SAUVEGARDES

Tome 1

LA VIE N'EST PAS UN LONG FLEUVE TRANQUILLE

Au secours ! Le monde est plein de menaces

La tuyauterie qui passe au dessus de mes serveurs a fuit ; tout a été inondé, il y a eu plein de court-circuits, et mes disques durs sont morts (c'est la faute au plombier)

La clim de ma salle machine est tombé en panne; il a fait 60° dans les racks, et les disques durs sont morts (c'est à la faute au plombier)

J'ai fait tomber mon portable, le disque dur est mort (c'est la faute à Newton)

On a volé mon ordi dans le TGV (c'est la faute au voleur)

LA VIE N'EST PAS UN LONG FLEUVE TRANQUILLE

Au secours ! Le monde est plein de menaces

Word **m'a bousillé mon fichier** `these.doc` **qui ne faisait que 1257 pages et 3198 Mo (c'est la faute à *Word* –ou à *Windows*-)**

J'ai eu un rançongiciel qui a crypté tous mes fichiers (c'est la faute au virus)

Un collègue distrait a fait un « `rm -rf / dirtest` **» et ça a supprimé tout le contenu de mon serveur (c'est la faute au collègue -ou à *Linux*-)**

Un pirate a fait un « `format c: /yes` **» (c'est la faute au pirate, ou à *Windows**)**

*** : Score : 1 pour Linux, 2 pour Windows**

LA VIE N'EST PAS UN LONG FLEUVE TRANQUILLE

Au secours ! Le monde est plein de menaces

Mon serveur *NAS* était en *RAID6* ; j'ai constaté par hasard que deux disques dur étaient en panne (pas grave, c'est du RAID 6) ; je les ai remplacés, mais pendant le *rebuild*, un troisième disque est tombé en panne… (c'est la faute à *Synology*)

Quand j'ai voulu restaurer, je me suis rendu compte que je n'avais pas sauvegardé les bons dossiers (c'est la faute au logiciel de sauvegarde)

Nous avons un super système de réplication synchrone vers un autre site ; tellement super, qu'un bug *MygreMSQL* s'est répercuté sur le site de secours en 3,5ms (c'est la faute à *MygreMSQL*)

LA VIE N'EST PAS UN LONG FLEUVE TRANQUILLE

Et alors, c'est grave docteur ?

Ça dépend des conséquences… Certaines données sont plus importantes que d'autres … Vous avez perdu quoi ?

- `StarWars-7-The_Force_Awakens-USDTSHDMA-FRAC3-Lost.mkv` : **aucune importance***

- `Réunion-20160326-compte_rendu.odt` : **gênant**

- `Univ Lille1-marché copieurs 2016-Cahier_des_charges.doc` : **saperlipopette ! 12 jours de boulot perdus, il va falloir tout refaire**

- `ma_these.doc` : **je suis très mal (surtout si elle fait 1257 pages)**

- `SIFAC-bases_de_donnees.mdf` : **l'Université est très mal**

*** : Sauf pour la MPAA**

LA VIE N'EST PAS UN LONG FLEUVE TRANQUILLE

Comment kon fait si on veut pas perdre ses données ?

Version *Canal*+ : ON MET EN ŒUVRE DES MÉCANISMES PERMETTANT DE SE PROTÉGER CONTRE LES PERTES DE DONNÉES

J'ai rien compris…

En clair : ON FAIT DES SAUVEGARDES ! (et accessoirement, des restaurations*…)

*** : Ne pas confondre Restauration Rapide et MacDonald's**

ON FAIT DES SAUVEGARDES

Aucune excuse pour ne pas en faire

« -Je manque de temps | d'argent | de motivation | de connaissances | de soutien | d'argument[1] pour faire des sauvegardes » **: <u>argument irrecevable !</u>**

- **➔ Le premier reproche que pourrait nous faire un utilisateur est de n'avoir pas protégé ses données**
- **➔ Mettre en œuvre des sauvegardes fait partie des « bonnes pratiques informatiques », autrement dit, des activités normales, régulières et obligatoires[2] d'un administrateur système ou d'un gestionnaire de parc**

1 : rayer les mentions inutiles
2 : ne rien rayer du tout

ON FAIT DES SAUVEGARDES
Bonnes pratiques

Détail des bonnes pratiques : norme *ISO 27002* et *PSSI-E*

***ISO 27002*, Code de bonne pratique pour la gestion de la sécurité de l'information, page 45, 10.5 Sauvegarde :**

« Objectif: maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.

Il convient de dresser des procédures de routine pour mettre en œuvre la politique et la stratégie de sauvegarde convenues stipulant de réaliser des copies de sauvegarde des données et de procéder à des répétitions pour que leur restauration puisse être effectuée en temps voulu. »

Règles de la *PSSI-E* : `PDT-STOCK, PDT-SAUV-LOC, PCA-LOCAL, PCA-SAUVE, PCA-PROT`

ON FAIT DES SAUVEGARDES
Bonnes pratiques

Bon, okay, okay, je vais faire des sauvegardes...

Merci de votre attention

QU'EST-CE QU'UNE BONNE SAUVEGARDE ?
Prévention des risques

Quitte à faire des sauvegardes, autant en faire des BONNES !

Une BONNE sauvegarde est une copie de données permettant de les protéger de (presque) TOUS les risques d'indisponibilité ou d'intégrité :

- **incendie,**
- **dégât des eaux,**
- **panne,**
- **vol,**
- **perte,**
- **bug de firmware, de driver, de logiciel,**
- **erreur de manipulation**
- **malveillance.**

QU'EST-CE QU'UNE BONNE SAUVEGARDE ?
Prévention des risques

Remarque : la décision de ne pas tenir compte d'un risque doit être prise par … les décideurs, en toute connaissance de cause :

- malveillance (interne ou externe) ?

- défaillance logicielle ?

- autres risques de probabilité plus faible* ?

*** : champ magnétique, éruption volcanique, tempête solaire, tremblement de terre, confusion entre les pistes de l'aéroport Lille-Lesquin et l'avenue Carl Gauss, dommages causés par la fission du noyau d'uranium, loi de Murphy, envoutement, etc…**

QU'EST-CE QU'UNE BONNE SAUVEGARDE ?
Respect du RPO / RTO

Une BONNE sauvegarde doit permettre de restaurer des données ayant une ancienneté acceptable (à vous de voir[1]) ; notion de « *Recovery Point Objective* » (*RPO*)

Une BONNE sauvegarde doit permettre de restaurer des données en un temps acceptable[2] (à vous de voir[1]) ; notion de « *Recovery Time Objective* » (*RTO*)

1 : Question souvent sans réponse : « où est votre tableau de *RTO/RPO* ? »
2 : Autrement dit, sans une trop longue interruption des services

QU'EST-CE QU'UNE BONNE SAUVEGARDE ?
MAUVAISE sauvegarde

à contrario, une MAUVAISE sauvegarde aurait les caractéristiques suivantes :

- absence de sauvegarde (aucune sauvegarde, sauvegarde volée, perdue, illisible, altérée),

OU

- trop veille copie de données (non respect du *RPO*),

OU

- trop longue durée de restauration (non respect du *RTO*).

QU'EST-CE QU'UNE BONNE SAUVEGARDE ?
RPO et *RTO*, c'est compliqué…

RTO **et** ***RPO*** **influencent les choix technologiques, la complexité et les coûts des mécanismes de sauvegarde**

Mais ***RTO*** **et** ***RPO*** **n'ont pas d'influence sur le but fondamental d'une sauvegarde (avoir une copie des données)**

➔ on n'en parlera pas aujourd'hui*

*** c'est déjà assez long comme ça (diplomatiquement correctement dit)**

REGLES FONDAMENTALES
(unique slide à retenir)

1) Avoir au moins une copie « hors-ligne » des données qu'on veut protéger, y compris pendant la sauvegarde ou une restauration

- automatisation totale impossible

2) Ne pas exposer toutes les copies aux mêmes risques physiques que les données de production (« primaires »)

- y compris aux risques de vol et de destruction volontaire

3) S'assurer régulièrement que les sauvegardes ont bien lieu

- par expérience : ne pas laisser l'utilisateur faire lui-même ses sauvegardes…

4) Effectuer régulièrement des tests de restauration !

REGLES FONDAMENTALES
(deuxième unique slide à retenir)

Remarque : les règles énoncées se rapprochent fortement de la règle usuelle du « *3-2-1* » (http://www.dpbestflow.org/backup/backup-overview)

La règle du *3-2-1* consiste à garder 3 exemplaires des données (y compris le jeu de données de production), sur 2 supports différents, dont 1 se trouve hors site

Avec « nos » règles, on cherche, de plus, à se prémunir du risque de malveillance (ex : rançongiciel, ou personnel un peu colérique) en conservant une copie hors-ligne (et pas seulement une copie sur un site distant)

REGLES FONDAMENTALES

Merci de votre attention

EXEMPLES
Ceci n'est pas une sauvegarde

Les mécanismes de redondance matérielle (*RAID 0*, *RAID 5*, *RAID 6*) ne sont pas des mécanismes de sauvegarde

- ne protègent que des pannes de disque dur, et encore, à condition de s'en rendre compte…

Les mécanismes de synchronisation AUTOMATIQUE (miroir de baies de stockage local ou distant, synchronisation par le réseau, « à la *rsync* » ou sur un *cloud*) ne sont pas des sauvegardes

- protègent des risques physiques et des pannes, mais pas des bug logiciels, ni des erreurs de manipulation (« `yes | rm -rf .` »), ni de la malveillance

Il serait peut-être temps que je sauvegarde ces slides…

EXEMPLES
Sauvegarde pas trop mauvaise

Copie ou synchronisation vers un dispositif « externe »
- disque dur, point de montage *NFS*, lecteur réseau, *Webdav*, *Cloud* (ex. service de *Backup HUBIC)*

MAIS, avec montage MANUEL de ce dispositif et démontage immédiat de ce dispositif à la fin de la sauvegarde

OU, avec montage automatique, mais avec un intervalle de temps entre chaque sauvegarde suffisamment long pour avoir le temps de se rendre compte d'une éventuelle altération des données de production

!! risque de perte des données de production et de la copie si un événement se produit pendant la sauvegarde (virus *cryptolocker*, mauvaise manip, ...) !!

EXEMPLES
Bonnes sauvegarde

Copie de copie :

1) copie sur un support amovible

2) si la copie s'est bien passée : copie de ce premier support amovible sur un deuxième support amovible A PARTIR D'UNE MACHINE N'AYANT PAS ACCES AUX DONNEES PRIMAIRES

3) stockage du deuxième support amovible dans un autre lieu, non soumis aux mêmes risques physiques que les données primaires

Copie en bascule :

- copie alternative sur deux supports amovibles

- stockage du support amovible le plus récent dans un autre lieu (permet de conserver deux versions des données, étalées dans le temps)

EXEMPLES

Très bonne sauvegarde (toute ressemblance, etc...)

Données de production sur site A et site B

1) sauvegardes quotidiennes sur site A (disque dur)

2) copie quotidienne de la sauvegarde, sur un stockage C1 situé au site B

3) vendredi : arrêt physique du stockage C1, démarrage d'un stockage C2 situé au site B

4) copie quotidienne de la sauvegarde, sur le stockage C2

5) vendredi J+7 : arrêt physique du stockage C2, démarrage du stockage C1

- boucle

*** Autrement dit : sauvegarde en local puis copie de la sauvegarde sur un autre site, sur deux stockages qui ne sont jamais en ligne en même temps**

EXEMPLES

Très bonne sauvegarde (toute ressemblance, etc...)

Scénarii + ou – catastrophe :

- perte d'une donnée de production : restauration à partir de la sauvegarde

- sinistre sur site B : restauration à partir de la sauvegarde (stockée sur site A)

- sinistre sur site A : restauration à partir de la copie de la sauvegarde, stockée sur site B (*RPO* max = 24h, RTO = long)

- malveillance détruisant tout ce qui est en ligne (ex : piratage d'un compte d'administration) : restauration à partir de la copie de la sauvegarde stockée sur le site B sur le serveur qui était hors-tension au moment du piratage (*RPO* : entre 24h et 7 jours)*

*** Et dépôt de plainte !**

DU CONCRET !

C'est bien beau tout ça, mais je fais quoi maintenant ?

Quels matériels ?

- disque dur *DAS*, *SAN*, *NAS*, *Virtual Tape Library*, bande magnétique, carte perforée ?

Quels logiciels (et quelles méthodes et fonctionnalités) ?

- *rsync*, *tar*, *robocopy*, *NTBackup*, *Bacula*, *Time Machine*, *Areca*, *VEEAM Endpoint Free*, *GHOST*, *Veeam Backup*, *Time Navigator*, … ?

Quel coûts ?

➔ Ce sera pour le tome 2*

*** un peu frustrant, non ?**

DES QUESTIONS ?
Cette fois, c'est vraiment fini