

TFM. Disseny de solucions telemàtiques d'aula basades en programari lliure.



Josep Girbés Ribes



Administració de xarxes i de sistemes operatius

Consultor: Miguel Martín Mateo
Tutor extern: Sergi Tur Badenas

Índex

1. Introducció
2. Objectius
3. Anàlisi de requeriments i estudi de viabilitat
 - 3.1 Necessitats i requeriments del client
 - 3.2 Anàlisi de la situació actual
 - 3.3 Definició de requeriments
 - 3.4 Estudi d'alternatives de solució
 - 3.5 Valoració i elecció de les possibles solucions
 - 3.6 Recursos econòmics i recursos humans
4. Disseny de la solució
5. Implementació
 - 5.1 Arquitectura servidor
 - 5.2 LDAP
 - 5.3 FusionDirectory
 - 5.4 DHCP
 - 5.5 DNS
 - 5.6 Samba
 - 5.7 Quotes
 - 5.8 Regles tallafocs d'aula
 - 5.9 FOG
6. Resultats
7. Valoració econòmica
8. Conclusions
9. Webgrafia

1. Introducció

- **Projecte Màster de Programari Lliure en la especialitat administració de xarxes i de sistemes operatius pel tal d'aportar solucions telemàtiques basades en programari lliure que cobreixen determinades necessitats mostrades per part de la coordinació d'informàtica de l'Institut de l'Ebre en relació a les aules d'informàtica i que podrien ser esteses a altres aules del centre.**
- **L'institut de l'Ebre:**
 - Centre de formació professional ubicat a Tortosa (Catalunya).
 - 1300 alumnes que cursen CFGM i CFGS de les famílies: Sanitat, Electricitat-Electrònica, Edificació i Obra Civil, Fabricació Mecànica i manteniment, Administrativa, Comerç, Serveis a la Comunitat i Informàtica.
 - 3 cicles d'informàtica: 1 CFGM SMX i 2 CFGS ASIX i DAM. 100 ordinadors repartits entre 4 aules i el departament d'informàtica.

2. Objectius

- Gran nombre d'ordinadors de l'aulari de la família d'informàtica fa necessari implementar determinades solucions d'aula basades en programari lliure per facilitar el seu manteniment, configuració, etc...
- Cal una eina que permeta fer un ús eficient de l'amplada de banda de la xarxa amb un filtrat personalitzat a nivell d'aula d'un determinat tipus de tràfic mitjançant regles de tallafocs implementades directament sobre el router principal.
- Cal muntar un entorn de proves per tal d'implementar solucions còmodes per gestionar i administrar de forma centralitzada. No es tracta d'una migració però els resultats obtinguts poden servir per donat el moment, tenir una opció ben estudiada de migració.
- Es farà ús de Virtualbox, per virtualitzar el sistema operatiu Ubuntu en diferents màquines: servidor *Servidorproves* (DHCP, DNS, LDAP, SAMBA, QUOTES), servidor *Webminfog* (Regles tallafocs + Fog), client *Ubuntu alumne*, client *Ubuntu professor* on es faran les proves de comprovació del correcte funcionament de les solucions implementades.

3 Anàlisis de requeriments i estudi de viabilitat

3.1 Necessitats i requeriments del client

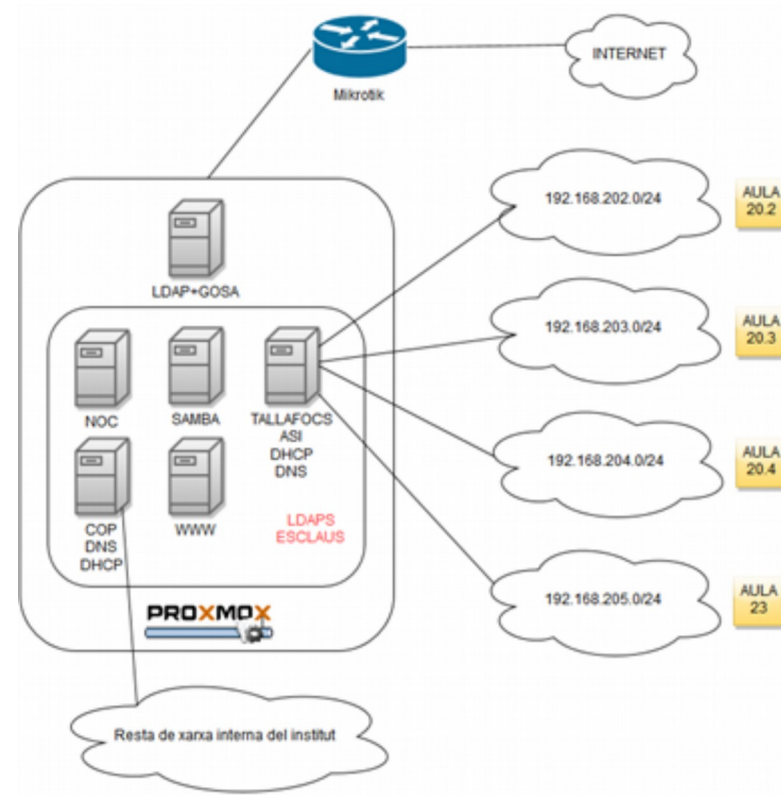
- Coordinació d'Informàtica es l'encarregada última de tot l'equipament informàtic de l'institut.
- Hi ha funcions delegades al Departament d'informàtica per tal de llevar-ne càrrega en la gestió i administració de les aules d'informàtica
- Aquest projecte intenta implementar una sèrie de solucions informàtiques per facilitar-ne aquesta tasca i per donar resposta a algunes demandes del professorat.
- A l'institut ja tenen una infraestructura muntada amb diferents servidors virtualitzats. Aquests no es poden tocar per fer proves perquè això afectaria al dia a dia de l'institut. Per tant cal muntar un entorn de proves similar apart.

3 Anàlisi de requeriments i estudi de viabilitat

3.2 Anàlisi de la situació actual

Resum infraestructura de CPD:

- Ubicat al departament de Coordinació d'informàtica.
- Router Mikrotik 1100 amb línia de fibra de 80 Mbps simètrics
- Servidor amb processador de 8 nuclis i 32 GB de RAM amb PROXMOX.
- Servidors principals virtualitzats als PROXMOX son Ubuntu 12.04 LTS:
 - Gosa + LDAP: Servidor principal de LDAP i GOSA
 - COP: Servidor de comunicacions principal (DHCP-DNS PRIMARI)
 - NS2: Servidor DNS secundari
 - Samba: Servidor principal Samba
 - WWW: Servidor web
 - TallafocsAsi: Servidor comunicacions aules d'informàtica.



3 Anàlisis de requeriments i estudi de viabilitat

3.3 Definició de requeriments

Solucions a muntar en entorn de proves basades en programari lliure sobre sistema operatiu GNU/Linux:

- Gestió de usuaris
- Gestió de quotes.
- Gestió de recursos compartits
- DHCP
- DNS
- Eina de clonatge d'equips i inventariat d'equips
- Implementació de regles tallafocs a nivell d'aula per filtrar determinats ports.

3 Anàlisi de requeriments i estudi de viabilitat

3.4 Estudi d'alternatives de solució

- Conveniència d'us d'eina de virtualització
- Existeix dos solucions basades en programari lliure (llicència GPLv2):
 - Proxmox VE: demana maquinari en exclusiu per a ell, ha d'estar instal·lat sobre maquina real (Hipervisor tipus 1). Accedir via web de forma remota. Ens obliga a tenir una màquina virtualitzar i una segona maquina remota per tal de poder gestionar-la
 - Virtualbox: Hipervisor tipus 2. Amb la qual cosa en un mateix maquinari amb uns requeriments mínims pots virtualitzar i configurar les màquines que s'estan virtualitzant.

3 Anàlisi de requeriments i estudi de viabilitat

3.5 Valoració i elecció de les possibles solucions

- Entorn de proves triat Virtualbox. Demana menys prestacions mínimes i maquinari per implementar entorn.
- Aplicacions triades:
 - Integració Ldap, DHCP, DNS, Quota amb FusionDirectory.
 - Gestió de usuaris: Openldap.
 - Gestió de recursos compartits: SAMBA.
 - Servidor DHCP: ISC (Internet System Consortium) DHCP (Dynamic Host Configuration Protocol) Server.
 - Servidor DNS: Bind9.
 - Gestió de quotes: Quota.
 - Eina de clonatge d'equips i inventariat d'equips: FOG
 - Implementació de regles tallafocs a nivell d'aula per filtrar determinats ports: comandes SSH a router Mikrotik + Webmin.

3 Anàlisi de requeriments i estudi de viabilitat

3.6 Recursos econòmics i recursos humans

- Programari: Al emprar programari lliure tindrem cost zero. Cost en llicències de programari privatiu:

Llicències de programari privatiu mínimes necessàries				
Concepte	Funcionalitat	Quantitat	Preu (€)	Total (€)
Windows 2012 Server R2	Director actiu, DHCP, DNS, compartició de recursos, quotes	1	1.097	1.097
Network Inventory Advisor	Inventariat 100 equips	1	199	199
VMware Workstation 12 pro	Virtualització entorn proves	1	251,95	251,95
Acronis Snap Deploy 5	Clonació de equips	1	98	98
				1.645,95

- Recursos humans: En cas d'haver de contractar a un tècnic el cost orientatiu seria:

Recursos humans				
Concepte	Funcionalitat	Quantitat	Preu (€/hora)	Total (€)
Administrador de sistemes GNU/LINUX	Instal·lació, configuració i prova de tot el programari necessari per assolir els objectius del projecte	47	40	1960

4. Disseny de la solució

- **VirtualBox com a eina de virtualització.**
- **Possibles interfícies gràfiques per gestionar els serveis: Apache Directory, Webmin i FusionDirectory. Es tria FusionDirectory perquè:**
 - Es un fork de GOSA (GOnicus System Administration),
 - Neix per les discrepàncies d'una comunitat de desenvolupadors de GOSA amb Gonicus que es la empresa que desenvolupa GOSA
 - La comunitat de FusionDirectory pretén impulsar aquest projecte d'una manera més oberta i oferir una major documentació.
 - Conté plugins que permet la administració de serveis centralitzada entre d'altres dels serveis: DHCP, DNS, SAMBA, Quota, SSH, Systems(per gestionar servidors des de FusionDirectory).
- **FOG com a eina de clonatge i inventariat d'equips.**
- **Comandes SSH a router Mikrotik + Webmin com a solució web que permeta mitjançant regles bàsiques de filtrat.**

5. implementació

5.1 Arquitectura servidor

- **Servidorproves:**

- S.O. GNU/Linux Ubuntu Server 14.04 64 bits.
- 60 GB disc dur.
- 2 GB de RAM.
- 5 targetes de xarxa virtuals.

- **Webminfog:**

- S.O. GNU/Linux Ubuntu Server 14.04 64 bits.
- 60 GB disc dur.
- 2 GB de RAM.
- 1 targeta de xarxa virtual.

5. implementació

5.2. LDAP + FusionDirectory

- Fem us de Openldap i el plugin Ldap de FusionDirectory.
- FusionDirectory eina amb llicència GPL v.2 i interfície web modular que facilita la gestió del directori LDAP amb plugins per gestionar: DHCP, DNS, SAMBA, Quotes...



5. implementació

5.3. DHCP

- Fem us de ISC DHCP i el plugin DHCP de FusionDirectory. DHCP treballarà junt al LDAP.
- Haurem de crear 4 àmbits amb rangs: 192.168.20X.3-192.168.20X.254, on la X correspon al número d'aula (1,2,3 i 4).
- Assignació informació DHCP del client a l'aula 204 (esquerra) i la informació que publica el servidor a la subxarxa 204 (dreta).

```
alumne-pc alumne # dhclient -v eth0
Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:da:69:28
Sending on   LPF/eth0/08:00:27:da:69:28
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 (xid=0x375c454c)
DHCPPREREQUEST of 192.168.204.3 on eth0 to 255.255.255.255 port 67 (xid=0x375c454c)
DHCPOFFER of 192.168.204.3 from 192.168.204.2
DHCPACK of 192.168.204.3 from 192.168.204.2
bound to 192.168.204.3 -- renewal in 228 seconds.
```

```
lease 192.168.204.3 {
  starts 6 2015/10/31 20:41:15;
  ends 6 2015/10/31 20:51:15;
  cltt 6 2015/10/31 20:41:15;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:da:69:28;
  client-hostname "alumne-pc";
}
```

5. implementació

5.5 DNS

- Fem us de Bind9 i el plugin Argonaut-Idap2zone de FusionDirectory. DNS treballarà junt al LDAP.
- Haurem de crear 4 zones: aula201, aula202, aula203 i aula204.
- Assignació informació DNS del client a l'aula 204 (esquerra) i la informació que publica el servidor a la subxarxa 204 (dreta).

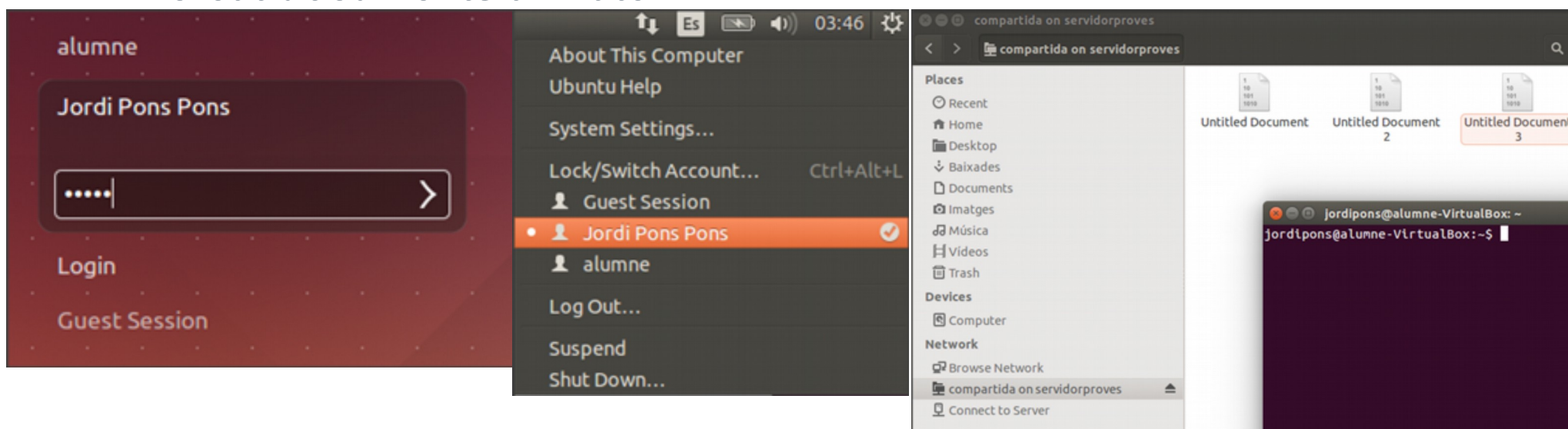
```
alumne@alumne-VirtualBox:~$ nmcli dev list iface eth0 | tail -n 15
IP4.ADDRESS[1]:                ip = 192.168.204.6/24, gw = 192.168.204.1
IP4.DNS[1]:                    192.168.204.2
IP4.DNS[2]:                    8.8.8.8
IP4.DOMAIN[1]:                 iesebre.com
DHCP4.OPTION[1]:              domain_name = iesebre.com
DHCP4.OPTION[2]:              expiry = 1447561977
DHCP4.OPTION[3]:              broadcast_address = 192.168.204.255
DHCP4.OPTION[4]:              dhcp_message_type = 5
DHCP4.OPTION[5]:              dhcp_lease_time = 600
DHCP4.OPTION[6]:              ip_address = 192.168.204.6
DHCP4.OPTION[7]:              routers = 192.168.204.1
DHCP4.OPTION[8]:              subnet_mask = 255.255.255.0
DHCP4.OPTION[9]:              domain_name_servers = 192.168.204.2 8.8.8.8
DHCP4.OPTION[10]:             network_number = 192.168.204.0
DHCP4.OPTION[11]:             dhcp_server identifier = 192.168.204.2
```

```
lease {
  interface "eth4";
  fixed-address 192.168.204.5;
  option subnet-mask 255.255.255.0;
  option routers 192.168.204.1;
  option dhcp-lease-time 600;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.204.2,8.8.8.8;
  option dhcp-server-identifier 192.168.204.2;
  option broadcast-address 192.168.204.255;
  option domain-name "iesebre.com";
  renew 0 2015/11/15 04:10:58;
  rebind 0 2015/11/15 04:14:53;
  expire 0 2015/11/15 04:16:08;
```

5. implementació

5.6 Samba

- Es combina Samba amb el plugin per a FusionDirectory amb integració amb LDAP.
- Hem agregat un usuari i un equip a Samba.
- Hem iniciat sessió amb l'usuari a l'equip, creat un recurs compartit i creat documents al mateix.



5. implementació

5.7 Quotes

- El plugin de FusionDirectory admet la configuració de quotes basades en Ldap.
- Compartim carpetes, ens crea un dispositiu i assignem quota a usuaris de Ldap

The image displays three screenshots from the FusionDirectory web interface. The top-left screenshot shows the 'Shares' configuration page with a table listing a share named 'compartida' of type 'CIFS' at path '/srv/samba/compartida/'. Below the table are input fields for 'Nom*' (compartidaquota), 'Type*' (CIFS), 'Description', 'Codepage*' (UTF-8), 'Path / Volume*' (/srv/samba/compartidaquota/), and 'Option'. The top-right screenshot shows the 'Shares' configuration page with a table listing a share named '/srv/samba/compartidaquota/' of type '(compartidaquota by CIFS)' with a 'Block size*' of 4096. Below the table are input fields for 'Device*', 'Comment' (carpeta amb quota), and 'Add'. The bottom screenshot shows the 'Quota information' page with a table listing a quota for '/srv/samba/compartidaquota/ - carpeta amb quota' with a current size of 19MiB, a limit of 20MiB, and a user 'servidorproves'. The table has columns for path, current size, limit, soft limit, and user. The bottom-right part of the screenshot shows the 'LDAP message support' and 'Quota warning message' configuration sections.

- La icona  fa referència a que s'han aplicat quotes al usuari

The image shows a user interface with a list of users. The first user is 'Pons Pons' with a quota icon. The second user is 'Jordi' with a quota icon. The third user is 'jordipons' with a quota icon. The interface also shows a search bar and a list of icons for various services.

5. implementació

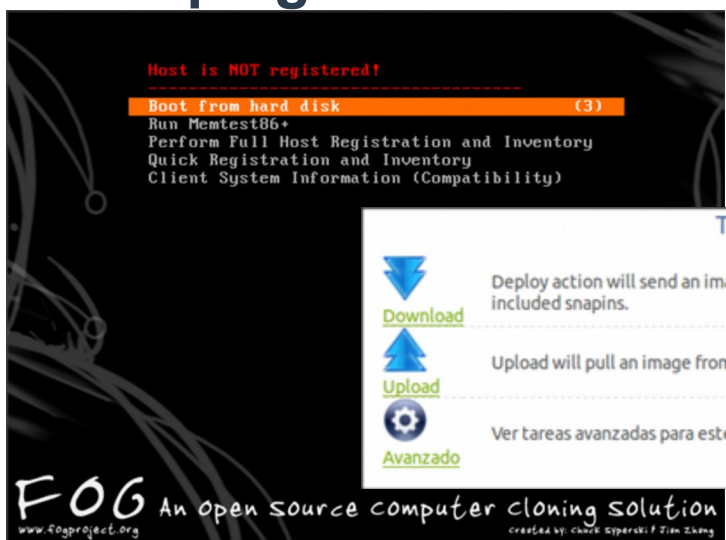
5.8 Regles tallafocs d'aula

- MV amb Mikrotik RouterOS 6.0
- Serà porta d'enllaç de totes les aules
- Part de la configuració feta per terminal altra per Gui Winbox.
- 7 targetes virtuals (4 per aules, 1 Lan, 1 Wan, 1 Només host)
- Regles de tallafocs:
 - Dos llistes, una per a IPs de servidors un altra per a PCs de profe perquè no tinguin cap restricció
 - S'executaran scripts amb ordres ssh amb regles al router amb clau DSA, s'analitzarà port i aula
 - El servidor WebminFog es l'encarregat d'enviar les ordres al router. Amb Webmin Custom Commands podrem configurar el router des de qualsevol aula.
 - Amb tres scripts crearem tres opcions:
 - Afegir filtre port aula: Demanarà paràmetre port i aula.
 - Eliminar filtre port aula: Demanarà paràmetre port i aula.
 - Mostrar totes regles filtrat

5. implementació

5.9 FOG

- Implementat en servidor WebminFog
- Farà us del DHCP de servidor Servidorproves, on configurarem a FusionDirectory els PXE services next-server 192.168.100.3 i filename.
- Registrarem equips, inventariarem, farem images i la desplegarem.



```
Partclone
Partclone v0.2.69 http://partclone.org
Starting to clone device (/dev/sda1) to image (/tmp/pigz1)
Reading Super Block
Calculating bitmap... Please wait... done!
File system: EXTFS
Device size: 10.2 GB = 2490112 Blocks
Space in use: 4.1 GB = 996809 Blocks
Free Space: 6.1 GB = 1493303 Blocks
Block size: 4096 Byte

Elapsed: 00:00:51 Remaining: 00:20:34 Rate: 190.60MB/min
Current Block: 60160 Total Block: 2490112

Data Block Process: 3.97%
Total Block Process: 2.42%
```

6. Resultats

- **El resultat del projecte proposat han estat assolits i amb resultat molt satisfactori.**
- **Ha estat vertaderament complicat trobar documentació per tal de desenvolupar determinats passos de la configuració.**
- **Aquesta memòria, és una eina fonamental per implementar Fusi3nDirectory a qualsevol organitzaci3, ja no hi ha cap manual que tracte aquesta eina amb tanta profunditat.**

7. Valoració econòmica

Com es va tractar al punt de la memòria 2.5 Recursos econòmics i recursos humans:

- Ús programari 100% lliure, fa que tinga un cost zero a nivell de llicències.
- A nivell maquinari, cost zero perquè es reutilitza maquinari ja existent
- Ús d'una connexió a internet proporcionada pel propi institut.
- A nivell recursos humans no té cap cost al formar part aquesta implantació de solucions del projecte final de màster .

8. Conclusions

- Ha estat molt interessant desenvolupar aquest projecte perquè m'ha proporcionat una idea molt aproximada del funcionament intern de la xarxa i sistemes del institut. Veient les dificultats a les que s'enfronta dia a dia el personal al càrrec.
- En explotació cal reduir al mínim tasques de configuració perquè afecten en gran mesura als sistemes i als usuaris.
- Es convenient trobar una sèrie de solucions que permeten gestionar els serveis bàsics d'una organització: DHCP, DNS, LDAP, Samba, etc amb la major comoditat possible i poder destinar els recursos humans a la atenció al usuari, el manteniment d'equips i programari de gestió d'alumnat.
- Les eines de control d'accés a serveis de xarxa amb funcionalitats de tallafocs facilitaràn el dia a dia al professorat per tal d'impedir el accés de xarxa a determinats serveis en determinats moments.
- L'eina de clonatge permetrà la ràpida posada en funcionament dels equips d'alumnes amb un complet procés d'inventariat que la eina permet.
- En resum, ha estat un projecte enriquidor a nivell personal i complexe però amb molt bons resultats a nivell tècnic.

9. Webgrafia

Web Windows 2012 Server R2
Web VMware Workstation 12 pro
Web Network Inventory Advisor
Web Acronis Snap Deploy 5
Web projecte Proxmox
Web projecte Fusiondirectory
Web projecte Virtualbox
Web projecte Openldap
Web projecte isc dhcp
Web projecte bind9
Web projecte fogproject
Web projecte samba
Web projecte ubuntu
Web projecte Webmin
Web Mikrotik

Aquesta obra està subjecta a una llicència



<http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca>

Gràcies per l'atenció prestada

Disseny de solucions telemàtiques d'aula basades en programari lliure.