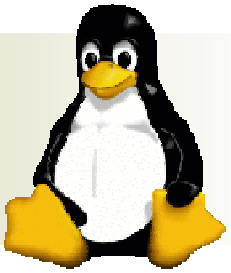
UNIVERSITAT OBERTA DE CATALUNYA
Enginyeria Tècnica en Informàtica de Sistemes

Treball Final de Carrera
Plataforma GNU/Linux
Migració de servidors Windows a Linux



Alumne: Kilian Chouza Fernández
kilian arroba chouza punto com
Dirigit per: Ermengol Bota
Data: Primer semestre de 2004

Índex

Objectius (1/2)

El principal objectiu d'aquest treball és el de realitzar una **guia orientada a** administradors d'entorns de servidors basats en Microsoft Windows per tal de **facilitar la migració** d'aquests **a un entorn GNU/Linux**. La migració està basada en un cas real, els requisits bàsics del qual són:

- Reducció màxima dels costos del programari.
- Augment de l'estabilitat.
- Augment del rendiment.
- Augment de la seguretat.
- No perdre cap funcionalitat.
- Màxima transparència pels usuaris del servidor: no han de notar cap efecte negatiu amb la migració.

Per tant, la selecció de les diferents solucions possibles s'ha fet tenint presents aquests requisits.

Objectius (2/2)

S'explicarà la instal·lació i configuració del següent:

- Linux.
- Servidor DHCP.
- Emulació d'un servidor PDC per tal de mantenir el domini de *Microsoft* existent.
- Servidor de correu electrònic amb filtratge de virus i correu no sol·licitat.
- Servidor LDAP que unificarà les bases de dades d'usuaris, contrasenyes i comptes de correu del servidor de domini i del servidor de correu electrònic en una única ubicació
- Servidor HTTP amb PHP i un *Sistema Gestor de Bases de Dades Relacionals.*
- Sistema de còpies de seguretat automatitzat.
- Monitoratge del maquinari del servidor.

Linux i DHCP (1/2)

- L'**elecció de la distribució de Linux** utilitzada no és una tasca fàcil per la gran quantitat que n'hi ha. S'ha seleccionat *Debian* ja que és una de les més esteses i amb bona reputació, i per tant, amb una comunitat d'usuaris més gran i més activa (amb fòrums, *chats*, planes web, etc.).

- S'ha escollit el **sistema de fitxers** *ReiserFS* per ser ràpid, estable i estar suportat per *Debian* durant la instal·lació d'aquest.

- S'ha fet una **divisió del disc dur en** un gran nombre de **particions** ja que això permet:
  - Aïllar i disminuir pèrdues de dades.
  - Limitar el creixement del volum de dades.
  - Augmentar l'eficiència de l'ús de l'espai.
  - Facilitar les còpies de seguretat del sistema.
  - Reduir la fragmentació.

Linux i DHCP (2/2)

- **Desactivació dels *dimonis*, serveis i mòduls innecessaris** per tal de disminuir la possibilitat que tinguin vulnerabilitats i el consum de recursos (memòria i processador)

- **Configuració de les interfícies de xarxa**

- Instal·lació i configuració del **servidor DHCP,** que permet la configuració automàtica i centralitzada d'alguns paràmetres per tots els ordinadors de la xarxa. Els paràmetres que s'han configurat han estat:
  - Adreça IP i màscara de xarxa.
  - Adreça de l'enrutador predeterminat.
  - Adreça del servidor DNS.
  - Adreça del servidor WINS.

LDAP (1/2)

- **LDAP és un protocol estandarditzat d'accés a directoris**. Un directori és semblant a una base de dades, però està especialment optimitzat per realitzar consultes i cerques.

- En l'actualitat els directoris s'utilitzen com a ubicació centralitzada per emmagatzemar dades importants a les empreses. **En aquesta migració s'ha utilitzat per emmagatzemar tots els usuaris, contrasenyes i comptes de correu**.

- **El programari utilitzat ha sigut *OpenLDAP*** que incorpora tant el servei de directori (el que vindria a ser la base de dades), com un dimoni que s'encarrega de rebre aquelles peticions amb protocol LDAP.

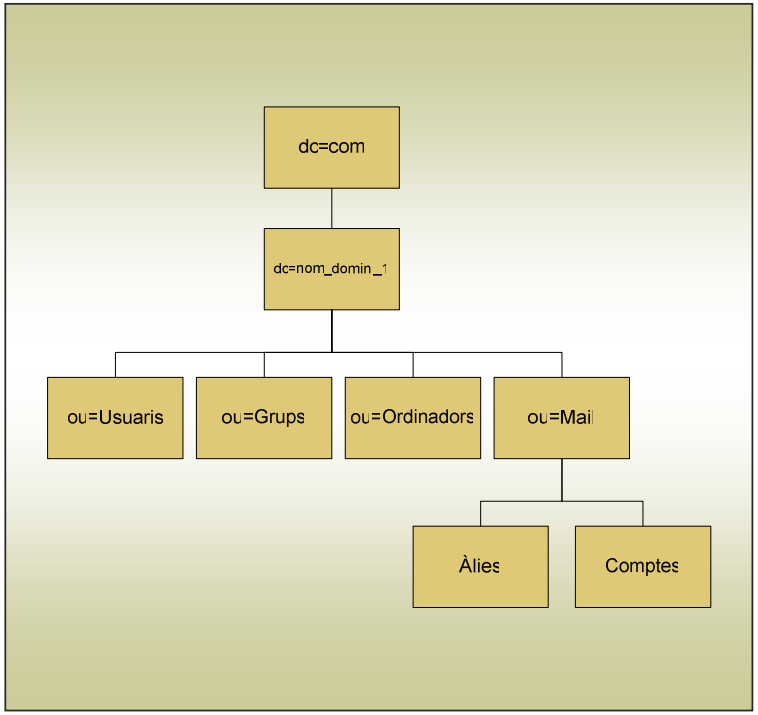
- Per tal d'augmentar la seguretat de les consultes que es fan al directori des d'altres màquines, **s'han habilitat les comunicacions SSL amb *OpenLDAP***. Per fer-ho ha calgut recompilar-lo amb les opcions pertinents.

LDAP (2/2)

La majoria del programari de *Linux* que requereix fer consultes d'usuaris, contrasenyes, grups d'usuaris, etc. fa ús de dues llibreries destinades a aquest fi **NSS** (*Name Service Switch*) i **PAM** (*Pluggable Authentication Modules*)

Existeixen dos afegits per NSS i PAM, anomenats `libnss-ldap` i `libpam-ldap`, per a que **llencin les seves consultes contra un servidor LDAP**.

S'han compilat amb suport per a comunicacions amb el protocol SSL, i s'han configurat per a que facin les consultes adequades per l'estructura de directori que s'ha implementat (veure el diagrama de la dreta)



Domini (1/2)

Autenticació centralitzada

Es vol simular un domini de *Microsoft Windows*, que actualment està compost d'un sol servidor PDC. Un PDC és un ordinador on s'allotgen els comptes d'usuari de tot el domini. Totes les autenticacions de tots els ordinadors del domini es fan contra aquest servidor.

- Per realitzar l'emulació d'un PDC s'ha instal·lat el programari *Samba*.
- ***Samba* s'ha configurat per tal d'obtenir del servidor LDAP la informació** de:
  - Usuaris.
  - Contrasenyes.
  - Grups d'usuaris.
  - Comptes de les màquines.
- Per tal de simplificar la manipulació de la informació del directori LDAP, s'han instal·lat unes utilitats anomenades *smbldap-tools*.

Domini (2/2)

Recursos compartits

Samba també permet simular **recursos compartits** als quals poden accedir els usuaris des de les seves estacions de treball amb *Windows*.

Samba estableix certs **permisos per a cada recurs**, basant-se bàsicament en:

- Els del sistema de fitxers de *Linux.* Sempre que ha estat possible s'ha fet servir aquest mètode.
- Els que s'estableixen al fitxer de configuració de *Samba*, que prevalen sobre els anteriors.

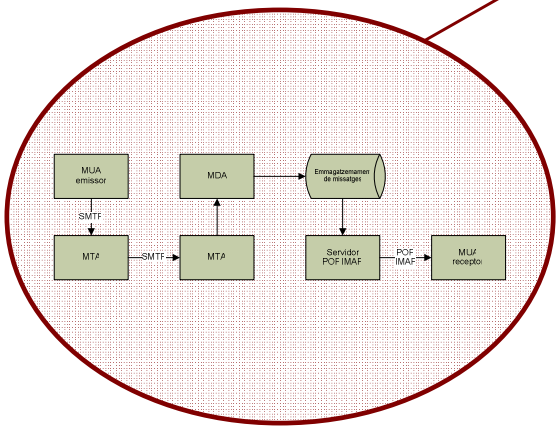
Servidor d'impressió

Un altre requisit és el de permetre a les màquines clients la **impressió amb una impressora connectada al servidor**. Hi ha diferents possibilitats de fer-ho, però s'ha escollit la més semblant a la que hi ha ara, consistent en que el servidor només faci de "passarel·la" entre la impressora i els clients. **Tot el processament dels treballs recau en els clients**.

Correu Electrònic (1/4)

Resum del flux d'un missatge

Un missatge és enviat per un emissor (MUA). El missatge passa per alguns MTA, fins que, finalment es rebut pel servidor MTA que allotja el compte de correu del destinatari. Posteriorment el MDA s'encarrega d'emmagatzemar el missatge. El destinatari, mitjançant el seu MUA, obté el missatge d'un servidor POP/IMAP que té accés als missatges emmagatzemats. Veure el següent esquema.



S'implementarà tota aquesta part; és a dir, l'enviament i recepció de missatges per a comptes de correu d'un o més dominis

Correu Electrònic (2/4)

MTA/MDA

Entre la gran varietat de solucions disponibles, **s'ha escollit *Postfix***. Pel que s'ha llegit sembla ser un dels més equilibrats (segur, fiable, eficient, fàcil de configurar, compatible amb LDAP, modular, llicència GPL...).

S'ha instal·lat una versió precompilada amb suport per a SSL i també per a les llibreries *Cyrus SASL.* Aquestes són utilitzades per poder implementar *SMTP Auth* (un mètode que només permet l'enviament de missatges electrònics a usuaris autenticats). Però, s'han trobat problemes d'incompatibilitat entre versions que, per falta de temps, han impedit implementar-lo.

Servidor POP3

Per a que els clients puguin rebre els missatges **s'ha instal·lat *Courier-POP3***. S'ha escollit aquest programari perquè usa el mateix format (*mailbox*) pels missatges que *Postfix* i que *Courier-IMAP* i *SquirrelMail* (correu web), que es preveuen instal·lar en un futur.

Correu Electrònic (3/4)

Seguretat

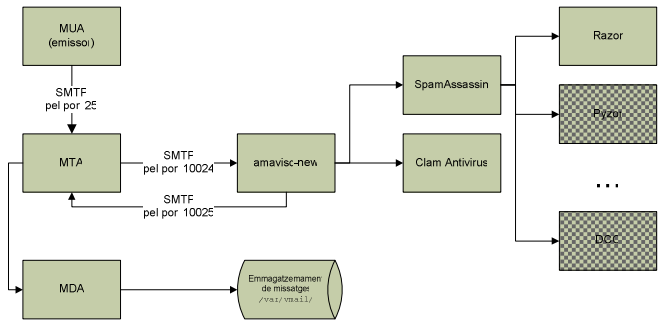
Les mesures de seguretat que s'han pres pel correu electrònic han estat:

- **Evitar ser *Open Relay*** permetent l'enviament de correu només a:
  - Màquines de la xarxa local.
  - Aquelles que s'autentiquin amb *SMTP Auth* o *POP-Before-SMTP.*

- ***Antispam* i *Antivirus***
  - *Postfix* filtra aquells missatges que:
    - No segueixen algunes de les regles bàsiques del protocol SMTP.
    - Aquells emissors que estan a determinades llistes negres (RBL).
  - La utilitat *amavisd-new* processa els missatges i els comprova amb:
    - *SpamAssassin* per tal d'identificar possibles missatges de *spam.* Alhora, *SpamAssassin* pot fer crides a altres utilitats per identificar aquest tipus de missatges, com per exemple a *Razor.*
    - Els *antivirus* instal·lats al sistema per tal d'evitar la propagació de virus per la xarxa local. S'ha instal·lat l'antivirus *Clam Antivirus.*

Correu Electrònic (4/4)

El flux que segueix un missatge al nostre sistema és el següent:



Sistema de còpies de seguretat

Existeixen multitud d'alternatives diferents per a la realització de còpies de seguretat. Per què sigui una solució semblant a l'actual es requereix:

- La **sincronització** de dos directoris fent que tots dos siguin exactament iguals. Amb l'excepció que al destí **es guarden còpies** (o versions) **dels arxius que s'esborren/modifiquen a l'origen**.
  - S'ha escollit la utilitat *rdiff-backup.*
  - S'ha desenvolupat un *script* per automatizar aquesta tasca.

- **Còpia de seguretat del sistema operatiu i les aplicacions**: bolcat exacte de les particions amb el sistema operatiu i el programari per poder restaurar-lo en cas d'alguna fallada greu (de programari o maquinari).
  - S'ha fet servir *PartImage* juntament amb el CD d'arrencada *SysRescueCD*.
  - També s'ha creat un *script* per automatitzar el procés.

Com a suport d'emmagatzematge per tots dos es fa servir un disc dur USB.

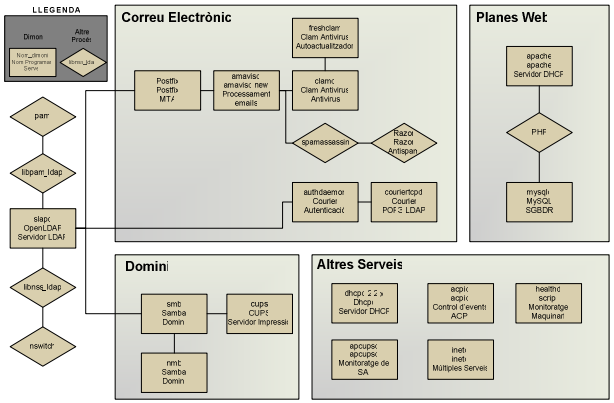
Monitoratge del maquinari

El monitoratge del voltatge, la temperatura i la velocitat de rotació dels ventiladors del servidor és crucial ja que, si els seus valors no es troben dins d'un determinat interval, es pot malmetre seriosament el maquinari de l'ordinador. Per això, s'ha previst:

- **Realització d'apagades controlades del servidor en cas de fallades del corrent elèctric** i esgotament de les bateries del SAI. Per dur a terme aquesta tasca s'ha instal·lat el *dimoni apcupsd*.

- **Monitoratge continu de voltatges, la temperatures i velocitats de rotació dels ventiladors** amb un *script* que s'ha desenvolupat (anomenat *healthd*), i que actua com un *dimoni* que, quan detecta un valor fora d'uns determinats intervals establerts, apaga immediatament l'ordinador.

Esquema de serveis i *dimonis*



Conclusions i resultats finals

- Després de fer la migració, els usuaris no han notat cap canvi significatiu entre la solució anterior i la solució GNU/Linux. Per la qual cosa, l'objectiu de la transparència i de no perdre cap funcionalitat s'han assolit.

- Tot el programari utilitzat ha estat programari lliure i gratuït, per tant s'ha assolit la reducció màxima dels costos del programari.

- El rendiment en general es manté igual, millorant en alguns aspectes. Per exemple, el rendiment de la xarxa ha augmentat considerablement i la còpia de fitxers grans a o des del servidor ja no col·lapsa tot el sistema.

- S'ha trobat *Linux* més estable, més ràpid i més transparent, (totes les opcions d'un programari estan a l'abast de l'usuari). Aquest últim punt, fa que es tingui més control sobre el que es fa, però té l'inconvenient que és més difícil d'administrar.

Línies futures

La gran amplitud de tecnologies que cobreix aquest treball fa impossible poder aprofundir-ne més. A continuació es comenten algunes possibles línies futures de treball:

- Implementar LVM per una major flexibilitat en el particionament dels discs.
- **Domini**: usar un servidor DNS enlloc d'un WINS, polítiques del sistema i d'altres característiques avançades.
- **Correu electrònic**: fer funcionar *SMTP Auth*, accés a les bústies amb el protocol IMAP, instal·lar una solució de correu web, utilització de SSL, provar altres eines *antispam, etc.*
- **Còpies de seguretat**: explicar altres mètodes, modificar *SysRescueCD* per automatitzar completament el procés, etc.
- **Altres serveis interessants**: FTP (amb LDAP i SSL), *proxy*, tallafocs, DNS, implementació d'una VPN, etc.
- **Altres aspectes**: cercar eines per facilitar l'administració del sistema, explicar la programació de tasques, la gestió dels registres d'activitat (*logs*), etc.