

~

Description générale du produit

Date 07 Avril 2020
Version de ce document V3.02

Contact :
Bruno Taverne
Courriel : btaverne@m81.eu
Téléphone : +33 6 20 27 22 17

Recover for i

1 Description du produit

1.1 Présentation générale

Le produit *Recover for i* a un objectif simple : **réduire les pertes de données à quelques minutes en cas “d’accident” sur votre Base de données.**

Nous entendons par “accident” sur la Base de données tout ce qui « corrompt » les données :

- suppression de tables,
- perte d'intégrité de la base de données,
- fichiers endommagés,
- ...

et ce, du fait d'une multitude de causes potentielles :

- manipulation accidentelle ou malveillante
- bugs de programmes interactifs ou batchs
- objet endommagé suite à une panne franche
- Données corrompues suite à un plantage de programme, ou du fait d'un upgrade ou d'une opération de maintenance qui tourne mal ...
- cyber criminalité : virus, cryptovirus, piratage, ...

Bien sûr, si vous ne disposez pas d'une solution de HA (High Availability) qui réplique au fil de l'eau les données sur une « Stand-by Database », la perte de données la plus importante est potentiellement celle générée par un sinistre ou un « crash » de plusieurs disques. En effet, là, la pénalité est immédiate : il faut repartir de la sauvegarde de la veille.

Mais aussi dans le cas de la corruption d'une seule table importante ... En effet, après des efforts souvent importants et stressants pour tenter de rétablir l'intégrité de la BD, il faut parfois se résoudre à repartir de la dernière sauvegarde et à perdre ainsi de quelques heures à plusieurs dizaines d'heures de données !

Les exemples “d'accidents” de tous types sont nombreux... Et heureusement pour les propriétaires d'IBM i la base de données DB2 for i n'a officiellement pas encore connu de virus ... jusqu'à ce que le premier se produise ...

L'idée de *Recover for i* est d'exporter sur un serveur externe, distinct de votre « IBM Power i », toutes les mises à jour qui sont réalisées sur la Base de données de production (création, suppression, mises à jour d'enregistrements) et, en cas d'accident, d'importer et de réappliquer ces mises à jour sur la base de données restaurée à partir de la dernière sauvegarde.

Résultat RPO (Recovery Point Objective) = quelques minutes au lieu de nombreuses heures !

Combiné avec notre produit *Flash for i*, *Recover for i* vous permet d'améliorer énormément les temps de redémarrage (RTO) et la granularité de la récupération des données (cf. chapitre 2)

Recover for i

1.2 Mode de fonctionnement

a) La journalisation

Le produit **Recover for i** se base sur la journalisation de la base de données de Production. Comme toutes les bases de données, « DB2 for i » historise toutes les modifications apportées aux données (ajout, suppression, modification) dans des « Journaux » de base de données (avec d'autre BD on parle de « Logs »...). Dans l'environnement IBM i, tout le monde a entendu parler du mécanisme de JOURNALISATION.

Les données journalisées sont stockées dans un « récepteur de Journal » attaché à un Journal.

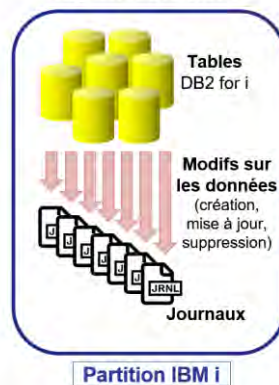
Des commandes système IBM i permettent à la demande (ou par programme) de détacher ces récepteurs de journaux (en les remplaçant immédiatement par de nouveaux récepteurs).

Des commandes système IBM i permettent à partir de ces journaux :

- de « détricoter » les dernières transactions,
- de réappliquer sur la BD à partir d'une étape donnée, les modifications enregistrées.

Ce potentiel est déjà utilisé par beaucoup d'ERP pour 'garantir' leurs transactions.

Recover for i est basé sur la protection 'native' de DB2 :
la journalisation



Il est possible avec **Recover for i** d'utiliser les journaux existants, mais aussi, si besoin, **Recover for i** peut se charger d'en créer de nouveaux.

Nota Bene : il y a 2 limites / écueils à la Journalisation standard :

- les journaux sont stockés sur les disques de la partition de production,
- le « détricotage ou rollback » des dernières transactions n'est pas toujours possible.

Recover for i

b) Export des Journaux

Ainsi **Recover for i** va externaliser les modifications effectuées sur la BD en détachant les récepteurs de journaux, et en les exportant vers un serveur de stockage externe à la partition IBM i. Ces opérations d'externalisation sont réalisées automatiquement, à intervalle régulier, par exemple toutes les 5 minutes. La fréquence est paramétrable. Les récepteurs sont simplement stockés sur le serveur de stockage externe, en prévision d'une utilisation ultérieure.

Le serveur de stockage externe doit disposer d'un peu d'espace disque afin de conserver les journaux d'une journée (voire 2 ou 3 journées). Avec **Recover for i**, il est possible de compresser les éléments envoyés sur le serveur de stockage pour réduire encore la place nécessaire.

Le serveur de stockage externe doit supporter le protocole FTP ou NFS, protocole standard de la plupart des serveurs de fichiers Windows, Linux ou NAS (ou autres appliances comme par exemple le NAS 'DiskStation' de Synology à quelques centaines d'Euros).

Le fait que le serveur FTP/NFS soit externe à la partition IBM i garanti que son contenu soit conservé en cas de « crash » matériel ou « d'accident de données ».

c) Import des Journaux et application

Dans quels cas et comment vont pouvoir être utilisés ces « Journaux » stockés à intervalles réguliers sur un serveur de stockage externe ?

Cas 1 : Crash disque SANS solution de secours

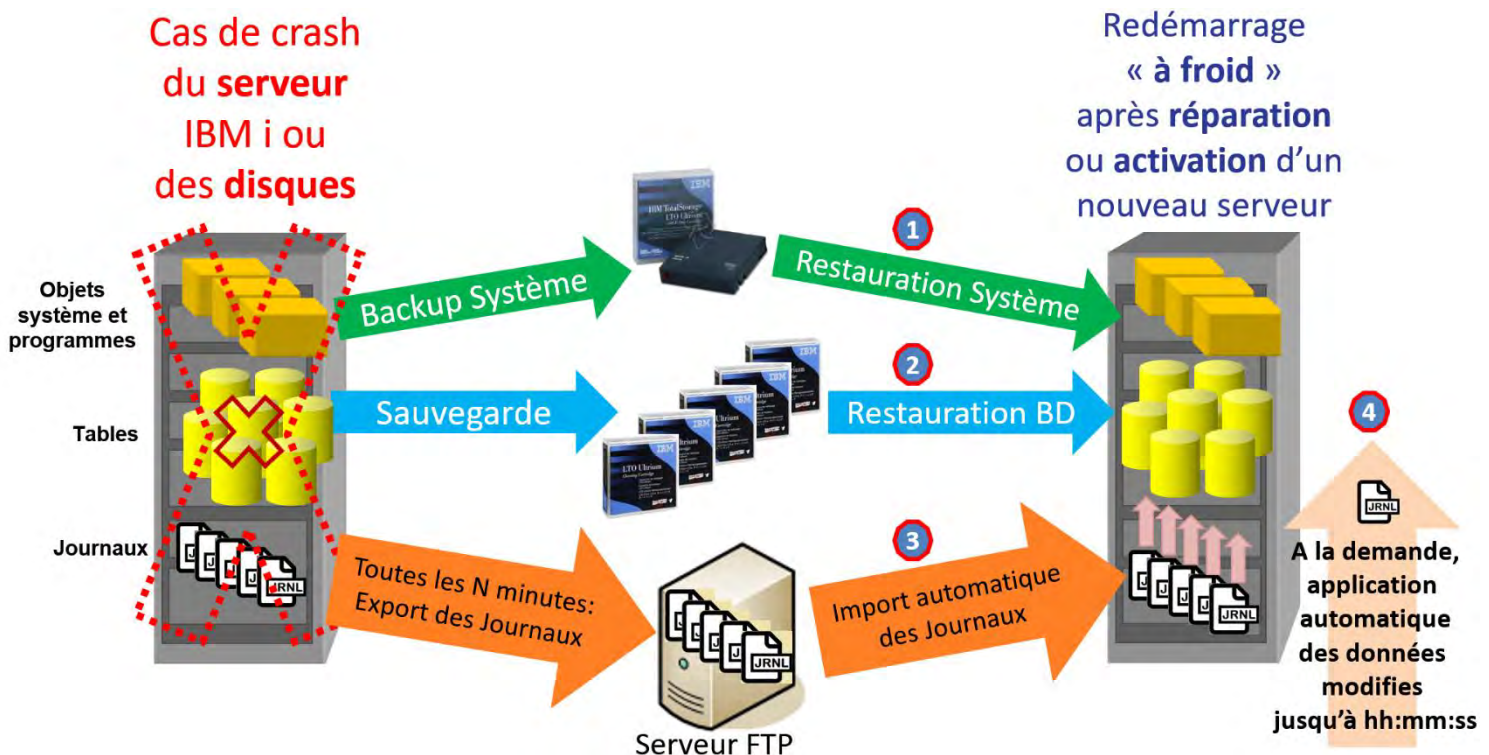
La base de données est perdue ...

Les étapes pour le redémarrage sont les suivantes :

- Réparation des disques par le SAV
- Restauration complète de la partition de Production
 - o à partir d'une sauvegarde système (SAVE21) ①
 - o puis de la dernière cartouche de sauvegarde quotidienne ②
- **Recover for i** est donc aussi restauré.
 - o Il va automatiquement retrouver et identifier les récepteurs de Journaux sur le serveur de stockage
 - o les rapatrier sur la partition IBM i ③
 - o et appliquer les modifications sur la base de données ④.

➔ **La base de données sera ainsi rétablie automatiquement telle qu'elle était quelques minutes avant le crash des disques !**

Recover for i



Variante 1bis : Sinistre complet SANS solution de HA

Par « solution de HA » nous voulons dire « solution de secours à chaud » du marché (réplication ou mirroring).

Après un sinistre, le serveur est « hors service » (voire même le bâtiment ou le site complet).

Dans ce cas, on en revient au cas n°1 précédent : les mêmes étapes de recovery sont à enchaîner, sauf qu'en amont il faut approvisionner un serveur intact ...

En cas de sinistre, l'externalisation du serveur de fichier FTP apparaît comme préférable ...

Variante 1ter : Sinistre avec solution de secours « à froid »

Cette variante consiste à disposer d'un serveur « de spare », sur un autre site ou d'un contrat de mise à disposition d'un serveur de secours ou d'une partition IBM i auprès d'un hébergeur ou Cloud Provider (= **PRA as a Service** ou **Rescue as a Service / RaaS**).

Dans ce dernier cas on peut configurer **Recover for i** afin que les Journaux soient envoyés sur un serveur de fichier du Cloud Provider. Le surcoût de quelques Go de stockage par rapport à l'offre RaaS de base sera réduit, alors que le résultat sera incomparable !

➔ **La partition de secours sera redémarrée avec la base de données telle qu'elle était quelques minutes avant le sinistre !**

Recover for i

Cas 2 : « Accident de données » AVEC ou SANS solution de HA

Si on dispose d'une solution de HA, après un sinistre on retrouve ses données sur le site de secours. En effet, elles sont répliquées sur la stand-by Database (solution « software ») ou mirrorées sur les disques miroirs (solution « hardware »).

Mais, quand il s'agit d'un « accident de données » (rappel : corruption, suppression de tables, fichiers endommagés, perte d'intégrité, cryptovirus, ...) alors AVEC ou SANS solution de HA, le résultat est le même : en effet **la solution de HA propage immédiatement « l'accident de données » sur la Base de données de secours** (Standby Database) !!! Et après des heures d'efforts, il faudra, HA ou pas, potentiellement se résoudre à repartir de la dernière sauvegarde en perdant plusieurs heures de données (et réaliser avoir investi beaucoup d'argent dans une solution de HA en croyant être à l'abri de ce genre de mésaventure 😞) ...

Dans le cas d'un « accident de données » (AVEC ou SANS solution de HA) le process est alors le suivant :

- Le serveur est toujours présent ainsi que la partition de Production :
 - o restauration de la dernière cartouche de sauvegarde quotidienne sur la partition de Production (ou sur une autre partition ou sur un autre serveur)
- **Recover for i :**
 - o va automatiquement retrouver et identifier les récepteurs de Journaux sur le serveur de stockage,
 - o les rapatrier sur la partition IBM i,
- L'administrateur va déterminer le moment où l'accident a eu lieu car il vaut mieux ne pas appliquer les modifications jusqu'au moment exact de l'accident ...
- **Recover for i :**
 - o Va appliquer automatiquement les modifications sur l'ensemble de la base de données restaurée jusqu'à quelques minutes avant « l'accident ».

➔ **Même en cas « d'accident de données » l'utilisation de *Recover for i* permet de ne pas perdre plus de quelques minutes de données !**

⇒ **Et *Recover for i* constitue donc un excellent complément à une solution de HA !!!**

Recover for i

2 'Recover for i' associé à 'Flash for i'

Flash for i, est un autre produit de M81, disponible depuis 4 ans et équipant 150 partitions IBM i (cf. site www.m81.eu/flash-for-i/)

Lorsque **Recover for i** est utilisé de façon conjointe avec **Flash for i** l'automatisation, les délais et la granularité sont améliorés.

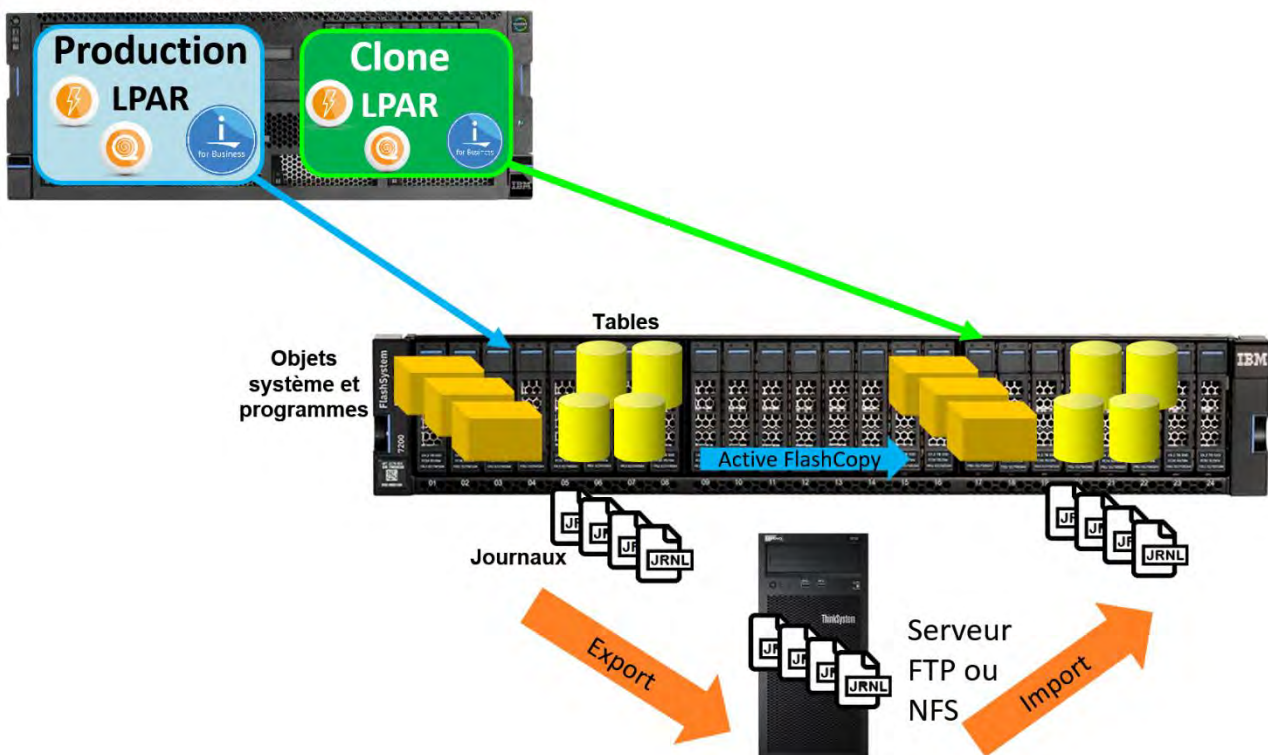
2.1 Mode de fonctionnement

Les opérations automatisées sont les suivantes:

- **Flash for i** (sur la partition de 'Prod') :
 - o pilote la création d'un 'clone' des disques de production
 - o démarre une partition 'clone' à partir des disques 'clones'
 Nota Bene : cette partition 'clone' peut par exemple être utilisée pour réaliser des sauvegardes sans arrêter les utilisateurs.
- **Recover for i** (sur la partition de 'Prod') :
 - o pilote le détachement des journaux de la base de données de production, toutes les N minutes
 - o réalise l'envoi et le stockage des journaux sur le serveur FTP
- **Recover for i** (sur la partition 'Clone') :
 - o recherche et détecte les journaux sur le serveur FTP
 - o les rapatrie et les restaure.

⇒ Les journaux sont donc présents sur la partition 'Clone' mais « dormants ».

Server de Production



Recover for i

En cas « d'accident de données » sur la base de données de Production (toujours SANS ou AVEC une solution de HA) :

- L'administrateur décide du moment exact jusqu'auquel **Recover for i** va réappliquer les modifications des Journaux sur la BD (et ce, depuis les journaux rapatriés précédemment)
- Au travers d'une unique commande **Recover for i** (sur la partition 'Clone') :
 - o va automatiquement réappliquer les données modifiées
 - sur la base de données 'Clone' (qui est dans le statut du moment de la création du dernier clone),
 - jusqu'au moment voulu (hh:mm:ss).

➔ **Une base de données complète, intègre, avec des données datant de quelques minutes avant « l'accident » est donc disponible et opérationnelle sur la partition 'CLONE'.**

Pour repasser en PRODUCTION avec une BD intègre, les administrateurs ont alors deux solutions :

- A. Copier manuellement les tables remises à niveau depuis la partition 'Clone' vers la partition de 'Prod'
- B. Démarrer la partition de Prod en utilisant les disques 'Clones' (contenant la base de données réactualisée).
Cette dernière technique est appelée par IBM « Reverse FlashCopy » et est documentée par M81.

➔ Ainsi, même en cas « d'accident de données » le duo **Recover for i** et **Flash for i** permet :

- de redémarrer très **rapidement**
- avec une base de données intègre complète,
 - o que ce soit en traitant 100% de la BD en une fois
 - o ou bien seulement les quelques **bibliothèques ou tables** ayant été corrompues.

2.2 Variante : opérations réalisées sur le site de secours

Avec une solution de secours en place (HA/DR Software ou Hardware)

⇒ *Le duo de produits "Flash for i" et "Recover for i" peut être utilisé sur la partition de secours.*

L'objectif reste le même : réduire au minimum la perte de données potentielle en cas « d'accident » sur la base de données de PROD (comme suppression de table, perte d'intégrité, corruption de base, etc...) sachant que l'incident est reproduit instantanément sur la base de données de secours par la solution de HA/DR en place .

⇒ *L'intérêt réside sur le fait que deux démarches peuvent être menées en parallèle :*



Recover for i

- tenter de rétablir l'intégrité de la base de Production sur la partition de Production
- réaliser les opérations de « recovery » de la BD sur la configuration de secours

Avec **Flash for i** et **Recover for i** utilisés sur la partition de **secours** toutes les opérations décrites au chapitre précédent (§2.1) peuvent être déroulées et permettre de redémarrer

- **rapidement**
- sur le **site de secours**
- avec **seulement quelques minutes de perte de données !**

3 Compléments

3.1 Avertissement

Le produit **Recover for i** n'est pas un produit de Haute Disponibilité (HA). Ses principales différences par rapport à un produit de HA sont les suivantes :

- La mise à jour des données dans la base de données cible n'est pas réalisée en temps réel.
- La sélection des objets à prendre en compte est effectuée au niveau de la bibliothèque. Il n'est pas possible d'exclure certains fichiers ou objets.
- Seules les bibliothèques et leur contenu sont pris en compte. Aucun traitement n'est fait sur l'IFS ou les DLO.

Pendant une phase avec une activité de développement intense, ce produit n'est pas adapté ; en effet :

- En cas de modification de la structure de la base de données seules les données mises à jour avant la modification seront prises en compte.
- La journalisation ne doit jamais être arrêtée.
- Le traitement des objets de type programmes ou commandes ne sont pris en compte que partiellement.

Bien que les programmes, objets systèmes, profils utilisateurs, données de configuration, journal d'Audit ne soient pas pris en charge dans les automatismes de Recover for i il est possible de lancer avec une commande, par exemple, une copie d'externalisation par jour de ces composants vers le serveur FTP.

Recover for i

3.2 Automatisation et suivi

Tous les traitements sont entièrement automatiques.

Toutes les opérations décrites ci-dessus sont réalisées sans aucun impact sur les utilisateurs ni sur les traitements en cours.

Plusieurs commandes permettent de visualiser (et contrôler) la situation de l'exportation, de l'importation et de la ré-application des Journaux.

Plusieurs commandes permettent de surveiller automatiquement le bon déroulement des opérations. Ces commandes peuvent être intégrées dans un outil de surveillance tel que Nagios par exemple (et bien sûr elles sont intégrées à notre produit **Control for i**)

3.3 Prérequis

- IBM i (OS/400) : Version 7.1 et au-dessus
- Stockage : un serveur FTP ou NFS externe (y compris toute 'appliance' ou NAS avec protocole FTP ou NFS intégré)
- Place disque nécessaire : le vécu montre, qu'en général, les journaux d'une journée occupent un volume relativement faible (mais il y peut y avoir des exceptions).

3.4 Quelques références



Ce document n'est pas contractuel. Il est fourni à titre informatif. M81 se réserve le droit de modifier les spécifications ou la forme des produits sans préavis et sans engager sa responsabilité.