
Six conseils pour la Protection des Données au sein des PME

Introduction

Tout comme les grandes entreprises, les petites et moyennes entreprises (PME) présentent une dépendance croissante à l'égard des données vitales stockées sur leurs serveurs. Des ressources limitées et la vulnérabilité aux interruptions font courir des risques accrus aux PME, et la confiance en une sauvegarde native pour un petit serveur d'entreprise peut créer des lacunes dans le plan de reprise d'activité. Alors que la sauvegarde native pour Windows Small Business Server offre un degré limité de protection, une sauvegarde sur bandes régulière peut rendre les PME vulnérables aux pertes de données et de temps dans des proportions qu'elles ne peuvent se permettre. La clé d'une solution efficace réside dans un plan de reprise d'activité complet, avec notamment un accès rapide à une copie à jour de vos données. Ce livre blanc fournit six conseils pour une stratégie de protection des données vitales dans les PME. Ces conseils, utilisés avec Double-Take[®] Availability de Double-Take[®] Software, peuvent aider les PME à se préserver des interruptions paralysantes et des pertes de données.

Dépendance à l'égard des données

Peu importe que vous soyez une très grande entreprise ou une PME, il est plus probable qu'improbable que vous dépendiez de vos données pour vos activités courantes. Des événements récents, tels que des pannes d'électricité localisées, des virus complexes et des catastrophes naturelles nous rappellent combien les données électroniques vitales peuvent être vulnérables¹, mais des études indiquent que les petites et moyennes entreprises (PME) prennent peu de mesures pour se protéger contre la perte de données. Dans un article récent, Gartner déclare que la direction des PME néglige en général ce qui peut être considéré comme des scénarios de sinistre « hypothétiques ».²

Non seulement les risques évoluent, mais la culture de l'entreprise également. Parmi les nouveaux facteurs renforçant l'impact des données perdues, citons la croissance exponentielle des données vitales générées chaque jour, les attentes des clients en termes de rétablissement rapide des services après une interruption d'activité et le besoin grandissant d'un accès continu à l'information.

Les défis actuels en termes de protection des données engendrent des risques importants pour les entreprises de toutes tailles, mais les PME rencontrent les risques les plus élevés. Souvent, elles ne disposent pas du personnel ou du budget pour une reprise d'activité acceptable et d'un plan en place, ou d'un site de reprise, ou celui-ci n'est pas suffisamment éloigné pour protéger le site principal en cas de catastrophe naturelle. Les PME possèdent en général leurs données vitales sur un seul serveur. Si le serveur tombe en panne, la plupart doivent le remettre en service et le restaurer complètement de suite, sous peine de conséquences coûteuses. En outre, les PME dans des secteurs réglementés sont soumises aux mêmes exigences de disponibilité des données et de protection que les grandes entreprises (par exemple, réglementations de type HIPAA, FDA Part 11, Sarbanes-Oxley et SEC Rule 17), mais sans les budgets nécessaires pour les remplir. Enfin, les conséquences financières sont souvent fatales aux PME. Dans son article sur les pannes informatiques dans la perspective des PME, Adian McDermott estime que l'interruption peut coûter à une petite entreprise entre 200 et 800 dollars par incident, par PC.³

Small Business Server : la sauvegarde native suffit-elle ?

Microsoft® Windows® Small Business Server (SBS) offre une flexibilité et une capacité supérieures pour les PME en proposant nombre des fonctionnalités utilisées par les grandes entreprises : courrier électronique, connexion Internet, sites Web, accès distant, prise en charge des périphériques mobiles, partage de fichiers et d'imprimantes, sauvegarde et restauration. SBS fournit également un utilitaire natif pour effectuer une sauvegarde régulière de base. Toutefois, se fier à une sauvegarde native pour couvrir tous les aspects d'une urgence ou d'un sinistre risque de rendre l'entreprise vulnérable à d'éventuelles lacunes de protection. La sauvegarde sur bande et sur disque ne permet de restaurer des données que jusqu'au point de la dernière sauvegarde correcte, soit le plus probablement la nuit passée : toutes les données créées depuis ce point seront perdues. Si la sauvegarde la plus récente est incomplète ou altérée, vous êtes alors obligé d'utiliser la précédente et perdez davantage de données. En outre, le délai de restauration de la sauvegarde peut ne pas respecter les objectifs en la matière car il faut restaurer les données du support de la sauvegarde native vers un disque avant de pouvoir les utiliser.

Planifier, clé de la réussite

Bien qu'une perspective optimiste joue un rôle majeur dans le développement d'une petite entreprise, la préparation au sinistre suppose pour son efficacité d'envisager le pire. Dans un article récent sur la continuité d'activité, l'association américaine des PME (United States Small Business Association ou SBA) a qualifié les petites entreprises

¹ Dans son article de Global Finance intitulé « Is Today's World Becoming Riskier? » (Le monde moderne présente-t-il plus de risques ?), le financier international Ajay Garg déclare que, bien qu'il soit impossible de répondre à sa question d'un point de vue technique, la nature du risque a changé en raison de la dépendance technologique croissante.

² Witty, Roberta J., et al. « SMBs Must Raise Awareness of Importance of Business Continuity/Disaster Recovery » (Les PME doivent mieux sensibiliser à l'importance de la continuité/reprise d'activité), Gartner.com, 5 novembre 2005.

³ McDermott, Adian. « A Small Business Approach to Computer Downtime » (Pannes informatiques dans la perspective des PME), www.user_groups.net.

d'épine dorsale de l'économie du pays. La SBA déclare que les petites entreprises représentent seules plus de 99 % de l'ensemble des entreprises comptant des salariés, emploient 50 % de l'ensemble des effectifs du secteur privé et génèrent près de 45 % la masse salariale du pays. Toutefois, les PME s'avèrent les plus vulnérables en cas de sinistre car la plupart n'ont pas pris les mesures requises pour se préparer. Bien qu'il soit difficile de contester l'importance de préparer votre entreprise à un sinistre, il reste facile de reporter la planification et le déploiement d'un plan en raison des préoccupations courantes et des contraintes de ressources. Cependant, la SBA estime que 25 à 40 % des entreprises ne rouvrent pas après un sinistre ou une interruption d'activité durable. À la lumière des récentes catastrophes naturelles et du contexte politique actuel, la SBA insiste sur le fait que la reprise d'activité des PME après un sinistre *dépend de la qualité de leur préparation à présent.*

Voici quelques questions que les PME doivent se poser :

- Sommes-nous préparés à un déménagement temporaire ?
- Disposons-nous de copies des données métier vitales et d'un accès à celles-ci ? (La SBA recommande de stocker les copies de sauvegarde sur un site distant, à au moins 80 kilomètres du site principal.)
- Disposons-nous d'un accès aux applications métier stratégiques ? (solution d'urgence pour la paie, la comptabilité, l'accès aux fournisseurs et ressources)
- Quel volume de données serait perdu en cas d'incident entre des sauvegardes ?
- Quel serait le délai de reprise d'activité ?
- Combien de temps allons-nous rester sans contact avec nos clients ?

Scénario de risque courant

Mardi, 16 heures. Le serveur tombe en panne chez le cabinet d'avocats Martin et Jeanson. Le personnel ne peut plus accéder au courrier électronique, la base de données des clients, le calendrier de rendez-vous, le calendrier des audiences, les données d'études et les répertoires de projets. Dans le meilleur des cas, d'ici mardi soir, le revendeur arrive avec les pièces nécessaires pour réparer le serveur et restaure la machine à partir de la sauvegarde sur bande de la nuit du lundi. D'ici mercredi matin, les utilisateurs peuvent reprendre leur activité, mais toutes les données et les heures de travail du mardi sont perdues. Un scénario plus probable est que le revendeur ne dispose pas de toutes les pièces en stock ou d'un technicien pour les installer. Il commande des pièces de rechange, mais ne les reçoit pas avant mercredi. Mercredi après-midi, il répare le serveur et lance la restauration à partir de la sauvegarde sur bande de la nuit du lundi. Le jeudi matin, les utilisateurs peuvent reprendre leur activité, mais les données les plus récentes dont ils disposent datent de la nuit de lundi. Deux journées de données et de productivité sont perdues. Dans le pire des cas, le revendeur ne dispose pas de toutes les pièces en stock. Il commande des pièces de rechange, mais ne les reçoit pas avant mercredi. Le mercredi après-midi, il répare le serveur et tente d'effectuer la restauration à partir de la sauvegarde sur bande de la nuit de lundi, mais sa qualité est telle qu'il doit restaurer celle de la nuit de dimanche. Le jeudi matin, les utilisateurs ont de nouveau accès aux applications du serveur, mais pas aux données postérieures au dernier week-end.

Que peut faire une PME pour minimiser l'impact potentiellement paralysant d'une perte de données ou d'une interruption ? Les six conseils suivants peuvent aider les PME à protéger plus efficacement leurs données vitales et à accélérer la reprise d'activité.

Six conseils pour protéger les données vitales

Conseil 1 – *Priorité aux personnes, politiques et procédures* Il est recommandé de mettre en place des personnes qualifiées, des politiques et procédures adéquates avant d'étudier la stratégie technologique. Désignez une personne dans l'entreprise en tant que responsable de la protection des données, chargé d'obtenir l'adhésion de la direction, de documenter les processus, d'analyser les options et de piloter les tests et la formation.

Ce responsable doit former un groupe pour déterminer la nature des données les plus vitales pour l'entreprise. Ce petit groupe doit intégrer les personnes dont l'avis va permettre de protéger les données métier les plus vitales. Dans une petite entreprise, il peut s'agir simplement de l'actionnaire ou de la direction. Dans une entreprise moyenne, un directeur de chaque fonction est probablement le plus judicieux. Le responsable de la protection des données doit identifier toutes les réglementations pertinentes qui influent sur les priorités en ce domaine de l'entreprise. Le groupe doit ensuite définir les applications stratégiques. Compte tenu des ressources limitées dans la plupart des PME, concentrez-vous au départ sur une ou deux applications clés dont l'inaccessibilité des données peut rapidement engendrer une perte financière (par exemple, site de commerce en ligne, base de données clients ou système de courrier électronique). L'accent mis sur la protection d'une ou deux applications stratégiques permet d'atteindre plus facilement les objectifs en termes de protection des données.

Conseil 2 – Stocker les données sur un site distant

Il est extrêmement important de stocker les données sur un site distant et à l'abri. De préférence, ce site est éloigné géographiquement afin de rester préservé en cas de sinistres d'envergure, tels que des séismes ou des ouragans. Envisagez les menaces les plus probables pour votre lieu d'activité.

Des coupures d'électricité locales se produisent-elles ? À quelle distance devez-vous stocker les données pour que le réseau électrique soit différent ?

Des séismes ou des ouragans se produisent-ils ? Conservez les données de sauvegarde à au moins 80 kilomètres du site principal.

Des pannes de serveur sont-elles probables ? Considérez les actions possibles pour accélérer la restauration du serveur de production.

Innovez pour définir un mode de sauvegarde rentable des données à distance. Par exemple, si votre siège se trouve à Paris et que votre administrateur informatique réside en banlieue, vous pouvez envisager d'installer un serveur de sauvegarde à son domicile connecté au serveur principal par ADSL ou câble.

Conseil 3 – Calculer les coûts des interruptions

Pour que votre direction apprécie la gravité du problème, vous aurez peut-être à estimer les coûts des interruptions pour les employés, les fournisseurs et les clients s'ils ne peuvent accéder aux données vitales. La méthode suivante permet d'estimer simplement le coût moyen par heure d'interruption.

Coût par incident = $(T_o + T_d) \times (H_r + L_r)$, où T_o = Durée de la panne et T_d = Ancienneté de la sauvegarde (de quand date la dernière sauvegarde ?)

Hr = Taux horaire du personnel (calcul du coût mensuel par service divisé par le nombre d'heures de travail)

Lr = Perte de chiffre d'affaires par heure (applicable si le service génère du profit. Une bonne règle consiste à évaluer la rentabilité sur trois mois et à diviser par le nombre d'heures de travail)

Définissez ensuite les objectifs de restauration pour vos applications. Pour ce faire, évaluez l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO) pour chaque application. Le RTO d'une application indique simplement en combien de temps vous devez restaurer ses données. Par exemple, 4 heures, 8 heures ou le jour ouvré suivant peut être tolérable pour des systèmes de courrier électronique. Le RPO d'une application indique la quantité de données que vous pouvez vous permettre de perdre depuis la dernière sauvegarde. S'agit-il de 2 minutes, 20 minutes ou 2 heures ? Estimez ensuite les coûts pour atteindre les RTO et RPO de chaque application.

En dernier lieu, faites comprendre et valider vos estimations des coûts d'interruption par votre direction, ainsi que les objectifs RTO et RPO nécessaires. Une fois tout le monde d'accord sur les coûts d'interruption et les objectifs RTO et RPO de l'entreprise, il s'avère plus facile de convenir de la stratégie et du budget pour la protection des données. Par exemple, si les actionnaires ou les dirigeants de l'entreprise conviennent que les coûts d'interruption atteignent environ 50 000 euros par an, ils vont très probablement accepter qu'un budget de 25 000 euros soit consacré à la protection des données.

Conseil 4 – Dépasser le cadre de la sauvegarde sur bande

Après avoir établi en combien de temps vous devez restaurer les applications stratégiques (RTO), la quantité de données que vous pouvez vous permettre de perdre (RPO) et votre budget, vous pouvez choisir la solution technologique adéquate. Comme de nombreuses PME, vous allez certainement découvrir que la technologie de sauvegarde classique ne suffit pas pour atteindre les objectifs RTO et RPO des applications stratégiques, en raison de sa propension à échouer et du délai de restauration avant de pouvoir accéder de nouveau aux données.

Si vos applications stratégiques s'exécutent sur plusieurs sites distants, la qualité et la cohérence des sauvegardes sur bandes locales posent aussi problème. Peu d'entreprises, quelle qu'en soit la taille, disposent sur ces sites de techniciens capables de nettoyer et de gérer les bandes, de vérifier qu'elles contiennent bien les données de sauvegarde et d'exécuter une restauration en cas de besoin.

Les PME font face à un dilemme : les systèmes de sauvegarde sur bande sont économiques et assez fiables, mais incompatibles avec les objectifs RPO et RTO élevés des applications stratégiques, et en général inefficaces pour les sites distants. La technologie de mise en miroir matérielle, qui utilise une copie distante pour permettre une mise en miroir synchrone entre deux sites, offre un excellent RPO, mais s'avère très coûteuse pour une PME, tant en termes d'achat que de gestion. En outre, elle est loin d'être idéale pour sauvegarder des sites distants qui présentent souvent des liaisons à bas débit, la mise en miroir matérielle exigeant une importante bande passante dédiée entre les sites.

Les solutions basées sur la réplication logicielle asynchrone peuvent atteindre l'objectif RPO acceptable pour les applications stratégiques sans le coût et la complexité de la réplication synchrone. La réplication logicielle ne porte que sur les blocs modifiés. Par rapport aux solutions de réplication synchrone, cette méthode crée une moindre charge sur les serveurs de production, accélère l'actualisation et permet de copier les données via des liaisons Internet à faible bande passante. Les solutions de réplication logicielle permettent également un basculement des applications et des serveurs pour un excellent RTO, les utilisateurs pouvant reprendre leur activité quelques minutes après une panne.

Conseil 5 – Faciliter la restauration directement par les utilisateurs

La plupart des PME ne disposent pas des ressources informatiques pour traiter des demandes individuelles de restauration de fichiers. Heureusement, des solutions comme Microsoft Windows Storage Server 2003 facilitent la restauration par les utilisateurs eux-mêmes. Par exemple, vous pouvez configurer Windows Storage Server 2003 pour créer un snapshot des données sur un serveur deux fois par jour. Si un utilisateur supprime ou effectue par accident des modifications définitives dans un document, il lui suffit de le sélectionner dans n'importe quel snapshot par un clic droit sur le fichier, de choisir Propriétés, d'afficher toutes les versions du fichier et de sélectionner celle voulue.

Conseil 6 – Vérifier la capacité de restauration Il est important de s'assurer que vous avez bien planifié la restauration optimale de vos applications stratégiques, en local ou sur un site différent. Pouvez-vous accéder rapidement à tous les éléments nécessaires pour la restauration ? Quelles sont les étapes spécifiques pour restaurer un serveur en panne ? Quelle serait la procédure si vous deviez transférer les activités et le personnel de l'entreprise sur un autre site ?

Double-Take Availability peut vous aider à effectuer une restauration sur un autre site ou une reprise rapide d'un site. Cette solution ne répliquant que les données modifiées, elle fonctionne bien sur de longues distances, même en cas de liaisons à bas débit.

Double-Take[®] Availability – La solution pour les PME

Double-Take Availability est la solution la plus efficace pour les petites et moyennes entreprises qui souhaitent bénéficier des avantages en termes de protection des données de la réplication logicielle asynchrone.

Double-Take Availability offre une solution éprouvée pour la réplication en temps réel des données vitales et un basculement automatisé afin d'assurer la disponibilité des applications. Double-Take Availability, certifié Microsoft[®] Windows[®] 2000 et 2003 à tous les niveaux, est l'un des seuls produits de réplication dans ce cas. **Il permet une protection comparable ou supérieure à de nombreuses solutions matérielles, mais à un coût bien plus abordable.**

Double-Take Availability réplique les modifications des fichiers par octet d'un serveur Windows vers un autre via tout réseau IP. Installé sur chaque serveur, le logiciel contrôle les modifications en temps réel apportées aux fichiers et les réplique vers un autre serveur pour les appliquer à une copie secondaire des données. Toutes les modifications sont transmises et appliquées dans l'ordre logique exact où elles surviennent sur le serveur de production, garantissant une copie cohérente des données sur le système secondaire.

Dépasser la protection minimale

Double-Take Availability ne se limite pas à la protection minimale des sauvegardes régulières en offrant une réplication des données continue sur disque, assurant une perte de données infime et une reprise rapide en cas de sinistre ou panne, à un coût abordable pour les PME.

Double-Take Availability enregistre en permanence les modifications au niveau octet effectuées et les répliques en local ou sur un site de reprise distant. Les modifications étant enregistrées en quasi temps réel, en cas de panne de disque, coupure de courant, erreur humaine ou catastrophe naturelle, vous ne perdez que quelques secondes de données, au lieu d'heures ou de jours entiers. Contrairement à d'autres solutions coûteuses qui limitent vos options de couverture géographique ou nécessitent des connexions réseau spéciales, Double-Take Availability fonctionne sans contrainte de distance à l'aide des réseaux IP existants, voire Internet. Vous pouvez placer le serveur cible aussi loin que souhaité pour garantir une protection maximale contre les sinistres.

Double-Take Availability ne répliquant que les octets modifiés, la bande passante utilisée pour sauvegarder les données reste minimale. Des fonctionnalités telles que la planification flexible du débit et la compression intelligente permettent de contrôler l'exécution de la réplication et la quantité de bande passante que le logiciel est autorisé à utiliser.

En cas de sinistre, la copie sur disque secondaire des données sert à restaurer rapidement le serveur de production. Double-Take Availability est indépendant du serveur, du matériel de stockage, du réseau et des applications, et fonctionne avec les services actuels.

Basculement de serveur intégral : ne limitez pas la protection à vos données

Double-Take Availability protège non seulement vos données, mais aussi vos systèmes. La fonctionnalité de basculement de serveur intégral garantit une protection complète, notamment du système d'exploitation, des applications et des données. Cette fonctionnalité se conjugue à des outils de pointe pour la protection de l'état du système et la restauration avec la réplication en temps réel, assurant la disponibilité des applications selon le besoin sans engendrer une complexité excessive pour les PME. Un simple clic sur un bouton suffit à restaurer complètement les systèmes. La fonctionnalité de basculement de serveur intégral protégeant l'état système du serveur de production, il est inutile de gérer isolément des service packs, des mises à jour d'application ou des correctifs sur le serveur secondaire, réduisant davantage la complexité inhérente au maintien de la disponibilité des applications.

Autre scénario de reprise avec Double-Take Availability

Double-Take Availability étant à présent installé à la fois sur le serveur principal et un serveur de secours économique situé au domicile de l'administrateur, le cabinet d'avocats Martin et Jeanson dispose d'une solution surpassant même le meilleur des cas décrit précédemment.

Mardi, 16 heures. Le serveur tombe en panne chez le cabinet d'avocats Martin et Jeanson. Le personnel ne peut plus accéder au courrier électronique, la base de données des clients, le calendrier de rendez-vous, le calendrier des audiences, les données d'études et les répertoires de projets. En moins de 15 minutes, Double-Take Availability a basculé automatiquement sur le serveur de secours, qui contient toutes les données jusqu'au mardi à 16 heures, au moment même de la panne du serveur de production. Les utilisateurs peuvent accéder à toutes les applications. Le mardi soir, le revendeur ou l'intégrateur arrive avec les pièces nécessaires pour réparer le serveur de production d'origine et lance sa resynchronisation à partir du serveur de secours, les utilisateurs pouvant toujours accéder à toutes leurs données intactes du mardi et sans impact sur l'activité du cabinet.⁴

Résumé

Comme les grandes entreprises, les petites et moyennes entreprises présentent une dépendance croissante à l'égard des données vitales stockées sur leurs serveurs. Toutefois, des ressources limitées et la vulnérabilité aux interruptions font courir des risques accrus aux PME. Auparavant, elles pouvaient se contenter de gérer cette situation, mais plus maintenant. En outre, se fier à une sauvegarde native pour les serveurs crée une menace pour la pérennité de l'entreprise, les statistiques indiquant qu'une grande proportion des PME qui subissent un sinistre doivent cesser leur activité. Alors que la sauvegarde native pour Windows Small Business Server offre un degré limité de protection, une sauvegarde sur bandes régulière peut rendre les PME vulnérables à d'importantes pertes de données et de temps en cas de sinistre. La clé d'une solution efficace réside dans un plan de reprise d'activité complet, avec notamment un accès rapide à une copie à jour de vos données. Double-Take Availability offre une solution de protection et de reprise complète à un coût abordable pour les PME.

⁴ Même dans le pire des cas où le revendeur doit commander des pièces, les utilisateurs peuvent continuer à travailler sur le serveur cible jusqu'à la restauration du serveur principal.

116 118 avenue Paul Doumer
92500 Rueil Malmaison
+33 1 47 77 1500
visionsolutions.com

© Copyright 2007, Vision Solutions, Inc. Tous droits réservés. IBM et System i sont des marques commerciales d'International Business Machines Corporation.

