

GNU/Linux – Desenvolupaments Intel·ligents

Daniel Alcalá Martínez
ETIS

Joaquín López Sánchez-Montañes

13/06/2011

RESUM

L'empresa Desenvolupaments Intel·ligents es dedica a la creació del software financer i borsari. Actualment esta formada per cinc treballadors. Tot el sistema informàtic esta basat en màquines amb plataformes Microsoft Windows.

En total l'empresa compta amb tretze ordinadors d'escriptori obsolets equipats amb processadors Pentium II i III; i amb sistema operatiu Windows XP, més un servidor de domini equipat amb processador Pentium III i el sistema operatiu Windows NT. Aquet servidor dona servei de fitxers, control de versions, autenticació d'usuaris, cua d'impressió i servidor de backup mitjançant cintes. Fa poc s'ha comprat un nou ordinador amb sistema operatiu GNU/Linux Kubuntu i s'està fent servir com ordinador d'escriptori i com servidor de treball en grup.

L'empresa es troba en procés d'expansió i de reestructuració i s'espera que s'incorporin nous treballadors en les pròximes setmanes. Es volen adquirir nous ordinadors tant per als treballadors que s'incorporaran a l'empresa com per els cinc ja existents. S'ha decidit aprofitar l'ocasió i el moment de reestructuració actual per implementar un nou sistema informàtic basat en GNU/Linux. Aquest és l'objecte d'aquest treball.

El nou sistema informàtic basat en GNU/Linux ha de incloure tots els equips clients (que seran els ordinadors nous) i els servidors (es reaprofitaran els ordinadors antics) cobrint tots els serveis que abans donava el servidors antics mitjançant aquest sistema operatiu i software lliure.

INDEX

1. INTRODUCCIÓ	6
1.1.1. ¿Que és GPL?	6
1.1.2. ¿Que és GNU?	6
1.1.3. ¿Que és el programari lliure?	6
1.1.4. ¿Que és la Free Software Foundation?	7
1.1.5. ¿Qui és Richard Stallman?	7
1.1.6. ¿Qui és Linus Torvalds?	7
1.1.7. ¿Qui és GNU/Linux?	8
1.2. Justificació del TFC	8
1.2.1. Punt de partida del TFC	8
1.2.2. Aportació del TFC	8
1.3. Descripció del TFC	9
1.4. Objectius del TFC	9
1.5. Enfocament i mètode a seguir	10
1.6. Planificació del TFC	11
1.7. Producte obtingut i dades generals	12
1.8. Breu descripció dels altres capítols	14
2. Estudi i elecció de distribucions GNU/Linux i software lliure	15
2.1. Estudi i recerca sobre distribucions GNU/Linux orientades a servidors. Tria de la distribució adequada per als servidors	15
2.2. Alternatives lliures als serveis de l'empresa	16
2.3. Estudi i recerca sobre distribucions GNU/Linux per als equips d'escriptori. Tria de la distribució adequada per als equips d'escriptori	17
2.4. Alternatives lliures al programari de l'empresa	17
3. Configuració comuns a tots els servidors i equips d'escriptori	18
3.1. Configuració comú a tots els servidors	18
3.1.1. Instal·lació de openSSH per administració remota	18
3.2. Configuració comuna a servidors i equips d'escriptori	19
3.2.1. Configuració de resolució de noms	19
4. Implementació del servidor PDC	19
4.1. Configuració pre-implementació del PDC	19
4.2. Instal·lació i configuració del servidor LDAP	20

4.2.1.	Configuració de l'estructura LDAP de l'empresa i creació d'usuaris i grups	21
4.2.2.	Prova de funcionament de LDAP	25
4.3.	Instal·lació i configuració del servidor Samba	25
4.3.1.	Configuració i integració de Samba amb LDAP	25
4.4.	Configuració del PDC per autenticar usuaris	28
4.5.	Prova d'autenticació d'un usuari del LDAP en un ordinador d'escriptori	29
5.	Implementació del servidor d'arxius	30
5.1.	Configuració de Samba com servidor d'arxius	30
5.2.	Implementació i configuració de les carpetes compartides	31
5.3.	Prova d'accés a les carpetes compartides des d'un ordinador d'escriptori	32
6.	Implementació del servidor d'impressió	33
6.1.	Configuració de Samba com servidor d'impressió amb CUPS	33
6.2.	Instal·lació d'impressora	34
6.3.	Prova d'accedir a la impressora compartida des de un ordinador d'escriptori	34
7.	Implementació del servidor de correu	35
7.1.	Instal·lació del servidor MTA Postfix (SMTP)	35
7.2.	Instal·lació i configuració de Dovecot (IMAP, POP3)	38
7.3.	Instal·lació i configuració de Squirrelmail (IMAP, webmail)	39
7.4.	Instal·lació i configuració de servei antiSpam i antivirus	40
7.4.1.	Configuració de ClamAV	40
7.4.2.	Configuració de Spamassassin	40
7.4.3.	Configuració de Amavisd-new	41
7.4.4.	Integració amb Postfix	41
7.5.	Prova d'enviament i recepció de correu entre usuaris	42
8.	Implementació del servidor de versions	43
8.1.	Instal·lació i configuració de CVS	43
9.	Implementació del servidor de documentació	44
9.1.	Instal·lació i configuració de MoinMoin	44
9.2.	Prova d'accés al servidor de documentació des de un client	46
10.	Implementació del servidor BDC	46
10.1.	Configuració de l'LDAP de PDC per sincronitzar amb l'LDAP del BDC	46
10.2.	Configuració de l'LDAP de BDC per sincronitzar amb l'LDAP del PDC	48
10.3.	Instal·lació i configuració de Samba per sincronitzar amb el PDC	48
11.	Implementació del servidor proxy	49

11.1.	Instal·lació i configuració d'Squid	49
11.2.	Restricció de llocs web.....	50
11.3.	Prova de servidor proxy.....	50
12.	Implementació del Firewall.....	51
12.1.	Activació i configuració del tallafocs	51
13.	Implementació del servidor VPN:.....	52
13.1.	Instal·lació del servidor VPN.....	52
13.2.	Creació de certificats per als servidor VPN.....	52
13.3.	Creació de certificat per als clients.....	53
13.4.	Configuració del servidor VPN.....	54
13.5.	Configuració del client VPN	55
14.	Implementació del servidor Web	55
14.1.	Instal·lació i configuració del servidor Web	55
14.2.	Prova del servidor Web des de una ordinador d'escriptori	56
15.	Configuració dels ordinadors d'escriptori	56
15.1.	Configurar l'ordiandor per autenticar-se contra el domini.....	56
15.2.	Configuració per exportar el home de l'usuari del servidor de domini.	57
15.3.	Configuració del servidor proxy.....	58
16.	Glossari.....	58
16.1.	Glossari.....	58
17.	Bibliografia:.....	61
17.1.	Bibliografia.....	61

1. INTRODUCCIÓ

1.1.1. ¿Que és GPL?

GNU és un acrònim recursiu de l'anglès "GNU's Not Unix" ("GNU no és Unix"). Va ser iniciat per Richard Stallman amb l'objectiu de crear un sistema operatiu lliure: el sistema GNU. El 27 de setembre de 1983 es va anunciar públicament el projecte per primera vegada al grup de notícies net.unix-wizards. A l'anunci general, van seguir diversos escrits de Richard Stallman, com el "Manifest GNU", que van establir les seves motivacions per realitzar el projecte GNU, entre les quals destaca "retornar a l'esperit de cooperació que hi havia als temps inicials a la comunitat d'usuaris d'ordinadors".

UNIX és un sistema operatiu privatiu molt popular, perquè està basat amb una arquitectura que ha demostrat ser tècnicament estable. El sistema GNU va ser dissenyat per ser completament compatible amb UNIX. El fet de ser compatible amb l'arquitectura UNIX implicà que GNU està compost de petites peces individuals de programari, moltes de les quals ja estaven disponibles, com el sistema d'edició de texts Tex i el sistema gràfic X Window, que van poder ser adaptats i reutilitzats; altres, en canvi es van haver de tornar a escriure.

Per assegurar que el programari de GNU fos sempre lliure perquè tots els usuaris el poguessin "executar, copiar, modificar i distribuir", el projecte havia de ser llançat sota una llicència dissenyada per garantir aquests drets i que evités les restriccions posteriors dels mateixos. La idea en anglès es coneix com a copyleft (en clara oposició al copyright), i està contingut a la llicència GPL.

1.1.2. ¿Que és GNU?

La Llicència Pública General GNU (GNU GPL, de l'anglès GNU General Public License) és un tipus de llicència per a programari que permet la còpia, distribució (comercial o no) i modificació del codi, sempre que qualsevol modificació es continui distribuint amb la mateixa llicència GPL. La llicència GPL no permet la distribució de programes executables sense el codi font corresponent o una oferta de com obtenir-lo gratuïtament.

Aquesta llicència va ser dissenyada originalment per Richard Stallman i el grup GNU, principalment Eben Moglen, com a alternativa al model de programari propietari predominant. Actualment, Linux és el programa sota llicència GPL amb més difusió.

1.1.3. ¿Que és el programari lliure?

El programari lliure (en anglès free software) és el programari que pot ser usat, estudiat i modificat sense restriccions, i que pot ser copiat i redistribuït bé en una versió modificada o sense modificar sense cap restricció, o bé amb unes restriccions mínimes per garantir que els futurs destinataris també tindran aquests drets.

Com que el programari es pot redistribuir lliurement, en general es pot trobar gratuïtament a Internet, o a un cost baix si l'adquirim per mitjà d'altres medis (CD-Rom, DVD, disquets...). A causa d'això, els models de negoci basats en programari lliure normalment es basen en proporcionar serveis de valor afegit com suport tècnic, cursos de preparació, personalització, integració, o certificació.

En general, es pot dir que un programa és lliure si permet les quatre llibertats definides per la Free Software Foundation:

- La llibertat d'executar el programa per qualsevol propòsit (llibertat 0).
- La llibertat de veure com funciona el programa i adaptar-lo a les necessitats pròpies (llibertat 1). L'accés al codi font és un requisit.
- La llibertat de redistribuir còpies (llibertat 2)

- La llibertat de millorar el programa i de distribuir-lo de nou amb les millores realitzades, per tal que tota la comunitat se'n pugui beneficiar (llibertat 3). Igual que a la llibertat 1, l'accés al codi font és un requisit.

1.1.4. ¿Que és la Free Software Foundation?

La Free Software Foundation (FSF) ("fundació pel programari lliure") és una iniciativa de Richard Stallman en defensa del programari lliure i en particular del projecte GNU.

Des de la seva fundació fins al la meitat dels anys 90 els fons de la FSF es van fer servir majoritàriament en ocupar programadors per escriure programari lliure. Atès que a partir de mitjans anys 90 i fins a la actualitat una multitud de companyies i individus s'han dedicat a escriure programari lliure, els empleats i voluntaris de la FSF treballen en els aspectes legals i estructurals de la comunitat pel programari lliure.

1.1.5. ¿Qui és Richard Stallman?

Richard Matthew Stallman (de nom en clau RMS) és un conegut activista del programari lliure.

Les seves obres més importants com a programador inclouen l'editor de text Emacs, el compilador GCC i el depurador GDB, sota el Projecte GNU. Però la seva influència és major en un marc moral, polític i legal pel moviment del programari lliure, com una alternativa al desenvolupament i distribució del programari privatiu. També és l'inventor del concepte Copyleft (tot i que no és ell qui li va posar nom), un mètode per llicenciar el programari perquè sigui sempre de lliure ús i modificació.

1.1.6. ¿Qui és Linus Torvalds?

Linus Benedict Torvalds (28 de desembre de 1969) és un informàtic finlandès (de la minoria sueca), creador i actual mantenidor del nucli Linux.

En la seva època d'estudiant universitari a Hèlsinki, a finals del setembre del 1991, començà la creació del nucli (o kernel) d'un sistema operatiu, ja que no podia fer front al preu dels sistemes Unix de l'època. Originalment, Linus va anomenar el seu projecte Freex (referint-se a un sistema Unix lliure, mentre que en anglès es pronunciaria igual que freaks), però finalment el va publicar amb el nom de Linux (mesclant el seu nom Linus amb Unix). Linus va involucrar molta més gent a través d'un missatge electrònic que va enviar a una llista de notícies electròniques (news), que per aquella època era el màxim exponent d'Internet. Al cap de poc, la primera versió va ser millorada i ampliada per altres informàtics de tot el món, que van poder llegir el codi font de Linux i, per tant, millorar-lo. En l'actualitat viu a Silicon Valley i encara col·labora amb milers de persones de tot arreu, treballant per millorar i adequar als nous temps el nucli Linux, organitzant-se per correu electrònic. Linux, que és distribuït lliurement amb llicència GPL, ha estat incorporat com a part fonamental de moltes distribucions de programari.

Les seves obres més importants com a programador inclouen l'editor de text Emacs, el compilador GCC i el depurador GDB, sota el Projecte GNU. Però la seva influència és major en un marc moral, polític i legal pel moviment del programari lliure, com una alternativa al desenvolupament i distribució del programari privatiu. També és l'inventor del concepte Copyleft (tot i que no és ell qui li va posar nom), un mètode per llicenciar el programari perquè sigui sempre de lliure ús i modificació.

1.1.7. ¿Qui és GNU/Linux?

Linux o GNU/Linux, és el sistema operatiu format pel nucli del sistema o kernel Linux, juntament amb les utilitats GNU. Avui en dia, hi ha moltes distribucions de programari basades en aquest sistema operatiu.

El kernel Linux va néixer en el 1991 a Hèlsinki quan Linus Torvalds va implementar un clon de UNIX basant-se en el seu coneixement del sistema operatiu Minix i les seves limitacions per tal d'aplicar-les a les noves possibilitats de gestió de memòria en mode protegit dels processadors Intel 386, una arquitectura molt comuna a l'any 1991 i amb millores substancials respecte anteriors versions de PCs i de les quals Minix no en treia profit. Les utilitats GNU, necessàries per tenir un sistema operatiu complet, tenen el seu origen en el projecte de Richard Stallman de crear un sistema operatiu lliure, que va començar el 1983, la Free Software Foundation.

Aquest sistema operatiu va créixer gràcies al treball col·laboratiu de programadors de tot el món, els quals se sumaren a la crida per a desenvolupadors que en Linus Torvalds va realitzar en quant va fer pública la primera versió del nucli del sistema operatiu.

Stallman insisteix que el nom correcte per aquest tipus de sistema operatiu és GNU/Linux, ja que les utilitats GNU són essencials pel seu funcionament. A la pràctica, la majoria de distribuïdors i usuaris utilitzen només el terme Linux per referir-se al sistema operatiu complet, bé per comoditat, o perquè consideren que el nucli és la part més rellevant i la que ha de donar nom al sistema. La majoria de distribucions utilitzen el terme "linux" per referir-se al sistema operatiu, tot i que n'hi ha que utilitzen "GNU/Linux"

1.2. Justificació del TFC

Des de ja fa temps em rondava pel cap la idea de aprendre o fer algun tipus de projecte a nivell acadèmic i personal del que seria una estructura i un sistema informàtic en una empresa basat en GNU/Linux ja que solament he tingut la oportunitat de treballar a nivell professional amb sistemes Microsoft Windows. Quan vaig llegir la proposta de TFC anomenada "Desenvolupaments Intel·ligents" i que proposava justament un projecte similar, vaig tenir clar que aquest seria el meu TFC.

1.2.1. Punt de partida del TFC

Els meus coneixements sobre GNU/Linux son a nivell d'usuari domèstic. A més, per una cosa o un altre, des de feia anys no havia tingut cap contacte amb GNU/Linux. Fa poc, em vam fer un curs de GNU/Linux bàsic a la feina que va fer que em retornés l'interès per aquest sistema operatiu i em va encoratjar a escollir el TFC sobre aquest tema.

1.2.2. Aportació del TFC

Crec que aquest TFC m'aportarà coneixements sobre els sistemes GNU/Linux a nivell d'una estructura i un sistema informàtic d'una empresa basat en GNU/Linux i els seus servidors i que em pot ser de gran utilitat de cara a la meua carrera professional. A més, em donarà l'impuls i l'interès per aprofundir més a fons sobre els temes explorats i altres relacionats ja que en tres mesos que dura la realització del TFC no es pot veure tot. Tot i això crec que la aportació de coneixements d'aquest TFC serà molt gran en comparació als coneixements d'inici.

1.3. Descripció del TFC

L'empresa Desenvolupaments Intel·ligents es dedica a la creació de software financer i borsari. Actualment esta formada per cinc empleats:

- Dos caps analistes/programadors
- Un analista/programador.
- Una secretaria/administrativa/recepcionista
- Un administrador de sistemes/web.

L'empresa es troba en procés d'expansió i es preveu que en els pròxims mesos es faran noves incorporacions de treballadors. El local disposa de tretze llocs de treball dels qual vuit estan lliures i, per tant, disponibles per ser ocupats.

La remesa actual d'ordinadors d'escriptori i servidors es troba obsoleta. Es compta amb els següents equips:

- Tretze ordinadors d'escriptori obsolets amb processador Pentium II i III i amb sistema operatiu Microsoft Windows XP.
- Un ordinador nou amb sistema operatiu Kubuntu GNU/Linux. Aquest equip es fa servir com a ordinador d'escriptori i també com a servidor de treball en grup.
- Un servidor obsolet amb processador Pentium III amb el sistema operatiu Windows NT 4. Fa la funció de servidor d'arxius, control de versions, autenticació d'usuaris, servidor d'impressió i servidor de backup de dades mitjançant cintes

A més, es disposa de dos servidors subcontractats a una empresa externa que donen servei de correu electrònic i de servei web a la nostra empresa. La web informativa de l'empresa s'allotja en aquest servidor web.

Es disposa de dos línies ADSL amb IP fixa i una línia de FAX gestionada per un mòdem/fax instal·lat en l'ordinador de la secretaria.

1.4. Objectius del TFC

L'objectiu general d'aquest projecte és reemplaçar els ordinadors d'escriptori Pentium II i II obsolets per ordinadors Pentium Core 2 Duo nous. Alguns d'aquets ordinadors antics seran reaprofitats com a servidors per donar els serveis necessaris per l'empresa. Tant la implementació dels nous entorns d'escriptori com dels servidor i totes aplicacions i serveis oferts és faran mitjançant el sistema operatiu GNU/Linux i software lliure.

En la reestructuració dels serveis oferts per els servidor s'han definit els següents objectius específics:

- Implementar un servidor GNU/Linux amb OpenLDAP i Samba que faci de PDC (Primari Domain Controller) que ofereixi els següents serveis:
 - Autenticació d'usuaris de forma centralitzada.
 - Servidor de fitxers.
 - Control de versions.
 - Gestió de documentació.
 - Servidor de correu (antivirus i antispam).

- Implementar un servidor BDC (Backup Domain Controller) que serveixi de backup al PDC per que els usuaris puguin continuar autenticar-se en cas caiguda del servidor principal. A més es replicaran els serveis que ofereix el PDC que sigui possible.
- Tant el PDC com el BDC emmagatzemarem el gros de les dades de l'empresa i solament s'accedirà des de la nostra xarxa interna.
- Implementar un servidor web que doni servei a 20 clients (mínim). Té que ser accessible per els empleats des de dintre i des de fora de la xarxa interna. Inclourà la pagina web, el sistema egrounware i farà servir la cinta com a copia de seguretat. S'estudiarà la possibilitat de reaprofitar el servidor antic Windows NT 4.
- Implementar un servidor amb la funció de Proxy, Firewall i VPN que doni accés als usuaris amb portàtils des de fora de l'empresa. Els empleats tindran accés a internet, però es vol mantenir un cert control de filtratge i tenir la possibilitat de restringir certs llocs.
- Els nous equips d'escriptori amb sistema operatiu GNU/Linux i amb totes les aplicacions i clients basats en software lliure treballaran contra aquests nous servidors.
- Els nous servidor s'implementaran aprofitant els ordinadors antics de escriptori especialment triats per aquesta qüestió. Els ordinador sobrants, s'aprofitaran per a proves de desenvolupament o de sistemes.

1.5. Enfocament i mètode a seguir

Degut a que actualment solament treballen cinc treballadors a l'empresa i després de valorar la situació, he desestimat un tipus de migració que impliqués la migració de comptés d'usuari del domini NT, bústies de correu (que son a un servidor extern), permisos NTFS, etc del sistema informàtic basat en Windows cap al nou basat en GNU/Linux. No faré conivure plataformes Windows i GNU/Linux i no aniré migrant els diferents recursos i serveis, sino que es muntarà tota la nova estructura des de zero. Crec que tenint solament cinc usuaris no val la pena complicar-se tant i acabaria sent més una molèstia que no una ajuda. També crec que el resultat final serà més ajustat al que el nosaltres volem.

El mètode a seguir consistirà en un primera etapa de preproducció on aniré muntant i provant tota la nova estructura i sistema informàtic totalment basada en GNU/Linux en paral·lel a la actual basada en Windows. Serà una etapa totalment transparent per als usuaris que continuaran treballant tranquil·lament com sempre amb els seus sistemes Windows.

Quan estigui totalment preparada i provada la nova estructura i sistema informàtic GNU/Linux, es passarà a la etapa de producció on els usuaris començaran a treballar amb el nova sistema informàtic, tant a nivell de servidor com a màquines d'escriptori, i deixaran de fer-ho amb el sistema basat en Windows que estarà inoperatiu però encara present físicament durant un temps de prova prudencial per si hi ha cap problema inesperat.

Una vegada passat el període de prova, es trauran definitivament totes les màquines basades en Windows i haurem arribat a la fi del nostre projecte.

1.6. Planificació del TFC

Etapa d'estudi i recerca:

#	Fita	Data Inici	Data Final	Total dies laborables	%	∑%
1	Estudiar i decidir quina distribució de GNU/Linux és la més adequada per als nous ordinadors d'escriptori	28/03/11	29/03/11	2	3,8%	3,8%
2	Estudiar quines aplicacions GNU/Linux substituiran a les anteriors aplicacions Windows que feina servir els usuaris	30/03/11	31/03/11	2	3,8%	7,7%
3	Estudiar i decidir quina distribució de GNU/Linux és la més adequada per als nous servidors.	01/04/11	04/04/11	2	3,8%	11,5%
4	Estudiar quines aplicacions de serveis GNU/Linux substituiran a les anteriors aplicacions de serveis Windows que donaven els anteriors servidors. També caldrà fer l'estudi sobre els nous serveis.	05/04/11	06/04/11	2	3,8%	15,4%

Etapa de preproducció:

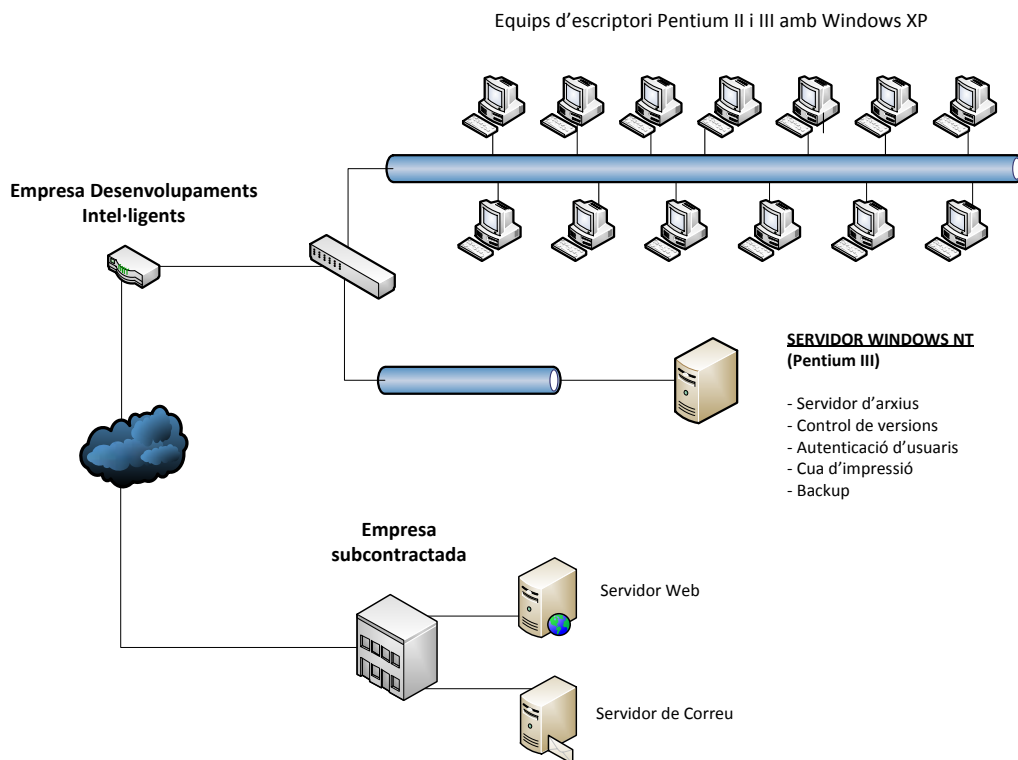
#	Fita	Data Inici	Data Final	Total dies laborables	%	∑%
5	Instal·lar el servidor GNU/Linux que serà el PDC.	07/04/11	07/04/11	1	1,9%	17,3%
6	Instal·lar els serveis LDAP amb OpenLDAP i SMB amb Samba al servidor PDC per oferir autenticació dels usuaris del domini.	08/04/11	14/04/11	5	9,6%	26,9%
7	Implementar aplicació de control de versions al PDC.	15/04/11	19/04/11	3	5,8%	32,7%
8	Implementar el gestor de documentació al PDC	20/04/11	26/04/11	3	5,8%	38,5%
9	Implementar el servei de correu (antivirus i antispam) al PDC.	27/04/11	02/05/11	4	7,7%	46,2%
10	Implementar el servei de cues d'impressió al PDC.	03/05/11	04/05/11	2	3,8%	50%
11	Implementar un servidor BDC de backup del PDC amb tots el seus serveis replicats: servei de OpenLDAP, Samba, aplicació de control de versions, el gestor de documentació, servei de correu i servei de cues d'impressió.	05/05/11	12/05/11	6	11,5%	61,5%
12	Implementar el servidor web.	13/05/11	17/05/11	3	5,8%	67,3%
13	Implementar el servidor Firewall, proxy, vpn.	18/05/11	24/05/11	5	9,6%	76,9%

Etapa de producció:

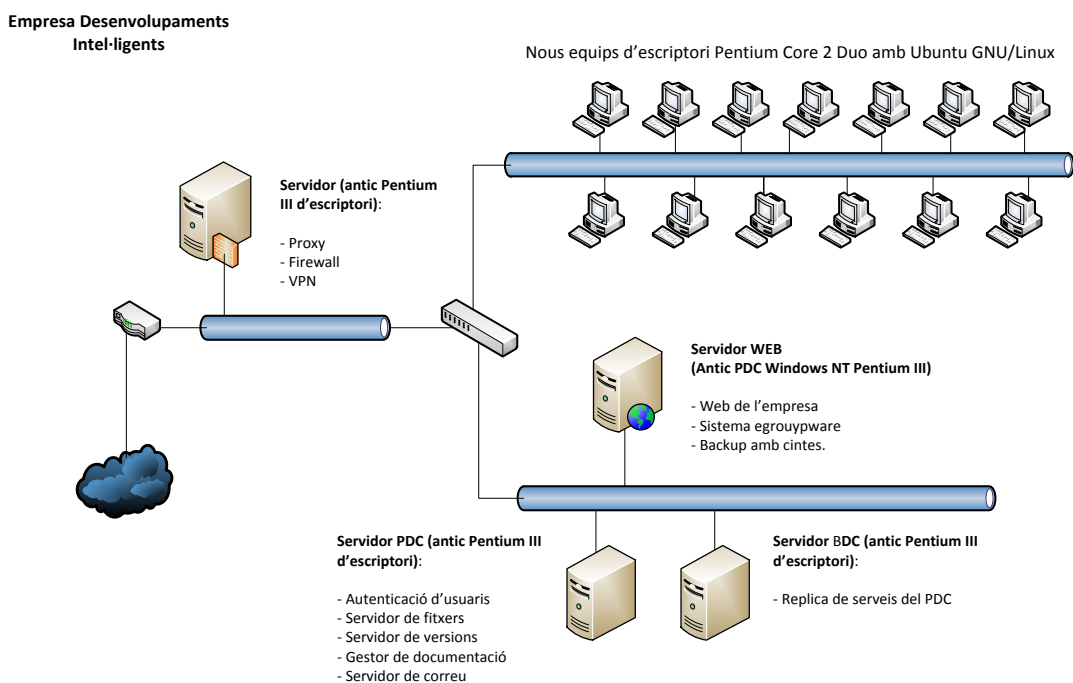
#	Fita	Data Inici	Data Final	Total dies laborables	%	∑%
14	Migració dels ordinadors d'escriptori restants al nou entorn GNU/Linux.	25/05/11	30/05/11	4	7,7%	84,6%
15	Apagada dels servidors antics i basats en Windows	31/05/11	31/05/11	1	1,9%	86,5%
16	Període de proves de la nova estructura de sistemes d'ordinadors d'escriptori i servidors GNU/Linux implementada al 100%.	01/06/11	08/06/11	5	9,6%	96,2%
17	Retirada definitiva dels antics servidors Windows que quedin funcionant.	09/06/11	10/06/11	2	3,8%	100%

1.7. Producte obtingut i dades generals

Al següent esquema es pot veure una representació de la estructura i sistema informàtic inicial basat en plataformes Windows:



El producte que volem obtenir, com ja s'ha explicat, es una nova estructura i sistema informàtic basat en GNU/Linux com representa el següent esquema i les següents taules:



Dades sobre la xarxa LAN:

Xarxa de l'empresa	192.168.1.0/24
Rang destinat a servidors	192.168.1.11 – 192.168.1.65
Rang destinat a ordinadors d'escriptori	192.168.1.65 – 192.168.1.199
Rang destinat a impressores i perifèrics	192.168.1.200 – 192.168.1.254
Domini	desint.local

Assignació d'IPs i noms:

Nom de màquina	Nom al domini	IP
pdcc	pdcc.desint.local	192.168.1.11
bdc	bdc.desint.local	192.168.1.12
proxy	proxy.desint.local	192.168.1.10
www	www.desint.local	192.168.1.13
client1	client1.desint.local	192.168.1.65
client2	client2.desint.local	192.168.1.66
client3	client3.desint.local	192.168.1.67
client4	client4.desint.local	192.168.1.68
client5	client5.desint.local	192.168.1.69
printer	printer.desint.local	192.168.1.200

Usuaris i grups:

Nom usuari	Càrrec	Usuari de xarxa	Grup
Leo Messi	Cap Analista/Programador	lmessi	CAPS
Xavi Hernández	Cap Analista/Programador	xhernandez	CAPS
David Villa	Analista/Programador	dvilla	PROGRAMADORS
Cristiana RONALDA	Secretaria administrativa	cronalda	ADMINISTRATIUS
Daniel Alcalá Martínez	Administrador de sistemes/web	dalcalam	SISTEMES

Recursos compartits:

Recursos compartits	Propietari	Grup amb permisos per accedir i permisos RW	Usuaris membres del grup.
/srv/Samba/share/sistemes	dalcalam	SISTEMES	dalcalam
/srv/Samba/share/programadors	dvilla	PROGRAMADORS	dvilla
/srv/Samba/share/caps	lmessi	CAPS	lmessi, xhernandez
/srv/Samba/share/administratius	cronalda	ADMINISTRATIUS	Cronalda
/srv/Samba/share/printers	Dalcalam	TOTS	TOTS

Bústies de correu:

Nom usuari	Càrrec
Leo Messi	lmessi@deisnt.local
Xavi Hernández	xhernandez@desint.local
David Villa	dvilla@@desint.local
Cristiana RONALDA	cronalda@desint.local
Daniel Alcalá Martínez	dalcalam@desint.local

1.8. Breu descripció dels altres capítols

- **Capítol 1 – Introducció:** Introducció al món GNU/Linux i el software lliure.
- **Capítol 2 – Estudi i elecció de distribucions GNU/Linux i software lliure:** Estudi de la millor distribució Linux per als servidor i equips d'escriptori. Elecció del software lliure que substituirà als software propietari.
- **Capítol 3 – Configuració comú a servidors i equips d'escriptori:** Configuració comú a tots el servidor, a tots els equips d'escriptori o a tot dos.
- **Capítol 4 – Implementació del servidor PDC:** Implementació del servidor controlador primari de domini mitjançant OpenLDAP y Samba.
- **Capítol 5 – Implementació del servidor d'arxius:** Implementació del servidor d'arxius amb Samba. Compartir carpetes i assignar permisos.
- **Capítol 6 – Implementació del servidor d'impressió:** Implementació del servidor d'impressió. Instal·lar i compartir impressora.
- **Capítol 7 – Implementació del servidor de correu:** Implementació del servidor de correu SMTP, IMAP i el webmail Squirrelmail.
- **Capítol 8 – Implementació del servidor de versions:** Implementació del sistema de control de versions dels fitxers.
- **Capítol 9 – Implementació del servidor de gestió de documentació:** Implementació del gestor de documentació de l'empresa amb MoinMoin.
- **Capítol 10 – Implementació del servidor BDC:** Implementació del servidor backup de controlador de domini. Replicarà els serveis que sigui possible del PDC.
- **Capítol 11 – Implementació del servidor Proxy:** Implementació del servidor que accedirà a internet en nom dels altres equips i controlarà els accessos a webs.
- **Capítol 12 – Implementació del Firewall:** Implementació del control de les comunicacions entrants i sortints de l'empresa.
- **Capítol 13 – Implementació del servidor VPN:** Implementació de la xarxa privada virtual per connexions des de l'exterior a la nostra LAN.
- **Capítol 14 – Implementació del servidor Web:** Implementació del servidor Web amb Apache i amb la web de la empresa.

- **Capítol 15 – Configuració dels equips d’escriptori:** Configuració dels ordinadors dels usuaris. Accediran als serveis oferts per els servidors.
- **Capítol 16 – Glossari:** Definició de termes i conceptes.
- **Capítol 17 – Bibliografia:** Referències consultades.

2. Estudi i elecció de distribucions GNU/Linux i software lliure

En aquest capítol s’estudia les diferents distribucions de GNU/Linux disponible i quina serà la més apropiada tant per als nostres servidor com per als equips d’escriptori. També es fa un estudi sobre les eines i serveis que es fan servir a l’empresa i quines eines de software lliure podem fer servir per substituir-les.

2.1. Estudi i recerca sobre distribucions GNU/Linux orientades a servidors. Tria de la distribució adequada per als servidors

Aquest estudi s’ha començat des del un punt de partida on el meu desconeixement sobre distribucions de GNU/Linux orientades a servidors o que, tot era inexistent. He comença cercant informació per internet, tant dels llocs web oficials de les distribucions com de molts fòrums existents a internet. Aquests últims m’han ajudat molt ja que la opinió i la experiència d’altres administradors de sistemes ha sigut determinant en fer una petita llista de distribucions candidates a ser l’elegida:

- Debian.
- Ubuntu Server Edition.
- Red Hat Enterprise.
- CentOS.
- Suse Enterprise.
- openSUSE.
- Fedora.
- Gentoo.

Com es pot veure, no totes les distribucions de la llista son orientades exclusivament a servidor com Gentoo, Fedora o CentOS però que son molt recomanades per aquesta fita.

En un primer escrutini, descartem Red Hat Enterprise i Suse Enterprise per ser de pagament. Son dos fantàstiques distribucions però no val la pena pagar per elles si no es que les hem d’instal·lar en grans granges de servidors. Per als nostres petits servidor de la nostra PYME tenim de sobra amb les distribucions gratuïtes. A més tenim CentOS que és un clon binari de Red Hat Linux compilat a partir del codi font alliberat per Red Hat i també comptem amb openSUSE que és la versió de codó obert de Suse Enterprise.

A l’hora de comparar les distribucions restants m’he trobat amb la sorpresa que no hi ha gaires diferències entre elles a quant als nostres objectius. Personalment m’esperava més diferències entre unes i altres o que estiguessin més orientades o especialitzades en uns tipus de servidors en concret. Però la realitat és que qualsevol d’aquestes seria una bona de decisió per implementar el nostres servidors per la nostra petita empresa i que aquests s’implementen de forma molt semblant amb solament petites diferències entre unes distribucions i altres segons la documentacions oficials.

Un primer requisit que té que complir la nostra distribució és el seu consum de recursos sigui petit ja que tenen que corre sobre ordinadors Pentium II o III. Un altra vegada em trobo que son molt semblants en quant als

recursos que requereixen. Requereixen un mínim de 64 MB de RAM i uns 600 MB de disc dur per una instal·lació mínima i sense X-Windows. A partir d'aquí els requisits poden augmentar fins 256 MB i uns 1GB - 2GB si volem fer servir X-Windows i instal·lar més paquets addicionals. Tot i que aquest requeriments poden augmentar segons les nostres necessitats com és lògic.

En quant a documentació també es troben molt parelles però en destaquen Debian amb una fantàstica documentació oferta per la comunitat Debian, Ubuntu també amb una fantàstica documentació oferta per Canonical Ltd, CentOS compatible al 100% amb la nombrosa documentació de Red Hat Enterprise i openSUSE que es troba en el mateix cas davant Suse Enterprise.

Tot i això hi ha dues distribucions que em criden més l'atenció: Debian 6.0.1 squeeze i Ubuntu server Enterprise 10.04 LTS. Els motius són els següents:

- **Debian 6.0.1 squeeze:** És la versió estable i recomanada per Debian. No compta amb els paquets més actualitzats en comparació amb altres distribucions però això mateix fa que estigui un esglaó per sobre de la resta en quant a estabilitat ja que tot està més que testejat. És considerada per molts la versió més estable. Això la fa atractiva per fer-la servir en els nostres servidors ja que la estabilitat és una característica molt desitjable. També compta amb una fantàstica documentació.
- **Ubuntu Server Edition 10.04 LTS:** És una distribució Linux basada en Debian que proporciona un sistema operatiu actualitzat i estable, amb un fort enfocament en la facilitat d'ús i instal·lació del sistema. Està patrocinat per Canonical Ltd., una companyia britànica propietat de l'empresari sud-africà Mark Shuttleworth. Tot i que Canonical comercialitza amb el suport tècnic d'Ubuntu, tant el sistema operatiu com la seva fantàstica documentació són mantinguts i oferts de forma gratuïta.

Les versions LTS (Long Time Support) compten amb un suport per part de Canonical Ltd de cinc anys. Lo que la fa molt atractiva per fer-la servir en els nostres servidors.

Per provar les dues he fet la instal·lació d'OpenLDAP en les dues respectives distribucions i m'he trobat que són molt semblants. Tot i això, seguint la documentació d'instal·lació d'OpenLDAP de Debian m'he trobat amb algun problema com per exemple trobar-me que l'arxiu `/etc/ldap/sldap.conf` no es troba on diu la documentació i tot i trobar-lo, editar-lo i copiar-lo també a la carpeta correcta no ha funcionat trobant-me una mica deseparat. Amb Ubuntu Server no he tingut aquest problema. Seguint la seva documentació oficial he pogut implementar el servidor OpenLDAP amb no més dificultats que barallar-me amb les meves pròpies mancances de coneixements.

Per aquest motiu i per que Ubuntu server al ser una versió LTS (Long Time Support) i, per tant, tenim suport per part de Canonical Ltd de cinc anys, finalment decideixo que **Ubuntu Server Enterprise 10.04 LTD** és la distribució triada per implementar els nostres servidors.

2.2. Alternatives lliures als serveis de l'empresa

A la següent taula s'especifiquen els serveis amb el que té que comptar la nostra empresa, els software propietari que s'ha fet servir fins ara i la alternativa basada en software lliure i GNU/Linux que hem d'implementar.

SERVEI	SOFTWARE PROPIETARI	SOFTWARE LLIURE
Domini	Microsoft Windows NT	OpenLDAP, Samba
Autenticació d'usuari	Microsoft Windows NT	OpenLDAP, Samba
Control de versions	Microsoft SourceSafe	CVS
Servidor d'arxius	Microsoft RDP, SMB, CIFS	Samba, NFS
Backup	Microsoft MSBackup	Dump, Restore
Cues impressió	Microsoft spool service (Windows NT)	CUPS
Gestió de documentació	Microsoft Sharepoint	MoinMoin
Web	Subcontractat	Apache
Correu	Subcontractat	Postfix, Dovecot, Squirrelmail, Amavis-new, Spamassassin, ClamAV

2.3. Estudi i recerca sobre distribucions GNU/Linux per als equips d'escriptori. Tria de la distribució adequada per als equips d'escriptori.

Com a l'hora de triar una distribució GNU/Linux per als nostres servidors, també he començat buscant informació per internet, tant dels llocs web oficials de les distribucions com de molts fòrums existents a internet per a triar una distribució per als nostres equips d'escriptori. Els més recomanats per als fòrums són Ubuntu, Fedora, Debian, Mandriva, Mint, openSUSE, Arch, Sabayon, CentOS, etc. Tenim un munt. Qualsevol d'aquestes distribucions seria una bona elecció ja totes tenen els software que necessitem en els seus repositoris.

Una característica important que ha de complir la nostra distribució és que estigui orientada a l'usuari final i que un usuari procedent de Windows es pugui adaptar fàcilment. En els fòrums d'internet molta gent recomana Ubuntu, Mandriva i Mint per aquests propòsits. Segons <http://distrowatch.com/>, Ubuntu és la distribució més emprada pels usuaris, seguida de Mint. Curiosament Mandriva és troba en el lloc 11 del ranking.

Per aquests motius, perquè ja tenim un equip amb Kubuntu, per que ja venen instal·lades moltes de les aplicacions que farem servir i per mantenir la homogeneïtat amb els nostres servidor Ubuntu Server Enterprise 10.04 LTS és decideix que els equips clients faran servir la distribució **GNU/Linux Ubuntu Desktop 10.10 o Kubuntu** segons si l'usuari prefereix fer servir GNOME o KDE.

2.4. Alternatives lliures al programari de l'empresa

A la següent taula s'especificuen els software propietari que necessitem i que fem servir en plataformes Windows XP i la seva alternativa basada en software lliure i GNU/Linux que implementarem.

SOFTWARE PROPIETARI	SOFTWARE LLIURE
Microsoft Word	LibreOffice Writer
Microsoft Excel	LibreOffice Calc
Microsoft Access	LibreOffice Base
Microsoft PowerPoint	LibreOffice Impress
Microsoft Outlook	Squirrelmail
Microsoft Project	OpenProj
Microsoft Visio	Kivio
Nero Burning Rom	Braseo
Microsoft Explorer	Mozilla Firefoz
MathType	LibreOffice Math
JCreator Pro	Eclipse
Microsoft Studio	KDevelop
Microsoft Visual Basic	Gambas

3. Configuració comuns a tots el servidors i equips d'escriptori

3.1. Configuració comú a tots els servidors

3.1.1. Instal·lació de openSSH per administració remota

Instal·larem openSSH en els nostres servidors per tal d'administrar-los de forma remota i segura. Ho fem de la següent manera:

```
sudo apt-get install openssh-server
```

Una vegada instal·lat, ho deixarem tal qual ja que la configuració per defecte és suficient i correcte.

A l'ordinador de l'administrador tindrem que instal·lar el client de openSSH. Ho fem amb la següent comanda:

```
sudo apt-get install openssh-client
```

3.2. Configuració comuna a servidors i equips d'escriptori

3.2.1. Configuració de resolució de noms

Per la correcta resolució de noms, configurem l'arxiu `/etc/hosts` de totes les màquines de la següent manera:

```
GNU nano 2.2.2      Archivo: /etc/hosts      Modificado
127.0.0.1          hostname hostname.desint.local localhost
127.0.1.1          hostname
192.168.1.11       proxy proxy.desint.local
192.168.1.11       pdc pdc.desint.local
192.168.1.12       bdc bdc.desint.local
192.168.1.13       web web.desint.local
```

On `hostname` és el nom de la màquina que estem configurant.

4. Implementació del servidor PDC

4.1. Configuració pre-implementació del PDC

Instal·larem el servei NFS de la següent manera:

```
sudo apt-get install nfs-kernel-server
```

Editem l'arxiu `/etc/hosts.allow` per acceptar connexions de la nostra xarxa interna:

```
GNU nano 2.2.2      Archivo: /etc/hosts.allow
portmap: 192.168.1.0/24
nfs: 192.168.1.0/24
```

Editem l'arxiu `/etc/exports`:

```
GNU nano 2.2.2      Archivo: /etc/exports
/home 192.168.1.0/24(rw, sync, no_root_squash, no_subtree_check)
```

Reiniciem el servei `portmap` i `nfs`:

```
sudo service portmap restart && sudo service nfs-kernel-server restart
```

Configurem aquets dos serveis per que es configurin automàticament a l'inici. Ho fem de la següent manera:

```

dalcalam@bdc:~$ sudo update-rc.d -f nfs-kernel-server defaults
System start/stop links for /etc/init.d/nfs-kernel-server already exist.
dalcalam@bdc:~$
dalcalam@bdc:~$ sudo update-rc.d -f portmap defaults
update-rc.d: warning: /etc/init.d/portmap missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
Adding system startup for /etc/init.d/portmap ...
/etc/rc0.d/K20portmap -> ../init.d/portmap
/etc/rc1.d/K20portmap -> ../init.d/portmap
/etc/rc6.d/K20portmap -> ../init.d/portmap
/etc/rc2.d/S20portmap -> ../init.d/portmap
/etc/rc3.d/S20portmap -> ../init.d/portmap
/etc/rc4.d/S20portmap -> ../init.d/portmap
/etc/rc5.d/S20portmap -> ../init.d/portmap
dalcalam@bdc:~$ _

```

4.2. Instal·lació i configuració del servidor LDAP

Primer de tot, hem d'instal·lar el servidor OpenLDAP, el dimoni slapd i un paquet que conté utilitats de gestió de LDAP anomenat ldap-utils:

```
sudo apt-get install slapd ldap-utils
```

Per defecte el dimoni sldap està configurat amb les mínimes opcions per executar-se.

OpenLDAP fa servir un directori independent que conté el Arbre d'Informació del Directori (DIT) cn = config. El cn = config (DIT) es fa servir per configurar dinàmicament el dimoni slapd, el que permet la modificació de les definicions d'esquemes, els índexs, ACLs, etc sense parar el servei.

El directori backend cn = config solament té una configuració mínima per defecte i tindrem que fer una configuració addicional per aquest. Afegirem uns esquemes ldif que l'ompliran amb una interfície i amb una combinació "clàssica" que serà compatible amb les aplicacions de llibreta de adreces i comptes UNIX Posix. Posix permet l'autenticació a varies aplicacions, com les aplicacions web, correu electrònic Mail Transfer Agent (MTA) d'aplicacions, etc.

Carreguem els arxius d'esquema necessaris cosine.ldif, nis.ldif i intergperson.ldif abans mencionats:

```

dalcalam@pdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine
.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"

dalcalam@pdc:~$
dalcalam@pdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ld
if
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"

dalcalam@pdc:~$
dalcalam@pdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetor
gperson.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"
dalcalam@pdc:~$

```

Creem l'arxiu amb l'esquema de backend (backend.desint.local.ldif) amb el següent contingut:

```
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

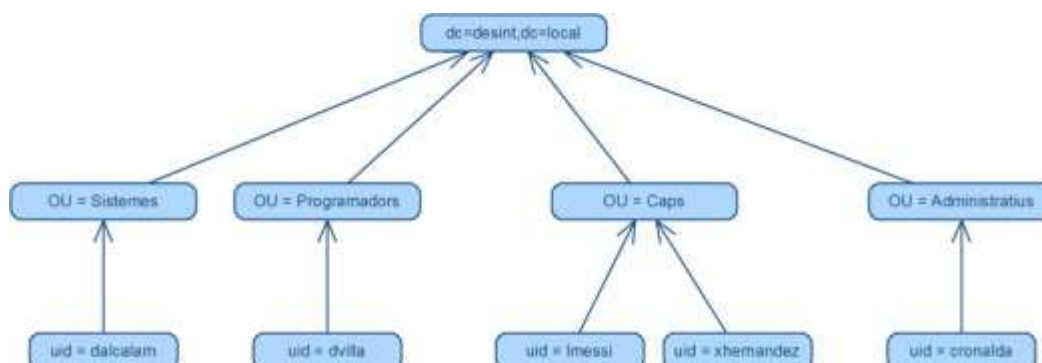
# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=desint,dc=local
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=desint,dc=local
olcRootPW: L3oM3ss1
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_ik_max_objects 1500
olcDbConfig: set_ik_max_locks 1500
olcDbConfig: set_ik_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=desint,dc=local" write by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=desint,dc=local" write by * read
```

Afegim aquest esquema a l'esquema del directori LDAP:

```
dalcalan@pdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.desint.local.ldif
if
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=module,cn=config"
adding new entry "olcDatabase=hdb,cn=config"
dalcalan@pdc:~$
```

4.2.1. Configuració de l'estructura LDAP de l'empresa i creació d'usuaris i grups

En aquest punt ja tenim el directori de frontend preparat per a ser "poblat". Per tant, ho farem creant el nostre frontend amb dn base: dc=desint, dc=local, les Unitats Organitzatives: Sistemes, Programadors, Caps i Administratius, i també creem els usuaris actuals de la nostra empresa amb uid: dalcalam, lmessi, dvilla, xhernandez i cronalda. Ens quedarà un esquema com el següent:



Per fer això , creem el fitxer d'esquema anomenat "frontend.desint.local.ldif" amb el contingut indicat a sota. Veiem a més entre les característiques dels usuaris, aprofitem i definim el directori home de l'usuari, la seva adreça de correu electrònic, li assignem un uid i un guid i definim els requisits de les contrasenyes:

```
# Create top-level object in domain
dn: dc=desint,dc=local
objectClass: top
objectClass: dcObject
objectclass: organization
o: Organización DESINT
dc: desint
description: LDAP DESINT

# USUARI ADMINISTRADOR:
dn: cn=admin,dc=desint,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: administrador LDAP
userPassword: L3oM3ss1

# UNITATS ORGANITZATIVES:
dn: ou=programadors,dc=desint,dc=local
objectClass: organizationalUnit
ou: programadors

dn: ou=sistemes,dc=desint,dc=local
objectClass: organizationalUnit
ou: sistemes

dn: ou=caps,dc=desint,dc=local
objectClass: organizationalUnit
ou: caps

dn: ou=administratiu,dc=desint,dc=local
objectClass: organizationalUnit
ou: administratiu

# USUARIS:
dn: uid=dalcalam,ou=sistemes,dc=desint,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: dalcalam
sn: Alcala Martinez
givenName: Daniel
cn: dalcalam
displayName: Daniel Alcala Martinez
uidNumber: 1000
gidNumber: 10000
userPassword: dani1234
gecos: Daniel Alcala Martinez
loginShell: /bin/bash
homeDirectory: /home/dalcalam
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: dalcalam@desint.local
title: Administrador de sistemes/Web
```

```
initials: DAM

dn: uid=lmessi,ou=caps,dc=desint,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: lmessi
sn: Messi
givenName: Leo
cn: lmessi
displayName: Leo Messi
uidNumber: 1001
gidNumber: 10000
userPassword: messi1234
gecos: Leo Messi
loginShell: /bin/bash
homeDirectory: /home/lmessi
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: lmessi@desint.local
title: Cap Analista/Programador
initials: LM
```

```
dn: uid=dvilla,ou=caps,dc=desint,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: dvilla
sn: David
givenName: Villa
cn: dvilla
displayName: David Villa
uidNumber: 1002
gidNumber: 10000
userPassword: villa1234
gecos: David Villa
loginShell: /bin/bash
homeDirectory: /home/dvilla
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: lvilla@desint.local
title: Cap Analista/Programador
initials: DV
```

```
dn: uid=xhernandez,ou=programadors,dc=desint,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: xhernandez
sn: Hernandez
givenName: Xavi
cn: xhernandez
displayName: Xavi Hernandez
uidNumber: 1003
gidNumber: 10000
userPassword: xavi1234
gecos: Xavi Hernandez
```

```
loginShell: /bin/bash
homeDirectory: /home/xhernandez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: xhernandez@desint.local
title: Analista/Programador
initials: LM

dn: uid=cronalda,ou=administratius,dc=desint,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: cronalda
sn: Ronalda
givenName: Cristiana
cn: cronalda
displayName: Cristiana Ronalda
uidNumber: 1004
gidNumber: 10000
userPassword: ronaldo1234
gecos: Cristiana Ronalda
loginShell: /bin/bash
homeDirectory: /home/cronalda
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: cronalda@desint.local
title: Secretaria/Administrativa/Recepcionista
initials: CR
```

Per afegir aquestes entrades al directori LDAP fem el següent:

```
dalcalam@pdc:~$ sudo ldapadd -x -D cn=admin,dc=desint,dc=local -W -f frontend.de
sint.local.ldif
Enter LDAP Password:
adding new entry "dc=desint,dc=local"

adding new entry "cn=admin,dc=desint,dc=local"

adding new entry "ou=programadors,dc=desint,dc=local"

adding new entry "ou=sistemes,dc=desint,dc=local"

adding new entry "ou=caps,dc=desint,dc=local"

adding new entry "ou=administratius,dc=desint,dc=local"

adding new entry "uid=dalcalam,ou=sistemes,dc=desint,dc=local"

adding new entry "uid=lmessi,ou=caps,dc=desint,dc=local"

adding new entry "uid=dvilla,ou=caps,dc=desint,dc=local"

adding new entry "uid=xhernandez,ou=programadors,dc=desint,dc=local"

adding new entry "uid=cronalda,ou=administratius,dc=desint,dc=local"
```


4.2.2. Prova de funcionament de LDAP

Podem comprovar que el contingut s'ha afegit correctament amb la utilitat `ldapsearch` que serveix per realitzar cerques en el directori LDAP. Consultem les dades següents:

```
dalcalam@pdc:~$ ldapsearch -xLLL -b "dc=desint,dc=local" uid=dalcalam uid displayname homeDirectory mail title
dn: uid=dalcalam,ou=usuaris,dc=desint,dc=local
uid: dalcalam
displayName: Daniel Alcala Martinez
homeDirectory: /home/dalcalam
mail: dalcalam@desint.local
title: Administrador de sistemes/Web
```

Veiem les dades de l'usuari `dalcalam`, per tant el nostre servidor LDAP funciona correctament i s'ha afegit l'estructura del fitxer `fronend.desint.local.ldif`.

4.3. Instal·lació i configuració del servidor Samba

Hi ha tres paquets necessaris per integrar Samba amb LDAP: `Samba`, `Samba-doc` i `Samba-tools`. Per tant, procedim a instal·lar-los:

```
sudo apt-get install Samba Samba-doc smbldap-tools
```

Estrictament parlant no és necessari el paquet `smbldap-tools`, però tret que tinguem un altre paquet o uns scripts, és necessari un mètode per administrar usuaris, grups i comptes d'equip.

4.3.1. Configuració i integració de Samba amb LDAP

Es necessari afegir els esquemes de Samba al directori LDAP. Aquests esquemes es troben en el paquet `Samba-doc`. Els tenim que descomprimir a `/etc/ldap/schema`:

```
dalcalam@pdc:~$ sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
dalcalam@pdc:~$ sudo gzip -d /etc/ldap/schema/samba.schema.gz
dalcalam@pdc:~$
```

Per fer això, primer creem un arxiu anomenat `schema_convert.conf` amb el següent contingut:

```
GNU nano 2.2.2      Archivo: schema_convert.conf
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/samba.schema
```

A continuació, creem un directori temporal i fem servir la comanda salpcat per crear el esquema per LDAP de la següent manera:

```
dalcalam@pdc:~$ mkdir /tmp/ldif_output
dalcalam@pdc:~$ slapcat -f schema_convert.conf -F /tmp/ldif_output/ -n0 -s "cn=(
12)samba,cn=schema,cn=config" > /tmp/cn=samba.ldif
dalcalam@pdc:~$
```

Veiem que s'ha generat l'arxiu Samba.ldif que conté el nostre esquema per integrar Samba al directori LDAP. Però encara queda li hem de fer un últim retoc:

Editem les següents línies del principi de l'arxiu de manera que quedin així:

```
dn: cn=Samba,cn=schema,cn=config
...
cn: Samba
```

i eliminem aquestes línies que es troben al final:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

Ara sí que tenim l'arxiu cn=Samba.ldif totalment preparat per afegir l'esquema de Samba al directori LDAP i que quedi totalment integrat a aquest. Ho fem de la següent manera:

```
dalcalam@pdc:~$
dalcalam@pdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/cn=samba.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=samba,cn=schema,cn=config"
dalcalam@pdc:~$
```

Una vegada afegit l'esquema Samba al directori LDAP, hem de configurar Samba editant l'arxiu /etc/samba/smb.conf amb els paràmetres del nostre domini, ldap, usuaris i seguretat de la següent manera:

```
[global]
workgroup = DESINT
server string = %h server (Samba, Ubuntu)
map to guest = Bad User
passdb backend = ldapsam:ldap://localhost
pam password change = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .
username map = /etc/samba/smbusers
unix password sync = Yes
syslog = 0
log file = /var/log/samba/log.%m
max log size = 100
panic action = /usr/share/samba/panic-action %d
security = user
encrypt passwords = yes
usershare allow guests = Yes

# LDAP Settings
```

```

passdb backend = ldapsam:ldap://127.0.0.1
ldap suffix = dc=desint,dc=local
ldap user suffix = ou=usuaris
ldap group suffix = ou=grups
ldap machine suffix = ou=ordinadors
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=admin,dc=desint,dc=local
ldap ssl = off
ldap passwd sync = yes

add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"

```

Reiniciem els dimonis de Samba per que agafi la nova configuració:

```

sudo restart smb
sudo restart nmbd

```

Ara que tenim l'entorn configurat correctament, poblarem el nostre esquema Samba-ldap de la següent manera:

```

dalcalam@pdc:~$ sudo smbldap-populate
Populating LDAP directory for domain WORKGROUP (S-1-5-21-3506734449-4139963510-2
072446952)
(using builtin directory structure)

entry dc=desint,dc=local already exist.
adding new entry: ou=usuaris,dc=desint,dc=local
adding new entry: ou=grups,dc=desint,dc=local
adding new entry: ou=ordinadors,dc=desint,dc=local
adding new entry: ou=Idmap,dc=desint,dc=local
adding new entry: uid=root,ou=usuaris,dc=desint,dc=local
adding new entry: uid=nobody,ou=usuaris,dc=desint,dc=local
adding new entry: cn=Domain Admins,ou=grups,dc=desint,dc=local
adding new entry: cn=Domain Users,ou=grups,dc=desint,dc=local
adding new entry: cn=Domain Guests,ou=grups,dc=desint,dc=local
adding new entry: cn=Domain Computers,ou=grups,dc=desint,dc=local
adding new entry: cn=Administrators,ou=grups,dc=desint,dc=local
adding new entry: cn=Account Operators,ou=grups,dc=desint,dc=local
adding new entry: cn=Print Operators,ou=grups,dc=desint,dc=local
adding new entry: cn=Backup Operators,ou=grups,dc=desint,dc=local
adding new entry: cn=Replicators,ou=grups,dc=desint,dc=local
adding new entry: sambaDomainName=WORKGROUP,dc=desint,dc=local

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
dalcalam@pdc:~$

```

SAMBA necessita conèixer el passwprd del administrador de LDAP. Li passem el password de la següent manera:

```

dalcalam@pdc:~$ sudo smbpasswd -w L3oM3ss1
Setting stored password for "cn=admin,dc=desint,dc=local" in secrets.tdb
dalcalam@pdc:~$

```

També podem afegir el nostre usuari al grup d'usuaris d'administradors de SAMBA-LDAP de la següent manera:

```

dalcalam@pdc:~$ sudo smbldap-groupmod -m 'dalcalam' 'Administrators'
adding user dalcalam to group Administrators

```

4.4. Configuració del PDC per autenticar usuaris

Per que els clients s'autentiquin contra aquest servidor de domini, tenim que instal·lar el paquet `ldap-auth-client`. Ho fem amb un assistent que iniciarem de la següent manera:

```
sudo apt-get --yes install ldap-auth-client
```

Ens aniran sortint una sèrie de finestres amb una sèrie de preguntes sobre la configuració. Responem de la següent manera:

```
Configuración de ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of
ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is
optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in
the event name service problems.

LDAP server Uniform Resource Identifier:
ldap:///192.168.1.11
<Aceptar>
```

```
Configuración de ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites use the components
of their domain names for this purpose. For example, the domain "example.net" would use
"dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:
dc=desint,dc=local
<Aceptar>
```

```
Configuración de ldap-auth-config
Please enter which version of the LDAP protocol should be used by ldaps. It is usually a
good idea to set this to the highest available version.

LDAP version to use:
3
2
<Aceptar>
```

```
Configuración de ldap-auth-config
This option will allow you to make password utilities that use pam to behave like you would
be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

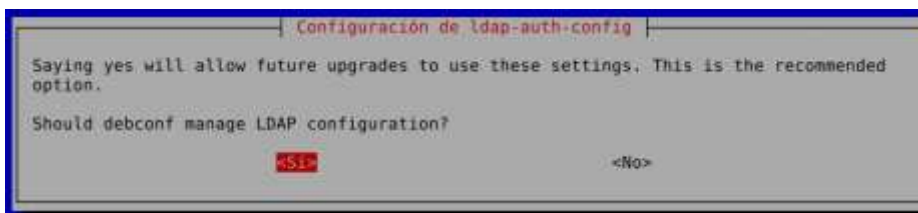
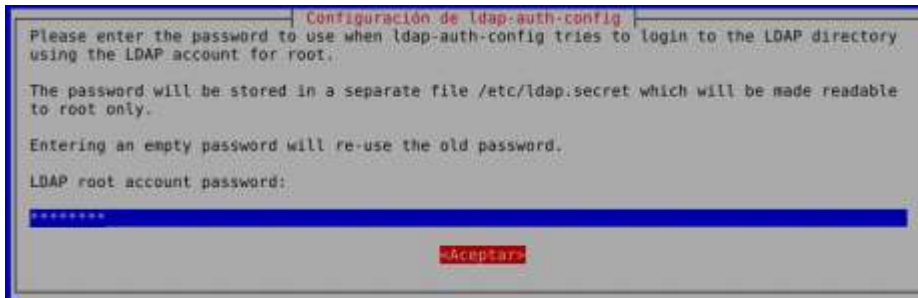
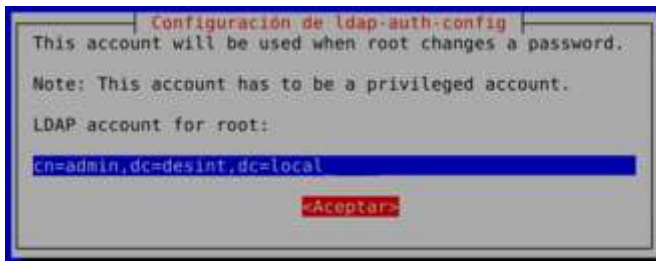
If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:
<Si> <No>
```

```
Configuración de ldap-auth-config
Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?
<Si> <No>
```



Per últim fem:

```
sudo apt-get --yes install ldap-auth-client
```

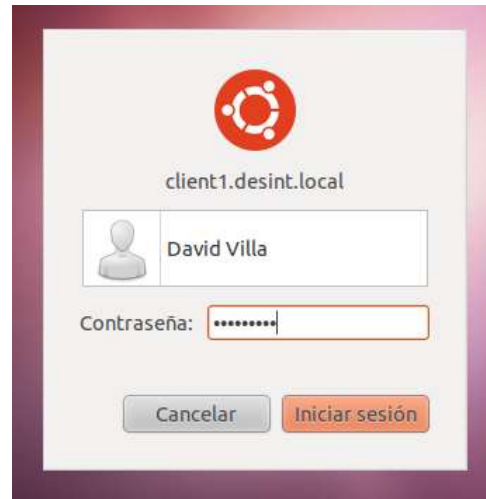
Li indiquem que els usuaris s'autenticaran mitjançant l'LDAP:



En aquest punt el servidor PDC esta implementat al 100% i és capaç d'autenticar usuaris.

4.5. Prova d'autenticació d'un usuari del LDAP en un ordinador d'escriptori:

Fem una prova d'autenticar-nos en un ordinador d'escriptori amb l'usuari David Villa (dvilla) que hem creat abans en l'LDAP:



Veiem que podem autenticar-nos correctament:

```
dom 5 de jun, 00:52 dvilla
dvilla@Client1: ~
Archivo Editar Ver Buscar Terminal Ayuda
dvilla@Client1:~$ finger-ldap
Login Name Tty Idle Login Time Office
dvilla David Villa tty8 7 Jun 5 00:50 (:0)
dvilla David Villa pts/0 Jun 5 00:51 (:0.0)
dvilla@Client1:~$
```

Abans aquest ordinador s'ha configurat per que validi els usuaris contra el PDC però això s'explicarà en altre capítol.

5. Implementació del servidor d'arxius

5.1. Configuració de Samba com servidor d'arxius

Li tenim que indicar a Samba quin és el password de l'administrador de l'LDAP. Ho fem de la següent manera:

```
dalcalam@pdc:~$ sudo smbpasswd -w L3oM3ss1
Setting stored password for "cn=admin,dc=desint,dc=local" in secrets.tdb
dalcalam@pdc:~$
```

Afegim a l'arxiu de configuració de Samba /etc/Samba/smb.conf les següents línies:

```
[share]
comment = Arxius Desint
path = /srv/Samba/share
browsable = yes
guest ok = yes
read only = on
create mask = 0755
```

Com veiem, compartirem la carpeta /srv/Samba/share. Aquesta carpeta serà la base de la nostra estructura de carpetes compartides.

Per finalitzar, reiniciem els dimonis de Samba:

```
sudo restart smbd
sudo restart nmbd
```

5.2. Implementació i configuració de les carpetes compartides:

Ja hem vist al punt anterior que la base o arrel de la nostra estructura de carpetes compartides és la carpeta /srv/Samba/share. A aquesta carpeta tothom té accés però a partir d'aquí cada grup tindrà accés a la seva carpeta però no a la de altres grups. En concret és vol crear l'estructura representada a la següent taula:

Carpeta compartida	Propietari	Grup amb permisos per accedir i permisos RW	Usuaris membres del grup.
/srv/Samba/share/sistemes	dalcalam	SISTEMES	dalcalam
/srv/Samba/share/programadors	dvilla	PROGRAMADORS	dvilla
/srv/Samba/share/caps	lmessi	CAPS	lmessi, xhernandez
/srv/Samba/share/administratius	cronalda	ADMINISTRATIUS	Cronalda

Comencem creant aquesta estructura de carpetes:

```
dalcalam@pdc:~$ sudo mkdir /srv/samba/share/sistemes
dalcalam@pdc:~$ sudo mkdir /srv/samba/share/programadors
dalcalam@pdc:~$ sudo mkdir /srv/samba/share/caps
dalcalam@pdc:~$ sudo mkdir /srv/samba/share/administratius
dalcalam@pdc:~$ ls /srv/samba/share/
administratius caps programadors sistemes
```

Per que Samba autentiï als usuaris de l'LDAP necessitem que estiguin relacionats amb el mateix password. Ho fem amb la comanda smbpasswd de la següent manera:

```
dalcalam@pdc:~$ sudo smbpasswd -a dalcalam
New SMB password:
Retype new SMB password:
Added user dalcalam.
dalcalam@pdc:~$ sudo smbpasswd -a dvilla
New SMB password:
Retype new SMB password:
Added user dvilla.
dalcalam@pdc:~$ sudo smbpasswd -a xhernandez
New SMB password:
Retype new SMB password:
Added user xhernandez.
dalcalam@pdc:~$ sudo smbpasswd -a lmessi
New SMB password:
Retype new SMB password:
Added user lmessi.
dalcalam@pdc:~$ sudo smbpasswd -a cronalda
New SMB password:
Retype new SMB password:
Added user cronalda.
dalcalam@pdc:~$ _
```

Afegim els usuaris al seus corresponents grups Samba:

```
dalcalam@pdc:~$ sudo smbldap-groupmod -m dalcalam sistemes
User dalcalam already in the group
dalcalam@pdc:~$ sudo smbldap-groupmod -m dvilla programadors
adding user dvilla to group programadors
dalcalam@pdc:~$ sudo smbldap-groupmod -m lmessi caps
User lmessi already in the group
dalcalam@pdc:~$ sudo smbldap-groupmod -m xhernandez caps
adding user xhernandez to group caps
dalcalam@pdc:~$ sudo smbldap-groupmod -m cronalda administratius
adding user cronalda to group administratius
```

Assignem el propietari i el grup corresponent a aquestes carpetes. Fem servir el paràmetre “-R” perquè les carpetes i arxius que anem guardant en aquesta carpetes heretin els permisos:

```
dalcalam@pdc:~$ sudo chown -R dalcalam.sistemes /srv/samba/share/sistemes
dalcalam@pdc:~$ sudo chown -R dvilla.programadors /srv/samba/share/programadors
dalcalam@pdc:~$ sudo chown -R lmessi.caps /srv/samba/share/caps
dalcalam@pdc:~$ sudo chown -R cronalda.administratius /srv/samba/share/administratius
dalcalam@pdc:~$
```

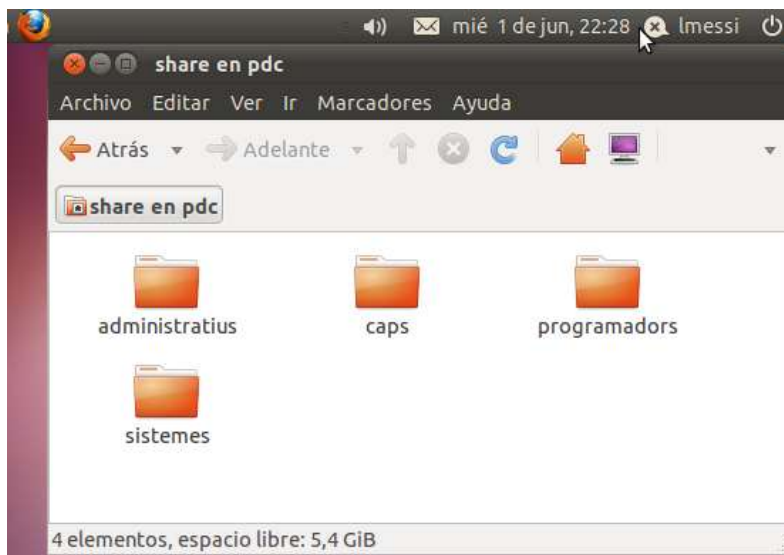
Assignem permisos de RWX sobre aquestes carpetes al propietari i al grup corresponent i evitem l'accés a usuaris d'altres grups:

```
dalcalam@pdc:~$ sudo chmod 770 -R /srv/samba/share/administratius
dalcalam@pdc:~$ sudo chmod 770 -R /srv/samba/share/programadors
dalcalam@pdc:~$ sudo chmod 770 -R /srv/samba/share/caps
dalcalam@pdc:~$ sudo chmod 770 -R /srv/samba/share/administratius
dalcalam@pdc:~$
```

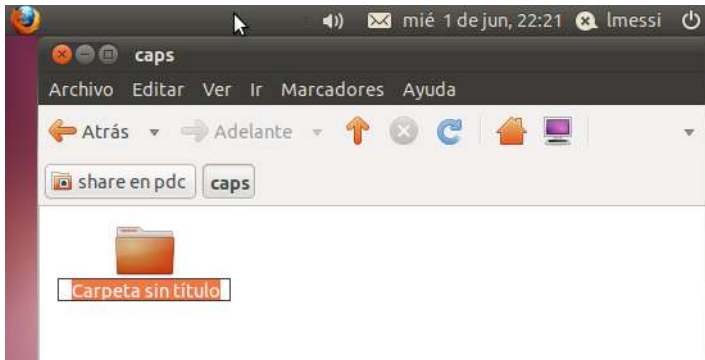
Ja tenim creada l'estructura de carpetes compartides amb els permisos d'accés a grups indicats a la taula anterior.

5.3. Prova d'accés a les carpetes compartides des d'un ordinador d'escriptori:

Iniciem sessió amb l'usuari del domini lmessi i accedim al recurs de xarxa “share” del nostre PDC:



Entrem a la carpeta “caps”. Veiem que tenim accés i que tenim permisos d’escriptura ja que l’usuari “lmessi” pertany al grup “caps”:



En canvi s’ intentem entrar a cap altra carpeta ens trobarem amb que se’ns denega l’accés ja que l’usuari “lmessi” no pertany al grup “programadors”:



6. Implementació del servidor d’impressió

6.1. Configuració de Samba com servidor d’impressió amb CUPS

Procedim a instal·lar CUPS de la següent manera:

```
sudo apt-get install cups
```

Per compartir impressores hem de afegir a l’arxiu /etc/Samba/smb.conf el següent:

```
[print$]
Coment = Print Drivers
Path = /var/lib/Samba/printers
browsable = yes
read only = yes
guest ok = yes
```

```
[printers]
Comment = All Printers
browsable = yes
path = /var/spool/Samba
printable = yes
guest ok = yes
read only = no
create mask = 0755
```

6.2. Instal·lació d'impressora

Com que encara no hem rebut la nova impressora de l'empresa HP Laserjet, provarem el servidor d'impressió instal·lant una impressora virtual de PDF. Ho fem de la següent manera:

```
sudo apt-get install cups-pdf
```

Automàticament tindrem la impressora compartida.

6.3. Prova d'accedir a la impressora compartida des de un ordinador d'escriptori

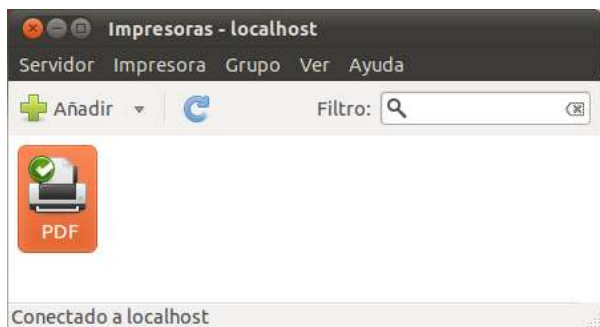
Des de un ordinador d'escriptori amb Ubuntu, anem a "Sistema -> Administració -> Impressores" . Ens demanarà la contrasenya de l'usuari root. Tot i això, ens autèntiquem com l'administrador de sistemes amb el seu usuari d'LDAP (dalcalam):



Elegim la opció "Impressora de xarxa -> Cercar impressora de xarxa" i en "Impressora SMB" posem la IP o el nom de domini del servidor (pdc.desint.local). Li donem a examinar i veiem que ens afegit "/PDF" de manera que ens queda "smb://pdc.desint.local/PDF". Això vol dir que a trobat la impressora compartida de PDF:



Li donem al botó “Endavant” i anem a una finestra on se’ns demana que seleccionem el driver de la impressora. Al ser una impressora virtual de PDF, no tenim el driver disponible en aquest llista. Per provar, escollim el driver genèric de text. Amb això no podem imprimir, però ens serveix per provar que el servidor d’impressió funciona correctament i podem compartir les impressores correctament. Li donem a botó “endavant”. Veiem que la impressora s’ha afegit correctament.



Comprovem que al quadre de diàleg d’impressió de l’libreOffice Word apareix la impressora que acabem d’afegir i en deixa seleccionar-la per imprimir:



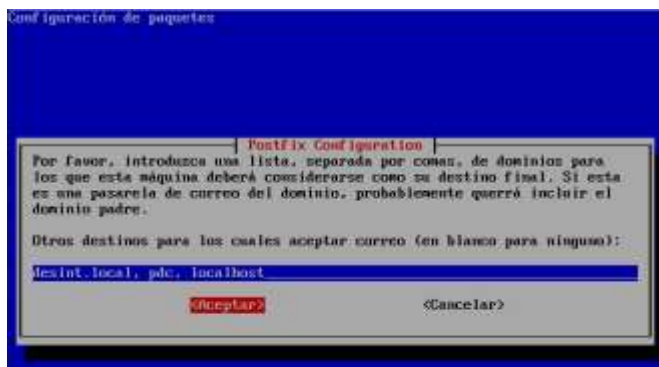
7. Implementació del servidor de correu

7.1. Instal·lació del servidor MTA Postfix (SMTP)

Per instal·lar Postfix, ho fem de la següent manera:

```
sudo apt-get install postfix
```

Ho configurem mitjançant un assistent que surt automàticament durant la instal·lació. Responem i seleccionem el següent:



Configuración de paquetes

Postfix Configuration

Si se fuerzan las actualizaciones sincronas, el correo será procesado más lentamente. Si no se fuerzan, existe la posibilidad remota de perder algunos correos si el sistema colapsa en un momento inoportuno y no está usando un sistema de archivos transaccional (como ext3).

¿Forzar actualizaciones sincronas en la cola de correo?

Sí No

Configuración de paquetes

Postfix Configuration

Especifique los bloques de red para los que esta máquina deberá reenviar el correo. El predeterminado es sólo para la máquina local, lo cual se requiere para algunos agentes de correo de usuario. El predeterminado incluye la máquina local tanto para IPv4 como IPv6. Si se conecta únicamente con una versión de IP, puede eliminar los valores no usados.

Si este sistema es un «smarthost» para un bloque de máquinas, debe especificar los bloques de red aquí, o el correo será rechazado en lugar de reenviado.

Para usar el predeterminado de postfix (que se basa en las redes conectadas), deje en blanco.

Redes locales:

Configuración de paquetes

Postfix Configuration

Por favor, especifique el límite que deberá colocar Postfix en los archivos de buzón de correo para prevenir errores de software. El valor de cero (0) significa ilimitado. El predeterminado por el desarrollador principal es 51200000.

Límite de tamaño de buzón de correo (en bytes):

Configuración de paquetes

Postfix Configuration

Indique el carácter que se usará para definir una extensión de dirección local.

Para no usar extensiones de dirección, deje la cadena en blanco.

Carácter de extensión de direcciones locales:



Ara ja tenim instal·lat el nostre servidor SMTP Postfix.

Configurem el format que tindran les bústies. Decidim que sigui Maildir. Ho fem de la següent manera:

```
sudo postconf -e 'home_mailbox = Maildir/'
```

```
dalcalam@pdc:/home$ sudo postconf -e 'home_mailbox = Maildir'
dalcalam@pdc:/home$
```

7.2. Instal·lació i configuració de Dovecot (IMAP, POP3)

Per instal·lar Dovecot procedim de la següent manera:

```
sudo apt-get install dovecot-imapd dovecot-pop3d
```

Tenim que configurar l'arxiu `/etc/dovecot/dovecot.conf`. Ho configurem per fer servir el protocol IMAP, bústies de tipus Maildir y fem referencia a l'arxiu `/etc/dovecot/dovecot-dap.conf` com argument per autenticar-nos ja que la validació dels usuaris també serà mitjançant l'LDAP. Ens queda de la següent manera:

```
# /etc/dovecot/dovecot.conf
protocols = imap
log_timestamp = "%Y-%m-%d %H:%M:%S "
first_valid_uid = 100
mail_debug = yes
mail_location = maildir:~/Maildir
disable_plaintext_auth = no
listen = *

auth default {
    mechanisms = plain

    socket listen {
        client {
            # The client socket is generally safe to export to everyone. Typical
            use
            # is to export it to your SMTP server so it can do SMTP AUTH lookups
            # using it.
            path = /var/spool/postfix/private/auth-client
```

```

        mode = 0660
        user = postfix
        group = postfix
    }
}

passdb ldap {
    args = /etc/dovecot/dovecot-ldap.conf
}
userdb ldap {
    args = /etc/dovecot/dovecot-ldap.conf
}
}

```

Configurem l'arxiu `/etc/dovecot/dovecot-dap.conf` amb les dades del servidor LDAP per tal de poder autenticar-nos:

```

hosts = 192.168.1.11
dn = cn=admin,dc=desint,dc=local
dnpass = L3oM3ss1
tls = no
auth_bind = yes
auth_bind_userdn = uid=%u,ou=usuaris,dc=desint,dc=local
base = ou=usuaris,dc=desint,dc=local
ldap_version = 3
base = ou=usuaris,dc=desint,dc=local
scope = subtree
user_attrs = homeDirectory=home,uidNumbre=uid,gidNumber=gid
user_filter = (&(objectClass=posixAccount)(uid=%u))
pass_attrs = uid=user,userPassword=password
pass_filter = (&(objectClass=posixAccount)(uid=%u))

```

7.3. Instal·lació i configuració de Squirrelmail (IMAP, webmai)

Per instal·lar Squirrelmail procedim de la següent manera:

```
sudo apt-get install squirrelmail httpd
```

Per configurar-lo, ho fem llançant un script de la següent manera:

```
sudo /usr/share/squirrelmail/config/./conf.pl
```

Accedim al següent menú de configuració:

```

SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >>

```

Anem a l'opció 1 on editarem:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Organization Preferences
1. Organization Name      : Desint Correu Web
```

I a la opció 2, editarem les dades del servidor de correu:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings

General
-----
1. Domain                : pdc.desint.local
2. Invert Time           : false
3. Sendmail or SMTP      : SMTP

A. Update IMAP Settings  : localhost:143 (other)
B. Update SMTP Settings  : localhost:25
```

Amb això tenim prou per el nostre servidor de correu. En aquest moment ja esta 100% operatiu.

7.4. Instal·lació i configuració de servei antiSpam i antivirus.

Instal·lem els paquets Amavisd-new (wrapper), Spamassasin (filtrar), ClamAV (antivirus):

```
sudo apt-get install amavisd-new spamassasin clamav-daemon
```

Instal·lem els paquets opcional pyzor razor ja que s'integren amb Spamassasin per una millor detecció d'Spam:

```
sudo apt-get install pyzor razor
```

7.4.1. Configuració de ClamAV.

La configuració per defecte de ClamAV ens és suficient però falta configurar ClamAV per que treballi conjuntament amb el filtre de correu. Per fer això tenim que afegir l'usuari clamav al grup amavis:

```
dalcalam@pdc:~$ sudo adduser clamav amavis
Añadiendo al usuario 'clamav' al grupo 'amavis' ...
Adding user clamav to group amavis
Hecho.
```

7.4.2. Configuració de Spamassasin.

Editem l'arxiu /etc/default/spamassasin per activar el dimoni spamassasin. Canviem ENABLED=1 per 0:

```
GNU nano 2.2.2      Archivo: /etc/default/spamassasin      Modificado
# /etc/default/spamassasin
# Duncan Findlay

# WARNING: please read README.spamd before using.
# There may be security risks.

# Change to one to enable spamd
ENABLED=1_
```


Iniciem el dimoni mencionat:

```
dalcalam@pdc:~$ sudo /etc/init.d/spamassassin start
Starting SpamAssassin Mail Filter Daemon: spamd.
```

7.4.3. Configuració de Amavisd-new.

Primer de tot activem la configuració d'Spam i antivirus de Amavisd-new editant el fitxer /etc/amavis/conf.d/15-content_filter_mode. Les següents línies tenen que quedar desmarcades:

```
use strict;

@bypass_virus_checks_maps = (
    \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);

@bypass_spam_checks_maps = (
    \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1; # insure a defined return
```

Reiniciem el dimoni amavis per que els canvis tinguin efecte:

```
dalcalam@pdc:~$ sudo /etc/init.d/amavis restart
Stopping amavisd: amavisd-new.
Starting amavisd: amavisd-new.
```

7.4.4. Integració amb Postfix.

Per integrar al nostre servidor Postfix el filtre de correu i antivirus que acabem de configurar, fem el següent:

```
dalcalam@pdc:~$ sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Seguidament, afegint les següents línies al final de l'arxiu /etc/postfix/master.cf:

```
smtp-amavis unix - - - - 2 smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
-o max_use=20

127.0.0.1:10025 inet n - - - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_delay_reject=no
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o smtpd_data_restrictions=reject_unauth_pipelining
-o smtpd_end_of_data_restrictions=
-o mynetworks=127.0.0.0/8
```

```
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o smtpd_client_connection_count_limit=0
-o smtpd_client_connection_rate_limit=0
-o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

També afegim les següents línies sota el servei “pickup”:

```
-o content_filter=
-o receive_override_options=no_header_body_checks
```

Reiniciem el servei Postfix per que els canvis tinguin efecte:

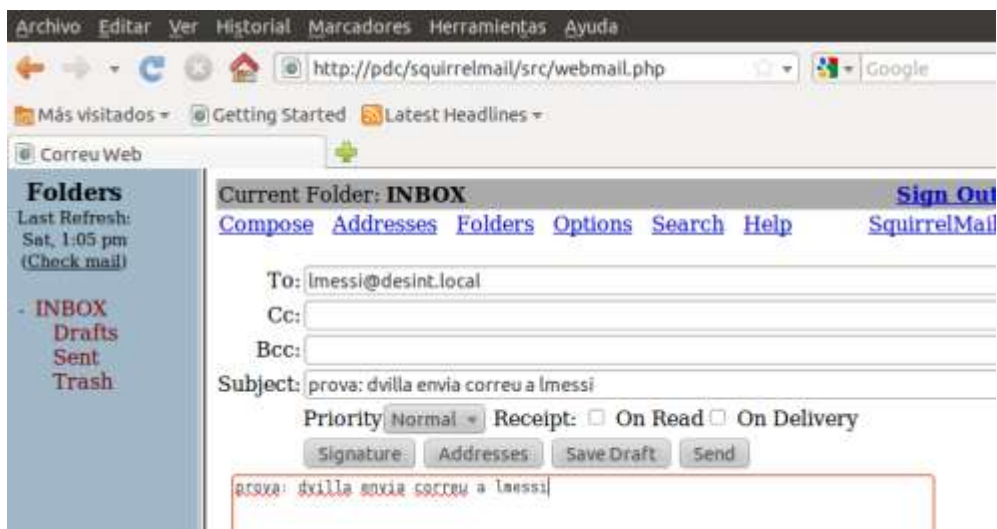
```
sudo /etc/init.d/postfix restart
```

7.5. Prova d'enviament i recepció de correu entre usuaris.

Per accedir al correu, tenim que obrir el navegador web i a l'adreça <http://pdc/squirrelmail/>.
Accedim a la pantalla d'autenticació:



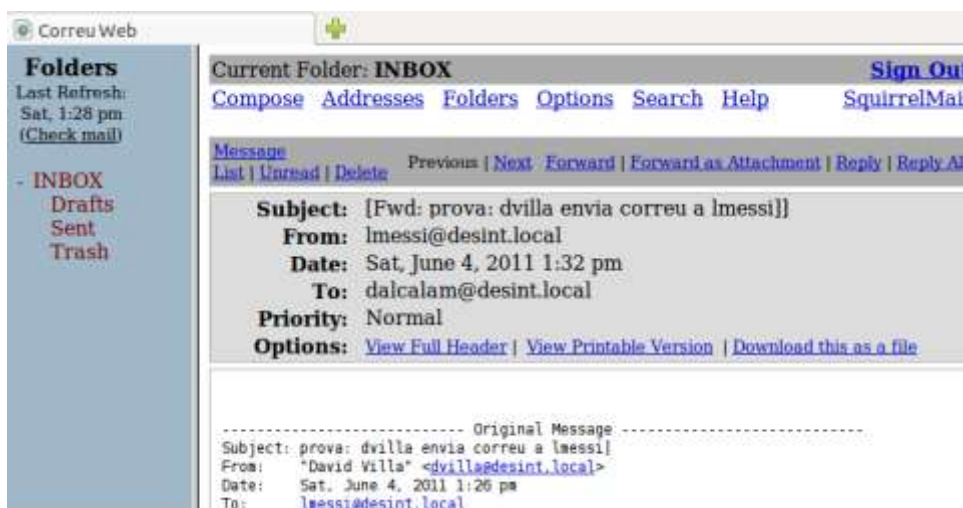
Ens auteniquem amb l'usuari “dvilla” i li enviem el següent correu s “lmessi”:



Ara, sortim del Webmail i tronem a entrar autenticar-nos amb l'usuari "lmessi". Anem a "INBOX" i obrim el correu rebut de "lvilla":



Ara, "lmessi" reenvia el correu a "dalcalam". Sortim del Webmail i tronem a entrar autenticar-nos amb aquest usuari:



Veiem que "dalcalam" ha rebut el correu correctament. Per tant, el servidor de correu funciona correctament.

8. Implementació del servidor de versions

8.1. Instal·lació i configuració de CVS

Per instal·lar CVS, fer servir la següent comanda:

```
sudo apt-get install cvs
```

Seguidament, instal·lem xinetd per a poder iniciar/aturar el servidor CVS. Ho fem de la següent manera:

```
sudo apt-get install xinetd
```

Una vegada tenim cvs i xinetd instal·lats, configurem xinetd per inicialitzar el servidor CVS. Ho fem editant l'arxiu `/etc/xinetd.d/cvspserver` de la següent manera:

```
service cvspserver
{
port = 2401
socket_type = stream
protocol = tcp
user = root
wait = no
type = UNLISTED
server = /usr/bin/cvs
server_args = -f—allow-root /var/lib/cvs pserver
disable = no
}
```

Veiem que el directori de repositoris de CVS serà: `/var/lib/cvs`.

Ja tenim instal·lat i configurat el servidor CVS. Reiniciem el servidor amb la nova configuració:

```
sudo /etc/initd.d/xinetd restart
```

Confirmem que el servei CVS esta corrent amb la següent comanda:

```
dalcalam@pdc:~$ sudo netstat -tap | grep cvs
Password:
tcp        0      0 *:*cvspserver      *:*                ESCUCHAR
1063/xinetd
dalcalam@pdc:~$
```

Per poder provar-lo es necessita tenir un client amb un entorn de desenvolupament com Eclipse o Netbeans. La feina de l'administrador de sistemes és tenir el servidor funcionament. Deleguem les proves d'aquest servidor als analistes/programadors.

9. Implementació del servidor de documentació

9.1. Instal·lació i configuració de MoinMoin

Instal·lem MoinMoin amb la següent comanda:

```
sudo apt-get install python-moinmoin
```

Creem la nostra Wiki anomenada "mywiki" a `/usr/share/mon/mywiki` i li afegim els directoris i arxius necessaris per que la Wiki es trobi en un estat inicial. També assignem permisos a la carpeta contenidora de la Wiki "mywiki":

```

dalcalam@pdc:~$ cd /usr/share/moin
dalcalam@pdc:/usr/share/moin$ sudo mkdir mywiki
dalcalam@pdc:/usr/share/moin$ sudo cp -R data mywiki
dalcalam@pdc:/usr/share/moin$ sudo cp -R underlay mywiki
dalcalam@pdc:/usr/share/moin$ sudo cp -server/moin.cgi mywiki
dalcalam@pdc:/usr/share/moin$ sudo cp server/moin.cgi mywiki
dalcalam@pdc:/usr/share/moin$ sudo chown -R www-data.www-data mywiki
dalcalam@pdc:/usr/share/moin$ sudo chmod -R ug+rwX mywiki
dalcalam@pdc:/usr/share/moin$ sudo chmod -R o-rwx mywiki
dalcalam@pdc:/usr/share/moin$

```

Configurem MoinMoin per que trobi el nou Wiki “mywiki”. Per fer això, editem l’arxiu /etc/moin/mywiki.py. Canviem la línia de la entrada “data_dir” i afegim una nova entrada “data_underlay_dir” amb el següent contingut:

```

GNU nano 2.2.2      Archivo: /etc/moin/mywiki.py      Modificado
# basic options (you normally need to change these)
sitename = u'MyWiki' # [Unicode]
interwikiname = u'MyWiki' # [Unicode]

# name of entry page / front page [Unicode], choose one of those:

# a) if most wiki content is in a single language
#page_front_page = u"MyStartingPage"

# b) if wiki content is maintained in many languages
page_front_page = u"FrontPage"

data_dir = '/usr/share/moin/mywiki/data/'
data_underlay_dir='/usr/share/moin/mywiki/underlay'

```

Ara configurem Apache perquè pugui accedir a la nostra Wiki “mywiki”. Per fer això, editem l’arxiu /etc/apache2/sites-avaible/default. Busquem l’etiqueta <Virtual Host> i dintre, li afegim les següents línies:

```

### moin
ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
alias /moin_static184 "/usr/share/moin/htdocs"
<Directory /usr/share/moin/htdocs>
Order allow,deny
allow from all
</Directory>
### end moin

```

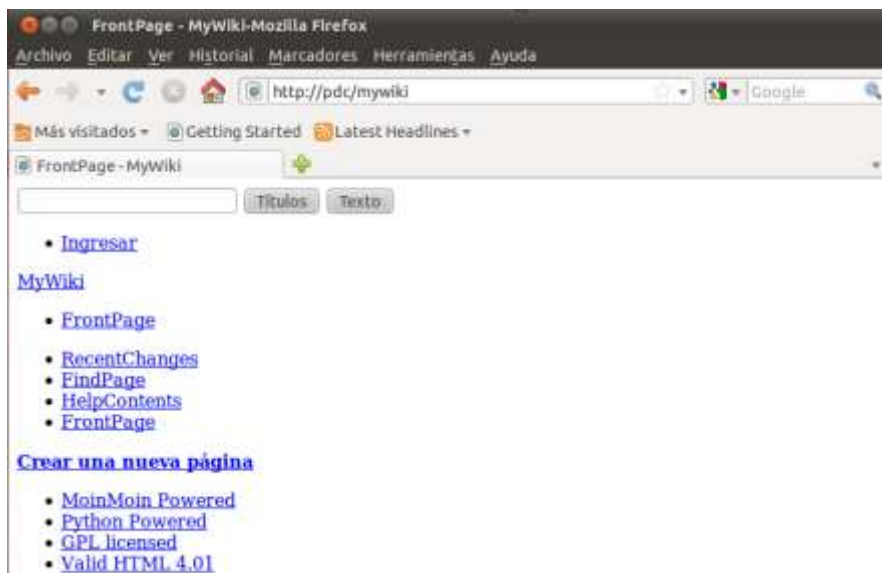
Seguidament, reiniciem el servei d’Apache de la següent manera:

```
sudo /etc/init.d/apache2 restart
```

Ja tenim el servidor de documentació MoinMoin instal·lar i configurat.

9.2. Prova d'accès al servidor de documentació des de un client.

Provem a accedir des de un client al nostre servidor de documentació:



Veiem que funciona correctament.

10. Implementació del servidor BDC

10.1. Configuració de l'LDAP de PDC per sincronitzar amb l'LDAP del BDC

La replicació es realitza amb el motor Syncrepl. Syncrepl permet que els canvis es sincronitzen amb un servidor secundari, el model del servidor primari. El servidor primari enviarà els canvis de directori LDAP al servidor secundari.

En el PDC, creem un arxiu anomenat provider_sync.ldif amb el següent contingut:

```
# Add indexes to the frontend db.
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

#Load the syncprov and accesslog modules.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
add: olcModuleLoad
olcModuleLoad: accesslog

# Accesslog database definitions
dn: olcDatabase={2}hdb,cn=config
```

```

objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=desint,dc=local
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl Provider for primary db
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# accesslog overlay definitions for primary db
dn: olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE
# scan the accesslog DB every day, and purge entries older than 7 days
olcAccessLogPurge: 07+00:00 01+00:00

```

Haurem d'ajustar el perfil de AppArmor per a Slap pe accedir a la "accesslog data base location". Per fer això, editem l'arxiu /etc/apparmor.d/usr.sbin.slapd i afegim:

```

/var/lib/ldap/accesslog/ r,
/var/lib/ldap/accesslog/** rwk,

```

Seguidament fem el següent:

```

dalcalam@pdc:~$ sudo -u openldap mkdir /var/lib/accesslog
dalcalam@pdc:~$ sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog
dalcalam@pdc:~$ sudo /etc/init.d/apparmor reload
* Reloading AppArmor profiles [ OK ]

```

Ara, afegim la nova estructura que hem creat a l'arxiu provider_sync.ldif al directori LDAP:

```

dalcalam@pdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcDatabase={2}hdb,cn=config"
adding new entry "olcOverlay=syncprov,olcDatabase={2}hdb,cn=config"
adding new entry "olcOverlay=syncprov,olcDatabase={1}hdb,cn=config"
adding new entry "olcOverlay=accesslog,olcDatabase={1}hdb,cn=config"

```

Amb això el servidor PDC sincronitzara el directori LDAP amb el directori LDAP del BDC.

Reinicem el servei slapd per que els canvis tinguin efecte:

```
sudo /etc/init.d/slapd restart
```

10.2. Configuració de l'LDAP de BDC per sincronitzar amb l'LDAP del PDC

Per configurar l'LDAP del BDC hem procedir a seguir els següents passos idèntics a la configuració del PDC i amb els mateixos arxius d'estructura de directori:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.example.com.ldif
sudo ldapadd -x -D cn=admin,dc=example,dc=com -W -f frontend.example.com.ldif
```

Ara, creem un arxiu anomenat consumer_sync.ldif amb el següent contingut:

```
#Load the syncprov module.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

# syncprov specific indices
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://pdc.desint.local bindmethod=simple binddn="cn=admin,dc=desint,dc=local"
credentials=secret searchbase="dc=desint,dc=local" logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)(reqResult=0))" schemachecking=on
type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://pdc.desint.local
```

Seguidament, afegim la nova estructura que hem creat a l'arxiu consumer_sync.ldif al directori LDAP del BDC:

```
dalcalam@bdc:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /home/dalcalam/consumer_sync.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config"
modifying entry "olcDatabase={1}hdb,cn=config"
```

10.3. Instal·lació i configuració de Samba per sincronitzar amb el PDC

Instal·lem els següents paquets:

```
sudo apt-get install samba libpam-smbpass
```


Editem els fitxer `/etc/samba/smb.conf`. Descomentem les següents línies de la secció [global]:

```
workgroup = WORKGROUP
...
security = user
```

En aquest mateix fitxer, descomentem en “Domains” les següents línies:

```
domain logons = yes
domain master = no
```

Ens assegurem que l'usuari administrador de Samba té privilegis per llegir a la carpeta `/var/lib/samba`:

```
dalcalam@bdc:~$ sudo chgrp -R admin /var/lib/samba
```

Reiniciem els serveis de samba per que els canvis tinguin efecte:

```
sudo restart smbd
sudo restart nmbd
```

11. Implementació del servidor proxy

11.1. Instal·lació i configuració d'Squid

Per instal·lar Squid procedim de la següent manera:

```
sudo apt-get install squid
```

Una vegada instal·lat, per configurar-lo hem d'editar l'arxiu `/etc/squid/squid.conf`. modifiquem les següents línies:

```
http_port 8888
visible_hostname proxy
acl fortytwo_network src 192.168.1.0/24

acl biz_network src 192.168.1.0/24
acl biz_hours time M T W T F 8:00-18:00
http_access allow biz_network biz_hours

cache_mem 16 MB
```

Amb això, aconseguim canviar el port d'escolta per defecte 3128 al port 8888, fem que el servidor s'anomeni “proxy”, configurem l'ACL per a tots els equips de la xarxa, restringim l'accès a internet a un horari determinat (8:00 – 18:00) i configurem una memòria cau de 16 MB.

Tenim que reiniciar el servei perquè la configuració sigui efectiva:

```
sudo /etc/init.d/squid restart
```

11.2. Restricció de llocs web.

Per restringir llocs web hem de crear un arxiu de text amb els llocs webs i les paraules clau que volem denegar. Creem l'arxiu `/etc/squid/llocsdenegats`:

```
GNU nano 2.2.2 Archivo: /etc/squid/llocsrestringits Modificado
www.megaupload.com
www.rapidshare.com
www.taringa.net
www.vagos.es
emule
spotify
sex
porn
mp3
xxx
adult
warez
```

Seguidament, afegim les següents línies al arxiu `/etc/squid/squid.conf`:

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
http_access deny all llocsrestringits
```

Tenim que reiniciar el servei perquè la configuració sigui efectiva:

```
sudo /etc/init.d/squid restart
```

11.3. Prova de servidor proxy.

Per provar el servidor proxy, intentem accedir a lloc web restringit www.megaupload.com:



Veiem que el servidor proxy ens restringeix l'accés. El que vol dir que està funcionant correctament.

12. Implementació del Firewall

12.1. Activació i configuració del tallafocs

L'eina de configuració del Firewall per defecte d'Ubuntu és UFW. Desenvolupat per facilitar la configuració de tallafocs iptables, UFW proporciona una manera fàcil de configurar-ho per a Firewall basat en host.

UFW per defecte està inicialment desactivat. L'activem de la següent manera:

```
dalcalam@pdc:~$ sudo ufw enable
Password:
El cortafuegos está activo y habilitado en el arranque del sistema
```

Inicialment deneguem totes les connexions de la següent manera:

```
dalcalam@proxym:~$ sudo ufw default deny
[sudo] password for dalcalam:
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
```

Permetem la connexió entre la nostre xarxa local:

```
dalcalam@proxym:~$ sudo ufw allow from 192.168.1.0/24
Regla agregada
```

Ara, configurarem el tallafocs per habilitar l'accés a internet per la nostra xarxa local que es troba darrera d'un router (NAT). Editem l'arxiu `/etc/ufw/sysctl.conf` i descomentem les següents línies:

```
net/ipv4/ip_forward=1
net/ipv6/conf/default/forwarding=1
```

Afegim les regles a l'arxiu `/etc/ufw/before.rules`. Ho fem editant-lo i afegint les següents línies:

```
# nat Table rules
*nat
:POSTROUTING ACCEPT [0:0]

# Forward traffic from eth1 through eth0.
-A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these nat table rules won't be processed
COMMIT
```

Finalment, deshabilitem y habilitem el Firewall per que els canvis tinguin efecte.

```
dalcalam@proxym:~$ sudo ufw disable && sudo ufw enable
El cortafuegos está detenido y desactivado en el arranque del sistema
El cortafuegos está activo y habilitado en el arranque del sistema
```



```

dalcalam@proxy:/etc/openvpn/easy-rsa$ ./pktool --server server
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'SP'
stateOrProvinceName :PRINTABLE:'BCN'
localityName      :PRINTABLE:'Barcelona'
organizationName  :T61STRING:'Desenvolupament Intel\0xFFFFFC2\0xFFFFFB7lig
ents'
commonName        :PRINTABLE:'server'
emailAddress      :IA5STRING:'dalcalam@desint.local'
Certificate is to be certified until Jun  9 15:39:53 2021 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
dalcalam@proxy:/etc/openvpn/easy-rsa$ cd keys
dalcalam@proxy:/etc/openvpn/easy-rsa/keys$ openvpn --genkey --secret ta.key
dalcalam@proxy:/etc/openvpn/easy-rsa/keys$ sudo cp server.crt server.key ca.crt
dh1024.pem ta.key /etc/openvpn

```

13.3. Creació de certificat per als clients.

En client VPN també necessitem un certificat per autenticar-nos al servidor. Per crear el certificat fem el següent:

```

dalcalam@proxy:/etc/openvpn/easy-rsa/keys$ cd /etc/openvpn/easy-rsa/
dalcalam@proxy:/etc/openvpn/easy-rsa$ source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/
keys
dalcalam@proxy:/etc/openvpn/easy-rsa$ ./pktool hostname
Generating a 1024 bit RSA private key
.....+++++
..+++++
writing new private key to 'hostname.key'
-----
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'SP'
stateOrProvinceName :PRINTABLE:'BCN'
localityName      :PRINTABLE:'Barcelona'
organizationName  :T61STRING:'Desenvolupament Intel\0xFFFFFC2\0xFFFFFB7lig
ents'
commonName        :PRINTABLE:'hostname'
emailAddress      :IA5STRING:'dalcalam@desint.local'
Certificate is to be certified until Jun  9 15:53:45 2021 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

```

Per fer servir el certificat en el client, hem de copiar els següents arxius en el client:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/hostname.crt
- /etc/openvpn/easy-rsa/keys/hostname.key
- /etc/openvpn/ta.key

Hem de canviar "hostname" per el nom de la màquina client.

13.4. Configuració del servidor VPN.

Per configurar el servidor VPN hem de crear l'arxiu `/etc/openvpn/server.conf`:

```
dalcalam@proxy:/$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/  
[sudo] password for dalcalam:  
dalcalam@proxy:/$ sudo gzip -d /etc/openvpn/server.conf.gz
```

Editem l'arxiu `/etc/openvpn/server.conf` amb les següents opcions:

```
local 172.18.100.101  
dev tap0  
up "/etc/openvpn/up.sh br0"  
down "/etc/openvpn/down.sh br0"  
;server 10.8.0.0 255.255.255.0  
server-bridge 172.18.100.101 255.255.255.0 172.18.100.105 172.18.100.200  
push "route 172.18.100.1 255.255.255.0"  
push "dhcp-option DNS 172.18.100.20"  
push "dhcp-option DOMAIN example.com"  
tls-auth ta.key 0 # This file is secret  
user nobody  
group nogroup
```

A continuació, creem un parell de scripts per afegir al interface tap per al pont. Primer creem l'script `/etc/openvpn/up.sh`:

```
#!/bin/sh  
  
BR=$1  
DEV=$2  
MTU=$3  
/sbin/ifconfig $DEV mtu $MTU promisc up  
/usr/sbin/brctl addif $BR $DEV
```

Y ara `/etc/openvpn/down.sh`:

```
#!/bin/sh  
  
BR=$1  
DEV=$2  
  
/usr/sbin/brctl delif $BR $DEV  
/sbin/ifconfig $DEV down
```

Assignem els següents permisos als scripts:

```
sudo chmod 755 /etc/openvpn/down.sh  
sudo chmod 755 /etc/openvpn/up.sh
```

Per acabar, reiniciem el servidor:

```
sudo /etc/init.d/openvpn restart
```

13.5. Configuració del client VPN

Instal·lem el client `openvpn` de la següent manera:

```
sudo apt-get install openvpn
```

Ara hem de copiar els certificats abans creats en el client a les següents carpetes:

- `/etc/openvpn/ca.crt`
- `/etc/openvpn/easy-rsa/keys/hostname.crt`
- `/etc/openvpn/easy-rsa/keys/hostname.key`
- `/etc/openvpn/ta.key`

Hem de canviar "hostname" per el nom de la màquina client.

Quan tenim copiats els certificats, fem el següent:

```
dalcalam@proxy:/$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
```

Editem l'arxiu `/etc/openvpn/client.conf` i canviem les següents línies:

```
dev tap
remote vpn.example.com 1194
cert hostname.crt
key hostname.key
tls-auth ta.key 1
```

Hem de canviar "hostname" per el nom de la màquina client.

Per finalitzar, reiniciem el servidor VPN:

```
sudo /etc/init.d/openvpn restart
```

14. Implementació del servidor Web

14.1. Instal·lació i configuració del servidor Web

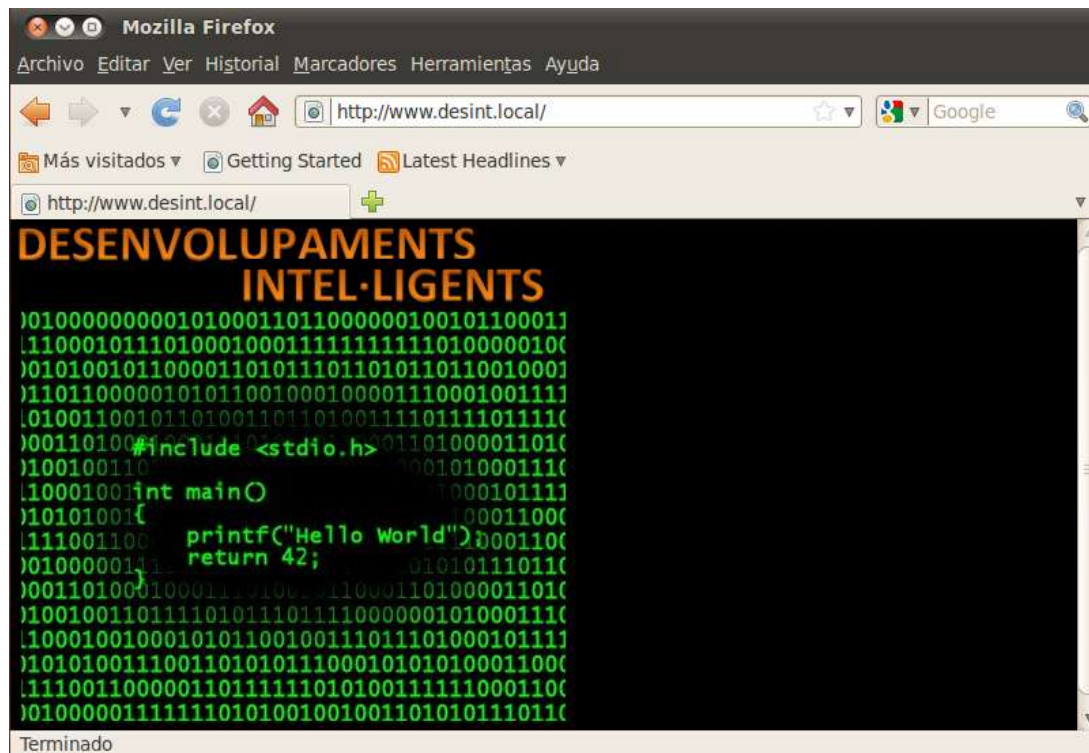
Instal·lem el paquet `apache2`:

```
sudo apt-get install apache2
```

Deixem la configuració per defecte. Copiem els arxius de la nostra web a al directori `/var/www` i ja tenim la nostra web funcionant.

14.2. Prova del servidor Web des de un ordinador d'escriptori

Accedim des de un ordinador d'escriptori a www.desint.local:



Veiem que accedim a la nostra web correctament.

15. Configuració dels ordinadors d'escriptori

15.1. Configurar l'ordinador per autenticar-se contra el domini

Per afegir un ordinador amb Ubuntu al domini, primer hem d'instal·lar els següents paquets:

```
sudo apt-get install auth-client-config libpam-ldap libnss-ldap
```

Ens sortirà un assistent per configurar el client. Contestem a les preguntes amb les següents respostes:

- **LDAP Server Uniform Resource Identifier:** ldap://192.168.1.11
- **Distinguished name of the search base:** dc=desint,dc=local
- **LDAP version to use:** 3
- **Make local root Database admin?:** Yes
- **Does the LDAP database require login?:** Yes
- **LDAP account for root:** cn=admin,dc=desint,dc=local
- **LDAP root account password:** L3oM3ss1

Editem l'arxiu `/etc/ldap.conf` i canviem les següents línies amb aels valors indicats:

```
host 192.168.1.11
base dc=desint,=dc=local
uri ldap://192.168.1.11
rootbinddn cn=admin,dc=desint,dc=local
bind_policy_soft
```

Copiem aquest arxiu a la destinació indicada:

```
Archivo Editar Ver Buscar Terminal Ayuda
user1@client1:~$ sudo cp /etc/ldap.conf /etc/ldap/ldap.conf
user1@client1:~$
```

Creem l'arxiu de perfil `/etc/auth-client-config/profile.d/open_ldap`. Afegim el següent contingut:

```
[open_ldap]
nss_passwd=passwd: compat ldap
nss_group=group: compat ldap
nss_shadow=shadow: compat ldap
pam_auth=auth          required      pam_env.so
auth          sufficient  pam_unix.so likeauth nullok
auth          sufficient  pam_ldap.so use_first_pass
auth          required    pam_deny.so
pam_account=account   sufficient pam_unix.so
account       sufficient  pam_ldap.so
account       required    pam_deny.so
pam_password=password sufficient  pam_unix.so nullok md5 shadow use_authok
password      sufficient  pam_ldap.so use_first_pass
password      required    pam_deny.so
pam_session=session  required    pam_limits.so
session       required    pam_mkhomedir.so skel=/etc/skel/
session       required    pam_unix.so
session       optional   pam_ldap.so
```

Activem el perfil d'autenticació LDAP que acabem de crear de la següent manera:

```
sudo auth-client-config -a -p open_ldap
```

Reiniciem l'ordinador per que els canvis tinguin efecte:

```
sudo reboot
```

15.2. Configuració per exportar el home de l'usuari del servidor de domini.

Si volem que es munti el home de l'usuari del servidor en l'ordinador d'escriptori, primer de tot hem d'instal·lar el següent paquet:

```
sudo apt-get install nfs-common
```

Seguidament, editem l'arxiu `/etc/fstab` afegint-li la següent línia:

```
192.168.1.11:/home /home nfs defaults 0 0
```

15.3. Configuració del servidor proxy

Per configurar el nostre proxy en els ordinadors d'escriptori amb Ubuntu, anem al menú Sistema i seleccionem "Preferències->Proxy de la red". El configurem de la següent manera:



16. Glossari

16.1. Glossari

Amavisd-new: És una interfície confiable i d'alt acompliment entre l'agent de transport de correu (MTA, Mail Transport Agent) i un o més supervisors de contingut, com és el cas de supervisors anti-virus, i/o SpamAssassin.

APACHE: El servidor HTTP Apache és un servidor web HTTP de codi obert per a plataformes Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh i altres, que implementa el protocol HTTP / 1.1 i la noció de lloc virtual.

BACKUP: Còpia d'informació que es realitza per tal de ser restaurada en cas de pèrdua de dades o en cas de ser requerida en posterioritat.

BDC (Backup Domain Controloller): En català Controlador de Còpia de Seguretat de Domini és un servidor que conté una còpia de la base de dades del directori del PDC i pot donar aquest servei en cas de caiguda del PDC. Es pot promocionar a PDC en cas necessari

ClamAV: És una eina utilitzada en la inspecció de missatges electrònics que permet identificar si el contingut del correu és un virus.

CUPS (Common Unix Printing System): És un sistema d'impressió modular per a sistemes operatius

de tipus Unix que permet que un ordinador actuï com a servidor d'impressió. Un ordinador que executa CUPS actua com un servidor que pot acceptar tasques d'impressió des d'altres ordinadors clients, els processa i els envia al servidor d'impressió apropiat.

CVS (Concurrent Versions System o simplement): És una aplicació informàtica que implementa un sistema de control de versions: manté el registre de tot el treball i els canvis en els fitxers (codi font principalment) que formen un projecte (de programa) i permet que diferents desenvolupadors (potencialment situats a gran distància) col·laborin. CVS s'ha fet popular al món del programari lliure. Els seus desenvolupadors difonen el sistema sota la llicència GPL.

Domini: En una xarxa d'àrea local, és un conjunt d'ordinadors connectats a la xarxa que confien a uns dels equips (anomenat controlador de domini) la administració dels usuaris i els privilegis que tenen aquests sobre els recursos compartits disponibles.

Dovecot: És un servidor de IMAP i POP3 de codi obert per a sistemes GNU/Linux / UNIX-like, escrit fonamentalment pensant en seguretat. Desenvolupat per Timo Sirainen.

Firewall: és un element de maquinari o programari utilitzat en una xarxa d'equips informàtics per controlar les comunicacions, permetent-les o prohibint-les segons les polítiques de xarxa que hagi definit l'organització responsable de la xarxa.

HTTP (HyperText Transfer Protocol): Estableix el protocol per a l'intercanvi de documents d'hipertext i multimèdia al web.

HTTPS (Hypertext Transfer Protocol sobre Secure Socket Layer): És la capçalera d'URI utilitzada per a indicar una connexió segura HTTP.

IMAP: Protocol d'accés als missatges d'Internet, de l'anglès Internet Message Access Protocol (antigament Internet Mail Access Protocol) és un protocol informàtic, basat en TCP/IP, que permet als usuaris llegir els seus correus electrònics en el servidor i tan sols descarregar missatges i fitxers adjunts en la màquina local quan sigui necessari.

LDAP (Lightweight Directory Acces Protocol): En català Protocol Lleuger d'Accés a Directoris) és un protocol de tipus client-servidor per accedir a un servei de directori. Es va fer servir inicialment com un Front-end o interfície final per a x.500, però també pot usar-se amb servidors de directori únics i amb altres tipus de servidors de directori. En aquest capítol veiem pas a pas com ho hem configurat per que ofereixi el servei d'autenticació d'usuaris. No obstant això, LDAP es pot utilitzar de moltes maneres: autenticació, directori compartit (per a clients de correu), llibreta d'adreces, etc

MTA (Mail Transfer Agent): És una aplicació informàtica que ens permet enviar missatges (correus) d'uns usuaris a altres, amb independència de la xarxa que aquests usuaris estiguin utilitzant. Entre els més usats trobem Postfix, sendmail i Exim.

NFS (Network File System): És un protocol de sistema de fitxers en xarxa originalment desenvolupat per Sun Microsystems el 1983, que permet a una computadora client accedir a fitxers a través de xarxa fàcilment, com si els dispositius físics d'emmagatzemament (normalment discs durs) estiguessin directament connectats a l'ordinador. NFS funciona sobre el protocol RPC.

PDC (Primary Domain Controloller): En català Controlador Primari de Domini és el controlador de domini principal. Aquest servidor conté la base de dades del directori i és el que dona aquest servei.

Per tant, és l'encarregat de validar als usuaris i controlar els privilegis que tenen aquests sobre els recursos compartits disponibles al nostre domini.

POP3 (Post Office Protocol versió 3): És un protocol que s'utilitza per recollir el correu electrònic. Es tracta d'un protocol força senzill que permet poques interaccions amb el servidor de correu, normalment el correu és recuperat i esborrat del servidor.

Postfix: És un servidor de correu de programari lliure / codi obert, un programa informàtic per a l'enrutament i enviament de correu electrònic, creat amb la intenció que sigui una alternativa més ràpida, fàcil d'administrar i segura al àmpliament utilitzat Sendmail.

Proxy: Un programa o dispositiu que realitza una acció en representació d'un altre. La seva finalitat més habitual és la de servidor proxy, que serveix per a permetre l'accés a Internet a tots els equips d'una organització quan només es pot disposar d'un únic equip connectat, això és, una única adreça IP.

OpenLDAP: És una implementació lliure i de codi obert del protocol Lightweight Directory Access Protocol (LDAP) desenvolupada pel projecte OpenLDAP. Està alliberada sota la seva pròpia llicència OpenLDAP Public License. LDAP és un protocol de comunicació independent de la plataforma.

OpenSSH (Open Secure Shell): és un conjunt d'aplicacions que permeten realitzar comunicacions xifrades a través d'una xarxa, utilitzant el protocol SSH. Va ser creat com una alternativa lliure i oberta al programa Secure Shell, que és programari propietari.

Samba: És una implementació lliure del protocol d'arxius compartits de Microsoft Windows (antigament anomenat SMB, actualment anomenat CIFS). D'aquesta forma, és possible que ordinadors amb GNU/Linux, Mac OS X o Unix actuïn com a servidors o actuïn com a clients en xarxes de Windows. Samba també pot validar usuaris fent de Controlador Principal de Domini (PDC), com a membre de domini i tot com un domini Active Directory per a xarxes basades en Windows; a part de ser capservidor cues d'impressió, directoris compartits i autenticar amb el seu propi arxiu d'usuaris.

SMTP (Simple Mail Transfer Protocol): És a dir protocol simple de transferència de correu i és un protocol de xarxa basat en text utilitzat per a l'intercanvi de missatges de correu electrònic entre ordinador i/o diversos dispositius (PDAs, mòbils, etc).

Spamassassin: És una eina per inspeccionar correus electrònics que permet determinar si es tracta d'un SPAM.

Squid: És un popular programa de software lliure que implementa un servidor proxy y un domini per memòria cau de pàgines web, publicat sota llicència GPL. Proporciona serveis de proxy i memòria cau per a Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), i altres protocols de xarxa populars

SquirrelMail: És una aplicació webmail creada per Nathan i Luke Ehresman i escrita en PHP. Pot ser instal·lat en la majoria de servidors web sempre que aquest suport PHP i el servidor web tingui accés a un servidor IMAP i un altre SMTP.

SSH (Secure Shell): És el nom d'un protocol i del programa que ho implementa, i serveix per accedir a màquines remotes a través d'una xarxa. Permet manejar per complet la computadora mitjançant un intèrpret de comandos, i també pot redirigir el tràfic de X per poder executar programes gràfics si

tenim un Servidor X (en sistemes Unix i Windows) corrent.

UFW (Uncomplicated Firewall): És un tallafocs dissenyat per ser de fàcil ús desenvolupat per Ubuntu. Utilitza la línia de comandos per configurar les iptables usant un petit nombre de comandos simples.

VPN: de les sigles en anglès de Virtual Private Network , és una tecnologia de xarxa que permet una extensió de la xarxa local sobre una xarxa pública o no controlada, com per exemple Internet.

17. Bibliografia:

17.1. Bibliografia.

Introducció al mon de GNU/Linux i programari lliure:

<http://ca.wikipedia.org/>

<http://es.wikipedia.org/>

Estudi sobre distribucions Linux:

<http://www.debian.org/index.es.html>

<http://www.ubuntu-es.org/>

<http://www.es.redhat.com/>

<http://fedoraproject.org/>

<http://es.opensuse.org/Bienvenidos a openSUSE.org>

<http://www.gentoo.org/>

<http://distrowatch.com/>

<http://www.espaciolinux.com/foros/?index.php>

<http://www.redes-linux.com/phpBB/index.php>

<http://www.linux-es.org/distribuciones>

<http://mundogeek.net/archivos/2010/02/06/la-mejor-distribucion-linux/>

Estudi sobre programari lliure per l'empresa:

<http://www.openldap.org/>

<http://www.samba.org/>

<http://www.cvshome.org/>

<http://www.cups.org/>

<http://www.apache.org/>

<http://www.postfix.org/>

<http://www.dovecot.org/>

<http://squirrelmail.org/>

<http://es.libreoffice.org/>

<http://openproj.org/>

<http://www.koffice.org/kivio/>

<http://projects.gnome.org/brasero/>

<http://www.eclipse.org/>

<http://www.kdevelop.org/>

<http://gambas.sourceforge.net/>

<http://www.espaciolinux.com/foros/?index.php>

<http://www.redes-linux.com/phpBB/index.php>

<http://www.ubuntu-es.org/forum>

Instal·lar i configurar openSSH:

<https://help.ubuntu.com/10.04/serverguide/C/openssh-server.html>

Instal·lar i configurar NFS:

<https://help.ubuntu.com/10.04/serverguide/C/network-file-system.html>

Implementació i configuració de LDAP:

<http://www.ldap-es.org/node/20>

<https://help.ubuntu.com/10.04/serverguide/C/openldap-server.html>

Samba-LDAP:

<http://ubuntuforums.org/archive/index.php/t-1104050.html>

http://elcorteingles.bdat.net/documentos/validacion_ldap/c294.html

Samba com servidor d'arxius:

<https://help.ubuntu.com/10.04/serverguide/C/samba-fileserver.html>

<https://help.ubuntu.com/10.04/serverguide/C/samba-fileprint-security.html>

Samba com servidor d'impressió :

<https://help.ubuntu.com/10.04/serverguide/C/samba-printserver.html>

<https://help.ubuntu.com/10.04/serverguide/C/samba-fileprint-security.html>

Servidor de correu SMTP, IMAP, Webmail, antiSpam:

<https://help.ubuntu.com/10.04/serverguide/C/postfix.html>

<https://help.ubuntu.com/10.04/serverguide/C/dovecot-server.html>

<https://help.ubuntu.com/community/Dovecot>

<http://wiki2.dovecot.org/>

<http://pedroreina.net/recetas/squirrelmail.html>

<http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-squirrelmail>

<https://help.ubuntu.com/10.04/serverguide/C/mail-filtering.html>

Servidor de versions:

<https://help.ubuntu.com/10.04/serverguide/C/cvs-server.html>

Servidor de gestió de documentació:

<https://help.ubuntu.com/10.04/serverguide/C/moinmoin.html>

Servidor proxy:

<https://help.ubuntu.com/10.04/serverguide/C/squid.html>

Firewall:

<https://help.ubuntu.com/10.04/serverguide/C/firewall.html>

http://es.wikipedia.org/wiki/Uncomplicated_Firewall

Servidor VPN:

<https://help.ubuntu.com/10.04/serverguide/C/vpn.html>

Servidor BDC:

<https://help.ubuntu.com/10.04/serverguide/C/samba-dc.html>

<https://help.ubuntu.com/10.04/serverguide/C/openldap-server.html>