

PRA - PCA

Les Sauvegardes de recours : définitions, usages, limites

Synthèse

Les sauvegardes de recours représentent le capital informationnel de l'entreprise qu'il faut absolument conserver, afin d'organiser une reprise ultime quand les plans prévus (PRA) échouent.

Nécessaires à la reprise suite à un sinistre informatique, elles doivent être exhaustives, cohérentes, intègres et mises hors du site objet du PRA.

Actuellement, il n'y a pas d'obligation réglementaire d'effectuer et de conserver des sauvegardes de recours.

L'existence de sites distants ne supprime pas la problématique des sauvegardes de recours.

Les volumes de données à protéger augmentant en permanence, il devient de plus en plus difficile de tout sauvegarder et d'obtenir des sauvegardes de recours cohérentes et complètes. Il existe deux pistes pour résoudre ce problème. La première consiste à se limiter à l'essentiel, à hiérarchiser pour ne conserver que les éléments réellement indispensables à une continuation de l'activité de l'entreprise. L'autre solution consiste à anticiper sur la question de la sauvegarde de recours en intégrant ce sujet à la conception et à la mise en place des applications.

Le transport comme le stockage externe des sauvegardes de recours nécessitent une protection particulière.

Contexte

Le CLUSIF distingue trois types de sauvegardes :

1. les **sauvegardes de production** utilisées pour la réfection des travaux. Le nombre de versions conservées et les points de prise dépendent de la politique de sauvegarde propre à une entreprise,

une entité, une plate-forme, etc., et varient donc énormément selon les contextes. Ces sauvegardes servent à la réfection de travaux et pour remédier à des pertes d'intégrité de données. Comme elles doivent rester facilement accessibles depuis le site de production, rien n'impose de les en extraire. De

nombreuses entreprises les externalisent cependant, ce qui leur procure un niveau de protection supplémentaire en cas de sinistre sur site.

2. les **sauvegardes de recours** suite à sinistre. Elles servent à restaurer le fonctionnement de l'informatique sur le site de secours en cas de besoin. Elles doivent être exhaustives, intègres, cohérentes et impérativement mises hors site pour rester utilisables quoi qu'il arrive. Elles contiennent les données, les applications, les flux et la documentation.
3. les **sauvegardes d'archivage**. Elles servent à restituer les données en réponse à des demandes légales ou contractuelles. Elles sont prises à des moments précis. Elles ont des périodes de conservation longues. Elles peuvent être soumises à des techniques de non-modification. La question de leur externalisation est complexe.

Dans un contexte actuel de type multi-sites, la typologie ci-dessous illustre mieux les types de sauvegardes selon les usages :

1. Sauvegardes de production locale,
2. Sauvegardes de production externalisées,
3. Historisation des données.

Les sauvegardes de production et les sauvegardes de recours diffèrent par leurs objectifs, mais aussi par la logique qui préside à leur création.

Problématique

Le fonctionnement en mode dual site, avec un site de production et un site de secours ou deux sites se secourant mutuellement, ne supprime pas la problématique des sauvegardes de recours. Ces dernières visent en effet à permettre une reprise de l'activité de l'entreprise depuis zéro en cas de sinistre total ayant détruit les données et les moyens de production informatique.

Il s'agit alors de repartir d'ailleurs, sur un autre site, avec d'autres matériels, mais en ayant conservé le cœur du capital informationnel de l'entreprise, cette partie des données, des applications et des procédures qu'il faut absolument préserver pour ne pas risquer que la reprise s'avère extrêmement difficile voire totalement impossible. Avec les sauvegardes de recours, il ne s'agit pas de reproduire l'existant à l'identique, de corriger ou de réparer, mais réellement de posséder les éléments indispensables à une reconstruction de l'activité, éventuellement sur un système d'information totalement neuf.

Destinées à reprendre l'activité suite à un problème majeur, les sauvegardes de recours doivent posséder un caractère fortement autonome. Il faut qu'elles contiennent tous les éléments nécessaires au redémarrage. Elles forment un tout, un ensemble complet et auto-suffisant conçu pour simplifier le travail de reconstruction.

Les sauvegardes de production n'ont pas ce caractère : chacune ne constitue qu'un bloc étroitement lié à d'autres blocs ; elles conviennent parfaitement à la correction d'une donnée corrompue, à la remontée d'une information perdue, mais elles sont fortement dépendantes d'autres sauvegardes.

On pourrait dire qu'une sauvegarde de production n'est qu'une brique dans un ensemble, et que l'assemblage des briques importe plus que l'existence de chaque brique ; alors que la sauvegarde de recours est plus comme un bâtiment qui doit se suffire à lui-même.

Techniquement cela correspond par exemple au fait qu'une sauvegarde de recours sera typiquement réalisée en mode « full », alors qu'une sauvegarde de production fonctionne sur un cycle 1 « full » + n « incrémentales ».

En termes de contenus, la sauvegarde de recours doit abriter une image aussi complète que possible du système d'information à protéger, ce qui veut dire qu'on y trouve les données, mais aussi les programmes (et leurs licences), voire des images des systèmes, et l'ensemble de la documentation associée.

L'inflation constante des volumes de données, pose cependant la question : les sauvegardes de recours peuvent-elles encore exister ?

Les systèmes, les applications, la documentation présentant une relative stabilité, les sauvegarder reste possible. Mais, il est difficile de prendre en compte la totalité des flux échangés dans l'entreprise. Même avec des mécanismes de réplication, la cohérence devient très complexe à gérer.

Un redémarrage à partir de ces supports de recours est devenu très difficile (non cohérence des données sauvegardées et forte complexité des opérations à conduire) induisant des temps de restauration prohibitifs. Un certain nombre de grosses entreprises ont abandonné la perspective de se doter de sauvegardes de recours.

Pourtant les auditeurs internes posent régulièrement la question : comment assurez-vous la reprise de l'activité si l'entreprise perd toutes ses données ?

Comment garantissez-vous que les informations sauvegardées sont suffisantes à une telle opération ?

Analyse

Les demandes des auditeurs ne peuvent pas constituer le seul horizon à prendre en compte concernant les sauvegardes de recours. La question à se poser semble plutôt : quels risques la sauvegarde de recours doit-elle couvrir ? Si l'entreprise possède deux sites informatiques répliqués, le risque de perte totale des deux est fortement réduit (voir le document « PRA et sinistre régional, de l'opportunité d'un troisième site informatique, le secours ultime »). Mais cela suffit-il ?

La sauvegarde de recours vise justement à faire face aux circonstances exceptionnelles, en disposant à l'extérieur d'une image cohérente et exhaustive du cœur de l'activité. Or, pour ce type d'éventualités, le recours aux sauvegardes d'archivage incluant les applications dans une version stable ne suffit pas compte tenu de leur ancienneté.

L'argument économique fait clairement comprendre qu'une sauvegarde cohérente de la totalité du système d'information devient impossible. Il faut donc sélectionner les applications à prendre en compte pour les sauvegardes de recours, et cela dépend des métiers de l'entreprise. Pour certaines d'entre elles, l'expérience montre qu'il suffit de sauvegarder en recours la partie du système d'information qui constitue le vrai patrimoine informationnel de l'entreprise et d'écarter le reste.

Aujourd'hui, la procédure la plus fréquente consiste à sauvegarder sur disques, puis sur cassettes. Beaucoup de sociétés fonctionnant en mode Dual Site n'externalisent plus leurs cassettes. Une sauvegarde de recours, cela peut consister à agréger plusieurs cassettes sur une cassette de recours qui se trouve ensuite externalisée. En cas de sinistre, il sera possible de repartir de là.

Dans les entreprises où le cœur d'activité réside encore sur Mainframe, dans celles où l'activité présente encore un caractère très centralisé en termes informatiques, la création d'une sauvegarde de recours incluant l'essentiel du patrimoine informationnel de l'entreprise reste possible. Avec des équipes compétentes, et même suite à un sinistre grave, il sera possible à partir de ces informations de reprendre les activités essentielles. L'historique sera perdu, mais pas le cœur d'activité en cours, les clients, les contrats, qui sera préservé. Mais les entreprises possédant des mainframes constituent aujourd'hui une exception par leur capacité à consolider leurs bases de données et à le faire sous un volume restreint.

Dans le monde « open », les choses sont beaucoup plus compliquées. Il reste en théorie possible de consolider les quelques bases de données les plus critiques. Mais les volumes de données parfois énormes et surtout leur dispersion rendent très difficile leur simple localisation. La question se pose alors de savoir où se trouvent les données à protéger ?

Ces données dès qu'elles possèdent une valeur critique bénéficient d'une protection par duplication, mais il n'existe pas de point focal de consolidation ce qui induit une perte de cohérence et rend très difficile la constitution d'une image globale de type sauvegarde de recours.

Dans le cas d'un groupe international possédant de nombreuses filiales, une même donnée se trouve copiée en de nombreux emplacements où elle vit ensuite de façon isolée et indépendante, sans opérations de resynchronisation des différentes versions de cette donnée à mesure qu'elle évolue dans le temps. Rapatrier ce type de données sur un site central devient impossible car les métiers sont largement indépendants. La cohérence ne peut être que locale, mais pas recréée au niveau global de l'entreprise.

Dans ce cas, la solution pour obtenir tout de même des sauvegardes de recours consiste à prendre en compte ce problème dès la conception d'une application. Non pas se demander quelle cassette sortir, mais quelle cassette produire, et se demander comment la construire.

Du fait de leur exhaustivité et de leur vaste périmètre, les sauvegardes de recours doivent rester confidentielles, et protégées en cas de vol. Les cartouches les contenant devraient donc être systématiquement chiffrées. Cette fonction, standard dans le monde Mainframe, reste plus rare et plus complexe à gérer dans le monde distribué. Il faudra mettre en place les procédures d'accès aux clés de chiffrement en cas de sinistre.

NB : en cas d'externalisation, Il est fortement conseillé de s'assurer que les clauses contractuelles couvrent les risques de perte, de divulgation d'informations, etc.

Il faut également valider le caractère opérationnel des sauvegardes de recours en prouvant qu'on peut les restaurer, et qu'elles sont exhaustives, en les restaurant une fois par an.

Sauvegardes de recours et urbanisation du SI

La question de la bonne gestion des sauvegardes de recours peut s'aborder sous l'angle d'une contribution à l'urbanisation du système d'information de l'entreprise.

Dans les entreprises de grande taille, les processus ont pris de l'indépendance, entraînant l'utilisation de copies multiples des jeux de données, ce qui pose la question de savoir où se trouvent les données de références. C'est le rôle des démarches d'urbanisation du SI et du travail de cartographie associé de répondre à ces questions. L'exercice de création des données des sauvegardes de recours sera donc l'occasion d'exploiter, de valider et de corriger éventuellement les référentiels d'urbanisation.

De plus, aujourd'hui les entreprises disposent d'infrastructures d'échanges de données, sous forme d'Enterprise Service Bus (ESB) et de Business Process Management (BPM). Ces évolutions contribuent à la meilleure maîtrise de la localisation des données vitales et à une meilleure gestion de leurs déplacements (en particulier avec la capacité à suspendre et temporiser des flux et à garder une trace centralisée des échanges). Grâce à la maturité tirée d'une démarche BPM, l'entreprise sait mieux localiser ses données, ce qui simplifie la démarche de création de sauvegarde de recours.

Les sauvegardes de recours ont donc de grands profits à tirer de ces évolutions. La sécurité est un sujet de base transverse à toute démarche d'urbanisation.

Conclusion

Les sauvegardes de recours sont essentielles pour assurer la reprise d'activité de l'entreprise quoi qu'il arrive. Compte tenu de la répartition des données dans le monde « open » et de l'augmentation des volumes à sauvegarder, il est de plus en plus difficile d'obtenir de telles sauvegardes.

Deux pistes peuvent résoudre ce problème :
ne sauvegarder que l'essentiel et anticiper en prévoyant dès la conception d'une application les sauvegardes de recours.

La survie d'une entreprise ne tient parfois qu'à un fichier...

CRIP

Club des Responsables d'Infrastructures et de Production

15 rue vignon 75008 PARIS - contact@crip-asso.fr

www.crip-asso.fr

Club de la Continuité d'Activité

73 rue Anatole France 92300 LEVALLOIS PERRET - contact@clubpca.eu

www.clubpca.eu

En application de la loi du 11 mars 1957, il est interdit de reproduire ; sous forme de copie, photocopie, reproduction, traduction ou conversion, le présent ouvrage que ce soit mécanique ou électronique, intégralement ou partiellement, sur quelque support que ce soit, sans autorisation du CRIP.