ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

Module : La Virtualisation

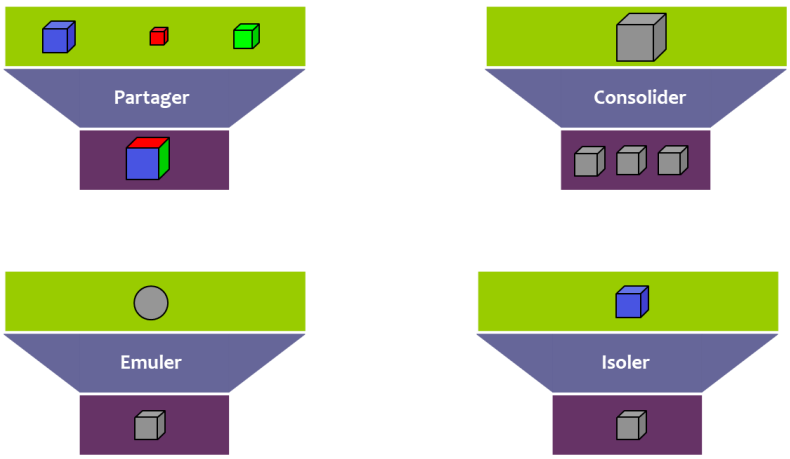
Filière : 4IIR
2024 - 2025
Pr M. Zbakh

Sommaire :

I. Principaux avantages de la virtualisation :

- **Optimisation des ressources :** Un serveur physique peut héberger plusieurs machines virtuelles, notamment le gaspillage de puissance de calcul.
- **Réduction des coûts :** Moins de matériel physique entraîne une baisse des coûts d'infrastructure de maintenance.
- **Flexibilité et évolutivité :** Déploiement, modification et suppression rapide des environnements en fonction des besoins.
- **Sécurité et isolation :** Chaque machine virtuelle fonctionne différemment, limitant les impacts en cas de panne ou d'attaque.
- **Facilité de gestion :** Grâce à des outils comme VMware, KVM, Hyper-V et OpenStack , l'administration des environnements virtualisés est simplifiée.

II. Les quatre raisons de la Virtualisation :



Partager :

Exemples : LPARs, VMs, virtual disks, VLANs

Avantages : Resource utilization, workload manageability, flexibility, isolation

Consolider :

Eemples : Virtual disks, IP routing to clones

Avantages : Management simplification, investment protection, scalability

Emuler :

Exemples : Arch. emulators, iSCSI, virtual tape

Avantages : Compatibility, software investment protection, interoperability, flexibility

Isoler :

Exemples : Spare CPU subst., CUoD, SAN-VC

Avantages : Continuous availability, flexibility, software investment protection

III. Types de Virtualisation :

1. Virtualisation de serveurs :

Concepts (déjà traité dans les chapitres précédents)

Il s'agit de l'ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine physique plusieurs systèmes d'exploitation et ou plusieurs applications, isolés les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.

La consolidation de serveurs permet de réduire le TCO (« Total Cost of Ownership » ou coût total de possession), le temps de maintenance, simplifier l'administration de l'infrastructure, sécuriser l'architecture systèmes et réseaux et mettre en œuvre des PRA.

2. Virtualisation du stockage :

La virtualisation du stockage consiste à regrouper les ressources de stockage pour une meilleure gestion et performance.

Elle désigne le regroupement (*pooling*) et l'abstraction de ressources de stockage physiques (SSD, disques durs, volumes RAID, NAS, bibliothèque de bandes, etc.) de manière à les présenter comme un espace de stockage unique et cohérent.

Pour cela, un système logiciel intercepte les demandes d'entrée/sortie (E/S) des machines physiques ou virtuelles et envoie ces demandes à l'emplacement physique approprié des dispositifs de stockage du pool.

Pour l'utilisateur, les différentes ressources de stockage qui composent le pool ne sont pas visibles, de sorte que le stockage virtuel apparait comme un seul lecteur physique, partage ou numéro d'unité logique (LUN) qui peut accepter des lectures et des écritures standard.

A. Objectifs de la virtualisation du stockage

À travers l'abstraction et le regroupement des ressources, la virtualisation du stockage vise un certain nombre d'objectifs.

Notamment :

- **Optimiser l'utilisation.** Elle permet d'améliorer l'utilisation des ressources de stockage disponibles dans les différentes baies de stockage ou les différents serveurs, en les centralisant et en les allouant aux différentes charges de travail selon leur besoin.
- **Simplifier la gestion.** Elle permet de faciliter l'approvisionnement, la migration et l'allocation du stockage à l'aide d'interfaces utilisateurs et d'API.
- **Améliorer la disponibilité.** Elle permet d'améliorer la protection des données contre les pannes grâce à de la redondance.
- **Améliorer l'évolutivité.** Elle permet d'étendre les capacités de stockage de manière flexible et sans interruption, en facilitant l'intégration de nouvelles ressources au sein de l'infrastructure existante.

B. Inconvénient de la virtualisation du stockage

Ces avantages ne sont pas gratuits. La virtualisation du stockage a également un certain nombre d'inconvénients.

Par exemple :

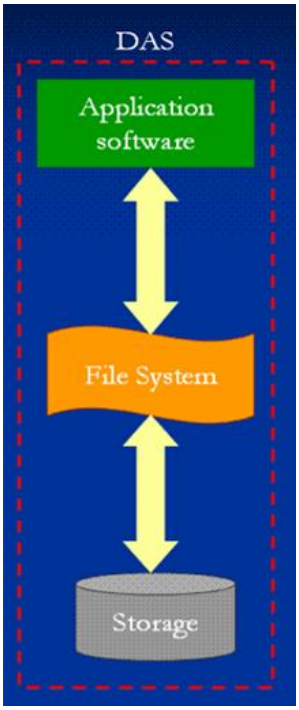
- **Complexité accrue.** La gestion des couches d'abstraction supplémentaires peut augmenter la complexité de l'infrastructure et nécessiter des compétences spécialisées pour l'administration.

- **Risques de sécurité.** L'unification des ressources et l'utilisation de systèmes logiciels peuvent créer des points de vulnérabilité uniques, et une mauvaise configuration peut exposer l'ensemble du stockage à des risques de sécurité.
- **Problèmes de performance.** L'ajout de couches virtuelles peut introduire une latence supplémentaire et des goulets d'étranglement, surtout si les ressources ne sont pas correctement dimensionnées ou optimisées.

C. Stockage local et virtualisation au niveau de l'hôte

Stockage local :

Le stockage local d'un ordinateur est composé de toutes les unités de stockage connectées directement à l'ordinateur (DAS ou *direct attached storage (Figure 1)*). Les principales interfaces sont:



DAS : Direct Attached Storage (DAS), càd d'un disque dur directement connecté à l'ordinateur qui utilise les protocoles ATA, SATA, eSATA, SCSI, SAS et Fibre Channel via des câbles dédiés

Figure 1 : Le stockage en DAS

- **SATA** (*serial ATA*) est une évolution du standard ATA (*Advanced Technology Attachment*) ou IDE qui était à l'origine une interface parallèle, et supporte des débits théoriques compris entre 1.5 et 6 Gbs selon la version.
- **SAS** (*serial attached SCSI*) est une évolution du standard SCSI (*Small Computer System Interface*) qui était également une interface parallèle, et supporte des débits théoriques compris entre 3 et 22.5 Gb/s selon la version.
- **NVMe** (*non-volatile memory express*) est une interface de communication qui permet d'utiliser au mieux la bande passante du bus PCIe (> 100 Gb/s).

Dans le cas des disques durs et des SSD bas de gamme, le débit est généralement limité par les disques. Les interfaces NVMe permettent d'utiliser pleinement les performances de SSD haut de gamme.

Unité de stockage physique :

Une unité de stockage physique peut être, par exemple :

- Un disque dur (hard disk drive ou HDD)
- Un disque électronique (solid-state drive ou SSD)
- Un volume RAID géré par un contrôleur matériel ou logiciel

Ces unités de stockage sont généralement des unités de stockage par bloc. Dans une telle unité, un bloc physique est la plus petite unité de mémoire adressable. La taille d'un bloc est fixée par le constructeur et est typiquement de 4096 octets dans les disques durs modernes et les SSD. Des unités plus anciennes peuvent encore utiliser des blocs de 512 octets.

Limite des unités de stockage physiques :

Il est possible d'installer un système de fichiers directement sur une unité de stockage Vierge. Toutefois, il est généralement nécessaire de subdiviser une unité en plusieurs partitions.

Chaque partition apparait comme une unité de stockage physique indépendante.

On utilise des partitions pour installer un système de fichiers différent (p. ex. FAT32 pour la partition de boot UEFI), ou pour éviter qu'un dépassement de capacité (p. ex., à cause des logs) n'affecte le fonctionnement du système d'exploitation (SE).

Le principal problème des partitions est qu'elles sont de taille fixe et qu'elles ne peuvent généralement pas être étendues en cas de besoin.

Une solution à ce problème est l'utilisation de la virtualisation du stockage dans le SE.

Virtualisation du stockage au niveau de l'hôte

La virtualisation du stockage au niveau de l'hôte consiste à virtualiser le stockage attaché à un hôte en utilisant son système d'exploitation. Les systèmes d'exploitation modernes disposent généralement d'outils permettant de virtualiser le stockage.

Par exemple :

- LVM (*logical volume manager*) sous Linux et NetBSD
- Storage Spaces sous Windows
- Core Storage sous macOS
- ZFS sous Linux et FreeBSD

Principe de la virtualisation du stockage au niveau de l'hôte

Tous ces systèmes reposent sur des principes similaires :

- Un volume physique (physical volume ou PV) est créé à partir d'une unité de stockage physique.

- Les volumes physiques sont regroupés en groupes de volumes (volume groups ou VG).
- Un groupe de volume peut être étendu dynamiquement par l'ajout d'un volume physique,
- Les volumes logiques (logical volume ou LV) sont des partitions d'un groupe de volume.
- Un volume logique peut être étendu dynamiquement tant qu'il y a de la place sur le groupe de volume.

Ces systèmes permettent également de créer des volumes redondants (RAID) et supportent généralement au moins la création de miroirs (RAID 1). Le ZFS n'utilise pas le RAID, mais dispose de fonctionnalités équivalentes.

Exemple : Logical Volume Manager sous Linux

Sous Linux, les volumes logiques apparaissent comme des dispositifs de type bloc dans le répertoire **/dev**. Les groupes de volume sont des répertoires (p. ex. **/dev/groupe1**) qui contiennent les volumes logiques (p. ex. **/dev/groupe1/data**) (Figure 2).

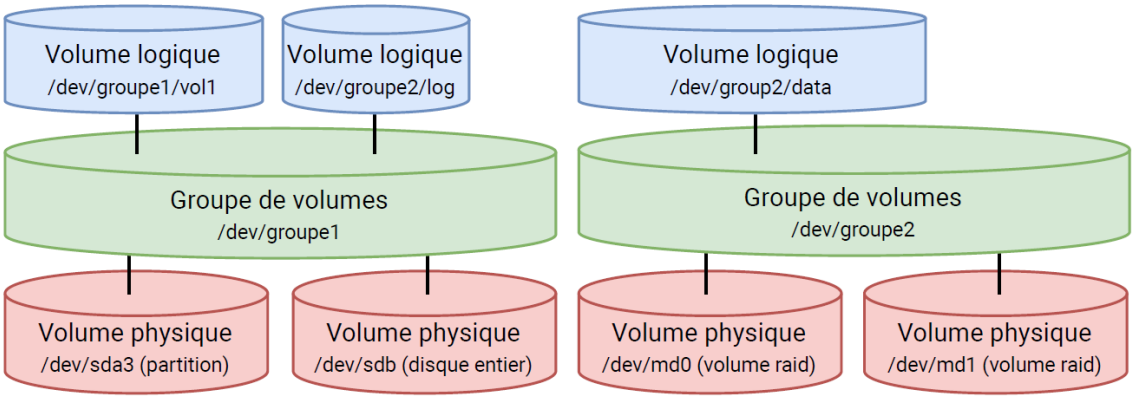


Figure 2 : Logical Volume Manager sous Linux

Snapshot

Les instantanés (snapshots) sont une fonctionnalité courante des systèmes de gestion de volumes logiques, qui permet de figer à un instant donné le contenu d'un volume de manière instantanée, grâce à la technique dite du *copy-on-write*. Cela signifie que les blocs ne sont pas copiés immédiatement, mais uniquement lorsque leur contenu est modifié.

Puisqu'il n'y a généralement pas de copie des données, un snapshot n'est pas à proprement parler une sauvegarde, mais il facilite la réalisation d'une sauvegarde cohérente, à chaud :

- Le système de sauvegarde prend un snapshot.
- Il copie le contenu du snapshot (qui est figé).
- Il supprime le snapshot.

L'espace de stockage nécessaire à un snapshot dépend de la fréquence des écritures et de la durée de vie du snapshot.

Snapshot — Illustration du *copy-on-write (Figure 3)*

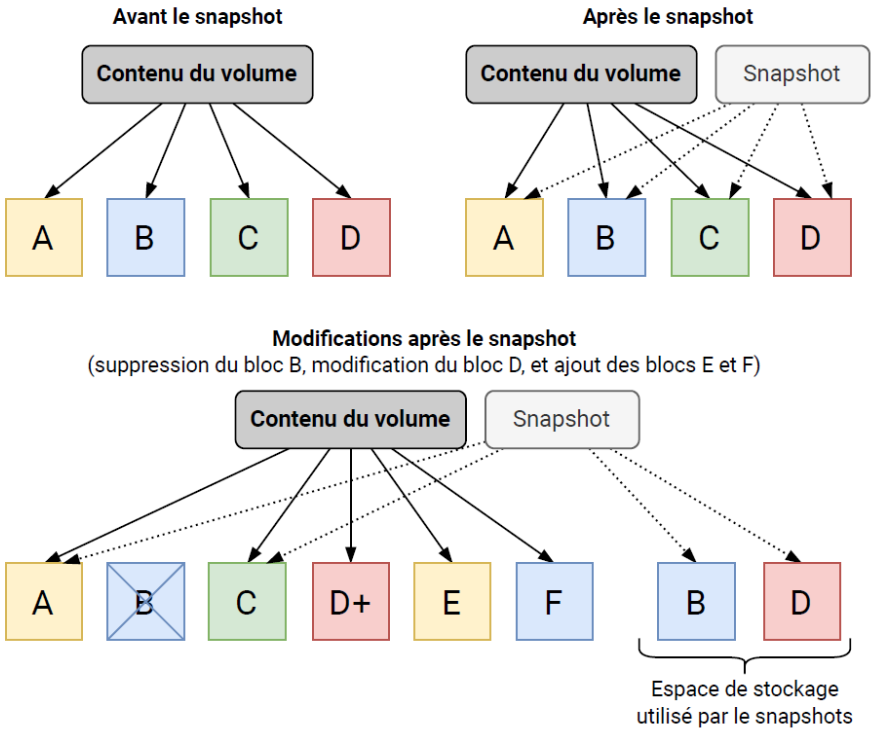


Figure 3 : Snapshot — Illustration du *copy-on-write*

D. Stockage centralisé

Problèmes du stockage local dans les serveurs

Dans le cas des serveurs, le stockage local pose plusieurs problèmes.

Il entraîne, par exemple :

- Une utilisation inefficace des ressources avec des capacités souvent sous-utilisées.
- Une complexité accrue pour la gestion et la sauvegarde des données.
- La nécessité d'une interruption de service lorsque les besoins de stockage dépassent la capacité disponible.

C'est pourquoi le stockage local est le plus souvent réduit à ce qu'il faut pour faire tourner le système d'exploitation et le reste est centralisé.

Stockage centralisé

La centralisation du stockage permet de résoudre ces problèmes en séparant le stockage des serveurs.

On peut distinguer au moins deux approche :

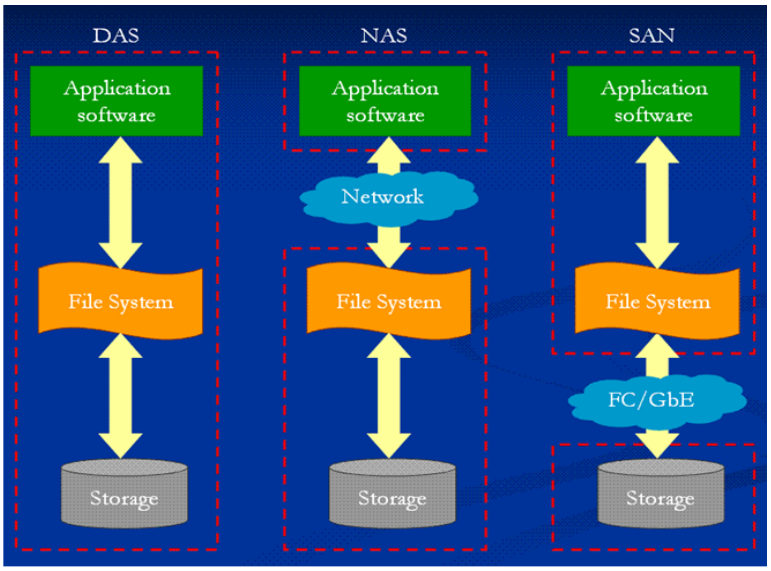
- La centralisation des dispositifs de stockage dans des baies de stockage, et la mise à disposition de volume logique à travers un réseau spécialisé appelé SAN (*storage area network (Figure 2)*).

- La centralisation de la gestion et de l'accès au stockage à l'aide d'un système de stockage distribué.

E. SAN, baies de stockage

Qu'est-ce qu'un SAN ?

Un SAN (Storage Area Network (Figure 4)) est un réseau dédié qui permet de connecter des serveurs à des unités de stockage partagées. Du point de vue de l'utilisateur, une unité de stockage du SAN à laquelle le serveur est connecté, apparait comme une unité de stockage par bloc locale.



Comparaison DAS/NAS/SAN:

- DAS : Direct Attached Storage (DAS), càd d'un disque dur directement connecté à l'ordinateur qui utilise les protocoles ATA, SATA, eSATA, SCSI, SAS et Fibre Channel via des câbles dédiés
- NAS : un serveur fournissant leurs fichiers à d'autres serveurs par le réseau
- SAN : est un réseau sur lequel circulent les données entre un système et son stockage

Figure 4 : Comparaison entre le stockage en DAS, NAS et SAN

Pour cela, les SAN utilisent des protocoles spécialisés comme FCP (*Fibre Channel protocol*) ou iSCSI. Ces protocoles supportent des vitesses de transfert élevées (jusqu'à plusieurs centaines de gigabits par seconde) et une faible latence.

En permettant la centralisation des ressources de stockage, un SAN facilite la gestion des ressources de stockage et permet d'en optimiser l'utilisation en allouant à chaque serveur ce dont il a besoin.

Qu'est-ce qu'une baie de stockage ?

Une baie de stockage (*storage array*) regroupe dans un même châssis, un ou deux serveurs spécialisés, appelés contrôleurs de stockage, et un relativement grand nombre (jusqu'à une centaine) d'unités de stockage physique (disques durs ou SSD).

Le contrôleur de stockage permet de créer et gérer les volumes RAID (typiquement RAID 6 ou RAID 10) et de mettre ces volumes à disposition sur le SAN. Chaque volume est identifié par un numéro appelé LUN (*logical unite number*).

Chaque volume peut être connecté à un ou plusieurs serveurs à travers un SAN.

Remarque : Un volume connecté à un serveur apparait comme une unité de stockage par bloc. Si plusieurs serveurs sont connectés à une même unité, il est important d'assurer que seul l'un d'entre eux peut y accéder en écriture, ou alors qu'un système de fichiers spécial appelé *clustered file system* est installé sur cette unité. Par exemple : VMware VMFS (*Virtual Machine File System*) ou Microsoft CSV (*Cluster Shared Volume*).

Exemples de baie de stockage (Figure 5)

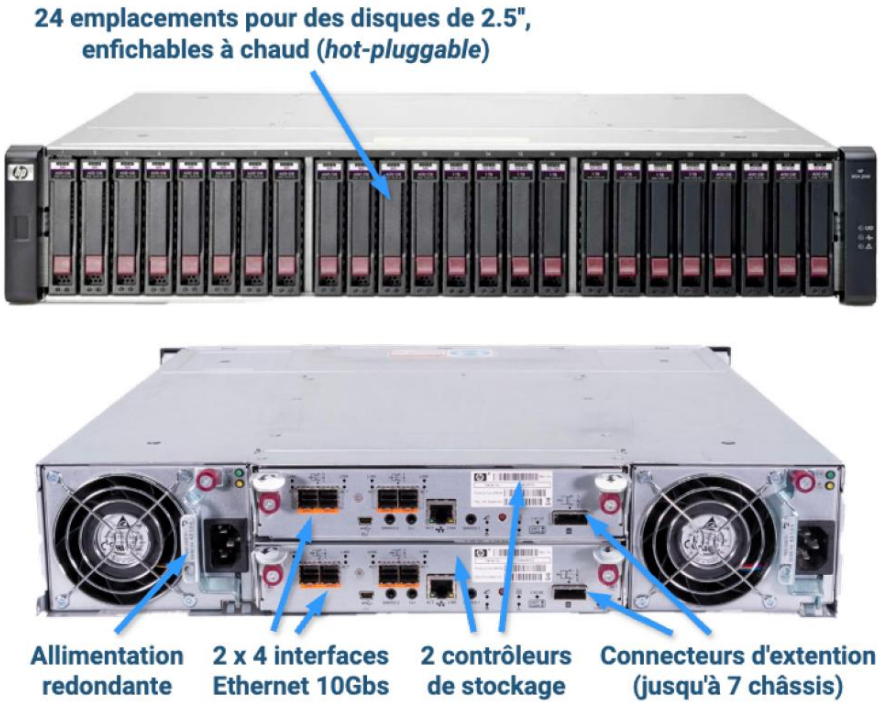


Figure 5 : Exemples de baie de stockage

Protocoles des SAN

Aujourd'hui, les débits élevés et la faible latence de l'Ethernet permettent sa mise en œuvre dans un SAN, mais cela n'a pas toujours été le cas. C'est pourquoi beaucoup de SAN utilisent plutôt le **Fibre Channel (FC)**, un type de réseau spécialement conçu pour le stockage.

Les principaux protocoles utilisés pour connecter un LUN à un serveur sont :

- **FCP** est une implémentation du protocole SCSI pour le réseau FC. Ce protocole peut également être utilisé sur un réseau Ethernet avec FCoE (*Fibre Channel over Ethernet*).
- **iSCSI** qui permet d'utiliser le protocole SCSI sur un réseau TCP/IP.
- **NVMe-oF** (*NVMe over fabric*) qui permet d'utiliser le protocole NVMe au-dessus d'un réseau FC ou Ethernet.

Pour utiliser ces protocoles, un serveur peut être équipé d'une carte réseau spéciale appelée HBA (*host bus adapter*) qui prend en charge une grande partie du protocole pour épargner les ressources du serveur.

LAN et SAN

Dans tous les cas, LAN et SAN sont des réseaux distincts pour éviter les interférences entre les différents types de trafic (Figure 6).

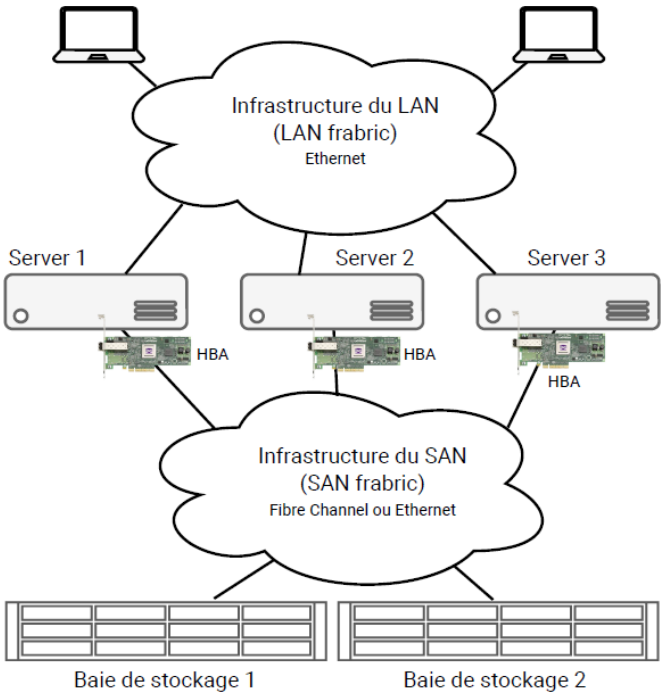


Figure 6 : Les réseaux LAN et SAN

Virtualisation au niveau de la baie de stockage

Avec un SAN, la virtualisation du stockage peut être mise en œuvre dans la baie de stockage. Puisqu'un contrôleur de stockage n'est rien d'autre qu'un serveur, le principe n'est pas très différent de celui de la virtualisation au niveau de l'hôte.

Dans un contrôleur de stockage, le logiciel de virtualisation permet typiquement :

- D'agréger plusieurs volumes RAID (les volumes physiques) en un **groupe de volumes**.
- De créer des **volumes logiques** de taille variable dans un groupe de volumes.
- D'étendre la capacité de ce volume logique tant qu'il reste de la place dans le groupe de volume.
- D'étendre la capacité d'un groupe de volume en ajoutant un volume physique à ce groupe.
- De réaliser des snapshots (instantané) d'un volume, pour conserver une copie de son contenu à un instant donné.

Schéma de principe (Figure 7)

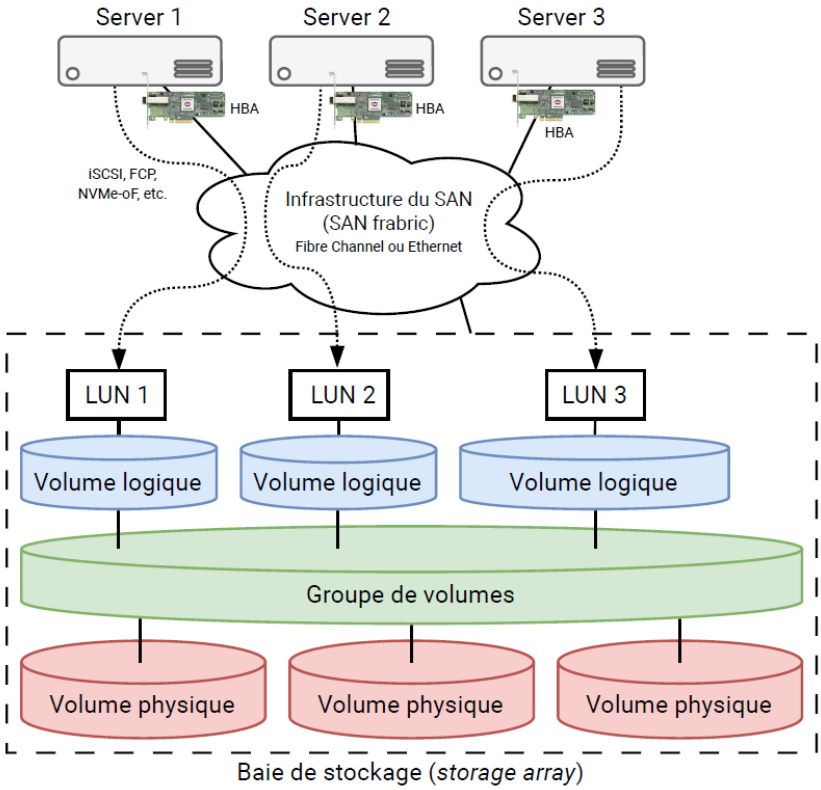


Figure 7 : Schéma de principe

Avantage et inconvénients

En plus de faciliter grandement la gestion des unités logiques, par rapport à l'utilisation de volumes physiques de taille fixe, comme dans le cas de la virtualisation du stockage au niveau de l'hôte, la virtualisation du stockage au niveau de la baie de stockage offre les avantages suivants :

- Centralisation de la gestion du stockage.
- Performance du logiciel optimisé pour le matériel.

Les principaux inconvénients de cette solution sont qu'elle repose sur du logiciel propriétaire, et qu'elle n'offre pas d'interface de gestion unifiée.

De plus, certaines fonctionnalités avancées, comme le stockage hiérarchisé (*tired storage*), peuvent être verrouillées et nécessiter l'achat de licence supplémentaire pour être activées.

F. Système de stockage distribué

Plutôt que de centraliser les disques dans des baies de stockage connectées avec un réseau spécialisé, une autre option est d'utiliser un système logiciel pour rendre la capacité des disques des différents serveurs, disponible sous la forme de volume, de pool d'objets, de partage, etc., accessible des moyens tels que iSCSI, API REST, SMB, NFS, etc.

Le stockage distribué est rendu possible par les débits importants et la faible latence des réseaux Ethernet.

Parmi les implémentations de stockage distribué, on peut mentionner :

- Red Hat Ceph (stockage par objet, par bloc, et par fichier)
- Red Hat Gluster (stockage par bloc et par fichier)
- SUSE Longhorn (stockage par bloc)
- StarWind VSAN (stockage par bloc)
- VMware vSAN (stockage par bloc)

Schéma de principe d'un système de stockage distribué (Figure 8)

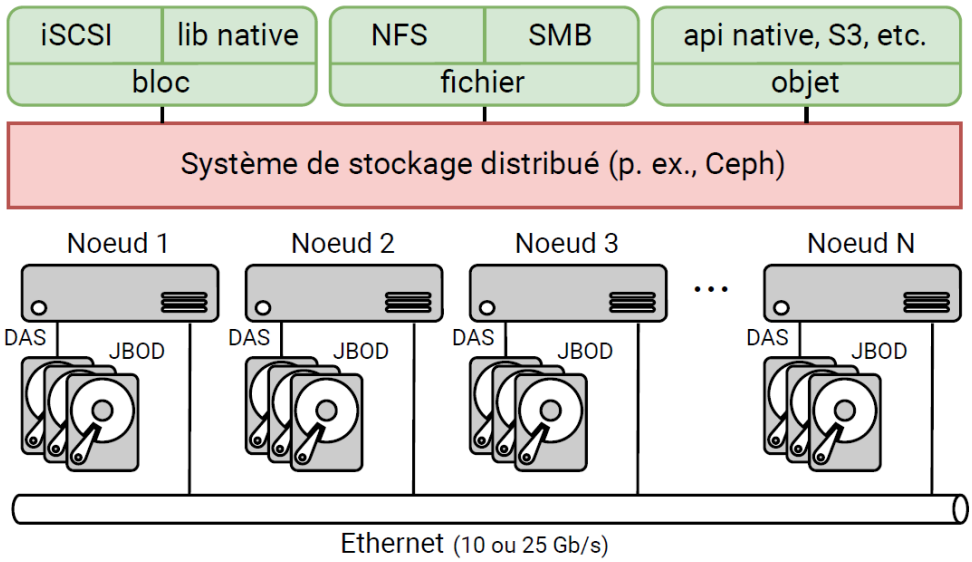


Figure 8 : Schéma de principe d'un système de stockage distribué

Grappe de serveurs et redondance

Pour assurer la disponibilité des données, un système de stockage distribué ne repose pas sur le RAID, mais sur la copie des données sur au moins trois hôtes différents d'une grappe de serveur (*cluster*). Il est possible d'augmenter le nombre de copies pour augmenter la tolérance de panne, mais on ne devrait pas utiliser moins de trois copies en production.

Pour réaliser une grappe de stockage distribuée avec trois copies, il est nécessaire d'avoir au moins trois nœuds (serveurs) équipés d'au moins un disque. Pour cinq copies, il est nécessaire d'avoir au moins cinq nœuds.

- Avec trois copies, la grappe continue à fonctionner en cas de panne d'un nœud.
- Avec cinq copies, la grappe continue à fonctionner en cas de panne de deux nœuds.
- Au-delà, il n'y a aucune perte de données, mais la grappe n'est plus en mesure de traiter de nouvelles requêtes.

Contrôleur de la grappe

Le système de stockage distribué nécessite un processus de contrôle, qui assure que les données sont bien répliquées dans les différents hôtes et qui maintient un index pour en mesure de retrouver ces données. Pour que la grappe fonctionne correctement, il doit y avoir à tout instant un et un seul contrôleur actif dans la grappe.

Pour avoir une grappe à haute disponibilité (high availability cluster ou HA cluster), qui continue à fonctionner en cas de panne, il est nécessaire d'avoir au moins un autre nœud avec un contrôleur secondaire qui maintient un réplica de l'index du contrôleur actif et qui est prêt à prendre le relai.

Pour assurer qu'il n'y ait qu'un contrôleur actif, ce contrôleur doit être élu, et pour assurer la cohérence des données, cette élection ne peut avoir lieu que s'il y a un nombre minimal de votants. Ce nombre minimal de votants est appelé quorum.

Dans un système distribué, le plus petit quorum est de deux. Pour assurer la disponibilité en cas de panne d'un nœud, il doit donc y avoir trois contrôleurs répartis sur trois nœuds.

Théorème CAP

Une grappe de serveurs est une forme de système distribué, c'est-à-dire un système qui utilise des ressources de différentes machines pour produire un résultat.

Selon le théorème CAP, un tel système ne peut assurer que deux des trois propriétés suivantes :

- Cohérence (*Consistency*)
- Disponibilité (*Availability*)
- Tolérance au partitionnement (*Partiton tolerance*)

Dans le cas d'un système de stockage distribué, la cohérence est primordiale. Il s'en suit que le système ne sera pas disponible (ou disponible en mode dégradé) dans le cas d'un partitionnement à cause de la panne d'un serveur ou du réseau.

Split-brain

Dans le cas d'une défaillance d'un équipement ou d'un câble réseau, il est possible que le réseau soit partitionné.

Faisons les hypothèses suivantes :

- Chaque partition contient une partie de la grappe

- Chaque partie de la grappe est accessible par une partie des clients

Pour chaque partie de la grappe, les nœuds de l'autre partie sont hors-ligne.

Si chaque partie de la grappe procède à l'élection d'un nouveau nœud actif, on se retrouve avec deux contrôleurs actifs. Mais comme ces contrôleurs ne peuvent pas communiquer entre eux, la cohérence des données n'est plus assurée.

Cette situation est appelée un ***split-brain*** et doit absolument être évitée.

Quorum

Comme nous l'avons déjà dit, un quorum est le nombre minimal de votants pour qu'un vote puisse avoir lieu.

Pour éviter un *split-brain* il faut :

- un nombre impair de nœuds dans la grappe
- un quorum correspondant à la moitié des nœuds + 1.

Avec trois nœuds et un quorum de deux :

- Avec un groupe de deux nœuds et un nœud isolé, seul le groupe de deux pourra élire un contrôleur actif.
- Avec trois nœuds isolés, aucune élection n'est possible.

De cette manière, on assure qu'il n'y a jamais plus d'un nœud actif.

Avantage et inconvénients

En plus des avantages d'un SAN avec des baies de stockage, un système de stockage distribué présente les avantages suivants :

- Réduction du risque d'enfermement propriétaire par l'utilisation de matériel courant (serveurs, ssd, disques durs) et hétérogène.
- Haute disponibilité et sécurité élevée.
- Support d'API standards comme l'API de S3 en plus d'interfaces plus traditionnelles comme iSCSI.
- Extensibilité quasi illimitée. Par exemple, en 2023, le CERN possède 17 cluster pour un total de 100 Po

Mais il peut également présenter quelques inconvénients :

- Coût élevé pour un petit cluster (seulement 1/3 du stockage disponible avec 3 nœuds).
- Plus complexe à mettre en œuvre et à gérer qu'un solution propriétaire.

Exemple d'un cluster Ceph (Figure 9)

L'image ci-contre montre une partie d'un cluster Ceph qui se trouve au CERN. Dans chaque rack, on voit deux châssis de 4 serveurs, et un châssis de 24 disques par serveur. Un groupe de 24 disques, appelé JBOD (*just a bunch of disk*), est connectés directement à chaque serveur (DAS ou *direct attached storage*).

Figure 9 : Exemple d'un cluster Ceph

G. Différents types de services de stockage

La centralisation et la virtualisation du stockage permettent d'optimiser l'allocation de la bonne capacité de stockages pour chaque charge de travail de l'infrastructure.

Mais cette capacité de stockage peut être mise à disposition de différente manières. On peut en distinguer au moins trois type de services :

- Service de stockage par bloc (*block storage*).
- Service de stockage par fichier (*file storage*).
- Service de stockage par objet (*object storage*).

Service de stockage par bloc

Un service de stockage par bloc présente une capacité de stockage sous la forme d'une unité de stockage par bloc qui apparait au système d'exploitation d'un serveur ou d'une machine virtuelle (VM) comme un disque local.

- Disque de démarrage (*boot drive*). Un serveur démarre sur disque local dans lequel est généralement installé le système d'exploitation.
- Ce type de stockage est également celui qui offre les meilleures performances (débit et opération d'E/S par seconde) et la plus faible latence.

Une unité de stockage par bloc ne peut pas être utilisée simultanément par plusieurs serveurs. Si une unité est connectée à tous les nœuds d'une grappe (*cluster*), il faut :

- Installer un système de fichiers pour cluster (*clustered file system*) sur cette unité.
- Assurer qu'à tout instant un seul serveur de la grappe ait le droit d'écrire sur cette unité.

Machine virtuel et disque virtuel

Comme pour un serveur physique, une machine VM démarre sur un disque local.

- Pour assurer de bonnes performances pour une VM, l'accès au disque doit être rapide et sûr.
- L'émulation n'est donc pas une option.
- Lorsque c'est possible, un accès direct à un volume physique ou virtuel de l'hôte est la meilleure option.
- Lorsque ce n'est pas le cas, la paravirtualisation est une très bonne seconde option. Le principe consiste à installer dans l'SE invités, un pilote qui accède à une image du disque virtuel en communiquant directement avec l'hyperviseur.

Image de disque virtuel

Une image de disque virtuel prend la forme d'un fichier stocké dans un système de fichiers accessible par l'hyperviseur.

Les principaux formats d'image de disque virtuel sont :

- **VMDK** (*Virtual Machine Disk*) : VMware WorkStation et ESXi
- **VHD** et **VHDX** (*Virtual Hard Drive*) : Microsoft Hyper-V
- **VDI** (*Virtual Disk Image*) : Oracle VirtualBox
- **Qcow2** (*Qemu copy-on-write*) et raw : KVM

Système de fichiers

En dehors de quelques cas particuliers, principalement des SGBD (Oracle, DB2, SQL Server, etc.), qui utilisent des partitions 'raw' pour optimiser les performances des E/S, il est assez rare qu'une application utilise directement une unité de stockage par bloc.

Le plus souvent, on installe un système de fichiers (p.ex., ext4 sous Linux, NTFS sous Windows, etc.) sur l'unité de stockage pour en faciliter l'utilisation :

- Un fichier est un ensemble de blocs, pas forcément contigu, associé à des métadonnées (nom, date de création, date de modification, etc.) et des attributs.
- Un répertoire est un fichier spécial dont le contenu est une liste de liens vers d'autres fichiers et répertoires, qui permet d'organiser les fichiers de manière hiérarchique.
- Les métadonnées et les attributs sont stockés de manière centralisée, indépendamment des données, dans une structure maintenue par le système de fichiers, par exemple, la *inode table* dans ext4 ou la *master file table* dans NTFS.

Avantages d'un système de fichiers

Parmi les avantages d'un système de fichier, on peut mentionner :

- **Facilite le nommage des fichiers.** Le nom d'un fichier doit être unique dans le répertoire où il se trouve, mais il n'a pas à être unique dans tout le système de fichier. Le chemin complet d'un fichier permet de l'identifier de manière unique dans le système de fichier.
- **Facilite la gestion des blocs**. Le système de fichier gère l'allocation et la libération des blocs pour augmenter ou réduire la taille d'un fichier lorsqu'on le modifie, ainsi que l'enchaînement des blocs non contigus.
- **Interface universelle**. Même si chaque système de fichiers a ses spécificités, l'interface d'accès est essentiellement toujours la même. Cela permet d'exposer tout ou partie d'un système de fichier à l'aide de protocole standard tel que SMB ou NFS à travers un réseau.

Serveur de fichiers et NAS

Un serveur de fichiers (*file server*) est un serveur qui partage un ou plusieurs répertoires de son système de fichier à travers un réseau à l'aide d'un protocole tel que SMB ou NFS.

Par rapport à une unité de stockage par bloc, un répertoire partagé (*shared folder*) :

- Peut être utilisé simultanément par plusieurs serveurs.
- A des débit souvent plus faible et une latence généralement plus élevé.
- Ne peut pas être utilisé comme disque de démarrage.

Un NAS (Network Attached Storage (Figure 2)) est un serveur optimisé pour le stockage et le partage des fichiers sur un LAN.

À la maison ou dans une petite entreprise, un NAS se présente souvent sous la forme d'un serveur « tout en un » avec un SE propriétaire géré via une interface web, utilisé pour exécuter diverses charges de travail supplémentaires (sauvegarde, serveur multimédia, etc.).

Service de stockage par fichier

Dans le cloud, un service de stockage par fichier (*file storage service*) permet de présenter une capacité de stockage de la même manière qu'un répertoire partagé sur un serveur de fichier ou un NAS.

Cela permet de migrer des données sur le cloud sans changer les habitudes des utilisateurs ou en maintenant la compatibilité avec des applications existantes.

Parmi les principaux cas d'utilisation des services de stockage par fichier, on peut mentionner :

- Collaboration, partage et diffusion de fichiers.
- Stockage de fichiers pour une application Web ou un système de gention de contenu.
- Stockage de fichiers log.
- Sauvegarde de base de données.

H. Service de stockage par objet

Limites du stockage par fichier

Le stockage par fichier, bien que largement utilisé et pratique, présente certaines limitations dans des environnements à grande échelle ou pour certaines applications modernes :

- **Utilisabilité.** Si le nombre de documents et la profondeur de la structure deviennent trop importants, il peut devenir difficile de nommer et retrouver facilement les fichiers.
- **Mise à l'échelle.** Bien qu'un système de fichier puisse théoriquement gérer des Po, en pratique, la limite est plutôt d'une centaine de To, principalement à cause de la centralisation des métadonnées et de l'indexation.
- **Performance.** La gestion centralisée des métadonnées et de la table d'allocation des blocs peut devenir un goulet d'étranglement avec un grand nombre d'accès simultanés.
- **Manque de flexibilité.** Les systèmes de fichiers ne sont pas toujours adaptés aux applications modernes qui manipulent des fichiers de données non structurées (images, vidéos, logs, etc.) pouvant atteindre de très grandes tailles.

Le stockage par objet

Le stockage par objet est un modèle de stockage qui gère les données sous forme d'objets, plutôt que de blocs (comme dans le stockage par bloc) ou de fichiers (comme dans le stockage par fichier).

Chaque objet est constitué de trois éléments :

- **Un identifiant unique.** Un identifiant global unique (comme un hash ou un UUID) qui permet de localiser l'objet dans le système de stockage.
- **Les données.** Les données à stocker, par exemple, une image, un document, etc.
- **Des métadonnées.** Des informations associées à l'objet, comme la date de création, le type de données, les permissions d'accès, ou d'autres attributs spécifiques définis par l'utilisateur ou le système.

Objets et bucket

Avec un service de stockage par fichier, on accède à un répertoire partagé via un protocole réseau comme SMB ou NFS.

Avec un service de stockage par objet, on accède à un *bucket* via une API REST au-dessus du protocole HTTP.

- Dans le jargon du stockage par objet, un bucket est l'équivalent d'un répertoire.
- Un bucket peut contenir un nombre illimité d'objets.
- Mais contrairement à un répertoire qui peut contenir des sous-répertoires, il n'est pas possible de créer un bucket dans un bucket.
- Les objets sont donc stockés « à plat » (sans structure hiérarchique) et doivent avoir un nom unique dans le bucket.

Limitation du stockage par objet

Avec un service de stockage par objet, la création ou la suppression d'un objet est similaire à la création d'un fichier. En revanche, il n'est pas possible de modifier une partie du contenu ou des métadonnées d'un objet.

Pour modifier un objet, il faut :

- Télécharger l'objet (*download*)
- Modifier les données de cet objet,
- Téléverser (*upload*) l'objet en entier.

Le stockage par objet n'est pas adapté pour le stockage de fichier dont le contenu doit être souvent modifié.

Cas d'utilisation du stockage par objet

Parmi les principaux cas d'utilisation du stockage par objet, on peut mentionner :

- Stockage et diffusion de contenu *riche media* (image, musique, vidéo).
- Analyse de big data.
- Sauvegarde et archivage.
- Enregistrement des données d'objets connectés (IoT).

Les services de stockage par objet sont généralement des services serverless et s'intègrent donc très bien avec d'autres services serverless comme le FaaS.

Température des données

On peut catégoriser les données en fonction de la fréquence d'accès à ces données :

- **Données chaudes (*hot data*).** Des données qui sont activement utilisées et régulièrement sollicitées. Ces données sont essentielles pour dans le traitement des transactions en ligne.
- **Données tièdes (*warm data*).** Des données moins sollitées que les données chaudes, mais qui doivent restées facilement accessibles. Ces données sont utilisées pour l'analyse ou la création de rapports périodique.
- **Données froide (*cold data*).** Des données rarement consultées. Ces données sont souvent stockées par obligation réglementaire, ou pour la conservation historique.

Température des données et types de service (Figure 10)

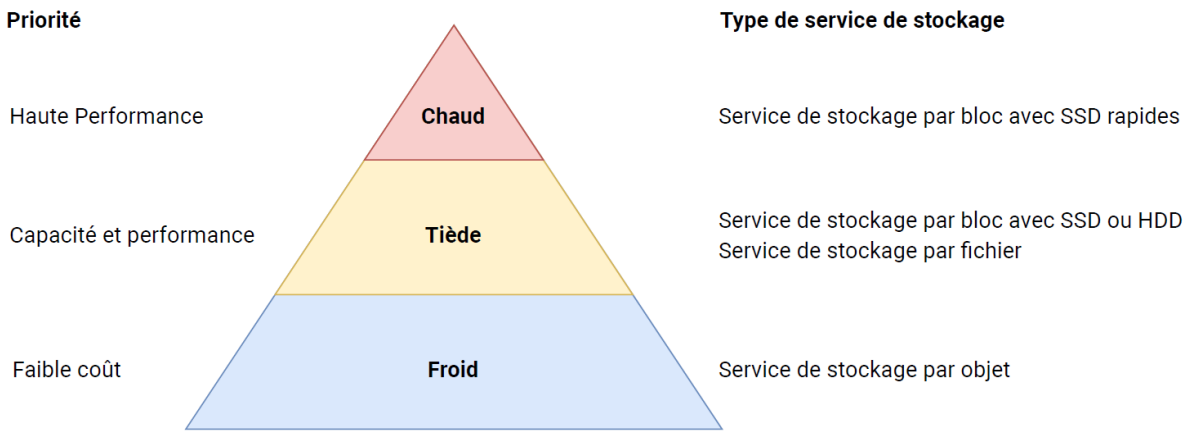


Figure 10 : Température des données et types de service

Classes de stockage

Le stockage par objet est toujours utilisé pour des données froides.

Toutefois, cette catégorie couvre des données encore un peu tièdes, jusqu'à des données gelées qui ne sont plus du tout utilisées.

C'est pourquoi il existe plusieurs classes de stockage par objet, selon que les données doivent être rapidement accessibles ou non en cas de besoins.

Par exemple, pour des données particulièrement froides, un service peut utiliser des bandes magnétiques pour réduire le coût du stockage. Dans ce cas, un accès aux données reste possible, mais cela peut alors demander plusieurs heures, et le coût de transfert est généralement sensiblement plus élevé.

Enfin, certains services peuvent mesurer la fréquence d'accès aux données et modifier dynamiquement la classe de stockage (*dynamic tiering*).

3. Virtualisation de réseau :

La virtualisation des réseaux est la transformation d'un réseau qui dépendait du matériel en un réseau basé sur des logiciels. Comme toutes les formes de virtualisation informatique, l'objectif fondamental de la virtualisation des réseaux est d'introduire une couche d'abstraction entre le matériel physique et les applications et services qui utilisent ce matériel.

Plus précisément, la virtualisation des réseaux permet de fournir des fonctions réseau ainsi que des ressources matérielles et logicielles indépendamment du matériel, sous la forme d'un réseau virtuel. Cette approche peut servir à regrouper de nombreux réseaux physiques, subdiviser un de ces réseaux ou connecter des machines virtuelles entre elles.

La virtualisation des réseaux permet aux fournisseurs de services numériques d'optimiser les ressources de leurs serveurs (c'est-à-dire moins de serveurs inactifs), d'utiliser des serveurs standard

pour des fonctions qui nécessitaient auparavant des équipements matériels propriétaires coûteux et d'améliorer la vitesse, la flexibilité ainsi que la fiabilité des réseaux.

Virtualisation des réseaux externe et virtualisation des réseaux interne

Il existe deux types de virtualisation des réseaux : la virtualisation externe et la virtualisation interne. La virtualisation externe permet de combiner des systèmes physiquement rattachés au même réseau local (LAN) en réseaux locaux virtuels (VLAN) indépendants ou, inversement, de diviser des réseaux LAN indépendants dans un même VLAN. Cette technologie permet aux fournisseurs de services d'améliorer l'efficacité d'un grand réseau.

Contrairement à la virtualisation des réseaux externe qui agit sur les systèmes en dehors d'un seul serveur, la virtualisation des réseaux interne agit au sein d'un serveur pour émuler un réseau physique. Cette technologie s'utilise généralement pour améliorer l'efficacité d'un serveur et implique la configuration d'un serveur avec des conteneurs logiciels. Les conteneurs permettent d'isoler des applications individuelles ou d'exécuter différents systèmes d'exploitation sur le même serveur.

L'intérêt de la virtualisation des réseaux

La virtualisation des réseaux permet de dissocier tous les éléments de l'infrastructure informatique physique (ressources de calcul, réseau et stockage) du matériel propriétaire et de les mettre en commun. À partir de ce regroupement, les ressources peuvent être déployées automatiquement là où elles sont le plus nécessaires, en fonction de l'évolution de la demande et des besoins de l'entreprise. La virtualisation des réseaux est particulièrement utile dans le secteur des télécommunications, où les opérateurs traditionnels doivent transformer leurs réseaux et leurs processus d'exploitation pour suivre les innovations technologiques.

Qu'il s'agisse de réalité virtuelle pour la chirurgie à distance ou de réseaux intelligents permettant aux ambulances de franchir les feux de signalisation rapidement et en toute sécurité, ces nouvelles avancées promettent des expériences radicalement améliorées et optimisées. Or, pour intégrer ces innovations, de nombreux opérateurs doivent transformer leurs réseaux qui, jusqu'ici, dépendaient du matériel. La virtualisation des réseaux leur offre l'agilité et l'évolutivité dont ils ont besoin pour suivre le rythme des innovations.

Avec les architectures cloud-native et le développement Open Source, les fournisseurs de cloud public hyperscale ont démontré qu'il était possible d'accélérer la distribution, le déploiement et le renouvellement des services. Les opérateurs de télécommunications peuvent adopter cette même approche pour renforcer leur niveau d'agilité, de flexibilité, de résilience et de sécurité. Ils peuvent gérer la complexité de l'infrastructure grâce à l' automatisation et à une plateforme horizontale commune. Ils peuvent également répondre aux exigences croissantes des consommateurs et des entreprises en matière de performances, de sécurité, de disponibilité et d'expérience utilisateur. Grâce aux architectures cloud-native et à l'automatisation, les opérateurs peuvent modifier et ajouter plus rapidement des services et des fonctions pour mieux répondre aux besoins et demandes de la clientèle.

Avantages de la virtualisation des réseaux

La plupart des fournisseurs de services numériques sont déjà engagés dans la virtualisation des fonctions réseau (NFV). La NFV permet de virtualiser les services réseau (routeurs, pare-feu, VPN et modules d'équilibrage de charge) traditionnellement exécutés sur du matériel propriétaire. Avec une

stratégie NFV, ces services sont regroupés dans des machines virtuelles ou des conteneurs sur du matériel standard, ce qui permet aux fournisseurs de services de faire fonctionner leur réseau sur des serveurs standard moins onéreux.

Une fois ces services virtualisés, les fournisseurs peuvent répartir les fonctions réseau sur différents serveurs ou les déplacer selon les besoins lorsque la demande évolue. Cette flexibilité permet d'accélérer le provisionnement du réseau, la mise à jour des services et la distribution des applications, sans nécessiter de ressources matérielles supplémentaires. La segmentation des charges de travail en machines virtuelles ou en conteneurs peut également renforcer la sécurité du réseau.

Cette approche :

- utilise moins de matériel (et du matériel moins cher) ;
- augmente la flexibilité et la portabilité des charges de travail ;
- permet de réorganiser les charges de travail facilement ;
- permet de mettre à l'échelle les ressources réseau de manière souple pour répondre à l'évolution de la demande.

Les avantages économiques d'une infrastructure réseau virtuelle peuvent être considérables, et le réseau d'accès radio (RAN) représente pour les opérateurs l'opportunité idéale de simplifier l'exploitation du réseau et d'améliorer la flexibilité, la disponibilité et l'efficacité. ACG Research estime que les opérateurs qui virtualisent entièrement le réseau RAN peuvent réduire de 44 % le coût total de possession (TCO).

Détails techniques sur la virtualisation de réseau Hyper-V dans Windows Server

La virtualisation de réseau offre plusieurs possibilités, le principe étant que plusieurs réseau virtuels (avec éventuellement des chevauchements d'adresses IP) s'exécutent sur une même infrastructure de réseau physique et chaque réseau virtuel fonctionne comme s'il s'agissait du seul réseau virtuel à s'exécuter sur l'infrastructure réseau partagée. La figure 11 illustre cette relation.

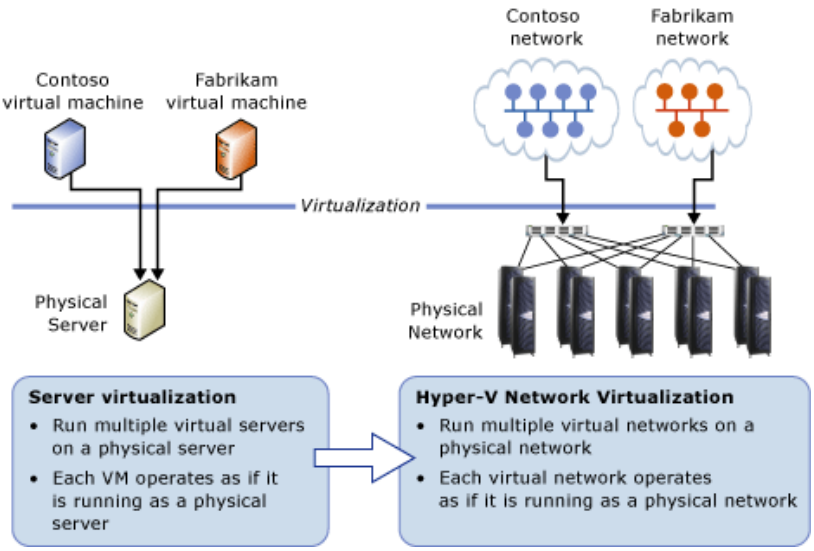


Figure 11 : Virtualisation de serveur comparée à la virtualisation de réseau

Principes de la virtualisation de réseau Hyper-V

Dans la virtualisation de réseau Hyper-V (HNV), un client ou un locataire est défini comme le «propriétaire» d'un ensemble de sous-réseaux IP déployés dans une entreprise ou un centre de

données. Un client peut être une société ou une entreprise avec plusieurs services ou unités commerciales dans un centre de données privé qui nécessitent une isolation réseau, ou un locataire dans un centre de données public hébergé par un fournisseur de services. Chaque client peut disposer d'un ou de plusieurs Réseaux virtuels dans le centre de données et chaque réseau virtuels se compose d'un ou de plusieurs Sous-réseaux virtuels.

Il existe deux implémentations HNV qui sont disponibles dans Windows Server 2016 : HNVv1 et HNVv2.

- **HNVv1**

HNVv1 est compatible avec Windows Server 2012 R2 et System Center 2012 R2 Virtual Machine Manager (VMM). La configuration de HNVv1 s'appuie sur la gestion WMI et les applets de commande Windows PowerShell (facilitées par System Center VMM) pour définir les paramètres d'isolation et les mappages et routage de l'adresse client (CA) - réseau virtuel - vers les adresses physiques (PA). Aucune fonctionnalité supplémentaire n'a été ajoutée à HNVv1 dans Windows Server 2016 et aucune nouvelle fonctionnalité n'est planifiée.

- SET Teaming et HNV V1 ne sont pas compatibles par plateforme.
- Pour utiliser des passerelles NVGRE HA, les utilisateurs doivent utiliser l'équipe LBFO ou Aucune équipe. ou
- Utilisez les passerelles déployées par le contrôleur de réseau avec le commutateur SET associé.

- **HNVv2**

Un nombre important de nouvelles fonctionnalités sont incluses dans HNVv2, qui est implémenté à l'aide de l'extension de transfert VFP (Azure Virtual Filtering Platform) dans le commutateur Hyper-V. HNVv2 est entièrement intégré à Microsoft Azure Stack, qui inclut le nouveau Contrôleur de réseau dans la pile SDN (Software Defined Networking). La stratégie de réseau virtuel est définie via le Contrôleur de réseau Microsoft à l'aide d'une API RESTful NorthBound (NB) et transférée à un agent hôte via plusieurs interfaces SouthBound (SBI), y compris OVSDB. L'agent hôte programme la stratégie dans l'extension VFP du commutateur Hyper-V où elle est appliquée.

Réseau virtuel

- Chaque réseau virtuel se compose d'un ou plusieurs sous-réseaux virtuels. Un réseau virtuel forme une limite d'isolation où les machines virtuelles au sein d'un réseau virtuel ne peuvent communiquer qu'entre elles. Traditionnellement, cette isolation était appliquée à l'aide de réseaux locaux virtuels avec une plage d'adresses IP séparée et une balise 802.1q ou un ID de réseau local virtuel. Toutefois, avec HNV, l'isolation est appliquée à l'aide de l'encapsulation NVGRE ou VXLAN pour créer des réseaux de superposition avec la possibilité de chevaucher des sous-réseaux IP entre des clients ou des locataires.

- Chaque réseau virtuel a un ID de domaine de routage (RDID) unique sur l'hôte. Ce RDID correspond approximativement à un ID de ressource pour identifier la ressource REST de réseau virtuel dans le contrôleur de réseau. La ressource REST de réseau virtuel est référencée à l'aide d'un espace de noms URI (Uniform Resource Identifier) avec l'ID de ressource ajouté.

Sous-réseaux virtuels

- Un sous-réseau virtuel implémente la sémantique de sous-réseau IP de couche 3 pour les ordinateurs virtuels qui font partie d'un même sous-réseau virtuel. Le sous-réseau virtuel

forme un domaine de diffusion (similaire à un VLAN) et l'isolation est appliquée à l'aide du champ TNI (ID réseau de locataire NVGRE) ou VNI (VXLAN Network Identifier).

- Chaque sous-réseau virtuel appartient à un seul réseau virtuel (RDID) et un ID de sous-réseau virtuel (VSID) unique est attribué à l'aide de la clé TNI ou VNI dans l'en-tête de paquet encapsulé. Le VSID doit être unique au sein du centre de données et est compris dans une plage allant de 4096 à 2^24-2.

L'un des principaux avantages du réseau virtuel et du domaine de routage est qu'il permet aux clients d'apporter leurs propres topologies de réseau (par exemple, des sous-réseaux IP) dans le cloud. La figure 12 montre un exemple dans lequel Contoso Corp possède deux réseaux distincts : le réseau Recherche et développement (« R&D Net ») et le réseau commercial (« Sales Net »). Comme ces réseaux ont des ID de domaine de routage différents, ils ne peuvent pas interagir ensemble. Autrement dit, le réseau R&D Net Contoso est isolé du réseau Sales Net Contoso, alors même que les deux appartiennent à Contoso Corp. Le réseau R&D Net Contoso contient trois sous-réseaux virtuels. Notez que les RDID et VSID sont uniques au sein d'un centre de données.

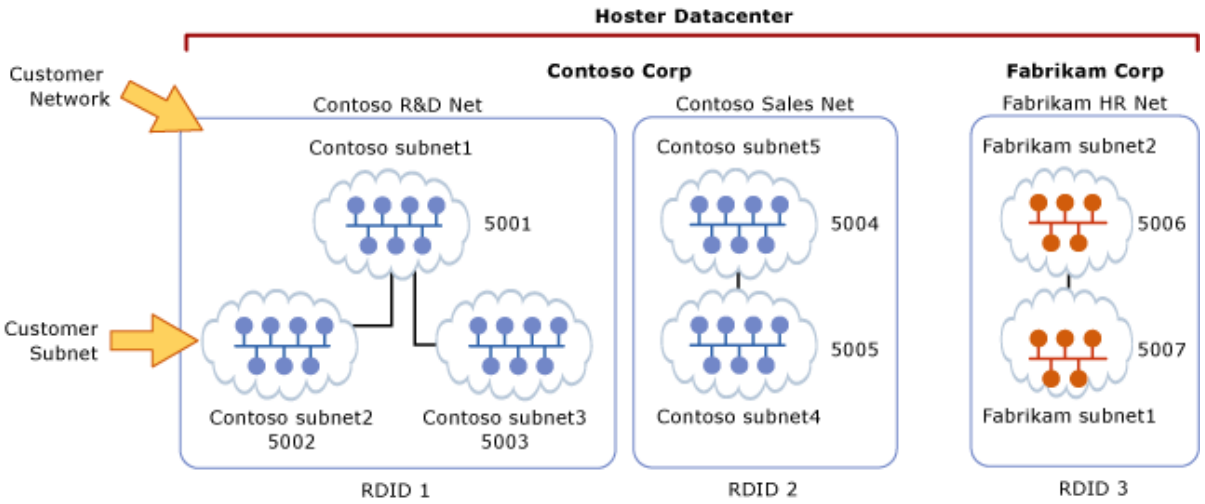


Figure 12 : réseaux client et sous-réseaux virtuels

Transfert de couche 2

Dans la figure 2, les paquets des machines virtuelles dans VSID 5001 peuvent être transférés aux machines virtuelles qui se trouvent également dans VSID 5001 via le commutateur Hyper-V. Les paquets entrants d'une machine virtuelle dans VSID 5001 sont envoyés à un VPort spécifique sur le commutateur Hyper-V. Les règles d'entrée (par exemple, encaps) et les mappages (par exemple, l'en-tête d'encapsulation) sont appliqués par le commutateur Hyper-V pour ces paquets. Les paquets sont ensuite transférés vers un autre VPort sur le commutateur Hyper-V (si la machine virtuelle de destination est attachée au même hôte) ou vers un commutateur Hyper-V différent sur un autre hôte (si la machine virtuelle de destination se trouve sur un autre hôte).

Routage de couche 3

De même, les paquets des machines virtuelles dans VSID 5001 peuvent être acheminés vers des machines virtuelles dans VSID 5002 ou VSID 5003 par le routeur distribué HNV qui est présent dans le

commutateur virtuel de chaque hôte Hyper-V. Lors de la remise du paquet au commutateur Hyper-V, HNV met à jour le VSID du paquet entrant par rapport au VSID de l'ordinateur virtuel de destination. Cela ne se produit que si les deux VSID se trouvent dans le même RDID. Par conséquent, les cartes réseau virtuelles associés à RDID1 ne peuvent pas envoyer de paquets aux cartes réseau virtuelles associées à RDID2 sans traverser une passerelle

Chaque sous-réseau virtuel définit un sous-réseau IP de couche 3 et une limite de domaine de diffusion de couche 2 similaire à un VLAN. Lorsqu'une machine virtuelle diffuse un paquet, HNV utilise la réplication de monodiffusion (UR) pour effectuer une copie du paquet d'origine et remplacer l'adresse IP et le MAC de destination par les adresses de chaque machine virtuelle qui se trouvent dans le même VSID.

En plus d'être un domaine de diffusion, le VSID assure une isolation. Une carte réseau virtuelle dans HNV est connectée à un port de commutateur Hyper-V dont les règles de liste de contrôle d'accès sont appliquées directement au port (ressource REST virtualNetworkInterface) ou au sous-réseau virtuel (VSID) dont elle fait partie.

Une règle ACL doit être appliquée au port du commutateur Hyper-V. Cette liste de contrôle d'accès peut être ALLOW ALL, DENY ALL ou être plus spécifique pour autoriser uniquement certains types de trafic en fonction de la correspondance à 5 tuples (Adresse IP source, Adresse IP de destination, port source, port de destination, protocole).

Passage et routage dans la virtualisation de réseau Hyper-V

HNVv2 implémente la commutation de couche 2 (L2) et la sémantique de routage de couche 3 correctes (L3) pour fonctionner comme un commutateur physique ou un routeur fonctionne. Lorsqu'une machine virtuelle connectée à un réseau virtuel HNV tente d'établir une connexion avec une autre machine virtuelle dans le même sous-réseau virtuel (VSID), elle doit d'abord connaître l'adresse MAC de l'autorité de certification de la machine virtuelle distante. S'il existe une entrée ARP pour l'adresse IP de la machine virtuelle de destination dans la table ARP de la machine virtuelle source, l'adresse MAC de cette entrée est utilisée. Si aucune entrée n'existe, la machine virtuelle source envoie une diffusion ARP avec une demande de retour de l'adresse MAC correspondant à l'adresse IP de la machine virtuelle de destination. Le commutateur Hyper-V intercepte cette requête et l'envoie à l'agent hôte. L'agent hôte recherche dans sa base de données locale une adresse MAC correspondante pour l'adresse IP de la machine virtuelle de destination demandée.

Si une adresse MAC est disponible, l'agent hôte injecte une réponse ARP et la renvoie à la machine virtuelle. Une fois que la pile réseau de la machine virtuelle contient toutes les informations d'en-tête L2 requises, la trame est envoyée au port Hyper-V correspondant sur le commutateur virtuel. En interne, le commutateur Hyper-V teste cette trame par rapport aux règles de correspondance de N-tuple affectées au V-Port et applique certaines transformations au frame en fonction de ces règles. Plus important encore, un ensemble de transformations d'encapsulation est appliqué pour construire l'en-tête d'encapsulation à l'aide de NVGRE ou VXLAN, en fonction de la stratégie définie sur le contrôleur de réseau. En fonction de la stratégie programmée par l'agent hôte, un mappage AC-AF est utilisé pour déterminer l'adresse IP de l'hôte Hyper-V où réside la machine virtuelle de destination. Le commutateur Hyper-V garantit que les règles d'acheminement et les balises de réseau local virtuel correctes sont appliquées au paquet externe afin qu'il atteigne l'adresse AF distante.

Si une machine virtuelle connectée à un réseau virtuel HNV souhaite créer une connexion avec une machine virtuelle dans un autre sous-réseau virtuel (VSID), le paquet doit être routé en conséquence. HNV suppose une topologie en étoile où il n'y a qu'une seule adresse IP dans l'espace d'autorité de

certification utilisée comme tronçon suivant pour atteindre tous les préfixes IP (c'est-à-dire un itinéraire/passerelle par défaut). Actuellement, cela applique une limitation à un itinéraire par défaut unique, et les itinéraires autres que les routes par défaut ne sont pas pris en charge.

Routage entre des sous-réseaux virtuels

Dans un réseau physique, un sous-réseau IP est un domaine de couche 2 (L2) où les ordinateurs (virtuels et physiques) peuvent communiquer directement entre eux. Le domaine L2 est un domaine de diffusion où les entrées ARP (carte d'adresses IP:MAC) sont apprises via les requêtes ARP qui sont diffusées sur toutes les interfaces et les réponses ARP sont renvoyées à l'hôte demandeur. L'ordinateur utilise les informations MAC apprises à partir de la réponse ARP pour construire complètement la trame L2, y compris les en-têtes Ethernet. Toutefois, si une adresse IP se trouve dans un autre sous-réseau L3, la requête ARP ne franchit pas cette limite L3. Au lieu de cela, une interface de routeur L3 (tronçon suivant ou passerelle par défaut) avec une adresse IP dans le sous-réseau source doit répondre à ces requêtes ARP avec sa propre adresse MAC.

Dans la mise en réseau Windows standard, un administrateur peut créer des itinéraires statiques et les affecter à une interface réseau. En outre, une « passerelle par défaut » est généralement configurée pour être l'adresse IP du tronçon suivant sur une interface où les paquets destinés à l'itinéraire par défaut (0.0.0.0/0) sont envoyés. Les paquets sont envoyés à cette passerelle par défaut si aucun itinéraire spécifique n'existe. Il s'agit en général du routeur pour votre réseau physique. HNV utilise un routeur intégré qui fait partie de chaque hôte et a une interface dans chaque VSID pour créer un routeur distribué pour les réseaux virtuels.

Étant donné que HNV suppose une topologie en étoile, le routeur distribué HNV agit comme une passerelle par défaut unique pour tout le trafic qui transite entre les sous-réseaux virtuels qui font partie du même réseau VSID. L'adresse utilisée comme passerelle par défaut est l'adresse IP la plus basse dans le VSID et est affectée au routeur distribué HNV. Ce routeur distribué représente un moyen très efficace de router correctement tout le trafic à l'intérieur d'un réseau VSID, car chaque hôte peut acheminer directement le trafic vers l'hôte approprié sans intermédiaire. Cela est particulièrement vrai lorsque deux ordinateurs virtuels du même réseau d'ordinateurs virtuels, mais de différents sous-réseaux virtuels, se trouvent sur le même hôte physique. Comme vous le verrez plus loin dans cette section, le paquet ne doit jamais quitter l'hôte physique.

Routage entre les sous-réseaux PA

Contrairement à HNVv1 qui a alloué une adresse IP PA pour chaque sous-réseau virtuel (VSID), HNVv2 utilise désormais une adresse IP PA par Switch-Embedded membre de l'équipe de cartes réseau SET (Teaming). Le déploiement par défaut suppose une équipe à deux cartes réseau et affecte deux adresses IP PA par hôte. Un seul hôte a des adresses IP PA attribuées à partir du même sous-réseau logique fournisseur (PA) sur le même VLAN. Deux machines virtuelles locataires dans le même sous-réseau virtuel peuvent en effet se trouver sur deux hôtes différents qui sont connectés à deux sous-réseaux logiques de fournisseur différents. HNV construit les en-têtes IP externes pour le paquet encapsulé en fonction du mappage CA-PA. Toutefois, il s'appuie sur la pile TCP/IP hôte vers ARP pour la passerelle PA par défaut, puis génère les en-têtes Ethernet externes en fonction de la réponse ARP. En règle générale, cette réponse ARP provient de l'interface SVI sur le commutateur physique ou le routeur L3 où l'hôte est connecté. HNV s'appuie donc sur le routeur L3 pour acheminer les paquets encapsulés entre les sous-réseaux logiques/VLAN du fournisseur.

Routage hors d'un réseau virtuel

La plupart des déploiements clients nécessitent une communication entre l'environnement HNV et les ressources qui ne font pas partie de ce même environnement. Les passerelles de virtualisation de réseau sont nécessaires pour permettre la communication entre les deux environnements. Les infrastructures nécessitant une passerelle HNV comprennent le Cloud privé et le Cloud hybride. Fondamentalement, les passerelles HNV sont requises pour le routage de couche 3 entre des réseaux internes et externes (physiques) (y compris NAT) ou entre différents sites et/ou clouds (privés ou publics) qui utilisent un tunnel IPSec VPN ou GRE.

Les passerelles peuvent présenter différents facteurs de forme physique. Elles peuvent être basées sur Windows Server 2016, incorporées dans un commutateur Top of Rack (TOR) agissant comme une passerelle VXLAN, accessibles via une adresse IP virtuelle (VIP) annoncée par un équilibreur de charge, placées dans d'autres appliances réseau existantes, ou peuvent être une nouvelle appliance réseau autonome.

Encapsulation de paquet

Dans HNV, chaque carte réseau virtuelle est associée à deux adresses IP :

- **Adresse client** (AC) Adresse IP assignée par le client, en fonction de son infrastructure intranet. Cette adresse permet au client d'échanger du trafic réseau avec l'ordinateur virtuel comme s'il n'avait pas été transféré sur un cloud public ou privé. L'adresse client est visible de l'ordinateur virtuel et accessible au client.
- **Adresse fournisseur** (AF) Adresse IP assignée par l'hébergeur ou les administrateurs du centre de données, en fonction de l'infrastructure de leur réseau physique. L'adresse fournisseur figure dans les paquets du réseau qui sont échangés avec le serveur exécutant Hyper-V qui héberge l'ordinateur virtuel. Cette adresse est visible sur le réseau physique, mais pas sur l'ordinateur virtuel.

Les adresses client préservent la topologie réseau du client, qui est virtualisée et dissociée des adresses et de la topologie du réseau physique sous-jacent, conformément à l'implémentation des adresses fournisseur. Le diagramme suivant (Figure 13) illustre la relation conceptuelle entre les adresses client des ordinateurs virtuels et les adresses fournisseur d'une infrastructure réseau à la suite d'une virtualisation de réseau.

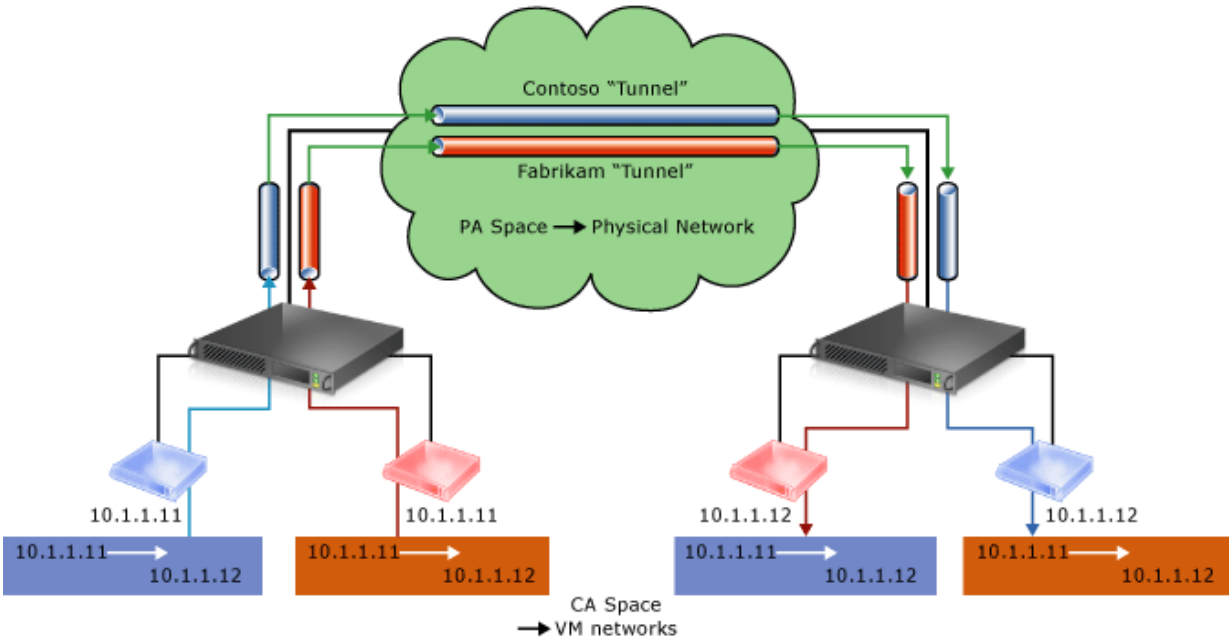


Figure 13 : diagramme conceptuel d'une virtualisation de réseau sur une infrastructure physique

Dans le diagramme, les ordinateurs virtuels client envoient des paquets de données dans l'espace d'adressage client, qui transitent par l'infrastructure réseau physique en empruntant leurs propres réseaux virtuels ou « tunnels ». Dans l'exemple ci-dessus, les tunnels peuvent être considérés comme des « enveloppes » pour les paquets de données Contoso et Fabrikam disposant d'étiquettes d'expédition (adresses fournisseur) vertes, qui doivent être remises par l'hôte source de gauche à l'hôte de destination de droite. La question essentielle est de savoir comment les hôtes déterminent les « adresses d'expédition » (fournisseur) correspondant aux adresses client Contoso et Fabrikam, comment l'« enveloppe » englobe les paquets et comment les hôtes de destination peuvent déballer les paquets et les remettre correctement aux ordinateurs virtuels de destination Contoso et Fabrikam.

Cette analogie simple a mis en évidence les principaux aspects de la virtualisation de réseau :

- Chaque adresse client d'ordinateur virtuel est mappée à une adresse fournisseur d'hôte physique. Plusieurs adresses client peuvent être associées à la même adresse fournisseur.
- Les ordinateurs virtuels envoient des paquets de données dans les espaces d'adressage client, qui sont mis dans une « enveloppe » avec une paire d'adresses fournisseur source et de destination en fonction du mappage.
- Les mappages entre adresses client et fournisseur doivent permettre aux hôtes de distinguer les paquets à destination des différents ordinateurs virtuels client.

Par conséquent, la virtualisation d'un réseau consiste à virtualiser les adresses réseau utilisées par les ordinateurs virtuels. Le contrôleur de réseau est responsable du mappage d'adresses et l'agent hôte gère la base de données de mappage à l'aide du schéma MS_VTEP. La section suivante décrit les mécanismes réels de la virtualisation d'adresses.

Architecture de la virtualisation de réseau Hyper-V

Dans Windows Server 2016, HNVv2 est implémenté à l'aide de la plateforme de filtrage virtuel Azure (VFP), qui est une extension de filtrage NDIS dans le commutateur Hyper-V. Le concept clé de VFP est

celui d'un moteur de flux Match-Action avec une API interne exposée à l'agent hôte SDN pour la programmation de la stratégie réseau. L'agent hôte SDN reçoit lui-même la stratégie réseau du contrôleur de réseau sur les canaux de communication OVSDB et WCF SouthBound. Non seulement la stratégie de réseau virtuel (par exemple le mappage AC-AF) est programmée à l'aide de VFP, mais une stratégie supplémentaire telle que les listes de contrôle d'accès, la qualité de service, etc.

La hiérarchie d'objets pour l'extension de transfert vSwitch et VFP est la suivante :

- vSwitch
    - Gestion des cartes réseau externes
    - Déchargements matériels de carte réseau
    - Règles de transfert globales
    - Port
        - Couche de transfert de sortie pour l'épinglage à cheveux
        - Listes d'espaces pour les mappages et les pools NAT
        - Table de flux unifiée
        - Couche VFP
            - Table de flux
            - Groupe
            - Règle
                - Les règles peuvent référencer des espaces

Dans le VFP, une couche est créée par type de stratégie (par exemple, Réseau virtuel) et est un ensemble générique de tables de règles/flux. Il n'a pas de fonctionnalités intrinsèques tant que des règles spécifiques n'ont pas été affectées à cette couche pour implémenter ces fonctionnalités. Chaque couche se voit attribuer une priorité et les couches sont affectées à un port par priorité croissante. Les règles sont organisées en groupes principalement en fonction de la direction et de la famille d'adresses IP. Une priorité est également attribuée aux groupes et, au maximum, une règle d'un groupe peut correspondre à un flux donné.

La logique de transfert pour le commutateur virtuel avec l'extension VFP est la suivante :

- Traitement d'entrée (entrée du point de vue du paquet entrant dans un port)
- Transfert
- Traitement de sortie (sortie du point de vue du paquet sortant d'un port)

Le VFP prend en charge le transfert MAC interne pour les types d'encapsulation NVGRE et VXLAN, ainsi que le transfert basé sur un réseau local virtuel MAC externe.

L'extension VFP a un chemin d'accès lent et un chemin d'accès rapide pour la traversée de paquets. Le premier paquet d'un flux doit parcourir tous les groupes de règles de chaque couche et effectuer une recherche de règle, ce qui est une opération coûteuse. Toutefois, une fois qu'un flux est inscrit dans la table de flux unifiée avec une liste d'actions (en fonction des règles correspondantes), tous les paquets suivants sont traités en fonction des entrées de la table de flux unifiée.

La stratégie HNV (Figure 14) est programmée par l'agent hôte. Chaque carte réseau d'ordinateur virtuel est configurée avec une adresse IPv4. Il s'agit des adresses client dont se serviront les ordinateurs virtuels pour communiquer entre eux et qui sont transportées dans les paquets IP en provenance des ordinateurs virtuels. HNV encapsule la trame d'autorité de certification dans une

trame pa basée sur les stratégies de virtualisation de réseau stockées dans la base de données de l'agent hôte.

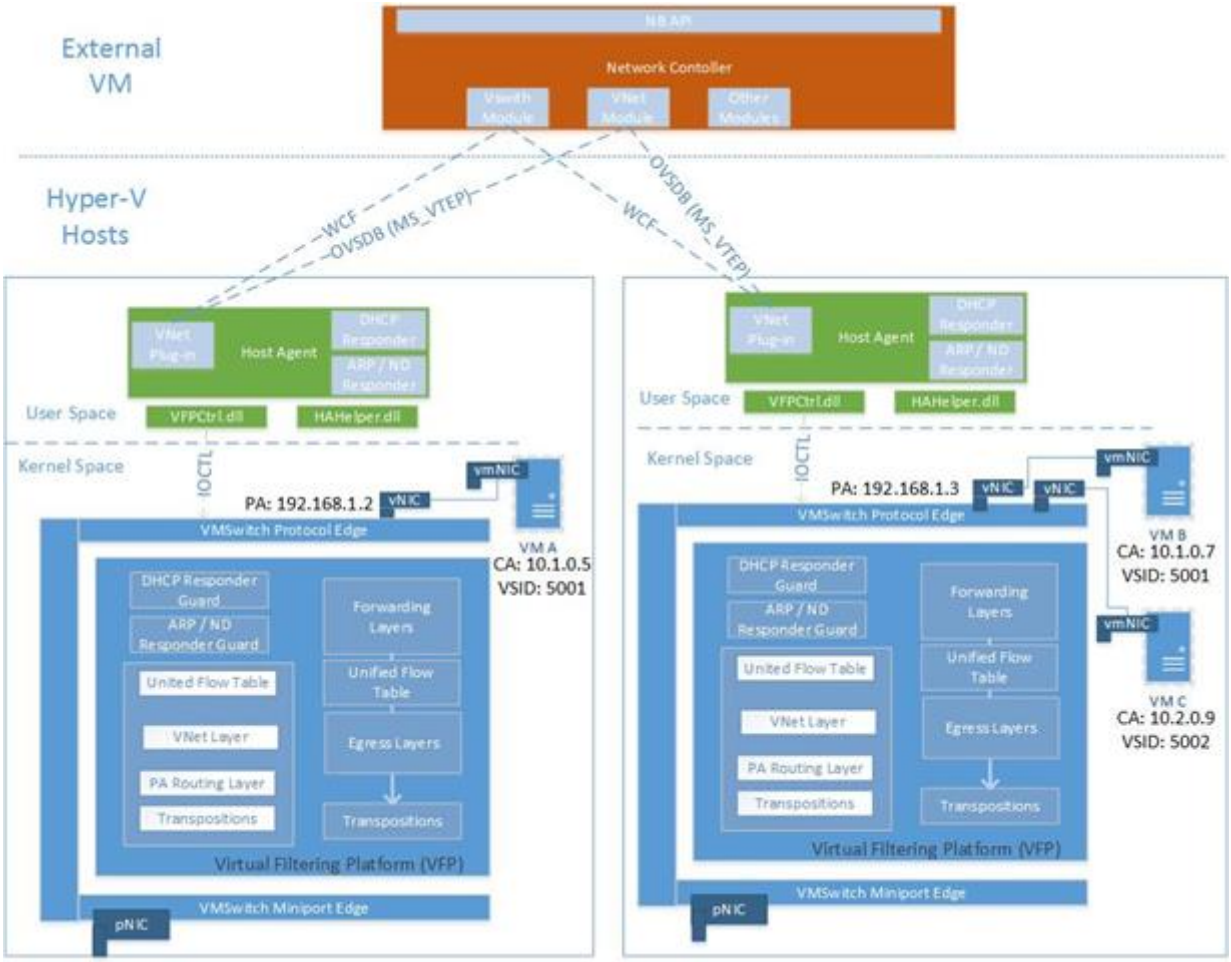


Figure 14 : Architecture HNV

4. Concept de la virtualisation du poste de travail

A. Le « Bureau Virtuel »

Vous pouvez gérer facilement vos données (e-mails, contacts, rendez-vous, documents, tâches, ...) dans votre bureau virtuel, accessible dans un simple navigateur Web à partir de tout ordinateur connecté à Internet ou d'un client léger au sein de votre entreprise.

Par exemple, les Technologies Terminal Server de Microsoft et « Presentation Server » de CITRIX permettent d'implémenter les bureaux virtuels.

B. Le « Streaming Applicatif »

Le streaming applicatif permet de déployer sur des parcs informatiques des applications sans les installer. A l'exécution de chaque application, une bulle applicative virtuelle est montée sur le système

d'exploitation. L'application exécutée dans cette bulle est isolée des autres applications et fonctionne de manière indépendante.

Les technologies principales utilisées sont « Presentation Server » de CITRIX et « SoftGrid » de Microsoft.

C. La Virtualisation du Poste de Travail

Le recours à une infrastructure de virtualisation du poste de travail permet de mettre en œuvre une infrastructure « client léger » qui optimise l'utilisation, l'administration, le coût total de propriété et la souplesse.

Des environnements de bureau complets peuvent être exécutés dans des machines virtuelles sur des serveurs de centre de données et les utilisateurs finaux peuvent y accéder depuis tout
PC ou client léger connecté au réseau d'entreprise.

Cette solution permet au service informatique de contrôler de façon centralisée les ressources informatiques des postes de travail et leurs données, de consolider des machines virtuelles et d'optimiser l'utilisation des ressources dans le centre de données.

Les utilisateurs ont ainsi la possibilité d'accéder à leur environnement de travail complet depuis n'importe quel site et n'importe quel client.

Présentation

Objectif : Dématérialiser le poste de travail avec uniformisation du matériel (universalité du modèle virtuel).
Les enjeux principaux des postes de travail sont :

- Déploiement
- Mobilité
- « Remote Office » / « Branch Office »
- Sécurité
- Périphériques et multimédia
- Green

Concept VDI (« voix, données, images » Câblage et connectique normalisée) :

- Connexion « un à un » entre le poste de travail et la machine virtuelle en session de bureau à distance,
- Les connexions s'effectuent à travers le réseau local d'entreprise,
- La session de bureau à distance est établie en connexion RDP (« **Remote Desktop**
- **Protocol »** est un protocole qui permet à un utilisateur de se connecter sur un ordinateur faisant tourner Microsoft Terminal Services. Des clients existent pour la quasi-totalité des versions de Windows, et pour d'autres systèmes d'exploitation, comme Linux.) depuis un poste de travail ou un terminal léger.

Architecture VDI (Figure 15)

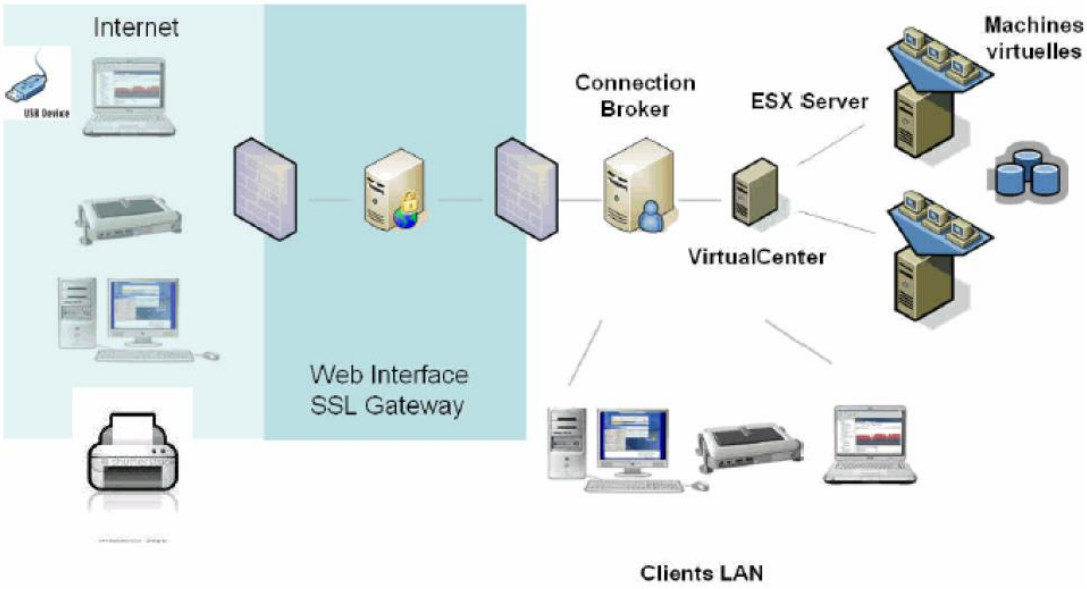


Figure 15 : Architecture VDI

Remarque :

L'Appliance « Connection Broker » : Le "Connection Broker" gère tous les types de postes clients. Il peut ainsi allouer à un utilisateur un PC virtuel, une session applicative avec déport d'affichage ou un PC

Lame. Le « Connection Broker » est le « service » qui est chargé de fournir à un utilisateur une connexion vers une machine virtuelle cliente. Il peut aussi, selon les éditeurs, gérer et provisionner ces mêmes machines virtuelles.

Exemple avec VMware : L'utilisateur se connecte au « Connection Broker » qui lui alloue une connexion vers une machine virtuelle hébergée sur la ferme ESX à laquelle est associé le « Connection Broker ».

Exemples de « Connection Brokers » : VMware VDM 2, Leostream, Provision Networks).

Expérience Utilisateur / Architecture WAN, LAN et Local (Figure 16)

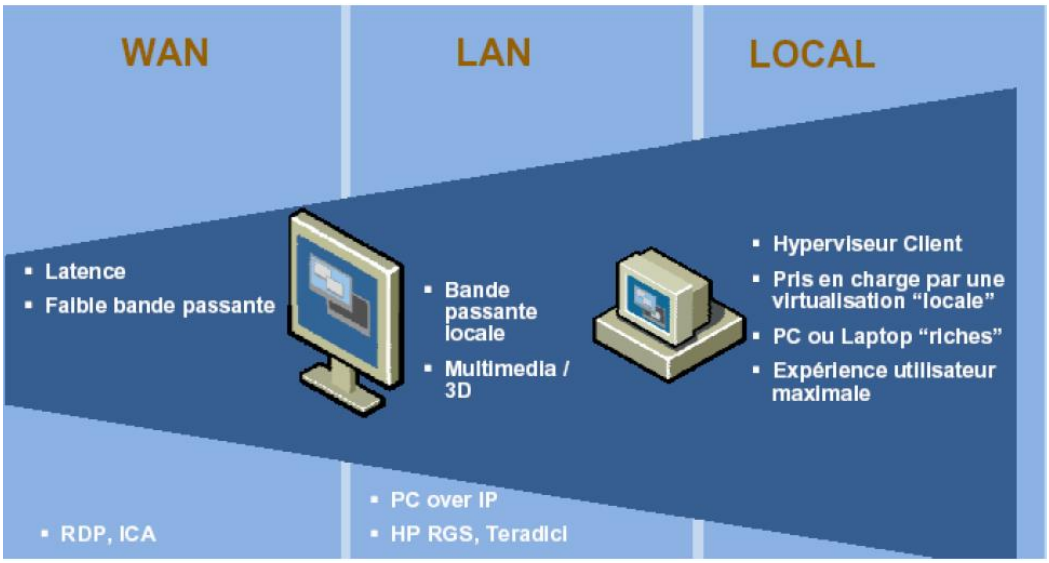


Figure 16 : Expérience Utilisateur / Architecture WAN, LAN et Local

Virtualisation du Poste de Travail : Principales technologies (Figure 17)

Technologie	Description	Acteurs
Client léger Windows	Applications exécutées sur un serveur, déport de l'interface utilisateur sur le PC.	Microsoft, Citrix (et fabricants de clients légers).
Virtualisation d'applications	Applications exécutées sur le PC mais isolées entre elles et du système. Distribution de l'application en mode streaming par un serveur.	Microsoft, Citrix, Altiris.
Virtualisation du PC	Virtualisation de l'environnement système de chaque PC, sur un serveur. Déport de l'interface utilisateur sur le PC physique.	VMware
Streaming de système d'exploitation	Mise à disposition d'un système d'exploitation, auprès des PC, par un serveur.	Ardence (racheté par Citrix).
PC lame	Centralisation physique de chaque PC sur un serveur lame. Déport de l'interface utilisateur sur un client léger.	ClearCube et HP

Figure 17 : Virtualisation du Poste de Travail : Principales technologies

5. Virtualisation des applications

Qu'est-ce que la virtualisation des applications ?

La virtualisation des applications est le processus d'abstraction (ou de séparation) d'une application du matériel informatique sous-jacent sur lequel elle est stockée. La virtualisation d'une application permet aux collaborateurs d'une entreprise d'accéder à cette application à partir de pratiquement n'importe quel appareil et de n'importe quel endroit, à condition qu'ils disposent d'une connexion Internet. Bien que les utilisateurs n'aient pas à installer physiquement l'application sur leurs appareils, ils peuvent interagir avec l'application presque comme s'ils l'avaient installée.

Il existe deux façons de créer une application virtuelle : la virtualisation des applications et la virtualisation des postes de travail. Avec la virtualisation des postes de travail, ou **infrastructure de postes de travail virtuels (VDI),** les applications sont exécutées sur des serveurs dans le datacenter d'une entreprise et les postes de travail complets des utilisateurs, y compris les systèmes d'exploitation, sont accessibles à distance via toute une série d'appareils. Ces applications peuvent être considérées comme « virtuelles », car elles ne sont pas réellement installées sur l'appareil physique de chaque utilisateur. Par ailleurs, les postes de travail virtualisés (y compris les applications) sont généralement stockés sur des machines virtuelles contrôlées par un hyperviseur.

La virtualisation des applications permet également d'accéder aux applications à distance sur n'importe quel appareil. Mais contrairement au VDI, la virtualisation d'applications ne virtualise qu'une application, et non le système d'exploitation qui l'entoure ou d'autres composants. Ces applications virtualisées sont essentiellement diffusées sur les appareils des utilisateurs. Alors que la VDI virtualise les applications et les systèmes d'exploitation, la virtualisation des applications se contente de virtualiser l'application elle-même.

Fonctionnement de la virtualisation des applications

Pour faire simple, la virtualisation d'applications « trompe » une application classique en lui faisant croire qu'elle est connectée au système d'exploitation d'un appareil distant alors que ce n'est pas le cas. Ce système fonctionne grâce à une couche de virtualisation entre l'application et le système d'exploitation de l'appareil distant de l'utilisateur. La couche de virtualisation agit comme un élément de l'environnement d'exécution et détourne les fichiers et les modifications du registre vers un fichier exécutable distinct au lieu de disperser ces données dans le système d'exploitation sous-jacent. Le fichier exécutable est stocké sur le serveur hôte en tant qu'image, ce qui signifie que les appareils des utilisateurs finaux ne sont pas exposés à des vulnérabilités ou à d'autres problèmes de sécurité, car les données de l'application n'y sont pas stockées.

Étant donné que toutes les données sont conservées dans un seul fichier, qu'elles n'affectent pas le système d'exploitation sur lequel elles sont exécutées et qu'elles restent « invisibles » pour les autres applications et systèmes sur l'appareil distant de l'utilisateur, la virtualisation des applications peut être utilisée sur toute une série d'appareils – et des applications qui étaient incompatibles les unes avec les autres peuvent désormais fonctionner sur le même appareil.

Lorsqu'un utilisateur travaille au sein d'une application virtualisée, toutes les modifications qu'il apporte aux nouvelles données qu'il saisit sont sauvegardées sur le serveur d'hébergement où réside l'application

réelle. La livraison à distance de l'application permet au service informatique de maintenir et de gérer les applications dans un lieu unique et centralisé et simplifie également les processus de correction et de mise à jour, car il suffit de mettre à jour l'application une seule fois et lorsque les utilisateurs y accèdent, ils accèdent à la version la plus récente.

Bien que la virtualisation des applications et la virtualisation des postes de travail soient souvent considérées comme des processus similaires, il ne s'agit pas de la même chose. Comme indiqué plus haut, la virtualisation des postes de travail par le biais du VDI offre aux utilisateurs une expérience de bureau à distance plus souple et plus complète. La virtualisation d'applications spécifiques plutôt que d'environnements de bureau entiers peut s'avérer plus rentable pour les entreprises qui sollicitent fortement une seule application. La virtualisation des applications peut également constituer un composant d'un processus plus complet de virtualisation des postes de travail.

Avantages de la virtualisation des applications

La virtualisation des applications présente de nombreux avantages :

- **Installation et déploiement simples** – Une application n'est installée qu'une seule fois sur le serveur hôte et est ensuite déployée à distance par la distribution d'un fichier .exe aux appareils des utilisateurs.
- **Gestion simple et centralisée** – Le service informatique peut superviser de nombreuses applications pour des milliers d'utilisateurs à partir d'un seul emplacement centralisé.
- **Flexibilité et évolutivité accrues** – Éliminez le temps et les efforts consacrés à l'installation répétée d'applications sur des centaines ou des milliers de terminaux. Lors de l'intégration des nouveaux collaborateurs, il suffit de leur donner un accès à distance aux applications déjà installées.
- **Prise en charge de la mobilité** – Les applications virtualisées favorisent la mobilité et la portabilité ; certains appareils ne peuvent pas gérer un environnement de bureau à distance intégral, mais presque tous les appareils peuvent gérer une application virtualisée.
- **Réduction du risque de panne du système** – Les applications virtualisées peuvent fonctionner en même temps que des applications avec lesquelles elles ne sont pas nécessairement compatibles. De plus, les problèmes techniques liés à une application virtualisée peuvent être gérés par le service informatique à partir du serveur centralisé.
- **Sécurité renforcée grâce à l'isolation** – Les applications qui fonctionnent virtuellement sont isolées les unes des autres, de sorte que si une application est compromise par une attaque ou un dysfonctionnement, les autres ne le sont pas automatiquement. De plus, en cas de perte ou de vol d'un appareil, les données de l'application restent en sécurité, car elles ne sont pas stockées sur les appareils, mais sur le serveur hôte.
- **Meilleur contrôle de l'accès** – Le service informatique contrôle mieux qui peut accéder à quelles applications, car il peut simplement refuser les autorisations d'accès aux utilisateurs qui ne sont plus autorisés ou qui ont quitté l'entreprise, sans avoir à désinstaller le logiciel de l'appareil de l'utilisateur.
- **Accès rapide et facile aux applications essentielles en déplacement** – Les utilisateurs distants peuvent accéder immédiatement aux applications dont ils ont besoin pour faire leur travail. Pas d'attente pour l'installation ni de longs temps de chargement.
- **Conformité plus simple aux réglementations** – Les données n'étant pas stockées sur les appareils, les entreprises peuvent se conformer aux réglementations en matière de sécurité et de confidentialité, telles que la loi HIPAA (Health Insurance Portability and Accountability

Act) et les normes de sécurité des données de l'industrie des cartes de paiement (Payment Card Industry Data Security Standards - PCI-DSS).

- **Possibilité d'exécuter des applications traditionnelles en même temps que les applications avancées actuelles** – La virtualisation permet aux entreprises d'exécuter des applications traditionnelles même si elles ne sont pas compatibles avec des applications plus modernes. Cet élément est important, car de nombreuses entreprises, en particulier dans les secteurs très réglementés tels que la finance et la santé, s'appuient encore largement sur des applications traditionnelles.
- **Résolution rapide et intuitive des incidents** – Le service informatique peut facilement ramener une application à un état antérieur si des données sont corrompues ou si un cyberattaquant s'infiltre dans le système. Il est ainsi plus facile de réagir aux incidents et de rester opérationnel après une attaque.
- **Réduction des problèmes de performances** – Lorsque les appareils sont surchargés d'applications, les performances peuvent s'en retrouver affectées. En conservant les applications sur un serveur hôte et en les diffusant à distance, les appareils des utilisateurs ne ralentiront pas et ne tomberont pas en panne à cause d'un nombre d'applications trop élevé.

Qui bénéficie de la virtualisation des applications

La virtualisation des applications offre des avantages à de nombreuses personnes au sein d'une entreprise :

Les utilisateurs finaux

Les utilisateurs finaux d'applications virtualisées ont la liberté d'utiliser les appareils qu'ils préfèrent et la flexibilité de travailler où et quand ils le souhaitent – en bénéficiant d'un accès à distance facile aux systèmes stratégiques dont ils ont besoin pour accomplir leur travail. Grâce aux applications virtuelles à distance, les collaborateurs peuvent changer d'appareil à volonté et n'ont pas à se soucier des problèmes de sécurité, d'installation ou de maintenance. Ils bénéficient de tous les avantages de l'accès à distance aux applications, sans l'inconvénient de devoir les gérer.

Les administrateurs informatiques

La virtualisation des applications réduit la charge de déploiement et de gestion des applications pour les services informatiques. Plutôt que de devoir installer des logiciels sur des centaines ou des milliers d'appareils, et de s'assurer ensuite que chacun d'entre eux reçoit les correctifs et les mises à jour en temps opportun, l'équipe informatique peut simplement déployer une application sur un serveur hôte et la rendre accessible à distance aux utilisateurs autorisés lorsque c'est nécessaire. Elle dispose d'un emplacement unique et centralisé pour les applications, ce qui lui permet d'en assurer la gestion et la maintenance de manière beaucoup plus rapide et efficace. Certaines études ont montré que la virtualisation des applications peut également aboutir à une réduction du nombre de tickets support, puisque les utilisateurs n'ont pas à se préoccuper des logiciels sur leurs appareils. La mise en œuvre de la sécurité et la configuration des politiques sont également plus faciles et plus rationnelles dans un emplacement centralisé. Le déclassement d'applications ou la suppression des autorisations d'accès des collaborateurs peuvent également être effectués en toute simplicité.

Les développeurs

La virtualisation des applications profite aux développeurs de logiciels et d'applications, car elle rend les ressources plus accessibles. Le service informatique peut virtualiser plusieurs applications et

environnements sur le même système afin que les équipes puissent tester leurs logiciels sur différentes versions ou différents types de systèmes d'exploitation et apporter les améliorations nécessaires. Grâce à la virtualisation, les développeurs peuvent également accéder ou tester en toute sécurité des fichiers susceptibles d'être contaminés ou corrompus, car la couche de virtualisation sépare l'application du système d'exploitation et la contamination ne pourra pas s'infiltrer dans l'ensemble du système.

Les entreprises

Grâce à la virtualisation des applications, les entreprises peuvent mettre en œuvre des initiatives BYOD de manière simple et sécurisée, et ne plus avoir à fournir des appareils appartenant à l'entreprise pour l'usage des collaborateurs. Cela peut contribuer à réduire les coûts. Les coûts se retrouvent également réduits au niveau des charges de travail informatiques. En effet, les équipes informatiques ne sont plus tenues de passer la majeure partie de leur temps à installer et à gérer des logiciels sur de nombreux appareils individuels. La rationalisation de la gestion informatique peut se traduire par des économies réelles pour une entreprise. Celle-ci peut accomplir davantage avec un personnel réduit et des dépenses d'investissement moindres dans la multiplicité des copies de logiciels. Les entreprises peuvent également bénéficier d'un accès facile et sécurisé aux applications, où et quand elles en ont besoin. Les collaborateurs restent ainsi productifs et efficaces, ce qui peut avoir un effet réel sur les résultats de l'entreprise.

Les défis de la virtualisation des applications

Comme toute technologie, la virtualisation des applications n'est pas la réponse à tous les cas d'utilisation ou à tous les besoins de l'entreprise. Certains défis peuvent se poser, notamment :

- **Les applications exigeantes en ressources graphiques peuvent être perturbées** – La latence dans ces types d'applications peut causer des saccades au cours du processus de rendu.
- **Les pilotes de périphériques peuvent affecter l'utilisation des périphériques** - Toute application nécessitant un pilote de périphérique spécifique au système d'exploitation peut rendre difficile l'utilisation d'équipements tels que des imprimantes ou des scanners.
- **La dépendance à un réseau stable** – Pour utiliser une application virtualisée, vous devez avoir accès à une connexion Internet fiable. Cela peut représenter un défi pour les collaborateurs qui se trouvent régulièrement dans des endroits isolés, sans couverture, etc.
- **Les logiciels de surveillance du réseau** – Les applications virtualisées peuvent causer des problèmes avec ces logiciels et rendre plus difficiles la détection et la résolution des problèmes de performance.
- **L'accès hors ligne** - Une application virtualisée doit être accessible hors ligne. Si ce n'est pas le cas, elle ne sera pas aussi utile à un télétravailleur qui ne bénéficie pas toujours d'une bonne couverture.

La différence entre la virtualisation des applications et l'installation traditionnelle des applications ?

Avant que la virtualisation ne devienne possible et largement utilisée dans tous les secteurs d'activité, les entreprises devaient installer manuellement les applications sur les appareils de chaque utilisateur. Il y a vingt ou trente ans, cette charge n'était peut-être pas aussi lourde qu'aujourd'hui, car les entreprises utilisaient moins d'applications. Aujourd'hui, cependant, le nombre d'applications a explosé et des centaines de millions d'applications sont développées chaque année. Il est impossible pour une entreprise de gérer et de maintenir toutes ses applications aujourd'hui sans la virtualisation et/ou les services basés sur le cloud.

L'installation et la gestion locales des applications prendraient trop de temps aux services informatiques d'aujourd'hui. La seule façon pour une entreprise de travailler avec autant d'applications est de les virtualiser et de les rendre disponibles à distance. La virtualisation des applications permet de fournir rapidement et facilement des applications critiques à pratiquement n'importe quel terminal qu'un collaborateur souhaite utiliser. La gestion et la mise à jour d'une application sont beaucoup plus rapides et rationalisées pour les services informatiques, car ils ne doivent gérer et mettre à jour cette application qu'une seule fois sur le serveur hôte (et non des milliers de fois sur chaque appareil).

L'installation manuelle des logiciels affecte également l'expérience de l'utilisateur final. Même si l'installation se fait en libre-service, les utilisateurs finaux doivent prendre le temps de télécharger et d'installer l'application sur leur appareil. De plus, la plupart des gens possèdent plusieurs appareils à partir desquels ils souhaitent travailler, tels qu'un smartphone, une tablette, un ordinateur portable ou un ordinateur de bureau. La virtualisation des applications rend l'accès aux applications si facile et si efficace pour les utilisateurs finaux, sans qu'il soit nécessaire de les installer, de les télécharger, de les gérer ou de les mettre à jour.

Virtualisation des applications vs. virtualisation des serveurs vs. virtualisation des postes de travail

Bien qu'elles soient similaires en ce sens qu'elles impliquent toutes la virtualisation, la virtualisation des applications diffère de la virtualisation des serveurs et de la virtualisation des postes de travail sur certains points clés.

La virtualisation des serveurs

La virtualisation des serveurs est le type de virtualisation le plus courant aujourd'hui. Elle permet aux entreprises de créer plusieurs machines virtuelles sur un seul serveur physique, et de les organiser en groupes. Cela permet aux services informatiques d'exploiter au mieux les ressources informatiques, de réseau et de stockage disponibles dans l'entreprise et peut simplifier et rationaliser la reprise en cas de dysfonctionnement d'un serveur. Cela permet également aux machines virtuelles d'exécuter sans problème des systèmes d'exploitation auparavant incompatibles sur la même machine.

La virtualisation des applications

La virtualisation des applications consiste à mettre une application à la disposition des utilisateurs distants sur une couche virtualisée qui sépare l'application du système d'exploitation et du matériel de l'utilisateur final. L'application est stockée sur un serveur hôte dans un datacenter ou une société d'hébergement tierce et toutes les actions effectuées par les utilisateurs dans cette application sont en fait exécutées sur le serveur hôte. À l'instar de la virtualisation des serveurs, la virtualisation des

applications permet aux utilisateurs de faire fonctionner des applications auparavant incompatibles sur différents systèmes d'exploitation, comme Microsoft Excel sur Linux via un navigateur Opera.

La virtualisation des postes de travail

La virtualisation des postes de travail consiste à virtualiser l'ensemble de l'environnement du poste de travail, qui comprend le système d'exploitation, les applications, les bases de données et d'autres composants. Quel que soit l'appareil qu'ils utilisent, les collaborateurs disposent de la même présentation et des mêmes fonctionnalités sur tous les appareils, car l'environnement de travail est sauvegardé sur un serveur hôte.

Utilisation d'un logiciel de virtualisation des applications

Lorsqu'il s'agit de trouver la bonne solution de virtualisation des applications, vous avez l'embarras du choix. Toutes les solutions ne se valent pas. Voici quelques considérations à prendre en compte lorsque vous devez choisir une solution et un fournisseur :

- **Adaptation aux besoins actuels et futurs** – La technologie évolue constamment et devient de plus en plus avancée. Vous avez besoin d'une solution de virtualisation qui réponde non seulement aux besoins d'aujourd'hui, mais qui puisse également anticiper et prendre en charge ceux de demain.
- **Flexibilité** – Au fur et à mesure que votre entreprise se développe, votre solution de virtualisation d'applications doit s'adapter. Recherchez une solution suffisamment sûre et évolutive et qui offre la flexibilité nécessaire pour exécuter des charges de travail sur site dans votre datacenter, dans le cloud ou à la périphérie.
- **Compatibilité et intégration** – Trouvez une solution qui fonctionne avec votre infrastructure existante et qui s'intègre à vos applications existantes ainsi qu'aux systèmes centraux tels que les serveurs de fichiers, les services d'annuaire et les magasins de données utilisateur. L'objectif est d'assurer un accès à distance transparent pour tous les utilisateurs et tous les appareils.
- **Support technique et après-vente** – Vous ne vous contentez pas d'acheter une solution, vous décidez également de vous associer à un fournisseur particulier. Veillez à ce que cette relation soit transparente et que l'équipe de support soit impliquée dès le départ et s'engage à assurer votre réussite.
- **Simplicité d'utilisation, de déploiement et de gestion** – Votre solution de virtualisation des applications doit être intuitive et facile à utiliser et à gérer. Elle ne doit pas nécessiter de compétences informatiques spécialisées. Elle est censée permettre d'alléger votre charge informatique et de faciliter l'adoption de certaines applications !
- **Coût** – De nombreux facteurs contribuent au coût total de possession (TCO), mais assurez-vous de trouver une solution qui offre un bon retour sur investissement (ROI). N'oubliez pas non plus de prendre en compte les économies cachées, telles que la possibilité de gérer des charges de travail plus importantes avec moins de personnel, etc.
- **Sécurité et conformité** – Vous avez besoin d'un système de virtualisation doté de fonctions de sécurité intégrées qui contrôlent et surveillent l'accès et l'utilisation. D'autres éléments à

prendre en compte sont le chiffrement des données de bout en bout, l'authentification multifactorielle et les systèmes de détection et de prévention des intrusions.

- **Licences** – Assurez-vous de bien comprendre la structure des licences des applications que vous souhaitez virtualiser. Vous devez être autorisé à exécuter l'application sur plusieurs machines.

Quelles sont les applications qui peuvent être virtualisées

De nombreuses applications, sinon la plupart, peuvent être virtualisées ; d'ailleurs, les experts ont tendance à aborder cette question en énumérant plutôt les types d'applications qui ne peuvent pas être virtualisées. Ils donnent notamment les recommandations suivantes :

- Toute application nécessitant une intégration ou une interaction avec le système d'exploitation, comme certains logiciels antivirus et de protection contre les logiciels malveillants
- Les applications avec pilotes qui requièrent un accès au système d'exploitation
- Les applications dotées de services intégrés qui commencent à fonctionner de manière indépendante au démarrage du système, par exemple, ou lorsque les utilisateurs se connectent, comme les clients de pare-feu
- Toute application faisant partie d'un système d'exploitation, telle que Windows Media Player ou certains navigateurs
- Les applications utilisant des extensions shell, telles que celles qui étendent un programme avec des fonctions supplémentaires
- Les applications volumineuses de plus de 4 Go
- Les applications dont les licences ne permettent pas la virtualisation
- Les applications traditionnelles dotées de fonctions de haute disponibilité intégrées qui risquent de ne pas fonctionner correctement si elles sont virtualisées

Quelles exigences matérielles et logicielles liées à la virtualisation des applications

En bref : « Ça dépend » – de nombreux facteurs, tels que le nombre d'employés de votre entreprise, le nombre et le type d'applications que vous envisagez de virtualiser. Il est préférable de consulter le fournisseur de la solution de virtualisation d'applications que vous choisissez pour connaître les exigences matérielles et logicielles qu'il recommande.

Les applications virtualisées peuvent-elles être utilisées hors ligne

Votre solution de virtualisation d'applications doit disposer d'une sorte de mode hors ligne permettant de travailler dans une application. Cela est recommandé parce que les utilisateurs ne se trouvent pas toujours dans des zones disposant d'une bonne connexion Internet. Assurez-vous que votre solution de virtualisation des applications fournit des informations complètes sur le travail hors ligne afin de pouvoir transmettre les instructions aux utilisateurs finaux. En règle générale, les solutions exigent que

l'application soit entièrement mise en cache avant de passer en mode hors ligne. De nombreuses solutions proposent également des contrôles que les administrateurs informatiques peuvent utiliser pour autoriser l'utilisation hors ligne ou fixer des limites quant au moment ou à l'endroit où elle est utilisée.

Les applications virtualisées peuvent-elles coexister avec les applications installées localement

Il est possible pour un utilisateur final d'avoir des applications installées localement sur son appareil qui fonctionnent en même temps que des applications virtualisées fournies par un serveur d'accès à distance. Les caractéristiques de cette fonctionnalité peuvent varier en fonction de la solution ou du fournisseur, alors n'hésitez pas à poser des questions lorsque vous étudiez les options de votre solution.

Quels sont les cas concrets d'utilisation de la virtualisation des applications

Il existe de nombreuses raisons pour lesquelles une entreprise choisit la virtualisation des applications plutôt qu'une autre stratégie de virtualisation, telle que le VDI. Voici quelques cas d'utilisation :

- **Mise en avant des initiatives BYOD** – La virtualisation des applications permet aux collaborateurs d'utiliser leurs propres appareils pour accéder aux applications essentielles de l'entreprise et y travailler.
- **Gestion des coûts** – Avec les applications virtualisées, vous n'avez pas besoin de fournir des appareils d'entreprise aux utilisateurs, ce qui permet d'économiser de l'argent. Il n'est pas non plus nécessaire de fournir du matériel ou des logiciels pour chaque appareil de l'entreprise. En outre, la charge informatique est réduite, ce qui permet aux équipes IT d'accomplir davantage avec moins de personnel.
- **Choix des applications** – La virtualisation des applications permet aux collaborateurs d'accéder à toutes les applications dont ils ont besoin pour travailler, où qu'ils soient et quel que soit l'appareil qu'ils souhaitent utiliser.
- **Éviter les problèmes de migration** – Les collaborateurs peuvent utiliser n'importe quelle application sur n'importe quel appareil, même si le système d'exploitation de leur appareil n'était pas compatible avec l'application à l'origine. Nul besoin de consacrer du temps et des efforts à la conversion des appareils à des systèmes d'exploitation spécifiques.
- **Utilisation d'applications internes fréquemment mises à jour** – La virtualisation permet de mettre à jour les applications aussi souvent que souhaité sans avoir à prendre le temps de mettre à jour des centaines ou des milliers d'appareils. L'application peut être mise à jour fréquemment, assurant ainsi que chaque fois qu'un utilisateur ouvre l'application, il accède à la dernière version.
- **Accès à distance sécurisé aux données sensibles** – Étant donné qu'aucune des données accédées dans une application n'est stockée sur l'appareil de l'utilisateur, la virtualisation des applications est une excellente idée pour les collaborateurs qui ont besoin d'accéder à distance à des applications critiques.

- **Prise en charge d'un grand nombre de collaborateurs** – Toute entreprise comptant des milliers de collaborateurs qui ont besoin d'accéder à des applications a tout intérêt à envisager la virtualisation des applications. Il s'agit du seul moyen de fournir un accès efficace tout en rationalisant la gestion et la maintenance.

IV. Types de migrations :

A. La migration P2V/V2V avec Hyper-V

À l'ère de la transformation numérique, les organisations cherchent constamment à améliorer la flexibilité, l'efficacité et le coût-efficacité de leur infrastructure informatique. Une démarche stratégique qui a gagné une traction significative est la migration des machines physiques traditionnelles vers des environnements virtualisés. L'Hyper-V de Microsoft, une technologie d'hyperviseur puissante, offre une plateforme idéale pour cette transition.

Avantages de conversion d'un serveur physique/VM vers Hyper-V

- **Optimisation des ressources :** Hyper-V permet une utilisation efficace des ressources matérielles en permettant à plusieurs machines virtuelles de fonctionner simultanément sur un seul hôte physique. Cette consolidation réduit le nombre de serveurs physiques requis, réduisant les dépenses en capital et la consommation d'énergie tout en maximisant la puissance informatique disponible.
- **Scalabilité et Flexibilité :** Avec Hyper-V, l'augmentation ou la réduction des ressources allouées aux VMs peut être effectuée sans effort, garantissant que les charges de travail reçoivent la puissance de traitement, la mémoire et le stockage nécessaires au fur et à mesure que les demandes fluctuent. De plus, les VMs peuvent être rapidement provisionnées, migrées ou répliquées sur les hôtes, permettant un équilibrage de charge de travail transparent, la reprise après sinistre et la continuité des activités.
- **Gérabilité améliorée :** Hyper-V s'intègre parfaitement à la suite System Center de Microsoft et aux services cloud Azure, fournissant des capacités de gestion centralisée, de surveillance et d'automatisation. Cela simplifie les tâches d'administration IT, rationalise les processus de mise à jour et de correction, et facilite la conformité avec les politiques de sécurité.
- **Environnements de test et de développement :** Hyper-V facilite la création d'environnements VM isolés et personnalisables, qui sont inestimables pour les tests logiciels, le développement d'applications, et à des fins de formation. Ces bacs à sable permettent aux équipes d'expérimenter sans impact sur les systèmes de production, accélérant l'innovation et réduisant les risques.
- **Passer à un nouvel environnement virtuel :** Hyper-V est la plateforme de virtualisation de Microsoft. Grâce à son intégration profonde avec le système d'exploitation Windows, son rapport coût-efficacité, sa large compatibilité matérielle et son support de pilotes, sa virtualisation de stockage et sa flexibilité, son support puissant pour le cloud computing et la conteneurisation, ses outils de gestion efficaces et ses fonctions de virtualisation avancées, il fournit une solution de virtualisation compatible, rentable, facile à gérer et riche en fonctionnalités pour les utilisateurs d'entreprise dans les environnements Windows. Son

intégration étroite avec la plateforme cloud Azure est particulièrement adaptée aux utilisateurs recherchant un déploiement de cloud hybride et exploitant pleinement les avantages de l'écosystème Microsoft.

Outils de conversion Hyper-V P2V

Plusieurs outils spécialisés ont été développés pour faciliter le processus de conversion des machines physiques (P2V) en machines virtuelles Hyper-V. Trois de ces outils se distinguent par leur efficacité et leur facilité d'utilisation :

Microsoft Virtual Machine Converter (MVMC) : Un utilitaire gratuit de Microsoft, MVMC est spécifiquement conçu pour convertir des serveurs physiques Windows et Linux, ainsi que des machines virtuelles VMware, en VM Hyper-V. Il offre une interface conviviale et un support de ligne de commande, garantissant la compatibilité avec divers scénarios d'automatisation.

Disk2vhd : Disk2vhd est un outil léger et autonome qui crée des images VHD ou VHDX de disques physiques ou de volumes, prêtes à être importées dans Hyper-V. Sa simplicité et l'absence d'exigences d'installation en font un choix attrayant pour les conversions P2V rapides, particulièrement dans les environnements plus petits.

Utilisation de MVMC pour la conversion Hyper-V P2V

1. Téléchargez la dernière version de **MVMC** sur le site officiel de Microsoft et installez le logiciel en suivant les instructions à l'écran.
2. Après l'installation, lancez l'assistant MVMC. Vous serez accueilli avec un écran de bienvenue. Cliquez sur **Next** pour continuer.
3. Dans la page **Machine Type**, sélectionnez **Physical machine conversion**. Dans l'écran suivant, fournissez l'adresse IP ou le nom de l'hôte de la machine physique que vous voulez convertir, ainsi que les identifiants d'authentification appropriés (nom d'utilisateur et mot de passe). Cliquez ensuite sur **Scan System** pour obtenir les informations de la machine physique.
4. Sélectionnez la partition physique qui doit être convertie et choisissez le type de disque virtuel.
5. Entrez le nom après la conversion en machine virtuelle et la configuration de CPU et de mémoire.
6. Entrez l'adresse, le nom d'utilisateur et le mot de passe de l'hôte Hyper-V cible, qui héberge la machine virtuelle convertie.
7. Spécifiez le chemin de stockage où les fichiers de la machine virtuelle seront stockés après la conversion (l'utilisation d'un chemin partagé nécessite une autorisation d'écriture).
8. Spécifiez le chemin de l'espace de travail de la machine virtuelle convertie.
9. Sélectionnez le statut de connexion de la carte réseau.
10. Consultez les informations récapitulatives, confirmez leur exactitude et cliquez sur **Next**.
11. Démarrez la conversion et attendez la fin de la conversion.

Après la conversion, vous pouvez voir la machine virtuelle qui a été créée automatiquement sur l'hôte Hyper-v.

Si vous voulez effectuer une migration V2V avec MVMC, il vous suffit de sélectionner **Virtual machine conversion** dans la page **Machine Type** et de suivre l'assistant.

Utilisation de Disk2vhd pour la conversion Hyper-V P2V

1. Téléchargez et exécutez Disk2vhd

Téléchargez l'exécutable portable **Disk2vhd** du site Web de Microsoft. Aucune installation n'est requise ; exécutez simplement l'exécutable sur la machine physique que vous souhaitez convertir.

2. Sélectionnez les disques ou volumes à convertir

Dans la fenêtre de Disk2vhd, vous verrez une liste de tous les disques et volumes disponibles sur la machine physique. Cochez les cases à côté des disques ou des volumes que vous souhaitez inclure dans la conversion, généralement le disque système (C:) et tous les disques de données supplémentaires. Notez que Disk2vhd peut effectuer la conversion tandis que le système est en ligne, réduisant ainsi le temps d'arrêt.

3. Spécifiez l'emplacement et le format de sortie

Output folder : Choisissez l'emplacement où vous souhaitez que Disk2vhd enregistre les fichiers VHD ou VHDX résultants. Assurez-vous qu'il y a suffisamment d'espace libre à l'emplacement spécifié pour accueillir les disques convertis.

Virtual hard disk format : Sélectionnez soit VHD soit VHDX. VHDX est généralement préféré pour ses limites de taille plus grandes et ses fonctionnalités avancées.

4. Initiez la Conversion

Cliquez sur **Create** pour démarrer le processus de conversion. Disk2vhd créera des images de disque virtuel des disques ou volumes sélectionnés, qui pourront ensuite être attachés à une nouvelle machine virtuelle Hyper-V.

5. Importer le VHD/VHDX dans Hyper-V

Une fois la conversion terminée, copiez les fichiers VHD ou VHDX générés sur l'hôte Hyper-V. Sur l'hôte Hyper-V :

a. Créez une nouvelle machine virtuelle à l'aide de l'Assistant Nouvelle Machine Virtuelle.
b. Pendant l'assistant, spécifiez les paramètres souhaités pour le nouveau VM, tels que l'allocation de mémoire, la configuration réseau et les services d'intégration.
c. Lorsqu'on vous demande de choisir un disque dur virtuel, sélectionnez Utiliser un disque dur virtuel existant et naviguez jusqu'à l'emplacement où vous avez copié les fichiers VHD/VHDX convertis.
d. Terminez l'assistant et votre machine physique convertie sera maintenant disponible en tant que machine virtuelle Hyper-V.

B. La migration V2V

La migration virtuelle à virtuelle est un processus consistant à migrer des machines virtuelles d'une plateforme de virtualisation à une autre. Il implique l'exportation de la configuration, des images de disque et des paramètres réseau des machines virtuelles, puis les importe sur la plateforme cible. Cette approche permet aux organisations d'assurer une migration et une mise à niveau fluides des machines

virtuelles et des applications lorsqu'elles doivent apporter des modifications à l'infrastructure de virtualisation ou regrouper différentes plateformes de virtualisation.

La migration virtuelle vers virtuelle n'est pas limitée à la même plateforme de virtualisation ; elle peut également être réalisée entre des plateformes de virtualisation différentes. Par exemple, passer de KVM à KVM ou de VMware à KVM est possible et n'exige pas que le type de machine virtuelle soit identique. Cette flexibilité prend en compte les différences entre les différents hôtes et les matériels virtuels, permettant aux machines virtuelles de migrer entre différents hôtes physiques pour un déplacement transparent des systèmes d'exploitation et des données.

C. Comment effectuer une migration virtuelle vers virtuelle ?

Lors d'une migration V2V, il est fréquent de devoir convertir le disque virtuel ou utiliser des outils de conversion VM v2v pour garantir le bon fonctionnement des machines virtuelles sur la plateforme cible. Ces outils de conversion VM v2v gèrent les problèmes de compatibilité entre les plateformes source et cible et réalisent les conversions et ajustements nécessaires pour assurer le démarrage et le bon fonctionnement des VM migrées. Voici 3 méthodes pour réaliser une migration V2V.

Type 1 : Migration hors ligne V2V

La migration hors ligne est également appelée migration régulière ou migration statique. Elle nécessite que la machine virtuelle soit suspendue avant la migration. Dans le cas d'un stockage partagé, seule l'état du système sera copié sur l'hôte de destination, servant à la reconstruction ultérieure de la machine virtuelle et à la restauration des tâches. Dans le cas d'un stockage local, à la fois l'image et l'état de la machine virtuelle seront copiés simultanément sur l'hôte de destination. Du point de vue de l'utilisateur, il y a une période claire de temps où le service n'est pas disponible. Ce type de méthode de migration est simple et facile à mettre en œuvre, et convient aux situations où la disponibilité du service n'est pas strictement requise.

Type 2 : Migration en ligne V2V

La migration en ligne, également appelée migration en direct, consiste à migrer une machine virtuelle (VM) tout en maintenant le fonctionnement normal des services sur cette VM.

La machine virtuelle est toujours en cours de migration entre différents hôtes physiques, et les étapes logiques sont quasiment identiques à la migration hors ligne. La différence réside dans le fait que, afin de garantir la disponibilité des services VM pendant le processus de migration, ce dernier présente une temps d'arrêt très court. Au stade préalable de la migration, le service fonctionne sur l'hôte source. Au stade précédent de la migration, le service fonctionne sur l'hôte source. Lorsque la migration atteint un certain stade, l'hôte de destination disposera alors des ressources nécessaires pour exécuter le système. Après un basculement très rapide, l'hôte source transférera le rôle d'administration à l'hôte de destination et le service continuera de s'exécuter sur l'hôte de destination. Pour le service en lui-même, étant donné que le temps de commutation est très court, les utilisateurs ne percevront pas d'interruption du service, donc le processus de migration est transparent pour eux. Comparé à la migration hors ligne, la migration en ligne convient aux scénarios nécessitant une haute disponibilité du service.

Actuellement, les outils de migration en ligne principaux, tels que **VMware VMotion** et **xenMotion** de XEN, nécessitent tous des dispositifs de stockage externe partagé centralisés tels que SAN (réseau de stockage) et NAS (stockage attaché au réseau) entre les machines physiques, afin que lors du traitement de la migration, les utilisateurs n'aient qu'à prendre en compte la migration de l'état d'exécution de la mémoire du système d'exploitation, ce qui permet d'obtenir une meilleure performance de migration.

De plus, dans certains cas où le stockage partagé n'est pas utilisé, la technologie de migration en ligne des blocs de stockage peut être utilisée pour mettre en œuvre la migration en ligne des machines virtuelles V2V. Par rapport à la migration en ligne basée sur le stockage partagé, ce type de méthode nécessite une migration simultanée des images de disque de la machine virtuelle et des états de la mémoire système, ce qui réduit les performances globales de la migration. Cependant, elle permet de transférer l'environnement informatique dans un scénario de stockage local distribué et d'assurer la disponibilité des services du système d'exploitation pendant le processus de migration, élargissant ainsi le champ d'application de la migration de machines virtuelles en ligne.

La technologie de migration en ligne V2V élimine la dépendance entre le logiciel et le matériel, constituant ainsi un outil puissant pour les opérations de gestion telles que les mises à niveau et l'entretien des systèmes logiciels et matériels.

Type 3 : Technologie de migration de mémoire V2V

Pour la migration de l'état de mémoire des VM, à la fois XEN et KVM utilisent la stratégie prédominante de pré-copie. Une fois le processus de migration démarré, la VM de la machine source continue de fonctionner tandis que celle de la machine cible est désactivée. La première boucle envoie toutes les données de pages de mémoire depuis la VM de la machine source vers celle de la machine cible, et chaque boucle subséquente envoie ensuite les pages sales de la mémoire qui ont été écrites par la VM lors du tour précédent de pré-copie. Jusqu'à ce que le moment soit propice pour la fin de la boucle de pré-copie, une phase de copie d'arrêt débutera. La machine source sera suspendue et ne génèrera plus de mises à jour de mémoire. Les pages sales du dernier tour de boucle sont transférées vers la VM de la machine cible. Ce mécanisme de pré-copie réduit considérablement la quantité de données de mémoire à transmettre pendant la phase de copie d'arrêt, réduisant ainsi de manière significative le temps d'arrêt.

Deux cas de migration V2V à faire comme TP :

1 : VMware vMotion

vMotion chez VMware est une fonctionnalité qui permet la migration en direct des machines virtuelles d'un hôte à un autre, sans interruption de service. Cela signifie que la machine virtuelle continue à fonctionner normalement pendant la migration, sans nécessiter de redémarrage

En résumé, vMotion permet de :

- **Migrer des machines virtuelles "à chaud" :** C'est-à-dire sans interrompre leur fonctionnement.
- **Transférer les données de la machine virtuelle :** Cela inclut l'état de la mémoire, l'état des périphériques et les disques virtuels.

- **Réduire les temps d'arrêt :** vMotion permet de maintenir la disponibilité des machines virtuelles pendant la migration.

Fonctionne de vMotion . La migration se fait en plusieurs étapes :

1. **Connexion à vCenter :** Il est nécessaire d'avoir un vCenter pour gérer les hôtes et les clusters.
2. **Sélection de la machine virtuelle :** On choisit la machine virtuelle que l'on souhaite migrer.
3. **Choix de l'hôte de destination :** On sélectionne l'hôte sur lequel la machine virtuelle sera déplacée.
4. **Migration :** vMotion transfère les données de la machine virtuelle vers le nouvel hôte, tout en maintenant le fonctionnement de la machine virtuelle.
5. **Transfert de l'exécution :** Une fois le transfert des données terminé, la machine virtuelle passe à l'exécution sur le nouvel hôte.

Les types de vMotion :

- **vMotion standard :** Permet de migrer la machine virtuelle en cours d'exécution d'un hôte à un autre.
- **Storage vMotion :** Permet de migrer le stockage (disques virtuels) d'une machine virtuelle d'un datastore à un autre, sans interruption.

2 : Migrer des machines virtuelles VMware ESXi vers Hyper-V

Suivez les étapes décrites sur le site : https://www.it-connect.fr/chapitres/hyper-v-migration-vm-vmware-esxi-vers-hyper-v/

C. La migration V2P

Le transfert de machine virtuelle vers machine physique (V2P) implique le transfert ou le portage d'une machine virtuelle vers une machine physique. Ce terme désigne la migration d'un système d'exploitation (SE), de programmes d'application et de données d'une VM ou d' une partition de disque vers le disque dur principal ou le disque SSD (Solid State Drive) d'un système cible. La cible peut être un ou plusieurs ordinateurs.

V2P permet de restaurer le contenu d'un disque dur d'un ordinateur ou d'un serveur réseau défaillant à partir d'un support de sauvegarde tel qu'un lecteur de bande. Il peut également être utilisé en conjonction avec une migration physique vers virtuelle (P2V) pour copier le système d'exploitation, les applications et les données d'un ordinateur vers une machine virtuelle, puis de cette machine virtuelle vers d'autres ordinateurs.

Démarrer avec le virtuel vers le physique

Il existe deux raisons principales pour lesquelles une migration V2P peut être nécessaire : pour convertir un fichier de disque dur virtuel (VHDX) en un lecteur physique et lorsqu'un environnement physique est requis pour certains déploiements.

Le V2P peut être réalisé manuellement en définissant l'environnement physique cible, par exemple un lecteur spécifique, puis en y installant le système d'exploitation, les applications et les données depuis l'environnement virtuel. Cependant, ce processus peut s'avérer complexe et incertain, surtout si le matériel du nouvel environnement diffère sensiblement de l'ancien.

Défis et bonnes pratiques pour la migration V2P

Bien qu'une migration V2P soit possible, le processus peut parfois échouer. Pour minimiser les risques d'échec, il est conseillé de suivre certaines bonnes pratiques.

Avant de lancer le processus V2P, il est essentiel d'effectuer une sauvegarde complète de la VM à convertir. Il est également important de connaître les identifiants d'un administrateur local (nom d'utilisateur et mot de passe), car lors du premier démarrage de la VM, celle-ci risque de ne pas disposer d'une connexion réseau et les identifiants mis en cache risquent de ne pas fonctionner.

Les problèmes de pilotes matériels, notamment l'incompatibilité des pilotes chargés avec le matériel présent, constituent un défi courant lors de la migration V2P. Pour réduire ce risque, il est conseillé de conserver un matériel aussi générique que possible en déplaçant les disques vers la chaîne IDE virtuelle pendant toute la durée du processus.

Tout le matériel en mode BIOS doit être adapté aux machines virtuelles de génération 1, et le matériel en mode UEFI doit être adapté aux machines virtuelles de génération 2. Il est également important de supprimer toutes les informations IP statiques de tous les adaptateurs virtuels.

Avant de continuer, la machine virtuelle doit être éteinte. Pour créer une image propre, utilisez un logiciel d'imagerie.

Une fois tous les éléments transférés de la VM vers la machine cible, il est essentiel de les tester pour vérifier que tout fonctionne correctement. Si tel est le cas, la VM source peut être supprimée.