

Audit des risques en sécurité des systèmes informatiques virtuels

Abhik Chaudhuri, MCA, PMP, est un expert informatique accrédité par IBM, qui possède une expérience dans la gestion de projets et l'administration de la sécurité informatique. Il peut être contacté à l'adresse suivante : abhik.chaudhuri@gmail.com.

SH (Basie) von Solms est directeur de recherche à l'Academy for Information Technology de l'université de Johannesburg, en Afrique du Sud. Il est spécialisé dans la recherche et le conseil sur la sécurité des informations, et travaille comme consultant dans ce domaine depuis une quinzaine d'années. Il est également membre de la Computer Society of South Africa et de la British Computer Society.

Dipanwita Chaudhuri, ACA (ICAI), MIIA, est responsable des services de conseils en gestion d'un cabinet d'experts-comptables réputé de Kolkata, en Inde. Elle est expert-comptable auprès de l'Asian Development Bank. Elle peut être contactée à l'adresse suivante : banerjee.dipanwita@gmail.com.

La virtualisation des systèmes informatiques a gagné en popularité et en importance au cours des dernières années, mais son origine remonte à 1972, quand IBM a introduit la technologie de la virtualisation dans les grands systèmes (mainframe). Pendant longtemps, les PDG et les directeurs informatiques des entreprises ont accepté les serveurs traditionnels pour gérer leurs activités quotidiennes ; toutefois, des études révèlent que cette approche se traduit par des gaspillages en termes de puissance de traitement et de ressources matérielles, car aucun serveur n'est exploité pleinement. Les récentes tendances montrent que les responsables informatiques cherchent d'urgence à réduire les dépenses informatiques et à promouvoir « l'informatique verte ». La virtualisation des systèmes informatiques joue un rôle essentiel dans cette perspective.

La virtualisation permet de réaliser des économies significatives en partageant l'espace de stockage et la capacité de l'unité centrale (UC). Toutefois, comme toute autre technologie, les systèmes informatiques virtuels ne sont pas exempts de risques. Si une entreprise veut bénéficier des avantages qu'offre la virtualisation, elle doit élaborer et mettre en œuvre une stratégie appropriée de réduction des risques. Les auditeurs en sécurité de l'information ont un rôle important à jouer dans l'audit des risques liés aux systèmes informatiques virtuels. Le présent article traite des systèmes informatiques virtuels et des risques leur sont inhérents et doivent être audités pour les réduire correctement. Il fournit un guide auquel on peut se référer pour sécuriser les systèmes informatiques virtuels et en auditer la sécurité.

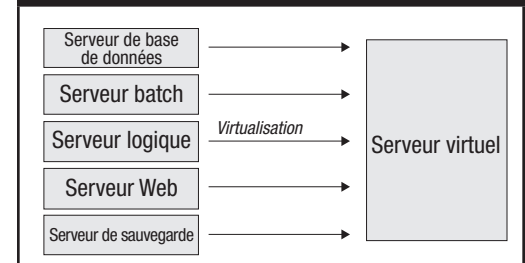
QU'EST-CE QUE LA VIRTUALISATION ?

La virtualisation est une technologie logicielle qui divise une ressource physique, par exemple un serveur, en plusieurs ressources virtuelles appelées « machines virtuelles » (voir la **figure 1**). La virtualisation aide à consolider les ressources physiques, à simplifier le déploiement et l'administration, et à réduire la consommation électrique et la capacité de refroidissement requises.

Dans un système informatique, la virtualisation ajoute une couche d'abstraction entre deux couches de ce système. Cette couche d'abstraction est une couche logicielle insérée entre le matériel et

les systèmes d'exploitation invités. Cette couche fait office de gestionnaire des ressources pour permettre le partage de la puissance de traitement et de la mémoire. Ce logiciel est appelé « moniteur de machines virtuelles » (MMV) ou « hyperviseur ». Les moniteurs de machines virtuelles virtualisent le matériel d'une machine physique et le partitionnent en plusieurs machines virtuelles séparées de façon logique. Le moniteur de machines virtuelles contrôle tous les événements qui se produisent à l'intérieur d'une machine virtuelle et applique sur cette dernière les stratégies de gestion des ressources. Plusieurs systèmes d'exploitation peuvent coexister sur la même machine virtuelle, tout en étant isolés les uns des autres, et peuvent fonctionner simultanément sur un même serveur. La virtualisation permet aux entreprises d'éliminer les serveurs matériels dédiés et de réduire ainsi leurs dépenses d'acquisition, de maintenance et d'électricité.

Figure 1—Passage d'une infrastructure physique à une infrastructure virtuelle



TYPES DE VIRTUALISATION

Bien que la technologie de virtualisation des serveurs soit la plus populaire, la virtualisation ne se limite pas qu'aux serveurs. Elle peut aussi s'appliquer aux systèmes d'exploitation, aux ordinateurs de bureau, aux applications, au stockage et aux réseaux. La technologie des machines virtuelles est également utilisée pour le stockage des données, par exemple les réseaux de stockage SAN, et à l'intérieur des systèmes d'exploitation, tels que Windows Server 2008 avec Hyper-V. La virtualisation dans un environnement distribué est la base de la grille informatique (grid computing) et de l'informatique en nuage (cloud computing), offrant une infrastructure informatique en tant qu'utilitaire, ou services à la demande.

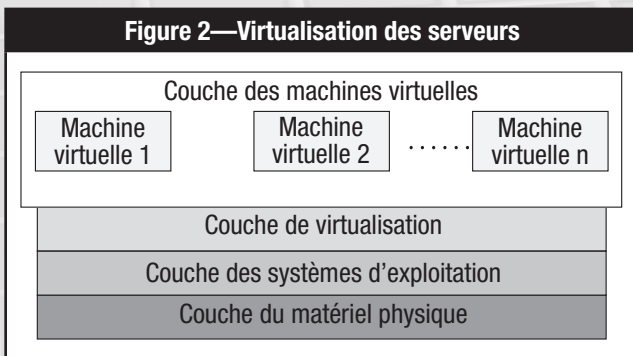
La virtualisation peut être classée dans trois catégories :

1. **Virtualisation du stockage**—Virtualise le stockage physique à partir de plusieurs périphériques de stockage en réseau, de sorte que ceux-ci apparaissent comme un périphérique de stockage unique. En règle générale, le terme « virtualisation » désigne la virtualisation des serveurs.
2. **Virtualisation des réseaux**—Combine les ressources informatiques sur un réseau en divisant la bande passante disponible en des canaux indépendants qui peuvent être affectés à un serveur ou à un périphérique particulier en temps réel.
3. **Virtualisation des serveurs**—Dissimule la nature physique des ressources serveurs, y compris le nombre et l'identité des serveurs, processeurs et systèmes d'exploitation individuels, aux logiciels qui s'exécutent sur ces ressources.

APERÇU DE L'ARCHITECTURE DE LA TECHNOLOGIE DE VIRTUALISATION DES SERVEURS

La virtualisation des serveurs permet l'exécution simultanée de plusieurs systèmes d'exploitation et applications sur un équipement unique. Les systèmes d'exploitation s'exécutent indépendamment les uns des autres dans des environnements isolés (les machines virtuelles). Une couche de virtualisation doit s'exécuter sur les systèmes d'exploitation de l'ordinateur en tant qu'application ou service afin de créer plusieurs environnements de machines virtuelles. Les systèmes d'exploitation et les applications qui s'exécutent sur une machine virtuelle peuvent accéder à des ressources UC, mémoire, disque et réseau similaires à celles d'un ordinateur physique.

La **figure 2** illustre à grands traits l'architecture de la technologie de virtualisation des serveurs.

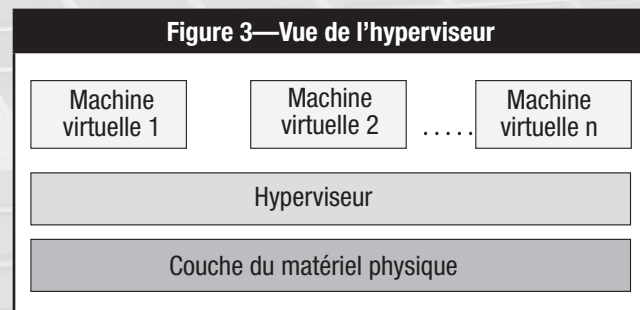


Les composants d'un serveur virtuel sont les suivants :

- **Matériel physique ou hôte de virtualisation**—Machine physique sur laquelle résident les environnements de machine virtuelle. Le nombre de machines virtuelles qui peuvent être prises en charge sur une machine physique unique varie selon la configuration et les caractéristiques du matériel.

- **Système d'exploitation hôte**—Système d'exploitation principal sur la machine physique. La couche de virtualisation réside sur ce système d'exploitation.
- **Couche de virtualisation**—Logiciel de virtualisation qui coordonne avec les systèmes d'exploitation hôtes les demandes émanant des machines virtuelles concernant le temps UC, la mémoire physique, les opérations de lecture et d'écriture sur les disques, les entrées/sorties (E/S) sur les réseaux, etc. Le logiciel de virtualisation est appelé « hyperviseur » (voir la **figure 3**). Il s'agit d'un composant primordial de la technologie de virtualisation. Il intercepte les demandes de ressources matérielles émanant des machines virtuelles qu'il héberge et il convertit ces demandes dans un format lisible par le matériel physique. De même, les demandes émanant du matériel physique sont converties par l'hyperviseur de sorte qu'elles puissent être interprétées par les machines virtuelles. L'hyperviseur découple les machines virtuelles des hôtes physiques en introduisant une couche d'abstraction entre les machines virtuelles et la couche du matériel physique.

Toutes les solutions de virtualisation ne font pas appel à un hyperviseur. Parmi celles qui utilisent effectivement un hyperviseur, nous pouvons citer notamment VMware ESX, VMware Virtual Infrastructure, Microsoft Hyper-V et Citrix XenSource.



- **Machine virtuelle**—Environnement indépendant et isolé créé par le logiciel de virtualisation. Les systèmes d'exploitation peuvent exécuter des machines virtuelles indépendamment les unes des autres.
- **Systèmes d'exploitation invités**—Systèmes d'exploitation installés sur les machines virtuelles. Ceux-ci s'exécutent sur le système d'exploitation hôte. La technologie de virtualisation permet l'exécution de plusieurs machines virtuelles équipées de systèmes d'exploitation invités hétérogènes de façon isolée et côte à côte sur la même machine physique. Les machines virtuelles ont leur propre matériel virtuel (p. ex., UC, mémoire RAM, disques, cartes réseau) sur lequel sont chargés les systèmes d'exploitation invités et les applications. Les systèmes d'exploitation invités s'exécutent de manière uniforme, quels que soient les composants physiques.

AVANTAGES DE LA VIRTUALISATION

La virtualisation des systèmes informatiques offre de nombreux avantages. C'est pourquoi elle est devenue si populaire. Outre qu'elle améliore l'agilité du service informatique, la virtualisation réduit les coûts de possession de l'infrastructure, grâce à la réduction du nombre total de serveurs physiques. Et en conséquence, elle permet d'abaisser considérablement les dépenses d'exploitation.

La virtualisation accélère la procédure d'allocation de ressources des serveurs et améliore la gestion des capacités. L'efficacité informatique est également accrue grâce au partage de la capacité de traitement de l'UC et à l'utilisation efficace du stockage. Les machines virtuelles sont capables d'exécuter différents systèmes d'exploitation et offrent plusieurs avantages, par exemple l'encapsulation, l'isolement et le partitionnement.

Les machines virtuelles sont encapsulées dans des fichiers, ce qui permet de les enregistrer, de les copier et d'allouer leurs ressources rapidement. Il est aussi possible de transférer du matériel virtuel, des systèmes d'exploitation, des applications et des environnements complètement configurés en l'espace de quelques secondes seulement d'un serveur physique vers un autre, ce qui permet une maintenance sans interruption de service et la consolidation continue des charges de travail.

Les machines virtuelles sont complètement isolées de la machine hôte et des autres machines virtuelles. En cas de panne d'une machine virtuelle, les autres ne sont pas affectées. Aucune perte de données n'est possible sur les machines virtuelles et les applications peuvent uniquement communiquer sur des connexions réseau configurées.

La virtualisation permet le partitionnement de plusieurs applications et la prise en charge de plusieurs systèmes d'exploitation au sein d'un seul système physique. Les serveurs peuvent être consolidés sous forme de machines virtuelles dans une architecture de type « scale-up » (pour une évolutivité verticale) ou « scale-out » (pour une évolutivité horizontale), et les ressources informatiques peuvent être traitées comme un groupe uniforme pouvant être alloué aux machines virtuelles de manière contrôlée.

Parmi les autres avantages significatifs de la virtualisation, on notera la séparation efficace des tâches, la prise en charge de la simulation avec plusieurs versions du même système d'exploitation ou de différents systèmes d'exploitation, davantage d'options de continuité et l'extension de l'environnement de test. Quelques grandes entreprises ont adopté la virtualisation pour améliorer leur résilience, aider à la reprise après sinistre et à la continuité d'activité.

Du point de vue de la sécurité, la virtualisation offre les avantages suivants :

- Meilleures capacités de diagnostic des problèmes

- Récupération plus rapide après une attaque
- Application des correctifs de façon plus sûre et efficace
- Meilleur contrôle des ressources des ordinateurs de bureau
- Dispositifs de sécurité plus rentables

RISQUES POUR LA SÉCURITÉ DANS LES SYSTÈMES INFORMATIQUES VIRTUELS

Bien qu'ils offrent de nombreux avantages, les systèmes informatiques virtuels ne sont pas exempts de risques ni complètement sécurisés. Les entreprises qui utilisent des systèmes informatiques virtuels doivent être attentives aux risques liés à la sécurité. « Comme dans les systèmes informatiques physiques, la plupart des vulnérabilités sont dues à des erreurs de configuration et de gestion. L'altération de la base de la virtualisation est le pire cas de figure qui puisse se produire. »¹ D'après Gartner, 60 % des serveurs virtualisés seront moins sécurisés que les serveurs physiques auxquels ils seront substitués d'ici à 2012.²

On identifie globalement trois types de risques pour la sécurité dans les systèmes informatiques virtuels :

1. **Vulnérabilité au niveau de l'architecture**—La couche d'abstraction existant entre le matériel physique et les systèmes virtualisés exécutant les services informatiques peut être la cible d'attaques potentielles. Le système d'exploitation invité étant exposé aux mêmes risques pour la sécurité qu'un système physique, des mesures de sécurité (p. ex., agents antivirus, protections contre les logiciels espions, gestion des identités) doivent être mises en œuvre sur toutes les machines virtuelles.

Les vulnérabilités au niveau de l'architecture peuvent être résolues comme décrit ci-dessous :

- Analyse des vulnérabilités—Les vulnérabilités au niveau de l'architecture peuvent être analysées en comparant les attributs actuels du système à un ensemble de critères de référence consistant en des exemples de systèmes valides et en notant les différences observées entre les deux ensembles d'attributs. La correction immédiate des différences permettra de renforcer la robustesse et la sécurité de l'architecture.
- Mises à jour régulières des fonctionnalités de sécurité sur les machines virtuelles—Toutes les mesures de sécurité doivent être tenues à jour.
- Gestion adéquate des correctifs sur les machines virtuelles—Les machines virtuelles doivent être correctement surveillées par le personnel informatique et les correctifs appropriés doivent être installés. Les correctifs adéquats doivent être régulièrement appliqués sur toutes les machines virtuelles, y compris celles qui sont en mode suspendu ou à l'arrêt.

– Mise en œuvre des meilleures pratiques en matière de réseau—Une machine virtuelle ou un groupe de machines virtuelles connectées à un réseau peuvent être la cible d’attaques réseau lancées à partir d’autres machines virtuelles connectées au même réseau. Les meilleures pratiques en matière de réseau doivent être respectées afin de durcir les interfaces réseau des machines virtuelles. Il est possible de procéder à la segmentation réseau des machines virtuelles afin de réduire les risques de divers types d’attaques réseau. Les zones de confiance peuvent être séparées à l’aide de périphériques de sécurité physiques.

2. Vulnérabilité logicielle—Le logiciel le plus important d’un système informatique virtuel est l’hyperviseur. Toute défaillance de la sécurité dans ce logiciel expose les machines virtuelles à des risques de pannes.

Les précautions suivantes sont indispensables pour éviter les vulnérabilités logicielles :

- Prévention d’un point de défaillance unique—L’attribut omniprésent de l’hyperviseur sur tous les hôtes virtuels posera problème si un code malicieux venait à compromettre une instance de l’hyperviseur. Une seule instance d’un logiciel malveillant capable de se répliquer peut rapidement exploiter tous les hyperviseurs installés dans l’environnement informatique réseau, générant alors un point de défaillance unique.
- Mises à jour de l’hyperviseur—Le logiciel de l’hyperviseur doit être régulièrement mis à jour avec les correctifs disponibles afin d’éliminer les défaillances de sécurité.
- Accès contrôlé aux machines virtuelles—Les droits d’accès privilégié doivent être convenablement verrouillés et l’accès contrôlé aux environnements virtuels doit être garanti pour réduire les risques d’exploitation du code par le biais de logiciels malveillants.
- Sécurité du système d’exploitation hôte—La couche de virtualisation résidant sur le système d’exploitation hôte, il convient de faire preuve d’une vigilance optimale pour protéger le système d’exploitation hôte contre les attaques de virus.
- Politique d’entreprise pour la sécurité des machines virtuelles—Un modèle de sécurité basé sur des politiques doit être appliqué aux hyperviseurs et au système d’exploitation hôte au niveau de l’entreprise.

3. Risques liés à la configuration—Du fait de la facilité de clonage et de copie des images, une nouvelle infrastructure peut être déployée en toute simplicité dans un environnement virtuel. Cela induit une dérive de la configuration ; en conséquence, le contrôle et la responsabilité du déploiement rapide d’environnements sont des tâches critiques.

Les étapes suivantes permettent de réduire les risques liés à la configuration :

- Évaluation de la configuration—Il convient d’évaluer régulièrement la configuration pour s’assurer d’un environnement virtuel connu et de confiance.
- Contrôles de la configuration de l’hyperviseur—L’intégrité de la configuration de l’hyperviseur doit être régulièrement vérifiée afin de réduire les risques et d’améliorer l’efficacité opérationnelle du système informatique virtuel.
- Autorisation et documentation appropriée des changements—Des changements peuvent être apportés instantanément aux machines virtuelles selon les besoins, mais tous doivent être autorisés et correctement documentés. Les changements de la configuration des machines virtuelles non détectés et non autorisés peuvent entraîner des failles de sécurité et rendre le système non conforme aux normes imposées par l’entreprise et les réglementations.
- Audit et contrôle de la configuration—La mise en œuvre d’une solution d’audit et de contrôle de la configuration appropriée sur les machines virtuelles peut contribuer à garantir la stabilité de l’environnement et la prévention des risques imprévus qui peuvent menacer le système informatique virtuel et l’entreprise. Il est possible de réduire les risques liés à la configuration en vérifiant régulièrement la configuration des composants par rapport aux normes définies.
- Modèles approuvés du déploiement de machines virtuelles—On doit disposer de modèles pour déployer les machines virtuelles et étudier toutes les modifications apportées aux normes et les approuver préalablement à leur mise en œuvre.
- Surveillance des événements—Tous les événements qui se produisent sur les machines virtuelles doivent être suivis à l’aide des journaux des hôtes serveur. Les modifications apportées à la configuration des hôtes, des machines virtuelles, des grappes (cluster), des groupes de ressources, des entrepôts de données et des réseaux virtuels doivent être contrôlées à l’état actif.
- Base de données de gestion des configurations (CMDB)—La description correcte de l’infrastructure doit être tenue à jour dans une base de données CMDB. Cette dernière doit contenir les informations concernant l’emplacement des images des machines virtuelles suspendues et le mappage de l’environnement physique sur l’environnement virtuel.

SÉCURITÉ DES SYSTÈMES INFORMATIQUES VIRTUELS— RESPONSABILITÉ DE ORGANISATIONNELLE

Il relève de la responsabilité de l'entreprise de définir les politiques et les procédures relatives aux systèmes informatiques virtuels. Lors de la définition du processus de déploiement de machines virtuelles, les responsables informatiques doivent travailler en collaboration avec les dirigeants de l'entreprise pour identifier les étapes et le calendrier de ces déploiements. En comparant les configurations du système à une politique de sécurité bien définie, reposant sur les critères de référence proposés par le Center for Internet Security (CIS) et l'agence américaine DISA (Defense Information Systems Agency (DISA)), l'équipe informatique peut avoir la certitude que les nouveaux déploiements seront conformes aux meilleures pratiques définies par l'entreprise. Veiller à ce que seuls les changements de la configuration approuvés soient mis en œuvre dans le cadre d'un processus bien conçu peut contribuer à réduire les risques liés aux changements dans un environnement virtuel.

Les rôles et les responsabilités dans un environnement informatique virtuel doivent être clairement définis et documentés. Même les administrateurs système ne doivent pas avoir plus de droits d'accès que nécessaire. La gestion correcte de la virtualisation requiert un processus de déploiement pour garantir que les nouvelles machines virtuelles respectent les normes définies par l'entreprise. Les politiques et les contrats de licence doivent être régulièrement mis à jour afin de veiller à leur conformité avec les réglementations en vigueur. Il relève de la responsabilité de l'entreprise de former son personnel à la technologie de virtualisation et aux fonctions de sécurité des systèmes informatiques virtuels.

Des politiques de protection des données doivent être définies au niveau de l'entreprise pour la récupération des informations importantes et des systèmes informatiques virtuels. Des politiques de sauvegarde et de récupération en cas de sinistre doivent être clairement définies et doivent indiquer des facteurs critiques, tels que la perte de données et les délais d'immobilisation acceptables ainsi que les sauvegardes au niveau des invités et des hôtes. En cas de compromission de l'ordinateur hôte, toutes les machines virtuelles peuvent devenir directement accessibles sur le serveur. Un intrus peut alors reconfigurer, déplacer et copier des machines virtuelles, exposant ainsi des données sensibles à des risques. Si un logiciel malveillant venait à pénétrer dans la couche de virtualisation, il aurait alors accès à toutes les machines virtuelles présentes sur l'ordinateur hôte, y compris les machines virtuelles de production, augmentant ainsi les risques pour la sécurité.

Les politiques de sécurité existantes du système informatique physique ne peuvent pas être copiées de manière aveugle pour l'environnement informatique virtuel.

Vous avez trouvé cet article intéressant ?

- Reportez-vous au Livre blanc de l'ISACA intitulé *Virtualization: Benefit and Challenges* (*Virtualisation : Avantages et difficultés*)

www.isaca.org/virtualization

- Participez à l'EuroCacs 2011, qui se tiendra du 20 au 23 mars à Manchester, en Angleterre (Royaume-Uni). Nous vous recommandons en particulier la session CL4 - « Security and Audit Issues for the Virtualization Environment » (Problèmes liés à la sécurité et l'audit dans l'environnement de virtualisation).

www.isaca.org/eurocacs2011

L'équipe technique doit collaborer avec l'équipe fonctionnelle pour mapper les politiques de sécurité existantes sur le système informatique virtuel. Un programme d'audit interne doit être développé spécifiquement pour le système informatique virtuel. Une gestion correcte des informations de sécurité doit être mise en place pour sécuriser le système virtualisé. Lors de l'élaboration des politiques de sécurité, une attention particulière doit être accordée à la sécurisation de la console de gestion ainsi que du système d'exploitation, des réseaux, du noyau, de la sauvegarde, des données et du déploiement des machines virtuelles, et du trafic sur les serveurs et le noyau des machines virtuelles. La direction doit donner des consignes concernant les mesures préventives et de détection par le biais de politiques de surveillance et d'audit bien définies et leur exécution assortie d'un suivi approprié.

AUDIT DES SYSTÈMES INFORMATIQUES VIRTUELS

Le fonctionnement des systèmes informatiques virtuels est différent de celui des systèmes à base de serveurs physiques. L'auditeur informatique doit connaître chaque aspect de la technologie des machines virtuelles et les risques associés à ces dernières. Pour réussir l'audit d'un système informatique virtuel, l'auditeur en sécurité de l'information doit avoir une connaissance adéquate de l'infrastructure des machines virtuelles, des points d'accès, des ports utilisés et non utilisés, des contrôles intégrés ou superposés ainsi que des partitions des serveurs.

L'auditeur informatique doit évaluer le besoin métier et l'avantage réel pour l'entreprise de transférer son environnement physique vers un environnement virtuel. Les principes, les meilleures pratiques et l'approche mis en œuvre pour l'audit d'un système informatique physique doivent être appliqués lors de l'audit de systèmes virtuels, auxquels s'ajoutent les points d'audit spécifiques à la technologie de virtualisation. Lors de l'audit d'un système informatique virtuel, l'auditeur

de la sécurité des informations doit évaluer les mesures de précaution mises en place par rapport à la connaissance du contexte et en valider la pertinence. Les politiques de sécurité être exemptes de tout défaut et doivent avec les procédures s'appuyer sur des procédures d'authentification, d'autorisation et de responsabilisation adéquates, afin de réduire les risques liés à un système informatique virtuel. L'entreprise doit mettre en place des contrôles d'accès physiques et logiques et l'auditeur doit vérifier la validité de tous les contrôles.

La console de gestion doit être sécurisée par des contrôles d'accès stricts et autorisée seulement à des utilisateurs spécifiques. Les contrôles d'accès logiques, tels que la sécurité des applications et la séparation des tâches, doivent être appliqués à tous les niveaux d'utilisateurs.

L'auditeur en sécurité de l'information doit évaluer le processus de création, de déploiement et de gestion des changements des machines virtuelles. La sécurité de l'hyperviseur étant primordiale, l'auditeur doit évaluer toutes les mesures de sécurité que lui applique l'entreprise. Il convient de prendre en compte l'état des machines virtuelles. Dans la mesure où elles peuvent avoir trois états, à savoir en marche, à l'arrêt ou suspendu, l'auditeur doit vérifier la moindre négligence en matière de sécurité sur les machines virtuelles qui sont à l'arrêt ou suspendues. L'auditeur doit également passer en revue les normes de configuration virtuelle et les procédures de contrôle de la configuration adoptées par l'entreprise pour la maintenance des systèmes virtuels. Tout écart par rapport aux normes et aux procédures de contrôle doit être considéré comme une défaillance matérielle et doit être signalé à la direction en vue de sa correction.

Une entreprise qui repose sur un système informatique virtuel doit disposer d'un système d'assistance adéquat en cas de sinistre ou de panne des serveurs de production. L'auditeur doit vérifier le plan de reprise après sinistre du système informatique virtuel et doit en évaluer les résultats des tests. Il doit également déterminer la suffisance des contrôles existants, par exemple les pare-feu, les systèmes de détection et de prévention d'intrusion, et la sécurité des ports réseau, afin que le système virtuel ne soit pas la proie d'attaques malveillantes externes. L'auditeur en sécurité de l'information doit connaître les meilleures pratiques régissant les machines virtuelles, en particulier les critères de référence proposés par le CIS et la DISA. Sur la base des aspects uniques de la technologie des machines virtuelles, l'auditeur de la sécurité des informations doit recueillir la preuve et la garantie des contrôles du système informatique virtuel.

POINTS D'AUDIT RELATIFS À LA SÉCURITÉ DES SYSTÈMES INFORMATIQUES VIRTUELS

Cette section propose un guide d'audit des systèmes informatiques virtuels qui peut servir de référence. Ce guide indique les points d'audit les plus significatifs pour les systèmes informatiques virtuels, comme souligné par les critères de référence et les meilleures pratiques proposés par le CIS, la DISA et VMware, fournisseur de produits de virtualisation.

Objectif du transfert d'un environnement physique vers un environnement virtuel

1. Y a-t-il une nécessité pour l'entreprise de passer d'un environnement physique à un environnement virtuel ?
2. Le système informatique virtuel a-t-il un impact sur la norme PCI DSS (Payment Card Industry Data Security Standard) et d'autres exigences réglementaires ?
3. La virtualisation permet-elle à l'entreprise d'atteindre ses objectifs ?

Évaluation des risques

4. Dispose-t-on du savoir-faire nécessaire pour prendre en charge le nouvel environnement ?
5. L'équipe qui doit utiliser et gérer l'environnement virtuel a-t-elle été correctement formée ?
6. Les procédures opérationnelles sont-elles régulièrement mises à jour ?
7. Y a-t-il un point de défaillance unique ?
8. Les zones de sécurité sont-elles séparées ou regroupées ?
9. Comment les ressources informatiques sont-elles séparées et regroupées dans l'environnement des machines virtuelles ?
10. Comment la sécurité de l'environnement des machines virtuelles est-elle gérée ?
11. La machine hôte est-elle accessible aux administrateurs ?
12. La console de gestion fait-elle l'objet de contrôles d'accès stricts et est-elle verrouillée pour des utilisateurs, des machines ou des partitions spécifiques ?

Compréhension de l'infrastructure et des contrôles

13. Les partitions exécutent-elles différents systèmes d'exploitation ?
14. Les partitions résident-elles sur un serveur unique ou sur plusieurs serveurs ?
15. Quelles sont les partitions existantes - pour quels environnements, dans quels boîtiers (c.-à-d. plan de réseau) ?
16. Chaque partition comprend-elle des contrôles similaires à ceux attendus pour un serveur ?
17. Est-ce que des contrôles s'appliquent à des utilisateurs spécifiques pour limiter leur accès ou leurs capacités de lecture/écriture ?
18. Est-ce qu'une convention de dénomination standard régit les noms de serveur, de partition et de bibliothèque/dossier ?
19. Quels sont les contrôles en place pour le déploiement de plusieurs copies d'un logiciel ?

Plan de réseau de l'environnement des machines virtuelles

20. Où se trouvent les types de systèmes suivants ?
 - Développement de systèmes
 - Test des systèmes
 - Systèmes de production
 - Serveurs des unités métier
21. Les environnements virtuels sont-ils séparés par sensibilité ?

Évaluation des politiques, des procédures et de la documentation

22. Évaluer les normes préparées par l'entreprise pour l'administration système et de la sécurité des systèmes informatiques virtuels.
23. Évaluer la procédure de création, de déploiement, de gestion et de modification des machines virtuelles.
24. Évaluer les politiques de verrouillage et de renforcement.
25. Évaluer l'exhaustivité et l'exactitude de la documentation des machines virtuelles.

Évaluation des contrôles

26. Les documents de contrôle des modifications font-ils référence à la bonne partition sur le serveur correct ?
27. Évaluer les capacités de sauvegarde.
28. Évaluer les options de récupération en cas de sinistre.
29. Les licences logicielles sont-elles à jour ?
30. Évaluer les contrats et les options de licence des fournisseurs.
31. À quelle fréquence les audits de la sécurité sont-ils réalisés ?
32. Évaluer les solutions tierces utilisées pour améliorer la sécurité de l'environnement virtuel et leur compatibilité avec le système informatique virtuel.
33. Évaluer les normes de contrôle définies par l'entreprise pour les systèmes informatiques virtuels.
34. L'utilisation des ressources et l'affectation des coûts entre les applications d'une infrastructure partagée sont-elles appropriées ?
35. Y a-t-il une extension anarchique d'images/virtuelle en raison d'une mauvaise gestion du système ?
36. Le système comprend-il des images orphelines ?
37. La sécurité de l'hyperviseur est-elle assurée ?
38. Évaluer les politiques de gestion de la capacité et de continuité des activités des systèmes informatiques virtuels.
39. Évaluer l'infrastructure de gestion de la configuration existante pour déterminer l'évolutivité et l'efficacité du système informatique virtuel.
40. Évaluer la procédure de gestion des correctifs des machines virtuelles.
41. Des services tels que des horloges d'ordinateurs de bureau ou des économiseurs d'écran (téléchargés à partir de sources inconnues) sont-ils installés sur les machines virtuelles ?
42. Y a-t-il des logiciels dont l'entreprise n'a pas particulièrement besoin ?
43. Le système est-il verrouillé pour éliminer les services inutiles ?
44. Les pare-feu hôtes sont-ils capables de détecter les intrusions ?

45. Une procédure d'analyse régulière des logiciels malveillants est-elle en place ?
46. L'hôte physique est-il utilisé à d'autres fins ?
47. Dispose-t-on d'un contrôle de l'hôte physique avec un logiciel de détection d'intrusion en fonction de l'hôte, tel qu'un vérificateur de l'intégrité des fichiers ?
48. Dispose-t-on d'une création régulière d'une nouvelle image de l'hôte physique à l'aide d'un logiciel de clonage ?
49. La sécurité du système informatique virtuel présente-t-elle des défaillances ?
50. Quels contrôles compensatoires ont été appliqués pour le système informatique virtuel ?
51. Évaluer la procédure de déploiement appliquée pour les systèmes informatiques virtuels.
52. Évaluer les contrôles de gestion, opérationnels et techniques appliqués pour les systèmes informatiques virtuels, et déterminer la présence de failles éventuelles.
53. Les politiques et les procédures relatives aux systèmes informatiques virtuels sont-elles régulièrement mises à jour ?
54. Évaluer le matériel requis et prévoir l'augmentation de la puissance de traitement et de la mémoire de manière à couvrir les besoins supplémentaires de la plate-forme des machines virtuelles afin d'identifier les seuils limites des systèmes informatiques virtuels.
55. Évaluer les exigences des disques au démarrage de façon à ce que les machines virtuelles les plus critiques soient chargées en premier lieu.
56. Chaque machine virtuelle est-elle dotée d'un disque physique dédié ?
57. L'accès physique au matériel et au système d'exploitation hôtes est-il restreint, comme requis ?
58. Dispose-t-on d'une prévention des vols de fichiers à l'aide d'un support externe (p. ex. disquette, CD/DVDRW, clés USB, lecteurs flash) ?
59. Dispose-t-on d'une capture du trafic entrant ou sortant via les interfaces réseau ?
60. Dispose-t-on d'une sécurité d'accès aux salles où sont installées les machines physiques ?
61. Dispose-t-on d'un verrouillage des boîtiers abritant les disques durs pour empêcher le retrait de ces disques ?
62. Dispose-t-on d'un démarrage à partir de tout périphérique à l'exception du disque dur principal ?
63. Le système d'entrée/sortie de base (BIOS) est-il protégé par un mot de passe afin que l'option de démarrage choisie ne puisse pas être modifiée ?
64. Dispose-t-on d'un contrôle de tous les ports externes via la configuration des systèmes hôtes et invités ou des applications tierces ?
65. La protection du système d'exploitation de base est-elle durcie contre les défaillances de la sécurité ?
66. L'hôte n'a-t-il que le nombre de comptes nécessaire pour gérer les machines virtuelles ?

- 67. Une politique de gestion des mots de passe est-elle en place pour garantir la définition de mots de passe longs et difficiles à deviner, la modification fréquente des mots de passe et leur communication uniquement aux employés qui doivent accéder aux systèmes ?
- 68. L'hôte a-t-il des services accessibles via le réseau ?
- 69. Une politique d'authentification des services qui doivent être exécutés et désactivés, ou éliminés complètement, et des services et programmes superflus, est-elle en place ?
- 70. Les correctifs appropriés sont-ils régulièrement installés sur l'hôte ?
- 71. Les correctifs destinés à l'hôte sont-ils d'abord testés sur une machine de test non utilisée pour la production avant d'être appliqués aux systèmes de production ?
- 72. Les machines virtuelles sont-elles correctement configurées de sorte qu'aucune machine virtuelle unique ne puisse monopoliser les ressources du système ?

Sécurité du réseau

- 73. Dispose-t-on d'une installation d'un pare-feu sur les ports de service de la couche des machines virtuelles ?
- 74. Dispose-t-on d'une permission d'accès distant à l'hôte ou à l'hyperviseur ?
- 75. Une infrastructure administrative séparée physiquement est-elle employée pour les fonctions de gestion, par exemple la création de nouvelles machines virtuelles ou la modification d'images existantes ?

Chiffrement des communications

- 76. Dispose-t-on d'un chiffrement des données pour sécuriser les communications ?
- 77. L'entreprise utilise-t-elle les protocoles HTTPS (Secured Hypertext Transmission Protocol), TLS (Transport Layer Security) ou SSH (Secure Shell) ou les réseaux privés virtuels (VPN) cryptés pour la communication des invités avec les hôtes ou des périphériques de gestion avec les hôtes ?
- 78. Des mesures approuvées par la direction sont-elles en place pour empêcher les usurpations d'adresses source, le détournement de connexions et de chemins et les attaques de type « man-in-the-middle » (ou attaque de l'intercepteur) ?

Contrôles d'accès logiques

- 79. Dispose-t-on de contrôles d'accès logiques sur les serveurs de virtualisation ?

Services et configuration

- 80. Dispose-t-on pour les hôtes à ressources limitées, d'une exécution des tâches de priorité faible aux heures creuses ou lorsque le système est inactif ?
- 81. Les fonctions telles que les économiseurs d'écran et les défragmenteurs sont-elles désactivées sur les ordinateurs de bureau virtuels ?

Partage de fichiers entre l'hôte et les invités

- 82. Les environnements de machines virtuelles prennent-ils en charge le partage de fichiers entre l'hôte et les invités et, si c'est le cas, l'entreprise en a-t-elle réellement besoin ?

Synchronisation d'horloge

- 83. Y a-t-il une dérive d'horloge sur les machines virtuelles ?

Déconnexion des périphériques non utilisés

- 84. Tous les périphériques non utilisés sont-ils déconnectés de la machine virtuelle ?

Approches de gestion à distance

- 85. Les outils de gestion à distance sont-ils cryptés et authentifiés ?

Application de correctifs et vulnérabilités

- 86. Les correctifs de sécurité les plus récents ont-ils été appliqués aux systèmes d'exploitation invités et hôtes ?
- 87. Les correctifs sont-ils testés avant leur installation dans un environnement de production ?

Journaux

- 88. L'hôte est-il configuré pour consigner les modifications apportées aux machines virtuelles, notamment les opérations de copie, transfert ou suppression sur l'hôte ?

Sauvegardes

- 89. Une image de toutes les machines virtuelles est-elle sauvegardée ?
- 90. Le flux de données des sauvegardes est-il crypté pour éviter le vol des images de serveurs ?

Protection contre les modifications externes

- 91. L'hyperviseur est-il protégé contre les modifications non autorisées ?
- 92. La machine virtuelle est-elle protégée contre les modifications non autorisées ?

Déni de service (DoS, Denial of Service)

- 93. La prévention des attaques de type DoS est-elle prévue ?
- 94. Comment le trafic réseau sur une machine virtuelle est-il authentifié ?

Divers

- 95. Les signatures et les logiciels antivirus les plus récents sont-ils installés sur toutes les machines virtuelles à l'état suspendu ou à l'arrêt ?
- 96. Les mises à jour et les correctifs les plus récents pour les systèmes d'exploitation invités sont-ils installés sur toutes les machines virtuelles à l'état suspendu ou à l'arrêt ?
- 97. Toutes les permissions nécessaires sont-elles configurées dans les fichiers de configuration et les fichiers de disques virtuels pour toutes les machines virtuelles ?

98. L'intégralité du trafic réseau est-elle gérée sur un segment réseau ou un réseau local virtuel (VLAN) dédié ?
La console de service et les machines virtuelles sont-elles configurées sur des segments réseau ou des réseaux VLAN distincts ?
99. Tous les groupes de ports sont-ils configurés avec une étiquette réseau qui identifie la fonction de chaque groupe de ports ?
100. Tous les groupes de ports non utilisés ont-ils été supprimés ?
101. Des permissions sur les fichiers journaux ont-elles été configurées pour en interdire l'accès aux utilisateurs non autorisés ?
102. Tous les journaux sont-ils envoyés à un serveur Syslog ?
103. Des abonnements aux notifications de mise à jour, de correctifs et de sécurité du fournisseur des serveurs sont-ils régulièrement souscrits ?
104. Les mises à jour et les correctifs les plus récents de la version logicielle des serveurs ont-ils été installés ?
105. Toutes les mises à jour de serveurs sont-elles testées dans un environnement de développement avant d'être installées sur les serveurs de production ?
106. Toutes les machines virtuelles et les applications tierces utilisées sont-elles documentées ?
107. L'entreprise a-t-elle défini des procédures de sauvegarde et de récupération de tous les serveurs et machines virtuelles ?
108. Le plan de reprise après sinistre couvre-t-il tous les serveurs de machine virtuelle, les machines virtuelles proprement dites et les périphériques nécessaires associés au système ?
109. Les fichiers de sauvegarde sont-ils stockés sur une partition logique distincte afin que la restauration puisse être effectuée en cas de pannes matérielles sur les serveurs de production physiques ?
110. L'UC et la mémoire des machines virtuelles sont-elles configurées avec un temps de cycle UC minimum pour garantir la disponibilité des machines virtuelles ?
111. Dispose-t-on d'une notification de l'administrateur système de l'infrastructure de virtualisation si le taux d'utilisation de l'UC ou de la mémoire d'une machine virtuelle excédait 90 % ?
112. Seuls les utilisateurs autorisés ont-ils accès à des actions spécifiques sur la machine virtuelle, et les noms/profils de ces utilisateurs sont-ils correctement documentés pour pouvoir être consultés rapidement ?
113. L'administrateur peut-il modifier les attributs et les permissions par défaut de la machine virtuelle sans autorisation préalable ?
114. Un processus de gestion de configuration documenté est-il mis en œuvre pour tous les ajouts de machines virtuelles et les modifications et suppressions d'utilisateurs, de groupes, de rôles et de permissions ?
115. La configuration de base est-elle documentée pour tous les utilisateurs, groupes, permissions, rôles et machines virtuelles ?
116. Toutes les modifications apportées aux rôles, permissions, groupes et utilisateurs de machines virtuelles sont-elles journalisées en vue de leur examen/suivi ?
117. Tous les journaux de machines virtuelles sont-ils passés en revue quotidiennement en vue d'identifier les activités suspectes/anormales ?
118. Le serveur de machine virtuelle est-il configuré en mode de verrouillage pour désactiver tous les accès distants à la racine ?
119. Tous les documents relatifs à l'infrastructure de virtualisation sont-ils à jour ?
120. Tous les accès aux images des systèmes d'exploitation sont-ils restreints aux utilisateurs autorisés seulement ?
121. Tous les modèles maîtres sont-ils stockés sur une partition distincte ?
122. L'accès aux modèles maîtres est-il restreint aux utilisateurs autorisés seulement ?
123. Une politique d'identification et d'affectation des machines virtuelles au personnel approprié a-t-elle été mise en place ?
124. Les fonctions de presse-papiers (copier/coller) et de déplacement par glisser-déposer ont-elles été désactivées sur toutes les machines virtuelles ?
125. L'horloge de toutes les machines virtuelles a-t-elle été synchronisée par un serveur d'horloge faisant autorité ?
126. Y a-t-il un comité de contrôle des modifications chargé de documenter et d'approuver tous les changements de nom des machines virtuelles de production ?
127. Toutes les machines virtuelles de test et de développement sont-elles séparées de façon logique des machines virtuelles de production ?
128. Une politique restreignant la copie ou le partage des fichiers de machines virtuelles sur les réseaux et sur des supports amovibles a-t-elle été mise en place ?
129. Tous les transferts de machines virtuelles d'un serveur physique à un autre sont-ils régulièrement consignés dans les journaux ?
130. Tous les transferts de machines virtuelles vers des supports amovibles (p. ex., DVD, CD, clés USB) sont-ils documentés ?
131. Les machines virtuelles sont-elles retirées du site uniquement après approbation et documentation de l'opération ?
132. Toutes les machines virtuelles de production sont-elles conservées dans une zone dont l'accès est contrôlé ?
133. Les restaurations de machines virtuelles sont-elles effectuées uniquement lorsque ces dernières sont déconnectées du réseau ?
134. Les fichiers journaux des systèmes d'exploitation de toutes les machines virtuelles sont-ils enregistrés en vue de leur audit avant la moindre restauration de machine virtuelle ?

135. Une taille maximale est-elle définie pour tous les fichiers journaux de machines virtuelles (500 kilooctets [ko] est la limite recommandée) ?
136. Tous les fichiers journaux de machines virtuelles sont-ils archivés pendant une période d'un an au moins ?
137. Toutes les machines virtuelles sont-elles sauvegardées conformément à leur niveau MAC (Media Access Control) ?
138. Toutes les machines virtuelles sont-elles correctement enregistrées dans le système de gestion des vulnérabilités (VMS) ?
139. Toutes les exigences des machines virtuelles sont-elles documentées avant la création de ces machines dans l'environnement du serveur de virtualisation ?
140. Le matériel non utilisé sur les machines virtuelles est-il retiré ou désactivé ?
141. Le système d'exploitation hôte est-il compatible avec la sélection de systèmes d'exploitation invités de la machine virtuelle ?

CONCLUSION

Le rythme auquel les entreprises adoptent la technologie de la virtualisation peut susciter quelques préoccupations si des fonctions de sécurité robustes ne sont pas appliquées aux systèmes informatiques virtuels. Une étude réalisée par Gartner indique que d'ici 2012, près de 50 % des serveurs installés à travers le monde seront virtualisés.³ Pour améliorer la sécurité et la robustesse des environnements informatiques virtuels, il est impératif de bien maîtriser la technologie de la virtualisation, afin de pouvoir installer et auditer correctement ces systèmes. Des techniques d'audit élémentaires, associées au contrôle adéquat des aspects propres à la technologie de la virtualisation, peuvent aider à réduire les risques de sécurité associés aux systèmes informatiques virtuels. Le guide d'audit fourni facilitera l'identification et la résolution des vulnérabilités dans les systèmes informatiques virtuels, et contribueront à améliorer l'efficacité opérationnelle des machines virtuelles. Les entreprises pourront ainsi profiter des avantages qu'offre la technologie de la virtualisation.

RÉFÉRENCES

Baldwin, Adrian; Simon Shiu; Yolanta Beres; 'Auditing in Shared Virtualized Environments', HP Laboratories, USA, 2008, www.hpl.hp.com/techreports/2008/HPL-2008-4.html

Brenner, Bill; 'The Security Benefits and Risks of Virtualization', *SearchSecurity.com*, 27 February 2008, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1302706,00.html

Bruzzese, J. Peter; *The Essentials Series: Virtualization and Disaster Recovery*, Realtime Publishers, USA, 2009

The Center for Internet Security; 'Virtual Machine Security Guidelines Version 1.0', USA, 2007

Cobb, Michael; 'Will Using Virtualization Software Put an Enterprise at Risk?', *SearchSecurity.com*, http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1248651,00.html

Desai, Anil; *The Definitive Guide to Virtual Platform Management*, Realtime Publishers, USA, 2009

Gartner; 'Gartner Says Virtualization Will Be the Highest-Impact Trend in Infrastructure and Operations Market Through 2012', USA, 2 April 2008, www.gartner.com/it/page.jsp?id=638207

Hewlett-Packard Development Company, 'Virtualization Solution Guide for Midsize Businesses', USA, June 2008

Hoelsing, Michael; 'Virtualization Usage, Risks and Audit Tools', JournalOnline, *ISACA Journal*, vol. 3, 2006, www.isaca.org/jonline

Kim, Gene; *Practical Steps to Mitigate Virtualization Security Risks*, Tripwire, USA 2008

Mann, Andi; '5 Key Virtualization Management Challenges—and How to Overcome Them', Enterprise Management Associates, 13 March 2009, www.enterprisemanagement.com/research/asset.php?id=1156

McLaughlin, Laurianne; 'How to Find and Fix 10 Real Security Threats on Your Virtual Servers', *CIO*, 14 November 2007, www.cio.com/article/154950/How_to_Find_and_Fix_Real_Security_Threats_on_Your_Virtual_Servers?source=artrel_top

Mukherjee, Soumen; Joy Mustafi; Abhik Chaudhuri; 'Grid Computing: The Future of Distributed Computing for High Performance Scientific and Business Applications', *Lecture Notes in Computer Science*, vol. 2571/2002, 2002

Norbeck, Don; 'Key Considerations for Leveraging Virtualization and Keeping Your Applications Available', *Virtual Strategy Magazine*, 30 July 2007, www.virtualstrategy.com/Features/Key-Considerations-for-Leveraging-Virtualization-and-Keeping-Your-Applications-Available.html

Ray, Edward; Eugene Schultz; 'Virtualization Security', Association for Computing Machinery (ACM) International Conference Proceeding Series, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, USA 2009

Rothman, Mike; 'Preparing for Virtualization Security Unknowns', SearchSecurity.com, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1254079,00.html

Singleton, Tommie W.; 'What Every IT Auditor Should Know About Auditing Virtual Machine Technology', *ISACA Journal*, vol. 6, 2008, www.isaca.org/archives

Shields, Greg; *The Essentials Series: Virtual Security Concerns & Solutions*, Realtime Publishers, USA, 2008

Shields, Greg; *The Shortcut Guide to Selecting the Right Virtualization Solution*, Realtime Publishers, USA, 2009

Shields, Greg; *The Shortcut Guide to Virtualization and Service Automation*, Realtime Publishers, USA, 2009

Small, Mike; 'Security in a Virtual IT World', *ITP.net*, 21 December 2008, www.itp.net/news/541434-security-in-a-virtual-it-world

Tripwire, 'Secure Virtualization: Achieve and Maintain IT Security in Virtual Environments', white paper, 1 July 2009

US Defense Information Systems Agency (DISA) for the US Department of Defense (DoD); 'ESX Server Security Technical Implementation Guide, Version 1, Release 1', USA, 28 April 2008

VMware, www.vmware.com/virtualization

Westervelt Robert; 'Virtualization Experts Debate Security of Thin, Robust Hypervisors', *SearchSecurity.com*, 23 April 2009, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1354642,00.html

NOTES DE BAS DE PAGE

¹ SANS, www.sans.org/thought-leaders/kim_thought_leader

² Gartner Inc., 'Gartner Says 60 percent of Virtualized Servers...', press release, March 2010

³ Baker, Adrienne; 'Gartner: Top Virtualization Security Risks and How to Combat Them', *Information Management*, www.information-management.com/news/virtualization_security_risks-10017445-1.html