PLAN

I. INTRODUCTION

La virtualisation, apparue depuis le début des années 80 suite aux travaux développés au centre scientifique d'IBM en collaboration avec le MIT, a comme intérêts principaux : l'utilisation optimale des ressources d'un parc de machines, l'économie sur le matériel par mutualisation (consommation électrique, entretien physique, surveillance, support, compatibilité matérielle, etc.) et allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné. Ainsi, au début des années 2000, après le développement et la popularisation par la société VMware d'un système propriétaire de virtualisation logicielle des architectures de type x86 pour les architectures de type x86, les logiciels libres Xen, KVM, QEMU, Bochs, Linux-VServer, Virtual Box et les logiciels propriétaires mais gratuits Virtual PC, Virtual Server et VMware Server ont achevé la popularisation de la virtualisation dans le monde x86. C'est alors que l'éditeur Microsoft, suite à l'avancée technologique notamment avec l'avènement des systèmes 64bits, a remplacé sa solution Virtual Server par l'Hyper-V. Dans notre travail, après avoir fait une présentation du concept de la virtualisation dans un premier temps, nous ferons une étude comparative entre Hyper-V et VMware ESX qui sont les deux solutions de virtualisation les plus prisées dans le milieu actuel de l'entreprise. Nous parlerons ensuite de l''Hyper-V pour terminer sur l'installation et l'administration de cet dernièr sous Windows 2008 Server R2 en renforçant la sécurité.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

II. CONCEPT DE LA VIRTUALISATION

Le concept de "virtualisation" couvre l'ensemble des techniques permettant de dissocier les caractéristiques physiques d'un système matériel ou logiciel des applications orientées utilisateurs. La virtualisation est utilisée pour permettre le fonctionnement de plusieurs machines virtuelles disposant chacune de leur système d'exploitation spécifique partageant la même infrastructure physique.

À l'heure où les ordinateurs personnels deviennent de plus en plus puissants, les entreprises sont aujourd'hui attirées par le « Cloud Computing ». Derrière ces deux mots se cache un certain nombre de concepts à assimiler pour bien en comprendre les principes. Cette partie, non exhaustive, a pour but de présenter le concept important de la virtualisation de système d'exploitation. Il se veut simplement un moyen aux initiés ou non-initiés de comprendre ou d'approfondir certains points pouvant paraitre obscurs.

Afin de rendre l'ensemble plus lisible, le thème complet a été découpé en plusieurs parties. Cette première partie présente les différentes technologies de virtualisation, l'architecture d'un hyperviseur ainsi que les mécanismes de gestion de la mémoire.

II.1 Définition

La virtualisation regroupe les différentes méthodes permettant d'exécuter plusieurs systèmes d'exploitation sur une même machine physique.

Il n'est pas rare aujourd'hui de voir des serveurs avec 10 cœurs pour le CPU et plus de 32Go de RAM. Cependant, la mise en place d'un seul système d'exploitation sur ce type de machine amène souvent à une sous-utilisation de cette dernière. En effet, très peu de logiciels sont faits pour gérer de telles quantités de ressources. Comment mettre correctement à profits ces dernières ? La virtualisation de systèmes d'exploitation est là pour ça.

Une machine virtuelle (VM), est une entité logique hébergée sur une machine physique (hôte). On retrouve sur la VM les mêmes composants que sur une machine physique (CPU, RAM, disque dur, carte réseau, etc.). Une machine virtuelle est limitée à l'exécution d'un système d'exploitation.

Les intérêts de la virtualisation sont :

- Une utilisation optimale des ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives) ainsi qu'une économie sur le matériel (consommation électrique, compatibilité logicielle et matérielle…)

- L'installation, le déploiement et la migration facile des machines virtuelles d'une machine physique à une autre, notamment dans le contexte d'une mise en production à partir d'un environnement de qualification ou de pré-production, livraison facilitée.
- Sécurisation d'un réseau (l'attaquant n'a accès qu'aux machines virtuelles)
- Isolation des différents utilisateurs simultanés d'une même machine

II.2 Virtualisation de type I et II

Vous vous en doutez, la virtualisation englobe de nombreuses technologies diverses, amenant à des performances différentes.

Pour rappel, on peut schématiser le fonctionnement d'un ordinateur de la façon suivante :

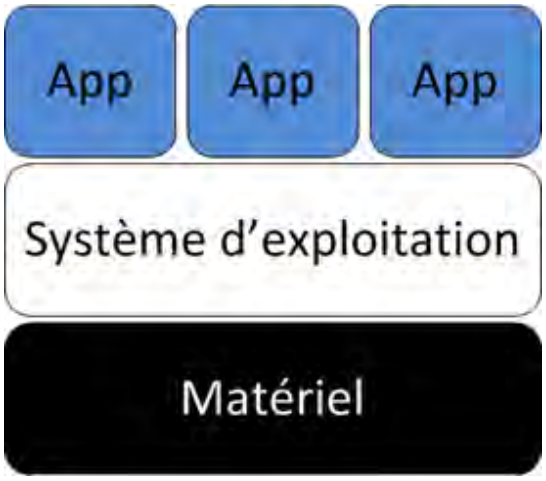


Image II.2.1 : Schéma de fonctionnement d'un ordinateur

Le système d'exploitation repose sur la couche matérielle de l'ordinateur. Il se charge de gérer les ressources pour lui-même ainsi que les différentes applications qu'il exécute.

La première technologie de virtualisation apparue, appelée virtualisation de type II, est un programme venant s'installer au-dessus du système d'exploitation comme n'importe quelle autre application. Il se charge de virtualiser les différents périphériques nécessaires aux machines virtuelles, et transmet les demandes de ressources au système d'exploitation hôte. On pourrait schématiser ce que l'on vient d'expliquer de la façon suivante :

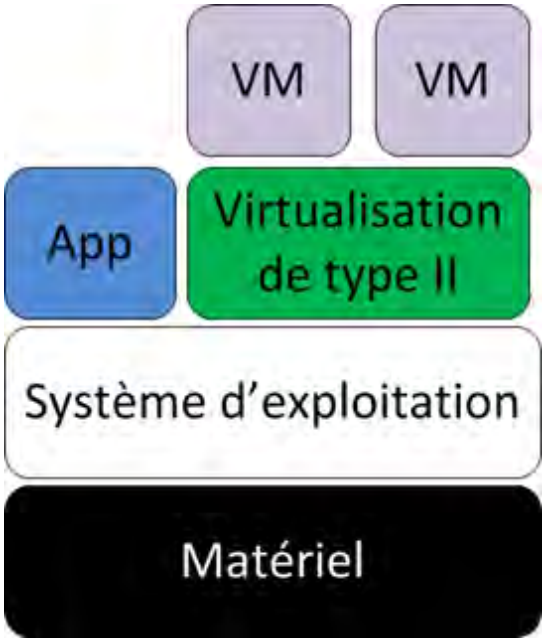
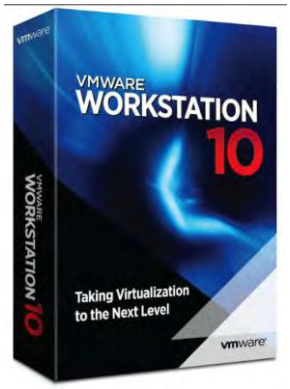


Image II.2.2 : Schéma de fonctionnement de la virtualisation de type II

Les exemples de ce type de logiciels sont nombreux : VMware Workstation, Microsoft Virtual PC, Oracle Virtualbox etc.



La limitation de ce type de virtualisation se fait généralement vite sentir. En effet, les systèmes d'exploitation clients que nous utilisons (Windows 8, 7, Mac OS X Client) ne sont pas fait pour gérer de nombreux accès simultanés aux ressources (RAM, disques dur, etc.).

Plus tard, est apparu une seconde technologie appelée virtualisation de type I. Cette technologie supprime le principal goulot d'étranglement, à savoir le système d'exploitation hôte, pour gérer lui-même les ressources physiques de la machine.

Dans ce cas, la couche logicielle, faisant le lien entre la machine hôte et les machines virtuelles, est appelé hyperviseur.

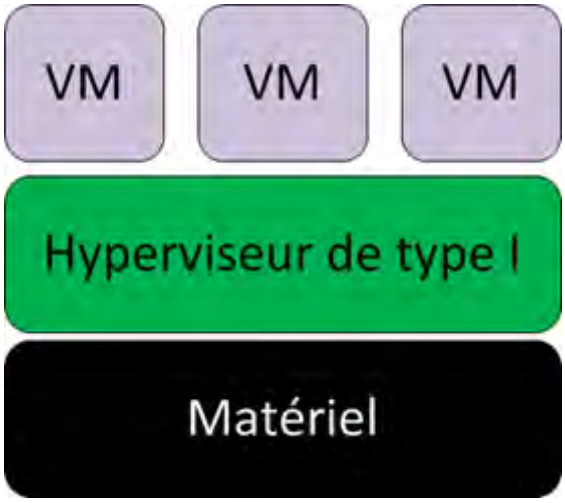


Image II.2.3 : Schéma de fonctionnement de la virtualisation de type I

Les hyperviseurs ont été spécialement conçus pour gérer les nombreux accès concourants que demande la virtualisation de système d'exploitation, rendant ainsi cette technologie beaucoup plus efficace.

Le leader sur cette technologie est VMware avec son hyperviseur ESXi. D'autres éditeurs sont présents, à savoir Microsoft avec Hyper-V et Citrix avec XenServer.

II.3 Architecture de l'hyperviseur

Comme on l'a dit, l'hyperviseur se charge de répartir les ressources matérielles en fonction des demandes des machines virtuelles clientes.

Pour ce qui est du processeur, c'est de façon matérielle que l'hyperviseur va se charger de transmettre des instructions de la VM au matériel, à l'aide des technologies Intel-VT ou AMD-V, présente directement sur vos processeurs.

La mémoire vive ou RAM, quant à elle, est le seul composant à être géré en mode utilisateur, afin de profiter des différents mécanismes de protection mis en place. En étant gérée dans l'espace utilisateur, on évite qu'une machine virtuelle aille écrire dans un espace mémoire réservé, ou alloué à une autre VM. Les

technologies de virtualisation de la **MMU**[1] accélèrent grandement l'accès à la mémoire physique depuis une machine virtuelle.

Les autres périphériques, quant à eux, nécessitent le passage en mode noyau pour être utilisés. Afin de garantir un maximum de sécurité, l'hyperviseur ne laisse pas d'accès direct en mode noyau. En effet, il met à disposition des composants, appelés « Virtual Service Provider » (VSP), permettant à la VM cliente de pouvoir consommer les périphériques. Du côté de la machine virtuelle, des drivers spéciaux, appelés « Virtual Service Clients » (**VSC**) sont installés pour permettre la communication avec les différents VSP. Si vous avez déjà utilisé des hyperviseurs, vous avez surement installés les outils invités de ces derniers (VMware tools, Integration Services for Hyper-V, XenServer Tools, etc.). C'est dans ces packages invités que sont présents les drivers des VSC. La communication entre les VSP et les VSC se fait à travers un composant appelé VMbus, qui n'est autre qu'un bus de communication entre les VM et l'hôte.

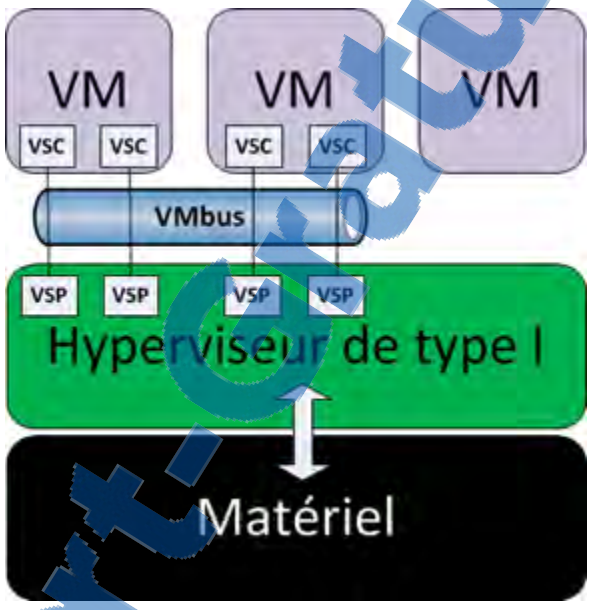


Image II.3.1 : Architecture de l'Hyperviseur de type I

GESTION DE LA MÉMOIRE

La RAM est actuellement le principal limiteur des infrastructures de virtualisation. Pour cela, les différents éditeurs ont développé de nombreuses techniques pour économiser un maximum de mémoire, sans pour autant dégrader les performances des VM. Les différents mécanismes sont détaillés à la suite :

[1] Une **unité de gestion mémoire** (**MMU** pour *memory management unit*) est un composant informatique responsable de l'accès à la mémoire demandée par le processeur. Sur le matériel ancien, elle était indépendante du processeur.

Rapport-Gratuit.com

ALLOCATION DYNAMIQUE

Lors de la définition d'une VM, une certaine quantité de RAM lui est allouée. La première technique de gestion de la mémoire consiste à réserver cette quantité de mémoire sur l'hôte. Pour une machine virtuelle utilisant 4Go de mémoire vive, 4Go sont utilisés sur la machine hôte. Cependant, il est rare qu'une VM utilise toute sa mémoire RAM. On se retrouve donc avec une certaine quantité de RAM allouée, sans être pour autant totalement utilisée. Pour contrer cela, différentes technologies de gestion dynamique de la RAM ont été développées :

II.3.1 VMWARE MEMORY OVERCOMMIT

Cette technique consiste à faire croire à la VM que la totalité de la mémoire demandée est disponible, tout en n'allouant que le minimum. Prenons un exemple:

Une VM est configurée pour avoir 4 Go de mémoire RAM, mais n'en utilise que 2,5 Go à un instant T. La machine virtuelle pensera disposer tout le temps des 4 Go, sauf que seulement 2,5 Go seront alloués au niveau de l'hôte, permettant d'utiliser les 1,5 Go restant pour autre chose.

II.3.2 MICROSOFT DYNAMIC MEMORY

Microsoft utilise une approche différente pour la gestion de la mémoire RAM. La VM est définie avec une quantité de mémoire au démarrage et une quantité maximum possible. Quand la VM démarre, elle ne voit que la quantité de RAM définie au démarrage. Si à un moment, la VM nécessite plus de mémoire que la quantité définie au démarrage, l'hôte va lui ajouter de la mémoire à chaud. L'hôte n'ajoutera pas plus de mémoire que la quantité de mémoire maximum définie au niveau de la machine virtuelle.

Quand la nécessité de mémoire diminue, un des driver, appelé ballooning va se charger de récupérer la mémoire RAM inutilisée.

L'approche est différente puisque dans ce cas, la machine voit réellement la mémoire qui lui est allouée.

II.3.3 VMWARE TRANSPARENT PAGE SHARING

Une des autres fonctionnalités que VMware met en place pour économiser de la mémoire. Transparent Page Sharing (TPS), va chercher des pages mémoire similaires entre plusieurs VM, afin de les singulariser. Par exemple, si vous avez 10 VMs Windows Server 2008 R2, une certaine quantité de la RAM va être similaire sur les machines virtuelles (dû au même système d'exploitation sur les différentes machines virtuelles). VMware va

alors faire pointer toutes ces pages mémoire virtuelles sur une même page mémoire physique, économisant ainsi de l'espace.

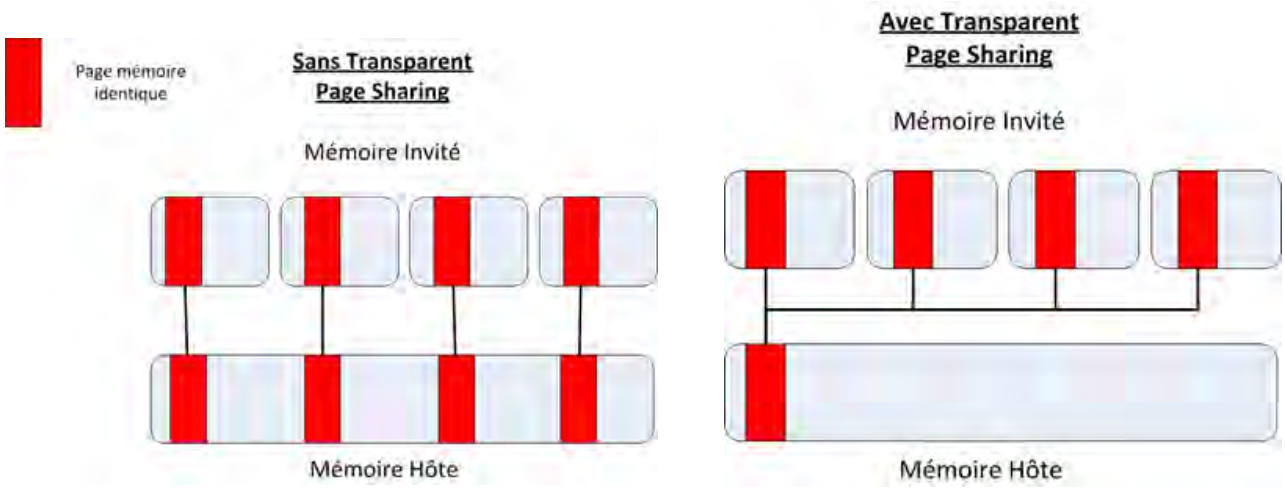


Image II.3.3.1 : Fonctionnement Sans Transparent Page Sharing

II.3.4 VMWARE BALLOONING

Cette fonctionnalité est différente du principe de ballooning présenté sur Microsoft Dynamic Memory.

VMware Ballooning est un mécanisme utilisé lorsque l'hôte commence à manquer de mémoire. Il faut garder à l'idée que si les mécanismes de ballooning sont exécutés sur votre VM, c'est que votre infrastructure virtuelle commence à montrer ses limites.

Le ballooning est un driver présent dans les machines virtuelles qui va gonfler en RAM, afin de réserver de la mémoire sur l'hôte, et éviter que la VM manque de mémoire vive. Cette technique est généralement utilisée sur les VM critiques de l'infrastructure virtuelle, et doit être utilisée avec parcimonie.

III. ÉTUDE COMPARATIVE ENTRE HYPER-V ET VMWARE ESX

Comme hyperviseurs les plus crédibles sur le marché de la virtualisation, VMware et Hyper V sont donc comparables. Ceci dit, il y a des distinctions notables et qui sont propres dans la conception de chacune des plateformes où nous trouverons des avantages et des inconvénients pour chacune.

Pour exposer l'importance et l'intérêt de la comparaison nous avons choisir certains critères de comparaison.

Les termes utilisés dans la suite :

- VMware

- Vi3 = Virtual Infrastructure 3
  - Hyperviseur ESX3
  - Administration: Virtual Center
- Vsphere4 (hyperviseur ESX4) remplace depuis fin mai 2013 vi3
  - Hyperviseur = ESX4
  - Administration= **VMware vCenter4**

- Microsoft
  - Hyperviseur = Hyper-V
  - Hyperviseur = Hyper-V R2 (Release2)
  - Administration=SCVMM2008 (**System Center Virtual Machine Monitor**)

III.1 Structure technique des hyperviseurs

Les produits VMware ESX et ESXi sont des hyperviseurs monolithiques. Dans une conception monolithique, l'hyperviseur gère l'accès au matériel pour chaque VM. Il contient les pilotes de périphériques pour tous les composants auxquels ces machines virtuelles doivent accéder, y compris les dispositifs d'entrée, réseau et de stockage. Cette configuration nécessite que les pilotes soient installés physiquement sur la couche hyperviseur, en plus d'un pilote spécial qui contrôle l'accès aux composants matériels.

Le plus grand avantage de la conception monolithique est qu'elle ne nécessite pas un système d'exploitation hôte. L'hyperviseur agit en tant que plate-forme d'exploitation qui prend en charge tous les systèmes d'exploitation virtuels fonctionnant sur le matériel. Un avantage clé que cette configuration offre, est une performance supérieure car ces systèmes d'exploitation se comportent comme s'ils sont effectivement en cours d'exécution sur la machine physique. L'Administration de la machine virtuelle est également simplifiée car le système d'exploitation hôte n'a pas besoin de fournir un accès à des outils qui gèrent ces environnements.

Le logiciel Hyper-V de Microsoft est un hyperviseur "microkernelizé". Ce produit particulier n'a pas de pilotes de périphériques à la couche hyperviseur. Au lieu de cela, les pilotes se trouvent dans les partitions des systèmes d'exploitation différents, où ils s'exécutent indépendamment pour chaque environnement virtuel individuel. En raison de cette configuration, Hyper-V est en mesure de profiter de certains avantages uniques sur VMware.

Hyper-V comme ESX4 tourne uniquement sur un environnement 64 bits :

III.1.1 GESTION DES PILOTES

Concernant la gestion des pilotes, on constate une différence importante chez Microsoft et Chez VMware.

Chez Microsoft, les pilotes sont ceux de Windows Server 2008. Ils sont également dans l'hyperviseur mais dialoguent avec des pilotes dits synthétiques, présents dans les machines virtuelles. L'avantage est que cela assure une compatibilité de plateforme plus importante mais l'inconvénient est que l'ajout de pilotes spécifiques peut poser problème car la majorité des bugs viennent de problèmes de pilotes.

Chez VMware, ils sont embarqués dans l'hyperviseur. L'éditeur garantit donc leur parfaite compatibilité, il faut vérifier que le serveur et les périphériques : stockage, réseau sont certifiés et validés pour VMware.

III.1.2 ARCHITECTURE VMWARE ESX

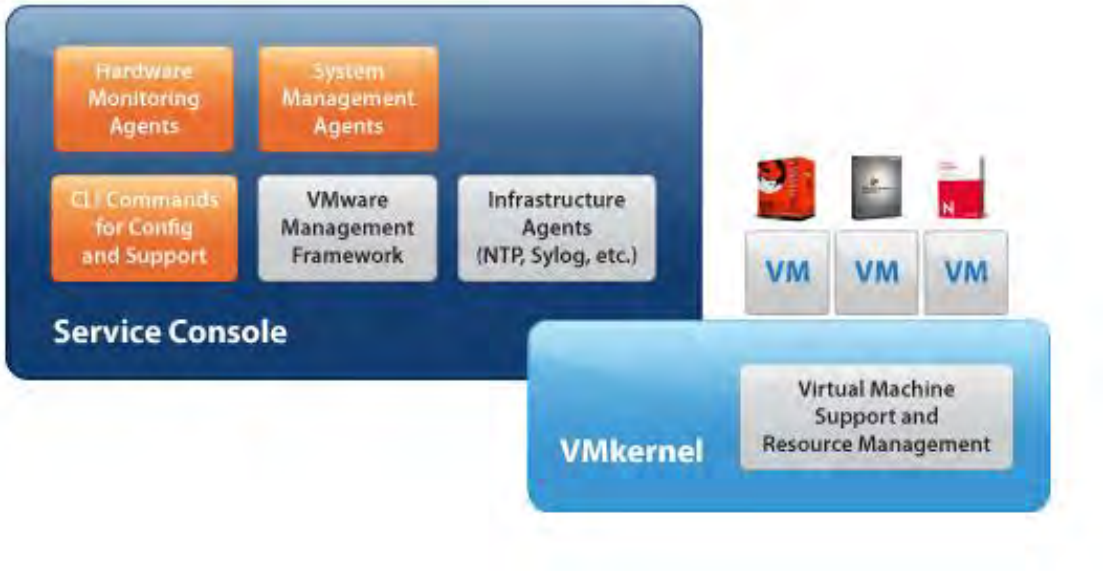


Image III.1.2.1: Architecture d'ESX

L'architecture de VMware ESX est composé de deux éléments : le Vmkernel et le service console.

Le Vmkernel

C'est un système entièrement développé par VMware, il est le cœur et le moteur de la virtualisation. Le Vmkernel accède directement au hardware et Schedule le temps CPU, gère la mémoire, les entrées sorties les accès disques et réseau et gère les machines virtuelles.

Le service console

Il contient des services tel que : un firewall, SNMP, Web Server, Remote KVM etc.

Il est une machine virtuelle basée sur du Red Hat Enterprise Linux (pour la version ESX4) qui donne accès au Vmkernel permettant ainsi de modifier et configurer les paramètres du serveur ESX.

III.1.3 ARCHITECTURE MICROSOFT HYPER-V

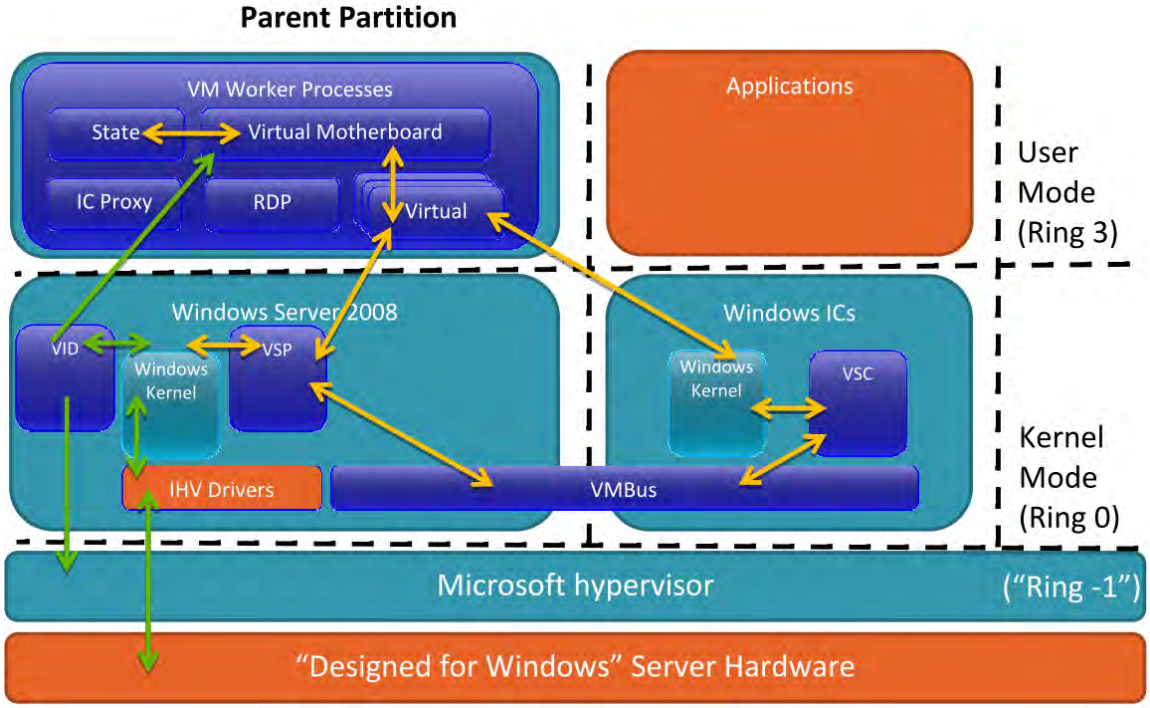


Image III.1.2.1: Architecture de Hyper-V

Dans l'architecture Hyper-V nous constatons les composants en mode utilisateur, les composants en mode noyau et les composants Micronoyau.

Les composants en mode utilisateur

Les composants sont :

- ✓ **Le processus de travail VM ou VM Worker Process**
- ✓ **State Machine** : applique les transitions d'état valides (par exemple les opérations de gestion de la console, Opérations Clients, et les événements de l'hôte). Il fournit des fonctionnalités de sauvegarde et état instantané ; fonctionne avec Virtual Infrastructure Driver (le pilote de l'infrastructure virtuelle), Virtual motherboard et virtual devices pour contrôler le Virtual Hardware State (état du matériel virtuel) ;
- ✓ **Virtual motherboard** ou Carte mère virtuelle : fonctionne avec State Machine pour contrôler le Virtual Hardware State

- ✓ **Virtual Devices** ou périphériques virtuels : tient compte des changements d'état effectués par la Virtual Motherboard. Il fonctionne avec VSP[2] pour contrôler l'état du matériel virtuel des périphériques synthétiques.
- ✓ **IC (Integration Component) Proxy** : fonctionne avec des composants d'intégration dans les partitions enfant pour gérer les transitions d'état pour l'arrêt de l'OS

Les composants en mode noyau

Ce sont :

- ✓ **Virtual Infrastructure Driver (VID)** ou pilote de l'infrastructure virtuelle : intervient dans la communication avec l'hyperviseur. Il lance également des requêtes à l'hyperviseur en utilisant le protocole hypercall ; il fournit aussi des informations sur l'état du matériel physique à State Machine
- ✓ **IHV Drivers** : gère l'interaction avec le matériel
- ✓ **VM Bus** : En bus mémoire, il permet la communication entre les partitions

Les composants Micronoyau

- ✓ Hyperviseur : Il gère un ensemble minimal de composants matériels: processeurs, Local APICS, Constant-rate, System Counter, System physical address space ; il met aussi l'accent sur la planification et l'isolement.

III.2 Fonctionnalités

Le tableau suivant montre les différences principales entre Hyper-V et VMware vi3 :

Fonctionnalités	Microsoft **WS2008 Hyper-V**	VMware **vi3**
Mémoire maximal du host	1024 Go	256 Go
vCPUs maximal en fonctionnement	192	192
vCPU maximal par client	4 vCPU	4 vCPU
Mémoire maximale par client	64 Go	64 Go
Nombre maximale de processeurs logiques (nombre de cœurs)	24	32

[2] Virtualization Service Provider (VSP) se connecte à VMBus et traite les demandes d'accès aux périphériques de partitions enfants

VMs 64-bit	Oui	Oui
Overcommitment, TPS, Ballooning	Non	Oui
Scripting Interface	WMI	WMware API / PowerShell
SMP VMs	4-voies	4 vois
Format du disque	VHD, pass-thru	VMDK, RDM
Ajout à chaud de CPU/mémoire/réseau/disque	Non	Disque seulement
Quick migration	Oui	Vmotion
User Interface	MMC 3.0	WEB
Concurrent shared disk in cluster	Non	Oui
Outil d'administration des VMs	Oui : SCVMM2008	Virtual Center

Le tableau suivant montre les différences principales entre Hyper-V R2 et VMware Vsphere4 :

Fonctionnalités	Microsoft **Hyper-V R2**	VMware **Vsphere4**
Mémoire maximale du host	1024 Go	512 Go
vCPUs maximal en fonctionnement	384	320
vCPU maximal par client	4 vCPU	4 vCPU
Mémoire maximale par client	64 Go	256 Go
Processeurs logiques (nombre de cœurs)	64	64
VMs 64-bit	Oui	Oui
Overcommitment, TPS, Ballooning	Non	Oui
Scripting Interface	WMI / PowerShell	WMware API / PowerShell
SMP VMs	4-voies	4 vois
Format du disque	VHD, pass-thru	VMDK, RDM

Ajout à chaud de CPU/mémoire/réseau/disque	Oui pour disque SCSI	Oui pour CPU/Mémoire/réseau/stockage[3]
Quick migration	Oui	Oui
User Interface	MMC	WEB
Concurrent shared disk in cluster	Oui	Oui
Outil d'administration des VMs	Oui : SCVMM2008	Vmware vCenter4

VMware offre des fonctionnalités supplémentaires bien supérieures à celles de Microsoft : Vmotion, Live migration, quick migration. Quelles sont les différences ?

Vmotion (inventé par VMware) existe depuis la version 2 de VMware et devance Microsoft sur la migration à chaud de VM sans interruption de service. DRS qui exploitent la fonctionnalité Vmotion pour basculer automatiquement les VM sur d'autres serveurs physiques existe également depuis quelques années. Vmotion sert principalement pour répartir la charge dans des fermes de serveurs et est également utiles lors de rajout d'un composant sur un serveur (la mémoire par exemple) sans arrêter la production.

Quick Migration définie par Microsoft. La VM est mise dans un état sauvegardé appelé hibernation (les informations de la mémoire sont écrites sur le disque dur) avant que la VM ne migre sur un autre serveur ce qui entraine un arrêt de service.

Live Migration (Microsoft) : identique à Vmotion de Vmware disponible avec HyperV R2. La migration se fait sans interruption de service.

Autres différences

L'autre nouveauté très importante avec Vsphere4 concerne la fonctionnalité de Fault Tolerance permettant ainsi de bénéficier d'une très haute disponibilité ou l'état d'une VM est répliqué en mode synchrone sur un autre serveur physique. En cas de défaillance d'un serveur physique il n'y aura aucune interruption de service car la VM synchronisée reprend automatiquement le service.

Cette technique est assez remarquable et permet à VMware de se positionner encore en entreprise très innovante et à la pointe de la technologie. Les autres nouveautés de Vsphere4 comme le Distributed Switch, linked clone, Thin provisioning, Host profiles sont des améliorations permettant de simplifier la tâche des administrateurs.

[3] Nécessite le redémarrage de la VM pour activation

VMware supporte un très grands nombre d'OS client (voir liste de compatibilité sur le site VMware) alors que l'Hyper-V ne propose aujourd'hui qu'un nombre très limité d'OS client.

Microsoft ne propose pas un spectre de fonctionnalité aussi large ce qui ne leur permet pas aujourd'hui d'adresser les grands comptes. À noter cependant que Hyper-V R2 propose HA gratuitement.

III.3 Administration

Microsoft et VMware offrent des fonctionnalités d'administration sensiblement équivalentes. La principale différence vient du fait qu'avec Virtual Center, VMware propose une solution ne gérant que des environnements virtualisés. Au contraire, Microsoft adapte sa gamme System Center (SC) existante. SC Configuration Manager, SC Operation Manager et bientôt SC Data Protection Manager permettent ainsi de superviser, mettre à jour et sauvegarder des machines virtuelles aussi bien que physiques. Microsoft y ajoute Virtual Machine Manager, qui permet notamment d'identifier les serveurs candidats à la virtualisation et les cibles matérielles.

III.4 Écosystèmes partenaires

VMware bénéficie déjà d'un vaste écosystème d'éditeurs tiers proposant des solutions complémentaires dédiées à la sauvegarde, à la réplication, à la migration ou à l'inventaire de machines virtuelles. Pour la sauvegarde des éditeurs comme Veeam Software ou Vizioncore (filiale de Quest Software) se sont imposés. Mais Microsoft rattrapera rapidement son retard en séduisant les mêmes éditeurs, qui annoncent tous le support d'Hyper-V.

III.5 Prix listés

Hyper-V est moins coûteux que VMware Infrastructure si on ne prend en compte que le coût des licences. D'autre part, dans nombre d'entreprises, son coût sera intégré dans un contrat de licence annuel. Autre atout : il est intégré à Windows Server 2008 vers lequel migreront tôt ou tard les comptes Microsoft. Quant au coût des systèmes installés dans les machines virtuelles, il sera le même quel que soit l'hyperviseur, mais différent selon la version de Windows Server - Standard, Enterprise ou Datacenter - qui comprennent respectivement une, quatre ou un nombre illimité de licences gratuites. VMware devra tôt ou tard adapter sa tarification pour rendre son offre accessible au plus grand nombre et notamment aux PME.

MICROSOFT		VMWARE		
Version	Prix liste	Version	Prix liste pour 1 processeur. 1 an support gold	Avec 3 ans support Gold/platinum
Standard (1 vm)	$999 (includes 5 CALs)	Standard	1068$	1491$/1618$
Enterprise (jusquà 4vm)	$3999 (includes 25 CALs)	Advanced	2717$	3448$/3675$
Datacenter (nombre de vm illimités)	$2999 (per socket)	Enterprise	3479$	4415$/4708$
Itanium	$2999 (per socket)	Enterprise plus	4229$	5366$/5723$
Web Server	$469 (no CALs required)			
Storage Server	TBD			
Compute Cluster Server	$469 (per node)			

Image III.5.1: Comparatif des prix Hyper-V et VMware (juin 2009)

III.6 VMware et Hyper-V : Avantages / Inconvénients

Hyper-V sous 2008 R2 tourne quasi-complètement sous Windows Server 2008 R2 dans son domaine de 0, ce qui rend le affecté par la plupart des failles de sécurité et attaques de Windows Server 2008 R2. VMware ESX 4 étant composé d'une petite empreinte basée sur RedHat dans sa console de service, ce qui le rend plus prune aux attaques et aux failles de sécurité que Hyper-V sous Windows Server 2008 R2.

➔ COÛT

Si vous cherchez à réaliser des économies, choisir la solution de virtualisation Microsoft Hyper-V constitue le meilleur choix. La solution VMware peut coûter jusqu'à six fois le prix de la solution Hyper-V selon Microsoft pour des prestations comparables. De plus il existe des versions gratuites d'Hyper-V mais également de VMware Server. Si le coût est le seul critère dans le match qui oppose Hyper-V à VMware c'est Microsoft qui sort vainqueur.

➔ SUPPORT

VMware et Microsoft offrent tous les deux un haut niveau de support. Microsoft possède cependant un léger avantage avec une qualification des drivers et du matériel compatible avec ses produits. Dans les deux cas de figures, il existe sur le marché des experts permettant de répondre aux problèmes ou bugs rencontrés. De même

de nombreux forum existent sur VMware mais également sur Hyper-V avec une communauté de MVP dévoués. Du côté support on accordera un match nul entre les deux éditeurs.

➔ AVIS FINAL SUR VMWARE ET HYPER-V

Plusieurs experts comme ceux chez Orbytes[4] par exemple sont partagés sur les différences entre VMware et Hyper-V pour dégager le meilleur produit. Mais ils sont unanimes sur un point. Le meilleur produit est **celui qui saura répondre aux besoins du client d'un point de vue technique mais également budgétaire et tarif**. Le rapport qualité / prix est très important mais il doit permettre de répondre aux exigences. Toutes les entreprises n'ont pas les mêmes besoins et les mêmes attentes vis à vis de leur solution de virtualisation. C'est pourquoi, pour les projets de virtualisation, il est primordial de faire valider ses besoins et la faisabilité par des consultants en prenant également en compte les contraintes budgétaires et la notion de temps.

IV. NOTION D'HYPER V

MOTIVATION DU CHOIX PORTÉE SUR LA SOLUTION

Selon un rapport publié[5] par la fameuse société IDC[6] dans un article du Wall Street Journal, Microsoft est entrain de ralentir progressivement la dominance de VMware dans l'espace de la virtualisation. Il a été noté qu'en 2008, les trackers IDC estimaient que 20,3% des systèmes virtualisés utilisaient Hyper-V. L'an dernier, c'est-à-dire en 2012, ce pourcentage était à 27,6%. Au même moment, la part de marché de VMware a baissé de 65,4% en 2008 à 56,8% en 2012.

Pour exemple, la société alimentaire internationale basée aux USA, Domino's Pizza[7] a commencé en 2011, en partie pour rester conforme à la Payment Card Industry Data Security Standard, la mise à niveau de 1500 serveurs de ses points de vente du système d'exploitation Windows XP vers Windows 2008 R2. Un bonus que Domino a obtenu par la mise à niveau vers Windows Server 2008 R2 est la technologie de virtualisation

---

[4] Source : ORBYTES.FR - **Comparaison VMWare Hyper-V et Xen Server** - http://www.orbytes.fr/vmware-contre-hyper-v/

[5] Source : **Hyper-V market share jumps more than 30% since 2008** - Published on 2 June 2013 http://www.virtualizationadmin.com/blogs/lowe/news/hyper-v-market-share-jumps-more-30-2008.html

[6] **International Data Corporation (IDC)** est une firme américaine des études de marché, d'analyse et de conseils, spécialisée dans les technologies de l'information, des télécommunications et de la technologie du consommateur. (http://en.wikipedia.org/wiki/International_Data_Corporation)

[7] Source : **Pizza Chain to Switch 10,000 Store Servers to Hyper-V to Increase Reliability, Performance** - http://www.microsoft.com/casestudies/Windows-Server-2008-R2-Datacenter/Domino-s-Pizza/Pizza-Chain-to-Switch-10-000-Store-Servers-to-Hyper-V-to-Increase-Reliability-Performance/710000002307

Hyper-V intégrée à ce système d'exploitation. Ainsi, le géant de la pizza envisage de migrer ses 10.000 serveurs localisés dans les magasins aux USA vers la technologie de virtualisation Hyper-V sur Windows Server 2008 R2 pour éliminer les problèmes de fiabilité et de performance qu'il a eu à expérimenter avec sa solution de virtualisation précédente. À ce jour, Domino utilise Microsoft System Center data center solutions pour gérer 15.000 serveurs avec seulement deux personnes, une grande réussite de l'efficacité.

L'hyperviseur Hyper-V étant une solution de plus en plus adaptée dans les entreprises modernes, et étant déjà intégré dans Windows 2008 R2 que nous avons utilisé lors de notre année universitaire, nous la choisirons comme objet d'étude dans le cadre de ce mémoire.

DÉFINITION D'HYPER-V

Hyper-V sortie sous le nom de code Viridian, est formellement connu sous le nom de Windows Server Virtualization, est un hyperviseur natif permettant la virtualisation des plateformes sur les systèmes x86-64.

Hyper-V se base sur les concepts de para-virtualisation et d'hyperviseur vus dans la section précédente.

Il existe sous deux variantes qui sont :

- Comme un rôle installable sous Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 et l'édition x64 de Windows 8 Pro ;
- Comme un produit autonome (Stand-Alone) appelé Hyper-V Server : Trois majeures versions ont jusque-là été publiées : Hyper-V Server 2008, Hyper-V Server 2008 R2 et Hyper-V Server 2012 (contenant la version actuelle d'Hyper-V). Ces versions du produit autonome sont gratuites.

Pour planifier et déployer efficacement Hyper-V dans Windows Server 2008 R2, nous devons comprendre les configurations requises et maximales du matériel physique et virtuel composant l'environnement informatique de serveur virtualisé. Nous devons tenir compte des valeurs maximales qui s'appliquent à chaque ordinateur virtuel ainsi que de celles applicables à l'ordinateur physique qui exécute le rôle Hyper-V.

SPÉCIFICATIONS ET CONFIGURATION SYSTÈME REQUISES

Les spécifications sont généralement identiques au système d'exploitation Windows 2008 Server

- Système d'exploitation hôte :
  - Pour installer le rôle Hyper-V : Windows Server 2008, Windows Server 2008 R2 Standard, Entreprise ou l'édition Datacenter, Windows Server 2012 Standard Edition ou l'édition Datacenter, ou

Windows 8 Pro ou l'édition Entreprise est nécessaire. Hyper-V est pris en charge uniquement sur les variantes x86-64 (64 bits) de Windows.

- Il peut être installé indépendamment du fait que l'installation soit complète ou Core (installation de base)

- Processeur
  - Un processeur x86-64, c'est-à-dire 64 bits
  - Le support Hardware-assisted virtualization. Celui-ci est disponible dans les processeurs incluant une option de virtualisation; spécifiquement, Intel VT ou AMD Virtualization (AMD-V, formellement sous le nom de code « Pacifica »).
  - Un processeur compatible **NX-bit**[8] doit être disponible et la **Data Execution Prevention (DEP)**[9] matérielle doit être activée
  - Bien que ce ne soit pas un prérequis officiel, Windows Server 2008 R2 et un processeur avec le support Second Level Address Translation[10] sont recommandés pour les stations de travails.
    - La translation d'adresse de second niveau est obligatoire pour Hyper-V dans Windows 8.

- Mémoire
  - Au minimum 2GB de RAM (Chaque machine virtuelle requiert sa propre mémoire, donc concrètement beaucoup plus encore
  - La version complète ou Core du GUI Hyper-V sous Windows Server 2008 Standard (x64) supporte au maximum jusqu'à 31Go de mémoire pour les machines virtuelles lancées, plus 1Go pour le parent OS d'Hyper-V
  - La mémoire totale maximum par système pour les hôtes Windows Server 2008 R2 : 32Go (Standard) ou 2To (Entreprise, Datacenter)
  - La mémoire totale maximum par système pour les hôtes Windows Server 2012 : 4To

- Systèmes d'exploitation invité :

[8] Le **NX Bit**, pour Never eXecute, est une technique utilisée dans les processeurs pour dissocier les zones de mémoire contenant des instructions, donc exécutables, des zones contenant des données. Ceci permet de faire de la protection d'espace exécutable protégeant le système des virus et chevaux de Troie utilisant les failles de dépassement de tampon : par exemple, un programme malveillant comme le ver Blaster, fait croire qu'il envoie des données, alors qu'il envoie du code corrompu.

[9] **Data Execution Prevention (DEP)** est un dispositif de sécurité intégré à de nombreux système d'exploitations modernes tels Linux, Mac OS X, iOS, Microsoft Windows et Android. Il est destiné à empêcher l'exécution de code depuis des blocs de mémoire censés contenir des données afin d'affaiblir les probabilités de réussite d'une attaque de type dépassement de tampon.

[10] **Second Level Address Translation** (SLAT) est une technologie de virtualisation assistée par matériel.

- Hyper-V dans Windows Server 2008 et 2008 R2 prend en charge des machines virtuelles avec au maximum 4 processeurs chacun (1, 2 ou 4 processeurs en fonction de l'OS invité) ;
- Hyper-V dans Windows Server 2012 prend en charge des machines virtuelles avec au maximum 64 processeurs chacun ;
- Hyper-V dans Windows Server 2008 et 2008 R2 prend en charge jusqu'à 384 machines virtuelles par système ;
- Hyper-V dans Windows Server 2012 prend en charge jusqu'à 1024 machines virtuelles actives par système ;
- Hyper-V prend en charge les machines virtuelles invité 32-bit (x86) et 64-bits (x64)

Microsoft Hyper-V Server

La variante autonome de Hyper-V Server ne nécessite pas une installation existante de Windows Server 2008 ou Windows Server 2008 R2. L'installation autonome est appelée Microsoft Hyper-V Server pour la version non-R2 et Microsoft Hyper-V Server 2008 R2. Microsoft Hyper-V server est fabriquée avec des composants de Windows et possède l'expérience utilisateur de Windows Server Core. Aucun des autres rôles de Windows Server sont disponibles dans Microsoft Hyper-V Server. Cette version prend en charge jusqu'à 64 machines virtuelles par système. La configuration requise de Microsoft Hyper-V Server sont les mêmes que pour les systèmes d'exploitation invités pris en charge et le processeur, mais diffèrent de ce qui suit :

- **RAM:** Minimum: 1 Go de RAM; Recommandé: 2 Go de RAM ou plus; Maximum 1 To.
- **Espace disque disponible:** Minimum: 8 Go; Recommandé: 20 Go ou plus.

FONCTIONS D'HYPER-V

Hyper-V fournit une infrastructure logicielle et des outils de gestion de base que nous pouvons utiliser pour créer et gérer un environnement informatique de serveur virtualisé. Cet environnement virtualisé peut être utilisé afin de réaliser différents objectifs professionnels liés à l'amélioration de l'efficacité et à la réduction des coûts. Un environnement de serveur virtualisé peut par exemple vous aider à effectuer les tâches suivantes :

- Réduire les coûts liés à l'exploitation et à la maintenance de serveurs physiques en augmentant l'utilisation de votre matériel. Vous pouvez réduire la quantité de matériel nécessaire pour exécuter vos charges de travail de serveur.
- Augmenter l'efficacité du développement et des tests en réduisant la durée nécessaire à la configuration du matériel et des logiciels et à la reproduction des environnements de test.

- Améliorer la disponibilité des serveurs sans utiliser autant d'ordinateurs physiques que dans une configuration de basculement qui utilise uniquement des ordinateurs physiques.

Hyper-V peut nous être utile si nous sommes :

- Un administrateur, un planificateur ou un concepteur informatique ;
- Un architecte informatique responsable de la gestion informatique et de la sécurité de l'organisation ;
- Un responsable des opérations informatiques qui recherche un moyen de réduire le coût total de propriété de son infrastructure de serveurs, à la fois en termes de coûts de puissance et de coûts de gestion ;
- Un développeur ou testeur de logiciels qui recherche un moyen d'augmenter la productivité en réduisant la durée nécessaire à la création et la configuration d'un serveur destiné au développement ou à des tests.

Principales fonctionnalités d'Hyper-V

Les principales fonctionnalités d'Hyper-V sont les suivantes :

- Virtualisation hyperviseur native 64 bits.
- Capacité d'exécuter simultanément des machines virtuelles 32 bits et 64 bits.
- Machines virtuelles monoprocesseurs et multiprocesseurs.
- Captures instantanées de machines virtuelles, qui capturent l'état, les données et la configuration matérielle d'une machine virtuelle en cours d'exécution. Comme les captures instantanées indiquent les états système, vous pouvez restaurer la machine virtuelle à un état précédent ;
- Prise en charge de grande mémoire de machine virtuelle.
- Prise en charge du réseau local virtuel (VLAN)
- Composant logiciel enfichable de gestion Microsoft Management Console (MMC).
- Interfaces WMI (Windows Management Instrumentation) documentées pour l'écriture de scripts et la gestion.

Dans Windows Server 2008 R2, Hyper-V ajoute les fonctionnalités suivantes :

- Migration dynamique

- Stockage d'ordinateur virtuel dynamique
- Prise en charge améliorée du processeur
- Prise en charge améliorée du réseau

V. INSTALLATION ET ADMINISTRATION DE HYPER-V SOUS WINDOWS 2008 SERVER R2

V.1 Prérequis d'installation sur VMWARE

Dans le cadre de ce mémoire, nous choisirons l'installation du rôle Hyper-V sous Windows Server 2008 R2 dans Vmware.

Les spécifications de notre environnement de test sont les suivantes :

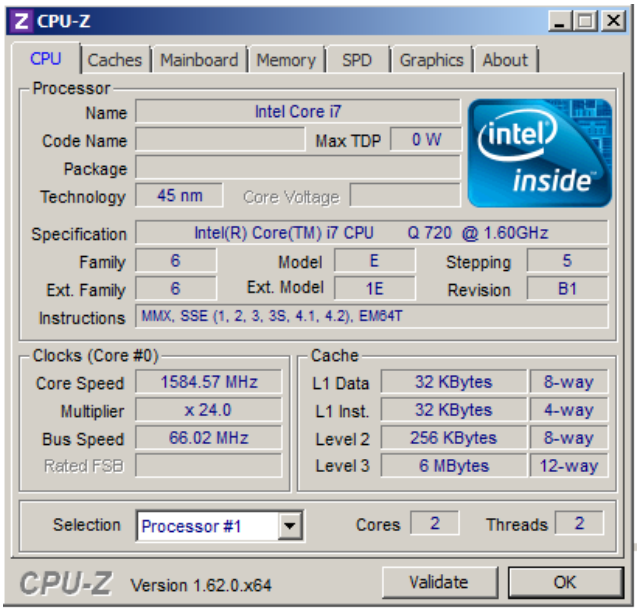
- OS: Windows Server 2008 R2 x64;
- Version : Entreprise,
- Processeur : Processeur Intel Core i7 720QM @1,6 Ghz ;
- RAM : 3 GB ;
- Espace Disque libre: 14 GB ;
- Périphériques : Lecteur DVD-Rom, Clavier, Souris

Hyper-V requiert un processeur Intel ou AMD 64 bits disposant des instructions de virtualisation Intel-VT ou AMD-V. Il faut noter que par défaut, ces instructions sont désactivées dans le BIOS de notre serveur.

Nous devons disposer d'un minimum de 1Go de mémoire vive, mais il est conseillé d'avoir plus de 2Go afin de pourvoir virtualiser plusieurs machines.

Il est aussi vivement recommandé d'activer le DEP (Data Execution Prevention) afin de sécuriser au maximum les données. Cette fonctionnalité empêche l'exécution de code depuis des blocs de mémoire contenant des données, un hacker accédant à une VM pourrait créer un Buffer overflows. Pour cette fonctionnalité, vous devez avoir Intel-Xd ou AMD-NX d'activé.

Pour vérifier les caractéristiques du processeur nous pouvons utiliser l'utilitaire gratuit CPU-Z disponible sur www.cpuid.com/cpuz.php



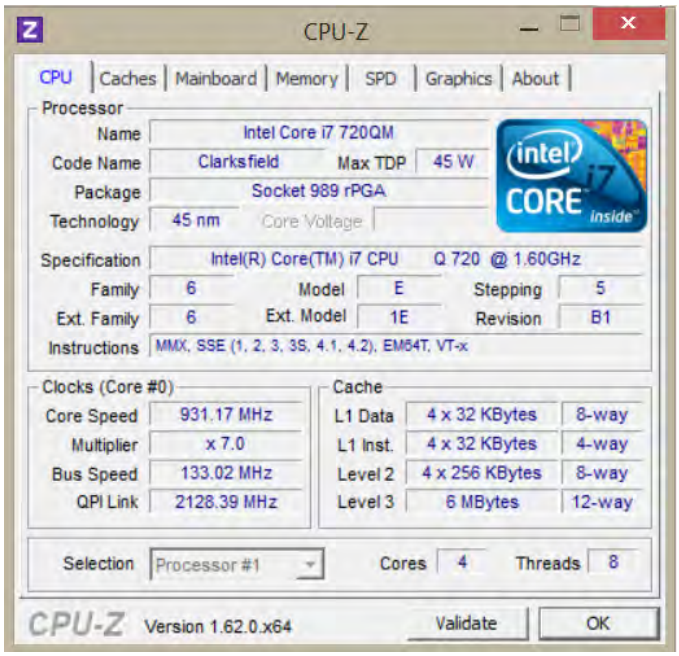


Image IV.1.1 : Vue du CPU sous VMWARE - **Image IV.1.2: Vue du CPU sous la machine hôte**

Nous constatons effectivement dans les instructions qu'Intel-Vt est absent dans le système sous VMware, bien qu'étant présente sur notre machine hôte. Pour ainsi activer cette instruction, nous mettons sous tension notre système, puis dans la configuration de la machine virtuelle VMware, dans la section Processors, nous cochons la case ***Virtualize Intel VT-x/EPT or AMD-V/RVI et Virtualize CPU performance counters :***

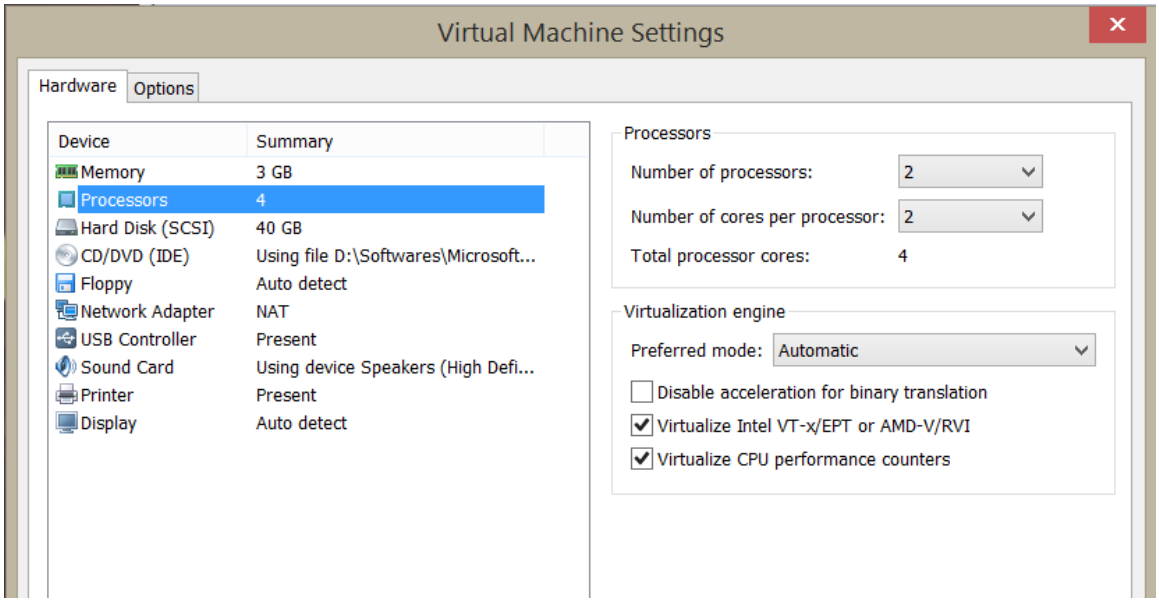


Image IV.1.3 : Paramètres de la machine virtuelle

N.B : Pour un système physique sur lequel on souhaite installer, l'instruction est à activer dans le BIOS

Après avoir démarré notre système, nous pouvons vérifier que notre système supporte bien la virtualisation avec l'apparition de l'instruction VT-X :

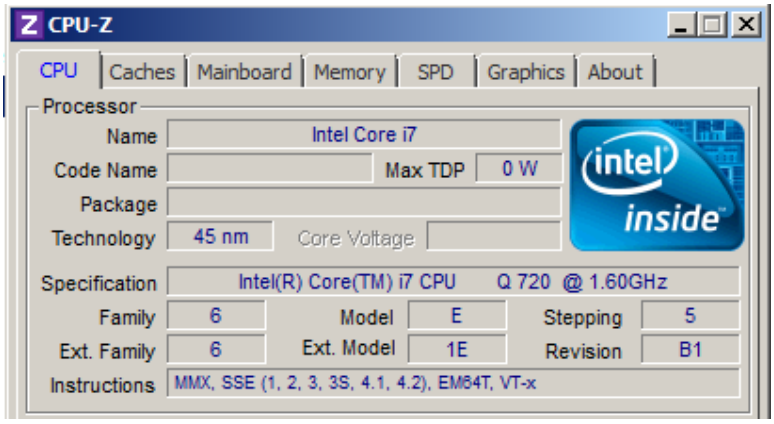


Image IV.1.3 : Vue du CPU avec l'instruction VT-x

Avant d'installer Hyper-V, nous allons nous basé sur le Guide de sécurité Hyper-V (disponible en téléchargement gratuit sur http://www.microsoft.com/en-us/download/details.aspx?id=16650). On trouve dans ce guide que nous résumerons dans la suite de notre projet :

- Comment installer et configurer le rôle Hyper-V en renforçant la sécurité ;
- Comment déléguer la gestion des machines virtuelles ;
- Comment protéger les machines virtuelles

V.2 Installation & configuration du rôle en renforçant la sécurité

Il existe deux catégories de contre-mesures:

V.2.1 Gestion de la sécurité du système d'exploitation

Lors de la configuration de l'ordinateur physique, vous pouvez faire plusieurs choses pour augmenter la sécurité globale du système d'exploitation de gestion et des machines virtuelles. Par exemple, vous pouvez réduire la surface d'attaque du système d'exploitation de gestion par l'installation de Hyper-V sur un ordinateur qui exécute Windows Server 2008 Server Core. Autres techniques, que vous pouvez utiliser comprennent l'installation de cartes réseau distinctes pour le système d'exploitation de gestion et pour les ordinateurs virtuels, et l'utilisation du système d'exploitation de gestion pour configurer les volumes de stockage logiques distincts pour chaque ordinateur virtuel.

➔ Mise à jour de l'OS

Toujours, pour nous assurer que le système d'exploitation n'a pas de failles exploitables connues, nous profitons tout d'abord des dernières mises à jour et patches, disponibles dans Windows Update :

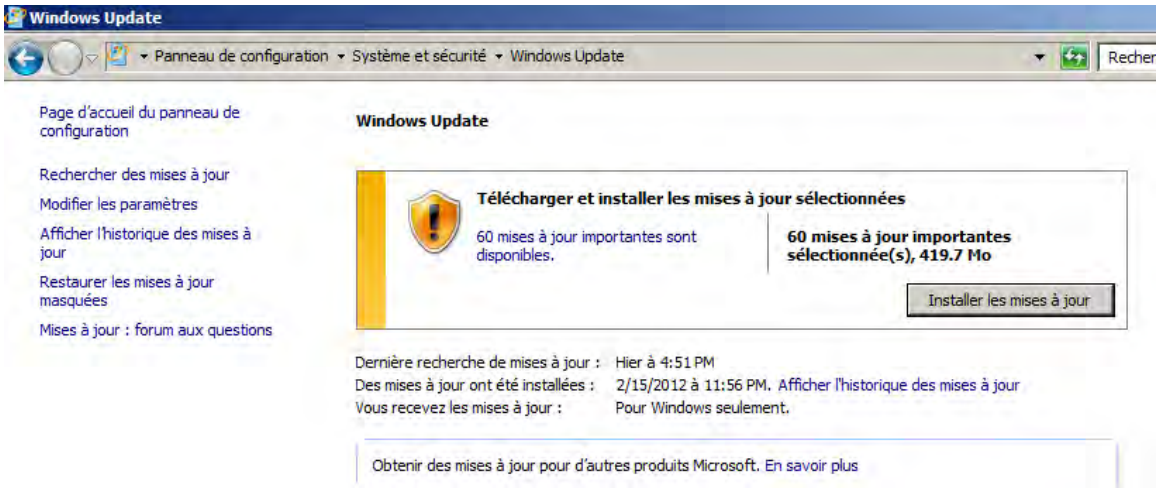


Image V.2.1.1: Windows Update

Dans le cas des hyperviseurs monolithiques comme VMware ESX qui sont annoncés pour leurs traits de performance, ils sont parfois sujets à des problèmes d'instabilité en raison des pilotes de périphériques incorporés directement dans leurs couches de fonctionnalité. Ce que cela signifie est que si un pilote est frappé par une mise à jour, bug ou faille de sécurité, l'ensemble de l'architecture virtuelle au sein de cette machine physique sera compromise.

En parlant de sécurité, il se trouve être l'un des défis les plus pressants de VMware à ce jour. La société fournit un accès à la plate-forme d'exploitation dans ses produits hyperviseur via des API, ce qui, malheureusement, rend possible pour les auteurs de logiciels malveillants d'insérer du code malveillant et de compromettre tous les environnements virtuels sur la machine physique. VMware a été mis en demeure grave lorsque le code source confidentielle de son hyperviseur ESX a été exposé[11] par des pirates.

Alors que les produits Microsoft sont associés à une longue histoire de problèmes de sécurité, la sécurité se trouve être l'un des plus forts arguments de vente de Hyper V. Parce que le « microkernelizé » n'autorise pas l'accès à l'API de la couche hyperviseur, les pirates ne peuvent pas compromettre une machine complète en intégrant un seul morceau de code malveillant. Ils doivent plutôt tenter de compromettre chaque machine virtuelle sur une base individuelle.

[11] Source : **VMware Source Code Leak Reveals Virtualization Security Concerns** – 3 mai 2012 - http://www.serverwatch.com/server-trends/vmware-source-code-leak-reveals-virtualization-security-concerns.html

Hyper V est également moins vulnérable aux problèmes de stabilité. Dès lors que les pilotes de périphériques sont en cours d'exécution au niveau virtuel, les mises à jour, bugs, ou autres problèmes potentiels liés aux pilotes ne peuvent affecter les machines virtuelles individuelles. Comme résultat, les risques que l'ensemble de l'infrastructure virtuelle soit affecté par les problèmes de stabilité d'une seule machine virtuelle sont considérablement réduits.

Mais tout comme le produit monolithique de VMware, la conception "microkernelizé" apporte à Hyper V certains inconvénients notables. Hyper V nécessite qu'un système d'exploitation soit installé pour que l'hyperviseur puisse fournir un accès matériel à tous les autres systèmes d'exploitation invités. Cette configuration laisse toute l'architecture virtuelle vulnérable aux temps d'arrêt. Par exemple, si le système d'exploitation crashe pour une raison quelconque, tous les systèmes d'exploitation invités et leurs machines virtuelles vont couler avec le navire.

Il serait donc prudent pour limiter les impacts, de désactiver les mises à jour automatique et appliquer celles-ci que pendant une heure de non-production.

➔ AJOUT DU RÔLE

À partir du gestionnaire du serveur, cliquons sur **Ajouter des rôles**. Dans la boite de dialogue qui apparait, dans la section **Rôles de serveurs**, cochons la case Hyper-V puis cliquons sur Suivant :

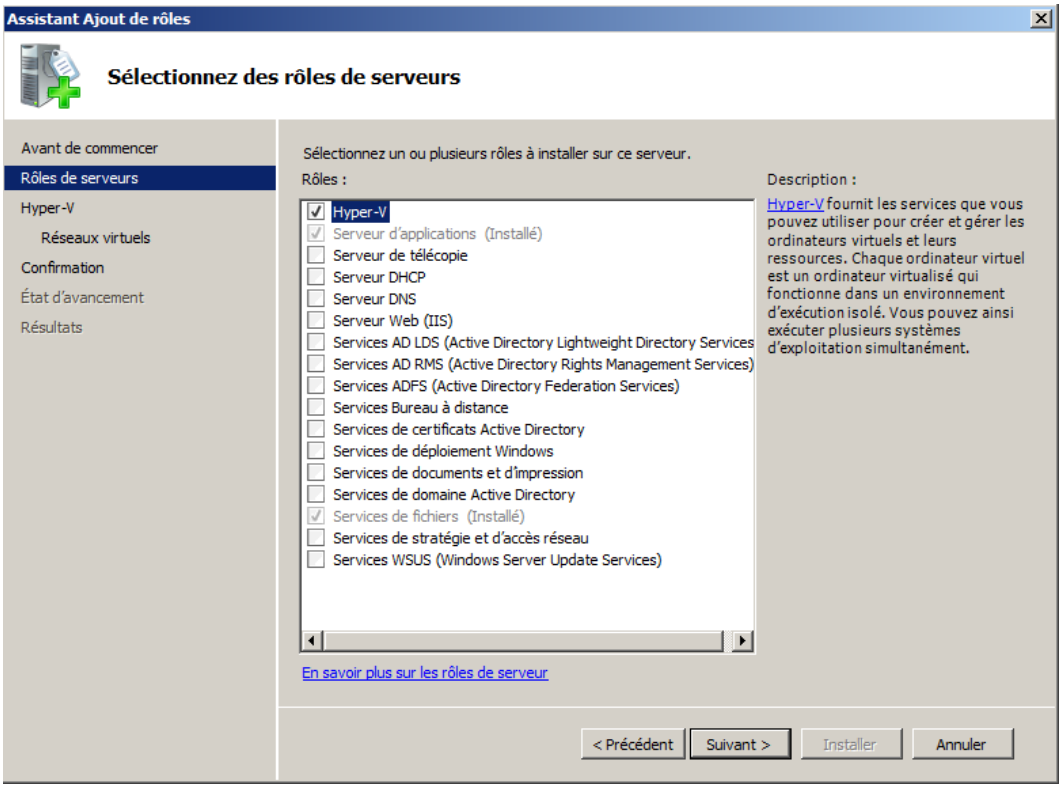


Image V.2.1.2: Ajout du rôle Hyper-V

Nous arrivons à la page Hyper-V. Sur celle-ci nous pouvons accéder à des informations concernant le rôle Hyper-V. Une fois ces informations lues, cliquons sur Suivant.

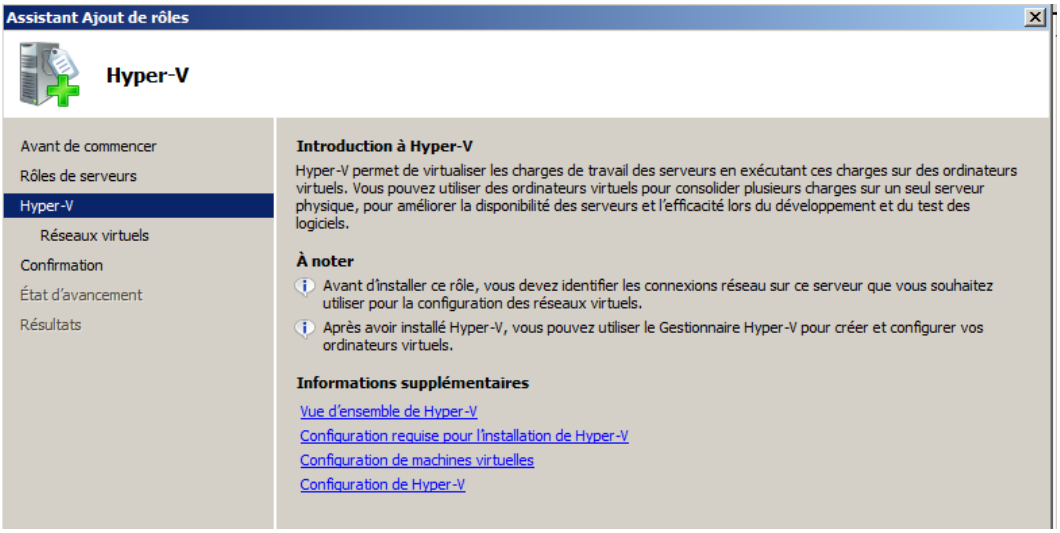


Image V.2.1.3: Introduction à Hyper-V

Sur cette page nous pouvons dès à présent créer notre réseau virtuel. Si on sélectionne notre carte réseau comme sur la capture d'écran ci-dessous, nous créons un réseau virtuel qui permettra notamment de faire communiquer notre machine hôte avec nos machines virtuelles. En fait à ce niveau, Hyper-V va virtualiser notre carte réseau pour pouvoir faire un réseau virtuel.

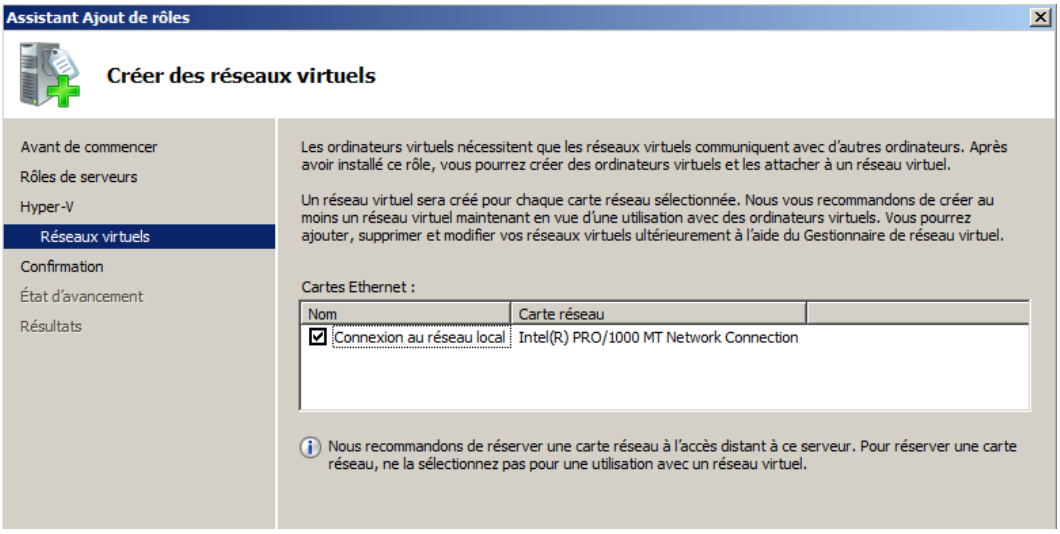


Image V.2.1.4: Création de réseaux virtuels

Sur la page de confirmation, nous voyons les informations sur l'installation avant que celle-ci ne soit faite. Si tout nous convient, cliquons sur ***Installer***.

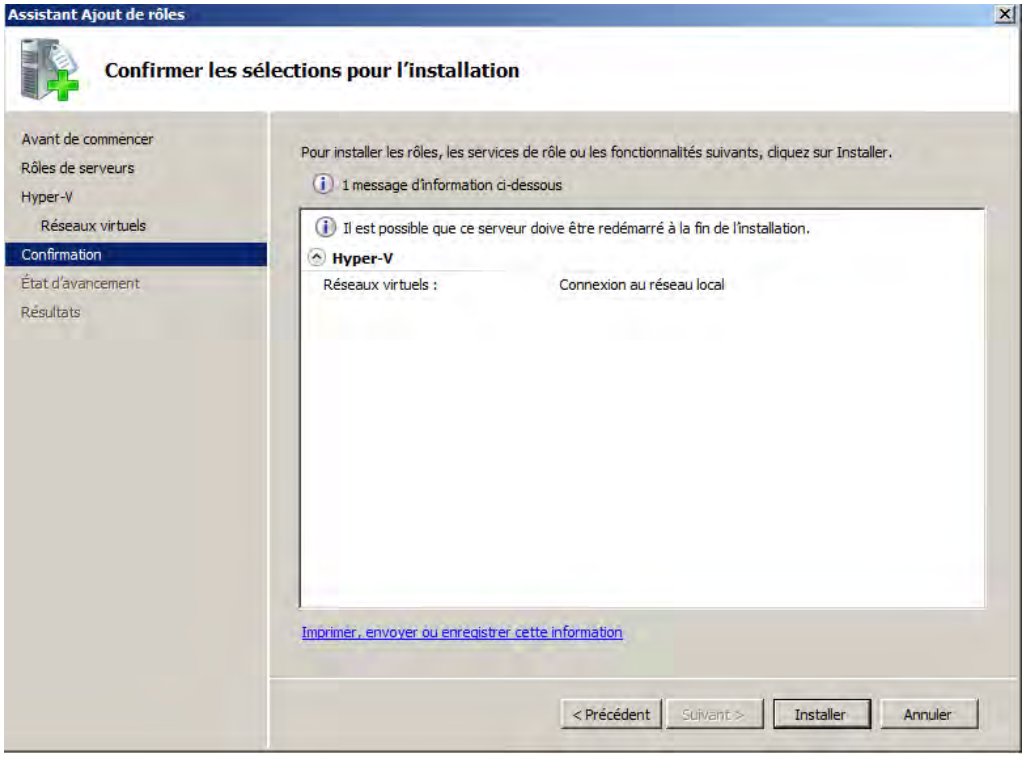


Image V.2.1.5: Confirmation de l'ajout du rôle

L'installation commence, nous patientions donc que celle-ci se termine :

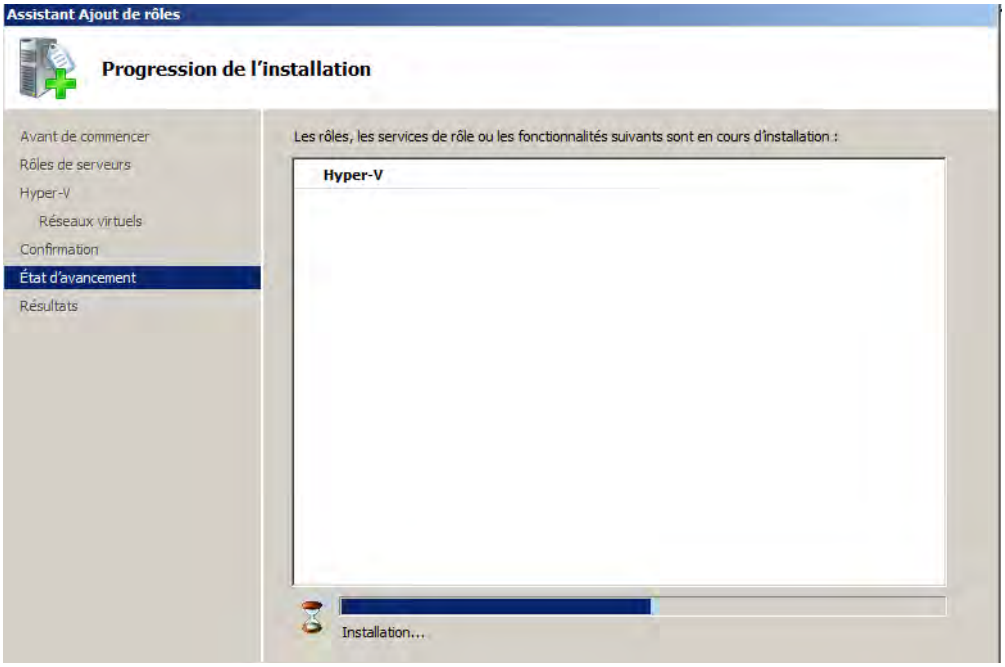


Image V.2.1.6: Progression de l'installation

Une fois l'installation terminée, nous devons impérativement redémarrer notre machine pour la prise en compte de l'ajout du rôle. Donc cliquons sur ***Fermer :***

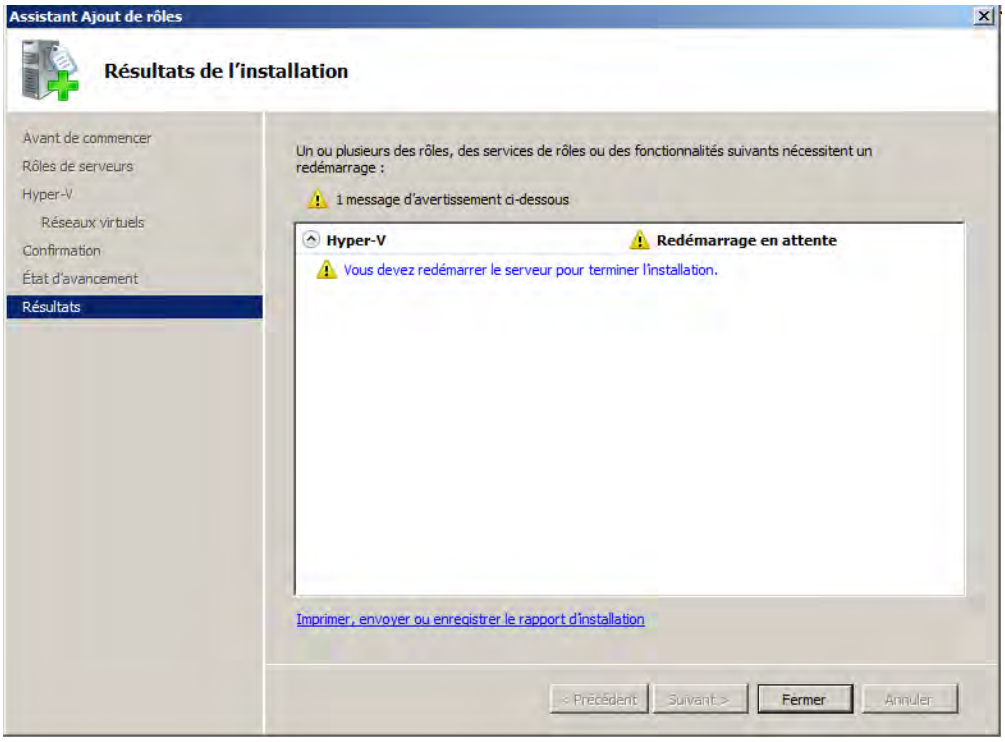


Image V.2.1.7: Résultats de l'installation

Il reste ensuite à confirmer le redémarrage en client sur ***Oui***, sur le prompt qui apparait

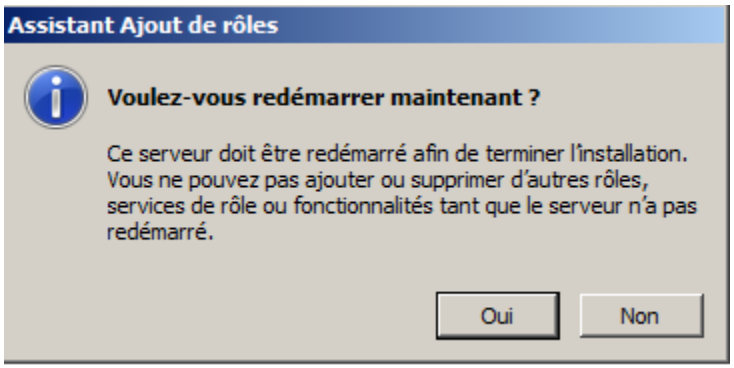


Image V.2.1.8: Prompt de redémarrage à la fin de l'installation

Après le redémarrage du système, notre serveur reprend la configuration d'Hyper-V

Une fois la configuration terminée, le serveur va nous indiquer que l'installation est terminée et que nous pouvons dès à présent utiliser Hyper-V. Cliquez sur Fermer

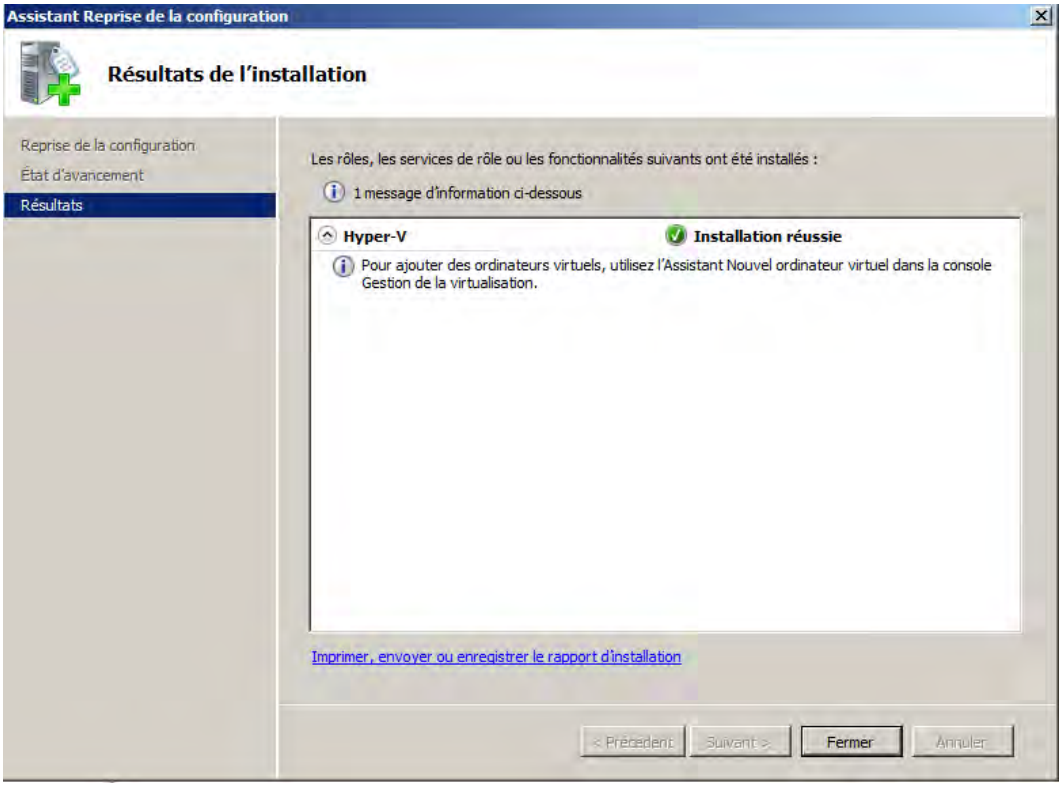


Image V.2.1.9: Installation réussie

Pour accéder au rôle Hyper-V, il nous suffit d'ouvrir le Gestionnaire d'Hyper-V disponible à partir du menu Démarrer ou à partir du gestionnaire du serveur.

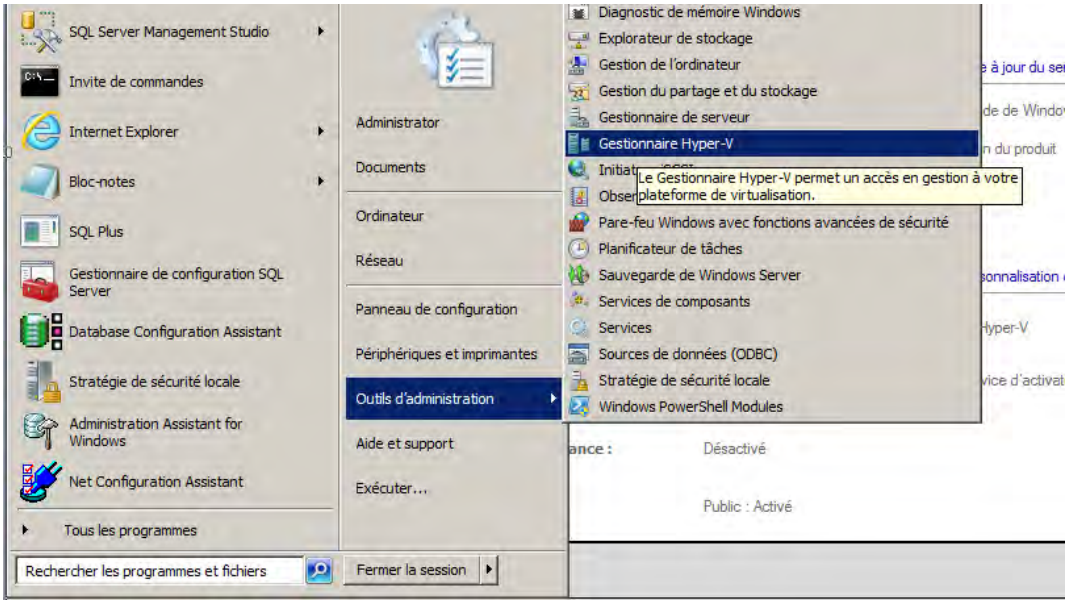


Image V.2.1.10: Lancement du Gestionnaire Hyper-V à partir du menu Démarrer

Nous accédons ainsi Gestionnaire Hyper-V où nous pourrons créer nos machines virtuelles, nos réseaux virtuels… Le Gestionnaire se présente comme ci-dessous :

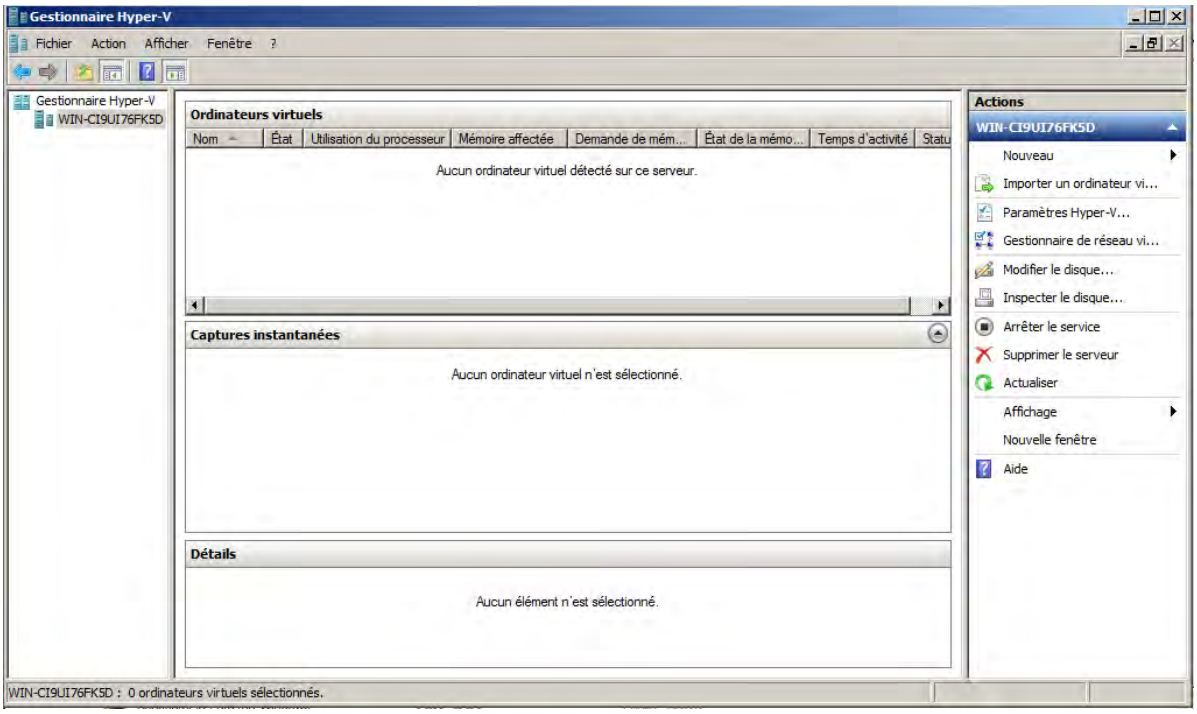


Image V.2.1.11: Fenêtre du Gestionnaire Hyper-V

Création d'un réseau virtuel

La configuration des interfaces réseau physiques de l'ordinateur exécutant Hyper-V peut contribuer à améliorer l'isolation du système d'exploitation de gestion des autres machines virtuelles. Microsoft recommande d'installer au moins deux cartes réseau sur l'ordinateur qui héberge Hyper-V. Dédier la première carte réseau pour l'usage exclusif du système d'exploitation de gestion et ensuite laisser les autres ordinateurs virtuels à utiliser les autres cartes réseau. La figure suivante illustre ce concept.

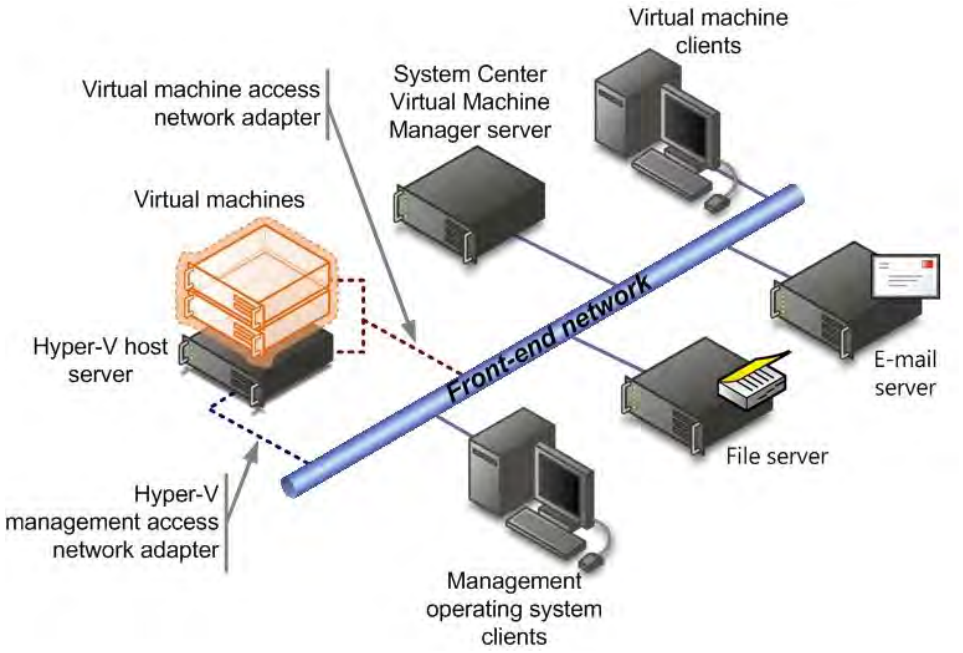


Image V.2.1.12: Architecture physique dans le réseau d'une entreprise

Avant la création de notre machine virtuelle, nous pouvons créer un réseau virtuel. Dans le volet droit, sous Actions, cliquons sur Gestionnaire de réseau virtuel

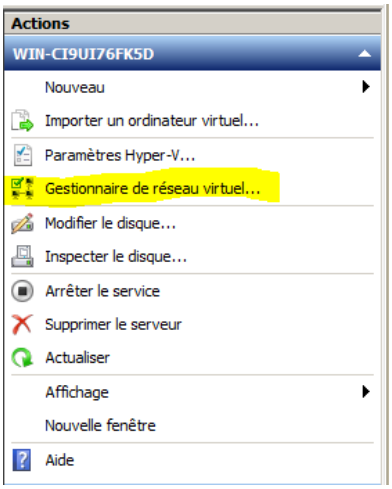


Image V.2.1.13: Menu Actions

Pour la création, nous avons trois choix possibles, à savoir :

- ✓ **Externe**

Crée une connexion à une carte réseau physique, de façon à ce que des ordinateurs virtuels puissent accéder à un réseau physique.

Le paramètre **Autoriser le système d'exploitation de gestion à partager cette carte réseau** contrôle si vous pouvez utiliser cette carte réseau physique pour accéder au système d'exploitation de gestion, qui est le système d'exploitation exécutant le rôle Hyper-V. Vous pouvez utiliser cette option pour isoler le système d'exploitation de gestion des communications entre les ordinateurs virtuels et les autres ordinateurs sur un réseau physique. Cependant, cela signifie également que vous ne pouvez pas vous connecter à distance au système d'exploitation de gestion via cette carte réseau si cette option est désactivée.

- ✓ **Interne**

Fournit des communications entre le système d'exploitation de gestion et des ordinateurs virtuels.

- ✓ **Privé**

Fournit des communications entre des ordinateurs virtuels uniquement.

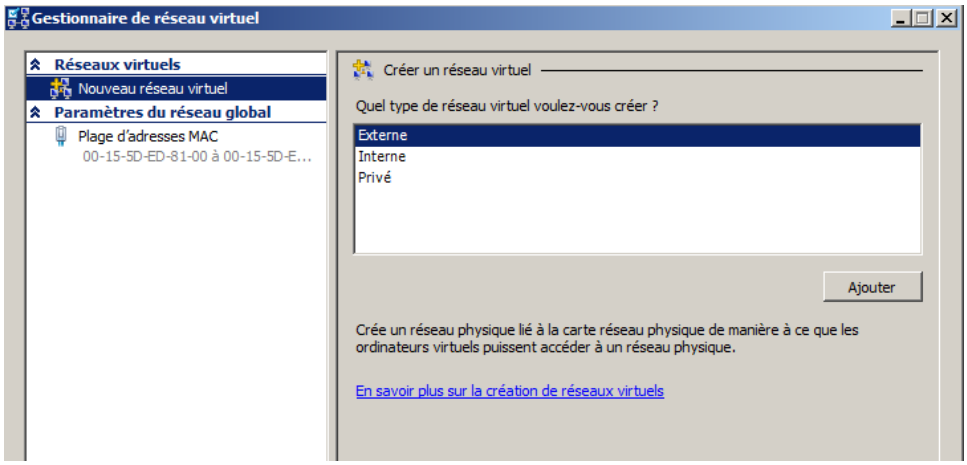


Image V.2.1.14: Gestionnaire de réseau virtuel

Après avoir cliqué sur le bouton **Ajouter**, nous pouvons personnaliser notre réseau créé comme suit:

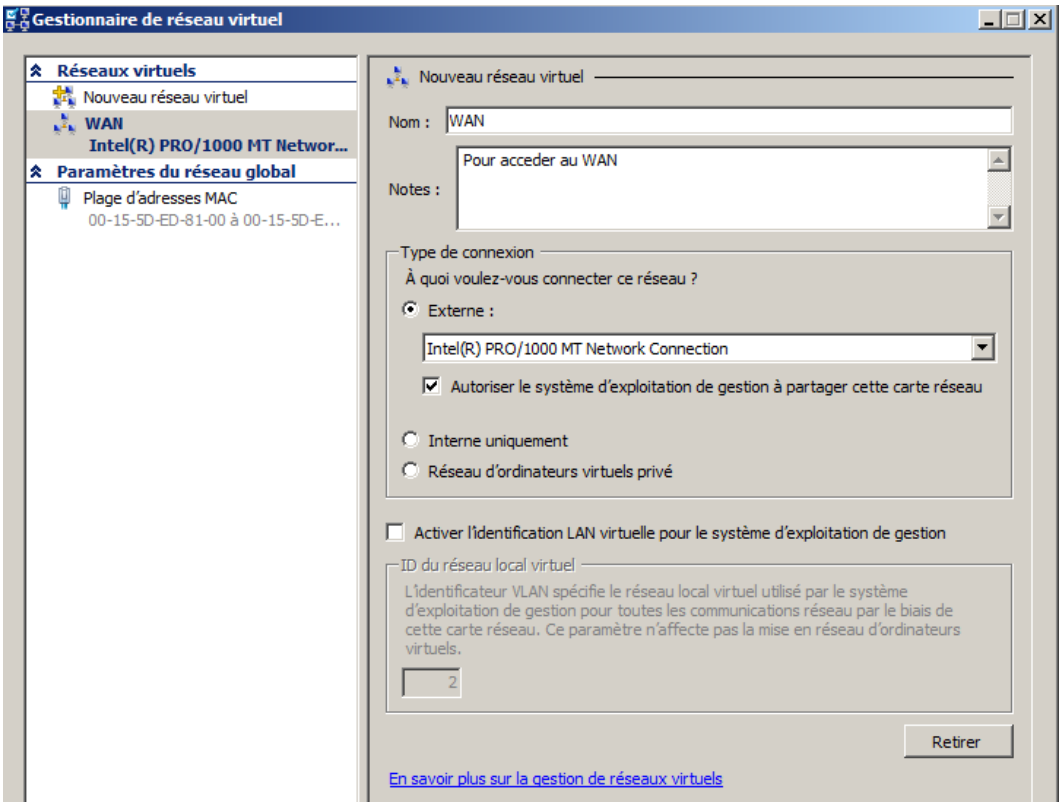


Image V.2.1.15: Personnalisation du réseau virtuel créé

Sécurisation des périphériques de stockage dédiés

Les fichiers qui contiennent des informations de configuration sur chaque ordinateur virtuel sont stockés par défaut dans le répertoire **%programdata%\Microsoft\Windows\Hyper-V**. Les fichiers de configuration d'ordinateur virtuels stockés dans ce répertoire sont relativement petits, et l'emplacement de stockage par défaut devrait être acceptable pour de nombreux scénarios.

N.B. : Si vous spécifiez un emplacement de stockage différent, assurez-vous que le compte Système et le groupe administrateurs ont des autorisations de contrôle total pour le nouveau dossier, et que l'accès par les autres comptes est strictement limité au besoin.

Commençons par les disques durs virtuels. Les disques virtuels sont un ensemble de fichiers qui vont représenter les disques durs de vos machines virtuelles.

- Pour en créer un nouveau, dans le volet Action allez dans « Nouveau» / « Disque dur… »

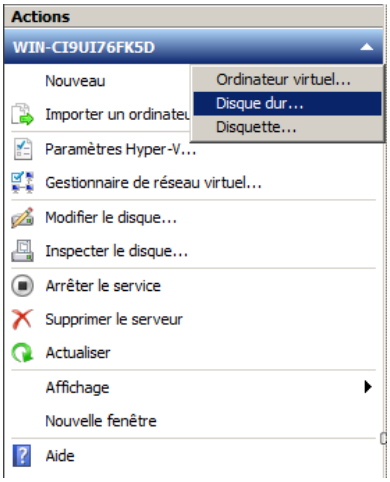


Image V.2.1.16: Création de Disque dur à partir du menu actions

- Cliquons sur « Suivant» :

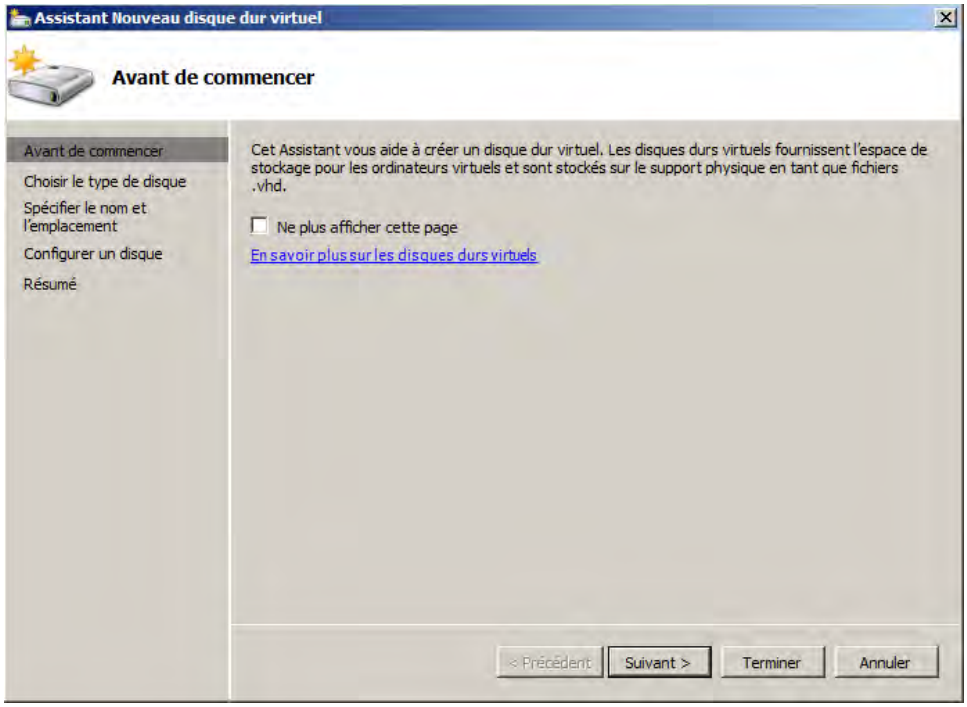


Image V.2.1.17: Boite de dialogue de l'assistant Nouveau disque dur virtuel

- Choisissons ensuite le type de votre disque dur. Nous avons trois choix possible :

✓ **Taille fixe** : Votre disque virtuel aura une taille fixe qui n'évoluera pas. Il prendra donc plus de place, mais sera plus performant.

✓ **Extension dynamique**: la taille réelle que prendra le disque virtuel évoluera en fonction des fichiers stockés dessus, jusqu'à sa limite. Si nous précisons une taille maximum de 127 Giga et que notre VM n'a que 8 Giga de données sur ce disque, alors notre .vhd n'utilisera que 8 Giga sur le disque dur physique (et non 127).

Note : Bien que votre disque grossit en fonction des données stockées dessus, il ne peut pas se réduire automatiquement si vous effacez des données.

✓ **Différentiation** : Ce type de disque est associé à un autre disque que vous voulez garder intacte. En utilisant ce type de disque, si vous effectuez des modifications qui ont des effets non attendu, vous pouvez facilement revenir à l'état précédent (en revenant à l'état du premier disque).

Image V.2.1.18: Choix du type de disque

- Une fois le type de disque choisi, entrons le nom du disque ainsi que le chemin où il sera stocké.

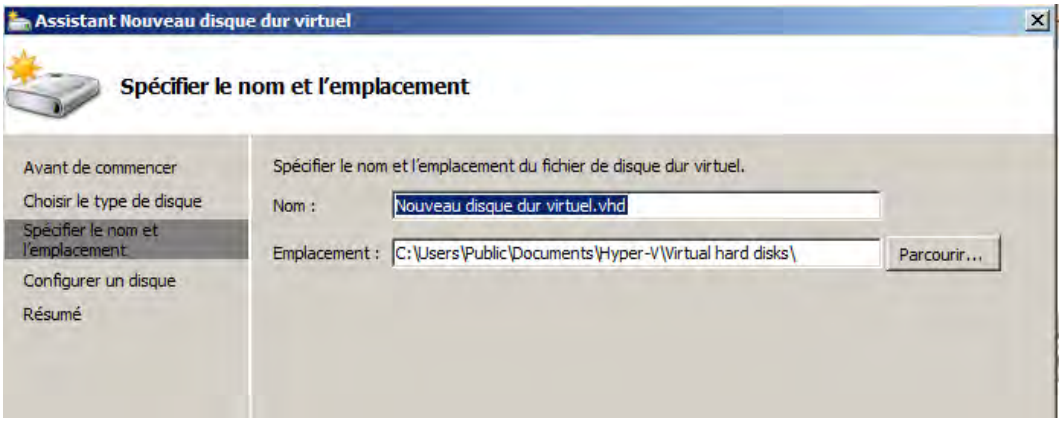


Image V.2.1.19: Spécification du nom et de l'emplacement du disque

- Pour terminer, entrons la taille du disque dur virtuel (maximum ou fixe selon le type choisi). Nous pouvons aussi choisir de copier un disque existant. Dans le cas où nous aurions choisi un disque de type « Différentiation », nous devons simplement préciser le disque de référence.

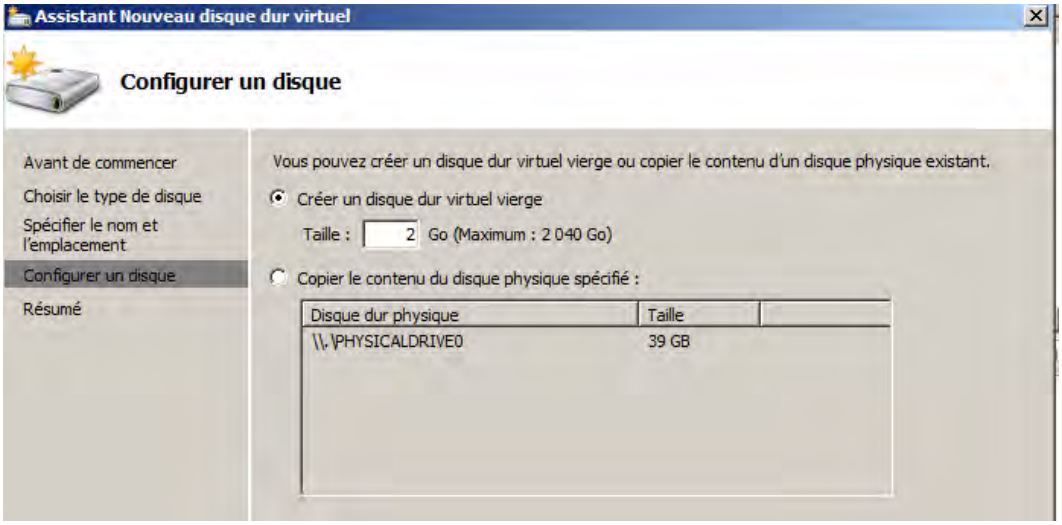


Image V.2.1.20: Configuration du disque

- Cliquons sur « Terminer » pour créer le disque.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

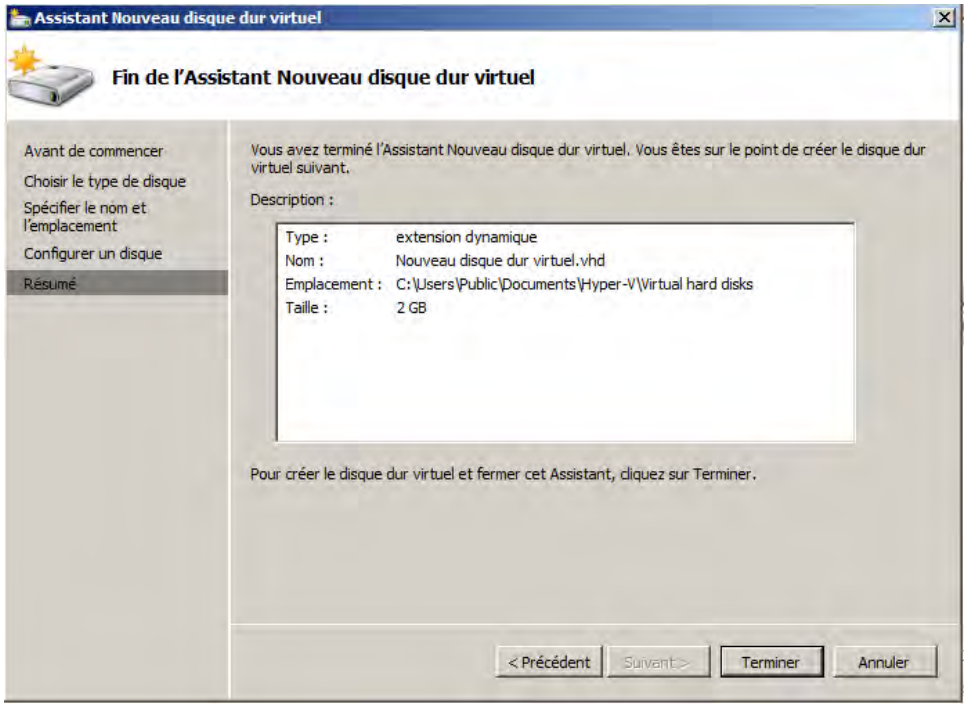


Image V.2.1.21: Fin de l'assistant

Nous savons maintenant créer un disque virtuel. Il y a deux autres actions disponibles pour ces disques : Modifier et Inspecter le disque..(Visibles dans le menu Actions):

La première, « Inspecter le disque », nous donne simplement un résumé de notre disque virtuel : lieu de stockage, nom du fichier, taille …

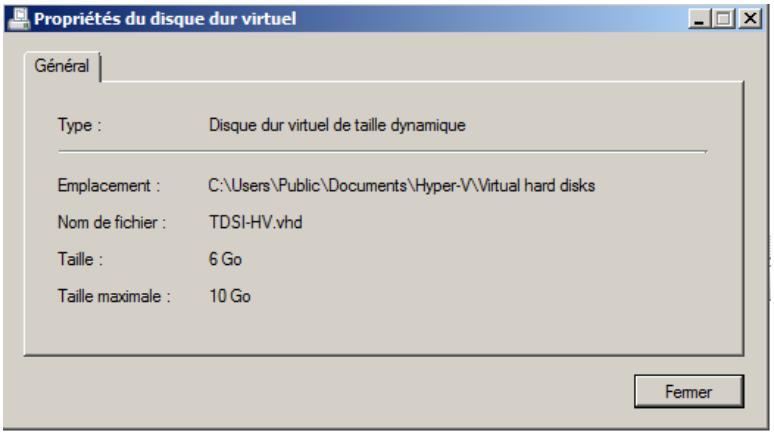


Image V.2.1.22: Propriétés du disque dur virtuel

La deuxième est plus intéressante. En allant dans « Modifier le disque », vous pouvez effectuer trois actions :

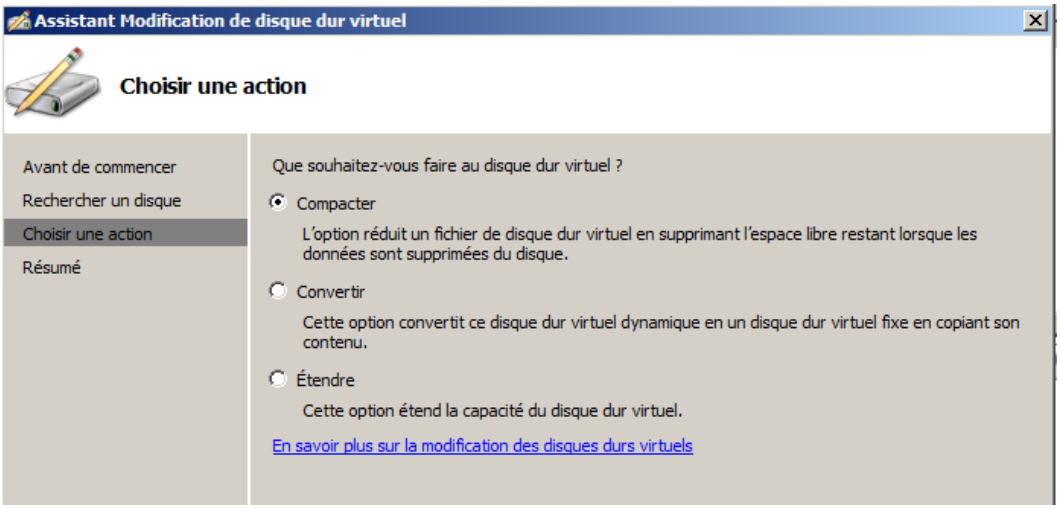


Image V.2.1.23: Assistant modification de disque dur virtuel

- ✓ Compacter : nous permet de réduire la taille de votre disque en supprimant les espaces vide laissés lors de la suppression de données (seulement pour les disques Extension dynamique)
- ✓ Convertir : nous permet de convertir un disque dynamique en disque à taille fixe ou inversement.
- ✓ Étendre : nous permet d'augmenter la taille de votre disque virtuel.

V.2.2 SÉCURITÉ DE LA MACHINE VIRTUELLE

Plusieurs paramètres de la machine virtuelle ont des répercussions sur la sécurité. Nous pouvons configurer certains de ces paramètres à l'aide de l'Assistant de la Machine virtuelle, et nous pouvons accéder à tous les paramètres après avoir créé un ordinateur virtuel via le Gestionnaire Hyper-V.

Configuration de la Machine virtuelle

Les considérations et les recommandations suivantes portent sur la configuration des machines virtuelles sur un ordinateur qui exécute Windows Server 2008 Hyper-V.

- **Déterminer** où stocker les fichiers de la machine virtuelle et les disques durs virtuels. Voir plus haut dans la section Sécurisation des périphériques de stockage dédié.
- **Décider** combien de mémoire à attribuer à une machine virtuelle. La mémoire sur l'ordinateur physique est attribuée à tous les ordinateurs virtuels sur le serveur, y compris l'ordinateur virtuel exécutant le système d'exploitation de gestion, le fait d'attribuer une quantité appropriée de mémoire à chaque machine virtuelle est donc important pour s'assurer de la disponibilité permanente de toutes les ressources des VMs. La quantité de mémoire à attribuer dépendra de la charge de travail de la machine virtuelle, de la quantité de mémoire physique disponible sur l'ordinateur et de la quantité de mémoire utilisée par les autres machines virtuelles fonctionnant sur le même ordinateur.
- **Imposer** des limites à l'utilisation du processeur. Par défaut, Hyper-V ne limite pas la quantité de puissance de traitement utilisée par les machines virtuelles. Une machine virtuelle compromise pouvant utiliser toute la puissance de traitement sur l'ordinateur physique pourrait rendre celui-ci et les autres VMs en cours très instables. Le nombre exact de processeurs logiques à utiliser et les limites qui vous devriez leur imposer

dépendra de la charge de travail effectué, du nombre de processeurs physiques et des noyaux installés sur l'ordinateur physique, et enfin de la puissance de processeur requise par d'autres machines virtuelles fonctionnant sur le même ordinateur. Pour garantir la disponibilité permanente de toutes les ressources de la VM, il faudra surveiller l'utilisation du processeur et ajuster les limites en conséquence.

- **Configurer** les périphériques de stockage uniquement requis pour un ordinateur virtuel. Donner à chaque VM un accès pour les disques durs physiques, disques durs virtuels et des périphériques de stockage amovibles dont il a besoin et rien d'autres. Si une machine virtuelle ne nécessite pas l'accès à une ressource comme un lecteur de CD/DVD, sauf lorsque vous installez le logiciel par exemple, on peut supprimer le lecteur virtuel ou sélectionner aucun comme média, lorsqu'il n'est pas en utilisation.
- **Activer** le support pour la synchronisation de l'heure. La synchronisation de l'heure peut être importante dans certains scénarios de vérification, parce que l'heure système des ordinateurs virtuels peut être en décalage avec le système d'exploitation de gestion pour les VMs qui sont sous forte charge constante. Pour la synchronisation de l'heure fonctionne, nous devons installer les Services d'intégration Hyper-V sur les ordinateurs virtuels.
- **Placer les machines virtuelles d'un niveau de confiance similaire sur le même ordinateur physique.** Pour maintenir la sécurité dans notre entreprise, nous déployons nos machines virtuelles de telle sorte que toutes les VMs sur un ordinateur physique donné partagent un niveau similaire de confiance, puis configurons l'ordinateur pour être au moins aussi sûr que la VM la plus sécurisé. Les VMs qui sont exposées à un accès externe, comme les serveurs Web, ou qui doivent être accessibles largement, nécessitent différentes mesures de sécurité que pour les serveurs dont l'accès est strictement contrôlé ou limité à un petit nombre d'utilisateurs.
- **Supprimer les VHD déclassés de haute sécurité**. Pour les machines virtuelles de haute sécurité contenant des informations sensibles, établir un processus de suppression sécurisée des fichiers VHD après le déclassement. Des outils tels que SDelete v 1.61, disponible en téléchargement sur Microsoft TechNet, peuvent contribuer à ce processus.
- **Rangez les fichiers de capture instantanée en toute sécurité**. Une capture instantanée est une image de "point dans le temps" de l'état d'une machine virtuelle dans lequel on peut retourner plus tard. Il est conceptuellement similaire au point de restauration système de Windows, ou aux « undos » disques utilisés par Virtual PC et Virtual Server. Stocker les clichés que vous créez avec leurs VHDs associés dans un emplacement aussi sécurisé.

Ajout d'une machine virtuelle

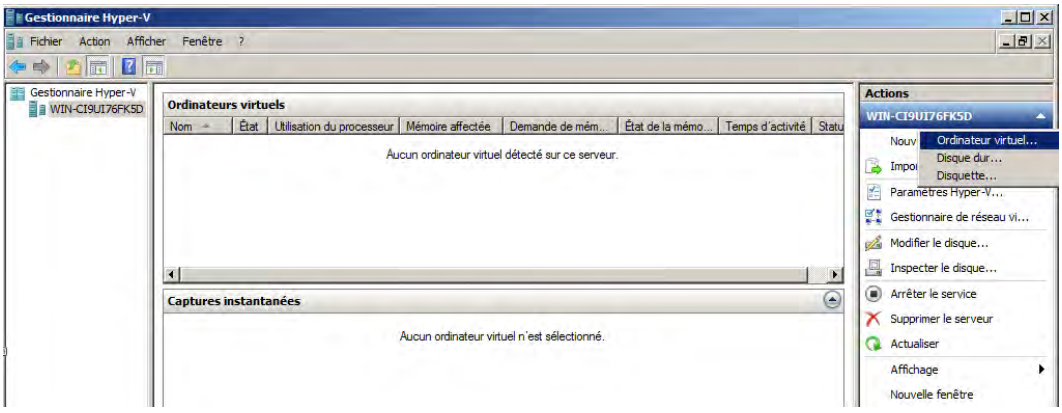


Image V.2.2.1: Ajout d'un ordinateur virtuel

On a le choix entre la création d'un ordinateur virtuel avec des valeurs par défaut et celle avec une configuration personnalisée.

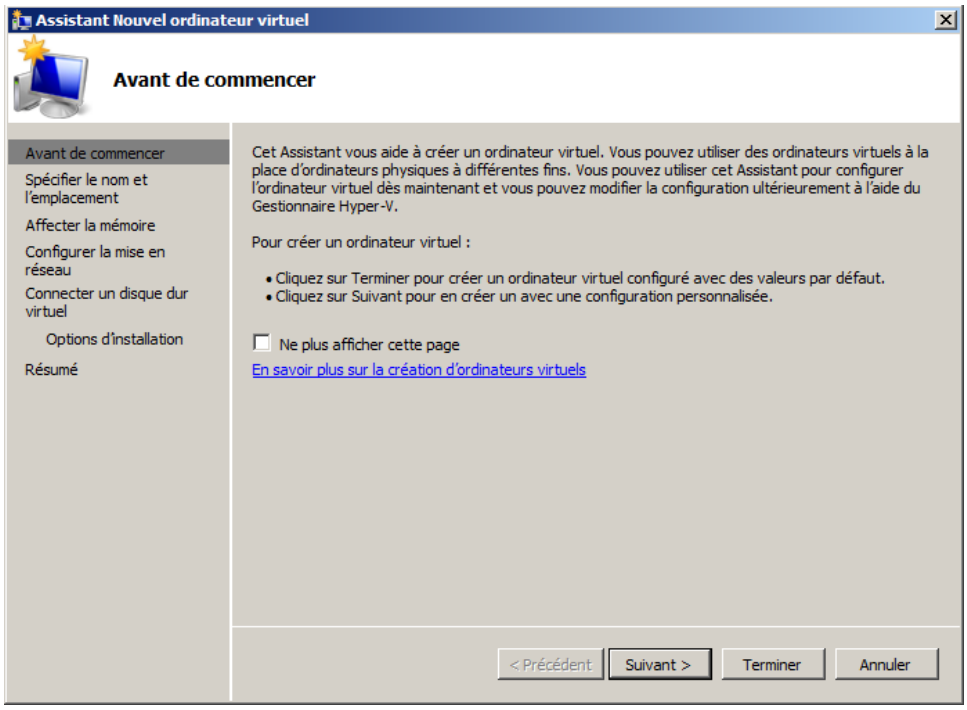


Image V.2.2.2: Page d'accueil de l'assistant

- **Choix du nom et de l'emplacement**

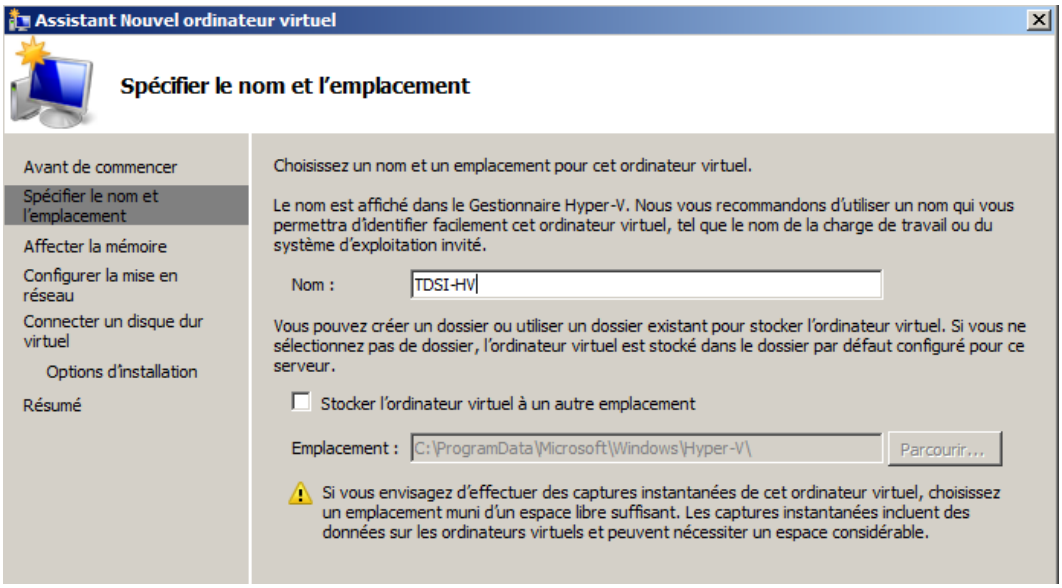


Image V.2.2.3: Spécification du nom et de l'emplacement

- **Affectation de la mémoire**

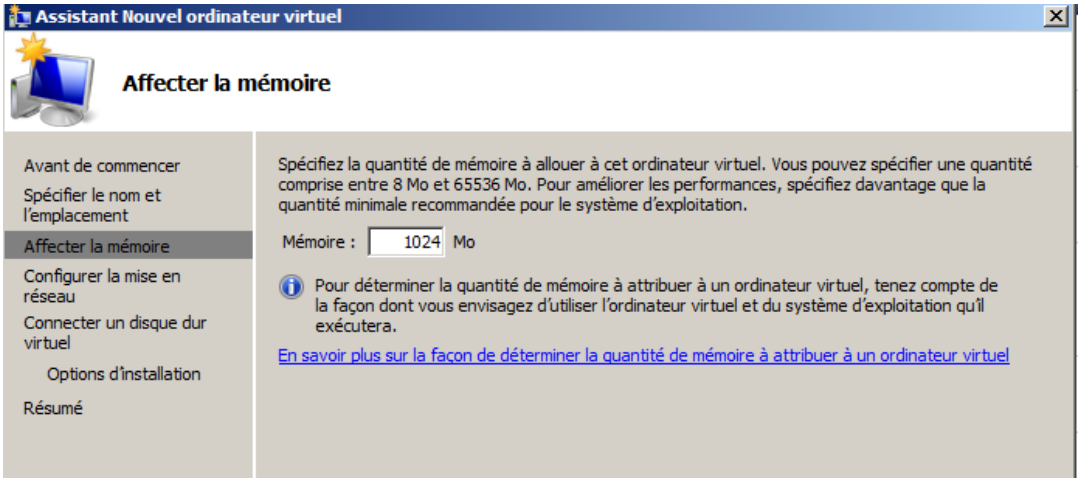


Image V.2.2.4: Affectation de la mémoire

- **Configuration de la mise en réseau**

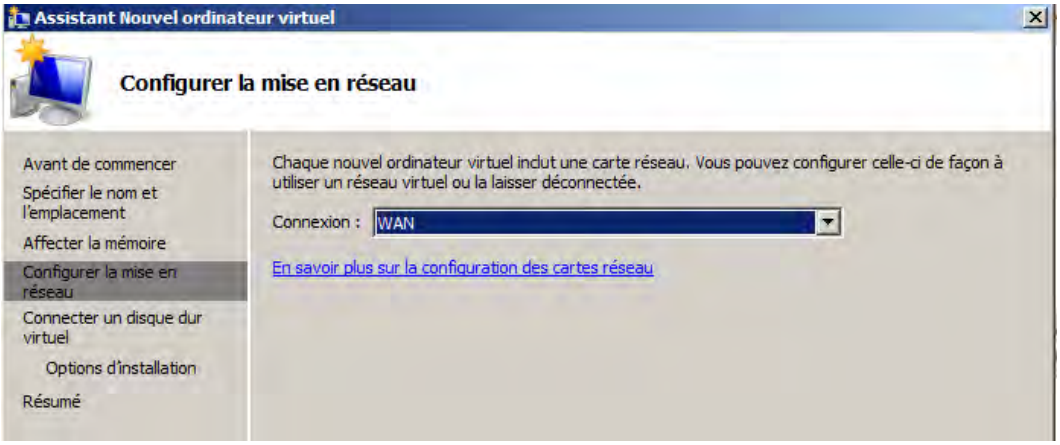


Image V.2.2.5: Configuration de la mise en réseau

- **Connexion d'un disque dur virtuel**

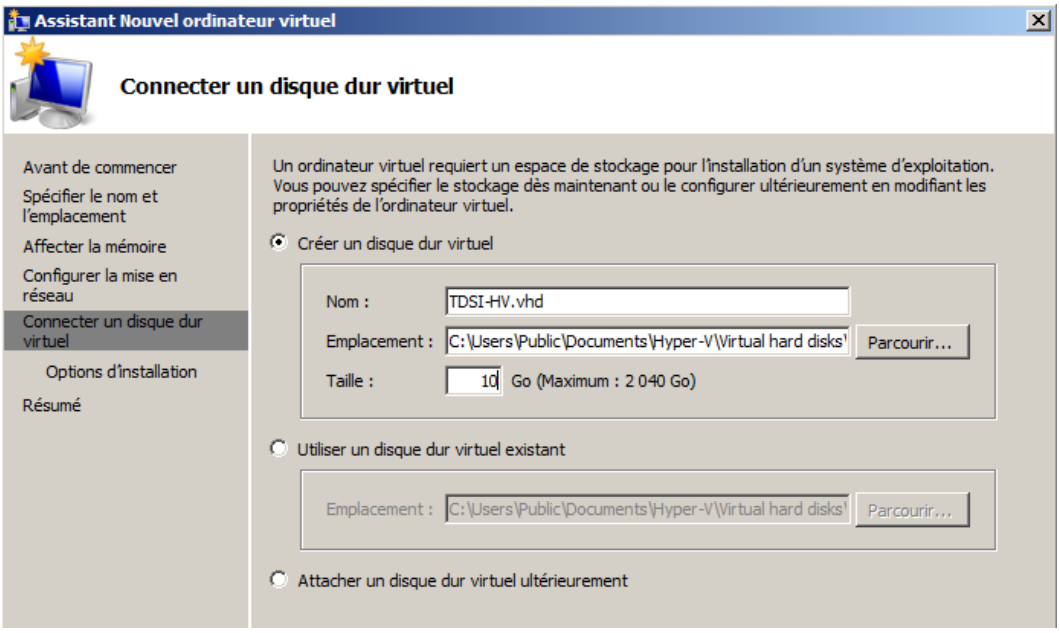


Image V.2.2.6: Connexion d'un disque dur virtuel

- **Option d'installation**

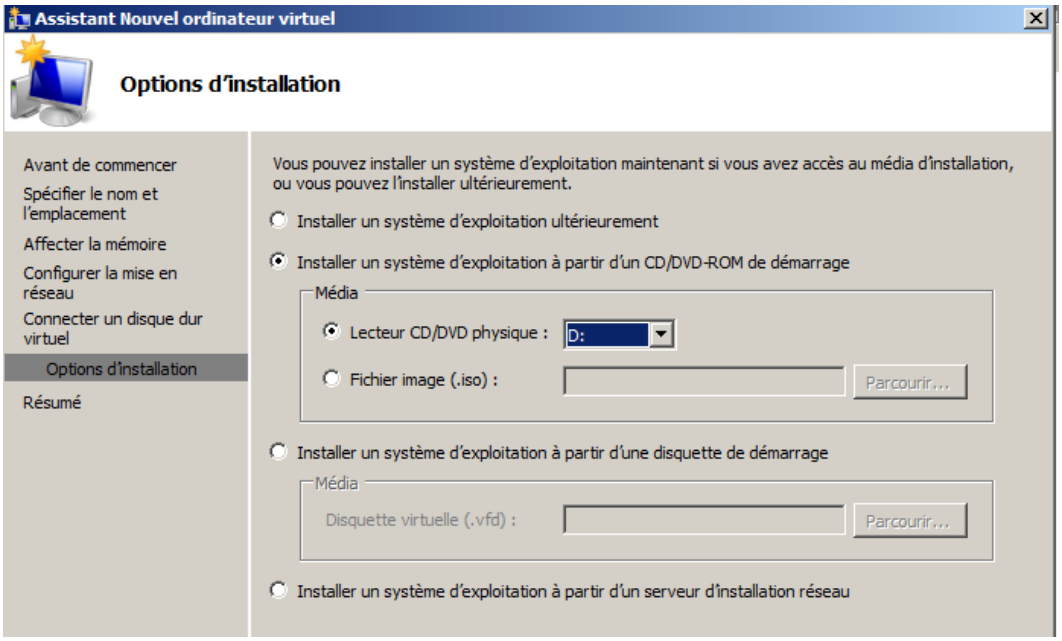


Image V.2.2.7: Option d'installation

- **Résumé de l'installation**

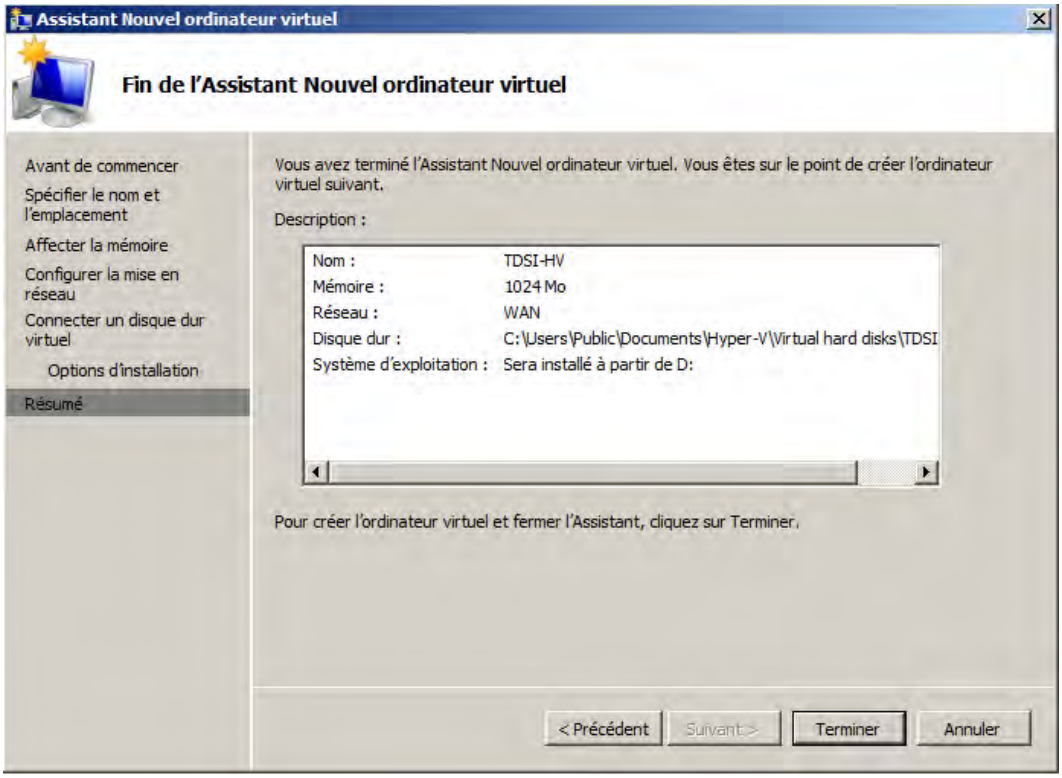


Image V.2.2.8: Fin de l'Assistant

À la fin, notre nouvel ordinateur virtuel apparait dans le gestionnaire d'Hyper-V :

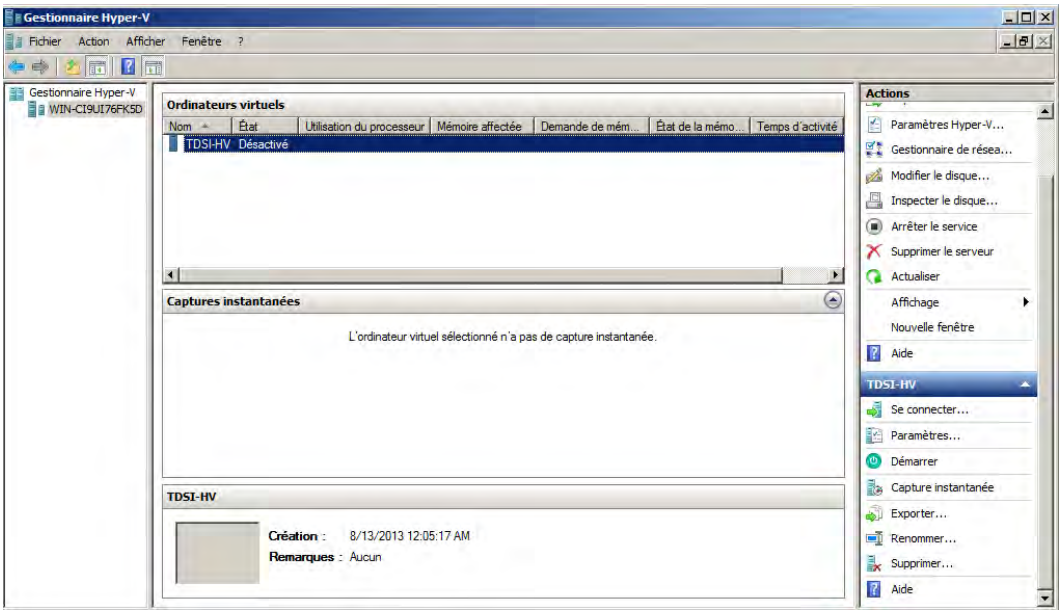


Image V.2.2.9: Option d'installation

VIRTUALISATION IMBRIQUÉE AVEC VMWARE

Lorsqu'on tente de démarrer la machine virtuelle nouvellement créée, on peut être confronté au message d'erreur suivant :

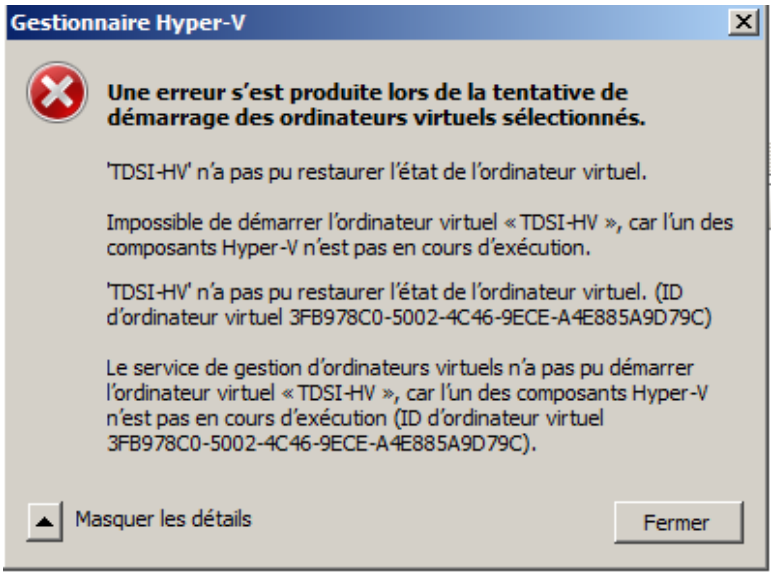


Image V.2.2.10: Message d'erreur

Ce message d'erreur survient généralement lorsqu'on essaie de créer une machine virtuelle sur une machine hôte aussi virtuelle. Pour remédier à cela, nous allons modifier le fichier de configuration de notre machine virtuelle Windows 2008 Server R2. Ce fichier se trouve dans l'emplacement de notre système. Exemple: ***C:\Users\SaMbA\Documents\Virtual Machines\Windows Server 2008 R2 x64***.

Mettons tout d'abord sous tension notre serveur puis modifions grâce à un éditeur (dans notre exemple Notepad++) le fichier de configuration **Windows 2008 Server x64.VMX** en ajoutant les trois lignes suivantes comme indiqué sur la capture:

hypervisor.cpuid.v0 = "FALSE" → Cette option va faire croire à Windows 2008 Server qu'il ne s'exécute pas en une instance virtualisée

vhv.enable = "TRUE" → Cette option permet la virtualisation imbriquée

mce.enable = "TRUE" → Cette option active Machine Check Exception (MCE), qui permettra à Windows 2008 Server de signaler des problèmes matériels CPU.

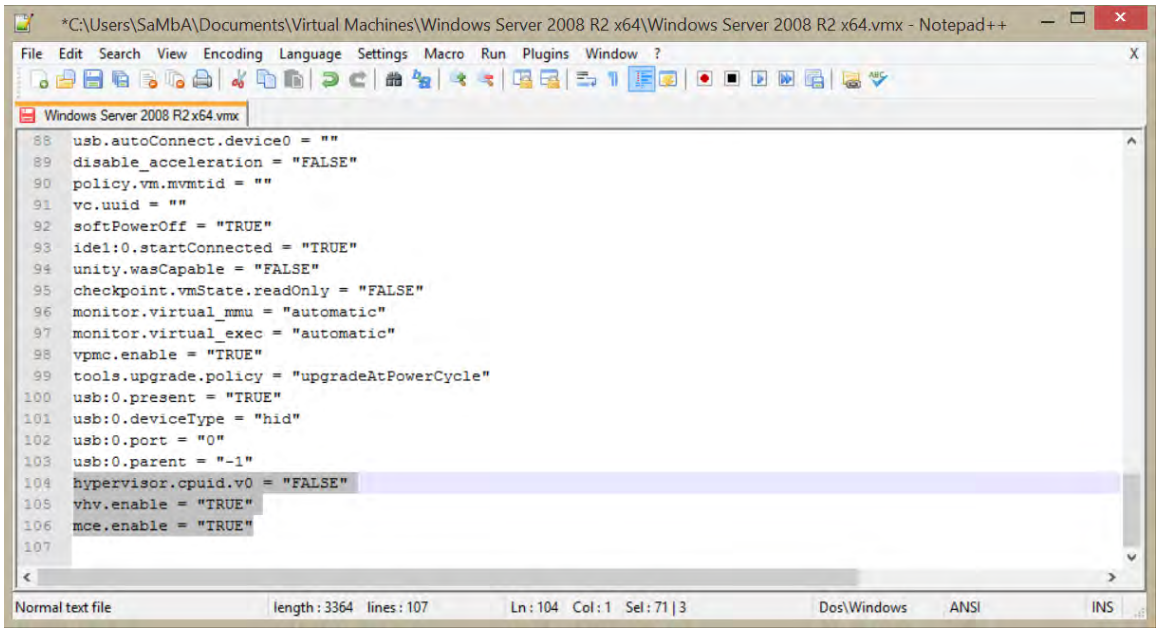


Image V.2.2.11: Édition du fichier de configuration

Après un nouveau démarrage du serveur, on peut à présent démarrer notre machine virtuelle :

Image V.2.2.12: Démarrage de la machine virtuelle

L'installation de la machine virtuelle se fait normalement, comme dans le cas d'une machine physique.

Actions de base

Les actions disponibles sur une VM se trouvent en bas à droite de la console Hyper-V. (ci-dessous, a gauche une VM éteinte et à droite une VM allumée).

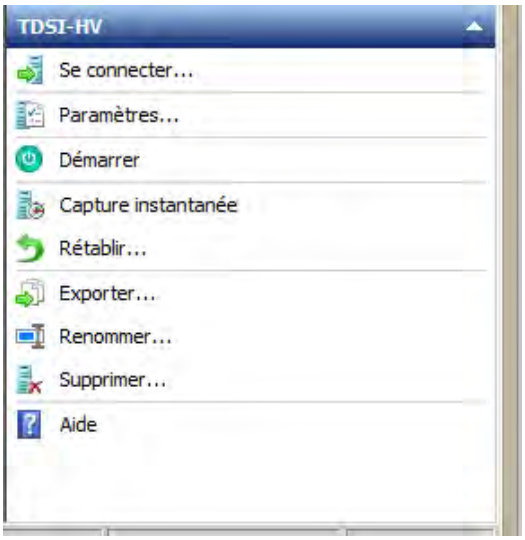


Image V.2.2.13: VM éteinte

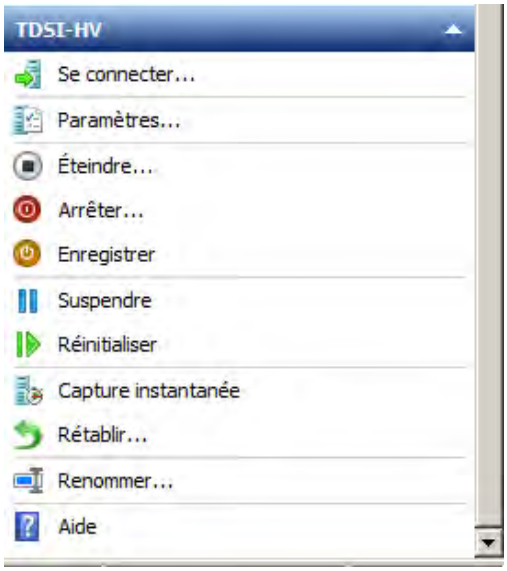


Image V.2.2.14: VM allumée

- **Se connecter** : nous permet de nous connecter à la machine virtuelle ;
- **Démarrer / Éteinte / Arrêter / Enregistrer** » vous permet de changer l'état de la machine :
  - ✓ Démarrer : la démarre.
  - ✓ Éteindre : l'éteint brutalement (comme si vous débranchiez la prise d'alimentation de la machine).
  - ✓ Arrêter : l'éteint correctement (comme si vous faisiez un « Démarrer/Arrêter l'ordinateur » sous Windows.
  - ✓ Enregistrer : met la VM en pause, c'est-à-dire qu'elle arrêtera de fonctionner mais redémarrera au même point que vous l'avez arrêté (les applications restent ouvertes).

N.B : Attention, il ne jamais mettre un DC en pause !!! Cela peut poser de gros problèmes au niveau de la réplication de l'AD. Si vous avez besoin de l'arrêter, faite un « Arrêter ».

- **Réinitialiser**: remet une machine à son état d'origine.
- **Supprimer** : supprime uniquement votre machine virtuelle, sans supprimer les disques virtuels associés.
- Pour la fonction Exporter, voir la partie suivante.
- Pour la fonction Capture instantanée, voir la partie 3.4.
- **Paramètres** : vous permet de changer la configuration matérielle virtualisée de votre machine virtuelle : ordre de boot du bios, RAM, disques virtuels, processeurs, cartes réseaux, port COM et lecteur de

disquette. Vous pouvez aussi modifier la configuration de la machine, comme son nom, le lieu où les Snapshot seront stockés, les « Integration Services », etc.

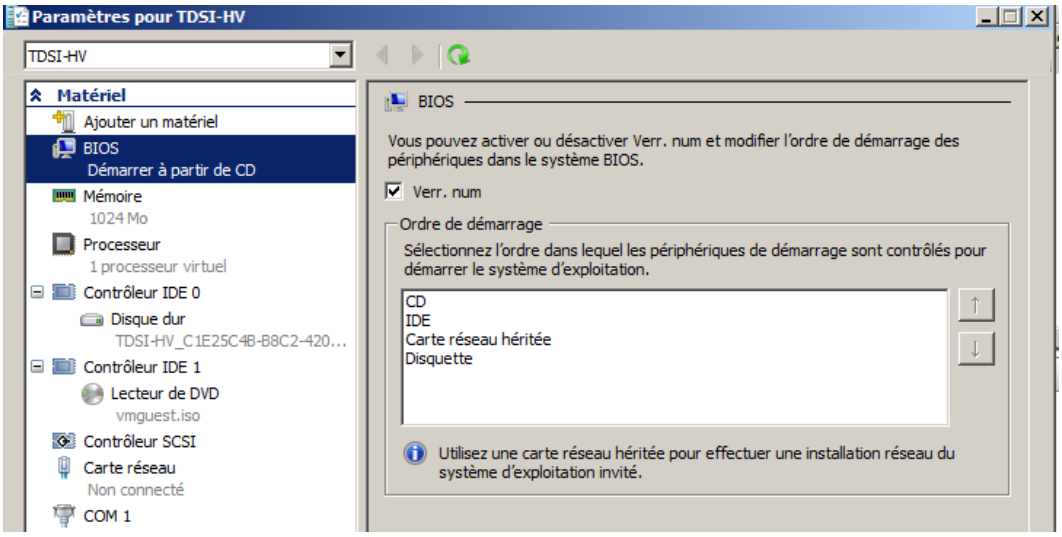


Image V.2.2.15: Paramètres de la machine virtuelle (BIOS)

- **BIOS** : On peut y activer ou désactiver Verr. Num et modifier l'ordre de démarrage des périphériques.
- **Mémoire**: Pour la configuration des options de mémoire de l'ordinateur virtuel

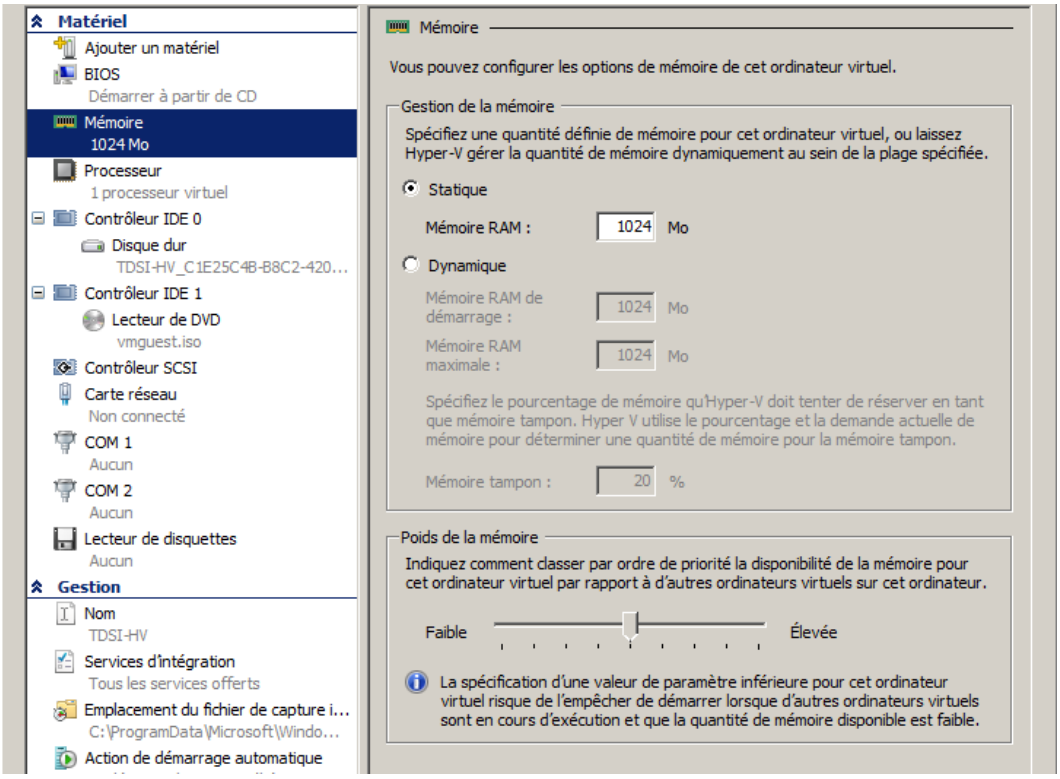


Image V.2.2.16: Paramètres de la machine virtuelle (Mémoire)

Décrivons d'abord brièvement l'utilité de chacune des options disponibles pour la mémoire dynamique.

1) Mémoire RAM de démarrage: il s'agit de la quantité de mémoire RAM allouée par Hyper-V à la VM au démarrage. Cette quantité de RAM doit correspondre à la quantité de mémoire dont a besoin la VM pour démarrer.
2) Mémoire RAM maximale: c'est la mémoire maximale attribuable par Hyper-V à la VM. L'ajout de mémoire se fait par la technologie "HotAdd".
3) Mémoire tampon : Il est basé sur le "Current Commit", autrement dit sur la mémoire allouée à l'instant t à la VM par Hyper-V. La valeur par défaut de la mémoire tampon est paramétrée à 20%.

La Mémoire tampon se calcule comme suit :

$$\boldsymbol{M\acute{e}moire\ tampom(Mo)} = \left(\frac{\mathbf{1}}{\mathbf{1} - \boldsymbol{M\acute{e}moire\ tampom}(\%)} - \mathbf{1}\right) * \boldsymbol{Current\ Commit\ (Mo)}$$

L'objectif de ce tampon est de permettre l'allocation très rapide de mémoire RAM supplémentaire lorsque la charge s'accroît sur la VM. La Mémoire tampon est donc une zone sur chaque VM où est pré-allouée de la RAM. Lors d'une montée en charge, le Global Memory Object (GMO) tentera donc en premier lieu (dans un processus pouvant aller jusqu'à 4 étapes si nécessaire) de fournir la RAM nécessaire via cette Mémoire tampon.

Cette Mémoire tampon est bornée à droite par la valeur de la Mémoire RAM maximale.

À retenir :

a. Vous définirez une valeur basse à cette zone tampon lorsque le logiciel fonctionnant à l'intérieur de la VM essaie d'utiliser autant de RAM que disponible. C'est typiquement le cas d'un serveur SQL.
b. Une valeur haute sera utilisée dans le cas où vous avez un processus qui peut avoir besoin d'un système de cache fichier important ou bien dans le cas où une application demande fréquemment une importante quantité de RAM supplémentaire et ensuite la relâche.
c. La mémoire cible de chaque VM est donc l'addition du Current Commit Charge (borné par les valeurs Minimum RAM et Maximum RAM) et du Memory Buffer.

4) Poids de la mémoire

Lors de la version beta du SP1 de 2008 R2, ce paramètre s'appelait "Memory Priority". Il a pour objectif de déterminer la façon dont les VMs sont impactées lorsqu'il y a lieu de redistribuer la mémoire. Le paramètre ne garantit en rien la disponibilité de la mémoire. C'est une des raisons qui, à l'époque, a poussé Microsoft à modifier le nom de ce paramètre.

Optimisation des machines virtualisées

Pour que les VM travaillent en mode de para-virtualisation, il est nécessaire d'installer les composants additionnels d'Hyper-V. L'installation se fait en cliquant au niveau du menu Action ***sur Insérer le disque d'installation des services d'intégration*** :

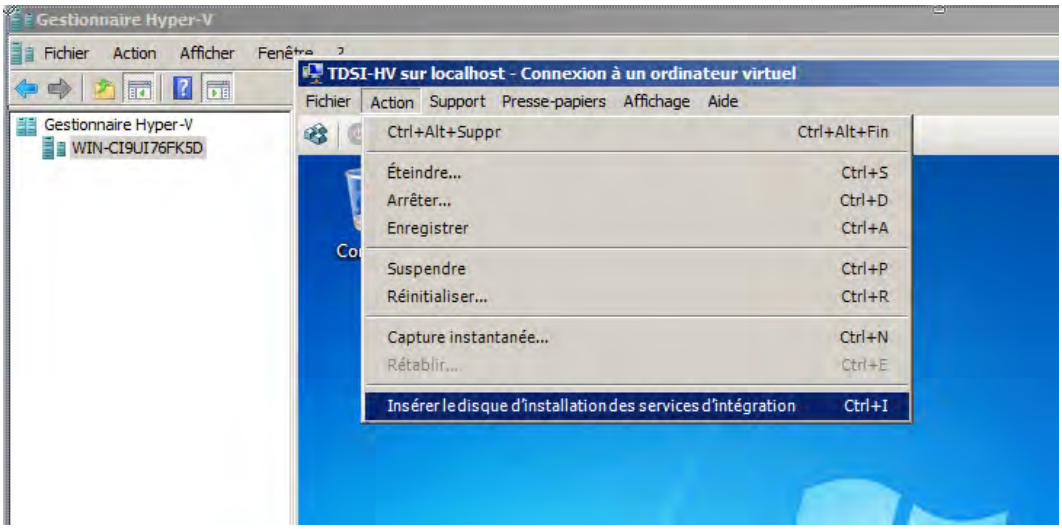


Image V.2.2.17: Installation des services d'intégration

Un CD va être monté dans le lecteur CD de la VM. Si l'exécution ne se fait pas automatiquement, lançons le fichier Setup et suivons les instructions à l'écran. Une fois terminé, nous aurons accès aux fonctionnalités des Services d'intégration Hyper-V

Lorsque notre système d'exploitation n'est pas compatible, nous aurons un message du genre :

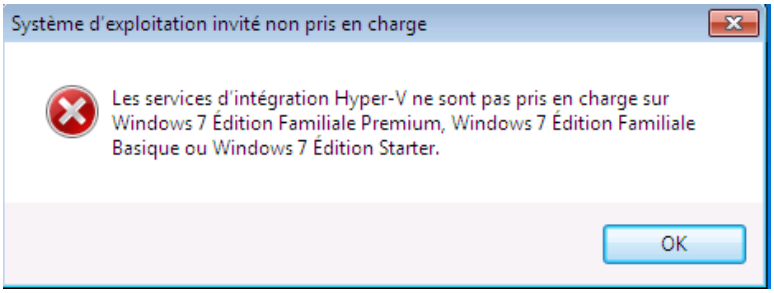


Image V.2.2.18: Erreur sur la prise en charge de l'OS invité

Gestion des captures instantanées

Grace au service Capture instantanée, il nous est possible de créer des sauvegardes à chaud de nos machines virtuelles :

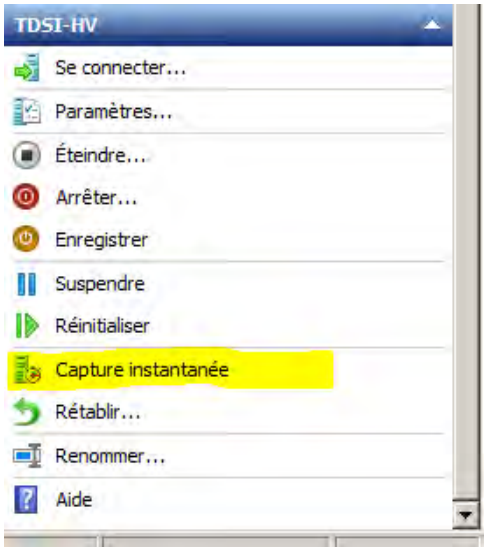


Image V.2.2.19: Prise d'une capture instantanée à partir du menu

Les sauvegardes effectuées apparaissent alors dans la partie centrale de la console d'administration et la sauvegarde la plus récente se situe le plus en bas.

Il sera possible d'appliquer telle ou telle sauvegarde a la VM en un simple clic.

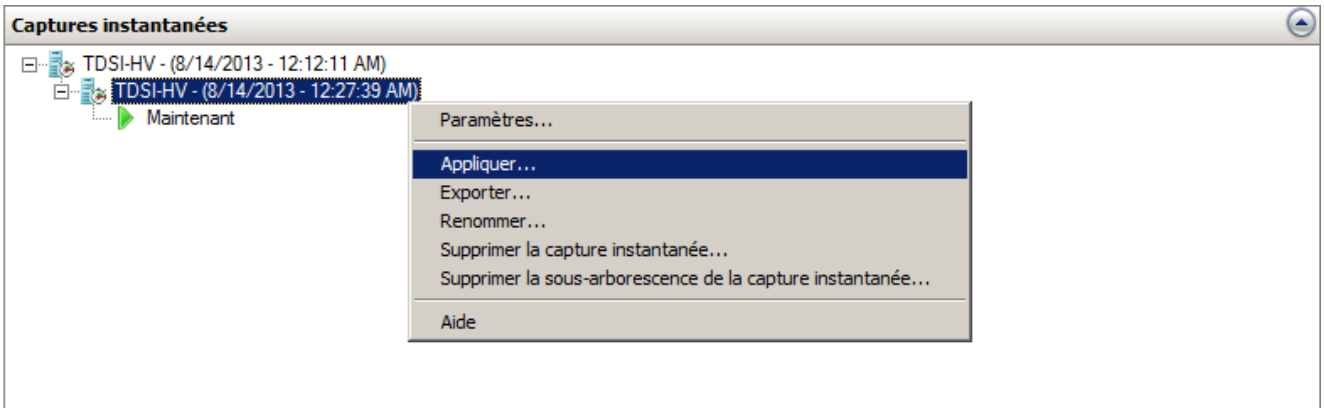


Image V.2.2.20: Différents options d'une capture instantanée

V.3 Délégation de la gestion de la machine virtuelle.

Cette partie fournit des conseils pour vous aider en toute prudence et en toute sécurité de déléguer l'accès administratif aux ressources de la machine virtuelle (VM) au sein d'une organisation. Un certain nombre d'outils est disponible pour administrer les VMs, des ordinateurs physiques et autres aspects d'une infrastructure de la machine virtuelle. Cette partie explique comment ces outils fonctionnent et comment contrôler l'accès administratif à des serveurs différents et à différents niveaux.

Lorsqu'un serveur physique unique est configuré pour supporter plusieurs instances du système d'exploitation, il est important d'assigner correctement des autorisations administratives à chaque instance afin de sécuriser l'environnement Hyper-V ™. L'étendue des opérations disponibles pour un compte d'administrateur dépendra sur où sera établi l'accès administratif pour un compte :

- **Les administrateurs de Hyper-V** sont des comptes administratifs qui ont accès administratifs complets pour la configuration réseau et de stockage de tous les ordinateurs virtuels sur un ordinateur physique de Hyper-V. Ils peuvent effectuer les modifications de configuration globale susceptible d'affecter tous les ordinateurs virtuels sur les ordinateurs physiques.
- **Les administrateurs de machine virtuelle** sont des comptes administratifs qui ont seulement un accès administratif à l'ordinateur virtuel sur lequel le compte a été établi. Hyper-V crée une limite de sécurité entre le système d'exploitation de gestion et les ordinateurs virtuels qui empêchent l'administration du système d'exploitation de gestion par les administrateurs de l'ordinateur virtuel.

Microsoft recommande de contrôler de prêt l'accès administratif au système d'exploitation de gestion et l'assigner uniquement aux membres du personnel avec un besoin valable de gérer le système de gestion d'exploitation et tous les ordinateurs virtuels sur un serveur physique Hyper-V. Pour des opérations typiques, Microsoft recommande de maintenir une séparation nette entre les administrateurs qui sont responsables de l'exploitation du serveur physique et le système d'exploitation de gestion, et les administrateurs qui sont chargés de gérer chacune des machines virtuelles.

V.3.1 UTILISATION DES OUTILS POUR DÉLÉGUER L'ACCÈS

L'interface utilisateur du gestionnaire Hyper-V dans le gestionnaire de serveur sur Windows Server 2008 est montrée précédemment dans la capture d'écran. Il est fourni dans le cadre du rôle Hyper-V, et permet aux utilisateurs désignés comme administrateurs du système d'exploitation de gestion de gérer les machines virtuelles sur l'ordinateur physique. Les administrateurs peuvent utiliser le Gestionnaire Hyper-V pour effectuer une variété de tâches de gestion sur l'ordinateur physique, y compris le démarrage et l'arrêt des machines virtuelles, l'importation et le déploiement de machines virtuelles sur l'ordinateur, et la gestion des snapshots. Par défaut, toute personne qui est un administrateur local du système d'exploitation de gestion peut utiliser le Gestionnaire Hyper-V sur l'ordinateur physique. En outre, l'utilisateur peut également utiliser le Gestionnaire Hyper-V pour gérer à distance Hyper-V sur d'autres serveurs dans un domaine pour lequel l'utilisateur a un accès administratif

V.3.2 DÉLÉGUER L'ACCÈS AVEC LE GESTIONNAIRE D'AUTORISATIONS

Par défaut, l'accès au gestionnaire de Hyper-V sur un ordinateur physique est réservé aux membres du groupe Administrateurs local sur le serveur. La configuration par défaut permet d'assurer la sécurité de la machine virtuelle en limitant le contrôle des machines virtuelles pour les utilisateurs qui ont déjà tous les droits d'administrateur sur l'ordinateur physique. Toutefois, dans certains scénarios, nous voudrons que des utilisateurs de confiance supplémentaires puissent avoir les autorisations appropriées pour gérer les ordinateurs virtuels à l'aide du Gestionnaire Hyper-V.

Par exemple, on voudrait pouvoir déléguer la gestion de la technologie Hyper-V à un groupe d'assistants pour mieux répondre aux besoins d'un grand déploiement Hyper-V décentralisé, mais notre organisation pourrait avoir des politiques de sécurité en vigueur qui découragent l'octroi d'un accès d'administration du serveur à des personnes en dehors d'un petit groupe d'administrateurs. Limiter l'accès administratif au système d'exploitation de gestion vous permet également d'utiliser des listes de contrôle d'accès (ACL) pour empêcher les utilisateurs non autorisés d'accéder à des disques durs virtuels et autres fichiers critiques à travers le système de fichiers.

Nous pouvons utiliser le gestionnaire d'autorisations (AzMan), un composant logiciel enfichable pour Microsoft Management Console (MMC), pour assigner aux utilisateurs et groupes sélectionnés le rôle Administrateur de Hyper-V afin qu'ils puissent utiliser le Gestionnaire Hyper-V sans être administrateurs de l'ordinateur physique lui-même. Le gestionnaire d'autorisations est un outil administratif pour définir et utiliser l'autorisation basée sur les rôles dans les applications qui sont conçues pour le soutenir. La stratégie d'autorisation basée sur les rôles spécifie un accès en termes de rôles d'utilisateur qui reflètent les exigences d'autorisation de l'application. Les utilisateurs se voient assignés des rôles basés sur leurs fonctions, et ces rôles sont des autorisations élevées pour effectuer des opérations ou tâches connexes. Les rôles et les tâches d'une application sont définis et enregistrés dans un magasin d'autorisations, qui peut être consulté et modifié à l'aide du gestionnaire d'autorisations.

Le magasin d'autorisations par défaut inclus avec Hyper-V définit 33 opérations différentes et un rôle d'administrateur pouvant accéder à chacun d'eux. Nous pouvons créer d'autres rôles qui peuvent accéder à un sous-ensemble d'opérations admissibles. Les rôles sont répertoriés dans les attributions de rôles dans le gestionnaire d'autorisations, ainsi que dans le nœud de définitions de rôles au-dessous du nœud de définitions.

Les trois tableaux suivants catégorisent toutes les opérations de Hyper-V qui peuvent être assignées aux rôles. (Source ***Hyper-V Security Guide***, page 25)

Table IV.3.2.1. Hyper-V Service Operations

Name	Description
Read service configuration	Authorizes reading configuration of the Virtual Machine Management Service
Reconfigure Service	Authorizes reconfiguration of Virtual Machine Management Service

Table IV.3.2.2. Hyper-V Network Operations

Name	Description
Bind External Ethernet Port	Authorizes binding to an external Ethernet port
Connect Virtual Switch Port	Authorizes connecting to a virtual switch port
Create Internal Ethernet Port	Authorizes creating an internal Ethernet port
Create Virtual Switch	Authorizes creating a new virtual switch
Create Virtual Switch Port	Authorizes creating a new virtual switch port
Delete Internal Ethernet Port	Authorizes deleting an internal Ethernet port
Delete Virtual Switch	Authorizes deleting a virtual switch
Delete Virtual Switch Port	Authorizes deleting a virtual switch port
Disconnect Virtual Switch Port	Authorizes disconnecting from a virtual switch port
Modify Internal Ethernet Port	Authorizes modifying the internal Ethernet port settings
Modify Switch Port Settings	Authorizes modifying the switch port settings
Modify Switch Settings	Authorizes modifying the switch settings
Change VLAN Configuration on Port	Authorizes modifying VLAN settings
Unbind External Ethernet Port	Authorizes unbinding from an external Ethernet port
View External Ethernet Ports	Authorizes viewing the available external Ethernet ports
View Internal Ethernet Ports	Authorizes viewing the available internal Ethernet ports
View LAN Endpoints	Authorizes viewing the LAN endpoints
View Switch Ports	Authorizes viewing the available switch ports
View Switches	Authorizes viewing the available switches

Name	Description
View Virtual Switch Management Service	Authorizes viewing the Virtual Switch Management Service
View VLAN Settings	Authorizes viewing the VLAN settings

Table IV.3.2.3. Hyper-V Virtual Machine Operations

Name	Description
Allow Input to Virtual Machine	Authorizes user to give input to the virtual machine
Allow Output from Virtual Machine	Authorizes viewing the output from a virtual machine
Change Virtual Machine Authorization Scope	Authorizes changing the scope of a virtual machine
Create Virtual Machine	Authorizes creating a virtual machine
Delete Virtual Machine	Authorizes deleting a virtual machine
Pause and Restart Virtual Machine	Authorizes pause and restart of a virtual machine
Reconfigure Virtual Machine	Authorizes reconfiguring a virtual machine
Start Virtual Machine	Authorizes starting the virtual machine
Stop Virtual Machine	Authorizes stopping the virtual machine
View Virtual Machine Configuration	Authorizes viewing the virtual machine configuration

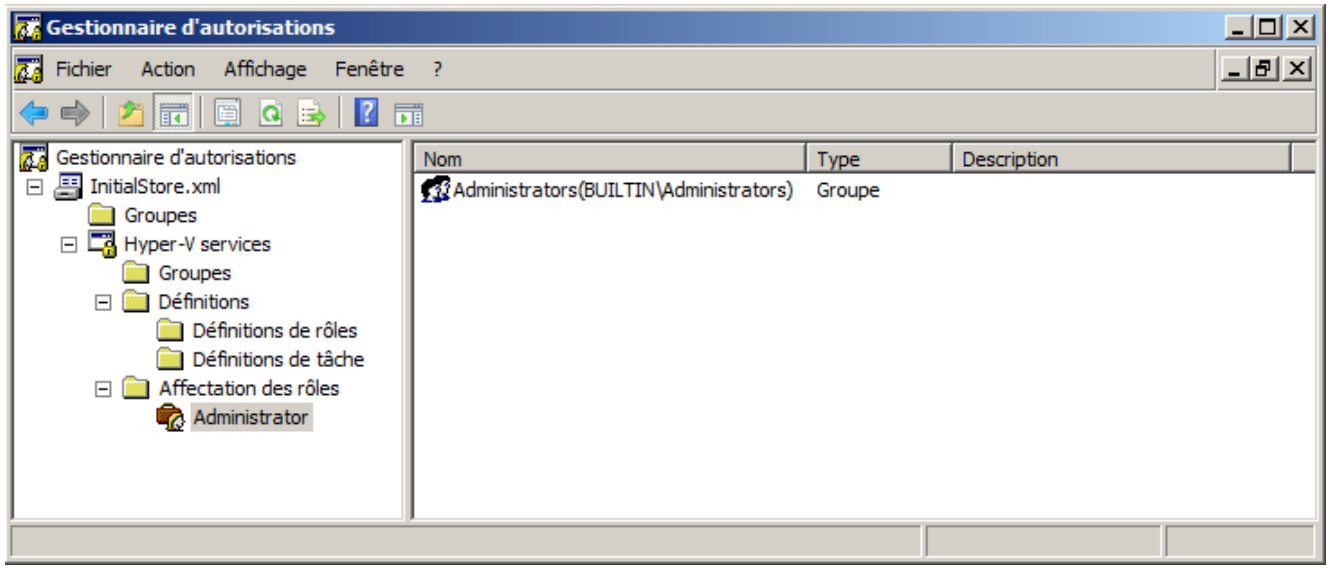


Image V.3.2.1: Gestionnaire d'autorisation

Tous les utilisateurs ayant reçus le rôle de l'administrateur par gestionnaire d'autorisations (illustrée par la figure précédente) ont un accès complet à la Gestionnaire Hyper-V et tous les ordinateurs virtuels déployés sur l'ordinateur physique et peuvent accéder à tous les 33 opérations de l'Hyper-V énumérées dans les trois tableaux précédents.

Pour utiliser le gestionnaire d'autorisations afin d'assigner le rôle Administrateur aux utilisateurs et groupes :

1. À partir de la console de gestion de l'ordinateur physique ou d'un poste de travail distant, cliquez sur ***Démarrer***, tapez ***azman.msc*** et puis appuyez sur entrée. La console de composant logiciel enfichable du gestionnaire d'autorisations s'affiche.
2. Faire un clic droit sur le gestionnaire d'autorisations dans l'arborescence, puis sélectionnez Ouvrir magasin d'autorisations.
3. La boîte de dialogue Ouvrir magasin d'autorisations s'affiche avec le fichier XML sélectionné comme type de magasin.
4. Effectuez l'une des opérations suivantes :
   - ✓ Si vous êtes sur l'ordinateur physique, spécifiez le chemin ***%programdata%\Microsoft\Windows\Hyper-V\InitialStore.xml*** dans la zone de texte Nom du magasin et cliquez sur OK.

     Remarque : Par défaut, seuls les administrateurs locaux ont accès à ce répertoire.
   - ✓ Si vous êtes sur une station de travail distante, spécifiez le chemin vers le fichier InitialStore.xml sur l'ordinateur physique dans la zone de texte Nom du magasin et cliquez sur OK. Par exemple, si Windows Server 2008 est installé sur le lecteur C:, vous pouvez spécifier

\\<nom du serveur>\c$\ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml.

5. Développez ***Hyper-V services*** sous InitialStore.xml, étendre ***Affectation de rôles*** et puis cliquez sur le rôle ***Administrateur***.
6. Cliquez sur ***Action***, pointez sur ***Affecter des utilisateurs et des groupes*** et puis cliquez sur ***À partir de Windows et Active Directory…***.
7. Dans la boîte de dialogue ***Sélectionnez des utilisateurs ou groupes***, sélectionnez les comptes d'utilisateurs et les groupes auxquels vous souhaitez affecter le rôle et cliquez sur OK.

V.3.3 System Center Virtual Machine Manager 2008

Microsoft System Center VMM 2008, qui est disponible comme produit séparé, est une solution de gestion complète pour les datacenters virtualisés. Comme montré dans la capture d'écran ci-dessous, VMM 2008 permet une utilisation accrue du serveur physique, une gestion centralisée de l'infrastructure de la machine virtuelle et le provisioning rapide de nouveaux ordinateurs virtuels par l'administrateur, aux administrateurs

désignés et aux utilisateurs finaux autorisés. VMM 2008 prend en charge Windows Server 2008 Hyper-V, Microsoft Virtual Server 2005 et ajoute le support pour les ordinateurs virtuels s'exécutant sur VMware ESX Server, ce qui permet de gérer de manière centralisée des environnements de machines virtuelles provenant de différents fournisseurs. Les nouvelles fonctionnalités ***Performance and Resource Optimization (PRO)*** and ***Intelligent Placement*** nous aident à répartir nos ressources informatiques virtuelles plus efficacement et à les surveiller pour les situations potentiellement gênantes.

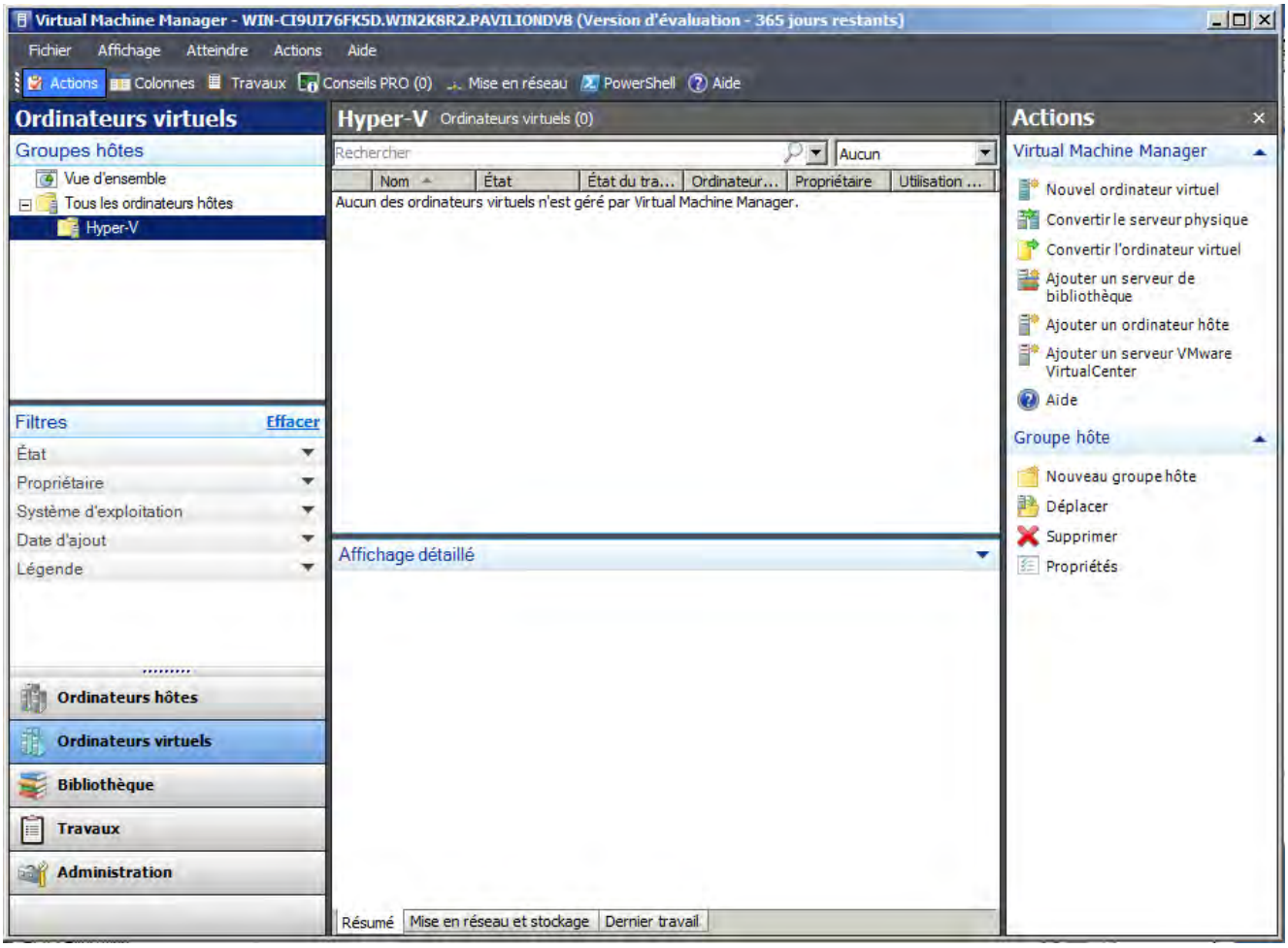


Image V.3.3.1: Virtual Machine Manager

VMM 2008 est une solution complète qui offre de nombreux outils de gestion des ressources de la machine virtuelle. Cependant, dans un contexte de sécurité, les caractéristiques les plus importantes de VMM 2008 concernent sa capacité à déléguer des autorisations administratives de machine virtuelle. VMM 2008 permet de créer des groupes d'ordinateurs physiques Hyper-V, ou des hôtes et gérer leurs accès administratifs individuellement. VMM 2008 permet également de créer des bibliothèques qui peuvent être utilisés pour

stocker des VMs lorsqu'elles ne sont pas utilisées et de stocker des ressources pour la création de nouveaux ordinateurs virtuels basés sur les modèles et profils standards.

❖ Rôle de l'administrateur délégué

Les utilisateurs appartenant à un rôle d'administrateur délégué peuvent utiliser la Console Administrateur VMM pour accéder à tous les hôtes et les serveurs de bibliothèque auxquels ils ont le droit de gérer, tel que déterminés par les paramètres de rôle. Les autres hôtes et serveurs de bibliothèque ne s'affichent pas dans la console et ne peuvent être gérés par l'utilisateur.

Pour ajouter un rôle d'utilisateur administrateur délégué dans VMM 2008

1. Dans la vue **Rôles d'utilisateur** à partir de la Console d'Administration VMM, cliquez sur Nouveau rôle d'utilisateur dans le volet Actions. L'Assistant nouveau rôle de l'utilisateur s'affiche.
2. Sur la page **Général**, tapez un nom de rôle d'utilisateur et une Description et puis sélectionnez Administrateur délégué dans la liste profil de rôle d'utilisateur. Cliquez sur suivant.
3. Sur la page **Ajouter des membres**, cliquez sur Ajouter et tapez les noms des utilisateurs Active Directory ou groupes à ajouter à ce rôle. Cliquez sur suivant.
4. Comme indiqué dans la capture d'écran suivante, sélectionnez les groupes hôtes et les serveurs de bibliothèque pour lesquels vous souhaitez permettre la gestion aux membres du rôle d'utilisateur. Cliquez sur suivant.

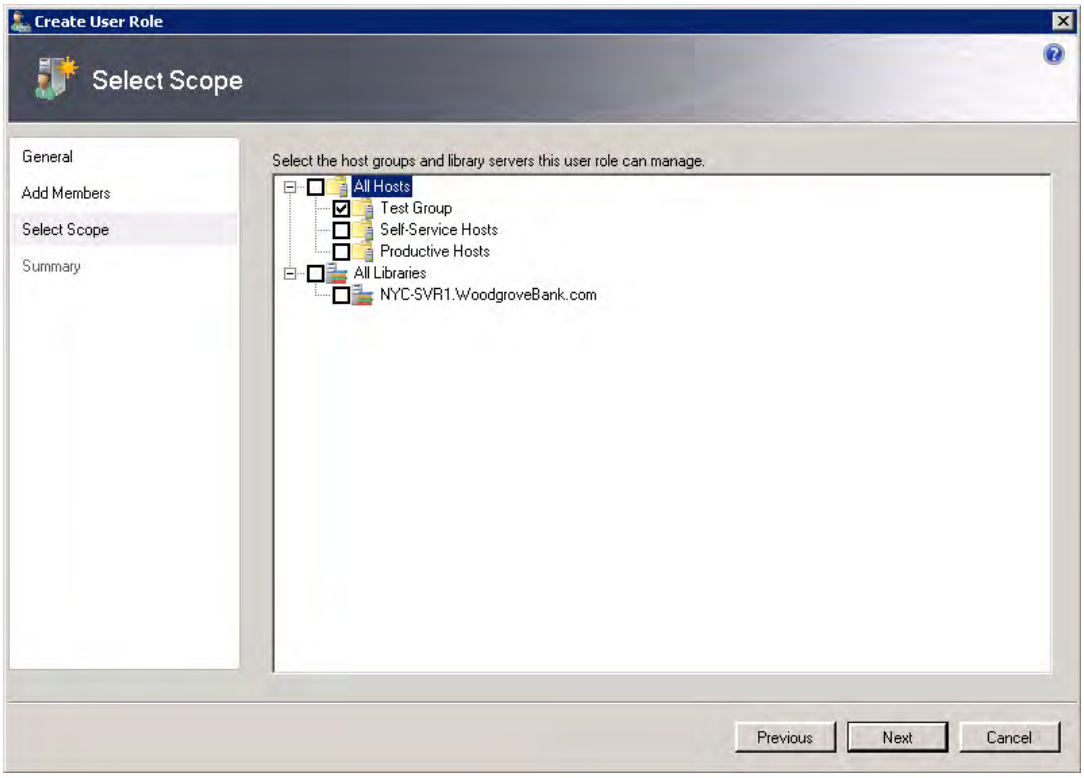


Image V.3.3.2: Création de rôle utilisateur

5. Sur la page Sommaire, on vérifie les paramètres de rôle de l'utilisateur et on clique sur Créer.

❖ Self Service Portal

Le Virtual Machine Manager Self-Service Portal est un site Web grâce à partir duquel les utilisateurs self-service peuvent créer et faire fonctionner leurs propres ordinateurs virtuels dans un environnement contrôlé. À l'aide du portail Self-Service, les utilisateurs self-service peuvent voir uniquement les ordinateurs virtuels leur appartenant, et ils sont autorisés à effectuer uniquement les actions permises au rôle de l'utilisateur associé à la machine virtuelle. Par exemple, vous pourrez créer un groupe d'utilisateurs self-service qui sont autorisés à démarrer, arrêter, suspendre et reprendre les machines virtuelles d'un groupe hôte, mais ne pas à effectuer d'autres actions administratives telles que la gestion des points de contrôle de la machine virtuelle ou la suppression de machines virtuelles.

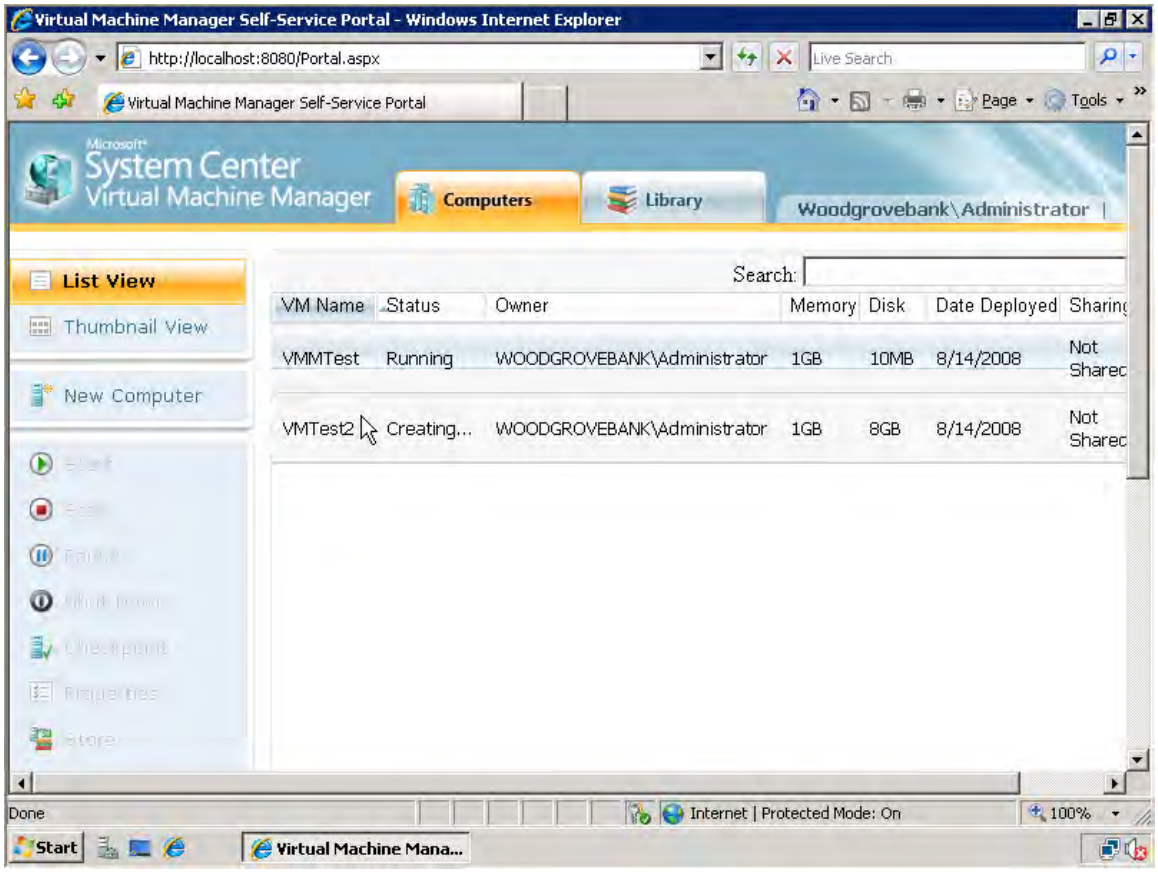


Image V.3.3.3: Self-service Portal

V.3.4 PROTECTION DES MACHINES VIRTUELLES

Cette partie donne des conseils pour sécuriser les fichiers utilisés pour créer et exécuter des machines virtuelles (VM), tels que les fichiers de configuration et les fichiers de disque dur virtuel (VHD). Elle comprend des recommandations sur les meilleures pratiques pour implémenter correctement un système autorisations de fichiers, le chiffrement, et l'audit qui aident à protéger vos ordinateurs virtuels et les fichiers de configuration

associés de tout accès non autorisé et de manipulations malveillantes. Cette partie comprend également les meilleures informations pratiques et ressources conçues pour vous aider à protéger les systèmes d'exploitation qui s'exécutent dans une machine virtuelle contre des menaces communes.

Méthodes de protection de machines virtuelles

Une machine virtuelle est constituée d'un ensemble de fichiers, y compris les fichiers VHD et fichiers qui définissent la configuration de la machine virtuelle. Certains scénarios de VM peuvent inclure des fichiers qui ne sont pas généralement associés à des ordinateurs physiques, tels que le contenu de la mémoire d'un serveur exécutant stockée sur le disque. Les applications qui stockent des informations sensibles telles que les mots de passe ou des hachages en mémoire mais non généralement sur le disque peuvent donc être plus à risque si exécutées dans des environnements virtualisés, en raison de la possibilité que des renseignements sensibles étant stockées sur le disque comme les informations d'état.

Sous forme de fichiers sur disque, les ressources de la machine virtuelle peuvent être sécurisée à l'aide de plusieurs techniques qui sont couramment utilisés pour stocker d'autres fichiers dans les environnements Windows Server, y compris la sécurité du système de fichiers, le cryptage et l'audit d'accès d'objet.

a) Configuration pointue du système d'exploitation de la VM et des Applications

Les mêmes mesures de sécurité et configuration pointue que nous appliquons à un ordinateur physique devraient être appliquées aux VMs. Nous devons effectuer des étapes de durcissement pour le rôle de serveur de la machine virtuelle comme il est indiqué dans la section « **Installation & Configuration du rôle en renforçant la sécurité**» dans la partie III, B, y compris la consultation du guide appropriée de Microsoft Solution Accelerator pour le système d'exploitation spécifique.

❖ Prérequis des Pare-feu et Antivirus

Chaque système d'exploitation s'exécutant sur une machine virtuelle a besoin de son propre logiciel de détection intrusion, antivirus et pare-feu en fonction de l'environnement.

❖ Considérations de la Politique de groupe

Comme les serveurs physiques, des machines virtuelles s'ajouteront aux unités d'organisation (OU) appropriées afin que les paramètres de stratégie de groupe s'appliquent correctement.

b) Utilisation de la sécurité du système de fichiers pour protéger les ressources de la VM

Vous pouvez utiliser des listes de contrôle d'accès (ACL) pour aider à protéger les fichiers VHD et fichiers de configuration d'ordinateur virtuel des accès non autorisés au niveau du système de fichier. Cette approche peut empêcher les scénarios comme une personne non autorisée à copier un disque dur virtuel d'un ordinateur Hyper-V ou d'une bibliothèque de serveur vers un autre emplacement, ou remplacer un fichier existant de la machine virtuelle avec une version modifiée. Cependant, l'utilisation des ACL pour limiter l'accès aux fichiers ou dossiers n'est pas un moyen efficace pour gérer l'accès administratif aux machines virtuelles eux-mêmes.
Chaque ordinateur virtuel s'exécute dans le contexte d'un processus de travail de machine virtuelle (vmwp.exe), qui s'exécute sous le compte ***NETWORK SERVICE*** et qui est en mesure d'accéder aux ressources de système de fichiers qui composent la machine virtuelle. Cette fonctionnalité permet à tout utilisateur disposant des autorisations nécessaires d'utiliser le Gestionnaire Hyper-V pour arrêter et démarrer les ordinateurs virtuels, de monter des disques durs virtuels et d'effectuer d'autres tâches de gestion. Un plan global de sécurité Hyper-V implique une combinaison des ACLs et d'outils tels que Virtual Machine Manager 2008 (VMM 2008) qui peut être utilisé pour restreindre les capacités de gestion de VM.

c) Utilisation du chiffrement pour protéger les ressources de la machine virtuelle

Windows BitLocker Drive Encryption (BitLocker) est une fonction de protection des données inclus avec Windows Server 2008. BitLocker est une fonction de logiciel basé sur le système d'exploitation qui fonctionne avec des caractéristiques de matériel du serveur et du firmware pour assurer l'amorçage d'un système d'exploitation sécurisé et le chiffrement de disque. Ce chiffrement protège physiquement les données et l'intégrité du système d'exploitation. La Protection physique basée BitLocker est présente, même lorsque le serveur n'est pas sous tension ou en fonctionnement, ce qui signifie que les données sont protégées même si le disque a été volé et monté sur un autre ordinateur à des fins d'extraction de données. BitLocker protège également les données si un pirate utilise un système d'exploitation différent ou exécute un logiciel de piratage pour accéder au disque.

d) Utilisation de l'audit pour suivre l'accès aux ressources de la VM

La sécurité du système de fichiers peut empêcher l'accès non autorisé aux ressources critiques de la VM, tels que les fichiers VHD. L'Audit d'accès aux objets peut aider à détecter les activités des utilisateurs potentiellement dangereuses.

L'activation de l'audit d'accès aux objets sur un ordinateur physique amène à journaliser chaque tentative d'un utilisateur pour accéder aux fichiers audités. Les tentatives d'accès réussies ou non peuvent être auditées. Si la sécurité ou l'intégrité des données stockées dans un fichier VHD est violé, la piste de vérification va révéler qui a consulté le fichier et quand, ce qui peut être utilisé pour déterminer qui était responsable de la violation.

Maintien des Machines virtuelles

Veiller à ce que les machines virtuelles sont mises à jour avec le système d'exploitation, les applications et mises à jour antivirus peut présenter des défis. Des machines virtuelles pourraient rester hors ligne (stockées dans un état hors exploitation) pour des périodes prolongées de temps quand elles ne sont pas nécessaires afin de libérer des ressources. Cependant, si une machine virtuelle est hors ligne il ne peut recevoir automatiquement des mises à jour par le biais de mécanismes tels que Windows Update ou Windows Software Update Services (WSUS). Si déployée et lancée, la machine virtuelle obsolète peut être vulnérable aux attaques ou pourrait être capable d'attaquer les autres ressources du réseau.

AIDE-MÉMOIRE DES MEILLEURES PRATIQUES DE LA SÉCURITÉ HYPER-V

La sécurisation de Hyper-V implique toutes les mesures nécessaires pour préserver un rôle de serveur de Windows Server 2008, plus quelques suppléments pour aider à sécuriser les ordinateurs virtuels, fichiers de configuration et données. La liste suivante des pratiques exemplaires recommandées sert d'aide-mémoire pour vous aider à améliorer la sécurité de votre environnement Hyper-V.

a) Configuration du système d'exploitation de gestion

Microsoft recommande de prêter une attention particulière aux meilleures pratiques suivantes pour sécuriser Hyper-V lors de la configuration du système d'exploitation de gestion:

- Utiliser une installation Server Core pour le système d'exploitation de gestion.
- Gardez le système d'exploitation de gestion à jour avec les dernières mises à jour de sécurité
- Utiliser un réseau séparé avec un adaptateur de réseau dédié pour le système d'exploitation de gestion de l'ordinateur physique Hyper-V.
- Sécurisé les périphériques de stockage où vous gardez les fichiers de ressources de machines virtuelles.
- Renforcer le système d'exploitation de gestion en utilisant les recommandations des paramètres de sécurité de base décrites dans le manuel de gestion de Windows Server 2008 Security Compliance.
- Configurer les composants logiciels d'analyse antivirus en temps réel installés sur le système d'exploitation de gestion pour exclure les ressources Hyper-V.
- Ne pas utiliser le système d'exploitation de gestion pour exécuter des applications.
- Ne pas accorder de droits administrateurs sur la machine virtuelle sur le système d'exploitation de gestion.
- Utiliser le niveau de sécurité de vos machines virtuelles afin de déterminer le niveau de sécurité de votre système d'exploitation de gestion.
- Utiliser BitLocker Drive Encryption pour protéger les ressources.

b) Configuration de la Machine virtuelle

Les méthodes suivantes peuvent nous aider à améliorer la sécurité lors de la configuration des machines virtuelles sur les serveurs exécutant le rôle Hyper-V :

- Configurer les machines virtuelles pour qu'elles utilisent des disques durs virtuels de taille fixe.
- Stocker les disques durs virtuels et les fichiers de capture instantanée dans un emplacement sécurisé.
- Décider de combien de mémoire à assigner à une machine virtuelle.
- Imposer des limites à l'utilisation du processeur.
- Configurer les adaptateurs réseau virtuels de chaque machine virtuelle pour se connecter au bon type de réseau virtuel pour isoler le trafic réseau selon les besoins.
- Configurer les périphériques de stockage requis uniquement pour un ordinateur virtuel.
- Renforcer le système d'exploitation exécuté sur chaque machine virtuelle selon le rôle de serveur qu'il exécute en utilisant les recommandations de paramètres de sécurité de base décrites dans Windows Server 2008 Security Compliance Management Toolkit.
- Configurer un antivirus, pare-feu et logiciel de détection d'intrusion au sein des machines virtuelles comme approprié et basé sur le rôle de serveur.
- S'assurer que les ordinateurs virtuels ont toutes les dernières mises en sécurité avant qu'ils soient déployés dans un environnement de production.
- Veiller à ce que les ordinateurs virtuels aient Integration Services installés.

VI. CONCLUSION

Hyper-V est plus qu'une évolution des précédents produits de virtualisation proposés par Microsoft. Il s'agit véritablement d'un changement complet de technologie de virtualisation. Résolument novateur par rapport aux produits concurrents Hyper-V associe para virtualisation et hyperviseur le tout pour un prix modique.

Il faut noter aussi VMware qui a toujours dominé le marché de la virtualisation se fait rattraper sur le point technologique par Microsoft. Aussi, avec son prix abordable, Microsoft avec Hyper-V gagne de plus en plus de place dans les entreprises.

La question qu'on doit enfin se poser est de savoir si même avec un environnement virtuel sécurisé, les données sont à l'abri des pirates.

VII. ANNEXES

WEBOGRAPHIE (*DATE DE CONSULTATION : AOÛT 2013*) :

Microsoft Virtual Server: http://en.wikipedia.org/wiki/Microsoft_Virtual_Server

Hyper-V: http://en.wikipedia.org/wiki/Hyper-V & http://fr.wikipedia.org/wiki/Hyper-V

VMware ESX: http://fr.wikipedia.org/wiki/VMware#VMware_ESX

Hyper-V FAQ : http://technet.microsoft.com/en-us/library/dd744892(v=ws.10).aspx

Installer le rôle Hyper-V sur une installation minimale de Windows Server 2008: http://technet.microsoft.com/fr-fr/library/cc794852(v=ws.10).aspx

Installation et configuration de Microsoft Hyper-V: http://root-lab.fr/2011/07/04/installation-et-configuration-de-microsoft-hyper-v-2/

Installation Hyper-V 2008 Server R2: http://idealogeek.fr/2013/installation-hyper-v-2008-server-r2/

Administration et utilisation d'Hyper-V R2: http://www.tuto-it.fr/UtilisationHyperV.php

Hyper-V essentials: http://www.virtuatopia.com/index.php/Hyper-V_Essentials

How to run Hyper-V nested in VMware Workstation: http://4sysops.com/archives/how-to-run-hyper-v-under-vmware-workstation/

Hyper-V Security Guide: http://www.microsoft.com/en-us/download/details.aspx?id=16650