« Ce que tout DSI a besoin de savoir sur la protection des données dans les environnements virtuels » (2)

Suite le la première partie de cet avis d'expert « Ce que tout DSI a besoin de savoir sur la protection des données dans les environnements virtuels ».

Gérer la complexité

Les machines virtuelles sont par nature des structures dynamiques qui introduisent divers types de perturbations dans l'univers relativement contrôlé de la protection des données. De nombreux facteurs sont à l'origine de cette complexité, en particulier la multiplication des machines virtuelles. Ces dernières sont si faciles à déployer que même des employés qui ne connaissent rien à la protection des données ou ne s'en préoccupent pas peuvent les créer, causant ainsi des soucis inutiles et des effets de bord parfois difficilement contrôlables aux responsables informatiques.

Il convient de réfléchir à plusieurs questions essentielles : comment l'application de sauvegarde s'intègre-t-elle à l'hyperviseur ? Certaines applications peuvent fonctionner directement avec cet outil pour réaliser l'inventaire et détecter automatiquement les nouveaux hôtes ou machines virtuelles créés ou ajoutés depuis la précédente sauvegarde. Cela garantit que les données seront protégées, indépendamment du mode de création des machines virtuelles.

Il faut aussi prendre en compte les sérieux problèmes de performance qui peuvent avoir des effets négatifs sur un environnement. Les applications de sauvegarde s'exécutent selon un calendrier, indépendamment des autres événements pouvant survenir dans l'environnement, et leurs tâches nécessitent des ressources (réseau, E/S disque, puissance de traitement) et des applications plus axées sur les environnements virtualisés. Ces applications peuvent généralement être déployées en tant que modèle OVF (appliance virtuelle) et utiliser moins de ressources, mais la fonctionnalité vMotion peut aussi y être désactivée lorsque leurs tâches arrivent à leur terme afin de libérer des ressources dont l'hôte a besoin pour d'autres machines virtuelles qui remplissent des fonctions plus stratégiques.

Il est également important de comprendre combien il est simple de procéder à des restaurations avec une application. Si cette dernière utilise un format propriétaire (comme la grande majorité des applications), elle seule a accès aux données, ce qui réduit considérablement les possibilités de restauration et engendre des conflits inutiles pour les ressources. Elle devra déployer un assistant virtuel pour restaurer les données de sorte que l'hyperviseur ou la base de données puisse comprendre ce qu'il ou elle reçoit. Les applications de sauvegarde capables de protéger les données dans leur format natif (sujet abordé dans la suite de cet avis) sont par nature plus souples et n'imposent pas de démarrer les machines virtuelles avant l'exploration, la recherche ou la restauration de fichiers individuels.

Fonctionnalités : lesquelles sont nécessaires ?

L'évolutivité d'une solution de protection des données virtuelles est un aspect essentiel à prendre en compte. Le rythme d'adoption des technologies de virtualisation ne faiblissant pas, la plupart des environnements qui vont probablement en bénéficier ont besoin d'une solution de protection des données évolutive, pas seulement du point de vue du support mais aussi à la volée, à mesure que le volume des données virtuelles augmente. La multiplication des machines virtuelles et les données superflues font grimper les coûts de la sauvegarde mais si cette dernière n'est pas capable d'accompagner la croissance des données des machines virtuelles, on peut légitimement s'interroger sur son utilité.

Les responsables informatiques ont besoin d'un système qui pourra évoluer facilement, pour que toutes les données soient toujours protégées. Les applications traditionnelles étaient conçues pour protéger des données physiques et celles qui leur ont succédé ne proposent pas forcément les fonctionnalités, l'interopérabilité avec les données issues de la virtualisation ni les hyperviseurs nécessaires pour répondre aux besoins d'aujourd'hui.

Les solutions proposant des liens directs avec l'hyperviseur offrent indéniablement un intérêt stratégique pour la protection des données virtuelles. Certains hyperviseurs mettent en œuvre des méthodes uniques pour réduire les données supplémentaires associées à leurs machines virtuelles ; toutefois, il est important qu'une solution de protection des données puisse aussi détecter automatiquement les nouvelles machines virtuelles de sorte que toutes les données soient protégées. En cas de déplacement de la machine virtuelle ou du magasin de données (datastore) qui lui est associé, l'application de sauvegarde protégera-t-elle encore ces données ?

Un système de protection ne devrait pas seulement protéger les données virtuelles mais aussi les données physiques qui continueront d'exister, même si leur volume n'augmentera pas forcément. La combinaison d'applications dédiées aux données virtuelles et de logiciels traditionnels pour les données physiques constitue la meilleure approche. Toutefois, une application dédiée à la virtualisation pourra éventuellement fonctionner en conjonction avec une application traditionnelle, en lui présentant les données virtuelles, de sorte que l'investissement que représentent les médias de sauvegarde, l'application de sauvegarde, les politiques et les procédures existants ne soit pas perdu.

La dernière question à se poser est celle-ci : une solution offre-t-elle de la souplesse sur le plan des médias de sauvegarde ? Peut-elle par exemple sauvegarder les données sur bande, dans le Cloud ou en appliquant la meilleure méthode à venir ? Les solutions de protection des données les plus plébiscitées seront celles qui peuvent tirer parti de n'importe quel média de sauvegarde non seulement pour la sauvegarde mais aussi pour l'archivage des machines virtuelles et des données associées. Par conséquent, vous devez vous assurer que toute application ou solution en place peut prendre en charge le disque, le Cloud, mais aussi la bande. Cette dernière reste le média de prédilection pour la sauvegarde et l'archivage de près de 80 % des organisations.

Compatibilité

Le terme « compatibilité » peut avoir plusieurs sens. Dans le contexte qui est le nôtre, nous parlons spécifiquement du type de format dans lequel l'application de sauvegarde « protège » les données sur leur destination cible. La plupart des applications utiliseront un format propriétaire qui permet à la seule application qui a réalisé la sauvegarde d'accéder aux données, ce qui élimine quasiment toute souplesse lors des choix de sauvegarde et de reprise après incident.

Mais ce n'est pas tout. Imaginez que vous utilisiez une application de sauvegarde qui peut protéger les données dans leur format natif sur la machine virtuelle ainsi que les données associées, ce qui élimine tout enfermement propriétaire et fait des données une véritable ressource non seulement pour l'utilisateur final mais aussi pour le département informatique. Conserver les données dans un format propriétaire limitera le recours aux technologies ITaaS ; l'application de sauvegarde peut rapidement devenir un frein puisqu'elle seule peut accéder et relire ces données.

Avec les applications qui utilisent le format natif, il est possible de vérifier que les données ne sont pas infectées par des virus, de contrôler la sécurité et la conformité, et d'utiliser des moteurs d'indexation en conjonction avec les données. Plus important encore, les applications qui sauvegardent les données dans leur format natif préservent la liberté de choix du média de sauvegarde et des autres applications qui pourront avoir besoin des données deux, cinq ou dix ans après leur stockage initial. Même si ce choix n'est jamais exercé, il est bon de savoir qu'il est possible.

Conclusion

Les données issues de la virtualisation continuent de s'imposer et les clients continueront de bénéficier des avantages de la virtualisation. Mais ils devront aussi apprendre à protéger au mieux la nouvelle structure de données que cette technologie introduit. Si les applications traditionnelles peuvent suffire aujourd'hui pour protéger les données virtuelles, qu'en sera-t-il demain ? Deviendront-elles un allié ou un ennemi de l'infrastructure virtuelle ?

Les clients devraient savoir en quoi et pourquoi les données virtuelles sont différentes des données physiques mais ne devraient pas craindre d'analyser les options disponibles pour les protéger. Certaines applications conçues à partir des méthodologies traditionnelles de protection des données ont été adaptées pour protéger les données virtuelles mais d'autres ont été créées pour les technologies de virtualisation et leurs environnements, et sont capables de tirer parti des fonctions et des souplesses des infrastructures virtuelles. Les unes et les autres présentent des atouts et des faiblesses ; la bonne nouvelle, c'est que vous avez le choix.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes