Mesures techniques : Redondance et sauvegarde

M231 — Appliquer la protection et la sécurité des données

Jérôme Frossard

EPAI

14 mai 2024

Plan

Plan

Introduction

Lors de la conception de bases de données, on cherche généralement à minimiser la redondance des données, principalement afin d'éviter des problèmes d'intégrité.

Cependant, il est parfois utile d'introduire volontairement de la redondance afin d'améliorer la fiabilité d'un système et la disponibilité des données.

Le but de cette présentation est d'aborder quelques-uns des principaux exemples de redondance souhaitable et volontaire :

- Redondance matérielle (RAID)
- Réplication de base de données
- Synchronisation des données dans un cloud
- Gestion de versions
- Sauvegarde des données et schémas de rotation

Plan

Qu'est-ce que la redondance matérielle ?

Pour la protection des données, la redondance matérielle constitue une **mesure préventive**. Elle augmente la **disponibilité des données** en réduisant les risques de perte de données et d'interruption de service.

Elle consiste à dupliquer certains composants d'un système informatique. Cela permet un **basculement** (*failover*) sur un composant passif en cas de panne du composant actif, ou une **répartition de charge** (*load balancing*) si tous les composants sont actifs.

Exemples de redondance matérielle :

- Alimentation de secours (UPS) et alimentations redondantes
- Redondance d'interfaces et d'équipements réseau (LACP, STP, etc.)
- Redondance de disques (RAID, etc.)
- Redondance de la mémoire vive (mémoire ECC, RAIM, etc.)
- Redondance de systèmes informatiques complets (grappe de serveurs ou ***cluster***)

Dans la suite de la présentation, notre attention va se porter sur les RAID et les clusters.

Redondance de disques : RAID

Un RAID (Redundant Array of Independent Disks) est une technologie de stockage qui combine **plusieurs disques durs ou SSD** en **une seule unité logique** pour augmenter la tolérance aux pannes et les performances.

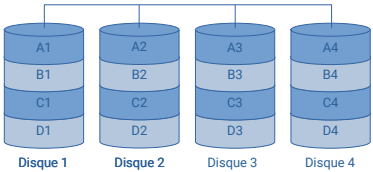
Il existe plusieurs **niveaux de RAID**, chacun offrant différents avantages et compromis. Les plus courants sont :

- **RAID 0** : agrégation par bande (*striping*), pas de redondance.
- **RAID 1** : miroir (*mirroring*)
- **RAID 5**, **RAID 6** : agrégation par bande avec parité simple (RAID 5) ou double (RAID 6)
- **RAID 10**, **RAID 50**, **RAID 60** : agrégation par bande (RAID 0) sur plusieurs unités logiques identiques (RAID 1, RAID 5 ou RAID 6)

Redondance de disques : RAID 0

Un **RAID 0** combine **deux disques ou plus** en une unité logique, sans aucune redondance. Ce n'est donc **pas vraiment un RAID**.

- Ne peut être utilisé que dans des situations où **seule la performance compte**.
- **Pas de tolérance de panne** et la fiabilité diminue avec l'augmentation du nombre de disques*.



- **Agrégation par bande (*striping*)** : les disques sont divisés en blocs de 128 à 512 kB. On remplit d'abord le 1er bloc de chaque disque, puis le 2e bloc de chaque disque, etc., pour former des bandes (*stripes*).

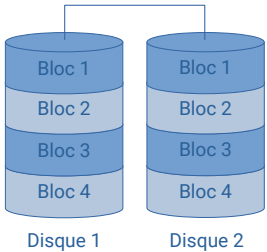
Dans un contexte de la protection des données, le RAID 0 n'a pas d'utilité, mais l'agrégation par bande est mise en œuvre dans tous les autres niveaux de RAID à l'exception du RAID 1.

***** Si un disque unique a un taux de panne annuel de 0.93%, celui d'un RAID 0 de 6 disques est de 5.5%.

Redondance de disques : RAID 1

Un **RAID 1** combine deux disques — parfois trois, rarement plus — en une unité logique. Les disques sont des **miroirs** les uns des autres.

- **Tolérance de panne :** Tolère la perte de **n – 1 disques** (n est le nombre de disques). Fiabilité très supérieure à celle d'un disque unique.
- **Performances :** Potentiellement supérieur en lecture, similaire en écriture.
- **Coût :** Au moins **50% de l'espace de stockage** installé.

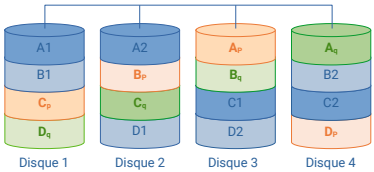


Le contrôleur écrit les données sur tous les disques, simultanément, au même emplacement, mais il peut lire, en même temps, un emplacement différent sur chaque disque.

Redondance de disques : RAID 6

Un **RAID 6** combine au moins quatre disques en une unité logique. Utilise l'**agrégation par bande** (*striping*) avec **deux blocs de parité par bande**. Ces blocs sont répartis sur les disques de manière cyclique .

- **Tolérance de panne :** Tolère la perte de **deux** disques. Fiabilité très supérieure à celle d'un disque unique.
- **Performances :** Augmentent avec le nombre de disques en lecture, moins bonne en écriture.



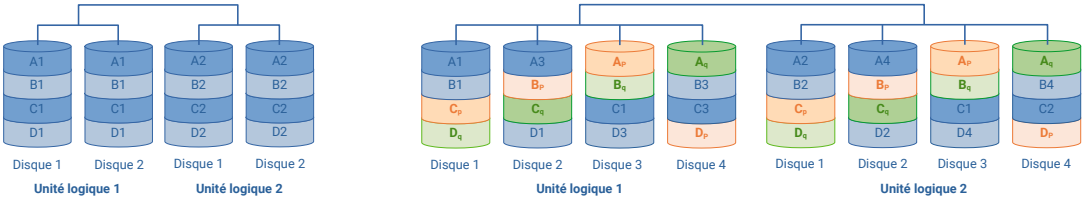
- **Coût :** Espace de stockage de **deux disques**, quel que soit le nombre de disques. Le coût diminue avec l'augmentation du nombre de disques, mais la fiabilité également.

Remarque : Avec un seul bloc de parité, le **RAID 5** a un coût moins élevé, mais il est limité en pratique à une **capacité maximale d'environ 10 TB**. Au-delà, le **risque de panne d'un second disque ou d'erreur non récupérable** lors de la reconstruction après la panne d'un disque devient **trop grand**.

Redondance de disques : RAID 10 et RAID 60

Les niveaux de RAID 10 et 60 consistent à faire un RAID 0 avec des unités logiques (RAID 1 ou RAID6) dans le but d'obtenir à la fois de bonnes **performances en lecture et en écriture** et une **tolérance de panne**.

- **Raid 10** : **très bonnes performances**, coût élevé (50% de l'espace de stockage)
- **RAID 60** : **bon compromis** entre performances et coût (deux disques par unité logique)



Gestion de volumes et stockage distribué

La gestion de volumes RAID peut être réalisée soit par un contrôleur **RAID matériel**, soit par le système d'exploitation avec une configuration matérielle **JBOD** (*just a bunch of disks*).

Les systèmes d'exploitation modernes disposent également de solutions de **virtualisation du stockage**, qui permettent une **gestion plus souple des volumes** tout en assurant la redondance des données. Par exemple :

- Windows Server Storage Spaces
- LVM (*Logical Volume Manager*) sous Linux
- ZFS (*Zettabyte File System*)

Enfin, on peut mentionner les solutions de **stockage distribué** comme **Ceph** ou **VMware vSAN**, qui reposent sur la redondance de systèmes informatiques complets.

Redondance de systèmes informatiques complets

Plusieurs systèmes informatiques redondants utilisés comme une seule entité constituent ce que l'on appelle une **grappe de serveurs (*cluster*)**. Par exemple :

- **Cluster de cibles iSCSI** : baie de stockage (*storage array*) dans un SAN.
- **Cluster de stockage** : système de stockage distribué (Ceph, vSAN, etc.)
- **Cluster de base de données** : réplication de bases de données.
- **Cluster de serveur de fichier** : réplication de fichiers.

Dans une grappe de serveur, un système individuel est appelé un nœud (*node*). Le plus souvent, chaque nœud est équipé de composants matériels redondants : alimentation, interfaces réseau, RAID.

On utilise un **répartiteur de charge (*load balancer*)** ou un proxy inverse pour distribuer les requêtes aux différents nœuds, ou un gestionnaire de ressource (*cluster resource manager*) pour automatiser le **basculement (*failover*)** vers un nouveau nœud actif.

Plan

Synchronisation des données

Dans un cluster de base de données ou de serveurs de fichier, chaque système contient une copie des données appelée **réplica**. Un mécanisme de **synchronisation des données** maintient la cohérence (*consistency*) entre les réplicas.

- **Réplication primaire-secondaire** (unidirectionnelle) : les données du système secondaire sont synchronisées avec celle du système primaire (données de référence). Pour assurer la cohérence, le système secondaire doit être en lecture seule. Il peut y avoir plusieurs systèmes secondaires.
- **Réplication primaire-primaire** (bidirectionnelle) : les données de tous les systèmes peuvent être modifiées et les données d'un système doivent être synchronisées avec celle de tous les autres. Des conflits peuvent survenir et leur résolution ne peut pas toujours être automatisée.

On peut utiliser des mécanismes de synchronisation similaires pour synchroniser des fichiers.

Synchronisation du répertoire personnel

La synchronisation du répertoire personnel permet aux utilisateur·rice·s de disposer de leurs documents sur tous leurs ordinateurs personnels (ordinateur portable, ordinateur de bureau, etc.), et offre une protection contre la perte de données en cas de panne.

Pour cela, on peut synchroniser les données :

- Vers un **serveur de fichiers** sur site :
  - Unison, rsync, lsyncd, etc.
- Vers un **service d'hébergement de fichier** (*file-hosting service*) en ligne :
  - sur site : NextCloud, OwnCloud, Seafile, etc.
  - public : OneDrive, Google Drive, DropBox, etc.

Peu de risque de conflit puisque l'on ne travaille pas simultanément sur plusieurs machines.

Synchronisation de serveur de fichier

L'utilisation de répertoires partagés dans un serveur de fichiers permet souvent d'améliorer la protection des données en facilitant notamment le contrôle d'accès et la sauvegarde.

Toutefois, en cas de panne d'un serveur de fichier, il peut être utile de disposer d'une copie du répertoire partagé sur un autre serveur de fichier afin d'éviter une interruption de service.

Pour cela, on peut synchroniser les données :

- entre les différents nœuds d'un cluster de serveurs de fichiers sur site (*on premise*)
- avec un service de partage de fichier hébergé (Microsoft Azur Files, Amazon S3 File Gateway, Google Cloud Filestore, etc.) qui supporte les protocoles SMB et NFS.

Protection des données et Cloud

La synchronisation des données dans le Cloud peut poser des problèmes de conformité aux exigences de la protection des données.

En particulier, l'utilisation de service d'hébergement de fichier en ligne personnel en milieu professionnel fait courir le risque de stocker des données personnelle ou sensible sur des serveurs soumis au *Patriot Act* qui en autorise l'accès au gouvernement étasunien.

Pour un usage professionnel, ces services doivent :

- Offrir des garanties quant à la localisation des données sur le territoire national
- Permettre la gestion des clés de chiffrement par le client (*tenant*).

Gestion de version et corbeille

La synchronisation des fichiers n'est pas une sauvegarde. Si un fichier est accidentellement modifié ou supprimé sur l'un des systèmes synchronisés, il est également sur les autres.

Pour mitiger le risque de perte de données, les services d'hébergement de fichiers ont généralement deux mécanismes :

- **Gestion de version** : permets de revenir à une version précédente d'un fichier. En principe une nouvelle version est créée à chaque modification enregistrée.
- **Corbeille** : permets de restaurer un fichier supprimé par erreur. La corbeille est généralement vidée automatiquement après un certain nombre de jours.

Ces deux mécanismes permettent de réduire le risque de perte de données accidentelles, mais cela n'élimine pas les autres risques (malware, sabotage, etc.).

Pour mitiger ces risques, il est nécessaire d'avoir une copie des données **figée dans le temps** sur un autre support : une sauvegarde.

Plan

Sauvegarde et restauration

De manière générale, la **sauvegarde (*backup*)** des données désigne les différentes stratégies et procédures permettant de se protéger contre la perte de donnée, et constitue une **mesure de prévention** essentielle pour **protection de données**.

La sauvegarde permet la **restauration (*recovery*)** des données, c.-à-d. leur reconstruction, en cas d'événements tels que :

- suppression ou modification accidentelle,
- corruption liée à une erreur logicielle (*bug*),
- défaillance matérielle,
- catastrophe d'origine humaine intentionnelle ou non (incendie, terrorisme, guerre, etc.)
- catastrophe naturelle (tremblement de terre, inondation, etc.)

Qu'est-ce qu'une sauvegarde ?

D'un point de vue technique, une sauvegarde est une **copie** d'un ensemble de données (un fichier, un répertoire, une base de données, etc.) stockées sur un **support différent** de celui des données originales, et idéalement conservé en un lieu différent.

Le support peut être, par exemple, une clé USB, un disque dur externe, un NAS, une bande magnétique (LTO), ou un service de stockage en ligne.

Pour être en conformité avec les exigences de protection des données, la copie doit :

- Préserver **l'intégrité et la cohérence** des données
- Être **protégée contre les accès non autorisés** (chiffrement).

La **sauvegarde** doit être distinguée de l'**archivage** dont le but est la conservation des données sur une longue durée. L'archivage est également soumis à d'autres contraintes en matière de protection des données (anonymisation, pseudonymisation, etc.)

RPO et RTO

Avant la survenue d'un sinistre, une entreprise doit savoir quelle est la perte de données admissible et en combien de temps le système doit être redémarré, pour assurer la continuité des opérations.

Ces deux informations sont appelées, respectivement RPO et RTO :

- **Point de récupération visé** (*recovery point objective*, **RPO**) : La perte de données maximale tolérable par l'entreprise. En pratique, c'est le temps maximal écoulé entre la dernière sauvegarde et la défaillance.
- **Temps de récupération visé** (*recovery time objective*, **RTO**) : est la durée maximum fixée par votre entreprise pour restaurer les opérations normales après une panne ou une perte de données.

Type de sauvegarde (1/2)

Le temps requis pour effectuer une copie complète des données peut dépasser l'objectif de point de récupération (RPO). De plus, si les données changent peu, le coût lié au stockage de multiples copies de données identiques s'ajoute à celui du temps.

Une première solution est d'utiliser différents **types de sauvegarde** :

- **Complète :** Sauvegarde de l'ensemble des données. Peut être utilisée comme base pour d'autres types de sauvegarde.
- **Incrémentale :** Sauvegarde des données modifiées depuis la dernière sauvegarde. Réduit le temps et l'espace de stockage nécessaires à la sauvegarde, mais augmente le temps nécessaire à la restauration (RTO).
- **Différentielle :** Sauvegarde des données modifiées depuis la dernière sauvegarde complète. Offre un compromis entre le temps nécessaire à la sauvegarde et celui nécessaire à la restauration, bien que l'espace de stockage requis soit supérieur à celui d'une sauvegarde incrémentale.

Type de sauvegarde (2/2)

Parmi les autres solutions, on peut mentionner :

- **Déduplication** : Pour éviter de stocker de multiple copie de données identique, le système n'en stocke qu'une seule copie et remplace les différentes copies par des références à cette copie. La déduplication peut être réalisée au niveau des blocs du disque, ou au niveau des fichiers.
- **Sauvegarde incrémentale inverse** : Avec une sauvegarde incrémentale, la dernière sauvegarde est toujours complète. Elle est calculée à partir de la sauvegarde précédente et de la nouvelle sauvegarde incrémentale. Combine les avantages en temps et espace de stockage de la sauvegarde incrémentale, et la simplicité de restauration de la sauvegarde complète.
- **Sauvegarde en continu (CDP)** : L'idée est de réduire le temps entre deux sauvegardes incrémentales au point de sauvegarder chaque écriture sur un volume. Cette solution est particulièrement indiquée pour des volumes de données importants et des fenêtres de sauvegarde extrêmement réduite.

Cohérence de la sauvegarde

Pour assurer la cohérence des données sauvegardées, il est important que les données ne soient pas modifiées durant la sauvegarde.

Il existe plusieurs solutions :

- **Sauvegarde à froid** : assure que les services susceptibles de modifier les fichiers sont à l'arrêt durant la sauvegarde.
- **Sauvegarde à chaud** : effectue une copie complète des fichiers sans garantir immédiatement la cohérence, puis effectue une synchronisation des changements d'une manière ou d'une autre.
- **Utilisation de snapshot** : sauvegarde d'un snapshot, qui est une image des données à un instant donné. Les snapshots sont gérés par le gestionnaire de volumes, qui doit supporter cette fonctionnalité.

Schémas de rotation des supports

Un schéma de rotation des supports permet de gérer efficacement les sauvegardes et de maximiser l'utilisation des supports de données, typiquement des bandes magnétiques.

Par exemple :

- **Grand-père-Père-Fils (GFS)** : Permet de sauvegarder des données à deux endroits différents avec trois fréquences de répétition (quotidienne, hebdomadaire, mensuelle). Utilise généralement des sauvegardes complètes sur les *pères* et *grands-pères*, et différentielles ou incrémentales sur les *fils*.
- **Tours de Hanoi** : Utilise au moins trois supports, auxquels on attribue une lettre (A, B, C, etc.). La lettre A représente le plus petit disque. L'ordre des supports correspond à celui du déplacement des disques dans le jeu. Le support A est utilisé tous les deux jours ; le support B, tous les 4 jours à partir du deuxième, et ainsi de suite.

Précautions nécessaires

Pour assurer l'efficacité d'une sauvegarde, il y a plusieurs précautions à prendre :

- **Tester régulièrement les sauvegardes** : Procéder à des tests de restauration, ou au moins vérifier l'intégrité des sauvegardes.
- **Observer le principe 3 2 1** : Trois copies, deux supports différents (p. ex. disque et bande magnétique), et une copie hors site. Une sauvegarde est souvent exécutée en deux étapes (*two stages*), d'abord du support original vers un disque de sauvegarde, puis du disque de sauvegarde vers une bande magnétique.
- **Automatiser et surveiller** : Le système de sauvegarde doit être automatique et doit inscrire les succès et les erreurs dans le journal du système d'exploitation. Une surveillance automatisée des journaux permet de lancer une alerte si une sauvegarde a échoué ou si elle n'a pas été exécutée.

Solutions de sauvegarde

Il existe de nombreuses solutions de sauvegarde, sous licence libre ou propriétaire.

Exemple de solutions de sauvegarde personnelles :

- **Libre** : BorgBackup, Rsync, lsyncd, etc.
- **Propriétaire** : Veeam Backup & Replication, Acronis Cyber Protect Home Office, etc.

Exemple de solutions de sauvegarde pour l'entreprise :

- **Libre** : Amanda, Bacula, BackupPC, etc.
- **Propriétaire** : Veeam Data Plateforme, Acronis Cyber Backup, etc.