

« Ce que tout DSI a besoin de savoir sur la protection des données dans les environnements virtuels » (Partie 1)

À l'heure actuelle, les services informatiques déploient rapidement des technologies de virtualisation ; en fait, selon Gartner, le taux de pénétration de la virtualisation des serveurs est déjà supérieur à 60 % et devrait dépasser 80 % d'ici à 2016. Dans ce contexte, les clients doivent relever le défi de l'incorporation de la protection des données et des méthodologies d'archivage pour leurs données virtualisées.

ESG a récemment indiqué que la résolution des problèmes liés à la protection des données virtualisées constituait l'une des principales priorités de 60 % des utilisateurs des technologies de virtualisation en 2013, un chiffre étonnant. Si les options disponibles pour protéger les données traditionnelles sont nombreuses, il en va tout autrement pour les données virtualisées.

Un autre rapport de Gartner établit que plus d'un tiers des organisations changeront de fournisseur pour leur solution de sauvegarde, en raison de facteurs comme le coût, la complexité ou les fonctionnalités. En me basant sur ce que j'ai entendu en discutant avec les clients, j'aimerais ajouter un quatrième facteur, la compatibilité. Cet article étudie ces quatre domaines et suggère des pistes pour surmonter les difficultés liées à la protection des données virtualisées.

Contenir les coûts

Steve Duplessie, fondateur et analyste principal d'ESG, a confessé récemment qu'il « *était stupéfait que des tâches informatiques basiques et routinières comme la protection des données posent aujourd'hui encore des problèmes majeurs aux clients* ». L'ajout de la virtualisation au paysage n'est pas nécessairement de nature à rendre les choses plus simples.

Quand ils commencent à envisager de protéger leurs données virtuelles, les clients peuvent avoir pour premier réflexe d'utiliser une application de sauvegarde traditionnelle existante, mais il convient d'aborder cette approche avec circonspection. En effet, un logiciel de sauvegarde traditionnel peut rapidement devenir trop onéreux pour gérer des données virtuelles.

La plupart des applications traditionnelles appliquent une facturation basée sur un agent par hôte ou parfois par machine virtuelle (VM), ce qui entraîne des frais de licence et de maintenance inutiles et augmente le temps consacré à la gestion des licences additionnelles. De plus, faute d'agents pour ces hôtes, de précieuses données risquent de ne pas être prises en compte lors de la sauvegarde suivante. A l'opposé, ajouter un agent de sauvegarde par défaut sur chaque machine virtuelle peut certes simplifier les tâches de déploiement, mais l'opération peut rapidement s'avérer onéreuse, et accroître inutilement la consommation des ressources (CPU, réseau...)

Lorsqu'ils doivent protéger des applications comme Exchange, SQL et SharePoint, ou exécuter d'autres tâches de protection des données (comme la sauvegarde sur bande ou la réplication

distante dans le cadre d'un PRA), la plupart des logiciels de sauvegarde nécessitent des plug-ins ou des licences complémentaires. Certains logiciels de sauvegarde traditionnels utilisent aujourd'hui des licences basées sur la capacité ; ils peuvent très bien convenir à certaines grandes entreprises, mais aussi entraîner une explosion des coûts et proposer des fonctions dont les utilisateurs n'ont pas forcément besoin.

Des applications de sauvegarde plus simples

Il faut s'intéresser aux applications de sauvegarde qui adoptent une approche plus simple en matière de licences, celles qui n'utilisent pas d'agents ni de plug-ins, ou ne facturent pas des fonctionnalités inutiles. En effet, les applications de ce type sont généralement moins onéreuses et leur méthodologie de déploiement permet aussi de réduire les frais généraux et d'éviter d'avoir à effectuer le suivi des licences. Surtout, elles garantissent que toutes les données du client sont sauvegardées, et pas seulement celles que leurs licences prévoient de capturer.

Sauvegarder plus de données que nécessaire fera grimper les coûts, et par conséquent augmenter le volume des données en ajoutant des machines virtuelles à un plan de sauvegarde risque d'entraîner une hausse exponentielle des dépenses. Les machines virtuelles génèrent beaucoup de données superflues (et inutiles pour la restauration), et des hyperviseurs ont été mis en place pour gérer ce problème de façon maîtrisée et remarquable.

Il convient donc de s'intéresser aux outils dédiés aux machines virtuelles qui tirent parti de ces fonctionnalités de l'hyperviseur et qui aident à éliminer ces données superflues. De plus, les technologies de déduplication pourront réduire l'espace de stockage nécessaire aux sauvegardes sur le site, ainsi que le volume des données envoyées et résidant dans le Cloud pour la reprise après incident et la sauvegarde hors site.

Enfin, les coûts supplémentaires associés à la sauvegarde des données virtuelles peuvent être liés à l'augmentation du nombre de serveurs physiques (ou serveurs de sauvegarde), à celle du nombre d'équipements de stockage pour ces données et au support technique additionnel que doit assurer l'éditeur pour la maintenance des données virtuelles.

Du côté du serveur de sauvegarde physique, des applications de sauvegarde sont conçues spécifiquement pour s'exécuter en tant qu'appiances virtuelles et tirer pleinement parti non seulement de l'infrastructure existante mais aussi de toutes les technologies associées à une machine virtuelle, par exemple vMotion et vStorage Motion dans les environnements VMware.

Dans la [seconde partie de notre avis d'expert](#), Stéphane Estevez évoque les pistes de la complexité, les fonctionnalités et la compatibilité de la protection des données dans les environnements virtuels.

Voir aussi

[Silicon.fr étend son site dédié à l'emploi IT](#)

[Silicon.fr en direct sur les smartphones et tablettes](#)