

# Chapitre 5

## La sécurité des données

### 1. Les risques de perte des données

La sauvegarde des données est essentielle pour une entreprise, quelle que soit sa taille, à partir du moment où toute information importante est stockée sur l'infrastructure de son réseau.

Il n'est pas indispensable systématiquement d'imaginer le pire, mais il est néanmoins rationnel de prendre en compte toutes les éventualités pouvant conduire à la perte partielle ou totale, temporaire ou définitive, des informations de l'entreprise. Voici quelques exemples de risques susceptibles d'affecter les données d'un système d'information :

- Dysfonctionnement du réseau électrique général pouvant amener des coupures avec pour conséquence des corruptions de données.
- Défaut du système d'exploitation.
- Virus informatiques et logiciels malveillants.
- Dommages ou pannes du matériel (disques durs...).
- Suppression de fichiers (accidentelle ou non).
- Altération, modification ou suppression d'informations à mauvais escient.
- Vol de matériels, de logiciels ; sabotages.
- Erreurs de traitement de données.
- Catastrophes naturelles.

L'éventualité de pertes de données importantes pour l'entreprise implique la nécessité d'effectuer des copies des données à l'aide de sauvegardes et d'archives pour toute l'infrastructure informatique (serveurs de production, de développement...).

## Les principes généraux

Des copies de sauvegarde de toutes les données opérationnelles doivent être effectuées pour permettre la reconstruction dans le cas où elles seraient détruites ou perdues.

L'application de sauvegarde doit être prévue pour être installée sur des serveurs de telle façon que les transferts de données soient le plus efficace possible et que la bande passante du réseau ne soit pas affectée surtout pendant les moments les plus utilisés par les applications métier de l'entreprise.

Il est fortement recommandé de stocker les copies de sauvegarde dans un emplacement sécurisé éloigné du site où se trouvent la plupart des systèmes critiques. Dans le cas d'un incident grave ou d'un sinistre affectant totalement ces systèmes, cette précaution permettra de remettre en service des machines équivalentes sur un site différent.

Les supports de sauvegarde utilisés pour les opérations de sauvegarde doivent être testés périodiquement pour s'assurer que les données peuvent être restaurées dans un état correct à chaque fois que cela est nécessaire.

Les principes généraux présentés sont valables pour la plupart des logiciels et applications de sauvegarde. Des différences peuvent exister. Chacune de ces applications possède des spécifications relatives à l'éditeur qui les a conçus et à l'environnement pour lequel il a été prévu. Chaque entreprise choisit son application de sauvegarde en fonction de son environnement et de ses décisions stratégiques.

Dans ce chapitre, les informations présentées peuvent être différentes selon les applications et leur éditeur. Toutefois, les principes décrits sont toujours valables.

## 2. La sauvegarde et la restauration

### 2.1 Concepts généraux

Il est utile, pour commencer, de définir les concepts principaux qui seront utilisés dans les prochains chapitres.

#### 2.1.1 Définitions

##### Le serveur de sauvegarde

Il s'agit d'un serveur équipé d'un ou de plusieurs périphériques de stockage, en général dédiés à cette fonction. Son rôle principal consiste à réaliser les phases de sauvegarde, d'archivage, de restauration de données (système d'exploitation, fichiers, bases de données...).

##### Le client de sauvegarde

Le serveur est également sauvegardé par l'application de sauvegarde, il est donc aussi client de l'application.

Les machines clientes sont aussi des serveurs, elles représentent les environnements à sauvegarder.

Le client comprend un ensemble de données à sauvegarder sur une machine spécifiée (serveur de fichiers, d'application...).

Plusieurs clients peuvent coexister sur une même machine physique, chaque client ayant ses propres attributs. Ce sont :

- Un nom : toujours le nom du serveur connu sur le réseau de l'entreprise.
- Des ensembles à sauvegarder ou save-sets : des noms de fichiers, de répertoires ou de systèmes de fichiers.
- L'appartenance à un groupe, un planning de sauvegarde, une directive, des politiques...
- Un alias : autre nom de la machine dans le réseau.

- Nœuds de stockage : liste prioritaire des périphériques locaux ou distants vers lesquels vont être envoyés les flux de données.
- Nœuds de stockage de clonage : liste prioritaire pour cette opération.
- Politiques de rétention des données et de recherche.

Les clients peuvent regrouper et posséder des attributs propres :

- Nom.
- Heure de démarrage.
- Type de démarrage.
- Politique de rétention des données et de recherche.

## L'application de sauvegarde

C'est le logiciel installé sur le serveur de sauvegarde. Sa fonction consiste à gérer les opérations sur les supports, les connexions sur les clients, à signaler les erreurs rencontrées.

## Les groupes d'utilisateurs et les droits d'accès

Dans l'application de sauvegarde, des groupes d'utilisateurs peuvent être créés pour les opérations de sauvegarde, de restauration ou d'archivage. Un utilisateur doit appartenir à un groupe avant de pouvoir se voir attribuer des droits d'accès particuliers. En effet, sauvegarder et restaurer revient à copier des données, il convient donc de limiter l'accès aux utilisateurs autorisés. Ce qui implique un système de sécurité relatif aux utilisateurs du type :

- Toute personne souhaitant utiliser le logiciel de sauvegarde doit être définie comme utilisateur dans l'application.
- Seul le propriétaire de la copie peut visualiser les données qu'il a sauvegardées.

D'autres autorisations peuvent être définies en fonction du contexte et des besoins des utilisateurs ou de l'environnement.

### Le planning de sauvegarde

La périodicité est définie en fonction des besoins et des niveaux de sauvegarde, elle peut être quotidienne, hebdomadaire ou mensuelle.

Ces lignes de conduite se définissent comme étant une combinaison de périodes (jour, semaine, mois, année) ou une fréquence de sauvegarde.

#### **2.1.2 La politique de sauvegarde**

Elle est définie en fonction du volume de données à copier, de la quantité d'information à garder ou éventuellement à perdre, de l'environnement technique, de la durée légale de conservation des données.

Cette politique consiste à définir :

- L'environnement du système d'information à sauvegarder (services, matériels, sites, utilisateurs...) et la façon dont les opérations sont réalisées.
- Le type et la quantité de données à stocker (fichiers utilisateurs ou applicatifs, comptes de messagerie, bases de données...). Le nombre de fichiers ou la taille des sauvegardes peut évoluer dans le temps avec l'ajout de nouvelles applications ou de données.
- La fréquence/périodicité des sauvegardes.
- Les lieux et moyens de stockage des sauvegardes.

### Politique de rétention des données sauvegardées

Deux types existent :

**Politique de recherche** : période de maintien des informations dans les index ou la base de données interne.

**Politique de rétention** : période de conservation des informations dans la bibliothèque ou l'ensemble de stockage des supports.

## 2.1.3 La sauvegarde

Il s'agit de l'opération consistant à créer une copie des données sur un média de stockage (bande magnétique, support optique, disque dur...). Cette réplique d'information est stockée et conservée pour une utilisation ultérieure de restauration dans le cas où l'original serait supprimé (involontairement ou volontairement), détruit ou endommagé.

Le logiciel qui copie les données vers un média s'appelle application de sauvegarde.

Dans la plupart des cas, la source correspond à des données enregistrées sur une unité de disques, par exemple des fichiers, des répertoires, des bases de données et des applications.

La destination est un support de stockage utilisant un matériel d'enregistrement et de lecture tel une unité de bande magnétique, un robot de sauvegarde (bandothèque), une unité de stockage composée de disques ou de supports optiques (DVD-ROM...), ou encore un stockage basé sur le réseau.

## 2.1.4 L'archivage

C'est une opération de copie identique à la sauvegarde, sauf que les données copiées sont stockées et conservées pour une durée plus longue. Cette opération peut s'avérer nécessaire pour des raisons légales et/ou administratives. Elle permet aussi de conserver l'état du système d'exploitation d'un serveur juste après une installation ou une mise à jour importante.

La destination est un support utilisant un périphérique spécifique équivalent à ceux définis pour la sauvegarde, le support WORM (*Write Once/Read Many*) peut être utilisé plus spécifiquement dans ce cas.

## 2.1.5 La restauration

Cette opération réalise la reconstruction des données originales à partir d'une copie de sauvegarde ou d'archivage.

Ce concept regroupe la préparation et la recopie proprement dite des données, certaines actions supplémentaires pour rendre les données exploitables sont parfois nécessaires.