VIRTUALISATION

Novembre 2020

Pr. Oussama Mohamed REDA

Intervenant:
Dr. Y.T.Benjelloune

Module: Cloud Computing

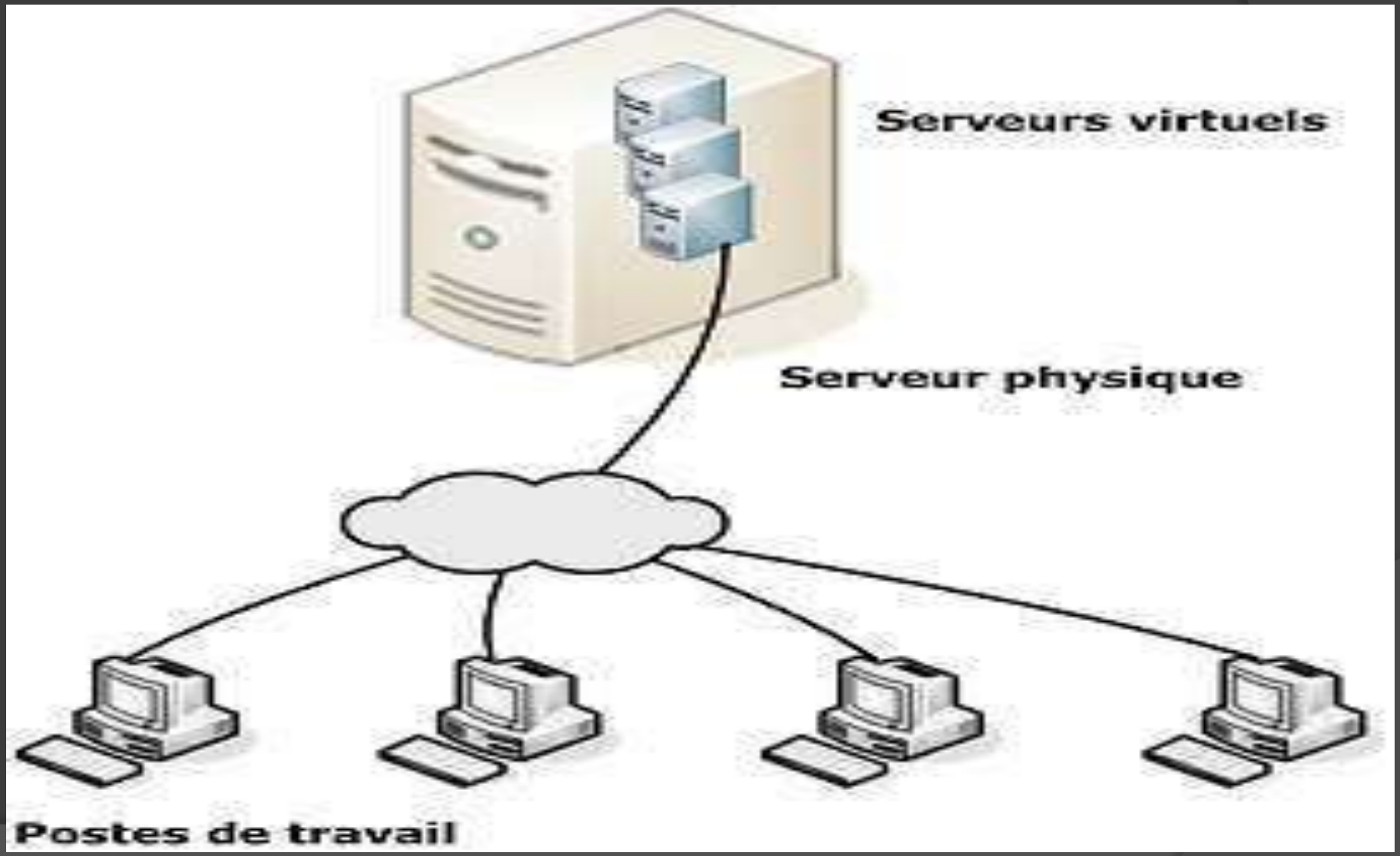
Virtualisation

- Introduction
- La machine virtuelle
- Hyperviseur
- Techniques de virtualisation
- Matériel de virtualisation
- Solutions de virtualisation

Définition

- **Virtualiser :** proposer, par l'intermédiaire d'une couche d'abstraction proche du matériel, une vue multiple d'un matériel unique, en sérialisant les appels vus concurrents de l'extérieur.
- La virtualisation de serveurs est un ensemble de techniques et d'outils permettant de faire tourner plusieurs systèmes d'exploitation sur un mémé serveur physique.
- Le principe de la virtualisation est donc un principe de partage : les differents systemes d'exploitation se partagent les ressources du serveur.
- La virtualisation s'appuie sur les logiciels pour simuler une fonctionnalité matérielle et créer un système informatique virtuel. Ce modèle permet aux services informatiques d'exécuter plusieurs systèmes virtuels (et plusieurs systèmes d'exploitation et applications) sur un seul et même serveur. Cela se traduit par des économies d'échelle et des gains d'efficacité.
- Plus tard, nous verrons « Le Cloud Computing ». Mais il faut savoir que celui-ci doit son apparition à la virtualisation. En effet la virtualisation est la pierre angulaire de plusieurs Clouds, puisque l'infrastructure virtualisée est indispensable pour assurer la flexibilité et l'évolutivité d'un Cloud.

Architecture virtualisé



Les principes de la virtualisation

- ***Le cloisonnement*** : chaque systeme d'exploitation a un fonctionnement independant, et ne peut interferer avec les autres en aucune maniere.
- ***La transparence*** : le fait de fonctionner en mode virtualise ne change rien au fonctionnement du systeme d'exploitation et a fortiori des applications.
- ***La transparence*** implique la compatibilite : toutes les applications peuvent tourner sur un systeme virtualise, et leur fonctionnement n'est en rien modifie.

Avantages de la virtualisation

- Usage optimale des ressources
- Installation, déploiement et migration facile
- Économie sur le matériel
- Sécurisation
- Isolation
- Allocation dynamique
- Diminution des risques

Composants d'un système virtuelle

- Le **système hôte (*host*)** est l'OS principal de l'ordinateur.
- Le **système invité (*guest*)** est l'OS installé à l'intérieur d'une machine virtuelle.
- Une **machine virtuelle (*VM*)** est un ordinateur virtuel qui utilise un système invité.
- Un ordinateur virtuel est aussi appelé **serveur privé virtuel** (*Virtual Private Server* ou VPS) ou environnement virtuel (*Virtual Environment* ou VE)

La machine physique (host machines)

- La machine physique est l'ordinateur physique, et les serveurs qui sont utilisés.
- Les machines physiques et les serveurs sont assembles par une combinaison du materiel physiques, un systeme d'exploitation et le logiciel qui tourne la dessus.
- Les composants majeurs d'une machine physique : un processeur CPU, RAM, Hard Disk, cartes de reseaux

La machine virtuelle (guest machines)

- un système informatique virtuel est un conteneur de logiciels parfaitement isolé intégrant un système d'exploitation et des applications. Chaque VM autonome est entièrement indépendante. 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 fine couche logicielle, appelée hyperviseur, dissocie les machines virtuelles de l'hôte, et alloue dynamiquement des ressources informatiques à chaque machine selon les besoins.

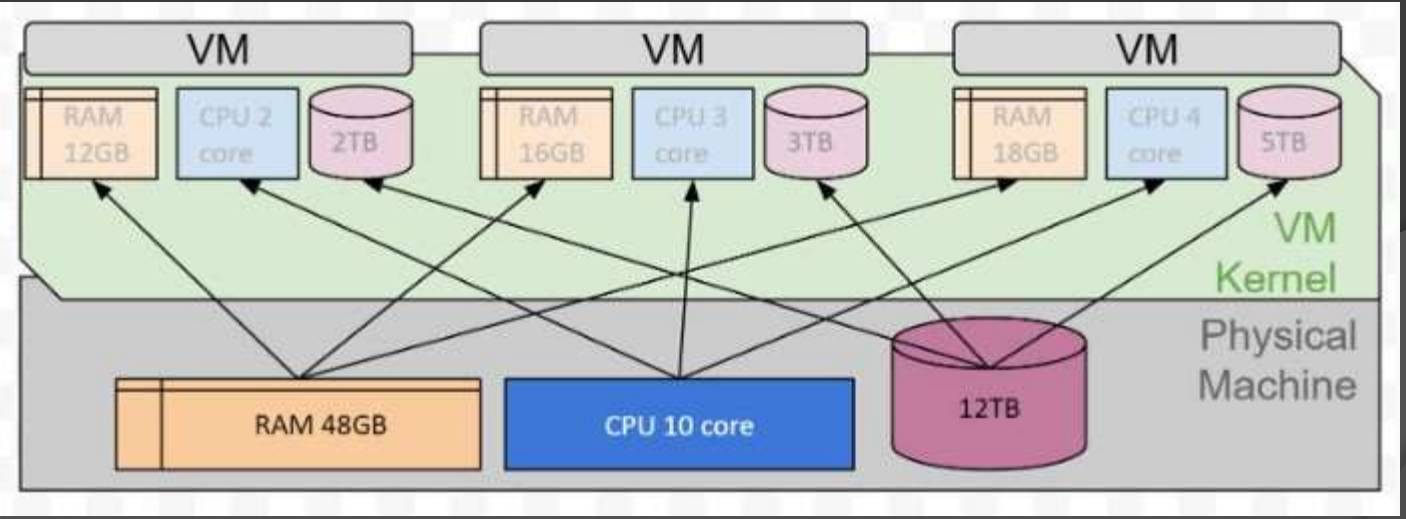
- Quelque soit la technologie utilisee, une machine virtuelle se compose de deux elements :
  - ***ressources*** : part de CPU alloues, memoire vive autorisee, nombre de cartes reseau virtuelles.
  - ***données*** : comme un serveur normal, on doit disposer d'un systeme d'exploitation, de bibliotheques, d'outils, d'applications et de leurs donnees.

La machine virtuelle (guest machines)

- Puisque les machines virtuelles fonctionnent comme des ordinateurs émulés indépendants, elles ont leur propre système d'exploitation et leurs propres logiciels / applications d'environnement.
- les machines virtuelles sont en fait mises en bac à sable à partir du reste de la machine physique et de son système d'exploitation et d'autres applications.
- Ceci est très utile, car nous pouvons utiliser plusieurs systèmes d'exploitation et environnements sur une seule machine physique à la fois.

Hyperviseur

- Pour creer des machines virtuelles (guest machines) sur une machine physique (host machine), nous avons besoin d'un logiciel hyperviseur.
- Un logiciel hyperviseur émule ou virtualise les composants de la machine physique en divisant le CPU, RAM, Disque dur et les cartes reseaux, et assigner ces ressources aux machines virtuelles (guest).

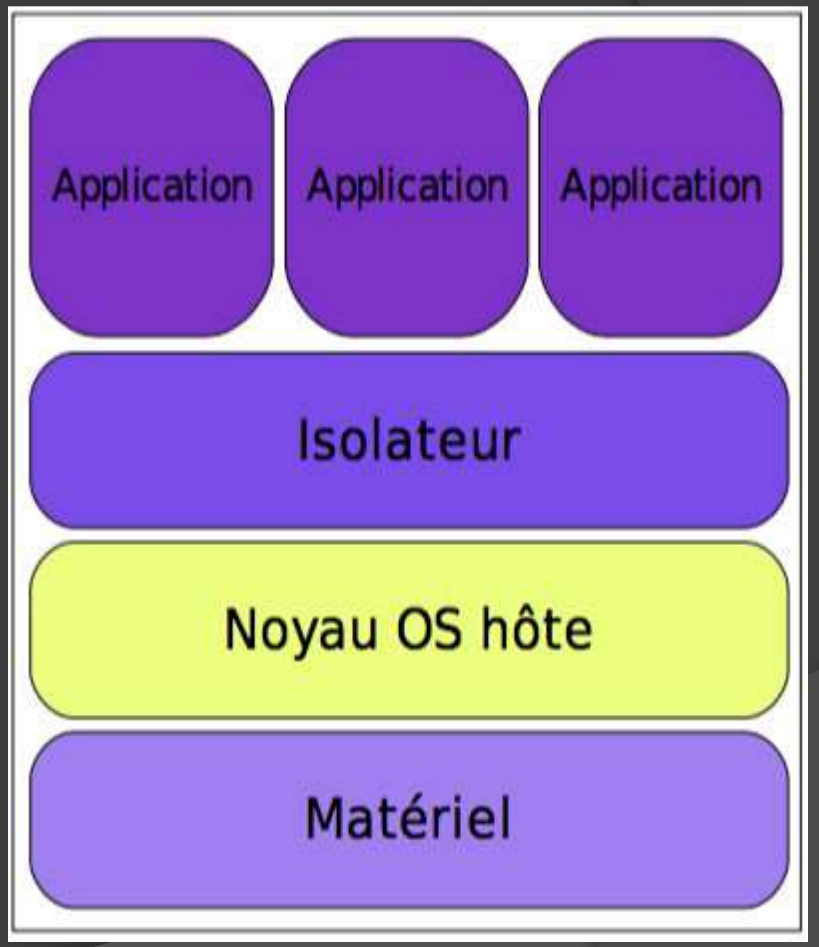


Techniques de virtualisation

- Virtualisation par application :
  - isolateur
- Virtualisation par serveur
  - machine virtuelle (Virtualisation complete)
- Para-virtualisation
  - Hyperviseur complet (type1 ou bar-metal)
  - Hyperviseur type 2
- Virtualisation par poste
- Virtualisation par Stockage
- Virtualisation par Cloud Computing

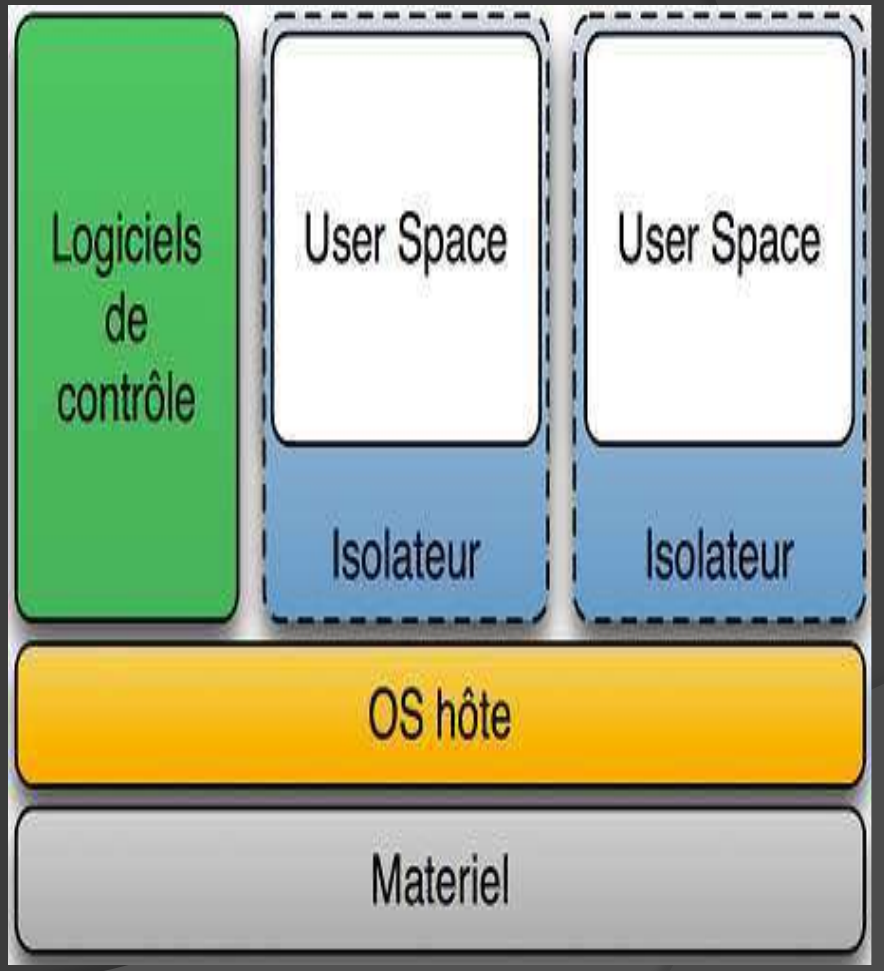
Technique de virtualisation d'OS ou isolateur (Virtualisation d'application)

- Isole l'exécution des applications dans des contextes d'exécution.
- Généralisation de la notion de « contexte » Unix, plus isolation des périphériques, et des systèmes de fichiers,
- Solution très performante et économique en mémoire mais Partage du code noyau (donc mauvaise isolation).
- Exemple : ***Docker,*** **chroot (changement de racine)**



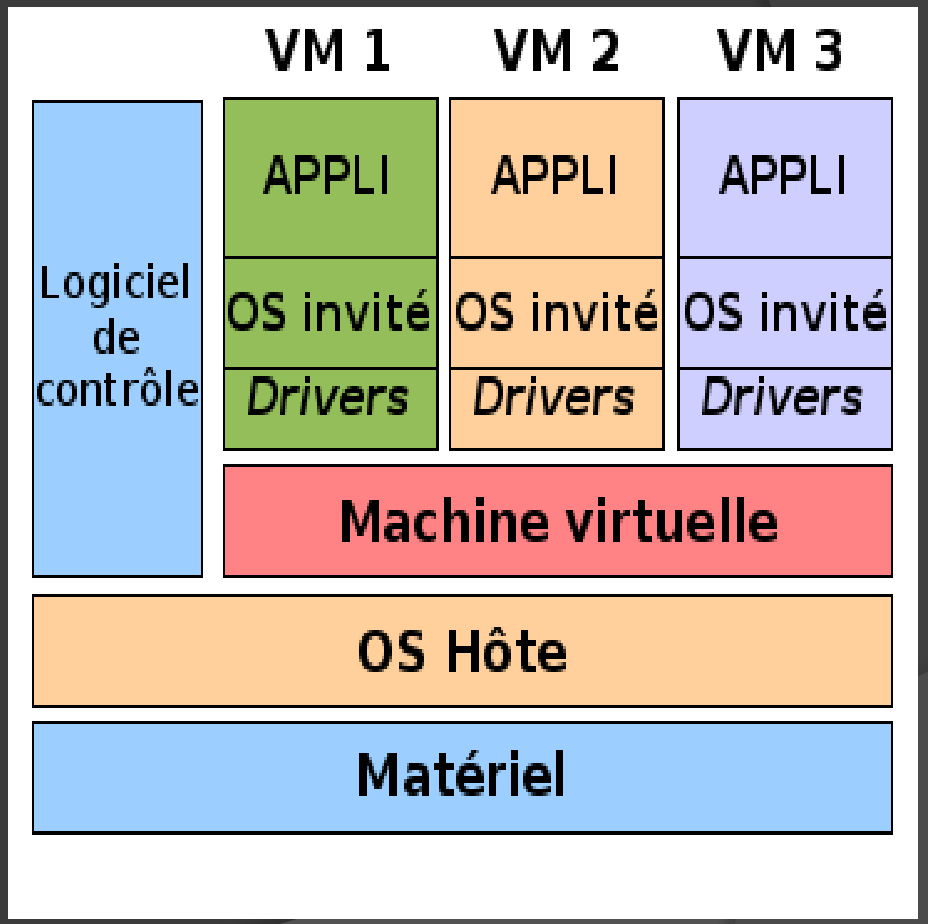
Les isolateurs

- Un isolateur est un logiciel permettant d'isoler l'execution des applications dans ce qui sont appeles des contextes, ou bien zones d'execution.
- L'isolateur permet ainsi de faire tourner plusieurs fois la meme application dans un mode multi-instance (plusieurs instances d'execution) meme si elle n'etait pas concue pour ca.
- Cette solution est tres performante, du fait du peu d'overhead (temps passe par un systeme a ne rien faire d'autre que se gerer), mais les environnements virtualises ne sont pas completement isoles.
- Uniquement lies aux systemes Linux, les isolateurs sont en fait composes de plusieurs elements et peuvent prendre plusieurs formes.
- 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).



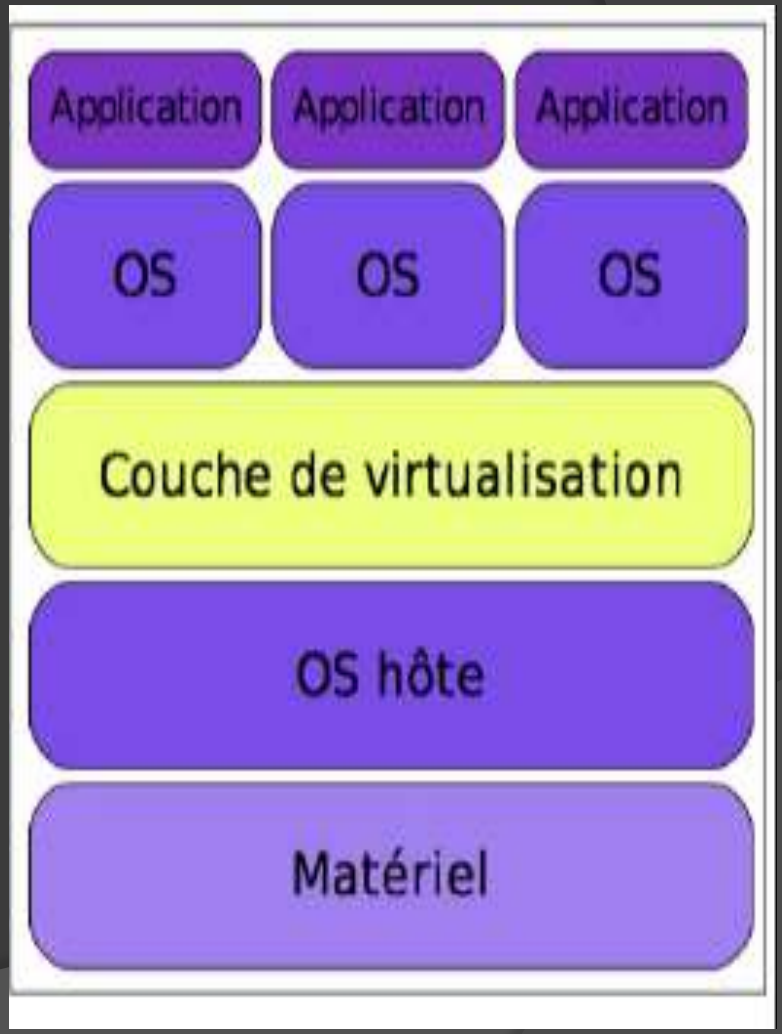
Technique de virtualisation par machine virtuelle

- ***Virtualisation complète*** :La virtualisation dite complete permet de faire fonctionner n'importe quel systeme d'exploitation en tant qu'invite dans une machine virtuelle. Pour l'utilisateur final, ce type de virtualisation est la plus simple a mettre en place et est la plus pratique.
- L'hyperviseur cree un environnement virtuel complet simulant litteralement un nouvel ordinateur complet, avec du "faux materiel". A quelques rares exceptions, le systeme d'exploitation invite (installe dans la machine virtuelle) ne communique qu'avec ce faux materiel simule, rendant etanche l'environnement virtualise.
- Ce type de virtualisation ne permet de virtualiser que des systemes d'exploitation prevus pour la meme architecture materielle que le processeur physique de l'ordinateur hote. Par exemple, un ordinateur equipe d'un processeur Intel x86 sera incapable de virtualiser un systeme d'exploitation prevu pour fonctionner dans une architecture PowerPC
- Exemple : VirtualBox - VMWare Player, VMWare Workstation- Parallels Desktop for Windows et Linux- KVM



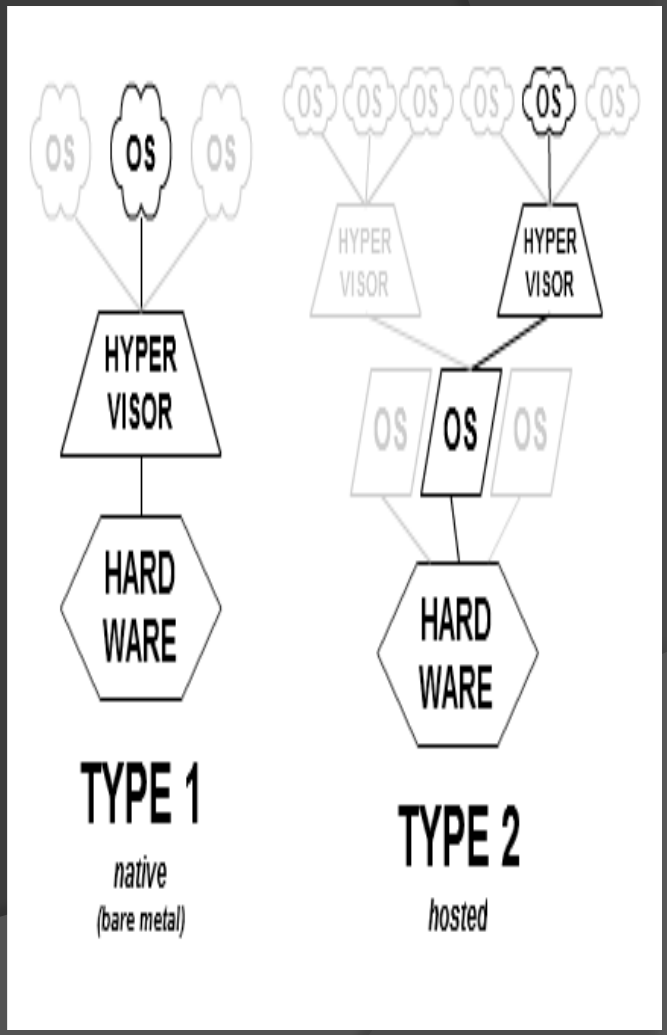
Technique de virtualisation par machine virtuelle

- Application installée sur l'OS Hote
- Virtualise et/ou émule le matériel
- Comparable à un émulateur mais accès « direct » au CPU, RAM, FS.
- Performances réduites si le CPU doit être émulé
- Bonne étanchéité entre les OS invités.
- Exemples : VirtualBox, QEMU, Vmware (workstation, fusion,player), Microsoft Virtual PC, Parallels desktop.



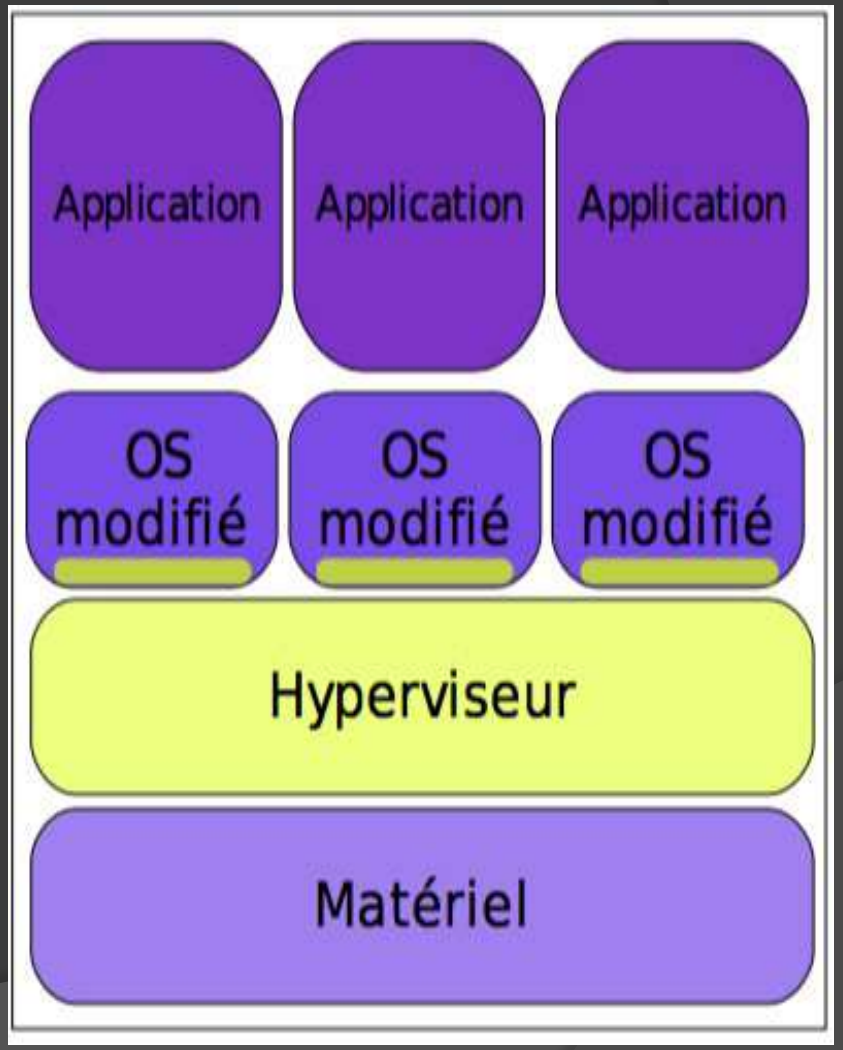
Les hyperviseurs

- Un hyperviseur est une plate-forme de virtualisation qui permet a plusieurs systemes d'exploitation de travailler sur une meme machine physique en meme temps.
- Un hyperviseur de type 1, ou natif, est un logiciel qui s'exécute directement sur une plateforme matérielle ; cette plateforme est alors considérée comme outil de contrôle de système d'exploitation. Un système d'exploitation secondaire peut, de ce fait, être exécuté au dessus du matériel. L'hyperviseur type 1 est un noyau hôte allégé et optimisé pour ne faire tourner initialement que des noyaux de systèmes d'exploitation invités adaptés et optimisés à cette architecture spécifique, ces systèmes invités ayant "conscience" d'être virtualités. Sur des processeurs ayant les instructions de virtualisation matérielle (AMD-V et Intel VT), le système d'exploitation invité n'a plus besoin d'être modifié pour pouvoir être exécuté dans un hyperviseur de type 1.Quelques exemples de tels hyperviseurs plus récents sont Xen, Oracle VM, ESX Server de VMware.
- Un hyperviseur de type 2 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 matériel. Les systèmes d'exploitation invités n'ayant pas conscience d'être virtualisés, ils n'ont pas besoin d'être adaptés. Quelques exemples de tels hyperviseurs sont VMware Workstation, VMware Fusion, l'hyperviseur open source QEMU, les produits Microsoft Virtual PC et Virtual Server, VirtualBox d'Oracle, de même que Parallels Workstation de SWsoft et Parallels Desktop.



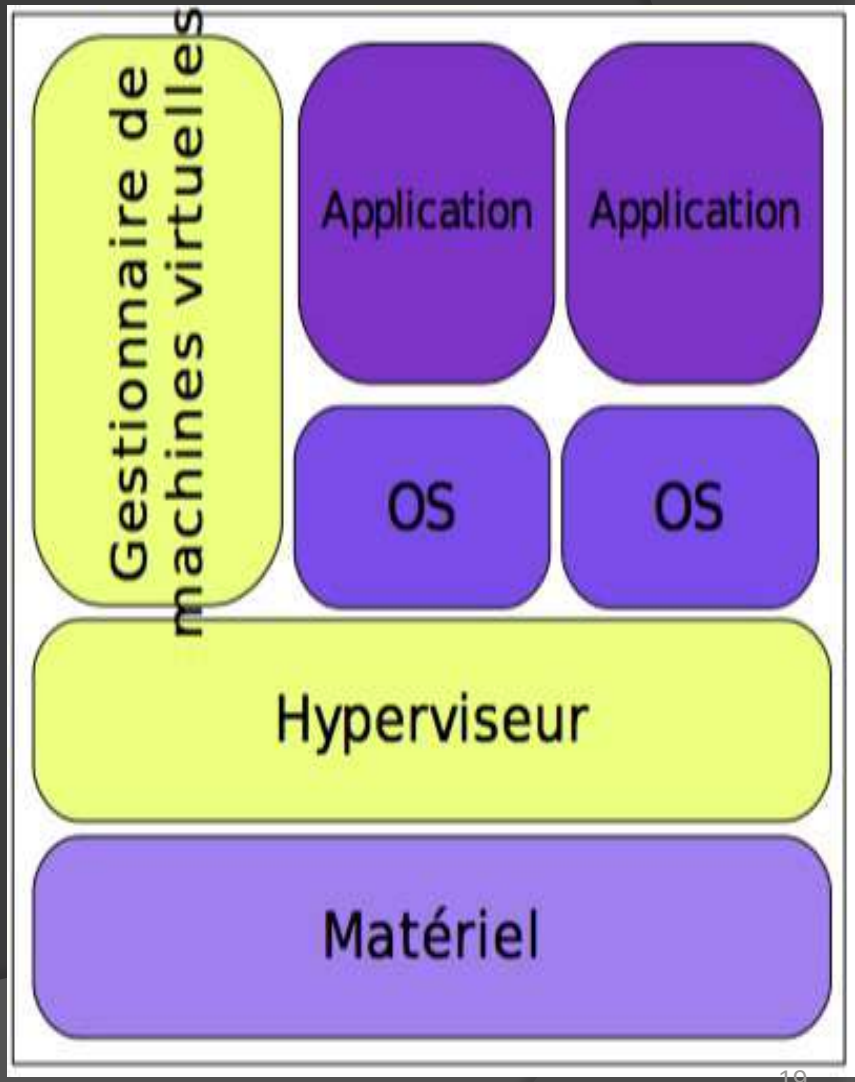
Techniques de virtualisation par Para-virtualisation

- La para-virtualisation fait intervenir un hyperviseur. Il s'agit d'un noyau allégé au dessus duquel viendront se greffer les systèmes invités. Contrairement à un système traditionnel de machines virtuelles où la virtualisation est transparente, avec la para-virtualisation, le système invité doit avoir conscience qu'il tourne dans un environnement virtuel ce qui implique d'employer un noyau modifié.
- Ce type de virtualisation permet des performances bien plus importantes que la virtualisation complète.
- L'hyperviseur et le systeme d'exploitation invité cooperent
- Noyau système allégé et optimisé,
- Noyau invités adaptés et optimisés pour fonctionner dans un environnement virtualisé, et prendre conscience qu'il tourne dans un environnement virtuel ce qui implique de deployer un noyau modifié.
- Utilisable sans les instructions spécifiques (ex : VT-x ou AMD-v). Impraticables pour les systèmes non libres.
- Exemple :Vmware vsphere, Xen *(moniteurs de contrôle* kvm, vmware esxi, xVM



Techniques de virtualisation par Hyperviseur complet (type1 ou bar-metal)

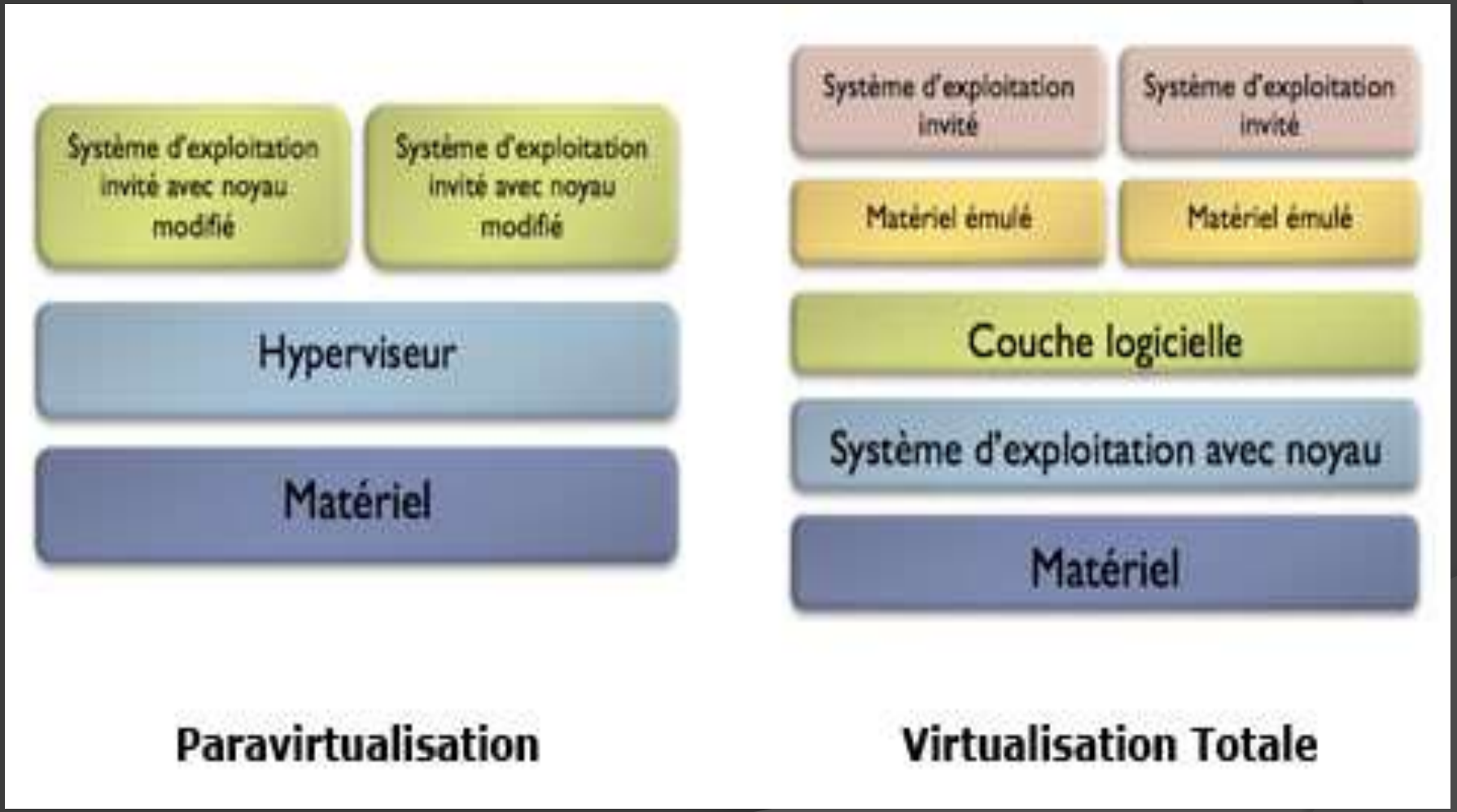
- Un système d'exploitation secondaire peut, de ce fait, être exécuté au-dessus du matériel, mais ne communique directement que via l'hyperviseur.
- Noyau système léger et optimisé
- Outils de supervision
- L'hyperviseur type 1 est un noyau hote allege et optimise pour ne faire tourner initialement que des noyaux de systemes d'exploitation invites adaptes et optimises a cette architecture specifique, ces systemes invites ayant ***"conscience" d'etre virtualises***.
- Permet l'exécution d'OS natifs.
- Sur des processeurs ayant les instructions de virtualisation matérielle (AMD-V et Intel VT), le système d'exploitation invité n'a plus besoin d'être modifié pour pouvoir être exécuté dans un hyperviseur de type 1.(Usage d'instructions dédiées à la virtualisation).
- Exemples: Oracle VM, Microsoft Hyper-V, ESX Server de VMware, l'hyperviseur LPAR de IBM



Techniques de virtualisation par Hyperviseur de type 2

- Un hyperviseur de Type 2 est un logiciel qui s'execute a l'interieur d'un autre systeme d'exploitation, on parle de virtualisation complete .
- Un systeme d'exploitation invite s'executera donc en troisieme niveau au-dessus du materiel.
- Les systemes d'exploitation invites n'ayant pas conscience d'etre virtualises, ils n'ont pas besoin d'etre adaptes.
- Quelques exemples de tels hyperviseurs sont VMware Workstation, VMware Fusion, l'hyperviseur open source QEMU, les produits Microsoft Virtual PC et Virtual Server, VirtualBox d'Oracle, de meme que Parallels Workstation de SWsoft et Parallels Desktop.
- **Limitations** : Ce type de virtualisation ne permet de virtualiser que des systèmes d'exploitation prévus pour la même architecture matérielle que le processeur physique de l'ordinateur hôte. Par exemple, un ordinateur équipé d'un processeur Intel x86 sera incapable de virtualiser un système d'exploitation prévu pour fonctionner dans une architecture PowerPC.

Différence entre les architectures



Virtualisation du stockage

- Gérer une interface qui permet de dissocier la gestion physique des disques (et de baies de stockage) vis-à-vis des serveurs qui l'utilisent.
- La virtualisation permet de masquer les spécifités physiques des unités de stockage.
- Côté utilisateur, les unités de stockage sont vues comme un unique volume
- Les systèmes de stockage fournissent soit des données en mode bloc, soit en mode fichier.
  - virtualisation en mode fichiers, en accédant au NAS en masquant les dépendances vis-à-vis de l'emplacement où les données sont physiquement stockées et l'acces au fichier s'effectue en mode NFS.
  - virtualisation en mode bloc, en introduisant un niveau d'abstraction entre le serveur et le système de stockage, ce qui donne plus de flexibilité pour les administrateurs (Exemple: IBM SAN Volume Controller, EMC Vplex)

Espace de stockage

- Dans les technologies de machine virtuelle, l'hyperviseur ne fournit au systeme virtualise qu'un espace de stockage.
- Il peut s'agir d'un volume, ou simplement d'un fichier, on peut placer l'integralite de cet espace sur un disque local, un reseau de stockage ou un autre serveur...
- L'utilisation d'un disque local est la solution la plus avantageuse en terme de performances et de facilite d'administration.
- Cependant, l'utilisation d'un stockage en reseau permet d'ouvrir la voie a de nouvelles fonctionnalites.

Stockage en réseau

- Les pleines capacites des hyperviseurs modernes ne peuvent s'exprimer qu'au travers d'un stockage en reseau, en effet les hyperviseurs sont generalement formant une force de travail globale qui se partageront les machines virtuelles a exécuter.
- Disposant d'un reseau de stockage, chaque hyperviseur a acces a toutes les machines virtuelles, et peut donc executer n'importe laquelle, et la transferer sans interruption a un autre hyperviseur en fonction de sa charge.

Serveur de stockage NAS

- Un serveur NAS (Network Attached Storage) est **un appareil de stockage de fichier connecté à un réseau local** (LAN).
- Ce type d'appareil permet le stockage et la récupération de données depuis une localisation centralisée pour les utilisateurs hétérogènes autorisés à accéder au réseau.
- Il est possible de se connecter à ce réseau spécifique par le biais d'une connexion Ethernet standard, ou directement en WiFi.
- Un NAS, ou stockage réseau (Network-Attached Storage) est simplement un serveur fournissant leurs fichiers a d'autres serveurs par le réseau.
- NFS (Network file storage) est le standard universel pour l'acces aux fichiers sur un reseau, c'est le protocole le plus utilise dans les NAS.

Serveur de stockage NAS

- il permet de stocker a distance les fichiers contenant les disques durs de la machine virtuelle. Ce dernier cas est déconseillé hors des environnements de test : NFS n'est pas adapte a la lecture aleatoire dans un seul fichier.
- En revanche pour un isolateur, stocker les donnees en NFS est interessant, et le deviendra encore plus avec les systemes de fichier de nouvelle generation tels que ZFS, HAMMER ou btrfs.
- En plus des materiels dedies, la plupart des systemes d'exploitation proposent une implementation serveur NFS, ce qui permet d'utiliser n'importe quel serveur comme serveur de stockage NFS.
- Ces derniers utilisent alors soit des disques locaux, soit leur propre reseau de stockage SAN.
- ***Le serveur NAS présente l'avantage d'être flexible et scalable***. Ainsi, en cas de besoin de capacité supplémentaire, il est possible d'ajouter de l'espace de stockage très facilement.
- C'est ce qu'on appelle *le scale-out ou en cluster (clustered).*

Serveur de stockage NAS

Un réseau de stockage SAN

- Un SAN, ou reseau de stockage (Storage Area Network), est un reseau sur lequel circulent les donnees entre un systeme et son stockage. C'est un réseau physique principalement en fibre optique, dont le but est de permettre la mise en relation des serveurs avec des baies de disques.
- Cette technique permet de deporter tout le stockage interne d'une machine vers un equipement dedie.
- Les SAN sont des equipements dedies, qui ne travaillent qu'aux plus basses couches du stockage, la notion de fichier leur est inconnue ; ils travaillent simplement sur des blocs de donnees et les fournit par le reseau a des serveurs qui eux sauront les utiliser.
- Cependant, les SAN les plus hauts de gamme sont dotes de capacites avancees, tel que la prise de cliche, ou encore la copie rapide de volumes.
- Les deux principaux protocoles d'acces a un SAN sont iSCSI et Fibre Channel.
- Les SAN constituent une plate-forme de communication qui exploite le protocole SCSI et virtualise totalement l'espace de stockage. Il travaille au niveau des blocs et non des fichiers comme les serveurs NAS.
- Les protocoles d'interconnexion utilisés pour la création d'un SAN sont les protocoles **Fibre Channel** et **iSCSI (*Internet Small Computer System Interface*)**.
- On peut dire q'un réseau de stockage SAN est un réseau local constitué de plusieurs périphériques
- Un commutateur SAN est un composant matériel qui connecte des serveurs à des pools partagés de périphériques de stockage. Il est consacré au déplacement du trafic de stockage dans un SAN.

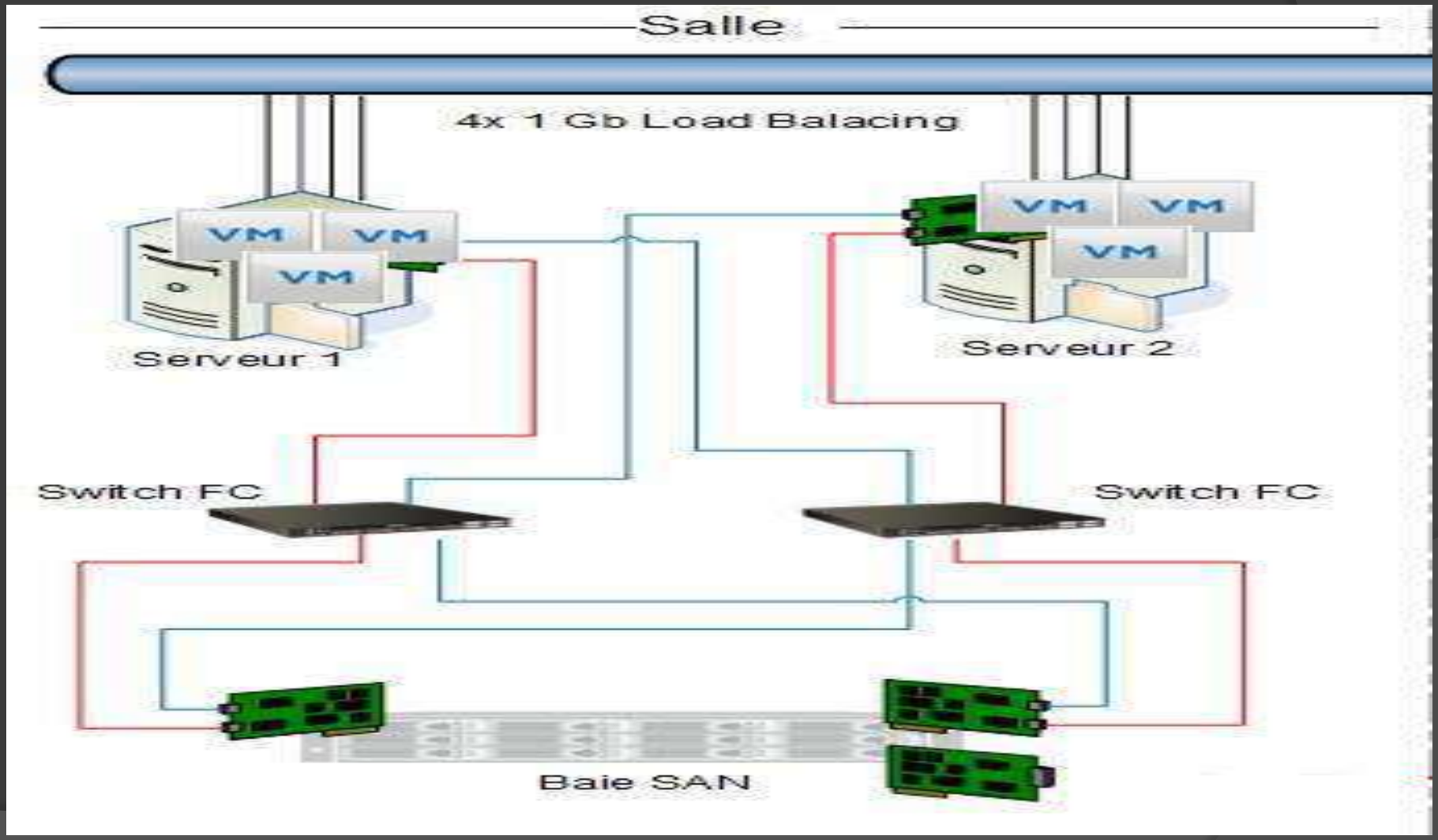
Le protocole d'acces iSCSI

- iSCSI (***Internet Small Computer System Interface***) est un protocole d'acces disque fonctionnant sur un reseau Ethernet, il permet d'implementer un reseau de stockage en profitant de la connectique et des equipements de commutation standards.
- Comme le NFS, il peut etre soit implemente par une baie de stockage dediee, ce qui assure les meilleures performances, soit par un serveur classique disposant du logiciel adequat, par exemple IET (iSCSI Entreprise Target) sous Linux.
- Voici un exemple de SAN : parmi les machines clientes du SAN, on retrouve un NAS : ces deux techniques peuvent etre combinees car elles ne travaillent pas au meme niveau.

Le protocole d’acces Fibre Channel

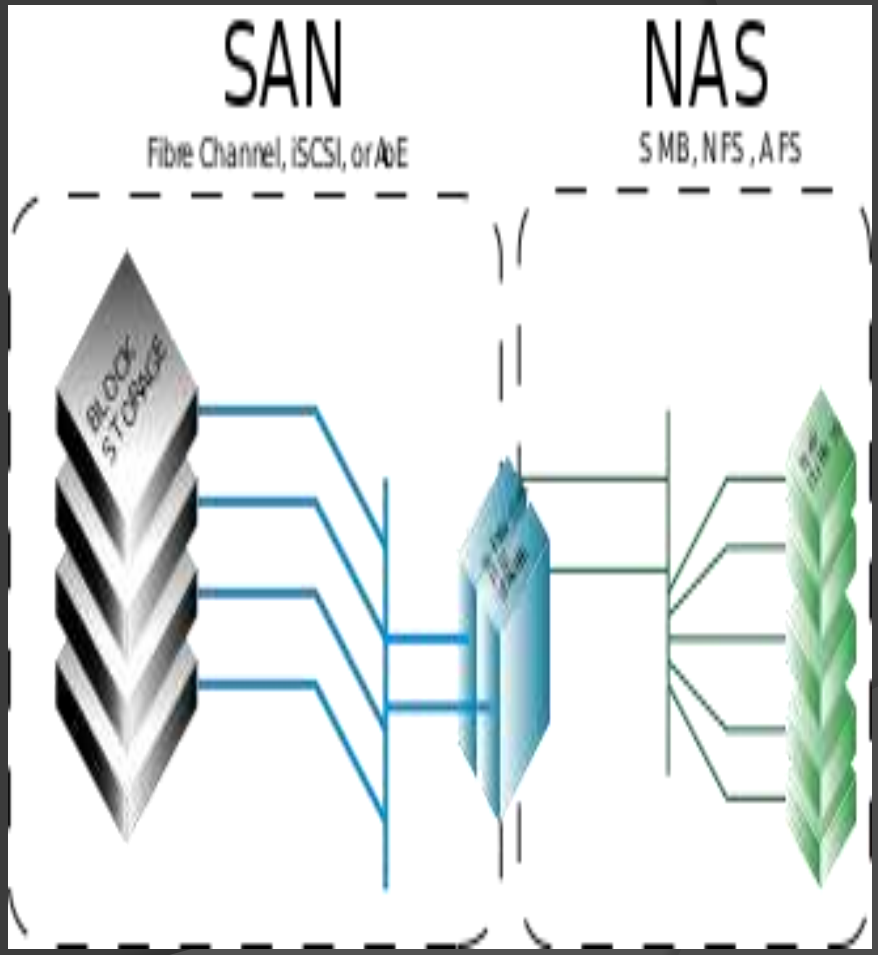
- La solution la plus haut-de-gamme pour implementer un reseau de stockage est l’utilisation d’une baie dediee et du protocole Fibre Channel.
- Base sur des fibres optiques il assure une latence et un debit bien meilleurs que iSCSI, a un prix bien sur plus eleve. Son principe d’utilisation est le meme qu’un SAN iSCSI.

Un réseau de stockage SAN



Comparaison entre SAN et NAS

- Dans le cas du NAS, la ressource de stockage est directement connectée au réseau IP de l'entreprise. Le serveur NAS intègre le support de multiples systèmes de fichiers réseau, tels que Common Internet File System (CIFS) protocole de partage de Microsoft et de Samba, Network File System (NFS) qui est un protocole de partage de fichiers Unix, ou encore AFP (AppleShare File Protocol) qui est l'équivalent pour la technologie Apple. Une fois connecté au réseau, il peut jouer le rôle de plusieurs serveurs de fichiers partagés.
- Dans le cas du SAN, les baies de stockage n'apparaissent pas comme des volumes partagés sur le réseau. Elles sont directement accessibles en mode bloc par le système de fichiers des serveurs. En clair, chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur. L'administrateur doit donc définir très précisément les Logical Unit Number (LUN, unités logiques), le masking et le zoning, pour qu'un serveur Unix n'accède pas aux mêmes ressources qu'un serveur Windows utilisant un système de fichiers différent.



Virtualisation du poste client

- Rendre le poste client en mode client léger.
- L'ensemble des ressources du poste client, données et logiciel, sont sur le serveur.
- L'administration est très nettement simplifiée tout comme la mobilité des utilisateurs (virtualisation du bureau).
- La virtualisation du poste client est un moyen radical mais efficace pour maîtriser le coût de possession.
- A titre d'exemple concret, voir les solutions de virtualisation du poste client de Citrix et XenServer.

Virtualisation par Cloud Computing

- La virtualisation facilite la mutualisation des ressources.
- Les spécifités techniques des unités informatiques de traitement et de stockage du Cloud Computing (Principe du cloud computing IaaS) sont transparentes pour l'utilisateur.
- La souplesse de montée en charge avec une capacité théoriquement infinie n'est pas le moindre des avantages.

Matériel de la virtualisation

- Le support de la virtualisation peut être intégré au processeur
- Virtualisation des accès mémoire
- Protection du processeur physique des accès bas niveaux
- Simplifie la virtualisation logicielle et réduit la dégradation de performance

Les processeurs et la virtualisation

- **Des processeurs NX/XD pour l'isolement des VM**
  - l'isolement consiste à empêcher un code d'application exécuté sur une VM d'accéder à l'espace mémoire utilisé par les autres VM
  - Les processeurs mettent en oeuvre ce type d'isolement de l'espace mémoire en utilisant un bit spécial qui permet de marquer certaines zones de la mémoire comme « non exécutables ».
  - Les processeurs AMD fournissent un bit NX (Never eXecute - ne jamais exécuter) et les processeurs Intel, un bit XD (eXecute Disable - désactiver l'exécution).
  - Cela empeche de perturber l' execution des VM en definissant une zone mémoire qui est marquée comme non exécutable, donc protégée, le processeur refuse d'y exécuter un code.
  - Il est toutefois judicieux de vérifier ce point dans la documentation du serveur ou de consulter le BIOS pour s'assurer que des options telles qu'Execute Disable Bit (bit de désactivation de l'exécution), NX Technology (technologie NX) et XD Support (prise en charge XD) sont activées.

Les processeurs et la virtualisation

- **Instructions LAHF et SAHF**
  - Dans les processeurs x86, le registre AH est ainsi connu comme registre « accumulateur »
  - Il est utilisé pour l'accès aux ports E/S, les opérations élémentaires à virgule flottante et les interruptions.
- Ces fonctions étant toutes essentielles dans un environnement virtualisé, les processeurs modernes peuvent en accélérer le traitement grâce à des commandes qui autorisent un contrôle direct du contenu du registre ; il s'agit des commandes Load AH from Flags (LAHF) et Save AH to Flags (SAHF).
- Un hyperviseur utilise ces instructions pour assurer un contrôle plus direct du traitement des E/S et IRQ (interrupt request) de chaque cœur de processeur.
- Tous les processeurs Intel et AMD actuels intègrent les instructions LAHF/SAHF en plus du jeu étendu d'instructions de virtualisation (Intel-VT et AMD-V).

Les processeurs et la virtualisation

- Les tables de pages étendues
  - dans un ordinateur virtualisé, cette traduction d'adresses doit s'effectuer à deux reprises chaque fois qu'un accès à la mémoire physique est nécessaire : la première fois pour l'instance hôte, la seconde pour l'instance invitée (la VM). Ce second niveau de traduction d'adresses complique la tâche du processeur, ce qui réduit les performances.
  - La traduction d'adresses est nécessaire car les processeurs doivent utiliser une table de pages ou un tampon de traduction (TLB, Translation Look-aside Buffer) pour convertir les adresses relatives en adresses physiques complètes quand une charge de travail a besoin d'accéder à la mémoire physique.
  - Les fonctions telles que SLAT d'Intel et RVI d'AMD améliorent les performances de virtualisation en étendant la table de pages afin de permettre à l'hyperviseur de déterminer les emplacements en mémoire physique des instances hôte et invitée en une seule étape au lieu de deux.

Les principales solutions (OpenSource)

- Qemu
- KVM
- XEN
- VirtualBox
- VMware
- OpenVZ
- Docker

Tableau comparatif

Hypervisor Attributes	VMware ESXi/ESX 4.1	Windows Server 2008 R2 with Hyper-V	Citrix XenServer 5.6
Small Disk Footprint	✓ 70 MB disk footprint (VMware ESXi)	⊘ >2GB with Server Core installation ~10GB with full Windows Server installation	⊘ 1.8GB
OS Independence	✓ No reliance on general purpose operating system (VMware ESXi)	⊘ Relies on Windows 2008 in Parent Partition	⊘ Relies on Linux in Dom management Partition
Hardened Drivers	✓ Optimized with hardware vendors	⊘ Generic Windows drivers	⊘ Generic Linux Drivers
Advanced Memory Management	✓ Ability to reclaim unused memory, de-duplicate memory pages, compress memory pages	⊘ No ability to reclaim unused physical memory, de-duplicate or compress pages	⊘ Recently added basic overcommit, but does not adjust memory allocation based on VM usage; no deduplication or compression of pages

XEN

- Xen est une solution de virtualisation open source developpee initialement par le departement informatique de l'Universite de Cambridge.
- Son developpement est aujourd'hui activement sponsorise par Citrix, qui a rachete l'editeur initial XenSource.
- Citrix distribue une version commerciale de Xen,
- nommee Citrix XenServer, particulierement adaptee a la virtualisation des
- OS Microsoft Windows et Linux RHEL et SLES. Elle est dotee d'une interface d'administration avancee, et d'un acces au support technique

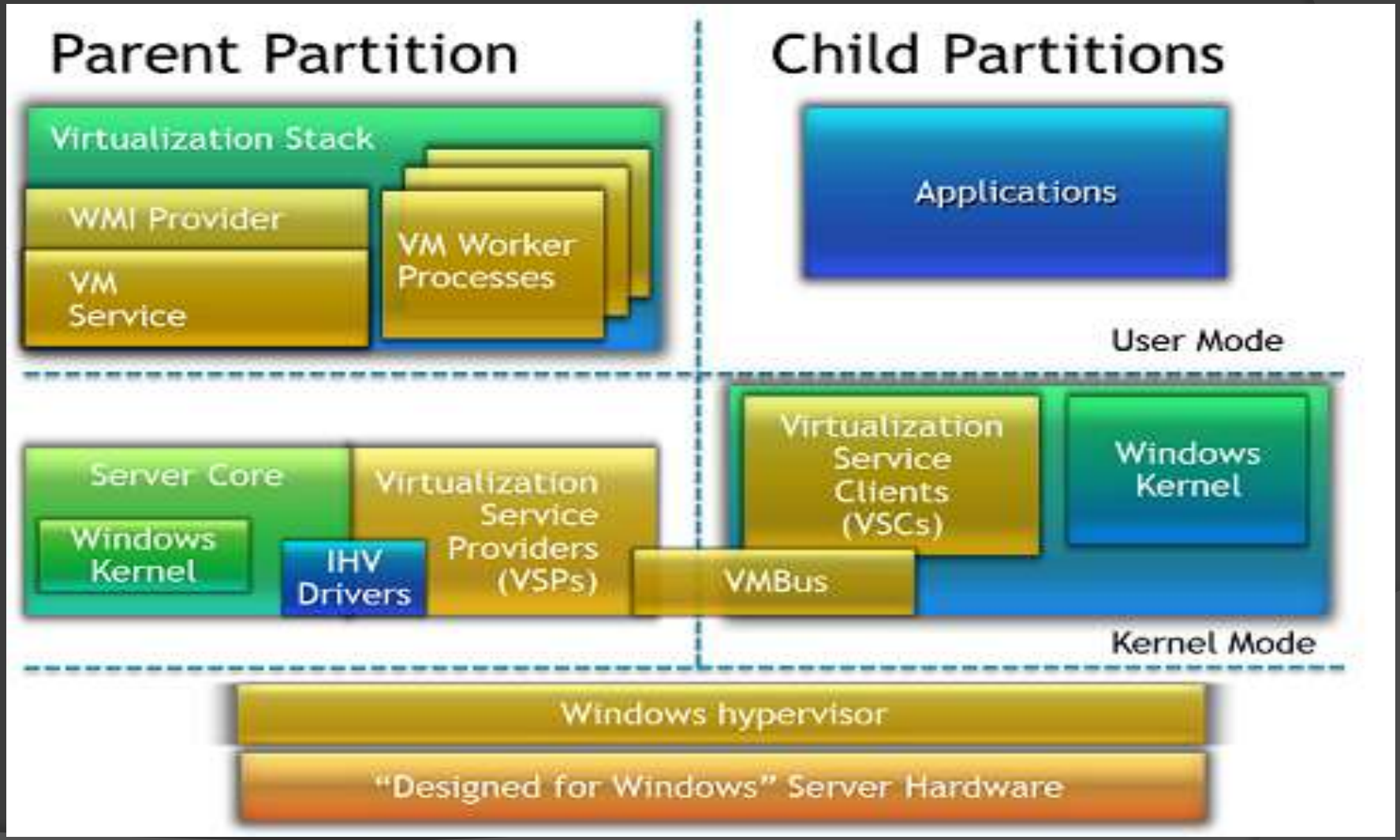
KVM

- KVM (Kernel-based Virtual Machine) est une machine virtuelle libre pour Linux.
- KVM, Kernel Virtual Machine, est integre depuis le noyau linux 2.6.20 et permet une virtualisation materielle et donc une acceleration de la virtualisation de systeme d'exploitation.
- Contrairement à des programmes comme VirtualBox, KVM fait appel au noyau du système d'exploitation de l'hébergeur pour émuler l'ordinateur ou le serveur physique
- C'est un systeme optimise pour la virtualisation de serveur (Pour virtualiser des systemes de type desktop, on peut lui preferer virtualbox.)
- KVM semble en effet plus performant en consommation de processeur mais plus lent pour l'emulation du peripherique graphique.

- Ne pas utiliser KVM en meme temps que VirtualBox. Il faudra en effet fermer KVM pour utiliser VirtualBox et vice versa. Ou desactiver le support de la virtualisation processeur dans VirtualBox.

VmWare-Vsphere

Microsoft Hyper-V

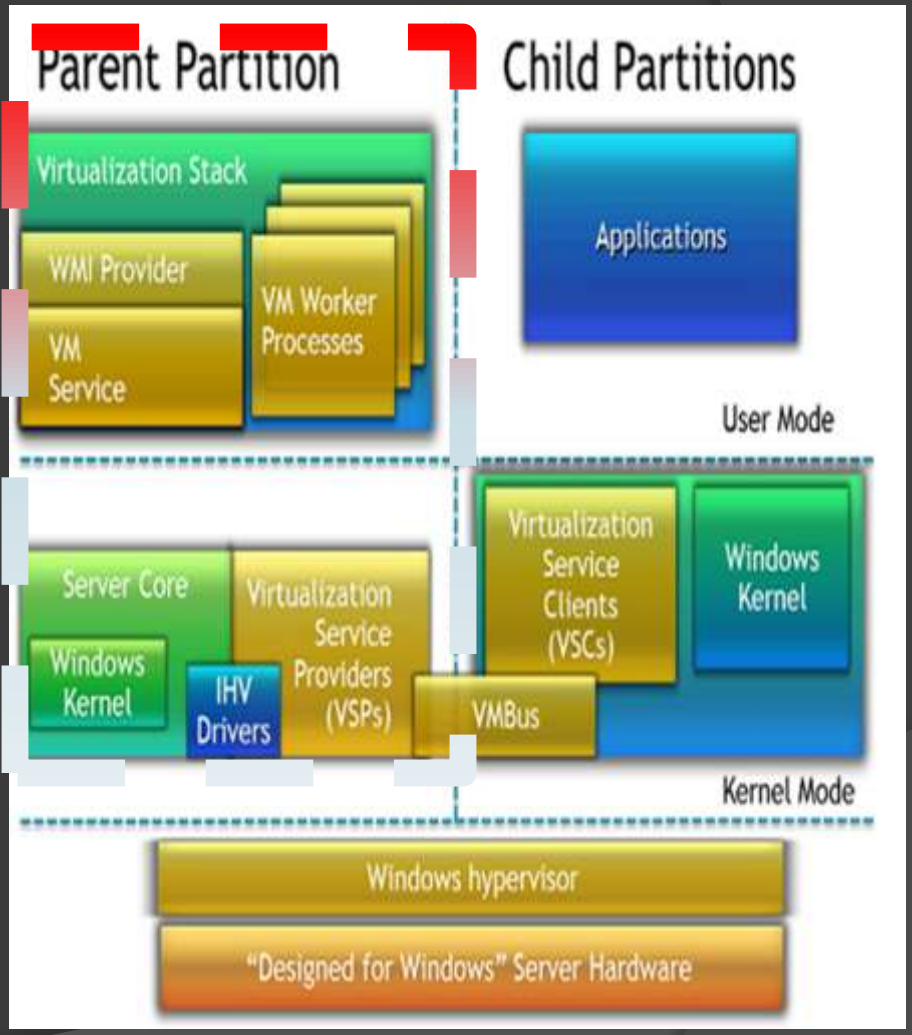


Microsoft Hyper-V

- la couche la plus basse appelée "Designed for windows server hardware » indique que seul materiel supporté par Microsoft sera accepté
- L’hyperviseur etablit la relation entre la machine physique et le virtuel, et separe la partie enfant et parent

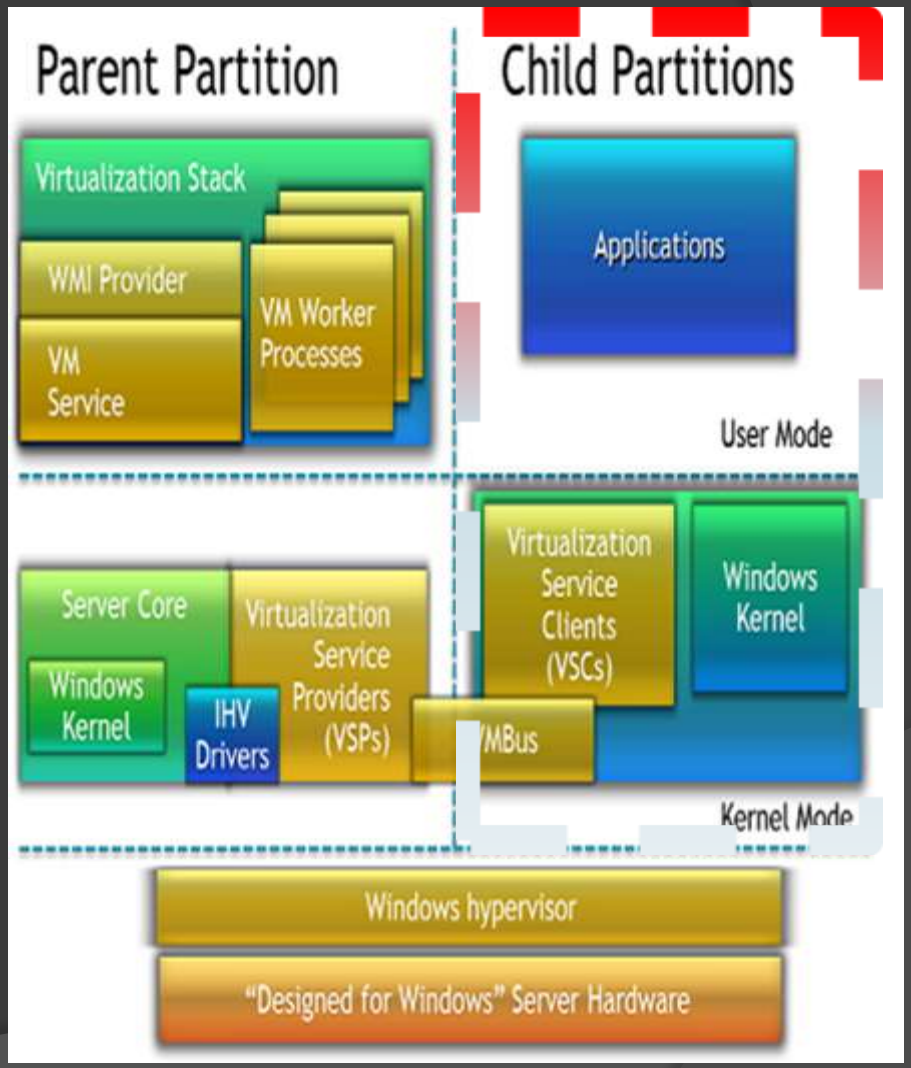
Microsoft Hyper-V: Partie Parent

- Cette partition est la base de l'installation, elle doit être installée obligatoirement en Windows 2008. De plus, c'est la partition parente qui offre les services de virtualisation aux partitions enfants.
- La description des partitions est réalisée en deux parties : le mode noyau et le mode utilisateur.
- le mode noyau :
  - Il contient le VSP (Virtualization services provider) qui permet l'émulation du matériel et de gérer les demandes d'accès à ce dernier.
  - Les drivers natifs sont également présent et assurent la connectivité avec le matériel physique
- le mode utilisateur:
  - VM Service: cette partie concerne le management des machines virtuelles pour toutes les partitions enfants
  - VM Worker Process : partie qui contient l'ensemble de la configuration des partitions enfants

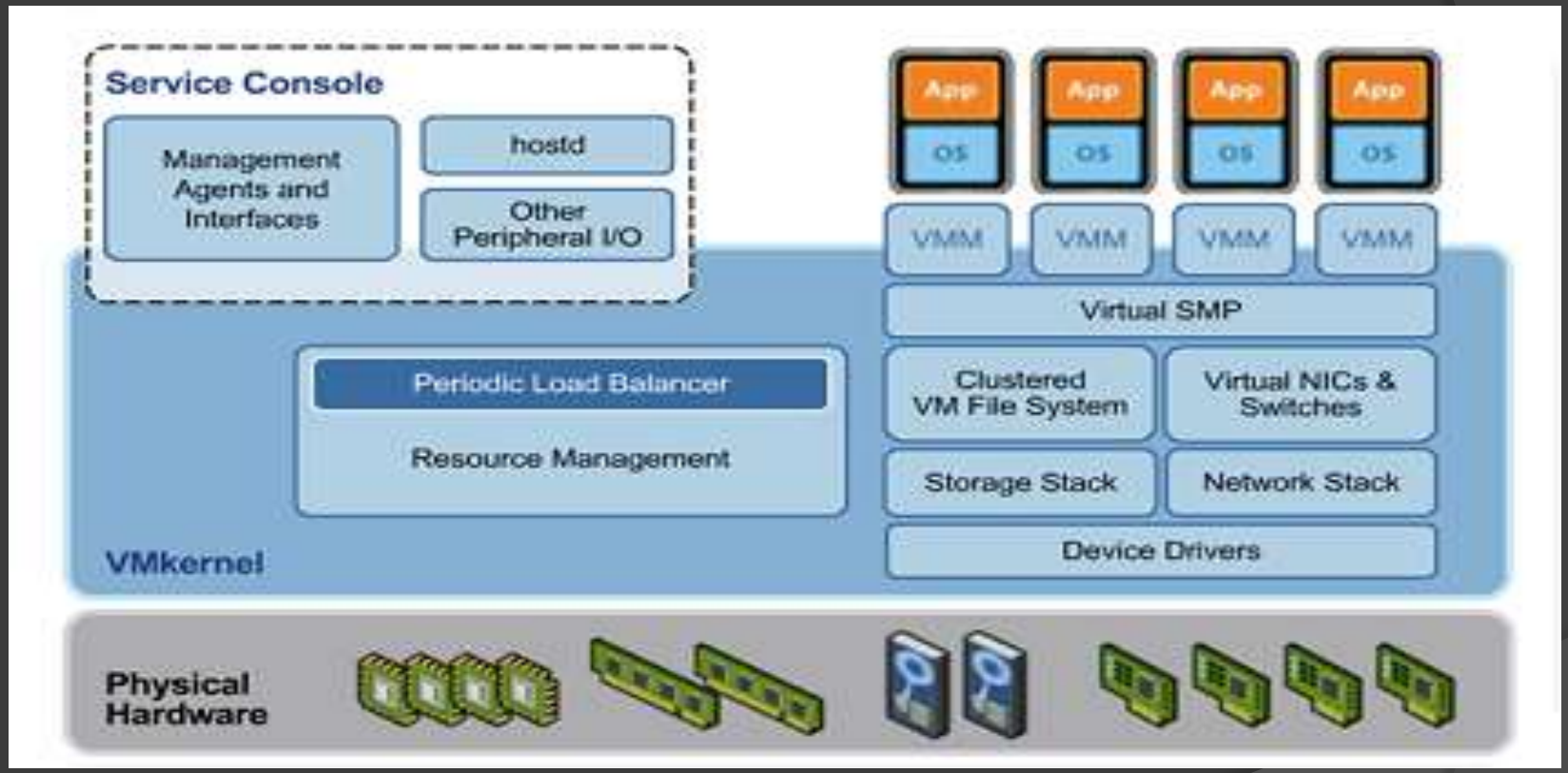


Microsoft Hyper-V: Partie enfant

- La partition enfant, contrairement à la partition parente, n'est pas unique. Il y en a une par machine virtuelle hébergée et gérée par la partition parente.
- L'application, le système virtuel mis en place, tourne dans le mode utilisateur de la partition enfant.
- Pour le mode noyau, deux points sont à détailler :
  - Les partitions enfants n'ont pas un accès direct au matériel elles utilisent donc le VSC (Virtualization service client) pour rediriger les demandes d'accès au matériel vers le VSP à travers le VMBUS



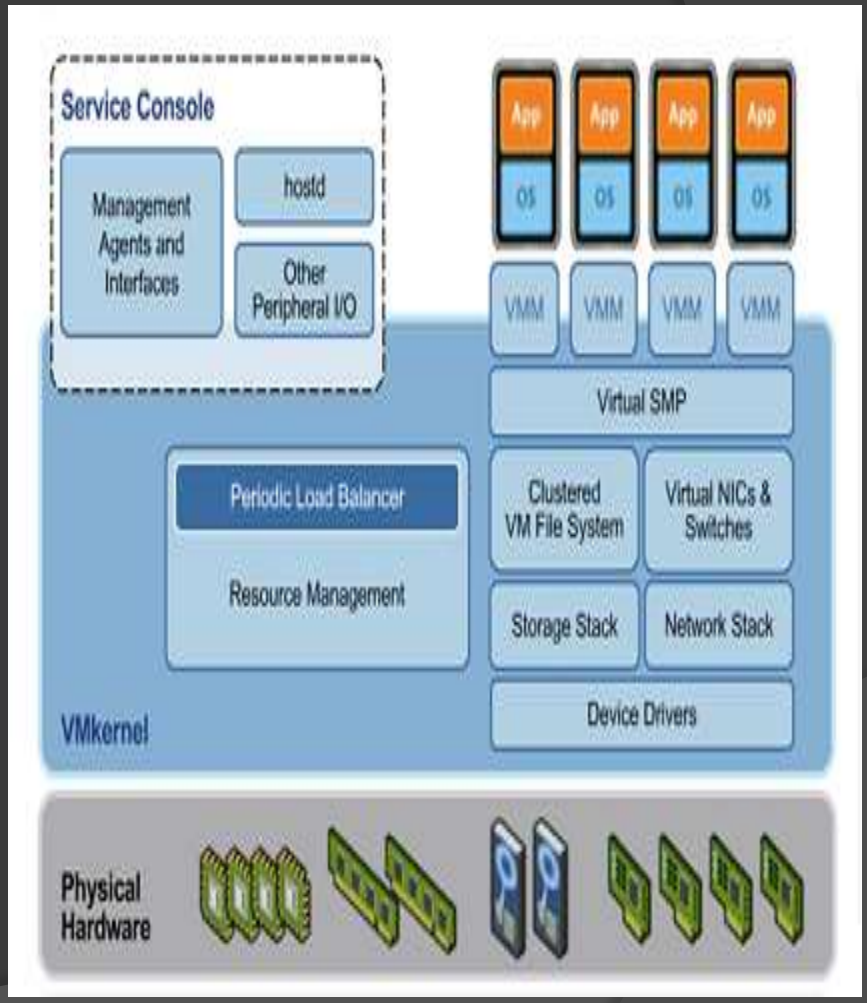
Vmware-Sphere: ESX



Architecture de l'hyperviseur Vmware-Sphere

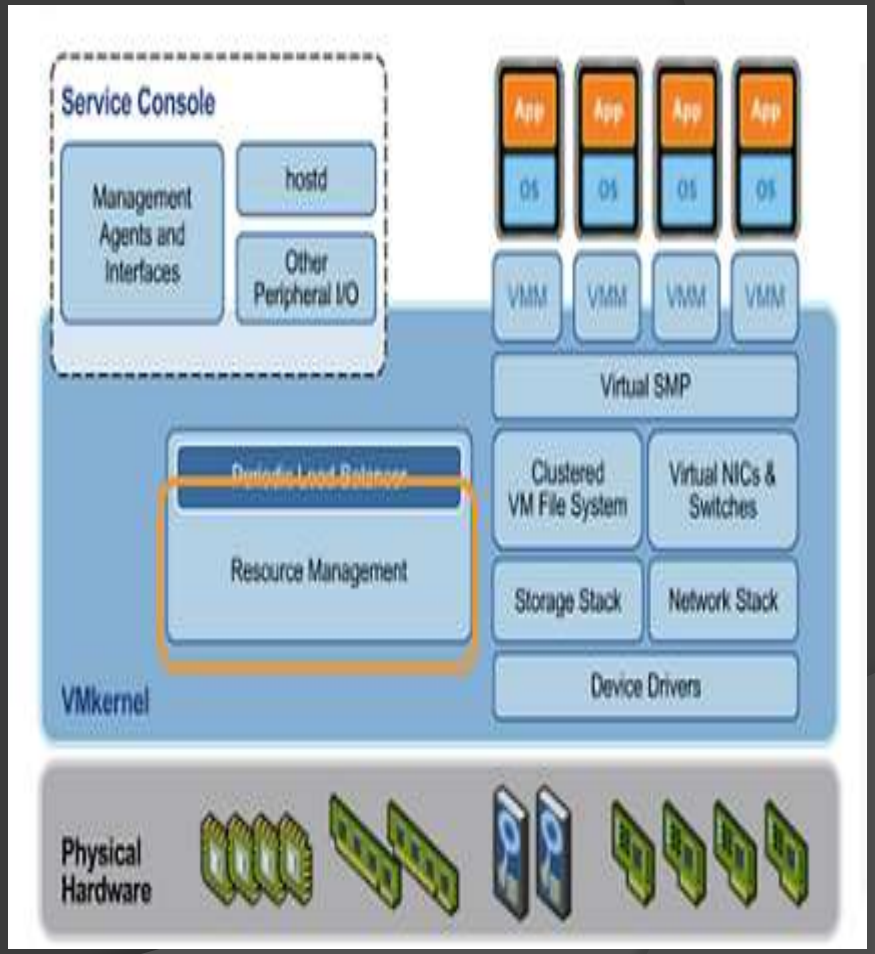
Vmware-Sphere

- **Virtual Machine Monitor**
  - La partie VMM est responsable de la virtualisation des processeurs
  - C'est VMM qui prend le contrôle de la machine virtuelle dès le démarrage
  - En somme, cela permet d'executer plusieurs environnements identiques sur une seule machine



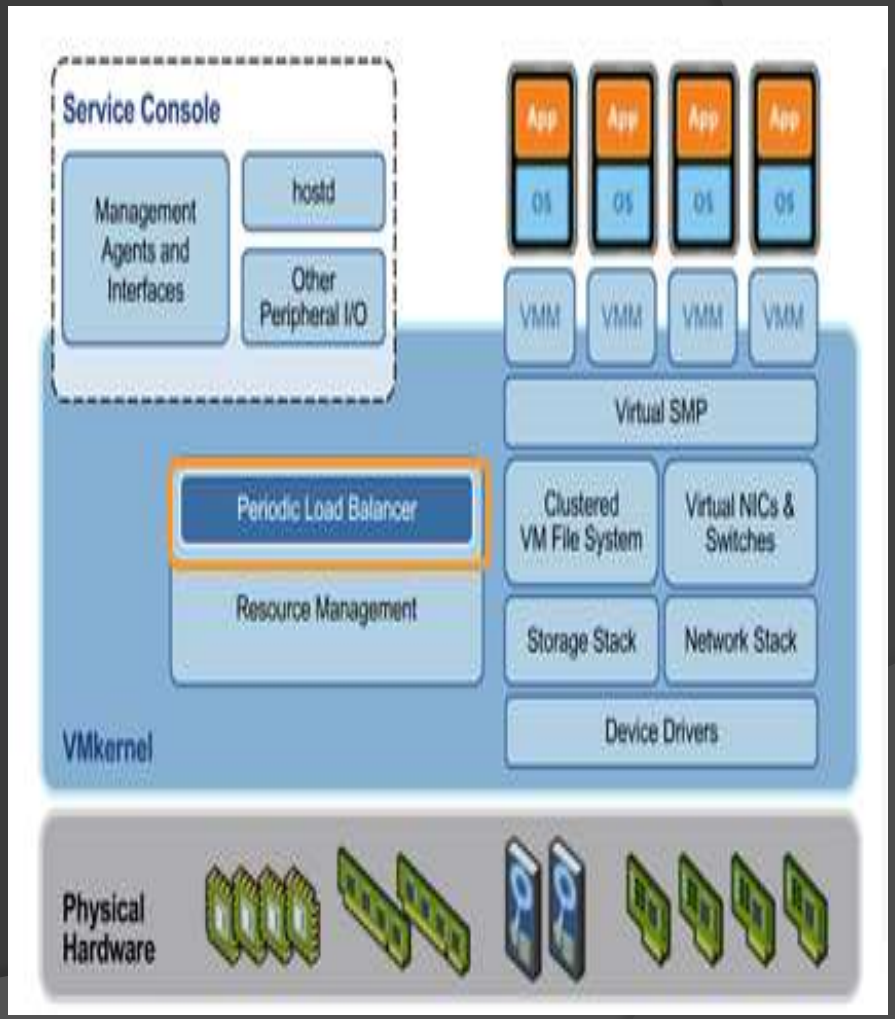
Vmware-Sphere: Resource Manager

- Il a pour charge de partitionner les ressources physiques entre les différentes machines
- Cela offre la possibilité aux administrateurs de spécifier des réservations et des limites pour les machines virtuelles
- Enfin, c'est ce ressource manager qui ordonance le temps d'accès au processeur



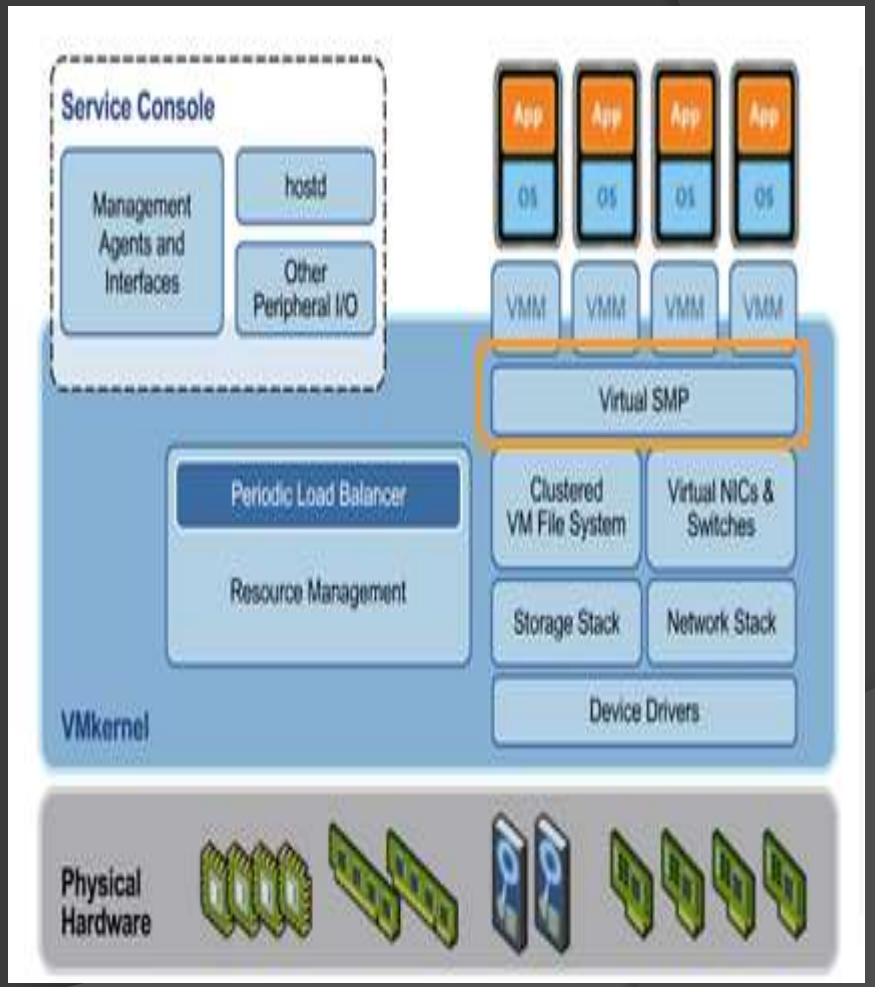
Vmware-Sphere: Periodic Load Balancer (l'équilibrage de charge périodique)

- La gestion du processeur est faite à deux endroits.
- En effet, le VMkernel ordonance les processeurs indépendamment tandis que le Periodic Load Balancer prévaut et décide sur quel processeur sera réellement ordonancé la VM.
- Sa fonction principale est de garantir une bonne répartition du processeur entre les machines virtuelles. Pour cela, il vérifie toutes les 20 millisecondes l'utilisation du processeur et migre les machines virtuelles en conséquence pour garantir cette bonne répartition.
- La migration des machines virtuelles peut etre effectue entre les serveurs du meme espace de stockage ou entre deux espaces de stockage.
- VMware offre la possibilité de changer la machine d'espace de stockage en déplaçant le home directory et ensuite on copie le contenu du disque entier dans la destination en prenant en compte les modifications apparus dans le premier disque.



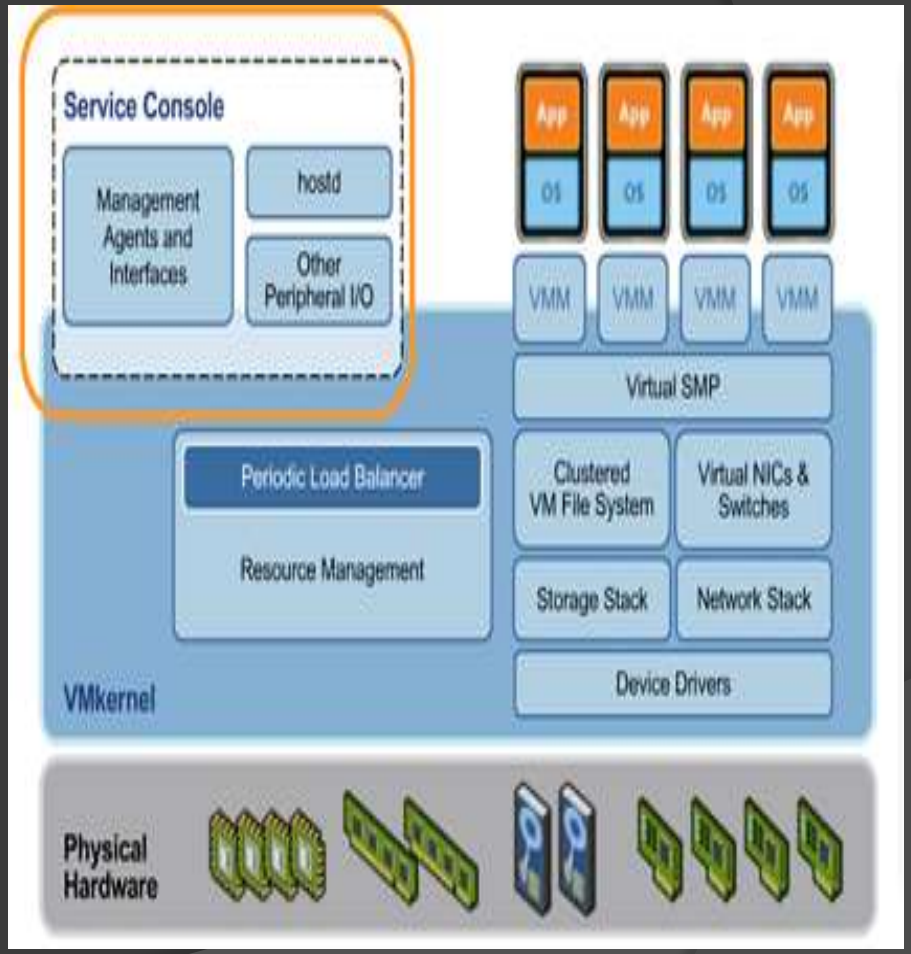
Vmware-Sphere: Virutal SMP

- Virtual SMP (Symetric Multi processing) permet à une machine virtuelle d'utiliser jusqu'à quatre processeurs physiques en même temps.
- Grâce à cela il devient possible de virtualiser les applications gourmandes en processeur (BDD, serveurs de messagerie).
- Avant l'implémentation de virtual SMP, un seul processeur était alloué à plusieurs machines.

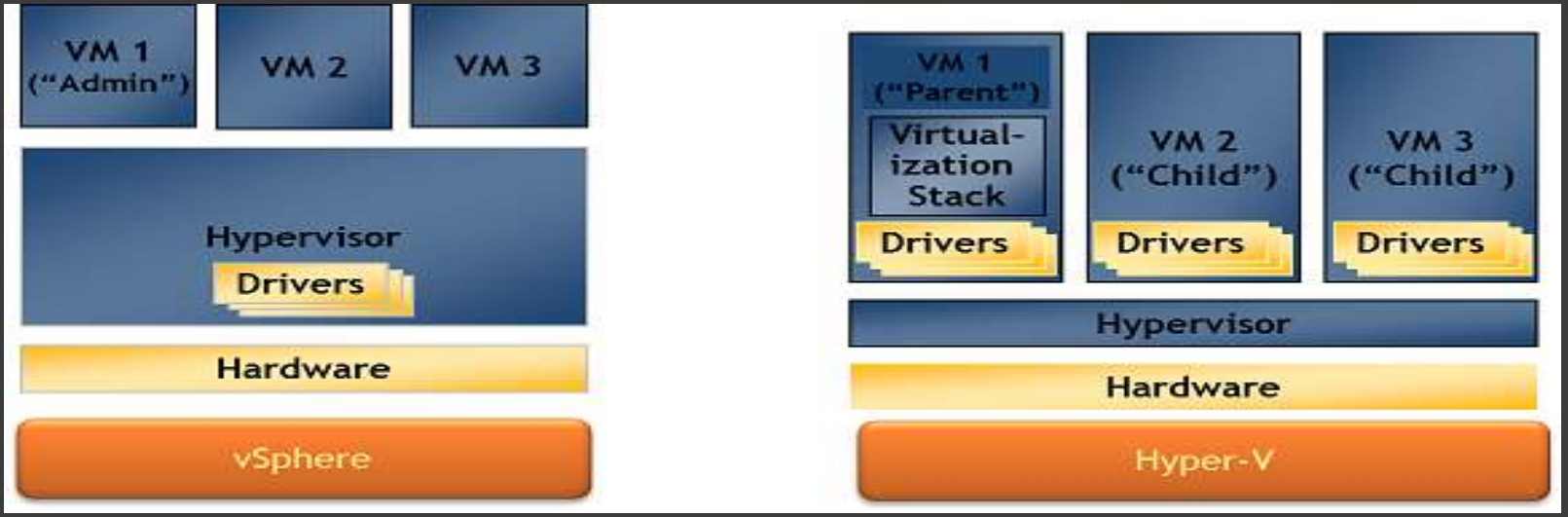


Vmware-Sphere: Service Console

- Il offre l'accès en ligne de commande à l'ESX
- Il offre également un accès web à l'ESX
- Enfin, il permet depuis cet accès distant de manager et monitorer voire même de créer des machines virtuelles



Comparaison entre les Hyperviseurs V-sphere et Hyper-V



- Chez Vmware, ils sont embarqués dans l'hyperviseur. L'éditeur s'efforce donc de garantir leur parfaite compatibilité, il faut donc toujours vérifier que le serveur et les périphériques (stockage, réseau) sont certifiés et validés pour Vmware.
- Hyper-V est un composant du système d'exploitation Windows Server. À ce titre, il supporte l'ensemble des matériels et des pilotes actuellement pris en charge par Windows.

L’emulateur de machine QEMU

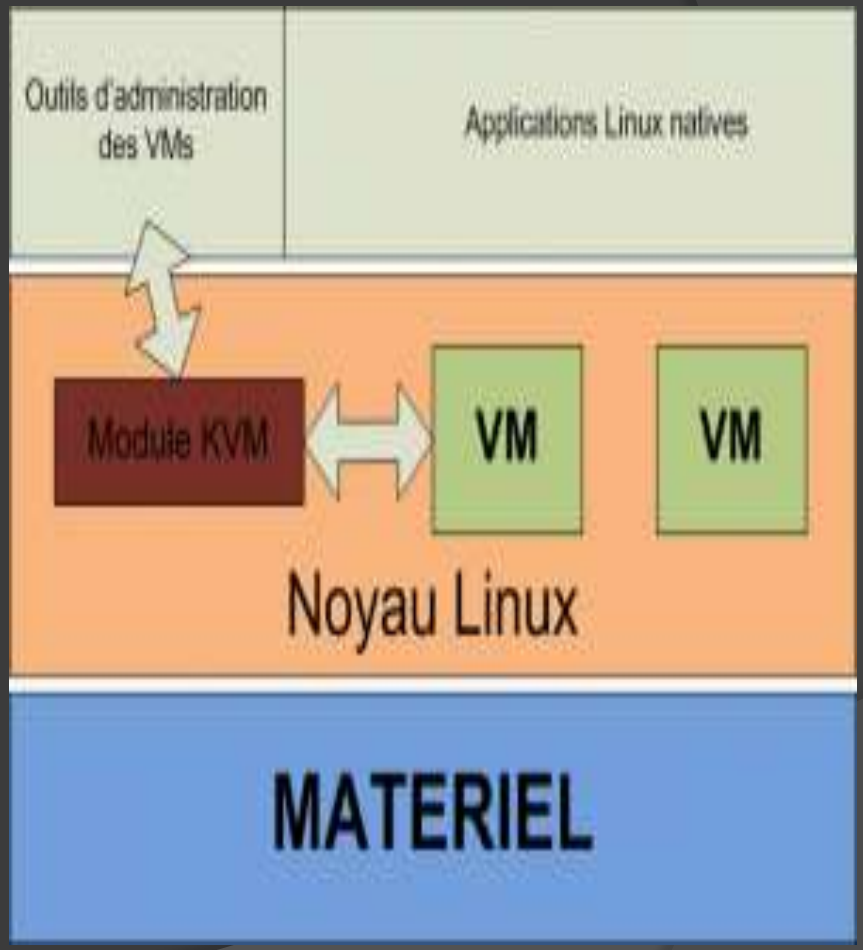
- Machine virtuelle complète
- Techniquement très aboutie
- Émulation complète de machine (x86,ARM,MIPS,…)
- L’usage du module *kQemu* pour une virtualisation
- accélérée.
- Émulation par recompilation sur un modèle « just-intime »
- Gourmand en mémoire
- Sans accéleration lent et charge l’hôte.
- Ex : VirtualBox et KVM reposent sur Qemu

KVM

- KVM pour Kernel Virtual Machine est une autre technologie de virtualisation Open Source et est distribuée sous licence GPLv2 ou LGPL.
- A l'origine fork de l'émulateur QEMU, les deux projets sont régulièrement synchronisés et la partie spécifique à KVM se concentre sur l'accélération matérielle des VM (profitant des jeux d'instructions des CPU) et sur l'intégration dans le noyau Linux. Le module noyau KVM est disponible nativement dans le noyau Linux depuis février 2007.

Architecture de KVM

- KVM est disponible sous forme de module Linux, intégré au noyau Linux.
- Le processus de démarrage du serveur hôte n'est pas modifié par la présence de KVM, et une machine virtuelle se résume à un processus Linux comme un autre.
- On peut comparer KVM à Virtualbox ou VMWare Workstation (hyperviseur de « type 2 »), à ceci près que, bien que l'administration de l'hyperviseur se fait depuis « l'espace utilisateur » (user-land), la machine virtuelle elle-même tourne en espace noyau (kernel-land).



Avantages et limites de KVM

- KVM ne supporte pas la paravirtualisation donc nécessite une CPU avec le support de la virtualisation matérielle.
- Pour obtenir des performances d'E/S satisfaisantes pour les VM HVM (hardware virtualised machine), KVM profite de l'intégration native des pilotes VirtIO (Virtual IO) dans le noyau Linux depuis la version 2.6.25 (avril 2008).
- Ces pilotes sont optimisés pour un contexte de virtualisation (PV on HVM). On profite ainsi de la facilité de la virtualisation complète (inutile de modifier le système invité) avec les performances de la paravirtualisation.
- Évidemment comme les drivers VirtIO ne sont pas intégrés d'office dans Microsoft Windows, ainsi comme c'est le cas pour Xen, il faudra les mettre en place a posteriori d'une installation d'une VM Windows.
- Bien qu'il existe des implémentations de KVM pour *BSD, KVM est d'abord développé pour Linux. Toutes les distributions majeures de GNU/Linux supportent KVM