Infraestructura d'empresa amb programari lliure

Autor: Vicente Martí Alberola

Consultor: Jose Manuel Castillo Pedrosa

Data Lliurament: 8 de juny de 2016

FITXA DEL PROJECTE FINAL

Títol del projecte:	*Infraestructura d'empresa amb programari lliure*
Nom de l'autor:	*Vicente Martí Alberola*
Nom del consultor:	*Jose Manuel Castillo Pedrosa*
Data de lliurament (mm/aaaa):	*06/2016*
Àrea del Projecte Final:	*Administració de xarxes i sistemes operatius*
Titulació:	*Enginyeria Informàtica (2^{n} cicle)*

Resum del Projecte :

Tot i que avui dia és més fàcil trobar alguna empresa que confie en aquestes solucions, el programari lliure, encara es vist però molts com programari gratuït i de baixa qualitat creat per aficionats a la informàtica i no realment per professionals. Per a gran part de directius d'empreses xicotetes, mitjanes i grans, el programari lliure no és una opció. Aquest estudi no vol aprofundir en els avantatges del programari lliure front el privatiu.

Atés la seua provada qualitat i suficiència per a ser la base dels grans serveis a Internet, aquest projecte, pretén donar una alternativa al programari privatiu que normalment s'utilitza a les empreses, be siguen petites, mitjanes o grans. S'ha tractat d'explicar cada una d'aquestes tecnologies així com una solució de programari lliure. A més es detalla com implementar cadascun d'aquests serveis.

Hipervisor de màquines virtuals, l'autenticació d'usuaris, l'assignació dinàmica d'adreces IP, resolució de noms, servei d'impressores compartides, servidor d'arxius , correu electrònic, gestor de contingut, servidor intermediari, servidor de VPN o un servidor d'arxius en núvol són alguns dels serveis estudiats a aquest projecte. De tots ells, es presentarà una solució de programari lliure de qualitat per oferir una alternativa real al programari privatiu

Abstract in English:

Although nowadays it is a easier to find a company that trusts these kind of technologies, free software is still seen by many people as free of charge , low quality software built by amateur developers and not made by IT professionals. For the majority of the senior management in all kind of companies free software is simply not an option. This paper does

not want to go deep into the advantages of free software compared to proprietary software.

Due to its proven quality in order to be the base of many big services in the Internet, this project aims to provide alternatives to the proprietary software usually used at all kind of companies. The objective has been to explain each of these technologies used in companies world wide and a free software alternative to the classic proprietary solutions in the market. Besides details of the implementation of every service will also be provided.

Virtual machines hypervisor, user authentication, dynamic IP addresses assignment, name resolution, print server, file server, email, content manager, proxy server, VPN server or cloud-based file server are some of the services analysed in this project. A free software solution will be provided for each service. A quality solution that will offer a real alternative to proprietary software.

Paraules clau (entre 4 i 8):

programari lliure proxmox postfix linux apache mysql php

Índex de continguts

Índex d'Il·lustracions

1. Introducció

A aquest capítol es fa un breu introducció tant dels objectius i motivacions d'aquest projecte com del mètode de treball i la planificació.

1.1 Context i justificació del Projecte

La majoria de mitjanes empreses conten amb un o més servidors interns que proveeixen diferents serveis al seus usuaris. Els més comuns són la validació d'usuaris en xarxa, un servidor amb recursos compartits com ara arxius o impressores o , a les empreses més grans, un servidor de correu electrònic. A més d'aquests serveis, també sovint trobem d'altres com ara la assignació dinàmica de direccions IP mitjançant DHCP, resolució de noms per DNS o un servidor proxy per filtrar l'accés a Internet.

Tot i que amb les tecnologies de virtualització presents al mercat el cost del maquinari emprat per allotjar aquest serveis ha disminuït, el cost de tindre tots aquests serveis internament a l'empresa comporta un cost molt important atès que la majoria de solucions al mercat tenen un cost per llicencia. A més, aquestes solucions solen ser de codi propietari. Per aquest motiu, normalment les empreses queden lligades a proveïdors de per vida atés que el programari propietari, de vegades, no segueix cap estàndard i no es personalitzable pel personal de l'empresa afegint així un cost important en serveis de manteniment. D'altra banda, una falla en el programari que puga exposar la informació de l'empresa pot tardar més en detectar-se.

En aquest context, i seguint molts dels estàndards que ja segueixen grans proveïdors a Internet, aquest projecte pretén oferir alternatives de programari lliure per a tots aquests serveis que tan útils són per a les empreses. L'objectiu és analitzar les alternatives de programari lliure que poden oferir una solució a les empreses a tots aquests problemes.

1.2 Objectius del Projecte

L'objectiu d'aquest estudi es trobar i implementar alternatives de programar lliure per als principals sistemes que s'utilitzen a una empresa tipus. La primera premissa per a escollir quin programari emprar per a cada servei es que siga de programari lliure. Sempre que es tinga opció, escollirem programari que també siga compatible amb plataformes de programari privatiu com ara Windows o MAC OS. A continuació s'enumeren els sistemes a implementar:

Hypervisor de maquines virtuals: Front altres solucions privatives com ara VMWare ESX o Hyper-V de Microsoft,farem ús de Proxmox. Proxmox és un entorn de virtualització de programari lliure basat en Debian (distribució Linux) i amb un kernel Red Hat Enterprise Linux modificat. Es documentarà les opcions d'alta disponibilitat de Proxmox

Autenticació d'usuaris en xarxa: Al mon del programari privatiu la solució més estesa per a poder autenticar usuaris en xarxa és el Directori Actiu de Microsoft. Com a alternativa trobem OpenLDAP.

Servidor DNS: A les empreses on s'utilitza Directori Actiu com a servei d'autenticació d'usuari, es sol emprar aquest mateix servidor com a servidor DNS intern. En el nostre cas, emprarem el servidor Bind per aquesta tasca. Documentació, anàlisis i implementació de la securització del servidor DNS(atacs coneguts,solucions i eines disponibles per mitigar els atacs)

Servidor DHCP: La manera més còmoda d'assignar direccions IP a tots els clients de la nostra xarxa és fent ús d'un servidor DHCP. Tot i que el nostre entorn no estarà preparat per poder crear diferents àmbits per assignar direccions a maquines en diferents VLANs (xarxes virtuals), es documentarà com fer-ho pas a pas a un servidor DHCP que correrà en una maquina amb una distribució Linux. També es donaran exemples de com assignar sempre la mateixa direcció IP a una màquina basant-se en la seua direcció MAC així com la tècnica de DHCP fingerprinting.

Servidor de fitxers: Per fer compatible la nostra solució amb ordinadors amb Windows, instal·larem un servidor samba. D'aquesta manera, obtindrem un entorn preparat per a qualsevol tipus de necessitat.

Servidor d'impressió: Farem ús de CUPS el qual ens permetrà que les impressores siguen accessibles per clients MAC OS. En aquest cas el combinarem amb samba per a que clients Windows tinguen accés a les nostres impressores.

Servidor de correu: En aquest cas farem ús de Postfix com a MTA. L'acompanyarem de Dovecot com a Local Delivery Agent i tots dos autenticaran contra el servidor LDAP. També s'implementarà un sistema antispam (spamassassin) i antivirus(clamav). L'estudi també inclourà la documentació per a la correcta configuració dels registres DNS necessaris per al bon funcionament del servei.

Servidor web corporativa/Intranet: Per a aquesta funció, emplearem el servidor web Apache i el gestor de continguts Wordpress. L'abast d'aquesta implementació es limitarà a la instal·lació i configuració bàsica tant del servidor web com del gestor de continguts. Queda fora del projecte el disseny de la pàgina web o la documentació de l'ús del gestor de continguts

Servidor de certificats: Instal·lació i configuració d'una entitat certificadora. Es generaran certificats per els serveis web disponibles i certificats d'usuari per a firmar i xifrar el correu.

Servidor cloud de fitxers: Per tal de donar opció a poder accedir als nostres documents des de qualsevol lloc implementarem un servidor Owncloud. També ens servirà com a eina per a fomentar el treball col·laboratiu. Com a punt important d'aquest sistema es farà un estudi detallat de com configurar el servei per a afavorir la escalabilitat del mateix. D'aquesta manera, facilitarem un important increment repentí d'usuaris.

Servidor VPN: Instal·lació i configuració d'OpenVPN per a poder accedir als fitxers emmagatzemats en Owncloud. Es documentarà quines són les millors pràctiques per a accedir a aquest servei

Servidor proxy per a accés a Internet: Instal·lació d'Squid com proxy server per a enrutar tot el trafic web a Internet dels clients de la xarxa.

1.3 Enfocament i mètode seguit

El treball consisteix en analitzar i implementar un entorn de treball professional estàndard només amb eines de programari lliure. Aquest estudi s'ha fet en un entorn de proves i pretén ser un esbos del que seria aquesta implementació en un entorn real.
La implementació es va realitzar creant quantes maquines virtuals foren necessàries per als diferents sistemes. Aquesta tasca es va realitzar instal·lant a un servidor físic un hypervisor de maquines virtuals on es va anar creant màquines per a cada servei estudiat. Per estalviar recursos de

maquinari, algun dels sistemes inclosos a aquest estudi comparteixen maquina virtual. S'especificarà per a quins d'ells es recomanaria un servidor dedicat en un entorn real.

Les especificacions de maquinari del servidor de màquines virtuals on s'han efectuat totes les proves són:

- **CPU:** Intel i5 amb tecnologia VT
- **Memòria RAM:** 16GB
- **Disc dur principal per a l'arranc:** Samsung EVO 840 256GB SSD
- **Disc dur secundari per emmagatzemar màquines virtuals i dades:** Seagate Barracuda 1TB
- **Interfície de xarxa:** Gigabit Ethernet

El programari base emprat per a la realització d'aquest projecte es llista a continuació:

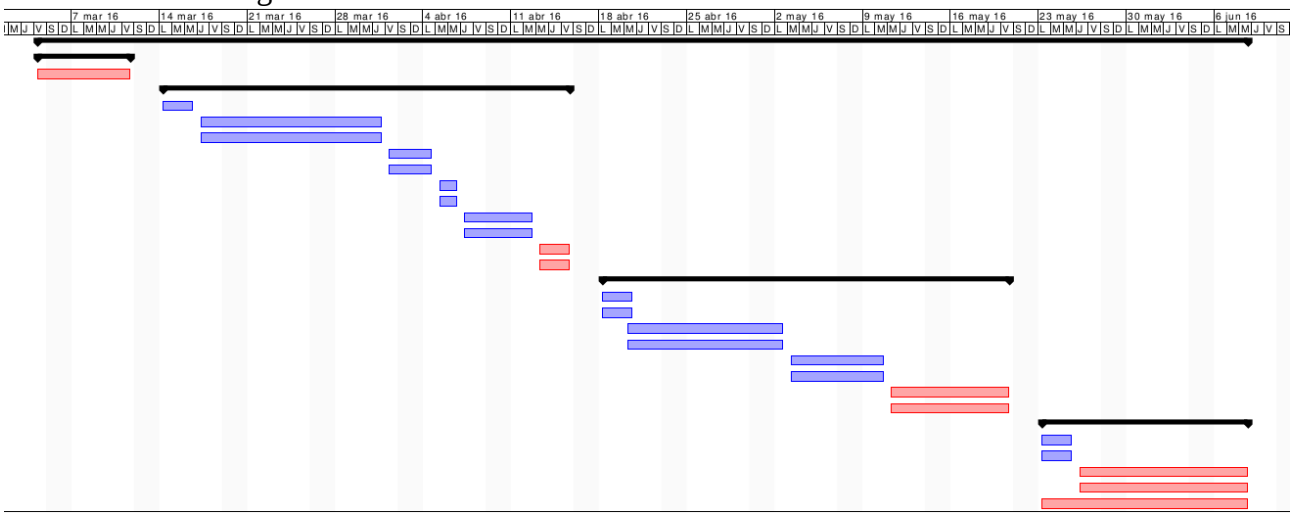
- Proxmox VE
- Ubuntu 14.04 (tant l'edició de servidor com la d'escriptori)
- Ubuntu 16.04

1.4 Planificació del projecte

A continuació és mostra les fites del projecte detallades:

		Nombre	Duracion	Inicio	Terminado
1		**PFC**	**69 days?**	**4/03/16 8:00**	**8/06/16 17:00**
2		**PAC1**	**6 days?**	**4/03/16 8:00**	**11/03/16 17:00**
3		Creació i entrega proposta	6 days?	4/03/16 8:00	11/03/16 17:00
4		**PAC2 40%-60%**	**25 days?**	**14/03/16 8:00**	**15/04/16 17:00**
5		Instalació i configuració Proxmox	3 days?	14/03/16 8:00	16/03/16 17:00
6		Instalació servidor autenticació	11 days?	17/03/16 8:00	31/03/16 17:00
7		Documentació instalació servidor aute...	11 days?	17/03/16 8:00	31/03/16 17:00
8		Instalació servidor DNS	2 days?	1/04/16 7:00	4/04/16 17:00
9		Documentació servidor DNS	2 days?	1/04/16 7:00	4/04/16 17:00
10		Instalació sevidor DHCP	2 days?	5/04/16 7:00	6/04/16 17:00
11		Documentació servidor DHCP	2 days?	5/04/16 7:00	6/04/16 17:00
12		Instalació servidor de fitxers	4 days?	7/04/16 7:00	12/04/16 17:00
13		Documentació servidor de fitxers	4 days?	7/04/16 7:00	12/04/16 17:00
14		Instalació d'entitat certificadora	3 days?	13/04/16 7:00	15/04/16 17:00
15		Instalació d'entitat certificadora	3 days?	13/04/16 7:00	15/04/16 17:00
16		**PAC3 80%-90%**	**25 days?**	**18/04/16 8:00**	**20/05/16 17:00**
17		Instalació servidor d'impresió	3 days?	18/04/16 8:00	20/04/16 17:00
18		Documentació servidor d'impresió	3 days?	18/04/16 8:00	20/04/16 17:00
19		Instalació servidor correu	9 days?	20/04/16 8:00	2/05/16 17:00
20		Documentació servidor correu	9 days?	20/04/16 8:00	2/05/16 17:00
21		Instalació servidor web/Intranet	6 days?	3/05/16 8:00	10/05/16 17:00
22		Documentació servidor web/Intranet	6 days?	3/05/16 8:00	10/05/16 17:00
23		Instalació servidor cloud de fitxers	8 days?	11/05/16 8:00	20/05/16 17:00
24		Documentació servidor cloud de fitxers	8 days?	11/05/16 8:00	20/05/16 17:00
25		**Entrega Final**	**13 days?**	**23/05/16 8:00**	**8/06/16 17:00**
26		Instalació de servidor proxy	3 days?	23/05/16 8:00	25/05/16 17:00
27		Documentació servidor proxy	3 days?	23/05/16 8:00	25/05/16 17:00
28		Instalació del servidor VPN	10 days?	26/05/16 8:00	8/06/16 17:00
29		Documentació del servidor VPN	10 days?	26/05/16 8:00	8/06/16 17:00
30		Finalització de la memoria i correcció d'...	13 days?	23/05/16 8:00	8/06/16 17:00

Per últim es detalla gràficament cada fita:



El projecte ha tingut una duració de tres mesos i quatre dies iniciant-se el 4 de març de l'any 2016 i finalitzant el 8 de Juny del mateix any
El projecte es va dividir en quatre grans fites les quals tenen les següents dates:

- **Creació i proposta de projecte(PAC1)** 11/03/2016
- **Lliurable 2 :** del 40% al 60% de la memòria(PAC2) 15/04/2016
- **Lliurable 3 :** del 80 al 90% de la memòria(PAC3) 20/05/2016
- **Lliurament final:** Memòria final amb tots els annexes(Entrega Final) 08/06/2016

Aquesta planificació es va complir rigorosament.

1.5 Productes obtinguts

Tal i com s'ha descrit en seccions anteriors, el producte obtingut serà un entorn que simularà l'infraestructura d'una empresa mitjana.

1.6 Descripció dels altres capítols de la memòria

La memòria final es divideix en desset capítols. Aquest és un esbos del contingut de cada capítol:

Capítol 1: Introducció

A aquest capítol s'explicaran els objectius i l'abast d'aquest projecte. També s'inclourà la planificació del projecte.

Capítols 2 – 12 : Serveis implementats

A cada capítol es farà tant una explicació de en que consisteix cada servei, quin és la seua funció i importància dins de una empresa. També es detallarà la instal·lació i configuració bàsiques del servei així com les funcions més destacables de cada producte i el seu nivell de integrabilitat en les tres plataformes principals d'usuaris(Linux,Windows i MAC OS).

Aquests capítols s'ordenaran per ordre d'instal·lació en aquest estudi. Aquest ordre s'ha decidit en base a la seua necessitat. Es començarà per els serveis bàsics i s'anirà afegint la resta de serveis que completaran l'infraestructura. L'ordre serà el següent:

Capítol 2: Hypervisor de maquines virtuals – Proxmox
Capítol 3: Servei d'autenticació d'usuaris – OpenLDAP
Capítol 4: Servidor DNS – Bind9
Capítol 5: Entitat certificadora
Capítol 6: Servidor DHCP
Capítol 7 : Servidor de fitxers - Samba
Capítol 8: Servidor d'impressió – CUPS
Capítol 9 Servidor web i gestor de contingut (Intranet)
Capítol 10: Servidor de correu – Postfix,Dovecot amb spamassassin i clamav
Capítol 11: Servidor cloud de fitxers – Owncloud
Capítol 12: Servidor Proxy :- Squid
Capítol 13 : Servidor VPN – OpenVPN

Capítol 14:Conclusions

A aquest capítol es farà un anàlisi de si s'han assolit els objectius inicials seguint la planificació i analitzant les causes tant de l'èxit com del fracàs de qualsevol d'aquests punts. A més, aquesta secció incloure possibles millores al projecte i futures línies d'investigació.

Capítol 15: Glossari

Capítol on es definiran els termes i acrònims utilitzats en la memòria

Capítol 16: Bibliografia

Descripció detallada de les fonts d'on s'ha tret la informació emprada per a la realització del projecte

Capítol 17: Annexos

S'afegiran documents d'interés que puguen completar la informació exposada a aquest projecte com ara algun manual d'administració d'algun dels serveis implementats.

2. Hipervisor de màquines virtuals

A aquesta secció es detalla què és un hipervisor de màquines virtuals i la instal·lació del producte escollit per a aquest projecte, Proxmox. A més es detalla la configuració dels aspectes més importants que Proxmox ofereix.

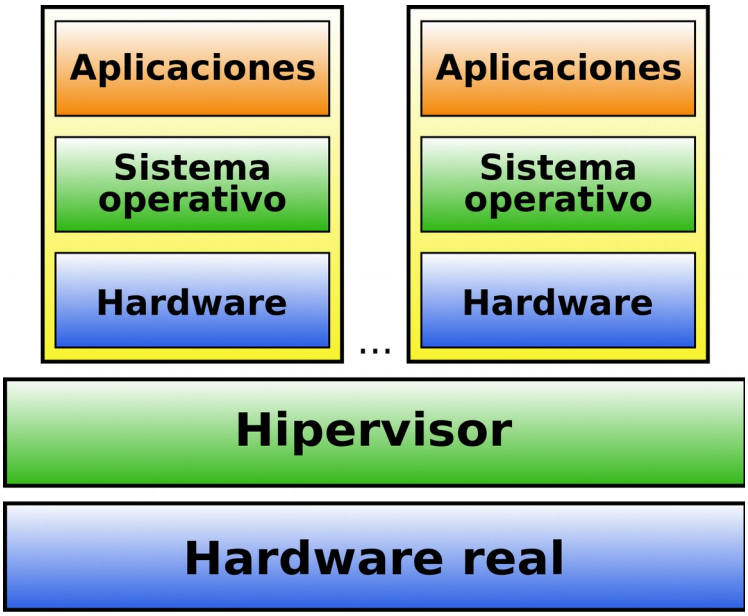
2.1 Què és un Hipervisor?

El hipervisor de màquines virtuals o monitor de màquines virtuals(VMM), és el nucli central d'algunes de les tecnologies de virtualització de maquinari presents al mercat avui dia. L'hipervisor és una aplicació que actua com a intermediari entre el sistema operatiu de les màquines virtuals o sistemes convidats i el maquinari on s'executen aquests sistemes oferint una plataforma operativa virtual o maquinari virtual i amagant el maquinari real del dispositiu on els sistemes convidats operen.

D'aquesta manera es poden executar múltiples màquines virtuals amb el seu sistema operatiu i les seues aplicacions a un sol servidor repartint els recursos d'aquest amb totes les màquines que allotja. Açò ens permet, si calculem bé les nostres necessitats, optimitzar els recursos de maquinari i no infrautilitzar-los .

Podem diferenciar dos tipus de hipervisors:

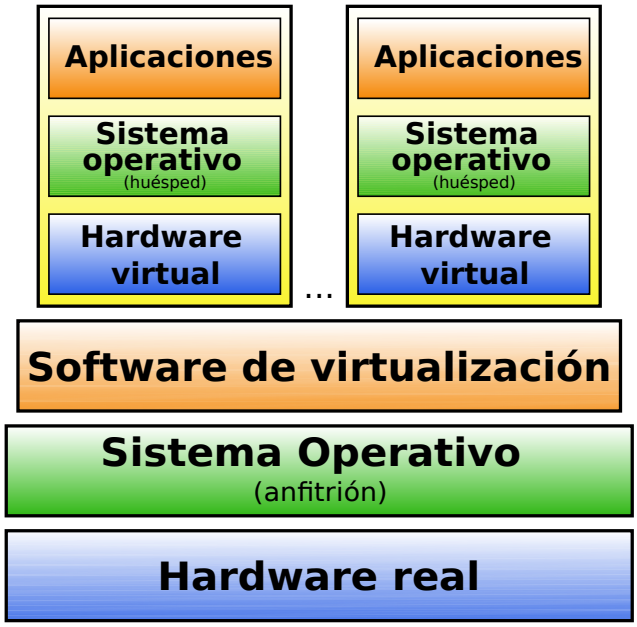
- **Hipervisor de tipus 1:** també coneguts com natius, unhosted o bare-metal. Són aquells hipervisors que s'executen directament sobre el maquinari físic. El hipervisor es carrega abans que tots els sistemes convidats i tots els accessos al maquinari són controlats per ell.



Il·lustració 2.1 Pila hypervisor màquines virtuals tipus 1

Avui dia les solucions més potents del mercat utilitzen aquest tipus de hipervisor. Cal destacar VMWare vSphere ESX, Citrix XenServer, Microsoft Hyper-V i Proxmox. Aquest últim és l'hipervisor escollit per a suportar totes les màquines virtuals necessàries per a la instal·lació dels diferents sistemes estudiats a aquest projecte.

- **Hipervisor de tipus 2:** En aquest cas la capa intermedi és un sistema operatiu on s'instal·la el programari de virtualització. D'aquesta manera les màquines virtuals interactuen amb el programari de virtualització i aquest amb el sistema operatiu que és l'encarregat de la comunicació amb el maquinari físic.

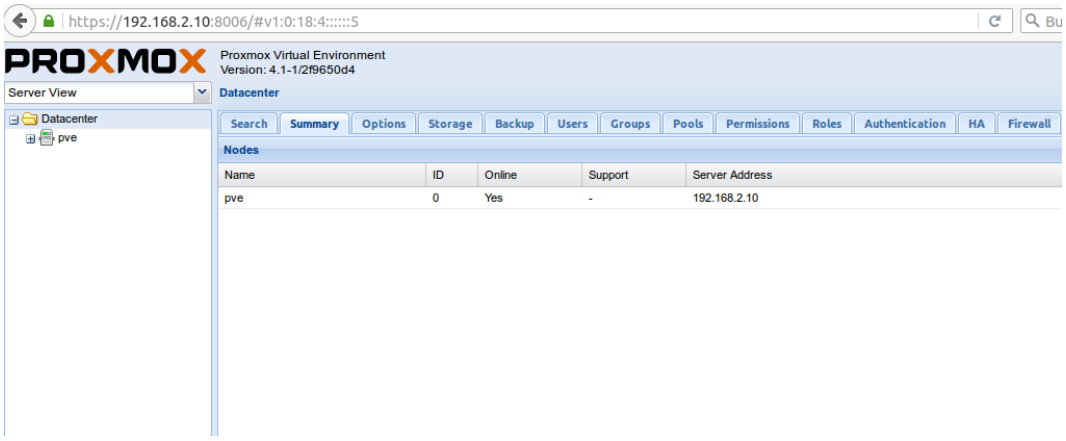


Il·lustració 2.2 Pila hypervisor tipus 2

Per aquest projecte la solució de programari lliure escollida és l'hipervisor de tipus 1 Promox.

2.2 Proxmox

Proxmox és una completa plataforma de programari lliure per a la virtualització de servidors. Està basat en la virtualització KVM i en la virtualització basada en contenidors. Proxmox, és capaç de gestionar tant maquines virtuals KVM , contenidors Linux (en anglés LXC o Linux containers), emmagatzemament, xarxes virtuals i clusters d'alta disponibilitat.
La seua administració es fa mitjançant una interfície web. Des d'aquesta interfície es poden realitzar totes les operacions necessàries per poder gestionar de manera eficient tots els aspectes relacionats amb la creació i manteniment de màquines virtuals, xarxes virtuals i l'emmagatzemament que aquestes necessiten.



Il·lustració 2.3 Interfície d'administració de Proxmox

Proxmox està basat en la distribució Linux Debian amb un kernel modificat de Red Hat Enterprise Linux i es distribueix baix la llicència GNU Affero General Public License (AGPL), v3 que dona qualsevol la possibilitat de fer ús del programari, modificar-lo i distribuir-lo

2.2.1 KVM i LXC

KVM (en anglés Kernel-based Virtual Machine) és una infraestructura de virtualització per al kernel de Linux que es va convertir en un hipervisor de màquines virtuals i que pot allotjar convidats Linux, Unix i Windows. Està compost per el mòdul kvm.ko que proporciona el nucli de la infraestructura de virtualització i un mòdul especific per al processador (kvm-intel.ko o kvm-amd.ko). Actualment KVM utilitza QEMU com a front-end.

LXC o en anglés Linux containers és una tecnologia de virtualització a nivell de sistema operatiu de Linux. Permet a un servidor físic executar diferents instancies de sistemes operatius aïllats. LXC no proveeix una màquina virtual, més be crea un entorn virtual que té el seu espai de processos i xarxes.

Aquestes són les tecnologies que utilitza Proxmox per crear les màquines virtuals. En el context d'aquest projecte, la millor opció és LXC atés que podem considerar els contenidors LXC com màquines virtuals lleugeres que optimitzaran millor els recursos físics. Per tant, s'aprofitarà el fet que tots els sistemes estudiats a aquest projecte corren baix servidors Linux.

2.3 Instal·lació i configuració de Proxmox

Per aquest projecte instal·larem la versió bare-metal de Proxmox, és a dir, directament sobre el maquinari. Tot el procés d'instal·lació tant de hipervisor com de la resta de sistemes es realitzarà emprant eines de programari lliure. S'ha utilitzat un ordinador portàtil amb Ubuntu 15.04 com a sistema operatiu per els primers passos d'aquest projecte i per l'administració de Proxmox.

La majoria dels passos descrits en aquest document valdran per a qualsevol distribució Linux. De no ser així quedarà especificat en quin sistema s'ha realitzat l'estudi amb una nota al final de la pàgina

2.3.1 Gravar Proxmox en USB

Primerament s'ha de descarregar l'imatge iso del lloc web de Proxmox:

http://www.proxmox.com/en/downloads/item/proxmox-ve-4-1-iso-installer

Tot seguit i amb l'ajuda del terminal gravarem la imatge iso en una llapissera USB seguint els següents passos[1]:

- Connectar una llapissera USB,obrir un terminal i executar:

  sudo dmesg

  A l'eixida d'aquesta instrucció hem de localitzar el dispositiu associat a la llapissera USB. Com es veu a la següent imatge, en el cas del nostre exemple el sistema ha identificat la llapissera com **/dev/sdb.**

1 Passos seguits amb ordinador portàtil executant Ubuntu 15.04

```
[16624.080190] usb-storage 1-3:1.0: USB Mass Storage device detected
[16624.080256] usb-storage 1-3:1.0: Quirks match for vid 13fe pid 3600: 4000
[16624.080272] scsi host4: usb-storage 1-3:1.0
[16624.080375] usbcore: registered new interface driver usb-storage
[16624.107916] usbcore: registered new interface driver uas
[16625.107027] scsi 4:0:0:0: Direct-Access              USB DISK 2.0     PMAP P(
: 0 ANSI: 4
[16625.107911] sd 4:0:0:0: Attached scsi generic sg1 type 0
[16626.391087] sd 4:0:0:0: [sdb] 61079552 512-byte logical blocks: (31.2 GB/29.
 GiB)
[16626.391258] sd 4:0:0:0: [sdb] Write Protect is off
[16626.391261] sd 4:0:0:0: [sdb] Mode Sense: 23 00 00 00
[16626.391406] sd 4:0:0:0: [sdb] No Caching mode page found
[16626.391409] sd 4:0:0:0: [sdb] Assuming drive cache: write through
[16626.421033]  sdb: sdb1
[16626.422653] sd 4:0:0:0: [sdb] Attached SCSI removable disk
tiko@tiko-LA:~$
```

Il·lustració 2.4 Porció del l'eixida de dmesg

- Canviar al directori on es troba l'imatge iso descarregada i executar:

  sudo dd if=nom_de_la_imatge of=dispositiu usb bs=4M
  sudo sync
  Exemple: ***dd if=proxmox-ve_4.1-2f9650d4-21.iso of=/dev/sdb bs=4M***

```
tiko@tiko-LA:~/Documentos/Software/ISOs$ sudo dd if=proxmox-ve_4.1-2f9650d4-21.i
so of=/dev/sdb bs=4M
171+1 registros leídos
171+1 registros escritos
718274560 bytes (718 MB) copiados, 8,0934 s, 88,7 MB/s
tiko@tiko-LA:~/Documentos/Software/ISOs$ sudo sync
tiko@tiko-LA:~/Documentos/Software/ISOs$
```

Il·lustració 2.5 Copiar iso a USB

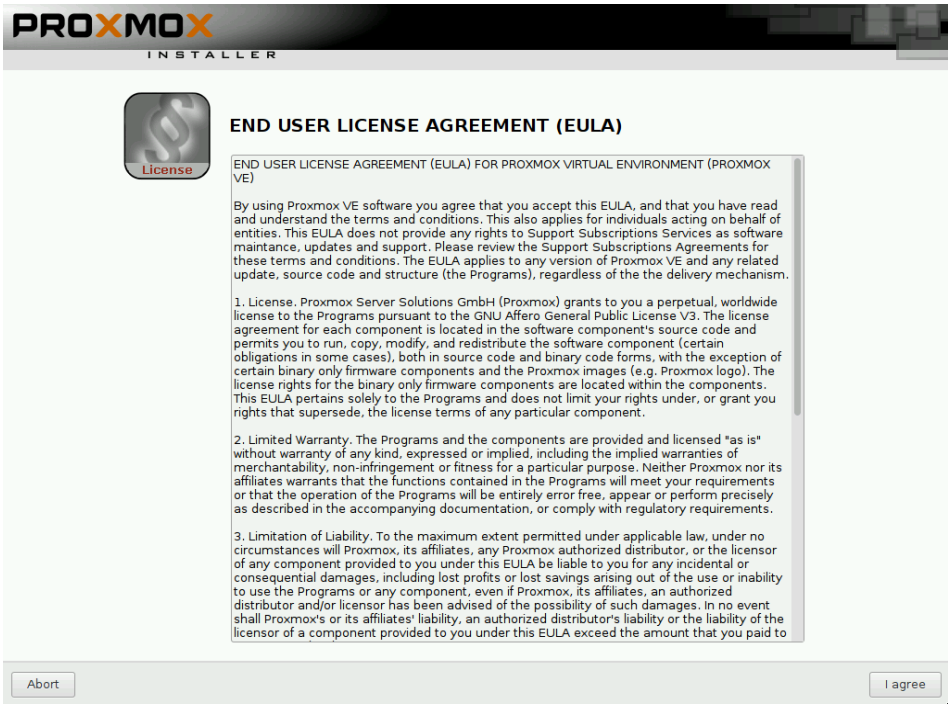
- Extraure la llapissera USB

2.3.2 Instal·lació pas a pas del hipervisor

- Arrancar l'ordinador amb la llapissera USB creada al pas anterior. En la pantalla de benvinguda seleccionar la opció **Install Proxmox VE** i pressionar la tecla **Enter**

Il·lustració 2.6 Pantalla inici instal·lació de Proxmox

- Acceptar els termes de la llicencia

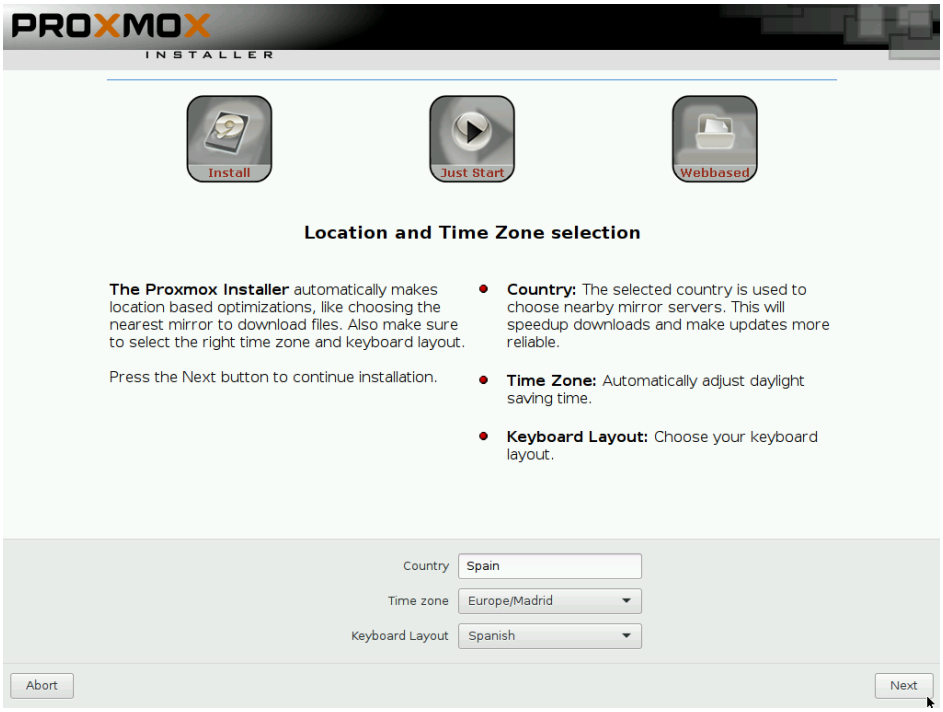


Il·lustració 2.7 Termes d'ús

- Seleccionar en el desplegable el dispositiu on es vol instal·lar Proxmox i polsar **Next**. Si només disposem d'un disc local el dispositiu serà **/dev/sda**. Si en tenim més d'un haurem d'escollir. La solució òptima per a un sistema en producció seria disc configurats en RAID amb una velocitat alta. Proxmox recomana discs SAS de quinze mil revolucions configurats en RAID 10.

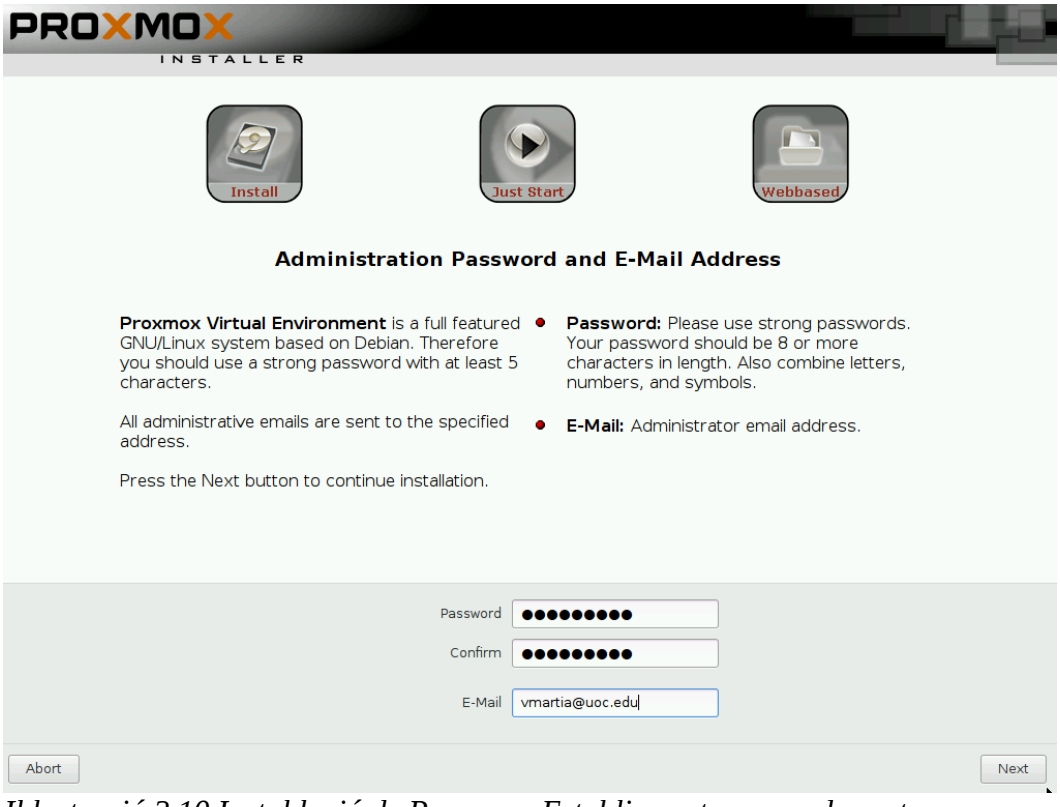
Il·lustració 2.8 Instal·lació de Proxmox: Emmagatzemament

- Seleccionar el país,la zona horària i el mapa de teclat.



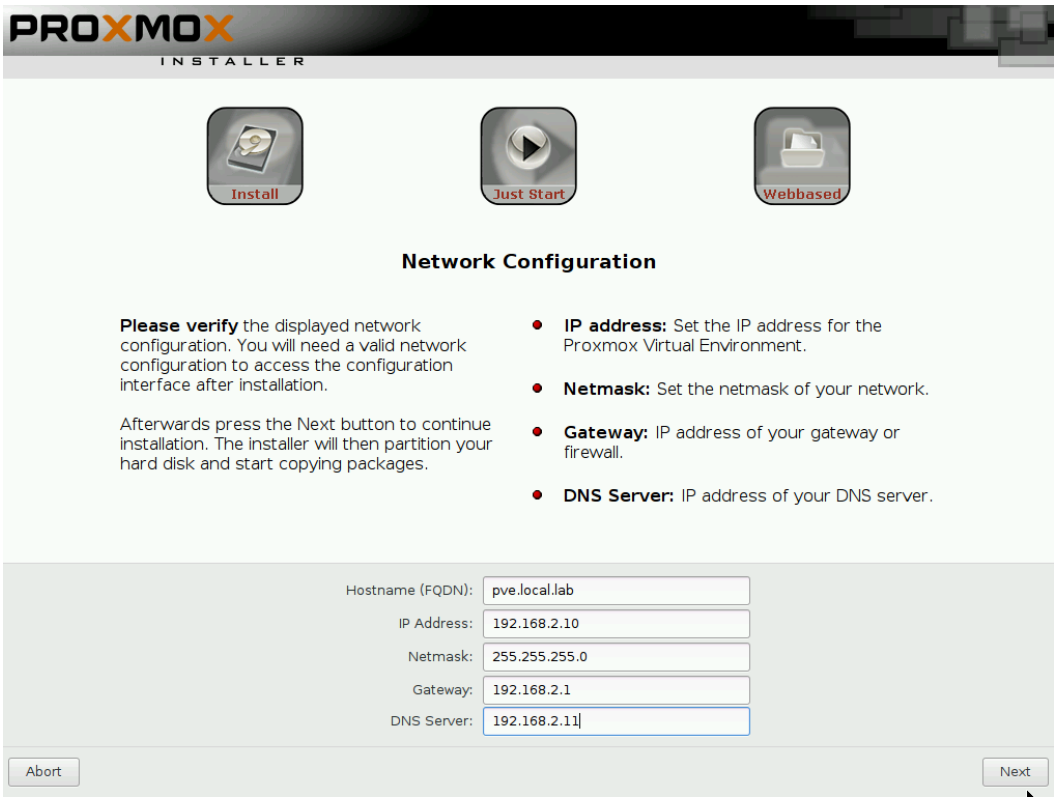
Il·lustració 2.9 Instal·lació de Proxmox: Zona horària

- Establit la contrasenya de l'usuari root i la direcció d'email de l'administrador



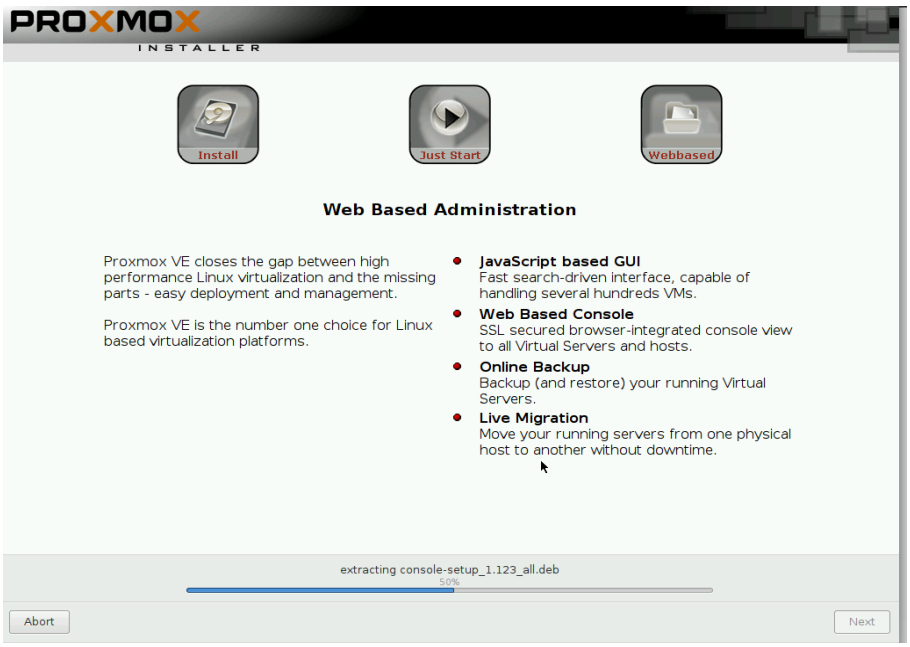
Il·lustració 2.10 Instal·lació de Proxmox: Establir contrasenya de root

- Establir el nom del servidor i la configuració IP.



Il·lustració 2.11 Instal·lació de Proxmox: Xarxa

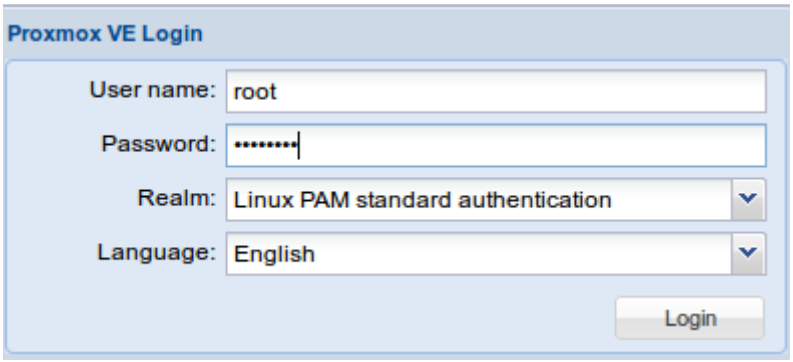
- A aquest punt començarà el procés de instal·lació



Il·lustració 2.12 Instal·lació de Proxmox: Progrés d'instal·lació

- Finalment el servidor es reiniciarà i ja podrem accedir a la seua interfície web amb la direcció https://IP-del-servidor:8006

Il·lustració 2.13 Login en terminal



Il·lustració 2.14 Pantalla de login de Proxmox

2.3.3 Configuració segon node per a alta disponibilitat

Proxmox disposa de tecnologia d'alta disponibilitat que permet les màquines virtuals i contenidors executar-se en diferents nodes agregats a un cluster de servidors Proxmox. D'aquesta manera si algun servidor té algun problema o l'administrador ha de d'aturar-lo per fer algun tipus d'actualització o manteniment, el servei no té per què sofrir cap parada.

2.3.3.1 Configuració cluster per a administració centralitzada

En cas de no tindre recursos de xarxa per el emmagatzemament de les màquines virtuals o contenidors, podem crear un cluster per administrar més d'una instancia de Proxmox des de qualsevol dels servidors membres del cluster.

Aquests són els passos a seguir:

- Connectar per ssh al servidor principal Proxmox i executar : pvecm create «nom del cluster»

```
root@pve-a:~# pvecm create pve-clr
Corosync Cluster Engine Authentication key generator.
Gathering 1024 bits for key from /dev/urandom.
Writing corosync key to /etc/corosync/authkey.
root@pve-a:~#
```

Il·lustració 2.16 Creació cluster Proxmox

- Per comprovar l'estat del cluster podem executar la instrucció **pvecm status.** En la imatge es pot comprovar que el cluster s'ha creat i que només té un membre.

```
root@pve-a:~# pvecm status
Quorum information
------------------
Date:             Sat Apr  9 00:24:54 2016
Quorum provider:  corosync_votequorum
Nodes:            1
Node ID:          0x00000001
Ring ID:          4
Quorate:          Yes

Votequorum information
----------------------
Expected votes:   1
Highest expected: 1
Total votes:      1
Quorum:           1
Flags:            Quorate

Membership information
----------------------
    Nodeid      Votes Name
0x00000001          1 192.168.1.10 (local)
root@pve-a:~#
```

Il·lustració 2.17 Consulta status cluster

- Modificar l'arxiu **/etc/hosts** de tots els servidors que formaran part del cluster i afegir una entrada per cada servidor. En el cas d'aquest exemple aquest seria el contingut del fitxer en cada servidor membre:(si tenim un servidor DNS local que siga capaç de resoldre les direccions de tots els servidor aquest pas no seria necessari):

```
  GNU nano 2.2.6                File: /etc/hosts

127.0.0.1 localhost.localdomain localhost
192.168.1.12 pve-b.local.lab pve-b pvelocalhost
192.168.1.10 pve-a.local.lab pve-a
192.168.1.14 pve-c.local.lab pve-c

# The following lines are desirable for IPv6 capable hosts

::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

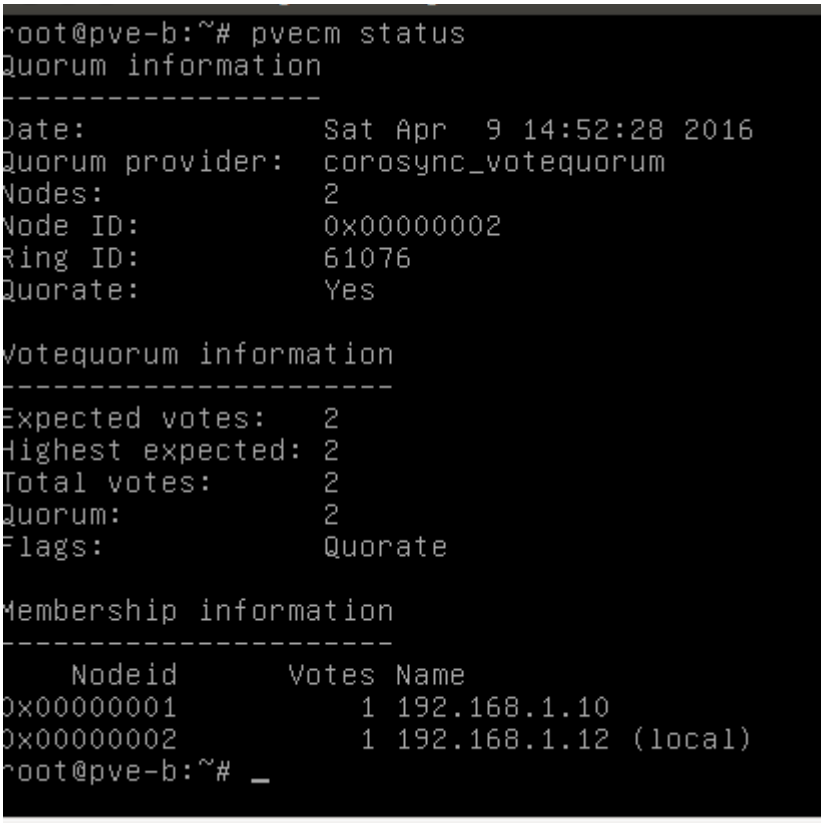
Il·lustració 2.18 Exemple arxiu /etc/hosts

- Connectar mitjançant ssh al segon node que es vol afegir al cluster i executar la instrucció pvcm add 192.168.1.10

```
root@pve-c:~# pvecm add 192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ECDSA key fingerprint is 41:c5:74:78:66:0a:3b:a5:9c:50:2f:49:bd:8f:b3:e6.
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.1.10's password:
copy corosync auth key
stopping pve-cluster service
backup old database
waiting for quorum...OK
generating node certificates
merge known_hosts file
restart services
successfully added node 'pve-c' to cluster.
root@pve-c:~#
```

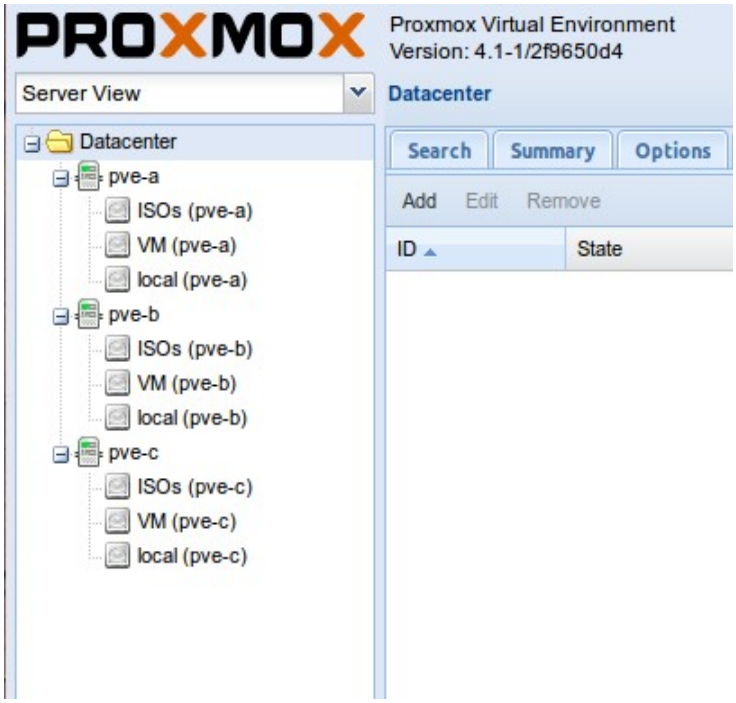
Il·lustració 2.19 Afegir node a cluster de Proxmox

Quan executem ara la instrucció ***pvecm status*** podem observar que el nombre de nodes s'ha incrementat.



Il·lustració 2.20 Pantalla de status de cluster amb dos nodes

- Ara ja es possible administrar totes les opcions de tots els nodes membres des de la interfície web d'administració:

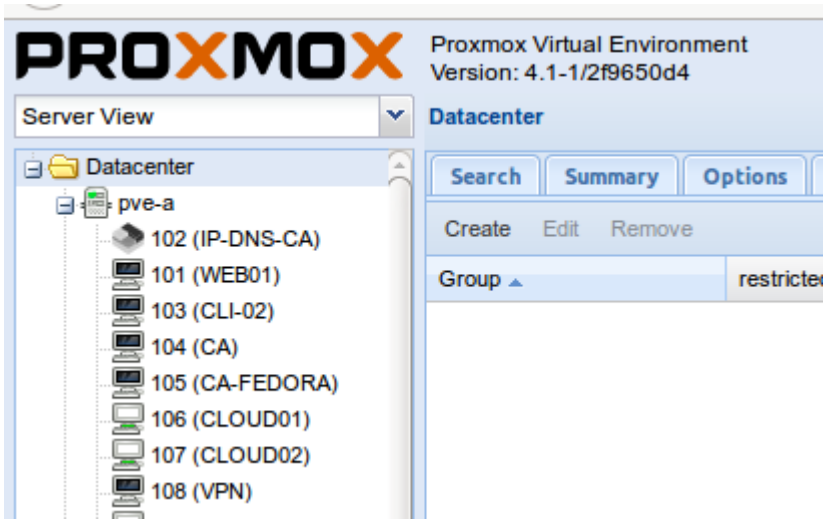


Il·lustració 2.21 Interfície d'administració Proxmox

2.3.3.2 Configuració d'alta disponibilitat en les màquines virtuals i contenidors

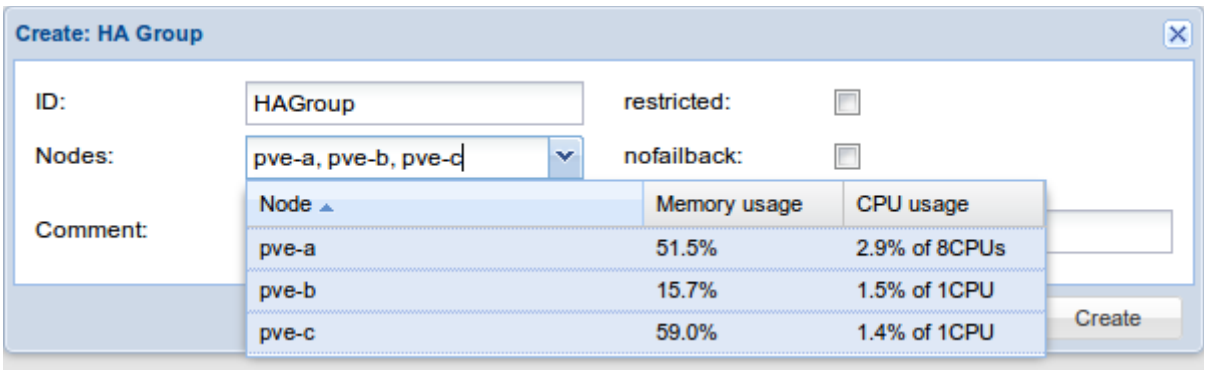
És essencial que cap dels elements de les maquines virtuals siga local per a poder aconseguir vertadera alta disponibilitat. Per a que la següent configuració puga funcionar, hem de crear tant els contenidors com les màquines virtuals amb recursos compartits. Pel que fa al emmagatzemament, podem crear un recurs NFS en xarxa o utilitzar un dispositiu d'emmagatzemament en xarxa. Quan ja el tenim habilitat, crearem la maquina virtual escollint aquest directori per a emmagatzemar-la.

Ara que ja tenim la maquina virtual que compleix els requisits per a poder ser gestionada amb el mecanisme d'alta disponibilitat que ofereix Proxmox s'ha de crear un grup de servidor on les maquines virtuals gestionades podran executar-se. Per a fer-ho farem clic en Datacenter en el panel de l'esquerra. Quan apareguen les pestanyes de configuració del Datacenter anirem a la pestanya HA . En el panel d'administració de HA, seleccionarem la pestanya Groups situada a la part inferior del panel central i polsarem el botó **Create**.



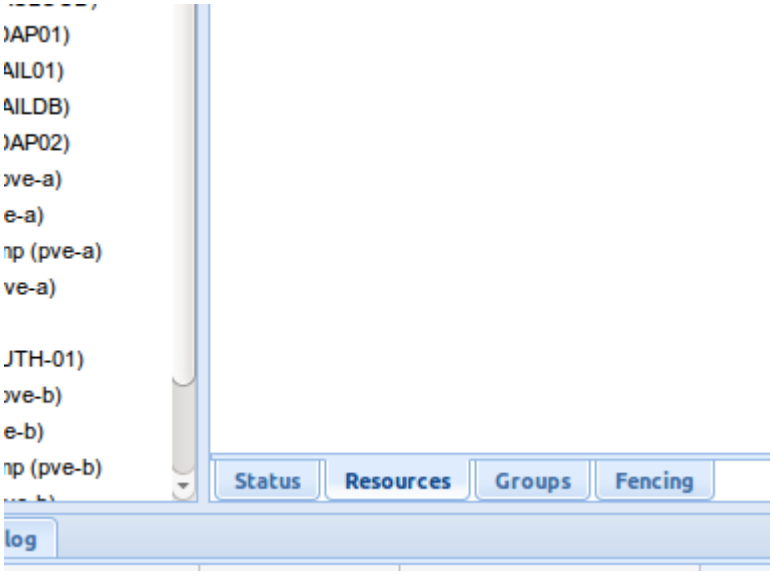
Il·lustració 2.22 Interfície creació grup HA

Assignarem un nom al grup de HA i seleccionarem tots els nodes que formaran part del grup. Formar part del grup significa que davant qualsevol contingència o si ens fa falta apagar un dels nodes per manteniment, les seues màquines virtual poden ser migrades als altres nodes del grup tant manual com automàticament. Per finalitzar, polsar create.

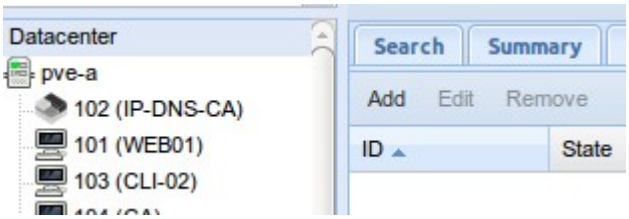


Il·lustració 2.23 Creació grup HA

A continuació, després de crear el grup, seleccionarem la pestanya **Resources** per a afegir una màquina al grup de HA que acabem de crear per a que siga gestionada pel sistema de HA de Proxmox. Polsarem el botó **Add** de la pestanya **Resources**.

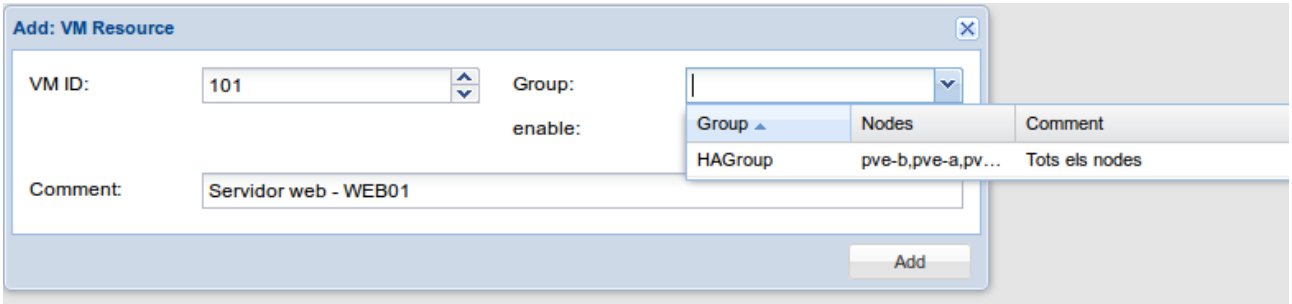


Il·lustració 2.24 Pestanya Resources HA



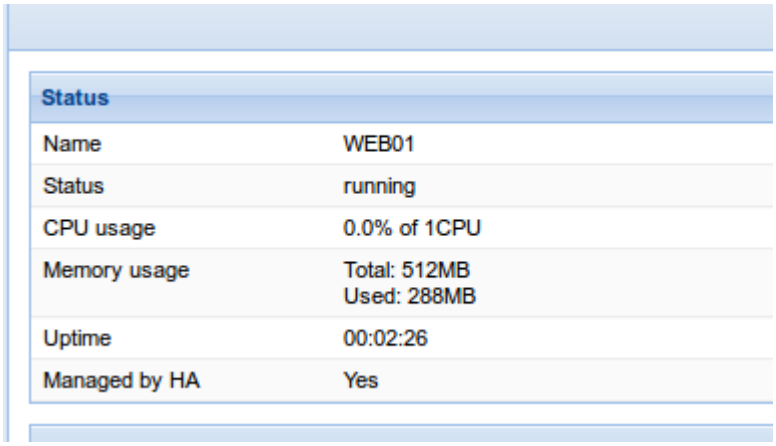
Il·lustració 2.25 Botó afegir recurs a grup HA

Omplirem la informació del servidor que volem afegir al grup gestionat i polsarem el botó **Add**. És important prendre nota del ID de la màquina que volem afegir abans de intentar afegir per a no errar.



Il·lustració 2.26 Afegir màquina virtual a HA

Com s'aprecia a la següent imatge, el servidor WEB01 d'aquest exemple ja està gestionat pels mecanismes d'alta disponibilitat de Proxmox.



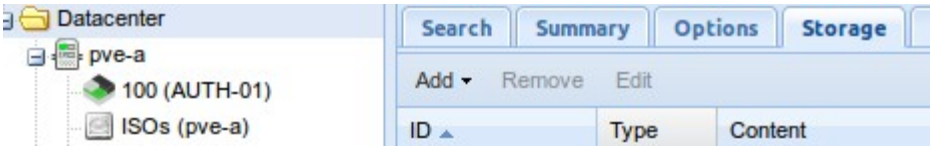
Il·lustració 2.27 Pestanya: Summary status màquina amb HA

2.3.4 Crear directori per a continguts

Tant per a la creació de màquines virtual com de contenidors així com per guardar els seus respectius discs virtuals, és necessari crear directoris a Proxmox. En la creació es defineix quin tipus de contingut volem emmagatzemar.

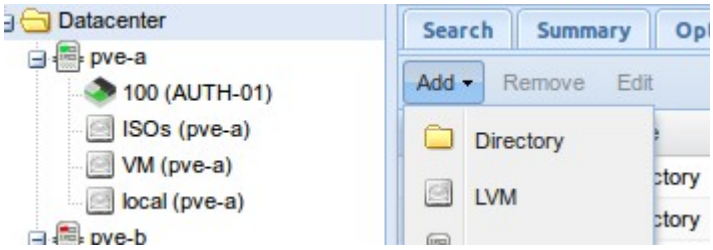
A continuació es detallen els passos a seguir per a la creació d'un directori:

- Seleccionar **Datacenter** en el panel de l'esquerra. En la pestanya **Storage** del panel centrar polsar el botó **Add.**



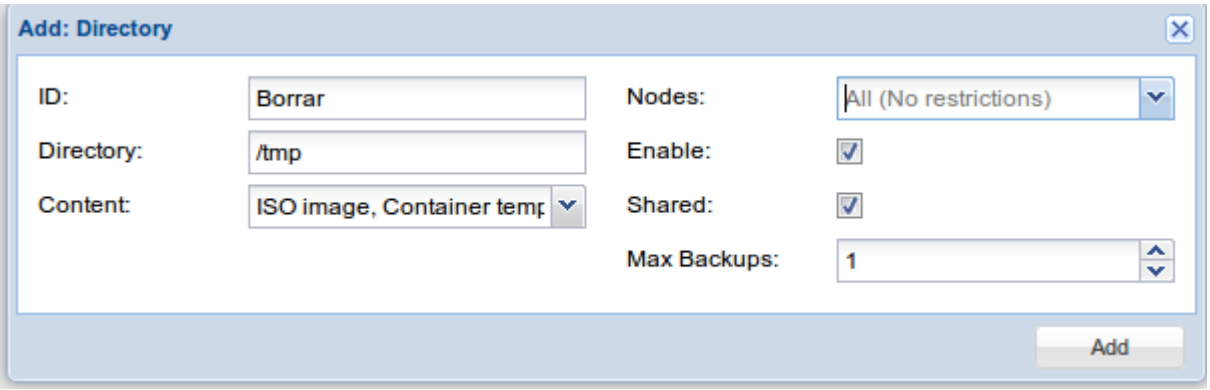
Il·lustració 2.28 Afegir directori en la pestanya Storage

- Al menú contextual seleccionar **Directory**



Il·lustració 2.29 Menú contextual de afegir directori

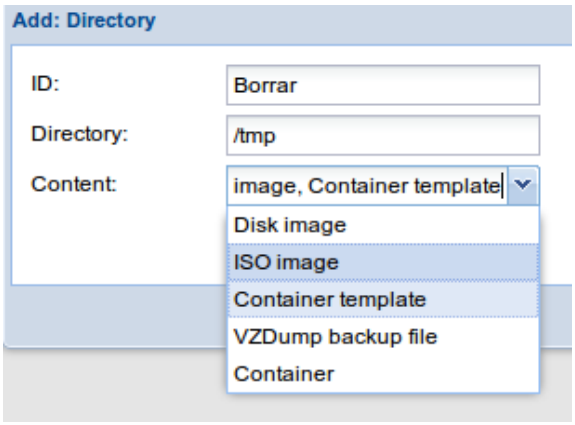
- Omplir els camps **ID** (identificar del directori),**Directory**(ruta local al servidor on esta físicament el directori),**Content**(seleccionar el tipus de contingut del directori), **Nodes**(nodes del cluster on es vol crear el directori) i marcar les caselles **Enable** i **Shared**. Per últim, es pot configurar també el nombre màxim de backups que es volen retindre del directori.



Il·lustració 2.30 Afegir directori

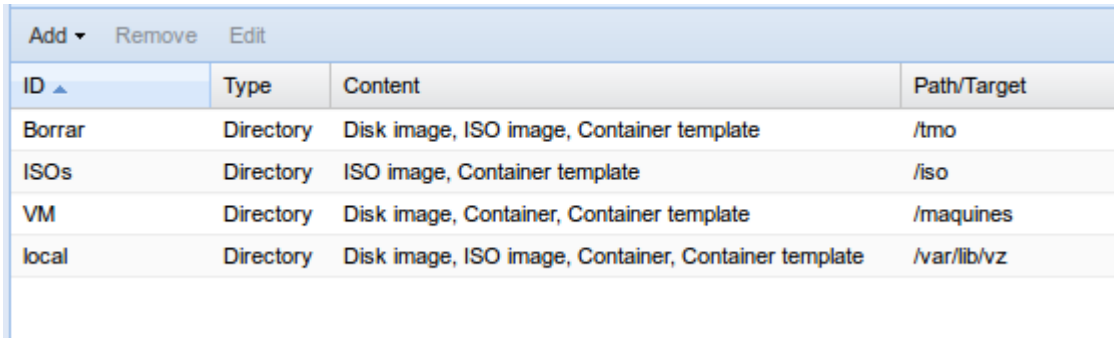
Com a tipus de contingut trobem els següents:

- **ISO imatge:** arxius iso de sistemes operatius que s'empren per instal·lar màquines virtuals
- **Container templates:** plantilles per crear contenidors LXC (aquest tipus de contingut és el que seria necessari per a l'exemple)
- **Disk image:** per emmagatzemar. els discs de les màquines virtuals
- **VZDump backup file:** per emmagatzemar. arxius de backup
- **Container:** per emmagatzemar contenidors



Il·lustració 2.31 Desplegable tipus directori

- Quan el procés ha finalitzat es podrà vore el nou directori en la llista de dispositius de emmagatzemament.



Il·lustració 2.32 Llista de directoris

2.3.5 Crear màquina virtual o contenidor

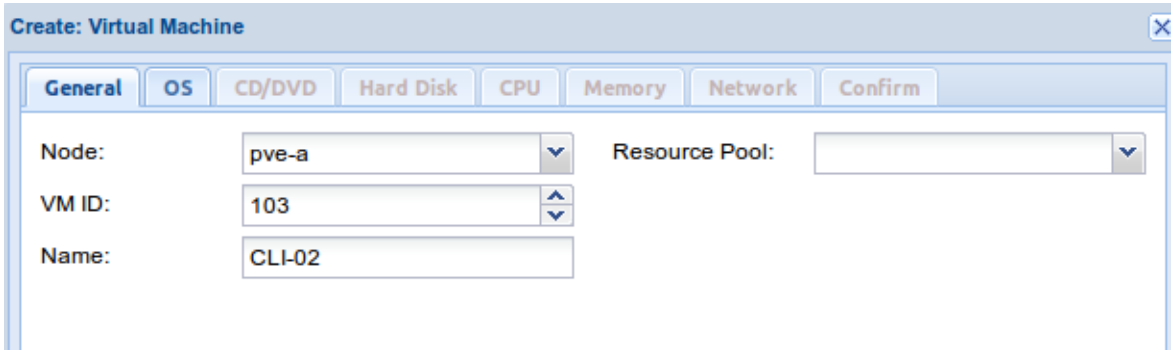
Amb Proxmox podem optar com ja s'ha explicat anteriorment entre crear màquines virtuals utilitzant la tecnologia KVM o contenidors Linux (LXC). Atenent a la natura d'aquest projecte emprarem majoritàriament contenidors Linux per la seua lleugeresa enfront les màquines virtuals convencionals tot i que la creació d'alguna màquina virtual també serà necessària. A continuació s'explica pas a pas com crear tant màquines virtuals com contenidors.

2.3.5.1 Creació de màquina virtual

Primerament, hem de carregar al servidor Promox la imatge iso que conté el sistema operatiu. Per a fer-ho, seleccionar en el panel de l'esquerra **Datacenter** , en l panel central seleccionar el directori on volem carregar el arxiu iso i polsar **Upload**. S'obrira una finestra on podrem buscar als directoris locals de la màquina des d'on ens hem connectat a Proxmox. Seleccionar l'arxiu iso a carregar i polsar **Ok**.

Quan ja tenim la imatge del sistema operatiu carregada podem crear la màquina virtual. Aquests són els passos per crear una màquina virtual KVM amb Proxmox:

- Polsant el botó **Create VM** que està a la part superior dreta de la interfície web, s'obrirà l'assistent per la creació d'una màquina virtual. A la primera pestanya trobem la informació relativa al node de Proxmox on volem crear la màquina virtual, l'ID de la màquina i el nom de la mateixa. També podrem assignar la màquina a un grup de recursos.

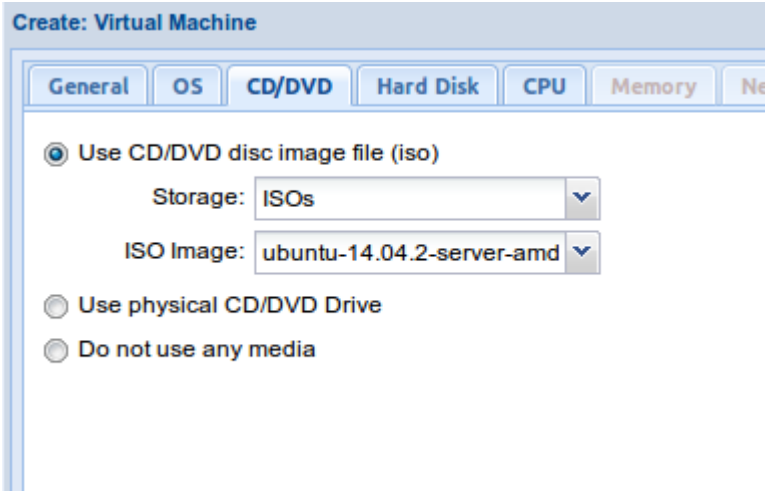


Il·lustració 2.33 Crear màquina virtual. Pestanya: General

- A la següent pestanya elegirem el sistema operatiu a instal·lar

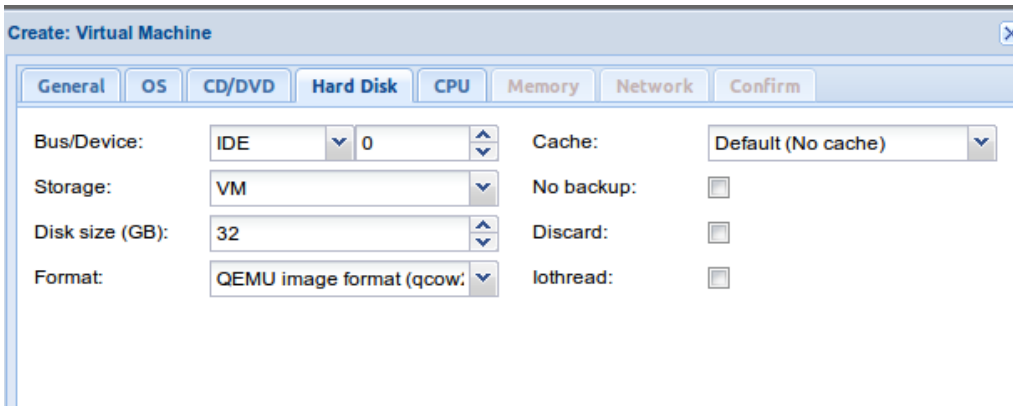
Il·lustració 2.34 Crear màquina virtual. Pestanya: OS

- A la tercera pestanya escollirem la ubicació de la imatge iso que hem carregat i el arxiu per a que al arrancar la màquina virtual estiga muntat a la unitat de CD/DVD per a començar la instal·lació.



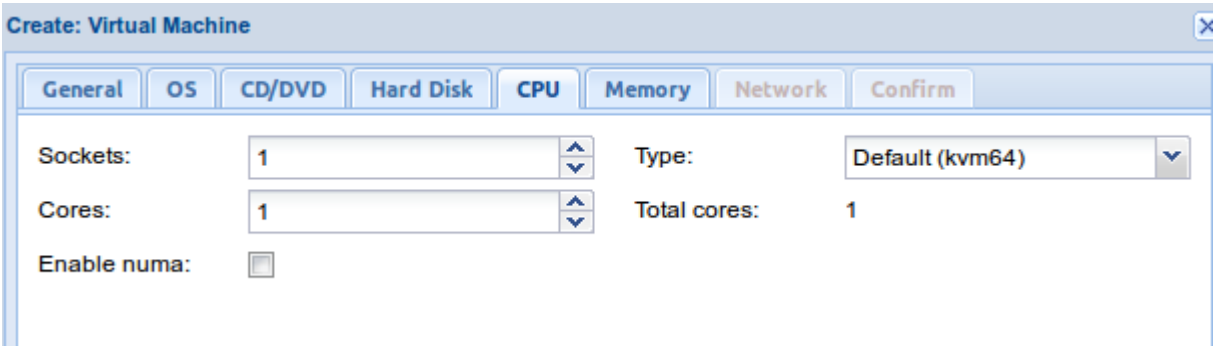
Il·lustració 2.35 Crear màquina virtual. Pestanya:CD/DVD

- A la pestanya **Hard Disk** trobem la configuració del disc dur virtual de la VM(màquina virtual). Seleccionar el tipus de dispositiu, la ubicació, la mida i el format del disc virtual.



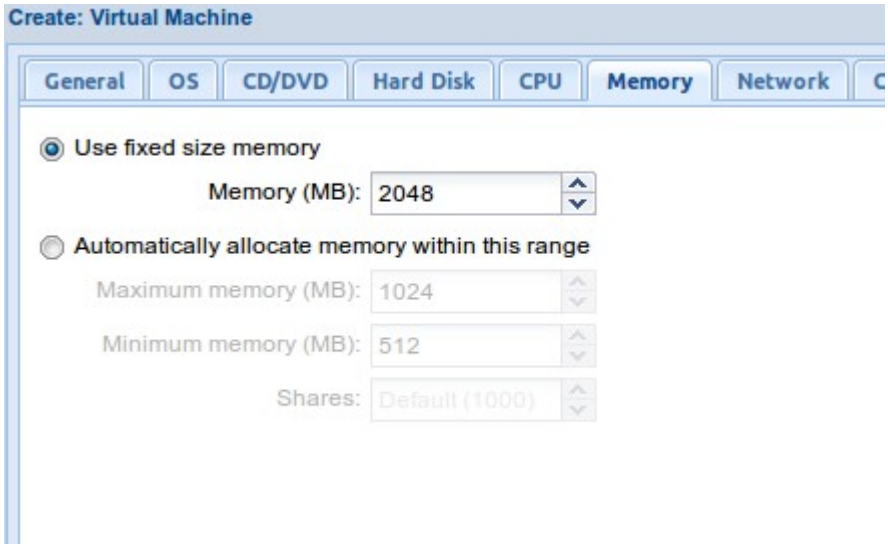
Il·lustració 2.36 Crear màquina virtual. Pestanya:Hard Disk

- A continuació es pot configurar la CPU(quantitat de CPUs i cores per CPU)



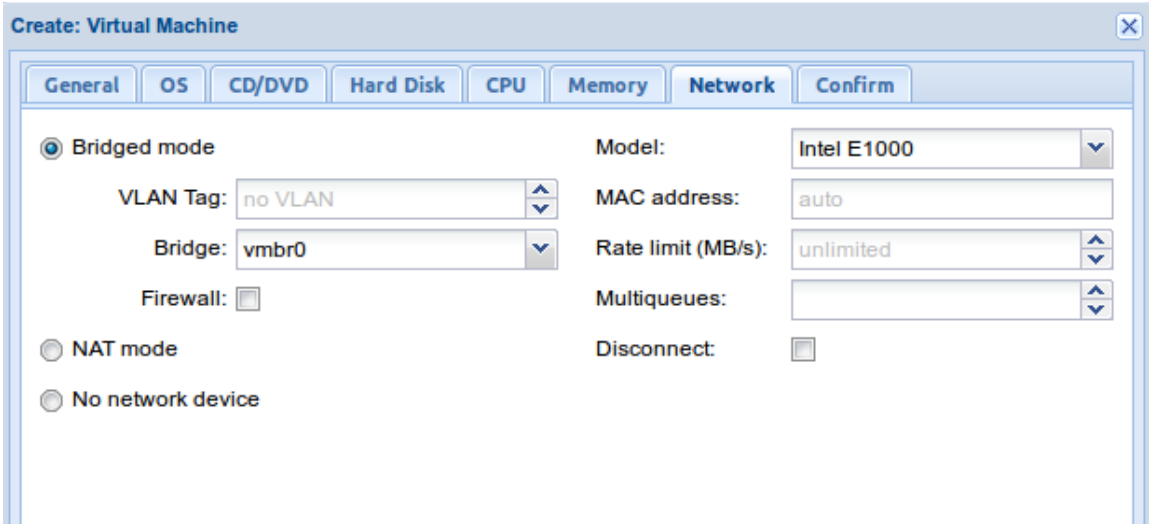
Il·lustració 2.37 Crear màquina virtual. Pestanya: CPU

- El següent pas és configurar la quantitat de memòria que es vol



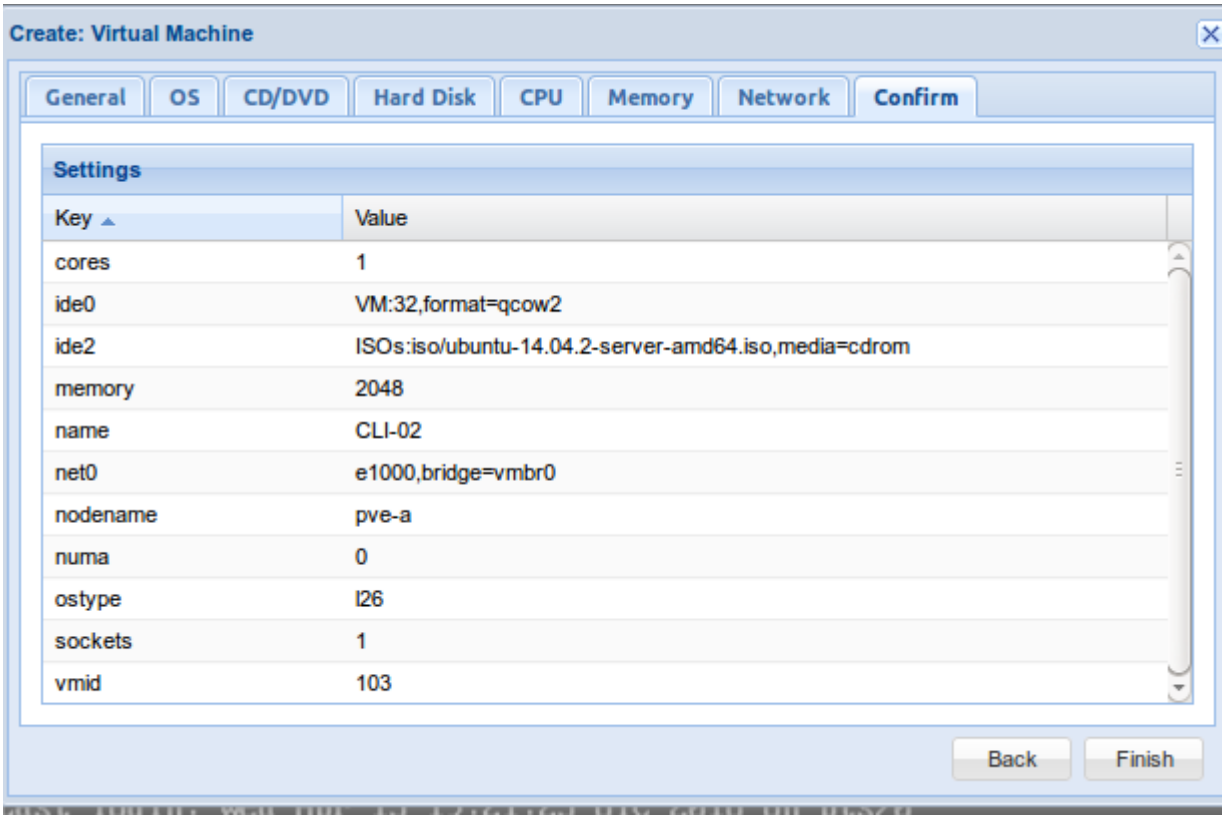
Il·lustració 2.38 Crear màquina virtual. Pestanya: Memory

- Per últim, configurar els paràmetres de xarxa i mode en que es vol connectar la interfície de xarxa.

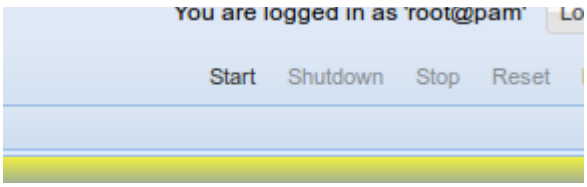


Il·lustració 2.39 Crear màquina virtual. Pestanya: Network

Abans de crear la màquina virtual es pot revisar la configuració escollida. Quan ja tenim la configuració desitjada polsem el botó Finish i començarà la creació de la màquina. Quan acaba el procés, seleccionar la màquina al panel de l'esquerra, seleccionar la pestanya **Console** i polsar el botó **Start**. La màquina virtual arrancarà i començarà el procés d'instal·lació del sistema operatiu escollit.



Il·lustració 2.40 Crear màquina virtual. Pestanya: Confirm



Il·lustració 2.41 Botó inici màquina virtual

2.3.5.2 Creació de contenidor Linux

El primer que s'ha de fer per crear un contenidor és descarregar una plantilla de la distribució Linux que volem instal·lar. Proxmox té disponibles varies distribucions en diferents versions. Primerament s'ha de fer login en la interfície web d'administració i seguir els següents passos:

- Seleccionar un directori al servidor que estiga configurat per emmagatzemar. Plantilles. En cas de no tenir cap es disposen de dues opcions:

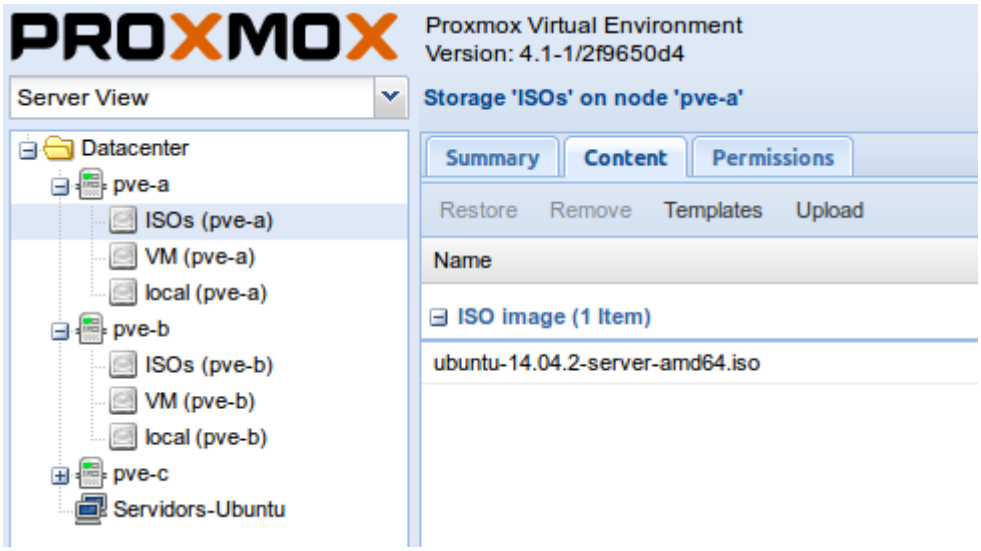
  a) Canviar el tipus de contingut del directori

  - Connectar per ssh al servidor Proxmox i executar la següent instrucció:
    pvesm set «nom_directori» --content vztmpl

- b) Crear un directori per a plantilles tal i com s'explica en la secció 2.3.4

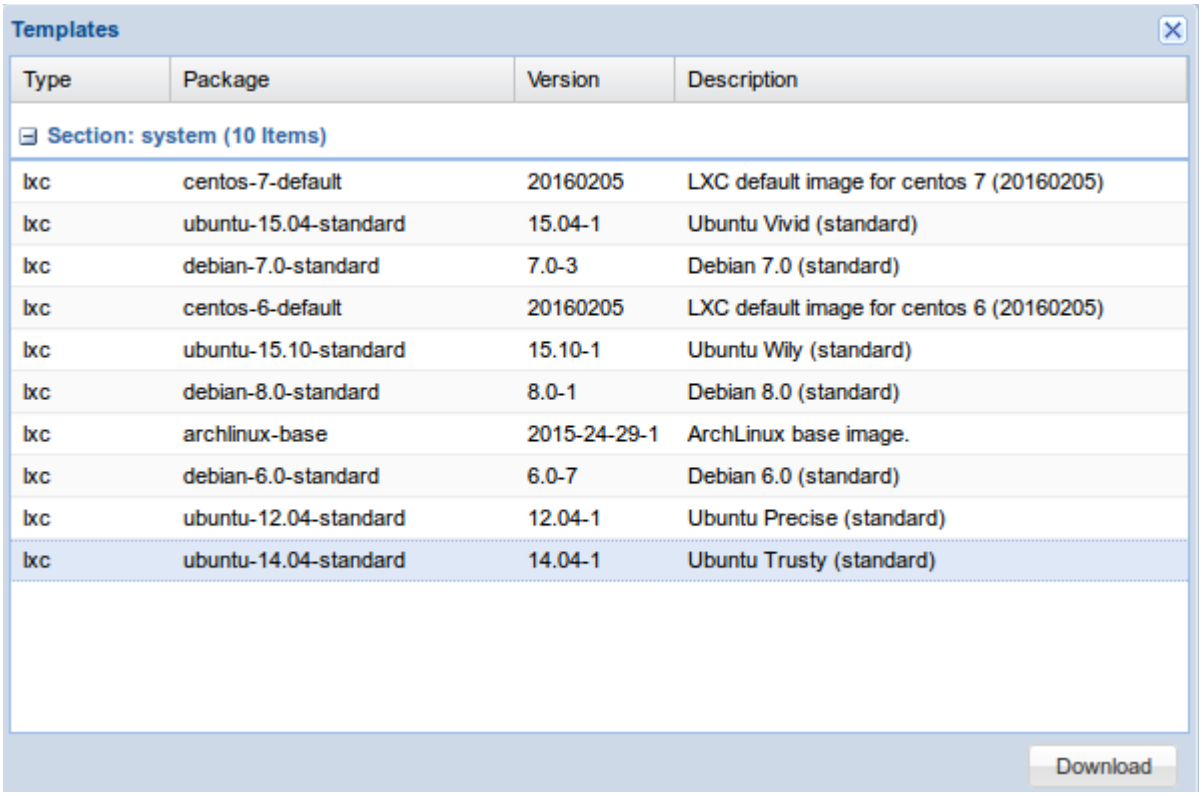
Quan ja tenim el directori per a les plantilles procedim a la seua descarrega seguint els passos que es detallen a continuació:

- Seleccionar en el panel de l'esquerra el directori on volem descarregar la plantilla:



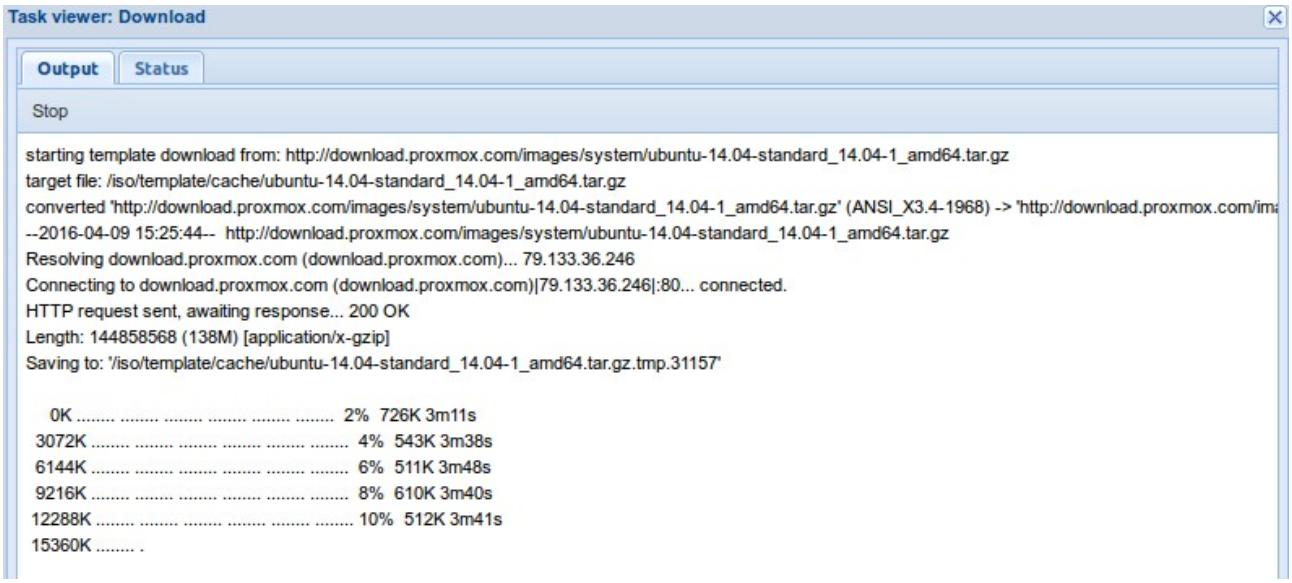
Il·lustració 2.42 Contingut directori

- Fer clic al botó **Templates**. Una llista de plantilles amb diferents distribucions Linux apareixerà. Seleccionar la que es vol instal·lar i fer clic en **Download.**



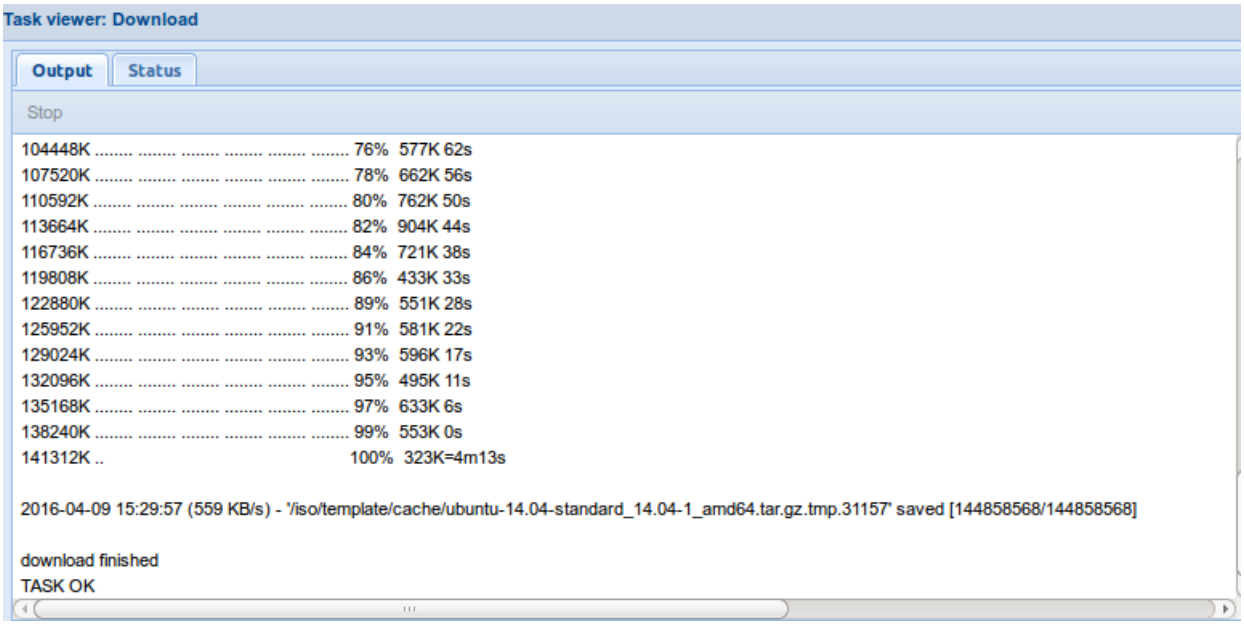
Il·lustració 2.43 Llista plantilles contenidors

El procés de descarrega començarà.



Il·lustració 2.44 Descàrrega plantilla

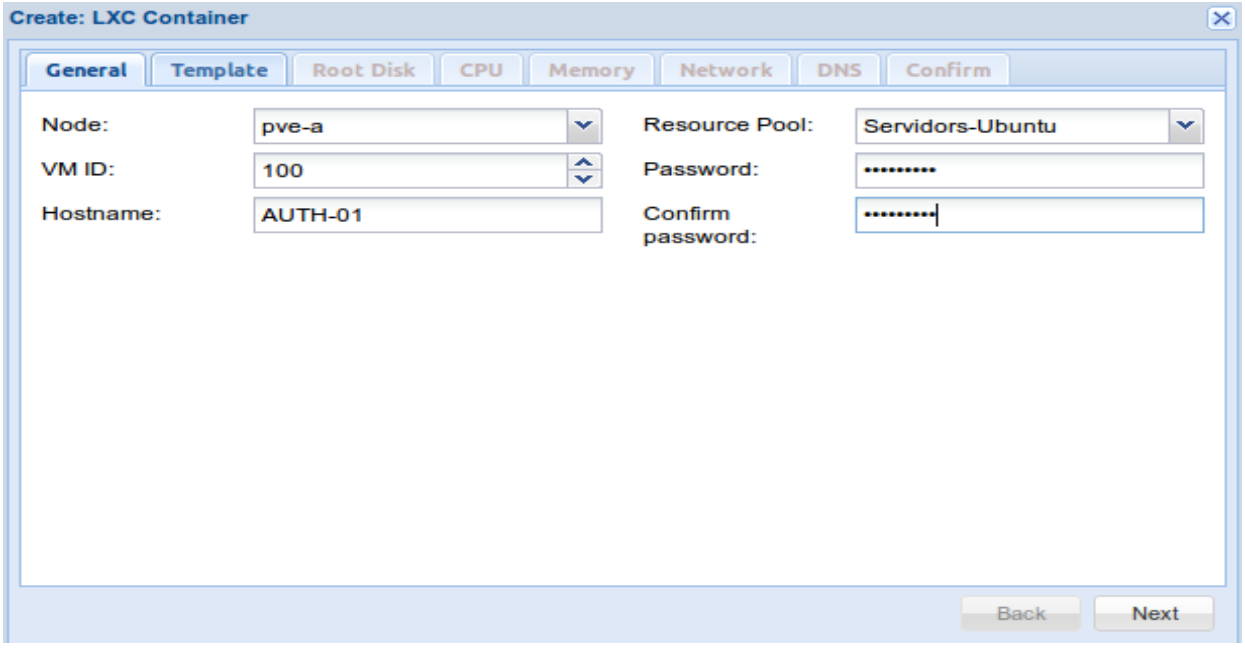
- Quan finalitze tancar la finestra de descarrega. La plantilla estarà visible a la llista de imatges ISO i plantilles.



Il·lustració 2.45 Descàrrega plantilla completada

Ara que ja està la plantilla descarregada al sistema podrem crear un contenidor emprant aquesta plantilla seguint les següents instruccions:

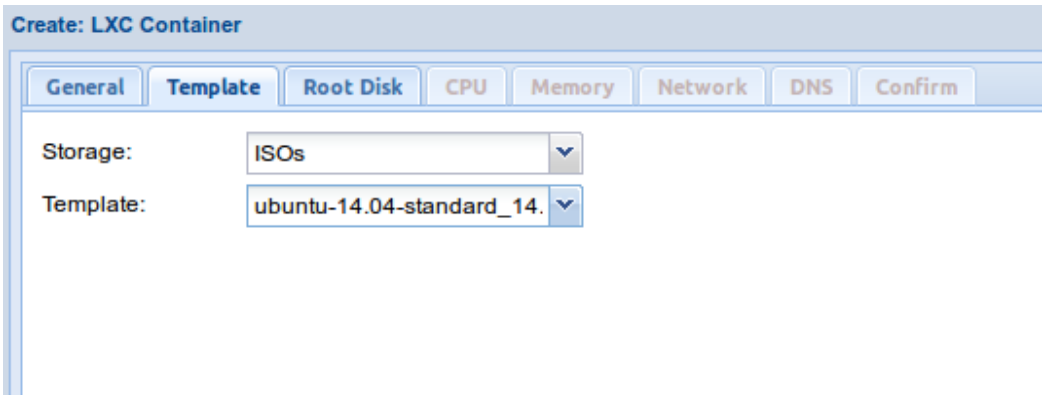
- Fer clic en el botó **Create CT** que es pot localitzar a la part superior dreta de la interfície d'administració. La finestra per a crear el contenidor apareixerà. En la primera pestanya plenarem la informació corresponent al node on volem crear el contenidor, el id que volem assignar-li al contenidor, el nom del contenidor, el nom del grup de recursos al que volem assignar el contenidor i la contrasenya del usuari root del contenidor.



Il·lustració 2.46 Creació contenidor. Pestanya: General

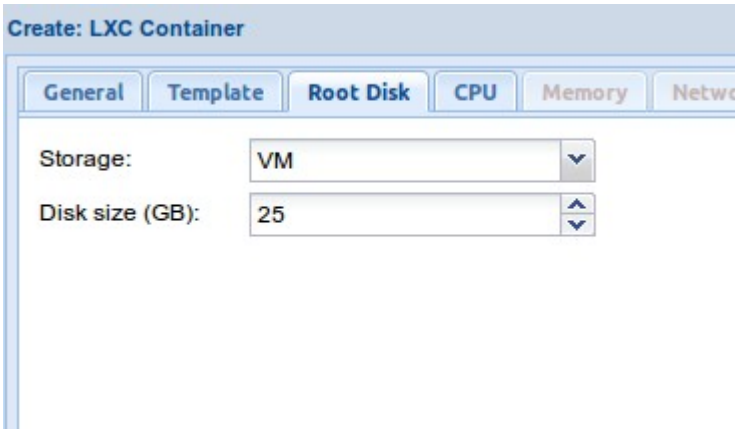
El camp **Resource pool** que correspon amb el grup de recursos al que volem assignar el contenidor és opcional. Els grups de recursos és una manera visual d'organitzar les nostres màquines virtuals i contenidors. La resta de camps són obligatoris.

- En la segon pestanya podrem elegir la plantilla a emprar per a desplegar el contenidor.



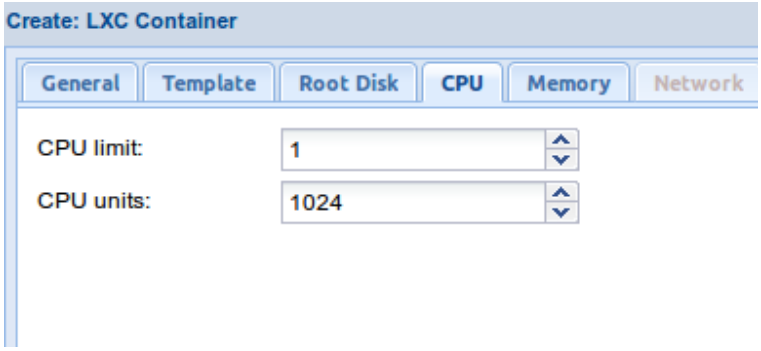
Il·lustració 2.47 Creació contenidor. Pestanya: Template

- En la tercera pestanya seleccionarem el directori on volem emmagatzemar. el contenidor i la mida del disc. En aquesta pestanya és important no seleccionar un directori local si volem que aquest contenidor tinga característiques d'alta disponibilitat



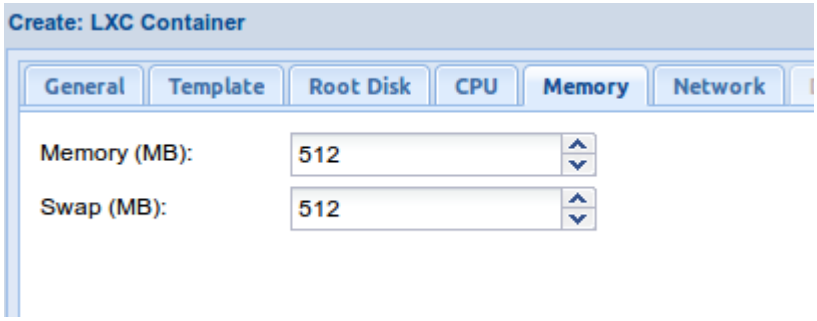
Il·lustració 2.48 Creació contenidor. Pestanya:Root Disk

- En aquesta pestanya escollirem la quantitat de CPUs que volem signar al contenidor.



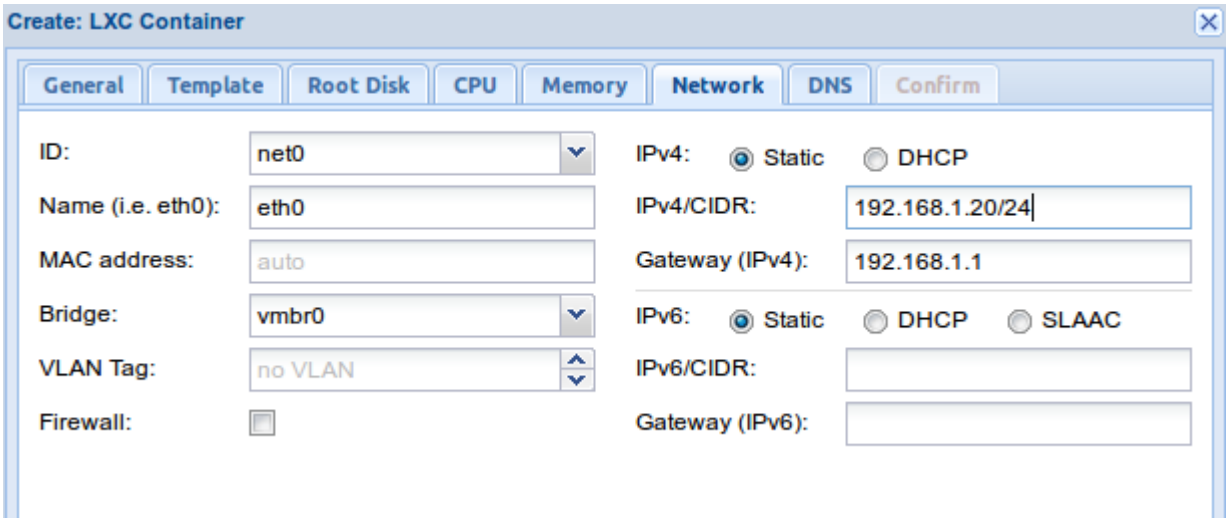
Il·lustració 2.49 Creació contenidor. Pestanya:CPU

- En aquesta cinquena pestanya definirem tant la memòria del contenidor com la mida de la partició swap.



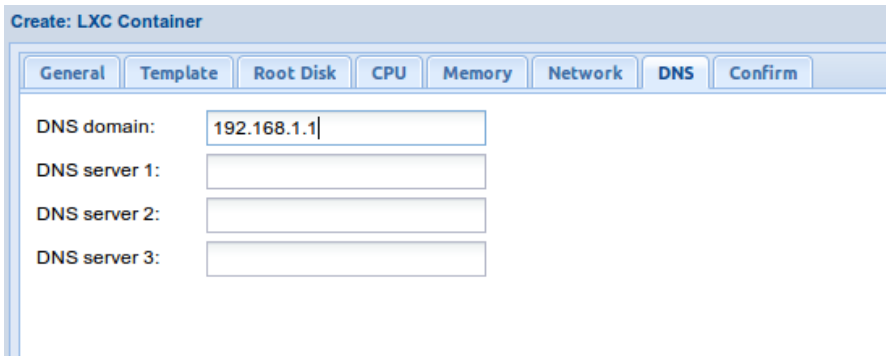
Il·lustració 2.50 Creació contenidor. Pestanya:Memory

- A continuació configurarem les opcions de la interfície de xarxa. Proxmox soporta VLAN a més de poder configurar la opció de tallafocs.



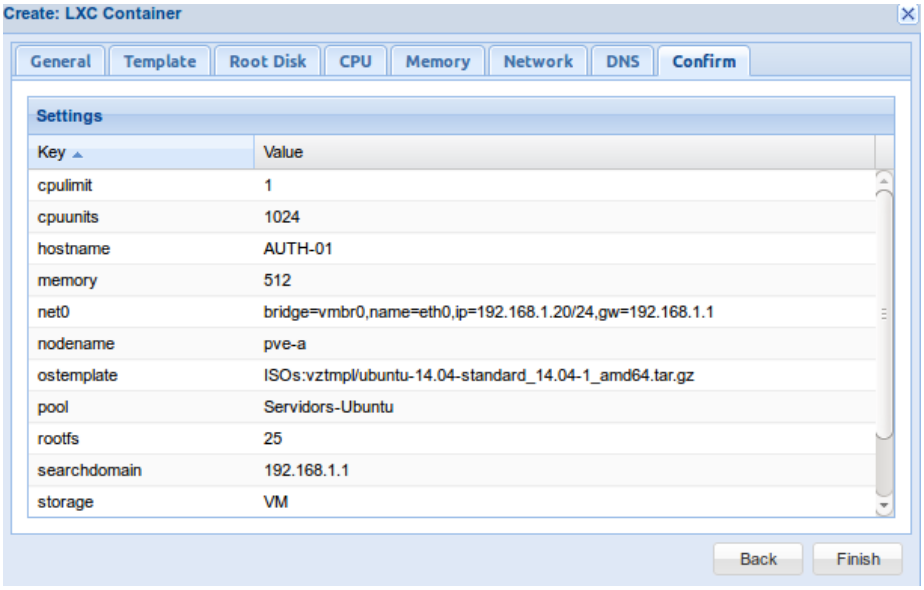
Il·lustració 2.51 Creació contenidor. Pestanya:Network

- Per últim configurarem els servidors DNS per al contenidor:

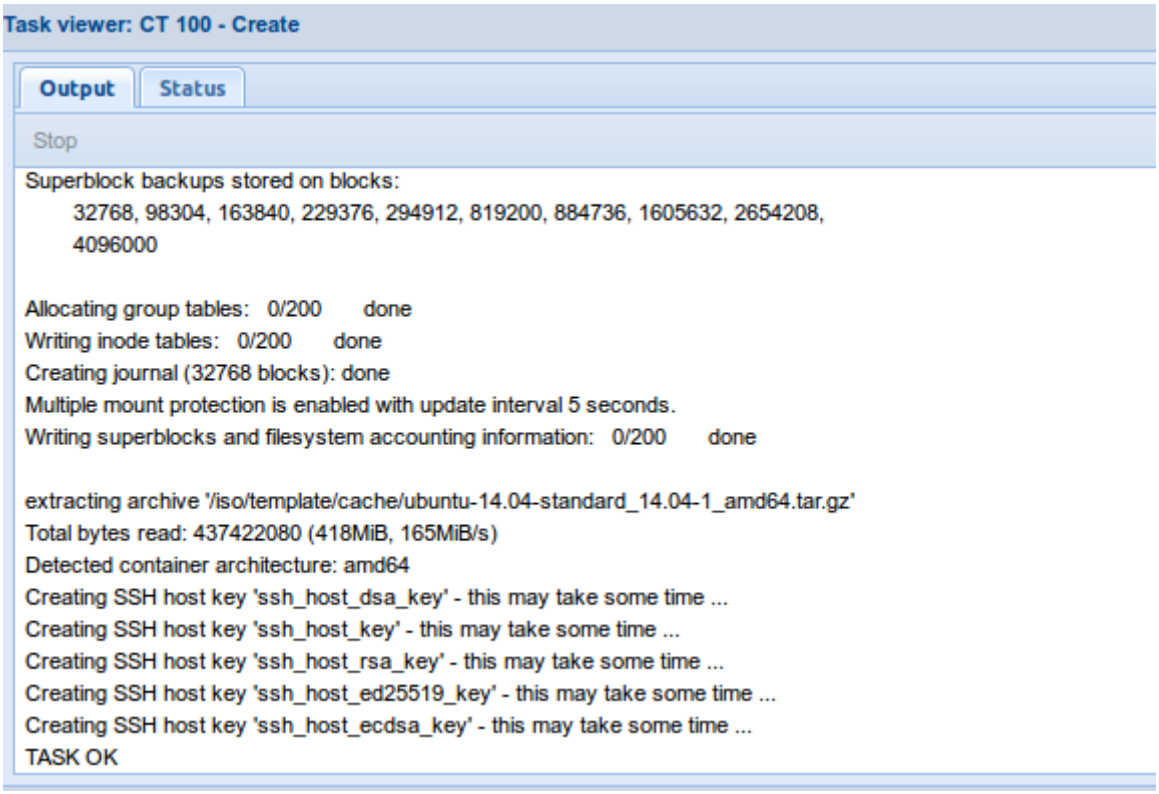


Il·lustració 2.52 Creació contenidor. Pestanya: DNS

- L'assistent mostrarà un resum de totes les opcions seleccionades. Si tot és correcte polsant en el botó **Finish** el procés de creació començarà. En qualsevol pas d'aquest assistent podem tornar enrere polsant **Back** per a canviar algun dels paràmetres configurats.

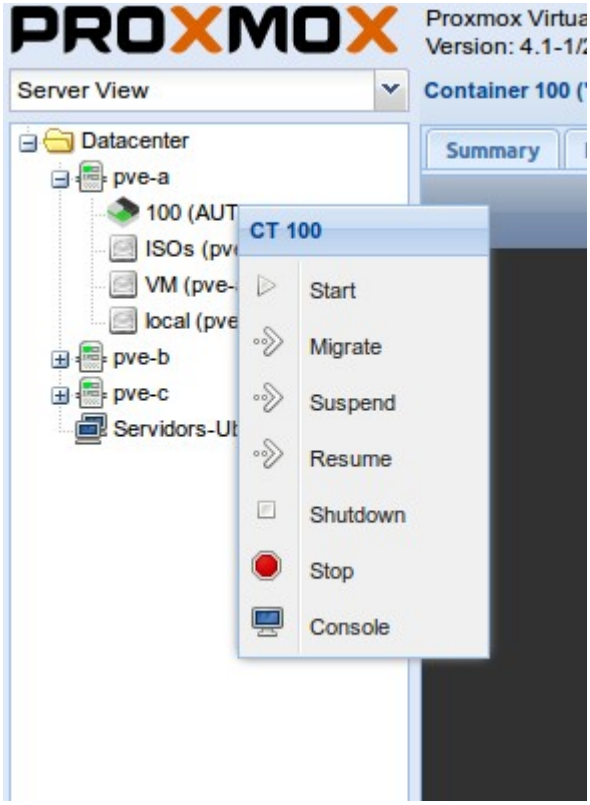


Il·lustració 2.53 Creació contenidor. Pestanya: Confirm



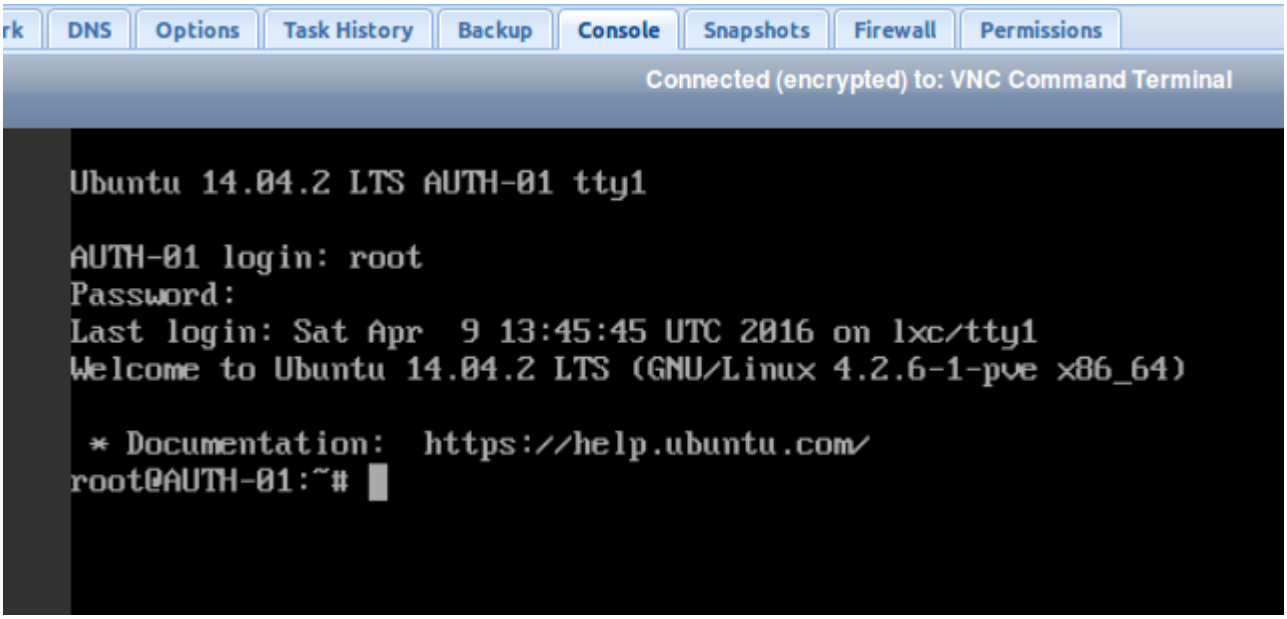
Il·lustració 2.54 Creació contenidor

Quan el procés de creació acaba, simplement tancuem la finestra. En la part esquerra de l'interfície d'administració podem trobar el nostre contenidor davall el node del cluster on l'hem creat. Per arrancar-lo farem clic amb el botó dret del ratolí i en el menú contextual pressionarem **Start.**



Il·lustració 2.55 Inici contenidor

Seleccionant la pestanya Console en el panel central de la interfície d'administració accedirem a la consola **NoVNC** que ens permetrà començar a treballar en el contenidor.



Il·lustració 2.56 Consola contenidor

3. Autenticació d'usuaris

En aquest capítol es presenta la solució d'autenticació d'usuaris escollida. Es fa una breu introducció del programari emprat així com una guia pas a pas de instal·lació i configuració. També s'explica com configurar un client Linux per a que s'autentica amb el servidor proposat.

3.1 OpenLDAP

LDAP (Lightweight Directory Access Protocol) és un protocol d'aplicació estàndard al mercat per accedir i mantindre serveis d'informació de directori distribuïts. Els serveis de directori permeten compartir informació sobre usuaris,sistemes, xarxes, serveis i aplicacions a través d'una xarxa. Com a exemple, els serveis de directori poden oferir qualsevol conjunt de registres, a sovint organitzats jeràrquicament, com ara un directori de correu electrònic corporatiu o un directori de telèfons.

En definitiva, LDAP facilita la creació de bases de dades jerarquitzades per emmagatzemar informació que pot ser compartida i accessible des d'una xarxa.
Amb aquestes característiques, és fàcil esbrinar que un del usos comuns d'un directori LDAP és proveir un magatzem central d'usuaris i contrasenyes. Açò permet diferents aplicacions i serveis connectar-se amb el servidor LDAP per a validar usuaris. Com a principal benefici, ofereix la possibilitat de tindre un lloc centralitzat on actualitzar informació d'un usuari incluint la seua contrasenya.

El protocol proporciona una interfície amb directoris que segueix la edició de 1993 del model X.500:

- Un registre consisteix en un conjunt d'atributs
- Un atribut té nom, tipus d'atribut i descripció d'atribut i un o més valors. Els atributs es defineixen al esquema.
- Cada registre té un identificador únic: el seu DN (Distringuished Name). El DN consisteix en el seu RDN (Relative Distringuished Name), construït amb alguns dels atributs del registre seguit del DN del seu registre pare. En termes de noms de fitxers, per a **/home/tiko/hola.txt**, el RDN seria **hola.txt.**

El DN d'un registre pot canviar si el registre es mou a una branca diferent de l'arbre. Per poder confiar que es troba el registre buscat, s'ha de proveir d'un Identificador Únic Universal (UUID per les seues sigles en anglés) al conjunt de atributs que formen el registre.

Aquest podria ser un exemple de registre LDAP:
dn: cn=Vicente Marti ,dc=local,dc=lab
cn: Vicente Marti
givenName: Vicente
sn: Marti
telephoneNumber: 611 111 111
telephoneNumber: +611 111 111
mail: tiko@local.lab
manager: cn=Juan Martinez,dc=local,dc=lab
objectClass: inetOrgPerson
objectClass: organizationalPerson

objectClass: person
objectClass: top

OpenLDAP és una implementació de programari lliure de LDAP. Desenvolupat per OpenLDAP Project va ser alliberat baix una llicencia de estil BSD anomenada OpenLDAP Public License. Atés que LDAP és un protocol independent de la plataforma, OpenLDAP esta disponible tant per a distribucions Linux com per a altres plataformes com Microsoft Windows, OS X o Solaris.

OpenLDAP es compon dels següents elements:

- **slapd:** el dimoni LDAP i els seus mòduls i eines associades.
- **Llibreries implementant el protocol LDAP i el Basic Encoding Rule(BER)** que són les només emprades per codificar la informació transmesa
- **Les utilitats de client com ara ldapsearch, ldapadd,ldapdelete i altres.** Aquests utilitats serveixen per a gestionar el servidor OpenLDAP des d'una terminal

3.2 Instal·lació i configuració del servidor OpenLDAP

Per a poder utilitzar SAMBA per autenticar usuaris primer hem d'instal·lar OpenLDAP com a backend. En les pròximes seccions s'explica la instal·lació d'ambdós i la configuració d'un client Linux per a que s'autentique amb el servidor.

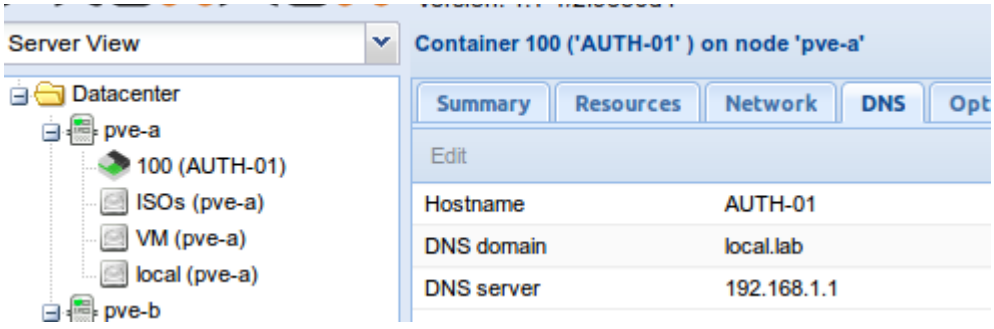
La instal·lació de OpenLDAP i Samba per a aquest projecte es fa sobre un contenidor Ubuntu 14.04.

3.2.1 Configuració de OpenLDAP

La instal·lació de OpenLDAP es realitza instal·lant el paquet slapd que conté el OpenLDAP server daemon. També és important instal·lar el paquet ldap-utils per tindre totes les eines necessàries per configurar OpenLDAP. La instal·lació de slapd crearà una configuració funcional. Entre d'altre coses crearà una instancia en la base de dades per a emmagatzemar la informació. Aquesta instancia tindrà com a sufix o base DN el nom de domini del servidor. Per aquest motiu és important revisar aquesta configuració abans de començar la instal·lació.

Es pot comprovar el nom de domini de dues maneres:

- A la interfície web de Proxmox, seleccionar el contenidor en el panel de l'esquerra i fent clic en la pestanya DNS. El valor del camp **DNS domain** deuria ser el del domini de la màquina(al exemple local.lab). En cas de no ser correcte i voler modificar-lo bastara amb fer doble clic en el camp i modificar-lo



Il·lustració 3.1 Nom del domini

- També es pot canviar al terminal del contenidor. Per a fer açò executar la instrucció sudo nano **/etc/hosts** . L'arxiu ha de contindre la següent línia:

  IP Contenidor NomdelaMàquina.domini NomdelaMàquina

```
tiko@AUTH-01:~$ sudo cat /etc/hostname
AUTH-01
tiko@AUTH-01:~$ sudo cat /etc/hosts
127.0.0.1       localhost
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.168.1.20 AUTH-01.local.lab AUTH-01
tiko@AUTH-01:~$
```

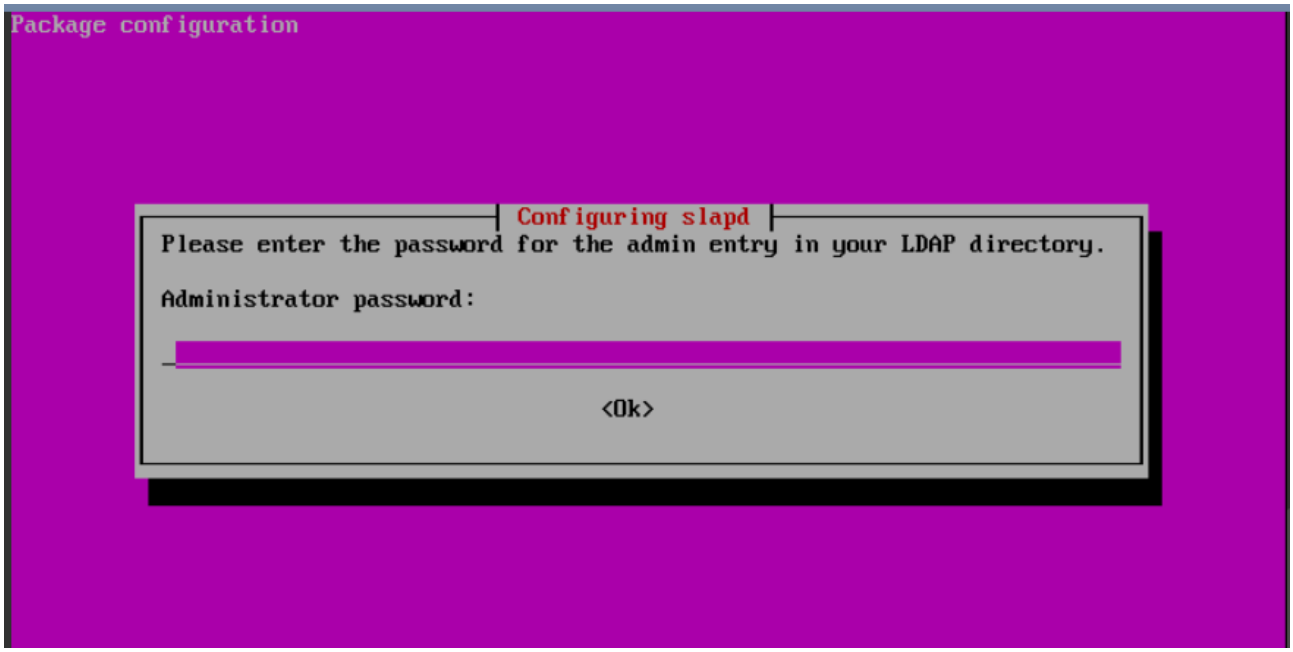
Il·lustració 3.2 Arxiu /etc/hosts

Ara que el nom del domini ja esta configurat correctament, instal·lar slapd i ldap-utils executant la instrucció ***«sudo apt-get install slapd ldap-utils -y»***

```
tiko@AUTH-01:~$ sudo apt-get install slapd ldap-utils -y
```

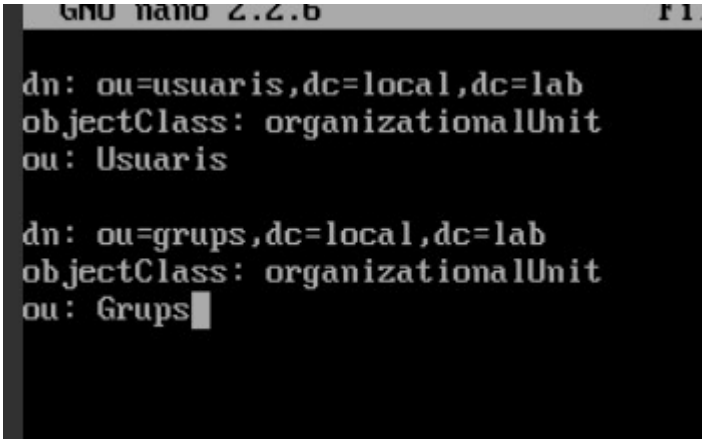
Il·lustració 3.3 Instal·lació OpenLDAP

Com ja s'ha esmentat, slapd és autoconfigurable i al acabar la instal·lació ens demanarà establir la contrasenya de l'usuari admin.



Il·lustració 3.4 Establir contrasenya del usuari admin en OpenLDAP

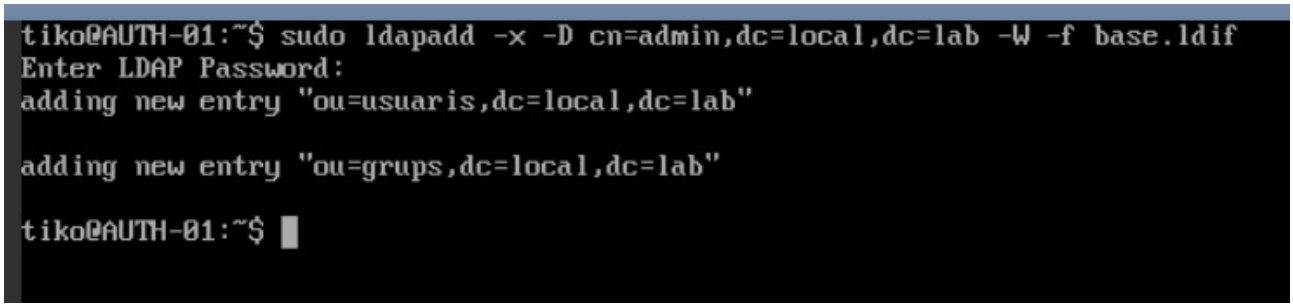
Ara és el moment de crear la estructura que es vol dins del servidor LDAP. Primerament crearem dues unitat organitzatives que poder ordenar millor els objectes dins de la base de dades. Crearem una unitat organitzativa per a usuaris i altra per a grups. En primer lloc, hi ha que crear un arxiu ldif com el que es mostra a la següent imatge amb la informació necessària per crear les unitats organitzatives:



Il·lustració 3.5 Exemple arxiu ldif: Creació OU

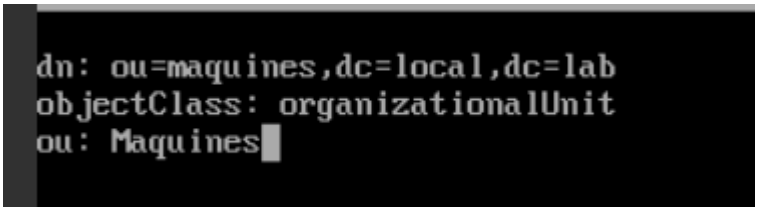
A continuació executant la instrucció ldapadd s'introdueix els objectes a la base de dades:

sudo ldapadd -x -D cn=admin,dc=local,dc=lab -W -f base.ldif

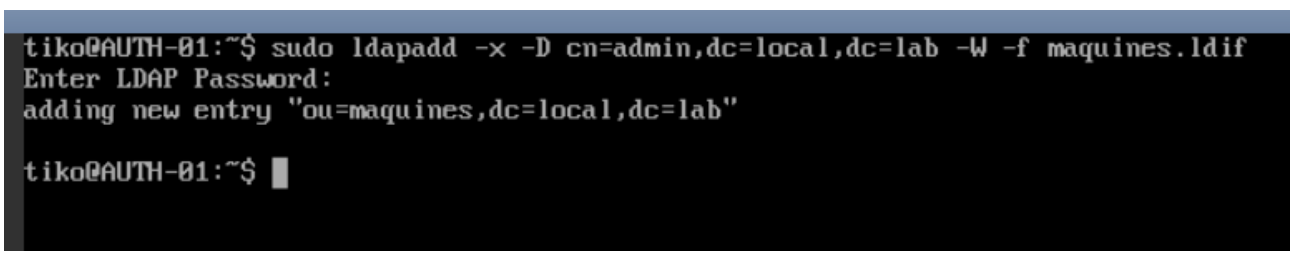


Il·lustració 3.6 Execució ldapadd

També crearem una unitat organitzativa per les màquines del nostre domini:



Il·lustració 3.7 Exemple arxiu ldif: Creació OU



Il·lustració 3.8 Execució ldapadd amb arxiu ldif

Per últim, afegirem un registre d'usuari a la base de dades. Per a fer-ho, hi ha que crear altre arxiu ldif amb la informació necessària tal i com es mostra a continuació a les imatges:

```
dn: uid=vmarti,ou=usuaris,dc=local,dc=lab
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: vmarti
sn: Marti
givenName: Vicente
cn: Vicente Marti
displayName: Vicente Marti
uidNumber: 2000
gidNumber: 10000
userPassword: 12345678
gecos: Vicente Marti
loginShell: /bin/bash
homeDirectory: /home/vmarti
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
```

Il·lustració 3.9 Exemple arxiu ldif: Creació usuari 1

```
shadowMax: 999999
shadowLastChange: 10877
mail: vmarti@local.lab
postalCode: 46021
o: local
initials: vm
```

Il·lustració 3.10 Exemple arxiu ldif: Creació usuari 2

Per introduir l'usuari a la base de dades executar de nou la instrucció ldapadd amb el arxiu que conté la informació de l'usuari:

sudo ldapadd -x -D cn=admin,dc=local,dc=lab -W -f usuaris.ldif

```
tiko@AUTH-01:~$ sudo ldapadd -x -D cn=admin,dc=local,dc=lab -W -f usuaris.ldif
Enter LDAP Password:
adding new entry "uid=vmarti,ou=usuaris,dc=local,dc=lab"

tiko@AUTH-01:~$
```

Il·lustració 3.11 Execució ldapadd amb arxiu ldif

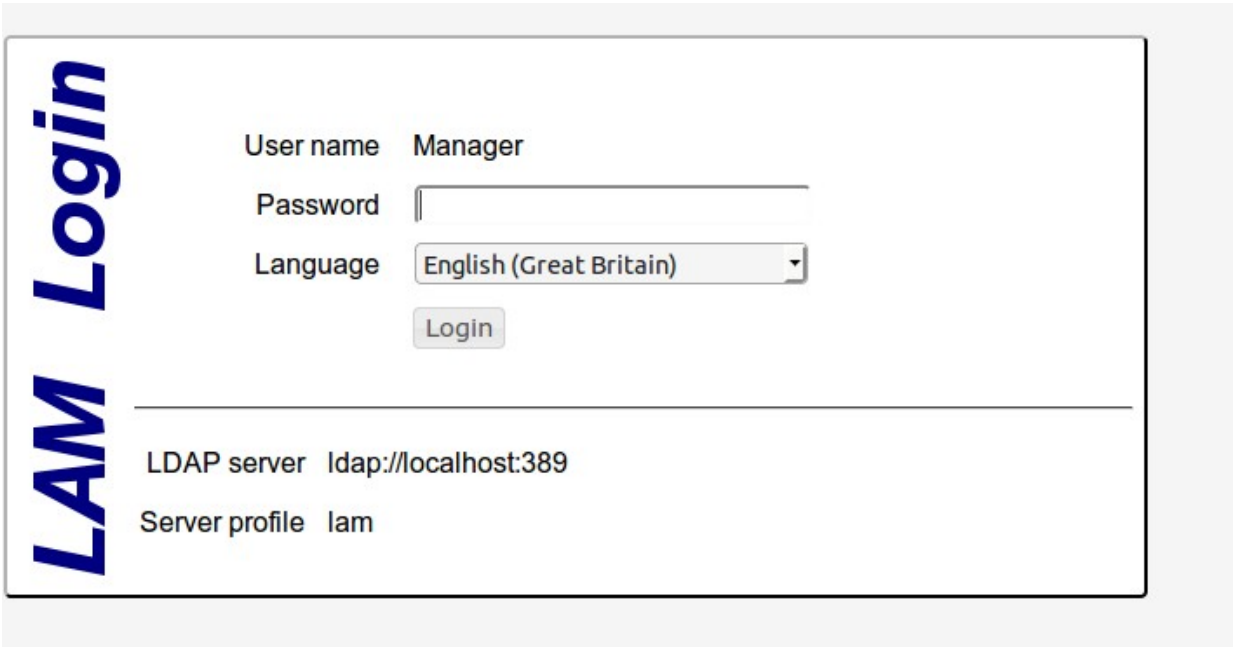
3.2.2 Instal·lació de LAM (LDAP Account Manager)

Atés que pot arribar a ser complicat gestionar OpenLDAP executant instruccions a una terminal, és recomanable instal·lar LAM (LDAP Account Manager) per a aquesta tasca. LAM és una interfície web que connecta amb el servidor LDAP i ajuda els administradors a crear, modificar i eliminar objectes en la base de dades.

Per instal·lar LAM, executar la instrucció ***sudo apt-get install ldap-account-manager -y***

Il·lustració 3.12 Instal·lació LAM

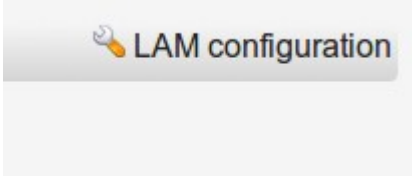
Quan finalitze la instal·lació podrem accedir a LAM mitjançant un navegador web en l'adreça https://IP_Maquina_Amb_LAM_Instal·lat/lam.



Il·lustració 3.13 Login LAM

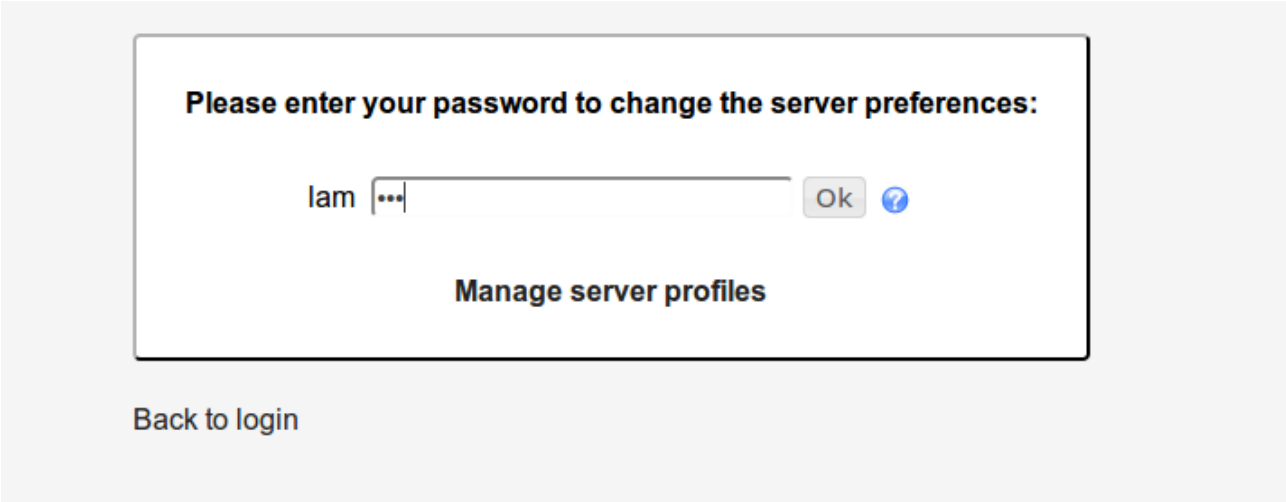
Per poder començar a utilitzar LAM cal configurar-lo perquè connecte correctament al nostre servidor LDAP seguint els següents passos:

- Accedir al configurador de LAM fent clic en l'enllaç que es pot trobar a la part superior dreta.



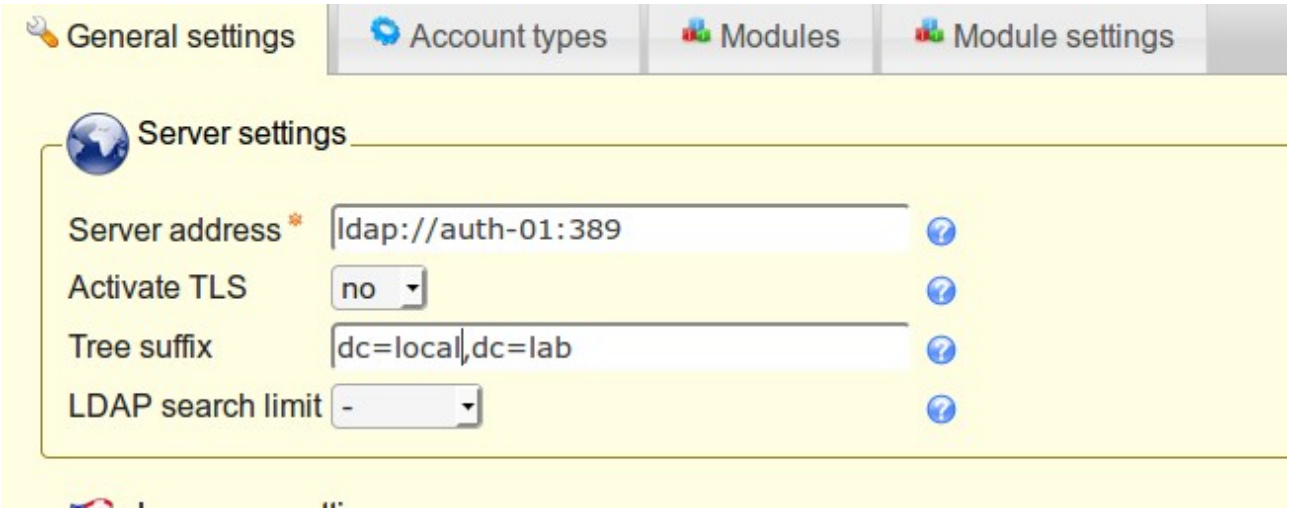
Il·lustració 3.14 Accés configuració LAM

- Fer inici de sessió en el gestor de perfils de LAM. La contrasenya per defecte és LAM



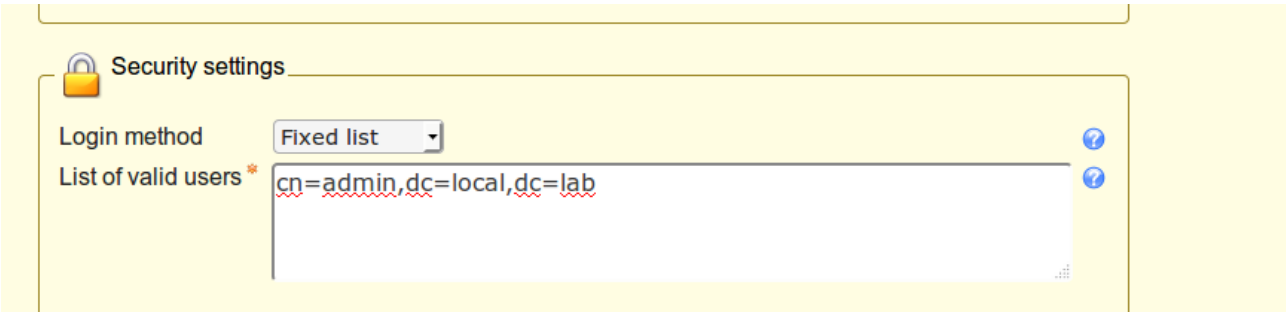
Il·lustració 3.15 Accés configuració LAM

- Modificar els camps server address amb la direcció del servidor ldap (podem utilitzar el nom del servidor si la màquina on esta LAM instal·lat sap resoldre'l. De no ser així utilitzar l'adreça IP) i el sufix del arbre (el nom del domini)



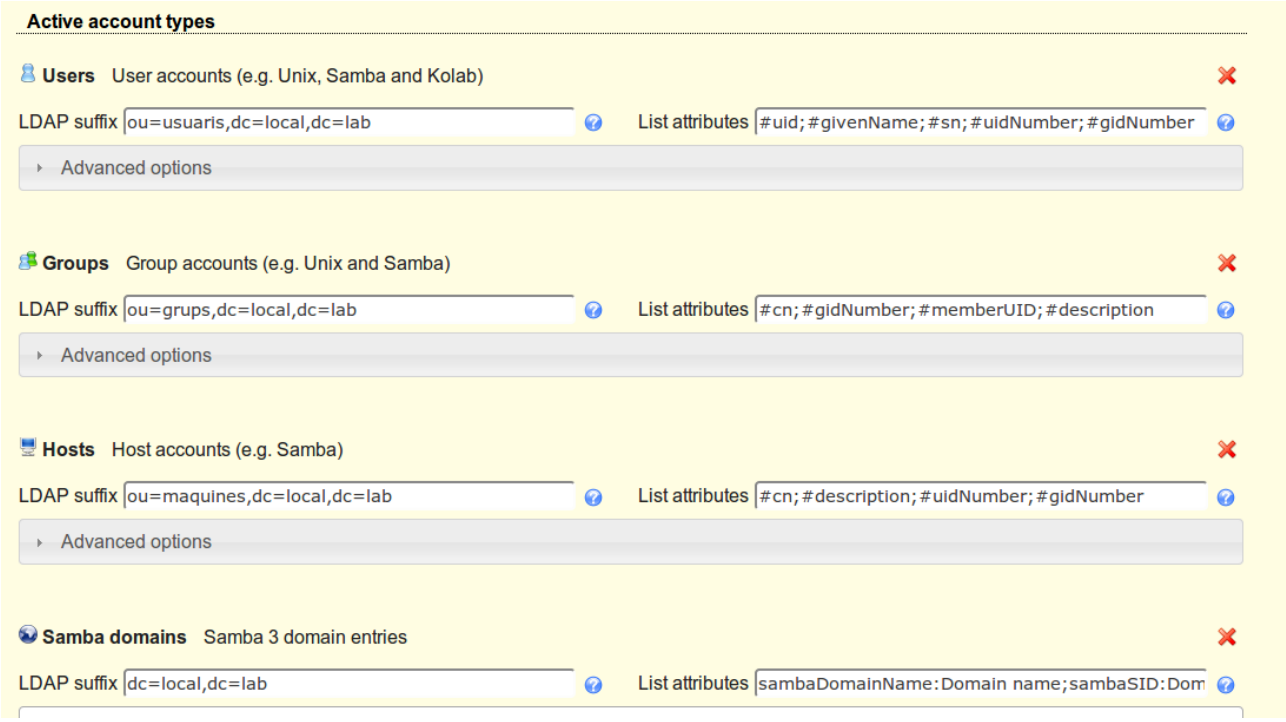
Il·lustració 3.16 Configuració paràmetres de servidor OpenLDAP en LAM

- A la ultima secció de la mateixa pantalla canviar el nom del usuari administrador del servidor LDAP.



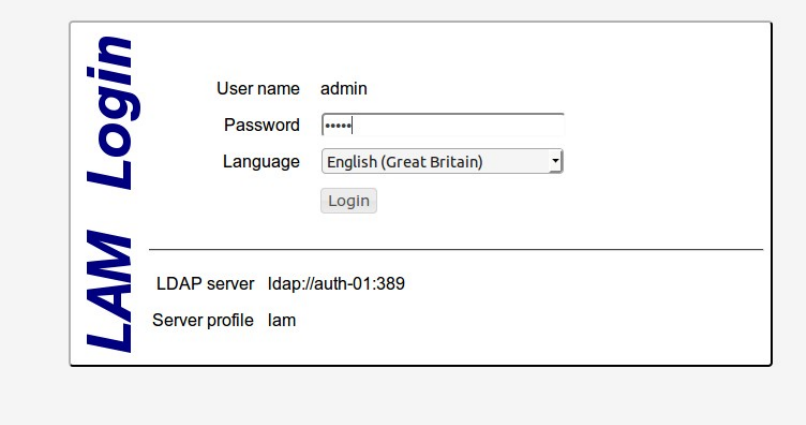
Il·lustració 3.17 Usuari administrador d'OpenLDAP

- En la pestanya **account types** modificar els sufixes LDAP amb el nom de les unitats organitzatives que s'han creat a la secció anterior per a cada tipus d'objecte.



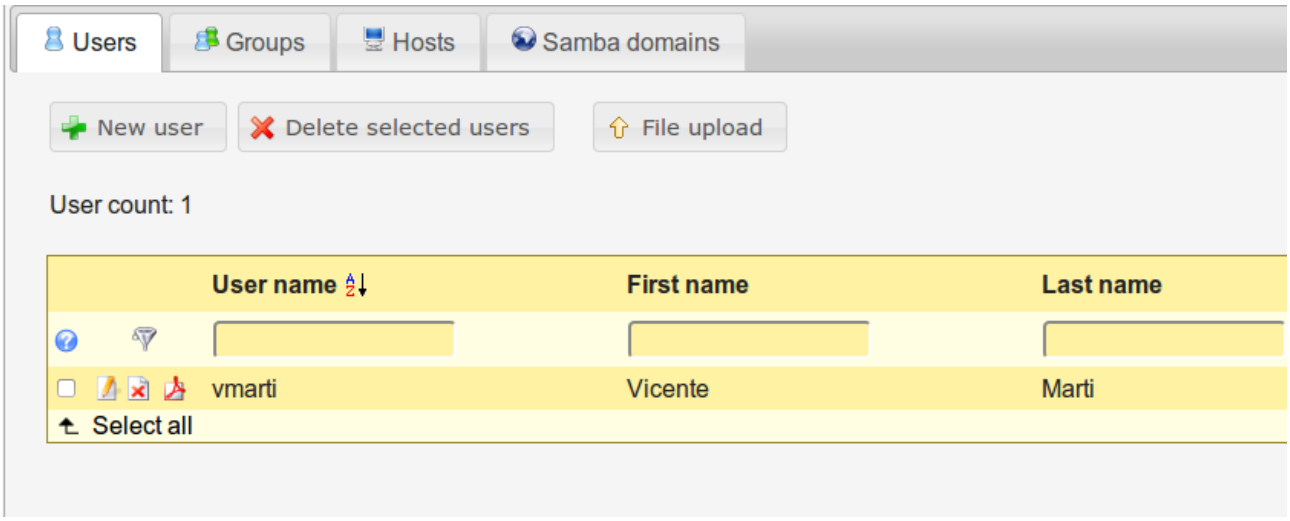
Il·lustració 3.18 OU per a cada tipus d'objecte

- Fer inici de sessió en LAM amb l'usuari administrador del servidor LDAP



Il·lustració 3.19 Login LAM

Si tot s'ha configurat correctament, veurem a la pestanya **Users** l'usuari creat a la secció anterior.

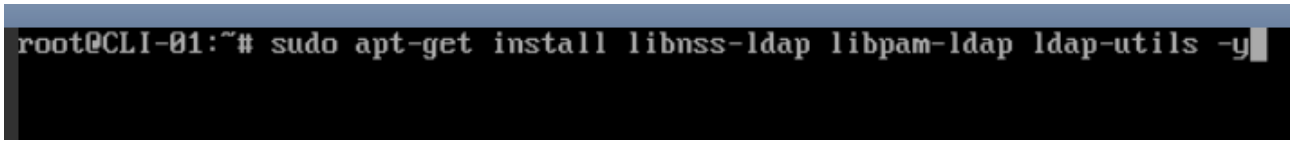


Il·lustració 3.20 Llista usuaris al servidor OpenLDAP

3.2.3 Configuració de client Linux per a autenticar amb LDAP

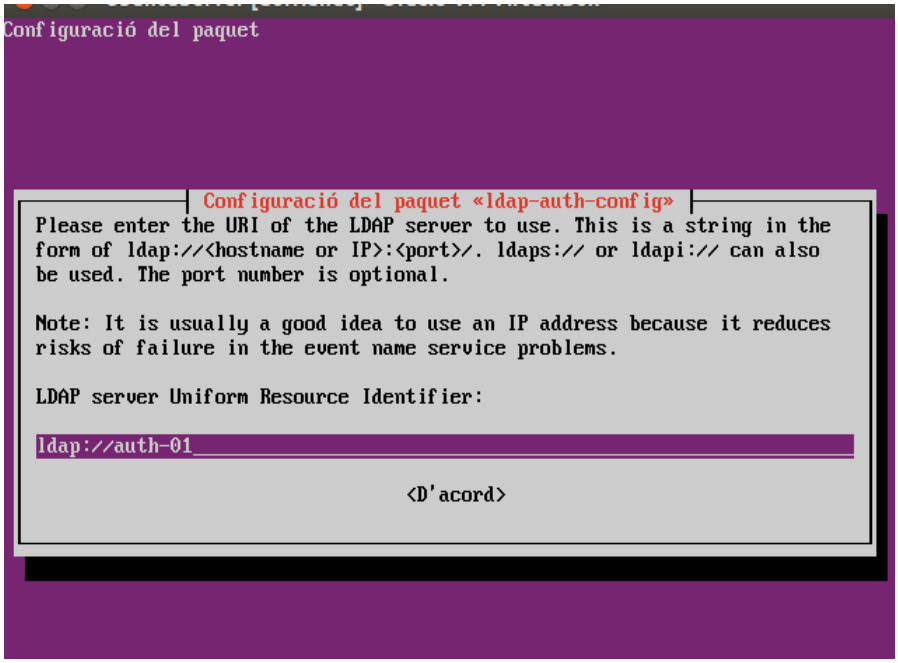
Per autenticar usuaris des de un client Linux[2] s'han de seguir els següents passos:

- Instal·lar els paquets libnss-ldap libpam-ldap i ldap-utils



Il·lustració 3.21 Instal·lació paquets per a màquina client

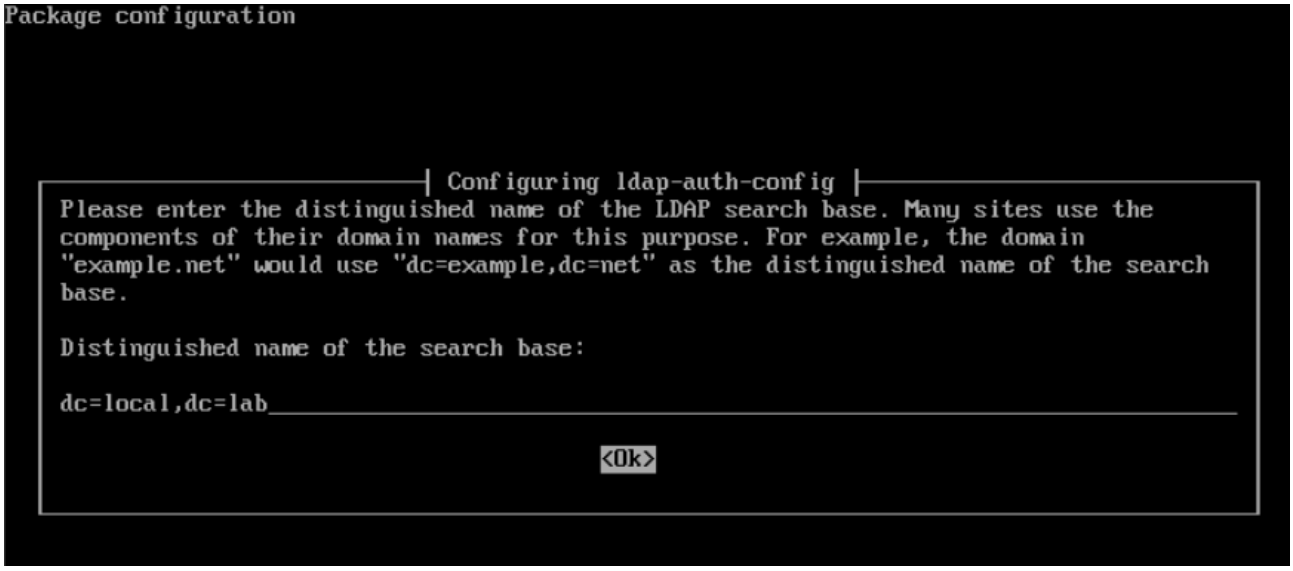
- Insertar el nom del servidor amb el següent format LDAP://Nom_del_servidor



Il·lustració 3.22 Establir direcció servidor OpenLDAP

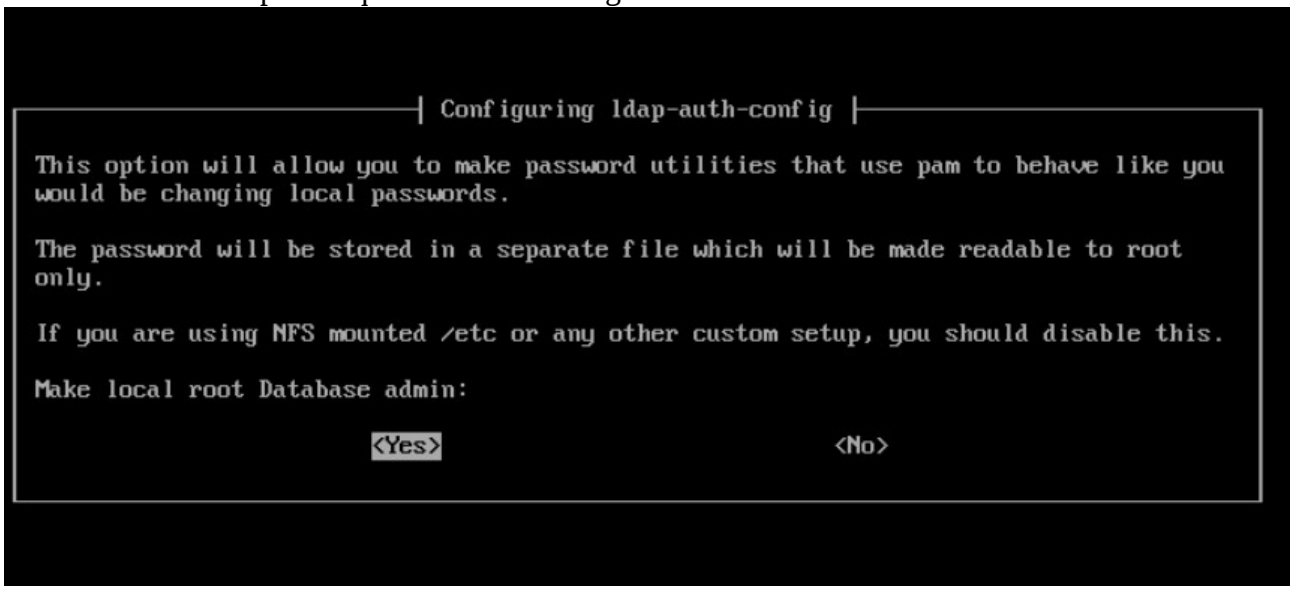
2 L'exemple està fet en Ubuntu. En altres distribucions amb altres escriptoris els noms dels paquets pot variar

- Modificar els valor del DN amb el nostre nom de domini



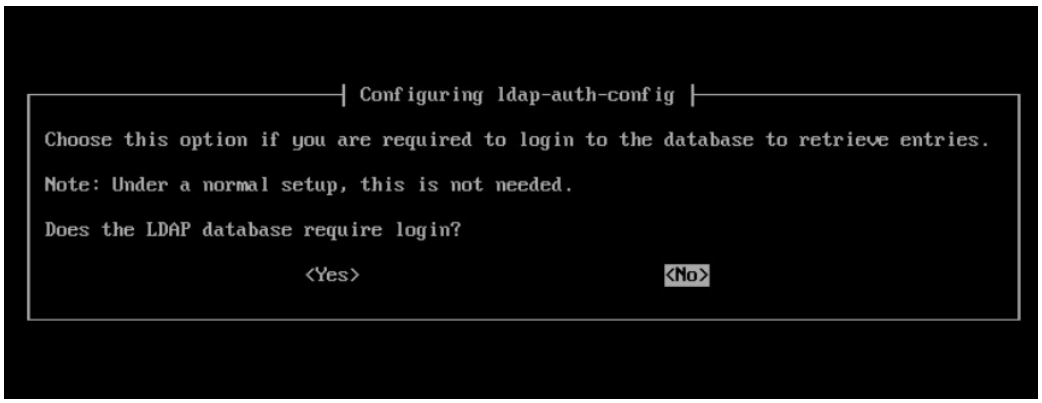
Il·lustració 3.23 Selecció de nom de domini

- Marcar Yes per fer que el usuari root siga administrador de la base de dades



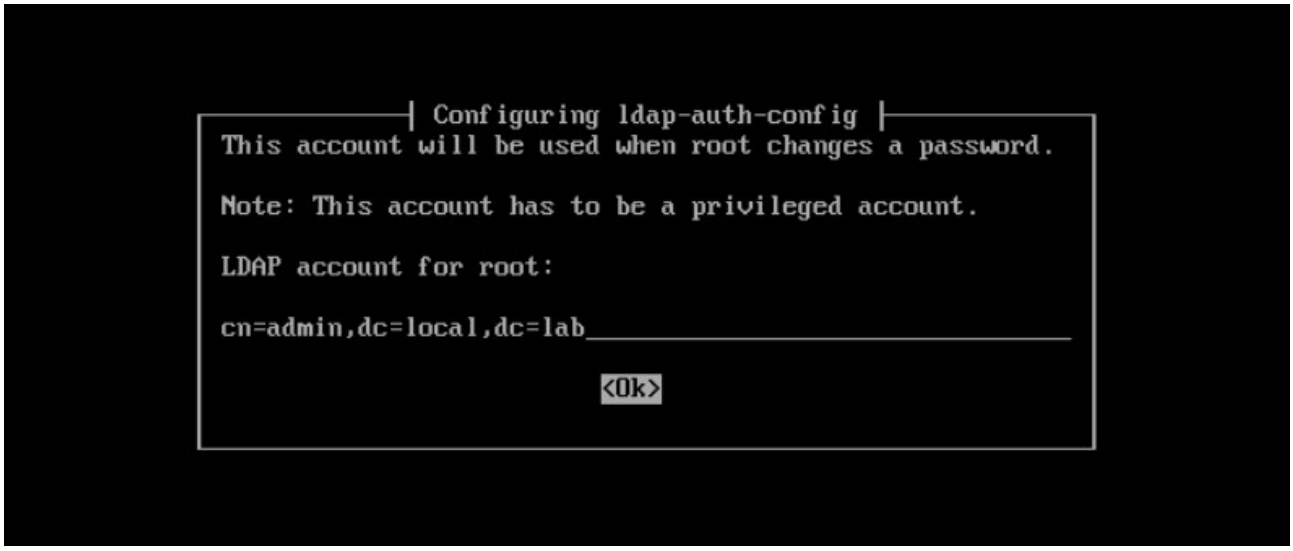
Il·lustració 3.24 Fer l'usuari root local administrador de la base de dades

- No és necessari que LDAP demane inici de sessió

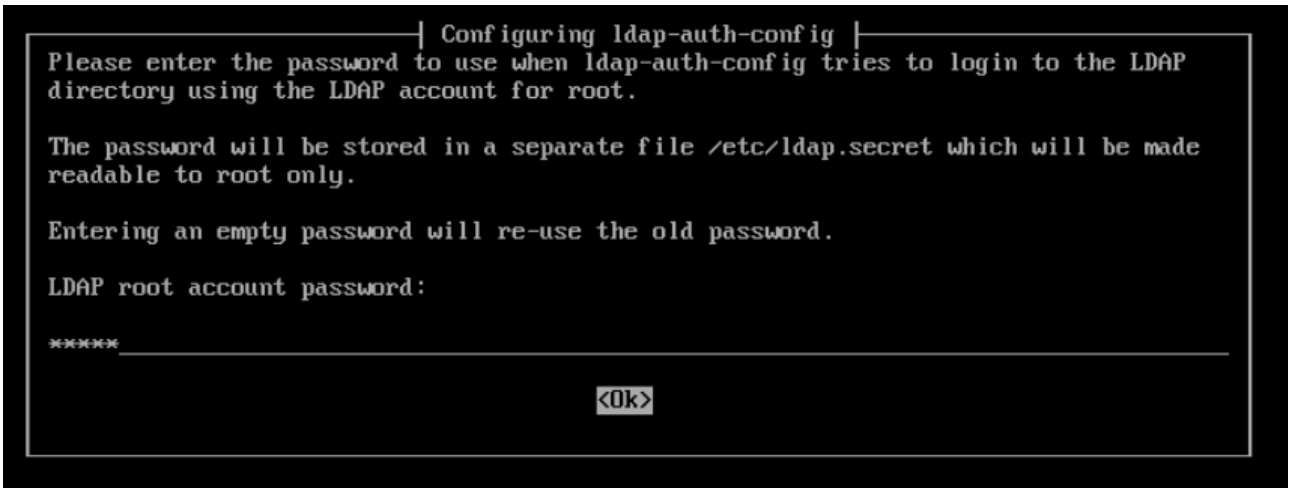


Il·lustració 3.25 Requerir Login a LDAP

- A la següent pantalla escriure el nom del usuari administrador de OpenLDAP en format LDAP. A continuació introduir la contrasenya



Il·lustració 3.26 Nom de l'usuari administrador d'OpenLDAP



Il·lustració 3.27 Contrasenya de l'usuari admin

- Modificar el fitxer **/etc/nsswitch.conf** afegint la paraula ldap al final de cada línia tal i com es mostra en la imatge.

Il·lustració 3.28 Configuració client per autenticació amb OpenLDAP 1

- Modificar l'arxiu **/etc/pam.d/common-password** esborrant a la línia 26 **use_authtok**

```
# here are the per-package modules (the "Primary" block)
password        [success=2 default=ignore]      pam_unix.so obscure sha512
password        [success=1 user_unknown=ignore default=die]     pam_ldap.so try_first_pass
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
```

Il·lustració 3.29 Configuració client per autenticació amb OpenLDAP 2

- Afegir la següent línia a **/etc/pam.d/common-session** :

  session optional pam_mkhomedir.so skel=/etc/skel umask=077

```
 GNU nano 2.4.2              File: /etc/pam.d/common-session

# The pam_umask module will set the umask according to the system defau
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessio
# See "man pam_umask".
session optional                        pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional                        pam_ldap.so
session optional        pam_systemd.so
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
```

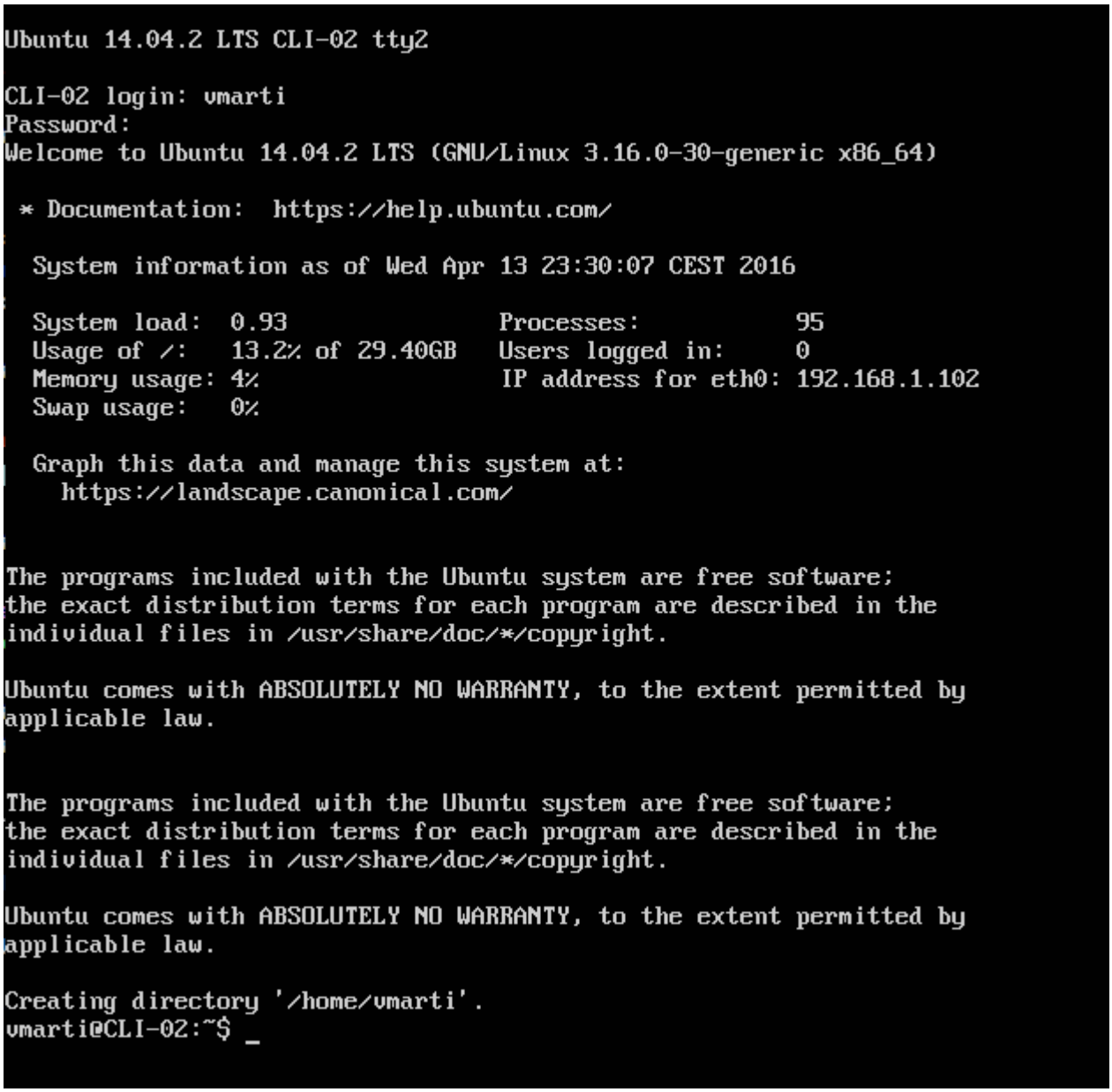
Il·lustració 3.30 Configuració client per autenticació amb OpenLDAP 3

- Reiniciar libnss-ldap amb la instrucció següent:

  sudo service libnss-ldap restart

```
tiko@UbuntuServer:~$ sudo service libnss-ldap restart
 * Running nssldap-update-ignoreusers...                          [ OK ]
tiko@UbuntuServer:~$ _
```

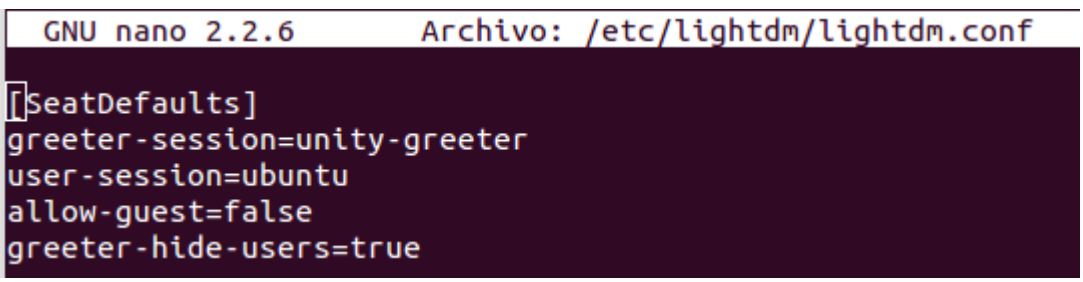
Il·lustració 3.31 Reiniciar servei libnss-ldap



Il·lustració 3.32 Exemple inici de sessió amb LDAP

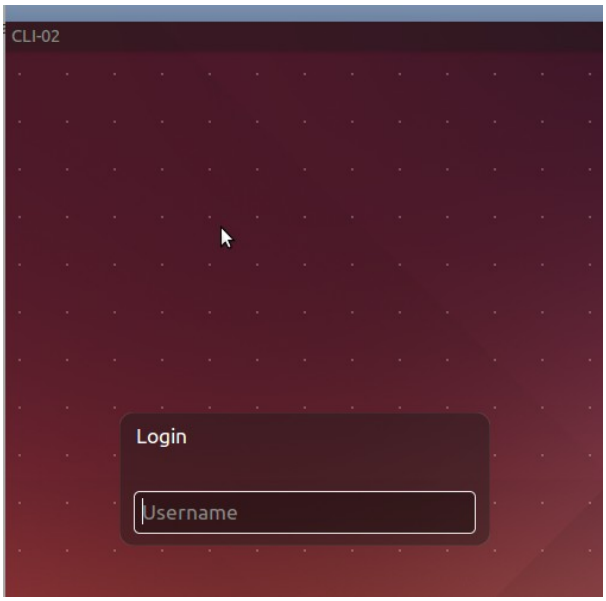
Ara ja podem tancar la sessió i tornar a iniciar-la amb l'usuari creat al servidor LDAP en seccions anteriors.

Per poder iniciar sessió autenticant els usuaris amb el servidor LDAP en l'entorn gràfic cal modificar l'arxiu **/etc/lightdm/lightdm.conf** (si no existeix hi haurà que crear-lo) tal i com mostra l'imatge

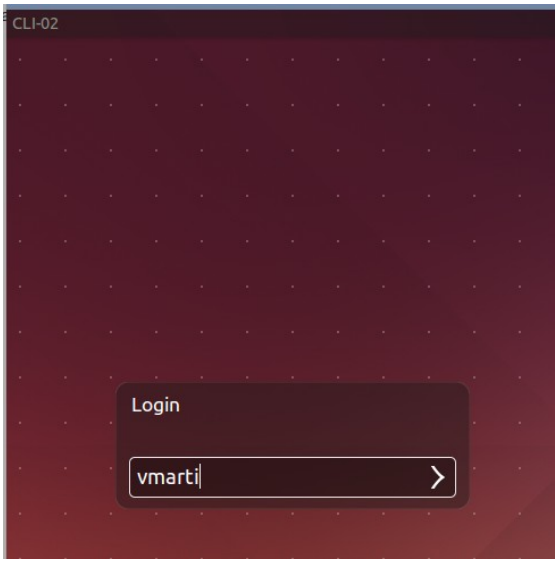


Il·lustració 3.33 Configuració Ubuntu per Login gràfic amb LDAP

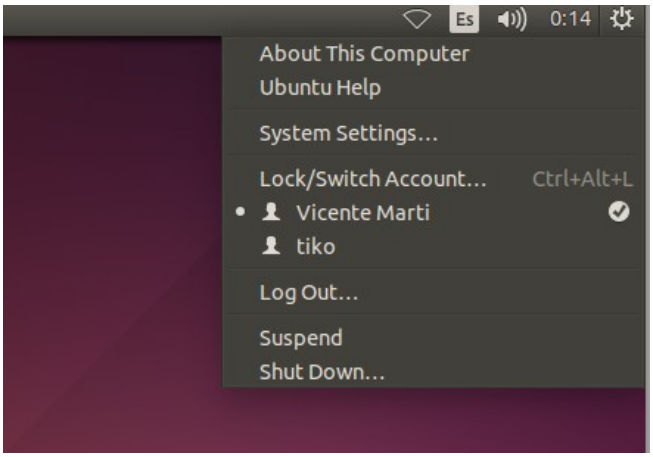
Després de reiniciar la màquina, ja serà possible iniciar la sessió amb els usuaris LDAP.



Il·lustració 3.34 Login Ubuntu amb LDAP 1



Il·lustració 3.35 Login Ubuntu amb LDAP 2



Il·lustració 3.36 Login Ubuntu amb LDAP 3

4. Servei de noms (DNS)

En aquesta secció s'explica què és un servidor de noms, quina és la seua utilitat i el seu funcionament. Per últim es detalla pas a pas la instal·lació del servidor de noms escollit per a aquest projecte.

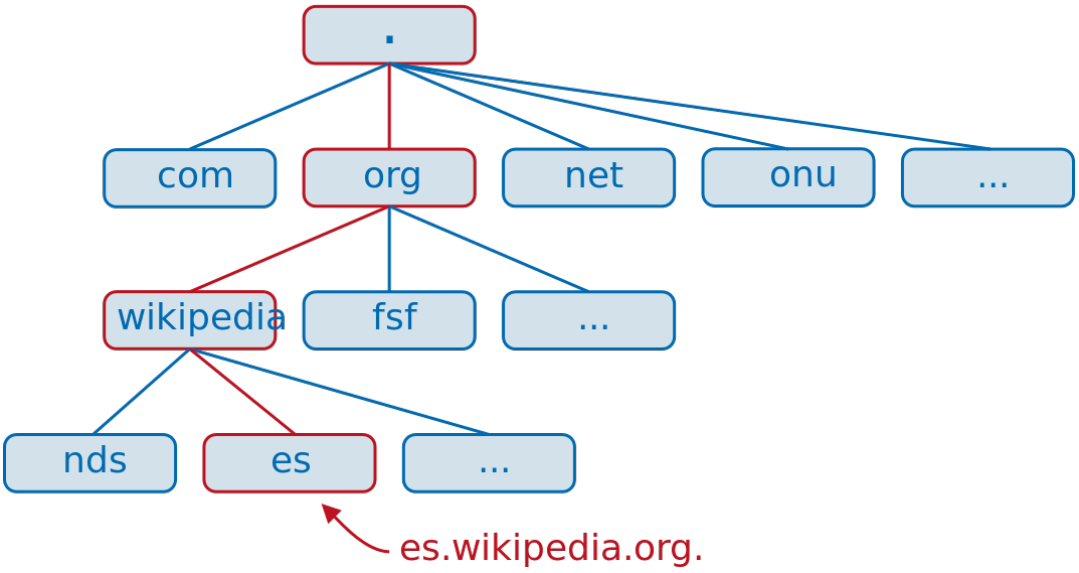
4.1 Què és DNS?

DNS són les sigles en anglés de sistema de noms de domini (Domain Name System). DNS és un sistema jeràrquic de nomenclatura per dispositius connectats a un xarxa, tant pública (Internet) com privada (un xarxa local a una organització per exemple). DNS utilitza una base de dades distribuïda i jerarquitzada on emmagatzema noms de domini en xarxes.

Tot i que es pot emmagatzemar. diferents tipus d'informació a cada nom, de manera genèrica s'utilitza fonamentalment per a l'assignació de noms de domini a direccions IP i per a la localització de servidors de correu a cada domini entre d'altres. DNS és el sistema encarregat de fer que quan qualsevol utilitza l'adreça www.google.es al seu buscador, aquest siga capaç de traduir aquest nom a una direcció IP i trobar el servidor. D'aquesta manera, la direcció podria canviar però el nom continuaria.

4.1.1 Jerarquia DNS

Com ja s'ha mencionat al punt anterior DNS és un sistema jeràrquic, és a dir, l'espai de noms té estructura d'arbre. Les fulles d'aquest arbre o nodes són els passos intermitjans d'un camí. Aquest camí comença al nivell més elevat que és punt. Aquest que normalment no s'inclou a les adreces és purament formal. Per tant l'adreça es.wikipedia.org. comença per aquest punt i va baixant l'arbre de node en node a org seguit de wikipedia i acabant en es.



Il·lustració 4.1 Diagrama jerarquia de noms DNS.

Quan qualsevol aplicació vol resoldre una direcció, primerament consulta la memòria cau local del dispositiu. Si l'adreça no està enviarà la petició al o els servidors DNS que tingui configurats la interfície de xarxa. Si aquest servidor o servidors no tenen l'adreça en la seua memòria cau o en la

seua base de dades perquè no són propietaris de zona, el servidor farà una consulta recursiva fins arribar al servidor DNS que tinga autoritat sobre la zona cercada. Quan rep la resposta, la emmagatzema a la seua memòria cau i retorna la resposta al client.

4.1.2 Tipus de servidors DNS

Hi ha tres tipus de servidors DNS:

- **Servidor primari o mestre:** Aquest servidor guarda informació sobre un espai de noms als seu fitxers.

- **Servidor secundari:** Obtenen la informació des de els servidor primaris a partir del que s'anomena una transferència de zona

- **Locals o cau:** No són servidors DNS pròpiament. Aquest tipus de servidor el que fa és reenviar les peticions DNS que rep i emmagatzema la resposta. Quan un client torna a preguntar per alguna de les adreces emmagatzemades a la seua base de dades,el servidor contesta fent així que les consultes per part dels clients tinguen una resposta més ràpida.

4.1.3 Tipus de registre DNS

Aquests són els principals registres DNS:

A: Aquest registra és el més comú i s'empra per traduir direccions de servidors a direccions IPv4.

AAAA: Realitza la mateixa funció que el registre de tipus A però amb direccions de tipus IPv6.

CNAME: S'empra per a crear noms addicionals o àlies per a servidor. Podria emprar-se per un servidor que allotja dos serveis (FTP i una pàgina web per exemple). Es crearia un registre CNAME per a cadascun dels servei però que es traduirien amb la mateixa direcció IP

NS: Aquest registre serveix per a identificar servidors de noms que emmagatzemen la informació d'una zona determinada (Name Server). Es poden tindre quants servidors de noms per zona es vulga.

MX: Amb aquest tipus de registre es defineix servidors de correu per a un domini determinat.

PTR: També conegut com a registre invers, funciona a l'inversa que el registre A. Tradueix direccions IPs en noms de domini. S'utilitzen en la zona DNS inversa.

SOA: Proporciona informació sobre el servidor DNS primari de la zona

4.2 Bind9

BIND (Berkeley Internet Name Domain, anteriorment: Berkeley Internet Name Daemon) és el servidor DNS més utilitzat a Internet, a sobre de tot en sistemes UNIX, en els quals es pot considerar un estàndard. Originalment escrit per estudiants de la Universitat de Califòrnia,Berkeley, bind es va reescriure pràcticament de zero donant lloc a bind9.

Entre d'altres coses açò es va fer per poder incorporar la DNSSEC(DNS security extensions) que són un conjunt d'extensions a DNS que serveixen per garantir coses com l'autenticitat de l'origen de

les dades DNS o la negació autenticada de l'existència i integritat de les dades, però no de seua disponibilitat o confidencialitat.

4.2.1 Instal·lació de bind9 en Ubuntu 14.04

A continuació es detalla la instal·lació bàsica de bind9 en un servidor Ubuntu:

- Obrir un terminal i instal·lar els paquets bind9 i dnsutils amb la instrucció

  sudo apt-get install bin9 dnsutils -y

  Si es fa amb l'usuari root no és necessari utilitzar la instrucció **sudo**

```
root@IP-DNS-CA:~# sudo apt-get install bind9 dnsutils -y
```

Il·lustració 4.2 Instal·lació servidor DNS Bind9

- Modificar el fitxer **/etc/bind/named.conf.local** amb els paràmetres que es poden vore a la captura següent.

```
// This is the primary configuration file for th
//
// Please read /usr/share/doc/bind9/README.Debia
// structure of BIND configuration files in Debi
// this configuration file.
//
// If you are just adding zones, please do that

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "local.lab" {

        type master
        file /var/lib/bind/db.local.lab
};
```

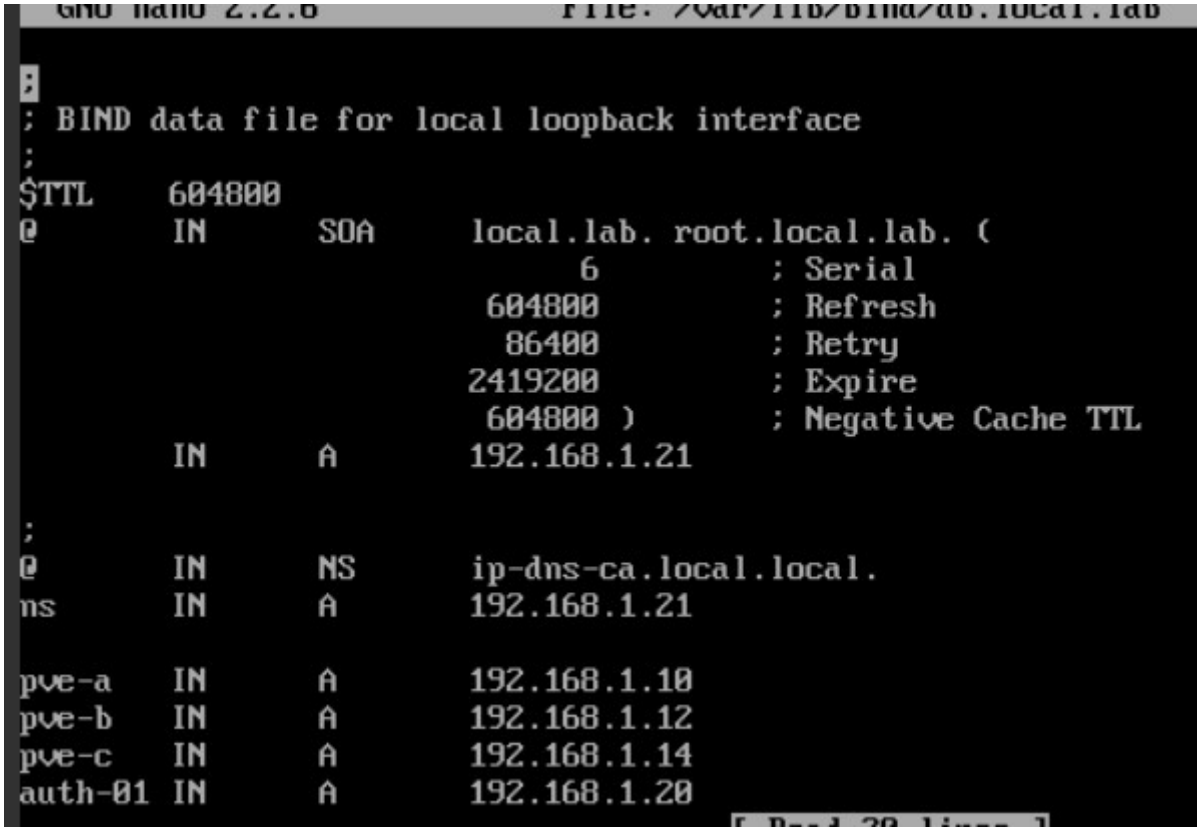
Il·lustració 4.3 Configuració servidor DNS 1

- Copiar el fitxer de exemple **/etc/bind/db.local** en el fitxer especificat en el camp file de **/etc/bind/named.conf.local**. En el nostre exemple **/var/lib/bind/db.local.lab**. Obrir **/var/lib/bind/db.local** amb **nano** per a editar-lo

```
root@IP-DNS-CA:~# cp /etc/bind/db.local /var/lib/bind/db.local.lab
root@IP-DNS-CA:~# nano /var/lib/bind/db.local.lab
```

Il·lustració 4.4 Configuració servidor DNS 2

- Editar l'arxiu **/var/lib/bind/db.local.lab** tal i com es mostra en la següent imatge:



Il·lustració 4.5 Configuració servidor DNS 3

- Per últim, atés que el servidor DNS només pot resoldre localment direccions del domini local.lab, harem de configurar forwarders (reenviadors en anglés) per a que el servidor DNS puga reenviar les peticions que no sap resoldre a altre servidor i començar així la cerca recursiva fins resoldre el nom. Per fer açò, edit el arxiu /etc/bind/named.conf.options descomentant la secció forwarders i afegint allí la direcció del nostre reenviador. En el cas d'aquest projecte utilitzarem com a reenviador el encaminador de la xarxa on estan configurats tots els servidors d'aquest projecte tal i com mostra la següent imatge:

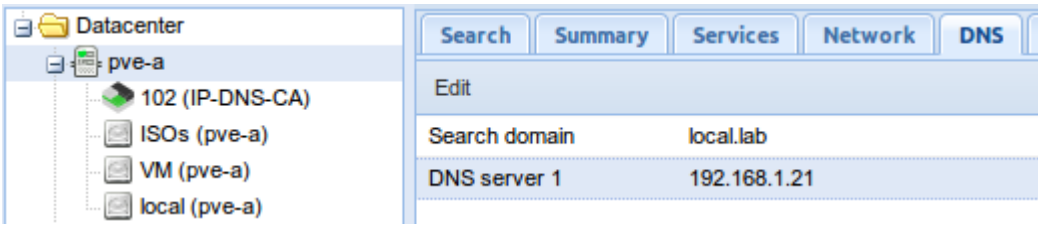
Il·lustració 4.6 Configuració reenviadors

4.2.1.1 Comprovació del funcionament del servei

Al fitxer d'exemple **/var/lib/bind/db.local.lab** que conté la base de dades de la zona que controla el nostre servidor, a més del servidor de noms s'ha afegit al servidor DNS els registres A dels 3 nodes de Proxmox i del servidor d'autenticació. Per a poder provar que el servei DNS funciona correctament resten dos passos més.

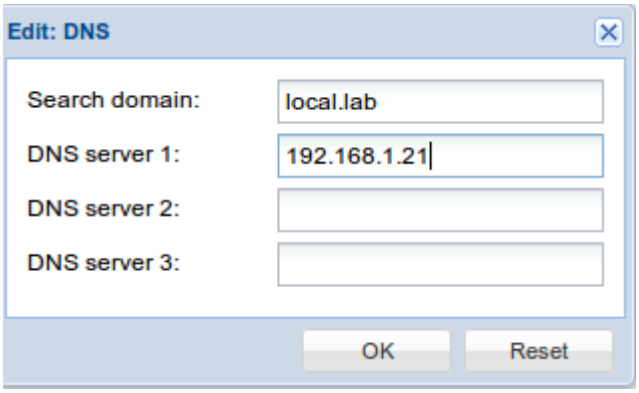
Primerament canviarem el servidor DNS que fan servir tant els nodes de Proxmox com el contenidor Linux on s'executa el servidor d'autenticació. Per a fer açò ens connectarem al panell d'administració de Proxmox i seleccionarem en el panel de l'esquerra l'element del que volem modificar el servidor DNS i seguir els passos que es detallen a continuació:

- Fer doble clic damunt el valor actual del camp DNS server 1:



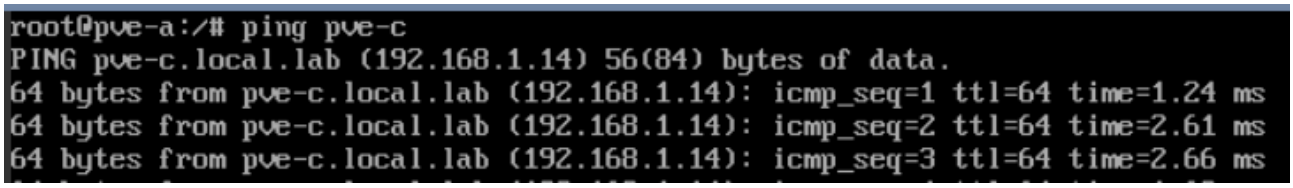
Il·lustració 4.7 Configurar servidor DNS 1

- Modificar l'adreça amb la direcció del nom servidor



Il·lustració 4.8 Configurar DNS contenidor 2

Per a comprovar que realment el node esta resolvent correctament les direccions internes amb el nou servidor executarem la instrucció ***ping «nom d'alguna màquina del domini»*** a la consola NoVNC en Proxmox. Si s'obté una resposta similar a la de la imatge següent el servidor funciona correctament :



Il·lustració 4.9 Test resolució de nom de la zona

Per a comprovar que el servidor resol be les direccions externes fent ús dels reenviadors configurats executarem la instrucció ***ping www.google.es***:

```
root@pve-a:~# ping www.google.es
PING www.google.es (216.58.211.99) 56(84) bytes of data.
64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_seq=1 ttl=55 time=31.8 ms
64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_seq=2 ttl=55 time=31.8 ms
64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_seq=3 ttl=55 time=31.5 ms
```

Il·lustració 4.10 Test resolució de nom extern a la zona

Per a fer aquest mateix canvi en un contenidor Linux, el procediment és exactament el mateix però amb una salvetat, el contenidor no pot estar en marxa. Per aquest motiu s'haurà de programar una aturada temporal del servei.

Per últim cal esmentar **nslookup**. Nslookup és una utilitat que ens servirà per fer consultes a qualsevol DNS ja siga de la nostra xarxa o no. Simplement s'executa nslookup des d'una terminal i amb la instrucció ***server «IP servidor DNS»*** podem escollir el servidor que volem consultar:

```
Default server: 192.168.1.21
Address: 192.168.1.21#53
> pve-a
Server:         192.168.1.21
Address:        192.168.1.21#53

Name:   pve-a.local.lab
Address: 192.168.1.10
> www.google.es
Server:         192.168.1.21
Address:        192.168.1.21#53

Non-authoritative answer:
Name:   www.google.es
Address: 216.58.211.99
```

Il·lustració 4.11 Consulta DNS

5. Autoritat certificadora

En aquest capítol s'explica què és una autoritat certificador i com implementa-la pas a pas en un servidor amb una distribució Linux com a sistema operatiu. A més, s'explica com crear un petició de certificat de servidor i s'emet aquest certificat.

5.1 Què és una autoritat certificadora?

En criptografia una autoritat certificadora és una entitat de confiança que emet o revoca certificats digitals. Aquests certificats són normalment emprats en la firma electrònica utilitzant criptografia de clave publica. La autoritat certificadora verifica la identitat de qui sol·licita un certificat abans de emetre-lo.

Els certificats contenen certa informació del sol·licitant i la seua clau pública i estan firmats electrònicament per la autoritat certificadora amb la seua clau privada. Tanmateix, la entitat certificadora té la autoritat de revocar un certificat que deixarà de ser valid. Un certificat pot identificar tant a una persona com a un servei(un servidor web per exemple).

El mecanisme d'una autoritat certificadora és el següent:

- **Sol·licitud del certificat:** Normalment la persona que vol demanar un certificat es connecta a una interfície web, complimentant certa informació identificativa i el servidor genera un parell de claus pública/privada. Amb aquesta informació el servidor genera un fitxer que conté una petició en format PKCS#10 que conte la clau publica i que es fa arribar a la autoritat certificadora escollida.

- **Verificació del sol·licitant:** Després de verificar la identitat del sol·licitant, s'envia el certificat firmat al sol·licitant que ja podrà fer ús del mateix.

Les autoritats certificadores disposen dels propis certificats públics. Aquests certificats contenen una clau privada que és la que s'utilitza per firmar els certificats que emeten. Un certificat pot estar auto-firmat quan no hi ha cap autoritat certificadora en un nivell superior que el firme. Aquest és el cas dels certificats arrel d'una autoritat certificadora que és l'element inicial en la jerarquia de certificació.

Una jerarquia de certificació consisteix una cadena d'autoritats certificadores que comença amb una autoritat certificadora auto-firmada. En cada nivell,existeix una o més autoritats certificadores que poden a be crear certificats finals per a persones , servidors etc o per a altre autoritats certificadores i continuar així la cadena. Totes les autoritats certificadores de la cadena han de tindre una política de certificació compatible amb la política de les autoritats certificadores de nivell superior.

Altre punt important és la confiança en les autoritats certificadores. Normalment aquesta confiança s'estableix instal·lant al dispositiu de l'usuari el certificar arrel de la entitat certificadora de la jerarquia en la que es vol confiar. Finalment, cal remarcar que els certificats digitals poden fer-se servir per identificar tant persones (certificat per presentar la renta, firmar un correu electrònic), com serveis(servidor web, servidor de correu).Com a autoritat certificadora o CA al mon del programari lliure la elecció era simple, OpenSSL. Es poden trobar els detalls d'instal·lació a l'annex II

6. Servidor DHCP

DHCP(per les seues sigles en anglés Dynamic Host Configuration Protocol) és el protocol amb arquitectura client/servidor on el servidor té una llista de direccions IP dinàmiques i les va assignant als clients conforme aquestes van quedant lliures.

6.1 Assignació d'adreces.

Un servidor DHCP manté una llista de les direccions assignades, les quals tenen un període de caducitat. Quan passa aquest període, si el client torna a demanar una direcció abans que aquesta siga assignada, rebrà la mateixa. Si per algun motiu, el client està desconnectat de la xarxa el temps suficient per a que aquesta direcció siga assignada a altre dispositiu,el client,, rebrà una direcció diferent. Aquest mètode s'anomena assignació de direccions dinàmica.

La assignació de les direccions es pot fer de dues formes més:

- **Assignació estàtica:** Es controla quina direcció se li assigna a cada client. D'aquesta manera cada client sempre rebrà la mateixa direcció i , a més, es pot controlar que clients no desitjats puguen rebre un direcció. Normalment aquest mètode s'implementa assignant direccions IP a direccions físiques(MAC) de cada dispositiu.

- **Assignació automàtica:** Assigna la direcció IP a cada client quan la demana i fins que el client la allibera. Aquest tipus d'assignació s'utilitza quan el nombre de dispositius a la xarxa no varia molt.

Els mètodes més estesos són la assignació dinàmica i l'assignació estàtica.

DHCP també pot assignar altres paràmetres de la configuració de xarxa com ara la direcció del servidor DNS, la porta d'enllaç, la direcció de publicació massiva(broadcast), la màscara de subxarxa, el temps màxim d'espera d'ARP, MTU(unitat de transferència màxima) per a la interfície de xarxa, servidors NIS(servei d'informació de xarxa per les seues sigles en anglés), servidors NTP(protocol d'hora) o el servidor SMTP(protocol de correu electrònic) entre d'altres.

6.2 DHCP fingerprinting

Una de les tècniques més interessants que ofereix DHCP és el fingerprinting. Quan un client fa una petició a un servidor DHCP, aquest pot demanar-li al client certa informació com ara quin tipus de dispositiu és, el fabricant o el sistema operatiu que està executant.

D'aquesta manera es poden categoritzar els dispositius, decidir quin tipus d'accés poden tindre a la xarxa basant-se en la direcció assignada o inclús no assignar-li cap adreça negant així la connexió a la xarxa de algun tipus de dispositiu determinat.

Si, per exemple, la direcció de l'empresa decideix que els dispositius mòbils no poden connectar-se a la xarxa corporativa i només poden tindre accés a Internet, amb DHCP fingerprinting podrem assignar direccions IP d'una VLAN especifica que només tinga accés a Internet.

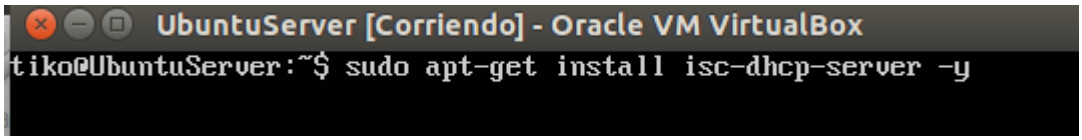
Aquests són alguns dels tipus de dispositius que es poden reconéixer amb DHCP fingerprinting:
- Mòbils i tabletes
- Escriptoris

- Servidors
- Encaminadors, commutadors o punts d'accés
- Videoconsoles
- Sistemes de veu sobre IP
- Impressores

6.3 Instal·lació i configuració d'un servidor DHCP a Ubuntu

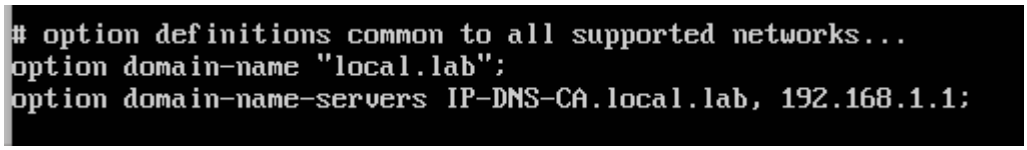
Aquests són els passos a seguir per a la instal·lació bàsica d'un servidor DHCP amb Ubuntu:

- Instal·lar el paquet **ics-dhcp-server** amb apt-get des d'un terminal:



Il·lustració 6.1 Instal·lació servidor DHCP

- Modificar les opcions domain-name amb el nom del domini de la nostra xarxa i domain-name-servers amb el nom dels servidors de DNS que es vol assignar als clients. Aquestes opcions s'aplicaran de manera global a totes les subxarxes que es configuren a aquest servidor.

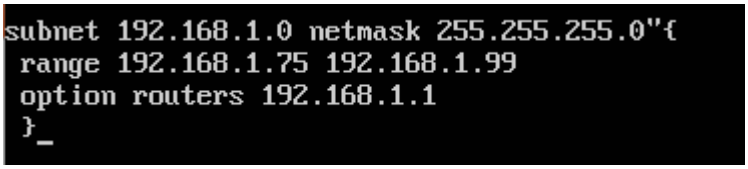


Il·lustració 6.2 Arxiu de configuració servidor DHCP 1

- Eliminar la # a la línia que es mostra en la següent imatge autoritzar el servidor a repartir direccions

Il·lustració 6.3 Arxiu de configuració servidor DHCP 2

- A la següent imatge es mostra la configuració per assignar adreces IP a una xarxa determinada. Amb aquesta configuració, el servidor repartirà direccions als dispositius de la xarxa 192.168.1.0 amb màscara 255.255.255.0 des de l'adreça 192.168.1.75 fins la 192.168.1.99. A tots ells els assignarà com a porta d'enllaç l'adreça 192.168.1.1



Il·lustració 6.4 Exemple assignació subxarxa

- Per últim, la imatge a continuació mostra com assignar una adreça estàtica a un client. Al exemple, el client amb nom de màquina CLI-01 que té com a adreça MAC 00:00:00:00:00:00 se li assignarà l'adreça IP 192.168.1.74 sempre.

Il·lustració 6.5 Assignació estàtica DHCP

Es poden crear tantes subxarxes com es vulga a un servidor DHCP. Hi ha que tindre en compte que per el mecanisme que el protocol utilitza, per a que un client puga contactar amb un servidor DHCP que esta a una xarxa o VLAN diferent, el commutador que comunica aquestes xarxes s'ha de configurar adequadament. Aquesta característica s'anomena de manera general DHCP relay.

7. Servei de fitxers compartits

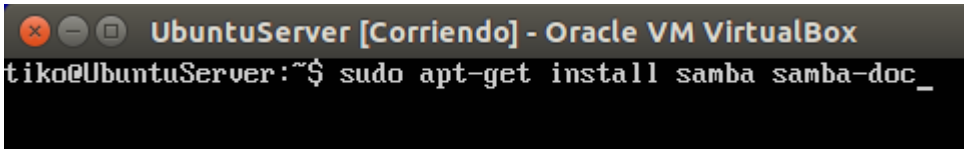
Tot i que aquest projecte té com a objectiu oferir alternatives de programari lliure única i exclusivament, per a la implementació del servei de fitxers compartits s'ha optat per Samba amb OpenLDAP de backend per aprofitar la interoperabilitat de SAMBA amb diferents plataformes oferint així una opció vàlida per a entorn híbrids on s'han de conviure, per exemple, ordinadors amb Windows i ordinadors amb Linux.

7.1 Què és Samba?

Samba és la re-implementació lliure del protocol de xarxa SMB/CIFS i va ser originalment desenvolupat per Andrew Tridgell. Samba proveeix servei de serveis de fitxers i impressió tant a clients Linux com Windows. També es pot integrar amb l'Active Directory de Microsoft.

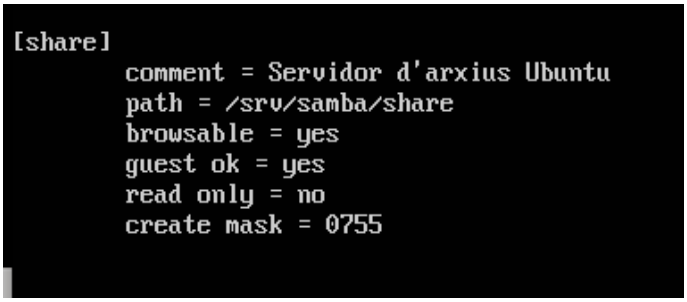
7.2 Instal·lació i configuració de Samba

- Instal·lar els paquets **samba** i **samba-doc** amb apt-get



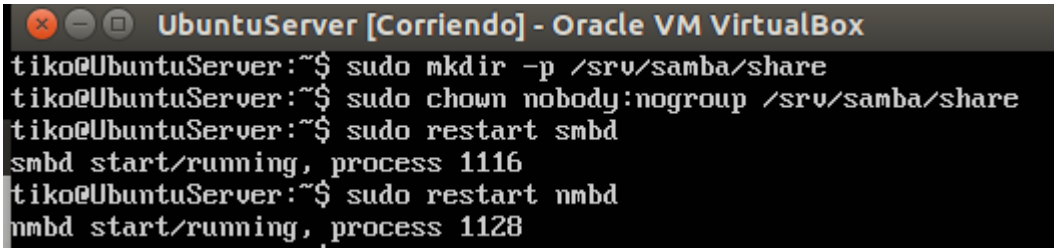
Il·lustració 7.1 Instal·lació samba

- Editar l'arxiu **/etc/samba/smb.conf** i afegir una nova secció al final amb la informació que hi ha a la següent imatge. Amb açò samba reconeixerà la carpeta **/srv/samba/share** com a un recurs compartit. El compartirà amb el nom **share**.



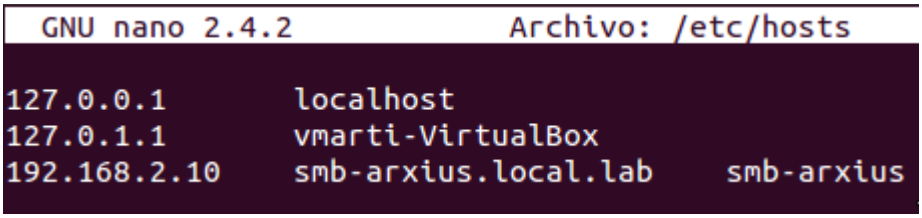
Il·lustració 7.2 Directiva en /etc/samba/smb.conf

- A continuació crearem el directori **/srv/samba/share** i li assignarem els permisos necessaris per poder accedir. Reiniciar els serveis de samba (smbd i nmbd)



Il·lustració 7.3 Configuració directori compartit

- Per accedir al recurs des d'un client amb Ubuntu 15.10 instal·lat, primerament afegirem a l'arxiu **/etc/hosts** el nom del servidor samba per poder així accedir amb el nom del servidor.

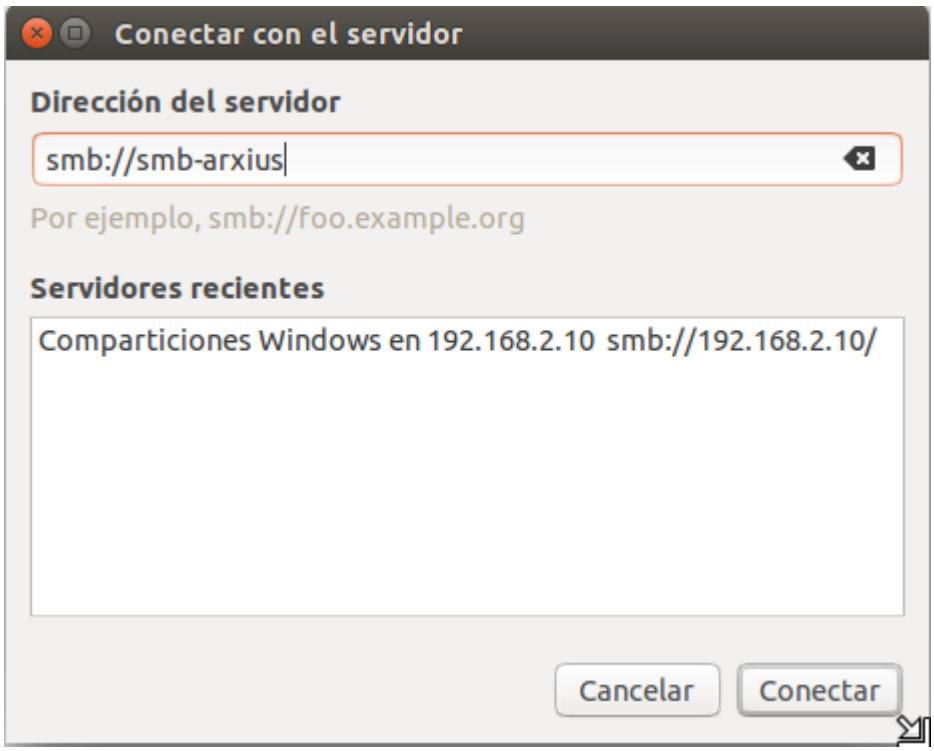


Il·lustració 7.4 Arxiu /etc/hosts

- Obrir l'explorador d'arxius fer clic en **«Connectar al servidor»** en el panel de l'esquerra

Il·lustració 7.5 Connectar amb servidor Samba 1

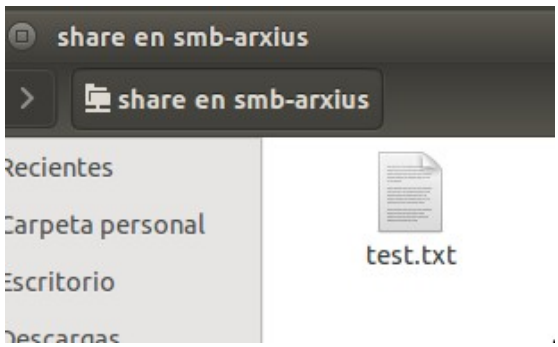
- Introduir la direcció del servidor samba amb el format smb://nom_del_servidor i connectar.



Il·lustració 7.6 Connectar amb servidor Samba 2

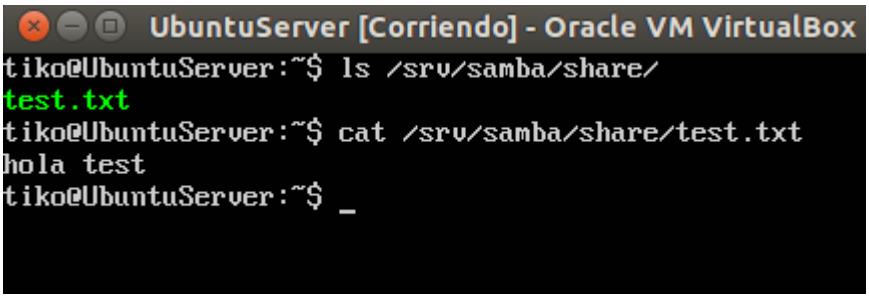
- S'obrirà una nova finestra amb tots els recursos compartits d'aquest servidor. Al exemple si obrim el recurs **«share»** podrem crear un arxiu i salvar-lo al recurs.

Il·lustració 7.7 Directoris compartits per Samba server



Il·lustració 7.8 Contingut directori compartit

- Si connectem de nou al servidor i llistem el contingut del directori local **/srv/samba/share** es pot vore que l'arxiu realment està al servidor. Per últim, es pot imprimir per pantalla el contingut de l'arxiu per comprovar que és el mateix.



Il·lustració 7.9 Contingut arxiu compartit

8. Servidor d'impressió

A aquesta secció es detalla la solució escollida per a la implementació del servidor d'impressió així com la instal·lació tant de la part del servidor com d'una impressora compartida des del servidor a un client.

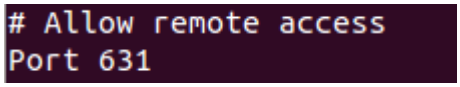
8.1 CUPS

CUPS (Common Unix Printing System) és un sistema modular estàndard per a computadores amb sistemes basats en Unix que permet l'ordinador actuar com a servidor de impressió. Desenvolupat per Apple Inc a finals dels anys 90 esta format per un administrador de cues d'impressió i un planificador de treballs, un filtre de sistema que converteix les dades d'impressió a un format que impressora pot entendre i un sistema backend que envia les dades a la impressora.

CUPS utilitza el protocol IPP (Internet Printing Protocol) com a base per a gestionar treballs d'impressió i cues. També proveeix les interfícies d'instruccions tradicionals per a sistemes d'impressió System V i Berkeley i dona soport al servidor d'impressió Berkeley, LPD (Line Printer Daemon protocol) així com soport limitat per al protocol SMB(server message block). CUPS té la seua pròpia interfície web per a l'administració tot i que hi han diferents interfícies disponibles.

8.2 Instal·lació i configuració servidor CUPS en Ubuntu 14.04

Per a instal·lar un servidor d'impressió utilitzant CUPS, hem d'instal·lar el paquet cups amb totes les seues dependències. Per fer açò, executarem a un terminal la instrucció sudo apt-get install cups. Tot seguit, modificar la directiva **#Allow remote access** al fitxer **/etc/cups/cupsd.conf** com es mostra a la imatge per a poder accedir des de qualsevol ordinador de la xarxa a la interfície web d'administració:

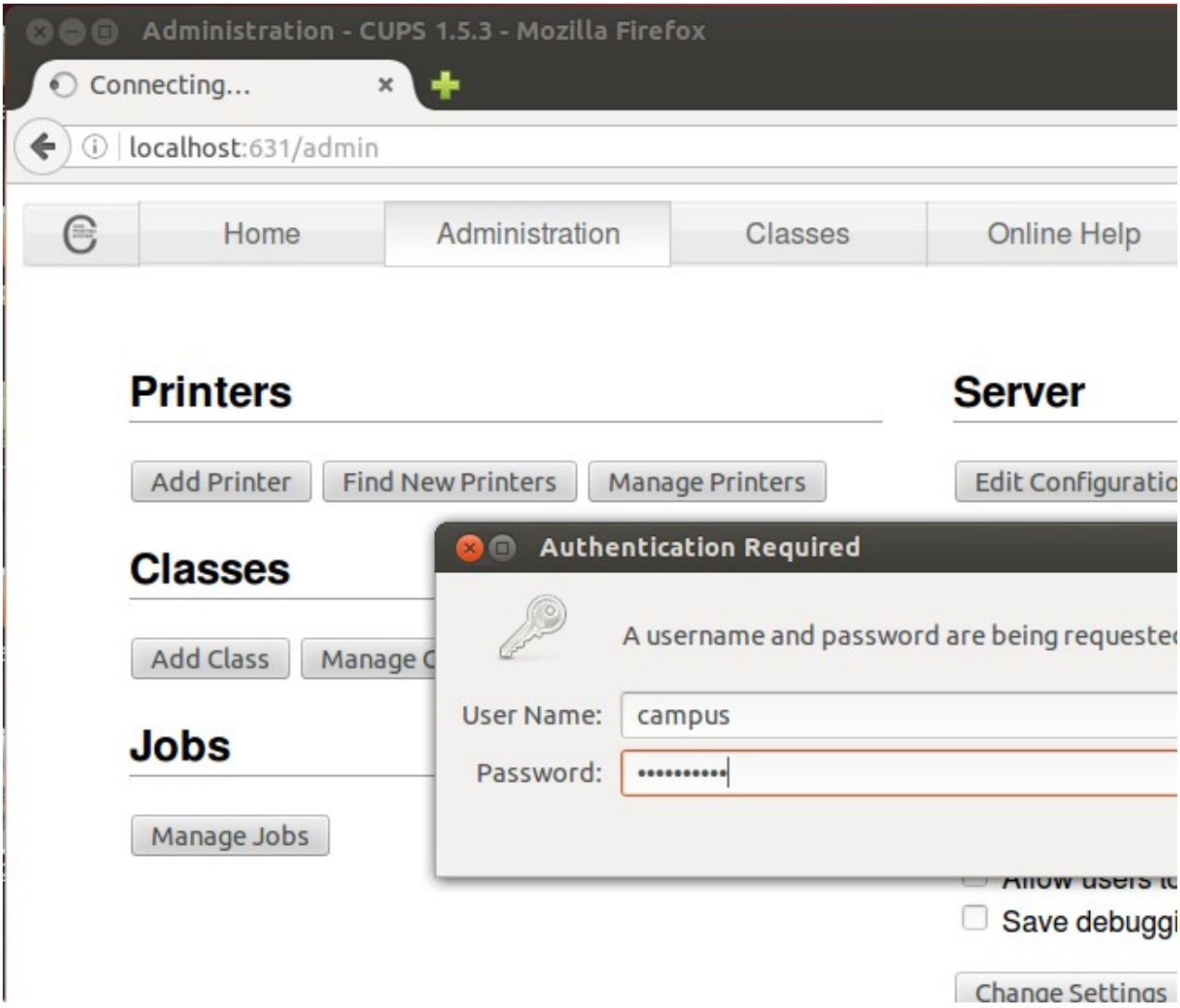


Il·lustració 8.1 Directiva cupsd.conf

Al servidor CUPS afegir l'usuari amb el qual accedirem (un usuari sudoer) al grup **lpadmin**.
Executar la instrucció ***sudo usermod -aG lpadmin nom_usuari*** a un terminal. Per seguretat, CUPS demanara un usuari amb contrasenya per poder accedir a la interfície. Com a bona practica evitarem l'ús de l'usuari root.
Per últim reiniciar el servidor CUPS amb la instrucció sudo systemctl restart cups.service . Per a connectar a l'interfície web de CUPS utilitzarem l'adreça http://ip_del_servidor:631/admin

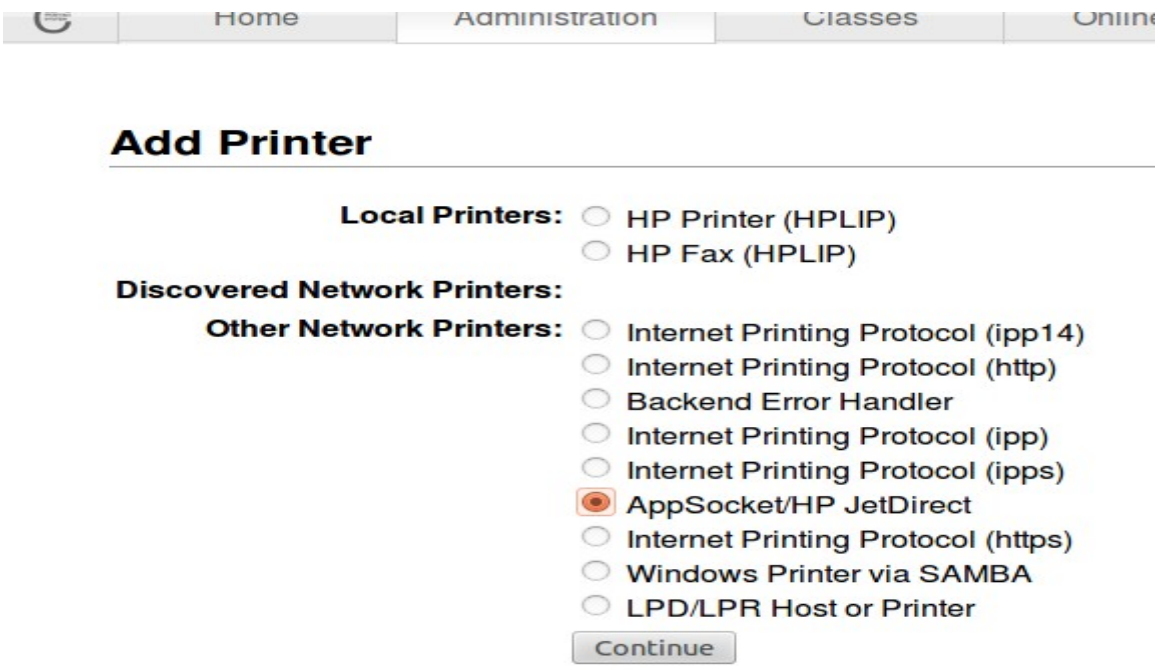
8.3 Afegir impressora al servidor

Primerament accedirem a la interfície web de CUPS amb http://ip_o_nom_del_servidor:631/admin. Fer clic a el botó **Add Printer**. Tot seguit es mostrarà una finestra on hem d'introduir les credencials de l'usuari que hem afegit al grup **lpadmin**.

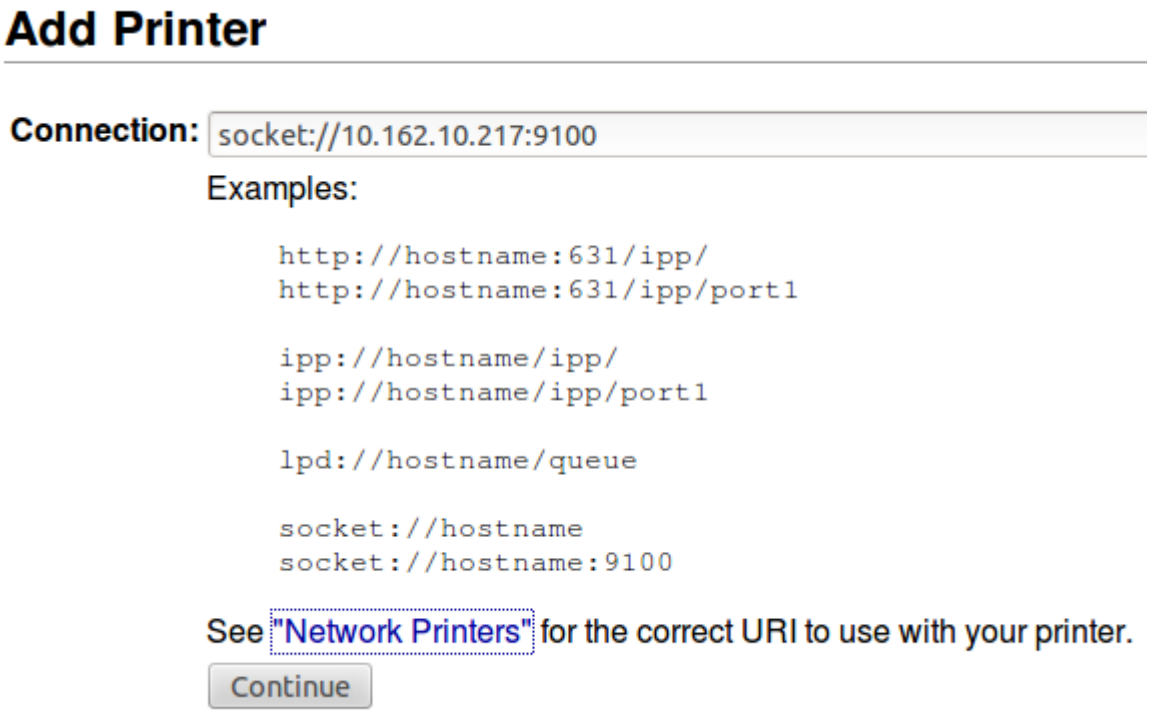


Il·lustració 8.2 Accés a la interfície d'administració de CUPS

Per al exemple, afegirem una impressora HP. Per a aquest tipus d'impressora seleccionar AppSocket/HP JetDirect (informació sobre el tipus de connexió per a cada impressora es pot trobar a http://ip_o_nom_del_servidor:631/help/network.html). Aquest protocol fa ús del port 9100

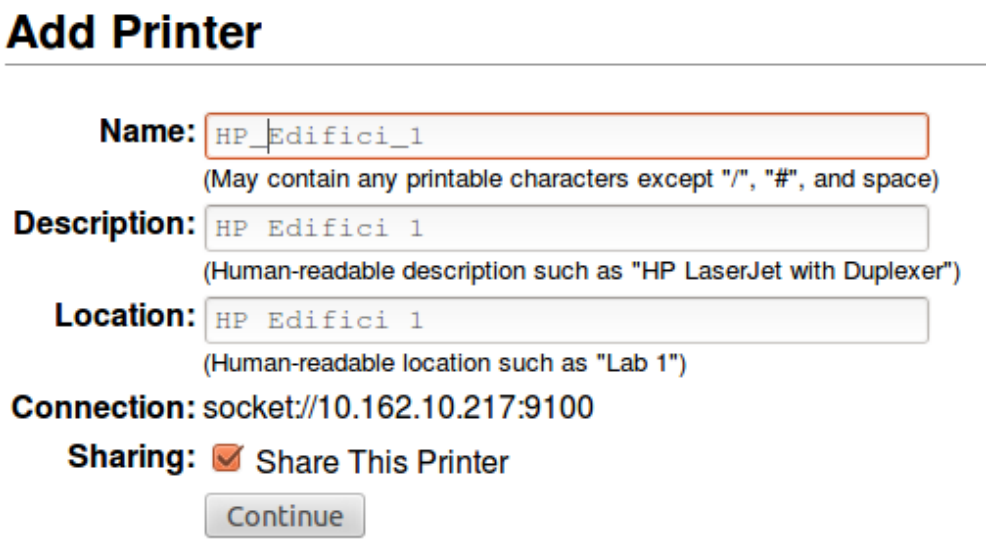


Il·lustració 8.3 Assistent per a afegir impressora 1



Il·lustració 8.4 Assistent per a afegir impressora 2

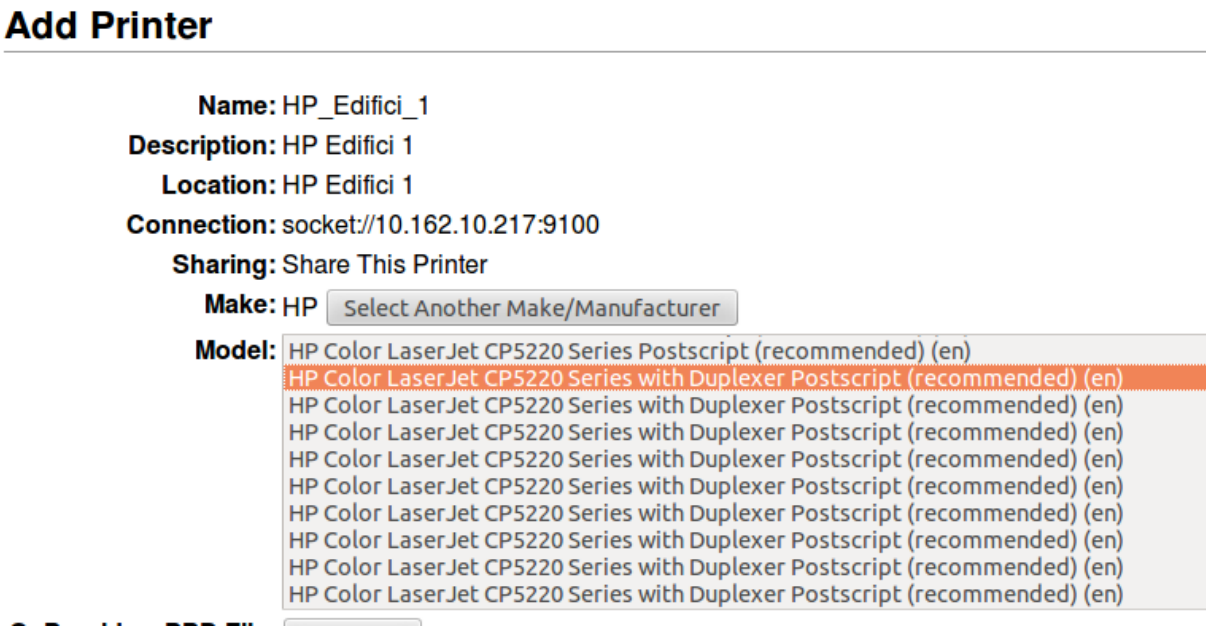
Li donarem un nom i una descripció a l'impressora. També especificarem una localització. A més, marcar la casella **Share This Printer** per fer que l'impressora sigui compartida



Il·lustració 8.5 Assistent per a afegir impressora 3

Per últim seleccionarem el controlador recomanat per a la impressora, seleccionant primerament la marca i polsant en **Continue**. Tot seguit, seleccionar el controlador recomanat i polsar el botó **Add printer**

Il·lustració 8.6 Selecció fabricant impressora



Il·lustració 8.7 Selecció model impressora

CUPS també és compatible amb Samba per tant aquesta impressora també es podria compartir per a clients Windows.

Per a més informació de com afegir aquesta impressora compartida a una maquina client Linux, consultar **Annex III – Instal·lació d'impressora compartida**

9. Servidor web i gestor de contingut(Intranet)

A aquesta secció es detallen els components escollits per a la instal·lació d'una pagina web que es pot fer servir com a Intranet de l'empresa. El producte escollit és Wordpress. A continuació s'explica el motiu d'aquesta elecció així com els elements necessaris per al seu correcte funcionament i la seua instal·lació.

9.1 LAMP

LAMP és un model de pila de serveis que normalment donen soport a aplicacions basades en web. El nom és l'acrònim dels quatre productes de codi obert que el componen, Linux , Apache, MySQL i PHP. Wordpress segueix aquest model per a funcionar.

9.2 Apache

Quan es parla de servidors web és inevitable parlar d'Apache HTTP Server. Apache és sense cap dubte el servidor web més utilitzat al mon. Desenvolupat des de 1995, Apache, va ser una de les peces clau del creixement de la World Wide Web. Apache es utilitzat majoritàriament en sistemes operatius basats en Unix però esta disponible per a gran quantitat de sistemes com ara Microsoft Windows, NetWare, OpenVMS o OS/2. Distribuït baix la llicència Apache, Apache és programari lliure i de codi obert. S'estima que Apache serveix el 50% de totes les pàgines web actives.

Apache soporta una gran varietat de funcionalitats. La majoria d'aquestes funcionalitats poden ser fàcilment activades amb mòduls compilats els quals estenen la funcionalitat bàsica d'Apache amb diferents característiques com ara soport a diferents llenguatges de programació com Perl,Python,Tcl o PHP, soport a mecanismes d'autenticació o soport per SSL o TLS.
A https://https.apache.org/docs/2.4/mod/ es pot trobar un index amb tots els mòduls disponibles per a l'ultima versió estable d'Apache.

9.3 MySQL i MariaDB

MySQL és el sistema de gestió de base de dades SQL relacionals de codi lliure més popular del mon. MySQL és probablement el millor sistema de gestió de base de dades relacionals quan de desenvolupament d'aplicacions basades en web es parla. Originàriament desenvolupat per l'empresa sueca MySQL AB, avui dia és propietat de la multinacional Oracle.

MySQL pot ser gestionat tant amb instruccions a una terminal com amb interfícies gràfiques. La interfície gràfica de codi obert més coneguda per a la gestió de MYSQL és phpMyAdmin.
PHP. Tot i que MySQL continua essent lliure, després de que Oracle adquirira l'empresa propietària de MySQL alguns membres de la comunitat, els quals tenien i tenen dubtes de que MySQL continue essent de codi obert, crearen branques alternatives basades en la versió oficial de MySQL. Una de les més completes és MariaDB que entre altes característiques soporta Galera cluster amb el qual es pot instal·lar 3 nodes o més en un cluster i que la aplicació puga escriure en tots ells en lloc del clàssic cluster de dos nodes lectura-escriptura.

9.4 Wordpress

Wordpress és un projecte de programari lliure que va nàixer a l'any 2003. Des d'aquell moment fins avui dia ha crescut d'una manera espectacular utilitzada en milions de llocs web. Wordpress començà essent una plataforma per a crear blogs però la seua evolució l'ha convertit en un complet sistema de gestió de contingut. Tot açò amb l'ajuda dels plugins, widgets i temes disponibles . El fet

de distribuir-se amb la llicencia GPLv2 que permet modificar el programa i redistribuir-lo ha facilitat les aportacions de la comunitat al mateix i ha ajudat al seu ràpid desenvolupament.

Wordpress pot fer ús de la pila LAMP per a funcionar. Realment, té PHP i MySQL o MariaDB com a requeriments indispensables. Wordpress recomana l'ús d'Apache o NGINX com servidors web però funcionaria amb qualsevol servidor que soportara PHP i MySQL. En aquest estudi, es farà ús de la pila completa per ser els estàndards de facto a la comunitat substituint MySQL clàssic per MariaDB.

9.5 Instal·lació de Wordpress en Ubuntu 14.04

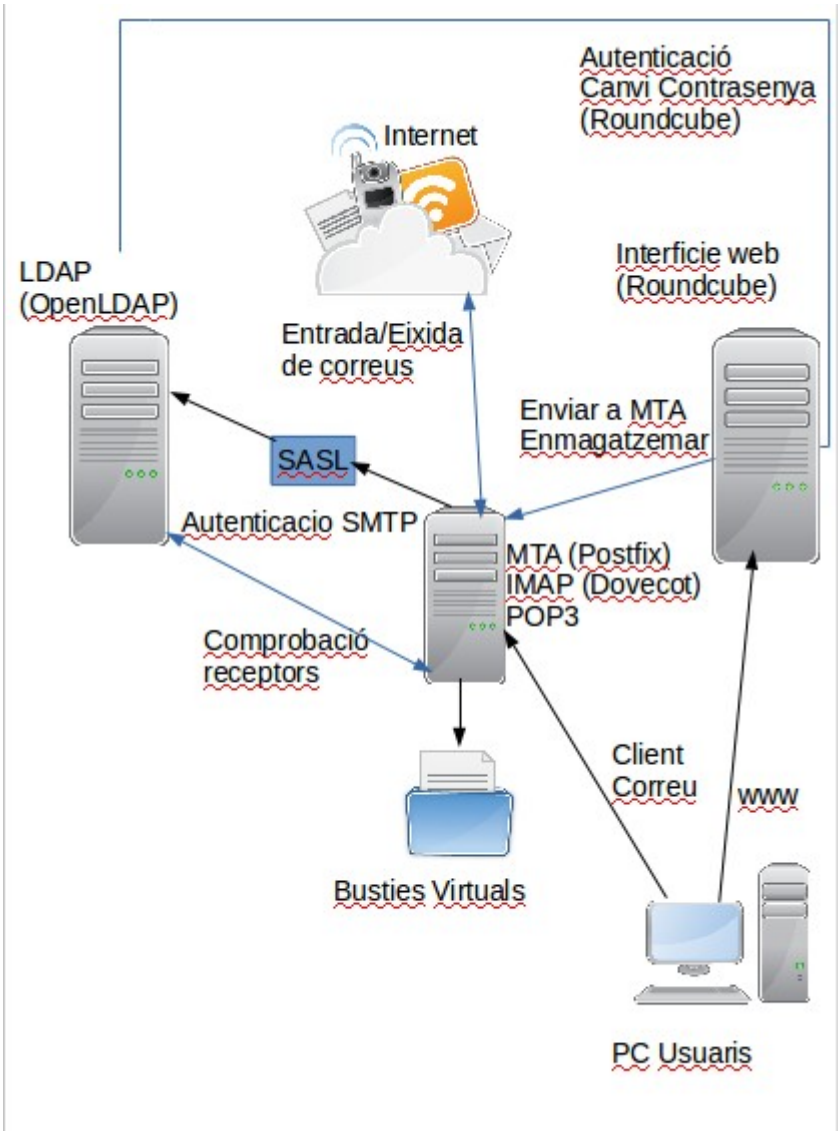
La instal·lació de Wordpress sobre Ubuntu 14.04 com a sistema Linux en la pila LAMP és relativament fàcil. Quan ja es té el sistema base instal·lat, hi ha que instal·lar el servidor web Apache, el motor de base de dades MySQL i el soport per a PHP des dels repositoris amb la instrucció apt-get. Quan ja tenim el programari base que soporta Wordpress instal·lat, es descarregarà la ultima versió estable des de la seua pagina web, copiar els fitxer al directori de dades d'Apache, modificar l'arxiu de configuració de Wordpress per a que puga connectar amb la base de dades i corregir els permisos a aquest directori per a que tot funcione correctament. Finalment, s'acabara la configuració amb la interfície web de Wordpress. La descripció detallada d'aquesta instal·lació es pot trobar a l'**annex IV – Instal·lació de Wordpress a Ubuntu 14.04**

10. Servei de correu electrònic

A aquesta secció es detalla la solució escollida per al servei de correu electrònic. Avui dia el correu electrònic és una de les ferramentes fonamentals a qualsevol empresa. Quan es creix el suficient com per a plantejar-se allotjar aquest servei a la infraestructura informàtica de la empresa, escollir un bon producte que s'adapti a les nostres necessitats és fonamental. La disponibilitat del servei i la seguretat tant de la informació emmagatzemada com del flux de correus són claus per a escollir un producte o altre. Atenent a aquests paràmetres, el sistema proposat a aquest estudi és una combinació de diferents sistemes que treballant conjuntament ofereixen una solució estable i segura.

10.1 Diagrama de la solució

A la següent imatge es mostra una vista de la solució proposta:



Il·lustració 10.1 Disseny arquitectura servei correu electrònic

Tots aquests serveis es poden instal·lar en un sol servidor en un entorn de proves. Per a entorns de producció amb usuaris reals es recomana separar-los. En els següents seccions s'explica cada component i la seua funció.

10.2 Registres DNS

Per a que un servei de correu electrònic funcione correctament quan es tracta de rebre i enviar correus electrònics des de i fins a altres dominis, hi ha que configurar una serie de registres DNS correctament. Aquests són els registres necessaris per a que el servidor funcione correctament:

- Registre de tipus A que apunte a la direcció IP publica del servidor de correu electrònic
- Registre de tipus PTR per a que funcione la resolució inversa
- Registre MX que apunte al nostre servidor de correu. Es podrà configurar una prioritat en cas de tindre més d'un servidor.

A més d'aquests registres bàsics hi ha un altre tipus de registre que resulta interessant des del punt de vista de la seguretat, el registre SPF. Aquest registre apunta als servidors de correu(MTA) que estan autoritzats a enviar correus en nom de algun usuari d'un domini determinat. Al cas d'aquest projecte es crearà un registre SPF que autoritze al servidor Postfix implementat a enviar correus en nom dels usuaris amb direccions @local.lab.

Si el MTA del destinatari, cada vegada que rep un correu electrònic de per exemple, vmarti@local.lab comprova que el servidor que està intentant entregar -lo,correspon amb el servidor definit al registre SPF acceptarà el correu. En cas contrari el correu es rebutjarà. D'aquesta manera es pot evitar rebre correus fraudulents amb la intenció de suplantar la identitat d'algú.
Tots aquest registres DNS es publicaran al servidor DNS propietari de la zona on es troba el nostre domini.

10.3 MTA – Postfix

MTA per les seues sigles en anglés (Mail Transport Agent) és la part d'un sistema de correu electrònic que s'encarrega del transport dels missatges al MTA del destinatari. Els MTAs es comuniquen entre ells amb el protocol SMTP (Simple Mail Transport Protocol) utilitzant el port 25.

En aquest estudi el MTA de programari lliure escollit per formar part del sistema de correu és Postfix. Postfix va nàixer com a alternativa al popular MTA Sendmail,més ràpid, més fàcil d'administrar i més segur. A la solució plantejada a aquest estudi, Postfix actuarà com a MTA transportant els correus que envien els usuaris del nostre domini als MTA dels destinataris. Així mateix entregarà al nostre MDA (Mail Delivery Agent) els correus entrants i que van dirigits als usuaris del nostre domini.

10.4 MDA – Dovecot

El MDA (Mail Delivery Agent) és l'encarregat de rebre els correus entrants des del MTA i emmagatzemar-los per a que els seus destinataris puguen llegir-los. En aquest utilitzarem Dovecot com a MDA. Per poder accedir a aquests correus Dovecot ofereix tant el protocol IMAP com POP3. POP3 és el més antic dels dos i s'utilitza per a recuperar els correus i generalment no deixa copia al servidor.

IMAP en canvi, s'utilitza per a sincronitzar l'estat de una bustia de correu en diferents clients de correu així com l'estat d'aquests correus. IMAP guarda una copia de cada correu al servidor fent així molt més fàcil la tasca. Els usuaris poden accedir a les seues busties amb un client de correu que en

general pot ser una aplicació d'escriptori o una interfície web.

10.5 Autenticació i validació de receptors

És necessari validar els usuaris amb busties de correu al nostre sistema a diferents nivells per garantir accés segur tant els recursos com a la informació que emmagatzema el sistema. Per a aquesta tasca contarem amb un servidor LDAP que serà OpenLDAP.

10.5.1 Autenticació SMTP – SASL

Antigament no era necessari validar la identitat d'un usuari que volia enviar un correu electrònic mitjançant un servidor de correu qualsevol. Per aquest motiu era molt fàcil falsificar la pròpia direcció quan s'enviava un correu. Aquest tipus de MTA reben també el nom de relé obert(Open Relay) i són utilitzats malintencionadament per a enviar SPAM.

Per evitar aquestes situacions es fa necessari establir una autenticació SMTP per a que només els usuaris autenticats puguen enviar correus mitjançant el nostre MTA. Per a fer aquesta autenticació es proposa utilitzar SASL.

SASL per les seues sigles en anglés Simple Authentication and Security Layer és un entorn de treball per autenticació i i autorització de protocols. El que aconseguim en SASL és separar el procés d'autenticació del protocol que requereix esta autenticació. D'aquesta manera es pot validar qualsevol servei que soporte SASL amb els mecanismes que SASL tinga inclosos. És a dir, si en el futur volem canviar el tipus d'autenticació d'un servei bastarà amb saber si SASL el soporta i configurar aquest per a utilitzar-lo.

Tot i que SASL proveeix mitjans per a un ús negociat del mecanisme escollit per a la autenticació, requereix d'alguna cosa més per xifrar el contingut d'aquesta negociació. Per aconseguir aquesta encriptació farem ús de TLS que en combinació amb SASL farà que el nostre mecanisme d'autenticació SMTP siga segur i eficient.

10.5.2 Autenticació LDAP del MDA (Dovecot)

A més de l'autenticació a nivell de protocol SMTP, també es fa necessari altre tipus d'autenticació. En el cas del MDA(Dovecot), en primer lloc ens farà falta que quan un usuari vullga accedir a la seua bustia, Dovecot valide les credencials d'aquest usuari abans de donar-li accés. Per últim, per a que Dovecot puga buscar la bustia d'un usuari per a entregar un correu electrònic, també ha de cercar aquest usuari i la informació emmagatzemada sobre aquest a algun lloc. Tant la validació dels usuaris, que és independent del protocol emprat (és a dir és necessària tant en IMAP com en POP3), com la cerca del destinatari d'un correu es farà mitjançant consultes a un servidor LDAP. El servidor LDAP escollit per a aquest project és OpenLDAP

10.6 Webmail – Roundcube

Per finalitzar, com ja s'ha esmentat anteriorment hi ha dues formes de recuperar els correus emmagatzemaments pel MDA. La primera és utilitzant POP3 o IMAP amb una aplicació d'escriptori i la segona és fer el mateix amb una interfície web que es connecta tant amb el MTA com amb el MDA per a permetre les mateixes opcions que amb l'aplicació d'escriptori via IMAP. Una de les interfícies web disponibles és Roundcube.

Disponible en setanta idiomes, Roundcube, és un dels projectes de programari lliure en aquest àmbit

que més força han tingut junt amb SquirrelMail. El principal avantatge d'aquesta interfície web és l'accessibilitat que li dona al servei atés que només fa falta un navegador d'Internet per a accedir. A més d'un servidor de pàgines web, per el que farem ús d'Apache, Roundcube, també requereix d'una instancia de base de dades per emmagatzemar les dades de configuració dels usuaris. En aquest estudi la autenticació d'usuaris i la llibreta de direccions global fan ús del servidor LDAP que ja s'ha vist en seccions anteriors.

10.7 Millores: ClamAV i SpamAssassin

Al disseny proposat és un disseny bàsic de servei de correu electrònic que inclou els elements necessaris per al seu funcionament. Igual que s'ha inclòs la autenticació SMTP al disseny per a millorar la seguretat i qualitat del servei, a un entorn professional s'haurien d'afegir dues aspectes més que completarien la solució amb tots els elements necessaris per a un funcionament professional.

En primer lloc hauríem de parlar d'una solució antivirus. Tot i que de vegades sembla que parlar d'una solució antivirus en màquines amb Linux no té sentit, quan es parla d'un servidor de correu hi ha que tindre en ment dues coses:

- A un servidor de correu es connecten clients per a recuperar els correus. Aquests clients poden estar instal·lat a qualsevol sistema operatiu i per tant si un dels nostres usuaris rep un correu amb un virus, es connecta des d'un client Windows i aquest virus es capaç d'encriptar el disc dur d'una màquina amb Windows, el PC risc d'infectar-se amb el conseqüent problema.

- Cap sistema està lliure de tindre una vulnerabilitat i poder ser infectat d'alguna manera. La pèrdua d'informació per una infecció o que el servidor puga ser controlat per una persona malintencionada pot provocar una pèrdua molt gran en la qualitat del servei.

Per aquest motiu, garantir el màxim possible que els correus electrònics enviats i rebuts per nostre servidor estan lliure de virus és fonamental. En aquest sentit la solució lliure per excel·lència i que a més millor s'integra amb el MTA(Postfix) escollit a aquest estudi és ClamAV. Dissenyat especialment per a servidors de correu que corren sobre Linux, ClamAV, és una eina que tot servidor de correu ha de tindre. Escaneig de fitxers comprimits en diferents formats, escaneig ràpid, soport per a la majoria de correus electrònics o les potents opcions disponibles en la terminal són algunes de les seues principals característiques.

Per últim, altre aspecte molt important en un servidor de correu és la gestió que es fa del spam. L'spam és el correu no desitjat que tots els usuaris reben a les seues busties si l'administrador del servidor de correu no fa res al respecte. Normalment el contingut d'aquests correu sol ser publicitari o intentant que el receptor caiga en algun tipus d'engany per estafar-lo. En el mon del programari lliure, una de les solucions més utilitzades per a minimitzar la quantitat de correu spam que un usuari rep és SpamAssassin.

SpamAssassin (i la majoria de productes antispam) s'integra amb el MTA i analitza els correus entrants amb diferents tècniques. Al acabar aquests anàlisis assigna un valor al correu electrònic que va de 0 a 5. Depenent de com estiga configurat, tots els correus que tinguen un valor igual o superior al configurat seran entregats. La resta es descartaran.

Seguint aquest mètode si configurem SpamAssassin per a que filtre correus amb un valor igual o superior a 0, tots els correus arribaran als seus destinataris. Per contra si es configura SpamAssassin amb un valor de 5, molts pocs correus seran entregats. Un valor acceptable per a no que el nombre de falsos positius, és a dir correus lícits que es cataloguen com a spam, podria ser 3.5.

Aquests anàlisis dels correus electrònics es fan amb tècniques heurístiques, utilitzant llistes DNS negres i blanques per a identificar servidors que envien spam massiu coneguts, filtres de detecció basats en checksums i hashcash com a mètode de prova de treball entre d'altres. Cal destacar que SpamAssassin intenta millorar-se a si mateix mitjançant filtres Bayesians, aprenent de correus que són spam i correus que no ho són. Per a aquest últim mètode l'usuari ha de alimentar SpamAssassin per a la qual cosa SpamAssassin proveïx de les instruccions de terminal necessàries.

Al exemple proposat en l'annex VI, també s'inclou amavis. Amavis és un filtre de contingut que fa ús de clamav i spamassassin.

10.8 Instal·lació de la solució de correu electrònic

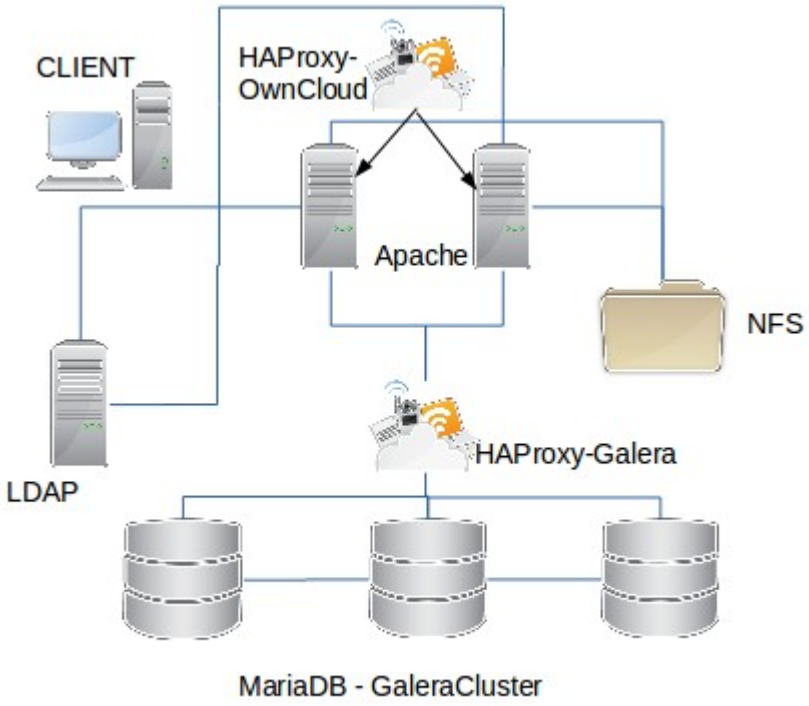
El procés detallat de la instal·lació del sistema proposat es pot trobar a l'**annex VI -Instal·lació solució de correu electrònic.**

11. Servidor de fitxers cloud

A aquesta secció es detallara la solució adoptada com a servidor de fitxers cloud. Al disseny d'aquesta solució s'han incorporat els mecanismes necessaris per a que el sistema siga tolerant a fallades i la càrrega puga ser balancejada entre diferents servidors. S'ha escollit Owncloud com a aplicació. Owncloud fa ús de una base de dades, un servidor web i un directori on emmagatzema les dades. Per la base de dades s'ha escollit MariaDB implementant un cluster Galera, el servidor web Apache i s'emmagatzemen les dades dels usuaris a un recurs compartit per NFS. Així mateix, la validació d'usuaris es farà mitjançant un servidor LDAP

11.1 Diagrama de la solució

A continuació es mostra el diagrama general de la solució proposada.



Il·lustració 11.1 Disseny arquitectura Owncloud

Com es veu a la imatge la proposta esta basada en separar els serveis que requereix OwnCloud per a funcionar correctament i fer treballar cada servei en cluster quan siga possible. Seguint com a punt de referencia la documentació oficial d'Owncloud, amb aquesta infraestructura, es podria donar servei des de 150 a 1000 usuaris (afegint algun servidor web més) amb una capacitat d'emmagatzematge de fins 200TB.

En qualsevol cas, aquest disseny és molt escalable i seria fàcil ampliar-lo en cas de ser necessari. En les següents seccions es detalla cada servei requerit i la seua funció dins de la solució proposta.

11.2 MariaDB

MariaDB és un gestor de base de dades derivat de MySQL amb llicencia GPL. Amb la compra de Sun Microsystems per part d'Oracle, un dels fundadors de MySQL AB, empresa creadora de

MySQL i que havia sigut comprada anteriorment per Sun, crea MariaDB per garantir que el projecte continuara baix els paràmetres del programari lliure. MariaDB continua avui dia essent desenvolupada per el seu fundador i la comunitat de desenvolupador de programari obert.

Al ser una derivada d'aquesta, MariaDB, té una alta compatibilitat amb MySQL atés que compartix les mateixes ordres, interfícies, APIs i biblioteques. De fet, la idea dels seus creadors és que es puguen intercanviar l'un per altre sense cap problema. En la practica MariaDB pot reemplaçar la mateixa versió de MySQL amb algunes diferencies com ara l'ampliació del nombre de mecanisme d'emmagatzemament, millor rendiment de l'optimitzador i per a molts ser més fàcil d'utilitzar.

En el diagrama plantejat, s'instal·laran tres servidors de base de dades amb MariaDB. Aquests servidors estaran configurats en cluster i tots ells estaran actius en mode escriptura. La capa d'aplicació accedirà a la base de dades mitjançant un balancejador de càrrega, HAProxy.

11.2.1 MariaDB Galera cluster

Amb MariaDB Galera Cluster es poden crear multi-màster clusters síncrons, és a dir que es pot escriure en qualsevol dels nodes del cluster i cada canvi és replicat en temps real en els demés nodes. Només esta disponible en la versió Linux de MariaDB i soporta els motors d'emmagatzemament XtraDB i InnoDB.

Algunes característiques més de GaleraDB són:

- Control automàtic de la pertinença d'un node al cluster
- Vertadera replicació paral·lela
- Connexió directa dels clients

Per a aquest projecte s'ha optat per aquesta solució atés que el que es busca és un sistema que siga el més escalable possible i Galera aporta eixa escalabilitat tant a nivell d'escriptura con de lectura en la base de dades. Cal destacar que amb aquesta solució també es dona un pas important per aconseguir que en ningun cas es puga produir una pèrdua d'informació.

Per últim, també es poden trobar millores en el rendiment en comparació amb els sistemes de clustering tradicionals per MySQL amb tan sols un node per l'escriptura i la resta per a lectura. El retard que normalment es produeix al llegir en un node esclau es redueix així com la latència des dels clients. A més, ens estalviem la faena extra que s'ocasiona quan el servidor màster del cluster es cau i tenim que convertir un dels esclaus en mestre.

A aquest estudi es proposa un disseny de Galera cluster amb tres nodes que seran accessibles mitjançant un balancejador de càrrega.

11.3 Owncloud: servidor web

Owncloud és principalment una alternativa lliure a les opcions privatives i comercials que hi ha al mercat en l'àmbit dels serveis emmagatzematge d'arxius en núvol.

La part visible per a l'usuari és la interfície web d'Owncloud. Accessible des de qualsevol navegador web és la porta d'entrada als arxius emmagatzemats pels usuaris així com les aplicacions que estiguen disponibles.

Il·lustració 11.2 Login Owncloud

Per a servir aquesta interfície web, OwnCloud fa ús d'un servidor web. A aquest projecte, tal i com ja s'ha fet amb anteriors productes, el servidor web escollit és Apache.

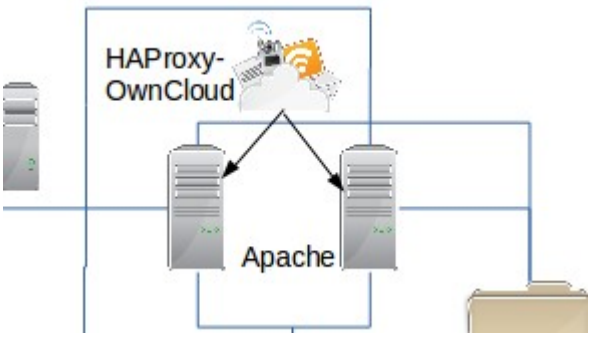
En el disseny plantejat, disposarem de dos servidors amb Apache instal·lat i un balancejador de càrrega amb HAProxy instal·lat per a distribuir les peticions d'accés garantint el millor servei possible i la optimització dels recursos. Així mateix, l'ús d'aquest balancejador farà molt més fàcil poder afegir més nodes en la capa d'accés d'Owncloud en cas de que el nombre d'usuaris que han de accedir al servei augmente.

11.4 HAProxy

HAProxy és probablement el més popular balancejador de càrrega TCP/HTTP de programari lliure. L'ús més comú que té és millorar el rendiment i la fiabilitat de diferents sistemes distribuint la càrrega entre diferents servidors, ajudant així aquesta millora de rendiment i afavorint la escalabilitat del servei balancejat.

HAProxy treballa bàsicament a les capes 4 (capa de transport) i 7 (capa d'aplicació) de la pila OSI. El tipus més fàcil de balanceig és el de capa 4: totes les peticions que li arriben a un port determinat són reenviades a un dels servidors que estan al back-end. El servidor que rep la petició del usuari li contesta directament.

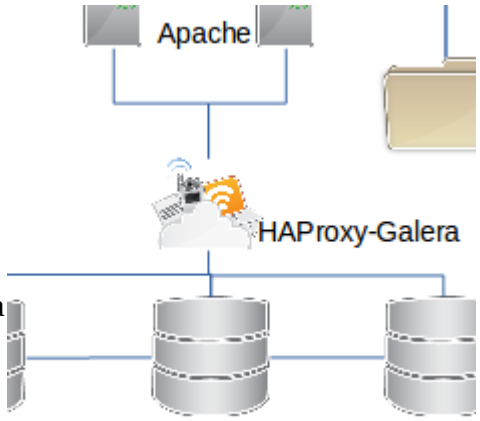
És important que la informació que aquests servidors poden llegir siga la mateixa per a que siga quin siga el servidor que conteste, l'usuari trobe respostes consistents Aquest és el tipus de balanceig emprat en la part frontal de la instal·lació d'Owncloud proposada tal i com es mostra a la il·lustració 11.3.



Il·lustració 11.3 Balanceig aplicació

Per a aconseguir aquesta integrat en la informació que gestionen els backend aquests accedeixen a la base de dades emprada per Owncloud mitjançant altra instancia d'HAProxy que redirecciona les peticions als servidors MariaDB tal i com es mostra en la imatge adjunta.

El balanceig de capa 7 funciona de manera diferent. En aquest les peticions són reenviades en base al contingut de la petició.



Il·lustració 11.4 Balanceig Galera

11.4.1 Algoritmes de balanceig, health check i sticky sessions.

HAProxy pot utilitzar diferents algoritmes de balanceig. A demés se li pot assignar un pes a cada servidor per a manipular la freqüència amb que un servidor es seleccionat. A continuació s'esmenten alguns:

- **Round Robin:** És l'algoritme per defecte. HAProxy selecció un servidor diferent cada vegada que rep una petició fins que ja els a utilitzat tots i torna a començar.
- **Leastconn:** El servidor que menys connexions actives té es seleccionat. Aquest algoritme és molt recomanable per a sessions llargues.
- **Source:** Amb aquest algoritme es calcula quin servidor serà seleccionant creant un hash de la direcció IP del client que envia la petició. D'aquesta manera s'intenta garantir que el client es connectarà sempre al mateix servidor.

En línia amb l'últim algoritme de balanceig, algunes aplicacions requereixen que el client sempre es connecte al mateix servidor. Owncloud requereix aquesta persistència a causa de la gestió local de les sessions en el servidor d'aplicacions. Açò s'aconsegueix amb el que s'anomena en anglés sticky sessions (o sessions persistents).

Altre dels aspectes destacable d'HAProxy és health check (comprovació de la salut). HAProxy comprova que els servidors backend estan disponibles abans d'enviar una petició. Si el servidor no contesta la comprovació, automàticament és deshabilitat i no se li reenvien més peticions fins que no torne a estar disponible.

A aquest estudi s'han utilitzat les sticky sessions i l'algoritme Source.

11.5 LDAP i NFS

Els últims aspectes a comentar de la implementació proposta d'Owncloud són la autenticació i l'emmagatzemament dels arxius dels usuaris. Per l'autenticació s'ha utilitzat un servidor LDAP. Com a la resta de productes estudiats a aquest projecte s'ha fet ús d'OpenLDAP.

Per a l'emmagatzemament dels arxius dels usuaris, s'ha creat un servidor NFS. NFS per les seues

sigles en anglés Network File System és un sistema de fitxers en xarxa amb arquitectura client-servidor. Funciona de tal forma que el servidor exporta a la xarxa una o més carpetes locals amb uns permisos definits. D'altra banda, els clients munten aquestes carpetes com si d'un disc local es tractara.

A la nostra proposta de projecte s'ha fet servir NFS en dos situacions. Primerament s'ha establert com a directori de dades , un directori al servidor NFS. Així, tots els servidors d'aplicació d'Owncloud accediran només a una copia dels arxius dels usuaris preservant així la seua integritat. D'altra banda, per a que tots els servidors d'aplicació tinguen la mateixa configuració , el directori /var/www/owncloud on estan tots els arxius d'Owncloud també estan a un directori NFS que es munta a cada servidor d'aplicacions abans de que arranque Apache. D'aquesta manera s'aconsegueix que tots ells tinguen la mateixa configuració.

11.5.1 Aplicacions en Owncloud

Owncloud no només és un servidor d'arxius en el núvol. També incorpora moltes aplicacions que es poden activar per a donar-li més funcionalitat al servei. Aplicacions de edició col·laborativa de documents, visualització integrada de diferents tipus de documents, calendaris, notes, reproductor de música, galeria de fotos o lector RSS són algunes d'elles.

Amb totes aquestes aplicacions no només podem afegir-li valor a l'experiència de l'usuari proporcionat-li a aquest algunes eines més, a més, podem afegir funcionalitat a nivell de gestió com ara un antivirus que s'integre amb Owncloud o un formulari de registre per instal·lacions que utilitzen la base de dades local. En aquest sentit una aplicació que s'ha tingut que instal·lar per a la implementació d'Owncloud proposada a aquest project és **LDAP User and Group Backend**. Aquesta aplicació és la que ens ha proporcionat la funcionalitat per poder validar usuaris amb el servidor LDAP

11.6 Instal·lació d'Owncloud

Per a la instal·lació de la solució proposada per a Owncloud s'ha d'instal·lar els node amb MariaDB del cluster Galera i configurar-los. Tot seguit s'instal·larà un servidor amb HAProxy per al balanceig dels nodes del cluster Galera. Després s'ha d'instal·lar tant el servidor NFS com el servidor LDAP i per últim s'instal·laran els servidors web amb els fitxers d'Owncloud i servidor amb HAProxy per a distribuir la càrrega. La descripció detallada de cada un d'aquest passos es pot trobar a l'**annex VII – Instal·lació i configuració d'Owncloud**

12. Servidor intermediari

A aquest secció s’explica què és un servidor intermediari (proxy) , els usos més comuns d’aquest tipus de servidor aixi com la solució de programari lliure (Squid) escollida per a aquest estudi.

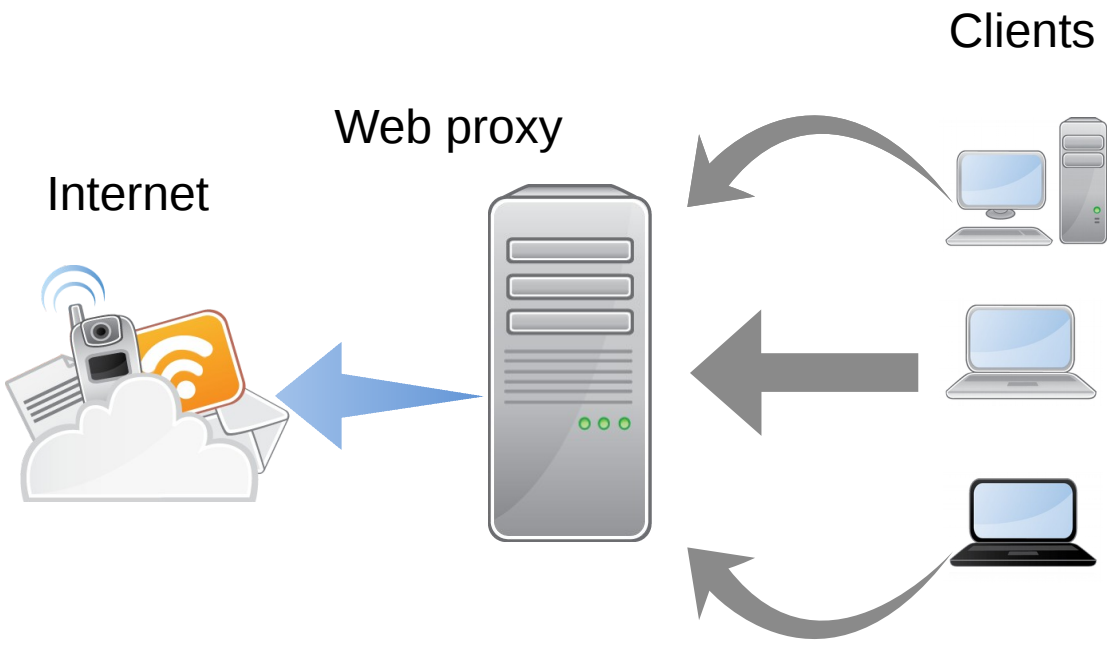
12.1 Què és un servidor intermediari o proxy server

En l'àmbit de les xarxes de computadors, un servidor intermediari o servidor proxy és una màquina que es situa entre els clients i el o els servidors on volen accedir aquests clients. D’aquesta manera el servidor proxy estableix connexions indirectes entre els clients i altres serveis de xarxa. El client envia una petició al servidor proxy i aquest demana una connexió, un arxiu o qualsevol altre recurs al servidor remot. Si hi ha contestació, el servidor intermediari contesta el client o be connectant-lo

amb el servidor remote o servint la informació des de la seua memòria cau.
Hi han tres tipus de servidors proxy:

- **Gateway:** Aquest tipus de servidor envia peticions i respostes sense modificar.
- **Forward proxy:** Normalment accessible des d'Internet es utilitzat per a connectar amb un ampli rang de fonts . En la majoria dels casos açò significa qualsevol lloc d'Internet.
- **Reverse proxy:** Serveix com a frontal d'algun servei per a controlar i protegir l'accés al mateix. Normalment, fa tasques de balejador de carrega, autenticació, desencriptació o memòria cau. El servidor HAProxy emprat al capítol d'Owncloud es un bon exemple d'aquest tipus de servidor intermediari

Un dels servidors intermediaris més comuns a qualsevol empresa és un servidor intermediari de serveis web. Hi ha molts motius per instal·lar un d'aquest servidors però cal destacar dos sobre els demés: control de les pagines a les que s'accedeix i velocitat d'accés.



Il·lustració 12.1 Exemple disseny implementació de servidor intermediari

Aquestes són les principals avantatges de l'ús d'un servidor intermediari a una xarxa:

- Control sobre les comunicacions
- Emmagatzemament de les pagines web a la memòria cau accelerant aixi accessos futurs
- Facilitat de crear un llistat de direccions prohibides
- Denegar la cerca de paraules prohibides
- Denegar l'accés a Internet d'un segment concret de la xarxa
- Mantindre informes de connexió per avaluar l'ús que es fa dels recursos
- Augment en la seguretat contra elements externs a la xarxa

Tot i que els avantatges són molts més que els inconvenients, a continuació es llisten els més importants:

- Per a que les aplicacions puguen accedir a la xarxa, hi ha que configurar-les una a una.

- Totes les comunicacions amb l'exterior passen pel servidor intermediari. És per això que es deu tindre un sistema tolerant a fallades per a no quedar-se mai sense servei
- El servidor requereix manteniment i per tant hem de tindre personal qualificat per a revisar, actualitzar, mantindre i reparar el servidor.

Altre aspecte important que un servidor intermediari pot proporcionar és anonimat. Des d'aquest punt de vista es poden diferenciar quatre tipus de servidor:

- **Servidor intermediari transparent:** Aquest tipus de servidor s'identifica a si mateix com a servidor intermediari i revela la direcció IP original mitjançant les capçaleres http. S'utilitzen normalment com a servidors de memòria cau per a servir llocs web més ràpidament als client als que serveix.
- **Servidor intermediari anònim:** Aquest tipus de servidor s'identifica a si mateix com a servidor intermediari però no exposa la direcció IP original del client. Aquest tipus de servidor és detectable però dona cert grau d'anonimat.
- **Servidor intermediari de distorsió:** Aquest servidor també s'identifica com a servidor intermediari però el que fa public és una direcció IP falsa a traves de les capçaleres http.
- **Servidor intermediari d'alt anonimat:** És el més anònim de tots. Aquest tipus no s'identifica com a servidor intermediari i no fa disponible la direcció IP original.

12.2 SQUID

Com a solucion de programari lliure es proposa Squid. Squid és un servidor intermediari web amb memòria cau. L'ús més estés d'Squid és com servidor intermediari i de memòria cau per a HTTP(s) i FTP entre d'altre protocols de xarxa. També soporta peticions SSL/TLS i actua com a memòria cau de les peticions DNS. D'entre els mètodes de memòria cau, Squid, soporta una gran varietat de protocols com ara ICP, HTCP, CARP i WCCP.

Lliberat baix llicencia GPL, Squid, és una gran solució per a gran varietat de necessitats. Un dels seus punts forts és que cobreix tant les necessitats d'una xicoteta oficina com les de una xarxa empresarial de grans dimensions. Squid, dissenyat per a sistemes operatius GNU/Linux, també es pot executar en altres sistemes basats en Unix o inclús sobre Windows.

12.3 Instal·lació i configuració d'Squid en Ubuntu 16.04

- Instal·lar Squid amb apt-get:

sudo apt-get install squid3

```
campus@ubuntu16:~$ sudo apt-get install squid3
[sudo] contrasenaya per a campus:
S'està llegint la llista de paquets… Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat… Fet
The following additional packages will be installed:
  libecap3 squid squid-common squid-langpack
Paquets suggerits:
  squidclient squid-cgi squid-purge smbclient winbindd
S'instal·laran els paquets NOUS següents:
  libecap3 squid squid-common squid-langpack squid3
0 actualitzats, 5 nous a instal·lar, 0 a suprimir i 138 no actualitzats.
S'ha d'obtenir 2686 kB d'arxius.
Després d'aquesta operació s'empraran 11,0 MB d'espai en disc addicional.
Voleu continuar? [S/n]
```

Il·lustració 12.2 Instal·lació de Squid

Per a configurar Squid hem d'editar l'arxiu **/etc/squid/squid.conf** . A continuació es detallen algunes de les configuracions bàsiques que es podem fer amb Squid:

- Habilitar l'ús d'Squid a una xarxa determinada i nomes en l'horari de l'empresa:

  http_access allow interna1 hores_interna1

  acl interna1 src 192.168.56.0/24
  acl hores_interna1 time M T W H F 8:00-18:00

Amb aquestes directives, s'habilita que els dispositius de la xarxa interna1 (192.168.56.0/24) puguen utilitzar Squid de Dilluns a Divendres(M T W H F són les inicials dels dies de la setmana en anglés excepte Dijous que es representa amb una H) de 8:00 a les 18:00.

- Denegar l'accés a Facebook.

  http_access deny acces_denegat
  http_access allow all

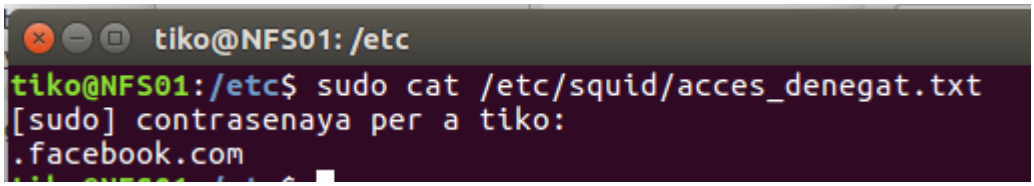
  acl acces_denegat url_regex "/etc/squid/acces_denegat.txt"

Amb aquestes directives denegem l'accés a les urls especificades a la acl acces_denegat. En aquesta acl podem observar que hem especificat que les urls prohibides estan a l'arxiu /etc/squid/acces_denegat.txt.

L'opció url_regex s'utilitza per poder fer ús d'expressions regulars al fitxer on s'emmagatzemen les urls que volem denegar, en aquest exemple **/etc/squid/acces_denegat.txt**. És important afegir la directiva ***http_access allow all*** per a permetre l'accés a la resta d'urls que no estan incloses a l'arxiu d'urls denegades.

Per a denegar l'accés a facebook.com i tots els seus subdominis, escriurem el següent a l'arxiu definit en la nostra acl:

.facebook.com



Il·lustració 12.3 Contingut de l'arxiu /etc/squid/acces_denegat.txt

És important el punt davant el nom del domino. Aquest punt el que farà és afegir a la llista tots els subdominis de facebook.com com per exemple es-es.facebook.com tant per http com per https.

Alguns altres paràmetres que són recomanables configurar a l'arxiu **/etc/squid/squid.conf** són els següents:

- Canviar el port per defecte d'Squid

  http_proxy 8888

- Limitar la quantitat de memòria RAM que empleada per Squid. Una bona mida és utilitzar un terç del total de memòria disponible al sistema. Com el nostre sistema disposa de 512MB utilitzarem 192 per a Squid i la resta per el sistema :

  cache_mem 192MB

- Establir la quantitat d'espai en disc utilitzat per a la memòria cau d'Squid. Com a referencia utilitzarem el 50% de l'espai disponible al sistema. A aquesta directiva, també hem de definir el format que utilitza Squid (ufs), el directori on volem que s'emmagatzeme la memòria cau, la mida en MB i el nombre de subdirectoris de primer i segon nivell.

  cache_dir ufs /var/spool/squid 20000 16 256

A l'annex VII es detalla com configurar Firefox i apt per a que utilitzen un servidor intermediari.

13. Servidor VPN

A aquesta secció es detalla que és un servidor VPN aixi com la solució basada en programari lliure recomanada.

13.1 VPN

Una VPN (en anglés Virtual Private Network) permet crear un connexió segura des d'una xarxa a altra a traves de Internet. Quan un dispositiu es connecta a un xarxa utilitzant un connexió VPN, el dispositiu podrà accedir als recursos d'aquesta xarxa com si es trobara físicament connectat a la mateixa.
Els usos més estesos d'una VPN són els següents:

1. Accedir a la xarxa de l'empresa quan s'esta de viatge o a casa: De vegades, és necessari connectar-se als recursos de l'empresa des de fora de la xarxa per estar de viatge de negocis o per a poder treballar des de casa. Una VPN solventa aquesta situació i permet els treballadors accedir als recursos empresarials des de qualsevol lloc on tinguen una connexió a Internet
2. Accedir a una xarxa domestica: Igualment es pot fer ús d'una VPN per a accedir a la xarxa que tenim a casa quan estem de vacances
3. Amagar dades de navegació: Si ens connectem a Internet a una xarxa publica (restaurants,hotels etc), tot el trafic que generem i que no estiga encriptat és potencialment visible per a qui puga saber on mirar. Amb una VPN l'únic visible serà la connexió a la VPN, la resta serà anònim
4. Evitar un bloqueig geogràfic: De vegades hi ha serveis que tenen un bloqueig geogràfic que evita que es puguen utilitzar des d'altres països per exemple. Amb una VPN situada al país on si que és possible gaudir d'aquests serveis es podria saltar el bloqueig

5. Evitar censures: Desafortunadament encara queden països on la llibertat a Internet i altres àmbits no existeix. Hi ha governs que censuren pagines que van en contra del regim i no són accessibles directament des de els proveïdors locals. Amb una VPN a un altre país, es pot evitar aquesta restricció i accedir al contingut censurat.

A continuació es detallen els dos tipus de VPN més comuns des del punt de vista de la seua arquitectura:

- **VPN d'accés remot:** Consisteix en que diferents usuaris o proveïdors situats a diferents llocs es connecten a traves d'Internet a una empresa. Quan ja s'han autenticat, normalment, tenen un nivell d'accés similar al que tindrien si foren físicament a l'empresa.
- **VPN punt a punt:** Aquesta arquitectura s'utilitza per a unir oficines o sucursals de la mateixa empresa entre elles o amb l'oficina central. D'aquesta manera es crea un enllaç permanent entre dos llocs creant aixi la sensació d'estar treballant a la mateixa xarxa

El protocol estàndard per a establir la encriptació de xarxes VPN és IPSEC però també s'utilitzen PPTP,L2F,L2TP,SSL/TLS o SSH. Cadascun d'ells amb els seus avantatges i inconvenients quant a la seguretat, facilitat d'ús , el manteniment i la quantitat de tipus de clients soportats.
Com a solució empresarial proposta en aquesta estudi s'ha escollit OpenVPN.

13.2 OpenVPN

OpenVPN és la solució VPN de programari lliure escollida. Creada a l'any 2001, ofereix una gran combinació quan a la seguretat que ofereix, la facilitat d'ús i la gran quantitat de característiques que inclou. OpenVPN incorpora dos mecanismes de seguretat, un basat en claus estàtiques pre-compartides i l'altra en SSL/TLS fent ús de certificats i claus RSA. Tot i que SSL/TLS amb l'ús de claus RSA és més segura, les claus estàtiques són més fàcils de configurar.
Alguns del principals avantatges d'OpenVPN són:

- Protecció dels usuaris remots
- Les connexions OpenVPN podes ser fetes a traves de gaire be qualsevol tallafocs. Si podem accedir a contingut https, un túnel OpenVPN deuria funcionar sense problemes
- Soport per a servidor intermediari
- Nomes requereix d'obrir un port en el tallafocs per a permetre les connexions atés que OpenVPN 2.0 accepta múltiples connexions al mateix port.
- Interfícies virtuals que permeten la implementació de regles de tallafocs molt especifiques
- Soport transparent per a IPs dinàmiques. S'elimina la necessitat de fer ús d'adreces estàtiques
- Tan els clients com el servidor poden estar a xarxes que fan ús d'IPs privades.
- Instal·lació fàcil en qualsevol plataforma

Com a principal inconvenient cal destacar que no és compatible amb IPSEC que actualment és l'estàndard de facto en solucions VPN. A l'annex IX es troba el detall d'una instal·lació bàsica d'OpenVPN

Conclusions i millores

Després d'analitzar tots els sistemes plantejats en un inici, és clar que hi han solucions millors que altres front als seus competidors. En l'apartat de virtualització, Proxmox, millora cada dia més i és una realitat si de mitjanes empreses estem parlant tot i que no seria descartable a la gran empresa. Tal vegada li queda camí per recórrer en alguns aspectes front a solucions com les de VMWare però és igual de cert que incorpora algunes coses com la tecnologia de contenidors que el fan estar molt a prop.

En els apartat tant d'autenticació d'usuari, com en el servei DHCP o els servidor DNS, en cap motiu es pot dir que les solucions de programari lliure són pitjors. OpenLDAP simplement implementa un estàndard de sobra provat i que res té que envejar al Directori Actiu de Microsoft. El mateix aplica al servei de DHCP i molt més a Bind què és probablement el servidor DNS de referència a Internet.

Si hi ha un aspecte on si que la solució proposada no és de gran qualitat és en CUPS. El servidor d'impressió no té un rendiment òptim però és important destacar que la majoria de problemes que algú es pot trobar són per falta de disponibilitat de controladors i en això el CUPS no té molt a vore. SAMBA és altre dels elements que demostra que el programari lliure és de qualitat.

Per últim, tant la solució de correu, com el gestor de continguts com el servidor d'arxius en núvol són solucions punteres al mercat que estan presents a quantitat de empreses de hosting que donen servei a moltíssimes empreses.

En definitiva, les conclusions que es poden traure d'aquest estudi són clares, hi ha alternatives de programari lliure per a qualsevol servei dels plantejats a aquest projecte. No és tan important destacar que hi han alternatives com el fet de que aquestes alternatives són en molts casos igual o de més qualitat que qualsevol dels seus competidors al mercat. Per tant una empresa amb programari lliure és viable.

Per al futur, hi ha molts aspectes que aprofundir de cada una d'aquestes tecnologies i que en aquest projecte no s'han tractat. La implementació de cada sistema ha sigut bàsica en alguns d'ells i més complexa en altres com ara el servei de correu electrònic, el servidor d'arxius en núvol (Owncloud) o l'hipervisor de màquines virtuals (Proxmox) tot i que en tots ells hi ha marge per a continuar treballant..

A continuació es destaca un o més aspectes a treballar en alguns d'ells:

- **Proxmox:** Aprofundir a nivell pràctic en l'alta disponibilitat, la creació de diferents VLANs i el sistema de backup
- **OpenLDAP:** Estudi de les possibilitat que ofereix OpenLDAP en l'àrea de l'alta disponibilitat.
- **DHCP:** Implementació del DHCP fingerprinting
- **SAMBA i CUPS:** Instal·lació de controladors d'impressores a clients Windows i integració amb OpenLDAP(Samba)

- **Servei de correu:** Creació de certificats d'usuaris per xifrar i signar els correus així com implementació de mecanismes d'alta disponibilitat. A més, aprofundir en les possibilitats que ofereix Amavis(tant ClamAV com SpamAssassin)
- **OpenVPN:** Estudi en profunditat de les opcions que ofereix la solució implementada i proves a un entorn real amb IP pública etc.
- **Servidor intermediari:** Ampliar la personalització del servei, estudiant els diferents filtres existents. Crear missatges de denegació personalitzats etc.

Altre aspecte important que no s'ha tractat del tot a aquest estudi és la integració de totes aquestes tecnologies formant un únic ecosistema. A l'estudi s'ha tractat cada sistema per separat tot i que la integració entre ells s'ha afegit al disseny de cada solució, en la implementació pràctica, els serveis comuns, no sempre han sigut els mateixos. Un exemple ha sigut el servidor d'autenticació OpenLDAP que a totes les proves ha estat el mateix. En canvi, els diferents certificats emprats en cada servei no s'han amb la mateixa CA.

Per últim, altre aspecte a investigar en el futur és la integració de tots els sistemes estudiats a aquest projecte amb sistemes d'altres plataformes. Un dels aspectes que no s'ha pogut tractar tot i ser un motiu per escollir una solució o altra ha sigut la integració amb sistemes del sistemes amb clients Windows. A més, queda pendent l'estudi d'aquesta integració a nivell de servidor també. Un clar exemple seria integrar el nostre servidor LDAP en un domini del Active Directory de Microsoft.

Glossari

Active Directory: Servei establert a un o més servidors on es creen objectes com ara usuaris, grups i màquines amb la finalitat d'administrar els seus inicis de sessió en els equips connectats a la xarxa. Com a protocol principal utilitza LDAP.

Apt-get: Instrucció de terminal del sistemes GNU/Linux basats en la distribució Debian que serveix per gestionar els paquets de programari

ARP (Address Resolution Protocol): Protocol de xarxa emprat per a traduir adreces IP (capa de xarxa) en adreces MAC (capa d'enllaç)

Balancejador de càrrega: Dispositiu de maquinari o programari que es situa davant un grup de servidors que atenen una aplicació i distribueixen les peticions dels clients entre ells intentant que la càrrega de cada membre del grup siga la mateixa. Aquesta distribució es fa emprant diferent algoritmes.

CA: És l'acrònim en anglés d'autoritat certificadora (Certification Authority). Entitat que expedeix certificats digitals per diferents propòsits com ara validar la identitat d'un servidor web o d'una persona

RSA: Algoritme de xifratge de clau pública. A aquest tipus d'algoritme, el client disposa de dues

claus, una pública que es pot distribuir a tothom i una privada que es manté en secret. Els missatges són xifrats amb la clau pública del receptor i només poden ser desxifrats amb la seua clau privada.

Commutador: Dispositiu digital que s'utilitza per a interconnectar màquines i que opera en la capa d'enllaç de la pila OSI.

Controlador de impressora: En terme generals, un controlador és l'aplicació que permet el sistema operatiu interactuar amb un dispositiu de maquinari, Un controlador de impressora seria l'encarregat de establir la comunicació entre el sistema operatiu i una impressora.

Direcció IP: Nombre que identifica de manera lògica i jeràrquica una interfície de xarxa que utilitze el protocol IP.

Direcció MAC: Identificador de 48 bits que correspon de forma única a una targeta o dispositiu de xarxa. També es coneix com a adreça física i és única per a cada dispositiu.

Distribució Linux: Distribució de programari basada en el nucli o kernel Linux que inclou un conjunt de paquets per satisfer les necessitats d'un segment d'usuaris en concret. Hi ha distribucions orientades a l'educació , a algun àrea científica o a l'usuari domèstic.

Encaminador: Dispositiu que proporciona connectivitat de xarxa el qual té com a funció principal enrutar paquets d'una xarxa a un altra.

FTP: Protocol de transferència d'arxius entre dos dispositius connectats a una xarxa TCP. Està basat en una arquitectura client-servidor.

GNU/Linux: Terme que s'empra per a denominar a la combinació del nucli o kernel Linux amb diferents paquets de programari que el converteixen en un sistema operatiu complet. Sinònim de distribució Linux.

Hash: Algoritmes que aconsegueixen generar a partir d'una entrada una eixida que resum el contingut de la entrada i que només es pot tornar a generar amb la mateixa entrada. Són molt útils per a comprovar que, per exemple, un arxiu no ha sigut modificat des de la seua publicació.

HTTP: Protocol que permet la transferència de informació en la World Wide Web

HTTPS: Protocol d'aplicació segur basat en http destinat a la transferència segura de dades al hipertext. És a dir, es la versió segura de HTTP.

IMAP: Protocol d'aplicació que permet l'accés a missatges de correu electrònic emmagatzemats a un servidor.

LAMP: Acrònim de Linux Apache MySQL i PHP. Són un conjunt de serveis de programari lliure que formen un ecosistema per a soportar aplicacions web.

LDAP: Són les sigles Lightweight Directory Access Protocol i fan referència a un protocol de la capa d'aplicació que permet l'accés a un servei de directori ordenat i distribuït per cercar diversa informació a un entorn de xarxa.

MAC OS: Sistema operatiu basat en Unix dels ordinadors personals fabricats per la multinacional americana Apple.

Màscara de xarxa: Combinació de bits que serveix per a delimitar l'àmbit d'una xarxa d'ordinadors.

MDA: Són les sigles de Mail Delivery Agent. Part d'un sistema de correu electrònic encarregada de rebre els correus des del MTA i emmagatzemar-los en les busties dels usuaris

MTA: Són les sigles de Mail Transport Agent. Part d'un sistema de correu electrònic que s'encarrega principalment de rebre missatges d'altre MTA i enviar missatges a altre MTA

MTU: Sigles en anglés de Maximum Transfer Unit. És la unitat que quantifica la mida en bytes de la unitat de dades més gran que es pot enviar amb un protocol de comunicacions determinat.

NIS: Protocol desenvolupat per Sun Microsystems per al enviament de dades de configuració en sistemes distribuïts com noms d'usuaris o equips entre computadors d'una xarxa.

NTP: Protocol d'Internet emprat per a sincronitzar rellotges de sistemes informàtics

OU: Del anglés Organizational Unit, s'utilitza en serveis de directori basat en LDAP per a organitzar usuaris, grups i màquines(o recursos en general) jeràrquicament.

PHP: Llenguatge de programació de programari lliure per a programar del costat del servidor que s'utilitza en pàgines web de contingut dinàmic.

Pila OSI: Model de pila de protocols que els organitza per capes on els protocols de les capes inferiors proporcionen serveis als protocols en capes superiors.

POP3: Protocol que s'utilitza per a recuperar correus electrònics emmagatzemats a un servidor.

Programari lliure: Programari que per elecció del seu autor pot ser copiat, modificat i distribuït. Es considera programari lliure si es pot utilitzar per a qualsevol propòsit, estudiar i modificar-lo per adaptar-lo a les nostres necessitats, si es pot distribuir lliurement i si es pot millorar el codi i distribuir-lo.

Proxy: Un proxy és una programa o dispositiu que realitza un acció en nom d'un altre. Per exemple, l'equip A envia una petició de servei a l'equip B que reenviarà aquest petició a l'equip C que mai sabrà que l'originador de la petició és l'equip A. Així mateix, A mai no sabrà que ha sigut C qui donat resposta a la seua petició.

Reenviador DNS: A un servidor DNS, un reenviador es altre servidor DNS que dona resposta a les consultes de zones de les quals no es propietari. És a dir, si el nostre servidor DNS només es propietari de la zona local.lab, si rep una consulta d'una màquina al domini remot.lab, aquesta consulta serà redireccionada al reenviador DNS.

RSS: Sigles de Really Simple Syndication , és un format XML per a compartir contingut en la web. S'utilitza per a difondre informació actualitzada freqüentment a usuaris subscrits a una font de continguts.

Servidor de fitxers en núvol: Servidor que emmagatzema arxius i que és accessible des de qualsevol lloc inclús Internet

SMB/CIFS: Protocol de xarxa utilitzat per a proveir accés compartit a arxius, impressores i ports serie.

SMTP: Protocol emprat per a l'enviament de correu electrònic. El seu port per defecte és el 25

Spam: Correu no desitjat que arriba a les busties del usuaris d'un sistema de correu.

SSL/TLS: Protocols criptogràfics que proporcionen comunicacions segures a un xarxa.

SSH: Acrònim de Secure Shell, és el nom del protocol i el programa que l'implementa que serveix per a accedir remotament a altres màquines a través d'una xarxa. Utilitzat generalment per controlar completament una computadora remote mitjançant un terminal d'instruccions.

Terminal: A aquest projecte quan es parla de terminal es refereix a la aplicació que implementa Bash (Bourne again shell) que és un programa informàtic que té com a funció interpretar instruccions i un llenguatge de programació

Ubuntu: Distribució Linux basat en Debian (altra distribució). Actualment és una de les distribucions Linux amb més volum d'usuaris.

URI: Cadena de caràcters que identifica un recurs de xarxa de manera unívoca

Virus informàtic: Programa informàtic que té com a finalitat alterar el comportament normal d'una computadora sense el coneixement i el consentiment del seu propietari.

Webmail: Terme que fa referencia a una aplicació de tipus web que serveix per a accedir a la bustia de correu d'un usuari i poder així gestionar el correu d'aquest usuari.

Windows: Sistema operatiu de programari privatiu de la empresa americana Microsoft. És instal·lat per defecte per la majoria de fabricants d'ordinadors personals i domina el mercat tant als segment domestic com al segment empresarial. Té tant versió de client com de servidor.

World Wide Web: Sistema de documents interconnectats i accessibles des d'Internet

Bibliografia

Llibres:

Gerald, Carl LDAP System Administration. O'Really

Dent, Kyle D. Postfix, The Definitive Guide. O'Really

Ahmed,Wasim (2015) Proxmox Cookbook. Packt Publishing Ltd

Dubois, Paul (2013) MySQL. Addison-Wesley

Recursos en línia:

http://www.proxmox.org/en/

http://www.openldap.org/

https://help.ubuntu.com/community/BIND9ServerHowto

https://www.openssl.org/

https://help.ubuntu.com/community/isc-dhcp-server

https://www.samba.org/

https://www.cups.org/

https://wordpress.org/

http://www.postfix.org/

http://www.dovecot.org/

http://www.postfix.org/SASL_README.html

https://roundcube.net/

https://owncloud.org/

https://mariadb.org/

https://httpd.apache.org/

http://www.squid-cache.org/

https://openvpn.net/

https://es.wikipedia.org

https://en.wikipedia.org

https://help.ubuntu.com/14.04/serverguide/openvpn.html

https://help.ubuntu.com/lts/serverguide/network-file-system.html

https://blog.sprinternet.at/2016/03/mariadb-10-1-galera-cluster-on-debian-8-jessie/

http://galeracluster.com/documentation-webpages/haproxy.html

https://www.digitalocean.com/community/tutorials/how-to-use-haproxy-to-set-up-mysql-load-balancing--3

http://stackoverflow.com/questions/1559955/host-xxx-xx-xxx-xxx-is-not-allowed-to-connect-to-this-mysql-server

https://www.digitalocean.com/community/tutorials/how-to-install-and-secure-phpmyadmin-on-ubuntu-16-04

https://help.ubuntu.com/lts/serverguide/network-file-system.html

https://doc.owncloud.org/server/9.0/admin_manual/installation/source_installation.html#prerequisites-label

http://tutorialforlinux.com/2014/05/16/how-to-enable-apache-ssl-on-linux-ubuntu-14-04-trusty-lts-easy-guide/

https://doc.owncloud.org/server/9.0/admin_manual/configuration_server/harden_server.html

https://www.dalemacartney.com/2013/11/25/scaling-web-applications-red-hat-storage/5/

https://help.ubuntu.com/lts/serverguide/squid.html

http://askubuntu.com/questions/89437/how-to-install-packages-with-apt-get-on-a-system-connected-via-proxy

http://windows.microsoft.com/es-es/windows-vista/what-is-a-proxy-server

http://whatismyipaddress.com/proxy-server

http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html

https://parabing.com/2014/06/openvpn-on-ubuntu/

https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-14-04

https://help.ubuntu.com/community/OpenVPN

http://acidx.net/wordpress/2014/06/installing-a-mailserver-with-postfix-dovecot-sasl-ldap-roundcube/

http://www.jimmy.co.at/weblog/2005/12/05/postfix-and-sasl-debian/

https://www.e-rave.nl/create-a-self-signed-ssl-key-for-postfix

http://postfix.state-of-mind.de/patrick.koetter/smtpauth/postfix_tls_support.html

http://acidx.net/wordpress/2014/04/basic-openldap-installation-configuration/

http://www.productionmonkeys.net/guides/qmail-server/addons/ldap-addressbook/roundcube-ldap-addressbook

https://discussions.apple.com/thread/3965674?tstart=0

https://github.com/roundcube/roundcubemail/wiki/Configuration:-LDAP-Address-Books

https://github.com/roundcube/roundcubemail/wiki/Installation

https://debian-administration.org/article/618/Certificate_Authority_CA_with_OpenSSL

https://help.ubuntu.com/community/OpenSSL

http://acidx.net/wordpress/2012/09/creating-a-certification-authority-and-a-server-certificate-on-ubuntu/

https://www.nanotutoriales.com/como-crear-un-certificado-ssl-de-firma-propia-con-openssl-y-apache-http-server

http://www.vicente-navarro.com/blog/2009/02/22/crear-los-certificados-ssl-para-nuestro-servidor-web-https-con-apache-openssl-y-debian-lenny/

Recursos lingüístics:

http://www.termcat.cat/ca/Cercaterm/

Annex I – Instruccions interessants emprades al projecte

A continuació es llisten les instruccions per a una terminal en Linux que s'han utilitzat durant la implementació dels diferents sistemes d'aquest projecte:

sudo: Instrucció que s'utilitza per executar altres instruccions però amb els privilegis d'altre usuari de manera segura, normalment l'usuari root, convertint-se temporalment en super usuari.

Usos: *sudo instrucció*

Exemple: *sudo dpkg -i algun-paquet.deb*

apt-get: Gestor de paquets de les distribucions GNU/Linux basades en Debian.

Usos: *(sudo) apt-get opció (paquet(s))*

Exemples: *sudo apt-get update* (per actualitzar la base de dades de paquets. S'utilitza normalment al obrir el terminal o després d'afegir un nou repositori de programari)

sudo apt-get install apache2 (per instal·lar un paquet)

cd: Instrucció emprada per a canviar de directori

Usos: *cd /directori*

Exemples: *cd /etc/postfix*

wget: S'utilitza per a descarregar un arxiu

Usos: *wget «direcció del arxiu»*

Exemple: *wget http://www.arxius.com/programa.tar.gz*

nano: Editor d'arxius de text

Usos: *nano nom_de_arxiu_de_text*

Exemple: *sudo nano /etc/network/interfaces*

cat: Mostra en pantalla el contingut d'un arxiu

Usos: cat *nom_de_arxiu_de_text*

Exemple: *sudo cat /etc/network/interfaces*

ssh: Estableix una connexió per ssh amb altra màquina que tinga corrent un servidor ssh

Usos: ssh *nom_usuari_remot@ip_o_nom_maquina_remota*

Exemple: *sudo ssh usuari@192.168.1.10*

scp: Transfereix per ssh arxius a altra màquina

Usos: scp *nom_de_arxiu usuari_remot@IP_o_nom_maquina_destí*

Exemple: *sudo scp text.txt usuari@192.168.1.20*

sudo scp text.txt usuari@192.168.120:/etc/postfix (copia l'arxiu al directori /etc/postfix de la màquina remota)

systemctl: *Serveix per a controlar systemd que es el gestor del sistema i els serveis per defecte a algunes distribucions Linux.*

Usos: *systemctl instrucció servei*

Exemple: *sudo systemctl status/start/stop/restart mariadb.service (dona ordres al servei MariaDB)*

service: Igual que systemctl però només interactua amb serveis. Interactua amb init.d scripts

Usos: service *ordre nom_de_servei*

Exemple: *sudo service apache2 restart*

ifconfig: Controla els paràmetres de les interfícies de xarxa. Sense arguments mostra la informació de totes les interfícies

Usos: *ifconfig*

ifconfig interfície

Exemple: *sudo ifconfig (mostra informació de totes les interfícies)*

sudo ifconfig eth0 (mostra informació només de la interfície eth0)

tar: Comprimeix i descomprimeix arxius i directoris

Usos: tar czvf nom_eixida nom_entrada (comprimir en format gzip)

tar xzvf arxiu.tar.gz (descomprimeix un arxiu en format gzip

Exemple: *sudo tar czvf arxiu.tar.gz /arxiu/maig/**

sudo tar xvzf arxiu.tar.gz

Annex II - Instal·lació d'una autoritat certificadora i creació d'un certificat

A continuació es detalla com crear un certificat de CA amb OpenSSL, crear un certificat per a un lloc web i importar el certificat de CA en un navegador per a que aquest confie en els certificats emesos per la nostra CA.

Creació de certificat de CA

Primerament crearem un certificat de CA amb el que signarem els certificats que emetrem amb la nostra CA. Per a fer-ho, hi ha que seguir els següents passos:

- Primerament localitzarem l'script CA.pl. Canviarem al directori on es troba i l'executarem:

  sudo updatedb
  sudo locate CA.pl
  cd /directori/de/CA.pl
  sudo ./CA.pl -newca

```
tiko@WEB01:~$ sudo locate CA.pl
/usr/lib/ssl/misc/CA.pl
/usr/share/man/man1/CA.pl.1ssl.gz
tiko@WEB01:~$ cd /usr/lib/ssl/misc/
tiko@WEB01:/usr/lib/ssl/misc$ sudo ./CA.pl -newca
```

Començarà el procés i s'ens preguntara informació sobre la nostra CA i la nostra empresa en definitiva.

```
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 2048 bit RSA private key
.....................+++
.....................................................................................
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:VLC
Locality Name (eg, city) []:VLC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Local Lab
Organizational Unit Name (eg, section) []:Local
Common Name (e.g. server FQDN or YOUR name) []:Local Lab CA
Email Address []:vmarti@local.lab
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
```

Per últim, si tot va correctament, s'ens mostrarà el contingut del certificat i es crearà un certificat x509 en format pem que podrem trobar a **/usr/lib/ssl/misc/demoCA/cacert.pem**:

```
Certificate Details:
        Serial Number: 11018593919463784949 (0x98e9e8ca6deb01f5)
        Validity
            Not Before: Jun  1 16:57:43 2016 GMT
            Not After : Jun  1 16:57:43 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = VLC
            organizationName          = Local Lab
            organizationalUnitName    = Local
            commonName                = Local Lab CA
            emailAddress              = vmarti@local.lab
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                DC:F5:A6:DC:A4:6A:23:84:CC:19:14:1D:C1:BE:F8:D3:5C:E5:FB:00
            X509v3 Authority Key Identifier:
                keyid:DC:F5:A6:DC:A4:6A:23:84:CC:19:14:1D:C1:BE:F8:D3:5C:E5:FB:00

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Jun  1 16:57:43 2019 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
```

Creació de certificat per a un lloc web

Ara que ja som una entitat certificadora crearem un certificat per al nostre lloc web01.local.lab.

Per a fer-ho primerament generarem una petició de certificat i una clau privada amb la instrucció ***sudo ./CA.pl -newreq*** que es pot trobar al directori **/usr/lib/ssl/misc**

```
tiko@WEB01:/usr/lib/ssl/misc$ sudo ./CA.pl -newreq
Generating a 2048 bit RSA private key
..............................+++
.....................................................................+++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:VLC
Locality Name (eg, city) []:VLC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WEB01
Organizational Unit Name (eg, section) []:WEB01
Common Name (e.g. server FQDN or YOUR name) []:web01.local.lab
Email Address []:vmarti@local.lab

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request is in newreq.pem, private key is in newkey.pem
tiko@WEB01:/usr/lib/ssl/misc$
```

Per últim signarem el certificat amb la instrucció ***sudo ./CA.pl -sign***

```
tiko@WEB01:/usr/lib/ssl/misc$ sudo ./CA.pl -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 11018593919463784950 (0x98e9e8ca6deb01f6)
        Validity
            Not Before: Jun  1 18:00:24 2016 GMT
            Not After : Jun  1 18:00:24 2017 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = VLC
            localityName              = VLC
            organizationName          = WEB01
            organizationalUnitName    = WEB01
            commonName                = web01.local.lab
            emailAddress              = vmarti@local.lab
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                01:C1:95:B0:17:C4:B9:50:80:7A:87:AA:D8:CD:EB:F8:95:74:5A:B4
            X509v3 Authority Key Identifier:
                keyid:DC:F5:A6:DC:A4:6A:23:84:CC:19:14:1D:C1:BE:F8:D3:5C:E5:FB:00

Certificate is to be certified until Jun  1 18:00:24 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Signed certificate is in newcert.pem
```

Ara copiarem el certificat i la clau al directori **/etc/ssl:**

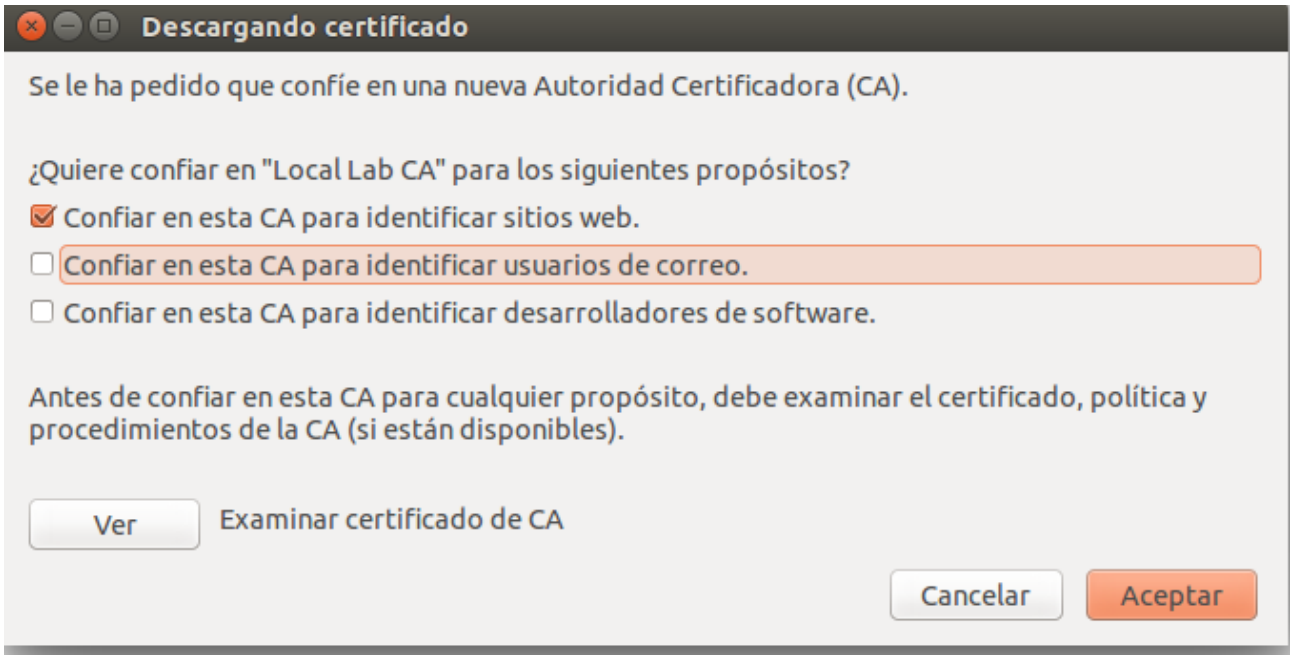
sudo mv newkey.pem /etc/ssl/private/web01.local.lab.key
sudo mv newcert.pem /etc/ssl/certs/web01.local.lab.crt

Per últim modificarem l'arxiu de configuració del lloc per a que utilitze els certificats i reiniciarem Apache:

```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
#SSLCertificateFile     /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateFile      /etc/ssl/certs/web01.local.lab.crt
#SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateKeyFile /etc/ssl/private/web01.local.lab.key
```

Importar el certificat de la CA a Firefox

Per últim, ens farà falta que el navegador web confie en la nostra CA quan el lloc web presente el seu certificat al connectar-se. Per aconseguir-ho copiarem l'arxiu **/usr/lib/ssl/misc/demoCA/cacert.pem** al sistema des d'on volem accedir al lloc web.
En les preferències de Firefox, anirem a la secció «**Avançat»** i en la pestanya certificats farem clic al botó **«Vore certificats»**. A la finestra que es mostrara, farem clic al botó **«Importar»** i tot seguit seleccionarem l'arxiu que acabem de copiar. S'ens mostrarà una finestra on seleccionarem per a que tipus de serveis confiem en la nostra CA.



Fem clic en **«Aceptar»** i ja podrem accedir al nostre lloc web sense cap error.

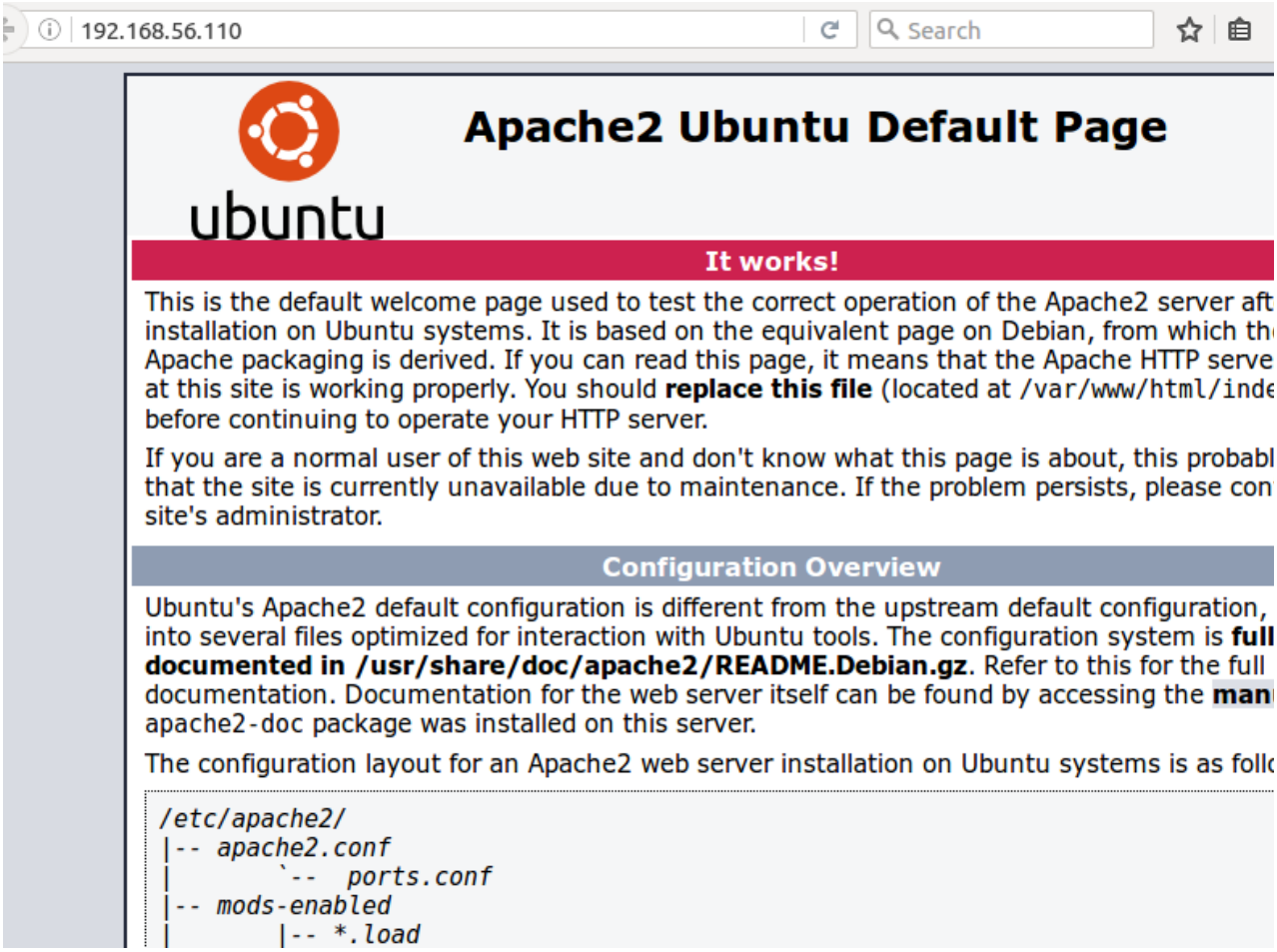
Annex III – Instal·lació d'Apache, MySQL i PHP5 (LAMP) en Ubuntu 14.04

Per a la instal·lació d'Apache utilitzarem apt-get per instal·lar-lo des dels repositoris d'Ubuntu:

sudo apt-get update
sudo apt-get install apache2

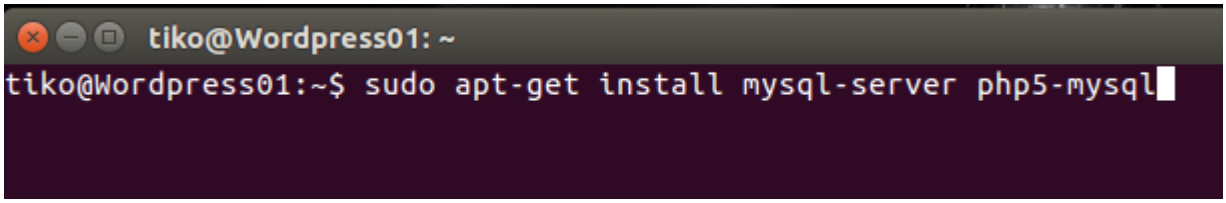
```
S'està llegint la llista de paquets… Fet
tiko@Wordpress01:~$ sudo apt-get install apache2
```

Quan acabe la instal·lació, si volem comprovar que Apache esta instal·lat i funcionant correctament, obrirem un navegador web i anirem a la direcció http://IP_del_Servidor . Si tot s'ha instal·lat correctament, deuríem accedir a la pagina per defecte d'Apache per a Ubuntu.

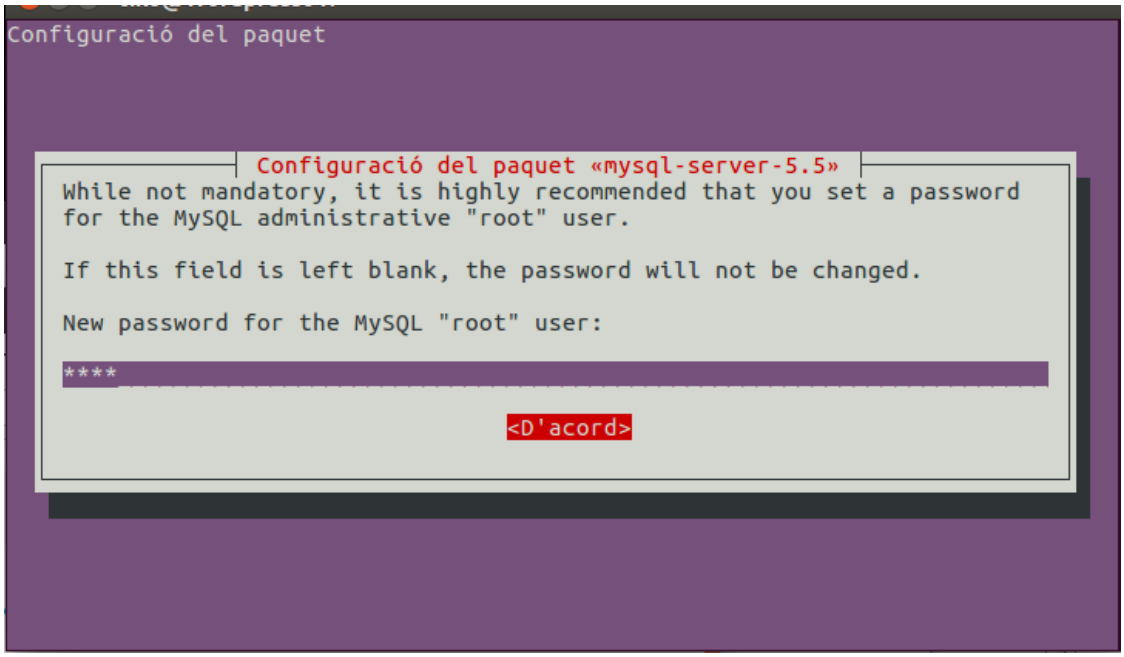


Tot seguit instal·larem MySQL amb soport per a php. Executarem la següent instrucció:

sudo apt-get install mysql-server php5-mysql



En el proces d'instal·lació s'ens preguntara la per la contrasenya de l'usuari root de MySQL.



Quan ja ha acabat la instal·lació crearem la estructura de directoris on s'emmagatzemarà la seua informació executant:

sudo mysql_install_db

```
tiko@Wordpress01:/var/www/html$ sudo mysql_install_db
[sudo] password for tiko:
Installing MySQL system tables...
160526 16:16:54 [Warning] Using unique option prefix key_buffer instead of key_b
uffer_size is deprecated and will be removed in a future release. Please use the
 full name instead.
```

Per últim millorarem un poc la seguretat de la nostra instal·lació de MySQL. Per a aconseguir-ho executarem la instrucció ***sudo mysql_secure_installation***

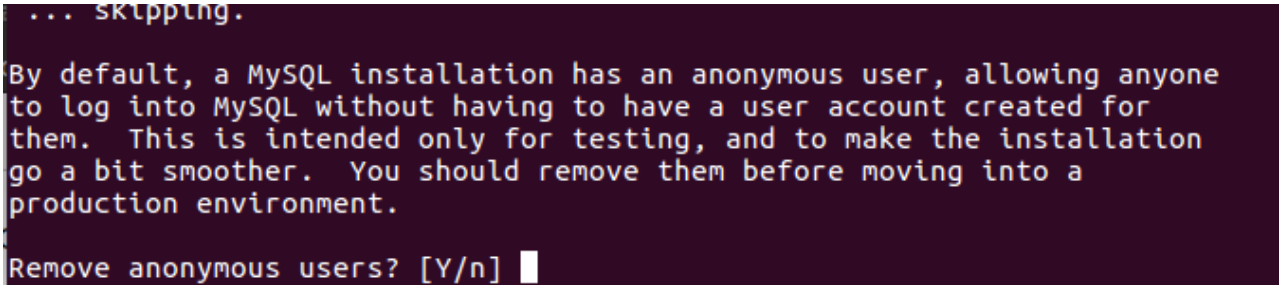
```
tiko@Wordpress01:~$ sudo mysql_secure_installation
```

Després de l'execució s'ens preguntara varies qüestions relatives a la seguretat de la instal·lació. Primerament podrem canviar la contrasenya de l'usuari root de MySQL. Al nostre exemple no serà necessari ja que l'hem establerta en la instal·lació de MySQL

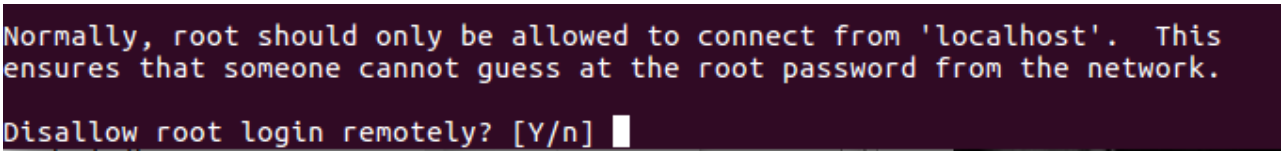
```
tiko@Wordpress01:~$ sudo mysql_secure_installation



NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!


In order to log into MySQL to secure it, we'll need the current
password for the root user.  If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
```

```
Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
```

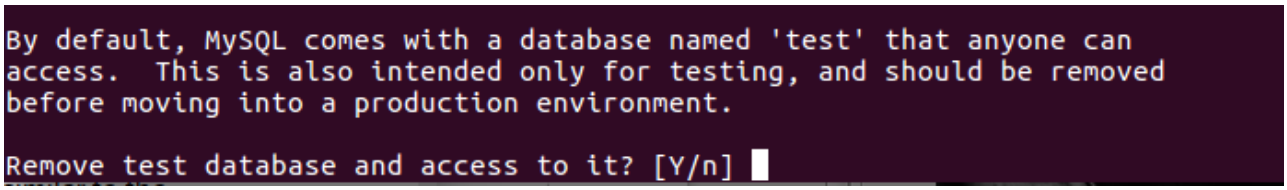
A la pregunta següent eliminarem els usuaris anònims seleccionant la resposta per defecte.



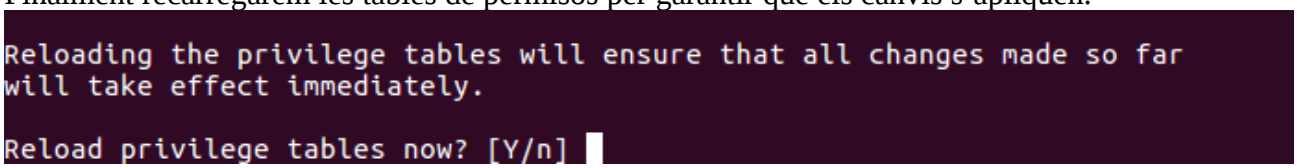
Deshabilitarem la autenticació remota amb l'usuari root.



Eliminarem les bases de dades de prova i els accessos a les mateixes.

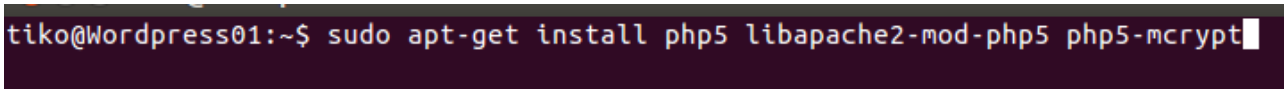


Finalment recarregarem les tables de permisos per garantir que els canvis s'apliquen.



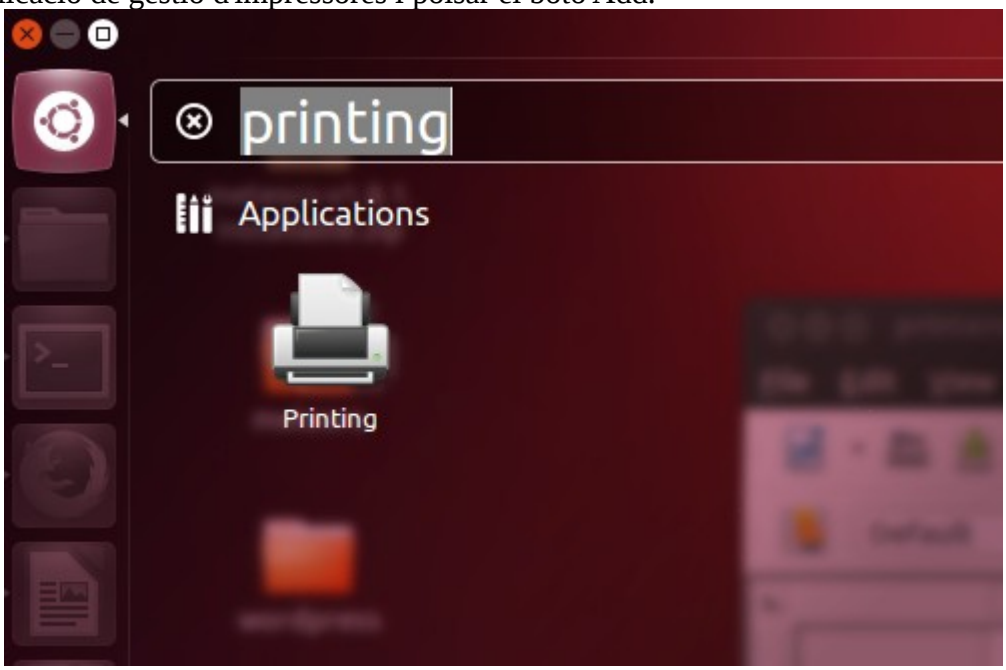
Per últim, instal·lar php5 i el seu modul corresponent d'Apache amb apt-get:

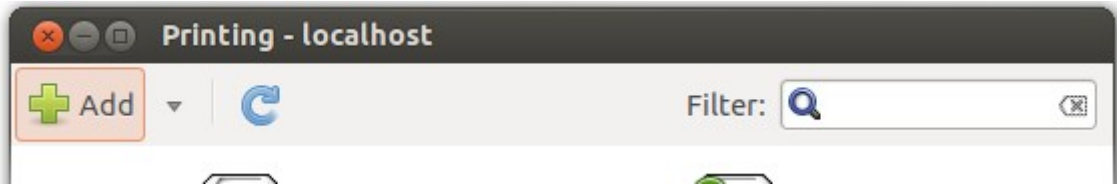
sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt



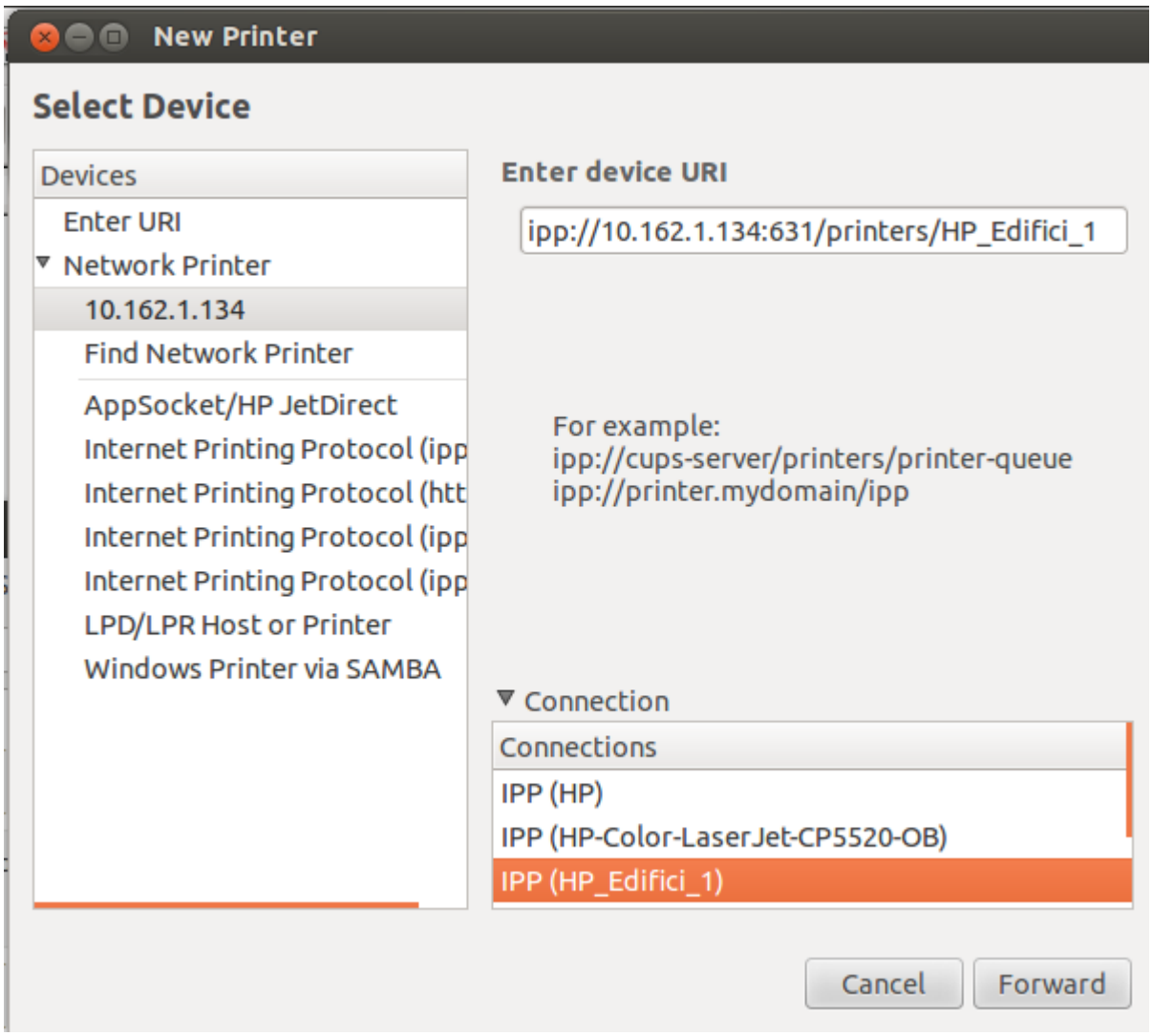
Annex IV – Instal·lació d'impressora compartida

A Ubuntu, pressionar la tecla Alt i escriure Printing (aquest exemple esta fet amb un sistema instal·lat en anglés. Si el sistema esta instal·lat en altre idioma utilitzar la paraula corresponent). Obrir la aplicació de gestió d'impressores i polsar el boto Add.

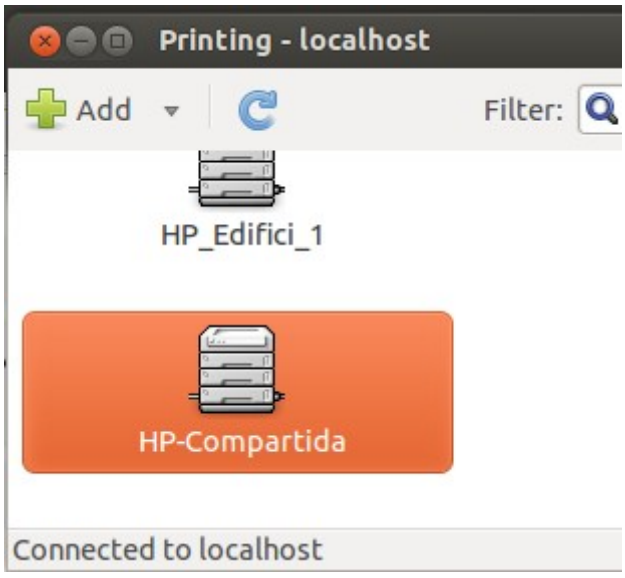




A la finestra que s'obrira seleccionar Network printer → Find network printer. A la caixa de cerca que es troba a la dreta, escriure la direcció o nom del servidor de impressió i polsar Find. A la part de baix es llistaran les connexions de les impressores compartides al servidor. Seleccionar la desitjada.



Fer clic en Forward i la impressora s'afegirà.



Annex V – Instal·lació de Wordpress a Ubuntu 14.04

Primerament es necessari instal·lar la pila LAMP (Linux Apache MySQL i PHP) per poder instal·lar Wordpress correctament. Els detall de la instal·lació d'Apache, MySQL i PHP es poden trobar a l'annex III.

Una vegada ja tenim tant Apache, MySQL com PHP instal·lats correctament passarem a configurar Wordpress. La primera cosa que s'ha de fer es configurar la base de dades MySQL. Per a fer-ho seguirem cal seguir els següents passos:

- Fer login al servidor MySQL des d'una terminal. Utilitzarem l'usuari root i la contrasenya definida en la instal·lació que s'ha fet seguint l'annex II. Executant la següent instrucció s'ens demanara la contrasenya de l'usuari root de MySQL.

  Mysql -u root -p

```
tiko@Wordpress01:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.5.49-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

- Crear la base de dades per a Wordpress executant:

  CREATE DATABASE wordpress;

- Crear l'usuari MySQL al qui donarem accés a la base de dades Wordpress executant les dos instruccions següents:

CREATE USER wordpress@localhost IDENTIFIED BY 'contrasenya'; (substituir contrasenya per la contrasenya que volem utilitzar per a aquest usuari)

GRANT PRIVILEGES ON wordpress.* TO wordpress@localhost; (el primer wordpress correspon al nom de la base de dades que hem creat i el segon al nom del usuari)

- Per últim, executarem la instrucció ***FLUSH PRIVILEGES;*** i eixirem de la línia d'instruccions amb la instrucció ***exit*** .

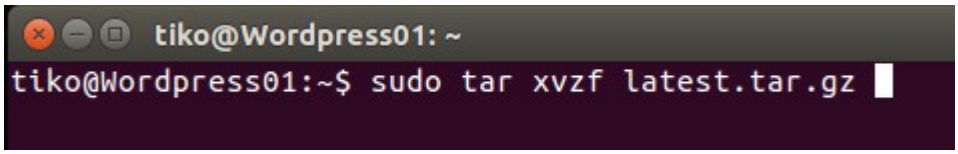
```
mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE USER wordpress@localhost IDENTIFIED BY 'wordpress';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON wordpress.* TO wordpress@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> EXIT
Bye
tiko@Wordpress01:~$
```

Ara que ja tenim MySQL configurat correctament descarregarem l'ultima versió estable de Wordpress amb wget:

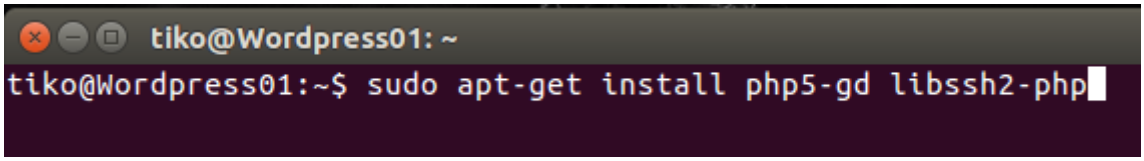
sudo wget http://wordpress.org/latest.tar.gz

```
tiko@Wordpress01: ~
tiko@Wordpress01:~$ sudo wget http://wordpress.org/latest.tar.gz
--2016-05-26 14:19:22--  http://wordpress.org/latest.tar.gz
Resolent wordpress.org (wordpress.org)... 66.155.40.250, 66.155.40.249
S'està connectant a wordpress.org (wordpress.org)|66.155.40.250|:80... conectat.
HTTP: Petició enviada, esperant resposta... 301 Moved Permanently
Localització: https://wordpress.org/latest.tar.gz [el següent]
--2016-05-26 14:19:22--  https://wordpress.org/latest.tar.gz
S'està connectant a wordpress.org (wordpress.org)|66.155.40.250|:443... conectat
.
HTTP: Petició enviada, esperant resposta... 200 OK
Longitud: 7770470 (7,4M) [application/octet-stream]
S'està desant a: «latest.tar.gz»

100%[======================================>] 7.770.470    615KB/s   en 47s

2016-05-26 14:20:10 (160 KB/s) - s'ha desat «latest.tar.gz» [7770470/7770470]

tiko@Wordpress01:~$
```

Descomprimirem l'arxiu amb ***sudo tar xvzf latest.tar.gz***



Per a poder treballar amb imatges, instal·lar plugins i actualitzar parts de Wordpress fent ús d'ssh, serà necessari instal·lar els paquets php5-gd i libssh2-php amb ***sudo apt-get install php5-gd libssh2-php*** :

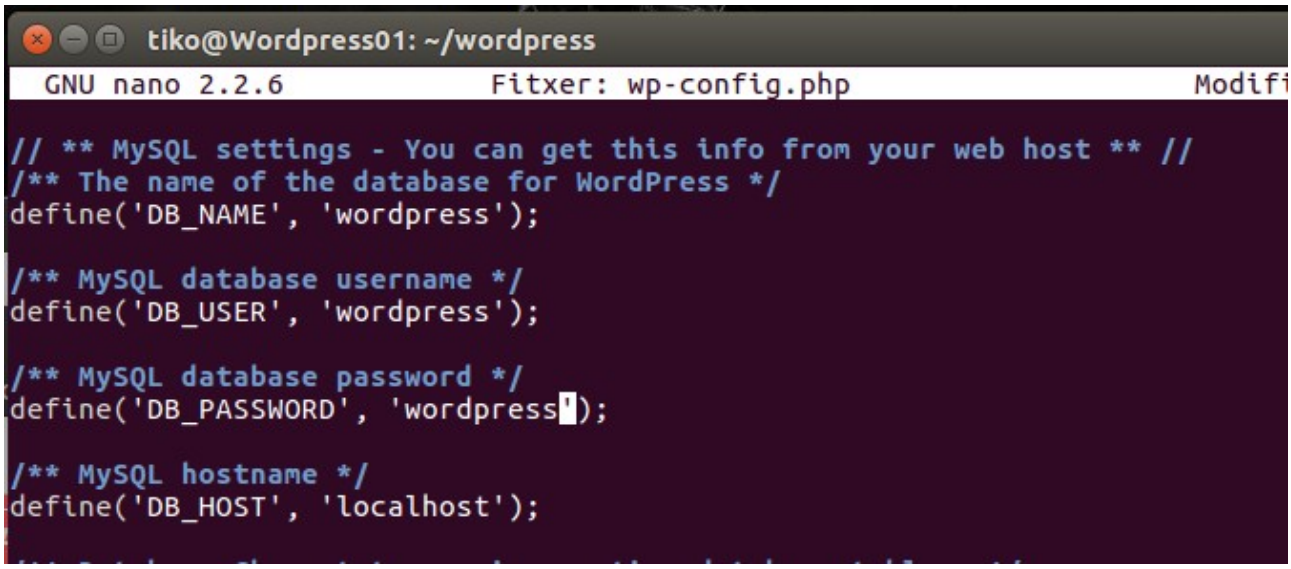


A continuació continuarem configurant l'accés a la base de dades Wordpress:

- Canviar al directori on hem descomprimit Wordpress i copiar l'arxiu wp-config-sample.php a wp-config.php amb la instrucció cp:

  sudo cp wp-config-sample.php wp-config.php

- Editar a wp-config.php el nom de la base de dades(DB_NAME), l'usuari amb accés a la base de dades (DB_USER) , la contrasenya del usuari MySQL amb accés a la base de dades(DB_PASSWORD) i el nom del servidor de base de dades (DB_HOST)

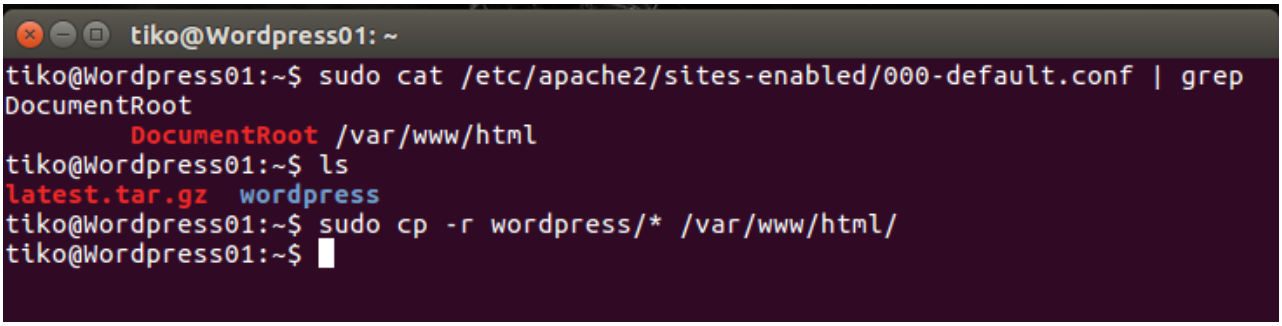


Per a poder accedir directament a Wordpress sense tindre que redireccionar cap carpeta al servidor web, copiarem els arxius que componen Wordpress a l'arrel de documents del nostre servidor web. Al nostre exemple l'arrel de documents utilitzada es la que té Apache per defecte (/var/www/html). En qualsevol cas, executant la següent instrucció podrem comprovar quina es l'arrel de documents del nostre servidor:

sudo cat /etc/apache2/sites-enabled/000-default.conf | grep DocumentRoot

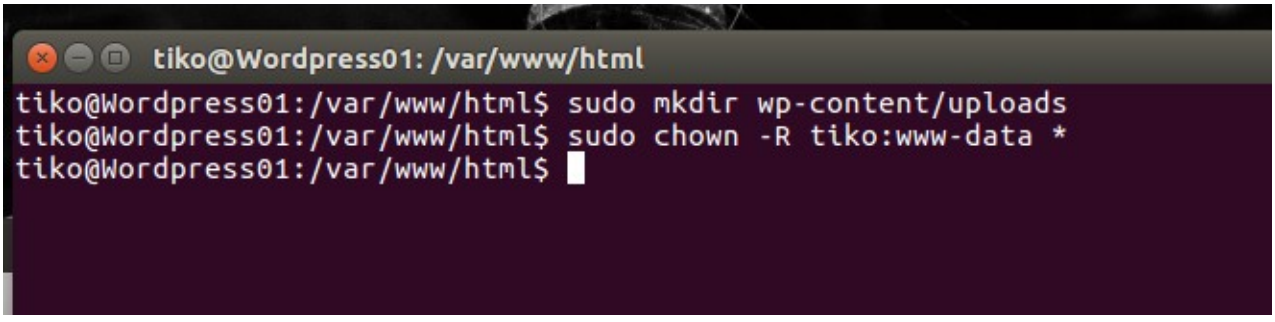
Per a copiar els arxius, canviarem al directori on tenim el directori amb els arxius de Wordpress i executarem:

sudo cp -r wordpress/* /var/www/html/



Tot seguit crearem la carpeta on pujarem els documents i modificarem els permisos de tots els arxius Wordpress per a que el nostre usuari sudoer (al nostre exemple tiko) i el grup www-data que es utilitzat per Apache puguen operar correctament amb tots els components Wordpress. Per a aconseguir-ho executarem:

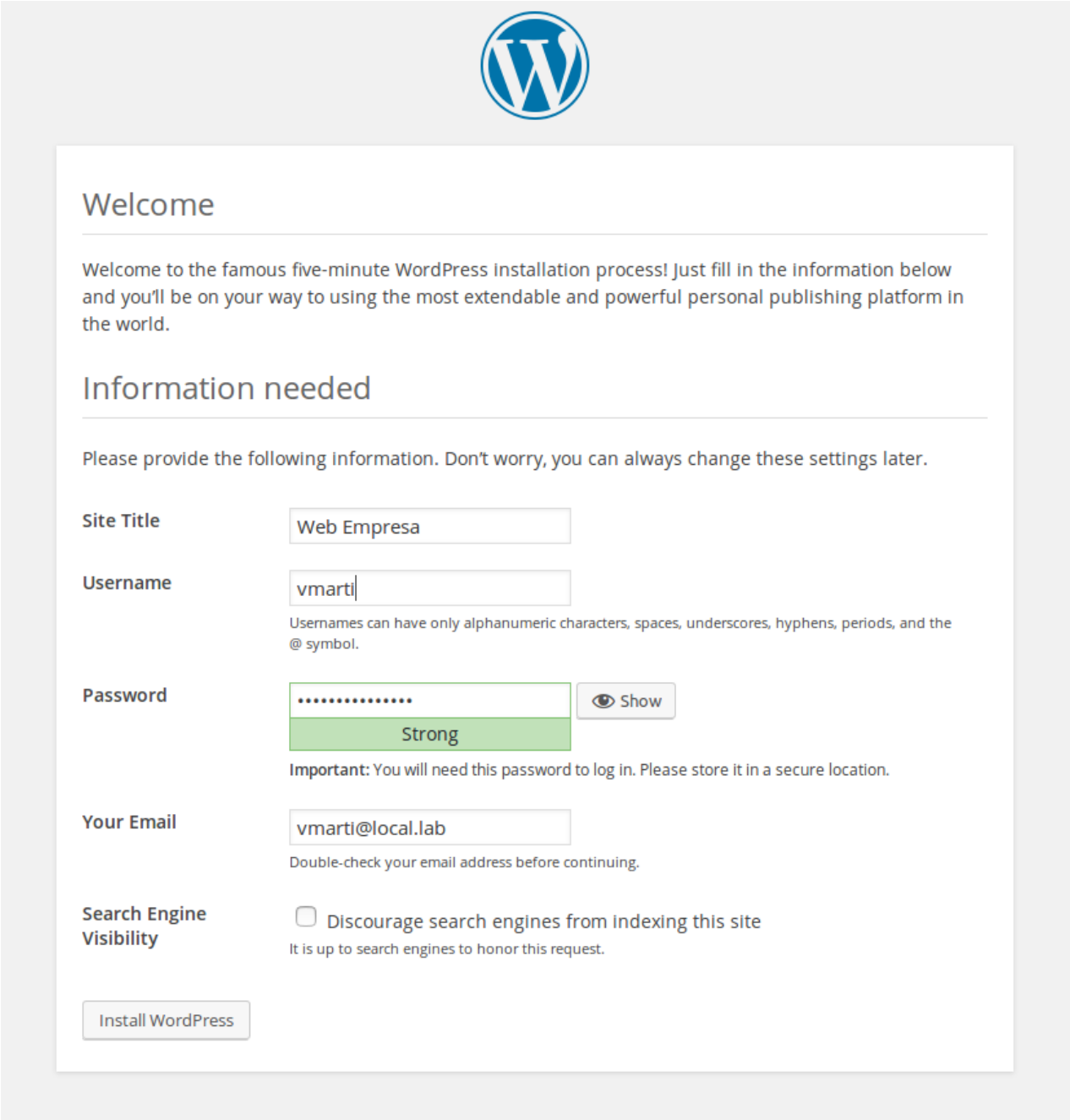
cd /var/www/html
sudo mkdir wp-content/uploads
***sudo chown -R tiko:www-data ** (substituir tiko pel nostre usuari sudoer)



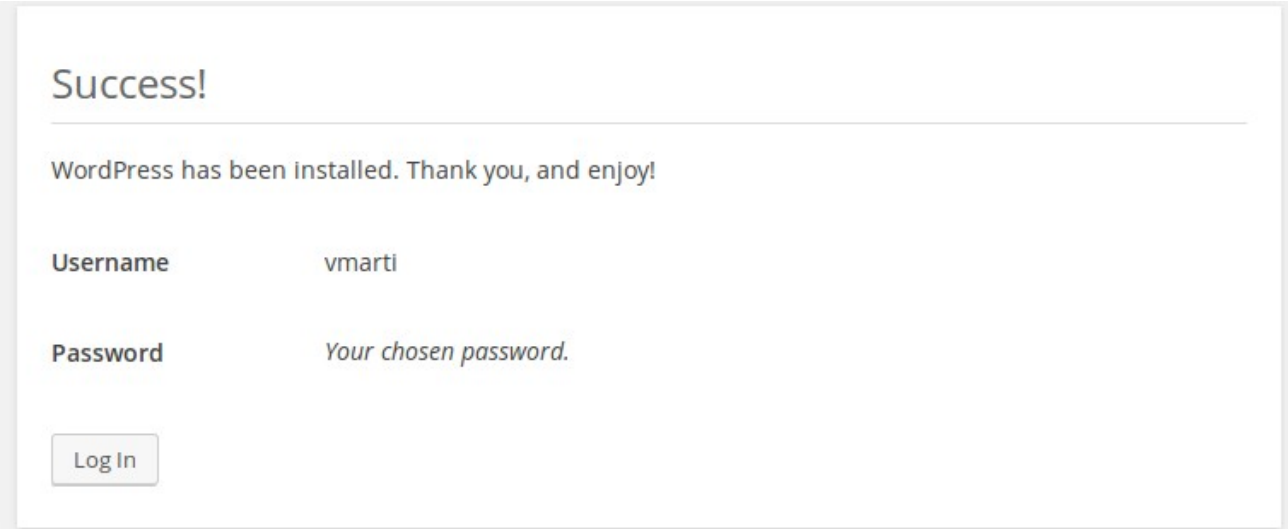
Esborrar l'arxiu per defecte d'Apache index.html del directori arrel de documents /var/www/html

```
tiko@Wordpress01:/var/www/html$ sudo cp index.html index.html.old
tiko@Wordpress01:/var/www/html$ sudo rm index.html
```

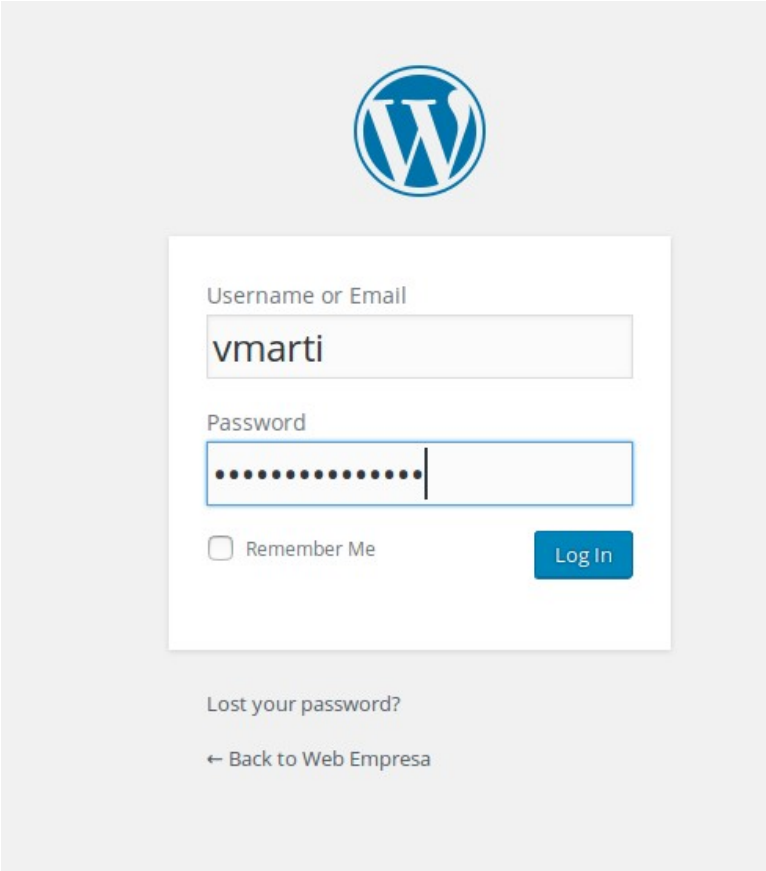
Finalment acabarem la configuració obrint un navegador web i accedint la nostra instal·lació de Wordpress amb la direcció http://IP_del_servidor. S'ens mostrara una ultima pantalla on configurar el nom de la nostra web, l'usuari i la contrasenya del nostre usuari per a accedir al panel d'administració de la pagina aixi com la nostra direcció de correu.



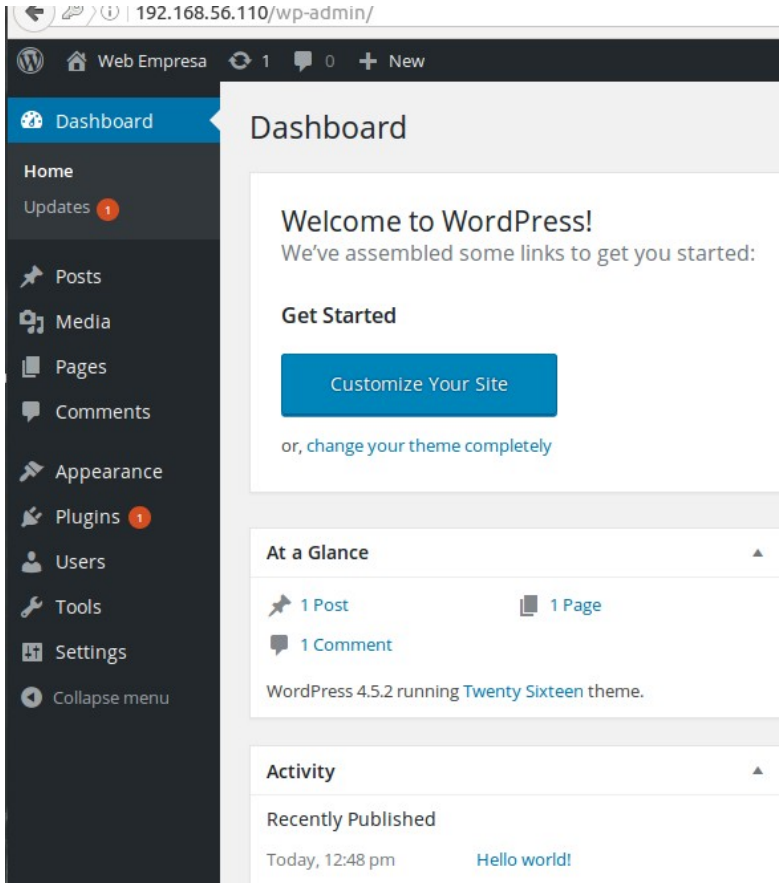
Després d'introduir les dades a la pantalla anterior i fer clic en ***Install Wordpress*** **,** si tot a anat correctament podrem vore la següent pantalla. Farem clic al boto ***Log in***

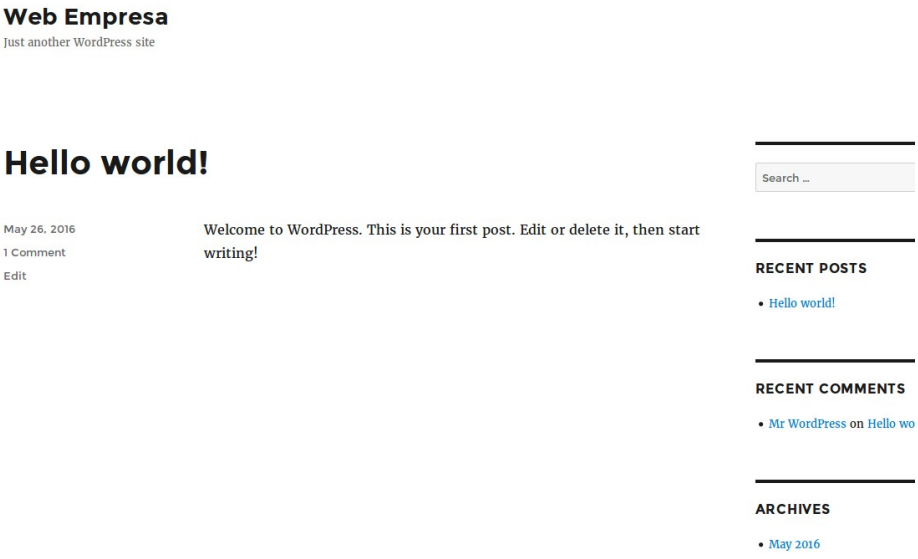


Anirem a la pantalla d'inici de sessió del panel d'administració de la nostra web (http://IP_del_Servidor/wp_admin) . Iniciarem sessió amb l'usuari i contrasenya del pas anterior



La nostra instal·lació de Wordpress ja esta preparada i llesta per a personalitzar-la





Annex VI – Instal·lació de servei de correu electrònic

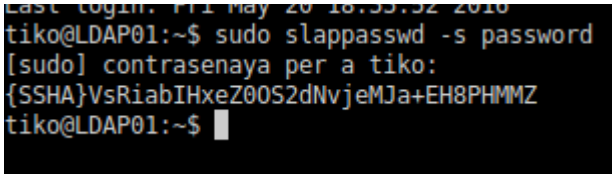
Tota aquesta configuració esta feta sobre màquines amb Ubuntu 14.04 o Ubuntu 16.04.
S'especificarà en cada moment la versió del servidor.

Primerament configurarem correctament el servidor LDAP per a poder crear usuaris amb els atributs necessaris per a poder crear-los amb una bustia de correu.

Configuració LDAP

Aquesta configuració es realitza al servidor LDAP instal·lat a la secció 3 amb Ubuntu 14.04

Per a modificar **cn=config** el qual conté la configuració LDAP un usuari administrador i una contrasenya han de ser creats. En primer lloc generarem la contrasenya amb la instrucció slappasswd executant ***sudo slappasswd -s contrasenya***

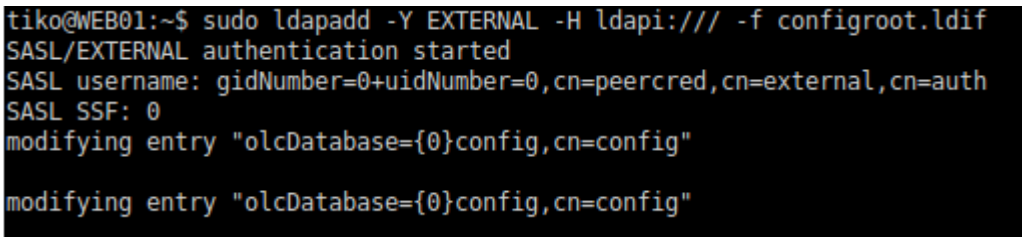


Tot seguit crearem l'arxiu configroot.ldif escriurem el següent modificant el contingut del camp oldRootPW del segon bloc amb l'eixida de la instrucció slappasswd que hem executat anteriorment.:

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootDN
olcRootDN: cn=admin,cn=config

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}Fqu0y5PH52Cpgd/moy0rosyZKsM17psE

A continuació executar la instrucció ***sudo ldapadd -Y EXTERNAL -H ldapi:/// -f configroot.ldif***



El següent pas es afegir l'esquema necessari per a integrar els usuaris LDAP amb el nostre sistema de correu.

Per a fer-ho, seguirem els següents passos:

- Descarregar el nou esquema

  sudo cd /etc/ldap/schema
  sudo wget http://www.postfix-buch.com/download/postfix-book.schema.gz
  sudo gunzip postfix-book.schema.gz

- Convertir l'esquema a format **ldif** per a poder carregar-lo. Farem açò amb la instrucció **slapcat**
  - Crear l'arxiu de configuració

    sudo cd /etc/ldap/schema
    sudo mkdir ldif_output
    sudo touch schema_convert.conf

  - Copiar les següents línies a **schema_convert.conf**

    include /etc/ldap/schema/core.schema
    include /etc/ldap/schema/cosine.schema
    include /etc/ldap/schema/nis.schema
    include /etc/ldap/schema/inetorgperson.schema
    include /etc/ldap/schema/postfix-book.schema

  - Començar la conversió

    sudo slapcat -f schema_convert.conf -F ./ldif_output/ -n0

- Copiar l'arxiu resultant a /etc/ldap/schema des de /etc/ldap/schema/cn=config/cn=schema. Canviar al usuari root amb ***sudo su*** per a copiar l'arxiu:

  sudo su

  cp postfix-book.ldif /etc/ldap/schema

```
root@LDAP01:/etc/ldap/schema/ldif_output/cn=config/cn=schema# pwd
/etc/ldap/schema/ldif_output/cn=config/cn=schema
root@LDAP01:/etc/ldap/schema/ldif_output/cn=config/cn=schema# cp cn\=\{4\}postfix-book.ldif /etc/ldap/schema/postfix-book.ldif
```

- Abans d'importar l'arxiu, fer les següents modificacions:
  - dn=postfix-book,cn=schema,cn=config
  - cn=postfix-book
  - Eliminar tot el que es trobe des de structuralObjectClass fins al final

- Importarem l'arxiu modificar amb la següent:

  sudo ldapadd -Y EXTERNAL -H ldapi:/// -f postfix-book.ldif

```
root@WEB01:/etc/ldap/schema# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f postfix-book.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=postfix-book,cn=schema,cn=config"
```

- Finalment afegirem una ACL al servidor LDAP per a que els usuaris en la ou=serveis puguen llegir l'atribut userPassword. Per a fer-ho, instal·larem l'aplicació Apache Studio a l'ordinador des d'on volem gestionar el servidor LDAP seguint les instruccions següents:
  - Instal·lar Java jre amb apt-get

    sudo apt-get install default-jre

  - Descarregar la versió apropiada per al nostre sistema (32 o 64 bits) des de la pàgina

  https://directory.apache.org/studio/download/download-linux.html.

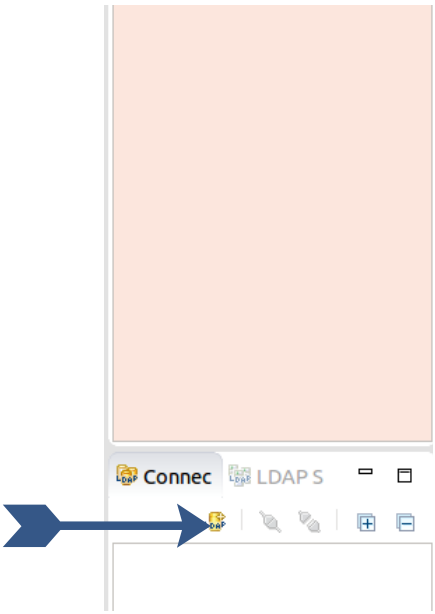
  - Descomprimir el contingut de la descarrega

  sudo tar -xvzf ApacheDirectoryStudio-*.tar.gz -C /home/usuari/ADS

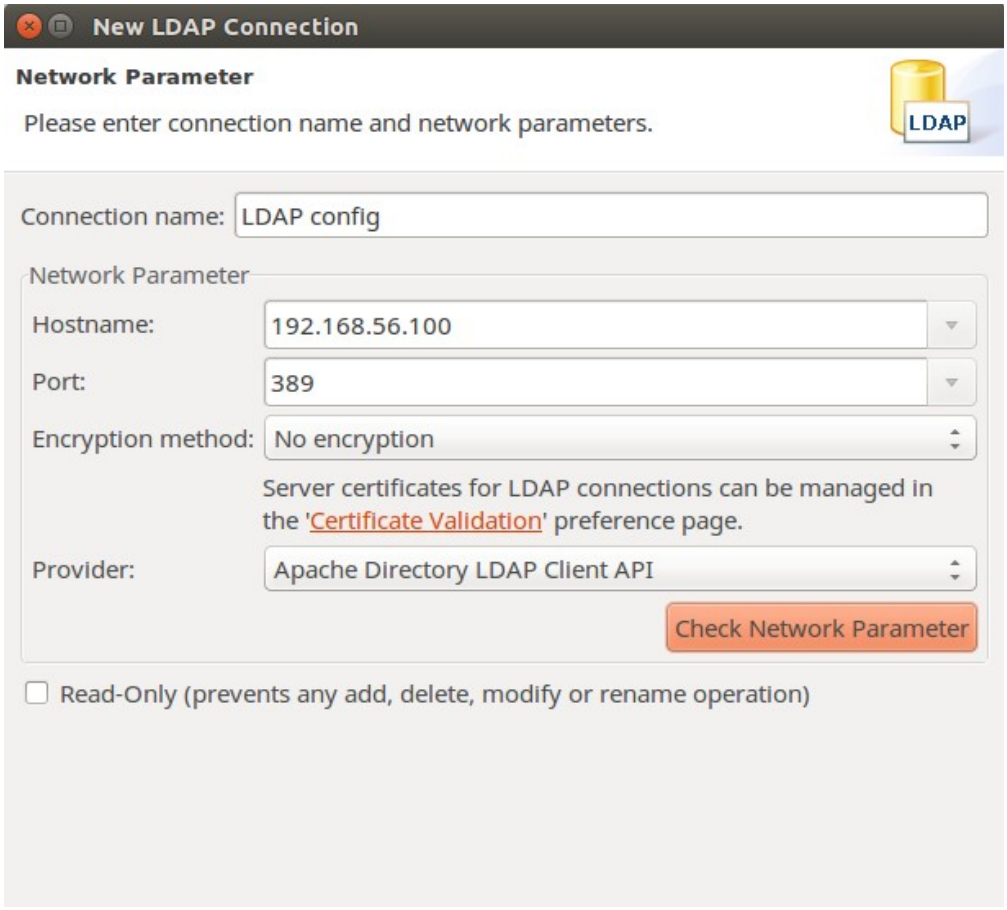
  - Executar ApacheDirectoryStudio

  ./ApacheDirectoryStudio

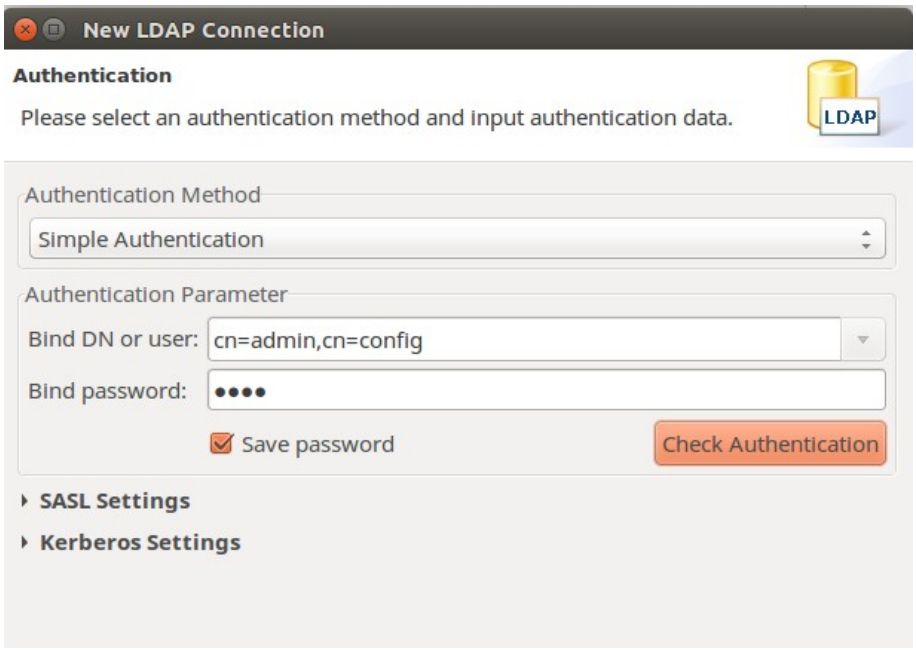
  - Crear una connexió per al arbre **cn=config**. Per obrir l'assistent i crear la connexió polsar la icona senyalada a la imatge que es troba a la secció inferior esquerra.



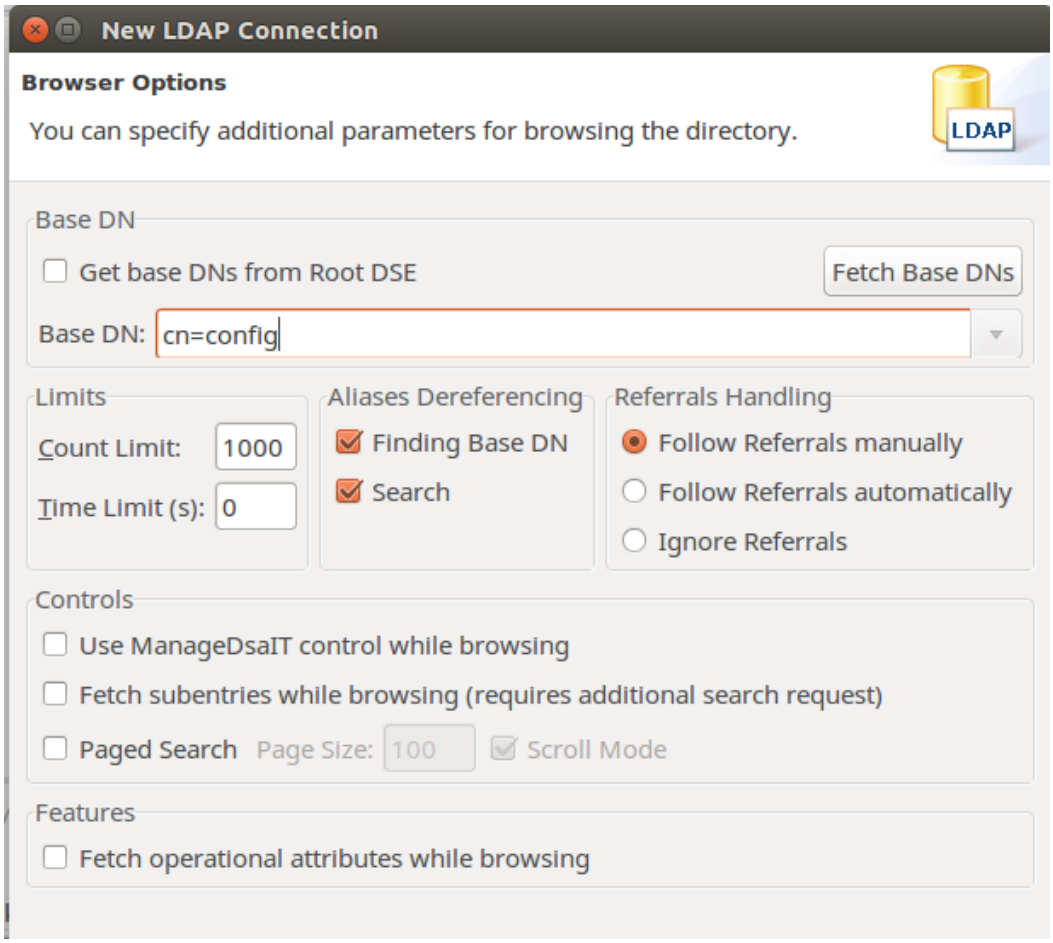
- Plenar els camps del formulari amb la IP del nostre servidor LDAP. Es pot comprovar que la connexió es podrà establir polsant el botó **«Check network parameter».** Polsa **«Next»**



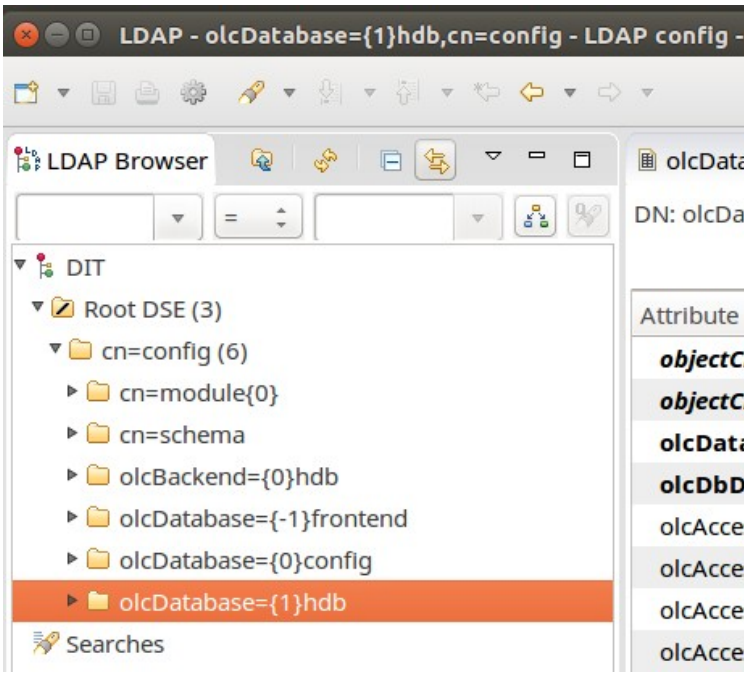
- Omplir els camps Bind DN i Bind password amb l'usuari i contrasenya que hem establert al principi d'aquesta secció amb important l'arxiu **configroot.ldif**



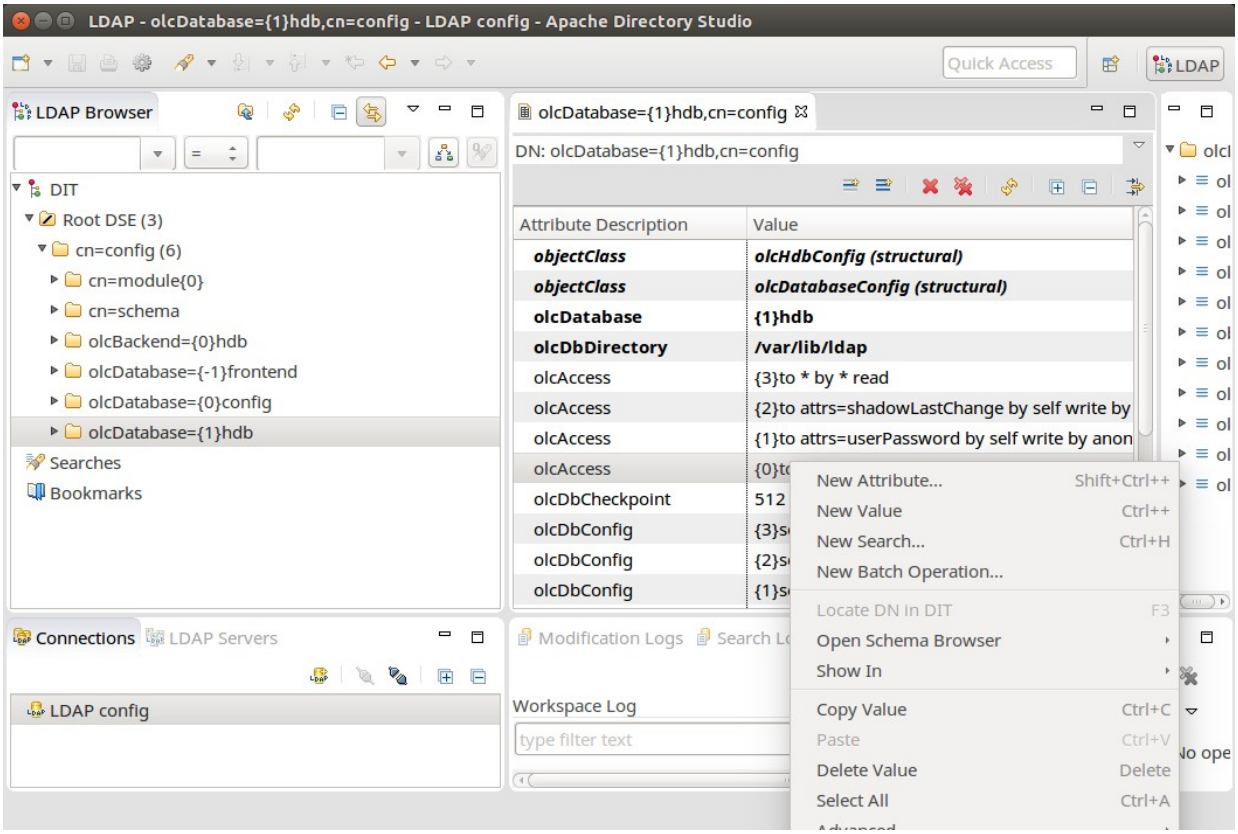
- Com a últim pas per a crear la connexió especificarem el **BASE DN** del arbre **cn=config** manualment desmarcant la casella **«Get BASE DN from Root DSE»**



  - Desplegar l'entrada **olcDatabase={1}hdb**



- Apareixeran 3 entrades amb el nom **olcAccess**. Modificar la entrada que tinga el valor que comença per **{0}** polsant amb el botó dret del ratolí sobre ella i seleccionant al menú contextual **Edit Entry With → Text Editor**



Substituirem el valor de l'entrada per el següent:

{0}to attrs=userPassword by self write by dn.subtree="ou=serveis,dc=local,dc=lab" read by anonymous auth by * none

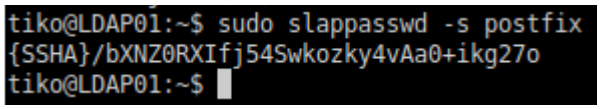
Per últim crearem els objectes LDAP que anem a utilitzar al nostre sistema de correu. En primer lloc crearem les unitats organitzatives per als usuaris que utilitzaran el nostre servei i per als usuaris de serveis que utilitzaran els diferents subsistemes per a comunicar-se amb el servidor LDAP. Per a fer-ho, crearem l'arxiu **ou.ldif** amb el següent contingut:

dn: ou=usuaris,dc=local,dc=lab
changetype: add
objectClass: organizationalUnit
objectClass: top
ou: usuaris

dn: ou=serveis,dc=local,dc=lab
changetype: add
objectClass: organizationalUnit
objectClass: top
ou: serveis

Tot seguit executarem la instrucció **sudo ldapadd -W -D cn=admin,dc=local,dc=lab -f ou.ldif** per a afegir les dos ou al nostre directori LDAP

Ara crearem els usuaris de serveis que ens faran falta, un per a postfix, un per a Dovecot i un altre per a Roundcube. Primerament generarem contrasenyes per a cadascun d'ells per a fer-ho executarem la instrucció ***sudo slappasswd -s «contrasenya»*** per a generar la contrasenya per a cada usuari:



Aquesta instrucció generarà un hash de la contrasenya que especifiquen (al exemple postfix). Quan ja tenim el hash de totes les contrasenyes, crearem l'arxiu **usuaris_serveis.ldif** amb la següent estructura per a cada usuari:

dn: uid=postfix,ou=serveis,dc=local,dc=lab
objectClass: organizationalPerson
objectClass: person
objectClass: top
objectClass: PostfixBookMailAccount
objectClass: extensibleObject
cn: postfix
givenName: postfix
mail: postfix@local.lab
mailEnabled: TRUE
mailGidNumber: 5000
mailHomeDirectory: /srv/vmail/postfix@local.lab
mailQuota: 10240
mailStorageDirectory: maildir:/srv/vmail/postfix@local.lab/Maildir
mailUidNumber: 5000
sn: postfix
uniqueIdentifier: postfix
userPassword: {SSHA}/bXNZ0RXIfj54Swkozky4vAa0+ikg27o

Per a cada usuari modificarem els camps dn, cn, givenName, mail, mailHomeDirectory, mailStorageDirectory i uniqueIdentifier amb el valor que corresponga a cada usuari(canviar postfix per Dovecot per exemple). També canviarem els valor de userPassword per el hash de la contrasenya que hem generat anteriorment per a cada usuari. Separarem cada bloc de valors per a cada usuari amb un salt de línia a l'arxiu **usuaris_serveis.ldif** i executarem la instrucció següent:

sudo ldapadd -W -D cn=admin,dc=local,dc=lab -f usuaris_serveis.ldif

Per últim repetirem aquesta mateixa operació però per als usuaris de correu que emplearem per a il·lustrar el nostre exemple. Canviarem els valors dels camps de l'apartat anterior acorde al nom del usuari, generant un nou hash de la contrasenya de l'usuari i canviant al **dn** la **ou** on volem crear els usuaris, en aquest exemple **ou=usuaris,dc=local,dc=lab**.

A continuació es mostra un exemple d'usuari:

dn: uid=vmarti,ou=usuaris,dc=local,dc=lab
objectClass: organizationalPerson
objectClass: person
objectClass: top
objectClass: PostfixBookMailAccount
objectClass: extensibleObject
cn: Vicente Marti
givenName: Marti
mail: vmarti@local.lab
mailEnabled: TRUE
mailGidNumber: 5000
mailHomeDirectory: /srv/vmail/vmarti@local.lab
mailQuota: 10240
mailStorageDirectory: maildir:/srv/vmail/vmarti@local.lab/Maildir
mailUidNumber: 5000
sn: Vicente
uniqueIdentifier: vmarti
userPassword: {SSHA}/bXNZ0RXIfj54Swkozky4vAa0+ikg27o

Per importar els usuaris tornarem a utilitzar la instrucció ldapadd però amb el nou arxiu:

sudo ldapadd -W -D cn=admin,dc=local,dc=lab -f usuaris_correu.ldif

Ara ja tenim la infraestructura LDAP necessària per a posar en marxa el nostre sistema de correu.

Instal·lació i configuració de Postfix

- Començarem instal·lant els paquets necessaris amb apt-get :

  sudo apt-get install postfix postfix-pcre postfix-ldap

- Canviar la configuració de l'arxiu /etc/postfix/main.cf. A continuació es pot trobar l'arxiu main.cf de la instal·lació feta a aquest estudi:

##
Base Settings
#####################

 # Listen on all interfaces
inet_interfaces = all

 # Use TCP IPv4
inet_protocols = ipv4

 # Greet connecting clients with this banner

```
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)

# Fully-qualified hostname
myhostname = mail01.local.lab

# Do not append domain part to incomplete addresses (this is the MUA's job)
append_dot_mydomain = no

# Trusted networks/hosts (these are allowed to relay without authentication)
mynetworks =
   # Local
   127.0.0.0/8
   # External
   192.168.1.20/32


##########################################################################################
####################
### Local Transport ###
#########################

# Disable local transport (so that system accounts can't receive mail)
local_transport = error:Local Transport Disabled

# Don't use local alias maps
alias_maps =

# Local domain (could be omitted, since it is automatically derived from $myhostname)
mydomain = local

# Mails for these domains will be transported locally
mydestination =
   $myhostname
   localhost.$mydomain
   localhost
##########################################################################################
####################
### Virtual Transport ###
############################

# Deliver mail for virtual recipients to Dovecot
virtual_transport = dovecot

# Process one mail at one time
dovecot_destination_recipient_limit = 1

# Valid virtual domains
virtual_mailbox_domains = hash:/etc/postfix/virtual_domains
```

```
# Valid virtual recipients
virtual_mailbox_maps = proxy:ldap:/etc/postfix/ldap_virtual_recipients.cf

# Virtual aliases
virtual_alias_maps = proxy:ldap:/etc/postfix/ldap_virtual_aliases.cf

##############################################################################
####################
### ESMTP Settings ###
######################

 ### SASL ###

# Enable SASL (required for SMTP authentication)
smtpd_sasl_auth_enable = yes

# Enable SASL for Outlook-Clients as well
broken_sasl_auth_clients = yes

### TLS ###

# Enable TLS (required to encrypt the plaintext SASL authentication)
smtpd_tls_security_level = may

# Only offer SASL in a TLS session
smtpd_tls_auth_only = no

# Certification Authority
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem


# Public Certificate
smtpd_tls_cert_file = /etc/ssl/certs/mail01.local.lab.crt

# Private Key (without passphrase)
smtpd_tls_key_file = /etc/ssl/private/mail01.local.lab.key

# Randomizer for key creation
tls_random_source = dev:/dev/urandom

# TLS related logging (set to 2 for debugging)
smtpd_tls_loglevel = 1

# Avoid Denial-Of-Service-Attacks
smtpd_client_new_tls_session_rate_limit = 10

# Activate TLS Session Cache
smtpd_tls_session_cache_database = btree:/etc/postfix/smtpd_session_cache
```

```
# Deny some TLS-Ciphers
smtpd_tls_exclude_ciphers =
        EXP
        EDH-RSA-DES-CBC-SHA
        ADH-DES-CBC-SHA
        DES-CBC-SHA
        SEED-SHA

# Diffie-Hellman Parameters for Perfect Forward Secrecy
# Can be created with:
# openssl dhparam -2 -out dh_512.pem 512
# openssl dhparam -2 -out dh_1024.pem 1024
smtpd_tls_dh512_param_file = ${config_directory}/certs/dh_512.pem
smtpd_tls_dh1024_param_file = ${config_directory}/certs/dh_1024.pem


##########################################################################################
####################
### Connection Policies ###
############################

# Reject Early Talkers
postscreen_greet_action = enforce


##########################################################################################
####################
### Session Policies ###
########################

# Recipient Restrictions (RCPT TO related)
smtpd_recipient_restrictions =
        reject_non_fqdn_recipient
        reject_unknown_recipient_domain
        # Allow relaying for SASL authenticated clients and trusted hosts/networks
        # This can be put to smtpd_relay_restrictions in Postfix 2.10 and later
        permit_sasl_authenticated
        permit_mynetworks
        # If not authenticated or on mynetworks, reject mailing to external addresses
        reject_unauth_destination
        # Reject the following hosts
        check_sender_ns_access cidr:/etc/postfix/drop.cidr
        check_sender_mx_access cidr:/etc/postfix/drop.cidr
        # Additional blacklist
        reject_rbl_client ix.dnsbl.manitu.net
        # Finally permit (relaying still requires SASL auth)
        # WARNING: Due to this permit, everyone will be able to send emails to internal addresses
without authentication. If this is set to reject though, the server does not receive ema$
```

permit

 # Reject the request if the sender is the null address and there are multiple recipients
smtpd_data_restrictions = reject_multi_recipient_bounce

 # Sender Restrictions
smtpd_sender_restrictions =
reject_non_fqdn_sender
reject_unknown_sender_domain
 # HELO/EHLO Restrictions
smtpd_helo_restrictions =
permit_mynetworks
check_helo_access pcre:/etc/postfix/identitycheck.pcre
#reject_non_fqdn_helo_hostname
reject_invalid_hostname

 # Deny VRFY recipient checks
disable_vrfy_command = yes

 # Require HELO
smtpd_helo_required = yes

 # Reject instantly if a restriction applies (do not wait until RCPT TO)
smtpd_delay_reject = no

 # Client Restrictions (IP Blacklist)
smtpd_client_restrictions = check_client_access cidr:/etc/postfix/drop.cidr
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s

- Modificar (o crear) l'arxiu **/etc/postfix/virtual_domains**

 # Domain Anything

local.lab OK

- Modificar (o crear) l'arxiu **/etc/postfix/ldap_virtual_recipients.cf**

bind = yes
bind_dn = uid=postfix,ou=services,dc=local,dc=lab
bind_pw = postfix
server_host = ldap://192.168.1.20:389
search_base = dc=local,dc=lab
domain = local.lab
query_filter = (&(mail=%s)(mailEnabled=TRUE))
#query_filter = (&(mail=%s))

result_attribute = mail

- Modificar (o crear) **/etc/postfix/ldap_virtual_aliases.cf**

bind = yes
bind_dn = uid=postfix,ou=services,dc=local,dc=lab
bind_pw = postfix
server_host = ldap://192.168.1.20:389
search_base = ou=usuaris,dc=local,dc=lab
domain = local.lab
query_filter = (&(mailAlias=%s)(mailEnabled=TRUE))
result_attribute = mail, email

- Crear l'arxiu /etc/postfix/identitycheck.pcre

 # Identity (RegEx) Action

/^(mail\.local\.lab)$/ REJECT Hostname Abuse: $1

/^(1\.2\.3\.4)$/ REJECT Hostname Abuse: $1

/^(\[1\.2\.3\.4\])$/ REJECT Hostname Abuse: $1

- Crear l'arxiu **/etc/postfix/drop.cidr**

 # IP/CIDR Action

1.2.3.0/24 REJECT BlacklistedX

Quan ja hem modificat tots els arxius esmentats manca convertir en format .db l'arxiu **virtual_domains** per a que Postfix el puga llegir atés que en **main.cf** es cridat com un mapa hash i es per això que es té que convertir. Per a fer-ho executarem la següent instrucció:

postmap hash:/etc/postfix/virtual_domains

Per últim arrancarem el servei executant ***sudo service postfix start***

Instal·lació de Dovecot

En primer lloc,instal·larem els paquets necessaris amb apt-get:

sudo apt-get install dovecot-core dovecot-imapd dovecot-pop3d dovecot-lmtpd dovecot-ldap

A continuació podem deshabilitar els protocols imaps i pop3s en cas de no utilitzar-lo. Al nostre exemple només deshabilitarem pop3s. Així mateix establirem els permisos el usuari i el grup per la authentication-userdb. Per a fer-ho editarem l'arxiu **/etc/dovecot/conf.d/10-master.conf** i buscarem les seccions on apareix inet_listener pop3s i unix_listener auth-userdb per a deixar-les com es mostra a continuació:

```
inet_listener pop3s {
   port = 0
   #port = 995
   #ssl = yes
}

unix_listener auth-userdb {
   mode = 0600
   user = vmail
   group = vmail
}
```

Tot seguit habilitarem els mecanismes d'autenticació que volem i deshabilitarem la autenticació basada en el sistema i habilitarem la autenticació LDAP. Tot açò s'aconsegueix editant l'arxiu **/etc/dovecot/conf.d/10-auth.conf** com es mostra a continuació:

```
auth_mechanisms = plain login
#!include auth-system.conf.ext
!include auth-ldap.conf.ext
```

Per a establir els paràmetres que tenen a vore en l'autenticació LDAP modificarem l'arxiu **/etc/dovecot/dovecot-ldap.conf.ext**:

```
hosts = IP_Servidor_LDAP
dn = uid=dovecot,ou=serveis,dc=local,dc=lab
dnpass = dovecot
ldap_version = 3
base = ou=usuaris,dc=local,dc=lab
user_attrs =
mailHomeDirectory=home,mailUidNumber=uid,mailGidNumber=gid,mailStorageDirectory=
mail
user_filter = (&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=%n))
pass_attrs = uniqueIdentifier=user,userPassword=password
pass_filter = (&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=%n))
default_pass_scheme = CRYPT
```

Per activar el registre en Dovecot editarem l'arxiu **/etc/dovecot/conf.d/10-logging.conf** i modificarem o afegirem les següents línies:

log_path = syslog
syslog_facility = mail
auth_debug = yes

Finalment mancaria establir la ruta dels certificats a emprar per dovecot i crear un usuari i grup de sistema amb el nom vmail (tal i com hem establert a l'arxiu **etc/dovecot/conf.d/10-master.conf.**

Abans d'establir la ruta on estan els certificats, primer hem de crear-los:

- Editar l'arxiu /usr/share/dovecot/dovecot-openssl.cnf i modificar els paràmetres tal i com es mostra a la imatge:

```
  GNU nano 2.5.3

#
# SSLeay configuration file for Dovecot.
#

RANDFILE               = /dev/urandom

[ req ]
default_bits           = 2048
default_keyfile        = privkey.pem
distinguished_name     = req_distinguished_name
prompt                 = no
policy                 = policy_anything
req_extensions         = v3_req
x509_extensions        = v3_req

[ req_distinguished_name ]
organizationName = Dovecot mail server
organizationalUnitName = local
commonName = mail01.local.lab
emailAddress = postmaster@local.lab

[ v3_req ]
basicConstraints       = CA:FALSE
```

- Executar mkcert.sh
  cd /usr/share/dovecot/
  sudo sh mkcert.sh

```
tiko@MAIL01:/usr/share/dovecot$ sudo sh mkcert.sh
Generating a 2048 bit RSA private key
...................+++
..........+++
writing new private key to '/etc/dovecot/private/dovecot.pem'
-----

subject= /O=Dovecot mail server/OU=local/CN=mail01.local.lab/emailAddress=postmaster@local.lab
SHA1 Fingerprint=9B:4C:8B:98:A2:89:F2:8D:57:3D:FF:BF:CC:34:AA:B7:F7:24:F6:6E
```

Per establir la ruta dels certificats editar l'arxiu ***/etc/dovecot/conf.d/10-ssl.conf:***

ssl_cert = </etc/dovecot/dovecot.pem

ssl_key = </etc/dovecot/private/dovecot.pem

Per a crear el usuari i el grup vmail executar les següents instruccions. És important assegurar-se que el directori /srv/vmail es crea:

addgroup --system --gid 5000 vmail

adduser --system --home /srv/vmail --uid 5000 --gid 5000 --disabled-password --disabled-login vmail

Per a arrancar Dovecot executar ***sudo service dovecot start***

Instal·lació i configuració de SASL

La instal·lació de SASL la farem mitjançant apt-get:

sudo apt-get install libsasl2-2 sasl2-bin

Tot seguit passem a configurar SASL. En primer lloc crearem l'arxiu /etc/postfix/sasl/smtpd.conf i l'editarem afegint les següents línies:

log_level: 3
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN

Modificar l'arxiu **/etc/default/saslauthd** amb aquests valors:

START=yes
MECHANISMS="ldap"
OPTIONS="-c -m /var/run/saslauthd"

Crear la configuració LDAP per a SASL en l'arxiu **/etc/saslauthd.conf**:

ldap_servers: ldap://IP_SERVIDOR_LDAP/
ldap_bind_dn: uid=dovecot,ou=serveis,dc=local,dc=lab
ldap_bind_pw: dovecot
ldap_timeout: 10
ldap_time_limit: 10
ldap_scope: sub
ldap_search_base: ou=usuaris,dc=local,dc=lab
ldap_auth_method: bind
ldap_filter: (&(uniqueIdentifier=%u)(mailEnabled=TRUE))
ldap_debug: 0
ldap_verbose: off
ldap_ssl: no
ldap_starttls: no
ldap_referrals: yes

Establir permisos en l'arxiu de configuració , afegir l'usuari sasl al grup postfix:

sudo chown root:sasl /etc/saslauthd.conf
sudo chmod 640 /etc/saslauthd.conf
sudo adduser postfix sasl

Crear un enllaç simbòlic per a que postfix puga comunicar amb sasl

rm -r /var/run/saslauthd/
mkdir -p /var/spool/postfix/var/run/saslauthd
ln -s /var/spool/postfix/var/run/saslauthd /var/run
chgrp sasl /var/spool/postfix/var/run/saslauth

Per últim arrancar sasl:

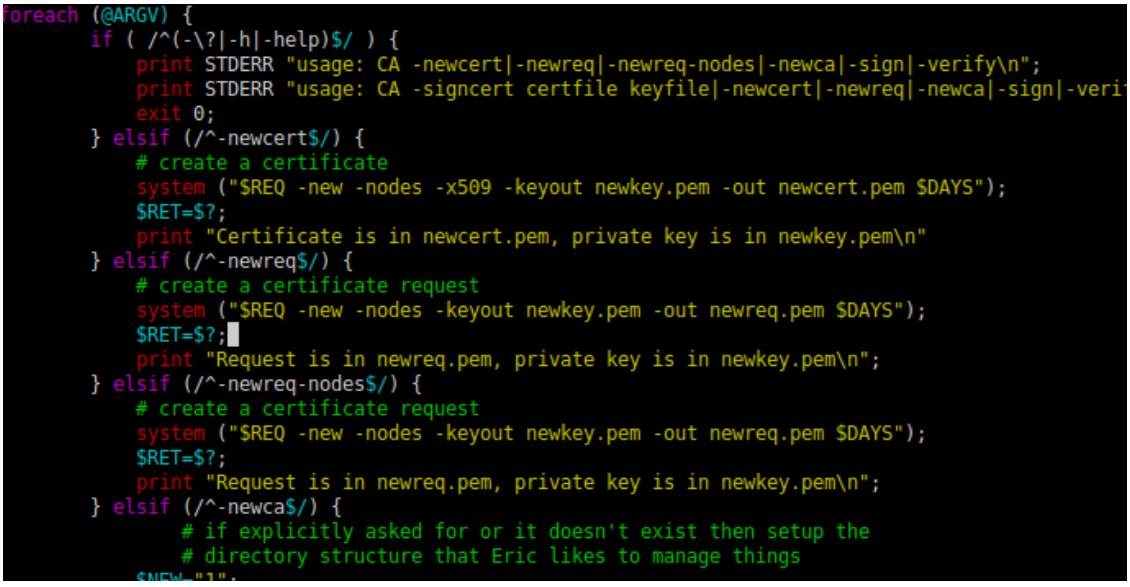
sudo service saslauthd start

Configurar TLS

Tot i que SASL ens proporciona un nivell més de seguretat, fins ara no hem habilitat cap mecanisme d'encriptació per a que la nostra informació viatge segura. Aquesta seguretat la aconseguim amb TLS. Per configurar TLS per a postfix editarem en primer lloc l'arxiu **/usr/lib/ssl/openssl.cnf** per no escriure la mateixa informació varies vegades. Buscarem els paràmetres que es mostren al següent exemple i els modificarem amb els valors que s'adapten a la nostra infraestructura.

countryName_default = ES
0.organizationName_default = local
organizationalUnitName_default = Mailserver
commonName_default = mail.local.lab
emailAddress_default = postmaster@local.lab

Per a crear els nostres certificats, primerament modificarem l'script **CA.pl** localitzat a **/usr/lib/ssl/misc .** Buscar les linies on apareix **$REQ** a afegir la opció -nodes tal i com es mostra a l'imatge:



Tot seguit generarem els certificats necessaris executant les següents instruccions:

- Crear el certificat de CA

  sudo ./CA.pl -newca

```
Certificate Details:
        Serial Number: 17979962948941927468 (0xf985a90a465e542c)
        Validity
            Not Before: May 31 19:02:55 2016 GMT
            Not After : May 31 19:02:55 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = VLC
            organizationName          = Local
            organizationalUnitName    = Mailserver
            commonName                = mail01.local.lab
            emailAddress              = postmaster@local.lab
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                14:53:BF:F8:AA:5A:7D:E4:9C:0E:3F:9A:12:EF:31:2D:2D:EA:34:E7
            X509v3 Authority Key Identifier:
                keyid:14:53:BF:F8:AA:5A:7D:E4:9C:0E:3F:9A:12:EF:31:2D:2D:EA:34:E7

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until May 31 19:02:55 2019 GMT (1095 days)

Write out database with 1 new entries
```

- Crear el certificat de servidor i signar-lo

  sudo ./CA.pl -newreq

```
tiko@MAIL01:/usr/lib/ssl/misc$ sudo ./CA.pl -newreq
Generating a 2048 bit RSA private key
.......................+++
.....................................................................................+++
writing new private key to 'newkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [Some-State]:VLC
Locality Name (eg, city) []:VLC
Organization Name (eg, company) [Local]:
Organizational Unit Name (eg, section) [Mailserver]:
Common Name (e.g. server FQDN or YOUR name) [mail01.local.lab]:
Email Address [postmaster@local.lab]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request is in newreq.pem, private key is in newkey.pem
tiko@MAIL01:/usr/lib/ssl/misc$
```

sudo ./CA.pl -sign

```
tiko@MAIL01:/usr/lib/ssl/misc$ sudo ./CA.pl -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 17979962948941927469 (0xf985a90a465e542d)
        Validity
            Not Before: May 31 19:06:48 2016 GMT
            Not After : May 31 19:06:48 2017 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = VLC
            localityName              = VLC
            organizationName          = Local
            organizationalUnitName    = Mailserver
            commonName                = mail01.local.lab
            emailAddress              = postmaster@local.lab
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                A6:1E:29:91:3E:1B:09:16:C0:5B:AB:58:1B:D2:61:3F:D2:D3:8E:90
            X509v3 Authority Key Identifier:
                keyid:14:53:BF:F8:AA:5A:7D:E4:9C:0E:3F:9A:12:EF:31:2D:2D:EA:34:E7

Certificate is to be certified until May 31 19:06:48 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Signed certificate is in newcert.pem
tiko@MAIL01:/usr/lib/ssl/misc$
```

Copiar tots els certificats generats al directori /etc/postfix

sudo cp newcert.pem /etc/postfix/
sudo cp newkey.pem /etc/postfix/
sudo cp newreq.pem /etc/postfix/
sudo cp demoCA/cacert.pem /etc/postfix/

Editar l'arxiu **/etc/postfix/main.cf** i modificar els següents paràmetres:

smtpd_use_tls = yes
#smtpd_tls_auth_only = yes
smtpd_tls_key_file = /etc/postfix/newkey.pem
smtpd_tls_cert_file = /etc/postfix/newcert.pem
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_loglevel = 3
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

Per últim reiniciarem Postfix amb la instrucció ***sudo service postfix restart*** i comprovarem que TLS esta habilitat seguint les següents instruccions:

telnet mail01.local.lab 25
EHLO client.local.lab
STARTTLS

```
tiko@MAIL01:/usr/lib/ssl/misc$ telnet mail01.local.lab 25
Trying 192.168.1.90...
Connected to MAIL01.local.lab.
Escape character is '^]'.
220 mail01.local.lab ESMTP Postfix (Ubuntu)
EHLO client.local
250-mail01.local.lab
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
STARTTLS
220 2.0.0 Ready to start TLS
```

Instal·lació de clamav i spamassassin amb amavis

Part important del sistema de correu electrònic és el seu filtre de contingut. És per això que instalarem amavis, el qual utilitza spamassassin com antispam i clamav com antivirus.

- Primerament instalarem tots els paquets necessaris per que amavis funcione correctament:

sudo apt install amavisd-new spamassassin clamav-daemon
sudo apt install opendkim postfix-policyd-spf-python

També instal·larem alguns paquets que ajudaran spamassassin a detectar més spam i algunes aplicacions de compressió que serviran per analitzar els arxius adjunts:

sudo apt install pyzor razor
sudo apt install arj cabextract cpio lhasa nomarch pax rar unrar unzip zip

Per una configuració bàsica les opcions per defecte de clamav s'adequaran perfectament a les nostres necessitats. Tot i això, afegirem l'usuari d'amavis al grup de clamav i l'usuari amavis al grup clamav per a que no tindre problemes de permisos:

sudo adduser clamav amavis
sudo adduser amavis clamav

Canviarem el valor **ENABLED** de 0 a 1 a l'arxiu **/etc/default/spamassassin.**

```
# If you're using systemd (default for jessie), the ENABLED setting is
# not used. Instead, enable spamd by issuing:
# systemctl enable spamassassin.service
# Change to "1" to enable spamd on systems using sysvinit:
ENABLED=1
```

Per últim arrancarem el dimoni de spamassassin amb la instrucció **sudo systemctl start spamassassin.service.**

Ara que ja tenim tant clamav com spamassassin configurats, passarem a configurar amavis:

- Habilitar la detecció d'spam i virus en amavis editant /etc/amavis/conf.d/15-content_filter_mode i descomentant les linies que es mostren a continuació:

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


#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


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

- Per a evitar que amavis marque els correus que no són analitzats per spamassassin(els correus interns per exemple) i aparega la paraula UNCHECKED en l'assumpte editarem l'arxiu **/etc/amavis/conf.d/21-Ubuntu-defaults** i afegirem la següent línia:

  $admin_maps_by_ccat{+CC_UNCHECKED} = undef;

- En cas de que el nostre registre mx siga diferent al nom de la màquina deuríem modificar el paràmetre **$myhostname** amb el nom complet amb el domini (FQDN) del nostre servidor. Així mateix, si el nostre servidor accepta correus de més d'un domini ho especificarem amb el paràmetre **@local_domains_acl .** Tots dos es poden trobar al arxiu **/etc/amavis/conf.d/50-user**:

```
#
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file
#
$myhostname = 'mail01.local.lab';
@local_domains_acl = ( "local.lab", "externs.local.lab" );

#
```

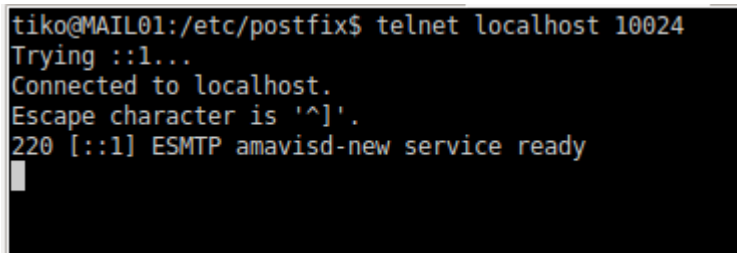
- Després d'aquests canvis reiniciarem el servei d'amavis per a que s'apliquen els canvis amb la instrucció ***sudo systemctl restart amavis.service.***

- Per últim integrarem amavis amb Postfix. Per a fer-ho primerament executarem la instrucció ***sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'.*** Tot seguint editarem /etc/postfix/master.cf i afegirem al final el següent:

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

127.0.0.1:10025 inet n - - - - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters
    -o content_filter=
    -o receive_override_options=no_header_body_checks
```

- Reiniciar Postfix amb ***sudo systemctl restart postfix.service***

Ara només resta comprovar que tot funciona correctament. Primerament comprovarem que amavis esta en marxa:



Per finalitzar comprovarem a les capçaleres de algun correu si realment se esta produint alguna anàlisis dels correus electrònics:

```
root@MAIL01:/srv/vmail/leire@local.lab/Maildir/cur# cat 1464975138.M852031P1729.MAIL01\,S\=1046\,W\=1073\:2\,S
Return-Path: <tiko@local.lab>
X-Original-To: leire@local.lab
Delivered-To: leire@local.lab
Received: from localhost (localhost [127.0.0.1])
        by mail01.local.lab (Postfix) with ESMTP id 301131C0DB5
        for <leire@local.lab>; Fri,  3 Jun 2016 19:32:18 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at local.lab
Received: from mail01.local.lab ([127.0.0.1])
        by localhost (mail01.local.lab [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id yiXiReZp3klr for <leire@local.lab>;
        Fri,  3 Jun 2016 19:31:37 +0200 (CEST)
Received: from 192.168.1.91 (unknown [192.168.1.91])
        by mail01.local.lab (Postfix) with ESMTPA id 64AD51C0D2C
        for <leire@local.lab>; Fri,  3 Jun 2016 19:31:36 +0200 (CEST)
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII;
 format=flowed
Content-Transfer-Encoding: 7bit
Date: Fri, 03 Jun 2016 19:31:36 +0200
From: tiko@local.lab
To: leire@local.lab
Subject: test amavis
Message-ID: <c622e15ba85794159a70f0d93b4f30a9@local.lab>
X-Sender: tiko@local.lab
User-Agent: Roundcube Webmail/1.2.0
```

Al nostre exemple només es pot apreciar el tag **X-Virus-Scanned** perquè les proves de laboratori no s'han fet amb el servidor publicat a Internet. Si ens arribarà un correu des de fora del nostre sistema deurà aparéixer també el tag **X-Spam-Status.**

Instal·lació de Roundcube

La primera cosa que farem serà instal·lar els paquets necessaris per a fer que Roundcube funcione correctament amb apt-get (aquesta instal·lació s'ha fet sobre Ubuntu 14.04):

apt-get install apache2 php5 mysql-server php5-mysql php5-mcrypt php5-intl php-pear php5-ldap

Tot seguit, descarregarem Roundcube, les descomprimirem al directori d'Apache i modificarem els permisos del directori d'Apache per a que tot funcione correctament:

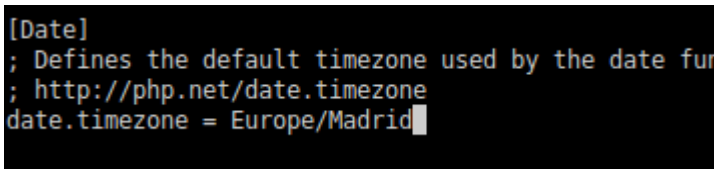
- Descarregar Roundcube i descomprimir

cd /var/www/html
wget https://github.com/roundcube/roundcubemail/releases/download/1.2.0/roundcubemail-1.2.0-complete.tar.gz
sudo tar xvzf roundcubemail-1.2.0-complete.tar.gz
sudo mv roundcubemail-1.2.0 roundcube
sudo rm roundcubemail-1.2.0-complete.tar.gz

- Modificar permisos

cd /var/www/html
sudo chown -R root:www-data roundcube
sudo chmod -R 750 roundcube
sudo chmod -R 720 roundcube/temp roundcube/logs

A continuació configurarem la zona horària a l'arxiu /etc/php5/apache2/php.ini amb el valor Europe/Madrid



Habilitar el modul mcrypt de php: i reiniciar Apache

php5enmod mcrypt
service apache2 restart
És el moment de configurar la base de dades que utilitzarà Roundcube:

- Connectar a la base de dades

mysql -u root -p

- Executar les següents instruccions MySQL

CREATE DATABASE roundcubemail CHARACTER SET utf8 COLLATE utf8_general_ci;

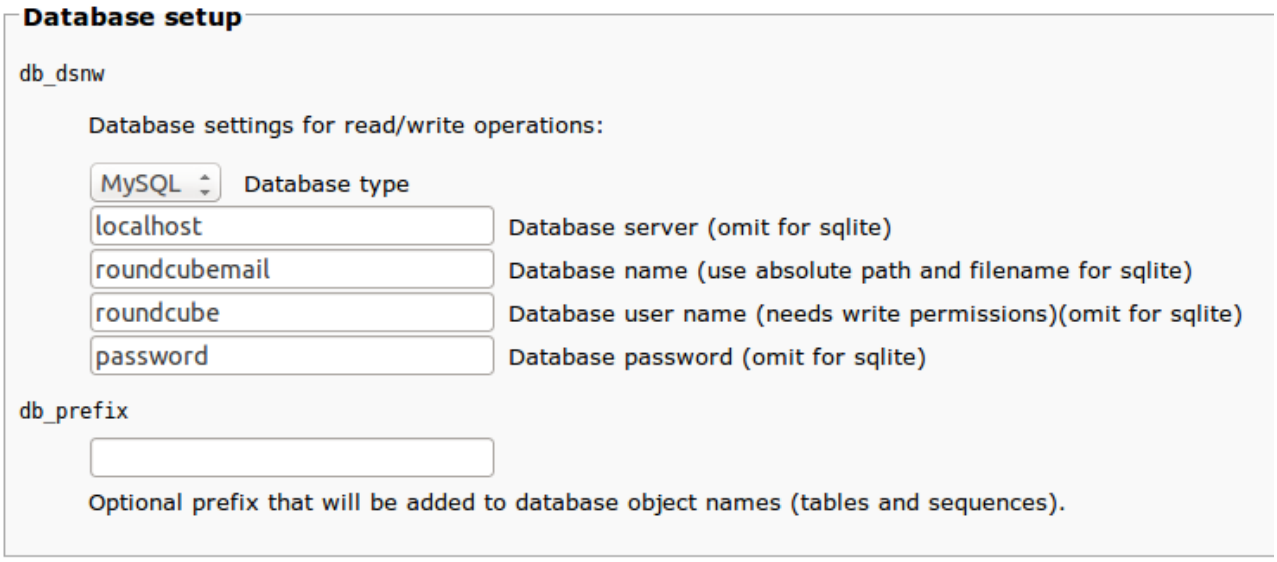
GRANT ALL PRIVILEGES ON roundcubemail.* TO roundcube@localhost IDENTIFIED BY 'password';

QUIT;

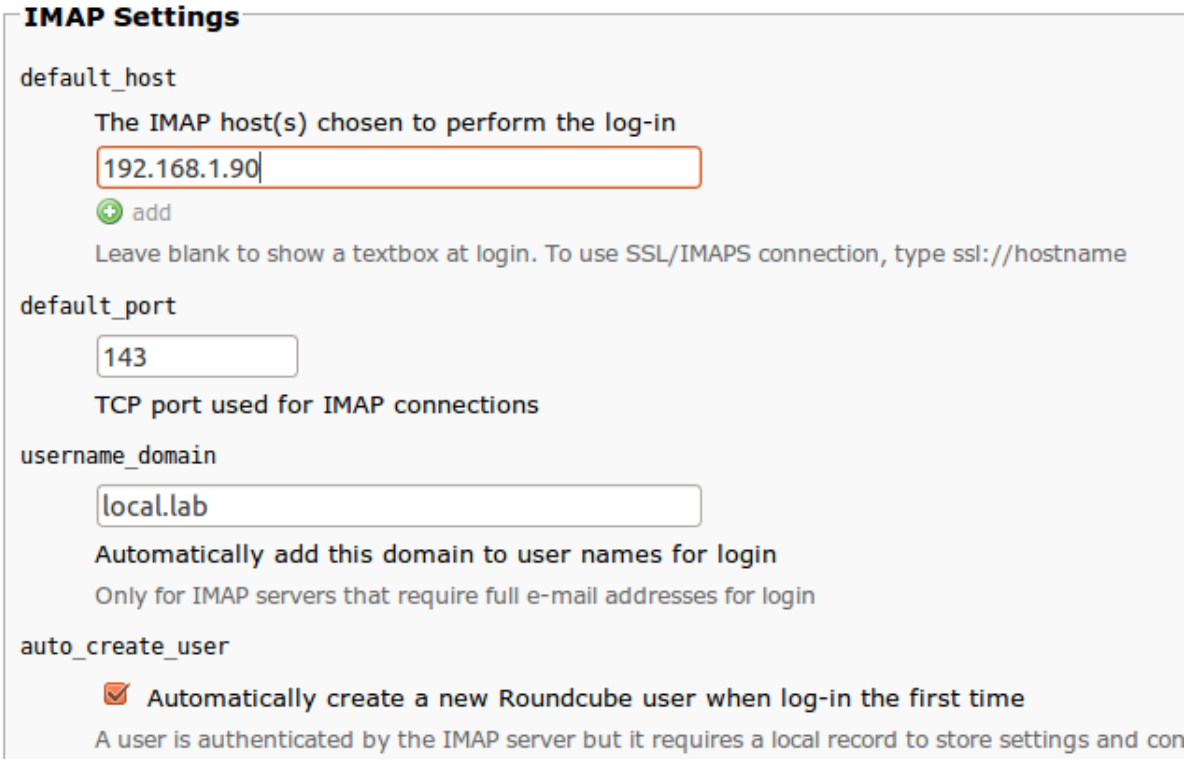
Per a finalitzar ambla configuració accedirem a la pàgina http://IP_del_Srv/roundcube/installer per a arrancar el instal·lador de Roundcube. Primerament veurem una pantalla on podrem comprovar si tenim instal·lats tots els elements necessaris per fer funciona Roundcube:

Si tot es correcte polsarem el botó **Next** per a continuar

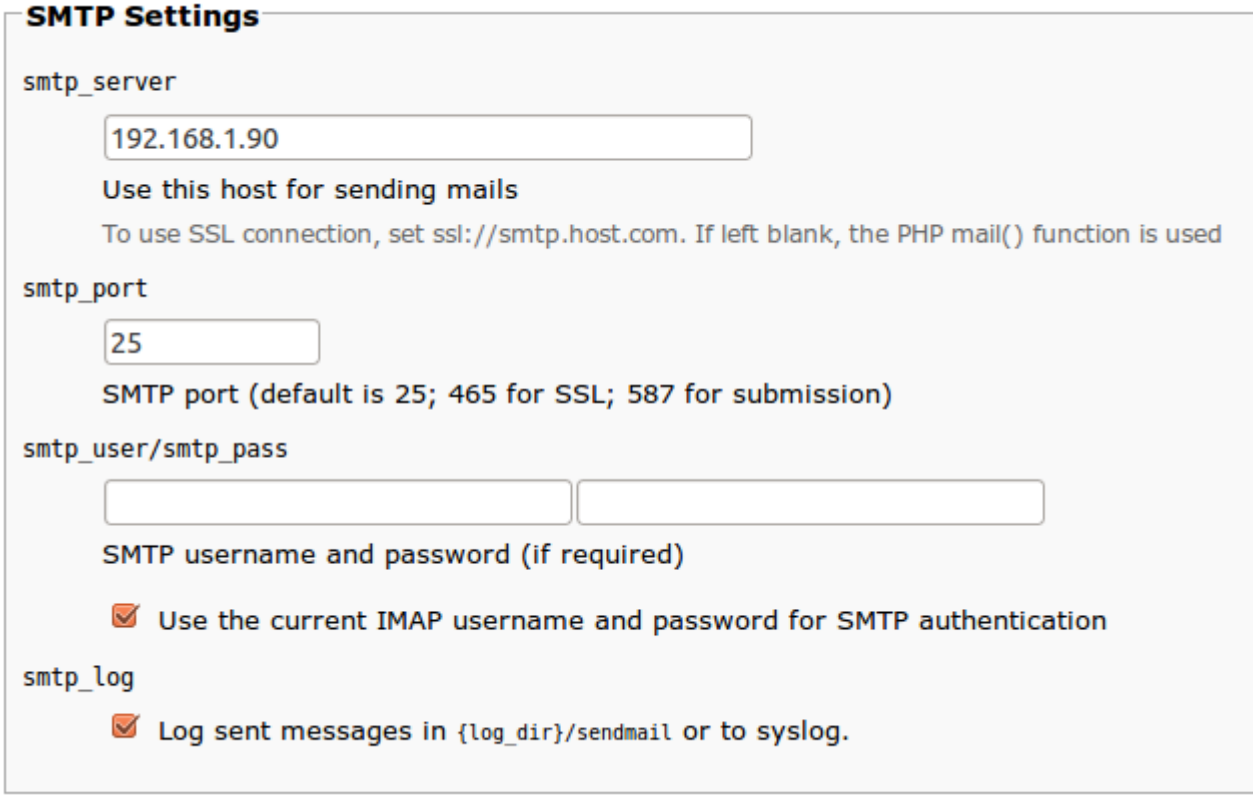
A la següent pantalla començarem a configurar tots els paràmetres per a que Roundcube puga connectar tant amb la base de dades de Roundcube com amb Postfix, Dovecot i el servidor LDAP. En primer lloc definirem els paràmetres de connexió amb la base de dades tal i com els hem definit en apartats anteriors d'aquest annex



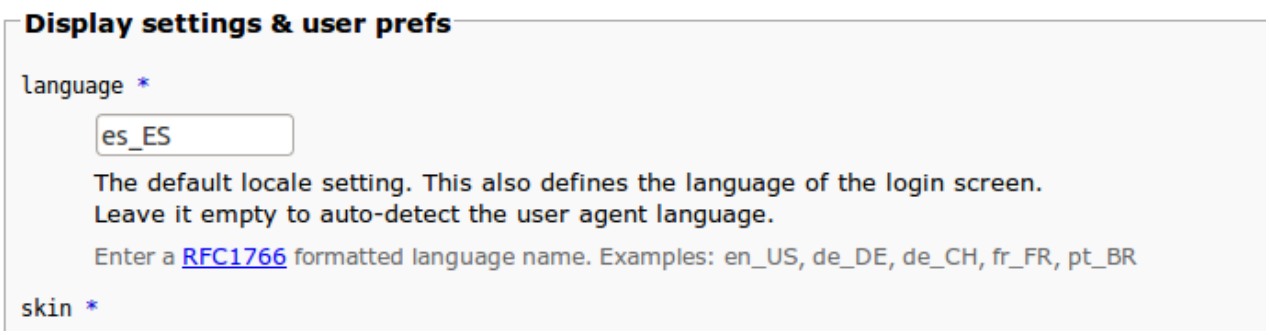
Continuarem amb la configuració del servidor IMAP (Dovecot) del que farà ús Roundcube per a recuperar els correus dels usuaris. Omplir el camp **username_domain** amb el domini dels nostres usuaris



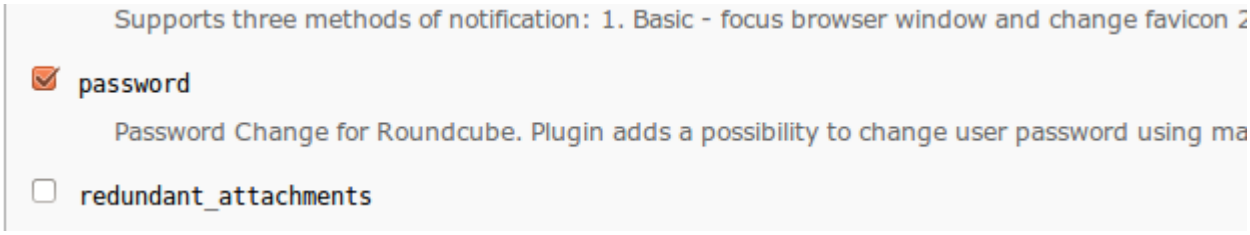
Tot seguit omplirem la informació relativa al servidor SMTP (Postfix). Marcar les caselles **«Use current IMAP username and password for SMTP authentication»**



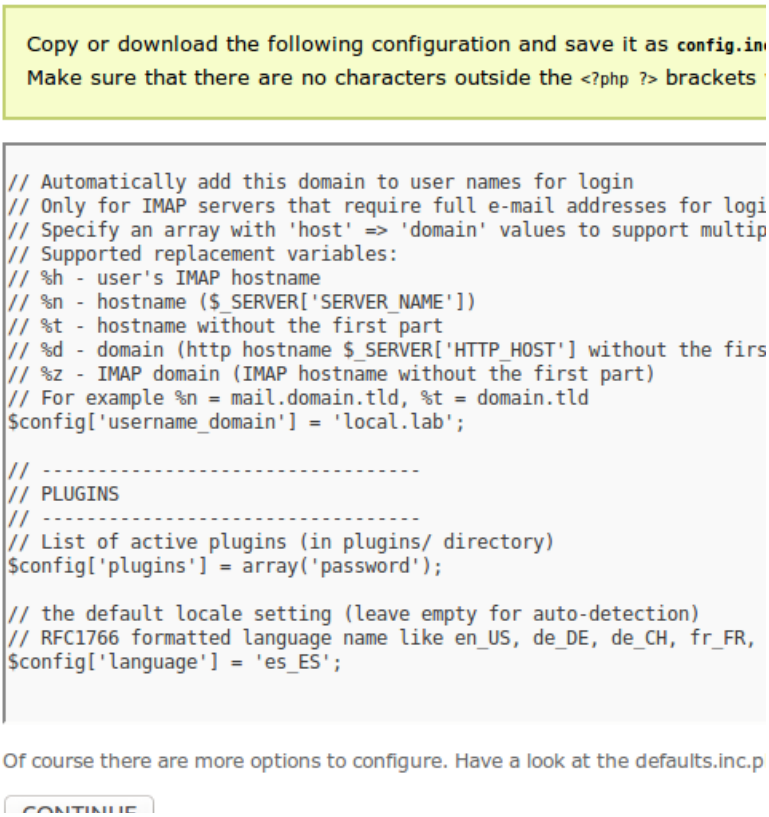
Establirem el llenguatge de l'interfície



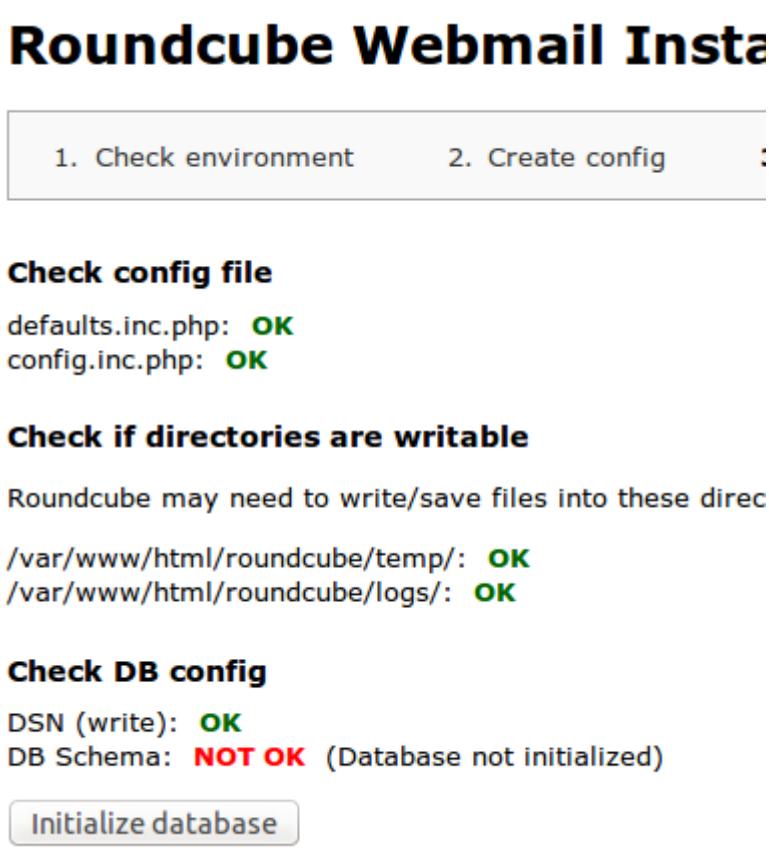
Per últim, activarem el plugin per a poder canviar la contrasenya dels usuaris des de Roundcube



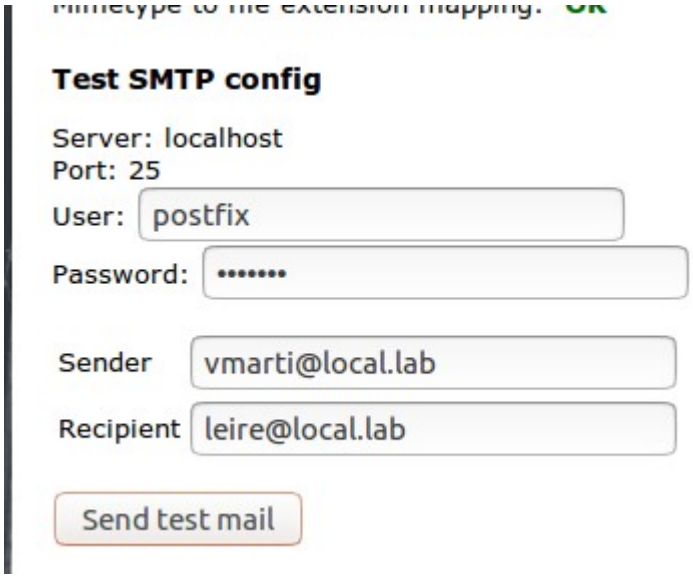
A la següent pantalla podem revisar la configuració que acabem de fer. Quan ja estem segurs d'haver configurat Roundcube correctament, polsem el botó **«Continue»**

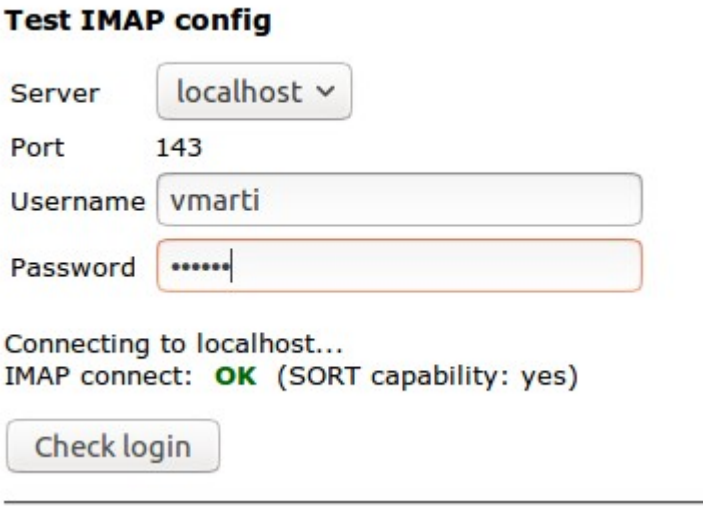


A continuació passarem a la pantalla on podrem comprovar que la nostra configuració funciona correctament. Abans de començar els tests, tindrem que inicialitzar la base de dades. D'aquesta manera també comprovarem que la informació relativa a la base de dades s'ha insertat correctament. Per a inicialitzar la base de dades polsarem el botó **«Initialize database»**

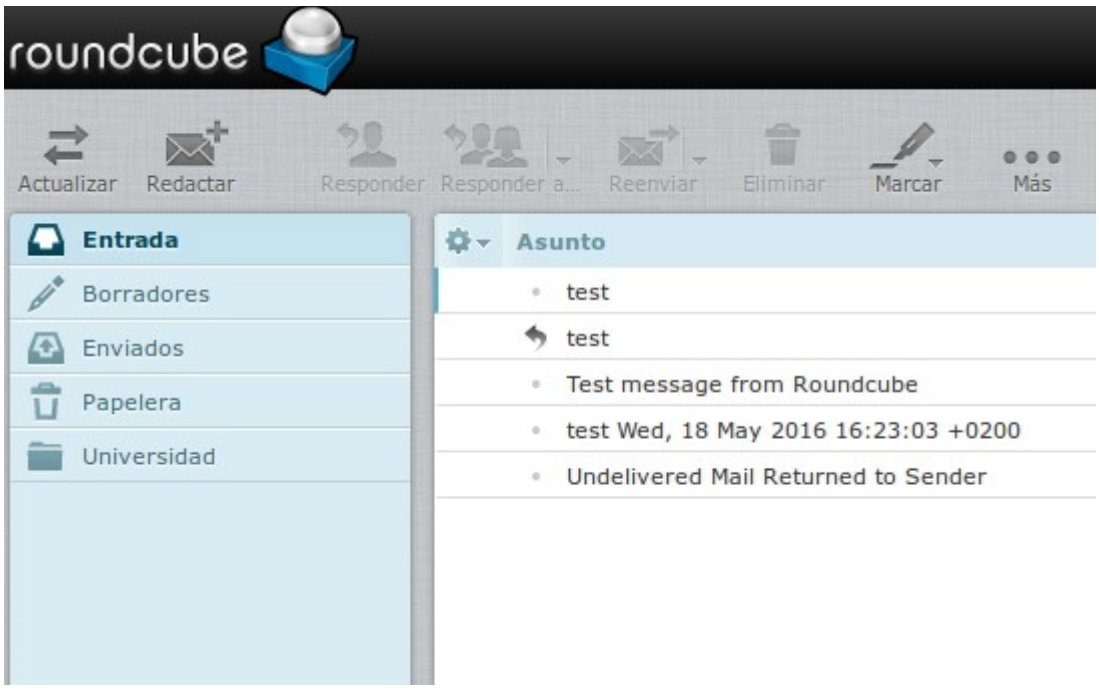


Una vegada la base de dades ha estat inicialitzada, podrem fer el test de la configuració tant del servidor SMTP com del servidor IMAP.





Si passem els tests, ja podrem accedir a Roundcube des de l'adreça http://IP_del_servidor/roundcube amb l'usuari que hem creat en la secció de configuració del servidor LDAP.

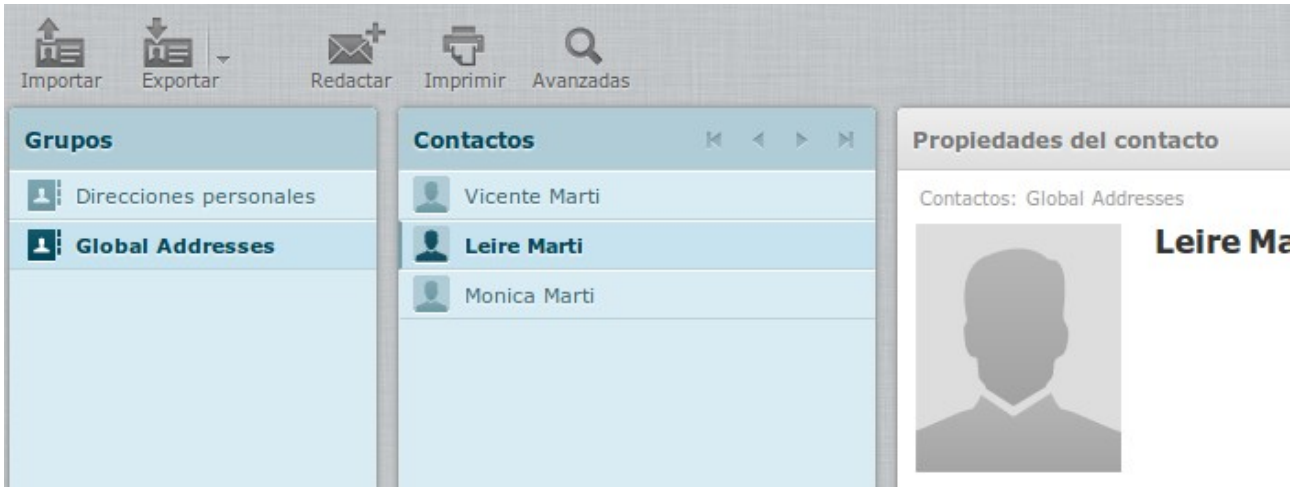


Per últim configurarem Roundcube per a que mostra en la llibreta de direccions global, els usuaris que tenim al nostre servidor LDAP. Per a fer-ho, afegirem les següents linies al nostre arxiu de configuració **/var/www/html/roundcube/config.inc.php:**

```
$config['ldap_public']['ldap'] = array(
  'name'         => 'Global Addresses',
  'hosts'        => array('localhost'),
  'port'         => 389,
  'use_tls'      => false,
  'ldap_version'  => 3,      // using LDAPv3
  'network_timeout' => 10,
  'user_specific' => false,
  'base_dn'      => 'ou=usuaris,dc=local,dc=lab',
  'bind_dn' => 'uid=roundcube,ou=serveis,dc=local,dc=lab',
  'bind_pw' => 'roundcube',
  'search_filter'  => '(objectClass=person)',
  'fieldmap' => array(
    // Roundcube  => LDAP:limit
    'name'       => 'cn',
    'surname'    => 'sn',
    'firstname'   => 'givenName',
    'jobtitle'    => 'title',
    'email'      => 'mail:*',
    'phone:home'  => 'homePhone',
    'phone:work'  => 'telephoneNumber',
    'phone:mobile' => 'mobile',
    'phone:pager' => 'pager',
    'phone:workfax' => 'facsimileTelephoneNumber',
    'street'     => 'street',
    'zipcode'    => 'postalCode',
    'region'     => 'st',
    'locality'    => 'l',
    'country'     => 'c',
    'organization' => 'o',
    'department'   => 'ou',
    'jobtitle'    => 'title',
    'notes'       => 'description',
    'photo'       => 'jpegPhoto',
   ),
  'sort'         => 'cn',       // El camp per el que s'ordenaran els usuaris
  'scope'        => 'sub',
  'filter'       => '(objectClass=organizationalPerson)',
  'fuzzy_search'   => true,
  'vlv'          => false,
  'vlv_search'    => false,
  'numsub_filter'  => '(objectClass=organizationalUnit)',
  'config_root_dn' => 'cn=config',
  'sizelimit'     => '0',        // Limit de usuaris a mostrar. 0 significa sense limit
```

'timelimit' => '0',
'referrals' => false,
'dereference' => 0,

Després d'afegir aquests valors, reiniciarem Apache amb la instrucció ***sudo service apache2 restart*** i ja podrem accedir als usuaris LDAP des de la nostra llibreta de direccions



Annex VII – Instal·lació i configuració d'Owncloud

En aquest annex s'explica els passos a seguir per la instal·lació i configuració de la solució OwnCloud proposada al capítol 11.

Instal·lació de MariaDB Galera Cluster en Ubuntu 16.04 server amb balanceig de càrrega

Per a la instal·lació del cluster de base dades amb MariaDB i Galera hi ha que seguir els següents passos en cada node membre del cluster.

Instal·lació de MariaDB

1. Instal·lar el paquet software-properties-common per a poder gestionar els repositoris on es troba tot el programari a instal·lar. Afegir el repositori de la versió d'Ubuntu on anem a instal·lar MariaDB(es pot comprovar les instruccions necessàries per a cada versió a https://downloads.mariadb.org/mariadb/repositories/#mirror=tedeco). Instal·larem l'última versió estable a la data de creació d'aquest document, MariaDB 10.1

```
sudo apt-get install software-properties-common
```

```
sudo apt-key adv --recv-keys –keyserver hkp://keyserver.ubuntu.com:80 0xF1656F24C74CD1D8
```

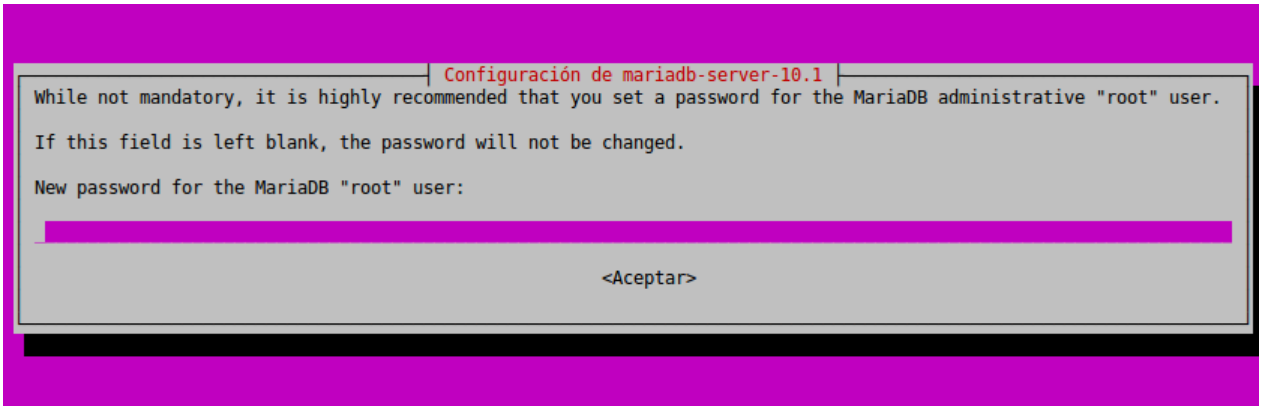
```
sudo add-apt-repository 'deb [arch=amd64,i386]
http://tedeco.fi.upm.es/mirror/mariadb/repo/10.1/ubuntu xenial main'
```

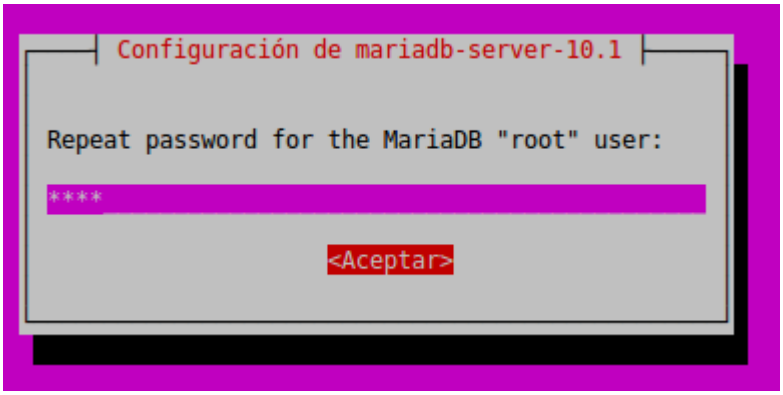
2. Instal·lar MariaDB (el soport per a galera cluster ja va inclòs en el paquet del servidor en aquesta versió)

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get install mariadb-server
   ```

   En el procés d'instal·lació establirem la contrasenya del usuari MariaDB root. La introduirem dues vegades.





Repetirem els passos 1 i 2 en tots els nodes que formaran el cluster.

Configuració i creació de Galera cluster

1. Primerament pararem el servei de MariaDB a tots els nodes executant la següent instrucció a cadascun d'ells:

   sudo systemctl stop mariadb.service

2. Crearem l'arxiu de configuració **/etc/mysql/conf.d/galera.cn** al primer node que hem creat

   [mysqld]

   #mysql settings
   binlog_format=ROW
   default-storage-engine=innodb
   innodb_autoinc_lock_mode=2
   innodb_doublewrite=1
   query_cache_size=0
   query_cache_type=0
   bind-address=0.0.0.0
   #galera settings
   wsrep_on=ON
   wsrep_provider=/usr/lib/galera/libgalera_smm.so
   wsrep_cluster_name="owncloud_cluster"
   wsrep_cluster_address=gcomm://IPs_dels_altres_nodes_separades_amb_coma
   wsrep_node_address=IP_del_node
   wsrep_sst_method=rsync

3. Copiar l'arxiu creat al punt anterior a tots els nodes i després modificar-lo amb els valor de cada servidor. Per a copiar l'arxiu podem executar la següent instrucció des del primer node configurat:

   sudo scp /etc/mysql/conf.d/galera.cnf usuari_sudoer@servidor_destí:/etc/mysql/conf.d/

4. Crear el cluster en el primer node, arrancar el node i comprovar seguint els següents passos:

   - Crear el cluster

     sudo galera_new_cluster

   - Arrancar el node

     sudo systemctl start mariadb.service

   - Comprovar que MariaDB a arrancat correctament:

     sudo systemctl status mariadb.service

```
tiko@DB01:~$ sudo systemctl status mariadb.service
● mariadb.service - MariaDB database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor
  Drop-In: /etc/systemd/system/mariadb.service.d
           └─migrated-from-my.cnf-settings.conf
   Active: active (running) since dv 2016-05-20 15:10:15 CEST; 1 weeks
  Process: 1426 ExecStartPost=/etc/mysql/debian-start (code=exited, sta
  Process: 1387 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -
 Main PID: 1390 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 33 (limit: 512)
   Memory: 60.7M
      CPU: 26min 29.247s
   CGroup: /system.slice/mariadb.service
           └─1390 /usr/sbin/mysqld --wsrep-new-cluster
```

5. Per últim, arrancar mariadb en cada node i comprovar que el cluster té tants nodes com servidors hem configurat.

   - Arrancar els nodes restants amb:

     sudo systemctl start mariadb.service

   - Executar en qualsevol d'ells la següent instrucció per verificar que tots estan afegits al cluster.(la contrasenya que es demana es la de l'usuari root de MariaDB)

```
tiko@DB01:~$ mysql -u root -p -e 'SELECT VARIABLE_VALUE as "cluster size" FROM INFORMATI
Enter password:
+--------------+
| cluster size |
+--------------+
| 3            |
+--------------+
tiko@DB01:~$
```

Instal·lació i configuració d'HAProxy per a MariaDB Galera Cluster en Ubuntu 16.04

Per a que la nostra base de dades siga tolerant a fallades i al mateix temps la càrrega de transaccions siga balancejada a tots els nodes que formen MariaDB Galera cluster farem ús d'HAProxy.

- Habilitar l'accés des del servidor amb HAProxy al cluster MariaDB. Per a fer-ho, habilitarem que l'inici de sessió amb l'usuari root siga possible des del servidor amb HAProxy. A qualsevol dels nodes del cluster executar el següent:

```
mysql -u root -p -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'ip_haproxy'
IDENTIFIED BY 'contrasenya usuari root de MariaDB' WITH GRANT OPTION; FLUSH
PRIVILEGES;"
```

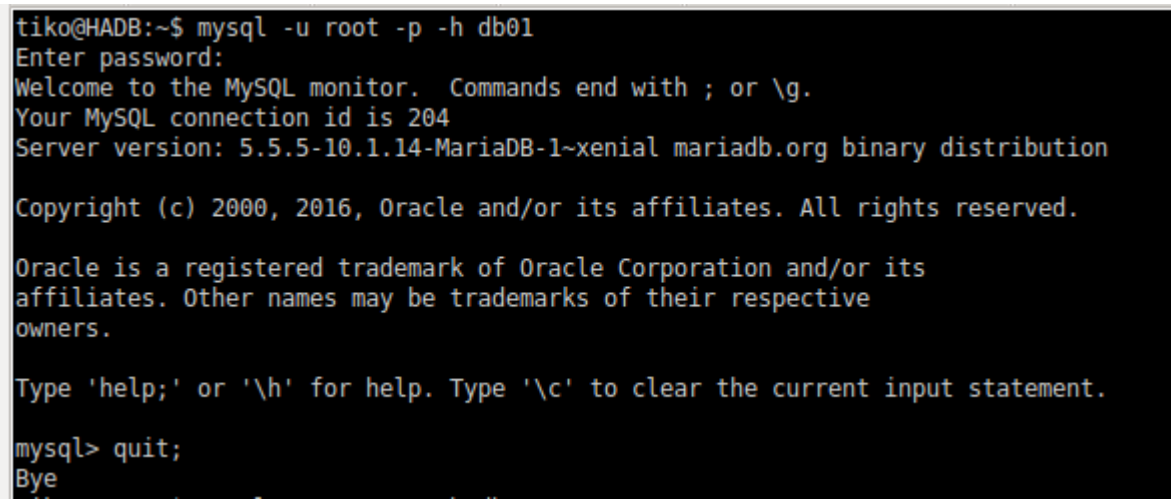
- Comprovar que es pot accedir a qualsevol node des del servidor HAProxy amb el client de mysql:

  Instal·lar mysql-client

  sudo apt-get install mysql-client

  Executar per a cada node del cluster des del servidor HAProxy:

  mysql -u root -p -h IP_o_nom_node_cluster



- Instal·lar haproxy

  sudo apt-get install haproxy -y

- Configurar HAProxy editant l'arxiu **/etc/haproxy/haproxy.cfg.** Afegir les següents linies al final de l'arxiu:

  listen galera

  bind ip_haproxy:3306

  mode tcp

  balance roundrobin

  server db01 ip_node1:3306 weight 1

  server db02 ip_node2:3306 weight 1

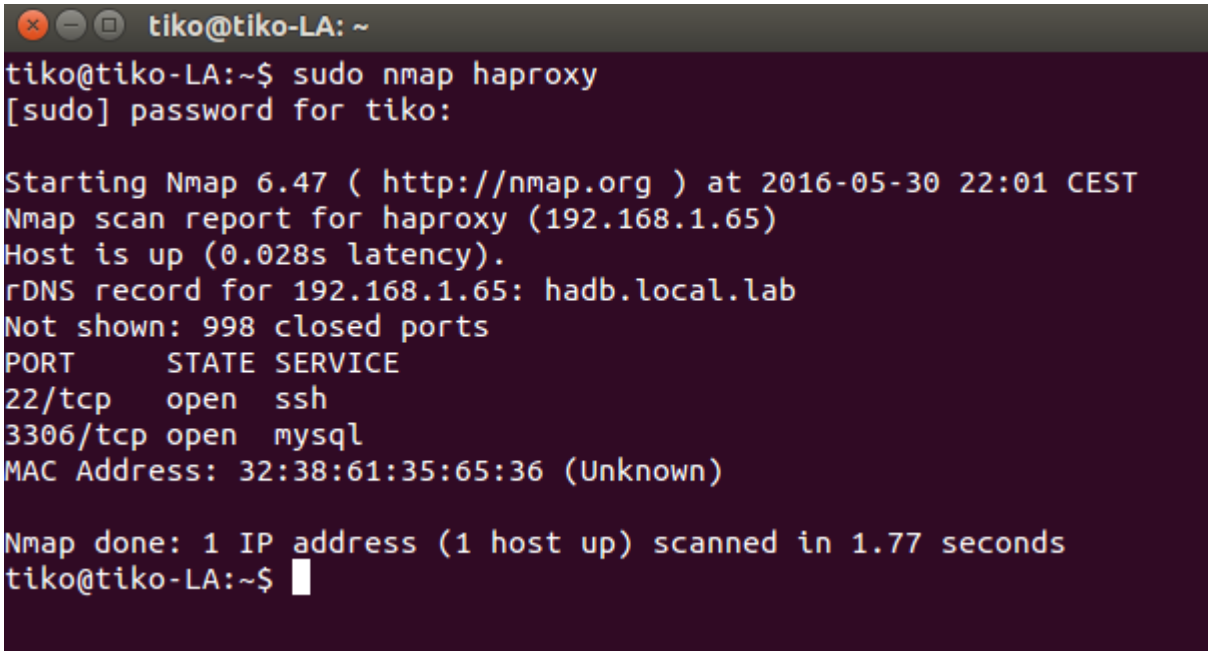
  server db03 ip_node3:3306 weight 1

- Reiniciar HAProxy:

  sudo systemctl restart haproxy.service

Podem comprovar que el servidor HAProxy esta escoltant al port que hem definit a l'arxiu de configuració amb executant nmap des de qualsevol ordinador que tinga accés per xarxa al servidor HAProxy:

sudo nmap IP_del_Servidor_HAProxy



Instal·lació servidor NFS

Per a poder tindre tant el directori on es guarda la informació dels usuaris com els fitxers d'aplicació en un lloc comú instal·larem un servidor NFS que exportara dos directoris: un per a les dades d'Owncloud i altre per muntar-lo al directori /var/www dels servidor d'aplicacions. A aquest últim guardarem els arxius d'aplicació d'Owncloud. A continuació es llisten els passos a seguir per configurar el servidor NFS en Ubuntu 16.04

- Instal·lar **nfs-kernel-server**:

  sudo apt-get install nfs-kernel-server

- Editar l'arxiu **/etc/exports** i afegir les linies següents al final:

  /share IP_OwnCloud1(rw,no_root_squash) IP_OwnCloud2(rw,no_root_squash)
  /web IP_OwnCloud1(rw,no_root_squash) IP_OwnCloud2(rw,no_root_squash)

Amb aquestes linies es compartiran els directoris /share i /web del nostre servidor NFS per a que només puguen accedir els servidors amb **IP_OwnCloud1 i IP_OwnCloud2.** Si els directoris no existeixen al servidor NFS tindrem que crear-los tal i com es mostra a continuació:

sudo mkdir /share
sudo mkdir /web

- Modificar els permisos dels directoris de la següent manera:

  sudo chown 770 /share
  sudo chown root:www-data /share

- Crear el directori html dins /web

  sudo mkdir /web/html

Instal·lació servidor d'aplicació OwnCloud en Ubuntu 14.04

Ara que ja tenim tot el que ens fa falta podem instal·lar els servidors d'accés d'Owncloud. Hi ha diferents maneres de fer-ho però al cas que ens ocupa, ens interessa instal·lar cada component per separat. Seguirem els següents passos:

1. Instal·lar els pre-requisits d'Owncloud:

sudo apt-get install apache2 libapache2-mod-php5
sudo apt-get install php5-gd php5-json php5-mysql php5-curl
sudo apt-get install php5-intl php5-mcrypt php5-imagick

2. Copiar /var/www/html/index.html al directori /web/html del servidor NFS:

sudo scp /var/www/html/index.html usuari_sudoer@IP_Servidor_NFS:/web/html

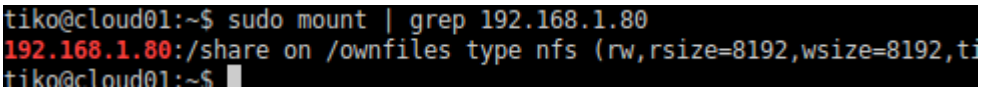
3. Modificar l'arxiu /etc/fstab per a que es munten els directoris compartits pel servidor NFS en l'inici. Per a que el servidor puga muntar els directoris NFS serà necessari instal·lar el paquet nfs-common amb la instrucció ***sudo apt-get install nfs-common. Afegir*** les següents linies al final de l'arxiu i reiniciar el servidor:

IP_Servidor_NFS:/share /ownfiles nfs rsize=8192,wsize=8192,timeo=14,intr
IP_Servidor:/web /var/www nfs rsize=8192,wsize=8192,timeo=14,intr

4. Després de reiniciar ens assegurarem que el directori /var/www del nostre servidor d'aplicacions correspon en realitat al directori /web del servidor NFS. Per a fer-ho executarem a un terminal el següent:

sudo mount | grep IP_Servidor_NFS

Si els directoris s'han muntat correctament deurem vore una imatge similar a la que be a continuació però mostrant ambdós directoris.



5.Descarregar i instal·lar els arxius d'Owncloud**(FER NOMÉS EN EL PRIMER NODE)** :

```
wget -nv https://download.owncloud.org/download/repositories/stable/Ubuntu_14.04/Release.key -O
Release.key
apt-key add - < Release.key

sh -c "echo 'deb http://download.owncloud.org/download/repositories/stable/Ubuntu_14.04/ /' >>
/etc/apt/sources.list.d/owncloud.list"

apt-get update
apt-get install owncloud-files
```

D'aquesta manera s'instal·laran sols els arxius d'Owncloud i ninguna de les altres dependències.

6. Habilitar Owncloud en Apache:

- Crear l'arxiu owncloud.conf en /etc/apache2/sites-available/ i afegir les següents linies:

```
Alias /owncloud "/var/www/owncloud/"
<Directory /var/www/owncloud/>
  Options +FollowSymlinks
AllowOverride All

<IfModule mod_dav.c>
Dav off
</IfModule>

SetEnv HOME /var/www/owncloud
 SetEnv HTTP_HOME /var/www/owncloud

</Directory>
```

- Executar la instrucció ***sudo a2ensite owncloud***

- Habilitar els següents mòduls amb la instrucció **a2enmod (ex: sudo a2enmod rewrite)**

  rewrite

  headers

  env

  dir

  mime

  ssl

- Habilitar lloc segur https:

  sudo a2ensite default-ssl

- Reiniciar Apache

  sudo systemctl restart apache2

7.Canviar els permisos a /var/www/owncloud**(FER NOMÉS AL PRIMER NODE)**

sudo chown -R www-data:www-data /var/www/owncloud/

8. Acabar la configuració d'Owncloud a la interfície web. Connectar a la interfície web en la direcció https://IP_servidor_OwnCloud/owncloud. Introduir el servidor de base de dades, l'usuari root de la base de dades i la localització del directori de dades així com el nom d'usuari i contrasenya que volem emprar a OwnCloud.

Repetir tots els passos descrits en aquesta secció excepte el punt 5 i el 7 en cada node. Si tot està correctament configurat quan intentem accedir a qualsevol dels nodes d'Owncloud la informació deuria ser coherent amb els altres servidor.

Configuració d'HAProxy per l'accés per l'interfície web

Per a la instal·lació d'HAProxy podem seguir les mateixes instruccions que a la instal·lació i configuració d'HAProxy per a MariaDB Galera Cluster descrita en la secció Instal·lació **i configuració d'HAProxy per a MariaDB Galera Cluster en Ubuntu 16.04.** però l'arxiu de configuració diferent.

Abans de modificar l'arxiu de configuració crearem un certificat per a poder utilitzar https per a connectar a Owncloud mitjançant HAProxy.:

- Executar les següents instruccions:

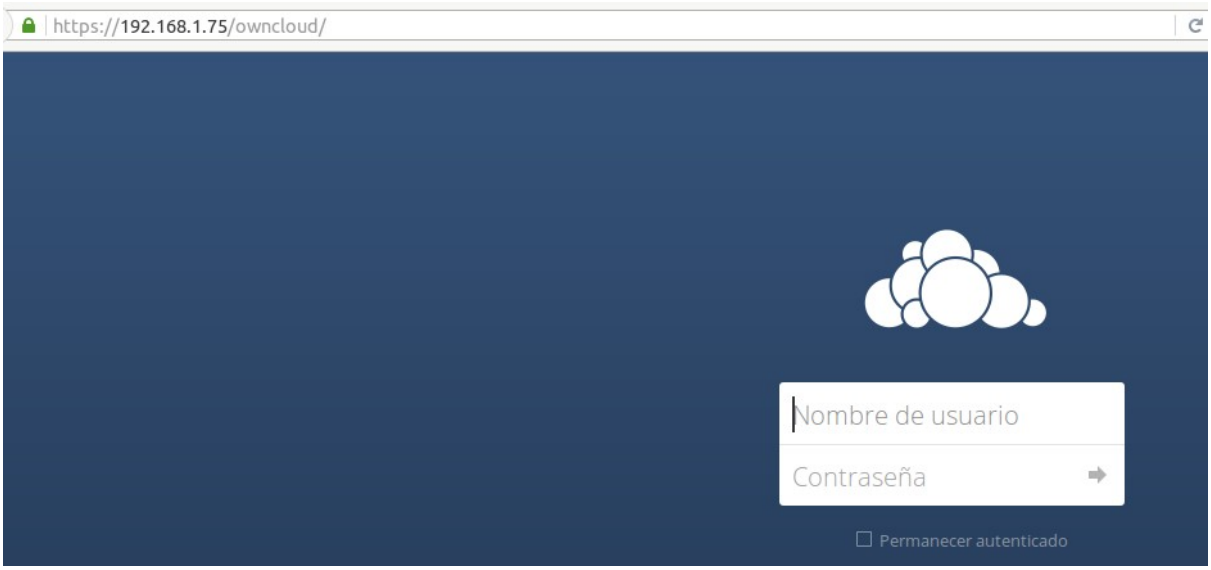
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/apache.key -out /etc/ssl/apache.crt
cd /etc/ssl
sudo cat apache.crt apache.key > owncloud.pem
sudo cp owncloud.pem /etc/ssl/private/owncloud.pem

Aquest seria un exemple per a l'arxiu **/etc/haproxy/haproxy.cfg.** Cal destacar l'ús del paràmetre appsession per usar sticky sessions seguint les recomanacions d'Owncloud**:**

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        stats socket /run/haproxy/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy
        daemon
        # Default SSL material locations
        ca-base /etc/ssl/certs
        crt-base /etc/ssl/private
        # Default ciphers to use on SSL-enabled listening sockets.
        # For more information, see ciphers(1SSL). This list is from:
        #  https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
        ssl-default-bind-ciphers
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:E
CDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS
        ssl-default-bind-options no-sslv3
#       option forwardfor
defaults
        log     global
        mode    http
        option httplog
        option dontlognull
      timeout connect 5000
      timeout client  50000
      timeout server  50000
```

```
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http
frontend http-in
   bind *:80
   reqadd X-Forwarded-Proto:\ http
   default_backend web_farm
backend web_farm
   balance source
   appsession PHPSESSID len 64 timeout 3h request-learn prefix
   server cloud01 IP_cloud01:80 maxconn 32 check
   server cloud02 IP_cloud02:80 maxconn 32 check
frontend https-in
   bind *:443 ssl crt /etc/ssl/private/owncloud.pem
   reqadd X-Forwarded-Proto:\ https
   default_backend web_farm_https
backend web_farm_https
  redirect scheme https if !{ ssl_fc }
  balance source
  appsession PHPSESSID len 64 timeout 3h request-learn prefix
  server cloud01 IP_Cloud01:80 maxconn 32 check
  server cloud02 IP_CLoud02:80 maxconn 32 check
```

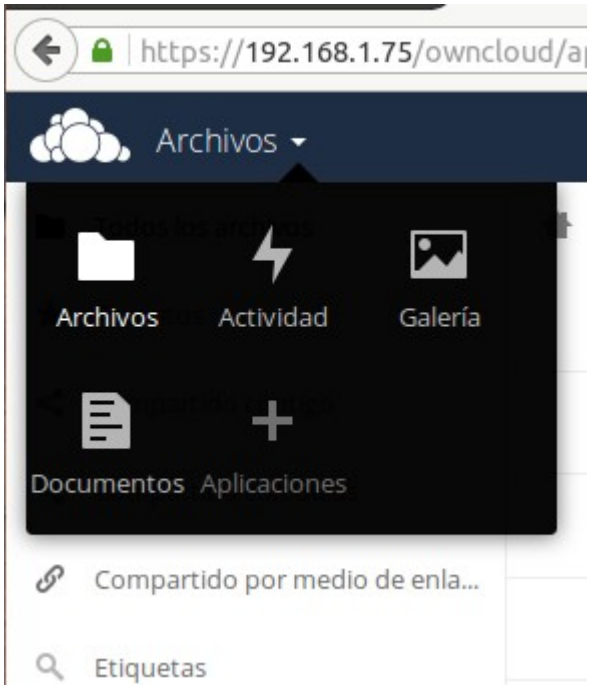
Per últim, podem accedir a la nostre instal·lació d'Owncloud amb l'adreça https://IP_servidor_HAProxy/owncloud:



Autenticació amb LDAP

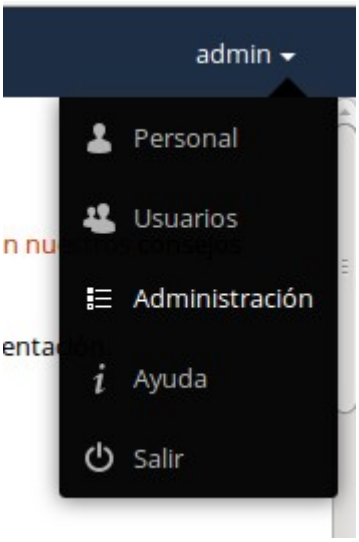
Per finalitzar la instal·lació d'Owncloud, habilitarem l'autenticació d'usuaris amb un servidor LDAP. A continuació es detallen els passos a seguir:

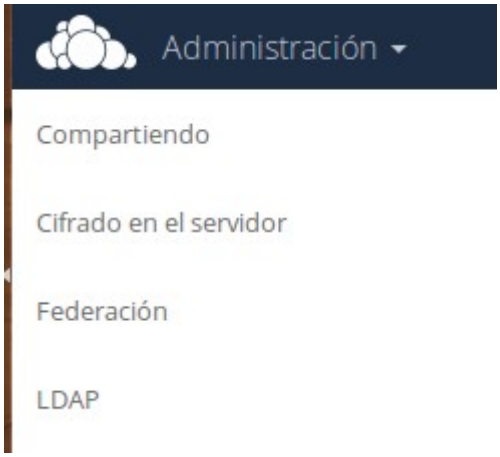
- Farem inici de sessió amb l'usuari admin i desplegarem el menú que i ha a la part superior esquerra os podem trobar totes les aplicacions instal·lades al nostre servidor Owncloud. Fer clic en **«Aplicaciones»**



- A la part esquerra seleccionarem el filtre **«No habilitado»** i buscarem l'aplicació **«LDAP user and group backend».**Polsarem el botó **«Activar»**

- Obrirem el panel d'administració fent clic al nom del usuari admin en la part superior dreta. Es desplegarà un menú on hem de clicar en **«Administración».** En la part esquerra del panel d'administració trobarem els diferents àmbits de configuració que ofereix la nostra instal·lació d'Owncloud. Farem clic en LDAP .



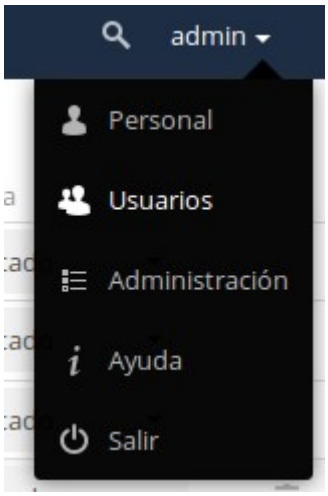


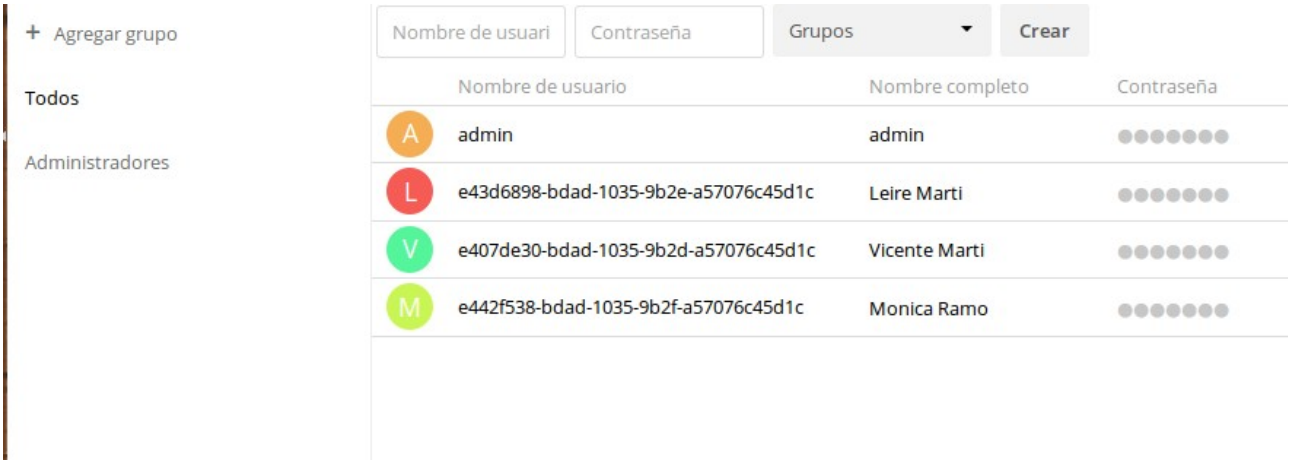
- Primerament omplirem la informació relativa al servidor:
  - IP del servidor LDAP i port on es servidor escolta les peticions. El port es pot detectar automàticament polsant el botó **«Detectar puerto».** El port per defecte és el 389.
  - Usuari que farà les consultes al servidor ldap. Aquest usuari ha de tindre permisos de lectura al menys de la unitat organitzativa on estan els usuaris i de lectura del seu camp userPassword (seguir configuració LDAP de l'annex VI)
  - Contrasenya del usuari que farà les consultes al servidor
  - Base DN per a les consultes. Pot ser o l'arrel del directori LDAP o directament una unitat organitzativa on tingam tots els usuaris a qui volem donar accés al servidor Owncloud.

- Passarem a la pestanya **«Usuarios»** . Ací seleccionarem el tipus d'objecte que correspon als nostres usuaris. Al exemple, els usuaris els hem creat de la classe InetOrgPerson. Verificarem la configuració i comprovarem que Owncloud ha trobat tots els usuaris esperats amb el botó **«Verificar configuració y contar usuarios»**

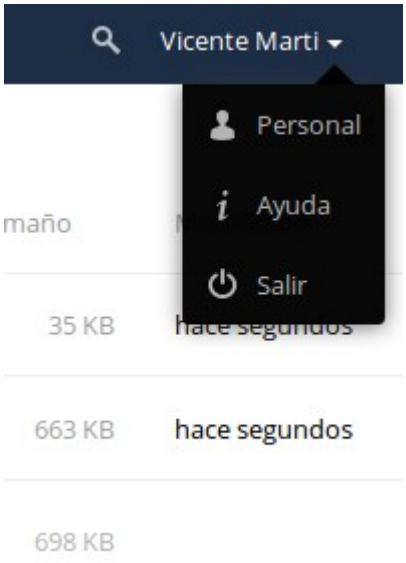
- En la pestanya **«Atributos de inicio de sesión»** quins atributs dels nostres usuaris podrem utilitzar per iniciar sessió en Owncloud.

- Podem comprovar que la configuració és correcta obrint el menú **«Usuarios»** clicant en el nom del nostre usuari admin a la part superior dreta. Quan s'obre la vista d'usuaris farem clic en **«Todos».** Si tot ha funcionat correctament deurem vore tots els nostres usuaris LDAP a la llista d'usuaris. Des d'aquí podrem canviar la seua contrasenya o assignar-los a un grup.





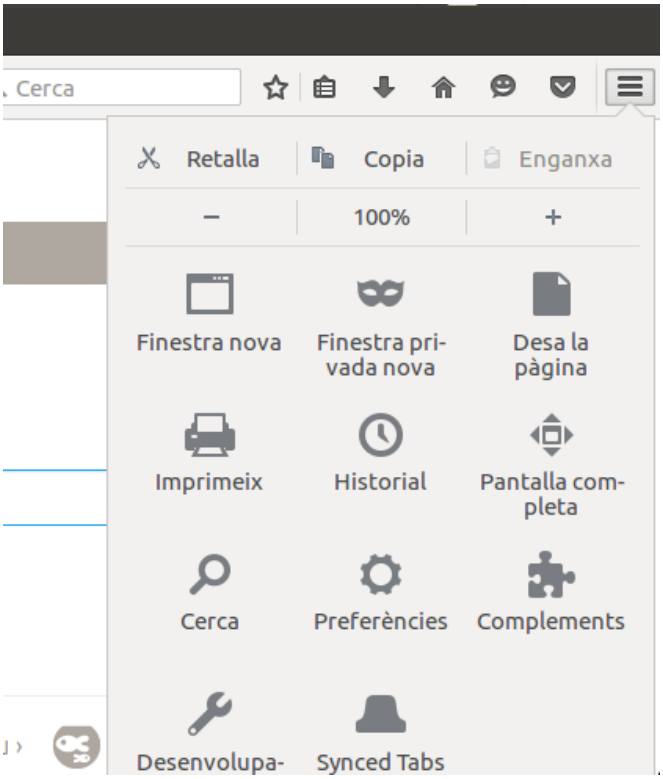
- Per últim, ens faltarà comprovar que realment podem iniciar la sessió al nostre servidor Owncloud.



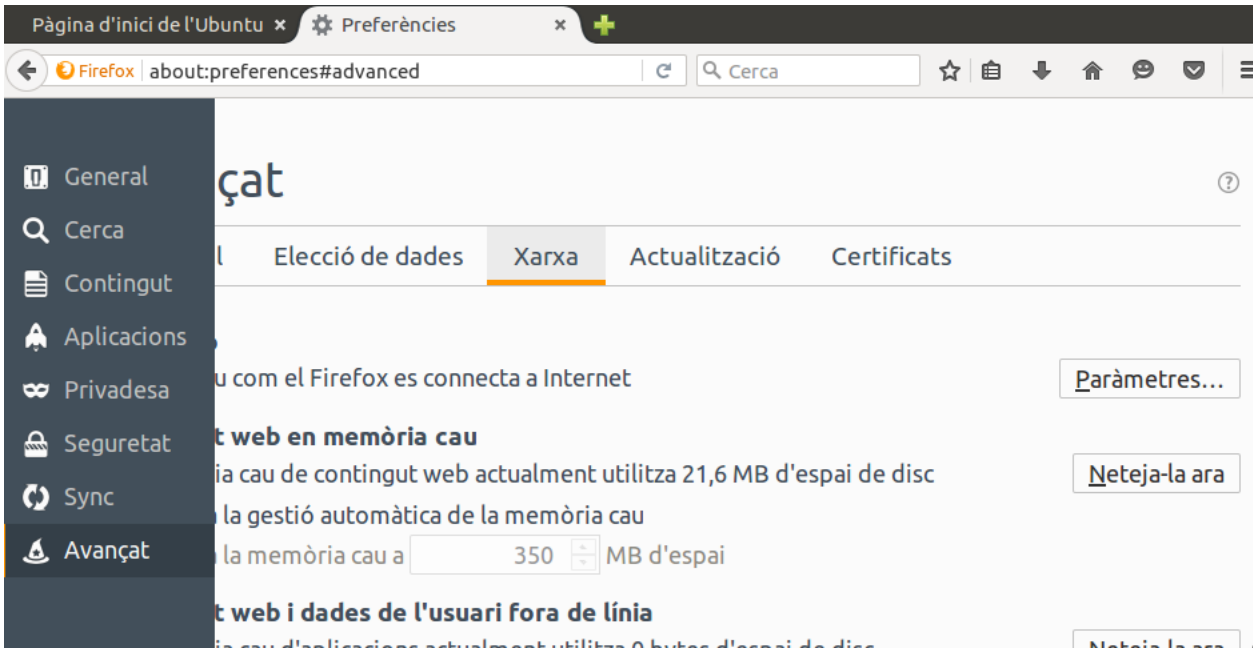
Annex VIII – Configuració de servidor intermediari en Firefox i apt

Configuració de servidor intermediari en Firefox

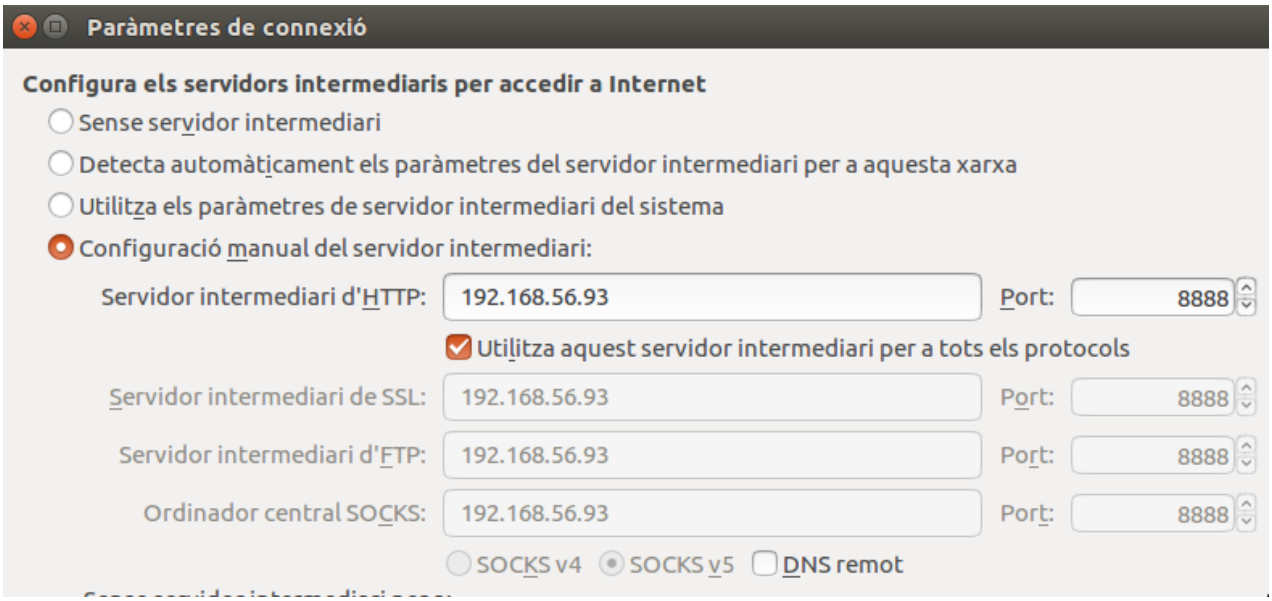
- Obrir les preferències de Firefox:



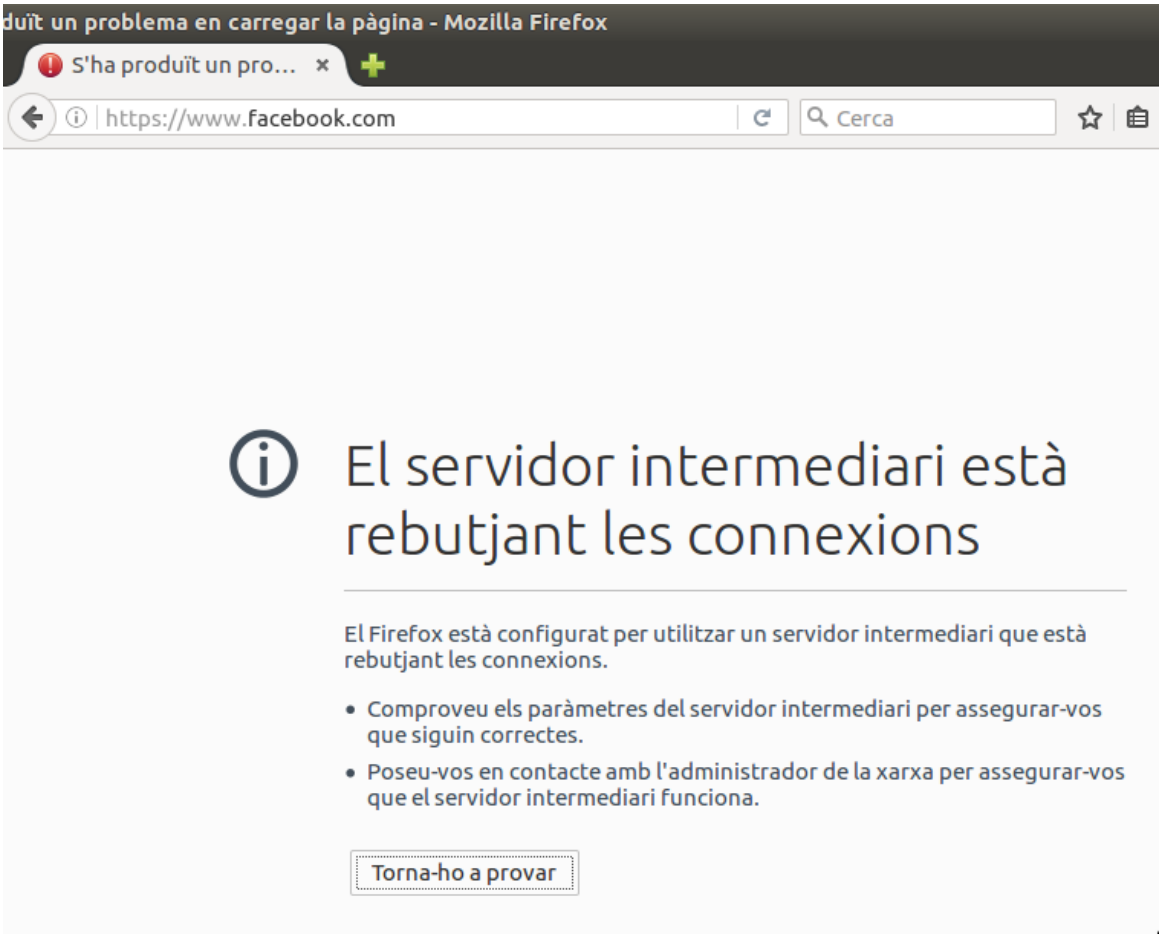
- En la secció Avançat, anar a la pestanya Xarxa i polsar el boto Paràmetres:



- Establir la IP del servidor intermediari, el port definit per a squid en **/etc/squid/squid.conf** i marcar la casella ***"Utilitza aquest servidor intermediari per a tots els protocols"***



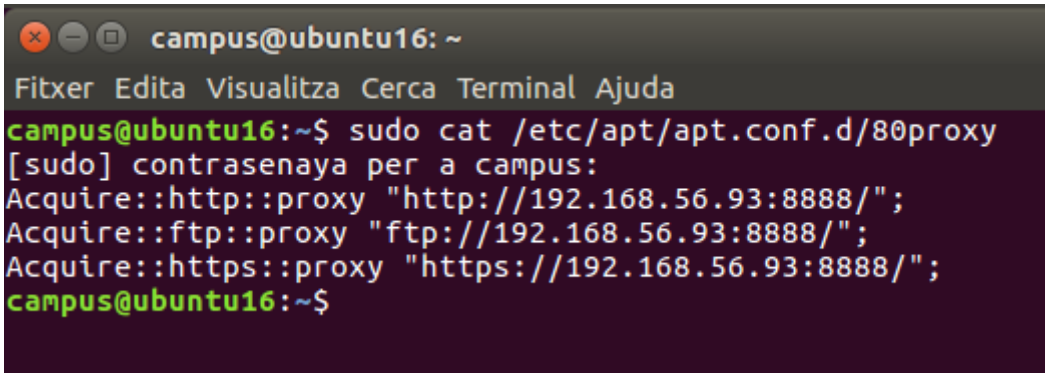
Com podem comprovar a la imatge següent Squid ja esta configurat:



Configuració d'apt-get per a funcionar amb un servidor intermediari

- Crear l'arxiu /etc/apt/apt.conf.d/80proxy i afegir les següents linies:

Acquire::http::proxy "http://192.168.56.93:8888/";
Acquire::ftp::proxy "ftp://192.168.56.93:8888/";
Acquire::https::proxy "https://192.168.56.93:8888/";



Annex IX – Instal·lació d'OpenVPN a Ubuntu 14.04

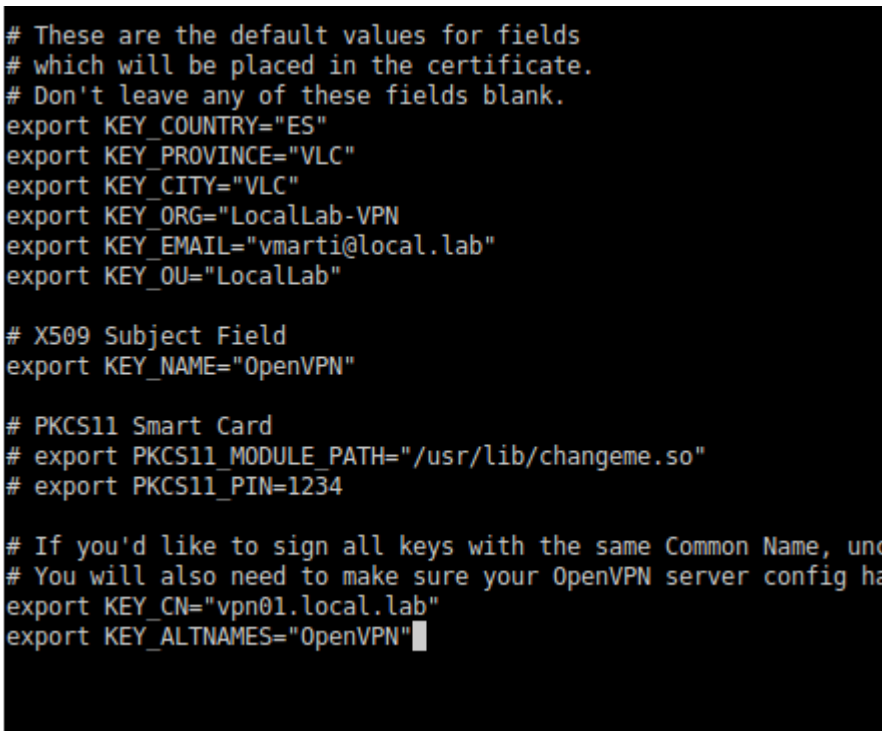
Primerament instal·larem els paquets necessaris per a poder fer OpenVPN funcionar correctament amb apt-get:

sudo apt-get -y install openvpn easy-rsa dnsmasq

A continuació, en farem super usuaris, crearem el directori **easy-rsa** en **/etc/openvpn** i copiarem el contingut de **/usr/share/easy-rsa:**

sudo su
cd /etc/openvpn
mkdir easyrsa
cp -r /usr/share/easy-rsa* /etc/openvpn/easy-rsa

Tot seguit crearem els certificats necessaris per a que OpenVPN funcione correctament. En primer lloc editarem l'arxiu **/etc/openvpn/easy-rsa/vars** per a canviar els valors de les variables que utilitzarem per a crear els certificats tal i com es mostra a l'imatge:



Ara crearem els certificats. Primer crearem el de la CA que firmarà la resta de certificats executant les següents instruccions:

source vars
./clean-all (no executar quan ja s'han creat els certificats perquè els esborrarà)
./build-ca

```
root@vpn01:/etc/openvpn/easy-rsa# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
root@vpn01:/etc/openvpn/easy-rsa# ./clean-all
root@vpn01:/etc/openvpn/easy-rsa# ./build-ca
Generating a 2048 bit RSA private key
..................+++
............................+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [VLC]:
Locality Name (eg, city) [VLC]:
Organization Name (eg, company) [Local Lab OpenVPN]:
Organizational Unit Name (eg, section) [LocalLab]:
Common Name (eg, your name or your server's hostname) [vpn01.local.lab]:
Name [OpenVPM]:
Email Address [vmarti@local.lab]:
root@vpn01:/etc/openvpn/easy-rsa#
```

A continuació crearem el certificat per al nostre servidor OpenVPN:

./build-key-server vpn01

```
root@vpn01:/etc/openvpn/easy-rsa# ./build-key-server vpn01
Generating a 2048 bit RSA private key
.....................................................+++
.....................................................+++
writing new private key to 'vpn01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [VLC]:
Locality Name (eg, city) [VLC]:
Organization Name (eg, company) [Local Lab OpenVPN]:
Organizational Unit Name (eg, section) [LocalLab]:
Common Name (eg, your name or your server's hostname) [vpn01]:vpn01.local.lab
Name [OpenVPM]:
Email Address [vmarti@local.lab]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ES'
stateOrProvinceName   :PRINTABLE:'VLC'
localityName          :PRINTABLE:'VLC'
organizationName      :PRINTABLE:'Local Lab OpenVPN'
organizationalUnitName:PRINTABLE:'LocalLab'
commonName            :PRINTABLE:'vpn01.local.lab'
name                  :PRINTABLE:'OpenVPM'
emailAddress          :IA5STRING:'vmarti@local.lab'
Certificate is to be certified until May 31 11:12:34 2026 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Tot seguit crearem el certificat Diffie-Hellman que ens servirà per a transmetre de manera segura informació per un canal insegur:

./build-dh

```
root@vpn01:/etc/openvpn/easy-rsa# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....................................................................
....+.....................................................................
....+.............+.....................................................
...++*++*
root@vpn01:/etc/openvpn/easy-rsa#
```

Per a finalitzar amb la creació dels certificats, crearem els certificat de client que utilitzarem per a connectar al nostre servidor VPN des del nostre ordinador:

./build-key client01

```
root@vpn01:/etc/openvpn/easy-rsa# ./build-key client01
Generating a 2048 bit RSA private key
.................................................+++
.....................................................................................................
writing new private key to 'client01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [VLC]:
Locality Name (eg, city) [VLC]:
Organization Name (eg, company) [Local Lab OpenVPN]:
Organizational Unit Name (eg, section) [LocalLab]:
Common Name (eg, your name or your server's hostname) [client01]:
Name [OpenVPM]:
Email Address [vmarti@local.lab]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ES'
stateOrProvinceName   :PRINTABLE:'VLC'
localityName          :PRINTABLE:'VLC'
organizationName      :PRINTABLE:'Local Lab OpenVPN'
organizationalUnitName:PRINTABLE:'LocalLab'
commonName            :PRINTABLE:'client01'
name                  :PRINTABLE:'OpenVPM'
emailAddress          :IA5STRING:'vmarti@local.lab'
Certificate is to be certified until May 31 11:21:39 2026 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@vpn01:/etc/openvpn/easy-rsa#
```

Ara és moment de crear l'arxiu de configuració /etc/openvpn/server.conf. A la imatge es mostra una configuració bàsica

```
ca ca.crt
cert vpn01.crt
key vpn01.key
dh dh2048.pem

dev tun0
server 192.168.2.0 255.255.255.0

push "route 192.168.1.0 255.255.255.0"

push "dhcp-option DOMAIN local.lab"
push "dhcp-option DNS 192.168.1.1"

keepalive 10 120

log openvpn.log

comp-lzo

push "redirect gateway def1 bypass-dhcp"
```

Per a que OpenVPN puga servir de servidor DNS als clients editarem l'arxiu **/etc/dnsmasq.conf** i descomentarem esborrant el signe # de davant dels paràmetres **listen-address i bind-interfaces.** Modificaren el valor de **listen-address** tal i com es mostra a la imatge:

```
# you use this.)
listen-address=127.0.0.1,192.168.1.41
# If you want dnsmasq to provide only DNS s
# configure it as shown above, and then use
```

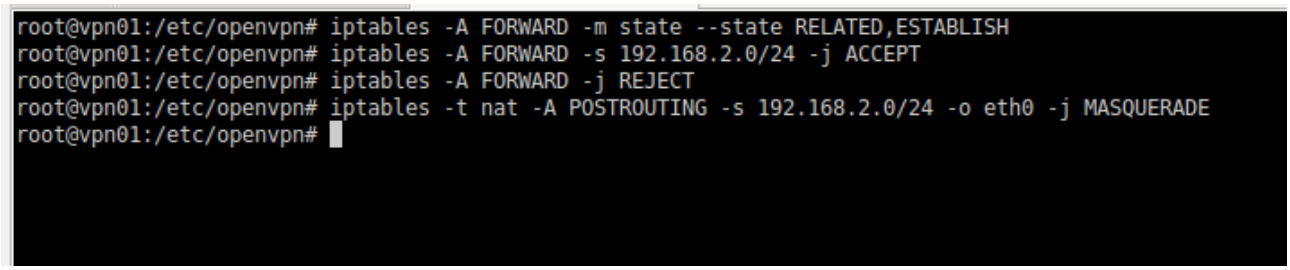
Per habilitar que OpenVPN puga enrutar els seus clients seguirem els següents:

- Executar la instrucció ***echo «1» > /proc/sys/net/ipv4/ip_forward***
- Editar l'arxiu /etc/sysctl.conf i descomentar el paràmetre ***net.ipv4.ip_forward=1***

```
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
```

Per últim afegirem les següents regles d'iptables. Al exemple, utilitzen la xarxa 192.168.2.0/24 com a xarxa per als clients VPN i eth0 és l'interfície connectada a Internet del nostre servidor. Adaptar aquests valors a cada cas.

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 192.168.2.0/24 -j ACCEPT
iptables -A FORWARD -j REJECT
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE



Ara que el servidor està correctament configurant reiniciarem el servei openvpn i el servei dnsmasq per a que s'apliquen els últims canvis:

service openvpn restart
service dnsmasq restart

Configuració del client VPN

Per a comprovar que la instal·lació del nostre servidor ha sigut satisfactòria, configurarem el nostre ordinador per poder connectar-se a OpenVPN. En primer lloc copiarem els certificats creats per al nostre ordinador amb la instrucció següents després de crear el directori ovpn-client al nostre directori personal:

- Al client:

  cd /home/usuari/
  sudo mkdir ovpn-client

- Des del servidor OpenVPN (hem de tindre openssh-server instal·lat al client):

  scp ca.crt client01.crt client01.key usuari@client01:/home/usuari/ovpn-client

Tot seguit instal·larem OpenVPN al client i crearem l'arxiu de configuració del client:

sudo apt-get install openvpn
cd /home/usuari/ovpn-client
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf .

Editarem l'arxiu ***/home/usuari/ovpn-client/client.conf*** tal i com es mostra a les imatges. Si el nostre ordinador no es capaç de resoldre l'adreça del servidor VPN podem utilitzar la IP. Els noms dels certificats han de correspondre amb els creats i copiats en passos anteriors:

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote vpn01.local.lab 1194
```

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client01.crt
key client01.key

# Verify server certificate by checkin
# that the certicate has the nsCertTyp
```

Per últim només cal executar com a usuari root o amb l'ajuda de sudo des del directori **/home/usuari/ovpn-client** la instrucció ***openvpn –config client.conf*** .

Amb la instrucció ifconfig podem comprovar que s'ha creat una interfície de xarxa virtual, tun0, i que se li ha assignat una direcció IP del rang que reparteix el nostre servidor VPN.

```
tun0      Link encap:UNSPEC  direcciónHW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00-00-00
          Direc. inet:192.168.2.6  P-t-P:192.168.2.5  Másc:255.255.255.255
          ACTIVO PUNTO A PUNTO FUNCIONANDO NOARP MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:117275 errores:0 perdidos:114833 overruns:0 carrier:0
          colisiones:0 long.colaTX:100
          Bytes RX:0 (0.0 B)  TX bytes:174219961 (174.2 MB)
```

Annex X – GNU Free Documentation License

GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain

any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a

section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the

Document well before redistributing any large number of copies, to
give them a chance to provide you with an updated version of the
Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under
the conditions of sections 2 and 3 above, provided that you release
the Modified Version under precisely this License, with the Modified
Version filling the role of the Document, thus licensing distribution
and modification of the Modified Version to whoever possesses a copy
of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct
   from that of the Document, and from those of previous versions
   (which should, if there were any, be listed in the History section
   of the Document). You may use the same title as a previous version
   if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities
   responsible for authorship of the modifications in the Modified
   Version, together with at least five of the principal authors of the
   Document (all of its principal authors, if it has fewer than five),
   unless they release you from this requirement.
C. State on the Title page the name of the publisher of the
   Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications
   adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice
   giving the public permission to use the Modified Version under the
   terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections
   and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add
   to it an item stating at least the title, year, new authors, and
   publisher of the Modified Version as given on the Title Page. If
   there is no section Entitled "History" in the Document, create one
   stating the title, year, authors, and publisher of the Document as
   given on its Title Page, then add an item describing the Modified
   Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for
   public access to a Transparent copy of the Document, and likewise
   the network locations given in the Document for previous versions
   it was based on. These may be placed in the "History" section.
   You may omit a network location for a work that was published at
   least four years before the Document itself, or if the original
   publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications",
   Preserve the Title of the section, and preserve in the section all
   the substance and tone of each of the contributor acknowledgements
   and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document,
   unaltered in their text and in their titles. Section numbers
   or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section
   may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements"
   or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document

except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (c) YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.