

Support de cours	
Patrice BEDE	Virtualisation

Virtualisation

Principes de la Virtualisation

La virtualisation c'est quoi ?

En résumé c'est un ensemble de mécanismes permettant de faire fonctionner sur une seule machine physique un ou plusieurs autres systèmes d'exploitation comme des machines physiques distinctes.

Dans le monde informatique et réseaux de communication, cette définition pourrait s'appliquer à différentes techniques qui sont :

- **La Simulation**

Un simulateur de réseau est un logiciel qui prédit le comportement d'un réseau informatique. Les réseaux informatiques étant devenus trop complexes et le matériel utilisé complexe à mettre en œuvre, des simulateurs de réseau sont utilisés.

Dans les simulateurs, le réseau informatique est modélisé avec des périphériques, des liens, des applications, etc. et les performances du réseau sont signalées.

La configuration du réseau décrit le réseau (nœuds, routeurs, commutateurs, liens) et les événements (transmissions de données, erreur de paquet, etc.).

Les résultats de sortie enregistrent chaque paquet, chaque événement qui s'est produit dans la simulation et sont utilisés pour l'analyse.

Ce sont de **logiciels** qui se contentent de reproduire le comportement de matériel réels. Ils sont utilisés pour apprendre le fonctionnement des réseaux, à administrer un matériel physique ou, quelquefois, pour présenter des PoC (Proof of Concept) de validation.

Leurs principaux défauts sont que le matériel simulé est souvent bridé par rapport au matériel réel et qu'ils ne peuvent pas s'interfacer avec ces matériels réels.

Les plus connus sont **Packet-Tracer** de **Cisco** et **e-NSP** de **Huawei**.

- **L'Emulation**

Le concept de l'émulateur se rapproche assez de celui de la virtualisation puisqu'il permet de présenter au système d'exploitation émulé du matériel qui n'est pas présent physiquement sur la machine qui l'héberge, et ce y compris l'**unité centrale de calcul**, c'est-à-dire le **processeur** et la **mémoire système** (RAM).

Le système d'exploitation tourne dans un environnement qui représente son environnement naturel même si celui-ci est complètement différent de l'environnement réel.


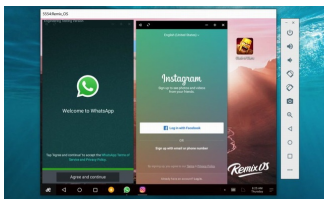
Mais ceci à un coût et les performances en sont considérablement réduites par rapport à la virtualisation.

Dans le domaine des jeux, nombreux sont les émulateurs de consoles qui permettent de continuer à jouer à de vieux jeux dont les consoles ne sont plus fabriquées.

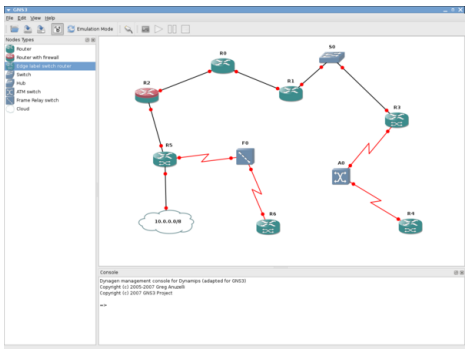
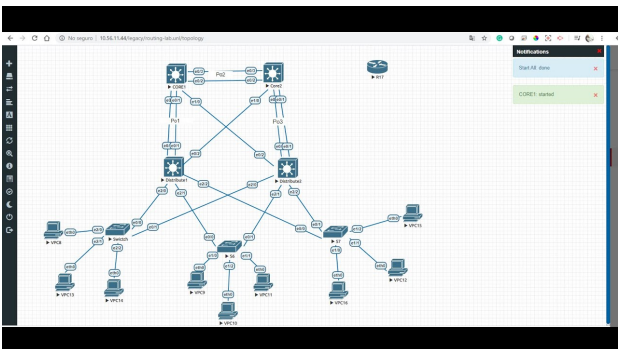
Dans le domaine informatique, la société Apple ayant utilisé très longtemps des processeurs PPC (PowerPC) au lieu de processeurs Intel/AMD, le seul moyen de faire tourner ces systèmes d'exploitation sur des PC standards était d'utiliser des logiciels d'émulation matériels.

Autre exemple, la bibliothèque de logiciels **Cygwin** permet d'émuler une ligne de commande Unix en environnement Windows.

Actuellement les développeurs d'applications pour smartphones utilisent également des émulateurs.

Emulateur de console	Emulateur Android
	

Dans le domaine du réseau l'émulateur **Dynamips** permet de faire tourner des routeurs et des switches **Cisco** en environnement virtuel. On le trouve notamment dans les logiciels **GNS3** et **EVE-NG**.

Emulateur Dynamips dans GNS3	Emulateur Dynamips dans EVE-NG
	

Le principal avantage d'un émulateur est que l'on est bien plus proche du matériel réel que dans le cas du simulateur et que ces matériels émulés peuvent s'interfacer avec des matériels réels.

Ils sont donc très souvent utilisés pour réaliser des **PoC (Proof of Concept)** de validation de solutions d'infrastructure.

• La Virtualisation

Ce concept est très proche de l'émulateur car la machine virtuelle ne voit pas non plus le matériel réel mais un matériel émulé par l'**hyperviseur** (carte réseau, disque dur ...) **à l'exception du processeur et de la Ram** (Unité Centrale) qui ne peut pas être caché à la machine virtuelle.

Bien sur tous les cœurs des processeurs ne sont pas affectés à la même machine virtuelle ce qui permet de répartir la charge de travail et d'adapter la puissance aux besoins.

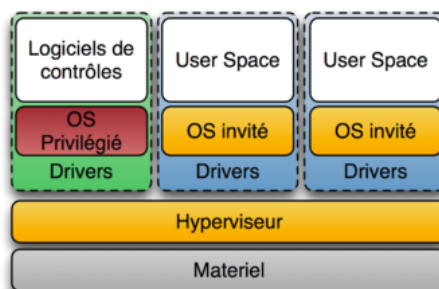
Le matériel virtuel (sauf le processeur) étant émulé, il est facile de copier une machine virtuelle d'un poste physique sur un autre même si leurs matériels physiques sont différents.

Dans la virtualisation on distingue 2 types de systèmes de virtualisation, appelés **Hyperviseurs**.

- Un **Hyperviseur de type 1** est un système d'exploitation très léger, optimisé pour gérer les accès des systèmes d'exploitation invités (les Machines Virtuelles) à l'architecture matérielle sous-jacente.

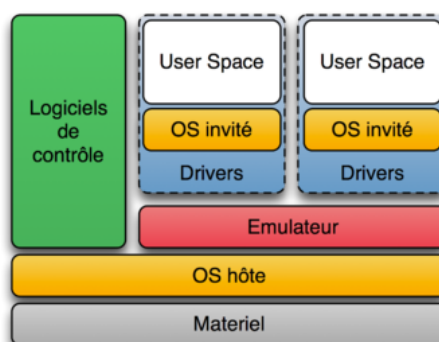
Actuellement c'est est la méthode de virtualisation d'infrastructure la plus performante mais elle a

pour inconvénient d'être contraignante et onéreuse, bien que permettant plus de flexibilité dans le cas de la gestion d'un datacenter.



Comme ils s'installent au niveau du matériel physique on les appelle aussi **Hyperviseurs Bare-Métal**.

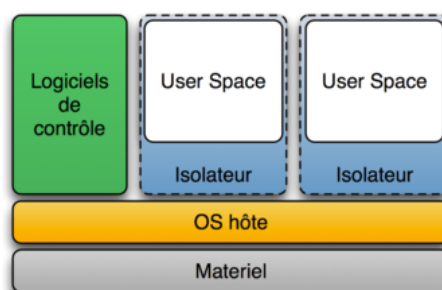
- Un **Hyperviseur de type 2** est un logiciel (généralement assez lourd) qui tourne en tant qu'application sur le système d'exploitation de la machine physique. Ce logiciel permet de lancer un ou plusieurs systèmes d'exploitation invités en virtualisant ou/et émulant le matériel pour ces systèmes d'exploitation invités, ces derniers croyant dialoguer directement avec ce matériel. Cette solution est très comparable à un émulateur, et parfois même confondue. Cependant le processeur et la Ram (l'unité centrale) sont directement accessibles aux machines virtuelles, alors que sur un émulateur l'unité centrale est simulée, Cette solution isole bien les OS invités, mais elle a un coût en performance



Il faut noter que la virtualisation ne touche pas exclusivement le système d'exploitation mais concerne aussi, maintenant, le stockage et même le réseau.

• L'Isolation

Une nouvelle technique offrant plus de souplesse et de réactivité est devenue majeure en informatique dans le monde des DevOps, il s'agit de l'isolation.




Cette technologie est ancienne, reposant sur le principe d'isolation d'une application au sein d'un système d'exploitation natif. Des outils dans le monde Unix comme **chroot** sous **Linux** ou les jails **sous BSD** existent depuis longtemps. Cette technologie a été améliorée par le principe des **containers** comme **LXC** ou encore **Docker**.

Le principe consiste à faire tourner une ou plusieurs applications au sein d'un container qui s'exécute lui-même dans un système d'exploitation natif qui partage ses ressources propres avec le container.

Techniques de Virtualisation

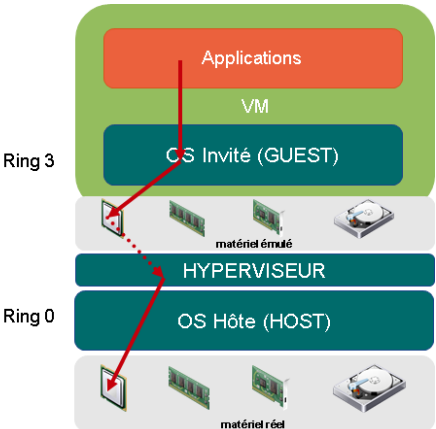
• Système d'exploitation installé nativement

Un système d'exploitation installé en natif (directement sur le matériel physique) est le seul à contrôler complètement ce matériel. Il utilise le niveau d'accès le plus important (appelé niveau Ring 0).

Principes	Technique
Applications en Espace Utilisateur (Ring 3)	Ring 3 Applications
Les Ring 1 et 2 sont réservés aux pilotes (drivers)	Ring 2 Peu Utilisé
Système d'exploitation en Espace Noyau	Ring 1 Peu Utilisé
Matériel Physique	Ring 0 Système d'exploitation
	

• La translation binaire

Le système d'exploitation Guest (la VM) ne peut pas contrôler le processeur. L'Hyperviseur le trompe en lui faisant croire qu'il est installé nativement, en interceptant ses appels systèmes et en les traduisant pour qu'ils puissent être exécutés par le système d'exploitation Host (installé en natif en Ring 0).

Avantages / Inconvénients	Technique
<p>Principal problème de la virtualisation : Le système d'exploitation de la VM se trouve en Espace Utilisateur</p> <p>Solution : L'Hyperviseur lui présente un matériel émulé (sauf le processeur) Les appels systèmes au processeur sont interceptés et traduits Première méthode de virtualisation Cette solution est relativement lente !</p>	

Mis en œuvre sans les **Hyperviseurs de type 2** comme **Vmware Workstation Pro** et **Oracle Virtualbox**

• La paravirtualisation

La **paravirtualisation** est une technique de virtualisation qui présente une interface logicielle similaire à du matériel réel à une VM mais optimisée pour ce type de fonctionnement, contrairement à l'émulation d'un périphérique matériel existant qui peut s'avérer lente et compliquée à implémenter. La couche de virtualisation s'exécute dans une partition parente qui dispose d'un accès direct aux périphériques matériels. La partition parente crée ensuite des partitions enfants dans lesquelles s'exécutent les systèmes d'exploitation Guest. Elle appelle pour cela l'interface de programmation **Hypercall**.

Avantages / Inconvénients	Technique
<p>Des Hypercall traversent le noyau de la VM jusqu'à l'Hyperviseur qui les traite.</p> <p>Le système d'exploitation de la VM doit donc être modifié pour les supporter</p> <p>Les performances atteintes sont proches du matériel natif</p> <p>Mais si le noyau est propriétaire (Microsoft) cette technique est limitée au propriétaire du noyau</p>	<p>Le diagramme illustre la paravirtualisation avec deux machines virtuelles (VM) : une VM Parent (Dom 0) et une VM Enfant (Dom U). Les applications sont exécutées dans le Ring 3. Le système d'exploitation (OS) de la VM Parent est un OS hôte virtualisé, tandis que celui de la VM Enfant est un OS invité modifié. Les deux VM sont connectées à un hyperviseur situé dans le Ring 0. Les appels hypercalls sont envoyés de la VM Enfant à l'hyperviseur via le Ring 1. Les périphériques matériels sont représentés dans le Ring 0.</p>

Mis en œuvre dans **Xen** et Microsoft **Hyper-V**.

• La virtualisation assistée par matériel

Une virtualisation complète est utilisée pour émuler un environnement matériel complet, ou une machine virtuelle, dans laquelle un système d'exploitation Guest non modifié s'exécute dans un isolement complet.

La virtualisation assistée par matériel a été ajoutée aux processeurs x86 (Intel VT-x ou AMD-V) en 2005 et 2006 (respectivement).

Avantages / Inconvénients	Technique
<p>Apparition d'un nouveau mode d'exécution appelé VMX</p> <p>L'Hyperviseur s'installe en Root Mode dans un nouveau Ring appelé Ring -1</p> <p>et est le seul à accéder au jeu complet d'instructions de virtualisation.</p> <p>La VM tourne dans un environnement isolé sans modifications.</p>	<p>Le diagramme illustre la virtualisation assistée par matériel. Une machine virtuelle (VM) est exécutée dans le Ring 3. Le système d'exploitation (OS) de la VM est un OS invité (GUEST) qui tourne dans le Ring 0. L'hyperviseur est installé en mode ROOT dans le Ring -1. Les périphériques matériels sont représentés dans le Ring 0. Les appels hypercalls sont envoyés de la VM à l'hyperviseur via le Ring 0.</p>

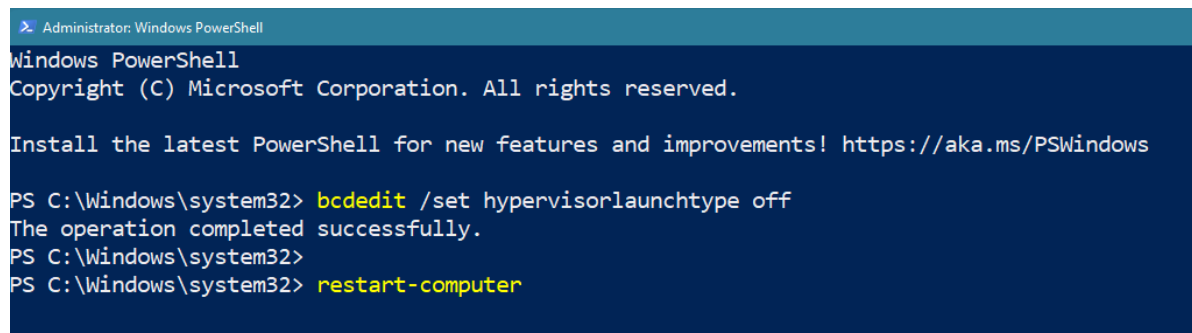
Mis en œuvre dans les Hyperviseurs de type 1 comme **Vmware Esxi**. Cette technique est aussi implémentée sur l'Hyperviseur Microsoft **Hyper-V** ainsi que dans d'autres hyperviseurs (KVM ...).

La virtualisation assistée par matériel est également appelée virtualisation accélérée, machine virtuelle matérielle (HVM) et virtualisation native.

ATTENTION : Sur Windows 10/11 l'installation de VMware Workstation alors que des composants Hyper-V sont installés par défaut peut conduire à des problèmes de virtualisation. Pour éviter cela il faut ouvrir une invite de commandes PowerShell en mode administrateur et taper la commande suivante :

bcdedit /set hypervisorlaunchtype off

puis redémarrer l'ordinateur !



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> bcdedit /set hypervisorlaunchtype off
The operation completed successfully.
PS C:\Windows\system32>
PS C:\Windows\system32> restart-computer
  
```

Techniques associés à la virtualisation

Les techniques explicitées ci-dessous sont basées sur l'Hyperviseur de type 2 "Vmware Workstation Pro".

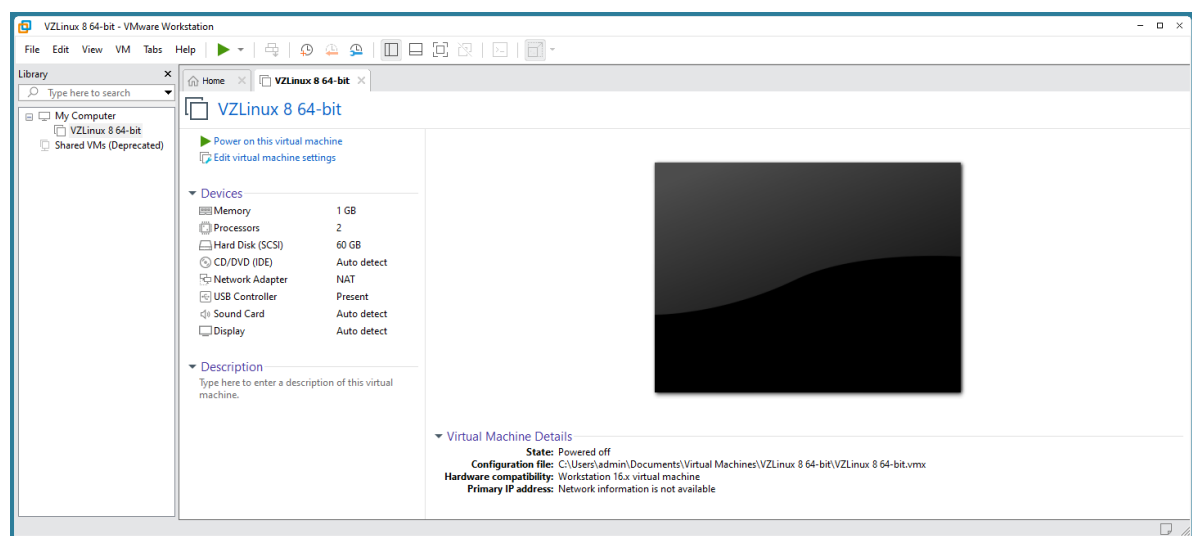
Elles se retrouvent quasiment identiques dans l'Hyperviseur de type 1 "Vmware Esxi" et elles peuvent être facilement transposées dans des Hyperviseurs de marque différente (comme VirtualBox).

- **La Machine Virtuelle (VM- Guest) vue par le système d'exploitation natif (Host)**

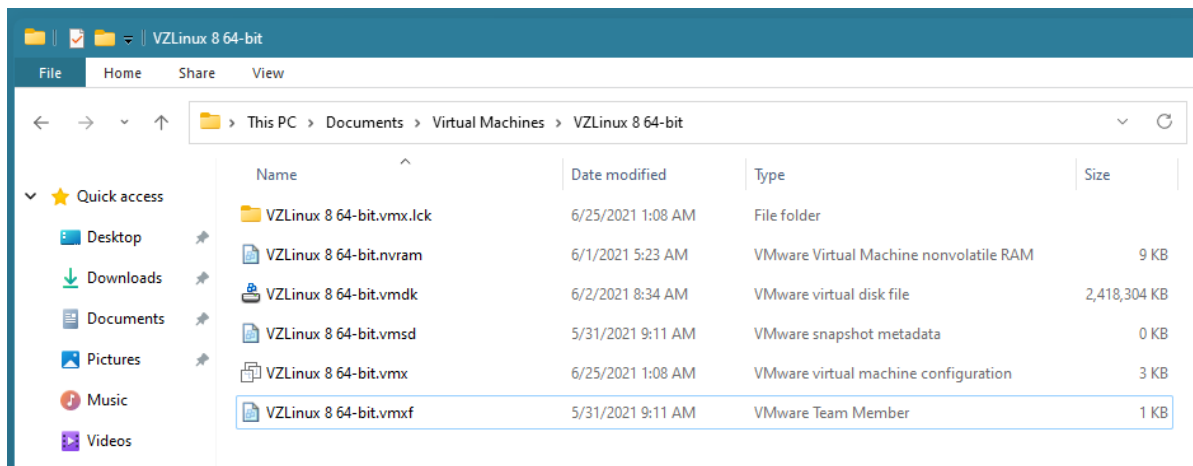
Pour le système d'exploitation installé en natif sur votre poste de travail (Windows 10/11, MacOS ..), la machine virtuelle n'est qu'un ensemble de fichiers stockés dans un répertoire.

C'est l'hyperviseur installé sur ce système d'exploitation (ici VMware Workstation) qui va animer ces fichiers au lancement de la machine virtuelle.

Voici la machine virtuelle vue par VMware Workstation (le système exploitation est un Linux).



Et la voici vue par le système d'exploitation de la machine réelle (Host).



Le fichier "VZLinux 8 64-bit.vmx" décrit la machine virtuelle, le fichier "VZLinux 8 64-bit.vmdk" est le disque dur et le fichier "VZLinux 8 64-bit.nvram" représente la mémoire de cette machine virtuelle.

Le fichier avec extension "VZLinux 8 64-bit.vmx" est le seul fichier éditable.

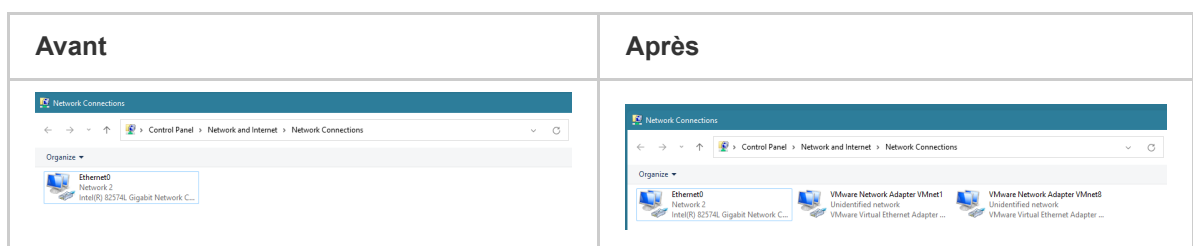
Il peut être modifié avec le bloc-notes (si vous savez ce que vous faites!).

• Le réseau des VM - Le Virtual Network Editor

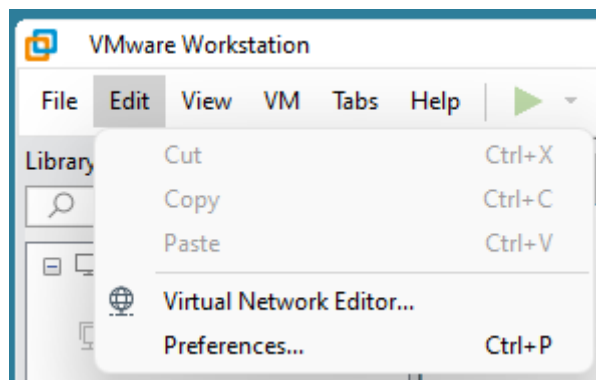
Une machine virtuelle est rarement installée sans disposer d'un accès réseau. Cet accès réseau va lui permettre de communiquer avec d'autres machines virtuelles installées sur le même Host et (éventuellement) d'accéder au réseau physique extérieur (voir à Internet).

Cet accès extérieur passe obligatoirement par une carte réseau physique (filaire ou wifi) installée sur le Host.

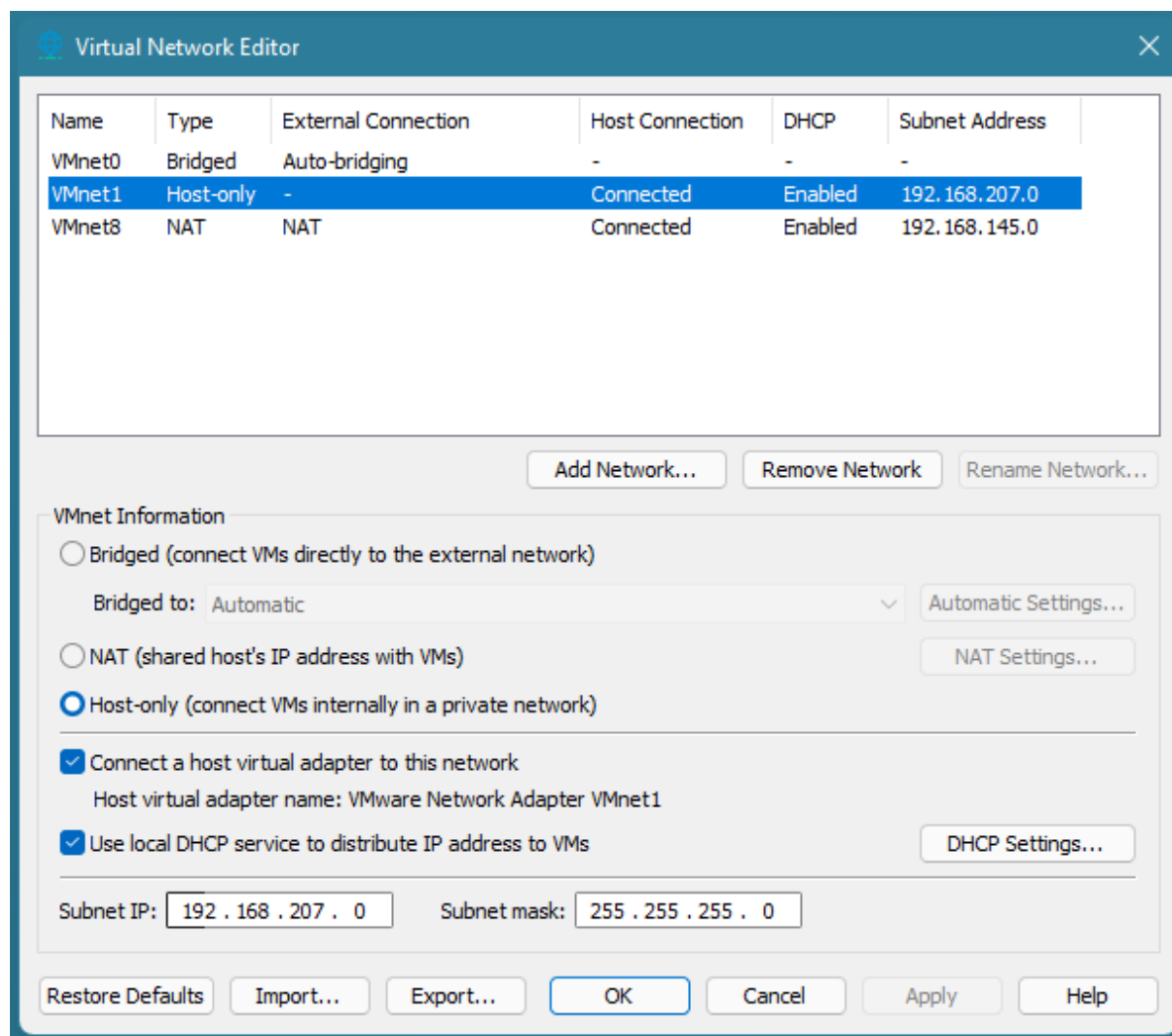
L'installation de VMware Workstation provoque l'apparition de nouvelles cartes réseau (virtuelles) dans votre ordinateur réel (Host).



Ces cartes réseaux servent à faire le lien entre votre ordinateur réel et des réseaux pour machines virtuelles pré-installés avec l'installation de VMware Workstation.



Le menu **"Edit > Virtual Network Editor"** de VMware Workstation vous permet de gérer ces réseaux et, éventuellement, d'en créer d'autres.



1. Le réseau **VMnet0** constitue un **bridge** (un pont) avec la carte réseau réelle (Ethernet ou WiFi) de votre ordinateur réel.
Toutes les machines virtuelles connectées à ce type de réseau apparaîtront depuis le réseau réel comme des ordinateurs supplémentaires disponibles.
2. Le réseau **VMnet1** constitue un réseau dit **Host-Only**.
Toutes les machines virtuelles connectées à ce réseau pourront travailler ensemble **mais** ne pourront **pas accéder** au réseau réel.

VMware tire au sort un numéro IP pour distribuer des adresses réseaux (ici c'est le 192.168.207.0/24). Ce réseau dispose d'un serveur DHCP intégré d'adresse 192.168.207.254 et l'adresse 192.168.207.1 ne doit pas être utilisée car réservée à la carte "VMware Network Adapter VMnet1" créée dans votre ordinateur réel.

Vous pouvez créer d'autres réseaux de ce type jusqu'au numéro VMnet19. Tous ces réseaux ne communiquent pas ensembles.

3. Le réseau **VMnet8** constitue un réseau dit **NAT**.

Toutes les machines virtuelles connectées à ce réseau pourront travailler ensembles et pourront **accéder** au réseau réel comme si elles étaient derrière une Box Internet.

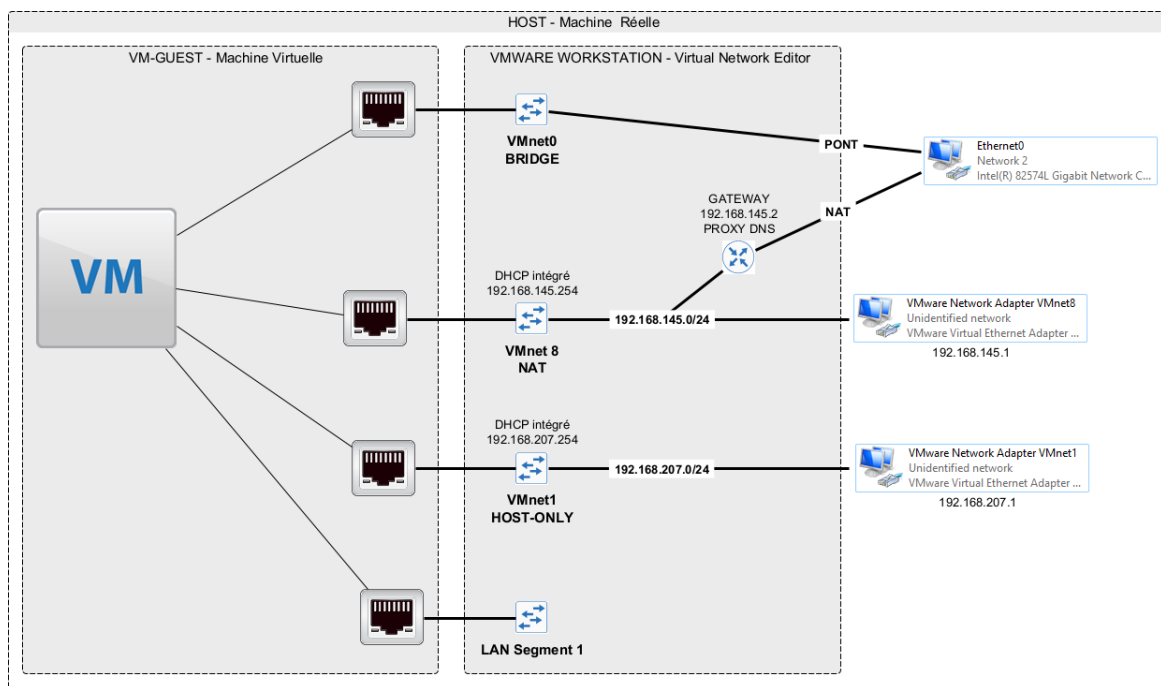
La translation d'adresse NAT fera que les machines virtuelles auront la même adresse que la carte réseau réelle vu du réseau réel (elles sont donc invisibles).

VMware tire au sort un numéro IP pour distribuer des adresses réseaux (ici c'est le 192.168.145.0/24). Ce réseau dispose d'un serveur DHCP intégré d'adresse 192.168.145.254 et l'adresse 192.168.145.1 ne doit pas être utilisée car réservée à la carte "VMware Network Adapter VMnet1" créée dans votre ordinateur réel.

Une autre adresse ne doit jamais être utilisée, l'adresse 192.168.145.2 car réservée à l'adresse de la pseudo Box Internet qui permet l'accès au réseau réel.

4. Il est possible également de constituer autant de réseaux virtuels appelés des "**LAN Segment**" que vous souhaitez. Ces réseaux agissent comme des réseaux de type Host-Only **mais** sans avoir de DHCP intégré et sans créer de carte réseau virtuelle dans l'ordinateur réel.

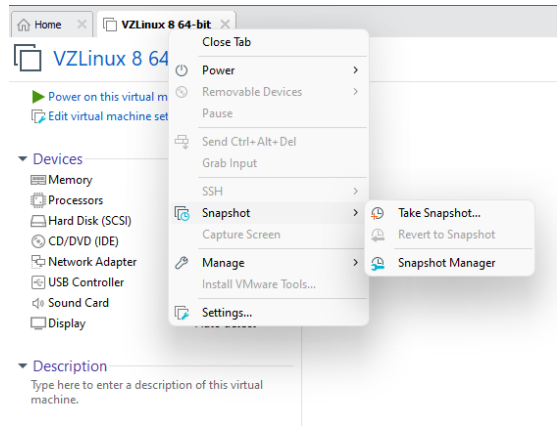
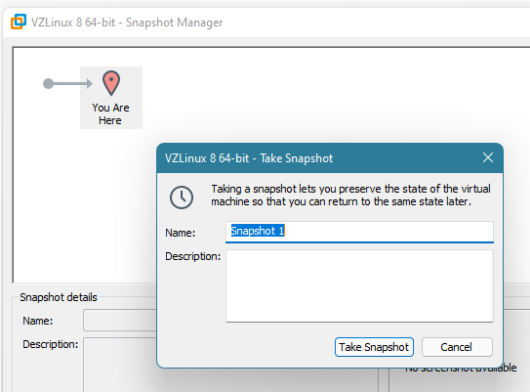
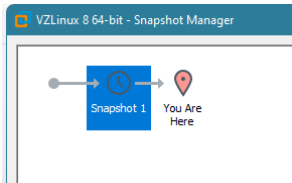
Le schéma ci-dessous essaye de synthétiser les différents types de réseau :



• Les snapshots

L'un des points forts des hyperviseurs est de permettre de figer l'état de la machine virtuelle à un moment donné sous la forme d'un snapshot (ou cliché instantané). Cette machine peut continuer à évoluer ensuite avec la possibilité de revenir à cet état antérieur à tout moment (pratique lorsque l'on teste une nouvelle application...).

Il est même possible de programmer la création de snapshots à intervalles réguliers.

Comment réaliser un snapshot	
<p>Cliquer droit sur l'onglet de la machine virtuelle</p>	
	<p>Choisir "Take Snapshot"</p> <p>Vous pouvez personnaliser les informations</p>
<p>Le snapshot est créé et apparait dans le Snapshot Manager</p>	

Un snapshot peut être réalisé machine virtuelle allumée ou éteinte.

• Le clonage

Le clonage permet de copier rapidement une machine virtuelle sans avoir à réinstaller le système d'exploitation.

ATTENTION : Le **clonage** ne peut se faire qu'à partir d'un **snapshot** réalisé **machine virtuelle éteinte**.

• **Linked Clone** - Clone lié :

Ce clone n'est pas une copie complète de la machine virtuelle d'origine (ou machine virtuelle parente).

Il pourra évoluer indépendamment de celle-ci mais doit toujours être capable de la joindre.

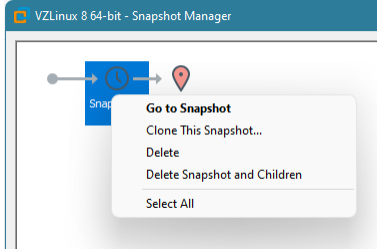

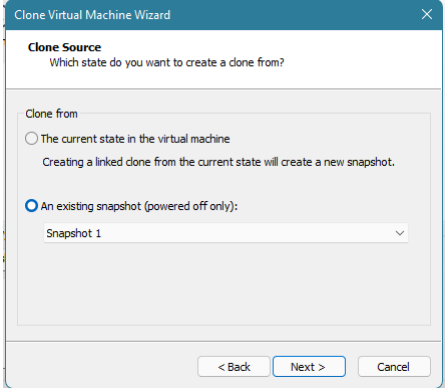
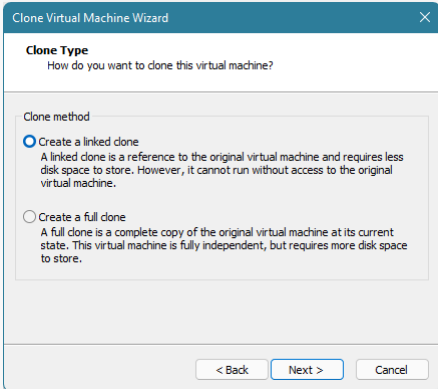
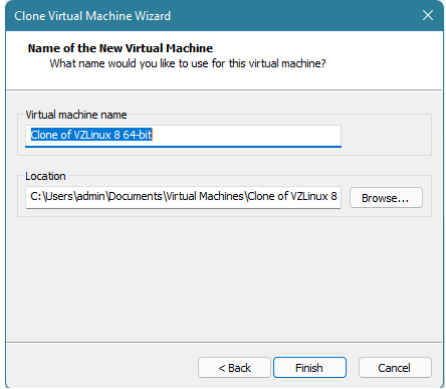
On ne peut donc pas l'exporter sur un autre disque dur sans copier également la machine virtuelle parente.

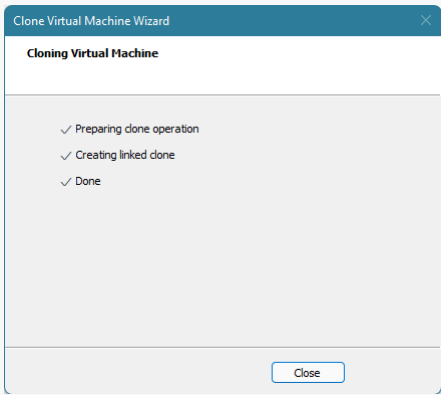
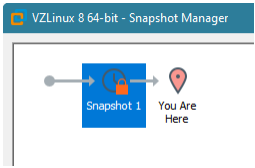
Son principal avantage est qu'il prend moins de place qu'une copie complète puisqu'il n'enregistrera que les différences avec la machine virtuelle parente (idéal sur un ordinateur portable ou la place disponible sur le disque dur est toujours limitée).

• **Full Clone** - Clone complet :

Ce clone constitue une copie complète de la machine virtuelle parente.

Il peut donc être exporté sur une autre unité disque mais il prend de base autant de place disque que celle-ci.

<h2>Réalisation d'un clone</h2> <p>Le clonage peut se faire à partir du gestionnaire de snapshots (Snapshot Manager) lié à la machine virtuelle.</p>	
	<p>Un assistant se lance</p>
<p>Il faut choisir un snapshot Choisir l'autre option revient à créer un nouveau snapshot</p>	
	<p>Choisir un clone lié ou complet en fonction de l'utilisation prévue</p>
<p>Donner un nom à la machine virtuelle clone et choisir son emplacement</p>	

Réalisation d'un clone	
	<p>Le clonage est terminé</p>
<p>Un cadenas apparaît sur le snapshot qui a servi de base au clonage pour indiquer que sa suppression entrainerait l'incapacité de fonctionner pour les clones liés à ce snapshot</p>	

Un clone lié indique toujours de quelle machine virtuelle parente il est issu.

Il ne doit **JAMAIS** perdre le lien avec la machine parente.

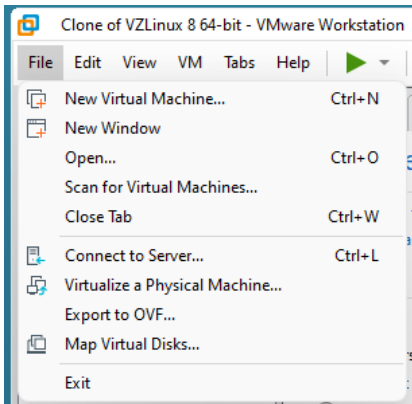
▼ Virtual Machine Details

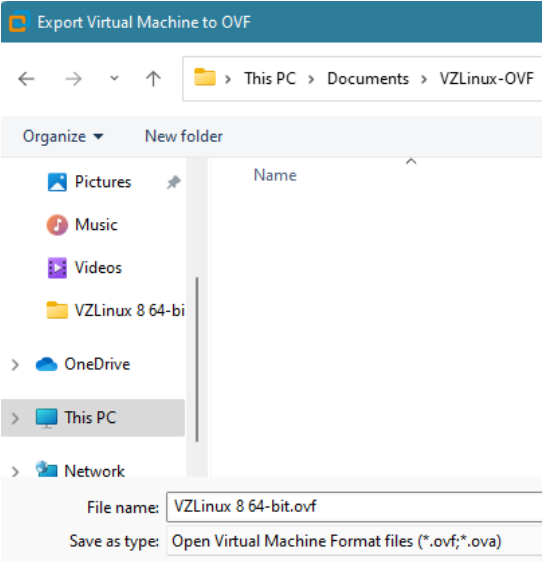

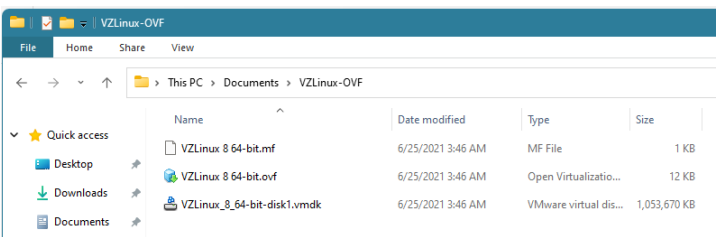
State: Powered off
Configuration file: C:\Users\admin\Documents\Virtual Machines\Clone of VZLinux 8 64-bit\Clone of VZLinux 8 64-bit.vmx
Clone of: C:\Users\admin\Documents\Virtual Machines\VZLinux 8 64-bit\VZLinux 8 64-bit.vmx
Hardware compatibility: Workstation 16.x virtual machine
Primary IP address: Network information is not available

• L'import/export des VM

Il existe un moyen d'exporter une machine virtuelle s'appuyant sur un format d'import/export reconnu par les principaux éditeurs d'hyperviseurs - le format **OVF**

L'exportation se fait dans un répertoire créé au préalable.

Exportation d'une machine virtuelle	
<p>L'exportation se fait à partir du menu "File"</p>	

Suite	
	Exportation vers le répertoire de destination
Export en cours	
	R�sultat de l'export

La machine virtuelle peut maintenant  tre export e vers un autre Hyperviseur - vers un autre VMware Workstation sur une autre machine, vers VirtualBox ou encore vers VMware ESXi.

Bien sur tous les snapshots ont disparu dans l'export et la machine export e ne contient que l' tat le plus r cent de la machine virtuelle