Seguretat passiva

Jordi Serra Ruiz

PID_00200499

Universitat Oberta de Catalunya

Índex

Introducció

La seguretat passiva és un dels aspectes més importants que cal tenir en compte a l'hora d'administrar o instal·lar un servidor, ja que, en principi, una vegada configurades les polítiques de seguretat passiva, no cal preocupar-se gaire del funcionament que tenen i, per tant, això fa que se n'oblidin fàcilment i si hi ha algun error o problema no ens en adonem fins que molts cops és massa tard. No obstant això, el fet d'haver d'estar constantment pendents de la seguretat passiva significa que les decisions preses a l'hora de configurar-la han estat errònies, i per tant realment no funciona correctament aquesta seguretat.

Per exemple, un cas típic és la caiguda de fluid elèctric. Per a solucionar aquest problema es pot decidir entre instal·lar un sistema d'alimentació ininterrompuda (SAI) o contractar una doble companyia de subministrament elèctric (així, en cas que falli una companyia es pot utilitzar l'altra) i fins i tot instal·lar dues fonts d'alimentació o més (la majoria dels fabricants de servidors ja tenen aquesta doble font d'alimentació en els equips).

Més endavant descriurem les polítiques de còpies de seguretat de les dades que hi ha en els equips informàtics: com s'ha de fer, quan i on. Tot això ho veurem en aquest mòdul.

Finalment, veurem els plans de risc, plans i documents en els quals descriurem l'actuació en el cas hipotètic que a l'empresa, i especialment a la sala on hi ha els servidors, hi hagi problemes. Mitjançant aquests plans aconseguirem mantenir els servidors en funcionament, o simplement fer una apagada segura de manera general de tots els serveis i servidors que té l'empresa.

Objectius

L'objectiu fixat per a aquest mòdul és que aprengueu a conèixer els diferents mètodes de seguretat passiva que hi ha. De manera més concreta, els objectius són els següents:

1. Conèixer els dispositius redundants que podem trobar en un ordinador: les fonts redundants, els discos i les targetes de xarxa.

2. Aprendre a dissenyar una bona política de còpies de seguretat o *backups*, tenint en compte la quantitat d'informació per a emmagatzemar, els dispositius que tenim a l'abast, el tipus d'informació de la qual volem fer una còpia de seguretat i la importància d'aquesta informació.

3. Conèixer i entendre què és un pla de risc i com ens pot ajudar en la seguretat de l'empresa en el dia a dia.

1. Elements redundants

Els elements redundants dels sistemes són els components que estan duplicats en la nostra màquina o fins i tot en la xarxa. Aquests elements que amb més freqüència estan duplicats són la font d'alimentació, els discos i les targetes de xarxa o comunicacions.

1.1. Fonts d'alimentació

La font d'alimentació és una part molt delicada de la nostra màquina. La xarxa elèctrica és susceptible de tenir pujades o baixades de tensió, les quals afecten sovint les fonts d'alimentació dels ordinadors i les danyen. Si nosaltres, com a administradors, som responsables d'un servidor d'alta disponibilitat, un servidor que ha de donar servei les vint-i-quatre hores i els set dies de la setmana (24 × 7), ens interessa que la màquina estigui en servei tot el temps que sigui possible. Una fallada en la font d'alimentació, malgrat que és una avaria molt ràpida de reparar, ens pot deixar sense servei. Cada cop més els servidors ja incorporen dos fonts d'alimentació, per la qual cosa la gestió d'aquesta característica se simplifica considerablement. Les fonts redundants es posen en funcionament quan detecten que la font principal no funciona. D'aquesta manera, el nostre servidor pot ser actiu mentre reparen la font danyada.

Cal tenir present que per a aconseguir un rendiment òptim de les fonts redundants és aconsellable tenir les dues fonts connectades a dues xarxes elèctriques diferents. D'aquesta manera, quan falla una de les xarxes, l'altra encara és operativa.

No sempre es pot aplicar la solució òptima, ja que en moltes ciutats només hi ha una empresa subministradora d'electricitat. En aquests casos, si tenim un SAI o un grup electrogen, podem tenir una font connectada als endolls que hi són compatibles, i l'altra, a la xarxa elèctrica normal. Així ens assegurem davant les possibles caigudes de la xarxa elèctrica o del SAI, tot i que aquestes caigudes es donen en molt pocs casos.

1.2. Discos

Uns altres components que molt sovint estan duplicats són els discos interns dels servidors. Aquest tipus de redundància es pot fer per programari o per maquinari, encara que és recomanable fer-ho via maquinari, ja que és més eficient. Des del punt de vista de la seguretat passiva, la redundància per maquinari dels discos és més robusta. Avui dia hi ha algunes marques d'ordinadors,

com per exemple HP, que venen unes bateries auxiliars per a les màquines que es connecten a la controladora per a assegurar la integritat dels discos davant una possible fallada elèctrica.

Si finalment optem per la redundància via maquinari, la nostra màquina ha de tenir una controladora de discos capaç de fer-la. Antigament, les úniques controladores capaces de fer redundància per maquinari de discos necessitaven que aquests discos fossin del tipus SCSI (interfície de sistema per a ordinadors petits o *small computer system interface*), més ràpids que els IDE (*integrated drive electronic*) a causa de la capacitat que tenen de treballar de manera asíncrona. Actualment, tot i que la majoria de les controladores continuen necessitant discos SCSI, en el mercat hi ha controladores capaces de fer redundància per maquinari que són compatibles amb IDE i sobretot ara amb els discos SATA (*serial at attachment*), molt més ràpids que els antics IDE i molt més barats que els SCSI, tot i que més lents.

En canvi, la redundància per programari no necessita cap controladora, ja que la còpia de la informació entre els diferents discos la fa un programa resident en memòria. Això fa que el sistema operatiu sigui més lent i les còpies siguin menys robustes a problemes elèctrics com baixades de tensió mentre es fa la còpia, però són molt més barates; en el cas de GNU/Linux són gratuïtes, i a més a més no tenen el principal i més greu problema que sí presenten les controladores maquinari: la compatibilitat entre controladores. En el cas de tenir una controladora maquinari que s'ha espatllat, caldrà canviar-la per una del mateix fabricant o fins i tot en molts casos del mateix model, per a poder recuperar la informació que hi ha guardada als discos, cosa que en molts casos obliga a comprar dues controladores maquinari per tenir aquest component duplicat. Evidentment, això no passa amb les controladores programari, ja que sempre es pot tornar a reinstal·lar el mateix sistema i les mateixes controladores de programari que es van instal·lar en el seu dia.

La redundància de discos s'anomena *RAID* (conjunt redundant de discos independents o *redundant array of independent –or inexpensive– disks*). Actualment hi ha molts administradors que recorren al RAID amb la intenció de prevenir la pèrdua d'informació, objectiu inassolible, d'altra banda, ja que hi pot ajudar, però no la pot prevenir. Per entendre per què, i ser capaços de planificar una estratègia de protecció d'informació més eficaç, primer hem d'entendre els diferents tipus de fallada que hi ha i com poden causar la pèrdua d'informació:

1) Esborrament accidental o intencionat de la informació: una de les causes principals de pèrdua d'informació és l'esborrament accidental o intencionat dels fitxers. Aquesta causa inclou des dels pirates informàtics o *hackers* dolents que han entrat al sistema, fins a l'error humà dels mateixos usuaris del domini. En aquest tipus de pèrdua d'informació la redundància de discos no ens pot

ajudar, ja que si s'elimina la informació de manera normal, desapareix també de tots els discos on es fa redundància. Per a mitigar aquest tipus de pèrdua és indispensable tenir una bona política de còpies de seguretat.

2) Fallada total o completa del disc: aquest tipus de pèrdua d'informació es produeix quan el capçal del disc s'incrusta en la superfície magnètica, o quan a causa d'una fallada elèctrica el disc queda danyat. En aquest tipus de pèrdua, la redundància de discos sí que ens és útil, ja que el RAID emmagatzema la informació encreuada en diferents discos i de manera redundant. Utilitzant el RAID pot ser que la fallada total d'un disc no produeixi cap pèrdua d'informació.

3) Pèrdua de fluid elèctric amb la corrupció de dades consegüent: hi ha qui pensa que pot verificar la tolerància a fallades provocant un treball intensiu del disc per a paralitzar després de sobte el subministrament elèctric. Aquesta acció normalment causa algun tipus de corrupció de la informació i no aconsegueix l'efecte que es volia. La redundància de disc no ens pot ajudar en el cas de corrupció de la informació. Aquest tipus de pèrdua o corrupció de la informació es pot evitar utilitzant sistemes de fitxers que siguin compatibles amb el *journaling*. A manera de recordatori direm que són els sistemes que porten un diari o *journal* en què s'anoten tots els accessos als discos (a quins blocs s'accedeix i quina informació es modifica).

4) Sectors defectuosos en un disc: la fallada més comuna dels discos és la pèrdua lenta però estable de blocs en el disc. Quan un sector està danyat no podem llegir la informació que contenia. Els sectors defectuosos són inevitables en un disc; de fet, un disc acabat de sortir de fàbrica pot contenir centenars (fins i tot milers) de blocs danyats. Actualment les controladores de discos poden detectar un bloc danyat i reassignar en lloc seu un nou bloc "sa". Tots els accessos subsegüents que fa el sistema operatiu a aquest sector són, de manera transparent, redireccionats. Aquest comportament a la llarga és perjudicial, ja que tots els blocs van fallant lentament, a causa dels salts del capçal sobre la superfície magnètica del disc. Arriba un moment en què la taula de blocs erronis és plena; llavors els blocs erronis es fan visibles al sistema operatiu. Tot i que aquesta fallada és la més comuna d'un disc, és, per desgràcia, la que té menys solucions. La redundància de disc en aquest cas tampoc no ens pot ajudar. Arribats a aquest punt, només podem fer que el sistema operatiu marqui tots els blocs danyats, però es tracta d'una operació molt lenta (en discos de 160 GB pot trigar un dia sencer) i s'ha d'executar sobre els discos desmuntats i només amb els que no formin part de cap dispositiu RAID ni LVM (volum lògic o *logical volume*).

5) Corrupció general del sistema: aquesta fallada es deu a la complicada regressió d'un sistema cap al caos total, que tard o d'hora fa que s'hagi de reinstal·lar el sistema. Com que els errors o *bugs* en el sistema operatiu, la base de dades o les aplicacions, més l'acumulació lenta d'informació corrupta, fan que un sistema es torni inutilitzable, no es pot fer gran cosa en aquests casos excepte evitar per tots els mitjans posar serveis crítics en màquines amb sistemes o

programari beta. Malauradament, encara que es facin còpies de seguretat de manera regular, és molt possible que aquests serveis hagin fet còpies de dades corruptes. En les versions més modernes de Windows i de la majoria de les versions GNU/Linux, aquest fenomen s'ha eradicat gairebé del tot. Fixem-nos que aquest tipus de corrupció del sistema també es pot deure a un maquinari en mal estat o mal connectat, o a un entorn amb molt soroll elèctric. Amb la corrupció total d'un sistema no hi ha cap estratègia que ens pugui ajudar a minimitzar les pèrdues.

Hi ha moltes maneres d'implementar el RAID, la majoria de les quans són una combinació de les tecnologies de duplicat, fraccionament i paritat (*mirroring, striping i parity*). El 1988 es van estandarditzar alguns mètodes. Els investigadors encarregats d'aquesta estandardització van anomenar *nivells* (*levels*) cadascun d'aquests mètodes d'estandardització. Aquesta elecció va ser una mica desafortunada, ja que la paraula *nivell* té connotacions de jerarquia, és a dir, sembla que indica que per a aconseguir un determinat nivell de RAID hem de fer tots els nivells inferiors, cosa que, en realitat, no passa. La utilització de la paraula *nivell* també té implícit, per a molta gent, que el nivell de RAID N +1 és millor que el nivell RAID N, cosa que és absolutament falsa. Els nivells en RAID són completament independents els uns dels altres, i cadascun està pensat per a donar solucions en àmbits diferents. Per tant, segons quina sigui la nostra necessitat utilitzarem un nivell de RAID o un altre.

Al començament el RAID definia cinc nivells i després se n'hi van afegir d'altres. Més endavant, a partir d'aquests nivells simples també es van definir diversos nivells múltiples, en els quals s'usava una combinació de dos nivells simples o més, per a crear nous nivells amb noves capacitats i limitacions. Molts d'aquests nivells de RAID avui dia encara estan en ús. Alguns nivells de RAID, tant si són simples com múltiples, han caigut en l'oblit perquè amb el temps s'ha demostrat que són inferiors a la resta de nivells, ja que no compensa els pocs avantatges que tenen. En aquesta secció veurem els trets principals dels diferents nivells de RAID. Hem de destacar que els nivells simples són molt més freqüents i populars que els nivells múltiples, perquè són més barats i més simples d'implementar i perquè, en general, ja satisfan la majoria dels usuaris. Només hi ha algunes aplicacions molt particulars que requereixen l'ús dels nivells múltiples de RAID. Hi ha vuit nivells simples de RAID, els més populars dels quals són el RAID 0, el RAID 1 i el RAID 5.

- **RAID 0**. Per a fer aquest nivell cal tenir com a mínim dos discos. Les característiques d'aquest nivell són les següents: utilitza la tecnologia coneguda com a *fraccionament*, que divideix les dades en diverses parts (tantes com discos tingui) i emmagatzema la informació en tots els discos alhora, és a dir, hi accedeix simultàniament; té un temps d'accés de lectura i escriptura molt ràpid; la velocitat de transferència augmenta segons el nombre de discos que tenim; no fa cap redundància d'informació i, per tant, no té cap tolerància a fallades.

- **RAID 1**. Per a fer aquest nivell cal tenir com a mínim dos discos. Aquest tipus de RAID és conegut com a *rèplica* (*mirror*), ja que escriu de manera simultània en els dos discos, de manera que quan falla un l'altre continua funcionant fins que puguem reparar el que està danyat. Aquest nivell, a causa de l'ús de la rèplica (*mirroring*), té una tolerància a fallades molt bona. L'inconvenient és el baix percentatge d'emmagatzematge que té (50%); és a dir, de la capacitat d'emmagatzematge total (dos discos), de manera efectiva només en tenim un.

- **RAID 2**. Aquest nivell és un dels que no es fan servir avui dia, per diverses raons: la gran complexitat que té, el cost elevat i la necessitat d'haver de tenir molts discos per a treballar. A més, aquest nivell utilitzava una tècnica no estàndard de RAID (rèplica, fraccionament i paritat), ja que es basava en un fraccionament de bit amb codificació de Hamming, que és una tècnica utilitzada comunament per a detectar i corregir errors en memòries d'estat sòlid. En un RAID de nivell 2, l'ECC (codi corrector d'errors o *error correction code*) s'intercala mitjançant diversos discos a escala de bit.

- **RAID 3**. Aquest nivell requereix com a mínim tres discos, que han de tenir les mateixes característiques i capacitat. El RAID de nivell 3 dedica un únic disc a emmagatzemar la informació de paritat. Fa servir una tècnica de fraccionament a escala de byte amb paritat dedicada i accedeix a tots els discos de manera simultània. Com que té un accés síncron als discos, no és recomanable fer servir aquest nivell en màquines multiusuari. La tolerància a fallades del RAID de nivell 3 és bona, ja que permet la caiguda d'un dels discos. Pel que fa a la taxa d'emmagatzematge, depèn del nombre de discos utilitzats. Si N és el nombre de discos, la taxa és de $N - 1/N$.

- **RAID 4**. Aquest nivell de RAID requereix, igual que el nivell 3, tres discos iguals. Fa servir una tècnica de fraccionament a escala de bloc amb paritat dedicada. Aquest nivell és molt semblant al nivell 3. La gran diferència és que accedeix als discos de manera independent. El RAID 4 és especialment apropiat per a emmagatzemar fitxers d'una mida molt gran, cosa que fa que sigui molt adequat per a aplicacions gràfiques. La tolerància a fallades és bona, ja que pot funcionar amb la caiguda d'un dels discos que té. La taxa d'emmagatzematge, igual que en el RAID de nivell 3, és de $N - 1/N$.

- **RAID 5**. Aquest nivell funciona igual que el nivell 4 però amb la paritat distribuïda, és a dir, cadascun dels discos que formen aquest RAID conté alhora informació i paritat. Aquesta característica el fa molt més eficient que el RAID 4, ja que elimina el coll d'ampolla que es crea en aquest RAID 4 (tots els accessos a disc requereixen llegir del disc de paritat). Aquest nivell de RAID és el més eficaç, el que té una relació rendiment-cost més bona i el més indicat per a treballar en entorns multiusuari. Igual que en els dos casos anteriors, requereix com a mínim tres discos, tolera la caiguda d'un disc i la taxa d'emmagatzematge és de $N - 1/N$.

- **RAID 6**. Aquest nivell demana com a mínim quatre discos. Utilitza la mateixa tècnica que el de nivell 5 però amb redundància distribuïda de paritat (a diferència dels nivells anteriors, que només tenien redundància d'informació). La tolerància a fallades és excel·lent, ja que admet la caiguda simultània de fins a dos discos. La taxa d'emmagatzematge, com que té redundància de paritat, disminueix en comparació de nivells anteriors i la situa a $N – 2/N$. Actualment aquest nivell de RAID s'utilitza poc, perquè el cost d'implantació que té és més alt que el d'altres nivells de RAID, ja que les controladores que fan falta són més complexes i, per tant, més cares que les d'altres nivells.

- **RAID 7**. A diferència dels altres nivells, no és un estàndard obert a la indústria. El nivell 7 no és més que una marca registrada per Storage Computer Corporation per a descriure'n el disseny de propietat.

Els nivells de RAID múltiple es fan servir per a millorar les característiques dels nivells de RAID simples que el formen. El nivell simple més combinat és el RAID 0, el qual s'uneix sovint amb els nivells redundants, com el nivell 1, 3 i 5. No hi ha totes les combinacions possibles entre nivells, cosa que és lògica, ja que la combinació pretén suplir els desavantatges d'un nivell amb els avantatges d'un altre. A més, no tindria sentit unir, per exemple, els nivells 4 i 5, ja que s'assemblen molt.

Abans de tractar amb deteniment cadascun dels nivells, hem de saber unes quantes coses sobre els nivells múltiples de RAID. Un nivell múltiple es crea dividint els discos en volums. A cadascun dels volums s'aplica un nivell simple de RAID i després un segon nivell entre els diferents volums per a crear un RAID de nivell superior. Per aquest motiu, a vegades, quan es parla d'aquest tipus de configuracions, es diu que són RAID imbricats.

Com que hi ha dos nivells, hi ha dues maneres de combinar-los, podem fer RAID X+Y o RAID Y+X. L'elecció del nivell que s'aplica primer i el que s'aplica després només afecta directament la tolerància a fallades del RAID resultant, ja que les característiques dels requisits dels controladors, la capacitat d'emmagatzematge, l'eficiència d'emmagatzematge i el funcionament són iguals en tots dos casos.

Aquesta diferència en la tolerància a fallades es veu molt més clara amb un exemple. Imaginem-nos que volem aplicar el RAID 0 i el RAID 1 sobre una màquina amb deu discos:

- Si fem servir RAID 0 primer (RAID 0+1), creem dos volums de cinc discos cadascun. Els discos 1, 2, 3, 4 i 5 formen el primer volum, que anomenem *A*, i els discos 6, 7, 8, 9 i 10 formen el segon, que anomenem *B*. Apliquem RAID 0 a cadascun dels volums (A i B) i després apliquem RAID 1 entre A i B. Ara imaginem-nos que falla el disc #2: tot el volum A queda danyat. Mentre es repara el disc #2 només ens queda B amb RAID 0; per tant, sense

redundància. Si falla qualsevol disc del volum B (per exemple, #9), perdem tota la informació.

- Si fem servir RAID 1 primer (RAID 1+0), creem cinc volums de dos discos. Els discos 1 i 2 formen el volum A; els discos 3 i 4, el B; els discos 5 i 6, el C; els discos 7 i 8, el D; i els discos 9 i 10, l'E. Apliquem RAID 1 a cada volum. Després apliquem RAID 0 entre A, B, C, D i E. Ara imaginem-nos que falla el disc #2: el volum A continua funcionant amb el disc #1 i el RAID 0 entre volums també continua funcionant. Ara imaginem-nos que també falla el disc #9: el volum E continua funcionant amb el disc #10; per tant, el RAID 0 continua funcionant.

El RAID 1+0 és molt més robust que el RAID 0+1, ja que el primer podria suportar una caiguda de fins a cinc discos, sempre que es trobin en volums diferents, mentre que en el segon, si cauen dos discos (un de cada volum), perdem tota la informació. El mateix efecte de la tolerància també s'aplica a la reconstrucció (*rebuild*) del RAID. No és el mateix reconstruir un volum de cinc discos (RAID 0+1) que reconstruir un únic disc (és el cas del RAID 1+0, en què només reparem el disc #2). Això s'ha de tenir molt en compte, ja que la regeneració d'un RAID, quan un dels discos que ha deixat de funcionar s'ha hagut de substituir per un de nou, és molt costosa en temps, poden passar moltes hores fins que es regenera un RAID d'algunes gigues.

Vegem a continuació quin tipus de nivells múltiples de RAID ens podem trobar:

- **RAID 0+1 o 1+0**. És el RAID múltiple més popular, ja que combina la rapidesa del RAID 0 amb la redundància del RAID 1. El desavantatge principal que té és que requereix com a mínim quatre discos, dels quals només n'hi ha dos que són per a emmagatzemar informació. Un altre desavantatge és que si volem augmentar de capacitat s'hi han d'afegir discos per parelles (de dos en dos), cosa que duplica el cost. Aquest nivell RAID és molt adequat en entorns de gran rendiment, amb tolerància a fallades però sense gaire necessitat de capacitat d'emmagatzematge. El RAID 1+0 és el més ràpid i segur de tots els nivells RAID, però també el més costós d'implementar.

- **RAID 0+3 o 3+0**. Utilitza la fracció a escala de byte amb la paritat dedicada i amb el fraccionament de bloc. El RAID 3+0 és més comú que el RAID 0+3. Aquest nivell de RAID dóna un rendiment més bo que el RAID 3, gràcies a les propietats de rapidesa del RAID 0, però és més a prop del rendiment del RAID 3 que no pas al que ofereix el RAID 0. El RAID 3+0 proporciona més bon rendiment de reconstrucció dels discos i més bona tolerància a fallades que el RAID 0+3, però en tots dos casos aquests factors depenen de la mida del RAID 3 en proporció al RAID 0. Aquest nivell és un dels menys utilitzats.

- **RAID 0+5 o 5+0**. Combina el fraccionament a escala de bloc amb paritat distribuïda del RAID 5 amb el fraccionament del RAID 0. El RAID 5+0 és més comú que el RAID 0+5. Tots dos casos milloren el rendiment i la tolerància a fallades que ofereix el RAID 5, especialment el RAID 5+0. Moltes de les característiques del RAID 5+0 són semblants al RAID 3+0. Aquest nivell és més preferible que el RAID 3+0 en entorns de transaccions, en què els fitxers són més petits. El nombre mínim de discos necessaris per a aquest nivell és de sis. Per això aquest nivell és molt complex i difícil d'implantar.

- **RAID 1+5 o 5+1**. Aquest nivell ofereix, sens dubte, la millor tolerància a fallades de tots els nivells RAID, fruit de la unió dels dos mètodes de RAID que ofereixen redundància (rèplica i paritat). Aquests dos nivells RAID (1+5 i 5+1) són molt semblants als nivells RAID 1+0 i RAID 0+1, però amb paritat distribuïda. Aquest nivell requereix com a mínim sis discos, i tots iguals. El cost d'aquesta implantació és molt alt, ja que necessita molts discos per a fer servir una capacitat d'emmagatzematge relativament baixa. Els grans desavantatges que té són el cost elevat i la complexitat. Aquests últims nivells de RAID múltiple són molt tolerants a fallades, però abans d'implantar-los podem buscar una altra mena de solucions basades en clústers o servidors redundants i implantar un nivell RAID 1+0, que ofereix molts dels beneficis d'aquests nivells amb un rendiment més bo i un preu més baix.

Pel que fa a la seguretat, tots els nivells RAID que ofereixen tolerància a fallades són bons nivells, però, entre aquests nivells, els més bons, pel preu i el rendiment que tenen, són RAID 1, RAID 5 i RAID 10. En general triarem un d'aquests tres segons les característiques de l'entorn i les necessitats del servidor. El cost també és un factor determinant en els nivells de seguretat que volem obtenir.

Per a instal·lar el RAID, en mode maquinari, en els entorns Windows generalment es força transparent i s'encarrega la pròpia controladora de gestionar tot. Però en sistemes GNU/Linux cal compilar el nucli o *kernel* si no ve per defecte aquest suport, tot i que en les darrers versions ja ho tenen en compte. D'una banda, hem de seleccionar el tipus de maquinari de què disposem per a fer RAID. Per fer-ho, hem de seleccionar les opcions següents en el nucli:

```
SCSI Support
[*] SCSI Support
SCSI low-level Drivers
Seleccionar el nostre maquinari
```

D'altra banda, hem de seleccionar quin tipus de RAID volem, mitjançant la configuració següent en el nucli:

```
Multi-device Support (RAID LVM)
```

```
[*] Multi-device Support
[*] RAID Support
[*] RAID Level 5
```

Una vegada hem seleccionat aquestes opcions en el nucli, ja el podem compilar i instal·lar. Normalment la configuració del RAID es fa des d'un programa que gestiona la controladora de disc, aplicació que està integrada en la mateixa targeta de la controladora. Per a accedir a aquest programa en el moment d'arrencada (després de la configuració del BIOS), ens surt un missatge que ens indica que si volem entrar a la configuració de la targeta RAID hem de prémer (normalment) Alt + F3. Aquesta consola interactiva ens permet crear volums, reconstruir-los o esborrar-los. A més, podem seleccionar el nivell RAID que volem que tingui cada volum.

1.3. Dispositius de xarxa

Tenir unes quantes targetes de xarxa no vol dir tenir targetes de xarxa redundants, ja que per necessitats del servidor és possible tenir una màquina connectada a diverses xarxes. Per exemple, un servidor que faci de servidor intermediari (*proxy*) de l'accés a Internet, necessitarà dues targetes de xarxa, una per a escoltar la xarxa interna de l'empresa i una altra per a la connexió a Internet; el mateix passa en els servidors que es dediquen a fer de tallafoc (*firewall*) de programari de tota la empresa: filtrarà el contingut que passa des d'Internet cap a la xarxa local i al revés. La redundància de targetes de xarxa, per tant, s'aconsegueix mitjançant un programari específic que gestiona una única connexió a la xarxa local. La finalitat d'aquesta redundància en les targetes de xarxa es deu, principalment, a dos motius:

- Tenir una targeta de còpia de seguretat per si la targeta principal falla. Aquesta solució, però, malgrat que té un cost molt baix, només ens prevé si falla la targeta de xarxa. Però, què passa si falla l'equip de comunicacions instal·lat a la xarxa local? Com que tenim dues targetes, podem connectar la secundària a un segon equip de comunicacions, una altra xarxa diferent de la principal; d'aquesta manera no solament ens protegim davant la fallada de la targeta de xarxa, sinó també davant la fallada de l'equip de comunicacions de la xarxa local. Ara bé, què passaria si el que falla és el nostre proveïdor d'Internet (ISP)? Llavors, aprofitant que tenim un segon equip de comunicacions, podem contractar un segon ISP. Com veiem, hi ha moltes opcions de redundància de xarxa. Com més ens protegim, però, més augmenta el cost de la implantació. S'ha d'arribar a un compromís de cost-seguretat amb el qual n'hi hagi prou per a satisfer les nostres necessitats reals. S'hauria de fer un estudi detalla de com és l'empresa i a què es dedica, per a saber si és important o no tenir aquest segon ISP redundant. Si només tenim una pàgina web per a fer publicitat de l'empresa, no cal tenir un ISP redundant. Si l'empresa es dedica al comerç electrònic, llavors

sí que és convenient tenir un proveïdor d'Internet redundant, perquè perdem diners per cada hora que estem sense connexió.

- Una altra raó per a tenir redundància de targeta de xarxa és per motius de balanceig de càrrega. Si tenim dues targetes a la mateixa xarxa que ofereixen els mateixos serveis amb balanceig de càrrega, podem atendre el doble de peticions de la xarxa local de manera simultània, és a dir, que totes les peticions que van de la xarxa local, dels ordinadors client de l'empresa cap al servidor, per recuperar fitxers, autenticar-se, resolució de noms, actualitzacions, etc. seran molt més ràpides perquè tenen doblat l'accés al servidor. Però si només es disposa d'una única sortida cap a la xarxa Internet, un sol IPS, l'augment de velocitat no es veurà incrementat en l'accés a Internet, ja que si la línia de sortida de l'ISP és un ADSL –o cable– a 20 Mbps i tenim dues targetes de xarxa de 1.000 MBps, és clar que el coll d'ampolla serà aquesta sortida a Internet. Per tant, amb aquesta configuració no té sentit tenir una targeta redundada amb balanceig de càrrega (tret que tinguem molt trànsit intern a l'empresa amb molts accessos a la nostra intranet que facin millorar molt el rendiment de les comunicacions internes).

2. Polítiques de còpies de seguretat

Hi ha un principi bàsic que com a administradors o caps de seguretat hem de tenir sempre molt present: els discos fallen. Actualment és difícil trobar un administrador de sistemes que no s'hagi vist involucrat en la pèrdua d'un disc. Per a això només hi ha una solució possible: fer una còpia de seguretat.

La majoria de vegades en què hi ha una pèrdua d'informació guardada en un disc es deu al fet que no s'ha planificat mai que aquestes dades s'havien de copiar i tenir guardades en un altre sistema per a recuperar-les després. La decisió de si s'ha de fer una còpia de seguretat o no és prou important per a no prendre-se-la a la lleugera. Per tant, en certa manera, quan planifiquem estem decidint de quines dades es farà la còpia de seguretat i de quines no: estem assumint quines dades estem disposats a perdre, ja que no les tindrem en cas de pèrdua d'informació.

Això no solament passa en l'àmbit empresarial: hi ha un estudi fet als Estats Units encarregat per l'empresa de discos durs Seagate el maig del 2012 en què el 54% dels enquestats van reconèixer haver perdut dades, ja siguin documents o fotografies digitals, que ja no poden recuperar. Però només l'11% de les persones a les quals es va fer l'enquesta reconeixen tenir un pla de còpies de seguretat de les dades en general a casa seva.

En la planificació de les dades de les quals es farà una còpia de seguretat no solament hem de preveure les dels usuaris, sinó també els arxius de configuració, les bases de dades, les biblioteques importants i tota la informació que sigui útil per a la nostra empresa.

Quan sabem quines són les dades que volem guardar en una còpia de seguretat, hem de decidir quan s'ha de fer aquesta còpia. Hi ha dades (les d'usuaris, per exemple) que cada dia tenen canvis; n'hi ha d'altres que canvien molt més a poc a poc, i, finalment, hi ha biblioteques i arxius de configuració que pot ser que no canviïn durant tota la vida útil de la nostra màquina, de manera que hem de determinar la freqüència de còpia de seguretat de cadascuna d'aquestes dades. Quan tenim tota aquesta informació podem començar a planificar les còpies de seguretat. Per a fer-ho, primer hem de saber els diferents nivells de còpies de seguretat que hi ha:

Nivell 0. Aquest nivell és conegut com a *còpia de seguretat total*. Fa còpia de totes les dades, marcades per a guardar, que hi ha dins de les particions o dels discos on es fa la còpia de seguretat. Aquest tipus de còpia sol tenir, depenent de la quantitat de dades que hi hagi, un cost temporal molt alt. És a dir, pot trigar força dies a fer-se.

Nivell 1-9. La majoria de les eines comercials designen aquests nivells amb un únic nom: incremental. Aquests nivells consisteixen a guardar només les dades que s'han modificat des de l'última còpia de seguretat total o de nivell inferior (per exemple, un incremental de nivell 2 fa una còpia de les dades que s'han modificat respecte a l'última còpia de nivell 0 i a l'última de nivell 1). Aquesta manera d'imbricar la informació la veurem molt més clara amb un exemple:

> Imaginem-nos que cada dissabte a la nit es fa una còpia de seguretat total de totes les carpetes i arxius del servidor i dilluns a la nit, el dia laborable següent, es fa una còpia incremental de nivell 1, és a dir, es copia tot el que s'ha modificat durant el dia. Què es pot fer dimarts a la nit? Si fem un incremental de nivell 1, copiem totes les dades que s'han modificat dimarts i dilluns, independentment que aquestes darreres dades s'hagin modificat dimarts o no, és a dir, es tornen a copiar totes les dades que s'han modificat des de dissabte. Si, al contrari, es fa un incremental de nivell 2, només es copien les dades modificades dimarts, i d'aquesta manera s'ocupa menys espai en el disc dur, ja que les dades modificades dilluns ja s'han guardat el dia anterior. En el cas d'haver de recuperar tots els sistema de fitxers, s'haurà de passar per totes les còpies diàries, ja que no n'hi haurà una on sigui tot el que s'ha modificat des de dissabte. El procés de recuperació de les dades és més lent, sobretot si no se sap quin dia s'ha fet la darrera modificació del fitxer que es vol recuperar.

En la majoria de les eines comercials de còpia de seguretat trobem el terme *diferencial*, amb el qual es designa de manera genèrica un tipus de còpia de seguretat incremental que fa còpies només de les dades que han canviat des de l'últim diferencial. Es tracta d'un incremental que no té en compte els nivells.

En aquest tipus d'eines comercials només es designen tres tipus de còpies: total, incremental i diferencial. La recomanació és una còpia total a la setmana, una còpia diferencial cada nit –en què es reflectiran els canvis que s'han produït al llarg d'aquell dia– i una còpia incremental només en els casos en què ens interessin els canvis que hi ha hagut des de l'última còpia total.

Un altre factor que hem de tenir en compte per a planificar la còpia de seguretat és el temps que triga a fer-la. En les totals es fa una còpia de totes les dades, tant si s'han modificat l'última setmana com si no. Per tant, si el disc és molt gran podem trigar moltes hores abans que no s'acabi. Per exemple, una còpia del disc d'usuaris de 500 GB pot trigar hores. Fem uns petits càlculs:

Si tenim un disc de dades amb tota la informació de la qual s'han de fer còpies de seguretat (per exemple, els discos d'usuaris, la comptabilitat, la pàgina web, els registres o *logs*, les configuracions del sistema, etc.) que ocupa uns 500 GB i disposem d'un disc dur SATA2 que té una transferència de dades de 300 MB/s, es trigarà 27 minuts a llegir aquestes dades, i 27 minuts més a guardar-les en un altre disc dur de les mateixes característiques. En cas que es guardessin en una cinta magnètica DLT (*digital line tape*) a 60 MB/s trigarien 2,3 hores a gravar-se, i el mateix que si féssim servir dispositius USB 2.0. En canvi, si la còpia es fa sobre un altre dispositiu que és a la xarxa i, per tant, les dades s'han de transmetre per una xarxa Ethernet a 100 Mb/s, trigaríem 11 hores a transmetre-les, amb la qual cosa col·lapsaríem la xarxa si es fa en un horari

laborable. En el cas de tenir una xarxa de comunicacions que funcioni a gigabits, aquestes 11 hores es converteixen en una hora, cosa que fa que la inversió valgui la pena perquè alleugereix la xarxa.

Per tant, és aconsellable fer aquests números abans de configurar quan es fan i com les còpies, ja que podem saturar el servidor o la xarxa en el moment de fer-les. Si arran dels resultats considerem que s'han de fer sobre un altre servidor, hem de tenir en compte que les dades han d'anar xifrades per la xarxa si surten de la nostra empresa, i això comporta un temps afegit de còmput de temps i més temps en la transmissió per la xarxa Internet, ja que no és la mateixa que hem vist fins ara.

Una vegada tenim totes aquestes dades, hem de planificar les còpies de seguretat. A continuació mostrem algunes de les planificacions més usuals que es fan.

- Total cada dia. És una planificació que només fem si el volum d'informació del qual volem fer la còpia és prou petit perquè es faci a la nit.

- Total setmanal i incremental (nivell 1) diari. L'avantatge principal d'aquest mètode és que només calen dos volums per a recuperar tota la informació. Això es deu al fet que cada dia es fa una còpia de seguretat de les modificacions que s'han produït al llarg de la setmana. Aquest tipus de política és la més recomanable si fem servir les utilitats simples de còpia de seguretat (`cpio`, `tar`, `dump`, `amanda`, `rdiff-backup` –entre d'altres– en GNU/Linux, i Windows Server Backup en Windows, que veurem més endavant). L'inconvenient, però, és que fem una còpia de seguretat de dades innecessàries. Imaginem-nos que un arxiu es modifica només el dilluns: al llarg de tota la setmana farem còpies de seguretat de manera innecessària d'aquest arxiu.

- Total setmanal, diferencial diari. L'avantatge principal d'aquest mètode és que les còpies de seguretat diàries són molt petites i, per tant, més ràpides. L'inconvenient més important és que si volem recuperar alguna cosa el divendres necessitem sis volums. Si fem servir eines comercials, aquest desavantatge es minimitza, ja que la majoria d'aquestes eines incorporen un sistema de gestió dels volums.

- Hi ha també altres filosofies de còpies de seguretat incrementals que treballen amb les progressions matemàtiques (sobretot l'anomenada *torre de Hanoi*). Mitjançant aquestes progressions es fan cada dia còpies de seguretat incrementals de diferents nivells (per exemple: 0, 3, 2, 5, 4, 7, 8, 9 i 1); amb això, aconseguim optimitzar el nombre de cintes en ús, optimitzar el temps de la còpia de seguretat i fins i tot arribar a fer una única còpia total al mes.

Les polítiques de còpies de seguretat que hem comentat no són les úniques. Se'n pot dissenyar una que s'ajusti més a les necessitats específiques de cada cas, segons el volum d'informació i de la freqüència de canvis que tinguem a l'empresa. Ara bé, cal tenir present que no hi haurà mai prou còpies de seguretat per a satisfer els usuaris. Per exemple, si falla el sistema un dimecres a la tarda, totes les dades modificades al llarg del matí no estan reflectides en cap còpia de seguretat. Una possible solució a aquest problema és l'ús de discos redundants (RAID). Si la fallada s'ha produït a l'ordinador de l'usuari, segurament no hi tindrem els discos redundats; per tant, és important oferir als usuaris unitats de treball remotes (unitats de xarxa), situades en el servidor, en les quals puguin guardar els documents.

Dins de les polítiques de còpies de seguretat hi ha un altre factor que s'ha de tenir en compte: durant quant temps estem disposats a guardar la còpia de seguretat? Si només utilitzem una única cinta (CD o dispositiu físic on es fan les còpies) per a cada dia, vol dir que si un usuari no s'adona que ha perdut alguna cosa abans d'una setmana ja no la podrem recuperar. Si guardem les cintes (o CD o DVD) durant més temps, en necessitarem moltes més. Caldrà un joc de set cintes per a cada setmana de més que decidim guardar.

Un altre factor que s'ha de tenir en compte és l'etiquetatge dels dispositius de còpia. Imaginem-nos que volem guardar les còpies de seguretat durant un mes. Això fa que tinguem quatre jocs complets de cintes, un per cada setmana. Hem de tenir molt clar quina cinta s'ha de posar cada dia de la setmana i no confondre cintes del mateix dia de la setmana però de setmanes diferents. Per tant, l'etiquetatge dels suports físics és molt important per a no perdre informació (en cas de posar una cinta que no toca) o per a recuperar de pressa la informació que necessitem.

Una vegada tinguem definida la política de còpies de seguretat i n'hàgim fet la primera, és hora de verificar que funciona correctament. No serveix de res fer còpies de seguretat si no hem comprovat que en podem recuperar la informació. Per a això, una vegada feta la primera còpia de seguretat intentarem recuperar informació. Per a no interferir en el funcionament del servidor utilitzem la funcionalitat que ens ofereixen les eines de còpies de seguretat per a recuperar dades en un directori diferent d'aquell en què es va fer la còpia. Per exemple, les dades de `/home/user` es poden recuperar a `/tmp/home/user` en el cas de GNU/Linux. D'aquesta manera es comprova que la còpia de seguretat funciona sense modificar les dades que hi ha en el nostre directori arrel.

Després de comprovar que les còpies de seguretat funcionen correctament, és a dir, que es poden recuperar tant els fitxers individuals com els discos sencers, ja podem començar a fer les còpies segons la política que hem definit.

2.1. Eines de còpies de seguretat en el GNU/Linux

En les distribucions estàndard del GNU/Linux trobem unes quantes eines molt bàsiques que ens poden ajudar a dur a terme una còpia de seguretat: són `dump`, `cpio`, `amanda` i `tar`. Aquestes eines tenen bastantes limitacions, però l'avantatge és que no representen cap cost econòmic addicional i són força fàcils d'instal·lar i configurar. Tot i que per defecte únicament hi ha instal·lada l'eina tar, ja que és el compressor d'arxius que es fa servir més sovint en el GNU/Linux, és molt recomanable que un administrador les sàpiga fer servir, ja que molt probablement les haurà d'utilitzar. En l'últim apartat d'aquesta secció veurem una eina amb llicència GNU anomenada `Amanda` que ens ofereix alguns dels avantatges de les eines comercials de còpies de seguretat.

2.1.1. Dump

L'ordre `dump` té associada l'ordre `restore`, per a recuperar-les. El funcionament d'aquesta eina és fer una còpia de seguretat de tot el sistema d'arxius en un únic fitxer, és a dir, normalment de tot el disc, o discos si els tenim muntats dins el sistema de fitxers. Encara que es creï un fitxer "regular", se sol guardar en un dispositiu extern de còpia de seguretat (normalment una cinta, robots de còpies de seguretat o DVD).

Consultar el manual

Per veure les opcions d'execució de les ordres `dump` i `restore`, consulteu el `man`.

L'ordre `dump` pot fer diferents tipus de còpies de seguretat. Aquests tipus són: la total i diferents nivells d'incremental. Per a fer-ho, té un paràmetre en què s'indica el nivell de còpia de seguretat que es vol fer (tal com hem descrit abans, els nivells de còpies de seguretat van del 0 al 9). Per indicar quin nivell de còpia de seguretat volem fer, passem el número a l'ordre d'execució:

```
root# dump 0 (fa una còpia de seguretat total)
root# dump 3 (fa una còpia de seguretat de nivell 3)
```

Hi ha opcions que tenen associat un paràmetre, però a diferència d'altres ordres en què cada opció va seguida del paràmetre que té, la sintaxi de l'ordre d'execució de `dump` és una mica complexa, ja que té el format següent:

```
root# dump 'options' 'parameters' filesystem
```

En què primer es posen totes les opcions de manera consecutiva i després tots els paràmetres, ja que l'ordre d'aquelles marca l'ordre d'aquests. Finalment, s'escriu el dispositiu on volem executar l'ordre `dump`.

Aquesta també té una opció, mitjançant una ordre que hi està associada anomenada `rdump`, que permet fer còpies de seguretat de màquines remotes. Aquesta opció és molt interessant per als administradors, ja que si configuren els permisos d'accés remot de manera correcta poden disposar d'un servidor de còpies de seguretat per a fer còpies de totes les màquines de la xarxa. D'aquesta manera es disposarà d'una còpia de seguretat de tots els equips informàtics

que hi ha en l'organització i, per tant, es reduirà al màxim el temps d'espera a restablir el servei de la organització en cas d'una fallada general produïda per alguna catàstrofe.

Per utilitzar l'ordre `rdump` hem de permetre al servidor de còpies de seguretat entrar als clients mitjançant l'ordre `rsh` i sense contrasenya. Per la poca seguretat que tenen aquest tipus d'accessos, és del tot desaconsellable utilitzar l'usuari arrel o *root* per a fer còpies de seguretat, per tant, es crearà un usuari de còpies remot amb els privilegis suficients per a entrar a les màquines des de la xarxa interna.

Les ordres `dump` i `restore` tenen moltes funcionalitats. Mitjançant un *shell script* podem automatitzar la còpia de seguretat i obtenir resultats molt satisfactoris. No obstant això, aquestes eines també tenen limitacions:

- No hi ha cap manera d'obtenir una imatge completa de tot el sistema.
- Per a automatitzar les tasques de còpia de seguretat calen *shell scripts*, que, malgrat que tenen molt bons resultats, han de ser creats per l'administrador, i pot ser que continguin alguna fallada.
- Quan fem `restore` ens surten tots els fitxers que hi ha d'haver en la còpia de seguretat, encara que s'hagin copiat malament o no se n'hagi fet la còpia de seguretat perquè diu que hi ha algun tipus d'error.
- Hi ha unes quantes versions d'aquestes aplicacions; cada distribució d'Unix o GNU/Linux pot fer servir versions diferents. Algunes d'aquestes versions de `dump` o `restore` poden ser incompatibles entre si.
- No tenen cap interfície que en faci més amigable la gestió.

Per instal·lar `dump` en la nostra màquina hem d'executar l'ordre següent:

```
root# apt-get install dump
```

L'ordre `man dump`

A més d'aquestes opcions, l'ordre `dump` en té moltes d'altres. Si volem conèixer aquestes opcions, hem de consultar el `man` mitjançant l'ordre `man dump`.

Un dels fitxers de configuració d'aquesta eina és `/etc/fstab`, el qual gestiona els dispositius que es munten en la màquina en temps d'arrencada.

El cinquè camp de cada línia d'aquest fitxer és un camp numèric. Si és 1, ens indica que s'han de fer còpies d'aquest dispositiu. Si és 0, ens indica que no se'n faran còpies (aquests còpies solen ser d'ús temporal o memòries cau d'aplicacions).

Exemple de còpia de seguretat

Un exemple d'execució d'una còpia de seguretat mitjançant l'ordre `dump` és el següent:

```
root# dump 0unbf 128 /dev/rmt/0cbn /home
```

Amb aquesta sentència indiquem a l'ordre `dump` que faci una còpia de seguretat de nivell 0 (primera opció, 0), que la mida dels blocs és de 128 (opció `b`) i que el dispositiu de còpia de seguretat és a `/dev/rmt/0cbn` (opció `f`). Les opcions `u` i `n` indiquen, respectivament, que s'actualitzin els arxius de `dump` i que enviï un correu electrònic als operadors de còpia de seguretat quan s'hagi acabat aquesta còpia.

Amb la instal·lació de la `dump` també hem instal·lat la de `restore`. Per recuperar un directori d'usuari executem una ordre semblant a la següent:

```
root# restore -xvybf 128 /dev/rmt/0cbn ./home/jordi
```

Aquesta ordre ens indica que recuperi tots els arxius i els directoris de manera recursiva que hi ha a partir de `/home/jordi` (opció `x`), que treballi en mode `verbose` (opció `v`) i que si detecta blocs dolents que continuï (opció `y`). Finalment, les opcions `b` i `f` tenen el mateix significat que en el cas de la `dump`: la mida dels blocs i el dispositiu.

Les opcions més importants de l'ordre `dump` són les següents:

1) `0-9`: nivells de còpies de seguretat que volem fer.

2) `a`: escriure a la cinta fins que s'acabi, sense tenir en compte els càlculs aproximats de la mida de la còpia de seguretat.

3) `k`: fer servir Kerberos[1] per a l'autenticació en el cas de còpies de seguretat remotes.

[(1)]Atenció: per a fer servir aquesta opció hem hagut d'haver compilat abans la dump amb suport a Kerberos.

4) `M`: permet fer molts volums.

5) `q`: fa que l'ordre `dump` avorti de manera immediata.

6) `S`: indica de manera estimada la quantitat d'espai necessari per a fer la còpia de seguretat.

7) `W`: indica a l'administrador quins sistemes són els que necessiten còpia de seguretat.

Si volem veure totes les opcions que permet fer l'ordre `dump`, hem d'executar l'ordre d'ajuda següent:

```
root# man dump
```

2.1.2. Cpio

La nostra segona opció per a poder fer còpies de seguretat de les dades seria fer-les amb l'ordre `cpio`. Aquesta ordre, malgrat que fa molt temps que està en actiu, no té la popularitat de l'ordre `dump` ni la de `tar`, que és una altra utilitat per a comprimir arxius. L'avantatge principal de la `cpio` és que accepta la llista de fitxers dels quals es vol fer una còpia de seguretat per l'entrada estàndard; és a dir, podem concatenar ordres mitjançant *pipes* –es representen mitjançant el símbol (`|`)–, per saber quins són els arxius dels quals hem de fer còpia de seguretat. Un exemple d'aquesta utilització de l'entrada estàndard per a fer còpies és el següent:

```
root# find /home -ctime 1 -print | cpio -o
```

Vegem les opcions que hi ha en l'ordre `dump`, però que no té `cpio`:

1) Fer còpies de seguretat incrementals, sense l'ajuda de l'ordre `find`. És a dir, `dump` té constància de quins arxius s'han modificat des de l'última còpia de seguretat total que s'ha fet amb la mateixa ordre, mentre que amb `cpio` s'ha de fer una cerca, per veure quins arxius s'han modificat des de la darrera còpia, i passar-ne la llista per l'entrada estàndard a l'ordre `cpio`.

L'exemple anterior fa precisament una còpia dels arxius del directori *home* que s'han modificat avui.

2) Fer el procés de restauració, `restore`, de manera interactiva.

Un exemple d'una còpia de seguretat amb l'ordre `cpio` és el següent:

```
root# ls | cpio -oOacv device
```

Aquesta ordre ens fa la còpia de tots els fitxers que surtin en l'ordre `ls` i ens envia la sortida de la llista del directori al dispositiu `device` (opció `O`). L'opció `a` ens deixa l'`atime` (l'última vegada que hi vam accedir) dels fitxers de la mateixa manera com estaven abans de fer la còpia de seguretat.

És aconsellable fer servir el `man` per a veure totes les opcions disponibles d'aquesta ordre.

Recuperem els fitxers amb l'ordre següent:

```
root# cpio -icktv < device
```

Aquesta ordre llegeix per l'entrada estàndard el dispositiu on hi ha emmagatzemada la còpia de seguretat i recupera els fitxers.

Les opcions més destacades de l'ordre `cpio` són les següents:

- `i`: execució en mode entrada.

- `m`: no modifica els temps dels fitxers (ni l'`atime`, ni el `ctime`).
- `o`: execució en mode sortida.
- `p`: execució en mode *bypass*.
- `r`: reanomena els fitxers de manera interactiva.
- `t`: mostra a la pantalla la taula de continguts de l'entrada.
- `no-preserve-owner`: quan extraiem una còpia posa com a propietari dels fitxers l'usuari que extreu els fitxers.
- `no-absolute-filenames`: extreu els fitxers amb el camí relatiu al fitxer actual. És a dir, el directori arrel per als fitxers que s'extreuen és el directori des d'on s'executa l'ordre.

Si volem veure totes les opcions de la `cpio`, hem de consultar el `man` mitjançant l'ordre següent:

```
root# man cpio
```

2.1.3. `Tar`

Si el que volem és fer una còpia de seguretat del sistema, probablement la millor opció és fer-la amb l'ordre `dump`. Ara bé, si només ens interessa fer una còpia de seguretat del *home* d'un usuari abans, per exemple, de donar-lo de baixa, l'aplicació `tar` és sens dubte la millor opció.

Tot i que l'ordre `tar` té un origen simultani a la `cpio`, té una acceptació més gran entre els usuaris; això es deu al fet que les operacions bàsiques de l'ordre `tar` són més simples (i més estàndards entre les diferents versions) que les de la `cpio`. Una mostra d'aquesta popularitat que té aquesta comanda és que la majoria dels fitxers que baixem d'Internet estan amb aquest tipus de compressió. Gràcies a la gran popularitat que té, és molt important que coneguem bé aquesta eina.

És aconsellable consultar el manual per a saber les opcions que té aquesta ordre.

Exemple d'execució

Un exemple d'execució amb l'ordre `tar` és aquest:

```
root# tar cvzf backup.tar.gz /home/jordi
```

Aquesta ordre ens crea un fitxer (opció `c`) anomenat `backup.tar.gz` amb el contingut recursiu, que és una opció per defecte, que ens informa de possibles errors o advertiments (opció `v`) del directori `/home/jordi`. A més, aquest fitxer s'ha comprimit fent servir l'aplicació `gunzip` (opció `z`).

Per a extreure el contingut d'aquest fitxer hem de fer servir l'ordre següent:

```
root# tar xvzf backup.tar.gz
```

L'opció `x` serveix per a extreure el contingut d'un arxiu `tar`.

Les opcions més destacades de l'ordre `tar` són les següents:

- `a`: afegeix fitxers a un arxiu `.tar`.
- `c`: crea un arxiu `.tar`.
- `d`: troba les diferències entre un arxiu `.tar` i el sistema d'arxius.
- `M`: crea molts arxius `.tar`.
- `r`: afegeix fitxers (al final) d'un arxiu `.tar`.
- `t`: mostra el contingut d'un arxiu `.tar`.
- `x`: extreu el contingut d'un arxiu `.tar`.
- `Z`: comprimeix el contingut d'un arxiu `.tar` amb l'ordre `compress`.
- `z`: comprimeix el contingut d'un arxiu `.tar` amb l'ordre `gzip`.
- `atime-preserve`: no modifica els temps d'accés als fitxers.

Per conèixer totes les opcions de la `tar`, hem d'executar l'ordre següent:

```
root# man tar
```

2.1.4. Amanda

L'aplicació Amanda (Advanced Maryland Automated Network Disk Archiver) és una eina de còpia de seguretat de distribució lliure desenvolupada per la Universitat de Maryland. Aquesta aplicació ofereix funcionalitats que són igualables als sistemes comercials de còpies de seguretat que trobem en el mercat.

L'Amanda estableix un servidor únic que permet fer còpies de seguretat de moltes màquines en un únic dispositiu. El dispositiu de còpia que fa servir l'Amanda són les cintes, és a dir, no es pot utilitzar ni CD ni DVD a menys que es virtualitzi una unitat de DVD com a unitat de cinta.

Per fer còpies de diferents màquines hem d'instal·lar clients de l'Amanda en cadascun dels servidors dels quals volem fer còpia de seguretat. Més endavant veurem els passos que cal seguir per a instal·lar el client de còpia de seguretat.

Una de les grans aportacions de l'Amanda és l'ús del disc d'emmagatzematge en el servidor de cintes. La idea és fer moltes còpies de seguretat en paral·lel i deixar la informació en el disc d'emmagatzematge, i després un procés independent s'encarrega de traspassar la informació del disc a les cintes. El fet d'utilitzar els discos proporciona més rapidesa i la possibilitat de fer les còpies de seguretat de més d'una màquina alhora. Un altre dels grans avantatges que ens ofereix són les anomenades *còpies programades*. Es defineix un cicle de còpia per a cada àrea amb la finalitat de controlar el temps màxim entre còpies completes. L'Amanda pren aquesta informació estadística sobre rendiments de còpies anteriors i estima la mida de les còpies per decidir quin nivell de còpia ha de fer servir; és a dir, quin nivell s'aplica a cada màquina per a cada dia de la setmana. Això s'allunya de la política de còpia de seguretat tradicional, però permet balancejar les còpies de manera que el temps d'execució de cadascuna sigui aproximadament constant d'un dia per l'altre.

Els protocols de còpia de fitxers de xarxa que fa servir l'Amanda són propis, és a dir, no utilitza ordres com `rsh`, `rdump` o res que s'hi assembli. Cada programa client de l'Amanda escriu en la sortida estàndard, on el servidor recull i transmet les dades copiades en el disc d'emmagatzematge i després en la cinta. Això permet inserir compressió i xifratge i, a més, mantenir un catàleg de la imatge per a recuperar-lo més endavant. Tant la compressió com el xifratge són transparents per a l'administrador, ja que l'Amanda utilitza aquestes dues eines integrades als seus propis programes de còpia de fitxers.

Aquesta aplicació està preparada per a treballar per lots (*batch*). Les màquines client que no siguin actives en el moment en què es fa la còpia són anotades i saltades; s'anota que d'aquesta màquina no se n'ha pogut fer còpia de seguretat i es passa a fer la de la següent de la llista. Si es produeixen errors en el dispositiu de cintes, fa que a partir d'aquell moment l'Amanda treballi en mode degradat, és a dir, només fa la còpia en el disc d'emmagatzematge. I una vegada resolt el problema amb les cintes, s'aboca (de manera manual) la informació del disc cap a les cintes.

Malgrat les múltiples funcionalitats que ofereix aquesta aplicació i la gran quantitat de clients que pot arribar a manejar, l'Amanda és relativament simple d'instal·lar i mantenir.

Per a instal.lar el servidor Amanda, n'hi ha prou de descarregar el fitxer `amanda-x.tar.gz` de la pàgina web http://www.amanda.org, descomprimir el fitxer en una carpeta, compilar i instal·lar el programa fent:

```
root# ./configure --with-user=backup --with-group=disk
root# make
```

```
root# make install
```

També es pot fer de manera més senzilla amb l'ordre `apt-get` del sistema, en què ja ens buscarà les dependències i ens dirà quins altres paquets aniria bé tenir també instal·lats en l'equip perquè l'aplicació Amanda funcioni correctament. En aquest cas ens suggereix que instal·lem tots aquests paquets per poder fer còpies també remotes.

```
root# apt-get install amanda-server amanda-client amanda-common gnuplot dump smbclient
openbsd-inetd cifs-utils
```

Això instal·larà i configurarà tota l'aplicació de còpies de seguretat.

Es poden canviar els directoris en el cas de fer servir la instal·lació manual (amb el `make`), però si no es canvien els directoris, cal utilitzar:

- `/usr/local/sbin`: per als programes que executa l'administrador.
- `/usr/local/bin`: per a les bilbioteques que necessita l'Amanda.
- `/usr/local/libexec`: per als programes propis de l'aplicació Amanda.
- `/usr/local/man`: per a la documentació de l'aplicació.

Una vegada tenim l'aplicació instal·lada a l'equip, és l'hora de configurar-la.

Primer s'ha d'editar el fitxer `/etc/Amanda/MyConfig/amanda.conf` i modificar els registres `org`, `mailto`, `tapecycle` i `tapedev`. El primer registre és el domini de l'organització on volem fer la còpia de seguretat. El segon és l'usuari de correu que rep les notificacions de funcionament de l'Amanda, tot i que no és necessari tenir-lo (i en cas de no tenir el servidor de correu activat no hi serà). El registre `tapecycle` fa referència al nombre de cintes que formen part de la rotació. En l'últim registre hem de configurar en quin dispositiu tenim mapat el dispositiu de cintes.

També hem de configurar el nom que posarem en les cintes. Per fer-ho, modifiquem el registre `labelstr` mitjançant les expressions regulars. Per defecte, les cintes tenen les etiquetes de `MyData00` a `Mydata99`.

També cal configurar els cicles de còpia amb el paràmetre `dumpcycle`. Fins i tot es pot afegir un paràmetre a l'aplicació Amanda que controla l'amplada de banda màxima que es vol assignar a aquesta aplicació en el cas de fer servir la xarxa per a fer la còpia de seguretat d'equips remots, de tal manera que si la xarxa està ocupada amb més trànsit del que està configurat, no es farà la còpia i s'esperarà que l'amplada de banda baixi fins a aquest valor i, per tant, es pugui iniciar la còpia per la xarxa. Això ho aconseguim amb el paràmetre `netusage`, on el valor assignat denota els KB per segon assignats.

En el cas d'instal·lar l'aplicació en un servidor en què hi hagi les unitats de cintes, en aquest fitxer es veurà la configuració d'aquest tipus de cinta que té instal·lat. Com ja s'ha comentat, l'Amanda únicament fa còpies de seguretat sobre dispositius de cinta, per la qual cosa si es vol fer servir un disc dur com a sortida de les còpies s'ha de canviar la configuració i definir el disc com una cinta virtual. Es pot fer de la manera següent:

1) Canviem el paràmetre `tapedevide` a "`no-such-devide`".

2) Canviem el paràmetre `rawtapedev` a "`no-such-device`".

3) Canviem el paràmetre `changerdev` a "`no-such-device`".

4) Canviem el paràmetre `typetype` a `disksave`.

5) Creem un nou tipus de cinta que serà el disc dur "`savedisk`" i per tant afegim la definició següent al fitxer de configuració:

```
define tapetype disksave
{comment "tape for disk"
length 1000 gbytes
filemark 0 kbytes
speed 2000 kbytes
}
```

6) Eliminem (o comentem amb `#`) la secció on es defineix "`holdingdisk`".

7) Canviem el valor de `reserve` a 30.

8) Eliminem o comentem el paràmetre `runtapes`.

9) Indiquem el punt de muntatge del disc on es vol fer la còpia amb `diskdir`.

10) Indiquem l'espai que es vol ocupar sobre aquest disc mb `disksize`.

Vegeu també

Al final d'aquesta secció es mostra un exemple d'aquest fitxer de configuració (extret d'http://www.sergio-gonzalez.com).

Una de les tasques que fa la instal·lació és crear un usuari, si no existeix, anomenat `backup` o a vegades `amanda`. Aquest usuari és el que hem d'utilitzar per a treballar amb l'aplicació de còpies de seguretat, d'aquesta manera no es configurarà des de l'usuari *root* i en el cas de tenir algun *0day* que afecti directament aquest programari no es disposaran de privilegis de *root* en el sistema.

El pas següent és etiquetar les cintes de manera correcta. Per fer-ho, hem d'executar l'ordre següent:

```
root# su - backup
backup$ amlabel MyConfigSet1 tape_label
```

Si el nostre dispositiu de cintes té més d'un *slot* de cintes, hem d'executar:

```
backup$ amlabel MyConfigSet1 tape_label slot num_slot
```

Noteu que s'ha canviat d'usuari i ara es fa servir l'usuari `backup`, o `amanda`, depenent del que s'hagi configurat en el fitxer `amanda.conf`.

En cas que per error s'introdueixi una cinta que no correspon per la numeració, és a dir, que necessita la cinta 2 i s'ha introduït la 3, l'aplicació Amanda ho detecta i no continuarà amb l'execució de la còpia de seguretat.

Ara fa falta incloure les màquines i els directoris dels quals volem fer la còpia de seguretat, ja sigui de tota la màquina o d'alguna carpeta. Imaginem que volem fer una còpia de seguretat de les particions `/home` i `/usr` d'una màquina anomenada `P1S1`. Per fer-ho, en el servidor hem de modificar l'arxiu `/etc/amanda/Myconfig/disklist` afegint-hi unes línies semblants a aquestes:

```
P1S1 /home comp-root-tar
P1S1 /usr comp-root-tar
```

Consultar el manual

Consulteu el `man` per veure el format de la instrucció i excloure directoris de còpia de seguretat.

Hi hem d'afegir una línia semblant a l'anterior per a cada partició de la màquina de la qual volem fer una còpia de seguretat. És a dir, si volem fer una còpia de tot l'equip i aquest té quatre particions (`/`, `/home`, `/usr`, `/var`), hem d'afegir quatre línies a aquest fitxer, una per cada partició. Si només té una partició, n'hi ha prou d'afegir-hi una sola línia amb el directori arrel per a fer una còpia de seguretat de tota la màquina. Si volem fer còpies de seguretat dels discos de la màquina dels quals és servidor l'Amanda, també hem d'afegir les línies corresponents en aquest fitxer. És recomanable fer servir el nom complet de la màquina i no `localhost` si fem la còpia de seguretat del servidor Amanda, així identificarem millor quina màquina s'està configurant i es podrà exportar la configuració.

En el fitxer de configuració de l'aplicació Amanda, hi ha la definició de cada un dels tipus de còpies de seguretat que es poden fer, i que en aquest fitxer `disklist` associarem a cada directori d'on es vol fer la còpia.

Finalment, només fa falta donar permisos. Hi ha dos tipus de permisos: el primer es fa al client perquè pugui entrar al servidor a fer les còpies de seguretat, i el segon es dóna al servidor perquè el client pugui entrar a restaurar les còpies de seguretat. Per fer-ho, hem de fer servir el *home* de l'usuari que utilitzarem per a fer la còpia de seguretat (per defecte és l'usuari `backup` o `amanda`), editar el fitxer `.amandahost` i afegir-hi una línia amb el nom de la màquina i l'usuari al qual volem entrar. Imaginem-nos que el servidor es diu `backupserver` i el client es diu `P1S1`. En el fitxer `.amandahost` del servidor hem de posar:

```
P1S1 backup
```

```
P1S1 root
```

I en el fitxer `.amandahost` del client afegim una línia semblant a la següent:

```
backupserver backup
```

Una vegada fets els passos anteriors, ja estem en disposició de fer una còpia de seguretat. Per fer-la, primer comprovem que estan posades les cintes corresponents a avui mitjançant l'ordre següent:

```
backup$ amcheck -t MyConfig
```

Una vegada feta la comprovació i solucionat els possibles errors que retorni aquesta aplicació que comprova el fitxer de configuració, executem la còpia de seguretat. Hem de fer servir l'ordre següent per dur a terme la còpia de seguretat corresponent a tot el dia d'avui sencer:

```
backup$ amdump MyConfig
```

Les opcions més importants d'`amcheck`

- `m`: no surt res per pantalla però envia un correu electrònic en cas que es detecti algun error.
- `c`: executa una revisió mèdica en el client.
- `l`: executa una revisió mèdica en el servidor local.
- `t`: executa una revisió mèdica en el dispositiu de cintes.
- `s`: executa una revisió mèdica en el servidor local i en el dispositiu de cintes (és el mateix que executar `amcheck` amb les opcions `lt`).
- `w`: activa la destrucció de la protecció contra escriptura. Atenció: aquest paràmetre és destructiu, és a dir, esborra la informació que hi havia en la cinta.

Si només volem fer la còpia de seguretat d'una única màquina, executem l'ordre següent:

```
backup$ amadump MyConfig Machine_name
```

Abans de començar a fer la còpia de seguretat de manera periòdica, hem de comprovar que la còpia funciona. La millor manera de fer-ho és restaurant un directori de la còpia de seguretat. Per a això, hem d'anar a una còpia de la màquina client i executar el següent:

```
root# amrecover MyConfig -s server_name backup
```

Entrem en una consola interactiva i hi executem les ordres següents:

```
Amrecover> cd directori_que_volem_restaurar
Amrecover> add fitxer_que_volem_restaurar
```

```
Amrecover> add directori_que_volem_restaurar
Amrecover> extract
```

Si la recuperació es fa de manera satisfactòria, ja podem començar a fer la còpia de seguretat de manera periòdica. Per fer-ho, hem d'afegir una línia en l'ordre `crontab`.

Per accedir a la `crontab` hem d'executar l'ordre

```
root# crontab -e
```

La línia que hi hem d'afegir és la següent:

```
10 01 * * 1-5 su backup -c "/usr/sbin/amdump MyConfig"
```

Mitjançant aquesta línia executem cada dia (de dilluns a divendres), a la una i deu de la matinada, la còpia de seguretat diària. Si volem que aquesta còpia es guardi en cintes, hem de posar cada dia les cintes que toquin en el dispositiu de cintes. Aquesta tasca s'ha de fer de manera manual. Com que executem l'Amanda com un procés i no com un dimoni, si volem parar el servidor de còpies de seguretat hem de matar el procés. Si volem afegir o treure una màquina del servidor de còpia de seguretat, hem de refer els passos anteriors de la configuració.

Exemple de fitxer `amanda.conf` (http://www.sergio-gonzalez.com):

```
#
# amanda.conf - sample Amanda configuration file.
#
# If your configuration is called, say, "DailySet1", then this file
# normally goes in /etc/amanda/DailySet1/amanda.conf.
#
# for explanation of the parameters refer to amanda(8) and
# /usr/doc/amanda/WHATS.NEW.gz

org "Diaria"          # your organization name for reports
mailto "amanda"       # space separated list of operators at your site
dumpuser "amanda"     # the user to run dumps under
#
inparallel 4          # maximum dumpers that will run in parallel
netusage  600         # maximum net bandwidth for Amanda, in KB per sec

# a filesystem is due for a full backup once every <dumpcycle> days
dumpcycle 4 weeks     # the number of days in the normal dump cycle
tapecycle 8 tapes     # the number of tapes in rotation

bumpsize 1 MB      # minimum savings (threshold) to bump level 1->2
```

```
bumpdays     1     # minimum days at each level
bumpmult     4     # threshold = bumpsize * (level-1)**bumpmult

#runtapes     9       # explained in WHATS.NEW
#tpchanger "no-changer" # the tape-changer glue script, see TAPE.CHANGERS
tapedev "no-such-device"     # Linux @ tuck, important: norewinding
rawtapedev "no-such-device"  # the raw device to be used (ftape only)
#changerfile "/mnt/amanda/changer"
changerdev "no-such-device"

tapetype DISKSAVE    # what kind of tape it is (see tapetypes below)
labelstr "^HISS[0-9][0-9]*$"  # label constraint regex: all tapes must match

diskdir "/mnt/backup"         # where the holding disk is
disksize 10 MB                # how much space can we use on it
reserve 30
#diskdir "/dumps/amanda/work" # additionaly holding disks can be specified
#diskdir "/mnt/disk4"
#disksize 1000 MB             # they are used round-robin


# Amanda needs a few MB of diskspace for the log and debug files,
# as well as a database.  This stuff can grow large, so the conf directory
# isn't usually appropriate.

infofile "/var/lib/amanda/DailySet1/curinfo"    # database filename
logfile  "/var/log/amanda/DailySet1/log"        # log filename

# where the index files live
indexdir "/var/lib/amanda/DailySet1/index"

# Specify holding disks.  These are used as a temporary staging area for
# dumps before they are written to tape and are recommended for most sites.
# The advantages include: tape drive is more likely to operate in streaming
# mode (which reduces tape and drive wear, reduces total dump time); multiple
# dumps can be done in parallel (which can dramatically reduce total dump time.
# The main disadvantage is that dumps on the holding disk need to be flushed
# (with amflush) to tape after an operating system crash or a tape failure.
# If no holding disks are specified then all dumps will be written directly
# to tape.  If a dump is too big to fit on the holding disk than it will be
# written directly to tape.  If more than one holding disk is specified then
# they will all be used round-robin.

#holdingdisk hd1 {
#    comment "main holding disk"
#    directory "/mnt/amanda1"   # where the holding disk is
#    use 30 Mb           # how much space can we use on it
```

```
#                       # a non-positive value means:
#                       #        use all space but that value
#    chunksize 1Mb      # size of chunk if you want big dump to be
#                       # dumped on multiple files on holding disks
#                       #  N Kb/Mb/Gb split images in chunks of size N
#                       #             The maximum value should be
#                       #             (MAX_FILE_SIZE - 1Mb)
#                       #  0          same as INT_MAX bytes
#}

# tapetypes
#
# Define the type of tape you use here, and use it in "tapetype" above.
# Some typical types of tapes are included here.  The tapetype tells amanda
# how many MB will fit on the tape, how big the filemarks are, and how
# fast the tape device is.
#
# For completeness Amanda should calculate the inter-record gaps too, but it
# doesn't.  For EXABYTE and DAT tapes this is ok.  Anyone using 9 tracks for
# amanda and need IRG calculations?  Drop me a note if so.

define tapetype DISKSAVE  {
   comment "Fake tape description for save to disk"
   length 1000 gbytes
   filemark 0 kbytes
   speed 2000 kbytes
}

define tapetype QIC-60 {
    comment "Archive Viper"
    length 60 mbytes
    filemark 100 kbytes         # don't know a better value
    speed 100 kbytes            # dito
}

define tapetype DEC-DLT2000 {
    comment "DEC Differential Digital Linear Tape 2000"
    length 15000 mbytes
    filemark 8 kbytes
    speed 1250 kbytes
}

# goluboff@butch.Colorado.EDU
# in amanda-users (Thu Dec 26 01:55:38 MEZ 1996)
define tapetype DLT {
    comment "DLT tape drives"
    length 20000 mbytes         # 20 Gig tapes
```

```
    filemark 2000 kbytes        # I don't know what this means
    speed 1500 kbytes
}

define tapetype SURESTORE-1200E {
    comment "HP AutoLoader"
    length 3900 mbytes
    filemark 100 kbytes
    speed 500 kbytes
}

define tapetype EXB-8500 {
    comment "Exabyte EXB-8500 drive on decent machine"
    length 4200 mbytes
    filemark 48 kbytes
    speed 474 kbytes
}

define tapetype EXB-8200 {
    comment "Exabyte EXB-8200 drive on decent machine"
    length 2200 mbytes
    filemark 2130 kbytes
    speed 240 kbytes
}

define tapetype HP-DAT {
    comment "DAT tape drives"
    length 1900 mbytes          # these numbers are not accurate
    filemark 100 kbytes         # but you get the idea
    speed 500 kbytes
}

define tapetype DAT {
    comment "DAT tape drives"
    length 1000 mbytes          # these numbers are not accurate
    filemark 100 kbytes         # but you get the idea
    speed 100 kbytes
}

define tapetype MIMSY-MEGATAPE {
    comment "Megatape (Exabyte based) drive through Emulex on Vax 8600"
    length 2200 mbytes
    filemark 2130 kbytes
    speed 170 kbytes            # limited by the Emulex bus interface, ugh
}

define tapetype QIC-3080 {
```

```
    comment "QIC 3080"
    length 2000 mbytes
    filemark 64 kbytes
    speed 250 kbytes
}

# dumptypes
#
# These are referred to by the disklist file.  The dumptype specifies
# certain "options" for dumping including:
#       index         - keep an index of the files backed up
#       compress-fast - (default) compress on the client using fast algorithm
#       compress-best - compress using the best (and slowww) algorithm
#       no-compress   - don't compress the dump output
#       srvcompress   - Compress dumps on the tape host instead of client
#                       machines.  This may be useful when a fast tape host
#                       is backing up slow clients.
#       record        - (default) record the dump in /etc/dumpdates
#       no-record     - don't record the dump, for testing
#       no-hold       - don't go to the holding disk, good for dumping
#                       the holding disk partition itself.
#       skip-full     - Skip the disk when a level 0 is due, to allow
#                       full backups outside Amanda, eg when the machine
#                       is in single-user mode.
#       skip-incr     - Skip the disk when the level 0 is NOT due.  This
#                       is used in archive configurations, where only full
#                       dumps are done and the tapes saved.
#       no-full       - Do a level 1 every night.  This can be used, for
#                       example, for small root filesystems that only change
#                       slightly relative to a site-wide prototype.  Amanda
#                       then backs up just the changes.
#
# Also, the dumptype specifies the priority level, where "low", "medium" and
# "high" are the allowed levels.  These are only really used when Amanda has
# no tape to write to because of some error.  In that "degraded mode", as
# many incrementals as will fit on the holding disk are done, higher priority
# first, to insure the important disks are dumped first.

define dumptype always-full {
    comment "Full dump of this filesystem always"
    options no-compress
    priority high
    dumpcycle 0
    maxcycle 0
}

define dumptype comp-user-tar {
```

```
    program "GNUTAR"
    comment "partitions dumped with tar"
    options compress-fast, index, exclude-list "/etc/amanda/exclude.gtar"
    priority medium
}

define dumptype comp-root-tar {
    program "GNUTAR"
    comment "Root partitions with compression"
    options compress-fast, index, exclude-list "/etc/amanda/exclude.gtar"
    priority low
}

define dumptype user-tar {
    program "GNUTAR"
    comment "partitions dumped with tar"
    options no-compress, index, exclude-list "/etc/amanda/exclude.gtar"
    priority medium
}

define dumptype high-tar {
    program "GNUTAR"
    comment "partitions dumped with tar"
    options no-compress, index, exclude-list "/etc/amanda/exclude.gtar"
    priority high
}

define dumptype root-tar {
    program "GNUTAR"
    comment "Root partitions dumped with tar"
    options no-compress, index, exclude-list "/etc/amanda/exclude.gtar"
    priority low
}

define dumptype comp-user {
    comment "Non-root partitions on reasonably fast machines"
    options compress-fast
    priority medium
}

define dumptype nocomp-user {
    comment "Non-root partitions on slow machines"
    options no-compress
    priority medium
}

define dumptype holding-disk {
```

```
    comment "The master-host holding disk itself"
    options no-hold
    priority medium
}

define dumptype comp-root {
    comment "Root partitions with compression"
    options compress-fast
    priority low
}

define dumptype nocomp-root {
    comment "Root partitions without compression"
    options no-compress
    priority low
}

define dumptype comp-high {
    comment "very important partitions on fast machines"
    options compress-best
    priority high
}

define dumptype nocomp-high {
    comment "very important partitions on slow machines"
    options no-compress
    priority high
}

define dumptype nocomp-test {
    comment "test dump without compression, no /etc/dumpdates recording"
    options no-compress, no-record
    priority medium
}

define dumptype comp-test {
    comment "test dump with compression, no /etc/dumpdates recording"
    options compress-fast, no-record
    priority medium
}
```

Exemple de fitxer `disklist`:

```
# sample Amanda2 disklist file, derived from CS.UMD.EDU's disklist
#
# If your configuration is called, say, "DailySet1", then this file
# normally goes in /etc/amanda/DailySet1/disklist.
```

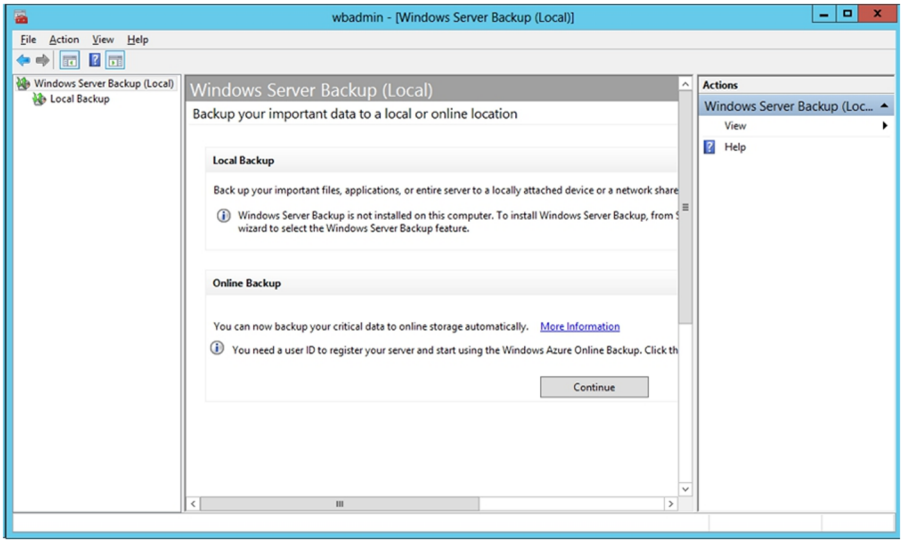
```
#
# File format is:
#
#       hostname diskdev dumptype
#
# where the dumptypes are defined by you in amanda.conf.
# Configuración

localhost /mnt/copia comp-root-tar
```

2.2. Eines de còpia de seguretat en el Windows Server

2.2.1. Realització de còpies de seguretat en el Windows Server 2012

Es pot accedir al programa de còpia de seguretat del Windows Server 2012 des de les eines administratives, el Windows Server Backup (vegeu la figura següent):

Windows Server Backup



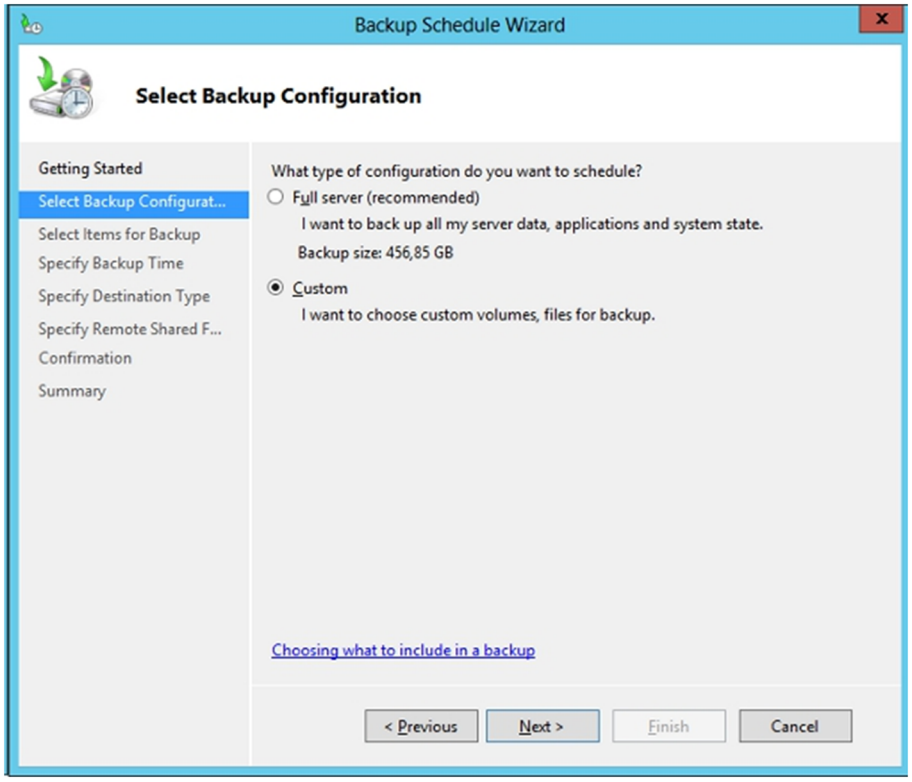
En aquesta figura podem veure com es poden fer les còpies de dues maneres diferents: una sobre el mateix servidor, en local, i l'altre mitjançant la xarxa Internet i el programa Azure Online Backup de Microsoft, que és un programari que ens ajuda a gestionar els servidors fent còpies i protegint dades en el núvol. Com es pot veure en la figura anterior, cap de les dues opcions està instal·lada per defecte en el servidor i s'ha de fer el procés d'instal·lació d'una característica o del programa Azure.

Només cal obrir l'administrador del servidor on hi ha els rols i característiques, buscar aquesta en la llista i dir-li que l'instal·li en el servidor.

Un cop s'ha instal·lat la característica, tornem a obrir el Windows Server Backup i ara sí que es poden configurar les còpies de seguretat en local. Hi ha dues opcions per a configurar-les: fer una còpia planificada o una còpia única, que s'executarà al moment i ja no es tornarà a fer.

El més normal serà planificar les còpies, tot i que puntualment es podria necessitar fer una còpia sencera en un moment donat fora de la planificació, possiblement perquè es vol instal·lar un nou maquinari dins el servidor, o un programari que pot interactuar amb altres parts i tenir problemes. Per tant, s'executarà l'assistent de còpies planificades. Únicament s'ha d'anar contestant a les diferents opcions que té depenent del que interessi més. Tot i que en el cas que s'ha de fer una còpia de tot el disc o de parts del disc, podem decidir fer-ne una còpia selectiva, ja que podem incloure les parts que ens interessen i excloure les parts de les quals no cal fer còpies de seguretat. La figura següent ens mostra la pantalla de la configuració d'aquestes còpies de seguretat:

Administrador de còpies de seguretat locals



En aquest cas es podrà incloure una configuració adient a les diferents necessitats i podrem seleccionar entre:

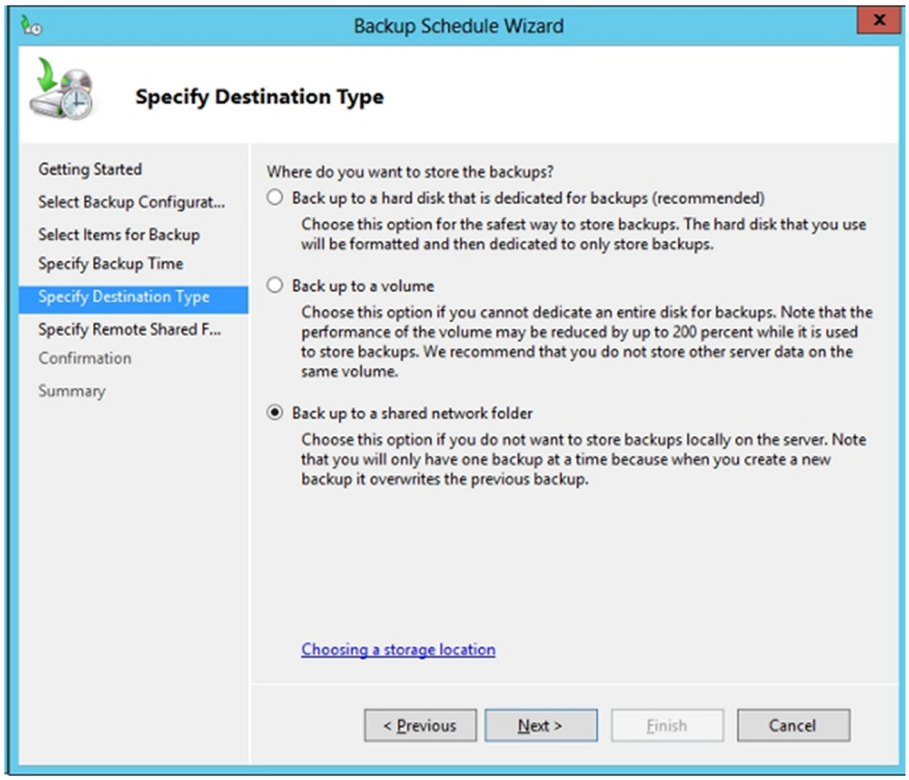
- Tot l'equip.
- L'estat del sistema (registre, configuració actual i estat del sistema o directori actiu si es tracta d'un controlador de domini).
- La part d'arrencada del sistema.
- Els discos durs.

I a més es podrà incloure en la mateixa pantalla les exclusions de la part que s'ha seleccionat i de la qual no cal fer còpies. Per exemple, si per comoditat s'ha seleccionat tot el disc dur, es pot excloure de fer còpies de les papereres de reciclatge dels usuaris, dels directoris temporals, dels directoris temporals de les actualitzacions, etc. fent que la còpia ocupi menys espai i temps.

El següent que s'ha de configurar és quan es fan les còpies de seguretat del que s'ha seleccionat: si és de tot el disc trigarà força i s'haurà de planificar per fer-ho a la nit; si és del directori d'usuaris i els perfils, s'haurà de fer quan ja hagin marxat tots i no hi hagi més canvis. Una qüestió important que s'ha de tenir en compte a l'hora de pensar en la manera com s'han de fer les còpies és que aquest programari no permet planificar còpies que no siguin diàries. Per tant, una còpia diària de tot el disc dur del servidor no té sentit i especificarem a l'administrador del Windows Backup Server que es facin les còpies dels discos sencers de manera incremental, cosa que en reduirà considerablement la mida. També el farem servir per a fer la còpia de la part que canvia cada dia, que podrien ser les carpetes i els perfils d'usuari. Per tant, caldrà afegir aquests directoris a la part on s'inclou allò de què es vol fer còpia, i no fer-la de tot el sistema.

El pas següent és configurar on es guarden els fitxers de les còpies. La figura mostra les tres opcions que hi ha disponibles: la primera opció és fer servir un disc dur específic per a aquesta finalitat, és la manera més segura ja que no hi accedirem per a altres propòsits, únicament per fer les còpies. La segona es utilitzar un disc compartit amb altres propòsits, però s'ha de tenir en compte que n'afectarà molt la capacitat. I la tercera és fer servir la xarxa per a tenir en un altre servidor les dades duplicades dels usuaris, per si li passa alguna cosa. És la més segura, però també la més lenta i costosa, ja que hem de tenir un altre equip preparat per a guardar-hi les dades. A més, s'haurà de fer servir un usuari que es validi en els dos equips (el remot i el servidor local); en aquest darrer cas, a més, ha de tenir el grup d'operadors de *backup*.

Configuració de la destinació de les còpies



Amb aquesta part ja queda configurada la còpia de seguretat de les dades dels usuaris o dels servidors sencers. Com podem veure, aquesta eina en local no es pot configurar gaire, ja que només permet una única política de còpies de seguretat, no permet fer dos tipus de còpies, ni podem fer incrementals o diferencials sobre carpetes d'usuari.

2.2.2. Altres eines de còpies de seguretat

Com s'ha vist, el programari que té per defecte el Windows Server és força reduït tenint en compte el que es podria necessitar en una empresa mitjana. Per a una empresa petita amb una desena d'usuaris potser ja aniria bé, però per a mitjanes i grans empreses és del tot insuficient.

Per solucionar aquesta mancança, Microsoft treu una plataforma anomenada *Azure* en la qual es pot treballar en el núvol i fer les còpies de seguretat directament des del mateix gestor de còpies, però en lloc de tenir un punt de xarxa local o un disc dur o USB instal·lat en el mateix servidor, ho gestiona tot amb un disc virtual pel qual s'ha de pagar en funció de la quantitat de transferència que es faci servir. Al web d'Azure es pot contractar i vincular l'espai d'aquest disc virtual al núvol amb el directori actiu que hi ha configurat en el servidor.

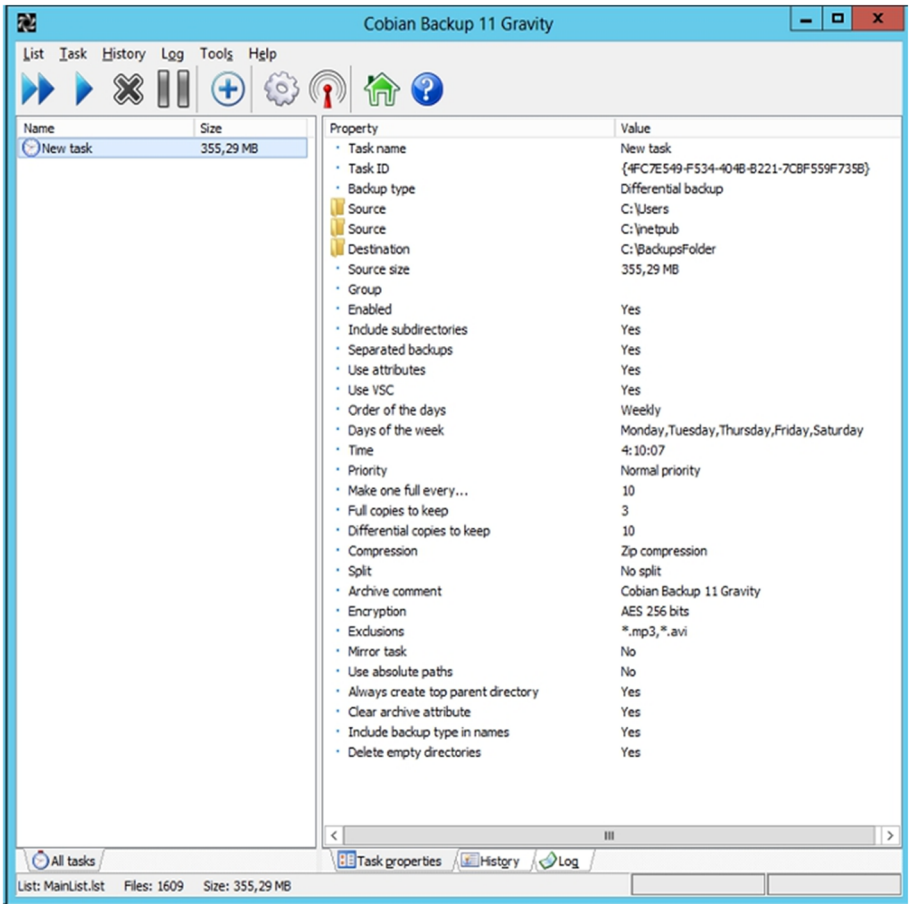
Web recomanat

Se'n pot trobar més informació a http://www.windowsazure.com

Una altra solució que es pot fer servir és utilitzar alguna de les múltiples eines que hi ha en el mercat que fan còpies de seguretat per a sistemes Windows. N'hi ha de pagament i gratuïtes; dins de les gratuïtes, en podem trobar una de molt lleugera i senzilla de fer anar com és la Cobian Backup, que en la darrera versió (11) es pot configurar perquè faci còpies incrementals, diferencials,

completes, de tot el disc i de directoris. D'altra banda, es poden fer les còpies sobre discos, per FTP, per xarxa local, etc. i es poden xifrar els documents de la còpia i comprimir-los perquè ocupin menys espai. En definitiva, la Cobian Backup és una eina molt completa per a poder fer còpies de seguretat amb molta facilitat. En la figura següent podem veure com s'ha configurat una còpia diferencial de les carpetes dels usuaris i de la pàgina web alguns dies de la setmana amb exclusions d'alguns fitxers i xifrant i comprimint els fitxers que compondran la còpia de seguretat.

Configuració d'una còpia de seguretat



2.2.3. Restauració de còpies de seguretat en el Windows Server 2012

Per restaurar una còpia de seguretat feta amb el programa de còpia de seguretat del Windows, seleccionem l'opció Assistent per a restauració de la pantalla inicial. A continuació s'inicia l'assistent. En la pantalla següent es mostren les còpies de seguretat que s'han fet. Podem restaurar una còpia o diverses còpies de seguretat, o fins i tot només una part d'aquestes còpies.

En segon lloc, podem seleccionar altres opcions de comportament de la còpia de seguretat com l'acció que cal fer quan els arxius que es restaurin ja siguin en el medi de destinació. Finalment, surt la pantalla de finalització de l'assistent de restauració de còpies de seguretat. Una vegada hem acabat comença el procés de restauració dels arxius.

2.3. Dispositius de còpia de seguretat

Els dispositius tradicionals de còpia de seguretat han estat des de fa molts anys les cintes. Això no impedeix, però, que siguin els únics dispositius de còpia de seguretat; també hi ha CD i DVD, els discos durs, els robots de grans discos de còpia, els servidors FTP o de fitxers, etc.

Els DVD són els dispositius de còpia de seguretat més estesos entre les petites i mitjanes empreses. Aquests dispositius també són els més utilitzats entre els usuaris domèstics que tenen necessitat de fer còpies de seguretat dels documents. L'èxit d'aquest dispositiu el trobem en el cost que té. Avui dia una gravadora de DVD té un cost molt baix. La limitació que té aquest dispositiu és la capacitat d'emmagatzemar informació, que és de 4,7 GB o 9,6 GB. Tot i que hi ha DVD regravables, la majoria de la gent fa servir els discos que només es poden gravar una vegada (si la còpia surt malament, hem de llençar el disc) perquè al final són molt més còmodes de fer servir, ja que no cal formatar-los i tenen un cost molt baix.

Les cintes han estat des del començament els dispositius de còpia de seguretat més utilitzats, ja que anteriorment no existien medis on poder guardar grans quantitats d'informació. Actualment són poques les empreses que, tot i requerir una gran capacitat de còpia de seguretat, fan servir les cintes com a dispositiu de còpia, ja que han quedat substituïdes pels grans robots de còpies de seguretat amb discos extraïbles i els servidors virtuals al núvol, on es poden fer les còpies directament sense tenir els problemes que poden tenir les còpies en local i l'emmagatzemament de les cintes.

Tot i això, hi ha petites i mitjanes empreses que encara fan servir les cintes magnètiques ja que tenen força avantatges:

1) La capacitat d'emmagatzemar informació. Poden arribar a emmagatzemar fins a 600 GB o més.

2) La capacitat d'ús. Una cinta es pot utilitzar moltes vegades.

Però l'inconvenient més gran és el preu i la lentitud que tenen. Aquesta lentitud es deu al fet que les cintes tenen accés seqüencial, és a dir, que per a arribar al registre 3 ha de passar primer per l'1 i pel 2; per tant, si es vol recuperar un fitxer que és al final de la cinta, s'ha de recórrer tota la cinta abans de recuperar-lo.

Hi ha moltes marques i dispositius de cinta. Gairebé cada marca utilitza una nomenclatura tipus de cinta diferent. Hi ha, però, dos tipus de cinta molt implantats en el mercat: les cintes DAT i les DLT.

Aquesta mena de nomenclatura ens indica la capacitat de la cinta sense comprimir i la capacitat amb les dades comprimides.

La cinta DLT clàssica té una capacitat de 40 GB a 80 GB. Actualment han sortit al mercat dispositius més moderns, que fan servir formats semblants al d'aquesta cinta. Són els anomenats *super-DLT*, que poden arribar a emmagatzemar de 300 GB a 600 GB d'informació. Els dispositius de cintes més freqüents en el mercat són els que tenen capacitat per a una sola cinta, però també n'hi ha amb capacitats superiors.

L'inconvenient és clarament el preu. Aquests dispositius són molt cars i, tot i que les cintes són cada vegada més ràpides, l'accés seqüencial sempre és un desavantatge. En resum, igual que hem de definir una política de còpia de seguretat que satisfaci els nostres requisits, hem de triar un dispositiu de còpia de seguretat que s'adapti a les nostres necessitats. Els factors que hem de tenir en compte són la capacitat d'informació de la qual volem fer una còpia de seguretat i el preu que estem disposats a pagar.

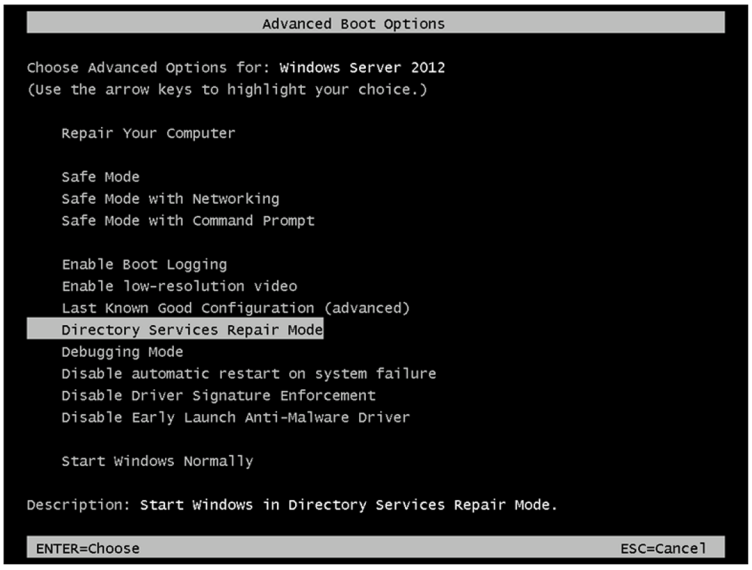
3. Sistemes de recuperació en el Windows Server 2012

A vegades, quan es produeix un error en el sistema, és possible solucionar el problema amb els mecanismes que proporciona el Windows. Vegem a continuació algun d'aquests mecanismes.

3.1. Arrencada en mode segur

Quan es produeix un error greu del sistema que fa que es quedi bloquejat, o que es reinicii automàticament o s'apagui l'ordinador, el sistema farà que en l'arrencada surti el menú d'opcions. A més, podem fer que surti un menú d'arrencada si premem la tecla F8 quan arrenca el sistema i tot just surt el logotip de Windows.

Opció d'arrencada del sistema



Les diferents opcions del menú d'inici que hem mostrat en la figura anterior ens permeten iniciar el sistema de diferents maneres:

1) Mode segur. Permet iniciar el sistema amb el mínim de controladors i serveis necessaris.

2) Mode segur amb funcions de xarxa. Igual que el mode segur, però habilita els controladors i serveis necessaris per a utilitzar la xarxa.

3) Mode segur amb símbol del sistema. Igual que el mode segur, però s'obre una sessió de línia d'ordres, en lloc de l'escriptori del Windows.

4) Habilitar el registre d'inici. Crea un arxiu de registre de totes les incidències d'inici dels components del sistema a mesura que es carreguen. Aquest arxiu de registres s'anomena *nrblog.txt* i es troba en la carpeta del Windows (per exemple, c:\windows). La resta d'opcions d'inici també creen aquest arxiu de registre (excepte l'opció d'utilitzar l'última configuració coneguda).

5) Habilitar el mode VGA. Inicia el sistema en mode VGA en comptes d'utilitzar el controlador de vídeo habitual.

6) L'última configuració bona coneguda. Inicia el sistema utilitzant la mateixa configuració que l'última vegada en què s'ha iniciat correctament el sistema, és a dir, l'última sessió en què no ha fallat cap controlador o servei en iniciar el sistema.

7) Mode de restauració dels serveis de directori. Permet recuperar la base de dades del directori actiu. Aquesta opció només és vàlida per a controladors de domini que ja estiguin configurats com a tals.

8) Mode de depuració. Serveix per a iniciar el sistema enviant informació de depuració mitjançant un cable de sèrie a un altre equip connectat, en el qual s'està executant un depurador.

9) Deshabilita l'arrencada automàtica en cas de detectar problemes greus en el servidor. Això pot ser útil en casos en que s'estigui configurant el maquinari.

10) Deshabilitar la comprovació dels controladors signats.

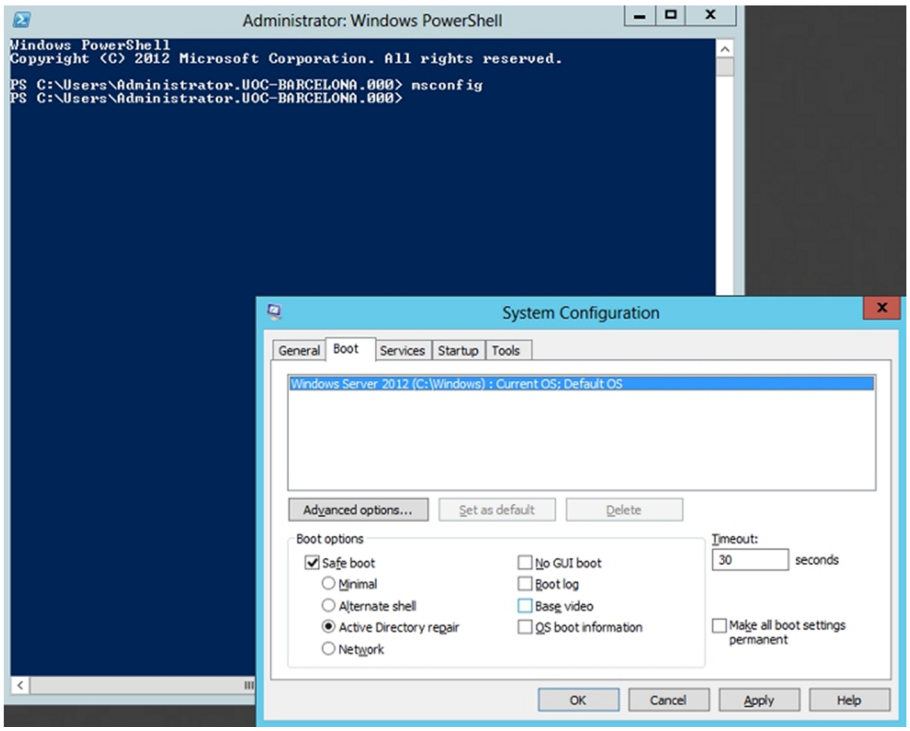
11) Deshabilita el llançament ràpid del controlador (*driver*) antimaliciós (*anti-malware*), per si tenim problemes amb aquest.

Un cop es reinicia en mode segur, s'haurà d'iniciar la sessió dins el servidor amb el domini de la màquina i l'administrador local, ja que el servidor de domini, el servidor de noms (DNS) i altres servidors deixaran de funcionar perquè no arrencarà el servei i es podran fer tasques de manteniment sense afectar tot el servei.

També es pot iniciar aquesta pantalla d'arrencada a partir del programa de configuració `msconfig.exe`, on podem fixar les diferents opcions que es vol en el moment de fer l'arrencada del sistema. En la figura següent es mostra aquesta aplicació. Es pot configurar perquè arrenqui uns serveis determinats, en mode segur, etc.

Un cop s'hagin solucionat els problemes i es vulgui tornar al sistema normal d'arrencada, s'ha de tornar a entrar al configurador d'arrencada (`msconfig.exe`) i desmarcar que s'iniciï en mode segur; altrament, tornaria a arrencar en aquesta mateixa configuració.

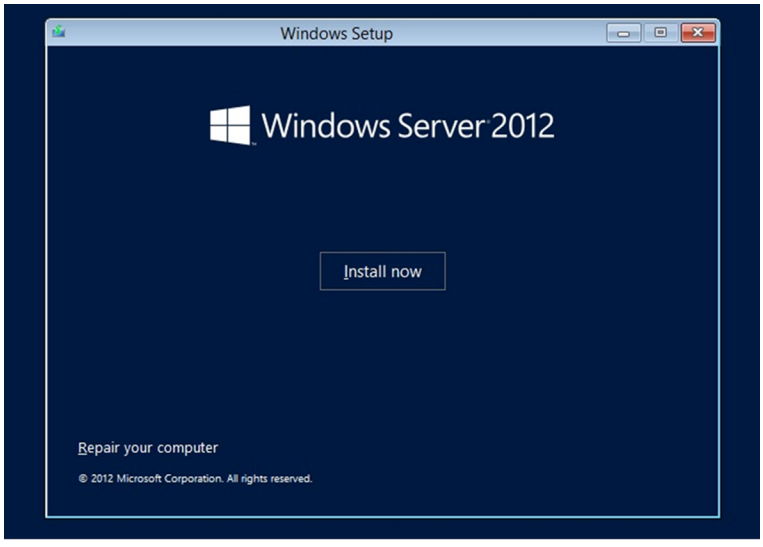
Configuració de l'arrencada del sistema



3.2. Sistemes de recuperació del Windows Server 2012

Quan volem recuperar un sistema en el qual no arrenca el mode gràfic, hem de recórrer a eines que ens proporciona el sistema operatiu, a les quals podem accedir arrencant amb el CD d'instal·lació del sistema. Per a totes aquestes eines, hem d'iniciar la instal·lació del sistema operatiu. Per al cas de la consola de recuperació, hem de deixar que inicií la instal·lació i, en el primer quadre de diàleg, triar l'opció de Recuperar el servidor, tal com mostra la figura següent.

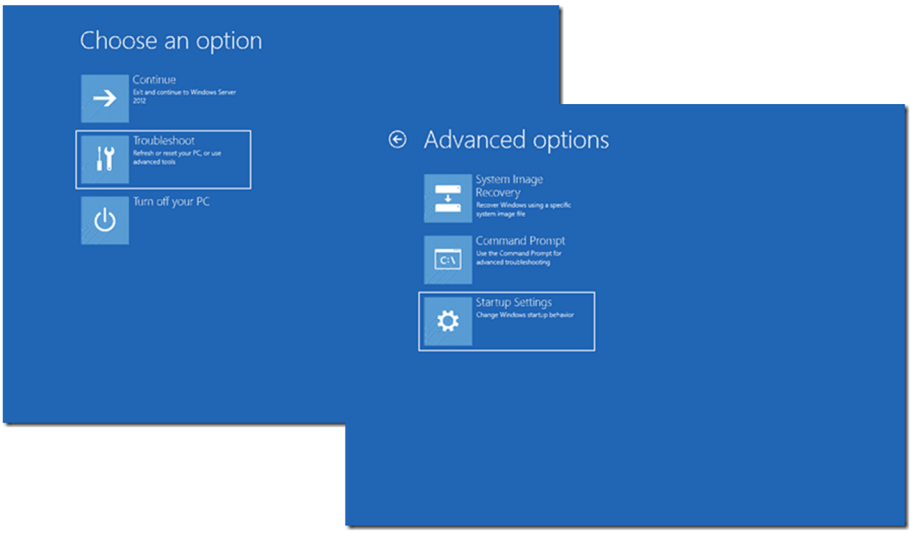
Pantalla per a recuperar el sistema



Un cop s'inicia el sistema en mode reparació, apareixen unes pantalles en les quals es pot triar el que es vol fer: com per exemple, iniciar una consola on poder interactuar amb el sistema orecuperar el sistema a partir d'una còpia

de seguretat feta amb anterioritat des del sistema operatiu amb el Windows Backup Server, si s'ha fet de tot el sistema, seleccionant la opció de *System Image Recovery*. Per tant, un cop tinguem el sistema completament instal·lat i configurat, és molt adient fer-ne una còpia sencera, i fins i tot poder-la fer regularment, ja que això ens permetrà poder recuperar tot el sistema d'una manera molt ràpida i poder tenir en producció el servidor tan aviat com sigui possible. L'avantatge de poder fer això en lloc de reinstal·lar tot el sistema una altra vegada des de l'inici és considerable, a més de poder recuperar tot el sistema operatiu net en el cas que s'hagi tingut una intrusió dins el sistema. La figura següentmostra les opcions que es poden dur a terme amb aquesta eina de recuperació del sistema.

Pantalles d'eines de recuperació del sistema



Queda a la nostra discreció fer les tasques necessàries per a recuperar el servidor de la fallada. Per exemple, si ens sembla que la fallada es deu a un servei instal·lat últimament, el podem parar des d'aquesta consola.

4. Plans de risc

Una de les mesures principals per a assegurar la continuïtat dels serveis és determinar els riscos a què ens enfrontem davant una fallada en el sistema. Això implica conèixer l'abast dels serveis crítics que hi estan involucrats, la incidència interna i externa que tenen i haver mesurat les possibles conseqüències d'una fallada. Per tant, cal preparar un conjunt d'accions que s'han de prendre en cas de fallada, tenint en compte que pot ser per un problema amb el maquinari o amb el programari (com virus, troians, atacs maliciosos, etc.). En això consisteix, precisament, un pla de risc.

En el procés de formulació del pla de risc, l'objectiu principal és complir totes les tasques necessàries de la fase proactiva, que és la fase anterior al risc. Una vegada es produeix l'esdeveniment, comença la fase reactiva i s'ha d'executar el pla corresponent.

Per a preparar un pla de risc, el primer pas és identificar els riscos a què estem sotmesos. Per això hem de determinar quins riscos ens poden provocar una fallada en el sistema i determinar quins són probables, quins són possibles i quins són crítics. Després, hem de determinar les prioritats d'aquests riscos basant-nos en l'entorn de la nostra empresa. És a dir, tot i que els riscos informàtics són semblants per a la majoria de les empreses, la prioritat que s'assigna a aquests riscos depèn de l'ús informàtic que duu a terme l'empresa.

Una vegada tenim identificats i prioritzats els riscos, hem de decidir quins generaran un pla de risc i quins no cal tenir implementats en un pla com aquest, a més de les característiques que ha de tenir aquest pla.

Per elaborar un pla de risc, per a cadascuna de les funcions que el componen, hem d'analitzar totes les alternatives de solució que permetin que els serveis continuïn funcionant encara que hi hagi algun inconvenient. Després d'analitzar totes les alternatives, confeccionem el pla. Les solucions del pla poden ser tècniques, d'atenció, de subministrament o solucions momentànies per a problemes puntuals (per exemple, en cas d'una fallada en el subministrament elèctric, l'ús d'un generador) o una combinació de tots aquests tipus de solució.

En generar el pla de risc s'ha de tenir en compte la identificació de les condicions que impliquen que es posi en marxa. En termes generals, el pla de risc ha de contenir els punts següents:

- **Objectiu del pla**. S'han d'indicar els components dels serveis crítics que es pretenen cobrir en relació amb el risc que es té en consideració. Aquests

components poden variar, i també el grau de cobertura que tenen, per als diferents riscos analitzats.

- **Criteri per a executar el pla**. Són les condicions amb les quals es considera que s'ha de començar a aplicar el pla de risc.

- **Temps esperat màxim de durada del pla**. És a dir, el temps màxim que es pot continuar operant amb aquestes condicions de risc.

- **Papers, responsabilitat i autoritat**. Això és clau per a la bona marxa del pla de risc. S'ha de determinar molt clarament quin és el paper de cadascun dels sectors de l'organització davant el risc i com s'alteren els procediments habituals per a donar lloc als procediments de risc. Aquí cal implicar molt clarament les persones i els departaments i marcar què és el que ha de fer cada persona i en quin moment.

- **Requisit de recursos**. Quins recursos es necessiten per a operar en el mode risc i quins dels recursos utilitzats habitualment no s'han de fer servir. Això ha d'estar documentat i verificat degudament, de la manera més exhaustiva que es pugui, fins i tot amb una relació de preus de tot allò que calgui adquirir i les prioritats.

Per entendre més bé com és un pla de risc en posarem un exemple. Imaginem-nos que la nostra empresa és una universitat a distància en la qual tots els alumnes fan les classes mitjançant l'ús del servidor web. El servidor té una targeta controladora de discos SCSI i els discos són externs (són fora del servidor) i es connecten al servidor mitjançant un cable SCSI a la controladora de discos; a més, tenim una altra màquina igual (el mateix maquinari) per a substituir el servidor en cas de fallada en el maquinari. Ara imaginem-nos que s'ha danyat la font d'alimentació del servidor principal.

El pla de risc s'ha d'assemblar a aquest:

1) Objectiu del pla: el servei web ha d'estar parat tan poca estona com es pugui.

2) Criteri d'execució del pla: quan es detecta que ha caigut el servidor web.

3) Temps esperat d'execució: cinc minuts.

4) Papers: personal de serveis informàtics que està de guàrdia en aquell moment. Per tant s'haurà de tenir en compte que hi ha d'haver persones de l'organització pendent d'alguna alarma. Dependrà de cada tipus d'organització i de quin temps d'espera es pot tenir. Si posem que han de ser només cinc minuts, s'haurà de tenir una persona les vint-i-quatre hores i els

set dies de la setmana a l'empresa per si salta una alarma com aquesta. En el cas de poder allargar el temps de resposta, amb un telèfon de contacte serà suficient i no caldrà tenir personal les vint-i-quatre hores del dia a l'empresa.

5) Requisits de recursos: un servidor de recanvi amb el mateix maquinari. El personal de serveis que està de guàrdia en el moment en què detecta que el servidor de pàgines web no funciona ha de fer el següent:

- Parar el servidor web (si la màquina està engegada).
- Desconnectar el cable SCSI de la targeta controladora de discos del servidor web.
- Connectar el cable SCSI a la targeta controladora de discos del servidor de recanvi.
- Engegar el servidor de recanvi.