Administració de servidors

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190190

Universitat Oberta de Catalunya

Índex

Introducció

Avui en dia els servidors ja no són ordinadors "de pel·lícula" que ocupen habitacions senceres, sinó que són ordinadors amb característiques especials de maquinari i de programari.

Si tenim el rol d'administrador, necessitem saber què tenen diferent dels ordinadors de sobretaula. Hem de saber què en podem esperar i què els podem demanar que facin. També és important tenir present tot el que hem de fer per a protegir-los, almenys físicament. Finalment, haurem de triar, configurar i mantenir el sistema operatiu.

Si tenim un rol més directiu, haurem de saber que els servidors són una peça clau en el sistema informàtic, ja que els ordinadors emmagatzemaran totes les dades i per tant és molt important tenir-los en les millors condicions possibles. Parar un servidor vol dir en molts casos parar el treball de molta gent de l'empresa.

Veurem quin maquinari hi podem connectar i quina és la configuració més adient depenent de la funció a què el vulguem destinar.

Cal tenir present que el servidor estarà connectat a la xarxa. Això n'afecta la configuració, i també s'ha de recordar que com a administrador de servidors hi ha un conjunt de tasques i de responsabilitats que hem de conèixer. Finalment, haurem de tenir cura de mantenir-lo i vigilar que sempre funcioni correctament.

Objectius

En els materials didàctics d'aquest mòdul presentem els continguts i les eines imprescindibles per a aconseguir les competències següents:

1. Conèixer les característiques que han de tenir els ordinadors que fan de servidors, els quals han de complir uns requisits de funcionament bastant estrictes.

2. Conèixer les característiques que han de tenir els sistemes operatius servidors, perquè han de complir unes funcions diferents i uns requisits de seguretat bastant estrictes.

3. Conèixer les possibles configuracions de servidors per a obtenir sistemes amb més bon rendiment. També comprendre les diferents combinacions i virtualitzacions de servidors amb objectius comuns o dispersos.

4. Saber els diferents tipus d'emmagatzematge, intern i extern, els seus components, configuracions i varietats per tal de garantir el rendiment i la seguretat del servidor.

5. Conèixer els diferents dispositius i polítiques de fer còpies de seguretat.

6. Conèixer els diversos components de maquinari que s'instal·len en un servidor per a poder obtenir un bon rendiment.

7. Conèixer les responsabilitats d'un administrador de servidors.

8. Saber com s'ha d'aplicar als servidors el concepte de seguretat.

1. Desmitificant el servidor

Quan es parla de servidors, hi ha una tendència generalitzada a creure que es tracta de màquines enormes que ocupen sales senceres i que es troben protegides en ambients especials i amb una seguretat de pel·lícula. En un principi, els servidors sí que ocupaven grans espais i tenien ambients especials. Fins i tot ara podem trobar alguns servidors centrals de tipus *host* o grups de servidors disposats físicament de manera que ofereixen aquest aspecte. Però el que és cert és que la majoria, individualment, mantenen una aparença molt semblant a una estació de treball qualsevol.

Així doncs, tot i que els servidors no són iguals a la imatge que tenim predefinida, sí que són àmpliament diferents en funcionalitat i servei a qualsevol ordinador personal.

> Avui els servidors no són diferents externament. El que varia és el programari i el maquinari instal·lats dins la carcassa externa.

Un servidor és una màquina que funciona 24 × 7 (vint-i-quatre hores els set dies de la setmana), i això vol dir que ha de tenir un maquinari preparat per a no parar mai (problemes d'escalfament) i suportar reparacions i la substitució de discos avariats en calent (sense apagar l'ordinador). També ha de poder aguantar centenars de peticions d'usuaris per mitjà de la xarxa amb temps de resposta acceptables. Fins i tot tenen sistemes perquè els usuaris accedeixin a la informació d'una manera selectiva, i gestionen cues d'impressió, mostren pàgines web, registren l'activitat total que es fa, gestionen el correu de l'organització i ja no ocupen habitacions senceres.

2. Funcions del servidor

Un servidor és un equip informàtic que posa recursos propis a disposició d'altres ordinadors (els clients). Per tant, actualment el concepte de servidor ja no està associat necessàriament a un ordinador.

Recursos d'un servidor

Els recursos que un servidor posa a disposició d'altres ordinadors poden ser dades, fitxers, aplicacions, impressora, disc, correu...

Podem distingir dos tipus de servidors:

- **Servidors físics**. Moltes vegades també s'anomenen servidors corporatius. És la quantitat d'ordinadors que hi ha en una organització dedicats exclusivament a tasques servidores.

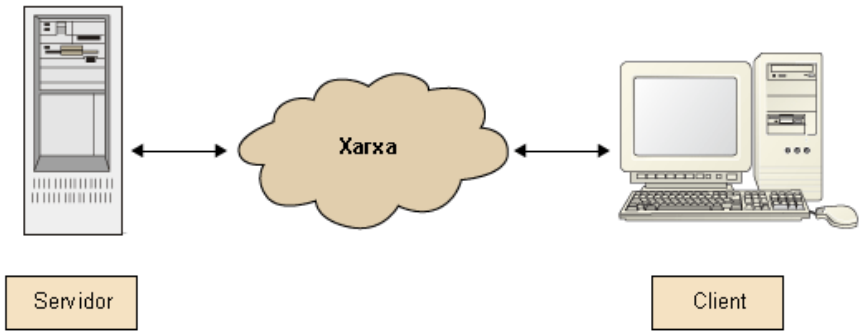
- **Servidors funcionals**. La quantitat de tasques que fan els servidors és molt gran. Conceptualment, un servidor proporciona recursos i, per tant, un ordinador físic pot donar servei a moltes coses. De la mateixa manera, un ordinador pot no estar dedicat a fer de servidor, però sí servir alguna cosa (**donar un servei**).

Amb les xarxes i la tecnologia client/servidor, un servidor és una aplicació que dóna (serveix) informació a un programa (client) que li demana mitjançant una connexió (normalment la xarxa) a partir d'un protocol.

Vegeu també

Sobre l'arquitectura client/servidor mireu més endavant l'apartat 4 en aquest mateix mòdul.

Esquema de l'arquitectura client/servidor



Així, doncs, podem trobar servidors de moltes coses: servidors de fitxers, servidors d'impressió, servidors web, servidors de notícies, servidors FTP, servidors de correu, servidors DNS, servidors buscausuaris[1].

(1)Servidors buscausuaris en anglès s'expressa com a *finger server*.

Com que són aplicacions, un ordinador pot oferir molts serveis a la vegada, és a dir, pot fer diverses funcions. Tindríem, doncs, un servidor físic que duu a terme funcionalment el paper de diversos servidors.

Normalment un servidor físic dóna diferents serveis, depèn bàsicament de quina destinació té i quina demanda té allò que serveix.

Exemple de serveis d'un servidor físic

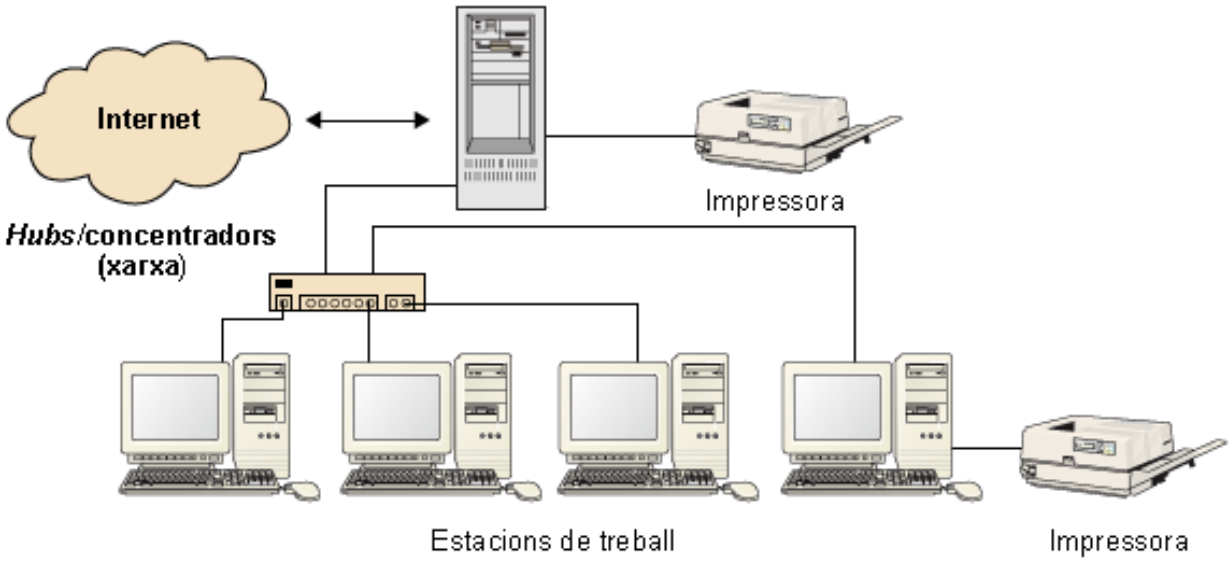
Una organització dedicada a la venda per Internet segurament tindrà un servidor físic dedicat a fer de servidor de web, mentre que en el cas d'una empresa que només tingui el catàleg dels seus productes, el servidor web estarà en un servidor que també ofereixi altres serveis com, per exemple, la comptabilitat (servidor de fitxers), els directoris d'usuari (servidor de fitxers) i el correu electrònic (servidor de correu).

Per tant, el nombre i la funció de servidors físics instal·lats depèn de l'activitat de l'organització, del programari que es faci servir i del pla estratègic (les futures ampliacions de programari i maquinari).

2.1. Requisits dels sistemes operatius en xarxa

La instal·lació del sistema operatiu (SO) en el servidor que triem ens ha de permetre una gran varietat de funcions necessàries. La idea de servidor està basada en la tecnologia client/servidor, però si a més permet una bona comunicació entre estacions de treball, molt millor. Amb la tecnologia de base tenim l'estructura següent:

Estructura de la tecnologia client/servidor



Per tant, l'SO[2] de xarxa ha de poder proporcionar bàsicament les funcions següents:

[(2)]Recordeu que "SO" és l'abreviatura de sistema operatiu.

- Servidor de fitxers:
  - Poder definir grups d'usuaris.
  - Compartir fitxers entre tots els usuaris.
  - Compartir fitxers entre els grups d'usuaris.

  - Que cada usuari tingui espai personal per a guardar la informació. El fet que estigui en el servidor en facilita la mobilitat i les còpies de seguretat.

- Servidor d'aplicacions:
  - Compartir programes entre tots els usuaris.
  - Compartir programes entre els grups d'usuaris.

- Servidor d'impressió:
  - Compartir les impressores.

- Servidor de correu:
  - Enviar i rebre missatges.

Tot això amb les restriccions de seguretat i permisos adients. Si a més a més cal que en la xarxa hi hagi seguretat complementària, com ara un tallafoc[3] o altres tipus de servidors –com un servidor web o un servidor de bases de dades–, s'hi han de poder instal·lar o s'ha de posar un altre servidor físic per a instal·lar-los-hi. En aquests casos, la comunicació entre els servidors és una qüestió important.

(3)Tallafoc en anglès s'expressa com a *firewall*.

3. Elements del servidor

Un servidor és un ordinador amb una configuració de maquinari i de programari ajustada a la funció que ha de dur a terme.

D'entrada els components són els mateixos que per a un ordinador de sobretaula. Així en un servidor podrem trobar monitor, teclat, ratolí, lector òptic (DVD), memòria RAM, placa de comunicacions, unitats d'emmagatzematge (discos durs), unitat de control de procés (CPU[4]), font d'alimentació, placa gràfica i placa base.

(4)La sigla "CPU" correspon a l'expressió anglesa *central processing unit*.

Alguns dels components no han de ser especials (el monitor, el teclat, el ratolí i la placa gràfica), mentre que pel que fa als altres components sí que n'hi ha de prestacions especials i s'han de mirar a fons.

3.1. Memòria RAM

Tots els usuaris demanen (fan peticions) a un servidor. Per tant, és important que ens pugui respondre com més aviat millor. Per aquest motiu, una bona quantitat de memòria RAM és molt important, i com més ràpida sigui la RAM que s'hi instal·li, millor. Si es tracta d'un servidor de bases de dades, aleshores la qüestió és molt més crítica i hem d'instal·lar la quantitat de RAM que recomana el venedor del producte de bases de dades per a assegurar un funcionament òptim.

És molt necessària una gran quantitat de memòria RAM.

3.2. Unitat de control de procés

En contra del pensament general, i exceptuant que sigui un servidor de bases de dades amb grans transaccions i operacions de bases de dades complexes, la CPU[5] no és excessivament crítica per al bon funcionament d'un servidor. n'hi ha prou amb una bona CPU i no calen sistemes multiCPU, en la majoria dels casos. La CPU és necessària en processos que demanen grans quantitats de càlcul, però no és el cas general d'un servidor de fitxers, d'un servidor d'impressió o d'un servidor web, per exemple. Podria ser el cas d'un gran servidor de bases de dades al qual es fessin moltes peticions que impliquessin consultes complexes i, per tant, molt de moviment en les taules, però segurament llavors seria

(5)Recordeu que "CPU" és la sigla d'unitat de control de procés.

més un indicador del fet que algun element de la base de dades està mal dissenyat, perquè aquest tipus de consultes no acostumen a ser freqüents sobre una base de dades (excepte si hi ha milers d'usuaris).

Generalment, la CPU no és crítica.

3.3. Placa base

És essencial que la placa base sigui de molt bona qualitat per a assegurar que hi ha una bona velocitat de transmissió entre tots els components del servidor. El bus del sistema forma part de la placa base[6] i és el component que permet la comunicació entre tots els dispositius de dins de l'ordinador. Entre una placa de bona qualitat i una que no ho sigui, el rendiment pot baixar d'una manera apreciable. El gran problema és que costa molt de detectar perquè tot funciona, encara que lleugerament més lent.

[6]La placa base també s'anomena *placa mare* o amb el seu equivalent anglès, *motherboard*.

La placa base és vital per al servidor.

3.4. Placa de comunicacions

La placa de comunicacions és el punt de comunicació entre el servidor i "tot el món". Per tant, la seva qualitat i velocitat determinen el comportament del servidor envers la xarxa. És un component crític.

Una placa 10/100 de parell trenat a un concentrador o a un commutador a 100 Mb ja no és una bona solució per a tenir un servidor ben connectat. Actualment, la gran quantitat de dades que circulen per la xarxa interna de l'organització fa que la connexió dels servidors ja es faci amb plaques de comunicació d'1 gigabyte, que donen velocitats de transferència molt altes. Com més ràpida sigui la connexió del servidor amb la xarxa, abans podrà atendre les demandes de les estacions de treball i anirà més descarregat (o més càrrega podrà suportar sense col·lapsar-se).

La placa de comunicacions determina la capacitat de transmetre informació a la xarxa del servidor.

3.5. Disposició física del servidor

La disposició física dels servidors és variada. Des de caixes especials per suportar l'escalfament (sobretot si tenen moltes unitats de disc) fins als sistemes rac on el teclat i la pantalla per a controlar els ordinadors s'implementen via xarxa.

Finalment trobem els sistemes *Blade*, on cada servidor s'integra com una làmina dins d'una estructura (*blade center*) on es comparteixen recursos, com l'accés a la xarxa, a una xarxa *Storage Area Network* (SAN), fonts d'alimentació, ventiladors...

Servidors en *Blade* dins d'un *blade center*

4. Configuracions de servidors

Les diverses necessitats d'una organització fan que sovint un equip no sigui suficient. De manera que és habitual que les organitzacions tinguin més d'un servidor físic per assolir els seus objectius. Podem trobar, doncs, un servidor que dugui a terme una o moltes tasques o molts servidors treballant per un propòsit comú. També és possible trobar servidors molt diferents entre ells, agrupats en un mateix espai duent a terme tasques diverses.

Aquestes combinacions, moltes vegades heterogènies de servidors, es basen en la funcionalitat. Així, si per exemple volem un servei de correu que difícilment falli, posarem un clúster de correu en alta disponibilitat. Això representa almenys dos servidors exclusivament dedicats al correu. Si a més ens cal un servei de fitxers molt gran, llavors posarem un servidor dedicat a *Network Attached Storage* (NAS) amb una llibreria de còpia de seguretat[7].

[(7)]Còpia de seguretat en anglès s'expressa com a *backup*.

Com podem veure, és la necessitat de l'organització el que configura l'estructura de servidors. A causa de l'entorn dinàmic de les organitzacions, s'hauria de fer una planificació inicial per a preveure, tant com sigui possible, les ampliacions que hi pugui haver per a no fer despeses i tasques d'organització del sistema informàtic que siguin insuficients en poc temps.

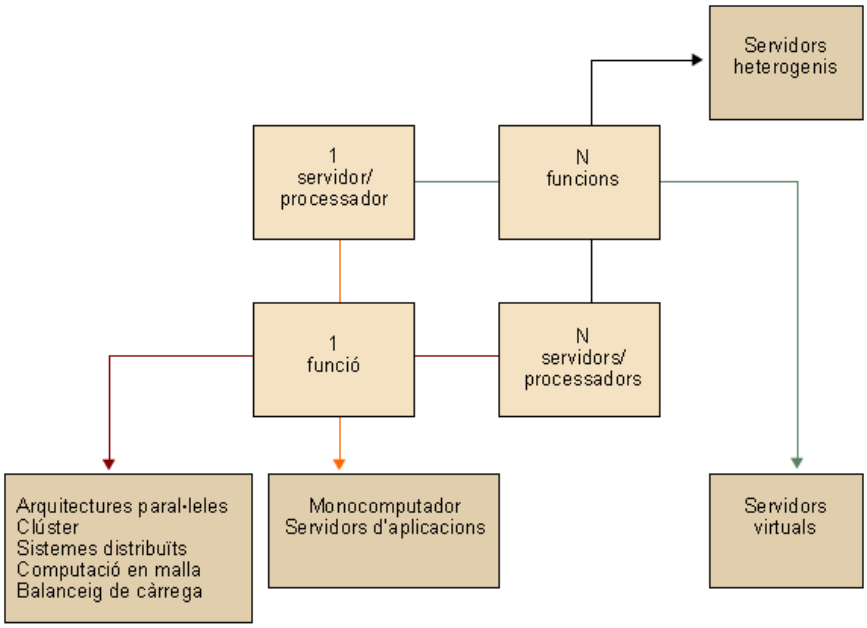
Vegeu també

Sobre com planificar el departament vegeu el mòdul "El sistema informàtic dins l'organització".

Aquesta gran varietat, atenent a la configuració i funció, fa necessària una classificació de les configuracions dels servidors. Aquesta classificació no pretén ser exhaustiva, sinó orientativa i didàctica, tot sabent que hi ha altres classificacions.

La configuració dels servidors ha de cobrir les necessitats específiques de l'organització.

Diagrama d'encreuaments



Aquest diagrama d'encreuaments defineix conceptualment els diferents tipus de servidors i els serveis que aquests poden oferir als seus clients connectats:

- **Un servidor/processador, una funció**. És el nivell més senzill de servidor, un sistema físic dedicat a una sola funció. Per exemple, un ordinador realitzant tasques de gestió de correu (servidor d'aplicacions).

- **Un servidor/processador, *N* funcions**. Si disposem d'un ordinador poc utilitzat quant a recursos, podem aprofitar aquest romanent per a oferir altres serveis als clients. Així doncs, tenim un ordinador optimitzant recursos i amb diverses funcions de servei.

- ***N* servidors/processadors, una funció**. En la nostra organització podem tenir serveis crítics, ja sigui per necessitat de servei, seguretat, o rendiment, que fan necessari un nombre de recursos molt important i escalable. Aquesta necessitat, desenvolupa les arquitectures on una sola tasca és tractada per més d'un ordinador.

- ***N* servidors/processadors, *N* funcions**. Quan diverses funcions són tractades per diferents ordinadors, tenim un sistema de servidors heterogeni, on poden aparèixer un gran nombre de combinacions possibles.

4.1. *Host* o sistema centralitzat

Podem distingir dos tipus de sistemes centralitzats: servidors virtuals i servidors d'aplicacions.

4.1.1. Servidors virtuals

Els servidors virtuals basen el funcionament en la tecnologia de la virtualització. La virtualització, essencialment, és donar a una computadora la possibilitat de realitzar el treball de múltiples computadores, compartint els recursos a través de diversos entorns. Típicament s'ha referit a una sola computadora capaç de fer treballar al mateix temps diferents sistemes operatius i serveis de forma segura.

Podem afirmar, doncs, que un servidor virtual és aquell servidor capaç de realitzar el treball de diversos servidors compartint els recursos del sistema, mitjançant un o més sistemes operatius de forma segura.

Els servidors virtuals tenen força avantatges que els fan atractius:

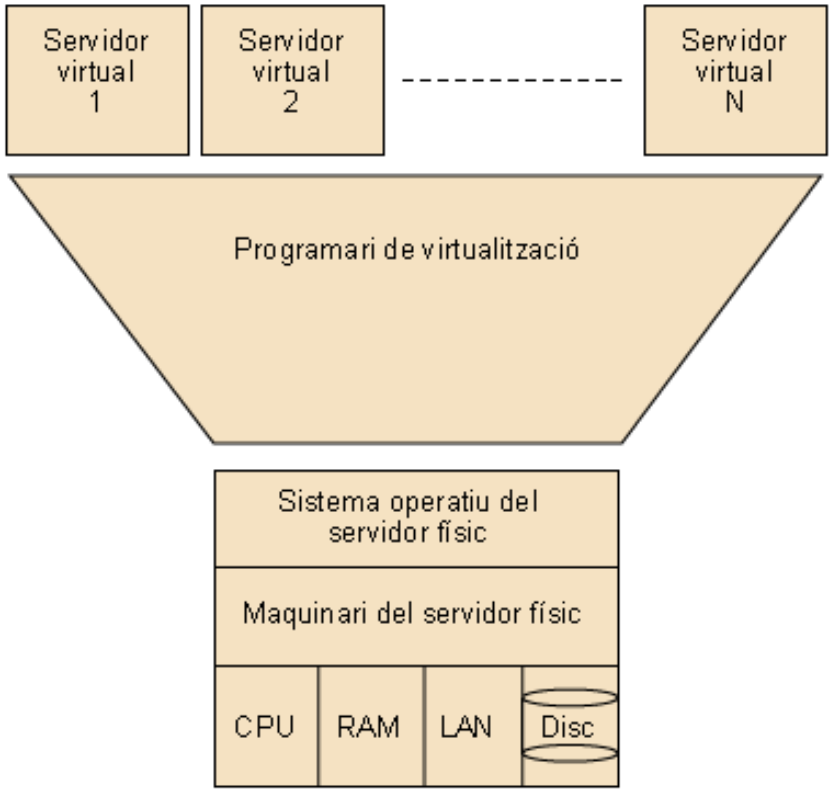
- Reducció del nombre de servidors físics.
- Reducció de l'espai dins el centre de dades.
- Reducció del consum d'energia.
- Compartició de recursos i eficiència d'utilització.
- Centralització i simplificació de la gestió.

Hi ha diversos sistemes de virtualització, depenent de la plataforma tecnològica del servidor físic.

Virtualitzadors comercials

Alguns virtualitzadors comercials coneguts són VMWARE, Windows Virtual Server, Linux Virtual Server, etc.

Esquema de servidor virtual



4.1.2. Servidors d'aplicacions

Un servidor d'aplicacions és un servidor avançat que permet gestionar aplicacions i tots els recursos necessaris associats com l'accés a Base de Dades, seguretat, manteniment... Un servidor d'aplicacions es relaciona normalment a un sistema de tres capes:

1) Primera capa[8]: Capa d'interacció amb l'usuari, basada en navegadors gràfics.

2) Capa intermèdia[9]: Servidor d'aplicacions en xarxa local.

3) Tercera capa[10]: servidor de base de dades.

Basat en la tecnologia Java 2 Platform, Enterprise Edition (J2EE), el servidor d'aplicacions és una màquina virtual Java[11] (JVM) que executa aplicacions d'usuari. El servidor d'aplicacions col·labora amb el servidor web per a oferir una resposta dinàmica i personalitzada a cada petició de client. A més, també dóna resposta avançada a codi d'aplicació, miniaplicacions de servidor[12], JavaServer Pages (JSP), **enterprise beans** i les classes que els donen suport.

(8)Primera capa en anglès s'expressa com a *front-end*.

(9)Capa intermèdia en anglès s'expressa com a *middle-tier*.

(10)Tercera capa en anglès s'expressa com a *back-end*.

(11)Màquina virtual Java en anglès s'expressa com a *Java Virtual Machine*.

(12)Miniaplicacions de servidor en anglès s'expressa com a *servlets*.

Un servidor d'aplicacions pot gestionar un gran nombre d'aplicacions, connexions a base de dades i recursos, la qual cosa fa que sigui un sistema versàtil, segur i de futur. Hi ha avantatges clars en emprar-los:

Vegeu també

Vegeu el mòdul "Administració del web" per a repassar aquests conceptes.

- **Integritat**. Gràcies a la centralització de les aplicacions, s'eviten els problemes d'actualitzacions i migracions en els sistemes client. Qualsevol canvi es fa centralitzat disminuint al mínim el risc.

- **Configuració centralitzada**. Els canvis de configuració de l'aplicació, com els accessos a la BD, es fan de forma centralitzada.

- **Seguretat**. El servidor d'aplicacions es converteix en el punt central d'accés a les dades, disminuint la diversitat i fent més fàcil una bona defensa.

- **Rendiment**. Es fa gestionant els accessos clients al servidor d'aplicacions i d'aquest al servidor de base de dades.

Servidors d'aplicacions comercials

Hi ha diversos servidors d'aplicacions al mercat. Aquesta és una llista dels més emprats: JBoss, IIS, WebSphere, Bea Weblogic, Tomcat...

4.2. Agregació de *hosts* o sistema distribuït

Podem distingir tres tipus de sistemes distribuïts: sistemes de balanceig de càrrega, clústers i *grids*.

4.2.1. Balanceig de càrrega (*Load balancers*)

Balancejar una càrrega significa dividir el total de treball que un sistema o computadora ha de fer entre dos o més sistemes o computadores.

Així doncs, aquesta divisió de càrrega permet realitzar el mateix treball en una porció de temps més reduïda, o, el que és el mateix, permet realitzar més càrrega de treball en el mateix temps total.

En organitzacions que donen servei web, botigues en línia (*on-line*), bancs, etc. es fa servir el balanceig de càrrega per a distribuir les peticions d'accés al web entre els diferents servidors de pàgines web que tenen a l'empresa o organització.

Els següents són alguns conceptes generals sobre el balanceig de càrrega:

- El balanceig de càrrega es pot implementar per maquinari, programari o una combinació dels dos.

- El balanceig de càrrega és especialment indicat per a entorns en què és molt difícil preveure el volum de càrrega de treball.

- El factor de divisió de càrrega es pot definir, donant més o menys càrrega a cada un dels sistemes implicats. Aquesta característica és la **càrrega asimètrica**.

4.2.2. Sistemes clúster

Un clúster és un grup de computadores interconnectades que treballen conjuntament en la solució d'un problema. Aquests sistemes constitueixen una solució flexible, de baix cost i de gran escalabilitat per a aplicacions que requereixen una elevada capacitat de computadora i memòria.

Un **clúster** és un grup d'equips independents que executen una sèrie d'aplicacions de forma conjunta i apareixen davant dels clients i aplicacions com un sol sistema.

Història dels clústers

Si mirem la història dels clústers, trobem que si bé no se sap la data exacta del primer clúster, es considera que la base científica del concepte del processament en paral·lel la va establir Gene Amdahl, que treballava a IBM, cap al 1967. El desenvolupament dels clústers ha estat sempre unit al de les xarxes de computadores, ja que des del començament es va buscar la unió dels sistemes informàtics per obtenir-ne més rendiment i capacitats. De totes formes, el primer clúster comercial va ser ARCNet, desenvolupat el 1977 per la corporació DataPoint. A partir d'aquí, tot un seguit de productes van popularitzar el concepte, fins a la posada en marxa del projecte Beowulf, el 1994, que implicava la interconnexió en xarxa local de computadors estàndard, i gestionava com aquests interactuaven entre si. La idea va ser un èxit que fins i tot la NASA va adoptar.

Característiques dels clústers

Els següents són les principals característiques dels clústers:

- Un clúster consta de 2 o més nodes connectats entre si per un canal de comunicació.

- Cada node únicament necessita un element de procés, memòria i una interfície per a comunicar-se amb la xarxa del clúster.

- Els clústers necessiten programari especialitzat, ja sigui com a aplicació o com a nucli.

- Tots els elements del clúster treballen per a complir una funcionalitat conjunta, sigui aquesta la que sigui. És la funcionalitat la que caracteritza el sistema.

Avantatges econòmics dels clústers

Els **avantatges econòmics** és una raó important per a la construcció de clústers. Redueix costos en la despesa inicial tant de planificació, d'instal·lació i també els costos associats al manteniment (el cost total[13]) comparats amb un "ordinador" de les prestacions equivalents.

[13]Cost total en anglès s'expressa com a *Total Cost of Ownership* (TCO).

Senzillesa dels clústers

La tecnologia que fa funcionar un clúster es basa en la unió d'elements senzills (que poden ser fins i tot ordinadors normals). I aquesta senzillesa és més beneficiosa quan parlem de disponibilitat de peces de recanvi (poden ser peces estàndard) o d'un temps d'aturada[14] reduït (no hi ha temps d'espera per a un tècnic enviat per la marca de l'equip).

[14]Temps d'aturada en anglès s'expressa com a *downtime.*

Disponibilitat dels clústers

La interconnexió de dos o més computadores treballant conjuntament en la solució d'un problema permet incrementar la disponibilitat de servei, ja que es divideix aproximadament el nombre de punts crítics de servei entre el nombre de nodes del clúster.

Escalabilitat dels clústers

Si l'SO del clúster ho permet, només cal connectar més equips a la xarxa del clúster, configurar-los correctament i ja tenim un clúster ampliat i millorat. Fins i tot millorant algun dels elements que formen part de cada node (memòria RAM o disc per exemple), s'obté una millora del rendiment o la disponibilitat.

Escalabilitat

L'**escalabilitat** és la capacitat d'un equip per a enfrontar-se a volums de treball cada cop més grans sense deixar de donar un nivell de rendiment acceptable. Hi ha dues classes d'escalabilitat:

- Maquinari o escalament vertical: basat en l'ús d'un gran equip amb una capacitat que augmenta a mesura que ho exigeix la càrrega de treball.
- Programari o escalament horitzontal: basat en l'ús d'un clúster fet de diversos equips de mitjana potència que funcionen de manera molt similar a com ho fan les unitats *Redundant Array of Inexpensive Disks* (RAID) de disc...

Rendiment dels clústers

L'increment de recursos assignats per a resoldre la mateixa càrrega de treball permet augmentar el rendiment del sistema com a conjunt.

Balanceig de càrrega dels clústers

La tecnologia de clúster de servidors per balanceig de càrrega millora la resposta a les peticions commutant aquestes entre els diversos nodes del clúster.

Vegeu també

Sobre el balanceig de càrrega vegeu el subapartat 4.2.1 en aquest mateix mòdul.

Components dels clústers

Els següents són els components d'un clúster:

- **Nodes**. Poden ser simples ordinadors, sistemes multiprocessadors o estacions de treball.
- **Sistemes operatius**. Han de ser de fàcil ús i accés, i a més permetre múltiples processos i usuaris.
- **Connexions de xarxa**. Els nodes d'un clúster poden connectar-se mitjançant una simple xarxa *Ethernet*, o es poden utilitzar tecnologies especials d'alta velocitat com *Fast Ethernet, Gigabit Ethernet*, Myrinet, Infiniband, SCI.
- **Programari intermediari**. El programari intermediari[15] és un programari que generalment actua entre el sistema operatiu i les aplicacions amb la finalitat de proveir una interfície única d'accés al sistema, denominada *Single System Image* (SSI), la qual genera la sensació a l'usuari que utilitza un únic ordinador molt potent.
- **Eines per a l'optimització i manteniment del sistema**. Migració de processos, *checkpoint-restart* (parar un o diversos processos, migrar-los a un altre node i continuar el seu funcionament), balanceig de càrrega, tolerància a fallades, etc.
- **Escalabilitat**. Ha de poder detectar automàticament nous nodes connectats al clúster per procedir a utilitzar-los.
- **Ambients de programació paral·lela**. Els ambients de programació paral·lela permeten implementar algoritmes que fan ús de recursos compartits: CPU[16], memòria, dades i serveis.

[15] Programari intermediari en anglès s'expressa com a *Middleware.*

[16] Recordeu que "CPU" és l'abreviatura de *Central Processing Unit*, en català Unitat de Control de Procés.

Tipus de clústers

Els clústers poden classificar-se segons les seves característiques. Es poden distingir:

- **Clústers d'alt rendiment**[17]. Son clústers que executen tasques que requereixen una gran capacitat computacional. Aquestes tasques poden comprometre els recursos del clúster per llargs períodes de temps.

[17] Clústers d'alt rendiment en anglès s'expressa com a *High Performance Clusters* (HPC).

- **Clústers d'alta disponibilitat**[18]. Son clústers dissenyats per a proporcionar disponibilitat i confiabilitat. La confiabilitat es proveeix mitjançant programari que detecta fallades del sistema i permet recuperar-se enfront d'aquestes, mentre que en maquinari s'evita tenir un únic punt de fallada.

(18)Clústers d'alta disponibilitat en anglès s'expressa com a *High Availability* (HA).

- **Clústers d'alta eficiència**[19]. Són clústers que estan dissenyats amb l'objectiu d'executar la major quantitat de tasques en el mínim temps possible.

(19)Clústers d'alta eficiència en anglès s'expressa com a *High Throughput* (HT).

4.2.3. Computació en malla (*Grid*)

La computació en *grid* o malla és un nou paradigma de computació distribuïda en el qual tots els recursos d'un nombre indeterminat de computadores són englobats com un únic superordinador de forma transparent.

Aquestes computadores englobades no estan connectades o enllaçades rígidament, és a dir, no tenen per què estar en el mateix punt geogràfic.

Els orígens de la computació en *Grid* es deuen a la idea de la compartició de recursos. La pràctica coneguda com a "computació distribuïda" ens porta als inicis de la informàtica. A finals dels anys 50 i principis dels 60, els investigadors es van adonar que necessitaven fer més eficients els sistemes que havien costat una fortuna; "els sistemes perden molt de temps esperant que els usuaris introdueixin dades". Els investigadors van raonar, aleshores, que diversos usuaris podrien compartir el sistema aprofitant el temps de processament no emprat.

El 1969 ja trobem una primera aproximació a la definició de *Grid* per part de Len Kleinrock que va suggerir profèticament:

> "Nosaltres probablement veurem l'extensió de les 'utilitats dels ordinadors', com les utilitats del corrent elèctric i telefòniques, que donaran servei a les cases i les oficines arreu del país."

El 1998, Carl Kesselman and Ian Foster van intentar una altra definició en el seu llibre *The Grid: Blueprint for a New Computing Infrastructure*.

Grid és la infraestructura de maquinari i el programari que proporciona un accés seriós, constant, penetrable i econòmic a capacitats computacionals d'alta qualitat.

En una revisió de la definició pels mateixos autors juntament amb Steve Tuecke, es va definir la computació *grid* com a compartició dels recursos coordinats i de la solució d'un problema en organitzacions virtuals dinàmiques i multiinstitucionals.

El sistema de computació en malla és un sistema que té les següents característiques:

1) Els seus recursos coordinats no estan subjectes a un control central. Un *Grid* integra i coordina recursos i usuaris que treballen amb diferents dominis – per exemple, estacions de treball d'usuaris enfront computadores centrals; unitats administratives diferenciades de la mateixa organització; o diferents organitzacions.

2) Utilitza un estàndard, obert, protocols i interfícies genèriques. Un *Grid* és fet de protocols genèrics i interfícies que tenen com a principals inconvenients l'autenticació, autorització, descobriment i accés als recursos. És important que aquests protocols siguin estàndards i oberts.

3) Entrega les qualitats no trivials de servei. Un *Grid* permet als recursos que la constitueixen ser emprats d'una forma coordinada entregant diferents qualitats de servei, relacionades per exemple amb el temps de resposta, rendiment, disponibilitat i seguretat, i/o l'assignació de múltiples recursos per conèixer les demandes dels usuaris, per tant, aquesta utilització dels sistemes combinats és significativament més gran que la suma de les seves parts.

Grid ofereix noves i més potents vies de treball, com els següents exemples:

- Portals científics: permet aprofitar els mètodes científics de resolució de problemes.

- Computació distribuïda: permet aprofitar la major capacitat que tenen les estacions de treball per a aconseguir uns substancials recursos de computació.

- Computació en temps real d'instrumentació: permet millorar la utilització d'aparells en temps real.

- Treball col·laboratiu: permet treballar en equip compartint recursos, però també els resultats dels diferents estudis per a la seva anàlisi.

5. Emmagatzematge

El disc dur és el component que emmagatzema la informació. És crític perquè, a més de contenir tota la informació de l'organització, és el dispositiu que dóna més sentit a tot el concepte de les xarxes. Sense els discos durs tota l'expansió de les xarxes pràcticament no tindria sentit, atès que gairebé totes les peticions que es fan a servidors són directament o indirectament peticions al disc.

La capacitat i velocitat dels discos són els dos aspectes bàsics i més importants a tenir en compte a l'hora de triar els discos que es volen posar en els servidors.

Quants discos ha de tenir el nostre servidor? Per a què els volem?

Un disc és un espai per a guardar informació que es divideix en parts anomenades particions.

Particions

Normalment no es recomana més de tres o quatre particions en un disc.

Si les particions poden ser de molts Gb, de què serveix particionar?

Particionar un disc té dues utilitats bàsiques. La primera, i més important, és que divideix el disc en zones independents. En estar formatada independentment, cada partició del disc és un disc lògic (no físic) diferent per l'SO. Per tant, en cas que per algun problema el sistema de fitxers quedi corromput i la informació de dins sigui inaccessible, el contingut es perd i la partició s'ha de reformatar. La resta de particions són accessibles i la informació es manté intacta. Fins i tot es pot recuperar tota la partició de la còpia de seguretat.

L'altra utilitat és que, en ser independents, poden estar formatades en sistemes de fitxers diferents. Per tant, fins i tot podem iniciar l'ordinador des de diferents particions, a partir de sistemes operatius diferents. s'utilitza molt en la preparació de màquines.

Tingueu present que si falla el disc físic, totes les particions queden inaccessibles i no es pot accedir a la informació que contenen.

5.1. Necessitats de l'organització

Les necessitats bàsiques de l'organització, a grans trets, són les següents:

- **Sistema**. La partició de sistema és necessària per a arrencar el servidor i perquè funcioni. Sempre es deixa una partició només per al sistema operatiu del servidor.

- **Usuaris**. La partició d'usuaris conté els directoris dels usuaris (les carpetes personals i si hi ha carpetes de grup).

- **Dades**. En la partició de dades normalment hi ha directoris amb dades de programes que han d'estar instal·lats localment en les estacions de treball, dades compartides per grups d'usuaris, i també hi pot haver un lloc per

a posar el "disc comú", que és una carpeta comuna a tota l'organització per a transferir coses.

- **Aplicacions bàsiques**. Les aplicacions que fan servir tots els usuaris. El programari base al qual necessiten accedir tots els usuaris i que ha d'estar a la xarxa. El permís ha de ser de lectura i execució per a tothom.

- **Aplicacions**. Aquesta partició conté les aplicacions que no són comunes a tothom, per això estan separades. Hi ha persones que les fan servir i d'altres que no. s'hi apliquen permisos per grups d'usuaris. A més de les aplicacions, molt possiblement hi trobarem dades associades a les aplicacions que funcionen.

- **Altres**. Tenint en compte les necessitats reals de l'organització, poden caldre altres particions. Servidors de bases de dades, particions per desenvolupament, etc.

Gestió informàtica

Aquesta partició només l'ha de veure el departament d'informàtica. Conté el programari, les eines, les preinstal·lacions, etc. necessaris perquè el departament pugui dur a terme la seva tasca i fer funcionar tot el sistema.

Per exemple, es pot utilitzar per a anar a una estació de treball i reinstal·lar un programari local (ofimàtica) sense dur CD-ROM ni res, només accedint a aquesta partició del disc amb els drets adients. Els usuaris no han de conèixer l'existència d'aquesta partició.

L'estructura final de tots els discos i les particions està condicionada per la necessitat, i no han de ser forçosament particions. Sempre és l'organització qui determina com es distribueix.

Les necessitats de l'organització determinen les particions que calen.

5.2. *Direct Attached Storage* (DAS)

Les tecnologies "tradicionals" d'emmagatzemament es basen en la connexió directa (física) del dispositiu al servidor o estació de treball. Com a conseqüència les aplicacions i els usuaris fan les peticions directament al sistema de fitxers. Fonamentalment hi ha quatre tipus de dispositius:

1) *Intelligent Drive Electronics* (IDE).

2) *Serial ATA* (SATA).

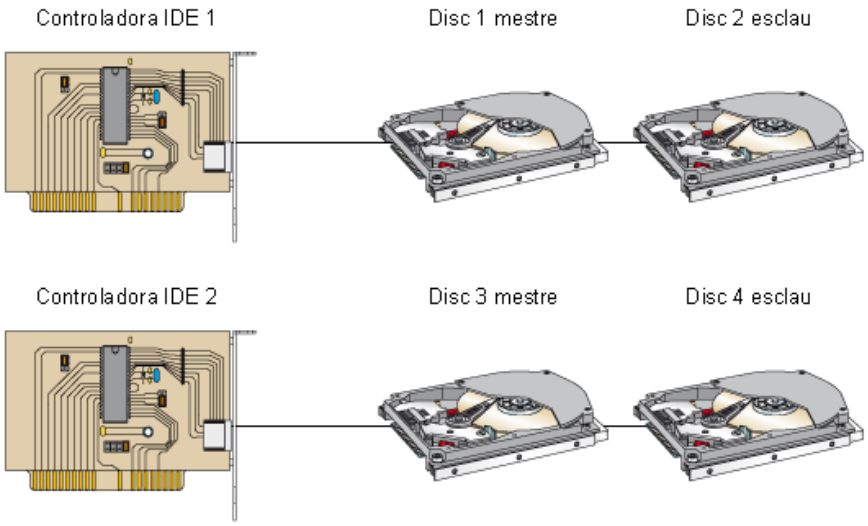
3) *Small Computer System Interface* (SCSI).

4) *Serial Attached SCSI* (SAS).

5.2.1. Discos *Intelligent Drive Electronics*

Els discos *Intelligent Drive Electronics* (IDE) poden ser de gran capacitat i són barats, amb l'inconvenient que no són gaire ràpids. Això fa que per a determinades situacions no sigui la millor opció en el servidor. A més a més, les arquitectures PC només permeten normalment fins a quatre discos IDE, perquè tenen dues controladores amb capacitat de dos discos cadascuna.

Discos suportats per les controladores IDE



Si hi ha algun DVD, necessita un d'aquests quatre llocs, per la qual cosa ens quedem amb només tres espais disponibles per a discos.

Els discos IDE es configuren de manera que un dels dos discos de la controladora és el mestre i l'altre, l'esclau. Això es fa modificant uns ponts[20] del disc, abans d'instal·lar-lo físicament dins de l'ordinador. Normalment un ordinador amb una arquitectura PC s'engega a partir del mestre de l'IDE 1 (disc 1, que, per tant, sempre hi ha de ser), sempre que no hi hagi controladors SCSI[21], que llavors es configura en la BIOS.

[20] Moltes vegades per a referir-nos als ponts es fa servir el terme anglès *jumper*.

[21] Recordeu que SCSI és l'abreviatura de *Small Computer System Interface*.

L'estàndard IDE va sorgir l'any 1981 amb una velocitat de transferència de 4 Mb/s aproximadament. Actualment, amb tots els canvis tecnològics i modificacions, s'ha arribat a ATA/ATAPI 5 (1999), amb una velocitat de transferència de 66 Mb/s aproximadament. Malgrat aquests avenços, té força limitacions, com per exemple que, mentre es fa servir el mestre de l'IDE 1, no es pot utilitzar l'esclau de l'IDE 1 (no es poden fer lectures paral·leles en la mateixa controladora).

Vista posterior d'un disc IDE

5.2.2. Discos *Serial ATA*

Els discos *Serial ATA* (SATA), amb els seus orígens situats al voltant del 2000, és la transició natural dels discos ATA o altrament anomenats IDE.

L'accés als discos es realitza en sèrie substituint a l'accés en paral·lel dels discos P-ATA (IDE). Aquest nou mètode d'accés proporciona millores respecte al seu antecessor:

- **Incrementa la velocitat de transmissió**. En una primera versió, aquesta velocitat es va situar en 1,5 Gb/s (SATA 150), però actualment es treballa amb una velocitat de transmissió de 3 Gb/s (SATA 300). s'està treballant per a aconseguir 6 Gb/s en un futur pròxim.

- **S'incrementa la longitud del cable de transmissió**. La longitud suportada actualment és de 2 metres.

- **Incrementa el nombre de dispositius SATA connectats**. Per a una estructura PC, es pot arribar fins a 16 dispositius SATA connectats a cada controlador (situat normalment a la placa mare).

- **Permet la connexió de discos "en calent"**. Permet afegir discos a la configuració, mentre el sistema està funcionant amb normalitat.

***External* SATA**

La tecnologia SATA ha permès la creació d'una petita variant: *external* SATA (eSATA), que facilita la connexió de dispositius externs.

5.2.3. Discos *Small Computer System Interface*

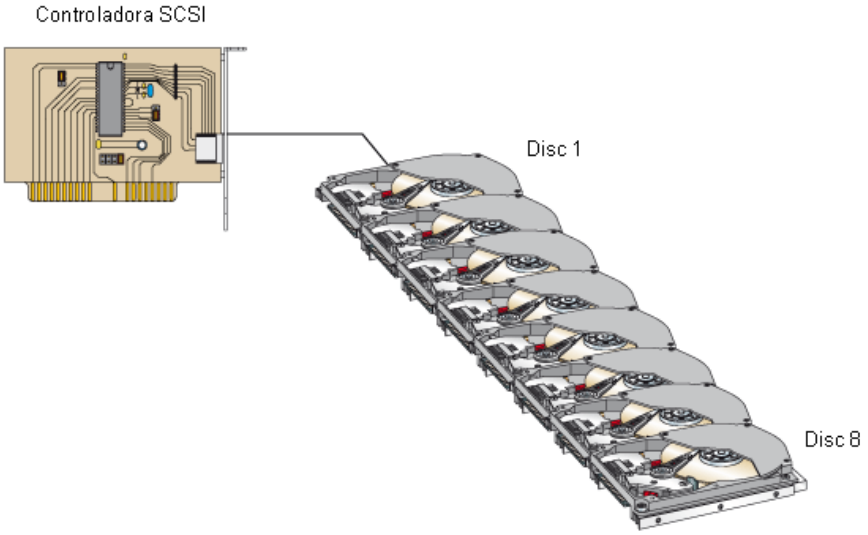
El disc *Small Computer System Interface* (SCSI) és un tipus de disc que és molt més ràpid, però també més car. És molt més adient per a servidors. Hi ha revisions d'SCSI, com per exemple l'anomenada Ultra Wide SCSI 2.

L'SCSI suporta fins a vuit dispositius per controladora (l'SCSI II fins a setze).

Dispositius en una cadena SCSI

Quan es parla de dispositius en una cadena SCSI es fa referència a discos durs, unitats de DVD, unitats de cinta, etc.

Cada controladora SCSI suporta vuit discos



La velocitat de transferència de les cadenes SCSI ha variat força amb les revisions, des de l'SCSI original, que anava a 5 Mb/s, fins a la darrera revisió, l'Ultra 640 SCSI, que té una velocitat de transferència de 640 Mb/s. Els busos SCSI permeten lectures i/o escriptures simultànies en la mateixa controladora i és, per tant, l'estàndard que s'utilitza en servidors corporatius.

En servidors d'arquitectura Unix també acostuma a ser un estàndard instal·lar discos durs SCSI, mentre que en arquitectures PC s'ha de tenir la precaució de fer-ho, ja que cal afegir un component de maquinari (una placa controladora) per a poder-ho suportar.

5.2.4. Discos *Serial Attached SCSI*

Igualment com succeeix amb els discos SATA, els discos *Serial Attached SCSI* (SAS) són l'evolució dels discos SCSI.

També, com succeïa amb SATA, SAS implementa la transmissió en sèrie entre el controlador i els dispositius, la qual cosa permet obtenir significatives millores:

- **Incrementa la velocitat de transmissió**. En la seva primera versió, aquesta velocitat s'ha situat en 3 Gb/s (SAS 3.0). s'està treballant per aconseguir 6 Gb/s en un futur pròxim.

- **S'incrementa la longitud del cable de transmissió**. La longitud externa suportada actualment és de 8 metres.

- **Incrementa el nombre de dispositius SAS connectats**. Per a una estructura PC, es pot arribar fins a 128 ports d'expansió de dispositius i fins a 16.384 discos SAS connectats.

- **Connexió de discos "en calent"**. Permet afegir discos a la configuració, mentre el sistema està funcionant amb normalitat.

Una bona política i gestió dels discos pot determinar el rendiment del servidor.

SATA o SAS?

Una pregunta natural que se'ns planteja a continuació sobre els discos SAS/SATA és: quan s'han d'emprar discos SATA i quan s'han d'emprar discos SAS?

La resposta està basada en les inherents diferències entre els discos SCSI i els discos ATA avui en dia. Els discos SCSI han estat dissenyats i fabricats per a complir amb els requisits empresarials d'alta disponibilitat i seguretat. Aquesta és la característica que ens ha de fer decidir.

5.2.5. Agrupacions de discos en el servidor

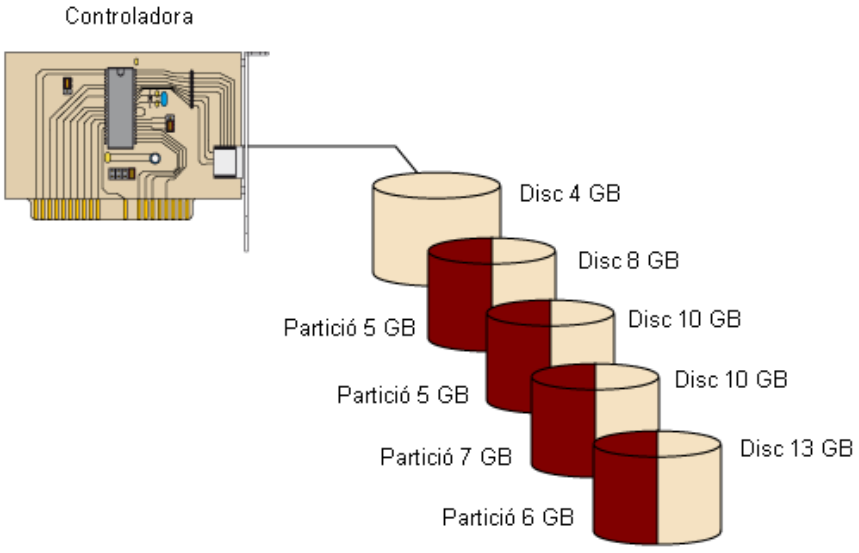
Els discos són sempre una de les peces clau en els servidors. Això ha provocat intents tecnològics per a millorar-ne la capacitat i el rendiment.

Multivolum

Què passa si ens pensem que tindrem una base de dades que ocuparà 18 Gb i només tenim dos discos de 12 Gb? Hi ha una solució per mitjà de l'SO que consisteix a convertir els dos discos de 12 Gb en un de 24 Gb. És la gestió multivolum.

En general la gestió multivolum es tracta d'ajuntar diverses particions físiques en una sola partició lògica d'una mida equivalent a la suma de les mides de les particions.

Esquema de gestió multivolum

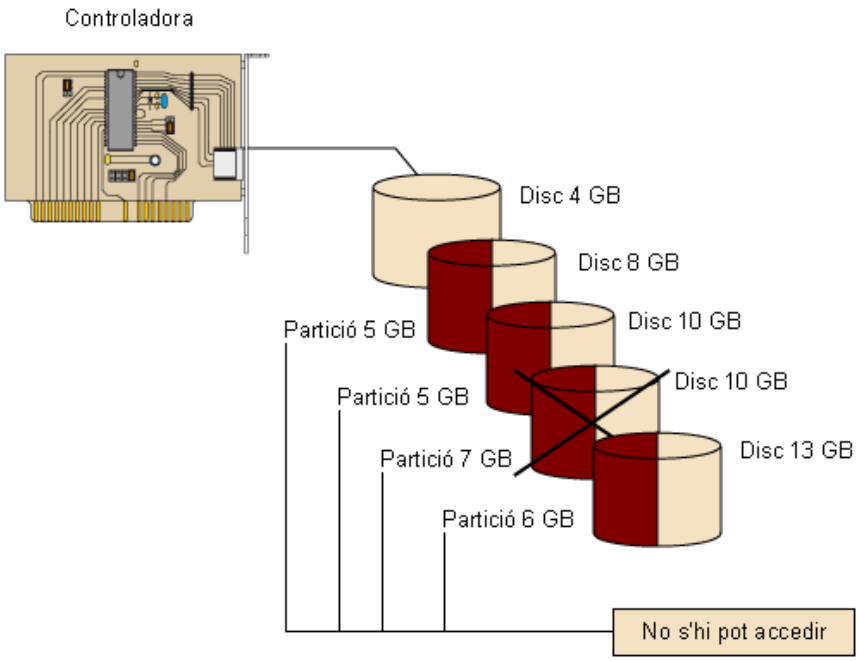


En l'esquema anterior la partició lògica total és 5 + 5 + 7 + 6 = 23 Gb.

El principal avantatge és que es pot obtenir una partició de la mida que es vulgui ajuntant particions de discos d'altres mides. Sovint les bases de dades necessiten discos molt grans.

El principal inconvenient és que si un disc falla físicament (s'espatlla) no podrem accedir a cap de les particions físiques que integren la partició mutivolum creada.

Si un disc falla no podrem accedir a la partició multivolum



Aquest problema, juntament amb el gran augment de capacitat dels discos (i la seva notable reducció de preus), fa que la solució que s'adopta sigui comprar i instal·lar discos de la capacitat que es necessita, ja que si cal fer un multivolum és símptoma que la informació que ha de contenir és crítica i la despesa d'un disc nou és petita en comparació amb la seguretat que guanya el servidor.

RAID

Davant dels problemes que genera la gestió multivolum, hi ha la solució *Redundant Array of Inexpensive Disks* (RAID). El RAID permet, per exemple, de tenir cinc discos funcionant i només aprofitar-ne quatre, però si falla qualsevol d'aquests quatre el servidor continua funcionant, perquè el cinquè conté informació redundant que ho permet.

Fins i tot permet de canviar el disc en calent, és a dir, sense parar el servidor es pot substituir el disc que ha deixat de funcionar per un de nou, que el mateix RAID torna a posar en funcionament.

El RAID es pot fer de diverses maneres, segons el grau de velocitat i seguretat que es necessiti. Es classifiquen en nivells:

- **RAID 0**. La informació es distribueix en diverses unitats, però no hi ha redundància. Per tant, no hi ha protecció en cas de fallada de disc.

- **RAID 1**. També anomenat **mirall**. Cada unitat està duplicada amb una unitat de suport. Per tant, amb sis unitats de disc, tres són de còpia. La informació es distribueix entre els discos.

- **RAID 2**. Hi ha distribució de dades pel que fa als bits sobre totes les unitats. No es fa servir perquè el RAID de nivell 3 està molt més estès.

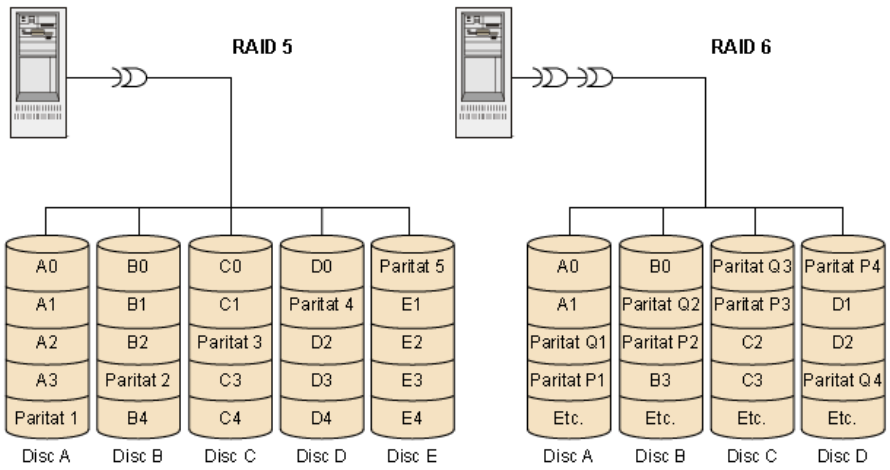
- **RAID 3**. Dades distribuïdes a nivell de bit (o de byte) en totes les unitats menys en una, que és la de paritat. Té molt bon rendiment de lectura, però en escriptura cada vegada s'ha d'actualitzar la unitat de paritat.

- **RAID 4**. Com el de nivell 3, però tot es fa a nivell de sector. Milloren els temps d'accés.

- **RAID 5**. s'escriuen en tots els sectors de totes les unitats, i s'afegeixen codis correctors a cada sector. Aquest nivell de RAID ofereix una escriptura més ràpida, perquè la informació de redundància es distribueix en totes les unitats. Les lectures a disc també tenen uns temps d'accés molt bons.

- **RAID 6**. Aquest nivell de RAID és similar al 5, però utilitzant dos codis correctors per a cada sector i grup de RAID. Les informacions de paritat es distribueixen entre tots els discos del grup.

Esquema dels RAID 5 i 6

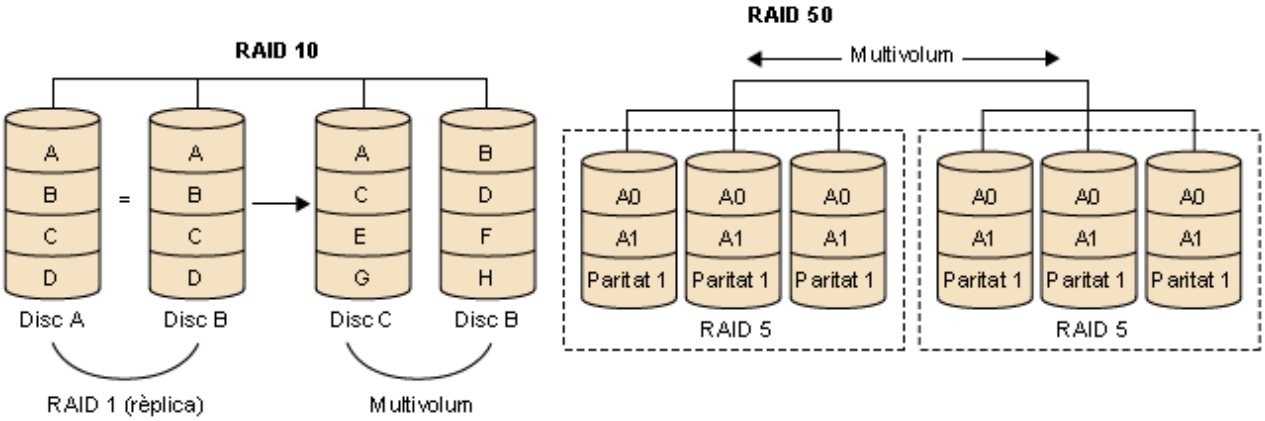


- **RAID 5e, 6e**. Aquests dos nivells de paritat es basen en els seus predecessors (5 i 6), però afegeixen un element més de seguretat: ***Hot spare***. Aquest és un nou disc en espera que entra a formar part del grup de RAID activament si un dels discos del mateix deixa el grup.

- **RAID 10**. Apareixen diverses combinacions de nivells de seguretat, a partir dels nivells bàsics comentats. Un d'ells és el nivell 10 = 1 + 0, el qual replicaria un grup de RAID 1 en un grup de discos amb RAID 0.

- **RAID 50**. Un grup de nivell 50 = 5 + 0 distribuiria la informació per multivolum entre dos grups de RAID 5.

Esquema dels RAID 10 i 50



Hi ha altres combinacions possibles i altres nivells de RAID no estàndards que proposen les companyies als seus clients.

La tècnica del RAID millora el rendiment, en distribuir la informació entre diverses unitats, i pot oferir redundància per a augmentar la seguretat.

Una vegada més, el RAID pot ser per programari o per maquinari. Si és per programari és més lent, i si és per maquinari és transparent a l'SO.

RAID comercials

Hi ha una gran quantitat de sistemes de RAID comercials interns i externs, però citem alguns fabricants, que es poden trobar en el web: Dell (PowerVault), Compaq, StorageTeK, Clarion, Hewlett Packard, IBM, RaidTec, etc.

5.2.6. Sistemes de fitxers

Una vegada hem fet les particions sobre els discos, necessitem fer una operació perquè el nostre sistema hi pugui treballar. s'ha de formatar la partició. Aquest pas és imprescindible, perquè informa el sistema operatiu i el disc de com es reparteix l'espai (mida del sector), de com es distribuirà lògicament dins el disc, i també es fan operacions per a millorar-ne el rendiment, malgrat que són dependents del mateix sistema operatiu. Per tant, el resultat d'aquesta formatació genera el sistema de fitxers, ja buit i preparat per a poder-hi posar informació. El sistema de fitxers que es triï per a formatar la partició també és molt important perquè té diverses característiques associades, com per exemple qüestions de seguretat.

File Allocation Table

El sistema de fitxers *File Allocation Table* (FAT) és força antic. Només suporta mides de fins a 2 Gb i no hi ha seguretat. És el sistema de fitxers dels PC de sobretaula d'abans.

La mida del *clúster*[22] (el nombre de sectors que guarda de cop) pot ser molt gran, i els sistemes operatius tenen una gran quantitat de fitxers petits, per la qual cosa es perd molt d'espai.

(22)Un clúster és un grup de sectors.

FAT32

El sistema de fitxers FAT32 és el mateix que el FAT[23], però suporta mides de disc superiors sense cap problema. La mida del clúster és molt més petita, per la qual cosa s'aprofita molt millor l'espai del disc. Tampoc no té seguretat.

(23)Recordeu que FAT vol dir *File Allocation Table*.

Sistema de fitxers NT

El sistema de fitxers NT[24] (NTFS) es va introduir amb l'aparició de Windows NT. Té una mida de sector i de clúster molt petita, de manera que s'aprofita molt bé l'espai de disc. Porta signatura de la partició, per la qual cosa el disc no es pot llegir en un altre ordinador. Porta seguretat en el sistema de fitxers, per la qual cosa els permisos estan a nivell del sistema de fitxers. Tot el conjunt, doncs, fa que sigui molt més robust.

(24)El sistema de fitxers NT s'expressa en anglès com a *NT File System*.

Sistemes de fitxers ufs, ext2 i ext3

Els sistemes de fitxers ufs, ext2 i ext3 són tres sistemes de fitxers que es fan servir molt en sistemes Unix i GNU/Linux. La mida de sector és de 256 bytes (molt petita). Té una estructura d'*inodes* per a gestionar els fitxers i la seguretat de Unix Standard.

El sistema de fitxers **ext3** ens ofereix la possibilitat de treballar amb ***journaling***, sistema mitjançant el qual se salven periòdicament els arxius oberts per tal d'evitar la pèrdua d'informació o la corrupció de les dades si es produeix una desconnexió no planificada. Aquest sistema de fitxers aporta més seguretat, tot i que per contra fa perdre recursos de màquina, assignats precisament a la tasca de *journaling*.

High Sierra File System

El sistema de fitxers *High Sierra File System* (HSFS) o ISO9660 és molt conegut. També és el format dels CD-ROM/DVD. Tots segueixen aquest format, tant els de dades com els d'àudio.

Sistemes de fitxers distribuïts

Un sistema de fitxers distribuïts permet emmagatzemar fitxers en un o més ordinadors (servidors), i permet que es facin accessibles a altres, anomenats clients. Aquests últims, poden gestionar i manipular els fitxers com si fossin locals.

Normalment, els sistemes de fitxers distribuïts inclouen eines automàtiques de replicació i de tolerància a errors. Totalment transparent a l'usuari, el sistema és capaç de replicar les dades entre els servidors i donar servei des d'un altre servidor en cas de fallada.

Hi ha diversos avantatges a tenir en compte dels sistemes de fitxers distribuïts:

- **Fitxers fàcilment accessibles**. Actualment es pot accedir a uns fitxers des de qualsevol punt del planeta. Només fa falta un ordinador connectat a la xarxa i un navegador.
- **Compartició de fitxers**. Facilita clarament el treball en grup i la interacció entre usuaris.
- **Simplificació de les còpies de seguretat**. Simplifica la còpia de seguretat dels fitxers, centrant l'acció en els servidors i no en els clients. S'evita en certa manera la dispersió de la informació.
- **Gran capacitat d'emmagatzematge**. Els servidors de fitxers proporcionen grans volums d'espai per a emmagatzemar fitxers, i redueixen el cost que suposaria replicar l'espai als ordinadors clients.
- **Simplificació de l'administració**. Des del punt de vista de l'administrador, aquest sistema simplifica molt la tasca, en tenir centralitzada tota la informació.

Altres sistemes de fitxers

Hi ha molts altres formats i sistemes de fitxers. Així, fent una ullada nostàlgica al passat, els disquets, per exemple, també tenen un format de sistemes de fitxer. En contraposició, mirant al futur, hi ha sistemes de fitxers distribuïts (The Google File System, WUALA, CODA, i molts d'altres) que han fet canviar la visió dels sistemes de fitxers.

5.3. *Storage Area Network* i *Network Attached Storage*

Les xarxes SAN[25] i els servidors de fitxers NAS[26] són agrupacions més grans de discos que la dels RAID.

[25] Recordeu que SAN és la sigla de *Storage Area Network*.

[26] Recordeu que "NAS" és la sigla de *Network Attached Storage*.

5.3.1. *Storage Area Network*

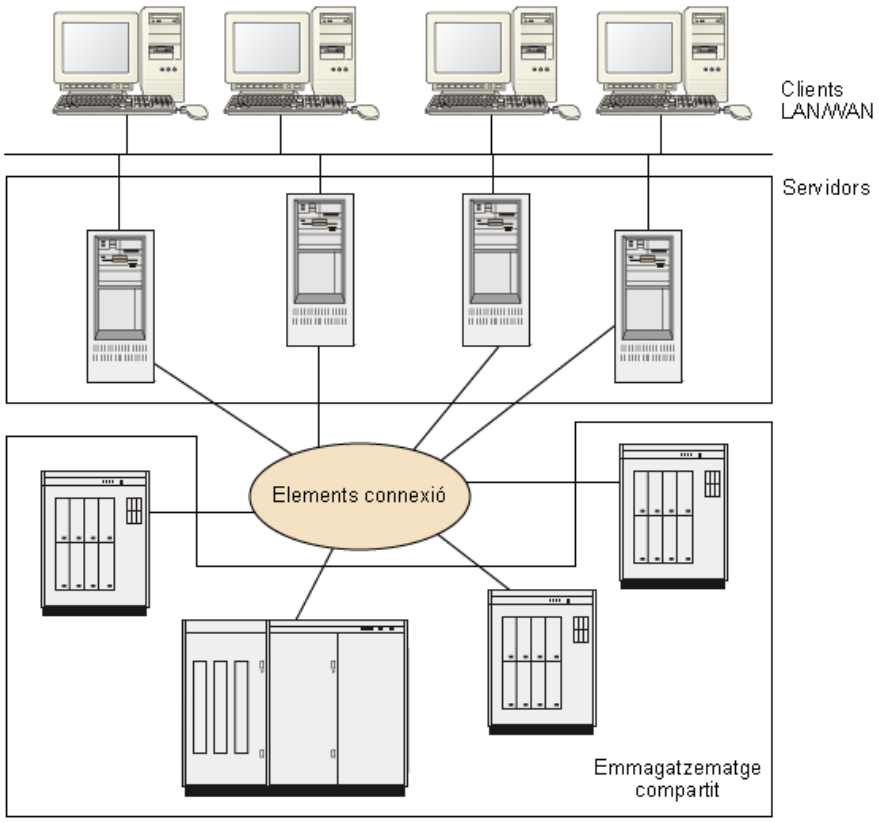
L'associació Storage Network Industry Association (SNIA) defineix *Storage Area Network* (SAN) com la xarxa que té com a objectiu principal transferir dades entre sistemes o computadores i elements d'emmagatzematge.

Una altra definició més senzilla de SAN és: xarxa especialitzada d'alta velocitat, que comunica servidors i dispositius d'emmagatzematge. Una SAN també pot ser un sistema d'emmagatzematge format per elements i dispositius d'emmagatzematge, computadores, aplicacions, programari de control, i tots aquests elements, comunicant-se mitjançant una xarxa.

Acessos a disc en una SAN

Els accessos a disc en una xarxa SAN són normalment (tot i que no sempre) a nivell de *Block I/O*.

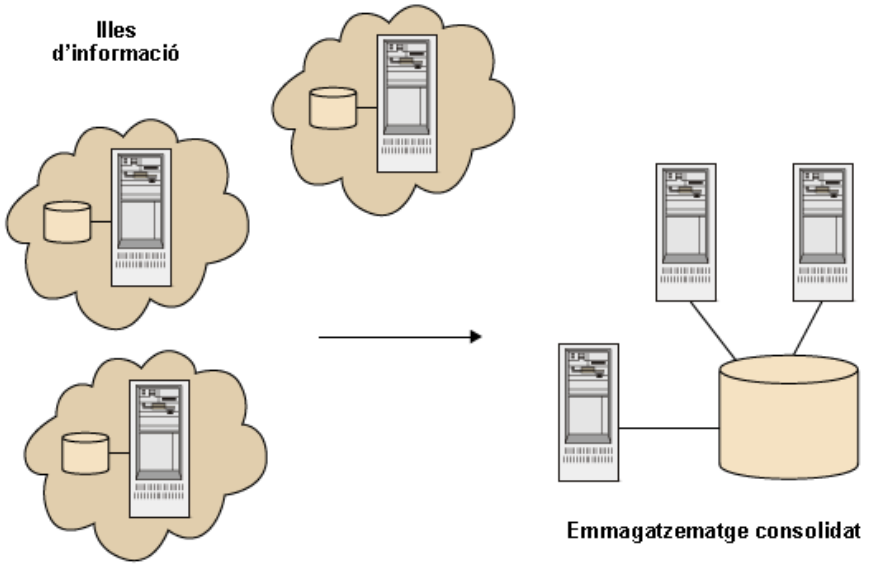
Esquema de SAN



Abans de parlar dels components, protocols i implementacions de les xarxes SAN, és bo que definim el perquè de la seva utilització. Quines motivacions tenim per optar per aquesta tecnologia?

La principal raó és que les organitzacions tenen cada vegada un major nombre de servidors, i aquests alhora necessiten constants augments de capacitat d'emmagatzematge. Per a evitar **illes d'informació**, on cada servidor controla el seu emmagatzematge independentment de la resta, cal emprar una nova tècnica que ens permeti la compartició global dels recursos d'emmagatzematge.

Les xarxes SAN eviten les illes d'informació.



Si revisem la història, als anys setanta i principis dels vuitanta, els sistemes *host* definien un model centralitzat, on les dades residien internament. l'evolució ens porta als anys vuitanta i noranta a sistemes amb dades distribuïdes gràcies al model client/servidor. El futur ens porta a un nou sistema de compartició global de recursos d'emmagatzematge per xarxa. És una nova era, la SAN.

Elements d'una xarxa SAN

Els elements d'una xarxa SAN es poden dividir en tres grans grups:

1) Servidors. Formen part d'una xarxa SAN tots aquells servidors que disposen de targetes específiques per a establir comunicació amb els elements de connexió.

2) Elements de connexió. Formen part d'aquest grup:

a) Cablejat: específic per a les xarxes SAN, sol ser cable de fibra òptica. n'hi ha de dos tipus, cablejat multimode de fibra de 50 microns per a distàncies curtes i monomode per a distàncies llargues (menys de 10 microns).

b) Commutador: commutadors especialitzats en comunicació en xarxes SAN.

c) Directors: commutador principal. Punt central de govern de les xarxes SAN.

d) Concentradors: fan la mateixa funció que els concentradors de xarxes, però especialitzats per a xarxes SAN.

e) Encaminadors: encaminadors especialitzats poden convertir senyals entre protocols de SAN.

Vegeu també

Vegeu més informació sobre els directors en el mòdul "Administració de la xarxa".

3) Emmagatzematge:

a) Sistemes de discos: dispositius especialitzats a servir emmagatzematge de disc.

b) Sistemes de cintes, bàsicament biblioteques de cinta com a elements de gestió de gran volum de dades per a *backup* i dispositius de cinta.

Connectivitat SAN

Comprèn totes les classes de maquinari, programari i components que permeten la interconnexió dels dispositius d'emmagatzematge i els servidors.

1) Capa baixa. La capa baixa comprèn les capes de connexió física i xarxes. Tenim diferents possibilitats:

Vegeu també

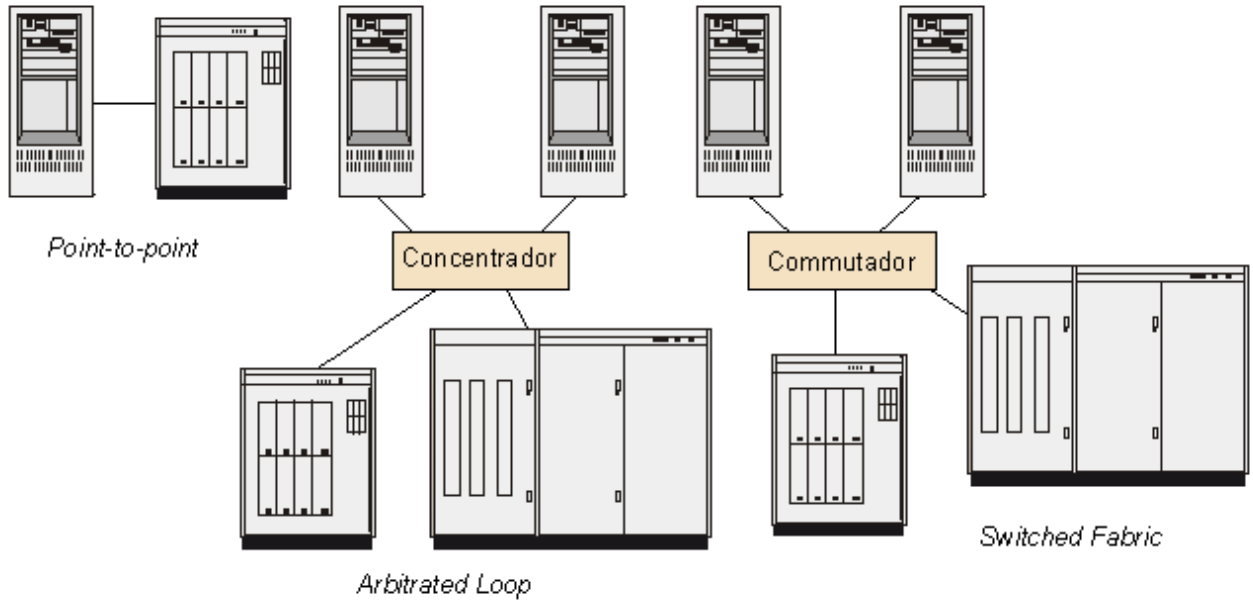
Reviseu l'estructura de capes de la torre OSI.

- *Ethernet*. Es construeix una topologia típicament de bus que pot arribar a una velocitat de 10 Gbps de dades.

- SCSI. És una interfície en paral·lel que pot treballar fins a 25 metres a una velocitat de 160 Mbps.

- *Fibre Channel* (FC). És una interfície en sèrie, normalment implementada amb cable de fibra òptica, que actualment és l'arquitectura més emprada per les xarxes SAN. Millora la velocitat i la distància de SCSI. Les seves possibles topologies són*: Point-to-point, Arbitrated Loop, Switched Fabric*.

Esquema de topologies *Fibre Channel*



2) Capa mitjana. La capa mitjana comprèn el protocol de transport i les capes de sessió:

- *Fibre Channel Protocol* (FCP). És el protocol de transport per a SCSI en *fibre channel*. És una tecnologia de Gigabit principalment emprada per a xarxes d'emmagatzematge. Els senyals de *fibre channel* poden enviar-se tant en parell trenat de coure com en cables de fibra òptica.

- iSCSI. És un protocol de transport de dades que transporta les comandes SCSI requerides mitjançant la tecnologia estàndard de xarxes (TCP/IP)

- *Fibre channel* per IP (FCIP). També és coneguda com FC *tunneling*. Mètode que permet la transmissió de FC[27] mitjançant xarxes IP.

- Internet FCP (iFCP). Mecanisme que permet trametre dades a dispositius d'emmagatzematge d'una SAN mitjançant TCP/IP via Internet.

[27]"FC" és la sigla de *Fibre Channel*.

Protocols propietaris

A banda dels protocols FCP[28], iSCSI, FCIP [29]i iFCP[30], hi ha altres protocols propietaris com ESCON o FICON.

[28]"FCP" és la sigla de *Fibre Channel Protocol*.

[29]"FCIP" és la sigla de *Fibre Channel* per IP.

[30]iFCP és la sigla d'Internet FCP.

3) **Capa alta**. La capa alta comprèn les capes de presentació i aplicació:

- *Server Attached Storage*. Inicialment l'emmagatzematge era compartit directament pel bus del servidor emprant una targeta de comunicacions adient i el dispositiu d'emmagatzematge era dedicat a un sol servidor. El servidor controlava les E/S cap al dispositiu. Actualment els dispositius d'emmagatzematge disposen d'una intel·ligència que els permet realitzar accions com la gestió de grups de RAID, disponibilitat de memòria Cache E/S, control d'unitats...

- *Network Attached Storage*

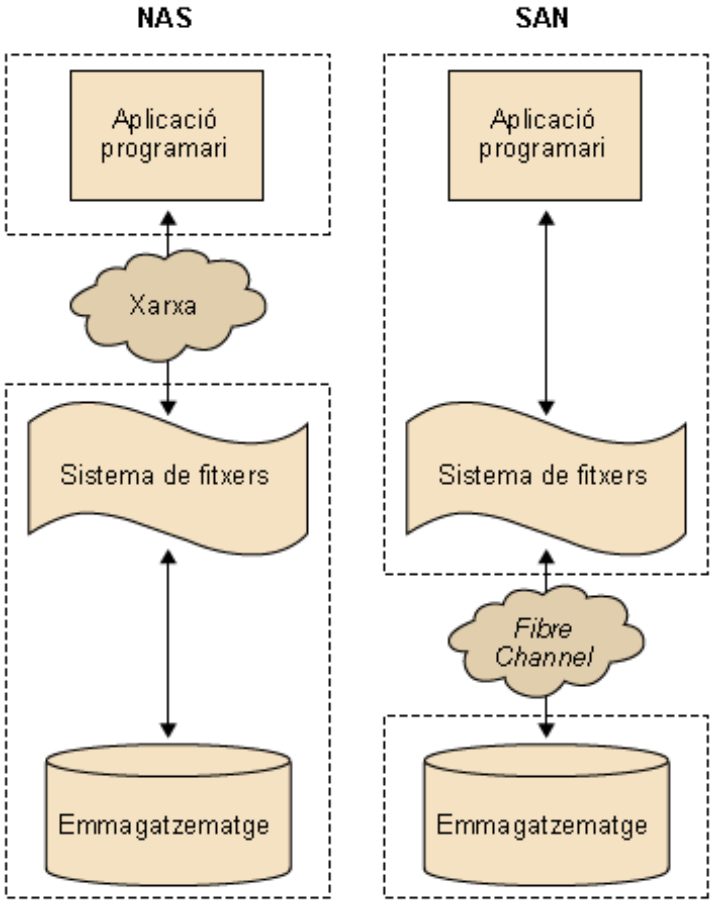
5.3.2. *Network Attached Storage*

Network Attached Storage (NAS) és bàsicament un servidor de fitxers connectat a una xarxa que serveix fitxers utilitzant un protocol. Un element NAS consisteix en una màquina que implementa els serveis de fitxers (emprant protocols d'accés com per exemple NFS o CIFS), i un o més dispositius, on les dades són emmagatzemades.

NAS proporciona capacitat d'emmagatzematge emprant la mateixa xarxa de comunicacions o una d'addicional de baix cost.

Així com els accessos que es realitzen en una SAN són la majoria de vegades com a *Block I/O*, en una NAS es realitzen com a sistema de fitxers. És a dir, les aplicacions accedeixen al sistema de fitxers que proporciona el mateix dispositiu NAS, mentre que en una SAN, el sistema de fitxers pertany al mateix servidor.

Comparació entre una SAN i un NAS

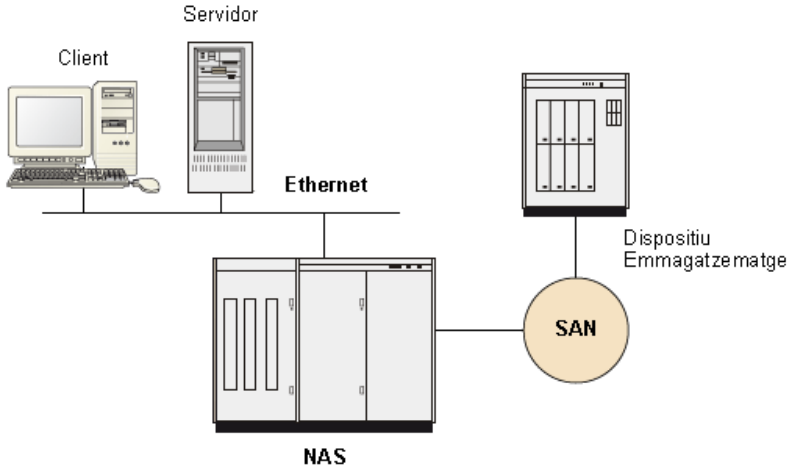


Sovint s'ha de prendre una decisió de disseny i triar entre una SAN o una NAS. Aquesta decisió, ha de venir reforçada per dues premisses bàsiques: velocitat de comunicació (rendiment d'accés a disc) i sistema d'accés (accés a nivell de bloc o de fitxers).

Solucions híbrides

Els sistemes NAS i SAN no són excloents; ben al contrari, es poden combinar i donar encara major flexibilitat i servei d'emmagatzematge als servidors. Un exemple seria tenir un servidor connectat a una NAS, la qual té els discos en un sistema d'emmagatzematge connectat a una SAN.

Combinació de NAS i SAN



6. Còpia de seguretat

Davant del problema de copiar la informació de l'organització per a evitar-ne la pèrdua hi ha molts dispositius (aparells físics) i tècniques. Hem de buscar els millors per a cada cas.

Els dispositius de còpia de seguretat[31] són els aparells físics que s'utilitzen per a fer còpies de seguretat de la informació dels servidors. Normalment les còpies són procediments que triguen hores a enllestir-se, i també es triga molt a recuperar els fitxers del dispositiu en què s'ha emmagatzemat la informació.

(31)Còpia de seguretat en anglès s'expressa com a *backup*.

6.1. Dispositius de còpia de seguretat

Per a fer còpies de seguretat hi ha disponibles diversos dispositius: cites, llibreries de còpia, gravadores DVD i discos durs.

6.1.1. *Digital Audio Tape*

Les cintes són el dispositiu més habitual que hi ha en els servidors. Els *Digital Audio Tape* (DAT) són molt habituals, generalment SCSI, i n'hi ha de diverses capacitats, que poden arribar fins a uns 20 GB per cinta.

Capacitat de les unitats de cinta

Quan es parla de capacitats de les unitats de cinta n'hi ha amb compressió o sense. Nosaltres parlem sempre de les que són sense compressió. Amb compressió la capacitat es pot duplicar o més.

És normal que un servidor tingui una unitat d'aquestes característiques i que diàriament es facin còpies de seguretat seguint alguna política de còpia.

6.1.2. *Digital Linear Tape*

Un altre tipus de cintes, les *Digital Linear Tape* (DLT), també són generalment SCSI i n'hi ha de diferents capacitats, que poden anar dels 20 GB fins als 100 GB per cinta (sense compressió), fent servir Super DLT (SDLT).

6.1.3. *Advanced Intelligent Tape*

Un tercer tipus de cintes, les *Advanced Intelligent Tape* (AIT), també són generalment SCSI i n'hi ha de diverses capacitats, entre 25 GB i 100 GB per cinta (amb AIT3). La variació d'aquesta capacitat depèn de la cinta, del tipus d'AIT que s'utilitzi i del nivell de compressió amb què es facin les còpies.

6.1.4. *Linear Tape Open*

Un nou tipus de cintes, les *Linear Tape Open* (LTO), són una nova tecnologia desenvolupada per Hewlett Packard, IBM i Seagate.

Aquests tipus de cintes han anat evolucionant ràpidament. Mentre que l'any 2000 parlàvem de LTO 1, que permetia fins a 100 GB de còpia per cinta, actualment la capacitat de les cintes LTO4 arriba fins a 800 GB sense compressió (1,6 TB amb compressió).

La seva velocitat de còpia pot arribar a 120 Mb/s, i ja estan planificades les versions LTO5 i LTO6, que permetran emmagatzemar fins a 3,2 TB a una velocitat de 270 Mb/s.

Altres cintes

Hi ha altres cintes, com per exemple l'Hexabyte, però les DAT (*digital audio tape*), DLT (*digital linear tape*), AIT (*advanced intelligent tape*) i LTO (*linear tape open*) són les més esteses.

6.1.5. Llibreries de còpia

Es pot donar el cas que la nostra organització manipuli quantitats de dades que ocupin diverses cintes de còpia al dia. En aquest cas, una sola persona es passaria el dia fent còpies de seguretat, i no acabaria mai. Quina és la solució per a aquests volums d'informació tan grans? Hi ha uns dispositius anomenats llibreries de còpia. Són externs, amb uns braços articulats, i contenen des de vint fins a dues mil cintes de còpia de seguretat (són com robots). Amb el programari adient, això es veu, per exemple, com una unitat de 400 TB per a guardar informació. El programari sap en quina cinta està emmagatzemada la còpia, quines cintes estan plenes, i maneja la política de substitució de cintes. Les llibreries de còpia només tenen sentit per a organitzacions de grans dimensions o bé que manegen quantitats d'informació molt grans.

Llibreries de còpia

Llibreries de còpia comercials

Hi ha diverses marques que fabriquen llibreries en col·laboració amb marques de programari, perquè puguin funcionar correctament amb els servidors en què s'instal·lin. Algunes d'aquestes marques, amb webs per a poder-ne veure els aparells, són Qualstar, Adic, Hewlett Packard, StorageTek, Quantum (ATL), etc.

6.1.6. Gravadora DVD

Una unitat de cinta és un component car i moltes vegades resulta difícil accedir (demana un temps considerable) a les dades que contenen. Per això, de vegades es considera la gravadora de DVD com una opció de còpies de seguretat. Permet de fer còpies dels elements següents:

- DVD gravables una vegada de 4,7 GB.
- DVD gravables moltes vegades de 4,7 GB.
- DVD gravables una vegada de 9,4 GB.
- DVD gravables moltes vegades de 9,4 GB.

Tot i que aquests són els volums més estàndard, podem trobar volums de DVD gravables una vegada de fins a 17 GB.

Actualment, els DVD gravables una vegada són una opció que cal tenir en compte en plantejar-se les còpies de seguretat, ja que tenen els avantatges següents:

- El cost de compra del dispositiu és baix.
- El cost de les unitats de còpia és baix.
- Són de gran capacitat (fins a 17 GB).
- Ofereixen una gran facilitat per a accedir a la informació guardada.

Que es faci servir o no com a mecanisme de còpia depèn sempre de la mida de l'organització, el volum de dades, etc.

Tendències

En poc temps veurem com el Blue Ray substitueix el DVD com a dispositiu de còpia. El *Blu-Ray* és un disc de la mateixa mida que un DVD (12 cm) i amb una capacitat de 25 GB per cara (50 GB en total a una velocitat de 36 Mbit/s). Existeix ja el BD-R i el BD-RE (gravable i el regravable) i hi ha prototips per augmentar la velocitat (2X) i desenvolupar un Blue Ray de 4 capes (100 GB per disc).

6.1.7. Disc dur

En sistemes crítics, i més tenint en compte el cost i la capacitat actual d'aquests dispositius, no s'ha de descartar mai la possibilitat de fer una còpia de seguretat (o fins i tot de copiar tota la informació) en un altre disc dur només dedicat a aquesta funció.

L'estratègia és fer una primera còpia de seguretat en aquest disc dur (es pot fer amb un procediment automàtic i diverses vegades al dia, si cal), i d'aquest disc, posteriorment, se'n farà una còpia de seguretat en un altre dispositiu (que pot ser una cinta).

De vegades, aquesta estratègia és necessària si el procediment de còpia necessita bloquejar la informació a la qual accedeix i és, per exemple, una gran base de dades de la qual depèn tota l'organització. La còpia de disc a disc, en funcionar internament, pels busos del sistema i amb velocitats de transferència molt elevades, necessita bloquejar molt poc temps la informació per a fer la còpia. Així, doncs, la interrupció per a fer aquesta tasca és pràcticament imperceptible.

Tendències

Gràcies a la proliferació de xarxes SAN o dispositius NAS que permeten una gran quantitat d'espai per a emmagatzemar, s'utilitzen cada cop més els discos com a dispositiu de còpia. Els mateixos proveïdors ofereixen eines específiques que permeten fer aquestes còpies transparents al sistema mateix.

6.1.8. On han de ser els dispositius de còpia?

El disc dur de què parlàvem, o els dispositius de còpia de seguretat (les unitats de cinta), per què han de ser en el mateix servidor?

Aquesta qüestió, que des del punt de vista lògic (davant del físic) és perfectament plausible, presenta en aquests moments greus inconvenients tecnològics. Des del punt de vista de la xarxa, podríem tenir la unitat de còpia en qualsevol lloc i transferir la informació per la xarxa. Sens dubte funcionarà, però aquests són alguns dels problemes que representa fer-ho:

- Podem col·lapsar la xarxa, ja que si fem una còpia de tot el servidor (l'opció habitual) transferirem per la xarxa una quantitat d'informació de l'ordre de diverses desenes de Gb.

- Tota la informació del servidor (suposadament segura) travessa la xarxa, de manera que potencialment hi ha el perill que la vegin persones alienes al procés (de dins o de fora de l'organització). Un risc de seguretat.

- Per a poder-ho fer s'ha de fer accessible per xarxa (amb permisos, contrasenyes, etc.) tot el disc del servidor. Això implica un altre risc de seguretat, perquè ni que després de fer la còpia es tregui que el disc sigui accessible, aquest disc hi serà unes quantes hores al dia (esperem no descuidar-nos cap dia de treure l'accés).

- L'amplada de banda de la xarxa i la dels busos de sistema (IDE, SCSI, bus intern, etc.) no són comparables, per la qual cosa la velocitat de transferència faria el temps de còpia extraordinàriament superior.

Per tant, el més aconsellable és tenir el dispositiu de còpia en el servidor on hi hagi la informació que s'ha de copiar.

Còpies per xarxa

Hem de descartar les còpies per xarxa? Rotundament, no. S'utilitzen per a fer còpies de seguretat d'informació que hi ha en les estacions de treball dels usuaris. Malgrat que al llarg dels materials es comenta que s'ha de procurar que n'hi hagi com menys millor, molt sovint hi ha informació a les estacions de treball. En aquest cas, però, són de l'ordre d'algunes desenes de MB com a molt. No triguen a fer-se i no penalitzen gaire la xarxa. En canvi, sí que s'ha d'anar amb compte amb les qüestions de protecció i seguretat.

6.2. Polítiques de còpia de seguretat

Una bona política de còpies de seguretat és la clau per a tenir segura la informació de l'organització.

Alguns dels motius per a fer còpies de seguretat són els següents:

- Protegir la informació contra una fallada del sistema o algun desastre natural.

- Protegir la informació dels usuaris (els fitxers) contra esborraments accidentals.

- Protegir la informació dels usuaris i de l'organització contra atacs per part de tercers.

- Duplicar la informació dels usuaris per seguretat, ja que es poden donar casos d'usos incorrectes que la deixin inconsistent o la modifiquin incorrectament.

- Possibilitar un traspàs de la informació quan s'actualitza o es reinstal·la el sistema.

6.2.1. Tipus de còpies de seguretat

Podem distingir els següents tipus de còpia de seguretat:

- **Còpia de seguretat completa**. També es coneix amb el nom de *còpia de seguretat total* o *còpia full dump*. Es fa una còpia de tota la partició del disc. Sovint la còpia es fa considerant el format del disc i sense tenir en compte el sistema de fitxers, ja que només cal conèixer la taula de particions del disc i en quina part hi ha la partició per a duplicar-la en un dispositiu. En aquests casos, la restauració no pot ser selectiva, s'ha de restaurar tota la partició i no es pot seleccionar només un fitxer. Hi ha també la còpia de seguretat completa del sistema de fitxers, en la qual sí que és possible una restauració selectiva.

- **Còpia de seguretat incremental**. En aquest cas, es guarden només els fitxers que s'han modificat des de l'última còpia de seguretat que s'ha fet. Les còpies de seguretat incrementals s'utilitzen conjuntament amb les còpies de seguretat completes en el que s'anomenen polítiques de còpies de seguretat.

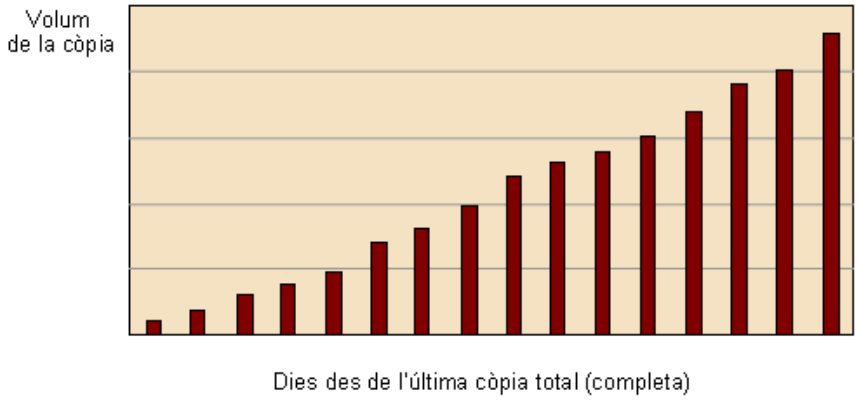
- **Còpia de seguretat selectiva**. També és possible fer una còpia de només uns fitxers determinats. Normalment això es duu a terme amb fitxers de comandes.

- **Còpia de seguretat diferencial**. Còpia de tots els fitxers que s'han modificat des de la darrera còpia total. Així doncs, si realitzem una còpia total cada dissabte i diferencial la resta de dies, la còpia de divendres contindrà tots els fitxers modificats des de dissabte.

Còpies de seguretat en cinta

Generalment les còpies de seguretat es fan sobre cinta, malgrat que no és l'únic dispositiu possible.

Esquema d'una còpia de seguretat diferencial



Tenim diversos avantatges de la còpia diferencial respecte a la còpia total. El primer, i com és natural, és que requereix menys espai, i el segon associat al primer és que redueix el temps o finestra de còpia.

Respecte a la còpia incremental aporta l'avantatge que en el procés de recuperació només necessitarem l'última còpia total i l'última còpia diferencial. Tanmateix, la còpia diferencial a partir del segon dia requerirà més espai i més temps o finestra de còpia.

6.2.2. Polítiques de còpies de seguretat

L'estratègia de com cal fer les còpies de seguretat és crítica per a assegurar que es faci tot correctament i que es pugui restaurar la informació quan calgui.

La necessitat de crear estratègies de còpies de seguretat prové del fet que actualment en els servidors els discos són de molta capacitat i, per tant, hi ha molta informació (tant d'usuaris com de sistema), i tota aquesta informació no cap en un sol dispositiu de sortida (en una sola cinta, per exemple). Finalment, la transferència dura hores i, per tant, s'han de buscar solucions per a optimitzar-ne l'ús.

Analitzem la variabilitat de la informació. Amb una ullada ràpida, ens podem adonar del següent:

- Hi ha informació que varia diàriament.
- Hi ha informació que es modifica molt poc al llarg del temps.
- Hi ha informació que no cal guardar en còpies de seguretat (els fitxers temporals, per exemple).

Així, doncs, una estratègia de còpia que ho copiï tot diàriament no sembla gaire encertada.

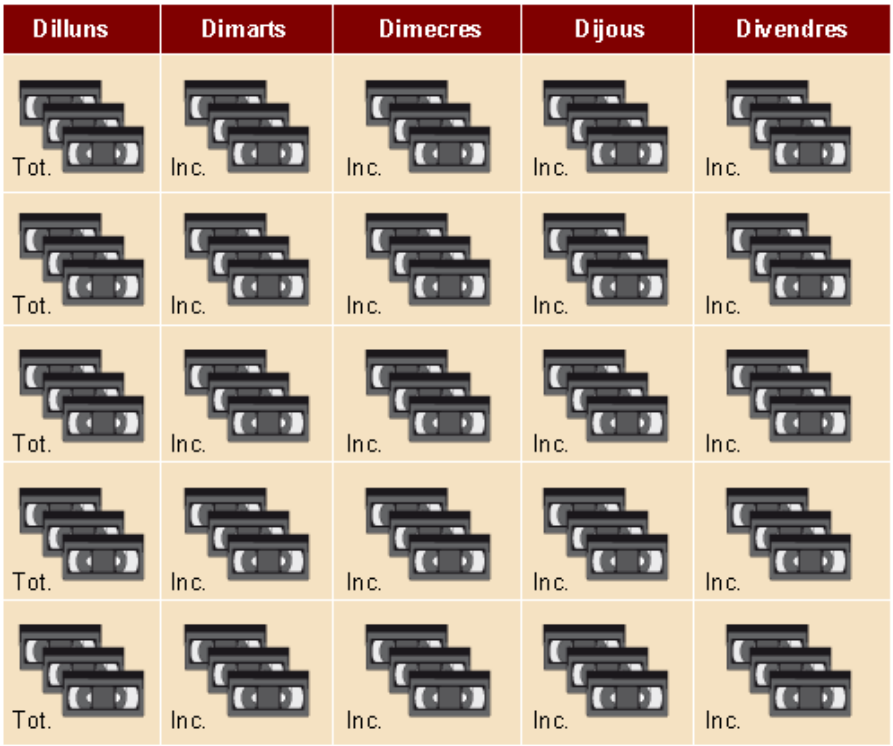
Vegeu també

Vegeu el mòdul "Administració de les dades" que parla sobre com i on poden estar les dades.

Sí que sembla clar que hem de fer una còpia diària de la informació que varia cada dia (acostuma a ser la informació de l'organització). Es pot trobar als servidors o distribuïda per tota l'organització. En qualsevol cas, cal que fem una còpia diària d'aquestes dades.

Amb la informació sobre la quantitat de dades que cal copiar (el volum) i sabent el dispositiu en què volem fer la còpia, tenim una idea aproximada de les cintes que necessitem. Una possible política de còpies és la següent:

Política de còpies de seguretat



Guardarem la primera còpia total de cada mes. d'aquesta manera, sempre és possible recuperar les dades de mesos anteriors.

Els avantatges són:

- La còpia és ràpida perquè no hi ha còpies totals diàriament, i les incrementals només copien els fitxers modificats durant el dia, que són pocs.

- s'estalvien cintes, ja que les còpies incrementals ocupen poc en relació amb les totals.

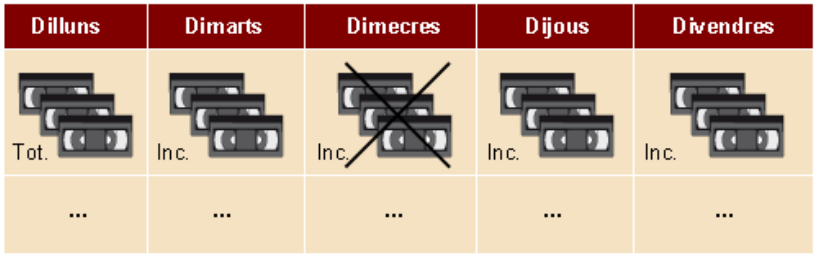
Els problemes són:

- Recuperar un fitxer requereix temps, perquè s'ha de passar pel joc de cintes des de l'ultima còpia total i totes les incrementals fins a arribar al fitxer de la data que es vol.

- Si falla una cinta incremental no es pot recuperar res dels jocs de cintes incrementals posteriors.

Exemple sobre els problemes d'una cinta incremental

És divendres i cal recuperar un fitxer de dijous. Una cinta del joc de dimecres ha fallat, i, per tant, no és possible recuperar la còpia incremental d'aquest dia. Com a conseqüència d'això, no és possible recuperar la còpia incremental de dijous, malgrat que el joc de cintes estigui en perfecte estat.



Aquest problema de les cintes incrementals fa que moltes organitzacions no utilitzin l'opció de les còpies incrementals pel risc que comporta i, per tant, es decanten per opcions de còpia **diferencial** o **completa** de les dades.

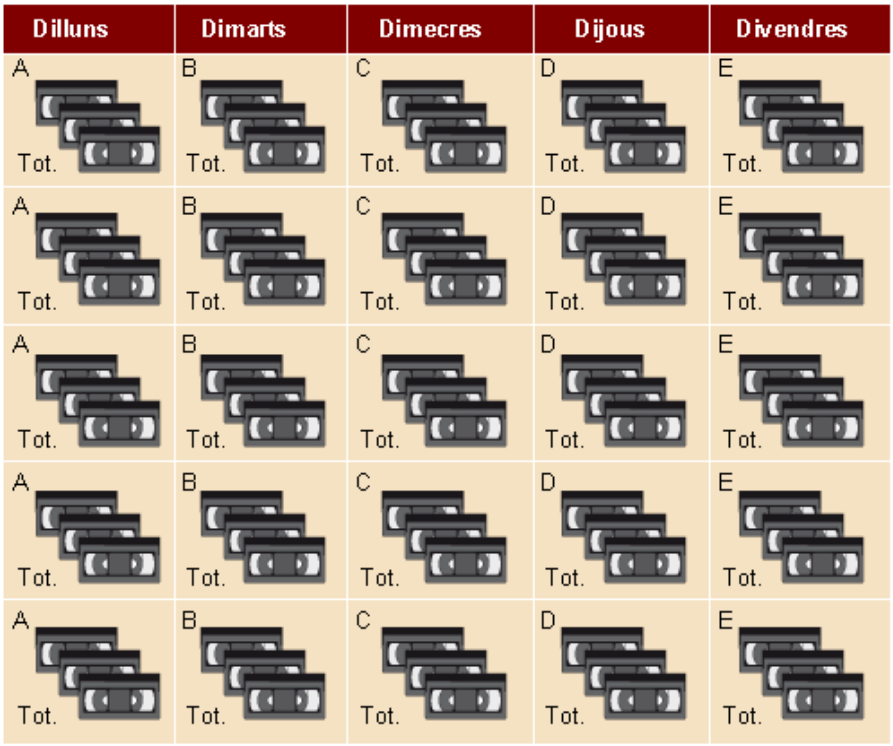
En el mateix exemple anterior si canviem les còpies incrementals per còpies diferencials, la còpia del dijous conté les dades de les còpies anteriors fins a la total; per tant, la pèrdua de la còpia del dimecres, en aquest cas, no seria un problema.

Ara bé, quina podria ser una manera d'estalviar cintes? Una possible política de còpies de seguretat és la següent:

- Anomenem els jocs de cintes A, B, C, D, E, etc.

- Cada mes guardarem un joc de cintes, de manera que tindrem una còpia de la informació mensual.

Política de còpies de seguretat



- El joc de cintes E de l'últim divendres del mes el guardarem per a no fer-lo servir. Al final de l'any tindrem dotze jocs de cintes amb la informació de l'organització. Haurem de decidir si alguns d'aquests jocs els tornem a fer servir o els continuem guardant.

6.2.3. Informació no variable

La informació no variable necessita uns altres criteris de valoració per a decidir la manera de tenir-ne còpia de seguretat. L'estratègia que s'acostuma a seguir és la següent:

Observació

L'estratègia que presentem aquí és una de les possibles, però en cap cas no és l'única ni la millor.

1) Informació de sistema. La informació de sistema dels servidors (les particions amb els operatius) es considera crítica. Perdre-la implica una fallada crítica de l'estructura informàtica. Per tant, com que els fitxers de log, de registre, etc. també varien bastant, s'acostumen a considerar com en el cas anterior i se'n fa una còpia diària.

2) Aplicacions. Les particions amb les aplicacions dels usuaris, tenint en compte que ja s'ha gestionat correctament la informació que varia diàriament, no és una informació que variï amb gaire freqüència, per la qual cosa fer una còpia diària vol dir carregar molt el sistema. Per tant, normalment només se'n fa una còpia manual (controlada pels administradors) quan hi ha modificacions sobre la partició.

3) Estacions de treball. També tenen informació de sistema, dades i aplicacions. Normalment, la informació de sistema (el sistema operatiu) i d'aplicacions és pràcticament igual en totes les estacions. Fer-ne una còpia diària desbordaria el sistema de còpies i col·lapsaria la xarxa per a guardar pràcticament la mateixa informació. En cas de desastre hi ha el mecanisme de restauració a partir d'imatges de les estacions de treball. A més a més, en principi a les estacions no hi hauria d'haver informació, però si n'hi ha ja s'ha comentat en l'apartat anterior que es fa una còpia diària exclusivament d'aquesta informació de l'estació de treball.

Vegeu també

Vegeu l'apartat 3.3.1. d'imatges de disc en el mòdul "Administració d'usuaris".

6.2.4. On es poden guardar les còpies de seguretat

Les còpies de seguretat tenen dues finalitats:

- Protegir-nos de fallades dels servidors.
- Protegir la informació de l'organització.

Amb tot el que hem fet fins ara només hem assolit el primer punt. El segon no, perquè si s'aconsegueix arribar fins on hi ha les còpies de seguretat, la informació està compromesa.

Normalment, els administradors tenen les còpies amb els servidors per a poder-los recuperar ràpidament en cas de fallada. Però hi ha d'haver una política en un segon nivell per a protegir la informació en cas d'intrusió física en la zona dels servidors o de desastre de l'organització que pot destruir aquesta zona (per exemple, un incendi). Recordeu els incendis de la torre Windsor de Madrid o el WTC de Nova York (EUA), on tot l'edifici va quedar completament destruït. Les empreses que tenien les còpies ubicades en altres llocs van poder recuperar el negoci en pocs dies, les altres ho van perdre tot, tant el suport informàtic com el paper. Si la informació és al mateix lloc (edifici), les còpies esdevenen inútils, per la qual cosa desmitificarem prèviament algunes recomanacions que es diuen:

- "Com que la zona de servidors està tancada amb pany i clau no hi ha perill". Si la intrusió física aconsegueix arribar a aquesta zona, tindrà accés a malmetre els servidors i a destruir (o fer desaparèixer) les còpies de seguretat.
- "Posem-les dins la caixa forta, que és ignífuga i no els pot passar res". Segurament als papers i a les monedes no, però a les cintes i el material magnètic (informàtic en general), sí: quan estan tancats en un receptacle metàl·lic, i si tenim la mala sort que hi ha un incendi, aquest receptacle pot arribar a diversos centenars de graus de temperatura. Amb un desastre d'aquesta magnitud els servidors perdran la informació, però les còpies de

seguretat hauran estat dins d'un "forn" que les podria fer completament inútils i, per tant, també s'hauria perdut la informació.

- "En el pitjor dels casos es torna a entrar tot, ja que està en paper". Fa un temps encara era cert. Ara, cada vegada menys. En qualsevol cas, certes precaucions físiques sobre les cintes poden evitar un problema d'un cost molt elevat. A més, atès l'ús creixent de les tecnologies intranet, molta informació ja no està en paper, sinó que es fa directament sobre sistemes informàtics. Molts sensors i màquines de producció recullen directament les dades en el sistema informàtic. L'ús de les tecnologies d'Internet fa que hi hagi informació que arribi per aquesta via sense suport paper. El paper ja no ho reflecteix tot.

- Organitzacions molt més crítiques amb les dades fins i tot tenen present la possibilitat que es produeixi un terratrèmol a la ciutat on són i extreuen les dades de manera segura a altres ciutats o estats. També poden tenir en compte tsunamis i radiacions nuclears.

6.2.5. Recomanacions

Sempre hi hauria d'haver, encara que no estigués actualitzada, una còpia de seguretat físicament fora de l'organització. Podria estar en una caixa forta d'un banc o en mans d'alguna persona de la direcció, per exemple. En cas de desastre pràcticament tindrem tota la informació, no s'haurà perdut gairebé res.

En cas que l'organització tanqui en alguns períodes com, per exemple, durant les vacances d'estiu, o en general en períodes en què la seguretat global de l'edifici es relaxa, és molt important que hi hagi una còpia fora de l'organització per a prevenir un desastre.

Actualment hi ha empreses que es dediquen a emmagatzemar còpies de seguretat seguint protocols de seguretat pactats conjuntament, a més de pactes de confidencialitat. Així doncs, aquesta última opció pot ser la més adient per a conservar les còpies de la nostra organització.

Obsessió?

L'alta seguretat recomana, especialment si hi ha dades crítiques, que la còpia de seguretat estigui guardada en una altra placa tectònica diferent d'on s'ubica l'organització. L'objectiu és que si hi ha un terratrèmol no pugui arribar a destruir la còpia. Normalment es tracta d'aproximadament un centenar de quilòmetres del lloc original.

6.3. Pla de contingència

Planificar tots els passos necessaris per tal permetre una recuperació enfront d'un desastre o una situació de crisi és el que anomenem pla de contingència[32].

(32)Pla de contingència en anglès s'expressa com a *disaster recovery plan*.

Els desastres són inevitables, en la majoria dels casos impredictibles i varien de tipus i de magnitud. La millor estratègia per a les organitzacions és la confecció d'un pla de contingència. Per a una organització, un desastre significa una disfunció brusca de part o de totes les seves operacions comercials, que poden provocar una pèrdua irreparable o fins i tot el tancament.

Per tal de minimitzar les pèrdues provocades pels desastres, és molt important tenir un bon pla de recuperació per a cada organització, departament i operació.

Vegeu també

Vegeu el mòdul "El sistema informàtic dins l'organització", sobre l'organització i el sistema informàtic per a la creació d'un pla de contingències.

7. Impressores

Les impressores són uns altres dispositius que es connecten al sistema informàtic i són controlades pels servidors de l'organització. Les estacions de treball no tenen impressores connectades físicament, i l'organització en té molt poques en relació amb el nombre d'estacions de treball, per la qual cosa és un recurs compartit, gestionat pel servidor mitjançant una cua d'impressió.

La cua d'impressió és un recurs de programari per a aconseguir que una impressora (inherentment no compartible) pugui ser compartida.

Per tant, en el servidor s'han de crear tantes cues d'impressió com impressores calgui gestionar. La manera de fer-ho varia segons el sistema operatiu, però s'acostumen a seguir dos passos:

1) Informar el sistema operatiu de quina impressora física hi ha connectada. En alguns SO com Windows es diu que cal instal·lar el controlador[33].

[33]Controlador en anglès s'expressa com a *driver*.

2) Crear la cua d'impressió i associar-la a la impressora.

Actualment hi ha molts tipus d'impressores, però bàsicament són dos els que es fan servir més: les impressores làser i les de raig de tinta.

7.1. Impressores làser

Les impressores làser són les més esteses i funcionen segons el principi de dibuixar la pàgina en un tambor especial amb un raig làser i després transferir-lo al paper amb una pols que es fixa amb calor. A grans trets, les seves característiques són les següents:

Característiques d'una impressora làser	
Cost	Alt
Qualitat d'impressió	Alta
Velocitat	Alta
Durada cartutx	Alta
Resolució	1.200 x 1.200 ppp
Pàgines per mes (aprox.)	15.000

Actualment, ja hi ha impressores làser de doble cara i també impressores làser de color, per la qual cosa els resultats, per un cost molt acceptable, són totalment professionals. Fins i tot hi ha papers especials, com films plàstics transparents per a fer transparències per a presentacions.

7.2. Impressores d'injecció de tinta

Tenen una altra utilitat. El seu cost és baix, i moltes vegades estan instal·lades en taules de despatx. Totes són de color (és inherent a aquestes impressores). Funcionen segons el principi de llançar una gota de tinta electroestàticament sobre el paper.

A grans trets, tenen aquestes característiques:

Característiques d'una impressora d'injecció de tinta	
Cost	Baix
Qualitat d'impressió	Mitjana
Velocitat	Baixa
Durada cartutx	Baixa
Resolució	1.200 x 1.200 ppp (però molt lenta)
Pàgines per mes (aprox.)	1.500

Cost del cartutx

A més de tenir poca durada, el cost del cartutx de tinta és elevat.

Actualment ja hi ha impressores d'injecció de tinta a doble cara per un cost molt ajustat. L'estalvi de paper és notable, i el petit increment en la compra es pot amortitzar en poc temps.

Si es volen imprimir transparències, no cal cap film especial. També hi ha el paper fotogràfic, un paper especial i de cost elevat, però si s'imprimeix amb qualitat fotogràfica (alta resolució) la qualitat és extraordinària.

Altres impressores

Cal no oblidar que hi ha altres impressores, com són les matricials, que si bé han caigut en desús són imprescindibles per a determinades aplicacions. N'hi ha d'altres d'especials, com les d'injecció de tinta amb paper fotogràfic A0 (com la Hewlett Packard DesignJet 10000S), que serveixen per a fer pòsters per a fires i congressos. Aquestes darreres són considerades per HP com a traçadors[34] i no com a impressores.

(34)Traçadors en àngles s'expressa com a *plotters*.

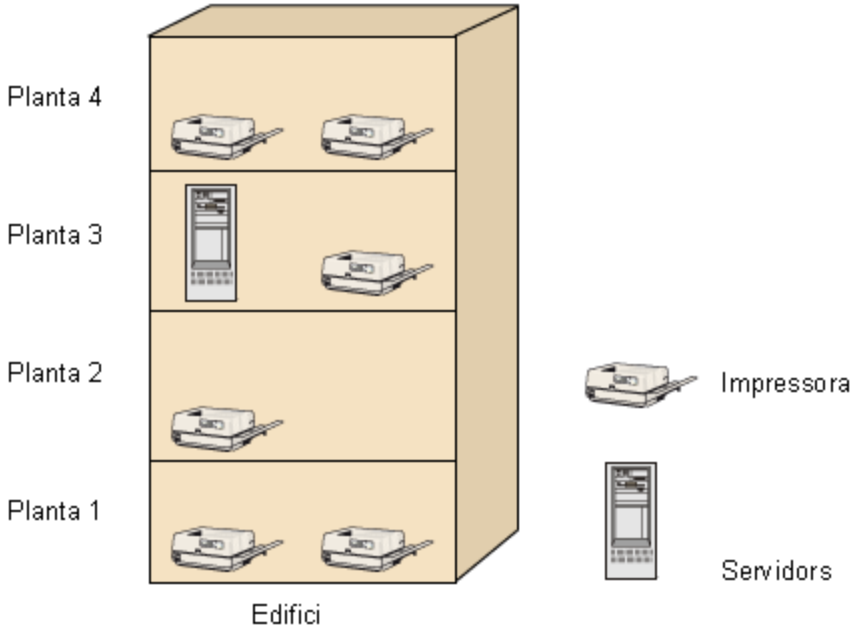
7.3. Impressores remotes

Impressores locals

Podem connectar dues impressores a un ordinador, i amb una placa afegida fins a quatre, però llavors es necessita un cable físic de l'ordinador fins a la impressora.

És molt habitual que l'organització necessiti impressores que estiguin controlades pel servidor, però que n'hagin d'estar allunyades físicament. Això fa que no hi puguin estar connectades directament (en local).

Suposem que la nostra necessitat per a imprimir sigui la següent:



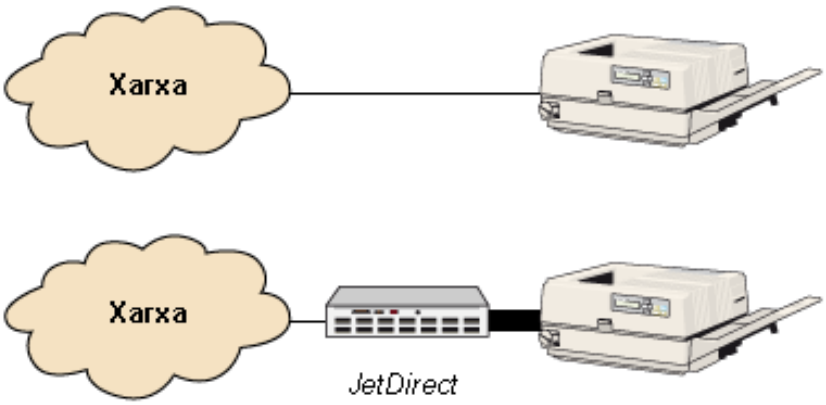
Tenim sis impressores i, per tant, les volem compartir entre tot el personal de l'edifici. La solució més senzilla és connectar-les a l'ordinador més pròxim i compartir-les. En aquest cas són locals per a l'ordinador al qual estan connectades i remotes per a la resta. El principal inconvenient és que només es poden fer servir quan l'ordinador a què es connecten funcioni, cosa que fa que a la pràctica aquesta solució sigui poc útil, especialment per a les impressores corporatives.

La solució que es fa servir per a les impressores remotes és la de connectar-les directament a la xarxa. Hi ha un cable de xarxa que connecta directament la impressora a la xarxa de l'organització.

En aquest cas, s'ha de configurar la impressora perquè es comporti com un dispositiu de xarxa, i després s'ha de configurar correctament en el servidor. Bàsicament els passos són els següents:

1) Connectar la impressora a la xarxa. La connexió física es redueix a connectar la impressora a la xarxa. Els models de gamma alta ja porten una connexió de xarxa, mentre que en els altres es pot fer amb un dispositiu que enllaça la xarxa amb la impressora. En aquest darrer cas es fa per mitjà del port paral·lel, o per USB els dispositius anomenats *servidors d'impressió*.

Esquema de connexió d'una impressora a la xarxa



2) Configurar el dispositiu de xarxa de la impressora. s'ha de configurar el dispositiu de xarxa. Sempre funcionen sobre protocol TCP/IP, per la qual cosa tenen una adreça IP. La configuració del dispositiu, una vegada connectat a la xarxa i engegat, es fa via web, mitjançant una connexió *telnet* al dispositiu o amb un programa específic. A partir d'aquí es configuren tots els paràmetres.

JetDirect

Sovint al dispositiu de xarxa de la impressora se'n diu *JetDirect*, tot i que aquests dispositius de xarxa són els de la marca Hewlett Packard.

3) Declarar en el servidor la impressora física (model, etc.). En el servidor s'ha d'informar que hi ha una impressora remota i de l'adreça IP que té. El tipus i el model d'impressora i les seves característiques rellevants.

4) Associar una cua d'impressió a aquesta impressora declarada. Finalment, cal associar una cua d'impressió a la impressora remota que s'ha creat i engegar-la.

Amb tot això, els usuaris ja podran enviar treballs –que el servidor gestionarà sense problemes– per la xarxa a la impressora. Els administradors gestionen aquesta impressora com si fos local, atès que la cua és al servidor i, per tant, la podrem aturar, arrencar, eliminar-ne treballs, etc.

7.4. *Internet Printing Protocol*

L'*Internet Printing Protocol* (IPP) defineix un mètode estàndard d'enviament de treballs d'impressió emprant Internet. Va ser desenvolupat pel consorci de companyies del sector: *Printer Working Group*.

IPP[35] proveeix un únic i simple estàndard per gestionar els processos d'impressió. En treballar amb TCP/IP, es poden adreçar a una xarxa local, a una intranet o bé a Internet.

(35)Recordeu que "IPP" és la sigla d'*Internet Printing Protocol*.

8. El corrent elèctric

El corrent elèctric és un dels grans oblidats en el moment de dissenyar la disposició dels equipaments. Malgrat això, resulta que els servidors, les estacions de treball, l'electrònica de xarxa, les impressores, els monitors, tots els dispositius i tota l'electrònica associada a la informàtica van connectats.

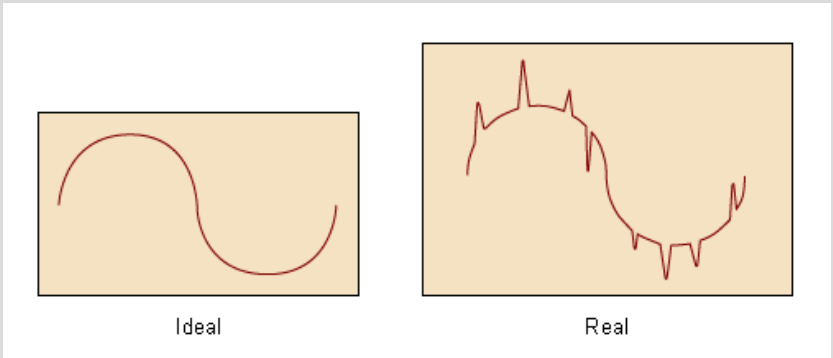
Ens limitem a endollar els equips i suposem que tindrem un corrent perfecte de 220 V, 60 Hz, vint-i-quatre hores al dia, set dies la setmana, tres-cents seixanta-cinc dies l'any. Aquest és un plantejament completament irreal. Ens hem de mirar el corrent elèctric des d'una perspectiva molt més realista.

El corrent elèctric alimenta tots els nostres dispositius i ordinadors, en depenem completament, i pot funcionar malament i ocasionar errors en els sistemes, fins i tot espatllar aparells.

Comencem a estudiar el corrent elèctric que passa per l'organització. Quins són els problemes més habituals que ens pot donar?

- Pics de tensió.
- Caigudes de corrent o microtalls.
- Proximitat amb altres línies. Els senyals d'altres línies properes (de tensió o de dades) influeixen en la qualitat global de la tensió.

Soroll és la suma de pics de tensió i caigudes de corrent.



Què genera aquest soroll en la línia? En general pot venir de tot arreu (qualsevol aparell elèctric), però especialment els motors elèctrics són molt propensos a generar soroll (per exemple, els ascensors, i també determinats elements d'il·luminació, com els fluorescents).

Les següents són conseqüències que pot tenir:

- **Pèrdua o corrupció de dades**. Si afecta l'equip, pot ocasionar canvis a l'atzar en l'electrònica, com per exemple canviar el valor d'alguna posició de memòria, per la qual cosa algun programa (o el sistema sencer) pot fallar.

- **Danys en l'equipament**. Si hi ha grans sobretensions, poden destruir els xips de les plaques de l'ordinador i també fer malbé controladores de disc (amb la conseqüent pèrdua d'informació), memòries, plaques base, etc., de manera que l'equip ja no funcionarà.

- **Desgast prematur**. Si un equip està alimentat amb corrent elèctric de mala qualitat (amb soroll), els circuits electrònics es desgasten abans del que és normal i l'equip falla sense motiu i d'una manera aleatòria. Els xips degeneren d'una manera desconeguda i els resultats són imprevisibles. Llavors poden passar coses com que hi hagi errors de paritat al cap de pocs minuts d'haver arrencat l'ordinador, quan en principi ha passat correctament els diagnòstics.

8.1. La presa de terra

Segons l'informe *Power and Ground for Distributed Computing*, de David Fench i Larry Fish, d'ONEACH Corporation:

"Els edificis tenen una presa de terra de baixa resistència per a protegir la gent de xocs elèctrics. La finalitat de la presa de terra és que el corrent la segueixi perquè hi ha menys resistència i, per tant, en cas de tocar algun aparell electrificat, la descàrrega no passi a través de la persona."

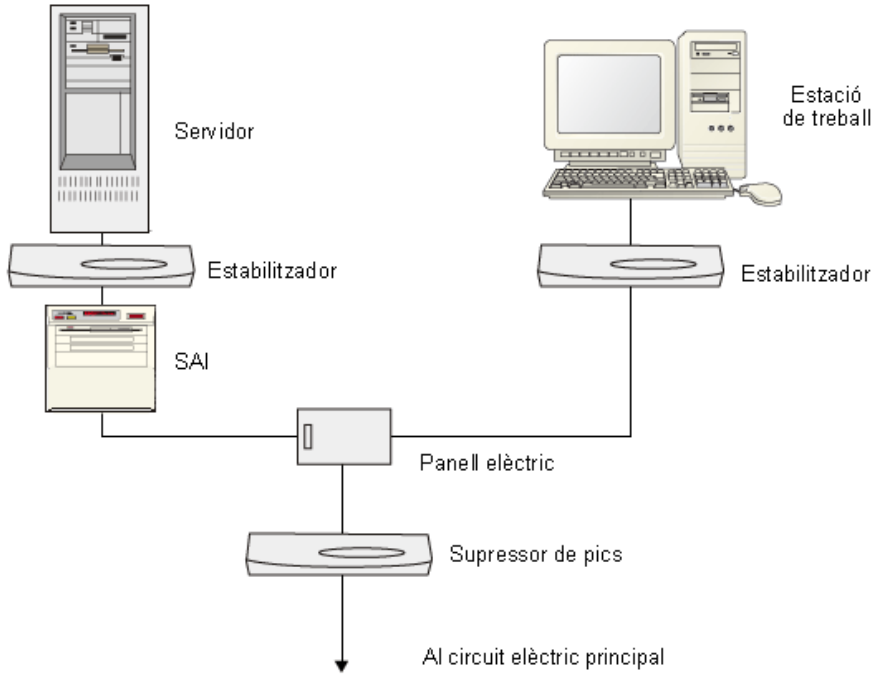
Derivació a terra

La presa de terra és una derivació a terra del corrent elèctric.

Ara bé, les preses de terra actuals no funcionen bé amb els requisits dels dispositius electrònics de la informàtica. El motiu és que moltes vegades el soroll de la línia travessa millor l'equip per a arribar a la presa de terra que el fil de l'alimentació. Això passa perquè en grans xarxes no hi ha un únic punt de presa de terra, de manera que el millor camí és travessar un ordinador.

La solució es proposa amb l'esquema de Fench i Fish.

Esquema de Fench i Fish



Els estabilitzadors aïllen el transformador del corrent i ofereixen una electricitat de qualitat i una bona presa de terra a l'equip. Si es pot, també s'haurien d'instal·lar estabilitzadors en les estacions de treball.

El sistema de suprimir els pics a l'entrada està motivat, perquè en qualsevol altre lloc desviaria els pics que arribessin a l'equip cap al terra, per la qual cosa podrien tornar a entrar al circuit per la mateixa presa de terra.

Finalment, s'ha d'anar amb compte quan es faci el cablejat per no instal·larlo paral·lel a altres circuits de potència. De vegades, el neutre es deriva a terra amb la intenció de solucionar problemes de soroll. Això pot provocar una ona de baixa freqüència repetitiva en el cable de xarxa que pot afectar les dades.

8.2. Sistema d'alimentació ininterrompuda

El sistema d'alimentació ininterrompuda (SAI) protegeix els servidors de talls de corrent i altres problemes amb la tensió.

La importància d'un bon corrent per als servidors es deu al fet que una manca de corrent sobtada (tall) no li permetrà d'aturar-se correctament. Això farà que les memòries intermèdies[36] es perdin i no s'hagin actualitzat en el disc, hagin quedat fitxers oberts i les transaccions no s'hagin completat. És possible que

[36]La memòria intermèdia en anglès s'expressa com a *cache*.

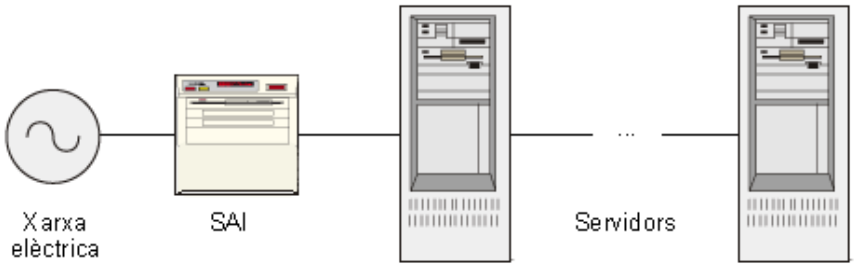
en tornar a posar en marxa el sistema, no es pugui engegar completament i es perdi informació i/o fitxers. Si algun fitxer és una base de dades, les conseqüències poden ser desastroses: s'ha de recuperar de la còpia de seguretat, però des que s'ha fet fins que hi ha hagut el tall s'ha perdut la informació i el temps invertit a entrar-la.

Memòries intermèdies amb bateries

Hi ha sistemes amb memòries intermèdies alimentades per bateries que permeten guardar fins a 72 hores les transaccions pendents.

Un SAI subministra corrent quan la xarxa elèctrica no en dóna, de manera que l'ordinador continua funcionant correctament, sense veure's afectat pel fet que no hi ha subministrament elèctric general. Això permet d'apagar els sistemes amb total normalitat.

Esquema de xarxa amb SAI



Les característiques més rellevants d'un SAI són les següents:

Consum d'un PC

Un ordinador tipus PC sol consumir entre 200 W i 300 W.

- **Potència que cal subministrar**. Són els watts de potència que pot donar el SAI quan no hi ha corrent d'entrada. Determina el nombre de servidors que hi podrem connectar.

- **Temps de durada de les bateries**. Els SAI porten bateries que es carreguen amb el corrent elèctric i són les que després donen electricitat quan falla el corrent general. El nombre de bateries determina el temps que podran subministrar corrent abans d'exhaurir-se.

- **Estabilitzador**. Aquesta característica significa que el SAI, a més a més, és capaç de suprimir el soroll. Malgrat això, necessita una presa de terra per a desviar aquest excés de corrent.

- **Temps de vida de les bateries**. Un SAI serveix de poc si falla quan ha de funcionar. Les bateries tenen una vida útil determinada. Traspassat aquest temps, no hi ha garanties que funcionin i que responguin correctament quan sigui necessari. És el fabricant del SAI qui diu cada quants anys s'han de canviar aquestes bateries.

- **Avís al servidor**. Actualment els SAI porten una línia (USB o sèrie) que arriba a l'ordinador. D'aquesta manera, quan entra en funcionament és capaç d'enviar un senyal al servidor, que amb el programari adient (subministrat amb el SAI) sap que es manté amb l'alimentació elèctrica del SAI. Es manté un diàleg que informa de l'estat de les bateries del SAI i de la seva durada.

Quan falta poc per a esgotar la càrrega de les bateries, el SAI n'informa el servidor i pot procedir a enviar missatges als usuaris i a fer una parada correcta, ordenada i automàtica de l'ordinador. Els servidors acostumen a estar preparats per a arrencar sols, sense intervenció de l'administrador, per la qual cosa quan es restableixi el subministrament elèctric normal, el servidor s'engegarà i tot tornarà a funcionar correctament.

9. Seguretat dels servidors

La seguretat és un tema molt ampli. Aquí, només comentem dos aspectes genèrics referits a la seguretat dels servidors. Aquesta seguretat l'ha de conèixer, aplicar i tenir en compte l'administrador de servidors, i afecta bàsicament el bon funcionament dels servidors corporatius.

Vegeu també

El tema de la seguretat està perfectament cobert en el mòdul "Administració de la seguretat".

9.1. Seguretat física dels servidors

Tot sistema de seguretat, malgrat que sembli molt evident, comença per la seguretat física. No serveix de res protegir tot el sistema informàtic contra tot tipus d'atacs per xarxa si és molt senzill arribar als servidors físicament.

Si podem accedir físicament a un ordinador, podrem accedir a la informació que conté.

Aquesta premissa indica que la informació està segura en la mesura que el servidor està físicament segur. Aquestes són algunes de les precaucions que es poden prendre:

- Tancar el recinte on hi ha el servidor quan no hi treballa ningú.
- Si s'ha de deixar el servidor sense ningú, cal bloquejar el sistema amb protectors de pantalla amb contrasenyes.
- Establir algun procediment en cas d'avaria perquè no desapareguin components amb informació (discos, cintes, etc.).
- Fixar físicament l'equip per a evitar robatoris (cadenes, entre d'altres).
- Si està connectat a la xarxa, pot ser interessant tenir l'equip connectat a un commutador[37] configurat perquè controli que només determinades adreces de placa es puguin connectar al servidor.
- Evitar que l'ordinador arrenqui des del disquet. Configurar-lo perquè només pugui arrencar des del disc dur. Si el servidor no la necessita, fins i tot es pot treure la unitat de disquet.
- Si el servidor té alguna clau per a obrir la carcassa, ha d'estar guardada i lluny del servidor.

(37) Commutador en anglès s'expressa com a *switch*.

- Posar les contrasenyes d'encendre l'ordinador i d'entrar en la configuració de la BIOS.

Activitat

Se us acudeixen altres recomanacions de seguretat? Comenteu-les en el fòrum de l'assignatura.

9.2. Programari

Vegeu també

La seguretat davant d'atacs en un sistema l'hem explicat en el mòdul "Administració de la seguretat".

També hi ha unes precaucions genèriques que es poden aplicar a tots els sistemes operatius. Aquesta seguretat de programari s'orienta a donar unes indicacions sobre les mesures generals que cal prendre per a tenir una màquina físicament més segura.

- Els comptes d'administrador o superusuari que tinguin contrasenyes ben fetes, amb una política de canvi periòdica. De fet, s'ha de seguir aquest criteri per a tots els comptes amb privilegis especials.

- Els comptes amb privilegis especials que no tinguin els noms esperats. Això vol dir que, si és possible, en un ordinador Unix el compte de superusuari no hauria de ser *root*, i en una màquina NT, el compte de màxims privilegis no hauria de ser *administrator* o administrador, perquè d'alguna manera significa donar pistes als possibles atacants. Per exemple, en el cas d'NT és possible (i recomanable) canviar el nom del compte d'administrador per un altre.

- No executar ni instal·lar programari en el servidor, perquè hi ha perill d'instal·lar-hi un virus o programes maliciosos.

- Tenir una política de grups i usuaris per a evitar forats de seguretat en aquest nivell.

9.3. Alta disponibilitat

Alta disponibilitat és la capacitat de mantenir operatives les aplicacions de l'organització, eliminant les parades dels sistemes d'informació. Els sistemes informàtics s'han d'haver configurat per tal de reduir al mínim percentatge el temps d'inactivitat o de manca de disponibilitat, per tal d'aconseguir la màxima cota d'utilitat. L'alta disponibilitat d'un sistema s'aconsegueix en reduir al mínim la possibilitat que un error de maquinari o un defecte de programari comporti la interrupció d'ús del sistema o la pèrdua de dades del sistema. Per tant, la disponibilitat d'un sistema i de les seves dades es pot millorar gràcies a la utilització avantatjosa dels components de maquinari o programari que serveixen per esmorteir l'impacte dels errors.

Mite dels 9

El mite del 9 és el temps que un sistema està actiu a l'any. Es busquen els 5 nous, un 99,999% que el sistema ha d'estar disponible. Això vol dir que en un any pot no estar actiu durant 5 minuts, no necessàriament consecutius.

99%	3 dies i 15 hores
99,9%	8 hores i 15 minuts
99,99%	53 minuts
99,999%	5 minuts
99,9999%	32 segons

Cada 9 que s'afegeix representa un increment de costos molt considerable.

Per aconseguir-ho, s'utilitzen components redundants i aïllats com, per exemple, busos dobles, dispositius d'E/S i còpies dobles de les dades.

L'objectiu és eliminar els períodes de falta de servei a l'usuari. Aquestes parades poden ser dos tipus:

- **Parades planificades**. Aquelles que són degudes a actualitzacions de programari o maquinari.

- **Parades no planificades**. Són les causades per un mal funcionament del maquinari o bé per un desastre ja sigui de caire natural (com ara inundacions o incendis) o de caire no natural (sabotatge, error humà...)

Hi ha organitzacions en què no és imprescindible un servei ininterromput del sistema informàtic. En aquestes és necessari un pla de recuperació de dades per tal de garantir que el temps i el cost de la interrupció seran mínims. En cas contrari, cal que disposem d'una solució d'alta disponibilitat, tot tenint en compte les necessitats reals de la companyia.

Vegeu també

Sobre el pla de recuperació de dades vegeu el subapartat 6.3 en aquest mateix mòdul.

Podem aconseguir alta disponibilitat a través de sistemes tolerants a fallades, o bé mitjançant tècniques de *clustering*. Els sistemes tolerants a fallades són sistemes molt costosos perquè cal assegurar la redundància dels components del seu maquinari i això implica un alt cost. Els sistemes que usen tècniques de *clustering* són més econòmics, ja que no cal utilitzar maquinari específic. A més a més, aquests sistemes ofereixen balanceig de càrrega, per la qual cosa en traiem doble profit amb un cost menor.

Serveis d'alta disponibilitat

L'alta disponibilitat es pot aplicar a qualsevol servei. Els més comuns són:

- Servidor DNS
- Servidor Web
- Servidor de bases de dades
- Servidor de fitxers
- Servidor de correu

9.3.1. Sistemes tolerants a fallades

Aquestes són algunes de les qüestions a tenir en compte en un sistema tolerant a fallades:

- **Redundància en el subministrament elèctric**. Un tall en el subministrament elèctric, encara que sigui de pocs segons, provocarà que durant un temps la nostra màquina estigui fora de servei. Per tant, és vital aconseguir que mai falti el subministrament elèctric. A part de garantir el subministrament, cal tenir en compte també les fluctuacions de tensió, que també poden afectar negativament els nostres equips. Per tant, cal valorar la instal·lació de SAI[38], grups electrògens, fonts d'alimentació redundants en el mateix equip (intercanviables en calent) o fins i tot contractes amb dues companyies elèctriques.

[(38)]Recordeu que SAI és l'abreviatura de sistema d'alimentació ininterrompuda.

Vegeu també

Sobre el corrent elèctric vegeu l'apartat 8 en aquest mateix mòdul.

- **Discos durs redundants**. Per a aconseguir un sistema tolerant a fallades, els discos han de ser redundants, ja que estan sotmesos a errors electrònics (pujades de tensió, per exemple) i a errors mecànics (avaries de capçals, per exemple).

Font d'alimentació redundant

- **Connexions de xarxa**. La xarxa s'ha convertit en un element indispensable per a les aplicacions actuals. És indispensable i per això cal garantir que la xarxa estarà disponible sempre. Per a aconseguir una xarxa tolerant a fallades, cal emprar dispositius de xarxa tolerants a fallades.

9.3.2. Clústers d'alta disponibilitat

Vegeu també

Sobre els discos durs redundants vegeu l'apartat 5, i en especial els subapartats 5.2.5 i 5.3 d'aquest mateix mòdul.

Els clústers d'alta disponibilitat i tolerància a fallades estan destinats a proporcionar disponibilitat ininterrompuda de recursos i serveis mitjançant la redundància. Si un node del clúster falla, les aplicacions i serveis que s'hi executen passaran a executar-se a un dels nodes disponibles.

Vegeu també

Sobre les connexions de xarxa vegeu el mòdul "Administració de la xarxa".

Alguns dels avantatges d'aquest tipus de configuracions són:

- **Escalabilitat**. Pot augmentar la capacitat de càlcul del clúster si s'afegeixen més processadors o equips.

- **Alta disponibilitat**. El clúster està dissenyat per evitar un únic punt d'error. Les aplicacions poden distribuir-se en més d'un equip, aconseguint un grau de paral·lelisme i una recuperació d'errors i proporcionant més disponibilitat.

Utilitat dels clústers d'alta disponibilitat

Els clústers d'alta disponibilitat se solen utilitzar per a sistemes de bases de dades d'aplicacions crítiques, servidors de correu, fitxers o aplicacions.

10. Aspectes legals

L'administrador de servidors és una figura que té al seu càrrec d'una manera directa i/o indirecta una gran quantitat d'informació de l'organització. Tota aquesta informació és sensible, per la qual cosa, a més a més de vetllar perquè estigui disponible i a l'abast de les persones que l'han de fer servir, és informació que l'administrador té poder per a manipular. On hi ha les fronteres legals de tot això? Què ha de fer si li demanen que extregui informació d'un cert lloc? O que la miri? I si li diuen que instal·li un programa que controli l'activitat dels usuaris sobre certa informació? Què pot fer i què no un administrador de servidors amb tota aquesta responsabilitat?

Malgrat que actualment la qüestió va variant força i que la legislació es mou en un panorama molt canviant, intentarem de fer un repàs a aquestes qüestions en el mòdul "Administració de la seguretat".

Vegeu també

Al subapartat 1.3 del mòdul "Administració de la seguretat", trobareu el protocol tècnic que cal seguir en cas d'atac als servidors.

Som conscients que en el moment en què apareix el problema un mateix ha de buscar assessorament legal per a resoldre'l, però considerem que una de les qüestions més importants és saber reconèixer, en matèria legal, quan hi ha un problema real i quan no.

10.1. Col·legis professionals

Actualment, hi ha els col·legis tècnics dels informàtics. Alguns dels seus objectius són els següents:

- Peritar treballs.
- Donar suport legal als informàtics davant de problemes.

Això permet de saber en qualsevol moment quan una acció que han dut a terme els administradors s'ha fet dins o fora de la legislació (si és legal o no) i les conseqüències que pot tenir. Moltes accions, aparentment innòcues, amaguen situacions potencialment problemàtiques. Una cosa tan senzilla com copiar una imatge d'Internet per a fer-la servir o obrir un fitxer del directori personal (carpeta personal en terminologia Windows) d'un usuari, pot violar la legislació vigent. Tenir clares les qüestions, els límits i les conseqüències que se'n poden derivar en cas de transgredir-los és una de les moltes funcions d'aquests col·legis.

11. Tasques/responsabilitats

Una possible relació de les tasques/responsabilitats de l'administrador de servidors podria ser la següent:

- Vetllar pel funcionament correcte dels servidors.
- Tenir cura de la protecció física dels servidors.
- Tenir cura de la còpia de seguretat dels servidors.
- Procurar pel bon funcionament dels subsistemes associats als servidors (cues d'impressió, correu electrònic, etc.).
- Assegurar la disponibilitat d'espai per al treball de les aplicacions i els usuaris.
- Vetllar per uns temps de resposta dels sistemes correctes.
- Assignar els grups d'usuaris i permisos en relació amb el que s'ha acordat amb el responsable d'informàtica.
- Vetllar per la seguretat del sistema.
- Mantenir el sistema operatiu actualitzat.
- Mantenir les aplicacions de què és responsable actualitzades.
- Garantir que la informació del sistema estigui protegida contra fallades, desastres naturals i eliminacions accidentals. Normalment això es fa mitjançant la còpia de seguretat.
- Protegir les dades/el contingut dels servidors.
- Assegurar la disponibilitat de la informació que conté.
- Assegurar l'accés al correu electrònic (des del punt de vista dels servidors).
- Configurar els servidors corporatius.

Activitat

Considereu que falta alguna tasca de l'administrador de servidors interessant? Ho podeu comentar en el fòrum de l'assignatura.

Resum

Hem vist com ha de ser físicament un servidor i les característiques de maquinari que cal tenir en compte. Hem aprofundit en les diferents configuracions dels servidors que ens permeten obtenir funcions i rendiments molt millors que un servidor aïllat. Ens hem adonat de la importància dels discos i de com es poden configurar i ajustar a les necessitats de l'organització, ja que n'és una de les qüestions clau.

Hem remarcat molt els dispositius de còpia de seguretat, les possibilitats i les polítiques possibles per a fer-ne, depenent de la mida i les necessitats de l'organització. Hem fet esment de la importància del corrent elèctric per a assegurar el funcionament i la vida dels servidors.

Finalment, hem comentat aspectes dels sistemes operatius i les responsabilitats de l'administrador de servidors.

Tampoc no hem descuidat la seguretat física dels nostres servidors, perquè contenen tota la informació de l'organització. Tota precaució és poca per a la nostra informació.

Activitats

1. Coneixeu algun sistema de fitxers distribuïts dels que actualment hi ha a la xarxa? (Per als que no en conegueu cap, trieu-ne un i connecteu-vos-hi.) Feu proves amb aquest sistema i compareu-lo amb els sistemes de fitxers tradicionals que coneixeu, per exemple el de la vostra estació de treball.

2. Cerqueu a la xarxa algun programari de virtualització de proves i creeu una màquina virtual. Intenteu instal·lar en aquesta màquina virtual un sistema GNU/Linux i verifiqueu com es poden aprofitar els recursos físics del sistema, com per exemple la targeta de xarxa, el disc, la memòria...

Exercicis d'autoavaluació

1. Suposant que en una organització tenen un servidor amb protecció de discos RAID-6e i una capacitat d'emmagatzematge molt gran, a part d'una gran quantitat de memòria RAM. Quin tipus de servidor creieu que pot ser i quin tipus de dades seria lògic que emmagatzemés?

2. Quin avantatge ens proporciona la còpia de seguretat diferencial enfront d'una còpia de seguretat incremental?

3. Per què creieu que un administrador d'un servidor triaria discos SAS per al seu servidor en comptes de discos SATA?

4. Us proposen d'implementar un sistema dedicat al servei de correus d'usuari, que ha de ser el més segur possible i escalable tenint en compte que l'organització creix en nombre d'empleat constantment. Quina opció de les següents triaríeu?

5. Escriu un petit text en què es relacionin els diferents elements: NAS, estació de treball, accés per bloc, LAN, SAN, dades d'usuari i element d'emmagatzematge.

Solucionari

Exercicis d'autoavaluació

1. Segons les dades que ens han subministrat podem deduir diferents aspectes funcionals del servidor.

Una gran quantitat d'emmagatzematge i una gran quantitat de RAM ens dirigeixen a un servidor destinat a servir dades.

La utilització d'un sistema de seguretat de discos RAID-6e utilitza dos codis correctors per a cada sector i grup de RAID a més d'un disc *Hot Spare* (en espera) per si un dels discos falla. Això significa que les dades emmagatzemades són molt importants i cal protegir-les.

Responent, doncs, a les preguntes, estem parlant d'un servidor d'emmagatzematge, possiblement d'un servidor de base de dades amb dades molt importants per a l'organització.

2. d. L'avantatge més gran que tenim és que salvem tots els objectes modificats des de l'última còpia total i a l'hora de restaurar el sistema només haurem de restaurar la còpia total i l'última diferencial.

3. Tal com s'indica en aquest mòdul, els discos SCSI han estat dissenyats i fabricats per a complir amb els requisits empresarials d'alta disponibilitat i seguretat. Així doncs, els discos SAS, que són l'evolució, també compleixen aquest objectiu.

4. e. Ja que tenint en compte que haurem de donar un sol servei (correu) i que ha de ser escalable, és a dir ha de poder servir un nombre indeterminat d'usuaris, la millor opció és un clúster, que pot ser, no cal dir-ho, un *load balancer* per a aprofitar la potència de treball.

5. Un usuari que treballa amb la seva estació de treball, hauria de tenir les seves dades més importants remotament a un servidor d'emmagatzematge, com per exemple una NAS. Per accedir a aquest servidor farà servir la xarxa LAN de comunicacions.

Tot i que l'usuari accedeixi a la NAS a cercar les seves dades, aquestes potser estan realment en un element d'emmagatzematge al qual accedeix el servidor NAS per bloc mitjançant una xarxa SAN.

Glossari

advanced intelligent tape *f* Vegeu **cinta avançada intel·ligent**.

AIT *f* Vegeu **cinta avançada intel·ligent**.

arsenal redundant de discos econòmics *m* Unitats de discos molt grans i redundància en el sistema per si falla un disc. Es tracta de distribuir la informació entre diverses unitats de disc.
en redundant array of inexpensive disks.
sigla: **RAID**.

alta disponibilitat *m* Instal·lació que intenta aconseguir el màxim de disponibilitat d'un sistema (24x7).

backup *m* Vegeu **còpia de seguretat**.

blade *f* Fulla o làmina. S'aplica a servidors en una targeta o làmina.

blade center *m* Cabina específica per a gestionar *blades*.

cinta àudio digital *f* Dispositiu per a fer còpies de seguretat en cinta.
en digital audio tape.
sigla: **DAT**.

cinta digital intel·ligent *f* Dispositiu per a fer còpies de seguretat en cinta.
en digital intelligent tape.
sigla: **DIT**.

cinta avançada intel·ligent *f* Dispositiu per a fer còpies de seguretat en cinta.
en advanced intelligent tape.
sigla: **AIT**.

clúster *m* Agrupació de servidors que donen servei a una tasca única.

còpia de seguretat *f* Mètode per a duplicar la informació de l'organització sobre un altre suport que sigui més segur.

CPU *f* Vegeu **unitat de control de procés**.

DAT *f* Vegeu **cinta àudio digital**.

descàrrega completa *f* Còpia de seguretat completa d'una partició de disc.
en full dump.

digital audio tape *f* Vegeu **cinta àudio digital**.

digital intelligent tape *m* Vegeu **cinta digital intel·ligent**.

directori *m* Espai lògic dins d'un disc, en què es guarden fitxers i directoris.
sin. **carpeta**.

disc dur *m* Dispositiu físic que serveix per a guardar informació.

DIT *f* Vegeu **cinta digital intel·ligent**.

full dump *f* Vegeu **descàrrega completa**.

IDE *m* Vegeu **lector electrònic intel·ligent**.

Grid *m* Computació en malla que permet interconnectar ordinadors dispersos per la xarxa per aprofitar la seva potència de càlcul.

impressora remota *f* Impressora que està connectada directament a la xarxa informàtica en lloc d'estar-ho a un ordinador. El servidor la gestiona a través de la xarxa, no localment, perquè no hi ha cable.

intelligent drive electronics *m* Vegeu **lector electrònic intel·ligent**.

interfície petita del sistema informàtic *f* Tipus de controladora de dispositius d'altes prestacions. s'hi poden connectar molts dispositius diferents, i les diverses revisions permeten de connectar fins a setze dispositius en la mateixa controladora.

en small computer system interface.
sigla: **SCSI**.

J2EE *f* *Java to enterprise edition*. Estàndard Java orientat a arquitectures d'empresa.

JVM *f* *Java virtual machine*. Màquina virtual de Java. Interpreta les comandes Java en un sistema.

lector electrònic intel·ligent *m* Tipus de controladora de dispositius de baix cost. Normalment s'hi connecten discos durs o CD-ROM. Cada controladora només pot suportar dos dispositius.
en intelligent drive electronics.
sigla: **IDE**.

memòria d'accés aleatori *f* Memòria volàtil que fan servir tots els ordinadors.
en random access memory.
sigla: **RAM**.

motherboard *f* Vegeu **placa base**.

NAS *f* Servidor de fitxers. Accés a nivell de fitxer.

partició *f* Divisió de l'espai intern del disc dur.

placa base *f* Component de l'ordinador que té els busos de sistema i l'àrbitre del bus. Controla tota la comunicació entre els diferents components. Conté la BIOS, l'espai per a muntar la CPU, la RAM i les ranures d'expansió (*slots*) per a la placa gràfica, la placa de xarxa, etc.
en motherboard.

pla de contingència *m* Estudi de l'impacte de possibles contingències i el seu tractament per tal de recuperar la normalitat funcional.

placa de xarxa *f* Component de l'ordinador que permet la comunicació entre la xarxa i els busos interns. El programari fa tota la lògica de sobre.

presa de terra *f* Conductor que es posa en contacte íntim amb el sòl.
(*Diccionari enciclopèdic*, Enciclopèdia Catalana, edició 1984).

RAID *m* Vegeu **arsenal redundant de discos econòmics**.

RAM *f* Vegeu **memòria d'accés aleatori**.

random acces memory *f* Vegeu **memòria d'accés aleatori**.

redundant array of inexpensive disks *m* Vegeu **arsenal redundant de discos econòmics**.

SAI *m* Vegeu **sistema d'alimentació ininterrompuda**.

SAN *m* *Store Area Network*. Xarxa especialitzada en comunicació entre servidors i element d'emmagatzematge.

SAS *m* *Serial Attached Scsi*. Protocol d'accés en sèrie a discos SCSI. Vegeu **SCSI**.

SATA *m* *Serial-ATA*. Protocol d'accés en sèrie a discos ATA. Vegeu **IDE** o **P-ATA**.

SCSI *f* Vegeu **interfície petita del sistema informàtic**.

servidor institucional *m* Ordinador que corre aplicacions amb tecnologia client/servidor i serveix peticions per la xarxa, sota demanda dels clients (estacions de treball).
sin. **servidor corporatiu**.

servidor virtual *m* Ordinador servidor físic que pot donar servei a diferents serveis virtuals, cadascun amb el seu propi sistema operatiu.

sistema d'alimentació ininterrompuda *m* Component que evita la caiguda dels servidors per manca de corrent elèctric, perquè s'encarrega de subministrar-ne quan no n'hi ha.
sigla: **SAI**.

sistema de fitxers *m* Configuració consistent en una partició per a posar-hi els fitxers.

small computer system interface *f* Vegeu **interfície petita del sistema informàtic**.

unitat de control de procés *f* Cervell de l'ordinador.
sigla: **CPU**.

velocitat de transferència *f* Velocitat en Mb/segon a què viatja la informació entre dos dispositius o components.

Bibliografia

Cockcroft, A. (1995). *Sun Performance and Tuning SPARC & Solaris*. Estats Units: Sun Microsystems.

Halliday, C. (1996). *Los secretos del PC*. Madrid: Anaya Multimedia.

IBM (2004). SAN Survival Guide [Disponible en línia]

Microsoft Corporation (1997). *Windows NT 4.0 Workstation Kit de Recursos*. Madrid: Mc Graw Hill.

Muellers, S. (1999). *Upgrading and Repairing PCs*. Estats Units: Que Corporation.

Sheldon, T. (1994). *Novell NetWare 4 Manual de Referencia*. Madrid: McGraw-Hill.

Sun Microsystems Ibérica (1994). *Administración de Sistemas Solaris 2.x*. Madrid.

National Institute of Standards and Technology (2002). *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30.