PLANS DE SECOURS INFORMATIQUES

PRINCIPES GENERAUX

&

ETAT DE L'ART SELON BV ASSOCIATES

SOMMAIRE

1 Principes généraux d'un plan de secours

1.1 Fonctions générales du plan de secours

Le plan de secours doit permettre une reprise de service en mode dégradé puis normal dans les délais acceptables, c'est à dire conformes aux souhaits des utilisateurs. Dans le cas où la durée prévisionnelle de cette indisponibilité excède la durée admise par les directions utilisatrices, la reprise de service normal doit pouvoir s'effectuer quelle que soit la raison de l'indisponibilité.

Le déclenchement du plan de secours fait l'objet d'une procédure décisionnelle spécifique conforme aux exigences définies contractuellement entre les directions utilisatrices et la Direction des Systèmes d'Information.

L'ordre de restitution des fonctions applicatives est défini au préalable entre les maîtrises d'ouvrage et la Direction des Systèmes d'Information, en prenant en compte les flux fonctionnels critiques identifiés au préalable lors de l'établissement du contrat de service.

Le plan de secours est validé régulièrement par des tests réels de mise en œuvre, les tests fonctionnels associés étant préalablement définis par les maîtrises d'ouvrage.

La stratégie de sauvegardes / restaurations doit être adaptée pour permettre l'activation du plan de secours défini dans les plus brefs délais.

1.2 Principes du plan de secours

1.2.1 La configuration d'urgence

En cas de sinistre majeur d'un site de production informatique, l'ensemble des équipements vitaux peut être détruit. Le plan de secours doit donc permettre la mise à disposition sous des délais raisonnables d'une configuration d'urgence susceptible d'accueillir les environnements nécessaires à la bonne marche de l'entreprise.

Le principe fondamental de tout plan de secours est de disposer rapidement d'une configuration capable d'accueillir les données vitales de l'entreprise.

Cet environnement peut être mis à disposition soit, en interne si les configurations existent, soit par un partenaire spécialisé, soit par un engagement du fournisseur de matériel à fournir des matériels sous des délais conformes aux dispositions d'urgence prévues dans le plan de secours.

1.2.2 La montée en charge

Une fois que la configuration dite « d'urgence » est opérationnelle, le passage à la phase de déploiement de matériel pour mise à disposition des autres fonctionnalités moins critiques est possible.

Cette montée en charge progressive du site de secours permet une réduction des coûts du plan de secours.

Plus la volumétrie est importante moins il est possible d'inclure l'ensemble des données et services associés dans la configuration d'urgence, d'où l'importance de valider l'ensemble des fonctions critiques. Ce sont les flux fonctionnels critiques qui donnent l'ordre de restitution des données et systèmes. La définition précise des données "impératives" de la configuration d'urgence permet alors de définir l'enveloppe budgétaire.

1.2.3 La maintenance opérationnelle du plan de secours

La définition d'un plan de secours ne peut faire abstraction de sa maintenance en mode opérationnel. Le recours au secours n'est à priori pas volontaire et intervient au moment où l'on s'y attend le moins, et c'est donc à ce moment précis qu'il devra parfaitement fonctionner. La garantie de fonctionnement ne peut s'obtenir que par des tests complets et réguliers. Idéalement, si les configurations de secours et de production sont identiques il est souhaitable de basculer à intervalles réguliers la configuration de secours en production et celle de production en secours, c'est la meilleure garantie de faisabilité qu'un responsable informatique puisse obtenir.

Si le basculement réel n'est pas fait, un doute subsiste toujours sur la complétude des tests effectués, car l'ensemble des utilisateurs ne sont en général pas impliqués et l'ensemble des

fonctions critiques ne sont pas testées. Il faut une rigueur sans faille pour inclure ou non les nouvelles fonctionnalités dans les procédures de test du plan de secours.

Un plan de secours est aussi vivant que l'est une configuration de production et à ce titre subit des mises à jour régulières qui font l'objet de recette comme tout système de production. En résumé un site de secours doit être considéré comme un site de production avec un contrat de service adapté au même titre que le site de production régulier.

1.3 Le contrat de service

Le contrat de service doit décrire les procédures applicables en réponse aux besoins de service des utilisateurs. La principale difficulté liée à l'explicitation de tout contrat de service est due à la nature de l'information manipulée dans le système d'information.
Les systèmes d'information stockent les informations qui sont des données provenant de flux fonctionnels divers et variés. Les systèmes d'information se trouvant au centre de ces flux, chacun d'eux doit avoir sa propre convention de service. Un flux s'opère entre un fournisseur (celui qui fournit l'information) et un client (qui utilise l'information) et de ce fait les deux parties sont liées par cette convention de service. Chaque convention de service de flux devra comporter les engagements de service de chacun et notamment en cas de reprise sur incident.
Avant de définir l'architecture technique, il est donc impératif d'établir le contrat de service adéquat, en fonction des exigences suivantes :

- délai de restauration : c'est le délai acceptable avant redémarrage suite à une décision de mise en œuvre du plan de secours.
- « fraîcheur » des données : la restauration sur l'environnement de backup se fait en utilisant une image du site de production avant son interruption. Les données restaurées peuvent être plus ou moins anciennes. En fonction de l'antériorité des données restaurées et donc de la quantité de données perdues, les solutions à mettre en place seront plus ou moins contraignantes.

Cette étape permettra aussi de déterminer si des réductions de service sont acceptables et envisageables lorsque le système d'information est en « backup » : Peut-on par exemple considérer que pour limiter le coût de l'infrastructure de backup, seuls certains utilisateurs ont accès aux données ? Ou bien que certaines fonctions ne soient pas disponibles ?

Peut-on aussi envisager d'avoir plusieurs niveaux de services en fonction de la criticité des éléments ?

1.4 Niveau de criticité des serveurs du système d'information

Dans le cas d'un incident grave sur un site de production, les applications sont réinstallées sur les serveurs de secours, puis le service est redémarré. Pendant cette période les applications habituellement hébergées par les serveurs de secours sont rendues indisponibles.

La définition de cette criticité des serveurs se fait en intégrant différentes contraintes :

- Dépendances et contraintes fonctionnelles : il s'agit de s'assurer que les fonctions critiques sont disponibles intégralement, l'absence d'un maillon même peu important rompt l'ensemble de la chaîne. A l'inverse, l'impact de l'utilisation d'un serveur de secours non dédié doit être précisé du point de vue des applications et de leurs utilisateurs.
- Dépendances et contraintes techniques : il est impératif de s'assurer que l'ensemble des serveurs de secours est homogène du point de vue des versions logicielles et matérielles. Cette homogénéité doit être garantie dans le temps (il est nécessaire de respecter les mêmes paliers techniques pour toutes ces machines).
- Dépendances et contraintes organisationnelles : l'ensemble des machines du système d'information et des serveurs de secours doit être exploité et administré par les mêmes équipes avec la même méthodologie. Les applications et les utilisateurs hébergés par les serveurs de secours doivent disposer de règles de fonctionnement :
    - En particulier en cas de backup du système d'information, comment doit-on procéder pour les arrêter ?
    - Doit-on les sauvegarder ?
    - Lors du retour en production (après utilisation pour le backup du système d'information), comment seront-ils redémarrés pour leur fonction première ?

1.5 Prise en compte des évolutions

L'ensemble des projets en cours doit être inventorié afin d'en mesurer l'impact sur le cœur névralgique du système d'information.

Les évolutions techniques doivent en particulier être prises en considération (OS, SGBD, etc.)

2 Simplifier le plan de secours

2.1 La complexité induite du plan de secours

La complexité du plan de secours est en relation exponentielle avec la complexité des configurations à secourir. Plus l'environnement est complexe, plus les mises à jour du secours sont complexes, plus les procédures sont difficiles à établir, à faire connaître et à faire respecter. Les coûts induits vont de même, longueur des tests réguliers, nombre d'acteurs mobilisés etc….. La stabilité de l'environnement à secourir facilite le maintien en état opérationnel du plan de secours, a contrario toute déstabilisation de cet environnement doit être étudié pour mesurer les conséquences des modifications à apporter sur le plan de secours. Dans le cas du système d'informations de l'entreprise, les modifications sont quasi permanentes, le plan de secours doit donc être établi afin d'en tenir compte.

La complexité forte, les volumes importants, les évolutions permanentes sont autant d'éléments qui rendent tout plan de secours plus difficile à élaborer et maintenir en état de fonctionnement, c'est pourquoi il est impératif de simplifier au maximum ce qui peut l'être. La simplification peut être obtenue par la réduction des volumes à restaurer, la diminution du nombre de serveurs à restituer, la simplification des procédures de restitution, etc…

2.2 Simplifier la configuration du secours

Une première façon de simplifier la configuration de secours est d'analyser les processus fonctionnels critiques pour définir un ordre de priorité des restitutions. Une autre façon de le faire est de partager les risques sur des sites géographiques distants : En effet le sinistre majeur redouté de tous est la destruction physique du site où sont hébergées les machines de production. La répartition géographique sur des sites différents permet de répartir le risque et de réduire le nombre de machines de la configuration de secours afin qu'elle puisse supporter le secours de tout site de production mais pas la totalité des configurations des différents sites.

2.3 Réduire les délais de restitution des données

La durée de restitution des serveurs dépend de :

- la durée de mise à disposition des configurations de secours,
- la durée de restauration des données et environnements,
- le délai de mise à jour des données incrémentales.

2.3.1 Le délai de mise à disposition des configurations de secours

Ce délai dépend directement de la solution choisie : Ce peut être un délai quasi immédiat si les configurations sont gérées en interne, à quelques heures définies contractuellement s'il s'agit d'une configuration gérée par un partenaire externe, à quelques jours voire semaines s'il s'agit d'un simple engagement des fournisseurs de matériel.

2.3.2 Le délai de restauration

Le délai de restauration est, à robotique identique, à peu près proportionnel au volume à restituer, il s'ensuit que plus le volume à restituer est important plus la durée de restauration est longue. Par ailleurs un volume important nécessite une configuration de secours plus complexe, plus longue à mettre en œuvre.

2.3.3 Le délai de mise à jour des données

Ce délai dépend de la fraîcheur des données restaurées. Il s'ensuit que plus les données restaurées sont anciennes plus la durée de mise à jour sera longue. La durée de restauration des données archivées de la bande au disque doit être prise en compte, autant que la durée nécessaire au recouvrement proprement dit.

2.3.4 Réduire les volumes

La réduction des volumes à restituer participe directement à la simplification globale, aussi est-il nécessaire de distinguer les données stables des données vivantes, les données vitales des données superflues, les données actuelles des données historiques…

Ce qui est valable pour les données, l'est également pour les fichiers d'exploitation. A quoi bon restaurer le fichier d'exploitation de la semaine dernière alors qu'il s'agit de permettre le redémarrage de la production du jour ?

3 Les règles du plan de secours

3.1 Disposer de points de synchronisations clairs

Compte tenu de la nature distribuée des systèmes d'information, il peut être impératif de disposer de points de synchronisation précis qui constituent une base de cohérence entre les différents serveurs.
Ces points de synchronisation doivent obéir aux règles suivantes :

1. Ils n'ont de valeur que, si à ce moment précis il est certain que nous disposons, à l'extérieur des sites de production, de l'ensemble des données nécessaires à la restitution des données au niveau du point de synchronisation.

2. L'ensemble des mises à jour entre deux points de synchronisation peut être refait, soit par nouvelle saisie, soit par nouvelle exécution.

Pour cela il faut être sûr de disposer à l'extérieur de chacun des sites de production d'une sauvegarde la plus récente possible et l'ensemble des redologs archivés de la base de données depuis la sauvegarde jusqu'au point de synchronisation. Il faut également disposer de la sauvegarde différentielle des données de production (fichiers…) entre le point de synchronisation et la dernière sauvegarde totale externalisée.

3.2 Isoler les moyens de sauvegarde à l'extérieur du ou des sites de production

En aucun cas, il ne doit être possible de perdre à la fois un serveur de production et la sauvegarde de son dernier point de synchronisation. La seule façon d'obtenir cette certitude est qu'il n'y ait aucun serveur de données du système d'information sur le site des serveurs de sauvegarde.

L'intérêt d'une telle démarche est d'être sûr, en cas de sinistre d'un site hébergeant des données du système d'information de disposer des moyens de restauration nécessaires.
La remise à niveau des données étant un problème suffisamment complexe à traiter, en cas de sinistre du site de sauvegarde les serveurs de production doivent avoir une autonomie suffisante pour attendre la mise en service du secours du site de sauvegarde.

3.3 Analyse des solutions techniques

Cette étape doit permettre de définir l'architecture technique et en particulier de déterminer les solutions techniques susceptibles d'être utilisées.
Notamment :

- les transferts de bandes,
- les transferts de fichiers,
- les transferts de delta,
- la duplication de bandes via le WAN,
- les possibilités de réplication de baies disques,

3.4 Stratégie de sauvegarde

Les sauvegardes ont un objectif double :

- restauration sur le site d'origine suite à une perte quelconque d'un ou de plusieurs fichiers,
- restauration sur le site de backup suite à une décision de mise en œuvre du plan de secours.

Elles doivent donc être utilisables facilement, rapidement et à tout moment. Le plan de sauvegarde doit déterminer :

- la nature des sauvegardes,

- les moyens de sauvegarde,
- la fréquence des sauvegardes,
- la durée de rétention des médias,
- la politique d'externalisation des médias,
- la duplication éventuelle de certaines sauvegardes,
- la politique d'envoi sur le second site de toutes les données différentielles.

3.5 Stratégie de restauration

La restauration consiste à remettre les systèmes et les applications dans un état cohérent tout en limitant le volume de données perdues. En s'appuyant sur l'existence des points de synchronisation, les restaurations doivent être faites de façon cohérente vis à vis des échanges inter-bases. Une base ne doit être ni « en retard », ni « en avance » par rapport aux autres.
La stratégie de restauration doit être définie lors de l'établissement du contrat de service et avoir identifié par priorité les applications à restaurer en premier.
La stratégie de restauration doit naturellement intégrer le fait que potentiellement tout le système d'information ne nécessite pas d'être restauré au même instant.

3.6 Inventaires techniques

En complément des cartographies établies, l'inventaire technique des serveurs à prendre en compte dans le plan de secours (« à backuper » et « backupant ») doit être réalisé : Version, configuration, performances et taux d'utilisation.
Une analyse fine du réseau et en particulier du WAN : liaisons, routeurs, débit utilisé, débit disponible, volumétrie des flux inter-machines et des interfaces, peut être effectuée.
Dans le cas où on envisage la répartition des serveurs sur 2 sites, ces éléments permettront de valider la répartition envisagée des serveurs sur les 2 sites, ainsi qu'une première estimation technique et financière des extensions de serveurs nécessaires.

3.7 Validations techniques

Les solutions techniques déterminées doivent être validées. Des tests en charge doivent être réalisés à partir de volumétries significatives et de jeux d'essais pertinents en tenant compte des contraintes de l'entreprise et tout particulièrement de la bande passante réseau. Ces tests doivent être significatifs, il est donc impératif de disposer des serveurs, robots, baies SAN en nombre et de volumétrie suffisante. Ces éléments devront être interconnectés sur des éléments réseaux à l'identique des serveurs en production.

Les actions suivantes pourront alors être réalisées (liste non exhaustive) :

- analyse du fonctionnement des sauvegardes actuelles,
- test de robot « déporté » à l'extérieur du site de production
- tests de duplication de bandes
- tests de réplication de données via les outils propres aux baies SAN,
- tests de restauration de sauvegarde externalisée,
- tests de remontée des données différentielles,
- tests de remontée et sauvegardes en central
- tests de restauration sur un serveur « backupant »
- tests de re-synchronisation d'environnements restaurés.
- ….

Les tests permettront de valider l'adéquation de l'architecture technique avec le contrat de service. Les stratégies de sauvegarde et de restauration seront confirmées.

3.8 Rapport détaillé du fonctionnement du plan de secours

Ce document doit présenter l'architecture d'exploitation, la configuration, les principes des sauvegardes et de restauration mis en œuvre dans le plan de secours. Les consignes organisationnelles et procédures de déclenchement y figurent également.