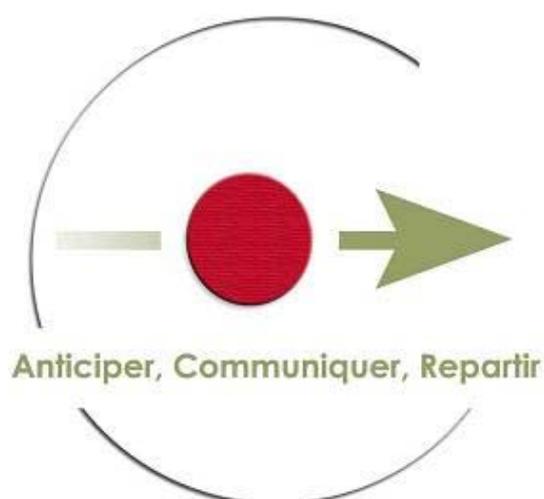


MAITRISEZ VOTRE SYSTEME DE SAUVEGARDE



FORUM 2006

" L'entreprise face aux risques industriels et environnementaux :
Anticiper, Communiquer et Repartir en cas de crise. "

PREFACE

La sauvegarde trop souvent oubliée des directions informatiques

Dans le courant de l'année 2000, 49% des entreprises européennes étaient incapables d'estimer la valeur de leurs données informatiques. En 2003, le Clusif publie des rapports éloquentes: 84% des entreprises françaises ne possèdent aucun plan de secours pour maintenir leur activité en cas de perte des ressources informatiques. Un dernier chiffre enfin, pour relier les précédents : 50% des entreprises qui subissent un sinistre important sans être équipées d'un système de sauvegarde pertinent meurent dans les deux ans qui suivent ledit sinistre.

Toute entreprise aimerait pouvoir se remettre instantanément d'un sinistre sans aucune perte de données. Si cet objectif est, soyons réaliste, impossible à atteindre, il est toutefois possible de tendre vers un niveau d'efficacité satisfaisant. Nous mettons à votre disposition, dans ces pages, les techniques et connaissances dont vous aurez besoin pour remettre en question vos sauvegardes.

Les techniques de sauvegardes sont nombreuses, modulables et peuvent être imbriquées à souhait. Le premier chapitre présente les trois principales familles de solutions, leurs avantages et inconvénients ainsi qu'une idée du coût de déploiement et de maintien.

Sauvegarder intelligemment pour repartir efficacement revient à formaliser ses objectifs de reprise en termes de RTO (*Recovery Time Objective*) et de RPO (*Recovery Point Objective*). Le RTO spécifie le délai maximum que l'entreprise tolère avant de reprendre son activité. Le RPO, pour sa part, désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une avarie. L'une ou l'autre de ces notions, voire un mélange intelligent des deux, sera à la base de votre politique de sauvegarde. Nous aborderons ce sujet dans le deuxième chapitre.

Enfin, il convient de remettre en question régulièrement son système de sauvegarde afin de l'adapter aux évolutions du système informatique. Ce que vous trouverez dans ces pages est à interpréter dans votre système d'information, et c'est certainement là que vous rencontrerez le plus de difficultés. Gardez bien à l'esprit que c'est un travail de longue haleine, fastidieux et parfois ingrat, mais qui peut aussi sauver votre entreprise en cas de sinistre.

SOMMAIRE

1. LES SOLUTIONS TECHNIQUES	3
1.1. Solution DAS (Directly Attached Storage).....	3
1.2. Solution réseau	5
1.3. Télésauvegarde	9
2. SAUVEGARDER INTELLIGEMMENT POUR REPARTIR EFFICACEMENT	12
2.1. Évaluer le point de reprise des données (RPO).....	12
2.2. Évaluer son temps de reprise maximum (RTO).....	12
2.3. Évaluer le coût de la perte / destruction des données.....	12
2.4. Quoi sauvegarder ?.....	13
2.5. Définir une politique de sauvegarde pertinente	14
CONCLUSION	15
BIBLIOGRAPHIE.....	16
CONTACTS.....	16

1. LES SOLUTIONS TECHNIQUES

1.1. SOLUTION DAS (DIRECTLY ATTACHED STORAGE)

Les solutions de stockage de type D.A.S. (Direct Attached Storage) consistent à connecter directement un périphérique au serveur ou à la station de travail. Il s'agit principalement d'un lecteur de bandes magnétiques mais d'autres solutions peuvent être envisagées comme le support optique ou les disques durs externes.

Le matériel existant

La bande magnétique

La bande magnétique est un support utilisé depuis 1950 pour le stockage d'information numérique. Il existe deux types de bandes : hélicoïdale¹ et linéaire².



Bande DDS-4

Ces technologies offrent une capacité de stockage importante. Les dernières générations de lecteurs peuvent atteindre une capacité de stockage maximale de 600 Go (Giga-octets).

Afin d'automatiser une partie du processus, les robots de sauvegarde acceptent plusieurs bandes magnétiques dont le chargement est automatisé.

Pour automatiser le processus de sauvegarde, les lecteurs de bande doivent être accompagnés d'un logiciel. Les grands constructeurs proposent leurs outils à un prix non négligeable. Microsoft intègre l'outil NtBackup dans tous les Windows Server mais ses performances ne sont pas excellentes. Les solutions libres sont présentes avec l'outil Amanda, mais nécessitent des compétences sur les systèmes Linux.

Autres supports amovibles

Il y a d'autres solutions possibles mais elles restent limitées par leur taille. Nous retiendrons uniquement les supports optiques (CD-ROM et DVD) et les disques durs externes.



CD-R

Les supports optiques offre une faible capacité (80 Mo à 9 Go voire plus dans l'avenir). Les vitesses de gravure sont assez lentes et il n'y a aucune automatisation du système. Les disques durs offrent un stockage de masse avec un temps d'accès très faible et un taux de transfert élevé par les interfaces USB2.0 et IEEE1394. Il est possible d'automatiser le processus de sauvegarde par des scripts³.

¹ **Hélicoïdale** : technologie utilisée pour écrire sur les bandes magnétiques. Les pistes sont inclinées afin d'optimiser la surface de la bande. La vitesse de défilement de la bande est moins élevée ce qui réduit le risque de casse mais les têtes de lecture sont plus sensibles à la poussière.

² **Linéaire** : [*Linear Tape Open*] technologie utilisée pour écrire sur les bandes magnétiques. Les pistes sont parallèles à la bande offrant un taux de transfert plus élevé mais un risque de casse plus important.

³ Un script est l'automatisation dans un fichier exécutable de traitements informatiques effectué régulièrement.

Avantages & Inconvénients

Avantages

- ✓ Les supports amovibles peuvent être externalisés (il s'agit de mettre les sauvegardes à l'abri en dehors de l'entreprise). Si le lieu de production est très endommagé, les sauvegardes ne seront pas détruites. Cependant, le coût du lieu de stockage est à prendre en compte.
- ✓ Le coût de l'investissement est abordable à toutes PME, quelque soit sa taille.

Inconvénients

- ✓ La permutation des supports de stockage n'est pas entièrement automatisée. Il est soumis aux erreurs humaines (oubli, perte, etc.).
- ✓ Les supports sont fragiles. Ils peuvent subir des chocs et des rayures. Les bandes magnétiques sont plus ou moins fragiles selon leur vitesse de défilement. Leur durée de vie est limitée à 200 / 300 passages. Quant aux lecteurs, ils sont sensibles à la poussière. Afin de faciliter leur remplacement, il est conseillé d'utiliser un type de bande standard. Les supports optiques peuvent, dans les cas les plus extrêmes, exploser dans le lecteur.
- ✓ Avec le temps, les supports amovibles peuvent se détériorer. Les CD-ROM de mauvaise qualité sont les plus exposés à ce phénomène. La période de conservation d'un support optique est théoriquement d'un siècle, estimation difficile à vérifier puisque la technologie existe depuis seulement une dizaine d'années. Les données stockées sur des bandes peuvent s'effacer au fil du temps. Pour éviter toute perte de données, il est important d'effectuer une réécriture après quelques années.
- ✓ Les applications telles que les bases de données doivent être fermées avant de lancer la sauvegarde. Pendant ce temps, il est impossible d'y effectuer toute modification. Cependant certains logiciels permettent de sauvegarder « à chaud » (c'est-à-dire en cours de fonctionnement) certaines bases de données.
- ✓ Les supports amovibles sont sensibles à l'environnement (électricité, température, humidité...). En particulier, les supports optiques sont facilement rayés et deviennent illisibles.
- ✓ La vitesse de transfert que proposent les lecteurs de bandes et de DVD est relativement faible. Il faut prévoir en moyenne entre deux à cinq heures pour effectuer la sauvegarde ou la restauration de la totalité des informations d'une bande. Le type LTO (Linear Tape Open) permet d'atteindre un débit de 80 Mo/s.

Que choisir ?

Une solution DAS est destinée à effectuer des sauvegardes journalières ou hebdomadaires afin d'externaliser vos données. Cette solution peut être associée à d'autres systèmes de sauvegarde afin d'effectuer des sauvegardes en parallèle.

La stratégie de la bande magnétique est d'effectuer une sauvegarde initiale puis des sauvegardes différentielles. Cela consiste à sauvegarder les fichiers nécessaires en fin de semaine puis à enregistrer les modifications effectuées sur une période donnée, généralement une semaine. À la fin de cette période d'automatisation, la permutation des bandes sera nécessaire.

Le choix du matériel et du type de bande s'effectue selon l'espace nécessaire. Il est possible de stocker énormément d'informations sur une seule bande. Cependant, en cas de dommage sur celle-ci, toutes les informations seront perdues. Les robots de sauvegarde sont prévus pour les sauvegardes importantes sur plusieurs bandes. Ainsi, le risque de perte totale des données est diminué.

Les lecteurs sont accessibles à partir de 400 € HT et les robots de sauvegarde sont disponibles à partir de 2 500 € HT (un lecteur avec 8 bandes). Il faut également prévoir le coût de renouvellement des bandes. En général, on renouvelle un quart du jeu total tous les ans.



Bibliothèque de sauvegarde sur bande

Le support optique est destiné à l'archivage pour conserver les données mortes, c'est à dire les données qui ne seront pas modifiées. Généralement, la sauvegarde est effectuée par l'utilisateur du fichier (ex: comptable, graphiste...). Les graveurs de DVD sont disponibles à partir de 40 € HT. Il est donc facile d'équiper les ordinateurs des personnes qui en ont l'utilité.

Les disques durs externes peuvent effectuer les mêmes opérations qu'un lecteur de bandes mais ils sont plus sensibles au choc.

1.2. SOLUTION RESEAU

Lorsque l'on parle de stockage en réseau, c'est par opposition à l'attachement direct (*les DAS*) où, comme nous venons de le voir, les unités de sauvegarde sont physiquement reliées à un serveur. Dans le cas du stockage en réseau, les unités de sauvegarde sont indépendantes d'un quelconque serveur, elles sont accessibles par le réseau, qu'il soit *Ethernet* ou fibre optique.

Le matériel

Network Attached Storage

Le NAS (*Network Attached System*) est un ensemble de disques durs, typiquement SCSI, regroupés sous la direction d'un contrôleur RAID (*certaines solutions incluent un second contrôleur pour assurer la tolérance de pannes*). L'unité est directement connectée au réseau *Ethernet* de l'entreprise. Le NAS intègre le



NAS

support de multiples systèmes de fichiers réseau, tels que CIFS (*Common Internet File System*, le protocole de partage de fichiers de Microsoft), NFS (*Network File System*, un protocole de partage de fichiers Unix) ou encore AFP (*AppleShare File Protocol*, le protocole de partage de fichiers d'Apple). Une fois connecté au réseau, il peut jouer le rôle de plusieurs serveurs de fichiers partagés.

Un NAS va donc stocker des données partagées, un peu comme un serveur de fichiers mais en plus solide, plus rapide et plus simple à administrer.

Storage Area Network

Le SAN (*Storage Area Network*) est un réseau spécialisé permettant de partager de l'espace de stockage à une librairie de sauvegarde et à des serveurs. Dans le cas du SAN, les baies de stockage n'apparaissent pas comme des volumes partagés sur le réseau. Elles sont directement accessibles en mode bloc par le système de fichiers des serveurs. En clair, chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur. L'administrateur doit donc définir très précisément la zone d'accès que possède un serveur sur le SAN, ceci afin d'éviter qu'un serveur Unix n'accède aux mêmes ressources qu'un serveur Windows utilisant un système de fichiers différent, par exemple.



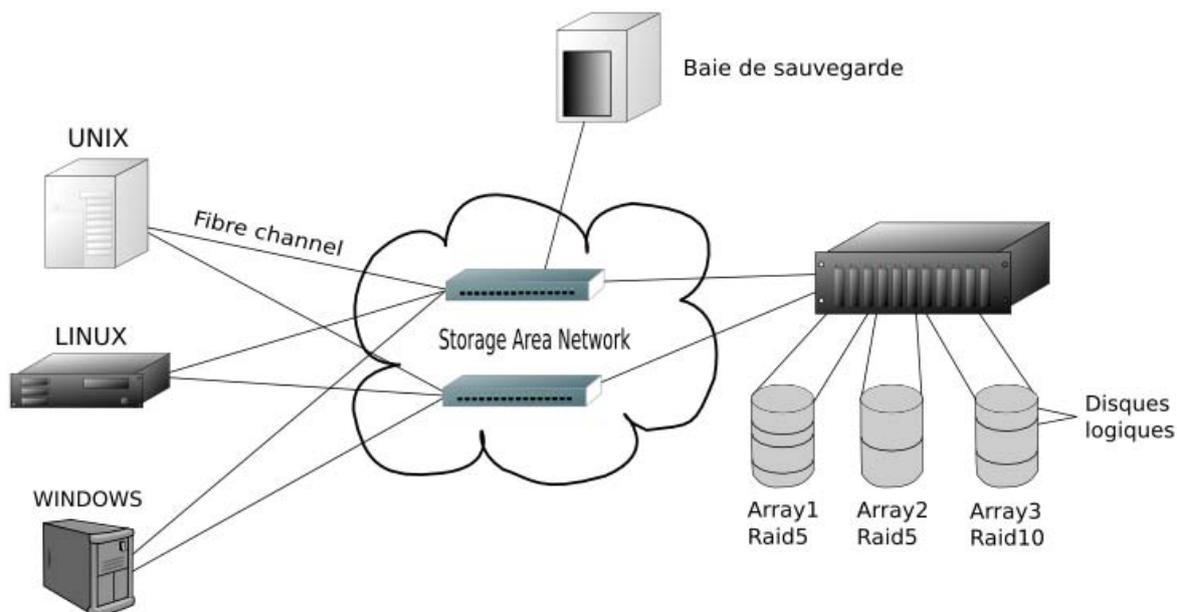
SAN IBM

Cette technologie permet de centraliser les systèmes d'exploitation sur le SAN, protégeant ainsi les données et les configurations des défaillances matérielles.

Le SAN est conçu pour fournir de l'espace disque rapide et fiable. La technologie la plus répandue pour y arriver est la fibre optique. Toutefois, les équipements relatifs à cette dernière étant très coûteux, deux nouvelles technologies ont vu le jour :

- ✓ iSCSI : ce sont des commandes SCSI qui passent sur *Ethernet*
- ✓ AOE : *ATA over Ethernet*, cette technologie est similaire à l'iSCSI mais avec les commandes ATA utilisée sur les connectiques des disques durs. Cette dernière est moins répandue car moins efficace que l'iSCSI.

Il y a encore peu de temps, on ne trouvait des SANs que dans les grands centres informatiques de société ayant besoin d'un grand volume de stockage très sécurisé. Les prix devenant plus raisonnables, des centres informatiques plus modestes s'équipent d'architectures SAN plus simples (*tel que représenté dans le schéma suivant*).



Le réseau SAN est indépendant du réseau *Ethernet* de l'entreprise. C'est ce qui fait sa force : aucune perturbation du trafic, tout le réseau SAN est dédié aux transferts de données. Les serveurs sont donc reliés à deux réseaux : celui de l'entreprise et celui du SAN.

Avantages & Inconvénients

Le stockage en réseau permet une gestion de la sauvegarde simplifiée à l'extrême : toutes les données du système d'information sont stockées dans des baies de disques parfaitement identifiées.

La question de la localisation des données ne se posant alors plus, il est possible de consacrer davantage de temps à leur hiérarchisation, par exemple.

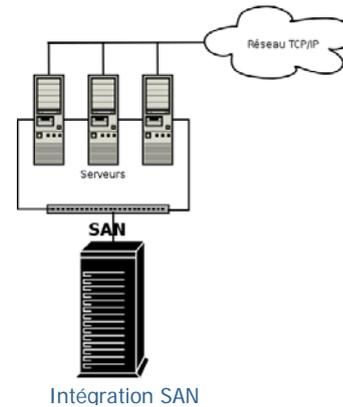
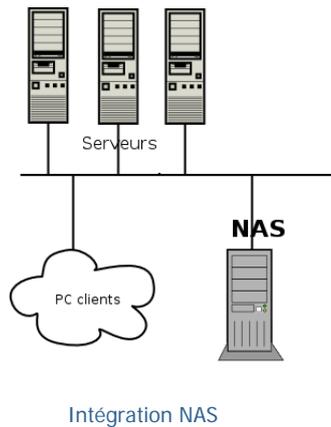
Le stockage en réseau permet des temps de reprises très bas. Il suffit de migrer la liaison du réseau de stockage défectueux vers le réseau de stockage de *backup*, ce qui se résume finalement à un changement d'adresse *IP*.

Il faut faire attention, en revanche, aux points de reprises (*les RTO, que nous aborderons au prochain chapitre*). On peut être tenté, avec ce type de solutions, de mettre en place une synchronisation des données. Veillez à n'utiliser cette dernière que pour des applications à la criticité élevée car une synchronisation peut très bien répandre des données corrompues sur vos *backups* (*corruption du serveur primaire et réplication de la corruption sur les serveurs secondaires*). Prudence donc.

D'un point de vue financier, les systèmes NAS, sont devenus très abordables. On trouve chez les principaux constructeurs (*Dell, HP, IBM, Digital Storage, ...*) des systèmes NAS aux environs de 1 500 € HT. Dell, par exemple, propose un NAS de 320 Go (*sans RAID configuré*), incluant une garantie d'intervention à J+1 sur 3 ans, pour 2 000 € HT.

Les SAN d'entrée de gamme sont beaucoup plus coûteux. Il faudra prévoir un budget d'au moins 10 000 € HT pour s'équiper d'un réseau SAN de petite taille, une structure complète pouvant rapidement coûter plusieurs dizaines de milliers d'euros.

Que choisir ?



NAS et SAN ne répondent pas aux mêmes besoins. Les NAS s'adaptent très facilement à des structures de petite et moyenne taille mais peuvent devenir complexes à administrer quand la quantité de données augmente rapidement. De plus, un NAS est forcément rattaché au site de production.

Les SAN sont coûteux et complexes mais ils offrent une adaptation aux changements d'échelle intéressante et peuvent être délocalisés et accédés par fibre optique, solution coûteuse mais de loin la plus sûre.

Voici un rapide comparatif de ces deux sous-familles :

NAS	SAN
Toutes les machines connectées au réseau local peuvent accéder aux données du NAS.	Seuls les serveurs équipés d'une carte réseau secondaire (<i>typiquement fibre optique</i>) peuvent se connecter au SAN
Les données sont considérées par nom de fichiers ou <i>meta-informations</i> (<i>propriétaire, permissions, etc...</i>)	Le SAN permet de travailler directement sur les blocs du système de fichiers.
Le NAS facilite le partage des données entre des systèmes d'exploitation disparates.	Le partage des données dépend des systèmes d'exploitation.
Le système de fichiers est géré par le contrôleur NAS.	Le système de fichiers est géré par le serveur pour sa zone.
Les sauvegardes sont faites sur les dossiers, donc sur les données existantes. On peut ensuite comparer les images.	Les sauvegardes sont faites sur les blocs, même si ces derniers sont vides. Le système de sauvegarde doit donc être au moins aussi grand que le système en production.

1.3. TELESAUVEGARDE

Une méthode intéressante, appelée télésauvegarde, est proposée par de nombreux prestataires de services. Pour un coût acceptable, diverses solutions sont proposées avec une gamme de services variés. Le principal atout du système de la télésauvegarde est la possibilité d'externaliser une copie de ses données vers un lieu géographiquement très éloigné.

La solution est accompagnée d'un petit logiciel propre au système de sauvegarde. Ce programme doit être installé sur un serveur dédié à la sauvegarde afin d'automatiser le processus. L'entreprise est par conséquent dispensée de mobiliser des ressources humaines pour réaliser ses sauvegardes régulières.

Selon le produit développé par le prestataire de service, des modules de gestion des éléments à sauvegarder sont disponibles et faciles à utiliser. Des systèmes de compression des fichiers existent pour minimiser la taille des données à transmettre. Toujours dans l'optique de transférer un minimum de données, seuls les fichiers modifiés sont envoyés. Quelques outils proposent aussi une sauvegarde des paramètres de configuration d'ordinateurs identifiés, des notifications d'anomalies de sauvegarde ou encore des rapports de sauvegarde.

Les points clefs d'une bonne télésauvegarde

Afin d'optimiser la télésauvegarde, les données doivent être centralisées dans l'entreprise. Il est plus simple de copier le contenu d'un seul serveur plutôt que de rechercher des bribes de données disséminées un peu partout. Typiquement, une bonne politique de télésauvegarde commence par une bonne politique de sauvegarde réseau. Ainsi, vous identifiez clairement où sont vos données, ce qui simplifie considérablement l'implémentation de la télésauvegarde.

Il existe des solutions propriétaires qui permettent de sauvegarder des données réparties en de nombreux points (*ordinateurs clients*) d'un réseau. Ces données sont ensuite centralisées sur une passerelle qui prend en charge l'acheminement vers le prestataire. Si ces solutions évitent la nécessité d'un stockage en réseau, elles rendent généralement la sauvegarde moins fiable et plus lente.

Enfin, une planification judicieuse de la télésauvegarde permet d'optimiser le débit de la connexion Internet. Plusieurs heures sont nécessaires à la réalisation d'une télésauvegarde, prévoyez donc un début de procédure vers 22 heures environ. Vous disposerez ainsi d'au moins neuf heures pour la réalisation complète du processus.

Coût d'une solution de télésauvegarde

Le coût moyen d'une télésauvegarde correspond généralement aux prix indiqués ci-dessous (*moyennes calculées début 2006*). Ce tableau ne prend pas en compte le coût de la liaison, qui peut facilement atteindre plusieurs milliers d'euros par mois.

Espace disponible	Prix mensuel HT
< 5 Go	75 €
< 30 Go	250 €
< 60 Go	500 €
< 100 Go	800 €

Le medium de communication

Connexion SDSL

Pour envoyer les données vers le centre de sauvegarde, il est nécessaire d'établir une liaison entre l'entreprise et celui-ci. La liaison par le biais d'Internet est la plus utilisée du fait de sa simplicité d'installation et de maintenance et de son coût raisonnable.

On utilise une liaison de type SDSL⁴ de façon à pouvoir envoyer et récupérer des données avec un même débit. Le temps de sauvegarde est donc identique au temps de restauration.

Les débits proposés actuellement varient de 4 Mbits/s à 10 Mbits/s pour 1000 € à 1400 €/mois. Toutefois, il est primordial de prendre en compte le taux de disponibilité et le débit garanti. Cette connexion permet de transférer 15 Go par nuit avec une ligne SDSL à 4 Mbits/s.

Liaison spécialisée et fibre optique

Pour remédier à la confidentialité des données, des liaisons spécialisées entre l'entreprise et le prestataire de sauvegarde garantissent encore plus de sûreté.

La fibre optique est un moyen de câblage qui offre un bien meilleur débit de l'ordre du Gigabit. En revanche, le câblage est très coûteux et son installation demeure contraignante. Des distances importantes se révèlent être aussi l'obstacle au choix de cette solution. La fibre optique est fragile et elle exige de l'entretien là aussi assez coûteux.



Fibre Optique

Sécurité

Vos données sont envoyées par une connexion sécurisée SSL (Secure Socket Layer). Différents cryptages sont utilisés pour la transmission des données.

⁴ SDSL (Symmetric Digital Subscriber Line) : liaison Internet dont le débit d'envoi et de réception sont identiques.

Ce procédé protège uniquement la liaison mais il faut rester vigilant quant à la sécurité sur les machines qui émettent et reçoivent ces sauvegardes.

Une solution complète de télésauvegarde est donc disponible à partir de 1 000 € HT par mois en fonction de la liaison choisie et du volume de données à sauvegarder.

Avantages & Inconvénients

Avantages

- ✓ Peu de ressources humaines à mobiliser.
- ✓ Les données sont sauvées dans un lieu éloigné de l'entreprise. En cas d'incident dans l'entreprise les données seront toujours disponibles.
- ✓ Le bon déroulement des sauvegardes est contrôlé par le prestataire de service.
- ✓ Pas d'investissement lourd dans du matériel spécifique

Inconvénients

- ✓ La rapidité de sauvegarde ou de récupération des données dépend du débit de la liaison.
- ✓ Nécessité d'une liaison assez coûteuse

2. SAUVEGARDER INTELLIGEMENT POUR REPARTIR EFFICACEMENT

Nous avons vu dans le chapitre précédent quelles sont les familles de solutions à votre disposition pour construire un système de sauvegarde efficace. Voyons maintenant comment intégrer ces solutions techniques dans une politique de sauvegarde intelligente.

2.1. ÉVALUER LE POINT DE REPRISE DES DONNÉES (RPO)

Le RPO, pour *Recovery Point Objective*, indique l'âge maximum acceptable des données au moment de l'incident. Il est très rare de voir des sauvegardes effectuées au cours de la journée car les volumes de données élevés impliquent une saturation du réseau et du serveur pendant la sauvegarde. Donc, dans la plupart des cas, les sauvegardes ont lieu la nuit.

Ce qui implique qu'en cas d'incident pendant la sauvegarde le RPO est placé à 24 heures, soit la sauvegarde de la nuit précédente.

Hormis dans le cas d'applications hautement critiques, c'est ce RPO qui est communément utilisé.

2.2. ÉVALUER SON TEMPS DE REPRISE MAXIMUM (RTO)

Le RTO, pour *Recovery Time Objective*, est le délai maximum acceptable pour redémarrer l'exploitation après un incident. Il est lié à la criticité des systèmes que l'on intègre dans notre politique. Cet aspect ne se limite pas à la sauvegarde mais va bien au-delà. Il faut prendre en compte trois aspects bien distincts :

- a. les contrats de maintenance des équipements (H+4 pour des systèmes très critiques, J+1 dans les cas plus généraux, J+2 pour des systèmes moins critiques) ;
- b. le personnel nécessaire pour redémarrer la structure, attribuer à chacun des rôles bien définis et formaliser le tout *via* une cellule de crise ;
- c. les sauvegardes, bien entendu. Où sont elles stockées, en combien de temps peut-on restaurer les données ?

Vous l'aurez compris: entre RPO et RTO, c'est ce dernier qui est le plus important. Si vous savez en combien de temps vous pouvez redémarrer, avec quelles données et quel est le rôle de chacun, alors vous avez fait la moitié du travail.

2.3. ÉVALUER LE COÛT DE LA PERTE / DESTRUCTION DES DONNÉES

Avant une éventuelle catastrophe, évaluer le coût de la perte et de la destruction des données est le rôle de l'analyse de risque. Il faut identifier et hiérarchiser les risques potentiels et chiffrer au mieux le coût de la perte (*incluant le coût de la reprise*). Cet aspect

est très variable d'une entreprise à une autre et peut être difficile à traiter. Toutefois, ne le négligez pas car le chiffrage de la perte est en lien direct avec la budgétisation des moyens de protection.

L'évaluation après une éventuelle catastrophe est beaucoup plus complexe. Il faut lancer un audit pour identifier l'impact réel de la destruction des données et estimer la perte financière. Les dédommagements dépendent des contrats d'assurances et des contrats de maintenance.

Deux exemples vécus suivent pour illustrer le coût de la perte/destruction :

- a. Une société A répond à un appel d'offre d'un très grand compte. Le commercial de la société A doit donc se rendre devant un jury pour y présenter le dossier de sa société. L'appel d'offre est important et de nombreux concurrents présentent également leurs solutions cette même journée. Où est la faille ? Le commercial se fait tout simplement voler son ordinateur portable dans sa voiture la veille ! Tout le travail accompli est volatilisé sans aucune sauvegarde. Le contrat est perdu et aucun recours n'est possible...
- b. Une société A possède un bureau dans une société B, cette dernière se chargeant des expéditions de la société A.

La société B est victime d'un incendie, détruisant en même temps les données de A et la sauvegarde sur bande, stockée dans un coffre sur le site, n'est pas restaurable. Résultat : toutes les traces des matériels expédiés sont perdues et A subit des pénalités dues au retard de livraisons.

Quels sont les recours ? A paie les pénalités et se retourne ensuite vers la société B et son assurance.

Les scénarii possibles sont infinis, essayer de tous les prévoir est impossible mais mettre en place des mesures adaptées à la valeur des données permet de réduire considérablement les risques.

2.4. QUOI SAUVEGARDER ?

Une politique de sauvegarde implique que l'on sauvegarde **tous** les fichiers de tous types présents sur tous les disques des systèmes centraux.

Il faut également vérifier que les utilisateurs ne stockent pas de données critiques sur leurs postes de travail (*comme notre commercial dans l'exemple précédent*). Pour pallier à ce problème, le stockage en réseau est plutôt efficace : on oblige les utilisateurs à travailler sur des partages réseaux plutôt qu'en local.

Les informations de configurations sont également importantes à sauvegarder. Les configurations des commutateurs, routeurs et autres équipements peuvent être longues à recréer. Une sauvegarde mensuelle ne prend que peu de temps et peut en faire gagner beaucoup.

La loi ne demande pas aux entreprises de tenir une quelconque politique de sauvegarde, elle ne parle que de l'archivage (*donc les données mortes*). Cet aspect appartient plus aux domaines de la gestion et de la comptabilité qu'à celui de l'informatique.

Enfin, les systèmes d'exploitation peuvent éviter d'être sauvegardés si leur configuration est suffisamment simple. Dans le cas contraire, une sauvegarde du système peut être appréciée afin d'éviter la lourde tâche de configuration.

Si seulement certains fichiers de configurations peuvent s'avérer critiques, un système d'exploitation ne l'est pas et vous n'aurez pas de mal à redéployer vos architectures systèmes.

2.5. DÉFINIR UNE POLITIQUE DE SAUVEGARDE PERTINENTE

Une seule solution de sauvegarde ne suffit pas : il faut en imbriquer plusieurs. Nous répertorions ci-dessous des méthodes qui ont fait leurs preuves :

Système DAS simple

- a. sauvegarde complète une fois par semaine
- b. sauvegarde différentielle le reste de la semaine
- c. dépôt des supports dans un emplacement externe

Système NAS+DAS

- a. données en production stockées sur NAS
- b. réplication journalière sur un deuxième NAS
- c. sauvegarde complète hebdomadaire sur bande
- d. dépôt des supports dans un emplacement externe

Système SAN+télesauvegarde

- a. données en production stockées sur SAN
- b. synchronisation de nuit par télesauvegarde (chez un fournisseur)

Ce ne sont que des idées imbriquant plusieurs solutions. À vous de définir la vôtre en fonction de votre budget et de vos besoins en RTO/RPO. Il existe tout de même des règles générales à respecter :

- posséder une sauvegarde à l'extérieur pour se protéger du risque incendie,
- tester ses sauvegardes régulièrement sur des machines qui ne sont pas en production.

CONCLUSION

La sauvegarde de l'information reste un compromis entre le coût d'investissement dans le matériel de sauvegarde et l'importance de vos données. C'est un choix délicat qui peut déterminer la survie de votre société suite à une crise.

Nous espérons que ce guide vous aura éclairé pour trouver la solution adéquate et que celle-ci vous sera fidèle en cas de nécessité.

Rappelons enfin que toutes ces techniques ne viennent qu'en complément des éléments essentiels qui constituent la sécurité d'une salle serveur, à savoir les onduleurs et le système de climatisation.

En complément de ce guide, nous avons créé une méthode pour auditer votre système de sauvegarde. Pour obtenir les grilles et la documentation de la méthode MASYS (Méthode d'Audit du SYstème de Sauvegarde), ou pour toutes autres questions, n'hésitez pas à nous contacter. La méthode que nous avons mise au point étant en évolution constante, nous vous ferons parvenir la dernière version.

BIBLIOGRAPHIE

- ✓ 01net : magazine d'information sur les nouvelles technologies (www.01net.com)
- ✓ ASP64 : fournisseur de solutions de stockage (www.asp64.com)
- ✓ Dell : prestataire de service (www.dell.com)
- ✓ HP : prestataire de service (www.hp.com)
- ✓ IBM : prestataire de service (www.ibm.com)
- ✓ NTT : intégrateur de solutions global (www.ntt.com)
- ✓ Wikipédia : encyclopédie numérique (www.wikipedia.fr)

CONTACTS

Didier BERNAUDEAU :	didier@bernaudeau.net
Adrien GOSSEAUME :	adrien.gosseaume@laposte.net
Julien VEHENT :	julien@linuxwall.info

Voici l'ensemble de nos guides, pour vous aider à
"Anticiper, Communiquer et Repartir en cas de crise ":

- Guide n° 1 : " MISE EN PLACE ET VALIDATION D'UNE CELLULE DE CRISE "
- Guide n° 2 : " MISE EN PLACE D'UN PLAN DE SECOURS INTERNE "
- Guide n° 3 : " LES INTERLOCUTEURS EXTERNES DE LA CRISE "
- Guide n° 4 : " STRATEGIE DE COMMUNICATION EN CAS DE CRISE"
- Guide n° 5 : " PLAN DE REPRISE EN CAS DE DESTRUCTION PARTIELLE DE
L'OUTIL DE PRODUCTION "
- Guide n° 6 : " PLAN DE REPRISE D'ACTIVITE : DESTRUCTION PARTIELLE DU
SYSTEME D'INFORMATION"
- Guide n° 7 : " MAITRISER VOTRE SYSTEME DE SAUVEGARDE "
- Guide n° 8 : " MISE EN PLACE D'UN RETOUR D'EXPERIENCE "