Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 26 septembre 2013

N° DAT-NT-011/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 19

Note technique

Problématiques de sécurité associées à la virtualisation des systèmes d'information

Public visé:

Développeur	✓
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Problématiques de sécurité associées à la virtualisation des systèmes d'information** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
LAM	BAS	SDE	26 septembre 2013

Évolutions du document :

Version	Date	Nature des modifications
1.0	29 mai 2012	Version initiale
1.1	26 septembre 2013	Corrections mineures de la note 1343/ANSSI du 29 mai 2012 et mise au format « Note technique »

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Préambule

Les technologies dites de «virtualisation» ont connu un essor important ces dernières années, lié notamment au développement de nouveaux usages comme l'informatique en nuage (cloud computing). Virtualiser un ensemble de serveurs est devenu aujourd'hui relativement aisé, et de nombreuses entreprises ont choisi de «virtualiser» leurs serveurs pour faire des économies de place, d'énergie et de budget. Mais les risques associés à l'utilisation de ces nouvelles technologies sont-ils systématiquement pris en compte ? Les conséquences de la virtualisation sont-elles correctement comprises et acceptées ?

L'objet de ce document est de présenter ces risques et les principaux points à considérer pour s'en prémunir. Il reste volontairement à un niveau technique intermédiaire afin d'être accessible au plus grand nombre, y compris à des lecteurs ne disposant pas de connaissances poussées en architecture des ordinateurs ou des réseaux. Il n'aborde pas le cas des systèmes traitant des informations classifiées de défense.

Le lecteur pressé pourra se rapporter au chapitre 6 qui présente une liste de points de contrôle permettant d'apprécier le niveau de sécurité d'un système d'information virtualisé.

2 Introduction

Virtualiser, c'est en essence, et en simplifiant à l'extrême, rendre indépendant du matériel le socle logiciel d'une machine. Virtualiser permet de faire s'exécuter sur une même machine plusieurs systèmes jusqu'alors installés sur des machines physiques distinctes, ou de migrer en quelques instants et de manière transparente un système d'une machine à une autre. Virtualiser nécessite de mettre en œuvre une solution de virtualisation qui assure la gestion des différents systèmes virtualisés et leur exécution.

De fait, de plus en plus de responsables informatiques se tournent vers les solutions de virtualisation, en raison des atouts supposés de ces technologies, par exemple :

- un meilleur taux d'utilisation des ressources informatiques, qui peut apporter en outre, dans certains cas, une économie d'énergie [1] ;
- une meilleure disponibilité des systèmes, dans la mesure où les systèmes deviennent facilement « clonables » ou « réplicables » en cas de panne matérielle. Certaines solutions permettent de déplacer automatiquement des systèmes d'une machine à une autre en cas d'incident ou de perte de performances. La facilité de clonage des systèmes est également particulièrement appréciée pour créer des environnements de test représentatifs de la réalité ;
- une meilleure répartition de charge, puisque la solution de virtualisation sait généralement répartir la charge entre les différentes machines ;
- de potentiels gains financiers ou d'encombrement.

Cependant, comme nous le verrons tout au long de ce document, la virtualisation introduit aussi de nouveaux risques, aussi bien techniques qu'organisationnels, qui viennent s'ajouter aux risques des systèmes d'information classiques.

Ces risques intrinsèques viennent contrebalancer les avantages mis en avant par les éditeurs de solutions, et force est de constater que les mesures de sécurité indispensables pour les couvrir viennent souvent obérer une partie des économies potentielles envisagées initialement.

La migration d'un système d'information vers des solutions de virtualisation, potentiellement irréversible, ne doit donc pas être envisagée uniquement dans une perspective de gain financier.

1. Démarche dite de « green computing » (réduction de l'empreinte écologique des systèmes d'information).

Toute organisation qui souhaite héberger certains services et données au sein d'un système utilisant ces technologies doit donc faire ce choix avec discernement et en toute connaissance des risques engendrés sur le plan de la sécurité.

3 La virtualisation : cadre d'emploi et concepts généraux

La virtualisation, de quoi s'agit-il ?

« **Virtualiser** » un objet informatique, ou le rendre virtuel, signifie le faire apparaître sous son seul aspect fonctionnel, indépendamment de la structure physique et logique sous-jacente [2]. Dans cette note, on ne traitera pas de systèmes tels que les clusters d'ordinateurs [3] ou certaines solutions de stockage de données [4] qui pourraient répondre à cette définition. Le périmètre couvert par ce document peut se résumer à deux cas :

- la virtualisation de la couche matérielle destinée à permettre l'exécution du système (en particulier d'un système d'exploitation) sans qu'il ait à se soucier de la réalité physique sur laquelle il s'appuie. Dans le cas présent, il s'agit bien de « matériel virtualisé », c'est-à-dire de matériel rendu virtuel pour le système d'exploitation qui l'emploie, et non pas d'un « système d'exploitation virtuel » comme on peut souvent le lire ;
- la virtualisation d'un système d'exploitation au profit de certaines applications pour que ces dernières puissent fonctionner sur ce dernier alors que cela n'était pas prévu initialement ou pour renforcer l'isolation entre applications.

Pour ces 2 cas, il existe une « **couche d'abstraction** » qui permet à l'application ou au système d'exploitation de fonctionner dans son environnement virtuel (voir figure 1).

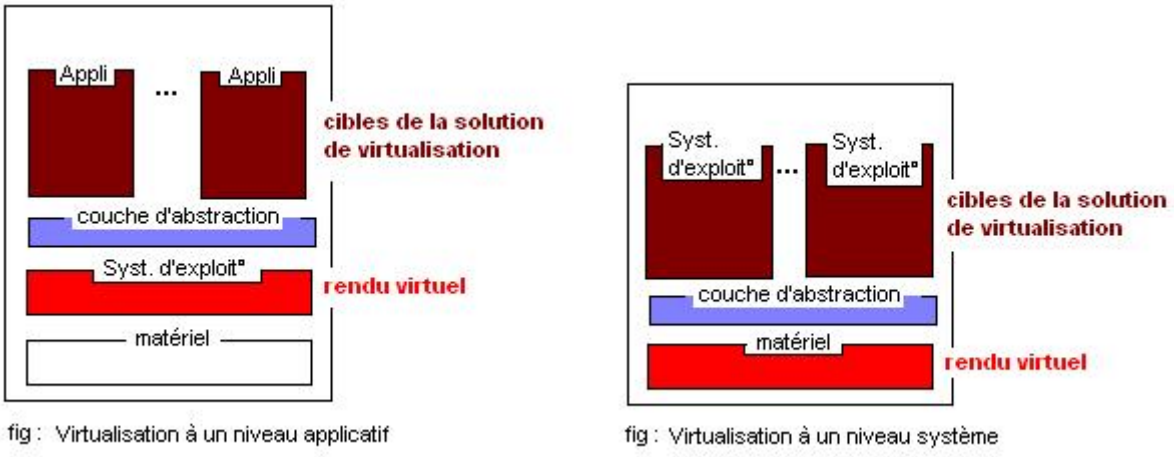

FIGURE 1 – Virtualisation à un niveau applicatif et virtualisation à un niveau système

2. Définition inspirée du « Petit Robert de la Langue française », nouvelle édition (version 2) – 2001.
3. En informatique, un cluster d'ordinateur est un ensemble d'ordinateurs qui peuvent héberger des processus lancés depuis un autre afin de bénéficier de ressources plus importantes.
4. Les solutions de stockage de données sur le réseau (NAS : Network Attached Storage) sont parfois appelées «filers» virtuels.

Niveaux de virtualisation et cibles de la virtualisation

Comme illustré précédemment, on retiendra donc dans la suite de ce document que la virtualisation ne s'applique qu'à deux niveaux :

- le niveau **applicatif**, dès lors que la solution de virtualisation cible une application et lui présente une couche d'abstraction correspondant à son environnement d'exécution. Une machine virtuelle Java (JVM) met par exemple en œuvre une virtualisation au niveau applicatif. Des applications Java développées à un haut niveau s'y exécutent et font abstraction de tout détail de plus bas niveau comme la nature du système d'exploitation ou du matériel sur lequel l'exécution a réellement lieu ;
- le niveau **système**, si la solution de virtualisation vise un système d'exploitation et lui présente une couche d'abstraction correspondant à un environnement matériel compatible. On trouve ainsi des solutions de virtualisation qui permettent de faire tourner simultanément plusieurs systèmes d'exploitation sur une même machine.

Remarque : Le terme « **cible** » qui sera utilisé tout au long de cette note décrit le composant s'exécutant directement sur la couche d'abstraction, c'est à dire une ou plusieurs applications dans le cas de la virtualisation au niveau applicatif, un ou plusieurs systèmes d'exploitation dans le cas de la virtualisation au niveau système.

Les différentes techniques de virtualisation

Les solutions de virtualisation ne reposent pas toutes sur les mêmes techniques. Les principales techniques utilisées sont décrites ci-après.

L'architecture des solutions de virtualisation **au niveau applicatif** repose généralement sur des techniques d'**émulation** et de **cloisonnement**.

L'**émulation** consiste à imiter le comportement d'une entité en présentant aux couches supérieures une interface logicielle caractéristique du fonctionnement de cette entité, indépendamment de l'architecture matérielle sous-jacente. Cette architecture est intéressante quand la cible doit s'exécuter sur de nombreux environnements différents, la couche d'abstraction réalisant le travail d'adaptation nécessaire au profit des applications qui deviennent ainsi portables.

Les solutions de virtualisation telles que *Citrix Application Stream (Citrix)*, *Symantec Workspace Virtualization (Symantec)*, *App-V (Microsoft)* ou *Softgrid (Microsoft)* sont des exemples de virtualisation applicative utilisant cette technique. Les solutions de virtualisation s'appuyant sur des moteurs d'exécution, telles que *Java Virtual Machine* (plusieurs implémentations), *.NET Framework (Microsoft)*, entrent également dans cette catégorie.

Le **cloisonnement** est quant à lui mis en place dans un but d'isolation ou de confinement. Les technologies *Linux Vserver*, *BSD jails* (« *chroot* »), *OpenVZ* ou *Zone Solaris* mettent en œuvre des zones isolées (cloisonnées) gérées par le système d'exploitation.

L'architecture des solutions de **virtualisation au niveau système** se décline pour sa part en trois catégories :

- la **paravirtualisation**, qui est gérée à la fois par la couche d'abstraction et par les cibles qui sont modifiées pour pouvoir s'exécuter sur la couche d'abstraction.
  Les solutions telles que *Xen* (GNU GPL), *VMware ESX/ESXi* et *VSphere (VMware)*, *Hyper-V (Microsoft)* reposent sur cette architecture [5]. C'est aussi le cas de la solution de virtualisation *PolyXene* développée pour la direction générale de l'armement par *Bertin Technologies*, évaluée selon les Critères Communs au niveau EAL5.

5. Cela peut se limiter à une adaptation des pilotes à des fins d'optimisation.

L'avantage principal du mode paravirtualisé est une meilleure performance que la virtualisation complète (voir ci-dessous). L'inconvénient majeur est que les systèmes d'exploitation ne sont pas utilisables sans modifications spécifiques ;

– la **virtualisation complète ou totale**, qui part du principe qu'aucune modification de la cible n'est autorisée pour lui permettre de fonctionner dans un environnement virtualisé. La technique de « traduction d'exécutable à la volée » (*binary translation*) est généralement utilisée. Elle consiste à adapter le code binaire lors de son exécution, séquence par séquence, pour remplacer certaines instructions par du code réalisé par la couche d'abstraction. Alternativement, les événements à traduire peuvent être interceptés dynamiquement au moment de leur exécution par une gestion d'exceptions adaptée.
Les solutions telles que *VMware Workstation (VMware)*, *virtualPC/Virtual Server (Microsoft)*, *VirtualBox (Oracle Corporation, dont une version en licence GNU GPL*[6]*)*, *QEMU*[7] *module kqemu exclu (licence GNU GPL)* sont des exemples de technologies appartenant à cette famille ;

– la **virtualisation assistée par le matériel** permet de gérer la virtualisation directement au niveau du matériel. Ce mode de virtualisation peut être utilisé en complément des autres architectures citées précédemment.
Les solutions reposant sur les composants matériels conçus spécifiquement tels que les processeurs (*Intel VT-x*, *AMD-V*) ou les composants gérant le cloisonnement des flux d'informations (*Intel VT-d*, *AMD IOMMU*[8]) sont des exemples de mécanismes matériels facilitant la mise en œuvre des technologies de virtualisation.
L'avantage de ces solutions est de pouvoir virtualiser des systèmes non spécifiquement modifiés, à l'instar de la virtualisation totale, tout en maintenant un niveau de performance quasi-natif. En revanche, ces technologies sont encore relativement jeunes et peu éprouvées.

Cadre de l'étude et terminologie

La suite de ce document s'appuie sur le cas de la virtualisation au niveau système pour identifier les risques spécifiques qu'il convient de considérer d'un point de vue de la sécurité et les mesures de contournement minimales qui doivent être mises en place. La plupart des risques et contre mesures identifiés s'appliquent également dans le cas de la virtualisation au niveau applicatif.

Les risques liés à l'hébergement mutualisé d'applications sur un même serveur sans virtualisation [9] ne sont pas traités ici. De même, le contexte du *Cloud Computing* externe (hébergé chez un fournisseur de ressources informatiques) n'est pas spécifiquement abordé dans le cadre de cette étude [10].

Pour faciliter la lecture de la suite du document, comme illustré sur la figure 2, nous considérons que :
– la couche d'abstraction est un système d'exploitation (SE) *hôte* ;

6. GNU GPL : GNU General Public License, licence de logiciel à source ouverte permettant de modifier le code source et permettant de redistribuer le code produit à condition de le faire sous la même licence.
7. QEMU est a priori la seule solution de cette liste à n'utiliser que la technique de la traduction d'exécutable à la volée ; les autres solutions utilisent plutôt la technique d'exceptions adaptées.
8. IOMMU : Input/Output Memory Management Unit, gestionnaire de mémoire pour les périphériques (se référer aux explications sur l'IOMMU au paragraphe 3.3).
9. Cas des hébergeurs spécialisés de sites web par exemple, qui hébergent la plupart du temps un grand nombre de sites web appartenant à des clients différents sur une même machine physique, sans faire appel à de la virtualisation, mais en utilisant simplement les fonctionnalités intrinsèques des serveurs web.
10. Voir le guide ANSSI pour maîtriser les risques liés à l'externalisation sur www.ssi.gouv.fr/externalisation.

– les cibles sont les systèmes d'exploitation invités qu'il accueille, encore appelés « instances », qui exécutent des applications ;
– il existe un module d'administration (Admin) qui permet d'administrer la solution de virtualisation.

Dans ce contexte, on retiendra que les termes suivants sont équivalents et peuvent donc être utilisés sans distinction :
– machine physique ou machine hôte ;
– système hôte, système d'exploitation de l'hôte, couche d'abstraction et également par abus de langage hyperviseur (l'hyperviseur est la partie de la couche d'abstraction plus spécifiquement responsable de la virtualisation pour les instances invitées) ;
– système invité, système, instance de la solution de virtualisation, cible ou machine virtuelle.

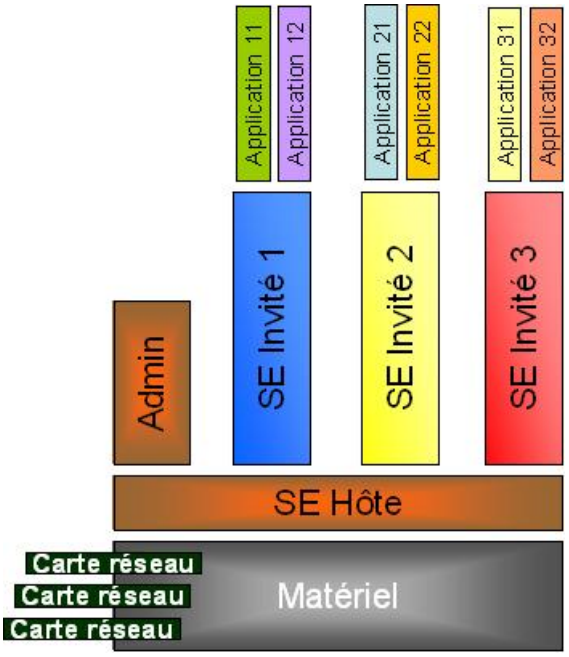

FIGURE 2 – Architecture type d'une machine « virtualisée »

Enfin, il se peut qu'une solution de virtualisation prévoie que des instances puissent migrer d'une machine physique à une autre (par exemple, pour des raisons de répartition de charge, ou à la suite de pannes sur la machine physique). Cela signifierait dans notre illustration que le « SE Invité 2 » par exemple pourrait être « déchargé » de la machine illustrée ci-dessus pour être « rechargé » sur une autre machine (n'apparaissant pas sur la figure). Les termes de « mobilité » ou « migration » d'une instance seront utilisés de manière équivalente dans le reste de ce document pour décrire une telle opération.

4 Les risques liés à la virtualisation

Les risques liés à la virtualisation des systèmes viennent s'ajouter aux risques « classiques » d'un système d'information. Ce sont des **risques nouveaux, additionnels**. En effet, tous les risques existant déjà pour une solution « sans virtualisation » perdurent a priori : les risques liés aux vulnérabilités des systèmes d'exploitation, les risques d'attaques basées sur le matériel ou les risques liés à une administration à distance non sécurisée.

Dans le cas d'un choix d'architecture regroupant plusieurs systèmes sur une même machine, on doit ainsi considérer :

- les risques pouvant toucher un système ;
- ceux portant sur la couche d'abstraction ;
- les risques induits par la combinaison des deux.

De plus, le fait de regrouper plusieurs services sur un même matériel augmente les risques portant sur chacun.

Il est donc important de connaître l'ensemble des risques pour en maîtriser l'impact en termes de confidentialité, d'intégrité et de disponibilité des données et des applications.

Risque 1 : Risque accru de compromission des systèmes

On entend ici par « *compromission* » la prise de contrôle par un acteur malveillant d'une brique utilisée dans le système virtualisé. Il peut s'agir d'une compromission d'un système invité depuis un autre système invité, ou du système hôte depuis un système invité.

On remarque qu'une compromission du système hôte peut éventuellement entraîner une compromission de l'ensemble des systèmes s'exécutant sur la machine. On note également que plus la compromission touche le système en profondeur, plus elle aura de conséquences sur les capacités de remise en service ultérieure du système.

Si une instance est compromise, comment décider si les autres instances qui s'exécutaient sur la machine hôte doivent être considérées comme compromises ? En cas de mise en œuvre de techniques de migration, comment déterminer précisément le domaine de propagation des instances compromises ?

Le principal évènement redouté suite à une compromission est **la fuite d'informations sensibles** ou, dans certains cas, des perturbations engendrées par une modification du système pouvant aller jusqu'à l'indisponibilité d'un service.

Les solutions permettant d'empêcher une compromission sont souvent délicates à mettre en œuvre. Il s'agira de **diminuer au maximum la surface d'attaque**. Il conviendra notamment que chaque brique (matériel, système d'exploitation hôte, systèmes d'exploitation invités etc.) soit à jour de tous les correctifs de sécurité. En particulier, l'emploi d'une solution de virtualisation imposant aux systèmes invités de fonctionner dans des configurations obsolescentes n'est pas acceptable.

Plus généralement, l'application stricte du principe de défense en profondeur [11] est indispensable. Pour cela, on veillera à utiliser uniquement des systèmes, hôtes et invités, pouvant être nativement sécurisés [12].

Les systèmes invités doivent en effet être durcis pour rendre difficile l'exploitation d'une faille potentielle présente dans la couche d'abstraction ou dans la couche matérielle.

11. La défense en profondeur consiste à mettre en place plusieurs techniques de sécurité complémentaires afin de réduire l'impact lorsqu'un composant particulier de sécurité est compromis ou défaillant.

12. Ces systèmes sont nativement sécurisés car ils mettent en œuvre certains mécanismes de sécurité : par exemple, le mécanisme du bit Nx (No-eXecute) qui permet au système de gérer des zones mémoire pour lesquelles toute exécution de code est interdite.

Enfin, il est généralement aisé de « remonter » un système invité défaillant sur une autre machine physique à partir d'une image saine. Néanmoins, seule la mise en œuvre du principe de défense en profondeur permet de localiser précisément l'origine de la compromission (système invité, système hôte, matériel, données, etc.).

Risque 2 : Accroissement du risque d'indisponibilité

Comme évoqué précédemment, une compromission peut engendrer une indisponibilité d'un service. Cependant, ce risque peut apparaître, même en l'absence de compromission. Ainsi, si d'une part un atout de la virtualisation est l'utilisation plus intensive des ressources informatiques, d'autre part, **la panne d'une ressource commune peut engendrer l'indisponibilité simultanée de plusieurs systèmes**. De même, **une attaque en disponibilité** sur un des systèmes (ou plus généralement sur une ressource commune) **impactera potentiellement tous les services** hébergés sur la même machine.

Là encore, les préconisations faites au point précédent s'appliquent. De plus, si des besoins en disponibilité différent sensiblement d'une application à une autre, il peut être **préférable de placer sur des machines dédiées celles dont les besoins en disponibilité sont les plus élevés**.

Risque 3 : Fuite d'information par manque de cloisonnement

Bien que les solutions de virtualisation mettent généralement en œuvre des mécanismes de cloisonnement des instances se partageant une même ressource, ces instances ne sont en pratique jamais totalement isolées. Dans certains cas, des flux existent entre les différentes instances (systèmes d'exploitation, applications, systèmes de stockage de données, ...), et ces flux peuvent engendrer des vulnérabilités.

La maîtrise des différents échanges internes à une même machine physique est par ailleurs particulièrement difficile. En effet, il sera généralement délicat de garantir que les ressources bas niveau partagées ne permettent pas des fuites d'information.

Pour illustrer ces propos, prenons l'exemple de l'accès au réseau d'une machine informatique. Dans une architecture sans virtualisation, les machines (au nombre de trois sur la figure 3) communiquent sur des réseaux physiques au moyen, par exemple, d'une carte réseau spécifique. Les flux de données sont ainsi traités, au niveau des machines, par chaque carte réseau et peuvent être identifiés précisément.

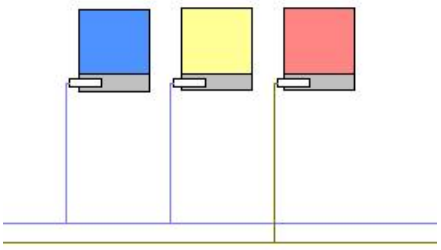

FIGURE 3 – Architecture sans virtualisation

Sur le schéma ci-dessus, les carrés de couleur et leur zone grise associée représentent des machines physiques ; le gris représente le matériel, les carrés de couleurs le logiciel s'exécutant sur chaque machine, les rectangles blancs représentent plus spécifiquement les cartes réseau.

Dans une architecture avec virtualisation, les machines virtuelles peuvent par exemple communiquer sur des réseaux physiques par le biais d'une carte unique appartenant à la machine physique qui les

héberge. Les flux de données de chaque machine virtuelle sont donc traités par cette unique carte réseau. Dès lors, il n'est pas possible de garantir un cloisonnement des flux au niveau de la ressource partagée. En cas d'erreur ou de compromission de la carte réseau, un accès aux données des différents flux d'information est possible (cf. figure 4).

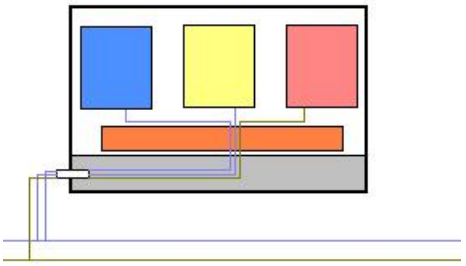

FIGURE 4 – Architecture avec virtualisation

Sur la figure 4 ci-dessus, la zone grise matérialise la machine physique ; trois machines virtuelles sont représentées par les rectangles bleu, jaune, rouge ; la zone orange représente la couche d'abstraction.

Dans ce contexte, pour mieux répondre au besoin de cloisonnement, le choix peut être fait d'avoir autant de cartes réseau que de machines virtuelles hébergées sur une machine physique (cf. figure 5). Il conviendrait idéalement de vérifier - mais une telle vérification est en pratique irréaliste - que les composants impliqués dans la chaîne de traitement du flux de données entre une machine virtuelle et la carte réseau attribuée gèrent correctement le cloisonnement des données suivant leur appartenance à une machine virtuelle. Par exemple, pour gérer le cloisonnement des flux d'entrées/sorties passant par la mémoire, un composant IOMMU peut être utilisé (représenté par le quadrillage dans la figure 5) ; mais si un contrôleur d'entrées/sorties non compatible avec le composant IOMMU est utilisé, il fera passer dans une zone mémoire commune tous les flux issus des différentes machines virtuelles, ce qui présente un risque de fuite d'informations, volontaire ou non.

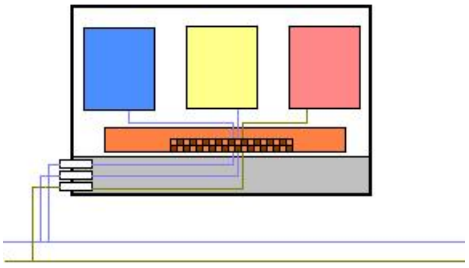

FIGURE 5 – Architecture avec virtualisation comprenant une carte réseau physique par système invité

Enfin, s'il s'avère que les objectifs de sécurité fixés en matière de cloisonnement ne peuvent être remplis par l'une ou l'autre des techniques évoquées précédemment, certains environnements (réseau par exemple) ne devront pas s'exécuter dans l'environnement virtualisé. Le choix d'un retour partiel à une solution classique (c'est à dire sans virtualisation) pourra alors être plus adapté à un bon cloisonnement des flux (cf. figure 6).

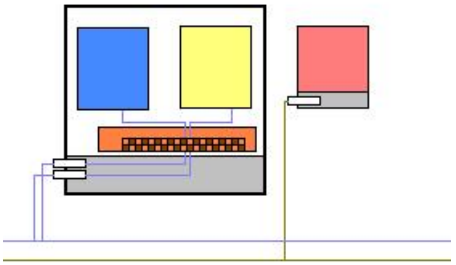

FIGURE 6 – Architecture mixte, avec et sans virtualisation

Les risques principaux induits par un défaut d'isolation sont la fuite d'information et l'atteinte à l'intégrité des données. Un moyen de réduire ces risques pourra être aussi, suivant les contextes, de garantir une bonne étanchéité des données par le biais de mécanismes de confidentialité et de contrôle d'intégrité des données de bout en bout (par exemple dans le cas du réseau, par l'utilisation d'IPsec).

Risque 4 : Complexification de l'administration et de la mise en œuvre

Lorsqu'une solution de virtualisation est utilisée, il est nécessaire d'administrer d'une part les différents systèmes invités, mais également la couche d'abstraction. Des exemples d'opérations d'administration nouvelles, induites par l'utilisation de technologies de virtualisation, sont les suivants :

- mise en place des quotas sur les ressources partagées entre différents systèmes ;
- gestion de l'ajout d'un disque ou d'un périphérique de stockage réseau (NAS) sans remise en question du cloisonnement mis en place entre machines virtuelles ;
- sauvegardes spécifiques liées aux opérations de virtualisation, protection de ces sauvegardes, opérations de restauration. La mobilité éventuelle des machines virtuelles lors des sauvegardes doit être prise en compte, ainsi que les corrélations fortes qui peuvent exister entre les sauvegardes des différents systèmes et des données.

Les tâches d'administration classiques peuvent également s'avérer plus complexes car les interventions sur la machine physique proprement dite (administrateur du système hôte), sur les instances qui y sont hébergées (administrateur(s) des systèmes invités), sur les périphériques de stockage physiques et virtuels (SAN / NAS) et sur les équipements réseau physiques et (éventuellement) virtuels peuvent devoir être réalisées séparément. En effet, si comme dans de nombreuses organisations de taille importante, les équipes gérant les serveurs, le stockage, le réseau et les sauvegardes sont disjointes, l'identification des responsabilités de chacun dans l'administration d'un système virtualisé est indispensable afin de limiter, autant que faire se peut, les erreurs de configuration, comme par exemple, le positionnement d'une machine virtuelle dans le mauvais réseau virtuel (VLAN).

L'administration des machines peut s'opérer localement ou à distance. S'il est généralement difficile d'administrer localement les systèmes invités, la question se pose pour la couche d'abstraction.

Le choix d'administration d'un système à distance ou non doit être fait en considérant tous les risques induits. Parmi de tels risques, on trouve l'usurpation du rôle d'administrateur permise suite à la mise en place d'un mécanisme d'authentification trop faible, la perte de confidentialité et/ou d'intégrité d'une commande circulant sur le réseau, la perte de traçabilité des opérations d'administration. Si l'organisation utilise des technologies d'informatique en nuage (*Cloud Computing*), une attention toute particulière doit être portée sur la gestion des machines virtuelles qui peut, dans certains cas, être très automatisée (guichet de demande d'une nouvelle machine virtuelle par un utilisateur métier, avec livraison immédiate, par exemple). Il convient ainsi de bien sécuriser l'ensemble des interfaces de gestion et de tracer toute action réalisée par leur biais.

Risque 5 : Complexification de la supervision

À l'instar des opérations d'administration, les opérations de supervision peuvent aussi s'avérer complexes, en particulier du fait du paradoxe qui existe entre la nécessité de cloisonnement des machines virtuelles et le souhait d'une vision d'ensemble lors des opérations de supervision. Compte-tenu des cloisonnements induits par la solution de virtualisation, il peut être difficile de tracer un événement ou une action de bout en bout.

De plus, la nécessité de disposer d'une vision d'ensemble impose que le personnel opérant les moyens de supervision soit autorisé à accéder aux informations du niveau de sensibilité le plus élevé des données traitées.

Risque 6 : Prolifération non souhaitée des données et des systèmes

La virtualisation rend les systèmes invités moins adhérents aux équipements. Leur migration sur différentes machines est donc possible, et la plupart du temps souhaitée. En conséquence, la localisation précise d'une donnée est complexifiée [13]. De même, il sera globalement plus difficile d'empêcher la copie frauduleuse d'une information.

Par ailleurs, les principes de migration des instances impliquent généralement que ces dernières soient sous forme « d'objets migrables ». Les risques de copie non maîtrisée (non respect des licences logicielles) des instances, de perte, de vol, de modification ou de perte de maîtrise des versions logicielles des instances (régression) sont importants.

Risque 7 : Incapacité à gérer voire à comprendre les erreurs

Les problèmes de fonctionnement et les erreurs peuvent être complexes à gérer techniquement dans une architecture s'appuyant sur une solution de virtualisation.

Par exemple, les erreurs qui pourraient survenir lors de l'arrêt puis la relance d'une instance seront soit rapportées au système hôte que l'instance quitte, soit au système hôte qui est en train de l'accueillir. Sans la prise en compte globale des erreurs d'un système s'appuyant sur la virtualisation, il se peut que des informations pertinentes permettant d'identifier leur cause soient perdues, ou a minima, que leur synthèse ne puisse pas être réalisée. Il convient donc de mettre en place une centralisation et une corrélation des journaux sur l'ensemble des systèmes. Cette corrélation pose évidemment des problèmes identiques à ceux identifiés précédemment pour la supervision.

Risque 8 : Investigations post incident plus difficiles

Les principes sur lesquels reposent les techniques de virtualisation peuvent rendre difficiles certaines investigations après un incident du fait du partage de ressources matérielles par plusieurs systèmes.

Ainsi, l'optimisation de la gestion de la mémoire vive effectuée par la solution de virtualisation rend plus délicate toute analyse de l'historique des états de la machine et donc le traitement d'un incident. L'optimisation qui consiste à réallouer à d'autres machines virtuelles l'espace en mémoire d'une machine virtuelle dès qu'elle n'est plus utilisée pose potentiellement des problèmes en matière d'analyse *post mortem*. Seule la connaissance précise du mode de fonctionnement des solutions de virtualisation permettra de retenir celles qui gèrent le plus rigoureusement les accès mémoire et facilitent des investigations *post* incidents.

13. Voir le guide spécifique sur l'externalisation rédigé par l'ANSSI. Vous pouvez le télécharger à l'adresse suivante : http://www.ssi.gouv.fr/externalisation/.

5 Recommandations

Compte tenu de ces différents risques, il convient de tenir compte des 9 recommandations qui suivent.

R1	La politique de sécurité du système faisant l'objet d'une démarche de virtualisation doit être mise à jour pour qu'y soient inclus certains items spécifiques à la technologie de virtualisation employée.

Définition précise des processus d'administration des systèmes hôtes et invités

Il s'agit de décrire de manière précise les règles relatives à l'administration des systèmes. Une règle peut être de ne pas autoriser l'administration distante de certaines machines compte tenu du degré de sensibilité des informations qu'elles hébergent, y compris ponctuellement. Il est par ailleurs recommandé de renforcer certains mécanismes de sécurité dans le cas d'administration distante (mise en œuvre de mécanismes d'authentification forte, de confidentialité et de contrôle d'intégrité, d'audit).

Description détaillée des configurations de système(s) attendues

Il s'agit de décrire de manière précise les configurations de système(s) attendues en identifiant clairement les mécanismes qui peuvent contribuer directement ou indirectement à couvrir les risques induits par la virtualisation. Tout paramètre système visant à améliorer les principes d'étanchéité et de non propagation des compromissions est ainsi à considérer.

Procédures de mise à niveau et de suivi des systèmes invités

La mise à niveau des systèmes invités consiste à mettre à jour une machine virtuelle (versions du système et de ses applications, maintien des licences nécessaires, application régulière des correctifs de sécurité, etc.) quel que soit l'état dans lequel elle se trouve (en exécution ou sous sa forme d'image stockée quelque part dans le système d'information).

Le suivi des systèmes invités quant à lui consiste à déterminer à tout instant et de manière précise la localisation d'une machine virtuelle.

Des procédures claires doivent être référencées dans la politique de sécurité du système ayant fait l'objet d'une virtualisation. Ces dernières prennent en compte les applications s'exécutant sur les machines virtuelles et les contraintes associées (ex : report d'une mise à jour).

Établissement des règles de localisation et de migration des systèmes

Afin de couvrir notamment le risque 6 ci-dessus, il sera nécessaire de définir une politique de localisation des systèmes invités et de migration. Cette politique devra notamment :

- décrire explicitement les types des machines physiques hôtes ;
- décrire explicitement les types des systèmes gérés ;
- définir les règles de localisation d'une machine virtuelle sur une machine hôte. Une de ces règles pourra être de refuser qu'une même ressource héberge des systèmes ayant des niveaux de sensibilité ou de confiance différents.

R2	Un processus de veille des vulnérabilités propres aux technologies de virtualisation utilisées au sein de l'organisme doit être mis en place.

Les alertes diffusées par les éditeurs de solutions de virtualisation doivent être particulièrement surveillées, de même que celles des éditeurs de systèmes d'exploitation et de matériels utilisés dans les architectures de virtualisation (serveurs, cartes réseau, équipements de stockage, etc...) et celles des CERT. Ceci est indispensable au maintien en condition de sécurité du système mettant en œuvre ces technologies dès lors que sont appliqués les correctifs couvrant l'apparition de vulnérabilités. En l'absence de correctif, une analyse doit être effectuée afin d'apprécier le risque et prendre les mesures organisationnelles adaptées pour le limiter.

On pourra ainsi établir une liste précise des technologies matérielles ou logicielles utilisées par l'entreprise et des vulnérabilités connues sur ces technologies. Lorsque le niveau de vulnérabilité d'une technologique atteindra un niveau jugé non acceptable, on devra envisager son retrait du service.

On devra préférer les solutions de virtualisation qualifiées par l'ANSSI, et à défaut certifiées, en s'assurant néanmoins que le niveau de l'évaluation et la cible de sécurité associées prennent bien en compte les problématiques évoquées précédemment (cloisonnement sûr des flux de données, etc.).

R3	Réduire la surface d'attaque de la solution de virtualisation.

Certaines solutions de virtualisation comportent des éléments d'authentification par défaut (mots de passe par défaut, certificats par défaut ou générés à la première initialisation de la machine). Il est impératif de changer les éléments d'authentification par défaut avant la mise en service opérationnelle de la solution. Par ailleurs, toutes les fonctions non strictement nécessaires au bon fonctionnement de la solution dans l'environnement opérationnel (exemple : migration à chaud de machines virtuelles entre deux serveurs hôtes) doivent systématiquement être désactivées.

R4	Concevoir une architecture respectant le principe de cloisonnement.

Les exigences de cloisonnement (isolation des flux) doivent être prises en compte dans la conception de l'architecture du système.

Cela conduit de fait à définir très précisément l'architecture matérielle nécessaire pour répondre au besoin fonctionnel en tenant compte des objectifs de sécurité fixés, et à décrire des règles précises à appliquer lors des évolutions du système.

L'exemple suivant concerne le cas du réseau, pour lequel certains problèmes potentiels ont déjà été sommairement présentés précédemment.

Suivant les cas et les contextes, l'architecture matérielle pourra ainsi prévoir au choix :
- une carte réseau physique distincte pour chaque machine virtuelle hébergée sur une machine physique. Ceci est à moduler si des moyens complémentaires garantissant un bon cloisonnement des flux (chiffrement IPsec) sont prévus par ailleurs ;
- une carte réseau physique distincte pour chaque groupe de machines virtuelles hébergé sur une machine physique, les machines virtuelles étant regroupées par exemple par niveau de sensibilité des informations manipulées. L'emploi là aussi de moyens complémentaires pour cloisonner correctement les flux peut moduler cette règle ;
- qu'une partie du système soit gérée en dehors de la solution de virtualisation. Cette situation pourra se produire si une application particulière a des besoins de sécurité supérieurs à d'autres.

R5	Utiliser des matériels gérant le cloisonnement.

Tout matériel, quel que soit son type (contrôleur disque, carte réseau, processeur, etc.) doit, autant que faire se peut, gérer le cloisonnement rendu nécessaire par la virtualisation (isolation des flux). Si le niveau d'exigences établi par la politique de sécurité ne peut être atteint, la pertinence de l'emploi des technologies de virtualisation devra être réévaluée.

Le choix d'un matériel ne supportant pas les mécanismes de cloisonnement devra être justifié et les risques induits assumés.

Par exemple, si la solution de virtualisation retenue est à même de gérer une IOMMU, on pourra rendre obligatoire l'utilisation de composants [14] compatibles avec cette IOMMU.

R6	Mettre à jour le plan de reprise ou de continuité d'activité.

Lors de la compromission d'un système, il est difficile d'affirmer que les autres systèmes s'exécutant sur la même machine ne sont pas affectés. Les plans de reprise et de continuité d'activité doivent donc tenir compte des spécificités liées à la virtualisation et être mis à jour en conséquence.

R7	Dédier une équipe d'administration à la solution de virtualisation distincte de celle des systèmes invités.

Dans une logique de séparation des rôles, il est nécessaire de prévoir une équipe d'administration de la solution de virtualisation qui soit indépendante de l'équipe d'administration des systèmes invités.

L'équipe d'administration de la solution de virtualisation doit avoir notamment en charge :
- l'administration des machines hôtes ;
- l'administration des équipements de stockage physiques (NAS/SAN) ;
- l'administration des équipements réseau physiques (et virtuels le cas échéant) ;
- l'administration de la solution de virtualisation (dans son ensemble) ;
- la gestion de la sécurité associée à la virtualisation et plus particulièrement le maintien d'un cloisonnement des instances hébergées du fait du partage de ressources ;
- éventuellement l'audit et la supervision des machines hôtes.

Cette équipe doit disposer du droit d'en connaître sur toutes les données, y compris celles ayant la sensibilité la plus élevée manipulées par les systèmes considérés sauf si elles soient chiffrées de telle sorte que l'équipe d'administration ne puisse techniquement y accéder.

R8	Prévoir une équipe d'administration des machines virtuelles (systèmes invités) indépendante de l'équipe d'administration de la solution de virtualisation.

L'équipe d'administration des machines virtuelles (systèmes invités) a notamment en charge :
- l'administration des systèmes d'exploitation invités ainsi que leurs applications ;
- la sécurité propre à ces systèmes et leurs applications ;
- éventuellement l'audit et la supervision de ces systèmes et leurs applications.

Cette équipe doit disposer du droit d'en connaître sur toutes les données traitées par les systèmes invités dont elle a la responsabilité y compris celles qui ont la sensibilité la plus élevée.

R9	Former les équipes d'administration, d'audit et de supervision aux techniques de virtualisation.

14. Le terme de composant est à prendre au sens large : il comprend aussi bien les composants matériels, que logiciels.

Il s'agit de former spécifiquement les administrateurs, les auditeurs et les superviseurs aux techniques de virtualisation afin qu'ils les maîtrisent et les sécurisent. Ces personnes doivent donc acquérir une bonne connaissance des technologies employées et être familiers des tâches d'administration système et réseau usuelles.

Il n'est pas nécessaire de former tous les administrateurs mais confier l'administration et la supervision des couches de virtualisation aux plus intéressés et expérimentés est un bon choix.

6 Points de contrôle

Comme évoqué à plusieurs reprises, la virtualisation des systèmes informatiques engendre des problématiques SSI spécifiques. L'objectif de ce chapitre est de rassembler l'ensemble des points de contrôle qui permettront d'apprécier le niveau de sécurité d'un système informatique virtualisé. Il conviendra de se référer aux chapitres précédents pour plus de détails sur chacun de ces points.

☐ L'architecture de la solution de virtualisation a été conçue en prenant en compte les éléments suivants :
- le niveau d'exigences en termes de sécurité d'une machine physique doit être au moins égal au niveau d'exigences du système invité ayant le besoin de sécurité le plus élevé ;
- une atteinte en intégrité d'un des systèmes invités sur une machine physique peut porter atteinte à la sécurité de tous ses systèmes invités ;
- le risque d'indisponibilité d'une application est plus élevé si elle est hébergée sur une machine virtuelle ;
- la migration non voulue des systèmes invités, de leurs applications et des données qu'elles traitent, d'une machine physique à une autre peut conduire à une circulation non souhaitée des données sur le réseau ;

☐ Les systèmes invités présents sur une même machine physique manipulent des données qui ont une sensibilité similaire ;

☐ Les systèmes invités présents sur une même machine physique appartiennent originellement à une même zone de confiance (Réseau d'entreprise interne, de production, de recherche et développement, etc.) ;

☐ Une carte réseau physique est utilisée par groupe de systèmes invités qui manipulent des données de même sensibilité, en particulier si aucun autre moyen complémentaire de protection des flux (tel le chiffrement) n'est prévu par ailleurs ;

☐ L'utilisation des ressources (processeur, mémoire, espace disque) par chaque machine virtuelle est limitée afin qu'aucune d'elles ne puisse monopoliser le système hôte au détriment des autres ;

☐ Des règles strictes, précises et cohérentes concernant la migration manuelle ou automatique des systèmes invités, de leurs applications et des données traitées entre différentes machines physiques sont établies ;

☐ Un réseau est dédié pour l'administration et la supervision des systèmes hôtes en s'appuyant sur des moyens réseau (cartes réseau, commutateurs) distincts de ceux utilisés par les systèmes invités ;

☐ Les postes dédiés à l'administration et à la supervision des machines virtuelles sont correctement sécurisés. En particulier, ils ne permettent pas l'accès à Internet ;

☐ Les administrateurs des machines hôtes doivent s'authentifier nominativement, et leurs actions sont journalisées ;

- ☐ Tous les éléments d'authentification (mots de passe, certificats) par défaut ont été supprimés ou modifiés ;
- ☐ La solution de virtualisation gère de manière adéquate le cloisonnement des données, y compris vis à vis des périphériques, par la mise en œuvre, entre autres, d'une IOMMU (*Input/Output Memory Management Unit*) ;
- ☐ La solution de virtualisation ne diminue pas le niveau de sécurité intrinsèque des systèmes invités. Par exemple, elle ne doit pas leur donner accès à des fonctionnalités matérielles sur lesquelles reposent certains de leurs mécanismes de sécurité ;
- ☐ Les systèmes hôtes et les systèmes invités sont impérativement sécurisés, notamment en durcissant les systèmes d'exploitation et en maîtrisant leur configuration. Ceci impose une gestion rigoureuse des supports d'installation et des mises à jour ;
- ☐ Les politiques et moyens techniques de mise à jour des systèmes invités, du système hôte et de la solution de virtualisation sont clairement définis, en particulier les mécanismes appliquant et contrôlant les mises à jour de sécurité des systèmes s'ils accèdent à Internet ou sont accessibles depuis Internet ;
- ☐ La solution de virtualisation a été évaluée d'un point de vue de la sécurité. Les mécanismes de cloisonnement entre les machines virtuelles font partie de la cible de sécurité s'il s'agit d'une certification ;
- ☐ L'ensemble des matériels, des systèmes et des couches de virtualisation est supervisé. Cela impose au minimum la journalisation des informations de virtualisation, la synchronisation temporelle des machines hôtes, des systèmes invités et des éléments actifs du réseau afin de pouvoir corréler les journaux ;
- ☐ La politique de sécurité existante prend bien en compte tous les points spécifiques à la solution de virtualisation mise en place ;
- ☐ Des administrateurs réseau et système sont formés aux techniques de la virtualisation. Les administrateurs de la solution de virtualisation sont choisis parmi les plus expérimentés ;
- ☐ Les administrateurs des machines hôtes et ceux des systèmes invités sont distincts ;
- ☐ Le personnel assurant l'administration et la supervision fait si possible l'objet d'une enquête de sécurité (voire, en fonction du contexte, d'une habilitation à accéder à des données de niveau de classification supérieur à celui des données traitées par les systèmes qu'il administre et/ou supervise) ;
- ☐ Les machines virtuelles sont créées et administrées en respectant des procédures rigoureuses. Ces procédures empêchent la prolifération non maîtrisée des images représentant les machines virtuelles et la copie ou le vol de ces images. Elles permettent de gérer la mise à jour de sécurité de ces images afin de garantir l'exécution des machines virtuelles dans leur version la plus à jour.