LIVRE BLANC :
FAIRE LE GRAND SAUT DE LA VIRTUALISATION

Problématiques de sécurité et de sauvegarde des environnements virtuels

Faire le grand saut de la virtualisation

Public cible : Directeurs, responsables et administrateurs informatiques (sécurité et sauvegarde) des moyennes entreprises

Confidence in a connected world. Symantec.

Sommaire

Présentation

De nombreuses entreprises de taille moyenne ont investi d'importantes ressources pour sécuriser et sauvegarder leurs serveurs, les postes clients, les données et l'infrastructure réseau globale dans un environnement client-serveur classique. Alors même qu'elles pensent pouvoir tirer parti sereinement de ces investissements, de nouvelles technologies comme le Cloud Computing et la virtualisation entrent en scène, avec leur lot d'avantages majeurs et de nouveaux enjeux.

En essence, le Cloud Computing consiste à utiliser via Internet des services tiers relativement évolutifs et fiables pour l'activité de l'entreprise, avec paiement à l'usage, comme SaaS (Software-as-a-Service) ou IaaS (Infrastructure-as-a-Service). La virtualisation est la première étape du Cloud Computing.

La virtualisation utilise un logiciel pour scinder un serveur physique en plusieurs machines virtuelles indépendantes, ce qui permet d'exploiter plus efficacement les ressources informatiques existantes. Il s'agit également d'un préalable au Cloud Computing, car elle met à disposition des ressources physiques et logiques à travers une couche de services virtuelle dans l'entreprise.

La virtualisation présente des atouts séduisants : gains de temps et d'argent importants, productivité accrue et meilleur service client. Les serveurs existants sont mieux utilisés, les machines les plus anciennes mises hors service et de l'espace peut être libéré. De plus, les coûts énergétiques baissent car le nombre de systèmes à alimenter et refroidir diminue.

En outre, la virtualisation améliore la fiabilité et les performances en assurant une haute disponibilité et une répartition de charge entre divers hôtes physiques. En cas de panne d'un serveur physique, la reprise est beaucoup plus rapide dans un environnement virtuel. Un simple basculement des serveurs virtuels vers une autre machine s'effectue sans impact sur les utilisateurs, et un seul responsable informatique peut gérer beaucoup plus de serveurs bien plus rapidement.

La virtualisation offre des avantages indéniables, mais elle demande une planification et une gestion rigoureuses pour garantir que vos données ne courent aucun risque de corruption et que l'accès est correctement contrôlé. Dans le cadre de votre migration vers un environnement virtuel, posez-vous les questions suivantes pour assurer une bonne gestion de la transition et vous permettre de tirer pleinement parti de cet environnement :

- Vos outils de sécurité et de sauvegarde existants vont-ils fonctionner dans l'environnement virtuel ?
- Etes-vous contraint d'utiliser des outils de sécurité et de sauvegarde différents pour vos environnements physiques et virtuels ?
- Vos outils de sécurité et de sauvegarde sont-ils complexes à utiliser ?
- Quel est l'impact de votre logiciel de sauvegarde sur vos besoins de stockage ?
- Ce logiciel est-il étroitement intégré à votre environnement virtuel ?
- Avez-vous défini des politiques pour éviter une croissance non maîtrisée de l'environnement virtuel ?

Etes-vous contraint d'utiliser des outils de sécurité et de sauvegarde différents pour vos environnements physiques et virtuels ?

La virtualisation doit simplifier, et non compliquer, votre environnement technologique. Plus vous installez de logiciels, d'appliances et de serveurs sur votre réseau, plus l'environnement gagne en complexité et plus la maintenance et la gestion requises s'alourdissent.

Les entreprises ont à présent pour mission de maintenir le degré de sécurité et de protection existant afin de sécuriser, protéger, sauvegarder et restaurer leurs machines virtuelles. La technologie adéquate assure la visibilité sur l'environnement virtuel afin que les entreprises puissent virtualiser et bénéficier des avantages plus rapidement.

Les solutions de pointe conçues pour l'environnement virtuel intègrent la sécurité, le stockage et la sauvegarde. Elles offrent également les avantages suivants :

- Capacité de gérer avec une seule console la protection des données sur des systèmes physiques et virtuels.
- Sauvegardes sans compromis au niveau de la restauration des fichiers et sans surcharge pour l'infrastructure.
- Déduplication pour éviter de stocker les mêmes données plusieurs fois (pour atteindre une réduction du stockage jusqu'à 90 %).
- Sécurité automatisée pour appliquer des politiques de sécurité appropriées et identifier immédiatement les risques ou les menaces.
- Garantie de la mise à jour des machines virtuelles (VM) et de leur conformité intégrale aux politiques de sécurité avant leur accès au réseau.[1]

Les outils de sécurité et de sauvegarde intégrés permettent aux équipes informatiques débordées de protéger leur infrastructure grâce à une seule interface, d'un seul fournisseur. Si vous utilisez plusieurs outils pour la sécurité et la sauvegarde de votre réseau, une solution de protection intégrée peut simplifier considérablement votre tâche.

Vos outils de sécurité et de sauvegarde sont-ils complexes à utiliser ?

Les responsables informatiques des entreprises de taille moyenne sont souvent obligés de maîtriser différentes technologies et votre logiciel de protection des environnements virtuels ne doit pas être trop complexe. Recherchez des solutions automatisées faciles à utiliser, avec une console conçue spécifiquement pour l'environnement virtuel. Evitez les solutions trop basiques dont la protection manque de puissance, ainsi que celles si complexes que leur utilisation s'avère un défi.

La solution adéquate peut protéger vos données, réduire les coûts de stockage et d'administration et automatiser les processus de gestion avec des fonctions d'archivage, de sauvegarde et de sécurité efficaces, le tout dans une console unique. Pour sécuriser votre environnement virtuel, veillez à ce que votre logiciel de protection soit intégré, efficace, rapide et convivial, avec des fonctions de sécurité éprouvées.

Quel est l'impact de votre logiciel de sauvegarde sur vos besoins de stockage ?

Si (ou quand) un sinistre survient, votre entreprise doit pouvoir exécuter une restauration rapide. Fait étonnant, la première erreur commise lors de la sauvegarde de l'environnement virtuel consiste justement à ne pas sauvegarder l'environnement virtuel. Dans un article de blog récent, basé sur une étude mondiale auprès de milliers d'utilisateurs, Symantec révèle que près des deux-tiers des machines virtuelles ne sont pas correctement sauvegardées, ce qui représente un risque majeur pour l'entreprise.[2]

Mal réalisée, la virtualisation des serveurs peut en fait entraîner une augmentation des besoins de stockage. La gestion inefficace du stockage est capable d'engloutir les économies obtenues grâce à la consolidation des serveurs. La sauvegarde de plusieurs versions d'un fichier constitue un bon exemple d'une mauvaise utilisation du stockage.

Un logiciel de sauvegarde sophistiqué détermine s'il fonctionne dans un environnement virtuel et sauvegarde correctement les données de chaque hyperviseur. Les solutions de gestion du stockage de pointe dédupliquent automatiquement (ne stockent qu'une version de chaque fichier), récupèrent l'espace inutilisé et virtualisent les pools de stockage pour garantir une réduction des besoins de stockage, et éviter l'inverse. Une solution optimisée pour l'environnement virtuel offre assurément les fonctions de sécurité, de sauvegarde et de gestion du stockage efficaces dont vous avez besoin.

Le logiciel est-il étroitement intégré à votre environnement virtuel ?

Les machines virtuelles fonctionnant dans leurs propres environnements, chacune d'elle peut dépendre de plusieurs systèmes de protection, ce qui complique leur gestion. Les outils de sauvegarde et de restauration classiques, basés sur des agents, ne sont pas

1-(sur site Web de Symantec : www.symantec.com/connect/blogs/symantec-v-ray-end-dark-ages-virtualization)
2-http://www.symantec.com/connect/blogs/ten-backup-mistakes-virtual-environment-part-1

adaptés à l'environnement virtuel. En effet, les agents, par nature, manquent de cohésion. Vous devez installer physiquement et gérer des agents pour chaque application sur le serveur virtuel. Ce processus long et lourd présente des risques pour la sécurité.

Une solution de pointe qui identifie votre environnement virtuel et s'y intègre peut rechercher les nouvelles machines virtuelles clientes. Elle centralise la gestion, minimise la configuration des tâches et l'administration, prend en charge plusieurs jeux de sauvegarde et offre un support étendu des applications et systèmes d'exploitation.

Sur VM Blog, on peut lire que les environnements virtuels peuvent difficilement faire l'objet d'un contrôle visuel et, compte tenu de la mobilité des serveurs virtuels et des problèmes connexes, qu'ils présentent souvent des configurations et des populations de serveurs dynamiques. Un tel contexte s'avère propice à la propagation des menaces, à la négligence de certains périphériques ou à la dissimulation d'activités inadéquates. Pour empêcher les oublis de configuration, les périphériques indésirables, les lacunes d'audit et d'autres problèmes, le système de sécurité doit maintenir un suivi permanent de tous les périphériques virtuels, les services et les communications.

En d'autres termes, si vous utilisez des systèmes de protection qui ne s'intègrent pas à l'environnement virtuel, vous n'êtes pas protégé.

Avez-vous défini des politiques pour éviter la prolifération des machines virtuelles ?

La prolifération des VM est la conséquence d'une croissance non maîtrisée de l'environnement virtuel : les administrateurs créent des VM pour chaque petite tâche et se trouvent confrontés à une explosion ingérable de leur nombre. Du fait de leur grande facilité de déploiement, elles sont souvent mises en service avec peu de considération quant à leur impact sur la sécurité et la gestion du réseau. Le déploiement d'une machine virtuelle s'avérant souvent bien plus facile que celui d'une nouvelle machine physique, faites preuve de bon sens. Créez, appliquez et contrôlez les politiques de gestion des machines virtuelles pour maintenir la stabilité de l'environnement virtuel.

Quelles conclusions tirer de tout cela ?

Il ne fait aucun doute que la virtualisation offre des avantages considérables pour les entreprises moyennes, notamment en termes d'efficacité, d'économies, de fiabilité et de performances. Toutefois, afin de bénéficier de ces avantages, les entreprises doivent adapter correctement leurs pratiques d'excellence, politiques, outils et procédures à l'environnement virtuel. Avec un minimum de précaution, de planification et de bon sens, votre déploiement de la virtualisation vous permet de mieux exploiter vos ressources et de délester votre équipe informatique pour qu'elle se consacre à des projets stratégiques contribuant au développement de l'entreprise. Vous serez ainsi en mesure de tirer pleinement parti de votre système d'informations pour gagner en compétitivité, gage de réussite.

A propos de Symantec

Symantec est un leader mondial des solutions de sécurité, de stockage et de gestion des systèmes destinées à aider les particuliers et les entreprises à sécuriser et gérer leur environnement informatique. Nos logiciels et services permettent d'assurer une protection plus complète et plus efficace contre davantage de risques à différents points et d'instaurer ainsi la confiance, quel que soit l'endroit où les informations sont utilisées ou stockées. La société Symantec, dont le siège social est basé à Mountain View en Californie, est présente dans 40 pays. Des informations supplémentaires sont disponibles à l'adresse www.symantec.fr.

Pour connaître les coordonnées des bureaux dans un pays spécifique, consultez notre site Web.

Symantec Limited
Ballycoolin Business Park
Blanchardstown
Dublin 15
Irlande
Tel. : +353 1 803 5400
Fax : +353 1 820 4055
www.symantec.com

Symantec aide les entreprises à sécuriser et à gérer leur environnement informatique au moyen de solutions de **virtualisation des terminaux**, de **virtualisation des serveurs** et de **virtualisation des applications**.

7/2012 21196714