# Cours 12 :

# Sauvegardes et logs

JACQUEMIN Mathieu

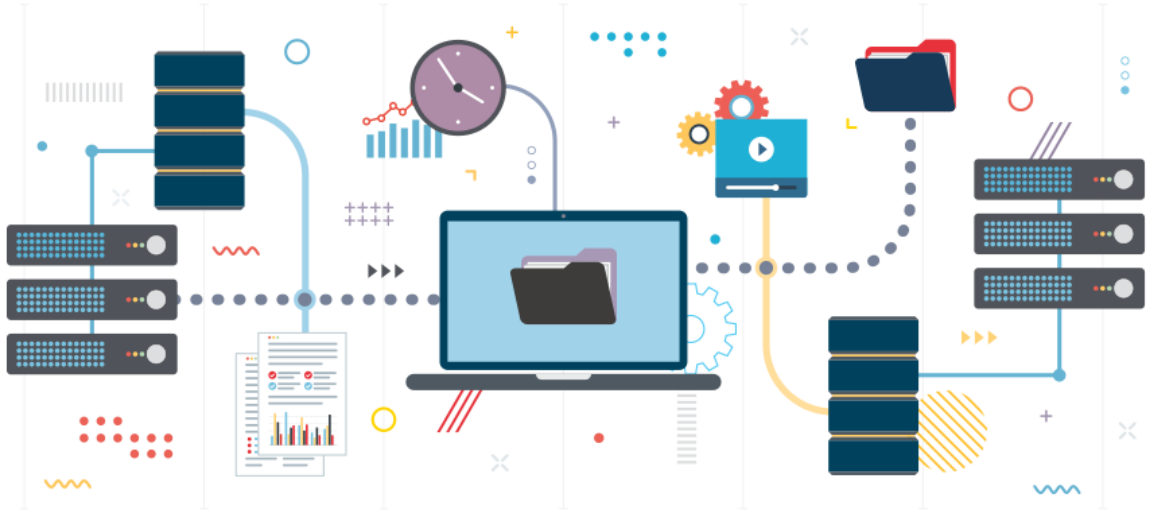
# Disclaimer



- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

# Introduction aux sauvegardes

**La sauvegarde de données (backup en anglais) consiste à dupliquer sur un support de stockage des données numériques afin d'avoir la capacité de les restaurer en cas d'incident ou de perte.**



# Introduction aux sauvegardes



**Les sauvegardes de données ont pour objectif de protéger les données contre la perte ou la corruption. En créant des copies de sauvegarde des données importantes et en les stockant dans des emplacements sécurisés**

# Introduction aux sauvegardes



Il existe plusieurs méthodes de sauvegarde, chacune ayant ses propres avantages et inconvénients. Les sauvegardes peuvent être complètes, différentielles ou incrémentielles, et elles peuvent être effectuées localement sur des périphériques de stockage ou dans le cloud.

# Risques associés à la perte de données



- Perte de productivité
- Perte financière
- Violation de la confidentialité
- Perte de confiance
- Risques de conformité
- Attaques de cybercriminel

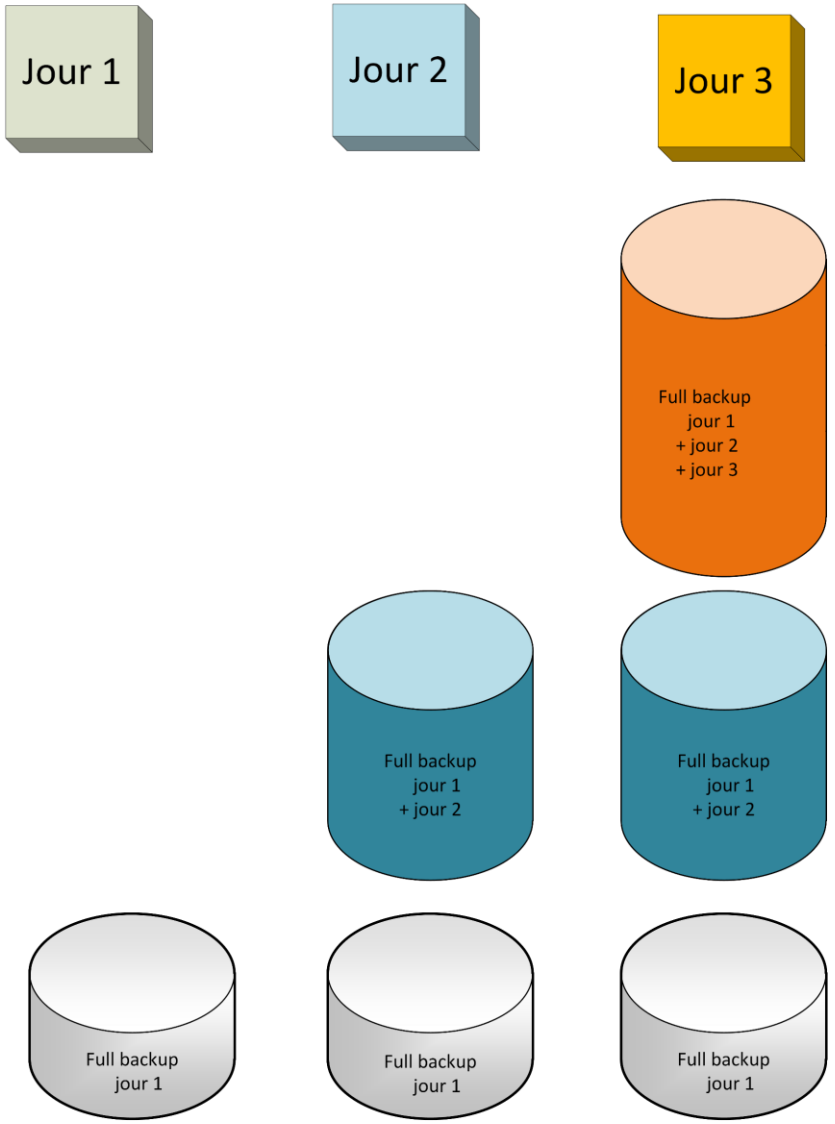
# Types de sauvegardes

## La sauvegarde complète

La sauvegarde complète consiste à copier intégralement toutes les données sélectionnées. Cela inclut tous les fichiers et répertoires, qu'ils aient été modifiés ou non depuis la dernière sauvegarde. Bien que cela nécessite souvent plus d'espace de stockage et de temps pour effectuer la sauvegarde, elle offre une simplicité et une fiabilité maximales lors de la restauration des données.

# Types de sauvegardes

Sauvegarde complète (Full backup)



# Types de sauvegardes

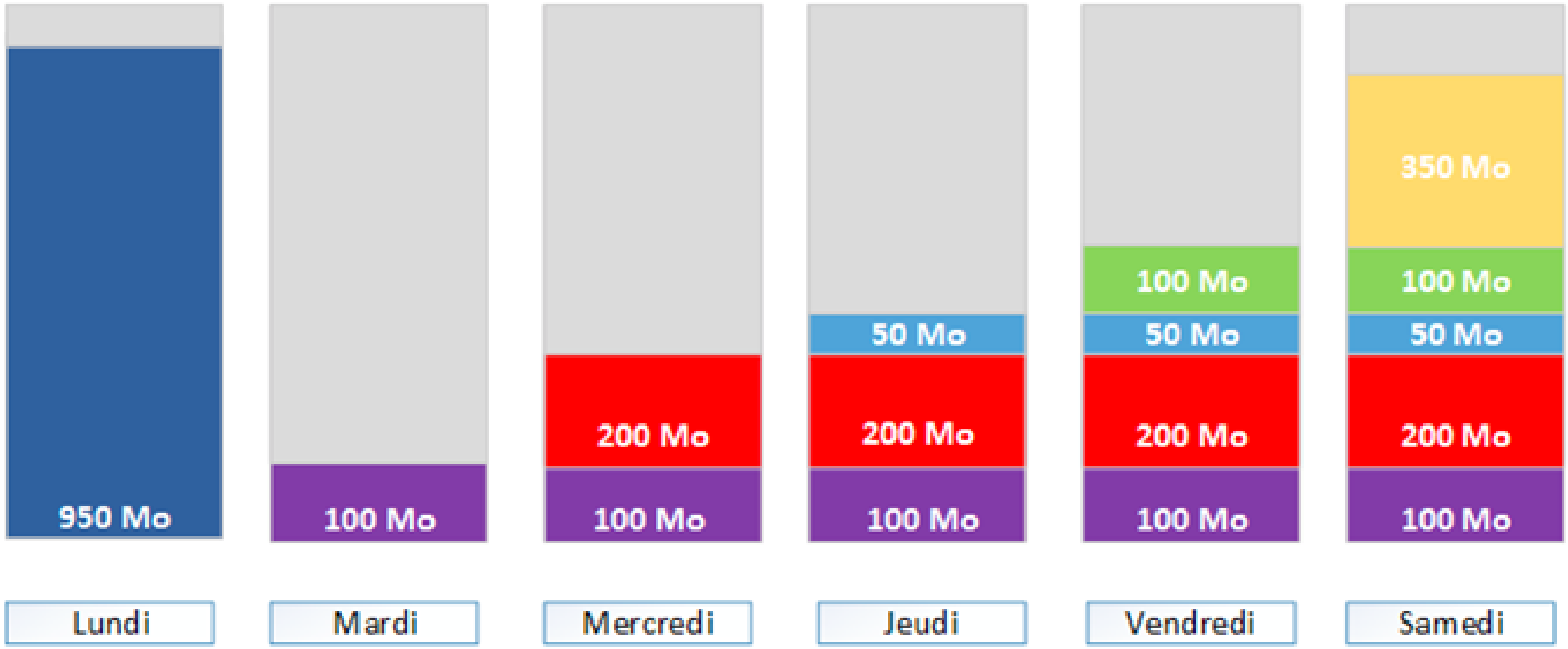
- A chaque sauvegarde complète, l'intégralité des données sont à nouveau copiées sur le support de sauvegarde
- Le temps de sauvegarde est long et proportionnel au volume de données à copier. La fréquence des sauvegardes est en général d'une semaine. Si les données changent très peu car il est alors possible d'espacer davantage les sauvegardes (1 fois par mois par exemple).
- Pour restaurer les données il suffit de prendre la dernière sauvegarde complète.
- Le temps de restauration est long et proportionnel au volume de données à copier.
- Il n'est pas nécessaire de garder les sauvegardes les plus anciennes sauf obligation réglementaire comme la conservation des logs de navigation sur Internet pendant une année.

# Types de sauvegardes

## La sauvegarde différentielle

Il est d'abord nécessaire de réaliser une première sauvegarde complète. Puis les sauvegardes suivantes sont différentielles c'est à dire que le logiciel de sauvegarde vérifie quels sont les fichiers qui ont été modifiés depuis la sauvegarde complète. Toutes les sauvegardes différentielles suivantes se feront toujours par rapport à la première sauvegarde complète.

# Types de sauvegardes



# Types de sauvegardes

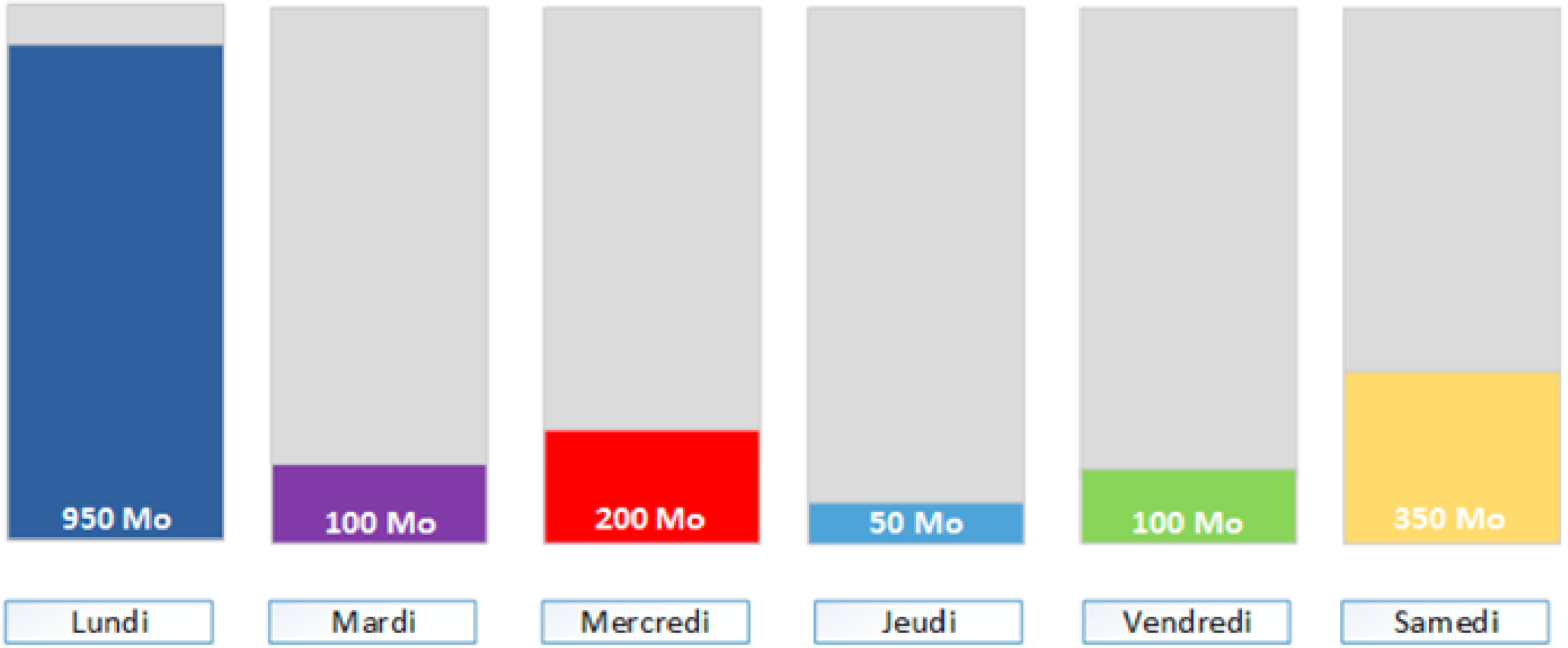
- La sauvegarde différentielle est plus rapide et utilise moins d'espace de stockage. Cela est très utile pour des sauvegardes fréquentes et donc journalières. Le temps de sauvegarde prendra davantage de temps au fur et à mesure car la comparaison des fichiers s'effectue toujours par rapport à la toute première sauvegarde complète.
- Seuls les fichiers modifiés depuis la sauvegarde complète sont sauvegardés.
- La restauration nécessite uniquement la dernière sauvegarde complète ainsi que la dernière sauvegarde différentielle. Le temps de restauration va augmenter avec les sauvegardes différentielles successives et il est nécessaire de refaire une sauvegarde complète de temps en temps pour améliorer les durées d'exécution de restauration.

# Types de sauvegardes

## La sauvegarde incrémentielle

Il est d'abord nécessaire de réaliser une première sauvegarde complète. Puis les sauvegardes suivantes sont incrémentales c'est à dire que le logiciel de sauvegarde vérifie quels sont les fichiers qui ont été modifiés ou créés depuis la sauvegarde précédente, complète ou incrémentale. De cette manière, seuls les fichiers modifiés seront pris en compte dans cette sauvegarde incrémentale.

# Types de sauvegardes



# Types de sauvegardes

- La sauvegarde incrémentale est très rapide et utilise un faible espace de stockage. Cela est très utile pour des sauvegardes fréquentes, journalières et même plusieurs fois par jour ;;
- Seuls les fichiers modifiés sont sauvegardés.
- La restauration est moins rapide car il est nécessaire d'utiliser la dernière sauvegarde complète ainsi que toutes les sauvegardes incrémentales réalisées depuis cette sauvegarde complète.

# Méthodes de sauvegarde

## La sauvegarde locale

**Les sauvegardes locales consistent à stocker les copies de sauvegarde sur des périphériques de stockage physiques situés sur site, tels que des disques durs externes, des serveurs de sauvegarde locaux ou des bandes magnétiques.**



# Méthodes de sauvegarde

**Avantages :**

- **Contrôle total sur les données : Les données sont stockées et gérées localement, offrant un contrôle total sur la sécurité et la disponibilité des données.**
- **Performances élevées : Les sauvegardes locales peuvent être plus rapides que les sauvegardes dans le cloud en raison de la vitesse des connexions locales.**

**Inconvénients :**

- **Vulnérabilité aux sinistres locaux : Les données sauvegardées localement peuvent être perdues en cas de sinistre local, tels qu'un incendie, un vol ou une catastrophe naturelle.**
- **Coût de maintenance : Les périphériques de stockage locaux nécessitent une maintenance régulière et peuvent entraîner des coûts supplémentaires pour les mises à niveau et le remplacement.**

# Méthodes de sauvegarde

## La sauvegarde distante (et cloud)

**Les sauvegardes distantes consistent à stocker les copies de sauvegarde sur des périphériques de stockage physiques situés en dehors du site de l'entreprise, généralement dans un centre de données distant ou sur un site de sauvegarde tiers.**



# Méthodes de sauvegarde

**Avantages :**

- **Protection contre les sinistres locaux : Les sauvegardes distantes offrent une protection contre les sinistres locaux en assurant que les données sauvegardées sont stockées en dehors du site principal de l'entreprise.**
- **Redondance géographique : Les sauvegardes distantes garantissent une redondance géographique des données, ce qui augmente la résilience et la disponibilité des données.**

**Inconvénients :**

- **Dépendance à l'égard des connexions réseau : Les sauvegardes distantes nécessitent une connexion réseau fiable et rapide, ce qui peut être un défi dans certaines situations.**
- **Coûts de bande passante : Les sauvegardes distantes peuvent entraîner des coûts supplémentaires liés à l'utilisation de la bande passante pour transférer les données vers le site distant.**

# Le plan de sauvegarde



Un plan de sauvegarde décrit en détail la stratégie et les procédures à suivre pour sauvegarder et restaurer les données de manière efficace et sécurisée.

Il inclut des informations telles que les types de sauvegarde à utiliser, la fréquence des sauvegardes, les périphériques de stockage à utiliser, les horaires de sauvegarde, les responsabilités des employés, les politiques de rotation des sauvegardes, et les procédures de restauration des données en cas de besoin.

# Exemple

- Types de Sauvegarde :

Sauvegarde complète hebdomadaire
Sauvegarde différentielle quotidienne
Sauvegarde incrémentielle toutes les heures pendant les heures de bureau

- Périphériques de Stockage :

Utilisation d'un disque dur externe pour les sauvegardes locales
Utilisation d'un service de stockage cloud pour les sauvegardes distantes

- Horaires de Sauvegarde :

Sauvegarde complète : tous les dimanches à 20h00
Sauvegarde différentielle : tous les jours à 18h00
Sauvegarde incrémentielle : toutes les heures pendant les heures de bureau (8h00-18h00)

- Rotation des Sauvegardes :

Rotation des disques durs externes tous les mois pour assurer une sauvegarde hors site
Conservation des sauvegardes cloud pendant une durée de rétention de 30 jours

- Responsabilités :

Le responsable informatique est chargé de superviser la planification et l'exécution des sauvegardes
Les utilisateurs sont responsables de la sauvegarde régulière de leurs données sur les serveurs partagés

# La règle du 3-2-1

La règle stipule que vous devez avoir au moins :

- 3 copies de vos données
- 2 sauvegardes stockées sur des types de supports différents
- 1 sauvegarde doit être stockée hors site ou sur le cloud

En suivant la règle des 3-2-1, les entreprises peuvent s'assurer une protection optimale de leurs données en créant des sauvegardes redondantes et résilientes. Cette stratégie permet de minimiser les risques de perte de données et de garantir la disponibilité des informations critiques en cas de besoin.

# La règle du 3-2-1

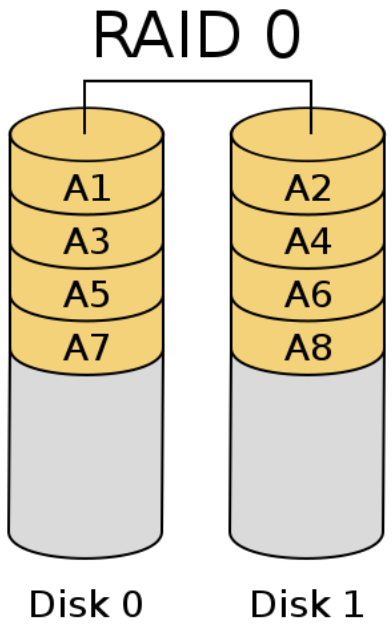
# Introduction au RAID

La technologie RAID (Redundant Array of Independent Disks ou regroupement redondant de disques indépendants) permet d'améliorer la sécurité et/ou la performance des disques d'un serveur (ou d'un pc).

Son principe consiste à répartir les données sur plusieurs disques durs. Cette répartition se fera différemment en fonction des priorités et du budget de l'entreprise. Certaines configurations privilégient la sécurité, d'autres la performance et certaines les deux.

# RAID 0

**La configuration RAID 0 permet d'améliorer la performance du système en répartissant 50% des données sur un disque et 50% sur l'autre. Les deux disques travaillant simultanément, on dispose ainsi de performances deux fois plus élevée.**



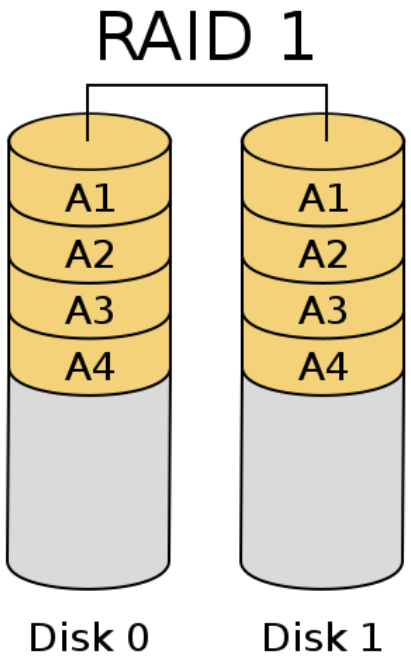

• Volumétrie utile = Volumétrie totale
Les données n'étant pas dupliquées, il n'y aura pas de perte de volume stockage.

• Sécurité des données : FAIBLE
Il est fortement déconseillé d'utiliser cette configuration pour des serveurs assurant les services critiques de votre entreprise. Les données n'étant à aucuns moments dupliquées seront perdues si un des deux disques venait à être défectueux.

• Fonctionne uniquement sur deux disques

# RAID 1 (ou RAID MIROIR)

**La configuration RAID 1 permet de sécuriser un système en disposant de deux disques avec exactement les mêmes données. Dans cette configuration on ne recherche pas la performance mais plutôt la sécurité.**

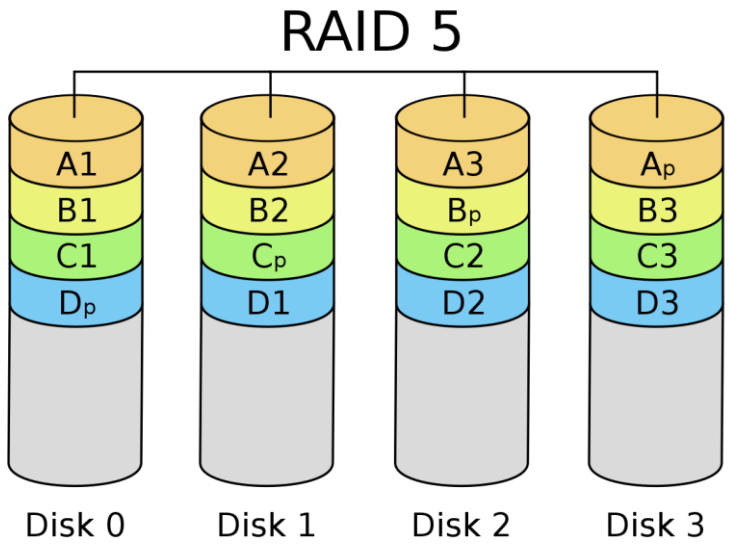



• Volumétrie utile = Volumétrie totale / 2
Le disque 1 contenant exactement les mêmes données que le disque 2, la volumétrie utile sera divisée par 2.

• Sécurité des données : BONNE
Si un disque venait à être défaillant, cela ne poserait pas de problèmes car le second prendrait directement le relais.

# RAID 5

**La configuration RAID 5, par un système de parité, répartit une petite partie des données sur chaque disque. Dans cette configuration, ce n'est pas la performance qu'on recherche mais plutôt la sécurité tout en économisant le volume de stockage.**



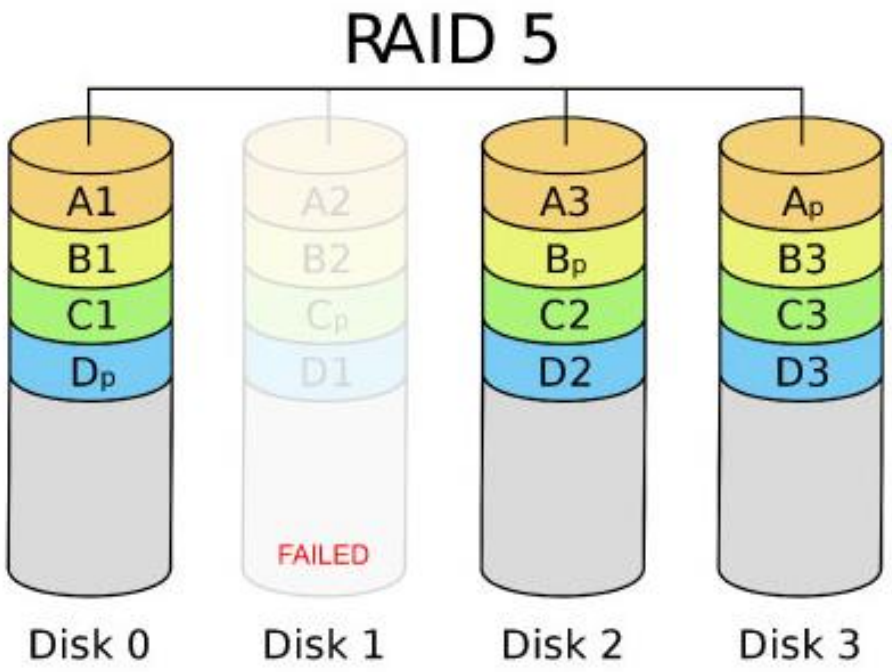

• Volumétrie utile = Nombre de disques - 1 X capacité d'un disque
Pour 3 disques de 200 Go, on aurait ainsi 3 -1 X 200 = 400 Go de volumétrie utile.

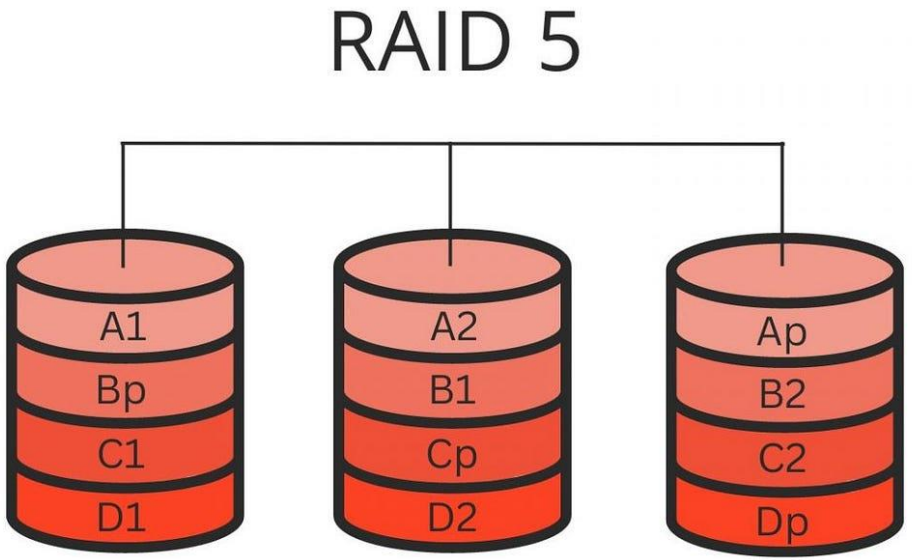
• Sécurité des données : CORRECTE
Dans cette configuration, on ne peut se permettre de perdre qu'un seul disque.

• Nombre de disques nécessaires : Au moins 3

# RAID 5

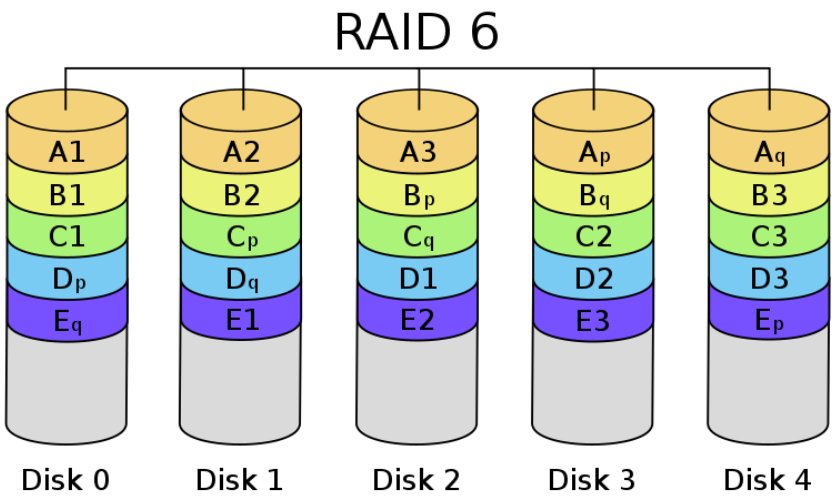



RAID 5
A1
B1
C1
Dp
A2
B2
Cp
D1
FAILED
A3
Bp
C2
D2
Ap
B3
C3
D3
Disk 0
Disk 1
Disk 2
Disk 3


RAID 5
A1
Bp
C1
D1
A2
B1
Cp
D2
Ap
B2
C2
Dp

# RAID 6

**La configuration RAID 6, fonctionne exactement de la même manière que le RAID 5, par un système de parité, mais cette fois avec 2 disques de parités à la place s'un seul**



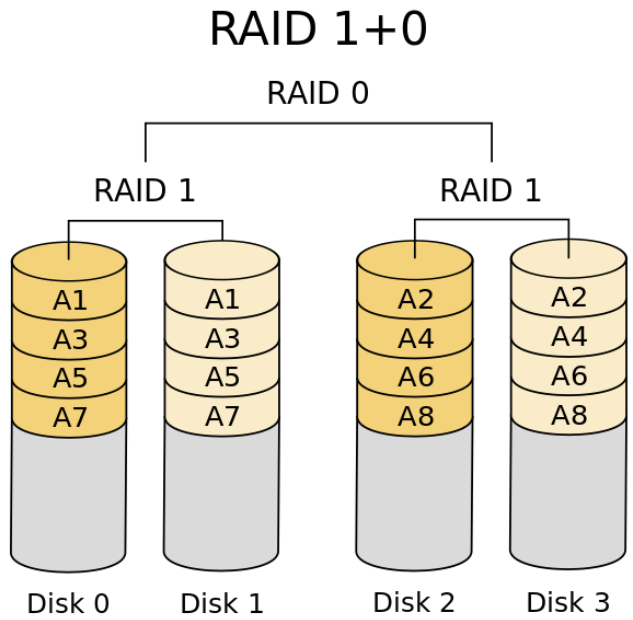

• Volumétrie utile = Nombre de disques - 2 X capacité d'un disque
Pour 5 disques de 200 Go, on aurait ainsi 5 -2 X 200 = 600 Go de volumétrie utile.

• Sécurité des données : TRES BONNE
Dans cette configuration, on peut se permettre de perdre 2 disques.

• Nombre de disques nécessaires : Au moins 4

# RAID 10 (1 + 0)

**La configuration RAID 10 répartit dans une première grappe les données en RAID 0, et dans une seconde grappe en RAID 1.Celle-ci permet ainsi de disposer du niveau de sécurité de la configuration RAID 1 avec les performances qu'offre la configuration RAID 0.**



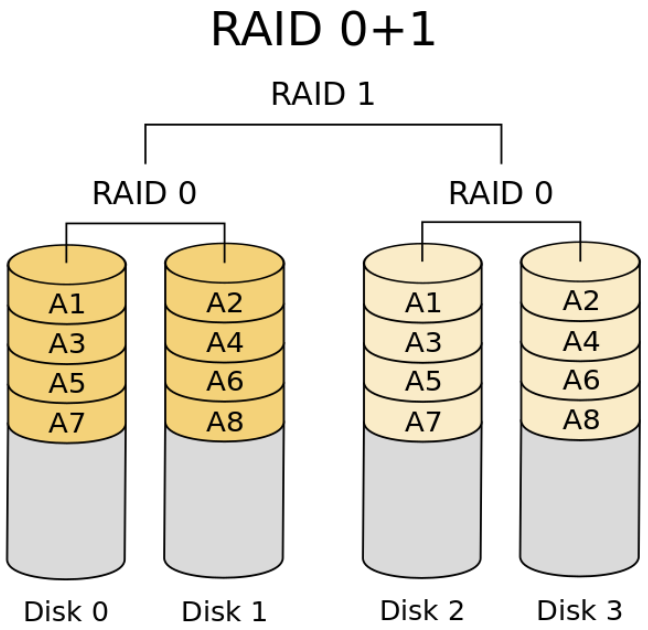

- Volumétrie utile = Volumétrie totale / 2

- Sécurité des données : BONNE
Cette configuration offre un très bon niveau de sécurité car pour qu'une défaillance globale apparaisse, il faudrait que tous les éléments d'une grappe présentent un défaut en même temps.

- Nombre de disques nécessaires : Au moins 4

# RAID 01 (0 + 1)

**A l'inverse de la configuration RAID 10, le RAID 01 répartit dans une première grappe les données en RAID 1, puis dans une seconde grappe en RAID 0.**



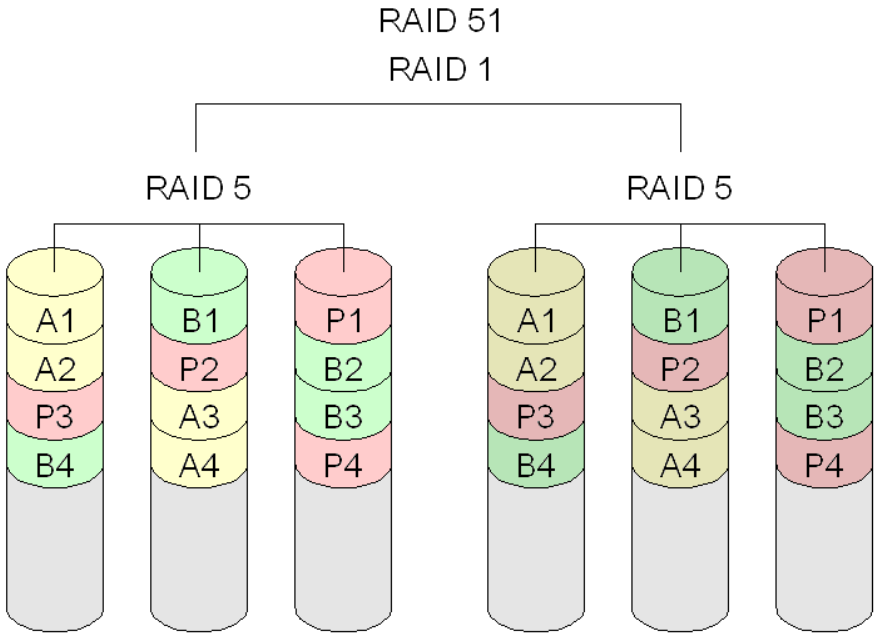

- Volumétrie utile = Volumétrie totale / 2

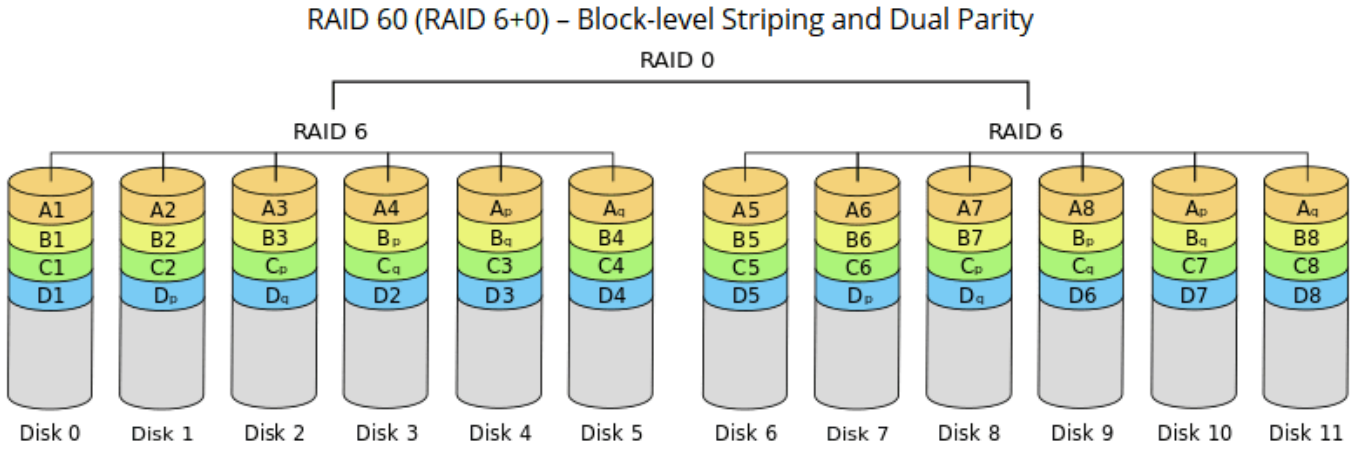
- Sécurité des données : MOYENNE

Dans cette configuration, si un disque présente un défaut, il entraîne une défaillance de toute la grappe et altère donc la performance du système.

# Autre RAID




RAID 51
RAID 1
RAID 5
RAID 5
A1
A2
P3
B4
B1
P2
A3
A4
P1
B2
B3
P4
A1
A2
P3
B4
B1
P2
A3
A4
P1
B2
B3
P4


RAID 60 (RAID 6+0) – Block-level Striping and Dual Parity
RAID 0
RAID 6
RAID 6
A1 B1 C1 D1
A2 B2 C2 Dp
A3 B3 Cp Dq
A4 Bp Cq D2
Ap Bq C3 D3
Aq B4 C4 D4
A5 B5 C5 D5
A6 B6 C6 Dp
A7 B7 Cp Dq
A8 Bp Cq D6
Ap Bq C7 D7
Aq B8 C8 D8
Disk 0
Disk 1
Disk 2
Disk 3
Disk 4
Disk 5
Disk 6
Disk 7
Disk 8
Disk 9
Disk 10
Disk 11

# Introduction aux logs

En informatique, les logs (journaux d'évènements) sont des fichiers qui enregistrent des événements qui se produisent sur un système d'exploitation ou tout autre équipement informatique, routeur, switch, serveur.

Ils sont essentiels pour la surveillance, le diagnostic des problèmes, la conformité réglementaire et la sécurité des systèmes.

# Les différents logs

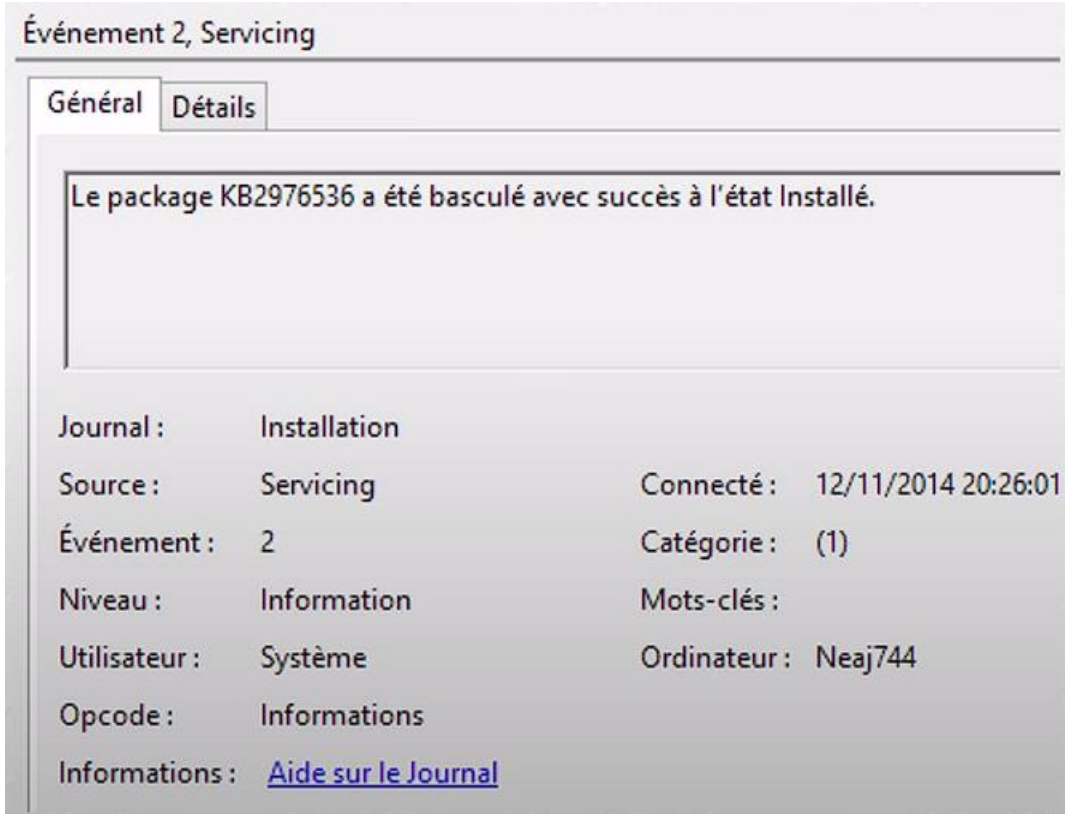
**Logs Système : Enregistrent les événements liés au fonctionnement du système d'exploitation, tels que les démarrages, les arrêts, les erreurs système et les pannes.**

**Logs de Sécurité : Enregistrent les tentatives d'accès, les violations de sécurité, les erreurs d'authentification et d'autres événements liés à la sécurité du système.**

**Logs d'Application : Enregistrent les événements générés par les applications installées sur le système, tels que les erreurs de programme, les activités de base de données, etc.**

**Logs Réseau : Enregistrent les activités réseau telles que les connexions entrantes et sortantes, les paquets rejetés, les tentatives d'intrusion et les performances du réseau.**

# Logs


Événement 2, Servicing
Général
Détails
Le package KB2976536 a été basculé avec succès à l'état Installé.
Journal : Installation
Source : Servicing
Connecté : 12/11/2014 20:26:01
Événement : 2
Catégorie : (1)
Niveau : Information
Mots-clés :
Utilisateur : Système
Ordinateur : Neaj744
Opcode : Informations
Informations : Aide sur le Journal

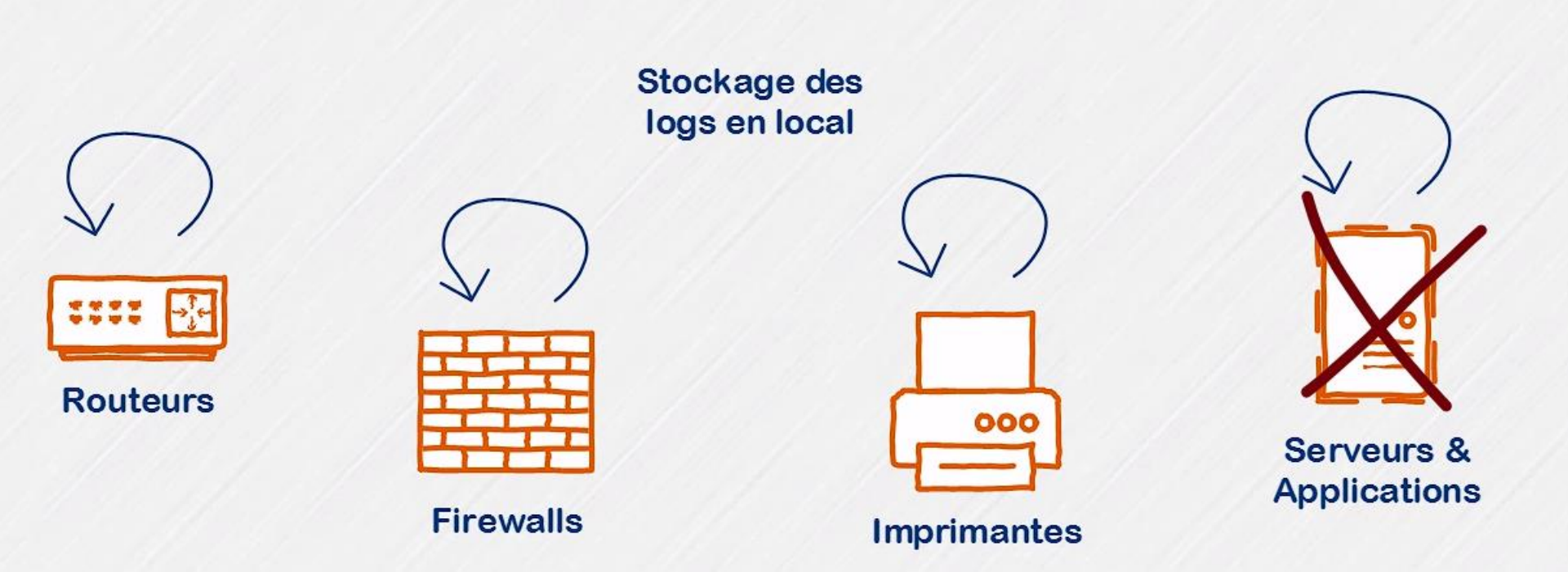

192.168.10.1 - - [13/Nov/2014:22:02:22 +0100] "GET /wordpress/phpBB3/styles/absolution/theme/images/useroffline.png HTTP/1.1" 200 3872 "http://192.168.10.128/wordpress/phpBB3/style.php?id=2&lang=en&sid=2cb4eee52b3388a15bd91ec997976a43" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0"
Nov 17 18:29:52 debian sshd[3479]: Server listening on 0.0.0.0 port 22.
Nov 17 18:29:52 debian sshd[3479]: Server listening on :: port 22.
Nov 17 18:30:34 debian login[3514]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=root
Nov 17 18:30:38 debian login[3514]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication failure

# L'analyse de logs

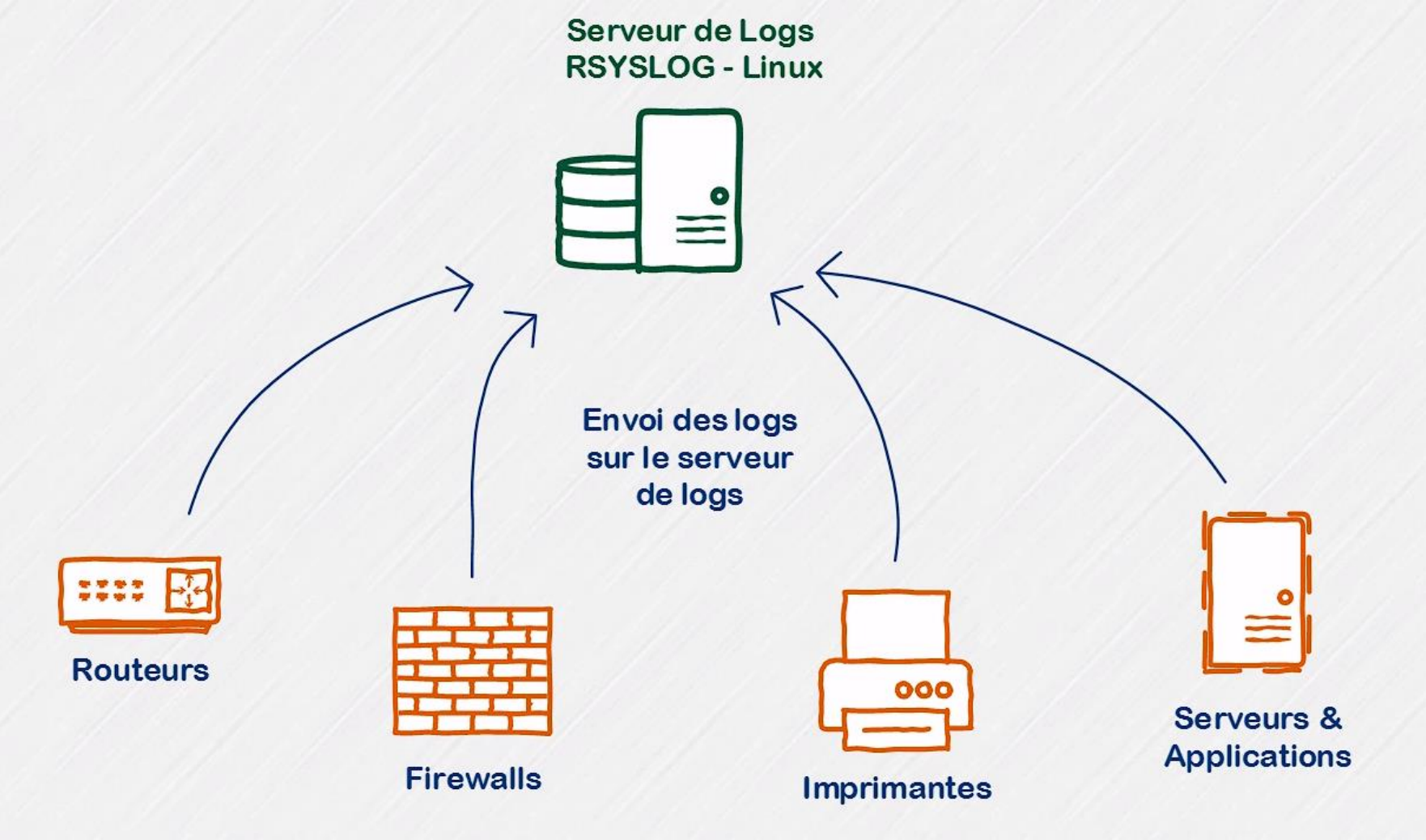
L'analyse des logs consiste à examiner les enregistrements pour détecter les anomalies, identifier les problèmes de performance, suivre les activités des utilisateurs et détecter les tentatives d'intrusion ou les violations de sécurité.

Des outils d'analyse des logs automatisent ce processus en permettant la recherche, le filtrage et la visualisation des données de journalisation.

# Logs


Stockage des logs en local
Routeurs
Firewalls
Imprimantes
Serveurs & Applications

# Logs


Serveur de Logs
RSYSLOG - Linux
Envoi des logs
sur le serveur
de logs
Routeurs
Firewalls
Imprimantes
Serveurs &
Applications

# Syslog

**Protocole qui sert à envoyer des fichiers du journal système ou des messages d'événements à un serveur dédié appelé serveur syslog.**