20/11/2017

COUSIN GILDAS

Exia CESI

Prosit 2.1 – Installation et maintenance d'un serveur



# Problématique :

Comment créer un plan permettant de gérer les pannes ?

Comment installer un serveur Linux ?

# Mots clés :

GED : La GED représente l'utilisation de moyens informatisés pour l'ensemble de la gestion d'un document électronique

# Plan d’action :

## Partie Etude

### Partie 1 – Les sauvegardes

#### 1.1. Données

Une sauvegarde n'est rien d'autre qu'une image statique des données sauvegardées. Elle représente une copie de ces données à un moment précis.

Les données doivent être regroupés car elles ne sont pas toutes pareils ; certaines se mette à jour tous les jours, d’autres tous les ans :

* Système d'exploitation : Change lors d’une maj
* Logiciels d'applications : Maj/Installation ou suppression
* Données d'applications : Execution de l’application (toutes les secondes ou chaque save)
* Données utilisateur : Non stop

#### 1.2 Types de sauvegardes

Trois types de sauvegardes :

* Les sauvegardes complètes : Ne vérifie pas si le fichier a changé
* Les sauvegardes incrémentielles : Si le fichier a changé depuis la date de la dernière sauvegarde enregistre le fichier sinon non. […] L'inconvénient majeur des sauvegardes incrémentielles est que la restauration de tout fichier donné nécessitera peut-être des recherches dans une ou plusieurs sauvegarde(s) incrémentielle(s) jusqu'à ce que le fichier en question puisse être localisé.
* Les sauvegardes différentielles : Même fonctionnement qu’incrémentielles mais est cumulatives. Ainsi, chaque sauvegarde différentielle contient tous les fichiers modifiés depuis la dernière sauvegarde complète, permettant par là-même une restauration complète en n'utilisant que la dernière sauvegarde complète et la dernière sauvegarde différentielle.

#### 1.3 Support de sauvegarde

Plusieurs support de sauvegarde :

* Bande : Bon marché/bon stockage, plutôt fiable. /!\ S’use, L'accès aux données stockées sur un tel support se fait de manière séquentielle. Doit avoir un suivi d’utilisation.
* Disque : couteux / Rapide. MAIS /!\ : non amovible en général. Fragiles. Pas un support d’archive. Certains centres de données sauvegardent sur disques durs et ensuite, une fois les sauvegardes effectuées, les enregistrent sur bande pour l'archivage. Cette approche permet la sauvegarde la plus rapide possible pendant le temps imparti pour cette opération.
* Réseau : Uniquement associé à des technologies de sauvegardes de masses. Ex : Faire un lien réseau rapide vers un centre de stockages distants. Si bonne largeur de bande pour le réseau, rapide. /!\ Cette approche ne résout pas le problème du stockage d'archives / Coute cher

<http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-fr-4/s1-disaster-backups.html>

### Partie 2 – Commandes Linux

1. Top – Linux Process Monitoring

2. VmStat – Virtual Memory Statistics

3. Lsof – List Open Files

4. Tcpdump – Network Packet Analyzer

5. Netstat – Network Statistics

6. Htop – Linux Process Monitoring

7. Iotop – Monitor Linux Disk I/O

8. Iostat – Input/Output Statistics

9. IPTraf – Real Time IP LAN Monitoring

10. Psacct or Acct – Monitor User Activity

11. Monit – Linux Process and Services Monitoring

12. NetHogs – Monitor Per Process Network Bandwidth

13. iftop – Network Bandwidth Monitoring

14. Monitorix – System and Network Monitoring

15. Arpwatch – Ethernet Activity Monitor

16. Suricata – Network Security Monitoring

17. VnStat PHP – Monitoring Network Bandwidth

18. Nagios – Network/Server Monitoring

19. Nmon: Monitor Linux Performance

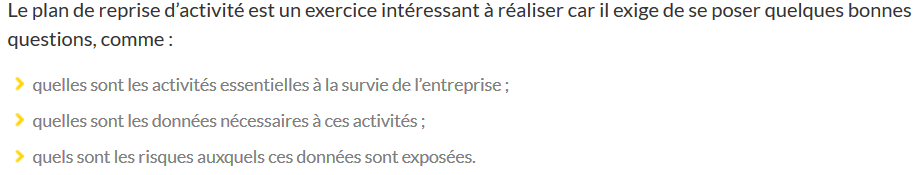
20. Collectl: All-in-One Performance Monitoring Tool

<https://www.tecmint.com/command-line-tools-to-monitor-linux-performance/>

<http://sgill.profweb.ca/spip/IMG/pdf/21_Performance.pdf>

### Partie 3 – Plan de reprises d’activités

Un plan de reprise d'activité est un document qui permet à une entreprise de prévoir, par anticipation, les démarches à entreprendre pour reconstruire et remettre en route un système informatique en cas d’accident important du centre informatique.



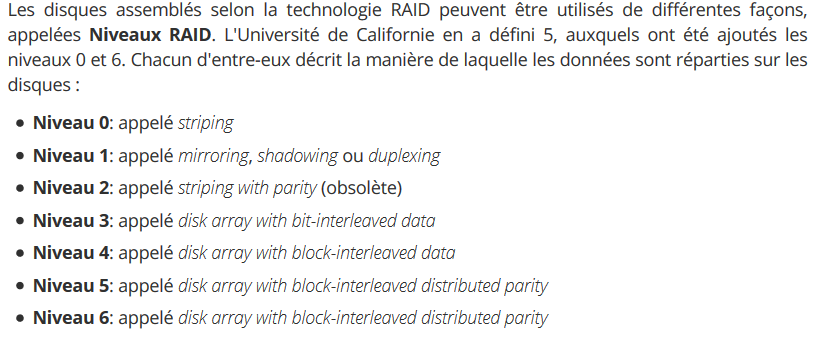
Le **RTO** désigne le temps maximal acceptable durant lequel une ressource informatique peut se trouver indisponible suite à un sinistre (Return Time on Objective).  
**RPO** est la Perte de données maximale admissible (Recovery Point Objective). Elle est également exprimée en temps (minutes / heures) car elle résulte de la différence entre la dernière sauvegarde et l’incident.



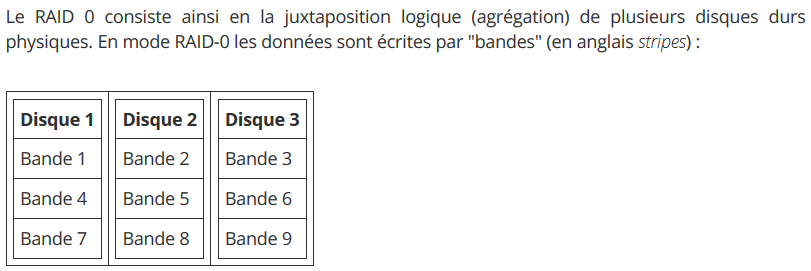
<http://www.journaldunet.com/business/dictionnaire-economique-et-financier/1199343-pra-plan-de-reprise-d-activite-definition-traduction/>

### Partie 4 - RAID

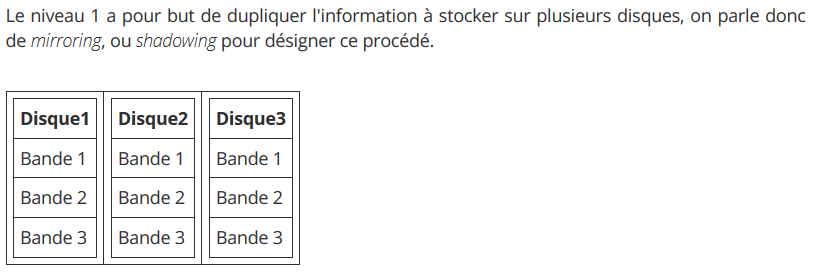
RAID (*Redundant Array of Inexpensive Disks*) permet de constituer **une** unité de stockage à partir de plusieurs [disques durs](http://www.commentcamarche.net/contents/740-disque-dur). L'unité ainsi créée (appelée **grappe**) a donc une grande tolérance aux pannes (haute disponibilité), ou bien une plus grande capacité/vitesse d'écriture. La répartition des données sur plusieurs disques durs permet donc d'en augmenter la sécurité et de fiabiliser les services associés.



Niveau 0 : Striping. consiste à stocker les données en les répartissant sur l'ensemble des disques de la grappe. De cette façon, il n'y a pas de redondance, on ne peut donc pas parler de tolérance aux pannes. En effet en cas de défaillance de l'un des disques, l'intégralité des données réparties sur les disques sera perdue.



Niveau 1 :

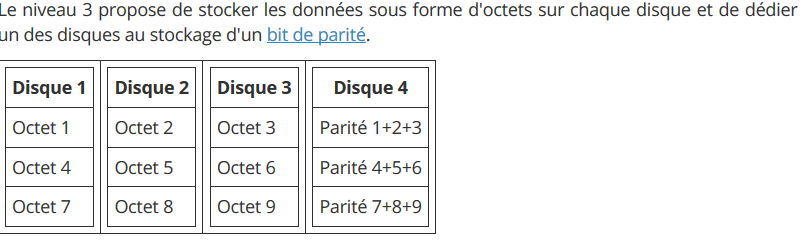


On obtient ainsi une plus grande sécurité des données, car si l'un des disques tombe en panne, les données sont sauvegardées sur l'autre. D'autre part, la lecture peut être beaucoup plus rapide lorsque les deux disques sont en fonctionnement. Enfin, étant donné que chaque disque possède son propre contrôleur, le serveur peut continuer à fonctionner même lorsque l'un des disques tombe en panne.

En contrepartie la technologie RAID1 est très onéreuse étant donné que seule la moitié de la capacité de stockage n'est effectivement utilisée.

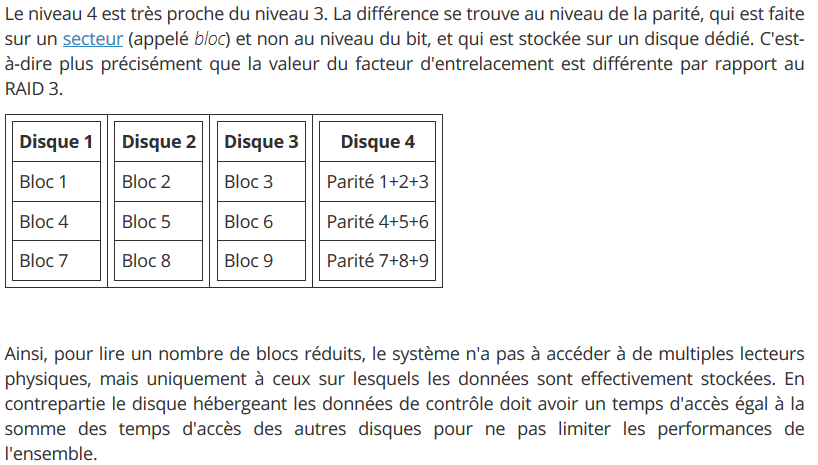
Niveau 2 : Obsolète

Niveau 3 :

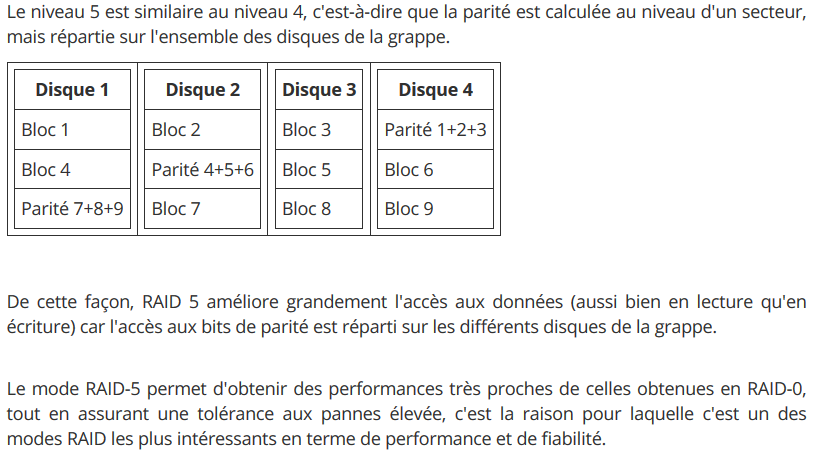


si l'un des disques venait à défaillir, il serait possible de reconstituer l'information à partir des autres disques. Après "reconstitution" le contenu du disque défaillant est de nouveau intègre. Par contre, si deux disques venaient à tomber en panne simultanément, il serait alors impossible de remédier à la perte de données.

Niveau 4 :



Niveau 5 :



Niveau 6 : Le niveau 6 a été ajouté aux niveaux définis par Berkeley. Il définit l'utilisation de 2 fonctions de parité, et donc leur stockage sur deux disques dédiés. Ce niveau permet ainsi d'assurer la redondance en cas d'avarie simultanée de deux disques. Cela signifie qu'il faut au moins 4 disques pour mettre en oeuvre un système RAID-6.

## Partie Workshop

passwd : mdp

ifconfig : ipconfig

192.168.74.130 / 255

etc/network/iface

/etc/ssh/sshd\_config

ps : liste des processus

kill + PID = tue proco

lsof -i : vérifier la connexion réseau

df : vérifier l'état des disque dur

shutdown -r = reboot (-t pour changer le temps avant lequel)

crontab

# Validation des pistes de solutions :

Il existe un monitor de perf sur linux qui s'appel : System Monitor.

On doit config l'interface réseau.

On doit (bien) nommer la machine.

On doit télécharger des paquets.

Connection a un DHCP.

Faire plusieurs types de serveurs à tempo diff.

Utiliser Apacheu 2.

Disques en RAID

Affecter un DNS

Créer une image « Master ».

Configurer les droits de plusieurs utilisateurs.

Configurer un accès distant.