Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

SOMMAIRE

[SOMMAIRE 2](#_Toc181727640)

[INTRODUCTION 1](#_Toc181727641)

[C’EST QUOI LA TECHNOLOGIE RAID ? 2](#_Toc181727642)

[QU’EST-CE QUE LE RAID matériel ? 2](#_Toc181727643)

[QU’EST-CE QUE LE RAID logiciel ? 2](#_Toc181727644)

[COMPARAISON DU RAID MATERIEL ET LOGICIEL 3](#_Toc181727645)

[I. INSTALLATION DU RAID 5 SOUS WINDOWS SERVER 2019 3](#_Toc181727646)

[INSTALLATION D’UN VOLUME RAID 5 DE 12 GO 8](#_Toc181727647)

[TEST D’ACCESSIBILITE SUITE A UNE PANNE DE DISQUE 13](#_Toc181727648)

[II. SAUVEGARDE DES DONNÉES UTILISATEURS 17](#_Toc181727649)

[INSTALLATION DU LOGICIEL IPERIUS SUR LE SERVEUR WINDOWS 2019 18](#_Toc181727650)

[III. SAUVEGARDE DES DONNÉES SYSTÈME SOUS WINDOWS 2019 31](#_Toc181727651)

[CREATION D'UNE TACHE POUR RESTAURER LE FICHIER TEST\_RAID5.TXT SAUVEGARDE LA NUIT PRECEDENTE 31](#_Toc181727652)

[RAISONS POUR EFFECTUER LA SAUVEGARDE DES DONNEES SYSTEME APRES 22H00 SOUS WINDOWS 2019 32](#_Toc181727653)

[CONCLUSION 34](#_Toc181727654)

[IV. WEBOGRAPHIE 35](#_Toc181727655)

INTRODUCTION

Dans le cadre de ce TP, l’objectif est de mettre en œuvre diverses solutions pour garantir la disponibilité des fichiers et des dossiers même en cas d’incident, en explorant plusieurs techniques de redondance et de sauvegarde de données. Pour cela, nous nous concentrerons sur deux aspects essentiels : la mise en place d’un système RAID 5 avec trois disques sur le serveur contrôleur de domaine Windows 2019, et la configuration d’un outil de sauvegarde planifiée sur un serveur Windows 2016.

Dans un premier temps, nous déploierons un système RAID 5 avec trois disques en format ReFS (Resilient File System). Ce système RAID 5 permet une tolérance aux pannes en répartissant les données et les informations de parité sur les différents disques. En cas de défaillance d'un disque, les données peuvent être reconstituées à partir des informations de parité des disques restants. Nous configurerons le RAID de manière qu'il se synchronise automatiquement lors de chaque modification du contenu d'un disque, en surveillant également leur état (disponibilité ou non), afin d’assurer une continuité de l’accès aux données.

Ensuite, sur le serveur Windows 2016, nous configureront un outil de sauvegarde, permettant la mise en place de divers types de sauvegarde dont une sauvegarde planifiée. Grâce à l’utilisation d’un fichier d’informations de sauvegarde, cet outil permet de réintégrer les éléments restaurés à leur emplacement d’origine à partir des sauvegardes précédemment effectuées.

## C’EST QUOI LA TECHNOLOGIE RAID ?

RAID, ou Redundant Array of Independent Disks, est une technique permettant de combiner plusieurs disques physiques en une unité logique qui peut améliorer les performances, la fiabilité ou les deux. Il existe différents niveaux de RAID, tels que RAID 0, RAID 1, RAID 5 et RAID 10, chacun avec sa propre configuration et ses propres avantages. Cependant, le RAID peut également être mis en œuvre de différentes manières : en utilisant du matériel ou des logiciels.

### QU’EST-CE QUE LE RAID matériel ?

Le RAID matériel est un type de RAID qui utilise une carte contrôleur ou une puce dédiée pour gérer la baie de disques. Le contrôleur gère toutes les opérations RAID, telles que la répartition des données, la mise en miroir, la parité et la récupération, sans dépendre du processeur ou de la mémoire du système hôte. Le RAID matériel dispose souvent d’une mémoire cache et d’une batterie de secours pour améliorer les performances et la protection des données. Le RAID matériel est généralement plus rapide, plus fiable et plus facile à configurer que le RAID logiciel, car il ne dépend pas du système d’exploitation ou des pilotes. Cependant, le RAID matériel présente également certains inconvénients, tels qu’un coût plus élevé, une compatibilité inférieure et une dépendance vis-à-vis d’un fournisseur.[[1]](#footnote-2)

### QU’EST-CE QUE LE RAID logiciel ?

Le RAID logiciel est un type de RAID qui utilise le logiciel du système hôte, tel que le système d’exploitation ou une application tierce, pour gérer la baie de disques. Le logiciel effectue toutes les opérations RAID, telles que la répartition des données, la mise en miroir, la parité et la récupération, à l’aide du processeur et de la mémoire du système hôte. Le RAID logiciel est généralement moins cher, plus flexible et plus compatible que le RAID matériel, car il ne nécessite aucun matériel spécial ou solution spécifique au fournisseur. Cependant, le RAID logiciel présente également certains inconvénients, tels que des performances inférieures, une consommation de ressources plus élevée et une plus grande complexité.

### COMPARAISON DU RAID MATERIEL ET LOGICIEL

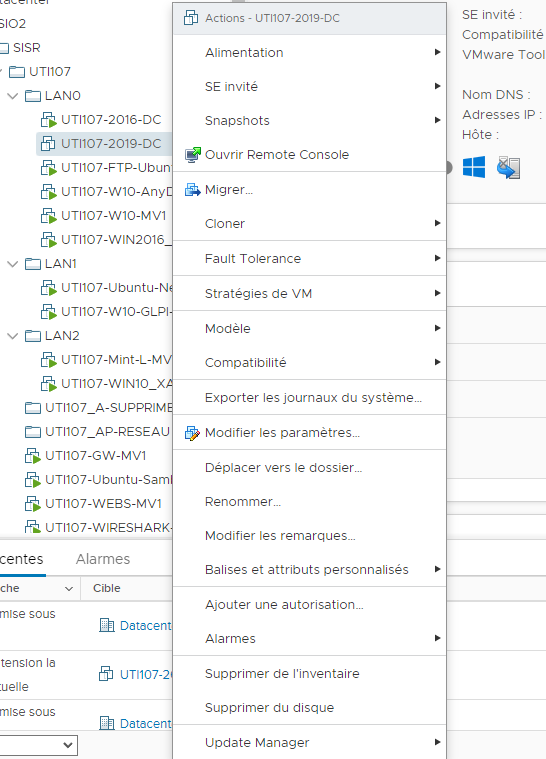
Ci-dessous seront listés dans un tableau, les avantages et les inconvénients à l’utilisation du RAID logiciel par rapport au RAID matériel :

|  |  |  |
| --- | --- | --- |
|  | **AVANTAGES** | **INCONVÉNIENTS** |
| **RAID logiciel** | Moins cher | Performances inférieures |
| Plus flexible | Consommation de ressources plus élevée |
| Plus compatible que le RAID matériel car c’est un logiciel | Plus grande complexité |
| **RAID matériel** | Plus facile à configuré car il ne dépend pas de l’OS ou des pilotes | Coût plus élevé |
| Dispose d’une mémoire cache et d’une batterie de secours | Compatibilité inférieure |
| Plus rapide | Dépendance vis-à-vis d’un fournisseur |
| Plus fiable en termes de sécurité |  |

# INSTALLATION DU RAID 5 SOUS WINDOWS SERVER 2019

**PROCEDURE POUR INSTALLER UN DISQUE DUR VIRTUEL SUPPLEMENTAIRE ET A L’AJOUT DES TROIS DISQUES DURS.**

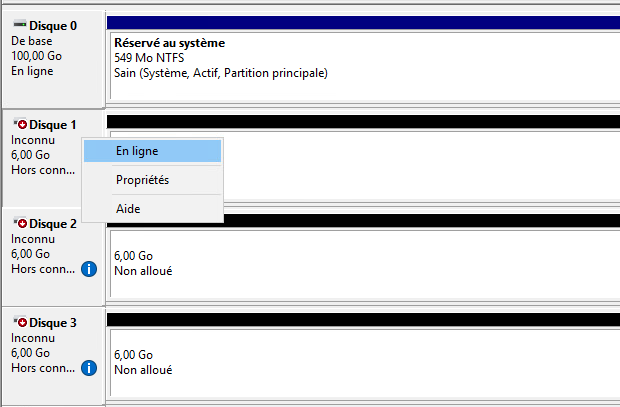
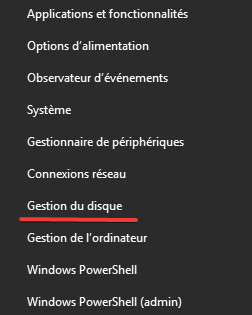
On travaille sur une machine virtuelle Windows Server 2019, il lui faudra quatre disques durs virtuels, un qui est utilisé par le système d’exploitation, et les trois autres qui seront utilisés pour les données. Il faudra définir un espace de 6 Go pour les trois disques durs virtuels de données. Pour installer notre disque virtuel, nous allons sur l’interface vSphere. Il faut s’assurer que notre Windows Server soit éteint, car s’il est allumé, nous ne pouvons pas ajouter de nouveau disque en SCSI depuis notre vSphere.

A screenshot of a computer

Description automatically generated

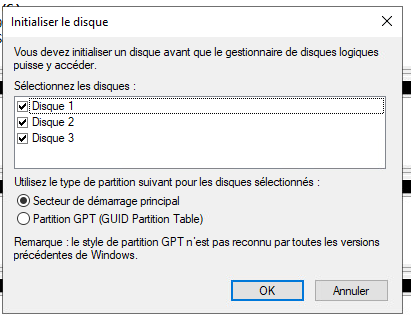
Pour créer le disque dans les paramètres de la machine, rappelons-le que nous devons en créer trois de 6 Go et qu’ils doivent être paramétrés sous un provisionnement du disque dynamique.

En production, on utilise un provisionnement du disque statique car les disques physiques ont une limite d’espace contrairement au disque virtuel qui dépendent de la totalité de l’espace disponible sur la baie. Sur le serveur Windows Server 2019, on ouvre l’outil de Gestion de disque en ouvrant le menu contextuel du bouton Démarrer.



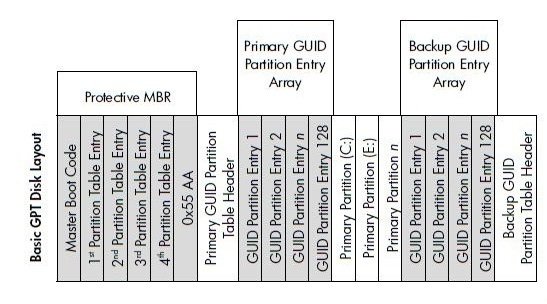
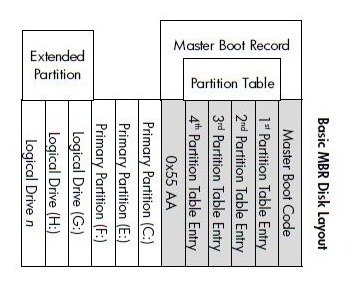
On remarque la présence des trois disques durs ajoutés précédemment. Cependant, ils ne sont pas opérationnels car il faut d’abord les initialiser avant que le gestionnaire de disques logique puisse y accéder. Pour cela, on clique sur « En Ligne » pour les trois disques ajoutés afin de les rendre accessibles par le système. En effet, les disques durs ajoutés sont par défaut en statuts « Hors Ligne », les rendant inaccessibles par le système. On clique ensuite sur « Initialiser le disque » après avoir de nouveau ouvert le menu contextuel sur un des trois disques.

Une image contenant texte, capture d’écran, affichage, Police

Description générée automatiquement

*DIFFÉRENCES ENTRE LE MASTER BOOT RECORD (MBR) ET LE GPT (GUID PARTITION TABLE)*

Le Master Boot Record (MBR) ou Secteur de démarrage principal, est un ancien schéma de partitionnement utilisé sur les disques durs. Situé au début du disque, il contient des informations sur la structure des partitions. Le MBR gère jusqu'à quatre partitions primaires ou trois primaires et une étendue, avec une capacité maximale de 2 To par disque. Ce système est compatible avec les BIOS, mais il devient obsolète face aux capacités de stockage modernes.



La Globally Unique Identifier Partition Table (GPT) est un schéma de partitionnement récent, conçu pour remplacer le MBR. Associé aux systèmes de démarrage UEFI, GPT permet une capacité de stockage allant jusqu'à 9.44 ZB, presque illimitée. Il prend en charge jusqu'à 128 partitions primaires et inclut des mécanismes de redondance et de vérification, offrant ainsi une meilleure protection des données.

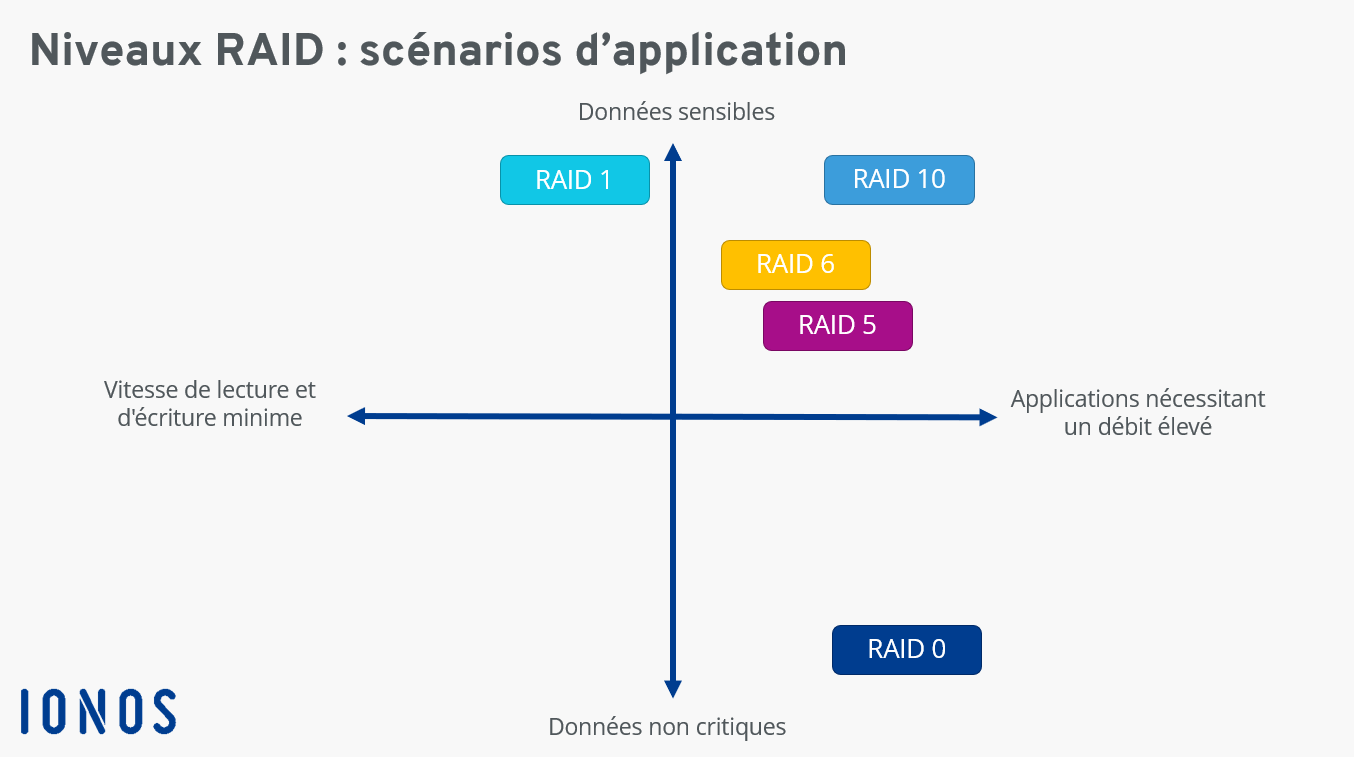
Les principales différences entre MBR et GPT concernent la capacité et la gestion des partitions. MBR limite la capacité à 2 To et ne peut gérer que quelques partitions, tandis que GPT permet une capacité presque illimitée et jusqu'à 128 partitions. En termes de démarrage, MBR est compatible avec les BIOS, alors que GPT nécessite UEFI, offrant des démarrages plus rapides et plus sécurisés. De plus, GPT assure une meilleure intégrité des données grâce à des mécanismes de sauvegarde, rendant GPT plus adapté aux systèmes modernes.

**NOTIONS DE DISQUE DE BASE ET DE DISQUE DYNAMIQUE**

Un **disque de base** est un type de stockage de données qui utilise un système de fichiers simple et est généralement utilisé pour les installations de systèmes d'exploitation. Il fonctionne de manière classique, avec une partition unique ou plusieurs partitions qui sont visibles par le système d'exploitation. Les disques de base ne permettent pas des fonctionnalités avancées comme la mise à l'échelle dynamique ou la gestion de volumes multiples.

Un **disque dynamique** offre des fonctionnalités plus avancées par rapport au disque de base. Il permet de créer plusieurs volumes sur un même disque physique, tels que des volumes simples, des volumes fractionnés, des volumes miroir et des volumes RAID. Les disques dynamiques facilitent également la gestion de l'espace de stockage en permettant d'ajouter ou de supprimer des disques sans avoir à reformater. Ils sont souvent utilisés dans des environnements nécessitant une haute disponibilité et une gestion flexible du stockage.

**Quels sont les types de volume proposés ? A quel type de RAID correspondent-ils ?**



Le Volume simple est un disque physique qui fonctionne comme une unité physique indépendante. Il correspond au **RAID 0**.

Le Volume fractionné combine des zones d’espace non alloué de plusieurs disques en un seul volume logique. Lorsque de nouvelles données sont écrites dans un volume fractionné, elles remplissent d’abord l’espace libre du premier disque, puis celui du disque suivant, et ainsi de suite. Il correspond au **RAID 0**.

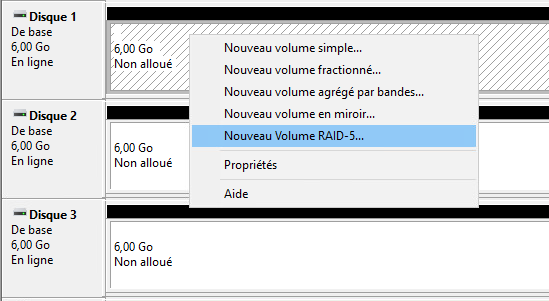
Le Volume agrégé par bandes est créé en combinant des zones d’espace libre sur deux disques ou plus en un seul volume logique. Ce type de volume n’offre pas de résistance aux défaillances, ce qui signifie que le volume entier tombera en panne dès que l’un des disques contenant un volume agrégé par bandes sera défaillant. Il correspond au **RAID 0** si les données sont entrelacées sur chaque disque qui constitue la grappe. Il peut correspondre au **RAID 5** si elle est à parité répartie.

Le Volume en miroir utilise deux copies sur des disques physiques distincts pour dupliquer les données. Lorsque de nouvelles données sont écrites sur le volume en miroir, elles sont écrites sur les deux copies. Si l’un des disques physiques tombe en panne, les données sur le disque deviennent indisponibles, mais le volume en miroir est un volume résistant aux défaillances, ce qui signifie que les données sur l’autre disque physique sont toujours utilisables. Il correspond au **RAID 1** et nécessite au minimum 2 disques pour être utilisable.[[2]](#footnote-3)

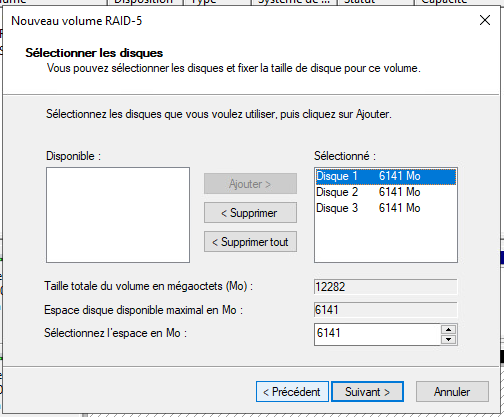
## INSTALLATION D’UN VOLUME RAID 5 DE 12 GO

On choisit de créer un nouveau volume RAID 5 car on veut que les données des disques soient constamment accessibles même par suite d’un incident. Le système de parité du RAID 5 nous offre la possibilité de synchroniser les données par rapport aux changements réalisés entre les disques, permettant ainsi d’avoir les mêmes données sur les trois disques.

Si un des trois disques n’est plus disponible, les données seront quand même accessibles car elles auront été préalablement copiées sur les deux disques restants et lorsque le disque indisponible est de nouveau accessible, les données présentes sur les deux disques restants seront copiées dessus.



On sélectionne les trois disques ajoutés afin de former un volume commun de 12282 Mo.



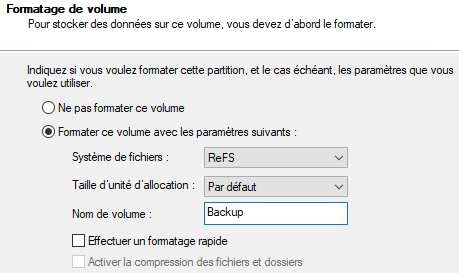
6141 Mo correspond à 6 Go, soit la taille du disque total individuellement. Les trois disques de 6 Go formeront un volume commun de 12282 Mo, soit 12 Go. Ainsi, le volume du RAID 5 que l’on crée aura au total 12,282 Go de taille.

On attribue une lettre disponible au volume RAID 5 que l'on est en train de créer. L’option « Monter dans le dossier NTFS vide suivant » permet de mettre en place le volume sur un répertoire à la place d’un lecteur monté pour, par exemple, économiser les lettres de lecteur et y accéder plus facilement dans le lecteur auquel le répertoire choisi est stocké.

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

On formate le volume en lui donnant un nom logique et en définissant le système de fichiers à utiliser. La taille d’unité d’allocation peut être nécessaire si on souhaite minimiser le gaspillage d’espace dans le cas où on a beaucoup de petits fichiers qui s’accumulent. On n’a pas besoin de définir une taille d’unité d’allocation pour le moment car on y stockera peu de données pour le moment, mais en production, cela peut être intéressant pour faire des économies d’espace sur le volume si par exemple, on ne sait pas quels types de données vont être stockés sur le volume.



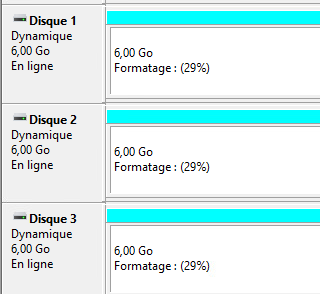
On choisit de formater en ReFS car il est conçu pour la résilience et la protection des données. Il corrige les erreurs qu’ils détectent ainsi que les corruptions. Il est optimisé pour gérer de très grands volumes de données pouvant dépasser la limite du format NTFS et gère aussi mieux les données non structurées grâce à l’intégrité des métadonnées et la gestion des espaces de stockage. Bref, ce format est plus adapté pour notre environnement de serveur de stockage de données.

Le format NTFS est utilisé par défaut par les versions récentes de Windows. Il est également compatible avec les versions antérieures de Windows. Il permet une meilleure sécurité en nous offrant la possibilité de gérer les permissions d’accès aux fichiers, d’accéder à un journal de modification pour, par exemple, récupérer des erreurs en cas de plantage, de chiffrer les données, de compresser les fichiers, de définir des quotas de disque, et les points de montage.

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

En cliquant sur « Suivant », un message d’avertissement apparaît nous informant que les disques 1, 2 et 3 qui sont par défaut des disques de base, seront convertis en disque dynamique pour que le RAID 5 fonctionne. Ce message nous dit qu’il ne sera pas possible d’installer un système d’exploitation sur ces disques, mais on n’aura pas besoin d’en installer car les trois disques seront utilisés pour stocker des données. On peut donc cliquer sur « Oui ».

Une image contenant texte, capture d’écran, affichage, nombre

Description générée automatiquement A screenshot of a computer

Description automatically generated

Les trois disques seront formatés et se resynchroniseront grâce à la parité, mais pour le moment, aucune donnée n'est présente sur le volume.

On teste à présent le fonctionnement du RAID 5 mis en place sur le volume configuré. Pour cela, on se connecte en tant qu’administrateur, on crée un répertoire « Documents » dans le volume E et on configure les droits de partage ainsi que les droits d’accès (NTFS). Pour les droits de partage, on donne le contrôle total au groupe « Tout le monde ». Pour les droits d’accès, on donne également le contrôle total pour les groupes présents par défaut.

Une image contenant texte, logiciel, capture d’écran, Icône d’ordinateur

Description générée automatiquement

En configurant le partage du répertoire « Documents », un nom du partage sera créé, ce nom permet d’accéder à ce répertoire via le nom du serveur contrôleur de domaine suivi du nom du répertoire sans devoir mettre à la place du nom du serveur AD, son adresse IP.

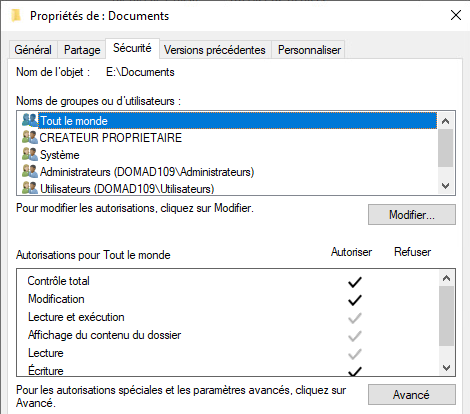


En production, on pense également à supprimer toutes les autorisations héritées afin que ce soient les membres des services qui puissent modifier leurs dossiers de partage.

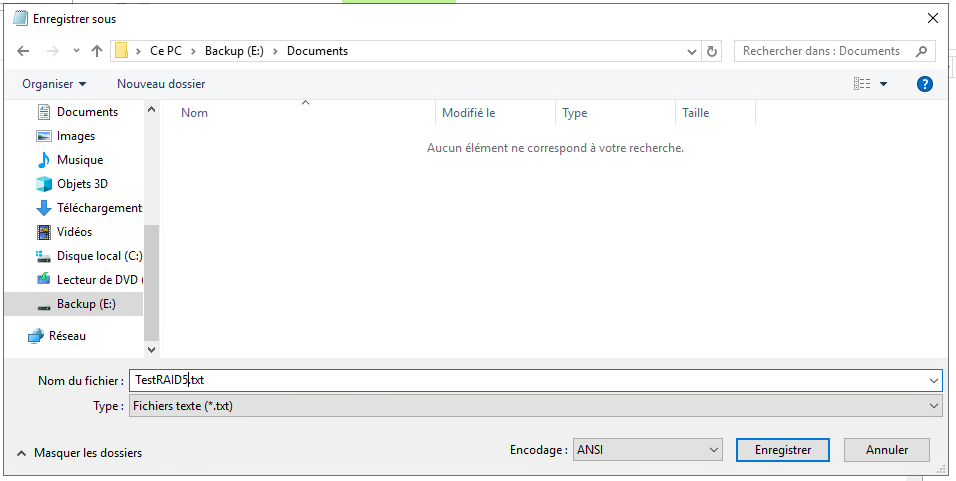
Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

On donne un contrôle total aux groupes pour l’accès au dossier. Si ce sont des dossiers spécifiques à un ou plusieurs services, on limite uniquement à ceux qui doivent y accéder et ceux qui n’ont pas besoin d’y accéder, on ne donne pas un contrôle total.



On crée ensuite un fichier texte « TestRAID5.txt » dans le répertoire « Documents ».



## TEST D’ACCESSIBILITE SUITE A UNE PANNE DE DISQUE

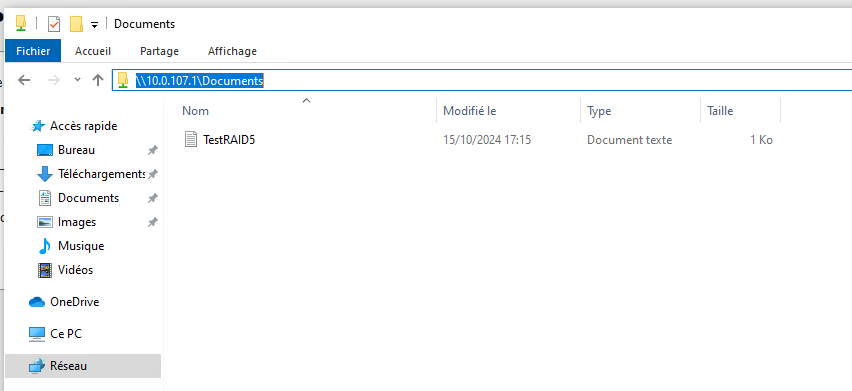
On commence par simuler une panne de disque en mettant hors connexion le premier disque du RAID5.

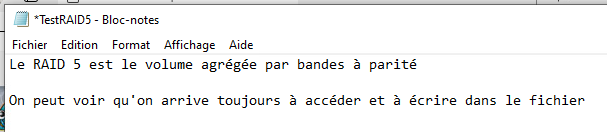
A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

On remarque que le volume ne peut pas faire de la redondance car un des disques est manquant. En effet, le disque 1 est en status « Hors Connexion ». On effectue un test depuis un poste client Windows 10 en se connectant sur un compte utilisateur relié au domaine Active Directory afin de vérifier le bon accès à ce fichier.

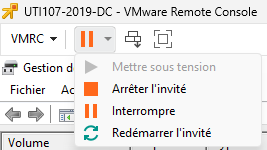




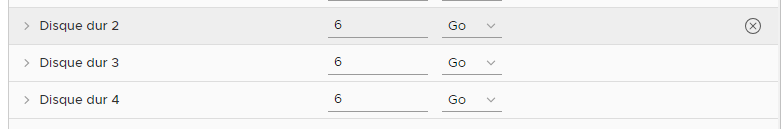
Les utilisateurs reliés à l’Active Directory ont accès au fichier partagé même si un des trois disques tombe en panne. Cela est dû grâce à la fonction de parité qui permet de reconstruire les données manquantes en utilisant les données restantes sur les disques disponibles.

*VÉRIFICATION DU STATUT DE CE DISQUE ET DE L’ACCÈS AU FICHIER*

Il nous est demandé, dans un premier temps, d’arrêter le serveur. On peut le faire de deux façons, la première est d’arrêter directement depuis VSphere ou VMWare en faisant « arrêter l’invité », ou tout simplement dans la machine Windows Server 2019 en faisant arrêter depuis le menu démarrer et en justifiant pour raison « autres ».



On se rend sur notre machine depuis la plateforme VSphere dans les machines de cette dernière pour retirer le disque défaillant.





Nous rallumons le serveur pour voir le résultat de notre déroulé en allant dans la gestion des disques.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementUne image contenant texte, Police, logiciel, nombre

Description générée automatiquement

On remarque que le disque défaillant est maintenant en statut « Manquant ». Cela signifie que le disque enlevé n’est plus détecté, il doit être remis pour être de nouveau fonctionnel dans un sens logiciel. Cependant, si le disque est défaillant physiquement, il faudra le remplacer par un nouveau sur son emplacement et l’ajouter au RAID 5. Si on ajoute un nouveau disque sur un emplacement inutilisé, il sera considéré comme un disque appart, non relié au RAID 5 configuré.

Bien sûr, vu que l’on est sous la plateforme vSphere, il est plus difficile de récupérer le disque défaillant supprimé de la banque de données car le disque virtuel relié aux deux autres disques du RAID 5 mis en place aura son fichier de disque VMDK (Virtual Machine Disk) supprimé définitivement. Cependant, si elle est dans un système de corbeille, il est possible de la récupérer afin de réactiver le disque, de même grâce à des snapshots ou sauvegardes de la machine.

Une image contenant texte, logiciel, nombre, Police

Description générée automatiquement

En effectuant de nouveau le test d’accès au fichier partagé, on remarque que l’utilisateur a toujours accès au fichier texte « TestRAID5 » et peut également écrire du texte dessus et sauvegarder ses modifications.

**9°) Quelle procédure doit-on suivre pour remonter le RAID5 ? Vérifiez que vous avez accès au fichier *TestRAID5.txt.***

À présent, on va arrêter le serveur et on remplace le disque défectueux par un nouveau non différent.

Une image contenant texte, capture d’écran, Police, nombre

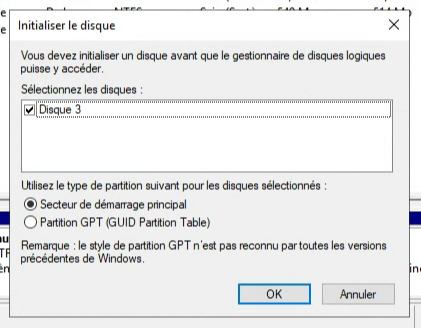
Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquementUne image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

Suite à l’ajout du nouveau disque, on nous demande directement de l’initialiser dans l’outil Gestion des disques.



Une fois initialisé, le disque ajouté sera en statut "Inconnu", il faudra le réactiver afin de pouvoir le relier au RAID 5 configuré. Également, le volume RAID 5 sera en statut « Echec de la redondance » car le troisième disque est indisponible. Cela ne signifie pas que le volume n’est pas fonctionnel.

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

On a bien accès au fichier texte car la parité a permis de reconstruire le fichier texte vers le nouveau disque ajouté dans le RAID 5.

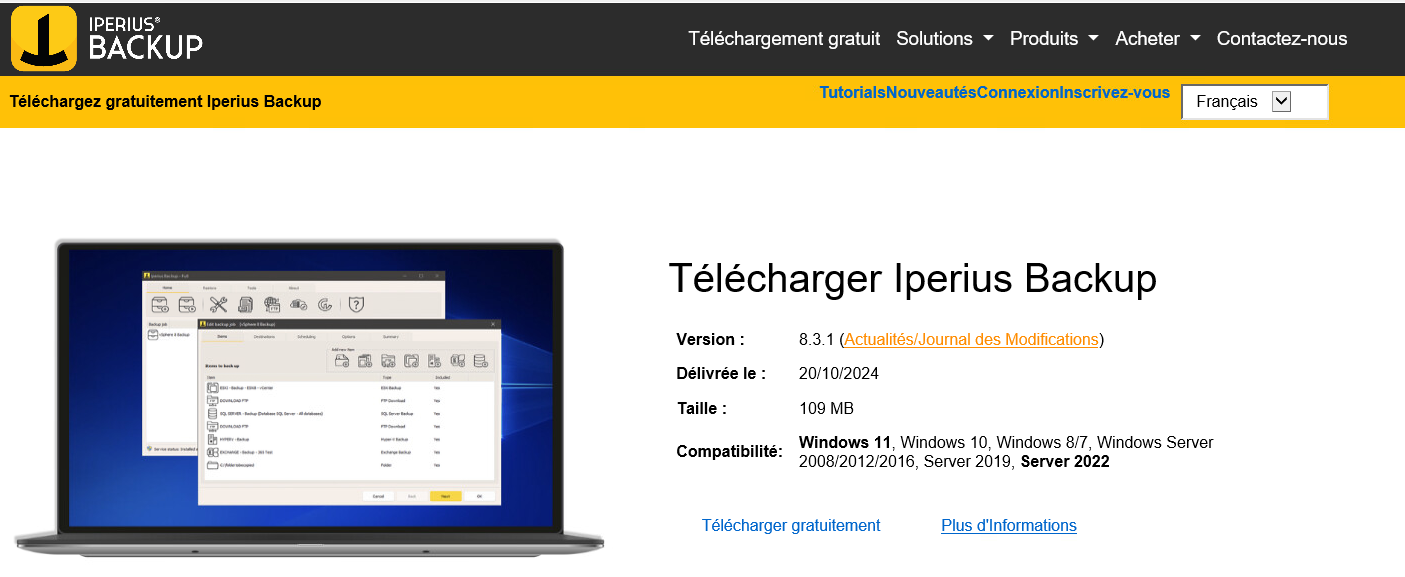
# SAUVEGARDE DES DONNÉES UTILISATEURS

Pour cette partie, on utilisera un second serveur Windows 2016. Sur la plateforme vSphere, elle sera nommée « SRV\_SECU ». On crée un volume F: nommé « sauve » en système de fichiers NTFS car c’est un format plus adapté pour de simples volumes. ReFS est préférable pour un système RAID car il fournit une redondance d’autres avantages tel que le support des volumes de grande taille.

Depuis la version 2008, Windows ne propose plus de solution complète de sauvegarde. En effet, avec la gestion des sauvegardes et restaurations Windows, il n’est pas possible de mettre en place une réelle stratégie de sauvegarde avec sauvegardes incrémentales et différentielles.

On utilisera un logiciel freemium spécialisé dans la sauvegarde et la restauration nommé **Iperius Backup** (à ne pas confondre avec l’outil de prise de contrôle à distance, Iperius Remote).

### INSTALLATION DU LOGICIEL IPERIUS SUR LE SERVEUR WINDOWS 2019



Pour installer le programme, il faut se rendre sur le site web officiel : iperiusbackup.fr.

En cliquant sur « Télécharger gratuitement », un exécutable de l’installeur du programme se télécharge. Le processus d’installation se fait comme d’autres programmes. Il n’y a pas de paramètres spécifiques à sélectionner à part le chemin auquel on souhaite installer le programme. A la fin du processus d’installation du programme, on peut laisser cocher le lancement automatique du programme.

En ouvrant le programme, une icône apparaît dans la zone de notification. En double cliquant dessus, la fenêtre principale du programme s’ouvre.

A screenshot of a computer

Description automatically generated

Il existe une version payante du logiciel Iperius, qui s’intitule Iperius Full.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Uniquement avec la version payante « Iperius Full »

Accessible avec la version gratuite

La version payante « Iperius Full » d'Iperius Backup propose plusieurs fonctionnalités avancées qui ne sont pas disponibles dans la version gratuite, qui ne permet que la sauvegarde basique de dossiers ou de fichiers individuels. Voici un aperçu des fonctionnalités exclusives à la version payante, ainsi que de leur intérêt :

**1. Sauvegarde d'Image Disque**

* Une image contenant texte, capture d’écran, Police, nombre

  Description générée automatiquement**Description** : Cette fonctionnalité permet de créer une image complète du disque, c'est-à-dire une copie exacte de l'intégralité du disque dur ou d'une partition.
* **Intérêt** : En cas de panne système ou de défaillance du disque dur, cette image permet de restaurer l'ordinateur exactement tel qu'il était au moment de la sauvegarde, avec le système d'exploitation, les applications, et les données intactes. Cela facilite grandement la reprise après sinistre en minimisant le temps d'arrêt.
* **Différence avec la version gratuite** : La version gratuite ne permet que des sauvegardes de fichiers, ce qui signifie qu’il faut réinstaller le système et les applications manuellement après une panne majeure.

**2. Téléchargement FTP**

* **Description** : Cette option permet de sauvegarder des données vers un serveur FTP, ou de les télécharger depuis celui-ci.
* **Intérêt** : Idéal pour stocker des données hors site, le transfert FTP permet de sauvegarder des fichiers vers des serveurs distants, améliorant la sécurité en cas de sinistre local (incendie, inondation, etc.).
* **Différence avec la version gratuite** : La version gratuite ne propose pas cette flexibilité, limitant les sauvegardes aux disques locaux ou à un réseau interne.

**3. Sauvegarde / Réplication VMware ESXi**

* **Description** : Cette fonctionnalité est dédiée aux environnements de virtualisation VMware, permettant de sauvegarder ou de répliquer des machines virtuelles sur un serveur VMware ESXi.
* **Intérêt** : Indispensable pour les entreprises qui utilisent la virtualisation pour optimiser leurs ressources, cette option permet de restaurer rapidement des machines virtuelles en cas de problème, minimisant ainsi l’impact sur la production.
* **Différence avec la version gratuite** : La version gratuite ne gère pas la virtualisation, ce qui limite l’intérêt pour les entreprises disposant de serveurs VMware.

**4. Sauvegarde Hyper-V**

* **Description** : Similaire à la sauvegarde VMware, mais pour l'environnement Microsoft Hyper-V, cette option permet de sauvegarder et de restaurer des machines virtuelles sous Hyper-V.
* **Intérêt** : Elle est cruciale pour les infrastructures utilisant Hyper-V comme hyperviseur, permettant une sauvegarde et une restauration faciles de machines virtuelles sans interrompre les autres services.
* **Différence avec la version gratuite** : La version gratuite ne supporte pas non plus Hyper-V, rendant les solutions de virtualisation difficilement gérables avec une version gratuite.

**5. Sauvegarde de Base de Données**

* **Description** : Cette fonctionnalité permet la sauvegarde de bases de données comme SQL Server, MySQL, PostgreSQL, Oracle, etc.
* **Intérêt** : Pour les entreprises qui utilisent des bases de données pour stocker des informations critiques (clients, transactions, etc.), cette option permet de protéger ces données et de les restaurer rapidement en cas de besoin.
* **Différence avec la version gratuite** : La version gratuite ne prend pas en charge la sauvegarde de bases de données, ce qui peut exposer les entreprises à des pertes de données critiques en cas d’incident.

**6. Microsoft 365**

* **Description** : Permet de sauvegarder les données de Microsoft 365, notamment les emails, calendriers, contacts, et fichiers de OneDrive.
* **Intérêt** : Avec la montée en puissance des solutions de travail en ligne et du télétravail, la sauvegarde des données Microsoft 365 est essentielle pour éviter les pertes de données accidentelles ou les attaques. Cette fonctionnalité permet de restaurer les données Microsoft 365 si elles sont effacées ou corrompues.
* **Différence avec la version gratuite** : La version gratuite ne permet aucune sauvegarde de services en ligne comme Microsoft 365, ce qui laisse les utilisateurs sans protection dans le cloud.

**Différences Notables entre la Version Gratuite et la Version Payante ("Iperius Full")**

* **Étendue des options de sauvegarde** : La version payante permet des sauvegardes avancées (sauvegarde disque, bases de données, machines virtuelles, cloud), là où la version gratuite ne permet que des sauvegardes de fichiers et dossiers.
* **Flexibilité et sécurité** : La version payante permet de stocker des sauvegardes sur différents supports (FTP, disque image, cloud) et d’automatiser la sauvegarde de services en ligne, ce qui n’est pas possible avec la version gratuite.
* **Cible professionnelle** : Les fonctionnalités avancées de la version payante visent les entreprises et les professionnels qui ont besoin de solutions de sauvegarde robustes pour garantir la continuité des opérations en cas de problème majeur. La version gratuite est limitée à une utilisation personnelle ou basique.

Maintenant comparons les fonctionnalités et leur disponibilité entres les versions gratuite et payante « Full » :

|  |  |  |
| --- | --- | --- |
| Fonctionnalités | Gratuit (Free) | Iperius Full |
| Sauvegarde d'image disque / Récupération après sinistre | Non | Oui |
| Clonage de disque dur - P2V / Restauration Hyper-V | Non | Oui |
| Disque de récupération avec Iperius Recovery Environment® | Non | Oui |
| Sauvegarde dans le cloud (Google, Amazon, etc.) | Non | Oui |
| Sauvegardes FTP/FTPS | Non | Oui |
| Interface avec Iperius Console | Non | Oui |
| Interface avec Iperius Online Storage | Non | Oui |
| Sauvegarde sur bande (DAT, LTO, USB, etc.) | Non | Oui |
| Sauvegarde des bases de données (SQL, MySQL, Oracle…) | Non | Oui |
| Sauvegarde et réplication VMware ESXi / vCenter | Non | Oui |
| Sauvegarde et restauration Hyper-V | Non | Oui |
| Sauvegarde Microsoft 365 (OneDrive, SharePoint, etc.) | Non | Oui |
| Chiffrement AES 256-bit | Oui | Oui |
| Compression ZIP 64 et sauvegarde incrémentielle | Oui | Oui |
| Notifications par email | Oui | Oui |
| Protection des sauvegardes contre les ransomware | Non | Oui |
| Mise à jour automatique | Non | Oui |
| Synchronisation (avec suppression des fichiers effacés) | Non | Oui |
| Exécution en tant que service | Non | Oui |
| Sauvegarde de fichiers ouverts (VSS) | Non | Oui |

La version « Iperius Full » est conçue pour des environnements professionnels, tandis que la version gratuite est limitée à des sauvegardes simples, offrant une couverture limitée en cas de sinistre.

#### CREATION D’UNE SAUVEGARDE COMPLETE IMMEDIATE

On clique sur « Créer une nouvelle sauvegarde » puis dans la section « Ajouter un nouvel élément », on clique sur « Dossier ou fichier » afin de sélectionner le répertoire de partage « Documents » contenu dans le disque Backup (E:) configuré précédemment dans le serveur contrôleur de domaine Windows 2019.

A screenshot of a computer

Description automatically generated

On se connecte sur un compte administrateur du service Active Directory du contrôleur de domaine Windows Server 2019 afin de pouvoir accéder au répertoire lors de la sauvegarde. Si on souhaite filtrer l’ajout d’élément, on peut spécifier les types d’extensions à uniquement inclure ou exclure. On peut également filtrer en fonction de la taille maximale, minimale ou égale. On peut aussi définir des exclusions de fichiers ou de dossiers spécifiques afin de ne pas les prendre en compte si on ne veut pas que certains dossiers ou fichiers à l’intérieur du répertoire défini soient pris en compte dans la tâche.

On laisse cocher la case « Recréer le chemin complet de l’élément » car cela permet de directement retrouver le chemin défini. Dans l’onglet « Destinations », on définit un répertoire auquel la sauvegarde sera réalisée. Dans notre cas, il faudra définir le disque « sauve (F:) ».

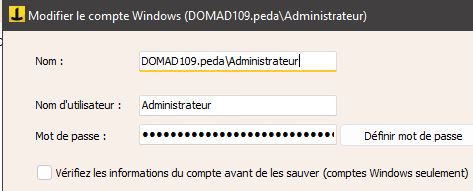
A screenshot of a computer

Description automatically generated

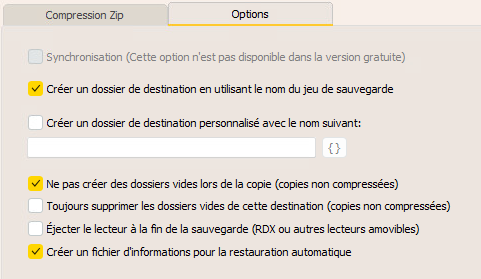
On sélectionne un compte administrateur et on définit le type de sauvegarde à réaliser. On choisit « Créer une sauvegarde complète à chaque fois et copier tous les fichiers » car on aura besoin d’une copie complète à sauvegarder du répertoire partagé « Backup » vers le disque sauve F:. Tous les fichiers de la source seront copiés vers la destination et les fichiers existants seront écrasés.

A screenshot of a computer

Description automatically generated



On peut compresser la sauvegarde dans un format Zip. Cela permet de partager la sauvegarde plus facilement, mais cela dépend de la taille de l’archive Zip. On n’active pas l’option car on veut simplement créer une sauvegarde immédiate du répertoire partagé Backup. On remarque également qu’il est possible de définir un mot de passe sur archive Zip si on active la compression. Cela permet de protéger l’accès au contenu.

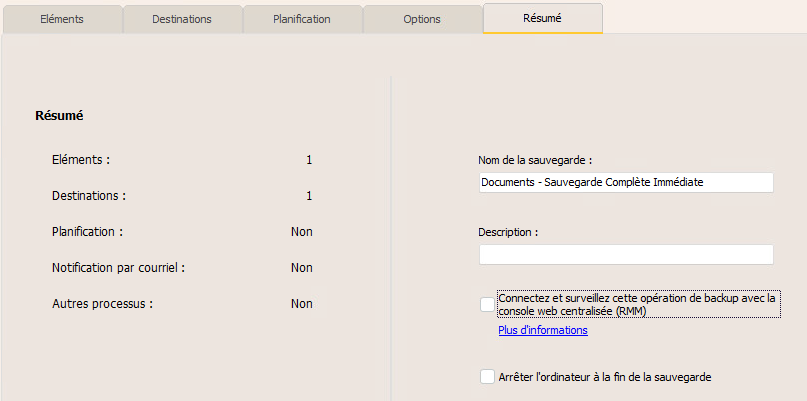


Dans l’onglet « Options », on remarque une option uniquement disponible via la version payante de Iperius Backup. Cette dernière permet de réaliser une synchronisation de la sauvegarde locale vers un support de stockage distant en y créant une copie qui est mise à jour selon les changements de la sauvegarde locale.

L’option « Créer un dossier de destination en utilisant le nom du jeu de sauvegarde » permet, comme son nom l’indique, de créer la sauvegarde dans un dossier qui aura comme nom le jeu (tâche) de sauvegarde que l’on est en train de configurer actuellement.

L’option « Ne pas créer des dossiers vides lors de la copie » doit être cochée afin de ne pas copier les dossiers vides de la source vers la destination. Bien sûr, si on avait activé la compression Zip, la suppression ne pourrait pas se faire dans l’archive Zip.

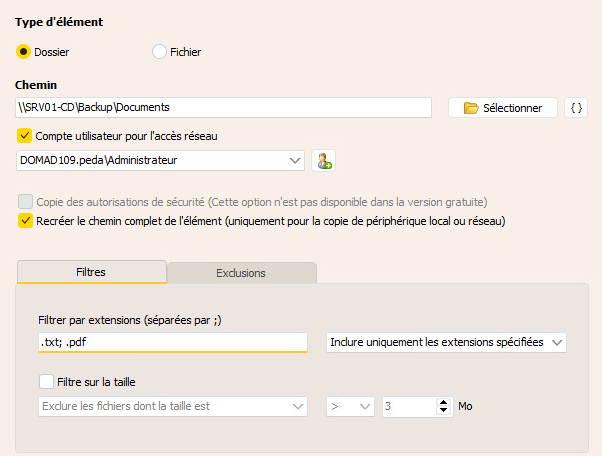
On coche la case « Créer un fichier d’informations pour la restauration automatique » car cela permet de restaurer des fichiers et dossiers supprimés via les informations contenues dans ce fichier. Dans l’onglet Résumé dans la fenêtre principale de configuration du nouveau jeu de sauvegarde, ont défini un nom pour la sauvegarde. Par défaut, le nom du dossier ou fichier sélectionné sera renseigné.



On décoche la case « Connectez et surveillez cette opération de backup avec la console web centralisée » car elle est principalement utilisée dans le cas où on souhaite utiliser un tableau de bord qui permet de visualiser toutes les opérations de sauvegarde configurées sur Iperius Backup.

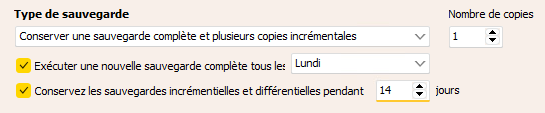
#### CREATION D’UNE SAUVEGARDE INCREMENTALE QUOTIDIENNE

Les éléments sources pour la sauvegarde incrémentale quotidienne seront toujours le répertoire Documents et ses fichiers Test\_RAID5.txt ainsi qu’une notice d’imprimante HP au format PDF. On sélectionne bien sûr un compte administrateur relié au service Active Directory du contrôleur de domaine afin de pouvoir copier le répertoire partagé vers le disque sauve (F:). On paramètre les filtres pour inclure uniquement les fichiers .txt et .pdf afin que Test\_RAID5.txt ainsi que la notice d’imprimantes puissent être incluses dans les sauvegardes et pas seulement le répertoire Documents.



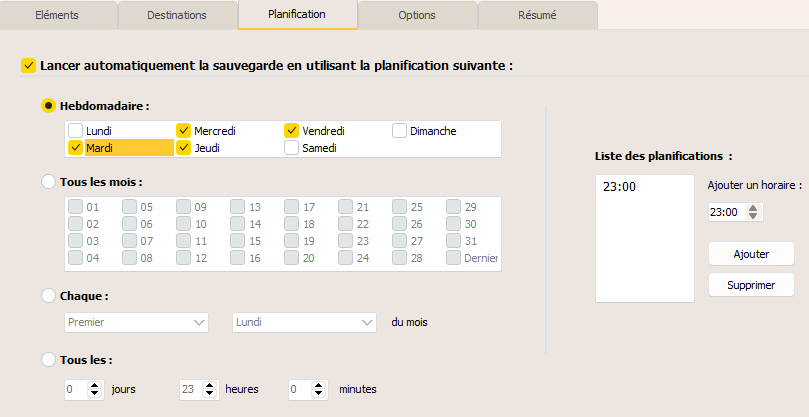
Pour la création d’une sauvegarde incrémentale quotidienne du mardi au vendredi à 23h00, on peut la fusionner avec la sauvegarde complète du lundi à 23h00. On met donc comme type de sauvegarde « Conserver une sauvegarde complète et plusieurs copies incrémentales ». Il n'y aura qu’une copie et la nouvelle sauvegarde complète sera exécutée tous les lundis. On peut laisser les paramètres de l’onglet « Options » par défaut et on n’active pas la compression Zip.

On coche la case « Conservez les sauvegardes incrémentielles et différentielles pendant » et on définit sous 14 jours car cela correspond à deux semaines.



Dans l’onglet « Planification », on peut configurer le moment auquel les sauvegardes seront réalisées. On veut créer une sauvegarde incrémentale de mardi à vendredi à la même heure, 23:00. On choisit donc le format de planification hebdomadaire et on ajoute l’horaire qui sera appliqué sur chaque jour coché.

On remarque qu’il est aussi possible de planifier en fonction des mois, les premiers ou derniers jours du moi actuel ou tous les xx jours, heures et minutes.



Une image contenant texte, capture d’écran, Police

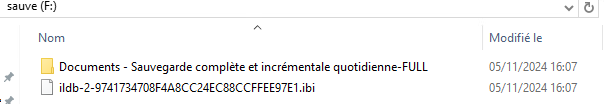
Description générée automatiquement Une image contenant texte, capture d’écran, Police, ligne

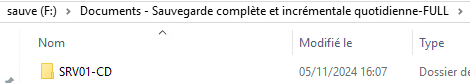
Description générée automatiquement

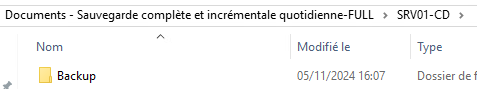
On lance la tâche de sauvegarde complète et incrémentale quotidienne. Une première sauvegarde est réalisée. Dans le disque sauve (F:), on supprime le fichier texte « Test\_RAID5.txt ».

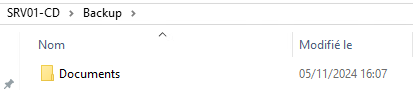
##### TEST DE LA SAUVEGARDE INCREMENTALE

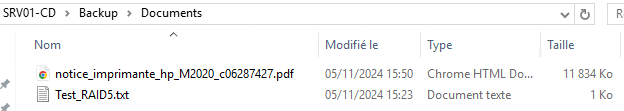
Première sauvegarde complète.





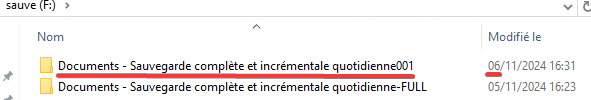


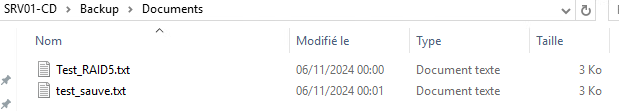




La totalité du répertoire partagé Documents a été copiée sur le disque sauve (F:) du serveur Windows 2016.

Première sauvegarde incrémentielle du mercredi.





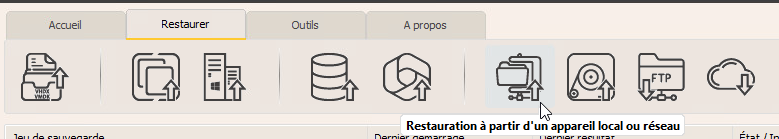
Un utilisateur a ajouté un nouveau fichier test\_sauve.txt dans le répertoire partagé Documents. Le fichier Test\_RAID5.txt a été modifié (3ko à la place de 1ko) mais la notice d’imprimante n’est pas présente car il n’a pas été modifié.

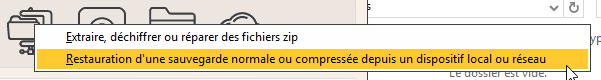
Il faut également savoir que si aucune modification n’a été faite dans la sauvegarde précédente, le jour suivant, la sauvegarde ne sera pas faite.

On supprime le fichier Test\_RAID5.txt du dossier Backup (E:) afin de créer une tâche de restauration pour pouvoir récupérer le fichier depuis la sauvegarde précédente.

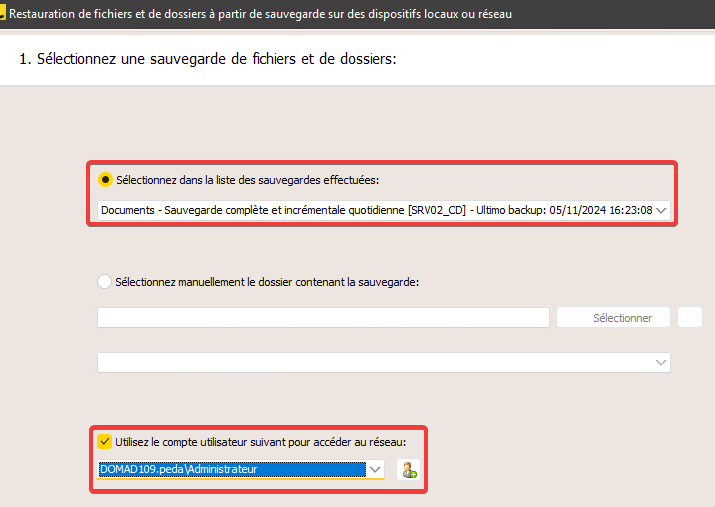
#### CREATION D’UNE TACHE DE RESTAURATION DU FICHIER TEST\_RAID5.TXT

Sur la fenêtre principale du programme Iperius Backup, il y a l’onglet « Restaurer ». Dans cet onglet, diverses méthodes de restaurations nous sont proposées. Celle qui nous intéresse est la « Restauration à partir d’un appareil local ou réseau » car on souhaite restaurer le fichier Test\_RAID5.txt supprimé précédemment. On choisit l’option « Restauration d’une sauvegarde normale ou compressée depuis un dispositif local ou réseau.





On retrouve nos sauvegardes dans une liste déroulante. On la sélectionne et on utilise un compte administrateur pour pouvoir y accéder.

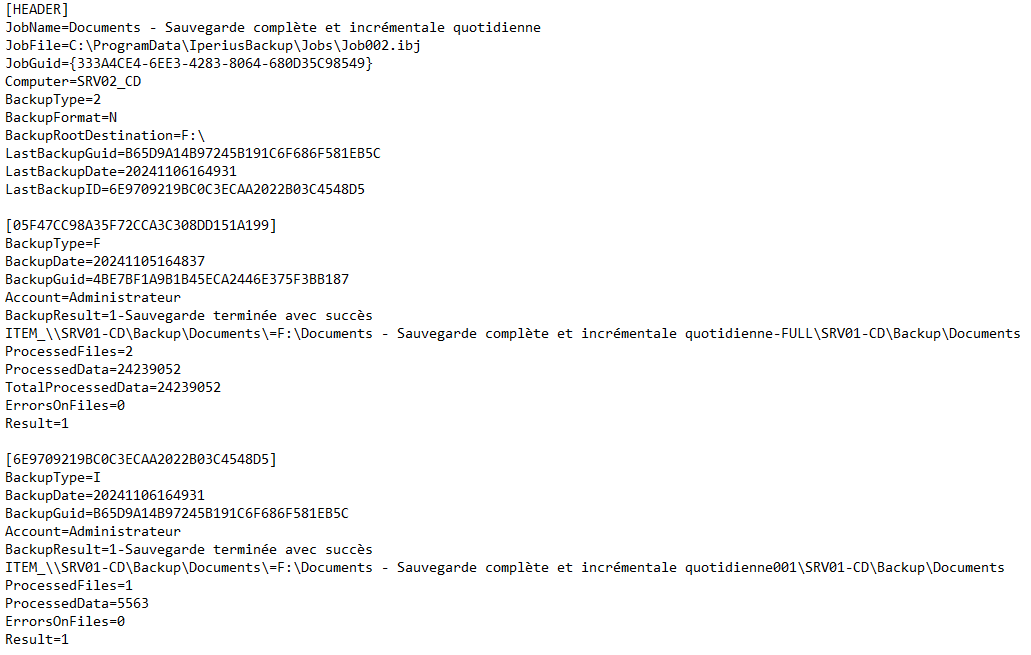


Le fichier en .ibi, qui est généré et mis à jour à chaque sauvegarde effectuée si on coche la case « Créer un fichier d’informations pour la restauration automatique » nous permet de récupérer les fichiers et dossiers supprimés dans une sauvegarde depuis une précédente.

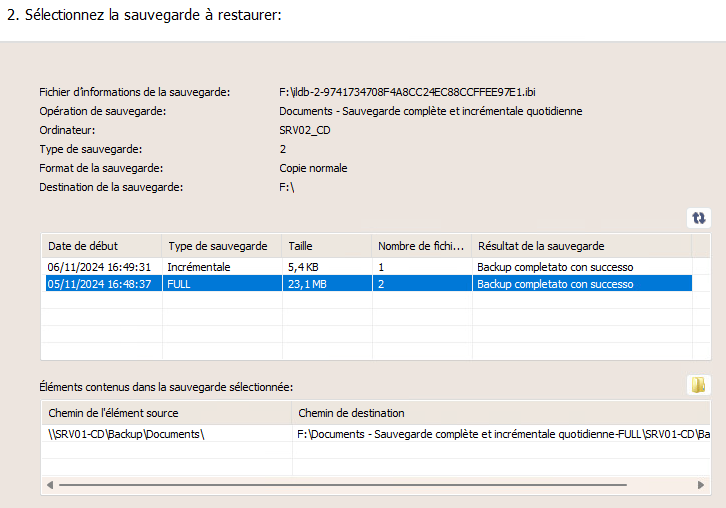
Ce fichier contient des informations de variables telles que le nom du jeu de sauvegarde, son fichier enregistré dans un dossier spécifique du répertoire du programme, son Globally Unique Identifier qui permet de l’identifier des autres jeux de sauvegardes créés par l’utilisateur, le nom de l’ordinateur, le type de sauvegarde, le format, sa destination et bien d’autres.

BackupType=F : signifie qu’il s’agit d’une sauvegarde complète, dans notre cas, il s’agit de la première sauvegarde réalisée pour le jeu de sauvegarde complète et incrémentale quotidienne. Il s’agit du répertoire « Documents – Sauvegarde complète et incrémentale quotidienne-FULL ».

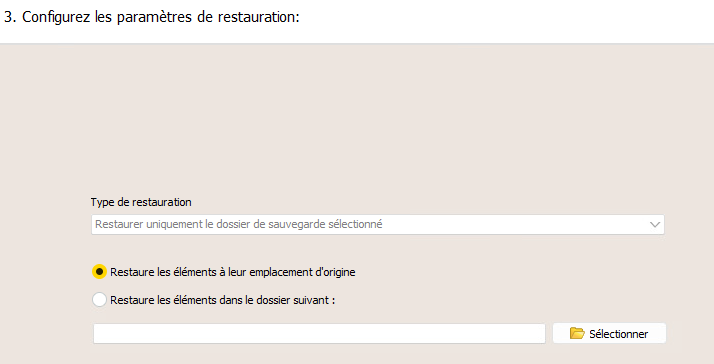
BackupType=I : signifie qu’il s’agit d’une sauvegarde incrémentielle. Il s’agit du répertoire « Documents – Sauvegarde complète et incrémentale quotidienne001 ».



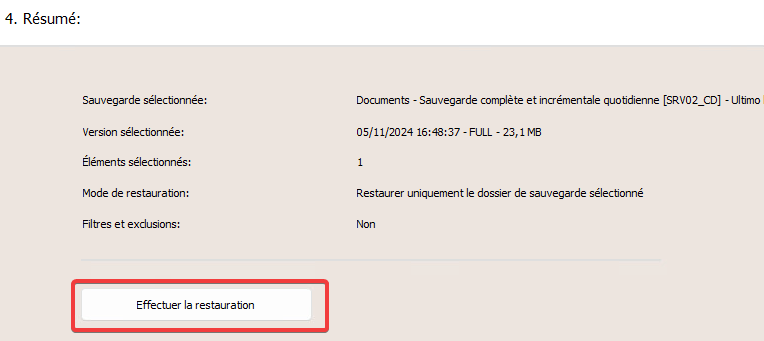
On sélectionne la sauvegarde complète.



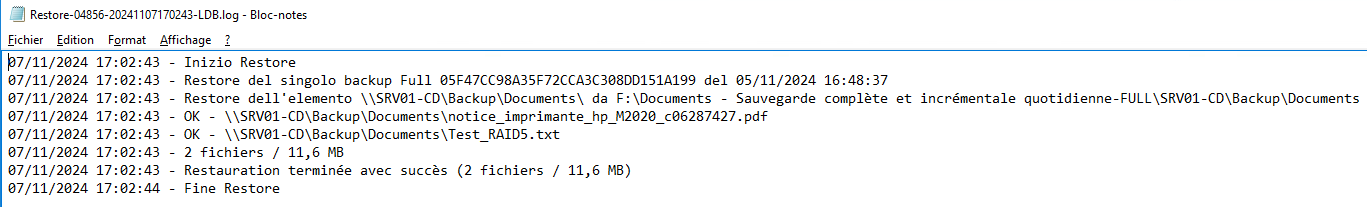
Ont choisi de restaurer les éléments à leur emplacement d’origine.



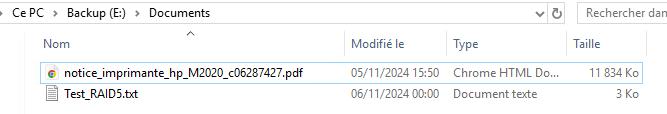
On clique sur « Effectuer la restauration » afin de lancer le processus de restauration des fichiers et dossiers.



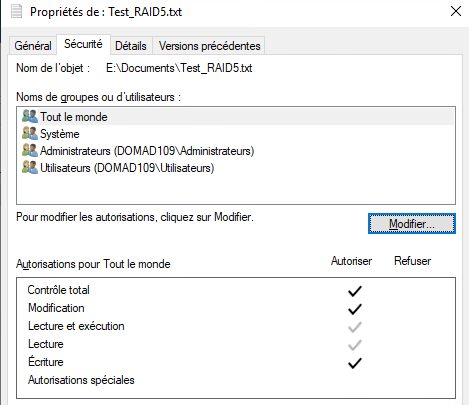
Un enregistrement d’événement concernant le résultat du processus s’ouvre.



En vérifiant le répertoire original Backup (E:) du serveur Windows 2019, on remarque que le fichier Test\_RAID5.txt a bien été restauré.



En vérifiant les permissions NTFS, celles qui sont dans l’onglet « Sécurité », on remarque bien que le groupe « Tout le monde » à le contrôle total sur le fichier.



# SAUVEGARDE DES DONNÉES SYSTÈME SOUS WINDOWS 2019

CREATION D'UNE TACHE POUR RESTAURER LE FICHIER TEST\_RAID5.TXT SAUVEGARDE LA NUIT PRECEDENTE

Pour garantir l'intégrité des sauvegardes, il est essentiel de procéder régulièrement à des tests de restauration des données. Ces tests permettent de s'assurer que les sauvegardes réalisées sont fonctionnelles et peuvent être utilisées en cas de besoin, notamment après une perte ou une corruption de données. Dans ce cas précis, l'objectif était de restaurer le fichier **Test\_RAID5.txt**, supprimé du dossier **Documents**, à partir de la sauvegarde effectuée la nuit précédente. Cette procédure a été réalisée à l'aide du logiciel **Iperius Backup**, qui offre des fonctionnalités de restauration efficaces et simples à mettre en œuvre.

Tout d'abord, pour restaurer le fichier, j'ai lancé l'application **Iperius Backup** et sélectionné l'option **Restaurer depuis une sauvegarde existante** dans l'onglet **Restaurer**. J'ai ensuite choisi le répertoire de sauvegarde **F:**, où les fichiers ont été sauvegardés la veille, et sélectionné la sauvegarde correspondante. Une fois la sauvegarde choisie, Iperius m’a permis de parcourir la structure des fichiers sauvegardés. J’ai alors trouvé le fichier **Test\_RAID5.txt** dans le répertoire approprié et l'ai sélectionné pour la restauration. Ensuite, j'ai opté pour l’option de restauration **à son emplacement d’origine**, c'est-à-dire dans le dossier **Documents** du volume **E:**.

La restauration a été effectuée sans encombre. Après avoir validé le processus, j'ai vérifié dans le dossier **Documents** que le fichier avait bien été restauré. Pour m'assurer que toutes les configurations du fichier avaient été correctement récupérées, j'ai vérifié le contenu du fichier, ce qui a montré qu'il était identique à la version précédemment sauvegardée. Ensuite, pour vérifier l'intégrité des **permissions NTFS** du fichier, j'ai fait un clic droit sur celui-ci, sélectionné **Propriétés**, et consulté l'onglet **Sécurité** pour vérifier que les permissions étaient identiques à celles de la version d'origine.

Le test de restauration réalisé confirme non seulement la fonctionnalité de la sauvegarde mais aussi que la procédure est fiable et peut être réutilisée en cas de besoin pour restaurer des fichiers supprimés ou corrompus.

## RAISONS POUR EFFECTUER LA SAUVEGARDE DES DONNEES SYSTEME APRES 22H00 SOUS WINDOWS 2019

Il est essentiel de sauvegarder les données système régulièrement afin de garantir la récupération du serveur en cas de défaillance. Pour Windows Server 2019, de nombreux experts recommandent de planifier ces sauvegardes **après 22h00**, et voici les raisons majeures qui justifient cette pratique.

* **Minimisation de l'impact sur les performances du serveur**  
  Une sauvegarde, notamment des données système, peut-être une opération gourmande en ressources. Lors de l’exécution de sauvegardes pendant la journée, alors que les utilisateurs sont actifs et que de nombreuses applications sont en cours d’exécution, l'impact sur les performances du serveur peut être considérable. Le système doit gérer simultanément les opérations de sauvegarde et les requêtes des utilisateurs, ce qui peut entraîner un ralentissement général des services, affectant ainsi la productivité des utilisateurs. Cela est particulièrement important dans les environnements d'entreprise où les serveurs hébergent des bases de données et des applications critiques. Pour atténuer cet impact, il est recommandé de planifier les sauvegardes en dehors des heures de pointe, de préférence **après 22h00**, lorsque l'activité des utilisateurs est minimalisée. Cette approche est bien documentée dans des guides sur l’optimisation des performances de sauvegarde.
* **Assurance de la cohérence des données sauvegardées**  
  Une autre raison importante de programmer les sauvegardes après 22h00 est l'assurance que les données système sont cohérentes. En effet, pendant la journée, les applications et services peuvent être en train d'écrire ou de modifier des données, notamment des bases de données actives, des fichiers de journalisation ou des fichiers de configuration système. Si une sauvegarde est effectuée pendant que ces fichiers sont en cours d'utilisation, il existe un risque de **corruption de données** ou d’incohérence dans les fichiers sauvegardés. La planification des sauvegardes après 22h00, lorsqu’il y a moins d’interactions avec le serveur, garantit que les processus sont terminés et que les fichiers système sont dans un état stable et cohérent. Cette stratégie est largement recommandée dans la gestion des sauvegardes de serveurs pour éviter les conflits d’écriture et garantir la fiabilité des données sauvegardées.

Ainsi, la planification des sauvegardes **après 22h00** est une pratique courante et recommandée pour éviter l’impact des sauvegardes sur les performances du serveur et garantir la cohérence et l’intégrité des données. Cela permet d’assurer que la récupération des données système se fasse sans risque de corruption et dans les meilleures conditions possibles.

CONCLUSION

En conclusion, ce TP a permis de mettre en pratique plusieurs compétences essentielles pour garantir la disponibilité des données et leur protection dans un environnement professionnel, tout en abordant certains défis techniques.

Tout d'abord, nous avons dû faire des choix quant au système de fichiers à utiliser entre ReFS et NTFS. Le protocole ReFS, bien que performant et plus résistant à la corruption que NTFS, reste moins compatible avec certaines applications et fonctions de Windows, ce qui a complexifié notre décision. De plus, lorsque nous avons simulé la défaillance d’un disque, nous avons constaté que le simple retrait du disque de l’inventaire dans VSphere ne suffisait pas. Il a fallu désactiver le disque manuellement dans la gestion des disques de Windows Server 2019, ce qui a ajouté une étape supplémentaire imprévue.

Le logiciel de sauvegarde Iperius Backup, bien que très performant, nous a également posé des difficultés. Lors de la modification des jeux de sauvegardes, l’actualisation de l’outil s’est avérée lente, et l’application ne répondait parfois plus lors de certains réglages, ralentissant ainsi notre travail.

Cependant, ce TP a également été riche en découvertes. Le système de fichiers ReFS, que nous avons approfondi, s’est révélé intéressant pour sa capacité à détecter et corriger automatiquement certaines corruptions, offrant ainsi une sécurité accrue par rapport à NTFS. Nous avons également découvert Iperius Backup, un outil puissant pour la sauvegarde et la restauration de données, permettant une sauvegarde complète et immédiate le lundi à 23h, et des sauvegardes incrémentielles du mardi au vendredi à 23h, une approche souple et adaptée à une politique de protection des données continue.

Enfin, ce TP nous a permis d’appliquer concrètement les concepts étudiés en cours ces dernières semaines, consolidant nos connaissances en gestion de la redondance des données et en automatisation des sauvegardes. Ces compétences seront sans nul doute utiles dans notre futur environnement professionnel, en nous préparant aux exigences de la disponibilité et de la sécurité des données en entreprise.

1. WEBOGRAPHIE
2. LinkedIn : **Quels sont les avantages et les inconvénients du RAID logiciel par rapport au RAID matériel ?**<https://fr.linkedin.com/advice/1/what-advantages-disadvantages-software-raid-versus?lang=fr#:~:text=Le%20RAID%20mat%C3%A9riel%20dispose%20souvent,d'exploitation%20ou%20des%20pilotes>.  
   //publié par [Systèmes de fichiers](https://www.linkedin.com/showcase/skills-file-systems/)
3. AOMEI - Différence **entre GPT et MBR Tout savoir** : https://www.diskpart.com/fr/resource/difference-entre-mbr-et-gpt.html
4. IONOS / Niveaux RAID - **comparaison des principales approches RAID** : <https://www.ionos.fr/digitalguide/serveur/securite/comparaison-des-niveaux-raid/>
5. Microsoft : **Disques de base et dynamiques :** <https://learn.microsoft.com/fr-fr/windows/win32/fileio/basic-and-dynamic-disks>
6. Wikipédia RAID (Informatique) : https://fr.wikipedia.org/wiki/RAID\_(informatique)
7. Iperius Backup - **Qu’est-ce que Iperius Backup ?** : <https://www.iperiusbackup.net/fr/quest-ce-que-iperius-backup/>
8. Iperius Backup - connecter votre espace de stockage objet Leviia (compatible S3) : <https://wiki.leviia.com/fr/article/iperius-backup-connecter-votre-espace-de-stockage-objet-leviia-compatible-s3-f0t5kq/>
9. TechTarget (anglais), **When should a backup job be scheduled for max performance?** <https://searchdatabackup.techtarget.com/answer/When-should-a-backup-job-be-scheduled-for-max-performance>
10. TechRepublic (anglais), **5 strategies for a successful backup plan** <https://www.techrepublic.com/article/5-strategies-for-a-successful-backup-plan/>
11. Iperius Backup - Choisissez une licence en fonction du type de sauvegarde : <https://www.iperiusbackup.fr/backup-software-windows.aspx>

1. [LinkedIn : Quels sont les avantages et les inconvénients du RAID logiciel par rapport au RAID matériel ?](https://fr.linkedin.com/advice/1/what-advantages-disadvantages-software-raid-versus?lang=fr#:~:text=Le%20RAID%20mat%C3%A9riel%20dispose%20souvent,d'exploitation%20ou%20des%20pilotes.) [↑](#footnote-ref-2)
2. [MiniTool : Quelle est la différence entre volume et partition sur l’OS Windows ?](https://www.minitool.com/fr/disque-partition/volume-vs-partition.html) [↑](#footnote-ref-3)