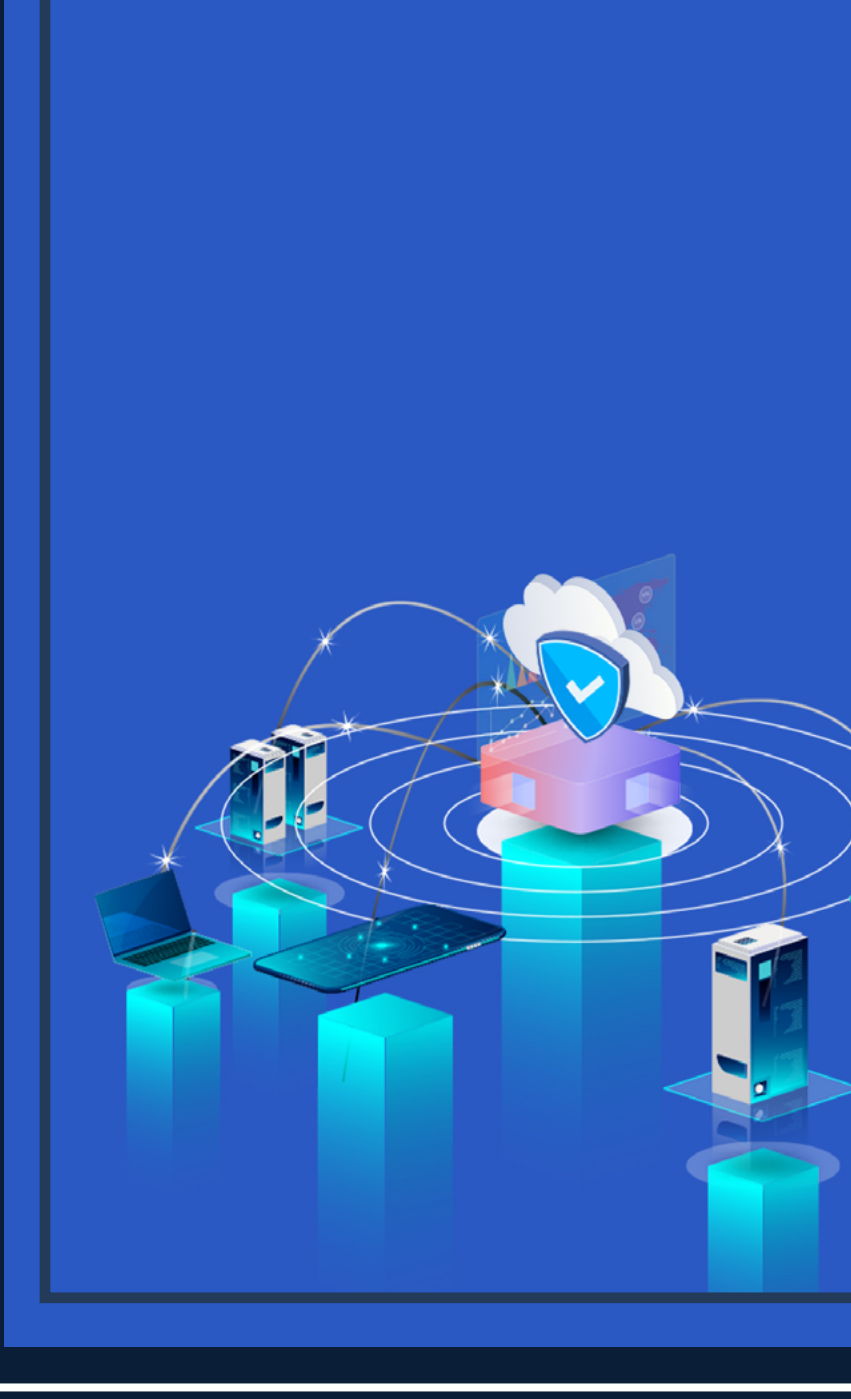
CCN-CERT

BP/15



Meilleures pratiques en matière de virtualisation

RAPPORT DE BONNES PRATIQUES

AOÛT **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Ëditér par

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP SEP-M-SW-KPSC, ou=sello electronico, serialNumber=S2800155J, o=CENTRO CRIPTOLÓGICO NACIONAL, c=ES 2021.09.11 08:36:18 +02'00'

Centro Criptológico Nacional, 2021

Date d'édition: Août 2021

Index

1. À propos du CCN-CERT, certificat gouvernemental national 5
2. Introduction 6
3. Les types de virtualisation 8
4. Les défis de la sécurité dans la virtualisation 9
5. Les types de réseaux virtualisés 10
6. Meilleures pratiques Hyper-V 11
6.1 Création de machines virtuelles et allocation de ressources 13
6.1.1 Mémoire RAM 14
6.1.2 Disc 16
6.2 Protection des ressources des machines virtuelles 18
6.3 Cifring 20
6.4 Isolation et configuration du réseau 23
6.5 Gestion des extensions de commutateurs 28
6.6 Services d'intégration 30
6.7 Sécurité basée sur la virtualisation pour les machines virtuelles de génération 32
6.8 Points de contrôle 33

7. Meilleures pratiques VMware Workstation / Player 34
7.1 Le cryptage et la restriction des machines virtuelles 35
7.2 Configuration des ressources 37
7.3 Isolation et configuration du réseau 39
7.4 Outils VMware 40
7.5 Protection des machines virtuelles sur les hôtes 41
7.6 Transfert de fichiers et de textes 42
7.7 Des instantanés de machines virtuelles 44

Index

8. Meilleures pratiques en matière de VirtualBox 45

8.1 Le cryptage des machines virtuelles 47

8.2 Isolation et configuration du réseau 50

8.3 Partage du presse-papiers 53

8.4 Drag and drop 54

8.5 Dossiers partagés 55

8.6 Instantanés dans VirtualBox 57

9. Machine de navigation sûre 58

10. Décalogue de recommandations 59

11. Glossaire 61

1. À propos du CCN-CERT, certificat gouvernemental national

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont définies dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma national de sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyber-incidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

2. Introduction

La virtualisation est un terme qui a été utilisé pour de multiples technologies. Dans le monde de l'informatique, on l'entend comme la recréation d'une ressource physique (matériel) ou logique (logiciel), au moyen d'un hyperviseur qui permet l'exécution de plusieurs environnements en même temps. Dans l'environnement de la machine virtuelle, l'hyperviseur permet l'utilisation simultanée du matériel pour plus d'un système d'exploitation, contrôle la couche physique (RAM, CPU, disque, etc.), à laquelle il est le seul à avoir accès, et présente aux machines virtuelles une interface matérielle compatible.

L'ordinateur qui fournit le support physique et sur lequel l'hyperviseur est installé est appelé l'hôte. La machine virtuelle qui interagit avec l'hyperviseur et où un système d'exploitation complet est généralement installé est appelée invité. Le nombre de machines virtuelles qu'un hôte peut prendre en charge dépend directement des ressources physiques disponibles et des exigences de chaque invité.

L'hyperviseur gère l'accès aux différentes ressources de manière individuelle et avec des degrés d'isolation variables, en fonction du modèle et des besoins. Sans elle, le matériel aurait des problèmes de décision lorsqu'il s'agit de répondre aux demandes d'utilisation de systèmes non connectés et non coordonnés.

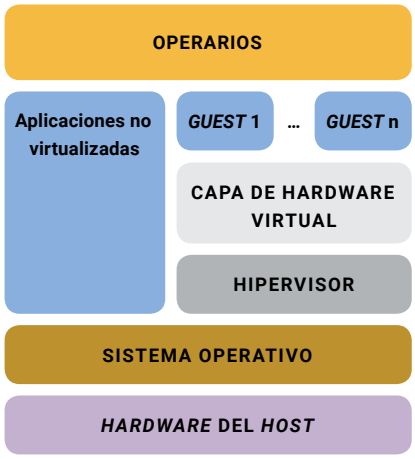
L'essor de la virtualisation s'est accompagné de l'utilisation du cloud, où ce système de partage des ressources est devenu presque indispensable. Bien qu'il existait déjà de multiples systèmes proposés par de nombreux fabricants, le développement et les progrès de ces systèmes ont augmenté de manière exponentielle. Actuellement, XenServer de Citrix, VMware ESXi de Dell, Oracle VM Server d'Oracle, VirtualBox d'Oracle et Hyper-V de Microsoft, entre autres, sont disponibles..

Le nombre de machines virtuelles qu'un *hôte* peut prendre en charge dépend directement des ressources physiques disponibles et des exigences de chaque *invité*

En ce qui concerne Microsoft, la multinationale a intégré des outils de virtualisation depuis le milieu de la première décennie de ce siècle. Avec la distribution du système d'exploitation Windows Server 2008, la version initiale de Hyper-V a été publiée. Depuis lors, à chaque nouvelle version, un hyperviseur doté de capacités plus nombreuses et améliorées a été inclus.

VMware a commencé à travailler sur la virtualisation en 1998. Cette société, filiale de Dell, est actuellement l'un des principaux fournisseurs de ce type de logiciels. Son hyperviseur fonctionne sur les principaux systèmes d'exploitation du marché (Windows, Linux et Mac OS). En outre, il dispose d'une version spécifique qui permet à l'hyperviseur de fonctionner sur du matériel de serveur physique, sans avoir besoin d'un système d'exploitation supplémentaire. Il offre également la possibilité de l'installer à partir d'une clé USB, de sorte que les ordinateurs dotés d'une entrée USB peuvent l'exécuter sans utiliser les disques durs, qui sont libérés pour les machines virtuelles.

VirtualBox, quant à lui, a été lancé en 1997 pour offrir un logiciel de virtualisation pour tous les principaux systèmes d'exploitation, y compris Solaris. Sa facilité d'utilisation et la licence GNU (General Public License version 2) l'ont rendu très populaire, notamment dans les environnements de bureau. Il appartient désormais à Oracle, qui possède également un autre hyperviseur performant (Oracle VM Server) conçu pour les entreprises et les environnements en nuage.



[Illustration 1]
Exemple d'un diagramme d'assemblage de plusieurs machines virtuelles.

L'essor de la virtualisation s'est accompagné de l'utilisation du cloud

3. Les types de virtualisation

Les principales taxonomies de la virtualisation dépendent de la manière dont le matériel est distribué et de ce qu'est l'élément virtualisé. En ce qui concerne le premier point, on appelle partitionnement la répartition d'une ressource physique telle que la RAM, le CPU, etc. L'une des façons d'y parvenir est d'attribuer des valeurs absolues et statiques (partitionnement dur).

Dans ces cas, la somme des ressources partielles sera toujours égale ou inférieure à la valeur totale existante. Par exemple, si un hôte à huit coeurs héberge trois machines virtuelles auxquelles on a attribué deux coeurs chacune, seule une nouvelle machine à un coeur peut être incluse (l'autre coeur doit être destiné au système d'exploitation et à l'hyperviseur). Ce mode d'allocation garantit des ressources et une plus grande isolation, mais n'optimise pas les éléments matériels.

Dans certains cas, afin d'optimiser les ressources, la majorité des hyperviseurs permettent une distribution des ressources avec sur-allocation (soft partitioning). En poursuivant l'exemple précédent, dans cet environnement, la somme des coeurs peut être supérieure au nombre réel de coeurs disponibles sur la machine. La raison de cette autorisation est que toutes les machines virtuelles n'atteindront jamais simultanément l'utilisation maximale de la capacité de traitement. Si tel était le cas, une distribution proportionnelle serait effectuée.

Lorsque vous souhaitez classer les éléments virtualisés par catégorie, les principales possibilités de virtualisation sont le matériel, les applications ou les sessions utilisateur.

Ce guide se concentre sur la virtualisation du matériel informatique, tant avec le partitionnement souple qu'avec le partitionnement dur.

Ce guide se concentre sur la virtualisation du matériel informatique, tant avec le partitionnement souple qu'avec le partitionnement dur

4. Les défis de la sécurité dans la virtualisation

La sécurité dans la virtualisation repose sur le même principe que tout autre système, à savoir "minimiser la surface d'exposition". Cependant, elle présente des particularités qui rendent la sécurisation de cette surface plus difficile, comme la multitude de ressources partagées ou les systèmes d'exploitation qui fonctionnent simultanément avec leurs propres applications sur la même machine physique.

Dans une situation où vous avez un hôte Windows 10 où plusieurs invités sont virtualisés avec la même version du système d'exploitation, vous devrez multiplier les efforts pour protéger chacune des machines (*hôte* et *invité*). Si vous incluez un système d'exploitation diamétralement différent, comme Oracle Linux, les efforts augmentent proportionnellement, mais les connaissances requises de l'administrateur système sont doublées. En outre, de bonnes pratiques de sécurité spécifiques aux hyperviseurs et à leur gestion doivent être appliquées.

Pour réduire la complexité de la gestion de ce type d'environnement, les fabricants appliquent leurs propres mesures (intégrées), qui sont de plus en plus efficaces et sûres : SMB 3.0 (avec cryptage de bout en bout), isolement du réseau, extensions de réseau, etc.

Les considérations générales qui s'appliquent aux systèmes non virtualisés doivent également être prises en compte. Par exemple, la navigation sur le web et le courrier électronique sont deux des principaux vecteurs d'attaque d'un système. Il n'existe pas de "configuration absolument sûre", mais un certain nombre de mesures de sécurité raisonnablement adéquates peuvent toujours être mises en oeuvre pour obtenir un environnement de travail fiable pour l'ensemble hyperviseur-hôte-invité.

En définitive, le principal enjeu de la virtualisation, en matière de sécurité, est de traiter le système comme s'il s'agissait d'un centre complet de traitement de données où sont établies des mesures périmétriques (appliquées à l'hôte) et des mesures individuelles pour chacune des machines hébergées sur celui-ci (appliquées à l'hôte et à chacune des machines virtuelles).

> **La navigation sur le web et le courrier électronique sont deux des principaux vecteurs d'attaque d'un système**

5. Les types de réseaux virtualisés

Lorsque vous créez des machines virtuelles sur un hôte unique, vous pouvez attribuer toutes les interfaces réseau physiques à un seul invité, associer toutes les machines virtuelles à un seul adaptateur ou effectuer une distribution plus équilibrée.

Dans la mesure du possible, il faut essayer de rationaliser l'allocation des ressources, car la surcharge d'une carte réseau par de nombreux invités pénalise considérablement les performances. Ceci est observable sur les serveurs physiques, mais encore plus sur les ordinateurs portables ou de bureau où il est difficile d'avoir plus d'une connexion réseau, soit à cause de l'équipement lui-même, soit à cause du manque de connexions disponibles sur les postes de travail des utilisateurs. En outre, l'utilisation individualisée des interfaces réseau va à l'encontre de l'esprit de la virtualisation, où l'utilisation des ressources par plus d'une instance est presque la norme.

Pour toutes ces raisons, les fournisseurs ont mis en place des stratégies de virtualisation du réseau qui permettent de partager la bande passante d'une ou plusieurs interfaces entre toutes les machines qui en ont besoin et qui sont hébergées sur l'hôte. La raison en est la création de cartes réseau virtuelles au niveau de la couche d'abstraction de la virtualisation, gérée par l'hyperviseur, qui sont attribuées aux invités. Les cartes réseau peuvent ensuite être laissées isolées ou connectées aux périphériques du réseau physique.

Le commutateur virtuel ajoute des fonctionnalités supplémentaires en étant une forme de partage du matériel du réseau hôte, dont l'équivalent dans un réseau de données physique serait l'installation d'un commutateur conventionnel. Il est créé et géré par l'hyperviseur, possède des fonctionnalités de couche 2 du modèle OSI, permettant par exemple la création de VLANs.

En outre, le fait de disposer de plusieurs commutateurs virtuels permet de gérer les réseaux d'invités avec un niveau d'isolation plus élevé.

La raison en est la création de cartes réseau virtuelles au niveau de la couche d'abstraction de la virtualisation, gérée par l'hyperviseur, qui sont attribuées aux *invités*

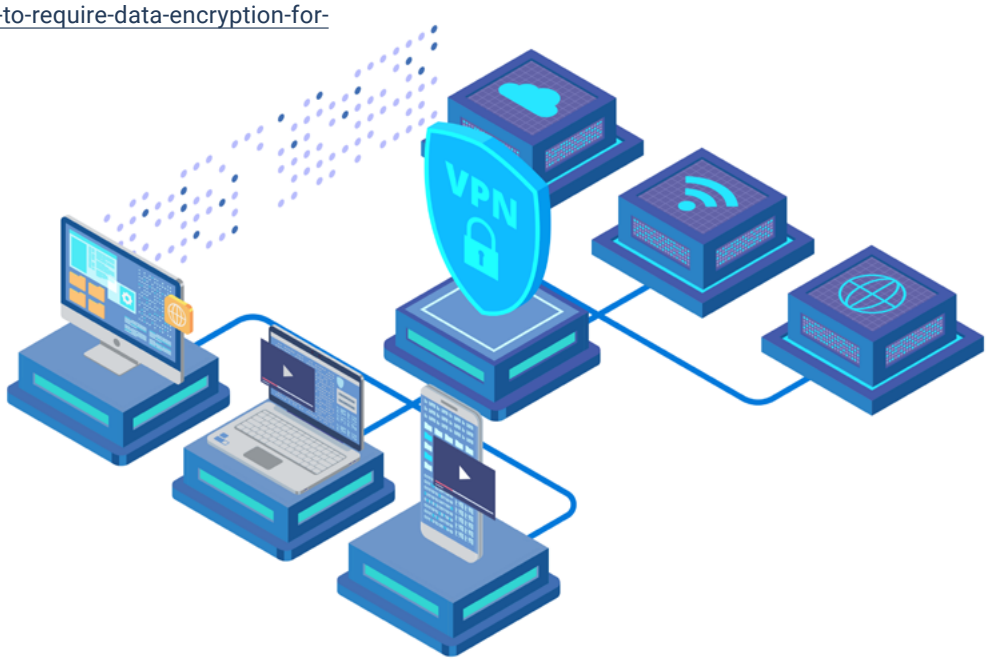
6. Meilleures pratiques Hyper-V

Hyper-V a deux (2) options d'installation sur les serveurs : le mode core et le mode graphique. La différence fondamentale est que le mode central ne dispose pas d'un environnement de gestion graphique à partir de la machine locale.

En termes de bonnes pratiques, celles-ci doivent être *orientées vers l'hôte* en premier lieu, puis vers chacune des machines hébergées.

L'administration de l'hyperviseur de Microsoft permet une gestion à distance. Cependant, il n'est pas recommandé de le faire uniquement avec les mesures propres au système, et des mesures supplémentaires telles que le cryptage des données de la connexion devraient être ajoutées. Voir la section "Setting Namespace Security to Require Data Encryption for Remote Connections" dans l'article Securing a Remote WMI Connection disponible via le lien suivant.

https://docs.microsoft.com/es-es/windows/desktop/WmiSdk/securing-a-remote-wmi-connection#setting-namespace-security-to-require-data-encryption-for-remote-connections



En ce qui concerne les systèmes d'accueil, les bonnes pratiques suivantes doivent être prises en compte :

a. **Mettre en place une gestion correcte des permissions, en empêchant l'accès aux fichiers à tout utilisateur qui n'en a pas besoin, que ce soit à distance ou localement.**

b. **Synchroniser le temps pour permettre un audit et un enregistrement fiables.**

c. **Gérez vos fichiers en toute sécurité. Pour ce faire, les fichiers seront cryptés avec *BitLocker* et ceux qui ne sont pas utilisés seront supprimés avec des outils sécurisés tels que Eraser pour Windows ou KillDisk pour GNU/Linux, ainsi que d'autres tels que HDDEraser (autodémarrage pour l'effacement total des disques).**

d. **Maintenir à jour les services d'hôte, d'invité et d'intégration. Au minimum, les correctifs de sécurité considérés comme importants et critiques doivent être installés.**

e. **Utilisez un produit de prévention des codes malveillants et des solutions de pare-feu sur les ordinateurs invités ou utilisez des extensions de commutateur qui les intègrent. L'application simultanée des deux options n'est pas incompatible.**

f. **Évitez d'avoir des CD ou DVD actifs sur les clients, car les images ISO elles-mêmes montées à partir du disque dur de l'hôte pourraient être un élément qui augmente la surface d'exposition.**

g. **Maintenez une isolation maximale du réseau, en ne créant que les connexions essentielles.**

h. **Dans la mesure du possible, évitez de partager les ressources entre les machines virtuelles ou avec l'hôte. En cas de nécessité absolue, maintenez une politique d'autorisation aussi restrictive que possible.**

Dans le cadre de la continuité du service, il est fortement recommandé d'effectuer des sauvegardes. Les fichiers de sauvegarde peuvent être stockés localement, sur les ressources du réseau ou sur des supports amovibles (par exemple, un disque dur USB externe). Dans ces cas, le cryptage des données est une nécessité, une mesure qui doit être imposée à tous les supports utilisés, qu'ils soient internes ou externes.

Les fichiers de sauvegarde peuvent être stockés localement, sur les ressources du réseau ou sur des supports amovibles

6.1 Création de machines virtuelles et allocation de ressources

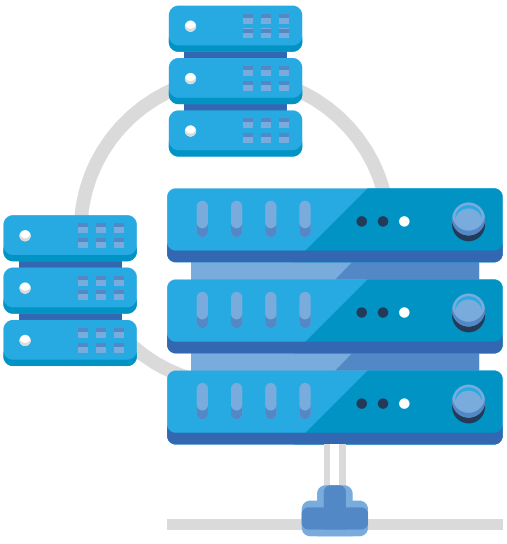
Pour créer un invité dans Hyper-V, on utilise un assistant qui est très similaire dans Windows 10 Professionnel ou Entreprise et dans les versions serveur. Cet assistant permet à la fois la création rapide de machines virtuelles et leur importation à partir d'autres environnements de virtualisation. La technologie de Microsoft prend en charge une grande variété de systèmes d'exploitation pour ordinateurs de bureau et serveurs, qu'il s'agisse de Windows ou de Linux.

L'allocation des ressources matérielles virtualisées peut se faire de deux manières. D'une part, à partir de Hyper-V Manager et dès que vous lancez l'assistant, tapez le nom de la machine et cliquez ensuite sur "Terminer". Dans ce cas, l'hyperviseur alloue automatiquement la RAM, l'espace disque et le réseau. En revanche, si vous choisissez de continuer avec l'assistant, vous pouvez définir manuellement les ressources et prendre en compte l'article de Microsoft sur l'optimisation des performances des serveurs Hyper-V, disponible via le lien suivant :

https://docs.microsoft.com/es-es/windows-server/administration/performance-tuning/role/hyper-v-server/

Afin d'utiliser correctement l'allocation des ressources, il est nécessaire de connaître certains concepts pour une meilleure gestion des ressources.

Afin d'utiliser correctement l'allocation des ressources, il est nécessaire de connaître certains concepts pour une meilleure gestion des ressources



6.1.1 Mémoire RAM

Dans Hyper-V, il existe deux (2) types d'allocation des ressources mémoire, l'allocation dynamique et l'allocation statique.

La mémoire dynamique est une fonctionnalité de Hyper-V qui permet à l'hyperviseur de gérer la consommation de RAM des invités d'un *hôte de manière flexible*. Par exemple, l'hyperviseur peut ajouter dynamiquement plus de RAM à un *invité* lorsque le système d'exploitation en a besoin ou récupérer l'excès de RAM lorsque l'*invité* est inactif. Cette technologie est particulièrement utile lorsque vous disposez d'un grand nombre de machines virtuelles inactives ou sous-exploitées.

Lorsque vous décidez d'utiliser la mémoire dynamique, vous devez définir certaines valeurs de configuration pour celle-ci. Si vous optez pour l'allocation statique, vous devez être particulièrement prudent avec les machines en cours d'exécution, car la RAM que vous choisissez sera réservée à l'invité dès son démarrage, même si vous ne l'utilisez pas.

Pour cette raison, il est nécessaire de faire particulièrement attention aux machines avec lesquelles vous commencez, en ne choisissant que celles qui sont essentielles.

- **Boot RAM :** est la quantité de RAM allouée à un *invité* au moment du démarrage. Cette valeur peut être identique à la "RAM minimale" ou supérieure, jusqu'à la "RAM maximale". La valeur de la RAM de démarrage ne peut être modifiée que lorsque la machine virtuelle est hors tension. Une fois que le démarrage de la machine virtuelle est terminé et que l'hyperviseur a démarré, il tentera d'utiliser la quantité de RAM configurée comme étant la RAM minimale.
- **RAM minimale :** La quantité minimale de RAM que l'*hôte* doit essayer d'allouer à une machine virtuelle lorsqu'elle démarre. Lorsque plusieurs mémoires demandent de la mémoire, l'hôte Hyper-V peut réaffecter la RAM de la machine virtuelle jusqu'à ce que sa valeur minimale de RAM soit atteinte.
- **RAM maximale :** est la quantité maximale de RAM que l'*hôte* fournira à la machine virtuelle. Cette option ne peut être augmentée que lorsque la machine virtuelle est en cours d'exécution et ne peut être diminuée que si la machine virtuelle est éteinte.
- **Mémoire tampon :** Il s'agit du pourcentage de mémoire que Hyper-V doit allouer à la machine virtuelle en tant que tampon. La valeur peut être définie dans une fourchette de 5 % à 200 %, 20 % étant la valeur par défaut.
- **Poids de la mémoire :** La priorité qui est configurée pour une machine virtuelle par rapport aux autres machines virtuelles fonctionnant sur le même hôte Hyper-V.

L'allocation statique de mémoire implique la réservation de la mémoire totale disponible sur l'*hôte*, ce qui se traduit par la nécessité de dimensionner correctement l'allocation afin qu'elle ne dépasse pas la mémoire totale disponible, en tenant compte des invités qui peuvent être actifs en même temps.

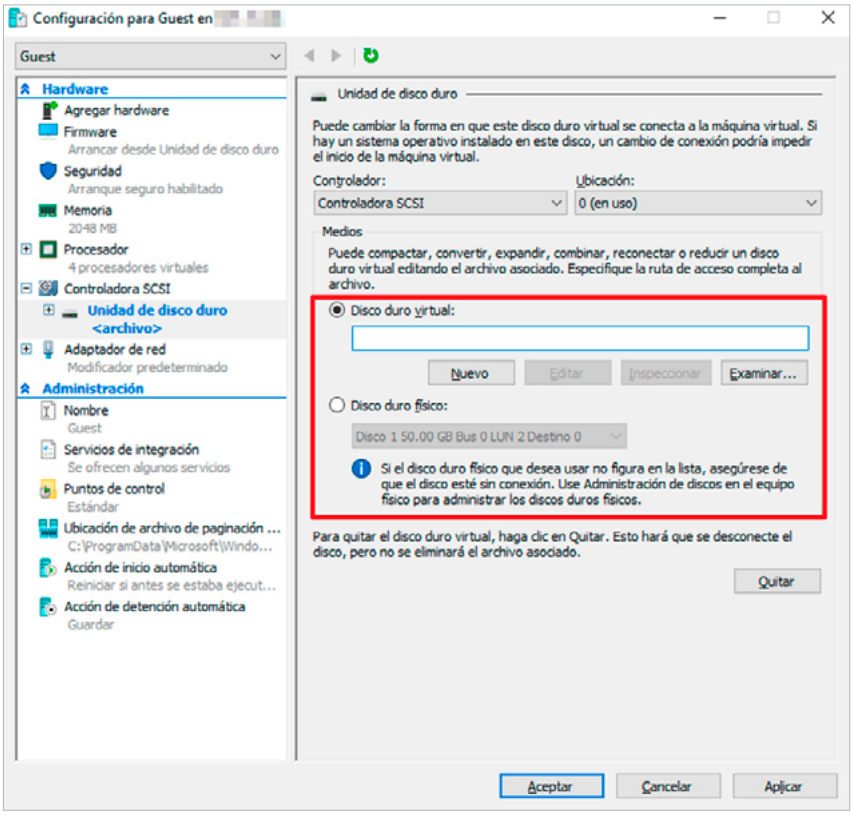
L'allocation statique de mémoire implique la réservation de la mémoire totale disponible sur l'*hôte*, ce qui se traduit par la nécessité de dimensionner correctement l'allocation

6.1.2 Disc

En termes d'allocation d'espace de stockage, il existe plusieurs configurations concernant le disque et les types de disques à sélectionner dans Hyper-V.

Deux (2) modèles de disques peuvent être créés ou attribués selon les besoins :

- **Disque dur virtuel :** il s'agit d'un disque qui est créé dans l'*hôte* pour être associé à la machine virtuelle où toutes les informations générées peuvent être stockées. Ces disques sont les plus utilisés car ils génèrent leur propre fichier qui peut subir diverses modifications tout en conservant la capacité de stockage, en étant capable d'effectuer, par exemple, des exportations, des points de contrôle, etc.
- **Disque dur physique :** cette configuration vous permet d'associer un disque appartenant à l'*hôte* (matériel réel) à la machine virtuelle. Cette option peut être utile dans certaines circonstances, cependant, le disque reste associé à la machine virtuelle et l'*hôte* ne peut pas utiliser le disque à d'autres fins. En outre, il faut tenir compte du fait que les performances fournies par le disque dans l'invité en dépendent directement. Pour pouvoir sélectionner cette option, le disque doit être en mode "hors ligne" sur l'*hôte*.



[Illustration 2] Sélection du disque dur dans l'assistant.

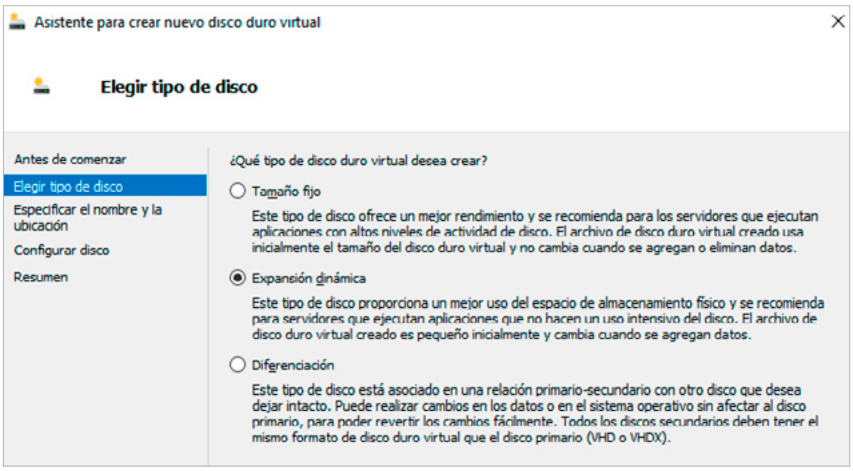
Quant au type de disque virtuel, les options suivantes peuvent être sélectionnées :

a. **Taille fixe :** Les disques durs virtuels fixes offrent une capacité de stockage en utilisant un fichier dont la taille est spécifiée pour le disque dur virtuel au moment de la création du disque. La taille du fichier reste "fixe", quelle que soit la quantité de données stockées. Cependant, l'assistant d'édition de disque dur virtuel peut être utilisé pour augmenter la taille du disque dur virtuel, ce qui augmente la taille du fichier. Ce paramètre est recommandé lorsque l'*invité* mis en oeuvre nécessite beaucoup de lecture/écriture du disque lui-même.

b. **Expansion dynamique :** Les disques durs virtuels de ce type fournissent la capacité de stockage nécessaire au stockage des données. La taille du fichier est petite lorsque le disque est créé et augmente jusqu'à la taille maximale allouée au fur et à mesure que des données sont ajoutées au disque. La taille du fichier ne diminue pas automatiquement lorsque les données sont supprimées du disque dur virtuel. Toutefois, il est possible de compacter le disque pour réduire la taille du fichier après avoir supprimé des données à l'aide de l'assistant d'édition de disque dur virtuel. Cette option est recommandée pour les machines virtuelles de test ou de laboratoire, ainsi que dans les environnements où l'on s'attend à une faible croissance et à une faible utilisation du disque.

c. **Différenciation :** Il s'agit de disques durs qui partent d'un disque dur virtuel primaire et permettent à l'utilisateur d'effectuer des modifications à partir de celui-ci sans l'altérer. Leur définition est exactement la même que celle du disque virtuel primaire en termes de type et de taille. La taille du fichier d'un disque de différenciation augmente au fur et à mesure que les modifications sont stockées sur le disque.

[Illustration 3] Sélection du "Type" de disque dur dans la machine virtuelle.

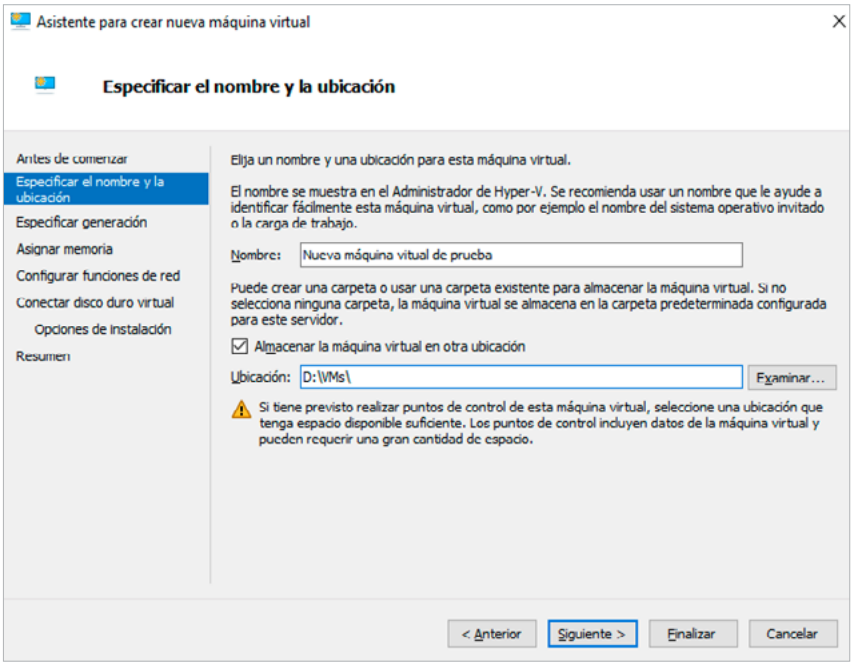


6.2 Protection des ressources des machines virtuelles

Chacune des machines virtuelles créées doit être protégée individuellement, à la fois dans les fonctionnalités attribuées par l'assistant de création et dans la machine elle-même.

Après le premier écran informatif de la première étape (où il n'est pas conseillé d'opter pour la création d'une machine avec des valeurs par défaut), dans la deuxième étape, vous devez sélectionner l'emplacement de la machine virtuelle. Il est conseillé d'utiliser un dossier dédié pour faciliter la protection de la machine virtuelle au moyen de permissions NTFS, du cryptage, etc. Si vous êtes sur une machine à un seul disque dur, vous devez considérer que l'utilisation de partitions peut réduire la surface d'exposition, mais cela est préjudiciable aux performances.

Le choix de l'emplacement peut faciliter la protection ultérieure de la machine virtuelle



[Illustration 4]
Sélection de l'emplacement de la machine virtuelle.

Le choix de l'emplacement peut faciliter la protection ultérieure de la machine virtuelle. À cette fin, le dossier dans lequel la définition de la machine virtuelle est stockée et les disques durs doivent avoir au moins les permissions suivantes :

[Tableau 1] Permissions de répertoire des machines virtuelles et des disques durs.

COMPTE	PERMIS	POSTULEZ À
Administrateurs	Contrôle total	Ce dossier, ses sous-dossiers et ses fichiers
Système	Contrôle total	Ce dossier, ses sous-dossiers et ses fichiers
Propriétaire du créateur	Contrôle total	Sous-dossiers et fichiers uniquement

Une fois que le dossier de destination finale des *invités qui seront* créés a été décidé, ce chemin peut être défini dans les propriétés générales de l'hyperviseur. Pour ce faire, cliquez sur "Hyper-V Configuration..." et dans la fenêtre qui s'ouvre, vous devrez modifier la configuration des sections "Disques durs virtuels" et "Machines virtuelles". Cela évite d'avoir à effectuer des modifications à chaque création de machine virtuelle.

Dans les cas où des utilisateurs ou des groupes supplémentaires doivent être ajoutés, il est recommandé d'utiliser le nombre minimum de permissions nécessaires et de les supprimer lorsqu'elles ne sont plus nécessaires. Microsoft, lors de l'installation de l'hyperviseur, crée le compte de groupe vide "Administrateurs Hyper-V". S'il est utilisé, il faut également lui donner des autorisations de contrôle total sur les dossiers.

Cette gestion de la liste de contrôle d'accès (ACL) empêchera les fichiers liés aux machines virtuelles d'être modifiés, copiés ou consultés sur le réseau de manière non autorisée par quiconque ne dispose pas d'une élévation de privilèges. Comme mesure supplémentaire, l'audit de l'accès aux dossiers d'hébergement des fichiers de virtualisation peut être activé pour suivre l'accès par les comptes autorisés et même pour les tentatives d'accès échouées à d'autres comptes.

Dans l'étape suivante, ce que Microsoft appelle la "Génération" est sélectionnée. Si le système d'exploitation invité peut fonctionner dans des environnements UEFI, la génération 2 doit être sélectionnée. L'UEFI offre une sécurité supplémentaire par rapport aux BIOS classiques.

REMARQUE :

pour en savoir plus sur l'interface micrologicielle extensible (UEFI) et obtenir ses spécifications, veuillez consulter le lien suivant : https://www.intel.es/content/www/es/es/architecture-and-technology/unified-extensible-firmware-interface/efi-homepage-general-technology.html

Le document CCN-CERT IA-08/15 BIOS Threats disponible via le lien suivant https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/789-ccn-cert-ia-08-15-amenaza-en-bios/file.html permet de renforcer la sécurité de ce type d'éléments

6.3 Cifred

Lorsque les machines virtuelles hébergées sur l'*hôte* l'exigent, les fichiers doivent être protégés à l'aide du cryptage *BitLocker*, à condition que la machine dispose de la capacité de cryptage BitLocker. Pour en savoir plus sur *BitLocker*, veuillez consulter le document Overview sur le site TechNet de Microsoft, disponible via le lien suivant.

https://docs.microsoft.com/es-es/previous-versions/windows/server/hh831713(v=ws.11)

Le chiffrement des fichiers au moyen de l'EFS (Encrypting File System) n'est pas une option valable, car cela ne permettrait pas l'utilisation des disques ou des fichiers de définition par des comptes autres que celui qui fournit le certificat utilisé pour le chiffrement. Dans certains environnements de domaine, des comptes de décryptage maîtres peuvent exister, mais il ne faut pas s'y fier sans être certain de leur existence. Vous trouverez plus d'informations sur le système de cryptage de fichiers (EFS) ici :

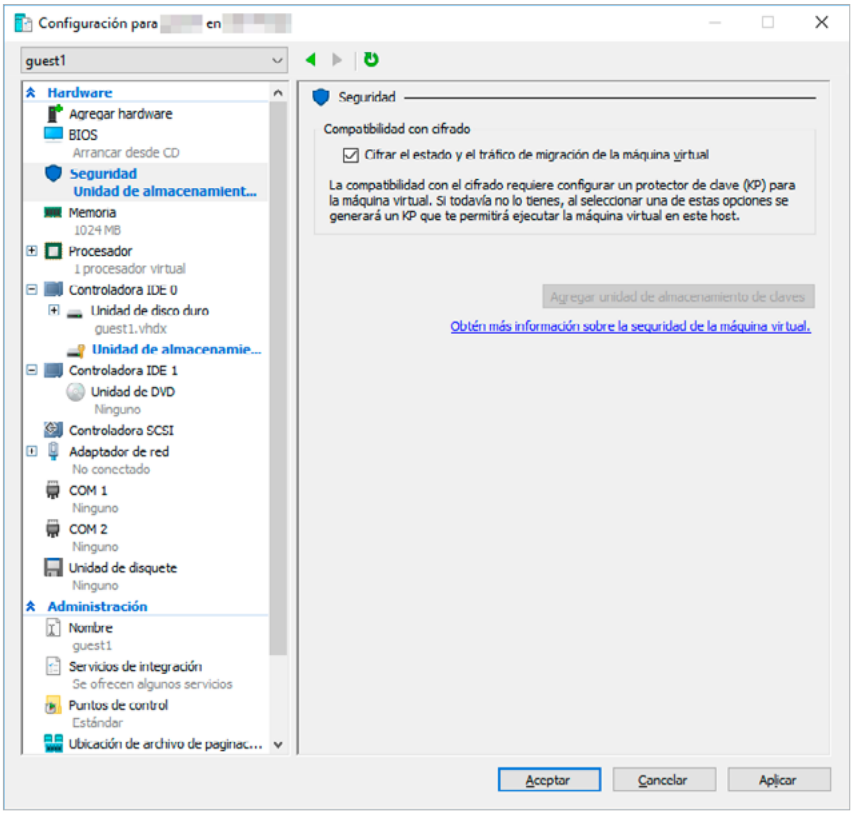
https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption

L'utilisation de *BitLocker* dans une machine virtuelle n'est pas généralement disponible. Cependant, le système EFS peut être utilisé, comme d'habitude, pour le cryptage de fichiers contenant des informations sensibles. Toutefois, toujours avec la mise en garde indiquée ci-dessus, concernant l'utilisateur unique qui peut y accéder.

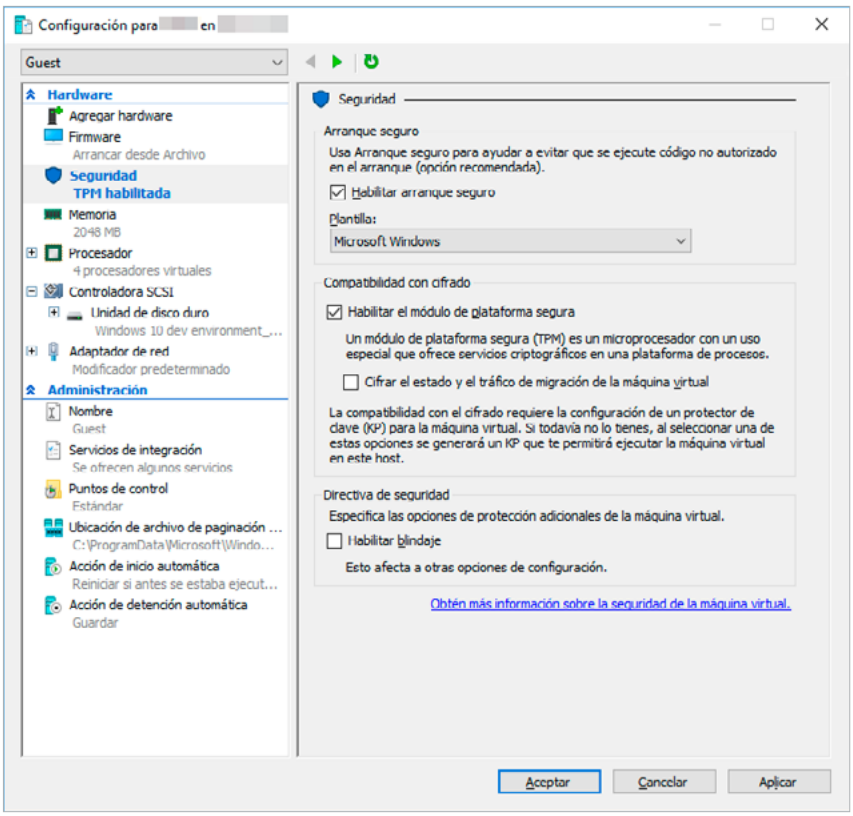
Jusqu'à présent, seules les machines virtuelles de génération 2 disposaient de la capacité de cryptage pour protéger les ressources qu'elles contiennent. La nouvelle version d'Hyper-V permet de protéger le disque du système d'exploitation à l'aide du cryptage de disque *BitLocker* sur les machines virtuelles de génération 1. Cette nouvelle fonctionnalité utilise un petit disque dédié pour stocker la clé *BitLocker* du disque système.

Lorsque les machines virtuelles hébergées sur l'*hôte* l'exigent, les fichiers doivent être protégés à l'aide du cryptage *BitLocker*

[Illustration 5] Configuration du chiffrement sur une machine de génération 1.



Comme indiqué ci-dessus, les machines virtuelles de génération 2 peuvent toujours utiliser la fonctionnalité d'une TPM virtuelle qui permet de crypter le disque de la machine virtuelle à l'aide de *BitLocker* comme s'il s'agissait d'une machine physique.



[Illustration 6] Configuration du chiffrement sur une machine de génération 2.

Une autre nouveauté d'Hyper-V 2016 est ce qu'on appelle les "Shielded Virtual Machines", qui permettent de crypter les machines virtuelles et leur état de manière à garantir qu'elles ne s'exécutent que sur des *hôtes* autorisés par le Host Protection Service. Vous trouverez de plus amples informations dans les liens suivants :

https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms-top-node

Les machines virtuelles blindées protègent les données et l'état de la machine virtuelle contre le vol et la manipulation des privilèges d'administrateur. Les machines virtuelles blindées fonctionnent avec les machines virtuelles de génération 2, qui fournissent le démarrage sécurisé requis, le firmware UEFI et la prise en charge du TPM virtuel (vTPM) 2.0. L'hôte Hyper-V doit exécuter Windows Server 2016 ou Windows 10, et le système d'exploitation invité hébergé dans la machine virtuelle doit être Windows Server 2012 ou supérieur.

Les machines virtuelles blindées offrent les avantages suivants :

- **Les disques sont cryptés.**
- **Le processus de fonctionnement des machines virtuelles est renforcé afin de prévenir toute manipulation éventuelle. (VMWP)**
- **Verrouillage direct PowerShell et accès à la console.**

Les machines virtuelles blindées protègent les données et l'état de la machine virtuelle contre le vol et la manipulation des privilèges d'administrateur

6.4 Isolation et configuration du réseau

La création de la machine virtuelle devrait, dans la plupart des cas, reposer sur un adaptateur réseau virtuel non connecté. Plus tard, une fois que toutes les mesures de sécurité nécessaires auront été mises en oeuvre, il sera attaché à l'interrupteur approprié. Microsoft met en oeuvre, par défaut, un certain nombre de mesures de sécurité qui permettent un haut degré d'isolation, mais cela doit être complété par de bonnes pratiques, car ce moyen de communication constituera la majorité de la surface exposée par les machines virtuelles.

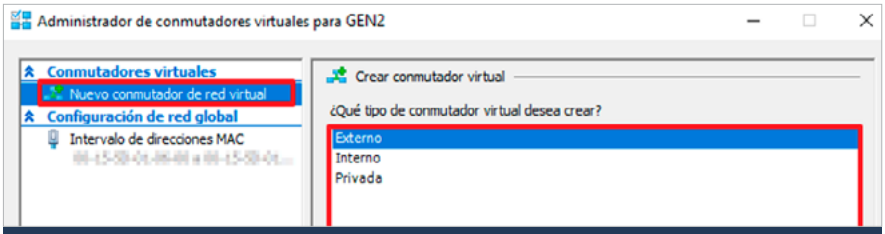
En ce qui concerne Hyper-V, cette technologie fonctionne avec une couche d'abstraction du réseau physique de l'*hôte* qui crée des commutateurs et des cartes réseau virtuels. C'est un choix de connecter ces cartes à ces *commutateurs* de façon permanente, temporaire ou pas du tout. Vous devez toujours opter pour la configuration minimale requise et donc, si aucune connectivité n'est requise, la machine virtuelle doit rester avec les paramètres de création par défaut. Les commutateurs de réseaux virtuels peuvent être externes, internes ou privés.

[Tableau 2] Description et exemples d'utilisation des commutateurs virtuels.

TYPE	DESCRIPTION	EXEMPLES D'UTILISATION
Externe	Crée un commutateur virtuel qui se lie à l'adaptateur de réseau physique afin que les machines virtuelles puissent avoir accès au réseau physique auquel il est connecté.	Les machines virtuelles ont besoin d'une connectivité Internet. Les machines virtuelles doivent être accessibles aux utilisateurs du réseau.
Interne	Il ne se connecte pas au réseau physique de l'*hôte*, mais crée un point de jonction qui peut être utilisé par toutes les machines virtuelles fonctionnant sur celui-ci, en plus de l'hôte lui-même.	Un réseau de machines virtuelles qui doivent interagir les unes avec les autres et où la machine *hôte* est utilisée comme client de test.
Privé	Il est identique à celui de l'interne, mais l'*hôte* n'est pas inclus comme membre de ce réseau.	Un réseau de machines virtuelles qui doivent interagir entre elles, mais pas avec d'autres machines.

Lorsqu'un commutateur est connecté au dispositif physique du réseau, le commutateur externe, il existe d'autres paramètres et variables qui doivent être pris en compte.

[Illustration 7] Écran de création d'un interrupteur externe.

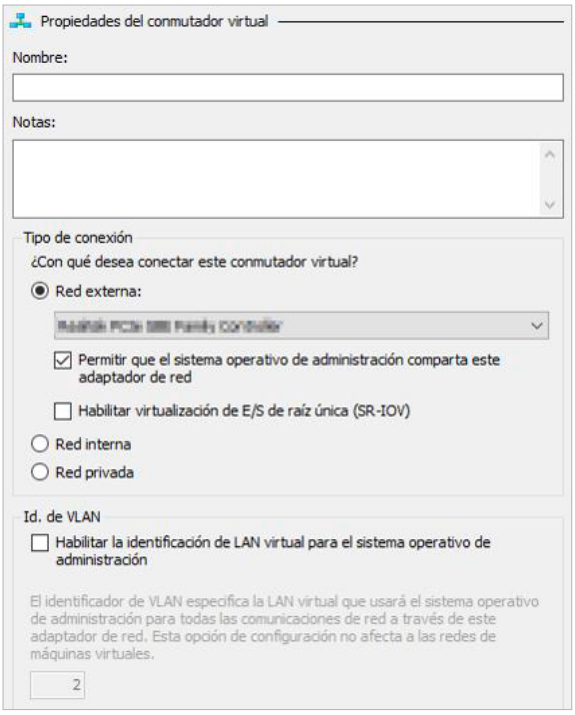


NOTE : Dans cet exemple, vous aurez une connectivité au réseau où l'adaptateur physique est hébergé.

La case à cocher par défaut, "Autoriser le système d'exploitation de gestion à partager cette carte réseau", confère des valeurs de partitionnement souple à cet élément hôte. Si vous ne la cochez pas, la valeur d'isolation du réseau sera élevée. **Mais l'adaptateur physique ne peut pas être utilisé sur d'autres commutateurs ou par l'hôte.**

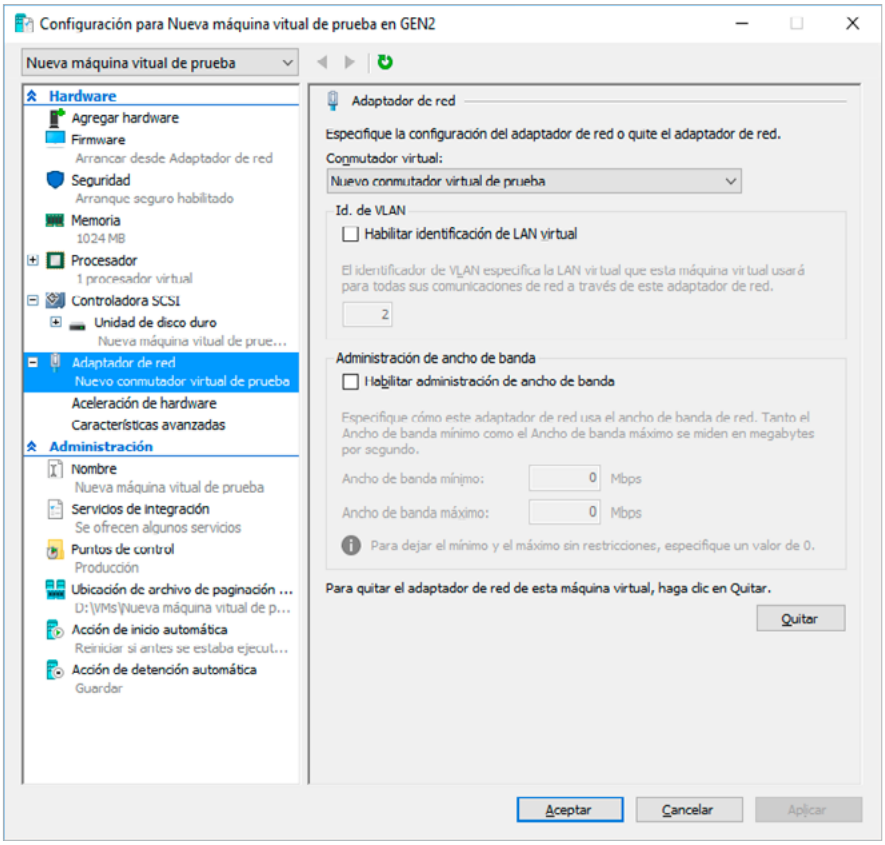
[Illustration 8] Propriétés d'un commutateur virtuel.

VLAN ID", s'il est activé, permettra à toutes les communications du système d'exploitation hôte d'être marquées par l'identifiant VLAN sélectionné dans la case ci-dessous (la valeur par défaut est (2). Cette option exige que le port physique du commutateur auquel le réseau physique de l'hôte est connecté autorise le trafic du VLAN choisi, soit parce que le port appartient à ce segment de réseau, soit parce que le port est une connexion de type trunk et que le VLAN est inclus dans la liste des réseaux autorisés. Il faut également s'assurer que les machines virtuelles utilisent ce commutateur et disposent d'une adresse IP valide dans le VLAN choisi.



Une fois que la machine virtuelle déconnectée a été créée et que les commutateurs de réseau virtuel souhaités ont été créés, il est temps de configurer les dispositifs de réseau virtuel comme requis. Pour ce faire, ouvrez la configuration de l'*invité* et sélectionnez "Adaptateur réseau".

[Illustration 9] Configuration d'une carte réseau d'une VM hébergée sur l'*hôte*.



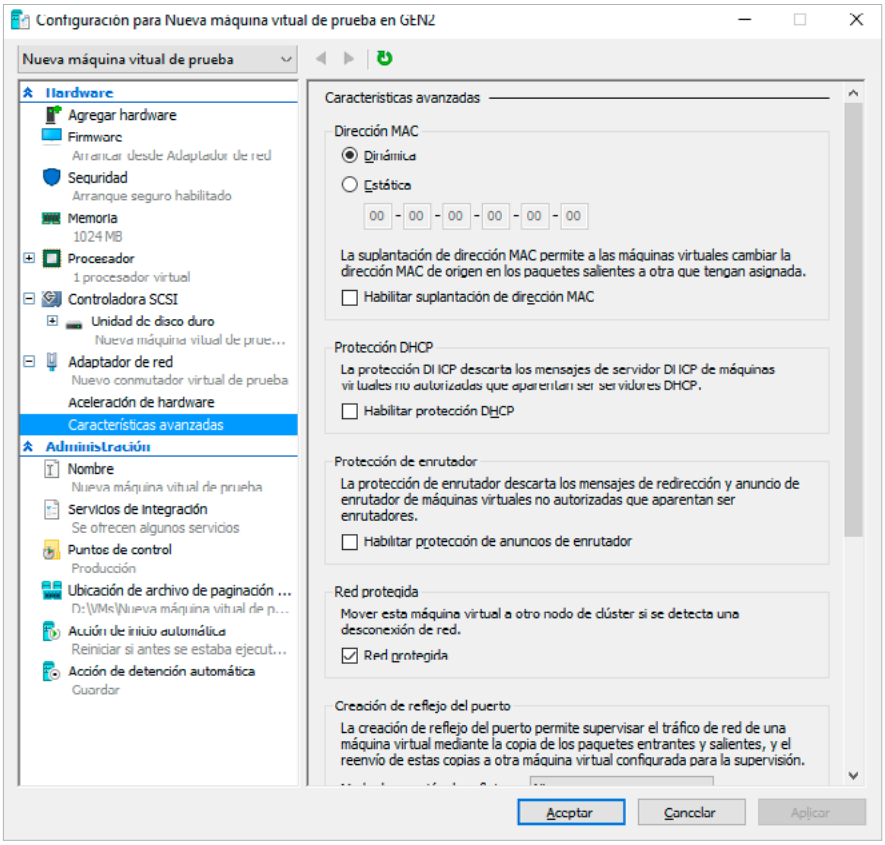
Au niveau de l'adaptateur réseau *invité*, l'option "VLAN ID" vous permet de sélectionner un identifiant de réseau local virtuel, mais uniquement pour ce seul périphérique, et non pour l'ensemble du commutateur. Il ne doit pas être sélectionné s'il est déjà configuré sur le *commutateur* virtuel en mode VLAN.

La "gestion de la bande passante" permet le "partitionnement doux" du réseau physique mentionné plus haut, ainsi que la réservation de la bande passante pour une carte réseau donnée. Dans le cas du minimum, la somme des partitions doit être inférieure à la valeur du dispositif physique auquel le commutateur virtuel est connecté. **Un montant réservé à l'*hôte* lui-même doit être déduit.** Par exemple, pour un réseau GigaEthernet, 100 Mbps seraient bloqués pour l'hôte.

L'option "Fonctions avancées" mène à une fenêtre où vous pouvez activer ou désactiver les variables réseau qui géreront les protections de cet élément.

L'option "Fonctions avancées" mène à une fenêtre où vous pouvez activer ou désactiver les variables réseau qui géreront les protections de cet élément

[Illustration 10] Fonctions avancées d'une carte réseau virtuelle.



Toutes les fonctionnalités de cette fenêtre sont nécessaires à un moment ou à un autre de la gestion, notamment pour les serveurs, car il n'existe généralement pas de valeurs idéales. Voici quelques conseils rapides qui peuvent être extrapolés à d'autres cas individuels.

[Tableau 3] Fonctions avancées de la carte réseau Hyper-V et exemples d'utilisation.

FONCTIONNALITÉ	DESCRIPTION	EXEMPLES D'UTILISATION
Adresse MAC	Permet l'attribution d'un MAC spécifique ou active le MAC Address Spoofing de la machine virtuelle.	Attribuer un MAC statique dans les tests des machines virtuelles qui sont sur la liste de contrôle d'accès aux périphériques réseau.
Protection DHCP	Protège contre les serveurs DHCP malveillants sur les machines virtualisées. Il est conseillé d'activer cette variable.	Cette option est désactivée pour un serveur virtualisé de test avec Active Directory et serveur DHCP, qui est également connecté à un réseau interne avec d'autres ordinateurs, dont certains sont des clients DHCP.
Protection du routeur	Protège contre les publicités frauduleuses. Il est conseillé d'activer cette variable.	Dans un environnement d'analyse forensique de machine virtuelle, il peut être activé pour observer s'il émet de tels messages.
Réseau protégé	Il s'agit d'une mesure de haute disponibilité.	Test de machines virtuelles dans des clusters à haute disponibilité.
Mise en miroir des ports	L'activation crée un port miroir où le trafic est doublé. L'activer peut augmenter la surface d'exposition.	Analyse du trafic pour l'audit de sécurité, sans altérer le réseau étudié.
Constitution d'une équipe NIC	La création de "Network Teams" est une mesure de haute disponibilité et de ressources accrues.	Test de haute disponibilité du réseau sur une machine virtuelle qui sera ensuite mise en production avec cette fonctionnalité.
Nomenclature des dispositifs	**L'activation de la propagation du nom pourrait entraîner une fuite d'informations,** généralement sans gravité, mais inutile. N'activez pas cette case sans un besoin spécifique.	Dans un environnement de test de machines Windows, sans données de sécurité, vous souhaitez faciliter la tâche de connexion des machines virtuelles dans un réseau interne (sur∑les commutateurs externes, elle ne doit en aucun cas être activée).

NOTE : vous trouverez de plus amples informations, ainsi que l'utilisation de PowerShell, pour ces fonctionnalités dans l'article "What's New in the Hyper-V Virtual Switch in Windows Server 2012" via le lien suivant :

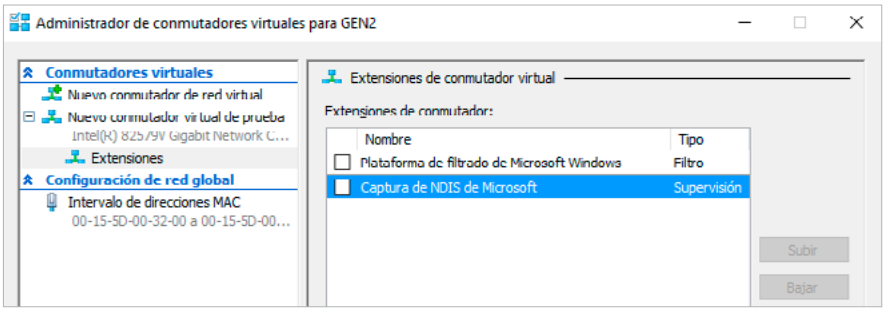
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj679878(v=ws.11)

6.5 Gestion des extensions de commutateurs

Les extensions de commutateur virtuel permettent d'inclure des logiciels tiers pour filtrer, capturer et transmettre le trafic réseau. La configuration sécurisée de chaque extension de commutateur dépend des paramètres des différents fournisseurs en général et de l'extension elle-même en particulier.

En ce qui concerne Hyper-V, il est fourni avec deux extensions installées, mais non activées. Il s'agit de la plate-forme de filtrage Microsoft Windows (WFP) et de la capture Microsoft NDIS.

[Illustration 11] Extensions par défaut d'un commutateur virtuel dans Hyper-V.



La première, WFP, devrait être activée si elle est requise par une extension tierce, avec la réserve qu'elle pourrait affecter certaines machines virtuelles. Veuillez vous référer à l'article de TechNet "Hyper-V : The WFP virtual switch extension should be enabled if it is required by third party extensions" disponible via le lien suivant pour plus d'informations.

https://social.technet.microsoft.com/wiki/contents/articles/13071.hyper-v-the-wfp-virtual-switch-extension-should-be-enabled-if-it-is-required-by-third-party-extensions.aspx

Cette architecture permet le filtrage et la modification des paquets du réseau, la surveillance, la connexion promiscuous et d'autres fonctions. L'extension de capture NDIS est une API qui permet d'installer des extensions sur le pilote de commutateur virtuel Hyper-V.

Les éditeurs de logiciels, tels que "5NINE SOFTWARE", disposent d'extensions qui permettent d'inclure un pare-feu virtuel, un antivirus, un système de détection des intrusions (IDS), une inspection des anomalies du réseau, une analyse du trafic réseau, un listing des connexions et des statistiques des machines virtuelles déployées sur un serveur Hyper-V.

L'extension de capture NDIS est une API qui permet d'installer des extensions sur le pilote de commutateur virtuel Hyper-V

6.6 Services d'intégration

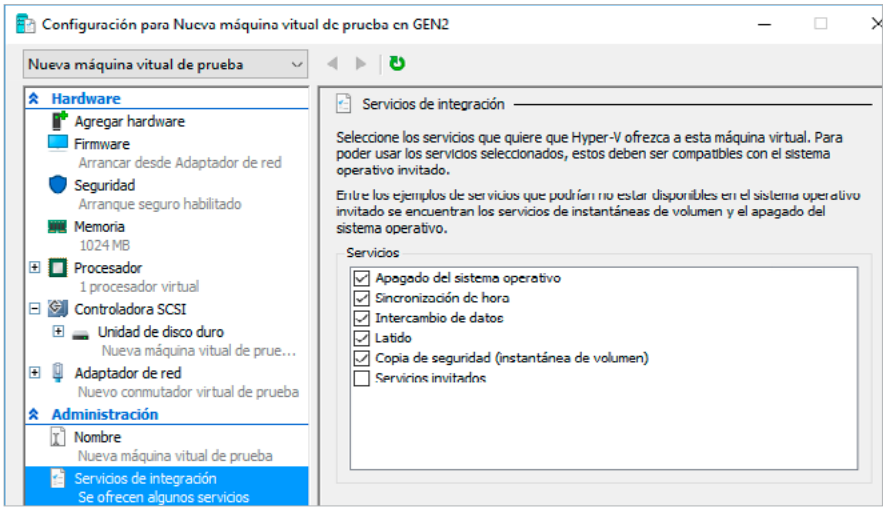
Les services d'intégration Hyper-V permettent la communication des machines virtuelles avec l'*hôte*. Leur installation présente de nombreux avantages pour l'amélioration des performances et le bon fonctionnement des *invités* (par exemple, la synchronisation temporelle), mais augmente la surface exposée aux attaques. Vous trouverez de plus amples informations dans l'article "Gestion des services d'intégrationHyper-V".

https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/manage/Manage-Hyper-V-integration-services

Sur les systèmes Windows, chacun des services d'intégration est installé en tant que service et peut être géré comme tel à partir de la console MMC

Ils fonctionnent en deux parties, donc pour qu'un service soit actif, il doit être activé aux deux extrémités, hôte et invité. Les invités avec les systèmes Windows Server 2008 R2 et Windows Vista SP2 et ultérieurs incorporent les services d'intégration par défaut.

Dans la configuration de chaque machine virtuelle Hyper-V, vous pouvez accéder aux services d'intégration. Par défaut, tous sont activés, sauf "Guest Services".



[Illustration 12] Services d'intégration.

Sur les systèmes Windows, chacun des services d'intégration est installé en tant que service et peut être géré comme tel à partir de la console MMC. Vous pouvez consulter les services via le lien suivant :

https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/reference/integration-services

NOM DU SERVICE	CONFIGURATION DU SERVEUR		SYSTÈME D'EXPLOITATION INVITÉ	
	CONFIGURATION PAR DÉFAUT DE LA MACHINE VIRTUELLE	VERSIONS QUI PRENNENT EN CHARGE L'EXÉCUTION SUR WINDOWS HYPER-V	NOM DU SERVICE WINDOWS	NOM DU PILOTE / DÉMON LINUX
Arrêter le système d'exploitation	Activé	Windows Server 2012 et versions ultérieures	Service d'arrêt de l'invité Hyper-V	hv_utils
Synchronisation du temps	Activé	Windows Server 2012 et versions ultérieures	Service de synchronisation du temps Hyper-V	hv_utils
Échange de données	Activé	Windows Server 2012 et versions ultérieures	Service d'échange de données Hyper-V	hv_utils et hv_kvp_daemon
Battement de coeur	Activé	Windows Server 2012 et versions ultérieures	Service Hyper-V Heartbeat	hv_utils
Sauvegarde (instantané de volume)	Activé	Windows Server 2012 et versions ultérieures	Demandeur d'instantanés de volume Hyper-V	hv_utils et hv_vss_daemon
Services aux clients	Non activé	Windows Server 2012 R2 et versions ultérieures	Interface des services du système invité Hyper-V	hv_utils et hv_fcopy_daemon

[Tableau 4] Liste des services d'intégration.

Le cas particulier du service d'intégration d'échange de données peut nécessiter l'installation d'un fichier ".cab", disponible dans le centre de téléchargement de Microsoft. Ce service permet l'échange d'informations pertinentes et utilise une clé d'enregistrement pour ces fonctions. Pour le téléchargement du service d'intégration de l'échange de données, veuillez visiter le lien Microsoft suivant :

https://support.microsoft.com/es-es/help/3071740/hyper-v-integration-components-update-for-windows-virtual-machines-that-are-running-on-a-windows-10-based-host.

L'activation du service d'intégration appelé "Guest Services" entraîne une communication entre l'*hôte* et l'*invité*, même s'il n'y a pas de réseau établi entre eux, et n'est donc pas recommandée dans les environnements sensibles.

6.7 Sécurité basée sur la virtualisation pour les machines virtuelles de génération

La fonctionnalité de sécurité basée sur la virtualisation est disponible dans Hyper-V 2016, offrant des fonctions telles que *Device Guard* et *Credential Guard*, qui assurent une protection accrue du système d'exploitation contre les attaques de codes malveillants. La sécurité basée sur la virtualisation est disponible pour les invités de génération 2 à partir de la version 8.

***Device Guard* est un groupe de fonctionnalités clés conçues pour renforcer un système informatique contre les codes malveillants.** Son objectif est d'empêcher l'exécution de code malveillant en veillant à ce que seul le bon code connu puisse être exécuté.

***Credential Guard* est une fonction spécifique, qui ne fait pas partie de *Device Guard*, et qui vise à isoler et à renforcer les systèmes des clés et des utilisateurs contre la compromission**, en aidant à minimiser l'impact et l'étendue d'une attaque "Pass the Hash" dans le cas où le code malveillant est déjà en cours d'exécution via un vecteur local ou réseau.

La première technologie qu'il convient de comprendre avant de se pencher sur ces deux fonctionnalités est le mode sécurisé virtuel (VSM). Le VSM est une fonction qui tire parti des extensions de virtualisation du CPU pour assurer une plus grande sécurité des données en mémoire.

De plus amples informations sur ces fonctionnalités sont disponibles sur le lien Technet suivant :

https://blogs.technet.microsoft.com/ash/2016/03/02/windows-10-device-guard-and-credential-guard-demystified/

Le VSM est une fonction qui tire parti des extensions de virtualisation du CPU pour assurer une plus grande sécurité des données en mémoire

6.8 Points de contrôle

Un point critique de tout environnement de virtualisation est la création et la gestion des *points de contrôle* ou de l'état des *invités*. Ils ne peuvent pas être considérés comme une sauvegarde de la machine ; il est préférable de considérer le *point de contrôle comme* un état cohérent d'une machine virtuelle à un moment précis.

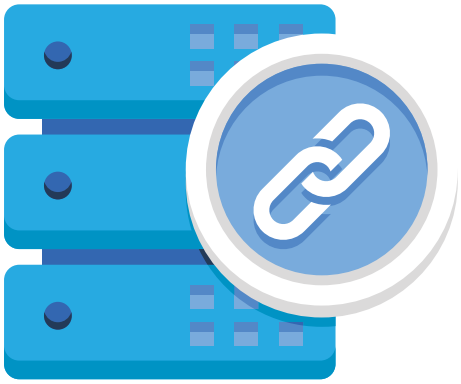
Un *point de contrôle* est un disque dur virtuel différentiel, qui a un nom spécial et une extension ". avhd [x]" et un fichier de configuration xml avec le nom GUID. En outre, il peut y avoir deux fichiers supplémentaires avec la mémoire de la machine virtuelle (VM) (.bin) et le statut du périphérique (.vsv) si la machine virtuelle était sous tension pendant la création du point de contrôle. Une fois le point de contrôle effectué, le disque de différenciation (. avhd [x]) devient un endroit où sont stockées les modifications temporaires apportées au disque original de la machine virtuelle, tandis que le disque original reste en mode lecture seule. Il n'est pas possible d'effectuer un *point de contrôle sur une* machine virtuelle qui utilise des disques virtuels pass-through (c'est-à-dire qui n'utilise pas de fichiers VHD-VHDX comme disques virtuels).

Pour cette raison, il est nécessaire de contrôler la génération de *points de contrôle* des machines invitées sur un *hôte en raison* de la dégradation qu'ils provoquent dans les systèmes, à la fois en raison de la création de nouveaux fichiers que l'hyperviseur doit gérer, mais aussi en raison de la consommation supplémentaire d'espace de stockage qu'ils génèrent.

Vous trouverez de plus amples informations sur le lien suivant de Microsoft :

https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/user-guide/checkpoints

Il n'est pas possible d'effectuer un *point de contrôle sur* une machine virtuelle qui utilise des disques virtuels pass-through



7. Meilleures pratiques VMware Workstation / Player

Cette section présente certaines des sections les plus pertinentes lorsqu'il s'agit d'établir de bonnes pratiques dans le processus de création et de gestion des machines virtuelles avec VMware Workstation.

L'environnement décrit dans ce document consiste en la création de postes de travail virtuels, c'est-à-dire la virtualisation sur des ordinateurs clients par le biais d'applications de bureau telles que Workstation Pro (qui fait l'objet d'une licence payante et permet la création et la gestion de machines virtuelles) et Workstation Player (logiciel gratuit qui ne permet que l'utilisation de machines virtuelles précédemment créées).

Parmi les produits proposés par VMware, il existe d'autres versions de serveurs de machines virtuelles plus professionnelles, comme ESX et ESXi.

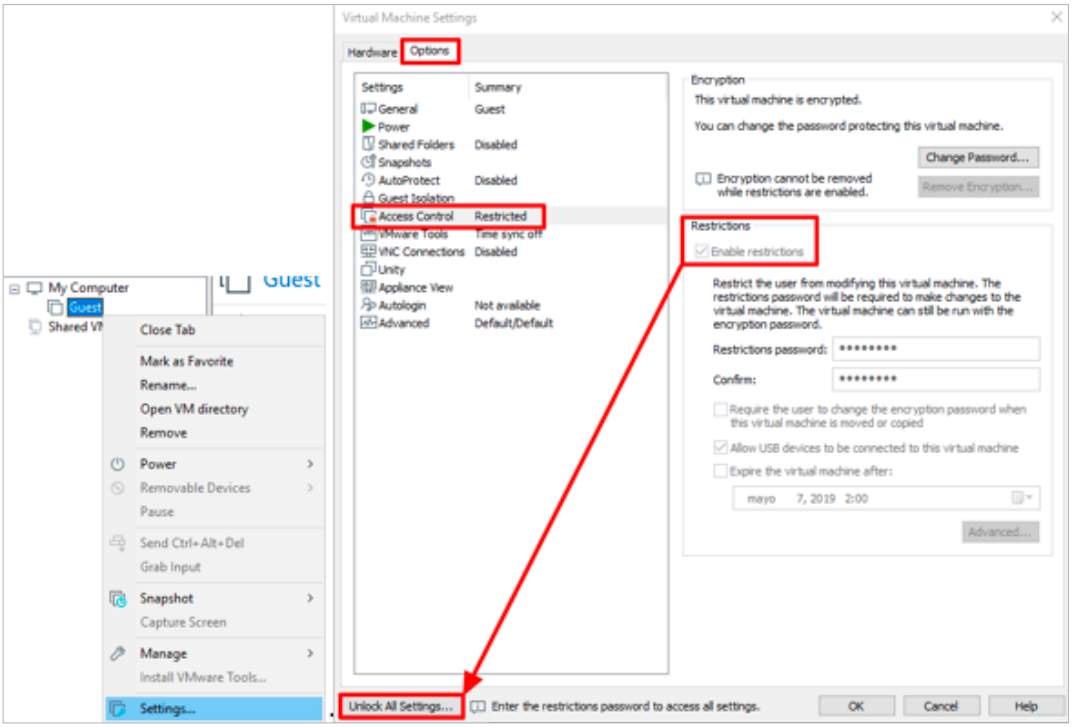
REMARQUE :
les exemples présentés ci-dessous sont tirés de VMware WorkStation Pro v.15, dont la licence est gratuite pour 30 jours

7.1 Le cryptage et la restriction des machines virtuelles

Dans un espace de travail comportant des machines physiques, que ce soit en phase de test ou dans des environnements de production, il est nécessaire de protéger les machines clientes afin d'empêcher les utilisateurs non autorisés de les allumer, de les déplacer ou de retirer des composants tels que la mémoire RAM, les cartes vidéo ou réseau, les disques durs, etc. Toutes ces actions peuvent entraîner des dysfonctionnements du système et, plus compromettant, le vol illégitime d'informations d'entreprise.

Dans les environnements virtuels, après avoir créé une machine virtuelle, la première tâche recommandée est de protéger l'accès à celle-ci, ainsi qu'à ses paramètres de configuration de base, afin d'éviter les dommages causés par une utilisation inappropriée. Ceci peut être fait au moyen des options de cryptage et de restriction, qui ne peuvent être configurées que lorsque la machine virtuelle est éteinte.

[Illustration 13] Options de cryptage et de restriction.



Le chiffrement permet de sécuriser l'accès à la machine virtuelle, y compris les composants qui lui sont affectés (mémoire RAM, disques externes, disques durs, etc.). Pour ce faire, il faut saisir un mot de passe qui sera demandé ultérieurement à chaque fois qu'il sera lancé dans la console de gestion, lorsqu'il sera exporté vers une autre console ou si l'on veut inverser le processus de cryptage. La durée du processus de cryptage dépend de la taille de la machine virtuelle. Une fois terminé, lorsque la console de gestion est redémarrée, la machine virtuelle aura une icône de cadenas fermé et une boîte de dialogue apparaîtra pour demander à l'utilisateur de saisir le mot de passe correspondant.

Cette restriction empêche les utilisateurs d'accéder aux paramètres de configuration de la machine virtuelle, à moins qu'ils ne saisissent un mot de passe spécifique. Si cette section n'est pas protégée, les utilisateurs pourraient effectuer des actions telles que permettre des connexions via VNC (un protocole de connexion à distance qui n'est pas sécurisé car il n'est pas crypté), partager des dossiers (avec le risque correspondant de perte d'informations) ou modifier le répertoire de travail où sont stockées les machines virtuelles.

Les options de cryptage et de restriction sont étroitement liées puisque si la première n'est pas activée, la seconde ne peut l'être, et si la seconde est activée, la première ne peut être désactivée.

Il est très important de stocker les mots de passe de cryptage et de restriction de manière pratique dans un registre sécurisé, car VMware ne dispose pas d'un système permettant de récupérer les clés perdues.

Cela signifie qu'en cas de perte des mots de passe, il ne sera pas possible de démarrer les machines virtuelles, de modifier leur configuration ou de passer outre le cryptage. De plus, il faut définir clairement quels utilisateurs auront accès à ces clés, car ils ont accès à l'exploitation des systèmes d'exploitation de l'entreprise, ce qui, dans certains cas, peut être critique.

Il est très important de stocker les mots de passe de cryptage et de restriction de manière pratique dans un registre sécurisé

7.2 Configuration des ressources

Dans le cadre du processus de création d'une machine virtuelle, il est recommandé de faire une planification préalable correcte des ressources matérielles qui vont être allouées en fonction des caractéristiques physiques disponibles.

Il est important d'avoir une vision globale de l'ensemble de l'infrastructure, c'est-à-dire qu'il faut tenir compte de toutes les machines virtuelles qui seront utilisées sur le même *hôte*, ainsi que des ressources dont l'hôte a besoin pour continuer à fonctionner correctement.

En règle générale, il est recommandé de minimiser le nombre de machines virtuelles avec lesquelles vous travaillez sur le même *hôte* afin d'éviter une utilisation inutile des ressources. De même, une fois l'environnement de travail bien défini, seules les machines virtuelles absolument indispensables doivent être démarrées. Garder au démarrage les machines virtuelles avec lesquelles vous ne travaillez pas vraiment est un gaspillage de ressources qui nuit au reste des machines virtuelles et à l'*hôte* lui-même, ce qui peut entraîner un ralentissement de l'exécution des processus, voire l'effondrement de l'ensemble du système.

En ce qui concerne l'espace disque, une allocation dynamique est recommandée, en particulier lorsque l'on travaille avec plusieurs machines virtuelles, afin de minimiser la quantité d'espace disque occupé et de ne l'augmenter qu'en cas de besoin.

Pour les applications qui sont très sensibles aux performances et à l'écriture, il est recommandé de prévoir une allocation d'espace permanente, adaptée aux besoins du logiciel en cours d'exécution. Il existe également une option permettant de diviser l'archive du disque en plusieurs fichiers de 2 Go. Cette option n'est recommandée que si le contenu de la machine virtuelle doit être stocké sur un support de faible capacité ou s'il doit être transmis sur un réseau dans un endroit où la bande passante est limitée.

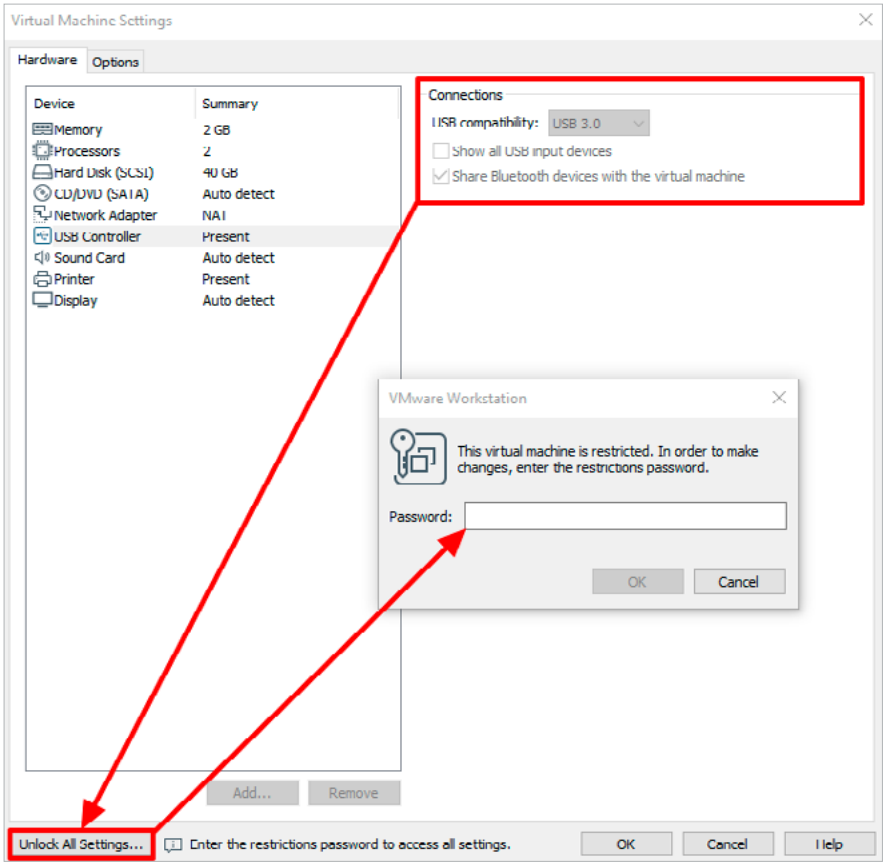
Il est recommandé de minimiser le nombre de machines virtuelles avec lesquelles vous travaillez sur le même *hôte* afin d'éviter une utilisation inutile des ressources.

Dans la mesure du possible, il faut utiliser un outil de somme de contrôle (CheckSum) pour vérifier l'intégrité des fichiers et, bien sûr, chiffrer le disque virtuel.

En revanche, **il n'est pas conseillé de laisser ouverte la possibilité de connecter des supports externes tels que des DVD ou des USB.** À cette fin, il est possible de restreindre les options de configuration, comme indiqué dans la section précédente. Si vous permettez à un utilisateur d'utiliser un fichier "iso" comme DVD de démarrage dans un système d'exploitation Linux, vous lui donnez la possibilité de chrooter, ce qui pourrait lui donner accès à la machine virtuelle et la contrôler.

De même, autoriser l'utilisation de clés USB peut conduire au vol non autorisé d'informations ou à l'installation de codes malveillants, de manière volontaire ou accidentelle. La meilleure option est donc de désactiver l'utilisation de supports externes par le biais de restrictions et de ne les activer qu'en cas de besoin, puis de les désactiver à nouveau après utilisation.

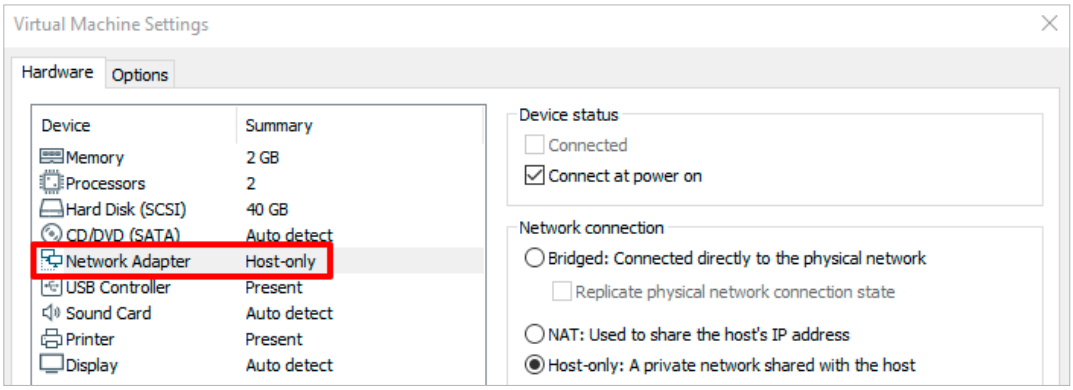
Autoriser l'utilisation de clés USB peut conduire au vol non autorisé d'informations ou à l'installation de codes malveillants



[Illustration 14] Ressources matérielles protégées par mot de passe.

7.3 Isolation et configuration du réseau

Les machines virtuelles chargées sur les versions Workstation Pro et Player doivent être isolées du reste du réseau et fonctionner, dans la mesure du possible, uniquement en mode "Host-Only" afin de ne pas affecter ou être affectées par l'infrastructure de production.



[Illustration 15] Réseau en mode "hôte seulement".

Cependant, il existe des situations où les machines virtuelles doivent être présentes sur le réseau, soit pour interagir avec d'autres machines, soit pour télécharger des paquets d'installation à partir d'Internet. Si cette interaction n'est pas absolument nécessaire ou constante, il est conseillé de configurer le dispositif de réseau principal pour qu'il agisse en mode "Hôte uniquement" et d'ajouter un second dispositif de réseau avec une présence sur le réseau externe qui ne sera activé qu'en cas de besoin, il est donc recommandé de le garder désactivé lorsqu'il n'est pas utilisé.

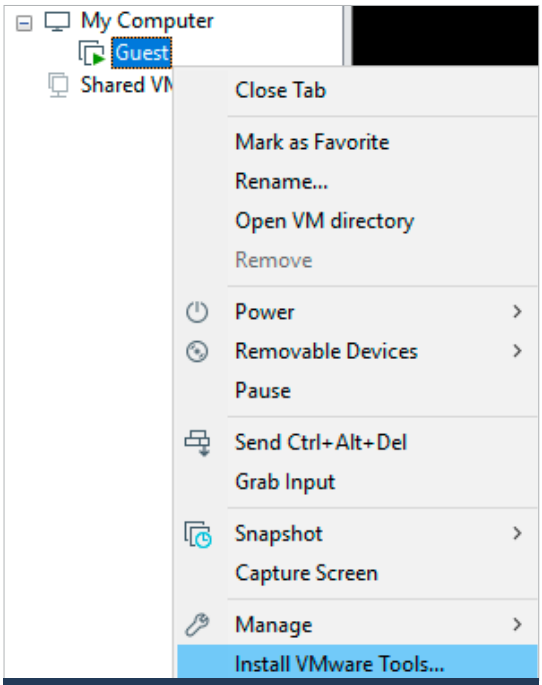
En ce qui concerne la connexion externe, **le mode "NAT" est préférable car il permet un meilleur contrôle du trafic réseau,** les machines virtuelles fonctionnant sur un réseau interne créé par l'*hôte*. La configuration en mode "Bridge" est plus facile à mettre en oeuvre, mais outre un contrôle moindre, elle peut surcharger le contrôleur de réseau si un grand nombre de machines virtuelles utilisent simultanément la même interface physique.

7.4 Outils VMware

L'installation des outils VMware n'est pas indispensable au fonctionnement des machines virtuelles. Cependant, il est indispensable si vous souhaitez opter pour certaines fonctions d'interaction entre l'*hôte* et la machine, comme le transfert de fichiers et de textes.

Avant d'installer les outils susmentionnés, il faut tenir compte du système d'exploitation de la machine virtuelle à utiliser. Presque tous les systèmes Windows ne posent aucun problème lorsqu'il s'agit d'effectuer cette action, mais toutes les distributions Linux ne la prennent pas en charge. Avec les dernières versions de Debian et Ubuntu, il n'y a généralement aucune difficulté.

Lors de l'installation des outils VMware, il faut garder à l'esprit qu'ils devront être mis à jour périodiquement pour optimiser leur fonctionnement.



[Illustration 16] Installation des outils VMware.

REMARQUE :

Ce document utilise la version actuelle de VMware WorkStation Pro v.15, avec une licence gratuite de 30 jours. Vous pouvez consulter le guide de compatibilité VMware au lien suivant : https://kb.vmware.com/s/article/2129859

7.5 Protection des machines virtuelles sur les *hôtes*

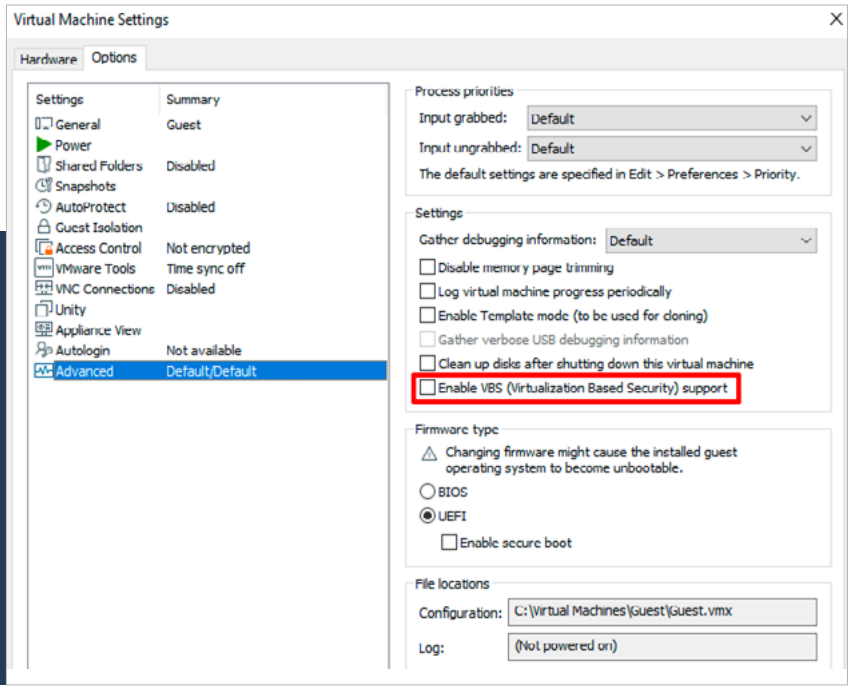
Pour renforcer la sécurité dans les environnements virtuels, la sécurité basée sur la virtualisation (VBS) peut être activée pour les machines virtuelles exécutant les derniers systèmes d'exploitation Microsoft Windows 10 et Microsoft Windows Server 2016.

La sécurité basée sur la virtualisation (VBS) utilise la technologie de virtualisation Hyper-V de Microsoft pour isoler les principaux services du système d'exploitation Windows dans un environnement virtuel distinct. Cette isolation fournit un niveau de protection supplémentaire en rendant impossible l'altération des services clés de votre environnement.

L'activation de VBS dans une machine virtuelle active automatiquement le matériel virtuel dont Windows a besoin pour la fonction VBS. Lorsque vous activez VBS, une variante Hyper-V démarre dans la machine virtuelle et Windows commence à s'exécuter à l'intérieur de la partition racine Hyper-V.

[Illustration 17] Option permettant d'activer le VBS.

Dans VMware Workstation, VBS peut être activé lors de la création d'une machine virtuelle. Alternativement, VBS peut être activé ou désactivé pour une machine virtuelle existante.



NOTE :

Vous trouverez de plus amples informations sur le lien suivant : https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.hostclient.doc/GUID-E2A6D2F4-BA66-48EC-98D5-35D8E2C3B192.html

7.6 Transfert de fichiers et de textes

Une fois les outils VMware installés, le presse-papiers peut être utilisé conjointement entre l'*hôte* et les machines virtuelles, et certains types de fichiers peuvent être transférés facilement. Pour ces derniers, il existe plusieurs méthodes, il faudra donc en choisir une ou plusieurs en fonction des besoins de chaque système.

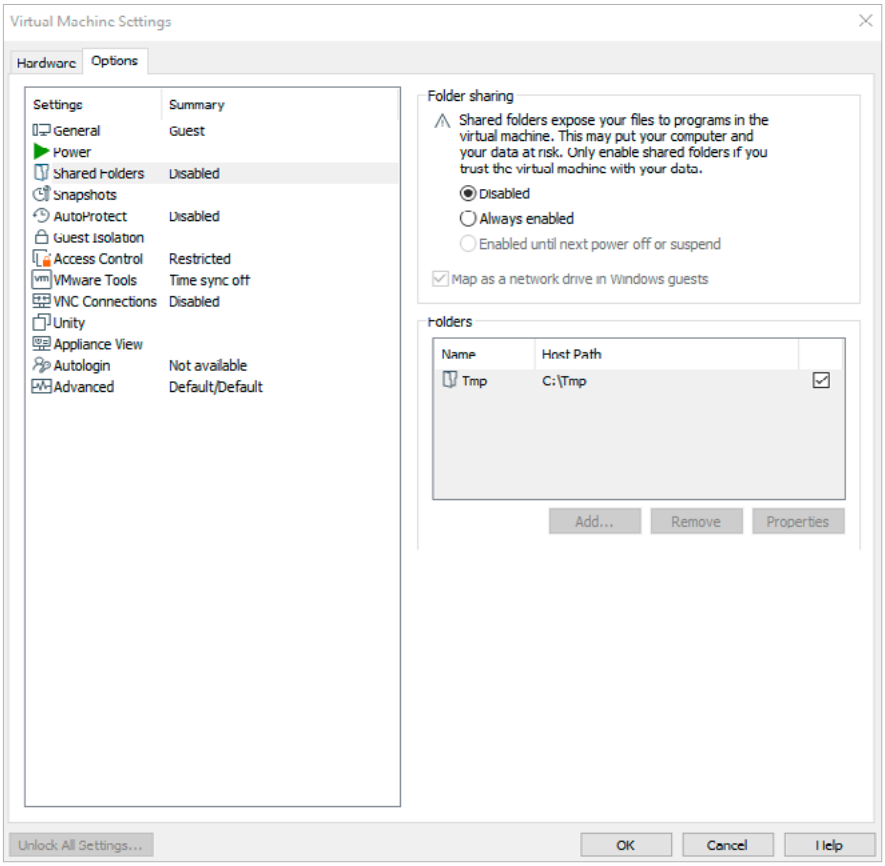
Le premier à mentionner est le "glisser-déposer", c'est-à-dire faire glisser des fichiers de l'ordinateur hôte vers la machine virtuelle ou vice versa. Il est facile à utiliser, mais peut poser des problèmes en raison des limitations de taille et de format de certains fichiers.

Vous pouvez également choisir d'utiliser la fonction "copier-coller". Outre une limitation du format et de la taille des fichiers, comme dans le cas précédent, elle présente l'inconvénient de ne pas fonctionner entre machines virtuelles.

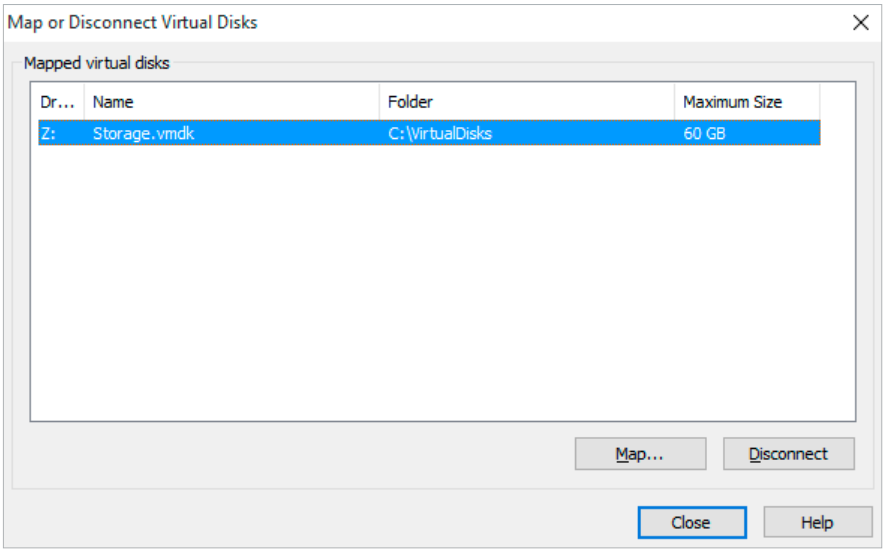
Troisièmement, il y a la possibilité de partager des dossiers. Cette solution est plus complexe à configurer que les précédentes, mais permet une désactivation facile lorsqu'elle n'est pas utilisée. Un inconvénient majeur est la possibilité que les fichiers soient corrompus s'ils sont utilisés par différentes machines simultanément.

Enfin, l'*hôte a la possibilité* de mapper un disque dur virtuel sur lequel les fichiers seront stockés. Ceci a l'avantage de permettre l'utilisation d'un point de rendez-vous entre plusieurs machines virtuelles et l'*hôte* sans quitter l'infrastructure de virtualisation. Si cette méthode est choisie, il est recommandé de crypter le disque dur virtuel.

[Illustration 18] Partage d'un dossier hôte avec l'un des *invités*.



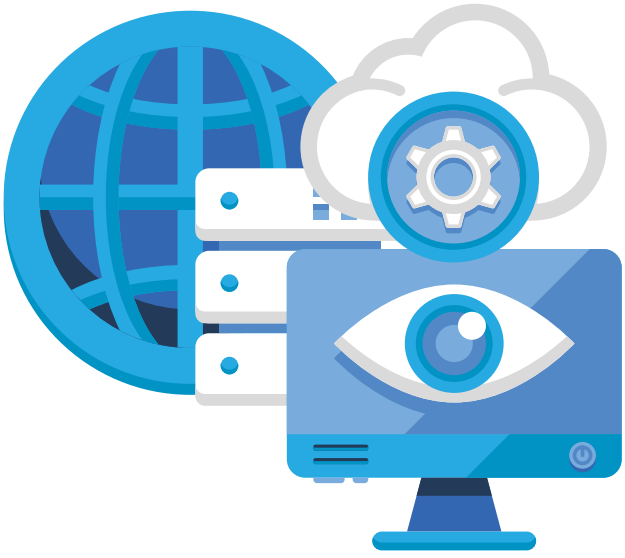
[Illustration 19] Fichier de disque dur virtuel mappé sur l'*hôte*.



Dans la mesure du possible, les travaux doivent être effectués localement. Mais s'il est nécessaire de partager des fichiers avec des utilisateurs ou des ordinateurs externes, il est fortement recommandé d'utiliser un système qui offre une méthode de validation robuste, comme ceux basés sur les services d'annuaire (par exemple Windows Active Directory).

7.7 Des instantanés de machines virtuelles

Comme dans tous les autres systèmes de virtualisation, il est possible de faire des points de contrôle ou d'état des machines virtuelles. Cette option ne doit pas être utilisée comme système de sauvegarde pour les machines virtuelles, car VMware les traite comme un registre où il stocke les modifications apportées au disque dur virtuel primaire, créant un nouveau disque de remplacement dès sa création.



REMARQUE :

vous trouverez de plus amples informations sur le lien suivant du fournisseur :

Best practices for using snapshots in the vSphere environment

8. Meilleures pratiques en matière de VirtualBox

Comme pour les autres hyperviseurs, les actions de protection et, en général, les meilleures pratiques doivent être orientées d'abord vers l'hôte, puis vers chacune des machines virtuelles hébergées.

Certaines des considérations générales à prendre en compte sont énumérées ci-dessous :

a. **Maintenez le logiciel de virtualisation à jour.** Cela peut être fait en activant l'option dans les préférences de VirtualBox ou en effectuant une vérification manuelle sous "Fichier" puis "Vérifier les mises à jour...".

b. **Maintenez à jour les ajouts d'invités sur toutes les machines virtuelles.** De même, les Extension Packs doivent être mis à jour.

c. **VirtualBox ne doit pas être exécuté avec des privilèges d'administrateur,** sauf pour les actions requises qui ne peuvent pas être effectuées sans privilèges et, en général, les autorisations les plus restrictives possibles doivent être maintenues.

d. **Limitez les connexions réseau afin que l'*hôte* et les *invités* disposent de la connectivité minimale requise.** De même, cette connexion doit être sécurisée par un système de pare-feu sur chacun des ordinateurs installés.

e. **Auditez régulièrement les journaux de sécurité pour détecter les comportements anormaux et créer une base de référence pour une comparaison si nécessaire.**

Les actions de protection et, en général, les meilleures pratiques doivent être orientées d'abord vers l'hôte, puis vers chacune des machines virtuelles hébergées

f. **Utilisez uniquement le site officiel d'Oracle comme source des installables.**

g. **Dans les environnements sandbox-antimalware, évitez d'installer les Guest Additions,** car elles permettent la communication avec l'*hôte* et deviennent un vecteur possible d'infection.

h. **Ne créez pas d'instantanés qui ne sont pas nécessaires et supprimez-les en toute sécurité si nécessaire.**

i. **Soyez extrêmement prudent lorsque vous utilisez des périphériques de stockage USB, des CD ou des DVD, car ils permettent l'entrée directe de logiciels dans les machines virtuelles.** Les premiers, en particulier, sont un vecteur d'entrée commun pour les codes malveillants.

j. **Évitez le gestionnaire d'hyperviseur en mode HTML car il n'utilise pas de connexion sécurisée.** Il est préférable d'utiliser l'application client-serveur "Oracle VM VirtualBox Administrator" (application de bureau), qui est plus sûre.

NOTE :

Site officiel de VirtualBox pour le téléchargement de leurs produits :

- https://www.oracle.com/virtualization/virtualbox/

- https://www.virtualbox.org/

8.1 Le cryptage des machines virtuelles

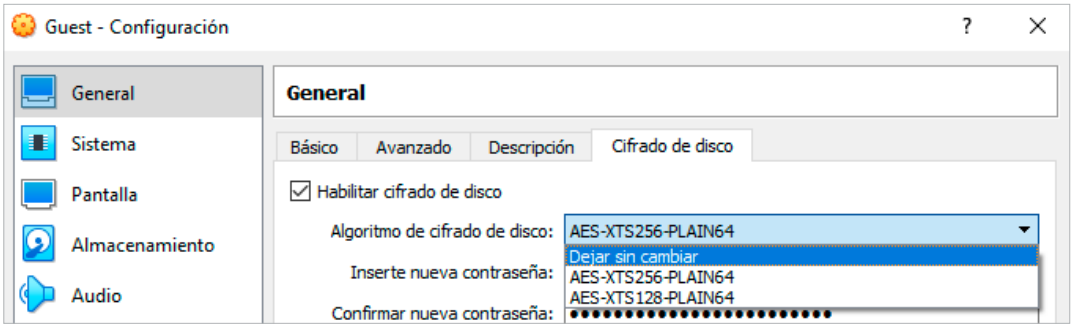
En ce qui concerne le cryptage des machines virtuelles, il est transparent pour l'invité et peut être appliqué au disque dur et à tous ses formats disponibles (VDI, VHD, VMDK).

VirtualBox, à partir de la version 5, incluait déjà le cryptage des disques durs des machines virtuelles en tant que fonction de sécurité, cependant, il est nécessaire d'installer un paquet d'extension pour pouvoir utiliser la fonction dans la configuration générale des machines virtuelles.

Pendant la création de la machine avec l'assistant graphique, le cryptage ne peut pas être configuré, donc si la machine est critique, il est conseillé de ne pas ajouter le disque tant que le cryptage avec le mot de passe n'a pas été activé. Il convient également de noter que le cryptage ajoute une charge de travail à l'hôte et que les machines créées avec cette méthode dans VirtualBox ne peuvent pas être transportées vers d'autres systèmes de virtualisation sans être décryptées au préalable.

REMARQUE :

vous pouvez choisir l'algorithme le plus sûr en fonction de l'importance et/ou de la criticité du système



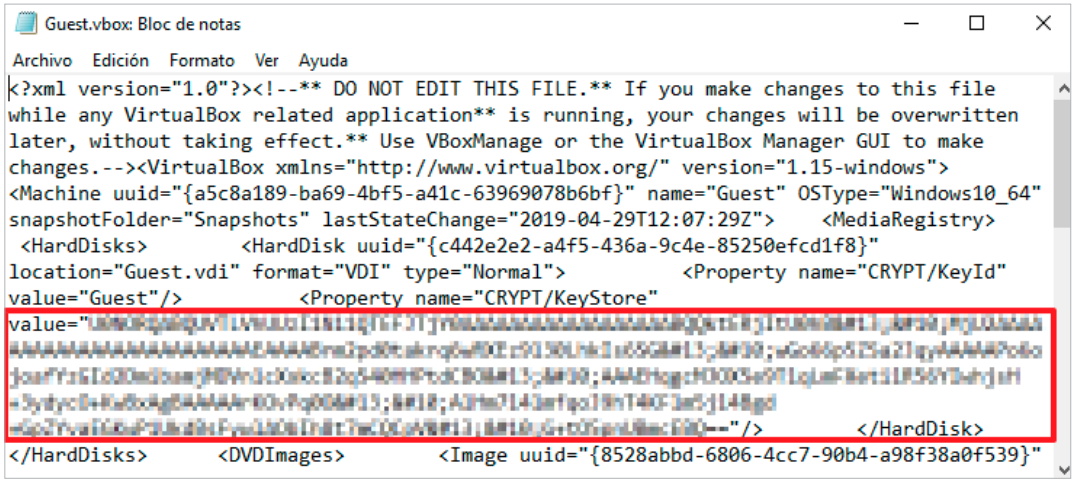
[Illustration 20] Activation du chiffrement dans la machine virtuelle.

Il est essentiel de souligner que la perte du mot de passe implique la perte irrémédiable des disques durs. Le mot de passe est stocké dans le fichier de configuration de la machine virtuelle, il est donc conseillé d'en avoir une copie de sauvegarde.

Le fichier de définition de la machine, qui comprend le codage du mot de passe en clair, doit être protégé par des autorisations NTFS, et doit être fait avant la création du mot de passe pour éviter les fuites dans la fenêtre de temps d'exposition.

La protection par cryptage Windows EFS n'est pas une alternative, car le cryptage est inversé au premier démarrage de l'*invité* dans VirtualBox.

Il est essentiel de souligner que la perte du mot de passe implique la perte irrémédiable des disques durs



[Illustration 21] Fichier de configuration de la machine virtuelle.

En revanche, **l'attribution de permissions au dossier dans lequel est stockée la définition des machines virtuelles et des disques durs doit être correctement planifiée afin d'éviter tout accès non autorisé** (par accident ou à la suite d'une attaque). Au moins les permissions suivantes doivent être configurées :

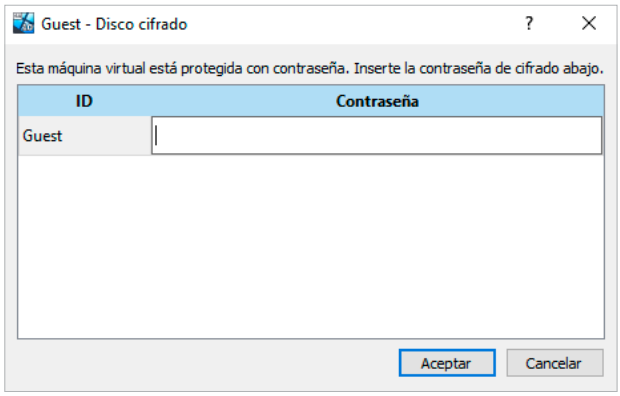
[Tableau 5] Permissions minimales pour les répertoires et les disques durs des machines virtuelles.

COMPTE	PERMIS	POSTULEZ À
Administrateurs	Contrôle total	Ce dossier, ses sous-dossiers et ses fichiers
Système	Contrôle total	Ce dossier, ses sous-dossiers et ses fichiers
Propriétaire du créateur	Contrôle total	Sous-dossiers et fichiers uniquement

NOTE : L'inclusion d'autres utilisateurs ou groupes doit être évaluée au cas par cas

Avec les autorisations du tableau ci-dessus, chaque utilisateur peut générer ses propres machines virtuelles, mais ne peut pas accéder aux machines invitées créées par d'autres. Tout administrateur d'*hôte* peut accéder à toutes les machines.

Lors du démarrage d'une machine virtuelle dont le disque est protégé par un mot de passe, le mot de passe sera requis à chaque démarrage de la machine virtuelle. Il existe certaines limites à l'utilisation du cryptage de disque, il est donc conseillé de consulter le manuel avant d'utiliser cette fonctionnalité. Par exemple, il est incompatible avec les *instantanés*, ou le mot de passe est chargé en mémoire et transféré à plat pendant l'utilisation de la machine virtuelle.



[Illustration 22] Fenêtre de demande de clé de chiffrement.

Le chiffrement de VirtualBox est compatible avec le chiffrement des disques physiques via *BitLocker*. Pour les environnements critiques, il convient donc d'utiliser les deux, et de mettre en place des mesures supplémentaires de protection par mot de passe.

8.2 Isolation et configuration du réseau

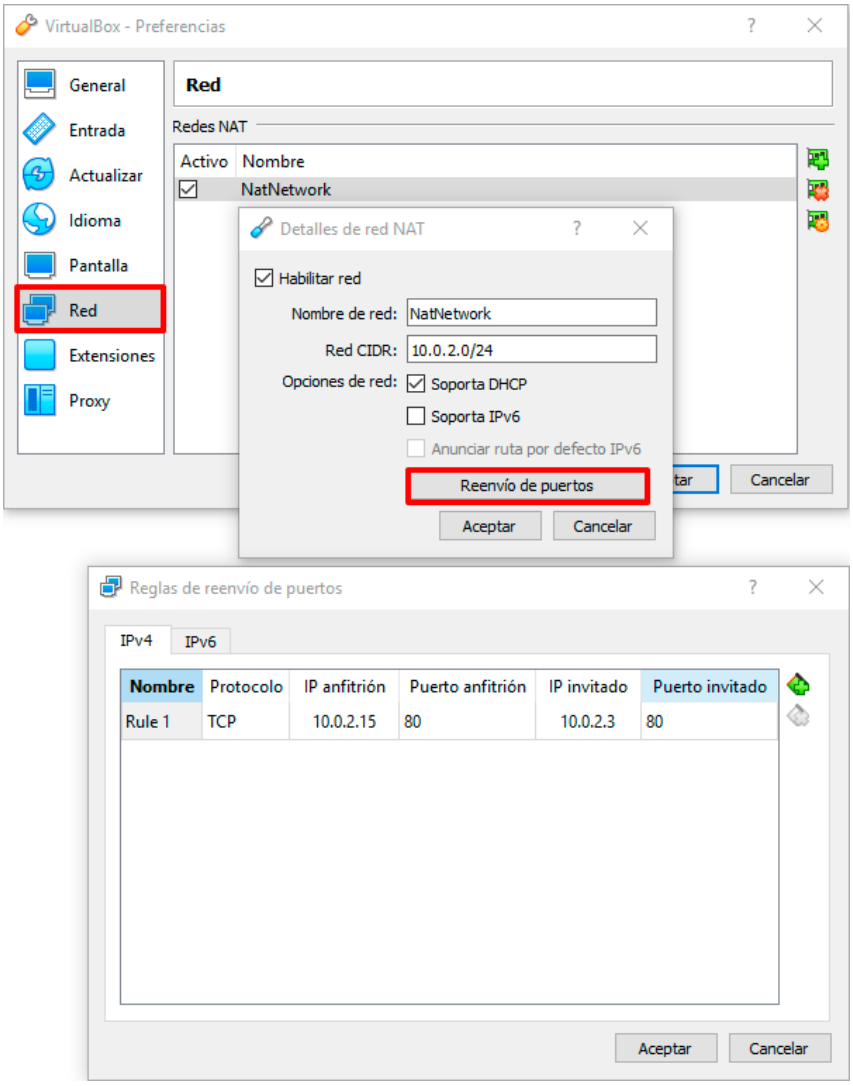
En ce qui concerne la connectivité dans VirtualBox, les périphériques de réseau virtuel invités peuvent être configurés dans l'un des états suivants :

- **Non connecté.**
- **NAT.**
- **Réseau NAT.**
- **Adaptateur de pont.**
- **Réseau interne.**
- **Adaptateur hôte seulement.**
- **Pilote générique.**
- **Avancé.**

La valeur par défaut attribuée à une nouvelle création est "NAT", de sorte que l'hyperviseur se comporte comme un routeur (dispositif de la couche 3 du modèle OSI). Cela donne à l'invité des capacités de connexion au réseau physique de l'hôte, mais cache les adresses IP et MAC aux ordinateurs externes.

Le pare-feu de l'*hôte* peut assurer la protection des machines virtuelles hébergées. Cela empêche la publication des services des serveurs hébergés en tant qu'*invité*, à l'exception de celui pour lequel cette option a été sélectionnée. Cela peut être considéré comme un avantage en matière de sécurité, mais aussi comme un obstacle si une connectivité multiple des invités à partir du réseau est nécessaire.

Lorsque la publication d'un serveur est nécessaire, VirtualBox peut être utilisé comme un routeur avec toutes les fonctionnalités de routeur possibles. Pour ce faire, un "réseau NAT" doit être créé, auquel les adaptateurs d'invités virtuels peuvent ensuite être connectés.



[Illustration 23] Création d'un "réseau NAT" avec la publication du port 80.

L'option "Bridge adapter" permet de connecter directement les invités via la connexion physique, qui se comporte comme un commutateur (couche 2 du modèle OSI). Cette configuration est pratique pour obtenir une connectivité externe, mais elle augmente considérablement la surface exposée, de sorte que chaque machine virtuelle doit être protégée par ses propres moyens (produit pour éviter les codes malveillants, pare-feu, IDS, etc.)

"Réseau interne" permet aux machines virtuelles de se connecter entre elles aux machines hébergées qui ont cette option sélectionnée et qui correspondent également au même identifiant de réseau. Il est donc possible de créer différents réseaux internes. Si vous avez besoin de tester des machines comme si elles étaient en réseau, c'est une option valable, mais vous devez créer votre propre réseau interne et ne connecter que les machines essentielles.

Si la visibilité du réseau nécessaire est avec l'*hôte*, il faut choisir l'option **"Adaptateur hôte seulement"**, qui reliera les ordinateurs hôte et invité.

Le terme **"conducteur générique"** n'est pas couramment utilisé. Permet de présenter un pilote réseau inclus dans VirtualBox ou dans un "Extension Pack".

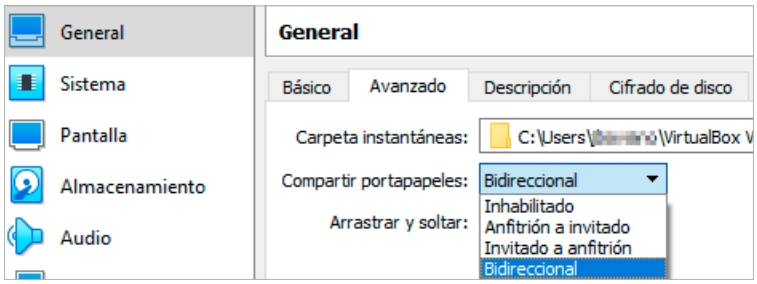
Lorsque l'option **"Avancé"** est activée, chacune des options permet la gestion des adresses MAC, l'activation du mode promiscuous, le type d'adaptateur et le transfert de port (chacun selon le cas).

Comme avec tout autre hyperviseur, **il est recommandé d'utiliser la configuration "Non connecté" chaque fois que possible et de passer d'une connectivité faible à une connectivité plus élevée.** Par exemple, passez de "Adapter only-host", au réseau interne, puis au NAT, puis au réseau NAT, etc.

Dans VirtualBox, il est possible de créer jusqu'à quatre cartes réseau virtuelles par *invité* et les mêmes précautions doivent être prises pour chacune d'entre elles. Il est important de tenir compte du fait que les cartes qui ne seront pas utilisées ne doivent pas être définies.

8.3 Partage du presse-papiers

L'outil de presse-papiers partagé présente une fonctionnalité généralement intéressante pour un travail rapide et pratique, mais il pourrait être un point d'échange de code nuisible. Il fonctionne indépendamment du type de réseau utilisé et peut fonctionner dans les deux sens ou dans l'un d'eux, entre l'*invité* et l'*hôte* ou vice versa. Cet outil nécessite l'installation de VirtualBox Guest Additions sur l'invité.



[Illustration 24] Configuration du presse-papiers.

L'outil de presse-papiers partagé présente une fonctionnalité généralement intéressante pour un travail rapide et pratique, mais il pourrait être un point d'échange de code nuisible

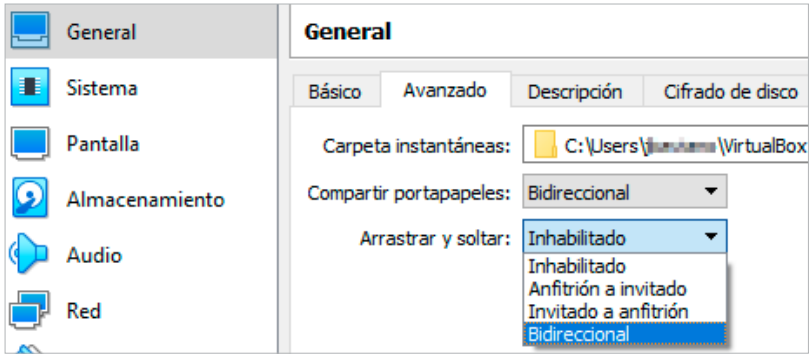
En règle générale, cette fonctionnalité doit rester désactivée, car un attaquant potentiel pourrait, par exemple, accéder à des informations sensibles stockées dans le presse-papiers de l'*hôte* en ayant préalablement accédé à un invité insuffisamment protégé. Si elle est requise pour des raisons de force majeure, elle ne doit être activée que pour la période indispensable.

REMARQUE :
Dans la configuration de la machine virtuelle dans VirtualBox, vous pouvez sélectionner le mode de fonctionnement du presse-papiers (par défaut, il est désactivé)

8.4 Drag and drop

Cette fonctionnalité, connue sous le nom de "drag & drop", vous permet de glisser et de déposer un objet (fichier, dossier ou texte brut) dans les deux sens, entre l'*invité* et l'*hôte* ou *vice versa*. Cet outil nécessite l'installation de VirtualBox Guest Additions sur l'invité.

Le choix des paramètres est le même que pour le presse-papiers partagé, ainsi que l'option par défaut, "Désactivé", et la recommandation de le conserver dans cet état. Si son utilisation est requise, elle doit être activée aussi longtemps que strictement nécessaire.



[Illustration 25] Configuration par glisser-déposer.

REMARQUE :

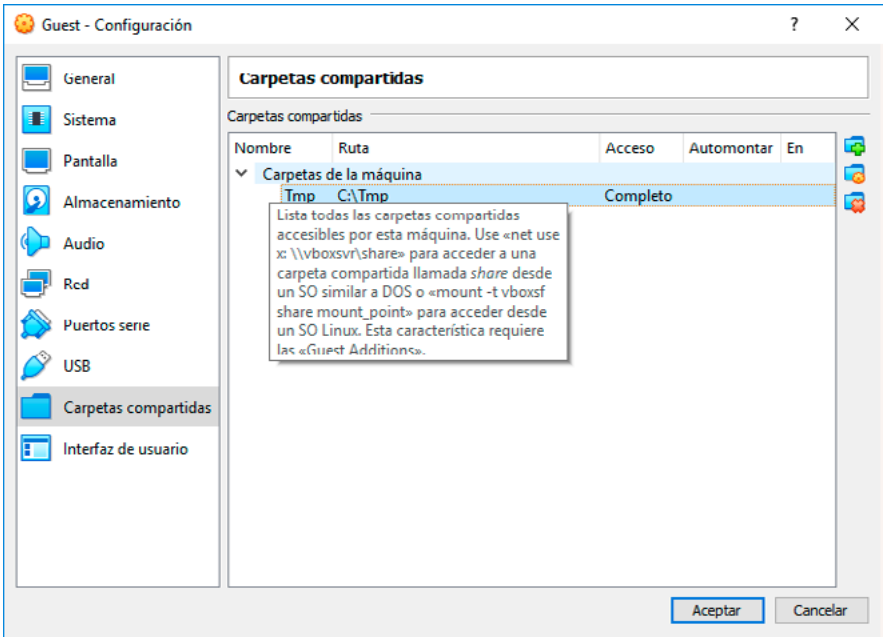
Dans la configuration de la machine virtuelle dans VirtualBox, vous pouvez sélectionner le mode de fonctionnement "glisser-déposer" (par défaut, il est désactivé).

8.5 Dossiers partagés

Dans ce cas, le terme "dossier partagé" ne fait pas référence à la ressource réseau créée par le système d'exploitation, mais à la fonctionnalité de VirtualBox qui est rendue disponible avec l'installation des "Guest Additions" sur l'invité. Cela permet de mettre à la disposition de l'invité un répertoire hébergé sur l'hôte, auquel il est possible d'accéder via les chemins de la convention de dénomination universelle (UNC) utilisés pour accéder aux ressources du réseau.

Pour une description de l'UNC, voir le lien suivant :

https://docs.microsoft.com/eses/dotnet/standard/io/file-path-formats#unc-paths



[Illustration 26] Configuration des dossiers partagés.

Par défaut, VirtualBox n'inclut pas de dossiers partagés. La décision de les créer doit être réfléchie, en adoptant les mesures de sécurité maximales pour protéger les informations traitées.

Une fois qu'un dossier partagé est défini, il se comporte comme une ressource réseau. Il est publié avec le nom donné lors de la création et avec la nomenclature "vboxsvr" pour le serveur. Si vous choisissez d'exécuter l'instruction "automount" sous Windows, le dossier sera monté immédiatement et sous Linux il sera monté de la même manière dans "/media" avec le préfixe "sf_".

Son utilisation est déconseillée car elle augmente la zone d'exposition (par exemple, la plupart des *ransomwares* chiffrent le lecteur de lettres Windows). Pour en savoir plus sur la protection contre les *ransomwares*, veuillez consulter le rapport sur les menaces *CCN-CERT IA-11/18 : Mesures de sécurité contre les ransomwares* et le guide de bonnes pratiques *CCN-CERT BP/04 Ransomware* associé sur le site Web du CCN-CERT.

Dans les dernières versions de VirtualBox, il est possible de définir le point de montage, ce qui permet de s'assurer que le point de montage est différent du point de montage standard et d'appliquer des mesures de sécurité supplémentaires sur le point de montage..

Comme indiqué dans les sections précédentes de ce guide, **le partage d'informations,** par quelque moyen que ce soit, **est toujours considéré comme une augmentation de la surface exposée aux attaques potentielles,** mais il est parfois nécessaire.

Par conséquent, des mesures appropriées doivent être prises, **car un attaquant accédant à l'invité aurait accès aux ressources partagées.** Entre autres actions, vous pouvez définir une limitation du temps de partage (lorsque la machine virtuelle est éteinte, la ressource partagée disparaît), minimiser les informations publiées, combiner les permissions disponibles dans VirtualBox avec les permissions NTFS de l'hôte, en les rendant aussi restrictives que possible, et, dans les environnements critiques, activer l'audit des fichiers. En outre, bien que cela n'empêche pas la fuite d'informations, il est possible de définir l'autorisation en lecture seule (la valeur par défaut est lecture-écriture).

Dans les dernières versions de VirtualBox, il est possible de définir le point de montage, ce qui permet de s'assurer que le point de montage est différent du point de montage standard

8.6 Instantanés dans VirtualBox

Les machines virtuelles dans VirtualBox sont composées d'une série de fichiers dans lesquels sont stockées des informations sur les disques durs, les caractéristiques et l'état actuel de la machine.

Chaque disque dur virtuel correspond à un fichier portant l'extension ".vdi", ".vhd" ou ".vdmk" (selon le type de disque sélectionné lors de la création de la machine virtuelle). Les paramètres de configuration sont stockés dans un fichier XML portant le nom de la machine en question. Dans les versions de VirtualBox postérieures à 4.0, ce fichier porte l'extension ".vbox", ce qui vous permet de démarrer la machine en double-cliquant dessus ou via un raccourci. Si, au lieu d'arrêter la machine, on a décidé de sauvegarder son état, il y aura également un fichier ".sav", qui sera supprimé dès que la machine sera à nouveau active.

Les instantanés sont un moyen de sauvegarder l'état de la machine virtuelle à un moment donné, à partir duquel toute modification apportée à celle-ci sera stockée dans un nouveau fichier ".vdi" pour chaque disque dur existant, en conservant les originaux intacts. Les instantanés successifs répéteront ce processus, ce qui peut augmenter considérablement l'espace occupé par la machine sur le disque *hôte*. Il est donc nécessaire de contrôler leur création et de gérer à la fois le nombre d'instantanés et leur maintenance dans le temps.

Les instantanés sont un moyen de sauvegarder l'état de la machine virtuelle à un moment donné

9. Machine de navigation sûre

Afin de compléter l'objectif de ce guide, une machine virtuelle configurée de manière sécurisée a été mise en place, orientée vers la navigation sur Internet. De cette manière, l'indépendance et l'isolation entre la machine virtuelle et l'ordinateur hôte sont garanties.

Le système d'exploitation utilisé pour la machine virtuelle est CentOS 7, dont la licence est gratuite et le guide de configuration sécurisée appliqué est "CCN-STIC 619 Secure Configuration of CentOS 7 (Standalone Client)".

Les données requises pour télécharger la machine virtuelle de navigation sécurisée sont énumérées cidessous :

Lien :
https://loreto.ccn-cert.cni.es/index.php/s/FpniMgp5Hx8Ml66

Clé de téléchargement : virtual

SHA256
49C16F00E00C91EEE30D634A1BFB4035E69C2ED4017D0DF8B5BFD7B635E61892

SHA1
209766E9771E375322F6A4EE3742A46C2DED5D0C

La machine virtuelle de navigation sécurisée est conçue pour être utilisée avec des produits logiciels de virtualisation (hyperviseurs) dont la licence est gratuite, par exemple :

Oracle VirtualBox: www.virtualbox.org/wiki/Downloads

VMware Workstation Player:
www.vmware.com/products/workstation-player.html

10. Décalogue de recommandations

Ce qui suit est un décalogue des meilleures pratiques génériques pour tous les types d'hyperviseurs.

Décalogue de sécurité pour les machines virtuelles

1. **Maintenir le système à jour :** l'installation des dernières mises à jour de sécurité sur le système d'exploitation et la disponibilité de la dernière version du logiciel de virtualisation réduisent considérablement l'exposition aux vecteurs d'attaque traités par les fournisseurs dans les correctifs de mise à jour.
2. **Séparation du réseau physique :** si possible, disposez d'au moins une carte réseau dédiée à l'infrastructure de virtualisation afin de séparer le flux réseau des machines virtuelles et de la machine physique qui les contient. En cas d'attaque sur le réseau de la machine physique, l'attaquant ne verra pas le flux réseau des machines virtuelles, ce qui permet de les sécuriser grâce à cette séparation des adaptateurs.
3. **Séparation des rôles et des autorisations :** il est conseillé de créer un groupe de sécurité spécifique pour l'utilisation des machines virtuelles, dont les utilisateurs membres seront limités à l'utilisation du programme de virtualisation sans possibilité d'effectuer des actions nécessitant une élévation de privilèges non liés à l'utilisation des machines virtuelles. De la même manière, il est recommandé de créer un répertoire pour héberger les fichiers de la machine virtuelle, où les permissions seront appliquées ultérieurement, au moyen d'ACL.
4. **Planifier le système virtualisé :** faire un aperçu préliminaire de ce que sera l'infrastructure de virtualisation permet de la mettre en oeuvre. Cette planification doit prendre en compte le dimensionnement de la création des machines virtuelles en fonction des besoins réels et des ressources matérielles disponibles sur l'hôte, en accordant une attention particulière au type de disques à sélectionner en fonction des services fournis par chaque machine virtuelle.
5. **Gestion des ressources :** les ressources de l'hyperviseur ne sont pas illimitées. Pour libérer ces ressources, il est conseillé de ne garder actives que les machines

virtuelles qui sont absolument nécessaires. De plus, la mise en place d'une politique de création de "snapshots/checkpoints" des machines virtuelles renforce également cette gestion, car ils impliquent une dégradation des hôtes. Cette création doit être contrôlée, tant en termes de nombre total créé que de temps pour les maintenir sur les hyperviseurs.

6. **Protection de l'information :** pour sécuriser les données critiques hébergées sur des supports virtualisés, il est conseillé de chiffrer les fichiers des machines virtuelles, les snapshots et les disques durs virtuels utilisés pour le stockage de la plate-forme de virtualisation. Il faut également crypter les supports de stockage externes contenant les fichiers de virtualisation de sauvegarde et les protéger de manière appropriée. De même, cryptez et conservez les carnets de mots de passe sous bonne garde pour éviter toute exfiltration éventuelle.

7. **Mise en oeuvre d'un pare-feu :** sécurisez avec une solution de pare-feu, physique ou logique, pour empêcher les codes malveillants et les tentatives d'attaque contre tous les systèmes d'exploitation invités.

8. **Mettre en place une politique de sauvegarde :** pour éviter de perdre les données ou la fonctionnalité des machines virtuelles en cas d'urgence, il est recommandé d'établir une politique de sauvegarde qui contient une copie complète de ces machines virtuelles. Ces sauvegardes doivent être effectuées de temps en temps ou à des moments critiques afin de pouvoir récupérer des informations ou même la fonctionnalité de la machine virtuelle. Il faut tenir compte du fait que les sauvegardes ont une taille importante et que, pour cette raison, il est conseillé de conserver peu de sauvegardes complètes et d'utiliser des copies incrémentielles.

9. **Documenter la plate-forme de virtualisation :** la documentation du système permet d'identifier rapidement les machines en désuétude et permet de libérer des ressources et d'obtenir une meilleure gestion du système. Il est conseillé de mettre à jour cette documentation à chaque modification pertinente apportée au système.

10. **Installez les agents de l'hyperviseur :** pensez à installer ces logiciels complémentaires tels que "Guest Additions" ou "Tools", car leur mise en oeuvre améliore les performances des machines virtuelles et ajoute des fonctionnalités telles que le presse-papiers partagé. Si tel est le cas, il est recommandé de les maintenir à jour, ainsi que le logiciel de virtualisation.

11. Glossaire

Cette section contient une description des termes les plus couramment utilisés dans ce document afin de permettre leur identification et leur compréhension au cours du document.

TERME	DESCRIPTION
Virtualisation	Il s'agit de l'abstraction des ressources d'un serveur physique, de sorte qu'une couche est créée entre le matériel de la machine physique (hôte ou hyperviseur) et le système d'exploitation de la machine virtuelle (*invité*).
Invité	Logiciel qui simule un ordinateur et peut exécuter des programmes comme s'il s'agissait d'un véritable ordinateur physique.
Machine virtuelle (VM)	Également appelé "l'*invité*".
Hyperviseur, *hôte*	Il s'agit de la plate-forme physique qui permet l'application de diverses techniques de contrôle de la virtualisation pour utiliser, en même temps, différents systèmes d'exploitation sur le même ordinateur.
Snapshot, *instantané* ou *point de contrôle*	Il représente l'état d'une machine virtuelle au moment où il a été pris. Il s'agit essentiellement d'un instantané de la machine virtuelle à un moment donné. Ceci ne doit pas être considéré comme une sauvegarde de la machine virtuelle.
Interrupteur	Il s'agit d'un dispositif permettant d'interconnecter des réseaux entre d'autres dispositifs ou équipements.
Réseau local virtuel (VLAN)	Il s'agit d'une méthode permettant de créer des réseaux qui sont logiquement indépendants, même s'ils font partie du même réseau physique.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


cn-cert
centro criptológico nacional
CCN
centro criptológico nacional