Kroll Ontrack : 5 erreurs courantes conduisant Ã la perte de donnÃ©es
Internet
PostÃ© par : JPilo
PubliÃ©e le : 7/6/2013 13:00:00

Kroll Ontrack, leader sur le marchÃ© de la rÃ©cupÃ©ration de donnÃ©es, de la recherche dâ informations et de preuves informatiques prÃ©sente **cinq des erreurs que commettent** le plus souvent les administrateurs informatiques et qui peuvent entraÃ®ner la perte de donnÃ©es.

Ã tant donnÃ© la complexitÃ© et la capacitÃ© des pÃ©riphÃ©riques de stockage et l'importance des donnÃ©es d'entreprise, la documentation et la mise en place des meilleures pratiques sont essentielles pour assurer la protection des donnÃ©es.

Â« *Comme les donnÃ©es sont stockÃ©es Ã de multiples endroits et sur de multiples appareils, leur perte Ã quelque niveau que ce soit peut Ãªtre trÃ¨s prÃ©judiciable, contraignant les administrateurs informatiques Ã trouver une rÃ©solution rapide aux problÃ¨mes et Ã minimiser le temps d'arrÃªt* Â», souligne **Paul Dujancourt**, directeur gÃ©nÃ©ral de Kroll Ontrack France. Â« *Devant une telle pression, il est possible que les Ã©quipes informatiques nÃ©gligent les pratiques Ã©tablies par l'ITIL pour la gestion des services informatiques, au profit d'une rÃ©solution rapide des problÃ¨mes, laissant les entreprises exposÃ©es au risque de perte de donnÃ©es* Â».

Pour rÃ©duire ce risque de perdre des donnÃ©es cruciales lors de la gestion des processus informatiques et de la rÃ©solution des problÃ¨mes informatiques, il faut Ã©viter de commettre les erreurs courantes rÃ©pertoriÃ©es ci-aprÃ¨s :

1) DÃ©faut de documentation et d'exÃ©cution des procÃ©dures informatiques, de sauvegarde et de conservation mises en place. C'est un problÃ¨me que Kroll Ontrack rencontre encore et toujours. Un serveur de test passe en production, mais personne n'a informÃ© le service informatique qu'il collecte dÃ©sormais de prÃ©cieuses donnÃ©es et que celles-ci ne sont pas sauvegardÃ©es. Autre cas : une documentation inexacte incite les administrateurs informatiques Ã dÃ©sactiver un rÃ©seau spÃ©cialisÃ© de stockage (SAN) qui est en rÃ©alitÃ© toujours en production, entraÃ®nant une perte de donnÃ©es.

2) DÃ©faut de mise Ã jour du systÃ¨me d'exploitation et du logiciel antivirus. Les journÃ©es sont chargÃ©es et les ressources trÃ¨s sollicitÃ©es, mais l'absence de mise Ã jour des logiciels antivirus et des correctifs de sÃ©curitÃ© des systÃ¨mes d'exploitation peut entraÃ®ner des failles de sÃ©curitÃ© dangereuses et des pertes de donnÃ©es importantes.

3) Sauvegarde inopÃ©rante. Une rÃ©cente Ã©tude menÃ©e auprÃ¨s des clients de Kroll Ontrack a rÃ©vÃ©lÃ© que 60 % d'entre eux avaient une sauvegarde en place au moment de la perte, mais qu'elle ne fonctionnait pas correctement lorsque la perte s'est produite. Faute de mettre en place et d'appliquer des procÃ©dures de sauvegarde ou de tester et vÃ©rifier l'intÃ©gritÃ© des sauvegardes, c'est la perte de donnÃ©es assurÃ©e.

4) Suppression de donnÃ©es qui sont toujours utilisÃ©es. Cela peut paraÃ®tre surprenant,

mais vous seriez Ã©tonnÃ© d'apprendre le nombre de fois oÃ¹ Kroll Ontrack rÃ©cupÃ¨re des donnÃ©es sur des bandes ou des rÃ©seaux de serveurs dont on pense qu'ils ne sont plus utilisÃ©s, mais qui contiennent toujours des donnÃ©es actives. Faites preuve de diligence et assurez-vous que les donnÃ©es que vous supprimez n'ont plus de valeur.

5) Absence de test des procÃ©dures de sÃ©curitÃ© informatique. La moindre faille dans la sÃ©curitÃ© informatique peut avoir des consÃ©quences dÃ©vastatrices, y compris la perte de donnÃ©es cruciales et des coÃ»ts importants. Limitez les mots de passe des administrateurs informatiques aux seuls utilisateurs qui en ont besoin et modifiez-les lorsqu'un administrateur informatique quitte l'entreprise. Certains des cas de perte de donnÃ©es les plus mÃ©morables de Kroll Ontrack sont dus Ã un employÃ© mÃ©content en possession d'un mot de passe actif qui a supprimÃ© dÃ©libÃ©rÃ©ment un nombre important de donnÃ©es cruciales pour l'entreprise.

MÃªme les services informatiques les plus aguerris seront confrontÃ©es un jour ou l'autre Ã des problÃ¨mes qui nÃ©cessiteront une prise de dÃ©cision rapide. Ils devront dÃ©cider au plus vite comment rÃ©agir et procÃ©der. Ci-dessous quelques conseils pratiques pour garantir la meilleure chance d'obtenir une rÃ©solution efficace et rÃ©duire le risque de perte de donnÃ©es.

â¢ Ã©vitez de paniquer et d'agir dans la prÃ©cipitation. Au moment de rÃ©soudre un problÃ¨me, prenez des dÃ©cisions judicieuses et informÃ©es. Envisagez les rÃ©percussions et considÃ©rez les consÃ©quences. La prise de dÃ©cisions irrÃ©flÃ©chie peut accentuer la perte de donnÃ©es et le temps d'arrÃªt, sans parler des coÃ»ts et ressources supplÃ©mentaires induits. En cas de perte de donnÃ©es, ne restaurez pas les donnÃ©es sur le mÃ©dia source Ã partir de la sauvegarde, puisque c'est lÃ que les donnÃ©es ont Ã©tÃ© perdues en premier lieu. Ne crÃ©ez pas non plus de nouvelles donnÃ©es sur le mÃ©dia source : elles pourraient altÃ©rer ou endommager les anciennes donnÃ©es.

â¢ Ayez confiance en vos compÃ©tences et connaissances. Vous faites partie de la solution, pas du problÃ¨me. Lorsque les dirigeants de votre entreprise vous mettent la pression pour que vous remettiez les systÃ¨mes en Ã©tat de fonctionnement coÃ»te que coÃ»te, posez-vous en expert. Aidez les dirigeants Ã Ã©viter les dÃ©cisions qui font plus de mal que de bien. Lorsque vous Ãªtes confrontÃ© Ã un cas potentiel de perte de donnÃ©es, mettez le mÃ©dia concernÃ© hors ligne, et faites vite ! Les donnÃ©es sont Ã©crasÃ©es trÃ¨s rapidement. Ne formatez surtout pas le mÃ©dia pour rÃ©soudre les altÃ©rations.

â¢ Ayez un plan. Suivez les processus Ã©tablis par l'ITIL et assurez-vous que la documentation du centre de traitements est exhaustive et revue frÃ©quemment pour Ãªtre sÃ»r qu'elle est Ã jour. Plus particuliÃ¨rement, n'exÃ©cutez pas des utilitaires de type CHKDSK/FSCK sur vos mÃ©dias, et ne mettez pas Ã jour les microprogrammes en cas de perte de donnÃ©es.

â¢ Connaissez votre environnement (et vos donnÃ©es !). Sachez ce que votre environnement de stockage peut supporter et Ã quelle vitesse il peut rÃ©cupÃ©rer. Sachez quelles donnÃ©es sont cruciales ou irremplaÃ§ables, si elles peuvent Ãªtre saisies Ã nouveau ou remplacÃ©es, et les coÃ»ts pour que ces donnÃ©es redeviennent opÃ©rationnelles. Ã©valuez les coÃ»ts et les risques lorsque vous devez dÃ©terminer ce qui est le plus urgent : remettre votre systÃ¨me en Ã©tat de fonctionnement rapidement ou protÃ©ger les donnÃ©es qui s'y trouvent.

â¢ En cas de doute, appelez un spÃ©cialiste de la rÃ©cupÃ©ration de donnÃ©es. Votre OEM peut certes constituer un bon point de dÃ©part, mais il n'est pas forcÃ©ment prÃ©occupÃ© par la valeur de vos donnÃ©es et le risque de perte de donnÃ©es au moment de remettre votre systÃ¨me en Ã©tat de fonctionnement. Consultez un spÃ©cialiste rÃ©putÃ© de la rÃ©cupÃ©ration de donnÃ©es si vous avez des craintes quant au risque de perte de donnÃ©es.