Virtualisation et Cloud, compliquent la reprise dâ□□activitÃ©s aprÃ¨s incident
Internet
PostÃ© par : JulieM
PubliÃ©e le : 30/11/2010 11:00:00

La nouvelle Ã©dition de lâ□□**Ã©tude annuelle de Symantec sur la reprise dâ□□activitÃ© aprÃ¨s incidents**Â rÃ©vÃ¨le un Ã©cart entre la durÃ©e prÃ©vue des arrÃªts du systÃ¨me et la rÃ©alitÃ©

Symantec annonce les rÃ©sultats de sa sixiÃ¨me Ã©tude annuelle Symantec Disaster Recovery, qui dÃ©montre qu'il est de plus en plus difficile de gÃ©rer les ressources virtuelles, physiques et de cloud computing disparates. En effet, la protection et la restauration des applications et des donnÃ©es stratÃ©giques est sans cesse plus complexe pour les entreprises. En outre, cette Ã©tude montre que les systÃ¨mes virtuels ne sont pas correctement protÃ©gÃ©s.

L'Ã©tude rÃ©vÃ¨le que prÃ¨s de la moitiÃ© (44 %) des donnÃ©es des systÃ¨mes virtuels ne sont pas sauvegardÃ©es rÃ©guliÃ¨rement, et que seulement une sociÃ©tÃ© consultÃ©e sur cinq utilise des technologies de duplication et de failover pour protÃ©ger les environnements virtuels. Les sociÃ©tÃ©s consultÃ©es ont Ã©galement indiquÃ© que 60 % des serveurs virtualisÃ©s ne sont pas couverts par leur plan de reprise aprÃ¨s incident actuel. Ce chiffre reprÃ©sente une augmentation importante par rapport aux 45 % rapportÃ©s par les sociÃ©tÃ©s consultÃ©es en 2009.

Des outils, une sÃ©curitÃ© et un contrÃ´le inadÃ©quats

La multiplicitÃ© des outils utilisÃ©s pour la gestion et la protection des applications et des donnÃ©es dans les environnements virtuels est Ã l'origine de difficultÃ©s majeures pour les DSI. En particulier, prÃ¨s de 6 personnes interrogÃ©es sur 10 (58 %) ayant rencontrÃ© des problÃ¨mes pour protÃ©ger les applications stratÃ©giques dans les environnements virtuels et physiques indiquent qu'il s'agit lÃ d'une prÃ©occupation importante pour leur entreprise.

Concernant le cloud computing, les sociÃ©tÃ©s consultÃ©es ont dÃ©clarÃ© exÃ©cuter prÃ¨s de la moitiÃ© de leurs applications dans un environnement virtualisÃ©. Deux tiers (66 %) rapportent que la sÃ©curitÃ© est leur principale prÃ©occupation vis-Ã -vis de la virtualisation des applications.

Cependant, leur principale difficultÃ© dans l'implÃ©mentation du cloud computing et la virtualisation du stockage rÃ©side dans le contrÃ´le du failover et la haute disponibilitÃ© des ressources (55 %).

Les problÃ¨mes de ressources et de capacitÃ© de stockage pÃ©nalisent la sauvegarde

Les personnes interrogÃ©es dÃ©clarent que 82 % des sauvegardes ne sont effectuÃ©es qu'une fois par semaine, voire moins frÃ©quemment, plutÃ´t que quotidiennement. Le manque de ressources et de capacitÃ© de stockage, ainsi qu'une adoption incomplÃ¨te de mÃ©thodes de protection avancÃ©es plus efficaces empÃªchent le dÃ©ploiement rapide d'environnements virtuels. En particulier :

â□¢ 59 % des personnes interrogÃ©es considÃ¨rent le manque de ressources (personnel, budget et espace) comme le principal problÃ¨me pour la sauvegarde des machines virtuelles.

â□¢ Elles dÃ©clarent que le manque de capacitÃ© de stockage principale (57 %) et de secours (60 %) gÃªne la protection des donnÃ©es stratÃ©giques.

â□¢ 50 % des entreprises consultÃ©es utilisent des mÃ©thodes avancÃ©es (sans client) pour rÃ©duire les rÃ©percussions de la sauvegarde des machines virtuelles.

Ã□cart entre la durÃ©e des arrÃªts du systÃ¨me et la restauration

L'Ã©tude a montrÃ© que la durÃ©e nÃ©cessaire Ã la reprise dâ□□activitÃ©s aprÃ¨s incident est deux fois plus longue que ce que croient les personnes interrogÃ©es. Lorsqu'on leur a demandÃ© ce qui se passerait si le datacenter principal de leur entreprise Ã©tait frappÃ© par un incident majeur, elles ont dÃ©clarÃ© :

â□¢ Estimer Ã deux heures le temps nÃ©cessaire pour redevenir opÃ©rationnelles Ã la suite d'une panne, contre quatre en 2009.

â□¢ La durÃ©e moyenne d'arrÃªt du systÃ¨me Ã la suite d'une panne au cours des 12 derniers mois Ã©tait de cinq heures, soit plus du double des deux heures attendues.

â□¢ Au cours de cette pÃ©riode, les entreprises ont enregistrÃ© en moyenne quatre arrÃªts du systÃ¨me.

Principales causes des arrÃªts du systÃ¨me

Concernant les principales causes des arrÃªts de leurs systÃ¨mes au cours des cinq derniÃ¨res annÃ©es, les entreprises consultÃ©es ont citÃ© les mises Ã jour du systÃ¨me, des pannes de courant ou d'autres pannes, ainsi que les cyberattaques. Plus prÃ©cisÃ©ment :

â□¢ 72 % mentionnent des pannes liÃ©es Ã des mises Ã jour entraÃ®nant 50,9 heures d'arrÃªt du systÃ¨me.

â□¢ 70 % mentionnent des pannes de courant et d'autres pannes entraÃ®nant 11,3 heures d'arrÃªt.

â□¢ 63 % mentionnent des pannes rÃ©sultant de cyberattaques au cours des 12 derniers mois ayant entraÃ®nÃ© 52,7 heures d'arrÃªt des systÃ¨mes.

Cette Ã©tude a Ã©galement rÃ©vÃ©lÃ© un Ã©cart entre les entreprises victimes de pannes de courant et techniques, et celles qui ont effectuÃ© une Ã©tude d'impact de ces pannes : curieusement, seules 26 % des sociÃ©tÃ©s consultÃ©es ont effectuÃ© une Ã©tude d'impact des

pannes de courant et techniques.

Citations et recommandations

â□¢ Â« *En adoptant de nouvelles technologies telles que la virtualisation et le cloud computing pour rÃ©duire leurs coÃ»ts et amÃ©liorer leurs actions pour la reprise dâ□□activitÃ©s aprÃ¨s incident, les entreprises ajoutent de la complexitÃ© Ã leur environnement et laissent leurs applications et donnÃ©es stratÃ©giques sans protection* Â», dÃ©clare **Vincent Videlaine**, directeur du Storage and Availability Management Group de Symantec. Â« *Les entreprises adopteront des outils qui fournissent des solutions globales avec une politique rÃ©guliÃ¨re Ã travers tous les environnements. Les DSI doivent tout de mÃªme privilÃ©gier la simplification et la standardisation pour se concentrer sur les meilleures pratiques fondamentales afin de rÃ©duire la durÃ©e des arrÃªts.* Â»

â□¢ Ã□galitÃ© de traitement pour tous les environnements : les donnÃ©es et les applications stratÃ©giques doivent Ãªtre traitÃ©es de la mÃªme maniÃ¨re dans tous les environnements (virtuels, de cloud computing, physiques) en termes d'Ã©valuation et de planification de la reprise aprÃ¨s incident.

â□¢ Utilisation d'outils intÃ©grÃ©s : en rÃ©duisant le nombre d'outils servant Ã la gestion des environnements physiques, virtuels et de cloud computing, les entreprises gagnent du temps, rÃ©duisent leurs coÃ»ts de formation et sont mieux en mesure d'automatiser les processus.

â□¢ Simplification de la protection des donnÃ©es : en adoptant des mÃ©thodes de sauvegarde non intrusives et la dÃ©duplication, les entreprises sauvegardent les donnÃ©es stratÃ©giques de leurs environnements virtuels et les dupliquent hors site plus efficacement.

â□¢ Planification et automatisation pour rÃ©duire les arrÃªts des systÃ¨mes : il est essentiel de hiÃ©rarchiser les activitÃ©s et les outils de planification chargÃ©s d'automatiser et d'exÃ©cuter les processus qui rÃ©duisent les temps d'arrÃªt pendant la mise Ã jour des systÃ¨mes.

â□¢ Anticiper les problÃ¨mes : cela implique de mettre en place des solutions qui dÃ©tectent les problÃ¨mes, rÃ©duisent la durÃ©e des arrÃªts et assurent une reprise plus rapide et plus conforme aux besoins de l'entreprise.

â□¢ Ã□viter les raccourcis : les entreprises doivent mettre en Å□uvre des technologies et des processus simples pour la protection en cas de panne, mais Ã©viter tout raccourci susceptible d'avoir des consÃ©quences dÃ©sastreuses.