Reprise d'activitÃ© aprÃ¨s sinistre et protection des donnÃ©es, question d'approche
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 26/7/2011 14:00:00

Pour leurs stratÃ©gies de sauvegarde et de restauration, les entreprises cherchent en gÃ©nÃ©ral dans deux directions diffÃ©rentes. Les stratÃ©gies de reprise d'activitÃ© aprÃ¨s sinistre consistent Ã protÃ©ger intÃ©gralement les systÃ¨mes, et la protection des donnÃ©es assure une protection au niveau des fichiers.

La stratÃ©gie la plus efficace consisterait Ã prendre en compte ces deux approches. Les PME peuvent ainsi bÃ©nÃ©ficier d'une plus grande flexibilitÃ© en optant pour une solution intÃ©grÃ©e, unifiant la reprise d'activitÃ© aprÃ¨s sinistre et la protection des donnÃ©es.

Au cours des derniÃ¨res annÃ©es, la situation des donnÃ©es dâentreprises a radicalement changÃ©, tant quantitativement que qualitativement. D'une part les volumes de donnÃ©es ont continuÃ© Ã augmenter de faÃ§on exponentielle en raison des nouvelles technologies et des nouveaux processus informatiques. D'autre part, les donnÃ©es stockÃ©es sont de plus en plus importantes pour l'entreprise, et les donnÃ©es considÃ©rÃ©es comme Â« critiques Â» sont de plus en plus nombreuses. Aujourd'hui, ce ne sont plus seulement les donnÃ©es des systÃ¨mes de CAO ou ERP qui sont capitales pour les entreprises. Les e-mails contenant des donnÃ©es contractuelles importantes ou de simples fiches techniques et descriptions de produits sont Ã©galement critiques et peuvent s'avÃ©rer dÃ©terminants quant Ã la responsabilitÃ© des fabricants.

Pour les services informatiques des entreprises, la sauvegarde de ces donnÃ©es est devenue plus que jamais une tÃ¢che cruciale ; il en va de la rÃ©ussite Ã©conomique de leur entreprise, voire de son existence. Par ailleurs, toutes les entreprises souhaitent pouvoir accÃ©der Ã leurs donnÃ©es 24h/24, 7j/7. Les entreprises travaillent en continu, par consÃ©quent, toute interruption peut entrainer une perte de productivitÃ© considÃ©rable. Les services informatiques doivent s'assurer que les fichiers et les systÃ¨mes restent disponibles, mÃªme en cas de suppression accidentelle ; d'incidents internes, tels que des pannes matÃ©rielles ou d'Ã©vÃ©nements externes, tels qu'un incendie, un accÃ¨s non autorisÃ© ou des sinistres naturels. Toutes ces exigences conduisent l'entreprise vers deux approches de sauvegarde :

â¢ La reprise d'activitÃ© aprÃ¨s sinistre considÃ¨re les donnÃ©es en tenant compte de l'intÃ©gralitÃ© du systÃ¨me. AprÃ¨s un incident, l'ensemble des donnÃ©es, y compris le systÃ¨me d'exploitation, les applications et les donnÃ©es de l'utilisateur, doit pouvoir Ãªtre restaurÃ© intÃ©gralement, le plus rapidement possible, pour limiter l'interruption de l'activitÃ©.

â¢ La protection des donnÃ©es met l'accent sur les donnÃ©es. Il est possible de distinguer plusieurs types de donnÃ©es, lesquelles, aprÃ¨s tout incident, sont restaurÃ©es dans un ordre spÃ©cifique en fonction de leur importance et de leur fonction dans les diffÃ©rentes applications.

La reprise d'activitÃ© aprÃ¨s sinistre permet de restaurer intÃ©gralement et en toute transparence un systÃ¨me dÃ©faillant et constitue donc un aspect fondamental de tout concept de sauvegarde. Toutefois, avec les volumes de donnÃ©es d'aujourd'hui, rÃ©aliser unesauvegarde complÃ¨te (systÃ¨me d'exploitation, applications, paramÃ¨tres et donnÃ©es inclus) prend plus de temps. Ainsi, pour des raisons essentiellement techniques, ces sauvegardes sont souvent rÃ©alisÃ©es Ã distance les unes des autres, mÃªme si, avec la technologie moderne de crÃ©ation d'image disque, la sauvegarde peut Ãªtre exÃ©cutÃ©e pendant les heures d'activitÃ© et qu'elle ne nÃ©cessite pas d'Ãªtre reportÃ©e sur des pÃ©riodes de faible activitÃ©.

Il en est de mÃªme pour la restauration. La reprise d'activitÃ© aprÃ¨s sinistre permet aux entreprises de reprendre leur activitÃ© sur une pÃ©riode donnÃ©e. En revanche, pour bon nombre d'incidents, surtout pour ceux qui se trouvent sous le Â« seuil de sinistre Â», la granularitÃ© des stratÃ©gies de reprise d'activitÃ© aprÃ¨s sinistre est souvent insuffisante. C'est pour cela que le concept de protection des donnÃ©es est important. En effet, il permet d'effectuer des sauvegardes et des restaurations au niveau des fichiers, et mÃªme directement au niveau des objets. Les sauvegardes peuvent Ãªtre rÃ©alisÃ©es plus rÃ©guliÃ¨rement, ce qui permet d'effectuer des restaurations ciblÃ©es de donnÃ©es spÃ©cifiques. Certaines solutions permettent mÃªme d'avoir une vision logique et pratique des fichiers sauvegardÃ©s, avec des fonctionnalitÃ©s de catalogage et de recherche. Cela permet d'Ã©viter d'avoir Ã parcourir toutes les archives des sauvegardes. Si des utilisateurs souhaitent que des fichiers spÃ©cifiques soient rapidement restaurÃ©s Ã partir d'une sauvegarde, les techniciens peuvent rÃ©pondre rapidement et efficacement Ã leur requÃªte.

Toutefois, si l'ensemble du systÃ¨me cesse de fonctionner en raison d'un dysfonctionnement matÃ©riel, la durÃ©e de restauration ne peut Ãªtre rÃ©duite qu'avec une stratÃ©gie de reprise d'activitÃ© efficace. Pour les entreprises, la question n'est donc pas de choisir entre ces deux approches. En effet, elles ont besoin d'une souplesse qui leur permet d'agir en toute situation, pour un systÃ¨me complet aussi bien que pour des fichiers spÃ©cifiques.

Solutions intÃ©grÃ©es

La reprise d'activitÃ© aprÃ¨s sinistre et la protection des donnÃ©es doivent aller de pair. Il faut reconnaÃ®tre que les solutions qui intÃ¨grent ces deux approches sont rares. D'ailleurs, le plus souvent, elles ne sont pas intÃ©grÃ©es au sein d'une solution unique. Bon nombre de fabricants ont simplement Ã©tendu une application existante en proposant des produits complÃ©mentaires. Pour ce qui est de la description du produit, ces combinaisons peuvent sembler unifiÃ©es, mais elles ne le sont pas en termes de technologie sous-jacente.

Sans parler de l'intercompatibilitÃ© des systÃ¨mes, qui entraÃ®ne une charge de travail d'administration considÃ©rable, surtout pour les PME. Dans les grandes entreprises qui emploient de nombreux administrateurs, implÃ©menter et gÃ©rer deux systÃ¨mes distincts, comme conserver le savoir-faire requis, ne pose aucun problÃ¨me. En revanche, pour les entreprises plus petites, avec des ressources informatiques limitÃ©es, la gestion en parallÃ¨le d'approches de sauvegarde diffÃ©rentes peut constituer une difficultÃ© insurmontable, qui, compte tenu de l'importance de cette tÃ¢che, peut avoir des consÃ©quences irrÃ©mÃ©diables.

Des solutions intÃ©grÃ©es par exemple, comme Acronis Backup & Recovery 11, combinent reprise d'activitÃ© aprÃ¨s sinistre et protection des donnÃ©es au sein d'une seule et mÃªme application. Avec une solution complÃ¨te, les entreprises peuvent effectuer des sauvegardes et des restaurations granulaires ou intÃ©grales, en environnements physiques et virtuels ou dans le cloud. Une interface utilisateur unifiÃ©e, intÃ©grant les deux approches, simplifie la protection des systÃ¨mes. Les PME peuvent Ã©galement dÃ©velopper des concepts de sÃ©curitÃ© Ã partir de cette base, qui couvre tous les aspects de la sauvegarde de leurs donnÃ©es stratÃ©giques.

[**Isabelle Delcuvellerie**, Acronis Country Manager pour la France et les pays MÃ©diterranÃ©ens]