Alta disponibilitat

Alba Batlle Linares

Índex

Introducció

En ple segle XXI hi ha un fet que és clar: la vida no és possible sense la informàtica. Amb el pas dels anys, la informàtica ha anat evolucionant des dels seus orígens en els camps de la investigació i la recerca per anar ficant-se cada cop més en les nostres vides, fins al punt que actualment gairebé totes les accions quotidianes estan relacionades d'alguna manera amb un procés informàtic. D'aquesta manera la informàtica ha deixat de ser una eina tecnològica per desenvolupar unes tasques concretes i s'ha convertit en una necessitat vital. Podem trobar centenars d'exemples al respecte: el món empresarial, on els sistemes d'informació són la clau sobre la qual es construeixen les empreses; les xarxes socials, que ocupen cada dia més hores en el temps d'oci de les persones...

Històricament, la informàtica es centrava a donar resposta a aquestes necessitats, construint solucions tècniques als diferents requeriments que anaven sorgint en la societat. Avui en dia això no és suficient, la dependència dels sistemes informàtics és total. Imaginem-nos que, per exemple, fem una transferència bancària d'un gran import i en aquell moment el sistema informàtic del banc deixa de funcionar. Què passa si s'han perdut les dades de la transacció? On han anat a parar els diners? Les conseqüències de la fallada del servei poden ser fatals. Això ha provocat que s'hagin de buscar solucions destinades a assegurar la continuïtat dels serveis. Així ha aparegut aquesta nova disciplina anomenada *alta disponibilitat*, que s'ocupa d'assegurar que els serveis imprescindibles sempre estiguin operatius, estudiant les causes de les possibles interrupcions i prenent les mesures adequades per evitar-les.

Al llarg del mòdul s'han donat a conèixer mètodes i tècniques de seguretat informàtica per tal d'evitar qualsevol atac als sistemes, garantint tres dels quatre principis bàsics de la seguretat: confidencialitat, fiabilitat i integritat. No obstant, no podem considerar que un sistema informàtic sigui del tot segur si no es pot garantir també la disponibilitat, tema que tractarem en aquesta última unitat formativa.

En l'apartat "Alta disponibilitat" estudiarem en què consisteix, com es mesura i quan es considera que un servei ofereix alta disponibilitat. Aprendrem el concepte de temps d'inactivitat i identificarem les principals causes que poden induir una fallada en els sistemes. A més, analitzarem detalladament les diferents solucions que permeten obtenir un servei continu de manera segura. El motiu pel qual un servei deixa de funcionar pot ser molt variat i imprevisible: un desastre natural com un llamp, terratrèmol o inundació a la seu d'un empresa on s'allotgen els servidors, un error humà en la manipulació dels equips, un mal manteniment, una fallada esporàdica d'un component... Per tant, cal buscar solucions específiques que donin resposta a riscos específics presents en els diferents nivells d'un sistema informàtic. Així, estudiarem les tècniques que s'apliquen per evitar les fallades de maquinari, els errors de programari, les interrupcions al subministrament

elèctric, les condicions climàtiques i una llarga llista de més amenaces que poden afectar al servei. Conceptes com *redundància*, *recuperació* o *independència* seran recurrents en les diferents solucions implementades.

En l'apartat "Virtualització" ens centrarem especialment en una solució específica d'alta disponibilitat: la virtualització. Així veurem de quina manera aquesta tècnica proporciona fiabilitat als sistemes, a més de portar altres avantatges com l'eficiència d'ús dels servidors i el conseqüent estalvi econòmic. Veurem les diferents variants de virtualització segons l'arquitectura implantada i els avantatges i inconvenients de les diferents opcions. També veurem una alternativa a la virtualització actualment en auge i que és més eficient, però té algunes limitacions: la tecnologia dels contenidors.

Al final d'aquesta unitat serem capaços de reconèixer si una solució és adequada o no per a un servei, avaluant no només la capacitat d'executar les funcionalitats necessàries sinó tenint en compte els seus requeriments de continuïtat en el servei i veient les diferents tècniques d'alta disponibilitat aplicades.

Resultats d'aprenentatge

En finalitzar aquesta unitat formativa, l'alumne/a:

1. Implanta solucions d'alta disponibilitat emprant tècniques de virtualització i configurant els entorns de prova.
    - Analitza supòsits i situacions en les quals es fa necessari implementar solucions d'alta disponibilitat.
    - Identifica solucions de maquinari per assegurar la continuïtat en el funcionament d'un sistema.
    - Avalua les possibilitats de la virtualització de sistemes per implementar solucions d'alta disponibilitat.
    - Implanta un servidor redundant que garanteixi la continuïtat de serveis en casos de caiguda del servidor principal.
    - Implanta un sistema de balanç de càrrega a l'entrada de la xarxa interna.
    - Implanta sistemes d'emmagatzematge redundant sobre servidors i dispositius específics.
    - Avalua la utilitat dels sistemes de clústers per augmentar la fiabilitat i productivitat del sistema.
    - Analitza solucions de futur per a un sistema amb demanda creixent.
    - Esquematitza i documenta solucions per a diferents supòsits amb necessitats d'alta disponibilitat.

1. Alta disponibilitat

Quan parlem de seguretat informàtica, estem parlant en definitiva de fiabilitat, confidencialitat, integritat i disponibilitat. Només si aconseguim complir totes aquestes condicions podrem dir que el nostre sistema és segur.

- **Fiabilitat**: funcionament correcte dels sistemes, realitzant les tasques tal com han estat previstes.
- **Confidencialitat**: garantir que l'accés a les dades del sistema està restringit únicament a les persones autoritzades.
- **Integritat**: assegurar que les dades del sistema no han estat manipulades per persones no autoritzades i que per tant no s'han vist alterades.
- **Disponibilitat**: capacitat del sistema per ser accessible i operatiu el màxim de temps possible.

Tan important és garantir una bona seguretat dels sistemes informàtics tot evitant l'entrada de persones alienes i assegurant la qualitat de les dades que s'hi emmagatzemen com que el sistema estigui disponible el màxim de temps possible. No serveix de res tenir un sistema 100% infal·lible si finalment no pot realitzar les tasques per a les quals s'ha creat i no està disponible a l'usuari.

Per tal d'assegurar la qualitat i la disponibilitat de les dades, fa uns anys que ha sorgit un nou concepte a l'hora de dissenyar els sistemes informàtics.

Els sistemes d'**alta disponibilitat** són sistemes informàtics que han estat dissenyats seguint un conjunt de normes i tècniques per tal que el sistema pugui estar disponible sempre o, si més no, el màxim de temps possible.

Aplicacions de l'alta disponibilitat

En els sistemes informàtics no només és important conèixer l'índex de disponibilitat. També hi ha altres tipus de serveis en els quals és interessant conèixer els temps d'inactivitat. El Metro de Barcelona, per exemple, genera estadístiques mensuals sobre el temps de funcionament del seu servei.

Aconseguir que els sistemes informàtics estiguin disponibles sempre és gairebé utòpic, ja que són molts els riscos que s'han de tenir en compte. No obstant això, les empreses preparen els seus sistemes per tal que estiguin disponibles el màxim temps possible.

1.1 L'alta disponibilitat en els sistemes informàtics

Les empreses són cada cop més dependents dels seus sistemes informàtics i, per tant, una aturada en els servidors els pot suposar elevades pèrdues tant econòmiques com materials. Fins i tot en casos extrems podria suposar la pèrdua de vides humanes. És per aquest motiu que cal dissenyar adequadament els

sistemes informàtics de manera que es trobin disponibles en qualsevol moment i que puguin oferir els seus serveis als usuaris de forma continuada.

Per tal que els sistemes informàtics tingui una elevada disponibilitat caldrà implantar solucions de programari i de maquinari. Cal tenir present que la majoria de solucions d'alta disponibilitat comporten uns costos força elevats.

En el procés de disseny cal determinar les necessitats d'alta disponibilitat que tindrà el nostre sistema i fins a quin nivell és necessari implantar aquest tipus de solucions, ja que a vegades per millorar la disponibilitat unes poques hores s'han de fer grans inversions econòmiques. Per exemple, no té associats els mateixos riscos l'aturada dels sistemes d'una torre de control, una entitat bancària o una botiga virtual que la del sistema comptable d'una perruqueria, un taller mecànic o una botiga de queviures.

En funció del tipus de negoci, no cal que els sistemes estiguin disponibles les vint-quatre hores del dia i, per tant, es poden programar aturades per realitzar tasques de manteniment. I en cas que es produeixi una aturada inesperada, sovint no impediran l'activitat econòmica que es desenvolupa.

Fa uns anys, l'alta disponibilitat estava únicament orientada a donar solució als sistemes informàtics de grans empreses. Tanmateix, en els últims anys s'han desenvolupat solucions menys costoses, fet que ha permès la implantació de solucions d'aquest tipus en empreses petites i mitjanes.

Determinades tasques de manteniment que realitzen els administradors (com actualitzacions, canvis de configuració o algunes còpies de seguretat) provoquen que el sistema deixin d'estar operatiu durant uns minuts. Aquest tipus d'aturades és el que s'anomenen *aturades planificades*, ja que els administradors les planifiquen per realitzar en moments que puguin tenir poc impacte en el funcionament de l'empresa. Estan controlades i es coneix per endavant la durada que tindran. Aquest tipus d'accions que generen un temps d'inactivitat s'acostumen a fer per les nits o en cap de setmana per tal d'afectar el mínim nombre d'usuaris, i sempre es notifiquen per endavant.

El **temps d'inactivitat** és el període de temps en què el nostre sistema no està operatiu i, per tant, no pot respondre a les peticions que realitzin els usuaris. En funció de les causes podem diferenciar dos tipus de temps d'inactivitat: **planificat** o **no planificat**.

D'altra banda, es troben els temps d'inactivitat no planificats, els quals poden ser causats per factors diversos. Per tal de poder identificar els possibles causants cal fer una avaluació de riscos. A continuació s'identifiquen alguns dels possibles riscos que caldrà tenir en compte:

- **Fallades de maquinari**: el sistema deixarà d'estar operatiu si es produeix una aturada en algun dels dispositius bàsics del servidor com són la font d'alimentació, el disc dur o bé la memòria.

- **Talls i fluctuacions del subministrament elèctric**: els sistemes informàtics són molt sensibles als canvis en el subministrament elèctric, que poden ser produïts per una fallada en les fonts d'alimentació locals, fluctuacions de tensió (tant pujades com caigudes de tensió) i per acabar, talls totals en el subministrament elèctric.

- **Pèrdua o bloqueig de la informació**: la informació del sistema pot ser inaccessible ja sigui per un atac o bé per una mala gestió dels usuaris.

- **Fallada en la infraestructura de comunicacions**: avui en dia la majoria de sistemes informàtics estan formats per la unió de diferents dispositius en una xarxa comuna. Un tall en la infraestructura de comunicacions suposarà la fallada del sistema complet, tant si es tracta de comunicacions locals com de comunicacions entre centres.

- **Saturació en els servidors de processament de dades**: sovint, el bloqueig del servidor per un volum de dades superior al que és capaç de gestionar pot suposar una caiguda del sistema.

Un cop s'han identificat els possibles riscos, cal dissenyar i implantar solucions d'alta disponibilitat per tal que si algun d'aquests riscos s'acabés manifestant no representés una fallada del funcionament del sistema informàtic.

Per dur a terme un projecte d'implantació d'alta disponibilitat caldrà que seguim les fases de projecte següents:

1. **Coneixement del sistema i identificació de riscos**: primer de tot cal conèixer en detall l'arquitectura del sistema on treballarem. Cal analitzar tots els components, per insignificants que puguin semblar, per poder identificar els dispositius més crítics i que, per tant, tindran un impacte més gran en cas de fallada.

2. **Establiment dels objectius a assolir**: s'han de definir juntament amb l'usuari quins han de ser els nivells de servei a assolir.

3. **Disseny i planificació**: un cop s'han establert els objectius, es buscaran les possibles solucions per donar resposta aquesta demanda. S'analitzaran una a una i s'escollirà la que més s'adeqüi a les nostres necessitats. Finalment, es realitzarà el disseny del nou sistema i es crearà la planificació del projecte.

4. **Implantació**: a partir del disseny realitzat i en base a la planificació elaborada, es procedirà a la implantació de la solució acordada. Cal ser curosos a l'hora d'implantar un sistema d'aquest tipus, de manera que l'usuari no noti canvis en la qualitat del servei.

5. **Mesura**: validar que la solució implantada assoleix els objectius establerts. En el cas que es produeixi alguna desviació es prendran les mesures correctives per tal de poder aconseguir la fita marcada.

6. **Control**: monitorar i controlar el sistema implantat per tal d'assegurar-nos que està treballant dins dels paràmetres establerts. Al llarg dels anys

els sistemes es van actualitzant i van afegint nous dispositius. Cal també controlar que aquestes variacions del disseny inicial no influeixen de manera negativa en el funcionament del sistema.

1.2 Com mesurar l'alta disponibilitat

Per tal de controlar els temps de disponibilitat dels sistemes informàtics s'ha creat una mètrica de càlcul. Aquesta mètrica es vàlida per a tots els sistemes informàtics. Primer de tot cal establir quina hauria de ser la disponibilitat del nostre sistema. És el que s'anomena SLA (*Service Level Agreement*) **acord del nivell de servei**, que en una empresa normal podria rondar entre 8x5 o un 10x5, depenent dels horaris dels treballadors, que garanteix que els sistemes estaran operatius els cinc dies laborables de la setmana dins de l'horari de treball. Hi ha altres tipus de sistemes, però, que necessiten d'una disponibilitat superior, com poden ser les entitats bancàries les quals han de tenir una acord de servei de 24x365, és a dir que es trobin operatius tots els dies de l'any les vint-i-quatre hores del dia. Aquests acords de servei d'alta disponibilitat també poden anomenar-se 24/7, com el seu nom indica els sistemes es trobaran operatius les vint-i-quatre hores del dia tots els dies de la setmana.

SLA

Els SLA (*Service Level Agreement*) o acords del nivell de servei s'acostumen a utilitzar per establir un contracte entre un proveïdor de servei i un client. En aquest contracte s'estableixen els nivells mínims de qualitat en base a diferents aspectes: temps de resposta, disponibilitat horària, personal assignat... Bàsicament, es realitzen contractes d'aquest tipus amb empreses de telecomunicacions i serveis externalitzats.

Un cop s'han determinat les hores de servei de cada sistema podem passar a calcular el total d'hores anuals que el sistema suposadament hauria d'estar operatiu. En el cas de sistemes d'alta disponibilitat, 24 x 365 = 8.760 hores/any. Si coneixem el total de temps d'inactivitat del sistema al llarg de l'any podem calcular el percentatge de disponibilitat aplicant la fórmula matemàticasegüent:

% disponibilitat = ((X – Y) / X) · 100
On X representa el nombre d'hores que el sistema hauria d'estar operatiu en referència a l'acord de nivell de servei de l'empresa i Y representa les hores d'inactivitat del sistema.

És interessant conèixer alguns dels càlculs més habituals d'índex de disponibilitat i temps d'inactivitat.

Exemple de càlcul de l'índex de disponibilitat

El cap d'informàtica d'un hospital ens ha demanat que calculem l'índex de disponibilitat del servidor on es troben emmagatzemats els expedients mèdics de tots els pacients. L'hospital disposa de servei d'urgències, que està obert les vint-i-quatre hores del dia tots els dies de l'any. Perquè els metges del servei puguin consultar els expedients mèdics s'han implantat algunes mesures d'alta disponibilitat, no obstant això, al llarg de l'any el servidor ha tingut un temps d'inactivitat acumulat de 53 minuts i 14 segons. El cap ens comenta que un índex de disponibilitat inferior a un 99,99% seria insuficient per al servidor de l'hospital.

Primer de tot hem d'identificar quin ha de ser el nombre d'hores que el servei hauria d'estar operatiu. En aquest cas hauríem d'aconseguir que el servidor estigués operatiu vint-i-quatre hores durant 365 dies de l'any per tant un total de 24 x 365 = 8.760 hores. Atès que el temps d'inactivitat està indicat en minuts i segons cal passar el temps d'inactivitat tot a hores per poder aplicar la fórmula. 53 min / 60 = 0,88 hores i 14 segons / 3.600 = 0,0038

hores. Per tant, els 53 minuts i 14 segons equivalen a 0,89 hores. Finalment, calculem l'índex de disponibilitat: ((8.760 – 0,89) / 8.760) · 100 = **99,98%**. Podem determinar que les solucions d'alta disponibilitat implantades no són suficients, ja que l'índex de disponibilitat obtingut és inferior a l'esperat.

Exemple de càlcul del temps d'inactivitat

En una gestoria on els treballadors fan un horari laboral de nou del matí a sis de la tarda, el servidor on s'emmagatzemen les dades de comptabilitat té un índex de disponibilitat del 99%. Quin temps d'inactivitat màxim ha acumulat el servidor al llarg de l'any per arribar a aquest índex d'inactivitat?

En aquest tipus d'exercicis, primer de tot s'ha de determinar el nombre d'hores que hauria d'haver estat operatiu el servidor. Com que no es tracta d'un sistema d'alta disponibilitat, el servidor de comptabilitat només hauria d'haver estat operatiu els dies laborables entre les 9 i les 18 h. Atès que en un any hi ha 240 dies laborables i la jornada laboral de la gestoria és de nou hores diàries, al llarg d'un any el sistema hauria d'haver estat operatiu un total de 240 x 9 = 2.160 hores. En aquest cas, a partir de l'índex de disponibilitat s'ha d'esbrinar el temps d'inactivitat. 99% = ((2.160 – t. inactivitat)) / 2.160. S'aïlla de la fórmula el temps d'inactivitat i s'obté un temps de 21,6 hores.

Exemple de relació entre l'índex de disponibilitat i el temps d'inactivitat

En una empresa d'allotjament web disposen actualment d'un índex d'inactivitat del 99%. Han rebut una oferta força interessant econòmicament d'una agència de viatges que opera per Internet. No obstant això, per acabar utilitzant els seus serveis exigeixen un índex de disponibilitat no inferior al 99,99%. Com s'hauria de reduir el temps d'inactivitat per tal que l'agència de viatges accepti allotjar el seu web en el servidor d'aquesta empresa?

En aquest cas, en tractar-se d'una empresa d'allotjament web, els seus servidors han d'estar operatius 24 hores x 365 dies = 8.760 hores/any. Si l'índex de disponibilitat és del 99%, substituint a la fórmula 99% = ((8.760 – t. inactivitat)) / 8.760 s'obté que el màxim temps d'inactivitat actual és de 87,6 hores. Si es millorés l'índex d'inactivitat al 99,99% = ((8.760 – t. inactivitat)) / 8.760 s'obtindria un temps d'inactivitat màxim de 0,876 hores. Per tant, s'haurien d'implantar millores d'alta disponibilitat per reduir el temps d'inactivitat en 87,6 – 0,876 = 86,724 hores.

A la taula 1.1 podeu veure un quadre resum de la relació entre l'índex de disponibilitat i el temps d'inactivitat per any, mes i dia d'un sistema d'alta disponibilitat.

Taula 1.1. Relació entre percentatge de disponibilitat i temps d'inactivitat per any, mes i dia d'un sistema 24x365

Disponibilitat	Temps inactiu/any	Temps inactiu/mes	Temps inactiu/dia
90%	36,5 d	73 h	2,4 h
95%	18,3 d	36,5 h	1,2 h
98%	7,3 d	14,6 h	28,8 min
99%	3,65 d	7,3 h	14,6 min
99,9%	8,8 h	43,8 min	1,46 min
99,99%	52,6 min	4,4 min	8,8 s
99,999%	5,3 min	26,3 s	0,9 s
99,9999%	31,5 s	2,6 s	0,08 s

Com es pot apreciar en la taula 1.1, per cada increment de disponibilitat, el temps d'inactivitat es redueix de manera significativa. D'altra banda, cal analitzar els costos associats que comporta una millora d'aquest tipus, ja que passar d'una

disponibilitat del 99% a una del 99,99% pot suposar duplicar el pressupost. Fins i tot se sol dir que per cada 9 que millorem en disponibilitat hauríem d'afegir un 0 en el pressupost.

Per aquest motiu és important establir una relació entre les millores econòmiques que ens suposarà augmentar la disponibilitat del nostre sistema i els costos que això comporta. A més, no totes les empreses necessiten tenir una disponibilitat del 99,999%. Només ho necessiten entitats bancàries, sistema de pagament amb targeta de crèdit de grans magatzems, botigues virtuals o torres de control, entre d'altres.

Tanmateix, és important que els administradors sàpiguen interpretar aquests resultats i que per analitzar la disponibilitat i fiabilitat dels seus sistemes no es basin únicament en aquests indicadors, ja que de vegades poden no ser del tot representatius. Per exemple ens podríem trobar amb un sistema amb una disponibilitat del 99,99%, que, tot i estar operatiu, presenta problemes de rendiment i no ofereix un bon servei als seus usuaris. Per tant, cal valorar també el tipus de servei que s'està oferint, no només els temps d'activitat dels dispositius. És per aquest motiu que cal també monitorar els serveis que ofereixen les nostres màquines.

1.3 Solucions d'alta disponibilitat

Un cop s'han identificat els possibles riscos als quals pot estar sotmès un sistema informàtic s'han d'implantar les solucions adients per evitar o mitigar el seu impacte. Les empreses que necessitin garantir una major disponibilitat dels seus serveis hauran d'incrementar les inversions en aquest àmbit per tal de cobrir totes les possibles circumstàncies.

Podem trobar solucions de tot tipus, des de redundància en els dispositius de maquinari a redundància en les comunicacions, passant per centres de processament de dades secundaris i plans de contingència.

1.3.1 Redundància en el maquinari

Un dels riscos que en cas de manifestar-se pot comportar uns majors temps d'inactivitat són les fallades en el maquinari. Si no han estat previstes, aquest tipus de fallades poden deixar el sistema totalment inoperatiu durant hores i fins i tot dies. Tots els elements del maquinari poden deixar de funcionar en un moment determinat, no obstant això, cal identificar quins són més crítics per a la continuïtat del funcionament del nostre sistema. Aquests són, bàsicament, les fonts d'alimentació, els discos durs i la memòria.

Per poder dimensionar adequadament la solució que més ens convé, cal conèixer les dades de fiabilitat dels diferents components que formen un servidor. Normalment, els fabricants d'equips electrònics aporten entre altres dades tècniques l'anomenat MTBF (de l'anglès *mean time between failures*), que és el temps mitjà entre fallades expressat en hores. Es tracta d'una dada estadística obtinguda a partir de proves de laboratori i dels resultats obtinguts de l'experiència amb els components electrònics més elementals, com poden ser els xips, els busos, les resistències... L'MTBF correspon exactament a la probabilitat inversa de fallada d'un sistema. Cal tenir present que varia segons els tipus de dispositius, el fabricants i les gammes de productes. A continuació s'indiquen alguns exemples d'MTBF:

- Disc dur: 10.000-20.000 hores
- Mòdem: 20.000-30.000 hores
- Ordinador personal: 1.000-5.000 hores
- Impressora: 2.000-4.000 hores

Normalment els valors de MTBF no són constants en el temps, sinó que es poden dividir en tres etapes ben diferenciades:

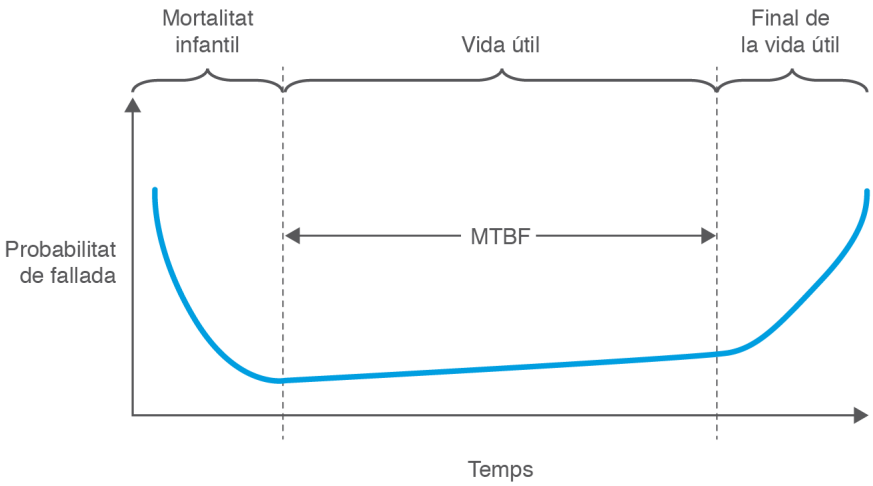
1. **Mortalitat infantil**: es considera que el primer any de vida d'un dispositiu és el període en què poden aparèixer més fallades. El motiu és clar: si hi ha hagut errors en la fabricació, males condiciones en l'emmagatzematge, defectes en els materials emprats per al muntatge o un tractament deficient en les manipulacions, és a l'inici del seu ús on aquests es manifestaran i causaran un mal funcionament.

2. **Vida útil**: passat un any sense fallades, es considera que un dispositiu entra en la seva vida útil i la probabilitat que falli passa a ser l'MTBF indicat pel fabricant, sempre i quan el dispositiu treballi en les condicions necessàries de temperatura, humitat, vibracions... recomanades pel fabricant.

3. **Final de la vida útil**: finalment, passat uns anys es considera que els components s'han degradat degut a l'ús, a la temperatura... i la probabilitat que fallin augmenta considerablement.

En a la figura 1.1 es mostra la fiabilitat d'un dispositiu en el temps, amb les tres etapes diferenciades.

FIGURA 1.1. Evolució de la probabilitat de fallada en el temps



Així, a l'hora de dissenyar els plans per aconseguir una alta disponibilitat en els dispositius de maquinari cal analitzar degudament les dades que aporta el fabricant. En funció d'aquesta anàlisi es pot determinar quines parts del sistema és necessari redundar, que és la principal solució per assegurar l'alta disponibilitat, ja que permet reduir la probabilitat de fallada per dos o, el que és el mateix, duplicar el valor de l'MTBF.

Exemple de càlcul del MTBF

Tenim un servidor que segons el fabricant té una probabilitat de fallada de 1 x 10^{-4}. Per tant, el seu MTBF és: 1 / Probabilitat de fallada = 10.000 hores de vida útil. Aquest valor indica que estadísticament el servidor fallarà cada 416 dies.

L'empresa considera que aquest valor és massa baix i que necessita una disponibilitat més elevada. Per això decideix redundar el dispositiu completament i que dos servidors treballin en paral·lel. D'aquesta manera, la fallada del sistema global només es produirà quan fallin els dos servidors a la vegada.

Per tant, P (sistema) = P (fallada servidor 1) · P (fallada servidor 2) = 10^{-8}.

L'MTBF serà de 100.000.000 hores: la disponibilitat global del sistema ha augmentat de manera significativa.

1.3.2 Redundància de servidors

Atès que en un servidor hi ha diversos components que poden deixar de funcionar i, en conseqüència, impedir al sistema oferir un nivell de servei adequat, s'acostuma a duplicar el servidor sencer. D'aquesta manera, sigui quin sigui el component que ha deixat de funcionar podem garantir un nivell de servei semblant al que s'ofereix en el servidor principal.

Es pot classificar la redundància de servidors en funció de la capacitat de resposta en cas de fallada:

- **Redundància en calent**: es tracta de dos servidors idèntics sincronitzats que treballen en paral·lel, però dels quals només un respon a les peticions del sistema. Disposen d'un programari de supervisió mútua. En cas que el servidor que està responent en aquell moment entri en fallada, el servidor en espera prendrà el relleu en un temps suficient perquè el servei no es vegi afectat, habitualment de l'ordre de pocs mil·lisegons.
- **Redundància intermèdia**: es tracta de dos servidors, un de principal que respon a les peticions del sistema i un de secundari que no està sincronitzat en temps real. El servidor secundari s'actualitza cada cert període de temps prèviament establert, per exemple un cop al dia o un cop per setmana. En cas de fallada es produeix una aturada en el servei, perquè el servidor secundari s'ha d'actualitzar amb les dades del sistema principal. Aquest tipus d'aturades poden durant entre pocs minuts i algunes hores.
- **Redundància freda**: es tracta de dos servidors, un de principal que respon a les peticions del sistema i un de secundari amb característiques semblants, però que no està operatiu. En cas de fallada s'hauria d'iniciar el servidor secundari, instal·lar el programari actualitzat i fer un bolcat de les dades. L'activació d'un sistema d'aquest tipus acostuma a requerir algunes hores i fins i tot algun dia.

1.3.3 Subministrament elèctric

Tan important és preveure arquitectures i solucions d'alta disponibilitat del maquinari com dels sistemes de subministrament elèctric. Sense una bona infraestructura que permeti l'alimentació ininterrompuda dels nostres sistemes és impossible assegurar una alta disponibilitat global.

Els talls en el subministrament elèctric poden produir-se per motius diversos. A continuació s'enumeren algunes de les fallades elèctriques que poden originar problemes en el funcionament d'un sistema informàtic:

- Talls en el subministrament elèctric de la companyia proveïdora de servei.
- Fallades elèctriques dins de la instal·lació de l'empresa a causa de curtcircuits, derivacions...
- Avaria d'un dispositiu elèctric com el transformador, la font d'alimentació...

Per tenir un sistema robust i obtenir el nivell de protecció adequat contra aquestes amenaces es poden utilitzar les solucions següents:

- **Redundància en el subministrament**: es recomana la contractació de dues línies de subministrament elèctric a dos proveïdors de serveis diferents. En el cas que això no sigui possible es recomana disposar de dues connexions

provinents de dues estacions transformadores diferents, d'aquesta manera la caiguda d'una part de la xarxa elèctrica no afectarà el funcionament de la empresa.

- **Arquitectura elèctrica redundada**: dins de l'arquitectura elèctrica de l'empresa es connectaran dues línies d'alimentació per a cada equip crític. Aquestes línies hauran de ser independents, amb protecció diferencial i magnetotèrmica independent. D'aquesta manera, si un dispositiu falla i fa disparar la protecció de capçalera, els altres dispositius no es veuran afectats. Per exemple, en dos servidors redundants s'hauria de disposar de dues línies independents per a cadascun d'ells.

- **Sistema d'alimentació ininterrompuda (SAI)**: aquest dispositiu serveix per estabilitzar la tensió d'entrada, evitar pics i microtalls. A més, aquests sistemes ofereixen protecció contra talls en els subministrament elèctric oferint a partir de bateries l'autonomia necessària per continuar amb l'activitat de l'empresa o per a l'apagament controlat dels sistemes. En casos en què es necessiti un nivell de disponibilitat molt elevat, es col·loquen dos SAI en paral·lel (no deixa de ser un dispositiu que també pot fallar).

- **Redundància de dispositius**: per acabar, també es poden produir fallades en les fonts d'alimentació dels mateixos equips. És per aquest motiu que molts fabricants ja ofereixen servidors amb dues fonts d'alimentació. Tanmateix, redundar totes les fonts d'alimentació de tots els servidors crítics pot suposar un cost massa elevat per a segons quina empresa. Com a alternativa existeixen els clústers d'alimentació (n+1). Aquests clústers estan formats per n fonts d'alimentació connectades en paral·lel que disposen de la potència necessària per a tota la instal·lació més una font addicional per si alguna fallés.

1.3.4 Sistemes d'emmagatzematge redundant

Per garantir el bon funcionament d'un sistema informàtic és important que la informació estigui sempre disponible o bé que en cas de fallada es pugui recuperar quan es necessiti sense que els usuaris se n'assabentin.

Tot i que els discos tenen cada vegada una capacitat més gran i són més fiables, continuen sent un dels principals punts dèbils dels sistemes informàtics. La tecnologia RAID (*Redundant Array of Independent Disks* o conjunt redundant de discos independents) ens permet assolir alts graus de fiabilitat en l'emmagatzematge de la informació.

Un **RAID** és un sistema d'emmagatzematge d'informació que permet combinar dos o més discos d'igual capacitat perquè siguin tractats pel sistema com una única unitat lògica. La informació es divideix i es replica, de manera que s'ofereixen diferents nivells de tolerància a fallades.

Els esquemes RAID poden ser gestionats per:

- **Maquinari**: en aquest cas es necessita una controladora RAID específica que permet alleugerir la càrrega del processador. Aplicant una solució de maquinari obtindrem una tolerància més alta a fallades i millorarem el rendiment de lectura i escriptura als discos. No obstant això, en afegir la controladora RAID també estem afegint un possible nou punt de fallada.
- **Programari**: el mateix sistema operatiu és l'encarregat de gestionar els discos i, per tant, el rendiment del sistema es veu afectat, ja que part del processador ha d'estar dedicat a aquesta gestió.

Com s'ha indicat, les arquitectures RAID gestionades per maquinari ofereixen un millor rendiment. A més, aquest tipus de solucions acostumen a admetre substitucions en calent (*hot swapping*), és a dir, permeten que els discos puguin ser substituïts sense necessitat d'aturar el sistema.

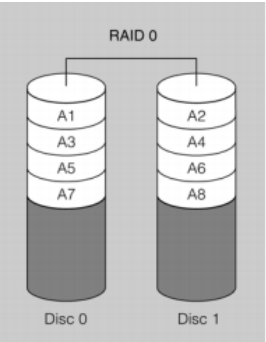
A continuació es detallen els esquemes RAID més comuns.

RAID 0

El RAID 0, també anomenat *stripping*, distribueix equitativament la informació entre els diferents discos durs, de manera que la capacitat de la unitat lògica és la suma de les capacitats dels discos que la formen. De tots els esquemes RAID, aquest és l'únic que no proporciona tolerància a fallades: si un dels discos del RAID falla es perden totes les dades.

Com podem veure en la figura 1.2, les dades es divideixen en petits blocs que es van emmagatzemant de forma alternada entre els diferents discos que formen el RAID. Aquesta manera d'emmagatzemar la informació permet que les lectures i escriptures en el disc puguin ser simultànies, la qual cosa augmenta la velocitat de transferència.

Figura 1.2. Distribució de la informació en un sistema RAID 0



Aquest esquema s'acostuma a utilitzar per millorar el rendiment en entorns on les dades no són crítiques, ja que una fallada en un dels disc suposaria la pèrdua total de la informació.

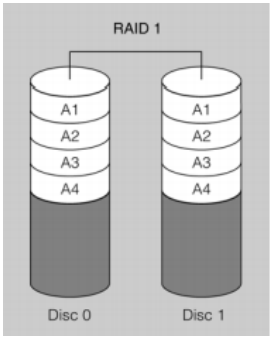
RAID 1

El RAID 1, també anomenat *mirror*, està format per la unió de dos o més disc durs. La capacitat de la unitat lògica correspon a la capacitat del disc més petit. En aquest esquema totes les dades es dupliquen en cadascun dels discos, d'aquesta manera si algun falla es poden recuperar totes les dades sempre que quedi un disc operatiu (figura 1.3).

El RAID 1 ens proporciona un bon nivell de tolerància a fallades, però empitjora l'eficiència pel que fa a l'emmagatzematge disponible, ja que es necessita el doble d'espai per emmagatzemar una informació determinada. La velocitat de lectura i escriptura és semblant a la que podem aconseguir en un sol disc.

Aquest tipus de solucions és recomanable per a empreses petites que volen aconseguir seguretat en l'emmagatzematge de dades sense fer una gran inversió.

FIGURA 1.3. Distribució de la informació en un sistema RAID 1



RAID 5

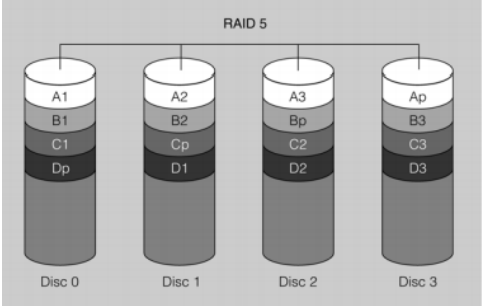
El RAID 5, també conegut com a *stripping amb paritat*, necessita un mínim de tres discos per poder-se implantar. La capacitat d'emmagatzematge de la unitat lògica correspon a la suma de les capacitats de tots els seus discos menys un.

Codis de paritat

Serveixen per detectar i corregir errors en les transmissions de dades. S'incorpora un conjunt de bits calculats a partir d'un algorisme al final del missatge original per tal que el receptor pugui verificar que les dades són correctes.

Tal com s'observa en la figura 1.4, la informació es divideix en petits blocs que es van emmagatzemant alternativament entre els diferents discos. S'introdueixen codis de paritat distribuïts entre els diferents discos per tal de garantir la recuperació de les dades. En el cas de que un dels discos falli es podrà recuperar la informació a partir de les dades emmagatzemades en la resta de discos i els codis de paritat.

FIGURA 1.4. Distribució de la informació en un sistema RAID 5



El RAID 5 ha aconseguit una gran popularitat, perquè ofereix redundància de dades a un cost baix.

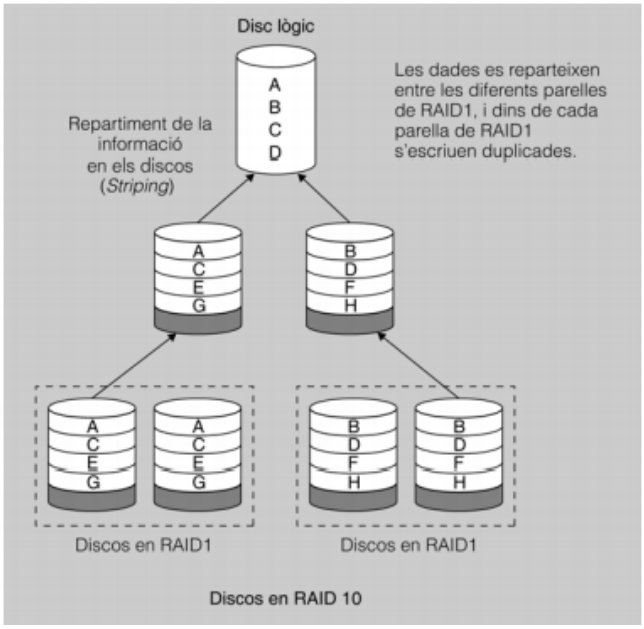
RAID 1+0

Algunes targetes controladores RAID permeten niar diferents esquemes RAID, de manera que ens podem beneficiar dels avantatges que ofereix cadascun. El RAID 1+0 és una combinació d'aquest tipus. Consisteix, concretament, a unir discos amb un RAID 1 com si es tractessin de discos físics en un RAID 0. D'aquesta manera, aconseguim la velocitat en els accessos que ens ofereix el RAID 0 en permetre accessos simultanis i la redundància que ens ofereixen els esquemes RAID 1.

Aquesta combinació es podria també realitzar a la inversa creant un RAID 0+1, però no és recomanable fer-ho, ja que en cas de fallada s'haurien de recuperar més discos.

Com es pot observar en la figura 1.5, per implementar una solució d'aquest tipus són necessaris quatre discos com a mínim, fet que incrementa notablement el cost de la solució.

Figura 1.5. Distribució de la informació en un sistema RAID 1+0



1.3.5 Centres de processament secundaris

Un centre de processament de dades (CPD) secundari està especialment dissenyat per entrar en funcionament quan per qualsevol contingència el centre principal deixa d'estar operatiu. Els costos d'adquisició i manteniment d'un CPD secundari són molt elevats. És per aquest motiu que només són recomanables per a empreses molt grans que requereixin d'una disponibilitat total.

Les característiques tècniques del CPD secundari han de ser les mateixes o molt semblants a les del CPD principal, ja que en cas que entri en funcionament haurà de poder oferir el mateix nivell de servei. A més, caldrà que compleixi amb les mateixes mesures de seguretat tant pel que fa a seguretat física com a la lògica per garantir la integritat de les dades. Es recomana ubicar el servidor secundari a uns 30 o 50 quilòmetres de distància del principal per evitar que els dos CPD es puguin veure compromesos en un mateix desastre natural. A l'hora de triar la ubicació, cal tenir present que quanta més distància hi hagi entre els dos CPD més retard hi haurà en les transmissions de dades i que, per tant, es pot produir un petit decalatge.

Les actualitzacions de dades entre els dos CPD poden ser de dos tipus:

- **Síncrones**: el CPD secundari rep en temps real els canvis que es produeixen en el CPD principal i manté en tot moment una còpia exacta de les dades. En el cas que es produeixi una emergència i entri en funcionament, podrà fer-se càrrec del servei amb la garantia de disposar de totes les dades actualitzades.
- **Asíncrones**: les actualitzacions no es fan en temps real sinó per lots. Per exemple, es poden fer còpies diàries per la nit al CPD principal i restaurar-les al CPD secundari el matí següent. En el cas que el centre secundari entri en funcionament s'ha de tenir present el possible decalatge temporal i actuar amb conseqüència.

En definitiva, sempre és més fiable un centre de processament de dades secundari amb actualitzacions síncrones que un amb actualitzacions asíncrones, perquè en cas de caiguda podrà disposar de tota la informació, mentre que en el que fa actualitzacions asíncrones podem tenir una pèrdua irrecuperable d'informació. D'altra banda, la implementació d'un sistema síncron és molt més cara que la d'un asíncron, ja que s'han d'establir canals de comunicació entre el centre principal i el secundari amb prou capacitat per enviar un gran volum de dades a temps real. A més, aquests costos es disparen com més gran sigui la distància entre els dos centres.

Els CPD secundaris amb actualitzacions asíncrones poden ser una bona solució per a empreses grans que no requereixin una disponibilitat total. Són més econòmics i no necessiten una infraestructura de telecomunicacions tan costosa.

Un altre aspecte a tenir en compte és com es realitzarà entre els dos centres la commutació de serveis. Aquest fet dependrà molt del tipus de servei que es vulgui

traslladar. Pel que fa als sistemes síncrons, la commutació de serveis acostuma a ser senzilla i ràpida, semblant a commutar equips redundants dins d'un mateix CPD. Pel que fa als centres asíncrons, acostuma a ser més complicada i menys automatitzada. Sovint es necessita fer una posada a punt del CPD i realitzar una restauració de les dades, fet que pot provocar temps d'ineficiència en el sistema.

1.3.6 Xarxes i sistemes d'emmagatzematge en xarxa

Les empreses generen un volum de dades cada cop més gran i fer una gestió eficient d'aquesta informació és cada cop més complicat. A més, els usuaris necessiten que les dades es trobin disponibles en tot moment des de diferents plataformes i dispositius. Amb aquest objectiu s'han desenvolupat dues solucions d'emmagatzematge en xarxa: el NAS (sistema d'emmagatzematge en xarxa) i el SAN (xarxa d'emmagatzematge).

Sistema d'emmagatzematge en xarxa (NAS)

Els sistemes d'emmagatzematge en xarxa o NAS (en anglès *Network-Attached Storage*) estan compostos per dispositius d'emmagatzematge que es connecten directament a la xarxa corporativa i permeten compartir les dades amb tots els usuaris de l'empresa (figura 1.6).

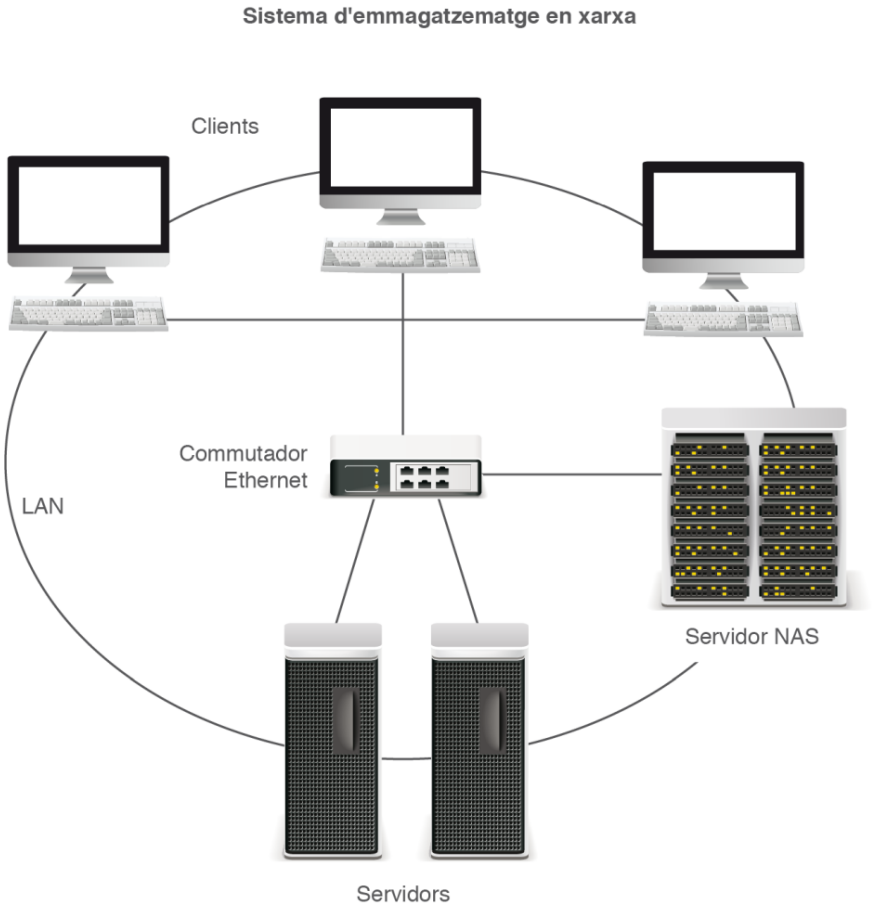
Els servidors NAS disposen d'un maquinari específic per traduir els diferents sistemes de fitxers, des del qual els usuaris poden accedir als dispositius d'emmagatzematge. Internament, els dispositius d'emmagatzematge tenen implantats esquemes RAID, la qual cosa els proporciona un bon rendiment i una alta tolerància a fallades. Podem afirmar que les dades estan protegides, ja que estan centralitzades en el sistema NAS, que té una estructura d'alta disponibilitat.

Per accedir a la informació emmagatzemada en un sistema NAS, s'han de fer servir les funcions del sistema de fitxers del mateix sistema operatiu. Així, les lectures de dades es realitzen a nivell de fitxers i no a nivell de blocs, com es fa habitualment en un sistema d'emmagatzematge local. Això fa que les consultes en el sistema NAS siguin més lentes que en un sistema d'emmagatzematge natiu, fet que pot provocar retards en sistemes que treballin a temps real, tot i que pot ser una molt bona solució per a empreses que no requereixin un temps de resposta tan ràpid.

Els sistemes NAS són fàcils d'instal·lar i d'administrar. A més, en els últims anys han baixat molt de preu i avui en dia són assequibles per a qualsevol empresa i fins i tot per a usuaris particulars.

Els protocols que utilitzen aquests sistemes són el CIFS, l'NFS i l'SMB. Fins i tot podem trobar distribucions de programari lliure que ofereixen serveis NAS, com FreeNas, NASLite i Openfiler, entre d'altres.

FIGURA 1.6. Arquitectura d'un sistema d'emmagatzematge en xarxa

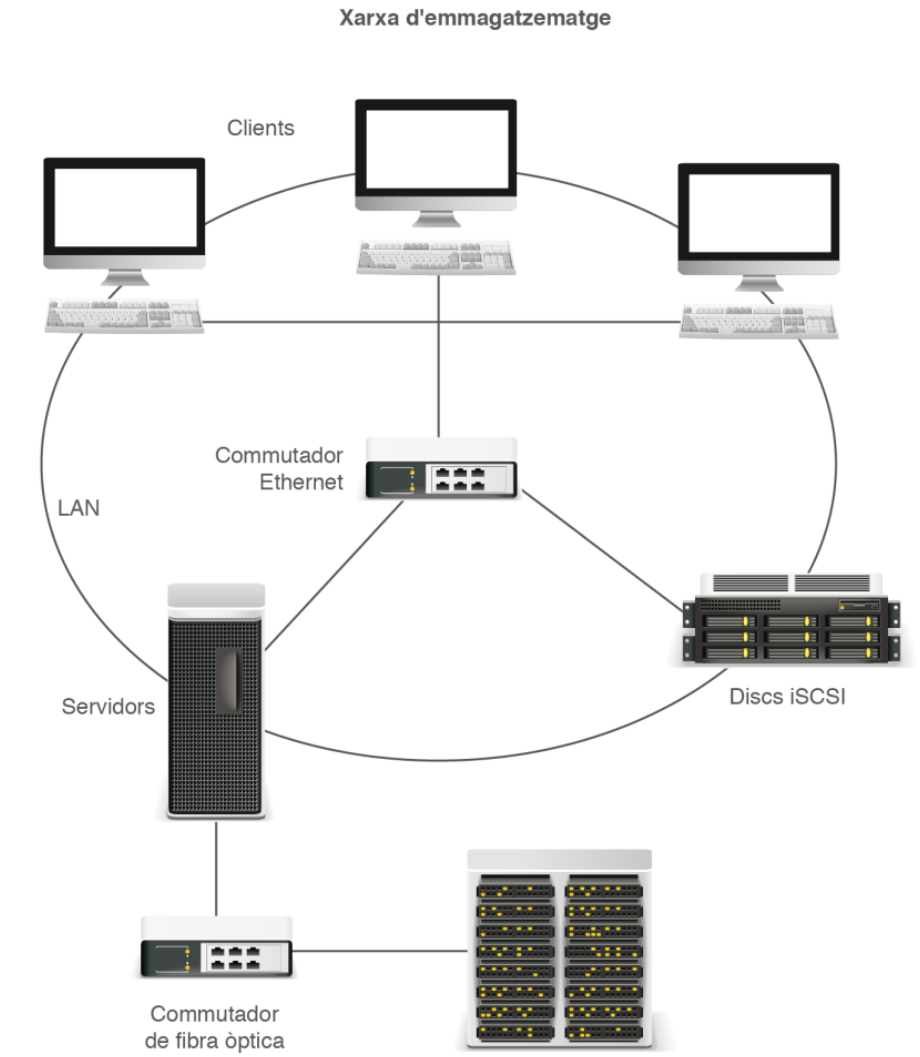


Xarxa d'emmagatzematge (SAN)

En les xarxes d'emmagatzematge o SAN (en anglès, *Storage Area Network*), els dispositius d'emmagatzematge estan connectats directament a una xarxa d'alta velocitat i els usuaris els poden gestionar des del seu sistema operatiu com si hi estiguessin connectats de forma local (figura 1.7).

Els dispositius d'emmagatzematge i els servidors estan connectats a la xarxa mitjançant fibra òptica o iSCSI, que garanteixen rapidesa i fiabilitat en les seves connexions. La fibra òptica proporciona més velocitat. Això no obstant, les targetes i els commutadors de fibra òptica són molt cars. És per aquest motiu que avui en dia la majoria de xarxes SAN utilitzen el protocol iSCSI, ja que les peticions SCSI s'envien pel protocol TCP/IP, sense necessitat d'instal·lar fibra òptica. No són tan ràpides, però permeten reduir costos.

Figura 1.7. Arquitectura d'una xarxa d'emmagatzematge



De tota manera, aquest tipus d'infraestructures són molt costoses i, per tant, només són assequibles per a empreses molt grans.

A diferència dels sistemes NAS, les xarxes SAN no estan orientades a fitxers, sinó a blocs, igual que els sistemes d'emmagatzematge local. D'aquesta manera, els accessos són molt més ràpids, la qual cosa en fa una bona solució per a sistemes a temps real.

Un dels avantatges de les xarxes SAN és que en tenir una connectivitat més alta, els servidors i els dispositius d'emmagatzematge poden estar-hi connectats més d'una vegada i, per tant, creen d'aquesta manera canals redundants, fet que n'augmenta la tolerància davant de fallades.

1.3.7 Solucions d'alta disponibilitat en bases de dades

Avui en dia les empreses treballen amb volums de dades molt grans i la tendència ens indica que en el futur encara s'emmagatzemaran més dades. Ara mateix, les empreses ja no mantenen únicament un llistat dels clients, sinó que acostumen a emmagatzemar altra informació rellevant com: els seus hàbits, aficions, llistat de compres realitzades... Amb tota aquesta informació es poden crear perfils de compres genèrics i individuals, d'aquesta manera l'empresa pot avançar-se a les tendències del mercat i realitzar campanyes publicitàries personalitzades.

Per facilitar les tasques de gestió i administració de les dades, aquesta informació es troba emmagatzemada en bases de dades que disposen de les eines necessàries per poder-ne fer una gestió eficient.

En els últims anys s'ha incrementat en el món empresarial l'ús del programari de gestió ERP (*Enterprise Resource Planning*), que ha fomentat la creació de grans bases de dades on se centralitza tota la informació de l'empresa. Aquest tipus de bases de dades acostuma a estar força exposat a fallades, ja que gestiona un volum de peticions molt elevat i això pot causar errors o caigudes del sistema. Per a moltes empreses, especialment les que tenen negocis molt dependents dels sistemes d'informació, com els bancs, una caiguda de la base de dades pot suposar pèrdues econòmiques importants. Per això les hem d'identificar com un dels punts més crítics del sistema.

La millor manera de reduir el nombre d'errors i fallades en una base de dades és disposar d'un bon disseny inicial que permeti una escalabilitat posterior. També cal que les aplicacions que treballen amb la base de dades realitzin només les peticions indispensables per obtenir la informació que necessiten.

En qualsevol cas, un bon disseny no garanteix que no tinguem cap tipus de fallada o caiguda del sistema. Per això cal que protegim les bases de dades amb sistemes d'alta disponibilitat. El sistema més habitual és disposar de la base de dades de producció, anomenada també *principal* o *primària*, i una base de dades secundària rèplica exacta de la primària. La base de dades replicada entrarà en funcionament quan es produeixi una fallada en la base de dades de producció o quan es realitzi alguna actualització. Per tal de millorar-ne la disponibilitat és recomanable que les dues bases de dades es trobin ubicades físicament en servidors diferents; així augmentarem la disponibilitat en cas d'una caiguda del servidor.

La còpia d'informació entre les dues bases de dades es pot fer de forma síncrona o asíncrona:

- **Síncrona**: en cada transacció que suposa una modificació de la base de dades es copien de manera automàtica tots els canvis a la base de dades secundària i no es dóna la transacció per acabada fins que no s'ha realitzat la modificació en ambdues bases de dades. Aquest mètode empitjora lleugerament el rendiment de la base de dades, ja que les transaccions són més llargues.

- **Asíncrona**: en aquest cas es potencia més el rendiment de la base de dades que la qualitat de les dades en cas de fallada. Es dóna per vàlida la transacció un cop s'han guardat els canvis a producció i es retarda lleugerament la còpia de dades al servidor secundari. Això pot generar petites diferències amb la base de dades original en el cas que s'hagi de restaurar.

Com que els sistemes síncrons tenen la informació actualitzada permeten fer una commutació automàtica de les bases de dades sense riscos. D'aquesta manera, si es produís una caiguda o errada en la base de dades principal, els sistemes de la empresa podrien funcionar amb normalitat amb la base de dades secundaria, sense que els seus usuaris se n'assabentessin.

D'altra banda, quan es produeix una fallada en la base de dades principal d'un sistema asíncron s'ha de forçar la commutació, fet que pot generar pèrdues de dades, ja que la base de dades secundària pot no trobar-se del tot actualitzada en el moment del canvi.

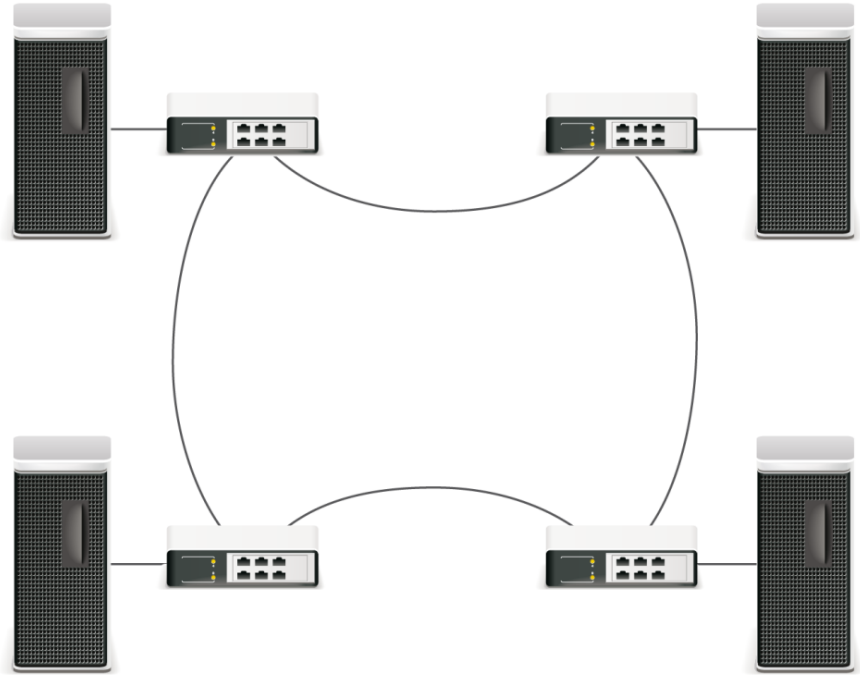
Els principals proveïdors de bases de dades ja ofereixen solucions asíncrones i de commutació automàtica de les dades. És el cas de Data Guard d'Oracle i l'AlwaysOn d'SQL Servers.

1.3.8 Redundància en les comunicacions

Les comunicacions no són menys importants que les bases de dades. No serveix de res tenir un servidor amb una disponibilitat del 100% si els clients no s'hi poden connectar. Per garantir aquesta connectivitat entre servidors i clients, la majoria de servidors disposen de dues targetes de xarxa. Així els serveis no es veuen afectats en cas de fallada. Tanmateix, el servidor pot treballar amb es dues targetes de xarxa com si fossin una de sola, sumant les seves capacitats i millorant el seu rendiment.

Tant si les comunicacions són internes com externes hi intervenen molts dispositius de xarxa (encaminadors, commutadors, concentradors...). La caiguda de qualsevol d'aquests dispositius pot suposar la caiguda del servei. És important redundar la majoria d'aquests dispositius en les xarxes internes de l'empresa perquè una caiguda no afecti a les comunicacions i, en definitiva, al servei ofert. A part dels dispositius de la xarxa també és important replicar els canals de connexió entre els principals dispositius per tal d'evitar que un tall en el canal provoqui la caiguda del sistema. Per això s'acostuma a construir les xarxes amb una arquitectura d'anell, de manera que la caiguda d'un canal entre dos nodes, per exemple per un tall accidental en una fibra òptica, no afecti a les comunicacions del sistema i tots els dispositius puguin seguir estant connectats entre sí i treballar amb total normalitat (figura 1.8).

FIGURA 1.8. Estructura d'una connexió en anell



Una xarxa en anell, però, pot originar alguns problemes en la selecció de rutes per part dels protocols i crear situacions de bucles infinits dins de la xarxa, en els quals els paquets es vagin enviant entre els dispositius de xarxa sense arribar mai a la seva destinació. Per això cal utilitzar protocols que permetin la resolució d'aquests problemes, com fa el protocol Ethernet amb la seva funcionalitat *Spanning Tree* (STP). Aquesta funcionalitat detecta automàticament en una xarxa quan s'ha creat un anell de redundància entre els dispositius, desactiva un dels enllaços entre els nodes de comunicació de manera automàtica i evita així la formació de bucles. Davant d'una fallada en un enllaç, l'STP activa l'enllaç que havia desactivat virtualment per evitar l'aparició de bucles i desactiva l'enllaç que ha caigut realment.

La majoria d'empreses disposen avui d'una xarxa d'oficines connectades entre elles per compartir recursos i dades. Tot i disposar d'una xarxa de comunicacions interna d'alta disponibilitat, aquestes comunicacions entre centres requereixen l'ús de xarxes de telecomunicacions públiques, com per exemple Internet. Així, doncs, els proveïdors de serveis passen a ser un dels punts més crítics del sistema. Una caiguda del proveïdor de servei d'Internet suposa unes pèrdues econòmiques significatives per a la empresa. No només es perden les comunicacions entre les diferents seus, sinó que també deixen d'estar disponibles altres serveis imprescindibles per al bon funcionament de la companyia com el correu electrònic, el web, es perden comunicacions amb els clients... a més que es pot generar la desconfiança de clients potencials.

Per garantir un bon accés a Internet i evitar tots aquests problemes, les empreses opten per contractar dues línies de comunicacions amb diferents proveïdors. Encara es millorarà més la disponibilitat si es contracta l'accés a Internet a dos

proveïdors que ofereixin una tecnologia diferent, per exemple fibra òptica i ADSL. Tanmateix, aquesta opció no sempre és viable.

Disposar de més d'un proveïdor d'accés a Internet ajuda a garantir la disponibilitat de les comunicacions en cas de caiguda del servei i, a més, permet realitzar un repartiment de càrrega entre les dues línies i millorar la seva capacitat.

1.3.9 Repartiment de càrrega

Tot i que el repartiment de càrrega no és una solució d'alta disponibilitat, serveix com a mesura preventiva, ja que permet gestionar el trànsit de la xarxa entre els diferents dispositius de manera que no es puguin saturar les interfícies i provocar una caiguda de les comunicacions. En el cas que una de les interfícies de xarxa caigués, es podrien mantenir les comunicacions a partir de les altres interfícies operatives. Per contra, el rendiment de la xarxa es veuria afectat.

1.3.10 Clúster de servidors

Un dels factors que més impacte pot tenir en el funcionament d'un sistema són les fallades del maquinari. Una caiguda del servidor principal pot tenir uns efectes devastadors i per això es recomana redundar aquest tipus de màquines. No obstant això, no s'ha d'oblidar que és una solució costosa i que no totes les empreses poden permetre-se-la.

Tanmateix, la redundància de servidors no és la única opció. Hi ha altres solucions més econòmiques i més ràpides per continuar amb l'activitat de negoci. Una de les solucions que més implanta a les empreses són els clústers de servidors d'alta disponibilitat.

Per facilitar la tasca de transferència de serveis i dades entre servidors en cas de fallada s'han desenvolupat noves arquitectures de servidors, els clústers.

> Un **clúster** és un conjunt d'unitats funcionals amb característiques similars interconnectades per mitjà d'una xarxa d'alta velocitat i configurades perquè actuïn coordinadament, com una sola unitat.

Els clústers es poden classificar segons la seva finalitat en:

- Clústers d'alt rendiment
- Clústers d'alta disponibilitat

Un **clúster d'alt rendiment** es basa en el processament en paral·lel, que consisteix a unir els diferents nodes en una xarxa i que parts d'un mateix programa s'executin

de forma paral·lela en els diferents processadors connectats. D'aquesta manera s'aconsegueixen sumar les capacitats de càlcul dels nodes que el componen. Sovint, aquestes formacions poden disposar d'un gran nombre d'ordinadors connectats per a la creació de supercomputadors. Aquest tipus d'arquitectura s'acostuma a utilitzar per a la resolució de problemes científics que requereixin processar un gran volum de dades. És el cas dels estudis sobre el genoma humà o el canvi climàtic.

Encara que la finalitat dels clústers d'alt rendiment no és l'alta disponibilitat, també acostumen a incorporar solucions d'aquest tipus, ja que no es podrà assolir un alt rendiment si no s'assegura una alta disponibilitat del sistema. Per això un clúster d'alt rendiment sempre oferirà millors prestacions que un únic ordinador amb igual capacitat de càlcul. A Catalunya, el supercomputador MareNostrum funciona amb aquesta tecnologia.

Supercomputador MareNostrum

A Catalunya tenim el supercomputador MareNostrum, basat en una tecnologia de clúster d'alt rendiment. Va ser creat l'any 2004 i encara avui és un dels superordinadors més potents de tot Europa. Està format per la unió de 10.280 processadors de 64 bits, una memòria de 20 terabytes, 280 terabytes de disc, que li proporcionen una capacitat de procés de 62 teraflops. El Barcelona Supercomputing Center (BSC) és l'organisme encarregat de la seva gestió i de seleccionar els projectes científics que en poden fer ús. S'hi desenvolupen tot tipus de projectes, com per exemple investigacions sobre el genoma humà o l'estructura de les proteïnes. Està ubicat en una antiga capella a les instal·lacions del campus de la UPC a Barcelona.

En un **clúster d'alta disponibilitat**, els diferents nodes que componen el clúster es troben monitorats en tot moment, de manera que si es produeix una fallada en el maquinari o programari d'algun dels nodes, es podran restaurar de forma automàtica els serveis caiguts en un altre servidor. Quan el node caigut torna a estar operatiu es restauren els seus serveis inicials i tot continua funcionant com ho feia abans de la caiguda. D'aquesta manera, la caiguda d'un dels servidors no afecta al funcionament global del sistema.

Els clústers d'alta disponibilitat no només són útils davant d'aturades no planificades, sinó que també són una bona solució per realitzar tasques de manteniment sense deixar d'oferir servei. A diferència dels clústers d'alt rendiment, no acostumen a disposar d'un gran nombre de nodes connectats; sovint es tracta únicament de la unió de dos nodes.

Existeixen diferents configuracions de clústers d'alta disponibilitat, tot i que les més comunes són l'actiu-actiu i l'actiu-passiu.

- **Configuració actiu-actiu**: tots els nodes estan operatius i poden executar els mateixos recursos de forma simultània. En el cas que es produís una fallada en un dels nodes, la resta de nodes del clúster podrien oferir els mateixos serveis, però augmentaria la càrrega dels altres nodes i la qualitat del servei es podria veure afectada. Aquesta configuració permet aprofitar molt millor els recursos del clúster, ja que tots els nodes poden treballar de forma simultània. La implantació d'un solució d'aquest tipus és bastant més complexe que una configuració actiu-passiu.

- **Configuració actiu-passiu**: el node actiu està operatiu i és l'encarregat d'oferir el servei als usuaris, mentre que el node passiu està aturat i només entra en funcionament quan el node actiu pateix una fallada. Aquest tipus de configuració és menys eficient que l'actiu-actiu, ja que en un moment determinat només s'aprofiten els recursos d'un dels dos nodes.

1.3.11 Plans de contingència

Siguin quines siguin les mesures que s'hagin aplicat per garantir l'alta disponibilitat en un sistema, sempre es poden produir fallades que no estiguessin contemplades o que no hagin pogut ser resoltes per les solucions implantades. En aquests casos només ens quedarà posar en funcionament el pla de contingència.

> El **pla de contingència** recull el conjunt de procediments alternatius que permetrien a l'empresa continuar treballant de manera normal en el cas que alguna de les seves funcionalitats es veiés afectada per un accident intern o extern.

A l'hora d'elaborar un pla de contingències, primer de tot cal realitzar una anàlisi de riscos. Aquesta anàlisi consisteix a identificar les causes i conseqüències de les amenaces que pot patir el nostre sistema. Per facilitar la feina, habitualment es dibuixen unes taules en les quals s'identifica per a cada una de les possibles amenaces la probabilitat que es produeixi i l'impacte que tindria en la continuïtat del negoci.

Un cop identificades totes les possibles amenaces es començaran a definir les solucions o processos per evitar que es produeixin o per mitigar-ne l'impacte. Es comença descrivint els processos d'aquelles amenaces que tenen una probabilitat i impacte alt, i s'acaba per les que són molt poc probables i tindrien un impacte molt baix.

Per a cadascuna de les amenaces identificades es descriuen diferents solucions. Algunes seran preventives, d'altres d'actuació i d'altres de recuperació.

- **Solucions preventives**: descriuen les accions que s'han de realitzar per evitar que es materialitzi aquesta amenaça.
- **Solucions d'actuació**: consisteixen en la descripció de les accions que s'han de realitzar un cop s'ha manifestat l'amenaça per tal de mitigar-ne l'impacte.
- **Solucions de recuperació**: són les accions que s'han de realitzar per recuperar el funcionament del sistema.

En un pla de contingència hi trobarem les solucions d'actuació per a tots els riscos identificats. En canvi, no sempre trobarem solucions preventives i de recuperació. Els procediments d'actuació han de contenir la informació següent: les accions a realitzar, la metodologia i el protocol a seguir, els materials necessaris, les persones implicades, les seves funcions i la persona responsable.

Els plans de contingència han ser revisats periòdicament, perquè no quedin obsolets i representin en tot moment la realitat de l'empresa. A part d'aquestes revisions periòdiques, cada cop que es posa en funcionament el pla se'n fa una valoració posterior per identificar possibles millores.

Pla de recuperació en cas de desastre

Un pla de recuperació en cas de desastre (en anglès, *Disaster Recovery Plan*) és un pla de contingència basat en els sistemes d'informació d'una empresa. En aquest pla s'identifiquen les amenaces que poden afectar al programari o maquinari del sistema, que poden causar una pèrdua de dades, en definitiva. Les empreses són cada cop més dependents de les tecnologies de la informació i per això si assegurem aquesta part de la companyia s'evitaran molts problemes derivats.

Aquest pla protegiria els sistemes d'informació contra desastres naturals com incendis i inundacions, actes vandàlics, talls en el subministrament elèctric, aturades del sistema i baixes de personal, entre altres situacions.

Es calcula que un 50% de les grans empreses estan protegides amb plans d'aquest tipus, mentre que en les petites i mitjanes empreses encara és una assignatura pendent, ja que només al voltant d'un 20% tenen plans de recuperació en cas de desastre. Algunes empreses destinen grans quantitats de diners a mantenir aquest tipus de plans. Tot i que poden tenir costos molt elevats, és preferible fer aquest tipus d'inversions que no que es produeixi una pèrdua de dades. Això suposaria pèrdues econòmiques importants per a la empresa i podria causar danys d'imatge irreparables.

Pla de continuïtat del negoci

Els plans de continuïtat de negoci (en anglès, *Business Continuity Plan*) són els plans de contingència que vetllen per la continuïtat de les funcions crítiques del negoci en cas de que es produeixi una interrupció no programada. En aquests tipus de plans, a part de disposar d'un pla de recuperació dels sistemes d'informació en cas de desastre, es detallen els procediments necessaris per poder continuar l'activitat. Per tant, es tracta de plans molt més complexos i que requereixen la implicació de tota la organització.

Perquè aquests plans siguin efectius cal generar una cultura de continuïtat de negoci i campanyes de sensibilització als treballadors, ja que és important que tot el personal participi en la elaboració del pla i sàpiga on trobar-lo quan faci falta.

En el seu procés d'elaboració és important que s'identifiquin les funcions crítiques del negoci i que s'elaborin plans preventius, d'actuació i recuperació per a cadascuna d'aquestes funcions, per tal de poder garantir un servei mínim en cas de contingència. Sovint no és fàcil identificar els processos més crítics o que poden tenir un major impacte de cara els clients. Per poder visualitzar tots aquests aspectes i poder prioritzar els diferents processos s'acostuma a realitzar una anàlisi d'impacte (en anglès, *Business Impact Analysis*). En aquestes anàlisis s'identifica per a cada funció l'impacte econòmic i d'imatge, temps de recuperació i els recursos requerits per continuar amb el seu funcionament. En base a aquestes anàlisis es prioritzen els processos i s'elaboren els procediments d'actuació.

2. Virtualització

Sovint, les empreses instal·len un servidor per cada servei a oferir. Aquesta és la opció més fàcil i segura, i garanteix una bona qualitat de servei. Podem trobar empreses que disposen d'un servidor específic per a l'allotjament web, que està en espera la gran part del dia i té un temps d'ús del 5-10%. I el mateix passa amb el servidor de correu, el de la base de dades...

Des de fa uns anys moltes empreses han utilitzat solucions de virtualització per millorar el rendiment del seu maquinari, a banda d'altres avantatges d'aquesta tecnologia, com per exemple l'alta disponibilitat.

La **virtualització** consisteix a crear amb un programa específic una capa d'abstracció sobre una màquina física perquè els seus recursos puguin ser compartits i utilitzats per múltiples usuaris. Es poden virtualitzar servidors, sistemes d'emmagatzematge, connexions de xarxa, estacions de treball, aplicacions i sistemes operatius.

Inicis de la virtualització

En els últims anys s'ha potenciat molt la virtualització a les empreses a causa dels nombrosos avantatges que ofereix. No obstant això, no es tracta de cap tecnologia nova, ja que en els anys 60 ja s'utilitzaven solucions d'aquest tipus. En aquell moment les empreses disposaven d'un únic supercomputador i virtualitzaven el sistema per tal que cada treballador pogués treballar amb una part d'aquest com si es tractés d'un ordinador independent.

No obstant això, l'ús principal de la virtualització és la creació de múltiples ordinadors o servidors completament independents, coneguts com a *màquines virtuals*, en un sol ordinador físic. Tot i que les màquines treballen de forma independent, comparteixen els mateixos recursos de maquinari (processador, memòria, disc dur i interfícies de xarxa). Això és possible gràcies a l'**hipervisor**, també anomenat **monitor de les màquines virtuals** o VMM (de l'anglès *Virtual Machine Monitor*), que és el programa que arbitra i gestiona dinàmicament aquests recursos entre totes les màquines virtuals.

2.1 Objectius de la virtualització

Enumerem a continuació alguns dels principals avantatges i objectius de les empreses que utilitzen la virtualització:

- **Millorar els índexs d'utilització del maquinari**: avui podem trobar molts servidors que tenen índexs d'utilització del 10 o el 15%. Això suposa una inutilització dels sistemes i, per tant, una pèrdua de diners en la inversió realitzada. Aplicant tècniques de virtualització podem oferir més d'un servei en una mateixa màquina física. D'aquesta manera aconseguirem índexs d'utilització d'un 70 o 90% i aconseguim fer més eficients les inversions realitzades.

- **Problemes d'espai en els centres de processament de dades**: en els últims anys ha augmentat molt el volum de dades digitals que han de tractar les empreses, ja que molts processos que abans eren manuals i es feien en paper ara estan digitalitzats. Altrament, també han augmentat els serveis de què disposen: servidors de pàgines web, intranets, correu electrònic... i, sovint, les sales de servidors havien estat dimensionades per a una altra realitat. Unificant processos gràcies la virtualització es poden pal·liar aquests problemes d'espai i evitar haver de fer reformes o crear nous CPD, ja que són molt costosos.

- **Reduir costos en el subministrament elèctric**: cada cop les empreses destinen més diners al subministrament elèctric a causa de l'increment de les tarifes i sobretot de l'increment del nombre d'aparells electrònics. Amb la virtualització es pot reduir el nombre de servidors físics i, per tant, la despesa en energia, contribuint a la conservació del medi ambient, moviment que en anglès s'anomena *green IT*.

- **Reduir costos d'operació**: els ordinadors no són autònoms del tot, necessiten ser monitorats, actualitzats, reparats i revisats pel personal tècnic de l'empresa. La virtualització ajuda a reduir els costos en aquestes operacions.

- **Afegir flexibilitat i escalabilitat**: les empreses canvien i ho fan molt ràpid. D'altra banda, els sistemes d'informació sovint són rígids i és difícil adaptar-los a les noves necessitats de l'empresa. Amb la virtualització, aquests canvis son molt més ràpids i els problemes d'escalabilitat desapareixen.

- **Pla de recuperació en cas de desastre**: una de les millors solucions en cas de desastre és disposar d'un centre de processament de dades secundari que pugui entrar en funcionament quan es produeixi una caiguda en el servei. No obstant això, aquesta solució és molt costosa i poc eficient, ja que si no es produeix cap caiguda el centre secundari estarà infrautilitzat. Algunes empreses sense tants recursos veuen en la virtualització una solució, ja que permet restaurar, crear o transferir màquines virtuals i continuar amb l'activitat de negoci en pocs minuts.

- **Compatibilitat d'aplicacions**: sovint, quan es realitzen actualitzacions en els sistemes, algunes aplicacions una mica antigues poden deixar de funcionar, ja que no estan pensades per treballar amb un sistema operatiu tan modern. Això pot suposar un problema en el funcionament de l'empresa ja que sovint es tracta d'aplicacions pròpies que van costar molts diners i que encara funcionen correctament. Amb la virtualització podem simular màquines més antigues per tal que aquestes aplicacions puguin continuar executant-se.

- **Entorn de proves**: abans de donar per vàlid un programa, els desenvolupadors necessiten executar-lo en un entorn el més semblant possible al servidor de producció. Per contra, s'ha de tenir present que en tractar-se d'un programa en fase de desenvolupament pot ser que encara no estigui prou depurat i que pugui produir algun problema en el funcionament del sistema. Per aquest motiu les proves es realitzen en un entorn controlat. La

virtualització permet proveir un entorn de proves econòmic, que es pot restaurar de forma ràpida en cas de fallada sense interrompre el funcionament del sistema productiu.

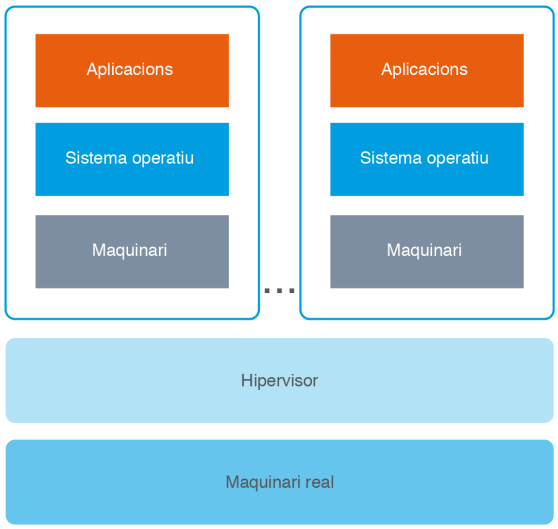
2.2 Virtualització de servidors

La virtualització de servidors consisteix en la creació de màquines virtuals amb el seu propi sistema operatiu que funcionen com si es tractessin de servidors totalment independents. D'aquesta manera, en un únic servidor físic es poden allotjar diferents servidors virtuals, els quals poden funcionar amb diferents sistemes operatius. Dins de la virtualització de servidors podem trobar diferents tècniques: la virtualització nativa, la virtualització allotjada i la paravirtualització.

2.2.1 Virtualització nativa

L'hipervisor s'executa directament en el maquinari físic per controlar l'assignació de recursos i memòria entre les diferents màquines virtuals, a més de proporcionar una interfície per a l'administració a alt nivell i eines per monitorar. Tal com s'observa en la figura 2.1, les màquines virtuals s'executen de manera simultània en un nivell superior.

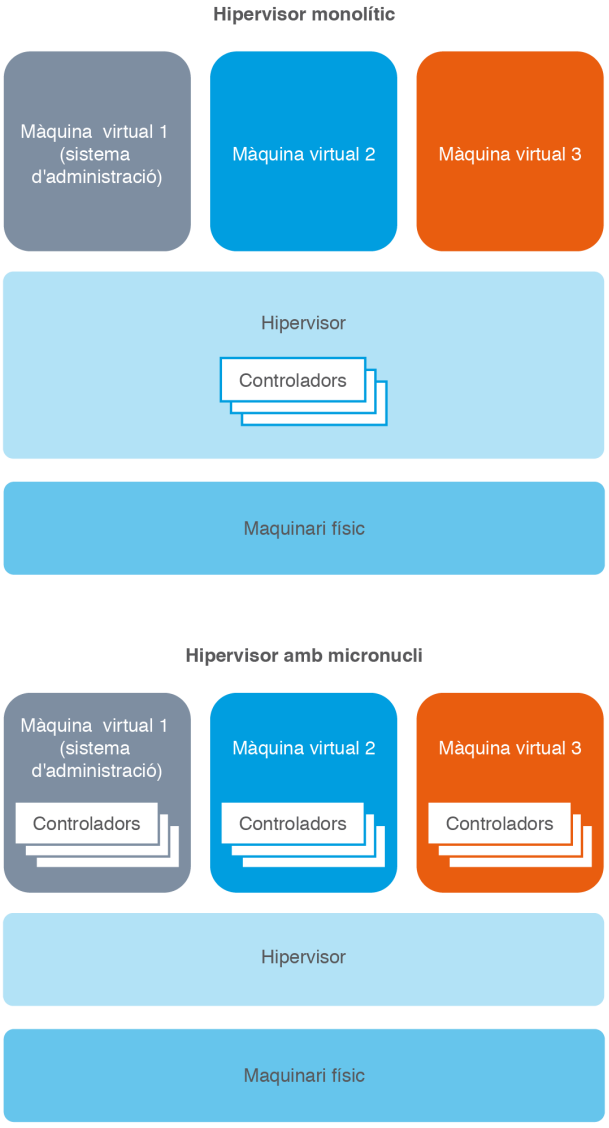
Figura 2.1. Estructura d'un sistema de virtualització natiu



L'hipervisor s'executa en l'anell 0 de la CPU i, per tant, els sistemes operatius de les màquines virtuals hauran d'estar modificats i utilitzar anells superiors. Això complica la virtualització nativa, ja que la majoria del sistemes operatius estan dissenyats perquè s'ubiquin en l'anell 0, perquè hi ha algunes tasques que només es poden realitzar en aquest nivell, com per exemple l'execució d'instruccions amb privilegis a la CPU o l'accés directe a la memòria.

D'altra banda, depenent de l'arquitectura, l'hipervisor pot disposar o no dels controladors necessaris per a la gestió dels recursos de maquinari o bé pot ser el mateix sistema operatiu de la màquina virtual el que els té prèviament instal·lats. En la figura 2.2 podem observar aquestes dues situacions.

FIGURA 2.2. Arquitectura dels hipervisors



Com que l'hipervisor té accés directe al maquinari, sempre oferirà un millor rendiment que la virtualització allotjada, ja que utilitza menys recursos.

Alguns exemples de virtualització nativa són VMware ESXi, VMware ESX, Xen, Citrix XenServer i Microsoft Hyper-V Server.

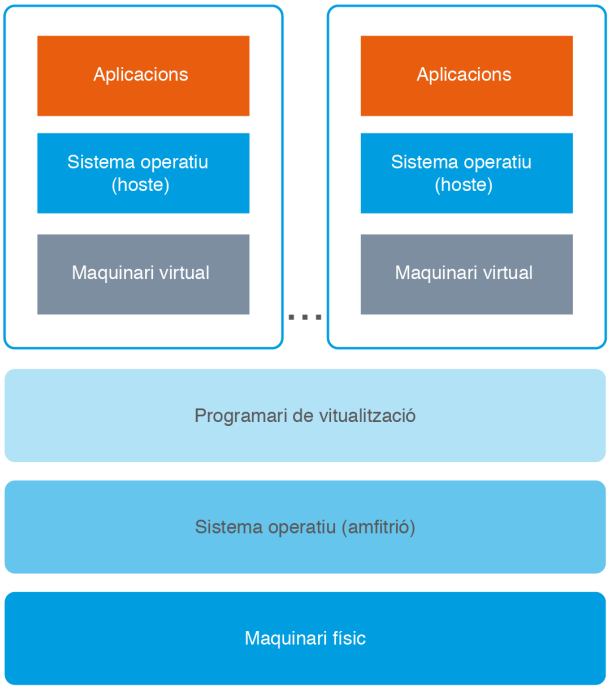
2.2.2 Virtualització allotjada

En la virtualització allotjada, l'hipervisor s'executa sobre un sistema operatiu convencional per després virtualitzar diferents sistemes operatius. En aquesta

arquitectura, l'hipervisor proporciona a cada màquina virtual tots els recursos de la màquina física, incloent una BIOS virtual i una memòria virtual. Aquesta situació fa que el sistema allotjat tingui la sensació que s'està executant directament en la màquina física en lloc d'en una màquina virtual dins d'una aplicació.

En la figura 2.3 podem observar l'estructura d'un sistema de virtualització allotjada.

Figura 2.3. Estructura d'un sistema de virtualització allotjada



La virtualització se situa en una capa més allunyada del programari que en la virtualització nativa, fet que afecta al rendiment de l'hipervisor.

Alguns exemples de virtualització allotjada són VirtualBox, VMware Workstation, VMware Server, VMware Player, QEMU, Microsoft Virtual PC i Microsoft Virtual Server.

2.2.3 Paravirtualització

En la paravirtualització, l'hipervisor està allotjat sobre el maquinari de la màquina física, és a dir que es tracta d'un sistema de virtualització nativa. Tal com es fa en la virtualització nativa, les màquines virtuals es creen sobre l'hipervisor, que és específic i més simple que els de virtualització nativa, ja que en la paravirtualització les màquines virtuals disposen de privilegis que els permeten accedir directament a alguns recursos de la màquina física.

Que les màquines virtuals puguin accedir directament a alguns recursos del sistema té com a objectiu millorar el temps d'execució, ja que algunes tasques

són molt més difícils d'executar si es realitzen des d'un entorn virtualitzat que si es realitzen directament en la màquina nativa. Els sistemes operatius utilitzats en les màquines virtuals d'un sistema de paravirtualització han de ser creats específicament per a aquesta utilitzat.

Per exemple, Xen ofereix una solució d'aquest tipus en la qual el rendiment de les màquines virtuals només es veu afectat entre un 2 i un 8% respecte del que obtindrien si estiguessin funcionant directament en la màquina física. Aquest projecte s'anomena XenWindowsGplPv.

2.3 Virtualització d'escriptoris

Els servidors no són els únics dispositius que es poden beneficiar dels avantatges de la virtualització en una empresa. També es poden virtualitzar els escriptoris, els sistemes d'emmagatzematge, aplicacions i xarxes.

La majoria d'empreses i organitzacions disposen de multitud de dispositius. En moltes companyies gairebé cada treballador disposa d'un ordinador, a part d'altres dispositius d'accés al sistema com ordinadors portàtils o dispositius mòbils. La gestió d'aquest volum de dispositius genera una càrrega de feina molt gran per al personal informàtic de l'empresa, ja que ha de realitzar tasques de manteniment, còpies de seguretat de les dades i actualitzar el sistemes operatius, els antivirus, les aplicacions o els pedaços de seguretat de cadascun d'aquests dispositius. No fer-ho podria causar grans problemes de seguretat. Per solucionar aquests problemes, les empreses comencen a implantar solucions de virtualització d'escriptoris.

La **virtualització d'escriptoris** trenca amb la concepció que l'escriptori són tots els programes i les dades ubicats en una màquina física, i el defineix com el conjunt d'aplicacions i dades amb què un usuari treballa, independentment del dispositiu amb què hi accedeixi.

Quan els usuaris treballen en un escriptori virtual, tots els programes i dades estan emmagatzemats en un servidor compartit on s'emmagatzemen i executen de manera centralitzada. Això permet als usuaris accedir als seus escriptoris des de qualsevol dispositiu, com un ordinador, un portàtil, un telèfon intel·ligent o un client lleuger. Sovint s'acostuma a utilitzar aquesta última opció, ja que els clients lleugers són més econòmics i fiables que els ordinadors convencionals, perquè en no disposar de discos d'emmagatzematge local redueixen la probabilitat de fallar.

En aquest tipus de virtualització és necessària una bona connexió entre el servidor i els clients. Si aquesta connexió és deficient, pot provocar problemes en el rendiment del sistema. S'ha desenvolupat una variant de virtualització d'escriptoris anomenada *Check In Check Out* en què els clients descarreguen a l'inici de la sessió el seu sistema i hi treballen en local sense necessitat de connectar-se constantment al servidor. Al final de la sessió tornen a fer un bolcat de l'escriptori al servidor principal, cosa que deixar el dispositiu utilitzat completament net.

S'acostuma a utilitzar aquesta variant en connexions poc fiables, com per exemple connexions d'usuaris que treballen des de casa o que estan de viatge.

En les primeres solucions de virtualització d'escriptoris es creava en el servidor una imatge de disc per a cada usuari de l'empresa. Això suposava un gran volum de dades emmagatzemades en el disc del servidor, la qual cosa podia provocar problemes d'espai. En canvi, avui en dia s'emmagatzema una única imatge que es pot clonar per a cada usuari i només s'emmagatzemen de manera separada les configuracions personals. Quan un usuari acaba la sessió, totes les dades i modificacions de configuració es tornen a emmagatzemar en el servidor i no queda cap informació en el dispositiu.

La virtualització d'escriptoris ofereix molts avantatges a les empreses:

- **Augment de la seguretat**: els usuaris executen un escriptori virtual ubicat en el centre de processament de dades. D'aquesta manera, els usuaris finals no poden ni instal·lar ni modificar el programari del seu escriptori. Són els administradors els encarregats de definir un perfil per a cada tipus de treballador i d'assignar-los únicament aquelles aplicacions que necessiten. Així, els administradors poden gestionar de manera centralitzada els escriptoris en comptes de fer-ho físicament, assegurant que els usuaris no puguin modificar res del sistema operatiu i que a més es realitzen totes les actualitzacions de seguretat i d'antivirus.
- **Seguretat de les dades**: les dades estan centralitzades en el servidor de l'empresa, la qual cosa impedeix als usuaris treballar amb fitxers ubicats en el seu disc local. Això facilita la realització de còpies de seguretat i garanteix que tota la informació compleix la normativa de seguretat de l'empresa. A més, evita que es puguin produir fuites o malversacions de dades confidencials. Amb la virtualització d'escriptoris és més difícil poder extreure documents de la empresa i, en cas de pèrdua o robatori d'un ordinador portàtil, no s'haurà de patir pel seu contingut, ja que no contindrà cap informació compromesa.
- **Reducció de costos**: la virtualització d'escriptoris permet reduir costos de manteniment per part del personal d'informàtica, ja que es podran mantenir tots els ordinadors de la empresa de manera centralitzada, sense necessitat de desplaçar-se físicament. D'altra banda, també permet reduir costos en maquinari. Com que les aplicacions s'executen en el servidor. no es necessiten estacions de treball d'última tecnologia. Sovint, amb un client lleuger (més barat que un ordinador convencional) connectat al servidor n'hi haurà prou. A més, la vida útil d'aquest tipus de dispositius és del voltant d'uns sis anys, mentre que la d'un ordinador normal és de tres.
- **Respecte al medi ambient**: en centralitzar tots els càlculs en el servidor, el consum elèctric dels clients lleugers és molt inferior que si s'executessin les aplicacions de forma distribuïda. És calcula que pot suposar un estalvi energètic d'entre el 50 i el 90%.
- **Continuïtat de negoci**: la virtualització d'escriptoris és una solució senzilla i eficient a implantar en un pla de recuperació en cas de desastre.

Les empreses que disposen d'aquesta tecnologia podran continuar la seva activitat des de qualsevol dispositiu que tingui connexió amb el servidor.

- R**educció del temps d'inactivitat**: en cas de fallada del maquinari o el programari, en pocs minuts es pot restaurar l'escriptori i continuar treballant amb el que s'estava fent en el mateix dispositiu o des d'un altre, la qual cosa redueix de manera significativa el temps d'inactivitat dels usuaris finals.
- **Millora de la productivitat**: en tractar-se d'escriptoris restringits, els treballadors no poden instal·lar programari no permès. D'aquesta manera es pot garantir que els usuaris només tenen accés a les aplicacions autoritzades per la empresa i que, per tant, dediquen tot el seu temps a la feina, sense distraccions que puguin reduir la seva productivitat.
- **Escalabilitat**: la virtualització d'escriptoris facilita gestionar el creixement d'una empresa i, en definitiva, l'escalabilitat dels seus sistemes. Quan un nou treballador entra a l'empresa, en pocs minuts pot disposar d'un escriptori amb totes les aplicacions necessàries.

Tot i el gran ventall d'avantatges que ofereix la virtualització d'escriptoris, encara són poques les empreses que han optat per implantar solucions d'aquest tipus. En canvi la majoria d'empreses s'han beneficiat dels avantatges de la virtualització de servidors ja que són solucions que aporten molts avantatges, relativament fàcils d'implantar, no requereixen una gran inversió i ofereixen beneficis immediats.

A la llarga, implantar solucions de virtualització d'escriptoris suposarà una reducció de costos per a l'empresa (manteniment, consum elèctric, vida útil dels dispositius). No obstant això, en el moment de la implantació s'ha de fer una inversió econòmica important en l'estructura de xarxa i servidors. A part, suposa canviar la filosofia de treball i el funcionament de tota l'empresa. Per tant, no es tracta únicament d'un canvi en el departament de sistemes, sinó que cal implicar tota la organització.

2.4 Virtualització d'aplicacions

A diferència de la virtualització d'escriptoris remots, en la virtualització d'aplicacions no es recrea totalment un ordinador, sinó que es virtualitza només una aplicació en concret. En aquest cas, cal interpretar la virtualització d'aplicacions com la separació dels llocs on s'executa l'aplicació i on es mostren les dades al usuari. Les aplicacions estan allotjades en el servidor principal, on s'executen a petició dels usuaris a través d'un terminal client. Dins de la virtualització d'aplicacions existeix una variant en què les aplicacions no s'executen en el servidor, sinó que es descarreguen i s'instal·len en el client cada cop que s'han d'utilitzar.

Aquest sistema pot semblar repetitiu, però permet als administradors controlar millor les aplicacions, assegurar-se que tots els usuaris utilitzen la última versió i

que disposen dels pedaços de seguretat instal·lats. Aquesta tècnica s'acostuma a utilitzar en organitzacions amb molts usuaris que han d'utilitzar diferents aplicacions, com per exemple els estudiants d'una universitat.

2.5 Eines per a la virtualització

Actualment existeixen eines per virtualitzar tant de pagament com gratuïtes. És important seleccionar el producte que més s'adeqüi a les nostres necessitats i que sigui compatible amb el programari a utilitzar.

2.5.1 Sistemes propietaris

A continuació es detallen els principals fabricants d'eines de virtualització.

- **VMware**: és la empresa líder del mercat de la virtualització. És la que porta més anys dedicant-se aquesta tecnologia i controla una gran part del mercat. La clau del seu èxit és oferir un bon producte i un excel·lent servei de suport. No obstant això, en els últims anys són moltes les empreses que ofereixen tecnologies similars a un preu més baix o fins i tot gratuïtament. Disposa d'un gran ventall de productes destinats a oferir solucions específiques a cada necessitat. La majoria d'ells són de pagament, tot i que també ofereix alguns productes de forma gratuïta.
  - **Virtualització de centres de processament de dades**: VMware vSphere, Go, vCloud, ESX Server
  - **Virtualització d'escriptoris**: VMware View, ThinApp, ACE, Workstation, Zimbra, MVP (Mobile Virtualization Platform) i Horizon
  - **Virtualització d'aplicacions**: família de productes VMware vFabric
  - **Productes de seguretat**: família de productes VMware vShield
  - **Sistemes de gestió**: família de productes VMware vCenter (gestió d'aplicacions, infraestructures i operacions)
  - **Productes per a MAC**: VMware Fusion
  - **Productes gratuïts**:VMware vSphere Hypervisor, Server, Player i ESXi
- **Microsoft**: empresa líder en el terreny dels sistemes operatius, va entrar en el món de la virtualització més tard, però ho ha fet amb empenta i s'ha guanyat un lloc en el mercat. A diferència de Vmware, Microsoft ha orientat els seus productes a les petites i mitjanes empreses, i es calcula que l'any 2012 Microsoft controlava al voltant del 85% del mercat de la virtualització en aquest sector. A més, Microsoft disposa d'un sistema operatiu propi i pot oferir una solució completa. Per acabar, el seu sistema operatiu Windows 8 inclou per defecte l'Hyper-V. A continuació s'enumeren els principals productes de virtualització de Microsoft.

  - **Virtualització de servidors**: Hyper-V a Windows Server 2008 R2
  - **Virtualització per a la creació de núvols privats**: Microsoft Dynamic Data Center Toolkit i Windows Azure
  - **Virtualització d'aplicacions**: Microsoft Application Virtualization
  - **Virtualització d'escriptoris**: Microsoft Enterprise Desktop Virtualization i Microsoft Virtual Desktop Virtualization

- **Citrix**: empresa multinacional fundada l'any 1989, subministra programari de virtualització de servidors, escriptoris, aplicacions i xarxa. Des del juny de 2009, el seu producte de virtualització de servidors anomenat XenServer pot ser descarregat de forma gratuïta des del seu web.

  - **Virtualització de servidors**: XenServer
  - **Virtualització d'escriptoris remots**: XenDesktop, XenClient, VDI-in-a-Box i XenReceiver.
  - **Virtualització d'aplicacions**: XenApp
  - **Gestió de les màquines virtuals**: NetScaler

2.5.2 Sistemes lliures

De mica en mica, han anat sorgint solucions de virtualització de distribució lliure. Algunes d'aquestes versions gratuïtes són més limitades que les seves versions de pagament, no obstant això, n'hi ha molta varietat i s'hi troben eines força completes, especialment les dissenyades per ser utilitzades en entorns Linux.

Sovint, les grans empreses opten per solucions empresarials, ja que ofereixen un millor suport, és més fàcil trobar-ne documentació i estan més esteses. Les eines de virtualització lliures es destinen majoritàriament a entorns de proves o a l'aprenentatge.

Gràcies a l'aparició d'aquestes eines de virtualització gratuïtes, s'ha pogut apropar la virtualització a tots tipus d'usuaris.

- **VMware**: és la empresa líder en el mercat, i tot i que les seves solucions acostumen a ser de pagament, ha llançat al mercat alguns productes de distribució lliure:

  - **VMware Server**:és una eina dissenyada per ser utilitzada tant a Windows com a Linux. És fàcil d'utilitzar i serveix perquè les empreses s'iniciïn en el món de la virtualització de servidors, optimitzant la utilització dels seus dispositius. Tot i que encara s'utilitza, a finals de 2011 VMware va anunciar que deixava de donar suport tècnic a aquest producte i que llançava altres eines de virtualització més específiques.
  - **VMware vSphere**: evolució del VMware Server, és un producte fàcil d'utilitzar, pensat perquè les empreses s'iniciïn en la virtualització de servidors de manera gratuïta en pocs minuts. Pot executar fins a 100 màquines virtuals i centralitzar-ne la gestió.

  - **VMware Player**: es tracta d'un petit programari de virtualització que permet reproduir màquines virtuals ja creades. És una manera ben senzilla d'entrar en el món de la virtualització a nivell d'usuari.
  - **VirtualBox**: eina de virtualització amb llicència GNU/GPL d'Oracle per a professionals i per a ús domèstic que permet disposar de més d'un sistema operatiu en un mateix ordinador. Ara mateix existeixen versions de VirtualBox per als principals sistemes operatius (Windows, Linux, Mac i Solaris) i s'hi poden virtualitzar un gran nombre de sistemes operatius: Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, DOS/Windows 3.x, Linux (2.4 i 2.6), Solaris, OpenSolaris, OS/2 i OpenBSD.

- **Virtual PC**: programa gestor de virtualització desenvolupat per Connectix i posteriorment adquirit per Windows. És una eina similar a VirtualBox amb la qual els usuaris poden disposar de més d'un sistema operatiu en un ordinador. Pot ser instal·lat en la majoria de versions del sistema operatiu Windows (7, Vista, XP, Server 2003, Server 2008) i pot allotjar els sistemes operatius següents: Server 2003 i 2008, NT, Vista, XP, 2000, OS/2, Me, MS-DOS, 98 6.22, 3.1, 3.11, 2.03, 1.01.

- **QEMU**: és un emulador d'arquitectures basades en x86 amb dos modes de funcionament: emulació del sistema complet i emulació en mode usuari.

  - **Mode complet**: emula un equip sencer, incloent-hi múltiples processadors i perifèrics. Aquest mode s'utilitza per executar sistemes operatius complets. En les últimes versions, el programa accepta fins a 15 arquitectures diferents.
  - **Mode usuari**: el programa pot executar aplicacions compilades per a un processador concret en un sistema que funciona sobre un processador diferent. Pot servir per solucionar problemes d'incompatibilitat entre arquitectures de 32 i 64 bits.

- **KVM (Kernel Virtual Machine)**: solució de virtualització completa en què s'utilitza el nucli de Linux com a hipervisor, de manera que tant el control dels dispositius com la planificació de les tasques i la gestió de la memòria del sistema les realitza el nucli, en anglès *kernel*. En aquest model, les màquines virtuals no deixen de ser un simple procés en el sistema.

- **Linux-Vserver**: sistema de virtualització a nivell de sistema operatiu que s'implementa com una sèrie de modificacions del nucli de Linux. Proporciona les eines necessàries per crear múltiples entorns d'usuari independents entre ells. Com que aquesta tecnologia no està lligada a cap arquitectura concreta, pot executar-se en microprocessadors (x86, x86-64, PowerPC, ARM...).

- **Xen**: solució de paravirtualització i que, per tant, compta amb un hipervisor que s'executa en el nivell més privilegiat de la màquina i que s'encarrega bàsicament de la planificació de tasques i de la gestió de la memòria. Tot i que sovint s'utilitza en entorns Linux, Xen no és un sistema de virtualització lligat al nucli de Linux, sinó que també pot ser utilitzat en versions modificades de NetBSD, Solaris, FreeBSD i Plan9.

2.5.3 Maquinari específic per virtualitzar

Es poden implementar solucions de vitualització en qualsevol servidor. Ara bé, això no vol dir que tots siguin iguals pel que fa a la virtualització; els seus rendiments poden variar considerablement. Per treure el millor partit a aquesta tecnologia, alguns proveïdors de components de maquinari ofereixen solucions orientades a la virtualització. Els dos proveïdors que més han despuntat en aquest camp són Hewlett-Packard i Dell.

- **Hewlett-Packard**: la gama de servidors ProLiant ofereix un gran ventall de solucions de virtualització amb diversos proveïdors: VMware, Citrix, Microsoft, Linux i Solaris. Amb VMware porten més de 10 anys treballant conjuntament. Són considerats líders en aquest sector gràcies a la gran integració entre els dos productes, que ofereix un excel·lent rendiment i un ús eficient de l'emmagatzematge, i evita problemes d'escalabilitat. Entre d'altres, ofereixen solucions per a la virtualització de servidors, escriptoris i fins i tot solucions en núvol.
- **Dell**: ha dissenyat la família de servidors PowerEdge per obtenir el millor rendiment possible en virtualització. Ha optimitzat alguns dels seus productes per tal d'adaptar-los a les necessitats de virtualització: densitat, flexibilitat i rendiment. Dell ha implementat solucions VMware des del primer hipervisor, que es va comercialitzar l'any 2001. No obstant això, en els últims anys han signat acords amb fabricants com Citrix i Microsoft per tal d'oferir un ventall més ampli de possibilitats en el món de la virtualització.

Significat de la nomenclatura de Dell

Dell utilitza per a la gamma PowerEdge una nomenclatura pròpia basada en una lletra i tres dígits. La lletra indica el tipus de servidor: (R) bastidor o *rack*, (M) modular, (T) torre. El primer dígit indica el nombre de sòcols del sistema: del 1 al 3 per a un sòcol, del 4 al 7 per a dos sòcols, 9 per a quatre sòcols i 8 per a dos o quatre sòcols, dependrà del processador. El segon dígit fa referència a la generació: 0 per a la generació 10, 1 per a la generació 11… El tercer dígit indica el fabricant del processador: 0 per a Intel i 5 per a AMD.

2.6 Configuració i utilització de les màquines virtuals

En els últims anys moltes empreses han optat per implantar solucions de virtualització en els seus servidors. Però implantar una solució d'aquest tipus no és una tasca fàcil, ja que els administradors han de disposar de coneixements sobre el tema, cosa que no sempre passa.

Primer cal establir uns objectius clars sobre quina és la finalitat d'aplicar aquesta tecnologia. Un cop es tingui clar l'objectiu, caldrà analitzar tots els productes que hi ha al mercat, tant de pagament com de programari lliure, per veure quin dóna millors resultats. No s'usa el mateix el programari per virtualitzar un servidor que per virtualitzar escriptoris.

Un cop s'ha escollit el tipus de virtualització i el producte que s'implantarà, cal comprovar que el nostre maquinari compleix els requeriments tècnics. Abans d'instal·lar el programa en el servidor de producció, cal fer un simulacre en un entorn de proves per poder valorar el seu funcionament. Si les proves realitzades

són satisfactòries, es pot procedir a la instal·lació del programa en els sistemes productius, prenent totes les mesures de precaució necessàries.

2.7 Migració en calent

Un dels grans avantatges de la virtualització és la gran flexibilitat que ofereix tant per la creació, eliminació i modificació dels recursos de les màquines virtuals com per al canvi de màquina física.

La **migració en calent** (en anglès, *live migration*) consisteix a poder traslladar una màquina virtual des d'una màquina física a una altra sense que l'usuari se n'adoni. S'anomena *migració en calent* ja que mentre s'està movent d'un lloc a un altre la màquina virtual continua estant operativa.

Els principals fabricants (VMware, Microsoft i Citrix) ja disposen de solucions que permeten aquest tipus de migracions.

La migració en calent pot canviar una màquina virtual d'un servidor físic a un altre de manera que el temps d'inactivitat sigui de mil·lisegons. No obstant això, no és una tasca fàcil, ja que s'ha de traslladar el contingut de la memòria, del disc dur, l'estat del processador i les connexions de xarxa. A continuació es detalla cadascun d'aquests aspectes:

- **Migració de la memòria**: es tracta d'un procés complicat, ja que mentre es transfereix aquesta informació del node origen al de destinació, la màquina continua fent modificacions. Aquest traspàs d'informació es pot realitzar de moltes maneres diferents, però sempre s'ha de prioritzar la que permeti minimitzar el temps d'inactivitat i el temps total de la migració.
- **Migració del disc dur**: és força similar al procés de migració de la memòria, tot i que en aquest cas el volum de dades que s'han de transmetre és major i per tant el temps de migració és superior. Per solucionar aquest problema, els fabricants utilitzen sistemes d'emmagatzematge centralitzat com per exemple SAN, NFS o iSCSI. D'aquesta manera, tots els servidors físics estan connectats a un mateix sistema d'emmagatzematge i quan una màquina virtual es mogui de servidor no serà necessària la migració del disc dur i es reduirà així considerablement el temps d'inactivitat.
- **Migració de connexions de xarxa**: per facilitar la migració de connexions de xarxa cal que tots els servidors formin part de la mateixa subxarxa. D'aquesta manera les adreces IP que utilitzin estaran dins del mateix rang. Quan una màquina virtual vulgui canviar de servidor físic, només haurà d'enviar un missatge ARP a l'adreça de difusió indicant l'adreça MAC de la nova targeta de xarxa. Com que aquest canvi només afecta a nivell físic, les connexions que la màquina virtual tenia establertes no es veuran afectades, ja que la seva adreça IP continuarà sent la mateixa.

- **Migració del processador**: en canviar de processador és quan realment es produeix la migració. Per aquest motiu ha de ser l'últim recurs que canviem de lloc. Primer passarem les dades, tant les del disc dur com les de la memòria, després les connexions i per acabar el processador, juntament amb alguna dada que hagi estat modificada amb posterioritat a la seva còpia. Cal tenir present el tipus de processadors dels servidors, ja que poden haver-hi incompatibilitats entre processadors de diferents fabricants.

La migració en calent permet millorar la gestió de rendiment de les màquines, ja que és una eina molt potent per als administradors de clústers. Permet separar el programari del maquinari on es troba allotjat i gestionar un clúster de servidors com si es tractés d'un domini.

La virtualització en calent ofereix molts avantatges. Entre d'altres, redueix el temps d'inactivitat en cas de fallada del maquinari, permet fer un repartiment de càrrega de màquines virtuals, afavoreix l'escalabilitat de les aplicacions i serveis i permet fer un ús més eficient del sistemes.

Aquests són alguns dels productes que permeten la migració en calent: VMware ESX, Hyper-V Windows Server 2008 R2, Xen, KVM i OpenVZ.

2.8 Virtualització i alta disponibilitat

La virtualització és una de les tècniques més eficients i més econòmiques per garantir l'alta disponibilitat en els sistemes d'informació. Pel gran nombre d'avantatges que ofereix, i no només en termes d'alta disponibilitat, és una de les solucions més adoptades per les empreses. En els últims anys han estat moltes les companyies que han apostat per aquesta tecnologia i es preveu que en un futur proper encara seran més les que apostaran per la virtualització.

A continuació es detallen els principals avantatges que aporta la virtualització en termes d'alta disponibilitat:

- **Alta disponibilitat de totes les aplicacions**: la virtualització ofereix una solució d'alta disponibilitat completa, ja que protegeix la continuïtat de negoci tant a nivell físic com a nivell lògic.
- **Repartiment de càrrega**: permet gestionar de manera eficient la càrrega dels servidors físics i evitar que es puguin saturar i entrar en fallada. Fa un ús eficient de les màquines físiques i aconsegueix un procés d'optimització continua.
- **Recuperació en cas de desastre**: simplifica i automatitza els fluxos de recuperació en cas de desastre (prevenció, actuació i recuperació). Converteix algunes instruccions manuals de recuperació en processos automatitzats. Fins i tot permet centralitzar la gestió del pla en cas de desastre des d'una plataforma de gestió.

- **Protecció i gestió dels escriptoris corporatius**: la virtualització d'escriptoris permet poder oferir als usuaris finals solucions d'alta disponibilitat. En cas de fallada del terminal d'accés, l'usuari podrà iniciar sessió en pocs segons des de qualsevol altre dispositiu connectat a la xarxa.

- **Flexibilitat i escalabilitat**: depenent de la demanda d'un servei, les màquines es podran readaptar per fer front a les diferents necessitats. La flexibilitat és molt més alta que en els models convencionals. S'aconsegueix que les màquines s'adaptin a la demanda real i s'evita així que hi pugui haver una sobresaturació i, per tant, una caiguda del sistema.

2.9 Informàtica en núvol

En els últims anys ha sorgit una nou concepte anomenat *informàtica en núvol* (en anglès, *cloud computing*), que permet a les empreses disposar de serveis o aplicacions d'alta disponibilitat sense necessitat de desplegar cap tipus d'infraestructura addicional. Aquesta solució ràpidament va ser adoptada per empreses de nova creació o amb pressupostos ajustats. I els seus bons resultats han fet que cada cop siguin més les companyies que estan adoptant solucions d'aquest tipus.

La informàtica en núvol és un sistema d'emmagatzematge i ús de recursos informàtics basat en el servei en xarxa, que consisteix a oferir a l'usuari un espai virtual, generalment a Internet, en què pot disposar de les versions més actualitzades de maquinari i programari.

Google Apps al Departament d'Ensenyament

L'any 2010 el Departament d'Ensenyament de Catalunya va fer la migració del seu correu intern XTEC a Google Apps, el servei de correu electrònic ofert per Google a les empreses. D'aquesta manera, els usuaris poden accedir al correu des de qualsevol dispositiu com si es tractés d'un compte de Gmail.

EyeOS

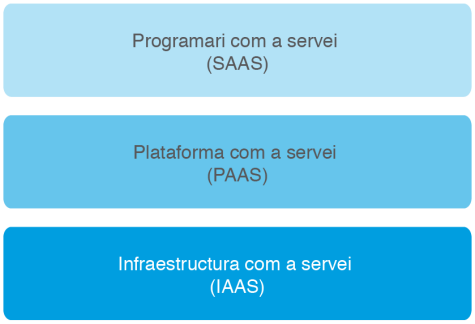
L'any 2006, un grup de joves programadors catalans van llançar al mercat el primer escriptori virtual en núvol. La idea va ser tot un èxit i en pocs mesos van tenir una gran acceptació arreu del món. L'objectiu era que els usuaris accedeixin a les seves aplicacions com si es tractés d'un sistema operatiu des de qualsevol lloc del món. Per defecte, eyeOS porta un gran nombre d'aplicacions, però a més se n'hi poden incloure d'altres i, si s'és programador, programar-ne de noves.

És un nou model de negoci que permet als usuaris accedir a un catàleg de serveis adaptables i flexibles a les necessitats de les empreses. Els usuaris paguen als proveïdors d'aquests serveis per l'ús que en fan. Aquests serveis es poden adaptar totalment a les demandes de negoci i se'n pot sol·licitar un augment o disminució si es produeix un pic o una davallada de feina. D'aquesta manera, les empreses disposen de serveis totalment flexibles sense haver-se de preocupar del maquinari, el manteniment o les actualitzacions.

Les empreses que ofereixen aquest tipus de serveis disposen d'una infraestructura basada en l'alta disponibilitat. La seva línia de negoci es basa en oferir serveis a uns clients distribuïts arreu del món i no es poden permetre una caiguda dels seus sistemes, per petita que sigui. Per evitar aquests temps d'inactivitat tenen implantats sistemes per garantir l'alta disponibilitat com la redundància en la xarxa, les xarxes d'emmagatzematge, la redundància de servidors, la redundància en el subministrament elèctric, els plans de contingència i la virtualització.

El concepte d'informàtica en núvol és molt ampli i engloba diferents models de negoci. Aquests es poden classificar de la manera següent (figura 2.4):

FIGURA 2.4. Tipus d'informàtica en núvol



- **Programari com a servei (SAAS)**: en anglès, *software as a service*. Es caracteritza per oferir com a servei una aplicació completa a la carta. Els usuaris es connecten a través d'una xarxa, habitualment Internet, al servidor del proveïdor. En aquest model de negoci no es paguen llicències de programari sinó que es paga per ús que se'n fa. Les aplicacions estan situades en una infraestructura pública. El proveïdor líder en solucions de programari com a servei és Salesforce, amb el seu CRM *customer relationship management* distribuït. No obstant això, en els últims anys han sorgit noves empreses que ofereixen aquest tipus de servei com Google Apps, Dropbox, Evernote, Basecamp o Workday.

- **Plataforma com a servei (PAAS)**: en anglès, *platform as a service*. És una solució intermèdia en què no només s'ofereix el maquinari, sinó que també contempla els elements bàsics per poder instal·lar una aplicació com són el sistema operatiu, els sistemes gestors de bases de dades i servidors d'aplicacions. Això permetrà al client instal·lar les seves pròpies aplicacions i despreocupar-se del manteniment del maquinari i del programari base. Un dels principals proveïdors de servei és Google App Engine, entre d'altres com Microsoft Azure o Force.

- **Infraestructura com a servei (IAAS)**: en anglès, *infrastructure as a service*. En aquesta capa s'ofereix com a servei la capacitat de procés i d'emmagatzematge, normalment mitjançant un plataforma de virtualització. En comptes d'adquirir servidors i habilitar centres de processament de dades, les empreses lloguen aquests recursos a un proveïdor extern. El principal proveïdor en el mercat és Amazon, amb Amazon EC2, tot i que de mica en mica van sorgint altres empreses com GoGrid o l'empresa catalana Abiquo.

Microsoft Office 365

Microsoft no ha volgut perdre el seu lideratge en paquets ofimàtics i l'any 2011 va llançar al mercat un nou producte d'informàtica en núvol, anomenat Microsoft Office 365. Aquest producte disposa de les eines ofimàtiques Excel, Word, PowerPoint, Outlook, Exchange, Sharepoint i un sistema de conferències de vídeo i àudio. Els usuaris no han d'instal·lar cap d'aquestes aplicacions, sinó que hi accedeixen per Internet i paguen una quota mensual.

Els objectius principals d'aquesta tecnologia són augmentar la flexibilitat, millorar l'accessibilitat, reduir els costos i millorar l'alta disponibilitat:

- **Alta disponibilitat**: permet a les empreses disposar de solucions d'alta disponibilitat a un preu reduït, molt per sota del que haurien d'invertir si implantessin solucions pròpies.

- **Reducció de costos**: com que l'empresa no disposa de servidors propis, no ha de realitzar la inversió inicial de tota aquesta infraestructura, que té un cost molt elevat i que, sovint, en petites i mitjanes empreses es troba infrautilitzada. A més, en no disposar de servidors propis, l'empresa no ha de destinar recursos al seu manteniment. Únicament cal adquirir uns terminals per accedir aquests serveis sense grans requisits tècnics, ja que el procés es realitza en el servidor.
- **Accessibilitat**: el fet d'utilitzar aquest tipus de solucions permet més flexibilitat en els usuaris, ja que poden accedir als recursos des de diferents tipus de dispositius, sistemes operatius i situació geogràfica.
- **Flexibilitat**: permet adaptar ràpidament els sistemes de l'empresa a les necessitats de negoci. Davant d'un creixement molt ràpid es pot donar resposta en qüestió d'hores quan en un sistema convencional es requeririen mesos de planificació i uns costos molt més elevats.

No obstant això, com qualsevol sistema que està en fase d'implantació també genera algunes incerteses en els usuaris, com, per exemple, el control del nivell de servei acordat, la dependència que genera amb el proveïdor de servei i la ubicació i seguretat de les dades.

- **Nivell de servei**: les empreses proveïdores s'han de comprometre a oferir un determinat nivell de servei prèviament acordat amb els usuaris. Sorgeixen dubtes sobre de quina manera s'estableix el nivell de servei a complir per part de les empreses proveïdores i com es pot verificar i controlar que s'estigui treballant dins dels nivells acordats.
- **Dependència**: implantar una solució d'aquest tipus genera una gran dependència amb el proveïdor de servei. Òbviament el grau de dependència dependrà del tipus d'informàtica en núvol que s'estigui aplicant, sent les solucions de programari com a servei, les PAAS, les més dependents. Sovint, en utilitzar solucions d'aquest tipus les empreses han d'adaptar la seva manera de treballar als productes oferts.
- **Ubicació de la informació**: una de les principals pors que tenen les empreses a l'hora d'implantar solucions d'aquest tipus és el fet que les dades no es trobin allotjades en la mateixa empresa, sinó que sigui una empresa externa la que tingui aquesta informació i la gestioni. Això genera als administradors incerteses sobre l'ús, la gestió i el compliment de la normativa associada a les dades.

Algunes de les solucions d'informàtica en núvol que més utilitzen les empreses són:

- **Google Apps**: és un servei de Google que ofereix a les empreses versions personalitzades dels seus propis productes: Gmail, Google Groups, Google Calendar, Google Talk, Google Docs i Google Sites. Alguns dels seus principals avantatges:

  - **Estalvi de costos**: les solucions de Google Apps permeten reduir costos de gestió i manteniment a les empreses. Es calcula que es poden reduir a una tercera part del que suposaria la implantació d'un servidor de correu propi. A goo.gl/HCOqv es detallen els càlculs de l'estalvi que suposaria una solució d'aquest tipus.
  - **Espai d'emmagatzematge superior**: la capacitat d'emmagatzematge de les bústies de correu és de 25 GB, molt superior als sistemes convencionals.
  - **Accés a través del mòbil**: permet accedir a l'aplicatiu des de dispositius mòbils Blackberry, iPhone, Windows Mobile i Android.
  - **Alta disponibilitat**: Google garanteix una disponibilitat dels seus serveis del 99,9% i utilitza la replicació síncrona de les dades entre diferents centres de dades.
  - **Control total i administratiu de les dades**: els administradors poden personalitzar totalment Google Apps per cobrir les necessitats que puguin tenir en relació a l'aparença, aspectes tècnics i empresarials.
  - **Assistència 24/7**: tot i ser molt intuïtiu i fàcil d'utilitzar ofereix assistència als administradors tots els dies de l'any les vint-i-quatre hores del dia.
  - **Compliment de la normativa i seguretat de la informació**: s'implanten les mateixes mesures de seguretat que en els serveis de Google i es garanteix la confidencialitat de les dades.

- **Dropbox**: sistema d'allotjament de fitxers multiplataforma. El servei permet emmagatzemar i sincronitzar fitxers en línia per ser consultats des de diferents dispositius. A més, també permet la compartició de fitxers entre diferents usuaris. Dropbox permet crear comptes gratuïts amb una capacitat de fins a 2 GB i de pagament fins a 1 TB per a grups de treball.

- **Evernote**: eina informàtica multiplataforma per a la gestió d'informació personal a base de notes. És una eina ideal per a executius, ja que permet centralitzar i gestionar de manera eficient informació rellevant com notes, imatges, idees... Disposa de versió gratuïta i de versió de pagament amb un capacitat d'emmagatzematge més alta.

- **Salesforce**: ofereix solucions de CRM per a la gestió dels clients, gestió d'oportunitats i campanyes de màrqueting, entre d'altres. A més, les seves funcionalitats es poden ampliar amb més de 1.000 aplicacions addicionals.

- **Endeve**: sistema de facturació en línia que permet a les empreses portar la gestió de la comptabilitat de l'empresa de manera eficient i centralitzada. Permet crear factures des de qualsevol lloc i dispositiu.

- **Google Drive**: paquet ofimàtic per treballar des de qualsevol dispositiu en l'elaboració de documents de text, fulls de càlcul, presentacions i dibuixos. Permet l'emmagatzematge i la compartició de documents entre diferents usuaris.

2.10 Contenidors

Una alternativa a la virtualització és l'ús de contenidors. Aquests permeten configurar els entorns de desplegament de manera que poden reproduir-se de forma idèntica en qualsevol màquina, independentment del sistema operatiu i la configuració de l'amfitrió.

Tot i que la utilització de **contenidors i màquines virtuals** pot semblar molt similar, no es tracta del mateix concepte.

- Els **contenidors** són molt més lleugers i pràcticament no afecten el rendiment de l'aplicació. El motiu és que utilitzen el mateix nucli del sistema operatiu. A més a més, l'espai que ocupa en disc és molt reduït, ja que només s'hi han d'afegir els fitxers específics que requereix l'aplicació que s'executa en el contenidor.
- Les **màquines virtuals** són instal·lacions completes del sistema operatiu i afegeixen capes extres a l'execució dels programes, ja que cada instrucció ha de passar pel sistema operatiu virtualitzat, el programari de virtualització, el maquinari de virtualització de l'equip hoste i el nucli del sistema operatiu hoste. Això té un cost significatiu en el rendiment. La preparació de la màquina virtual també és més costosa, en haver-se de fer una instal·lació completa i, també, requreix més espai al disc. Un avantatge de la virtualització és que es poden fer servir màquines virtuals amb diferents sistemes operatius independentment de quin estigui instal·lat a la màquina hoste (per exemple, una màquina virtual amb Linux pot executar-se en una màquina hoste amb Windows).

Informació addicional sobre contenidors

Podeu trobar-ne més informació a l'enllaç següent: goo.gl/N44YOg.

En el cas de sistemes distribuïts (una aplicació desplegada a múltiples màquines), és molt útil utilitzar contenidors, ja que només cal preparar el contenidor una vegada i instal·lar-lo en tants servidors com sigui necessari. Aquest és un dels motius pels quals Google fa servir contenidors per desplegar les seves aplicacions en lloc d'haver de configurar milers d'equips individualment. Un inconvenient, però, d'aquesta tecnologia és que no poden fer-se servir contenidors que utilitzen un sistema operatiu en una màquina amb un sistema operatiu diferent (per exemple, no es pot utilitzar un contenidor de Linux en una màquina amb Windows).

Contenidors en entorns virtualitzats

En cas d'haver de treballar amb contenidors en ordinadors amb un sistema operatiu diferent del del contenidor, es pot recórrer a la utilització de màquines virtuals. Cal tenir en compte que es perd part de l'eficiència proporcionada per aquesta tecnologia, però és habitual treballar d'aquesta manera en entorns de desenvolupament, ja que l'equip de programadors pot treballar amb el sistema operatiu que s'adapti més bé a les seves necessitats. A més a més, en aquests casos, la pèrdua de rendiment no és crítica.

Docker és un sistema de contenidors amb llicència de programari lliure.

Tot i que aquesta tecnologia dels contenidors es troba disponible des dels anys 80 al sistema operatiu UNIX, fins a l'aparició de Docker, l'any 2013, no era

gaire popular. Actualment és fàcil trobar proveïdors de serveis d'allotjament que admeten Docker i permeten fer el desplegament de les aplicacions automàticament (per exemple, Amazon Web Services i Google Cloud).

2.10.1 Linux Containers

Linux Containers és el nom del projecte darrere les tecnologies LXC, LXD i LXCFS que té com a objectiu proporcionar un entorn neutral per al desenvolupament de les tecnologies de contenidors a Linux.

- **LXC** és un conjunt d'eines per a la creació de contenidors sobre Linux.
- **LXD** proporciona una nova interfície per treballar amb LXC mitjançant una única eina de línia d'ordres i una forma de treballar més similar a la que s'utilitza habitualment amb màquines virtuals.
- **LXCFS** és un sistema de fitxer per noms d'usuari (FUSE, en anglès) que soluciona alguns problemes amb què es troben els usuaris que fan servir un sistema de contenidors.

Quan es treballa amb aquestes tecnologies es recomana utilitzar la distribució de Linux Ubuntu, ja que inclou totes les dependències necessàries, i Cannonical Ltd inclou suport a llarg termini (LTS o *long term support*, en anglès) per a LXC a les seves pròpies distribucions de tipus *LTS*.

OpenStack

OpenStack és un sistema operatiu per a núvols que permet controlar una gran quantitat de recursos mitjançant un centre de dades. Se'n pot trobar més informació a l'enllaç següent: goo.gl/SZWz5s.

El component LXC és la base del sistema de contenidors i el seu objectiu és crear un entorn el més proper possible a una instal·lació estàndard de Linux, però fent servir el mateix nucli del sistema operatiu de la màquina on s'executa.

Per altra banda, el component LXD fa servir la implementació de LXC internament, però afegeix un sistema de càrrega d'imatges per crear els contenidors. Els contenidors es gestionen de manera similar a com es faria si fossin màquines virtuals i permet realitzar aquestes operacions a través de la xarxa.

Un altre avantatge de fer servir LXD és que pot utilitzar-se conjuntament amb OpenStack (mitjançant el connector nova-lxd), de manera que es pot treballar al núvol tant amb contenidors com amb màquines virtuals de forma transparent de cara als usuaris. Això obre la porta a fer servir sistemes més avançats que incloguin servidors de càrrega i la creació automatitzada d'instàncies, per exemple, per augmentar el nombre de contenidors que serveixen una determinada aplicació segons el nombre d'usuaris connectats al sistema.

2.10.2 Contenidors: Docker

Docker és un sistema de contenidors basat en el nucli de Linux. Es tracta de programari lliure i entre els principals col·laboradors hi ha empreses com Google, IBM, Cisco, Microsoft i Red Hat.

Anteriorment, per utilitzar Docker en sistemes operatius no basats en Linux, s'utilitzava Docker Toolbox. Aquesta eina, però, es troba obsoleta i no s'ha d'utilitzar amb els sistemes operatius actuals.

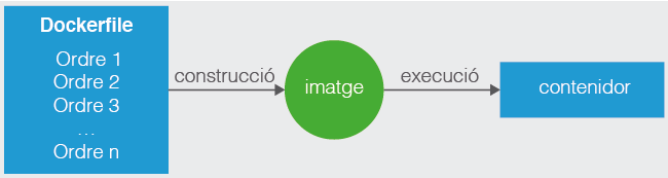
Com que es tracta d'un contenidor basat en Linux, no pot utilitzar-se directament a màquines amb altres sistemes operatius, però és possible utilitzar-lo en altres entorns de desenvolupament mitjançant la virtualització. Al seu web hi ha enllaços a instal·ladors que simplifiquen aquesta tasca i inclouen tots els fitxers necessaris per instal·lar Docker a Linux, Mac i Windows.

Alguns avantatges de desplegar una aplicació utilitzant Docker són els següents:

- L'aplicació funciona igual en el servidor de proves que en el de producció perquè l'entorn és el mateix.
- Cada aplicació es troba aïllada de la resta d'aplicacions, en el seu propi contenidor.
- No cal instal·lar cap altre component, a banda de Docker, per executar l'aplicació en un altre equip. L'aplicació funciona directament en instal·lar el contenidor, perquè totes les dependències es troben al contenidor.

Els contenidors de Docker són instàncies d'una imatge que conté tots els fitxers necessaris empaquetats per crear el contenidor en un sol fitxer. Al seu torn, aquesta imatge és construïda a partir d'un fitxer anomenat Dockerfile, que conté totes les ordres necessàries per assemblar-la (vegeu la figura 2.5).

Figura 2.5. Procés d'execució d'un contenidor



El primer pas per treballar amb contenidors de Docker és instal·lar-lo fent servir l'enllaç següent: goo.gl/n7d5qg. En aquesta pàgina es pot trobar l'instal·lador per utilitzar Docker amb Mac, Windows i diferents distribucions de Linux. La instal·lació és molt simple en tots els sistemes operatius, però en cas de dubte recordeu que podeu trobar tota la informació necessària a la mateixa pàgina de descàrrega.

Una vegada instal·lat, cal executar-lo. En la majoria de sistemes operatius, es necessiten permisos d'administrador per poder gestionar la xarxa. Per comprovar que s'ha instal·lat amb èxit, obriu una finestra amb la terminal o el símbol del sistema (segons quin sistema operatiu feu servir) i escriviu-hi *docker -v*.

El resultat ha de ser similar al següent:

```
~ $ docker -v
Docker version 17.03.1-ce, build c6d412e
```

2.10.3 Creació i desplegament d'un contenidor amb Docker

Per veure el funcionament d'un contenidor, cal crear-ne un per executar una aplicació en PHP que mostri per pantalla el missatge: "Hola món!". Primer, creeu un directori anomenat *prova-docker*, on es desaran tots els fitxers d'aquest projecte. Dintre d'aquest directori, creeu-ne un altre anomenat *src* amb un fitxer de text pla anomenat index.php i el contingut següent:

```
<?php

echo "Hola món!";
```

Repositori d'imatges per Docker

Podeu trobar imatges de Docker fiables per utilitzar com a base a l'enllaç següent: hub.docker.com. En aquest repositori hi ha tant imatges oficials (més fiables) com públiques.

Per poder executar aquesta aplicació és necessari un sistema operatiu, un servidor web (per exemple, Apache) i PHP. Per indicar a Docker que ha d'incloure la imatge, creeu un fitxer de text pla dins del directori *prova-docker* anomenat Dockerfile.

Docker requereix el nom d'una imatge per fer-la servir com a base. Aquestes imatges inclouen els fitxers propis de la distribució (per exemple, Ubuntu o Debian) i en alguns casos algunes aplicacions preinstal·lades com PHP o MySql.

L'enllaç a la imatge de Docker oficial per a PHP es troba a l'enllaç següent: hub.docker.com/_/php/. Al principi de la pàgina hi ha la llista d'imatges disponibles (vegeu la figura 2.6).

FIGURA 2.6. Imatge de Docker oficial PHP

Supported tags and respective `Dockerfile` links

- `7.1.3-cli`, `7.1-cli`, `7-cli`, `cli`, `7.1.3`, `7.1`, `7`, `latest` (*7.1/Dockerfile*)
- `7.1.3-alpine`, `7.1-alpine`, `7-alpine`, `alpine` (*7.1/alpine/Dockerfile*)
- `7.1.3-apache`, `7.1-apache`, `7-apache`, `apache` (*7.1/apache/Dockerfile*)
- `7.1.3-fpm`, `7.1-fpm`, `7-fpm`, `fpm` (*7.1/fpm/Dockerfile*)
- `7.1.3-fpm-alpine`, `7.1-fpm-alpine`, `7-fpm-alpine`, `fpm-alpine` (*7.1/fpm/alpine/Dockerfile*)
- `7.1.3-zts`, `7.1-zts`, `7-zts`, `zts` (*7.1/zts/Dockerfile*)
- `7.1.3-zts-alpine`, `7.1-zts-alpine`, `7-zts-alpine`, `zts-alpine` (*7.1/zts/alpine/Dockerfile*)
- `7.0.17-cli`, `7.0-cli`, `7.0.17`, `7.0` (*7.0/Dockerfile*)
- `7.0.17-alpine`, `7.0-alpine` (*7.0/alpine/Dockerfile*)
- `7.0.17-apache`, `7.0-apache` (*7.0/apache/Dockerfile*)
- `7.0.17-fpm`, `7.0-fpm` (*7.0/fpm/Dockerfile*)
- `7.0.17-fpm-alpine`, `7.0-fpm-alpine` (*7.0/fpm/alpine/Dockerfile*)
- `7.0.17-zts`, `7.0-zts` (*7.0/zts/Dockerfile*)
- `7.0.17-zts-alpine`, `7.0-zts-alpine` (*7.0/zts/alpine/Dockerfile*)
- `5.6.30-cli`, `5.6-cli`, `5-cli`, `5.6.30`, `5.6`, `5` (*5.6/Dockerfile*)
- `5.6.30-alpine`, `5.6-alpine`, `5-alpine` (*5.6/alpine/Dockerfile*)
- `5.6.30-apache`, `5.6-apache`, `5-apache` (*5.6/apache/Dockerfile*)
- `5.6.30-fpm`, `5.6-fpm`, `5-fpm` (*5.6/fpm/Dockerfile*)
- `5.6.30-fpm-alpine`, `5.6-fpm-alpine`, `5-fpm-alpine` (*5.6/fpm/alpine/Dockerfile*)
- `5.6.30-zts`, `5.6-zts`, `5-zts` (*5.6/zts/Dockerfile*)
- `5.6.30-zts-alpine`, `5.6-zts-alpine`, `5-zts-alpine` (*5.6/zts/alpine/Dockerfile*)

For detailed information about the published artifacts of each of the above supported tags (image metadata, transfer size, etc), please see the `repos/php` directory in the `docker-library/repo-info` GitHub repo.

Com es pot apreciar, el llistat és força extens. Si voleu més informació sobre cadascuna de les opcions, podeu consultar la mateixa pàgina. En aquest exemple es fa servir el servidor web Apache i, per consegüent, la imatge base correspon a la fila "7.1.3-apache, 7.1-apache, 7-apache, apache".

Fixeu-vos que a cada fila es mostren, d'esquerra a dreta, les opcions disponibles, de la més concreta a la més genèrica. És a dir, si s'especifica `7.1.3-apache` es farà servir la imatge amb la versió 7.1.3 de PHP i Apache, mentre que si s'especifica en el fitxer `7-apache` es farà servir una versió de PHP 7, però no sabreu quina (habitualment la més recent que s'hagi afegit a aquest repositori). En un cas encara més extrem, si només s'especifica `apache`, la versió de PHP podria ser qualsevol (per exemple, PHP 8 o 9).

Per aquests motius es recomana fer servir sempre una versió concreta. En cas contrari, es poden produir incompatibilitats en les aplicacions i, fins i tot, pot passar que a partir d'una mateixa imatge base es generin diferents imatges, ja que la versió pot canviar en qualsevol moment.

Habitualment els números de versió d'un programa indiquen les diferències següents:

- El primer indica el número de la versió, i no acostuma a ser completament compatible amb l'anterior (per exemple, PHP 7.0 no és compatible amb PHP 5.6).
- El segon número s'utilitza quan s'afegeixen noves funcionalitats.
- El tercer número indica correccions.

Així doncs, a l'hora de seleccionar una imatge, normalment només cal indicar els dos primers números de versió. Per exemple, si s'indica `7.1` com a versió, s'inclou la versió més recent amb totes les correccions actualitzades.

Per indicar a Docker la imatge base, es fa amb l'ordre FROM seguida del nom del repositori (php), dos punts (:) i el nom de la imatge (per exemple, `7.1-apache`):

```
1 FROM php:7.1-apache
```

Com que es vol copiar l'aplicació dins del contenidor, cal utilitzar l'ordre COPY indicant la ruta d'origen i la ruta de destí:

```
1 COPY src/ /var/www/html
```

Aquesta és la ruta que utilitza aquesta imatge en concret, que està basada en la distribució de Debian de Linux. Per saber a quina distribució pertany una imatge i tot el que conté, només cal clicar l'enllaç a la dreta de cada fila per accedir al fitxer Dockfile utilitzat per crear-la.

Finalment, cal indicar a Docker que cal exposar el port 80 del contenidor per poder accedir a la pàgina web. Per fer-ho s'utilitza l'ordre `EXPOSE`:

```
EXPOSE 80
```

Així doncs, el contingut del fitxer Dockerfile per crear la imatge ha de ser:

```
FROM php:7.1-apache
COPY src/ /var/www/html
EXPOSE 80
```

Una vegada creat el fitxer Dockerfile i desat dintre de la carpeta *prova-docker*, per generar la imatge heu d'escriure a la línia d'ordres:

```
docker build -t hola-mon .
```

El paràmetre `-t` es fa servir per indicar el nom de la imatge (en aquest cas, "hola-mon") i el punt final indica que es crearà en el mateix directori. Una vegada es premi la tecla retorn, començaran a descarregar-se els fitxers necessaris per crear la imatge.

El resultat ha de ser similar al següent:

```
~/prova-docker $ docker build -t hola-mon .
Sending build context to Docker daemon 3.584 kB
Step 1/3 : FROM php:7.1-apache
7.1-apache: Pulling from library/php
6d827a3ef358: Pull complete
87fe8fbc743a: Pull complete
f6d1a8d304ab: Pull complete
caf3547d9b73: Pull complete
1004db2760ff: Pull complete
66e2d66a547e: Pull complete
bbfaa62c234a: Pull complete
19ce8807f4d1: Pull complete
63f8d35ca798: Pull complete
a5594b4d2a52: Pull complete
42f1cbd038cf: Pull complete
a739656e85cb: Pull complete
97b6a5f245a1: Pull complete
Digest: sha256:c865c723fbe6a41ccc9006c6c3f3c0225ad06f3ab69c752419d6cd8f7ca51e5e
Status: Downloaded newer image for php:7.1-apache
 ---> b177bfebca36
Step 2/3 : COPY src/ /var/www/html
 ---> a021f0647910
Removing intermediate container 4db2b286aeca
Step 3/3 : EXPOSE 80
 ---> Running in f1da636d83b5
 ---> e991d0ca6063
Removing intermediate container f1da636d83b5
Successfully built e991d0ca6063
```

Seguidament, per executar el contenidor, heu d'escriure des de la línia d'ordres:

```
docker run -p 80:80 hola-mon
```

L'opció `run` indica que es vol executar una instància de la imatge "hola-mon". Fixeu-vos que el nom de la imatge ha d'anar al final de l'ordre. L'opció `-p` indica la redirecció de ports (és el primer el port de la màquina hoste i el segon el port del contenidor). És a dir, s'executarà el contenidor "hola-mon" i es podrà accedir al seu port 80 des del port 80 de la màquina hoste.

El resultat d'executar-lo ha de ser similar al següent:

```
AH00558: apache2: Could not reliably determine the server's fully qualified
    domain name, using 172.17.0.2. Set the 'ServerName' directive globally to
    suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified
    domain name, using 172.17.0.2. Set the 'ServerName' directive globally to
    suppress this message
[Sat Apr 08 12:36:18.758692 2017] [mpm_prefork:notice] [pid 1] AH00163: Apache
    /2.4.10 (Debian) PHP/7.1.3 configured -- resuming normal operations
[Sat Apr 08 12:36:18.758735 2017] [core:notice] [pid 1] AH00094: Command line:
    'apache2 -D FOREGROUND'
```

Tot i que es mostren missatges d'advertència d'Apache, l'aplicació ha de funcionar correctament. Per comprovar-ho només heu d'obrir el vostre navegador i introduir com a URL "localhost". Hauria de mostrar-se per pantalla el missatge "Hola món!".

En cas de voler utilitzar un port diferent de la màquina hoste (per exemple, el 8080, per accedir des de l'URL `localhost:8080`), només cal executar la imatge canviant aquest port, tal com es mostra en l'exemple següent:

```
docker run -p 8080:80 hola-mon
```

Si proveu de modificar el fitxer index.php i actualitzeu la pàgina al navegador, veureu que els canvis no s'hi veuen reflectits. Això és d'esperar, perquè l'aplicació s'ha copiat dins del contenidor. Si es vol actualitzar l'aplicació, cal tornar a construir el contenidor.

Hi ha casos en què aquest comportament no és el desitjat (per exemple, durant el desenvolupament). Per solucionar aquest problema, Docker ofereix l'opció de muntar volums que funcionaran com a directoris compartits entre la màquina hoste i el contenidor.

Per muntar un volum, s'ha de fer des de la línia d'ordres utilitzant l'opció `-v` i indicant el nom del directori de la màquina hoste, dos punts (:), i el nom del directori al contenidor.

```
docker run -p 80:80 -v /provar-docker/src/:/var/www/html/ hola-mon
```

Cal destacar que s'ha d'utilitzar la ruta absoluta. No és vàlid fer servir ~ per indicar que es tracta de la carpeta de l'usuari actual a Linux o Unix, ni `..` per indicar que es tracta del directori pare.

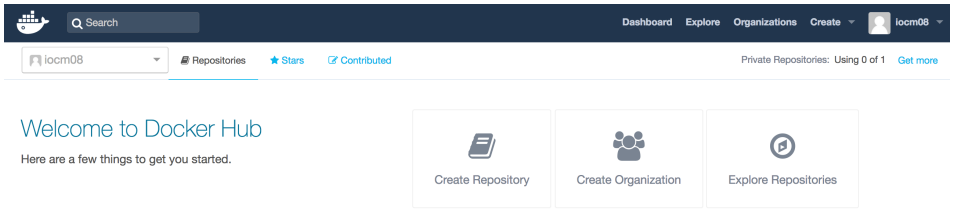
Fixeu-vos que, per muntar un contenidor, s'ha de fer des de la línia d'ordres i no al fitxer Dockerfile: d'aquesta manera s'evita que es trenqui la portabilitat. Com que es tracta de recursos externs al contenidor, Docker no pot assegurar que aquests estiguin disponibles en qualsevol equip.

Si llisteu el contingut del vostre directori, no veureu la imatge creada enlloc. Això és normal: no forma part de la vostra aplicació i no tindria sentit que es mostrés en aquest directori. Per veure un llistat de les imatges instal·lades, s'utilitza l'ordre docker images i el resultat serà similar al següent:

```
REPOSITORY          TAG                 IMAGE ID            CREATED
                SIZE
hola-mon            latest              e991d0ca6063        56 minutes ago
          387 MB
php                 7.1-apache          b177bfebca36        2 weeks ago
             387 MB
```

Per poder desplegar l'aplicació l'heu de pujar al repositori d'imatges de Docker. Per fer-ho, necessiteu crear un compte a Docker Hub (hub.docker.com). Una vegada creat el compte i confirmat mitjançant l'enllaç rebut al correu, podeu connectar amb la pàgina (vegeu la figura 2.7).

FIGURA 2.7. Pàgina principal d'usuari a Docker Hub



Per poder pujar la imatge al repositori, heu d'autenticar-vos amb el nom d'usuari i la contrasenya des de la línia d'ordres, fent servir l'ordre `docker login`. No cal passar cap paràmetre, però us demanarà el nom d'usuari i la contrasenya. El resultat serà similar al següent:

```
~/prova-docker $ docker login
Login with your Docker ID to push and pull images from Docker Hub. If you don't
     have a Docker ID, head over to https://hub.docker.com to create one.
Username: iocm08
Password:
Login Succeeded
```

El següent pas és etiquetar la imatge per pujar-la al repositori. Per fer-ho, cal saber l'identificador (ID) de la imatge i fer servir l'ordre `docker tag` seguida de l'ID, l'espai de noms (que es correspon amb el nom d'usuari de Docker Hub), el nom del repositori, dos punts (:) i l'etiqueta (*tag*, en anglès).

Podeu veure l'identificador de la imatge executant l'ordre docker images, que us mostrarà el llistat d'imatges amb el seu repositori, l'etiqueta, l'identificador, quant fa que es va crear i la mida.

Per exemple, per poder pujar el contenidor amb identificador "0991d0ca6063" al repositori "iocmo8/hola-mon", cal executar l'ordre següent:

```
docker tag e991d0ca6063 iocm08/hola-mon:latest
```

En executar docker images, el resultat serà similar al següent:

```
~/prova-docker $ docker images
REPOSITORY            TAG                 IMAGE ID            CREATED
                SIZE
hola-mon              latest              e991d0ca6063        2 hours ago
             387 MB
iocm08/hola-mon       latest              e991d0ca6063        2 hours ago
             387 MB
```

```
5 php                 7.1-apache          b177bfebca36        2 weeks ago
            387 MB
```

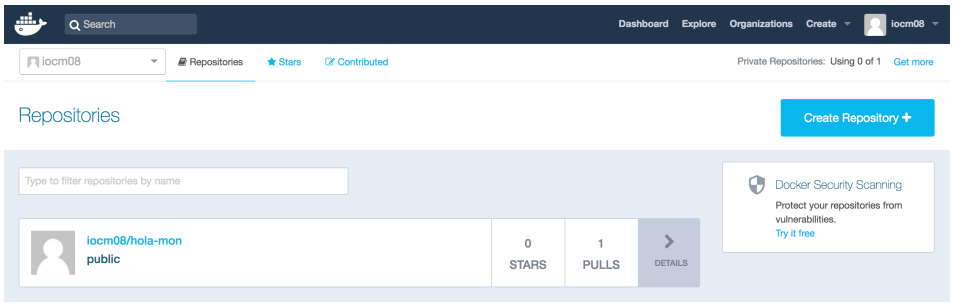
Fixeu-vos que a banda de la imatge utilitzada com a base i la imatge del contenidor creat originalment, s'ha afegit una nova imatge que inclou l'espai de noms, però conserva l'identificador original.

Seguidament, podeu pujar la imatge a Docker Hub fent servir l'ordre `docker push`, i el resultat serà similar al següent:

```
1  The push refers to a repository [docker.io/iocm08/hola-mon]
2  2c16acb979ce: Pushed
3  1c6da1b67140: Mounted from library/php
4  524998ac985c: Mounted from library/php
5  b0048e0cd0f0: Mounted from library/php
6  0739f0fe8939: Mounted from library/php
7  8f3f5d50c083: Mounted from library/php
8  46af8a5b5036: Mounted from library/php
9  4b63183c9b32: Mounted from library/php
10 5e34f9b1cc0a: Mounted from library/php
11 882b0937fe95: Mounted from library/php
12 6b42159d1088: Mounted from library/php
13 0e985d879eb0: Mounted from library/php
14 2b6ca8b57a27: Mounted from library/php
15 5d6cbe0dbcf9: Mounted from library/php
16 latest: digest: sha256:
       bd3d069c537bdadc9587e52d9a88e1c06b7d4bd56c3b304cbb590fbbdb36dfaf size:
       3242
```

Si actualitzeu la pàgina web amb l'usuari autenticat a Docker Hub, veureu com ha aparegut el repositori "hola-mon", tal com apareix a la figura 2.8).

FIGURA 2.8. Pàgina principal d'usuari a Docker Hub



Per poder provar que el contenidor s'ha pujat correctament, podeu descarregar-lo i provar de posar-lo en marxa, però primer heu d'eliminar la imatge creada. Per eliminar una imatge o un *tag*, s'ha d'utilitzar l'ordre `docker rmi`, indicant el nom de la imatge i l'etiqueta en cas que aquesta no sigui "latest" (que fa referència a l'última).

És possible que alguna de les imatges o etiquetes siguin utilitzades per algun contenidor (encara que els contenidors s'hagin aturat). Per forçar-ne l'eliminació, s'ha de fer servir l'opció `-force`. Així doncs, per eliminar la imatge "hola-mon" i l'etiqueta "iocm08/hola-mon", suposant que la segona estigui sent utilitzada, es fa de la manera següent:

```
1 docker rmi hola-mon
2 docker rmi iocm08/hola-mon --force
```

El resultat serà similar al següent:

```
Untagged: hola-mon:latest
Untagged: iocm08/hola-mon:latest
Untagged: iocm08/hola-mon@sha256:
    bd3d069c537bdadc9587e52d9a88e1c06b7d4bd56c3b304cbb590fbbdb36dfaf
Deleted: sha256:
    e991d0ca60632dcf5795cb8e18da70f3aa814b0309539c003ad0bbb468686f7d
Deleted: sha256:
    a021f0647910f846584fdd047aa9e4ec5fb9aebfcbfa2e0ff08c843ac7f10ada
```

Si executeu l'ordre `docker images`, comprovareu que només hi ha la imatge base utilitzada per crear la vostra imatge:

```
~/prova-docker $ docker images
REPOSITORY            TAG                 IMAGE ID            CREATED
                  SIZE
php                   7.1-apache          b177bfebca36        2 weeks ago
             387 MB
```

Per acabar, podeu descarregar la imatge utilitzant l'ordre `docker pull` i indicant el repositori on es troba (espai de noms i nom del repositori). Aquesta informació també es pot trobar a la pàgina d'usuari de Docker Hub fent clic al repositori que vulgueu descarregar. Per exemple, per descarregar la imatge del repositori "iocm08/hola-mon", heu d'utilitzar l'ordre següent:

```
docker pull iocm08/hola-mon
```

El resultat que obtindreu serà similar al següent:

```
~/prova-docker $ docker pull iocm08/hola-mon
Using default tag: latest
latest: Pulling from iocm08/hola-mon
6d827a3ef358: Already exists
87fe8fbc743a: Already exists
f6d1a8d304ab: Already exists
caf3547d9b73: Already exists
1004db2760ff: Already exists
66e2d66a547e: Already exists
bbfaa62c234a: Already exists
19ce8807f4d1: Already exists
63f8d35ca798: Already exists
a5594b4d2a52: Already exists
42f1cbd038cf: Already exists
a739656e85cb: Already exists
97b6a5f245a1: Already exists
a8f59612df6a: Already exists
Digest: sha256:bd3d069c537bdadc9587e52d9a88e1c06b7d4bd56c3b304cbb590fbbdb36dfaf
Status: Downloaded newer image for iocm08/hola-mon:latest
```

Un cop més, podeu utilitzar l'ordre `docker images` per comprovar que la imatge és al sistema i que pot executar-se amb `docker run`. Per exemple, en el cas del contenidor "iocm08/hola-mon" el resultat seria el següent:

```
~/prova-docker $ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED
                  SIZE
iocm08/hola-mon     latest              e991d0ca6063        2 hours ago
             387 MB
```

```
4 php                 7.1-apache          b177bfebca36        2 weeks ago
            387 MB
```

I per executar-lo es faria servir aquesta ordre:

```
1 docker run iocm08/hola-mon
```

Fixeu-vos que tot i que el contenidor original no feia servir cap espai de noms, quan s'utilitza una imatge descarregada s'ha d'incloure. En cas contrari, Docker no la troba.

Com heu pogut comprovar, començar a utilitzar Docker no és excessivament complicat, però dominar totes les seves opcions i els desplegaments a una escala major és força complex. Cal tenir en compte que aquí només s'ha presentat un exemple molt simple, però que us pot servir per iniciar-vos en la utilització de contenidors.

Altres aspectes de la utilització de Docker que cal tenir en compte són els següents:

- Quan acaba la tasca que s'està executant al contenidor, el contenidor s'atura automàticament.
- Cada aplicació s'executa en un contenidor diferent, ja que cada contenidor està lligat a un únic procés.
- Un mateix equip pot tenir múltiples contenidors funcionant al mateix temps. Per veure els contenidors en execució es pot fer servir l'ordre `docker ps`.
- Docker fa servir un sistema de capes per generar les imatges; aquestes capes es corresponen amb les línies del fitxer Dockerfile.
- Per automatitzar el desplegament s'acostuma a utilitzar altres eines i serveis de desplegament com Kubernetes (kubernetes.io) o Ansible (www.ansible.com).