Administració de servidors

Jordi Serra Ruiz

PID_00200498

UOC
Universitat Oberta de Catalunya

Índex

Introducció

El primer que cal fer per a parlar de seguretat en un sistema informàtic és decidir quin sistema operatiu instal·lem a la màquina, ja sigui en una de nova o en una en la qual s'hagi decidit canviar les funcions, pensant si serà un servidor, de fitxers, de llocs web, d'impressió, etc.

En aquest mòdul descrivim tot el que fa falta per a preparar un sistema informàtic i instal·lar-hi un servidor: com s'ha de fer la partició del disc adequadament per a cadascun dels sistemes operatius, on s'ha d'instal·lar el programari del servidor, etc.

No farem aquí una discussió de quin sistema operatiu s'ha d'instal·lar en un servidor, ja que això depèn molt de la política de cadascuna de les empreses i en definitiva de l'experiència de cada administrador de sistemes, que és qui l'instal·la i després l'ha de mantenir.

Es descriu, doncs, què cal tenir en compte per a instal·lar un servidor basat en GNU/Linux i, després, en el Windows Server 2012.

Quan tinguem clares les consideracions preliminars, descriurem la instal·lació i configuració dels servidors i acabarem descrivint l'administració i el manteniment d'aquests servidors. La seguretat en els sistemes, tant si són servidors, dispositius de xarxa, mòbils com qualsevol altre sistema, no s'acaba en la instal·lació, ja que com es pot veure cada dia, els atacs són continus i amb unes tècniques noves cada dia. Per tant, l'actualització i el manteniment dels sistemes és el més important que hi ha en aquest sentit.

Objectius

Aquest mòdul té els objectius següents:

1. Analitzar els requisits necessaris per a dimensionar un servidor que s'ha d'implantar en una empresa, tant si és una pime com una gran corporació.

2. Planificar la instal·lació d'una màquina ponderant els sistemes d'arxius, fent la partició dels discos i dimensionant les particions que formaran el servidor.

3. Instal·lar un servidor mitjançant el sistema operatiu, activar els protocols de xarxa necessaris i els mecanismes d'autenticació que utilitzarem en el servidor.

4. Conèixer les eines bàsiques que ens poden fer servei a l'hora d'administrar un servidor.

1. Anàlisi de requisits

1.1. GNU/Linux

El primer que hem de considerar en la instal·lació d'un servidor és saber quin tipus de servidor volem instal·lar. Per fer-ho, hem de pensar prèviament en una sèrie de punts molt importants:

- Quants usuaris hi haurà en el sistema, en valor absolut. No cal saber-ho de manera exacta, però sí en una magnitud bastant aproximada, ja que després ens serà molt difícil redimensionar tot el sistema si, per exemple, s'ha dimensionat per a vint empleats i després n'hi ha dos-cents.

- Quins serveis s'han d'oferir dins el sistema informàtic

- Quants usuaris estaran connectats de manera simultània; això ens marcarà molt el tipus de xarxa i les connexions.

- Com seran les connexions dels usuaris: la durada, el tipus (interactiva, remota, passiva, *batch*, etc.), entre d'altres.

Una vegada hem resolt aquests requisits els hem d'analitzar per a dimensionar el servidor de manera correcta; per a fer-ho, cal preveure, també, l'escalabilitat del servidor, tenir prevista una possible ampliació del negoci i, per tant, de les necessitats que demanaran als servidors.

Cal tenir present que per a dimensionar els sistemes bé s'han de tenir en compte tots els factors, i també les combinacions possibles d'aquests factors. És a dir, si oferim correu electrònic, hem de considerar que avui dia els correus gratuïts ja ofereixen una capacitat superior a unes desenes de gigabytes d'espai per usuari, i si, a més, oferim un espai perquè els usuaris pengin el seu lloc web, parlem de 250 MB més. Si a aquests dos serveis hi afegim el de disc de xarxa, en el qual els usuaris guarden els documents, i suposant que els oferim 500 MB d'espai, ens trobem que un usuari pot arribar a ocupar 5 GB fàcilment. I per a dimensionar de manera correcta sempre va bé preveure el "pitjor" cas.

Una vegada tenim una idea de la quantitat de disc per usuari, l'hem de multiplicar pel nombre d'usuaris que tindrem. Abans de multiplicar-la per la quantitat d'usuaris, però, n'hem de preveure el creixement. És a dir, quan el servidor faci poc que està instal·lat tindrem cent cinquanta usuaris, però en cinc o sis anys (que és més o menys l'esperança de vida d'un servidor), tindrem un creixement de deu usuaris per any. Això fa dos-cents deu usuaris en total.

Si multipliquem els usuaris per la quantitat d'espai que necessitaran (210 × 5 GB) ens surt poc més de 1.050 GB de disc. A aquesta quantitat hi hem d'afegir un 15% o 20% perquè el disc estigui "sanejat". Així, veiem que, només per als usuaris, necessitem més d'1 terabyte d'espai de disc. Hem de tenir present que a aquesta quantitat hi cal afegir l'espai que ocupa el sistema per a fixar de manera concreta la quantitat de disc dur.

Un altre aspecte que hem de considerar és que necessitarem un terabyte i mig (imaginem-nos que només necessitem 250 GB per al sistema i totes les aplicacions) útils. És a dir, si finalment adoptem un sistema de redundància de disc (del tipus RAID), a la quantitat útil que obtenim hi hem d'afegir la part de redundància.

Aquesta part depèn del sistema redundant que tinguem. Si és RAID 1 (rèplica o *mirror*), hem de multiplicar aquesta quantitat per 2. Si és RAID 5 (com a mínim tres discos de la mateixa mida), hi hem d'afegir un terç de l'espai útil. Per tant, fins i tot abans de comprar els equips, els discos i la circuiteria de xarxa, s'ha de pensar molt bé tot el que hi posarem i quant ens durarà, ja que si hi posem la quantitat d'espai justa per als requisits d'avui, demà segur que tindrem un problema.

Hi ha raonaments semblants que ens portaran a valorar la memòria RAM, la xarxa o la velocitat de procés. Cal destacar que a vegades arribarem a raonaments una mica "inversemblants", com per exemple que el nostre servidor només necessitarà una velocitat de procés de 400 MHz. Això vol dir que hem de posar com a servidor un Pentium II? No. Aquesta conclusió, ens invalida el nostre raonament? No. Per a això dimensionem, per a obtenir resultats que no ens serveixen? No. Aquesta conclusió només mostra que la velocitat de procés no és un factor crític per al nostre servidor.

Per a avaluar quants usuaris estaran connectats de manera simultània, una altra vegada hem de saber l'entorn en què hi serà el servidor o conjunt de servidors. No és el mateix que els ordinadors tinguin tot el programari en local i els usuaris es connectin a una intranet per compartir fitxers, que els ordinadors tinguin el programari instal·lat de manera administrativa i amb les dades en el servidor. En el primer cas, els nostres usuaris es connectaran de manera puntual amb el servidor, mentre que en el segon els usuaris estaran gairebé sempre connectats.

En el cas concret de l'Ubuntu, que és el sistema GNU/Linux que més endavant explicarem com s'ha d'instal·lar, els requisits del sistema recomanats són els següents:

- CPU compatible amb Intel (i486 o superior).

- 256 MB de RAM utilitzant el mode gràfic, que permet l'ús d'aplicacions ofimàtiques.
- Disc dur de 3 GB com a mínim.
- Unitat de CD-ROM, o unitat de disc i CD-ROM (IDE/ATAPI o SCSI) normal.
- Targeta compatible amb SVGA.
- Ratolins en sèrie o PS/2 o compatible amb IMPS/2 o USB.

1.1.1. Configuracions de maquinari recomanades

Els sistemes operatius són, *a priori*, independents del maquinari en el qual s'executen, tot i que sempre hi ha excepcions. Perquè el sistema operatiu (SO), però, s'entengui amb el maquinari, calen els programes controladors o *drivers* específics de cada maquinari. Els controladors són programes que depenen del sistema operatiu que interactuen directament amb el maquinari, ja que són responsables de la comunicació entre el SO i el maquinari.

Ens podem trobar amb cert maquinari que no pot funcionar amb GNU/Linux, ja que no hi ha cap controlador compatible per a aquest sistema operatiu. Una manera simple de saber si el maquinari que volem comprar és compatible és buscant el logotip de Tux (el pingüí) a la capsa[1], tot i que algunes vegades ho pot ser sense que el fabricant ho indiqui.

(1)Si no tenim la capsa del programari, ho podem consultar a la xarxa Internet mitjançant l'URL: http://www.tldp.org/howto/hardware-howto/index.html.

1.1.2. Consideracions del programari

Un dels possibles serveis d'un servidor és el de proporcionar programari als usuaris connectats. Aquest programari segurament també té uns requisits mínims que cal considerar; si a aquests requisits hi afegim el fet de donar servei als usuaris, ens trobem que també hem de dimensionar el servidor segons el programari que volem proporcionar.

Podem tenir un servidor de fitxers que necessita poca RAM, poca CPU o GPU però necessita una molt bona targeta de xarxa per a servir els fitxers, però també podem necessitar un servidor en què s'executi un programa de càlcul o disseny gràfic, i per tant, la xarxa no serà crítica, però la RAM i la CPU i GPU sí. Les aplicacions que s'executen en els servidors a vegades també poden condicionar el tipus de servidor que s'ha d'instal·lar.

1.2. Windows Server 2012

1.2.1. Diferents versions de Windows Server 2012

- **Foundation:** aquesta versió està pensada per a petites empreses, ja que no té possibilitats de fer virtualització amb l'Hyper-V i només disposa de quinze usuaris com a molt dins el directori actiu. Clarament està pensada per a una empresa molt petita de pocs usuaris.

- **Essentials:** com l'anterior, no disposa de virtualització de màquines, no es poden tenir màquines virtuals amb l'Hyper-V, però es poden tenir fins a vint-i-cinc usuaris en el directori actiu de l'empresa. Està pensada per a petites empreses però que necessitin alguna cosa més que no pas la Foundation, ja que hi ha alguns temes dins els papers dels servidors que varien una mica, com per exemple els escriptoris remots o la preconfiguració de l'accés al núvol Internet.

- **Standard:** en aquest cas tenim usuaris il·limitats però únicament es poden tenir dues màquines virtuals per cada llicència del Windows Server 2012; en podríem tenir, per tant, més d'una llicència per a poder disposar de més màquines virtuals dins el servidor. Cada usuari que vulguem que es connecti a aquest servidor haurà de tenir una llicència CAL de connexió al servidor.

- **Datacenter:** aquesta versió disposa de tot inclòs, usuaris il·limitats i màquines virtuals com es vulgui i tantes com es vulguin. Evidentment, és una versió per a grans companyies que necessiten molts usuaris i màquines virtuals i que permet crear un núvol virtual privat dins l'empresa , i també s'ha de dir que és la més cara amb diferència. Com el cas anterior, també caldrà disposar de les llicències CAL per a cada client que es vulgui connectar al servidor.

Nom versió	Llicències/usuaris	Preu aproximat
Foundation	1 servidor/15 usuaris	OEM (preinstal·lat)
Essentials	1 servidor/25 usuaris	400 €
Standard	Per processador/il·limitat + CAL	800 €
Datacenter	Per processador/il·limitat + CAL	4.000 €

Aquestes llicencies CAL que es necessiten són les corresponents als clients del Windows que cal instal·lar en el servidor, a més del client, per tal que es puguin connectar i treballar amb el servidor.

Una de les coses interessants que gestionen totes quatre versions són les actualitzacions dels sistemes client, ja que incorporen WSUS, que és el sistema d'actualització automàtica del Windows. Per tant, des del servidor es podrà controlar completament què i quan s'instal·len les actualitzacions en els servidors i ordinadors client que hi ha a l'empresa, dins la xarxa local.

Abans de decidir-se per una llicència, s'han de consultar en aquest cas les pàgines web del fabricant on s'especifiquen totes les possibilitats de cada una de les versions, ja que potser necessitem una versió que permeti accedir a fitxers compartits o a l'escriptori remot en una petita empresa, però la versió Foundation no ho permet i per tant s'haurà d'optar per una versió més àmplia com podria ser l'Standard.

En aquest material ens centrarem en la versió estàndard, ja que és la més comuna i la de propòsit més general. Així, doncs, quan parlem del Windows Server 2012 ens referirem a la versió Standard Edition.

1.2.2. Requisits mínims de maquinari per al Windows Server 2012

Els requisits de maquinari necessaris per a un rendiment adequat del sistema operatiu Windows Server 2012 són els següents:

1) Un processador a 1,4 GHz de 64 bits. Només hi ha versió per a 64 bits.

2) 512 MB de memòria RAM.

3) L'espai de disc dur lliure necessari per a la instal·lació és de 32 GB, tot i que aquesta mida pot variar segons el nombre de components que es volen instal·lar i altres factors, com per exemple:

- El mètode utilitzat per a la instal·lació (la instal·lació mitjançant una xarxa necessita més espai que si s'instal·la des del disc compacte).

- La mida de l'arxiu de paginació. En equips amb més de 16 GB de memòria RAM es necessita més espai de disc dur per a emmagatzemar aquest fitxer de paginació, la hibernació i possibles bolcatges de memòria.

4) L'espai de disc dur ocupat al final de la instal·lació és més petit que la mida necessària per a la instal·lació i depèn del nombre de components instal·lats.

5) Un monitor VGA o de més resolució.

6) Un teclat.

7) Un ratolí.

8) Una unitat de DVD, si s'ha de fer la instal·lació des del DVD.

9) Un adaptador o uns quants adaptadors de xarxa compatibles amb el Windows i els cables corresponents, i també un servidor des del qual es pugui oferir accés a la xarxa, si s'ha de fer la instal·lació des de la xarxa.

1.2.3. Llistes de compatibilitat de maquinari amb el Windows Server 2012

La llista de compatibilitat de maquinari del Windows Server 2012 indica quins components de maquinari són compatibles (és a dir, que funcionen correctament) amb el Windows Server 2012. Si hi ha un maquinari que no surt en aquesta llista, no està garantit el bon funcionament en el Windows Server 2012.

Pàgina web

La llista de compatibilitat de maquinari es pot consultar al web de Microsoft.

1.2.4. Consideracions de programari en el Windows Server 2012

Igual que per al cas anterior, hi ha una llista de compatibilitat de programari amb el Windows Server 2012, anàloga a la llista de compatibilitat de maquinari. Abans de comprar i instal·lar un programari determinat, és convenient comprovar que és compatible amb el Windows Server 2012. Si el programari no es troba en la llista de compatibilitat, no està garantit que funcioni correctament.

El sistema ja avisa dels problemes que hi pot haver en el moment d'instal·lar els nous programaris, però hi ha algunes eines del Microsoft per a diagnosticar i resoldre alguns problemes de compatibilitat. En concret, el Windows Application Compatibility Toolkit[2] proporciona eines com l'Application Verifier, que comprova si una aplicació determinada compleix o no els requisits per a ser compatible, o l'Application Compatibility Analyzer, que fa una comprovació de compatibilitat per a tots els programes instal·lats en un ordinador o més d'un.

[(2)]Aquest paquet d'eines es pot baixar gratuïtament en aquest URL: http://www.microsoft.com/en-us/download/details.aspx?id=7352.

2. Instal·lació del servidor GNU/Linux

2.1. Planificació de la instal·lació del sistema operatiu

Abans de començar a instal·lar un servidor, de qualsevol fabricant, s'han de prendre unes quantes decisions que ens marcaran el tipus de servidor que acabarem instal·lant a la màquina. La majoria d'aquestes decisions afecten els discos, ja que hem de decidir on s'ha d'instal·lar el sistema, quin espai necessitem i quin tipus de sistema de fitxers utilitzarem. Aquestes decisions les hem de prendre amb l'ajuda de l'anàlisi de requisits que hem fet del sistema.

En un sistema basat en GNU/Linux, una de les primeres decisions que hem de prendre, i de les més importants, ja que ens podem trobar que el sistema no funciona correctament, és on posarem l'espai d'intercanvi o *swap* i com ho farem. En posar l'espai d'intercanvi en una partició separada s'aconsegueix més eficiència d'ús. Malgrat que podem forçar el Linux a fer servir com a espai d'intercanvi un fitxer regular, no és recomanable fer-ho.

Què és el *swap*

El *swap* és un espai físic dins el disc dur de l'equip informàtic d'ús temporal per a un sistema operatiu que permet utilitzar l'espai de disc dur com a memòria virtual. Quan el sistema treballa, utilitza la memòria RAM per a accedir a les dades que fa servir d'una manera més ràpida que si les busca en el disc.

Si la nostra màquina requereix més informació de la que cap a la RAM, llavors utilitza l'espai reservat com a *swap*. Per tant, el *swap* ens permet "ampliar" la memòria RAM, però a canvi de perdre velocitat (ja que l'espai d'intercanvi és en el disc). Hem de tenir present que el *swap* té un ús "esporàdic"; si la nostra màquina treballa molt en mode *swap*, ens haurem de plantejar ampliar la memòria RAM per guanyar en velocitat i en fiabilitat del disc, ja que l'accés de la memòria *swap* al disc fa que aquest quedi molt malmès.

Una vegada hem decidit que posarem l'espai d'intercanvi, *swap*, en una partició separada del sistema, hem de decidir la mida d'aquesta partició. És aconsellable que la mida final depengui de la memòria RAM que té el servidor. Si tenim un servidor amb poca memòria RAM, és recomanable posar com a espai d'intercanvi el doble de la memòria del sistema. Si tenim un servidor amb molta memòria, hem de posar com a mida de la partició de *swap* la mateixa quantitat de RAM. Cal tenir en compte que en arquitectures de 32 bits (i386) la mida màxima per a un espai d'intercanvi és de 2 GB. Una qüestió que s'ha de plantejar, tant en el cas dels servidors com en el cas dels ordinadors dels clients, és que per a poder hibernar el sistema es necessitarà més memòria *swap* de la que es disposi en realitat, ja que en cas contrari el sistema no podrà copiar la memòria real en el fitxer o partició *swap*. Això s'ha de tenir molt en compte si es disposa de portàtils, ja que en el cas d'un servidor no té gaire sentit poder-lo hibernar.

Si som en un entorn domèstic, amb aquestes dues particions, la d'intercanvi (*swap*) i la de sistema, anomenada *arrel* (/), ja podem començar la instal·lació del sistema. No obstant això, en la majoria dels entorns multiusuari és recomanable donar al GNU/Linux més que el nombre mínim de particions.

Hi ha dos motius principals per a augmentar el nombre de particions, i tots dos fan referència a la seguretat. El primer motiu és que, si es deteriora el sistema, sempre és més fàcil recuperar una partició que recuperar tot el disc. A més, si es deteriora qualsevol altra partició que no sigui la del sistema, el servidor es continua podent inicialitzar i es pot intentar solucionar el problema. El segon motiu és per una qüestió de recursos. Imaginem-nos que es perd el control d'una aplicació. Si aquesta aplicació s'executa en mode d'usuari privilegiat, anirà escrivint en el disc fins a esgotar tot l'espai. El fet de no tenir espai en el disc no és bo per a un sistema operatiu basat en GNU/Linux, ja que a part de l'espai d'intercanvi, el sistema necessita utilitzar fitxers reals per a funcionar.

El correu brossa

Si el nostre servidor rep molt correu brossa (*spam*), o es treballa amb molts fitxers que no es van esborrant, i per tant van ocupant cada cop més porció de disc, pot arribar a saturar el disc, i per tant, si el disc no té particions que separin el sistema operatiu de les dades que poden créixer sense conductor, quan se saturi pot col·lapsar el sistema.

Abans de donar pas a les particions que utilitzarem, hem de tenir present que el fet de fer particions ens "hipoteca". Si fem particions massa petites, haurem de reinstal·lar el sistema o moure dades contínuament per obtenir espai; si fem particions massa grans, tindrem molt d'espai no utilitzat en cada partició. La recomanació de particions per a sistemes multiusuari és posar els directoris `usr`, `var` i `home` en particions separades de la partició arrel. La partició arrel (/) sempre ha de contenir físicament els directoris `etc`, `bin`, `sbin`, `lib` i `dev`, o altrament no es podrà arrencar. Aquestes particions han d'estar forçosament a l'arrel del sistema de fitxers de GNU/Linux. Hi ha distribucions que recomanen la separació del directori arrel en una partició diferent de la partició arrel. Si fem aquesta partició, l'espai destinat a la partició arrel pot ser que no hagi de ser de més de 50 MB. Usualment n'hi ha prou amb una mida de la partició arrel de 2 GB.

La partició `usr` conté tots els programes, totes les biblioteques i tota la documentació d'usuari, i es troben, respectivament, en els directoris `bin`, `lib` i `share`. Aquesta part del sistema de fitxers és la que necessita la part més gran de l'espai. Si es volen instal·lar més paquets, s'ha d'incrementar la quantitat d'espai que es dóna a aquesta partició.

Tots els usuaris del sistema que tinguin espai de disc tindran un directori personal en la partició `home`. La mida d'aquesta partició depèn de quants usuaris utilitzaran el sistema i quins fitxers s'emmagatzemaran en els directoris. En la nostra anàlisi de requisits ja hem hagut de calcular aquest espai.

En la partició `var` hi ha les dades variables, com els llocs web, els correus electrònics, els fitxers de registre (*log*) i la memòria cau o *cache* d'APT. La mida d'aquesta partició depèn molt de l'ús de l'ordinador. Per tant, aquesta partició, malgrat que no és gaire important, l'hem de tenir sempre controlada perquè és la que *a priori* té més probabilitats que es desbordi i provoqui problemes.

2.1.1. Sistema d'arxius

En l'apartat anterior hem parlat de la manera com han de ser les particions que s'han de definir en el disc dur, però les ha de gestionar un sistema de fitxers. Aquesta és la manera que té el sistema operatiu de gestionar, organitzar i mantenir la jerarquia de fitxers en els dispositius d'emmagatzematge, normalment discos durs. Si fem una abstracció del sistema de fitxers ho podem arribar a interpretar com un sistema orientat a objectes, en el qual els objectes són construccions de programari (estructura de dades i funcions i mètodes associats) dels tipus següents:

- **Superbloc:** manté informació relacionada amb els sistemes de fitxers muntats. El representa un bloc de control de sistema emmagatzemat en el disc (per a sistemes basats en disc).

- ***Inode*:** manté informació relacionada amb un fitxer individual. Cada *inode* conté la metainformació del fitxer (propietari, grup, data i hora de creació, modificació i últim accés), més un conjunt de punters en els blocs del disc que emmagatzemen les dades del fitxer. Emmagatzema tota la informació sobre el fitxer excepte el fitxer pròpiament dit.

- **Fitxer:** manté la informació relacionada amb la interacció d'un fitxer obert i un procés. Aquest objecte hi és només quan un procés interactua amb el fitxer.

- ***Dentry*:** enllaça una entrada de directori (*pathname*) amb el fitxer corresponent. Els objectes *dentry* usats recentment són emmagatzemats en una memòria cau (*dentry cache*) per a accelerar la translació des d'un nom de fitxer a l'*inode* corresponent.

El sistema d'arxius per defecte del sistema GNU/Linux és l'anomenat *ext3*, o fins i tot darrerament l'*ext4*.

No és, però, l'únic sistema de fitxers que hi ha en un entorn de GNU/Linux. De fet, en Linux distingim entre tres grans grups de sistemes de fitxers: els de disc, els de xarxa i els dispositius especials. De tots els sistemes de fitxers, en aquest apartat en comentarem dos: l'*ext2*, que està quedant en desús en favor dels successors que té, l'*ext3* i l'*ext4*, precisament l'altre del qual parlarem. Aquests dos sistemes pertanyen a la categoria de sistemes de fitxers de disc.

L'*ext2* és el sistema de fitxers que es va estendre més dins del GNU/Linux. El va dissenyar Wayne Davidson amb la col·laboració de Stephen Tweedie i Theodore Ts'o. L'*ext2* està basat en *inodes* (assignació indexada). Cada *inode* manté la metainformació del fitxer i els punters en els blocs amb les dades "reals".

El sistema de fitxers *ext3* és una extensió amb *journaling* del sistema de fitxers *ext2*. Un sistema amb *journaling* és un sistema de fitxers tolerant a fallades en el qual la integritat de les dades està assegurada perquè les modificacions de la metainformació dels fitxers són gravades primer en un registre cronològic (*log* o *journal*, que implementa una llista de transaccions) abans que siguin modificats els blocs originals. Si hi ha una fallada del sistema, un sistema amb registre cronològic assegura que sigui recuperada la consistència del sistema de fitxers. El mètode més comú és el de gravar prèviament qualsevol modificació de la metainformació en una àrea especial del disc; el sistema gravarà realment les dades quan s'haurà completat l'actualització dels registres.

El cas d'*ext4* és un conjunt d'extensions compatibles cap endarrere que no es van voler incorporar a *ext3* per a evitar problemes d'inestabilitat. Principalment estén els límits del sistema de fitxers i hi afegeix millores de rendiment. Una millora molt destacada en aquest sentit és la millora del temps de comprovació del sistema de fitxers. Els blocs lliures es marquen com a tals i permeten a la utilitat `e2fsck` poder-los ignorar.

Un cas especial de sistema d'arxius és el *swap*. Si hem decidit que el nostre sistema tingui una partició d'intercanvi, hem d'assignar a aquesta partició el sistema d'arxius de tipus *Linux swap*. Si no marquem la partició amb aquest sistema d'arxius, el nostre sistema no tindrà una partició d'intercanvi.

Cal destacar que aquesta partició no és directament visible ni des del GNU/Linux, ni des del Windows, és a dir, que no rn veurem mai el contingut (els fitxers i directoris).

2.1.2. Muntatge de les particions

En aquest apartat veurem en què consisteix l'operació de muntatge i com es fa, en les diferents maneres que hi ha.

En sistemes basats en el Windows, la manera d'accedir a les particions és entrant a cadascuna de les unitats que hi ha (`A:, C:, D:, E:, F:`, etc.). En canvi, els sistemes basats en GNU/Linux tracten tots els dispositius, els discos, com si fossin fitxers. Aquest simple fet dóna molta flexibilitat al sistema, ja que ens permet fer servir tots els mecanismes destinats a fitxers en els dispositius. Per a accedir a qualsevol dispositiu d'emmagatzematge, primer hem de fer una operació de muntatge d'aquesta unitat. Aquest idea de muntar un dispositiu no queda clara si no s'entén com està estructurat l'arbre de directoris d'un sistema basat en GNU/Linux.

L'arbre de les carpetes té un directori arrel que es representa amb el símbol `/`; a dins hi ha els directoris `etc, bin, usr, var, sbin, boot, dev, lib, mnt, opt, proc` i `home` propis del sistema operatiu. Aquesta estructura apareix de la mateixa manera, independentment de les particions que fem o d'on siguin aquestes particions. Això té un gran avantatge, ja que una vegada estan

muntats els dispositius (USB, CD-ROM, particions del disc dur, etc.), tenim un únic arbre de directoris i ens podem desplaçar per aquest arbre de manera independent als dispositius, ja que ens és completament transparent en quin dispositiu som. El desavantatge de tenir aquest tipus d'estructura és que cada vegada que, per exemple, volem copiar un fitxer ubicat en una memòria USB en el disc o en un altre lloc, com pot ser per mitjà de la xarxa, hem de fer els passos següents en l'ordre indicat:

- Inserir l'USB.
- Muntar l'USB.
- Copiar els fitxers.
- Desmuntar l'USB.
- Treure l'USB.

Hi ha dues maneres de muntar un dispositiu. La primera és de manera "explícita" amb l'ordre `mount`. Aquesta ordre s'utilitza de la manera següent:

```
mount -t tipus_sistema dispositiu punt_muntatge
```

Un exemple d'execució d'aquesta ordre per a muntar una partició és el següent:

```
mount -ext4 /dev/hda2 /usr
```

Aquesta ordre munta el dispositiu `/dev/hda2` en el punt de muntatge `/usr` i utilitza ext4 com a sistema d'arxius. Per a fer-ho, prèviament hem de tenir formatat el dispositiu `/dev/hda2` com un sistema ext4.

Les particions són un cas particular de muntatge, ja que hem de saber quin és el dispositiu que volem muntar. Hi ha altres sistemes d'emmagatzematge, com el disquet o el CD, ja que el dispositiu és comú en tots els sistemes operatius basats en GNU/Linux. El disquet és el dispositiu `/dev/fd0` i el CD-ROM (si és IDE) és a `/dev/cdrom` (normalment hi surt aquest enllaç). La gran diferència, però, respecte a un sistema basat en Windows és que una vegada muntat el dispositiu no podem "treure" el CD, l'USB o el disquet fins que hàgim desmuntat aquest dispositiu. Per a desmuntar un dispositiu fem servir l'ordre `umount`.

Per exemple, si ara volem desmuntar la partició que abans hem muntat, hem d'executar:

```
umount dispositiu
umount punt de muntatge
```

En cas de voler desmuntar el dispositiu de l'exemple anterior, hem d'executar:

```
umount /dev/hda2
```

o

```
umount /usr
```

Amb qualsevol d'aquestes dues ordres aconseguim desmuntar la partició, ja que és igual si desmuntem el sistema d'emmagatzematge pel dispositiu o pel punt de muntatge. Si el que ens interessa és veure què hi ha muntat en el sistema en un moment concret, utilitzem l'ordre `mount` sense cap argument i obtenim com a sortida del sistema una taula dels dispositius muntats i els punts de muntatge. Vegem a continuació un exemple d'execució de l'ordre `mount`.

```
root# mount
/dev/hda5 on / type ext3(rw,errors=remount-ro)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/hda1 on /boot type ext3 (rw)
/dev/hda6 on /usr type ext3 (rw)
/dev/hda7 on /var type ext3 (rw)
/dev/hda9 on /home type ext3 (rw)
```

La segona opció que hi ha per a muntar dispositius en el GNU/Linux és amb el fitxer `/etc/fstab`. Aquest fitxer es llegeix en temps d'arrencada, i si tenim ben definits els dispositius, els tipus i els punts de muntatge, es muntaran tots en temps d'arrencada.

```
# <Sis. fitxers> <Punt muntatge> <Tipus> <Opcions> <abocament> <passada>
/dev/hda5 / ext3 errors=remount-ro 0 1
/dev/hda8 none swap sw 0 0
proc /proc proc defaults 0 0
/dev/fd0 /mount/floppy auto user,noauto 0 0
/dev/sda /mount/usb vfat rw,user,noauto 0 0
/dev/cdrom /cdrom iso9660 ro,user,noauto 0 0
/dev/hda1 /boot ext3 defaults 0 2
/dev/hda6 /usr ext3 defaults 0 2
/dev/hda7 /var ext3 defaults 0 2
/dev/hda9 /home ext3 defaults 0 0
```

D'aquest fitxer hi ha diverses coses que cal remarcar.

- La partició de *swap* no té punt de muntatge, una cosa normal, ja que aquesta partició només és accessible per al sistema de fitxers, per a utilitzar-la com a partició d'intercanvi amb la memòria.

- Els dispositius `/dev/fd0` (disquets), `/dev/sda` (USB) i `/dev/cdrom` (CD-ROM), malgrat que apareixen en aquest fitxer, no es munten fins que introduïm un CD, un USB o un disquet a les ranures corresponents. Hem de tenir en compte que, encara que hi introduïm un CD (o DVD), un USB o un disquet, no se'ns muntaran aquests sistemes d'emmagatzematge tret que el sistema estigui configurat per a l'automuntatge. Per això recomanem que aprengueu a muntar aquests dispositius de manera manual. Tot i que les memòries USB ja es munten en quasi tots els casos de manera automàtica, això s'ha de tenir en compte en els casos dels servidors en què sigui perillosa l'execució de programes no controlats per mitjà d'un dispositiu USB, ja que no cal ser *root* per a muntar aquests dispositius.

- El dispositiu `proc`. Aquest dispositiu té un significat especial. El que hi ha en aquest directori no són fitxers, sinó el valor de moltes de les variables que utilitza el nucli o *kernel* del sistema durant l'execució del sistema operatiu.

- Si us heu fixat en l'exemple del fitxer `/etc/fstab`, haureu vist que algunes particions tenen com a opcions `defaults`. Aquesta opció ens configura la partició com a `rw, exec, nouser, suid, async, dev` i `auto`.

Tant en el fitxer d'exemple `/etc/fstab` com mitjançant l'opció `-t` del `mount` ens obliguen a posar el tipus de sistema d'arxius que volem muntar. Si no ho fem, pren per defecte l'*ext3*. Per a muntar dispositius d'emmagatzematge del tipus `vfat`, `fat32` i `NTFS`, avui dia és poc probable que hàgim de compilar el nucli del sistema perquè reconegui aquests tipus de sistemes d'arxius, ja que són els més utilitzats en tots els sistemes.

El paquet del GNU/Linux anomenat `autofs`, que detecta automàticament la inserció d'algun dispositiu en el sistema i el munta sense haver d'executar cap ordre, ja ve per defecte en quasi totes les distribucions, però és important conèixer quin és el paquet que ens farà muntar tots aquests dispositius, per incloure'l o fins i tot per desinstal·lar-lo si cal.

2.1.3. Administració de discos

Els discos, igual que la majoria dels serveis d'un servidor, s'han d'administrar. En aquest apartat explicarem com es fa aquesta administració i en què consisteix.

Si el que volem és visualitzar l'espai usat i lliure de cada partició, ho hem de fer amb l'ordre `df` (*disc free*), que ens mostra els resultats en bytes; com que actualment els discos són molt grans, però, pot resultar enutjós veure aquestes

quantitats expressades en bytes. Si volem visualitzar més còmodament aquests resultats, podem fer servir les opcions `-k`, `-m` o `-h`, que mostren els resultats en kilobytes, megabytes o de manera "humana", respectivament.

Un exemple de visualització de l'ordre `df -h` és el següent:

```
S.fitxers Mida Usat Disp Us% Muntatge en
/dev/hda5 4,0G 277M 3,5G 8% /
Tmpfs 125M 0 125M 0% /dev/shm
/dev/hda1 198M 13M 176M 7% /boot
/dev/hda6 4,0G 1,8G 2,0G 48% /usr
/dev/hda7 4,0G 1,7G 2,2G 44% /var
/dev/hda9 25G 19G 5,0G 79% /home
```

Una de les tasques més bàsiques des del punt de vista de la seguretat és controlar que no s'esgotin els recursos de les màquines, és a dir, que l'equip deixi de donar servei perquè s'ha esgotat algun recurs, com pot ser la memòria o el disc dur. Per a això hem de fer servir l'ordre `df`, per a veure l'estat dels discos. Una partició o disc "sanejat" és aquella que té menys d'un 85% o 90% d'ús. Aquest paràmetre depèn de la mida d'aquesta partició, ja que no és el mateix un 90% de 10 GB que de 800 GB. El marge ha de ser més gran encara en la partició arrel del sistema, ja que si aquesta partició se satura el servidor no arrencarà.

A continuació enumerarem unes tasques que poden ajudar a mantenir els discos sanejats. Algunes d'aquestes tasques són "físiques" (fer alguna cosa) i d'altres són "polítiques" (de bon ús del sistema que hem d'aprendre nosaltres i fer aprendre els usuaris):

1) Els directoris `/tmp` i `/var/tmp` solen estar a la disposició de molts processos en què s'escriu molta informació temporal. S'han de netejar periòdicament aquests directoris. Hi ha moltes distribucions que ja disposen de mesures per a aquests casos, com eliminar els continguts d'aquests directoris durant l'arrencada de la màquina, però n'hi ha algunes que estan enfocades a tenir el GNU/Linux com a estació de treball i no pas com a servidor. Si utilitzem el GNU/Linux per al nostre servidor, com que ens interessa que les nostres màquines estiguin tot el temps en servei, i com que netegem aquests fitxers només en temps d'arrencada i no parem el servidor durant uns quants mesos, podem arribar igualment a la saturació. Una manera més pràctica de solucionar aquest problema és esborrar cada dia aquests directoris. Per a fer-ho, s'ha d'utilitzar el `crontab` del sistema. El `crontab` és l'aplicació que té el sistema per a executar de manera periòdica (cada hora, cada dia, cada mes, cada dimecres, etc.) alguna tasca, ordre o *shell script*. Per a accedir al `crontab` des de l'usuari arrel, cal executar l'ordre `crontab -e` i afegir-hi les línies següents:

```
05 04 * * * /bin/rm -rf /var/tmp/*
10 04 * * * /bin/rm -rf /tmp/*
```

Amb aquestes dues línies aconseguim que cada dia a les quatre i cinc i a les quatre i deu de la matinada s'esborrin els continguts d'aquests directoris.

2) Hem de controlar la mida dels registres per a evitar un desbordament. Els registres són, normalment, a `/var/log` o a `/var/adm/log`, i en aquest tipus de fitxers, segons el sistema, poden arribar a ser molt grans. Com que en els registres es guarden tots els esdeveniments del sistema, no és aconsellable eliminar-los. Una tasca que ha de fer l'administrador de manera periòdica és revisar els registres, ja que ens donen informació sobre tots els fets que hi ha hagut en el servidor. El que sí que podem fer és guardar-los periòdicament (per exemple, cada setmana) de manera comprimida, i els que siguin anteriors a un període de dos mesos, eliminar-los. També podem guardar tots els registres en dispositius extraïbles.

3) Un altre punt en què es pot desbordar el sistema és en l'espai dels usuaris.

Alguns d'aquests casos són els següents:

- Els correus electrònics. Els podem educar perquè esborrin periòdicament els missatges o bé hi podem posar un sistema de quotes de correu. Més endavant veurem com s'han de configurar les quotes de correu.

- L'espai de disc dels usuaris. Podem tornar a demanar als usuaris que esborrin periòdicament coses o hi podem posar un sistema de quotes de disc.

- La memòria cau dels navegadors també és un espai on es pot arribar a escriure molta informació. És recomanable esborrar-la periòdicament; per a fer-ho, o eduquem els nostres usuaris a fer aquesta tasca de manera periòdica, o la fem nosaltres mitjançant un *shell script* que recorri tots els usuaris buscant aquestes carpetes i que n'elimini el contingut.

- Si els nostres usuaris utilitzen eines de compilació, els fitxers *core* solen tenir mides molt grans. Els podem eliminar, de manera periòdica, mitjançant una cerca per l'espai d'usuaris.

Una altra instrucció que ens pot fer servei és l'ordre `e2fsck`, que fa una "revisió mèdica" del disc i comprova la integritat de les dades. S'executa de la manera següent:

```
e2fsck -t tipus_sistema dispositiu [opcions]
```

Una dada molt important és que, per a executar aquesta ordre sobre un dispositiu, aquest dispositiu ha d'estar desmuntat. Si no, pot danyar el sistema.

2.2. Instal·lació del servidor

En aquest apartat detallarem com s'instal·la un servidor Linux. Per a fer-ho, utilitzarem la distribució per a servidor de GNU/Linux, Debian, en la versió 6, darrera versió en el moment d'imprimir aquests materials. Hi ha diferents maneres de fer aquesta instal·lació, però la més senzilla és baixar de la pàgina web de Debian la instal·lació per xarxa (*netinst*), ja que això farà que amb un CD i amb poc temps puguem instal·lar el sistema. Amb aquesta instal·lació únicament es baixaran aquelles parts del sistema operatiu que es vol realment instal·lar, així reduïm la mida de la baixada total i per tant no esgotem l'amplada de banda del la xarxa.

El document bàsic que ens proporciona Debian per a la instal·lació es troba directament a la pàgina web de Debian. Cada distribució tindrà el seu document d'instal·lació. En el cas de la distribució que es fa servir en aquest taller es pot trobar en l'adreça `http://www.debian.org/releases/stable/installmanual`, on hi ha els enllaços a totes les arquitectures i idiomes possibles. Podem trobar solucions, per exemple, a no disposar d'una unitat de DVD-ROM arrencable (bootable).

Aquesta instal·lació es portarà a terme en un ordinador estàndard sobre un disc dur SATA petit. Pel que fa a controladors i discos SCSI, si aquests són mitjanament estàndard, seran detectats sense cap problema durant el procés d'arrencada, igual que els discos IDE.

Abans de fer la instal·lació ens hem d'assegurar que el CD-ROM del nostre servidor és la primera opció en temps d'arrencada. Una vegada tenim el CD-ROM com a primera opció, introduïm el CD del Debian i inicialitzem la màquina.

2.2.1. Abans de començar la instal·lació

És molt important que abans d'iniciar la instal·lació mirem si disposem d'un espai mínim en el nostre disc dur on fer-la (es recomana disposar, com a mínim, entre 20 i 30 GB d'espai lliure, només per al sistema). Es podria donar el cas que un altre sistema operatiu ja estigui en el disc dur i ocupi quasi tot el disc i no deixi gens d'espai per al nou sistema. Però si el disc és nou, podem començar directament amb la instal·lació, malgrat que pensem instal·lar-hi també un altre sistema operatiu (n'hi haurà prou que reservem l'espai que considerem amb el tipus de partició que necessiti).

Si disposem d'un espai que prèviament havíem reservat, perquè ja teníem en ment instal·lar-hi el GNU/Linux, o tenim una partició de qualsevol altre sistema operatiu en què el vulguem instal·lar, també podem prosseguir amb la instal·lació, és a dir, arrencar des del DVD-ROM.

Però si tenim tot el disc dur ocupat en una sola partició dedicada a un altre sistema operatiu (cosa molt poc recomanable, ja que en general això fa disminuir el rendiment de qualsevol sistema operatiu, i en especial d'aquells amb sistemes de fitxers poc consistents), hem d'alliberar espai per a poder-hi instal·lar el Debian GNU/Linux en el cas de voler disposar dels dos sistemes, tot i que mai no seran simultanis. La dificultat de fer aquesta operació dependrà estrictament de quin sistema de fitxers contingui aquesta partició.

Probablement, el sistema operatiu en qüestió és de la família de productes de Microsoft; si el sistema de fitxers és de tipus FAT o FAT32 (utilitzats per les antigues versions: MSDOS, Windows 95 i Windows 98) el problema és relativament senzill de resoldre, ja que la distribució ens facilita una aplicació anomenada `fips20.exe` que ens assistirà en la repartició del disc dur i en la creació d'espai per a instal·lar-hi el GNU/Linux. En el cas del sistemes de fitxers FAT o FAT32 no hi ha cap problema d'interpretació des del GNU/Linux, i per tant, podrem trobar també altres eines de repartició del disc lliures a la Xarxa.

Si ja hi tenim instal·lat un sistema operatiu GNU/Linux, podem utilitzar una de les moltes aplicacions que hi ha per a redimensionar particions de discos durs i crear-ne de noves. Per exemple `partman` (eina original de GNU/Linux), `cfdisk`, o els editors gràfics `gparted` (escriptori Gnome) o `qtparted` (escriptori KDE). Aquestes aplicacions gestionen tant sistemes de fitxers de tipus FAT o FAT32 com NTFS.

Si no es disposa de cap sistema operatiu GNU/Linux ja instal·lat en el disc, podem utilitzar el Gparted Live-CD, que és un *live-CD* que conté un sistema operatiu GNU/Linux petit i bàsic que s'executa directament des del CD-ROM i que conté l'aplicació `Gparted`. Aquesta ens hauria de permetre poder reparticionar, i per tant, crear una partició nova per al nou sistema operatiu, en el disc on hi hagi també un Windows XP, Vista, 7 o 8, amb NTFS com a sistema de fitxers. No sempre funcionaran correctament, poden donar problemes i no permetre aquest reparticionament en alguns tipus de discos durs.

Com a última opció, sempre podem recórrer a aplicacions comercials. Però en tots els casos és molt important fer una còpia de totes les dades que sigui important resguardar (tot i que ja s'hauria d'haver fet abans), ja que estem accedint a dades i movent-les dels discos i sempre poden fallar aquests o l'electricitat. Per tant, no farem aquest pas sense tenir copiades totes les dades necessàries per a poder tornar a tenir el sistema inicial un altre cop operatiu en el mateix punt on era abans.

Independentment de l'aplicació que utilitzem per a crear la partició, abans sempre cal desfragmentar el disc. El desfragmentador de disc és una utilitat que permet analitzar discos locals, i trobar i consolidar carpetes i arxius fragmentats (separats en l'espai). També pot desfragmentar discos des d'una línia d'ordres mitjançant l'ordre `defrag`. Amb això evitarem problemes, ja que podem tenir arxius fragmentats i una part d'aquests al final de la partició. Per

tant, en redimensionar i prendre espai en aquesta part final, ens carregaríem aquests fitxers i, depenent del tipus, en el millor dels casos, perdríem la informació, però si són del sistema, podríem inutilitzar el sistema operatiu.

Una altra opció, que de fet seria la millor, és disposar d'un disc dur petit i nou (o formatat) que no calgui reparticionar, ja que podrem disposar de tot el disc. En aquest cas no tindrem cap problema amb les dades o sistemes operatius anteriors, ja que el sistema s'instal·larà en el nou disc i no es tocarà per a res l'anterior.

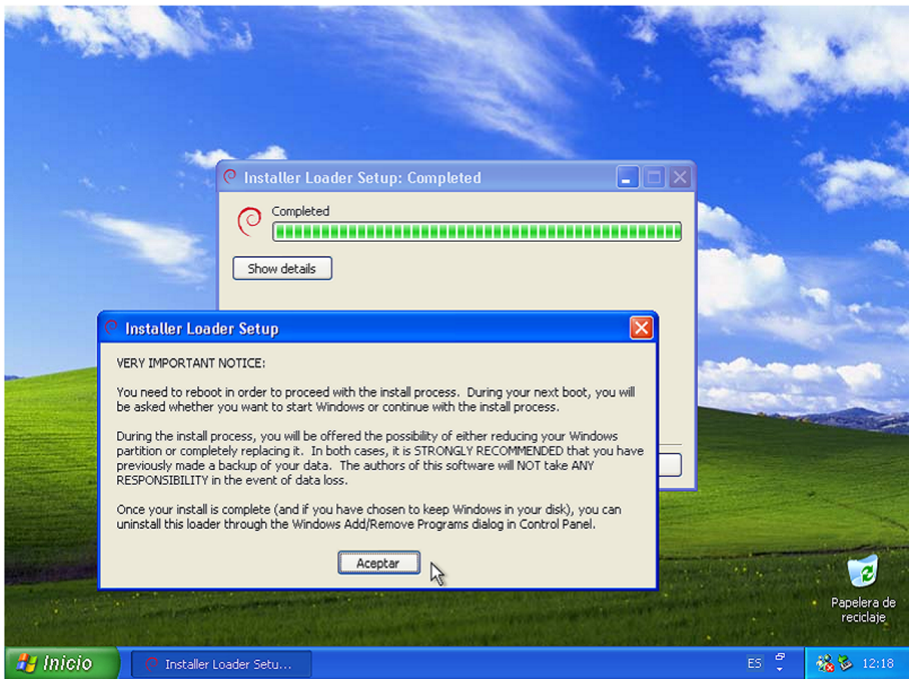
2.2.2. Arrencada del sistema d'instal·lació

Arribats a aquest punt, podem començar la instal·lació pròpiament dita. Per a això, arrencarem l'ordinador, ens assegurarem que el primer dispositiu a l'hora d'arrencar (*boot*) sigui la unitat de DVD-ROM (entrant a la BIOS) i hi posarem el CD que hem baixat i cremat en un CD. Al cap d'uns moments ens apareixerà una pantalla de benvinguda com la de la figura següent:

Inici d'instal·lació del Debian

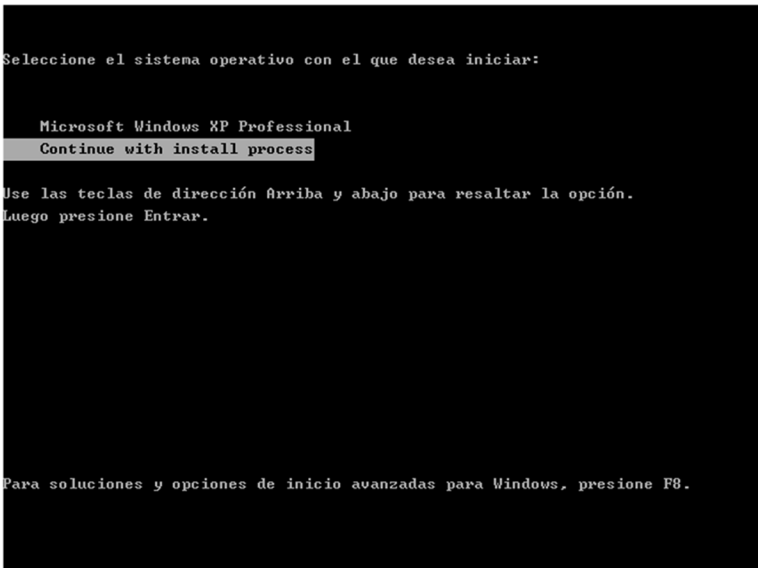
També es pot iniciar la instal·lació des del sistema operatiu que ja hi ha instal·lat en l'ordinador, simplement introduint el CD d'instal·lació del Debian i executant el fitxer `setup.exe`. Ens apareixerà una finestra en la qual ens demanarà l'idioma en què volem fer el procés d'instal·lació i començarà a copiar arxius en el disc dur per tal de tornar a reiniciar el sistema i arrencar amb el CD del Debian, sense tocar, per tant, la BIOS del sistema. Un cop acabat el procés s'haurà de reiniciar l'ordinador.

Instal·lació des del Windows



I en el moment d'arrencada ens demanarà si es vol continuar amb la instal·lació o arrencar amb l'antic sistema operatiu ja instal·lat en el disc.

Arrencada del sistema



A partir d'aquí ens sortirà la mateixa pantalla d'inici de la instal·lació del sistema GNU/Linux com si s'hagués fet canviant la BIOS per arrencar amb el lector de CD/DVD.

En les opcions avançades de la primera pantalla d'instal·lació trobarem un altre menú que ens permetrà fer la instal·lació de diferents maneres i podrem canviar l'escriptori que es faci servir, la instal·lació en mode expert, en què es pot configurar més acuradament tot el sistema. També es pot fer una recuperació del sistema a partir d'arrencar el CD amb l'opció de recuperació (*res-*

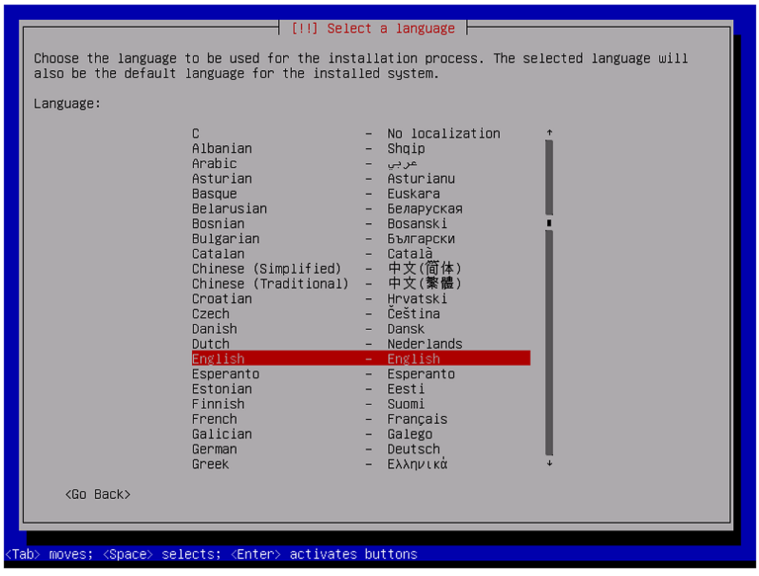
cue mode). Però aquesta part queda fora de la introducció al sistema operatiu que es vol donar en aquests materials. En tots els casos i, com abans, hi ha la possibilitat de fer la instal·lació dins un entorn gràfic o en una consola, i els resultats finals seran idèntics, encara que en el cas de fer servir l'entorn gràfic el procés serà més senzill.

Pantalla d'inici

2.2.3. Configuracions bàsiques per a fer la instal·lació

Si entrem a l'enllaç d'instal·lació de la primera figura veurem la pantalla següent, on s'inicia el procés d'instal·lació, i ens demana amb quin idioma es vol fer la instal·lació del sistema operatiu en el disc dur.

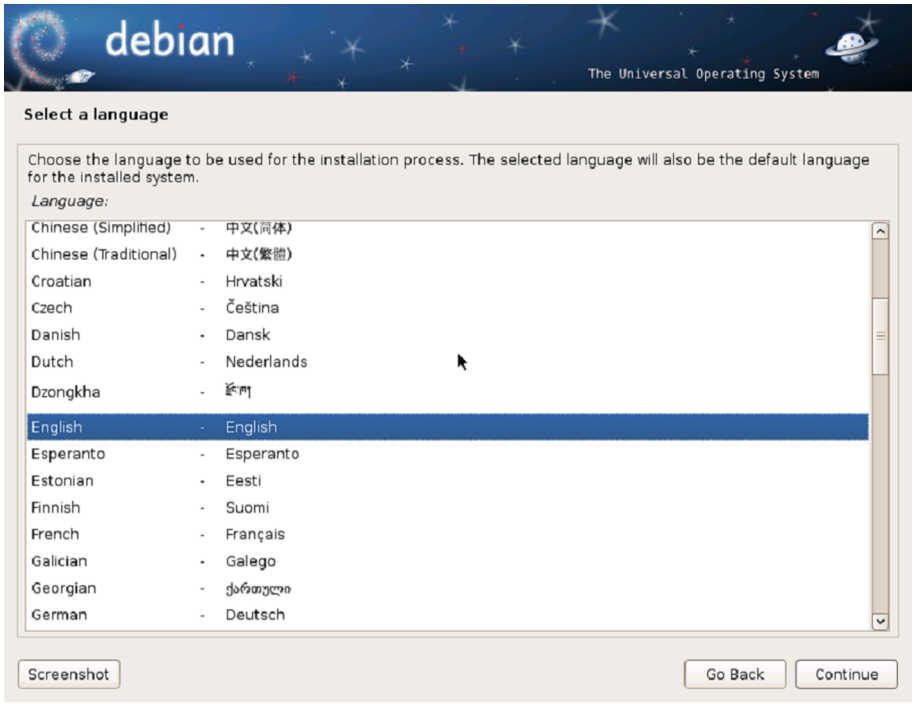
Primeres configuracions



Però si entrem a la instal·lació gràfica veurem que s'accedeix a les mateixes pantalles, però amb el ratolí en aquest cas en funcionament, i serà molt més còmoda la instal·lació. El procés és idèntic en els dos casos, encara que varia una mica en el cas de la instal·lació de sistema en mode expert, que ens demanarà alguns paràmetres de configuració addicionals.

Tornem, doncs, a iniciar el procés d'instal·lació, però en aquest cas amb l'opció gràfica i la instal·lació normal. El primer que s'ha de decidir és el llenguatge de la instal·lació. Podem optar per molts idiomes; escollirem el més adient.

Selecció de l'idioma



A partir d'aquí ens va demanant el tipus de teclat que es fa servir, i seleccionarem el teclat espanyol, la zona horària on som i la localització dels *locales* de les configuracions específiques per a cada regió i teclat.

A partir d'aquest moment ja es pot accedir a un intèrpret d'ordres (*shell*) del sistema per si de cas en calgués un; s'hi accedeix amb la combinació de les tecles Ctrl + Alt + F2 i quan ens ho digui, la tecla Enter. Aquest intèrpret serà molt bàsic, però podrem fer alguna prova.

En la TTY1 (Crtl + Alt + F1) el sistema va deixant els missatges dels esdeveniments que va fent i mostrarà els registres del sistema, que també es poden trobar en el fitxer `/var/log/messages`.

Per a tornar un altre cop a la sessió gràfica s'ha de canviar a la TTY5 (Crtl + Alt + F5). Aquestes TTY podrien canviar en les diferents distribucions i possiblement en versions diferents de la mateixa distribució, però és segur que existeixen en alguna sessió.

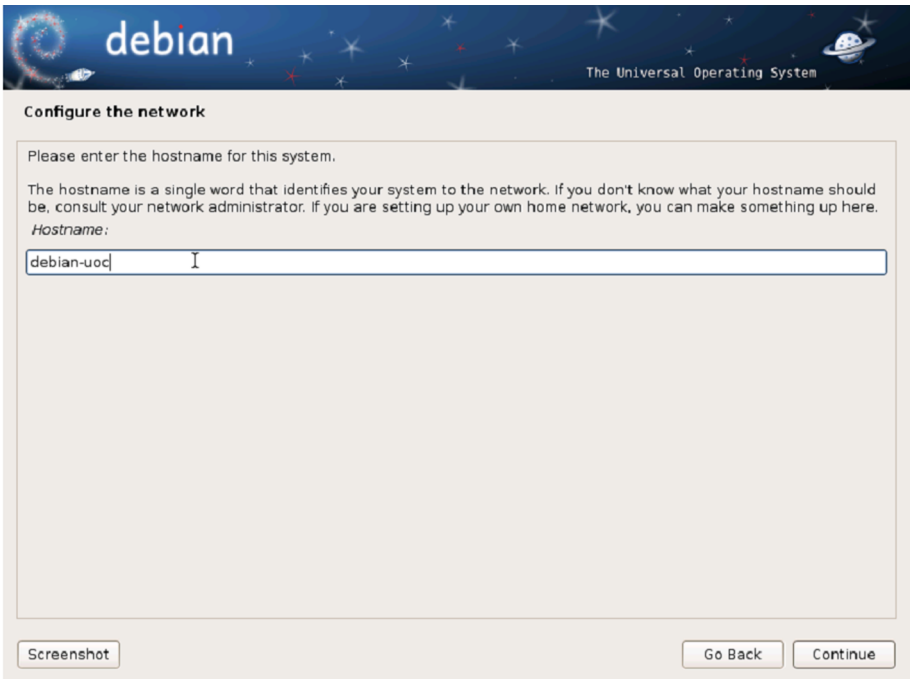
El pas següent és la configuració de la xarxa de comunicacions, i en el cas que el Debian tingui els controladors del dispositiu de xarxa i trobi un servidor d'adreces i per DHCP en pugui obtenir una no ens preguntarà res, i per tant no caldrà configurar res ni donar-li cap mena de dada pel que fa a la xarxa.

Normalment els encaminadors que les operadores de telecomunicacions proporcionen ja tenen activat aquest servidor d'adreces, i per tant no hauríem de tenir problemes, però si no el tenen activat i no es pot o no es vol activar, haurem d'introduir totes les dades relatives a la xarxa local, com l'adreça IP del sistema que estem instal·lant, la màscara de xarxa, la porta d'enllaç i els servidors de noms que s'han de fer servir. Tot això es pot trobar mirant les configuracions d'altres equips de la xarxa, canviant l'adreça IP en cada equip, o en la configuració de l'encaminador de què es disposi.

Aquest pas és important que es faci bé, ja que en ser una instal·lació mitjançant la xarxa, si no es disposa d'aquesta no es podrà acabar correctament i s'impedirà que es pugui instal·lar tot el programari necessari per al funcionament del sistema i les seves aplicacions. Per tant, abans d'iniciar la configuració de la xarxa, si no tenim activat el DHCP en l'encaminador o en un servidor propi, hem de tenir a mà els paràmetres relatius a la xarxa, per no haver de parar la instal·lació a mitges.

El següent que s'ha de configurar és el nom de l'equip; cada un té un nom diferent, per a identificar-lo dins una xarxa. Es pot posar el que es vulgui, però és preferible posar-hi alguna cosa que ens faciliti identificar-ne el propòsit. En el cas de tenir un sistema únic per a casa, qualsevol nom servirà, però per a una empresa en la qual hi pot haver milers d'ordinadors, una mínima política de noms facilitarà molt la feina a l'hora de localitzar un ordinador que doni problemes i s'hagi de fer alguna tasca de manteniment, canviar-lo, reinstal·lar-lo, etc.

Nom de l'equip



En la part de la configuració de la xarxa ja només queda emmarcar el sistema en un domini, en un grup d'ordinadors que comparteixen una mateixa "sala" dins la xarxa, ja que tots aquells ordinadors que estiguin dins el mateix domini no tindran problemes per a veure's entre si i, així, poder compartir molt més fàcilment la informació. Podem deixar per defecte aquesta informació per a ordinadors domèstics, si només en tenim un, o posar el nom del domini que hi hagi a casa o a l'empresa on s'hagi d'instal·lar el sistema.

2.2.4. Usuaris i contrasenyes

Els passos següents són la configuració dels usuaris inicials del sistema; el primer que s'ha de fer és decidir la contrasenya de l'usuari amb permisos d'administració del sistema, el *root*. Aquesta contrasenya ha de ser prou complicada perquè no sigui fàcil de reproduir per a una altra persona sense que la sàpiga prèviament. Actualment els ordinadors estan tots connectats a Internet, i per tant exposats als atacs de les persones que volen obtenir accés a totes les màquines per poder, com a mínim, tenir-ne el control i poder-ne atacar d'altres des de la nostra màquina.

Una bona contrasenya és la que disposa de lletres, xifres i signes de puntuació com @, !, $, +, =, . (punt), , (coma), etc. En el cas de tenir un teclat espanyol també és recomanable fer servir lletres que no es troben en altres teclats, com la *ç* o la *ñ*. Una altra qüestió molt important és que l'usuari *root* s'ha de deshabilitar en l'entrada i no es podrà entrar al sistema com a *root*, per la qual cosa serà necessari entrar al sistema com un usuari normal i executar les ordres que

es vulgui com a *root* amb la instrucció `sudo`, que permet executar ordres des dels usuaris normals amb privilegis de *root*, sempre que s'hagi habilitat l'usuari per fer-ho.

El següent que s'ha de fer és la configuració del primer usuari del sistema, que es farà servir per a tot el que no siguin tasques d'administració del sistema. Opcionalment se'n pot donar un nom complet i després el nom que es vol que faci servir com a usuari.

Usuari del sistema

En el cas de la instal·lació, si no posem contrasenya a l'usuari *root*, aquest primer usuari que es crea en la instal·lació tindrà automàticament els drets de poder fer servir la instrucció `sudo` per a poder fer tasques administratives, ja que l'usuari *root* no existirà.

2.2.5. Rellotge del sistema

Queda configurar el rellotge del sistema, dient a quina franja horària som i, per tant, es vol configurar el sistema operatiu. En el cas de no tenir problemes, simplement demana a partir de la configuració dels *locales* que se li ha dit al principi quina franja horària volem. Cal tenir en compte que hi ha països que en tenen més d'una, com per exemple Espanya, en la qual n'hi ha una de diferent per a les illes Canàries.

2.2.6. Partició del disc dur

A partir d'aquí ja es comencen a complicar les decisions i a tenir més problemes en les repercussions, ja que ara s'ha d'afrontar el particionament del disc. Ens demana quin disc volem fer servir per a instal·lar el sistema i si volem o no fer-hi particions.

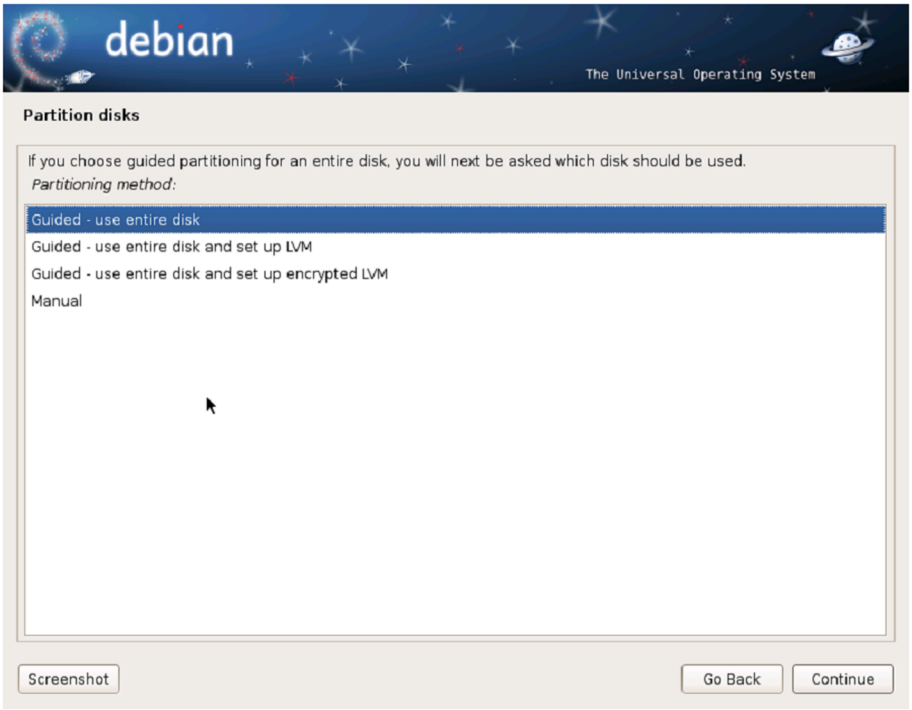
A l'hora de particionar els discos, la mida, les característiques i el nombre de particions depenen en gran manera del tipus d'ús i de la quantitat de disc dur de què es disposi. En tractar-se d'una instal·lació amb finalitats educatives, es facilita seguidament la informació sobre les particions que es crearan suposant que es treballa sobre un espai entre els vint i els trenta gigabytes destinats a la nova instal·lació.

Com a mínim cal crear dues particions: una primera per a muntar el sistema i l'altra, de *swap* o intercanvi de memòria. Per tal d'augmentar l'eficiència del sistema, nosaltres crearem sis particions, i d'aquesta manera el sistema serà més flexible i molt més eficient, ja que se separaran completament els programes, el sistema, els arxius d'usuari, etc.

El primer que s'ha de decidir és en quin disc s'instal·larà el sistema: si només en tenim un podem anar directament a l'enllaç de particionament guiat; si en disposem de més d'un, en seleccionem un per tal de fer-hi la instal·lació.

En tots dos casos arribarem a la configuració del particionament guiat, on el seleccionarem, ja que altres tipus de configuracions, com el RAID dels discos o la configuració en LVM dels discos, queden fora de l'abast d'aquests materials.

Particionament del disc



Discos RAID i LVM

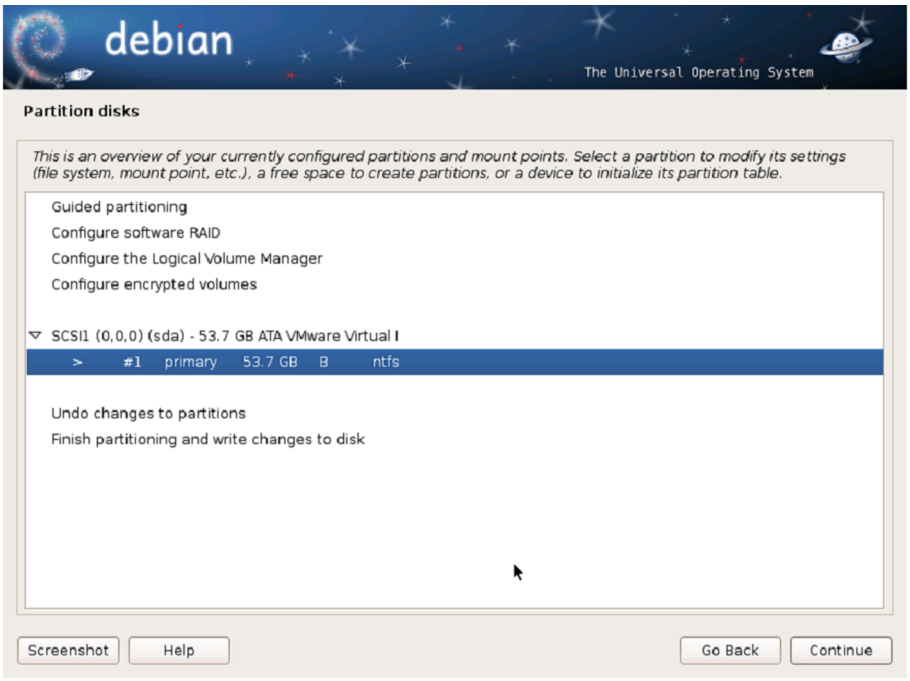
La configuració en RAID dels discos implica tenir més de dos discos en l'ordinador, que configurarem per poder tenir tolerància a fallades en un dels discos. Hi ha diversos tipus possibles, depenent de cada configuració.

La configuració *logical volume manager* permet tenir més de dos discos configurats perquè el sistema i l'usuari els vegin com un de sol molt més gran, amb la capacitat de tots els discos junts. Aquesta configuració no permet tolerància a fallades, i si es trenca un disc es perd tota la informació.

En el cas de tenir un altre sistema operatiu en el disc, s'ha d'anar amb més cura amb el que s'està fent, ja que si seleccionem el procés guiat de tot el disc s'esborrarà tot el contingut perquè l'estem fent sobre el disc sencer. Per tant, el que s'ha de fer abans de fer les particions per al nou sistema és dividir el disc en dos, una part per al sistema antic, i una altra per al nou GNU/Linux, que després tornarem a partir. Per tant, en aquest moment s'haurà de seleccionar el procés manual per a particionar el disc. Com s'ha dit, en el cas de disposar d'un disc separat per a poder instal·lar el nou sistema operatiu aquest problema no el tindrem, i es podrà fer el particionament guiat directament.

El pas següent (vegeu la figura següent) és seleccionar el disc que volem particionar en dos i després clicar en l'opció de canviar de mida la partició.

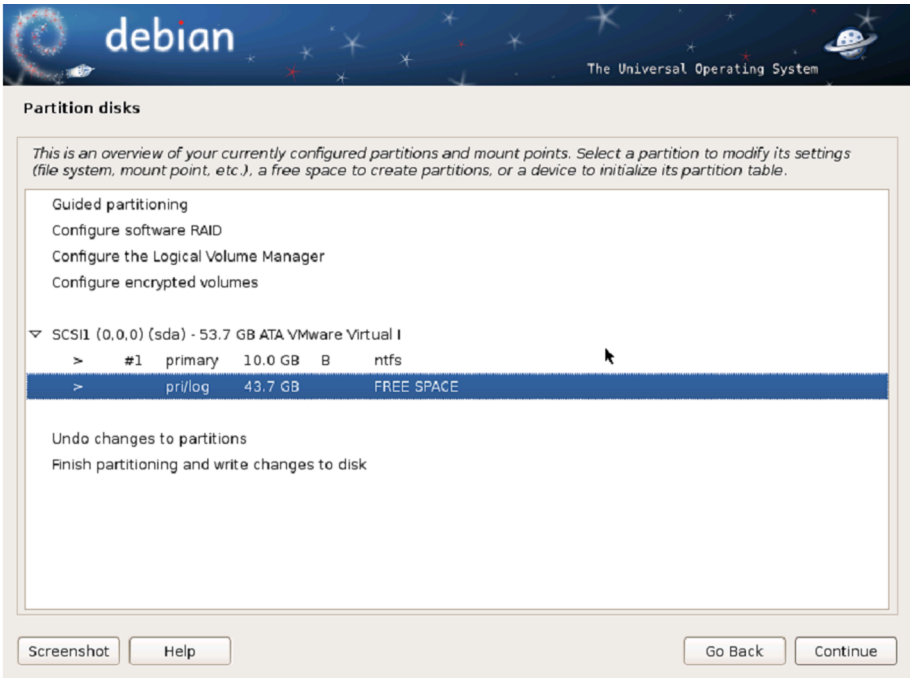
Partició per a instal·lar



Un cop dins de l'opció, s'ha d'indicar com es fan les dues parts. Es pot indicar la capacitat de la primera, en gigabytes, per exemple, o indicant el percentatge que es vol per a la primera partició sobre el total del disc.

Un cop acabat el procés de divisió del disc dur, que depenent de la capacitat del disc pot trigar bastant, el procés d'instal·lació tornarà a la pantalla de fer les particions, però ara veurem que han aparegut dues particions grans del disc que teníem abans: una amb el sistema de fitxers del sistema operatiu antic i una de nova amb tot l'espai lliure i sense sistema de fitxers.

Particions creada per a instal·lar el Debian

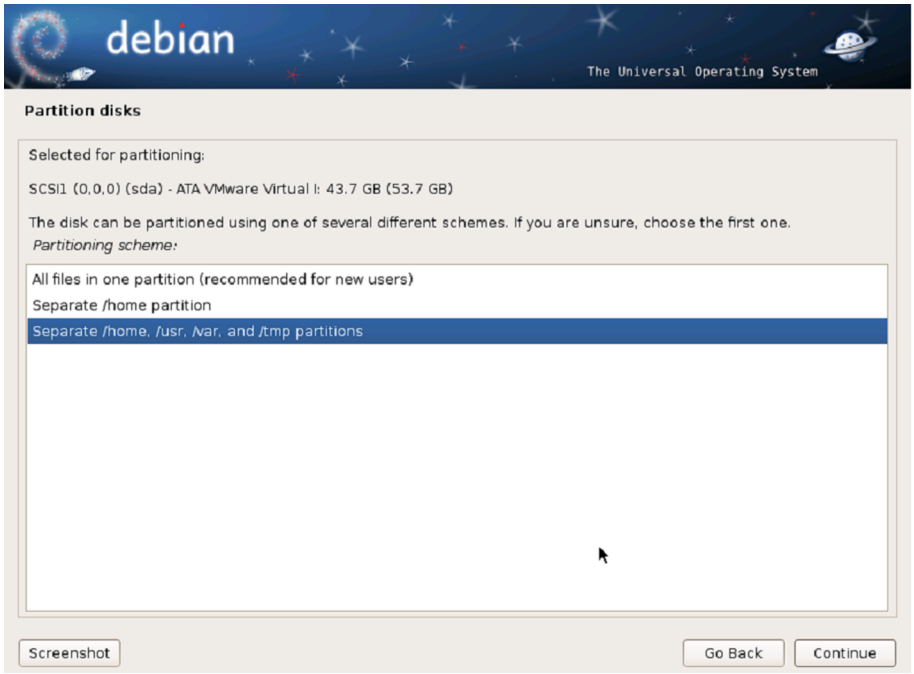


Seleccionarem la part nova que s'ha creat per a instal·lar el sistema, i crearem la partició d'aquesta part que encara no està creada en el disc, simplement deixant que es faci la partició automàticament sobre tot l'espai lliure que hi ha ara en el disc. Ara ja es disposa de dues grans particions: una per al sistema operatiu antic, el que hi havia en el disc dur, i l'altra per al nou, però en una sola part. Recordem que aquesta s'ha de tornar a dividir, almenys per a poder fer l'àrea del sistema operatiu i la d'intercanvi (tot i que realment no caldria, el rendiment del sistema baixaria considerablement).

Aquest procés seria idèntic en el cas de tenir dos discos: en aquest cas, en lloc de seleccionar la segona part lliure del disc, seleccionaríem el segon disc dur. I el procés a partir d'aquí seria idèntic.

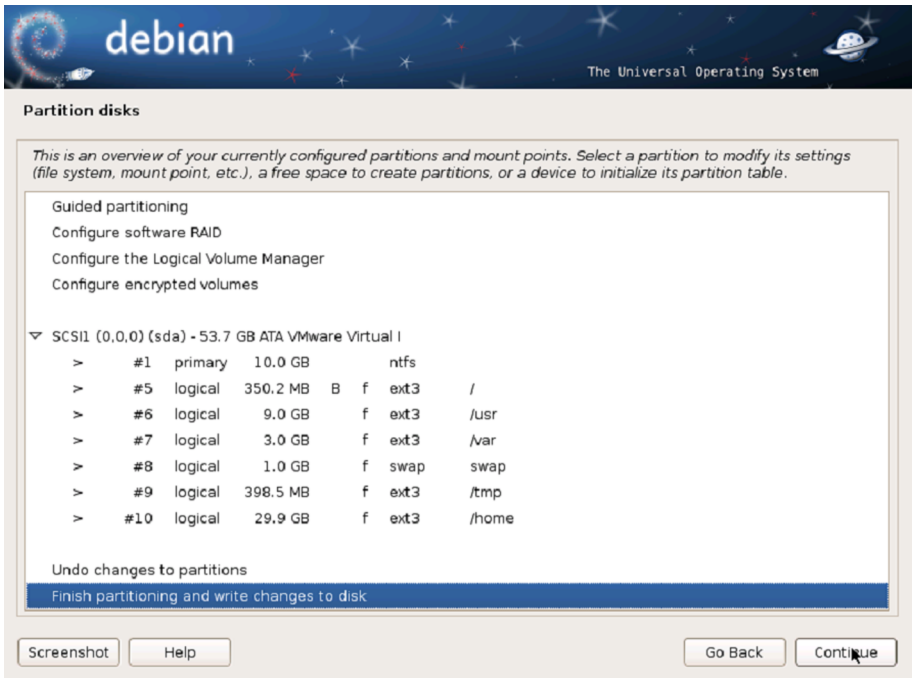
El més recomanable és dividir les dades d'usuari, les de les aplicacions, i el sistema, ja que això permet actualitzar-lo, i fins i tot canviar de distribució sense perdre mai les dades d'usuari. Es podria formatar la part del sistema sense perdre mai les nostres dades. Per tant, en el pas de particionar el disc de manera guiada seleccionarem que se separin els directoris `/home`, `/usr`, `/var` i `/tmp`.

Creació de les particions de sistema



Finalment, el procés acaba amb l'escriptura en el disc de totes les noves particions, en les quals s'han creat sis noves parts a banda de la inicial amb el sistema operatiu antic. Podem veure que ja s'ha dividit amb les mides que el sistema necessita. Aquestes mides seran diferents tenint en compte la capacitat de la partició, o el disc sencer, que s'assigna per a fer la instal·lació del nou sistema operatiu. Per tant, només queda finalitzar i escriure els canvis en el disc dur.

Particions creades



També es pot fer aquest procés manualment, creant les particions una a una especificant-ne la mida, el punt de muntatge, el tipus de fitxer, etc.

Per a crear una nova partició, cal seleccionar l'opció adequada i a continuació, si encara es poden crear particions primàries (cal tenir en compte que el nombre màxim són quatre), ens preguntarà si la volem crear com a partició primària o lògica; després, hem d'especificar la mida de la partició, i, finalment, la ubicació física en el disc (és recomanable que abans de començar a fraccionar el disc fem un petit esquema de com ho volem fer i que a continuació creem les particions a partir d'aquesta darrera partició feta). A més, és important tenir aquest esquema per a veure quines mides tindrà cada una abans de començar i no haver de tornar a esborrar particions perquè no es tenen clares les mides.

La primera partició és la destinada a allotjar l'arrel (/); aquesta no ha de ser gaire gran i per això s'hi destinarà menys d'un deu per cent del disc dur (o partició dedicada al GNU/Linux), preferentment en una partició primària, però si no en disposem, la podem crear com a partició lògica sense donar-hi més importància. Li indiquem que la partició serà al principi de l'espai lliure i que el tipus de sistema d'arxius triat per a la partició és *ext3*.

La segona es destinarà a la partició d'intercanvi (*swap*). Es recomana que aquesta tingui, com a mínim, una mida igual a la de la memòria RAM, 512 MB, 1.024 MB,etc. Tot i que per a sistemes amb menys d'1 GB de memòria hauria de ser una mica més del doble, en sistemes amb molta més memòria no cal tenir el mateix, tot i que és recomanable. En el cas de voler hibernar el sistema, sobretot en instal·lacions en portàtils, és important tenir com mínim el doble de la memòria física assignada a la partició de *swap*, ja que per hibernar el GNU/Linux fa una còpia de la memòria real en l'àrea de *swap* i si no hi cap, o ja està

força ocupada per dades perquè la memòria física està saturada, no es podrà hibernar el sistema. Aquesta partició també és preferible que sigui primària, però si ha de ser lògica, tampoc no repercutirà en el rendiment del sistema. Si tenim més d'una instal·lació de GNU/Linux en el mateix ordinador, es pot utilitzar la mateixa partició *swap* per a totes, ja que la informació que s'hi pugui emmagatzemar durant el funcionament del sistema és totalment volàtil. El tipus de sistema d'arxius per a la partició *swap* serà d'intercanvi (*swap area*).

La tercera partició serà per al directori *usr* (`/usr`); cal tenir present que aquesta partició inclourà gran part del programari que s'hi instal·li, per la qual cosa haurà de tenir una mida significativa, entorn d'un quaranta per cent del disc. El seu sistema d'arxius serà *ext3*.

La quarta partició es destinarà al directori *var* (`/var`), on s'allotgen biblioteques, fitxers de registre, etc. Igual que les anteriors, també serà *ext3*. I no cal que tingui una gran mida.

La cinquena partició estarà destinada a allotjar els directoris personals dels usuaris (`/home`), la finalitat dels quals és emmagatzemar les dades dels usuaris, i, depenent de la mida del disc dur, se li pot assignar la resta de la mida del disc dur, en funció del nombre d'usuaris i de l'ús que es farà del sistema: no és el mateix tenir un equip dedicat a edició de vídeo que un per a tractar documents d'ofimàtica o navegar per Internet; les dades que s'han d'emmagatzemar afectaran força aquesta partició de dades d'usuaris. Aquesta partició també serà *ext3*.

L'espai restant, la sisena partició, es destinarà al directori de fitxers temporals (`/tmp`) i el seu sistema d'arxius també serà *ext3*, amb una mida relativament petita, ja que són fitxers temporals que es poden anar esborrant.

La distribució de particions anterior és només una proposta que té dos objectius: d'una banda, pretén millorar el rendiment que ofereix una instal·lació basada únicament en una o dues particions i, d'una altra banda, dóna més robustesa al sistema. Entre altres avantatges, tenir les dades repartides entre diferents particions provoca que la corrupció d'una no impliqui automàticament la pèrdua de tota la informació del sistema. Òbviament, es poden crear altres particions o ometre algunes de les propostes (l'ordre de les particions no afecta el comportament del sistema).

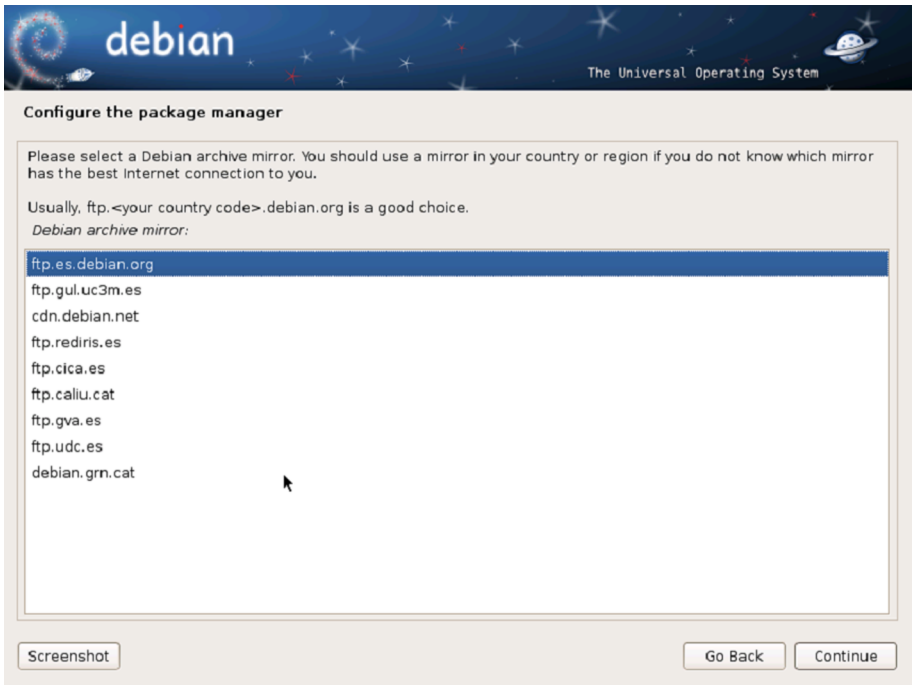
2.2.7. Instal·lació del sistema base

Ara l'instal·lador començarà a copiar en el disc dur el sistema base que ens permetrà després seleccionar el que es vol instal·lar i accedir a la xarxa per acabar d'obtenir i instal·lar les aplicacions necessàries per a tenir tot el sistema a punt.

Per a poder seleccionar després els paquets hem d'escollir una rèplica de les moltes que té el Debian per tot el món. És recomanable per temes de temps escollir la que hi ha al propi país o el més a prop, ja que així la latència serà molt menor. També es pot seleccionar la rèplica que creiem o sabem que té més amplada de banda, perquè així trigarem menys temps a baixar-nos d'Internet les aplicacions. Però en principi tot està replicat en totes i no hem de tenir cap problema en l'elecció més enllà del temps de baixada dels fitxers.

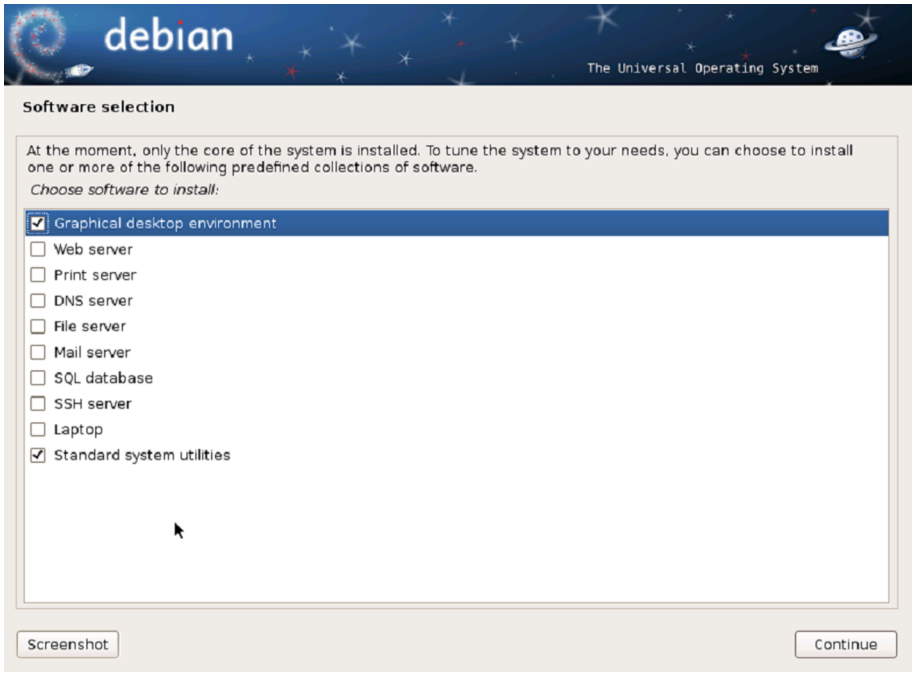
En el cas de necessitar un servidor intermediari (*proxy*) per a tenir accés a Internet des de l'ordinador en el qual s'està fent la instal·lació, s'haurà d'especificar abans de poder accedir a les rèpliques; en cas de tenir accés directe, no cal indicar res en el camp de la configuració del servidor intermediari.

Configuració de les rèpliques del programari



2.2.8. Instal·lació de programes

Selecció del programari



A partir de la utilitat que es vulgui donar al sistema operatiu, cal seleccionar les diferents utilitats i eines que es requereixin. En el cas de tenir un sistema bàsic per a començar a treballar amb el GNU/Linux, només cal tenir l'entorn gràfic i les utilitats bàsiques del sistema i deixar tots els programes i utilitats dels servidors per a quan es disposi de més coneixement del sistema. En el cas de tenir un servidor, en aquest pas ja serà possible instal·lar tots aquells components que siguin necessaris, com el servidor de fitxers, el de pàgines web, el servidor SSH, etc.

Aquest procés pot ser força llarg depenent de la velocitat de baixada de la connexió a Internet que es tingui, ja que ara es baixaran tots els fitxers de les aplicacions que s'estan instal·lant en el disc dur.

Un cop acabat, instal·larà el sistema d'arrencada en el cas de tenir un altre sistema operatiu abans, i indicarà quin s'ha trobat; si realment es vol instal·lar aquest gestor es podria optar per fer-ne servir algun altre, o no instal·lar-ne cap en aquest moment. Per a poder accedir als dos sistemes operatius és necessari tenir un gestor d'arrencada per a les particions dels discos durs. És recomanable instal·lar aquest, que ja configura sol el programa d'instal·lació del GNU/Linux.

Si tot ha anat correctament, finalment apareix la pantalla que ens diu que ja s'ha completat tota la instal·lació, i per tant ja podem iniciar el sistema.

Per a poder fer servir l'usuari amb què es treballarà normalment, el que es dóna d'alta en el moment de la instal·lació, en tasques d'administració, cal donar accés a l'ordre `sudo`, i això es fa amb la instrucció `visudo`, amb què podem afegir els usuaris a la llista d'admesos per a fer servir l'ordre `sudo` i, per tant, per a operar com a *root* en el sistema.

Finalment, per a tenir accés a un nombre més gran de paquets, s'ha d'activar el repositori *non-free*. Per a fer-ho, cal iniciar la sessió en la màquina i obrir un terminal des de l'usuari d'accés, canviar-se a l'usuari *root* amb l'ordre `sudo` i, finalment, editar el fitxer `/etc/apt/sources.list` amb qualsevol editor de text (`vi`, `gedit`, etc.).

```
# sudo root
Password: *****
# vi /etc/apt/sources.list
...
deb http://ftp.es.debian.org/debian/ squeeze non-free
deb-src http://ftp.es.debian.org/debian/ squeeze non-free
...
```

També es pot fer de manera gràfica amb l'aplicació de fonts del programari, dins el menú de sistema, on directament es pot seleccionar el programari no lliure.

2.2.9. Activació de serveis i protocols de xarxa

En aquest apartat mostrarem com s'instal·la i es configura la xarxa en un sistema operatiu basat en el GNU/Linux. Un requisit per a la instal·lació és tenir una targeta de xarxa, no un mòdem, ja que amb el mòdem no tenim un accés a una xarxa pròpiament dita, sinó només a un ordinador que rep la nostra trucada i fa de pont cap a Internet. Actualment, la majoria de les grans distribucions de GNU/Linux ja s'instal·len amb l'opció de treball en xarxa activada, però antigament no era així.

Malgrat que estigui activat el treball en xarxa, és possible que hàgim de compilar el nucli. Això es deu al fet que en el nucli hi ha definits els tipus de targetes de xarxa, conegudes també com a NIC (*network interface card*), compatibles directament amb el sistema. Si fem servir un tipus de targeta molt específic, hem de compilar el nucli i afegir-hi la nostra targeta de xarxa. Per fer-ho, hem de seleccionar el nostre tipus de targeta de la llista de dispositius compatibles, guardar la configuració i executar les ordres que compilen el nucli. Si fem servir targetes de xarxa conegudes (3Com, Intel, Ne2000, etc.) i una distribució de les més utilitzades (Red Hat, Caldera, Suse, Debian, Ubuntu), ens estalviarem haver de compilar el nucli, ja que la gran majoria de targetes són compatibles.

Hem de saber quin dispositiu utilitza la targeta de xarxa. Si només tenim una targeta de xarxa, és molt probable que el nostre dispositiu sigui el `/dev/eth0`, però per a assegurar-nos-en hem d'executar l'ordre `dmesg` i buscar el dispositiu de xarxa en la llista de dispositius que retorna aquesta instrucció. Podrem veure si es troba a `eth0`, a `wlan0`, o quin és el dispositiu al qual està connectat.

Amb `dmesg | grep eth0` podrem saber si ens diu que és el dispositiu `eth0`; si no podem buscar per `wlan0`, o algun altre.

Abans de configurar el protocol IP, és molt important tenir les dades de configuració de la xarxa. Aquestes dades les ha de facilitar el proveïdor de servei ISP o l'administrador de la xarxa a la qual es vol connectar la màquina. En aquestes dades hi ha de constar:

- L'adreça IP.
- La màscara de xarxa.
- La passarel·la predeterminada (*gateway*).
- El servidor de noms (DNS) primari i, opcionalment, el secundari.
- El tipus d'adreça (estàtica o dinàmica).

En el cas d'un servidor, és important tenir adreces fixades des de la mateixa màquina i no fer servir clients de DHCP que ens podrien donar adreces diferents depenent de les circumstàncies. Així ens assegurem que sempre tindrà la mateixa IP, i per tant els ordinadors connectats no hauran de canviar mai l'adreça.

Ara que tenim totes les dades necessàries podem començar a configurar la xarxa.

Hi ha molts altres paràmetres de configuració, des de l'adreça IP, la màscara d'aquesta adreça, la passarel·la, etc. Per a més informació, consulteu el manual (`man`). La configuració que obtenim mitjançant l'execució d'aquesta ordre és una configuració temporal i quan tornem a arrencar la màquina, la configuració s'haurà perdut. Segons la distribució GNU/Linux que tinguem, és possible que en arrencar ens detecti la xarxa, i si la nostra xarxa es configura mitjançant DHCP, el sistema ja ens la configura de manera automàtica.

Si la nostra xarxa no utilitza DHCP o el sistema no ens configura la xarxa en temps d'arrencada, l'hem de configurar nosaltres mateixos perquè funcioni de manera permanent. La manera de configurar permanentment la xarxa té lleugeres modificacions segons la distribució del GNU/Linux que utilitzem. En el cas concret del Debian es configura de la manera següent:

L'ordre `ifconfig`

Una instrucció bàsica a l'hora de configurar la xarxa és l'ordre `ifconfig`. Si l'executem sense cap paràmetre, ens mostra la configuració actual. Si, per exemple, però, volem configurar un dispositiu de xarxa `eth0` amb adreça IP dinàmica, hem d'executar des de *root* `# ifconfig eth0 up`.

Què és el `man`?

El `man` és una ajuda que ens ofereix el sistema sobre les ordres i els paràmetres d'aquestes ordres. Per consultar aquesta ajuda hem d'executar `man comanda`, en què `comanda` és l'ordre que volem consultar.

1) Editar el fitxer `/etc/network/interfaces`.

2) Afegir a la línia `auto` el nou dispositiu.

3) Si configurem amb una adreça IP dinàmica hi hem d'afegir:

```
iface eth0 inet dhcp
```

4) Si configurem amb una adreça IP estàtica hi hem d'afegir:

```
iface eth0 inet static address vostra_adreça_IP netmask
vostra_mascara_IP gateway vostra_gateway_IP
```

Arribats a aquest punt ja tenim adreça IP; ara ens falta configurar el servidor de noms de domini (DNS) i les rutes. Per a més informació sobre el fitxer `interfaces`, consulteu el `man` (`man 5 interfaces`). Per a configurar el DNS hem d'editar el fitxer `/etc/resolv.conf` i afegir-hi una línia amb la informació següent.

```
nameserver vostre_servidor_DNS
```

Si tenim servidor secundari de DNS, hi hem d'afegir una segona línia amb les dades d'aquest servidor secundari. Si l'adreça IP és d'assignació dinàmica, el DNS és un paràmetre que rebrem per DHCP; per tant, no hem de configurar res.

En la majoria de les distribucions, quan es configura una interfície de xarxa amb la seva adreça IP normalment ja s'hi afegeix la ruta estàndard corresponent. Si no s'hi ha afegit, però, o no en tenim prou amb la ruta estàndard, hem de configurar les rutes.

Per a configurar les rutes d'encaminament (*routing*) cal que estigui configurat com a mínim un dispositiu de xarxa. L'ordre que s'utilitza en aquest cas és `route`.

L'ordre `route`

L'ordre `route` sense cap paràmetre ens mostra la taula d'encaminament que hi ha activa en aquell moment. Per a afegir-hi una ruta, hem de fer servir els paràmetres `route add options`, i per a esborrar-ne una, `route del options`. Per a més informació sobre aquestes opcions, consulteu el `man`.

2.2.10. Protocols i sistemes d'autenticació d'usuaris

Hi ha diversos mètodes d'autenticació dels usuaris en sistemes basats en el GNU/Linux. Els mètodes que comentarem a continuació són, o han estat, molt comuns.

El primer mètode i el més simple és l'autenticació mitjançant el fitxer `/etc/passwd`. Cada línia d'aquest fitxer conté tota la informació d'un usuari. Els camps estan separats pel signe (:). El primer registre de la línia és l'identificador d'usuari. El segon registre és la contrasenya o *password*.

```
jordi: abcfl3yjFYN4Q:1000:1000:Jordi Serra:/home/jordi:/bin/bash
```

La contrasenya es trobava en text pla (al començament de l'era Unix) o xifrada, mitjançant la codificació *crypt* (com en l'exemple superior). La segona manera d'autenticar és mitjançant el fitxer `/etc/shadow`. És una versió millorada del mètode anterior. En el registre *password* (el segon camp) del `/etc/passwd` s'hi posa la lletra `x`; llavors el sistema busca la contrasenya en el fitxer `/etc/shadow`. Aquest fitxer té un format semblant al fitxer `/etc/passwd` però canvien els valors de la majoria dels registres. Igual que en el cas anterior, el primer camp és l'usuari i el segon -separat per (:)-, la contrasenya codificada mitjançant *crypt* o MD5. L'avantatge d'aquest mètode respecte a l'anterior és que ningú (excepte l'usuari *root*) no té accés a aquest fitxer, ni de lectura. Per tant, fa més difícil poder accedir a aquesta informació.

Els mètodes que comentarem a partir d'ara són mètodes que requereixen la instal·lació d'un programa anomenat *pluggable authentication module* (PAM). El PAM és un joc de biblioteques compartides que habiliten l'administrador local del sistema a triar la manera en què els programes autenticaran els usuaris. Dit d'una altra manera, és possible intercanviar els mètodes d'autenticació que fa servir una aplicació que funcioni amb el PAM sense haver de (reescriure o) compilar la configuració d'aquesta aplicació. Encara més, es pot actualitzar el sistema d'autenticació local sense tocar les aplicacions pròpiament dites. Aquesta aplicació dóna molta flexibilitat a l'administrador a l'hora de configurar i garantir els privilegis del seu sistema.

Un altre mètode d'autenticació és mitjançant la base de dades. Cal disposar d'una base de dades, sigui local o remota, amb una taula en què hi hagi els usuaris. Aquesta taula ha de contenir com a mínim el camp de l'usuari i la contrasenya. Per autenticar d'aquesta manera hem de configurar els PAM indicant-hi on hi ha la base de dades, quin usuari cal per a accedir a la base de dades, quina taula hem de fer servir i quins camps contenen la informació d'usuari i contrasenya.

Una versió millorada d'aquest últim mètode és l'anomenat *lightweight directory access protocol* (LDAP). Com indica el nom, es tracta d'un client molt lleuger per a accedir a serveis de directori. Un directori és semblant a una base de dades, però tendeix a contenir informació més descriptiva dels atributs. En un directori la informació es llegeix molt més del que s'escriu. Hi ha moltes maneres de configurar un servidor LDAP; una és fent servir el PAM. Per a configurar el PAM amb l'LDAP hem de saber on hi ha el directori (el nom de la màquina que ofereix el servei d'LDAP, i el port per on parla el servidor), si cal un usuari per a accedir al directori i quins atributs necessitem per a autenticar (usuari i contrasenya). Encara que sembli una contradicció, a vegades cal un usuari i una contrasenya vàlids per a autenticar els usuaris. És a dir, que només hi ha determinats usuaris que tinguin el privilegi d'autenticar els usuaris. A vegades, aquest tipus de doble autenticació és més perjudicial que beneficiosa.

Usurpadors d'autenticitat

Imaginem-nos que un pirata informàtic és capaç de capturar una petició LDAP d'autenticació normal. Està en possessió d'un usuari sense privilegis. Ara imaginem-nos que captura una petició LDAP d'autenticació amb un usuari amb privilegis d'autenticar. La captura d'aquesta petició té molt més valor, ja que a més d'un usuari normal té en poder seu un usuari amb privilegis sobre el directori.

L'última manera d'autenticar que comentarem en aquest apartat (n'hi ha moltes més, però aquí només comentem algunes de les més habituals) s'anomena *remote authentication dial in user service* (*Radius*). El mètode d'autenticació *Radius* també té associada una base de dades al darrere. El que el fa diferent dels altres mètodes és que és compatible amb molts protocols d'autenticació (PAP, CHAP, EAP, MD5, etc.) i, a part de tenir la capacitat d'*accounting*, és capaç de determinar per a cada usuari el tipus de servei que ha d'oferir. Fins ara l'han fet servir molt els ISP per a donar servei als seus usuaris de marcatge. Actualment també s'utilitza molt per a autenticar els usuaris de xarxes sense fil. Aquesta nova aplicació de *Radius* es deu al fet que s'han desenvolupat una sèrie de protocols segurs (xifrats) a nivell dos, per a donar servei a xarxes tradicionalment insegures (xarxes sense fil).

Per triar un protocol d'autenticació per a la nostra màquina hem de tenir presents dos aspectes: l'entorn i la seguretat. L'entorn ens marca quin tipus de necessitats tenim. No és el mateix tenir una màquina amb tots els serveis d'usuari que tenir una màquina per a cada servei i els usuaris accedint a totes aquestes màquines. En el primer cas, amb `/etc/shadow` i codificació MD5 n'hi ha prou. En el segon, és recomanable tenir un servidor dedicat a autenticar i que tots els servidors hi acudeixin per donar accés als usuaris. En aquest cas, des del punt de vista de la seguretat, és recomanable fer servir LDAP o *Radius*.

3. Instal·lació del servidor Windows 2012 Server

3.1. Instal·lació

Abans d'instal·lar el Windows Server 2012 hi ha uns quants paràmetres que s'han de decidir sobre el procés d'instal·lació. A continuació repassem els més importants.

3.1.1. Triar l'origen de la instal·lació

El Windows Server 2012 es pot instal·lar des del CD-ROM/DVD si el BIOS de l'ordinador admet l'arrencada des d'una unitat de disc compacte. Si no, cal iniciar la instal·lació des dels disquets d'arrencada. Una altra possibilitat de fer la instal·lació és per la xarxa, tot i que serà considerablement més lent, ja que s'hi han de passar tots els fitxers, que en alguns casos podria estar en producció i, per tant, donant servei a altres servidors i clients.

3.1.2. Procés d'instal·lació

Amb aquesta versió del sistema operatiu Windows s'ha minimitzat molt la interacció amb el procés d'instal·lació. Bàsicament, ara el procés demana l'idioma en què es vol instal·lar el sistema, en el cas de tenir una versió multilingüe, i el tipus de teclat que es té instal·lat en la màquina, per a entrar ja directament en el procés d'instal·lació pròpiament de tots els fitxers necessaris. Un cop s'hagi introduït el número de llicència corresponent a la versió que es vol instal·lar, de les quatre en què es distribueix el sistema operatiu, es passa a la primera decisió més important que s'ha de prendre, ja que es pot instal·lar el sistema operatiu Windows Server 2012 de dues maneres molt diferents, tot i que *a posteriori* es poden canviar i passar d'una a l'altra amb certa facilitat. Així doncs, tenim dues possibilitats:

1) Windows Server 2012 Standard (*Server Core Installation*)

2) Windows Server 2012 Standard (*Server with a GUI*)

Descriurem ara molt breument les diferències més important que hi ha entre les dues instal·lacions.

3.1.3. *Server Core Installation*

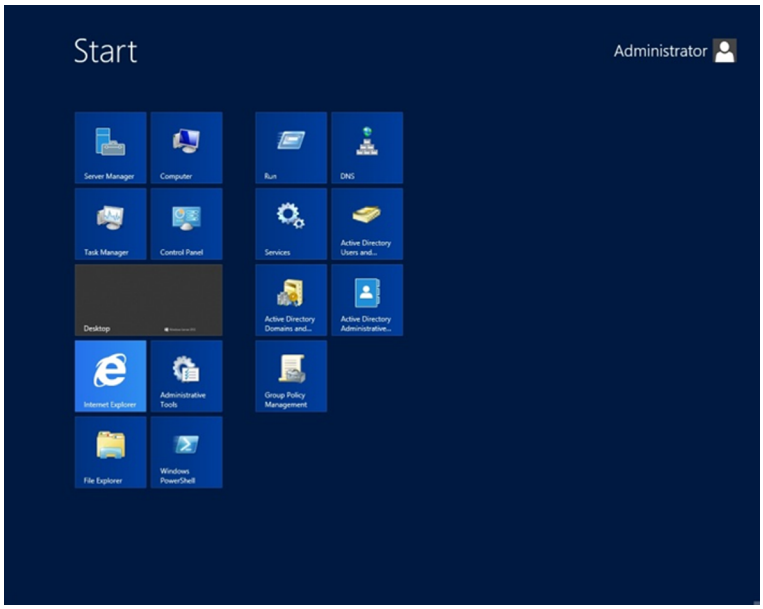
En aquest cas el sistema que s'acaba instal·lant no disposa de cap interfície gràfica, un cop s'entra al sistema per treballar-hi s'obre una consola i tot s'ha de fer des de la línia d'ordres amb el nou intèrpret Power Shell.

Aquesta modalitat permet disposar de sistemes que ocupen molt poc disc, la instal·lació del sistema operatiu no té res més que el necessari per a funcionar i donar servei a tot el que es vagi configurant. En un principi no hi ha cap servei o programa complementari del sistema operatiu, és a dir, que s'haurà d'incloure tot allò que sigui necessari per a treballar amb aquest servidor. A part de la localització del disc on es vol fer la instal·lació, no es demana res més, per la qual cosai s'obté una instal·lació molt ràpida i senzilla completament funcional.

3.1.4. *Server with GUI*

Al contrari, en el segon cas, la instal·lació també introdueix en el sistema tota la interfície gràfica a la qual s'està més acostumat amb tots els sistemes operatius de la família Windows. Més concretament, la nova interfície anomenada Metro, que es va iniciar en els dispositius mòbils que portaven el Windows Phone 7. La figura següent mostra un exemple de què queda després d'instal·lar el sistema i alguna aplicació.

Nova interfície Metro del Windows



3.1.5. Planejar particions de discos

Durant el procés d'instal·lació del Windows Server 2012, a part de l'idioma en què es vol configurar el teclat i el sistema, es pot seleccionar on es vol instal·lar el Windows Server 2012. Això vol dir que es poden crear particions específiques per a instal·lar-lo en un disc més gran, amb altres sistemes o directament en tot els discos durs. L'instal·lador crearà una partició petita, d'uns quants megabytes, per temes d'administració del sistema, que serà inaccessible des del sistema operatiu. Per tant, a l'hora de fer la instal·lació s'ha de tenir en compte que la mida que se li posi es veurà una mica afectada, encara que amb els discos de què actualment disposem no afectarà gairebé res en la capacitat. És recomanable fer servir una partició relativament petita per a instal·lar el sistema operatiu i les poques aplicacions que es poden fer servir des del servidor i deixar una partició molt més gran per a fer-la servir de disc d'usuaris, si és un servidor dedicat a fer de servidor de fitxers, o per a tenir els fitxers d'una pàgina web, etc. D'aquesta manera serà molt més fàcil l'administració de tot el servidor, ja que es disposaran completament separades les dades i el sistema. Des del procés d'instal·lació es pot assignar una petita part per al sistema, fent una partició i instal·lant-hi el sistema, i posteriorment des de l'administrador de discos de què disposa el Windows Server 2012 configurar la resta de particions que siguin necessàries. El funcionament d'aquest particionador del disc dur i l'administrador de discos és força senzill i intuïtiu i queda fora del contingut d'aquests materials.

Web recomanat

En la pàgina següent hi ha més informació sobre planificació de particions i sobre la instal·lació del sistema operatiu de Windows.

http://technet.microsoft.com/es-es/library/jj134246.aspx

3.1.6. Sistema d'arxius

Ja des de la versió Windows Server 2008, el sistema de fitxers que implementen aquests sistemes operatius és l'NTFS, i deixa de banda el FAT i FAT32 com a natius per a poder instal·lar el sistema. Encara que pot llegir els discos externs portàtils i les memòries USB que es puguin fer servir, ja que segur que aquests formats es continuen utilitzant en algunes d'aquestes memòries externes.

Aquesta decisió ja va comportar un gran salt en temes de seguretat, ja que no permetia que un servidor tingués un sistema de fitxers sense seguretat com són FAT i FAT32, però per compatibilitat amb un sistema ja molt antic en les versions anteriors es permetia poder fer servir aquests sistemes de fitxers.

El procés d'instal·lació continua formatant la partició si fos necessari, és a dir, en el cas que s'hagi fet una nova partició, i copia els arxius necessaris per a la instal·lació en el disc. Una vegada acabades aquestes operacions, el programa d'instal·lació reinicia per primera vegada el servidor per acabar definitivament la instal·lació.

Després de reiniciar per primera vegada, es llança la instal·lació en el mode gràfic, per a ultimar les tasques d'instal·lació i finalment, sense cap més pregunta, tindrem ja instal·lat el sistema.

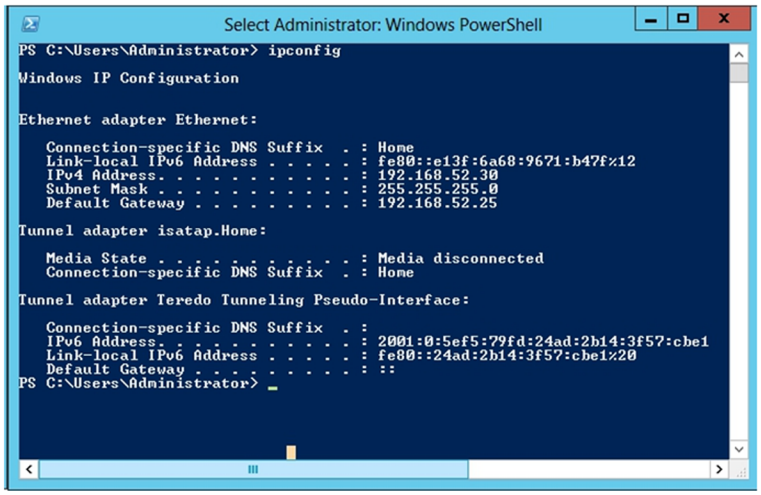
3.1.7. Primeres modificacions

Un cop reiniciat el sistema, ja és completament operatiu, tot i que no disposarà de cap paper de servidor, ja que per defecte no en té cap de preinstal·lat.

El primer que hem de fer és configurar els paràmetres de la xarxa, que per defecte els agafarà per DHCP, i en un servidor això no és el més adient, ja que podríem tenir problemes a la llarga si el servidor d'adreces IP canvia per algun motiu l'adreça del servidor. Tots els clients deixarien de tenir accés al servidor automàticament.

Per a canviar l'adreça IP del servidor només cal obrir el tauler de control i configurar correctament els paràmetres del protocol IPv4 o IPv6, depenent de la configuració de xarxa que es tingui en cada institució. En aquest cas val a dir que, tot i que no s'assigni una IP al protocol IPv6, el Windows Server 2012 convertirà l'adreça que s'introdueixi en el protocol d'IPv4 a IPv6. De manera que, internament, sobre la xarxa interna, es treballarà sempre sobre IPv6. Això ho podem veure en l'ordre `ipconfig`, en la figura següent, en què es pot veure com, tot i tenir només assignada l'adreça IPv4, també en té una de configurada per a IPv6 que fa servir per a la xarxa Microsoft que pugui crear dins de l'organització.

Configuració IPv4 i IPv6



La cosa important següent que s'ha de fer és canviar el nom del servidor i posar-lo en un domini si cal, ja que per defecte el procés d'instal·lació en donarà un d'aleatori que no servirà per a poder identificar ràpidament el servidor dins de l'organització.

El nom i el domini es poden canviar en el tauler de control, dins la categoria de propietats del sistema. Ara s'ha de triar el nom de l'equip, que és una seqüència de caràcters que identifica el servidor dins d'un domini o grup de treball. És important, per tant, no utilitzar cap nom d'equip que ja es faci servir. És útil assignar noms als equips que ens recordin la funcionalitat que tenen. Per

exemple, *BD_Central* o *BD* pot ser el nom d'equip per al servidor que emmagatzemi les bases de dades de l'organització, i *Website* pot ser el servidor que contingui el lloc web de l'organització.

En el cas que el servidor que estiguem instal·lant tingui el paper de servidor de domini, ja que l'instal·lem posteriorment, no cal que se li assigni un nom de domini de la xarxa, ja que l'agafarà directament del paper que es configuri posteriorment. En el cas de pertànyer a una xarxa ja establerta, sí que s'haurà d'incloure en la xarxa reescrivint el nom del domini.

D'altra banda, la contrasenya de l'administrador és un punt important amb vista a la seguretat del servidor. De vegades, quan es fan proves en un ordinador personal, se sol ometre aquesta contrasenya per comoditat, però un servidor en producció ha de tenir assignada una contrasenya d'administrador per a evitar intrusions en el sistema. I aquesta contrasenya només l'han de saber les persones que tinguin drets d'administració sobre aquest servidor.

Un altre factor que s'ha de tenir en compte a l'hora d'establir una contrasenya, sigui d'administrador o d'usuari corrent, és que sigui una cadena de lletres i xifres sense sentit, que no estiguin relacionades amb cap dada personal, com la data de naixement, el nom o cognoms, etc. A més, és recomanable no apuntar la contrasenya en cap paper o mitjà digital, i canviar-la sovint, per evitar que la descobreixin.

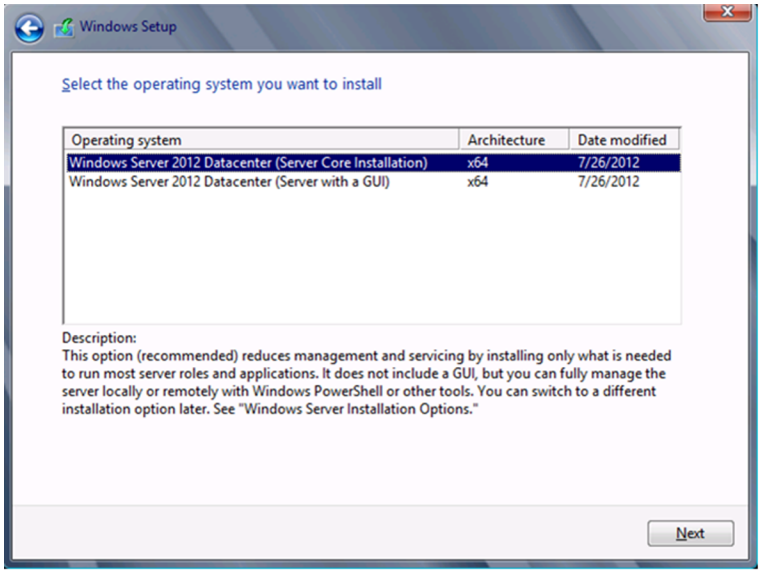
El Windows Server 2012 introdueix un sistema de qualitat de contrasenya per defecte que ens avisa en cas que la que hem establert sigui feble i ens informa que cal triar-ne una de més segura i ens dóna indicacions sobre quins criteris ha de complir (almenys els dos primers i, com a mínim, tres dels següents):

- Ha de tenir més de vuit caràcters.
- No ha de tenir parts del nom d'usuari a què pertany.
- Ha de tenir alguna lletra en majúscules.
- Ha de tenir alguna lletra en minúscules.
- Ha de tenir alguna xifra.
- Ha de tenir algun caràcter no alfanumèric ($, &, #, etc.).

3.1.8. Instal·lació del sistema Core

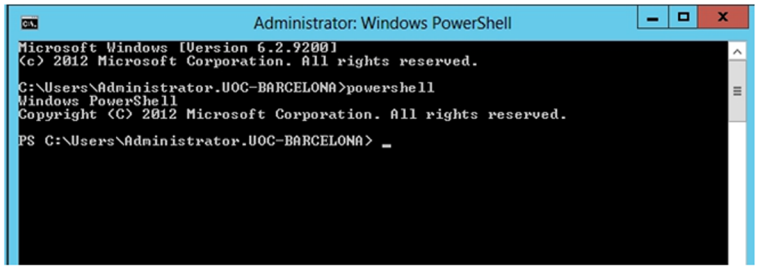
Una de les noves característiques que té el Windows Server 2012 és que permet la instal·lació de tot el sistema en una versió molt reduïda i que un cop instal·lada consumeix els recursos mínims en el sistema operatiu.

Tipus d'instal·lacions del Windows Server 2012



Serà necessari seleccionar l'opció de la instal·lació del Server Core Installation per a tenir al final un sistema tan petit com sigui possible. Únicament disposarà d'una consola d'instruccions per a interactuar amb l'administrador, tot i que des d'aquesta es pot cridar el nou intèrpret anomenat *Power Shell*, en el qual es poden fer moltes més coses que amb l'antiga consola d'ordres, i que a més ens permetrà configurar completament tot el sistema, mostrada a la figura següent. Permet des de configurar la xarxa, instal·lar nous papers, configurar-los, etc.

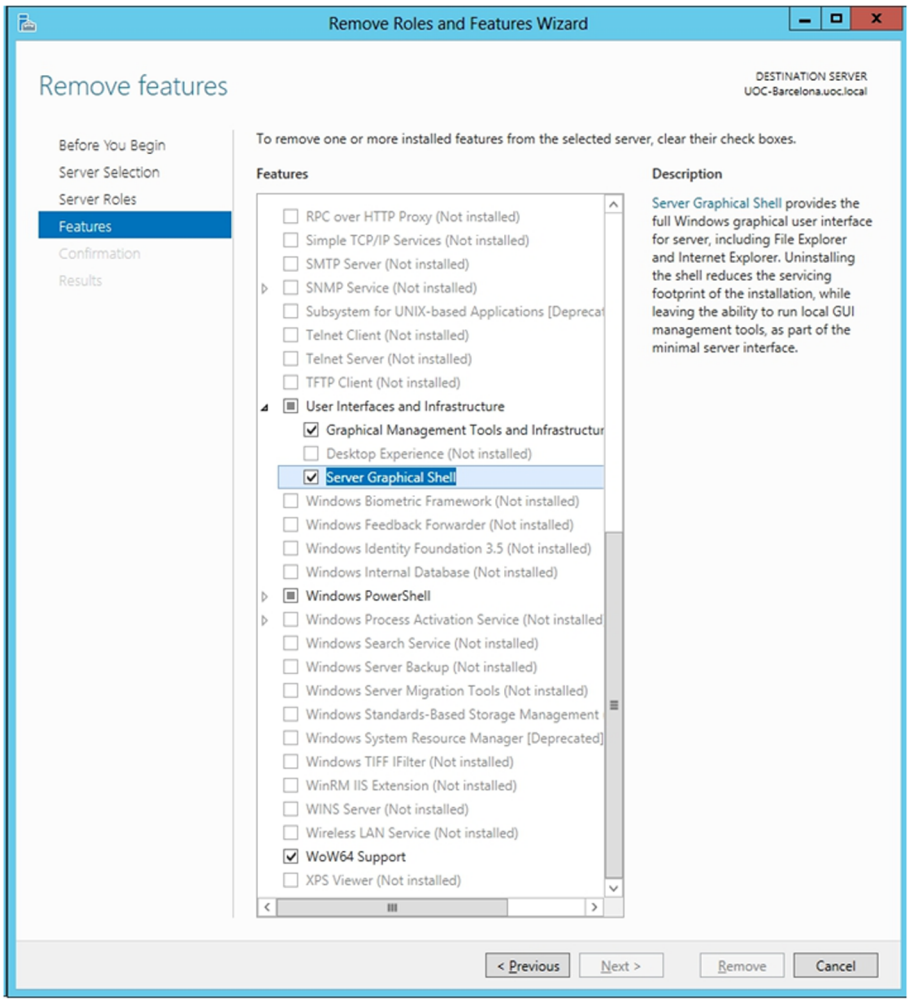
Consola d'instruccions i Power Shell



També es pot passar d'un sistema a un altre un cop instal·lat i configurat, per la qual cosa sempre serà més còmode instal·lar la versió completa, amb la interfície gràfica, configurar-ho tot, instal·lar tots els papers, característiques, usuaris, polítiques de seguretat, etc., i després passar a la versió Core per tal de fer el sistema molt més ràpid i segur.

Per a passar de la versió GUI a la versió Core cal desinstal·lar una de les característiques que s'instal·len per defecte en aquesta versió. Per a fer això caldrà obrir l'administrador del servidor i en la configuració entrar en l'eina de desinstal·lar papers i característiques. Aquí cal eliminar del sistema la característica d'*Infraestructura i interfície d'usuari*, tal com mostra la figura següent. S'hauran d'eliminar completament totes les subcaracterístiques que té.

Característica d'infraestructura i interfície d'usuari



En reiniciar el sistema, ja no apareixerà la interfície d'usuari que apareix per defecte, i el sistema serà únicament accessible mitjançant la consola d'ordres.

Podem tenir una versió intermèdia entre la versió Core i la GUI, en la qual es disposarà de la versió Core, però amb una interfície gràfica mínima per a algunes eines del sistema. Això ho aconseguirem eliminant únicament el servidor d'ordres gràfiques que està seleccionat en la figura anterior.

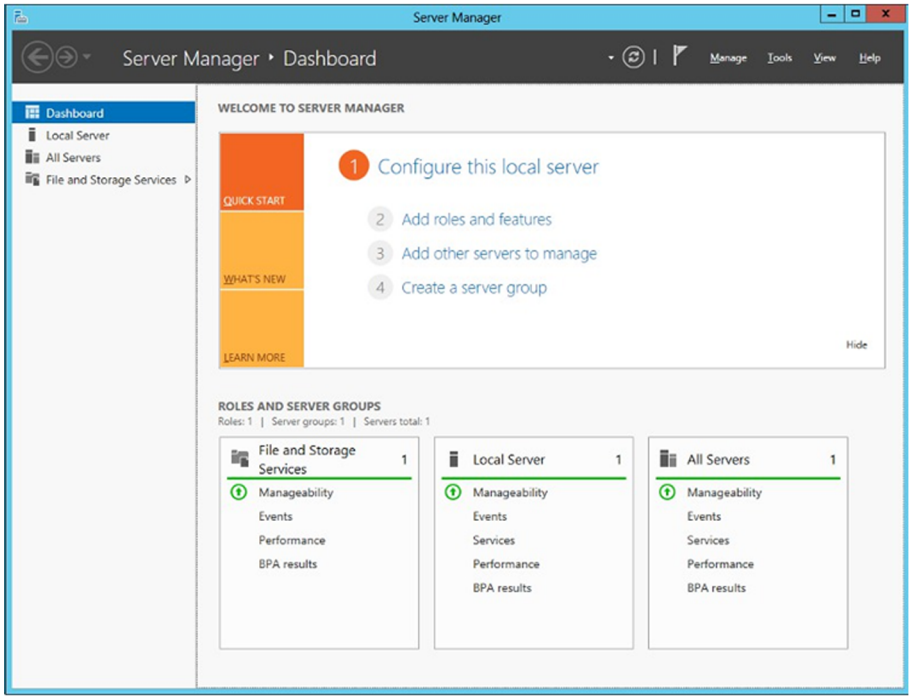
També es pot passar de la versió Core a la versió GUI, instal·lant pas per pas la interfície a partir del disc d'instal·lació del Windows Server 2012 i la línia d'ordres. Aquests passos es poden trobar en l'adreça: http://technet.microsoft.com/en-us/library/hh831786.

3.2. Configuració del servidor

Una vegada instal·lat el sistema operatiu, podem canviar alguns paràmetres dels diferents serveis del servidor per configurar-ne el comportament.

En arrencar el sistema, el Windows Server 2012 ja ens obre una finestra en què podem configurar tot el necessari, i fins i tot hi ha una guia inicial de què és el que s'ha de fer.

Tasques inicials d'administració



Des d'aquesta pantalla es pot anar al primer enllaç, en què hi ha la configuració inicial del servidor, i des d'on es poden tenir totes les característiques del servidor completament controlades.

Des d'aquesta mateixa pantalla es pot crear un grup de servidors que estiguin tots en la mateixa empresa i que formaran part del directori actiu del servidor. D'aquesta manera es podran gestionar remotament tots els servidors, sense haver d'anar-hi físicament o mitjançant el protocol RDP (l'escriptori remot). Així, des d'aquest administrador podem gestionar tota la xarxa de servidors a la vegada i, per tant, tenir una visió molt més acurada del que està passant en tota la xarxa. Anirem afegint els papers i característiques als diferents servidors des d'un únic punt de gestió.

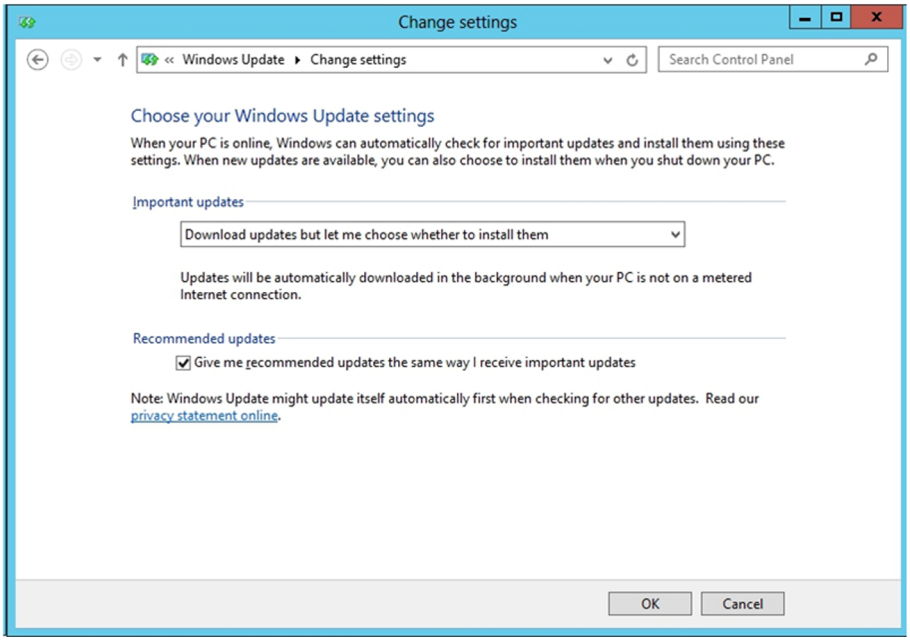
Una altra de les coses que s'han de fer des d'un bon principi és configurar el servidor perquè s'actualitzi correctament. I això es fa mitjançant les actualitzacions periòdiques que fa Microsoft, que cada segon dimarts de mes envia les correccions per mitjà del sistema d'actualitzacions automàtiques. És important tenir una bona política d'actualitzacions i saber en tot moment què és el que es vol actualitzar. En sistemes en què hi pot haver programari de tercers o és

molt crític el funcionament dels servidors, abans d'aplicar una actualització és important documentar-se de què pot afectar, quins altres programes afecta, i què fa al sistema. Ens podríem trobar amb actualitzacions que modifiquin una DLL o una API del sistema, i això faria que un programari fet a mida que hi accedeix a deixi de funcionar.

En alguns casos en què el funcionament del sistema és molt important, les actualitzacions es fan en horari fora de la jornada normal de treball per a poder tornar enrere en el cas que passi el que s'ha comentat abans. O si és el cas, que una actualització demani reiniciar el servidor.

Per tant, és important configurar el sistema d'actualitzacions perquè no instal·li els nous components quan el sistema vulgui sinó que l'administrador decideixi quan i quines actualitzacions es fan. La millor opció és configurar-lo de manera que ens pregunti quines actualitzacions es volen baixar si tenim programari que interactua amb API del sistema que poden ser canviades, i que puguem dir quan s'instal·len, i poder reiniciar el sistema quan sigui més adient. La figura següent mostra una configuració típica d'aquestes polítiques d'actualitzacions.

Configuració del Windows Update



3.2.1. Canvi del nom

El primer que caldrà fer en arrencar per primer cop el sistema després de la instal·lació és canviar-li el nom, ja que en posa un d'aleatori. Això es fa en el tauler de control, i dins de Sistema i seguretat es troba l'enllaç per a poder fer el canvi de la configuració del nom.

En aquest pas s'ha de decidir quina política de noms es fa servir, ja que el nom de cada equip l'hauria de diferenciar i identificar ràpidament. Un nom com `servidor1` no ens aportarà informació si des de la xarxa veiem aquest nom, però si li posem un nom com `S1DNS`, `S1HTTP` o `S1Files` sabrem ràpidament que es tracta del servidor 1 i que està dedicat a les tasques de resolució de noms, de pàgines web, de servidor de fitxers, etc. Això, que pot ser útil per als administradors de sistemes, es pot tornar en contra en el cas de la seguretat, ja que ràpidament un atacant (intern o extern) sabrà quines IP estan assignades als servidors més importants. Per tant, el que sembla més raonable és tenir una codificació pròpia a l'hora d'assignar els noms, i que si es coneix aquesta codificació sigui ràpid saber què fa cada servidor.

3.2.2. Activació de serveis i protocols de xarxa

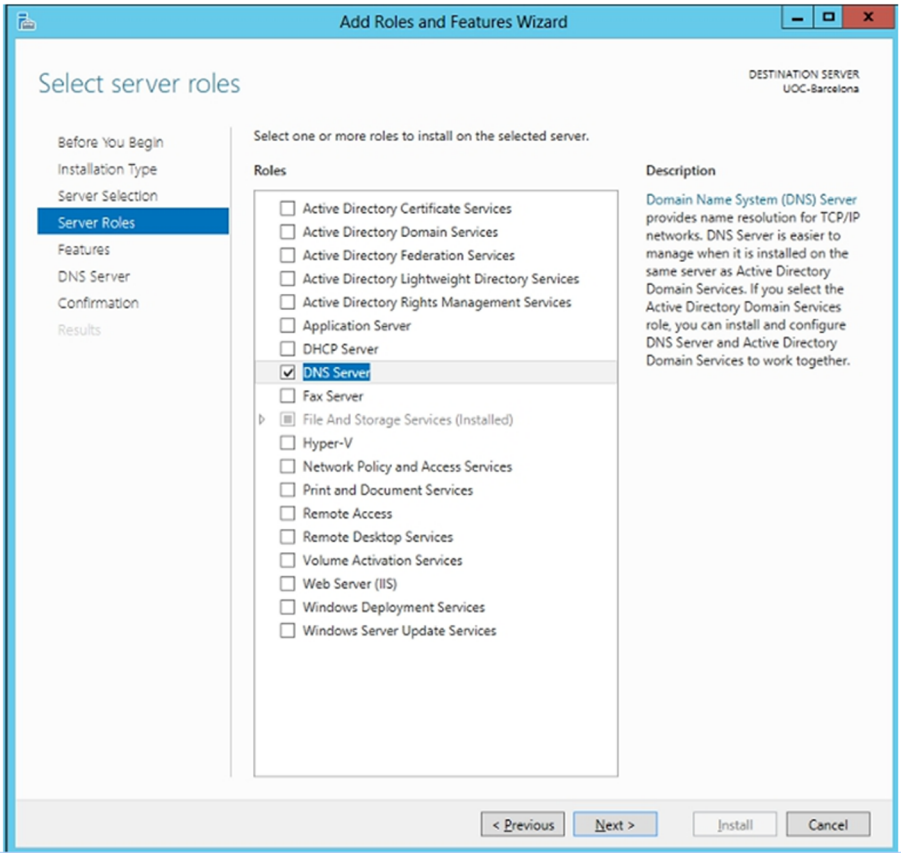
Un cop tenim el nom assignat al nou servidor, només cal fer la configuració dels paràmetres de xarxa. Podem configurar els paràmetres de xarxa mitjançant l'opció Connexions de xarxa del tauler de control. Aquí serà important donar una IP fixa al servidor, ja que podríem tenir problemes després si ho tenim per defecte, tal com es queda després de la instal·lació fent servir el *dynamic host configuration protocol* (DHCP). En la finestra de connexions de xarxa hi ha totes les connexions configurades en el sistema. A més, hi podem afegir connexions noves o eliminar-ne de les que ja hi ha. Per a configurar una connexió de xarxa podem utilitzar l'opció Propietats del menú contextual que surt en fer clic amb el botó secundari del ratolí damunt de la icona de la connexió. En obrir la finestra de propietats de la connexió, veiem els diferents serveis i protocols instal·lats. Per a instal·lar i configurar altres serveis o protocols fem clic sobre Instal·lar i ens surten els protocols disponibles. Rarament s'haurà d'incloure un nou protocol de comunicació, però en xarxes antigues sí que es podria donar el cas. També podem configurar un protocol o servei que ja hi ha instal·lat mitjançant el botó Propietats. Per exemple, per configurar l'accés a Internet del servidor, hem de modificar les propietats del protocol TCP/IP. En la finestra de propietats de TCP/IP podem modificar la IP del servidor, de manera que quedi fixada, i les IP dels servidors de DNS (noms de domini). En aquest cas, dels DNS, i per tal de poder configurar després el servidor com a servidor de domini i poder tenir el directori actiu (*active directory*), haurem de posar en el DNS primari el *localhost*, és a dir, l'adreça 127.0.0.1, i com a secundari, o un altre servidor DNS de suport de què es disposi, o els DNS que hagi subministrat el proveïdor d'Internet que es tingui contractat.

3.2.3. Papers del servidor

Com ja s'ha introduït en el Windows Server 2008, el sistema operatiu Windows Server 2012 està compost de papers que s'han d'anar seleccionant i instal·lant en el sistema. Aquests papers són les funcionalitats que es vol donar al sistema, ja que per defecte, després de la instal·lació el sistema no farà res més que un sistema d'escriptori, ja que no té cap característica addicional instal·lada.

Alguns d'aquests papers es mostraran posteriorment, però els més usuals són el de l'AD (*active directory*), el DNS (*domain name server*), el de *web server* (IIS), etc. La figura següent mostra els possibles papers que es poden instal·lar en el sistema.

Llista dels papers del Windows Server 2012



El primer que s'ha de fer és instal·lar el servidor de DNS, per a poder fer després la resolució interna de noms dins la xarxa d'ordinadors client que es connectaran al servidor de domini; sense aquest DNS no es podria fer la resta de coses i configurar i fer segur l'entorn d'una manera centralitzada i segura. Només cal instal·lar el paper, seguir les instruccions i ja es disposa d'un DNS local. Apareixerà a la interfície Metro l'enllaç a la configuració del DNS. Ara haurem de crear en l'administrador de DNS una nova zona per a poder-la incloure després en el directori actiu.

3.2.4. Protocols i sistemes d'autenticació d'usuaris

El Windows Server 2012 té un sistema d'inici de sessió únic, en el qual l'usuari inicia sessió en el domini una sola vegada mitjançant una única contrasenya o targeta intel·ligent i després pot accedir a tots els recursos a què té accés sense haver de reescriure la contrasenya o requerir-ne una de diferent per a cada equip del domini. L'autenticació d'usuaris en el Windows Server 2012 consta de dues fases: l'inici de sessió interactiu i l'autenticació de xarxa.

1) Inici de sessió interactiu

Kerberos V5-1.11 constitueix el protocol de seguretat principal per a l'autenticació dins d'un domini. El protocol Kerberos V5 comprova la identitat de l'usuari i els serveis de xarxa.

L'inici de sessió interactiu comprova les dades d'identificació de l'usuari en un compte de domini (accés a qualsevol recurs del domini) o en un equip local (accés solament als recursos de l'equip local). En iniciar sessió, l'usuari introdueix les credencials o utilitza una targeta intel·ligent per a tenir accés al sistema. Si el compte és de domini, es fa servir el protocol Kerberos V5 per a l'autenticació, o Kerberos V5 amb certificats si s'utilitza una targeta intel·ligent. En cas d'inici de sessió en un compte local, les credencials de l'usuari es comproven amb les dades emmagatzemades en l'administrador de comptes de seguretat (SAM).

2) Autenticació de xarxa

Mitjançant l'autenticació de xarxa s'identifica un usuari en qualsevol servei de xarxa a què intenti accedir. En aquest procés d'autenticació s'utilitzen protocols com Kerberos V5, nivell segur de sòcols (*socket*), o seguretat del nivell de transport (SSL/TLS). Per als usuaris d'un compte de domini, el procés d'autenticació és automàtic (inici de sessió únic). En canvi, els usuaris de comptes locals (usuaris de la màquina local, no del domini) han de proporcionar les credencials cada vegada que volen tenir accés a un recurs de xarxa.

Web recomanat

Trobareu més informació sobre protocols d'autenticació d'usuaris del Windows Server 2012 en l'adreça següent:
http://technet.microsoft.com/en-us/library/hh831747.aspx

3.2.5. Configuració d'un servidor de domini Windows. Paper del Directori actiu

Un servidor de domini consisteix en un servidor de la xarxa que permet controlar tots els equips i dispositius que en formen part, de manera que un usuari pugui accedir al domini i entrar en els equips en què està autoritzat, introduint la contrasenya una sola vegada. El controlador de domini permet centralitzar l'administració i seguretat d'una xarxa.

Què és un domini?

Un domini consisteix en un grup d'equips que formen part d'una xarxa i comparteixen una base de dades de directori comuna. Els dominis s'organitzen en nivells i s'administren com a unitats amb regles i procediments comuns. Cada domini té un nom únic.

Per a configurar el servidor com un controlador de domini, cal instal·lar el paper de Directori actiu, que emmagatzema informació sobre els objectes de la xarxa i facilita la cerca i utilització d'aquesta informació als usuaris i administradors.

El directori actiu utilitza un magatzem de dades estructurat com a base per a una organització lògica i jeràrquica de la informació del directori. Aquest magatzem de dades, anomenat també *directori*, conté informació sobre els objectes de directori actiu, els quals solen incloure recursos compartits com servidors, volums, impressores, comptes d'usuari de xarxa o comptes d'equip, al

mateix temps que permeten als usuaris i a les aplicacions accedir als recursos. Alhora, proporcionen una manera coherent d'assignar noms, de descriure, localitzar, obtenir accés, administrar i protegir la informació d'aquests recursos.

El directori actiu és una implementació dels protocols de noms i directoris estàndard d'Internet (X.500 i LDAP). Utilitza un motor de bases de dades per a processar les transaccions i, a més, és compatible amb diversos estàndards d'interfícies de programació d'aplicacions.

La seguretat està integrada en el directori actiu mitjançant l'autenticació de l'inici de sessió i el control d'accés als objectes del directori. Amb un únic inici de sessió en la xarxa, els administradors poden administrar dades del directori i de l'organització en qualsevol punt, i els usuaris autoritzats poden tenir accés a recursos en qualsevol lloc. L'administració basada en directives facilita la tasca de l'administrador fins i tot en les xarxes més complexes.

Web recomanat

En l'URL següent hi ha informació extensa sobre el directori actiu, les funcionalitats que té, com està organitzat, la seguretat, etc.:

http://technet.microsoft.com/en-us/library/hh831484.aspx

1) Configuració de DNS

De manera predeterminada, i en el cas que no s'hagi instal·lat prèviament, l'assistent per a instal·lació del directori actiu intenta situar un servidor DNS autoritzat en el nou domini, a partir de la llista de servidors DNS configurats que admetran una actualització dinàmica d'un registre de recursos de servei (SRV). Si en troba, tots els registres adequats per al controlador de domini es registren automàticament amb el servidor DNS, una vegada reiniciat el controlador de domini. Si no troba cap servidor DNS que accepti actualitzacions dinàmiques, sigui perquè el servidor DNS no hi és compatible o perquè no estan habilitades per al domini, l'assistent per a la instal·lació del directori actiu segueix els passos següents per assegurar que el procés d'instal·lació es completa amb el registre necessari dels registres de recursos SRV:

- El servei DNS s'instal·la en el controlador de domini i es configura automàticament amb una zona basada en el domini del Directori actiu. És a dir, si no està instal·lat prèviament l'instal·la en el procés de la instal·lació del directori actiu.

- Per exemple, si el domini que va triar per al primer domini del bosc dels directoris actius (ja es veurà què vol dir en el moment d'instal·lar el directori actiu) era exemple.microsoft.com, s'agrega una zona l'arrel de la qual és en el nom de domini DNS d'exemple.microsoft.com i es configura per a utilitzar el servei de servidor DNS en el nou controlador de domini.

- Es crea un arxiu de text que conté els registres de recursos DNS adequats per al controlador de domini. L'arxiu `Netlogon.dns` es crea en la carpeta `arrelSistema\System32\Config` i conté tots els registres necessaris per a guardar els registres de recursos del controlador de domini. El servei NetLogon utilitza `Netlogon.dns`, que admet directori actiu en els servidors DNS que no executen el Windows Server 2012. Si utilitza un servidor

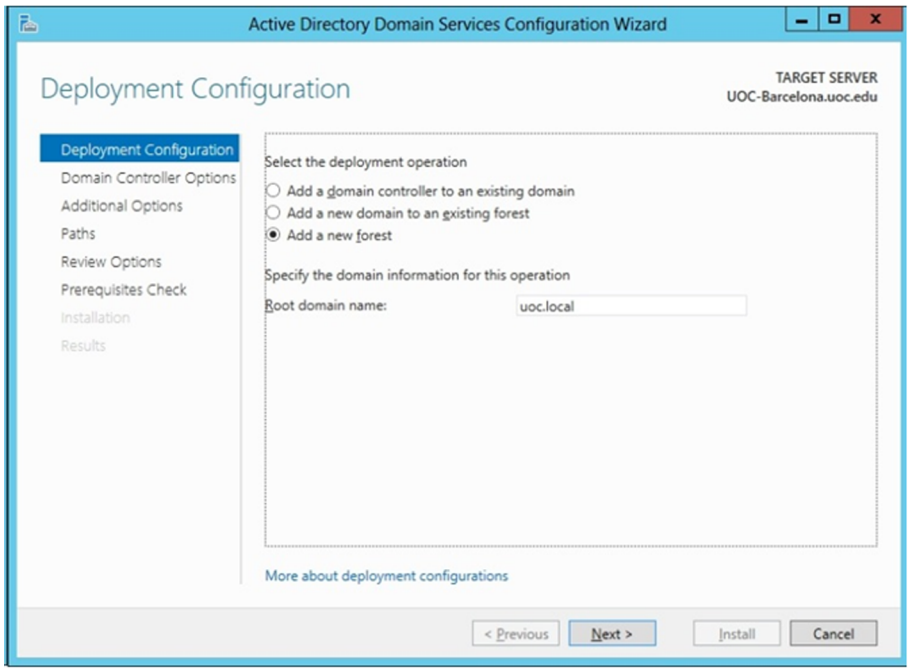
DNS que admet el registre de recursos SRV però que no admet actualitzacions dinàmiques, pot importar els registres de `Netlogon.dns` a l'arxiu de la zona principal adequada amb la finalitat de configurar manualment la zona principal en aquest servidor perquè admeti directori actiu.

Si no hi ha servidors DNS disponibles en la xarxa, es pot optar per instal·lar i configurar manualment un servidor DNS local, quan s'instal·li el directori actiu amb l'assistent per a instal·lar-lo. O instal·lar-lo abans i configurar-lo perquè funcioni després correctament amb el directori actiu. El servidor DNS s'instal·la en el servidor en què s'executa l'assistent i les opcions del servidor DNS preferit es configuren perquè utilitzi el nou servidor DNS local. S'ha de tenir en compte que més endavant haurem de configurar totes les estacions de treball i servidors membres del domini amb el client de DNS configurat contra el nostre nou servidor de DNS. En cas contrari, no serem capaços de trobar el domini ni els recursos que té. Després és recomanable configurar els "reenviadors" o *forwarders* del servidor de DNS amb els servidors DNS del nostre proveïdor d'Internet.

2) Instal·lació del directori actiu

Podem instal·lar ara el directori actiu des de la finestra de configuració del servidor, incloent-hi el nou paper d'aquest. Només cal, doncs, seleccionar el nou paper i instal·lar-lo en el sistema. Un cop fet tot el procés, l'administrador del servidor avisa amb una notificació que s'ha de promoure el nou paper de directori actiu controlador de domini. Entrant directament a l'enllaç s'obrirà l'administador, on podrem donar un nom al controlador de domini, en aquest cas `uoc.local`, tal com es pot veure en la figura següent.

Nou bosc de directori actiu

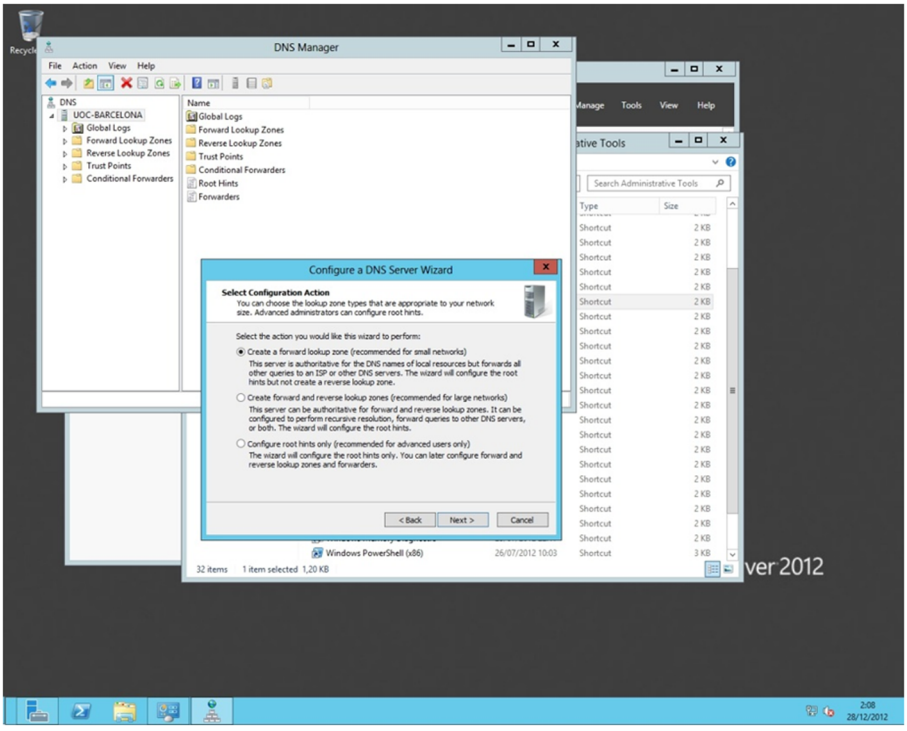


Segueix la instal·lació amb la contrasenya del domini i la compatibilitat que es vol tenir; si es vol més compatibilitat amb altres sistemes operatius de Microsoft més antics, s'haurà de seleccionar Windows 2003 Server o 2008 Server. Evidentment, pel que fa a seguretat, el millor és seleccionar el darrer, el Windows Server 2012, ja que té les darreres característiques que s'han dissenyat específicament per a aquest sistema, i disposa de més seguretat que la resta de configuracions possibles. Continua amb algunes característiques més sobre ubicacions de fitxers i opcions, i la contrasenya de l'administrador del domini, que pot ser diferent de la contrasenya de l'administrador local del Windows Server 2012.

Un cop ja tenim acabada la configuració del directori actiu, es reiniciarà la màquina i ja es podrà veure la pantalla d'entrada, ara ja mitjançant el nou domini, ja que ens demana un usuari legítim del domini, que en el cas de l'administrador seria `UOC\administrador`.

El pas següent que s'ha de fer és la vinculació del servidor DNS amb el directori actiu, i així fer que els ordinadors client de la xarxa puguin veure el servidor del directori actiu i vincular-s'hi i, per tant, validar-se contra el domini nou que s'ha creat. Això es fa ràpidament obrint l'administrador del servei de DNS i executant l'assistent de configuració. Per a una petita empresa la primera opció ja és suficient, com en la figura següent.

Configuració DNS amb assistent



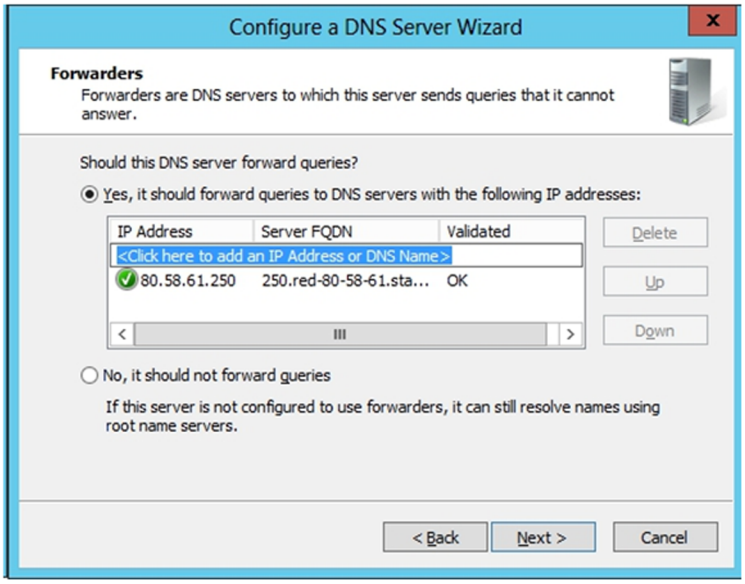
A continuació ens demanarà un nom per al servei i li'n podem posar un de semblant a `dns.uoc.local`, que és el que teníem ja assignat al domini del directori actiu com a `uoc.local`. Posteriorment, només cal seleccionar l'opció d'actualització segura a partir del directori actiu i així ens assegurarem que no s'actualitza el DNS de fonts insegures i serà més difícil rebre un atac de *DNS spoofing*.

DNS spoofing

Es tracta d'una tècnica relativament nova, en la qual un atacant envia al servidor de noms una relació de nom de domini - IP falsa. Així fa que una petició al nom del domini en el navegador d'Internet faci que en lloc d'anar a l'adreça IP real de la pàgina web vagi a una de falsejada preparada per l'atacant i que és idèntica a la pàgina bona. L'atac es pot dur a terme en fer aquestes actualitzacions si permetem que el nostre servidor s'actualitzi des de sistemes no controlats.

Per acabar només cal indicar-li on ha de fer les consultes en el cas que no pugui resoldre per ell mateix l'adreça real d'Internet. Només caldrà indicar-hi un servidor de DNS que la ISP ens hagi donat com a vàlid per a la connexió a Internet que es tingui contractada.

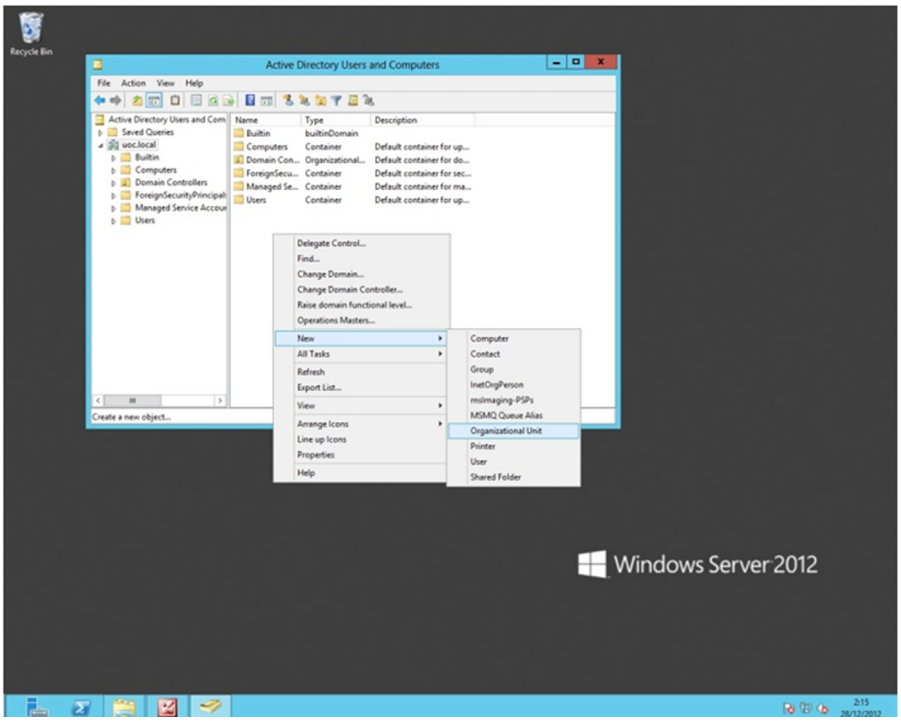
Configuració del DNS



Amb això finalitza la instal·lació dels servidor de manera funcional. A partir d'aquí és necessari anar omplint el directori actiu amb les unitats organitzatives que es vulguin tenir definides, els usuaris que poden o no estar dins aquestes unitats, els grups, els ordinadors, etc.

Les unitats organitzatives les podem assimilar als departaments, edificis, seccions, etc.; ens ajudaran a crear una còpia de l'organització per tal de poder diferenciar o trobar més ràpidament els usuaris. Per exemple, una organització amb dues seus, una a Barcelona i una altra a Madrid, disposaria de dues unitats organitzatives separades per cada seu, i així podríem incloure els usuaris i grups, si es vol, en cada una d'aquestes. Això facilita el canvi en les regles dels ordinadors, ja que si assignem regles generals a les diferents unitats tots els usuaris, grups i ordinadors es veuran afectats, sense haver de fer els canvis un a un.

Estructura del directori actiu, creació d'una unitat organitzativa



Els grups permetran que els diferents usuaris de l'organització, tot i estar en diferents unitats organitzatives, puguin estar agrupats en un grup i tenir tots els privilegis que es puguin assignar a un grup concret. Per exemple, es poden crear grups per a accedir a diferents discos o particions, i així cada grup pot tenir una àrea de fitxers completament diferent de la resta i no veure la informació més enllà del que li pertoca.

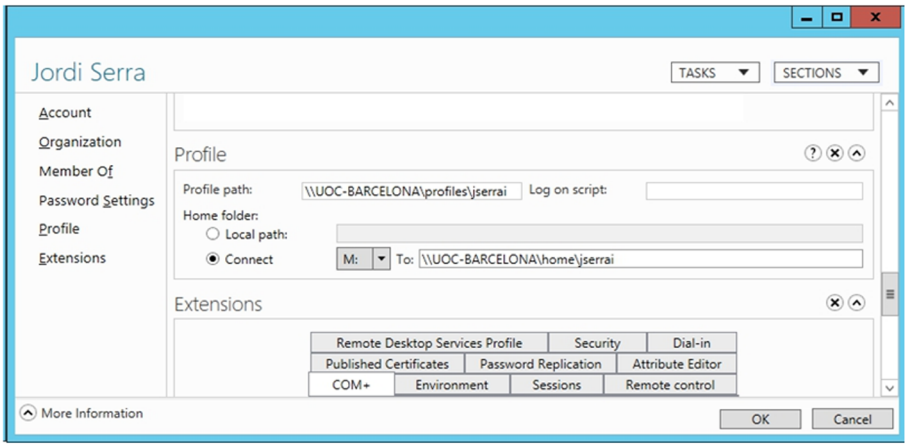
Si ja tinguéssim un servidor de domini en la xarxa, es podria afegir un altre controlador al domini propi. En el cas de l'esquema de directori actiu i dels dominis Windows 2012, tots els controladors de domini són multimàster, que vol dir que tots poden escriure en el directori i crear, actualitzar o esborrar dades alhora. Així, doncs, no hi ha cap controlador de domini en un domini Windows que sigui més important que un altre; tots comparteixen i mantenen replicada la informació del directori, i ofereixen així redundància i tolerància a fallades, a més de balanceig de càrrega en les operacions de domini.

L'organització de dominis del Windows Server 2012 és jeràrquica i podem tenir un esquema lògic de tots els nostres dominis i subdominis en forma d'arbre. Del conjunt d'arbres de domini *se'n diu bosc de dominis*; per tant, aquest nou servidor de domini que es pot instal·lar s'haurà d'afegir al bosc de dominis que s'ha iniciat amb la instal·lació del primer servidor de domini en la xarxa de l'organització.

Per tal de poder connectar i endreçar els fitxers d'usuari i els fitxers dels perfils, cal crear i compartir dues carpetes en algun lloc del sistema de fitxers. Podem crear les dues carpetes a dins el directori `c:\users` que crea el sistema, i compartir-les amb tots els permisos oberts per a tothom, i després ja es tancaran

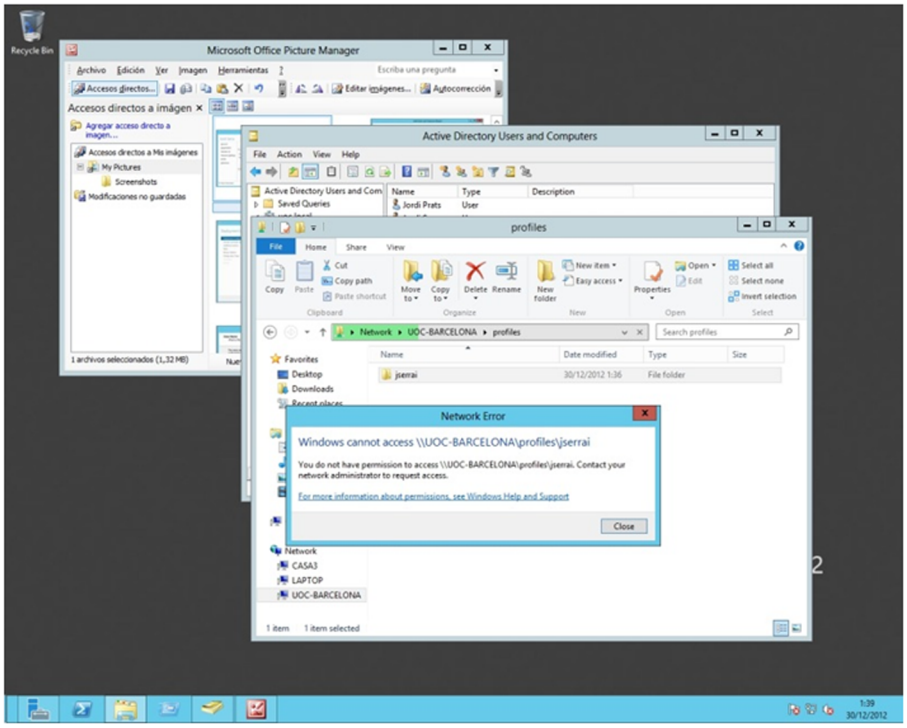
els directoris interns de cada usuari perquè ningú més no pugui tenir accés a aquests directoris personals. Per defecte els perfils no es guarden en el servidor, sinó que són locals en les màquines on es creen, cosa que fa que no es puguin fer amb facilitat les còpies de seguretat dels perfils de cada usuari i que cada usuari estigui més lligat a un únic lloc de treball. Així, per a cada usuari s'haurà de definir on té cada carpeta personal dins les propietats dels usuaris. La figura següent en mostra un exemple.

Configuració de la ruta del perfil i de la carpeta personal



Com veurem més endavant, és important poder fer còpies de seguretat de tot allò que sigui important per a l'empresa i en quasi tots els casos els documents creats per tots els usuaris ho seran, i tenir-los dispersos pels diferents equips no ajudarà a un bon manteniment d'aquests.

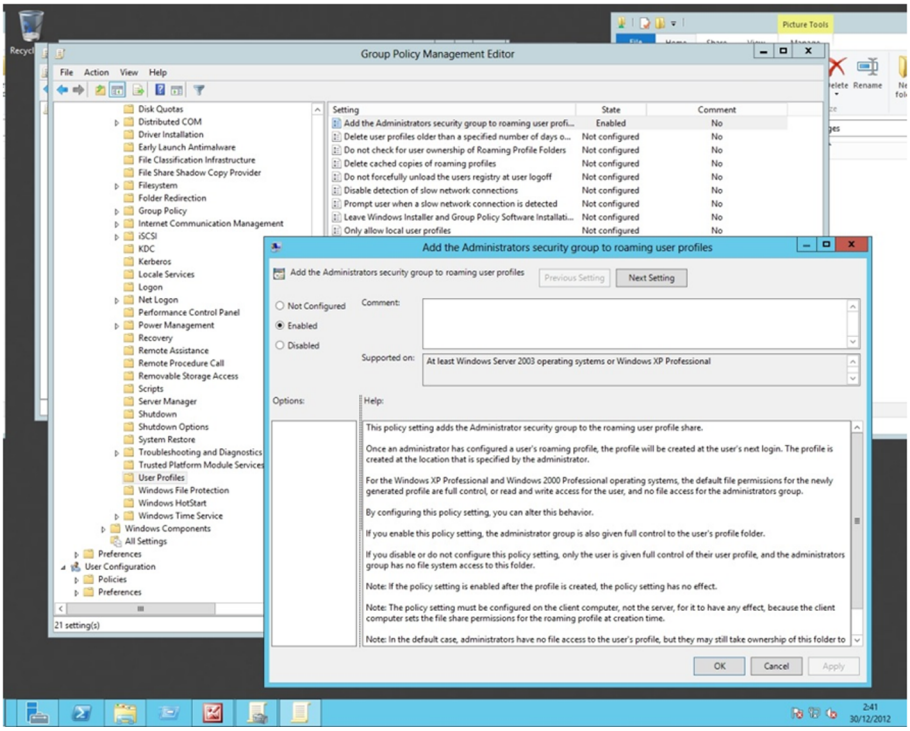
Error en accedir a la carpeta dels perfils d'usuaris



Per defecte, els directoris de cada perfil d'usuari no són accessibles per cap altre usuari que no sigui l'usuari mateix, i per tant, no es poden fer còpies de seguretat d'aquests fitxers tret que es canviï la política d'accés. La figura anterior mostra un exemple de l'error que retorna el sistema.

Per a poder canviar aquesta política, és important que abans de promocionar el servidor de domini, i per tant, abans de definir els usuaris, es configuri l'accés a les carpetes dels perfils d'usuari, o no es podrà fer *a posteriori* i s'haurà de desinstal·lar el servidor de domini per a poder atorgar aquest privilegi a l'administrador. La figura següent mostra com s'han de canviar les polítiques de grup per tal que l'administrador pugui entrar als directoris dels perfils i així poder fer còpies de seguretat d'aquests arxius.

Configuració de l'accés als fitxers del perfil



3) Serveis de certificat

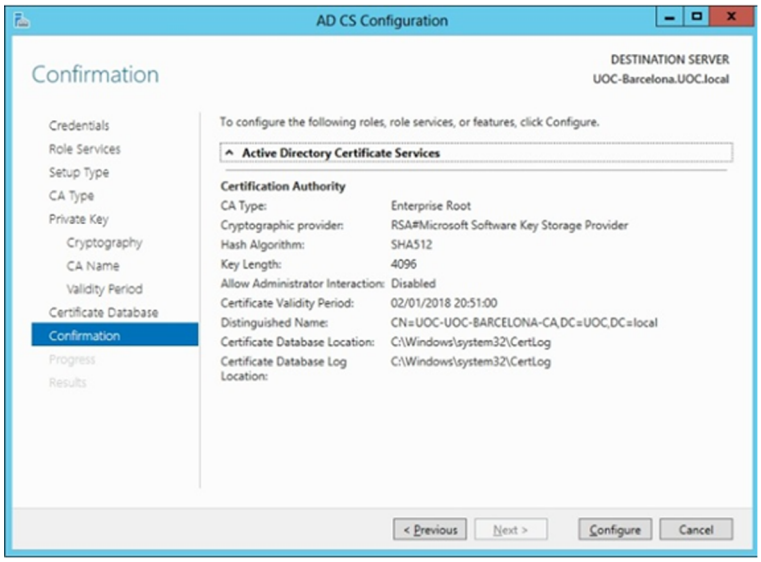
Un altre dels papers interessants que es poden incloure en el servidor són els serveis de certificat, disponible en el Windows Server 2012. Es pot instal·lar en el servidor i ens permetrà emetre i administrar certificats d'infraestructura de clau pública PKI. Així doncs, podrem fer identificacions, signatures digitals i fer transaccions segures.

Un cop instal·lat ens demana que es configuri correctament amb les credencials de l'administrador, i continua amb la configuració de l'entitat de certificació que s'ha de crear dins el servidor. La primera serà de tipus *root* i li hem de dir que és la primera, i per tant s'ha de crear una clau privada nova.

El pas següent és seleccionar les característiques criptogràfiques, que per defecte ja funcionaran bé, tot i que es pot millorar canviant a SHA512. Aquí mai no agafarem MD5 o inferior i no és recomanable fer servir SHA1, ja que podria ser insegur. La longitud de la clau també ens aportarà més seguretat com més gran sigui.

La figura següent mostra la configuració final que serà aplicada al nou paper.

Configuració del servidor de certificats



4) Serveis de gestió de drets (RMS)

A més de poder protegir els documents amb els permisos associats als fitxers, a les carpetes, als usuaris i als grups, el Windows Server 2012 pot gestionar un altre servei que va una mica més enllà en la gestió dels documents i dels permisos que es donen als usuaris per a poder-hi accedir.

Podem necessitar protegir la informació de l'empresa de manera que no pugui ser manipulada de manera intencionada, o que sigui visible als usuaris que no l'han de veure. Així, el servei de gestió de drets afegeix una manera de protegir els fitxers encara més forta que no pas els permisos que ja té el servidor.

Simplement s'haurà d'afegir aquest paper i totes les seves dependències al servidor i configurar-lo quan ho demani perquè gestioni els usuaris del directori actiu ja creat.

Aquest servei afegirà a cada fitxer uns permisos especials que sempre estaran lligats al fitxer; d'aquesta manera encara que es canviï de carpeta, s'enviï per correu, l'obri o el copiï un altre usuari, sempre tindrà els mateixos permisos i per tant no el podrà obrir qui no hi està autoritzat. A més, aquests permi-

sos poden ser temporals: es pot assignar una data de caducitat a l'accés d'un determinat fitxer, i en caducar, automàticament l'usuari deixarà de tenir els permisos i no el podrà obrir, copiar, imprimir, etc.

Això afegeix molta més seguretat al sistema, tot i que requereix tenir instal·lats més papers i característiques, com el servidor de pàgines web.

5) Configuració d'un client del domini

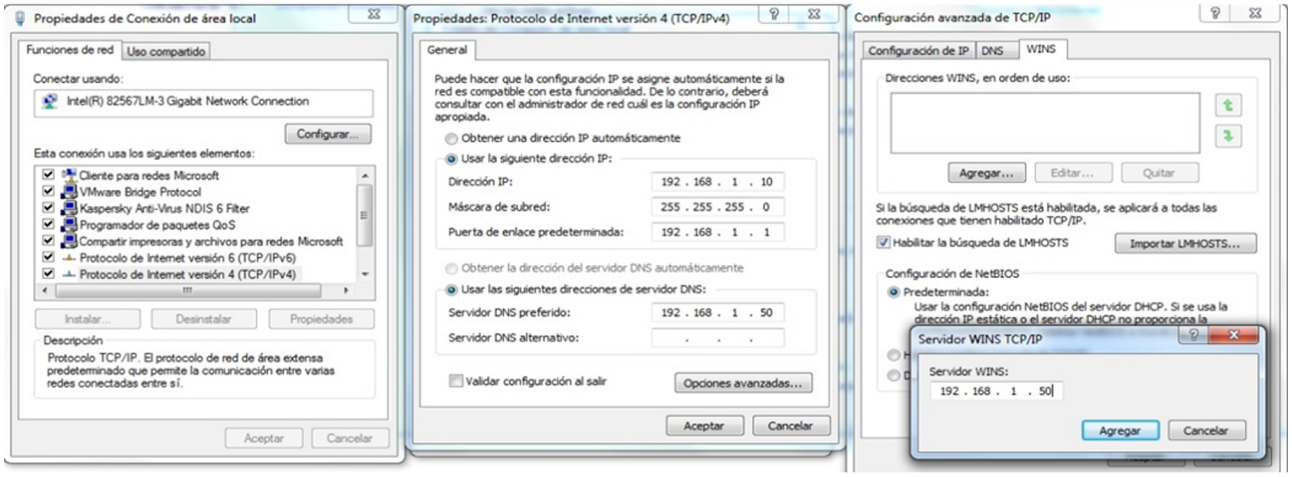
El primer que s'ha de fer a l'hora d'incloure un nou equip en el domini, i per tant en la xarxa que es vol crear, és indicar el DNS que ha de fer servir per a poder trobar els noms dels servidors i la resta d'equips de la xarxa pròpia. En el servidor s'ha instal·lat el servidor de noms (DNS) perquè el servidor faci la traducció de noms de màquines a IP reals. Per tant, ara en els clients, com a adreça de servidor DNS, s'ha de configurar i posar la mateixa que té el servidor DNS esmentat. No cal incorporar-ne cap més, ja que el servidor de noms propi s'encarregarà de canviar els noms de pàgines web per les IP reals d'Internet a l'hora de fer les peticions per a navegar per la xarxa Internet.

En el cas de disposar encara de clients amb el sistema operatiu Windows XP, més antics o altres sistemes operatius d'un altre tipus, s'haurà d'instal·lar en el servidor de domini que hem configurat abans la característica WINS, que és un servidor de noms de xarxa que fan servir les versions antigues de Windows i que serà necessari per a poder ajuntar aquests sistemes amb el nou sistema del Windows Server 2012.

Per a fer això només cal obrir l'administrador del servidor i instal·lar la característica WINS (*Windows Internet name server*), que convertirà els noms NetBIOS dels equips de la xarxa informàtica a adreces IP reals. D'aquesta manera es podran incloure tots aquells equips que treballin únicament amb les adreces NetBIOS dins la xarxa Ethernet.

En els equips client, per tant, s'haurà de configurar perquè vagi a buscar el servidor WINS a l'adreça del servidor on s'hagi instal·lat aquesta característica, tal com mostra la figura següent.

Configuració del WINS en el client



El pas següent és canviar el grup de treball pel domini que s'ha creat. Això dependrà de cada sistema, però en general, per a la família Windows es pot fer a partir del tauler de control, a "Sistema i Seguretat i sistema. S'hi podrà canviar la configuració del grup de treball predeterminat pel nou domini.

A continuació hi ha la llista d'una sèrie de referències en les quals s'explica com s'han de configurar diferents sistemes operatius client amb dominis Windows:

1) Windows XP, Vista, 7 i 8:
http://www.wown.com/articles_tutorials/wxpjoind.html

2) Windows 95 o 98:
http://www.wown.com/articles_tutorials/w2ksvw9x.html

3) Windows NT 4:
http://www.wown.com/articles_tutorials/nt4jw2kd.html

4) Linux:
http://www.wown.com/articles_tutorials/
Authenticating-Linux-Active-Directory.html

Amb això ja haurem aconseguit tenir el sistema client i servidor configurat. En el moment de tornar a iniciar el client, es veurà com ara es demana un nom d'usuari i contrasenya, però aquest cop demanarà els usuaris del domini, i només hi podran entrar aquells usuaris que l'administrador hagi configurat prèviament.

En les carpetes configurades dins el servidor per a guardar els perfils s'aniran creant les noves carpetes a mesura que es vagin obrint les sessions dels usuaris en els ordinadors client.

4. Administració i manteniment del servidor GNU/ Linux

La informàtica no dista gaire de la majoria de les coses que passen al món; el més fàcil és instal·lar un sistema, el més difícil és mantenir-lo. Normalment l'administrador de sistemes ha de fer diverses tasques de manera periòdica i repetitiva. La llista següent ens mostra algunes de les tasques de l'administrador de sistemes, ja que, segons com sigui el sistema o l'entorn, en pot fer unes o altres.

La llista només mostra les més conegudes sense cap ordre concret:

- **Gestió d'usuaris i grups:** donar d'alta i de baixa els usuaris constitueix una de les principals tasques de qualsevol administrador. Hem de destacar que les polítiques de donar d'alta o de baixa un usuari normalment són responsabilitat dels directius de l'empresa o de l'àrea d'informàtica. Aquesta tasca té una importància especial, i per això més endavant dedicarem un apartat a explicar com es fa.

- **Gestió de recursos del sistema:** hem d'estar atents a quins serveis oferim, com els oferim i a qui donem accés a determinats recursos. Qualsevol recurs compartit ha de ser administrat. Això es deu al fet que, o bé els usuaris no són conscients que els recursos que hi ha a la seva disposició són compartits amb altres usuaris, o bé abusen d'aquests recursos. Per a gestionar-los de manera correcta hi ha molts recursos que accepten quotes d'usuari (CPU, memòria, disc, etc.). Un cas particular d'aquesta gestió el constitueixen les quotes del sistema de fitxers. Igual que la gestió d'usuaris, aquesta tasca la veurem amb més deteniment en un apartat posterior.

- **Gestió dels sistemes de fitxers:** la gestió dels sistemes de fitxers constitueix un altre dels punts principals de l'administrador. En la secció dedicada a administrar els discos hem comentat les tasques de l'administrador respecte a aquesta gestió.

- **Arrencada i apagada del sistema:** qualsevol sistema basat en Unix pot configurar el sistema d'arrencada i apagada. Llavors podem configurar quins serveis oferim en l'arrencada de la màquina i quan cal parar-los.

- **Seguretat del sistema:** seguretat local del sistema, és a dir, que cada usuari tingui accés a tot el que necessita però no a recursos que no té assignats.

- **Còpia de seguretat i restauració del sistema:** avui dia és imprescindible tenir una política de còpies de seguretat. L'administrador té la responsabi-

litat de definir aquesta política i dur-la a terme. A causa de la importància d'aquesta tasca més endavant dedicarem un mòdul a parlar-ne.

- **Gestió d'impressió i cues:** els sistemes Unix es poden utilitzar com a sistemes d'impressió per a controlar una impressora o més d'una connectades al sistema, i també per a gestionar les cues de treball que els usuaris o les aplicacions facin servir.

- ***Accounting* (o *log*) de sistema:** en els registres del sistema és on s'escriuen totes les incidències que hi ha. L'administrador té la tasca de revisar aquests registres i veure si els serveis funcionen de manera correcta o si hi ha anomalies. En cas d'una intrusió en la màquina, guardem aquests registres en un lloc segur per tenir proves del delicte.

- **Personalització del sistema:** el nucli del sistema és un paquet obert altament configurable. L'administrador té la tasca de tenir un nucli adequat i optimitzat per al servidor que gestiona. També és important, per a mantenir-lo tan actualitzat i segur com es pugui, incloure-hi les actualitzacions que van sortint, sobretot les de seguretat.

- **Automatització de tasques rutinàries:** moltes de les tasques de l'administrador són rutinàries o fàcils d'automatitzar. L'administrador és qui decideix quina tasca automatitza i com ho duu a terme.

4.1. Permisos de fitxers i directoris

Un tema del qual l'administrador ha d'estar molt pendent són els permisos dels dispositius, fitxers i directoris. Tots els recursos del sistema tenen el mateix tipus de permisos. El que canvia és el significat que tenen segons si és un fitxer o un directori.

La propietat que tots els recursos tinguin el mateix tipus de permisos ens la dóna el sistema de fitxers. Com hem vist abans, el sistema d'arxius tracta tots els recursos del sistema com si fossin fitxers. Hi ha tres grups de permisos. El primer grup fa referència als permisos del propietari, el segon indica els permisos del grup i el tercer el componen els permisos del món (tots els usuaris que no són ni propietaris ni formen part del grup). Cadascun dels grups té tres tipus de permisos, això és, lectura, escriptura i execució, que se simbolitzen amb una `r`, una `w` i una `x`, respectivament. Si, per exemple, el propietari té permís de lectura sobre un fitxer, apareix una `r`; si no en té, apareix un (`-`). Per veure els permisos dels fitxers del directori on som hem d'executar l'ordre `ls -l`.

L'assignació de permisos a un usuari es fa de la manera següent:

1) Se li apliquen els permisos de propietari quan és propietari d'un fitxer.

2) Se li apliquen els permisos de grup quan pertany al grup corresponent al fitxer.

3) Se li apliquen els permisos de la resta quan no és cap dels casos anteriors.

L'assignació de permisos es fa en aquest ordre seqüencial; per tant, si a un usuari, per a un fitxer qualsevol, se li apliquen els permisos de propietari, els altres dos grups de permisos no tenen rellevància per a aquest usuari respecte al fitxer en qüestió. L'única excepció a aquest mètode la constitueix l'usuari *root*. A aquest usuari només l'afecten els permisos quan és el propietari dels arxius o directoris; si no és el cas, pot llegir, modificar i esborrar qualsevol fitxer en qualsevol directori.

Un exemple dels permisos d'uns fitxers és aquest:

```
Nom de fitxer  Propietari Grup Permisos
/home/jordi/test.txt jordi uoc rwxrwxrwx
/home/jordi/readme.txt jordi uoc rw-rw----
/home/jordi/documents jordi uoc rw-rw----
/home/jordi/temp jordi uoc drwx------
```

Hem de tenir present el significat de cadascun dels permisos, ja que la interpretació és diferent segons si és un fitxer o un directori.

En un fitxer, el permís de lectura permet editar el fitxer, el permís d'escriptura permet modificar el fitxer i el permís d'execució permet executar el fitxer. En un directori, el significat és diferent: el de lectura permet veure el contingut del directori, el d'escriptura permet crear i esborrar fitxers, i el d'execució permet travessar el directori.

Un factor molt important per als directoris és que els permisos s'apliquen cada vegada que l'usuari es mou per l'arbre de directoris. Per tant, un usuari, per arribar al seu directori arrel, per exemple, ha de tenir permisos d'execució en tots els directoris que ha de travessar; si no, aquest usuari no pot emmagatzemar els fitxers en el seu directori arrel, encara que hi tingués tots els permisos i en fos el propietari. En el cas de l'exemple anterior, l'usuari `jordi` ha de tenir permisos d'execució en els directoris (`/`) i `/home`.

L'administrador té la tasca d'assegurar-se que tots els usuaris tinguin els permisos correctes per a accedir a tot el que han d'accedir, i no accedir a res més.

Una cosa que cal destacar és que, per a canviar els permisos d'un fitxer, hem de ser propietaris d'aquest fitxer o directori (o executar aquest canvi de permisos com a usuari *root*).

Per a canviar els permisos dels fitxers o directoris hem d'utilitzar les ordres que mostrem a continuació:

- `chmod`: aquesta ordre canvia els permisos específics (`rwx`) d'un fitxer o directori.

- `chown`: aquesta ordre canvia el propietari d'un fitxer o directori.

- `chgrp`: aquesta ordre canvia el grup d'un fitxer o directori.

4.2. Altes,baixes i modificacions d'usuaris

El GNU/Linux, igual que la majoria dels sistemes operatius, està pensat per a donar suport a usuaris. Els usuaris, per defecte en el Linux, sí que tenen un compte (amb les seves dades) juntament amb l'espai de disc assignat perquè hi puguin emmagatzemar els fitxers o directoris. Aquest espai de disc, en principi, només el pot utilitzar l'usuari en qüestió, però es pot canviar mitjançant els permisos del directori.

Un sistema operatiu basat en el GNU/Linux té tres tipus de comptes diferents:

1) El de l'administrador, amb identificador *root*. Aquest compte, per a evitar problemes de seguretat, solament s'ha d'utilitzar per a les operacions d'administració. Hem de tenir present que la majoria dels permisos de fitxer no afecten l'usuari *root*, de manera que aquest usuari és el que té més permisos i un accés més complet a la màquina i als arxius de configuració. En conseqüència, també és el que pot causar més dany per errors o omissions. Un bon administrador ha d'evitar de fer servir el compte de *root* com si fos un usuari més, de manera que es recomana deixar-lo només per a operacions d'administració. Els intrusos intentaran accedir a la màquina per "forats" o pels comptes d'usuari i, una vegada a dins, miraran de canviar-se a administradors per tenir tots els privilegis possibles sobre la màquina.

2) Comptes d'usuaris: els comptes normals dels usuaris. Normalment, aquests comptes tenen permisos restringits al seu espai de disc i a algunes zones particulars (per exemple, el directori temporal `/tmp`). Aquests comptes també poden fer servir tots els dispositius per als quals tenen permisos.

3) Comptes especials dels serveis `www-data`, `lp`, etc. En el Linux hi ha diversos serveis que s'executen amb un usuari concret. No hi ha cap usuari que utilitzi aquests comptes, sinó que els fa servir el sistema de manera interna. Així, evita que serveis poc segurs s'executin amb privilegis de *root*. Tots els serveis que estan en execució pertanyen a un usuari. Hi ha determinats processos que permeten la configuració de l'usuari propietari. La majoria d'aquests processos tenen associat un compte especial que no permet l'entrada interactiva d'aquest usuari a la màquina, però permet que aquests processos tinguin un

propietari diferent de *root*. Des del punt de vista de la seguretat, va bé que fem servir aquests comptes per a executar els processos associats, ja que si aquest procés té vulnerabilitats val més que els usuaris que l'executen no tinguin gaires privilegis en la màquina.

Es crea normalment un usuari mitjançant l'especificació d'un nom (identificador d'usuari, que ha de ser únic en el sistema), una contrasenya, un directori personal que hi està associat (per a emmagatzemar-hi la informació) i un tipus d'intèrpret. La informació dels usuaris del sistema està inclosa en els arxius següents:

```
/etc/passwd
/etc/shadow
/etc/group
```

Vegem a continuació unes línies d'exemple del fitxer `/etc/passwd`:

```
root:x:0:0:root:/root:/bin/bash
jordi:x:1000:1000:Jordi Serra:/home/jordi:/bin/bash
```

En què (`:`) és el separador de cadascun dels camps. Si hi surten dos (`:`) seguits, indica que aquest camp és buit:

- `jordi`: identificador d'usuari en el sistema. Ha de ser un identificador únic.
- `x`: contrasenya de l'usuari codificada; si hi ha una `x` vol dir que és en el fitxer `/etc/shadow`.
- `1000`: codi de l'usuari. En anglès, d'aquest camp se'n diu *user ID* (UID); el fa servir el sistema com a codi d'identitat de l'usuari. Igual que el nom, aquest número ha de ser únic en el sistema. L'assigna el sistema per defecte.
- `1000`: codi del grup principal a què pertany. En anglès, d'aquest camp se'n diu *group ID* (GID); la informació del grup és en el fitxer `/etc/group`.
- `Jordi Serra`: aquest camp és un comentari; s'hi sol posar el nom complet de l'usuari, el document d'identitat o qualsevol altra informació d'ajuda a l'administrador.
- `/home/jordi`: directori personal associat al seu compte. S'ha de posar el camí absolut des del directori arrel.
- `/bin/bash`: intèrpret interactiu que utilitzarà l'usuari quan interactuï amb el sistema, en mode text o gràfic.

En versions anteriors del GNU/Linux, el fitxer `/etc/passwd` solia contenir les contrasenyes dels usuaris de manera xifrada, però el problema era que qualsevol usuari podia veure el fitxer. En el moment en què es van dissenyar els *cracks* que intentaven trobar mitjançant la força bruta la contrasenya fent servir la contrasenya xifrada com a punt de partida (codificada amb el sistema *crypt*), es va modificar el fitxer `/etc/passwd` perquè no hi sortís la paraula clau codificada. Per això, avui dia ja no es posen les contrasenyes en aquest arxiu, i només hi ha una `x`, que indica que són en un altre fitxer, que és només de lectura per a l'usuari arrel. Aquest altre arxiu on hi ha les paraules clau xifrades és el fitxer `/etc/shadow`, el contingut del qual pot ser una cosa semblant a la següent:

```
jordi:2n26TS47RxagQ:12440:0:99999:7:::
```

Aquí hi ha l'identificador de l'usuari juntament amb la contrasenya xifrada. A més, hi surten com a camps separats per `:`:

- Dies des de l'1 de gener de 1970 des que la contrasenya es va canviar per última vegada.
- Dies que falten perquè es canviï (amb 0 no cal canviar-la).
- Dies al cap dels quals cal canviar-la (o sigui, termini de canvi).
- Dies en què s'avisarà l'usuari abans que li expiri el termini.
- Dies al cap dels quals, una vegada expirat el termini, se li deshabilitarà el compte.
- Dies des de l'1 gener de 1970 des que el compte està deshabilitat.
- I un camp reservat.

Si volem seguir una política de canvi de contrasenyes, és a dir, obligar els usuaris a fer que canviïn la contrasenya algunes vegades a l'any, hem de posar un valor diferent de zero en els camps segon, tercer, quart i cinquè, o fer-ho amb l'aplicació gràfica de gestió d'usuaris i grups.

A `/etc/group` hi ha la informació dels grups d'usuaris:

```
root::0:
uoc::1000:
```

En què tenim que el primer camp és el nom del grup (identificador), que ha de ser únic. Entre els grups, no hi pot haver dos grups amb el mateix nom, tot i que hi pot haver un usuari i un grup amb el mateix nom. El segon camp

és la contrasenya del grup (aquest camp no és d'ús comú). L'últim camp és l'identificador numèric del grup; aquest número ha de ser únic (entre els diferents grups).

Hi ha dues maneres de vincular un usuari a un grup. La primera és mitjançant `/etc/passwd`: es posa, en el camp corresponent a l'identificador de grup, el grup a què pertany l'usuari. La segona manera de vincular usuaris a grups consisteix a afegir al final de la línia del grup els usuaris que pertanyen a aquest grup separats per comes.

Vegem a continuació una sèrie d'ordres útils per a aquesta administració d'usuaris:

- `adduser`: afegir un usuari al sistema.

- `deluser`: esborrar un usuari del sistema.

- `addgroup, delgroup`: el mateix per a grups.

- `passwd`: canvia la contrasenya d'un usuari. Aquesta ordre es pot executar com a usuari, i llavors ens demana primer la contrasenya vella i després que hi posem la nova (aquesta petició la fa per duplicat per assegurar-se que s'ha posat de manera correcta). En cas d'executar aquesta ordre com a usuari administrador, s'ha d'especificar l'usuari al qual canviarà la contrasenya (si no, canviaria la seva pròpia contrasenya) i no ha de posar la contrasenya antiga d'aquest usuari. És potser l'ordre que fa servir més el *root*, pensant en els usuaris, quan se'ls oblida la contrasenya antiga.

- `su`: una manera de canviar d'identitat. La utilitzen tant els usuaris com el *root* per a canviar l'usuari actual. En el cas de l'administrador, és molt utilitzat per a verificar que el compte de l'usuari funciona correctament. N'hi ha diferents variants: `su` (sense paràmetres, serveix per a passar a usuari *root*, i, sempre que es tingui la contrasenya de *root*, ens permet, quan som en un compte d'usuari, passar a *root* per fer alguna tasca). La sentència `su iduser` canvia l'usuari a `iduser`, però deixa l'entorn tal com està, és a dir, en el mateix directori. La instrucció `su - iduser` duu a terme una substitució total, com si l'altre usuari hagués entrat en el sistema fent un inici de sessió (*login*).

Com a administradors va bé que no fem servir l'usuari *root* com el nostre usuari habitual de treball. Ara bé, si el nostre usuari de treball no té privilegis per a fer res, a llarg termini deixarem de fer servir el nostre usuari per a utilitzar el de *root*. Perquè no passi això va bé posar-hi que el nostre usuari pertany al grup de *root*. D'aquesta manera, el nostre usuari tindrà alguns privilegis i no caldrà utilitzar tan sovint el de *root*. Igual que el grup de *root*, hi ha altres grups que es creen per defecte en instal·lar la màquina. Hi ha molts d'aquests grups que afecten serveis de la xarxa (correu electrònic, *news*, servidor intermediari,

fax, etc.); n'hi ha que es refereixen a diferents serveis que s'hi poden instal·lar (impressores, cintes, disquets o *floppies*, CD-ROM, àudio, etc.); i, finalment, n'hi ha d'altres que fa referència als processos de la màquina (dimoni o *daemon*, *root*, *adm*, etc.).

Hem de tenir present que tots els fitxers i ordres que hem comentat fan referència a l'administració d'una única màquina. Si el nostre sistema consta de més d'una màquina que comparteixen els usuaris, se solen fer servir aplicacions de gestió dels usuaris (LDAP, NIS, Radius, etc.).

4.2.1. Com ha de ser una contrasenya

La política de seguretat que hi ha en cada organització ha de fixar els requisits perquè una contrasenya es consideri acceptable dins de l'àmbit d'aquella organització. No obstant això, hi ha algunes consideracions acceptades comunament:

- Tots els comptes d'usuari, sense excepció, han de tenir associada una contrasenya. Si hi ha usuaris que no s'utilitzen (*nobody*, correu electrònic, etc.), han de tenir el compte deshabilitat.

- L'usuari, en la seva primera connexió a la xarxa, ha de ser forçat a canviar de contrasenya.

- La llargada de les contrasenyes no ha de ser inferior a set caràcters.

- Les contrasenyes no han de ser paraules simples que trobaríem en un diccionari.

- La contrasenya no ha de ser el nom dels fills ni cap nom de cap personatge (de cinema, de literatura, real o de ficció).

- La contrasenya no ha de contenir l'identificador o el nom de l'usuari.

- Les contrasenyes han de caducar, com a màxim, cada sis mesos. El període mínim de validesa d'una contrasenya ha de ser d'un dia. Depenent del tipus d'organització es podria reduir aquest temps que la contrasenya és vàlida.

- Quan es faci un canvi de contrasenya, la nova ha de ser diferent de les que ha utilitzat abans l'usuari. En alguns sistemes, fins i tot es comprova que sigui substancialment diferent de les altres contrasenyes utilitzades. És a dir, si fins ara teníem com a contrasenya `ePFeter1`, no acceptarà que la nova sigui `ePFeter2`.

- Periòdicament, s'ha de fer una auditoria per a verificar que es compleixen els requisits de la política de seguretat.

Si no podem posar res d'això, què podem posar en la nostra contrasenya?

Una contrasenya ha d'estar formada per caràcters alfanumèrics (xifres i lletres) i ha de ser *key sensitive*, és a dir, que hi puguem posar minúscules i majúscules. Llavors el problema és com ho hem de fer per recordar la nostra pròpia contrasenya.

Un mètode per a posar bones contrasenyes i perquè les puguem recordar és que formin part d'una frase. Per exemple, la frase "Anyone who has never made a mistake has never tried anything new" (Albert Einstein). Si prenem la primera lletra de cada paraula tenim `Awhnmamhntan`. Ara, per similitud, convertim la lletra *A* en el nombre 4 i tenim `4whnmamhntan`. Si som uns romàntics, direm que la paraula més important d'aquesta frase és *new* i, per tant, la posarem en majúscula, de manera que la contrasenya ens quedarà finalment així: `4whnmamhntaN`. Aquesta contrasenya compleix totes les especificacions i, a més, és fàcil de recordar.

4.2.2. Desxifrador de contrasenyes

Hi ha moltes eines a la Xarxa que tenen la finalitat d'obtenir tantes parelles d'usuari/contrasenya com puguin per a accedir a la màquina, i tenen com a objectiu principal aconseguir un compte amb privilegis (si pot ser *root*).

Una de les eines més esteses que fa aquesta funció és l'anomenada *John The Ripper*. Per a instal·lar aquesta eina en la màquina hem d'executar l'ordre:

```
Root# apt-get install john
```

Un atac de força bruta

Un atac de força bruta és l'atac en què es van provant totes les combinacions possibles fins a trobar la correcta.

Les versions antigues d'aquesta eina miren de desxifrar les contrasenyes de tots els usuaris. Això només és qüestió de temps i de recursos. Fent servir un atac de força bruta podem arribar a desxifrar totes les contrasenyes de la màquina.

A causa de problemes de compatibilitat amb la llei de protecció de dades, és a dir, que no és legal que un administrador sàpiga les contrasenyes dels seus usuaris, les versions modernes d'aquesta eina només intenten desxifrar la contrasenya de l'administrador.

4.3. Quotes de disc

Una tasca important per a l'administrador de la màquina és mantenir el sistema de fitxers. En un apartat anterior hem vist com s'ha de fer per a mantenir els discos perquè es conservin sanejats. Mantenir els discos sanejats implica que hi hagi prou espai perquè tothom pugui treballar, fins i tot el sistema operatiu. Perquè tots puguem treballar és imprescindible que ningú no abusi

dels recursos que ens ofereix el sistema de fitxers. Un dels mètodes per a evitar que ningú no abusi de l'espai lliure del sistema de fitxers és assignar quotes als usuaris.

Hi ha un paquet per al GNU/Linux que ens permet assignar quotes als usuaris. En la majoria de les distribucions, si volem que el nostre sistema sigui compatible amb les quotes, hem de seguir dos passos. D'una banda, instal·lar els paquets `quota` i `quotatool`, que ens permeten tenir quotes. Per instal·lar aquests paquets, hem d'executar les ordres següents:

```
Root# apt-get install quota
Root# apt-get install quotatool
```

L'aplicació de quotes ens permet especificar límits en dos aspectes de l'emmagatzematge d'informació: el nombre d'*inodes* que pot tenir un usuari i el nombre de blocs que també pot tenir assignats un usuari. Les quotes també tenen dos tipus de límit: el límit programari i el límit maquinari. El primer tipus ens indica la màxima quantitat d'espai de disc que pot tenir un usuari en una partició, que, combinat amb el temps màxim permès de superar el límit, actua com un límit en què l'usuari rep avisos que li notifiquen que ha ultrapassat el límit que estableix el sistema. El segon tipus de límit, el maquinari, especifica el límit absolut que no pot ultrapassar un usuari en cap concepte. El període de gràcia és el temps que passa entre que l'usuari viola el límit programari i rep la notificació que l'ha ultrapassat.

Les ordres que intervenen en l'assignació de quotes són les següents:

1) `edquota`: ens permet crear i modificar la quota d'un usuari.

2) `quotachek`: s'utilitza per a escanejar les quotes d'un sistema i actualitzar les quotes dels usuaris.

3) `repquota`: produeix un informe sobre els usuaris del sistema i la seva quota.

4) `quotaon`: activa les quotes d'un sistema de fitxers.

5) `quotaoff`: desactiva les quotes d'un sistema de fitxers.

Web recomanat

Si voleu aprofundir en la manera d'habilitar les quotes en un sistema basat en GNU/Linux, consulteu l'adreça següent: http://www.tldp.org/howto/quota.html

4.4. Eines bàsiques

L'administrador de sistemes GNU/Linux s'ha d'enfrontar diàriament a una gran quantitat de tasques. En general, en la filosofia Unix no hi sol haver una única eina per a cada tasca o una sola manera de fer les coses. L'habitual és que els sistemes Unix proporcionin una gran quantitat d'eines més o menys simples per a afrontar les tasques. Per a això, és molt recomanable saber fer servir les eines que el sistema ens posa a l'abast.

4.4.1. Documentació

El primer gran bloc d'eines que hem de saber utilitzar el constitueix la documentació que el sistema, o les aplicacions, posen a la nostra disposició. Hi ha moltes fonts d'informació dins del sistema, però destacarem les més importants:

- `man`: és l'ajuda bàsica i més utilitzada de totes les que mostrarem. Ens permet consultar el manual del GNU/Linux. Aquest manual està agrupat en diverses seccions. Per a obtenir l'ajuda que hi està associada, en tenim prou amb `man ordre`. Cada pàgina ens descriu l'ordre, les opcions que té, de vegades alguns exemples, i ordres que hi estan relacionades. Com que el `man` té diverses seccions, és possible que ens trobem que una determinada pàgina sigui disponible en diverses seccions (cadascuna d'aquestes seccions mostra informació diferent); en aquest cas, cal especificar quina secció volem visualitzar mitjançant la línia d'ordres `man n ordre` (en què `n` és el número de secció). Una ordre interessant que està relacionada amb l'ordre `man` és `apropos ordre`, que ens pot servir per a localitzar pàgines `man` que parlin d'un tema determinat (associat amb la paraula buscada).

- Documentació de les aplicacions: hi ha moltes aplicacions que, a més de mostrar molta informació en el `man`, ens proporcionen una informació addicional que trobarem a `/usr/doc/`, on es crea un directori per cada paquet d'aplicació.

4.4.2. Intèrpret d'ordres

Un altre gran bloc d'eines bàsiques el constitueixen els intèrprets d'ordres (*shells*). El terme *shell* s'utilitza per a anomenar un programa que serveix d'interfície entre l'usuari i el nucli del sistema. Aquestes interfícies poden ser en mode text o en mode gràfic.

L'intèrpret d'ordres en mode text és una eina que permet als usuaris comunicar-se amb el sistema mitjançant ordres, que els usuaris introdueixen en l'intèrpret i que el sistema interpreta. D'aquesta interfície en mode text també se'n diu línia d'ordres. L'intèrpret en mode gràfic té un gestor de finestres en què el sistema ofereix que algunes aplicacions (del sistema) s'executin en mode gràfic. Malgrat disposar de finestres, però, hi ha algunes ordres del sistema que encara s'han d'introduir per línia d'ordres. Els entorns gràfics tenen emuladors de terminals amb aquesta finalitat.

Hi ha dues maneres d'accedir a un intèrpret d'ordres, tant si és de text com gràfic: en consola o remot. L'accés en consola es fa quan un usuari té accés (físic) a la màquina. L'usuari s'asseu davant del sistema i introdueix les ordres.

L'accés remot es produeix quan l'usuari accedeix a la màquina mitjançant una xarxa. En aquest cas, el sistema ha de tenir instal·lats sistemes de consola remota (*rlogin*, *telnet*, SSH, X Window, etc.).

Una de les eines més interessants i potents, pensant en l'administrador d'una màquina, que ens ofereixen els intèrprets són els *shell scripts*, fitxers de text que contenen seqüències d'ordres de sistema, més una sèrie d'ordres pròpies de l'intèrpret interactiu, més les estructures de control necessàries per a processar el flux del programa (dels tipus `while`, `for`, etc.).

Els intèrprets d'ordres són molt importants dins d'un sistema. Els motius principals d'aquesta importància els resumim en les dues raons següents:

- La manera principal d'automatitzar processos és la que duu a terme l'administrador creant intèrprets d'ordres.

- La configuració del sistema i de la majoria dels serveis es fa mitjançant eines proporcionades en forma d'intèrprets d'ordres.

4.4.3. Processos

El sistema operatiu basat en GNU/Linux és un sistema anomenat *multiprocés*. Això vol dir que és capaç d'executar de manera simultània més d'un procés. Hi ha diversos tipus de processos:

- Processos de sistema: són els processos associats al funcionament local de la màquina, del nucli o dels serveis. D'aquest últim tipus de procés també se'n diu *dimoni* o *daemon*. La majoria dels processos de sistema estan associats a l'usuari *root*, malgrat que aquest usuari no té cap consola oberta en el sistema (tant remota com interactiva). Hi ha determinats serveis que s'executen associats a usuaris "virtuals", que només existeixen en el sistema per a facilitar l'execució d'un determinat servei (`lp`, `www-data`, correu electrònic, etc.).

- Processos d'usuaris del sistema: els processos associats a l'execució de les aplicacions d'usuari, tant si es tracta de tasques interactives en mode text com de tasques interactives en mode gràfic. Un cas especial dels processos d'usuari és el cas del *root*: tots els processos que executa el *root* (que no siguin de sistema) són processos de l'usuari administrador.

La gestió dels processos d'una màquina la podem fer mitjançant les ordres següents:

- `ps`: el resultat de l'execució d'aquesta ordre és una llista amb els processos que hi ha en execució en aquell moment. Per defecte, mostra els processos

de l'usuari que ha executat l'ordre. Hi ha moltes opcions disponibles (vegeu `man`), però una de les que fa servir més l'administrador és `ps aux`.

- `top`: és una ordre que ens mostra els processos en execució però ordenats per consum de CPU. Aquesta llista s'actualitza a intervals.

- `kill`: té la funció d'eliminar processos, tant si són d'usuari com de sistema. Només es poden matar els processos dels quals som propietaris (o dels quals som *root*). La manera d'execució més comuna per a l'administrador és `kill -9 PID`. El PID (*process identifier*) l'obtenim executant el `ps`.

4.4.4. L'editor `vi`

Hi ha molts editors de fitxers. N'hi ha que fan servir entorns gràfics i n'hi ha que fan servir mode text. Ara, l'editor que s'instal·la amb el sistema operatiu –tret que el primer que fem sigui instal·lar un editor de fitxers–, el que tenim per a modificar els fitxers de configuració, es diu `vi`.

L'editor `vi`, malgrat que és molt potent, té una interacció amb l'usuari molt difícil. Si no s'està acostumat a fer-lo servir, modificar unes lletres d'un fitxer pot resultar una tasca molt complicada. No obstant això, cal que aprenguem a fer-lo servir perquè ens podem trobar màquines que només tenen aquest editor. Té dos modes d'operació: el mode d'inserció i el mode normal. Per a entrar al mode d'inserció hem de prémer la tecla `i`; a partir d'aquí podem introduir text en el fitxer. Per passar al mode normal hem de prémer Ctrl + F3 o ESC.

En mode normal ens permet gravar i fer les operacions de copiar i enganxar, o sortir-ne. Per sortir gravant de l'editor hem d'estar en mode normal i prémer `:wq`.

5. Administració i manteniment del servidor Windows Server 2012

El Windows Server 2012 incorpora moltes eines per a administrar els servidors que utilitzen un entorn o una interfície gràfica comuns, anomenat *Microsoft management console* (MMC). L'MMC és extensible i hi ha eines d'altres empreses que l'utilitzen per a agregar eines d'administració al sistema. Diversos fabricants han creat eines que s'ajuden d'aquesta consola i del directori actiu per facilitar la gestió dels usuaris i de la seguretat. A més, podem crear consoles MMC a la mida de les nostres necessitats, i fins i tot confeccionar-les per a distribuir-les després amb la finalitat que hi hagi determinades gestions que les executin usuaris en els quals deleguem alguna tasca administrativa, com per exemple el canvi de contrasenya dels usuaris del domini.

Disposa també de l'administrador del servidor: tenim tots els papers instal·lats en la màquina en aquesta aplicació que els permet configurar ràpidament i de manera simple. A més, dóna una visió ràpida dels problemes que puguin tenir.

Per cada un dels papers, el Windows Server 2012 incorporarà les eines necessàries per a l'administració i configuració pròpies, com per exemple el servidor de noms DNS. En el moment d'instal·lar el servidor també s'instal·la l'eina de configuració i s'incorpora a la resta d'eines de què ja disposa el servidor.

5.1. Gestió d'usuaris

En el Windows Server 2012 podem gestionar els usuaris que tenen accés al sistema, i també els privilegis que té cadascun d'aquests usuaris. Per a gestionar-los més bé, aquests usuaris es poden organitzar per grups, o fins i tot dins d'unitats organitzatives o entitats, amb un paper determinat; així, a l'hora d'atorgar un privilegi, se sol atorgar a un determinat grup o entitat, en lloc de fer-ho a tots els usuaris que el componen d'un en un. Això comporta una seguretat afegida, ja que en el cas que un usuari amb privilegis elevats, perquè està en una posició de l'empresa que ho requereix, és canviat de responsabilitats, només cal canviar-lo de grup, i per tant se li canviaran tots els privilegis automàticament, sense haver de pensar en quins privilegis ha de continuar tenint i quins no, i sobretot descuidar-nos de treure privilegis importants que ja no hauria de tenir.

Els privilegis, a part de l'accés al sistema, es configuren des del servei que requereix seguretat. A continuació es fa una llista d'alguns serveis que permeten indicar els usuaris autoritzats:

- Accés a carpetes fitxers, impressores

- Ús de connexions de xarxa
- Accés a bases de dades
- Tasques d'administració

És convenient, amb vista a millorar la seguretat, repassar els comptes d'usuari que ha creat automàticament el sistema durant el procés d'instal·lació per eliminar els que no calen o protegir-los amb alguna contrasenya coneguda. Molts cops hi ha usuaris convidats o usuaris que es creen automàticament per a fer tasques que després deixen de tenir sentit, però no es bloquegen o eliminen, i poden ser un possible punt d'entrada al sistema.

5.1.1. Gestió d'usuaris sense directori actiu

Si no s'ha instal·lat el directori actiu en el servidor, utilitzem l'eina Administració d'equips que hi ha dins de la carpeta Eines administratives per a crear i gestionar usuaris. Dins d'aquesta eina veiem que hi ha diverses utilitats per a gestionar l'equip, organitzades en forma d'arbre. Entre aquestes utilitats trobem l'opció Usuaris locals i grups, en què es mostren dues carpetes en les quals s'emmagatzemen els usuaris de l'equip i els grups, respectivament.

Per crear usuaris o grups, hem de fer clic amb el botó secundari del ratolí sobre la carpeta corresponent i seleccionar l'opció Usuari nou o Grup nou. En crear un usuari nou, ens surt la finestra de creació d'usuaris, en la qual ens demanen les dades de l'usuari i la contrasenya. A part del nom d'usuari i la contrasenya inicial, podem establir algunes de les opcions següents:

- L'usuari ha de canviar la contrasenya en l'inici de sessió següent. Per defecte s'ha de fer servir perquè l'usuari l'hagi de canviar i configurar-ne una de pròpia i més segura.
- L'usuari no pot canviar la contrasenya. Pensant en la seguretat val més desactivar aquesta opció, ja que com més temps s'estigui sense canviar una contrasenya, més probabilitats hi ha que un usuari no autoritzat la descobreixi.
- La contrasenya no caduca mai. Igual que l'opció anterior, val més mantenir-la deshabilitada pensant en la seguretat.
- Compte deshabilitat: si se selecciona aquesta opció, es denega l'accés de l'usuari al sistema, però se'n guardala informació per si més endavant es torna a habilitar. És útil per a comptes que han d'estar un temps deshabilitats i no cal que estiguin actius, i per tant podrien ser focus d'atacs.

Una vegada creat un usuari, en podem visualitzar les propietats mitjançant l'opció Propietats del menú Acció o del menú contextual de l'usuari en la llista d'usuaris de la dreta. També és possible modificar la contrasenya d'un usuari mitjançant l'opció Establir contrasenya del menú Acció o del menú contextual.

En prémer Crear, la finestra es manté oberta com la finestra de creació d'usuaris. Una vegada creat el grup, en podem visualitzar les propietats mitjançant l'opció Propietats del menú Acció o del menú contextual del grup en la llista de grups de la dreta. Per a agregar usuaris a grups utilitzem l'opció Agregar a grup del menú Acció o del menú contextual del grup. En la finestra de selecció d'usuaris que formen part del grup podem seleccionar els usuaris o grups que ja hi ha i afegir-los mitjançant el botó Agregar. En la part inferior surt una llista de tots els usuaris o grups agregats al grup actual.

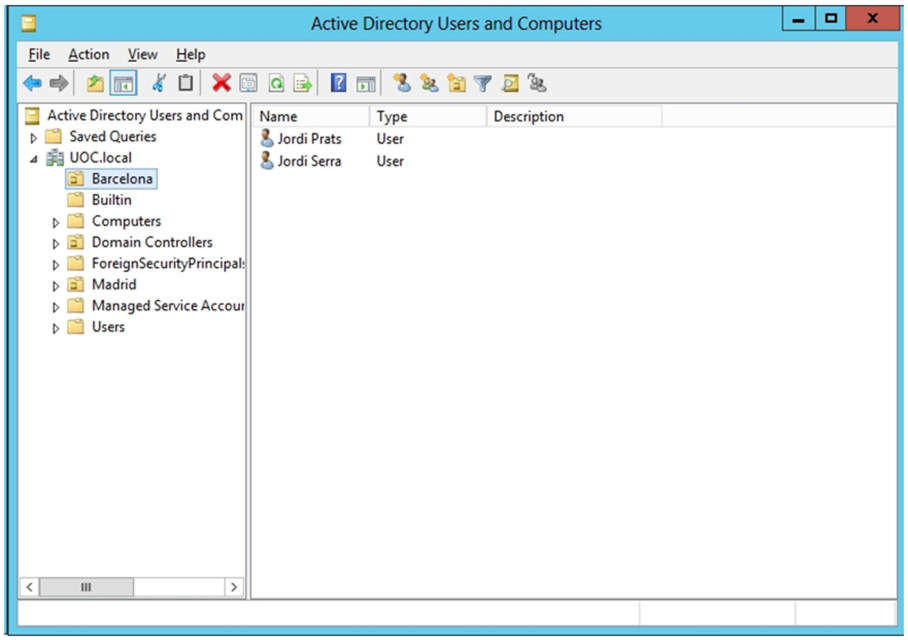
Els grups es crearan de manera similar: només cal fer Crear grup i donar el nom. Com veiem, el Windows Server 2012 crea alguns grups predefinits, com per exemple el grup d'administradors, que té permisos per a fer tasques d'administració del sistema, i té accés a tots els directoris del sistema de fitxers. Cal destacar que totes les opcions descrites en aquest apartat només s'apliquen a servidors que no siguin controladors de domini, ja que aquests controladors tenen instal·lat el directori actiu i per tant no tenen SAM local amb usuaris i grups locals.

5.1.2. Gestió d'usuaris amb directori actiu

Si s'ha instal·lat el directori actiu per a configurar el servidor com a controlador de domini, en accedir a l'eina anterior la gestió d'usuaris i grups veurem que ja no es mostra. Els comptes d'usuaris s'han de gestionar amb el complement d'usuaris de directori actiu, de manera que hem d'utilitzar aquesta eina per a crear o modificar usuaris o grups. Un servidor de domini només permet gestionar comptes de domini; per tant, no permet usuaris locals. Aquesta eina o complement del directori actiu s'anomena *Usuaris i equips d'Active Directory*. També és en la carpeta Eines administratives.

En fer clic amb el botó secundari del ratolí sobre una de les carpetes de l'arbre de l'esquerra surt un menú contextual amb les diferents opcions, entre les quals hi ha les opcions per a crear nous grups o usuaris. En crear un nou usuari cal introduir-ne les dades personals, i també el nom d'inici de sessió assignat (*login*). També cal establir una contrasenya i les característiques que té (si s'ha de canviar la contrasenya en l'inici de sessió següent, si la contrasenya no caduca, si es pot no canviar o si el compte d'usuari està deshabilitat inicialment).

Eina de creació i configuració d'usuaris i equips



En crear un nou grup, cal introduir-ne el nom, l'àmbit i el tipus, que podran ser de seguretat o distribució. També es pot introduir el nom del grup compatible amb versions del sistema anteriors al Windows 2000, encara que s'ha de tenir en compte que mantenir compatibilitat amb sistemes anteriors pot comportar problemes de seguretat. El tipus d'un grup pot ser de seguretat o de distribució. Els grups de seguretat es mostren en les llistes de control d'accés discrecional (*discretionary access control list* o DACL), que defineixen els permisos sobre recursos i objectes. A més, es poden utilitzar com a entitats de correu electrònic, de manera que, en enviar un missatge al grup, aquest missatge s'envia a tots els membres del grup. En canvi, els grups de distribució no surten en les llistes DACL. Aquests grups són preferibles si no es requereix donar permisos directament al grup, o utilitzar-lo com a entitat de correu electrònic.

L'àmbit del grup identifica l'abast d'aplicació del grup a l'arbre o al bosc de dominis. Hi ha tres àmbits diferents:

- **Universal:** poden tenir com a membres grups i comptes de qualsevol domini de Windows 200x en l'arbre o el bosc de dominis i s'hi poden concedir permisos en qualsevol domini de l'arbre o el bosc de dominis. Només es poden utilitzar quan hem elevat el nivell funcional del domini a mode natiu.

- **Global:** poden tenir com a membres grups i comptes només del domini en el qual s'ha definit el grup i s'hi poden concedir permisos en qualsevol domini del bosc.

Web recomanat

Trobareu més informació sobre gestió d'usuaris i grups amb directori actiu en l'adreça següent: http://technet.microsoft.com/en-us/library/hh801901.aspx

- **Local:** poden tenir com a membres els grups i els comptes d'un domini de Windows 200x o Windows NT, i només es poden utilitzar per a concedir permisos en un domini.

5.2. Quotes de disc

Les quotes de disc defineixen la quantitat d'espai en el disc dur que pot ocupar un determinat compte d'usuari. Per habilitar quotes de disc, accedim a les propietats del disc en el qual les volem activar, mitjançant l'opció Propietats del menú contextual. Dins d'aquesta finestra de propietats, entrem a la pestanya Quota.

Des de la pestanya Quota podem habilitar les quotes en el disc i configurar-ne altres propietats com denegar espai de disc a comptes que excedeixin la quota o no, establir el límit de quota de disc per a usuaris nous i el nivell d'advertiment a partir del qual s'avisa l'usuari que és a punt d'excedir la quota disponible, o finalment activar el registre dels excessos de quota produïts. També es pot configurar la quota permesa per a cada usuari o grup d'usuaris. Per fer-ho, fem clic sobre el botó Valors de quota... i ens surt la finestra de configuració de quotes per a cada usuari. Per a afegir una restricció de quota seleccionem l'opció Nova entrada de quota del menú Quota.

A continuació, afegim a la llista de la part inferior els usuaris afectats per la quota que definirem. Finalment, n'especifiquem els límits. En acceptar aquests límits, surten en la llista d'entrades de quota els nous usuaris amb les restriccions respectives.

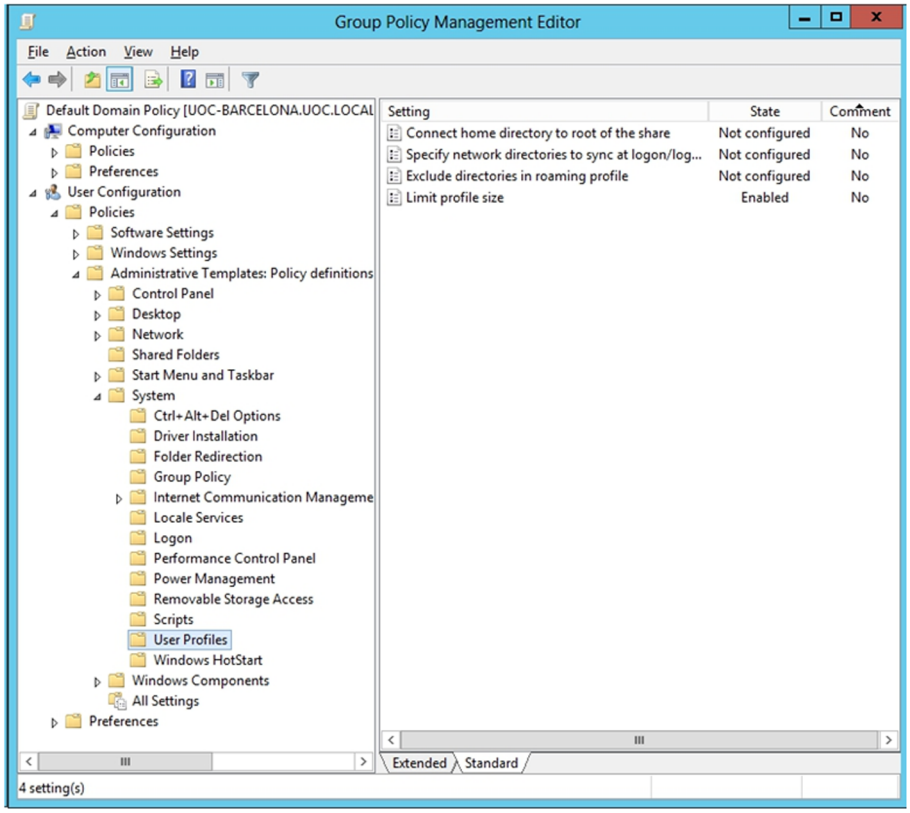
Des del servidor i mitjançant el directori actiu, també es pot imposar a tots els usuaris, estiguin en l'equip que sigui, una quota de disc local. Això ho podem fer obrint el gestor de polítiques de grup i cercant la política que fa referència a les quotes de disc i forçar que els usuaris tinguin una quantitat fixa d'espai en disc. Ho trobarem en la branca següent de les polítiques de grup:

Configuració del PC -> Polítiques -> Plantilles administratives -> Sistema -> Quota de disc.

S'hi pot habilitar i marcar el màxim i el llindar per a enviar un avís de superació de la quota de disc. De la mateixa manera, podem limitar la mida del perfil mòbil de cada usuari, perquè no es puguin tenir perfils massa grans que poden fer que la xarxa se saturi en els moments d'entrada i sortida de l'entitat. A més, tindrem més controlat l'espai de disc del servidor on es guarden els perfils de cada usuari. Això ho farem a partir de la política de grup següent:

Configuració d'usuari -> Polítiques -> Plantilles administratives -> Sistema -> Perfil d'usuari.

Editor de polítiques de grup per als perfils d'usuari



5.3. Eines bàsiques

Les eines bàsiques d'administració del sistema operatiu a escala local, en el servidor, es troben en la carpeta Eines administratives, que podem trobar en la interfície Metro. A continuació en veurem algunes de les més importants.

5.3.1. Serveis

Els serveis són aplicacions o processos que s'executen en segon pla, que no tenen interfície gràfica d'usuari. Aquests serveis duen a terme una sèrie de tasques que no requereixen interacció amb l'usuari o reben peticions d'altres aplicacions per a fer una tasca o una altra. En la finestra de serveis veiem els serveis instal·lats en el sistema, com per exemple la cua d'impressió o el coordinador de transaccions. Hi veiem també l'estat de cadascun d'aquests serveis, activar o desactivar serveis, o configurar serveis perquè s'iniciïn automàticament en iniciar el Windows o de manera manual.

5.3.2. Configuració del servidor

Hi ha l'eina Administració del servidor, que surt la primera vegada que s'inicia el sistema després de la instal·lació i que no desapareixerà fins que no es configuri d'una altra manera en les propietats d'aquesta eina. També la podem iniciar manualment quan sigui necessari. Aquesta finestra permet configurar diversos aspectes del servidor per a configurar-lo com a controlador de domini (instal·lant el directori actiu), com a servidor d'arxius o d'impressió, com a

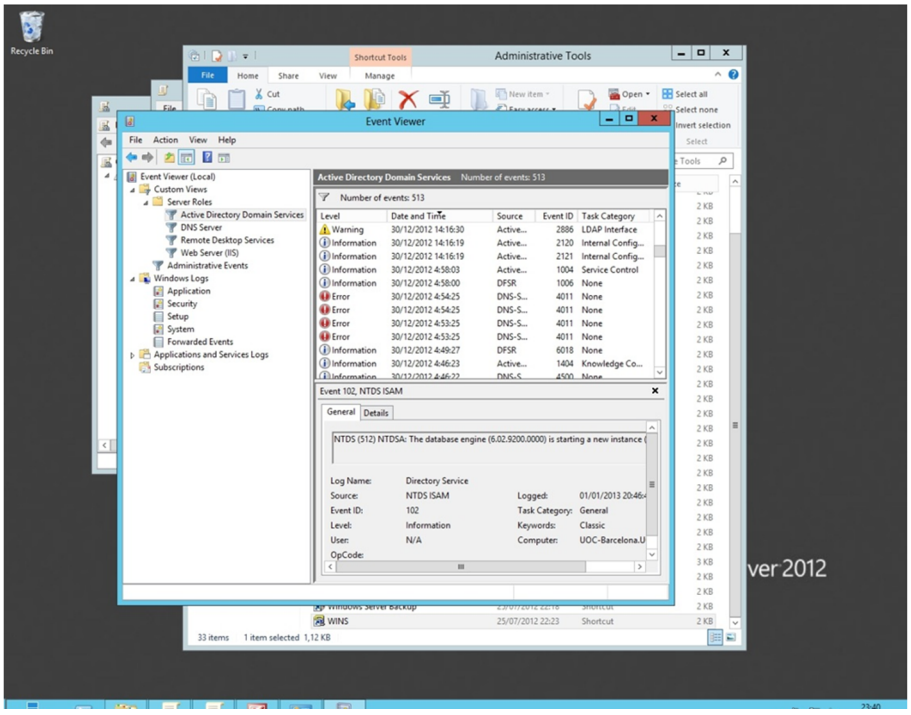
servidor web o servidor d'aplicacions, etc. És on s'han d'anar afegint i traient tots els papers i característiques que es vulguin donar al servidor. A més, quan hi ha un error en el sistema que està relacionat amb algun dels papers o característiques, és aquí on el sistema avisa de manera visual que hi ha un error. Ràpidament es pot veure quin error s'ha produït.

5.3.3. Visor d'incidències

Quan es produeix algun error, ja sigui en un dels papers, característiques o en el sistema operatiu mateix, es desa en un fitxer de registres del sistema. D'aquesta manera el sistema es comunica amb els administradors, i són aquests els que han d'anar a visualitzar aquests fitxers de registre. Des del visor d'incidències (o visor d'esdeveniments) veiem els errors o problemes que s'han produït en el sistema, i també informació addicional sobre l'error. Aquests informes d'error ens permeten veure si hi ha cap fallada en alguna aplicació o en la seguretat del sistema i donen informació addicional per tal de poder cercar informació, tant en el web de Microsoft com en fòrums especialitzats.

Els esdeveniments estan dividits en categories i grups. Així, podem trobar els registres d'esdeveniment del sistema operatiu, dels servidors instal·lats, etc., separats en els apartats que mostra la figura següent.

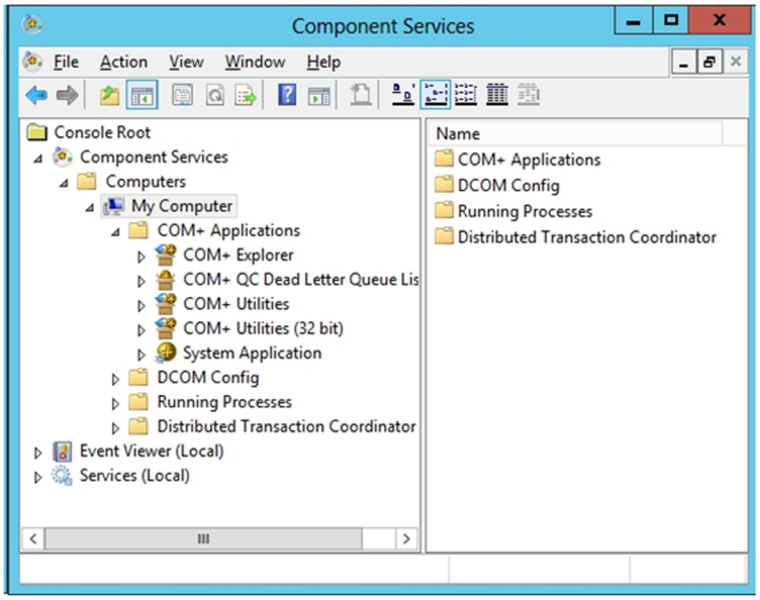
Exemple del visor d'esdeveniments



5.3.4. Serveis de components (COM)

Els components COM (*common object model*) són components de programari situats en el registre del sistema que poden utilitzar altres aplicacions. La finestra de serveis de components mostra els components COM instal·lats en el sistema. També mostra informació sobre el controlador de transaccions distribuïdes. En tenim un exemple en la figura següent.

Components COM

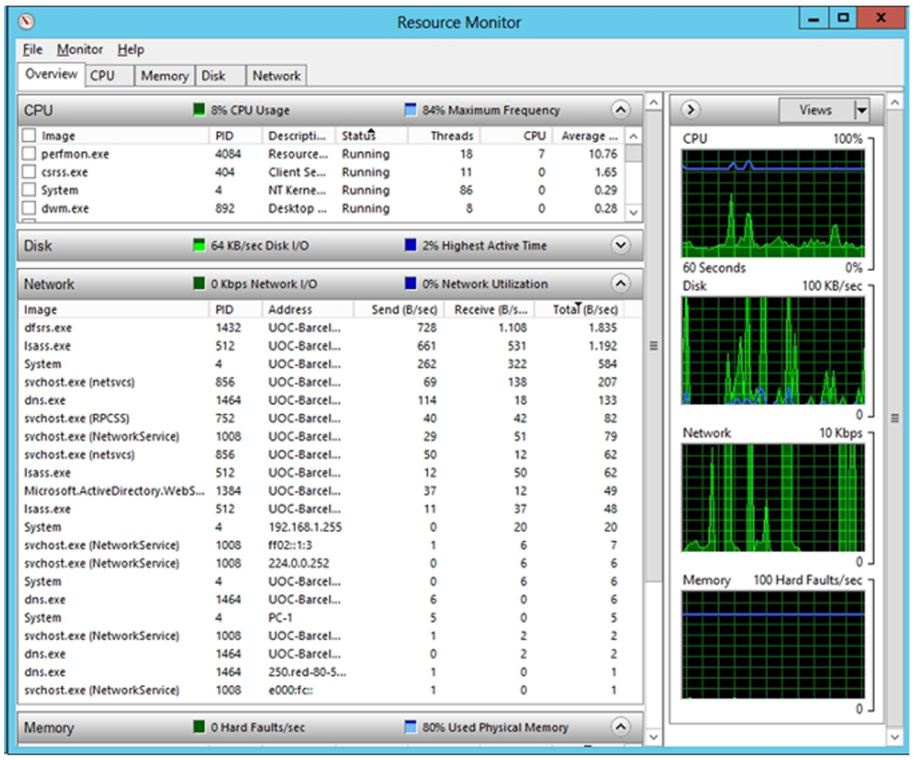


5.3.5. Rendiment

El monitor de rendiment permet fer un control sobre el rendiment del sistema. Ofereix la possibilitat de seleccionar entre molts comptadors de rendiment (memòria, ús del processador, ús en disc, xarxa, etc.) i fa un gràfic dels valors dels comptadors seleccionats al llarg del temps. En aquesta versió del sistema operatiu, l'eina de control del rendiment del servidor dóna molta informació addicional al rendiment, i es pot veure com, per exemple, consumeixen l'amplada de banda les diferents aplicacions que hi ha en cada moment executant-se, i així podem veure ràpidament si hi ha alguna aplicació maliciosa que està fent servir la xarxa per a comunicar-se, enviar correu brossa, baixar algun altre programa, etc.

La figura següent mostra un exemple de les aplicacions que estan fent servir la xarxa Ethernet.

Rendiment de la xarxa de comunicacions del servidor



5.3.6. Administració d'equips

Algunes de les consoles d'eines anteriors i algunes més s'agrupen en la consola predeterminada que ve en el sistema operatiu administració d'equips.

A continuació descriurem breument les diferents eines d'administració d'equips:

- **Visor d'incidències:** mostra les incidències o els errors produïts en el sistema.

- **Informació del sistema:** proporciona dades sobre el sistema, com maquinari, components i programari instal·lat, etc.

- **Registres i alertes de rendiment:** mostra i configura les alertes de rendiment del sistema.

- **Carpetes compartides:** permet configurar les carpetes compartides amb altres equips.

- **Administració de dispositius**: permet configurar dispositius maquinari.

- **Usuaris locals i grups:** gestiona usuaris i grups de l'equip.

- **Administració de discos:** permet gestionar els diferents volums de discos disponibles, fer particions de discos, formatar, canviar la lletra d'accés a una unitat, etc.

- **Compactador de disc:** optimitza l'emplaçament dels arxius en disc per a millorar-ne l'accés.

- **Unitats lògiques:** gestiona les unitats lògiques definides en l'equip.

- **Mitjans d'emmagatzematge:** controla dispositius d'emmagatzematge extraïbles i intercanviables.

- **Serveis i aplicacions:** conté una altra sèrie d'eines per a controlar serveis i aplicacions del sistema (DHCP, WMI, Index Server, IIS, WINS, DNS, etc.).

Si tenim un controlador de domini, podem administrar els diferents equips del domini amb l'eina Usuaris i equips d'Active Directory, seleccionant l'equip que s'ha d'administrar i fent clic en l'opció Administrar.

5.4. Eines de protecció del Windows Server 2012

5.4.1. Assistent de configuració de la seguretat

L'assistent de configuració de la seguretat o *security configuration wizard* (SCW) és una eina de reducció de superfície d'atac per a servidors de la família Microsoft Windows Server. L'SCW determina el nivell de funcionalitat mínima que requereix el servidor per a funcionar i proporcionar els serveis correctament, al mateix temps que deshabilita les funcionalitats que no hi fan falta.

Webs recomanats

Per a més informació sobre l'SCW, consulteu "Security Configuration Wizard for Windows Server 2012" al lloc web del Microsoft Windows Server 2012:

http://technet.microsoft.com/en-us/library/cc754997.aspx

http://technet.microsoft.com/en-us/windowsserver/hh534429

http://technet.microsoft.com/en-us/library/hh831360.aspx

Passos que segueix l'SCW:

1) Deshabilita els serveis innecessaris.

2) Bloqueja els ports que no s'utilitzen.

3) Permet la configuració específica de seguretat en ports que queden oberts.

4) Prohibeix les extensions de l'IIS que no són necessàries, si és aplicable.

5) Redueix l'exposició a riscos dels protocols SMB, Lanman i LDAP.

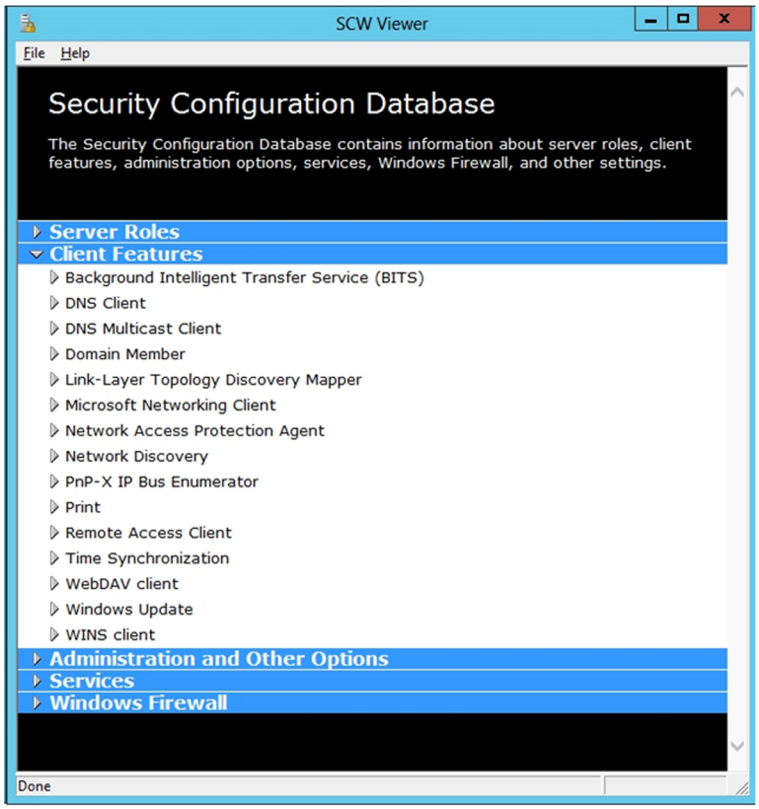
6) Defineix una política d'auditoria de seguretat alta.

7) L'SCW guia en el procés de crear, editar, aplicar o retirar una política de seguretat basada en els papers seleccionats del servidor. Les polítiques de seguretat creades amb l'SCW són arxius XML que, quan s'apliquen, configuren serveis, la seguretat de la xarxa, valors específics de registre, polítiques d'auditors i, si és aplicable, el servei d'informació d'Internet.

El procediment de protecció dels servidors es basa a executar el programari de l'assistent de configuració de la seguretat de Microsoft*securityconfiguration wizard* . A més, es comproven i revisen mitjançant tots els punts febles que la *Microsoft security guide* aconsella revisar. Després, es du a terme la comprovació que els serveis funcionen correctament i que la protecció és correcta.

Iniciem l'SCW, des de la interfície Metro o des de les eines administratives, i seguim fins a la pantalla següent, en la qual es poden seleccionar diferents opcions com crear una nova política de seguretat, editar-ne una d'existent, aplicar una política ja existent o desfer els canvis d'una política que ja es va aplicar amb anterioritat. Com que és la primera vegada que es fa una política, en crearem una de nova sobre el mateix servidor que estem configurant; es podria fer sobre un altre de manera remota, però no serà aquest el cas. Comença a processar i analitzar la política aplicada en el servidor actualment i extreu un registre molt complet. Podem veure aquest registre amb el botó View Configuration Database. La figura mostra un exemple d'aquesta recopilació inicial de tots els paràmetres de seguretat que ha trobat ja configurats en el sistema.

Visor SCW. Configuració inicial



A continuació, l'assistent es divideix en quatre grans parts:

1) Configuració basada en els papers Microsoft que té el servidor.

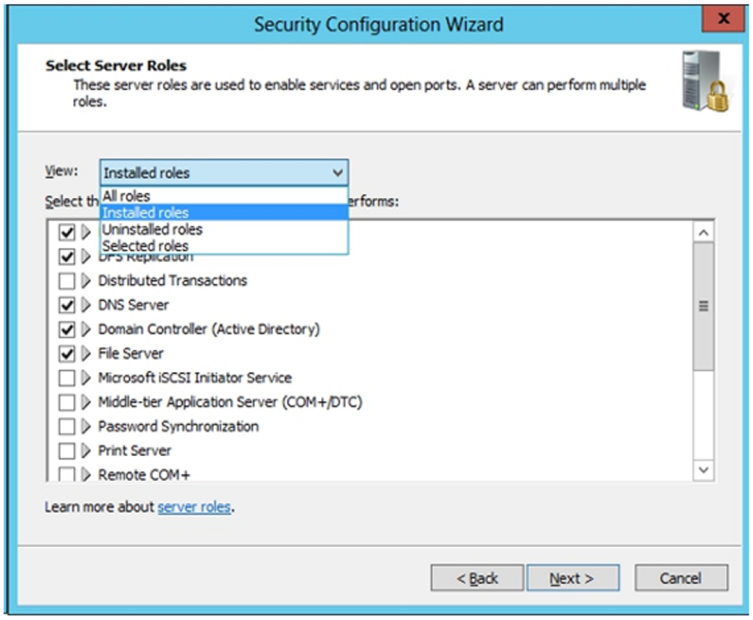
2) Configuració de seguretat de la xarxa.

3) Configuració del registre.

4) Polítiques d'auditoria.

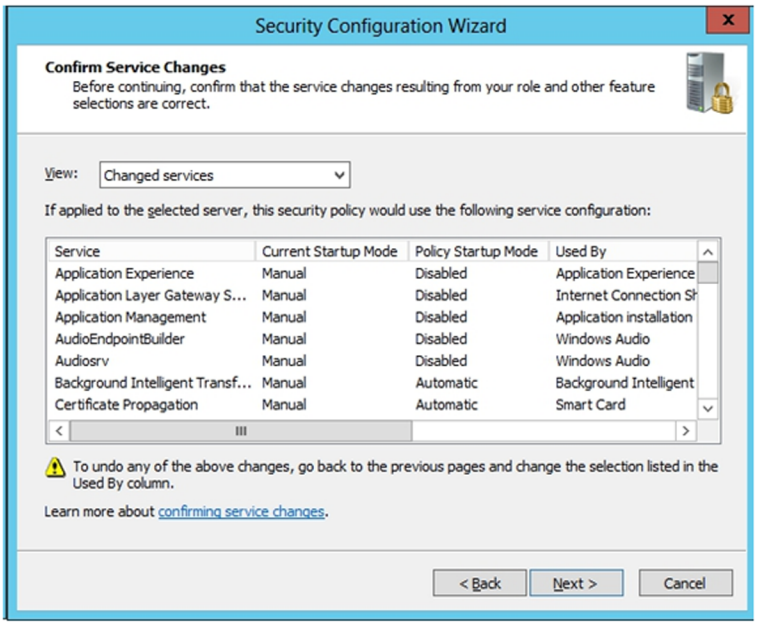
La figura següent ens mostra els papers que l'assistent ha detectat que té el nostre servidor. Si volem, hi afegim els que nosaltres considerem necessaris. Es pot veure com fa una llista dels que troba que estan instal·lats i dels que es poden configurar.

Selecció de papers per fer segurs



El següent que ens mostra l'assistent és quines característiques i programes client ha detectat que utilitza el servidor per a accedir a altres serveis d'altres màquines; hem de triar els que ens sembla que necessitarà el servidor. Alhora, ens ensenya quins programes destinats a l'administració del servidor, com l'RPC, els serveis de còpia de seguretat que obren ports o l'aplicació de polítiques de grups, utilitza el nostre servidor. A més, ens mostra quins serveis aliens al sistema operatiu i a les eines Microsoft tenim en el servidor i ens permet triar quins són vàlids i quins no. Finalment, mostra un resum de les accions que prendrà depenent de les dades que hi acabem d'introduir.

Canvis que aplicarà l'SCW



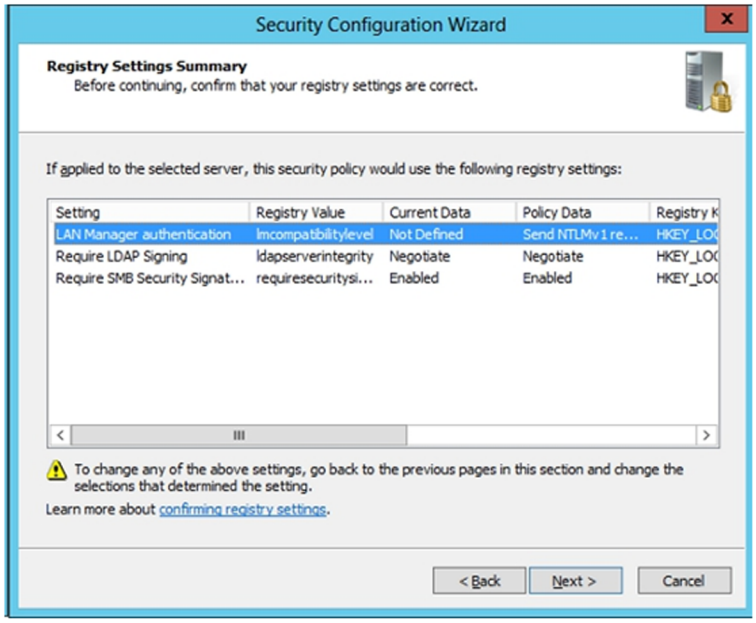
Com veiem en la figura anterior, apaga i deshabilita els serveis que ha detectat que no són necessaris per al funcionament correcte del servidor, i deixa els que són necessaris i els que li hem dit específicament.

A continuació configurarem la part de la configuració de seguretat de la xarxa d'una manera molt similar a l'anterior. Ens mostra les regles a partir dels protocols que fan servir els papers i aplicacions que fan servir la xarxa, i per tant podem aquí bloquejar els protocols i regles perquè no puguin tenir accés a la xarxa.

El punt següent consisteix a protegir la configuració específica de seguretat del registre. Bàsicament, aquestes configuracions serveixen per a protegir la manera com es comuniquen entre si els servidors NT i posteriors, perquè ho facin de manera segura. La primera que ens mostra consisteix a forçar que les comunicacions per SMB (NetBIOS) siguin signades. La pantalla següent demana per les comunicacions contra l'LDAP del directori actiu si també han d'estar signades. La següent és la manera com s'ha de comportar l'autenticació de dominis Windows des del nostre servidor cap a màquines externes.

Al final, ens mostra un resum dels canvis que es faran en el registre segons les dades subministrades.

Canvis en el registre



L'últim punt de l'assistent el constitueix la configuració de la política d'auditories, que serveixen per a mantenir un control exhaustiu dels accessos al servidor, tant de la xarxa com d'arxius. Ho configurem perquè s'auditin les activitats que han tingut èxit i les que no. Així es podran controlar molt més els possibles atacs o manipulacions al sistema que hagin funcionat i els que no.

Finalment, es guarda la configuració de la política en un directori, per a poder recuperar-la posteriorment i s'aplica perquè tingui efecte sobre el servidor en el mateix instant.

Cal comprovar que els serveis de la màquina no han quedat afectats i que continuen funcionant correctament. Tots aquells serveis que abans funcionaven s'han de revisar per si s'ha seleccionat algun protocol malament i s'ha bloquejat el servei. S'ha de remarcar que, com que protegim la xarxa, es canvia la configuració del tallafoc de màquina del servidor, cosa que cal tenir en compte a partir del moment en què s'inicia per si hi volem afegir nous serveis o programes que accedeixin a l'exterior. Si no volem que arrenqui el tallafoc d'estació, s'ha de fer un *skip* de l'apartat de protecció de la xarxa i no configurar aquest punt de l'assistent, tot i que és molt aconsellable configurar correctament aquest punt. Sempre serà millor configurar correctament el tallafoc amb els protocols o ports que s'han de fer servir des de l'exterior, que no pas no tenir-ne cap i deixar el servidor completament vulnerable als atacs de xarxa.

5.4.2. Política d'aplicació de pedaços de seguretat crítics de Microsoft

Tan important com la protecció del sistema és l'actualització sistemàtica de tot el sistema operatiu de Windows amb els pedaços de seguretat crítics que publica periòdicament Microsoft. Es recomana que encara que ens trobem després d'un tallafoc, o incomunicats de l'exterior, es faci aquesta actualització del sistema de manera automàtica mitjançant les actualitzacions automàtiques.

El més recomanable és configurar-ho per a baixar les actualitzacions automàtiques del lloc web de Microsoft i que ens permeti triar quan les volem instal·lar, encara que automatitzar tot el procés en un servidor pot ser perillós, ja que si la instal·lació d'un pedaç requereix reiniciar la màquina es farà de manera automàtica a l'hora especificada. Aquesta opció pot ser bona en estacions de treball, però per a servidors és recomanable ser una mica més conservadors i poder decidir quan volem actualitzar el sistema operatiu. Podem fer que les actualitzacions s'apliquin en el moment en què el servidor no està en ús i que s'apliquin en el moment de reiniciar la màquina. El sistema avisarà que té tasques de manteniment pendent i que s'ha de reiniciar per a fer efectives les actualitzacions pendents.

També es pot afegir al servidor el paper del *Windows server update services* (WSUS), que proporcionarà un servidor d'actualitzacions de pedaços per a tots els ordinadors de l'empresa. Es pot fer un filtratge dels que es considerin que no cal instal·lar, o el que és més important, reduir l'ús de la xarxa a Internet, ja que ara les actualitzacions, en lloc d'anar al servidor de Microsoft per mitjà de l'encaminador i l'IPS, aniran únicament mitjançant la xarxa local Ethernet al servidor WSUS acabat d'instal·lar. En el cas de tenir una petita empresa amb deu ordinadors no ens caldrà fer aquesta instal·lació, però per a empreses grans amb centenars o milers de PC sí que resulta un guany considerable en l'amplada de banda tenir un punt intern d'actualitzacions, ja que només cal baixar els programes i servir-los a tots els altres ordinadors client de la xarxa. Aquests ordinadors s'hauran de configurar perquè vagin a buscar les actualitzacions al servidor intern de l'organització i no als servidors de Microsoft.