Chapitre 15

Pré-requis

☒Connaître les principes d'une sauvegarde de données.

☒Connaître les principes d'une restauration de données.

☒Connaître les bases d'un plan de reprise d'activité.

Objectifs

☒Savoir implémenter un plan de reprise d'activité en cas de sinistre.

☒Savoir définir une stratégie de sauvegarde.

☒Savoir implémenter la sauvegarde sous Windows Server 2012 R2.

☒Savoir restaurer des données effacées d'un serveur de fichiers.

☒Savoir récupérer des objets supprimés accidentellement d'un annuaire.

A. Présentation de la récupération d'urgence

De nos jours, de plus en plus de sociétés fonctionnent en utilisant au quotidien l'outil informatique (serveurs, postes de travail, terminaux fixes ou mobiles, e-mails, etc.). Les données manipulées sont multiples présentes sous différents supports, accessibles à un ou plusieurs utilisateurs et sont plus ou moins confidentielles. Pour beaucoup d'entreprises, l'essentiel de l'activité est basée sur des données numériques (contrats, factures, commandes, gestion de stocks, produits, services en ligne, sites web, projets, etc.). C'est pourquoi la perte de données informatiques lors d'un sinistre peut s'avérer vitale pour une entreprise (incendie, suppression accidentelle, crash, piratage, vol, etc.). D'après les statistiques, une entreprise qui perd l'essentiel de ses données informatique suite à un crash ou une mauvaise manipulation a un pourcentage de chance plus élevé de cesser toute activité dans les semaines suivant le sinistre, si aucun plan de récupération d'urgence n'a été mis en place au préalable. C'est pourquoi la sauvegarde est un point crucial, commun à presque toutes les entreprises. Mettre en place une infrastructure informatique, signifie également de planifier et mettre en place des solutions pour la restaurer en cas de sinistre.

1. Récupération d'urgence

La récupération d'urgence consiste à restaurer le service qui a été détérioré suite à un sinistre. Pour cela, une entreprise peut, par exemple, mettre en place un Plan de Reprise d'Activité (PRA) qui consiste à définir les tâches et actions à réaliser pour restaurer, en un temps record, le service offert aux utilisateurs. Un PRA comprend notamment un plan de sauvegarde qui consiste à définir une stratégie visant à sauvegarder l'ensemble des données de la société afin de pouvoir les restaurer si besoin. Avant de mettre en place une stratégie de sauvegarde, une entreprise doit d'abord faire une étude préliminaire qui aidera à mieux cibler les besoins et ainsi, orienter la bonne implémentation du plan de sauvegarde. Afin de répondre au mieux aux exigences requises par un système informatique, il convient de respecter et suivre les bonnes pratiques définies dans les normes ITIL (*Information Technology Infrastructure Library*).

Les bonnes pratiques figurant dans les ouvrages ITIL préconisent de répondre aux questions suivantes avant de mettre en place un plan de récupération d'urgence :

- **Définir les éléments à sécuriser et/ou sauvegarder** : sécuriser ou sauvegarder l'ensemble du périmètre informatique occasionne des coûts (logiciels, matériels, espace de stockage disque ou sur bande, redondance des équipements, etc.). C'est pourquoi il convient d'évaluer à l'avance la volumétrie à sauvegarder en faisant la sélection des éléments à conserver.
- **Évaluer les coûts de la sauvegarde** : plus il y a de données à sauvegarder, plus le coût du plan de sauvegarde est élevé (équipement de sauvegarde, espace disque, etc.). Pour maîtriser son budget, il est important de ne pas négliger l'évaluation des coûts liés à la sauvegarde. Tous les éléments de l'infrastructure de sauvegarde doivent être évalués, comme le matériel, les logiciels, la volumétrie, les coûts de rétention, les coûts de stockage ainsi que les coûts humains (administrateur, technicien, etc.).
- **Définir les clauses du contrat de niveau de service** : les ouvrages décrivant les bonnes pratiques informatiques mentionnent le fait qu'il est important de définir à l'avance le niveau de service apporté aux utilisateurs. Ces clauses doivent être recensées dans un document exposant clairement la qualité de service attendue (ce contrat client-fournisseur est également appelé SLA : *Service Level Agreement*), ainsi que les délais d'interruption de service maximum en cas de panne ou sinistre. La durée maximale d'interruption du service pouvant être tolérée avant la reprise de l'activité, est également appelé RTO (*Recovery Time Objective*) d'après les ouvrages ITIL.
- **Définir les pertes de données acceptables en cas de sinistre** : lors d'un sinistre, il est possible de restaurer les données perdues ou corrompues d'un serveur à un instant T, si la politique de sauvegarde mise en place est opérationnelle. Cependant, les données saisies quelques minutes avant le sinistre par les utilisateurs peuvent ne pas avoir été sauvegardées. Ce qui, implicitement, veut dire qu'il n'est plus possible de restaurer ces éléments non sauvegardés. C'est pourquoi il est important de définir la tolérance de perte de données en cas de sinistre dans un document spécifique, également appelé RPO (*Recovery Point Objective*) dans les ouvrages ITIL.
- **Définir la stratégie de rétention des sauvegardes** : lorsque les sauvegardes sont réalisées sur bande, online, ou sur disque, de l'espace de stockage est consommé. La politique de rétention des sauvegardes définit le temps que ces archives sauvegardées doivent être conservées avant écrasement par une nouvelle sauvegarde ou simple destruction. Plus la stratégie de rétention impose un délai de conservation des sauvegardes élevé, et plus il est facile pour un administrateur de restaurer des données supprimées depuis quelques jours. Le cas se présente surtout pour les situations de suppression accidentelle de données. Par exemple, si un utilisateur supprime accidentellement un dossier important et qu'aucun utilisateur ne s'en rend compte pendant deux semaines… Il sera alors impossible pour un administrateur de restaurer les données supprimées si la politique de rétention des sauvegardes impose une rotation par écrasement des archives plus vieille d'une semaine. Afin de pouvoir restaurer dans différentes situations, il est possible de mettre deux plans de sauvegarde simultanément. Par exemple, un plan de sauvegarde hebdomadaire sur disque peut réaliser des archives avec un délai de rétention sur quatre semaines, tandis qu'un autre plan de sauvegarde mensuel sur bande peut réaliser des archives avec un délai de rétention sur un an.

- **Définir une stratégie de restauration des données** : il existe différentes méthodes pour restaurer des données en fonction des méthodes de sauvegarde ou récupération mises en place pour sécuriser l'infrastructure informatique. Lors d'un sinistre, il convient de déterminer à l'avance les méthodes de récupération des données en fonction de telle ou telle situation. Une stratégie de restauration doit être définie en accord avec les clauses définies dans les contrats de qualité de service. Par exemple, si un utilisateur perd un fichier, il sera plus rapide de tenter une restauration des données en jetant un œil dans le cache des clichés instantanés plutôt que de rapatrier une bande du centre de stockage des archives sauvegardées. Plus vite les données sont restaurées et plus grand est le pourcentage pour les administrateurs de respecter les clauses de qualité de service, ainsi que le temps d'interruption maximale admissible pour les utilisateurs. Tout plan de sauvegarde mis en place doit être validé et testé régulièrement afin de s'assurer que la stratégie de restauration est opérationnelle et que les données sauvegardées sont exploitables. Il arrive bien trop souvent qu'une entreprise sauvegarde des données sur bande et que le jour où une restauration s'impose, les administrateurs se retrouvent impuissants face à une bande vierge ou contenant des données inexploitables. Il faut donc systématiquement tester que le processus de restauration fonctionne et que les fichiers restaurés sont accessibles par les utilisateurs. Cela garantit ainsi l'intégrité des données restaurées ainsi que la qualité de service apporté.

2. Présentation de la sauvegarde

Il existe plusieurs technologies de sauvegarde des données, plusieurs supports de destination, plusieurs éditeurs tiers ; que les solutions utilisent des composants matériels ou logicielles.

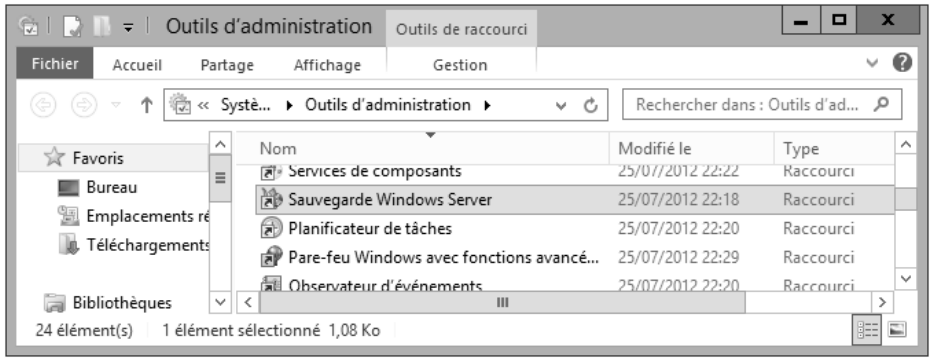
On retrouve notamment des sauvegardes de données sur les supports suivants :

- **Cloud**
- **Disques durs internes/externes**
- **Supports amovibles**
- **CD/DVD ROM**
- **Emplacements réseau**
- **Réplication des données (sur un équipement redondé ou un emplacement géographique différent)**
- **Bandes de sauvegarde**
- **Clichés instantanés**
- **RAID**
- **Snapshots (sauvegarde de l'état du système à un instant précis)**

La plupart des solutions logicielles existantes issues d'éditeurs tiers utilisent des composants qui nécessitent un serveur sur lequel installer la solution de sauvegarde et des agents installés sur chaque serveur pour assurer la communication et le transfert des données à sauvegarder. Ce manuel ne couvre que la solution de sauvegarde intégrée au système d'exploitation Windows Server 2012 R2 (fonctionnalité **Sauvegarde Windows Server**), les clichés instantanés (**Shadow Copy**), ainsi que le système de sauvegarde de type Cloud proposé par Microsoft et nommé **Windows Azure Online Backup**.

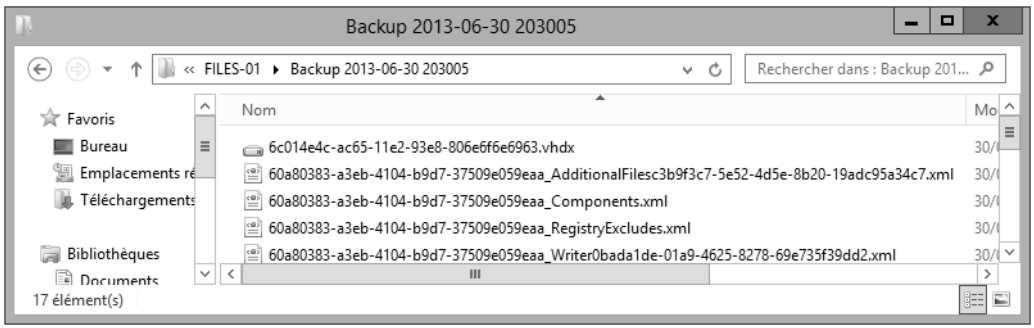
3. Sauvegarde Windows Server

Le système d'exploitation Microsoft Windows Server 2012 R2 intègre nativement la fonctionnalité de serveur nommée **Sauvegarde Windows Server**.
Une fois installé, cet utilitaire se présente sous la forme d'un composant logiciel enfichable accessible depuis le répertoire système **%Windir%\system32\wbadmin.msc**, les outils d'administration du système d'exploitation ou via le Gestionnaire de serveur.

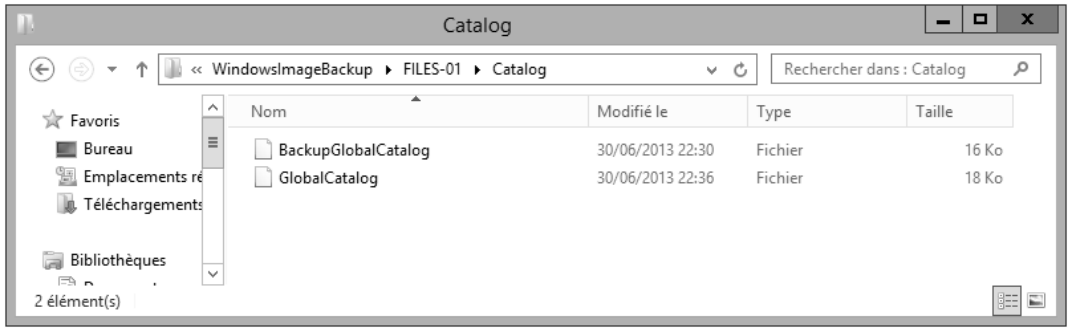


Cet utilitaire permet notamment de gérer les sauvegardes locales (emplacement réseau, volume disque) ou en ligne (**Windows Azure Online Backup**).

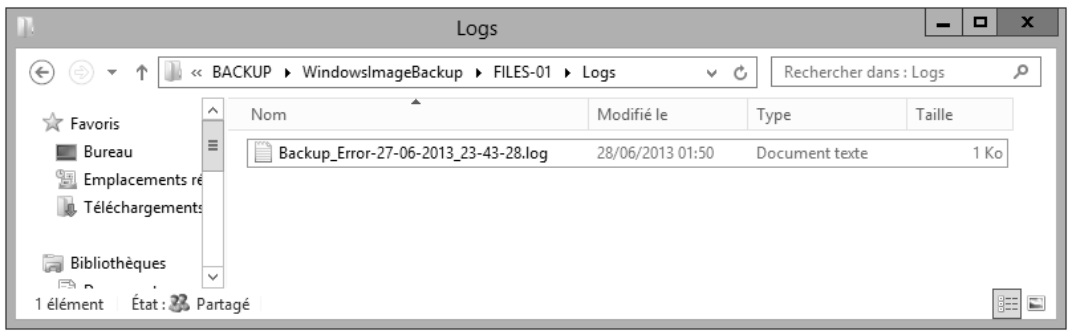
Lorsqu'une sauvegarde est exécutée via cet outil, le composant logiciel enfichable *Sauvegarde Windows Server*, crée un disque virtuel du volume à archiver. Ce disque virtuel est un fichier image au format *.vhdx, qui est le nouveau format de stockage des machines virtuelles sous Microsoft Hyper-V3. Les disques virtuels VHDX peuvent supporter 64 To de données. Le disque virtuel dédié à la sauvegarde des données est créé à l'emplacement suivant :
[Lecteur:\]\WindowsImageBackup\[Nom du serveur]\Backup [Date de la sauvegarde]



Il est possible de naviguer à tout moment dans ces fichiers image de disque dur au travers du composant logiciel enfichable. L'utilitaire crée les fichiers *BackupGlobalCatalog* et *GlobalCatalog* qui enregistrent la configuration des volumes sauvegardés dans l'arborescence suivante :
[Lecteur:\]\WindowsImageBackup\[Nom du serveur]\Catalog



Chaque sauvegarde réalisée doit être vérifiée afin de s'assurer que les données sont accessibles en cas de demande de restauration en urgence. Si un incident survient pendant le processus de sauvegarde, l'utilitaire enregistre des logs d'erreurs à l'emplacement suivant :
[Lecteur:\]\WindowsImageBackup\[Nom du serveur]\Logs



L'utilitaire de sauvegarde permet l'archivage de l'ensemble des données des systèmes d'exploitation Windows Server, ainsi que des machines virtuelles fonctionnant sous Hyper-V.

a. Gestion de la sauvegarde Windows Server

La console de gestion **Sauvegarde Windows Server** permet de gérer les types **Sauvegarde locale** ou **Sauvegarde en ligne**. Le menu **Actions** de la **Sauvegarde locale** permet de gérer les éléments suivants :