

Sécuriser l'administration de la virtualisation

Rapport d'étude de marché rédigé par ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
Préparé pour RSA, la division Sécurité d'EMC,

mars 2010



RECHERCHE EN GESTION INFORMATIQUE,
ANALYSE ET CONSEILS SECTORIELS

Sommaire

Résumé analytique.....	3
Administration sécurisée : la priorité pour la sécurité de la virtualisation.....	3
Gestion de la consolidation des ressources	4
Contrôle de l'exposition aux risques	4
Le terme « instantané » prend un autre sens.....	4
Les images de machines virtuelles sont aussi des données.....	5
L'impact de l'administration.....	5
Relever le défi.....	5
Commencer par une stratégie	5
Planifier : conception d'une configuration appropriée	6
Exécuter : sécurité administrative des opérations.....	7
Vérifier : contrôle des actions administratives.....	7
Agir : importance critique de la réponse	9
Vers l'avenir.....	10
Point de vue d'EMA	10
À propos de RSA	12

Résumé analytique

La virtualisation est l'une des technologies de l'information les plus révolutionnaires de ces dernières années. Ce que de nombreuses entreprises ne mesurent pas encore tout à fait cependant, c'est l'impact considérable que la virtualisation exerce également sur la sécurité. Avec la virtualisation, les investissements informatiques génèrent des bénéfices optimaux avec une plus grande flexibilité. Mais elle introduit également de nouveaux risques, dont la plupart sont sans précédent dans le domaine de l'informatique traditionnelle.

Contrairement aux systèmes physiques, plusieurs machines virtuelles invitées partagent un même hôte. Les machines virtuelles peuvent être configurées hors ligne et déployées à la demande, créant un environnement bien plus dynamique. Une fonctionnalité virtualisée telle que la mise en réseau fait abstraction de sa topologie physique.

La sécurisation de ces fonctionnalités dépend directement du contrôle administratif. Il en résulte un besoin de sécurité accru en matière d'administration de la virtualisation et les processus et technologies destinés à la sécurisation de l'administration doivent être « orientés virtualisation ».

Dans ce rapport, Enterprise Management Associates (EMA) décrit une approche systématique de la sécurisation de l'administration des systèmes virtualisés, en se basant sur la philosophie « Planifier, faire, vérifier, agir » reprise dans la série de normes ISO 27000. Alors que l'on assiste aux prémices de la virtualisation des points d'accès, tous les regards sont tournés vers l'administration de la virtualisation dans le datacenter, qui est au centre des préoccupations actuelles.

Des directives sur la sécurisation des opérations d'administration liées aux systèmes VMware, systèmes particulièrement renommés en matière de virtualisation, et sur l'utilisation des outils et technologies d'EMC et de sa division Sécurité, RSA, sont mises en avant pour vous aider. Les lecteurs doivent prendre conscience des fonctionnalités indispensables à une administration sécurisée de la virtualisation, en s'appuyant notamment sur les conseils prodigués, par exemple, dans les publications *Security Hardening* proposées par VMware.

Administration sécurisée : la priorité pour la sécurité de la virtualisation

Chaque génération informatique offre des technologies révolutionnaires, mais très peu d'entre elles ont égalé l'impact de la virtualisation sur les datacenters. La valeur qu'elle génère en matière de consolidation des ressources, de provisionnement à la demande et de maintenance hors ligne permet d'apporter aux systèmes informatiques une plus grande flexibilité. Ils sont ainsi mieux adaptés aux besoins des entreprises.

Néanmoins, il est *impossible* d'obtenir une parfaite adéquation entre les systèmes proposés et les besoins des entreprises tant que les risques induits par la virtualisation ne sont pas compris et maîtrisés. Certains de ces risques sont sans précédent ou presque dans les environnements physiques.

Avec la virtualisation, les investissements informatiques génèrent des bénéfices optimaux avec une plus grande flexibilité. Mais elle introduit également de nouveaux risques, dont la plupart sont sans précédent dans le domaine de l'informatique traditionnelle.

Gestion de la consolidation des ressources

Par exemple, les systèmes invités virtualisés partageant une plate-forme physique commune peuvent présenter différents niveaux de sensibilité en termes d'opérations, d'exposition de leur réseau ou d'informations gérées. Une machine virtuelle invitée exposée à un réseau public peut courir le risque d'exposer des données sensibles gérées par un autre invité sur le même hôte.

Dans le passé, les interactions aussi risquées étaient essentiellement contrôlées via une isolation physique ou logique. Cependant, dans le cadre de la virtualisation, les risques de violation de l'isolation sont accrus du fait de la consolidation des fonctionnalités sur un hôte partagé. Certains gros détaillants n'ont pas validé leur conformité aux normes de sécurité des données PCI (Payment Card Industry) à cause de tels problèmes.

Contrôle de l'exposition aux risques

Même de simples modifications de la configuration d'un serveur ou de la topologie d'un réseau peuvent révéler des faiblesses, comme un défaut logiciel non corrigé ou un accès réseau susceptible d'engendrer une prise de contrôle du système. La virtualisation quant à elle, a le potentiel d'amplifier considérablement cette exposition, lorsqu'une configuration de machine virtuelle est répliquée à maintes reprises en environnement de production.

La possibilité de déplacer et déployer des systèmes virtuels à la demande peut également accroître les risques. Les entreprises supposent qu'un certain nombre de serveurs doivent être gérés. Mais la virtualisation à la demande peut faire augmenter ce nombre significativement si elle n'est pas contrôlée. La « prolifération » due à la virtualisation a une incidence importante à plusieurs niveaux :

- Elle accroît le volume des expositions aux risques (ou « surface d'attaque ») si des mesures de sécurité appropriées et cohérentes ne sont pas appliquées à l'ensemble de l'environnement virtuel.
- Elle expose l'entreprise à des violations de licences logicielles.
- Elle peut introduire des violations de conformité relatives à la gestion des données privées, à la séparation des systèmes et réseaux, à une journalisation adéquate et à un contrôle des ressources et des modifications.

Le terme « instantané » prend un autre sens

Contrairement aux environnements physiques, où les modifications prennent effet immédiatement, les modifications apportées à une machine virtuelle sont habituellement effectuées hors ligne et ne sont effectives qu'après le déploiement de l'image en production. Un certain délai peut donc s'écouler avant l'application des modifications, une fois que celles-ci ont été définies dans l'image principale ou la configuration de service d'une machine virtuelle. Si les modifications sont effectuées pour des raisons de sécurité, une telle latence est susceptible de prolonger l'exposition aux risques.

Un autre facteur d'instantanéité spécifique de la virtualisation est la possibilité de suspendre une machine virtuelle. Le démarrage et l'arrêt d'un service peuvent être journalisés en tant qu'événement au niveau du système. Cependant, sans visibilité dans l'infrastructure de virtualisation, la suspension de la machine virtuelle peut passer inaperçue avec les méthodes de surveillance traditionnelles. Il en résulte un risque accru d'observer un dysfonctionnement, voire la déconnexion des fonctionnalités critiques, du fait de problèmes de sécurité non détectés.

Les images de machines virtuelles sont aussi des données

Une image de machine virtuelle est effectivement constituée d'un fichier ou d'un ensemble de fichiers stockés sous forme de données. Ces données peuvent être copiées puis exécutées ultérieurement dans un environnement non contrôlé, contournant ainsi les protections autorisées. Il est donc essentiel de contrôler en priorité l'accès aux systèmes de stockage gérant de telles données.

L'impact de l'administration

Notez le rôle essentiel que jouent l'administration et la gestion dans chacun de ces exemples. Un privilège d'administration permet de définir des images de machines virtuelles, de récupérer des images de machines virtuelles stockées sous forme de données, de contrôler leur déploiement et gestion en production. Cela augmente le besoin de sécuriser les actions et privilèges d'administration.

Ces facteurs augmentent le besoin de sécuriser les actions et privilèges d'administration. Ils soulignent également l'importance des contrôles orientés virtualisation.

Cela souligne également l'importance des contrôles orientés virtualisation. Une visibilité de l'infrastructure virtuelle est également nécessaire pour détecter des facteurs tels que la consolidation, le déplacement et la suspension de machines virtuelles, ainsi que le contrôle des images de machines virtuelles en tant que données. Sans cette visibilité, les tâches administratives présentant des risques pourraient passer inaperçues. Sans contrôles spécifiques de la virtualisation, elles pourraient également ne pas être gérées.

Relever le défi

La sécurisation de l'administration de la virtualisation doit donc devenir la priorité principale pour la sécurité de la virtualisation elle-même. Cependant, les entreprises ne sont pas nécessairement au fait des meilleures méthodes de sécurisation des privilèges de gestion et d'administration de la virtualisation. Cela demande une prise en compte de tous les facteurs impliqués afin de développer un plan d'action efficace.

Commencer par une stratégie

En d'autres termes, cela implique l'adoption d'une approche stratégique, correspondant aux exigences de l'entreprise. Une telle approche est reflétée dans la série de normes ISO 27000 sur la gestion de la sécurité, souvent citées comme directives à respecter dans le domaine de la gestion de la sécurité informatique. Les normes ISO recommandent essentiellement d'adopter une approche systématique, qui décrit une séquence logique permettant aux entreprises de définir, mettre en oeuvre et contrôler leurs objectifs, en mettant l'accent sur l'action. Cette approche est fréquemment synthétisée ainsi :

Cela implique l'adoption d'une approche stratégique correspondant aux exigences de l'entreprise.

Planifier, exécuter, vérifier, agir

Les normes ISO représentent un ensemble de directives pouvant être appliquées au cas général. Les directives spécifiques des technologies utilisées doivent être consultées pour sécuriser la mise en oeuvre en elle-même. Les organismes tels que le Computer Security Institute (CSI) proposent de telles directives, mais les fournisseurs proposent également leurs propres directives, dans la plupart des cas. VMware, par exemple, propose des directives sur le *renforcement de la sécurité*, appliquées aux technologies de virtualisation VMware¹. Ces documents contiennent des informations utiles sur la sécurisation de l'administration des environnements virtualisés.

¹ http://www.vmware.com/pdf/vi3_security_hardening_wp.pdf (mars 2010)

Planifier : conception d'une configuration appropriée

La préservation du contrôle administratif constitue un objectif implicite en vertu des principes de sécurité fondamentaux qui s'appliquent à la fois dans les environnements virtuels et dans les environnements physiques. La sécurisation de l'administration de la virtualisation commence donc par la sécurisation de l'environnement physique et l'extension de ces principes à la virtualisation.

- Limiter les expositions pouvant mener à un accès non autorisé via des privilèges élevés.
- Installer les outils de sécurité habituels tels que des systèmes anti-programmes malveillants, de pare-feu et de prévention des intrusions au niveau de l'hôte.
- Désactiver les fonctions inutiles ou superflues.
- Réserver des ressources système aux processus de gestion des services : gestion des correctifs, des modifications, des ressources et de configuration.
- Les configurations sécurisées doivent être conçues dans des modèles renforcés, afin de s'assurer que lors du déploiement de nouveaux systèmes, ces derniers sont configurés correctement. Cela comprend la configuration de l'hôte physique, de l'hyperviseur et de chaque machine virtuelle invitée.

La segmentation réseau implique une dimension supplémentaire dans les environnements virtualisés puisque les machines virtuelles invitées possèdent chacune leurs propres connexions : aux topologies de réseaux physiques et logiques en dehors de l'hôte virtualisé ainsi que dans l'hôte lui-même.

- Dans la plupart des cas, les communications réseau entre les machines virtuelles invitées doivent être isolées. Les technologies telles que VMware vShield Zones peuvent limiter le trafic inter-machines virtuelles ainsi que les expositions aux risques qui en résultent, étendant les principes éprouvés de la segmentation réseau au monde virtuel.
- La connexion à des interfaces physiques spécifiques peut renforcer cette isolation protectrice et atténuer les risques relatifs aux configurations logicielles.

La configuration des systèmes de gestion de la virtualisation est particulièrement importante puisque ces derniers exercent un contrôle direct sur les fonctionnalités. VMware vCenter propose par exemple l'administration centralisée d'environnements VMware et doit donc être déployé avec précaution.

- Limiter l'accès administratif à l'hôte sur lequel vCenter s'exécute. vCenter lui-même doit s'exécuter sous un compte d'administrateur distinct, fourni spécialement à cette fin.
- Les réseaux de gestion et de production doivent être isolés les uns des autres afin de limiter le risque d'accès non autorisé aux fonctionnalités d'administration.

Lorsqu'un accès administratif est autorisé, le principe des privilèges minimaux doit s'appliquer.

- Autant que possible, l'accès administratif doit être lié à des comptes individuels. L'accès à des comptes d'administrateurs partagés, par exemple un compte racine, doit être restreint, de même que l'utilisation d'outils tels que « su » doit être limitée.

- Le contrôle d'accès basé sur les rôles (RBAC) permet de diviser les fonctions d'administration en rôles individuels pouvant être invoqués par des utilisateurs autorisés si nécessaire. Grâce à la possibilité de créer des rôles personnalisés, VMware vCenter constitue une solution intégrée de définition et de division des privilèges d'administration par rôles.

Le contrôle de l'environnement est essentiel, en particulier en ce qui concerne la surveillance des actions et de l'accès administratifs, autorisés ou non. Les entreprises doivent prévoir de déployer des outils de gestion des événements permettant une visibilité des risques inhérents à la virtualisation. Dans cette optique, il convient de contrôler l'accès aux ressources de stockage des images de machines virtuelles.

- De même, la division en rôles par RBAC doit permettre de garantir que les personnes disposant de droits d'accès d'administrateur ne peuvent pas altérer les preuves des actions d'administration effectuées.

Exécuter : sécurité administrative des opérations

Après le déploiement de la virtualisation, il convient de veiller au maintien des principes d'exposition limitée et de privilèges minimaux dans le cadre de la gestion des opérations. Pour ce faire, il est possible de s'appuyer sur les outils de gestion ultrasécurisés ou ultraciblés disponibles.

- Dans l'environnement VMware, ESX Service Console peut donner accès à de nombreuses fonctionnalités avec un contrôle limité. Un meilleur niveau de contrôle peut être atteint via des outils plus précis basés sur les fonctionnalités de vCenter, comme PowerCLI et les kits d'outils contenant l'API vSphere.
- Ces outils tirent le meilleur parti de vCenter : ils appliquent un contrôle et une surveillance centralisés des privilèges. Ils fournissent également un accès administratif basé sur des rôles grâce aux rôles personnalisés de vCenter.
- Le recours à une authentification forte peut également renforcer la sécurisation de l'accès aux privilèges d'administration. Certaines exigences de conformité telles que les normes de sécurité des données PCI nécessitent spécifiquement une authentification à deux facteurs pour un accès administratif à distance. L'un des exemples les plus répandus d'authentification à deux facteurs est la technologie de mot de passe unique de RSA SecurID, longtemps utilisée pour sécuriser l'accès administratif dans de nombreuses entreprises, à travers le monde entier.

Après le déploiement de virtualisation, les principes de l'exposition limitée et des privilèges minimum doivent continuer d'être suivis pour la gestion des opérations.

Vérifier : contrôle des actions administratives

La mise en place d'une fonctionnalité de surveillance lors de la phase de planification est essentielle, mais elle doit être utilisée efficacement pendant le déroulement des opérations. Dans le rapport de recherche² sur la violation de données rédigé par Verizon Business en 2009, 66 % des victimes étaient en possession de preuves suffisantes dans leurs journaux pour découvrir une faille. Encore aurait-il fallu qu'ils soient plus attentifs à leurs analyses. Le volume d'informations de surveillance généré constitue pour beaucoup la source du problème. Cette masse de données est difficile, voire impossible, à gérer sans les outils destinés à classer les alertes signalant les risques importants par ordre de priorité.

² W. H. Baker et al, 2009 *Data Breach Investigations Report*, Verizon Business, Avril 2009.

Le recours aux systèmes de gestion des informations et événements de sécurité (SIEM) constitue la solution de choix pour relever ces défis. Cependant, afin de gagner en efficacité en termes de contrôle de l'administration de la virtualisation, ces systèmes doivent bénéficier d'une visibilité complète sur les différents événements :

- **Événements de tout type d'environnement** : la surveillance doit recouvrir des événements non spécifiques de la virtualisation, mais qui ont une incidence sur la gestion de la sécurité de cette dernière. Exemple :
 - Les événements doivent être corrélés avec les modifications informatiques. La surveillance des modifications informatiques est un principe fondamental de la gestion informatique qui renforce le contrôle des modifications et améliore la fiabilité informatique. En termes de sécurité, la détection des modifications peut révéler des menaces.
 - Les événements doivent être corrélés avec l'accès administratif. Cela peut permettre d'identifier les accès administratifs non autorisés ou les attaques de sécurité exploitant des privilèges d'administration. Il en résulte également une gestion informatique plus fiable, puisque les causes premières des problèmes de performances ou de disponibilité découlant d'actions d'administration sont plus faciles à identifier.
 - L'accès aux ressources de stockage contenant les images de machines virtuelles doit être surveillé afin d'être protégé contre le déploiement et l'analyse de systèmes virtuels non autorisés.
- **Événements spécifiques de la virtualisation** : les outils d'analyse doivent également bénéficier d'une visibilité sur les activités d'administration spécifiques de la virtualisation. Cela est particulièrement critique lorsque ces événements n'ont pas d'équivalent ou peu dans un environnement physique :
 - Les actions d'administration entraînant des modifications de l'état de la machine virtuelle doivent être surveillées. L'arrêt et le démarrage d'un service sur un serveur physique peuvent être détectés par des outils conventionnels, mais ce n'est pas le cas des problèmes spécifiques de la virtualisation tels que l'interruption des machines virtuelles. Les machines virtuelles peuvent également être déplacées d'un hôte physique à un autre, ce qui peut constituer une violation des règles. Les outils d'analyse doivent bénéficier d'une visibilité sur l'infrastructure de virtualisation dans ces cas précis.
 - Dans la plupart des cas, apporter des modifications à la configuration d'une machine virtuelle requiert de la mettre hors ligne et de monter son image à nouveau, opération qui n'est pas aussi intuitive que le redémarrage d'un serveur physique. Lorsque des modifications sont définies dans les images principales des machines virtuelles, l'analyse doit garantir leur mise en production opportune. Cette opération peut être critique lors de la correction des failles de sécurité exploitées activement.

Les outils d'analyse doivent également bénéficier d'une visibilité sur les activités d'administration spécifiques de la virtualisation. Cela est particulièrement critique lorsque ces événements n'ont pas d'équivalent ou peu dans un environnement physique.

- Les tentatives non autorisées de copier ou de « cloner » les machines virtuelles doivent être détectées pour que les informations ou systèmes sensibles ne soient pas exposés hors de l'environnement autorisé et contrôlé.
- La « prolifération » de la virtualisation doit être surveillée et maîtrisée afin de garantir la gestion correcte de la virtualisation, le contrôle adéquat des environnements réglementés et la réduction de l'exposition aux risques résultant du développement de la surface d'attaque.

Les plates-formes SIEM telles que RSA enVision® fournissent une visibilité complète des activités des environnements physiques aussi bien que virtualisés. Les familles d'outils de configuration et de gestion des modifications d'EMC et de VMware, tels que VMware vCenter Server Configuration Manager, proposent une configuration et une visibilité sur les modifications orientées virtualisation, ce qui peut être mis en corrélation avec l'analyse des événements. Ce sont des exemples de technologies bénéficiant d'une visibilité suffisante sur l'infrastructure de virtualisation pour garantir que les problèmes directement liés à la virtualisation ne soient pas négligés.

Agir : importance critique de la réponse

Surveiller est une chose, agir en est une autre, comme le suggèrent les recherches sur la violation de données. Même lorsque des systèmes de gestion des événements mettent en corrélation et identifient des problèmes prioritaires, des mesures doivent être prises, tout d'abord pour réagir au problème mais également pour empêcher qu'il ne se reproduise et mieux sécuriser la gestion de la virtualisation par la suite.

Surveiller est une chose, agir en est une autre, comme le suggèrent les recherches sur la violation de données.

Des principes généraux peuvent également être appliqués à tous les types d'environnement, même aux environnements spécifiques de la virtualisation :

- **Évaluer l'exhaustivité de la réponse.** Lorsque des failles de sécurité sont découvertes, l'exposition doit être localisée et confirmée dans d'autres environnements. Les systèmes de gestion de la configuration peuvent non seulement vérifier la présence de l'exposition lorsqu'elle survient, mais également la corriger directement via une modification de configuration.
- **Adopter une approche proactive.** Au-delà de la surveillance, la « vérification » doit également inclure l'évaluation régulière de l'efficacité des programmes. Cela permet de s'assurer que la virtualisation est gérée de manière responsable alors que les technologies, scénarios d'utilisation et exigences métiers évoluent. Les modifications impliquant systématiquement une exception aux processus de gestion en place, par exemple, peuvent amener à une réévaluation de ces processus.
- **Développer la sensibilisation à la virtualisation.** Il faut reconnaître que la virtualisation peut avoir une incidence importante sur les domaines de gestion existants, tels que la gestion de la configuration. L'environnement virtuel est beaucoup plus dynamique que les anciens systèmes. Les machines virtuelles peuvent se déplacer très librement entre plusieurs hôtes physiques. Les modifications peuvent être appliquées hors ligne, ce qui réduit l'incidence de ces dernières sur les environnements de production, mais les équipes techniques doivent s'assurer que ces modifications sont mises en production correctement.

Les entreprises souhaitent s'assurer que leurs outils d'administration bénéficient d'une visibilité correcte sur l'infrastructure de virtualisation, et ce afin d'éviter d'être désagréablement surprises par ces problèmes spécifiques de la virtualisation.

- **Relier l'infrastructure virtuelle à la gestion du service informatique.** Les systèmes de surveillance peuvent générer un ticket d'incident en réponse à des événements spécifiques. Cela permet de suivre les incidents et d'y donner une conclusion satisfaisante, impliquant notamment une analyse approfondie ou d'autres opérations de suivi si nécessaire. Inversement, un ticket d'incident peut être utilisé pour autoriser un événement de modification spécifique, dont le résultat, satisfaisant ou non, est répercuté dans les systèmes de surveillance.

Vers l'avenir

Enfin, la réponse doit tenir compte de l'évolution de la technologie, dans ce cas précis, de l'évolution constante de la virtualisation, de sa gestion et des risques inhérents à cette dernière.

Les technologies émergentes telles que Virtual Desktop Infrastructure (VDI) augmentent les besoins en matière d'outils de gestion de la sécurité « orientés virtualisation ». RSA enVision, par exemple, s'intègre avec VMware View afin de fournir des informations relatives à la connexion ou déconnexion d'un utilisateur, à la déconnexion des systèmes, au branchement de périphériques comme des périphériques USB, etc.

Ces fonctionnalités ne font pas simplement concurrence aux possibilités de nombreux environnements non virtualisés, elles les surpassent. Ce n'est qu'un exemple parmi d'autres, illustrant l'impact positif de la virtualisation du point d'accès sur la gestion de la sécurité au point d'accès. D'autres innovations qui renforceront certainement la sécurité de la virtualisation et par là même, la gestion des risques administratifs inhérents aux environnements virtuels, incluent l'adoption systématique des technologies VMsafe de VMware pour l'amélioration de la visibilité et du contrôle de la sécurité de la virtualisation.

Point de vue d'EMA

Afin de concrétiser la promesse faite par la virtualisation, les entreprises doivent gérer les risques qui y sont liés de manière fiable : cette gestion des risques est d'autant plus importante lorsqu'il s'agit de préserver l'administration de la virtualisation.

De par sa relation avec VMware, leader du marché dans le domaine des technologies de virtualisation, et grâce aux capacités de sa division Sécurité RSA, EMC se démarque de ses concurrents en offrant une solution répondant aux exigences de gestion d'une virtualisation responsable. Ses liens uniques avec VMware lui offrent une visibilité tout aussi unique dans les portefeuilles de virtualisation les plus efficaces du secteur, notamment les plates-formes de gestion orientées virtualisation de VMware. La famille RSA de ressources SIEM et une authentification forte fournissent des fonctions indispensables en termes de visibilité sur les actions à privilèges élevés et en termes de contrôles rigoureux de l'accès administratif. Parallèlement, les portefeuilles de gestion d'EMC et de VMware réunis offrent des fonctions de gestion de configuration essentielles pour garantir un contrôle sécurisé de la virtualisation, avec notamment la gestion du cycle de vie complet du stockage sécurisé des images de machines virtuelles pour préserver les fonctionnalités d'administration enregistrées dans la configuration de la machine virtuelle.

De par sa relation stratégique avec VMware, leader du marché dans le domaine des technologies de virtualisation, et appuyé par les capacités de sa division Sécurité RSA, EMC se démarque des autres fournisseurs en proposant une gestion responsable de la virtualisation.

L'alignement de ces fonctionnalités donne à EMC, RSA et VMware une compréhension caractéristique des relations virtuelles, entre hôtes et invités, dans les systèmes, réseaux, bases de données et applications virtualisés. La création d'objectifs d'intégration et de collaboration communs à ces groupes de fournisseurs qui se soutiennent mutuellement est tout aussi importante. Celle-ci permet d'identifier les facteurs tels que des points d'intégration spécifiques accélérant l'adoption et le déploiement de mesures de sécurité. Résultat : on observe une réduction des coûts globaux liés à la sécurisation de la gestion de la virtualisation. C'est la conjugaison de ces facteurs qui contribue à promouvoir EMC et VMware comme fournisseurs privilégiés de solutions garantissant une gestion sécurisée et responsable de la virtualisation. Grâce à ces deux acteurs, la virtualisation tient toutes ses promesses.

À propos de RSA

RSA, la division Sécurité d'EMC, est le premier fournisseur de solutions de sécurité pour les professionnels. En aidant les entreprises à relever leurs défis les plus complexes et les plus critiques en matière de sécurité, RSA contribue au succès des plus grandes sociétés leaders dans le monde. Grâce à son approche orientée informations, RSA protège l'intégrité et la confidentialité des données tout au long de leur cycle de vie, quels que soient leur évolution, les personnes qui y accèdent ou leur mode d'utilisation.

RSA offre les solutions les plus innovantes du marché dans les domaines suivants : sécurisation des identités et contrôle d'accès, prévention contre la perte de données, cryptage et [gestion des clés](#), conformité et gestion des informations de sécurité, protection contre la fraude. Ces solutions garantissent la sécurité nécessaire à des millions d'identités utilisateurs, à leurs transactions et aux données qu'ils génèrent. Pour plus d'informations, rendez-vous sur www.RSA.com et www.emc2.fr.

À propos d'Enterprise Management Associates, Inc.

Fondé en 1996, Enterprise Management Associates (EMA) est un cabinet d'analystes qui met un point d'honneur à délivrer des analyses rigoureuses et approfondies, l'objectif étant de fournir une visibilité maximale sur la gamme complète des technologies de gestion informatique. Les analystes d'EMA utilisent une combinaison unique d'expérience pratique, de perception des meilleures pratiques du secteur et de connaissances approfondies des solutions actuelles et en projet pour aider leurs clients à atteindre leurs objectifs. Pour en savoir plus sur les services de recherche, d'analyse et de conseil d'EMA, destinés aux professionnels de l'informatique d'entreprise et aux fournisseurs informatiques, consultez le site www.enterprisemanagement.com ou suivez [EMA sur Twitter](#).

Ce rapport ne peut être copié, reproduit, stocké dans un système de récupération ou transmis, en totalité ou en partie, sans l'autorisation écrite d'Enterprise Management Associates, Inc. Toutes les opinions et estimations contenues dans ce rapport représentent notre jugement à cette date et sont sujettes à modification sans avertissement préalable. Les noms de produits mentionnés dans ce rapport peuvent être des marques commerciales et/ou des marques déposées de leurs détenteurs respectifs. « EMA » et « Enterprise Management Associates » sont des marques commerciales d'Enterprise Management Associates, Inc. aux États-Unis et dans d'autres pays.

©2010 Enterprise Management Associates, Inc. Tous droits réservés. EMATM, ENTERPRISE MANAGEMENT ASSOCIATES® et le symbole mobius sont des marques déposées ou des marques de droit commun d'Enterprise Management Associates, Inc.

Corporate Headquarters:

5777 Central Avenue, Suite 105

Boulder, CO 80301

Phone: +1 303.543.9500

Fax: +1 303.543.7687

<http://www.enterprisemanagement.com/>



2042.031010