

la disponibilité des données

www.ofppt.info

Sommaire

1.	Sauvegarde et archivage.....	2
1.1.	Introduction	2
1.2.	Quand le disque dur s'en mêle.....	2
1.3.	Organiser la vie de la donnée dans l'entreprise	3
2.	Plan de continuité d'activité	8
2.1.	Introduction	8
2.2.	Etapas de la mise en place d'un plan de continuité	8
2.2.1.	Analyse de risque et d'impact	8
2.2.2.	Choix de la stratégie de sécurisation.....	9
2.3.	Développement du plan	12
2.4.	Exercices et maintenance.....	12
2.5.	Plan de Continuité d'Activité ou Plan de Secours Informatique ?	13

1. Sauvegarde et archivage

1.1. Introduction

Il paraîtrait presque normal de confondre sauvegarde et archivage. Après tout, il s'agit dans les deux cas de stocker des données sur un support de masse afin de les conserver. Ce serait cependant une erreur ! Et comprendre la différence qui existe entre une sauvegarde et une archive permet de mieux appréhender le cycle de vie de la donnée dans l'entreprise et le choix des solutions techniques.

Pour cela, un retour historique s'impose. Les vétérans de l'informatique parlaient plus volontiers de stockage "chaud" ou "froid" plutôt que de sauvegarde ou d'archivage. Le stockage dit "chaud" était la donnée immédiatement accessible et facilement modifiable. A l'opposé, le stockage dit "froid" désignait la donnée archivée sur un support à très forte capacité de stockage, mais dont l'inconvénient était de ne pas permettre une récupération rapide et granulaire des informations. Ainsi, une fois les enregistrements "descendus" sur une bande magnétique, la récupération d'un fichier particulier situé en milieu de bande pouvait prendre plusieurs heures et n'était de ce fait utilisée qu'en dernier recours.

De cette distinction finalement technique découlent les notions de sauvegarde et d'archivage. Les données sauvegardées sont susceptibles d'être récupérées rapidement et peuvent être modifiées à volonté. Mais au delà d'un certain délai, ou lorsque la donnée a été "consommée" et traitée, elle est enregistrée sur une bande où elle ne sera plus modifiée (archivée, donc) afin d'être conservée en l'état.

En résumé: on n'accède quasiment jamais aux archives tandis que l'on passe son temps à modifier des sauvegardes, ne serait-ce que pour les mettre à jour !

1.2. Quand le disque dur s'en mêle

Deux autres raisons ont contribué à cette distinction historique entre sauvegarde et archivage et à la spécialisation des supports : la capacité de stockage et le coût du support rendaient le disque dur hors de portée des solutions d'archivage tandis que la bande magnétique ou le disque optique jouissaient d'un rapport capacité / prix particulièrement intéressant. De plus, seuls les supports magnétiques et optiques permettaient l'écriture unique (**WORM**, pour Write Once Read Many), une fonctionnalité très prisée notamment dans les métiers de la banque et de la finance.

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	2 - 30

L'évolution des technologies a cependant rendu caduques ces considérations techniques. Le prix des disques durs, en baisse constante, rend désormais cette technologie tout aussi adaptée aux opérations de sauvegarde que d'archivage, avec dans ce dernier cas des temps d'accès aux données archivées largement supérieurs à ceux d'une bande magnétique ou d'un disque optique. Et il existe maintenant des disques durs WORM (non réinscriptibles) capables de satisfaire aux exigences de l'archivage légal. Par ailleurs, les coûts de maintenance et d'évolution des disques durs sont largement inférieurs à ceux d'une solution de stockage de masse traditionnelle, et leur évolution se révèle très granulaire : il suffit d'ajouter des disques à un **SAN** (Storage Area Network) afin d'augmenter immédiatement la capacité de stockage globale.

Libérée des contraintes techniques, la notion de sauvegarde et d'archivage se recentre ainsi désormais sur la notion de donnée "vivante" (elle peut être modifiée) ou "morte" (elle a été figée pour des raisons organisationnelles ou légales). Dans tous les cas, cependant, elle demeurera accessible rapidement en ligne.

1.3. Organiser la vie de la donnée dans l'entreprise

Même si la technologie fusionne les usages, la distinction entre sauvegarde et archivage doit cependant toujours être faite par l'entreprise d'un point de vue organisationnel. Quelles sont les données qui doivent régulièrement être modifiées et sauvegardées et comment maximiser leur disponibilité et simplifier leur mise à jour ? A quel point une donnée doit-elle être figée et sortie du circuit pour être conservée sur une longue durée ? Comment alors optimiser le stockage en termes d'espace et de sécurité ? Et quelles données sont concernées par ce traitement ?

Autant de questions dont la réponse - probablement unique à chaque entreprise - ne peut venir qu'une fois la distinction clairement établie entre sauvegarde et archivage. Même si désormais les supports sont identiques !

2. Les plans de disponibilité

2.1. *L'analyse d'impacts commerciale*

L'analyse d'impacts est la première étape cruciale dans la mise en place d'un plan de continuité. Souvent oubliée ou laissée pour compte, elle permet à une entreprise d'identifier les fonctions d'affaire et activités critiques qui doivent faire l'objet d'un plan de continuité.

L'analyse d'impact permet à une entreprise de maximiser les efforts investis en matière de continuité en mettant l'accent sur les fonctions et activités critiques seulement.

De plus, elle permet de sensibiliser la haute direction d'une entreprise à l'importance de la mise en place d'un plan de relève en faisant ressortir les impacts d'un arrêt des opérations.

L'analyse d'impacts détermine, à partir de critères bien précis, le temps d'arrêt maximal pour chacune des fonctions. La connaissance de ce temps d'arrêt maximal permet d'orienter le choix des stratégies de relève afin d'optimiser les efforts.

Les impacts analysés sont d'ordre :

- Financiers
- Humains
- Organisationnels
- Contractuels ;

2.2. *Le plan de contingence*

Le plan de contingence, contrairement au plan de relève, a pour but de protéger l'entreprise contre une menace bien précise.

Que ce soit face à une possibilité de conflit de travail ou face au bug de l'an 2000, la planification de la contingence ne doit jamais être prise à la légère.

Certaines personnes pourraient être tentées de dire qu'un bon plan de relève répond aux besoins de contingence. Ces personnes ont raison en partie seulement. La différence entre ces 2 plans réside principalement

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	4 - 30

dans les stratégies déployées. Comme le risque est connu à l'avance, les stratégies associées à un plan de contingence sont beaucoup plus précises.

L'exemple du «bug» de l'an 2000 démontrait bien cette différence. Alors qu'un plan de relève traditionnel prévoit l'utilisation d'un site de relève distant pour se protéger d'un sinistre, Les plans de contingence pouvaient très bien assumer que le site de production demeurerait fonctionnel.

Certaines portions d'un plan de relève et d'un plan de contingence sont similaires, donc récupérables. Le processus décisionnel, le comité de gestion de crise et l'établissement d'un centre de commande peuvent généralement être récupérés

3.Le plans de relève informatiques

Le plans de relève informatiques sont les précurseurs des plans de relève corporatifs.

Longtemps considérée comme une fonction essentielle des entreprises, celles ci se rendent compte aujourd'hui que l'informatique est rarement leur raison d'être. C'est ce qui explique que plusieurs grandes entreprises se tournent vers la sous-traitance ou l'impartition.

Plusieurs stratégies s'offrent à nous et des choix éclairés doivent être faits afin de maintenir les coûts de continuité à un niveau acceptable.

Le choix du site de relève (interne ou commercial) et du type de site désiré (équipé complètement, partiellement ou non équipé) influence grandement le coût de la relève.

L'avènement des liens de télécommunications à très haut débit, à coût modéré permet d'être beaucoup plus imaginatif qu'il y a 10 ans. La distance entre le site de production et de relève est de moins en moins un critère de sélection. Les données critiques peuvent maintenant être protégées jusqu'à la dernière transaction sur des distances impressionnantes.

La protection des données par de simples prises de copies, suivi d'une sortie manuelle dans une voûte devient presque désuète puisque souvent ils peuvent être pris à distance, offrant ainsi une protection instantanée. Notons que la possibilité de prendre des copies à distance est disponible maintenant pour toutes les entreprises, grandes ou petites.

Plusieurs plans de relève ne comportent qu'une suite de procédures techniques destinées à relever l'environnement informatique. La portion administrative est souvent laissée de côté, à tort. Un processus clair et documenté d'évaluation des dommages et d'activation du plan permet

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	5 - 30

d'accélérer la prise de décision, donc la mise en place de l'environnement de relève.

Un plan devrait comporter un processus d'évaluation, d'activation et d'escalade, une procédure de mise en place au site de relève, les procédures de remontée des environnements de base et des applications, différentes listes (personnel, équipement, liens, fournisseurs, documentation, etc...), et une section décrivant le manuel, sa structure et son processus de maintenance

Tel que mentionné à la page « Plan de relève informatique », les plans de relève corporatifs ou administratifs, sont les successeurs aux plans de relève informatique pour la majeure partie des entreprises.

3.1. Plan de relève corporatif

Un plan de relève corporatif permet de protéger une entreprise contre tout événement qui pourrait engendrer un arrêt de ses opérations.

Quand on pense « arrêt des opérations » on a tendance à penser aux sinistres majeurs tel feu, inondation et tremblement de terre. Un bon plan de relève doit adresser ces alternatives, mais doit principalement être ciblé vers les risques potentiels.

Pour se protéger contre ces risques potentiels, des stratégies de relève ou plans d'actions seront élaborés. Ces stratégies identifieront un ou des sites de production alternatifs, les composantes requises ainsi que des processus de remplacement de ces composantes à court, moyen ou long terme et les ressources humaines et informationnelles requises pour que l'entreprise puisse continuer d'opérer.

Des mesures de protection seront mise en place afin de protéger les données informatiques ou opérationnelles contre un bris ou un sinistre.

La structure du plan de relève corporatif est similaire au plan de relève informatique. La différence entre ces 2 plans provient du fait qu'un plan de relève informatique est un sous-ensemble du plan de relève corporatif.

Le plan de relève corporatif sera constitué des processus et procédures suivants :

- un processus d'évaluation du sinistre ;
- une procédure d'activation du plan
- une procédure d'appel et d'escalade

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	6 - 30

- une procédure d'activation et de mise en place du ou des sites alternatifs ;
- une procédure de recouvrement des environnements informatiques et bureautiques affectés
- une procédure pour rediriger les liens de télécommunications voix et données au(x) site(s) alternatif(s)
- les procédures de récupération des données informatiques et opérationnelles
- les procédures administratives
- un processus de maintenance afin d'éviter la désuétude du plan

les listes utiles (ressources humaines, ressources physiques, liens de télécommunications, équipements requis, papeterie et formulaires, données vitales).

Afin de gérer toutes ces informations, il existe des outils spécialisés qui faciliteront le développement et le maintien des plans de relève. Certains outils sont valables alors que d'autres n'ont que peu de valeur ajoutée. L'utilisation d'un bon traitement de texte, jumelé à une structure de plan bien définie peuvent très bien faire l'affaire.

L'utilisation d'experts en continuité des affaires permet d'accélérer les étapes de développement d'un plan de relève et ainsi donc, de réduire les coûts de développement et d'accélérer la protection de l'entreprise.

3.2. Continuité des affaires

Au Québec, l'intérêt des grandes entreprises pour les plans de relève s'est réveillé suite au feu de la Plaza Alexis Nihon, à la fin des années 1980, où étaient établis les locaux informatiques de chaîne alimentaire Steinberg. Cette firme, venait de compléter l'élaboration de son plan de relève informatique et de terminer un test dans son site de relève.

C'est à ce moment là que plusieurs dirigeants québécois ont réalisé leur niveau de dépendance envers leur centre informatique et qu'ils ont démarré l'élaboration des premiers plans de relève informatique.

Une fois ces plans réalisés, une autre question se posait : Mon application est maintenant protégée, mais qu'advierait-il si un sinistre affectait le client de cette application ? Et c'est en réponse à cette

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	7 - 30

question que les plans de relève corporatifs sont apparus.

Depuis, plusieurs sociétés importantes se sont dotées de plans afin de répondre à un sinistre majeur. Mais, est-ce uniquement ce type d'évènement qui peut vous affecter ?

L'industrie de la relève tend de plus en plus à utiliser le concept de « Continuité des affaires ».

Par ce concept, nous analysons tout type d'évènements qui pourraient entraver la bonne marche d'une entreprise, donc la continuité de ses affaires. L'utilisation d'une telle étude, de concert avec une analyse d'impacts commerciale, nous permet de produire un plan d'action afin de mettre en place des mesures préventives et correctrices qui sont adaptées aux besoins de l'entreprise.

Avec en main un programme de prévention adapté, un plan de relève adéquat pour pallier à tout type d'interruption de services, un plan de maintenance formel, des tests complets et fréquents et un programme de formation adéquat, vous pourrez dormir paisiblement sans vous demander si votre entreprise sera là demain, ou la semaine prochaine...

4. Plan de continuité d'activité

4.1. Introduction

Un plan de continuité d'activité, parfois aussi appelé "plan de reprise d'activité", a pour but la reprise des activités après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise.

4.2. Etapes de la mise en place d'un plan de continuité

4.2.1. Analyse de risque et d'impact

Pour qu'un plan de continuité soit réellement adapté aux exigences de l'entreprise, il doit reposer sur une analyse de risque et une analyse d'impact :

L'analyse de risque débute par une identification des menaces sur l'informatique. Les menaces peuvent être d'origine humaine (attaque délibérée ou maladresse) ou d'origine « naturelle »; elles peuvent être internes à l'entreprise ou externes. On déduit ensuite le risque qui découle des menaces identifiées; on mesure l'impact possible de ces risques. Enfin, on décide de mettre en œuvre des mesures d'atténuation des risques en se concentrant sur ceux qui ont un impact significatif. Par exemple, si le risque de panne d'un équipement risque de tout paralyser,

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	8 - 30

on installe un équipement redondant. Les mesures d'atténuation de risque qui sont mises en œuvre diminuent le niveau de risque, mais elles ne l'annulent pas: il subsiste toujours un risque résiduel, qui sera couvert soit par le plan de continuité, soit par d'autres moyens (assurance, voire acceptation du risque)

L'analyse d'impact consiste à évaluer quel est l'impact d'un risque qui se matérialise et à déterminer à partir de quand cet impact est intolérable, généralement parce qu'il met en danger les processus essentiels (donc, la survie) de l'entreprise. L'analyse d'impact se fait sur base de désastres: on considère des désastres extrêmes, voire improbables (par exemple, la destruction totale du bâtiment) et on détermine les impacts financiers, humains, légaux, etc., pour des durées d'interruption de plus en plus longues jusqu'à ce qu'on atteigne l'impact maximal tolérable. Le résultat principal de l'analyse d'impact est donc une donnée temporelle: c'est la durée maximale admissible d'une interruption de chaque processus de l'entreprise. En tenant compte des ressources informatiques (réseaux, serveurs, PCs...) dont chaque processus dépend, on peut en déduire le temps maximal d'indisponibilité de chacune de ces ressources, en d'autres termes, le temps maximal après lequel une ressource informatique doit avoir été remise en fonction. Une analyse de risque réussie est le résultat d'une action collective impliquant tous les acteurs du système d'information: techniciens, utilisateurs et managers.

4.2.2. Choix de la stratégie de sécurisation

Il existe plusieurs méthodes pour assurer la continuité de service d'un système d'information. Certaines sont techniques (choix des outils, méthodes de protection d'accès et de sauvegarde des données), d'autres reposent sur le comportement individuel des utilisateurs (extinction des postes informatiques après usage, utilisation raisonnable des capacités de transfert d'informations, respect des mesures de sécurité), sur des règles et connaissances collectives (protection incendie, sécurité d'accès aux locaux, connaissance de l'organisation informatique interne de l'entreprise) et de plus en plus sur des conventions passées avec des prestataires (copie des programmes, mise à disposition de matériel de secours, assistance au dépannage).

Les méthodes se distinguent entre **préventives** (éviter la discontinuité) et **curatives** (rétablir la continuité après un sinistre). Les méthodes préventives sont souvent privilégiées, mais décrire les méthodes curatives est une nécessité car aucun système n'est fiable à 100 %.

Mesures préventives

La sauvegarde des données

La préservation des données passe par des copies de sauvegarde régulières. Il est important de ne pas stocker ces copies de sauvegarde à côté du matériel informatique, voire dans la même pièce car elles disparaîtraient en même temps que les données à sauvegarder en cas

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	9 - 30

d'incendie, de dégât des eaux, de vol, etc. Lorsqu'il est probable que les sauvegardes disparaissent avec le matériel, le stockage des copies de sauvegarde peut alors être nécessaire dans un autre lieu différent et distant.

L'analyse d'impact a fourni des exigences exprimées en temps maximal de rétablissement des ressources après un désastre (RTO Recovery Time Objective) et la perte maximale de données (Recovery Point Objective). La stratégie doit garantir que ces exigences seront observées.

- **Les systèmes de secours**

Il s'agit de disposer d'un système informatique équivalent à celui pour lequel on veut limiter l'indisponibilité : ordinateurs, périphériques, systèmes d'exploitation, programmes particuliers, etc. Une des solutions consiste à créer et maintenir un **site de secours**, contenant un système en ordre de marche capable de prendre le relais du système défaillant. Selon que le système de secours sera implanté sur le site d'exploitation ou sur un lieu géographiquement différent, on parlera d'un secours *in situ* ou d'un secours *déporté*.

Pour répondre aux problématiques de recouvrement de désastre, on utilise de plus en plus fréquemment des sites délocalisés, c'est-à-dire physiquement séparés des utilisateurs, de quelques centaines de mètres à plusieurs centaines de kilomètres : plus le site est éloigné, moins il risque d'être touché par un désastre affectant le site de production. Mais la solution est d'autant plus chère, car la bande passante qui permet de transférer des données d'un site vers l'autre est alors généralement plus coûteuse et risque d'être moins performante. Cependant la généralisation des réseaux longues distances et la baisse des coûts de transmission rendent moins contraignante la notion de distance : le coût du site ou la compétence des opérateurs (leur capacité à démarrer le secours rapidement et rendre l'accès aux utilisateurs) sont d'autres arguments de choix.

Les sites de secours (*in situ* ou déportés) se classent selon les types suivants :

salle blanche (une salle machine protégée par des procédure d'accès particulières, généralement secourue électriquement). Par extension, on parle de *salle noire* pour un salle blanche entièrement pilotée à distance, sans aucun opérateur à l'intérieur.

site chaud : site de secours où l'ensemble des serveurs et autres systèmes sont allumés, à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêt à fonctionner. Le site doit aussi fournir l'ensemble des infrastructures pour accueillir l'ensemble du personnel à tout moment et permet une reprise d'activité dans des délais

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	10 - 30

relativement courts (quelques heures). Un tel site revient quasiment à doubler les capacités informatiques de l'entreprise (on parle de **redondance**) et présente donc un poids budgétaire non négligeable.

site froid : site de secours qui peut avoir une autre utilisation en temps normal (ex : gymnase). Les serveurs et autres systèmes sont stockés mais non installés, connectés, etc. Lors d'un sinistre, un important travail doit être effectué pour mettre en service le site ce qui conduit à des temps de reprise long (quelques jours). Mais son coût de fonctionnement, hors période d'activation, est faible voire nul.

site tiède : site de secours intermédiaire. En général on trouve des machines installées (mise à jour décalée par rapport au site de production) avec les données sur bande mais non importées dans les systèmes de données.

Il est aussi possible d'utiliser des systèmes distribués sur plusieurs sites (diminution du risque de panne par effet de foisonnement) ou un site de secours mobile qui correspond à un camion transportant des serveurs et autres systèmes, permettant de n'avoir besoin que d'un système de secours pour plusieurs sites, en tablant sur l'improbabilité qu'une panne touche simultanément plusieurs sites.

Plus les temps de rétablissement garantis sont courts, plus la stratégie est coûteuse. Il faut donc choisir la stratégie qui offre le meilleur équilibre entre le coût et la rapidité de reprise.

D'autre part pour des problématiques de haute disponibilité on a recours aussi à de la redondance mais de manière plus locale.

- Doublement d'alimentation des baies des serveurs
- Redondance des disques en utilisant la technologie RAID
- Redondance de serveurs avec des systèmes de load balancing (répartition des requêtes) ou de heartbeat (un serveur demande régulièrement sur le réseau si son homologue est en fonctionnement et lorsque l'autre serveur ne répond pas, le serveur de secours prend le relais).

Il est aussi possible de recourir à un site secondaire de haute disponibilité qui se situe généralement près du site de production (moins de 10 kilomètres) afin de permettre de les relier avec de la fibre optique et synchroniser les données des deux sites en quasi temps réel de manière synchrone ou asynchrone selon les technologies utilisées, les besoins et contraintes techniques.

Mesures curatives

Selon la gravité du sinistre et la criticité du système en panne, les mesures de rétablissement seront différentes.

- **La reprise des données**

Dans cette hypothèse, seules des données ont été perdues. L'utilisation des sauvegardes est nécessaire et la méthode, pour simplifier, consiste à réimplanter le dernier jeu de sauvegardes. Cela peut se faire dans un laps de temps court (quelques heures), si l'on a bien identifié les données

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	11 - 30

à reprendre et si les méthodes et outils de réimplantation sont accessibles et connus.

- **Le redémarrage des applications**

A un seuil de panne plus important, une ou des applications sont indisponibles. L'utilisation d'un site de secours est envisageable, le temps de rendre disponible l'application en cause.

- **Le redémarrage des machine**

Provisoire : utilisation des sites de secours

Définitif : après dépannage de la machine d'exploitation habituelle, y rebasculer les utilisateurs, en s'assurant de ne pas perdre de données et si possible de ne pas déconnecter les utilisateurs.

4.3. Développement du plan

Le plan de reprise contient les informations suivantes :

- La composition et le rôle des "équipes de pilotage du plan de reprise". Ces équipes se situent au niveau stratégique :
 1. les dirigeants qui ont autorité pour engager des dépenses,
 2. le porte-parole en charge des contacts avec les tiers : la presse, les clients et les fournisseurs, etc.,
 3. au niveau tactique, les responsables qui coordonnent les actions,
 4. au niveau opérationnel, les hommes de terrain qui travaillent sur le site sinistré et sur le site de remplacement.

La composition de ces équipes doit être connue et à jour, ainsi que les personnes de remplacement et les moyens de les prévenir. Les membres des équipes doivent recevoir une formation.

- Les procédures qui mettent la stratégie en œuvre. Ceci inclut les procédures d'intervention immédiate (qui prévenir ? qui peut démarrer le plan et sur quels critères ? où les équipes doivent-elles se réunir ? etc.),
- Les procédures pour rétablir les services essentiels, y compris le rôle des prestataires externes
- Les procédures doivent être accessibles aux membres des équipes de pilotage, même en cas d'indisponibilité des bâtiments.

4.4. Exercices et maintenance

Le plan doit être régulièrement essayé au cours d'exercices. Un exercice peut être une simple revue des procédures, éventuellement un jeu de rôles entre les équipes de pilotage. Un exercice peut aussi être mené en grandeur réelle, mais peut se limiter à la reprise d'une ressource (par

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	12 - 30

exemple, le serveur principal), ou à une seule fonction du plan (par exemple, la procédure d'intervention immédiate). Le but de l'exercice est multiple :

- Vérifier que les procédures permettent d'assurer la continuité d'activité
- Vérifier que le plan est complet et réalisable
- Maintenir un niveau de compétence suffisant parmi les équipes de pilotage
- Évaluer la résistance au stress des équipes de pilotage

Un plan doit aussi être revu et mis à jour régulièrement (au moins une fois par an) pour tenir compte de l'évolution de la technologie et des objectifs de l'entreprise. La seule façon efficace de mettre à jour le PCA est d'en sous traiter la maintenance aux métiers afin qu'il soit réactualisé à chaque réunion mensuelle de service.

4.5. Plan de Continuité d'Activité ou Plan de Secours Informatique ?

Le Plan de Continuité d'Activité décrit dans cet article n'est en réalité que le volet informatique d'un Plan de Continuité d'Activité complet d'entreprise. Il s'apparente donc à un Plan de Secours Informatique. Un Plan de Continuité d'Activité (ou "Business Continuity Plan") ne se limite pas à la continuité du système d'information, il prend également en compte le repli des utilisateurs, le risque sanitaire (pandémie, grippe aviaire), l'organisation permettant la gestion de crise (astreintes, cellules de crise ...), la communication de crise, des mesures de contournement pour les métiers, les fonctions transverses ([RH](#), logistique, etc.).

Si l'on prend l'exemple d'une banque dont l'informatique est hébergée sur un site distant et qui voit sa salle des marchés détruite par un incendie, celle-ci déclenchera son Plan de Continuité d'Activité en repliant ses équipes sur un site de secours. Ce site de secours est constitué de positions de travail (le terme "position" représente un bureau, un ou deux écrans, une unité centrale, un téléphone), sur lesquels les utilisateurs pourront poursuivre leur activité : leur numéro de téléphone est transféré sur leur position de secours, l'image de leur poste informatique aura été reconstruite, ils disposeront des lignes de communication nécessaires (réseau interne et externe), le site de secours utilisateur est lui-même relié au site d'hébergement informatique (ou au site de secours si celui-ci est également impacté par le sinistre). Pour que le redémarrage informatique soit exploitable par les utilisateurs du système, les aspects techniques doivent être croisés avec l'organisation humaine.

5. Conception de services de sauvegarde et de restauration

Pour assurer le bon fonctionnement de leur activité, les entreprises s'appuient sur des données critiques. Les technologies de sauvegarde et de restauration constituent la clé de voûte des stratégies de protection

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	13 - 30

des données, stratégies qui permettent aux entreprises de répondre aux exigences de disponibilité et d'accessibilité des données. Les serveurs de données peuvent mettre en œuvre des technologies de redondance des composants et de tolérance de pannes (telles que les clusters de serveur, la mise en miroir de logiciels ou de matériels) pour garantir une disponibilité élevée en répliquant les données cruciales. Utilisées seules, ces technologies ne peuvent cependant pas résoudre les problèmes que peuvent provoquer la suppression ou la corruption de données qui se produisent en cas de bogue de l'application, de virus, de vulnérabilités de sécurité ou d'erreurs de l'utilisateur. Vous pouvez en outre avoir besoin de conserver des informations sous forme archivée pour des raisons d'audit juridique ou industriel. Ce besoin peut s'étendre aux données de transaction, aux documents et aux informations d'échange telles que le courrier électronique. Vous devez donc disposer d'une stratégie de protection des données comprenant un plan complet de sauvegarde et de restauration pour protéger vos données de toute panne ou catastrophe imprévue. Cette stratégie doit de plus être conforme aux exigences industrielles de conservation des données.



5.1. Définition du service

Il existe un certain nombre de technologies qui offrent différentes options d'implémentation de la sauvegarde et de la restauration. Vous devez choisir une de ces technologies en fonction des exigences de votre activité et des accords sur le niveau de service (SLA) définis par votre organisation pour chacun des services fournis par son centre de données. Ainsi, un service de messagerie peut être considéré comme le service le plus critique fourni par votre centre de données. L'accord sur le niveau de service de la messagerie doit donc se voir associer plus de ressources que les accords des autres services. Les accords sur les niveaux de services doivent être définis en collaboration avec les utilisateurs de chaque service.

5.2. Stratégies de sauvegarde

Un certain nombre de facteurs sont à prendre en compte lors de la planification de la solution : sauvegarde des éléments nécessaires seulement, planification soigneuse des sauvegardes et choix du type approprié de sauvegarde à exécuter.

5.2.1. Nécessité d'éviter les sauvegardes superflues

Lorsque vous concevez une stratégie de sauvegarde, vous pouvez être tenté d'exécuter une sauvegarde intégrale de chaque serveur de l'environnement. Gardez à l'esprit cependant que votre objectif est de restaurer correctement l'environnement après une panne ou une catastrophe. Votre stratégie de sauvegarde doit donc se concentrer sur les objectifs suivants :

- les données à restaurer doivent être aisément localisables ;

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	14 - 30

- la restauration doit s'avérer aussi rapide que possible.

Si vous sauvegardez tous les serveurs sans distinction, vous aurez un gros volume de données à restaurer. Bien que les produits de sauvegarde et de restauration permettent une restauration rapide des données, le temps d'arrêt peut s'allonger si vous devez tout restaurer à partir d'une bande. Ainsi, la plupart des produits de sauvegarde nécessitent l'exécution des étapes suivantes :

- réinstallation du système d'exploitation ;
- réinstallation du logiciel de sauvegarde ;
- restauration des données sauvegardées sur bande.

Plus vous sauvegardez de fichiers, plus la sauvegarde est longue, et surtout, plus la restauration des fichiers prend de temps. Après une catastrophe, le facteur temps est une donnée majeure. C'est pourquoi il importe que le processus de restauration soit aussi court que possible. En outre, les grosses sauvegardes effectuées de manière régulière ont un effet néfaste sur les performances du réseau à moins que vous ne mettiez en place un réseau de sauvegarde dédié.

Une fois que vous avez déterminé la stratégie de sauvegarde optimale pour votre environnement, il est indispensable d'effectuer une restauration-test sur la globalité du réseau test. Cet essai permet d'identifier les zones à problème et constitue une expérience utile en matière de restauration des systèmes dans l'environnement sans subir la pression de la remise en ligne du système de production.

5.2.2. Choix du moment approprié pour les sauvegardes

Chaque type d'environnement présente différentes opportunités pour effectuer une sauvegarde efficace en interrompant le moins possible les utilisateurs. Ainsi, la sauvegarde d'un environnement de commerce électronique n'a pas la même implication que la sauvegarde de l'infrastructure d'un réseau local d'entreprise. Sur un réseau LAN d'entreprise, l'utilisation est moindre en dehors des principales heures de travail. Dans un environnement de commerce électronique, l'utilisation augmente généralement en début de soirée et peut se poursuivre ainsi jusqu'aux premières heures de la matinée, particulièrement si la base de clients couvre plusieurs fuseaux horaires. C'est pour cette raison qu'il n'est pas possible de déterminer l'heure idéale de sauvegarde de votre environnement. Vous pouvez toutefois réduire l'impact de la sauvegarde, si vous suivez ces grandes lignes :

- planifiez les sauvegardes pour éviter les heures d'utilisation maximale ;
- ne sauvegardez pas les données superflues ;
- procédez à des essais réguliers de restauration sur un réseau test pour vérifier que les sauvegardes sont correctement effectuées.

5.2.3. Choix du support de stockage le mieux adapté

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	15 - 30

Après avoir déterminé le type de sauvegarde à effectuer et le moment approprié pour cette opération, vous devez également étudier les types de supports de stockage disponibles et sélectionner le support le mieux adapté.

Lorsque vous choisissez un support de stockage, tenez compte des points suivants :

- quantité de données à sauvegarder ;
- type de données à sauvegarder ;
- fenêtre de sauvegarde ;
- environnement ;
- distance entre les systèmes à sauvegarder et le périphérique de stockage ;
- budget de votre entreprise ;
- accords sur les niveaux de service pour la restauration des données.

Le tableau 1 récapitule les avantages et inconvénients des types de supports de sauvegarde les plus courants.

Tableau 1 : Comparatif des types de supports de sauvegarde

Type de support de sauvegarde	Avantages	Inconvénients
Bande	Assure une sauvegarde rapide et une longue conservation des données. Offre une capacité de stockage étendue. Plus économique que les disques magnétiques et magnéto-optiques.	S'use plus rapidement et se révèle plus sujet aux erreurs que les disques magnétiques et magnéto-optiques. Difficile à configurer et à maintenir, particulièrement dans une configuration de réseau de stockage (SAN). Requiert un nettoyage périodique des périphériques.
Disque magnétique	Facile à configurer et à entretenir. Utilisable pour les données intermédiaires.	Support le plus onéreux pour un stockage initial.
Disque magnéto-optique	Affiche la plus longue durée de vie sans dégradation du support.	Ralentit la sauvegarde et la restauration des données. Limite le choix du matériel.

5.3. Mode de sauvegarde

Le mode de sauvegarde détermine la façon dont la sauvegarde a lieu en fonction des données à sauvegarder. Il existe deux méthodes pour sauvegarder les données :

- Sauvegardes en ligne : les sauvegardes s'effectuent pendant que les données restent accessibles à tous les utilisateurs.

- Sauvegardes hors ligne : les sauvegardes concernent les données qui sont d'abord mises hors de portée des utilisateurs.

5.3.1. Sauvegardes en ligne

Les sauvegardes en ligne ont lieu pendant que le système est en ligne. C'est la stratégie de l'interruption la plus courte. Ce type de sauvegarde est généralement utilisé pour les applications devant être disponibles 24 heures/24, telles que Microsoft Exchange Server et Microsoft SQL Server™, les deux prenant en charge les sauvegardes en ligne.

Avantages

Parmi les avantages des sauvegardes en ligne, on retient :

- Pas d'interruption de service : Les applications et les données restent entièrement accessibles aux utilisateurs pendant le processus de sauvegarde.
- La sauvegarde hors des heures de travail n'est plus nécessaire : Les sauvegardes en ligne peuvent être programmées pendant les heures normales de bureau.
- Sauvegarde partielle ou totale : Les sauvegardes peuvent être partielles ou totales.

Inconvénients

Parmi les inconvénients des sauvegardes en ligne, on retient :

- Performances du serveur : Au cours du processus de sauvegarde, il est possible que les performances des serveurs de production se dégradent.
- Fichiers ouverts
- Si certaines applications sont actives pendant le processus de sauvegarde, il est possible que les fichiers de données ouverts ne soient pas sauvegardés.

5.3.2. Sauvegardes hors ligne

Les sauvegardes hors ligne sont effectuées en mettant hors ligne le système et les services. Vous pouvez les utiliser si vous avez besoin d'un instantané du système ou si l'application ne prend pas en charge les sauvegardes en ligne.

Avantages

Parmi les avantages des sauvegardes hors ligne, on retient :

- Sauvegarde partielle ou totale : Avec les sauvegardes hors ligne, vous pouvez choisir entre une sauvegarde partielle ou totale.
- Performances : Les sauvegardes hors ligne offrent de meilleures performances de sauvegarde car le serveur peut être dédié à la tâche de sauvegarde.

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	17 - 30

- Sauvegarde de tous les fichiers : Toutes les données sont sauvegardées dans la mesure où aucune application n'est en cours d'exécution et donc qu'aucun fichier n'est ouvert pendant le processus de sauvegarde.

Inconvénient

- Interruption du service : L'inconvénient des sauvegardes hors ligne est que les données ne sont pas accessibles à l'utilisateur pendant l'exécution du processus de sauvegarde.



5.4. Types de sauvegarde

Les différents types de sauvegarde peuvent être utilisés pour des sauvegardes hors ligne ou en ligne. Ce sont les exigences d'accord sur le niveau de sauvegarde de l'environnement, de fenêtre de sauvegarde et de durée de restauration qui déterminent la méthode ou la combinaison de méthodes optimales pour cet environnement.

5.4.1. Sauvegardes intégrales

Une sauvegarde intégrale capture la moindre petite donnée, fichiers compris, sur tous les disques durs. Chaque fichier est repéré comme ayant été sauvegardé, ce qui signifie que l'attribut archive est effacé ou réinitialisé. Vous pouvez utiliser une bande de sauvegarde intégrale à jour pour restaurer entièrement le serveur à un instant T.

5.4.2. Sauvegardes incrémentielles

Une sauvegarde incrémentielle capture la moindre donnée qui a été modifiée depuis la dernière sauvegarde intégrale ou incrémentielle. Vous devez utiliser une bande de sauvegarde intégrale (son ancienneté importe peu) et tous les jeux suivants de sauvegardes incrémentielles pour restaurer un serveur. Une sauvegarde incrémentielle repère les fichiers comme ayant été sauvegardés, ce qui signifie que l'attribut archive est effacé ou réinitialisé.

Avantages

Parmi les avantages des sauvegardes incrémentielles, on retient :

- • Optimisation du temps :Le processus de sauvegarde prend moins de temps dans la mesure où ne sont copiées sur la bande que les données modifiées ou créées depuis la dernière sauvegarde incrémentielle ou intégrale.
- • Optimisation du support de sauvegarde :La sauvegarde incrémentielle utilise moins de bande puisque ne sont copiées sur la bande que les données modifiées ou créées depuis la dernière sauvegarde incrémentielle ou intégrale.

Inconvénients

Parmi les inconvénients des sauvegardes incrémentielles, on retient :

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	18 - 30

- Complexité de la restauration complète : La restauration d'un système complet doit passer par la restauration d'un ensemble incrémentiel de plusieurs bandes.
- • Restaurations partielles chronophages : Une restauration partielle implique de rechercher sur plusieurs bandes les données requises.

5.4.3. Sauvegardes différentielles

Une sauvegarde différentielle capture les données qui ont été modifiées depuis la dernière sauvegarde intégrale. Pour effectuer une restauration du système, vous aurez besoin de la bande de sauvegarde intégrale et de la bande de sauvegarde différentielle la plus récente. Ce type de sauvegarde ne repère pas les fichiers comme ayant été sauvegardés (l'attribut archive n'est pas effacé).

Avantage

- Restauration rapide : L'avantage que présentent les sauvegardes différentielles tient dans le fait que leurs restaurations sont plus rapides que celles des sauvegardes incrémentielles car elles impliquent moins de bandes. Une restauration complète nécessite deux jeux de bandes au plus : la bande de la dernière sauvegarde intégrale et celle la dernière sauvegarde différentielle.

Inconvénients

Parmi les inconvénients des sauvegardes différentielles, on retient :

- Des sauvegardes plus volumineuses et plus longues : Les sauvegardes différentielles demandent plus d'espace sur la bande et plus de temps que les sauvegardes incrémentielles car plus la période qui vous sépare de la dernière sauvegarde intégrale est longue, plus il y aura de données à copier sur la bande différentielle.
- Augmentation de la durée de la sauvegarde : Le volume de données à sauvegarder augmente chaque jour qui suit une sauvegarde intégrale.

5.5. Topologies de sauvegarde

À l'origine, le seul type de technologie de stockage qui nécessitait une sauvegarde impliquait l'utilisation de disques durs connectés directement aux adaptateurs de stockage sur les serveurs. Aujourd'hui, ce type de stockage est connu sous le nom de stockage direct connecté (DAS). Le paysage de la sauvegarde et de la restauration a nettement évolué avec le développement de technologies telles que les SAN et NAS. Les environnements SAN en particulier fournissent un moyen intéressant d'optimiser et de simplifier le processus de sauvegarde et de restauration.

Les topologies de sauvegarde et de restauration peuvent être classées en fonction de la technologie de stockage (DAS, NAS ou SAN) à

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	19 - 30

sauvegarder. Les topologies couvrant chaque type de stockage sont respectivement la sauvegarde par serveur local, les sauvegardes NAS liées à un réseau LAN et les systèmes sur SAN.

5.5.1. Sauvegarde et restauration par serveur local

Dans le cadre d'une configuration de sauvegarde par serveur local, chaque serveur se connecte à son propre dispositif de sauvegarde, via généralement un bus SCSI (Small Computer System Interface). La bande passante du réseau local (LAN) n'est pas utilisée ici, mais vous devez gérer manuellement le support de stockage sur le serveur local.

La figure 1 présente un mécanisme type de sauvegarde et restauration par serveur local.

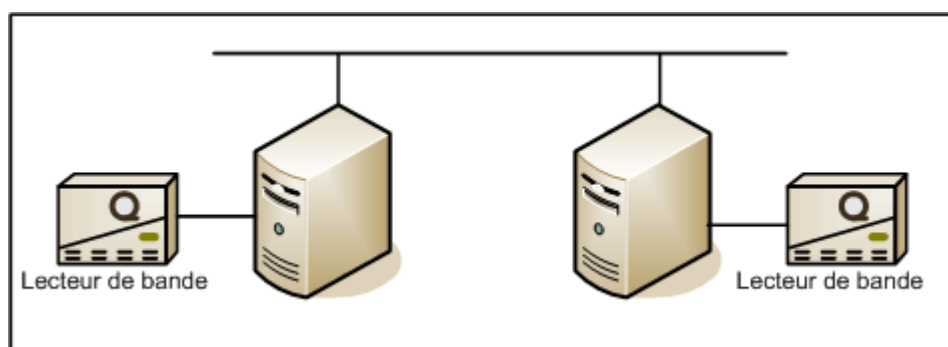


Figure
Sauvegarde et restauration par serveur local

1

Avantages

Parmi les avantages de la sauvegarde et de la restauration par serveur local, on retient :

- Ressources réseau non consommées : Les configurations de sauvegarde et de restauration par serveur local n'utilisent pas la bande passante du réseau car les serveurs sont généralement connectés aux dispositifs à bandes par une interface SCSI.
- Une sauvegarde et une restauration plus rapides : Ces sauvegardes peuvent être plus rapides que toute autre configuration de sauvegarde dans la mesure où les données n'ont pas à transiter sur le réseau.

Inconvénients

Parmi les inconvénients de la sauvegarde et de la restauration par serveur local, on retient :

- Capacité limitée de gestion centralisée et d'évolution possible : La configuration de sauvegarde et de restauration par serveur local n'offre pas de possibilités d'évolution ni de gestion centralisée car les supports de stockage doivent être gérés localement, au niveau de chaque serveur.
- Des coûts plus élevés en termes de logiciels de sauvegarde et de bandes : Cette configuration peut augmenter considérablement les coûts en licences de logiciel de sauvegarde et en périphériques à bandes dans la mesure où vous devez configurer une sauvegarde par serveur et les gérer individuellement.

5.5.2. Sauvegarde et restauration par réseau LAN

Les installations de sauvegarde par réseau LAN constituent une solution courante dans les entreprises et sont utilisées depuis un certain temps déjà. Un logiciel de sauvegarde LAN de l'entreprise fait appel à une architecture multi-couche selon laquelle certains serveurs de sauvegarde démarrent leur activité et collectent des méta-données (également appelées données de contrôle) sur les données sauvegardées pendant que d'autres serveurs (appelés serveurs de support) gèrent effectivement les données transférées sur les lecteurs de bandes.

Les technologies de sauvegarde LAN de l'entreprise sont généralement composées de trois éléments :

- Un serveur central de sauvegarde : Ce serveur héberge le moteur de sauvegarde qui contrôle l'environnement de sauvegarde.
- Un serveur de support : Ce serveur gère le mouvement des données et contrôle les ressources des supports.
- Des agents clients : Il s'agit des agents spécifiques d'applications, tels que pour les données Exchange, les données SQL Server et les données du système de fichiers.

La figure 2 illustre un système de sauvegarde et de restauration logique LAN

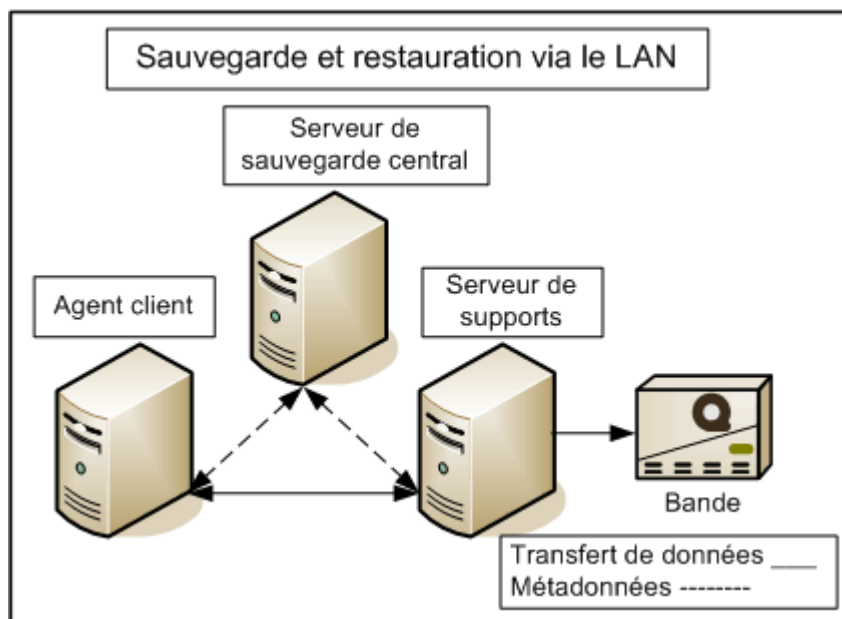


Figure
Sauvegarde et restauration par réseau LAN

2

Avantages

Parmi les avantages de la sauvegarde et de la restauration par réseau LAN, on retient :

- Les lecteurs de bandes n'ont plus besoin d'être connectés directement aux serveurs pour la sauvegarde.
- L'application de sauvegarde s'exécute sur des serveurs de sauvegarde dédiés.
- Les agents clients dirigent les données du LAN vers un serveur de sauvegarde.
- Meilleures possibilités d'évolution et partage des dispositifs à bandes.

Inconvénients

Parmi les inconvénients de la sauvegarde et de la restauration par réseau LAN, on retient :

- Les lots volumineux de données peuvent entraîner une dégradation des performances des serveurs et du réseau.
- Le trafic supplémentaire généré par la sauvegarde consomme la bande passante du réseau.
- La planification des sauvegardes et des restaurations peut devenir critique.
-

La sauvegarde de dispositifs NAS peut s'appuyer sur des agents de sauvegarde ou sur le protocole de gestion des données réseau (NDMP). Pour plus d'informations, reportez-vous à la section « Conception de services de sauvegarde et de restauration ».

5.5.3. Sauvegarde et restauration sur SAN

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	22 - 30

La possibilité d'intégrer des sous-systèmes d'espace disque à la sauvegarde et à la restauration vous offre un certain nombre d'options pour déployer les solutions de protection des données dans des environnements SAN. Les technologies sous-jacentes SAN fournissent plusieurs alternatives de sauvegarde et de restauration des données résidant sur un stockage SAN.

La figure 3 illustre un scénario de sauvegarde sur SAN

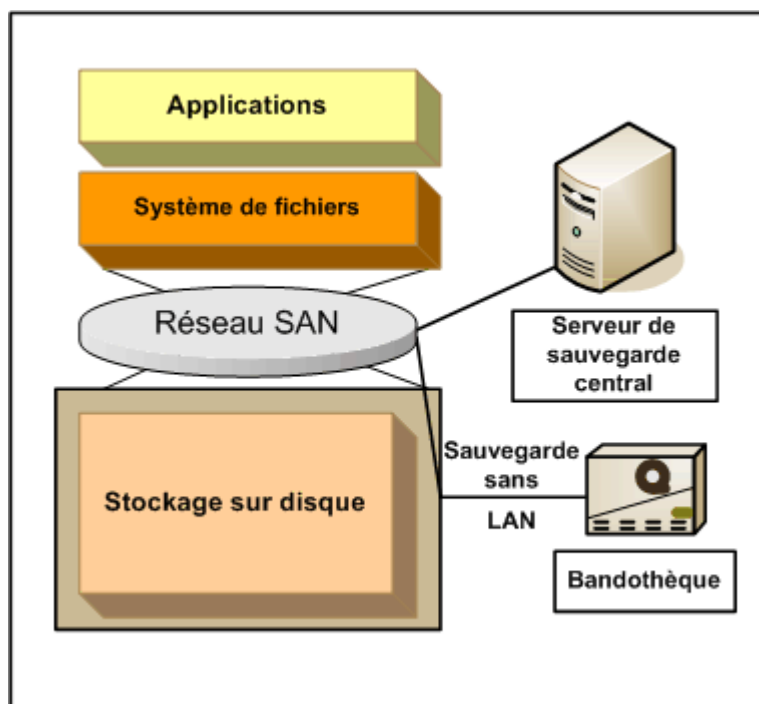


Figure
Exemple de scénario de sauvegarde sur SAN

3

Avantages

Parmi les avantages de la sauvegarde et de la restauration sur SAN, on retient :

- Une charge réduite du serveur : Le chemin entre le dispositif de stockage et celui de sauvegarde n'implique pas la présence d'un serveur, ce qui signifie que la charge du serveur est réduite.
- Une charge réduite du réseau : Les sauvegardes peuvent s'effectuer sans avoir à faire transiter les données sur le réseau LAN.
- Une solution de stockage optimisée : Les réseaux SAN sont conçus pour optimiser l'efficacité des transferts de données et permettre ainsi d'accélérer les processus de sauvegarde et de restauration.

Inconvénients

Parmi les inconvénients de la sauvegarde et de la restauration sur SAN, on retient :

- Les dépenses : Les sauvegardes sur SAN nécessitent un réseau SAN, dont la conception et le déploiement s'avèrent coûteux.

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	23 - 30

- La compatibilité des dispositifs : Les équipements de sauvegarde et de restauration doivent être compatibles SAN.

5.5.4. Utilisation de disques pour les sauvegardes intermédiaires

Les disques sont des solutions viables et économiques de stockage des données sur le court terme. Ils autorisent une restauration rapide dans le cas d'une deuxième copie des données critiques. Bien que vous puissiez réduire dans une certaine mesure les temps d'arrêt système grâce aux technologies RAID (Redundant Array of Independent Disks) et de tolérance aux pannes, protéger de la sorte des données peu utilisées ou peu importantes peut se révéler onéreux. La stratégie à implémenter consiste donc à échelonner les sauvegardes intermédiaires et les images d'instantanés sur un disque local ou un disque sur SAN. Les données peuvent être copiées en permanence de disque à disque. Elles peuvent être sauvegardées sur bande à intervalle régulier, la fréquence de la copie dépendant des exigences de chaque implémentation.

Échelonner les sauvegardes de données est important car cela vous donne la possibilité de déplacer les données vers un emplacement secondaire avant de les transférer sur bande. Vous pouvez planifier les copies de données pour qu'elles entraînent le moins de surcharge possible du serveur et des performances d'application tout en augmentant la disponibilité des données avant leur transfert sur bande. Déplacer une copie de données vers un stockage en ligne secondaire avant de la transférer sur bande permet de tirer parti d'une restauration rapide de la plupart des données récentes, qui n'ont pas encore été sauvegardées sur bande. Cette méthode fournit en outre une protection temporaire de seconde couche à partir de laquelle vous pouvez déplacer les données vers la bande sans mettre en branle les longues procédures de restauration de bande, même si la capacité de conservation des données dans l'instantané et leur accès en ligne sont limités à 24 heures. Vous pouvez déplacer les données vers la bande et effacer l'espace disque pour l'instantané suivant. En outre, sauvegarder la copie d'instantané et non la copie principale en ligne est un processus essentiellement sans fenêtre dédiée.



6.L'élaboration d'une stratégie de sauvegarde

6.1. Introduction :

Mettre en place un plan de sauvegarde des données critiques est crucial pour une entreprise. Mais il faut évaluer précisément ses besoins, face à l'offre existante, pour choisir de façon optimale matériel, logiciels et supports de stockage.

Les événements tragiques du 11 septembre nous ont tous montré le potentiel dévastateur d'un sinistre physique. De même, de nombreuses entreprises examinent avec attention leur stratégie de sauvegarde pour garantir l'intégrité des données, la fiabilité et la continuité de leur activité en cas d'incident.

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	24 - 30

L'élaboration d'une bonne stratégie de sauvegarde nécessite une planification prudente, allant de la sélection des matériels à la détermination du schéma de sauvegarde et autres questions logistiques. Chaque étape nécessite une analyse soignée à la lumière de facteurs tels que le personnel, l'expertise technique et le budget. Nous allons examiner tous ces facteurs et détailler les besoins d'une stratégie de sauvegarde réussie.

6.2. Choix du système de sauvegarde adéquat

Une entreprise doit tout d'abord déterminer la plate-forme (matérielle) de sauvegarde qu'elle utilisera pour la protection de ses données. Les options sont nombreuses, allant des systèmes complets de duplication de données qui créent des copies hors site, jusqu'aux systèmes traditionnels utilisant des bandes. Le budget et l'expertise requise déterminent le ou les choix le(s) plus adapté(s) pour votre entreprise.

Les systèmes à bande magnétique sont généralement les moins chers et les moins complexes du point de vue technique parmi les choix offerts actuellement sur le marché. Nous allons principalement étudier les systèmes à bande, puisqu'ils répondent à la plupart des besoins pour les audits et rapports des entreprises actuellement.

Avant de pouvoir définir votre stratégie de sauvegarde, vous devez d'abord déterminer le volume de données à protéger. Cette information vous aidera à choisir le type de système nécessaire, allant des unités à une bande aux chargeurs automatiques ou systèmes de stockage pouvant gérer des centaines de bandes à la fois.

Déterminer ce qui sera protégé va au-delà de la récapitulation du total des données présentes sur vos serveurs, car ces données ne sont pour la plupart pas cruciales pour votre entreprise. Les principaux exemples sont les programmes et fichiers d'application, qui sont facilement restaurés depuis les supports d'origine, et les fichiers personnels des utilisateurs, tels que les MP3.

Une fois que vous connaissez la quantité de données à protéger, vous pouvez déterminer le type de matériel répondant le mieux à vos besoins. Les systèmes de bande DDS ne conviennent généralement qu'aux entreprises de petite taille ayant moins de 10 Go de données à protéger. Pour les professions libérales, c'est un très bon choix, car les lecteurs de bande sont économiques et considérés comme fiables. De nombreuses options de chargeurs automatiques ou systèmes en rack sont disponibles pour cette plate-forme, permettant également à ces bandes magnétiques de couvrir la plupart des besoins des PME.

Pour les entreprises de grande taille, les systèmes de bande DLT sont quelque peu plus onéreux, mais offrent une capacité sensiblement plus importante en données. Les systèmes DLT peuvent s'étendre pour

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	25 - 30

répondre aux besoins en protection des données de la plupart des entreprises, quelle que soit leur taille. Les systèmes de chargeurs automatiques et de rack sont également disponibles pour cette plateforme, comprenant des robots et autres formes de systèmes automatisés de permutation des supports pour gérer les besoins des entreprises, même les plus grandes.

Une fois le matériel choisi, vient le tour du logiciel. Il existe de nombreux et excellents systèmes de sauvegarde sur le marché. Chacun propose des fonctions similaires ; examinez donc les interfaces, le prix et autres éléments pour déterminer lequel convient pour votre entreprise. Deux des principaux produits sont ARCserve de Computer Associates et BackupExec de la société Veritas.

6.3. *Détermination de votre méthode*

L'étape suivante consiste à déterminer la meilleure méthode pour la sauvegarde de vos données. Les systèmes de sauvegarde offrent pour la plupart une grande variété d'options. Les plus courantes sont les suivantes :

☐ **complète** : cette méthode transfère sur bande une copie de toutes les données concernées par la sauvegarde, indépendamment de la modification des données depuis l'exécution de la précédente sauvegarde ;

☐ **différentielle** : cette méthode sauvegarde tous les fichiers modifiés depuis la précédente sauvegarde complète, indépendamment de leur modification depuis la dernière opération de sauvegarde, quel que soit son type ;

☐ **incrémentale** : ici, se verront transférer sur bande les seuls fichiers modifiés depuis la dernière opération de sauvegarde, quel que soit son type (complète, différentielle ou incrémentale).

La méthode choisie dépendra essentiellement de la capacité de vos bandes et de vos besoins en restauration, très rapide ou non. Par exemple, en effectuant quotidiennement une sauvegarde complète, vous aurez besoin d'une capacité très élevée sur bande, mais seule la dernière bande de sauvegarde sera nécessaire pour restaurer toutes vos données.

Inversement, en effectuant une sauvegarde complète une fois par semaine avec une sauvegarde incrémentale quotidienne, vous aurez besoin de beaucoup moins d'espace sur bande, mais les opérations de récupération nécessiteront de réaliser sur les serveurs la restauration de la dernière sauvegarde complète et de chaque sauvegarde incrémentale. De nombreuses entreprises utilisent une combinaison de méthodes leur permettant d'économiser l'espace sur bande, tout en autorisant cependant une restauration rapide des données. La règle est

généralement d'effectuer des sauvegardes hebdomadaires complètes et des sauvegardes journalières incrémentales.

6.4. *Permutation des bandes*

Vous devrez ensuite développer un plan de permutation des bandes et déterminer l'endroit où les stocker. Malheureusement, les entreprises entreposent pour la plupart les supports de sauvegarde à environ un mètre des serveurs à protéger. Comme nous l'ont montré les sinistres physiques récents, ce n'est pas une méthode de premier choix pour protéger les données, car les bandes risquent fort d'être détruites avec les serveurs en cas d'incendie, par exemple. Les supports doivent être entreposés hors site, dans un endroit sûr où l'on peut les récupérer rapidement en cas de besoin.

Un plan adroit de permutation de bandes est essentiel pour réduire les coûts du support et du stockage hors site. En réutilisant les bandes après une période déterminée, les plans de permutation de bandes garantissent le stockage hors site d'un nombre minimal de bandes. Les schémas de permutation existent en diverses sortes et complexités.

Le schéma de permutation peut-être le plus courant est le cycle Grand-père-Père-Fils, utilisé depuis longtemps et qui s'est révélé efficace. Dans la version d'origine de ce schéma, on effectue les sauvegardes complètes à deux intervalles différents. Le premier est mensuel et on entrepose immédiatement le support hors site (grand-père). On effectue également des sauvegardes hebdomadaires complètes (père) et on les conserve généralement sur site pendant la semaine de leur utilisation, puis on les place hors site pendant un nombre prédéterminé de cycles hebdomadaires (deux ou trois cycles suffisent généralement).

Les sauvegardes incrémentales journalières (fils) s'effectuent et se conservent également sur site pendant la semaine de leur usage, puis on les place hors site avec la sauvegarde hebdomadaire correspondante selon le même calendrier cyclique. À la fin d'un cycle pour un jeu de bandes, celles-ci peuvent être réutilisées. On conserve chaque bande mensuelle pendant 12 mois avant de la réutiliser.

On conserve généralement les jeux de bandes hebdomadaires pendant environ trois semaines après leur départ de la salle du serveur (soit pendant quatre semaines), puis on les réutilise. Le nombre de réutilisations d'une bande dépend du type de support ; il est préférable de demander au fabricant le nombre de réutilisations conseillé pour chaque bande.

Les schémas de permutation Grand-père-Père-Fils permettent d'entreposer immédiatement les sauvegardes mensuelles en un endroit sûr, tandis que l'on conserve la plupart des sauvegardes complètes et incrémentales hebdomadaires pour réaliser sur le champ une restauration. On les stocke ensuite hors site en cas de panne. Si ce système présente des limites (vous pouvez perdre une semaine de

données en cas d'incendie ou autre catastrophe), il procure la sécurité la plus élevée au coût le plus bas.

Votre entreprise peut bien sûr nécessiter davantage de sécurité, auquel cas vous pouvez toujours expédier les bandes hors site dès leur création. Ce système est efficace pour la protection des données, mais il faudra rapatrier ces bandes sur site pour effectuer la restauration, ce qui entraînera des frais supplémentaires.

www.ofppt.info	Document	Millésime	Page
	la disponibilité des données.doc	août 14	28 - 30

Pour approfondir le sujet....

Proposition de références utiles permettant d'approfondir le thème abordé

Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support