Migració de servidor de centre

Administració de xarxes i de sistemes operatius

Autor
Arnaldo González de Mingo

Consultor
Miguel Martín Mateo

Tutora
Rosa Maria Riera Ubach

Artés, maig 2013

Llicència

Resum

El projecte “Migració de servidor de centre” té com a propòsit principal la migració de servidors i la creació de nous serveis utilitzant programari lliure, dins l'entorn d'un centre educatiu. El projecte contempla la renovació, reutilització i reubicació de servidors, i la reestructuració de la xarxa docent per tal d'adaptar-la a la nova situació.

Una de les actuacions és la creació d'un controlador de domini amb OpenLDAP i Samba, en substitució de l'Active Directory de l'antic servidor de centre. D'aquesta manera s'assegura que cada usuari disposa d'un espai personal i espais compartits on intercanviar documents.

El projecte també proposa la creació d'un nou servei on alumnes i professors puguin accedir als seus espais personals des d'Internet. El servlet Davenport ens ofereix la possibilitat d'accedir via WebDAV a un recurs compartit de Samba a través d'un contenidor. Es contempla utilitzar el servidor Tomcat com a contenidor del servlet.

Taula de continguts

1. Introducció

L'institut Miquel Bosch i Jover és un centre educatiu de secundària situat en el poble d'Artés dins de la comarca del Bages. Actualment hi estudien uns 450 alumnes, repartits entre secundària obligatòria i batxillerat. Recull alumnes d'Artés, i dels municipis propers: Avinyó, Santa Maria d'Oló, Calders i Monistrol de Calders.

Al llarg dels anys i a causa de l'increment del nombre d'alumnes el centre ha patit diferents ampliacions fins arribar a la situació actual. Paral·lelament, el nombre i l'ús dels ordinadors també s'ha incrementat i generalitzat. Amb l'entrada del centre en el projecte Educat 1x1 fa dos anys, pràcticament totes les aules disposen de pissarra digital i ordinador multimèdia.

Totes aquestes ampliacions s'han fet mantenint el mateix servidor, un vell ordinador amb el sistema operatiu Windows 2000 Server, que des de l'any 2003 ha donat servei d'autenticació, espais personals i espais compartits a tots els alumnes, professors i personal no docent. Amb els anys, el servei s'ha anat degradant, i actualment el servidor presenta, de tant en tant, problemes de desconnexió, fent que els usuaris no puguin accedir als espais compartits.

Vista la situació, i des de la comissió TIC del centre, es va plantejar la possibilitat de canviar de servidor i demanar a l'AMPA del centre el finançament d'un nou servidor. La resposta va ser positiva i actualment el centre disposa d'un nou servidor preparat per a ser utilitzat.

Gràcies al conveni de cooperació educativa entre la Fundació per a la Universitat Oberta de Catalunya i el mateix institut, hem pogut tirar endavant aquest projecte de migració del servidor cap al programari lliure.

1.1 Objectius

Els objectius del projecte que es volen assolir són els següents:

- Renovar el servidor de centre amb un nou equip. Una màquina nova ens oferirà una fiabilitat i un rendiment superiors.

- Elaborar un nou servei de directori i autenticació. Mantenint l'esquema actual, cada usuari disposarà d'un espai personal i podrà accedir als espais compartits des de la Intranet del centre.

- Oferir nous serveis als usuaris. Amb la utilització dels Netbooks per part dels alumnes i dels ordinadors personals per part dels professors, la demanda generalitzada és poder accedir als espais personals i compartits, no tant sols des de la Intranet, sinó també des d'Internet. Aquest serà un dels objectius del projecte.

- Optimitzar el servei d'impressió de centre. Al llarg dels anys les impressores del centre s'han anat instal·lant sense cap planificació, el projecte ens ofereix una oportunitat per racionalitzar aquest servei.

- Mantenir el servidor actualitzat. El programari lliure ens brinda l'oportunitat, sense problemes de llicències privatives, de mantenir el servidor més actualitzat i segur.

1.2 Estructura de la memòria

La memòria s'estructura en diferents apartats. En el primer apartat es fa una introducció, indicant el motiu principal pel qual s'ha escollit el projecte i es defineixen els objectius inicials plantejats.

En el segon apartat es fa l'estudi de viabilitat en el qual, un cop recollides les necessitats i requisits plantejats pel centre educatiu i feta l'anàlisi de la situació inicial, es defineixen els requisits que haurà de complir el nou sistema. S'estudien alternatives, maquinari disponible i costos del projecte.

En el tercer apartat es defineixen de manera exacta els requisits del projecte, amb l'objectiu de facilitar la preparació del seu disseny i la seva arquitectura.

En l'apartat quart s'inicia el procés de disseny de la solució seleccionant els serveis i la seva ubicació física en els ordinadors disponibles. També s'analitza com integrar aquests nous elements dins la xarxa del centre.

L'objectiu principal de l'apartat cinquè és la construcció ordenada del

sistema a partir del disseny abans analitzat.

Al llarg de l'apartat sisè es fan proves de funcionament i es comenten les aportacions del projecte, tant des del punt de vista dels usuaris com dels administradors. També hi ha un resum de les implicacions econòmiques que ha representat per al centre el dur a terme aquest projecte.

En l'apartat de conclusions es fa una valoració final del projecte, analitzant els objectius aconseguits i els no aconseguits, així com una valoració a nivell personal.

La memòria acaba amb la bibliografia, webgrafia i annexos, on troben alguns dels arxius de configuració dels serveis implantats.

2. Estudi de viabilitat

Començarem l'estudi de viabilitat recollint les necessitats i requisits plantejats pel centre educatiu. Tot seguit farem una anàlisi de l'arquitectura de xarxa del centre, per tal de definir els requisits que haurà de complir el nou sistema. Per acabar, mirarem les alternatives de solució que tenim, així com el maquinari disponible i els costos del projecte.

2.1 Necessitats i requisits plantejats pel centre

Després de diferents reunions portades a terme per la comissió TIC del centre, es van establir una sèrie de requisits, que el projecte de canvi de servidor hauria d'assegurar:

- Migrar tots els serveis de l'actual servidor cap al programari lliure.
- Continuar amb el mateix model d'autenticació: nom d'usuari i contrasenya.
- Mantenir l'actual esquema d'espais personals i espais compartits accessibles des de la Intranet.
- Afegir un nou servei que permeti accedir als espais personals i espais compartits des d'Internet.
- Implantar un sistema centralitzat d'impressió.
- Automatitzar l'actual sistema de còpies de seguretat del servidor.

De moment, la comissió fixa la migració cap al programari lliure a nivell de servidors, i posposa l'aplicació a la resta d'estacions de treball del centre per més endavant. Algunes de les raons que han portat a prendre aquesta decisió són les limitacions en la dedicació horària per part del coordinador d'informàtica i la manca de pressupost que actualment pateix el centre.

2.2 Anàlisi de la situació actual

Primer de tot, caldrà fer una anàlisi de l'arquitectura de xarxa de què disposa el centre actualment. Aquest estudi inicial ens facilitarà posteriorment determinar quines adequacions i quins canvis caldrà fer per tal d'implementar els requisits exigits pel projecte.

La xarxa educativa del centre està estructurada en 5 subxarxes o VLANs diferents (veure Annex A). El nom de cada VLAN i el rang d'IP's associada per a cada VLAN queda resumit en la taula següent:

Nom VLAN	Rang d'IP's per a cada VLAN
VLAN 2: Educativa cable	192.168.0.0/22
VLAN 4: Gestió de commutadors i punts d'accés	192.168.140.0/24
VLAN 5 - Convidats Wi-Fi Eduroam	192.168.150.0/24
VLAN 7 - Educativa Wi-Fi educat	192.168.168.0/21
VLAN 10 - Administració	192.168.110.0/24

Taula 1. Estructura de VLANs del centre

Dins VLAN 2 tenim incorporats tots els equips docents del centre: ordinadors de les aules ordinàries, aula d'informàtica, biblioteca, sala de professors i departaments.

Per a VLAN 4 s'habilita el rang IP 192.168.140.0/24 dedicat a la gestió de commutadors i de la controladora dels punts d'accés.

VLAN 5 dóna accés a Internet per a aquells visitants que participen en el projecte Eduroam.

VLAN 7 és la xarxa educativa Wi-Fi educat. Mitjançant aquesta xarxa, els alumnes es connecten a Internet amb el seu portàtil.

VLAN 10 està reservada per a tots els equips d'administració del centre: ordinadors de secretaria, consergeria, cap d'estudis i direcció.

Com a dispositius principals podem identificar:

Servidor de centre. Es tracta d'un ordinador amb processador Intel Core 2 Duo, 4 GB de memòria RAM i disposa de dos discos de 400 GB en RAID 1 per cobrir les necessitats de redundància. Les còpies de seguretat es fan mitjançant un disc extern de 1 TB. El sistema de còpies no està automatitzat.

Amb el sistema operatiu Windows Server 2000, dóna servei de directori i permet l'accés dels usuaris als recursos compartits. Té activat el servei DNS que és utilitzat de forma interna dintre de la Intranet. Forma part de la VLAN 2 i té adreçament 192.168.0.207.

Encaminador XEBA. Abans de la implantació del projecte EduCAT 2.0, era l'únic dispositiu que permetia la sortida cap a Internet. Actualment està balancejat amb la resta d'ADSL del projecte EduCAT 2.0. El centre no té accés a la seva configuració, que és controlada pel Departament d'Ensenyament.

ROSC0. Switch principal que segmenta les VLANs i delega la gestió al tallafocs FORTIGATE.

Servidor web faltes. Ordinador Pentium D Dual Core, d'1 GB de memòria RAM i 150 GB de disc dur. Actualment no disposa de cap sistema automatitzat de còpies de seguretat.

Forma part de la infraestructura que l'institut va implantar per tal de portar el control de faltes d'assistència mitjançant PDA (projecte que va ser dut a terme fa quatre anys per una empresa de la comarca).

Utilitza el sistema operatiu Windows Server 2003 i el programa EasyPHP (Apache, MySQL, PHP) per enllaçar via web el servidor amb les PDAs. També té activat el servei DNS per resoldre el domini del centre de les consultes que arriben de l'exterior. Actualment tant l'ordinador com les PDAs són propietat del centre.

ADSL propi. El centre té accés a la seva configuració. Encamina les peticions en el ports 80 i 56 cap al servidor de faltes.

Controladora Wi-Fi. Controla els punts d'accés del projecte EduCAT 2.0. És propietat de Telefonica i el centre no té accés a la seva configuració.

Fortigate. Fa les funcions d'encaminador i tallafocs. També s'encarrega

del balanceig de càrrega entre les tres ADSL del projecte EduCAT 2.0 i ofereix servei DHCP als NetBooks. Gestiona les diferents VLANs, fent que la visibilitat entre elles sigui la següent:

	VLAN 2	VLAN 4	VLAN 5	VLAN 7	VLAN 10	Servidors locals
VLAN 2	Sí	No	No	No	No	Sí
VLAN 4	No	Sí	No	No	No	No
VLAN 5	No	No	Sí	No	No	No
VLAN 7	No	No	No	Sí	No	No
VLAN 10	No	No	No	No	Sí	Sí

Taula 2. Visibilitat entre VLANs

És propietat de Telefonica i el centre no té accés a la seva configuració.

BlueCoat. Fa les funcions de proxy-caché i filtre de continguts del projecte EduCAT 2.0. És propietat de Telefonica i el centre no té accés a la seva configuració.

La resta d'equips del centre estan incorporats a la VLAN 2. Distribuïts per diferents espais, utilitzen Windows XP Professional com a sistema operatiu. Un únic ordinador utilitza Windows Vista.

2.3 Definició de requisits del sistema

Un cop feta l'anàlisi de la situació actual i tenint en consideració els requisits d'entrada plantejats per la comissió TIC, podem establir una definició de requisits del nou sistema:

- Cada usuari ha de poder accedir a les dades independentment de l'ordinador del centre que faci servir.
- Tots els usuaris han de poder accedir al seu espai personal i espais compartits des d'Internet.
- Migrar tots els serveis de l'actual servidor de centre cap al programari lliure.
- Garantir un sistema de discos redundants en el nou servidor de centre.

- Mantenir connexions segures amb el servidor de faltes.
- Migrar tots els serveis de l'actual servidor de faltes cap al programari lliure.
- Protegir la xarxa educativa del centre de possibles atacs exteriors.
- Implantar un sistema centralitzat d'impressió.
- Automatitzar el sistema de còpies de seguretat, tant del servidor de centre com del servidor de faltes.
- Mantenir la resta d'elements de la xarxa amb la configuració actual.

2.4 Estudi d'alternatives i elecció de les possibles solucions

Bàsicament, el projecte tracta de la migració de serveis i servidors cap al programari lliure. Afecta únicament els servidors del centre i les aplicacions o serveis que s'hi executen. Serà necessari decidir la distribució GNU/Linux amb què treballaran aquests servidors.

Linkat és la distribució GNU/Linux que el Departament d'Ensenyament va posar a disposició de la comunitat educativa. Es basa en OpenSUSE i la versió actual és la Linkat 4. Una de les avantatges de la Linkat és que incorpora una serie de scripts que automatitzen la configuració del model de servidor de centre. Aquesta automatització pot resultar un inconvenient i un niu de mals de cap quan es vol fer una configuració més personalitzada i adaptada a les característiques del centre. Moltes vegades, aquests scripts modifiquen directament els arxius de configuració dels diferents serveis i impedeixen tenir un control directe sobre aquests. Aquesta última valoració ens ha fet descartar aquesta distribució.

De la resta de distribucions conegudes, totes disposen de la seva versió per a servidor. Abans d'escollir-ne una en concret, hem fixat les condicions que hauria de complir:

- Que s'adapti al nostre maquinari disponible.

- Que ofereixi actualitzacions durant un temps raonable.
- Que sigui estable i segura.
- Que disposi d'una amplia infraestructura d'ajuda als usuaris.
- Que s'adapti al nostre pressupost.

També hem elaborat una comparativa per facilitar-ne l'elecció. Les taules 3 i 4 recullen aquesta comparativa.

Distribució	**RHEL**	**CentOS**	**Debian**	**Ubuntu Server**
Organització	Red Hat Inc. www.redhat.com	CentOS Project www.centos.org	Debian Project www.debian.org	Canonical www.ubuntu.com
Llicència	GPL	GPL	GPL	GPL
Darrera versió estable	6.3 (2011)	6.3 (2012)	6 Squeeze (2011)	12.04 LTS (2012)
Cost	Pel suport: mínim 349 US$ per servidor	Gratuïta, basada en Red Hat (donacions)	Gratuïta (donacions)	Basada en Debian Pel suport: 320 US$ per servidor
Funcionalitats suportades	Sistema operatiu base per servidor. Optimitzat per sistemes multi-nucli Gestió de recursos optimitzada Seguretat integral Tecnologies avançades d'emmagatzematge en memòria cau que li permeten escalar segons les seves necessitats sense afegir complexitat. Virtualització integrada Redundància amb alta disponibilitat	Mateixes característiques que RHEL, només que no inclou suport	Sistema operatiu base per servidor No està certificat en optimització en sistemes multi-nucli. No està certificat en Gestió de recursos optimitzada No està certificat en Seguretat integral La gestió de memòria la fa l'usuari, no hi ha eines avançades per a la gestió de memòria Virtualització integrada Redundància amb alta disponibilitat	Sistema operatiu base per servidor No està certificat en optimització en sistemes multi-nucli Gestió de recursos optimitzada Seguretat integral La gestió de memòria la fa l'usuari, no hi ha eines avançades per a la gestió de memòria Virtualització integrada Redundància amb alta disponibilitat

Taula 3. Comparativa entre diferents distribucions: dades identificatives i característiques tècniques

Distribució	Principals avantatges	Principals inconvenients
RHEL 	Assegura una solució integrada i adaptada al servidor, permetent les millors prestacions i optimitzant l'ús dels recursos (inclòs sistemes multi-nucli) Adaptada i certificada per sistemes de desenvolupament Molt estable Suport per part dels principals fabricants de maquinari 7 anys de suport (10 amb ELS)	Llicència anual de suport, 349 US$ per servidor Repositoris de programari oficial limitats
CentOS 	Assegura una solució integrada i adaptada al servidor permetent les millors prestacions, optimitzant l'ús dels recursos (inclòs sistemes multi-nucli) Compatible 100 % amb RHEL Adaptada i certificada per sistemes de desenvolupament Molt popular Suport fins a 7 anys	Sense suport tècnic comercial Actualitzacions amb un cert retard respecte RHEL Només suporta de forma oficial x86 i x86_64 Repositoris de programari oficial limitats
Debian 	Molt popular, és el sistema més estimat pels seguidors del programari lliure Moltes solucions i idees en els fòrums Adaptada i certificada per aplicacions i sistemes de desenvolupament Suporta una gran quantitat d'arquitectures (11 en la versió 6) Suport aproximat de 3 anys El seus repositoris oficials mantenen una gran quantitat de paquets	No disposa de suport tècnic oficial No hi ha un suport específic ni garantia per alguns entorns específics L'administrador s'ha de preocupar de gestionar els recursos per aconseguir les millors prestacions
Ubuntu Server 	Assegura una solució integrada i adaptada al servidor, permetent les millors prestacions, optimitzant l'ús dels recursos (però en aquest cas no s'inclouen els sistemes multi-nucli com a RHEL) Té una gran quantitat de paquets en els seus repositoris però només una part són suportats Ofereix 5 anys de suport Adaptada i certificada per aplicacions i sistemes de desenvolupament	Llicència anual de suport, 320 US$ per servidor Actualment només suporta x86 i x86_64 No és necessàriament compatible amb Debian No hi ha un suport específic ni garantia per alguns entorns específics

Taula 4. Comparativa entre diferents distribucions: avantatges i inconvenients

Descartades aquelles que representin un cost addicional pel centre, finalment ens decantem per Debian; ja que es tracta d'una de les distribucions més veteranes, que sempre ha mantingut una política de versions i paquets molt estricta per tal d'assolir un nivell de qualitat alt. Suporta una gran quantitat d'arquitectures, onze en la versió Debian Squeeze. Els seus repositoris oficials mantenen una gran quantitat de paquets i per a cada versió es dóna suport durant aproximadament tres anys.

També disposa d'una sèrie d'eines que faciliten la feina tant als desenvolupadors com als usuaris en general. En la mateixa web trobem una Wiki, en constant actualització, on es dóna solució als problemes més comuns, s'ofereixen guies i altres documents. També podem accedir a l'IRC (Internet Relay Chat), un canal de comunicació en temps real que permet solucionar els problemes ràpidament.

2.5 Maquinari disponible i costos del projecte

Com s'ha indicat en la introducció, el centre disposa d'un nou servidor preparat per ser configurat i posat en marxa. Es tracta d'un ordinador Dell PowerEdge T410 amb processador Intel Xeon, 8 GB de memòria RAM i disposa de controladora RAID i quatre discos de 500 GB. Per cobrir les necessitats de redundància s'ha configurat en RAID 5. En el seu moment va costar uns 2450 euros. La resta d'elements que puguin formar part del nou disseny del sistema, hauran de sortir de la reutilització i reubicació dels antics servidors: el servidor de centre i el servidor de faltes. En total, tenim a la nostra disposició tres servidors.

Degut a la situació econòmica actual, el centre no pot fer front a noves despeses i serà necessari tirar endavant el projecte amb el maquinari abans esmentat. La despesa prevista en nou material és zero.

Al coincidir en la mateixa persona coordinador d'informàtica del centre i alumne de l'assignatura “Pràctiques externes del Màster en Programari Lliure”, el cost en recursos humans previst és zero.

3. Anàlisi del sistema

Tot seguit definim de manera exacta els requisits del projecte amb l'objectiu de facilitar-nos la preparació del seu disseny i la seva arquitectura.

3.1 Requisits exactes del projecte

Requisits legals. Atès que el centre educatiu processarà dades relatives als alumnes, en alguns casos confidencials, ens obliga a complir totes les normatives vigents en protecció de dades i accés a la informació. En el disseny s'haurà de tenir en compte aquesta normativa. També caldrà respectar tots aquells dispositius que no són propietat del centre, en quant a manipulacions o canvis de configuració.

Requisits de llicències. Totes les actuacions es basaran en programari lliure, caldrà conèixer i respectar els termes de les llicències dels programes instal·lats, i tenir present la declinació de responsabilitat per part dels autors de les aplicacions en cas d'error. També s'haurà de vigilar les possibles incompatibilitats entre les llicències de les aplicacions instal·lades.

Requisits d'accés únic a la Intranet. El nou disseny ens ha de permetre que qualsevol usuari pugui accedir a les dades independentment de l'ordinador del centre que faci servir. Haurem d'assegurar que els clients Windows podran accedir i compartir la informació emmagatzemada en el servidor. La manera de fer-ho és configurar un servidor controlador de domini amb la parella OpenLDAP i Samba.

Requisits d'accés web. Caldrà configurar el servidor de faltes perquè únicament accepti connexions segures mitjançant el protocol HTTPS.

Requisits del sistema de seguretat. Per evitar possibles intrusions des de l'exterior s'haurà de tenir un disseny basat en un tallafocs amb una definició clara de zona desmilitaritzada. Per a tasques administratives dels servidors s'utilitzarà el servei de connexió segura SSH.

Requisits d'impressió en xarxa. Mitjançant Samba i CUPS es podrà posar en funcionament un servei d'impressió centralitzat.

Requisits de gestió de les còpies de seguretat. El sistema haurà de disposar d'un servei de còpies de seguretat automatitzat tant del servidor de centre com de la base de dades del servidor de faltes.

Requisits d'accés únic des d'Internet. El servei ha de permetre a alumnes i professors accedir als seus espais personals des d'Internet. El servlet Davenport permet accedir via WebDAV a un recurs compartit de Samba a través d'un contenidor. Com a contenidor del servlet s'utilitzarà el servidor Tomcat, i l'accés al servidor haurà de ser segur.

Requeriments tecnològics, de manteniment i administració. L'administració i manteniment posteriors corren a càrrec del coordinador d'informàtica del centre. Al llarg de la implantació del projecte i durant els períodes de proves està previst fer sessions de formació dirigides als membres de la comissió TIC del centre.

Requeriments de formació. Caldrà preveure sessions de formació dirigides tant al professorat com a l'alumnat que mostrin les noves funcionalitats del sistema. També serà necessari complementar aquestes sessions amb documents explicatius sobre les configuracions a realitzar sobre els equips clients per tal d'accedir a aquests nous serveis.

3.2 Especificació del pla de proves

Accés al servidor des de la Intranet. Qualsevol usuari ha de poder accedir des dels ordinadors del centre, mitjançant nom d'usuari i contrasenya al seu espai personal i espais compartits corresponents. S'haurà de comprovar que l'usuari té accés total al seu espai i comprovar que en tot moment es compleixen les condicions establertes de permisos en accedir als espais compartits.

Accés al servidor des d'Internet. Qualsevol usuari ha de poder accedir des d'Internet , mitjançant nom d'usuari i contrasenya al seu espai personal i espais compartits corresponents. L'accés haurà de ser segur. S'haurà de verificar que l'usuari té accés total al seu espai i comprovar que en tot moment es compleixen les condicions establertes de permisos en accedir als espais compartits.

Accés al servidor de faltes. Qualsevol professor ha de poder accedir al servidor de faltes, tant des de la Intranet com des d'Internet, i un cop validat amb un nom d'usuari i contrasenya, realitzar consultes en el servidor web. L'accés haurà de ser segur.

DNS intern. L'administrador, des de diferents ordinadors del centre, haurà de comprovar el bon funcionament del DNS intern del servidor de faltes.

DNS extern. L'administrador haurà de comprovar, des d'Internet, que el domini del centre es resolt satisfactòriament per el DNS extern del servidor de faltes.

Tallafocs. Caldrà comprovar el bon funcionament del tallafocs. Com a administrador es comprovarà que des de l'exterior es redirigeix el tràfic cap al servidor de faltes situat en la zona desmilitaritzada, només a través dels ports prefixats. També es comprovarà que el tallafocs permet el tràfic entre el servidor de faltes i el servidor de centre. Des de la Intranet s'haurà de verificar que es permet el tràfic cap al servidor de faltes i a Internet.

Accés SSH. L'administrador ha de poder accedir mitjançant connexions segures SSH als servidors. S'hauria de comprovar que l'accés és factible tant des de la Intranet com des d'Internet.

4. Disseny de la solució

Un cop definits els requisits del projecte, iniciem el procés de disseny de la solució seleccionant els serveis i la seva ubicació física en els ordinadors disponibles. També caldrà analitzar com integrem aquests nous elements dins la xarxa del centre.

4.1 Definició de l'arquitectura del sistema

A nivell d'arquitectura de xarxa, la solució proposada (veure Annex A) queda resumida en el diagrama següent (Figura 1):

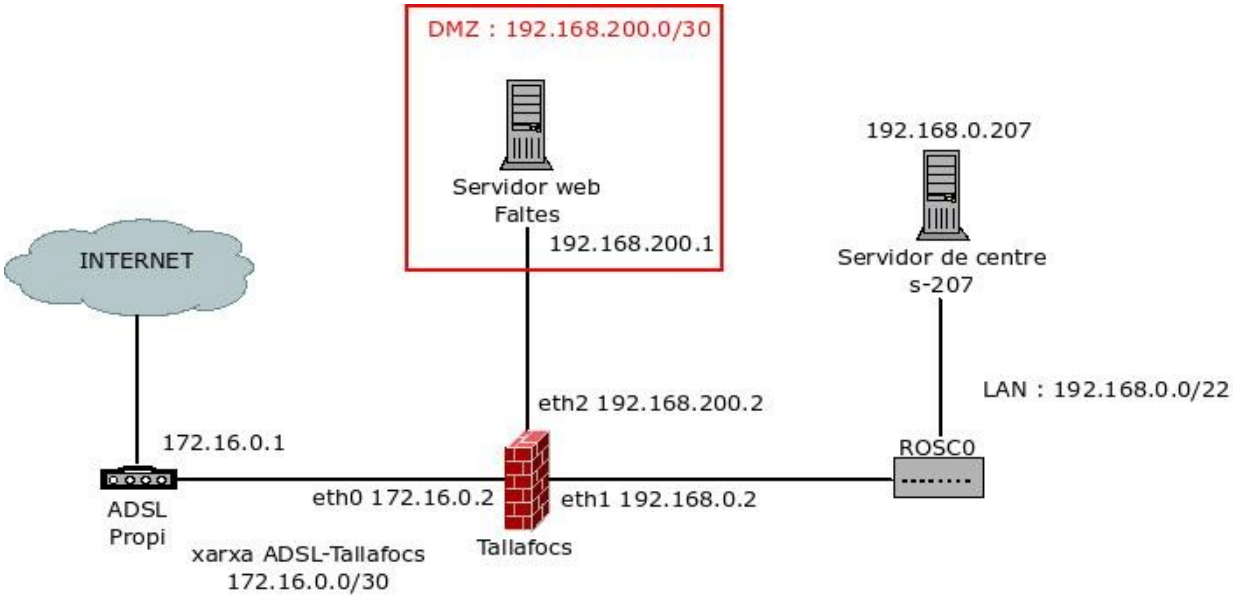

Figura 1. Solució proposada: creació d'una zona desmilitaritzada i incorporació d'un tallafocs

Bàsicament la intervenció contempla:

- El servidor de centre és reemplaçat per un de nou. Ubicat en la xarxa interna 192.168.0.0/22, té assignada una IP fixa 192.168.0.207. La ruta per defecte de la xarxa interna és 192.168.0.2.

- Creació d'una zona desmilitaritzada (DMZ), on ubicarem el servidor de faltes. L'antic servidor de centre farà aquestes funcions. En la zona

desmilitaritzada tenim una xarxa 192.168.200.0/30. Al servidor de faltes se li assigna una IP fixa 192.168.200.1 i com a porta d'enllaç 192.168.200.2.

- S'afegeix un nou element tallafocs a la xarxa, per protegir la xarxa interna i encaminar les possibles consultes que es facin des de l'exterior. S'aprofitarà l'antic servidor de faltes per fer aquestes funcions. Amb tres targetes de xarxa, la ruta per defecte del tallafocs és 172.16.0.1

- S'assigna una IP interna 172.16.0.1 al router.

4.2 Comportament dels nous elements

En la taula 5 es resumeixen els serveis i programari que està previst instal·lar en els nous elements, així com els sistema operatiu que utilitzaran.

Element	Nom	Serveis que ofereix	Programari utilitzat
Servidor de centre	s-207	▪ Controlador de domini ▪ Connexió segura amb SSH ▪ Còpies de seguretat en xarxa	▪ Sistema operatiu: Debian 6 Squeeze ▪ OpenLDAP i Samba ▪ OpenSSH · Bacula
Servidor de faltes	assistpda	▪ Servidor web ▪ Servidor d'aplicacions ▪ Servidor de noms DNS ▪ Connexió segura amb SSH	▪ Sistema operatiu: Debian 6 Squeeze ▪ Apache, MySQL i PHP ▪ Tomcat ▪ Servlet Davenport ▪ Bind ▪ OpenSSH
Tallafocs	fw	▪ Bloquejar l'accés no permès des de l'exterior ▪ Limitar les connexions de la xarxa local amb l'exterior ▪ Connexió segura amb SSH	▪ Sistema operatiu: Debian 6 Squeeze ▪ Iptables ▪ OpenSSH

Taula 5. Resum de serveis i programari que està previst instal·lar-hi

ADSL. S'haurà de configurar perquè les peticions de consultes des de l'exterior s'encaminin mitjançant NAT cap al tallafocs.

4.3 Disseny del domini

Una de les tasques del nou servidor de centre és actuar com a controlador de domini. Analitzem a continuació els requeriments del nou domini:

- **Nom del domini**. El nom del domini és **iesmiquelbosch** i l'extensió **cat**. El nom distingit del domini és **dc=iesmiquelbosch, dc=cat**.

- Unitat organitzativa **Users (ou=Users)**. Aquesta unitat organitzativa conté tots els usuaris individuals del domini.

- Cada usuari del domini s'identifica de manera unívoca mitjançant un identificador d'usuari **(uid=agonzalez)**. El seu nom distingit és, per exemple, **uid=agonzalez, ou=Users, dc=iesmiquelbosch, dc=cat**.

- Unitat organitzativa **Groups (ou=Groups)**. Aquesta unitat organitzativa conté tots els grups d'usuaris.

- Cadascun dels grups d'usuaris s'identifica de manera unívoca amb un nom de grup **(cn=alumnes)**. El seu nom distingit és **cn=alumnes, ou=Groups, dc=iesmiquelbosch, dc=cat**.

- Unitat organitzativa **Computers (ou=Computers)**. Aquesta unitat organitzativa conté el nom de tots els ordinadors que formen part del domini.

- Cada ordinador del domini s'identifica de manera unívoca mitjançant un identificador **(uid=aidi170$)**. El seu nom distingit és **uid=aidi170$, ou=Computers, dc=iesmiquelbosch, dc=cat**.

La figura 2 representa en forma d'arbre, els objectes del domini descrits anteriorment.

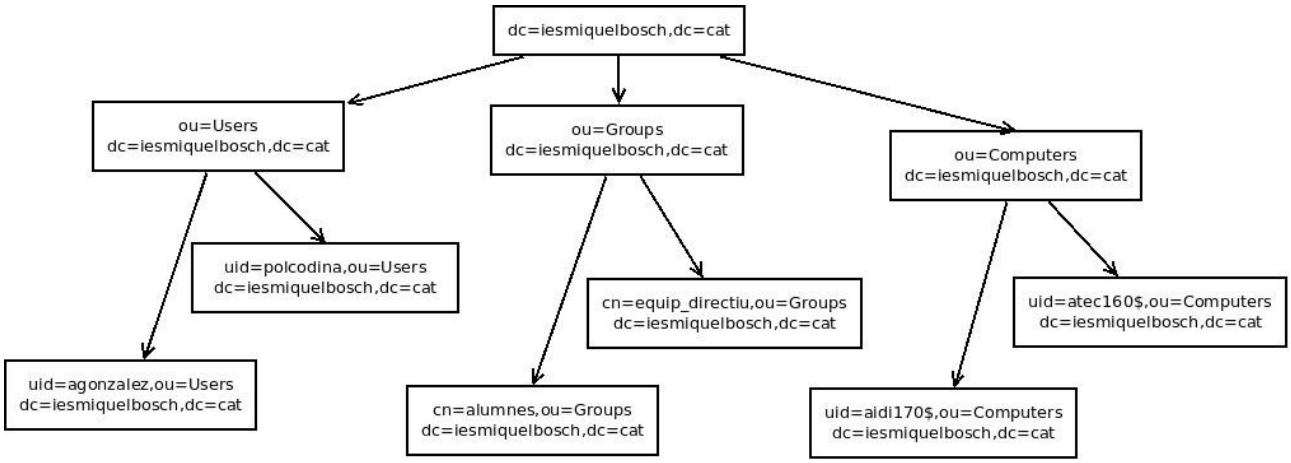

Figura 2. Esquema del domini iesmiquelbosch.cat

Com es pot apreciar, el disseny del directori LDAP és totalment horitzontal.

4.3.1 Grups primaris i grups secundaris

Està previst crear quatre grups primaris. Qualsevol usuari del domini estarà assignat a algun d'aquests grups. La taula següent resumeix qui forma part de cada grup, el nom i l'identificador (GID) de cada grup.

Usuaris que en formen part	Nom del grup	GID
Professors del centre	profes	2000
Alumnes del centre	alumnes	3000
Personal d'administració i serveis	pas	4000
Mares i pares d'alumnes	ampa	5000

Taula 6. Definició de grups primaris

A part, cada professor pot pertànyer a un o més grups secundaris. Es defineixen dotze grups secundaris; el professorat que en forma part, el nom i

l'identificador de cada grup, que queda resumit en la taula següent:

Professors que en formen part	Nom del grup	GID
Professors de l'equip directiu	equip_directiu	2001
Professors del Departament de Matemàtiques	mates	2002
Professors del Departament de Ciències Naturals	experimentals	2003
Professors del Departament de Català	catala	2004
Professors del Departament de Llengües Estrangeres	estrangeres	2005
Professors del Departament de Visual i Plàstica	visual_plastica	2006
Professors del Departament de Castellà	castella	2007
Professors del Departament de Música	musica	2008
Professors del Departament d'Educació Física	educacio_fisica	2009
Professors del Departament de Ciències Socials	socials	2010
Professors del Departament de Tecnologia	tecno	2011
Professors del Departament d'Orientació	orientacio	2012

Taula 7. Definició dels grups secundaris del professorat

Tot alumne pertany a algun dels grups secundaris següents:

Alumnes que en formen part	Nom del grup	GID
Alumnes de 1r ESO	1ESO	3001
Alumnes de 2n ESO	2ESO	3002
Alumnes de 3r ESO	3ESO	3003
Alumnes de 4t ESO	4ESO	3004
Alumnes de 1r Batxillerat	1BAT	3005
Alumnes de 2n Batxillerat	2BAT	3006

Taula 8. Definició dels grups secundaris de l'alumnat

Dos són els grups secundaris del personal no docent.

Personal no docent que en forma part	Nom del grup	GID
Personal de secretaria	secretaria	4001
Personal de consergeria	consergeria	4002

Taula 9. Definició dels grups secundaris del personal no docent

4.3.2 Espais personals i espais compartits

En aquest apartat detallem la política que serà aplicada als espais personals i espais compartits del domini.

Carpetes personals. Tot usuari donat d'alta en el domini té accés a una carpeta personal. Els professors també tenen accés a les carpetes personals dels alumnes, on poden crear documents, modificar-los o compartir-los amb ells.

Espais compartits alumnes. Cada alumne pot accedir a un espai compartit del seu nivell. L'accés a aquest espai per part de l'alumnat és únicament de lectura. El professorat, per la seva part, hi té accés total. Es defineixen sis espais compartits pels alumnes, un per cada nivell, quatre per l'ESO i dos per al batxillerat. La taula 10 resumeix el nom de cada espai compartit i el grup d'alumnes que hi tenen accés.

Grup d'alumnes que tenen accés	Nom de l'espai compartit
Alumnes de 1r ESO	espai_comu_1ESO
Alumnes de 2n ESO	espai_comu_2ESO
Alumnes de 3r ESO	espai_comu_3ESO
Alumnes de 4t ESO	espai_comu_4ESO
Alumnes de 1r Batxillerat	espai_comu_1BAT
Alumnes de 2n Batxillerat	espai_comu_2BAT

Taula 10. Definició dels espais compartits de l'alumnat

Espais compartits professorat. Tots els professors tenen accés a un espai comú on poden intercanviar documents. Cada departament contempla un espai comú on únicament els membres d'aquell departament tenen accés total. L'equip directiu del centre també té el seu propi espai comú, únicament els membres de l'equip directiu hi tindran accés.

Grup de professors que tenen accés	Nom de l'espai compartit
Tot el professorat	espai_comu_profes
Membres de l'equip directiu	espai_comu_equip_directiu
Professors del Departament de Matemàtiques	espai_comu_mates
Professors del Departament de Ciències Naturals	espai_comu_experimentals
Professors del Departament de Català	espai_comu_catala
Professors del Departament de Llengües Estrangeres	espai_comu_estrangeres
Professors del Departament de Visual i Plàstica	espai_comu_visual_plastica

Grup de professors que tenen accés	Nom de l'espai compartit
Professors del Departament de Castellà	espai_comu_castella
Professors del Departament de Música	espai_comu_musica
Professors del Departament d'Educació Física	espai_comu_educacio_fisica
Professors del Departament de Ciències Socials	espai_comu_socials
Professors del Departament de Tecnologia	espai_comu_tecno
Professors del Departament d'Orientació	espai_comu_orientacio

Taula 11. Definició dels espais compartits del professorat

Les figures 3 i 4 resumeixen l'estructura de directoris de les carpetes personals i carpetes compartides. Les carpetes personals s'han representat en color blau, les carpetes compartides en groc.

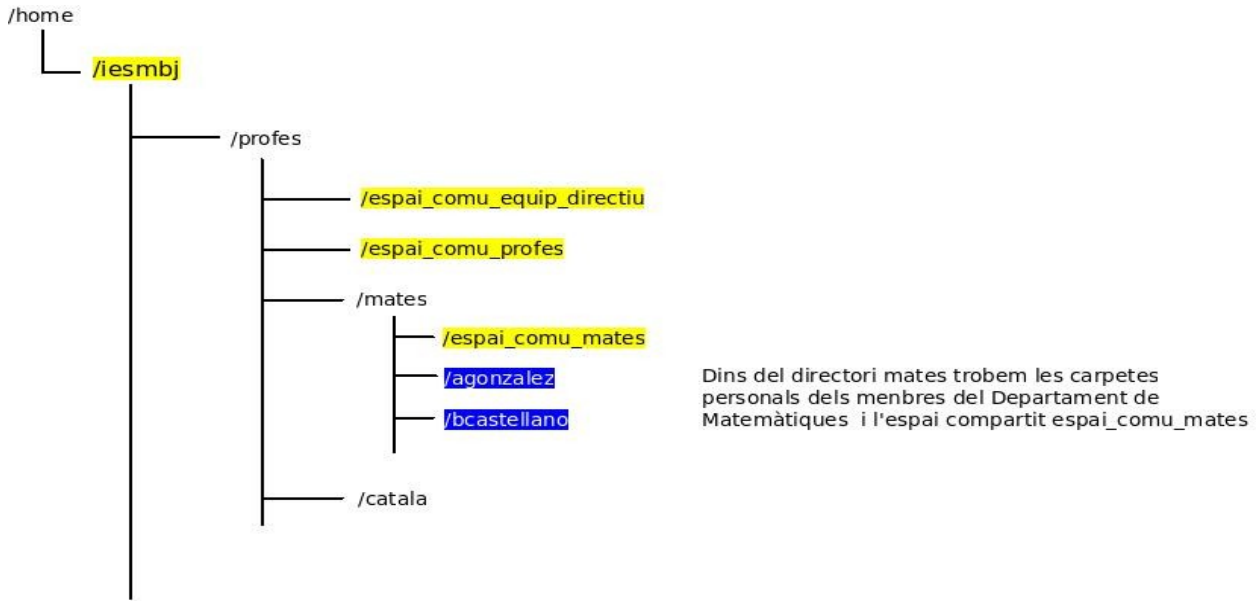

Figura 3. Estructura dels directoris de les carpetes personals i carpetes compartides del professorat

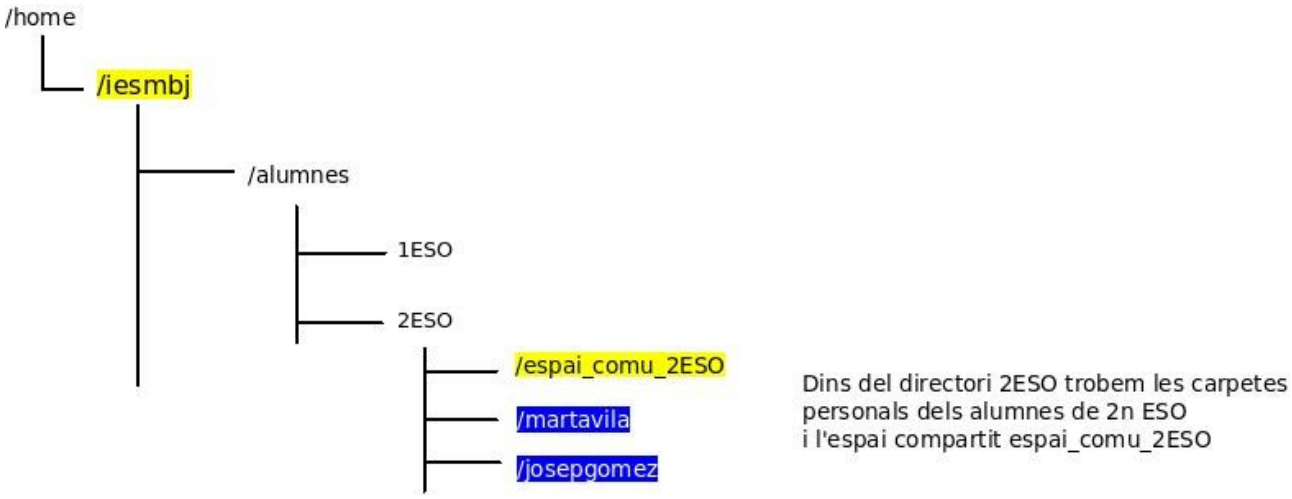

Figura 4. Estructura dels directoris de les carpetes personals i carpetes compartides de l'alumnat

5. Implementació de la solució

L'objectiu principal d'aquest apartat és la construcció ordenada del sistema a partir del disseny abans analitzat. El fet que certs elements estiguin en producció ens obliga a seguir un ordre en la intervenció. Aquest podria ser el següent:

- Servidor de centre: instal·lació i configuració dels nous serveis.
- Integració del nou servidor de centre en el sistema.
- Servidor de faltes: instal·lació i configuració dels nous serveis.
- Configuració del tallafocs.
- Configuració de l'ADSL i integració del servidor de faltes i tallafocs.

5.1 Servidor de centre

La intervenció sobre el servidor de centre ha estat la següent:

- Instal·lació del sistema operatiu Debian 6 Squeeze. ([6])
- Modificació de la configuració inicial del servei SSH. ([2] Capítol 4 – SSH; [3] Capítol 7 – Administración remota segura con SSH; [6])
- Configuració del servidor de centre com un controlador de domini (PDC) amb OpenLDAP i Samba. ([3] Capítol 12 – Directorio de red centralizado con OpenLDAP; [1]; [6])
- Instal·lació i configuració del servei de còpies de seguretat. ([9])

Tot seguit s'expliquen, en diferents seccions, els passos duts a terme per a la seva configuració.

5.1.1 Servei SSH

SSH ha estat l'únic servei seleccionat en el moment d'instal·lar el sistema

operatiu. Per raons de seguretat s'han modificat alguns paràmetres de l'arxiu de configuració **/etc/ssh/sshd-config**. Aquests canvis han estat:

- Modificar el port on escolta el dimoni sshd.
- No permetre l'accés de l'usuari root al servidor via SSH.
- Anul·lar l'accés tradicional al servidor mitjançant nom d'usuari i contrasenya.
- Indicar al servidor on es troba la clau pública de l'usuari, per tal d'utilitzar-la per a l'autenticació.

La resta de paràmetres s'han deixat com estaven en la configuració per defecte.

```
root@s-207:~# nano /etc/ssh/sshd_config
```

```
Port 50207
PermitRootLogin no
PasswordAuthentication no
AuthorizedKeysFile      %h/.ssh/authorized_keys
```

S'ha creat un nou usuari específic per a les connexions remotes.

```
root@s-207:~# useradd -m -s /bin/bash manaia
root@s-207:~# passwd manaia
Introduïu la nova contrasenya d'UNIX:
Torneu a escriure la nova contrasenya d'UNIX:
passwd: s'ha actualitzat la contrasenya satisfactòriament
```

Des de l'ordinador de l'administrador, utilitzem l'eina **ssh-keygen** per a la creació de la clau púbica i la clau privada.

```
arnaldo@ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/arnaldo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/arnaldo/.ssh/id_rsa.
Your public key has been saved in /home/arnaldo/.ssh/id_rsa.pub.
The key fingerprint is:
a9:b7:8c:19:61:5d:4d:f4:dd:7d:19:bc:18:92:4c:7f arnaldo@ubuntu
The key's randomart image is:
+--[ RSA 2048]----+
```

```
|           oo+ .. |
|            *.o o=|
|           . o.+E*|
|        . o   ....|
|       o S        |
|      . o         |
|       o .        |
|        * .       |
|       o o        |
+------------------+
```

La utilitat **ssh-copy-id** insereix directament la clau pública en l'arxiu **authorized_keys** de l'usuari que utilitzarem per fer les connexions SSH.

```
arnaldo@ubuntu:~$ ssh-copy-id manaia@s-207.iesmiquelbosch.cat
```

Per últim, reiniciem el servei.

```
root@s-207:~# /etc/init.d/ssh restart
Restarting OpenBSD Secure Shell server: sshd.
```

5.1.2 Servei LDAP

En aquesta secció instal·larem i configurarem un servidor LDAP amb la implementació lliure OpenLDAP, junt amb les eines d'administració i client.

Instal·lació del servidor LDAP

Per realitzar la instal·lació executarem la comanda:

```
root@s-207:~# apt-get install slapd ldap-utils
```

Quan s'instal·la el paquet slapd, l'assistent de configuració ens demana la contrasenya de l'administrador del directori LDAP (Figura 5).

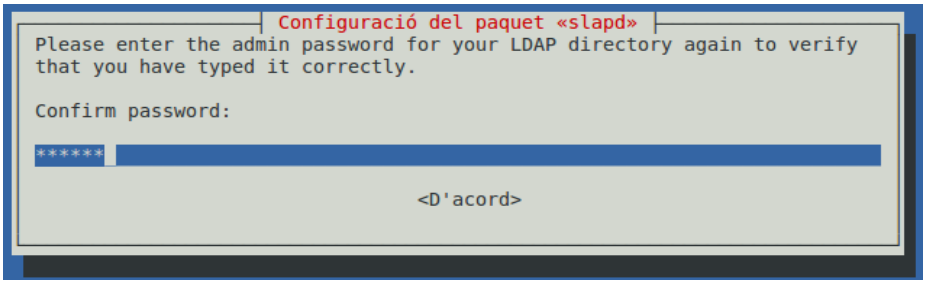

Figura 5. L'assistent de configuració demana la contrasenya de l'administrador

L'assistent postinstal·lació ens configurarà automàticament un directori, utilitzant com a nom distingit d'aquest el nom de domini que tingui configurat el servidor, en el nostre cas **dc=iesmiquelbosch,dc=cat**.

Un cop feta la instal·lació, podem comprovar l'estructura bàsica del directori. Farem una recerca autenticant-nos com usuari administrador i utilitzant com a base **dc=iesmiquelbosc, dc=cat**.

```
root@s-207:~# ldapsearch -x -D "cn=admin,dc=iesmiquelbosch,dc=cat" -b
"dc=iesmiquelbosch,dc=cat" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=iesmiquelbosch,dc=cat> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# iesmiquelbosch.cat
dn: dc=iesmiquelbosch,dc=cat
objectClass: top
objectClass: dcObject
objectClass: organization
o: iesmiquelbosch.cat
dc: iesmiquelbosch

# admin, iesmiquelbosch.cat
dn: cn=admin,dc=iesmiquelbosch,dc=cat
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9NE9mcUZsQ3F3K2JFbHJ4M3N3V3J1VW0zSU1VQ0VJcEw=

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Configuració de les llistes de control d'accés (ACL)

Editem l'arxiu **oclAcces.ldif** per tal de modificar alguns dels paràmetres de les llistes de control d'accés que vénen per defecte.

```
dn: olcDatabase={1}hdb,cn=config
```

```
changetype: modify
replace: olcAccess
olcAccess: to attrs=userPassword by dn="cn=admin,dc=iesmiquelbosch,dc=cat" 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=iesmiquelbosch,dc=cat" write by * read
```

I afegim les modificacions:

```
root@s-207:~# ldapmodify -Y EXTERNAL -H ldapi:/// -f oclAccess.ldif
```

Agregant l'esquema Samba

Els esquemes que vénen per defecte en la configuració de l'slapd són els necessaris per poder treballar amb comptes Linux. Aquests esquemes no permeten emmagatzemar atributs pels comptes d'usuaris i dominis Samba. OpenLDAP permet la càrrega d'esquemes externs per poder guardar aquest tipus d'informació.

Haurem d'instal·lar el paquet samba-doc, el qual conté l'arxiu **samba.shema**, que defineix els atributs Samba.

```
root@s-207:~# apt-get install samba-doc
```

Descomprimim el fitxer d'esquema i el copiem al directori **/etc/ldap/schema/**.

```
root@s-207:~# zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz >
/etc/ldap/schema/samba.schema
```

El següent pas serà afegir l'esquema a la branca cn=config del directori LDAP. Editem l'arxiu **schema_convertir.conf** amb el contingut següent:

```
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
```

Per guardar la sortida que generarà aquest fitxer de configuració, creem un directori temporal.

```
root@s-207:~# mkdir ldif_sortida
```

Utilitzem slapcat per convertir els fitxers d'esquema en el format apropiat per LDAP.

```
root@s-207:~# slapcat -f schema_convertir.conf -F ldif_sortida -n0 -s
"cn={12}samba,cn=schema,cn=config" > cn=samba.ldif
```

Editem el fitxer generat i eliminem el **{12}** de les primeres línies i les últimes línies a partir de **structuralObjectClass: olcSchemaConfig** .

L'últim pas és incorporar l'esquema nou al directori LDAP.

```
root@s-207:~# ldapadd -Y EXTERNAL -H ldapi:/// -f cn\=samba.ldif
```

Configuració dels índexs més utilitzats

Per millorar el rendiment del directori és important que els atributs més utilitzats per els clients LDAP, estiguin degudament indexats en la base de dades del directori LDAP. Per a tal fi, creem el fitxer **samba_indexs.ldif**, amb el contingut següent:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
```

```
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

Mitjançant ldapmodify carreguem els nous índexs.

```
root@s-207:~# ldapmodify -Y EXTERNAL -H ldapi:/// -f samba_indexs.ldif
```

Configuració del servidor per fer consultes segures

Si volem que les consultes fetes al servidor LDAP des de qualsevol altre ordinador siguin segures, caldrà configurar-lo perquè les sessions siguin encriptades.

Primer de tot hem de crear un certificat. Utilitzarem la utilitat certtool per crear aquest certificat. Abans instal·larem la llibreria gnutls-bin.

```
root@s-207:~# apt-get install gnutls-bin
```

Ara ja podem crear la clau privada per al certificat d'autoritat.

```
root@s-207:~# certtool --generate-privkey --outfile /etc/ssl/private/ca_clau.pem
```

Editem l'arxiu **/etc/ssl/ca.info** amb la informació per generar el certificat autosignat.

```
cn = INS Miquel Bosch i Jover
ca
cert_signing_key
```

Creem el certificat d'autoritat autosignat:

```
root@s-207:~# certtool --generate-self-signed --load-privkey
/etc/ssl/private/ca_clau.pem --template /etc/ssl/ca.info --outfile
/etc/ssl/certs/ca_cert.pem
```

Seguidament, creem la clau privada per al servidor.

```
root@s-207:~# certtool --generate-privkey --outfile /etc/ssl/private/s-
207_slapd_clau.pem
```

Editem l'arxiu **/etc/ssl/s-207.info** amb la informació per signar el

certificat del servidor amb el certificat d'autoritat.

```
organization = INS Miquel Bosch i Jover
cn = s-207.iesmiquelbosch.cat
tls_www_server
encryption_key
signing_key
```

Finalment, creem el certificat del servidor.

```
root@s-207:~# certtool --generate-certificate --load-privkey /etc/ssl/private/s-207_slapd_clau.pem --load-ca-certificate /etc/ssl/certs/ca_cert.pem --load-ca-privkey /etc/ssl/private/ca_clau.pem --template /etc/ssl/s-207.info --outfile /etc/ssl/certs/s-207_slapd_cert.pem
```

Per tal d'integrar aquests certificats i clau en el directori LDAP, editem l'arxiu **ssl.ldif** amb el contingut següent:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/ca_cert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/s-207_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/s-207_slapd_clau.pem
```

Apliquem els canvis amb l'eina **ldapmodify**.

```
root@s-207:~# ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldif
```

Caldrà afegir els usuaris openldap dins del grup ssl-cert perquè aquests puguin accedir a la clau del servidor. Abans, cal instal·lar el paquet ssl-cert.

```
root@s-207:~# apt-get install ssl-cert
root@s-207:~# adduser openldap ssl-cert
root@s-207:~# chgrp ssl-cert /etc/ssl/private/s-207_slapd_clau.pem
root@s-207:~# chmod g+r /etc/ssl/private/s-207_slapd_clau.pem
```

Per últim, reiniciem el servei.

```
root@s-207:~# /etc/init.d/slapd restart
```

Configuració de la resolució d'identitats

Perquè el sistema pugui realitzar la resolució d'identitats utilitzant com a font d'origen el directori LDAP cal instal·lar el paquet libnss-ldapd.

```
root@s-207:~# apt-get install libnss-ldapd
S'instal·laran els paquets NOUS següents:
  libnss-ldapd libpam-ldapd nscd nslcd
```

Durant la instal·lació ens demana l'adreça i la base de cerca del servidor LDAP, en el nostre cas **`ldap://127.0.0.1/`** i **`dc=iesmiquelbosch,dc=cat`**.

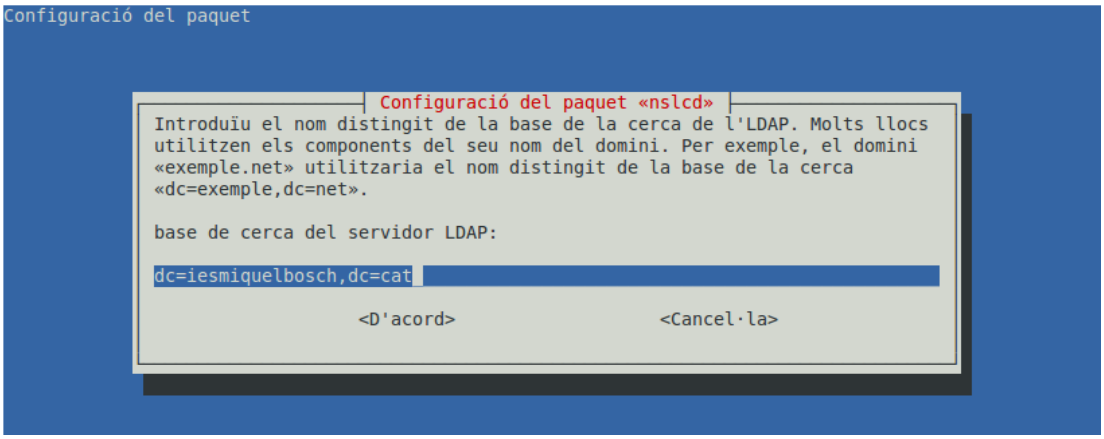

Figura 6. Assistent de configuració del paquet nslcd

També cal indicar-li al servidor que utilitzi el directori LDAP com a font d'informació sobre els usuaris i els grups. En l'apartat serveis de noms a configurar, seleccionem: passwd, shadow i group.

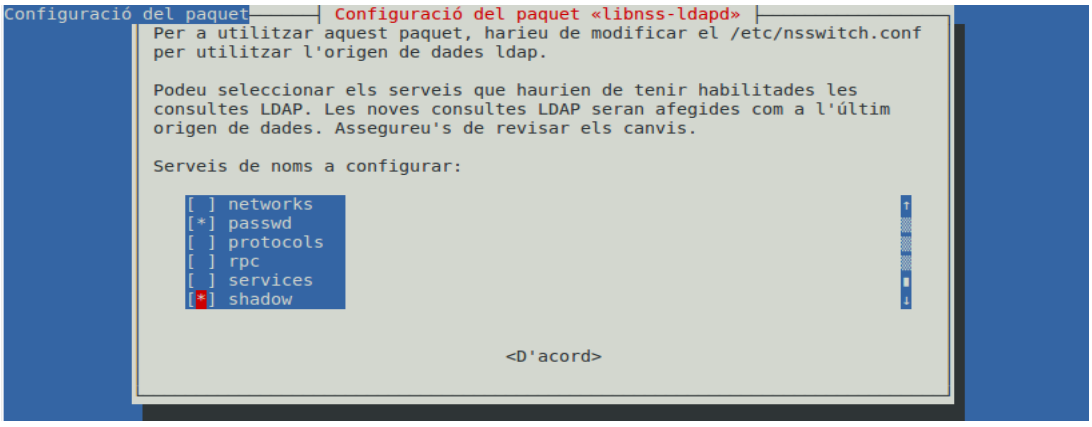

Figura 7. Indiquem al servidor que utilitzi el directori LDAP com a font d'informació

5.1.3 Servei Samba

En aquest apartat configurarem el servidor Samba perquè esdevingui un controlador de domini i utilitzarem les eines smbldap-tools per integrar Samba amb LDAP.

Instal·lació del servidor Samba

Per realitzar la instal·lació executarem la comanda:

```
root@s-207:~# apt-get install samba smbldap-tools
```

Guardem l'arxiu original de configuració i el canviem per el que ve d'exemple en el paquet smbldap-tools.

```
root@s-207:~# mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
root@s-207:~# cp /usr/share/doc/smbldap-tools/examples/smb.conf
/etc/samba/smb.conf
```

Configuració de Samba

Editem l'arxiu **smb.comf** i fem les primeres adaptacions al nostre entorn. S'especifiquen aquí únicament les línies modificades respecte a l'original.

- **Secció [global]**

Indiquem el nom del domini i el nom NetBIOS del servidor Samba.

```
workgroup = IESMIQUELBOSCH
netbios name = s-207
```

Indiquem a Samba que intenti actualitzar les contrasenyes amb el directori LDAP.

```
ldap passwd sync = yes
```

Establim la codificació de caràcters compatible tant amb Unix com amb DOS.

```
Dos charset = CP932
Unix charset = UTF-8
```

L'script d'inici de sessió té el format nom d'usuari punt bat.

```
logon script = %U.bat
```

Unitat en la qual es muntarà la carpeta personal de l'usuari.

```
logon drive = P:
```

Li indiquem qui és l'administrador del domini, descomentem i afegim un parell d'scripts que s'utilitzaran per l'administració dels grups del domini.

```
ldap admin dn = cn=admin,dc=iesmiquelbosch,dc=cat
ldap suffix = dc=iesmiquelbosch,dc=cat
delete group script = /usr/sbin/smbldap-groupdel "%g"
set primary group script = /usr/sbin/smbldap-usermod -g ‘%g’ ‘%u’
```

No és necessari el xifrat, Samba i LDAP estan corrent en la mateixa màquina.

```
ldap ssl = no
```

- **Recurs compartit [homes]**

Per tal que els usuaris puguin accedir a les carpetes personals, s'ha creat la secció [homes].

```
[homes]
      comment = Directoris Home
      browseable = no
      read only = no
```

Creem el directori on estaran situats els scripts d'inici de sessió.

```
root@s-207:~# mkdir -p /srv/samba/netlogon
```

- **Recurs compartit [netlogon]**

Compartim el directori d'inici de sessió dels clients Windows.

```
[netlogon]
        path = /srv/samba/netlogon
        browseable = No
        read only = yes
```

Finalment comentem el recurs compartit [profiles], ja que no farem ús dels perfils mòbils. També es comenta el recurs compartit d'exemple [public].

Reiniciem el servei perquè les modificacions tinguin efecte.

```
root@s-207:~# /etc/init.d/samba restart
Stopping Samba daemons: nmbd smbd.
Starting Samba daemons: nmbd smbd.
```

Configuració del paquet smbldap-tools

En aquests moments podem configurar el paquet smbldap-tools perquè sigui coherent amb el nostre entorn. El paquet incorpora un script que ens facilita la feina. Descomprimim i iniciem l'script.

```
root@s-207:~# gzip -d /usr/share/doc/smbldap-tools/configure.pl.gz
root@s-207:~# perl /usr/share/doc/smbldap-tools/configure.pl
```

S'indiquen en negreta alguns dels paràmetres més rellevants.

```
root@s-207:/srv/samba# perl /usr/share/doc/smbldap-tools/configure.pl

Let's start configuring the smbldap-tools scripts ...

. workgroup name: name of the domain Samba act as a PDC
  workgroup name [IESMIQUELBOSCH] >
. netbios name: netbios name of the samba controler
  netbios name [s-207] >
. logon drive: local path to which the home directory will be connected (for NT
Workstations). Ex: 'H:'
  logon drive [P:] >
. logon home: home directory location (for Win95/98 or NT Workstation).
  (use %U as username) Ex:'\\s-207\%U'
  logon home (press the "." character if you don't want homeDirectory) [\\s-
207\%U] >
. logon path: directory where roaming profiles are stored. Ex:'\\s-207\profiles\
```

```
%U'
  logon path (press the "." character if you don't want roaming profile) [\\s-
207\profiles\%U] > .
. home directory prefix (use %U as username) [/home/%U] >
. default users' homeDirectory mode [700] >
. default user netlogon script (use %U as username) [%U.bat] >
  default password validation time (time in days) [45] > 99999
. ldap suffix [dc=iesmiquelbosch,dc=cat] >
. ldap group suffix [ou=Groups] >
. ldap user suffix [ou=Users] >
. ldap machine suffix [ou=Computers] >
. Idmap suffix [ou=Idmap] >
. sambaUnixIdPooldn: object where you want to store the next uidNumber
  and gidNumber available for new users and groups
  sambaUnixIdPooldn object (relative to ${suffix})
[sambaDomainName=IESMIQUELBOSCH] >
. ldap master server: IP adress or DNS name of the master (writable) ldap server
  ldap master server [127.0.0.1] >
. ldap master port [389] >
. ldap master bind dn [cn=admin,dc=iesmiquelbosch,dc=cat] >
  ldap master bind password [] >
. ldap slave server: IP adress or DNS name of the slave ldap server: can also be
the master one
  ldap slave server [127.0.0.1] >
. ldap slave port [389] >
. ldap slave bind dn [cn=admin,dc=iesmiquelbosch,dc=cat] >
. ldap slave bind password [] >
. ldap tls support (1/0) [0] >
. SID for domain IESMIQUELBOSCH: SID of the domain (can be obtained with 'net
getlocalsid s-207')
  SID for domain IESMIQUELBOSCH [S-1-5-21-4292635378-147005420-2892692318] >
. unix password encryption: encryption used for unix passwords
  unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA) [SSHA] >
. default user gidNumber [513] >
. default computer gidNumber [515] >
. default login shell [/bin/bash] >
. default skeleton directory [/etc/skel] >
. default domain name to append to mail adress [] >
-==========-==========-==========-==========-==========-==========-==========
Use of uninitialized value $# in concatenation (.) or string at
/usr/share/doc/smbldap-tools/configure.pl line 314, <STDIN> line 34.
backup old configuration files:
  /etc/smbldap-tools/smbldap.conf->/etc/smbldap-tools/smbldap.conf.old
  /etc/smbldap-tools/smbldap_bind.conf->/etc/smbldap-tools/smbldap_bind.conf.old
writing new configuration file:
  /etc/smbldap-tools/smbldap.conf done.
  /etc/smbldap-tools/smbldap_bind.conf done.
```

Omplint el directori LDAP amb smbldap-populate

L'script smbldap-populate ens afegeix els usuaris i grups, convertint l'estructura del directori LDAP en la d'un controlador de domini.

```
root@s-207:~# smbldap-populate
Populating LDAP directory for domain IESMIQUELBOSCH (S-1-5-21-4292635378-
147005420-2892692318)
(using builtin directory structure)
```

```
entry dc=iesmiquelbosch,dc=cat already exist.
adding new entry: ou=Users,dc=iesmiquelbosch,dc=cat
adding new entry: ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: ou=Computers,dc=iesmiquelbosch,dc=cat
adding new entry: ou=Idmap,dc=iesmiquelbosch,dc=cat
adding new entry: uid=root,ou=Users,dc=iesmiquelbosch,dc=cat
adding new entry: uid=nobody,ou=Users,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Domain Admins,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Domain Users,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Domain Guests,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Domain Computers,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Administrators,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Account Operators,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Print Operators,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Backup Operators,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: cn=Replicators,ou=Groups,dc=iesmiquelbosch,dc=cat
adding new entry: sambaDomainName=IESMIQUELBOSCH,dc=iesmiquelbosch,dc=cat

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
```

Perquè Samba pugui agregar o modificar els comptes del directori LDAP és necessari que conegui la contrasenya de l'administrador del directori. Per especificar la contrasenya de l'administrador utilitzem la comanda:

```
root@s-207:~# smbpasswd -w ********
Setting stored password for "cn=admin,dc=iesmiquelbosch,dc=cat" in secrets.tdb
```

El compte root creat en el directori LDAP s'utilitzarà com a usuari root local i com a administrador del domini. Cal indicar-li la localització del directori personal i establir la shell.

```
root@s-207:~# smbldap-usermod -d /root -s /bin/bash root
```

5.1.4 Donant forma al domini iesmiquelbosch.cat

Els elements bàsics del domini ja els tenim creats. A partir d'ara caldrà crear els grups i les estructures de directoris i recursos compartits.

Creació dels grups primaris i grups secundaris

Basant-nos en el disseny previ definim els grups primaris i grups secundaris del domini. Per fer-ho utilitzem el manament **smbldap-groupadd**

```
root@s-207:~# smbldap-groupadd -a profes
```

Estructura de directoris i recursos compartits

Ara és el moment d'establir l'estructura de directoris que ens servirà per definir la ubicació de les carpetes personals i dels recursos compartits del domini.

Creem els directoris **profes**, **alumnes**, **pas** i **ampa**, tots ells pengen del directori arrel **iesmbj**. A la figura 8 veiem l'estructura. En color groc s'identifiquen els directoris que seran accessibles com a un recurs compartit des de Samba. Utilitzem el manament següent per crear-los.

```
root@s-207:~# mkdir -p /home/iesmbj/{profes,alumnes,pas,ampa}
```

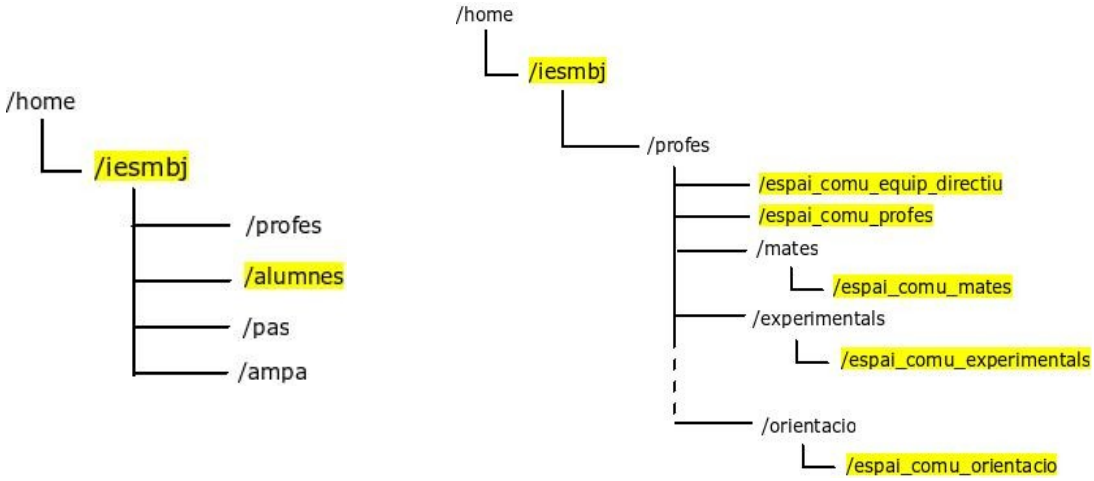

Figura 8. Estructura de directoris i espais compartits

El directori **profes** conté els recursos compartits **espai_comu_profes** i **espai_comu_equip_directiu** i un directori per a cada departament. Els creem amb la comanda següent:

```
root@s-207:~# mkdir /home/iesmbj/profes/
{espai_comu_profes,espai_comu_equip_directiu,mates,experimentals,catala,estrange
res,visual_plastica,castella,musica,educacio_fisica,socials,tecno,orientacio}
```

En el directori de cada departament trobem l'espai comú del departament.

```
root@s-207:~# mkdir /home/iesmbj/profes/mates/espai_comu_mates
root@s-207:~# mkdir /home/iesmbj/profes/experimentals/espai_comu_experimentals
```

```
....
root@s-207:~# mkdir /home/iesmbj/profes/tecno/espai_comu_tecno
root@s-207:~# mkdir /home/iesmbj/profes/orientacio/espai_comu_orientacio
```

El directori alumnes conté una carpeta per a cada nivell. Dins de cada una d'aquestes carpetes s'ubica l'espai compartit del nivell corresponent (Figura 9).

```
root@s-207:~# mkdir /home/iesmbj/alumnes/{1ESO,2ESO,3ESO,4ESO,1BAT,2BAT}
root@s-207:~# mkdir /home/iesmbj/alumnes/1ESO/espai_comu_1ESO
....
root@s-207:~# mkdir /home/iesmbj/alumnes/2BAT/espai_comu_2BAT
```

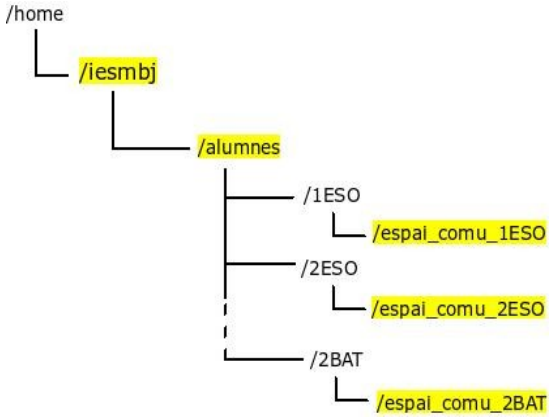

Figura 9. Estructura de directoris i espais compartits dels alumnes

El directori **pas** conté els directoris **secretaria** i **consergeria**. Dins de cada un d'aquests trobem els espais compartits del personal de secretaria i consergeria respectivament (Figura 10).

```
root@s-207:~# mkdir /home/iesmbj/pas/{secretaria,consergeria}
root@s-207:~# mkdir /home/iesmbj/pas/secretaria/espai_comu_secretaria
root@s-207:~# mkdir /home/iesmbj/pas/consergeria/espai_comu_consergeria
```

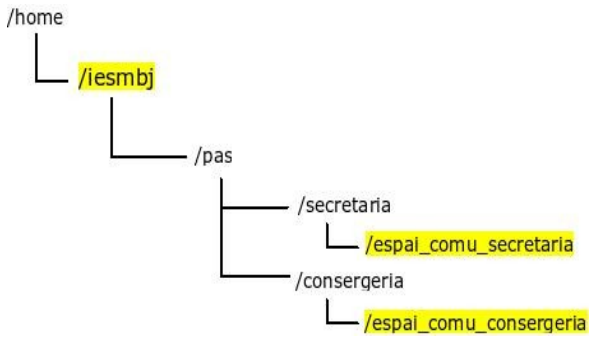

Figura 10. Espais compartits del personal no docent

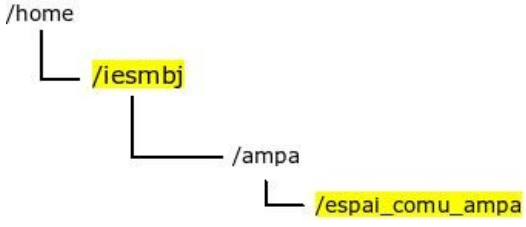

Figura 11. Espai compartit de l'AMPA

L'espai compartit dels pares es troba dins el directori **ampa** (Figura 11).

```
root@s-207:~# mkdir /home/iesmbj/ampa/espai_comu_ampa
```

Utilitzarem llistes de control d'accés (ACL) per definir els grups d'usuaris que tenen accés a un determinat recurs compartit. Primer verifiquem que el kernel tingui suport per treballar amb ACL.

```
root@s-207:~# grep POSIX_ACL /boot/config-`uname -r`
CONFIG_EXT2_FS_POSIX_ACL=y
CONFIG_EXT3_FS_POSIX_ACL=y
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_REISERFS_FS_POSIX_ACL=y
CONFIG_JFS_POSIX_ACL=y
CONFIG_FS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
CONFIG_OCFS2_FS_POSIX_ACL=y
CONFIG_BTRFS_FS_POSIX_ACL=y
CONFIG_TMPFS_POSIX_ACL=y
CONFIG_JFFS2_FS_POSIX_ACL=y
```

Un cop comprovat, instal·lem el paquet acl.

```
root@s-207:~# apt-get install acl
```

Per poder fer ús de les ACL hem de muntar el suport d'ACL per a la partició que conté les carpetes, en el nostre cas la partició **/home**. Editem l'arxiu **/etc/fstab** i afegim **acl** a les opcions de muntatge de la partició.

```
UUID=5cce8078-8367-4be4-a615-de1a79268594 /home   ext3    acl,defaults   0    2
```

Reiniciem el sistema i apliquem les ACL als diferents recursos compartits. Els administradors del domini han de tenir accés total a tots els recursos compartits.

```
root@s-207:~# setfacl -R -m g:512:rwx /home/iesmbj
root@s-207:~# setfacl -d -R -m g:512:rwx /home/iesmbj
```

A continuació es detallen els drets d'accés específics per a cadascun dels recursos compartits.

[iesmbj] Únicament tenen accés els administradors del domini.

```
root@s-207:~# setfacl -m o::--x /home/iesmbj
root@s-207:~# setfacl -d -m o::--- /home/iesmbj
```

[alumnes] Els professors tenen accés, però no poden crear o modificar l'estructura de directoris.

```
root@s-207:~# setfacl -R -m g:profes:r-x,o::--x /home/iesmbj/alumnes
root@s-207:~# setfacl -d -R -m g:profes:r-x,o::--x /home/iesmbj/alumnes
```

[espai_comu_equip_directiu] Els membres de l'equip directiu tenen accés total.

```
root@s-207:~# setfacl -m g:equip_directiu:rwx,o::---
/home/iesmbj/profes/espai_comu_equip_directiu
root@s-207:~# setfacl -d -m g:equip_directiu:rwx,o::---
/home/iesmbj/profes/espai_comu_equip_directiu
```

[espai_comu_profes] Accés total per a tot el professorat.

```
root@s-207:~# setfacl -m g:profes:rwx,o::---
/home/iesmbj/profes/espai_comu_profes
root@s-207:~# setfacl -d -m g:profes:rwx,o::---
/home/iesmbj/profes/espai_comu_profes
```

Per a cada un dels departaments, només els membres del departament tenen accés total a l'espai comú.

[espai_comu_mates] Només els membres del grup mates poden crear documents o modificar-los.

```
root@s-207:~# setfacl -m g:mates:rwx,o::---
/home/iesmbj/profes/mates/espai_comu_mates
root@s-207:~# setfacl -d -m g:mates:rwx,o::---
/home/iesmbj/profes/mates/espai_comu_mates
```

De la mateixa manera es defineixen per a la resta de departaments.

[espai_comu_1ESO] Els professors poden crear carpetes o modificar documents i els alumnes d'1ESO només tenen dret de lectura.

```
root@s-207:~# setfacl -m g:profes:rwx,g:1ESO:r-x,o::---
/home/iesmbj/alumnes/1ESO/espai_comu_1ESO
```

```
root@s-207:~# setfacl -d -m g:profes:rwx,g:1ESO:r-x,o::---
/home/iesmbj/alumnes/1ESO/espai_comu_1ESO
```

De la mateixa manera es defineixen per a la resta de nivells.

[espai_comu_secretaria] El personal de secretaria pot compartir els seus documents.

```
root@s-207:~# setfacl -m g:secretaria:rwx,o::---
/home/iesmbj/pas/secretaria/espai_comu_secretaria
root@s-207:~# setfacl -d -m g:secretaria:rwx,o::---
/home/iesmbj/pas/secretaria/espai_comu_secretaria
```

[espai_comu_consergeria] El personal de consergeria comparteix els seus documents en aquest espai.

```
root@s-207:~# setfacl -m g:secretaria:rwx,o::---
/home/iesmbj/pas/consergeria/espai_comu_consergeria
root@s-207:~# setfacl -d -m g:secretaria:rwx,o::---
/home/iesmbj/pas/consergeria/espai_comu_consergeria
```

[espai_comu_ampa] Els pares i mares d'alumnes tenen un lloc on compartir documents.

```
root@s-207:~# setfacl -m g:ampa:rwx,o::--- /home/iesmbj/ampa/espai_comu_ampa
root@s-207:~# setfacl -d -m g:ampa:rwx,o::--- /home/iesmbj/ampa/espai_comu_ampa
```

També volem que Samba tingui en compte els atributs DOS dels arxius Windows. Verifiquem primer que Samba detecta les biblioteques compatibles amb els atributs estesos.

```
root@s-207:~# smbd -b | grep XATTR
   HAVE_SYS_XATTR_H
   HAVE_ATTR_XATTR_H
   HAVE_FGETXATTR
   HAVE_FLISTXATTR
   HAVE_FREMOVEXATTR
   HAVE_FSETXATTR
   HAVE_GETXATTR
   HAVE_LGETXATTR
   HAVE_LISTXATTR
   HAVE_LLISTXATTR
   HAVE_LREMOVEXATTR
   HAVE_LSETXATTR
   HAVE_REMOVEXATTR
   HAVE_SETXATTR
```

Comprovem que el sistema d'arxius no inclou compatibilitat.

```
root@s-207:~# mount | grep sda6
/dev/sda6 on /home type ext3 (rw,acl)
```

Haurem d'instal·lar el paquet **attr** si volem que el sistema d'arxius sigui compatible amb els atributs estesos.

```
root@s-207:~# apt-get install attr
```

Per fer ús dels atributs estesos, editem l'arxiu **/etc/fstab** i afegim **user_xattr** a les opcions de muntatge de la partició.

```
UUID=5cce8078-8367-4be4-a615-de1a79268594 /home ext3 user_xattr,acl,defaults 0 2
```

Finalment afegim en l'arxiu de configuració de Samba la definició dels recursos compartits amb els paràmetres adients per tenir en compte els atributs i llistes d'accés.

```
[homes]
      comment = Directoris Home
      browseable = no
      read only = no
      store dos attributes = yes
      nt acl support = yes
      map acl inherit = yes
      inherit acls = yes
```

De la mateixa manera es configuren la resta de recursos compartits.

```
[espai_comu_mates]
        path = /home/iesmbj/profes/mates/espai_comu_mates
        browseable = no
        read only = no
        store dos attributes = yes
        nt acl support = yes
        map acl inherit = yes
        inherit acls = yes
```

Carpetes personals

El criteri utilitzat per a definir la ubicació de les carpetes personals ha estat el següent:

- La carpeta personal de cada professor està situada en el directori del

departament.

- Cada alumne té assignada una carpeta personal que es troba ubicada en el directori del seu nivell.
- El personal de secretaria i consergeria disposen d'espais personals localitzats en els directoris secretaria i consergeria respectivament.
- Les carpetes personals dels pares d'alumnes es situen en el directori ampa.

Alta d'usuaris

S'han escrit dos scripts (veure Annex B) per facilitar la tasca de donar d'alta als usuaris. En tots els casos l'script fa ús d'un arxiu de text amb les dades dels nous usuaris.

Per donar d'alta el professorat utilitzem l'script **`profes_nous.sh`**. Bàsicament fa el següent:

- Crea la carpeta personal dins del directori del departament al qual pertany.
- Assigna a l'usuari el grup profes com a grup primari.
- Assigna com a grup secundari, el grup del departament al qual pertany.
- Configura l'usuari sense shell.
- Crea l'script d'inici de sessió i el guarda en el directori **`/srv/samba/netlogon`**.

L'script **`alumnes_nous.sh`** dóna d'alta l'alumnat. Els manaments que executa fan el següent:

- Crea la carpeta personal dins del directori del nivell al qual pertany i li dóna permisos perquè el grup profes pugui compartir documents.

- Assigna a l'alumne el grup alumnes com a grup primari.
- Assigna com a grup secundari, el nivell al qual pertany.
- Configura l'usuari sense shell.
- Crea l'script d'inici de sessió i el guarda en el directori **`/srv/samba/netlogon`**.

5.1.5 Servei de còpies de seguretat

Bacula és un sistema de gestió de còpies de seguretat centralitzat que permet treballar en xarxa. Consta de tres serveis:

- **Director**: component central, gestiona tots els recursos de forma centralitzada i coordina la resta de elements.
- **File Daemon** (servei client): controla l'accés a les dades de les quals volem fer les còpies de seguretat.
- **Storage Daemon** (servei d'emmagatzemament): rep les dades i controla el seu emmagatzemament.

Aquests serveis poden estar centralitzats o distribuïts per la xarxa. En el nostre centre, el servei Director i servei d'emmagatzemament estaran ubicats en el servidor de centre. El servei d'emmagatzemament utilitzarà un disc extern com a suport físic per fer les còpies.

Com a clients actuaran el mateix servidor de centre i el servidor de faltes, per tal d'assegurar còpies de tots els espais personals i espais compartits del servidor de centre i de la base de dades del servidor de faltes. Si es veu necessari no es descarta la possibilitat d'afegir nous clients al sistema.

Director

Tot seguit, indiquem els passos fets per a configurar el servidor de centre com a Director del servei de còpies de seguretat.

Bacula utilitza una base de dades per desar la informació de les operacions realitzades al llarg del temps. El primer que haurem de fer és instal·lar-n'hi una.

```
root@s-207:~# apt-get install mysql-server
```

Durant la instal·lació se'ns demana el nom d'usuari i la contrasenya de l'administrador de la base de dades.

Ara ja podem instal·lar el servei Director. En la instal·lació es crea la base de dades bacula i se'ns demana el nom d'usuari i la contrasenya del seu administrador.

```
root@s-207:~# apt-get install bacula-director-mysql
```

L'arxiu de configuració el trobem a **/etc/bacula/bacula-dir.conf** ,cal modificar-lo per adaptar-lo a les polítiques del nostre sistema de còpies de seguretat. La configuració definitiva es pot veure a l'Annex C.

Servei d'emmagatzemament

Cal instal·lar i configurar el servei encarregat de gestionar la unitat de disc on es guardaran les còpies de seguretat.

```
root@s-207:~# apt-get install bacula-sd-mysql
```

A l'Annex C trobem l'arxiu definitiu de la configuració d'aquest servei **/etc/bacula/bacula-sd.conf**

Servei client

El servidor de centre conté arxius que també volem guardar. Caldrà configurar-lo com a client.

```
root@s-207:~# apt-get install bacula-fd
```

L'arxiu de configuració del servei el trobem a **/etc/bacula/bacula-fd.conf** (veure Annex C).

Bacula consola

Per tal de gestionar les còpies, executar-les, restaurar-les i altres tasques administratives, s'ha instal·lat en el servidor el programa bacula-console.

```
root@s-207:~# apt-get install bacula-console
```

En l'arxiu de configuració indiquem el nom del Director, la seva adreça IP i el port utilitzat i la contrasenya per accedir-hi.

```
root@s-207:~# nano /etc/bacula/bconsole.conf
```

```
#
# Bacula User Agent (or Console) Configuration File
#

Director {
  Name = s-207-dir
  DIRport = 9101
  address = 192.168.0.207
  Password = "x9tkKeZdfDjSgJeD1lTarCa32yP8EsfwjSjsIuO9n/J7"
}
```

5.2 Servidor de faltes

La intervenció sobre el servidor de faltes ha estat la següent:

- Instal·lació del sistema operatiu Debian 6 Squeeze. ([6])
- Modificació de la configuració inicial del servei SSH. ([2] Capítol 4 – SSH; [3] Capítol 7 – Administración remota segura con SSH; [6])
- Posada en marxa del servei DNS. ([2] Capítol 2 – DNS; [6])
- Instal·lació i configuració d'Apache, MySQL i PHP. ([2] Capítol 5 – WEB; [6])
- Instal·lació i configuració de Tomcat i del servlet Davenport. ([6]; [8])
- Posada en marxa del servei client Bacula. ([9])

Tot seguit s'expliquen, en diferents seccions, els passos duts a terme per a la seva configuració.

5.2.1 Servei SSH

S'ha modificat la configuració inicial seguint el mateix criteri que en el servidor de centre. El port utilitzat en les connexions remotes serà el 52001.

5.2.2 Servei DNS

El servei DNS ha de resoldre tant les peticions externes fetes des d'Internet (secció externa), com les fetes des de la Intranet (secció interna).

Després d'instal·lar els paquets bind9, bind9-doc i bind9utils, el pas següent ha estat configurar l'arxiu **/etc/bind/named.conf**. En aquest arxiu s'indica la ruta dels arxius que defineixen les zones que s'utilitzaran en cada secció. Comentem la tercera línia perquè no s'incloguin directament les zones per defecte.

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
#include "/etc/bind/named.conf.default-zones";
include "/etc/bind/named.conf.internal-zones";
include "/etc/bind/named.conf.external-zones";
```

En l'arxiu **/etc/bind/named.conf.internal-zones** definim les zones de la secció interna. Per qüestions de seguretat i d'optimització, en les consultes internes s'acceptaran les peticions recursives i en les consultes externes no.

```
root@assistpda:~# nano /etc/bind/named.conf.internal-zones
```

```
view "internal" {
match-clients {localhost;192.168.0.0/22; };
allow-recursion {localhost;192.168.0.0/22; };

zone "." {
type hint;
file "db.root";
```

```
};

zone "iesmiquelbosch.cat" {
type master;
file "db.iesmiquelbosch.cat.lan";
allow-update { none; };
};


zone "168.192.in-addr.arpa" {
type master;
file "db.168.192";
allow-update { none; };
};

zone "localhost" {
type master;
file "db.local";
};

zone "127.in-addr.arpa" {
type master;
file "db.127";
};

zone "0.in-addr.arpa" {
type master;
file "db.0";
};

zone "255.in-addr.arpa" {
type master;
file "db.255";
};
};
```

En l'arxiu **db.iesmiquelbosch.cat.lan** indiquem la configuració de variables de renovació i la resolució directa dels servidors en les consultes internes.

```
root@assistpda:~# nano /etc/bind/db.iesmiquelbosch.cat.lan
```

```
;
; BIND zone file for iesmiquelbosch.cat
;

$TTL  3D
@     IN    SOA   www.iesmiquelbosch.cat. root.iesmiquelbosch.cat. (
                        2012051103      ; serial
                        8H              ; refresh
                        2H              ; retry
                        4W              ; expire
                        1D )            ; minimum
;
            NS          www
            MX    10    www.iesmiquelbosch.cat.
s-207       A           192.168.0.207
www         A           192.168.200.1
```

La resolució inversa la definim en l'arxiu **/etc/bind/db.168.192**

```
root@assistpda:~# nano /etc/bind/db.168.192
```

```
;
; BIND zone file for 192.168.xxx.xxx
;

$TTL    3D
@       IN      SOA     www.iesmiquelbosch.cat.    root.iesmiquelbosch.cat. (
                        2012051104      ; serial
                        8H              ; refresh
                        2H              ; retry
                        4W              ; expire
                        1D )            ; minimum
;
            NS          www.iesmiquelbosch.cat.
1.200       PTR         www.iesmiquelbosch.cat.
207.0       PTR         s-207.iesmiquelbosch.cat.
```

Les zones de la secció externa les trobem a l'arxiu **/etc/bind/named.conf.external-zones.**

```
root@assistpda:~# nano /etc/bind/named.conf.external-zones
```

```
view "external" {
match-clients {
any;
};
recursion no;

zone "." {
type hint;
file "db.root";
};

zone "iesmiquelbosch.cat" {
type master;
file "db.iesmiquelbosch.cat.wan";
allow-update { none; };
};
};
```

L'arxiu **db.iesmiquelbosch.cat.wan** defineix la resolució directa del servidor en les consultes externes.

```
root@assistpda:~# nano /etc/bind/db.iesmiquelbosch.cat.wan
```

```
;
; BIND zone file for iesmiquelbosch.cat
;

$TTL    3D
@       IN      SOA     dns1.iesmiquelbosch.cat.    root.iesmiquelbosch.cat.(
                        2013190202      ; serial
                        8H              ; refresh
                        2H              ; retry
                        4W              ; expire
                        1D )            ; minimum
;
            NS          dns1.iesmiquelbosch.cat.
            A           212.170.108.94
            MX 10       dns1.iesmiquelbosch.cat.
dns1        A           212.170.108.94
www         CNAME       dns1
```

És necessari canviar la directiva **directory "/var/cache/bind"** de l'arxiu **/etc/bind/named.conf.options**, per indicar-li al servidor on buscar els arxius de les zones creades.

```
root@assistpda:~# nano /etc/bind/named.conf.options
```

```
      options {
      directory "/etc/bind";
      auth-nxdomain no;    # conform to RFC1035
      #listen-on-v6 { any; };
};
```

Només ens queda configurar l'arxiu **/etc/resolv.conf**

```
root@assistpda:~# nano /etc/resolv.conf
```

```
domain iesmiquelbosch.cat
search iesmiquelbosch.cat
nameserver 127.0.0.1
```

Per últim, reiniciar el servei.

```
root@assistpda:~# /etc/init.d/bind9 restart
```

5.2.3 Configuració del servidor web segur

El servidor de faltes utilitza un parell de mòduls adaptats a la maqueta de la intraweb del Departament d'Ensenyament. La versió utilitzada per nosaltres

es basa en PostNuke i cal instal·lar l'Apache, MySQL i PHP per a la seva posada en marxa.

```
root@assistpda:~# apt-get install apache2 libapache2-mod-php5 mysql-server php5-mysql
```

Durant la instal·lació es demana la contrasenya de l'administrador de la base de dades MySQL.

Si volem que les consultes fetes al servidor de faltes des de qualsevol altre ordinador siguin segures, caldrà configurar-lo perquè les sessions estiguin encriptades.

Primer de tot hem de crear un certificat. Utilitzarem la utilitat certtool per crear aquest certificat. Abans instal·larem la llibreria gnutls-bin.

```
root@assistpda:~# apt-get install gnutls-bin
```

Ara ja podem crear la clau privada per al certificat d'autoritat.

```
root@assistpda:~# certtool --generate-privkey --outfile
/etc/ssl/private/ca_clau.pem
```

Editem l'arxiu **/etc/ssl/ca.info** amb la informació per generar el certificat autosignat.

```
cn = INS Miquel Bosch i Jover
ca
cert_signing_key
```

Creem el certificat d'autoritat autosignat:

```
root@assistpda:~# certtool --generate-self-signed --load-privkey
/etc/ssl/private/ca_clau.pem --template /etc/ssl/ca.info --outfile
/etc/ssl/certs/ca_cert.pem
```

Seguidament, creem la clau privada per al servidor.

```
root@assistpda:~# certtool --generate-privkey --outfile
/etc/ssl/private/assistpda_clau.pem
```

Editem l'arxiu **/etc/ssl/assistpda.info** amb la informació per signar el

certificat del servidor amb el certificat d'autoritat.

```
organization = INS Miquel Bosch i Jover
cn = www.iesmiquelbosch.cat
tls_www_server
encryption_key
signing_key
```

Finalment, creem el certificat del servidor.

```
root@assistpda:~# certtool --generate-certificate --load-privkey
/etc/ssl/private/assistpda_clau.pem --load-ca-certificate
/etc/ssl/certs/ca_cert.pem --load-ca-privkey /etc/ssl/private/ca_clau.pem
--template /etc/ssl/assistpda.info --outfile /etc/ssl/certs/assistpda_cert.pem
```

Escrivim la configuració del nou lloc web, de manera que les peticions en el port 80 siguin redirigides cap al port 443.

```
root@assistpda:~# nano /etc/apache2/sites-available/assistpda
```

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName www.iesmiquelbosch.cat
        DocumentRoot /var/www
        RewriteEngine on
        RewriteRule ^/(.*)$ https://www.iesmiquelbosch.cat/$1 [R=permanent]
</VirtualHost>

<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www
        ServerName www.iesmiquelbosch.cat
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

        SSLEngine on
        SSLCertificateFile    /etc/ssl/certs/assistpda_cert.pem
        SSLCertificateKeyFile /etc/ssl/private/assistpda_clau.pem

</VirtualHost>
```

Cal habilitar els mòduls ssl i rewrite per fer ús de la nova configuració.

```
root@assistpda:~# a2enmod ssl
root@assistpda:~# a2enmod rewrite
```

Ara l'únic que ens queda és deshabilitar el lloc web que ve per defecte, habilitar el nou i reiniciar el servidor.

```
root@assistpda:~# a2dissite 000-default
root@assistpda:~# a2ensite assistpda
root@assistpda:~# /etc/init.d/apache2 restart
```

5.2.4 Configuració del servidor d'aplicacions i del servlet Davenport

En aquest apartat configurarem el servidor d'aplicacions Tomcat com a contenidor del servlet Davenport.

Instal·lació de Tomcat

Per començar instal·lem Java 6 i ens baixem la última versió de Tomcat.

```
root@assistpda:~# apt-get install openjdk-6-jre
```

```
root@assistpda:~# wget http://apache.multidist.com/tomcat/tomcat-
7/v7.0.35/bin/apache-tomcat-7.0.35.tar.gz
```

Descomprimim i instal·lem l'aplicació en el directori **/opt/tomcat**. També ens assegurem que els scripts del directori **/opt/tomcat/bin** tenen permís d'execució.

```
root@assistpda:~# tar xvfz apache-tomcat-7.0.35.tar.gz
root@assistpda:~# mv apache-tomcat-7.0.35 /opt/tomcat
root@assistpda:~# chmod +x /opt/tomcat/bin/*.sh
```

Creem el grup i l'usuari tomcat; aquest tindrà com a directori propi, el directori on hem instal·lat Tomcat.

```
root@assistpda:~# groupadd tomcat
root@assistpda:~# useradd -g tomcat -d /opt/tomcat tomcat
root@assistpda:~# usermod -G www-data tomcat
root@assistpda:~# chown tomcat:tomcat /opt/tomcat -R
```

Per tal que el servei s'iniciï de forma automàtica, escriurem l'script següent:

```
root@assistpda:~# nano /etc/init.d/tomcat
```

```
#!/bin/sh

export JAVA_HOME=/usr/lib/jvm/java-6-openjdk
export CATALINA_HOME=/opt/tomcat
export TOMCAT_OWNER=tomcat

start(){
      echo -n "Iniciant Tomcat:  "
      su $TOMCAT_OWNER -c $CATALINA_HOME/bin/startup.sh
}

stop(){
      echo -n "Aturant Tomcat:  "
      su $TOMCAT_OWNER -c $CATALINA_HOME/bin/shutdown.sh
}

case $1 in
start)
      start
      ;;
stop)
      stop
      ;;
restart)
      stop
      start
      ;;
*)
echo "Ús: tomcat {start|stop|restart}"
exit
esac
```

A l'script creat li donem permisos d'execució i amb el manament **update-rc.d** creem de forma automàtica els enllaços necessaris per tal d'iniciar/aturar el nou servei.

```
root@assistpda:~# chmod +x /etc/init.d/tomcat
```

```
root@assistpda:~# update-rc.d tomcat defaults
```

Per acabar, definim l'administrador del servidor d'aplicacions.

```
root@assistpda:~# nano /opt/tomcat/conf/tomcat-users.xml
```

```
 <role rolename="manager"/>
  <role rolename="manager-gui"/>
  <role rolename="admin"/>
  <role rolename="admin-gui"/>
  <user username="admin" password="******" roles="admin,admin-
gui,manager,manager-gui"/>
```

Configuració del servidor Tomcat segur

Volem que les connexions des d'Internet siguin segures. Per aconseguir-ho, primer generem un certificat autosignat per al servidor amb l'eina keytool, que guardarem en la carpeta **conf** del Tomcat.

```
root@assistpda:~# keytool -genkey -alias tomcat -keyalg RSA -keystore
/opt/tomcat/conf/assistpda.jks
```

Falta dir-li a Tomcat que utilitzi SSL. Editem l'arxiu **server.xml** de la configuració de Tomcat i li indiquem la ubicació de l'arxiu keystore i la seva contrasenya.

```
root@assistpda:~# nano /opt/tomcat/conf/server.xml
```

```
  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
              maxThreads="150" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS"
              keystoreFile="/opt/tomcat/conf/assistpda.jks"
              keystorePass="*********" />
```

Instal·lació del servlet Davenport

Davenport és un servlet que permet accedir mitjançant WebDAV a un espai compartit Samba o Windows a través d'un contenidor com Tomcat.

Primer ens baixem el servlet.

```
root@assistpda:~#wget
http://sourceforge.net/projects/davenport/files/davenport/0.9.11/davenport-
0.9.11.tgz
```

El descomprimim i el copiem al directori d'aplicacions de Tomcat.

```
root@assistpda:~# tar -xvzf davenport-0.9.11.tgz
root@assistpda:~# cp -r davenport-0.9.11/webapps/*
/opt/tomcat/webapps/davenport
```

També actualitzem la llibreria **jcifs** que utilitza Davenport per a comunicar-se amb el servidor Samba.

```
root@assistpda:~# cd /opt/tomcat/webapps/davenport/WEB-INF/lib/
root@assistpda:/opt/tomcat/webapps/davenport/WEB-INF/lib# wget
http://jcifs.samba.org/src/jcifs-1.3.17.jar
root@assistpda:/opt/tomcat/webapps/davenport/WEB-INF/lib# rm jcifs-1.2.13.jar
```

Només ens queda modificar alguns dels paràmetres de l'arxiu de configuració del servlet per adaptar-lo al nostre sistema.

```
root@assistpda:/opt/tomcat/webapps/davenport/WEB-INF# nano web.xml
```

Els paràmetres següents indiquen: el domini, l'adreça del controlador de domini i l'adreça del servidor WINS.

```
    <init-param>
        <param-name>jcifs.smb.client.domain</param-name>
        <param-value>IESMIQUELBOSCH</param-value>
    </init-param>
    <init-param>
        <param-name>jcifs.http.domainController</param-name>
        <param-value>192.168.0.207</param-value>
    </init-param>
    <init-param>
        <param-name>jcifs.netbios.wins</param-name>
        <param-value>192.168.0.207</param-value>
    </init-param>
```

El sistema d'autenticació utilitzat serà l'autenticació bàsica HTTP sota una connexió segura. Configurem Davenport perquè no ofereixi NTLM com a mecanisme d'autenticació.

```
    <init-param>
        <param-name>enableNtlm</param-name>
        <param-value>false</param-value>
    </init-param>
```

"INS Miquel Bosch i Jover" és el nom del servidor presentat pel sistema d'autenticació en el moment de demanar les credencials als usuaris.

```
    <init-param>
        <param-name>jcifs.http.basicRealm</param-name>
        <param-value>INS Miquel Bosch i Jover</param-value>
    </init-param>
```

UTF-8 serà el joc de caràcters utilitzat per interpretar les peticions dels clients.

```
    <init-param>
        <param-name>request-uri.charset</param-name>
        <param-value>UTF-8</param-value>
    </init-param>
```

La resta de paràmetres es deixen amb la configuració inicial.

5.2.5 Servei client Bacula

El servidor de faltes serà un client del sistema de còpies de seguretat del centre. Ens interessa tenir còpies de la base de dades de l'aplicatiu que gestiona el control de faltes. Per aconseguir-ho s'ha programat el cron perquè cada dia faci un bolcat de les bases de dades en el directori **/assistpda-db** del servidor de faltes. En concret, cron executa l'script:

```
#!/bin/bash
mysqldump --opt -uroot -p******  -hlocalhost assist > /assistpda-db/$(date +%d%m
%Y.%H%M).assist.sql
```

Per tenir còpies de seguretat dels bolcats, s'ha configurat el servidor de faltes com a client Bacula, fent còpies de seguretat del director **/assistpda-db** periòdicament. També es farà còpia dels directoris **/var/www** i

/opt/tomcat/webapps/davenport. El contingut sencer de l'arxiu de configuració **/ect/bacula/bacula-fd.conf** el trobem a l'Annex C.

5.3 Tallafocs

La intervenció sobre el tallafocs ha estat la següent:

- Instal·lació del sistema operatiu Debian 6 Squeeze. ([6])
- Modificació de la configuració inicial del servei SSH. ([2] Capítol 4 – SSH; [3] Capítol 7 – Administración remota segura con SSH; [6])
- Definició de les regles iptables. ([3] Capítol 3 -Creación de un cortafuegos en Linux; [7])

5.3.1 Servei SSH

Hem canviat la configuració inicial del servei SSH seguint els mateixos criteris de seguretat que els utilitzats en les configuracions dels servidors. Es farà servir el port 50002 per a les connexions remotes.

5.3.2 Definició de les regles iptables

En aquesta secció implementarem un tallafocs amb l'aplicació iptables. La seva funció serà filtrar el tràfic de paquets entre les diferents xarxes: Internet, Intranet i DMZ. Per aconseguir-ho, hem definit un conjunt de regles, resumides en els punts següents:

- Política per defecte DENEGAR.
- Tot el que vingui d'Internet als ports 53,80,443,8443,52001 es redirigeix al servidor de faltes.

- Tot el que vingui d'Internet al port 50207 es redirigeix al servidor de centre.
- Tots els paquets que surtin del tallafocs cap a Internet se'ls canvia l'adreça origen.
- Es permeten connexions SSH amb el tallafocs des d'Internet.
- Es permeten connexions SSH amb el tallafocs des de la Intranet.
- Es permeten consultes al servidor de faltes HTTP i HTTPS des d'Internet.
- Es permeten consultes al servidor de faltes DNS des d'Internet.
- Es permeten consultes al servidor de faltes TOMCAT des d'Internet.
- El servidor de faltes ha de poder consultar el servidor de centre SMB.
- El servidor de faltes ha de poder consultar altres servidors DNS.
- El servidor de faltes ha de poder consultar altres servidors HTTP.
- Es permeten connexions SSH amb el servidor de faltes des d'Internet.
- Els usuaris de la Intranet han de poder consultar el servidor DNS.
- Es permeten connexions SSH cap a el servidor de faltes des de la Intranet.
- Es permeten connexions HTTP i HTTPS des de la Intranet.
- Es permeten consultes del correu des de la Intranet.
- Es permeten consultes al servidor TOMCAT des de la Intranet.
- Es permeten connexions SSH al servidor de centre des d'Internet.
- Bacula ha de poder consultar el port 9102 del client.

- Els ports 9101, 9103 del servidor de centre han de ser accessibles per al client Bacula.

L'script final **iptables_fw.sh** amb totes les regles aplicades el podem veure a l'Annex D. En l'script s'han definit dues noves cadenes: **paquets_tcp_incorrectes** i **paquets_tcp_permesos**. La primera intenta evitar l'atac per suplantació d'identitat IP spoofing i rebutja tots els paquets en estat NEW que no tinguin establert el bit SYN.

```
iptables -A paquets_tcp_incorrectes -p tcp --tcp-flags SYN,ACK SYN,ACK -m state
--state NEW -j REJECT --reject-with tcp-reset
iptables -A paquets_tcp_incorrectes -p tcp ! --syn -m state --state NEW -j LOG
--log-prefix "NEW sense syn:"
iptables -A paquets_tcp_incorrectes -p tcp ! --syn -m state --state NEW -j DROP
```

Les regles anteriors s'han afegit a les cadenes INPUT, OUTPUT i FORWARD.

La segona cadena comença comprovant si es troba davant un paquet SYN, si és el cas, li permet el pas. Comprova després si el paquet prové d'una connexió ja establerta o relacionada, en cas afirmatiu el deixa passar. L'última regla rebutja tota la resta de paquets.

```
iptables -A paquets_tcp_permesos -p TCP --syn -j ACCEPT
iptables -A paquets_tcp_permesos -p TCP -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A paquets_tcp_permesos -p TCP -j DROP
```

6. Resultats, proves i valoració econòmica

En aquest apartat es fa un resum dels resultats obtinguts, així com les implicacions econòmiques que ha representat per al centre dur a terme aquest projecte.

6.1 Resultats i proves de funcionament

A nivell d'administradors, el sistema ofereix la possibilitat de connectar via SSH amb els servidors de forma segura amb criptografia pública, utilitzant un port i nom d'usuari específic. Les línies següents mostren una connexió amb el servidor de faltes.

```
arnaldo@ubuntu:~$ ssh -p 52001 manaia@www.iesmiquelbosch.cat
Linux assistpda 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May  1 16:20:02 2013 from 172.16.0.1
manaia@assistpda:~$
```

Amb la consola del programa Bacula, l'administrador pot fer còpies de seguretat o restaurar arxius i directoris. Aquí reproduïm una sessió de còpia de seguretat del servidor de faltes.

```
root@s-207:/home/manaia# bconsole
Connecting to Director 192.168.0.207:9101
1000 OK: s-207-dir Version: 5.0.2 (28 April 2010)
Enter a period to cancel a command.
*run
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
A job name must be specified.
The defined Job resources are:
     1: Backup assistpda
     2: Backup s-207
     3: Backup Cataleg
     4: Restaurar assistpda
     5: Restaurar s-207
     6: Restaurar Cataleg
Select Job resource (1-6): 1
Run Backup job
JobName:  Backup assistpda
Level:    Incremental
Client:   assistpda-fd
```

```
FileSet:  assistpda-db
Pool:     Default (From Job resource)
Storage:  File (From Job resource)
When:     2013-05-01 16:28:15
Priority: 10
OK to run? (yes/mod/no): yes
Job queued. JobId=41
*
```

S'ha configurat perquè l'administrador rebi en forma de correu electrònic les notificacions dels treballs fets pel sistema de còpies de seguretat (veure figura 12).

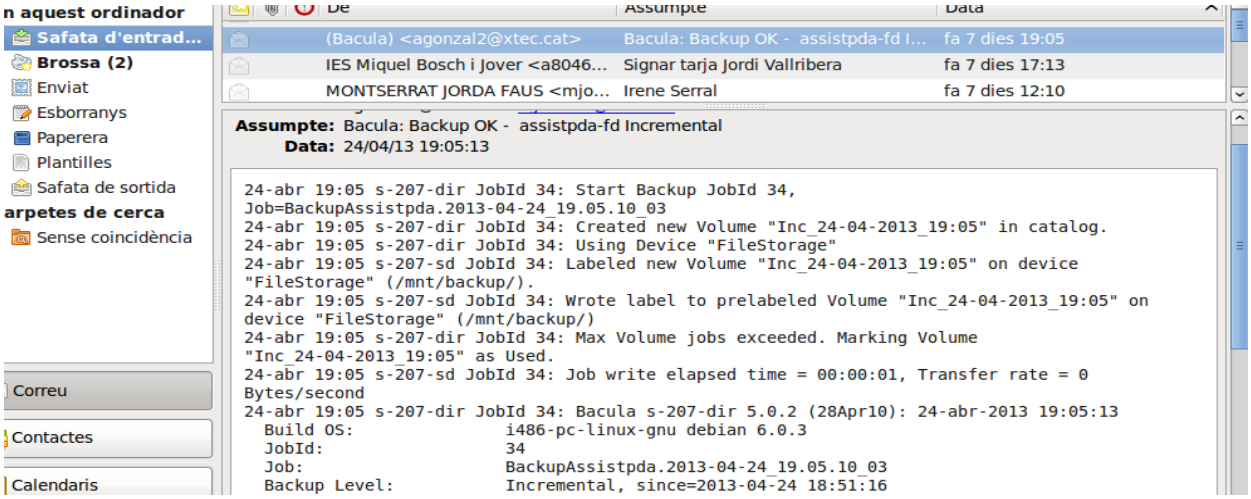

Figura 12. Bacula informa l'administrador del treball fet

Des del punt de vista dels usuaris, el projecte aporta millores i nous serveis. A partir d'ara, tot usuari del domini té accés al seu espai personal i espais compartits, tant des de la Intranet com des d'Internet.

Des de la Intranet, un cop iniciada la sessió, l'usuari pot guardar els documents en el seu espai personal o compartir-los en els espais comuns, com podem veure a la figura 13.

Figura 13. L'usuari té accés a les diferents unitats de xarxa on pot compartir documents

Utilitzant un programa client WebDAV, com per exemple Cyberduck, els usuaris Windows o Mac poden accedir, també des d'Internet, als espais personals i espais compartits (Figures 14 i 15).

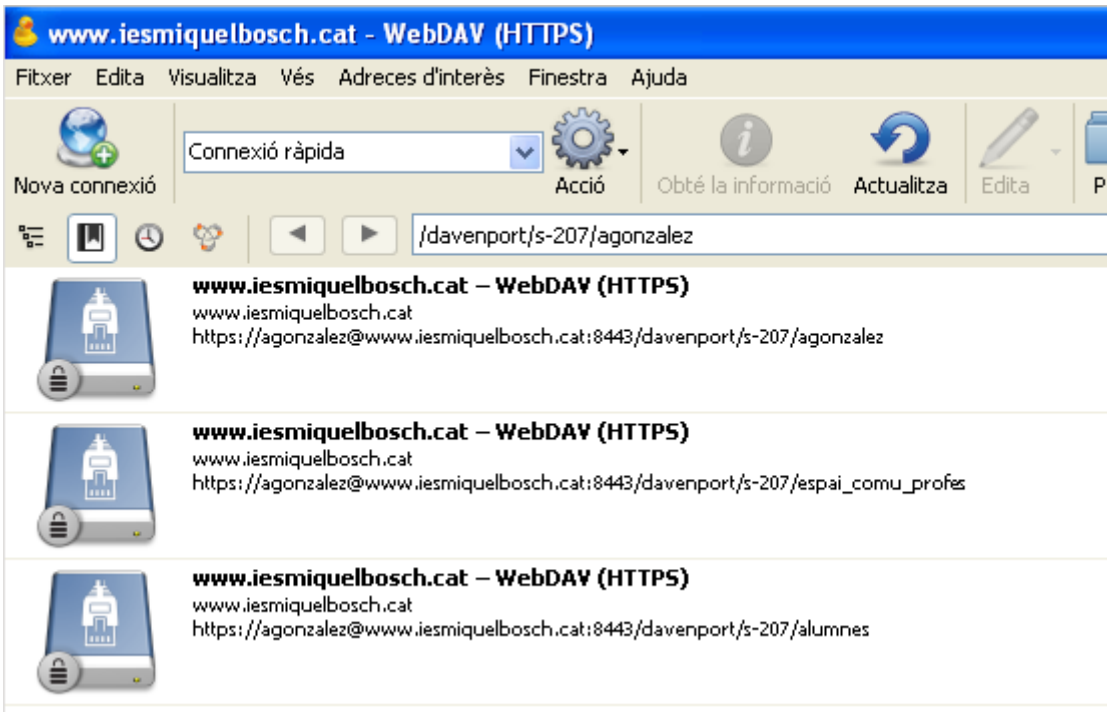

Figura 14. Accedint als espais personals i espais compartits des d'Internet

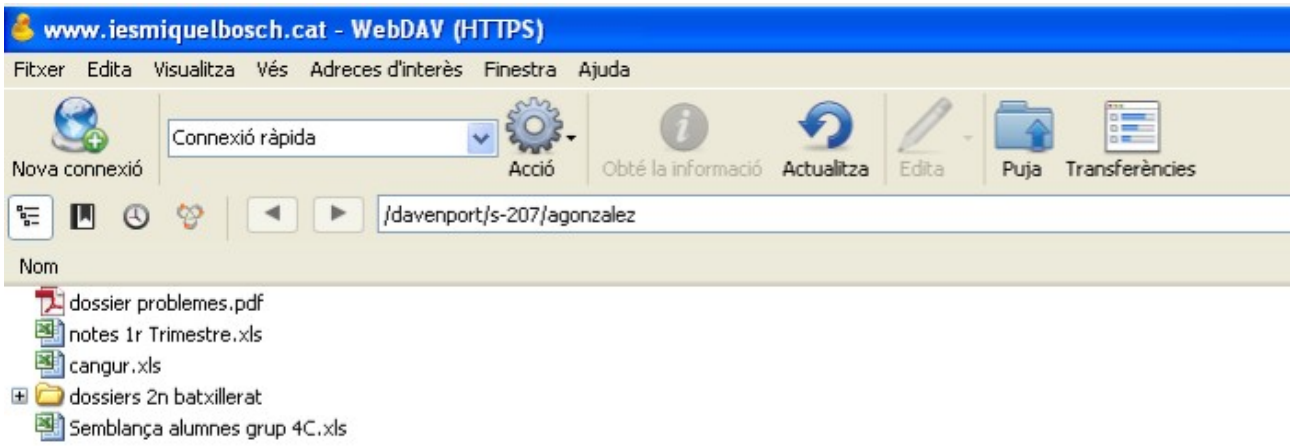

Figura 15. Consultant els documents personals des d'Internet

Els usuaris GNU/Linux també poden accedir als seus espais personals i espais compartits des d'Internet. Utilitzant un client WebDAV, com per exemple Cadaver, podem realitzar diferents operacions sobre els arxius, moure o copiar, crear nous directoris, etc. Aquí veiem un exemple de sessió.

```
arnaldo@ubuntu:~$ cadaver https://www.iesmiquelbosch.cat:8443/davenport/s-
207/agonzalez
WARNING: Untrusted server certificate presented for `www.iesmiquelbosch.cat':
Issued to: INS Miquel Bosch i Jover, Departament d'Ensenyament, Artés,
Barcelona, ES
Issued by: INS Miquel Bosch i Jover, Departament d'Ensenyament, Artés,
Barcelona, ES
Certificate is valid from Thu, 28 Feb 2013 17:32:17 GMT to Fri, 28 Feb 2014
17:32:17 GMT
Do you wish to accept the certificate? (y/n) y
Authentication required for iesmiquelbosch.cat on server
`www.iesmiquelbosch.cat':
Username: agonzalez
Password:
dav:/davenport/s-207/agonzalez/> mkcol "2n BTX"
Creating `2n BTX': succeeded.
dav:/davenport/s-207/agonzalez/> ls
Listing collection `/davenport/s-207/agonzalez/': succeeded.
Coll:   2n BAT                                  0     mar 17 20:37
Coll:   2n BTX                                  0     mar 17 20:56
Coll:   3r ESO                                  0     mar 15 23:06
Coll:   4t ESO                                  0     mar 15 23:28
Coll:   dossiers 2n batxillerat                 0     mar 15 23:06
        .bash_logout                          220     feb  7 17:16
        .bashrc                              3184     feb  7 17:16
        .profile                              675     feb  7 17:16
        Semblança alumnes grup 4C.xls      489984     mar 10 19:59
        cangur.xls                          32768     mar  5 18:27
        cangur4.xls                         32768     mar 15 21:25
        dossier problemes.pdf             1924073     mar  3 21:08
        notes 1r Trimestre.xls             214016     mar 10 23:55
dav:/davenport/s-207/agonzalez/>  get cangur.xls
Downloading `/davenport/s-207/agonzalez/cangur.xls' to cangur.xls:
Progress: [============================>] 100,0% of 32768 bytes succeeded.
dav:/davenport/s-207/agonzalez/> quit
Connection to `www.iesmiquelbosch.cat' closed.
arnaldo@ubuntu:~$
```

L'accés al servidor de faltes, ja sigui des de la Intranet o des d'Internet, es fa de forma segura (Figura 16).

Figura 16. Accés segur al servidor de faltes

La comunicació entre les PDAs i el servidor de faltes, que fins ara es feia de forma insegura, a partir d'ara serà xifrada (Figura 17).

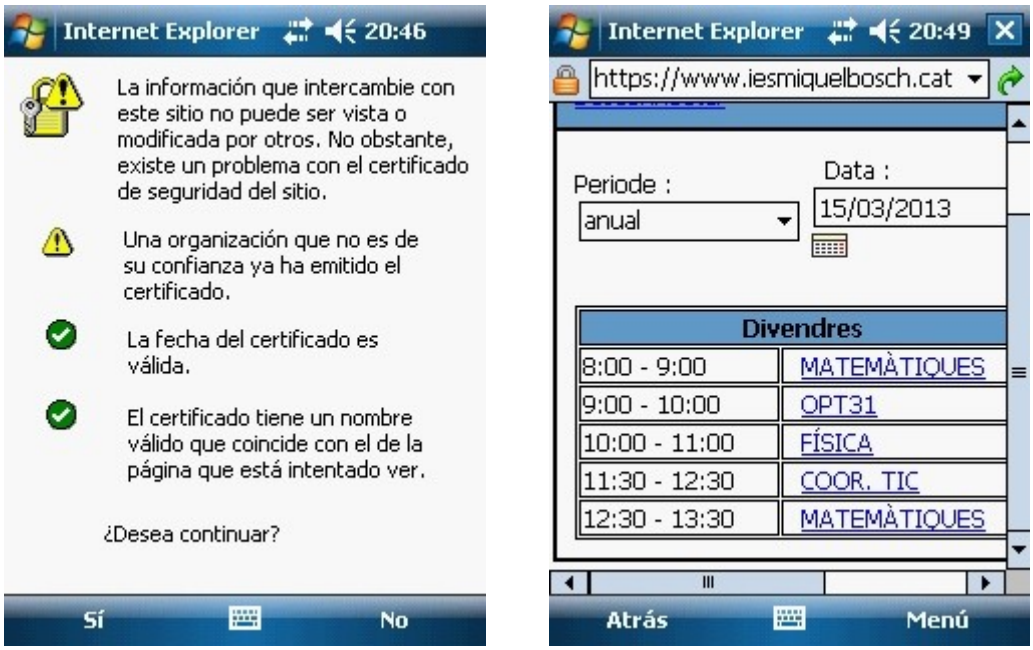

Figura 17. Comunicació segura a l'hora de passar llista

6.2 Valoració econòmica

Respecte a la valoració econòmica, i com ja s'havia previst en l'estudi de viabilitat, la despesa d'aquest projecte ha estat zero. Cal esmentar alguns factors que han fet possible aquest miracle. En primer lloc, abans de l'inici del projecte el centre ja disposava d'un servidor nou, que estava pendent de ser configurat i posat en marxa. En segon lloc, s'han reutilitzat i reubicat els antics servidors, donant-los una segona oportunitat. I finalment, el fet de coincidir en la mateixa persona coordinador d'informàtica del centre i alumne de l'assignatura “Pràctiques externes del Màster en Programari Lliure”, ha fet que el cost en recursos humans hagi estat zero.

També hem comptat la despesa que hagués representat per al centre en el supòsit que les circumstàncies anteriors no s'haguessin donat. En aquest cas, i comptant amb la reutilització i reubicació dels antics servidors, el cost de material es reduiria al cost del nou servidor de centre. En la taula 12 es desglossa el cost del projecte, identificant el cost dels recursos materials i el dels recursos humans.

Recursos materials:			
Element	**Quantitat**	**Cost unitat**	**Cost**
Nou servidor de centre Intel Xeon, 8 GB de memòria RAM i disposa de controladora RAID i quatre discos de 1TB	1	3200	3200
		Total	3.200,00 €
Recursos humans:			
Actuacions		**Hores**	**Cost**
Servidor de centre		90	5400
Servidor de faltes		50	3000
Tallafocs		30	1800
Implantació i proves de funcionament		15	900
		Total	11.100,00 €
		Cost total	**14.300,00 €**

Taula 12. Valoració econòmica del projecte

7. Conclusions

Fent una mirada retrospectiva als objectius plantejats inicialment en aquest projecte, podem afirmar que la majoria han estat assolits.

- S'ha renovat el servidor de centre, amb una màquina amb més rendiment i fiabilitat.
- En tot moment s'ha utilitzat programari lliure, això ens permet mantenir els servidors actualitzats i sense despeses de llicències privatives.
- S'ha elaborat un nou servei de directori i autenticació, on cada usuari disposa d'un espai personal i espais compartits d'intercanvi de documents.
- Es dóna als usuaris la possibilitat d'accedir des d'Internet als seus espais personals i espais compartits.

Altres intervencions no previstes en els objectius inicials i que ha calgut portar a terme, fonamentalment per qüestions de seguretat, han estat les següents:

- Protegir la xarxa interna mitjançant un tallafocs.
- Crear una zona desmilitaritzada per atendre les consultes al servidor de faltes des d'Internet.
- Migrar el servidor de faltes cap al programari lliure. Inicialment el servidor de faltes utilitzava el programa EasyPHP per oferir els serveis web.
- Protegir les comunicacions amb el servidor de faltes utilitzant connexions segures HTTPS.
- Automatitzar el sistema de còpies de seguretat, tant del servidor de centre com del servidor de faltes.

Com sempre, el temps ha quedat curt. Un dels objectius inicials pendent és la implantació d'un sistema centralitzat d'impressió. Serà una de les tasques a realitzar en el futur.

A nivell personal també voldria recollir alguna de les reflexions i impressions que em vénen al cap un cop finalitzat el projecte.

D'entrada valorar molt positivament el poder haver fet les pràctiques en el mateix centre on treballo. El fet de coincidir en la mateixa persona coordinador d'informàtica i alumne en pràctiques m'ha facilitat les coses a l'hora de tirar endavant el projecte, donant-me un marge de llibertat, que potser en altres circumstàncies no hagués estat possible. Tanmateix prens consciència que la feina feta no cau en un pou sense fons i que el centre en pot sortir beneficiat.

Els coneixements adquirits amb la realització del projecte són múltiples i molt valuosos. En primer lloc, m'han aportat un major coneixement sobre la xarxa educativa del centre i la relació entre els diferents dispositius que la conformen, donant-me seguretat i confiança en la meva tasca de coordinació. En segon lloc, al tractar-se en gran part d'una migració de servidors i al ser configurats des de zero, m'he vist en l'obligació d'aprofundir en la configuració de serveis i servidors, a un nivell més alt que el vist al llarg del Màster.

D'altra banda, de problemes tampoc no n'han faltat. Escollir aquell paquet que millor s'adapti a la configuració que s'està muntant, de vegades es converteix en un feina d'artesania. Instal·lar i configurar aplicatius que mai abans havies utilitzat, requereix temps i paciència. Precisament, la raó per la qual es va escollir Debian com a distribució va ser el recolzament que en tot moment s'obté dels seus seguidors.

És evident que el projecte representa una petita aportació a favor del programari lliure. Ha estat una migració de servidors, una de les més fàcils de dur a terme, sense la implicació dels usuaris finals. Queda molta feina per fer i molta tasca de divulgació si volem estendre la migració a la resta de màquines del centre.

De totes maneres, podem afirmar que gràcies a aquest projecte, el programari lliure ha començat a instal·lar-se en el nostre centre. Esperem que sigui per sempre.

8. Bibliografia

[1] Carter, Gerald; Ts, Jay; Eckstein, Robert (2008). *Samba*. Ediciones Anaya Multimedia.

[2] Llinares, Raúl; Ferri, Josué (2009). *Instal·lació i configuració de serveis TCP/IP en servidors GNU/Linux*. Editorial UPV.

[3] Schroder, Carla (2009). *Redes en linux. Guía de referencia.* Ediciones Anaya Multimedia.

[4] Siever, Ellen; Figgins, Stephen; Love, Robert; Robbins, Arnold (2010). *Linux*. Ediciones Anaya Multimedia.

[5] Material docent de la UOC:

Serra, Jordi; Suppi, Remo; Jorba, Josep (2009). *Projecte en administració de xarxes i sistemes operatius en entorns de programari lliure*. Versió en PDF disponible a: http://cv.uoc.es/cdocent/F0GSMRKVDQBZD295WEVZ.pdf. FOUC.

9. Webgrafia

[6] Projecte Debian: (maig 2013)
http://www.debian.org/index.ca.html
http://wiki.debian.org/es/FrontPage

[7] Tutorial Iptables: (maig 2013)
http://rlworkman.net/howtos/iptables/spanish/chunkyhtml/index.html

[8] Servlet Davenport: (maig 2013)
http://davenport.sourceforge.net/

[9] Projecte Bacula: (maig 2013)
http://www.bacula.org/es/

Annex A

Esquema de l'arquitectura de xarxa del centre abans de la intervenció (Figura A.1).

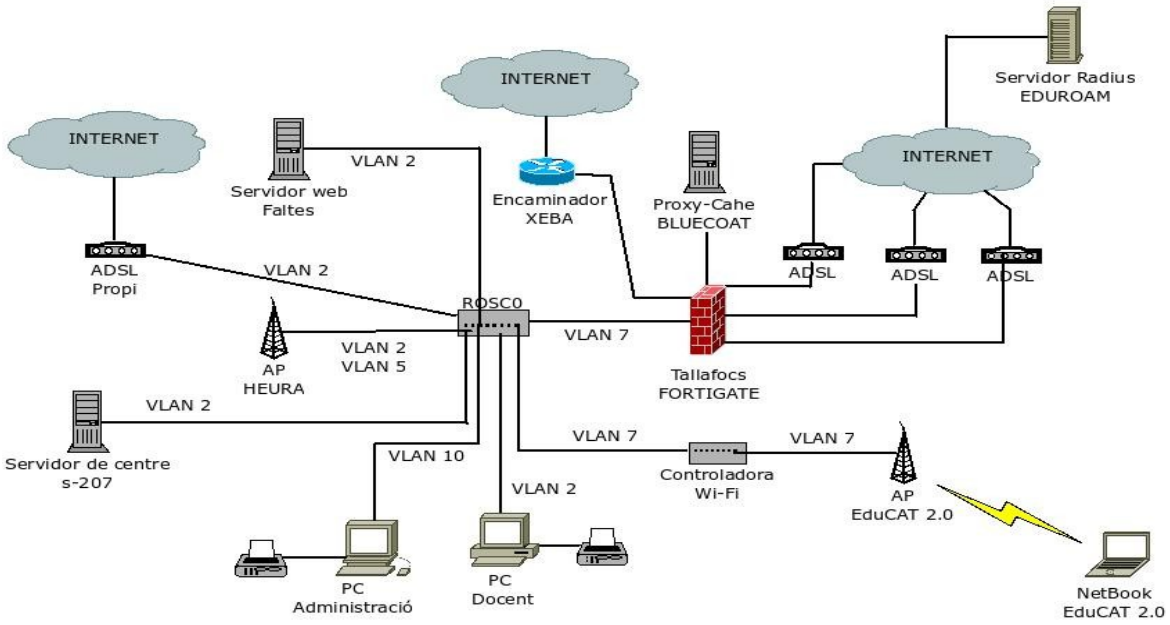

Figura A.1. Estat inicial de la xarxa educativa del centre

Solució proposada: creació d'una zona desmilitaritzada (DMZ) i incorporació d'un tallafocs (Figura A.2).

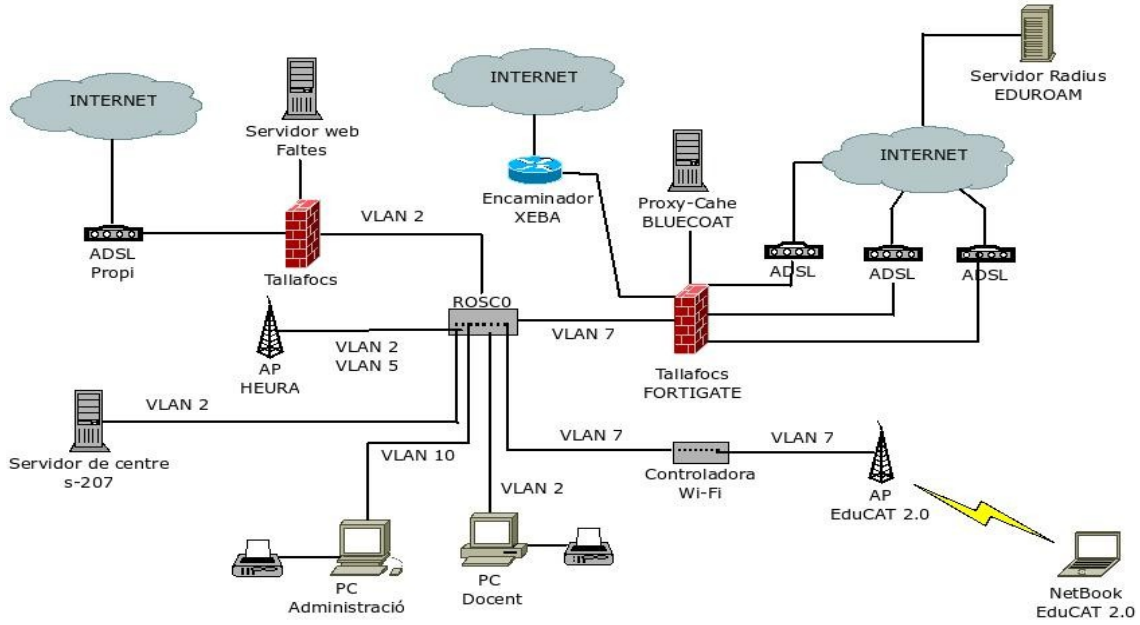

Figura A.2. Amb el Tallafocs i la DMZ es protegeix la xarxa educativa del centre de possibles atacs exteriors

Annex B

Scripts per donar d'alta alumnes i professors. A l'script se li passa un arxiu de text amb les dades dels usuaris.

Script **profes_nous.sh**

```
#! /bin/bash
vi -c ":wq! ++enc=iso-8859-15" profes
dia=$( date +%H:%M:%S_%d-%m-%Y)
echo -e "$1 $dia" >> altes.txt
echo -e "Dades de connexió dels nous usuaris/àries creats/des\n" >> altes.txt
while IFS=, read nom cognom1 cognom2 nomusuari contrasenya departament
do
cognoms="$cognom1 $cognom2"
smbldap-useradd -a -m -g profes -E $nomusuari.bat -s /bin/false -d
/home/iesmbj/profes/$departament/$nomusuari -N $nom -S "$cognoms" -G
$departament $nomusuari
setfacl -m u:$nomusuari:rwx,g::---,o::--- /home/iesmbj/profes/$departament/
$nomusuari
setfacl -d -m u:$nomusuari:rwx,g::---,o::--- /home/iesmbj/profes/$departament/
$nomusuari
echo -e $contrasenya\\n$contrasenya | smbldap-passwd $nomusuari
echo "NET USE q: \\\s-207\espai_comu_profes" >> /srv/samba/netlogon/
$nomusuari.bat
echo "NET USE r: \\\s-207\espai_comu_$departament" >> /srv/samba/netlogon/
$nomusuari.bat
echo "NET USE s: \\\s-207\alumnes" >> /srv/samba/netlogon/$nomusuari.bat
echo -e "$nom $cognom1 $cognom2\n\
Departament:\t $departament\n\
Nom d'usuari:\t $nomusuari\n\
Contrasenya :\t $contrasenya\n\
Carpeta personal:\t /home/iesmbj/profes/$departament/$nomusuari\n\
---" >> altes.txt
done < $1
```

Script **alumnes_nous.sh**

```
#! /bin/bash
vi -c ":wq! ++enc=iso-8859-15" alumnes
dia=$( date +%H:%M:%S_%d-%m-%Y)
echo -e "$1 $dia" >> altes.txt
echo -e "Dades de connexió dels nous usuaris/àries creats/des\n" >> altes.txt
while IFS=, read nom cognom1 cognom2 nomusuari contrasenya curs
do
cognoms="$cognom1 $cognom2"
smbldap-useradd -a -m -g alumnes -E $nomusuari.bat -s /bin/false -d
/home/iesmbj/alumnes/$curs/$nomusuari -N "$nom" -S "$cognoms" -G $curs
$nomusuari
setfacl -m u:$nomusuari:rwx,g:profes:rwx,g::---,o::--- /home/iesmbj/alumnes/
$curs/$nomusuari
setfacl -d -m u:$nomusuari:rwx,g:profes:rwx,g::---,o::--- /home/iesmbj/alumnes/
$curs/$nomusuari
```

```
echo –e $contrasenya\\n$contrasenya | smbldap-passwd $nomusuari
echo "NET USE q: \\\s-207\espai_comu_$curs" >  /srv/samba/netlogon/
$nomusuari.bat
echo –e "$nom $cognom1 $cognom2\n\
Curs:\t $curs\n\
Nom d'usuari:\t $nomusuari\n\
Contrasenya :\t $contrasenya\n\
Carpeta personal:\t /home/iesmbj/alumnes/$curs/$nomusuari\n\
---" >> altes.txt
done < $1
```

Annex C

Arxius de configuració del servei de còpies de seguretat.

Director (servidor de centre): **`/etc/bacula/bacula-dir.conf`**

```
#
#
# CONFIGURACIÓ BACULA DIRECTOR
#
# adaptació de l'arxiu de configuració
# original bacula-dir.conf
#
#
#Default Bacula Director Configuration file
#
#  The only thing that MUST be changed is to add one or more
#   file or directory names in the Include directive of the
#   FileSet resource.
#
#  For Bacula release 5.0.2 (28 April 2010) -- debian 6.0.3
#
#  You might also want to change the default email address
#   from root to your address.  See the "mail" and "operator"
#   directives in the Messages resource.
#

Director {                            # define myself
  Name = s-207-dir
  DIRport = 9101                # where we listen for UA connections
  QueryFile = "/etc/bacula/scripts/query.sql"
  WorkingDirectory = "/var/lib/bacula"
  PidDirectory = "/var/run/bacula"
  Maximum Concurrent Jobs = 1
  Password = "x9tkKeZdfDjSgJeD1lTarCa32yP8EsfwjSjsIuO9n/J7"   # Console password
  Messages = Daemon
  DirAddress = 192.168.0.207
}

# Generic catalog service
Catalog {
  Name = MyCatalog
  dbname = bacula; DB Address = "127.0.0.1"; dbuser = "bacula"; dbpassword =
"*******"
}


#
#
# CLIENT s-207
#
#

Client {
  Name = s-207-fd
  Address = 192.168.0.207
  FDPort = 9102
  Catalog = MyCatalog
```

```
  Password = "eXgw6hb9t0z1Y4qVob9mMxXgZzNohIaWM"     # password for FileDaemon
  File Retention = 30 days            # 30 days
  Job Retention = 6 months            # six months
  AutoPrune = yes                     # Prune expired Jobs/Files
}

#
#
# CLIENT assistpda
#
#

Client {
  Name = assistpda-fd
  Address = 192.168.200.1
  FDPort = 9102
  Catalog = MyCatalog
  Password = "eXgw6hb9t0z1Y4qVob9mMxXgZzNohIaWM2"    # password for FileDaemon 2
  File Retention = 30 days            # 30 days
  Job Retention = 6 months            # six months
  AutoPrune = yes                     # Prune expired Jobs/Files
}

#
#
# FILESET BACKUP assistpda
#
#

FileSet {
      Name = "assistpda-db"
      Include {
            Options {
            signature = SHA1
            }
      File = /assistpda-db
      File = /var/www
      File = /opt/tomcat/webapps/davenport
      }
}

#
#
# FILESET BACKUP s-207
#
#

FileSet {
  Name = "iesmbj"
  Include {
        Options {
                signature = SHA1
                compression = GZIP9
                onefs = yes
                aclsupport = yes
                }
        File = /home/iesmbj
      File = /root
  }
}
```

```
#
#
# FILESET BACKUP Cataleg
#
#


FileSet {
  Name = "Catalog"
  Include {
    Options {
      signature = SHA1
    }
    File = "/var/lib/bacula/bacula.sql"
  }
}


#
#
# TREBALL  BACKUP  assistpda
#
#

Job {
        Name = "Backup assistpda"
        JobDefs = assistpda-def
        Client = assistpda-fd
    }

JobDefs {
        Name = "assistpda-def"
        Type = Backup
        Level = Incremental
        FileSet = assistpda-db
        Pool = Default
        Full Backup Pool = Pool-Full
        Incremental Backup Pool = Pool-Inc
        Schedule = WeeklyCycle
        Storage = File
        Messages = Standard
        Priority = 10
        Write Bootstrap = "/var/lib/bacula/assistpda.bsr"
}

#
#
# TREBALL  BACKUP  s-207
#
#

Job {
        Name = "Backup s-207"
        JobDefs = s-207-def
        Client = s-207-fd
    }

JobDefs {
        Name = "s-207-def"
        Type = Backup
        Level = Incremental
```

```
        FileSet = iesmbj
        Pool = Default
        Full Backup Pool = Pool-Full
        Incremental Backup Pool = Pool-Inc
        Schedule = WeeklyCycle
        Storage = File
        Messages = Standard
        Priority = 10
        Write Bootstrap = "/var/lib/bacula/s-207.bsr"
}

#
#
# TREBALL  BACKUP  Cataleg
#
#

Job {
        Name = "Backup Cataleg"
        JobDefs = catalog-def
        Client = s-207-fd
    }

JobDefs {
        Name = "catalog-def"
        Type = Backup
        Level = Full
        FileSet = Catalog
        Pool = Catalog
        Schedule = WeeklyCycleAfterBackup
        Storage = File
        Messages = Standard
        Priority = 15
        RunBeforeJob = "/etc/bacula/scripts/make_catalog_backup bacula bacula
bacula localhost"
        RunAfterJob  = "/etc/bacula/scripts/delete_catalog_backup"
        Write Bootstrap = "/var/lib/bacula/BackupCatalog.bsr"
}

#
#
# RESTAURAR assistpda
#
#

Job {
        Name = "Restaurar assistpda"
        Type = Restore
        Client = "assistpda-fd"
        FileSet = assistpda-db
        Storage = File
        Pool = Default
        Full Backup Pool = Pool-Full
        Incremental Backup Pool = Pool-Inc
        Messages = "Standard"
        Where = /tmp
}

#
#
# RESTAURAR    s-207
```

```
#
#

Job {
        Name = "Restaurar s-207"
        Type = Restore
        Client = "s-207-fd"
        FileSet = iesmbj
        Storage = File
        Pool = Default
        Full Backup Pool = Pool-Full
        Incremental Backup Pool = Pool-Inc
        Messages = "Standard"
        Where = /tmp
}

#
#
# RESTAURAR    Cataleg
#
#

Job {
        Name = "Restaurar Cataleg"
        Type = Restore
        Client = "s-207-fd"
        FileSet = Catalog
        Storage = File
        Pool = Catalog
        Messages = "Standard"
        Where = /tmp

}

#
#
# LOGS I ENVIAMENTS DE CORREUS
#
#
#
# Reasonable message delivery -- send most everything to email address
#  and to the console
Messages {
  Name = Standard
#
# NOTE! If you send to two email or more email addresses, you will need
#  to replace the %r in the from field (-f part) with a single valid
#  email address in both the mailcommand and the operatorcommand.
#  What this does is, it sets the email address that emails would display
#  in the FROM field, which is by default the same email as they're being
#  sent to.  However, if you send email to more than one address, then
#  you'll have to set the FROM address manually, to a single address.
#  for example, a 'no-reply@mydomain.com', is better since that tends to
#  tell (most) people that its coming from an automated source.

#

  mailcommand = "/usr/bin/sendEmail -s smtp.gmail.com:587 -xu agonzal2@xtec.cat
-xp ****** -f \"\(Bacula\) \<%r\>\" -u \"Bacula: %t %e of %c %l\" -t %r"
  operatorcommand = "/usr/bin/sendEmail -s smtp.gmail.com:587 -xu
agonzal2@xtec.cat -xp ****** -f \"\(Bacula\) \<%r\>\" -u \"Bacula: Intervention
```

```
needed for %j\" -t %r"
  mail = agonzal2@xtec.cat = all, !skipped
  operator = agonzal2@xtec.cat = mount
  console = all, !skipped, !saved
#
# WARNING! the following will create a file that you must cycle from
#          time to time as it will grow indefinitely. However, it will
#          also keep all your messages if they scroll off the console.
#
  append = "/var/lib/bacula/log" = all, !skipped
  catalog = all
}


#
# Message delivery for daemon messages (no job).
Messages {
  Name = Daemon
  mailcommand = "/usr/bin/sendEmail -s smtp.gmail.com:587 -xu agonzal2@xtec.cat
-xp ******  -f \"\(Bacula\) \<%r\>\" -u \"Bacula daemon message\" -t %r"
  mail = agonzal2@xtec.cat = all, !skipped
  console = all, !skipped, !saved
  append = "/var/lib/bacula/log" = all, !skipped
}

#
#
# POOL DEFAULT
#
#

Pool {
        Name = "Default"
        Pool Type = "Backup"
        Recycle = yes                       # Bacula can automatically recycle
Volumes
        AutoPrune = yes                     # Prune expired volumes
        Volume Retention = 3 months         # 6 mois
        Maximum Volume Jobs = 1
}

#
#
# POOL FULL
#
#

Pool {
        Name = "Pool-Full"
        Pool Type = "Backup"
        Recycle = yes                       # Bacula can automatically recycle
Volumes
        AutoPrune = yes                     # Prune expired volumes
        Volume Retention = 3 months
        Maximum Volume Bytes = 10G          # Limit Volume size to something
reasonable
        Maximum Volume Jobs = 1
        Maximum Volumes = 50               # Limit number of Volumes in Pool
        Label Format = "Full_${Day:p/2/0/r}-${Month:p/2/0/r}-${Year}_$
{Hour:p/2/0/r}:${Minute:p/2/0/r}"
}
```

```
#
#
# POOL INCREMENTAL
#
#

Pool {
        Name = "Pool-Inc"
        Pool Type = "Backup"
        Recycle = yes                        # Bacula can automatically recycle
Volumes
        AutoPrune = yes                      # Prune expired volumes
        Volume Retention = 2 months
        Maximum Volume Jobs = 1
        Maximum Volumes = 50                # Limit number of Volumes in Pool
        Label Format = "Inc_${Day:p/2/0/r}-${Month:p/2/0/r}-${Year}_$
{Hour:p/2/0/r}:${Minute:p/2/0/r}"
}

#
#
# POOL   CATALOG
#
#

Pool {
        Name = "Catalog"
        Pool Type = "Backup"
        Recycle = yes                        # Bacula can automatically recycle
Volumes
        AutoPrune = yes                      # Prune expired volumes
        Volume Retention = 2 months
        Maximum Volume Jobs = 1
        Maximum Volumes = 50                # Limit number of Volumes in Pool
        Label Format = "Cat-${Day:p/2/0/r}-${Month:p/2/0/r}-${Year}_$
{Hour:p/2/0/r}:${Minute:p/2/0/r}"
}

#
#
# POOL SCRATCH
#
#

Pool {
        Name = "Scratch"
        Pool Type = "Backup"
}

#
#
# SCHEDULE BACKUP
#
#

#
# When to do the backups, full backup on first sunday of the month,
#  differential (i.e. incremental since full) every other sunday,
#  and incremental backups other days
Schedule {
```

```
  Name = "WeeklyCycle"
  Run = Full 1st sun at 2:00
  Run = Incremental mon-sat at 2:00
}

# This schedule does the catalog. It starts after the WeeklyCycle
Schedule {
  Name = "WeeklyCycleAfterBackup"
  Run = Full sun-sat at 3:00
}

#
#
# DISPOSITIU D'EMMAGATZEMAMENT
#
#

# Definition of file storage device
Storage {
  Name = File
# Do not use "localhost" here
  Address = 192.168.0.207                # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "9SWPSDVUYoULQHJxRwZMfK2UYZa0t6dGQ"
  Device = FileStorage
  Media Type = File
}
```

Servei d'emmagatzemament (servidor de centre): **`/etc/bacula/bacula-sd.conf`**

```
#
# Default Bacula Storage Daemon Configuration file
#
#  For Bacula release 5.0.2 (28 April 2010) -- debian 6.0.3
#
# You may need to change the name of your tape drive
#   on the "Archive Device" directive in the Device
#   resource.  If you change the Name and/or the
#   "Media Type" in the Device resource, please ensure
#   that dird.conf has corresponding changes.
#

Storage {                             # definition of myself
  Name = s-207-sd
  SDPort = 9103                  # Director's port
  WorkingDirectory = "/var/lib/bacula"
  Pid Directory = "/var/run/bacula"
  Maximum Concurrent Jobs = 20
  SDAddress = 192.168.0.207
}

#
# List Directors who are permitted to contact Storage daemon
#
Director {
  Name = s-207-dir
```

```
  Password = "9SWPSDVUYoULQHJxRwZMfK2UYZa0t6dGQ"
}

#
# Devices supported by this Storage daemon
# To connect, the Director's bacula-dir.conf must have the
#  same Name and MediaType.
#

Device {
  Name = FileStorage
  Media Type = File
  Archive Device = /mnt/backup/
  LabelMedia = yes;                   # lets Bacula label unlabeled media
  Random Access = Yes;
  AutomaticMount = yes;               # when device opened, read it
  RemovableMedia = no;
  AlwaysOpen = no;
}

#
# Send all messages to the Director,
# mount messages also are sent to the email address
#
Messages {
  Name = Standard
  director = s-207-dir = all
}
```

Servei client (servidor de centre): **`/etc/bacula/bacula-fd.conf`**

```
#
# Default  Bacula File Daemon Configuration file
#
#  For Bacula release 5.0.2 (28 April 2010) -- debian 6.0.3
#
# There is not much to change here except perhaps the
# File daemon Name to
#

#
# List Directors who are permitted to contact this File daemon
#
Director {
  Name = s-207-dir
  Password = "eXgw6hb9t0z1Y4qVob9mMxXgZzNohIaWM"
}

#
# "Global" File daemon configuration specifications
#
FileDaemon {                          # this is me
  Name = s-207-fd
  FDport = 9102                  # where we listen for the director
  WorkingDirectory = /var/lib/bacula
  Pid Directory = /var/run/bacula
  Maximum Concurrent Jobs = 20
  FDAddress = 192.168.0.207
}
```

```
# Send all messages except skipped files back to Director
Messages {
  Name = Standard
  director = s-207-dir = all, !skipped, !restored
}
```

Servei client (servidor de faltes): **`/etc/bacula/bacula-fd.conf`**

```
#
# Default  Bacula File Daemon Configuration file
#
#  For Bacula release 5.0.2 (28 April 2010) -- debian 6.0.3
#
# There is not much to change here except perhaps the
# File daemon Name to
#

#
# List Directors who are permitted to contact this File daemon
#
Director {
  Name = s-207-dir
  Password = "eXgw6hb9t0z1Y4qVob9mMxXgZzNohIaWM2"
}

#
# "Global" File daemon configuration specifications
#
FileDaemon {                          # this is me
  Name = assistpda-fd
  FDport = 9102                  # where we listen for the director
  WorkingDirectory = /var/lib/bacula
  Pid Directory = /var/run/bacula
  Maximum Concurrent Jobs = 20
  FDAddress = 192.168.200.1
}

# Send all messages except skipped files back to Director
Messages {
  Name = Standard
  director = s-207-dir = all, !skipped, !restored
}
```

Annex D

Script **iptables_fw.sh** de configuració del tallafocs.

```
#!/bin/sh

#
# Configuració Internet ( WAN )
#

WAN_IP="172.16.0.2"
WAN_IFACE="eth0"

#
# Configuració xarxa local ( LAN )
#

LAN_IP="192.168.0.2"
LAN_IFACE="eth1"
LAN_S207_IP="192.168.0.207"

#
# Zona desmilitaritzada ( DMZ )
#

DMZ_ASSISTPDA_IP="192.168.200.1"
DMZ_IP="192.168.200.2"
DMZ_IFACE="eth2"

#
# Netegem les regles anteriors i posem els comptadors a zero
#

iptables -F
iptables -X
iptables -Z
iptables -t nat -F

#
# Activem el reenviament en el tallafocs
#

echo "1" > /proc/sys/net/ipv4/ip_forward

#
# Establim les polítiques per defecte
#

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#
# Es crea una cadena pels paquets tcp incorrectes
#

iptables -N paquets_tcp_incorrectes
```

```
#
# Es crea una cadena pels paquets tcp permesos
#

iptables -N paquets_tcp_permesos

#
# Cadena paquets_tcp_incorrectes
#

iptables -A paquets_tcp_incorrectes -p tcp --tcp-flags SYN,ACK SYN,ACK -m state
--state NEW -j REJECT --reject-with tcp-reset
iptables -A paquets_tcp_incorrectes -p tcp ! --syn -m state --state NEW -j LOG
--log-prefix "NEW sense syn:"
iptables -A paquets_tcp_incorrectes -p tcp ! --syn -m state --state NEW -j DROP

#
# Cadena paquets_tcp_permesos
#

iptables -A paquets_tcp_permesos -p TCP --syn -j ACCEPT
iptables -A paquets_tcp_permesos -p TCP -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A paquets_tcp_permesos -p TCP -j DROP

#
# Cadena PREROUTING
#

iptables -t nat -A PREROUTING -p TCP -i $WAN_IFACE -d $WAN_IP -m multiport
--dport 53,80,443,8443 -j DNAT --to-destination $DMZ_ASSISTPDA_IP
iptables -t nat -A PREROUTING -p UDP -i $WAN_IFACE -d $WAN_IP --dport 53 -j DNAT
--to-destination $DMZ_ASSISTPDA_IP:53
iptables -t nat -A PREROUTING -p TCP -i $WAN_IFACE -d $WAN_IP --dport 52001 -j
DNAT --to-destination $DMZ_ASSISTPDA_IP:52001
iptables -t nat -A PREROUTING -p TCP -i $WAN_IFACE -d $WAN_IP --dport 50207 -j
DNAT --to-destination $LAN_S207_IP:50207

#
# Cadena POSTROUTING
#

#
# Tots els paquets que surtin del tallafocs cap a Internet se'ls canvia l'adreça
origen
#

iptables -t nat -A POSTROUTING -o $WAN_IFACE -j SNAT --to-source $WAN_IP

#
# Cadena INPUT
#

#
# Els paquets TCP incorrectes no els volem
#

iptables -A INPUT -p tcp -j paquets_tcp_incorrectes

#
```

```
# Secció Tallafocs
#

#
# Es permeten connexions SSH amb el tallafocs des de l'exterior
#

iptables -A INPUT -p TCP --sport 1024:65535 -i $WAN_IFACE -d $WAN_IP --dport
50002 -j paquets_tcp_permesos

#
# Es permeten connexions SSH amb el tallafocs des de la LAN
#

iptables -A INPUT -p TCP --sport 1024:65535 -i $LAN_IFACE -d $LAN_IP --dport
50002 -j paquets_tcp_permesos

#
# Cadena OUTPUT
#

#
# Els paquets TCP incorrectes no els volem
#

iptables -A OUTPUT -p tcp -j paquets_tcp_incorrectes

#
# Secció Tallafocs
#

#
# Es permeten connexions SSH amb el tallafocs des de l'exterior
#

iptables -A OUTPUT -p TCP --dport 1024:65535 -o $WAN_IFACE -s $WAN_IP --sport
50002 -m state --state ESTABLISHED -j ACCEPT

#
# Es permeten connexions SSH amb el tallafocs des de la LAN
#

iptables -A OUTPUT -p TCP --dport 1024:65535 -o $LAN_IFACE -s $LAN_IP --sport
50002 -m state --state ESTABLISHED -j ACCEPT

#
# Cadena FORWARD
#

#
# Els paquets TCP incorrectes no els volem
#

iptables -A FORWARD -p tcp -j paquets_tcp_incorrectes

#
# Secció DMZ - Servidor de faltes
#
#

#
```

```
# Es permeten consultes al servidor de faltes HTTP i HTTPS des de l'exterior
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 80 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p TCP --sport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 443 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE  -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 443 -m state --state ESTABLISHED -j ACCEPT

#
# Es permeten consultes al servidor de faltes DNS des de l'exterior
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 53 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 53 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p UDP --sport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 53 -j ACCEPT
iptables -A FORWARD -p UDP --dport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 53 -j ACCEPT

#
# Es permeten consultes al servidor TOMCAT des de l'exterior
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 8443 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 8443 -m state --state ESTABLISHED -j ACCEPT

#
# El servidor de faltes ha de poder consultar el servidor de centre
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -d
$LAN_S207_IP --dport 445 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -s
$LAN_S207_IP --sport 445 -m state --state ESTABLISHED -j ACCEPT

#
# El servidor de faltes ha de poder consultar altres servidors DNS
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --dport 53 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --sport 53 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p UDP --sport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --dport 53 -j ACCEPT
iptables -A FORWARD -p UDP --dport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --sport 53 -j ACCEPT

#
# El servidor de faltes ha de poder consultar altres servidors HTTP
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
```

```
$DMZ_ASSISTPDA_IP --dport 80 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --sport 80 -m state --state ESTABLISHED -j ACCEPT

#
# Es permeten connexions SSH amb el servidor de faltes des de l'exterior
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $WAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 52001 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $WAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 52001 -m state --state ESTABLISHED -j ACCEPT

#
# Secció LAN - Servidor de centre
#

#
# Els usuaris de la LAN han de poder consultar el servidor DNS
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 53 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 53 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p UDP --sport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 53 -j ACCEPT
iptables -A FORWARD -p UDP --dport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 53 -j ACCEPT

#
# Es permeten connexions SSH cap a el servidor de faltes des de la LAN
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 52001 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 52001 -m state --state ESTABLISHED -j ACCEPT

#
# Es permeten connexions HTTP i HTTPS des de la LAN
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE --dport 80 -j
paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -o $LAN_IFACE --sport 80 -m state
--state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE --dport 443 -j
paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -o $LAN_IFACE --sport 443 -m state
--state ESTABLISHED -j ACCEPT

#
# Es permeten consultes del correu de la xtec des de la LAN
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE --dport 465 -j
paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -o $LAN_IFACE --sport 465 -m state
--state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE --dport 587 -j
```

```
paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -o $LAN_IFACE --sport 587 -m state
--state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE --dport 995 -j
paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -o $LAN_IFACE --sport 995 -m state
--state ESTABLISHED -j ACCEPT

#
# Es permeten consultes al servidor TOMCAT des de la LAN
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 8443 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 8443 -m state --state ESTABLISHED -j ACCEPT

#
# Es permeten connexions SSH al servidor de centre des de l'exterior
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $WAN_IFACE -o $LAN_IFACE -d
$LAN_S207_IP --dport 50207 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $LAN_IFACE -o $WAN_IFACE -s
$LAN_S207_IP --sport 50207 -m state --state ESTABLISHED -j ACCEPT

#
# Bacula ha de poder consultar el port 9102 del client
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -d
$DMZ_ASSISTPDA_IP --dport 9102 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -s
$DMZ_ASSISTPDA_IP --sport 9102 -m state --state ESTABLISHED -j ACCEPT

#
# Els ports 9101, 9103 del servidor de centre han de ser accessibles pel client
Bacula
#

iptables -A FORWARD -p TCP --sport 1024:65535 -i $DMZ_IFACE -o $LAN_IFACE -d
$LAN_S207_IP --dport 9101:9103 -j paquets_tcp_permesos
iptables -A FORWARD -p TCP --dport 1024:65535 -i $LAN_IFACE -o $DMZ_IFACE -s
$LAN_S207_IP --sport 9101:9103 -m state --state ESTABLISHED -j ACCEPT
```