Cours virtualisation et Cloud Computing

Preparer par : Nawal lounis

Leçon1- Principes de la virtualisation

CONTENU :

I. Introduction et définitions
II. Les différents types de virtualisation
III. Les domaines de la virtualisation
IV. Avantages & inconvénients de la virtualisation
V. Outils de virtualisation
VI. Centres de données et la virtualisation
VII. Sécurité et virtualisation

I. INTRODUCTION Et Définitions

Lorsqu'on parle d'informatique, on cite généralement deux concepts : Le concept du matériel et le concept du logiciel. Le matériel et logiciel sont deux domaines différents, le premier fournit les équipements physiques constituant les ordinateurs, le second fournit les données et les applications qui parcourt un ordinateur.

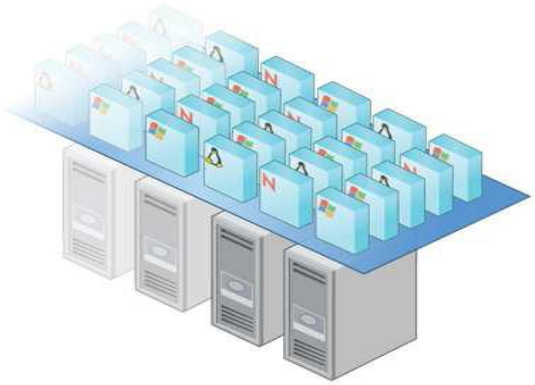
La virtualisation permet de changer exactement l'approche de l'informatique en repoussant les limites du matériel, le matériel étant cycliquement obsolète et tombant régulièrement en panne. L'objectif de la virtualisation est de brise la connexion réelle entre la couche matérielle et logiciel de l'informatique

1. C'est quoi la virtualisation

La virtualisation est une couche d'abstraction qui brise la connexion réelle entre le matériel physique et le système d'exploitation. Une infrastructure virtuelle est une solution au niveau de l'entreprise qui fournit une informatique puissante et fluide qui maximise l'utilisation des ressources et les économies de coûts.

Les machines virtuelles sont l'élément clé d'une infrastructure virtuelle. La virtualisation permet d'exécuter plusieurs machines virtuelles avec des systèmes d'exploitation hétérogènes et aux applications d'être exécutées en isolation, côte à côte sur la même machine physique.

En utilisant la virtualisation, vous pouvez déplacer dynamiquement des ressources où elles sont nécessaires et déplacer le traitement où il convient. C'est possible parce que la virtualisation détache le système d'exploitation et ses applications du matériel sur lequel ils sont exécutés



2. HOTE ET MACHINES VIRTUELLES :

Un hôte : est un ordinateur qui emploie le logiciel de virtualisation pour exécuter des machines virtuelles. En général, un hôte est un ordinateur exécutant le logiciel VMWARE WORKSTATION ou ESXI...

Les hôtes fournissent des ressources CPU et mémoire utilisées par les machines virtuelles Et leur donnent l'accès au stockage et aux réseaux. Plusieurs machines virtuelles peuvent traiter le même hôte en même temps.

Une machine virtuelle: est un ordinateur logiciel qui, comme un ordinateur physique, exécute un système d'exploitation et des applications. Un système d'exploitation installé sur une machine virtuelle s'appelle un système d'exploitation client.

Chaque machine virtuelle possède des périphériques virtuels qui fournissent la même fonctionnalité que le matériel physique. Les machines virtuelles obtiennent le CPU et la mémoire, les cartes vidéo, l'accès au stockage et la connectivité réseau à partir des hôtes sur lesquels elles s'exécutent.

Les machines virtuelles ne sont pas des émulateurs (pratiquer le même comportement qu'un matériel physique) ou des simulateurs (modéliser un système réel). Ce sont des vraies machines qui peuvent faire les mêmes choses que les ordinateurs physiques et plus encore. En raison de la flexibilité des machines virtuelles, les ordinateurs physiques deviennent moins un moyen de fournir des services (applications, bases de données et ainsi de suite) et plus un moyen d'héberger les machines virtuelles qui fournissent ces services.

Dans VMWARE WORKSTATION, les machines virtuelles sont exécutées sur des hôtes. Plusieurs machines virtuelles peuvent fonctionner sur le même hôte en même temps.

3. Hyperviseur :

Avec la virtualisation, le système d'exploitation (OS) invité accède à l'architecture matérielle sous-jacente par l'intermédiaire d'un noyau système très léger nommé hyperviseur. L'hyperviseur agit comme un arbitre entre les systèmes invités. Il attribue du temps processeur et des ressources à chacun, redirige les requêtes d'entrées sorties vers les ressources physiques, veille au confinement des invités dans leur propre espace (Renaud, 2005). Il existe deux types d'hyperviseur

a. Hyperviseur de type 1 :

Un hyperviseur de Type 1 ou natif, voire « bare metal » (littéralement « métal nu »), est un logiciel qui s'exécute directement sur une plateforme matérielle (Wikipedia, 2013). Avec un hyperviseur de Type 1, le système d'exploitation invité accède à l'architecture matérielle sous-jacente par l'intermédiaire d'un noyau système très léger (Wikipedia, 2013).

- ✓ L'hyperviseur de Type 1 agit comme un arbitre entre les systèmes invités. Il attribue du temps processeur et des ressources à chacun, redirige les requêtes d'entrées-sorties vers les ressources physiques, veille au confinement des invités dans leur propre espace (Renaud, 2005).

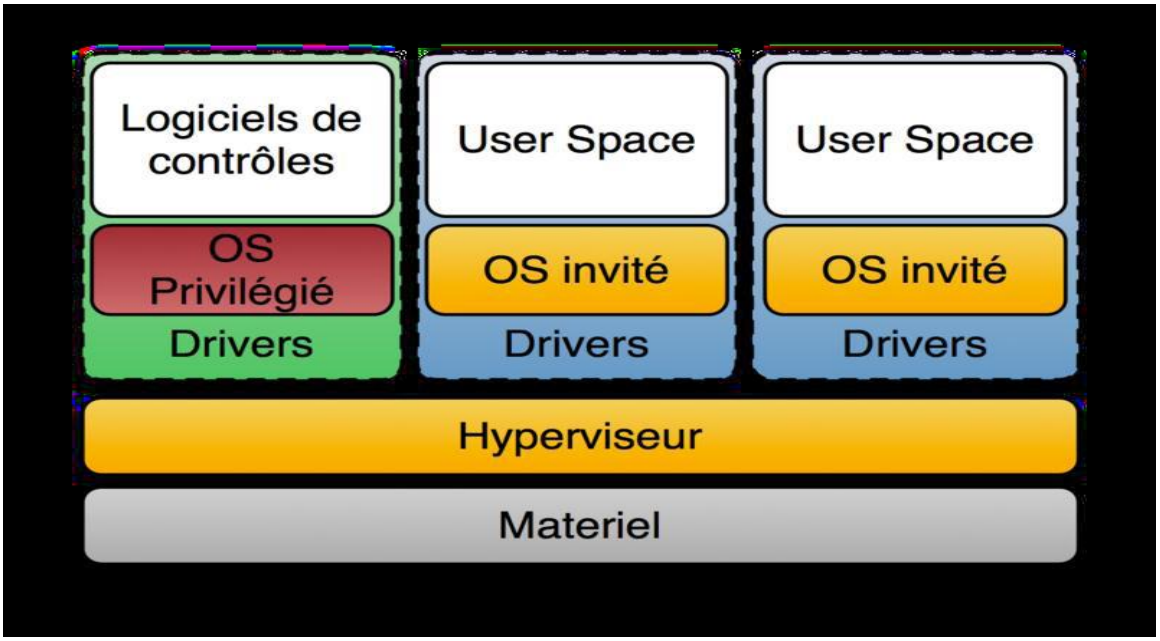


Figure 3 - hyperviseur de Type 1

L'hyperviseur de Type 1 est la méthode de virtualisation d'infrastructure la plus performante dans le cas de la virtualisation d'un centre de traitement de données (Wikipedia, 2013). Plusieurs éditeurs proposent des solutions logicielles de virtualisation avec hyperviseur comme VMware vSphere, Citrix XenServer, Microsoft Hyper-V, Promox VE.

b. Hyperviseur de Type 2 :

Un hyperviseur de Type 2 est un logiciel de virtualisation des systèmes qui s'exécute à l'intérieur d'un autre système d'exploitation (Wikipedia, 2013). L'hyperviseur de Type 2 est consommateur de ressources. L'hyperviseur de Type 2 recrée, par voie logicielle, un environnement d'exécution complet pour un programme ou un système invité. Toutes les opérations de l'invité sont interceptées et traduites pour être exécutées par l'environnement hôte, ce qui est une méthode très consommatrice en ressources (Renaud, 2005). Le schéma suivant illustre le mécanisme d'hyperviseur de Type 2 (Wikipedia, 2013) .

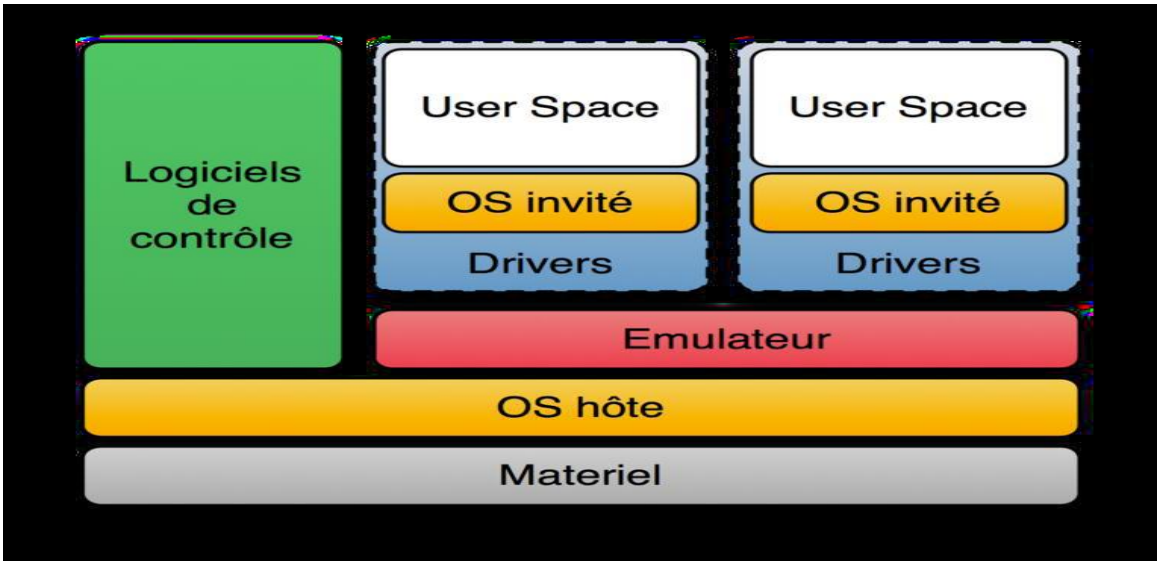


Figure 4 - hyperviseur de Type 2

Une solution de virtualisation avec un hyperviseur de Type 2 est plutôt destinée à des usages de tests et n'est pas adaptée à des contextes de production. Plusieurs éditeurs proposent des solutions logicielles, faciles à mettre en oeuvre, avec des technologies d'émulation comme Microsoft Virtual PC, Oracle VM VirtualBox, VMware Player.

II. Les différents types de virtualisation :

il existe plusieurs types 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.

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

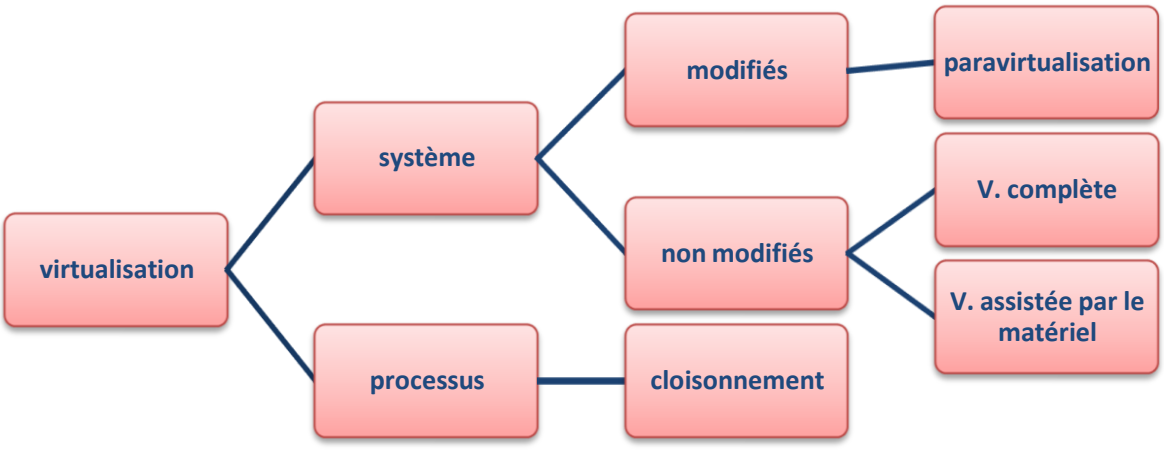


Figure 4 : Types de Virtualisation

1. Virtualisation complète

La virtualisation complète (full virtualization), dénommée ainsi par opposition à la para-virtualisation, consiste à émuler l'intégralité d'une machine physique pour le système invité. 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.

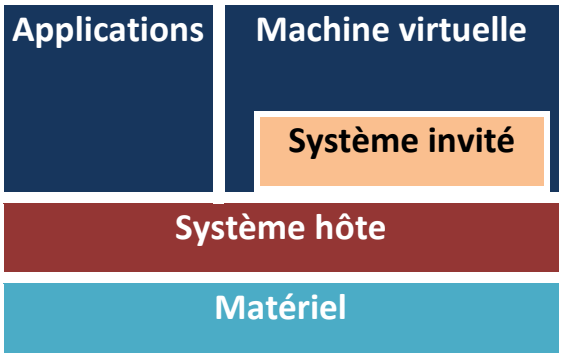


Figure 5 : Modèle de virtualisation complète

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.

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)

2. la para-virtualisation ;

La para-virtualisation est 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 machine virtuelle, cette dernière s'exécutant au dessus d'un système hôte. Toutefois, dans une solution de para-virtualisation, le système invité est modifié pour être exécuté par la machine virtuelle.

La para-virtualisation évite d'utiliser un système hôte complet pour faire la virtualisation. A la place, un noyau très léger de système d'exploitation hôte est utilisé. Les performances sont bien meilleures en para-virtualisation qu'en virtualisation complète.

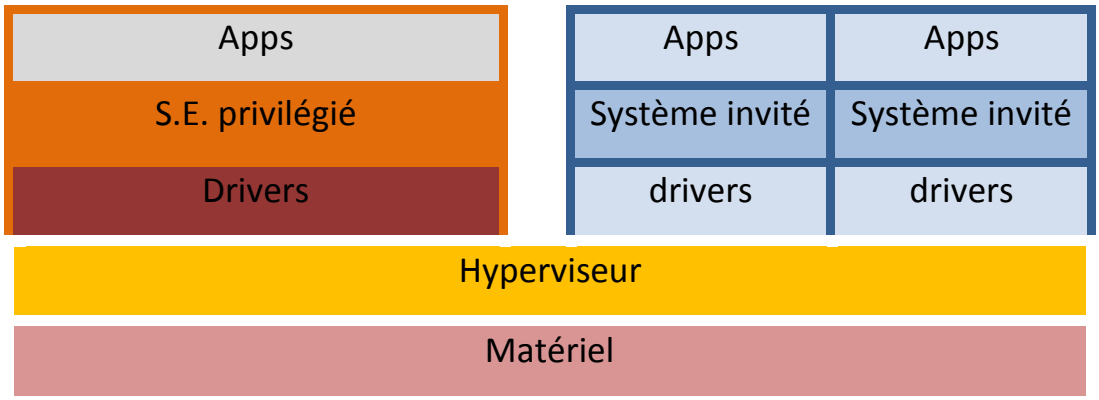


Figure 6 : modèle de paravirtualisation

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

3. le cloisonnement.

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

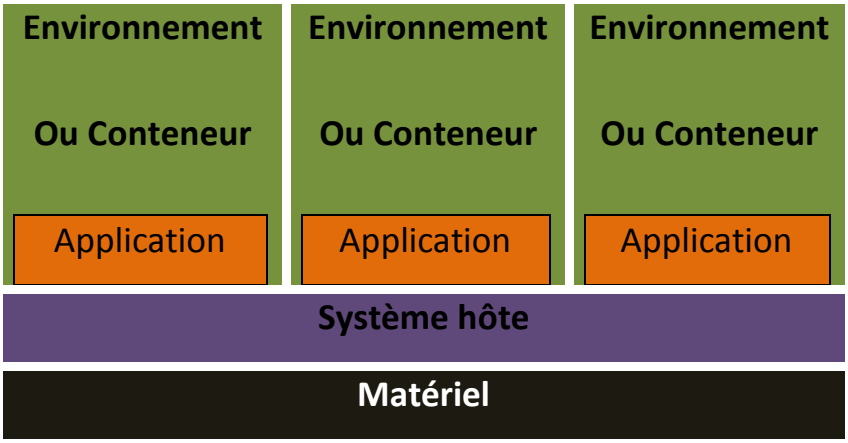


Figure 7 : modèle de cloisonnement

4. la virtualisation assistée par le matériel ;

Face a l'essor de la virtualisation de serveurs, les constructeurs de micro-processeurs, tel qu'Intel et AMD, ont décidés d'apporter leur propre nouveaux processeurs assistants à la virtualisation sur le marché.

- Intel-VT pour Intel Virtual Technology
- AMD-V pour AMD Virtualization

On parlera alors de virtualisation assisté matérielle, ou encore hardware-assisted virtualization.

Dans la virtualisation assistée par le matériel, des instructions sont ajoutées au processeur pour qu'il serve d'hyperviseur à l'aide du « HAL » (Hardware Abstraction Layer). Les systèmes d'exploitation invités sont au même niveau que ceux hôtes.

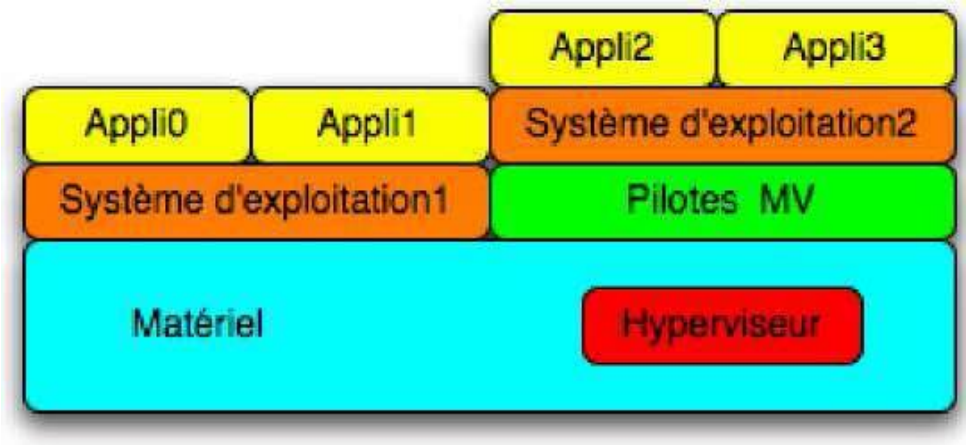


Figure 8: la virtualisation matériel.

- ✓ **Avantages :** certains processeurs permettent un accès direct à la mémoire des invités. Les performances sont optimales. Les processeurs ne sont pas émulés et les systemes d'exploitation inchangés.
- ✓ **Inconvénient :** il faut un processeur spécifique qui supporte les nouvelles instructions (HAL). Ainsi, si une machine ne comporte pas ce type de processeur, alors il est nécessaire de s'équiper d'une machine récente qui comportera un processeur compatible.

III. Les domaines de la virtualisation :

1. La virtualisation d'applications

a. Principe :

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 le quel elles sont exécutées. Elle consiste à encapsuler l'application et son contexte d'exécution système dans un environnement cloisonné.

La virtualisation d'application va nécessiter l'ajout d'une couche logicielle supplémentaire entre un programme donné et le système d'exploitation ; son 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.

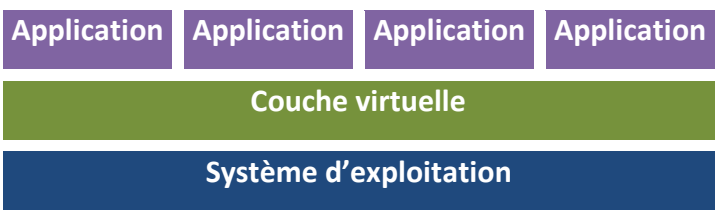


Figure 8 : Virtualisation d'applications

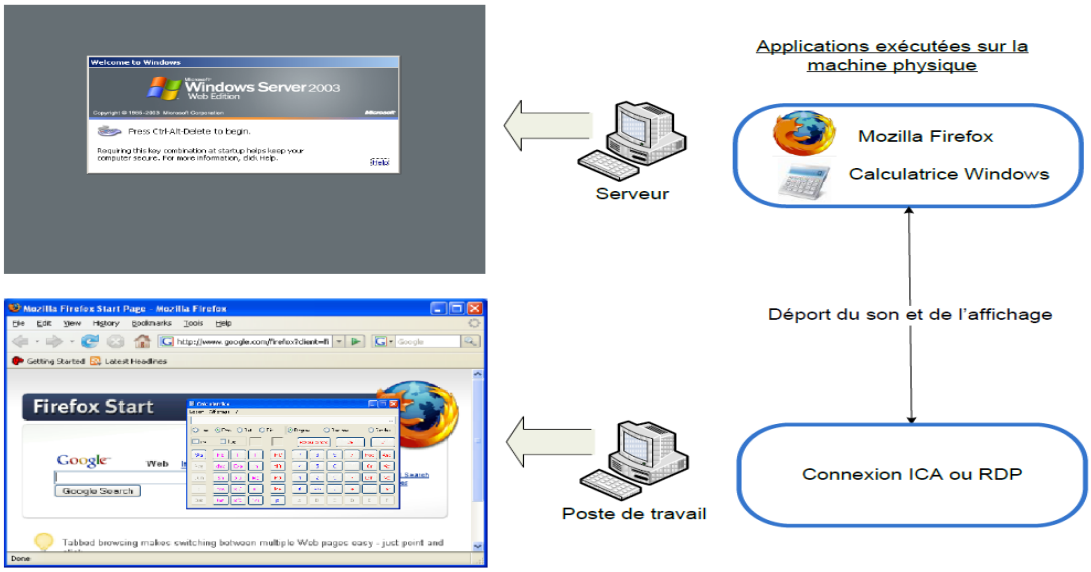
En analysant la figure ci-avant, on peut dire que la couche virtuelle va ajouter des avantages au système virtuel en permettant d'exécuter des applications conçues pour d'autres systèmes.

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 virtuelle ne viendra pas interagir avec les fichiers de configuration du système.

b. Technologies relevant de la virtualisation d'applications :

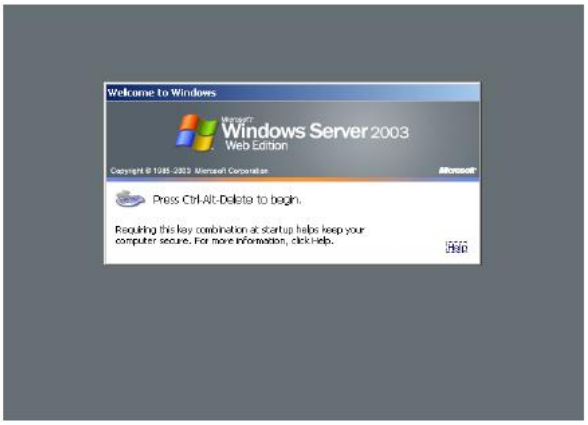
- ✓ **L'exécution de l'application à distance :** Le moyen le plus simple de permettre l'utilisation d'une application sans l'installer est de l'exécuter sur un serveur et d'envoyer l'image et le son que l'application génère sur le poste de travail.

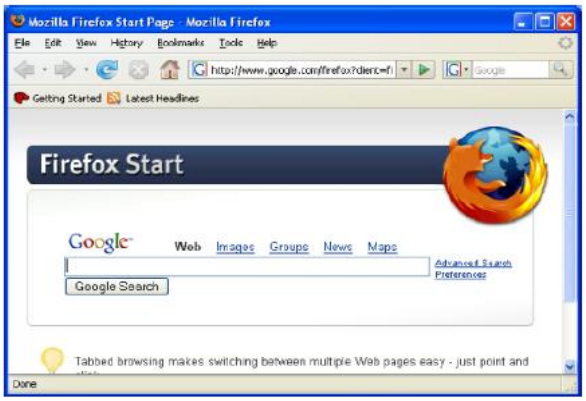


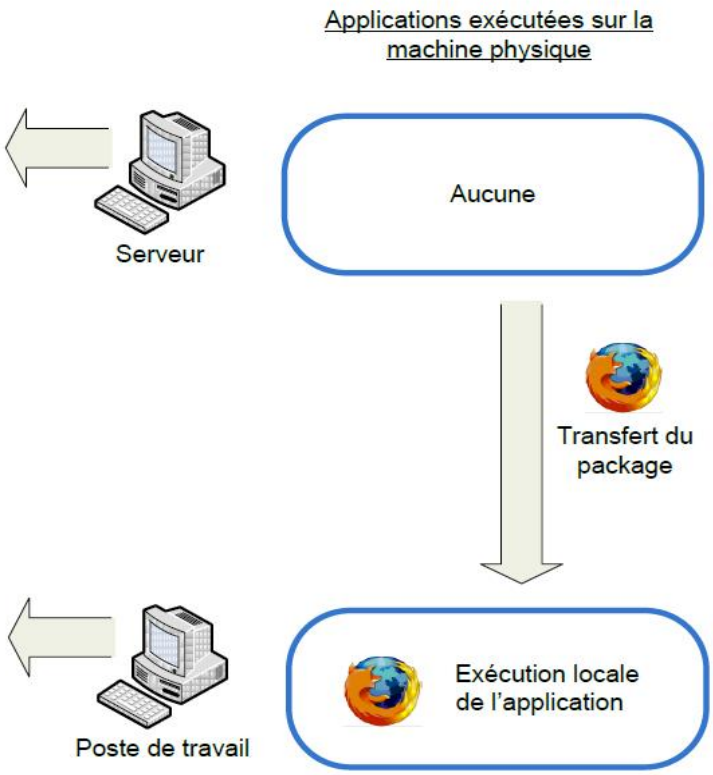
Ceci permet de fournir des applications aux utilisateurs des postes de travail sans avoir à les installer sur les postes. Il faut en revanche les installer sur le serveur, et cela pose parfois problème : certaines applications ne sont pas faites pour fonctionner dans un système d'exploitation pour serveur.

D'autre part, la charge engendrée par l'exécution des applications sur le serveur peut devenir problématique. Enfin, certaines applications ne peuvent pas être exécutées plusieurs fois simultanément. Il est donc impossible dans ce cas de servir plusieurs utilisateurs en même temps.

- ✓ **Le streaming d'application** : Pour parer à ces problèmes, une autre méthode de virtualisation d'application a été développée : le streaming, aussi appelé « installation à la demande ». Dans ce mode, lorsque qu'un utilisateur tente de lancer une application, le serveur envoie au poste de travail tous les fichiers dont l'application a besoin pour s'exécuter, et l'application est exécutée par le poste de travail, avec ses propres ressources. Cela suppose donc que le serveur dispose d'un package contenant tous les fichiers dont a besoin l'application, et qu'il l'envoie au client







Le problème de cette solution est qu'il faut créer ces fameux packages. La création des packages est basées sur le principe de surveiller l'installation de l'application et regrouper dans le package tous les fichiers ajoutés et toutes les modifications faites au registre.

Cette installation surveillée doit être effectuée sur un ordinateur « propre », autrement dit sur lequel n'est installé que le système d'exploitation (et éventuellement les mises à jour de ce système d'exploitation).

En effet, lors de son installation, une application vérifie si certains des fichiers qu'elle doit installer sont déjà présents sur le système, et le cas échéant, ne les ajoute pas. L'outil de surveillance de l'installation ne les remarque donc pas, et le package ne peut pas être exécuté sur un ordinateur ne disposant pas de ces fichiers.

Pour les mêmes raisons, il est déconseillé de packager une application sur un système d'exploitation différent de celui avec lequel elle va être utilisée.

2. La virtualisation de réseaux

De manière générale, 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. 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.

On distingue plusieurs types de réseaux virtuels :

- **Les réseaux virtuels de niveau 1, appelés réseaux virtuels par port (port-based VLAN**): ils définissent un réseau virtuel en fonction des ports de raccordement sur le commutateur (switch). Ainsi, 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.
- **Les réseaux virtuels de niveau 2, appelés réseaux virtuels par adresse MAC (MAC address-based VLAN) :** ils 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.
- **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.

Les avantages qu'offrent les réseaux virtuels sont les suivants :

- Une réduction du traffic de diffusion, puisque celui-ci est à présent contenu au sein de chaque réseau virtuel ;
- Une sécurité accrue puisque l'information est encapsulée dans une couche supplémentaire ;
- Une meilleure flexibilité puisqu'une modification de la structure des réseaux peut être réalisée en modifiant la configuration du commutateur.

3. La virtualisation de stockage

Dans une machine virtuelle, les données sont stockées sur un disque dur virtuel. Ce disque dur se présente sous forme de fichier dans le système de fichiers de l'hôte :

- VHD chez Microsoft
- VDI chez Oracle
- VMDK chez VMWare
- OVF pour le format ouvert

Tous les formats de disques durs virtuels (VDI, VHD, VMDK, OVF) sont transformables dans d'autres sans difficulté particulière.

Figure 2 : Fenêtre de choix de type de disque virtuel lors de la création d'une nouvelle machine virtuelle

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.

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.

4. La virtualisation de serveurs

D'une manière générale, 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 de serveur permet de :

- Regrouper plusieurs serveurs physiques sous-employés sur un seul hôte qui exécute des systèmes virtuels ;
- Réduire la surface au sol, la consommation électrique, le besoin de climatisation et le nombre d'administrateurs ;
- Réaliser des économies (locaux, consommation électrique, personnel).

Figure 3 : Virtualisation des serveurs

IV. Avantages & 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 mêmes des risques sont soulevés suite à l'utilisation de cette technologie.

Quels sont les intérêts de la virtualisation ?

1. Optimisation des ressources (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives) ;
2. Installation, sauvegarde, déploiement et migration faciles des machines virtuelles ;
3. Economie sur le matériel par mutualisation (consommation électrique, entretien physique, etc.) ;
4. Sécurisation et/ou isolation d'un réseau ;
5. Diminution des risques liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de ressources étant alors transparent ;
6. Une reprise automatique lors des incidents. La virtualisation permet d'améliorer la prévention et la gestion des pannes ainsi que le plan de reprise de l'activité du système. En effet, les équipements virtuels étant constitués d'un ensemble de fichiers, il est très simple de les sauvegarder.

Quels sont les inconvénients de la virtualisation ?

1. 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.
2. 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. 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.
3. 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.

V. Outils de virtualisation :

Le marché de virtualisation est très riche, dans cette section en s'intéresse aux produit les plus connus.

1. Xen :

Xen est une solution de virtualisation open source, plus précisément un hyperviseur de machine virtuelle. Son développement a débuté sous la forme d'un projet de recherche de

l'université de Cambridge au Royaume-Uni. La société XenSource a par la suite été créée et en a poursuivi le développement. Xen est en partie intégré à la partie principale du noyau linux depuis la version 3.0.

Xen permet d'exécuter plusieurs systèmes d'exploitation (et leurs applications) de manière isolée sur une même machine physique sur plate-forme x86, x86-64, IA-64 et PowerPC, ARM Cortex-A7 et Cortex-A15 (bientôt sur SPARC). Les systèmes d'exploitation invités partagent ainsi les ressources de la machine hôte.

Xen est un « paravirtualiseur » ou un « hyperviseur » de machines virtuelles. Les systèmes d'exploitation invités ont « conscience » du Xen sous-jacent, ils ont besoin d'être « portés » (adaptés) pour fonctionner sur Xen. Linux, NetBSD, FreeBSD, Plan 9 et GNU Hurd peuvent d'ores et déjà fonctionner sur Xen.

Xen 3 peut également exécuter des systèmes non modifiés comme Windows sur des processeurs supportant les technologies VT d'Intel ou AMD-V.

Les architectures x86, x64, IA-64, PowerPC et ARM et SPARC sont supportées. Le multiprocesseur (SMP) et partiellement l'*Hyper-Threading* sont supportés.

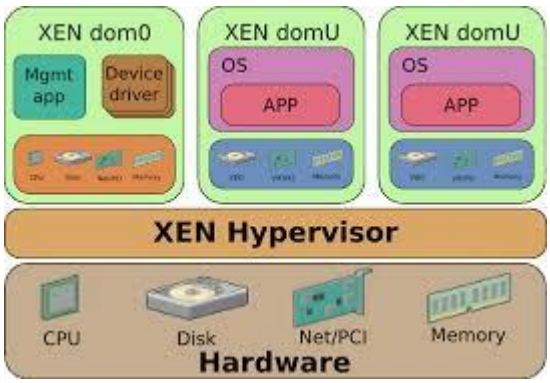


Figure 8 : architecture de Xen

2. KVM :

KVM (**Kernel-based Virtual Machine**) est un hyperviseur libre de type I pour Linux. KVM est intégré dans le noyau Linux depuis la version 2.6.20.

Il fonctionne originellement sur les processeurs à architectures x86 disposants des instructions de Virtualisation Intel VT ou AMD-V. Depuis, KVM a été porté pour les architectures Power PC, IA-64 ainsi que ARM depuis le noyau Linux 3.9. KVM donc permet une accélération

de virtualisation de système d'exploitation. C'est est un système optimisé pour la virtualisation de serveur. KVM semble plus performent en consommation de processeur mais plus lent pour l'émulation du périphériques graphiques.

KVM fourni une meilleur compatibilité avec les systèmes d'exploitation anciennes ou peu populaires. KVM est complètement libre, performant et très facile à installer et à utiliser. L'interface graphique virt-manager pourra aider à paramétrer KVM et pourra rendre la vie plus simple pour les administrateurs réseaux. Mais vous ne pouvez pas utiliser KVM en même temps avec Virtuel Box. En faudra en effet fermer KVM pour utiliser Virtuel Box et vice versa. Ou désactiver le support de virtualisation Processeur dans VirtuelBox.

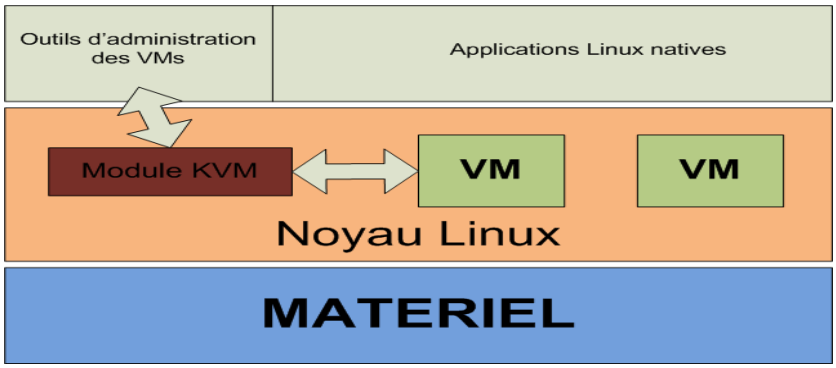


Figure 9 : architecture de KVM

3. VMware ESX

Ce produit s'installe sur la couche matérielle (on parle d'hyperviseur de type 1), et non sur un système d'exploitation « hôte ». Le logiciel de virtualisation de type VMware ESX permet des machines virtuelles complètes pour les systèmes d'exploitation invités, incluant même un BIOS C'est une architecture similaire à Xen (pas de système hôte visible), en revanche les systèmes invités n'ont pas à être modifiés, et n'ont pas accès directement au matériel de la machine.

VMware ESX permet une gestion plus précise des ressources de chaque machine virtuelle et de meilleures performances. La solution VMware ESX est la solution la plus industrielle de la gamme. VMware ESX est basé sur une distribution RHEL5 (Red Hat Enterprise Linux 5) modifiée, et comprend deux modules :

- **VMKERNEL** : Ce module « noyau » gère et hiérarchise l'ensemble des ressources matérielles (mémoire, processeur, disques, réseaux) en fonction de chaque serveur, et gère les ressources physiques pour ESX.
- **SERVICE CONSOLE** : permet la gestion de l'hyperviseur en mode commande. Accessible depuis le port 22 (SSH), cette console sert à lancer certaines commandes inaccessibles depuis

l'interface graphique ou encore de parcourir les dossiers dans lesquels sont stockés les machines virtuelles. Enfin elle peut permettre de collecter des informations de débogage sur les machines virtuelles ou sur le serveur ESX.

La gestion des serveurs se fait à l'aide d'un navigateur via une interface web, à l'aide d'une console cliente (Virtual Infrastructure Client) ou d'un outil de gestion centralisé VMware nommé Virtual Center. La Service Console est devenue une machine virtuelle à part entière dans vSphere(logiciel d'infrastructure Cloud de l'editeur VMware), et la Service Console est absente de la version ESXi du produit.

4. **Hyper-V** :

Hyper-V également connu sous le nom de Windows Server Virtualisation, est un système de virtualisation basé sur un hyperviseur 64 bits de la version de Windows Server 2008. Il permet à un serveur physique de devenir Hyperviseur et ainsi gérer et héberger des machines virtuelles communément appelées VM (*virtual machines*).

Grâce à cette technologie il est possible d'exécuter virtuellement plusieurs systèmes d'exploitation sur une même machine physique et ainsi d'isoler ces systèmes d'exploitation les uns des autres.

Les ressources de l'hyperviseur sont alors mutualisées pour différentes VM, ce qui présente un intérêt économique car auparavant il fallait envisager une machine physique par serveur.

Il est possible d'utiliser la console Hyper-V sur Windows 7. Dans le sens inverse, de nombreux systèmes d'exploitation peuvent tourner à l'intérieur de Hyper-V :

- ✓ pour les systèmes d'exploitation Microsoft : Windows 10 (sauf Home Edition), Windows 8.1, Windows 8, Windows 7 (sauf édition familiale), Windows Vista SP1/SP2 (sauf édition familiale), Windows Server 2012, Windows Server 2008 x64 SP1/SP2 & R2, Windows Server 2003 x64 SP2 & R2 SP2, Windows 2000 SP4, Windows XP Professionnel SP2/SP3 & x64 SP2
- ✓ Pour les systèmes d'exploitation Linux:
  - SUSE Linux Enterprise Server 10 SP1/SP2 & 11,
  - Red Hat Enterprise Linux 5.2 x64 et versions ultérieures ;
  - Ubuntu 12.04 LTS et versions ultérieures.

VI. Centres de données et la virtualisation :

Un centre de traitement de données (Data Centre en anglais) est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'informatique d'une ou plusieurs entreprise(s).Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires.

Un Datacenter est une infrastructure immobilière et technique destinée à l'hébergement d'une concentration importante des équipements informatiques. Il est composé :

• De salles sécurisées pour accueillir les équipements informatiques :
  - ✓ les baies, armoires de raccordement pour les serveurs, aux dimensions standardisées ;
  - ✓ les serveurs applicatifs, sur lesquels sont exécutés les logiciels ;
  - ✓ les serveurs de données, qui assurent le stockage des données ;
  - ✓ d'équipements réseau interconnectant les serveurs. Il s'agit notamment des routeurs, parefeu, répartiteurs et commutateurs ;

• d'infrastructures techniques assurant la continuité de l'alimentation électrique, du refroidissement des serveurs et de l'accès au réseau à Très Haut Débit pour l'ensemble de ces ressources ;

• de points d'accès aux réseaux électriques à haute tension et aux réseaux de télécommunication Très Haut Débit,

• d'un bâtiment spécialisé et sécurisé intégrant l'ensemble de ces composants.

Un Datacenter constitue ainsi un site sécurisé pouvant héberger des services numériques nécessitant une haute disponibilité

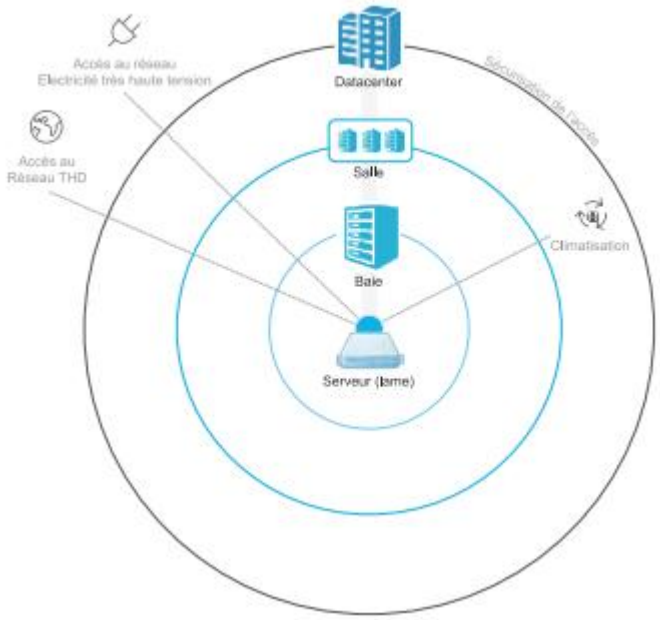


Figure : éléments constrictif d'un Datacenter

Les enjeux du Datacenter : dans cette section nous avons citez les principales enjeux pour les datacenters

- ✓ **La Haute disponibilité :** Pour assurer une « Haute disponibilité », il est important que les ressources nécessaires à la mise à disposition d'un service puissent pallier toute défaillance. les *Datacenters* dupliquent donc les infrastructures et incluent des mécanismes de redondance permettant de basculer automatiquement les données et applications sur un site de repli en cas de défaillance du site principal.
- ✓ **Efficacité énergétique d'un Datacenter :** les constructeurs sont engagés depuis 10 ans dans une course à la réduction des PUE('indice d'efficacité énergétique) pour améliorer l'image écoresponsable de leurs équipements, mais surtout pour améliorer la rentabilité des sites et proposer des tarifs plus compétitifs
- ✓ **La continuité de l'alimentation électrique :** la concentration d'équipements informatiques fait d'un *Datacenter* un gros consommateur d'électricité. Pour alimenter les serveurs hébergés sans les détériorer, la continuité et la stabilité du courant sont des facteurs critiques. le *Datacenter* doit disposer de générateur de secours en capacité de produire sa propre énergie localement sur une durée minimale supérieure à la garantie de temps de rétablissement du fournisseur d'électricité.
- ✓ **La maitrise des systèmes de refroidissement :** la distribution et la consommation d'énergie électrique par les équipements informatiques dé-gagent beaucoup de chaleur. Dans un *Datacenter*, où la densité des équipements est importante, la température dépasse rapidement les seuils recommandés pour le bon fonctionnement des équipements. un dispositif de refroidissement est donc nécessaire.
- ✓ **La maîtrise des accès aux réseaux :** Pour offrir une accessibilité optimale à ses clients, un *Datacenter* doit disposer d'une bande passante importante sur les réseaux des opérateurs. on privilégiera la proximité d'un point d'échange internet pour implanter un *Datacenter* et bénéfcier ainsi de l'interconnexion avec un maximum d'opérateurs sur un réseau très Haut Débit.
- ✓ **La sécurisation du site :** pour la sécurisation du site le *Datacenter* doit répondre à différentes exigences de sécurité : la sécurité d'accès, qui comprend les sas d'accès et les technologies d'authentifcation des personnes (lecteur de badge, digicode, lecteur d'empreintes digitales, etc.) et la surveillance continue et les systèmes d'alerte en cas d'incident (arrêt du refroidissement,fuite du refroidissement à eau …).

La virtualisation donne de plus pour les centres de données :

Pour les grandes entreprises, la virtualisation est la manière la plus efficace de réduire les dépenses informatiques tout en stimulant l'efficacité et la flexibilité.

VMware® vSphere with Operations Management™, la plate-forme de virtualisation et de gestion du Cloud la plus performante du marché permet de simplifier l'infrastructure informatique. La virtualisation avec VMware permet aux entreprises :

- Réduisez les coûts d'investissement et d'exploitation en augmentant l'efficacité énergétique, tout en limitant le besoin en matériel grâce à la consolidation de serveurs, diminuer les coûts d'exploitation grâce à l'automatisation, et de, tout en limitant la perte de revenus en réduisant les interruptions de service planifiées
- Optimisez les fonctions de continuité et de reprise d'activité pour votre infrastructure virtualisée à l'aide des solutions de reprise d'activité améliorées et simplifiées de VMware® vCenter Site Recovery Manager™
- Virtualisez les applications stratégiques de l'entreprise, notamment les bases de données Oracle Database, Microsoft SQL Server, SAP HANA, SAP Sybase), les applications commerciales (SAP Business Suite, Microsoft Exchange, SQL Server, SharePoint, SAP), et garantissez les meilleurs niveaux de SLA et de performances
- Bénéficiez de l'automatisation basée sur des règles, et garantissez les performances et la conformité avec une infrastructure rationalisée en utilisant VMware vCenter Operations Management Suite pour la gestion de la virtualisation.

VII. Sécurité et virtualisation :

1) **La virtualisation pour la sécurité :** dans cette section nous avons cité quelques avantages en sécurité fourni par la virtualisation
    1. **Isolation :** Chaque machine virtuelle est isolée des autres y compris du système hôte... elle possède ses propres paquetages et services, ses propres utilisateurs, ses propres processus, sa propre adresse IP et son propre « file system ». et les seuls échanges entre machines virtuelles se font via l'interface réseau. Et par conséquent, si une machine virtuelle se plante, les autres n'en sont pas affectées (sauf si dépendances).
    2. On peut rendre la machine physique invisible du réseau et ne lancer que des machines virtuelles ce qui permet de sécuriser et/ou isoler un réseau (cassage des OS virtuels, mais pas des OS hôtes qui sont invisibles pour l'attaquant) en plus la machine hôte invisible peut faire tourner des IDS, des tripwire …

3. **Honeypots :** machine pot de miel destinées à être livré en pâture aux pirates, et recueillir des informations en provenance de pirates informatiques... permet de ne pas risquer de compromettre une machine physique.

2) Les risques les plus courants de la virtualisation :

1. Risques liés à un mauvais usage des consoles d'administration : Les impacts d'une mauvaise configuration sont immédiats qui peut engendre un

    a. Arrêt multiple d'instances
    b. Activation de fonctions de décloisonnement
    c. Activation de fonctions de mobilité VM
    d. …..

2. Risques de rebond entre systèmes invités via un décloisonnement réseau
    a. Visibilité inter-instances
    b. Problématiques de routage…
3. Risques liés au stockage : **La criticité du stockage augmente toujours**
    a. Concentration des données (SPOF)
    b. Destruction des données OS
    c. Atteinte à la confidentialité de multiples VMs (OS et des données)
    d. …
4. Risques liés à de mauvaises pratiques de gestion de la plateforme de virtualisation
    a. Prolifération des VM / gestion des inventaires
    b. Problèmes de performances / Capacity Planning
    c. Maintien en condition opérationnelle de la plateforme de virtualisation
    d. …

En plus de ces risques les plus courants en trouve d'autre risques comme :

1. **Le Décloisonnement :** Décloisonnement via des failles sur l'hyperviseur
2. **Le Déni de service :** Impact d'une instance sur l'autre en terme de performance/disponibilité

Se sont des risques réels, mais finalement **peu rencontrés.**

Tripwire est un logiciel de contrôle d'intégrité, permettant de s'assurer que les fichiers sensibles sur un ordinateur ne sont pas modifiés sans que cela ne déclenche une alerte

Sources :

Wikipedia. 2013. Hyperviseur. *Wikipedia.* [En ligne] 15 06 2013. http://fr.wikipedia.org/wiki/Hyperviseur.