyens complémentaires sont utilisés pour améliorer la haute disponibilité :
 - **Mise en place d'une infrastructure matérielle spécialisée** : généralement en se basant sur la redondance matérielle en créant un cluster de haute-disponibilité (par opposition à un cluster de calcul) :
 - une grappe d'ordinateurs dont le but est d'assurer un service en évitant au maximum les indisponibilités.
 - **Mise en place de processus adaptés** : permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur.

Scalabilité (Scalability)

- Les charges réelles d'applications sont souvent dynamiques.
 - le dimensionnement statique de ressources est voué soit au gaspillage, s'il est basé sur une estimation du pire scénario, soit à la dégradation de performance, s'il est basé sur la charge moyenne.

Grâce aux modèles Informatique récentes, les ressources peuvent être allouées à la demande et le dimensionnement adapté à la variation de la charge.

Scalabilité (Scalability)

- La scalabilité peut faire référence à la capacité d'un système à accroître sa capacité de calcul sous une charge accrue quand des ressources (généralement du matériel) sont ajoutées.
- La scalabilité est une capacité recherchée des applications de base de données, des moniteurs de transactions et des systèmes d'exploitation.

Elasticité

- Il est habituel de considérer l'élasticité et la scalabilité comme étant des synonymes.
- **Élasticité:**
 - Élasticité est une propriété d'un objet qui retrouve sa forme d'origine après avoir été déformé.
 - Mécanisme d'élasticité fait varier les ressources allouées en fonction de la charge pour satisfaire une QdS.
- **Scalabilité:**
 - Capacité d'un système à accroître sa capacité de calcul sous une charge accrue quand des ressources sont ajoutées.
 - Accroissement linéaire
 - Pas d'attentions sur les ressources non utilisées ou sous utilisées
 - Insensible à la fluctuation et à la dimension temps

La distinction entre la scalabilité et l'élasticité tient essentiellement dans le fait que la scalabilité permet de supporter les augmentations de charges de travail **grâce à l'ajout de ressources** alors que l'élasticité adapte les ressources à la volée en fonction des besoins **à la hausse comme à la baisse**.

Elasticité

- Le ***cloud computing*** permet en principe une élasticité virtuellement sans limite.
- Dans l'idéal, on aimerait bénéficier d'une fonction presse-bouton, pour allouer davantage de ressources aux applications en production.
- Instantanément, les performances seraient alors améliorées ou le nombre d'utilisateurs supportés augmenterait.

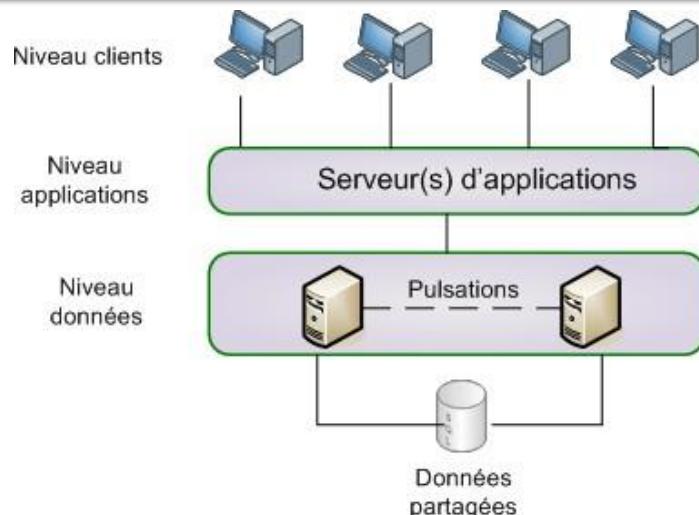
- On distingue deux types d'élasticité:
 - **Elasticité verticale** : on augmente la puissance ou la mémoire des serveurs sans en augmenter le nombre. « Cela permet typiquement de réduire le temps de traitement de chaque requête »
 - Mais cette méthode est contrainte par les capacités des serveurs les plus puissants, en termes de nombre de cœurs et de taille mémoire.
 - **Elasticité horizontale**: on augmente le nombre de serveurs ce que ne pose généralement pas de problème pour les infrastructures Web et la difficulté se concentre davantage sur le code applicatif.
 - Il est possible d'allouer un process Java à un thread que l'on peut exécuter sur un cœur virtuel, mais pour répartir vraiment l'exécution d'une application complète sur plusieurs serveurs virtuels, cela reste compliqué.

Elasticité

- Une action d'élasticité **manuelle** est effectuée par une intervention manuelle de l'utilisateur.
- Une action d'élasticité **automatique** est effectuée automatiquement selon deux modes :
 - **Réactif** : les actions d'élasticité sont déclenchées en fonction de certains seuils et/ou des règles, le système réagit à la charge (*charge de travail ou utilisation des ressources*) et déclenche des actions pour adapter les changements en conséquence.
 - **Proactif** : cette approche met en œuvre des techniques de prévision, anticipe les besoins futurs et déclenche des actions basées sur cette anticipation.

Basculement (failover)

- Le basculement est la capacité d'un équipement à basculer automatiquement vers un réseau ou un système alternatif ou en veille.
 - Cette capacité existe pour tout type d'équipements réseau: du serveur au routeur en passant par les pare-feu et les commutateurs réseau (*switch*).
- Le basculement intervient généralement sans action humaine et même bien souvent sans aucun message d'alerte.
- Le basculement est conçu pour être totalement transparent.



Basculement (failover)

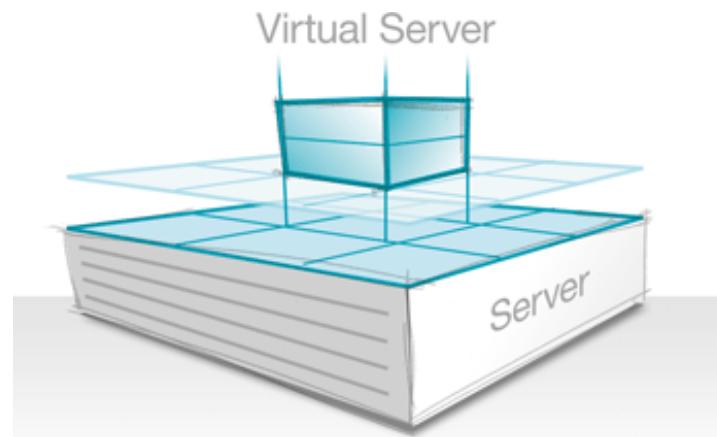
- Les concepteurs de systèmes prévoient généralement cette possibilité dans les serveurs ou les réseaux qui nécessitent une disponibilité permanente (*HA=High Availability*).
- Dans certains cas, le basculement automatique n'est pas souhaité et le basculement requiert une action humaine ;
 - automatisation avec approbation humaine.
- Il existe deux modes principaux de basculement :
 - **actif/actif** : qui s'apparente plus à de l'équilibrage de charge (*load-balancing*) ;
 - **actif/passif** : le mode classique couramment répandu, où l'équipement secondaire (passif) est en mode veille tant que l'équipement primaire (actif) ne rencontre aucun problème.

Machine physique / Machine Virtuelle

- La **virtualisation** fait appel au **logiciel** pour **simuler l'existence du matériel** et créer un **système informatique virtuel**.
 - Modèle permet d'exécuter plusieurs systèmes virtuels et plusieurs systèmes d'exploitation et applications sur un seul et même serveur.
- Il se traduit ainsi par des économies d'échelle et des gains d'efficacité.

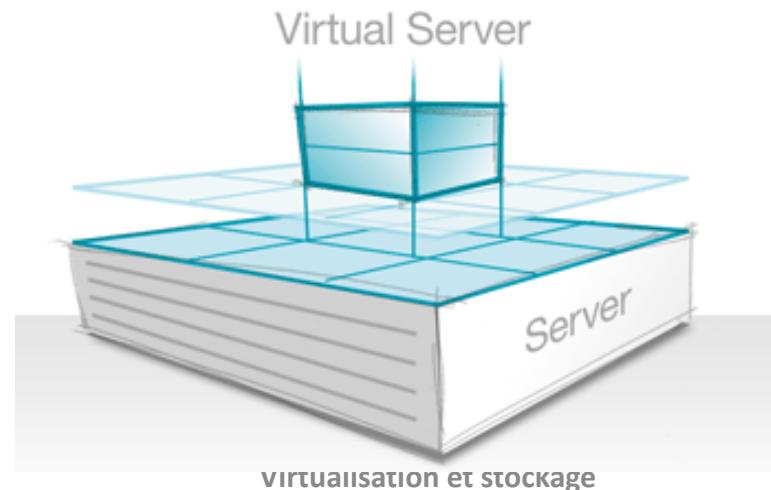
Machine physique / Machine Virtuelle

- Chaque système informatique virtuel correspond à une « machine virtuelle » (VM)
 - C'est-à-dire à un ***conteneur de logiciels*** totalement isolé, et doté d'un système d'exploitation et d'applications.
- Chaque VM est une entité autonome et complètement indépendante.



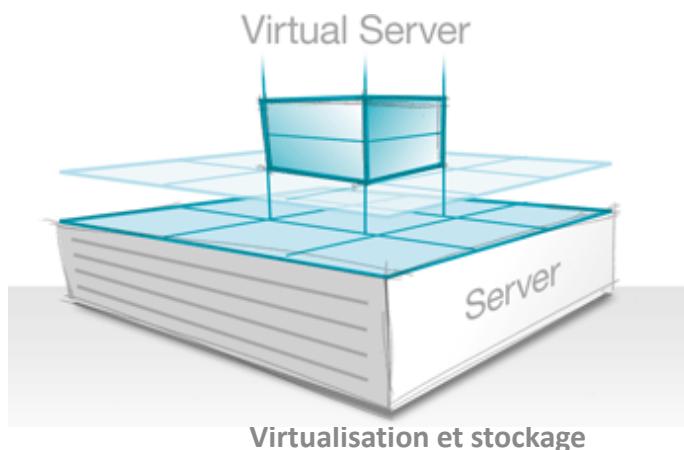
Machine physique / Machine Virtuelle

- L'installation de plusieurs VM sur un ordinateur permet d'exécuter différents systèmes d'exploitation et applications sur un seul et même serveur physique, ou « **hôte** ».
- Une couche logicielle fine appelée **hyperviseur** découpe les machines virtuelles de l'hôte et alloue dynamiquement les ressources informatiques aux différentes machines suivant les besoins.



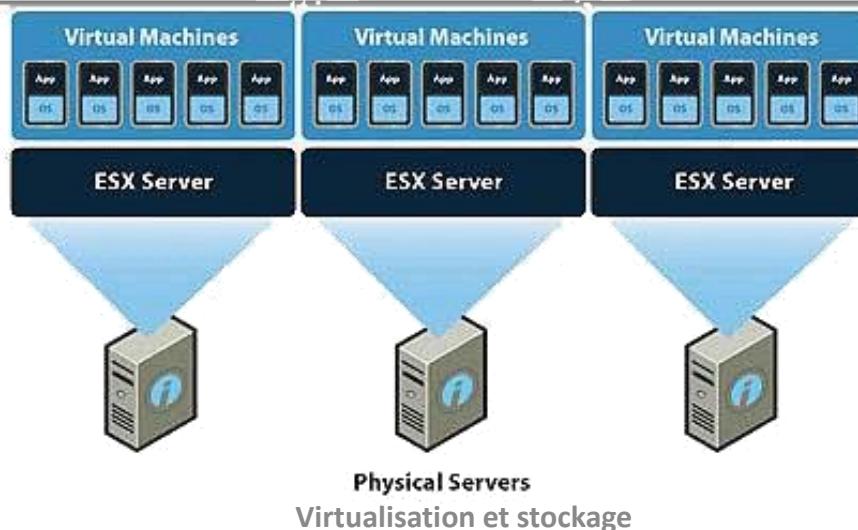
Serveur virtuel

- Un **serveur virtuel** (*virtual server*, *virtual private server* ou *virtual dedicated server*) est une **machine virtuelle**.
- Un **serveur virtuel** est un conteneur de logiciel complètement isolé capable de gérer ses propres systèmes d'exploitation et applications comme s'il s'agissait d'un ordinateur physique, en utilisant des techniques de *virtualisation*.



Serveur virtuel

- Un **serveur virtuel** se comporte exactement comme un ordinateur physique et contient son propre virtuel CPU, RAM, disque dur et carte réseau.
- Un système d'exploitation ne peut pas faire la différence entre un **serveur virtuel** et un **serveur physique**.
- Ainsi, la **machine virtuelle** offre de nombreux avantage comparé au **matériel physique**.



Propriétés clés des machines virtuelles

- Les caractéristiques des VM offrent plusieurs avantages.
 - **Partitionnement**
 - Exécutez plusieurs systèmes d'exploitation sur une machine physique
 - Répartissez les ressources système entre les machines virtuelles
 - **Isolation**
 - Assurez l'isolation des pannes et la protection de la sécurité au niveau matériel
 - Maintenez les performances en déployant des contrôles avancés des ressources
 - **Encapsulation**
 - Enregistrez dans des fichiers l'état complet des différentes machines virtuelles
 - Déplacez et copiez des machines virtuelles aussi facilement que des fichiers
 - **Interopérabilité du matériel**
 - Provisionnez ou migrez n'importe quelle machine virtuelle vers n'importe quel serveur physique

Les conteneurs (*Container*)

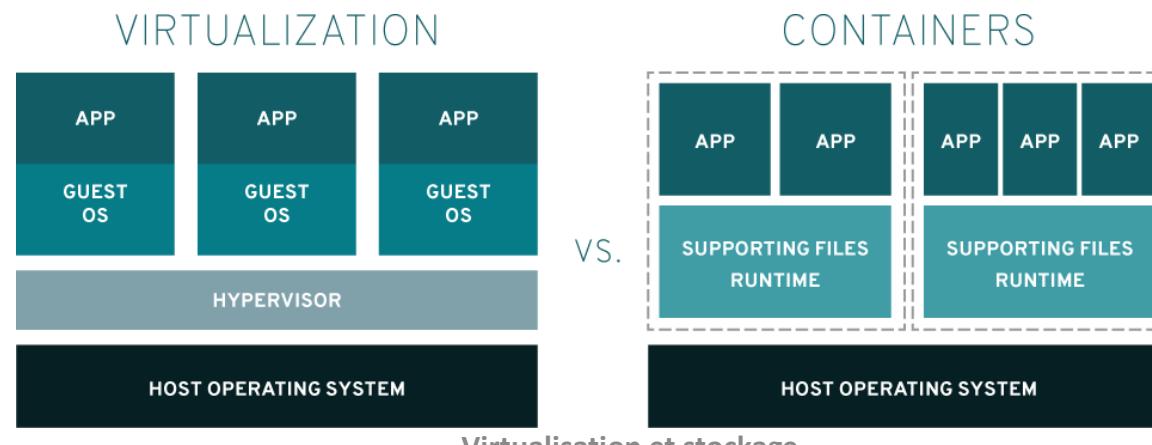
- Une alternative à la virtualisation matérielle est donnée par **la virtualisation du système d'exploitation**.
 - C'est ainsi que diverses applications de serveurs sont réalisées dans des environnements virtuels isolés, ce qu'on appelle les conteneurs, qui fonctionnent sur le même système d'exploitation.
 - On parle de **virtualisation par conteneur**.

Les conteneurs (*Container*)

- Les conteneurs logiciels sont considérés comme des applications pour le serveur.
- Pour installer une application, il faut charger le conteneur correspondant dans un format portable (*une image*) avec toutes les données nécessaires sur l'ordinateur et le démarrer dans un environnement virtualisé.
- Les conteneurs présentent aux administrateurs des données complètes qui servent au fonctionnement d'une application serveur.

Les machines ne sont-elles que des conteneurs?

- La virtualisation fournit les ressources que les conteneurs peuvent utiliser.
- Ces VM sont des environnements dans lesquels les conteneurs peuvent être exécutés, mais les conteneurs ne sont pas liés aux environnements virtuels.
- Les VM disposent de fonctionnalités limitées, car les hyperviseurs utilisés pour les créer dépendent des ressources limitées d'une machine physique.
- En revanche, les conteneurs partagent le même noyau de système d'exploitation et regroupent les applications avec leur environnement d'exécution.



Pourquoi virtualiser ?

Retour sur la virtualisation

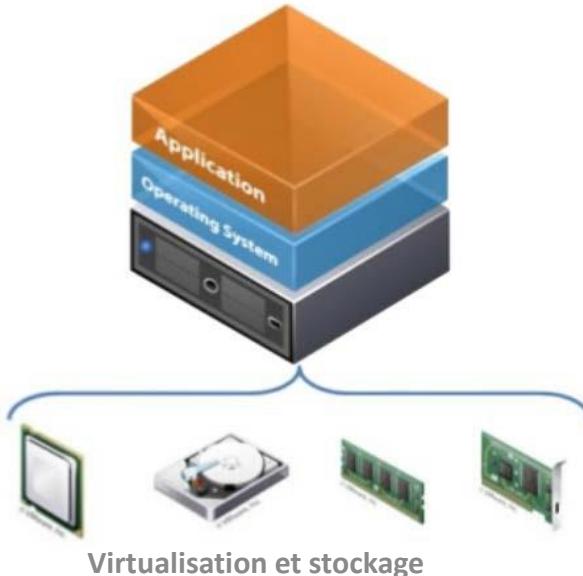
- La virtualisation transforme du matériel en logiciel et permet de ne conserver que les *firmwares* des différentes cartes d'un serveur et de les utiliser au sein d'un serveur virtuel.



- On appelle donc virtualisation l'ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation et/ou plusieurs applications séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.
- Il faut ajouter à cela les technologies de virtualisation de réseau et d'application.

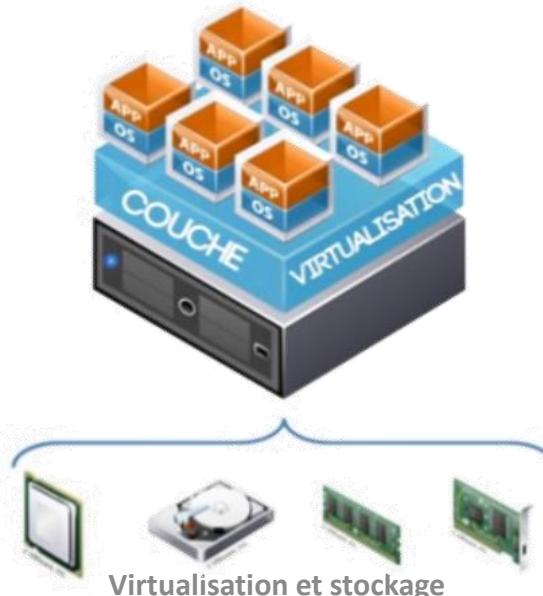
Pourquoi virtualiser ?

- **Architecture x86 traditionnelle**
 - **Un** système d'exploitation **par** machine
 - Exécution de plusieurs applications **par** serveur augmente le risque d'interruption de service global
 - En général: **1** serveur = **1** application



Pourquoi virtualiser ?

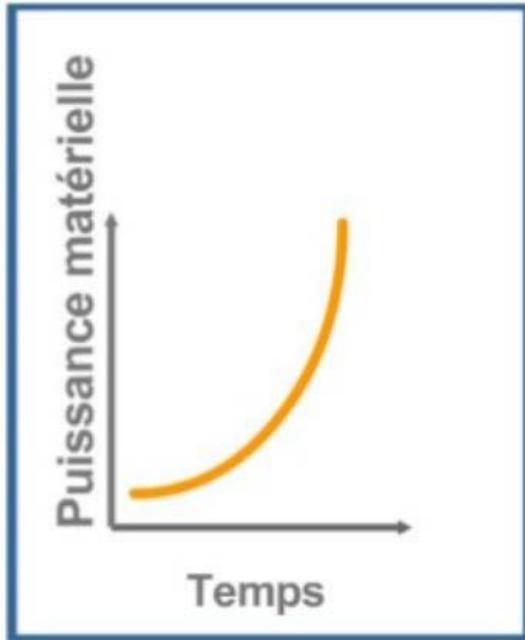
- **Architecture x86 virtualisée**
 - Ajout de la couche de virtualisation
 - Chaque machine virtuelle possède ses propres applications et système d'exploitation
 - Possibilités d'exécuter plusieurs systèmes d'exploitations sur la même machine physique



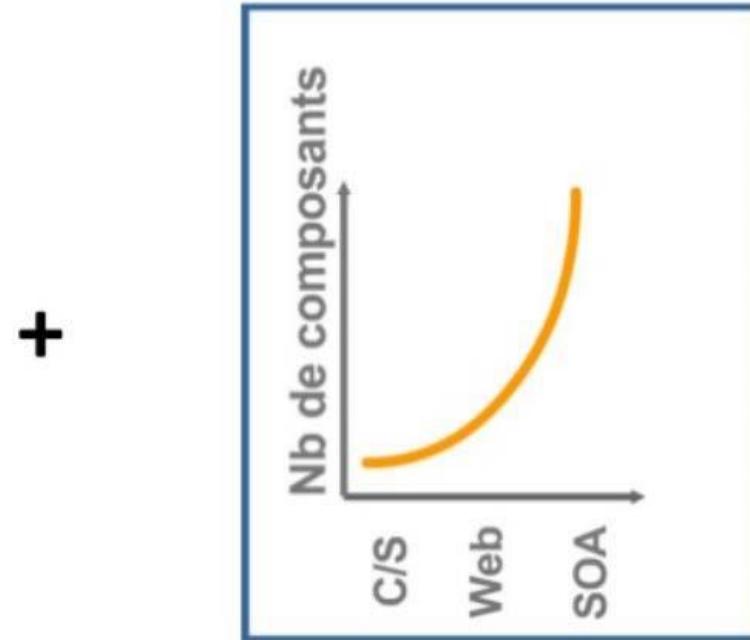
Pourquoi virtualiser ?

- Tendance conduisant à une utilisation inefficace

Matériel serveur plus puissant

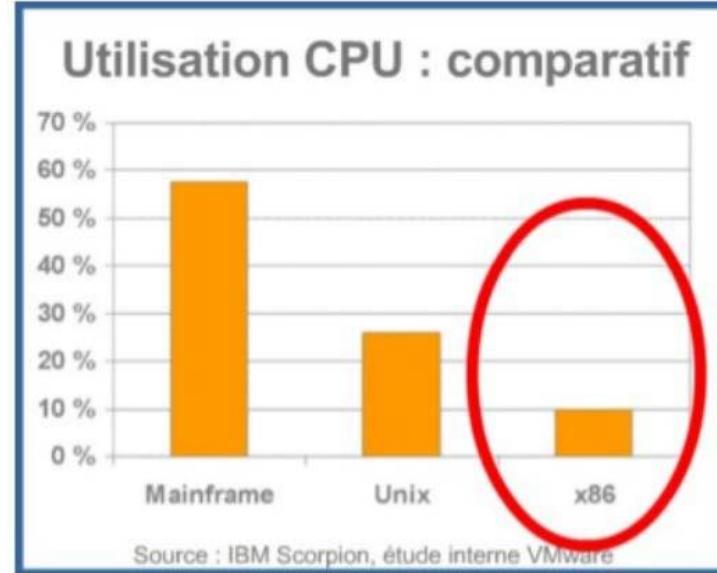


Exploitation du nombre de composant physique et logique



Pourquoi virtualiser ?

- Diminution du taux d'utilisation CPU sur x86
 - Taux d'utilisation CPU de l'unité centrale sur x86 de plus en plus faible (multi-coeur)
 - Utilisation CPU de 5 à 15 % sur serveur x86



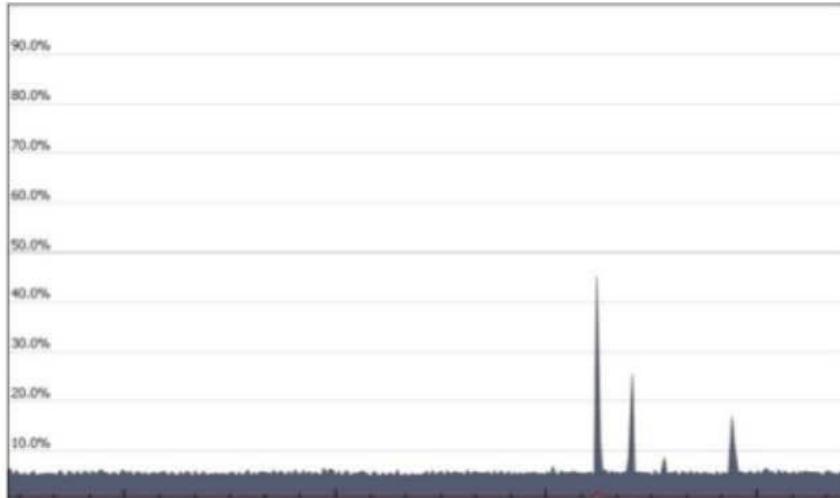
Paradoxe :

Nombre et complexité **croissante** des machines et **manque** d'efficacité

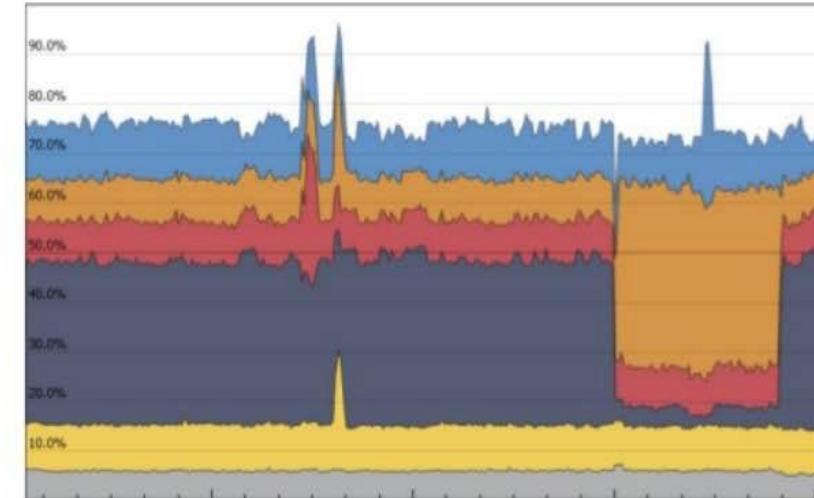
Pourquoi virtualiser ?

- Efficacité d'utilisation des serveurs x86

Sans la virtualisation



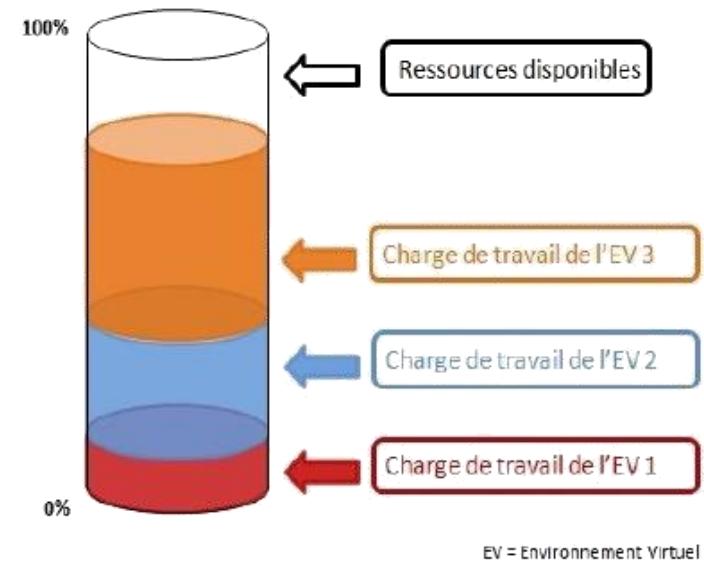
Avec la virtualisation



- La virtualisation permet de consolider les charges de travail des serveurs **sous-exploités** sur un seul serveur tout en maîtrisant le taux d'utilisation global

Pourquoi virtualiser ?

- De cette manière, comme le montre le schéma, on optimise le rendement de chacun des serveurs physiques.
- La virtualisation va apporter une solution efficace:
 - plutôt que de faire tourner une seule application sur le serveur physique, on va installer sur celui-ci plusieurs serveurs virtuels exécutant chacun une application bien précise, et c'est le logiciel de virtualisation qui se charge de répartir équitablement les ressources entre les différentes instances.
- L'idée est alors de récupérer ces ressources disponibles afin d'en faire bénéficier d'autres applications.



Pourquoi virtualiser ?

- Prolifération des serveurs : Manque d'espace



Pourquoi virtualiser ?

- **Plan de reprise d'activité (*Disaster Recovery Plan ou DRP*) (sur échec)**
 - Permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

- Le DRP doit permettre, en cas de sinistre, de basculer sur un système de relève capable de prendre en charge les besoins informatiques nécessaires à la survie de l'entreprise.
- Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise.



5 bonnes raisons d'adopter la virtualisation

(1) Rentabiliser davantage les ressources existantes :

regrouper les ressources communes en sortant du schéma « une application = un serveur » grâce à la consolidation des serveurs.

(2) Réduire les coûts en minimisant l'infrastructure physique et en améliorant le rapport serveur/administrateur :

les serveurs et les équipements matériels associés sont en nombre réduit. Cela se traduit par une diminution des frais immobiliers et des besoins en alimentation et en ventilation. Des outils de gestion plus performants permet d'optimiser le rapport serveur/administrateur de sorte que les besoins en effectifs sont également réduits.

5 bonnes raisons d'adopter la virtualisation

(3) Augmenter la disponibilité du matériel et des applications pour une amélioration de la continuité d'activité : sauvegarder et migrer des environnements virtuels complets sans interruption dans le service.

Éviter les interruptions planifiées et trouver immédiatement la solution à des problèmes imprévus.

(4) Gagner en flexibilité opérationnelle : s'adapter à l'évolution du marché grâce à une gestion dynamique des ressources, un provisionnement accéléré des serveurs et un déploiement optimal des postes de travail et des applications.

5 bonnes raisons d'adopter la virtualisation

(5) Améliorer la gérabilité et la sécurité des postes de travail : déployer, gérer et surveiller des environnements de postes de travail sécurisés auxquels les utilisateurs peuvent accéder localement ou à distance.

Spécificités de la virtualisation

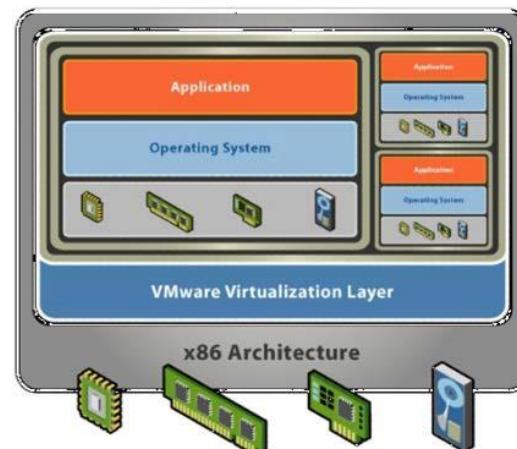
La compatibilité

- **Compatibilité**
 - Périphériques matériels
 - Systèmes d'exploitation
 - Applications

Serveur physique



**Machine virtuelle à
l'intérieur d'un serveur
physique**



L'isolation

- **Isolation**

- Les machines virtuelles s'exécutent de manière indépendantes
- Elles sont protégées les unes des autres

Quatre machines physiques



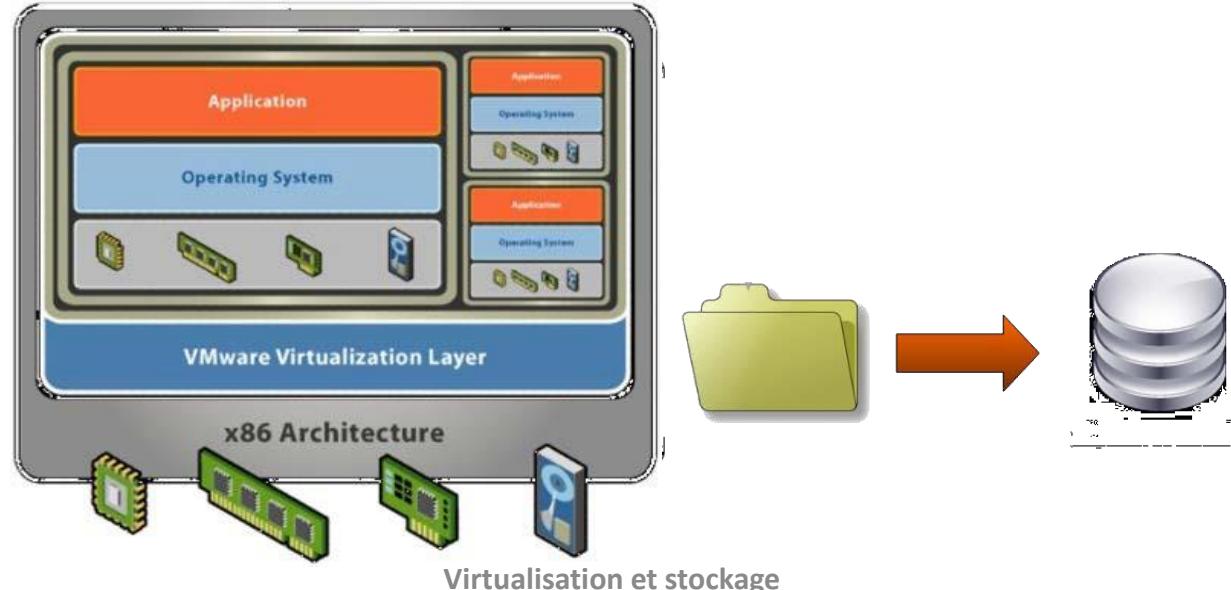
Quatre machines virtuelle sur un serveur physique



L'encapsulation

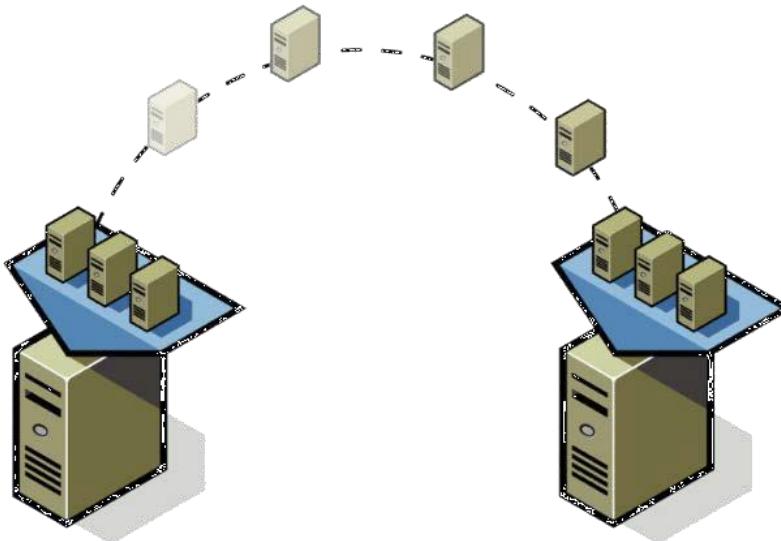
- **L'encapsulation**

- L'Etat complet d'une machine virtuelle est contenu dans un fichier.
- Procédure de provisionnement de serveur similaire à la copie d'un fichier
- Procédure de migration de serveur similaire à la migration de données
- Possibilités d'utiliser les techniques de gestion des données pour gérer les serveurs



L'indépendance matérielle

- **Indépendance matérielle**
 - Les machines virtuelles détectent toujours le même ensemble matériel, indépendant du matériel physique.
 - Les pilotes sont indépendants du matériel de la machine dans laquelle ils sont installés
 - Les machines virtuelles peuvent être déplacées vers un matériel différent, sans modifications ...
 - ... d'un ordinateur portable à un poste de travail et à un serveur haut de gamme.



Virtualisation et stockage

Notion de Consolidation, Rationalisation et Concentration

Consolidation

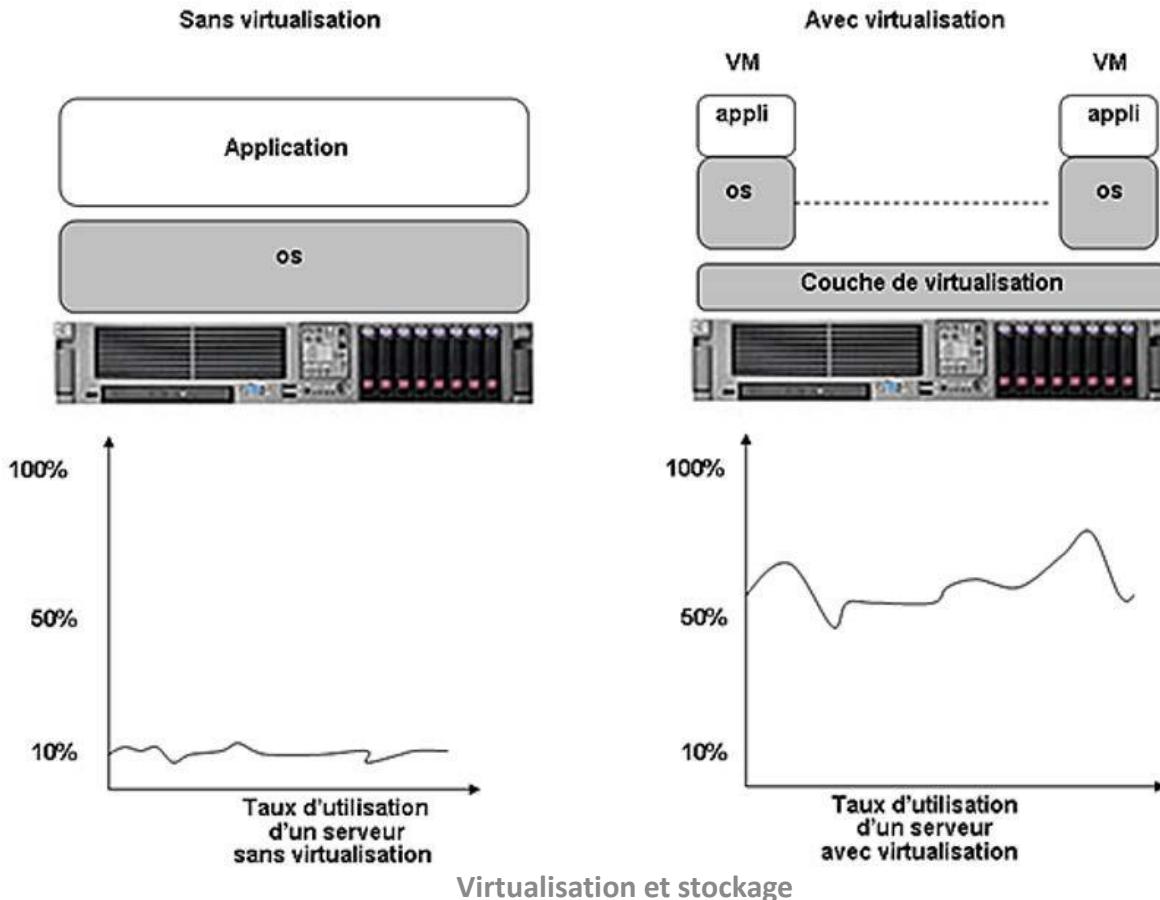
- La consolidation de serveurs englobe toutes les stratégies et technologies capables de réduire le nombre ou la répartition géographique des serveurs que possède et gère une entreprise.
- Lorsqu'on minimise le nombre de serveurs et les connexions entre eux, les systèmes d'information fonctionnent de façon plus transparente.

- Contrer la tendance :
 - 1 application = 1 serveur
- Amener les serveurs à des taux d'utilisation de plus de 50 %
- Réduire les besoins en énergie et en climatisation.



Consolidation

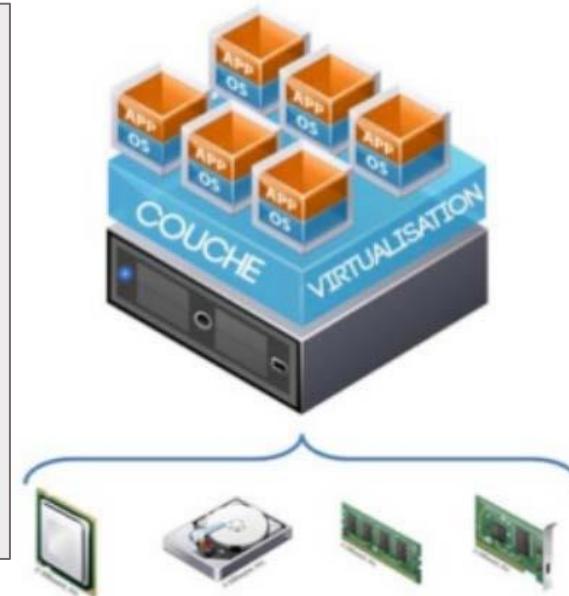
- Optimisation du taux d'utilisation des ressources des serveurs



Rationalisation

- Suppression des équipements superflus et redondants sans utilité.
 - Exemple le plus frappant : carte RAID, carte HBA, disques durs

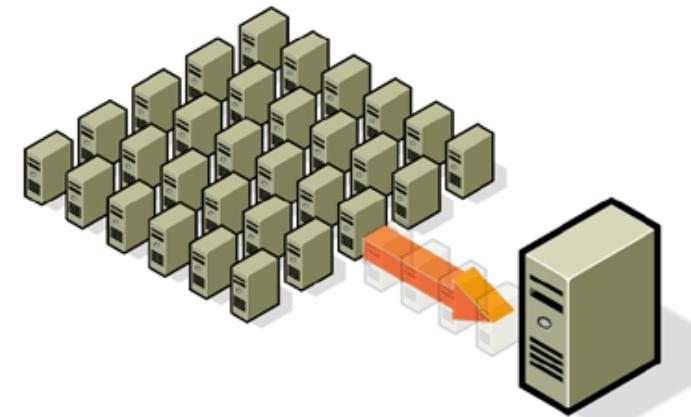
- Le fait de rationaliser l'infrastructure:
 - Réduit de façon rigoureuse le nombre de tous ces équipements matériels.
 - Réduit les couts financiers
 - Réduit le temps de gestion de ces équipements au quotidien
 - Simplifie l'architecture physique.



Un contrôleur HBA (Host Bus Adapter) est une carte d'extension qui permet de connecter un système hôte (serveur / poste de travail) à un bus externe réseau de stockage.

Concentration

- Utilisation des différents formats de serveurs :
 - Rack, Lames, Tours, Blade Center
- Réduction du besoin de place
- Réduction de l'espace occupé par les infrastructures serveurs



Virtualisation :

Avantages & inconvénients

Les avantages de la virtualisation

- **Réductions des coûts** : Economie possible jusqu'à 20 à 40% ou plus selon les cas.
 - **Réduction des coûts matériels** : Diminution du nombre de matériels nécessaire au bon fonctionnement de l'infrastructure.
 - **Réduction de la facture énergétique** : La rationalisation de l'infrastructure réduit la consommation électrique de l'ensemble ainsi que les besoins en climatisation.

Les avantages de la virtualisation

- **Amélioration de la qualité de Service :**
 - **Réduction du temps d'indisponibilité des applications critiques** : Les fonctionnalités évoluées de la virtualisation permettent de réduire les interruptions de services.
 - **Provisioning instantané** : permet de mettre en service un nouveau serveur facilement et en quelques minutes (exemple : par clonage de la machine).
 - **Répartition de charge dynamique** : La virtualisation permet de répartir dynamiquement la charge de travail en offrant à chaque application les ressources dont elle a besoin même en cas de fortes activités.
 - **Mise en place de PRA** : La virtualisation gère le système tout entier comme des fichiers totalement indépendants du matériel. La mise d'un PRA (Plan de Reprise d'Activité) en est grandement facilité.

Les avantages de la virtualisation

- **Simplification des tâches d'administration :**
Réduction du nombre d'équipement

+

Sauvegarde instantanée par snapshot

+

Homogénéité de l'infrastructure

=

Moins de maintenance

Simplification du travail

Meilleure maîtrise de l'infrastructure

Les inconvénients de la virtualisation

- Comme toute technologie, la virtualisation offre aux particuliers et aux entreprises des gains sur tous les plans.
- Cependant, des inconvénients et même des risques sont soulevés suite à l'utilisation de cette technologie.

Les inconvénients de la virtualisation

- Plusieurs environnements virtuels s'exécutent sur une unique machine physique, si cette machine tombe en panne, alors les services fournis par les environnements virtuels sont interrompus.
- Un recours à des machines puissantes : La virtualisation permet de réaliser des économies puisque moins de machines physiques sont nécessaires. Néanmoins, les outils de virtualisations sont des applications très gourmandes en ressources et nécessitent des machines puissantes.

Les inconvénients de la virtualisation

- Il est évidemment possible d'utiliser la virtualisation sur des machines plus modestes, mais un manque de mémoire ou de capacité CPU peut faire chuter les performances de manière dramatique.
- Une dégradation des performances : Bien qu'elle soit implémentée sur des machines puissantes, la virtualisation peut réduire les performances des applications.
 - Suivant le type de virtualisation envisagé, cette perte de performances peut ou non être significative.

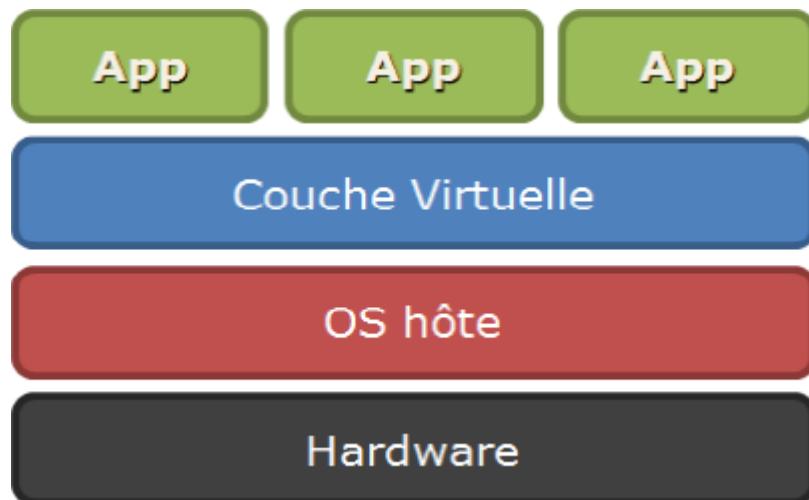
Les domaines de la virtualisation

Les domaines de la virtualisation

- La virtualisation se décompose concrètement en plusieurs domaines :
 - La **virtualisation des applications** : ou publication d'applications vise à permettre aux utilisateurs un accès à distance aux applications installées sur un serveur depuis n'importe quel poste de travail.
 - La **virtualisation de réseaux** : partager une même infrastructure physique réseau au profit de plusieurs réseaux virtuels isolés.
 - La **virtualisation du stockage** : séparer la présentation logique et réalité physique des ressources de stockage pour un accès aux ressources indépendamment des protocoles utilisés.
 - La **virtualisation des serveurs** : consiste à créer plusieurs "images" de serveurs sur un même serveur afin de mutualiser les ressources non utilisées.
 - La **virtualisation des postes de travail** : permet l'installation d'ordinateurs complets sur des serveurs.
 - ...

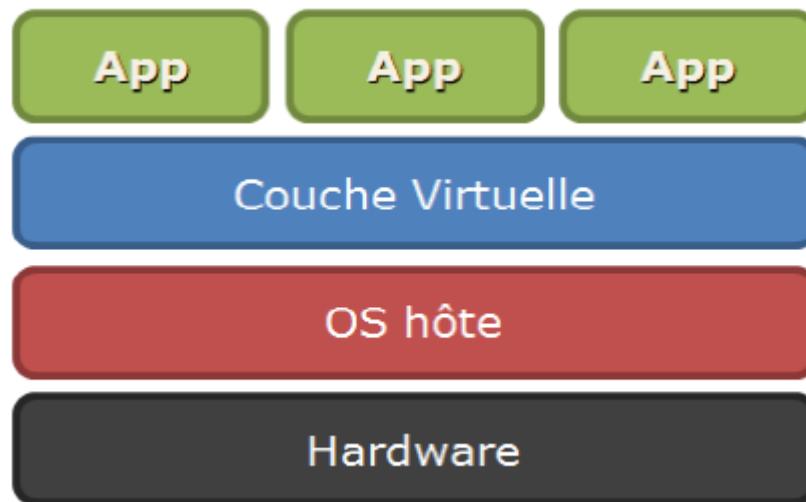
La virtualisation d'applications

- La **virtualisation d'application** est une technologie logicielle qui va permettre d'améliorer la portabilité et la compatibilité des applications en les isolant du système d'exploitation sur lequel elles sont exécutées.
- Elle consiste à encapsuler l'application et son contexte d'exécution système dans un environnement cloisonné.



La virtualisation d'applications

- La **virtualisation d'application** va nécessiter l'ajout d'une couche logicielle supplémentaire entre un programme donné et le système d'exploitation ;
- Le but est d'intercepter toutes les opérations d'accès ou de modification de fichiers ou de la base de registre afin de les rediriger de manière totalement transparente vers une localisation virtuelle (généralement un fichier).

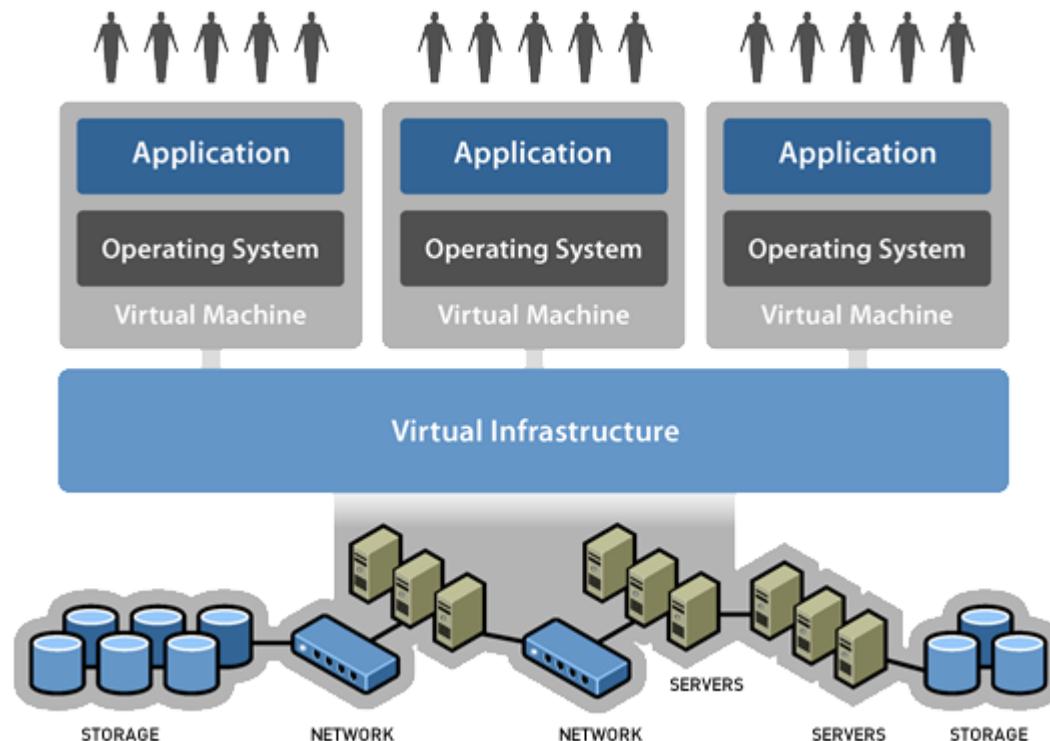


La virtualisation d'applications

- On peut dire que la couche virtuelle va ajouter des avantages au système virtualisé en permettant d'exécuter des applications conçues pour d'autres systèmes.
- **Exemple :**
 - Wine est un logiciel qui permet d'exécuter certains programmes Windows sous Ubuntu.
<http://www.winehq.org/>
- On peut aussi citer l'avantage gagné au niveau de la protection du système d'exploitation hôte en s'assurant que l'application virtualisée ne viendra pas interagir avec les fichiers de configuration du système.

La virtualisation de réseaux

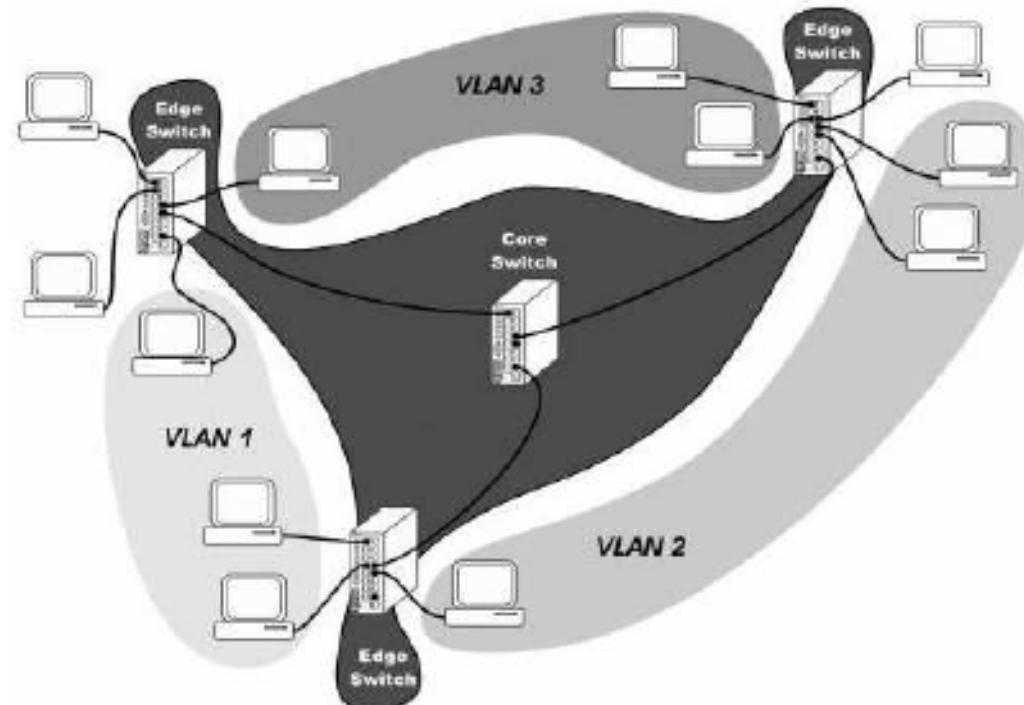
- La **virtualisation des réseaux** consiste à partager une même infrastructure physique (débit des liens, ressources CPU des routeurs,...) au profit de plusieurs réseaux virtuels isolés.



Virtualisation et stockage

La virtualisation de réseaux

- Un VLAN (***Virtual Local Area Network***) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
- Puisqu'un VLAN est une entité logique, sa création et sa configuration sont réalisées de manière logicielle et non matérielle.



La virtualisation de réseaux

- On distingue plusieurs types de réseaux virtuels :
 - **Les réseaux virtuels de niveau 1** : appelés réseaux virtuels par port (*port-based VLAN*)
 - **Les réseaux virtuels de niveau 2** : appelés réseaux virtuels par adresse MAC (*MAC address-based VLAN*)
 - **Les réseaux virtuels de niveau 3**: deux types de VLAN de niveau 3 :
 - **Les réseaux virtuels par adresse de sous-réseau** (*Network address-based VLAN*)
 - **Les réseaux virtuels par protocole** (*Protocol-based VLAN*)

La virtualisation de réseaux

- **Les réseaux virtuels de niveau 1 (*port-based VLAN*):**
 - Définissent un réseau virtuel en fonction des ports de raccordement sur le commutateur (*switch*).
 - Chaque port du commutateur est associé à un réseau virtuel, indépendamment de la machine qui y est physiquement raccordée.
 - Le principal inconvénient d'un VLAN de niveau 1 est sa rigidité:
 - si une station se raccorde physiquement au réseau par l'intermédiaire d'un autre port du commutateur, alors il est nécessaire de reconfigurer ce commutateur afin de réintégrer la station dans le bon réseau virtuel.

La virtualisation de réseaux

- **Les réseaux virtuels de niveau 2 (*MAC address-based VLAN*):**
 - Consistent à définir un réseau virtuel sur base des adresses MAC des stations.
 - Une adresse MAC est un identifiant unique implémenté dans chaque adaptateur réseau.
 - Ce type de VLAN est beaucoup plus souple que le précédent car il est indépendant de la localisation de la machine.

La virtualisation de réseaux

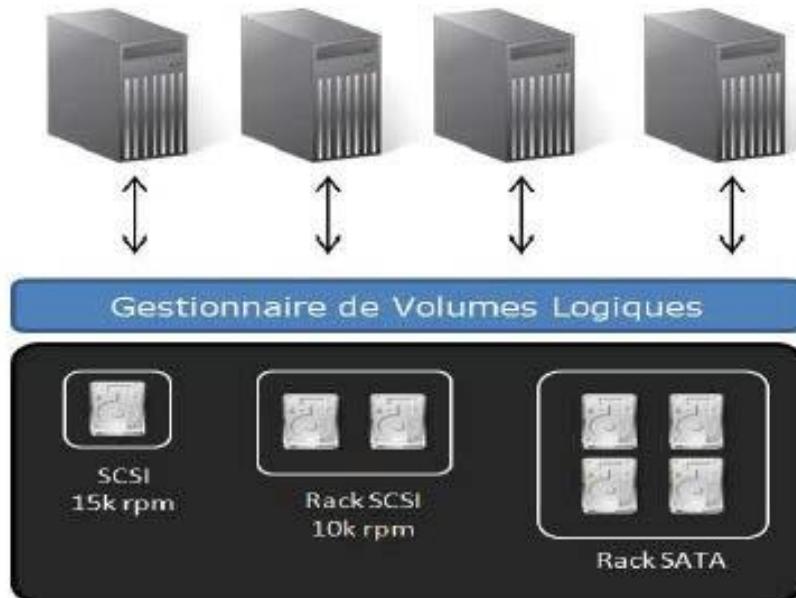
- **Les réseaux virtuels de niveau 3:** On distingue principalement deux types de VLAN de niveau 3 :
 - **Les réseaux virtuels par adresse de sous-réseau (*Network address-based VLAN*):**
 - ils déterminent les réseaux virtuels sur base de l'adresse IP source des segments.
 - Ce type de réseau virtuel est très flexible puisque les commutateurs adaptent automatiquement leur configuration lorsqu'une station est déplacée.
 - **Les réseaux virtuels par protocole (*Protocol-based VLAN*):**
 - Dans ce cas, les réseaux virtuels sont créés sur base des protocoles utilisés (TCP/IP, IPX,...) et les stations sont regroupées en réseaux virtuels suivant le protocole qu'elles utilisent.

La virtualisation de réseaux

- Les avantages qu'offrent les réseaux virtuels sont les suivants :
 - améliorer la sécurité
 - séparation des trafics
 - mise en place d'une politique d'accès
 - Faciliter la gestion des utilisateurs
 - ajout, déplacement
 - Améliorer la gestion des trafics
 - limiter le phénomène de broadcast sur le LAN
 - séparer les trafics selon la QoS

Virtualisation du stockage

- **Virtualisation du stockage** : est une technique qui sépare la représentation logique et la réalité physique de l'espace de stockage.
 - Son but est de faire abstraction des périphériques de stockage utilisé et des interfaces qui leur sont associés (SATA, SCSI,...) afin de limiter l'impact des modifications structurelles de l'architecture de stockage.



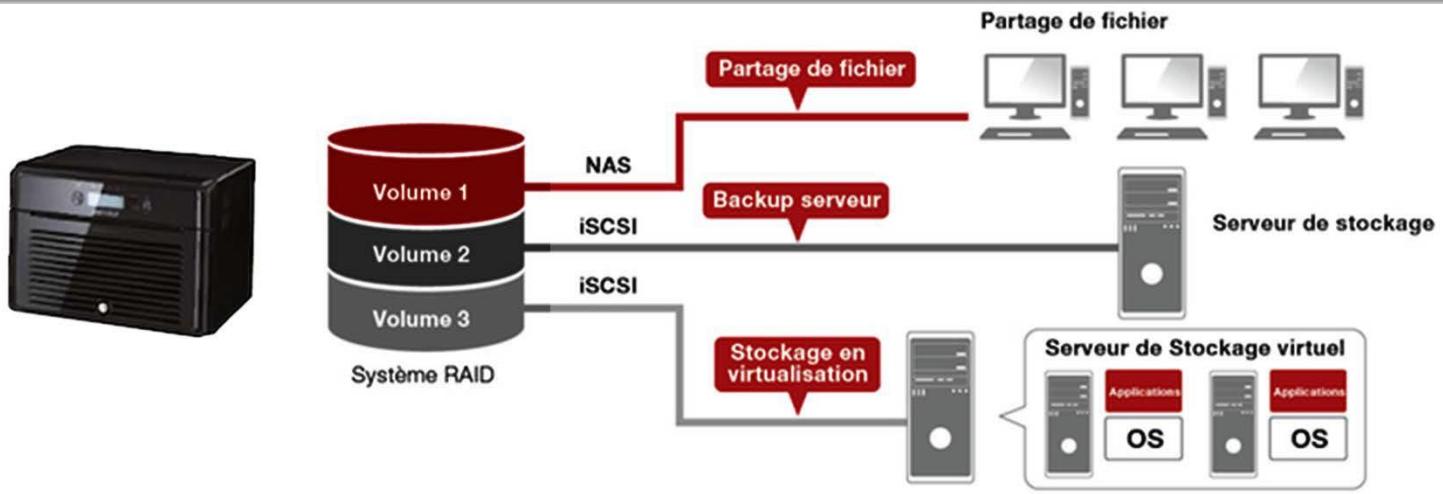
Virtualisation du stockage

- Ce type de virtualisation fait appel à une application d'administration de volumes logiques (Logical Volume Manager, LVM).
 - une couche logicielle qui va permettre de regrouper plusieurs espaces de stockage, appelés volumes physiques, pour ensuite découper cet espace global suivant la demande en partitions virtuelles appelées volumes logiques.
- Ce processus de virtualisation peut être vu comme une extension du modèle de partitionnement classique des disques dur.



Virtualisation du stockage

- La couche d'abstraction intermédiaire agit comme un courtier (*broker*) de capacité :
 - elle fournit de l'espace de stockage aux applications,
 - fait cohabiter des environnements hétérogènes dans une même représentation,
 - permet l'adjonction de capacité à la volée,
 - et laisse l'administrateur appliquer une politique unifiée de gestion des données.



Virtualisation du stockage

- Dans le cas d'un système de stockage, la virtualisation peut se faire de deux façons:
 - **Virtualisation en mode bloc (SAN)**, en introduisant un niveau d'abstraction entre le serveur et le système de stockage.
 - Les données en mode bloc sont accédées à travers des protocoles tels que Fibre Channel, iSCSI, SAS, FICON ou autres.
 - **Virtualisation en mode fichiers**, en accédant au **(NAS)** en masquant les dépendances vis-à-vis de l'emplacement où les données sont physiquement stockées.
 - L'accès en mode fichier se fait à travers NFS ou SMB.

Virtualisation du stockage

- **Fibre Channel** : protocole défini par la norme ANSI X3T11 permettant une connexion haut débit (de l'ordre du gigabit par seconde) entre un ordinateur et son système de stockage ou d'autre type de périphérique.
- **iSCSI (Internet Small Computer System Interface)** : protocole de stockage en réseau basé sur le protocole IP destiné à relier les installations de stockage de données.
- **SAS (Serial Attached SCSI)** : technique d'interface pour disques durs qui constitue une évolution des bus SCSI en termes de performances, et apporte le mode de transmission en série de l'interface SATA (Serial Advanced Technology Attachment).
- **FICON (FIber CONnection)** : nom déposé par IBM pour un protocole **Fiber Channel** normalisé de raccordement de systèmes par fibre optique.

Virtualisation du stockage

- **NFS (Network File System)** : système de fichiers en réseau, est à l'origine un protocole développé par Sun Microsystems en 1984 qui permet à un ordinateur d'accéder via un réseau à des fichiers distants.
 - Il fait partie de la couche application du modèle OSI et utilise le protocole RPC.
- **SMB (Server Message Block)** : protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.
 - Dans l'ancien Windows NT 4, il était appelé CIFS (Common Internet File System).
 - Dans Vista, Windows 7 et Windows 8, il est appelé SMB 2.

Virtualisation du stockage

- Utilisation : accessible par tout protocole
 - La virtualisation est une réponse à la gestion de la disparité des ressources de stockage : équipements, protocoles d'accès, environnements d'exploitation.
 - Elle permet à tout client (serveur, application, poste de travail) d'accéder à tout équipement de stockage par tout protocole.
 - Elle organise les ressources de stockage sous la forme d'une capacité unique, comme un disque de grande taille, qu'exploitent les applications.
 - Elle distribue les données en mode bloc sur l'infrastructure de stockage, en appliquant les politiques de gestion définies par l'administrateur (réPLICATION, sauvegarde, mirroring distant, caches...).

Virtualisation du stockage

- Utilisation : accessible par tout protocole
 - La virtualisation fait du stockage un système indépendant de l'applicatif.
 - Il devient possible de différer une sauvegarde en la conservant sur disque, d'améliorer les performances d'accès aux données, de repenser le ***striping Raid*** ou d'ajouter de la capacité sans interférer avec la production.
 - Elle allège aussi le coût élevé de la gestion du stockage.
 - La virtualisation permettrait de réduire ces coûts de gestion de 30 à 50 % selon la complexité de l'infrastructure installée.
 - Reste que la virtualisation manque de standards et d'une définition unifiée.
 - Parfois limitée au SAN, aux disques, ou à la sauvegarde, elle devrait pourtant s'étendre à terme à l'ensemble des opérations et des ressources de stockage : DAS, NAS et SAN.

Virtualisation du stockage

- Les disques virtuels peuvent être statiques ou dynamiques.
 - Dans le cas où le disque est statique, si on crée un disque de 50 Go, le fichier de disque virtuel fera 50 Go sur le système hôte.
 - Avec un disque dynamique, le fichier de disque virtuel se remplit au fur et à mesure qu'il est utilisé.
 - Un disque de 50 Go dans lequel il n'y a pas de données ne pèsera dans le système de fichiers hôte grande chose.

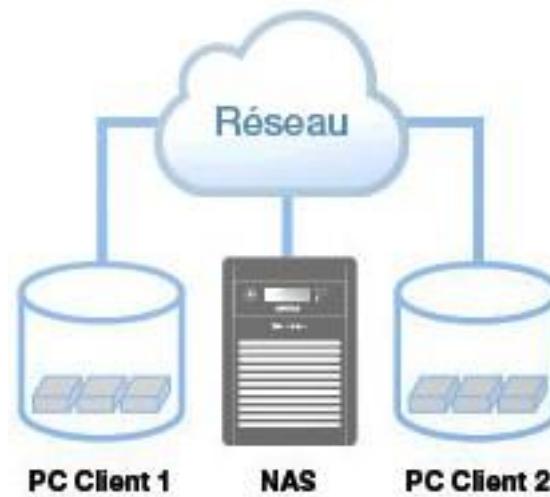
Virtualisation du stockage

- La virtualisation de stockage permet :
 - d'adjoindre un périphérique de stockage supplémentaire sans interruption des services;
 - de regrouper des unités de disques durs de différentes vitesses, de différentes tailles et de différents constructeurs ;
 - de réallouer dynamiquement de l'espace de stockage : Ainsi, un serveur nécessitant un espace de stockage supplémentaire pourra rechercher des ressources non allouées sur le disque logique. Inversement, un serveur nécessitant moins d'espace de stockage pourra libérer cet espace et le rendre disponible pour d'autres serveurs.

Technologie de stockage

- **NAS (Network Attached Storage)** : support de stockage de données de l'ordinateur au niveau des fichiers*, relié à un réseau informatique fournissant un accès aux données à un groupe hétérogène de clients.

Network Attached Storage



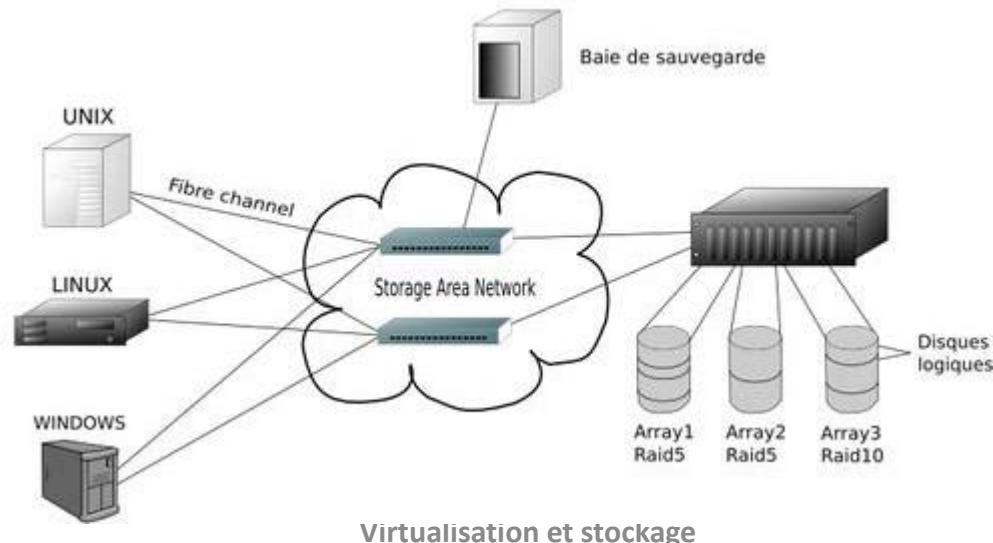
"**Niveau de fichier**" signifie qu'un NAS reçoit des données sous la forme de fichiers envoyés par un client sur le réseau.

Technologie de stockage

- **NAS** opère non seulement comme un serveur de fichiers, mais il est spécialisé pour cette tâche.
- Par conséquent, le NAS fournit à la fois une capacité de stockage et un système de fichiers interne pour stocker les fichiers reçus.
- Le trafic de données entre les clients et le NAS est basé sur des protocoles, tels que :
 - SMB/CIFS (Server Message Block /Common Internet File System)
 - FTP (File Transfer Protocol)
 - NFS (Network File System)

Technologie de stockage

- **SAN (Storage Area Network)** : réseau dédié qui fournit un accès à un stockage de données consolidé en mode bloc.
- Les **SAN** sont principalement utilisés pour créer des périphériques de stockage tels que des baies de disques accessibles aux serveurs afin que les périphériques apparaissent comme des périphériques localement attachés au système d'exploitation.



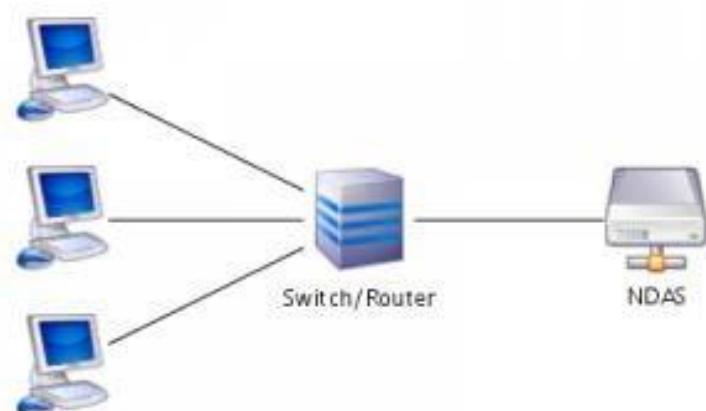
Technologie de stockage

- **DAS (Direct Attached Storage)** : terme utilisé pour un système de disque en attachement direct, par opposition au NAS qui est en attachement réseau.
- Le système disque ainsi installé n'est accessible directement qu'aux ordinateurs auquel il est raccordé, le plus souvent en protocole USB.



Technologie de stockage

- **NDAS (Network Direct Attached Storage)** : une sorte de NAS, autrement dit, un système de disque réseau.
- Il diffère de NAS car il faut installer un logiciel NDAS sur chaque poste pour accéder au disque réseau.
- Le disque est vu comme un disque local par chaque machine.
- L'accès se fait sans passer par TCP/IP, mais directement par l'adresse MAC.
- Le protocole utilisé est LPX.



Technologie de stockage

- D'habitude, le périphérique de stockage du SAN est généralement inaccessible via le réseau local par les autres périphériques, ce qui constitue l'effet inverse d'un NAS.
- Les SAN utilisent généralement iSCSI. Ce protocole permet aux clients (appelés « initiateurs ») d'envoyer des commandes aux périphériques de stockage iSCSI (cibles) sur des serveurs distants.
- Les entreprises peuvent ainsi consolider le stockage dans des baies de stockage sur datacenter tout en fournissant des hôtes (comme des serveurs de base de données et Web), comme s'il s'agissait de disques attachés en local.

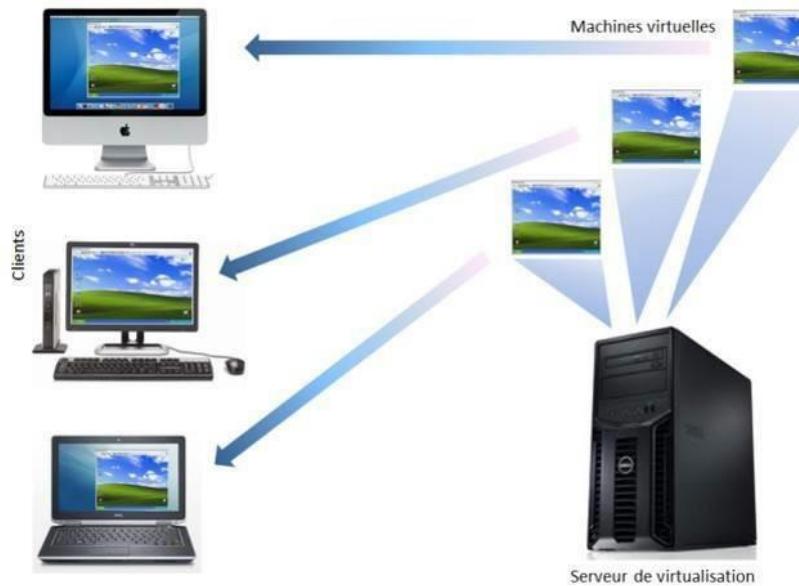
La virtualisation de serveurs

- La **virtualisation de serveur** est un principe permettant de faire fonctionner simultanément, sur un seul serveur physique, plusieurs serveurs virtuels.
- Cette technique permet aux entreprises d'utiliser des serveurs virtuels en lieu et place de serveurs physiques.
- Si cette virtualisation est faite au sein de la même entreprise, le but est de mieux utiliser la capacité de chaque serveur par une mise en commun de leur capacité.



La virtualisation des postes de travail

- La virtualisation du poste de travail (*VDI : Virtual Desktop Infrastructure*) fait partie de la grande famille de la virtualisation avec celle dédiée aux serveurs et au stockage.
- Le grand principe de la virtualisation du poste de travail consiste à afficher sur un, des dizaines, centaines voire des milliers de postes physiques, une image virtuelle du poste utilisateur qui est en fait réellement exécutée sur un serveur distant.



La virtualisation des postes de travail

- Derrière ce grand principe, on trouve cependant plusieurs formes de virtualisation du poste de travail.
- La plus ancienne est celle de la virtualisation d'applications centralisée (*Server Based Computing*), consistant à virtualiser les applications mais pas l'ensemble du système d'exploitation.
- Alors que l'utilisateur visualise (et utilise) sur son poste une image des applications réellement exécutées sur un serveur distant, le système d'exploitation, lui, tourne toujours sur le poste client.
- Une variante existe qui est celle de la virtualisation d'applications par isolation.

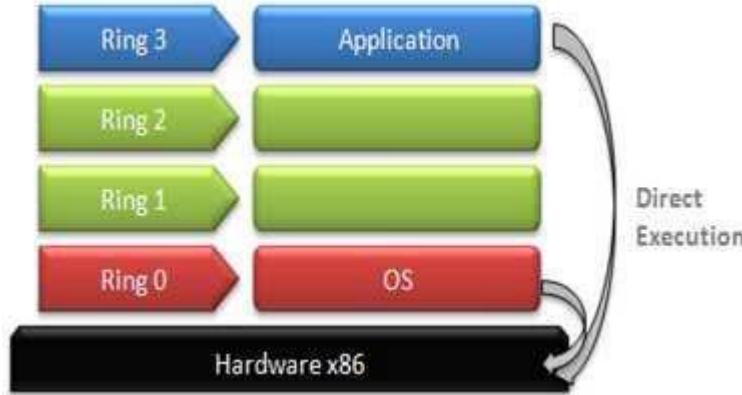
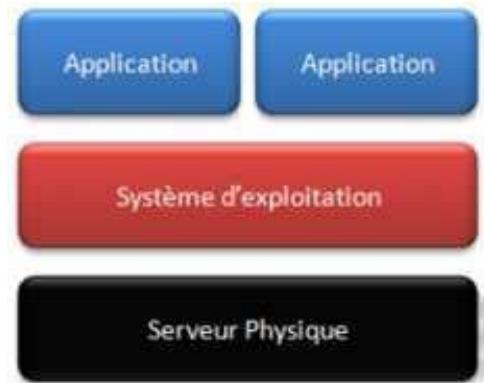
La virtualisation des postes de travail

- **Avantages de la virtualisation de postes de travail**
 - **Economie** : Le fait de remplacer les PC classiques par des points d'accès permet de diminuer les coûts de possessions.
 - **Ecologie** : Le VDI permet de faire des économies d'énergie (extinction programmée de tout le parc). Un PC lourd consomme 100 Watt, un point d'accès seulement 20 Watt, globalement la virtualisation des postes de travail permet jusqu'à 80% d'économie d'énergie, argument intéressant dans le cadre d'une démarche RSE.
 - **Simplicité** : Le VDI permet de faciliter le travail du service informatique en centralisant la gestion du parc (création d'une image pour 100 ou 200 utilisateurs par exemple). La maintenance est donc très facilité.
 - **Sécurité** : Le VDI permet l'homogénéité du parc informatique, possibilité de faire des machine Read Only → retour à l'état du Master à chaque démarrage donc plus aucun virus à chaque démarrage.

Théorie sur la virtualisation de serveurs

Théorie sur la virtualisation de serveurs

- Architecture classique sur un serveur traditionnel :



- Le système d'exploitation, et plus précisément le noyau (kernel-mode) s'exécute avec un niveau de privilège de ring 0.
- Les applications (user-mode) s'exécutent quant à elles au niveau du ring 3.
- Un processus de ring 0 est autorisé à manipuler un processus de ring 3.
- L'inverse n'est pas possible.
- En effet, le système d'exploitation est autorisé à lancer, contrôler, et à stopper une application.
- Une application ne peut contrôler le système d'exploitation.

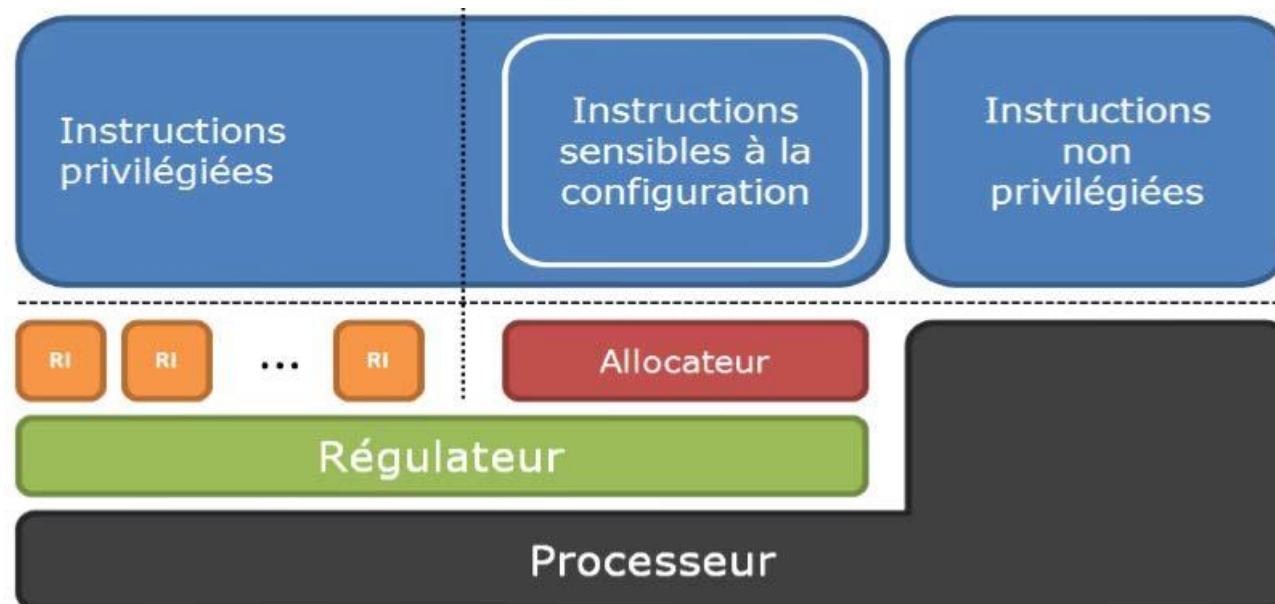
Théorie sur la virtualisation de serveurs

- La virtualisation de serveur apporte une couche de virtualisation offrant la possibilité d'exécuter plusieurs environnements virtuels, tout en assurant leur isolation.
- On appelle ces environnements virtuels des « machines virtuelles » ou encore VM (Virtuel Machine).
- Les systèmes d'exploitation installés dans une machine virtuelle sont appelés « Guest OS ».



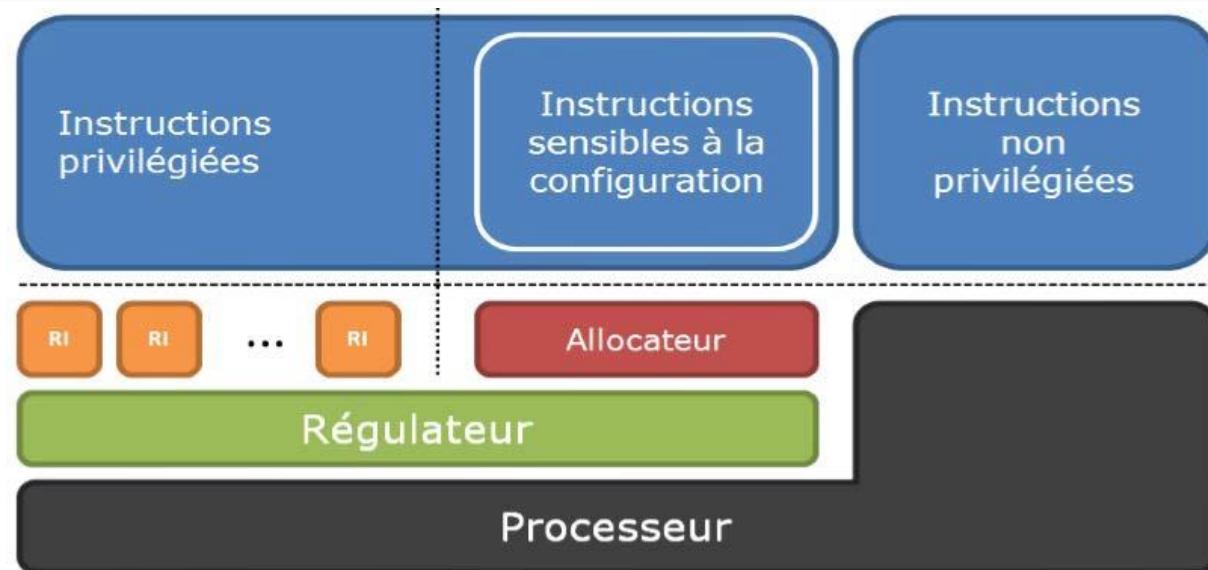
Hyperviseur

- L'hyperviseur (aussi appelé VMM pour *Virtual Machine Monitor*) est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une machine physique en même temps.
- C'est bien une couche logicielle qui s'insère entre le matériel et les différents systèmes d'exploitation.



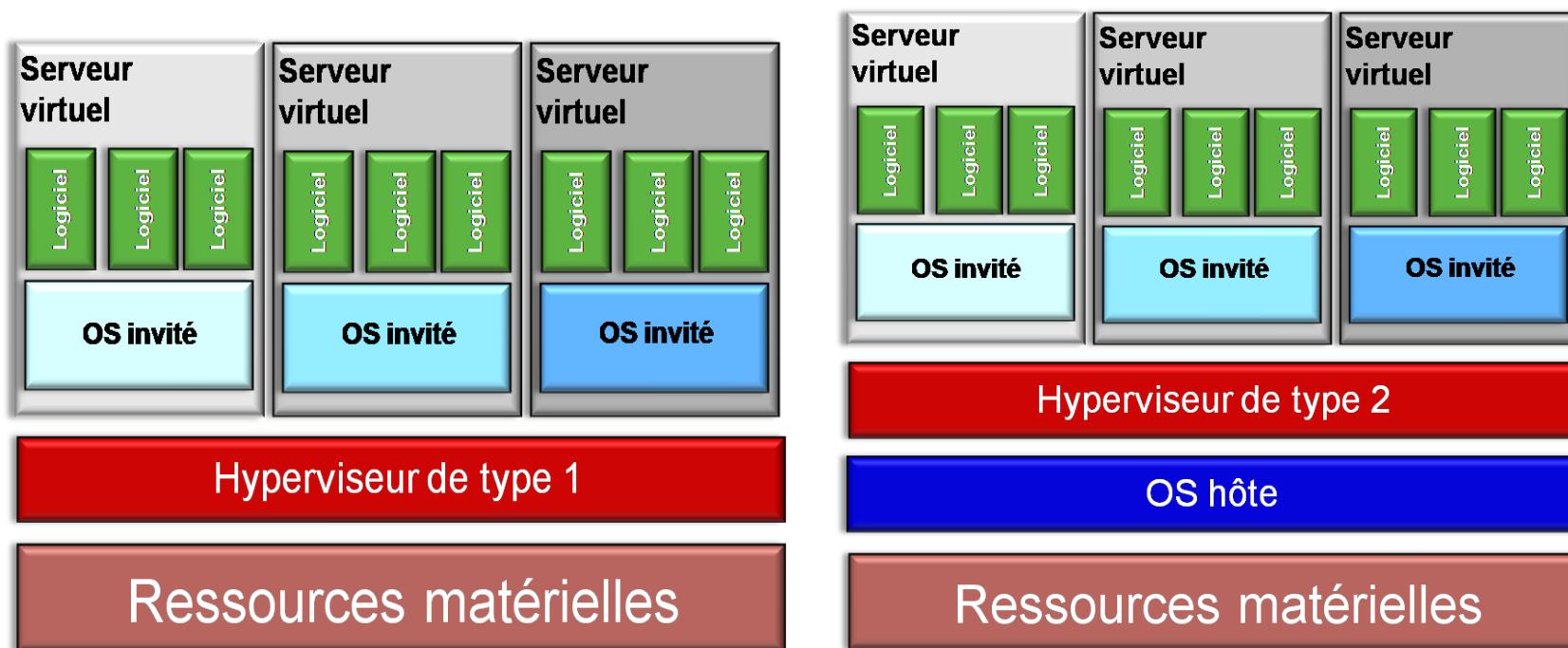
Composants d'un hyperviseur

- **Les modules d'un hyperviseur peuvent être regroupés en trois catégories :**
 - **Le régulateur (dispatcher)** : il peut être considéré comme le module de contrôle de plus haut niveau de l'hyperviseur.
 - **L'allocateur** : son rôle est de déterminer quelle(s) ressource(s) doivent être allouées aux applications virtualisées.
 - **Des interpréteurs** : à chacune des instructions privilégiées (à l'exception de celles qui sont prises en charge par l'allocateur), on va associer une routine d'interprétation.



Types d'hyperviseur

- Il existe deux types d'hyperviseurs :
 - Un hyperviseur de type I
 - Un hyperviseur de type II



Types d'hyperviseur

- **Un hyperviseur de type I** : (natif ou bare metal) est un logiciel qui s'exécute directement sur une plateforme matérielle donnée (comme outil de contrôle de système d'exploitation).
 - Il doit gérer lui-même toutes les ressources matérielles du serveur et propose ainsi des machines virtuelles aux systèmes invités.
 - Il implémente donc la plupart des services que fournissent les noyaux des systèmes d'exploitation.
 - Un système d'exploitation secondaire peut de ce fait être exécuté au dessus du hardware.

Exemples

- Xen de The Xen Project, XenSource, Inc.
- VMware : propriétaire, hyperviseur sur plateforme x86 (produits *ESX* et *ESXi*)
- Microsoft Hyper-V Server : propriétaire (Microsoft), hyperviseur sur plateforme x64 uniquement.

Types d'hyperviseur

- **Un hyperviseur de type II** : ou appelé host-based est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation.
 - Un système d'exploitation invité s'exécutera donc en troisième niveau au dessus du hardware (matériel).
 - Ce logiciel permet de lancer un ou plusieurs OS invités.

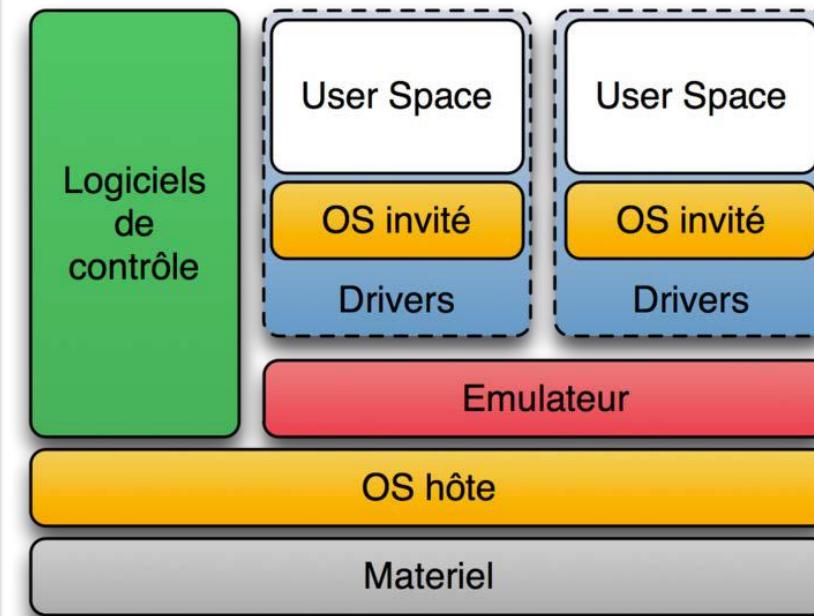
Exemples

- Microsoft VirtualPC et Microsoft VirtualServer : propriétaire, émulateur de plateforme x86
- VirtualBox : émulateur de plateforme x86.
- VMware : propriétaire, émulateur de plateforme x86 (produits VMware Server, VMware Player et VMware Workstation).

Types d'hyperviseur

- **L'émulateur (cas spécifique)** : il consiste à utiliser un système d'exploitation (ou un programme) sur un système qui n'utilise pas la même architecture.

- Les émulateurs sont soit externes (des programmes) soit intégrés au système.
- L'émulation est la technique qui offre le plus haut niveau d'abstraction de la plateforme.
- Pour les autres techniques de virtualisation tous les exécutables doivent être compilés pour le processeur physiquement disponible sur le serveur.
- Le projet QEMU est une solution open source de virtualisation par émulation.



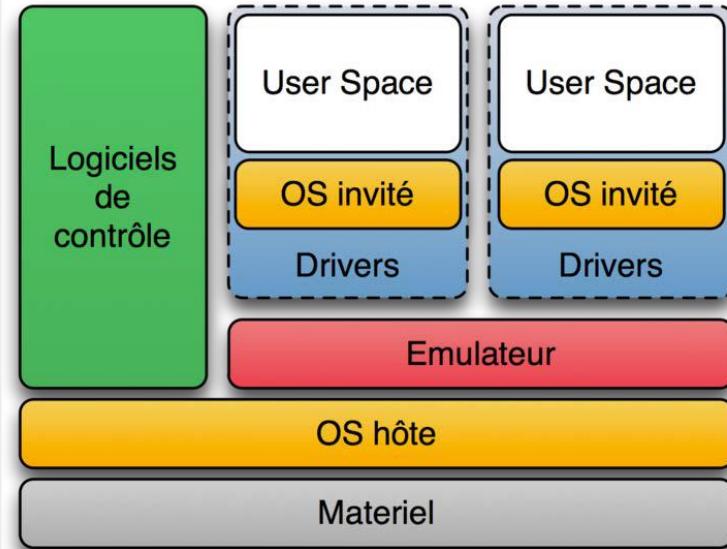
Les méthodes de virtualisation

Les méthodes de virtualisation

- La virtualisation doit s'adapter aux différentes briques technologiques d'une infrastructure.
- 3 variantes d'architecture de virtualisation existent:
 - **L'émulateur**
 - **L'isolateur**
 - **L'hyperviseur et para-virtualisateur**

L'émulateur ou partitionnement

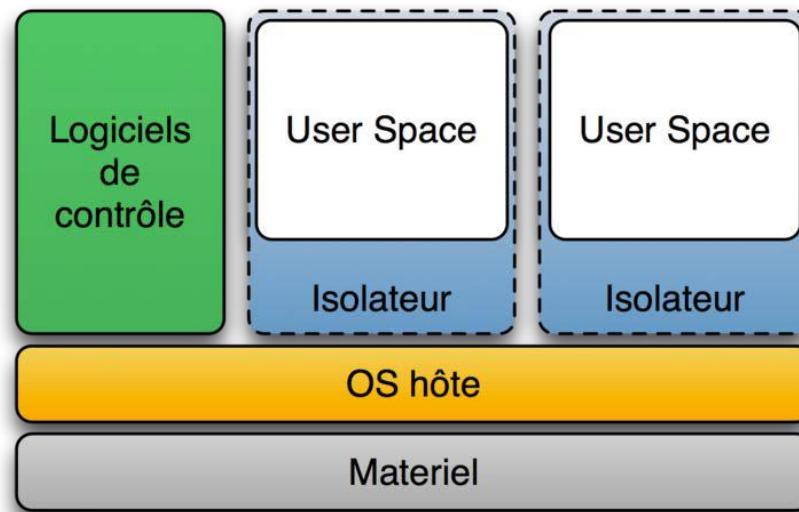
- **Emulation ou partitionnement:**
 - L'émulation consiste à simuler l'exécution d'un programme en interprétant chacune des instructions destinées au micro-processeur.
- **Avantages:**
 - Facilité de mise en œuvre et d'utilisation,
 - très bonne compatibilité d'OS
- **Inconvénients:**
 - Mauvaises performances, matériel émulé



Faire fonctionner de multiples MV en même temps sur un même serveur physique

L'isolateur

- Un isolateur est une couche logicielle permettant d'isoler des applications dans ces contextes d'exécution différentes.
- L'isolateur permet ainsi de faire tourner plusieurs fois la même application dans un mode multi-instance (plusieurs instances d'exécution) même si elle n'était pas conçue pour ça.

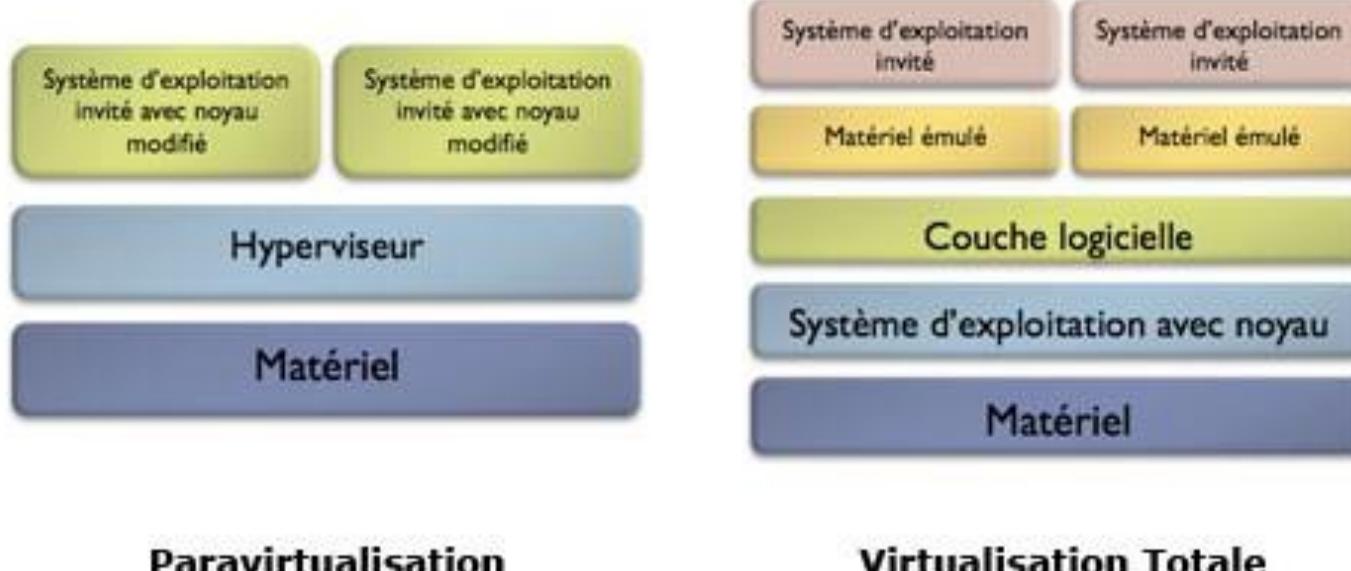


L'isolateur

- L'isolation permet de séparer un système en plusieurs contextes ou environnements. Chacun d'entre eux est régi par l'OS hôte, mais les programmes de chaque contexte ne peuvent communiquer qu'avec les processus et les ressources associées à leur propre contexte
- **Exemple :** Linux-VServer (isolation des processus en espace utilisateur) ; chroot (isolation changement de racine) ; BSD Jail (isolation en espace utilisateur) ; OpenVZ : libre, (partitionnement au niveau noyau sous Linux) ; LXC : libre, (usage des Cgroups du noyau Linux).

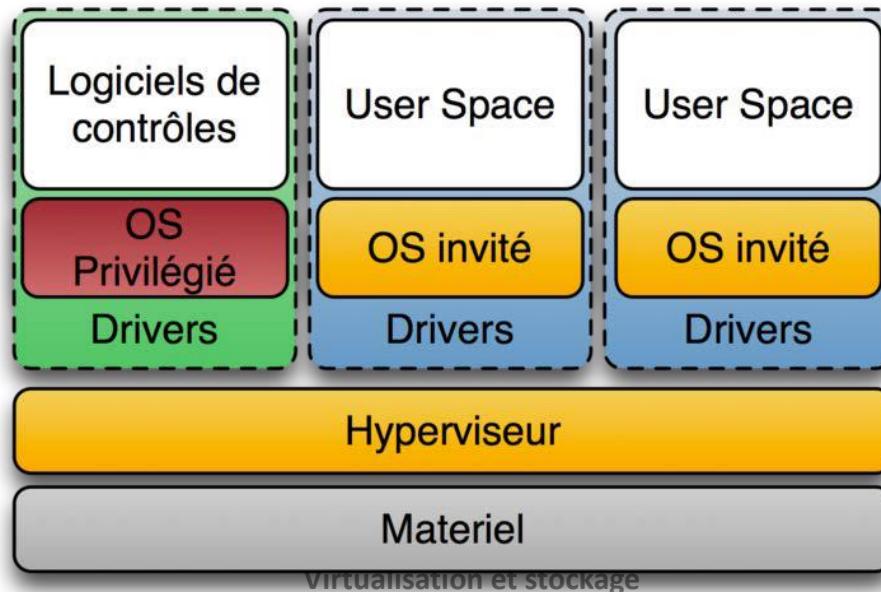
L'hyperviseur / Paravirtualisateur

- **La paravirtualisation** adopte une vision radicalement différente.
- Au lieu de chercher à faire croire aux systèmes d'exploitation qu'ils s'exécutent sur une machine physique, il est possible d'adapter le système d'exploitation à la couche de virtualisation.



L'hyperviseur / Paravirtualisateur

- **L'hyperviseur** intègre son propre OS (ou micro OS) de taille réduite et de préférence peu consommateur en ressources.
 - VMware ESX, HyperV, Xen Citrix
- **L'Hyperviseur** alloue aux machines virtuelles des ressources matérielles:



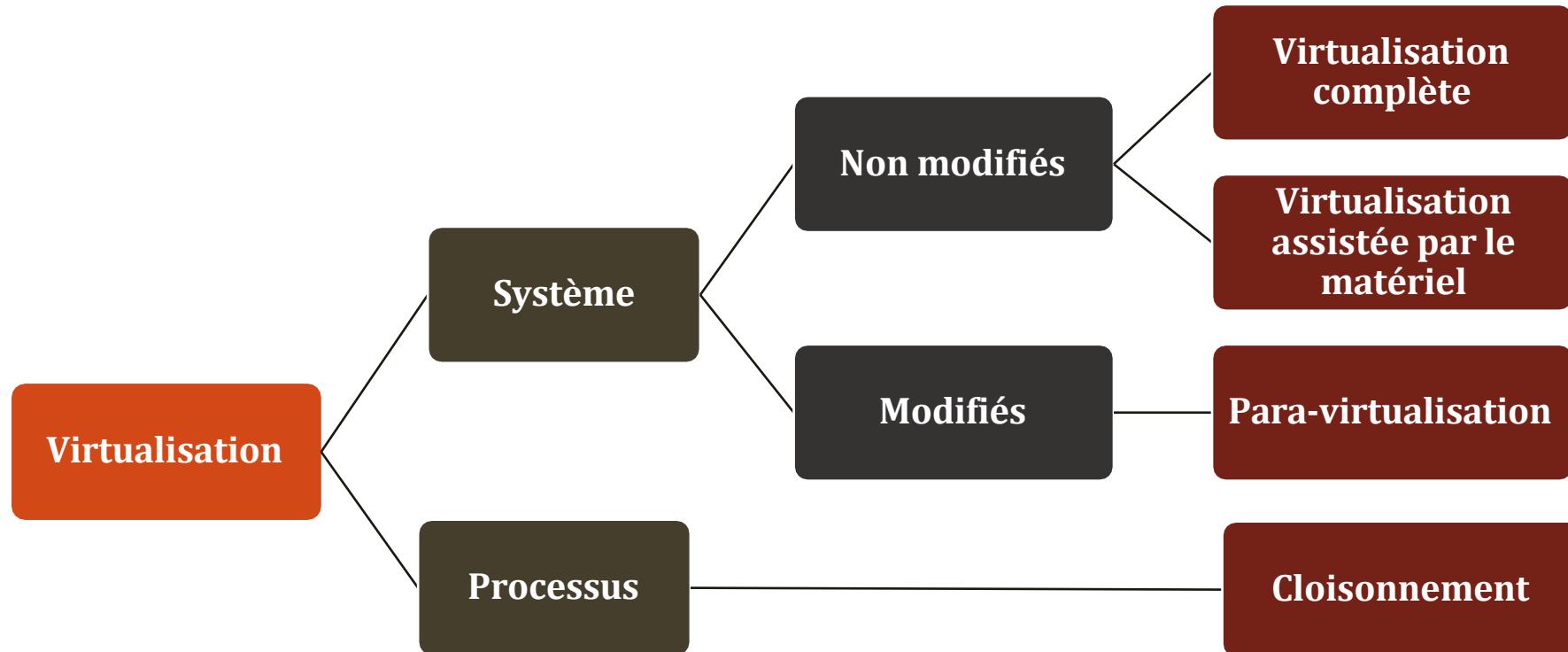
Les différents types de virtualisation

Les différents types de virtualisation

- Tout d'abord, il existe plusieurs catégories de virtualisation, utilisant chacune des technologies différentes.
- Les technologies les plus répandues sont :
 - la virtualisation complète ;
 - la para-virtualisation ;
 - la virtualisation assistée par le matériel ;
 - le cloisonnement.

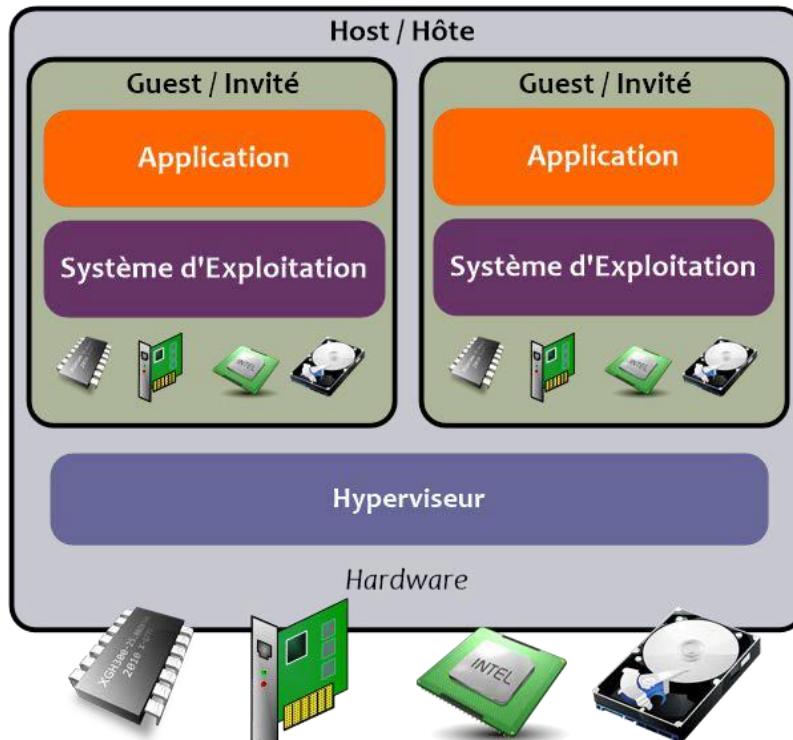
Les différents types de virtualisation

- On peut classer les différents types de virtualisation selon le modèle suivant :



La virtualisation complète

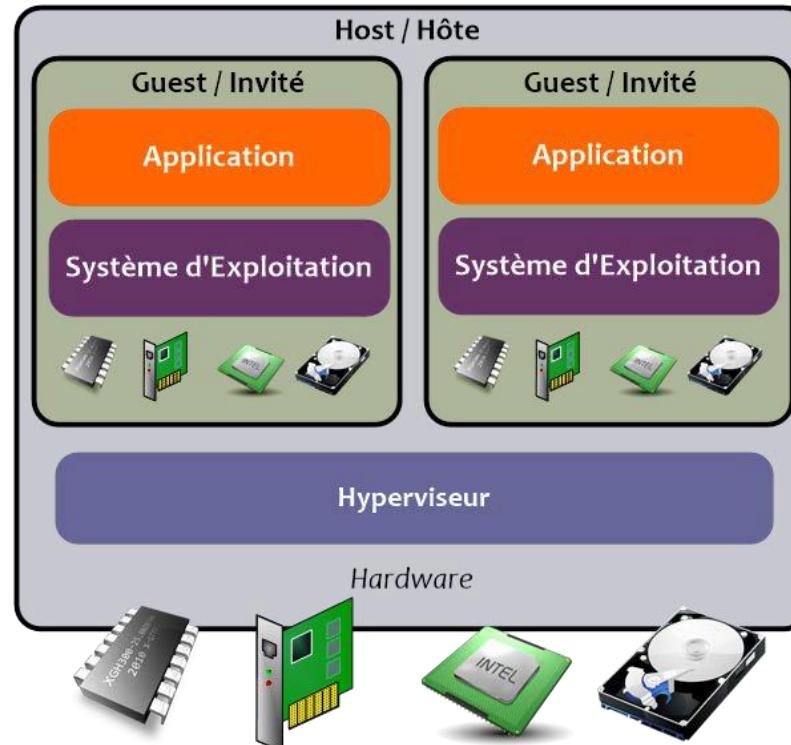
- **La virtualisation complète (*full virtualization*):** consiste à créer des environnements virtuels qui sont une copie d'une machine physique (mémoire, disques,...) pour le système invité.



Virtualisation et stockage

La virtualisation complète

- Le **système invité** « croit » s'exécuter sur une véritable machine physique.
- Le logiciel chargé d'émuler cette machine s'appelle une **machine virtuelle**, son rôle est de transformer les instructions du système invité en instructions pour le système hôte.

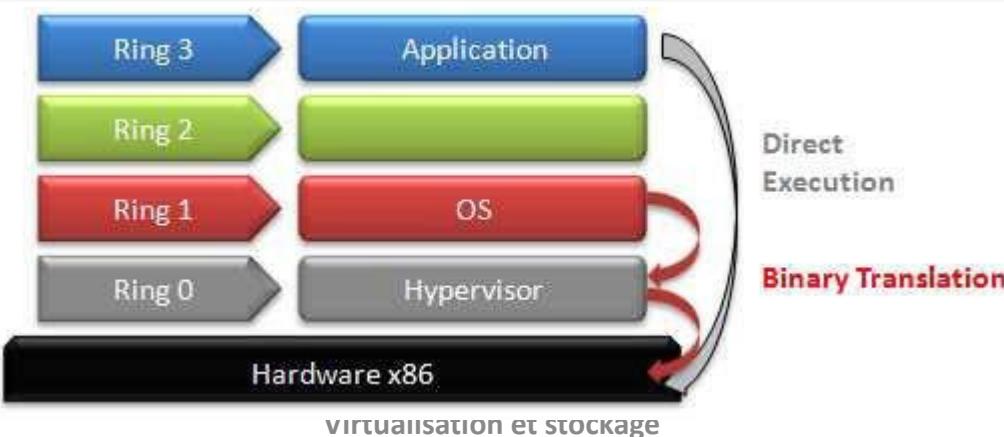


La virtualisation complète

- Le système s'exécutant dans la machine virtuelle est un système d'exploitation à part entière, tel qu'on pourrait en installer sur une machine physique :
 - Microsoft Windows, GNU/Linux, Mac OS X, etc.
- Cette particularité est la caractéristique principale de la virtualisation complète :
 - les systèmes invités n'ont pas à être modifiés pour être utilisés dans une machine virtuelle utilisant une technologie de virtualisation.
- Dans la pratique, c'est le cas pour les systèmes d'exploitation et les machines virtuelles les plus répandus.

La virtualisation complète

- Les machines virtuelles se basent sur deux principes :
 - **la traduction binaire des instructions que le noyau du système virtualisé souhaite exécuter:** La traduction binaire repose donc sur un travail d'analyse des instructions exécutées par le noyau du système invité. Cette traduction peut s'avérer indispensable pour assurer le maintien de la stabilité du système dans sa globalité.
 - **l'exécution directe des instructions relatives aux applications utilisateurs:** Les instructions utilisateurs sont quant à elles exécutées directement car l'hyperviseur fait la supposition qu'elles ne sont pas dangereuses pour le système. Elles s'exécutent donc comme s'il n'existe aucune couche de virtualisation.



La virtualisation complète

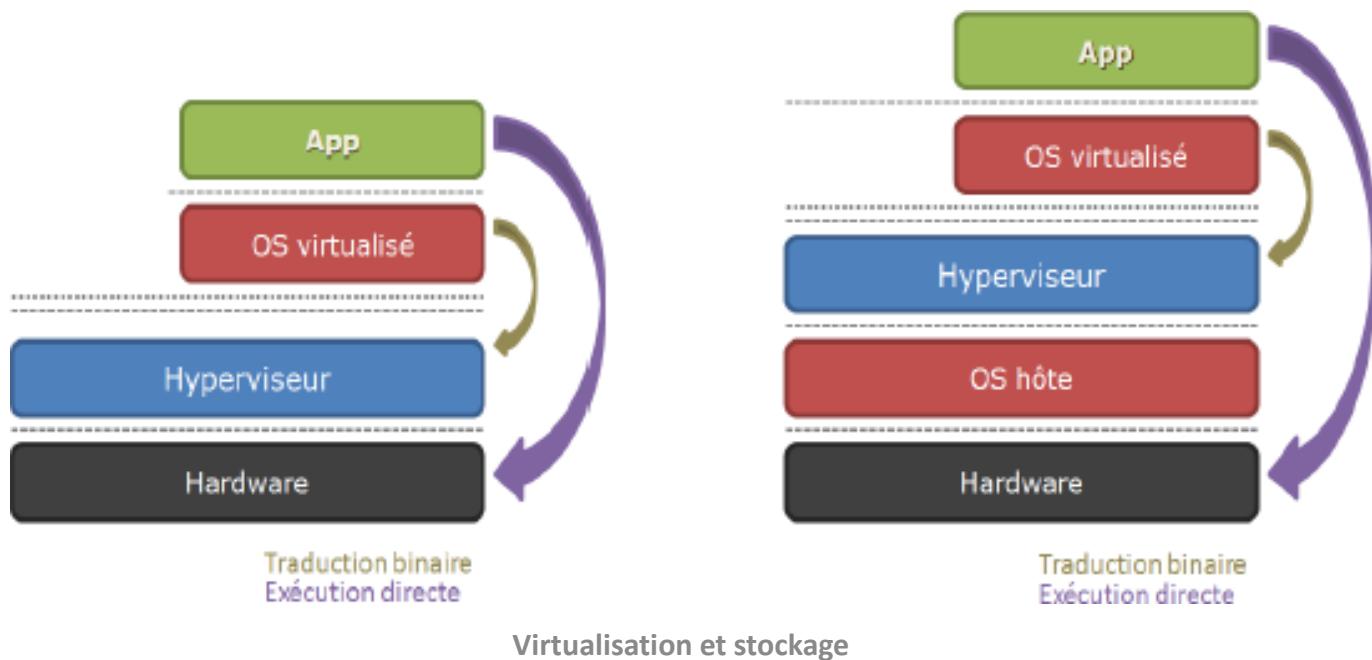
- Cette technique fournit un environnement matériel virtuel représentant une architecture réelle.
- Cela consiste donc à émuler l'intégralité d'une machine physique.
- Cette technique de virtualisation est gérée par un logiciel que l'on nomme « l'hyperviseur ».
 - Celui-ci s'occupe de la gestion des accès mémoire, les processus et les fonctions proches du matériel réel.

La virtualisation complète

- **Avantages :**
 - permet de faire fonctionner plusieurs systèmes différents sur la même machine physique.
 - meilleures performances que l'émulation du fait de l'accès plus rapide au matériel.
- **Inconvénients :**
 - consommation importantes des ressources (la consommation est fonction du nombre de machines virtuelles).
 - les performances ne sont pas optimales dans l'usage de certains périphériques: type carte accélératrice 3D. De plus, il y a réduction des systèmes d'exploitation virtualisables.
- **Utilisations :**
 - Faire tourner des systèmes d'exploitation virtuellement en les laissant accéder aux différents périphériques au travers des pilotes installés sur le système hôte. Des logiciels tels que VMWare Workstation ou VirtualPC de Microsoft l'utilisent.

La virtualisation complète

- Il existe deux types de virtualisation complète : celles où l'hyperviseur est une application installée sur un système d'exploitation hôte, et celles où l'hyperviseur est installé en lieu et place du système d'exploitation hôte.
- A gauche, l'hyperviseur gère lui même le hardware sous jacent; à droite, l'hyperviseur transmet les requêtes aux systèmes d'exploitation hôte



La virtualisation complète

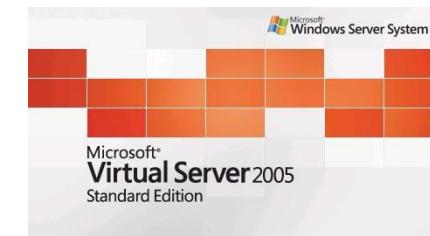
- **Exemples :**
 - **Microsoft VirtualPC et Microsoft VirtualServer** : propriétaire, émulateur de plateforme x86
 - **Parallels** : propriétaire, superviseur x86 pour MAC OSX(Intel)
 - **VirtualBox** : émulateur de plateforme x86
 - **VMware** : propriétaire, émulateur de plateforme x86 (VMware Server, VMware Player, VMware Workstation, VMware Fusion)



VirtualBox

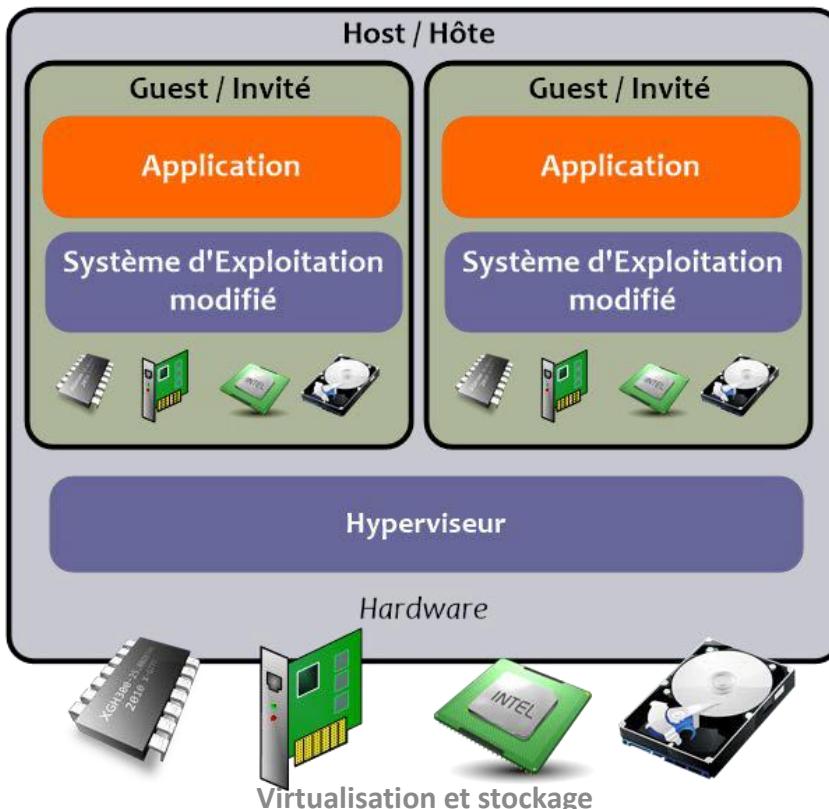


Virtualisation et stockage



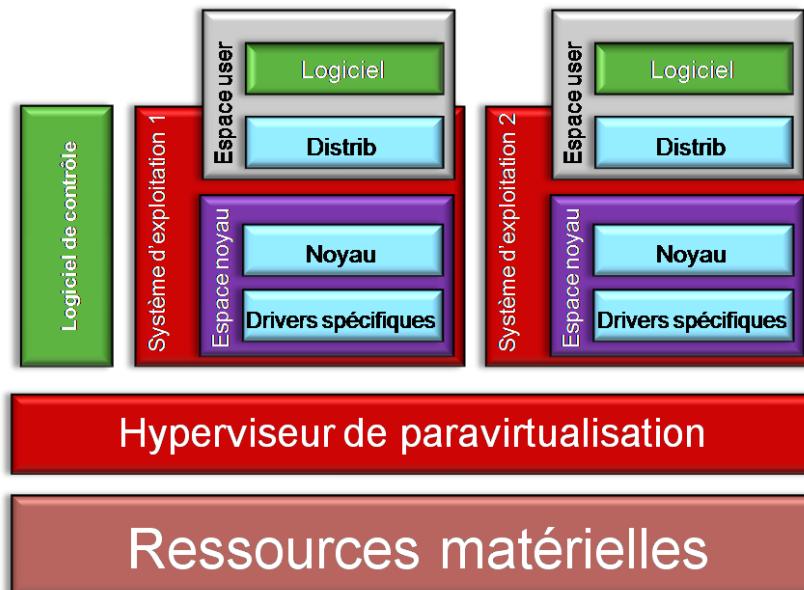
La para-virtualisation

- La **para-virtualisation** : très proche du concept de la **virtualisation complète**, dans le sens où c'est toujours un système d'exploitation complet qui s'exécute sur le matériel émulé par une **VM**, cette dernière s'exécutant au dessus d'un système hôte.



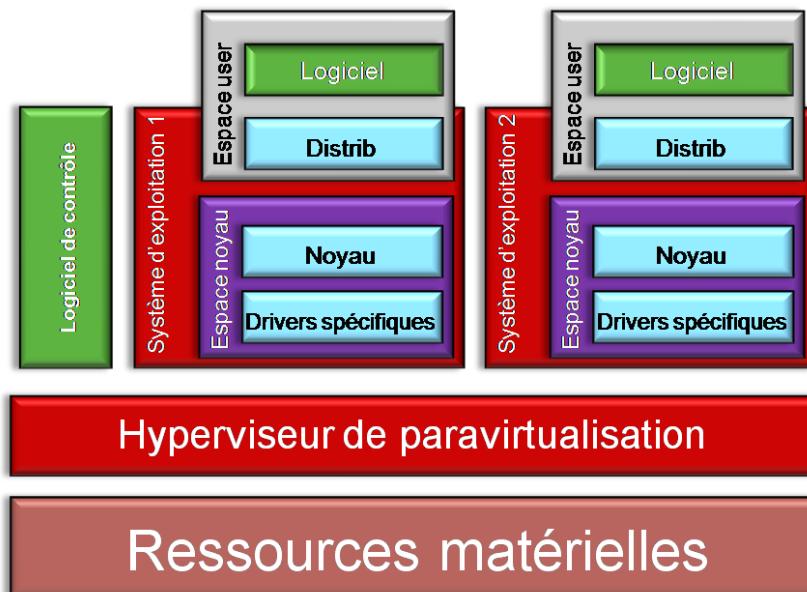
La para-virtualisation

- Toutefois, dans une solution de **para-virtualisation**, le système invité est modifié pour être exécuté par la VM.
- Elle s'appuie sur une couche hyperviseur, qui gère totalement l'interface avec les ressources matérielles, et sur laquelle on peut installer différents systèmes d'exploitations.



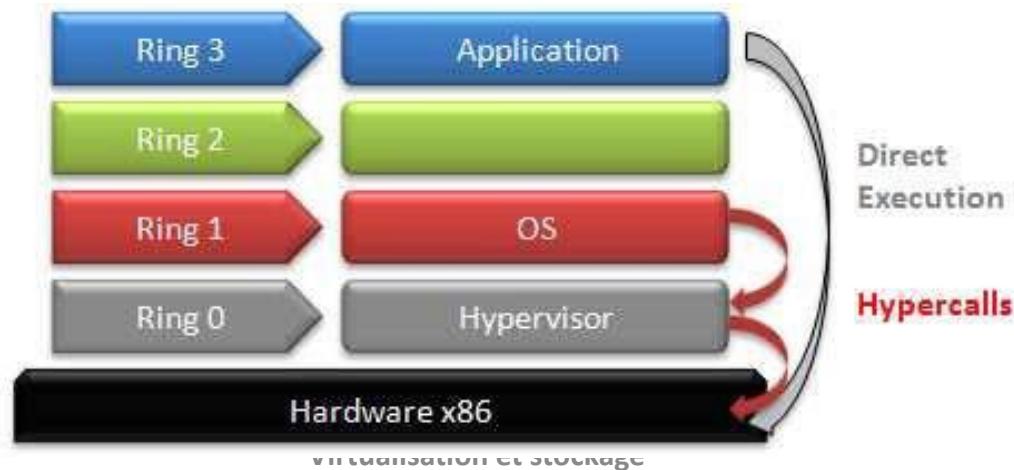
La para-virtualisation

- Contrairement à la virtualisation complète, il y a une collaboration directe entre l'hyperviseur et ses systèmes « invités ».
- C'est pourquoi, les systèmes d'exploitation « invités » doivent subir une modification pour communiquer directement avec un hyperviseur au lieu de communiquer avec une machine physique.



La para-virtualisation

- La para-virtualisation implique une modification du noyau du système d'exploitation virtualisé afin de remplacer les instructions non virtualisables par des hyper-appels (hypercalls) qui vont communiquer directement avec la couche virtuelle de l'hyperviseur.
- L'hyperviseur fournit également un ensemble d'interfaces d'hyper-appels pour d'autres opérations critiques du noyau telles que les opérations de gestion de la mémoire, des interruptions.
- La para-virtualisation est différente de la virtualisation complète où le système virtualisé n'est pas conscient de son état et les instructions critiques sont piégées et traduites.



La para-virtualisation

- Le principal atout de la para-virtualisation réside dans ses faibles couts de virtualisation, mais ses performances par rapport à la virtualisation complète dépendent fortement de la charge de travail de la machine physique.
- Puisque la para-virtualisation ne supporte pas les systèmes non modifiés (et, par conséquent, les systèmes propriétaires tels que Microsoft Windows), sa portabilité et sa compatibilité sont réduites.
- La para-virtualisation introduit également des problèmes de maintenance et de support au sein d'environnements de développement puisqu'elle nécessite des modifications du noyau du système.

La para-virtualisation

- **Avantages :**
 - performances accrues et stabilité.
- **Inconvénients :**
 - les systèmes d'exploitation invités doivent être modifiés afin de tourner avec l'hyperviseur (Nécessite une adaptation du noyau des systèmes invités)
 - La machine virtuelle doit pouvoir tourner sur le processeur (physique) de la machine hôte.
- **Utilisations :**
 - Des logiciels comme Xen, Microsoft Hyper-V.

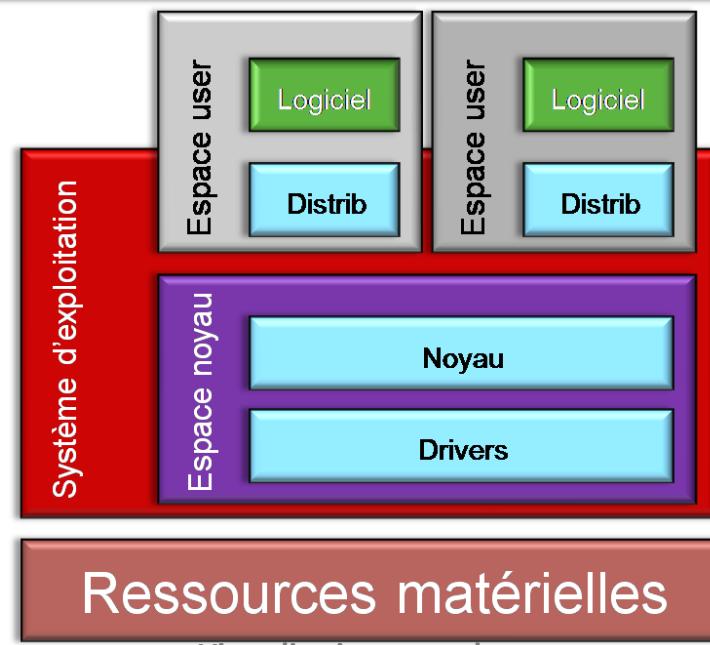
La para-virtualisation

- **Exemples :**
 - **Xen** : projet OpenSource précurseur dans le monde du libre, version commercialisée par Citrix
 - **KVM** : projet hyperviseur intégré dans le noyau linux (Développé par Qumranet, racheté par RedHat)
 - **ESX/ESXi** : hyperviseur leader de VMWare
 - **Hyper-V** : hyperviseur de Microsoft



Virtualisation par partitionnement

- La virtualisation par partitionnement (appelée aussi par isolation) consiste, comme son nom l'indique, à isoler les systèmes virtualisés du reste de la machine hôte.
 - L'isolation entre les machines virtuelles est gérée au niveau du noyau : celui-ci partitionne les ressources (CPU, mémoire, file system).



Virtualisation par partitionnement

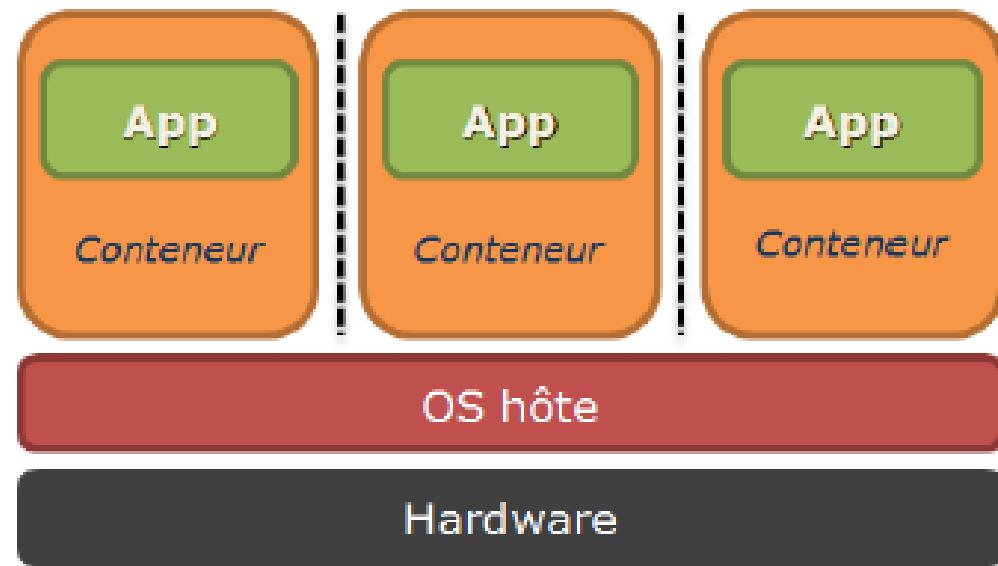
- La virtualisation par partitionnement est donc d'une isolation des « processus », des « utilisateurs » et d'une mise en cage (chroot) des différents « file system » des machines virtuelles.
 - pas d'émulation d'un système comme dans les autres techniques de virtualisation.
 - Le noyau est partagé entre les machines virtuelles et le système hôte.
 - C'est ainsi que l'on peut faire cohabiter différents systèmes d'exploitation, à condition qu'elles partagent le même noyau.

Virtualisation par partitionnement

- L'inconvénient est donc qu'on ne peut virtualiser que des systèmes Linux.
- L'outil de virtualisation va faire fonctionner le nouvel OS sur l'OS principal avec une gestion plus ou moins fine des ressources allouables et des outils de gestion.
- Il ne sera pas possible (en principe) de sortir de cette arborescence.
- Le système invité sera suffisamment autonome pour qu'il puisse installer des composants et se mettre à jour.

Virtualisation par partitionnement

- Un conteneur est en fait un répertoire, qui va contenir une arborescence complète d'un système d'exploitation, avec tous les fichiers nécessaires à son bon fonctionnement.



Virtualisation par partitionnement

- **Avantage :**
 - permet de faire fonctionner plusieurs instances du même système de façon étanche.
- **Inconvénients :**
 - ne permet de faire fonctionner qu'un seul type de système (des systèmes Linux).
- **Utilisations :**
 - Linux VServer, Virtuozzo.

La virtualisation matérielle

- La nécessité de développer des solutions de virtualisation assistées par le processeur a fait son apparition avec la prolifération des systèmes à base d'architecture x86.
- Ce type de processeur contient un jeu d'instructions implémentant un ensemble de primitives de bas niveau qui facilitent la virtualisation.
- A l'aide de la virtualisation matérielle, l'hyperviseur est en mesure de virtualiser correctement l'ensemble des instructions de l'architecture x86.
- Les deux principaux fabricants de processeurs sur le marché, Intel et AMD, ont inaugurés une nouvelle gamme de processeurs incluant une technologie d'aide matérielle à la virtualisation.
- Cette technologie est connue sous le nom de Intel VT-x (anciennement Vanderpool) et AMD-V (anciennement Pacifia).
- Ces technologies permettent le support de plusieurs systèmes d'exploitations différents sans modifier le système invité.

La virtualisation matérielle

- Globalement, les technologies des deux concurrents sont semblables et nous ne les différencierons pas.
- D'un point de vue pratique, ces processeurs incluent un nouveau mode d'exécution appelé Extension de Machine Virtuelle (Virtual Machine Extension, VMX).
- Puisque l'hyperviseur et l'environnement virtuel ne peuvent pas se trouver au même niveau de privilèges, ce nouveau mode d'exécution va ajouter cinq anneaux supplémentaires regroupés en deux niveaux.
 - Le premier, appelé niveau racine correspond à un anneau qui se trouverait sous l'anneau 03 (le niveau racine a donc un contrôle absolu des ressources).
 - Le second, appelé niveau normal, correspond aux quatre anciens anneaux (ils sont donc regroupes au sein d'un niveau de privilèges unique).

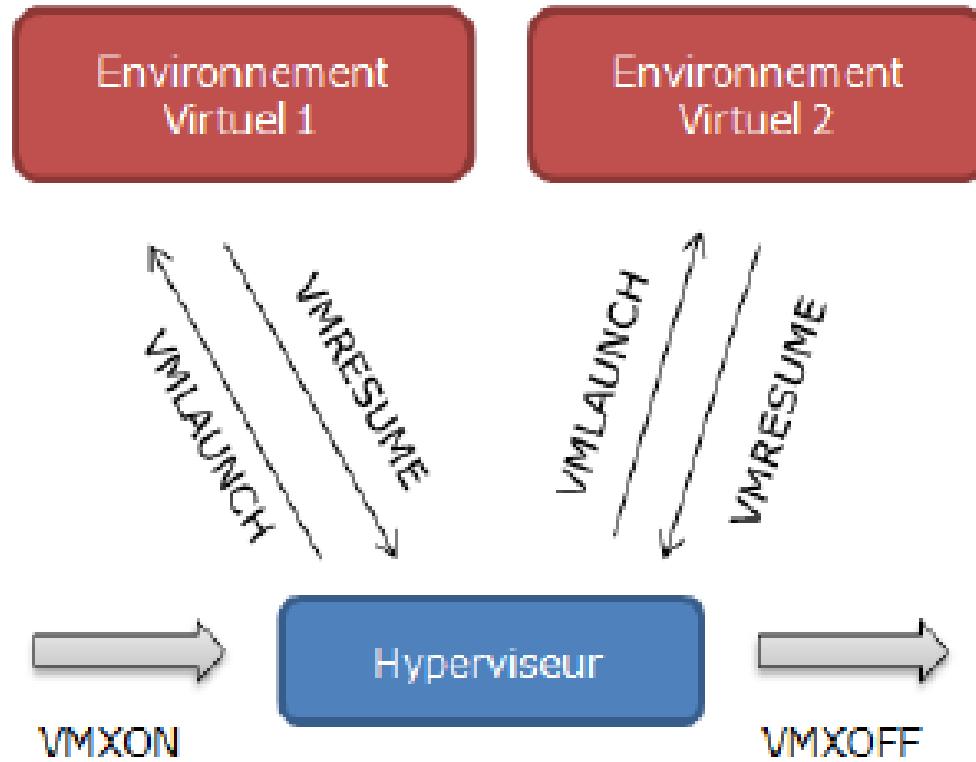
La virtualisation matérielle

- Puisque l'hyperviseur doit gérer la répartition des ressources, il s'exécute au niveau racine tandis que les environnements virtuels s'exécutent au niveau normal.
- Pour entrer dans le mode d'exécution virtuel, le processus exécute une instruction particulière (VMXON chez Intel) et, symétriquement, pour quitter le mode virtuel, le processus exécute l'instruction inverse (VMXOFF chez Intel).
- Lorsque l'hyperviseur est lancé, il peut passer du mode racine au mode normal (et donc, donner le contrôle à un environnement virtuel) à l'aide d'une autre instruction (appelée VMLAUNCH chez Intel) et, symétriquement, l'hyperviseur reprendra le contrôle et passera au niveau racine au moyen de l'instruction inverse (VMRESUME chez Intel).

La virtualisation matérielle

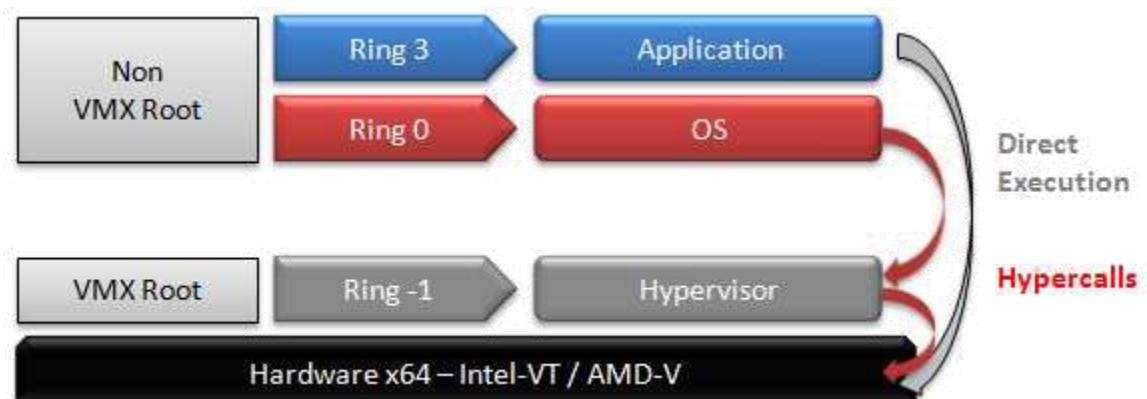
- Les technologies de virtualisation matérielle d'Intel et AMD implémentent également des instructions qui permettent d'accélérer les sauvegardes et restaurations de contexte.
- En effet, lorsqu'un hyperviseur veut donner le contrôle à un autre environnement virtuel, il doit:
 - sauvegarder le contexte d'exécution de l'environnement virtuel actuellement actif
 - et restaurer le contexte d'exécution de l'environnement virtuel à qui il s'apprête à donner le contrôle.

La virtualisation matérielle



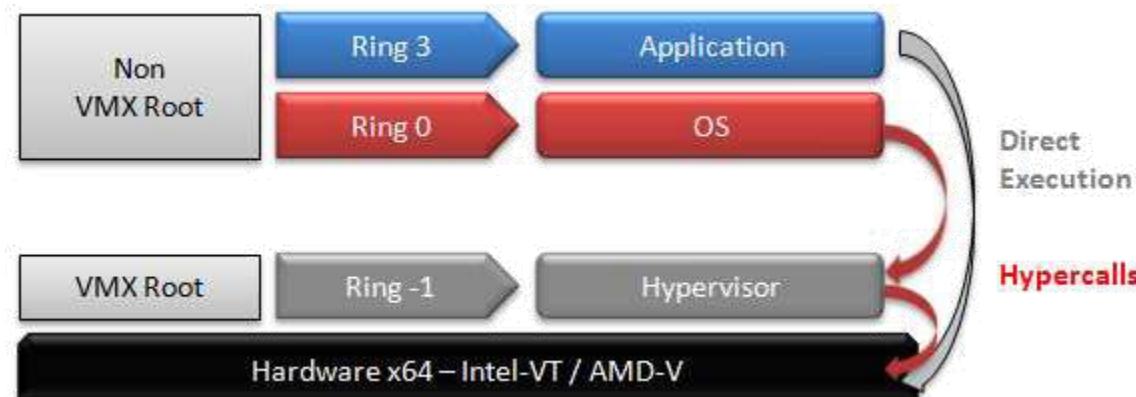
La virtualisation matérielle

- Le principe consiste à ajouter un ring au niveau -1 appelé **VMX Root**, les rings traditionnels étant appelés **VMX Non-Root**.
- Afin de séparer l'hyperviseur et les systèmes d'exploitation des machines virtuelles, celui-ci est placé au niveau du ring -1 et bénéficie des nouvelles instructions de virtualisation, lui permettant ainsi de gérer les environnements virtuels plus efficacement.



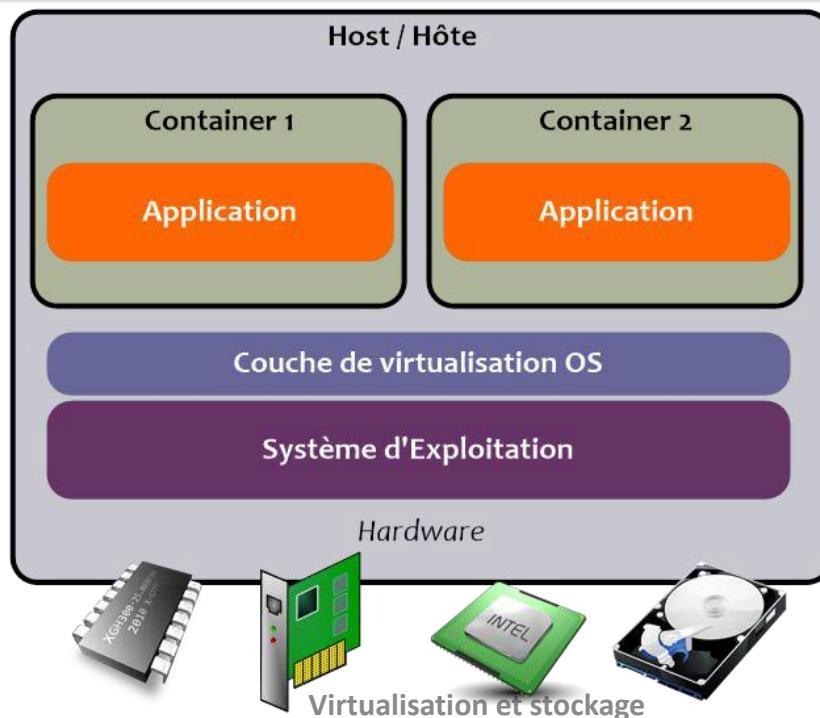
La virtualisation matérielle

- Le système d'exploitation des machines virtuelles est alors placé au ring 0, et communiquera avec l'hyperviseur via des instructions hypercalls.
- Les applications des Guest OS (et de l'Host OS dans le cas d'un hyperviseur de Type-2) restent exécutées au ring 3.



Le cloisonnement

- Le cloisonnement vise à séparer fortement les processus s'exécutant sur un même système d'exploitation et ce en isolant chaque processus dans un conteneur dont il est théoriquement impossible de sortir.
- Un processus isolé de la sorte ne saura pas quels autres processus s'exécutent sur le même système, et n'aura qu'une vision limitée de son environnement.



Le cloisonnement

- Le but principal de cette technologie est d'améliorer la sécurité du système d'exploitation et des applications.
- Le cloisonnement, ou aussi appelé la virtualisation d'environnement, concerne uniquement la partie applicative.
- Il n'y a qu'un système d'exploitation utilisé mais l'application ou l'environnement utilisateur ou logiciel est cloisonné de sorte que les processus soient indépendants.

Le cloisonnement

- **Exemple:** Parallels Virtuzzo
- **Avantages:**
 - Meilleure performance, scalabilité supérieure (en terme de ratio de consolidation)
- **Inconvénients:**
 - Isolation moindre (tous les containers dépendent de l'OS virtualisé)
 - OS host = OS guest