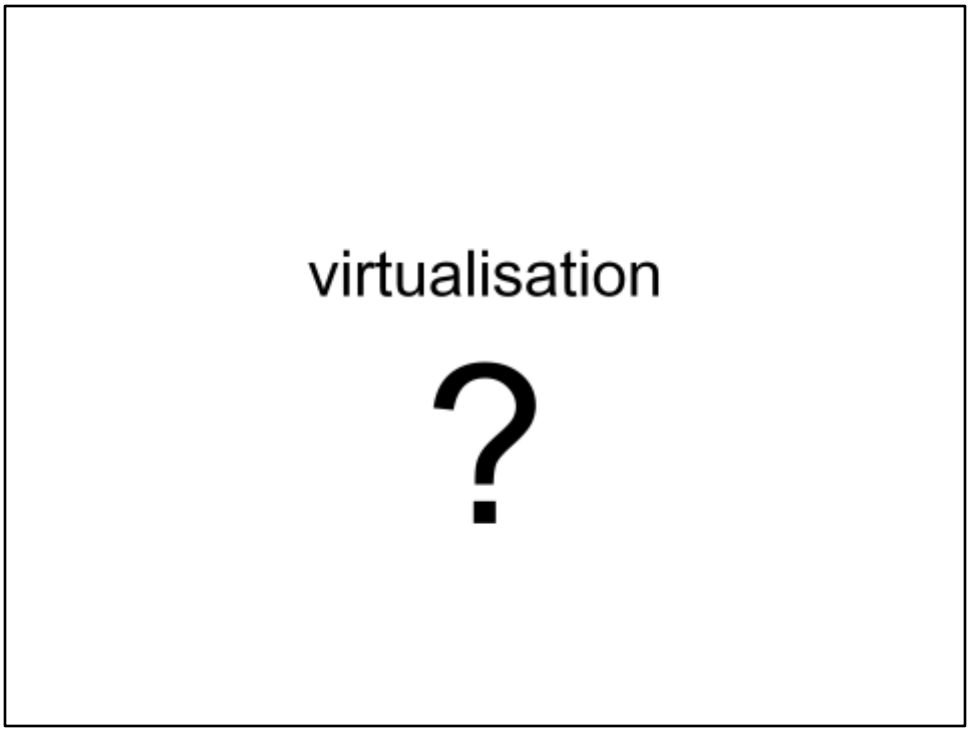
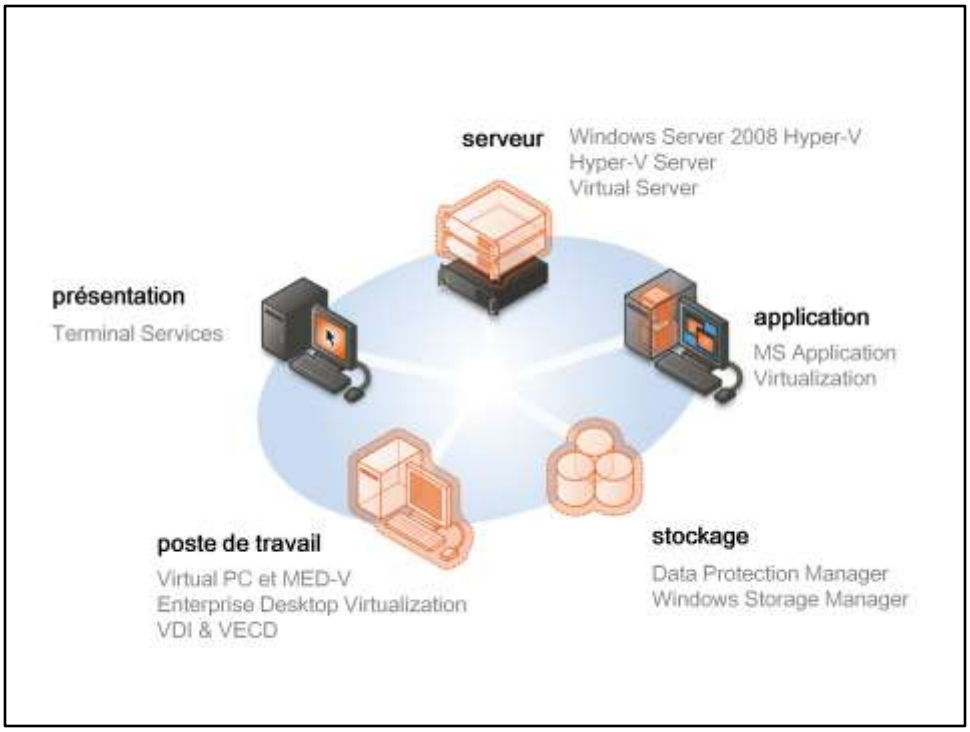
virtualisation & sécurité avec Hyper-V

Cyril Voisin
Chef de programme Sécurité
Microsoft France
https://blogs.technet.com/voy



Virtualization is the isolation of one computing resource from the others
Virtualization results in more ***efficient resource utilization***, and enables ***greater flexibility*** and simplified ***change management***

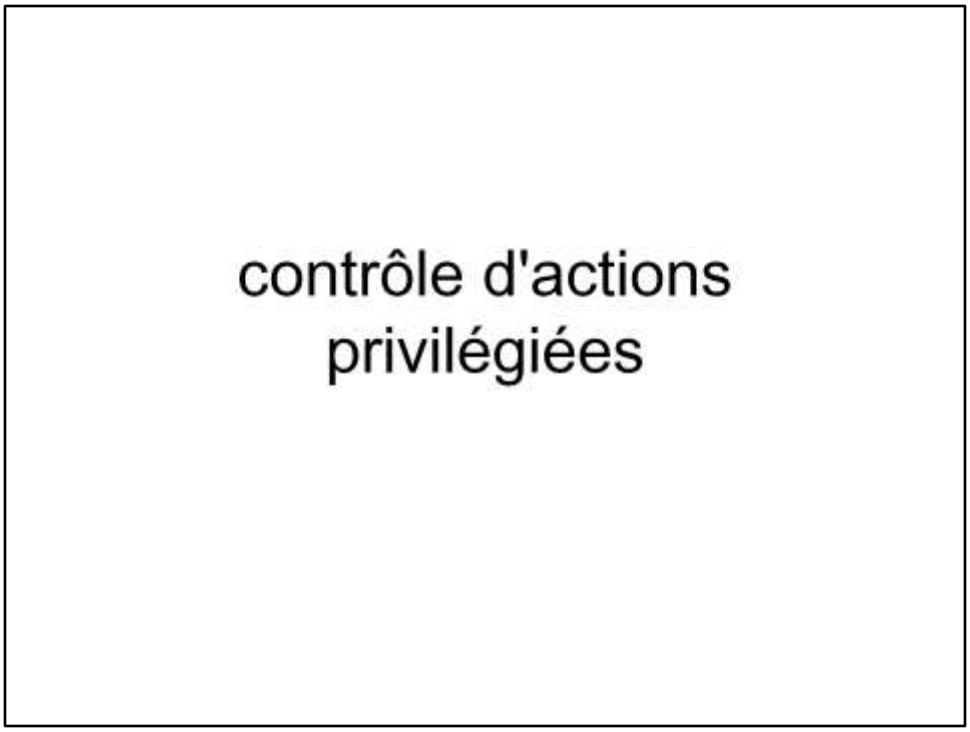
SOLUTIONS DE VIRTUALISATION MICROSOFT



App-V (ex SoftGrid)
VDI = Virtual Desktop Infrastructure (OS client sur machine serveur Hyper-V), s'appuie sur VECD
VECD = Windows Vista Enterprise Centralized Desktop
MED-V (ex Kidaro) : MS Enterprise Desktop Virtualization

au centre : gestion de la virtualisation avec System Center (et notamment SCVMM)

VIRTUALISATION DE MACHINES

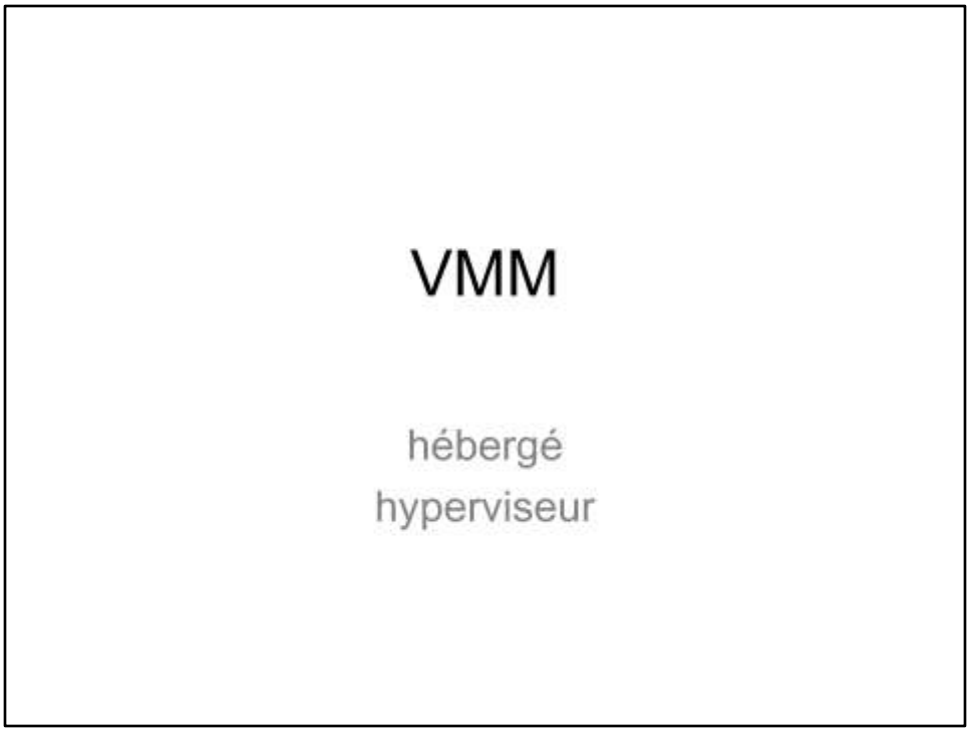


http://www.microsoft.com/virtualization/products.mspx

La virtualisation d'une machine requiert le contrôle des opérations privilégiées

- Les registres du CPU et le matériel impliqué dans la gestion de la mémoire
- Les périphériques matériels

Virtualisation signifie généralement émulation mais peut aussi signifier un accès contrôlé à un état privilégié



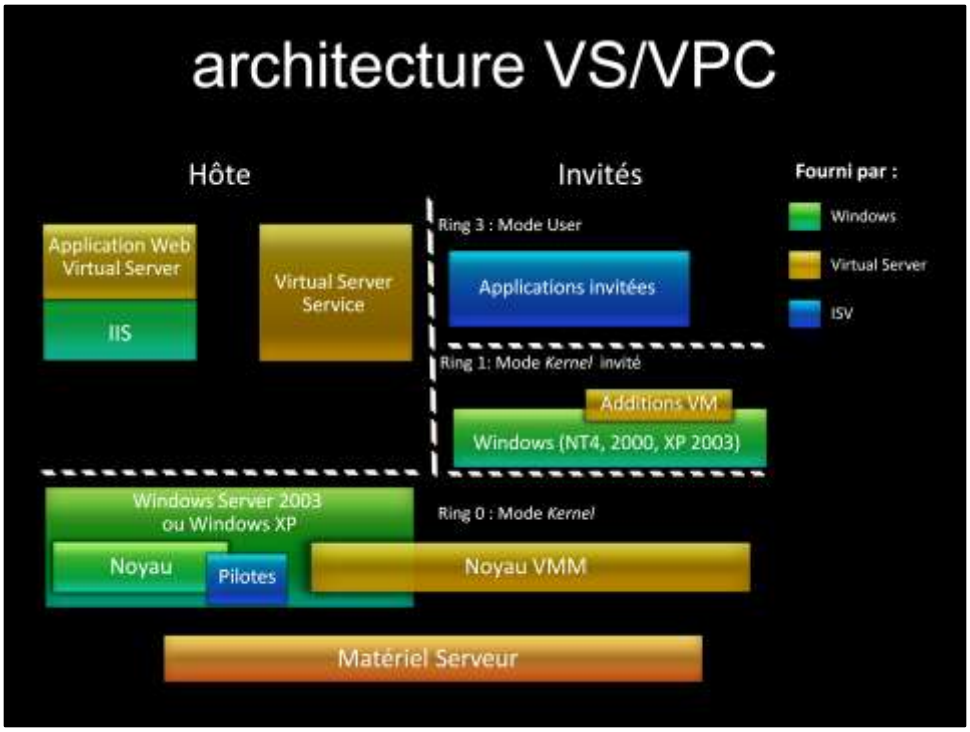
Le cœur du logiciel de virtualisation est appelé *Virtual Machine Monitor* (VMM)

Il y a deux approches à la virtualisation d'une machine

- La virtualisation hébergée
- La virtualisation à base d'hyperviseur

virtualisation hébergée

Virtual Server
Virtual PC



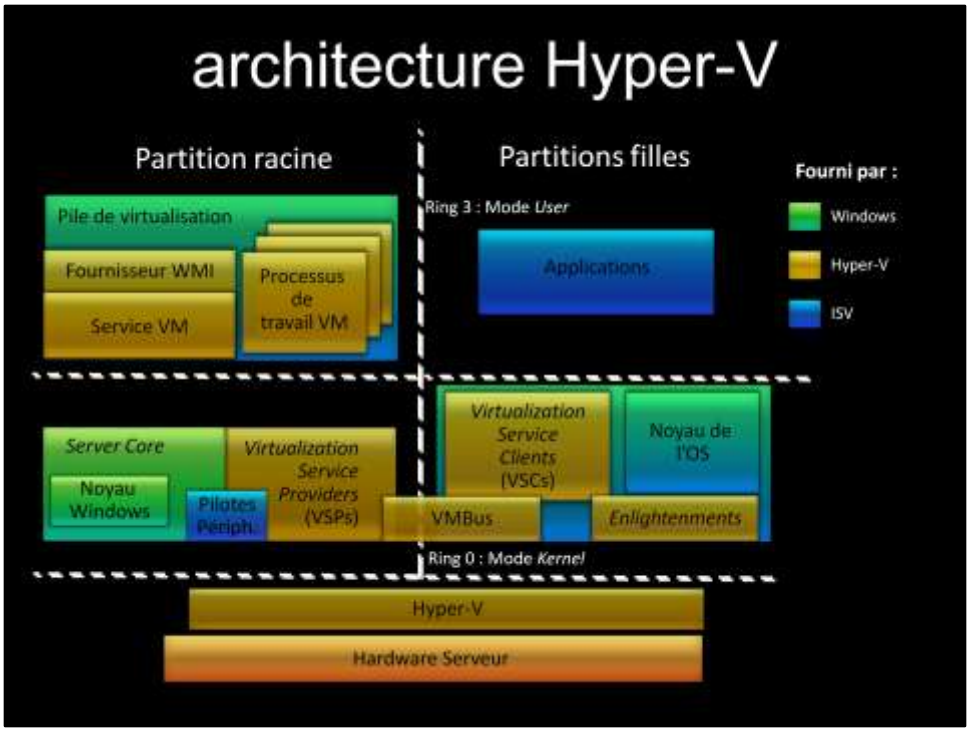
architecture virtualisation hébergée

Dans le cadre d'une virtualisation hébergée, le VMM s'exécute avec le même privilège que le noyau du système d'exploitation hôte

- Le niveau de privilège *kernel* de la machine invitée est inférieur au noyau du système hôte mais est plus élevé que le code en mode *user* s'exécutant au sein de la machine invitée (notion de « compression d'anneau » – voir plus loin et en annexe)

virtualisation par hyperviseur

micro noyau



Un hyperviseur de ce type est un fin micronoyau de virtualisation

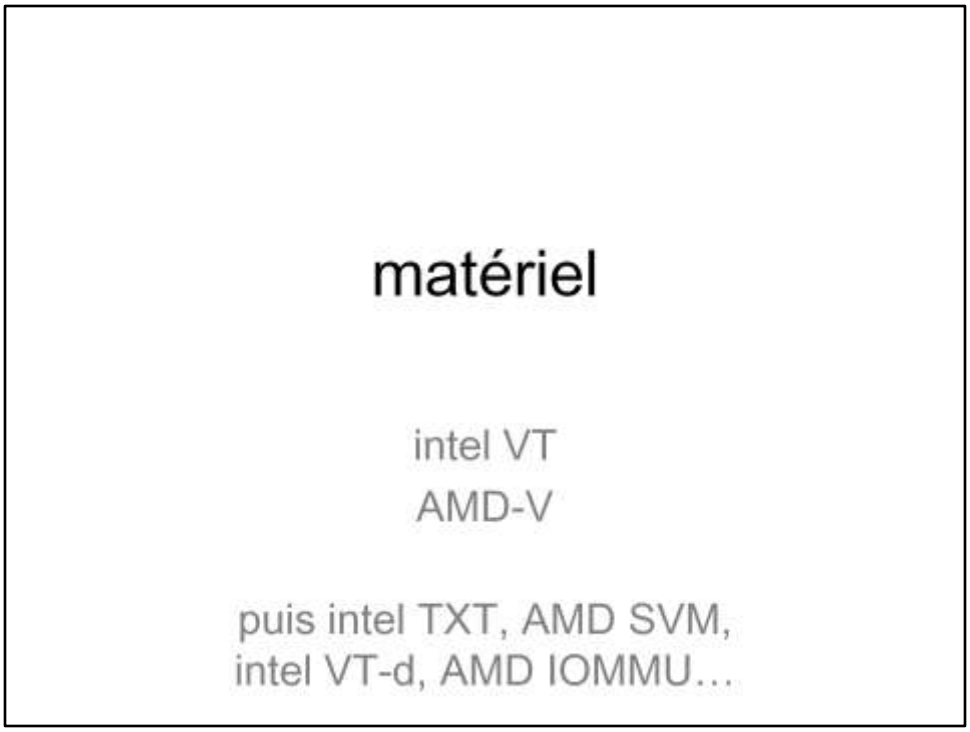
Le système est partitionné en machines virtuelles

Tout ce qui a pu l'être a été évacué au sein d'une partition spécifique dite « partition racine » (ou « parente »)

L'hyperviseur implémente la gestion des ressources des partitions, y compris l'ordonnancement (des cœurs) et la gestion de la mémoire

note :

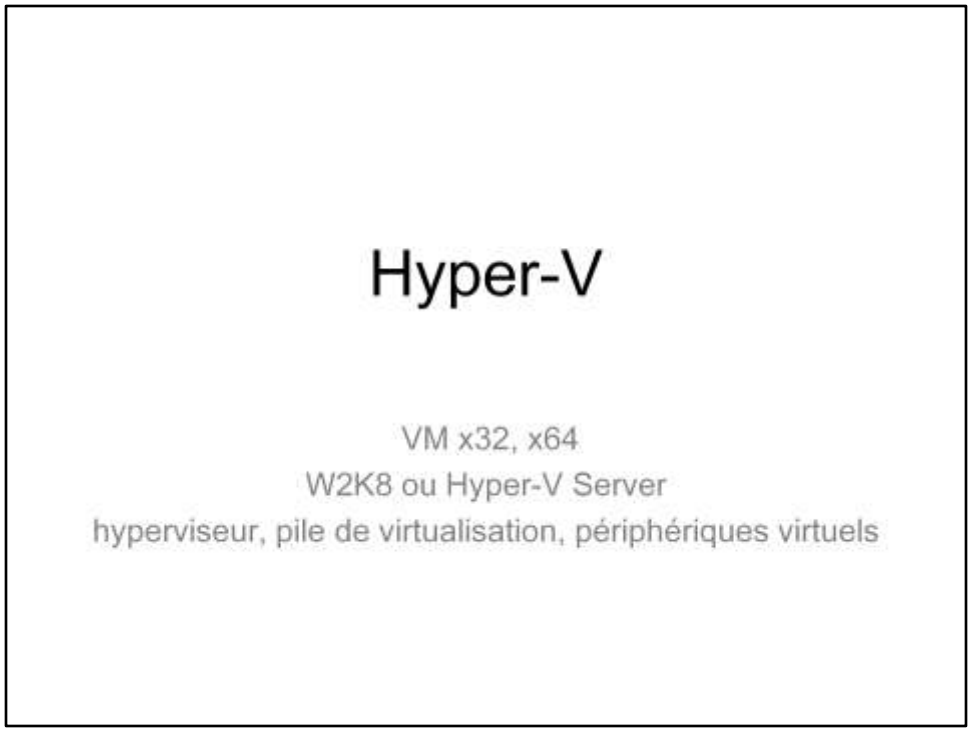
1 VMBus par VM vers la racine



extensions des CPU Intel VT et AMD-V ("monitor mode", sorte d'anneau -1)

extensions des CPU/chipsets Intel TXT et AMD SVM pour lancer un hyperviseur ou un VMM
DMA remapping (IOMMU) : device assignment support (protection against malicious DMA transfers)

hyperviseur = noyau de partitionnement (la partition est la frontière d'isolation; peu de fonctions de virtualisation, s'appuie sur une pile de virtualisation)
très fine couche logicielle (micronoyau, très fiable, base pour une TCB réduite)
pas de pilotes de périphériques (deux versions : Intel et AMD), pas de code de 3ce partie
les pilotes s'exécutent dans une partition (tire partie de la large base de pilotes disponibles pour Windows)
interface bien définie qui permet de créer la prise en charge de tout OS comme VM



Dans le cas d'Hyper-V
- La gestion et la configuration sont typiquement effectuées via un système d'exploitation maître s'exécutant au sein de la « partition racine »
- Les pilotes de périphériques s'exécutent au sein du système d'exploitation « racine »

virtualisation de machine pour des OS invités x32 ou x64, multiprocesseur…
rôle de Windows Server 2008 x64, également disponible séparément
3 composants majeurs : hyperviseur, pile de virtualisation, périphériques virtuels.

Composant de Windows Server 2008

- Version finale disponible
- S'installe comme un rôle sur *Server Core (*plus de détails dans la session « Virtualisation de machines : présent et futur ») ou sur un serveur complet

Dépend du support hardware pour pouvoir s'exécuter avec un niveau de privilège plus élevé que le *kernel* de la partition racine (on parle quelquefois d' « anneau -1 » pour le niveau d'exécution de l'hyperviseur)

- Elimine la compression d'anneau
- Supporté seulement sur Intel VT ou AMD-V
- Supporté seulement sur du hardware x64, support d'invités 32/64 bits

Avantages d'une partition racine Windows

- Compatibilité complète des pilotes de périphérique déjà existants
- Services de gestion
- Infrastructure de service
- Obligation du respect de la politique de ressource des invités

1.Hyperviseur
Le noyau de partitionnement
- La partition est la frontière d'isolation
- Peu de fonctions de virtualisation ; dépend de la pile de virtualisation

Très fine couche de logiciel

SÉCURITÉ DE HYPER-V

Objectifs

Protéger les clients de Microsoft en

- Réduisant le ***nombre*** de vulnérabilités
- Réduisant la ***gravité*** des vulnérabilités

Principes clés

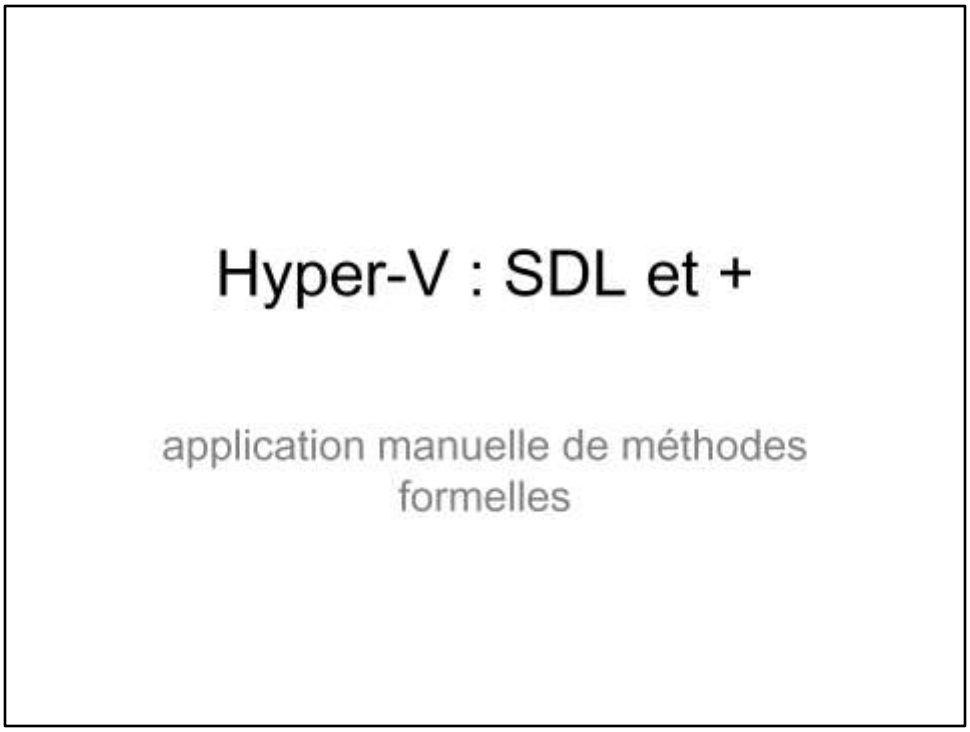
Prescriptif mais néanmoins pragmatique

Proactif – pas seulement de la "recherche de *bugs*"

Elimination en amont des problèmes de sécurité

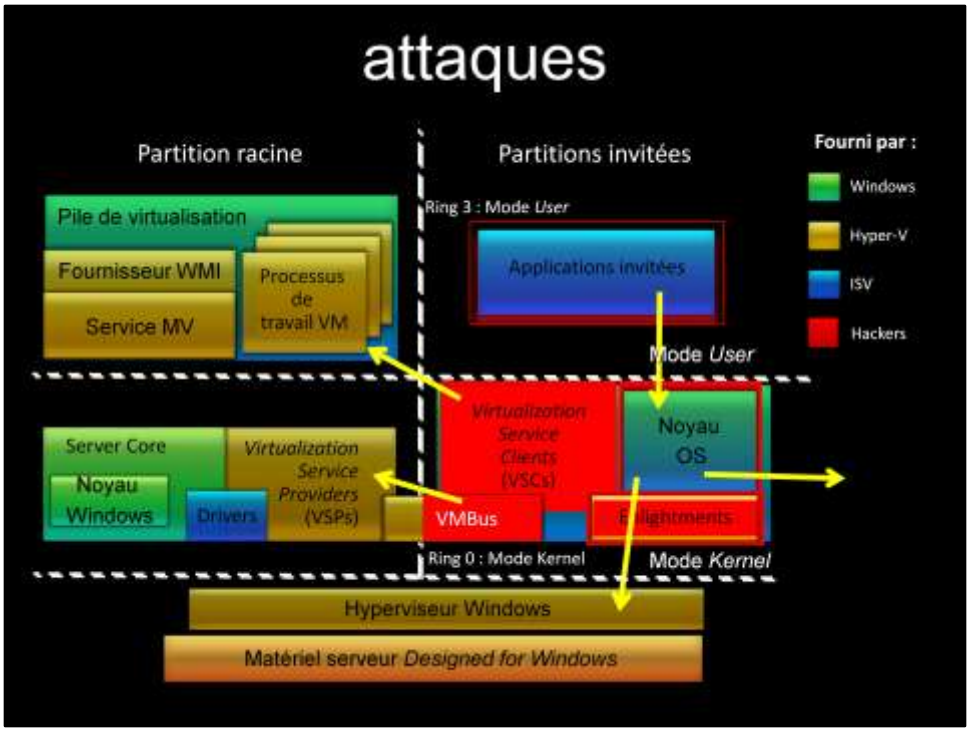
Sécurité par conception

Chez Microsoft, nous pensons que fournir des logiciels sécurisés nécessite
Engagement des dirigeants →SDL est un politique obligatoire chez Microsoft depuis 2004

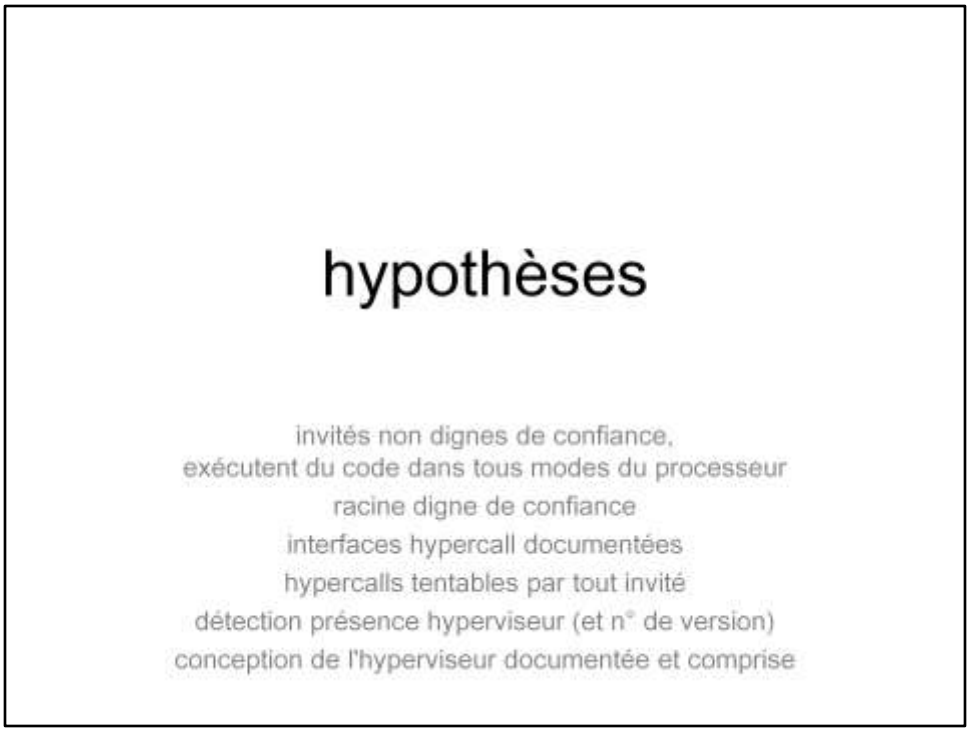


modèle formel du design et tests effectués sur la base du modèle
modèles formels des algorithmes les plus intéressants (notamment TLB virtualization) avant et pendant le développement
après développement : vérification mécanique de l'hyperviseur (code en C et assembleur)

les outils utilisés sont développés par l'EMIC en Allemagne et la plupart de l'annotation du code est faite par U. Saarbrucken



notes :
pas de partage de mémoire (chaque VM a son propre espace d'adressage)
pas de communication entre VM à part par le réseau
les VM ne peuvent pas faire d'attaque DMA car elles n'ont jamais accès directement au matériel
les VM et la racine ne peuvent pas écrire dans l'hyperviseur



Les invités sont indignes de confiance

La racine doit être digne de confiance pour les invités ainsi que pour l'hyperviseur (lancement, attaques DMA,…)

Le code au sein des invités peut s'exécuter dans tous les modes, anneaux et segments disponibles des processeurs

Les interfaces Hypercall (les API simples exposées par l'hyperviseur) seront bien documentées et donc largement utilisables pour les attaquants

- Ces spécifications sont disponibles en mode OSP (Open Specification Promise) en http://www.microsoft.com/downloads/thankyou.aspx?familyId=91e2e518-c62c-4ff2-8e50-3a37ea4100f5&displayLang=en

Tous les Hypercalls peuvent être tentés par les invités

On peut détecter que vous exécutez du code sur un hyperviseur

- On vous donnera même la version…

La conception interne de l'hyperviseur sera bien documentée et donc comprise

isolation : sécurité, pannes, resources
fiabilité : base de code minimale, conception strictement en couches, pas d'extensibilité
montée en charge : cœurs de CPU, mémoire gigantesque
l'hyperviseur ordonnance les cœurs (et pas les processeurs logiques, contenus dans des cœurs, contenus dans des processeurs physiques)

- Une isolation forte entre les partitions
- Protéger la confidentialité et l'intégrité des données des invités
- Séparation
  - Il y a des *pools* de ressources uniques de l'hyperviseur par invité
  - Il ya a des processus de travail séparés par invité qui gèrent l'état de chaque

CE QUI N EST PAS PRIS EN COMPTE (DU MOINS DANS CETTE VERSION)

Les choses que nous ne faisons pas au sein d'Hyper-V*

- Atténuer les fuites du hardware par transparence (attaques par inférence)
- Atténuer les canaux cachés
- Garantir la disponibilité
- Protéger les invités de la racine
- Protéger l'hyperviseur de la racine
- Utiliser du hardware digne de confiance
  - TPM, affectation de périphérique, protection DMA, lancement sécurisé

renforcement intégré

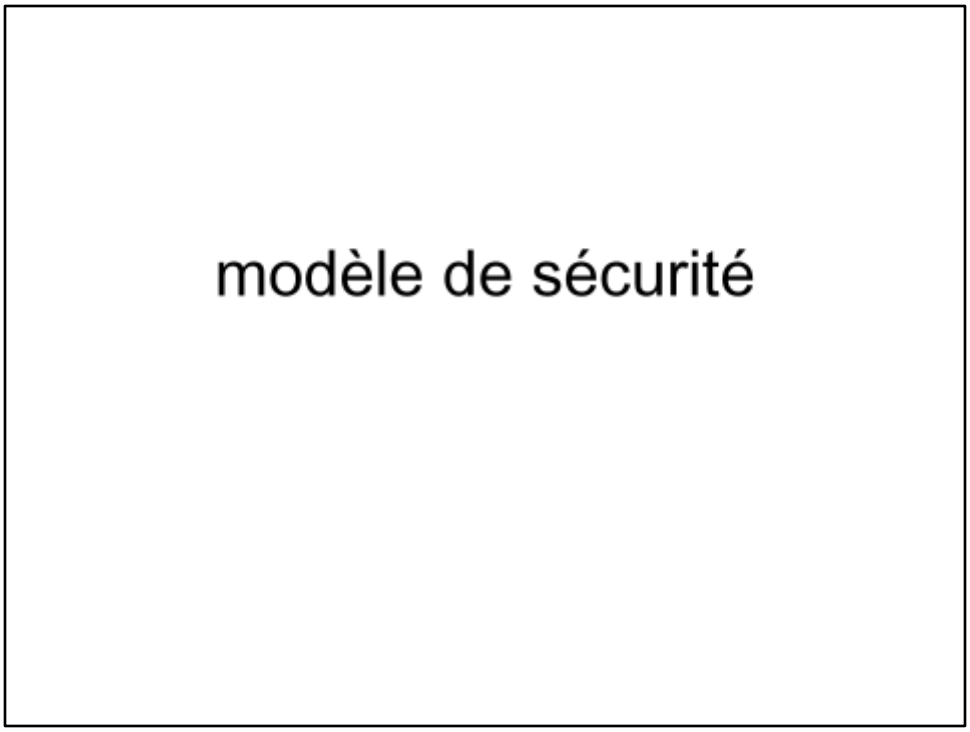
L'hyperviseur a un espace d'adressage séparé
- Les adresses des invités sont différentes des adresses de l'hyperviseur

Pas de code tiers au sein de l'hyperviseur
Un nombre limité de canaux depuis les invités vers l'hyperviseur
- Pas de chose du genre IOCTL
  - Un IOCTL (Input/output control) est un élément d'interface de type *user-to-kernel* ; les IOCTL sont utilisés typiquement pour permettre à un code en mode *user* de communiquer avec des périphériques ou des composants du noyau

La communication « invité à invité » à travers l'hyperviseur est prohibée
Pas de mémoire partagée mappée entre les invités
Les invités ne touchent jamais le hardware réel d'E/S

L'hyperviseur est construit avec
- Les *cookies* qui servent à protéger la pile (/GS)
- Le mode *Hardware No eXecute* (NX)
- Les pages de code marquées en lecture seule
- Des pages de garde mémoire
- Une gestion d'exception limitée
- Le binaire de l'hyperviseur signé

L'hyperviseur et la racine sont passés à travers SDL
- Modélisation des menaces
- Analyse statique
- Test de *fuzzing*
- Test de pénétration



Mémoire
- La mise en correspondance de l'adresse physique et de la partition est maintenue par l'hyperviseur
- Le modèle d'appartenance est de type parent/enfant sur la mémoire
- L'hyperviseur peut se superposer aux droits d'accès dans les tables de page des invités (R, W, X)

CPU
- Le hardware garantit l'isolation des caches et registres, le vidage du TLB, l'interception des instructions

E/S
- L'hyperviseur rend obligatoire la politique de sécurité du parent pour tous les accès des invités aux ports d'E/S
- La politique d'Hyper-V v1 est que les invités n'ont pas d'accès au véritable hardware

Interface hyperviseur
- Modèle de privilèges par partition
- Les invités ont accès aux hypercalls, aux instructions, aux MSR (*Model Specific Registers*) avec un impact en termes de sécurité qui est contrôlé en fonction de la politique de sécurité du parent
- La politique de sécurité d'Hyper-V v1 est que les invités n'ont pas d'accès aux instructions privilégiées

Utilise l'*Authorization Manager* (AzMan)
- Autorisation et contrôle d'accès avec un fin niveau de granularité
- Basé rôle et département (RBAC – *Role-Based Access Control*)
- Séparation claire du rôle d'administration des groupes de

VIRTUEL OU PHYSIQUE
SIMILARITÉS

ce qui ne change pas

déploiement et config technologies de sécurité
protection contre les attaques complexes
accès sécurisé aux biens matériels ou virtuels
gestion des identités et des rôles
maintien à jour des machines
visibilité sur l'état sanitaire
réponse à incident

- Deploying and properly configuring security technologies
- Protecting against complex attacks – securing virtual and physical machines
- Enabling secure access to virtual and physical assets based on policy
- Managing identities and their rights to manage physical and virtual machines
- Ensuring software running in virtual and physical machines remains up-to-date
- Getting critical visibility into security state into endpoints and virtual machines
- Responding to and remediating security issues

VIRTUEL OU PHYSIQUE
DIFFÉRENCES

ce qui change

sécuriser la couche virtualisation
(*hyperjacking*)
surface d'attaque plus grande
maintien à jour des machines éteintes
risque accru en cas de vol ou perte
isolation des VM
surveillance du trafic VM à VM

Securing the virtualization layer

- "Hyperjacking": Compromising hypervisor
- "Blue pill": Concept of installing rogue hypervisor
- Ensuring trusted platform on which virtual machines run

Increased attack surface and vulnerability potential

- Denial of service possible by compromising hypervisor
- Virtual "appliances" offer benefits but also potential vulns
- Ensuring offline virtual machines stay in compliance

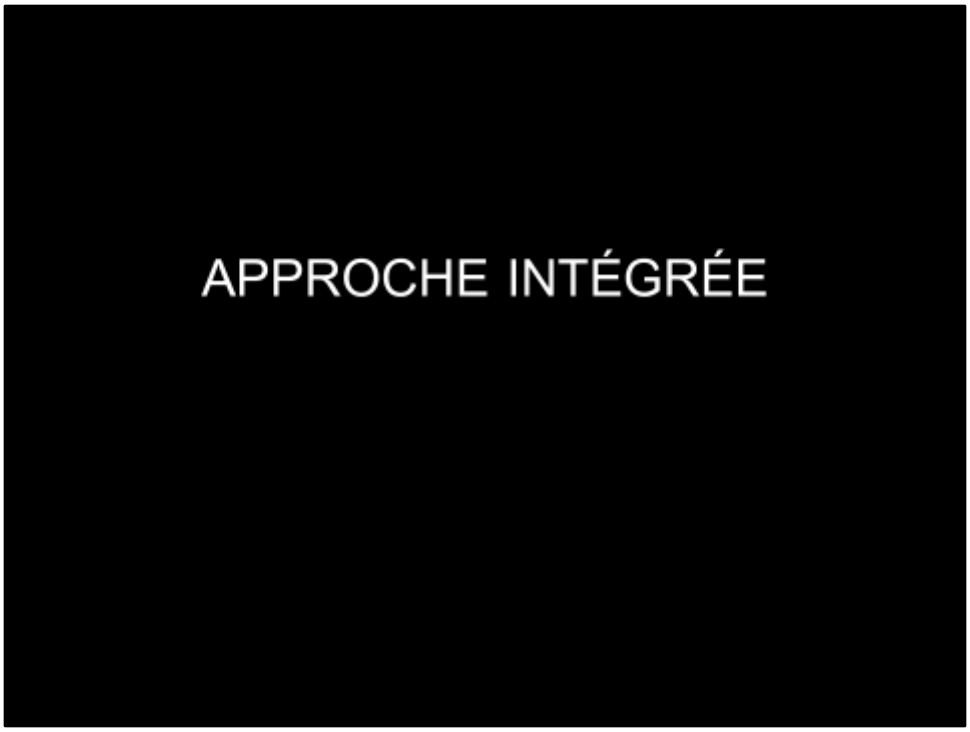
Increased asset concentration on devices

- If physical machine lost or stolen, so are the VMs on it

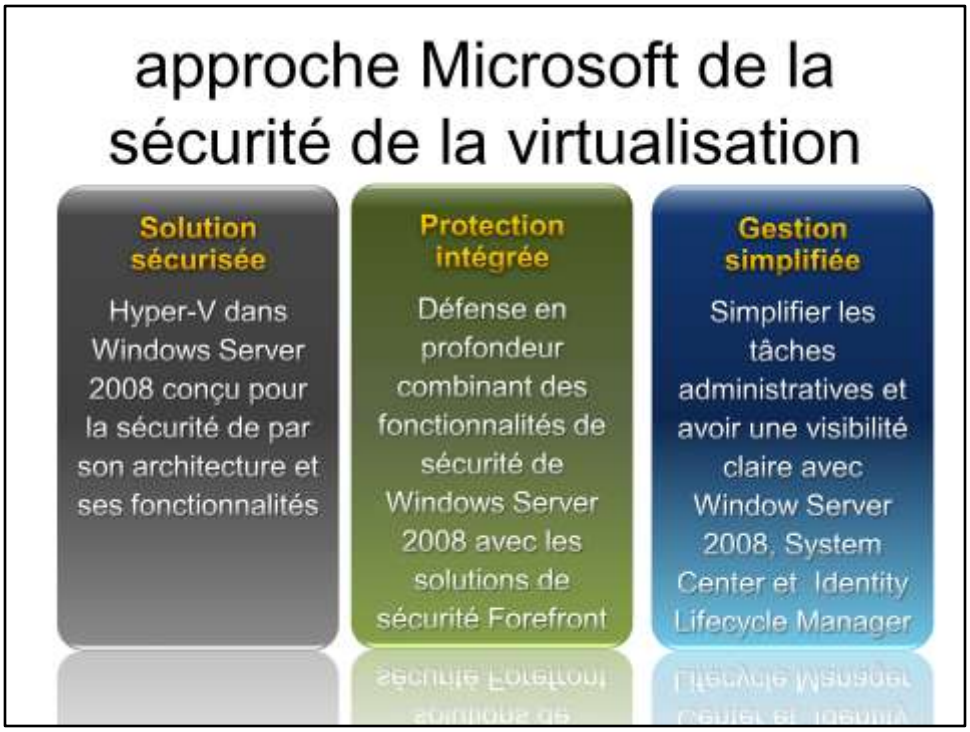
Isolating virtual machines from each other

Monitoring VM to VM traffic

- Only enabling communication where policies can be enforced



pour sécuriser les biens physiques et virtuels



We'll now talk in greater detail about each aspect of our integrated approach to virtualization security, covering three key areas:

- Secure computing solution: Windows Server 2008 and Hyper-V were designed to provide a secure computing platform across both physical and virtual environments, enabled through next-generation architecture and security features
- Integrated protection: We'll cover the integrated, defense-in-depth protection across physical and virtual environments that Microsoft delivers, combining Windows Server 2008 security features with complementary security solutions
- Simplified management: A secure environment is also a well-managed environment enabled through simplified administration and clear visibility. Lastly, we'll talk about virtualization management through Microsoft solutions – covering virtual machine administration, identity management, patching, and related areas.

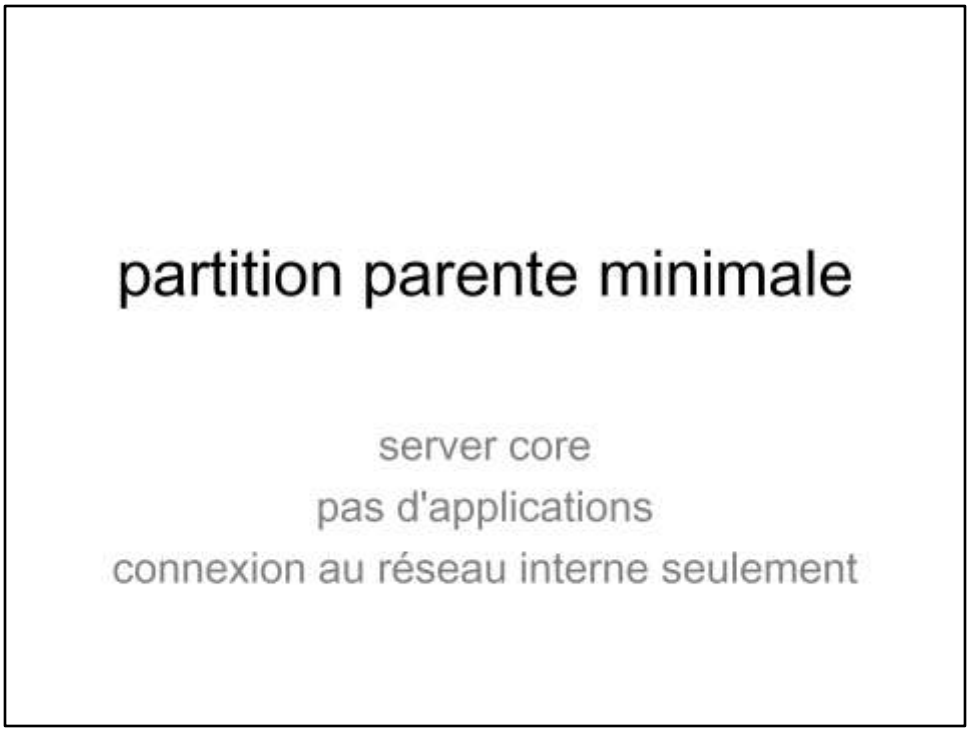
Hyper-V in Production
TAP, RDP & MSIT Hyper-V Deployments
Thousands of Hyper-V VMs in PRODUCTION
Windows Server 2003/2008 Roles:
File, Print, AD, RODC, IIS/Web, TS, Application Services, DHCP, DNS, WSS and more…
Microsoft Server Products:
SQL, Exchange, HPC, ISA, Sharepoint, Project Server, VSTS, BizTalk, Configuration Manager, Operations Manager, Virtual Machine Manager & more…

Hyper-V Stats:
Performance Blockers: ZERO
Deployment Blockers: ZERO
Application Compatibility Bugs: ZERO
Scalability Blockers: ZERO

Production
Hyper-V Powering Microsoft Internet Properties
TechNet: 100% Hyper-V
http://technet.microsoft.com
~1 million hits a DAY
MSDN:
http://msdn.microsoft.com
~3 million hits a DAY
Virtualizing TechNet & MSDN Whitepaper
http://download.microsoft.com/download/6/C/5/6C559B56-8556-4097-8C81-2D4E762CD48E/MSCOM_Virtualizes_MSDN_TechNet_on_Hyper-V.docx

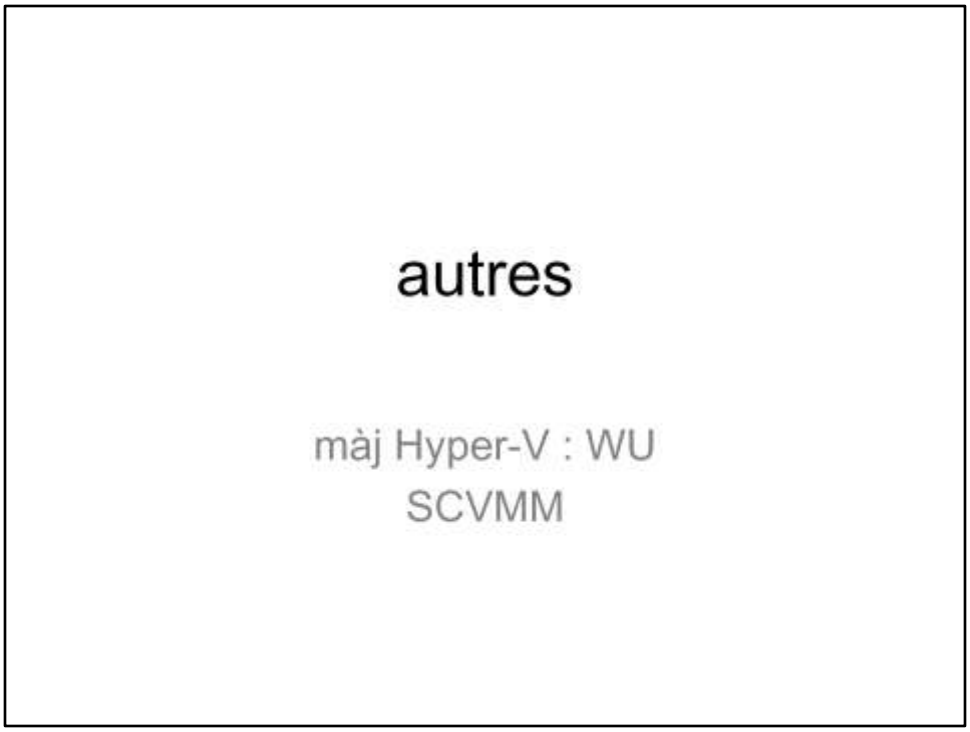
-Handles 15,000 requests per second
-1.2 billion page views per month
-280 million worldwide unique users per month
-~5000 content contributors internally
-300GB of contentAs of End of June 2008 –50% of workload is fully virtualizedDo you think

SCVMM



Minimiser les risques au sein de la partition racine

- Utiliser *Server Core*
  - Ne pas exécuter d'applications arbitraires, pas de navigation web
  - Exécuter vos applications et vos services dans les partitions invités
- Connecter uniquement au réseau interne
  - Exposer seulement les invités au trafic Internet



Patcher l'hyperviseur
- Windows Update

Gérer beaucoup de machines virtuelles
- Utiliser System Center Virtual Machine Manager

Deux machines virtuelles ne peuvent pas avoir le même degré d'isolation que deux machines physiques :

- Attaques par inférence
- Canaux cachés

Il n'est pas recommandé d'héberger deux machines virtuelles d'un niveau de confiance trop différents sur le même système

- Par exemple un serveur Web front-end et un serveur de certificats

migration Virtual Server vers Hyper-V

désinstaller les additions d'abord

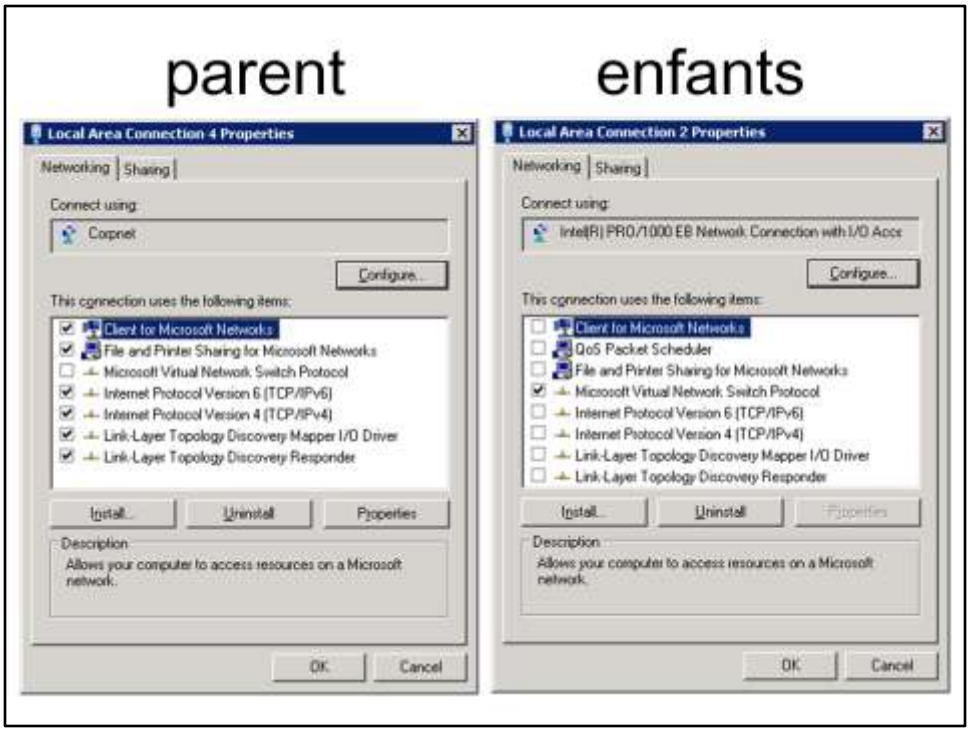
2 cartes réseau physiques mini

une pour la gestion

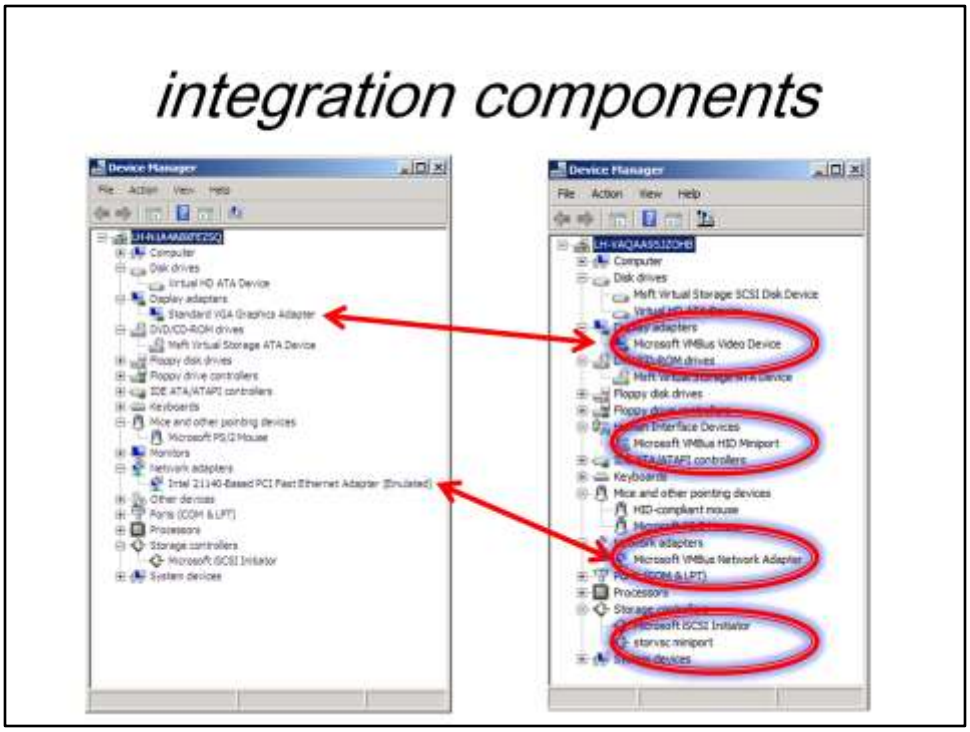
les autres pour les VM

iSCSI dédié

ne pas exposer l'hôte au trafic Internet


parent
enfants
Local Area Connection 4 Properties
Networking
Sharing
Connect using:
Corpnet
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Microsoft Virtual Network Switch Protocol
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
OK
Cancel
Local Area Connection 2 Properties
Networking
Sharing
Connect using:
Intel(R) PRO/1000 EB Network Connection with I/O Acce
Configure...
This connection uses the following items:
Client for Microsoft Networks
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Microsoft Virtual Network Switch Protocol
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
OK
Cancel

mise en Cluster



à ne pas oublier (ici émulation vs composants d'intrégation)

antivirus

parent : tout sauf .vhd
tous les enfants

BitLocker

autres bonnes pratiques

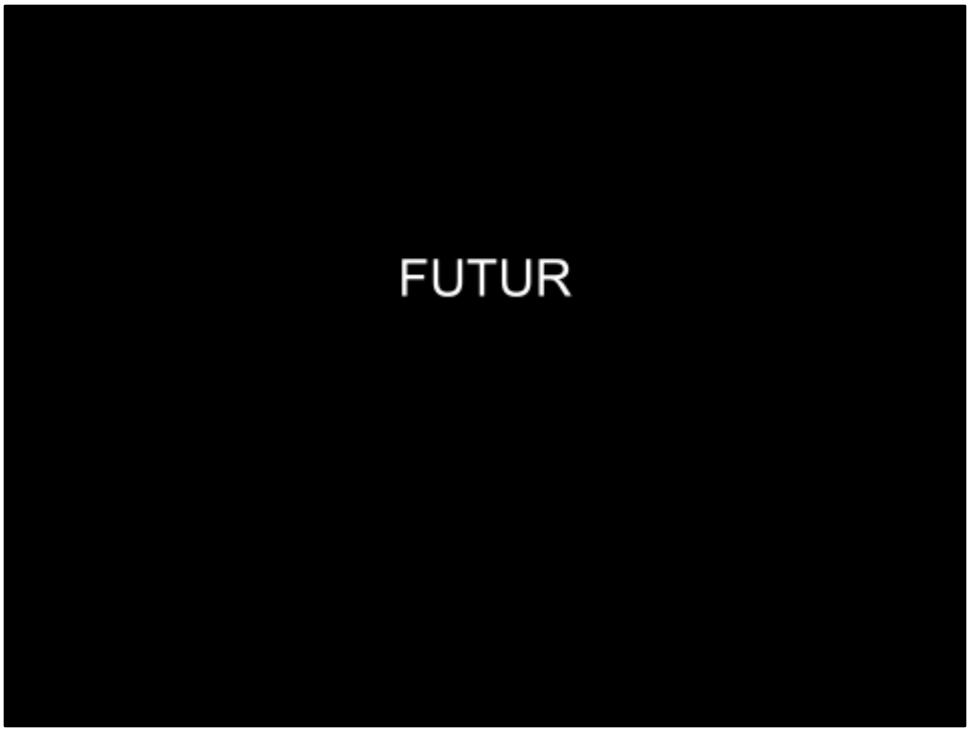
Mitigate Bottlenecks
- Processors
- Memory
- Storage
  - Don't run everything off a single spindle…
- Networking

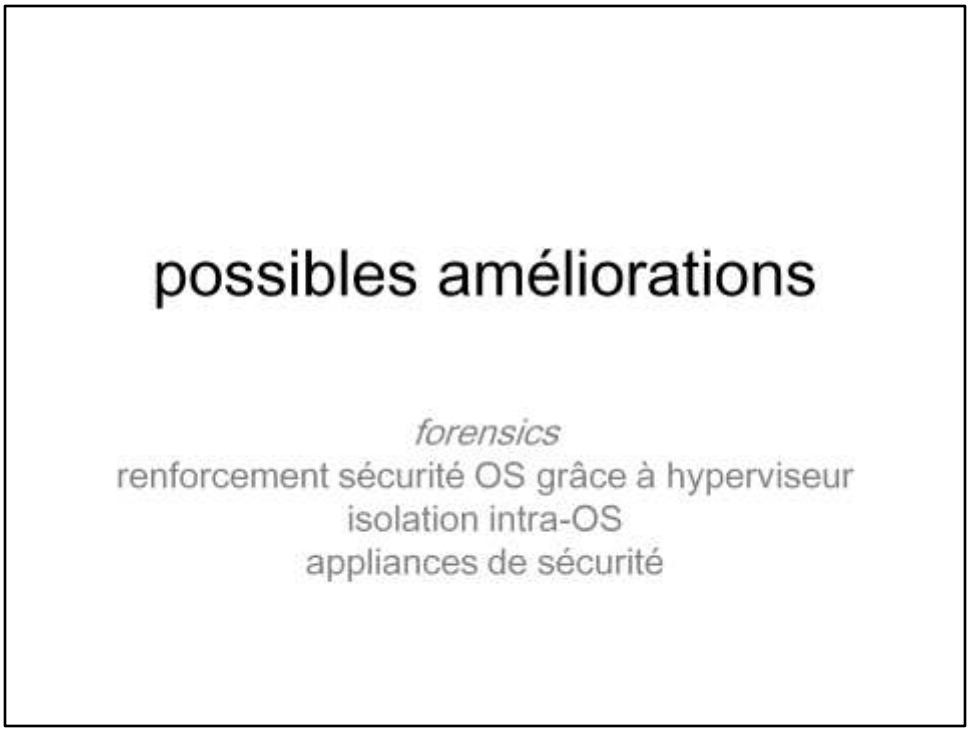
VHD Compaction/Expansion
- Run it on a non-production system

Use .isos
- Great performance
- Can be mounted and unmounted remotely
- Having them in SCVMM Library fast & convenient

CREATING VM
Use SCVMM Library
Steps:
1. Create virtual machine
2. Install guest operating system
3. Install integration components
4. Install anti-virus
5. Install management agents
6. SYSPREP
7. Add it to the VMM Library

Windows Server 2003
- Creat vms using 2-way to ensure an MP HAL


FUTUR



Il existe de nombreux types de virtualisation (applications, OS, machines) avec, à chaque fois, un niveau plus élevé d'isolation (et de surcoût)
La virtualisation constitue un outil puissant pour l'isolation et l'analyse de virus
Elle permet d'améliorer les capacités d'analyse *forensic* pour les systèmes d'exploitation compromis
Elle permet d'investir dans le renforcement de la sécurité des OS à travers les fonctionnalités des hyperviseurs
A le potentiel pour une meilleure isolation intra-OS (par exemple la séparation en *Ring 0* des drivers)
On peut tirer parti des machines virtuelles pour héberger des *appliances* de sécurité

La surveillance réseau MV à MV
Gérer le niveau de patch des systèmes d'exploitation des MV
La fuite d'informations entre les partitions en raison du matériel partagé
Une plus large surface d'attaque que les machines « normales »
Haute disponibilité – attaques des SLA
Menaces créées par les hyperviseurs malfaisants, non autorisés (*rootkits* en mode hyperviseur)

recherche de solutions

Lancement sécurisé

- Intel TXT™ (senter) et AMD SVM™ (skinit)
- Donne au propriétaire de la machine la possibilité de contrôler quel est le code qui peut utiliser le matériel de virtualisation
- Le matériel rend obligatoire le respect de la politique de sécurisé en bloquant le lancement d'hyperviseurs non autorisés
- Permet à des hyperviseurs de se protéger eux-mêmes contre la falsification

Remappage de DMA

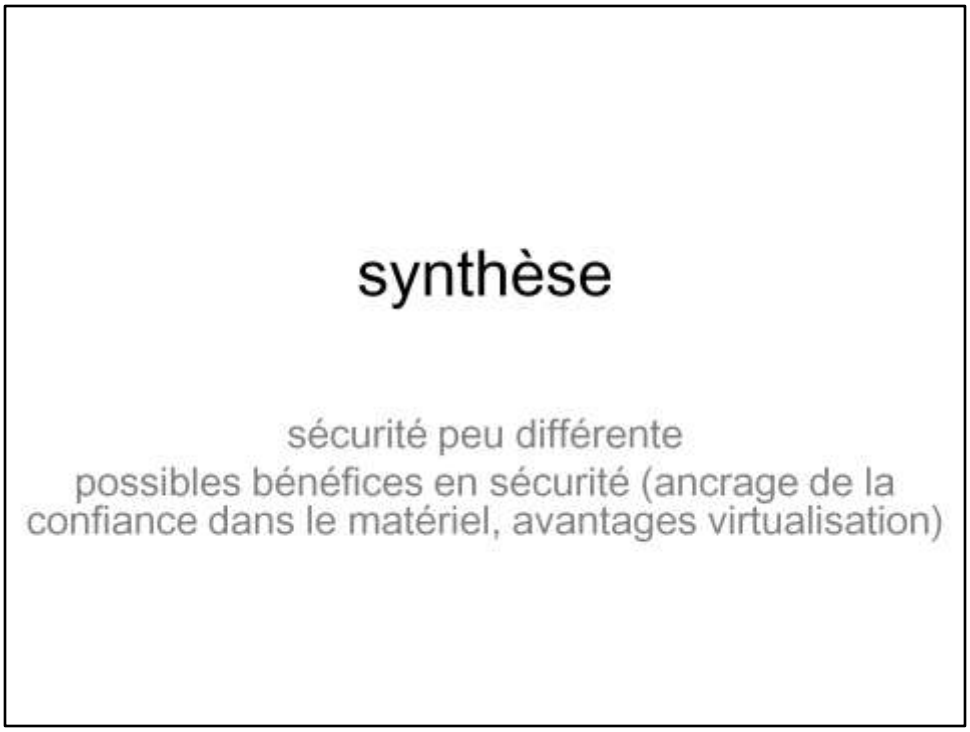
- Intel VT-d et AMD IOMMU
- Donne aux invités l'accès au véritable hardware pour leur permettre des accès hautes performances
- Permet à l'hyperviseur de se protéger lui-même contre des attaques de type DMA

(non commentée à l'oral)

Many things are similar in securing the virtual environment, but there are key differences

We're delivering an integrated, simplified approach to IT security across physical and virtual environments

- Secure computing platform: Hyper-V's architecture
- Integrated protection: WS08 + complementary Microsoft solutions (Terminal Services, Softgrid, Forefront)
- Simplified management: Hyper-V + System Center + Identity Lifecycle Manager + tools / guidance



La généralisation des machines virtuelles et des hyperviseurs va certainement poser des problèmes de sécurité mais ceux-ci ne sont pas fondamentalement différents de ceux qui existaient déjà
Les progrès du matériel permettent d'ancrer de plus en plus la confiance dans le matériel
La virtualisation permet d'envisager de futurs bénéfices en termes de sécurité

webcast de Bernard Ourghanlian et présentation complète de 70+ diapos