

Instal·lació i configuració de sistemes operatius lliures

Juan José López Zamorano

Sistemes operatius en xarxa

Índex

Introducció	5
Resultats d'aprenentatge	7
1 Sistemes operatius lliures. Instal·lació de sistemes GNU/Linux	9
1.1 Orígens del programari lliure	9
1.2 GNU	10
1.3 GNU/Linux	11
1.4 Distribucions GNU/Linux	12
1.5 Documentació i recursos	14
1.6 Instal·lació de sistemes GNU/Linux	15
1.6.1 Consideracions prèvies per a la instal·lació de sistemes GNU/Linux	15
1.6.2 Gestió de les particions de disc	16
1.6.3 Tipus d'instal·lacions	25
1.6.4 Instal·lació Ubuntu	28
2 Configuració i monitoratge en sistemes GNU/Linux	37
2.1 Ordres i fitxers bàsics de configuració GNU/Linux	37
2.1.1 L'intèrpret d'ordres	37
2.1.2 Sintaxi de les ordres	39
2.1.3 Fitxers de configuració més utilitzats en el GNU/Linux	39
2.2 Gestió de paquets en el GNU/Linux	40
2.2.1 Gestió de paquets DEB	42
2.2.2 Gestió de paquets RPM	50
2.3 Actualització del sistema operatiu	52
2.3.1 Actualització de l'Ubuntu Desktop Edition	52
2.3.2 Actualització de l'Ubuntu Server Edition	53
2.4 Interpretació dels processos d'arrencada i aturada als sistemes GNU/Linux	54
2.4.1 Procés d'arrencada	54
2.4.2 Gestors d'arrencada	56
2.4.3 El procés init	56
2.4.4 Procés d'aturada	60
2.5 Configuració dels paràmetres de xarxa als sistemes GNU/Linux	60
2.5.1 Detecció i configuració del maquinari de xarxa	60
2.5.2 Assignació de paràmetres de xarxa	61
2.5.3 Eines de xarxa	63
2.6 Automatització de tasques als sistemes GNU/Linux	68
2.7 Connexió remota als sistemes GNU/Linux	71
2.8 Monitoratge i manteniment de sistemes GNU/Linux	73
2.8.1 Monitoratge de la CPU	75
2.8.2 Monitoratge de la memòria	76
2.8.3 Monitoratge de l'emmagatzematge	76
2.8.4 Monitoratge de la xarxa	77

2.8.5	Eines i ordres de monitoratge	78
2.9	Documentació del sistema	86
3	Serveis de directori	89
3.1	Què és un directori?	89
3.2	Que és un servei de directori?	90
3.2.1	Què no és un servei de directori?	90
3.2.2	Utilitats d'un servei de directori	92
3.2.3	Arquitectura del servei de directori	95
3.2.4	Serveis de directori distribuïts	95
3.2.5	Seguretat del servei de directori	96
3.3	LDAP	96
3.3.1	Ús de l'LDAP	97
3.3.2	Orígens de l'LDAP	98
3.3.3	Funcionament de l'LDAP	99
3.3.4	Avantatges en l'ús de l'LDAP	99
3.3.5	Estructura del directori LDAP	100
3.3.6	El format d'intercanvi de dades LDIF	104
3.3.7	Operacions de l'LDAP en el directori	104
3.4	Instal·lació i configuració d'un servei de directori als sistemes GNU/Linux	107
3.4.1	Introducció a l'OpenLDAP	108
3.4.2	Instal·lació OpenLDAP	108
3.4.3	Instal·lació del servidor OpenLDAP	109
3.4.4	Instal·lació del client OpenLDAP	110
3.4.5	Configuració del servidor OpenLDAP	111
3.4.6	Configuració del client OpenLDAP	113
3.4.7	Gestió del servei OpenLDAP	114
4	Autenticació d'usuaris en xarxes GNU/Linux	125
4.1	Què és un domini?	125
4.2	Autenticació en els sistemes GNU/Linux	127
4.2.1	Mecanisme general d'autenticació	127
4.2.2	Gestió d'usuaris en els sistemes GNU/Linux	128
4.2.3	L'arxiu /etc/passwd	130
4.2.4	L'arxiu /etc/group	131
4.2.5	L'arxiu /etc/shadow	131
4.2.6	Eines de gestió d'usuaris	132
4.2.7	Perfils d'usuari	134
4.2.8	Altres mecanismes d'autenticació en els sistemes GNU/Linux	137

Introducció

Els sistemes operatius constitueixen una part fonamental de qualsevol sistema informàtic. S'encarreguen de comunicar els usuaris amb el maquinari del sistema i així permeten aprofitar tota la potència i tots els avantatges que proporcionen els ordinadors.

Els sistemes operatius lliures i tot el programari de codi obert ofereixen una alternativa de negoci dins el mercat informàtic que cada vegada està més consolidada. Els sistemes operatius lliures es caracteritzen per ser robustos, fiables, adaptables i potents, propietats que fan que moltes vegades superin els sistemes operatius de propietat. Aquest també és el motiu pel qual els sistemes lliures cada vegada són més presents en les organitzacions i les institucions, en què implementen una gran varietat d'escenaris i solucions juntament amb altres tipus de sistemes o no.

Al llarg de la unitat “Instal·lació i configuració de sistemes operatius lliures” introduirem l'alumnat en l'ús i la filosofia dels sistemes operatius lliures perquè pugui assolir els coneixements necessaris sobre els temes que es tracten des d'aquest punt de vista. D'aquesta manera, podrà conèixer millor el funcionament dels sistemes operatius lliures i les propietats que tenen. Això li proporcionarà la capacitat per escollir, com a tècnic, dins l'ampli ventall de possibilitats que ofereix el mercat del sistemes operatius.

En l'apartat “Sistemes operatius lliures. Instal·lació de sistemes GNU/Linux” es fa un repàs de la història dels sistemes operatius lliures i del programari lliure. S'expliquen la filosofia i les característiques que el determinen i es fa referència a les distribucions de sistemes operatius lliures més utilitzades en l'actualitat. Per altra banda, també s'ensenya el procés d'instal·lació d'un sistema operatiu lliure en la versió servidor, i els passos que s'han de seguir o tenir en compte abans de la instal·lació del sistema operatiu en un equip que estigui connectat en xarxa amb altres màquines.

En l'apartat “Configuració i monitoratge en sistemes GNU/Linux” s'expliquen ordres, fitxers i aplicacions útils per fer la configuració, l'actualització i el monitoratge d'un sistema operatiu lliure una vegada instal·lat. També es mostra amb detall el procés d'arrencada i aturada del sistema i la configuració dels paràmetres de xarxa de l'equip. A més, s'explica el procés d'automatització de tasques i es tracten els conceptes i la importància del monitoratge i el manteniment dels sistemes operatius en xarxa. Finalment, es repassa el procés de documentació que es porta a terme durant el monitoratge i el manteniment del sistema.

En l'apartat “Serveis de directori” es defineixen els conceptes de servei de directori. A més, es fa una comparativa entre un servei de directori i altres serveis que poden semblar similars i que es fan servir en l'àmbit dels sistemes operatius connectats en xarxa, com serveis web, SGBD, sistemes de fitxers, etc. Una vegada introduïts els conceptes, s'expliquen els orígens, les característiques,

l’arquitectura i el funcionament d’un dels protocols de servei de directori més utilitzat, l’LDAP. Per tal d’introduir totalment l’alumnat en la utilització dels conceptes i els protocols exposats anteriorment, s’explica el procés d’instal·lació, configuració i utilització d’una de les implementacions de codi obert del protocol LDAP més utilitzades, l’OpenLDAP. Finalment, es mostra l’ús d’eines gràfiques per a la implementació d’un directori sobre l’OpenLDAP.

En l’apartat “Autenticació d’usuaris en xarxes GNU/Linux” es mostra el concepte de *domini* entès des del punt de vista dels sistemes operatius lliures. A continuació, es repassa el procés de gestió d’usuaris i grups, i també les ordres i els fitxers que hi estan relacionats. Després es descriuen els diversos mecanismes d’autenticació d’usuaris i grups en els sistemes lliures. Finalment, es mostra el procés d’implementació d’un sistema d’autenticació en xarxa de màquines GNU/Linux per mitjà d’un servei de directori.

Per treballar els continguts d’aquesta unitat, és convenient anar fent les activitats i els exercicis d’autoavaluació. És possible que l’alumnat ja conegui alguns dels conceptes, ordres o eines que apareixen en la unitat formativa. Es tracta, però, de contextualitzar al màxim possible l’ús d’aquests conceptes amb els temes tractats.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Instal·la i monitoritza sistemes operatius en xarxa lliures, descrivint característiques, eines utilitzades. Realitza tasques de gestió sobre dominis utilitzant eines d'administració de dominis i interpretant la documentació tècnica.
 - Realitza l'estudi de compatibilitat del sistema informàtic. Planifica el particionament del disc. Selecciona i aplica els sistemes d'arxius i components a instal·lar. Instal·la i actualitza el sistema .Comprova el correcte funcionament i la connectivitat dels sistemes operatius i programari instal·lats.
 - Diferencia els modes d'instal·lació. Automatització d'instal·lacions i tasques.
 - Interpreta la informació de configuració del sistema operatiu en xarxa i realitza tasques de manteniment del programari instal·lat en el sistema i de configuració de l'entorn.
 - Instal·la, configura i descriu les característiques de programes de monitorització. Identifica problemes de rendiment en el sistema a partir de les traces generades pel propi sistema.
 - Documenta adequadament els processos realitzats d'instal·lació i monitorització, les incidències aparegudes i les solucions aportades.
 - Identifica la funció de servei de directori i domini, l'estructura, els seus elements i nomenclatura. Realitza la instal·lació i configuració bàsica del servei de directori i estableix relacions de confiança.
 - Utilitza eines gràfiques d'administració de domini i consoles d'administració.
 - Utilitza agrupacions d'elements per a la creació de models administratius. Crea, configura i gestiona comptes d'usuari, grups, equips i diferents tipus de perfils.
 - Especifica el propòsit dels grups, els seus tipus i àmbits i gestiona la pertinença d'usuaris a grups. Identifica les característiques d'usuaris i grups predeterminats i especials. Utilitza eines per a l'administració d'usuaris i grups, incloses en el sistema operatiu en xarxa.
 - Aplica directives a la gestió del domini. Identifica tipus de directives.
 - Verifica la correcció de les tasques realitzades i documenta adequadament les tasques de gestió i administració de dominis realitzades .
 - Cerca i interpreta documentació tècnica en les llengües oficials i en les de més ús al sector.

1. Sistemes operatius lliures. Instal·lació de sistemes GNU/Linux

La situació en els orígens dels sistemes operatius era totalment diferent de l'actual. Inicialment les empreses d'informàtica no donaven cap valor als sistemes operatius, actitud que va canviar quan es van adonar de la possibilitat de negoci que hi havia en la comercialització dels sistemes.

Aquest canvi va impulsar l'aparició de projectes i moviments que promovien la llibertat del programari, d'entre els més destacats es troba GNU/Linux. Sota les premisses i els estàndards del projecte GNU/Linux existeixen moltíssimes distribucions que proporcionen sistemes operatius robustos i de qualitat alternatius als sistemes operatius de propietat. Els sistemes GNU/Linux estan basats en el sistema operatiu Unix, però a diferència d'aquest, són sistemes lliures i oberts.

Abans de procedir a la instal·lació de qualsevol sistema operatiu de la família GNU/Linux, heu de tenir en compte una sèrie de consideracions que determinaran, entre altres coses, la distribució que s'ha d'instal·lar, el tipus de sistema operatiu, client o servidor, els mecanismes o les infraestructures emprats per a la instal·lació, el tipus de sistema de fitxers utilitzats en el suport d'emmagatzematge on instal·lem el sistema, etc.

Una vegada considerats tots els factors previs a la instal·lació, heu de seguir una sèrie de passos per instal·lar un sistema operatiu Ubuntu Server Edition.

1.1 Orígens del programari lliure

A finals de la dècada dels anys seixanta i durant els inicis de la dels setanta, el panorama en el món de la informàtica era totalment diferent a l'actual.

Les grans empreses informàtiques no donaven la importància que actualment es dóna al programari. Els fabricants d'ordinadors mateixos incorporaven a les seves màquines algun tipus de sistema operatiu i aplicacions sense donar-hi cap valor. Les persones que feien ús de la informàtica en àmbits universitaris i empresarials creaven i compartien el programari sense restriccions.

Els Bell Labs (**AT&T**) van desenvolupar les primeres versions d'**UNIX** en aquest entorn. Les característiques principals de l'**UNIX** eren les següents:

- Sistema multitasca i multiusuari.
- Gran capacitat per a la gestió de xarxes.
- Compatibilitat amb maquinari de diferents fabricants.
- Robustesa i estabilitat.

Programari propietari

El terme *programari propietari* fa referència a qualsevol programa informàtic en què els usuaris tenen limitades les possibilitats d'usar-lo, modificar-lo o redistribuir-lo (amb modificacions o sense). També es considera de propietat si el codi font del programa no està disponible o si és d'accés restringit.

Totes aquestes característiques van fer que l'UNIX obtingués una popularitat extraordinària.

A la dècada dels anys vuitanta aquesta situació va canviar. Les màquines utilitzaven majoritàriament programari propietari, cosa que impedia als usuaris conèixer, modificar o redistribuir el codi dels programes.

En aquesta nova situació, a Richard Stallman, programador que aleshores treballava al MIT (Massachusetts Institute of Technology), no li va agradar gens veure que cada vegada era més difícil aconseguir el codi font dels programes que utilitzava per adaptar-los a les seves necessitats.

Així doncs, Stallman va decidir iniciar un gran projecte per intentar obrir una altra vegada el codi font dels programes. Conscient que no podria aconseguir que les companyies tornessin a obrir el codi dels programes, es va proposar crear un nou sistema operatiu que no tingués les restriccions que tenien els sistemes que hi havia en aquell moment. D'aquesta manera, va començar un projecte anomenat **GNU**.

1.2 GNU

GNU és un acrònim recursiu que significa 'GNU no és UNIX' (*GNU's not UNIX*).



El logotip de GNU és el cap d'un nyu.

FSF

La Free Software Foundation (Fundació per al Programari Lliure) és una organització creada a l'octubre de 1985 per Richard Stallman i altres entusiastes del programari lliure amb el propòsit de difondre aquest moviment.

Entenem que són de programari lliure els programes que ens permeten obtenir-ne el codi font i també estudiar-los, modificar-los i redistribuir-los sense que ens obliguin a pagar per fer-ho.

El projecte GNU compta amb el suport de la Free Software Foundation, que el dota de cobertura econòmica, legal i logística.

La filosofia que la Free Software Foundation té del programari es defineix a partir de les quatre llibertats següents:

- Llibertat de poder usar el programa amb qualsevol propòsit. No és possible obligar a executar-lo només en un determinat nombre de màquines o sota unes condicions específiques.
- Llibertat per estudiar com funciona el programa i adaptar-lo a les necessitats pròpies. L'accés al codi font és una condició necessària per garantir aquesta llibertat. Si fos d'una altra manera, s'hauria d'aplicar enginyeria inversa.
- Llibertat per distribuir lliurement còpies del programari.

- Llibertat per millorar el programa i fer públiques les pròpies millores en benefici de tota la comunitat. L'accés al codi font, per tant, és un requisit imprescindible per assegurar aquesta llibertat.

Per donar totes aquestes llibertats al programari que es desenvolupa en el projecte GNU i als usuaris finals, es va escriure la llicència GPL (*general public license*), amb la qual s'ha protegit tot aquest tipus de codi. Aquesta llicència posa per escrit les idees comentades anteriorment.

Val a dir que no hem de confondre el terme *lliure* amb el terme *gratuït*. Atès que totes dues paraules equivalen a *free* en anglès, hi pot haver confusió. El programari lliure no ha de ser gratuït. Podem demanar els diners que vulguem pels programes i el codi font, el suport que podem oferir als usuaris, els llibres que venguem o el material que proporcionem, tal com fan moltes companyies que distribueixen GNU/Linux.

Llicències GNU

La GPL no és l'única llicència que hi ha en el projecte GNU (n'hi ha d'altres com l'LGPL, l'MGPL o la GFDL) ni tampoc és l'única que regula els terminis d'utilització del programari lliure (BSD, OpenSSL, MIT License). Tanmateix, sí que podem dir que és la més important i que és la llicència en què es basen algunes de la resta de les llicències utilitzades en el món del programari lliure.

1.3 GNU/Linux

A finals de la dècada dels anys vuitanta, el projecte GNU disposava d'una sèrie d'elements que li donaven certa robustesa. Tenia unes pretensions ben definides quant a finalitat i funcionament. A més, GNU també comptava amb una fundació que li donava suport, una llicència que li aportava un marc legal i filosòfic i una sèrie d'aplicacions de codi obert, com l'editor de textos Emacs, el compilador GCC o l'intèrpret d'ordres Bash. No obstant això, no disposava del component clau: el nucli (*kernel*).

El 1991, un estudiant de la Universitat d'Hèlsinki, Linus Torvalds, va decidir crear el seu propi nucli per a un sistema operatiu nou, que va anomenar *Linux*. El Linux intentava millorar el sistema operatiu MINIX, un sistema amb finalitats docents basat en l'UNIX, creat uns anys enrere pel professor de la Universitat d'Holanda Andrew Tanenbaum.

La idea de Linus Torvalds era crear un UNIX per a PC, amb la finalitat que tothom el pogués utilitzar en el seu ordinador. Linus va donar a conèixer el seu projecte en un fòrum de debat de MINIX i poc després va aportar la seva part del codi del nucli del Linux. Aquesta iniciativa va obtenir una resposta ràpida i massiva d'experts informàtics d'arreu del món, que hi van aportar coneixements i treball per tal de continuar el desenvolupament del nucli del Linux. El projecte ràpidament va adoptar la llicència GNU i es va convertir, així, en el nucli del sistema operatiu del projecte GNU. Es va formar el que ara es coneix com a GNU/Linux.

GNU/Linux és un dels termes emprats per referir-se al sistema operatiu lliure similar a l'UNIX que utilitzà el nucli Linux i eines de sistema GNU.



El Tux i el nyu són els logotip de Linux i GNU.

Nucli (kernel)

En informàtica, el *nucli* (també conegut amb l'anglisme *kernel*) és la part fonamental d'un sistema operatiu. És el programari responsable de facilitar accés segur al maquinari de l'ordinador als diferents programes. És a dir, és l'encarregat de gestionar recursos per mitjà de serveis de crida al sistema.

Només el 2% del codi del nucli Linux actual està escrit per Linus Torvalds. Tanmateix, es considera que Torvalds és el pare del nucli.

A banda del projecte GNU/Linux també es van desenvolupar altres projectes relacionats amb el programari lliure, com el BSD o l'Open Source Initiative, que

també es fan servir actualment.

1.4 Distribucions GNU/Linux

Hem de tenir en compte que els sistemes GNU/Linux estan formats per tres grans grups d'aplicacions:

1. El sistema o nucli del sistema. És l'erència de Linus Torvalds i actualment és la versió 2.6.X. Podem trobar la darrera versió del nucli a Internet i descarregar-la lliurement. Aquest nucli, però, no incorpora cap eina que es pugui fer servir. Constitueix un sistema base per arrencar i comunicar-se amb el maquinari de l'ordinador (aproximadament un 3% del total del codi GNU del sistema).
2. El conjunt d'aplicacions de distribució lliure que completen el sistema base. Són editors, compiladors i utilitats diverses del sistema que en permeten l'explotació. Representen la major part del sistema base i, en concret, un total d'un 30% del codi d'una distribució GNU/Linux estàndard. La majoria d'aquestes aplicacions deriven directament del projecte GNU de la Free Software Foundation.
3. Tota la resta d'aplicacions que no formen part del sistema base. Aquí hi ha la major part de les aplicacions i els serveis d'explotació del sistema: Apache, Samba, SQUID, SSH, NAMED, KDE, GNOME, etc. Segons el tipus de distribució GNU/Linux, qualsevol aplicació d'aquest gran paquet (el més nombrós) ha de complir estrictament l'estàndard GNU (llicència GPL o similar).

Totes les aplicacions estan disponibles gratuïtament a Internet. Tanmateix, per evitar la tasca de cerca i descàrrega, algunes distribucions presenten paquets de col·leccions d'aplicacions que juntament amb el nucli completen el sistema operatiu. Actualment, hi ha moltes distribucions diferents basades en GNU/Linux.

Per tal que un sistema operatiu compleixi l'estàndard GNU/Linux cal, principalment, estar sota les llicències promogudes per l'FSF de tal manera que es respectin els preceptes de la filosofia del programari lliure; també ha de complir que el seu nucli estigui basat en el nucli Linux i a més el sistema ha de fer servir l'estàndard jeràrquic en l'estructura de directoris principals i els seus continguts, és a dir, que les distribucions respecten el *filesystem hierarchy standard* o FHS.

Les diferències que hi ha entre aquestes distribucions les determinen, sobretot, la ubicació dels arxius en el sistema, la gestió de recursos o la utilització d'aplicacions determinades (per exemple, sistemes d'instal·lació de paquets, entorn d'escriptori, etc.).

A continuació, descriurem algunes de les distribucions GNU/Linux més conegudes o utilitzades (figura 1.1):

Filesystem hierarchy standard o FHS

FHS és una norma que defineix els directoris principals i els seus continguts en el sistema operatiu GNU/Linux i altres sistemes de la família Unix. Es va dissenyar originalment el 1994 per a estandarditzar el sistema d'arxius de les distribucions de Linux, basant-se en l'organització de directoris tradicional dels sistemes Unix.

FIGURA 1.1

De dalt a baix i d'esquerra a dreta, els logotips de: Fedora, Suse, Red Hat, Linkat, Ubuntu, Debian

Sobre el sistema gestor de paquets podeu veure l'apartat "Configuració i monitoratge en sistemes GNU/Linux".

Red Hat Linux: és una de les distribucions més populars i també una de les més antigues. Està desenvolupada per una empresa nord-americana que inicialment la va comercialitzar com un sistema operatiu per a servidors. Va ser la creadora de l'eina RPM per a l'administració de paquets, que posteriorment han incorporat altres distribucions. També va ser la primera distribució que la va utilitzar. En l'actualitat, la Red Hat Linux se centra en la versió empresarial de la distribució Red Hat Enterprise Linux. No obstant això, hi ha una versió lliure del projecte que manté una comunitat anomenada Fedora Core. Tot i que és independent de la Red Hat Linux, l'empresa hi dóna suport. Actualment, el sistema operatiu Fedora és un dels sistemes més utilitzats pels usuaris de la comunitat GNU/Linux.

Suse Linux: és una de les distribucions més conegudes que hi ha a escala mundial. La distribució Suse la va desenvolupar una empresa alemanya i després la va adquirir la multinacional nord-americana Novell. Novell va impulsar el projecte OpenSuse per tal de fer el codi més obert i obtenir el suport de més desenvolupadors i usuaris de la comunitat GNU/Linux. La virtut principal d'aquesta distribució és que és una de les més senzilles d'instal·lar i administrar, ja que disposa de múltiples assistents gràfics que permeten completar diverses tasques. En destaca l'eina d'instal·lació i configuració d'aplicacions YaST. La Suse utilitza el sistema de paquets RPM originari de la Red Hat.

Debian: és una de les distribucions que fa més temps que és en el mercat. Encara existeix i ha evolucionat. S'hi basen moltes altres distribucions. La desenvolupen i la mantenen col·laboradors d'arreu del món i, quant a infraestructura, només rep suport d'alguna empresa. El sistema de gestió de paquets de la Debian permet diferenciar clarament el programari lliure del que no ho és. D'aquesta manera, ofereix la possibilitat de crear tot el sistema només amb programes de programari lliure. La Debian i les distribucions derivades utilitzen el format de paquet .deb i incorporen les eines adequades per fer anar aquest tipus de paquet, com ara dpkg, apt o aptitude. La Debian és una de les distribucions més estables i segures que hi ha.

Ubuntu: actualment, és la distribució més utilitzada. També és la que farem servir per fer les pràctiques d'aquesta unitat. La Ubuntu és una distribució basada en la

Debian i està patrocinada per l'empresa Canonical, que en manté la distribució lliure i gratuïta. La Ubuntu allibera una versió nova cada sis mesos que rep el suport de Canonical durant un determinat temps. A més, disposa de tot el suport de la comunitat de programari lliure. En la Ubuntu podem trobar diverses derivacions o sabors fonamentalment dependents de l'entorn d'escriptori que utilitzen. Entre d'altres, hi ha la Ubuntu Desktop, que utilitza l'entorn d'escriptori GNOME; Kubuntu, que utilitza l'entorn KDE; Xubuntu, que utilitza l'entorn XFCE; Edubunu, orientada a àmbits educatius, i Ubuntu Server, sense entorn gràfic i orientada a la utilització en servidors.

Entorn d'escriptori

Qualsevol sistema GNU/Linux pot funcionar tant en entorn gràfic com en mode terminal. El mode terminal és més comú en distribucions per a servidors, mentre que la interfície gràfica està més orientada a l'usuari final. Un escriptori és un conjunt d'elements conformat per finestres, icones i similars que faciliten la utilització del computador. Els escriptoris més populars en Linux són: GNOME, KDE, LXDE, Xfce, Xf.

Linkat: és la distribució GNU/Linux del Departament d'Ensenyament de la Generalitat de Catalunya. Està basada en la distribució Suse Linux Enterprise Desktop. El sistema gestor de paquets, com el de la Suse, està basat en l'RPM. Actualment, és la versió 3 i utilitza per defecte l'entorn d'escriptori GNOME, encara que també estan disponibles els entorns de KDE i XFCE.

Ordre man

Linux proporciona un sistema d'ajuda basat en text al qual s'accedeix mitjançant l'ordre man. L'ordre és l'abreviatura de **manual**.

L'ordre man ens proporciona ajuda sobre les ordres, els fitxers de configuració, les funcions i altres ítems del sistema. La sintaxi general de l'ordre man és
`; $man <element a consultar>`

D'una manera recursiva, podem utilitzar la mateixa ordre man per consultar el manual de l'ordre man;
`$man man`

Els manuals de Linux estan organitzats en nou categories, les quals es poden consultar en el manual de man.

1.5 Documentació i recursos

Des de l'inici del projecte GNU/Linux, els desenvolupadors i els usuaris del programari lliure s'han comunicat mitjançant Internet. Per això a la xarxa sempre s'ha pogut trobar molta informació sobre el projecte, les aplicacions i les distribucions implicades. La majoria de programes estan disponibles a Internet, empaquetats en algun dels sistemes que hi ha o bé directament per mitjà del seu codi font. Moltes de les distribucions que hi ha també es poden baixar d'Internet lliurement. Tot i així, si volem disposar del suport que ofereixen algunes companyies, la millor manera és comprar el material que proporcionen (CD, manuals, etc.) i registrar-s'hi.

En l'àmbit del programari lliure, una de les capacitats clau per moure-s'hi amb soltesa és saber trobar la informació que necessitem. Saber buscar i trobar la documentació o els recursos que s'adaptin als problemes que tenim ens ajudarà a estalviar temps i esforç. Les fonts principals en què podem trobar informació per resoldre problemes i aprofundir en diversos temes són les següents: la documentació generada per la comunitat de programari lliure, que ens podem descarregar gratuïtament de la xarxa; els fòrums, les llistes de correu, els grups de notícies relacionades amb el programari lliure, els com-es-fa (*how-to manuals*), les pàgines de les diverses distribucions, la documentació incorporada en el sistema, per exemple mitjançant l'ordre man, etc.

1.6 Instal·lació de sistemes GNU/Linux

Abans d'iniciar el procés d'instal·lació d'un sistema operatiu lliure GNU/Linux (en el nostre cas, la versió Server de la distribució Ubuntu), cal tenir en compte un seguit de consideracions: quina serà la utilització del sistema operatiu, quin maquinari tenim, els diferents tipus d'instal·lació que podem fer i les possibilitats que tenim per fer particions en el suport d'emmagatzematge en què residirà el sistema.

1.6.1 Consideracions prèvies per a la instal·lació de sistemes GNU/Linux

Abans d'iniciar la instal·lació del sistema operatiu en un equip, ens hem de fer una sèrie de preguntes:

1. **Quina serà la utilització del sistema operatiu?** Hem de respondre quin és el propòsit general per al qual volem el sistema o quin és el paper de la màquina en la xarxa. Ens hem de formular, entre altres, les preguntes següents:
 - Si és un servidor o una estació de treball.
 - Si és un servidor, quins tipus de serveis oferirà.
 - Les aplicacions necessàries.
 - La càrrega de dades que suportarà.
 - La quantitat i el tipus de trànsit de xarxa (local o extern).
 - El nombre d'usuaris del sistema.
2. **Quin maquinari tenim?** Hem de tenir molt clar el maquinari de què disposem.
 - Processador.
 - Memòria RAM.
 - Disc dur.
 - Targeta gràfica.
 - Lector de CD/DVD.
 - Targeta de xarxa.
3. **Quin tipus d'instal·lació farem?** Hem de saber quins suports, quines eines i quines infraestructures tenim per fer la instal·lació del sistema operatiu.
 - CD/DVD.
 - Utilitzar el sistema de xarxa, mitjançant FTP o HTTP.
 - Restaurar una imatge del sistema o clonar un disc dur.

- Altres formes: USB, LiveCD personalitzat, etc.

4. Quantes particions necessitem i de quin tipus? Hem de determinar el nombre de particions necessàries per al sistema i el tipus de sistema de fitxers de cadascuna.

- Nombre de particions primàries i tipus.
- Nombre de particions lògiques i tipus.

Podeu veure els conceptes de *particions primàries* i *lògiques* en l'apartat "Tipus de particions".

Elecció de la distribució

Moltes vegades, l'elecció d'una distribució depèn de l'empresa en què instal·lem el sistema o del sabor que més ens agradi. Moltes distribucions s'adaptaran correctament a les característiques d'ús que busquem.

Una vegada aclarides aquestes qüestions, podem decidir quina és la distribució i la versió que més ens interessa instal·lar. Per exemple, podem escollir distribucions orientades a l'àmbit empresarial, com la Red Hat o la Suse, o distribucions que tenen un ampli suport de la comunitat, com la Debian i la Ubuntu. Decidirem si volem utilitzar versions Desktop, en cas que instal·lem el sistema en una estació de treball, o Server, en cas que sigui per a un servidor de la xarxa. També haurem de tenir en compte les necessitats de maquinari específiques, com ara 64 o 32 bits, etc.

1.6.2 Gestió de les particions de disc

Abans d'instal·lar el sistema operatiu, us heu de plantejar el nombre, el tipus i la grandària de les particions que necessiteu en el disc dur de la màquina. Les haureu de crear amb alguna eina específica. Una vegada hagueu distribuït l'espai en el suport d'emmagatzematge, heu d'instal·lar el sistema.

Ús de les particions de disc

Podríem definir *partició* de la manera següent:

Una **partició de disc** és el nom genèric que rep cadascuna de les divisions que hi ha en una sola unitat física d'emmagatzematge de dades.

Cada partició representa una unitat lògica dins d'una unitat física. La funció principal de les particions és organitzar les dades en el suport d'emmagatzematge.

Els motius principals pels quals es recomana utilitzar particions en els discs durs són els següents:

- **Seguretat:** la informació la podeu tenir emmagatzemada en diferents particions. D'aquesta manera, si una partició es fa malbé, hi ha la possibilitat de recuperar la informació que hi ha emmagatzemada en les altres.
- **Coexistència de sistemes operatius:** si voleu tenir diferents sistemes operatius instal·lats en el mateix equip, és recomanable instal·lar cada sistema en un partició diferent, sobretot si tenen sistemes de fitxers distints.

- **Memòria virtual:** en els sistemes operatius GNU/Linux és recomanable utilitzar una partició del disc dur anomenada *swap*, que es fa servir per descarregar la memòria RAM.

Tota partició té un sistema propi d'arxius o format. Qualsevol sistema operatiu interpreta, utilitza i manipula cada partició com un disc físic independent, tot i que totes les partitions siguin en un únic disc físic.

Abans d'explicar el procés de partició, cal fer una consideració important sobre el tipus de sistema que voleu instal·lar. És a dir, cal que tingueu en compte els diferents escenaris, per als quals ens calen solucions diversificades.

Per exemple, en un servidor real serà pràcticament imprescindible una disposició de discs en RAID 1 (mirall) com a mínim que ens asseguri una recuperació del sistema en el cas que una de les unitats de disc falli.

En altres casos, com en servidors de prova, estacions de treball o instal·lacions duals, el procés de partició no té tanta importància.

Tot i que hi ha receptes que indiquen els percentatges aconsellats per a cada partició del sistema, aquest procés depèn molt de la utilitat que es dóna al sistema GNU/Linux i de les aplicacions que s'hi instal·lin. Per tant, queda a la vostra discreció una vegada hagiu valorat els principis bàsics del sistema.

En la majoria de sistemes GNU/Linux es requereixen almenys dues partitions:

- **/:** conté el sistema arrel i, si no hi ha cap altre punt de muntatge, tot el sistema.
- **swap:** és necessària per paginar la memòria RAM en el disc dur quan la RAM disponible s'acaba. També es pot crear una *swap* (àrea d'intercanvi) que sigui un fitxer, tot i que no és una solució tan eficient.

Cal tenir en compte que les mides proposades poden variar molt segons l'ús que vulgueu fer del sistema. Hi ha tantes possibilitats que és impossible proposar solucions que siguin universalment acceptables. La taula 1.1 mostra un exemple de directoris que es poden muntar en partitions separades.

TAULA 1.1. Directoris susceptibles de ser muntats en diferents partitions.

Partició (punt de muntatge)	Mida típica	Descripció
swap (no es monta)	1,5 a 2 vegades la RAM	És una memòria secundària a la RAM. És més lenta, però és necessària quan la RAM s'acaba. Es pot treballar sense àrea d'intercanvi, però quan el sistema es quedí sense RAM no paginarà correctament (és un error difícil de detectar, ja que sembla que l'ordinador simplement es pengi).

Gràcies a elements com les màquines virtuals, les ordres com dd i les imatges de disc, podeu tenir múltiples sistemes operatius en una mateixa partició.

RAID

Sistema d'emmagatzematge que utilitza múltiples discs durs, entre els quals distribueix o replica les dades. Aquest sistema comporta tota una sèrie de beneficis per al sistema informàtic: més integritat, més tolerància quant a errades, més velocitat de transferència de dades (*throughput*) i més capacitat.

TAULA 1.1 (continuació)

Partició (punt de muntatge)	Mida típica	Descripció
/home	Mínim 200 MB	En distribucions modernes és necessari un mínim de 200 MB per guardar els fitxers de configuració d'usuari de les aplicacions. A partir d'aquí, el valor màxim depèn de l'ús que cada usuari faci de l'ordinador.
/boot	20 - 200 MB	Guarda els fitxers d'arrencada del sistema (el nucli del sistema i els seus fitxers de suport). Heu de tenir en compte que les distribucions modernes van guardant els diferents nuclis que s'instal·len, cosa que fa que l'espai del boot augmenti amb el temps.
/usr	500 MB - 20 G	Conté la majoria de fitxers d'aplicacions GNU/Linux.
/opt	100 MB - ?	Carpeta de calaix de sastre on es col·loquen totes les aplicacions de tercers, és a dir, les aplicacions que no estan incloses en la distribució. Els paquets comercials s'acostumen a posar en aquesta carpeta.
/var	100 MB - ?	Conté les dades variables del sistema (bases de dades, cues, fitxers d'aplicacions, etc.). Depèn molt del tipus de sistema, però en una màquina que fa de servidor la partició pot ser més gran i la que té la informació més rellevant.
/tmp	100 MB - ?	Conté els fitxers temporals dels usuaris ordinaris. En sistemes amb molts usuaris pot ser una carpeta força gran.
/mnt	—	S'utilitza com a lloc per crear els punts de muntatge de dispositius removibles, com ara CD/DVD-ROM, memòries flaix, etc.
/media	—	Equivalent a /mnt.

El directori /dev, a partir de la versió 2.4 del nucli, es gestiona amb udev mitjançant un sistema de fitxers especial.

Alguns sistemes operatius, com el DOS o el Windows, necessiten carregar el sistema des d'una partició primària. En el GNU/Linux aquesta restricció no hi és.

Disc formatat

Un disc físic completament formatat consisteix, en realitat, en una partició primària que ocupa tot l'espai del disc i posseeix un sistema d'arxius. Pràcticament qualsevol sistema operatiu que reconegui el format d'aquest tipus de particions les pot detectar i els pot assignar una unitat.

Hi ha carpetes, com les següents, que mai no es posen en particions diferents. Totes se situaran en la partició en què es munti l'arrel /:

- /etc
- /bin i /sbin
- /lib
- /dev

Tipus de particions de disc

Hi ha tres tipus diferents de particions:

Partició primària: és la primera divisió que es fa en el suport d'emmagatzematge. És obligatori que hi hagi, almenys, una partició primària. En un suport d'emmagatzematge hi pot haver quatre particions primàries o tres particions primàries i una d'estesa (en el GNU/Linux es numeren de l'1 al 4). Han d'estar inscrites en la taula de particions que és en el primer sector del disc dur, en què n'hi ha de figurar alguna com a activa. Que la partició estigui activa vol dir que el programa d'inicialització li cedirà el control en el moment de l'arrencada (si no hi ha cap gestor d'arrencada instal·lat com GRUB o LILO).

Partició estesa: és un altre tipus de partició que actua com una partició primària. Serveix per contenir-hi unitats lògiques. Va ser ideada per trencar la limitació de quatre particions primàries en un sol disc físic. Només hi pot haver una partició d'aquest tipus per disc i només serveix per contenir particions lògiques. Per tant, és l'únic tipus de partició que no suporta un sistema d'arxius directament.

Partició lògica: ocupa una porció d'una partició estesa o la seva totalitat. Cada partició lògica es pot formatar amb un tipus específic de sistema d'arxius i se li pot assignar un directori del sistema. Les particions lògiques també es numeren. Així, en els sistemes GNU/Linux, sempre es comencen a numerar a partir del 5. No tots els sistemes operatius es poden instal·lar en una partició lògica. En funció de les capacitats del nucli i del maquinari, hi pot haver des de particions lògiques il·limitades fins a una partició estesa.

Sistema de fitxers

Un dels elements fonamentals que hem de tenir en compte a l'hora d'instal·lar un sistema operatiu determinat en una màquina és el sistema de fitxers que volem o podem utilitzar en el suport d'emmagatzematge en què instal·larem el sistema.

Els sistemes de fitxers indiquen la manera de gestionar els fitxers dins de les particions del suport d'emmagatzematge en què resideix el sistema operatiu.

Els sistemes de fitxers poden presentar diferents característiques segons la complexitat que tinguin. Alguns exemples d'aquestes característiques poden ser els següents: la previsió d'apagades, la indexació per a recerques ràpides, la possibilitat de recuperar dades o la reducció de la fragmentació per agilitzar la lectura de les dades.

Hi ha diversos tipus de sistemes de fitxers, normalment lligats a sistemes operatius concrets. Entre els més representatius hi ha els següents:

FAT32 o VFAT: és el sistema de fitxers tradicional de l'MS-DOS i de les primeres versions del Windows. Per aquesta raó, es considera un sistema universal, encara que té una gran fragmentació i és un mica inestable.

NTFS: sistema del Windows usat a partir de les versions 2000 i XP. És molt estable. El problema és que és de propietat, i per tant altres sistemes operatius no hi poden accedir de manera transparent. Des del GNU/Linux només se'n recomana

Journaling

El *journaling* és un mecanisme mitjançant el qual un sistema informàtic pot implementar transaccions. També es coneix com a *registre per diari*. Es basa a portar un diari (*journal*) en què s'emmagaçza la informació necessària per restablir les dades afectades per la transacció en cas que falli.

la lectura, ja que l'escriptura és una mica arriscada.

ext2: fins fa poc era el sistema estàndard del GNU/Linux. Té una fragmentació molt baixa, encara que és una mica lent a l'hora de manejar arxius molt grans.

ext3: és un sistema d'arxius amb registre per diari. El registre per diari soluciona el problema de les inconsistències implementant transaccions (similar a les bases de dades). És la versió millorada de l'ext2, amb previsió de pèrdua de dades per errades del disc dur o apagades. En contraprestació, és totalment impossible recuperar dades esborrades. El format ext3 és perfectament compatible amb el sistema d'arxius ext2. Actualment, és el més difós dins la comunitat GNU/Linux i es considera que és l'estàndard.

ext4: és una millora compatible de l'ext3. La novetat principal de l'ext4 és la possibilitat de fer “extent”, és a dir, la possibilitat de reservar una àrea contigua per a un arxiu. Això pot reduir, i fins i tot eliminar completament, la fragmentació d'arxius. Algunes millores són el suport de sistemes de fitxers fins a 1024 PiB, millor ús de la CPU i millores en les operacions de lectura i escriptura. L'ext4 és el sistema d'arxius per defecte de la Ubuntu des de la Ubuntu Jaunty.

reiserFS: és el sistema d'arxius per defecte d'algunes distribucions com la GNU/Linux o la Suse. Utilitza registre per diari i organitza els arxius de manera que les operacions que s'hi fan s'agilitzen molt.

swap: és el sistema d'arxius per a la partició d'intercanvi del GNU/Linux. És recomanable que els sistemes GNU/Linux tinguin una partició d'aquest tipus per carregar els programes i no saturar la memòria RAM.

Estructura de directoris GNU/Linux

Abans d'instal·lar un sistema operatiu GNU/Linux, és necessari conèixer o repasar l'estructura de directoris bàsica que conforma el sistema.

Podem definir l'estructura de directoris com una estructura de dades que utilitza un sistema operatiu per emmagatzemar i organitzar els fitxers en un suport d'emmagatzematge.

L'arrel de l'estructura d'un sistema de tipus GNU/Linux s'identifica amb una / i d'aquesta arrel en pengen diferents directoris que, a la vegada, contenen altres directoris i/o fitxers.

En la taula 1.2 es pot veure l'**FHS** (*filesystem hierarchy standard*) o **jerarquia estàndard de fitxers**, general del sistemes GNU/Linux, i una breu descripció del que podem trobar en cada directori. Segons les distribucions GNU/Linux que utilitzeu hi pot haver alguns canvis.

Grandària swap

Les regles, totalment empíriques, solen dir que és necessària una àrea d'intercanvi que faci el doble que la memòria RAM. Tanmateix, a partir d'1 GB de RAM és certament innecessari l'ús d'una àrea d'intercanvi, excepte per a sistemes de càlcul intensiu amb grans despeses de memòria.

Es poden veure els sistemes de fitxers suportats per la Ubuntu a `/usr/src/linux-headers-2.6.28-11/fs`

TAULA 1.2. Directoris GNU/Linux

Directori	Descripció
/	Directori arrel del qual pengen tots els directoris del sistema.
/dev	Dispositius físics del sistema, és a dir, el maquinari.
/etc	Arxius de configuració del sistema.
/sbin	Programes dels quals només pot llançar l'execució el superusuari.
/bin	Programes que poden ser llançats per tots els usuaris del sistema. Els programes d'aquest directori i de l'anterior es poden invocar introduint directament el nom a la consola.
/lib	Biblioteques necessàries perquè s'executin els programes que teniu a /sbin i /bin.
/proc	Arxius que envien o reben informació del nucli sobre els processos. És un directori virtual, és a dir, s'emmagatzema en memòria RAM. Cal anar en compte abans de modificar-ne el contingut.
/usr	Programes d'ús general per a tots els usuaris.
/tmp	Fitxers temporals.
/var	Informació variable com registres (<i>logs</i>) del sistema i fitxers de dades dels serveis del sistema.
/boot	Arxius de configuració de l'arrancada del sistema.
/media	Unitats físiques externes que hi hagi muntades: discos durs, memòries USB, CD, DVD, etc.
/mnt	És un directori semblant a /media, però es fa servir majoritàriament pels usuaris. Serveix per muntar discos durs i particions de manera temporal en el sistema.
/opt	Directori en què instal·lem les aplicacions no estàndard del sistema.
/srv	Dades que serveix el sistema.
/home	Directoris personals de tots els membres del sistema.

Una de les característiques dels sistemes UNIX i dels seus derivats és la manera de tractar a escala de sistema els dispositius de maquinari.

Tots els dispositius de maquinari estan identificats a escala de sistema per un dispositiu lògic que en GNU/Linux s'identifica amb un fitxer “especial” dins de l’arbre del sistema principal.

Dispositius en el GNU/Linux

En els sistemes GNU/Linux hi ha dues possibilitats a l'hora de determinar els noms dels dispositius:

- **Sistemes amb la llibreria libata:** tots els dispositius segueixen la forma /dev/sd*. Totes les distribucions modernes (2009) treballen amb aquesta llibreria.
- **Sistemes sense la llibreria libata:** es diferencia entre dispositius SCSI

(/dev/sd*) i dispositius IDE (/dev/hd*). Els dispositius SATA es tracten com a dispositius SCSI en aquests tipus de sistemes. Les versions més antigues dels sistemes operatius utilitzen aquest sistema.

Sota el directori /dev hi ha els fitxers que fan referència a diferents dispositius del sistema. Per exemple, amb la llibreria libata:

- **/dev/sda:** fa referència al dispositiu IDE del canal primari en disposició Master.
- **/dev/sdb:** fa referència al dispositiu IDE del canal primari en disposició Slave.
- **/dev/sdc:** fa referència al dispositiu IDE del canal secundari en disposició Master.
- **/dev/sdd:** fa referència al dispositiu IDE del canal secundari en disposició Slave.

Com ja sabem, en els sistemes GNU/Linux es permet un màxim de quatre particions primàries per dispositiu. Si voleu fer anar més de quatre particions, us caldrà crear particions lògiques. Cada partició es distingirà per un fitxer de dispositiu associat. La regla per fer la distinció és senzilla: les particions s'identifiquen amb el sufix del dispositiu lògic i un número, afegit al final, que indica l'ordre que ocupa la partició dins del disc, segons sigui primària o lògica.

Eines per a la gestió de particions. GParted

Les aplicacions utilitzades per a la gestió de les particions en els suports d'emmagatzematge són conegudes com a *gestors* o *editors de particions*. Aquestes aplicacions us permetran, entre altres tasques, crear particions, esborrar-les, redimensionar-les, copiar-les i donar-los format.

Hi ha moltes aplicacions en el mercat. Són molt variades. Algunes són lliures i d'altres són de propietat.

A continuació, us explicarem el funcionament del gestor de particions GParted, una aplicació que porta incorporat el LiveCD de la Ubuntu.

GParted

El GParted és el gestor de particions de l'entorn d'escriptori **GNOME**. Utilitzem aquest programa per **crear, esborrar, formatar, copiar i redimensionar particions**. Aquestes funcions permeten crear fàcilment espai per a nous sistemes operatius, a més d'estruir i reorganitzar l'ús del disc dur.

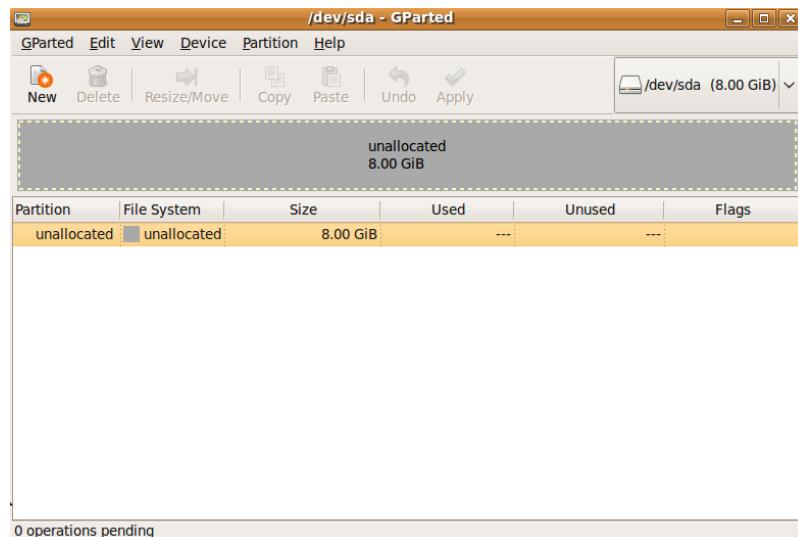
El primer pas que heu de seguir per fer servir el GParted és arrencar la màquina des del LiveCD de la Ubuntu. A continuació, apareixerà un menú que us permetrà escollir l'idioma de la interfície. Una vegada tingueu la interfície en el vostre

idioma, seleccioneu l'opció ***Proveu l'Ubuntu sense fer cap canvi en el vostre ordinador.***

Un cop l'escriptori s'ha carregat amb el **LiveCD**, aneu al menú **System > Administration > Partition Editor**.

Una vegada seleccionada l'opció, se us obrirà l'aplicació i podreu veure la distribució de les particions del vostre disc dur. Vegeu la figura 1.2 de l'exemple sense particionar.

FIGURA 1.2. Visió de l'eina Gparted amb un disc dur sense particionar

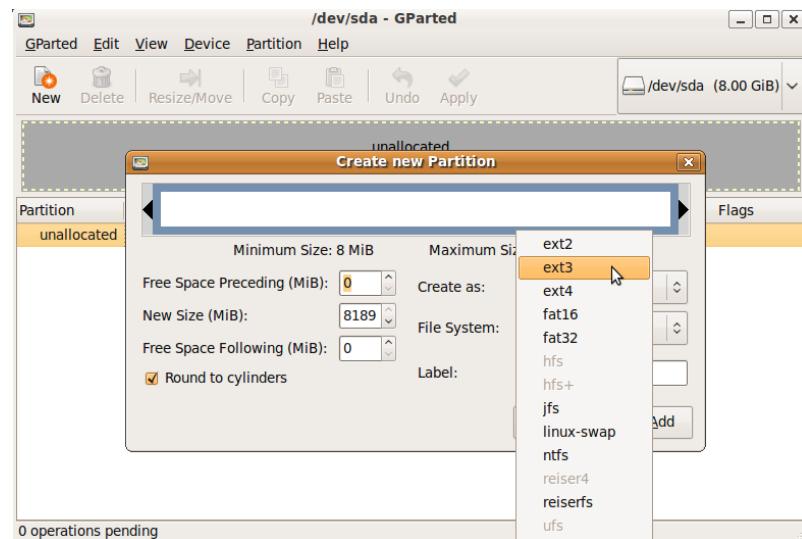


Per crear noves particions en l'espai sense partir del disc dur, seleccioneu la partició -en aquest cas *unallocated*-, i premeu el botó **New**. Us apareixerà el quadre que podeu veure en la figura 1.3.

En prémer el botó **New**, se us obrirà el quadre de diàleg per a la creació de la nova partició. En aquest quadre podreu seleccionar, entre d'altres opcions, **l'espai buit precedent a la partició, l'espai que ocuparà la partició i l'espai buit posterior a la partició que heu de crear**. A més, podreu escollir el **tipus de la nova partició**, primària o estesa. Si seleccioneu la partició estesa, l'haureu de crear prèviament per poder crear particions lògiques a dins.

Per comprovar tots els formats i les accions suportades pel GParted, seleccioneu l'acció *File System Support* del menú *View*.

En seleccionar una partició primària també podeu escollir el **format d'arxius** que voleu donar a aquesta partició. En el menú apareix una llista desplegable dels tipus suportats per GParted. L'opció **Label** indica el nom de l'**etiqueta del volum**. L'opció **Round to cylinders** permet arrodonir les dimensions de la partició en la **grandària del cilindre** per tal d'optimitzar l'espai en el disc. Si desabilitieu la casella anterior, establireu la grandària de la partició en Mbs.

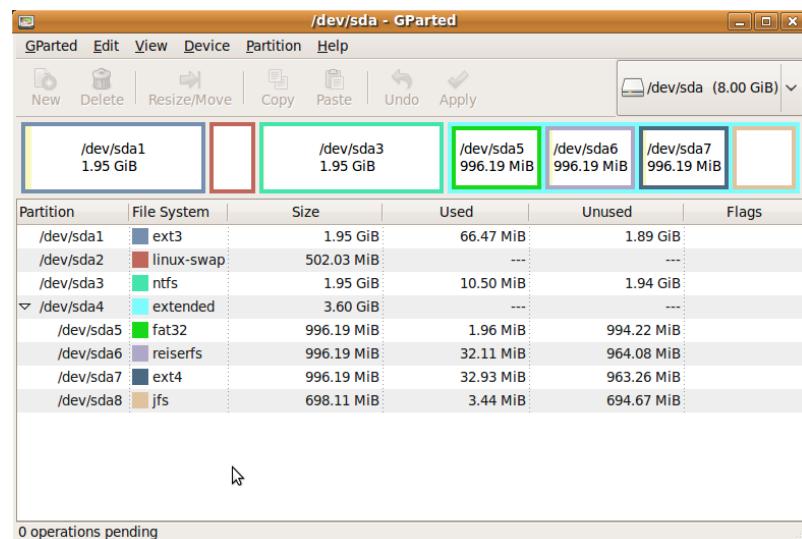
FIGURA 1.3. Quadre que mostra els sistemes de fitxers suportats per Gparted

Una vegada especificats els paràmetres de configuració, premeu el botó **Add**.

Seguint amb l'exemple, podeu crear tres particions primàries: la primera al començament de l'espai de particions de 2 Gb amb format ext3, a continuació, una partició de tipus linux-swap d'1 Gb, i, finalment, una altra partició de tipus ntfs de 2 Gb de grandària. També podeu crear una partició estesa de 4 Gb amb quatre particions lògiques d'1 Gb cadascuna i de tipus ext4.

En prémer el botó **Add** no es creen directament les particions en el disc dur, sinó que encara podeu modificar o esborrar les particions i continuar fent-ne de noves. Els canvis no tindran efecte en el disc dur fins que no premeu el botó **Apply**.

Apliqueu els canvis i, en finalitzar el procés, tindreu creades les particions que voleu en el disc dur de l'equip. La figura 1.4 us ho mostra.

FIGURA 1.4. Particions de diferents grandàries i sistemes de fitxers amb Gparted

Feu sempre les pràctiques en màquines virtuals o en equips no susceptibles de perdre informació important.

Les opcions d'esborrar, redimensionar i copiar particions es poden aplicar si se selecciona la partició implicada i s'escull l'opció pertinent en el menú **Partition**.

Tingueu sempre en compte que si una partició està muntada té un cadenat al costat-, l'haureu de desmontar per poder-hi fer les accions que vulgueu. Per modificar la partició d'intercanvi també l'haureu de desactivar.

1.6.3 Tipus d'instal·lacions

Els diferents tipus d'instal·lacions depenen dels sistemes d'instal·lació de què disposem.

El sistema d'instal·lació constitueix el conjunt de recursos o dispositius que s'utilitzaran per fer la instal·lació del sistema.

A l'hora d'escoldir un sistema i un tipus d'instal·lació, heu de considerar diversos factors, com ara quantes instal·lacions fareu, quantes instal·lacions diferents fareu i de quina infraestructura disposeu.

Actualment, gairebé totes les distribucions ofereixen diverses possibilitats per instal·lar-les. A més, és possible, en general, combinar diferents sistemes d'instal·lació.

Instal·lació mitjançant CD/DVD

La instal·lació mitjançant un CD o un DVD és la més comuna i la que utilitzarem si volem instal·lar el sistema operatiu en un nombre reduït d'equips.

L'element necessari per fer aquest tipus d'instal·lació és el CD o el DVD de la distribució GNU/Linux que volem instal·lar.

Cada distribució us proporciona una sèrie de CD o DVD amb unes característiques concretes. Per exemple, CD o DVD d'instal·lació de diferents versions (server, desktop), LiveCD, CD per a la configuració de la instal·lació en xarxa, CD de rescat o CD de dipòsits, entre altres.

Per veure el procés d'instal·lació d'un sistema operatiu amb CD aneu directament a l'apartat "Instal·lació Ubuntu".

Podeu aconseguir aquests CD i DVD per diverses vies, com ara revistes d'informàtica, botigues d'ordinadors o distribuïdors. També podeu descarregar la imatge (.iso) d'Internet i copiar-la en un suport. En algunes distribucions, com en el cas de la Ubuntu, fins i tot les podeu demanar per correu en la pàgina web de la distribució.

Una vegada tingueu els CD o els DVD, haureu de seguir una sèrie de passos per instal·lar el sistema operatiu a l'equip. (Abans d'iniciar la instal·lació, però, convé que prepareu i configureu, amb les particions necessàries, el disc dur en què instal·lareu el sistema operatiu.) Els passos a seguir són els següents:

1. Configurar l'arrencada des del lector de CD/DVD en el BIOS de l'equip.

L'entrada al BIOS i a la configuració d'aquest sistema depèn del tipus de màquina.

2. Inserir el CD/DVD al lector i engegar l'equip per tal que l'arrencada del sistema operatiu comenci des del CD/DVD.
3. Seguir l'assistent de configuració en cada cas.

Instal·lació per mitjà de la xarxa

La instal·lació per mitjà de la xarxa és la que fareu servir si voleu instal·lar un sistema operatiu en un nombre elevat d'equips. Aquest tipus d'instal·lació requereix una determinada infraestructura.

Primer de tot, heu de disposar d'una targeta de xarxa PXE per poder arrencar i instal·lar el sistema operatiu des de la xarxa. A més, heu de tenir el BIOS configurat per iniciar l'arrencada en xarxa. Si no, heu de tenir els CD/DVD o disquets de configuració de la instal·lació en xarxa del sistema operatiu. També necessiteu un servidor en la xarxa des del qual es pugui carregar el sistema.

Targeta PXE

Una targeta PXE és aquella que permet funcionar amb *preboot execution environment* o entorn d'execució de prearrencada, un entorn per arrencar i instal·lar sistemes operatius en ordinadors mitjançant una xarxa, de manera independent dels dispositius d'emmagatzematge de dades disponibles o dels sistemes operatius instal·lats.

En parlar de xarxa, heu de considerar dues possibilitats:

Dipòsit

Un *dipòsit* és una base de dades centralitzada en què s'emmagatzema i es manté informació digital, habitualment bases de dades o arxius informàtics.

1. Internet: teniu la possibilitat d'instal·lar el sistema operatiu directament des d'Internet.

La majoria de sistemes GNU/Linux estan preparats per descarregar i actualitzar els seus paquets, fins i tot el sistema operatiu, per mitjà dels dipòsits que podem trobar a Internet. No és tan comú instal·lar la totalitat del sistema operatiu per mitjà d'Internet. Encara que aquesta opció no és gaire recomanable, si no es disposa d'una connexió amb una taxa de transferència elevada, comporta molts avantatges respecte a una instal·lació que es faci mitjançant CD, ja que permet instal·lar les últimes versions disponibles dels paquets.

Algunes distribucions, com la Ubuntu, la Fedora o la Suse, proporcionen CD (MinimalCD) que instal·len els paquets necessaris per descarregar el sistema base des dels dipòsits.

2. Xarxa local: la instal·lació del sistema operatiu es fa per mitjà dels dipòsits o les imatges que hi ha en la LAN.

La instal·lació del sistema per la xarxa local es pot fer de maneres diferents. Una de les més comunes és utilitzar un servidor NFS, com DRBL juntament amb eines com Clonezilla o Fog que ens permeten generar i gestionar les imatges que cal instal·lar, encara que també es poden utilitzar CD/DVD d'instal·lació o rèpliques (*mirrors*) de dipòsits disponibles a partir de la xarxa local.

Per tal de fer la instal·lació d'aquesta manera, haureu de configurar el servidor, tenir una imatge del sistema operatiu allotjada en els recursos que comparteix i

configurar el client perquè comenci la instal·lació des de la xarxa.

Instal·lació mitjançant la clonació d'un disc dur

La instal·lació d'un o diversos sistemes mitjançant la clonació d'un disc dur és un bon mecanisme per fer còpies de seguretat o instal·lacions massives. Aquesta instal·lació us permet copiar un sistema operatiu instal·lat en un disc dur o en una partició del disc a un altre disc dur. Si els discs durs estan ubicats en diferents màquines, convé que totes dues tinguin un maquinari similar perquè la instal·lació funcioni correctament, sobretot en el Windows.

Per fer la clonació o la partició del disc dur que teniu instal·lat en el sistema operatiu, haureu de fer servir programari específic. Podeu utilitzar diversos programes de codi obert, com ara **Clonezilla** i **Partimatge**. Com a recurs dels sistemes operatius GNU/Linux, és important mencionar l'ordre de sistema **dd**.

La clonació es pot fer amb els discs connectats en el mateix equip o per mitjà de la xarxa.

Un mètode que ens permet combinar la instal·lació per mitjà de xarxa i la clonació, i crear un sistema d'instal·lació remota és la utilització conjunta d'eines com **Clonezilla** i un **servidor DRBL** o l'eina **fog**.

Altres instal·lacions

Podeu instal·lar un sistema operatiu des d'altres mitjans o suports informàtics com, per exemple, els següents:

- **USB:** moltes distribucions GNU/Linux incorporen utilitats que permeten carregar el sistema operatiu des del port USB. Aquest mètode té la limitació que només pot arrencar en una màquina la placa base de la qual suporti l'arrencada des d'un mitjà USB.
- **Live CD/DVD personalitzat:** hi ha eines com Remastersys, Ubuntu Customization Kit o Reconstructor que permeten a qualsevol usuari crear fàcilment un Live CD/DVD personalitzat d'una instal·lació existent, que podeu utilitzar com a còpia de seguretat o per fer la instal·lació en una altra màquina.
- **Màquines virtuals:** una màquina virtual és un programari que emula un ordinador dins d'un altre ordinador. L'ús més estès de les màquines virtuals és la prova de sistemes operatius i la interacció entre ells per mitjà de la xarxa. Tot i que la instal·lació del sistema operatiu en una màquina virtual es farà d'alguna de les maneres que hem comentat abans, hem cregut convenient destacar el concepte de *màquina virtual* i esmentar-ne la importància. Entre les aplicacions de virtualització que hi ha, cal destacar VMware, Quemu i l'aplicació de codi obert VirtualBox.

Com a resum de l'apartat, cal dir que el grau d'interacció de l'usuari que requereix una instal·lació depèn del sistema i del tipus d'instal·lació que es faci. Cada sistema té avantatges i inconvenients. Una instal·lació estàndard ens permet anar pas a pas, cosa que és extremadament útil per adequar el sistema a les nostres necessitats i possibilitats, mentre que un sistema d'instal·lació totalment automàtic requereix unes infraestructures i uns coneixements més avançats. Per tant, constitueix una inversió, tant de temps com d'infraestructura, que només es justifica si el nombre de sistemes a instal·lar és molt gran.

Per exemple, es podria plantejar la implementació d'aquest tipus d'instal·lació en un departament en què hi hagués ordinadors destinats a ús personal i ordinadors destinats a servidors que es dediquessin a fer còpies de seguretat (*backups*), i on el nombre d'ordinadors augmentés sovint.

El fet que l'entorn gràfic no estigui instal·lat per defecte en la versió Server de l'Ubuntu, la dota de més seguretat, ja que com menys serveis carregats hi hagi, menys possibilitats hi haurà que es produueixin errades.

1.6.4 Instal·lació Ubuntu

Un cop assolits els coneixements sobre el procés d'instal·lació d'alguna versió orientada a estacions de treball o equips client d'algun sistema operatiu GNU/Linux, podeu iniciar el procés d'instal·lació de la versió Server del sistema operatiu GNU/Linux Ubuntu.

L'Ubuntu Server està orientat i optimitzat per treballar en servidors dedicats, sense entorn gràfic. Les diferències principals que hi ha entre les versions Desktop i Server se centren en algunes funcionalitats del nucli del sistema i en els serveis que tenen instal·lats. Totes dues versions, però, poden fer de servidor o d'estació de treball indistintament.

Instal·lació de la Ubuntu Server Edition

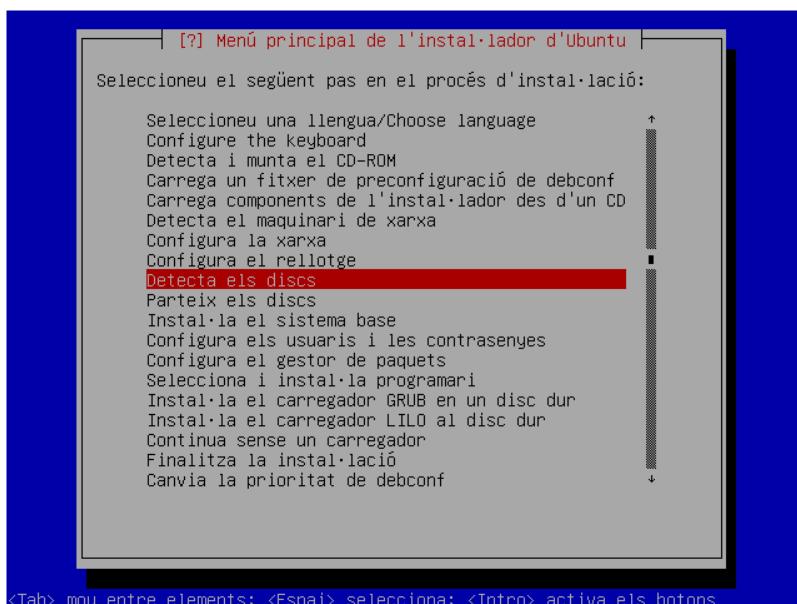
En la instal·lació heu d'utilitzar com a suport el CD de la Ubuntu 9.04 Server Edition. El podem aconseguir de manera senzilla descarregant l'arxiu d'imatge (.iso) de la pàgina d'Ubuntu. Des de la pàgina d'Ubuntu s'expliquen totes les maneres que hi ha d'aconseguir un CD/DVD de la distribució.

El primer pas que haureu de fer és configurar el BIOS de l'equip en què instal·larem el sistema perquè arrenqui des del lector de CD. Una vegada configurat, cal que inserim el CD en el lector i arrenquem el sistema. Després d'escolhir l'idioma de la interfície, ens apareixerà la pantalla següent (vegeu la figura 1.5).

FIGURA 1.5. Pantalla d'inici del procés d'instal·lació d'Ubuntu Server

Per instal·lar el sistema operatiu, seleccionem l'opció ***Instal·la l'Ubuntu per a un servidor***. A continuació, apareixerà un menú de text que ens guiarà durant tota la instal·lació del sistema servidor. L'ús d'aquest menú és molt senzill: per moure'ns per les opcions utilitzarem les tecles del cursor o la tabulació i per escollir una opció premerem el botó *Enter*. La primera pantalla que apareix ens permet escollir el país en què es troba l'equip. Aleshores seleccionarem el país corresponent i continuarem la instal·lació.

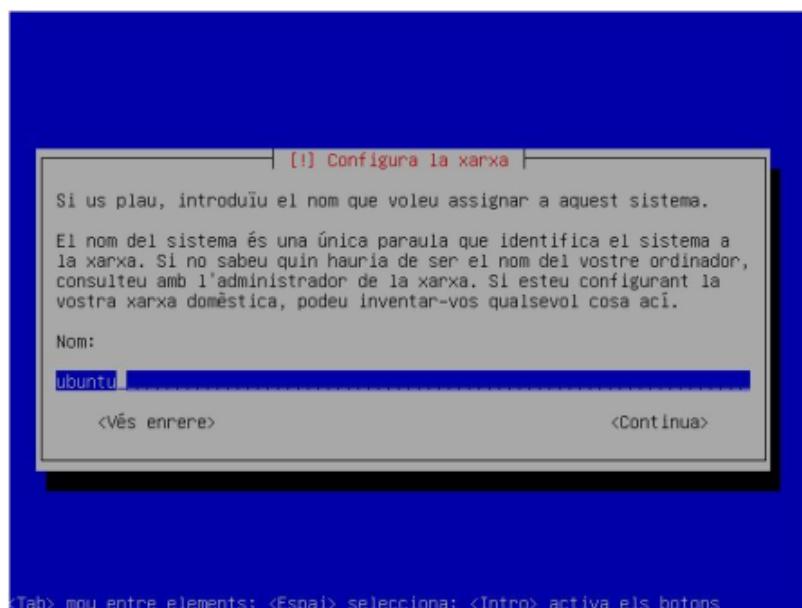
El pas següent ens dóna dues opcions: permetre que el sistema detecti la configuració del nostre teclat o bé triar una configuració de la llista que hi ha. Escolliu l'última opció, que és la més senzilla. En la llista, cal que escollim el país corresponent i, dins el país, la configuració correcta del teclat.

FIGURA 1.6. Menú principal de l'instal·lador d'Ubuntu Server

Si en qualsevol moment de la instal·lació volem tornar enrere, podrem escollir el pas al qual volem accedir a partir d'una llista com la que es mostra en la figura 1.6.

Després d'escollir la configuració del teclat, apareixerà aquesta pantalla (vegeu la figura 1.7).

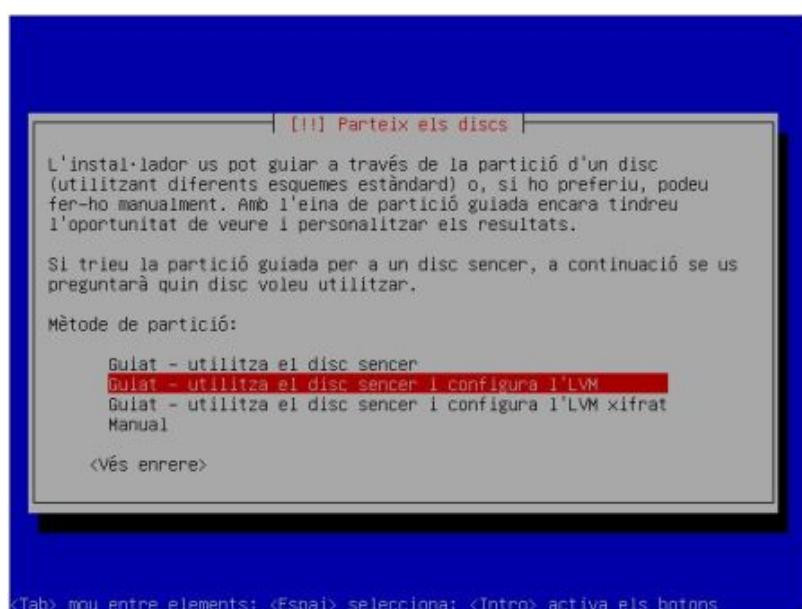
FIGURA 1.7. Pantalla on especificuem el nom de la màquina a la xarxa



Cal que especifiquem el nom de la nostra màquina en la xarxa.

A continuació, establím el fus horari del país en què es troba l'equip. Després ens apareixerà la pantalla següent (vegeu la figura 1.8).

FIGURA 1.8. Menú de selecció del mètode de partició del disc

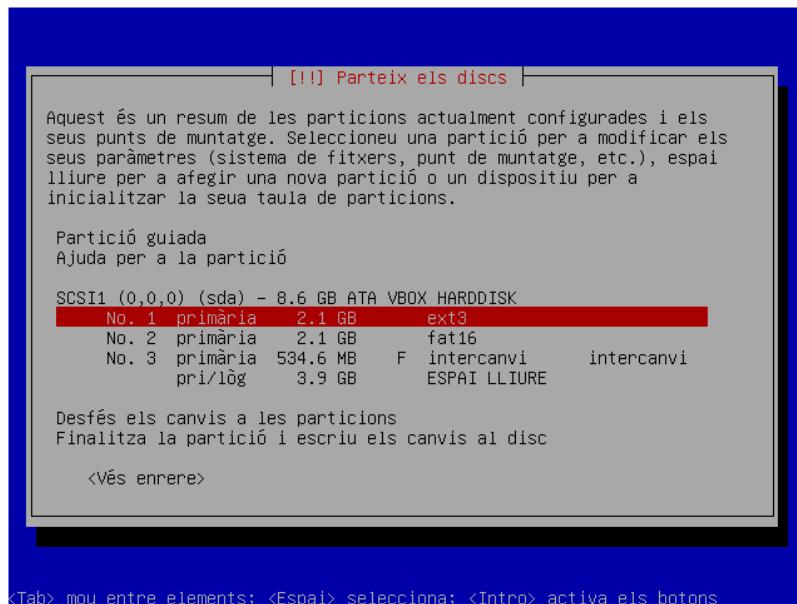


En aquesta pantalla podem seleccionar el mètode de partició que volem utilitzar.

Podem escollir entre quatre mètodes.

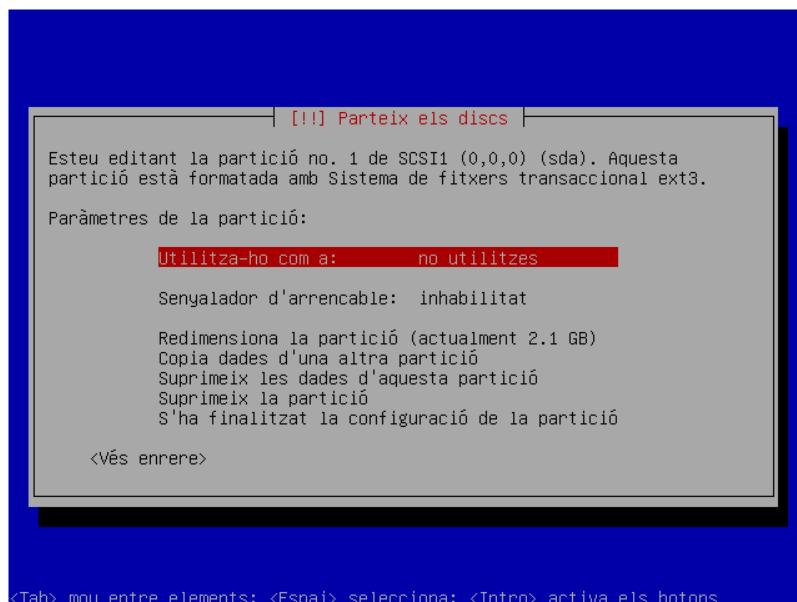
Manual: ens permetrà crear i formatar les particions en els discos durs del sistema. Si ja tenim particions creades en el suport d'emmagatzematge, haurem d'escollir aquesta opció i muntar els diferents directoris del sistema en les particions que vulguem. Així, en seleccionar aquesta opció, apareixerà una pantalla similar a la de la figura 1.9.

FIGURA 1.9. Resum de particions configurades i els seus punts de muntatge



Hem de seleccionar la partició en què volem muntar cada directori prement la tecla *Intro*. Veurem un menú com el següent (vegeu la figura 1.10).

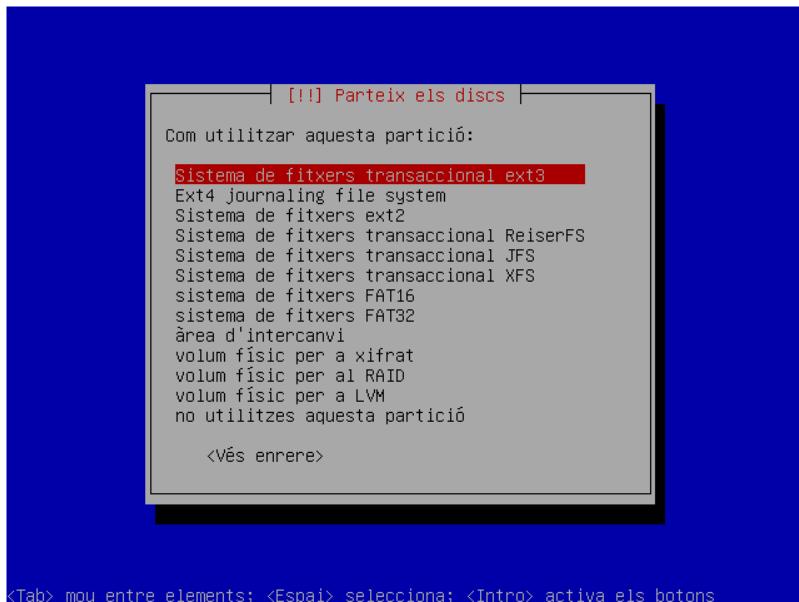
FIGURA 1.10. Pantalla d'edició de les opcions de cada partició



En el menú anterior podem anar seleccionant cada camp de la partició i especificant-ne els valors. Per exemple, en el primer camp hem d'especificar amb

quin sistema de fitxers volem utilitzar la partició seleccionada. Si premem *Intro*, ens mostrarà els sistemes de fitxers següents (vegeu la figura 1.11).

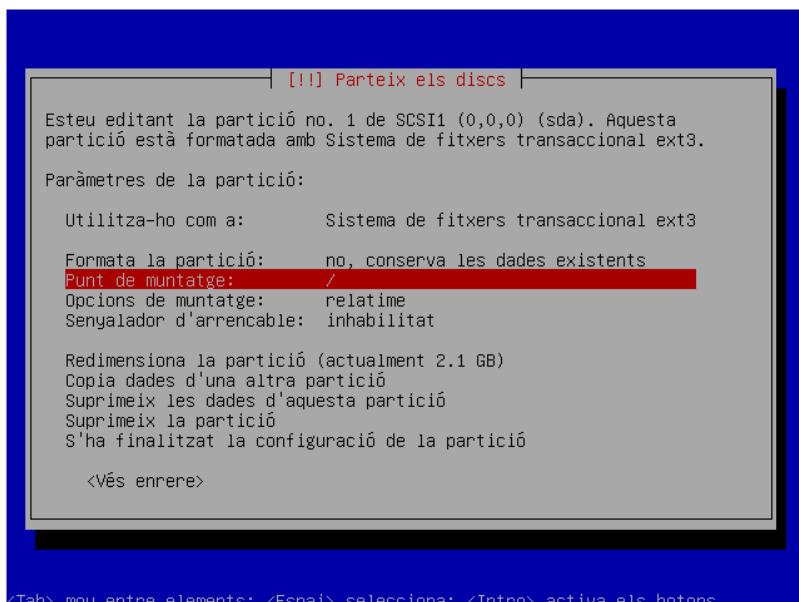
FIGURA 1.11. Pantalla de selecció del tipus de sistema de fitxers per a la partició



Si la partició està formatada, escollirem el sistema de fitxers en què hem fet la formatació. Si no està formatada, hi podem donar format mitjançant l'opció *Formata la partició*.

Tot seguit, cal que determinem quin directori muntem en la partició, **com a mínim hem de determinar una partició per al directori arrel del sistema /**. Seleccionarem, tal com veiem en la figura 1.12, el camp *Punt de muntatge* per especificar el directori que volem muntar en la partició. Hem de seguir la seqüència anterior per a cadascuna de les particions en què vulguem muntar un sistema de directoris.

FIGURA 1.12. Pantalla d'edició de les opcions de la partició



També podem especificar que una partició es pugui arrencar si habilitem l'opció *Senyalador d'arrencable*. Normalment farem això si hem muntat el directori /boot en la partició.

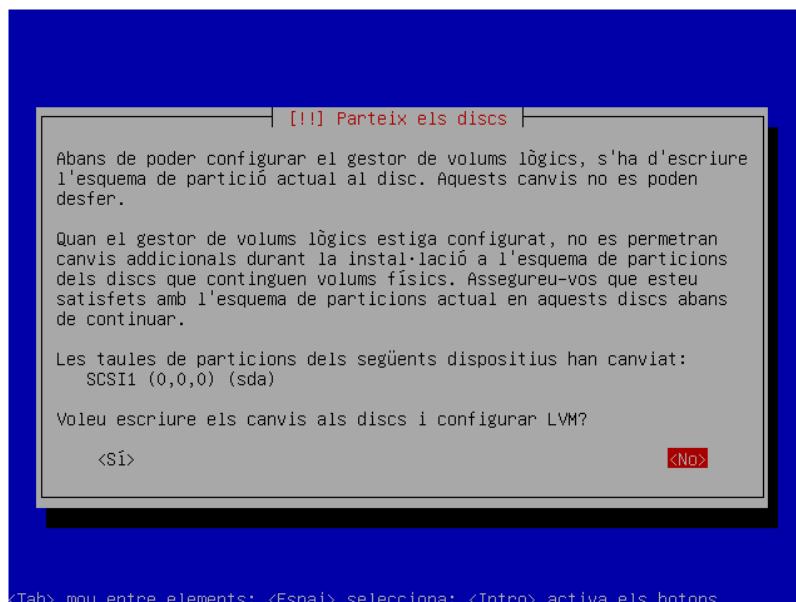
Una vegada finalitzada la configuració de la partició, continuem amb l'opció **S'ha finalitzat la configuració de la partició**. En funció de les opcions de muntatge de directoris, se'ns advertirà dels canvis que es duran a terme i se'ns preguntarà si volem continuar. Hem de llegir atentament totes les pantalles d'avertència que apareixen per evitar fer malbé les dades del suport d'emmagatzematge, si n'hi ha.

Els altres mètodes d'instal·lació que podem utilitzar són els següents:

- **Guia – utilitza el disc sencer**, instal·larà el sistema en tot el disc en una única partició sense respectar les particions que ja hi ha.
- **Guia – utilitza el disc sencer i configura l'LVM xifrat**, instal·larà el sistema en tot el disc en una única partició sense respectar les particions que ja hi ha i ens configurarà el gestor de volums lògics xifrat, que xifrarà la informació i ens demanarà una contrasenya d'accés.
- **Guia – utilitza el disc sencer i configura l'LVM**, instal·larà el sistema en tot el disc en una única partició sense respectar les particions que ja hi ha i ens configurarà el gestor de volums lògics.

El gestor o administrador de volums lògics LVM permet, entre altres, crear unitats lògiques a partir d'un o més discs durs, redimensionar particions en calent i assignar els noms que vulguem als volums per a gestionar-los. Aquests comportaments resulten molt útils a un servidor en explotació.

FIGURA 1.13. Pantalla de confirmació dels canvis



Si en comptes d'escollir la instal·lació manual escollim aquesta última opció, ens apareix una pantalla que permet seleccionar el disc dur que volem partir, és a dir,

Taula de particions

La taula de particions està allotjada a partir del byte 446 de l'MBR (*master boot record*) i ocupa 64 bytes. Conté 4 registres de 16 bytes que defineixen les particions primàries. En aquests registres s'emmagatzema tota la informació bàsica sobre la partió: si es pot arrencar o no, el format, la grandària i el sector d'inici

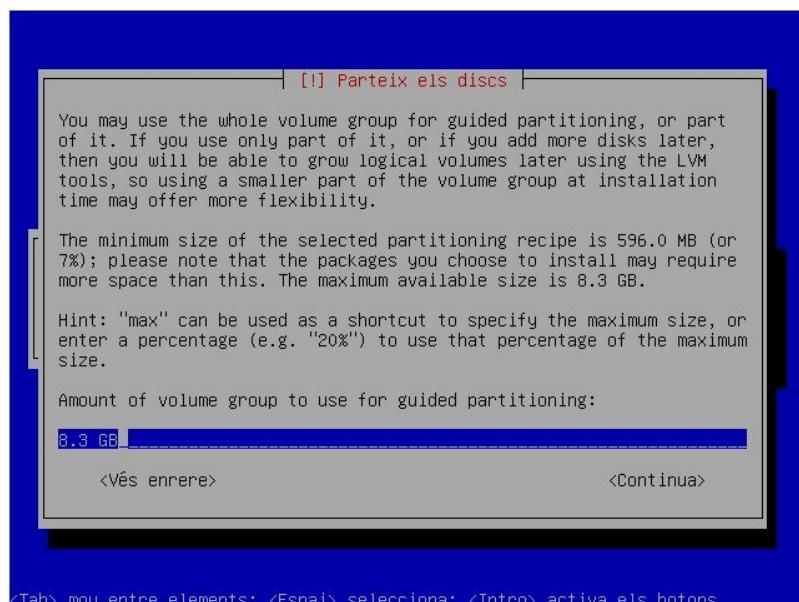
el disc en què volem instal·lar el sistema operatiu. Una vegada seleccionat el disc, ens mostra la pantalla següent (vegeu la figura 1.13).

En aquest pas de la instal·lació ens adverteix que els canvis que s'aplicaran no es podran desfer, ja que se sobreescrivrà la taula de particions del disc seleccionat. Hem d'estar segurs que les particions que tenim són les que volem. Si és així, escollim Sí.

Si tornem enrere, podem dimensionar la grandària de les particions.

Quan ens pregunti si volem escriure els canvis en el disc i configurar l'LVM, cal que cliquem a Sí. Apareixerà la pantalla següent (vegeu la figura 1.14).

FIGURA 1.14. Pantalla on establím la grandària del volum que volem gestionar amb LVM

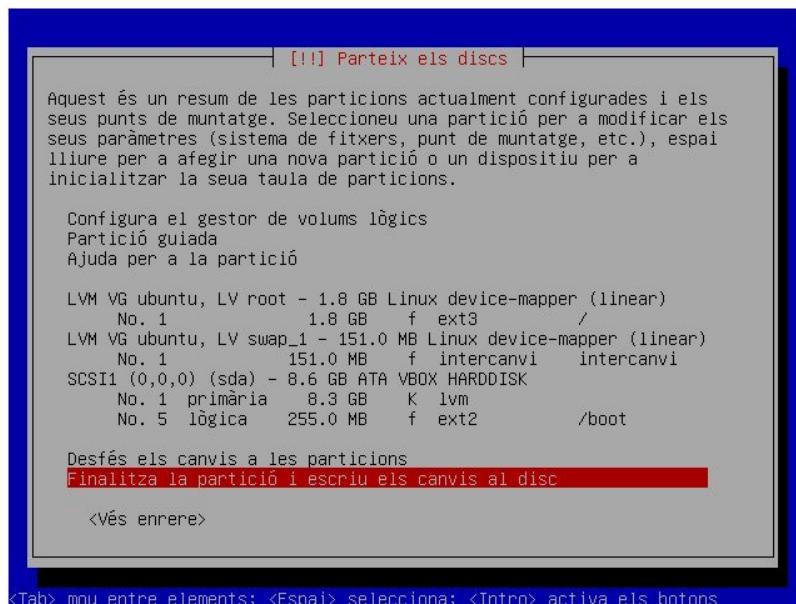


Establir la grandària del volum que volem gestionar amb l'LVM. Si la grandària és petita ens permetrà modificar-la mitjançant les eines de l'LVM i ens oferirà més flexibilitat.

Per defecte, ens crearà una partió primària en format ext3 i una partió d'intercanvi. Les dues particions ocuparan la grandària que hem determinat en la pantalla anterior. En la partió ext3 es muntarà l'arrel del sistema. En un partió lògica formatada en ext2 fora del volum, ens muntarà el directori /boot. La partió que contingui /boot no podrà formar part d'un volum lògic, ja que els carregadors d'arrancada no solen suportar aquest sistema de fitxers (aquesta configuració la podem modificar posteriorment).

Seguidament ens mostra el resum de les particions que farà i els punts de muntatge. Si hi estem d'acord, cal que fem clic a l'opció **Finalitza la partió i escriu els canvis al disc** (vegeu la figura 1.15). A continuació, apareixerà una pantalla de confirmació. Si confirmem la pantalla anterior començarà a instal·lar el sistema operatiu.

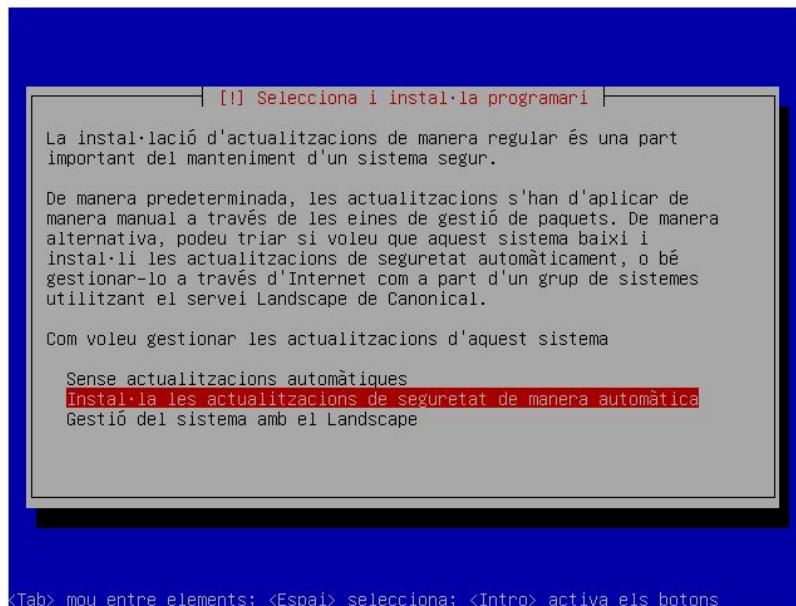
FIGURA 1.15. Pantalla de resum on podem finalitzar el procés de partició i escriure els canvis



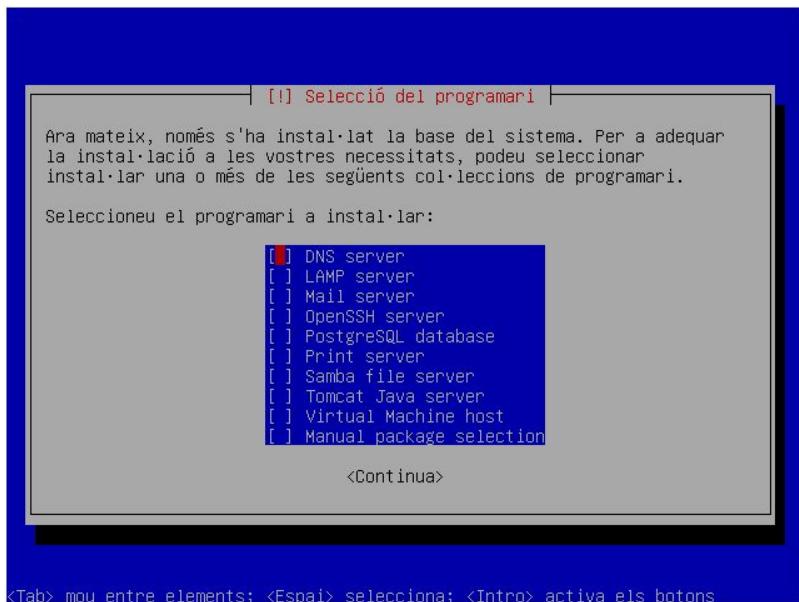
Tot seguit apareixeran més pantalles en què podrem configurar el nom i la contrasenya de l'usuari per defecte. També podrem decidir si utilitzem un servidor intermediari (*proxy*) per connectar l'equip a la xarxa:

En les pantalles següents, com la que es mostra en la figura 1.16, també podem escollir la manera de gestionar les actualitzacions.

FIGURA 1.16. Menú que permet especificar la gestió de les actualitzacions



Fins i tot podem determinar quins tipus de serveis i paquets volem instal·lar en el nostre servidor (eina tasksel). En funció dels serveis que instal·lem, ens apareixeran algunes pantalles més que ens permetran configurar-los (vegeu la figura 1.17).

FIGURA 1.17. Eina tasksel

Una vegada configurats els serveis escollits continuará la instal·lació.

Finalment, apareixerà una pantalla per escollir el punt en què volem instal·lar el gestor d'arrancada LILO. Si el volem utilitzar com a gestor d'arrencada predeterminat, l'instal·larem en el registre mestre d'arrencada. En canvi, si volem fer servir un altre gestor d'arrencada, com ara el GRUB, instal·larem el LILO en una partició d'Ubuntu nova. Posteriorment, haurem d'instal·lar i configurar el GRUB en el sistema.

Quan acabi el procés d'instal·lació, per comprovar que tot ha anat bé, traurem el CD i reiniciarem l'equip. En iniciar el sistema apareixerà una pantalla d'inici de sessió (*login*) com la que es mostra a continuació en la figura 1.18. Ens demanarà que introduïm el nom i la contrasenya de l'usuari per defecte. Així doncs, cal que comprovem que hi tenim accés i que els paràmetres que hem configurat en la instal·lació són correctes.

FIGURA 1.18. Pantalla d'inici del sistema Ubuntu Server una vegada instal·lat

```
Ubuntu 9.04 ubuntu tty1
ubuntu login: ioc
Password:
Last login: Sat Nov 14 12:55:34 CET 2009 on tty1
Linux ubuntu 2.6.28-11-generic #42-Ubuntu SMP Fri Apr 17 01:57:59 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ioc@ubuntu:~$ _
```

2. Configuració i monitoratge en sistemes GNU/Linux

Una vegada instal·lat el sistema operatiu, l'heu de poder configurar i actualitzar segons les vostres necessitats. En el procés de configuració del sistema heu de saber instal·lar i desinstal·lar els paquets de les aplicacions, els serveis i les utilitats que calguin. També heu de saber com configurar els paràmetres de xarxa perquè l'equip tingui accés a l'exterior. Per altra banda, és interessant conèixer el procés d'aturada i arrencada del sistema i les eines per configurar tasques automatitzades.

Per tal de poder configurar el sistema operatiu, heu d'aprendre a comunicar-vos-hi mitjançant les ordres bàsiques relacionades amb les diverses parts del sistema. Heu de conèixer, entendre i modificar els fitxers de configuració del sistema més utilitzats, els quals ens permeten determinar els paràmetres que especificaran el funcionament del sistema operatiu.

2.1 Ordres i fitxers bàsics de configuració GNU/Linux

En un sistema operatiu GNU/Linux amb entorn gràfic, com ara l'Ubuntu Desktop Edition, moltes de les ordres que transmeteu al sistema es poden fer mitjançant l'entorn d'escriptori amb botons, finestres, quadres de diàleg i editors sofisticats de text. Les eines gràfiques (GUI) ofereixen una estètica millorada i una major simplificació. Per això consumeixen més recursos computacionals i, en general, redueixen la funcionalitat assolible. Tanmateix, no sempre us trobareu amb sistemes amb l'entorn gràfic instal·lat, com en el cas dels servidors dedicats. També pot ser que l'entorn gràfic no funcioni per diversos motius. En qualsevol d'aquests casos us heu de poder comunicar amb el sistema per mitjà de l'intèrpret d'ordres (*shell*).

Com a tècnics, heu de poder configurar el sistema operatiu en qualsevol situació. La configuració per ordres és més seria, robusta i fiable que la configuració gràfica. Al cap i a la fi, les eines gràfiques fan servir *scripts* que interpreta algun intèrpret d'ordres.

2.1.1 L'intèrpret d'ordres

Per tal de poder treure el màxim partit al sistema, gestionar-lo, configurar-lo i fer guions (*scripts*) que ens permetin automatitzar tasques, hem de tenir clar en què consisteix i com s'utilitza una de les eines més potents que ens proporciona el sistema operatiu, l'intèrpret d'ordres. Així doncs, podríem definir l'intèrpret d'ordres o *shell* (embolcall) de la manera següent:

L'**intèrpret d'ordres** és un programa informàtic que actua d'interfície entre l'usuari i el sistema operatiu. Té la finalitat d'establir la comunicació entre tots dos. Per fer-ho, interpreta i executa les ordres que l'usuari escriu des del teclat i, a continuació, torna la resposta per pantalla.

L'intèrpret d'ordres estàndard és el Bash, però n'hi ha molts més, com sh, csh, ksh, dash.

Prompt

Es diu *prompt* al caràcter o conjunt de caràcters que es mostren en una línia de comandes per indicar que el sistema està a l'espera d'ordres. El prompt pot variar depenent de l'intèrpret de comandes i sol ser configurable.

Per indicar que espera una instrucció, l'intèrpret d'ordres presenta un *prompt* al començament de la línia. Segons la configuració predefinida per l'editor de la distribució del GNU/Linux que utilitzem, aquest *prompt* pot tenir diferents aspectes.

El caràcter final d'aquests *prompts* indica el tipus d'usuari connectat:

- \$: usuari sense drets especials.
- #: administrador amb tots els drets necessaris per a la configuració i el manteniment del sistema.

Per defecte, la versió Ubuntu Server Edition treballa sense entorn gràfic i, una vegada carregat el sistema, us hi haureu de comunicar mitjançant la línia d'ordres. En la versió Ubuntu Desktop Edition hi ha un emulador de terminal amb la línia d'ordres en la ubicació: *Aplicacions > Accessoris > Terminal*. Per accedir-hi i obrir diferents sessions de terminal també podeu pulsar la combinació de tecles ***Ctrl + Alt + F1 i, tot seguit, F6***, amb les quals desapareixerà l'entorn gràfic. Per tal de carregar la sessió en què funciona l'entorn gràfic polem ***Ctrl + Alt + F7***.

L'arxiu /etc/shells mostra els intèrprets d'ordres coneguts en un sistema Linux.

Sense cap mena de dubte, una de les ajudes més utilitzades i que més facilita l'ús del terminal és l'ajuda en l'acabament d'ordres. La majoria d'intèrprets d'ordres moderns proporciona aquesta ajuda que consisteix a finalitzar ordres que estan escrites d'una manera parcial.

És important tenir clara la diferència entre l'intèrpret d'ordres i els terminals. Sovint s'utilitzen els termes *línia d'ordres*, *terminal*, *shell*, *intèrpret de línia d'ordres*, *consola* com si fossin la mateixa cosa. El terminal és el component de maquinari (antics teletips) o el programa que executa l'intèrpret d'ordres o *shell*.

Podem dir que hi ha tres tipus de terminals:

- Teletips o teleimpressores: són el antecessors del concepte de *terminal* modern. Van aparèixer en la dècada de 1920 i els primers sistemes eren sistemes completament mecànics formats per una màquina d'escriure connectada directament a una impressora.
- Terminals virtuals: són els terminals als quals podem accedir amb la combinació de tecles Ctrl+Alt+Fx en què x és el número de terminal. La principal diferència amb els emuladors de terminal és que els terminals virtuals no s'executen dins d'un entorn gràfic X Window.

- Emuladors de terminal: són aplicacions que emulen un terminal. Normalment són aplicacions que s'executen en un entorn gràfic X Window i emulen un terminal dins de la finestra de l'aplicació.

Els emuladors de terminal són aplicacions de les quals es poden executar múltiples instàncies, cadascuna d'elles completament independent de les altres.

2.1.2 Sintaxi de les ordres

És important conèixer la sintaxi de les ordres per evitar que hi hagi gaires errors d'escriptura.

En l'expressió més simple, sense opcions ni arguments, una ordre es transmet al sistema quan se n'escriu el nom en la línia d'ordres.

1 [prompt]\$ ordre

Si s'han d'especificar **arguments**, s'afegeixen a continuació de l'ordre en la mateixa línia, separats per un espai.

1 [prompt]\$ ordre arg1 arg2

Els tractaments o la sortida d'una ordre GNU/Linux sovint es poden modificar mitjançant una opció. Hi pot haver diverses desenes d'opcions amb diferents sintaxis per a una mateixa ordre.

Si no teniu clar quines opcions té cada ordre, podeu consultar la documentació del sistema o utilitzar l'ordre man.

Principalment, hi ha dos tipus d'opcions: les **opcions monocaràcter**, heretades de l'UNIX, precedides pel caràcter **-**, i les **opcions llargues**, afegides pel projecte GNU, precedides pels caràcters **--**. Totes dues s'han d'escriure separades per un caràcter d'espai després de l'ordre i abans dels eventuals arguments.

2.1.3 Fitxers de configuració més utilitzats en el GNU/Linux

Dins dels sistemes operatius GNU/Linux hi ha moltíssims fitxers de configuració. Tenen la finalitat d'establir els paràmetres de funcionament de les aplicacions o els processos que configuren. Podeu trobar, entre altres, els fitxers de configuració següents:

- Arrencada del sistema.
- Cadascun dels serveis i aplicacions disponibles en l'equip.
- Xarxa.
- Entorn gràfic.

- Diferents dispositius de maquinari.
- Usuaris.
- Gestió de paquets i dipòsits.

En general, n'hi ha un per a cada aspecte susceptible de configuració en el sistema operatiu.

La majoria d'arxius de configuració els podeu trobar en el directori **/etc**.

A continuació, es mostren alguns dels fitxers de configuració més utilitzats o més importants per la funció que fan:

- **/etc/fstab** Aquest arxiu conté informació sobre els dispositius que es muntaran automàticament durant l'arrencada del sistema.
- **/etc/apt/sources.list** Aquest arxiu conté informació sobre els dipòsits del sistema operatiu.
- **/etc/passwd** Aquest arxiu controla l'ús d'usuaris, en contrasenyes, amb permisos i grups que pertanyen a cada usuari.
- **/boot/grub/menu.lst** Aquí hi ha la configuració del GRUB (gestor d'arrencada).
- **/etc/X11/xorg.conf** Aquest arxiu conté la configuració de l'entorn gràfic (pantalla, teclat, ratolí, targeta gràfica, etc.).
- **/etc/network/interfaces** Aquest arxiu conté les dades de configuració de la xarxa.
- **/etc/init.d/** Aquest directori conté *scripts* d'inici, arrencada i recàrrega de la majoria de serveis del sistema.

Per editar aquests arxius podeu utilitzar els editors de text que hi ha en el sistema. Entre els més utilitzats i que no depenen de l'entorn gràfic hi ha, per exemple, el Vi, el nano, el JOE, etc.

Abans de modificar un arxiu de configuració és important fer-ne una còpia de seguretat per tal de poder tornar enrere i resoldre possibles errors de configuració.

2.2 Gestió de paquets en el GNU/Linux

En els sistemes GNU/Linux els programes que instal·leu són conjunts de paquets. En instal·lar una aplicació en aquests sistemes, en realitat s'instal·len paquets de programari en el sistema operatiu.

Un *paquet de programari* és un arxiu que conté una sèrie de fitxers que es distribueixen conjuntament i permeten la instal·lació d'un programa. La raó principal de la distribució conjunta és que el funcionament de cada fitxer en complementa o en requereix uns altres.

Això pot semblar un desavantatge en principi, però el sistema de paqueteria confereix molta potència i sostenibilitat a aquests sistemes. Hi ha moltes aplicacions que simplifiquen la tasca d'instal·lació, cosa que el converteix en el sistema d'instal·lació de programari més simple i segur que hi ha actualment.

Hi ha diferents tipus de paquets en funció de si estan compilats per a una determinada distribució GNU/Linux o no. Els paquets compilats per a una distribució es coneixen com a *paquets binaris*. Els més comuns són els .rpm, que utilitzen Red Hat, Suse i derivats, i els .deb, que utilitzen Debian, Ubuntu i derivats. Els paquets no compilats es coneixen com a *paquets font*. Habitualment els trobem empaquetats i comprimits amb formats com .tar.gz o tar.bz2.

Els *paquets binaris* són paquets construïts específicament per a algun tipus d'ordinador o arquitectura.

Els *paquets font* són senzillament paquets que inclouen codi font, i generalment els pot utilitzar qualsevol tipus de màquina si el codi es compila de manera correcta.

També podeu trobar els anomenats *paquets virtuals* (*tonto* o *dummy*). Són paquets buits de contingut amb un nom genèric que proveeixen altres paquets mitjançant dependències. El paquet Apache2 n'és un exemple.

Normalment tots els paquets per a una determinada distribució els podeu trobar en els dipòsits.

Un paquet deb/rpm també es pot convertir en un altre format de paquet i viceversa utilitzant l'aplicació Alien.

Un *dipòsit* és un lloc centralitzat on s'emmagatzema i es manté informació digital, habitualment bases de dades o arxius informàtics.

Els dipòsits estan preparats per distribuir-se habitualment mitjançant una xarxa informàtica com Internet. Tanmateix, també els podem trobar en servidors de xarxa LAN (intranet) o en un mitjà físic, com un CD o un DVD. Els dipòsits poden ser d'accés públic o poden estar protegits, de manera que es necessita una autenticació prèvia per accedir-hi.

És molt més aconsellable instal·lar paquets des dels dipòsits en línia amb els gestors de paquets. Una de les raons és que els paquets dels dipòsits en línia estan actualitzats i permeten satisfer les dependències entre paquets, cosa que fa que el procés d'instal·lació sigui més senzill.

Dipòsits Ubuntu

A banda dels dipòsits en línia, Ubuntu proporciona una URL en què podeu descarregar tots els paquets oficials disponibles per a una determinada versió.

La dependència d'un paquet consisteix en el fet que un altre paquet s'ha d'instal·lar prèviament perquè el primer paquet funcioni correctament.

Els *gestors de paquets* són aplicacions que permeten gestionar paquets. Són eines que faciliten les tasques més habituals relacionades amb la gestió de paquets (instal·lació, cerques, eliminacions, etc.)

A continuació veurem un resum de la instal·lació dels diferents tipus de paquets binaris principals des de la línia d'ordres i amb entorn gràfic.

2.2.1 Gestió de paquets DEB

El sistema de paquets DEB és el sistema de paquets de programari que utilitza la distribució Debian i distribucions derivades. La seva estabilitat, el seu grau d'actualització, la seva robustesa i rapidesa a l'hora de buscar dependències han fet que sigui un dels tipus de paquets més utilitzats actualment. Altres distribucions importants que han adoptat aquest sistema de paquets són Ubuntu, Knoppix, eBox.

Els paquets *deb* són arxius ar estàndard de l'UNIX que inclouen dos arxius tar, en format gzip, bzip2 o lzma. L'un conté la informació de control (scripts de manteniment i metadades) i l'altre els fitxers que s'instal·laran en el sistema.

Normalment també inclouen un fitxer sense comprimir anomenat *debian-binary*, que conté la versió del format dels paquets Debian. Aquest tipus de paquets són originaris del sistema Debian i han estat adoptats pels seus derivats, com Ubuntu.

Entre les característiques principals hi ha les següents:

- Polítiques de qualitat estrictes abans d'alliberar versions de paquets noves.
 - Faciliten l'aplicació d'actualitzacions sense necessitat de reiniciar la màquina.
 - Permeten configurar l'aplicació en el moment de la instal·lació (debconf).
 - Permeten tasques prèvies a l'eliminació, la instal·lació i/o configuració d'un paquet.
 - Són utilitzats en totes les distribucions de la família Debian.

El programa principal utilitzat per gestionar aquest tipus de fitxers és el `dpkg`, tot i que sovint s'utilitza mitjançant els frontals (*front ends*) `apt` i `aptitude`. També podeu utilitzar interfícies gràfiques com el `Synaptic`, el `PackageKit` o el `Gdebi`.

Heu de diferenciar entre el nom del paquet i el nom del fitxer .deb que el conté. Vegeu els exemple següents:

- Nom del paquet: nmap
- Nom del fitxer: nmap_4.76-0ubuntu4_i386.deb

Aleshores, per instal·lar el paquet de l'exemple fareu el següent:

```
1 $sudo apt-get install nmap
```

Els fitxers .deb dels paquets instal·lats els podem trobar en la carpeta **/var/cache/apt/archives**

A continuació, veureu les diferents aplicacions o ordres per gestionar paquets .deb.

DPKG

Dpkg és l'abreviatura de *Debian package* i es tracta d'un equipament lògic per a la gestió dels paquets en Debian i altres distribucions GNU/Linux basades en Debian com Ubuntu. Així doncs, la seva definició seria la següent:

El programa dpkg és la base del sistema de gestió de paquets del sistema operatiu Debian GNU/Linux. S'utilitza per instal·lar i desinstal·lar els paquets .deb i també per proporcionar-ne informació sobre aquests paquets.

El dpkg és en si mateix una eina de baix nivell. Cal un frontal d'alt nivell per portar els paquets des de llocs remots o resoldre conflictes complexos en les dependències de paquets. Normalment com a usuaris utilitzarem aquestes eines d'alt nivell. El sistema Debian compta amb l'APT per fer aquesta tasca.

Entre les opcions més interessants de l'eina dpkg hi ha les següents:

Accions de consulta:

- Llista els paquets que compleixen un determinat patró: dpkg -l | -list nom_paquet_patró
- Mostra l'estatus actual d'un paquet i la metainformació del paquet: dpkg -s | -status paquet
- Mostra la llista de fitxers instal·lats: dpkg -L | -listfiles paquet
- Busca un fitxer concret dins dels paquets instal·lats: dpkg -S | -search nom_fitxer_patró
- Mostra detalls sobre un paquet instal·lat: dpkg -p | -print-avail paquet
- Mostra informació sobre un paquet desinstal·lat: dpkg -I | -info paquet

Accions de modificació del sistema (cal ser superusuari):

- Instal·la un paquet a partir d'un fitxer .deb.: `dpkg -i | -install fitxer_del_paquet`
- Torna a configurar un paquet ja instal·lat. Executa l'*script* de postinstal·lació: `dpkg -configure paquet`
- Elimina un paquet però deixa els fitxers de configuració de sistema: `dpkg -r | -remove paquet`
- Elimina un paquet i també els fitxers de configuració: `dpkg -P | -purge paquet`
- Busca fitxers instal·lats parcialment en el sistema i suggereix què fer-ne: `dpkg -C | -audit`

APT

APT és el sistema gestor de paquets d'alt nivell o *front-end* utilitzat per dpkg i, concretament, pels sistemes Debian i derivats; així doncs, podem dir de l'APT que:

L'APT no és un programa en si mateix, sinó una llibreria de funcions C++ utilitzada per altres programes de línia d'ordres, com ara apt-get o apt-cache, entre altres.

Per veure les ordres que ens proporciona l'**APT** podem utilitzar la instrucció següent: `$dpkg -L apt | grep bin`

El resultat de la qual seria el següent:

```

1 /usr/bin
2 /usr/bin/apt-cache
3 /usr/bin/apt-cdrom
4 /usr/bin/apt-config
5 /usr/bin/apt-get
6 /usr/bin/apt-key
7 /usr/bin/apt-mark

```

Abans de veure les ordres que s'utilitzen per gestionar paquets, heu de mencionar l'arxiu **/etc/apt/sources.list**. Aquest arxiu és imprescindible per al funcionament de l'APT, ja que conté la informació dels dipòsits de programari des dels quals es descarregaran els paquets .deb que volem instal·lar en el sistema.

Per defecte, està configurat per descarregar els paquets de la xarxa, però el podeu editar i canviar per descarregar-los des de CD o DVD o per modificar els dipòsits que hi ha i afegir-n'hi de nous.

Per veure tots els arxius de configuració emprareu la instrucció **dpkg -L apt | grep etc**

Per instal·lar paquets .deb utilitzarem l'ordre **sudo apt-get install nom_paquet**
Vegeu aquest exemple:

```

1 $sudo apt-get install nmap

```

Per desinstal·lar paquets .deb utilitzarem l'ordre **apt-get remove [-purge] nom_paquet**. Vegeu-ne l'exemple:

```
1 $sudo apt-get remove nmap
```

L'opcio **purge** també elimina qualsevol fitxer de configuració del paquet desinstal·lat.

Les ordres següents són igualment interessants:

- Actualitza els dipòsits. Cada cop que feu un canvi en els dipòsits o vulgueu comprovar si teniu les últimes versions dels paquets en els dipòsits, heu d'executar una actualització (update) abans: `apt-get update`
- Actualitza tots els paquets instal·lats en les últimes versions que hi ha en els dipòsits: `apt-get upgrade`
- Esborra paquets del sistema que ja no s'utilitzen, és a dir, paquets marcats com a instal·lats automàticament i que ja no es fan servir: `apt-get autoremove`
- Esborra paquets descarregats. Mitjançant aquesta ordre es guanya espai en el disc dur: `apt-get clean`

També és interessant conèixer l'ordre `apt-cache`. L'ordre `apt-cache` no manipula el sistema, però ofereix operacions per buscar i generar sortides interessants en els paquets. Les opcions més utilitzades són les següents:

- Busca algun paquet amb el patró: `apt-cache search patró`
- Mostra la informació detallada d'un paquet: `apt-cache show nom_paquet`
- Mostra les dependències d'un paquet: `apt-cache depends nom_paquet`

APTITUDE

Aptitude és una altra de les eines més utilitzades per a la gestió de paquets .deb, utilitzà com la resta d'eines la llibreria d'APT. Podem definir Aptitude com:

L'aptitude és una interfície gràfica en mode text (ncurses) per a l'APT. També es pot utilitzar com a ordre en la línia d'ordres.

La sintaxi i els resultats són molt semblants als de l'apt-get i l'apt-cache tot i que no funcionen ben bé igual, sobretot pel que fa al maneig de les dependències i a les opcions i la formatació de la sortida per pantalla. L'aptitude elimina les dependències que queden orfes en desinstal·lar un paquet. L'APT no ho fa automàticament, sinó que hem d'utilitzar l'ordre `clean`.

Per instal·lar paquets .deb amb l'aptitude utilitzarem l'ordre **aptitude install nompaquet**. Vegeu l'exemple següent: `$aptitude install traceroute`

Per desinstalar paquets .deb amb l'aptitude utilitzarem l'ordre **aptitude remove/purge nompaquet**. Vegeu-ne l'exemple: \$aptitude remove mysql-server-5.1

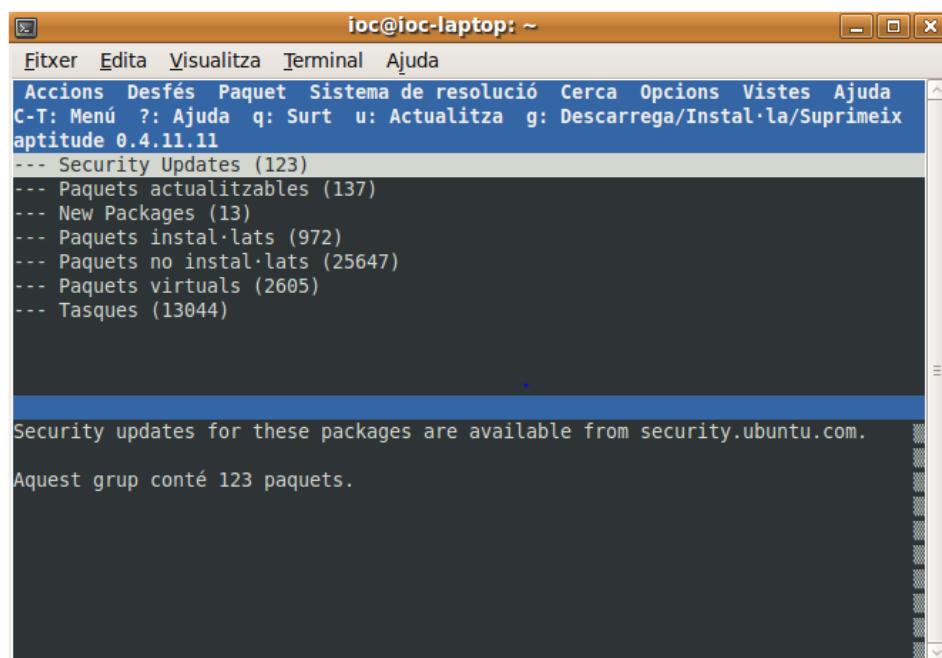
L'opció **purge** també elimina qualsevol fitxer de configuració del paquet desinstal·lat.

Les ordres següents també són interessants:

- Actualitza els dipòsits: aptitude update
- Actualitza tots els paquets instal·lats en les últimes versions que hi ha en els dipòsits: aptitude upgrade
- Cerca algun paquet amb el patró: aptitude search patró

Si executem l'aptitude en mode gràfic ens apareix una pantalla com la següent (vegeu figura 2.1).

FIGURA 2.1. Menú en format text d'Aptitude



Per fer servir la interfície gràfica haurem d'utilitzar les tecles següents, cadascuna de les quals té la seva funció:

- Actualitza els dipòsits: u. Fa el mateix que l'ordre \$sudo aptitude update.
- Actualitza tots els paquets instal·lats: U. Fa el mateix que l'ordre \$sudo aptitude upgrade.
- Quit, surt del programa: q
- Marca un paquet per instal·lar: +
- Marca un paquet per desinstalar: -

- La primera g mostra les tasques pendents i la segona g les aplica: gg
- Ajuda: ?
- Cerca un paquet per nom: /nom

Per tal d'instal·lar un paquet amb la interfície gràfica de l'aptitude seguirem els passos següents:

1. Localitzem el paquet en la categoria *Paquets no instal·lats*, mitjançant les tecles del cursor i la tecla *INTRO*.
2. Seleccionem el paquet que volem instal·lar i premem la tecla +. El paquet es posarà en verd.
3. Premem la tecla g i ens presentarà un resum de les accions que es faran a continuació.
4. Premem g altra vegada i començarà la descàrrega i la posterior instal·lació del paquet.

La primera columna reflecteix l'estat actual de cada paquet. S'usa la llegenda següent:

- Paquet instal·lat: i
- Paquet no instal·lat, però la configuració del paquet encara és en el sistema:
c
- Paquet eliminat del sistema: p
- Paquet virtual: v
- Paquet trencat: B
- Arxius desempaquetats, però el paquet està sense configurar: o
- A mig configurar, la configuració va fallar i s'ha de reparar: C
- A mig configurar, va fallar l'eliminació i s'ha de reparar: H

Instal·lació i actualització de paquets en mode gràfic

Gairebé tots els sistemes GNU/Linux, en les versions amb interfície gràfica, incorporen gestors de paquets en mode gràfic per facilitar les tasques d'instal·lació, desinstal·lació, recerca i configuració de paquets.

El funcionament dels diferents gestors de paquets gràfics de cada distribució és molt semblant. Nosaltres analitzarem el funcionament del Synaptic, un dels gestor de paquets gràfic que incorpora l'Ubuntu Desktop Edition.

Synaptic

Synaptic és una altra de les eines més utilitzades, sobretot en entorns d'escriptori GNOME, per a la gestió de paquets .deb. També utilitza la llibreria APT; el podem definir com a:

El Synaptic és un programa que implementa una interfície gràfica per al gestor de paquets APT en l'entorn d'escriptori GNOME.

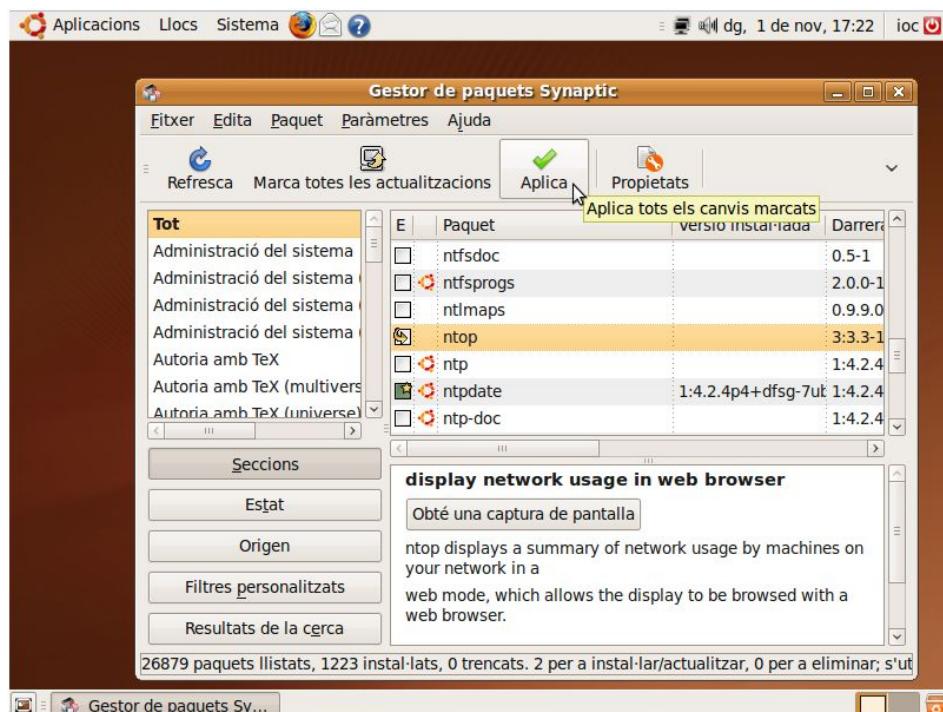
Normalment el Synaptic s'utilitza per a sistemes basats en paquets .deb, encara que també es pot fer servir en sistemes basats en paquets .rpm.

El funcionament del Synaptic és fàcil i intuitiu, de manera que qualsevol persona sense coneixements específics sobre el funcionament del sistema el pot utilitzar. Per accedir-hi anirem al menú **Sistema > Administració > Gestor de paquets Synaptic**.

Se'ns obrirà el quadre de diàleg de l'aplicació. A la dreta del quadre de diàleg hi ha la llista de paquets disponibles i la descripció del paquet que seleccionem. A l'esquerra hi ha diferents opcions per buscar els paquets que necessitem. En la part superior hi ha diversos botons i menús.

La casella del costat del nom de cada paquet en determina l'estat: blanc si no està instal·lat i verd si està instal·lat.

FIGURA 2.2. Instal·lació de paquets amb Synaptics

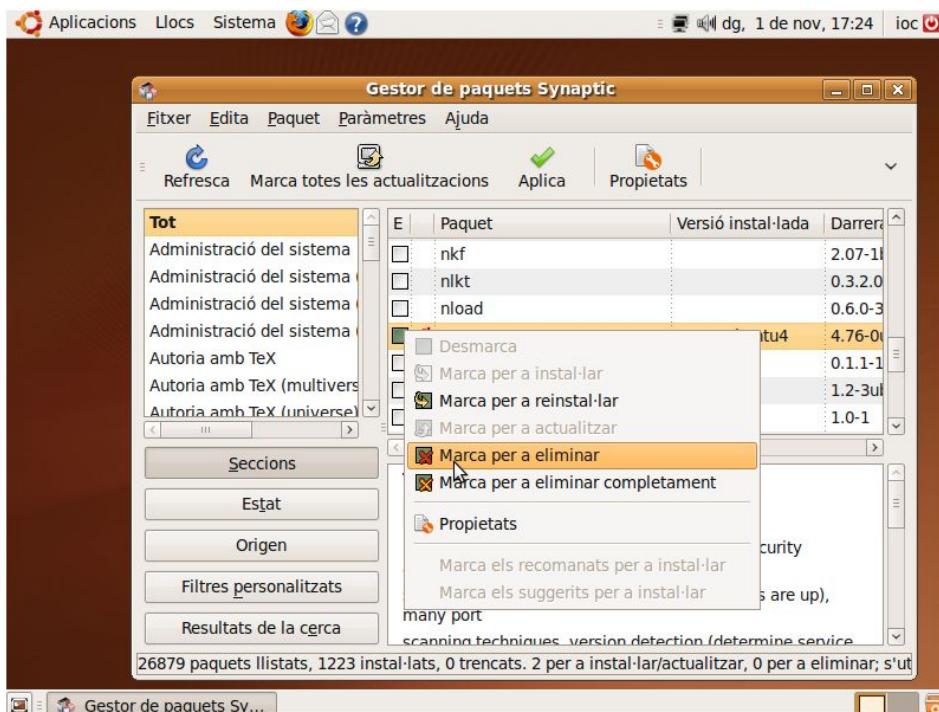


Per instal·lar paquets amb el Synaptic els hem de buscar. Seguidament, hi hem de fer doble clic al damunt. També podem fer servir el botó dret del ratolí i seleccionar l'opció **Marcar-los per instal·lar**. Una vegada marcats tots els paquets que volem instal·lar, cliquem a **Aplica**. Si els paquets tenen dependències d'altres paquets, ens preguntarà si també les volem instal·lar. Vegem-ne l'exemple en la figura 2.2.

Per desinstal·lar un paquet com en la figura 2.3 (ha de tenir la casella verda al costat), hi hem de clicar al damunt amb el botó dret del ratolí i seleccionar **Marca per eliminar** o **Marca per eliminar completament segons calgui**. A continuació,

hem de fer clic a **Aplica**.

FIGURA 2.3. Desinstal·lació de paquets amb Synaptic



Quan un paquet instal·lat té una estrelleta en la casella d'estat vol dir que hi ha actualitzacions disponibles d'aquest paquet i el podem Marcar per actualitzar.

Des del Synaptic, entre altres coses, també podem actualitzar tots els paquets instal·lats i modificar la configuració de les llistes de dipòsits de paquets de l'APT.

Tasksel

En els sistemes basats en Debian també hi podeu trobar l'aplicació Tasksel:

El Tasksel és un sistema d'instal·lació que ens permet instal·lar de manera senzilla tasques o agrupacions de paquets que instal·lats conjuntament proveeixin una funcionalitat comuna.

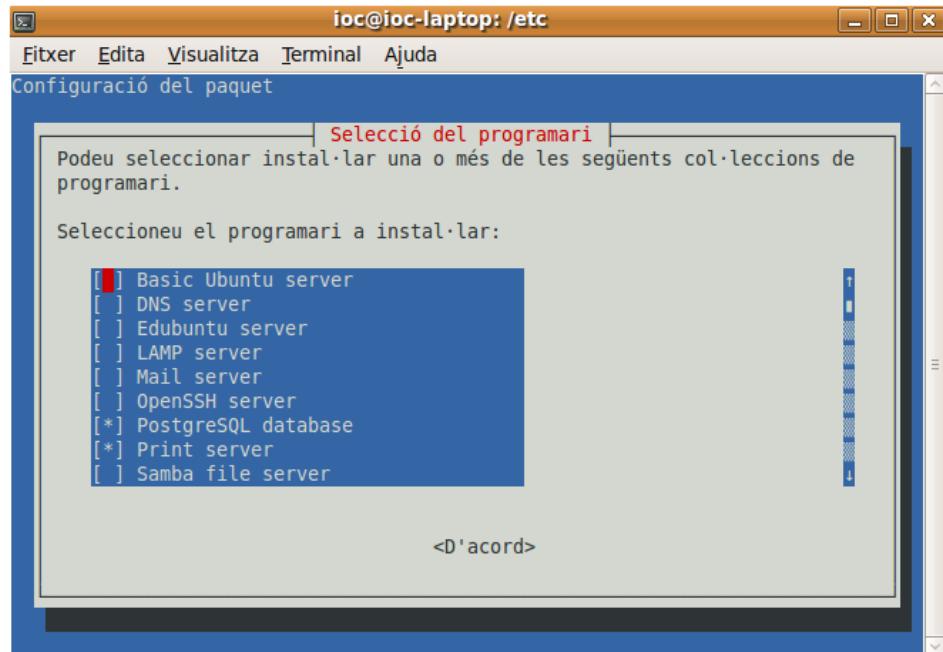
Per exemple, hi ha tasques per instal·lar un sistema LAMP o entorns d'escriptori com el GNOME o el KDE.

Per tal d'iniciar el sistema d'instal·lació, hem d'executar l'ordre tasksel, que inicia una interfície gràfica en mode text que ens permet seleccionar l'agrupació de paquets que volem instal·lar, generalment serveis. Per altra banda, l'aplicació tasksel s'executa per defecte en instal·lar el sistema Ubuntu Server Edition. D'aquesta manera, permet instal·lar el sistema operatiu amb els serveis o les funcionalitats que necessitem. En podem veure l'aspecte en la figura 2.4.

Execució de gestors

Mai no hi pot haver més d'una aplicació de gestió de paquets oberta al mateix temps. Si una aplicació de gestió de paquets es penja pot deixar bloquejat l'accés al dipòsit.

Aneu en compte, si deseleccioneu algunes de les aplicacions marquades amb * es desinstal·laran

FIGURA 2.4. Visió de tasksel

2.2.2 Gestió de paquets RPM

El sistema de paquets RPM el va crear la companyia Red Hat. Per això es diu RPM (*Red Hat package manager*). Amb el temps, d'altres distribucions han anat adoptant aquest sistema d'empaquetatge de fitxers. Les distribucions principals que l'han adoptat són Fedora, Suse i Mandrake.

Un paquet de programari construït amb RPM constitueix un conjunt de fitxers i informació que hi està associada com un nom, una versió i una descripció que acaben amb l'estensió rpm.

RPM

Els paquets amb format rpm utilitzen principalment l'ordre rpm per a la instal·lació. La sintaxi general d'una ordre d'instal·lació rpm és la següent:

```
1 rpm -i [opcions] [paquets]
```

Les opcions poden ser algunes de les següents:

- **-test:** efectua el procés d'instal·lació d'un paquet, però no l'instal·la realment. S'utilitza més aviat per detectar problemes que puguin sorgir en la instal·lació.
- **-nodeps:** no s'efectuen verificacions de dependències abans de la instal·lació d'un paquet.
- **-force:** força la instal·lació d'un paquet encara que sorgeixin problemes.

Vegeu l'exemple següent:

```
1 rpm -i — nodeps vim-4.5-2.i386.rpm
```

La manera d'actualització de l'rpm proporciona un mètode senzill per renovar paquets ja instal·lats en versions més modernes. El seu ús és similar al de la instal·lació:

```
1 rpm -U [opcions] [paquets]
```

Vegeu l'exemple següent:

```
1 rpm -U vim-4.5-2.i386.rpm
```

La manera de desinstal·lar l'RPM proporciona un mètode net per eliminar els arxius que pertanyen a un determinat paquet i que són en diferents llocs. Molts paquets instal·len fitxers en /etc, /usr i /lib, cosa que fa que eliminar-los pugui ser complicat. Amb l'RPM, però, un paquet complet es pot desinstal·lar mitjançant l'ordre següent:

```
1 rpm -e [opcions] [paquets]
```

Vegeu l'exemple següent:

```
1 rpm -e vim-4.5-2.i386.rpm
```

YUM

L'aplicació **YUM** també és una eina important per administrar paquets RPM. S'utilitza en distribucions importants com Fedora o CentOS. A més, el sistema de dipòsits yum s'ha convertit en un estàndard per als dipòsits basats en l'RPM. Sistemes com l'openSUSE basen els seus dipòsits en yum. Podem fer l'analogia amb apt en els paquets Debian. Es pot considerar, doncs, que yum és el frontal de l'rpm. La sintaxi és similar a la de l'rpm:

```
1 yum [opcions] [comandes] [paquet ...]
```

Les ordres, entre altres, poden ser les següents:

- Per instal·lar paquets: `install`. Vegeu l'exemple següent: `yum install tsclient`
- Per actualitzar paquets: `update`.

L'ordre `update` actualitza els paquets que troba a continuació. Si no li especificuem un paquet, actualitza tots els paquets amb l'última versió. Vegeu-ne un exemple: `yum update`

- Per esborrar paquets: `remove` o `erase`. Per exemple: `yum remove tsclient` o `yum erase tsclient`

Els dipòsits des dels quals l'eina yum descarrega els paquets es configuren a la carpeta **/etc/yum.repos.d**. L'estructura del dipòsit és diferent a la de Debian, però la funcionalitat és la mateixa.

L'eina yum també disposa de molts entorns gràfics, com ara **pirut** o **packagekit**.

2.3 Actualització del sistema operatiu

Els sistemes GNU/Linux, per la filosofia que segueixen, s'actualitzen constantment. Cada cert temps les distribucions GNU/Linux ofereixen versions noves dels seus sistemes amb noves utilitats, aplicacions, llibreries, mòduls, millors de seguretat i optimització de recursos, entre altres.

En algunes darreres versions, la versió del nucli del sistema també pot canviar respecte a la versió anterior. Així, s'afegeix, per exemple, suport a dispositius o eines que abans no tenien.

Durant el cicle de vida de cadascuna de les versions de les distin tes distribucions GNU/Linux, apareixen actualitzacions de paquets, mòduls i aplicacions que es poden actualitzar individualment mitjançant els gestors de paquets o els gestors d'actualitzacions de cada distribució. Tanmateix, arriba un moment en què per qüestions de seguretat, rendiment, compatibilitat i obsolescència convé actualitzar el sistema operatiu sencer.

Actualitzar el sistema operatiu consisteix a migrar a una versió nova i actualitzada del mateix sistema sense perdre les dades que hi ha.

Abans d'actualitzar el sistema haureu de comprovar que l'equip compleixi el requisits de maquinari del sistema nou. També haureu de fer còpies de seguretat, sobretot dels fitxers de configuració del sistema (/etc) i de les dades dels usuaris (/home).

L'actualització del sistema la podeu fer de diferents maneres. Les principals són des d'un suport físic (CD/DVD o USB) o des de la xarxa. Aquesta última és la més recomanada, ja que els paquets estaran actualitzats.

2.3.1 Actualització de l'Ubuntu Desktop Edition

A continuació veureu com actualitzar la versió Desktop mitjançant les eines gràfiques que proporciona la distribució.

Per actualitzar el sistema, si teniu accés a la xarxa, haureu de fer el següent:

Anar al menú **Sistema > Administració > Gestor d'actualitzacions**.

Tot seguit s'obrirà el **Gestor d'actualitzacions**, en què es veuen, entre altres, els paquets que el sistema ens recomana actualitzar. Per actualitzar tot el sistema ha d'aparèixer la disponibilitat d'una versió nova. Si cliqueu a *Actualitza*, tal com es

veu en la figura 2.5, el sistema es començarà a actualitzar amb la darrera versió.

FIGURA 2.5. Gestor d'actualitzacions



Si no teniu accés a la xarxa, haureu d'utilitzar el CD d'instal·lació alternativa de l'Ubuntu per actualitzar el sistema.

2.3.2 Actualització de l'Ubuntu Server Edition

Per tal d'actualitzar el sistema operatiu amb la versió Server de l'Ubuntu, heu d'instal·lar el paquet **update-manager-core**:

```
1 $sudo apt-get install update-manager-core
```

Editeu el fitxer **/etc/update-manager/release-upgrades** i establiu el següent:

```
1 Prompt=normal
```

Executeu l'ordre d'actualització:

```
1 $sudo do-release-upgrade
```

Confirmeu que voleu actualitzar el sistema operatiu i començarà l'actualització des de xarxa. Al final del procés el sistema us preguntarà si voleu eliminar els paquets obsolets. Li heu de dir que sí. Després de l'actualització el sistema s'haurà de reiniciar. Una vegada reiniciat, ja tindreu l'Ubuntu Server Edition actualitzat.

Si no teniu accés a la xarxa haureu d'utilitzar el CD d'instal·lació alternativa de l'Ubuntu per tal d'actualitzar el sistema.

2.4 Interpretació dels processos d'arrencada i aturada als sistemes GNU/Linux

Es coneix com a *procés d'arrencada* tot allò que succeeix en el vostre ordinador des que l'engegueu fins que el sistema està operatiu al cent per cent.

El procés d'arrencada comença amb el BIOS. En iniciar l'ordinador, el BIOS passa a buscar el sistema o sistemes operatius que hi ha instal·lats en l'equip. Cada vegada és més habitual fer que coexisteixin diversos sistemes operatius en un mateix ordinador. Així doncs, cal que durant l'arrencada pugueu triar quin d'aquests sistemes voleu executar. Aquesta tasca la fa un programa anomenat *gestor d'arrencada*, que normalment resideix en el disc dur. El gestor d'arrencada és el primer programa que s'executa i dóna pas a un menú per escollir el sistema que es vol arrencar. Posteriorment, en el cas del GNU/Linux, es carrega el nucli i s'executa el procés init.

D'altra banda, el procés que fa l'apagada d'una màquina l'anomenem *procés d'aturada*.

Es coneix com a *procés d'aturada* tot allò què succeeix en el vostre ordinador des que donem l'ordre d'aturada fins que el sistema deixa d'estar operatiu. El procés d'aturada ofereix a l'administrador del sistema una sèrie d'opcions com ara apagar o reiniciar el sistema.

2.4.1 Procés d'arrencada

A continuació veurem els passos que executa seqüencialment un sistema operatiu GNU/Linux per iniciar-se; aquesta seqüència s'anomena *procés d'arrencada*.

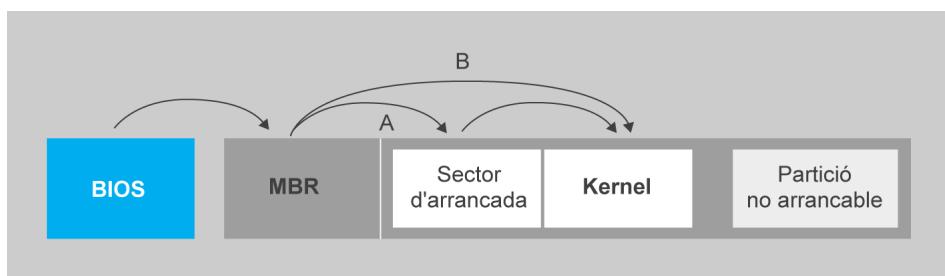
Per ordre d'execució els passos del procés d'arrencada són els següents:

1. L'ordinador s'engega i s'executa el BIOS.
2. El BIOS verifica el maquinari bàsic (procés POST), inicia altres dispositius (targeta gràfica, controladors SCSI, etc.) i, finalment, cerca dispositius d'arrencada: disquet, CD, disc dur, etc.
3. Un cop el maquinari és reconegut i executat correctament, el BIOS carrega i executa el programa Initial Program Loader (IPL), també conegut com a *fase 1 (stage 1)* del gestor d'arrencada. Aquest programa és en el *master boot record* (sector 0) del dispositiu seleccionat com a dispositiu d'arrencada.

4. Després de la fase 1 del carregador de l'arrencada (*bootloader*) s'executa la fase 2. Alguns gestors d'arrencada (com grub), entremig d'aquestes fases, executen la fase 1.5, fase opcional i que permet tenir accés a més sistemes de fitxers.
5. El gestor d'arrencada sovint ofereix a l'usuari un menú amb diferents opcions de càrrega. Un cop seleccionada una opció, s'executa el sistema operatiu mitjançant la càrrega en memòria del nucli del sistema. A continuació, les primeres tasques del nucli consisteixen a configurar funcions bàsiques d'accés al maquinari.
6. El nucli executa la funció `start_kernel()`, que efectua la majoria de la configuració del sistema (interrupcions, gestió de memòria, inicialització de dispositius, controladors, etc.).
7. El nucli executa dos processos, el procés **scheduler** i el procés **init** de manera separada.
8. El procés **scheduler** pren el control del sistema i és l'encarregat de gestionar els processos i la multitasca del sistema. El nucli queda inactiu (idle) i espera peticions d'accés a l'espai del nucli.
9. El procés **init** s'executa en espai d'usuari i executa els scripts d'inicialització del sistema. Aquests scripts configuren serveis que no són per defecte del sistema operatiu amb l'objectiu de crear un entorn d'usuari.
 - (a) Execució de `/etc/rc.d/rc.sysinit` (muntatge de particions).
 - (b) Execució de guions de crida a processos dimoni.
 - (c) Activació de terminals de consola.
 - (d) Activació de l'entorn gràfic.
10. Finalment, es proporciona a l'usuari una pàgina d'inici de sessió que pot ser per línia d'ordres o per entorn gràfic. També és possible configurar l'entorn per tal que l'usuari entri sense necessitat de fer *login*.

En la figura 2.6 podeu veure de manera esquemàtica aquest procés.

FIGURA 2.6. Esquema del procés d'arrencada.



2.4.2 Gestors d'arrencada

Un gestor d'arrencada és el primer programari que s'executa quan s'arrenca un ordinador. És el responsable de carregar i transferir el control a un altre programari: el nucli del sistema operatiu, per exemple, el del GNU/Linux.

El nucli, al seu torn, inicia la resta del sistema operatiu. Els gestors d'arrencada més coneguts i utilitzats són el **LILO** (Linux Loader), que cada vegada es fa servir menys, i el **GRUB** (*grand unified bootloader*). El gestor d'arrencada és un programa mínim que s'instal·la en un dispositiu arrencable. El lloc més habitual és l'MBR del primer disc dur o el sector d'arrencada d'un disquet.

2.4.3 El procés init

El procés **init** és el primer procés que executa el nucli en iniciar-se. És un procés dimoni i, com que és el primer, té el PID número 1. L'arrencada que fa el procés init en el GNU/Linux està basada en l'init de la versió System V de l'UNIX (davant de l'arrencada basada en BSD). El procés init coordina la resta del procés d'arrencada i es configura amb el fitxer `/etc/inittab`, que permet definir diversos paràmetres de funcionament.

Procés dimoni

Un dimoni o daemon (*disk and execution monitor*), és un tipus especial de procés informàtic que s'executa d'una manera contínua en segon terme, en comptes de ser controlat directament per l'usuari, és a dir, és un procés no interactiu. Generalment, els dimonis no disposen d'una “interfície” directa amb l'usuari, ja sigui gràfica o textual i no fan ús de les entrades i sortides estàndard per comunicar errors o registrar-ne el funcionament, sinó que usen arxius del sistema en zones especials com `/var/log/` o utilitzen altres dimonis especialitzats en aquest registre com el `syslogd`.

Procés init a l'Ubuntu

L'Ubuntu i el Fedora no utilitzen el fitxer `inittab`, sinó el dimoni controlat per esdeveniments `upstart`. La configuració del procés init en l'Ubuntu la trobareu en la carpeta `/etc/event.d`

El primer procés que s'executa en el sistema és l'init. El procés init llegeix la informació inicial del sistema de l'arxiu de text `/etc/inittab` i, a partir d'aquesta informació, inicia la resta de processos.

La cronologia d'execució del procés init és la següent:

- En l'arxiu de configuració `/etc/inittab` s'indica que s'executi el guió que s'encarrega d'arrencar el sistema normalment `/etc/rc.d/rc.sysinit`. Aquest guió és el responsable d'arrencar els serveis bàsics: activar l'`swap`, carregar els mòduls necessaris del nucli, inicialitzar la xarxa, revisar tots els sistemes de fitxers (`fsck`) indicats en el fitxer `/etc/fstab` i muntar-los, etc.
- El guió encarregat d'arrencar el sistema, acaba invocant un altre script (normalment l'`/etc/init.d/rc.local`), que serà el que s'haurà de modificar en el cas que es necessiti que el procés init faci alguna tasca addicional durant l'arrencada.

- Una vegada finalitzada l'execució d'aquest script, el control torna al procés init, que llegeix el paràmetre initdefault del fitxer de configuració.

Aquest paràmetre indica el *runlevel* en el qual s'ha d'arrencar el sistema. El procés init executarà l'script /etc/init.d/rc per portar el sistema al *runlevel* configurat. Aquest script també s'utilitza quan es fa un canvi de *runlevel*.

Els *runlevels* especificuen com funciona un sistema en un moment determinat, és a dir, els serveis que es vol que ofereixi (i els que no) en cada moment.

En cadascun dels nivells el sistema GNU/Linux arrenca o atura una sèrie de processos que determinen les característiques del nivell i què s'hi pot fer:

- Un sistema pot estar configurat perquè en un nivell d'execució determinat s'ofereixin serveis externs (per exemple, serveis web i DNS), però no interns.
- El mateix sistema pot estar configurat perquè en un altre nivell d'execució s'ofereixin serveis interns (per exemple, serveis DHCP i NFS), però no externs.
- Canviant un *runlevel* per un altre s'aconsegueix que el sistema funcioni d'una manera o d'una altra (per exemple, aturant els serveis externs i arrencant els interns o a l'inrevés).

Nivells d'execució (runlevels)

A continuació veureu una taula (taula 2.1) que mostra els nivells d'execució o runlevels que hi ha en els sistemes GNU/Linux i la descripció de cadascun.

TAULA 2.1. Nivells d'execució.

Nivell d'execució	Descripció
0	Atura el sistema. És un nivell especial que permet a l'administrador aturar el sistema de manera ràpida.
1,s,S	<i>Single user mode</i> (mode d'usuari únic, a vegades anomenat <i>mode de manteniment</i>). En aquest nivell, només funcionen els serveis bàsics del sistema (per exemple, no funciona ni el cron ni el syslog). S'utilitza per fer tasques de manteniment del sistema de fitxers.
2	Multiusuari sense compartició de fitxers NFS.
3	Mode multiusuari complet. Habitualment aquest nivell s'utilitza com a nivell per defecte per al procés init.
4	Normalment no s'utilitza.
5	Mode multiusuari complet amb <i>login</i> mitjançant interfície gràfica. En aquest nivell es llança el sistema X Window. També pot ser el nivell per defecte, però hi pot haver problemes si les X no arrenquen correctament.
6	Rastreja el sistema. És un nivell especial que permet a l'administrador reiniciar el sistema.

Mode monousuari

El mode monousuari (*single user*) es pot fer servir per corregir problemes amb sistemes de fitxers corruptes que el sistema no pot resoldre automàticament. També s'utilitza per instal·lar programari i altres tasques de configuració del sistema que s'han de fer sense que hi hagi cap usuari connectat, com ara les còpies de seguretat del sistema. En aquest mode l'únic procés d'usuari que es llança és el *sulogin*, que només permet la validació com a arrel (*root*). Per tant, l'únic usuari que pot treballar en aquest mode serà el superusuari.

Scripts de control dels serveis

Els serveis que estan instal·lats en el sistema creen un *script* situat en el directori /etc/init.d, que permet controlar el servei (arrencar-lo, aturar-lo, reiniciar-lo, etc.). Quan l'argument stop es passa al nom de l'script, el dimoni s'atura. Amb el paràmetre start, en canvi, s'arrenca. Hi ha altres opcions, com ara restart, reload o status.

Arrencada automàtica de serveis

El fet que un servei estigui instal·lat no vol dir que estigui configurat per arrencar-se automàticament en iniciar el sistema. Per això s'ha d'activar.

Un servei que estigui activat s'arrencarà automàticament.

Per veure tots els serveis instal·lats i l'estat en què es troben (activat/desactivat) s'ha d'usar l'ordre **chkconfig**.

- **chkconfig servei off**: Desactiva un servei. chkconfig syslog off
- **chkconfig servei on**: Activa un servei. chkconfig syslog on

En realitat, l'ordre **chkconfig** invoca l'ordre **insserv** per activar o desactivar els serveis.

Configuració dels serveis per runlevel

Quan s'activa un servei, el que realment es fa és configurar certs *runlevels* perquè arrenquin o aturin els serveis en entrar-hi. Mitjançant un fitxer de configuració s'indican els *runlevels* en què es configura un servei activat. Aquest fitxer és el mateix que permet controlar els serveis (els fitxers de control del directori /etc/init.d).

Amb el paràmetre **Default-Start** i **Default-Stop** es defineixen els *runlevels* en què un servei s'arrenca o s'atura quan està funcionant. Quan el servei està desactivat no s'arrenca ni s'atura en cap *runlevel*.

Per modificar la configuració s'haurà de desactivar el servei, modificar el paràmetre i tornar a activar el servei.

Configuració dels runlevels

Durant el procés d'arrencada l'*script* **/etc/init.d/rc** és l' que efectua els passos necessaris per entrar en un *runlevel* o passar d'un *runlevel* a un altre.

Per configurar els runlevels heu d'accendir al directori **/etc/init.d/**, on trobem una sèrie de directoris, un per a cada nivell d'execució:**rc0.d – rc6.d**.

Aquest directori conté scripts individuals d'aturada i arrencada per a cada servei en el sistema. En cadascun dels directoris dels *runlevels* (**/etc/rc.d/rc0.d** en el **/etc/rc.d/rc6.d**) hi ha enllaços simbòlics que apunten als scripts del directori **/etc/init.d**.

Aquests enllaços tenen la sintaxi següent:

[K|S][número_seqüència][descripció]

- **K|S**: La K significa 'kill' i la S significa 'start'. Així doncs, la S indica els serveis que s'han d'estar executant en el nivell i la K els que deuen estar aturats.
- **número_seqüència**: indica l'ordre en què els serveis s'han d'arrencar o aturar. Primer s'executen els de seqüència més baixa. Si són iguals, s'escull per ordre alfabètic.
- **descripció**: normalment el nom de l'*script* que està enllaçat. El procés init no utilitza aquest nom, però serveix per facilitar-ne la identificació a l'administrador.

Quan el procés **init** entra en un nivell d'execució examina els enllaços del directori associat, els llista alfabèticament i els executa amb un paràmetre: **start** si comença per **S** i **stop** si comença per **K**.

Durant l'arrencada, per tal de seleccionar el nivell d'execució per defecte, el procés **init** llegeix el fitxer de configuració **/etc/inittab** i cerca una línia amb la paraula **initdefault** (de la forma **id:n:initdefault**), en què **n** és un número de nivell d'execució vàlid. Aquest número indica el nivell d'execució o *runlevel* que carregarà el sistema per defecte. Hem d'anar amb compte i no posar mai el nivell 0 o el nivell 6, ja que provocaríem que el sistema no es pogués arrencar.

Per conèixer el nivell d'execució en què ens trobem una vegada arrencat el sistema podem utilitzar l'ordre **runlevel**, la qual mostra el nivell d'execució actual i l'anterior mitjançant un número. Si no s'ha efectuat cap canvi de nivell, el nivell anterior apareixerà com a **N**.

Per tal de canviar el nivell d'execució podem utilitzar l'ordre **init** o **telinit**. Aquesta última és un enllaç a init. Així doncs, el nivell es pot indicar amb el número de nivell corresponent o si volem canviar al mode **monousuari** amb les lletres **S** o **s**.

Per exemple, l'ordre següent ens passaria del *runlevel* actual al *runlevel 3*: `$sudo init 3`

2.4.4 Procés d'aturada

En els sistemes GNU/Linux hi ha una ordre per aturar el sistema, l'ordre **shutdown**.

L'ordre shutdown és la responsable de l'aturada del sistema. L'administrador té els privilegis necessaris per executar-la directament. Amb aquesta ordre el sistema es pot aturar, apagar o reiniciar. Pot enviar un missatge a tots els terminals del sistema perquè els usuaris sàpiguen que hi hauria una apagada imminent.

Les ordres que pot executar shutdown són **reboot**, **halt** i **poweroff**. Són les que realment reinician, aturen o apaguen el sistema, respectivament. L'ordre **poweroff** és equivalent a **halt -p**.

Per conèixer totes les opcions de l'ordre shutdown podeu consultar el manual del sistema amb l'ordre man shutdown.

2.5 Configuració dels paràmetres de xarxa als sistemes GNU/Linux

Heu de considerar la importància del procés de configuració dels paràmetres de xarxa en els sistemes operatius GNU/Linux.

Qualsevol sistema operatiu GNU/Linux està preparat per treballar en xarxa, ja que incorpora suport natiu per a TCP/IP. En alguns sistemes GNU i, en concret, en l'Ubuntu, la configuració de xarxa s'efectua per defecte durant la instal·lació. Tanmateix, hi ha diverses ordres que permeten comprovar i modificar aquesta configuració. Els passos que heu de seguir per configurar-la correctament són:

- Detecció i configuració del maquinari de xarxa.
- Assignació dels paràmetres de xarxa, adreça IP, màscara de xarxa, porta d'enllaç, nom de la màquina a la xarxa, servidor DNS.

L'ordre lspci proporciona informació sobre el bus PCI i altres dispositius del sistema, grep filtra els resultats pel patró que segueix.

2.5.1 Detecció i configuració del maquinari de xarxa

El primer pas per poder configurar el maquinari de xarxa del vostre equip, una vegada arrencat, és confirmar que el sistema operatiu n'ha detectat els dispositius

de xarxa. Heu d'assegurar-vos que el sistema ha detectat i reconegut la targeta o targetes de xarxa que teniu instal·lades. Si no les ha detectat, haureu de determinar si el nucli del sistema suporta els controladors de les targetes. En aquest cas haureu de tenir o descarregar els mòduls adequats per tal de modificar-los i compilar-hi el nucli.

Per tal de saber si la targeta de xarxa que teniu instal·lada en l'equip s'ha detectat i mostrar-ne alguns dels paràmetres, podeu utilitzar l'ordre següent:

```
1 lspci | grep Ethernet
```

2.5.2 Assignació de paràmetres de xarxa

Una vegada us hagiu assegurat que els dispositius físics de xarxa de l'equip funcionen correctament, heu de determinar si la configuració dels paràmetres de xarxa assignats per defecte a la instal·lació del sistema és correcta o l'heu de modificar.

Els paràmetres que heu de tenir en compte són els següents:

- Adreça IP
- Màscara de xarxa
- Porta d'enllaç
- Nom de l'equip en la xarxa
- Servidor de DNS

També és interessant tenir en compte les taules de rutes del vostre equip, sobretot si actua com un encaminador a la xarxa.

Els paràmetres anteriors es poden establir automàticament de manera dinàmica si disposeu d'un servidor DHCP a la xarxa. En aquest cas només haureu d'indicar en el fitxer corresponent que la configuració s'establirà mitjançant DHCP. Si els paràmetres de xarxa anteriors no els determina un servidor DHCP, és a dir, són estàtics, els haureu d'establir manualment.

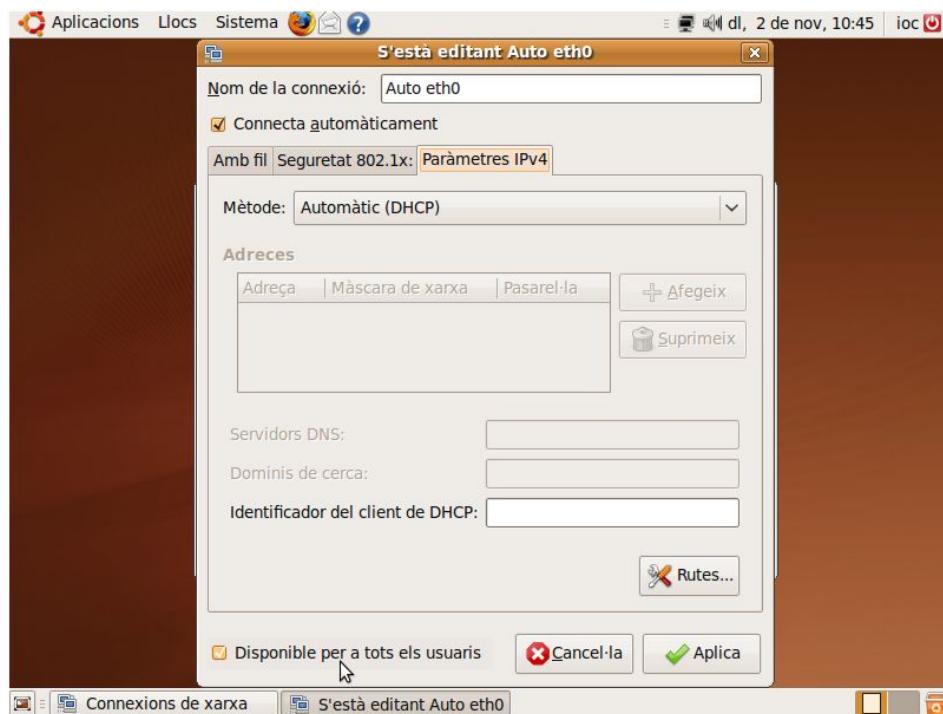
En l'Ubuntu 9.04 Desktop Edition aquestes configuracions les podem fer gràficament o mitjançant la línia d'ordres. Aquesta última opció és la mateixa per a la versió Server.

Per tal d'establir els paràmetres de xarxa gràficament, feu clic amb el botó dret del ratolí al damunt de la icona de xarxa de la part superior esquerra de la pantalla i seleccioneu l'opció **Edita les connexions**.

Depenent del tipus de configuració que tingueu (amb fil o sense, dsl, etc.), seleccioneu la interfície que voleu configurar i polseu el botó **Edita**. A continuació

apareixerà un quadre en què heu de seleccionar la pestanya **Parametres IPv4**. Tal com podeu veure en la figura 2.7, hi heu d'establir els paràmetres de configuració que vulgueu mitjançant les diverses opcions que ofereix.

FIGURA 2.7. Assistent gràfic per configurar els paràmetres de xarxa



Per fer la configuració mitjançant la línia d'ordres heu d'editar el fitxer **/etc/network/interfaces**. Per exemple:

```
1 $sudo nano /etc/network/interfaces
```

En el fitxer hi ha d'haver les línies següents per configurar dinàmicament els paràmetres de xarxa amb un servidor DHCP:

```
1 auto ethx
2 iface ethx inet dhcp
```

La x és el número de la interfície de xarxa. Hi haurà tantes repetitions d'aquestes línies en el fitxer com targetes de xarxa necessiteu configurar.

Per configurar estàticament els paràmetres de xarxa, afegiu en el fitxer les línies que apareixen en l'exemple següent:

```
1 auto eth0
2 iface eth0 inet static
3 address 192.168.3.90
4 netmask 255.255.255.0
5 gateway 192.168.3.1
```

Address especifica l'adreça IP de l'equip, *netmask*, la màscara de xarxa utilitzada, i *gateway*, la porta d'enllaç de la xarxa. L'Ubuntu configura el DNS i els noms de màquines de la mateixa manera que altres distribucions.

Utilitza dos fitxers:

- **/etc/hosts**: Per a la resolució estàtica de noms.
- **/etc/resolv.conf**: Per a la resolució de noms mitjançant DNS.

El fitxer **/etc/hosts** és el fitxer que el sistema llegirà per defecte si la vostra màquina no utilitza un servidor DNS. Si l'editeu, **\$sudo nano /etc/hosts**, veureu el següent:

```
1 127.0.0.1 localhost  
2 192.168.0.1 nomdomini
```

Podeu establir manualment el nom i l'adreça de les màquines que voleu resoldre.

Per establir manualment el servidor DNS de la xarxa, editeu el fitxer **/etc/resolv.conf**. Per exemple:

```
1 $sudo nano /etc/resolv.conf
```

A continuació, veurem el següent:

```
1 domain local.lan  
2 search local.lan  
3 nameserver 213.0.1.1  
4 nameserver 217.0.1.2
```

Els paràmetres *domain* i *search* indiquen el domini a què pertany la màquina i el paràmetre *nameserver* indica els servidors de DNS als quals l'equip consultarà per a la resolució de noms. L'ordre de línia de DNS determina quin servidor es consultarà primer.

Després de fer els canvis en els diversos fitxers de configuració dels paràmetres de xarxa, heu de reiniciar els serveis de xarxa perquè els canvis tinguin efecte amb l'ordre:

```
1 /etc/init.d/networking restart
```

2.5.3 Eines de xarxa

Una vegada configurats els paràmetres de xarxa del sistema, heu de comprovar que funcionin correctament. Per fer-ho podeu utilitzar una sèrie d'ordres o eines que hi ha en tots els sistemes operatius GNU/Linux. Aquestes ordres serveixen per fer el monitoratge del funcionament de la xarxa. Les ordres principals són les següents:

Ordre ping

L'ordre ping és una de les ordres més utilitzades per diagnosticar el funcionament dels diferents elements d'interconnexió o nodes d'una xarxa.

ICMP és un subprotocol de control i notificació d'errors del protocol IP.

L'ordre **ping** és molt útil per comprovar si una màquina concreta és accessible per mitjà de la xarxa IP. Aquesta ordre utilitza el protocol ICMP i més concretament el paquet echo request.

L'origen del nom constitueix una analogia amb el ping-pong (envies un “ping” i rep una confirmació, “pong”). L'ordre ping estima el temps en mil·lisegons que tarda un paquet a fer el trajecte d'anada i tornada. Aquesta ordre és útil per comprovar si la connexió a Internet funciona o si una màquina és a la xarxa. Vegeu l'exemple següent:

Per comprovar que el servidor web de Google està funcionant, executaríem l'ordre següent:

```
1 $ping -c 4 google.com
2 Pinging www.l.google.com [64.233.183.103] with 32 bytes of data:
3 Reply from 64.233.183.103: bytes=32 time=12ms TTL=244
4 Reply from 64.233.183.103: bytes=32 time=12ms TTL=244
5 Reply from 64.233.183.103: bytes=32 time=12ms TTL=244
6 Reply from 64.233.183.103: bytes=32 time=12ms TTL=244
7 Ping statistics for 64.233.183.103:
8 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
9 Approximate round trip times in milli-seconds:
10 Minimum = 12ms, Maximum = 12ms, Average = 12ms
```

Si el servidor respon com en aquest exemple, l'ordre ping ens retorna la IP del servidor, els bytes del paquet, el temps que ha trigat a respondre i el *time to live* o nombre de salts possibles de cada paquet fins al servidor. A més, al final mostra un resum de les estadístiques de l'ordre ping.

Ordre traceroute

L'ordre **traceroute** permet seguir la pista dels paquets que van d'un node de xarxa a un altre i especificar el camí que han recorregut.

Aquesta ordre no ha d'estar instal·lada per defecte en el sistema. La podeu instal·lar a l'Ubuntu amb l'ordre següent:

```
1 $sudo apt-get install traceroute
```

Per fer ús de traceroute cal escriure, després de l'ordre, l'adreça de xarxa o el nom del domini al qual voleu arribar. Vegeu l'exemple següent:

Volem conèixer el camí, és a dir, els nodes pels quals passaran els paquets, en establir una comunicació amb el servidor de Google. Així executem l'ordre següent:

```
1 $traceroute www.google.com
2 traceroute to www.l.google.com (64.233.169.99), 64 hops max, 40 byte packets
3 1      1 ms      1 ms      1 ms  192.168.1.1
4 2      *      53 ms    116 ms  192.168.153.1
5 3    48 ms     48 ms     45 ms  66.Red-80-58-123.staticIP.rima-tde.n 3.66]
6 4    48 ms     48 ms     46 ms  So-3-0-0-0-grtbcnes1.red.telefonica-t
[84.16.9.253]
```

```

7   5   68 ms    67 ms    88 ms Xe11-0-0-0-grtpartv1.red.telefonica-t
8     [84.16.13.142]
9   6   65 ms    64 ms    64 ms G00GLE-xe-9-0-0-grtpartv1.red.tele sale.net
10    \[84.16.6.106]
11   7   66 ms    67 ms    68 ms 209.85.251.40
12   8   140 ms   74 ms    74 ms 209.85.243.111
13   9   72 ms    75 ms    72 ms 72.14.236.191
14  10   78 ms    72 ms    84 ms 209.85.243.93
14  11   72 ms    74 ms    75 ms wy-in-f99.1e100.net [209.85.227.99]

```

L'ordre ens retorna la IP del servidor Google, el nombre de salts (nodes) pels quals passen els nostres paquets, la IP o el nom de màquina de cada node i el temps d'anada i tornada de les tres proves que fa l'ordre traceroute per a cada salt.

Ordre ifconfig

L'ordre **ifconfig** és una eina GNU/Linux per configurar i consultar els paràmetres de les interfícies de xarxa del sistema.

L'ordre ifconfig és una eina bàsica per conèixer i configurar els paràmetres de xarxa d'un equip, en permet conèixer i configurar les IP de les interfícies de xarxa, les MAC, els errors i les estadístiques de transmissió, entre altres informacions. Així doncs:

Si executem l'ordre sense paràmetres ens mostra la informació de cadascuna de les interfícies de xarxa configurades a l'equip.

L'ordre **ifconfig** potser no mostra totes les interfícies de xarxa d'un equip depenent de si són sense fil, etc.

```

1 $ifconfig
2   eth0 Link encap:Ethernet HWaddr 00:0A:E6:C6:07:85
3     inet addr:132.18.0.16 Bcast:132.18.0.255 Mask:255.255.255.0
4       inet6 addr: fe80::20a:e6ff:fe:785/64 Scope:Link
5         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
6         RX packets:18458 errors:0 dropped:0 overruns:0 frame:0
7         TX packets:8982 errors:0 dropped:0 overruns:0 carrier:0
8         collisions:0 txqueuelen:1000
9         RX bytes:4015093 (3.8 MiB) TX bytes:1449812 (1.3 MiB)
10        Interrupt:10 Base address:0xd400

```

En la primera línia podem veure el nom de la interfície, eth0, l'adreça IP, l'adreça de broadcast i la MAC; en la línia següent ens mostra, entre altres dades, l'adreça ipv6 corresponent. La línia següent ens proporciona la grandària màxima (MTU) dels paquets transmesos per aquesta interfície i la mètrica; la resta de línies ens mostren estadístiques sobre els paquets rebuts i enviats per la interfície i dades referents al maquinari com el nombre d'interrupció de la targeta de xarxa i l'adreça de memòria relacionada.

Ordre netstat

L'ordre **netstat** és una eina per veure les connexions actives d'un ordinador, tant d'entrada com de sortida.

La informació que es retorna inclou el protocol en ús, les adreces IP (tant locals com remotes), els ports locals i remots utilitzats i l'estat de la connexió. Vegeu l'exemple següent:

```
1 $netstat -nr
```

- **-n**: significa que retorna diverses ip en comptes de noms dns.
- **-r**: significa que mostri la taula de rutes.

Per veure tots els ports oberts, cal fer el següent:

```
1 $netstat -a
```

Per consultar els ports en escolta, cal fer el següent:

```
1 $netstat -l
```

Ordre nmap

L'ordre **nmap** ens serveix per rastrejar els ports d'una màquina i mostrar-ne l'estat. S'utilitza sobretot per avaluar la seguretat del sistema i per veure els serveis que ofereix.

Ho hem de tenir en compte, ja que també pot ser utilitzada en contra nostra amb finalitats malicioses.

Vegeu l'exemple següent:

Per comprovar quins ports estan oberts en el nostre equip, podem executar des del mateix l'ordre següent:

```
1 $sudo nmap localhost
2 Starting Nmap 4.76 ( http://nmap.org ) at 2010-03-30 20:11 CEST
3 Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
4 Warning: RateMeter::update: negative time delta; now=1269972704.235719;
5   \last_update_tv=1269972704.235809
6 Interesting ports on localhost (127.0.0.1):
7 Not shown: 989 closed ports
8 PORT      STATE SERVICE
9 22/tcp     open  ssh
10 80/tcp    open  http
11 139/tcp   open  netbios-ssn
12 389/tcp   open  ldap
13 445/tcp   open  microsoft-ds
14 631/tcp   open  ipp
15 2049/tcp  open  nfs
16 Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Aquesta ordre ens mostra per defecte tots els ports tcp, especificant-ne el número i el protocol al qual correspon, que tenim oberts.

Ordre route

L'ordre **route** permet veure i manipular la taula de rutes del sistema operatiu. La taula de rutes emmagatzema les rutes en els diferents nodes de la xarxa.

Aquesta opció és molt interessant si el vostre equip s'encarrega d'encaminar el trànsit de la vostra xarxa. Vegeu l'exemple que es mostra a continuació:

Per consultar la taula de rutes de l'equip en el qual ens trobem utilitzem la comanda següent:

```

1 $route
2 Kernel IP routing table
3 Destination      Gateway      Genmask      Flags Metric Ref Use Iface
4 10.0.2.0          *          255.255.255.0 U   1 0      0      eth0
5 link-local        *          255.255.0.0   U      1000 0      0      eth0
6 default    10.0.2.2 0.0.0.0 UG 0 0 0 eth0

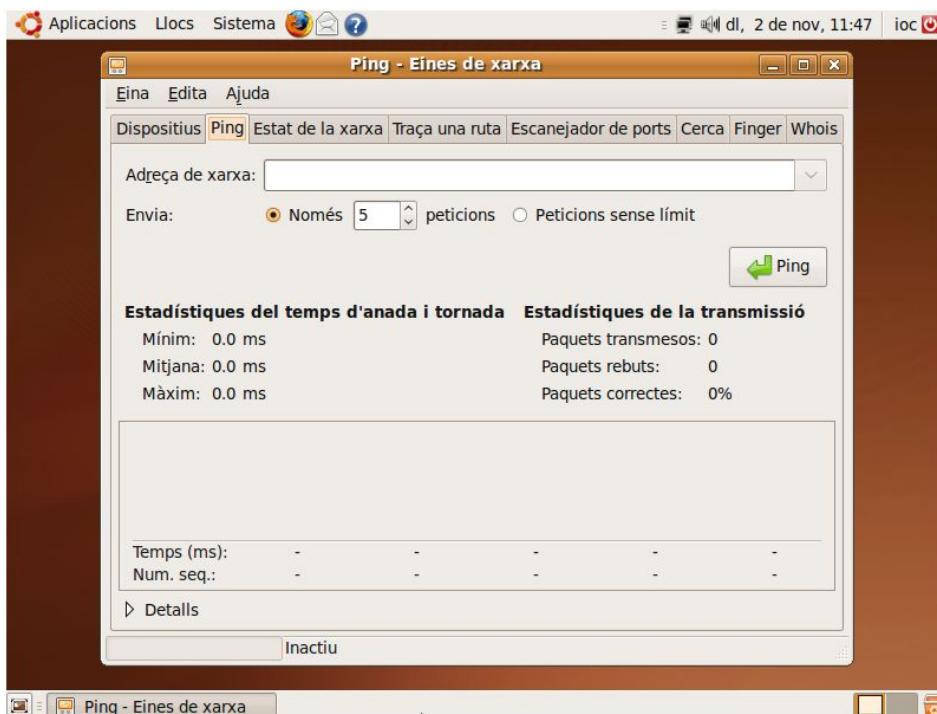
```

Aquesta ordre ens mostra les rutes configurades en el nostre sistema, és a dir, ens apareixen les IP de les xarxes cap on el nostre sistema enviarà directament els paquets que hi vagin destinats, sempre que hi hagi una ruta per defecte, que normalment coincideix amb la passarel·la (*gateway*) de la xarxa.

En l'Ubuntu 9.04 Desktop Edition podeu fer ús d'aquestes eines de manera gràfica mitjançant el menú *Sistema > Administració > Eines de xarxa*:

Se us obrirà una aplicació com la de la figura 2.8 des de la qual podreu utilitzar totes les ordres comentades anteriorment i algunes més.

FIGURA 2.8. Eines de xarxa de GNOME



Ordre ip

L'ordre ip és dins del paquet **iproute2**.

El paquet iproute2 és un conjunt d'eines molt potents per administrar interfícies de xarxa i connexions en sistemes GNU/Linux. Aquest paquet reemplaça completament les funcionalitats presents en les ordres ifconfig, route i arp. Les amplia i arriba a tenir característiques similars a les que proveeixen dispositius que estan exclusivament dedicats a l'encaminament i al control de trànsit.

Aquest paquet el podem trobar inclòs en el Debian i el Red Hat amb versions del nucli a partir de la 2.2.

La sintaxi i la descripció de l'ordre ip es detalla a continuació:

¹ `ip [opciones] objecte [ordre[arguments]]`

L'objecte pot tenir els valors següents:

- Utilitzat per configurar els objectes físics o lògics de la xarxa: link
- Serveix per manejar adreces associades als diferents dispositius. Cada dispositiu ha de tenir, almenys, una adreça associada: address
- Permet als usuaris veure els enllaços de veïnatge, afegir entrades de veïnatge noves i esborrar les antigues: neighbour
- Permet als usuaris veure les polítiques d'encaminament i canviar-les: rule
- Permet als usuaris veure les taules d'encaminament i canviar-ne les regles: route
- Permet als usuaris veure els túnels IP i les propietats que tenen, i canviar-los: tunnel
- Permet als usuaris veure les adreces multienllaç i les propietats que tenen, i canviar-les: maddr
- Permet als usuaris establir, canviar o esborrar l'encaminament multienllaç: mroute
- Permet als usuaris monitoritzar contínuament l'estat dels dispositius, les adreces i les rutes: monitor

2.6 Automatització de tasques als sistemes GNU/Linux

L'automatització de tasques és uns dels mètodes de treball que més faciliten la feina dels tècnics, ja que eviten la interacció directa amb el sistema per fer qualsevol conjunt de tasques. Així doncs, podem definir l'automatització de tasques de la manera següent:

L'automatització de tasques és el conjunt de mètodes que serveixen per fer tasques repetitives en un ordinador. El principi bàsic d'automatitzar és que l'usuari del sistema no intervingui en un procés sistemàtic real. Si hi intervé, aquesta intervenció ha de ser mínima.

El procés d'automatitzar depèn de certes activitats metòdiques prèviament programades ordenadament i que poden ser repetitives mitjançant cicles, com ara l'execució de determinats *scripts*.

Per mantenir el funcionament correcte d'un sistema complex com el GNU/Linux s'ha de fer molta feina.

Moltes de les tasques que s'han d'efectuar són rutinàries: rotació dels fitxers de registre, neteja de fitxers i directoris temporals, reconstrucció de bases de dades del sistema, còpies de seguretat, etc. A continuació, veureu algunes de les eines que us ofereix el GNU/Linux per automatitzar diverses tasques.

Cron

Una de les eines més utilitzades en els sistemes GNU/Linux per automatitzar tasques és l'eina cron.

Cron és un servei de planificació de tasques basat en temps que s'utilitza molt en sistemes operatius basats en l'UNIX.

El Cron és el nom del programa que permet als usuaris de sistemes GNU/Linux **executar ordres o guions d'intèrpret d'ordres de manera automàtica en una data i un temps específics**. Sovint els administradors de sistemes fan servir aquest programa com a eina per automatitzar tasques d'administració.

Per fer-lo servir utilitzem l'ordre crontab:

- Per editar el fitxer de planificació de l'usuari: `-e`
- Per visualitzar el fitxer de planificació de l'usuari: `-l`
- Per esborrar el fitxer crontab: `-r`
- Operarà amb el fitxer crontab de l'usuari indicat: `-u user`

Només l'usuari primari pot editar o eliminar el fitxer crontab d'altres usuaris.

Mitjançant les ordres anteriors programarem les tasques per a l'usuari *logejat* en el sistema en aquell moment.

Per tal de programar tasques per a tot el sistema, editeu el fitxer **/etc/crontab** i afegiu-hi les tasques que voleu programar amb el format específic que dóna el fitxer. El podem veure en la figura 2.9.

FIGURA 2.9. Exemple del fitxer

```
ioc@ioc-laptop: ~
Fitxer Edita Visualitzar Terminal Ajuda
GNU nano 2.0.9           Fitxer: /etc/crontab

# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$...
47 6      * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$...
52 6      1 * * *  root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$...
#
```

[17 línies llegides]

^G Ajuda **^O Desa** **^R Llegeix** **^Y Pàg Ant** **^K Retalla** **^C Pos Act**
^X Surt **^J Justifica** **^W Cerca** **^V Pàg Seg** **^U Desf** **^T Ortografia**

La sintaxi del fitxer /etc/crontab és la següent:

- La columna **m** fa referència als **minuts** i va de **0** a **59**.
- La columna **h** fa referència a l'**hora** i va de **0** a **23**.
- La columna **dom** determina el **dia d'1 a 31**.
- La columna **mon** estableix el **mes d'1** (gener) a **12** (desembre).
- La columna **dow** marca el **dia de la setmana** de **0** (diumenge) a **6** (dissabte).
- **User** determina l'usuari que ha programat la tasca i **command** la tasca o el programa a efectuar.

Es poden escriure comentaris començant la línia amb **#**. També es pot substituir qualsevol paràmetre per *****, que indica que tindrà qualsevol valor en el camp corresponent.

Per exemple, per executar un programa una vegada al dia a les 6.15 h, introduirem la línia següent en el fitxer /etc/crontab:

1	15 6 * * * programa
---	---------------------

Es poden indicar diversos valors per a un camp separant-los per comes (1,3,6) o especificar un rang de valors (3-7).

Ordre at

L'ordre at és un altra de les eines que ens proporcionen els sistemes GNU/Linux per executar tasques de manera automàtica i programada.

L'ordre at permet programar treballs que s'executaran a una hora determinada una sola vegada.

La sintaxi és la següent:

```
1 at -f fitxer temps
```

temps: Pot indicar una **hora** (HH:MM) o una **data** (amb el format MMDDYY, MM/DD/YY o MM.DD.YY).

Hi ha molts formats disponibles per indicar el moment de l'execució:

```
1 now midnight tomorrow teatime
```

També es pot indicar temps de la manera següent:

- **now + 5 minutes**, és a dir, 'd'aquí a 5 minuts'.
- **6:15pm tomorrow**, és a dir, 'demà a les 6.15 de la tarda'.
- **9pm + 2 days**, és a dir, 'a les 9 de la tarda d'aquí a dos dies'.

Per exemple, executar una tasca d'aquí a deu minuts:

```
1 $at -f tasca.sh now + 10 minutes
```

Quan es programa una tasca amb l'ordre at es genera un *job* amb un número que permet gestionar-lo. La sortida d'at és fa enviant un correu electrònic a l'usuari que ha programat la tasca. També podeu utilitzar altres opcions:

- **at -l o atq**: Per veure les tasques pendents.
- **at -c num_job**: Per veure el contingut d'una feina.
- **at -d num_job o atrm num_job**: Per esborrar una feina.

Quan es programa una at i dóna un error "atd is not running", llavors s'ha d'executar l'ordre rcatd restart.

2.7 Connexió remota als sistemes GNU/Linux

La possibilitat de poder-se connectar remotament per mitjà de xarxa des d'un equip a una determinada màquina o node, per manejar-la com si la tinguéssim al davant, és una tasca imprescindible per a l'administració de qualsevol sistema informàtic.

En els sistemes GNU/Linux tenim dues possibilitats per fer aquesta connexió de manera senzilla mitjançant l'arquitectura client/servidor. Es pot fer via Telnet o via SSH (*secure shell*).

La connexió mitjançant el protocol Telnet és una connexió poc segura, ja que totes les dades, inclosos els noms d'usuari i les contrasenyes, viatgen per la xarxa en text pla, sense xifrar.

El fet que la informació viatgi sense xifrar permetria a algú que espiés el tràfic de la xarxa capturar les dades i accedir a la xarxa il·lícitament. Una altra falta de seguretat per la qual no es recomana utilitzar aquest protocol és la manca d'un esquema d'autenticació que permeti assegurar que la comunicació s'estableix entre les màquines adequades i que, per tant, no ha estat interceptada. El protocol Telnet s'utilitza sobretot per a la configuració local d'encaminadors (*routers*).

El protocol SSH treballa de manera similar al protocol Telnet. La diferència principal és que el protocol SSH fa servir tècniques de xifratge que fan que la informació que viatja pel mitjà de comunicació no sigui llegible i que, per tant, cap tercera persona pugui descobrir l'usuari i la contrasenya de la connexió ni tampoc el que s'escriu durant tota la sessió.

El protocol SSH ens permet efectuar múltiples tasques de manera segura, com ara còpies i transferències segures de fitxers mitjançant les ordres scp i sftp. Qualsevol aplicació que utilitzi el protocol TCP es pot fer servir per mitjà d'un túnel segur amb protocol SSH, cosa que proporciona una alternativa potent per crear sistemes VPN. La versió lliure i oberta del protocol SSH, que és de propietat, és l'OpenSSH.

En tots dos casos, Telnet i SSH, la comunicació s'estableix entre servidors i clients. Les màquines a les quals ens volem connectar hauran de tenir instal·lada l'aplicació servidor i les màquines des de les quals ens volem connectar, l'aplicació client. Vegem el procés d'instal·lació i configuració d'un servei SSH en un equip amb l'Ubuntu 9.04 Server Edition.

Per tal d'instal·lar el servei en una màquina, executeu el següent:

```
1 $sudo apt-get install ssh-server
```

Si només voleu instal·lar el client, feu el següent:

```
1 $sudo apt-get install ssh-client
```

Si els voleu instal·lar tot dos, feu el següent:

```
1 $sudo apt-get install ssh
```

Quan el servei SSH s'instal·la es creen un parell de claus, una de pública i una altra de privada, que s'utilitzen per autenticar, en intercanviar-se, tant el client com el servidor.

Abans de connectar-vos a una màquina en producció, hauríeu de fer certes modificacions de seguretat en els fitxers de configuració del servei. En el cas de l'OpenSSH, aquests fitxers són a **/etc/ssh/sshd_config**.

Les modificacions principals per fer més robusta la seguretat de la connexió han de ser les següents:

- Canviar el port de connexió, normalment el 22, per un altre port que no es faci servir. D'aquesta manera s'evitaran atacs a aquest port comú (paràmetre Port).
- Assegurar-se que la versió del protocol utilitzat és la 2 (paràmetre Protocol).
- Modificar el temps de què disposa l'usuari remot per establir la comunicació, que ha de ser tan curt com sigui possible, per tal d'evitar *scripts* que aprofitin aquest temps (paràmetre LoginGraceTime).
- Modificar el nombre d'intents de connexió consecutius, per tal d'evitar atacs de força bruta (paràmetre MaxAuthTries).
- No permetre la connexió de l'usuari primari per evitar *scripts* que utilitzin aquest usuari per esbrinar-ne la contrasenya (paràmetre PermitRootLogin).
- Restringir al màxim el nombre d'usuaris connectats (paràmetre MaxStartups).
- Establir, si és possible, una llista per restringir els usuaris amb permisos per connectar-se remotament (paràmetre AllowUsers).

Per tal que els canvis en el fitxer de configuració tinguin efecte, cal reiniciar el servei:

```
1 $sudo /etc/init.d/ssh restart
```

Una vegada configurat el servidor, per poder connectar-vos remotament des d'una màquina client heu d'utilitzar bàsicament l'ordre següent:

```
1 $ssh -p port usuari@ip_del_ordinador_remot
```

A continuació se us demanarà la contrasenya de l'usuari, que ha d'estar donat d'alta en el sistema remot. Una vegada validats en el sistema, podeu treballar-hi com si fossiu al davant de la màquina remota.

2.8 Monitoratge i manteniment de sistemes GNU/Linux

El monitoratge i el manteniment són els dos processos més importants i necessaris en qualsevol sistema operatiu, sobretot si es tracta de sistemes operatius connectats en xarxa i en producció, per tal de garantir que el sistema funcioni correctament. Els processos de monitoratge i manteniment són complementaris. Per fer-ne un bon manteniment, abans cal fer un monitoratge del sistema per tal de trobar possibles punts febles o colls d'ampolla i solucionar-los.

Coll d'ampolla

Coll d'ampolla fa referència a la situació en la qual la capacitat de processament d'un dispositiu és més gran que la capacitat de transmissió d'informació del bus o de la xarxa als quals es troba connectat el dispositiu.

En moltes situacions es tendeix a no donar la importància que cal al monitoratge dels sistemes, de manera que es produeixen en molts d'aquests casos errors inesperats o pèrdues de dades i de temps irreparables. Hem de tenir clar que el monitoratge del sistema ens permet conèixer les causes i evitar el mal funcionament del sistema, i també implementar les mesures necessàries per millorar-ne el rendiment.

El *monitoratge* és un procés constant que fa referència a la supervisió necessària per a l'execució i la consecució dels objectius del sistema informàtic. És el procés per mitjà del qual ens assegurarem que la configuració del nostre sistema és adequada i eficaç per a les tasques que se li han assignat. D'aquesta manera s'evita que hi hagi possibles desviacions.

El monitoratge pot detectar les interferències que hi pugui haver en el funcionament del sistema. Gràcies a aquest procés, l'estructuració o les polítiques de seguretat, de manteniment i de configuració del sistema es poden corregir.

Abans de poder fer el monitoratge del sistema, heu de saber de quins recursos disposeu per tal de poder-los controlar. Tots els sistemes operatius connectats a la xarxa disposen dels recursos següents:

- CPU, capacitat de processament de dades, depèn en gran manera del tipus i de la quantitat de processadors de la màquina.
- Memòria, quantitat de dades que es poden emmagatzemar en la memòria volàtil (RAM o swap) per ser processades.
- Emmagatzematge, capacitat d'emmagatzematge de dades permanents del sistema; es pot tractar de discos durs o de dispositius removibles.
- Amplada de banda, quantitat de dades que es poden enviar a través d'una connexió de xarxa del sistema, generalment la targeta de xarxa, en un moment determinat.

Podeu simplificar el concepte de monitoratge del sistema de manera que només obtingueu informació relativa a la utilització d'un o més recursos d'aquest sistema. No obstant això, rarament el procés de monitoratge és tan simple. Heu de tenir en compte la informació de manera conjunta per tal de fer una anàlisi general del funcionament del sistema.

Cal examinar en cada cas la situació del sistema que voleu monitorar. En general, podeu trobar dos escenaris:

- El sistema experimenta problemes de rendiment i el voleu millorar.
- El sistema funciona bé i voleu que continuï així.

En ambdues opcions haureu d'analitzar les dades extretes del procés de monitoratge per tal d'aconseguir el vostre objectiu. Heu de tenir en compte que per a cadascun dels recursos anteriors podeu obtenir una gran quantitat de dades.

El monitoratge del rendiment del sistema sovint és un procés iteratiu. Aquests passos es repeteixen diverses vegades fins que s'aconsegueix el millor rendiment possible. La raó principal és que els recursos del sistema i la utilització d'aquests recursos tendeixen a estar molt relacionats, cosa que significa que sovint l'eliminació d'un coll d'ampolla en descobreix un altre.

2.8.1 Monitoratge de la CPU

Fer el monitoratge de la CPU significa determinar el percentatge d'utilització d'aquesta unitat per les diferents tasques efectuades.

El moment idoni per examinar detalladament les dades d'ús de la CPU i començar a determinar en quin punt es consumeix la major part de la capacitat de processament és quan el percentatge d'ús de la unitat arriba al 100%.

Algunes de les estadístiques més populars d'utilització de la CPU són les següents:

Usuari contra Sistema

Es té en compte el percentatge de temps que la CPU dedica a processar tasques a escala d'usuari en oposició a les tasques a escala de sistema. L'anàlisi d'aquests percentatges d'ocupació de la CPU pot indicar si la càrrega d'un sistema es deu principalment a les aplicacions que s'estan executant o a la sobrecàrrega del sistema operatiu. Que hi hagi percentatges de processament alts a escala d'usuari tendeix a ser bo (voldrà dir que els usuaris experimenten un rendiment satisfactori). En canvi, que hi hagi percentatges de processament alts a escala de sistema tendeix a apuntar problemes que poden ser generats per diverses causes, i per trobar la o les causes reals de saturació de la CPU cal investigar el funcionament del sistema més a fons.

Canvis de context

Un canvi de context ocorre quan la CPU atura l'execució d'un procés i comença a executar-ne un altre. Com que cada context requereix que el sistema operatiu prengui el control de la CPU, els canvis de context excessius i els nivells alts de consum de la CPU a escala de sistema tendeixen a estar molt relacionats.

Interrupcions

Les interrupcions són situacions en què el processament que fa la CPU canvia de cop i volta. Generalment, les interrupcions ocorren a causa de l'activitat del maquinari, com ara un dispositiu d'entrada i sortida que acaba una operació, o del programari, com ara interrupcions de programari que controlen el processament d'una aplicació. Un excés d'interrupcions per part d'un dispositiu o una aplicació podria determinar que funcionessin incorrectament.

Processos executables

Un procés pot tenir diferents estats. Quan l'estat d'un procés es torna executable

vol dir que aquest procés necessitarà temps de CPU per fer la seva tasca. Com que només hi pot haver un procés en execució en cada moment en la CPU, la resta de processos executables estaran en estat d'espera. D'aquesta manera, mitjançant el monitoratge del nombre de processos executables és possible determinar com de compromesa està la CPU del sistema.

2.8.2 Monitoratge de la memòria

La memòria del sistema és una àrea en què hi ha una gran quantitat d'estadístiques de rendiment.

Les estadístiques següents representen una descripció de les estadístiques d'administració de memòria més utilitzades:

Pàgines dintre/fora

Aquestes estadístiques fan possible mesurar el flux de pàgines des de la memòria del sistema als dispositius d'emmagatzematge massiu (normalment, unitats de disc). Altes taxes d'aquestes estadístiques poden representar que el sistema no disposa de gaire memòria física i que està consumint més recursos del sistema en moure les pàgines dintre i fora de memòria que no pas en executar aplicacions.

Pàgines actives/inactives

Aquestes estadístiques mostren que les pàgines residents en memòria s'estan utilitzant. Una falta de pàgines inactives pot apuntar una mancança de memòria física.

Pàgines lliures, compartides, en memòria intermèdia o en memòria cau

Aquestes estadístiques proporcionen detalls addicionals sobre les estadístiques més simples de pàgines actives/inactives. Mitjançant aquestes estadístiques és possible determinar la barreja general d'utilització de memòria.

Intercanvi dintre/fora

Aquestes estadístiques mostren el comportament general de la memòria d'intercanvi del sistema (*swap*). Taxes excessives poden indicar que no hi ha gaire memòria física.

2.8.3 Monitoratge de l'emmagatzematge

El monitoratge de l'emmagatzematge normalment té lloc en dos nivells diferents:

- Monitorar l'espai en disc.
- Monitorar els problemes de rendiment relacionats amb l'emmagatzematge.

Podeu tenir en compte les estadístiques següents a l'hora de monitorar l'emma-gatzematge:

Espai lliure

Probablement, l'espai lliure és el recurs que heu de vigilar més de prop. Heu de procurar que el vostre sistema sempre disposi d'una quantitat adequada d'emma-gatzematge per tal de cobrir-ne les necessitats.

Estadístiques relacionades amb el sistema d'arxius

Aquestes estadístiques subministren detalls addicionals sobre el percentatge d'es-pai lliure. Tindrem en consideració, per exemple, el nombre d'arxius i directoris, la grandària mitjana dels arxius, etc. Aquestes estadístiques fan possible configu-rar el sistema perquè tingui el millor rendiment, ja que, per exemple, la càrrega d'E/S imposada per un sistema d'arxius ple de molts petits arxius no és la mateixa que la càrrega imposada per un sistema d'arxius ple amb un únic arxiu enorme.

Transferències per segon

Aquesta estadística constitueix una bona manera de determinar si s'estan arribant a les limitacions de transferència de senyals d'un dispositiu en particular.

Lectures/escriptures per segon

Són estadístiques amb un desglossament més detallat de les transferències per segon. Aquestes estadístiques ens permeten entendre millor la naturalesa de les càrregues d'E/S que està experimentant un dispositiu d'emmagatzematge. Això pot ser crític, ja que algunes tecnologies d'emmagatzematge tenen característiques de funcionament molt diferents entre operacions de lectura i escriptura.

2.8.4 Monitoratge de la xarxa

El monitoratge de la xarxa s'ha de centrar en dos aspectes importants:

- Monitorar el rendiment de la xarxa, taxa de transferència, col·lisions, etc.
- Monitorar la seguretat de la xarxa, accessos indeguts, atacs al sistema, etc.

De vegades aquests dos aspectes van lligats, ja que pot ser que un atac al sistema afecti el rendiment. Tant si teniu una LAN sense accés des d'Internet com si oferiu qualsevol tipus de servei a l'exterior, hem de controlar que tant els paràmetres de rendiment com els de seguretat estiguin dins dels límits establerts per la política del sistema.

Podeu tenir en compte les estadístiques següents per fer el monitoratge de la xarxa:

Bytes rebuts/enviats

Les estadístiques de la interfície de xarxa proporcionen un indicatiu de la utilitza-

ció de l'amplada de banda de la xarxa.

Comptes i taxes d'interfície

Aquestes estadístiques donen indicacions de col·lisions excessives, errors de transmissió/recepció i altres. Amb l'ús d'aquestes estadístiques és possible resoldre problemes de la xarxa abans d'utilitzar les eines de diagnòstic de la xarxa més comunes.

És aconsellable utilitzar diverses eines de diagnòstic de xarxa que és complementin mútuament. La gran majoria de les eines actuals generen informes, gràfics i/o registres. L'anàlisi i la interpretació d'aquests elements us proporcionarà la informació necessària per gestionar correctament el sistema en xarxa. És a dir, les analisis de la informació obtinguda us ajudaran a prendre decisions sobre possibles canvis, modificacions o rectificacions de la topologia de xarxa i dels sistemes operatius que hi hagi.

A tall de resum de l'apartat de monitoratge, cal dir que heu de ser conscients que les estadístiques d'utilització de la CPU poden acabar apuntant un problema en el subsistema d'E/S o que les estadístiques d'utilització de memòria poden indicar que hi ha un defecte en una aplicació.

Per tant, quan se supervisa el funcionament del sistema, no és possible examinar una estadística de manera totalment aïllada. Només és possible extreure informació significativa de qualsevol característica de rendiment mitjançant l'examen del quadre complet.

2.8.5 Eines i ordres de monitoratge

El GNU/Linux incorpora nombroses ordres de monitoratge en el sistema. A més, en el mercat també hi ha moltes aplicacions de codi lliure que permeten fer el monitoratge dels sistemes.

A continuació, veurem algunes de les ordres i les eines lliures més utilitzades en el monitoratge de sistemes:

Ordres de monitoratge

Els sistemes GNU/Linux incorporen moltes ordres que tenen la funció de proporcionar dades pràctiques per al monitoratge del sistema. A continuació, en veurem algunes de les més utilitzades.

Ordre top

L'ordre top mostra una llista dels processos del sistema. Aquesta llista s'actualitza freqüentment, de manera que proporciona informació en temps real sobre el funcionament del sistema. Els processos s'ordenen per l'ús de CPU i mostren el PID,

l'usuari, el tant per cent de CPU consumit o el tant per cent de memòria utilitzada, entre altres dades dels processos. L'ordre top és molt útil per als administradors de sistema, ja que mostra els usuaris que consumeixen una quantitat específica de CPU en un moment determinat en temps real. En la figura 2.10 veiem un exemple de les dades que es mostren en executar aquesta ordre.

FIGURA 2.10. Mostra de l'execució de l'ordre top

```

top - 11:27:51 up 32 min,  2 users,  load average: 0.09, 0.10, 0.15
Tasks: 120 total,   2 running, 118 sleeping,   0 stopped,   0 zombie
Cpu(s): 0.7%us, 0.0%sy, 0.0%ni, 99.0%id, 0.0%wa, 0.3%hi, 0.0%ssi, 0.0%st
Mem: 509448k total, 419444k used, 90004k free, 32680k buffers
Swap: 409616k total, 10660k used, 398956k free, 239984k cached

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM TIME+ COMMAND
2735 root      20   0 39724 16m 6588 S  0.7  3.3  0:14.18 Xorg
 14 root      15  -5     0     0  0 S  0.3  0.0  0:01.41 ata/0
  1 root      20   0 3084 596 540 S  0.0  0.1  0:01.31 init
  2 root      15  -5     0     0  0 S  0.0  0.0  0:00.00 kthreadd
  3 root      RT  -5     0     0  0 S  0.0  0.0  0:00.00 migration/0
  4 root      15  -5     0     0  0 S  0.0  0.0  0:00.00 ksoftirqd/0
  5 root      RT  -5     0     0  0 S  0.0  0.0  0:00.00 watchdog/0
  6 root      15  -5     0     0  0 S  0.0  0.0  0:00.13 events/0
  7 root      15  -5     0     0  0 S  0.0  0.0  0:00.00 khelper
  8 root      RT  -5     0     0  0 S  0.0  0.0  0:00.00 kstop/0
  9 root      15  -5     0     0  0 S  0.0  0.0  0:00.00 kintegrityd/0
 10 root     15  -5     0     0  0 S  0.0  0.0  0:00.10 kblockd/0
 11 root     15  -5     0     0  0 S  0.0  0.0  0:00.00 kacpid
 12 root     15  -5     0     0  0 S  0.0  0.0  0:00.00 kacpi_notify
 13 root     15  -5     0     0  0 S  0.0  0.0  0:00.00 cqueue

```

Ordre vmstat

Amb vmstat és possible obtenir una vista general dels processos, la memòria, l'espai d'intercanvi, les entrades i les sortides i l'activitat de la CPU mitjançant línies, tal com podem veure en la figura 2.11.

FIGURA 2.11. Visió de l'execució de vmstat

```

procs      --memory--  --swap--  --io--  -system-  --cpu--
r b swpd free buff cache si so bi bo in cs us sy id wa
4 0 10660 89880 32696 239992 0 4 200 54 84 201 6 4 87 3

```

La informació que proporciona l'ordre vmstat és la següent:

1. Informació sobre els **processos Procs**:

- **r**: Indica el nombre de processos en espera per temps d'execució en la CPU.
- **b**: Indica el nombre de processos adormits que esperen un recurs.

2. Informació sobre la **memòria Memory**:

- **swpd**: Indica la quantitat de memòria virtual utilitzada.
- **free**: Mostra la quantitat de memòria sense utilitzar.

- **buff:** Mostra la quantitat de memòria utilitzada com a memòria intermèdia (*buffer*).
- **cache:** Indica la quantitat de memòria utilitzada com a memòria cau (*cache*).
- **inact:** Fa referència a la quantitat de memòria inactiva (amb l'opció *-a*).
- **active:** Mostra la quantitat de memòria activa (amb l'opció *-a*).

3. Informació sobre l'àrea d'intercanvi Swap:

- **si:** Mostra la quantitat de memòria d'intercanvi utilitzada des del disc dur o d'entrada (/s).
- **so:** Mostra la quantitat de memòria d'intercanvi utilitzada cap al disc dur o de sortida (/s).

4. Informació sobre els dispositius d'entrada i sortida IO:

- **bi:** Blocs rebuts des d'un dispositiu (blocks/s).
- **bo:** Blocs enviats a un dispositiu (blocks/s).

5. Informació sobre el sistema System:

- **in:** Mostra el nombre d'interrupcions per segon, incloent-hi el rellotge del sistema.
- **cs:** Indica el nombre de canvis de context per segon.

6. Informació sobre la CPU, són percentatges sobre el temps total de CPU:

- **us:** Temps consumit executant codi que no pertany al nucli del sistema (temps d'usuari).
- **sy:** Temps consumit executant codi que pertany al nucli del sistema (temps de sistema).
- **id:** Temps consumit funcionant en buit.
- **wa:** Temps consumit esperant operacions d'E/S.

Ordre tcpdump

La utilitat principal de l'eina **tcpdump** és analitzar el trànsit que circula per la xarxa. Aquesta eina ens permet capturar i mostrar en temps real els paquets transmesos i rebuts per mitjà de la interfície de xarxa de l'equip en el qual s'està executant. El tcpdump és un detector (*sniffer*) i funciona en la majoria dels sistemes operatius UNIX: GNU/Linux, Solaris, BSD, Mac OS X, HP-UX i AIX, entre altres. En aquests sistemes, el tcpdump utilitza la biblioteca libpcap per capturar els paquets que circulen per la xarxa.

Ús de l'ordre tcpdump

Alguns protocols com Telnet i HTTP no xifren les dades que envien en la xarxa. Un usuari que tingués el control d'un encaminador per mitjà del qual circulés trànsit no xifrat podria utilitzar el tcpdump per aconseguir contrasenyes o altres informacions.

Les utilitats principals són les següents:

- Depurar aplicacions que utilitzen la xarxa per comunicar-se.
- Depurar la xarxa mateixa.

- Capturar i llegir dades enviades per altres usuaris o ordinadors.

Normalment, el tcpdump s'utilitza amb filters que determinen les dades que s'han de capturar. Per exemple:

Capturar trànsit amb l'adreça 192.168.1.1 d'origen

```
1 $sudo tcpdump src host 192.168.1.1
```

Capturar trànsit amb l'adreça 192.168.1.2 de destinació

```
1 $sudo tcpdump host 192.168.1.2
```

Capturar trànsit amb destinació a l'adreça MAC 20:60:A1:AB:70:22

```
1 $sudo tcpdump ether dst 20:60:A1:AB:70:22
```

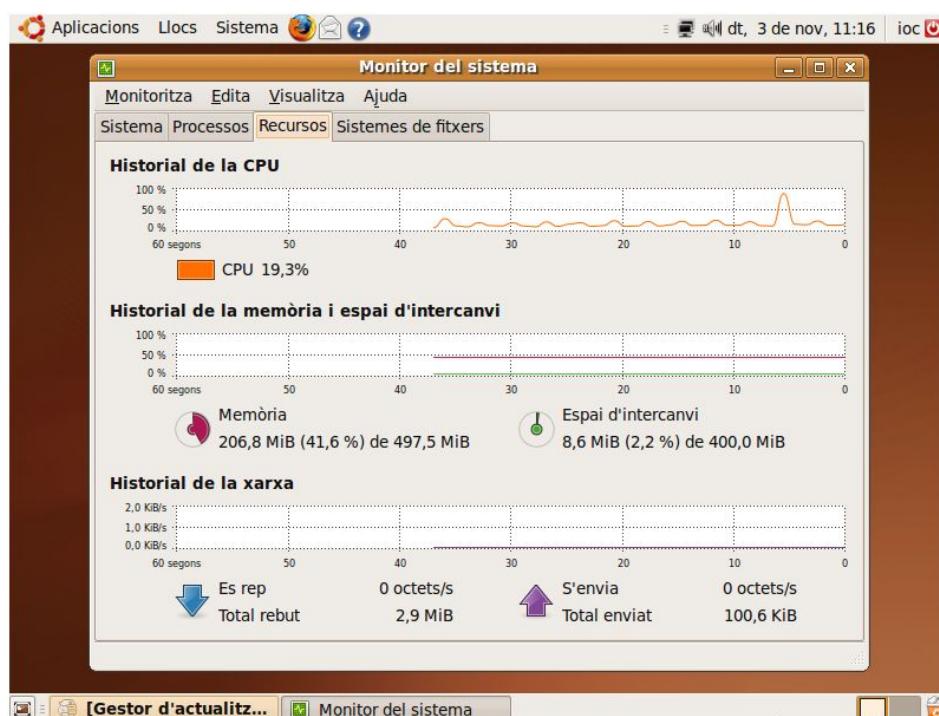
Aplicacions de monitoratge

Hi ha moltes aplicacions per als sistemes GNU/Linux que tenen la funció de mostrar gràficament dades útils per al monitoratge del sistema. A continuació, en veurem algunes de les més utilitzades.

Monitor del sistema

L'Ubuntu Desktop Edition incorpora per a l'escriptori GNOME una aplicació de monitoratge coneguda com a *monitor del sistema*. El monitor del sistema el podem trobar en el menú *Sistema > Administració > Monitor del sistema* (vegeu figura 2.12).

FIGURA 2.12. Monitor del sistema a Ubuntu



Tal com mostra la imatge anterior, aquesta aplicació ens permet controlar l'ús que

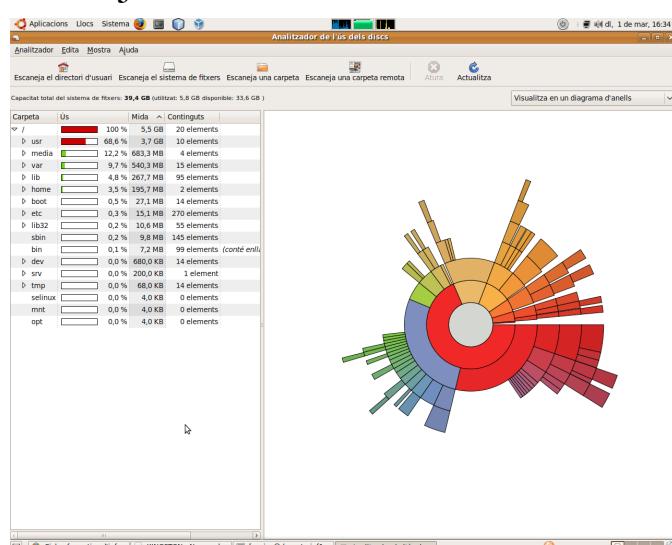
s'està fent dels recursos del sistema, la CPU, la memòria, el disc dur o el trànsit d'interfície de xarxa, entre altres, de manera gràfica.

Baobab

És una altra eina molt interessant que també està incorporada en la versió 9.04 de l'Ubuntu i que permet visualitzar de manera gràfica l'espai ocupat en el disc dur. Amb el baobab podem veure facilment quines carpetes ocupen més espai i desplegar l'arbre de directoris per veure la grandària exacta de cadascun dels subdirectoris. L'eina també disposa d'un cercador d'arxius i detecta en temps real els canvis que es fan en el sistema de fitxers, també el muntatge i el desmuntatge d'unitats.

El **Baobab** és molt útil per veure l'espai que ocupa cada usuari en la màquina o determinar quines carpetes s'haurien de netejar primer per fer espai en el disc dur. A més, s'integra amb els scripts del **Nautilus** per poder-lo llançar mitjançant el botó secundari del ratolí des de qualsevol carpeta. En podem veure l'aspecte en la figura 2.13.

FIGURA 2.13. Pantalla de Baobab



Detectors (*sniffers*)

Un packet sniffer és un programa de captura de trames de xarxa. És habitual que, per qüestions de topologia de xarxa i de material, diversos ordinadors i dispositius de xarxa comparteixin el mitjà de transmissió (cable coaxial, UTP, fibra òptica, etc.). Això possibilita que un ordinador capturi les trames d'informació que no van destinades a aquesta màquina.

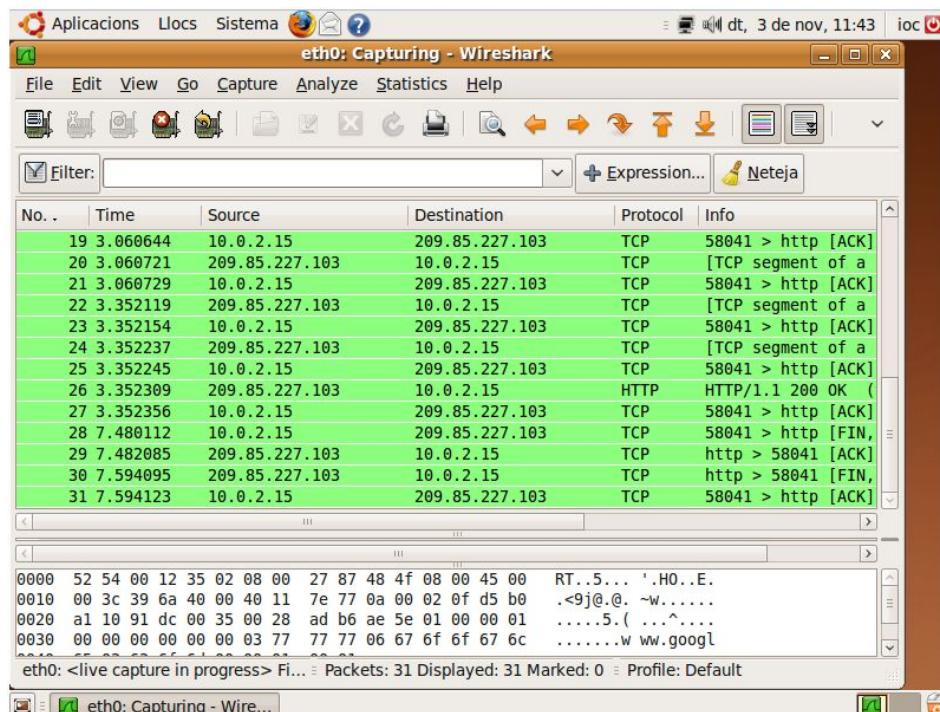
Per aconseguir capturar la informació no destinada a l'ordinador en què s'executa, el detector posa la targeta de xarxa en un estat conegut, com ara en “mode promiscu”. D'aquesta manera, en la capa d'enllaç de dades, les trames no destinades al MAC de la targeta no es descarten i es pot capturar tot el trànsit que viatja per la xarxa. Els packet sniffers tenen diversos usos, com fer el

monitoratge de xarxes per detectar i analitzar fallades o fer enginyeria inversa de protocols de xarxa. També és habitual fer-los servir amb fins malicioses, com furtar contrasenyes, interceptar missatges de correu electrònic, espiar converses de xat, etc.

Els usos principals que pot tenir són els següents:

- Captura automàtica de contrasenyes enviades en clar i noms d'usuari de la xarxa. Moltes vegades els pirates utilitzen aquesta capacitat per atacar sistemes *a posteriori*.
- Conversió del trànsit de xarxa en un format intel·ligible pels humans.
- Anàlisi de fallades per descobrir problemes en la xarxa, com ara per quina raó l'ordinador A no pot establir una comunicació amb l'ordinador B.
- Mesurament del trànsit, mitjançant el qual és possible descobrir colls d'ampolla en algun lloc de la xarxa.
- Detecció d'intrusos, tot i que hi ha programes específics anomenats IDS (*intrusion detection system*, sistema de detecció d'intrusos). Aquests programes són pràcticament detectors amb funcionalitats específiques.
- Creació de registres de xarxa, de manera que els intrusos no puguin detectar que són investigats.
- Als desenvolupadors, en aplicacions client-servidor, els permet analitzar la informació real que es transmet per la xarxa.

FIGURA 2.14. Exemple de Wireshark



Hi ha una gran quantitat de packet sniffers per a Ethernet/LAN. Alguns dels més coneguts són el Wireshark (Ethereal), l'Ettercap i el Tcpdump. També n'hi ha

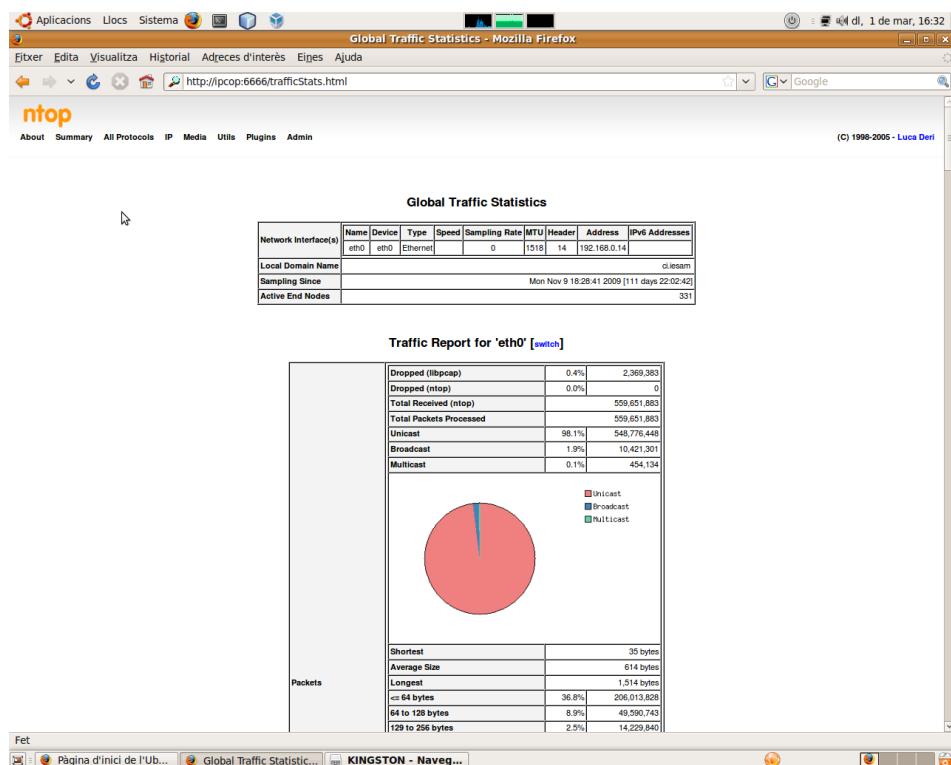
molts per a xarxes sense fil, com el Kismet o el Network Stumbler. En la figura 2.14 es mostra l'aspecte de l'eina Wireshark:

Ntop

L'Ntop (Network top) permet el monitoratge en temps real dels usuaris i les aplicacions que consumeixen recursos de xarxa en un moment concret. També possibilita la detecció de configuracions incorrectes d'algún equip o servei.

L'Ntop està desenvolupat dins del projecte GNU i disposa d'un microservidor web que permet veure la sortida de manera remota amb qualsevol navegador. Ho podem veure en la figura 2.15. Els protocols que l'Ntop pot monitorar són els següents: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios. Dins del TCP/UDP, és capaç d'agrupar-los per FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS i X11. El programari d'aquesta eina està desenvolupat per a plataformes GNU/Linux i Windows.

FIGURA 2.15. Exemple d'Ntop



Nagios

El Nagios és un sistema de codi obert de monitoratge de xarxes àmpliament utilitzat que vigila els equips (maquinari) i els serveis (programari) que s'especifiquen en la configuració. Avisa si el comportament d'aquests elements no és adequat.

Entre les característiques principals d'aquest sistema hi ha les següents:

- Monitoratge de serveis de xarxa (SMTP, POP3, HTTP, SNMP, etc.).
- Monitoratge dels recursos de sistemes maquinari (càrrega del processador, ús dels discos i memòria, estat dels ports, etc.).

- Independència dels sistemes operatius.
 - Possibilitat de monitoratge remot mitjançant túNELS SSL xifrats o SSH.
 - Possibilitat de programar *plugins* específics per a sistemes nous.

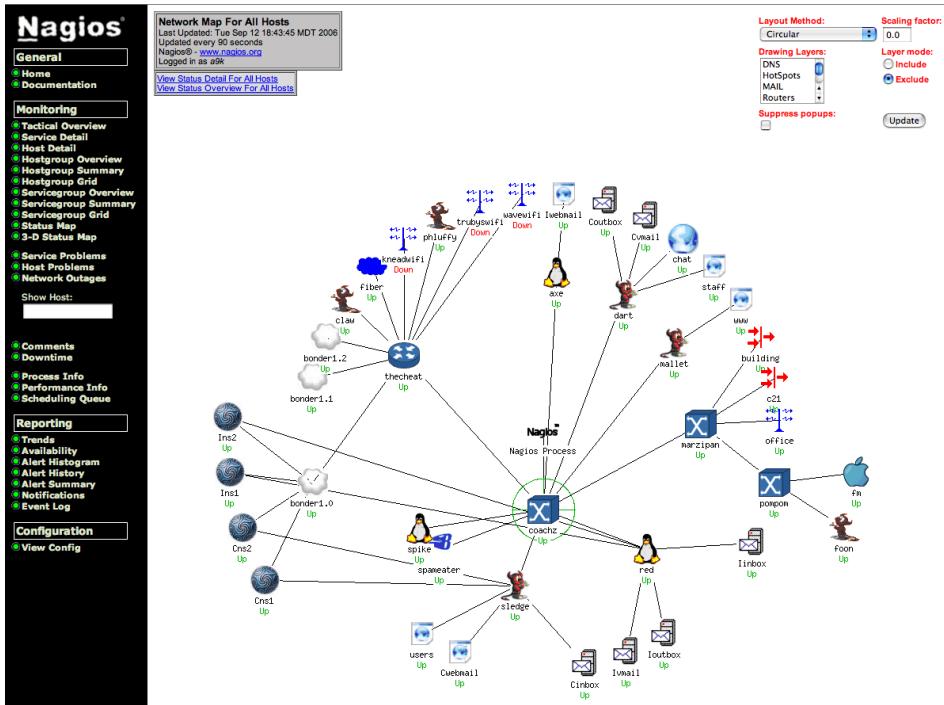
Es tracta d'un programari que proporciona una gran versatilitat per consultar pràcticament qualsevol paràmetre d'interès d'un sistema i genera alertes quan aquests paràmetres excedeixen dels marges definits. Els administradors poden rebre aquestes alertes mitjançant correu electrònic i missatges SMS.

A més, permet la visualització de l'estat de la xarxa en temps real per mitjà d'interfície web, amb la possibilitat de generar informes i gràfics de comportament dels sistemes que són objecte de monitoratge. Es mostra en la figura 2.16. A més, el Nagios permet la visualització del llistat de notificacions enviades, l'historial de problemes, els arxius de registres, etc.

El Nagios va ser originalment dissenyat per ser executat en el GNU/Linux, però també funciona correctament en altres sistemes derivats de l'UNIX. L'únic aspecte negatiu pot ser la complexitat a l'hora d'establir els paràmetres de configuració i donar d'alta tots els equips que es volen monitorar.

El Nagios està llicenciat sota la GNU General Public License Version.

FIGURA 2.16. Exemple de Nagios



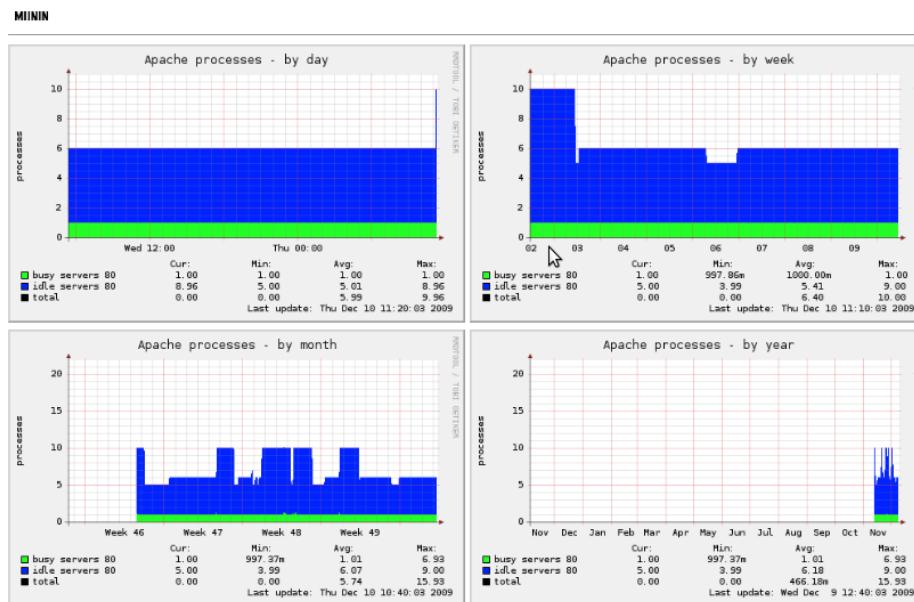
Munin

El Munin és una aplicació de monitoratge del sistema i de la xarxa que presenta les dades de manera gràfica per mitjà d'una interfície web. El Munin és en els dipòsits del Debian, cosa que fa que sigui molt senzill instal·lar-lo en els derivats d'aquest sistema.

Amb Munin es pot fer fàcilment el monitoratge del rendiment dels ordinadors, les xarxes i els serveis. A més, un gran nombre de connectors de control estan disponibles a Munin.

El Munin utilitza l'eina RRDtool, està escrit en Perl i funciona amb l'arquitectura client/servidor, de manera que el servidor es connecta a tots els clients en intervals regulars i els demana les dades. A continuació, emmagatzema les dades en els arxius RRD i si cal actualitza els gràfics. En la figura 2.17 veiem un exemple de les dades que ofereix.

FIGURA 2.17. Exemple de Munin



2.9 Documentació del sistema

La documentació de sistemes és el conjunt d'informació que ens diu què fan els sistemes, com ho fan i per a qui ho fan. La documentació consisteix en el material que explica les característiques tècniques i les operacions d'un sistema.

També considerem que és documentació el registre físic, generalment per escrit, que conté els elements següents: polítiques i normes referents al desenvolupament, la implantació, l'operació i el manteniment del sistema.

Documentar els processos i les incidències que sorgeixen durant la instal·lació, la configuració, el manteniment i el monitoratge del sistema és una tasca fonamental en qualsevol sistema. La documentació és essencial per proporcionar informació d'un sistema a qui l'hagi d'utilitzar o mantenir. La documentació també és necessària per permetre l'auditoria del sistema i per ensenyar als usuaris com interactuar-hi i als operadors com fer-lo funcionar. La documentació ha de ser

una tasca contínua per a qualsevol tècnic que treballi amb sistemes informàtics.

Hem de documentar, principalment, els elements següents:

Polítiques

Les polítiques s'escriuen per formalitzar i aclarir els criteris a l'hora de gestionar el sistema. Aquestes polítiques estableixen la manera com es manegen les sol·licituds de recursos o d'assistència. La naturalesa, l'estil i el mètode de les polítiques varien segons l'organització.

Procediments

Els procediments són seqüències de passos sobre accions que s'han de fer per arribar a una tasca determinada. Els procediments a documentar inclouen procediments de còpies de seguretat, procediments d'administració de comptes d'usuaris, procediments d'informes de problemes, etc.

Modificacions

Les modificacions d'alguns aspectes del sistema constitueixen un element fonamental i constant en el manteniment dels sistemes. Per exemple, configurar el sistema per a un màxim rendiment, ajustar *scripts*, modificar arxius de configuració, etc. Tots aquests canvis haurien d'estar documentats d'alguna manera. En cas contrari, podem trobar molta confusió sobre els canvis que es van fer uns mesos enrere. Algunes organitzacions utilitzen mètodes més complexos per fer un seguiment dels canvis, però en molts casos només cal una simple revisió històrica al començament de l'arxiu que s'està modificant. Com a mínim, cada entrada en la revisió històrica hauria de contenir el següent:

- El nom o les inicials de la persona que executa el canvi.
- La data en què es va fer el canvi.
- La raó del canvi.

A l'hora d'elaborar la documentació del sistema informàtic, podem utilitzar diversos mètodes o suports com documents de textos, documents gràfics, diagrames, wikis (també es poden combinar). Sempre que sigui possible utilitzarem captures de pantalla, informes i registres dels sistemes o de les eines emprades.

3. Serveis de directori

Per assolir els coneixements adequats necessiteu conèixer els conceptes de *directori* i *servei de directori*. A més, convé saber en què consisteix, per a què s'utilitza i com funciona el protocol de servei de directori més utilitzat en els sistemes lliures, l'LDAP. Per poder desenvolupar tots els coneixements adquirits cal instal·lar, configurar i administrar l'OpenLDAP, el projecte de codi obert que proporciona tant el servidor com el client del protocol LDAP. Convé conèixer diverses eines gràfiques per administrar el servei de directori i veure un exemple d'instal·lació i funcionament d'una d'aquestes eines, concretament la phpLDAPAdmin.

3.1 Què és un directori?

Per entendre bé què és un directori en l'àmbit dels sistemes operatius, s'agafa com a exemple un directori clàssic, com ara una agenda telefònica. En una agenda telefònica s'emmagatzema de manera organitzada diversa informació sobre les persones que interessen: nom, cognoms, adreça, número de telèfon, empresa, etc.

Aquesta informació s'estructura en diversos camps que estan relacionats. Així, per exemple, si es busca el cognom d'una persona, s'obté un o uns telèfons que hi estan associats, com en el cas dels registres d'una base de dades.

La finalitat dels directoris clàssics és, per tant, emmagatzemar físicament la informació de manera estructurada per tal de facilitar l'accés a les dades necessàries i l'actualització.

Per simplificar, es pot dir que la finalitat dels directoris electrònics és la mateixa que la dels clàssics, tot i que el tipus d'informació que s'hi emmagatzema, la manera de treballar-hi i el suport físic que tenen és diferent. Aquest tipus de directoris estan orientats a emmagatzemar, en algun suport informàtic, informació relativa a una o diverses xarxes d'ordinadors.

Un *directori* és una base de dades especialitzada que emmagatzema informació sobre els recursos o les entitats que hi ha en una xarxa, com ara usuaris, ordinadors o impressores, i la posa a disposició dels usuaris de la xarxa.

Així doncs, la informació que s'emmagatzema en els directoris està relacionada amb la ubicació i les propietats dels objectes que hi ha en una xarxa informàtica.

La funció principal d'un directori electrònic és tenir la informació organitzada de manera estructurada perquè des dels diferents llocs de la xarxa que disposen d'un

Directori enfocat de directori de sistema

No heu de confondre aquest tipus de directori amb el directori del sistema d'arxius, que serveix per agrupar arxius dins d'un suport d'emmagatzematge.

servi de directori es pugui accedir a les dades que s'hi emmagatzemen i actualitzar-les. El directori permet que aquestes accions es facin de manera ràpida, eficient i segura.

Hi ha diferents tipus de directoris en funció de la informació que s'hi emmagatzema, de l'àmbit en què s'implementa i del servei de directori que s'utilitza.

3.2 Que és un servei de directori?

Directori enfront de servei de directori

Podeu tenir dubtes sobre la diferència que hi ha entre un directori i un servei de directori, tot i que moltes publicacions no fan cap distinció entre l'un i l'altre. Convé separar aquests dos conceptes per entendre'ls millor.

Una vegada explicat el concepte de directori, queda més clar en què consisteix un servei de directori.

Un *servei de directori* constitueix un conjunt d'elements, format per programari i maquinari, que treballen plegats per emmagatzemar, organitzar i gestionar la informació referent als usuaris i els recursos d'una xarxa. Els serveis de directori actuen com una capa d'abstracció entre els usuaris i els recursos compartits i permeten als administradors gestionar l'accés dels usuaris als recursos de la xarxa.

Per tant, el directori constitueix la base de dades en què s'emmagatzema la informació, mentre que el servei de directori és la infraestructura física i lògica que permet gestionar les dades del directori.

3.2.1 Què no és un servei de directori?

Encara que coneuem en què consisteix un servei de directori, és necessari tenir clar quin tipus de programes o aplicacions són un servei de directori i quins no. Per evitar confusions cal saber les diferències que hi ha entre un servei de directori i altres programes o serveis. Aquestes diferències no sols rauen en el tipus de programes o serveis, sinó també en la seva estructura i el seu mode de funcionament. Comparem, doncs, alguns d'aquests programes o serveis que sovint es confonen amb un servei de directori.

Serveis de directori enfront de sistemes gestors de bases de dades

S'ha dit que un directori és una base de dades. Cal recordar, però, que és especialitzada i que, per tant, les característiques que té són diferents a les d'una base de dades relacional de propòsit general. Les diferències principals que hi ha són les següents:

- Els serveis de directori **estan optimitzats per a operacions de lectura**, mentre que les bases de dades convencionals estan optimitzades per a

operacions de lectura i escriptura.

- Els serveis de directori estan **optimitzats per emmagatzemar informació relativament estàtica**, de manera que no és recomanable emmagatzemar-hi informació que es modifiqui freqüentment.
- Les dades que hi ha en els serveis de directori segueixen una **estructura totalmente jeràrquica**. A vegades aquest tipus d'estructura és més problemàtica que l'estructura relacional, ja que fa que sigui més complicat establir relacions entre objectes de la base de dades. Normalment, les relacions s'hi han d'establir de manera explícita mitjançant llistes d'objectes. Actualment, però, tot i que predominen les bases de dades relacionals, cada vegada hi ha més dissenys de bases de dades jeràrquiques (bases de dades orientades a objectes, XML, etc.).
- Els directoris **no suporten transaccions**. Les *transaccions* són operacions implementades generalment en els sistemes gestors de les bases de dades que permeten controlar l'execució d'una operació complexa, de manera que aquesta operació es completa totalment o no s'executa. Normalment, el tipus d'informació que s'emmagatzema en un directori no requereix una consistència tan estricta com la informació que s'emmagatzema en les bases de dades convencionals. Per exemple, es considera acceptable que l'adreça d'una persona no estigui actualitzada de manera temporal.
- A diferència de les bases de dades comunes, en els directoris hi pot haver **atributs multivalorats**. És a dir, que dins d'un mateix camp s'emmagatzemin múltiples valors vàlids. Per exemple, múltiples números de telèfon emmagatzemats en el camp *telèfon*.
- La majoria de les bases de dades convencionals utilitzen **el llenguatge de consulta SQL**, que permet desenvolupar funcions de consulta i actualització complexes a costa de la grandària i la complexitat de l'aplicació. Els serveis de directori basats en l'LDAP, per exemple, utilitzen un protocol simplificat i optimitzat que es pot utilitzar per construir aplicacions simples i petites.

En general, **els patrons de disseny de les bases de dades relacionals no són aplicables als serveis de directori**.

Serveis de directori enfront de sistemes de fitxers

Les diferències fonamentals entre els serveis de directori i els sistemes de fitxers són les següents:

- Els directoris **estan optimitzats per emmagatzemar petits fragments d'informació que es poden estructurar com a entrades amb diferents atributs**. En canvi, els sistemes de fitxers contenen arxius de diverses grandàries.

- Els sistemes de fitxers permeten **accedir a un fitxer i, una vegada a dins, posicionar-se** en un determinat punt. En canvi, els directoris només permeten accedir a un atribut i, una vegada a dins, no hi ha manera de posicionar-se en cap punt. Per tant, s'ha de llegir completament.

Serveis de directoris enfocats en serveis web

Hi ha moltes aplicacions basades en el servei web, però aquest servei està **centralitzat a proporcionar una interfície d'usuari agradable**. El servei web en cap moment posseeix les capacitats de cerca que té el servei de directori.

Si voleu que els usuaris accedeixin a la informació que hi ha en una base de dades, segurament el servei web és la millor elecció. Tanmateix, **si voleu que una gran varietat d'aplicacions puguin accedir a la informació, haureu d'utilitzar un servei de directori**.

Serveis de directoris enfocats en serveis DNS

El servei DNS s'encarrega de traduir noms de domini a adreces IP, i a l'inrevés. Aquest servei té una lleugera similitud amb el servei de directori, ja que tots dos proporcionen una interfície d'accés a una base de dades jeràrquica. Tanmateix, difereixen en altres aspectes, com ara els següents:

- Els serveis DNS estan optimitzats per a la transformació de noms d'ordinadors a adreces IP, mentre que els serveis de directori estan optimitzats de manera més general.
- La informació emmagatzemada en el servei DNS té una estructura fixa, mentre que el servei de directori sol permetre l'estensió d'aquesta estructura.
- Els serveis DNS operen amb protocols no orientats a connexió (UDP), mentre que els serveis de directori soelen utilitzar protocols orientats a connexió (TCP).

3.2.2 Utilitats d'un servei de directori

Algunes de les utilitats principals dels serveis de directori són la cerca i gestió d'informació dins d'una xarxa i el fet de garantir la seguretat d'accés a la xarxa mitjançant el seu ús per a l'autenticació d'usuaris. De les seves utilitats principals gairebé la més utilitzada o implementada és la del manteniment de la seguretat de xarxes locals.

Trobar informació

Una de les utilitats principals d'un servei de directori és **buscar la informació emmagatzemada dels objectes que hi ha en la xarxa**.

El directori emmagatzema informació sobre algunes propietats dels objectes que podeu trobar en la xarxa i el servei de directori proporciona als usuaris facilitats per gestionar la informació sobre aquests objectes.

Per exemple, mitjançant la utilització d'un servei de directori, els objectes es referencien pel nom i no pas per l'adreça física. D'aquesta manera, d'una banda s'aconsegueix ocultar a l'usuari la complexitat de l'organització i, de l'altra, se l'aïlla dels canvis que s'hi produueixen.

Gestionar informació

De vegades no és suficient tenir la informació emmagatzemada en un directori. **És molt important poder accedir al directori des de totes les aplicacions que són susceptibles d'utilitzar-lo.**

El fet d'utilitzar un servei de directori per centralitzar la informació necessària per al funcionament de diverses aplicacions ens estalvia molt d'esforç a l'hora d'implementar les estructures de dades per a cada aplicació i a l'hora de mantenir el sincronisme i la consistència entre les dades emmagatzemades. Per exemple, si tenim en la nostra xarxa un servidor web en què s'autentiquen usuaris, la solució més senzilla pot ser implementar una base de dades amb els usuaris en el servidor i gestionar-la des del mateix servidor.

Tanmateix, si afegim més servidors web, o d'un altre tipus, en la xarxa i també necessitem autenticar-hi usuaris, haurem d'implementar una base de dades per a cada servidor amb els mateixos usuaris, possiblement, a més de mantenir les dades sincronitzades per evitar inconsistències.

En aquest cas, la millor solució seria implementar un servei de directori en què les dades estiguessin centralitzades i tots els servidors poguessin accedir a un únic directori comú. Això comportaria un estalvi de temps i d'esforç en la creació de les bases de dades i en el treball d'inserció i sincronització de les dades.

La idea és que aquest directori comú proporcioni les funcionalitats que reclamen les aplicacions i que, a més, sigui multiplataforma, s'hi pugui accedir per mitjà d'un protocol estàndard i ofereixi una IPA estàndard.

Un dels avantatges principals és que quan es disposa d'una infraestructura de directori d'aquest tipus, els programadors aprofiten el temps que tenen per desenvolupar aplicacions i no pas serveis de directori específics. Per tant, la utilització del servei de directori en les aplicacions pot facilitar-ne el desenvolupament i ampliar-ne la funcionalitat.

Implementació d'un servei de directori

Òbviament, hem de tenir en compte els avantatges que té un servei de directori. Tanmateix,

IPA

Una IPA (en anglès, API, *application program interface*) o interfície de programa d'aplicació constitueix el conjunt de funcions i procediments o mètodes, en la programació orientada a objecte, que ofereix una biblioteca d'una aplicació perquè un altre programari l'utilitzi com una capa d'abstracció. Una IPA representa una interfície de comunicació entre elements de programari.

també hem de considerar que a vegades la implementació i la gestió d'un servei de directori pot ser complicada. Quan el volum de dades a tractar sigui petit, pot ser que no compensi generar tota la infraestructura d'un servei de directori.

Podem dir que un servei de directori a què poden accedir multitud d'aplicacions es converteix en una part vital del sistema en proporcionar un accés uniforme a les persones, els recursos i altres objectes del sistema. És a dir, el directori es veu com un tot uniforme i no pas com un conjunt de parts independents.

Quan les aplicacions utilitzen un servei de directori comú, dissenyat de manera adequada, és més fàcil controlar els riscos de fallada i concentrar els esforços a millorar l'administració d'aquest servei i la tolerància a fallades.

Seguretat

Els serveis de directori poden fer funcions d'autenticació d'usuari mitjançant dos tipus de mecanismes:

1. **Autenticació simple**, en què el directori manté emmagatzemada la contrasenya de cada usuari. Quan l'usuari accedeix al directori, fa una comparació amb el valor emmagatzemat. Si ho comparem amb una carta, equivaldria al servei que ofereix la signatura que hi ha a peu de pàgina.
2. **Autenticació forta**, en què el directori manté emmagatzemades claus de xifratge per autenticar l'usuari. Seguint amb la comparació, el xifratge de missatges equivaldria a tancar el sobre i afegir-hi un lacre digital per impedir que terceres persones l'obrissin.

Per altra banda, el servei de directori és el suport ideal per a la distribució dels certificats electrònics personals. Concretament, el directori resol dos problemes principals:

La **gestió de la infraestructura de clau pública**, ja que permet fer el següent:

- **Crear certificats**: permet incorporar al certificat les dades contingudes en el servidor en què s'implementa el servei de directori.
- **Distribuir certificats**: permet tenir accessibles mitjançant un protocol estàndard els certificats electrònics.
- **Destruir certificats**: permet implementar la revocació d'un certificat amb la simple operació d'esborrar el certificat del servidor en què tenim el servei de directori.

El **problema de la ubicació dels certificats**. El directori és el lloc natural en què els usuaris poden accedir als certificats de la resta d'usuaris d'una manera còmoda i fàcil d'integrar amb la resta d'aplicacions.

3.2.3 Arquitectura del servei de directori

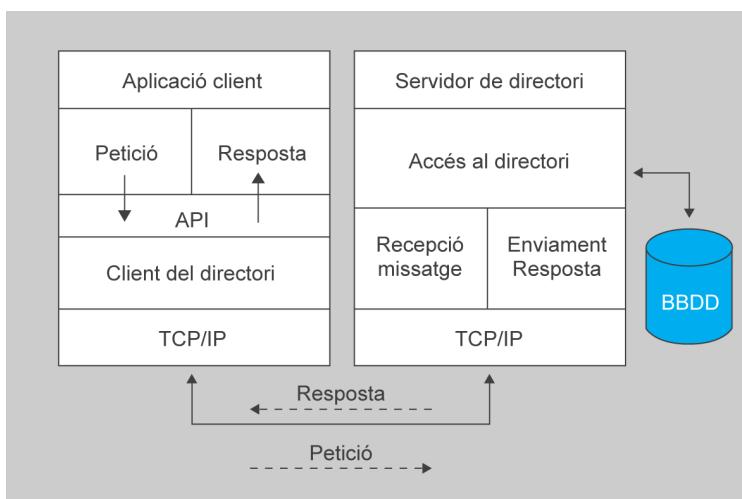
És convenient tenir clara l'arquitectura del servei de directori per entendre'n millor el funcionament i la raó d'ésser.

Cal conèixer que els serveis de directori se solen implementar seguint el model client-servidor, de manera que una aplicació que vol accedir al directori no accedeix directament a la base de dades, sinó que crida una funció de la IPA que envia un missatge a un procés en el servidor. Aquest procés accedeix al directori i retorna el resultat de l'operació.

Algunes vegades el servidor es pot convertir en el client de l'altre servidor a fi d'aconseguir la informació necessària per processar la petició que se li ha fet.

Seguint aquesta arquitectura (figura 3.1), el client no depèn de l'arquitectura del servidor i el servidor pot implementar el directori de la manera més convenient.

FIGURA 3.1. Esquema de l'arquitectura del servei de directori



3.2.4 Serveis de directori distribuïts

Resulta interessant saber en què consisteix un servei de directori distribuït a diferència d'un servei de directori centralitzat.

El servei de directori pot estar centralitzat o distribuït. En cas d'estar centralitzat, un únic servidor subministra tot el servei de directori i respon totes les consultes dels clients. Si el directori està distribuït, hi ha diversos servidors que proporcionen el servei de directori.

Quan el servei de directori està distribuït, les dades poden estar fraccionades o replicades. Quan la informació està fraccionada, cada servidor del servei de directori emmagatzema un subconjunt únic de la informació. És a dir, una entrada només s'emmagatzema en un servidor. Quan la informació està replicada, una entrada es pot emmagatzemar en diversos servidors. Generalment, quan el servei de directori està distribuït, una part de la informació està fraccionada i una altra part està replicada.

3.2.5 Seguretat del servei de directori

La seguretat de la informació emmagatzemada en el directori és un dels aspectes fonamentals a tenir en compte en els serveis de directori. Alguns directoris han de permetre l'accés públic, però qualsevol usuari no ha de poder efectuar qualsevol operació. Per exemple, qualsevol usuari pot buscar l'adreça de correu d'un empleat, però només l'empleat o l'administrador pot tenir permís per modificar-la.

La política de seguretat defineix quin usuari té quin tipus d'accés sobre quina informació.

Els serveis de directori han de permetre les capacitats bàsiques per implementar una política de seguretat. Encara que els serveis mateixos puguin no incorporar aquestes capacitats, han d'estar integrats amb un servei de xarxa fiable que proporcioni aquests serveis bàsics de seguretat.

Inicialment es necessita un mètode per autenticar l'usuari. Una vegada s'ha verificat la identitat del client, es pot determinar si està autoritzat a portar a terme l'operació sol·licitada o no. Generalment les autoritzacions estan basades en l'ACL (*access control list*). Aquestes llistes es poden unir als objectes o als atributs que hi ha en el directori. Per facilitar l'administració d'aquestes llistes, els usuaris amb els mateixos permisos s'agrupen en grups de seguretat.

ACL és un concepte de seguretat utilitzat per donar o no privilegis a un objecte determinat que està fent una consulta.

3.3 LDAP

Cal que conegeu la definició, l'origen, el funcionament i les diverses utilitats d'una de les especificacions més utilitzades en el món de les xarxes per implementar serveis de directoris, el protocol LDAP.

LDAP és la sigla de *lightweight directory access protocol* o protocol d'accés a directoris lleugers. El podem definir de la manera següent:

L'LDAP és un protocol obert a escala d'aplicació, del tipus client-servidor, que s'utilitza per accedir a un servei de directori.

Hi ha moltes implementacions “comercials” que utilitzen l'LDAP o que hi estan

basades. Entre les més importants, hi ha les següents:

- Microsoft Active Directory
- Red Hat Directory Server / Fedora Directory Server
- Novell Directory Services
- Sun Directory Server
- OpenLdap

L'OpenLdap es farà servir per veure el procés d'instal·lació i configuració d'un servei de directori amb l'LDAP.

3.3.1 Ús de l'LDAP

Típicament, l'LDAP s'utilitza per emmagatzemar la informació dels usuaris i els recursos d'un domini. Sovint també es fa servir per inventariar recursos de xarxa (màquines, impressores, servidors, etc.) o directoris de recursos humans.

L'objectiu principal és permetre l'autenticació en xarxa. Amb aquesta finalitat es pot utilitzar de manera conjunta amb una gran quantitat d'aplicacions que disposen de suport per a l'LDAP, com ara les següents:

- Sistemes d'autenticació per a pàgines web: alguns dels gestors de continguts més coneguts disposen de sistemes d'autenticació per mitjà de l'LDAP.
- Sistemes de control d'entrades a edificis, oficines, etc.
- Sistemes de correu electrònic. Grans sistemes formats per més d'un servidor que accedeixen a un dipòsit de dades comú.
- Sistemes d'allotjament de pàgines web i FTP, amb el dipòsit de dades d'usuari compartit.
- Grans sistemes d'autenticació basats en el RADIUS per controlar els accessos dels usuaris a una xarxa de connexió o un proveïdor d'Internet.
- Servidors de certificats públics i claus de seguretat.
- Autenticació única per a la personalització d'aplicacions.
- Perfilss d'usuaris centralitzats per permetre itinerància (*roaming*).
- Llibretes d'adreses compartides.

Per entendre millor la utilitat del protocol, cal que imagineu que en la vostra xarxa disposeu d'un servidor LDAP. Si configureu tots els PC i tots els serveis de la xarxa perquè s'hi autentiquin, n'hi haurà prou de crear els comptes d'usuari i els grups d'usuari en el vostre servidor LDAP per tal que els usuaris puguin fer ús del

sistema i dels serveis que ofereix des de qualsevol lloc de la xarxa. És un sistema ideal per centralitzar l'administració d'usuaris en un únic lloc.

En general, l'LDAP s'utilitza quan es vol accedir a una base de dades des de diferents plataformes i des de múltiples ordinadors o aplicacions ubicats en una xarxa i quan els registres de la base de dades canvien poc (poques vegades al dia o menys). En la figura 3.2 podem veure un exemple d'un servei de directori en línia.

FIGURA 3.2. Exemple d'un servei de directori en línia

Universitat Politècnica de Catalunya	
Llista de membres del Consell de Direcció	
Llista de les Units	
Nom	Universidad Politécnica de Cataluña Universitat Politècnica de Catalunya UPC
Localitat	Barcelona
Adreça	UPC C. Jordi Girona, 31 08034 Barcelona SPAIN
Telèfon	34 93 4016200
URL	Web de la Universitat Politècnica de Catalunya
Descripció	Universitat Politècnica Universidad Politécnica Technical University
Domini Internet associat	upc.edu

3.3.2 Orígens de l'LDAP

Escalabilitat

L'escalabilitat és la propietat desitjable d'un sistema, una xarxa o un procés, que indica la seva habilitat per a estendre el marge d'operacions sense perdre qualitat, a més de manejar el creixement continu de treball de manera fluida i estar preparat per a fer-se més gran sense perdre qualitat en els serveis oferts.

Hi ha diferents estàndards que especificen les característiques dels serveis de directori. L'estàndard X.500 potser és el més conegut i utilitzat.

L'estàndard X.500 organitza les entrades en el directori de manera jeràrquica. A més, entre les característiques que té destaca la capacitat d'emmagatzemar una gran quantitat de dades, la fàcil escalabilitat i la gran capacitat de cerca.

L'estàndard X.500 defineix un protocol que permet l'accés a les dades del servei de directori denominat *DAP* (*directory access protocol*). El protocol DAP resulta molt complex i pesat a l'hora d'implementar aplicacions que hi treballen, ja que les aplicacions requereixen molts recursos i temps d'implementació perquè el protocol està definit sobre la pila completa de nivells OSI, és a dir, perquè s'ha de tenir en compte en implementar cadascun dels set nivell teòrics del model OSI, en comptes dels quatre del nivell pràctic TCP/IP.

Així doncs, com a alternativa més lleugera al protocol DAP apareix el protocol LDAP.

Actualment s'utilitzen els certificats X.509 en criptografia de clau pública.

L'LDAP sorgeix com una alternativa al DAP per accedir a directoris del tipus X.500. L'LDAP ofereix un protocol lleuger gairebé equivalent, però molt més senzill i eficient, dissenyat per operar directament sobre el model TCP/IP.

3.3.3 Funcionament de l'LDAP

El servei de directori LDAP, com gairebé tots els serveis de directori, té una arquitectura client-servidor.

En aquest model un o més servidors LDAP contenen les dades que conformen l'arbre de directori LDAP o base de dades jeràrquica. L'aplicació que fa de client LDAP es connecta amb el servidor LDAP (normalment utilitza el port 389) i li fa una consulta. El servidor contesta amb la resposta corresponent o bé indica el lloc on el client pot trobar més informació. Normalment aquest lloc serà un altre servidor LDAP.

No importa amb quin servidor LDAP es connecti el client, ja que sempre observarà la mateixa vista del directori. És a dir, el nom amb el qual es fa la consulta a un servidor LDAP fa referència a la mateixa entrada a què faria referència en un altre servidor LDAP.

3.3.4 Avantatges en l'ús de l'LDAP

L'ús de directoris LDAP s'ha popularitzat cada vegada més a l'hora de fer servir serveis de directori, ja que té molts avantatges sobre altres tipus de sistemes d'emmagatzematge i recuperació de dades. Els directoris LDAP són compatibles o utilitzats per a la implementació de molts sistemes, organitzacions i aplicacions tant lliures com propietàries al món de la informàtica com, per exemple, OpenLDAP, Windows , MySQL, SAMBA, etc.

Així doncs, el directori LDAP destaca sobre els altres tipus de bases de dades per les característiques següents:

- És molt ràpid en la lectura de registres.
- Permet replicar el servidor de manera molt senzilla i econòmica.
- Moltes aplicacions de tot tipus tenen interfícies de connexió amb LDAP i s'hi poden integrar fàcilment.
- Disposa d'un model de noms globals que assegura que totes les entrades són úniques.

- Permet múltiples directoris independents.
- Funciona sobre TCP/IP i SSL/TLS.
- La majoria de servidors LDAP són fàcils d'instal·lar, mantenir i optimitzar, encara que la configuració és una mica tediosa.

3.3.5 Estructura del directori LDAP

Com que l'LDAP va néixer com a alternativa lleugera al DAP per a l'accés a servidors X.500, segueix el model d'estructura de l'estàndard X.500, tot i que és una mica restringit. A continuació, veureu cadascun dels elements que componen l'estructura del directori LDAP i les relacions que hi ha entre ells.

1. Entrada

Un dels conceptes fonamentals dels directoris LDAP és el concepte d'*entrada*. Així doncs:

Les entrades són les estructures de dades en què el directori emmagatzema i organitza la informació. La unitat bàsica d'informació emmagatzemada en el directori LDAP és l'entrada.

2. Objecte

Els elements als quals fan referència les entrades del directori, i per tant són els elements que conformen lògicament el directori, són els objectes:

Cada entrada del directori descriu un objecte, com ara una persona, un grup, una organització, una impressora, un servidor, etc. Per tant, els objectes són els elements del món real als quals representen les entrades del directori.

3. Atribut

Les propietats o els valors que identifiquen els objectes del directori són determinats pels atributs.

Cadascun dels objectes o entrades té un conjunt d'atributs. Tots els atributs que pertanyen a un objecte s'identifiquen mitjançant un nom o acrònim significatiu, són d'un cert tipus i poden tenir un o diversos valors associats. El tipus defineix la classe d'informació que els atributs emmagatzemen i els valors són la informació en si. La sintaxi dels atributs depèn del tipus d'atribut.

Per exemple, un atribut del tipus *cn* (*common name*) pot contenir el valor “Pere Pérez López”. Un atribut del tipus *email* pot contenir un valor “pperez-lop@exemple.com”. Hi ha dos tipus d'atributs especials:

- **Nom distingit.** Cada entrada té un atribut especial anomenat *distinguished name* o *nom distingit* (DN), que la identifica unívocament en la base de dades del directori. Per tant, podem dir que el DN s'utilitza per referir-se a una entrada sense ambigüïtats.
- **Nom distingit relatiu.** Els *noms distingits relativs* o *relatives distinguished names* (RDN) són les seqüències més petites que componen un nom distingit (DN). Els RDN són parells de valors formats per un atribut de l'entrada més el seu valor amb la forma.

¹ <nom_atribut>=<valor>

Per entendre millor els conceptes de DN i RDN, els podem comparar amb un sistema de fitxers de qualsevol sistema operatiu en què **el DN és el camí absolut al fitxer i el RDN és el camí relatiu**.

La resta d'atributs de l'entrada depenen de l'objecte que descrigui aquesta entrada. Per exemple, les entrades que descriuen persones soLEN tenir, entre altres, atributs com *cn* (*common name*) per descriure el nom comú, *sn* (*surname*) per al cognom, *mail* per a l'adreça de correu electrònic, etc.

4. Arbre d'informació del directori

L'estructura de les diferents entrades del directori és formada per l'arbre d'informació del directori.

Les entrades estan organitzades en forma d'arbre basant-se en els DN. L'arbre d'entrades de directori es coneix com a *directory information tree* o *arbre d'informació del directori* (DIT).

Se suposa que un directori emmagatzema informació sobre els objectes que hi ha en una certa organització. Cada directori posseeix com a arrel (o base, en terminologia LDAP) la ubicació d'aquesta organització, de manera que **la base es converteix de manera natural en el sufix dels noms distingits de totes les entrades que manté el directori**.

A partir d'aquesta base, l'arbre se subdivideix en els nodes i subnodes necessaris per tal d'estructurar de manera adequada els objectes de l'organització, objectes que se situen finalment com les fulles de l'arbre.

Cada RDN es correspon amb una branca de l'arbre d'informació del directori (DIT). Cada branca parteix de l'arrel (base) i acaba en les fulles en què se situen els objectes del directori. No hi pot haver entrades soltes, és a dir, que no depenguin d'un RDN o pare. Només l'entrada arrel pot no tenir entrada pare. En cas d'afegir una entrada en un punt inexistent en el directori, el servidor retornarà un missatge d'error i no efectuarà l'operació. Aquesta estructura permet que el directori emmagatzemi la informació de la manera més convenient. Per exemple, es pot crear un grup que contingui totes les persones de l'organització i un altre que en contingui tots els grups.

El nom distingit (DN) de cada entrada del directori, per tant, és una cadena de caràcters formada per parells

¹ <tipus_atribut>=<valor>

(RDN) separats per comes, que representen la ruta invertida que duu des de la posició lògica de l'entrada en l'arbre (fulla) fins a l'arrel (base). **D'aquesta manera, el nom distingit (DN) de cada entrada en descriu la posició que ocupa en l'arbre de l'organització, i viceversa.**

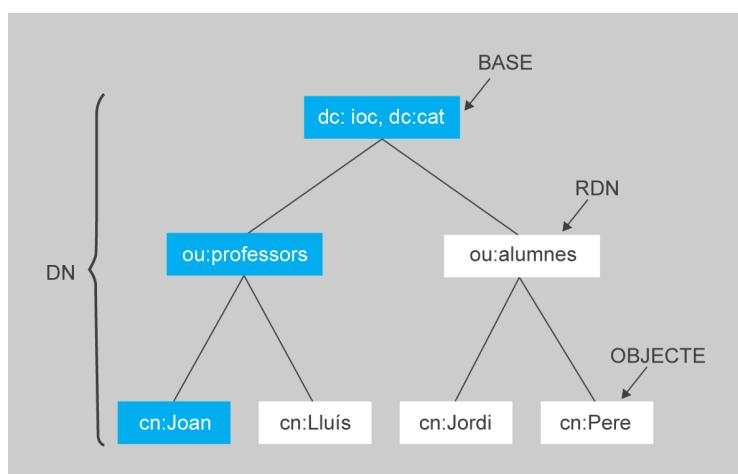
Hi ha dues maneres de nomenar o estructurar l'arbre d'un directori LDAP:

- **Estructura “tradicional”:** formada pel país i l'estat on se situa l'organització i, a continuació, el nom d'aquesta organització. Per exemple, l'arrel o base de l'Institut Obert de Catalunya podria ser alguna cosa així: o=ioc st=catalunya, c=cat.
- **Estructura basada en noms de domini d'Internet, és a dir, en DNS:** aquesta estructura utilitza els dominis DNS per nomenar l'arrel de l'organització. En aquest cas, la base de l'IOC seria la següent: dc=ioc, dc=cat.

Utilitzarem el nomenclament basat en DNS, ja que és la nomenclatura més utilitzada i permet localitzar servidors LDAP mitjançant cerques DNS.

En la figura 3.3 vegem un exemple de l'estructura d'un directori.

FIGURA 3.3. Exemple d'arbre del directori ioc.cat utilitzant el model DNS



D'acord amb aquesta figura, l'entrada corresponent a l'objecte professor "joan" tindria com a nom distingit "cn=joan, ou=professor, dc=ioc, dc=cat". La base del directori o arrel de l'arbre d'informació es correspondria amb "dc:ioc,dc=cat".

Cadascuna de la resta de caixes per separat es correspondrien amb els RDN de l'arbre.

5. Esquema

Cada entrada o objecte en el directori pot tenir, com hem dit, un conjunt d'atributs tan descriptius com es vulgui.

La definició dels possibles tipus d'objectes i dels atributs que els componen (incloent-hi el nom, el tipus, el valor o valors admesos i les restriccions), que el directori d'un servidor LDAP pot utilitzar, la fa el servidor mateix mitjançant el denominat *esquema (schema)* del directori. Per tant, l'esquema conté les definicions dels objectes que es poden donar d'alta en el directori.

La definició de cada atribut que pertany a un objecte en els distints esquemes del servei determina si és **opcional o obligatori** (ordres MAY o MUST). També és possible que els objectes heretin atributs d'altres objectes. Per exemple, en l'esquema, l'opció SUP defineix l'objecte pare de l'objecte en qüestió.

Atès que cada servidor pot definir el seu propi esquema, per permetre la interoperabilitat entre diferents servidors de directori, els atributs i les classes d'objectes estan estandarditzats per la IANA i tenen un número d'identificació de l'objecte (*object ID*).

Vegem un exemple de fragments d'un esquema:

```

1 attributetype **( 2.5.4.42 NAME ( 'givenName' 'gn' )**
2 DESC 'RFC2256: first name(s) for which the entity is known by'
3 SUP name )
4
5 objectclass ( **2.5.6.6 NAME 'person'** SUP top STRUCTURAL
6 MUST ( sn $ cn )
7 MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )

```

6. Classes d'objecte

Cada objecte és definit per la classe a la qual pertany.

La classe de l'objecte és una descripció general d'un tipus d'objecte i, per tant, especifica implícitament la resta d'atributs d'aquest objecte, d'acord amb la definició establerta en l'esquema.

Cada objecte necessita, a més del nom distingit que l'identifica, la seva classe d'objecte, que s'especifica mitjançant l'atribut **objectClass**. La classe de l'objecte

ha de constar en l'esquema o esquemes actius en el servidor LDAP. Un mateix objecte pot pertànyer a diferents classes simultàniament, de manera que hi pot haver molts **objectClass** per a un mateix objecte en el directori.

A més de les classes bàsiques d'objectes definides en els esquemes, l'administrador del servei LDAP pot definir dins dels esquemes els seus propis objectes o especificar en el servidor LDAP els esquemes que necessiti.

3.3.6 El format d'intercanvi de dades LDIF

El format LDIF (*LDAP data interchange format*) és l'estàndard per representar les entrades del directori LDAP en format text.

Resulta molt útil conèixer aquest tipus de representació perquè és el format que els servidors LDAP (l'OpenLDAP, entre altres) utilitzen per defecte per inserir informació en el directori i extreure'n. Així, segons el format LDIF, una entrada del directori consisteix en dues parts:

- 1. El DN o nom distingit**, que ha de figurar en la primera línia de l'entrada i que es compon de la cadena dn seguida del DN complet de l'entrada.
- 2. Els atributs de l'entrada**. Cada atribut es compon d'un nom d'atribut, seguit del caràcter dos punts i el valor de l'atribut. Si hi ha atributs multivalorats, han de posar-se seguits.

No hi ha cap ordre preestablert per a la col·locació dels atributs, però és convenient llistar primer l'atribut **objectClass** per millorar la llegibilitat de l'entrada.

Seguint amb l'exemple anterior, a continuació es mostra un subconjunt dels atributs de l'alumne Pere:

```
dn: cn=joan, ou=professors, dc=ioc, dc=cat objectClass: person cn: joan sn: Perez description: professor mail: joan@ioc.cat
```

Cal tenir en compte que una entrada pot canviar de posició dins de l'arbre i modificar el seu DN. Per això tots els objectes tenen un *universally unique identifier* (UUID) que els identifica de manera única.

3.3.7 Operacions de l'LDAP en el directori

L'estàndard LDAP proporciona un model que permet controlar l'accés a les dades que hi ha en el directori. Aquest model defineix un conjunt d'operacions dividides en tres grups:

- **Operacions de consulta**, permeten fer cerques en el directori i recuperar dades.

- **Operacions d'actualització**, permeten afegir, esborrar, reanomenar i modificar entrades del directori.
- **Operacions d'autenticació i control**, permeten la identificació dels clients i del directori i el control de certs aspectes d'una sessió.

Operacions de consulta

Les operacions de consulta permeten buscar i obtenir informació emmagatzemada en el directori.

L'**operació search** permet buscar en el directori les entrades que compleixen les especificacions indicades. Aquestes especificacions permeten indicar el punt d'inici de la cerca, la profunditat, els valors que han de tenir determinats atributs i els atributs que es retornaran. Per fer la recerca, s'han d'especificar els paràmetres següents:

- **Base**: especifica el DN en què s'indica el punt de partida per a la cerca.
- **Scope**: àmbit en què es farà la cerca, pot tenir diferents valors:
 - **Base**, només es cerca en l'entrada base.
 - **One**, es cerca en el nivell immediatament inferior a l'entrada base.
 - **Subtree**, es cerca en tot el subarbre sota l'entrada base.
- **Filtre de cerca**: indica el criteri que s'aplicarà a la cerca.
- **Atributs a retornar**: es pot indicar quins atributs es retornen i si es retorna el valor de l'atribut o el tipus de dada que conté.
- **Alias derreferencing**: indica si el servidor ha de seguir les entrades referral o, per contra, la petició s'ha d'enviar al servidor referenciat.
- **Límit**: indica el nombre màxim d'entrades que es retornaran o el temps que es farà servir per fer aquesta cerca. Els serveis poden imposar límits més estrictes que els que indiquin els clients.

També hi ha l'**operació compare**, que és similar a l'operació de cerca i utilitza un filtre d'equiparació. La diferència rau en el fet que quan hi ha una entrada que compleix les especificacions, però no té l'atribut que es vol retornar, el directori retorna un valor especial a fi d'indicar que aquesta entrada, tot i complir els requisits, no disposa de l'atribut.

Operacions d'actualització

Hi ha quatre operacions que permeten afegir, esborrar, reanomenar (modificar el DN) i modificar el contingut de les entrades del directori. Aquestes operacions són les següents:

Referral

Referral és el procés pel qual un servidor LDAP, en comptes de tornar un resultat, torna una referència a un altre servidor LDAP que pot contenir la informació que es vol.

1. Operació add

Aquesta operació permet afegir entrades noves en el directori. Com a paràmetres, rep el DN de l'entrada que cal crear i també els atributs i els valors que hi estan associats. Per poder fer aquesta operació, s'han de complir les condicions següents:

- El node pare de l'entrada ha de ser en el directori.
- No hi ha d'haver cap altra entrada amb el mateix DN.
- L'entrada ha de complir els requisits específics en l'esquema.
- El control d'accisos ha de permetre aquesta operació.

2. Operació delete

Aquesta operació permet eliminar entrades del directori. Com a paràmetres, rep el DN de l'entrada a esborrar. Per poder fer aquesta operació, s'han de complir les condicions següents:

- L'entrada a esborrar ha de ser en el directori.
- Aquesta entrada no pot tenir cap fill.
- El control d'accisos ha de permetre aquesta operació.

3. Operació rename

Aquesta operació permet modificar el DN d'una entrada. Per poder reanomenar una entrada, s'han de complir les condicions següents:

- L'entrada a reanomenar ha d'exsistir.
- No hi pot haver una entrada amb el DN nou.
- El control d'accisos ha de permetre aquesta operació.

4. Operació modify

Permet modificar els atributs d'una entrada. Per poder executar aquesta operació, s'han de complir les condicions següents:

- L'entrada a modificar ha d'exsistir.
- L'entrada resultant s'ha d'ajustar a l'esquema.
- El control d'accisos ha de permetre l'actualització.

Aquest punt indica que les operacions en LDAP són atòmiques. Si alguna de les modificacions falla, tota l'operació d'actualització falla.

Operacions d'autenticació i control

L'LDAP incorpora dues operacions d'autenticació (bind i unbind) i una de control (abandon).

1. Operació bind

Aquesta operació permet autenticar el client en el directori. Hi ha diversos tipus d'autenticació en funció de les operacions que volem fer en el directori. Entre els diferents tipus d'autenticació, hi podem trobar els següents:

- **Sessions anònimes.** Les sessions anònimes, en què no s'ha especificat l'usuari ni la contrasenya, solament tenen sentit per a operacions de cerca, ja que no s'ha fet cap tipus de comprovació de la identitat del client.
- **Sessions autenticades.** L'autenticació bàsica consisteix a enviar al servidor el nom distingit i la contrasenya de l'usuari en text clar per establir la connexió. El servidor considera que el client s'ha autenticat si la contrasenya coincideix amb l'emmagatzemada en el camp userPassword. Aquesta informació s'envia en text clar des del client al servidor, cosa que implica un risc de seguretat molt alt.
- **Sessions xifrades.** L'LDAP també té en compte l'establiment de sessions xifrades. En aquest tipus de sessions, el client envia el nom distingit de l'usuari, el mètode d'autenticació que farà servir i les credencials necessàries per autenticar-se. El mecanisme SASL estableix els mètodes d'autenticació estàndard. L'avantatge principal d'aquest disseny rau en el fet que permet l'ampliació a mètodes d'autenticació nous mitjançant el mètode external. De fet, l'SSL (i el seu successor, TSL) utilitzen aquest mètode.

2. Operació unbind

Aquesta operació tanca la connexió amb el servidor LDAP.

3. Operació abandon

Aquesta operació permet indicar al servidor LDAP que el client abandona l'operació en curs.

3.4 Instal·lació i configuració d'un servei de directori als sistemes GNU/Linux

Resulta fonamental conèixer els processos d'instal·lació i configuració bàsica d'un servei de directori en un sistema GNU/Linux, concretament l'OpenLDAP. Abans, però, per conèixer millor el programari utilitzat, heu de saber en què consisteix el projecte OpenLDAP.

3.4.1 Introducció a l'OpenLDAP

L'OpenLDAP és una implementació de codi obert i gratuïta de l'estàndard LDAP desenvolupada pel projecte OpenLDAP.

L'any 1998 Kurt Zeilenga va iniciar el projecte OpenLDAP. L'OpenLDAP va començar com un clon de la implementació LDAP de la Universitat de Michigan, entitat en què es va desenvolupar originalment l'LDAP i que actualment també treballa en l'evolució d'aquest protocol.



Logotipus del projecte OpenLDAP

Bàsicament, l'OpenLDAP posseeix tres components principals:

- **slapd:** Format per al servidor LDAP i algunes eines de gestió.
- **ldap-utils:** Paquet que agrupa alguns programes client com l'ldapsearch, l'ldapadd, l'ldapdelete o l'ldapcat, entre d'altres.
- **Biblioteques que implementen el protocol LDAP,** com liblber i libldap.

3.4.2 Instal·lació OpenLDAP

La primera qüestió que hem de tenir en compte abans d'instal·lar un servei de directori mitjançant l'OpenLDAP és escollir bé el maquinari i el programari que farem servir.

Per instal·lar el servidor OpenLDAP en què emmagatzemarem la base de dades del directori i en què recaurà la major part del processament de les consultes al sistema, hem de tenir en compte les recomanacions següents:

- **Processador:** si és possible, és millor que utilitzem servidors amb multiprocessador.
- **Suport d'emmagatzemament:** és convenient utilitzar un disc dur per al sistema operatiu i un altre per emmagatzemar la base de dades de l'OpenLDAP. Si no és possible, almenys hauríem d'utilitzar dues particions separades. Aquesta és l'optimització més important.
- **Grandària de la memòria:** dependrà del nombre d'entrades que tingui el directori i del nombre d'atributs que usi cada entrada. Normalment necessitarem entre 2 GB i 4 GB de memòria.

No és imprescindible disposar d'aquests recursos de maquinari o programari per poder utilitzar l'OpenLDAP, només són recomanacions.

Una vegada tinguem el maquinari necessari per instal·lar el servidor OpenLDAP, haurem de tenir en compte les recomanacions següents a l'hora d'instal·lar el sistema operatiu:

- Tria una instal·lació simple, només amb els complements imprescindibles.
- Actualitzar el sistema operatiu amb els últims components de programari.
- Tria un sistema d'arxius adequat, normalment l'ext3 o l'ext4 per a GNU/Linux.
- Aturar tots els serveis i dimonis que no s'hagin de fer servir.
- Monitorar el servidor.
- Optimitzar els paràmetres del sistema operatiu. Cal que ens assegurem que la memòria, el processador i els suports d'emmagatzematge funcionen correctament.

3.4.3 Instal·lació del servidor OpenLDAP

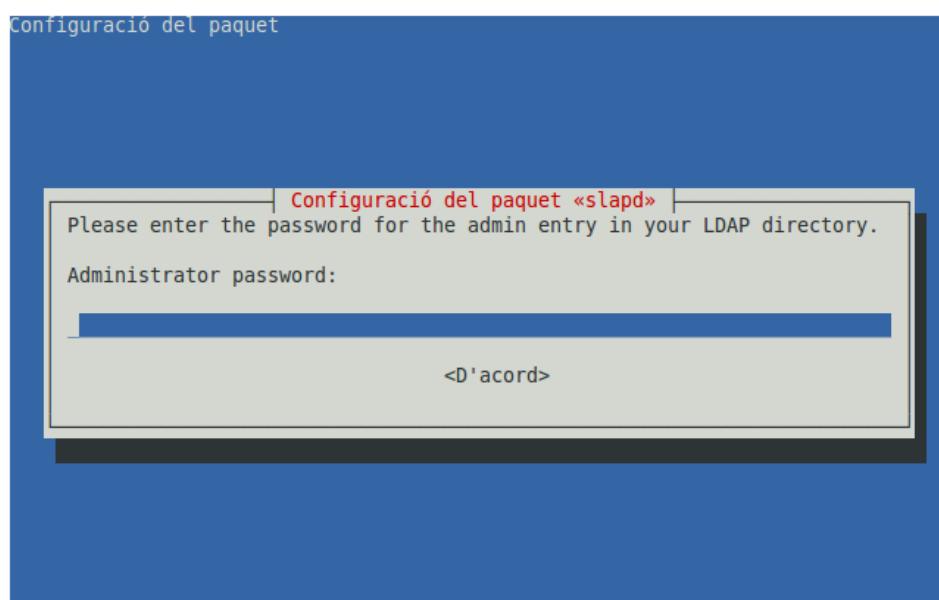
Una vegada tingueu el maquinari i el sistema operatiu que necessiteu enllestits, passeu al pas següent: la instal·lació del servidor OpenLDAP. Feu servir la versió 9.04 del sistema operatiu GNU/Linux Ubuntu.

El paquet necessari per instal·lar el servidor OpenLDAP el podeu trobar en els dipòsits de l'Ubuntu: és el paquet **slapd**. També és convenient instal·lar el paquet **db4.2-util**, ja que proporciona diverses eines per manipular bases de dades amb format de bases de dades de Berkeley v4.2, que serà la base de dades que utilitzareu per al servidor OpenLDAP. Caldrà escollir-la durant la configuració del servidor. Per instal·lar aquests dos paquets executareu l'ordre següent:

```
1 $sudo apt-get install slapd db4.2-util
```

Durant la instal·lació, us preguntarà la contrasenya de l'administrador del servei LDAP, com veiem en la figura 3.4, dues vegades per evitar errors d'escriptura.

FIGURA 3.4. Pantalla d'introducció de la contrasenya per a l'administrador del servei LDAP



Una vegada instal·lat el servidor OpenLDAP, podeu consultar els distints tipus de fitxers que s'han afegit al sistema.

- Amb l'ordre:

```
1  dpkg -L slapd | grep bin
```

llistem els fitxers executables o les ordres instal·lades. Aquestes ordres són necessàries per gestionar el servidor i la base de dades.

- Feu servir les ordres:

```
1  dpkg -L slapd | grep man
```

i

```
1  dpkg -L slapd | grep doc
```

per consultar els manuals i la documentació sobre el servidor respectivament.

- L'ordre:

```
1  dpkg -L slapd | grep etc
```

us ajudarà a conèixer quins són els fitxers de configuració del servidor OpenLDAP.

- Finalment, l'ordre:

```
1  dpkg -L slapd | grep schema
```

us mostrarà els esquemes LDAP que el servidor OpenLDAP utilitza per defecte.

3.4.4 Instal·lació del client OpenLDAP

Una vegada instal·lat el servidor OpenLDAP, per poder accedir als serveis que proporciona des dels equips connectats en xarxa heu d'instal·lar l'aplicació client OpenLDAP.

Per instal·lar el client OpenLDAP, escolliu el paquet **ldap-utils**, que també podeu trobar en els dipòsits de l'Ubuntu. Executeu l'ordre següent:

```
1  $sudo apt-get install ldap-utils
```

Amb l'ordre **dpkg -L ldap-utils | grep bin** podeu consultar els executables o les ordres instal·lades pel paquet ldap-utils, és a dir, el client OpenLDAP.

3.4.5 Configuració del servidor OpenLDAP

La configuració del servidor OpenLDAP en les versions anteriors a l'OpenLDAP 2.4 s'efectuava per mitjà del fitxer **/etc/ldap/slapd.conf**.

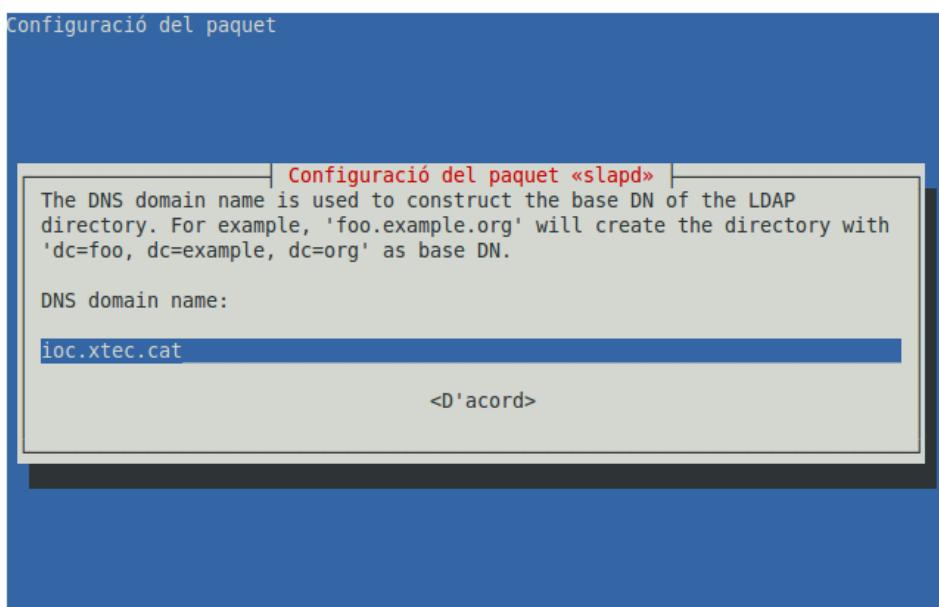
Aquest fitxer emmagatzemava la configuració general del servidor i es podia editar per modificar les opcions de configuració. A partir de la versió 2.4, la configuració del servidor es gestiona de manera distinta. Per configurar el servidor, les versions noves fan servir el directori **/etc/ldap/slapd.d**, que permet fer la configuració en temps d'execució mitjançant una entrada de **l'arbre d'informació del directori** (DIT) anomenada *cn=config*. Aquest nou tipus de gestió de la configuració estàvia haver d'aturar el servei i tornar-lo a arrencar cada vegada que modifiquem algun paràmetre de la configuració. Tot i així, en les versions noves podem especificar que l'arxiu de configuració continuï essent **/etc/ldap/slapd.conf**. Aquest arxiu es pot editar manualment per establir els paràmetres de configuració que es vulguin. Tant si utilitzem l'arxiu **/etc/ldap/slapd.conf** per configurar el servidor com si no, hi ha una manera més senzilla que editar aquest arxiu. Aquesta manera consisteix a fer servir l'assistent de configuració que ens proporciona el paquet **slapd** per configurar el servidor.

Per iniciar la configuració, heu d'executar l'ordre següent: **\$sudo dpkg-reconfigure slapd**

La primera pregunta que fa l'assistent és si voleu ometre la configuració del servidor LDAP. Òbviament heu de respondre que no, ja que precisament el que voleu fer és configurar el servidor LDAP.

El directori OpenLDAP ha de tenir una base de la qual penja la resta d'elements. Com a nom de la base, habitualment s'utilitza el nom del domini. Per exemple, si el vostre domini és **ioc.xtec.cat**, seria habitual que la base per al directori OpenLDAP fos **dc=ioc,dc=xtec,dc=cat**.

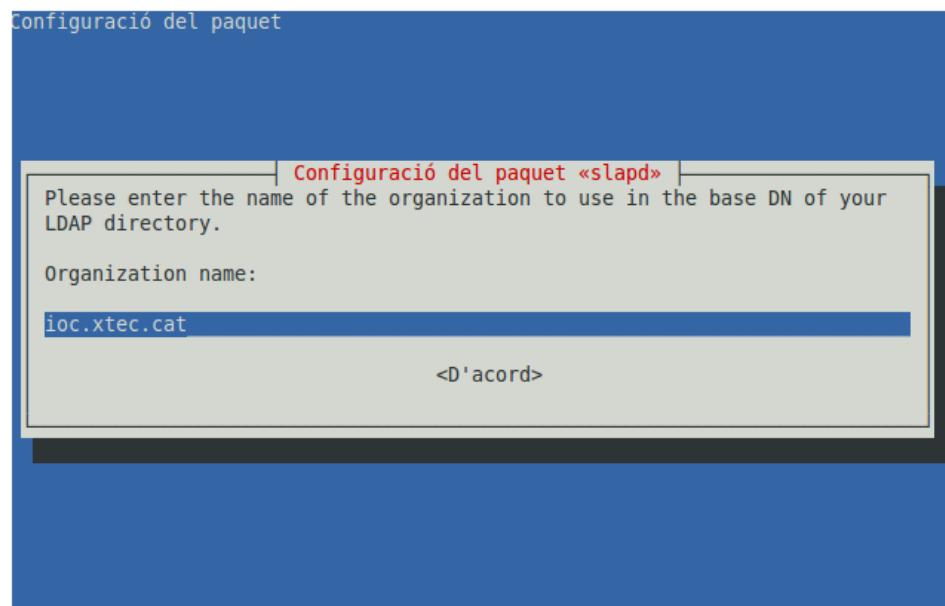
FIGURA 3.5. Introducció del DNS al configurar **slapd**



A continuació, com veiem en la figura 3.5, l'assistent us pregunta quin és el nom del vostre domini. L'OpenLDAP utilitzarà aquest nom per crear tots els noms distingits de les entrades del directori, és a dir, el nom identificatiu de la base del vostre directori OpenLDAP.

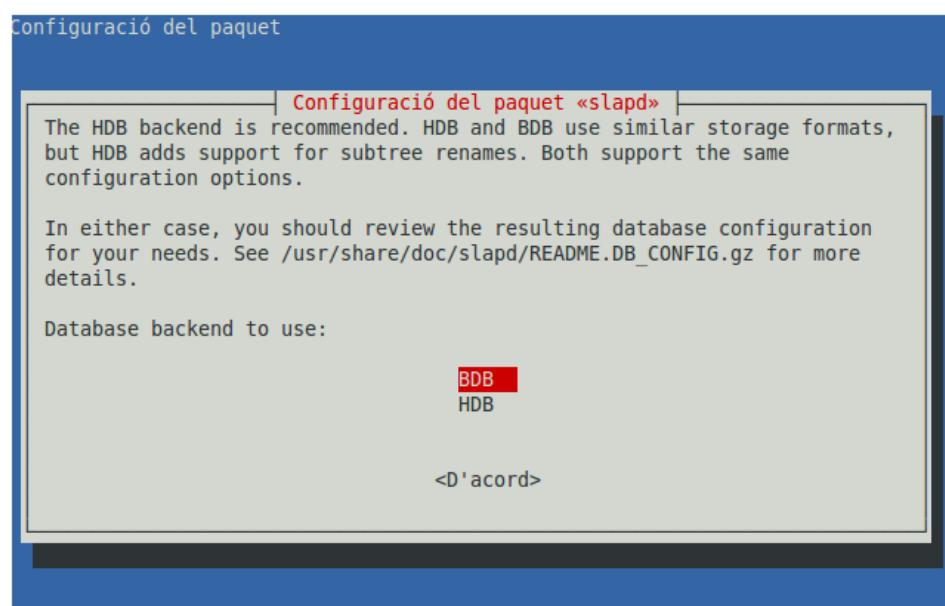
Després us pregunta quin és el nom de la vostra organització, com mostra la figura 3.6. Cal que hi introduïu el mateix nom que el del domini, però no té per què coincidir.

FIGURA 3.6. Introducció de la base del directori al configurar slapd



Tot seguit se us informarà sobre els possibles gestors de bases de dades per emmagatzemar el directori i us preguntarà quin sistema voleu utilitzar, tal com veiem en la figura 3.7. És recomanable fer servir el sistema BDB (Berkeley DB), ja que aquest tipus de base de dades segueix l'estàndard FHS.

FIGURA 3.7. Selecció del tipus de base de dades al configurar slapd



A continuació, us preguntarà si voleu que s'elimini la base de dades quan desinstal·leu l'slapd. Aquesta elecció depèn de la gestió de la informació que es fa en cada organització. Heu de respondre que sí.

En el cas que hi hagi una base de dades LDAP prèvia, ens preguntarà si la volem moure. Si la volem conservar, respondrem que sí. Si no la volem conservar, direm que no, ja que això ens estalviarà espai en el disc.

Després us demanarà quina contrasenya voleu assignar a l'usuari admin (administrador) del servei OpenLDAP. Aquest usuari es crea automàticament en fer la instal·lació del servei i posseeix el privilegi de fer qualsevol operació en el servei de directori. La contrasenya la demanarà dues vegades per evitar errors d'escriptura.

Finalment us demanarà si voleu fer servir l'LDAP versió 2. Heu de dir que no perquè gairebé no s'utilitza.

Una vegada acabat el procés de configuració, cal comprovar que no hi hagi cap error i que generi l'usuari admin. Si és així, ja tindreu el vostre servidor OpenLDAP preparat per poder-hi treballar.

És interessant saber que el procés d'arrencada i aturada manual del servidor LDAP es fa de la mateixa manera que en tots els serveis en l'Ubuntu. El servei disposa d'un script d'arrancada i aturada en la carpeta **/etc/init.d**.

Per tal d'arrencar o reiniciar el servidor LDAP, executeu l'ordre següent:

```
1 $/etc/init.d/slappd restart
```

Podeu establir l'arrencada automàtica del servidor LDAP en iniciar el sistema amb l'ordre següent:

```
1 $update-rc.d slappd defaults
```

3.4.6 Configuració del client OpenLDAP

Podeu fer servir dos tipus de configuració en els equips clients:

- **Configuració per hoste (*host*)**, la més habitual, en què es fa servir el fitxer **/etc/ldap/ldap.conf**.
- **Configuració per usuari**, en què es fa servir el fitxer **~/.ldaprc**.

Els fitxers de configuració s'utilitzen per configurar paràmetres per defecte de la màquina client o de l'usuari client. En la configuració per hoste (*host*) podem editar i modificar el fitxer de configuració del client **/etc/ldap/ldap.conf** per establir els paràmetres de configuració que vulguem.

Per exemple, en la configuració podeu establir quines seran la base i la URL del servidor OpenLDAP al qual es connectarà el client per defecte. Per fer-ho, cal editar el fitxer de configuració i fer-hi les modificacions pertinentes:

```

1 $sudo nano /etc/ldap/ldap.conf
2
3 #BASE dc=example, dc=com
4 #URI ldap://ldap.example.com ldap://ldap-master.example.com:666
5 BASE dc=ioc,dc=xtec,dc=cat
6 URI ldap://localhost

```

En la configuració per usuari, els usuaris poden crear un arxiu de configuració opcional, anomenat **ldaprc** o **~/.ldaprc**, en el seu directori de treball que es farà servir per reemplaçar la configuració per defecte del client OpenLDAP.

Si hi ha qualsevol dubte sobre la sintaxi o les opcions dels fitxers de configuració del client OpenLDAP, es pot consultar el manual mitjançant l'ordre següent:

```
1 $man ldap.conf
```

3.4.7 Gestió del servei OpenLDAP

Una vegada instal·lat i configurat el servidor OpenLDAP, cal gestionar el servei per obtenir els resultats esperats. Principalment, la gestió del servei consistirà a dissenyar l'estructura del directori, introduir-hi les dades i, després, consultar-les.

Per tal d'accendir al directori OpenLDAP i poder crear-hi, modificar-hi i consultar-hi elements, hi ha dues opcions. La primera opció és fer servir les ordres que proporcionen tant el servidor com el client mitjançant la línia d'ordres. La segona opció és utilitzar un explorador de directoris LDAP gràfic. Totes dues opcions acompleixen els estàndards de les operacions LDAP en el directori que s'han explicat anteriorment.

Gestió del directori mitjançant la línia d'ordres

Primer veurem quines ordres ens proporciona l'OpenLDAP i perquè serveixen. Mitjançant l'ordre `dpkg -L slapd | grep bin`, llistem cadascuna de les ordres instal·lades per al servidor:

```

1 $dpkg -L slapd | grep bin
2   /usr/sbin
3     /usr/sbin/slapd
4     /usr/sbin/slappadd
5     /usr/sbin/slapcat
6     /usr/sbin/slapdn
7     /usr/sbin/slapiindex
8     /usr/sbin/slappasswd
9     /usr/sbin/slapttest

```

Vegem quina utilitat té cadascuna de les ordres instal·lades:

- **slapd**, és el servidor OpenLDAP independent.
- **slapadd**, s'utilitza per afegir entrades especificades en el format d'intercanvi de directori LDAP (LDIF) en una base de dades slapd.
- **slapcat**, s'utilitza per passar tota la base de dades de l'OpenLDAP a format LDIF.
- **slapdn**, s'utilitza per comprovar la conformitat dels DN amb els esquemes que es defineixen en el servidor OpenLDAP (slapd).
- **slapindex**, s'utilitza per regenerar índexs slapd basats en el contingut actual d'una base de dades.
- **slappasswd**, és una utilitat de contrasenyes OpenLDAP.
- **slaptest**, s'utilitza per comprovar que la sintaxi de l'arxiu de configuració slapd.conf sigui correcta.

Amb l'ordre **dpkg -L ldap-utils | grep bin** podem consultar les ordres que instal·la el paquet ldap-utils, és a dir, el client OpenLDAP:

```

1 $sudo dpkg -L ldap-utils | grep bin
2   /usr/bin/ldapdelete
3   /usr/bin/ldapmodrdn
4   /usr/bin/ldapsearch
5   /usr/bin/ldapcompare
6   /usr/bin/ldapmodify
7   /usr/bin/ldappasswd
8   /usr/bin/ldapwhoami
9   /usr/bin/ldapexop
10  /usr/bin/ldapadd

```

Vegem quina utilitat té cada ordre o programa instal·lat:

- **ldapdelete**, s'utilitza per esborrar una o més entrades del directori.
- **ldapmodrdn**, serveix per modificar els RDN de les entrades.
- **ldapsearch**, s'utilitza per fer una cerca mitjançant els paràmetres específics, possiblement és l'ordre més utilitzada.
- **ldapcompare**, fa una comparança mitjançant els paràmetres específicats.
- **ldapmodify**, serveix per modificar les entrades del directori.
- **ldappasswd**, és una eina que s'utilitza per establir la contrasenya d'un usuari LDAP.
- **ldapwhoami**, la funció és fer una operació whoami i determinar amb quin usuari hem fet un bind o login.
- **ldapexop**, permet executar operacions esteses, definides per una organització d'estandardització o un venedor de directori particular, per exemple PAM.
- **ldapadd**, s'usa per afegir entrades, és igual que l'ordre ldapmodify -a.

Totes aquestes ordres **han d'obrir una connexió amb el servidor LDAP, és a dir, s'han d'autenticar per portar a terme la seva tasca.**

Per defecte, l'OpenLdap permet operacions de lectura anònimes i operacions d'escriptura només a l'usuari admin. Tot i que aquest comportament es pot modificar en la configuració, no és recomanable si no es tenen en compte totes les conseqüències que pot comportar en el servei de directori.

En totes les ordres serà necessari especificar l'usuari, la paraula de pas, la màquina en què ens volem autenticar i alguna altra opció. Així, les opcions comunes a totes les ordres són les següents:

- **-D binddn** : Determina el nom distintiu de l'usuari amb el qual ens volem connectar al servidor. El binddn es correspon amb la identificació única del node en què es troba l'usuari dins l'arbre LDAP.
- **-W** : Ens pregunta per línia de comandes la paraula de pas. També es pot especificar mitjançant -w password. (Cal anar amb compte perquè d'aquesta manera la contrasenya aniria en text clar.)
- **-H ldapurl**: Especifica la URL (s) de referència del servidor OpenLDAP (s) en què el client es vol autenticar. En la sintaxi només estan permesos els camps protocol / host / port i s'espera una o diverses URL, separades per espais en blanc o comes.
- **h -ldaphost** : Especifica el nom de màquina del servidor en comptes de la URL de l'opció anterior.
- **-x** : Determina que s'utilitzarà l'autenticació simple en lloc de SASL.

Vegeu els exemples següents:

- Connectar amb el servidor local amb autenticació simple amb l'usuari admin per tal d'afegir les entrades que hi ha en un fitxer amb format .ldif i que abans ens demani la contrasenya:

¹ `$ldapadd -x -H ldaps localhost -D "cn=admin" -W -f exemple.ldif`

- Connectar amb el servidor local amb autenticació simple i buscar la informació disponible sobre la base del directori dc=ioc, dc=xtec,dc=cat.

¹ `$ldapsearch -x -h localhost -b 'dc=ioc,dc=xtec,dc=cat'`

Recordem que les operacions de lectura són anònimes per defecte. La resta d'opcions de cadascuna de les ordres es poden consultar mitjançant l'ordre següent:

¹ `man nom_comanda`

Deixem que l'alumne explori el significat i el funcionament de la resta d'ordres i opcións. Atès el funcionament intuïtiu d'un explorador de directoris gràfic, cal coneixer els processos d'instal·lació, configuració i utilització de l'explorador.

Gestió del directori mitjançant exploradors gràfics

Hi ha molts exploradors de directori LDAP, tant de pagament com lliures. Entre les aplicacions lliures, destaquem l'**Apache Directory Studio**, el **LAM (LDAP Account Manager)** i les aplicacions web **Gosa** i **phpLDAPadmin**.

Nosaltres utilitzarem l'aplicació phpLDAPadmin per exemplificar el funcionament d'una eina gràfica d'administració de l'OpenLDAP.

PhpLDAPadmin

El PhpLDAPadmin és una eina per a l'administració gràfica de servidors LDAP, escrita en php i accessible per mitjà d'una interfície web.

El PhpLDAPadmin proporciona una vista jeràrquica basada en l'arbre d'informació del directori amb la qual es pot navegar per tota l'estructura de directori. Permet veure els esquemes LDAP, fer cerques, crear, esborrar, copiar i editar entrades LDAP i, fins i tot, copiar entrades entre servidors LDAP.

Instal·lació del phpLDAPadmin

Com que és una aplicació escrita en php i basada en web, hem de tenir prèviament instal·lat en el nostre sistema com a mínim un servidor web i un intèrpret de php. Podem fer servir l'eina del sistema tasksel per instal·lar el programari LAMP que cobrirà les nostres necessitats. Una vegada instal·lat el programari necessari, podem instal·lar el phpLDAPadmin. Per instal·lar l'aplicació, executem l'ordre següent:

```
1 $sudo apt-get install phpldapadmin
```

Per tal que l'aplicació funcioni correctament, ens hem d'assegurar que el servei OpenLDAP s'està executant en el port 389, que la versió de php és la correcta i que tenim el mòdul LDAP per a php.

Després d'instal·lar el phpLDAPadmin, per accedir al frontal ens hem d'assegurar que el servidor web, en aquest cas Apache, funciona. Per fer-ho, podem executar l'ordre següent:

```
1 $sudo /etc/init.d/apache2 restart
```

Si el resultat és [OK] podem obrir una sessió del navegador web i accedir a la interfície gràfica. Per fer-ho, caldrà introduir el següent en la línia d'adreses:

```
1 http://localhost/phpldapadmin
```

Front end

Els exploradors gràfics de directori només són un frontal (*front end*) per facilitar la tasca als usuaris. Realment aquests exploradors, per fer les seves tasques, fan servir les ordres del sistema que s'han explicat anteriorment.

Aclariment

Com ja hem comentat, l'administració del servidor LDAP es pot fer des de la línia d'ordres en qualsevol sistema que no tingui entorn gràfic (pot ser el nostre cas), ja que hem instal·lat un Ubuntu Server Edition. També es poden utilitzar eines gràfiques instal·lades en altres màquines que, mitjançant la connexió via web, ens permeten gestionar el servei OpenLDAP.

Error

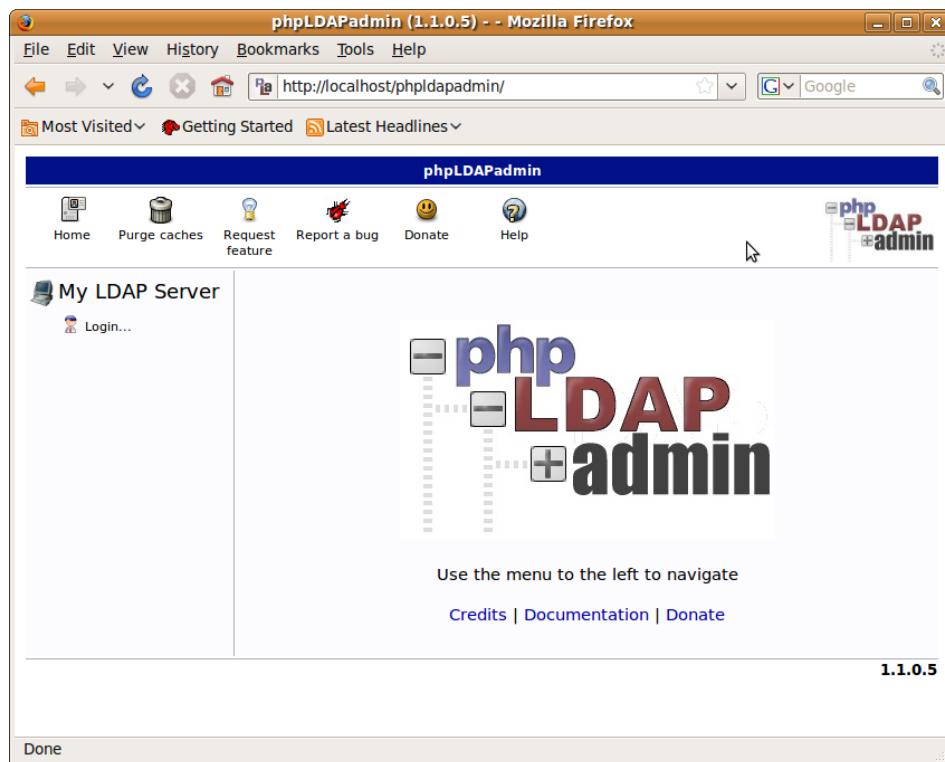
Es pot produir l'error següent:

```
Memory Limit low. Your
php memory limit is low -
currently 16M
```

En aquest cas, hauríem d'augmentar la memòria a 64M, per exemple, en el fitxer `etc/php5/apache2/php.ini`.

Ens apareixerà la finestra que veiem en la figura 3.8.

FIGURA 3.8. Pantalla inicial phpldapadmin



Configuració del phpLDAPAdmin

La configuració del phpLDAPAdmin s'emmagatzema en un arxiu anomenat **/etc/phpldapadmin/config.php**. Aquest arxiu conté sentències php que configuren el funcionament del phpLDAPAdmin i comentaris que expliquen les sentències. Aquest comentaris són molt útils com a ajuda a l'usuari per a la configuració. Haurem d'editar i modificar aquest arxiu per a qualsevol configuració nova que vulguem que adquiereixi l'aplicació per defecte.

Per exemple, per tal que mostri gràficament l'arbre del directori que tenim configurat en el nostre servidor OpenLDAP, haurem de fer els canvis següents:

Deixar en blanc els paràmetres de la matriu (*array*) de la línia següent que per defecte són dc=example, dc=com'

Abans

```

1  /* Array of base DNs of your LDAP server.
2   Leave this blank to have phpLDAPAdmin auto-detect it for you. */
3
4
5 $ldapservers->SetValue($i,'server','base',array('dc=example,dc=com'));

```

Després

```

1  /* Array of base DNs of your LDAP server.
2   Leave this blank to have phpLDAPAdmin auto-detect it for you. */
3
4
5 $ldapservers->SetValue($i,'server','base',array());

```

També es pot configurar l'arxiu config.php perquè el phpLDAPAdmin pugui gestionar múltiples servidors LDAP. Hauríem de modificar les línies següents:

```

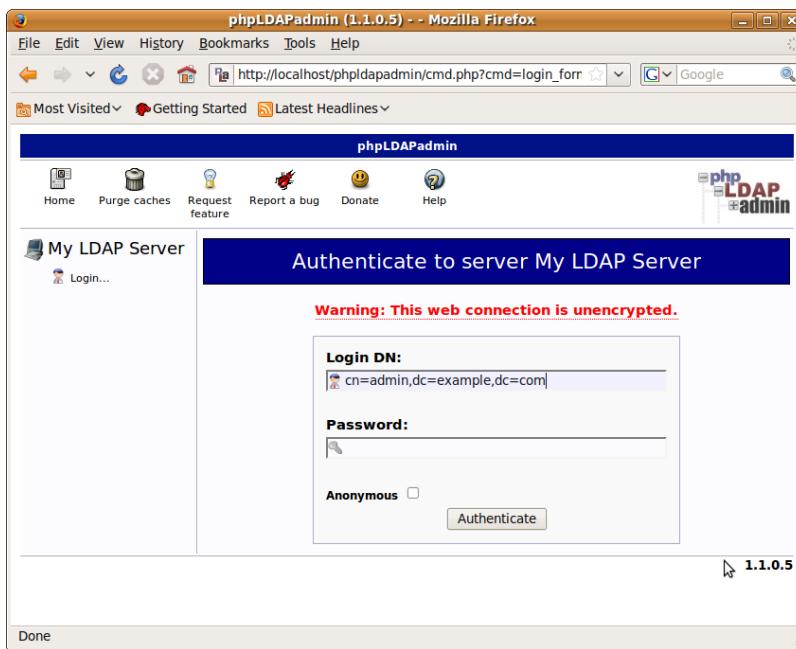
1 /* If you want to configure additional LDAP servers, do so below. *
2  * Remove the commented lines and use this section as a template for all *
3  * your other LDAP servers.*/
4 $i++;
5 $ldapservers->SetValue($i,'server','name','LDAP Server');
6 $ldapservers->SetValue($i,'server','host','127.0.0.1');
7 $ldapservers->SetValue($i,'server','port','389');
8 $ldapservers->SetValue($i,'server','base',array(''));
9 $ldapservers->SetValue($i,'server','auth_type','cookie');
```

Creació i gestió del directori amb el phpLDAPAdmin

Una vegada configurada l'aplicació i adaptada a les nostres necessitats, el pas següent és introduir les dades a l'arbre o arbres de directoris que volem administrar. Per senzillesa, només gestionarem un directori, el directori configurat en els exemples anteriors amb el servidor OpenLDAP.

El primer pas per accedir a la gestió del directori és autenticar-se en la pantalla inicial de l'aplicació, que podem veure en la figura 3.9. Per fer-ho, haurem d'introduir el nom del domini del servidor OpenLDAP que volem gestionar i la contrasenya d'administrador. Recordem que si ens validem com a usuaris anònims, només podrem fer operacions de consulta. Per a qualsevol altra operació ens hem d'autenticar com a administrador:

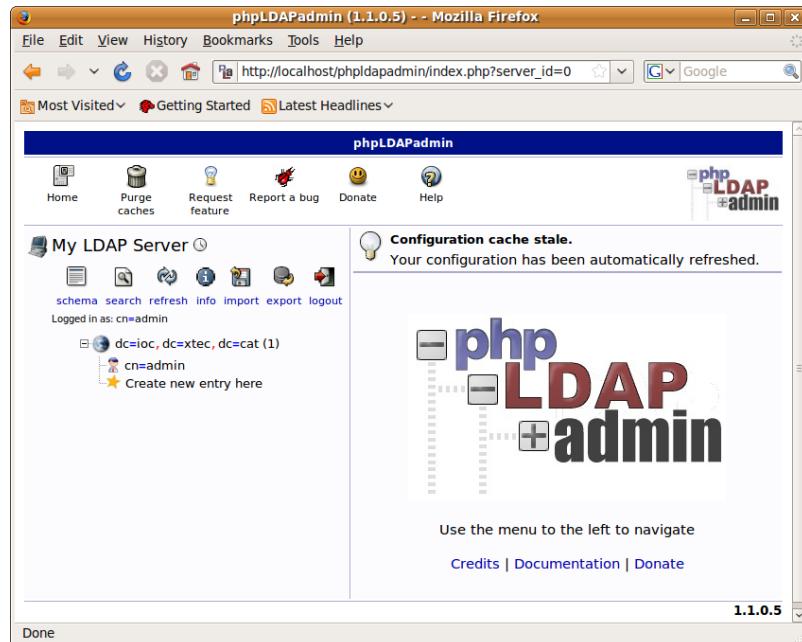
FIGURA 3.9. Pantalla de login de phpldapadmin



Per tal d'autenticar-nos com a administrador en l'aplicació, cal que en la casella **Login DN** introduïm **cn=admin** seguit del nom de la base del directori que hem establert en la configuració del servidor OpenLDAP, en aquest cas **dc=ioc,dc=xtec,dc=cat**. En la casella **Password** hem d'introduir la contrasenya d'administrador també establerta en configurar el servidor. Si les dades són

correctes, accedirem a una finestra similar a la de la pantalla que es mostra en la figura 3.10.

FIGURA 3.10. Pantalla inicial després d'autenticar-se al directori



Aquesta és la pantalla general per mitjà de la qual podem gestionar les dades del nostre directori. Observem que ja ens apareix l'arbre de directori (DIT) que hem configurat anteriorment (prèviament hem modificat el fitxer /etc/phpldapadmin/config.php, com hem comentat abans).

Per introduir les dades del directori amb el phpLDAPadmin, tenim dues opcions: importar un fitxer en format LDIF o bé utilitzar la interfície gràfica que ens proporciona l'aplicació per crear-les. Vegem totes dues opcions.

La importació de dades des d'un fitxer LDIF requereix que el fitxer tingui el format correcte perquè l'aplicació ho interpreti adequadament. Un exemple de fitxer seria el següent:

```

1 dn: cn=Juan Perez Perez,dc=ioc,dc=xtec,dc=cat
2   givenName: Juan
3   sn: Perez Perez
4   cn: Juan Perez Perez
5   o: IOC
6   l: Barcelona
7   mail: juanp@ioc.xtec.cat
8   objectClass: inetOrgPerson
9   objectClass: top
10  objectClass: posixAccount
11  userPassword: {MD5}7MG0cT7vQcbuYe8NY/J0mw==
12  gidNumber: 100
13  homeDirectory: /home/juanp
14  uid: juanp
15  uidNumber: 1

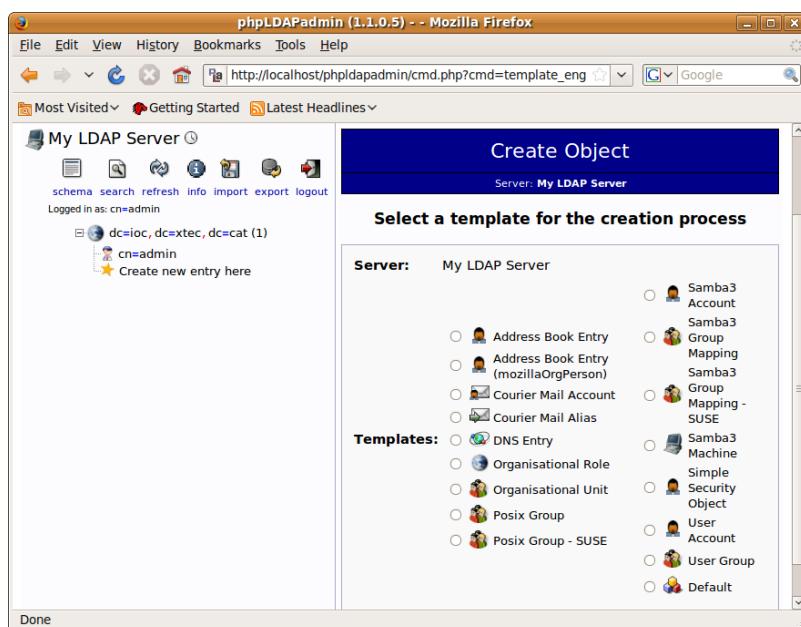
```

Una vegada tinguem el fitxer amb el format correcte, seleccionarem l'opció **import**, que apareix al damunt de l'arbre de directori i ens permetrà seleccionar el fitxer d'importació que volem. Després de seleccionar-lo, cal que cliquem a

Proceed. Si no hi ha cap error, ens afegirà les entrades corresponents a l'arbre del directori.

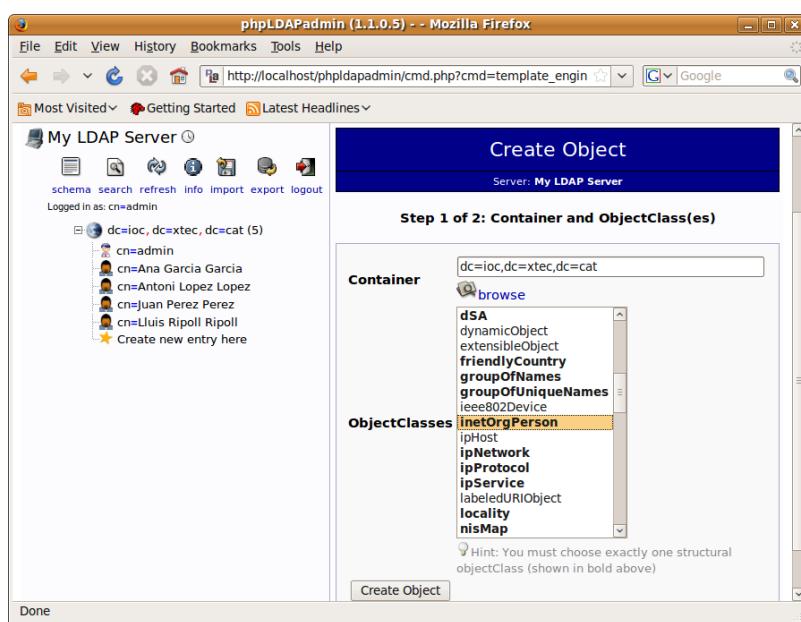
Si volem introduir les dades manualment, haurem de seleccionar **Create new entry here**. A continuació, apareixerà la pantalla de la figura 3.11, en què podrem escollir el tipus d'entrada que volem afegir a l'arbre del directori.

FIGURA 3.11. Introducció de dades al directori



Si la classe d'objecte que busquem no apareix en les plantilles per defecte, podem seleccionar l'opció **Default**, que ens permetrà escollir entre tots els objectes possibles del directori LDAP, com veiem en la figura 3.12.

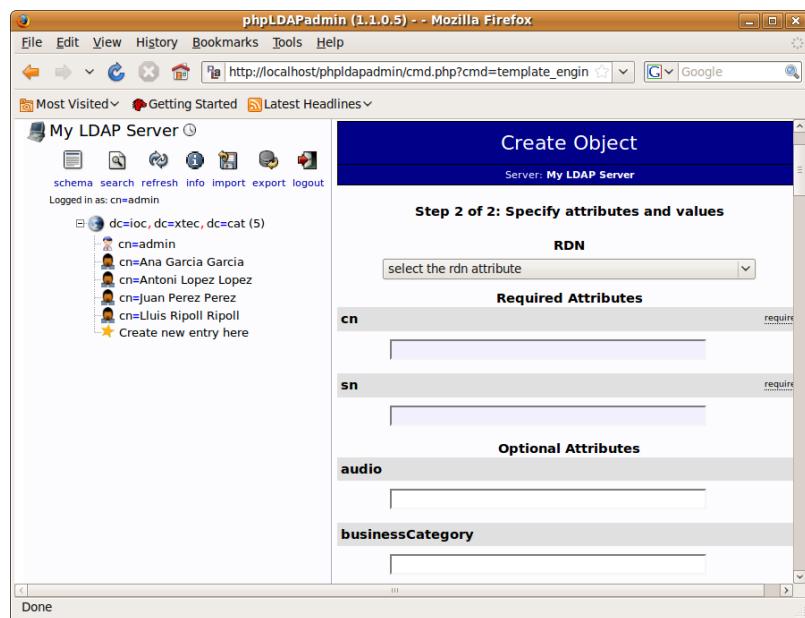
FIGURA 3.12. Selecció del la classe de l'objecte



Una vegada seleccionat l'objecte, només caldrà emplenar els atributs que ens

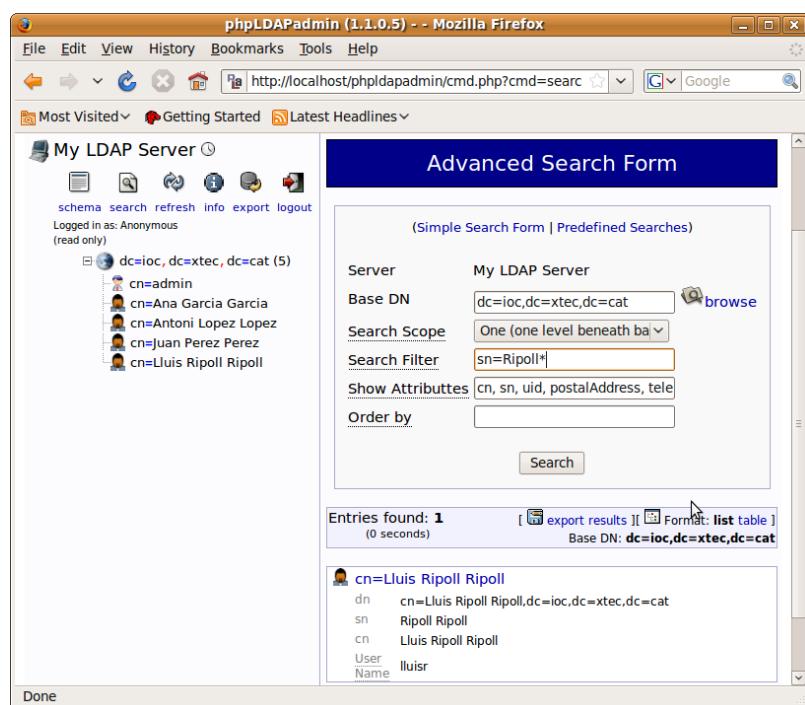
demaní per tal de crear-lo, com veiem en la figura 3.13. Recordem que cada objecte pot tenir atributs opcionals i obligatoris. L'aplicació només ens permetrà crear un objecte si n'emplenem tots els atributs obligatoris.

FIGURA 3.13. Introducció dels valors dels atributs de l'objecte creat



Altres opcions imprescindibles, definides en el model estàndard de l'LDAP, que ens proporciona el phpLDAPadmin són la cerca de dades dins del directori (ldapsearch) i l'exportació del directori en un fitxer (ldapcat). La cerca d'informació en el directori s'efectua mitjançant una sèrie de paràmetres que ens permeten delimitar el rang de cerca i determinar el format de sortida de les dades. Per fer la cerca premem el botó **search**. A continuació, ens apareixerà la pantalla de la figura 3.14.

FIGURA 3.14. Opcions de recerca

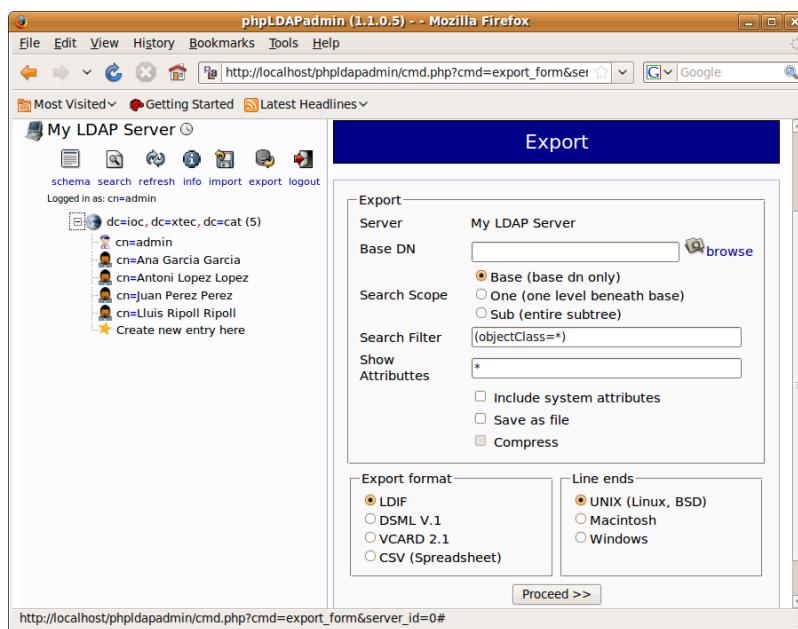


El significat dels paràmetres o els camps que podem especificar per a la cerca són els següents:

- **Base DN:** especifica el DN en què s'indica el punt de partida per a la cerca.
- **Search Scope:** àmbit de la recerca, pot ser:
 - **Base:** només es cerca en l'entrada base.
 - **One:** es cerca en el nivell immediatament inferior a l'entrada base.
 - **Subtree:** es cerca en tot el subarbre sota l'entrada base.
- **Search Filter:** filtre de cerca, indica el criteri de cerca.
- **Show attributes:** atributs a mostrar, es pot indicar quins atributs es retornen i si es retorna el valor de l'atribut o el tipus de dada que conté.
- **Order by:** determina l'ordre de les dades retornades.

Per exportar les dades del directori a un fitxer de text, cal que seleccionem l'opció **export**, que apareix al damunt de l'arbre del directori. Apareixerà la pantalla que es mostra en la figura 3.15, en què podrem escollir els paràmetres que determinaran les dades que volem i amb quin format les volem exportar. Després de seleccionar les dades, clicarem a **Proceed**. Si marquem la casella **Save as file**, ens generarà el fitxer amb les dades corresponents i el format especificat.

FIGURA 3.15. Opcions d'exportació de dades



Es poden fer més operacions amb aquest o altres exploradors gràfics. Deixarem que els alumnes explorin la resta d'opcions i d'altres eines gràfiques per gestionar el directori.

4. Autenticació d'usuaris en xarxes GNU/Linux

Per entendre el funcionament de l'autenticació d'usuaris en xarxes GNU/Linux és necessari conèixer el significat del concepte *domini* i quina és la traducció d'aquest concepte en sistemes GNU/Linux. També és imprescindible saber com funciona el sistema de gestió d'usuaris i grups en els sistemes GNU/Linux i el procés de configuració de l'autenticació d'usuaris en una xarxa formada per xarxes GNU/Linux.

4.1 Què és un domini?

Quan parlem de *domini* podem referir-nos a dos conceptes:

- Domini d'Internet
- Domini d'administració de sistemes

Un *domini d'Internet* és una estructura jeràrquica de noms separats per punts que, per mitjà dels servidors de noms de domini, permet determinar la ubicació (adreça IP) d'un equip connectat a Internet.

Cada nom de l'estructura determina un servidor DNS que coneix l'adreça IP de l'equip amb el nom anterior en l'estructura (excepte el primer nom que determina el node en qüestió).

L'objectiu, juntament amb el servei de noms de domini, és traduir les adreces IP dels nodes actius de la xarxa en paraules més fàcils de recordar per a les persones.

També podeu utilitzar el servei de noms de domini en la vostra xarxa local per identificar les màquines de la xarxa amb noms.

Des del punt de vista de l'administració de sistemes, un *domini* constitueix un conjunt d'equips interconnectats en una xarxa local que comparteixen informació administrativa centralitzada (usuaris, grups, contrasenyes, etc.). Aquesta informació es fa servir per poder autenticar-se i crear un entorn inicial de treball per als usuaris que, segons els seus permisos, podran accedir als recursos que proporciona el sistema.

L'autenticació per mitjà de la xarxa en sistemes GNU/Linux requereix fonamentalment la disponibilitat d'almenys un o diversos ordinadors que emmagatzeminen físicament aquesta informació i que la comuniquin a la resta de màquines connectades en xarxa, quan sigui necessari, mitjançant un esquema client-servidor.

Domini Windows

El concepte de domini en l'administració de sistemes és pròpiament un concepte Windows. En aquest àmbit, un *domini* fa referència a un conjunt de recursos de xarxes, controlats per servidors NT, als quals un usuari pot accedir mitjançant un únic usuari i contrasenya. Quan parlem de domini en sistemes GNU/Linux fem referència a l'autenticació d'usuaris en xarxa, és a dir, a un grup de màquines que s'autentiquen per mitjà d'un o diversos servidors en què hi ha la base de dades dels usuaris amb els seus atributs o, dit d'una altra manera, el directori d'usuaris.

Per exemple, quan un usuari vol iniciar una sessió en qualsevol ordinador client del grup d'autenticació (domini), aquest ordinador haurà de validar les dades de l'usuari en el servidor i obtenir del mateix servidor tota la informació necessària per poder crear el context inicial de treball per a l'usuari.

En el món GNU/Linux, l'autenticació per mitjà de la xarxa se solia implementar mitjançant els NIS (*network information services*), que tenia moltes variants. No obstant això, **la integració de serveis de directori en GNU/Linux, com l'LDAP, ha possibilitat la incorporació d'aquesta tecnologia, molt més potent i escalable que el NIS, en la implementació de dominis.**

Per exemple, en el Windows 2000 la implementació del concepte de domini es fa mitjançant el denominat **directorii actiu** (*active directory*), un servei de directori basat en diferents estàndards, com l'LDAP i el DNS.

Els serveis NFS i Samba els veurem en la unitat "Compartir recursos en xarxa i seguretat en sistemes lliures i propietaris". El muntatge, la configuració i la gestió d'un domini amb el Samba i l'LDAP, en la unitat "Integració de sistemes lliures i propietaris".

En GNU/Linux s'aconsegueix un efecte similar al del directori actiu en combinar un servei que actua com a servidor de comptes i grups i un altre servei que permet exportar directoris a màquines remotes. En concret, aquests serveis són l'LDAP, el Samba o l'NFS, respectivament.

Aquest tipus de sistemes normalment s'utilitzen en empreses i organitzacions mitjanes i grans.

Avantatges:

- Administració centralitzada: el domini sencer es pot administrar des d'una sola base de dades.
- Procés d'autenticació únic (*single logon process*): el control d'accés als recursos es pot fer amb un sol *login*.
- Escalabilitat: és un sistema més escalable, és a dir, el sistema té una habilitat més gran per estendre el marge d'operacions sense perdre qualitat, a més de compaginar un creixement continu de treball d'una manera fluida.

Inconvenients:

- Els inconvenients típics dels sistemes centralitzats: si cau el servidor, cau tota la xarxa. D'aquesta manera, és molt important la seguretat del sistema i utilitzar recursos com ara la replicació del sistema, la redundància, les còpies de seguretat, etc.

Redundància i replicació

Redundància fa referència a l'emmagatzematge de les mateixes dades diverses vegades en diferents llocs, normalment dins del mateix sistema.

Replicació fa referència a la còpia i al transport de dades entre dos o més servidors, per tal d'augmentar la disponibilitat de les dades.

- La complexitat de configuració i manteniment potser no compensa si es tracta d'un nombre reduït de màquines.

4.2 Autenticació en els sistemes GNU/Linux

Cal conèixer com es gestiona l'autenticació tradicional en els sistemes GNU/Linux. Per entendre millor el funcionament de l'autenticació en els sistemes GNU/Linux, és necessari saber quins arxius i eines utilitzen els sistemes per gestionar els comptes d'usuaris i grups, i els perfils que tenen.

L'autenticació és l'acte d'establiment o confirmació d'alguna cosa o persona com a autèntica. L'autenticació d'un objecte pot significar la confirmació de la seva procedència, mentre que l'autenticació d'una persona sovint consisteix a verificar-ne la identitat.

L'autenticació es pot considerar un dels tres passos fonamentals en termes de seguretat de xarxes. Aquests passos són els següents:

1. Autenticació, és el procés de verificar la identitat digital del remitent d'una comunicació, com una petició per connectar-se. El remitent que és autenticat pot ser una persona que usa un ordinador, un ordinador o un programa de l'ordinador.

Per exemple, en un servei de directori l'autenticació és una manera d'assegurar que els usuaris són qui diuen que són, és a dir, que l'usuari que intenta fer funcions en el sistema és, de fet, l'usuari que té l'autorització per fer-les.

2. Autorització, és el procés pel qual la xarxa autoritza l'usuari identificat a accedir a determinats recursos d'aquesta xarxa.

3. Auditoria, mitjançant la qual la xarxa o els sistemes associats registren tots els accessos als recursos que fan els usuaris autoritzats o no.

4.2.1 Mecanisme general d'autenticació

La major part dels sistemes informàtics i de xarxes mantenen d'una manera o altra una relació d'usuaris associats normalment amb un perfil de seguretat, amb privilegis i permisos.

L'autenticació dels usuaris permet que aquests sistemes assumeixin amb una seguretat raonable que qui s'hi connecta és qui diu ser. D'aquesta manera, les accions que s'executen en el sistema després es poden referir a l'usuari i el sistema pot aplicar els mecanismes d'autorització i auditoria oportuns. Per tant, el primer element necessari per a l'autenticació és que hi hagi identitats amb un identificador únic o *login*.

El procés general d'autenticació consta dels passos següents:

1. L'usuari sol·licita accés a un sistema.

2. El sistema sol·licita a l'usuari que s'autentiqui.
3. L'usuari aporta les credencials que l'identifiquen i permeten verificar l'autenticitat de la identificació.
4. El sistema valida segons les seves regles si les credencials aportades són suficients per donar accés a l'usuari o no.

4.2.2 Gestió d'usuaris en els sistemes GNU/Linux

Per entendre millor la gestió d'usuaris en els sistemes GNU/Linux, cal que tingueu presents els conceptes següents:

Els *comptes d'usuari* permeten la identificació d'accés al sistema o a la xarxa. Són estructures de dades administratives que permeten reunir totes les dades associades a un mateix usuari. En un sistema GNU/Linux, els comptes d'usuaris poden estar lligats a usuaris reals, és a dir, persones físiques que utilitzen el sistema. També els poden utilitzar aplicacions específiques per fer servir els permisos i els drets del sistema. Els comptes d'usuari engloben el conjunt d'atributs que caracteritzen l'usuari i també tots els fitxers i els directoris associats a l'usuari. Cal una base de dades per emmagatzemar els usuaris. Tradicionalment, els sistemes GNU/Linux emmagatzemaven la informació dels comptes d'usuaris en l'arxiu /etc/passwd.

Els *grups* són estructures lògiques que es fan servir per organitzar els usuaris amb un propòsit i unes característiques comuns. Quan es concedeix la pertinença a un grup a un usuari, se li assignen automàticament totes les propietats, drets, característiques, permisos i privilegis d'aquest grup. Els sistemes GNU/Linux emmagatzemaven la informació dels distints grups en l'arxiu /etc/group.

Cada usuari i grup del sistema té un identificador únic anomenat *userid* (UID) i *groupid* (GID), respectivament. El sistema utilitza aquest identificador, en comptes de noms, per diferenciar unívocament entre els usuaris i els grups.

La funció principal de l'existència dels usuaris i els grups en els sistemes GNU/Linux és la d'autenticació, que permet accedir al sistema. Cada usuari disposa d'un nom d'usuari o *login* i una contrasenya que haurà d'utilitzar per iniciar una sessió en el sistema. El sistema, mitjançant el procés d'autenticació, comprovarà que l'usuari existeix i que la paraula de pas que fa servir coincideix amb la contrasenya emmagatzemada de manera encriptada. Una vegada dins del sistema, cada usuari disposarà dels permisos i els drets que determini el grup al qual pertany i d'un perfil establert per defecte.

A més de l'autenticació en el sistema, una de les utilitats principals dels usuaris i els grups és la gestió dels recursos del sistema. Per exemple, quan es crea un fitxer

El *login* s'utilitza per la comoditat de les persones, ja que resulta més fàcil recordar-se d'un nom que no pas d'un identificador numèric.

El perfil, per defecte, pot ser determinat per l'administrador del sistema.

en el sistema, se li assigna automàticament un usuari i un grup. De la mateixa manera, al fitxer se li assignen els permisos d'escriptura, lectura i execució per a l'usuari propietari del fitxer, per al grup al qual pertany el propietari i per a la resta d'usuaris del sistema.

umask

El paràmetre que determina quins permisos s'apliquen a un arxiu o un directori nou és l'umask. Aquest paràmetre es configura a l'arxiu /etc/bashrc. Els sistemes GNU/Linux permeten especificar les màscares de dues maneres, mitjançant un permís per defecte, també anomenat *màscara simbòlica*, per exemple, u=rwx,g=rwx,o=, o mitjançant un nombre en octal que controla quins permisos s'emmascararan, no s'establiran, per a qualsevol arxiu nou, per exemple, 007. Així doncs, tradicionalment, el valor d'umask es configura en mode octal a 022, que només permet tots els permisos a l'usuari que crea l'arxiu o el directori. A la resta d'usuaris, inclosos els del seu grup, només els dóna permisos de lectura.

Quan instal·leu un sistema GNU/Linux, per defecte es creen una sèrie d'usuaris i grups necessaris perquè el sistema i algunes aplicacions funcionin correctament. Podeu distingir tres tipus de comptes d'usuari i tres tipus de comptes de grup. Entre els comptes d'usuari, hi ha els següents:

- **root:** aquest compte correspon a l'administrador del sistema que s'encarrega de les tasques administratives del sistema. No està afectat pels drets d'accés als arxius i pot efectuar més o menys qualsevol tasca en el sistema. Per tant, aquest compte és imprescindible per a l'administració del sistema. El seu UID és 0.
- **Usuaris de sistema:** hi ha una sèrie de comptes que no s'assignen a persones físiques. Aquests comptes serveixen per facilitar l'administració dels drets d'accés de certes aplicacions i dimonis. Solen tenir com a UID un número entre l'1 i el 499. Ordres com useradd o groupadd tenen una opció (-r, --system) que permet crear usuaris o grups de sistema, com ara bin, daemon, sync, apache, etc.
- **Usuaris:** aquests usuaris es corresponen amb la resta de comptes d'usuari del sistema. Aquest tipus de comptes s'associen a persones reals i una de les funcions principals que fan és permetre als usuaris estàndards connectar-se i utilitzar els recursos de l'equip. Normalment, l'UID d'un usuari és un número superior a 999, encara que aquests rangs es poden configurar.

Quant als diferents tipus de grups en el GNU/Linux, hi ha els següents:

- **root:** el seu GID és 0. Es correspon amb el grup principal de l'administrador.
- **Grups de sistema:** tenen la mateixa funció que els comptes del mateix nom i permeten donar els mateixos drets d'accés a una sèrie d'aplicacions.
- **Grups d'usuaris:** representen una sèrie de persones reals que han d'accendir als mateixos arxius. Normalment tenen un GID superior o igual a 500 o 1000, en funció de com estigui configurat el sistema.

Quan creem un usuari, per facilitar la gestió dels permisos i els drets, el sistema crea un grup d'usuari nou amb el nom de l'usuari mateix. L'usuari és l'únic membre d'aquest grup.

Els arxius de configuració en què s'emmagatzema la informació dels usuaris, els grups i les contrasenyes, i mitjançant els quals es gestiona l'autenticació i la seguretat d'accés als sistemes GNU/Linux, són els arxius **/etc/passwd**, **/etc/group** i **/etc/shadow**. El contingut i el funcionament d'aquests arxius s'explica a continuació.

4.2.3 L'arxiu /etc/passwd

L'arxiu **/etc/passwd** és el que utilitzen els sistemes GNU/Linux per emmagatzemar la informació dels usuaris del sistema. Tots els usuaris han de tenir una entrada en aquest arxiu per poder accedir al sistema.

Per defecte, l'arxiu **/etc/passwd** és propietat de l'usuari root i proporciona tot els permisos. La resta d'usuaris del sistema només poden llegir l'arxiu. L'arxiu **/etc/passwd** està format per una sèrie de línies que contenen un conjunt de camps separats per dos punts. Cadascuna d'aquestes línies emmagatzema informació d'un usuari. El format és el següent:

1 `nom_us:clau:UID:GID:coment:dir_us:prog_inici`

- **nom_us:** Aquest camp és el nom d'usuari (*login*) que s'utilitza per accedir al sistema, és un camp obligatori.
- **clau:** Aquest camp correspon a la clau que l'usuari utilitza per accedir al sistema. El camp clau està encriptat i realment no s'emmagatzema en aquest arxiu, sinó en l'arxiu **/etc/shadow**. La raó per la qual la clau s'emmagatzema en un arxiu distint és la seguretat, ja que tots els usuaris del sistema tenen permisos de lectura sobre l'arxiu **/etc/passwd** i es podrien utilitzar tècniques de *cracking* per desencriptar les claus d'altres usuaris. Normalment apareix una *x* en el camp.
- **UID:** És el número que identifica unívocament l'usuari i, per tant, no es pot repetir. També és un camp obligatori per a cada usuari. Per defecte, l'usuari root té el valor 0.
- **GID:** Aquest camp és el número que identifica el grup de l'usuari i està associat a una línia en l'arxiu **/etc/group**. Cada usuari ha de pertànyer, com a mínim, a un grup.
- **coment:** En aquest camp s'emmagatzemen dades de l'usuari, com ara el telèfon, l'adreça, etc. Aquestes dades se separen per comes i són opcionals.
- **dir_us:** Aquest camp determina el camí (*path*) complet del directori. En funció de l'ordre que utilitzem per crear l'usuari, aquest directori es generarà automàticament en crear l'usuari o no.

- **prog_inici:** Aquest camp especifica el programa que s'ha d'executar cada vegada que l'usuari accedeix al sistema. Normalment, aquest programa es correspon amb l'embolcall (*shell*) amb què l'usuari ha de treballar.

4.2.4 L'arxiu /etc/group

L'arxiu */etc/group* és el que utilitzen els sistemes GNU/Linux per emmagatzemar la informació dels grups que hi ha en el sistema. Tots els grups han de tenir una entrada en aquest arxiu i tots els usuaris han de pertànyer a algun grup.

L'arxiu */etc/group* és propietat de l'usuari root. La resta d'usuaris del sistema només el poden llegir. L'arxiu */etc/group* està format per una sèrie de línies que contenen un conjunt de camps separats per dos punts. Cadascuna d'aquestes línies emmagatzema informació d'un grup. El format és el següent:

¹ nom_grup:clau:GID:lista_components

- **nom_grup:** Aquest camp correspon al nom amb el qual s'identifica el grup.
- **clau:** Correspon a la clau xifrada assignada al grup. Actualment no s'utilitza. Aquesta clau, si hi és, s'emmagatzema en l'arxiu */etc/gshadow*, que té la mateixa funcionalitat que l'arxiu */etc/shadow*, és a dir, emmagatzemar les claus encriptades. En aquest cas, però, per als grups.
- **GID:** aquest camp determina el número identificador del grup, que ha de ser igual al dels usuaris que pertanyen a aquest grup i que apareix en l'arxiu */etc/passwd*.
- **lista_components:** és una llista dels usuaris, separats per comes, que pertanyen al grup.

4.2.5 L'arxiu /etc/shadow

L'arxiu */etc/shadow* és l'arxiu en què els sistemes GNU/Linux emmagatzemen les contrasenyes xifrades dels usuaris per garantir l'accés al sistema. Per motius de seguretat, aquest arxiu només el pot editar el superusuari i només el poden llegir els usuaris que pertanyen al grup del superusuari.

L'arxiu */etc/shadow* emmagatzema la informació en files que contenen les dades següents:

¹ nom_us:clau:ult_canvi:pue_canvi:ha_de_canvi:avís:cad:desha:reservat

- **nom_us:** és el nom que l'usuari utilitza per identificar-se en el sistema.

- **clau:** aquest camp correspon a la contrasenya xifrada de l'usuari anterior.
- **ult_canvi:** són els dies que han transcorregut des de l'1 de gener de 1970 fins el dia que es va canviar la contrasenya per última vegada. Serveix per calcular quant de temps fa que no es canvia la contrasenya.
- **ha_de_canvi:** són els dies que han de passar perquè un usuari pugui canviar la seva contrasenya.
- **avís:** aquest camp determina el nombre de dies d'antelació amb els quals s'avisarà un usuari perquè canvii la contrasenya abans que caduqui.
- **cad:** aquest camp especifica el nombre de dies que han de transcórrer des que la contrasenya ha expirat fins que es deshabilita.
- **deshà:** nombre de dies, des de l'1 de gener de 1970, que fa que el compte està deshabilitat.
- **reservat:** camp reservat per al sistema.

Per tal d'ingressar en el sistema amb un usuari, podeu utilitzar les ordres amb nom_usuari o login nom_usuari.

4.2.6 Eines de gestió d'usuaris

Els sistemes GNU/Linux incorporen una sèrie d'eines, tant per línia d'ordres com gràfiques, per gestionar els usuraris i els grups del sistema. Entre les ordres que proporciona el sistema, hi ha les següents:

- **useradd, adduser, groupadd, addgroup:** aquestes ordres permeten al superusuari crear usuraris i grups nous en el sistema. Depenen de la distribució amb la qual treballem, aquestes ordres funcionen igual o no. En l'Ubuntu hi ha diferències entre aquestes ordres. Les ordres adduser i addgroup són més completes, ja que realment són *scripts* de Perl que utilitzen les ordres useradd i groupadd per crear usuraris i grups. De fet, les ordres adduser i addgroup ens permeten crear tots els paràmetres (la contrasenya, el directori de l'usuari, etc.) dels usuraris i els grups alhora. L'ordre useradd posseeix un fitxer de configuració anomenat */etc/default/useradd*, en què podem configurar els paràmetres per defecte que es fan servir per crear usuraris nous. Per exemple, podem especificar un directori distint a */etc/skel* per crear els directoris dels usuraris a partir d'aquest.
- **usermod, groupmod:** són ordres que es fan servir per modificar la informació sobre els usuraris i els grups respectivament. Només les pot utilitzar l'usuari root.
- **userdel, deluser, groupdel, delgroup:** permeten al superusuari esborrar usuraris i grups del sistema. El funcionament també depèn de cada distribució, com en el cas de les ordres de creació.
- **passwd:** ordre que es fa servir per establir o actualitzar la contrasenya dels usuraris que hi ha en el sistema.

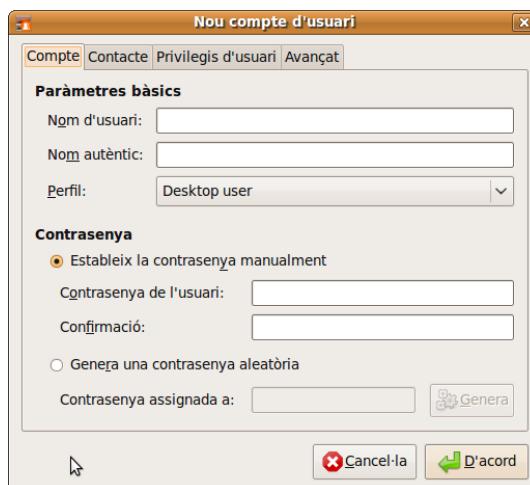
- **users:** aquesta ordre s'utilitza per imprimir els noms dels usuaris que actualment estan connectats a la màquina.
- **groups:** ordre que es fa servir per veure els usuaris que hi ha en el sistema.
- **id:** ordre que mostra l'usuari amb el qual s'ha ingressat en el sistema i els grups als quals pertany aquest usuari.
- **pwck:** ordre que permet comprovar la integritat dels fitxers d'autenticació, tant /etc/passwd com /etc/shadow.
- **chage:** ordre que permet modificar les dades d'expiració de les paraules de pas dels usuaris.

L'Ubuntu també proveeix una interfície gràfica senzilla per gestionar els usuaris i els grups, com es pot observar en la figura 4.1. Hi podeu accedir mitjançant el menú *Sistema > Administració > Usuaris i grups*.

FIGURA 4.1. Interfície gràfica de gestió d'usuaris



FIGURA 4.2. Quadre de creació d'un nou usuari



S'obrirà un quadre que us mostrarà els usuaris i els grups del sistema. Haureu de **desbloquejar** la finestra. Caldrà que introduïu la contrasenya de superusuari per poder afegir, modificar o esborrar usuaris o grups. Després de desbloquejar la finestra anterior i seleccionar si voleu modificar o afegir un usuari nou, us apareixerà un quadre com el de la figura 4.2, en què podreu especificar els diferents

paràmetres de cada usuari. Per treballar amb grups, premeu el botó **Gestiona els grups**.

4.2.7 Perfil d'usuari

En la majoria de sistemes en xarxa interessa que els usuaris es puguin presentar en més d'una estació de treball i que aquesta connexió sigui independent del lloc, de manera que el treball en una estació o una altra sigui transparent. A més, pot interessar a l'administrador tenir la possibilitat de forçar l'ús de determinats programes o restringir els canvis en l'aparença de la interfície gràfica a certs grups d'usuaris. D'aquesta manera, els sistemes operatius GNU/Linux incorporen utilitats que associen a cada compte d'usuari o grup un perfil concret.

Els perfils d'usuari permeten configurar l'entorn de treball personalitzat de cada usuari. Permeten definir elements com l'entorn d'escriptori, la configuració de xarxa, les impressores, etc.

Hi ha diferents tipus de perfils d'usuari:

- **Perfil d'usuari local**, es crea la primera vegada que un usuari inicia una sessió a la màquina i s'emmagatzema en el disc dur local. Totes les modificacions efectuades en aquest tipus de perfil són específiques de l'equip concret en què s'han efectuat.
- **Perfil d'usuari mòbil**, està orientat a l'autenticació en xarxa mitjançant servidors. Aquest tipus de perfil el crea l'administrador del sistema i s'emmagatzema en un servidor. El perfil es descarrega a l'equip local quan l'usuari inicia la sessió.

Per entendre millor com funcionen els perfils d'usuaris i els fitxers implicats en la configuració, cal veure primer els tipus d'intèrprets d'ordres que podeu trobar en els sistemes GNU/Linux i els fitxers que s'executen per a cada tipus. Generalment, la majoria de distribucions GNU/Linux utilitzen per defecte l'intèrpret d'ordres bash. Durant el procés d'arrencada del sistema, s'executa una sèrie d'*scripts* amb l'objectiu de crear un entorn d'usuari. Entre aquests *scripts* hi ha els que activen els terminals de consola i l'entorn gràfic. En activar aquests serveis s'invoca un intèrpret d'ordres (*shell*). Cal diferenciar, però, dos tipus d'intèrprets d'ordres en funció de la manera com s'executen.

- **Interactive shell o intèrpret d'ordres interactiu.** Per invocar aquest tipus d'intèrpret d'ordres no s'indica cap paràmetre. També es pot indicar implícitament amb -i.
- **Non-interactive shells o intèrpret d'ordres no interactiu.** Per invocar aquest tipus d'intèrpret s'utilitza l'opció -c. Aquest intèrpret no

llegeix ni executa cap dels fitxers de configuració. Per exemple: -c /path_fins_la_comanda, bash -c /path_fins_la_comanda

Els intèrprets d'ordres interactius poden ser, a la vegada, de dos tipus:

- **Login shell o intèrpret d'ordres de login:** és l'intèrpret d'ordres que s'executa amb els paràmetres - (cap paràmetre) o –login. Normalment només s'executa durant el procés de *login* al sistema. Per exemple, en iniciar un intèrpret d'ordres des d'una consola virtual, en polsar la combinació de tecles *Ctrl + Alt + F1*, en iniciar una sessió gràfica amb un gestor de pantalla (*display manager*), en iniciar una connexió SSH, és a dir, en executar, per exemple, les ordres **bash –, bash –login, ssh user@host**.
- **Non-login shells o intèrpret d'ordres de no login:** constitueix la resta d'execucions d'intèrprets d'ordres. És el tipus d'intèrpret d'ordre que s'executa una eina de terminal, com xterm o gnome-terminal. Es carregaria un intèrpret d'ordres no login, per exemple, en executar les ordres **bash, xterm**.

Configuració de sistema (per-system basis)

Segons l'estàndard FHS (Filesystem Hierarchy Standard), els fitxers de configuració que afecten tot el sistema (*per-system basis*) han de ser en la carpeta /etc. Passa el mateix amb els perfils. Aquests fitxers de configuració globals contenen les configuracions per defecte per a tots els usuaris del sistema. Cal tenir en compte, però, que les configuracions de cada usuari poden sobreescriure les configuracions globals.

FHS és una norma que defineix els directoris principals i els seus continguts en el sistema operatiu GNU/Linux i altres sistemes de la família Unix.

El més habitual és que els fitxers de configuració globals només els puguin editar l'administrador del sistema (usuari root) o els usuaris que tinguin permisos per administrar el sistema. Els fitxers són els següents:

1. /etc/profile: fitxer de configuració de la bash a escala de sistema. **Només s'utilitza amb les bash que siguin de login.** Per tant, aquest *script* només s'interpreta en la connexió de l'usuari. Així, durant l'execució d'aquest *script* es pot efectuar una sèrie d'operacions d'interès general per als usuaris, com ara les següents:

- Executar l'ordre umask per modificar els permisos per defecte a l'hora de crear arxius nous.
- Analitzar si hi ha l'arxiu /etc/motd, que permet especificar un missatge de benvinguda a cada usuari. Si hi és, se'n llista el contingut.
- Establir els paràmetres per defecte per al terminal.
- Analitzar si l'usuari que s'acaba d'identificar té correu en la seva bústia. Si és així, es visualitza un missatge d'avís.

2. /etc/bash.bashrc o /etc/bashrc:

fitxer de configuració de la bash a escala de sistema. Només s'utilitza amb les bash que no siguin de login.

En definitiva, aquests fitxers permeten configurar diverses opcions de la bash, com ara les variables d'entorn, executar ordres cada cop que s'executi l'intèrpret d'ordres, etc. Bàsicament, com que s'executen abans de començar a utilitzar l'intèrpret d'ordres, permeten configurar l'entorn de treball d'aquest intèrpret per a tots els usuaris.

Configuració d'usuari (per-user basis)

També segons l'estàndard FHS, els fitxers que són propietat dels usuaris del sistema són en la carpeta /home. Dins d'aquesta carpeta cada usuari sol ser el propietari de la carpeta /home/nom_usuari. Per exemple, l'usuari Pere és propietari de la carpeta següent:

/home/pere

Com que els fitxers de la carpeta *home* d'un usuari són propietat seva, l'usuari els pot llegir, modificar i, fins i tot, eliminar. Per raons de seguretat, els fitxers de configuració soLEN ser fitxers ocults, és a dir, comencen per “.” (punt). Per veure aquests fitxers cal utilitzar el paràmetre -a de l'ordre ls.

Els fitxers de configuració de la bash a escala d'usuari (*per-user basis*) són els següents:

- **.bashrc:** s'executa només en iniciar una bash de no login.
- **.bash_profile, o .bash_login o .profile:** s'executa un només en iniciar una bash de login.
- **.bash_logout:** S'executa en finalitzar una bash. Inclou, per exemple, les ordres de neteja automàtica (esborrar arxius de treball temporals) i la còpia de dades personals.

Fitxers ocults

Utilitzar fitxers ocults té dos objectius. En primer lloc, amagar fitxers que normalment l'usuari no modifica directament, ja que ho fan les aplicacions. En segon lloc, fa més difícil que l'usuari modifiqui aquests fitxers per error. Se suposa que només l'usuari que sap què fa pot modificar directament aquests fitxers.

La *home* sovint es referencia amb el símbol ~ i, per tant, sovint parlem dels fitxers ~/.bashrc, ~/.bash_logout, etc.

Cal tenir en compte que els usuaris poden modificar els fitxers de la seva *home*. Així doncs, no podeu fer “configuracions obligatòries” mitjançant aquests fitxers. També cal pensar que aquests fitxers normalment s'executen després dels fitxers de configuració de sistema i que, per tant, poden sobreescrivir les configuracions de sistema.

L'ordre d'execució dels fitxers per als distints tipus d'intèrprets d'ordres són els següents:

Login SHELL

Els fitxers es llegeixen i s'executen en l'ordre següent en el cas de la bash:

1. /etc/profile, és el primer que s'executa si hi és. Si no, es passa al fitxer següent.

2. ~/.bash_profile, ~/.bash_login o ~/.profile, després de llegir l'arxiu /etc/profile, si hi és, el procés bash busca els arxius ~/.bash_profile, ~/.bash_login o ~/.profile en aquest ordre. Executa les ordres que hi ha en el primer script que troba i que es pot llegir. Els arxius anteriors només s'interpreten en la connexió amb login. Per tant, les modificacions aportades només es tenen en compte després d'una connexió nova de l'usuari.

3. ~/.bashrc, encara que es tracta d'un fitxer de no login s'executa perquè és cridat implícitament als fitxers de configuració de login.

Es pot evitar que s'executin aquests fitxers si s'utilitza el paràmetre **- - noprofile** en invocar l'intèrpret d'ordres.

No login SHELL

Quan s'executa un intèrpret d'ordres interactiu que no és de login, la bash llegeix i executa les ordres dels fitxers:

1. /etc/bashrc

2. ~/.bashrc

Es pot evitar que s'executin aquests fitxers si s'utilitza el paràmetre **- - norc** en invocar l'intèrpret d'ordres.

Si voleu establir un perfil comú d'usuari per defecte, podeu emmagatzemar els arxius ~/.profile, ~/.bashrc, ~/.bash_logout en el directori **/etc/skel**. En el moment de crear un usuari nou, el contingut es copiarà al directori *home* de l'usuari nou. Cal tenir en compte que els canvis fets en els fitxers de la carpeta /etc/skel només s'apliquen als usuaris nous, no als usuaris que ja hi són.

Si qualsevol dels fitxers de configuració hi és, però l'usuari no el pot llegir, la bash mostra un error.

Per exemple, si creem un usuari nou anomenat *ioc*, en crear el seu compte es crearà un directori nou anomenat */home/ioc*, que serà una còpia del directori /etc/skel.

4.2.8 Altres mecanismes d'autenticació en els sistemes GNU/Linux

A banda de l'autenticació tradicional, els sistemes GNU/Linux permeten utilitzar altres mecanismes d'autenticació. De la gestió i la configuració dels mecanismes d'autenticació diferents al mecanisme tradicional per a les aplicacions en els sistemes GNU/Linux, se n'encarrega el sistema Linux PAM.

PAM (pluggable authentication module)

El mecanisme més utilitzat per les aplicacions per a l'autenticació d'usuaris es diu *PAM* (*pluggable authentication module*) i el podem definir com a:

El PAM és un mecanisme que les aplicacions fan servir per a l'autenticació d'usuaris. No és un model d'autenticació en si, sinó un mecanisme que proporciona una interfície entre les aplicacions d'usuari i els diferents mètodes d'autenticació. D'aquesta manera, intenta solucionar un dels problemes clàssics de l'autenticació d'usuaris: el fet que una vegada que s'ha definit i implantat un mecanisme d'autenticació determinat en un entorn, sigui difícil canviar-lo.

El PAM està compost per un paquet de llibreries compartides que permeten especificar la manera com les diverses aplicacions autenticaran els usuaris.

La utilització del PAM comporta una sèrie d'avantatges. Per exemple, permet utilitzar sistemes d'autenticació diferents del mecanisme tradicional d'autenticació dels sistemes GNU/Linux, fitxer /etc/passwords, sense necessitat de canviar el disseny de les aplicacions. És a dir, podem comunicar les nostres aplicacions amb els mètodes d'autenticació que volem d'una manera transparent. També permet desenvolupar programes amb independència de l'esquema d'autenticació. Utilitza mòduls d'autenticació en temps d'execució i així no ha de tornar a compilar per canviar l'esquema d'autenticació.

El PAM és un producte de SUN i hi ha diverses implementacions que depenen del sistema que es faci servir. La implementació del PAM en el GNU/Linux es coneix amb el nom de *Linux PAM*.

La majoria de sistemes GNU/Linux incorporen l'aplicació Linux PAM en instal·lar-los. Això fa que s'incorporin una sèrie de mòduls bàsics per treballar amb l'autenticació bàsica (paquet libpam-modules). També s'hi poden afegir mòduls addicionals per treballar amb altres autenticacions, com ara l'LDAP.

La gran majoria de les aplicacions dels sistemes GNU/Linux estan preparades per utilitzar el Linux PAM. És a dir, són PAM-aware i utilitzen els diversos mòduls o llibreries que proporciona el PAM per autenticar-se en el sistema.

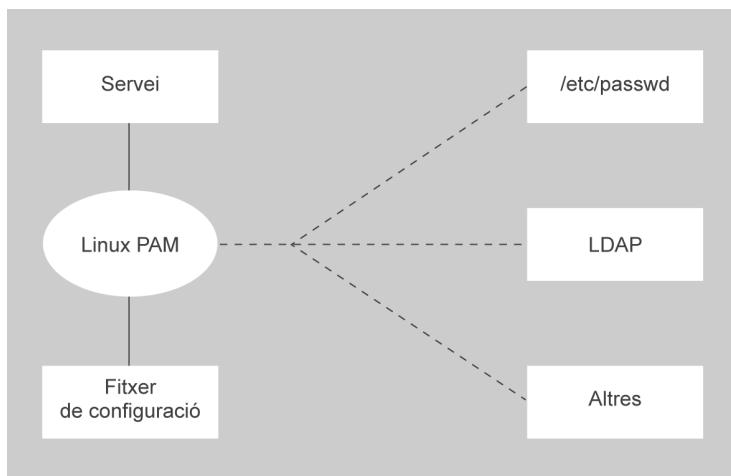
La configuració del funcionament del Linux PAM es fa per mitjà del fitxer **/etc/pam.conf**, en què hi ha totes les dades de configuració juntes, o bé per mitjà de diversos arxius dins del directori **/etc/pam.d**, cosa que facilita el maneig i la comprensió de la configuració.

Quan s'inicia una aplicació preparada per autenticar-se mitjançant el PAM, s'activa la seva comunicació amb la IPA del PAM. Entre altres coses, això força la lectura de l'arxiu de configuració **/etc/pam.conf** o dels arxius de configuració sota el directori **/etc/pam.d** (quan hi ha un arxiu de configuració correcte sota aquest directori, s'ignora l'arxiu /etc/pam.conf).

Com mostra l'esquema de la figura 4.3, els fitxers de configuració del Linux PAM especificuen qui serà el mecanisme d'autenticació per a cada servei o aplicació del sistema. Per tant, no cal modificar el codi del sistema ni de cap aplicació.

IPA

Una IPA (en anglès, API, application program interface) o interfície de programa d'aplicació constitueix el conjunt de funcions i procediments o mètodes, en la programació orientada a objecte, que ofereix una biblioteca d'una aplicació perquè un altre programari l'utilitzi com una capa d'abstracció.

FIGURA 4.3. Esquema PAM

Dins el directori **/etc/pam.d** podeu configurar la manera com cada element s'haurà d'autenticar, els serveis o les aplicacions que requereixen autenticació en el sistema. Per no haver de repetir la configuració per a cada servei, hi ha una sèrie d'arxius comuns, el nom dels quals comença per *common*. Els arxius de configuració de cada servei fan referència a aquests arxius comuns mitjançant una línia @include amb el nom de l'arxiu. Utilitzar aquesta línia té el mateix resultat que copiar el text de l'arxiu al qual fan referència en el fitxer que la conté. Els arxius comuns són **common-auth**, **common-account**, **common-session** i **common-password**.

A continuació s'explica la funcionalitat i la sintaxi d'aquests arxius.

Tots quatre arxius estan formats per línies que determinen una sèrie de regles d'actuació. Cada línia executarà un mòdul que s'encarregarà de l'autenticació. Aquestes regles estan formades per un conjunt de camps amb el format següent:

¹ type control module-path module-arguments

1. Camp type

El camp type especifica l'àmbit al qual afectarà la regla. Els possibles valors són el següents:

- **account:** permet determinar qüestions que no són purament d'autenticació, sinó que estan més relacionades amb la verificació dels comptes d'usuaris. Per exemple, comprovar si la contrasenya ha expirat, comprovar si un compte d'usuari té permès accedir a un servei, etc. Les regles d'aquest tipus les trobem en el fitxer **common-account**.
- **auth:** proporciona el mecanisme d'autenticació, és a dir, com determinem que l'usuari és qui diu que és. Normalment aquesta comprovació es fa amb un *login* i una paraula de pas, però no totes les autenticacions han de ser d'aquest tipus. Per exemple, es poden fer autenticacions basades en maquinari, com targetes intel·ligents o dispositius biomètrics. Només caldria afegir els mòduls adequats per a cada dispositiu.

També s'encarrega de l'assignació de grups. Les regles d'aquest tipus les trobem en el fitxer **common-auth**.

- **password:** proveeix els mecanismes necessaris per actualitzar la contrasenya de l'usuari. Per exemple, especifica el tipus de xifratge que s'aplicarà a la paraula de pas, sha512, md5, etc. Les regles d'aquest tipus les trobem en el fitxer **common-password** i depenen en gran mesura de les que s'especifiquen en el fitxer common-auth.
- **session:** ofereix la possibilitat de fer tasques abans i després que l'usuari s'autentiqui. Per exemple, muntar un directori, activar *logins*, etc. Les regles d'aquest tipus les trobem en el fitxer **common-session**.

2. Camp control

Determina què cal fer un cop l'execució sigui correcta o incorrecta. Hi ha dues sintaxis per a aquest camp: una de senzilla d'un camp i una altra que especifica més d'un camp dins de claudàtors []. Per a la sintaxi bàsica, els possibles valors que pot tenir aquest camp són els següents:

- **requisite:** si el mòdul falla, es denega l'accés a l'usuari immediatament.
- **required:** si el mòdul falla, es denega l'autenticació, però es continua l'execució de la resta de mòduls abans de tornar el control a l'aplicació.
- **sufficient:** el resultat del mòdul s'ignora si falla. Si és un èxit només serà un èxit de tota la pila, és a dir, si cap mòdul *required* ha fallat.
- **optional:** s'ignora el resultat del mòdul. Només és necessari per tal que l'autenticació sigui un èxit.

3. Camp module-path

Especifica el nom del mòdul que és en el directori /lib/security o el camí absolut, és a dir, el nom del directori més el del mòdul, com, per exemple, /lib/security/pam_unix.so.

4. Camp module-arguments

Permet determinar els arguments que es passaran al mòdul. Els arguments varien segons el mòdul.

Així doncs, veiem com a mostra la sintaxi del fitxer common-auth. Per exemple:

```

1 $cat /etc/pam.d/common-auth
2 # here are the per-package modules (the "Primary" block)
3 auth [success=1 default=ignore] pam_unix.so nullok_secure
4 # here's the fallback if no module succeeds
5 auth requisite pam_deny.so
6 # prime the stack with a positive return value if there isn't one already;
7 # this avoids us returning an error just because nothing sets a success code
8 # since the modules above will each just jump around
9 auth required pam_permit.so
10 # and here are more per-package modules (the "Additional" block)
11 auth optional pam_smbpass.so migrate
12 # end of pam-auth-update config

```

Autenticació LDAP

Una vegada conegit el concepte i el funcionament dels serveis de directori i els mètodes d'autenticació en els sistemes GNU/Linux, veurem com podem implementar un mecanisme d'autenticació per mitjà de xarxa en aquests sistemes (domini), en què un conjunt d'equips interconnectats s'autentiquen per mitjà d'un servidor LDAP. Aquesta autenticació permetrà iniciar una sessió de treball en cada màquina i que les aplicacions i els serveis de cada equip es puguen validar de manera transparent mitjançant usuaris i grups que hi hagi en un servidor LDAP.

El procés de configuració per autenticar una estació de treball GNU/Linux en un servidor OpenLDAP el podeu dividir en quatre fases:

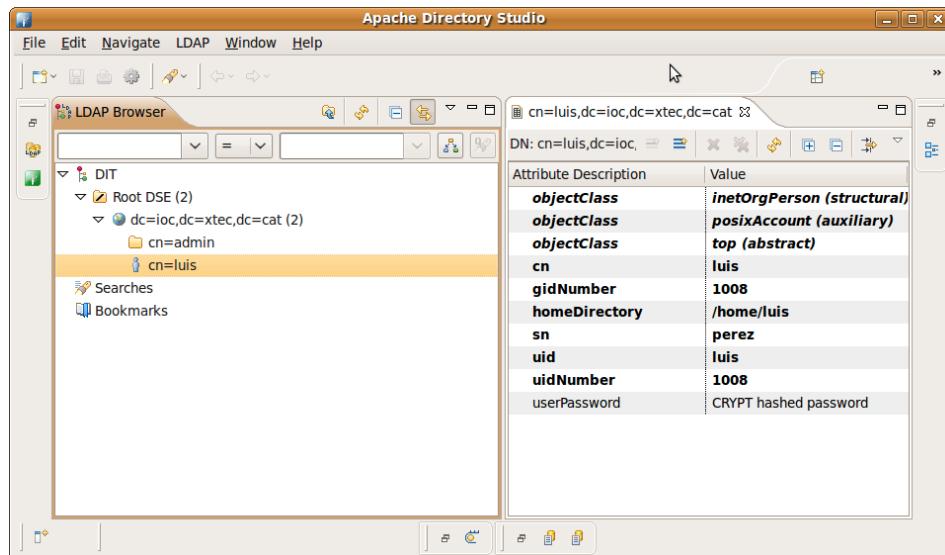
1. Crear o importar els usuaris que es vulguen amb el format adequat al servidor OpenLDAP per poder fer l'autenticació satisfactòriament.
2. Substituir les bases de dades d'usuaris locals dels fitxers /etc/passwd, /etc/groups, /etc/shadow per una base de dades centralitzada amb l'OpenLDAP. Per aconseguir-ho, heu de configurar l'NSS (*name service switch*) per mitjà del fitxer de configuració /etc/nsswitch.conf.
3. Configurar les aplicacions per autenticar-se amb l'OpenLDAP. S'aconsegueix mitjançant el PAM i les aplicacions PAM-aware.
4. Fase de refinament. Aquesta fase no és necessària, però és útil per millorar el funcionament de l'autenticació. Utilitzeu programes com l'NSCD, que proporciona un memòria cau (*cache*) de noms i, d'aquesta manera, permet augmentar el rendiment de les consultes al directori OpenLDAP.

Creació dels usuaris adequats en el servidor OpenLDAP

La finalitat del servidor LDAP és que serveixi de magatzem d'usuaris i grups per autenticar sistemes GNU/Linux i diversos serveis. En primer lloc, hauríeu de crear una estructura que parteixi de la base del nostre directori per emmagatzemar aquesta informació.

L'OpenLDAP proporciona, per mitjà de l'esquema NIS (/etc/ldap/schema/-nis.schema), les classes d'objectes (*objectClass*), PosixAccount i PosixGroup, que permeten crear comptes d'usuaris i grups compatibles amb els sistemes GNU/Linux. És a dir, proporcionen usuaris i grups amb la mateixa estructura i els mateixos atributs que utilitzen per defecte els sistemes GNU/Linux i que ens permetran autenticar-nos en el sistema.

Per exemple, com es pot veure en la figura 4.4, un objecte PosixAccount ha de tenir una sèrie d'atributs obligatoris, com ara uid, uidNumber, gidNumber i homeDirectory, que es corresponen amb els atributs emmagatzemats en l'arxiu /etc/passwd per als usuaris GNU/Linux.

FIGURA 4.4. Visió amb Apache Directory Studio dels atributs d'un objecte

Migració d'usuaris

Si teniu usuaris creats en els sistemes locals i voleu que siguin en el servidor d'autenticació, no us caldrà tornar a crear-los manualment en el servidor, ja que hi ha la possibilitat de migrar automàticament els usuaris locals al directori LDAP. Per fer aquesta migració, haureu d'utilitzar les eines que us proporciona el paquet *migrationtools*. Per instal·lar aquest paquet, feu servir l'ordre següent:

```
1 $sudo apt-get install migrationtools
```

Aquest paquet us instal·larà una sèrie d'*scripts* en el directori */usr/share/migrationtools* que us han de permetre migrar informació del sistema GNU/Linux a un servidor LDAP amb el format correcte. Per fer la migració al servidor LDAP dels usuaris que vulgueu del vostre sistema GNU/Linux, heu de fer una sèrie d'accions que es descriuen a continuació:

- 1 Aneu al directori */usr/share/migrationtools*:

```
1 $cd /usr/share/migrationtools
```

- 2 Executeu l'script *migrate_passwd.pl* i feu servir com a paràmetres el fitxer origen, */etc/passwd* (en què hi ha els usuaris) i el fitxer destinació (en què voleu emmagatzemar la informació a migrar). Per exemple, */home/ioc/usuaris.ldif*. Us heu d'assegurar que el fitxer de sortida té el format *.ldif*. L'ordre seria la següent:

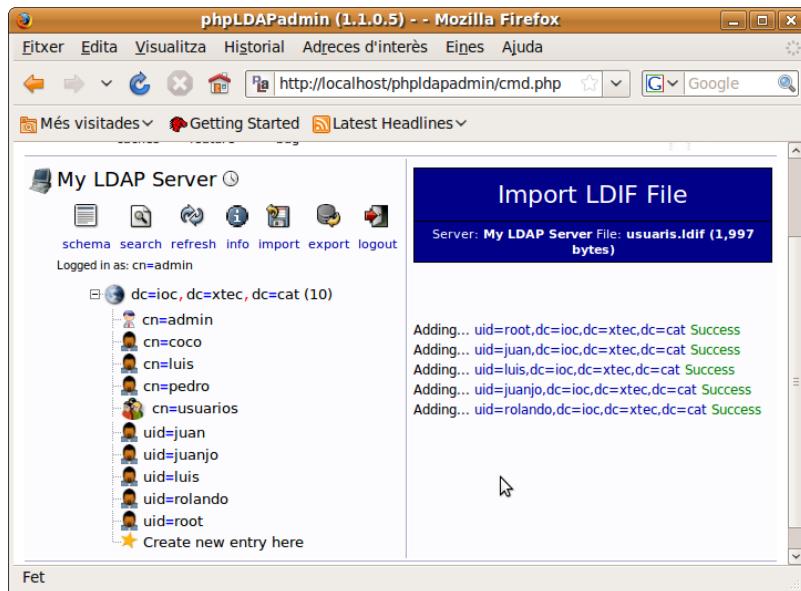
```
1 $sudo ./migrate_passwd.pl /etc/passwd /home/ioc/usuaris.ldif
```

- 3 Una vegada tingueu el fitxer destinació creat (en aquest exemple, *usuaris.ldif*), l'heu d'editar. Assegureu-vos que els camps dn de l'inici de cada objecte són correctes i elimineu els comptes d'usuaris que no vulgueu migrar (per exemple, els usuaris del sistema).

- 4 Després de modificar i desar el fitxer, haureu d'importar-ne les dades al servidor LDAP. Ho podeu fer, per exemple, mitjançant l'opció *import* del gestor de directori

phpLDAPadmin, com es veu en la figura 4.5. D'aquesta manera, afegiu els usuaris del vostre sistema al directori del servidor LDAP.

FIGURA 4.5. Importació de dades amb phpLDAPadmin



Una vegada crea o migrats els usuaris corresponents al servidor OpenLDAP, només caldrà configurar les estacions de treball per tal d'utilitzar aquests usuaris.

Configuració de l'NSS (name service switch)

El pas següent en el procés de configuració de l'autenticació del sistema és la configuració de l'NSS. Vegem en què consisteix exactament.

L'NSS proporciona una interfície per configurar diferents bases de dades en què s'emmagatzemen els comptes d'usuaris i claus, com /etc/passwd, /etc/group, /etc/shadow, /etc/host o LDAP, i accedir-hi. Per tant, us permet reemplaçar els fitxers bàsics de configuració d'usuaris GNU/Linux per altres bases de dades que ja hi ha. La idea és que el sistema es pugui configurar sense haver de tocar el codi font.

La configuració de l'NSS es fa per mitjà de l'arxiu **/etc/nsswitch.conf**. Aquest arxiu està format per una sèrie de línies amb crides a bases de dades. En cada línia s'indica quina és l'ordre per resoldre una consulta per a una base de dades específica, en la qual s'emmagatzemen els noms d'usuari, grups, equips, etc.

Les bases de dades amb les quals treballa l'NSS són les següents:

- **passwd:** paraules de pas dels usuaris.
- **group:** grups d'usuaris.
- **shadow:** paraules de pas al fitxer shadow del usuaris.

Migration tools

Fixeu-vos en el contingut del directori `usr/share/migrationtools`. Es tracta de tota una sèrie d'*scripts* que us permetran migrar elements del vostre sistema a l'LDAP. Com ja heu vist, podeu migrar usuaris, però també grups, hostes, serveis, etc.

- **ethers:** números Ethernet, interfícies de xarxa.
- **hosts:** noms de màquina i números.
- **netgroup:** usuaris i màquines de xarxa.
- **networks:** noms i números de xarxes.
- **protocols:** noms i números de protocols.
- **rpc:** noms i números de crides remotes a procediments.
- **services:** serveis de xarxes.
- **aliases:** àlies de correu electrònic, utilitzats per Sendmail.

Les bases de dades que us interessen per a l'autenticació són les de passwd, group i shadow. En el fitxer **/etc/nsswitch.conf** trobareu les línies següents:

```
1 passwd:    files
2     group:    files
3     shadow:   files
```

En cada línia del fitxer /etc/nsswitch.conf, les paraules que hi ha al costat de cada base de dades indiquen diferents serveis de bases de dades en què el sistema buscarà les dades dels usuaris, els grups i les contrasenyes per autenticar l'entrada en el sistema. D'aquesta manera, podeu indicar, introduint serveis de bases de dades l'un darrere l'altre, l'ordre de les bases de dades que ha de llegir el sistema GNU/Linux per fer l'autenticació.

Els serveis suportats per defecte són els següents:

- **files:** fa referència a fitxers emmagatzemats en el directori /etc del sistema.
- **compat:** inclou només els fitxers passwd, groups i shadow emmagatzemats en el directori /etc del sistema, els quals són compatibles amb l'estil de signes + i – del NIS.
- **db:** fa referència a bases de dades en format Berkeley.
- **dns:** s'utilitza per indicar que els hostes utilitzen el DNS.
- **hesiod:** utilitza *hesiod name service*. Aquest servei emmagatzema la informació d'alguns fitxers com /etc/passwd o /etc/groups en servidors DNS.
- **nis:** utilitza el mapa NIS.
- **nisplus:** fa servir la taula NIS plus.

NIS

El NIS és un protocol de servei directori. Segueix una arquitectura client-servidor i el seu objectiu és distribuir i compartir informació en una xarxa d'ordinadors. S'utilitza per mantenir informació centralitzada d'usuaris, però també es pot fer servir per a noms de màquina (DNS), correus electrònics aliats i altres bases de dades basades en text.

L'avantatge principal és que és fàcil i ràpid de configurar. D'altra banda, el problema principal del NIS és que no és un protocol "gaire" segur i és millor utilitzar altres sistemes més segurs com el Kerberos o l'LDAP. Val a dir, també, que és una solució de gestió d'usuaris de domini que cada cop s'utilitza menys (a favor d'altres tecnologies com l'Active Directory o l'LDAP) i que és una solució poc flexible i poc escalable.

Com s'ha comentat, aquests són els serveis que l'NSS proporciona per defecte. Tanmateix, s'hi poden afegir altres tipus de serveis. En aquest cas, us interessa que es pugui llegir informació del servei LDAP. Per això heu d'instal·lar el paquet libnss-ldap. Per fer-ho, executeu l'ordre següent:

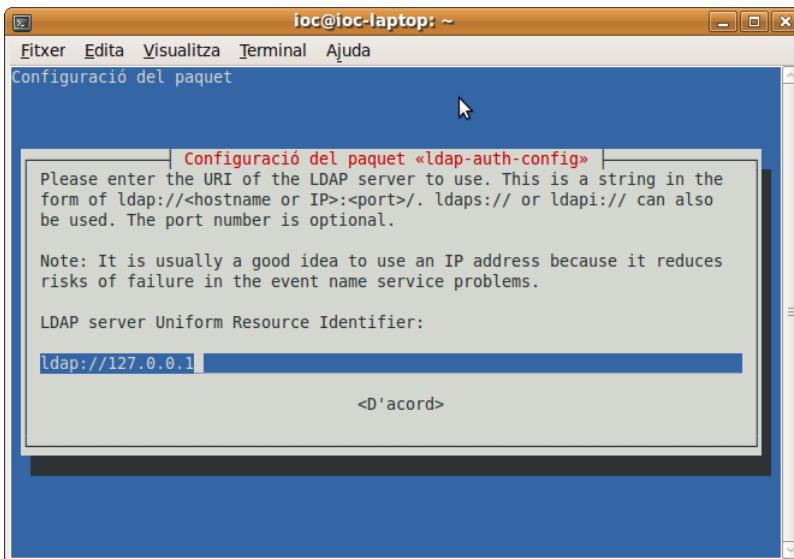
```
1 $sudo apt-get install libnss-ldap
```

Si feu la instal·lació d'aquest paquet en l'Ubuntu, us instal·larà alhora els paquets libnss-ldap i libpam-ldap, a més dels paquets de configuració auth-client-config, ldap-auth-client i ldap-auth-config. El paquet libpam-ldap s'utilitza per a la configuració del PAM amb l'LDAP i ens servirà per a la configuració del pas següent.

Quan executeu l'ordre d'instal·lació, us aniran apareixent una sèrie de menús (deb-conf) en què cal configurar les dades corresponents al vostre servidor OpenLDAP. Aquesta configuració, en l'Ubuntu, serveix tant per al paquet libnss-ldap com per al paquet libpam-ldap.

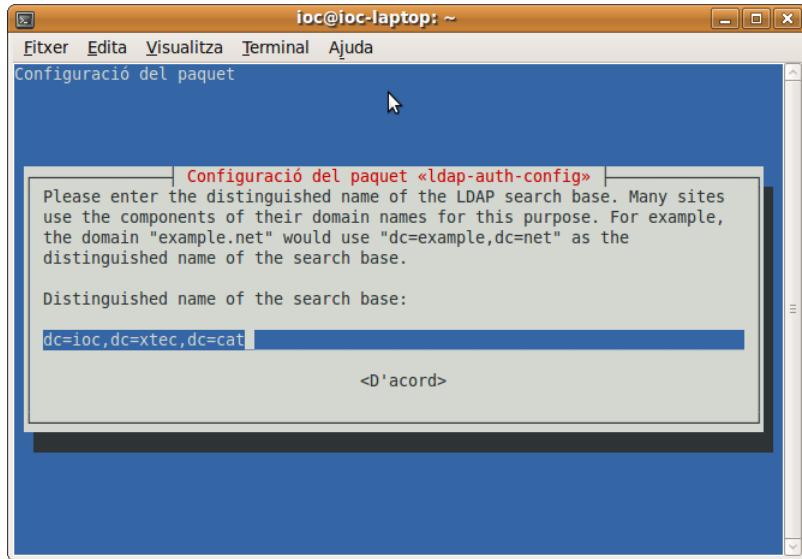
El primer menú que us apareix, com el de la figura 4.6, demana el nom o l'adreça IP del servidor OpenLDAP sobre el qual voleu autenticar-vos.

FIGURA 4.6. Menú inicial de configuració del paquet ldap-auth-config



A continuació, com es veu en la figura 4.7, haureu d'especificar el DN (nom distingit) de la base (arrel) del servidor OpenLDAP a partir de la qual cercareu les dades per a la validació.

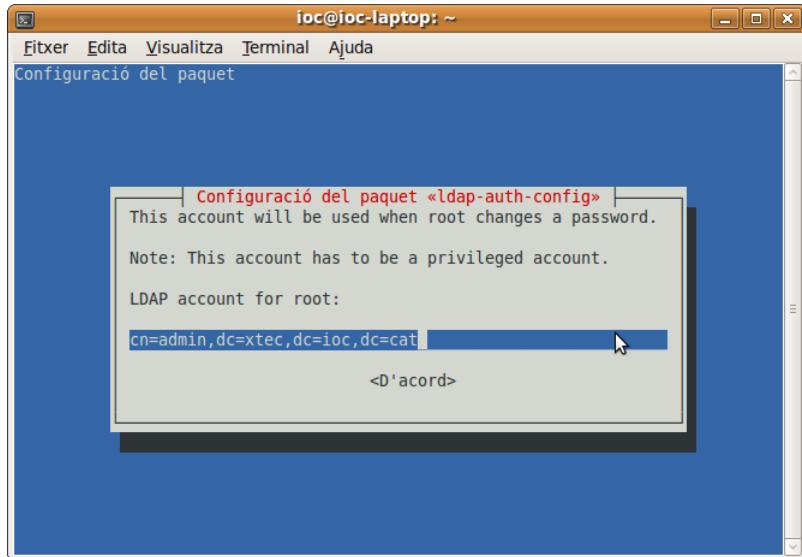
FIGURA 4.7. Especificació de la base del directori en la configuració del paquet ldap-auth-config



Continueu i us preguntarà quina versió de l'LDAP voleu utilitzar. Seleccioneu la versió 3.

Com ja sabem, el procés de configuració mitjançant els diferents menús també configura el PAM. Així, en el menú següent us preguntarà si voleu que les aplicacions que canvien les claus per mitjà del PAM es comportin com si ho fessin de manera local. Contesteu que sí i a continuació us preguntarà si voleu autenticar-vos per accedir al directori de l'OpenLDAP. Contesteu que no. En l'opció següent del menú, com veiem en la figura 4.8, haureu d'introduir el compte d'administrador del servidor OpenLDAP. Per fer-ho, heu de repetir tot el DN de la base i afegir-hi el cn (*common name*) del superusuari o l'administrador. Aquest compte es farà servir quan es canviï la contrasenya d'administrador.

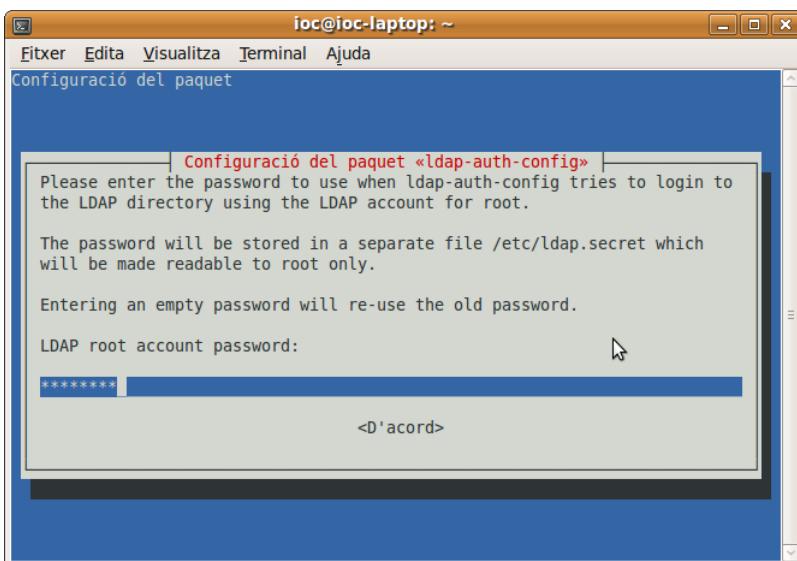
FIGURA 4.8. Especificació de la base del directori per a l'usuari root



La finestra següent, mostrada en la figura 4.9, sol·licita que introduïu la contrasenya amb la qual l'administrador accedeix al servidor OpenLDAP. Heu d'anar

en compte, perquè la contrasenya que hi introduïu s'emmagatzemarà en text pla, sense xifrar, en el fitxer /etc/ldap.secret. Encara que aquest fitxer només el pugui llegir l'usuari root, l'heu de tenir en compte per garantir la seguretat del servidor OpenLDAP. En cas de reconfigurar el paquet, si no hi introduïm cap contrasenya s'utilitzarà la contrasenya antiga.

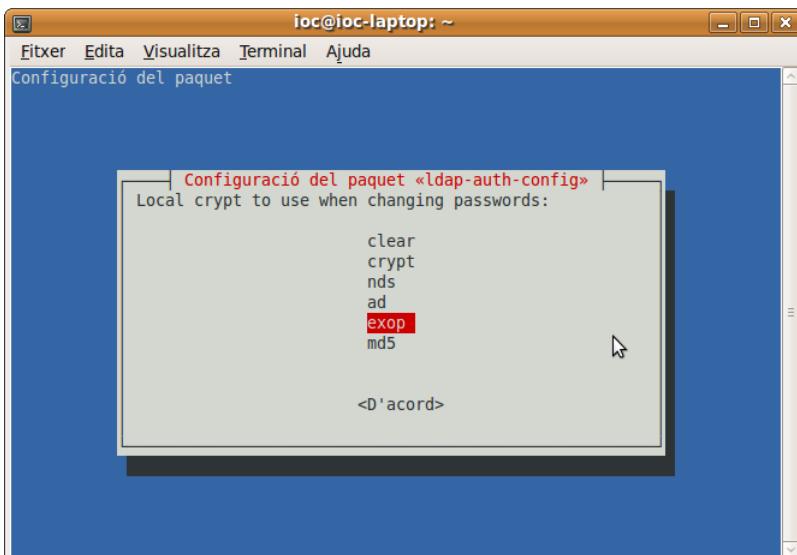
FIGURA 4.9. Introducció de la contrasenya de l'administrador



A vegades, mitjançant els menús que van apareixent en l'Ubuntu, els paquets no s'instal·len bé o no apareixen totes les opcions de configuració. Per solucionar-ho, podeu editar i modificar directament el fitxer de configuració /etc/ldap.conf, en què hi ha les dades de configuració per als paquets libnss-ldap i libpam-ldap. També podeu, de manera més senzilla, tornar a configurar els paquets executant l'ordre següent:

¹ \$dpkg-reconfigure ldap-auth-config

FIGURA 4.10. Menú d'elecció del tipus d'encriptació



Si executeu aquesta ordre us tornaran a aparèixer els menús anteriors, en què haureu d'especificar les dades noves de configuració. A més, però, us apareixeran dos menús nous. El primer explica els distints formats d'encriptació amb els quals podeu emmagatzemar les contrasenyes en els mòduls del PAM. El segon, mostrat en la figura 4.10, permet escollir entre algun dels formats que s'han explicat en el menú anterior.

El mètode d'encriptació que triareu per emmagatzemar les claus serà *exop*. D'aquesta manera, el libpam-ldap utilitzarà l'algorisme de hash especificat en l'arxiu de configuració del servidor OpenLDAP, en lloc de fer l'operació hash localment i escriure el resultat en la base de dades directament.

Una vegada instal·lats i configurats els paquets libnss-ldap i libpam-ldap, us caldrà modificar el fitxer /etc/nsswitch.conf per tal de finalitzar el primer pas. El fitxer quedarà de la manera següent:

```
1  passwd:  files  ldap
2      group:   files  ldap
3      shadow:  files  ldap
```

D'aquesta manera, li estem indicant l'ordre que el sistema GNU/Linux ha de fer servir per fer l'autenticació. Aquest ordre determina que primer ha de consultar els fitxers locals i, si no hi troba la informació que busca, ha de consultar el directori LDAP. Aquesta és la manera més recomanable de fer l'autenticació.

Recomanacions

D'altra banda, és recomanable tenir l'usuari root en els fitxers locals exclusivament i la resta d'usuaris emmagatzemats en el directori. D'aquesta manera, el superusuari sempre hi tindrà accés i la resta d'usuaris s'autentifiquen per mitjà del servidor LDAP. No és recomanable tenir l'usuari root en el servidor LDAP o invertir l'ordre de l'autenticació, ja que, en cas de fallada del servidor LDAP, podeu quedar-vos sense accés a la màquina.

És convenient provar l'autenticació. Per fer-ho, caldrà tenir diverses consoles de root obertes perquè en cas de fallada no hi hagi problemes per entrar a la màquina i poder modificar aquests fitxers. Tingueu en compte que, en estar modificant el procés d'autenticació, qualsevol fallada en la configuració us pot deixar sense accés a la màquina, de manera que haurieu d'arrancar mitjançant altres mecanismes. El sistema ja estaria preparat per autenticar-se amb un servidor LDAP. A continuació, veureu la configuració que s'ha de fer per establir la manera com s'autentiquen els serveis i les aplicacions del sistema que ho requereixen.

Configuració del PAM

Per tal de configurar la manera com s'autentificarà cada servei i aplicació que necessita autenticació en el sistema LDAP, heu d'editar i modificar alguns dels arxius del directori **/etc/pam.d**.

Per evitar configurar els arxius de cada servei o aplicació, hi ha una sèrie d'arxius comuns, que afecten la majoria de serveis i aplicacions, el nom dels quals comença per *common*. Els arxius comuns són els següents:

- **/etc/pam.d/common-auth**, utilitzat per a les aplicacions o els serveis per autenticar-se.
- **/etc/pam.d/common-account**, utilitzat per poder disposar d'un compte.
- **/etc/pam.d/common-session**, utilitzat per iniciar una sessió.
- **/etc/pam.d/common-password**, utilitzat per poder canviar la contrasenya.

Tots aquests arxius contenen una línia que fa referència a la llibreria **pam_unix.so**, utilitzada per a l'autenticació contra els arxius GNU/Linux. En el vostre cas, per aconseguir que els serveis i les aplicacions del vostre sistema es puguin autenticar per mitjà d'un servidor LDAP, heu d'interessa que primer s'utilitzi la llibreria **pam_ldap.so**, que es fa servir per a l'autenticació contra un servidor LDAP. Per fer-ho, heu d'afegir la línia corresponent a la llibreria pam_ldap.so per sobre de la línia corresponent a la llibreria pam_unix.so en els arxius common. Així, les aplicacions s'autenticaran primer contra el servidor LDAP i, si l'autenticació falla, provaran d'autenticar-se després amb els arxius GNU/Linux.

1. Configuració de l'arxiu common-auth

Per tal que els serveis i les aplicacions del sistema utilitzin les llibreries pam-ldap per autenticar l'usuari, heu d'afegir a l'arxiu **/etc/pam.d/common-auth** la línia següent:

auth sufficient pam_ldap.so Aquesta línia la ubicarem al damunt de la línia en què aparegui la llibreria pam_unix.so. A continuació d'aquesta última línia, afegirem la sentència **use_first_pass** per evitar que us demani dues vegades la contrasenya quan intenteu validar-vos amb un usuari donat d'alta en el servidor LDAP. Per tant, l'arxiu quedà de la manera següent:

auth sufficient pam_ldap.so auth required pam_unix.so use_first_pass **2. Configuració de l'arxiu common-account**

Per permetre que els serveis i les aplicacions del sistema comprovin el compte d'usuari mitjançant les llibreries pam-ldap, heu d'afegir a l'arxiu **/etc/pam.d/common-account** la línia següent, al damunt de la línia de la llibreria pam_unix.so:

1 account sufficient pam_ldap.so

LDAP. Per tant, l'arxiu quedà així:

1 account sufficient pam_ldap.so
2 account required pam_unix.so

3. Configuració de l'arxiu common-session

Per tal que els serveis i les aplicacions del sistema obtinguin els paràmetres de la sessió d'usuari de les llibreries pam-ldap, cal que afegiu a l'arxiu **/etc/pam.d/common-session**, al darrere de la línia en què hi hagi la llibreria pam_unix.so, la línia següent:

1 session optional pam_ldap.so

4. Configuració de l'arxiu common-password

Per tal que els serveis i les aplicacions del sistema pugin modificar la contrasenya d'usuari mitjançant les llibreries pam-ldap, cal que afegiu a l'arxiu **/etc/pam.d/common-password** la línia següent, al damunt de la línia en què apareix la llibreria pam_unix.so:

```
1 password sufficient pam_ldap.so
```

Configuració gràfica PAM

La configuració del PAM per autenticar les aplicacions amb la llibreria LDAP es pot fer sense tocar cap fitxer de configuració amb eines gràfiques com Webmin.

5. Configuració particular per a cada servei

Si voleu que alguns serveis o aplicacions s'autentiquin de manera diferent, podeu editar l'arxiu corresponent, com ara **/etc/pam.d/su**, **/etc/pam.d/ssh** o **/etc/pam.d/ftp**, eliminar la línia que comença per **@include** i introduir-hi la configuració particular que vulgueu.

6. Provar l'autenticació

El vostre servidor LDAP ja hauria d'autenticar correctament. Podeu provar l'autenticació dels serveis mitjançant l'ordre pamtest, que és en el paquet libpam-dotfile. Abans, però, l'haureu d'instal·lar amb l'ordre següent: sudo apt-get install libpam-dotfile

Per exemple, si voleu provar si el servei passwd funciona, és a dir, canviar la contrasenya sobre un usuari del directori LDAP, podeu executar l'ordre següent:

```
1 $sudo pamtest passwd lluis
2   Trying to authenticate for service.
3   Password: (Introduim la contrasenya d'en Lluís.)
4   Authentication successful. (L'autenticació ha estat satisfactòria.)
```

Des d'una consola, per exemple, podeu provar de canviar, mitjançant l'ordre su (su=switch user - canviar d'usuari), un usuari que sigui en el directori LDAP. Si tot funciona bé, automàticament demanarà la contrasenya per validar l'usuari. Exemple en l'Ubuntu.

```
1 $ioc@ioc: su pepe
2   Password: (Ens demana la contrasenya d'en Pepe. La hi introduïm.)
3   pepe@ioc; (Canvia correctament l'usuari Pepe.)
```

Les opcions de configuració del PAM són molt variades. Per obtenir-ne més informació, podem instal·lar el paquet **libpam-doc**, que instal·la força documentació sobre aquest tema en el directori **/usr/share/doc/libpam-doc**.

L'autenticació d'usuaris i aplicacions ja estaria enllestida en el vostre sistema GNU/Linux. A continuació, veureu com refinjar el mecanisme d'autenticació per tal de fer-lo més ràpid. També veureu algunes eines molt útils per migrar la informació dels usuaris locals del sistema al directori que hi ha en el servidor LDAP.

NSCD (name service cache daemon)

Com a últim pas, per agilitzar l'accés al directori i augmentar-ne el rendiment, encara que no és necessari, cal instal·lar el dimoni ncsd.

El dimoni nscd proporciona un memòria cau (*cache*) de noms per fer més ràpides les peticions als serveis de noms més comuns. Normalment s'utilitza amb el servei LDAP per augmentar el rendiment de les consultes al directori.

Per instal·lar el dimoni, heu d'utilitzar el paquet `nscd` i executar l'ordre següent:

```
1 $sudo apt-get install nscd
```

Per controlar el dimoni, podeu utilitzar els *scripts* que hi ha en el directori **/etc/init.d**, que permeten aturar-lo, iniciar-lo, reiniciar-lo, etc.

El fitxer de configuració del servei és el fitxer **/etc/nscd.conf**. Si l'editeu, podeu comprovar que fa de memòria cau (*cache*) de les bases de dades **passwd**, **groups** i **hosts**.

Per tal que funcioni millor, és recomanable treure les línies **persistent host yes** i **shared host yes** del fitxer de configuració. Amb la primera línia eviteu que el servei emmagatzemi constantment la informació dels hostes, encara que reinicieu el dimoni. D'aquesta manera, us assegureu que la memòria cau (*cache*) no us retorna dades errònies d'una consulta i us mostri hostes que ja no són en el directori. Amb la segona línia desactiveu l'intercanvi de les dades dels hostes entre els clients `nscd`.

Heu de considerar les conseqüències que comporta una memòria cau (*cache*). És a dir, heu de tenir en compte que si feu canvis en el servidor LDAP, els canvis no repercutiran instantàniament en el client, sinó que haureu de reiniciar el servei perquè això ocorri.

Finalment, cal remarcar que tot el procés d'autenticació amb un servei LDAP, que hem vist anteriorment, només us proporciona l'autenticació d'usuaris GNU/Linux en xarxa. Si voleu que els clients muntin les seves *home* a partir dels directoris *home* centralitzats en el servidor LDAP, heu d'utilitzar serveis com l'NFS o el Samba.

Per entendre el significat de cada paràmetre del fitxer `/etc/nscd.conf`, podeu fer servir el manual del sistema amb `man nscd.conf`.

Muntar *home* en el client LDAP

Per muntar els directoris *home* en el client, podeu fer servir el mètode tradicional, configurar el fitxer `/etc/fstab`, o utilitzar l'ordre **automount**, que treu la informació de l'element que s'ha de muntar de l'arbre LDAP.