Cloud computing et virtualisation, ennemis de la sauvegarde des données?

Il est de plus en plus difficile de gérer les ressources virtuelles, physiques et de 'cloud computing' disparates. Telle est la conclusion de la 6e étude annuelle Symantec Disaster Recovery, qui ne manque pas de lui fournir des arguments. Pour l'éditeur, la virtualisation des données et des applications complique considérablement la gestion des sauvegardes et la protection des systèmes pour les entreprises.

Ainsi, 44 % des données des systèmes virtuels ne seraient pas sauvegardées régulièrement. Seulement une société sur cinq (20 %) protègerait son environnement virtuel à l'aide de technologie de duplication et de *failover* (basculement automatique en cas de défaillance d'un serveur vers un autre). Plus inquiétant, 60 % des serveurs virtualisés ne seraient pas couverts par un plan de reprise en cas d'incident. Un chiffre en augmentation, comparé aux 45 % constatés en 2009.

Des outils difficiles à maitriser?

La difficulté à maîtriser les outils de protection des applications et données explique en partie cette situation alors que les solutions de virtualisation se multiplient, tant dans les offres que dans les adoptions. Pour 58 % des DSI interrogées ayant rencontré des problèmes de protection, il s'agit d'une préoccupation importante pour leur entreprise.

La sécurité des offres de 'cloud computing' reste également une question majeure pour 66 % des sondés. Une question d'autant plus pointue que la principale difficulté pour implémenter le 'cloud' et la virtualisation du stockage tient au contrôle du *failover* et la haute disponibilité des ressources pour une large majorité des sondés (55 %).

Une perception de la réalité qui serait faussée

Cette situation impacterait directement la qualité des sauvegardes. Ainsi, celles-ci ne sont effectuées qu'une fois par semaine au mieux dans 82 % des cas, alors qu'elles devraient l'être quotidiennement. Pour y parvenir, il faudrait palier le manque de ressources et à l'adoption d'une véritable solution de backup dédiée. C'est du moins l'interprétation des personnes interrogées dont 59 % pointent le manque de moyens (humain, budgétaire et d'espace) pour assurer une politique de sauvegarde digne de ce nom.

Un défaut de perception de la réalité explique également pour partie la négligence des entreprises. Ainsi, la plupart des personnes interrogées estiment à 2 heures le temps de reprise d'activité suite à un incident de leur 'datacenter' alors que la durée moyenne d'arrêt des systèmes s'est élevé à 5 heures au cour des 12 derniers mois. Ces arrêts s'expliquent principalement par les mises à jour système (72 % des sondés), des pannes d'électricité (70 %) et les conséquences d'une cyberattaque (63 %). Ces causes ont respectivement entraîné 50,9, 11,3 et 52,7 heures d'interruption des systèmes. Paradoxalement, seules 26 % des entreprises ont effectué une étude d'impact des pannes de courant et techniques.

« En adoptant de nouvelles technologies telles que la virtualisation et le 'cloud computing' pour réduire leurs

coûts et améliorer leurs actions pour la reprise d'activités après incident, les entreprises ajoutent de la complexité à leur environnement et laissent leurs applications et données stratégiques sans protection, résume **Vincent Videlaine**, directeur de l'unité *Storage and Availability Management* chez Symantec. Et de recommander aux entreprises d'adopter *des outils qui fournissent des solutions globales avec une politique régulière à travers tous les environnements. Les DSI doivent tout de même privilégier la simplification et la standardisation pour se concentrer sur les meilleures pratiques fondamentales afin de réduire la durée des arrêts. »* Des outils qui devraient bien exister chez Symantec… – entre autres.