Backups: Presentació per a l'assignatura ASO-FIB 11/12/2006

Xavier Ramírez

Continguts

Introducció
Les dades

El centre de l'univers

Actualment, tot gira entorn de la informació i moltes vegades aquesta és el resultat del processament de dades emmagatzemades.
Les dades informàtiques en concret són una necessitat vital per a les empreses.

Tipus de dades

- Dades de les que tenim un backup i podem recuperar.
- Dades que *encara* no hem perdut.

Introducció
Per què fer backups?

Perill constant

Les dades informàtiques poden perdre's per vàries raons:

- Esborrat accidental
- Virus
- Accés malintencionat
- Avaria elèctrica/hardware
- Desastres naturals

Darreres paraules d'un ex-sysadmin

"Backups per a què? No necessitem aquesta despesa inútil"

Plans de contingència
Precedents

Estadística

Un estudi nord-americà afirma que un 20% de les empreses que pateix una pèrdua important de dades es veu obligada a tancar.

Atacs de l'11 de setembre de 2001

- Pèrdues milionàries a més de 10.000 empreses.
- Moltes van haver de tancar.
- Va quedar en evidència la manca de previsió davant una emergència.
- Les que tenien un bon pla, van restablir la seva activitat normal en menys d'una setmana.

Plans de contingència

Un pla de contingència o *Document Recovery Plan* encamina el curs d'acció d'una empresa davant possibles desastres que impliquin la pèrdua de dades.

Documents

- Emergència
- Backups
- Restabliment
- Simulació
- Manteniment

Plans de contingència
Emergència

Davant del desastre

- Indica les accions que s'han de prendre immediatament després del desastre.
- Diagrama d'organització amb gestor i principals coordinadors.
- Defineix clarament les responsabilitats de cadascun.

Plans de contingència
Backup

Polítiques de backup

- Element primordial i necessari per a la recuperació.
- Considerar totes les alternatives tecnològiques del moment.
- Quan fer els backups.
- Com fer-los.

Plans de contingència
Recuperació

Passos a seguir

- Establir capacitat real de recuperació d'informació crítica en un cert temps acceptable.
- Recursos necessaris per garantir un funcionament mínim.
- Identificar processos crítics.
- Ha de proporcionar els noms, telèfons, formació necessària i altra informació essencial.
- Indica responsables d'acció i contemplar recursos humans disponibles.

Plans de contingència
Simulació

A través de simulacres és possible detectar si els plans de contingència respecten els aspectes prioritaris requerits.

Verificació del pla

- Realitzar tests de forma periòdica.
- Programar simulacions de desastres reals.
- Permeten detectar problemes potencials.
- Els resultats són revisats per la gent que fa la simulació.
- Aquests resultats són la clau per identificar possibles defectes del pla de contingència.

Plans de contingència
Manteniment

Com en qualsevol cicle de desenvolupament d'un projecte existeix una fase de manteniment.

No oblidar

- Assegura la vigència del pla de contingència.
- Qualsevol canvi afegit es documenta basant-se en les simulacions.

Plans de contingència

Per concloure

L'existència d'un pla de contingència es considera un control de correcció. No tracta tant de preveure o detectar possibles desastres, sinó de minimitzar les pèrdues ocasionades.

- Els desastres succeeixen.
- Tenir un pla a l'empresa per poder recuperar les funcions d'una forma ràpida.
- Obliga a discernir processos crítics i no crítics.
- Garanteix així que la activitat crítica no es veurà aturada.

De què fer backups?

Totes les dades són importants en un sistema, però unes més que d'altres i per tant tenen prioritat en el moment de fer backups.

Important

- Fitxers de configuració
- Bases de dades
- Dades d'usuari
- Repositoris

Evitar fer backups de dades supèrflues com ara pel·lícules i música ens permetrà reduir el temps de backup i fer un millor ús de l'espai disponible.

On fer els backups?

Backup extern

Sempre s'ha de tenir com a mínim una còpia fora de la màquina de la qual estem fent el backup.

Dispositius

- Disquette/Pendrive
- CD/DVD
- Discs durs extraïbles (interfície S-ATA permet *Hot Swap*)
- Backups online
- Cintes (des de les antigues ZIP/Jazz fins les DLT/LTO)

Política de backups
Quan i com els fem

Generalment és suficient:

- Realitzar un backup complet cada setmana.
- Realitzar un backup incremental cada dia.

Avantatges

- Accelera molt els backups $\Rightarrow$ menys dades.
- Útil en cas de poques variacions.

Inconvenients

- Cada sessió depén de l'anterior fins al darrer backup complet.
- Major risc de perdre dades

Emmagatzemar backups

Un backup espatllat no serveix de res, per això hi ha algunes consideracions a tenir en compte.

Com tenir cura

- No guardar-los en la mateixa sala que les màquines.
- Guardar-los en un lloc protegit com ara caixes blindades especials (ignífugues i hidròfugues)
- Normes de manteniment del suport físic (allunyats de camps magnètics, etc)
- No deixar-los en llocs fàcilment accessibles $\Rightarrow$ tenen dades privades!

Eines de backup

Segons el volum de dades i el nombre de màquines de que volguem fer backups escollirem unes eines o altres.

Màquina local

- **dump:** Dels més antics i segons alguns *benchmarks* un dels millors.
- **tar.[gz|bz2]:** Empacador molt flexible.
- **rsync:** Utilitat per sincronitzar directoris que es trobin o no en la mateixa màquina.
- **rdiffbackup:** Usa *rdiff* (basat en *rsync*) per fer backups incrementals.
- **duplicity:** Backups remots encriptats (usa rdiff, tar i gnupg)

Eines de backup

Backup amb rsync i cron

```
frikjan@maelstrom ~ $ crontab -e

00 02 * * * rsync -r -e ssh --delete /home/frikjan/Uni user@outsideServer:backups/Uni
00 03 * * * rsync -r -e ssh --delete /etc/ user@outsideServer:backups/etc
```

Podem afegir ara una rotació de backups també usant el cron al servidor:

Rotació de backups

```
30 03 * * 7 cp -f ~/backups/2wUni.tar.bz2 ~/backups/3wUni.tar.bz2
35 03 * * 7 cp -f ~/backups/1wUni.tar.bz2 ~/backups/2wUni.tar.bz2
40 03 * * 7 cp -f ~/backups/1wUni.tar.bz2
45 03 * * 7 tar cjf ~/backups/1wUni.tar.bz2 ~/backups/Uni/
```

Eines de backup

Per a xarxes de mitjana/gran envergadura tenim 3 eines lliures de renom (de comercials n'hi ha moltes més)

Xarxa d'ordinadors

- **Bacula:** *It comes by night and sucks the vital essence from your computers*.
- **Amanda:** Advanced Maryland Automatic Network Disk Archiver
- **DIBS:** Distributed Internet Backup System

Eines de backup
Bacula

Catalogada com una de les millors eines lliures existents i equiparable (segons alguns) a les millors eines comercials.
El seu funcionament el controlen tres *daemons*:

- **Director:** Gestiona cada quan es fan els backups, a on, etc.
- **Storage daemon:** Gestiona els diferents dispositius.
- **File daemon:** Accés als fitxers.

Eines de backup
Bacula

Característiques principals

- Documentació molt bona i extensa.
- Instal·lació i configuració relativament senzilla.
- Backups a través de NFS i Samba.
- Programació de tasques.
- Suport per diferents SGBDs.
- Possibilitat d'encriptar els backups.
- i moltes més...

Eines de backup
Amanda

Un altre gestor de backups molt popular degut a la seva senzillesa i prestacions.

Característiques

- Usa utilitats del sistema com tar o dump.
- Backups contra robot de cintes i array de discs simultàniament.
- Si el SO suporta el dispositiu, Amanda també.
- Backups de sistemes Windows a través de Samba.
- Encriptació i compressió de dades.

Eines de backup
DIBS

Extensió del concepte de P2P (*Peer to peer*) al món dels backups.

Característiques

- NO és una xarxa de compartició de dades.
- Les dades i transmissions estan encriptades amb *GnuPG* per evitar violació de privacitat.
- El backup es distribueix a varis usuaris tal com passaria en *BitTorrent* i altres xarxes (redundància de dades). S'usen codis (*Reed-Solomon*) per garantir el màxim avantatge de la redundància. És similar al funcionament de sistemes RAID.

Conclusions

La majoria d'aspectes a tenir en compte alhora de fer backups són força evidents si hom usa el sentit comú.

Podem fer un símil amb una pòlissa d'assegurances, ningú no la vol usar però si algun dia ens passa alguna cosa, agraïrem les precaucions preses.

Fi

Torn de preguntes?