Cours de virtualisation

Partie II

Faculté des Sciences de Rabat / Master IPS 2022-2023

- **Hyperviseur (hypervisor)**: **bare-metal (type 1) vs hosted (type 2)**

Plate-forme logicielle de virtualisation qui permet l'exécution simultanée de plusieurs systèmes d'exploitation sur une même machine physique; synonyme: gestionnaire de machines virtuelles

- **Hôte (host) =** machine physique sur laquelle s'exécute l'hyperviseur , elle se compose de :
  - Plusieurs processeurs multicœurs,
  - Plusieurs gigaoctets (Go) de RAM,
  - Plusieurs téraoctets (To) d'espace disque
  - Stockage en réseau (NAS, Network Attached Storage) ou d'un réseau de stockage (SAN, Storage Area Network)
- **Système Invité (guest) =** OS installé à l'intérieur d'une machine virtuelle

- **Machine Virtuelle (VM)** :

Système d'exploitation s'exécutant à l'aide d'un hyperviseur et dont le matériel est partiellement ou totalement émulé ==> est un **ordinateur virtuel** qui utilise un **système invité**

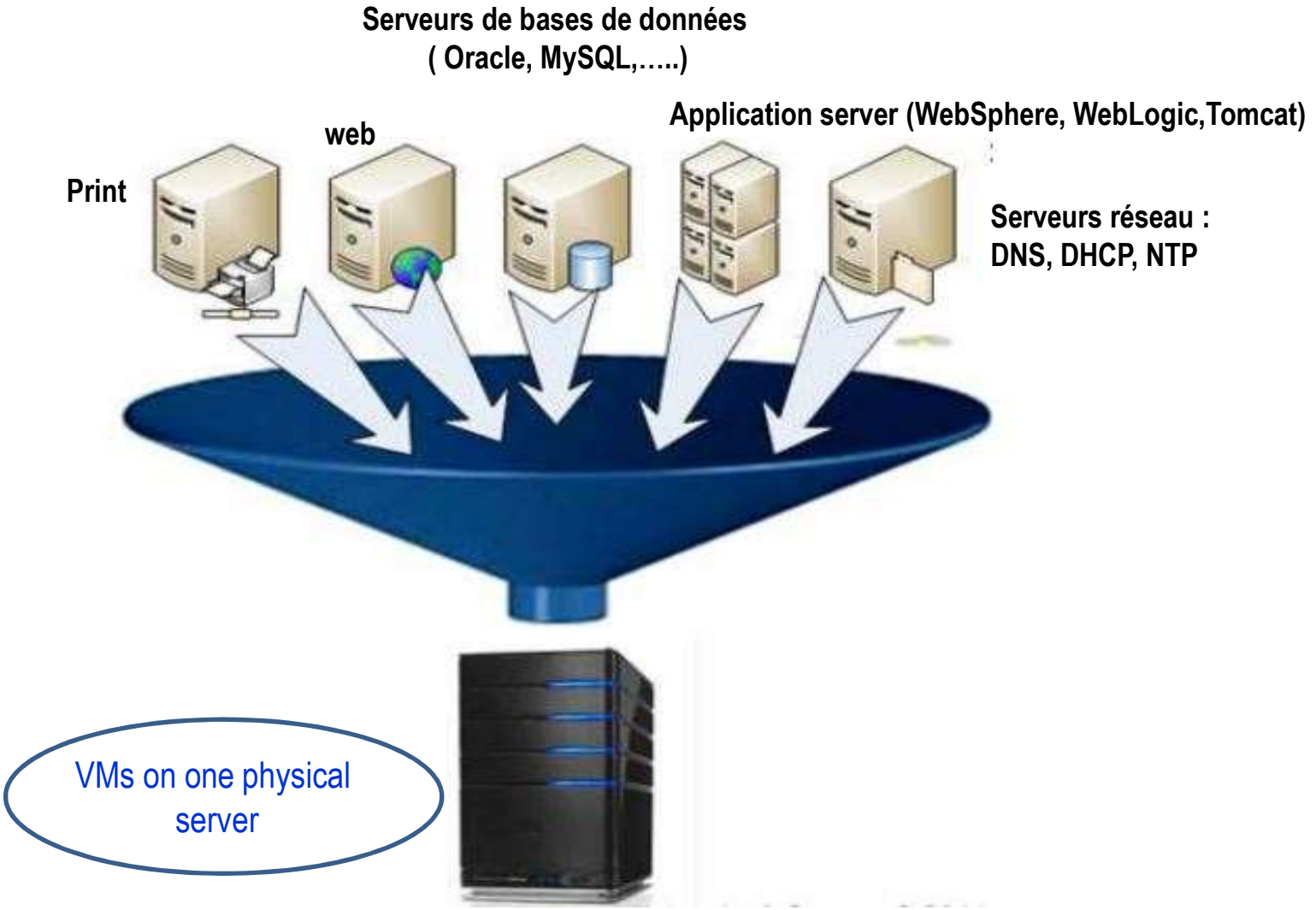
- **Virtuel** :

Il s'agit du portage ou de la création d'un environnement système complet (OS + Applications) au sein d'une VM

- **Migration « Live »** (**Vmotion**, **Storage Vmotion**) :

Déplacement d'un invité d'un hôte à un autre sans interruption de service

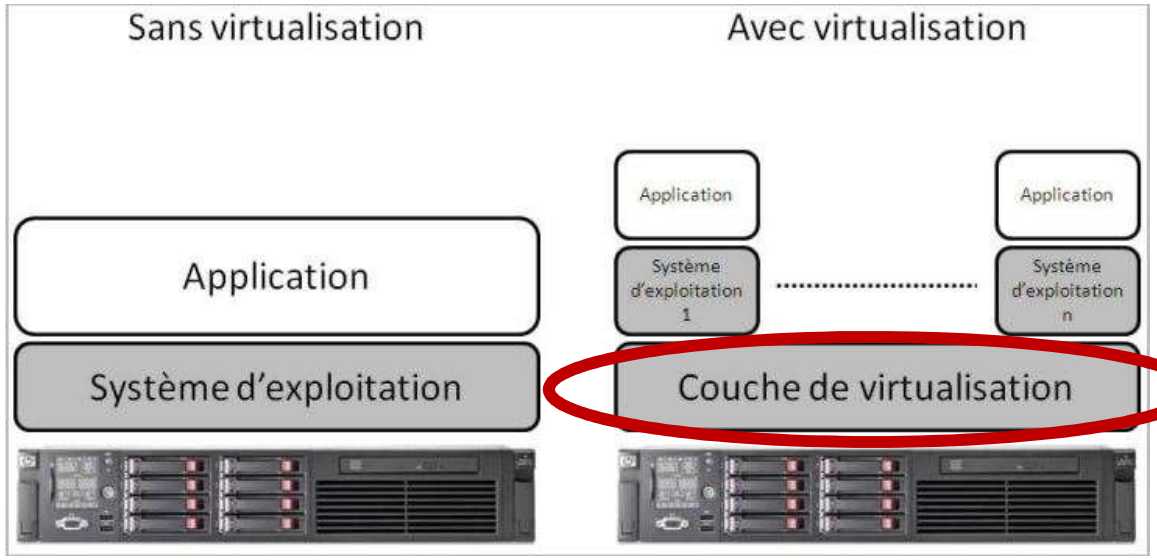
Candidats à la virtualisation



N.B: **Il n'y a pas non plus de restriction quant aux systèmes d'exploitation** (Windows , Linux , solaris,…)

Introduction : Consolidation

Objectif : Optimisation du taux d'utilisation des serveurs.



➢ **Sans virtualisation** (architecture x86 traditionnelle), un **seul système** peut être opérationnel sur une **machine physique**.

== > **Exécution de plusieurs applications / serveur augmente le risque d'interruption de service global.**

== > En général, **1 serveur = 1 application**

➢ **Avec la virtualisation** (architecture x86 virtualisée), chaque machine virtuelle possède ses propres applications et système d'exploitation.

== > **Possibilités d'exécuter plusieurs systèmes d'exploitations sur la même machine physique**

Serveur virtuel

Question 5 : Qu'est ce qu'un serveur virtuel

- Il s'agit d'un **conteneur de logiciel complètement isolé** qui est 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**.
- Il 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

Question 6 : Quels sont les avantages d'un serveur virtuel?

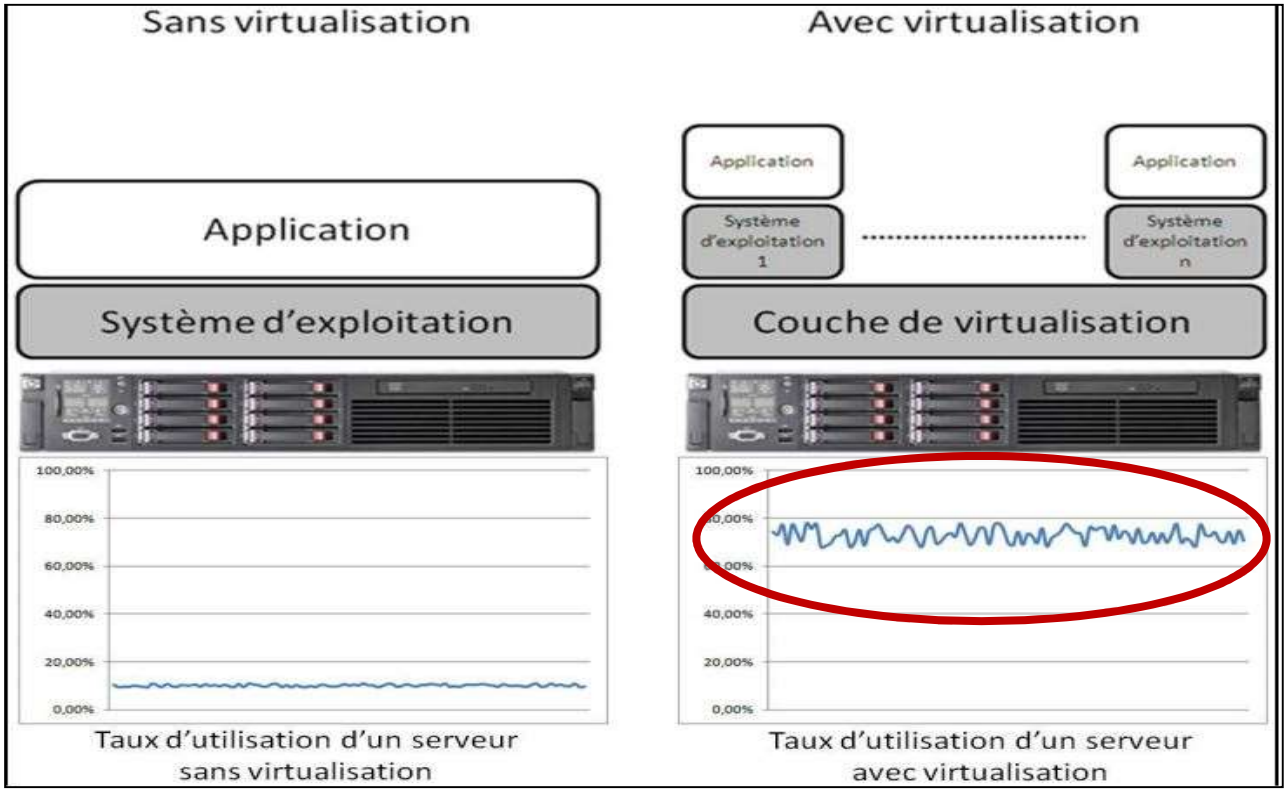
Réponse :

Compatibilité , Isolation, Encapsulation, Indépendance matériel

Serveur virtuel

- **Compatibilité** : les serveurs virtuels sont compatibles avec tout les standards x86 et autres
- **Isolation** : les serveurs virtuels sont isolés des autres machines comme si elles étaient des machines physiques.
- **Encapsulage (imbriquement)** : les serveurs virtuels encapsulent un environnement informatique complet
- **Indépendance matériel** : les serveurs virtuels fonctionnent indépendamment du matériel.

Introduction : Consolidation



➢Plus le nombre de serveurs hébergés augmente; plus la **consolidation** est efficace et permet de réduire les différents coûts liés à la couche physique (énergie, refroidissement, maintenance, achat, …).

Exercices

Exercice 1 :

Quelle est la différence entre **consolidation**, **rationalisation** et **concentration**?

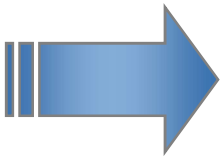
Exercice 2 : Quelles sont les raisons principales de consolider des services web ?

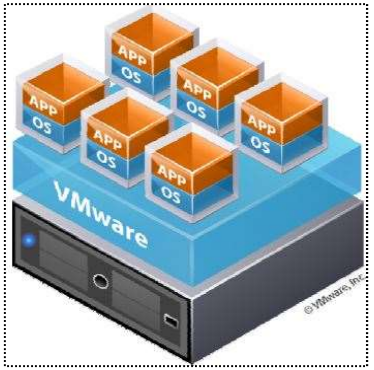
Introduction : Définition (1/2)

➢ **Virtualisation** : 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.

- Simuler, au sein d'un **serveur physique**, l'existence de plusieurs systèmes d'exploitation **cloisonnés** et **mutualisés**.
- Donc, il s'agit d'une technologie qui **transforme du matériel en logiciel** par **allocation dynamique** de **ressources physiques** (**CPU, RAM, stockage et réseau**) aux différentes machines virtuelles.
- **L'ordinateur hôte "voit" ses machines virtuelles comme des applications auxquelles il dédie ou distribue ses ressources.**

Architecture traditionnelle:
- Un seul système d'exploitation
- Une seule application



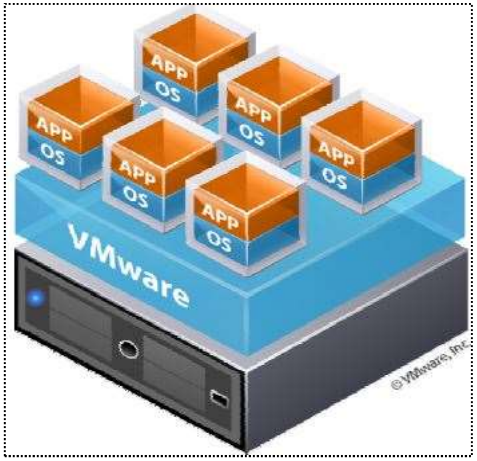


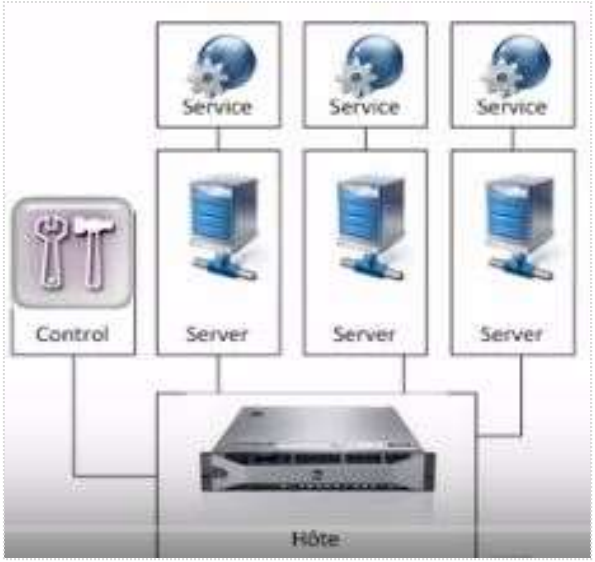
Architecture virtuelle:
- Virtualise plusieurs VMs par utilisation d'un Hyperviseur (Vmware)

Introduction : Définition (2/2)

➢ Selon le **type de virtualisation** choisi, un système principal (OS ou logiciel) s'interpose entre la **machine physique** et une **collection de machines virtualisées** en s'occupant de leurs gestion dans quelques secondes en terme de :

- Création;
- Duplication;
- Suppression;
- Supervision, …





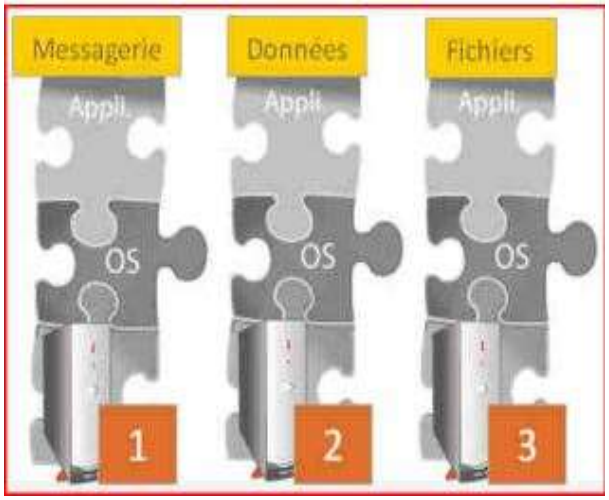
L'ordinateur hôte "voit" ses machines virtuelles comme des applications auxquelles il dédie ou distribue ses ressources

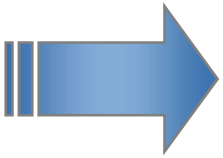
Quels usages de la virtualisation ?

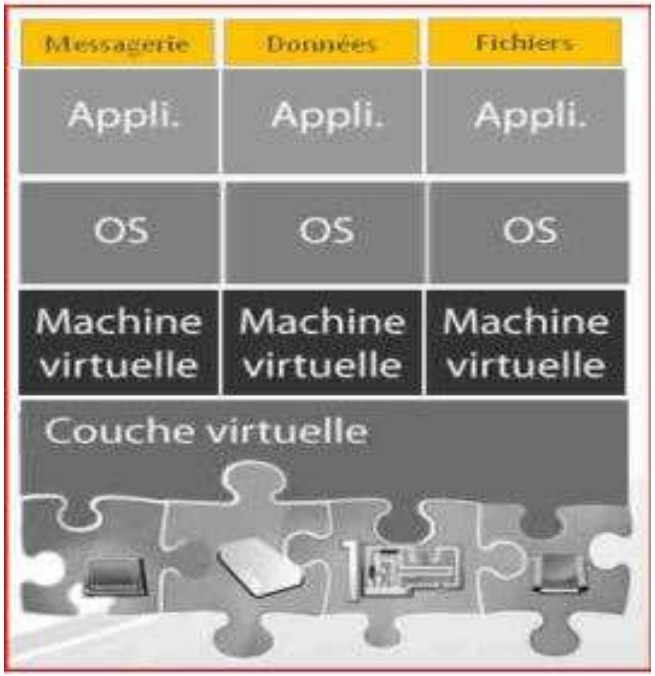
➢ **Mutualisation des ressources** et **regroupement de systèmes divers** sur une machine physique unique (tout en les maintenant logiquement séparés)

➢Exécution simultanée de plusieurs OS sur une même machine (mieux que le multiboot !)

➢Essai d'un système avant mise en exploitation (cassage et possibilité de recommencer sans casser le système d'exploitation hôte)

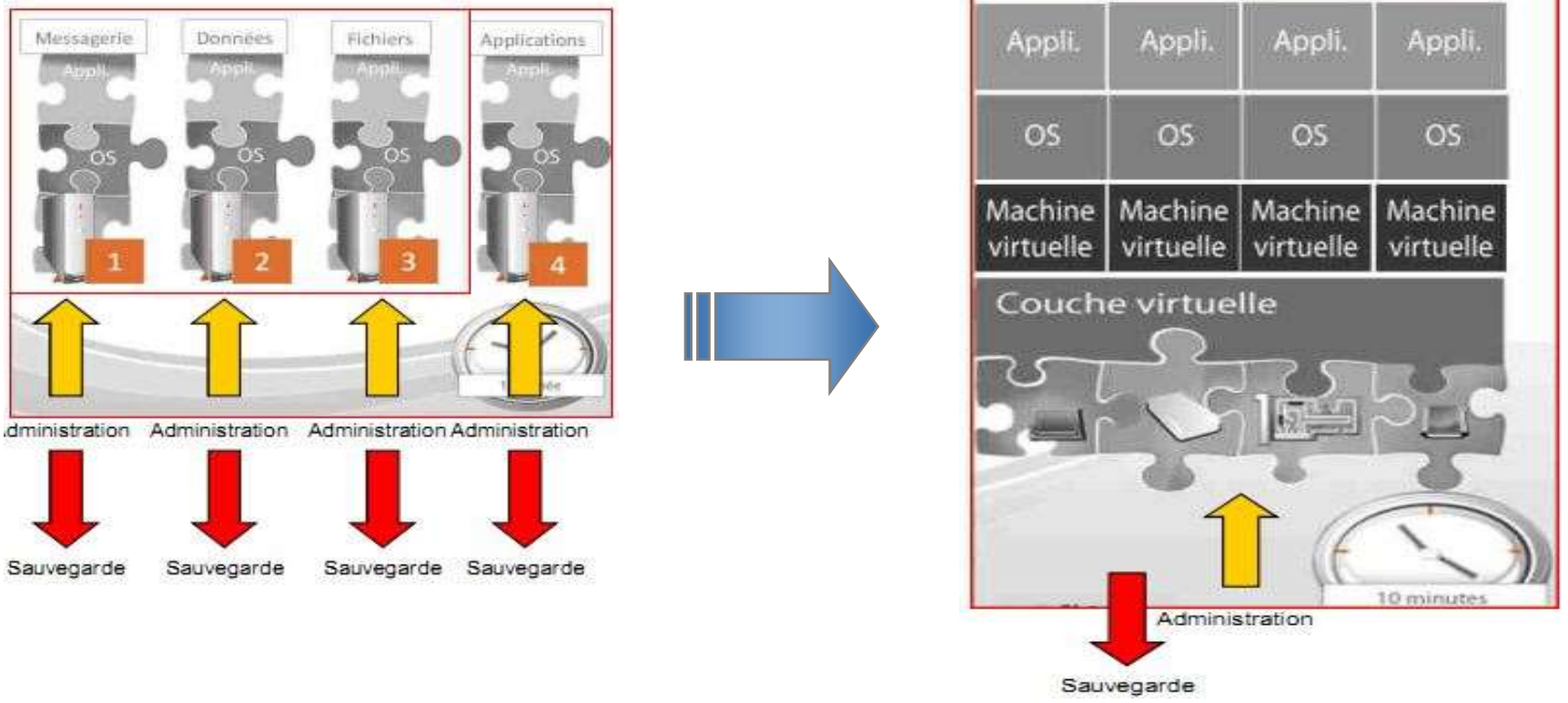




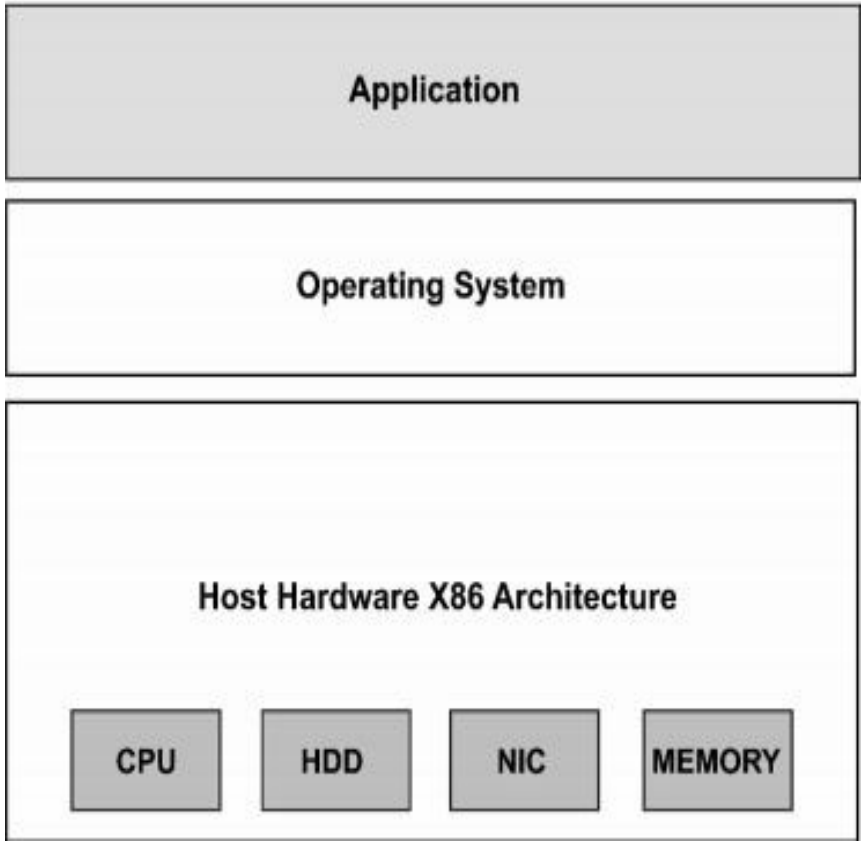


➢ Evolutivité, simplification de la configuration

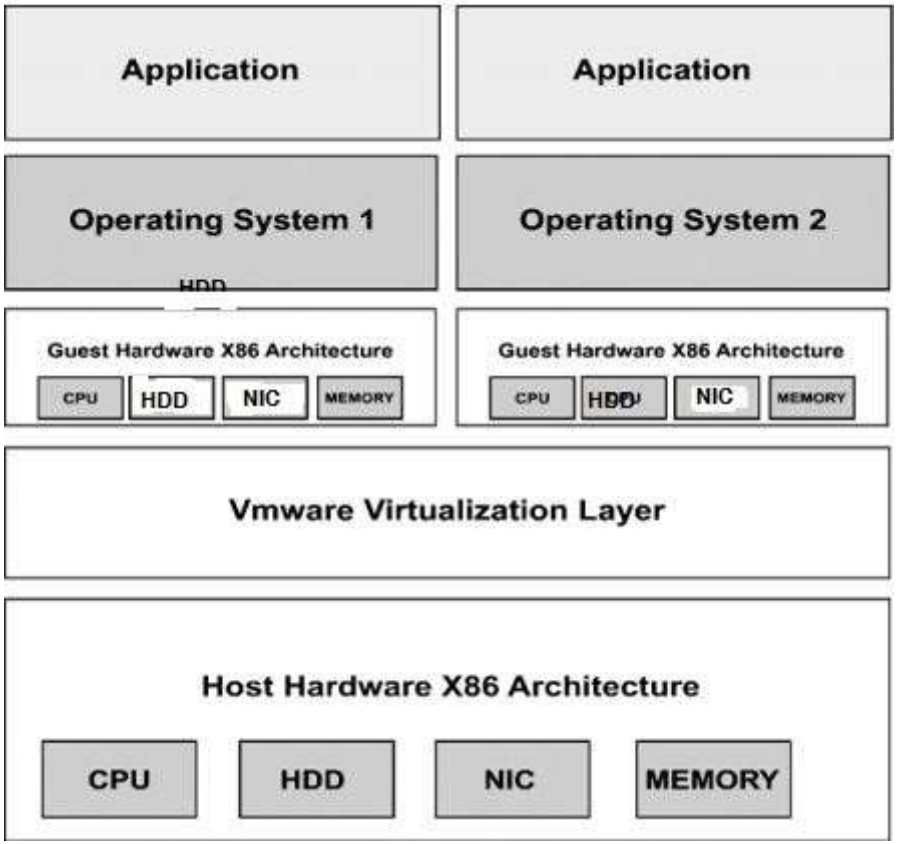
Exemple: ajout d'un serveur d'application



Rappel



A machine before virtualization.

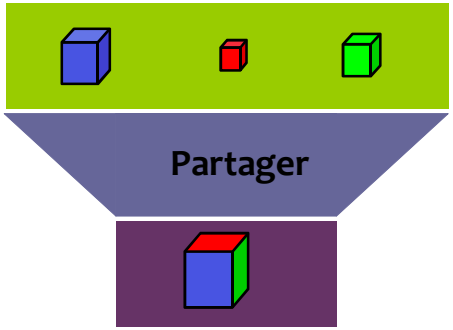


A machine after virtualization.

Pourquoi la virtualisation ? (1/4)

➢ **Efficient utilization of resources (optimization) /consolidation**:

Utilisation **maximale de la capacité** informatique du matériel physique (resources) **partagé entre les VMs** :



- Sans virtualisation, la plupart des matériels ne connaissaient qu'un taux d'utilisation de **5 à 15%** du **CPU** ou/et du **mémoire**.
- Avec la virtualisation tels que VMware, un serveur peut être utilisé en toute sécurité par plusieurs VMs de traitement jusqu'à **75 % à 80 %** sur une base continue en terme de **CPU** et **mémoire**.

Exemple:

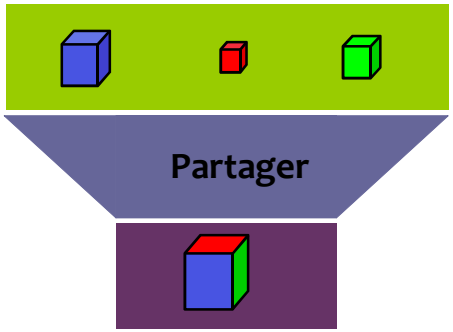
Prenons le cas où un **serveur physique a été acheté pour exécuter une application q**ui ne fonctionne que pendant la **soirée**.

Lorsque la **demande n'est pas traitée**, par exemple le matin ou l'après-midi, la boîte matérielle est inactive, ce qui est un **énorme gaspillage** de ressources.

Avec VMs, le serveur physique utilisera mieux ses ressources.

Pourquoi la virtualisation ? (1/4)

Flexibility :



- Assignation très souple des serveurs à différents usages : puissance de calcul, stockage.
- Ces affectations peuvent être modulées en fonction des contraintes particulières (montée en charge, certains mois ou certains jours par exemple)

Examples :

- **VMs :** software constructs that run in a hypervisor (logiciels qui fonctionnent dans un hyperviseur)
- **Virtual disks:** software components that emulate an actual disk storage device.

- **VLANs (**Virtual local area network) : Il s'agit de créer sur un meme switch plusieurs réseaux indépendants ne pouvant communiquer entre eux.

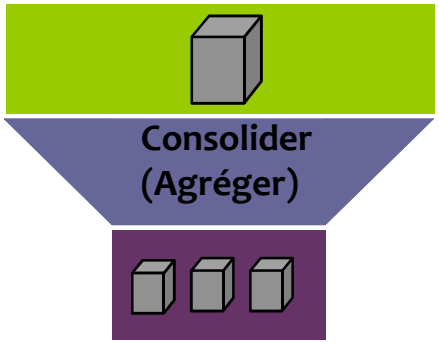
- **Logical PARtition (LPAR) ou partitionnement logique (IBM) :** est un sous-ensemble des ressources matérielles de l'ordinateur **(processeur, mémoire et stockage)** qui apparaissant comme un serveur distinct dans le cadre de la virtualisation.

Une partition est une partie d'un disque dur matériel destinée à accueillir un système de fichiers.

Pourquoi la virtualisation ? (2/4)

➢ **Easier management / centralized management** :

Créer des **flux de travail automatisés** de gestion des **services IT** c à d définir les collections de machines et d'applications virtuelles en tant que services par outils automatisés de déploiement et de configuration



Exemple :

- You can automate power management (Alimentation),
- Balance workloads on your various virtual machines,
- Convert a physical server into a virtual machine,
- Provision new servers,
- Migrate VMs from a failed server to an active one.

➢ **Réduire les besoins en énergie , climatisation et en surface au sol**.

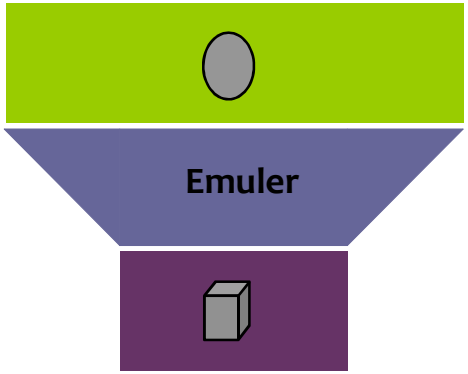
➢ **Examples :**

- **Virtual disks,**
- **IP routing to clones :**

The concept refers to **on-demand generation** (cloning) of **host routes** (/32).

In ARP, The route to a directly attached Ethernet network is installed as a 'cloning' route, causing routes to individual hosts on that network to be created on demand.

Pourquoi la virtualisation(¾)



➢Action de **reproduction du contexte d'exécution d'un système sur un autre** **c**-à-d simuler le fonctionnement de n'importe quel ordinateur (processeur et matériel) sur un autre ordinateur même si celui-ci est technologiquement différent.

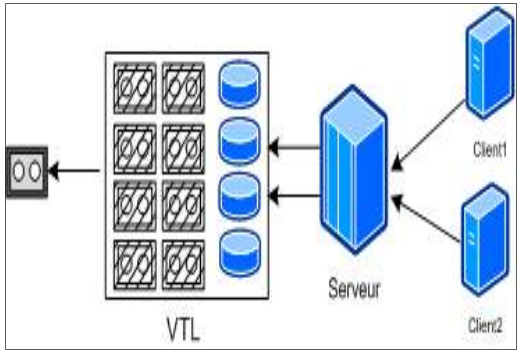
Autrement dit ,**imitation du comportement physique d'un matériel par un logiciel**

Exemples:

- **Virtual Tape** (Emuler espace disque en bandes magnétiques)

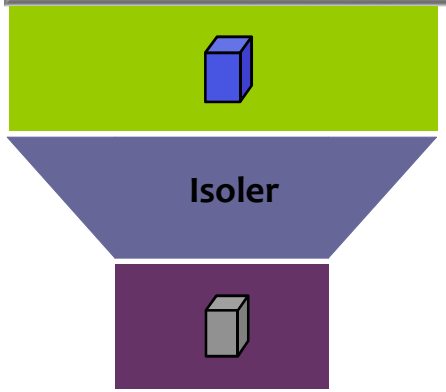
Virtual Tape Library : système de **stockage** informatique incluant un serveur, une grappe de disques et un logiciel capable d'**émuler** cet espace disque en bandes magnétiques.

- **Internet Small Computer System Interface (iSCSI)**: Protocole de la couche de transport qui transporte les blocs de données entre un initiateur iSCSI (**Open-iSCSI sur Linux**) et une cible iSCSI installée sur un dispositif de stockage sur **le réseau IP**.



Virtual Tape Library

Pourquoi la virtualisation(4/4)



➢ **VMs s'exécutent de manière indépendantes**

- Arrêt d'un OS virtuelle mais pas le OS hôte qui est invisible pour l'attaquant.
- Test d'architectures applicatives et réseau
- Isolation des différents utilisateurs simultanés d'une même machine
- Environnment d'éxecution cloisonné sans interférence avec les ressources installées localement.

Exemples :

- **Linux Vserver :** isolation des processus en espace utilisateur
- **OpenVZ :** partitionnement au niveau noyau sous Linux
- **chroot** (**ch**ange **root)**: isolation changement de racine.
- **Capacity Upgrade on Demand (CUoD)** :

Packaging standard du i890 (Power 770 server IBM) qui permet d'activer un ou plusieurs coeurs de processeur inactifs ou une ou plusieurs unités de mémoire inactives sans devoir redémarrer votre serveur ni interrompre vos activités.

- **Storage Area Network (**SAN-VC) :

Partition logique dans un réseau de stockage physique SAN(**Partage des blocs de disques**) qui permet d'isoler le **trafic dans des parties spécifiques** d'un réseau SAN. Si un problème se produit dans une partition logique, il peut être géré avec un minimum de perturbation pour le reste du réseau.

Bénéfices : Economiques

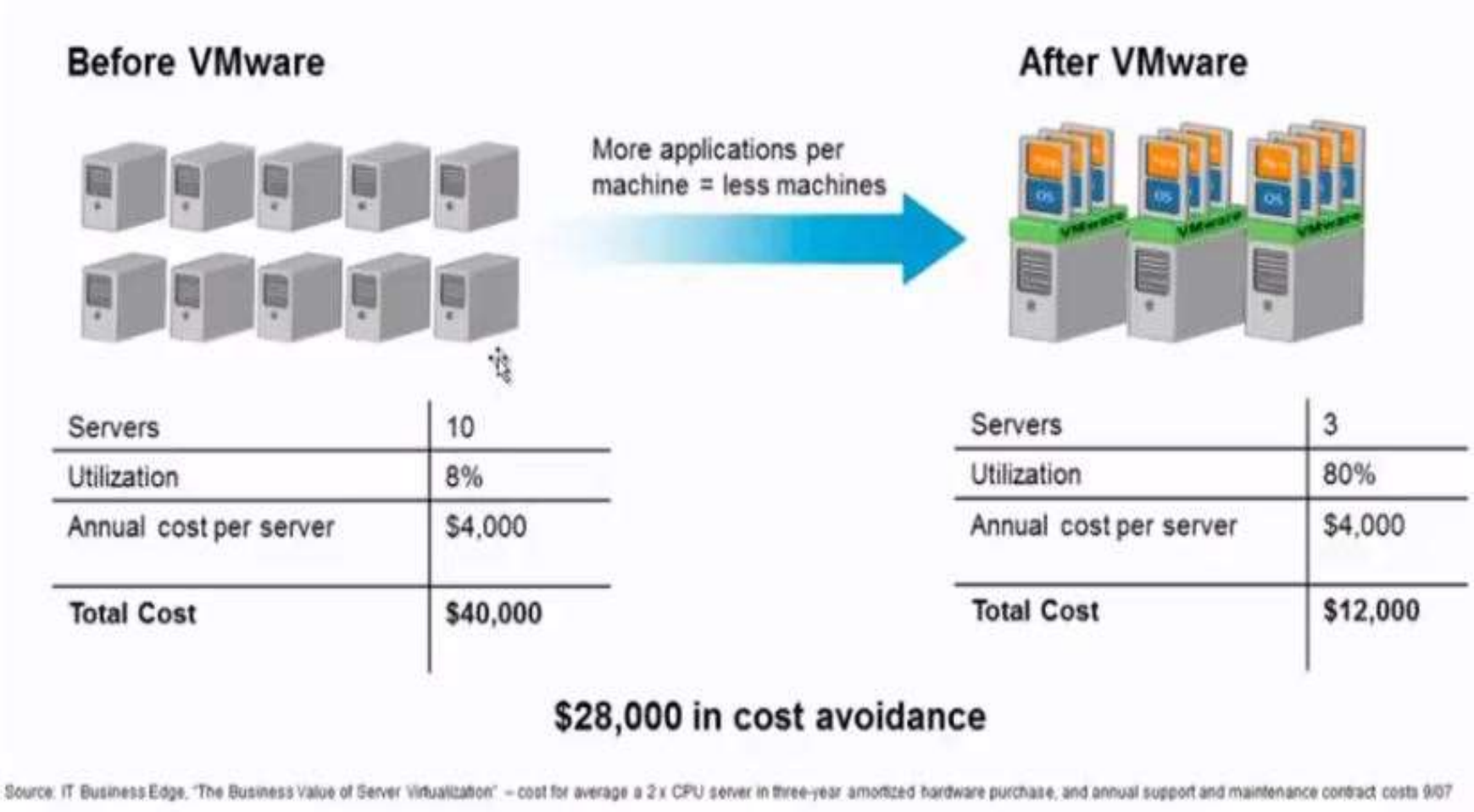
- Mutualisation des ressources permet :
  - Diminution le besoin en matériel informatique
  - Diminution de la consommation électrique.
  - Simplicité du monotoring et de l'entretien physique

- Réduction du coût d'acquisition et de gestion du matériel

  >> Frais de : rack, électricité, climatisation, réseau,….

- Réduction du coût d'exploitation en terme de :
  - Energie via un meilleur taux d'utilisation
  - Refroidissement,
  - Immobilier par économie d'espace dans les centres de calculs (occupation au sol)

Bénéfices : Exemple Economique (1)



Résultat : cost avoidance

Bénéfices : Exemple économique (2)

ROI (*Return On Investment*) pour une banque Suisse:

- de 166 serveurs physiques Windows à 9 serveurs VMware ESX (ratio de consolidation = 18,4)
- de 1 169 514 kWh/an à 114 097 kWh/an
- de 303 771 BTU à 29 636 BTU

  BTU (British Thermal Unit) = utilisée pour mesurer la dissipation de chaleur d'un équipement électrique
- de 500 tonnes/an de CO^2 à 49 tonnes/an
- facture électrique: de 110 168 € à 10 748 €

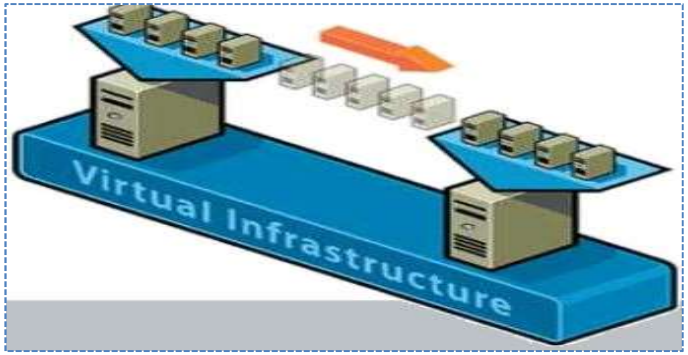
Bénéfices : Facilité d'administration (1/2)

➢ Installation, déploiement et migration aisées des machines virtuelles entre serveurs physiques (Rapidité de déploiement) :

- ♦ Simple à déplacer et copier (fiabilité) :
  - • Tout est inclus dans des fichiers
  - • Independent du matériel physique (hôte)
- ♦ Facile à gérer :
  - • Isolée des autres VMs
  - • Non affectée par tout changement matériel
- ♦ VMotion :

Migration en temps réel des VMs en fonctionnement (.vdk, .vmk,…) d'un serveur physique vers un autre sans interruption de service.

Exemple: un administrateur qui veut arrêter le 1er serveur pour une raison, le client ne va rien sentir lors de l'utilisation de son ordinateur sans savoir que sa VM a changé complètement le serveur.



Bénéfices : Facilité d'administration (2/2)

- Mise à disposition d'environnements de tests et validation aux équipes informatiques rapide, fiable et qui ne nécessite pas l'immobilisation de ressources matérielles quelque fois sous utilisées.

- Exécuter et lancer plusieurs types de systèmes d'exploitation (Linux, Mac OS, Windows) en même temps.

- Tester et réparer une récupération d'accident et dimensionnement des serveurs faciles.

- Consolidation des serveurs et optimisation de l'infrastructure (optimiser le taux d'utilisation des ressources par regroupement des ressources communes)

- Cloisement ou chaque système d'exploitation fonctionne d'une façon indépendante et sans aucune interférence mutuelle.

- Flexibilité : Faire autant de manipulations d'une façon simple
  - Ajout des composantes telles que disque dur, mémoire, cpu,
  - Création des **snapshots** ou **copie ponctuelle** (**point in time copy**)

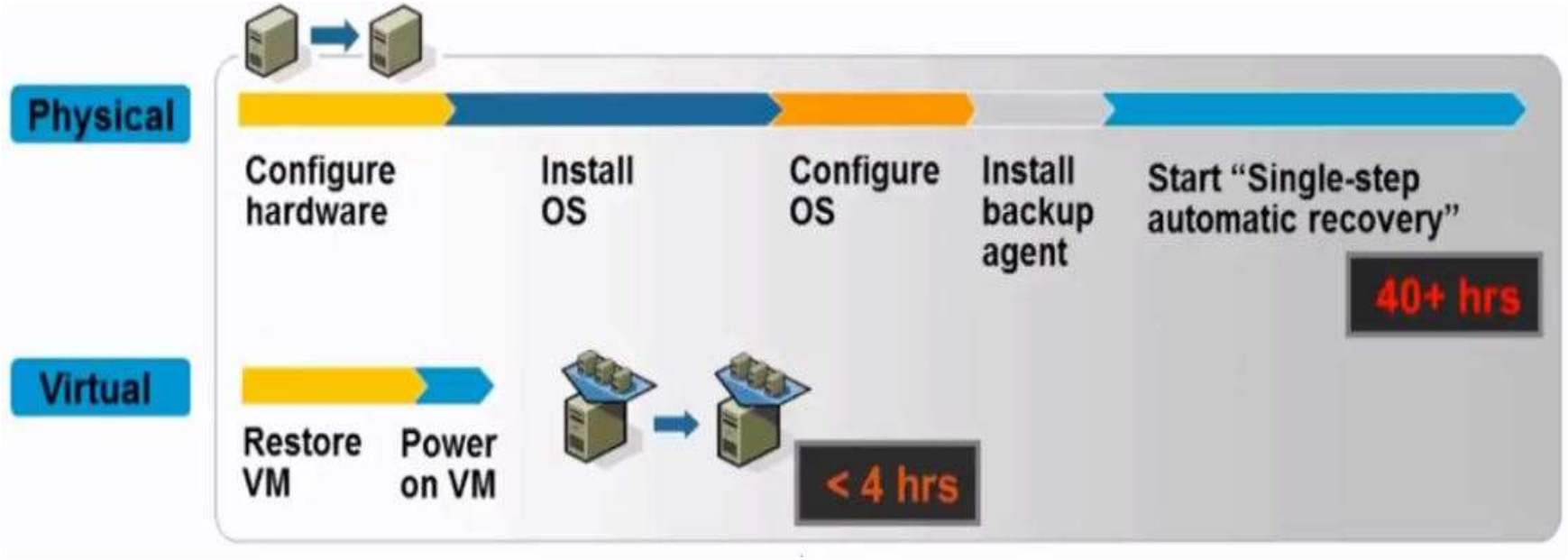
Bénéfices : Sécurisation

- **Isolation** (séparation) des systèmes virtuels et hôtes (invisibles) réduit les risques d'attaques (cassage des OS virtuels, mais pas les systèmes d'exploitation **hôtes**) et de compromission des machines:
  - Si il y a un problème sur une VM, les autres VMs ne seront pas impactées.
  - VM n'est pas consciente qu'elle est machine virtuelle,elle se comporte comme machine physique

Bénéfices : Sécurisation

- **Répartition** (isolation) des différents utilisateurs simultanés d'une même machine
- **Diminution des risques** liés au **dimensionnement** des serveurs, l'ajout de puissance (nouveau serveur …) étant alors transparent.
- **Répartition dynamique de charge (load balancing)** par allocation dynamique des ressources, puisque la virtualisation sait répartir la charge entre les différentes machines.
- **Meilleure disponibilité des systèmes** :
  - Déplacement automatique ;
  - Facilité de clonage des systèmes;
  - Sauvegarde des VMs
  - …
- **Traçabilité** des actions administratives

Bénéfices : Save Time During Disaster Recovery



- Eliminate recovery steps
- Standarize recovery process

Risques : Décloisonnement et Déni de service

Décloisonnement

Décloisonnement via des failles sur l'hyperviseur
(**Difficulté de maîtriser les différents échanges internes à une même machine physique**)

Oui, le risque existe …

- Il est délicat de garantir que les **ressources bas niveau partagées ne permettent pas des fuites d'information.**
- Possibilité que les utilisateurs d'une VM d'en sortir pour accéder aux autres VMs et à l'hyperviseur

Exemple :
En cas d'erreur ou de **compromission** de la carte réseau de la machine physique qui héberge les VMs, un **accès aux données** des différents flux d'information est possible.

Déni de service

Impact d'une instance sur l'autre en terme de performance/disponibilité

Oui, le risque existe…

Pic de charge, déni de service…

1) Volumétrie
Saturer la bande passante

2) Protocolaire
- Fragmentation (sur-fragmenter les paquets pour encombrer le CPU)
- Ouverture de sessions

3) Applicative
Saturation des services CPU / RAM-
> Cherche les fonctions non optimisées et en abuser

Des risques réels, mais finalement **peu rencontrés !**

Risques liés au gestion

L'historique des plateformes de virtualisation nous joue encore des tours !

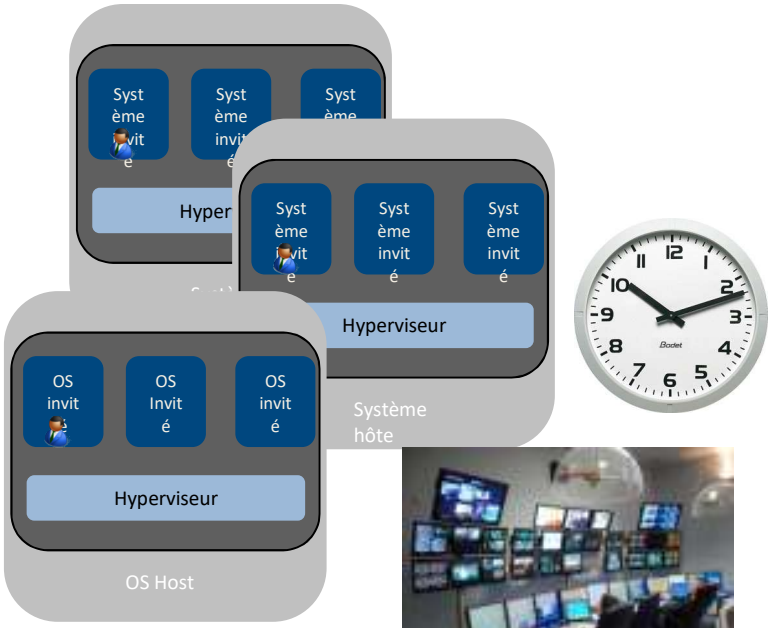
- **Prolifération des VM (VM sprawl)** :
  >> Hyper-sollicitation inutile de l'infrastructure par l'ajout indispensable des VMs
  >> Accroissement des couts de licences sans raison (copie VMs non maitrisée)

- **Centralisation** = problèmes d'infrastructure réseau, stockage, sauvegardes...

- **Capacity Planning**:
  La compromission du système hôte impacte le timing et la capacité de remise en service ultérieure du système.
  >> **Planification des besoins et prise de décisions d'investissements avec optimisation continue des serveurs(** VMware Capacity Planner, ...).

- **Risque d'erreurs de configuration** =
  - Arrêt multiples d'instances,
  - Activation de la mobilité des VMs,
  - Activation de fonctions de décloisonnement.

- **Défaut de séparation des tâches** entre les équipes système et réseau, avec tous les risques d'erreur, voire de malveillance, dus à la concentration de ces responsabilités.....



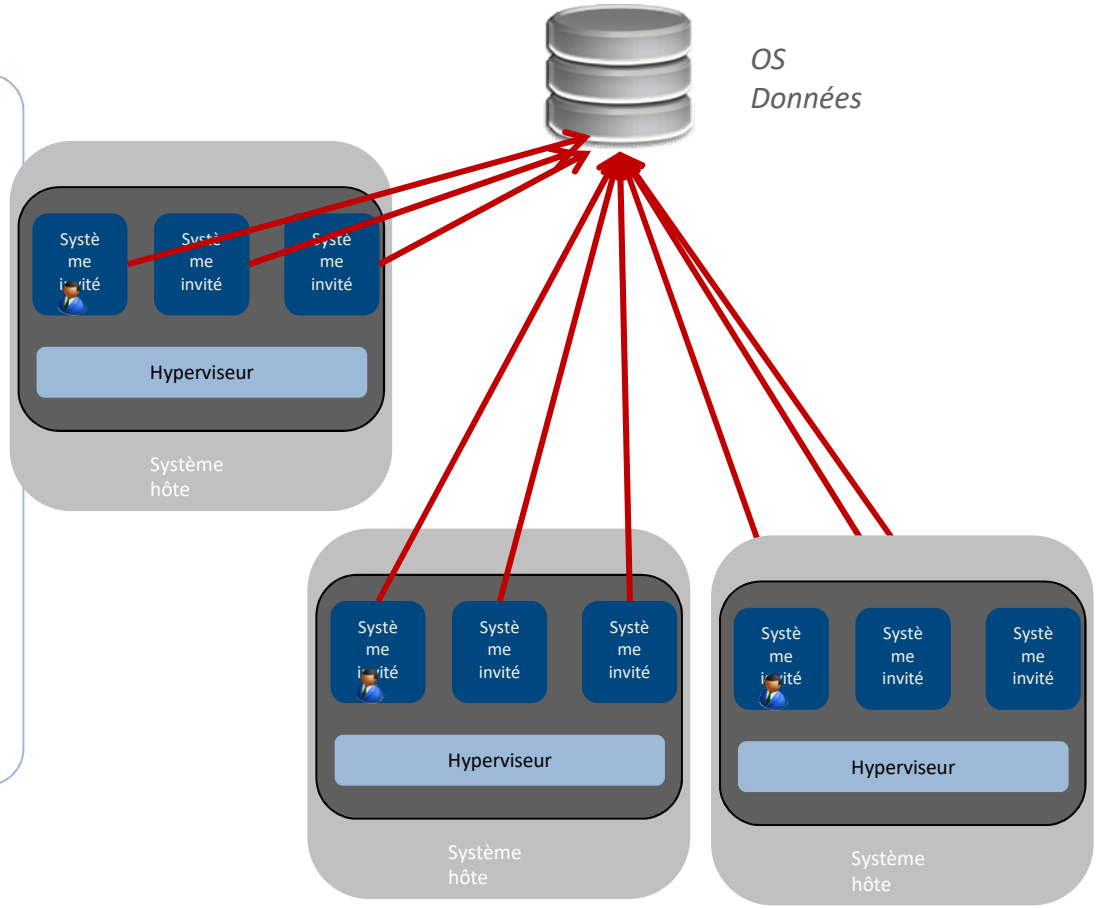
Risques liés au stockage

La criticité du stockage augmente toujours !

- Concentration des données (Single Point Of Failure ou SPOF)

(Le fait que les actifs réseaux ne soient pas doublés constitue un point unique de défaillance)

- Destruction des données OS
- Atteinte à la confidentialité de multiples VMs (OS et des données)
- Performances I/O



Risque : Ecosystème

Console d'administration

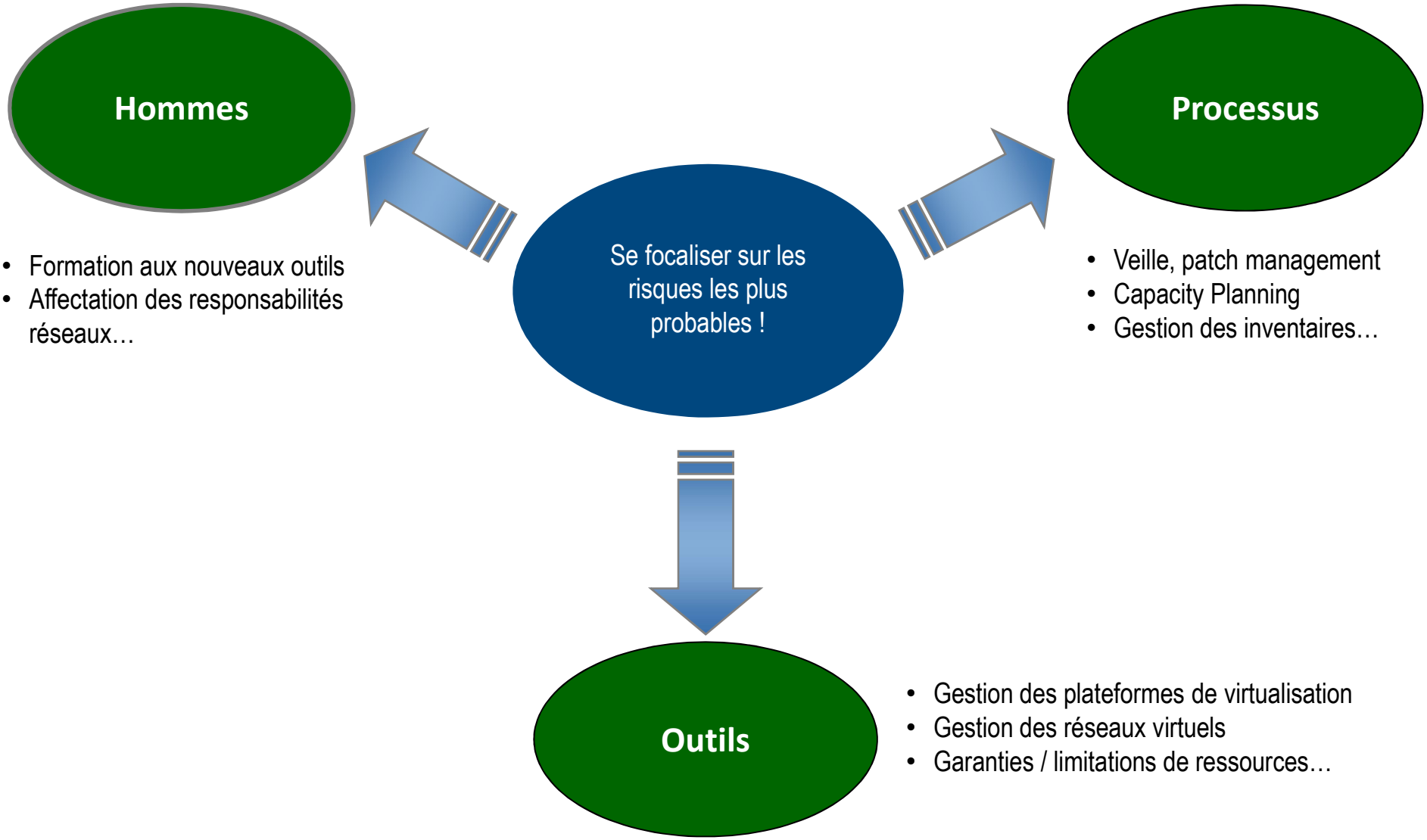
Stockage

Un incident sur l'**écosystème** impacte potentiellement de nombreux services métiers !

Réseau

Pratiques de gestion

Comment encadrer ces risques ?



- Formation aux nouveaux outils
- Affectation des responsabilités réseaux…

- Veille, patch management
- Capacity Planning
- Gestion des inventaires…

- Gestion des plateformes de virtualisation
- Gestion des réseaux virtuels
- Garanties / limitations de ressources…