I.E.S CLARA DEL REY
CONSEJERIA DE EDUCACION
Comunidad de Madrid

MEMORIA FINAL DE PROYECTO

IMPLANTAR UN DOMINIO DE USUARIOS EN UBUNTU SERVER USANDO LDAP

CICLO FORMATIVO DE GRADO SUPERIOR

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS Y REDES

AUTOR

IVÁN LOZANO FERNÁNDEZ

COORDINADOR

PABLO LEAL RUILOBA

CURSO

2020 / 2021

I.E.S CLARA DEL REY

Índice

Índice de figuras

1.Introducción

Se va a implementar con la herramienta VirutalBox dos máquinas virtuales. Se utilizará una maquina Ubuntu 20.04 que hará de servidor LDAP y se creará un árbol de directorios. También se usará un Ubuntu cliente para poder autenticar los usuarios en el servidor LDAP.

El objetivo principal de esta práctica es crear un servidor LDAP funcional en el que tenga configurado un servicio DNS y a través de él poder acceder al árbol de directorios de LDAP para poder gestionar las Unidades Organizativas, grupos y usuarios. Por otro lado, los usuarios tienen que poder autenticarse desde un cliente y acceder a su propio directorio home.

Two virtual machines will be implemented with the VirutalBox tool. An Ubuntu 20.04 machine will be used as LDAP server and a directory tree will be created. An Ubuntu client will also be used to authenticate users on the LDAP server.

The main objective of this practice is to create a functional LDAP server with a DNS service configured and through it to access the LDAP directory tree in order to manage the Organisational Units, groups and users. On the other hand, users must be able to authenticate from a client and access their own home directory.

2. Descripción del proyecto

Para realizar este proyecto se ha utilizado 2 máquinas virtuales. Una con **Ubuntu server 20.04** que contiene dos tarjetas de red: **una como adaptador puente para que el servidor resuelva los DNS y que los clientes de la red puedan acceder al exterior y otra interna para comunicarse con el cliente.**

Tiene un servicio de DNS instalado para crear el domino (asir.es) por el cual los usuarios van a acceder y el servicio **OpenLDAP** que va a permitir al administrador del sistema controlar las unidades organizativas, grupos y usuarios dentro de la red. También va a almacenar los directorios de los usuarios que estén dentro del dominio.

La otra máquina virtual que se ha implementado es un **Ubuntu Escritorio 20.04** que contiene una tarjeta de red interna para poder comunicarse con el servidor. Esta máquina permite al administrador controlar a los usuarios de forma gráfica. También se va a utilizar para permitir a los usuarios autenticarse con su cuenta del domino y así darles acceso a iniciar sesión desde cualquier equipo que este dentro de la red para que puedan acceder a su directorio personal ya que esta almacenado en la máquina de Ubuntu Server.

3. ¿Qué es un servidor LDAP? ¿Para qué sirve?

LDAP (Lightweight Directory Access Protocol o en español **Protocolo Ligero de Acceso a Directorio**) es un servicio de directorio. Se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. **Este protocolo se utiliza a nivel de aplicación** para acceder a los servicios de directorio remoto.

LDAP aparece muchas veces asociado a Active Directory, un sistema de Windows que **gestiona el inicio de sesión de los usuarios.**

3.1 Requisitos previos

Servidor

Para crear un servidor con LDAP tiene que cumplir los siguientes requisitos**:**

- Maquina con posibilidad de usar **Ubuntu server 20.04**

- IP fija en este caso será 192.168.15.1

- DNS configurado en este caso será asir.es

Cliente

Para unir un cliente al servidor LDAP tiene que cumplir los siguientes requisitos**:**

- Maquina con posibilidad de usar **Ubuntu Cliente 20.04**

- DNS apuntando al servidor

3.2 Funcionamiento

El funcionamiento de acceso y administración es muy similar a Active Directory de Windows. Cuando el cliente LDAP se conecta con el servidor, podrá realizar dos acciones básicas, bien consultar y obtener información del directorio, o modificarla.

- Si un cliente consulta la información el servidor LDAP puede conectarla directamente si tienen un directorio alojado en él, o bien redirigir la solicitud hasta otro servidor que efectivamente tenga esta información. Este podrá ser local, o remoto.

- Si un cliente quiere modificar la información del directorio, el servidor comprobará si el usuario que está accediendo a este directorio tiene permisos de administrador o no. Entonces, la información y gestión de un directorio LDAP se podrá hacer de forma remota.

El **puerto de conexión** para el protocolo LDAP es el **TCP 389,** aunque por supuesto, se podrá modificar por el usuario y establecerlo en el que desee si así se lo indica al servidor.

3.3 Estructura de directorios

Los datos LDAP son estructurados y jerárquicos. La estructura es definida por «esquemas» («schemas») que describen el tipo de objetos que la base de datos puede almacenar junto con una lista de todos sus atributos posibles. La sintaxis utilizada para hacer referencia a un objeto particular en la base de datos está basada en esta estructura, lo que explica su complejidad.

Los servidores de directorio LDAP almacenan su información jerárquicamente, no distinto a un sistema de ficheros UNIX. La jerarquía provee de un método para agrupamiento (y subagrupamiento) lógico de ciertos items juntos. Estos agrupamientos pueden ser útiles en un número de situaciones:

- **Delegación de "autoridad"** para uno o más grupos de datos a otro servidor o a otro sitio (site)
- **Replicación de datos**
- **Seguridad y control de acceso**
- **Escalabilidad**

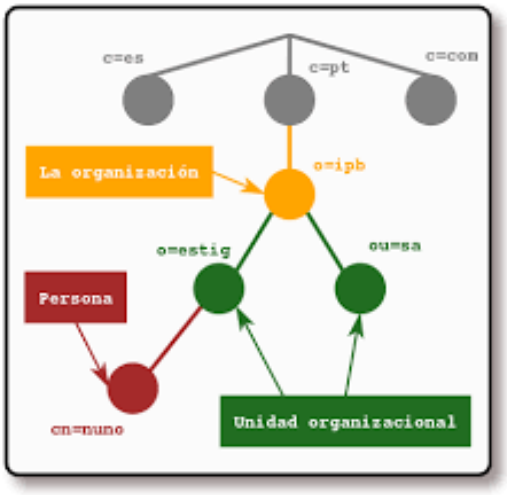


Figura 3.1 Esquema de árbol de directorios

3.4 Estructura de una URL de acceso en LDAP

Al efectuar conexiones remotas a un servidor LDAP, necesitaremos del uso de direcciones URL para obtener información de éste. La estructura básica

ldap://servidor:puerto/DN?atributos?ambito?filtros?extensiones

- **Servidor o host**: es la dirección IP o nombre de dominio del servidor LDAP

- **Puerto**: el puerto de conexión del servidor, por defecto será el 389

- **DN**: nombre distinguido para usar en la búsqueda

- **Atributos**: es una lista de campos a devolver separados por comas

- **Ámbito o scope**: es el ámbito de la búsqueda

- **Filtros**: para filtra la búsqueda según el identificador del objeto, por ejemplo.

- **Extensiones**: serán las cadenas de caracteres extensiones de la URL en LDAP.

Por ejemplo:

ldap://asir.es/cn=Ivan,dc=asir,cd=es

Estamos buscando todos los usuarios que haya en la entrada de Ivan en asir.es.

Además de esta notación, también tendremos una versión de LADP con certificado de seguridad SSL, cuyo identificador para la URL será “ldaps:”.

3.5 Ventajas y desventajas de un servidor LDAP

Ventajas

- Muy rápido en la lectura de registros.

- Permite replicar el servidor de forma muy sencilla y económica.

- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente.

- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.

- Usa un sistema jerárquico de almacenamiento de información.

- Permite múltiples directorios independientes.

- Funciona sobre TCP/IP y SSL.

- La mayoría de aplicaciones disponen de soporte para LDAP.

- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

Desventajas

- Debe de existir un servidor de réplica sino al caer el servidor cae el sistema.

- No tiene una interfaz de administración por defecto.

- El control de los usuarios no es muy bueno ya que no cuenta con un sistema dedicado al control de usuarios.

- Complicado de configurar ya que es un sistema complejo

3.6 Otras alternativas a LDAP

Active Directory: es un almacén de datos de directorio con licencia Microsoft e implementado en sus sistemas operativos server desde Windows 2000. Realmente bajo la estructura de Active Directory se encuentra un esquema LDAPv3, por lo que también es compatible con otros sistemas que implemente este protocolo en sus directorios.

Red Hat Directory Server: es un servidor que también se basa en LDAP similar a Active Directory, pero mediante una herramienta de código abierto. Dentro de este directorio podremos almacenar objetos como usuarios claves, grupos, políticas de permisos, etc.

Apache Directory Server: otra de las grandes implementaciones que utilizan LDAP es el directorio con licencia de Apache Software. Además, implementa otros protocolos como Kerberos y NTP y cuenta con una interfaz de vistas propias de las bases de datos relacionales.

Novell Directory Services: este es el servidor de directorio propio de Novell para gestionar el acceso a un almacén de recursos en uno o varios servidores conectados en red. Se compone de una estructura de base de datos jerárquica orientada a objetos en la que se almacenan todos los objetivos típicos de los directorios.

Open DS: es un directorio basado en java de SUN Microsystems, que posteriormente se liberaría para todos los usuarios. Está desarrollado en JAVA el necesitaremos el paquete Java Runtime Environmet para que éste funcione.

4.Creación del laboratorio

4.1 Instalación y configuración de Ubuntu Servidor

Primero tenemos que crear las máquinas virtuales. Para ello vamos a Virtual Box y añadimos una nueva máquina. Creamos una para Ubuntu server con 2 GB de RAM, 15 GB de disco duro, le asignamos el adaptador de red 1 a modo puente y el adaptador de red 2 a red interna.

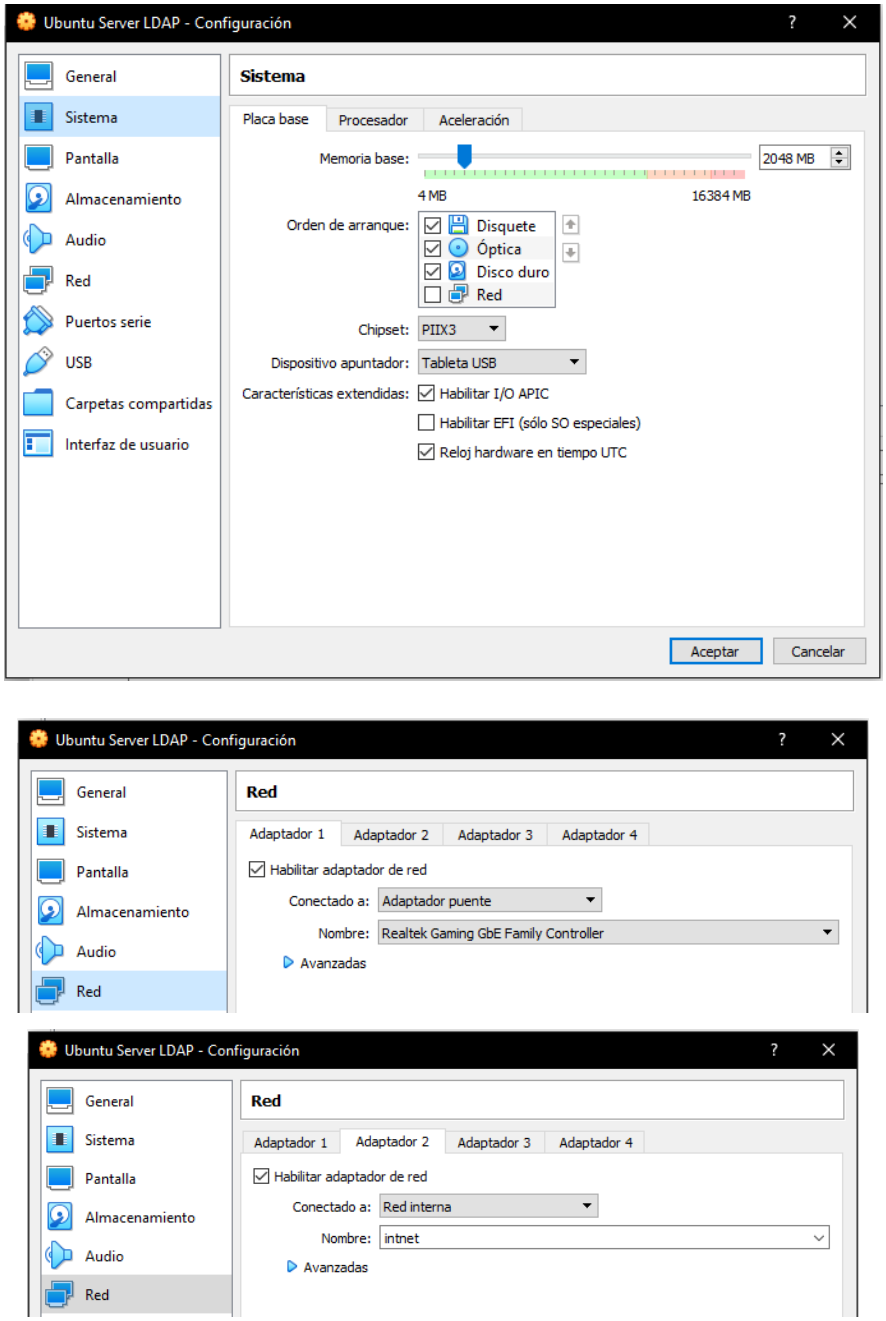
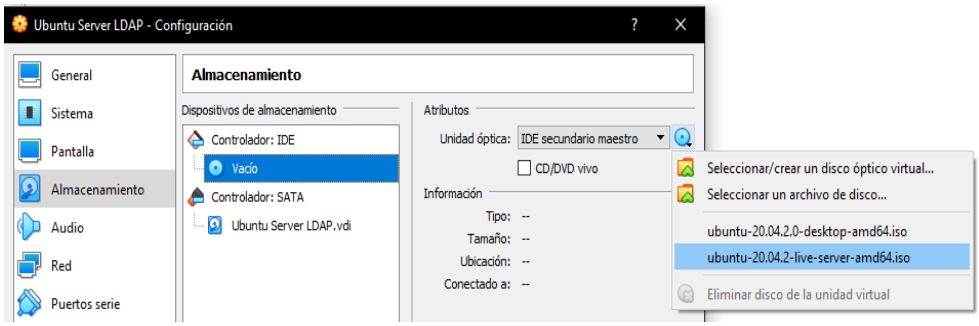


Figura 4.1. Configuración de tarjetas Ubuntu Server

Acto seguido instalaremos Ubuntu server en la maquina creada. Introducimos el archivo ISO en el apartado de almacenamiento, pulsamos en el icono del CD y la añadimos. Cuando ya este añadido iniciamos la maquina y procedemos a instalar. Primero seleccionamos nuestro idioma.



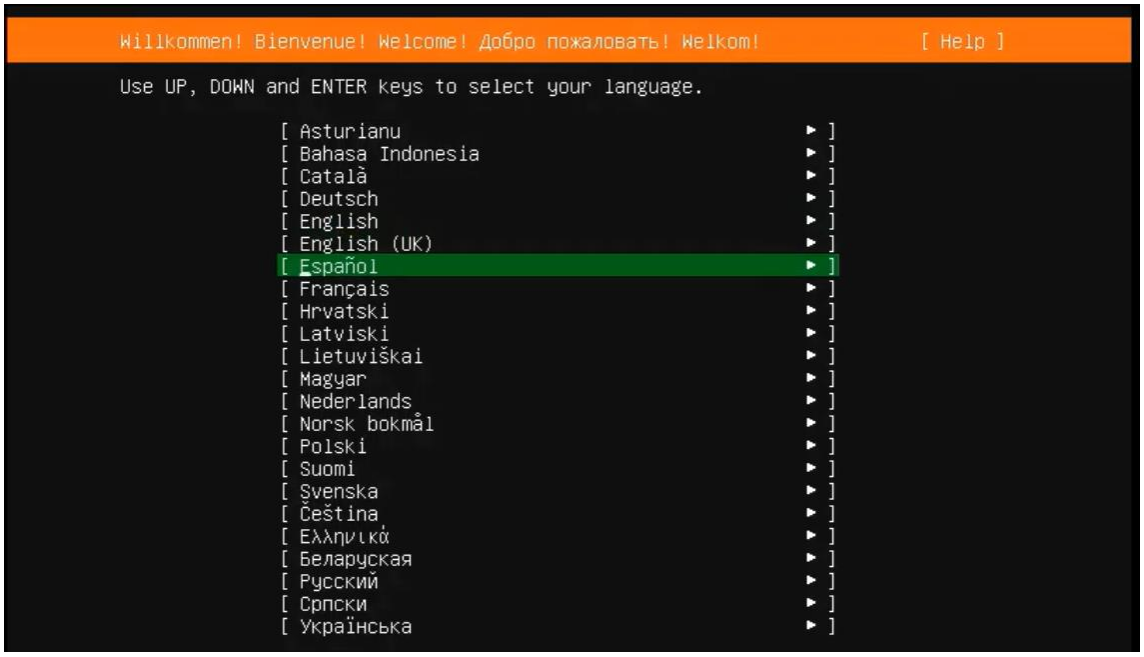


Figura 4.2. Selección de idioma en Ubuntu Server

Continuamos sin actualizar y seleccionamos el tipo de teclado.

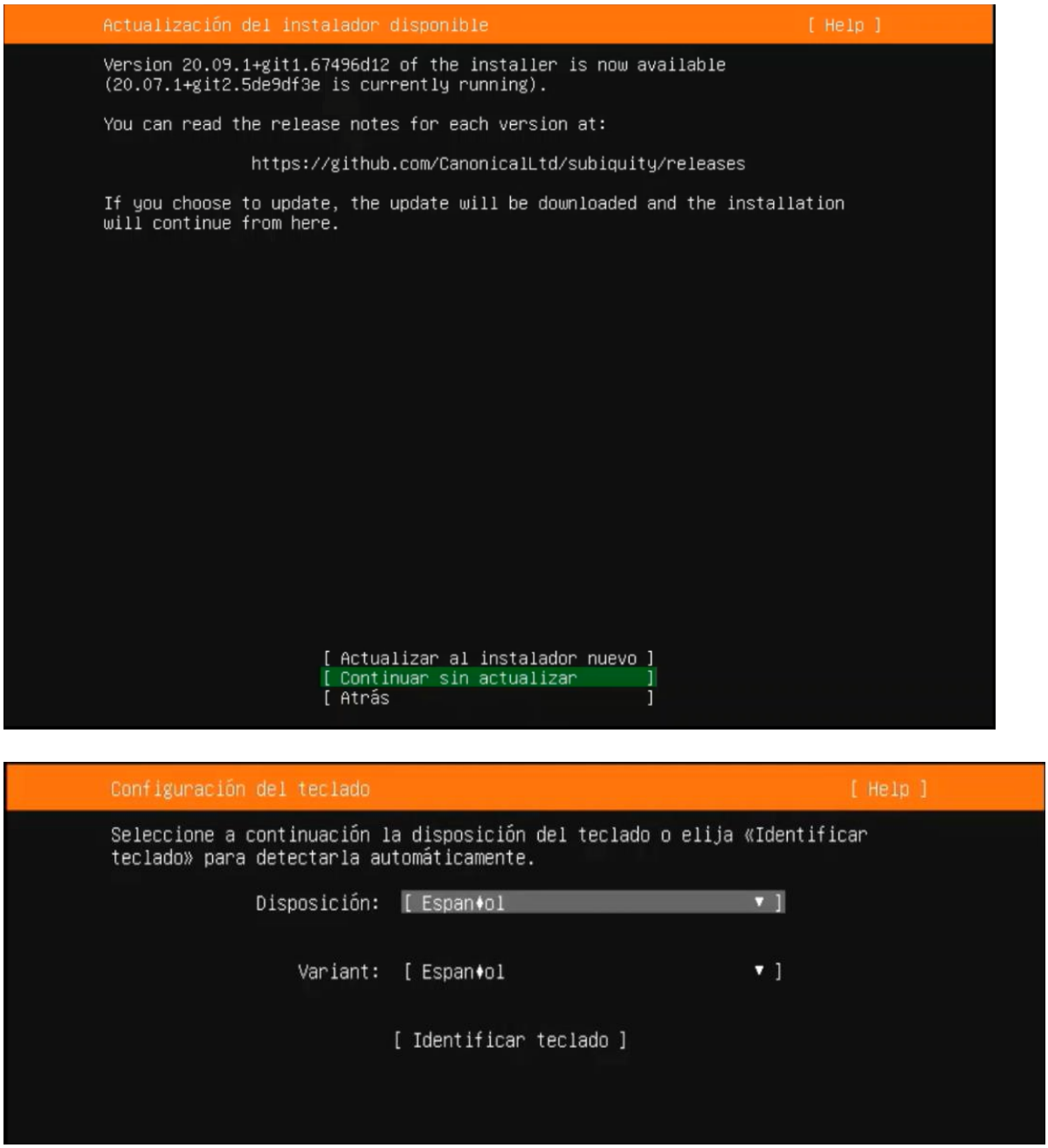
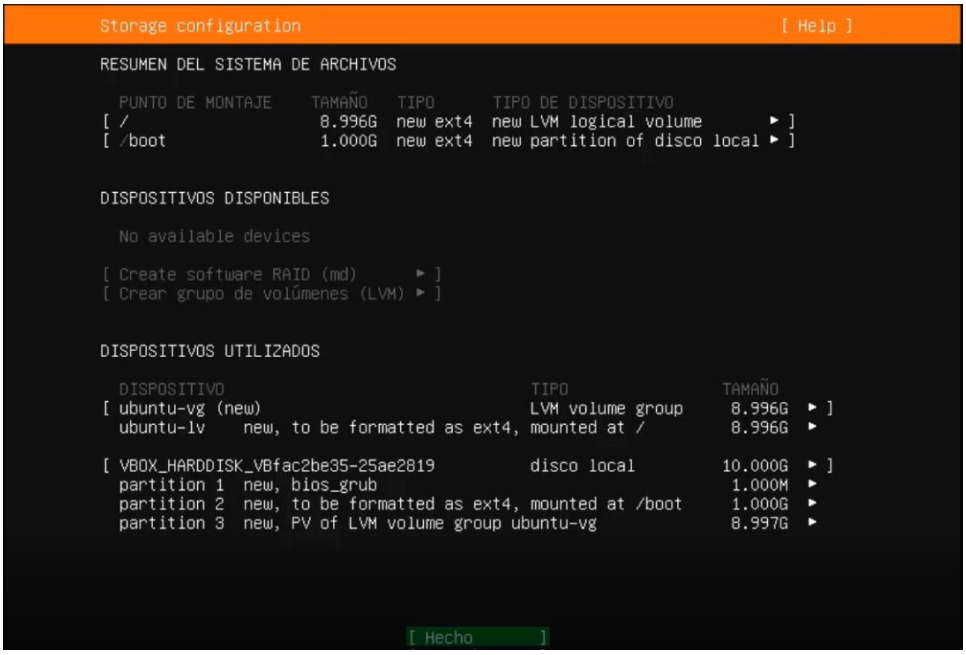


Figura 4.3. Actualización y selección de tipo de teclado

En este apartado seleccionamos que use el disco entero. Configuramos el nombre del servidor y el usuario administrador de la máquina. Cuando los hayamos creado comenzara la instalación del sistema.



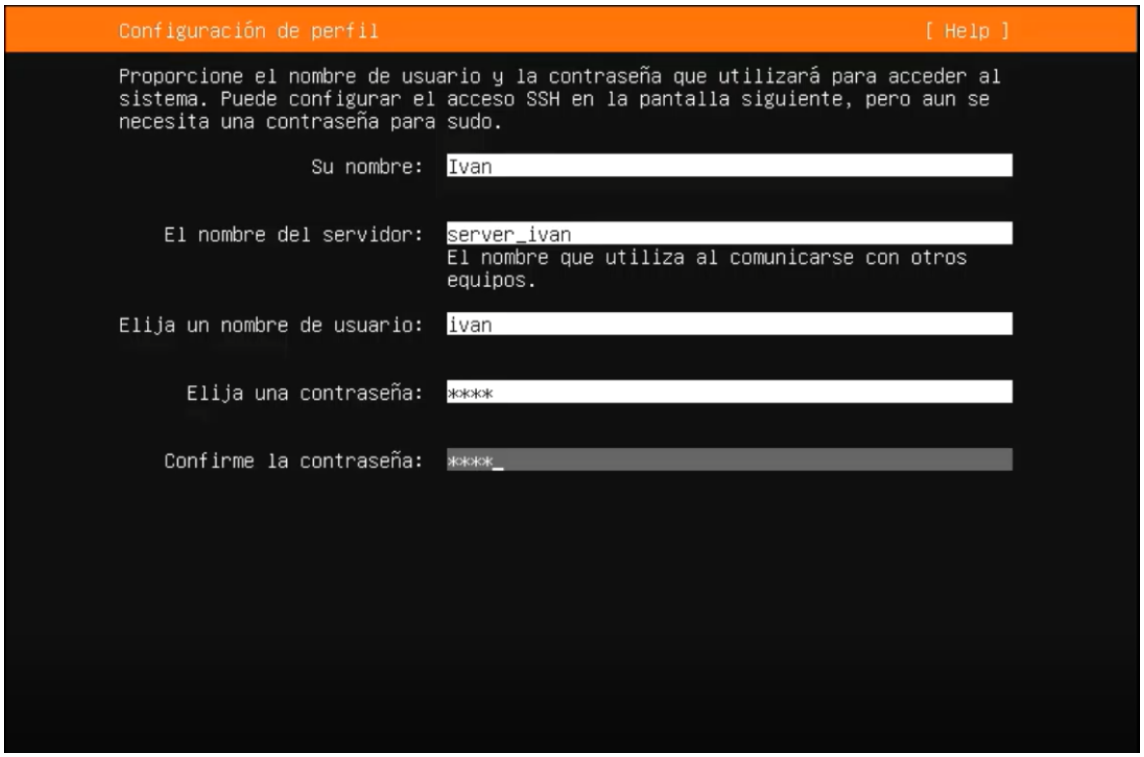


Figura 4.4. Particionado del disco duro y creación de usuario admin

4.1.1 Configurar interfaces en el servidor

Para configurar las interfaces en Ubuntu tenemos que modificar el archivo que contiene la configuración de interfaces. Con el siguiente comando nos situaremos en el archivo para modificarlo.

comando: ***sudo nano /etc/netplan/00-installer-config.yaml***

Lo configuramos como en la siguiente imagen:

PD: Tiene que estar tal y como en la imagen. Si hay algún espacio mal no funciona.

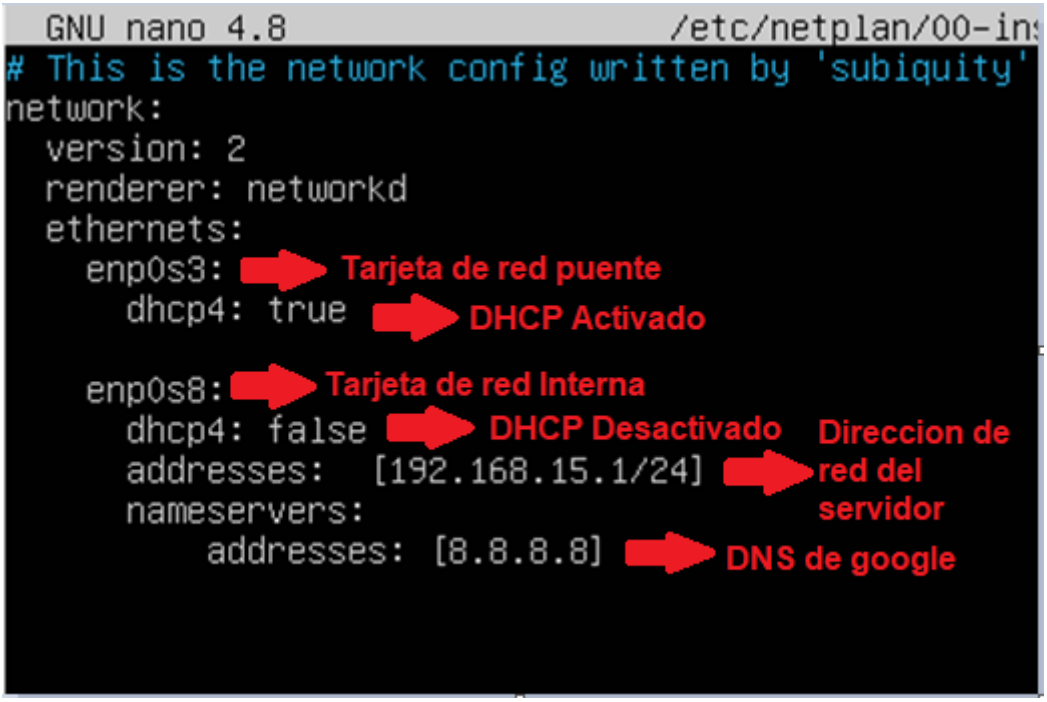


Figura 4.5. Configuración de interfaz servidor

Cuando estén configuradas como en la imagen guardamos el archivo con **ctrl+o** y salimos de el con **ctrl+x** e introducimos el siguiente comando para verificar que están configuradas correctamente.

Comando: ***netplan apply***

Si por algún casual está mal configurado saldrá un mensaje diciendo donde está el error situado.

4.1.2 Cambiar el nombre del servidor

Ahora vamos a identificar el servidor junto con el dominio que vamos a crear posteriormente. Introducimos el comando ***sudo nano /etc/hosts*** y añadimos la siguiente línea:

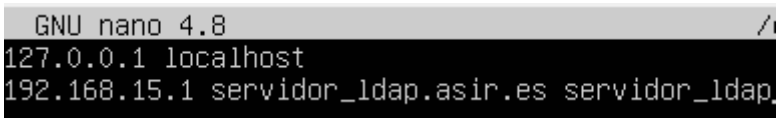


Figura 4.6. Cámbio de nombre al servidor

192.168.15.1 → IP del servidor

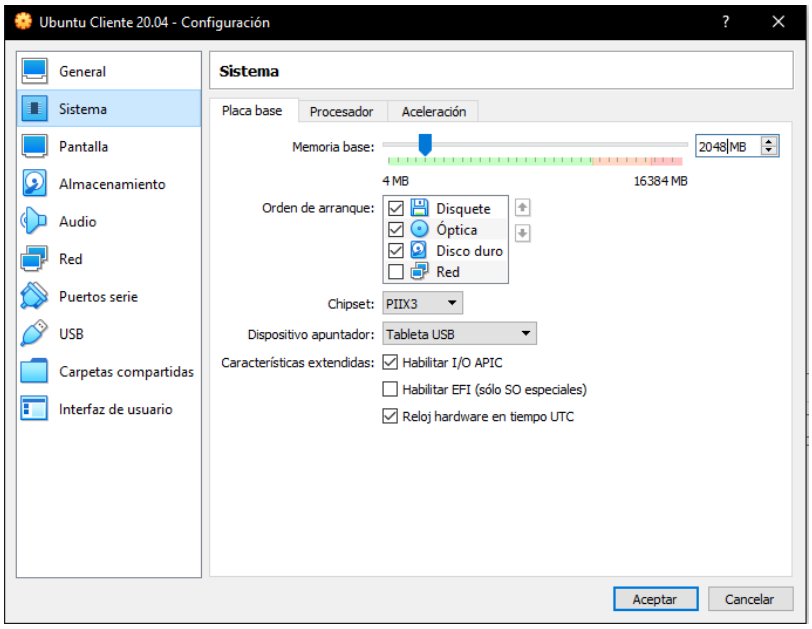
Servidor_ldap.asir.es → Nombre del servidor + dominio de la red que vamos a usar

Servidor_ldap → Nombre del servidor

Cuando estén configuradas como en la imagen guardamos el archivo con **ctrl+o** y salimos de el con **ctrl+x.**

4.2 Instalación y configuración de Ubuntu Cliente

Para crear la de Ubuntu server repetimos el mismo proceso, vamos a Virtual Box y añadimos una nueva máquina. Le asignamos 2 GB de RAM, 15 GB de disco duro y le asignamos el adaptador de red a red interna para que se pueda comunicar con el servidor



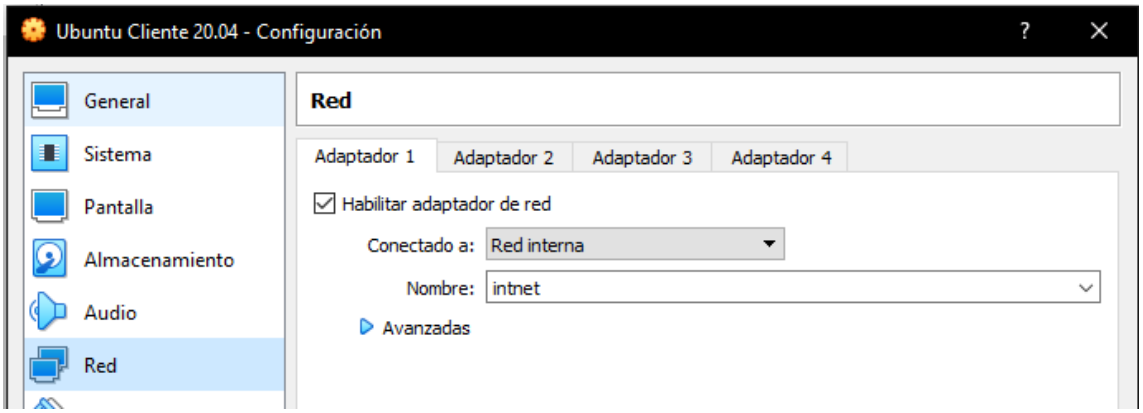


Figura 4.7. Configuración de tarjeta Ubuntu Cliente

Introducimos el archivo ISO en el apartado de almacenamiento, pulsamos en el icono del CD y la añadimos. Iniciamos la maquina y comenzara la instalación del sistema. Seleccionamos un idioma y le damos a instalar

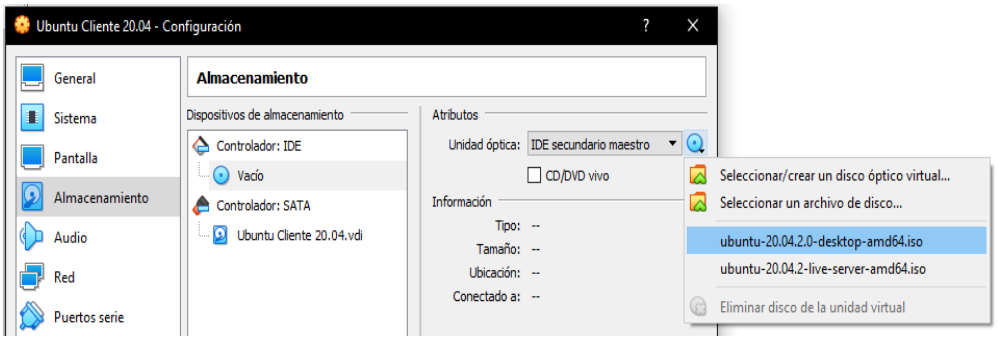


Figura 4. 8.Instalación de Ubutnu Cliente

Seleccionamos el tipo de teclado que vamos a usar, seleccionamos instalación normal y pulsamos siguiente. En la siguiente ventana dejamos marcada la opción de “Borrar disco e instalar Ubuntu” y pulsamos Instalar.

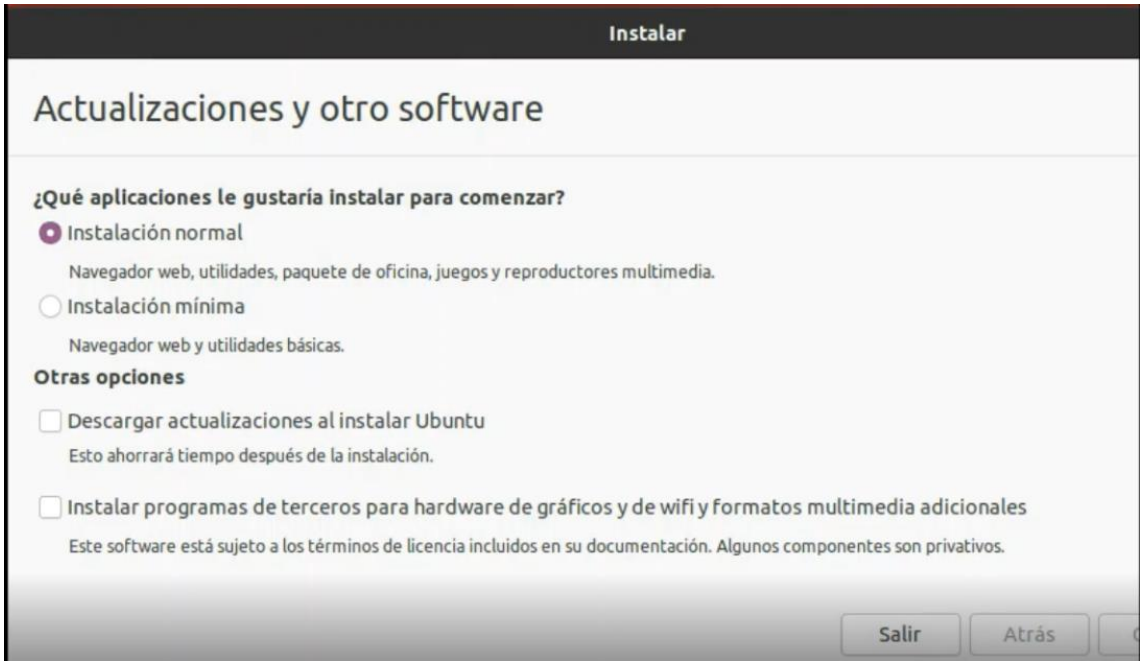


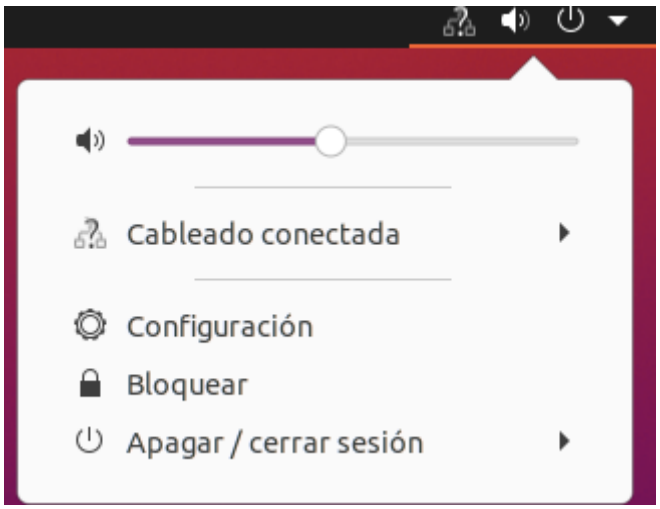
Figura 4.9. Tipo de instalación y particionado

Rellenamos los campos del usuario administrador y comenzara la instalación. Después de que se instale el sistema, retiramos el disco y pulsamos enter.

Figura 4.10. Creación de usuario admin

4.2.1 Configuración de interfaz Cliente

Nos dirigimos al apartado de ajustes en la barra de tareas de Ubuntu, pulsamos configuración. Después vamos al apartado de Cableado y pulsamos el engranaje.



Configuramos la tarjeta como en la siguiente imagen.

Figura 4.11. Panel de red y configuración de tarjeta

Cuando hayamos terminado apagamos y encendemos la interfaz para que se apliquen los cambios.

Figura 4.12. Configuración de interfaz Ubuntu Cliente

4.3 Creación del dominio

4.3.1 Instalación del servicio de dominio

Para crear el dominio primero debemos instalar el servicio **bind9** en nuestro servidor con los siguientes comandos:

sudo apt update → Actualiza los repositorios

sudo nano apt-install bind9 → Instala el servicio bind9

Cuando se haya instalado se creará un directorio nuevo en **/etc/bind** donde se encontrará todo lo relacionado con la configuración del servicio.

Nos situamos en el archivo **named.conf.options** con el siguiente comando: ***sudo nano /etc/bind/named.conf.options***

Ahora vamos a cambiar los **forwarders** del servidor DNS a los de Google **8.8.8.8** para que en el caso de que no encuentre una dirección la pueda consultar. Cuando se haya modificado guardamos y salimos del archivo.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        // 0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

```
forwarders {
   8.8.8.8;
};
```

Figura 4. 13. Cambio de forwarders

Después pasaremos a editar el archivo con el comando ***sudo nano /etc/bind/named.conf.local***. En este archivo especificaremos las zonas de búsqueda directa e inversa del servicio DNS. El dominio de nuestra zona directa y la subred de la zona inversa. También tendremos que incluir qué tipo de servicio es (maestro o esclavo) y en que archivos hará la búsqueda de nombres.

Modificaremos el archivo como en la siguiente imagen:

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

//ZONA DIRECTA
zone "asir.es"{
     type master;
     file "/etc/bind/db.asir";
};

//ZONA INVERSA
zone "15.168.192.in-addr.arpa" {
      type master;
      file "/etc/bind/db.192";
      notify yes;
};
```

Figura 4.14. Creación de Zonas en DNS

Cuando hayamos terminado de modificar el archivo guardamos y salimos. Con el comando ***named-checkconf*** se puede comprobar que no hay ningún error de sintaxis en el fichero.

4.3.2 Configuración de tablas de búsqueda directa DNS

Ahora vamos a crear el archivo que contiene los datos de la zona directa. Para no tener que escribir el archivo desde cero, copiamos el archivo **db.127** y lo copiamos al archivo **db.asir** con el comando ***sudo cp db.127 db.asir***. Cuando este copiado lo modificamos con el comando ***sudo nano /etc/bind/asir.db***

El archivo de la zona directa contiene las tablas de búsqueda directa.

Las primeras líneas son unos parámetros relacionados con la actualización del DNS (número de serie y periodos de actuación).

La siguiente línea indica quién es el servidor primario (NS = Name Server). Las siguientes líneas especifican las @IP's de los diferentes PC's componentes del dominio. Hay otros hosts A y alias de los nombres www y ftp en el mismo host que el servidor. En la siguiente imagen puedes ver como quedaría el fichero:

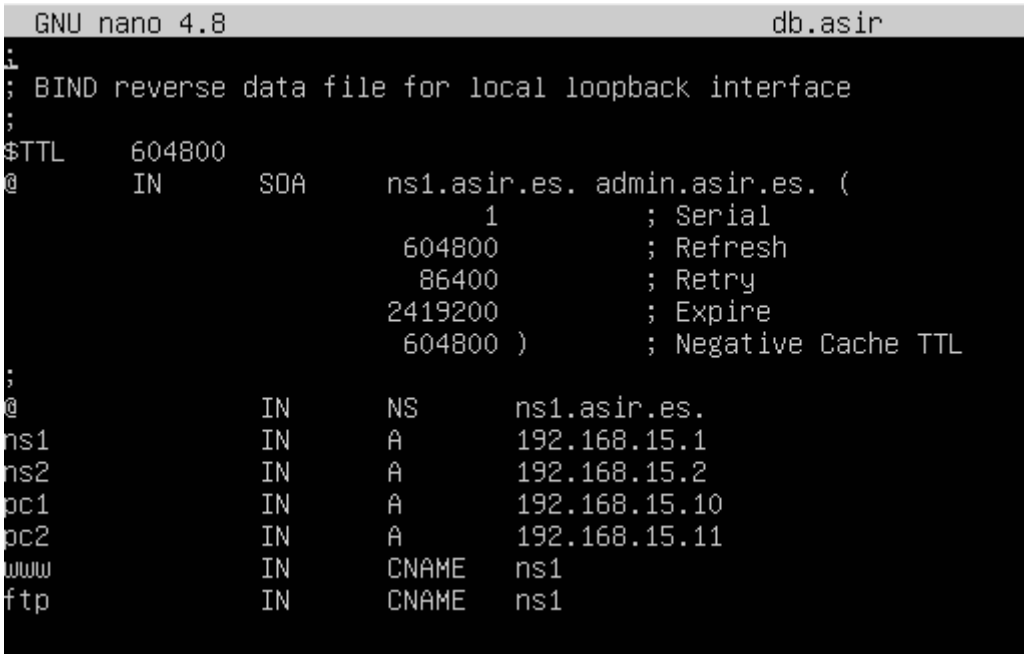


Figura 4.15. Archivo de configuración de zona directa DNS

Cuando hayamos modificado el archivo como en la imagen guardamos y salimos.

Ahora vamos a crear y modificar la zona inversa*. Hacemos la mismo que con el anterior archivo copiamos el archivo db.127 y lo pegamos al archivo db.192.

sudo cp db.127 db.asir

Después lo modificamos como en la siguiente imagen:

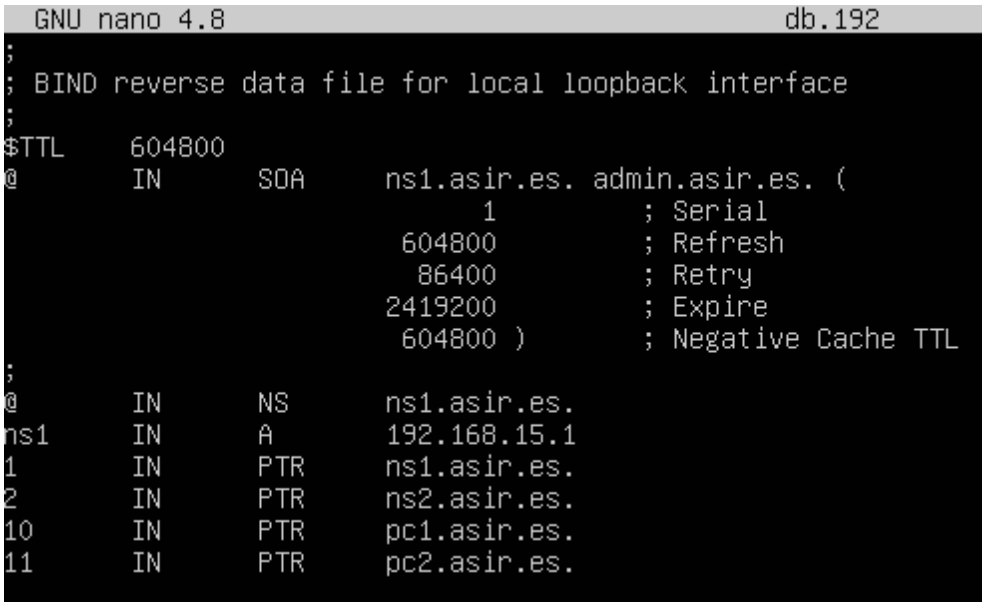


Figura 4. 16. Archivo de configuración zona inversa DNS

Cuando estén creados los dos archivos podemos comprobar si están correctamente con los siguientes comandos. En el caso que no lo estén nos saldrá un mensaje diciendo que hay un error de sintaxis.

named-checkzone asir.es /etc/bind/db.asir

named-checkzone asir.es /etc/bind/db.192

Si esta todo correctamente reiniciamos el servicio con el comando sudo ***service bind9 restart*** para que se apliquen los cambios realizados.

4.3.3 Configuración de resolvers

Por último, vamos a instalar un **resolver** ya que el que viene por defecto en Linux es más tedioso de configurar.

Lo instalamos con el comando ***sudo apt install resolvconf***

Modificamos el fichero con ***sudo nano /etc/resolvconf/resolv.conf.d/tail*** y añadimos la siguiente línea **nameserver 192.168.15.1**

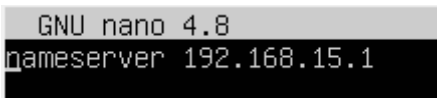


Figura 4.17. Añadir servidor al resolver

Cuando se haya seguido estos pasos reiniciamos la maquina finalmente y hacemos el comando ***service bind9 status*** para ver el estado del servidor.

Si aparece todo como en la siguiente imagen está configurado correctamente.

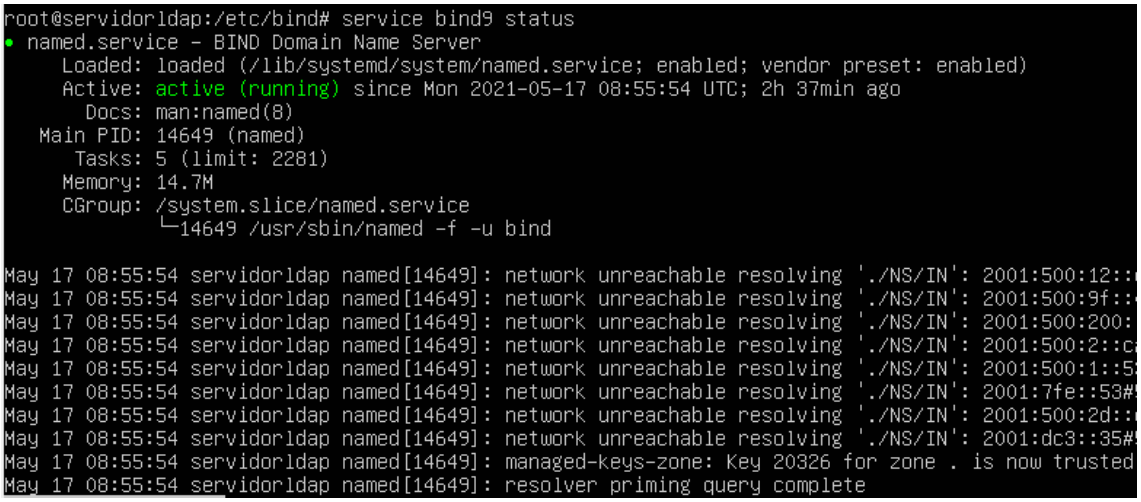


Figura 4.18. Comprobación de estado del servicio DNS

4.4 Servicio LDAP en el Servidor

4.4.1 Instalación del servicio OpenLDAP

Para instalar **OpenLDAP** en el servidor tenemos que ejecutar el comando sudo ***apt install slapd ldap-utils*** . Se abrirá un instalador en el que tenemos que asignarle el dominio, ponerle un nombre a nuestra organización y crear unas credenciales al usuario admin.

Figura 4.19. Proceso de instalación OpenLDAP

4.4.2 Configuración de archivos

Ahora vamos a modificar el archivo de configuración de LDAP con el comando ***sudo nano /etc/ldap/ldap.conf*** para añadirle nuestro dominio y la IP que va a utilizar el servidor:

```
  GNU nano 4.8                                  /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=asir,dc=es
URI     ldap://192.168.15.1:309

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

Figura 4.20. Configuración de archivo ldap.conf

Después vamos a ir al archivo de configuración que permite al servidor compartir la información con los clientes con el ***comando sudo nano /etc/nsswitch.conf***.Lo configuramos de la siguiente manera

```
passwd:         compat  systemd ldap
group:          compat  systemd ldap
shadow:         compat
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Figura 4.21. Configuración de archivo nsswitch.conf

4.4.3 Instalación de apartado grafico para gestionar usuarios

Para configurar que podamos gestionar los usuarios de forma gráfica tenemos que realizar el siguiente comando ***sudo apt install phpldapadmin***.

Cuando este instalado modificamos el archivo de configuración de PHP con el comando ***sudo nano /etc/phpldapadmin/config.php*** , pulsamos ctrl + w escribimos “127” y modificamos lo siguiente:

```
$servers->setValue('server','host','192.168.15.1');
```

```
$servers->setValue('server','base',array('dc=asir,dc=es'));
```

Figura 4.22. Configuración de PHPLDAPadmin

Después vamos a **Ubuntu Cliente**, abrimos un buscador e introducimos la siguiente URL www.asir.es/phpldapadmin.

Introducimos el usuario admin y nuestro domino.

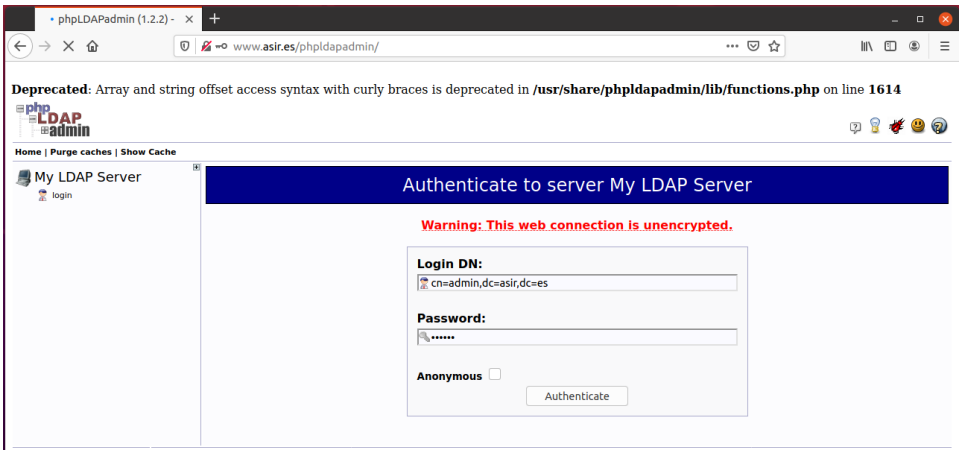


Figura 4.23. Página de inicio PHPLDAPadmin

4.4.4 Instalación OpenPAM: autenticación de usuarios

Para que los usuarios se puedan conectar al servidor y crear un directorio /home en el tenemos que instalar PAM con el siguiente comando ***sudo apt install libnss-ldap libpam-ldap***.

Se abrirá un instalador en el que le tenemos que introducir la IP del servidor LDAP, añadirle el nombre de nuestro domino, seleccionar una versión y añadirle el usuario admin y contraseña

Figura 4.24. Proceso de instalación de PAM en Ubuntu Servidor

Para que el cliente tenga permisos para crear la carpeta /home en el servidor tenemos que modificar el archivo **mkhomedir** con el comando **nano /user/share/pam-configs/mkhomedir:**

Figura 4.25. Configuración del archivo mkhomedir

Después escribimos el comando **pam-auth-update** para actualizar los cambios y seleccionamos con el espacio el apartado que pone **create home directory on login** y pulsamos enter

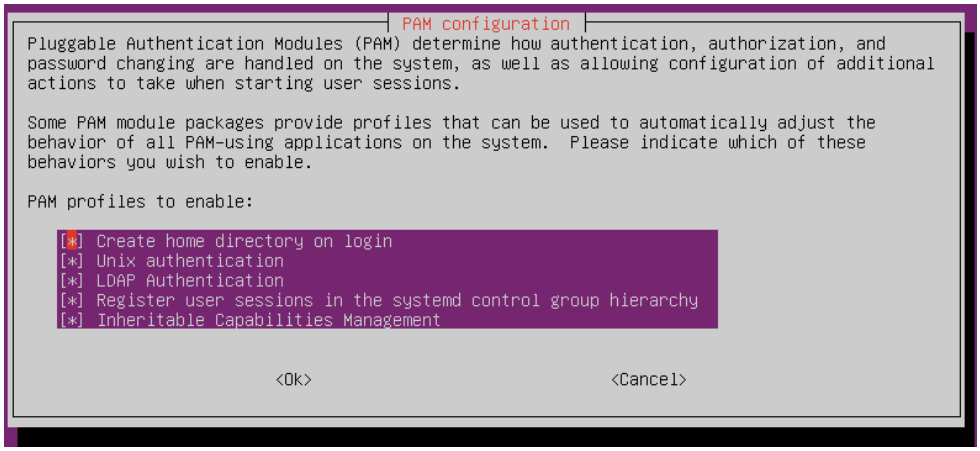


Figura 4.26. Instalación del archivo mkhomedir

Ahora vamos a permitir autorizar el inicio de sesión modificando el archivo **common-account** con el comando ***sudo nano /etc/pam.d/common-account*** e introducimos las siguientes líneas al final del archivo. Después hacemos lo mismo, pero con el archivo de sesión con el comando ***sudo nano /etc/pam.d/common-session*** y añadimos lo siguiente al final

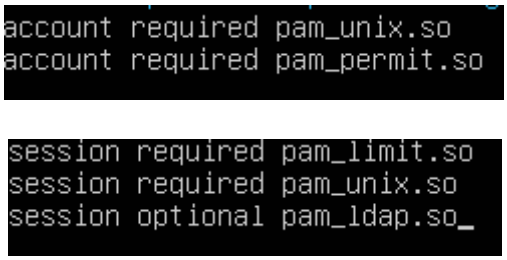


Figura 4.27. Configuración del inicio de sesion

4.5 Servicio LDAP en el cliente

4.5.1 Introducir el cliente al dominio

Primero tenemos que instalar las librerías de PAM para poder autenticar los usuarios con el comando ***sudo apt install libpam-ldap nss-updatedb libnss-db nscd ldap-utils -y***. *Se* abrirá un instalador en el que tenemos que introducir la IP del servidor LDAP, el dominio, versión y el usuario **admin** con su contraseña

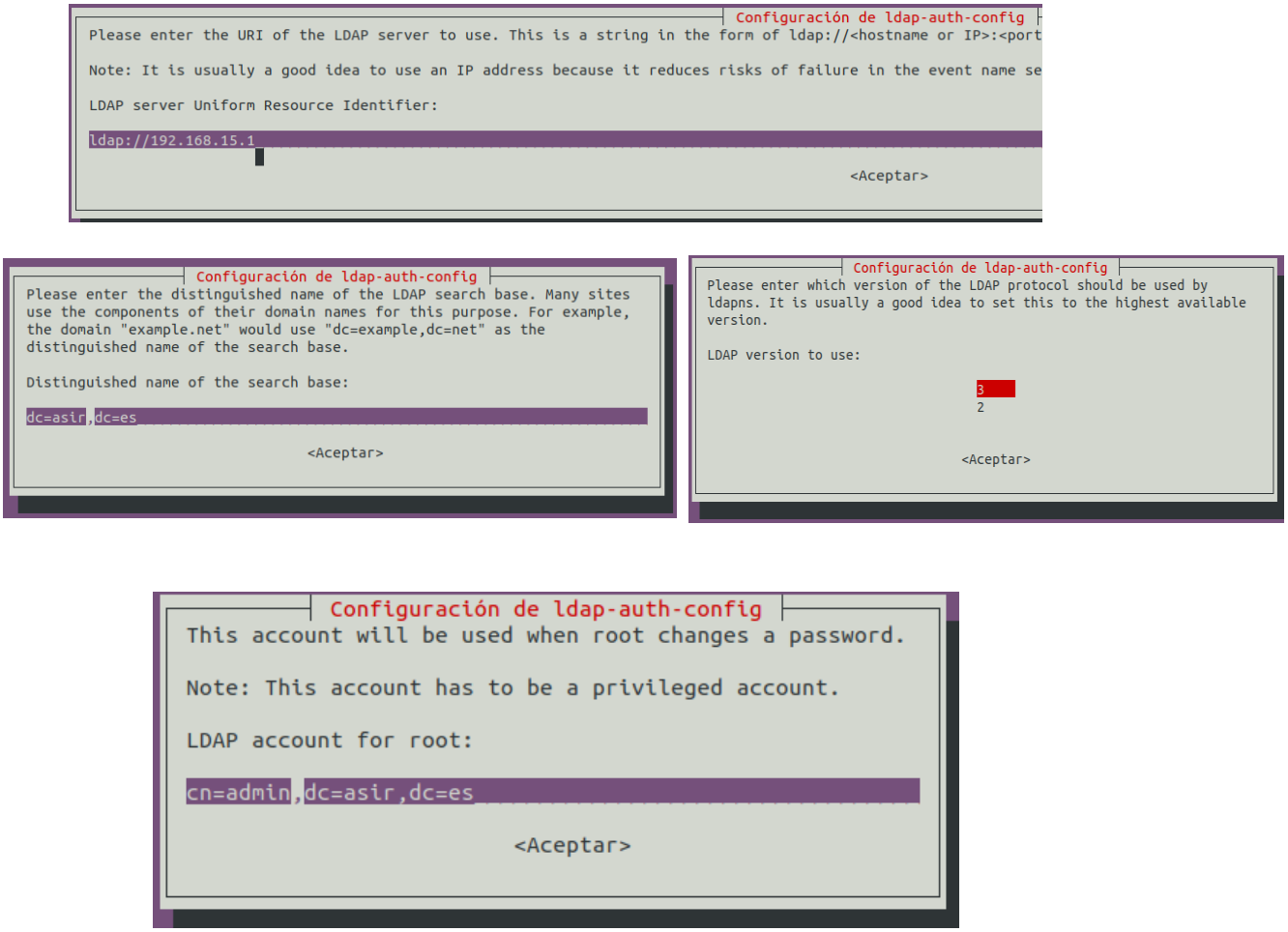


Figura 4.28. Introducción de Ubuntu cliente en el dominio

Cuando este dentro del domino se configurarán los archivos **nsswitch.conf** y **common-session** con la configuración del servidor automáticamente.

4.5.2 Creación de Unidades organizativas, grupos y usuarios

Para crear unidades organizativas, grupos y usuarios tenemos que ir en el cliente a la dirección de nuestro servidor DNS www.asir.es/phpldapadmin..

Nos saldrá una página web en la que nos pedirá un login introducimos los datos que introducimos en el apartado de Instalación de OpenLDAP.

Cuando estemos logeados nos aparecerá en la parte de la izquierda el árbol de nuestro dominio. Si pulsamos en la estrella nos dará la opción de crear varios apartados en este caso vamos a ver a como crear un árbol organizado:

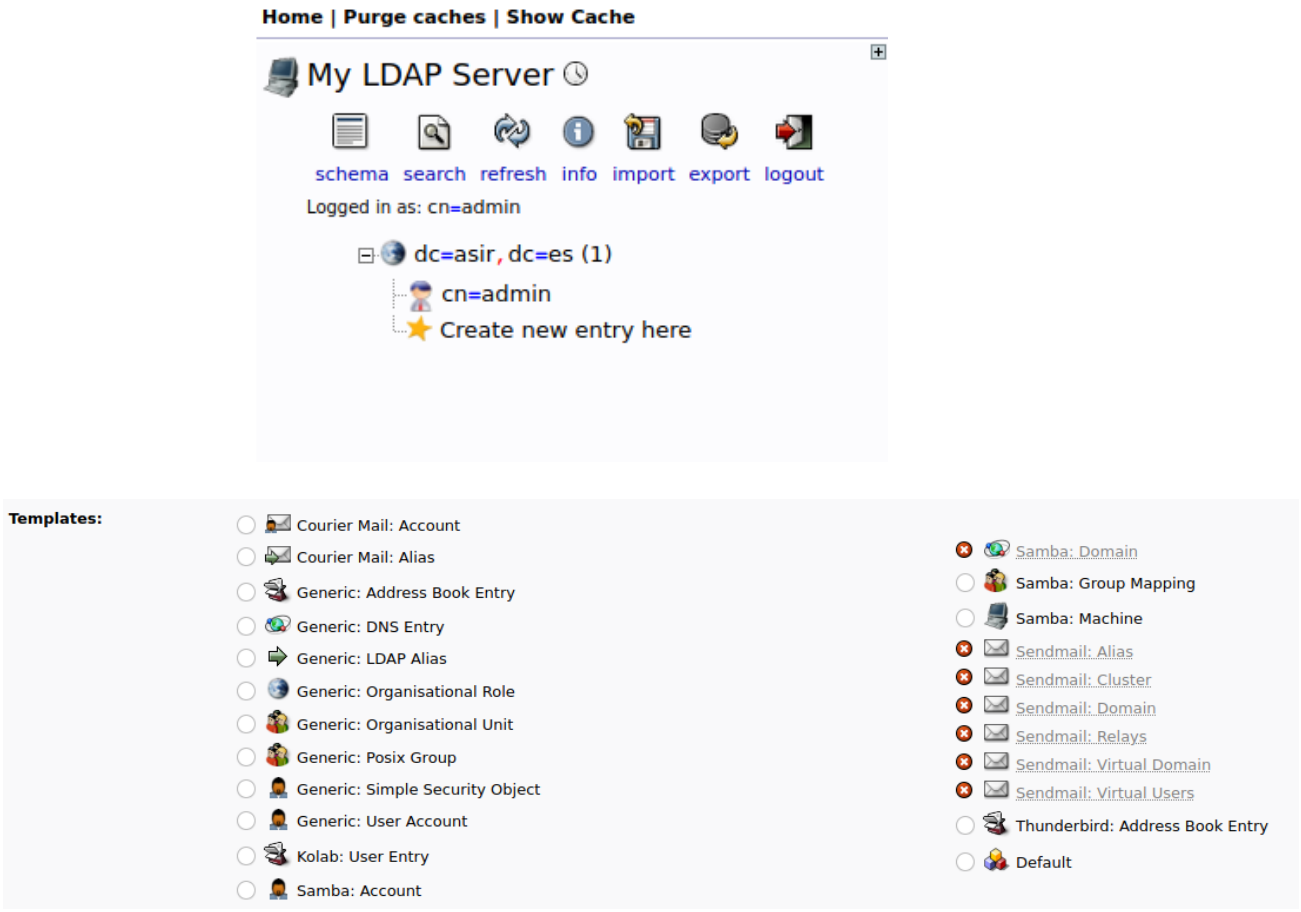


Figura 4.29. Página de creación de atributos en PHPLDAPadmin

Primero vamos a crear la unidad organizativa “Sistemas” que va a contener el grupo “Técnicos” con los usuarios “Paco” y “Pepe”. Para ello pulsamos en la opción de **Generic: Organisational Unit** y le damos un nombre en este caso Sistemas y pulsamos en el botón **Create Object.** Confirmamos que los datos están correctamente y pulsamos **commit**

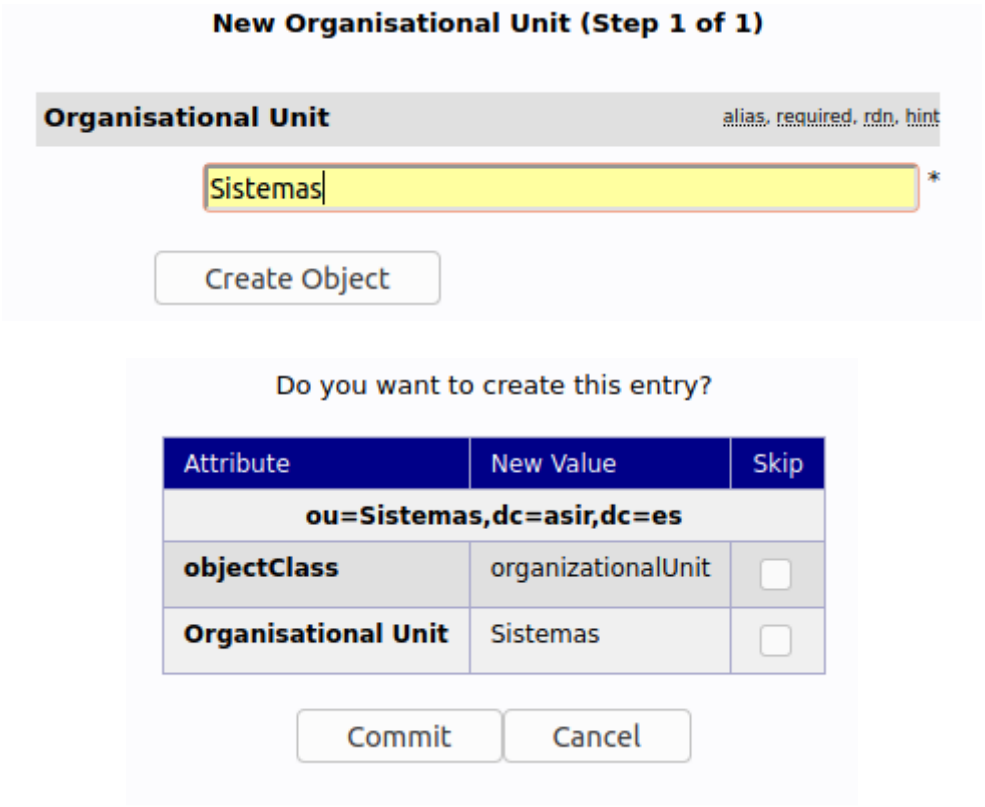
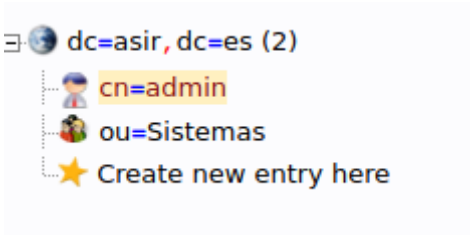
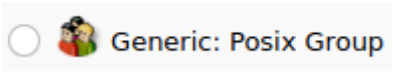


Figura 4.30. Creación de Unidad Organizativa

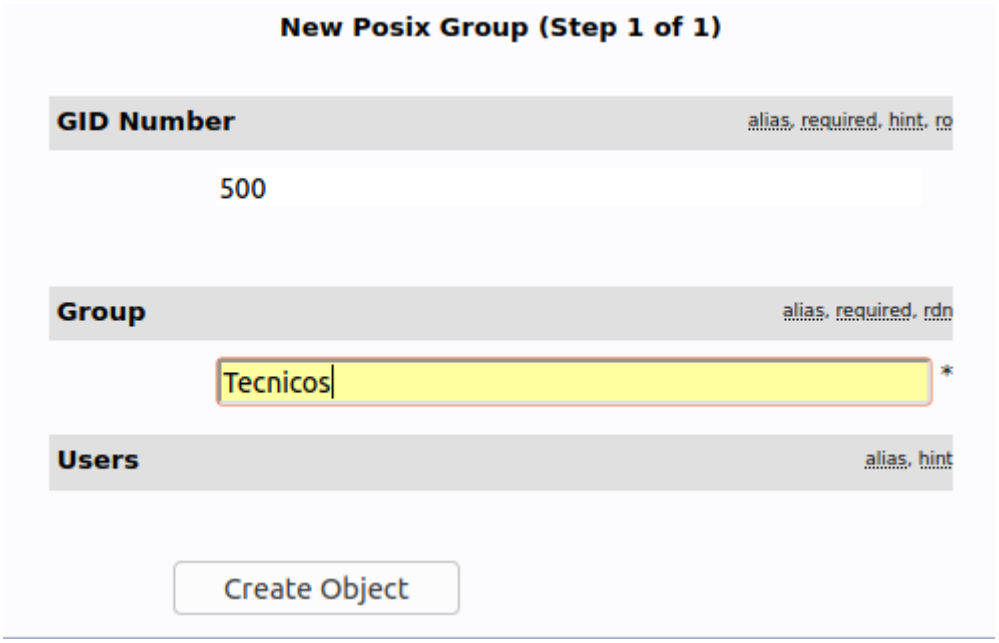
Si nos fijamos en el árbol de nuestro dominio estará creado:



Ahora vamos a crear el grupo “Técnicos”. Pulsamos en la unidad organizativa de Sistemas, pulsamos en la estrella y seleccionamos **Generic: Posix Group**



Nos asignará un GID para el grupo, seleccionamos un nombre y nos dará la opción de añadir usuarios al grupo. En este caso no nos sale usuarios porque no están creados todavía.



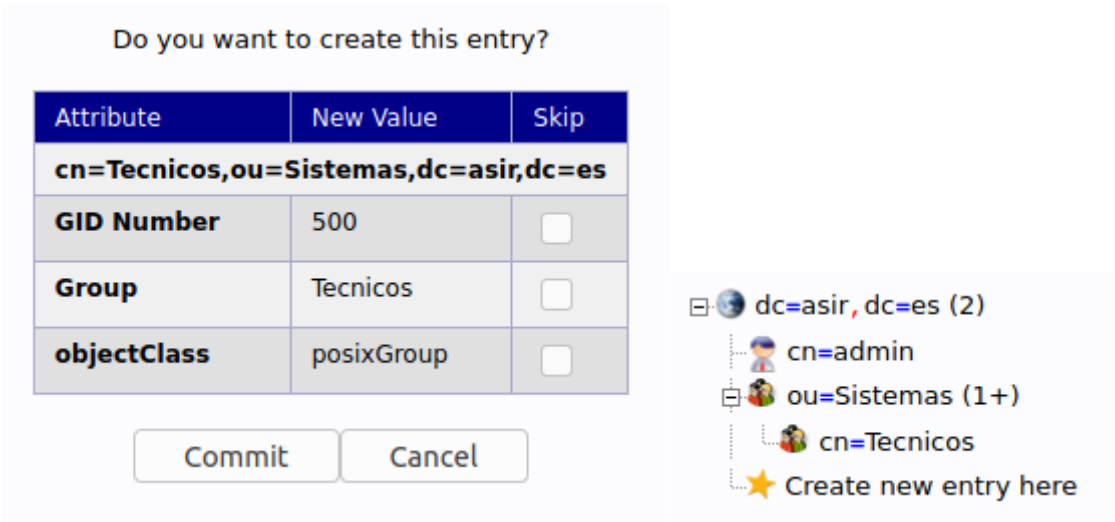


Figura 4.31. Creación de Grupo en PHPLDAPadmin

Por último, vamos a crear usuarios. Pulsamos el grupo en el árbol de dominio y pinchamos en la estrella. Seleccionamos **Generic: User Account**

Rellenamos los datos que nos piden y pulsamos en **create object**:

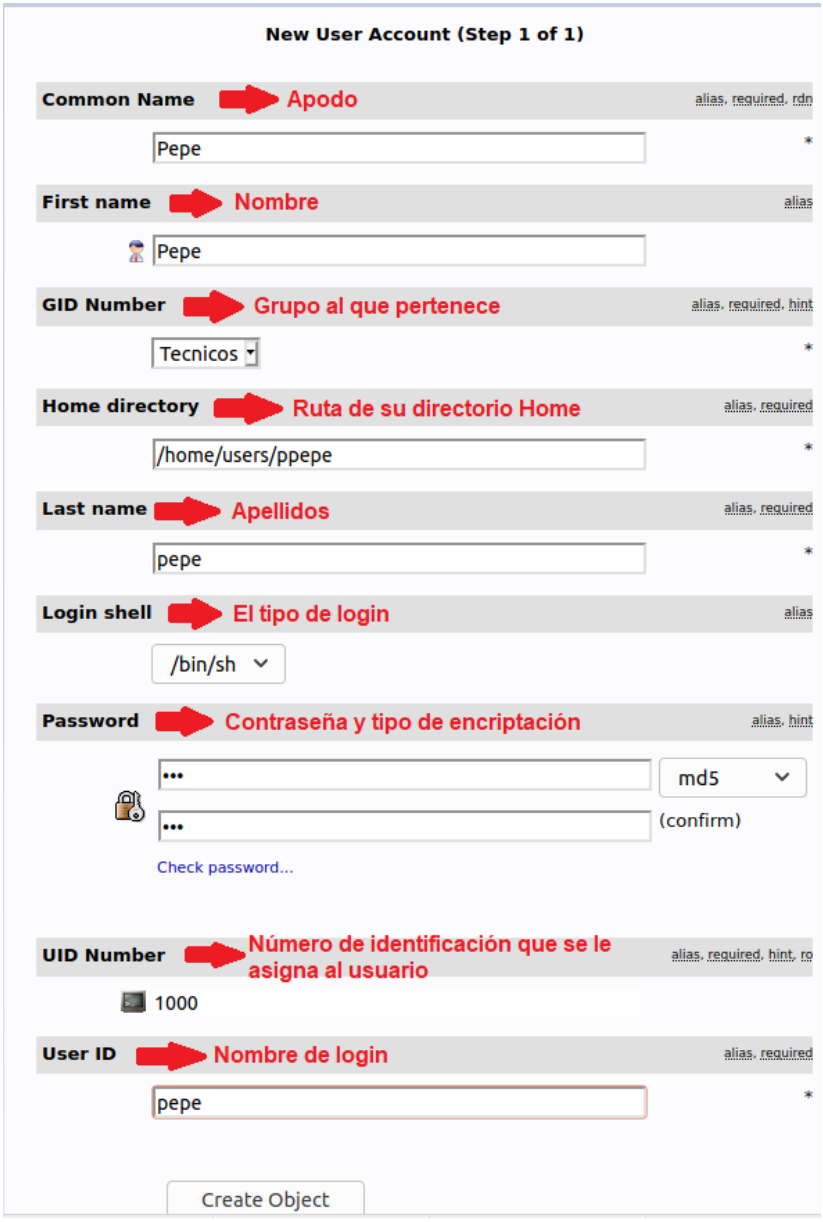


Figura 4.32. Panel de creación de usuario en PHPLDAPadmin

Comprobamos que esta todo correctamente y pulsamos **commit**. Creamos el usuario Paco realizando el mismo proceso.

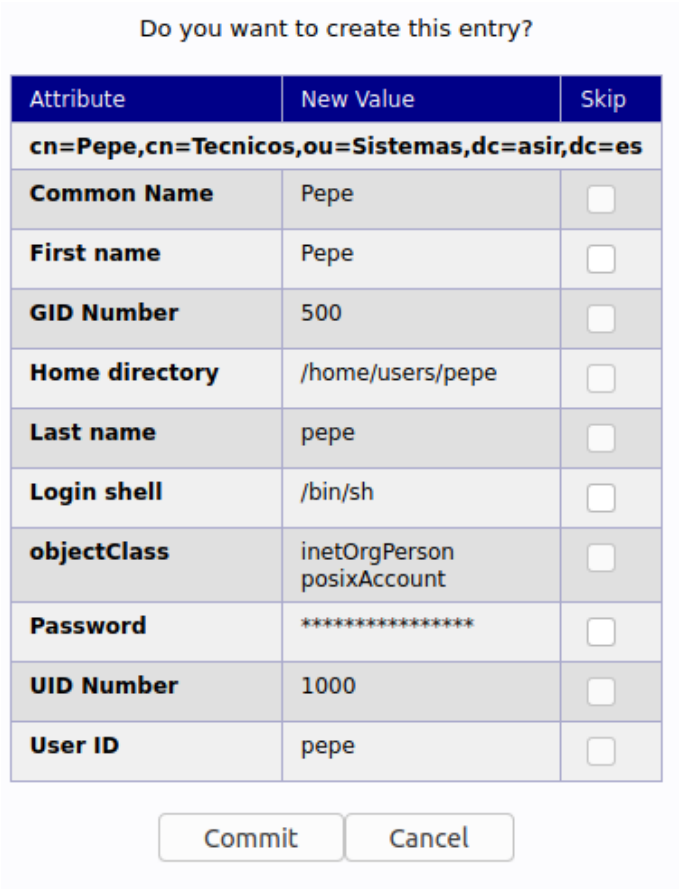


Figura 4. 33. Árbol de directorio PHPLDAPadmin

Si introducimos el comando **slapcat** en Ubuntu server podemos comprobar que lo está creando en el servidor

```
dn: cn=Paco,cn=Tecnicos,ou=Sistemas,dc=asir,dc=es
cn: Paco
givenName: Paco
gidNumber: 500
homeDirectory: /home/users/paco
sn: Paco
loginShell: /bin/sh
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
userPassword:: e01ENX1JQ3k1WXF4WkIxdVdTd2NWTFNOTGNBPTO=
uidNumber: 1001
uid: paco
structuralObjectClass: inetOrgPerson
entryUUID: 747da1a0-518f-103b-8366-8dba4b923950
creatorsName: cn=admin,dc=asir,dc=es
createTimestamp: 20210525102647Z
entryCSN: 20210525102647.749228Z#000000#000#000000
modifiersName: cn=admin,dc=asir,dc=es
modifyTimestamp: 20210525102647Z
```

Figura 4.34. Árbol de directorio en Ubuntu Servidor

4.5.3 Autenticación de usuarios

Cuando este todo creado vamos a intentar autenticar los usuarios en el **cliente**.

Iniciamos sesión con Pepe y cómo podemos ver en **Ubuntu cliente** nos crea un directorio para él en **/home/users/pepe**. Iniciamos sesión en el servidor y comprobamos que ha creado también el directorio.

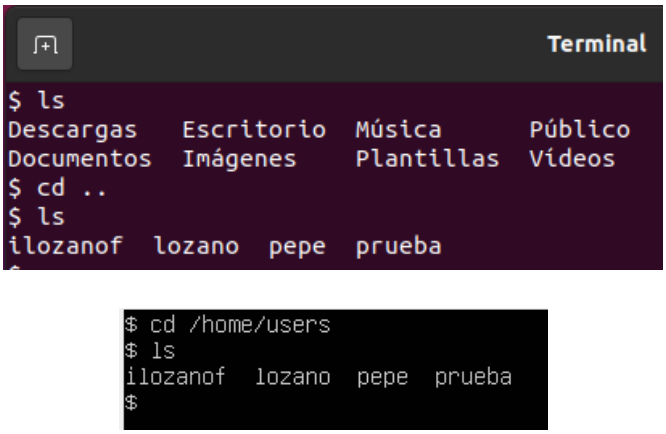


Figura 4.35. Comprobación del directorio home

Si hemos realizado los pasos correctamente y todas las comprobaciones previas salen como en las imágenes daremos por concluida la práctica de LDAP.

5.Conclusión

LDAP es un protocolo dedicado al acceso unificado de información. Por ejemplo, todas las diferentes listas de usuarios en el interior de su empresa pueden ser fusionadas en un solo directorio LDAP. Este directorio, a continuación, podrá ser consultado desde cualquier aplicación habilitada para LDAP a la que le sirva la información. El directorio también podrá ser utilizado por los usuarios que necesiten información sobre éste.

Una de las ventajas a destacar de este protocolo es que es fácil de instalar, mantener y optimizar. También permite replicar el servidor de forma sencilla y económica. Además, es un protocolo muy rápido en la lectura de registros.

Otra cosa a destacar de este protocolo es que casi todas las aplicaciones disponen de un soporte para este, esto puede ser realmente útil si tenemos algún problema con alguna de las aplicaciones. También muchas aplicaciones actuales tienen interfaces de conexión a LDAP y se pueden integrar fácilmente en nuestro servidor

Otra ventaja sería es que dispone de nombres globales que asegura que todas las entradas sean únicas

Lo malo de este protocolo a diferencia de AC es que no puedes tener tan controlado a los usuarios de la red ya que no tiene un sistema de permisos muy amplio.

Otro inconveniente que le veo a este servicio es que no tiene un sistema para administrar directivas como en AC que puedes hacer por ejemplo que un grupo de usuarios tenga ciertos permisos sobre una carpeta o que puedan acceder a panel de control sin ningún problema. En LDAP lo máximo que puedes utilizar scripts para automatizar tareas

LDAP soporta un número de bases de datos back-end en las que se guardan directorios. Esto puede permitir que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que volcar.

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. Puede ser útil para consolidar información de toda una organización dentro de un repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, puede usar LDAP como directorio central, accesible desde cualquier parte de la red.

6. Glosario de Términos y Acrónimos

OpenLDAP: es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP).

OpenPAM: es una biblioteca PAM de código abierto que se centra en la simplicidad, corrección y limpieza.

Resolver: recibe un nombre y lo traduce. el resolver debe conocer uno o más servidores de nombres a quienes enviarles la consulta. Esta información se configura en cada máquina, colocando la dirección IP del servidor (por supuesto, no es posible usar el nombre en este lugar). La traducción completa se le pide al servidor local.

IP: es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella

DNS: es un sistema de bases de datos distribuidas que sirve para gestionar nombres de hosts y las direcciones IP asociadas a ellos.

Zona directa: La zona de búsqueda directa resuelve los nombres de host en direcciones IP y albergan los registros de recursos comunes

Zona inversa: determina la dirección IP a partir de un nombre de dominio o de host determinado.

Dominio: es un nombre único que identifica a una subárea de Internet.

Unidad Organizativa: proporcionan un mecanismo para asignar una estructura de unidad organizativa jerárquica a los perfiles y las conciliaciones. Aportan valor al aplicar filtros y generar informes.

Directorio home: Es el directorio de los usuarios estándar, y, por lo tanto, el destinado a almacenar todos los archivos del usuario, como documentos, fotos, vídeos, música, plantillas, etc.

URL: es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres de acuerdo con un formato modélico y estándar que designa recursos en una red como, por ejemplo, Internet.

Forwarder: asignación o reenvío de puertos para transmitir información a través de una red. También se encarga de transmitir paquetes de información entre servidores externos a los servidores internos de una red particular.

7.Bibliografía y referencias

- SASTRE TORAL, Teresa - Instalación y configuración del servicio DNS, Laboratorio_ut2, paginas 22 – 26.
- LARA, Jesús - Libro OpenLDAP fácil, marzo de 2014.
- ANTONIO CASTILLO, José “LDAP: Qué es y para qué se utiliza este protocolo”, enero de 2019, paginas 6 – 8 https://www.profesionalreview.com/2019/01/05/ldap/
- ProngeR TV - Cómo instalar y configurar LDAP Server y Cliente Ubuntu 16.04 - Tutorial 2020, enero de 2020 https://www.youtube.com/watch?v=3ZIwyKenBU4
- FPInf0rmatica - OpenLDAP con Ubuntu 14: configuración de servidor y cliente, febrero de 2015 https://www.youtube.com/watch?v=2yjhxGNbDjo
- MUTAI, Josphat - Configure LDAP Client on Ubuntu 20.04, octubre de 2020 https://computingforgeeks.com/how-to-configure-ubuntu-as-ldap-client/
- MOLINA COBALLES, Alberto - Autenticación LDAP en GNU/Linux, enero de 2008 https://albertomolina.files.wordpress.com/2008/07/autenticacion_ldap.pdf