

51 platega I-II-III

Indice

Platega I.....	1
Configuración red nat.....	1
Exportación máquina debian.....	7
Actualizado de los paquetes, exportado de una máquina Debian.....	8
Búsqueda de paquetes.....	11
Instalar y desinstalar paquetes.....	12
Configuración de dbase.....	15
Configuración manual de la red.....	15
Cambiado de hostname.....	17
Editado del archivo /etc/host.....	18
Administración remota del servidor.....	20
Redireccionamiento de puertos.....	20
Instalación de openssh-server.....	20
Inicio de sesión mediante ssh.....	21
Secure copy.....	22
Trabajo con Ubuntu.....	25
Instalación y configuración.....	25
Exportamos la OVA.....	28
Creamos la máquina uclient01.....	28
Configuración de red mediante la interfaz gráfica.....	28
Cambiado de hostname.....	29
Editado fichero hosts.....	30
Administración remota del servidor.....	32
Redireccionamiento de puertos.....	32
Inicio de sesión mediante ssh.....	32
Conectividad entre las máquinas.....	33
Configuración del servidor DNS.....	34
Creación de zonas directa e inversa.....	36
Configuración de zonas directa e inversa.....	37
Comprobación de sintaxis de ficheros de configuración.....	39
Reload bind9.....	40
Configuración client-side servidor DNS.....	41
Comprobación del funcionamiento del DNS.....	41
Configuración del DNS en el cliente.....	43
Escenario 1-C.....	45
Instalación y configuración de servicio de DHCP (server-side) Debian.....	45
Configuración del cliente: uclient02.....	49
Reserva de IPs.....	51
Configuración de reservas de IP en dserver00.....	51
Configuración de uclient02.....	53
Asignación automática de hostname.....	54
Configuración en el servidor DHCP.....	54
Configuración en el cliente para configurar su nome de equipo mediante el servidor DHCP	
.....	55
Escenario 1.D - Configuración de DNS dinámico: DDNS.....	58
Configuración de DDNS en dserver00.....	58

Configuración client-side.....	62
Finalización.....	62
Platega II.....	63
Instalar y configurar slapd.....	63
Utilidades ldap: paquete ldap-utils.....	69
Instalación y comprobación de funcionamiento.....	69
Administración de unidades organizativas, usuarios e grupos en LDAP con ldap-utils.....	74
Creación de unidades organizativas.....	74
Modificación de unidades organizativas.....	76
Eliminar Unidades Organizativas.....	79
Unidades Organizativas: ejercicio para o/a lector/a.....	81
Administración de grupos.....	84
Administración de usuarios.....	85
Añadir usuarios a los grupos secundarios.....	87
Eliminar/modificar usuarios.....	88
Usuarios: ejercicio para el lector.....	90
.....	93
Cambiar la contraseña de un usuario.....	94
Herramientas incluidas con el servidor LDAP.....	96
Configuración del cliente LDAP.....	97
Instalar los paquetes necesarios.....	97
Configuración cliente LDAP en dserver00 e uclient02.....	101
Configuración de cliente LDAP en uclient02.....	102
Configuración de cliente LDAP en dserver00.....	103
Herramientas para administración do LDAP: ldapscripts, LDAP Account Manager (LAM) y Jxplorer.....	105
Administración mediante scripts.....	105
Gestión de usuarios y grupos.....	107
LDAP Account Manager (LAM).....	107
Instalamos el LAM.....	107
Configuración de LAM.....	108
Iniciar sesión por primera vez.....	113
Crear grupos en LAM. Ejercicio.....	116
Crear usuarios en LAM.....	116
Jxplorer.....	119
Autenticación segura contra LDAP. Uso de TLS/SSL: LDAPS.....	121
Creación de los certificados digitales.....	124
Creación de la autoridad de certificación.....	124
Generar la solicitud de firma del certificado (CSR).....	127
Generar el certificado a partir do CSR.....	129
Configuración do servidor LDAP.....	130
Configuración del cliente.....	135
Comprobación mediante ettercap.....	139
Platega III.....	140
Creación y configuración del esqueleto de la estructura de carpetas.....	140
Formateado de las particiones.....	144
Montado de las particiones.....	145
Creado del esqueleto.....	148

51 Platega I_II_III

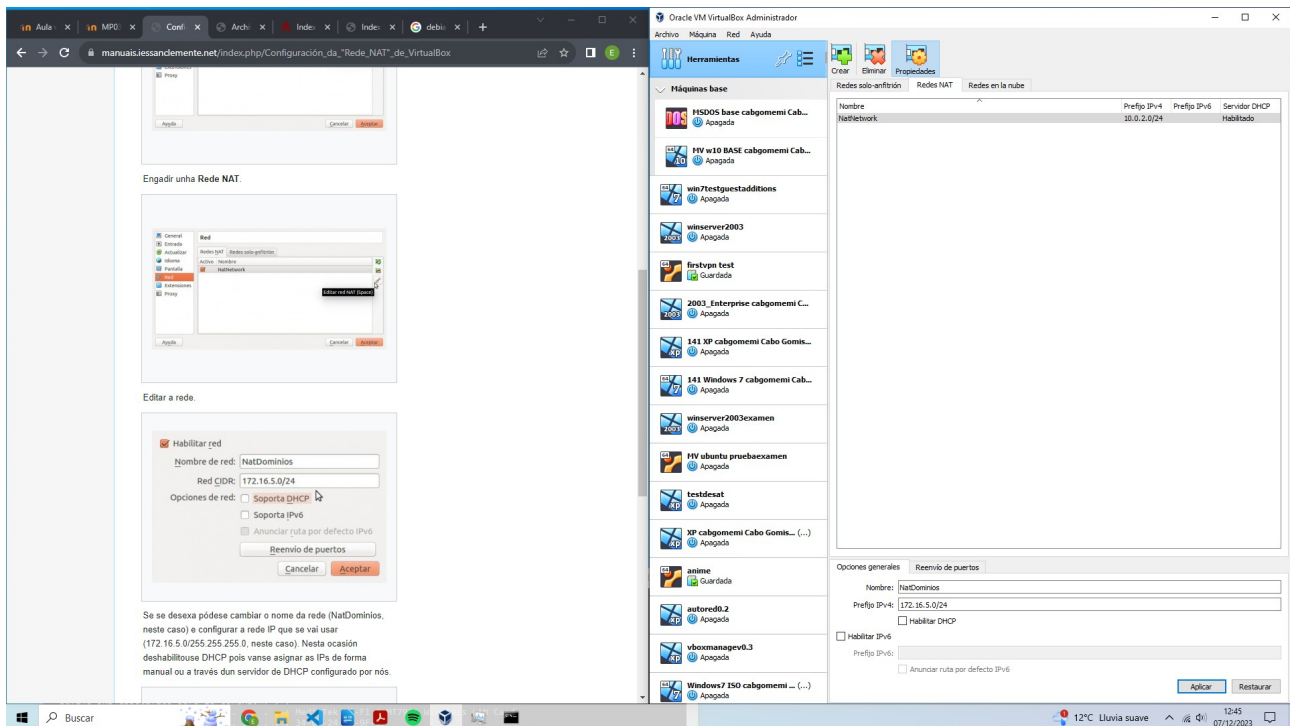
Copiado del /etc/skel ./.....	152
Instalación del servidor NFS. Exportaciones.....	155
PLATEGA IV Cuotas de disco y copias de seguridad.....	157

Platega I

Configuración red nat

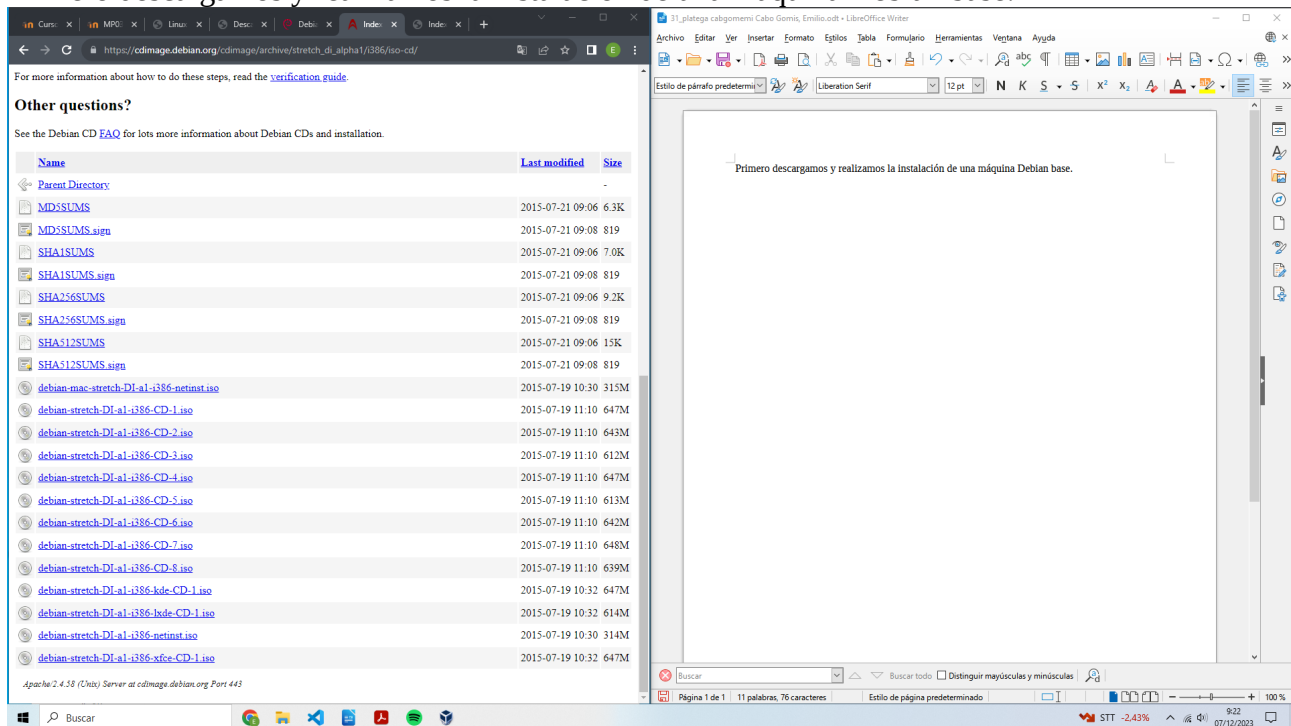
Antes de continuar deberemos configurar una red NAT para que las máquinas que creemos puedan comunicarse entre ellas e internet.

Lo configuramos entrando en herramientas > red > nat > añadir nueva > configurar.



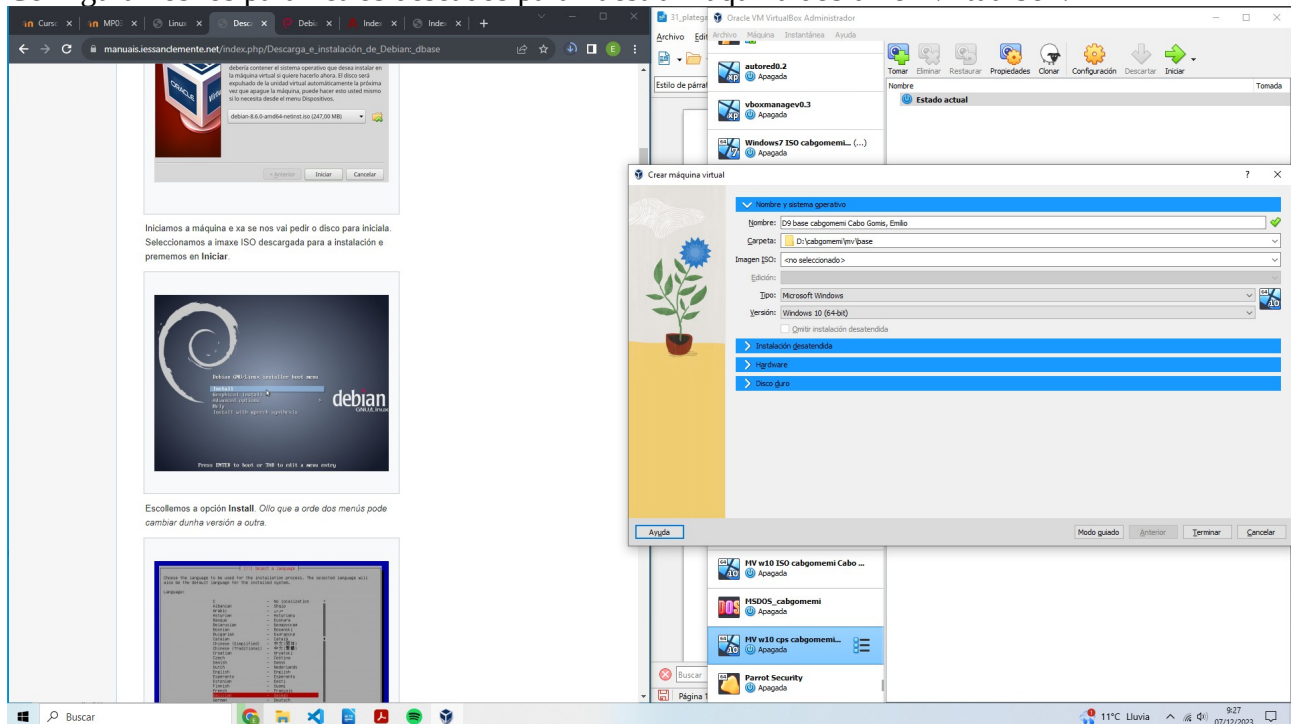
Menú configuración de red NAT.

Primero descargamos y realizamos la instalación de una máquina Debian base.



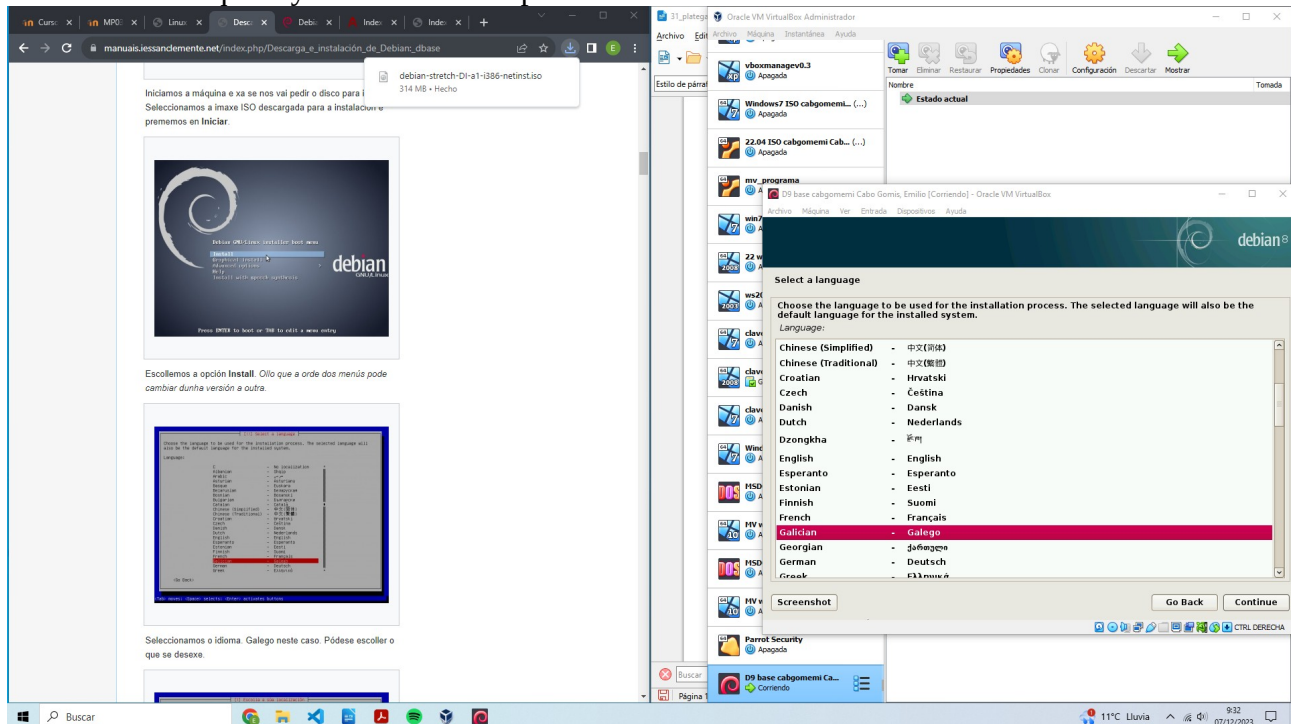
Captura de pantalla mostrando las versiones archivadas de Debian

Configuramos los parámetros deseados para nuestra máquina debian en virtualbox.



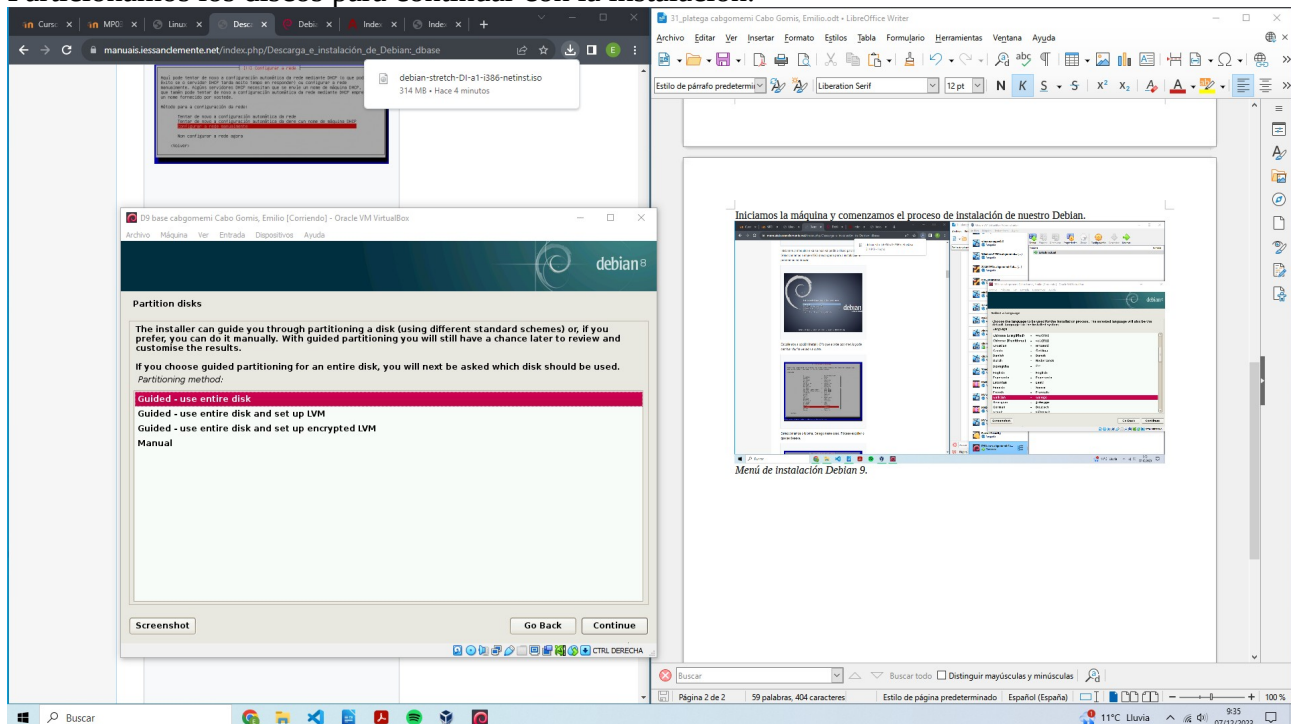
Menú de configuración de virtualbox para los ajustes de la máquina virtual.

Iniciamos la máquina y comenzamos el proceso de instalación de nuestro Debian.



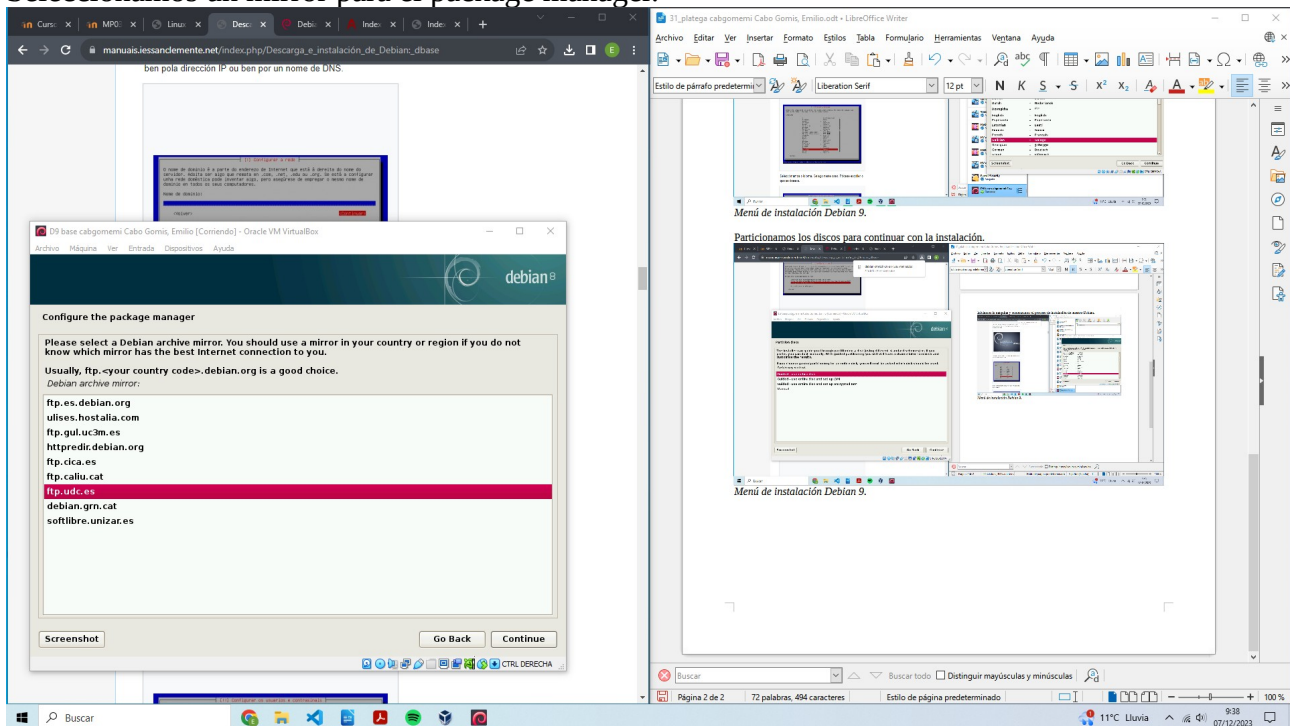
Menú de instalación Debian 9.

Particionamos los discos para continuar con la instalación.



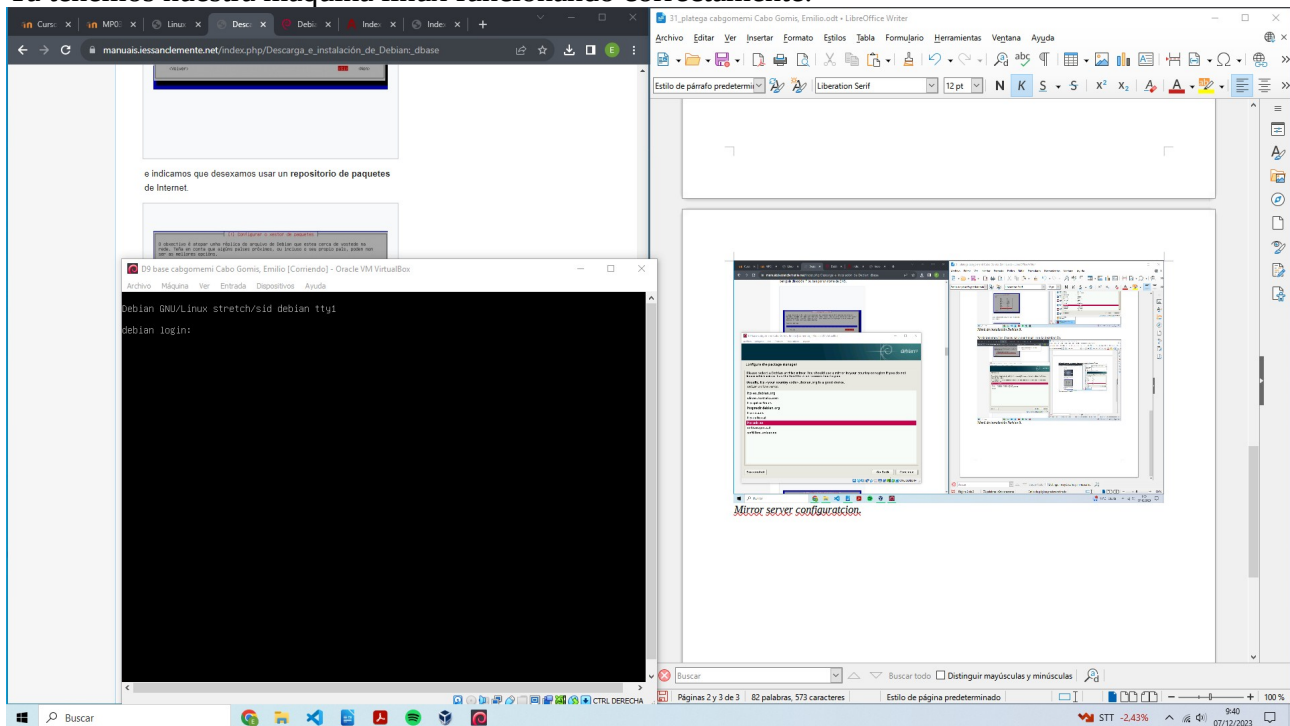
Menú de instalación Debian 9.

Seleccionamos un mirror para el package manager.



Mirror server configuratcion.

Ya tenemos nuestra máquina linux funcionando correctamente.



TTY de debian9

En caso de que nos dé problemas añadir los repositorios de debian. Deberemos emplear una versión posterior. Cómo Debian 12.2

En caso de seguir esa ruta deberemos no instalar un entorno gráfico.

51 Platega I_II_III

Comprobaremos el estado de la instalación realizando algunos comandos.

Df -h

The screenshot shows a web browser window on the left displaying a tutorial for Debian installation. The tutorial includes sections for 'Preparación sistema base Debian', 'Revisar configuración mínima', and 'Con clear limpiamos a pantalla'. The terminal window on the right shows the output of the 'df -h' command, displaying disk space usage for various partitions.

```
Debian GNU/Linux 12 debian tty1
debian login: administrador
Password:
Linux debian 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
administrador@debian:~$ df -h
Sist. Fich. Tamaño Usado  Disp Usos% Montado en
udev          482M   0  482M   0% /dev
tmpfs         57M  528K   96M   1% /run
/dev/sda1     6.8G  1.2G   5.3G  19% /
tmpfs         481M   0  481M   0% /dev/shm
tmpfs         5.0M   0  5.0M   0% /run/lock
/dev/sda6     12G  40K   12G   1% /home
tmpfs         57M   0   57M   0% /run/user/1000
administrador@debian:~$
```

Comprobamos que la máquina ha sido correctamente configurada.

Hostname

The screenshot shows a web browser window on the left displaying a tutorial for Debian installation. The tutorial includes sections for 'Con ls amosamos o contenido dun directorio, coa opción -a amosamos os todo: ficheiros ocultos e non ocultos', 'Comprobamos o nome do sistema, este almacénase en /etc/hostname', and 'Revisamos a configuración IP no ficheiro /etc/network/interfaces'. The terminal window on the right shows the output of the 'hostname' command, displaying the system name 'debian'.

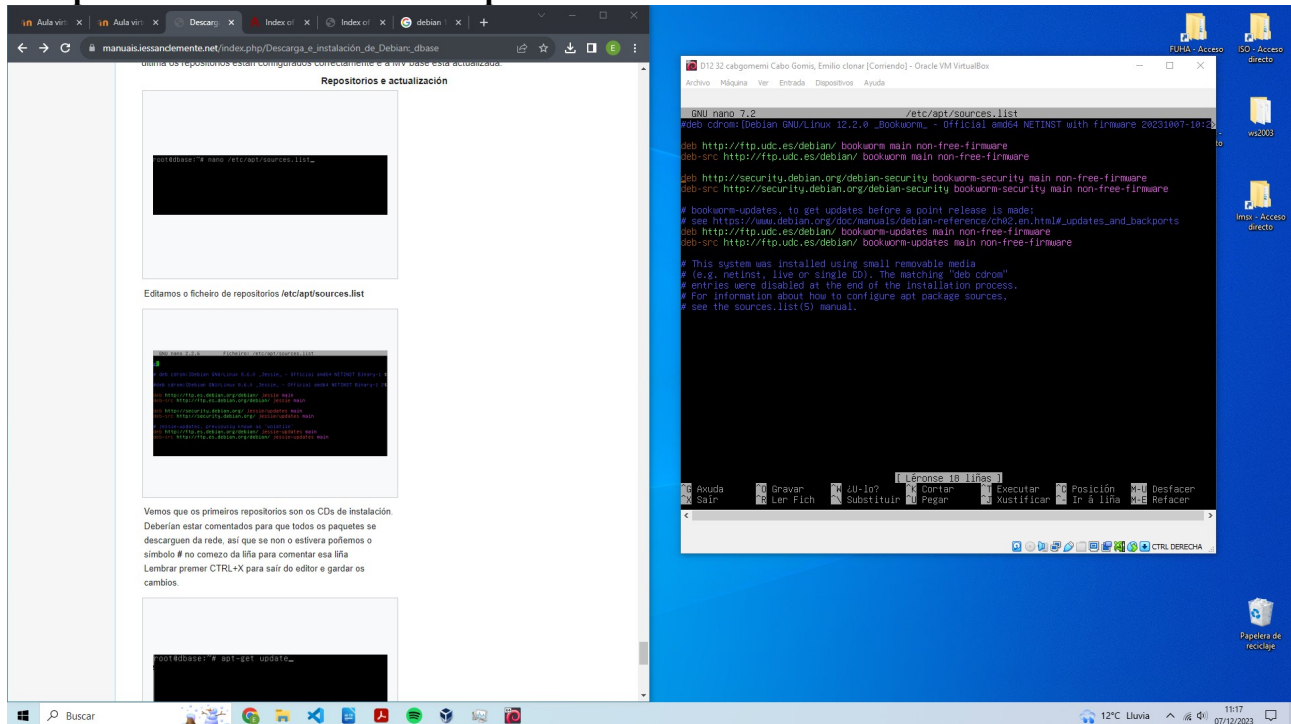
```
Debian GNU/Linux 12 debian tty1
debian login: administrador
Password:
Linux debian 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
administrador@debian:~$ df -h
Sist. Fich. Tamaño Usado  Disp Usos% Montado en
udev          482M   0  482M   0% /dev
tmpfs         57M  528K   96M   1% /run
/dev/sda1     6.8G  1.2G   5.3G  19% /
tmpfs         481M   0  481M   0% /dev/shm
tmpfs         5.0M   0  5.0M   0% /run/lock
/dev/sda6     12G  40K   12G   1% /home
tmpfs         57M   0   57M   0% /run/user/1000
administrador@debian:~$ cat /etc/hostname/interfaces
cat: /etc/hostname/interfaces: Non é un directorio
administrador@debian:~$ hostname
debian
administrador@debian:~$
```

Comprobamos que la máquina ha sido correctamente configurada.

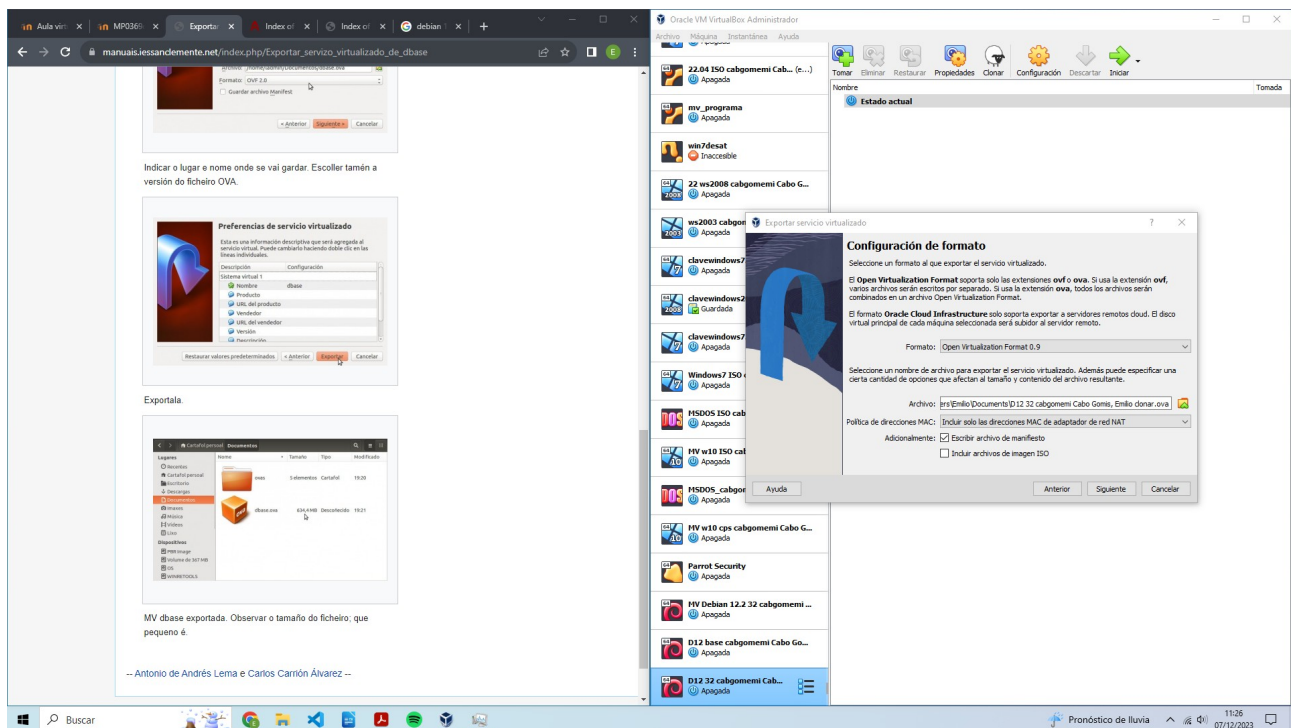
Comprobamos los sources de los repos.



Comprobamos que la máquina ha sido correctamente configurada.

Exportación máquina debian

Exportaremos nuestra máquina debian a OVA para poder reutilizarla múltiples veces.

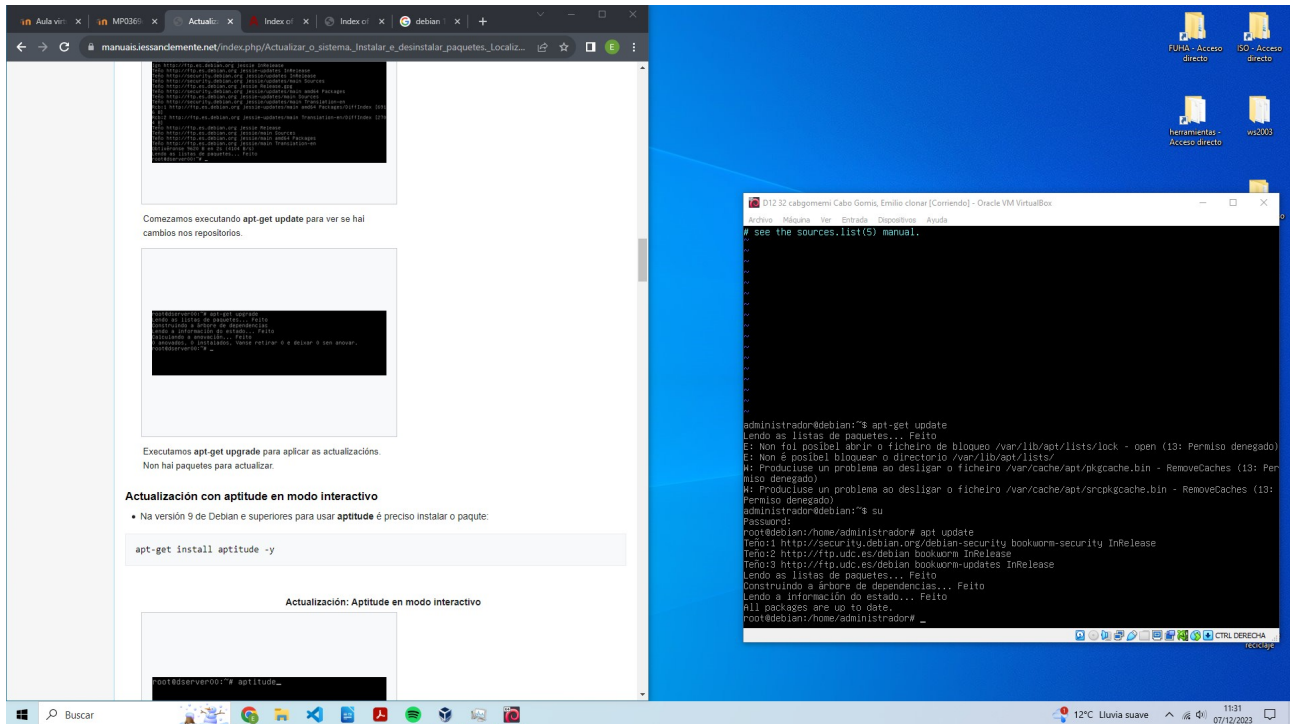


Menú para la exportación de una máquina debían a formato OVA.

Actualizado de los paquetes, exportado de una máquina Debian.

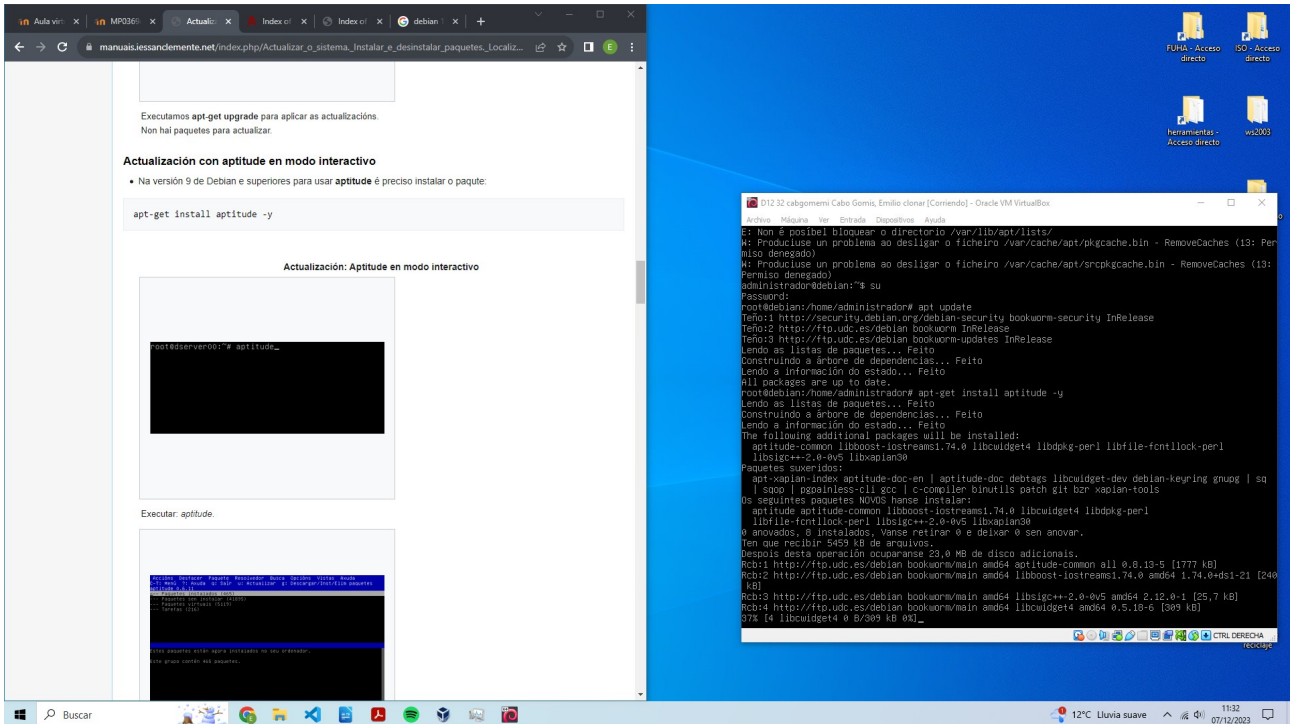
Para ejecutar los siguientes comandos deberemos ser root.

Comprobamos si hay cambios en los repositorios.



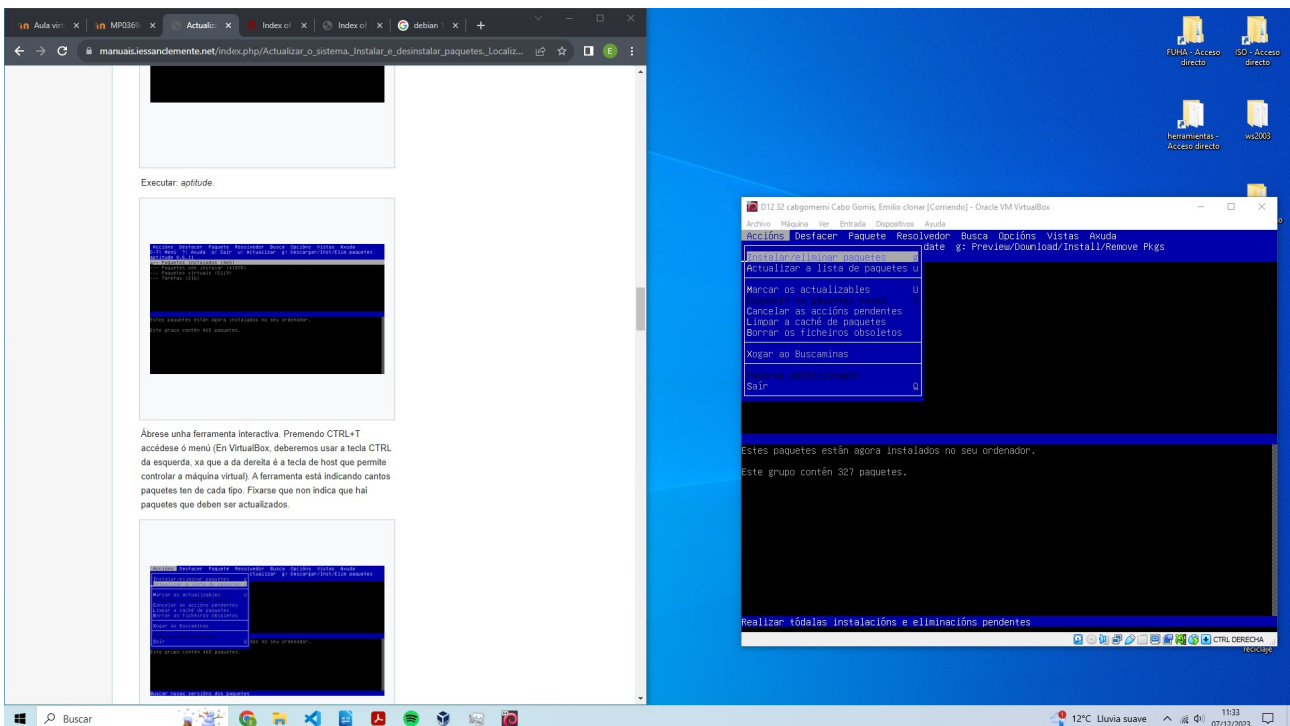
Ouput comando apt-update

Instalaremos aptitude en modo interactivo.



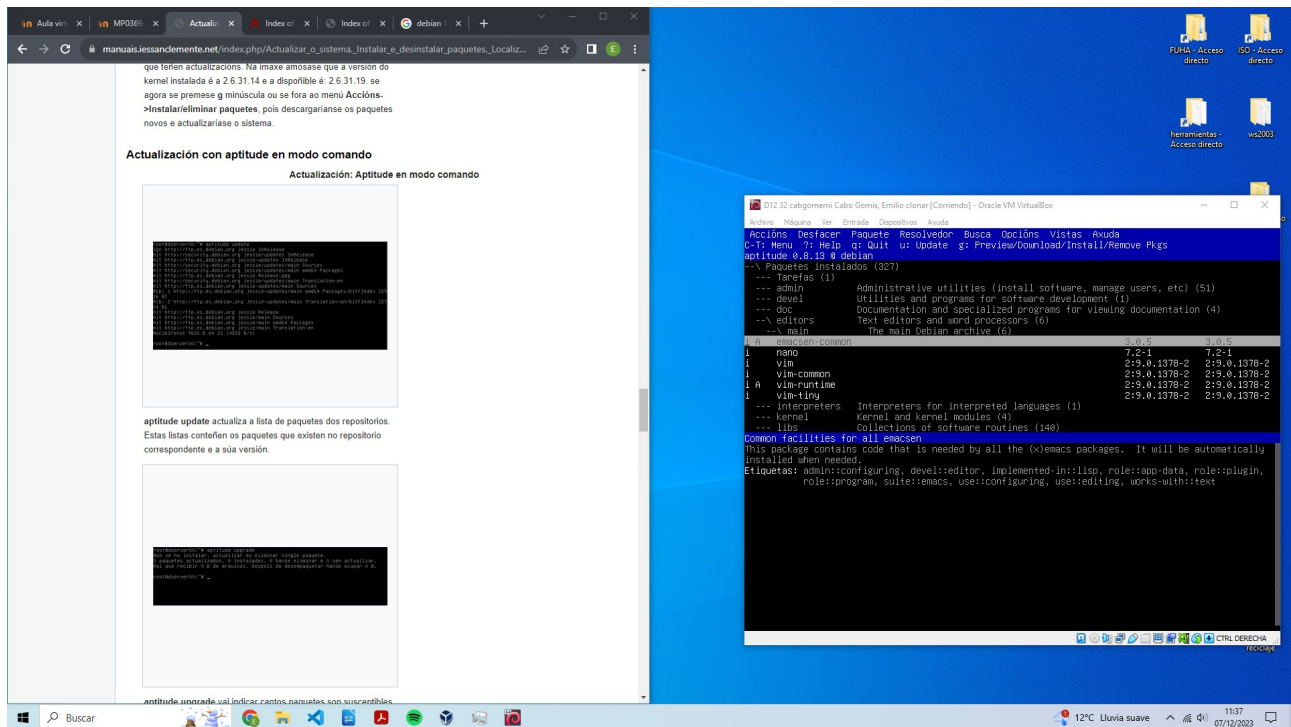
Instalación de aptitude.

Ejecutamos el programa mediante el comando **aptitude**.



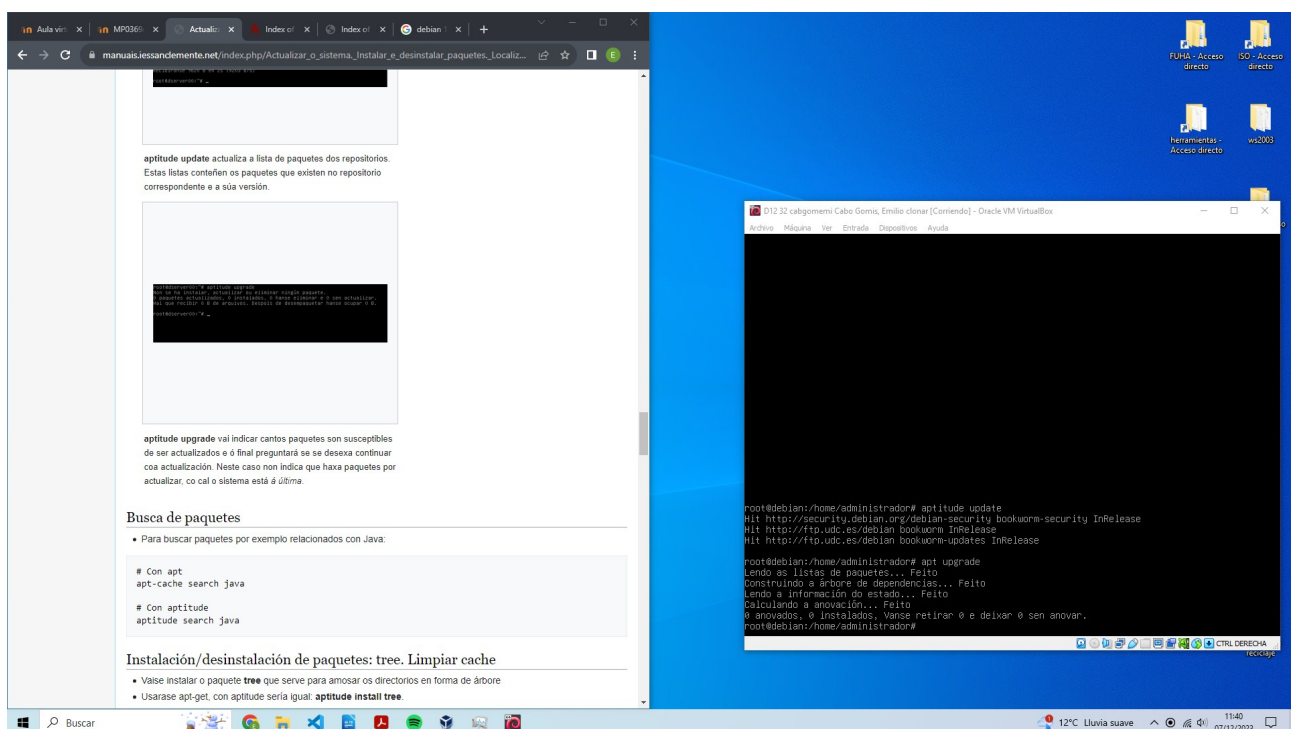
Menú inicial del programa aptitude.

Podemos comprobar mediante este programa algunos de los paquetes instalados, clasificados en su categoría.



Menú del programa aptitude.

Actualizar los paquetes en el sistema.



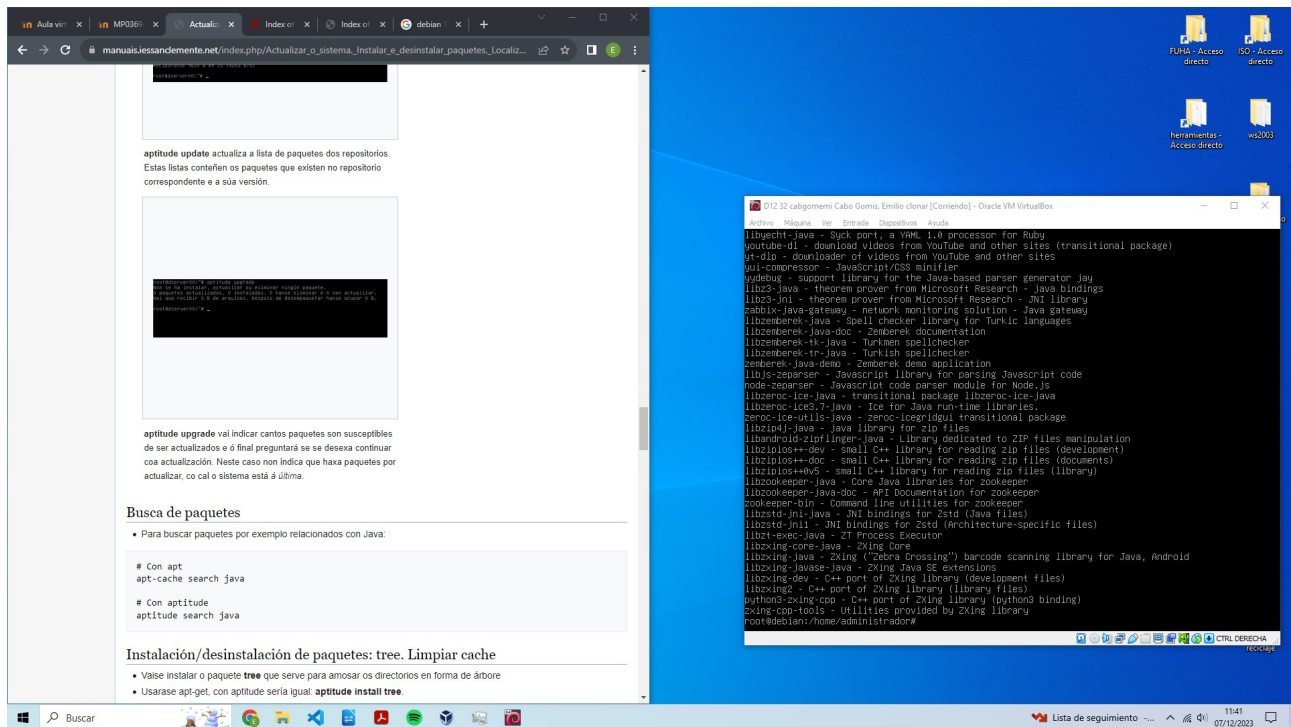
Output comando apt-upgrade

El hecho de que no se hayan actualizado paquetes nos indica que todos los paquetes han sido correctamente actualizados.

Búsqueda de paquetes

Para buscar paquetes relacionados

apt-cache search java

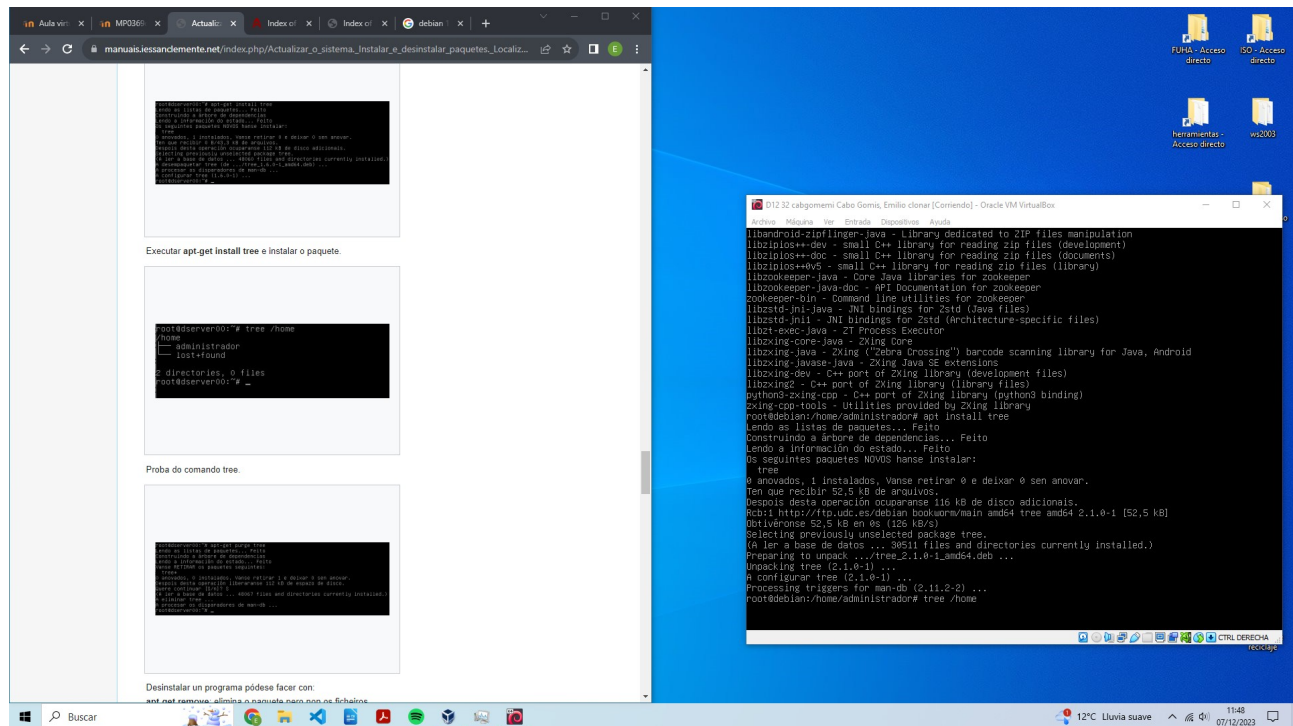


Output comando search

Instalar y desinstalar paquetes

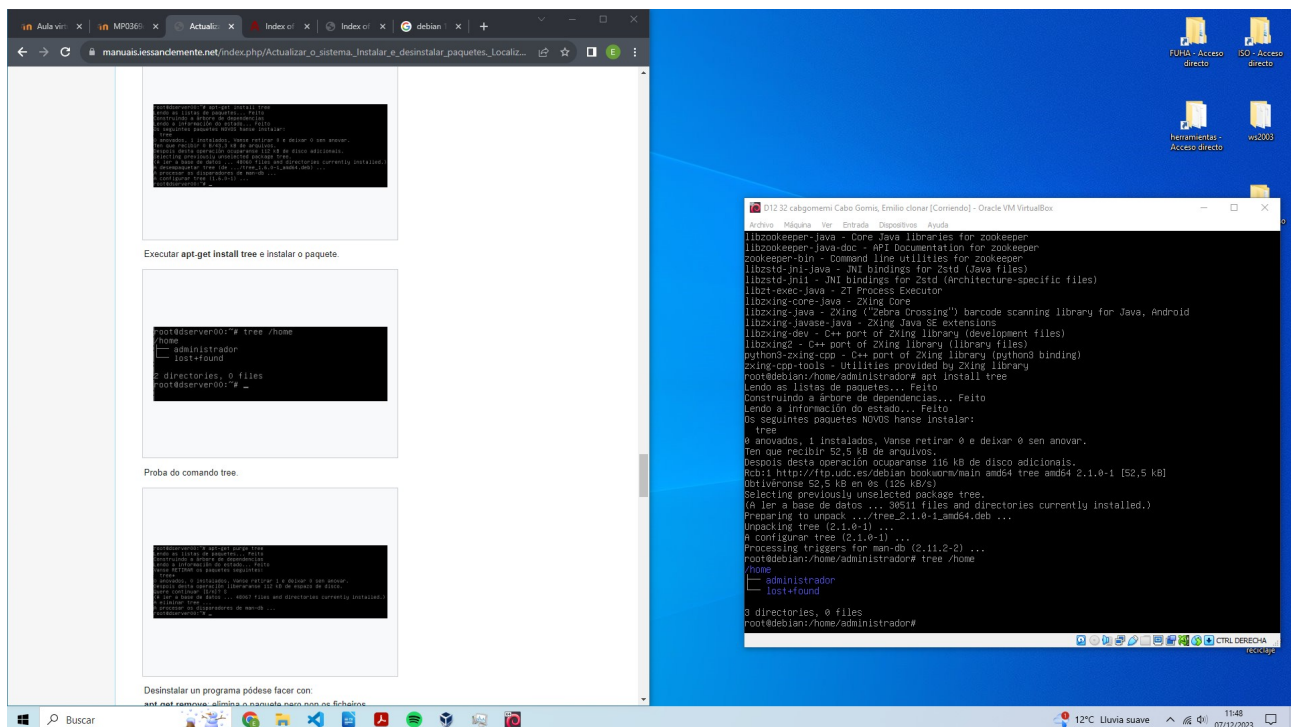
Apt install tree

Mediante ese comando lo que haremos será instalar un paquete para visualizar la estructura del sistema de archivos.



Output del comando install.

Comprobamos su funcionamiento.



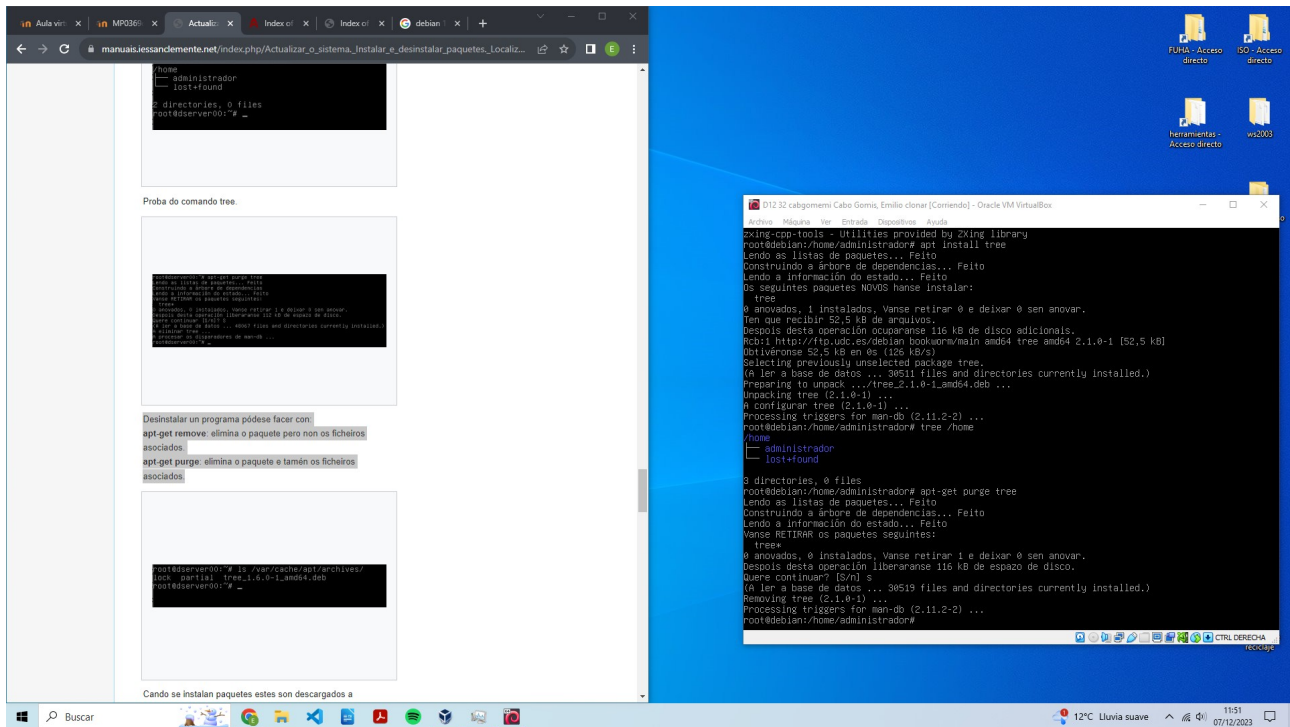
Output del comando tree.

Desinstalar paquetes:

`apt-get remove`: Elimina el paquete, pero no los archivos asociados.

`apt-get purge`: Elimina el paquete y también los archivos asociados.

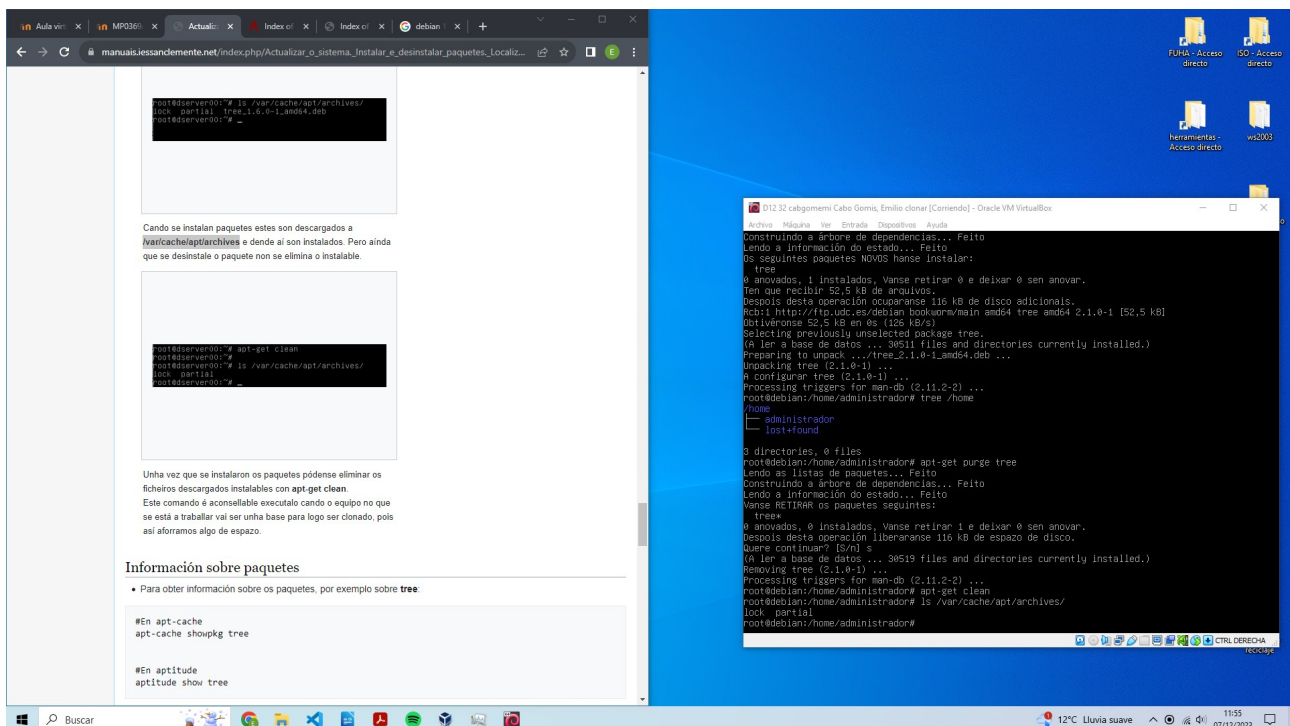
Realizaremos el segundo comando para purgar y también eliminar los archivos asociados.



Output del comando purge.

Para eliminar completamente un paquete instalado.

Deberemos eliminarlo del directorio: '/var/cache/apt/archives' eso lo haremos mediante el comando apt-get clean.



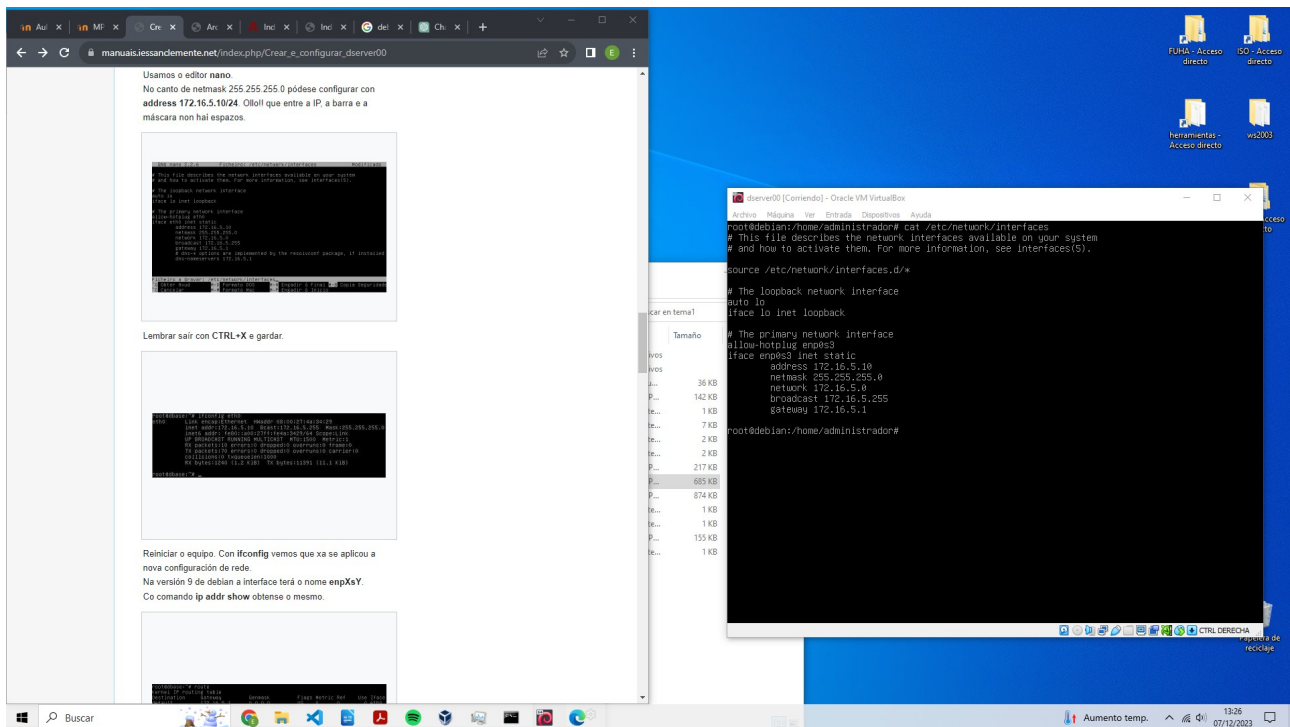
Output sobre el directorio '/var/cache/apt/archives'.

Configuración de dbase

Comprobamos que nuestra máquina debian dbase está configurada en Red NAT y a su vez conectada a la red NAT que configuramos previamente.

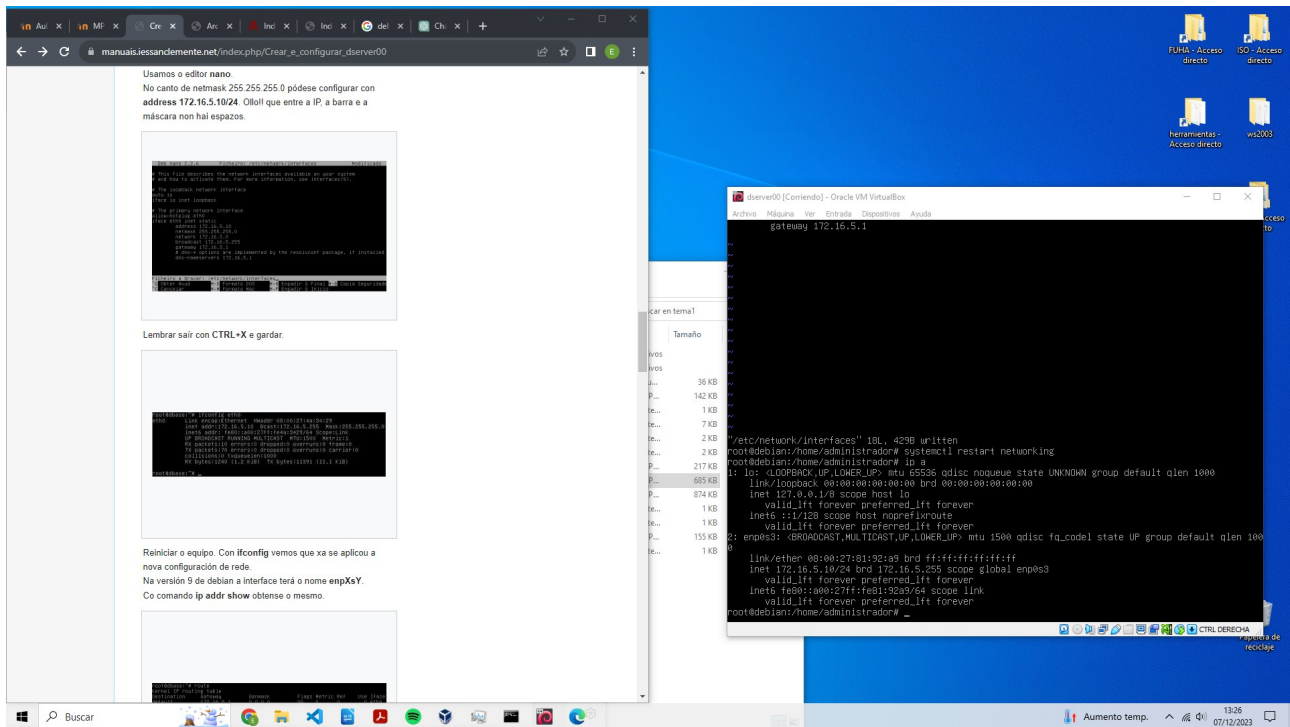
Configuración manual de la red

Realizaremos la configuración manual de red editando el fichero /etc/network/interfaces



Contenido del fichero /etc/network/interfaces.

Comprobamos que la configuración de ha aplicado correctamente

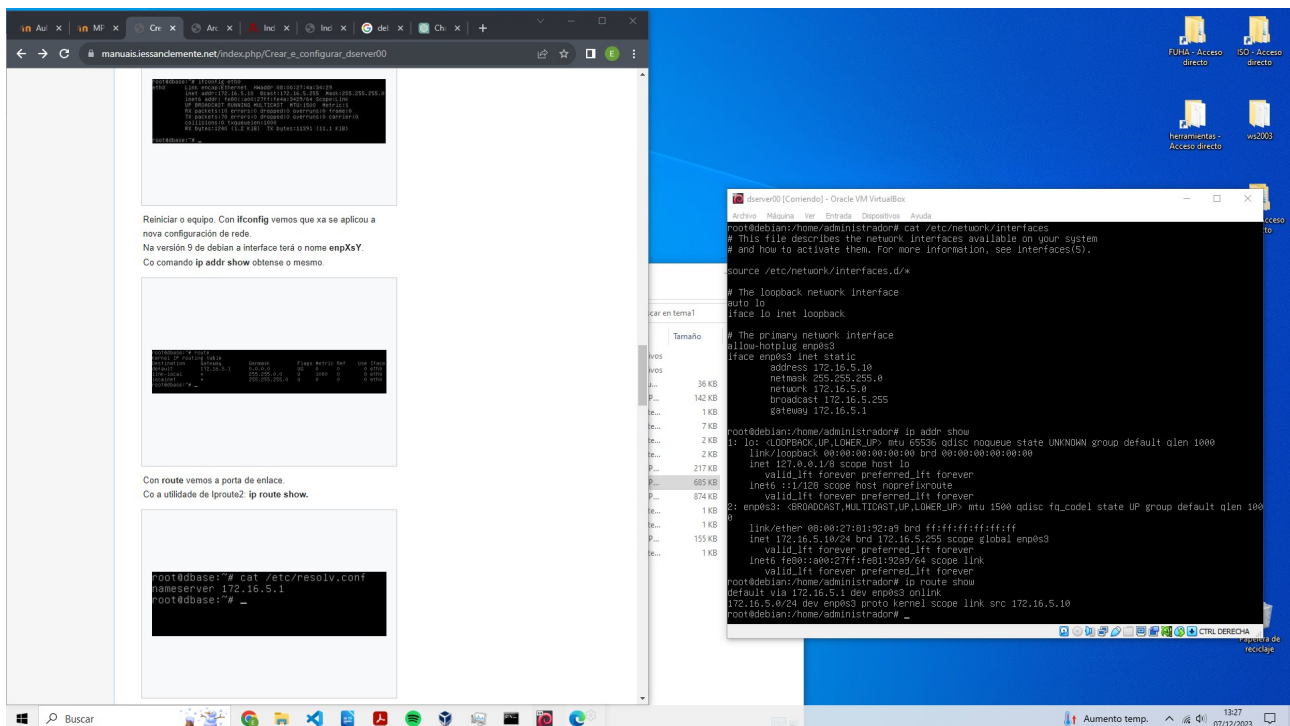


Output comando `ip a`.

Otras maneras de comprobar que la configuración de red es efectiva.

Ip addr show

ip route show

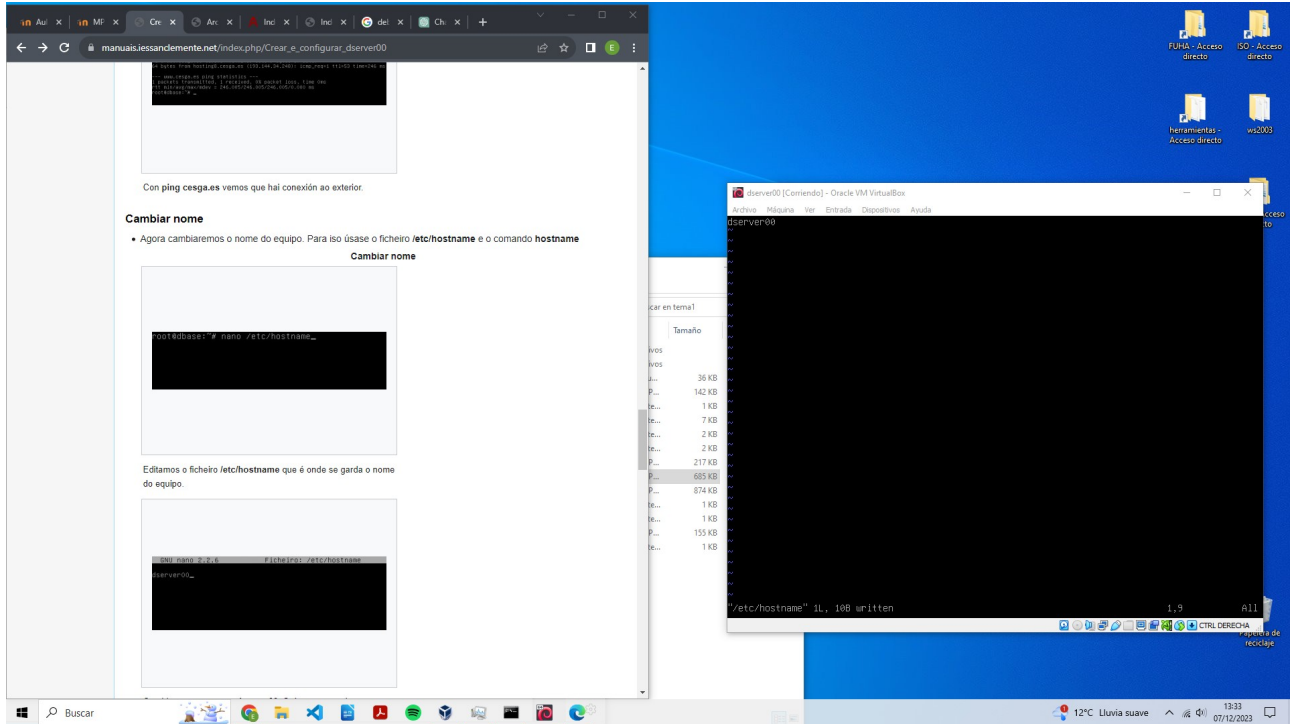


Output comando de comprobación de la configuración de red.

Cambiado de hostname

Editamos el contenido del fichero /etc/hostname

Introducimos el nombre dserver00

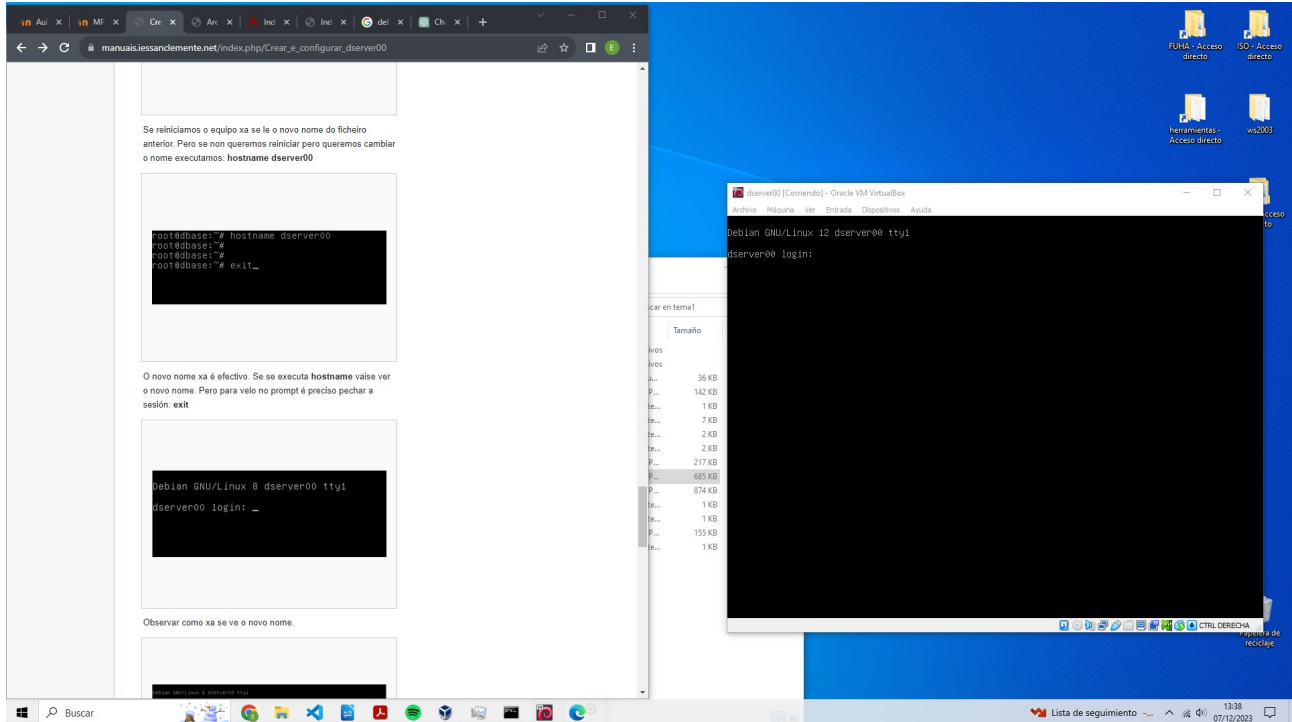


contenido del fichero /etc/hostname

En caso de no querer reiniciar el equipo deberemos realizar el comando **hostname dserver00**

En este caso los cambios se harían efectivos al salir sesión. **Exit.**

Al reiniciar el equipo el nombre ya es efectivo



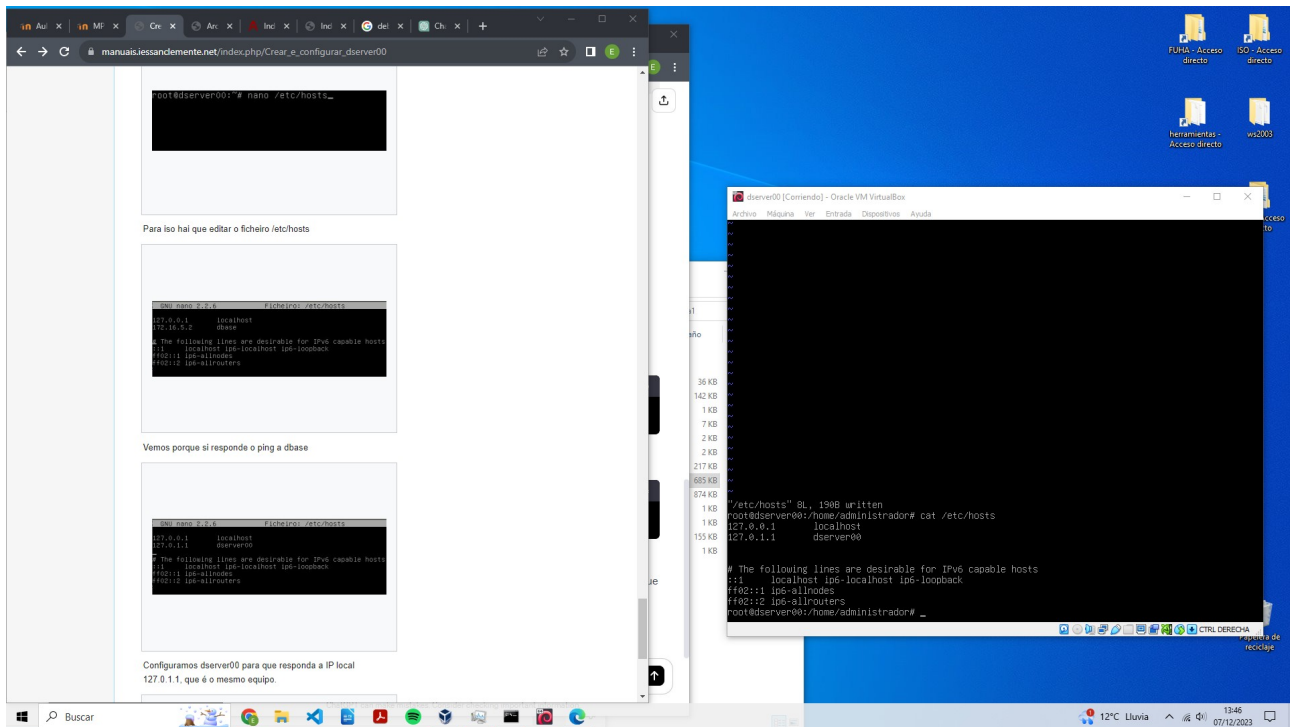
Inicio de sesión.

Editado del archivo **/etc/host**

Editaremos este archivo para que al hacer ping nos responda nuestro equipo.

Este archivo se utiliza para resolver nombres de host a direcciones IP localmente antes de recurrir a los servidores DNS.

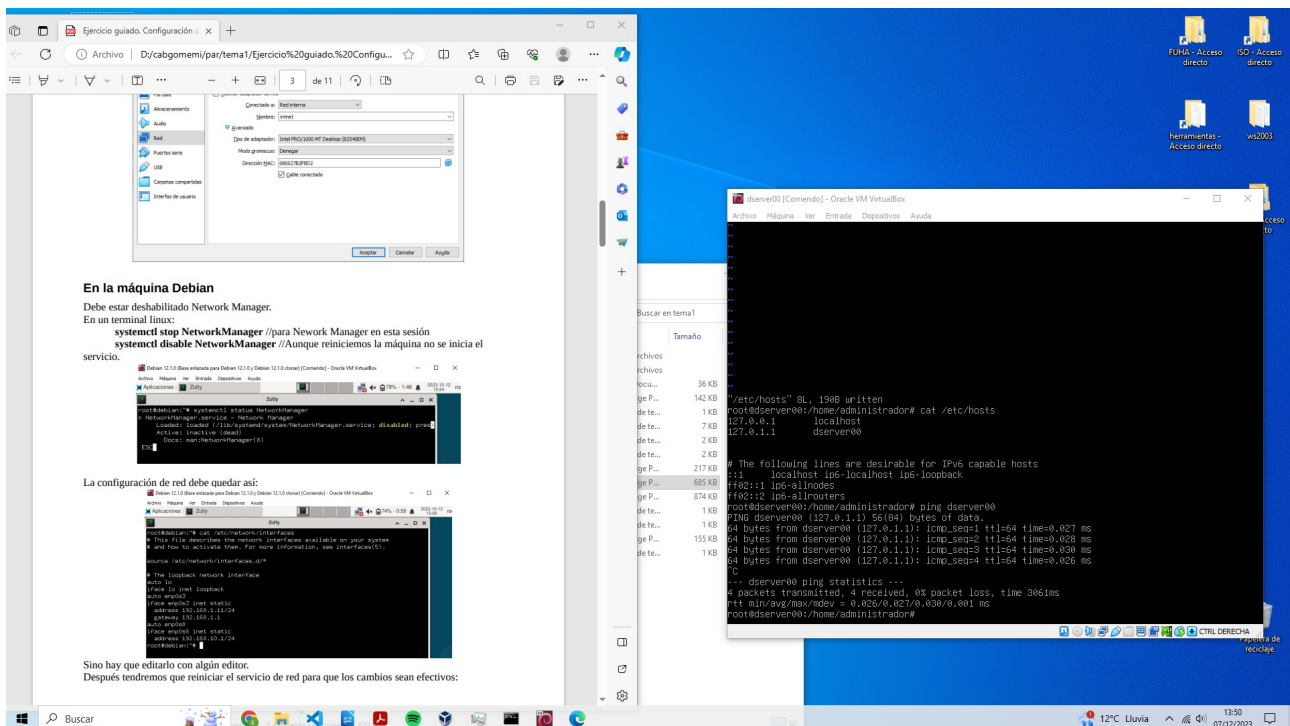
Editamos el archivo **/etc/hosts** para que tenga el siguiente contenido.



Contenido `/etc/hosts`.

Comprobamos que efectivamente los cambios han tenido efecto.

Ping dsverv00



Ping output.

Administración remota del servidor

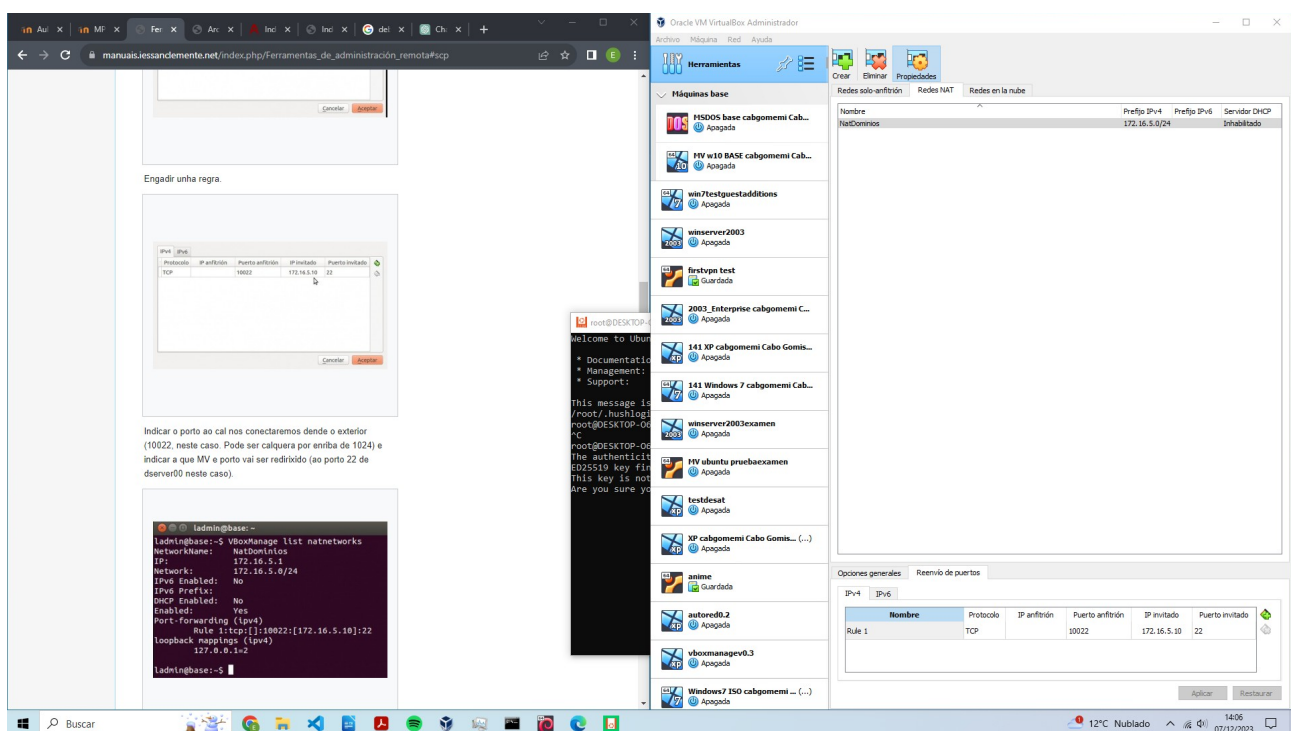
Redireccionamiento de puertos

Para poder acceder desde el exterior al interior de la red NAT es necesario que configuremos una regla en nuestra red nat.

La configuraremos de la siguiente manera.

Entraremos en el menú en el que configuramos la red NAT anteriormente > reenvío de puertos.

Aplicaremos la siguiente regla:

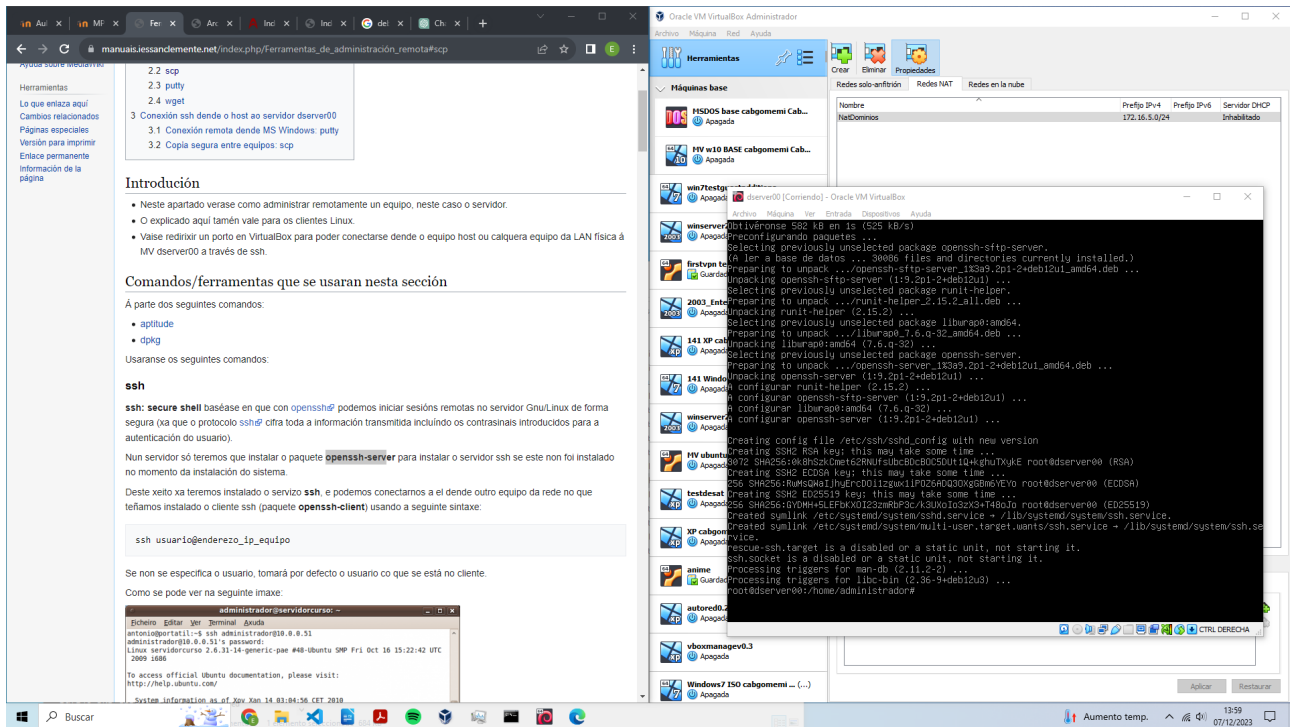


Menú configuración reenvío de puertos.

Instalación de openssh-server

Realizaremos la instalación del paquete openssh-server en nuestro dserver00.

Apt install openssh-server



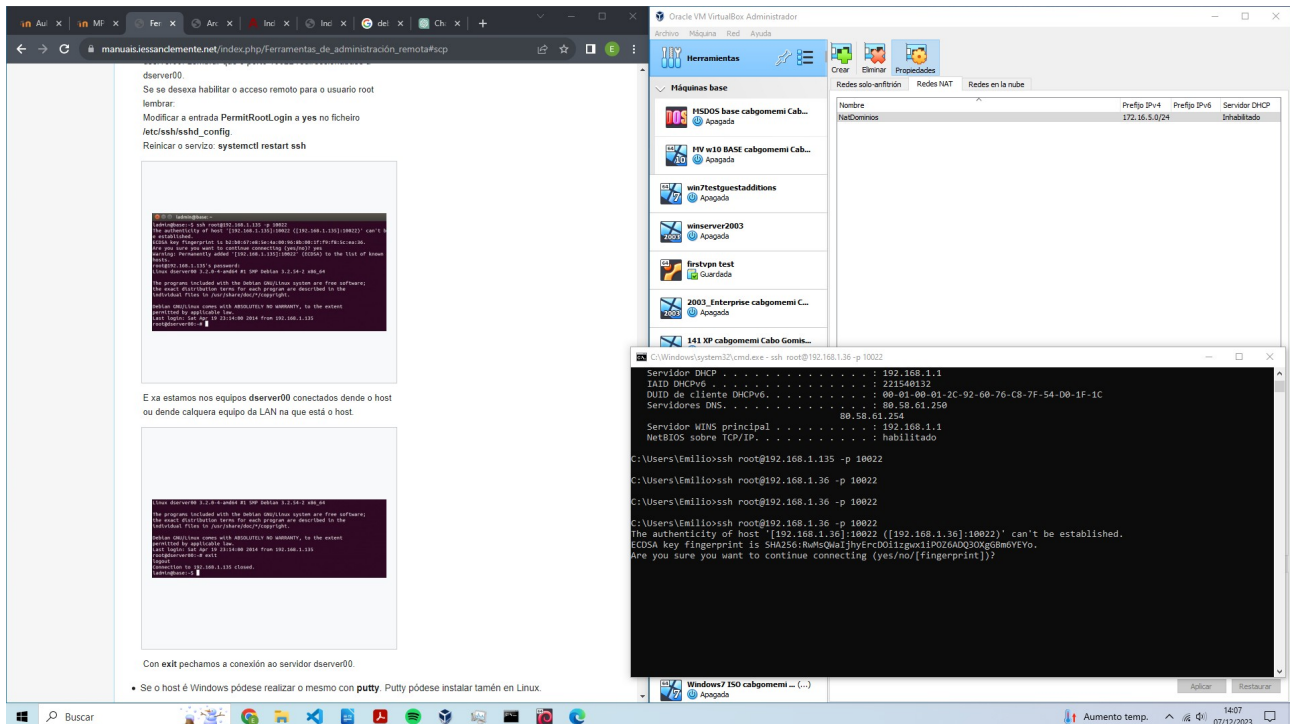
Output del comando de instalación openssh-server.

Inicio de sesión mediante ssh

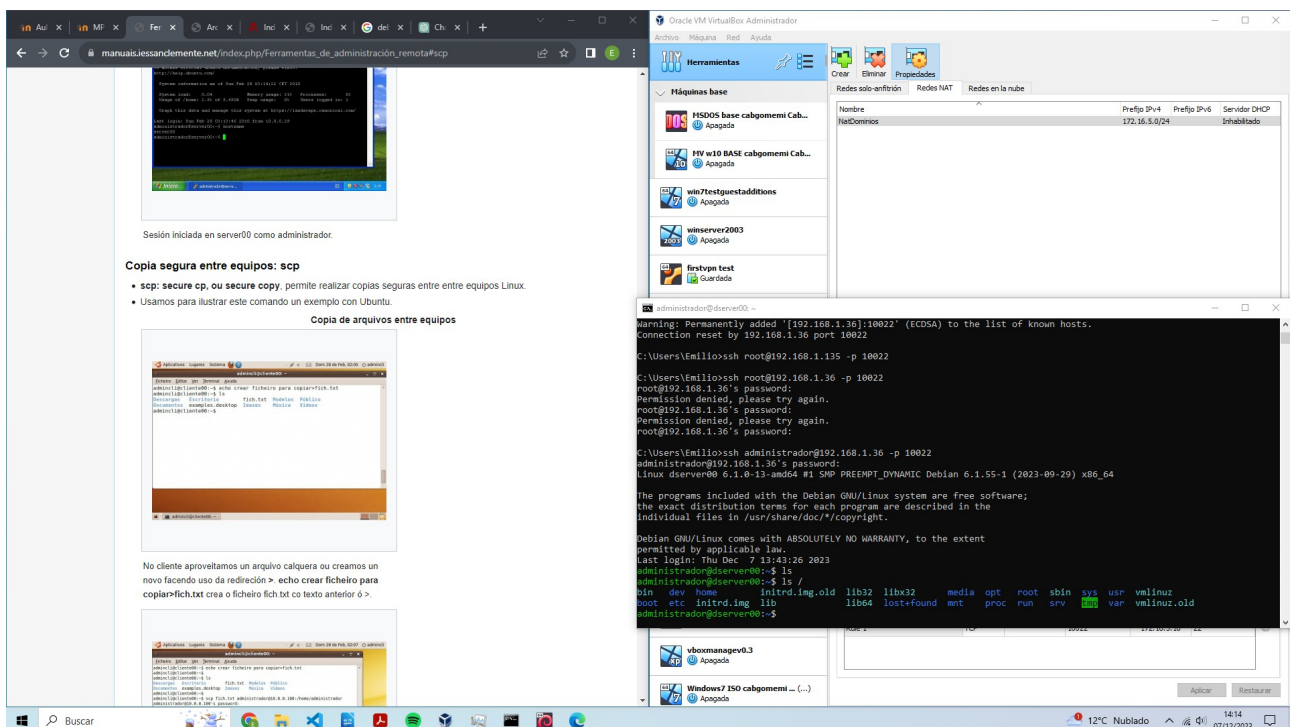
Introducimos el comando ssh [root@iphos](#) -p 10022

Introducimos yes y entramos en la máquina.

En la documentación del IES San Clemente nos indica que en el caso de que queramos realizarlo mediante un host windows necesitaremos un programa externo. Aunque ahora windows ya ofrece nativamente soporte para ssh. Incluso podemos instalar WSL.



Ssh output.



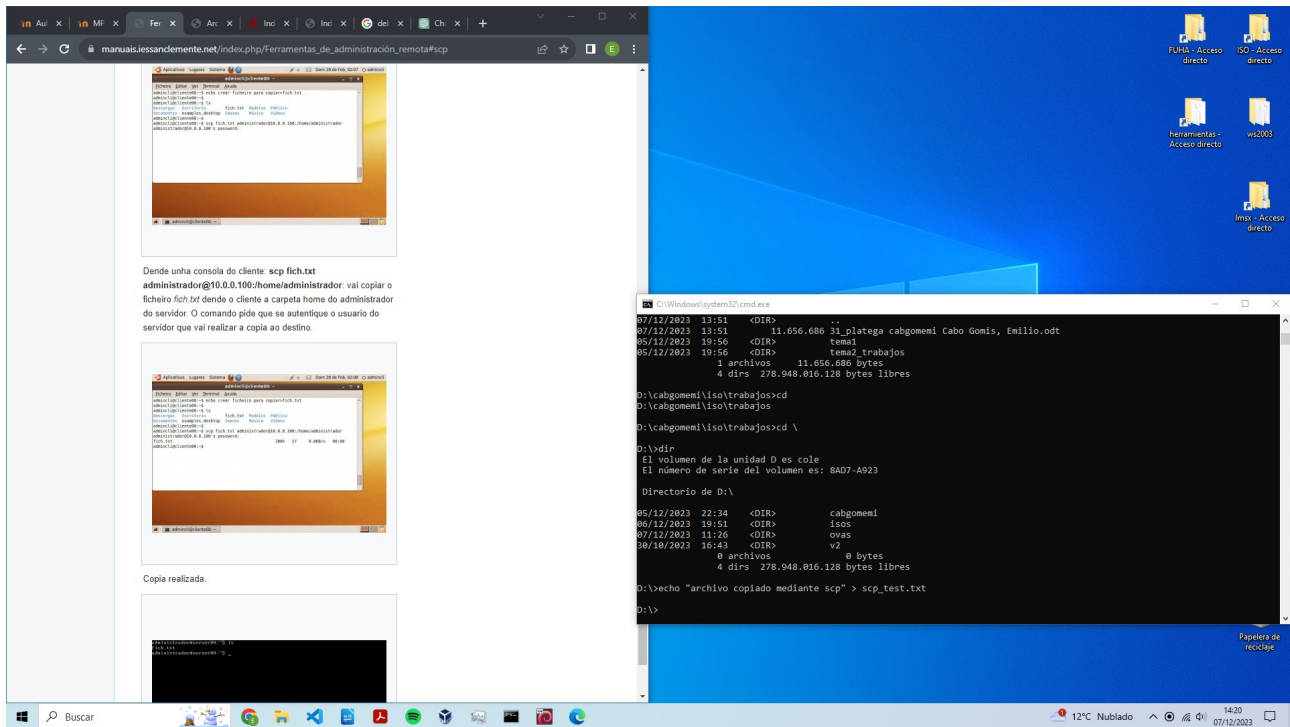
Administrando la máquina debian desde la máquina host.

Secure copy

Para copiar archivos de una máquina a otra de manera segura y remota emplearemos el comando SCP

Primero crearemos un archivo para copiar desde la máquina anfitriona.

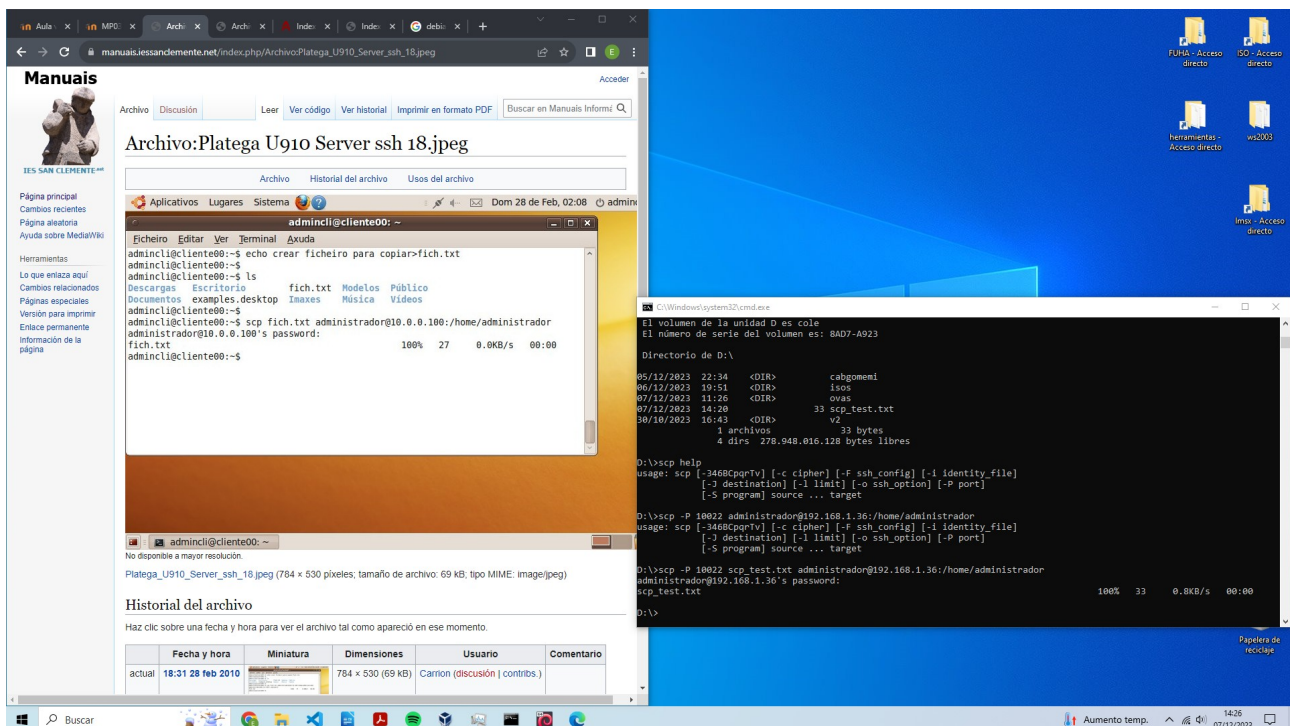
51 Platega I_II_III



Creación de un archivo para copiar.

Debemos recordar que debido a que estamos operando desde fuera de la red nat debemos especificar el puerto al que hacer el SCP.

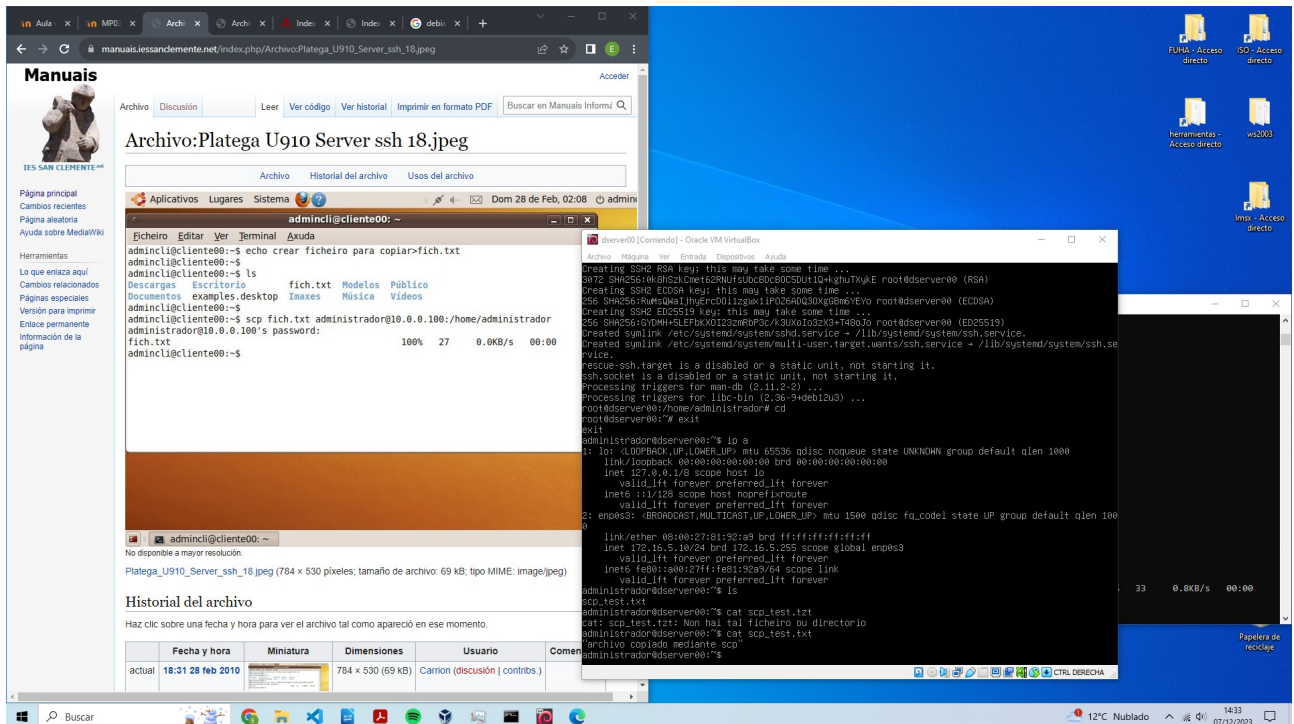
Lo copiaremos mediante el comando SCP de esta manera.



SCP comando.

51 Platega I_II_III

Comprobamos que el contenido del archivo es el correcto.

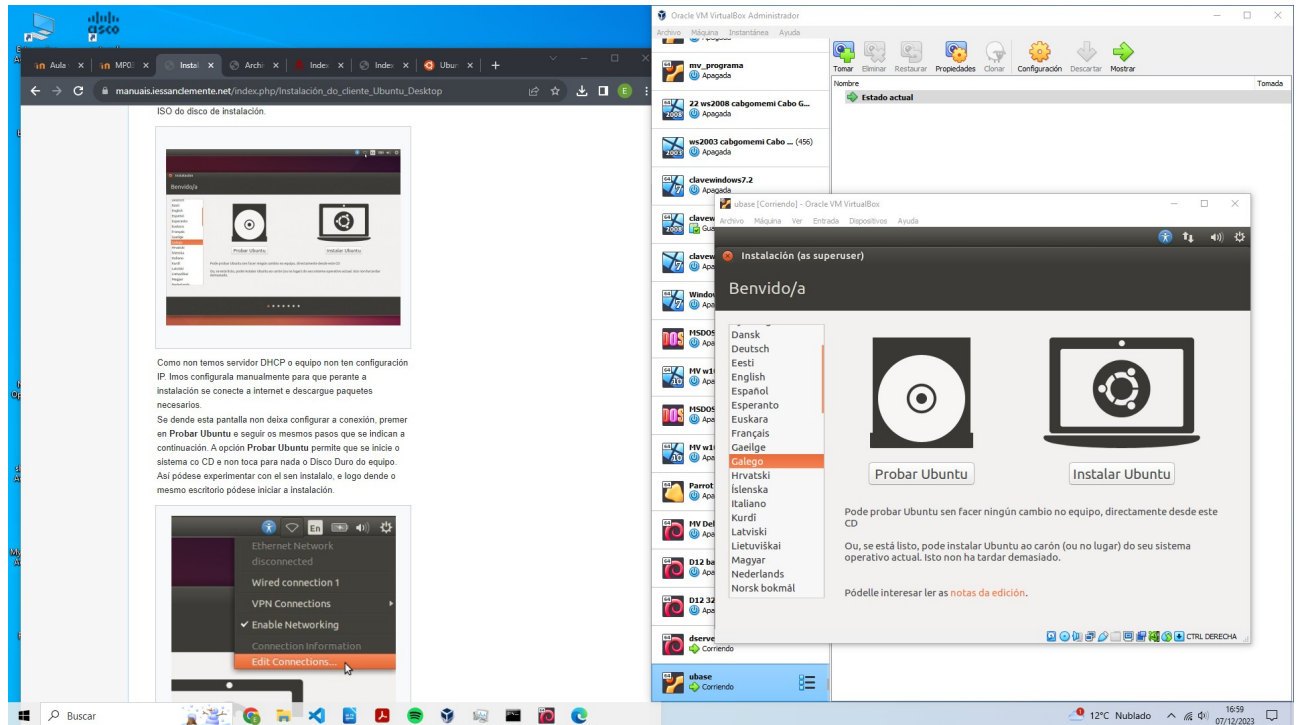


Comando SCP.

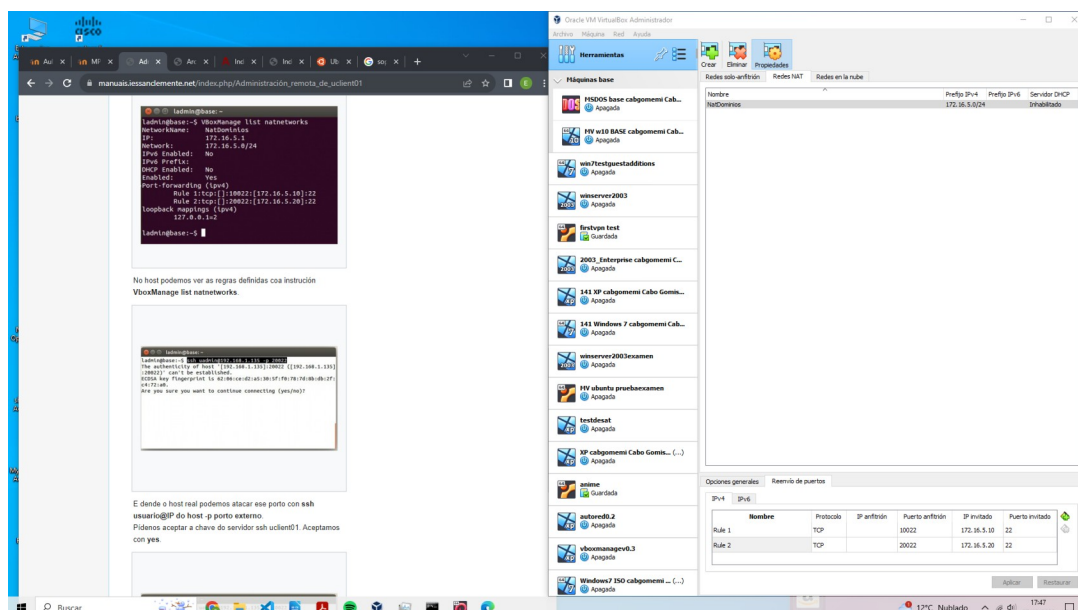
Trabajo con Ubuntu. Instalación y configuración

Creamos la máquina ubuntu base mediante el menú de configuración de virtualbox.

Menú de configuración de hardware.



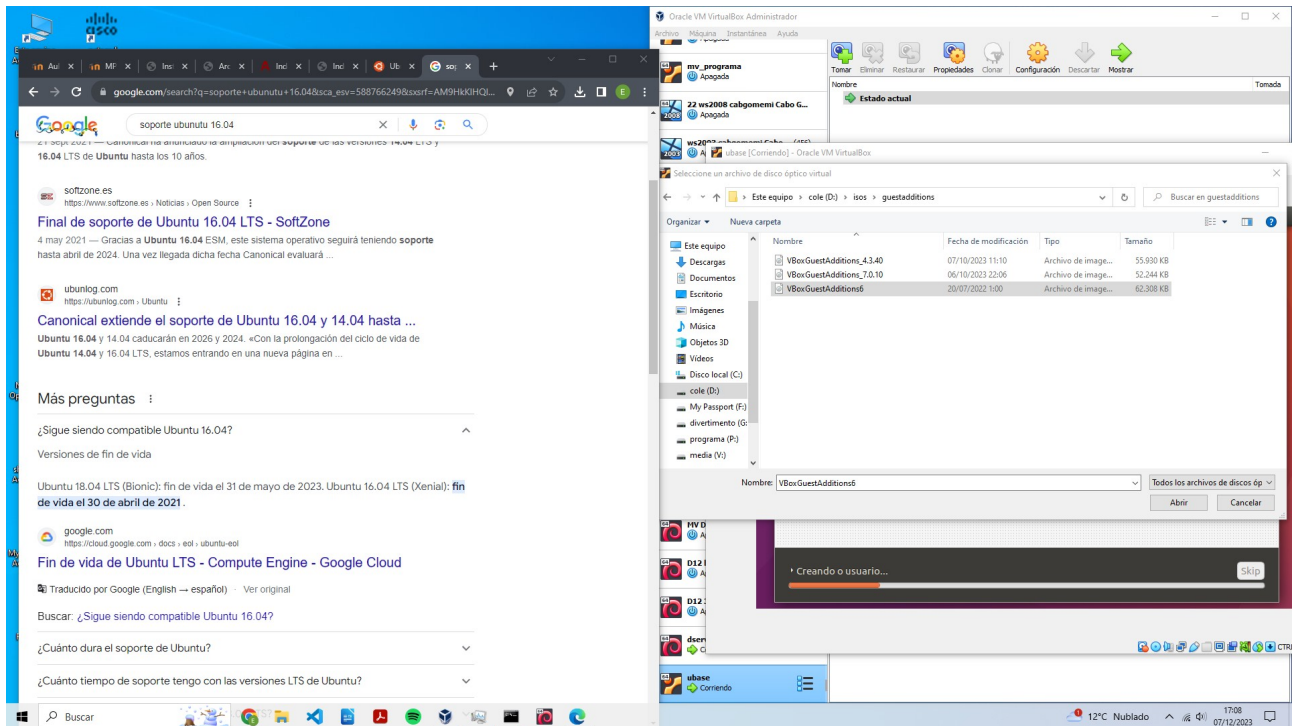
Instalamos el ubuntu mediante el menú del instalador. *Instalador ubuntu*



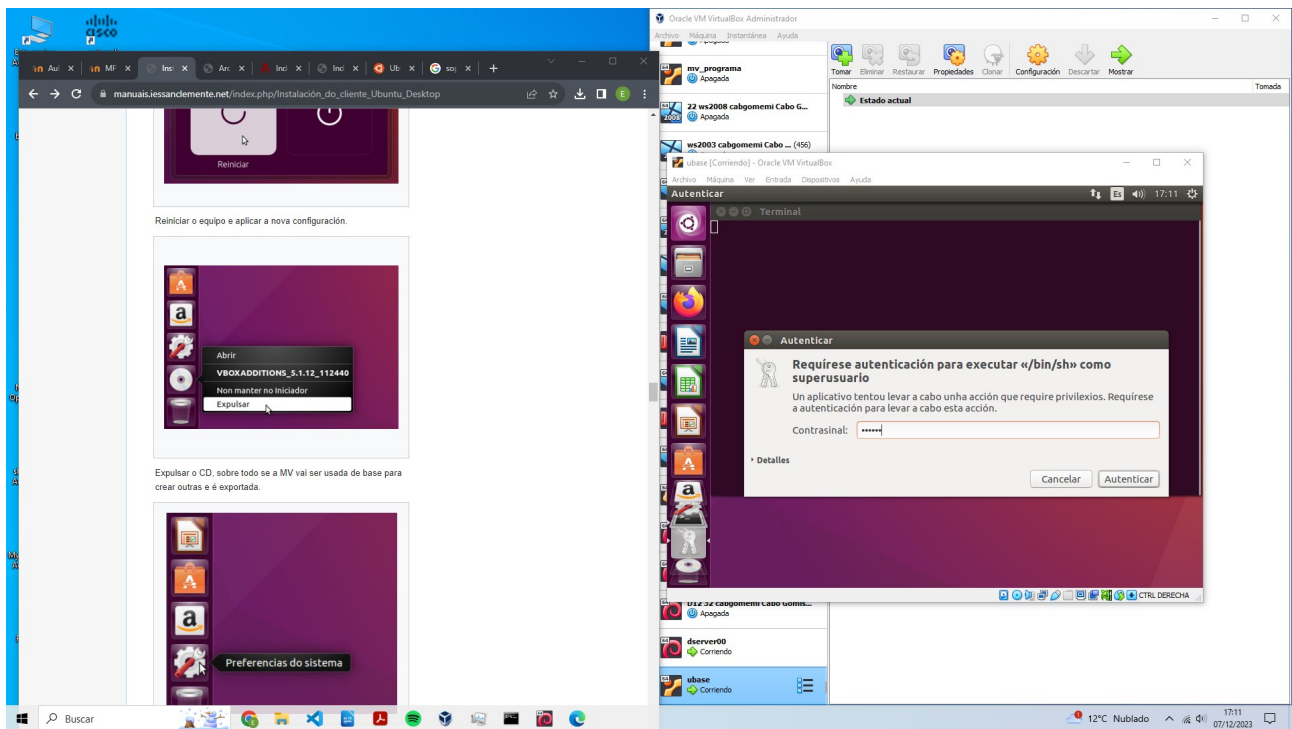
Instalamos las guest additions.

51 Platega I_II_III

Introducimos el CD de las guest additions y ejecutamos como programa su contenido.

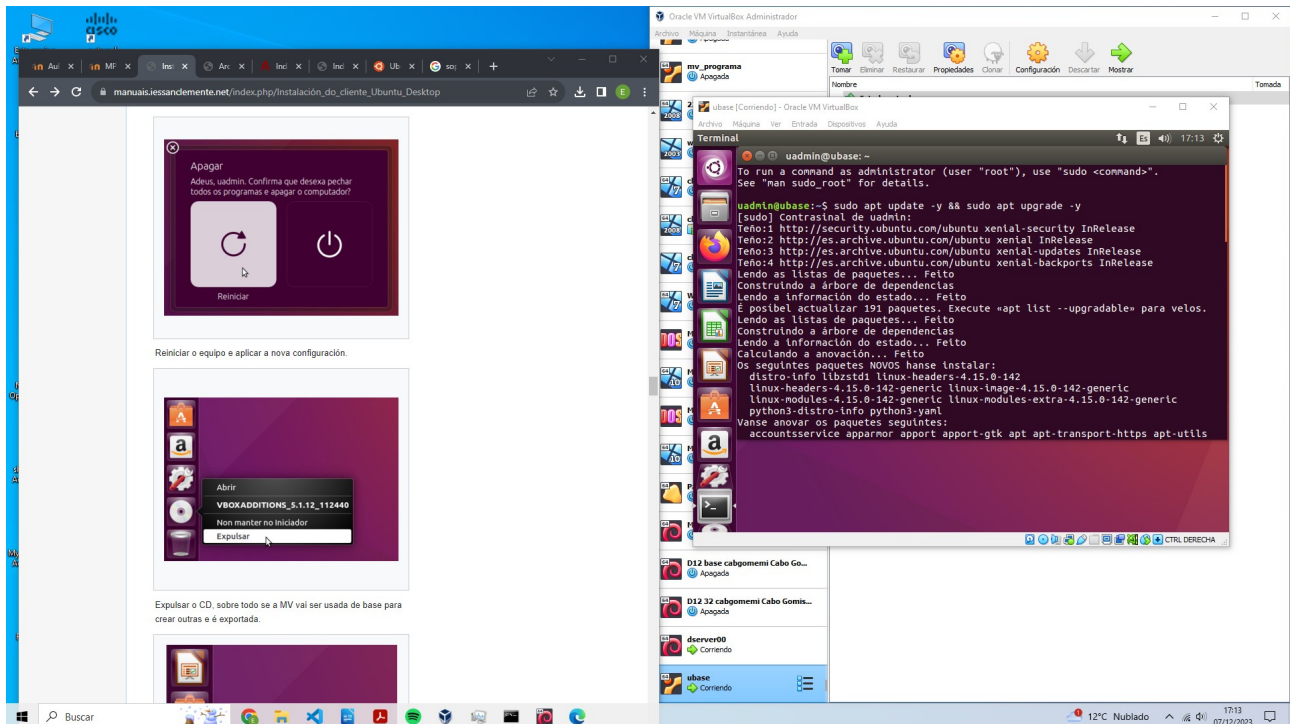


Seleccionado de las guest additions



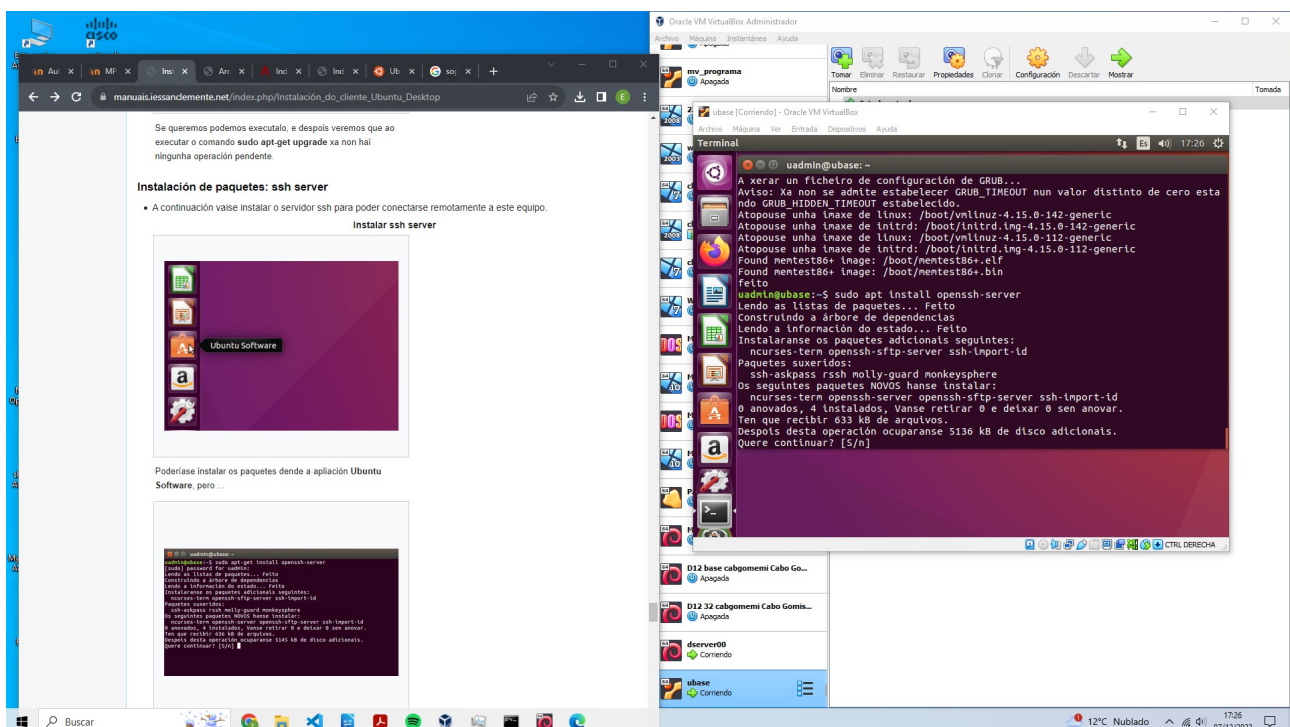
Instalar las guest additions.

Actualizamos el sistema mediante el comando **sudo apt update && sudo apt upgrade**



Output del comando.

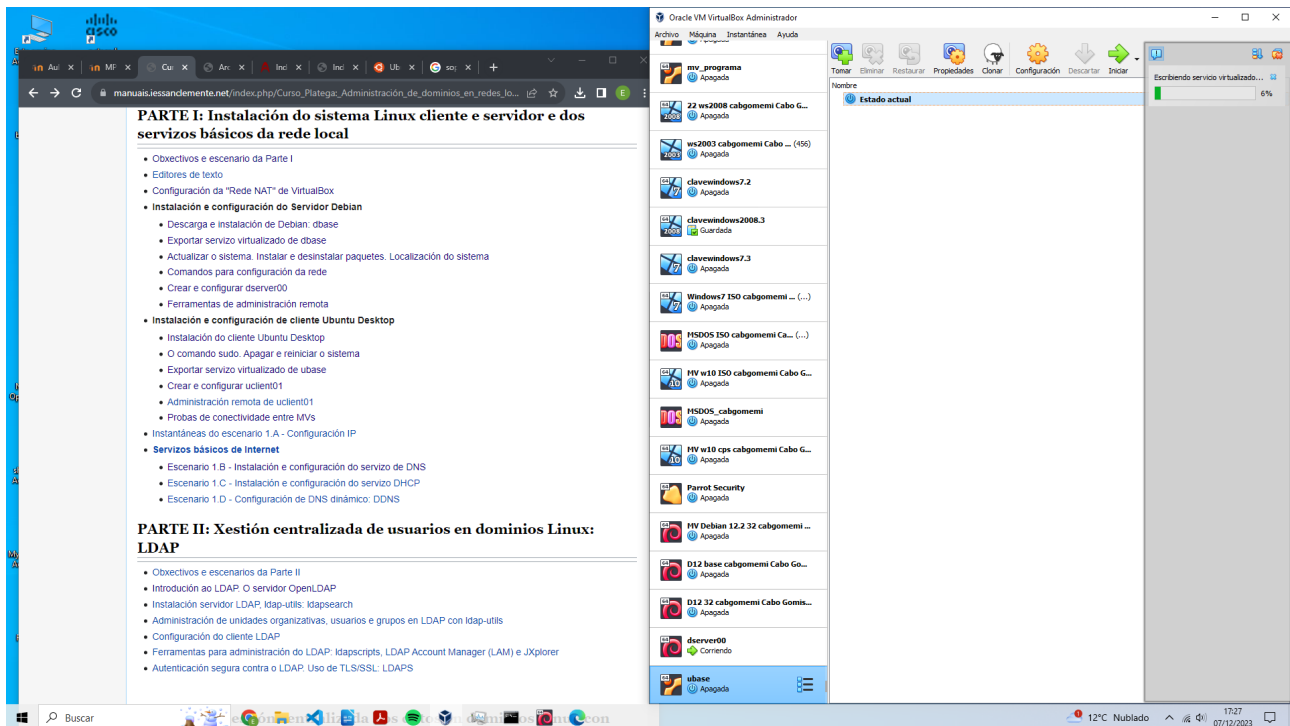
Instalamos el paquete **openssh-server**



Instalación del paquete **openssh server**.

Exportamos la OVA

Exportamos la máquina en formato OVA para poder utilizarla en otros trabajos como máquina base.



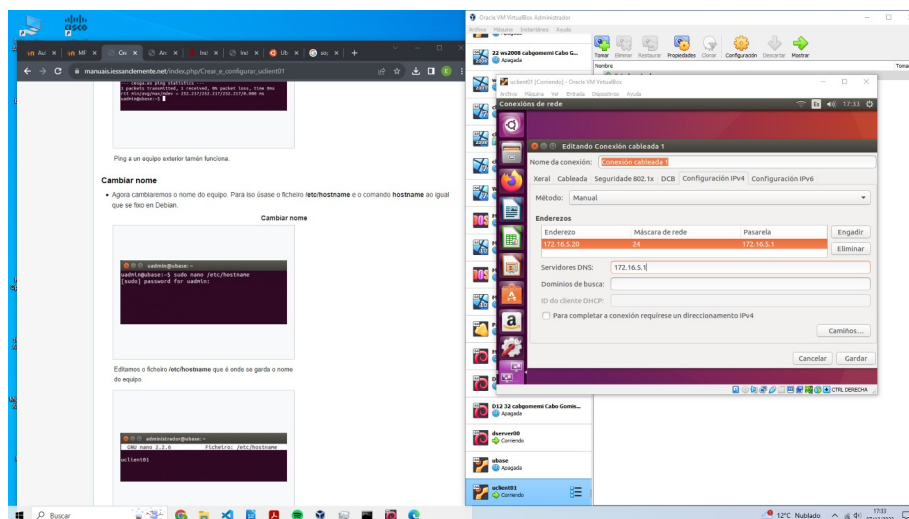
Máquina exportándose.

Creamos la máquina uclient01

Al crear la máquina regeneraremos la dirección MAC de la máquina.

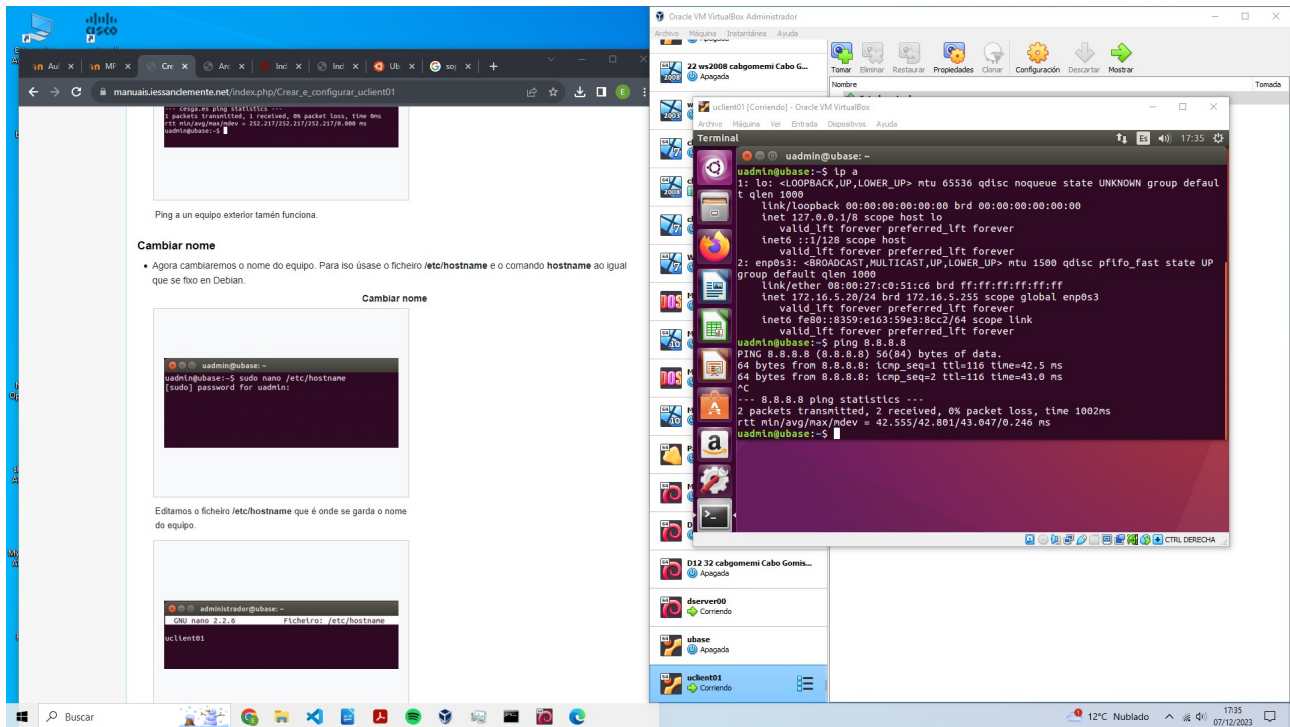
Configuración de red mediante la interfaz gráfica

Aplicamos la siguiente configuración de red.



Menú de configuración de red Ubuntu 16.04

Comprobamos la conectividad al exterior mediante el siguiente comando.

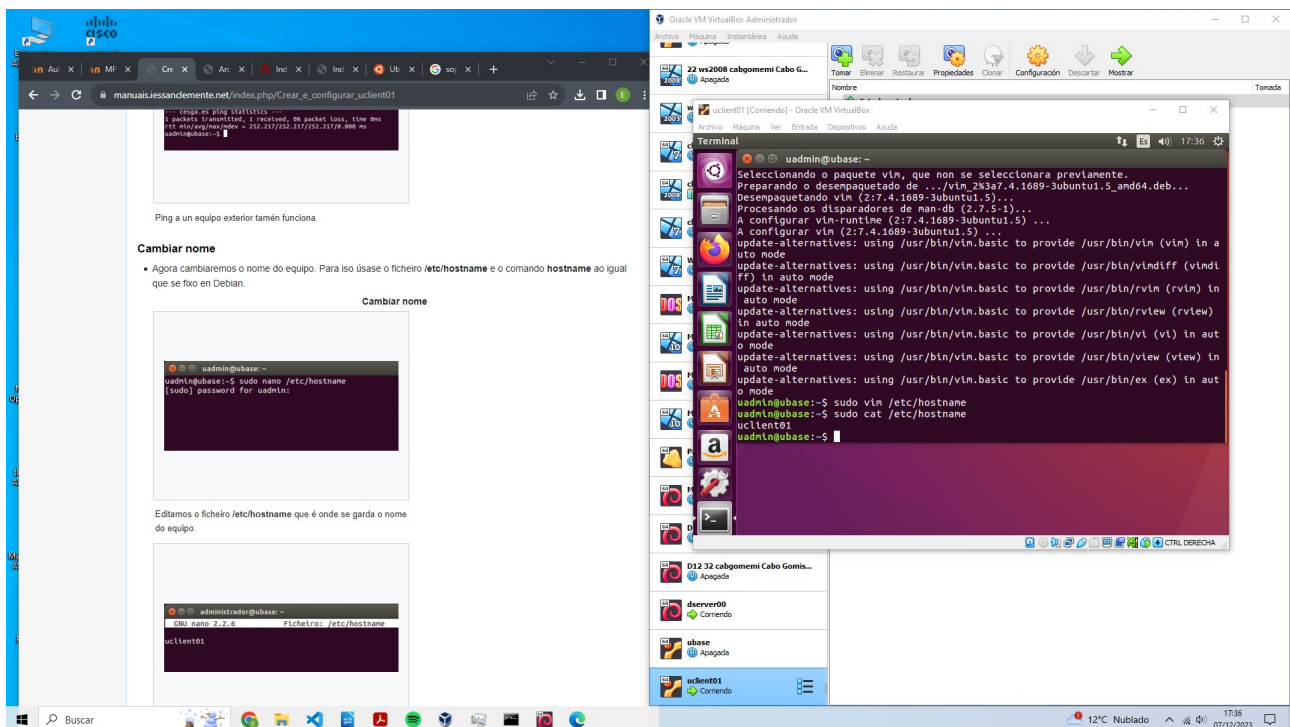


Output comando ping

Cambiado de hostname

Editamos el contenido del fichero /etc/hostname

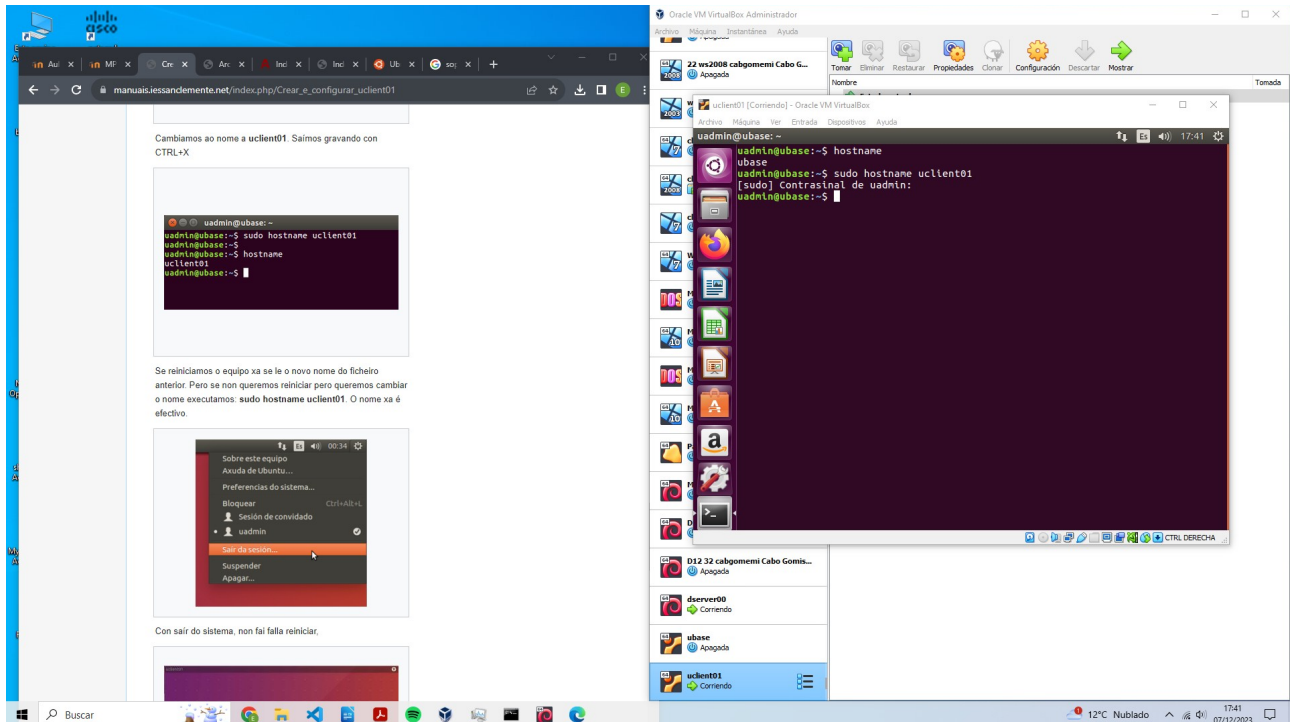
Introducimos el nombre uclient01



Contenido del fichero de configuración /etc/hostname.

Para que los cambios sean efectivos deberemos reiniciar el equipo.

Para cambiar el nombre de usuario sin salir de la sesión deberemos introducir el comando **sudo hostname ucllient01**



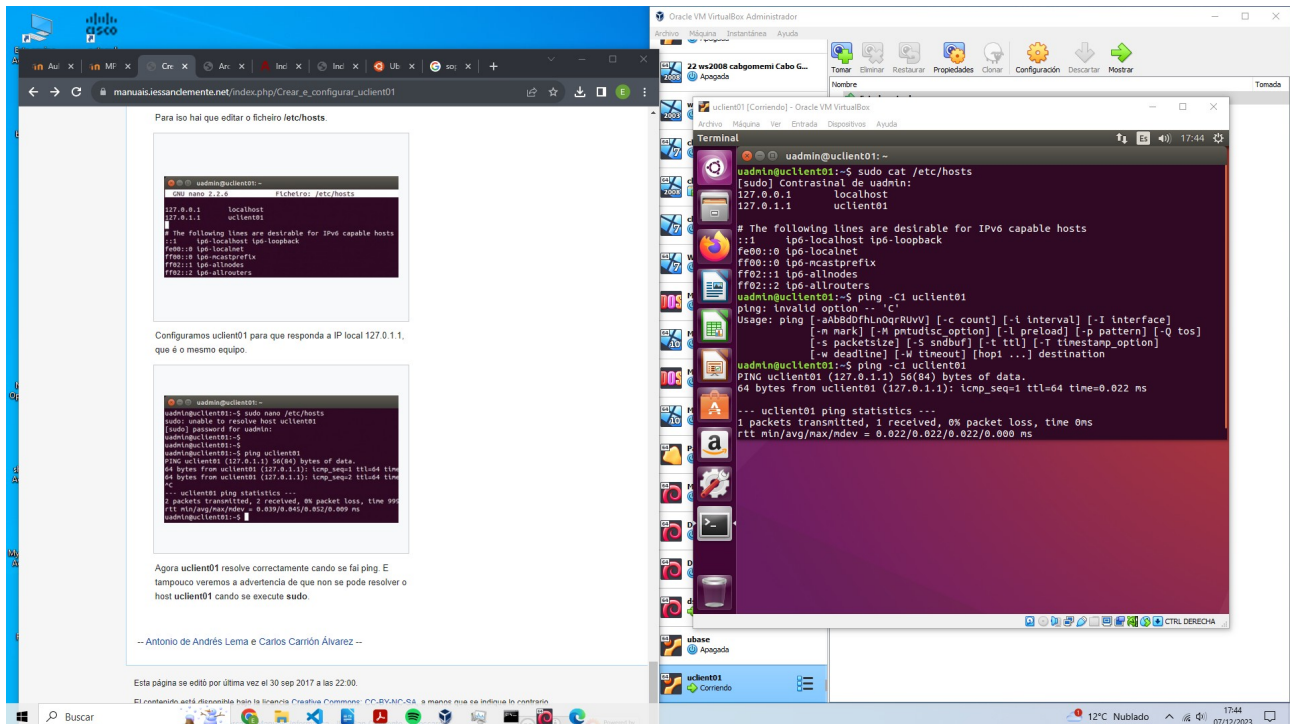
Output del comando

Editado fichero hosts

Editaremos este archivo para que al hacer ping nos responda nuestro equipo.

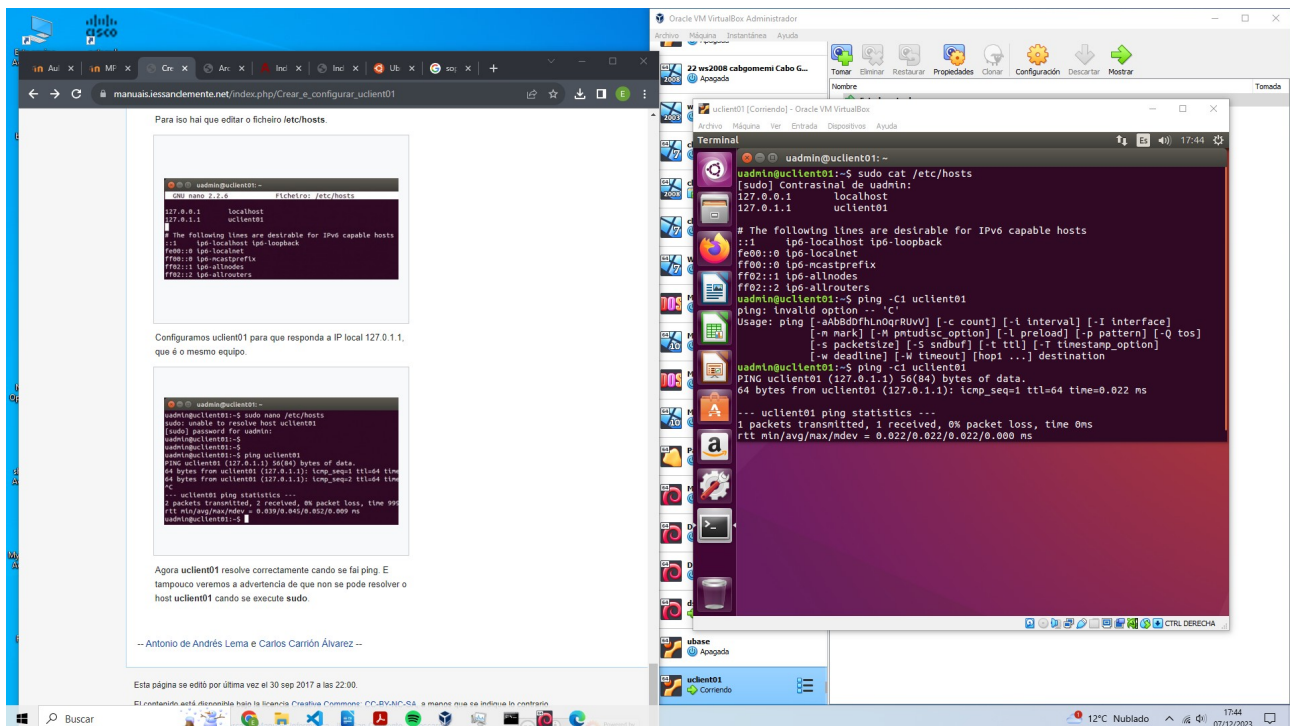
Este archivo se utiliza para resolver nombres de host a direcciones IP localmente antes de recurrir a los servidores DNS.

Editamos el archivo `/etc/hosts` para que tenga el siguiente contenido.



Contenido `/etc/hosts`

Comprobamos que la máquina es capaz de resolver el nombre.



Output del comando `ping`.

Administración remota del servidor

Redireccionamiento de puertos

Para poder acceder desde el exterior al interior de la red NAT es necesario que configuremos una regla en nuestra red nat.

La configuraremos de la siguiente manera.

Entraremos en el menú en el que configuramos la red NAT anteriormente > reenvío de puertos.

Aplicaremos la siguiente regla:

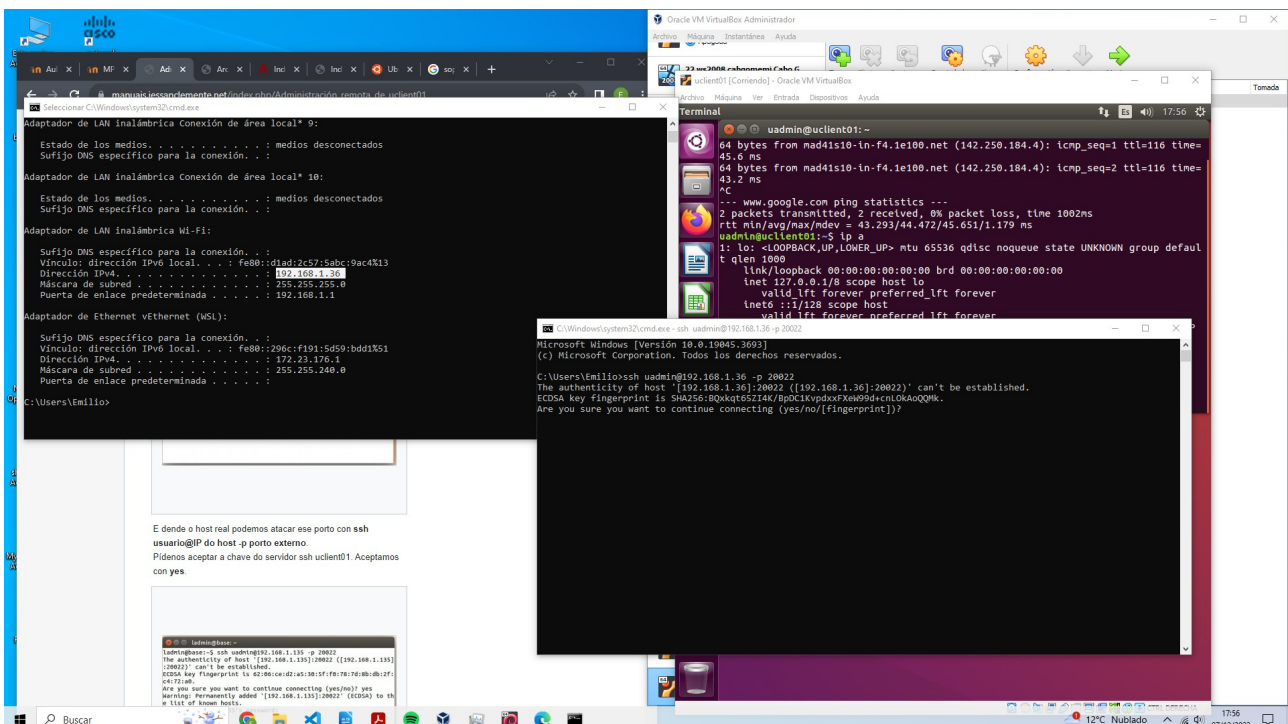
Menú configuración reenvío de puertos.

Inicio de sesión mediante ssh

Introducimos el comando `ssh uclient@iphost -p 20022`

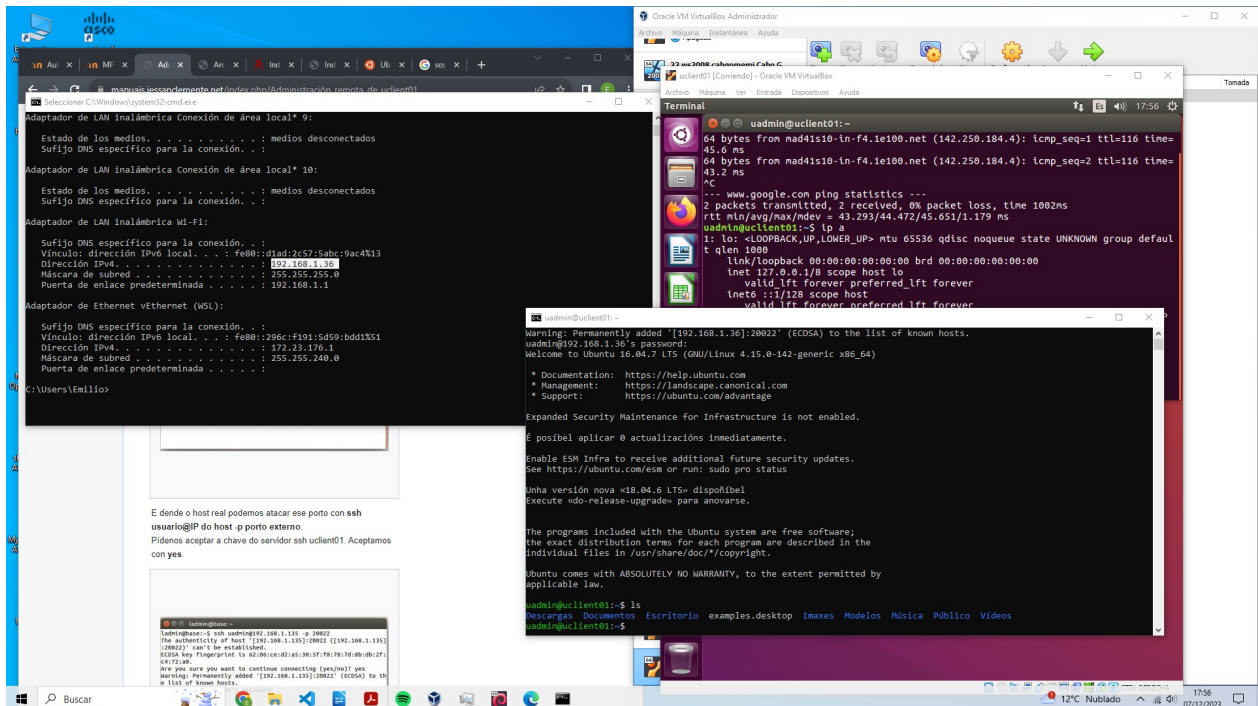
Introducimos yes y entramos en la máquina.

En la documentación del IES san clemente nos indica que en el caso de que queramos realizarlo mediante un host windows necesitaremos un programa externo. Aunque ahora windows ya ofrece nativamente soporte para ssh. Incluso podemos instalar WSL.



Output de la primera conexión de ssh.

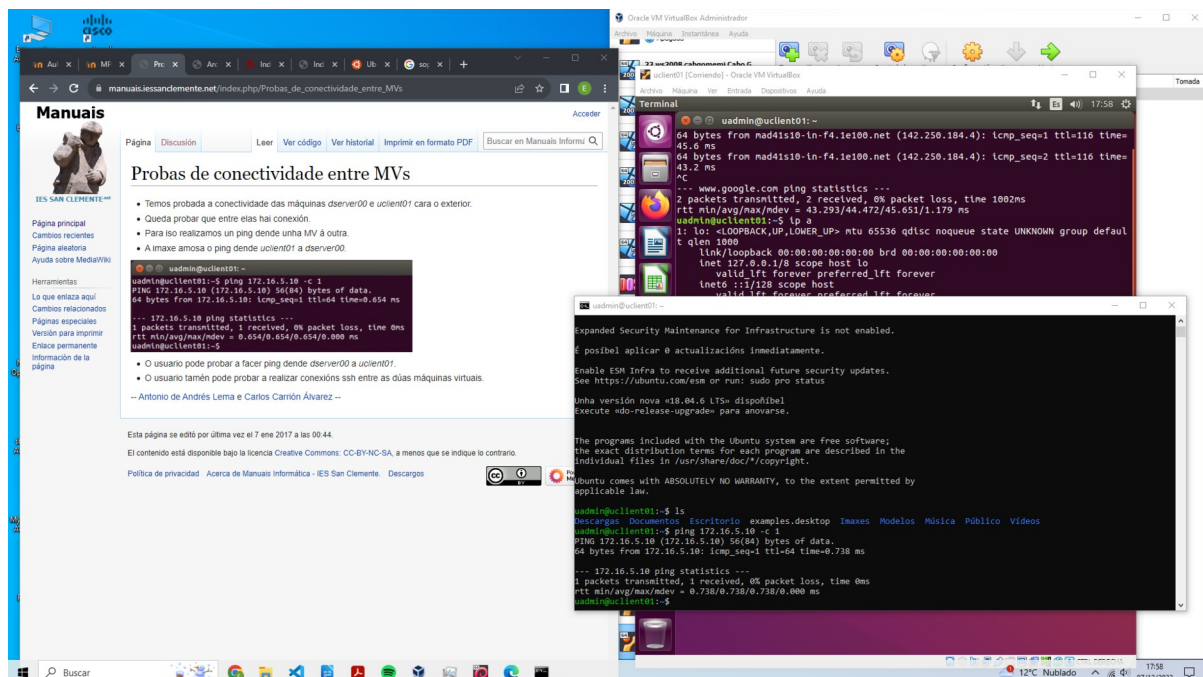
Hacemos click en yes. Comprobamos que efectivamente podemos administrar la máquina remotamente desde el exterior de la red NAT.



Máquina uclient1 siendo administrada remotamente mediante la máquina host.

Conectividad entre las máquinas

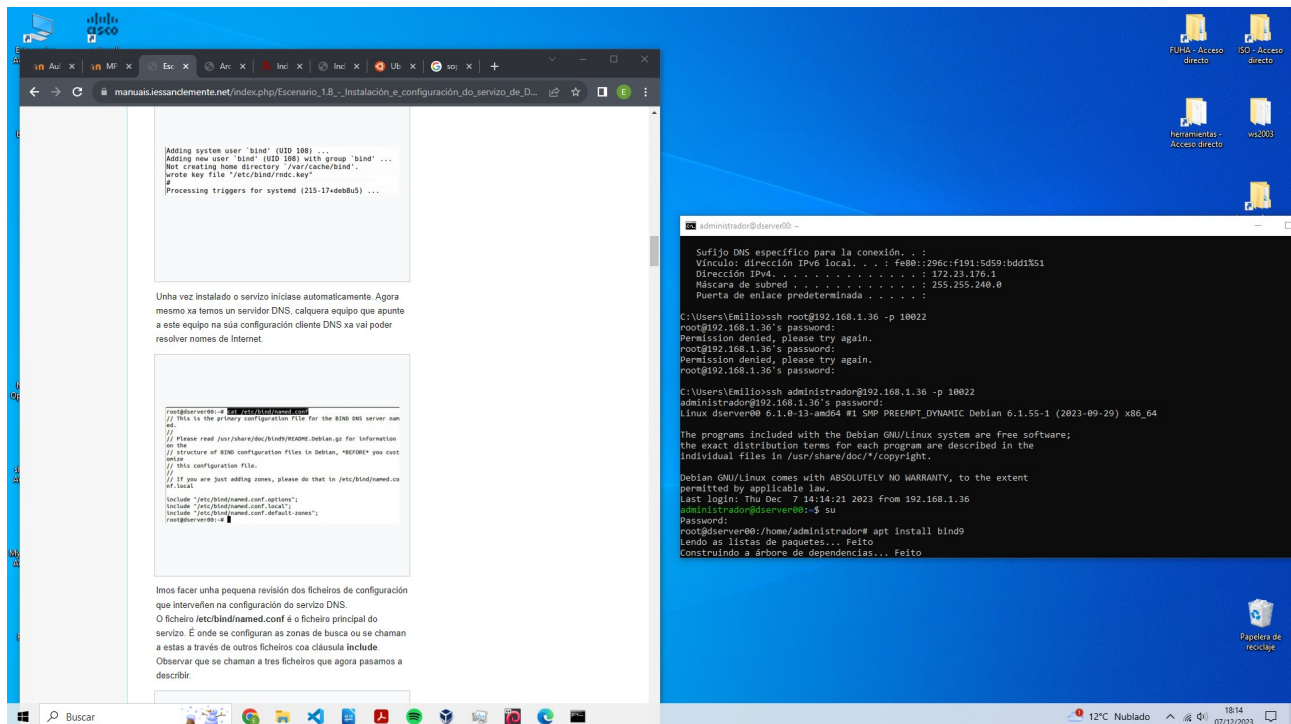
Mediante esta comprobación hemos verificado que las máquinas pueden ser tanto administradas remotamente mediante la redireccionamiento de puertos tanto que podemos realizar una comunicación entre ambas máquinas.



Ping entre las dos máquinas de manera remota.

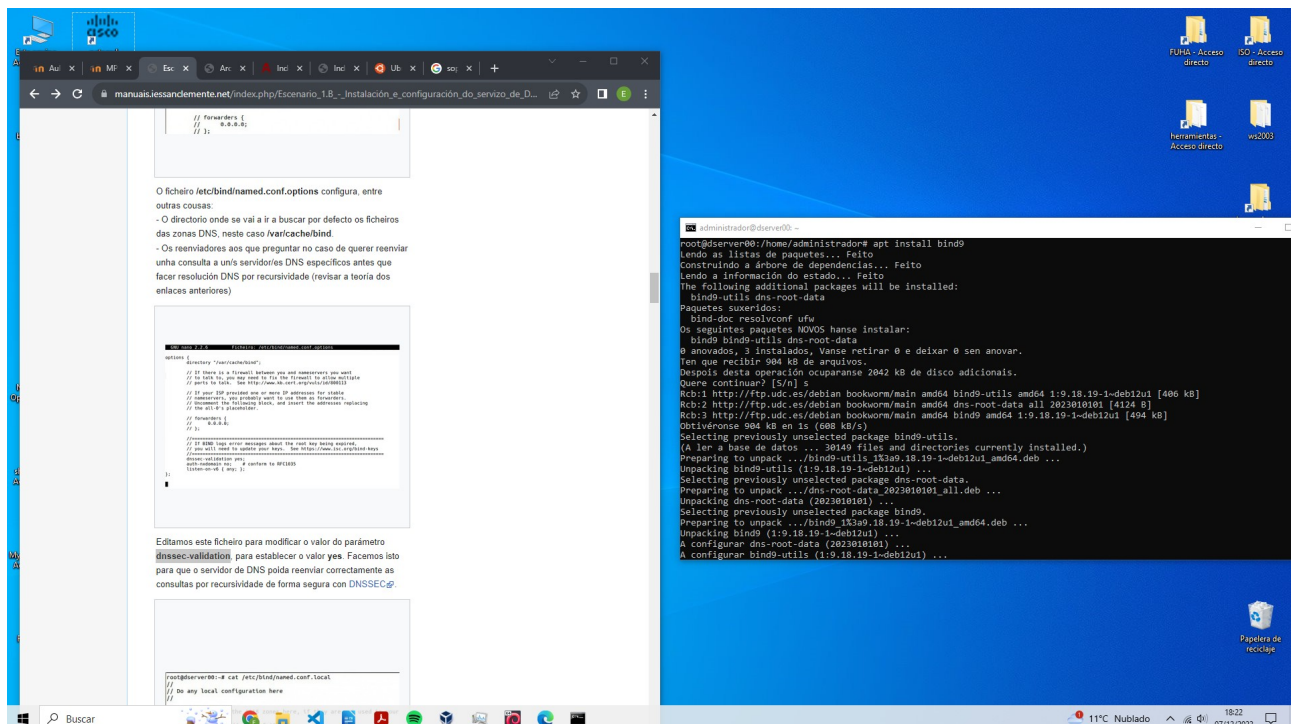
Configuración del servidor DNS

Iniciamos sesión desde la máquina host a la máquina virtual servidor.



Inicio de sesión mediante la máquina host.

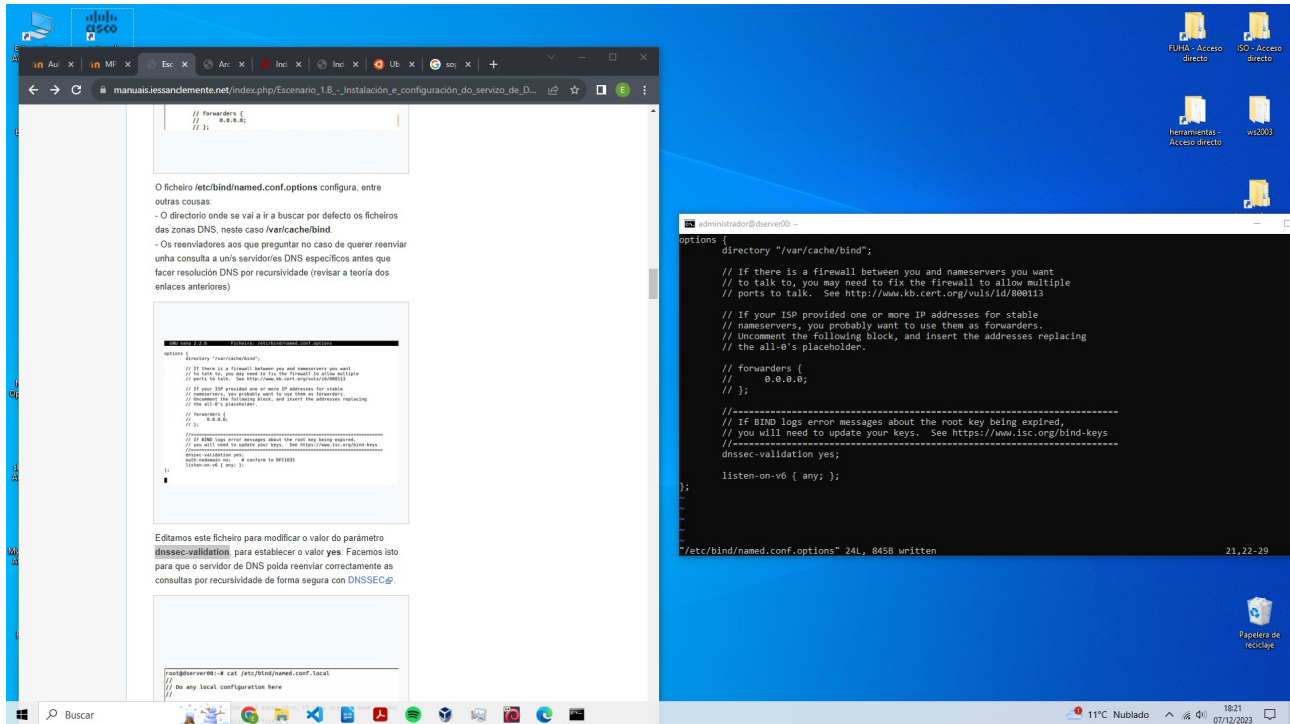
Instalamos el paquet bind9 para la administración remota.



Resultado de la instalación.

Editamos el archivo `/etc/bind/named.conf.options`

Nos aseguramos que en la línea **dnssec-validation** ponga **yes**



Archivo `/etc/bind/named.conf.options`

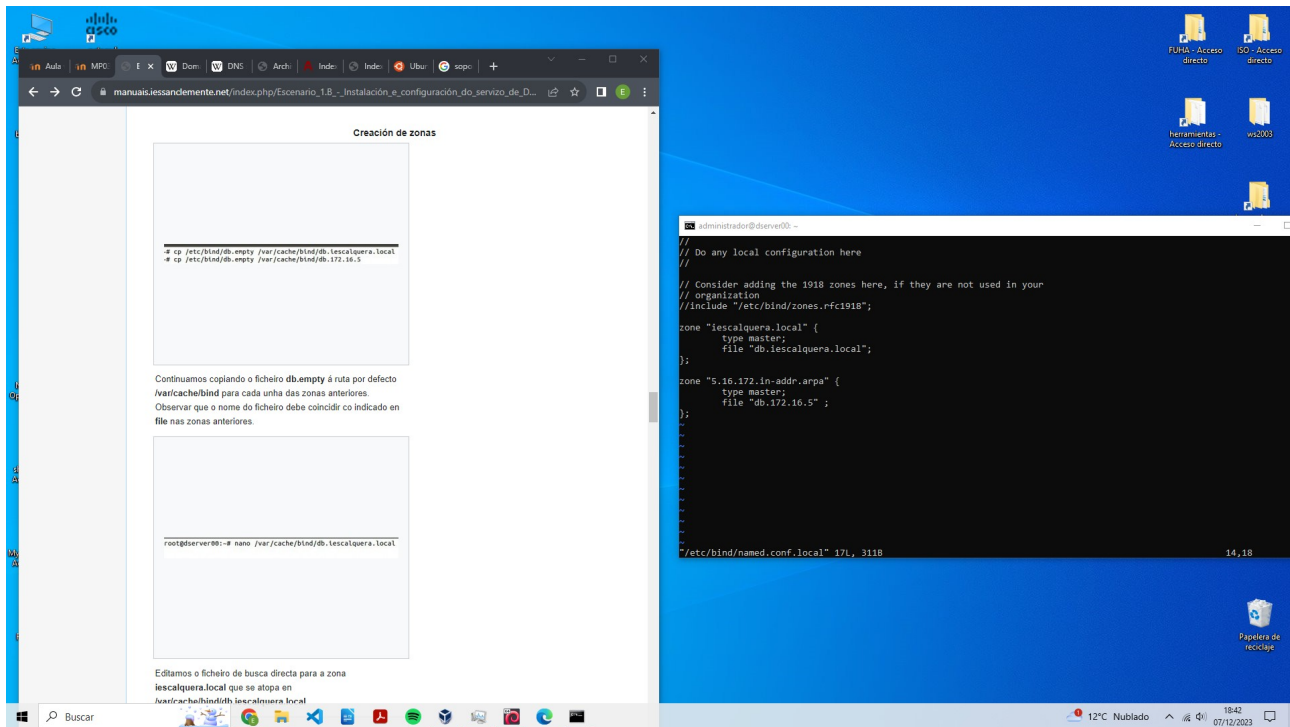
Creación de zonas directa e inversa

Crearemos una zona directa e inversa,

La zona directa es para traducir direcciones IP a nombres de dominio iescalquera.local

La zona inversa es para traducir nombres de equipos para la red 172.16.5.XX.

Añadimos las siguientes líneas al archivo de configuración.



Configuración servidor DNS.

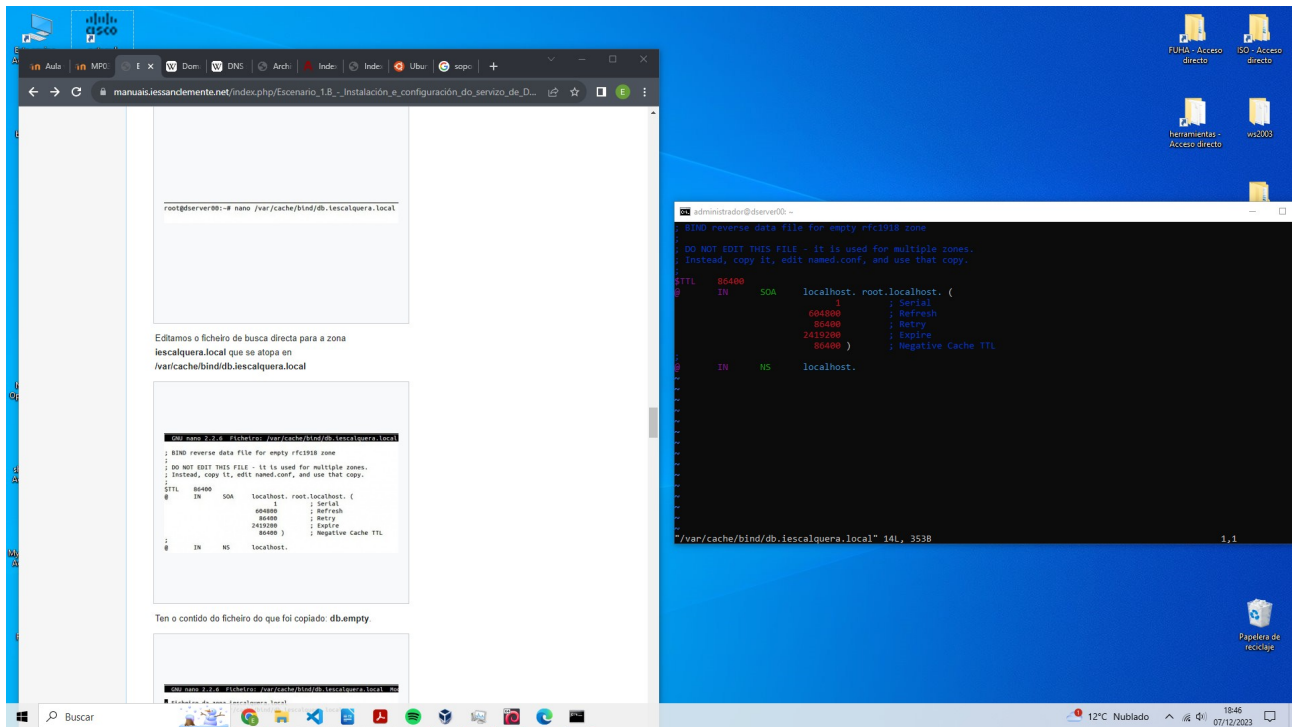
Configuración de zonas directa e inversa

Ejecutamos el siguiente comando:

```
cp /etc/bind/db.empty /var/cache/bind/db.iescalquera.local
```

```
cp /etc/bind/db.empty /var/cache/bind/db.172.16.5
```

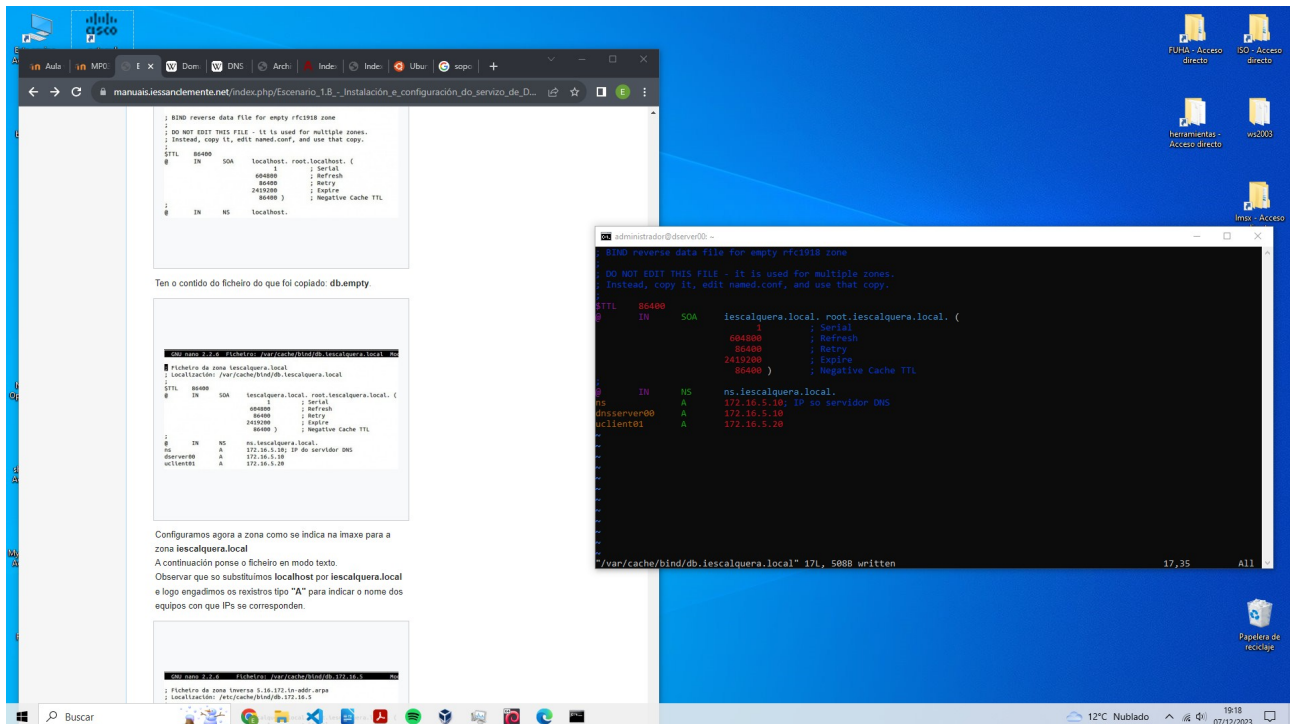
Editamos el fichero /var/cache/bind/db.iescalquera.local



Versión default.

Aplicaremos la siguiente configuración.

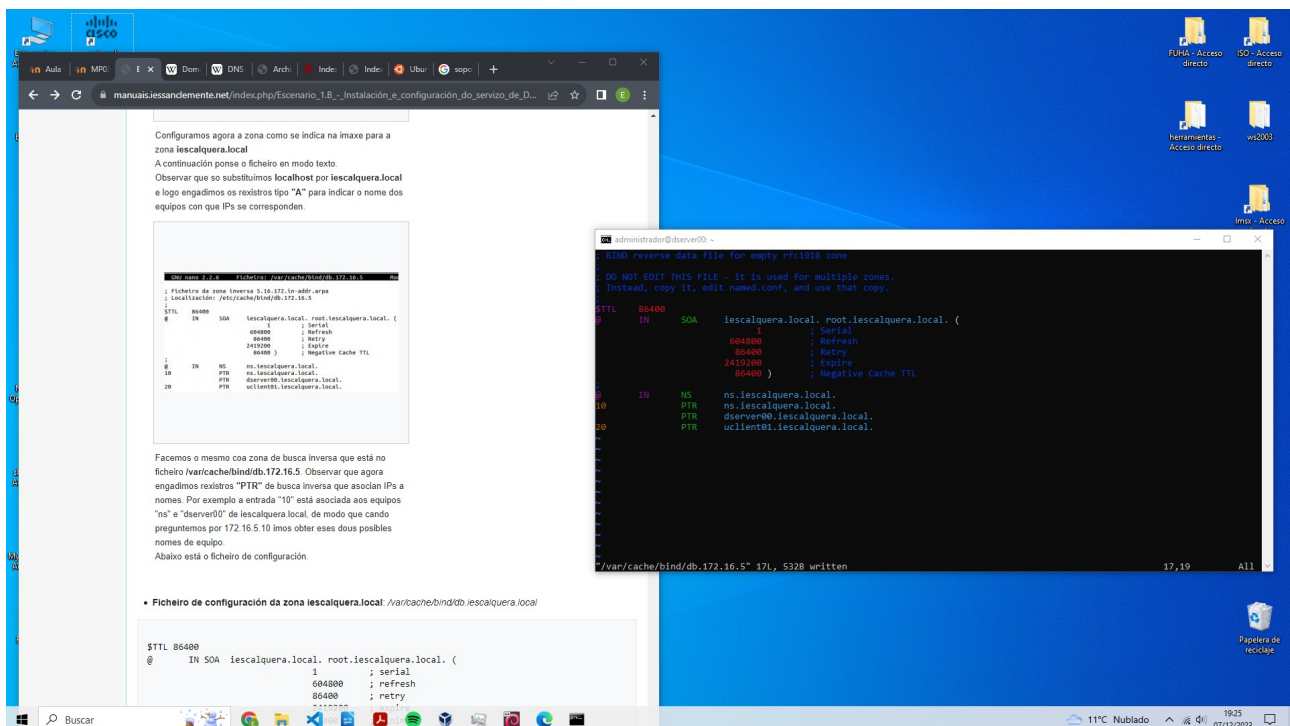
Lo que estamos haciendo aquí es relacionar direcciones IP con nombres.



Configuración definitiva fichero /var/cache/bind/db.iescalquera.local

Ahora realizaremos la configuración inversa del DNS

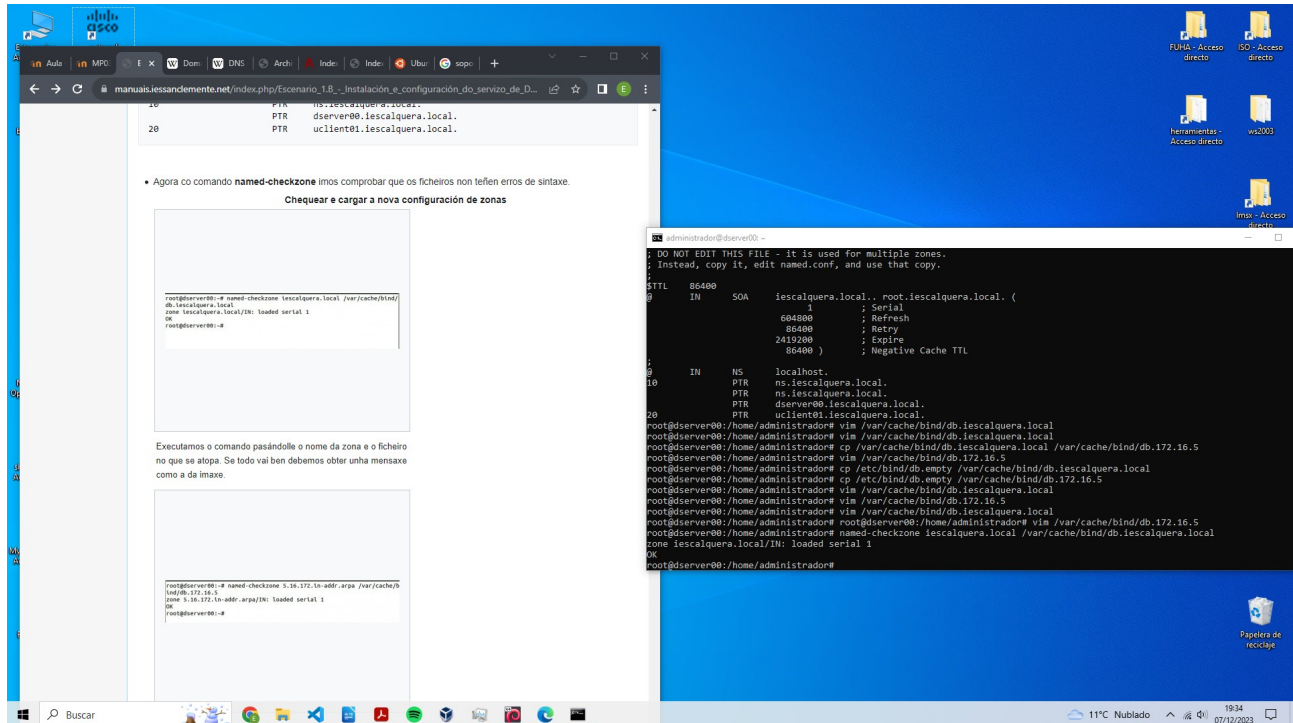
Debemos recordar que lo que estamos haciendo en este fichero es relacionar inversamente direcciones IP terminadas en 10 con dserver00 y direcciones IP terminadas en 20 con uclient01.



Configuración definitiva del fichero /var/cache/bind/db.iescalquera.local

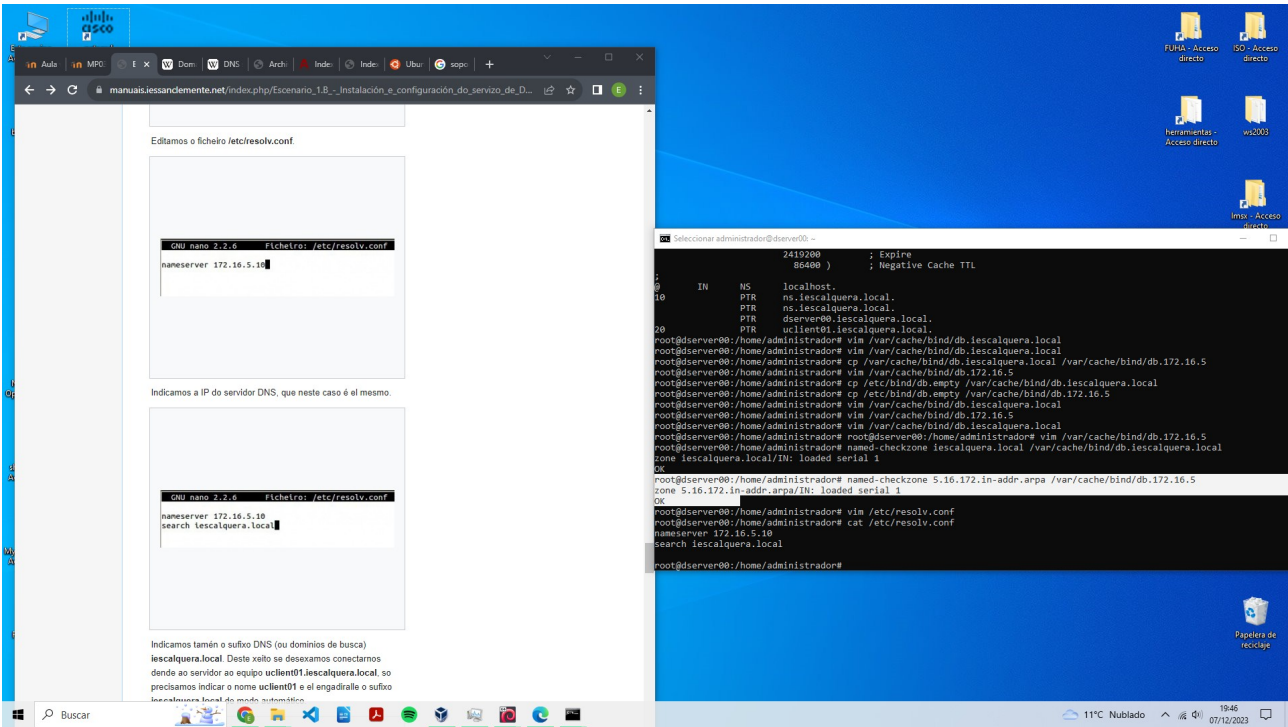
Comprobación de sintaxis de ficheros de configuración.

Comprobamos el primer fichero mediante el comando **named-checkzone iescalquera.local /var/cache/bind/db.iescalquera.local**



Comprobación de sintaxis del primer fichero de configuración.

Comprobamos el segundo fichero mediante el comando. **named-checkzone 5.16.172.in-addr.arpa /var/cache/bind/db.172.16.5**

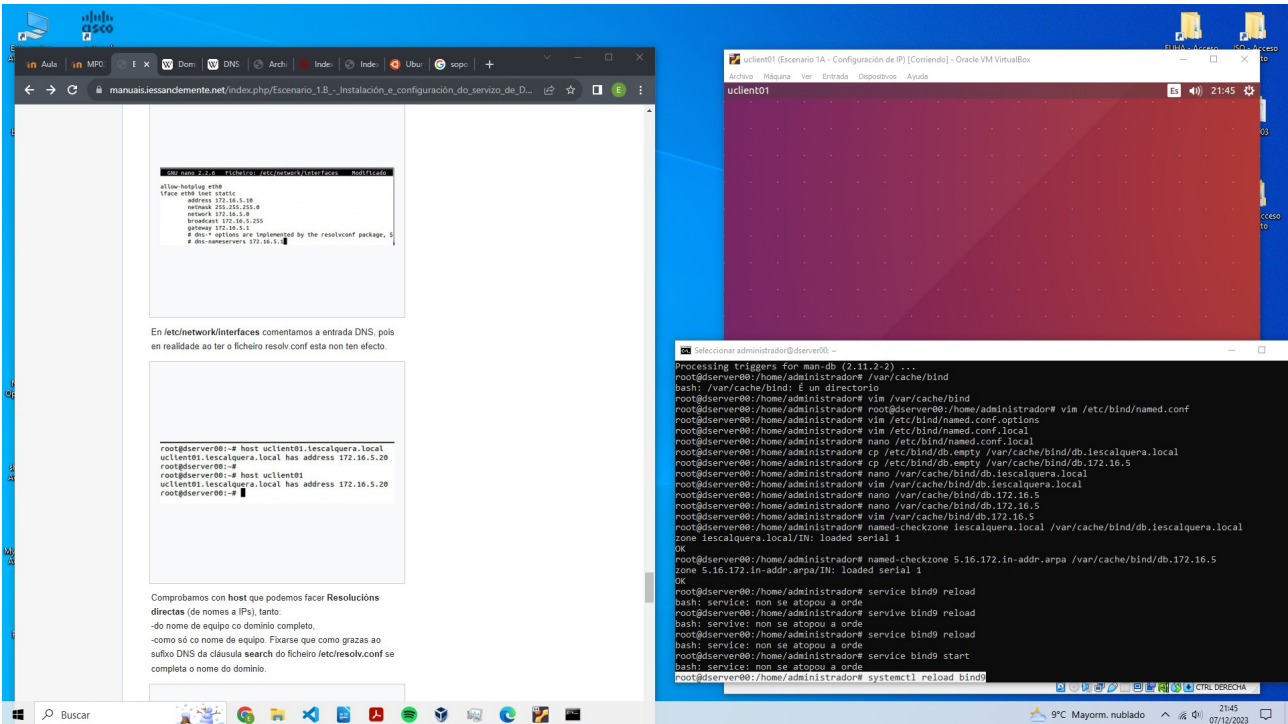


Comprobación de sintaxis del segundo fichero de configuración.

Reload bind9

Recargamos la configuración del server mediante el comando

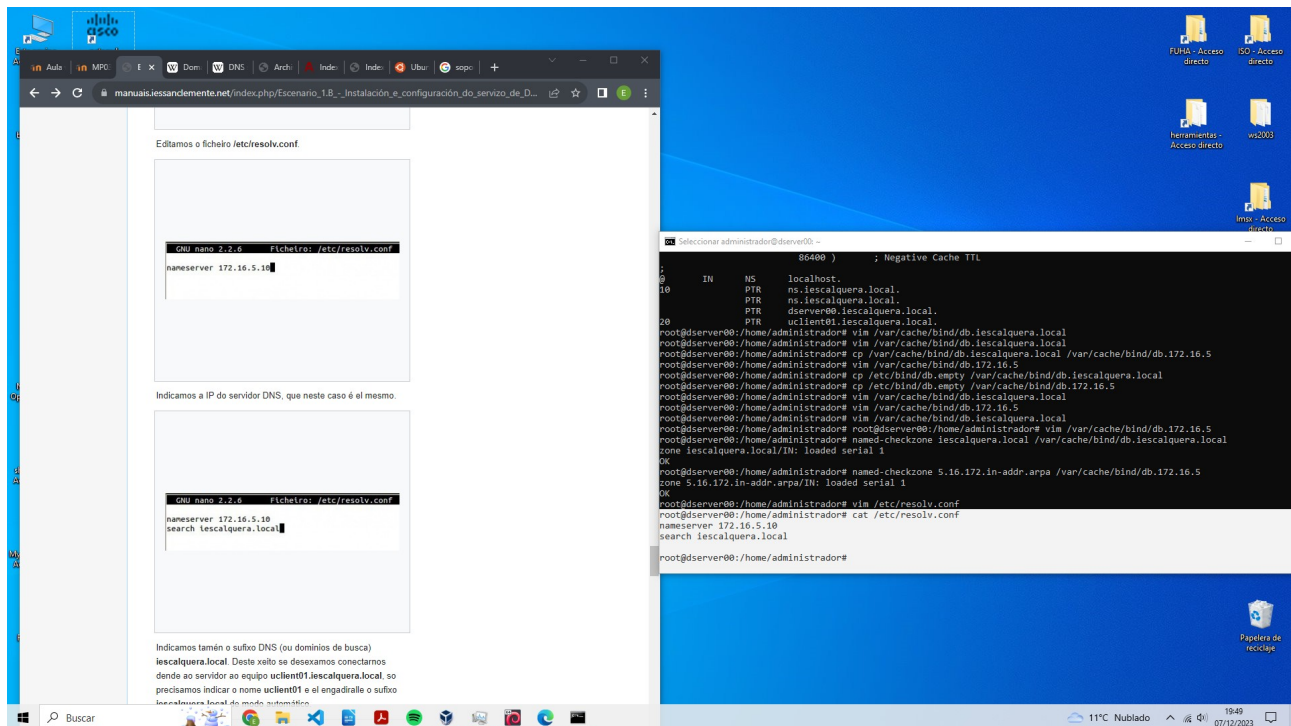
```
systemctl bind9 reload.
```



Output del reinicio.

Configuración client-side servidor DNS

Editamos el fichero `/etc/resolv.conf` para configurar nuestro servidor DNS



Configuración del fichero `/etc/resolv.conf`

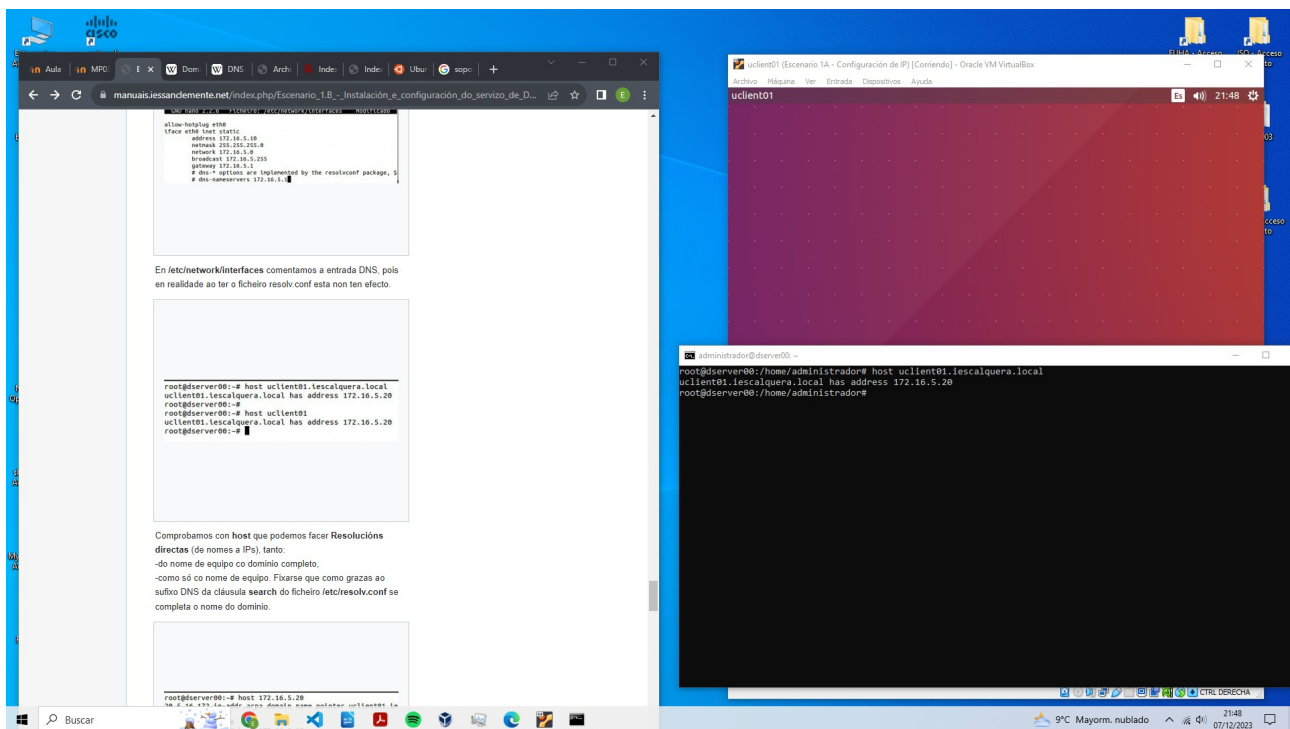
**La sección search es para que en caso de que queramos referirnos al uclient01 se autocomplete mediante el resolv.conf*

Comprobación del funcionamiento del DNS

Comprobamos la correcta funcionalidad del DNS mediante los siguientes comandos.

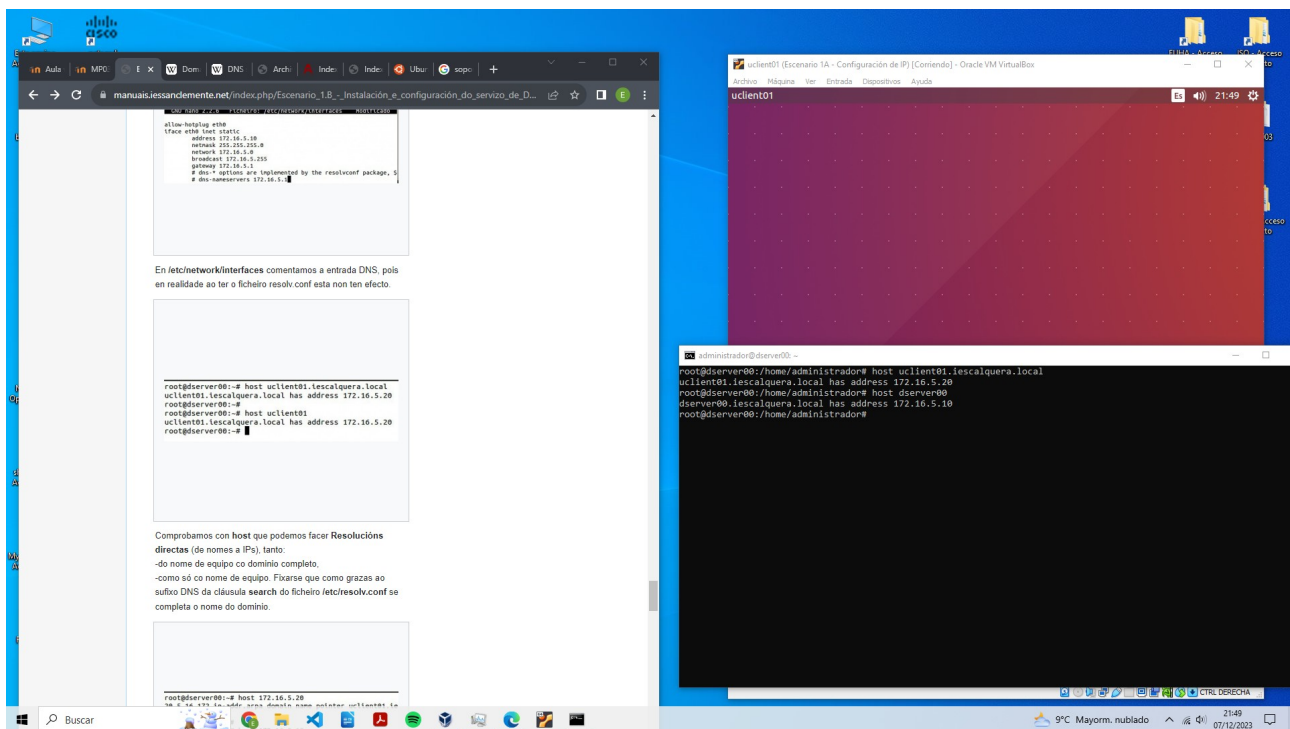
host uclient01.iescalquera.local

51 Platega I_II_III



Output test

host dserver00

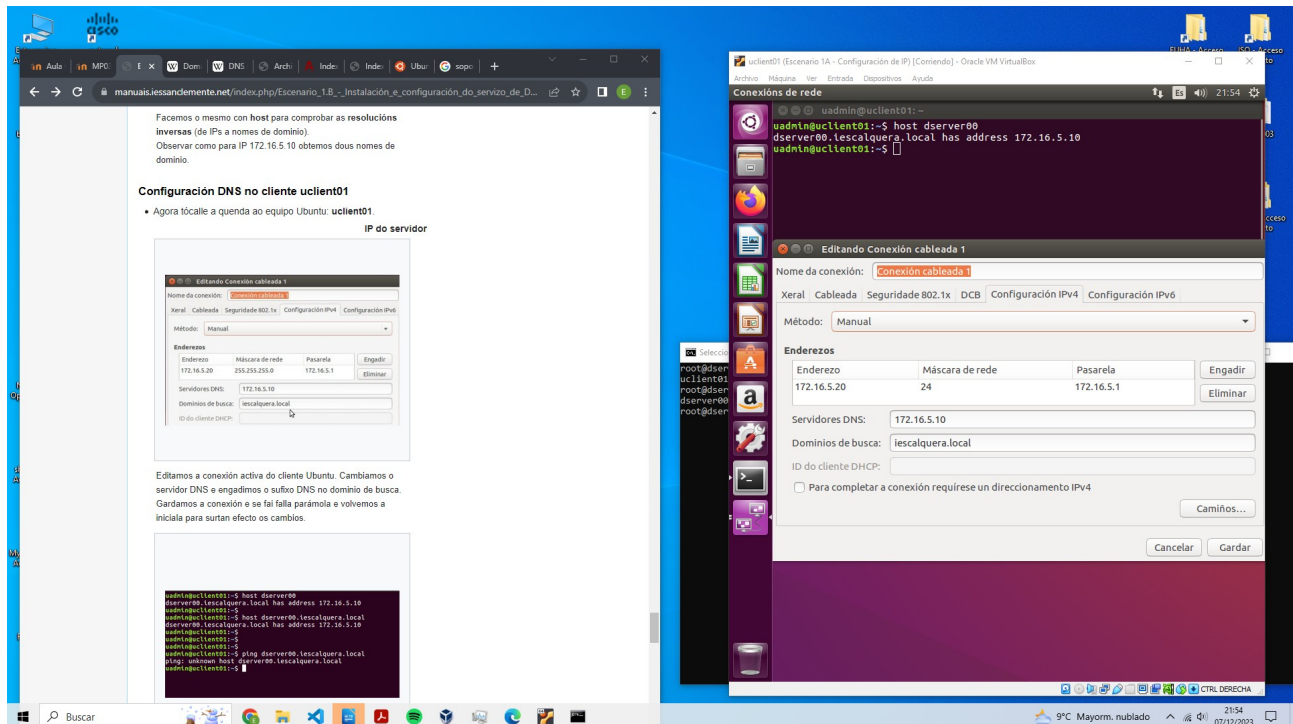


Output test

Configuración del DNS en el cliente:

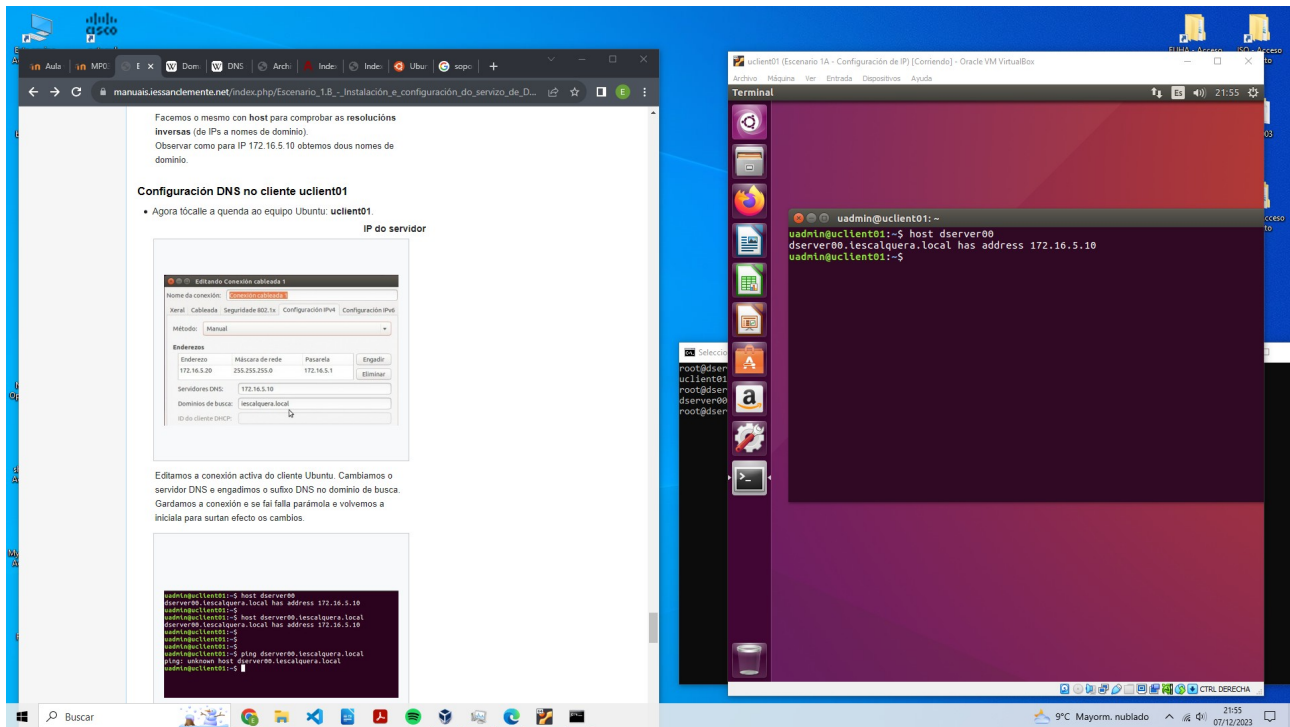
Configuramos el dominio de búsqueda mediante la edición de la conectividad aplicando la siguiente configuración en el menú de configuración de red gráfico.

En caso de querer hacerlo mediante comandos, dado que ubuntu está basado en Debian lo haríamos de la misma manera.



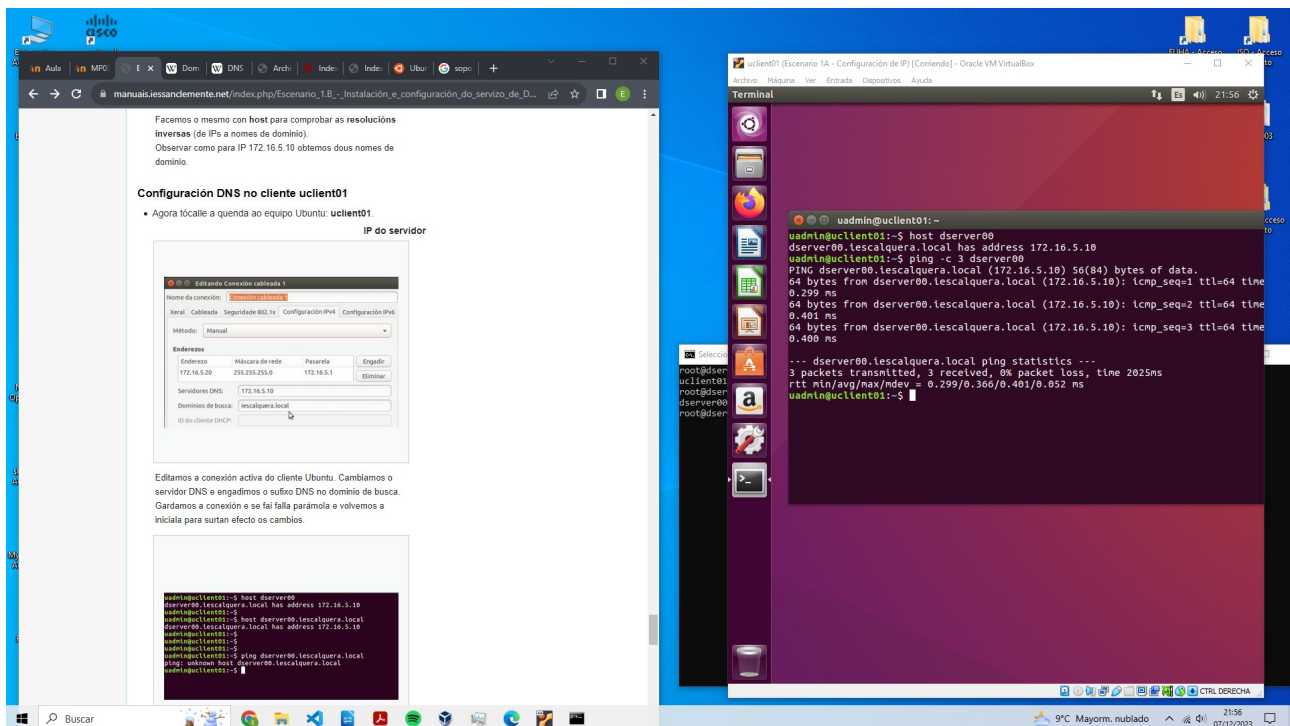
Dominio de búsqueda.

Comprobamos que es capaz de resolver los nombres aplicando los mismos comandos.



Output test

Intentamos realizar un ping.



Output test

Escenario 1-C

Instalación y configuración de servicio de DHCP (server-side) Debian.

Iniciamos la máquina Debian para empezar a trabajar con ella.

Instalaremos el servicio de DHCP.

The screenshot shows a web browser on the left displaying a tutorial for installing DHCP on Debian. The tutorial text includes instructions to use `apt-get install isc-dhcp-server` and mentions that the service will fail to start without a configured IP range. On the right, a terminal window shows the command `apt-get install isc-dhcp-server` being executed. The output shows the installation of the `isc-dhcp-server` package and its dependencies. Below the installation output, the terminal shows the command `systemctl start isc-dhcp-server` being executed, which results in a failure. The error message indicates that the service failed to start because the control process exited with an error code. The terminal also shows the command `systemctl status isc-dhcp-server` being executed, which shows the service is in a failed state.

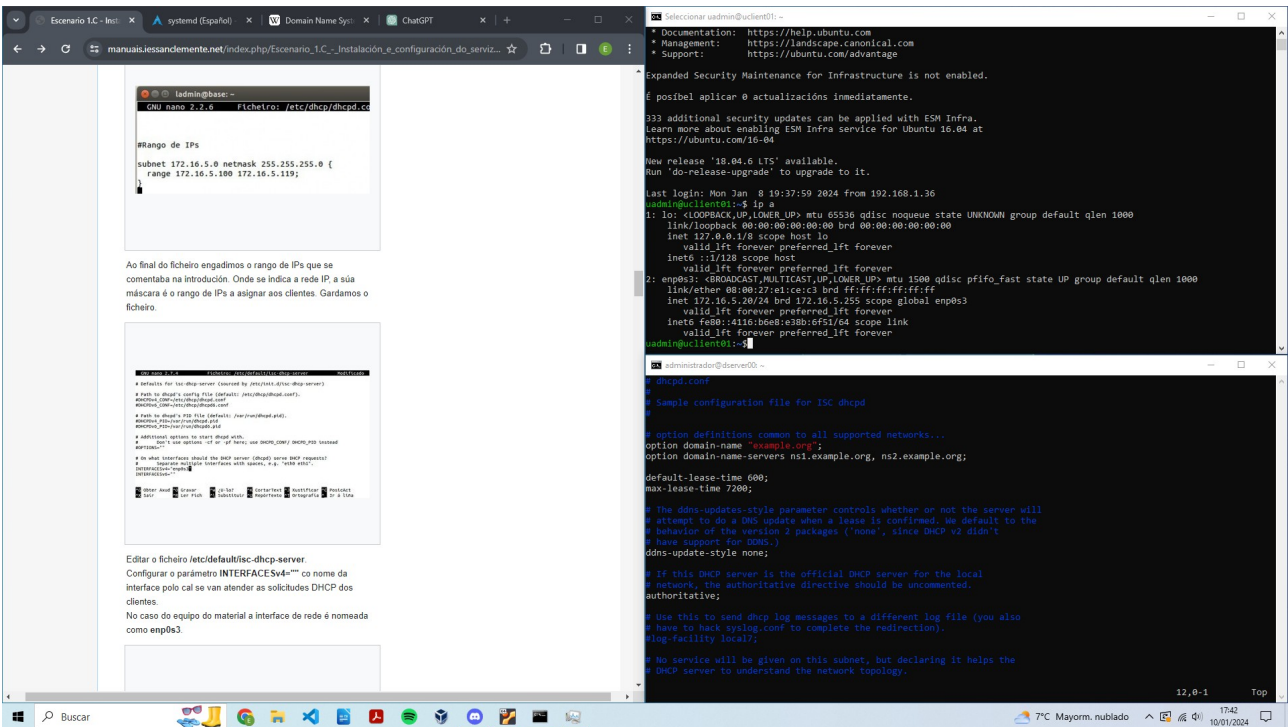
Apt install

Al finalizar la instalación intentará iniciarse automáticamente pero nos dará error. Dado que primero deberemos asignar un rango de IP.

Editaremos el archivo. `/etc/dhcp/dhcpd.conf`

Descomentamos la opción “authoritative” para indicar que el servidor es el servidor DHCP oficial de la LAN.

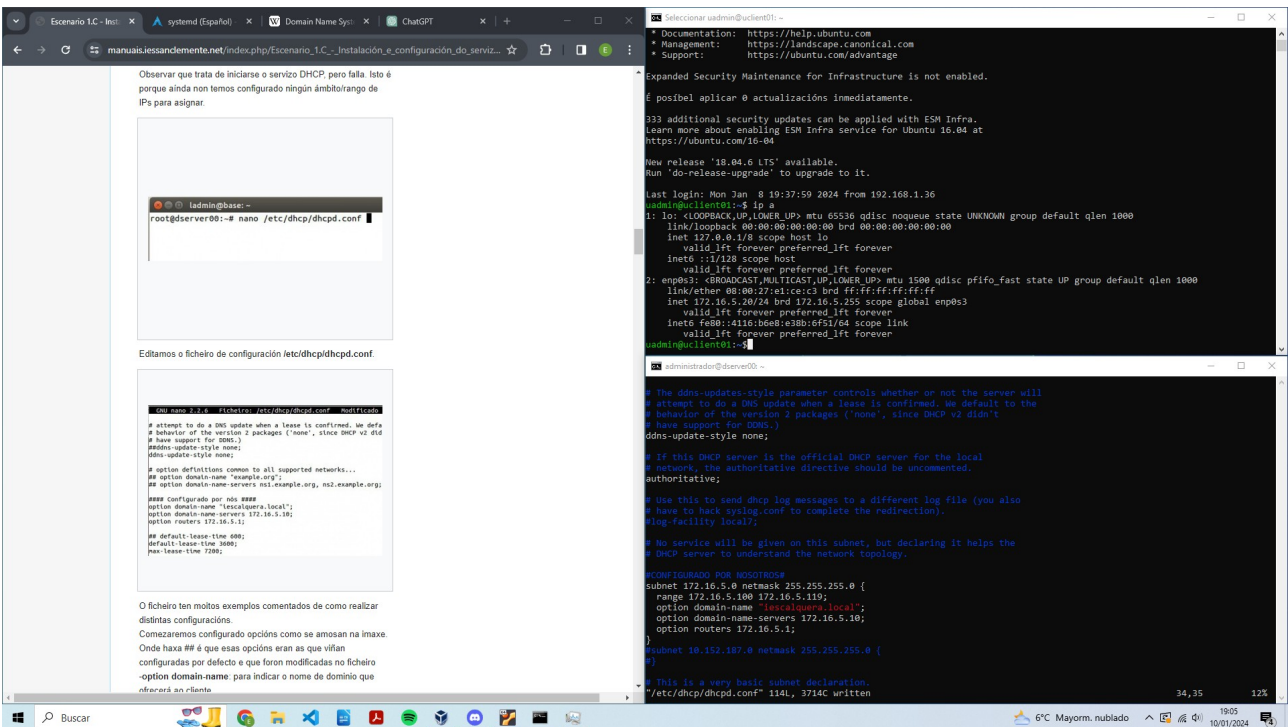
51 Platega I_II_III



Descomentado authoritative.

Configuramos el rango de IP y servidores de DNS y el search. Dado que estos son parámetros proporcionados por el DHCP.

Lo he configurado de una manera algo distinta al PLATEGA pero es una manera mas clara, y dentro del archivo de configuración hay ejemplos que lo realizan de la misma manera.



Configuración rango de IP.

Editaremos el fichero **etc/default/isc-dhcp-server**

Ponemos el nombre de la interfaz de red IPv4 en nuestro caso el nombre es **enp0s3**

```

# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPD_CONF=/etc/dhcp/dhcpd.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here, use DHCPD_CONF/ DHCPD_PID instead
OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""

```

Editar o ficheiro **etc/default/isc-dhcp-server**

Configurar o parámetro **INTERFACESv4** co nome da interface polo cal se van atender as solicitudes DHCP dos clientes.

No caso do equipo do material a interface de rede é nomeada como **enp0s3**.

```

root@server00:~# systemctl start isc-dhcp-server
root@server00:~#
root@server00:~#

```

Iniciar o servizo de DHCP: **systemctl start isc-dhcp-server**.

Tamén se pode usar **service isc-dhcp-server start**.

Olo que cando o servizo é iniciado/parado correctamente o comando non amosa ningunha información de saída.

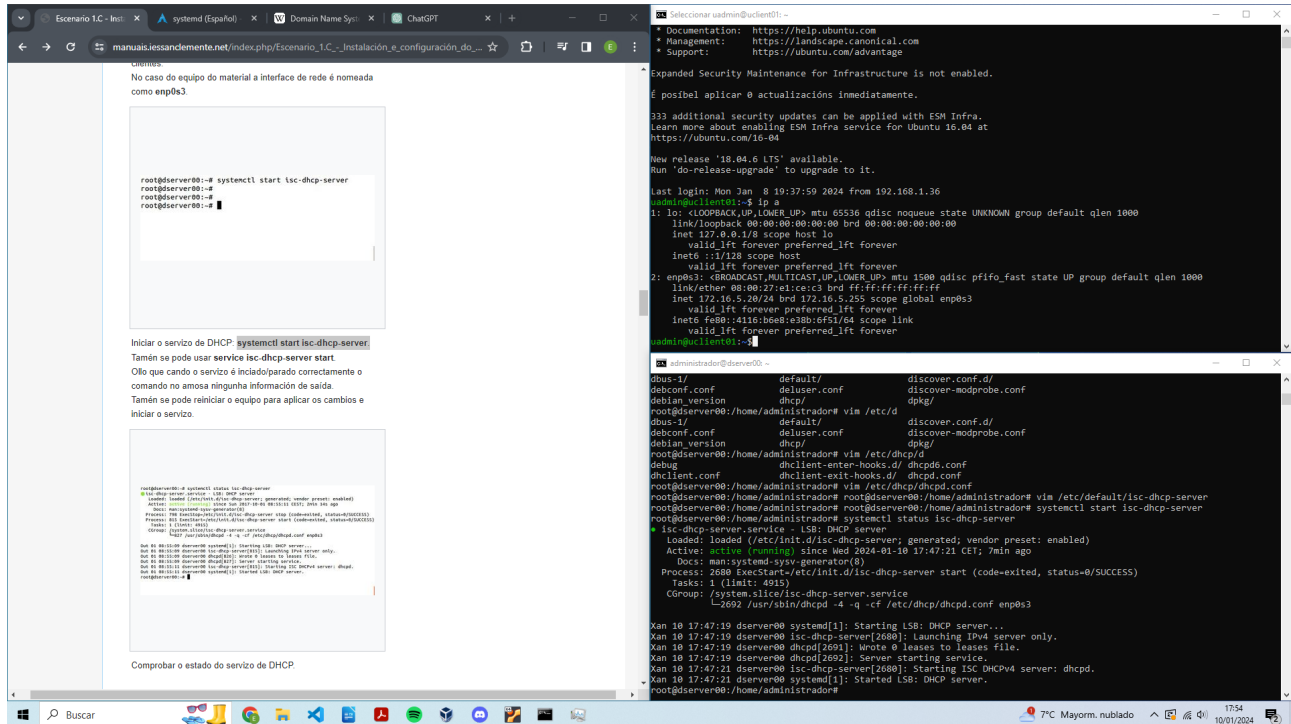
Tamén se pode reiniciar o equipo para aplicar os cambios e iniciar o servizo.

*Editado del fichero **etc/default/isc-dhcp-server**.*

Iniciamos el servicio mediante el comando **systemctl start isc-dhcp-server**

Comprobamos el status del servicio mediante el comando.

Systemctl status isc-dhcp-server



No caso do equipo do material a interface de rede é nomeada como `enp0s3`.

```
root@server00:~# systemctl start isc-dhcp-server
root@server00:~# systemctl status isc-dhcp-server
systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP server
   Loaded: loaded (/etc/systemd/system/isc-dhcp-server.service; vendor preset: enabled)
   Active: active (running) since Wed 2024-01-10 17:47:21 CET; 7min ago
     Docs: man:systemd-sysv-generator(8)
    Process: 2688 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Main PID: 2688 (systemd)
     CGroup: /system.slice/isc-dhcp-server.service
            └─2692 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s3
```

Iniciar o servizo de DHCP: `systemctl start isc-dhcp-server`
 Tamén se pode usar `service isc-dhcp-server start`.
 Oílo que cando o servizo é iniciado/parado correctamente o comando non amosa ningunha información de saída.
 Tamén se pode reiniciar o equipo para aplicar os cambios e iniciar o servizo.

```
root@server00:~# systemctl status isc-dhcp-server
systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP server
   Loaded: loaded (/etc/systemd/system/isc-dhcp-server.service; vendor preset: enabled)
   Active: active (running) since Wed 2024-01-10 17:47:21 CET; 7min ago
     Docs: man:systemd-sysv-generator(8)
    Process: 2688 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Main PID: 2688 (systemd)
     CGroup: /system.slice/isc-dhcp-server.service
            └─2692 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s3
```

Comprobar o estado do servizo de DHCP

```
root@server00:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:e1:c1:c3 brd ff:ff:ff:ff:ff:ff
    inet 172.16.5.10/24 brd 172.16.5.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::411c:b0a2:c2b0:f51c4 scope link
        valid_lft forever preferred_lft forever
```

```
root@server00:~# systemctl status isc-dhcp-server
systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated; vendor preset: enabled)
   Active: active (running) since Wed 2024-01-10 17:47:21 CET; 7min ago
     Docs: man:systemd-sysv-generator(8)
    Process: 2688 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Main PID: 2688 (systemd)
     CGroup: /system.slice/isc-dhcp-server.service
            └─2692 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s3
```

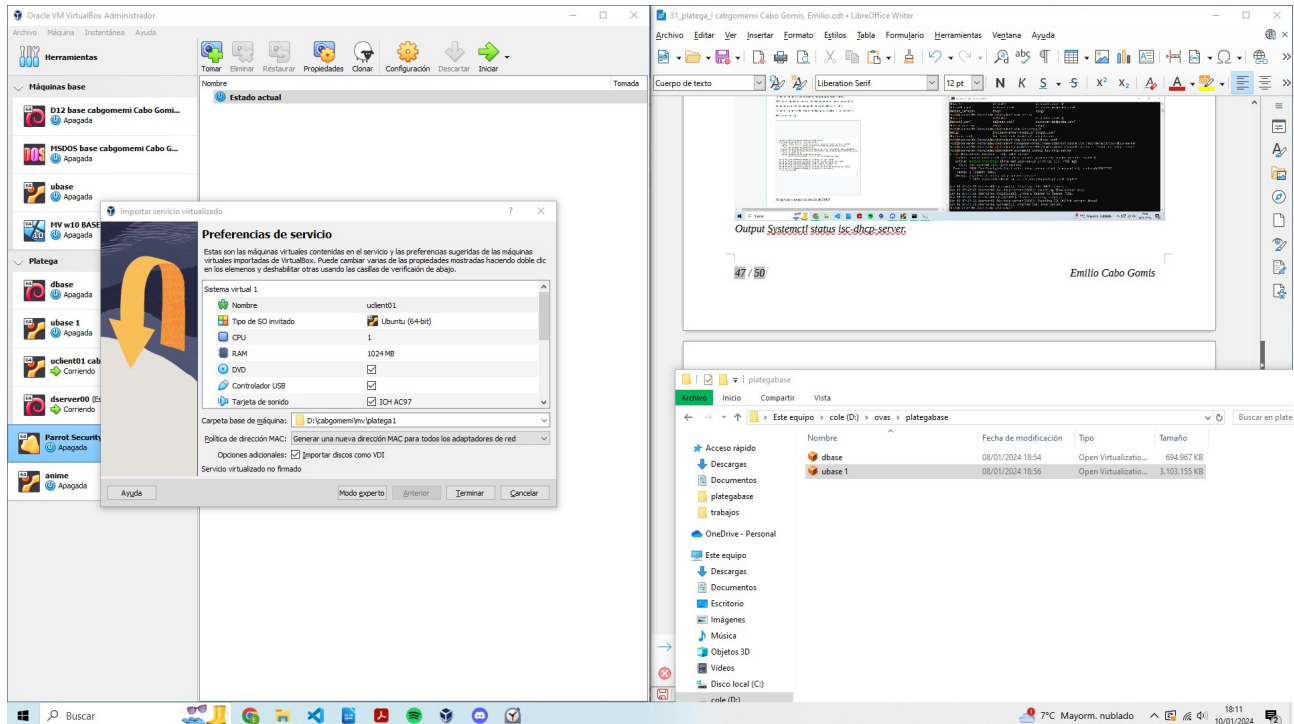
```
Xan 10 17:47:19 dserver00 systemd[1]: Starting LSB: DHCP server...
Xan 10 17:47:19 dserver00 isc-dhcp-server[2688]: Launching IPv4 server only.
Xan 10 17:47:19 dserver00 dhcpd[2691]: Wrote 0 leases to leases file.
Xan 10 17:47:19 dserver00 dhcpd[2691]: Server starting service.
Xan 10 17:47:21 dserver00 isc-dhcp-server[2688]: Starting ISC DHCPv4 server: dhcpd.
Xan 10 17:47:21 dserver00 systemd[1]: Started LSB: DHCP server.
root@server00:~#
```

Output **Systemctl status isc-dhcp-server**.

Configuración del cliente: uclient02

Iniciamos una máquina base.

Deberemos acordarnos de regenerar la dirección MAC para que no haya 2 máquinas con la misma dirección MAC.

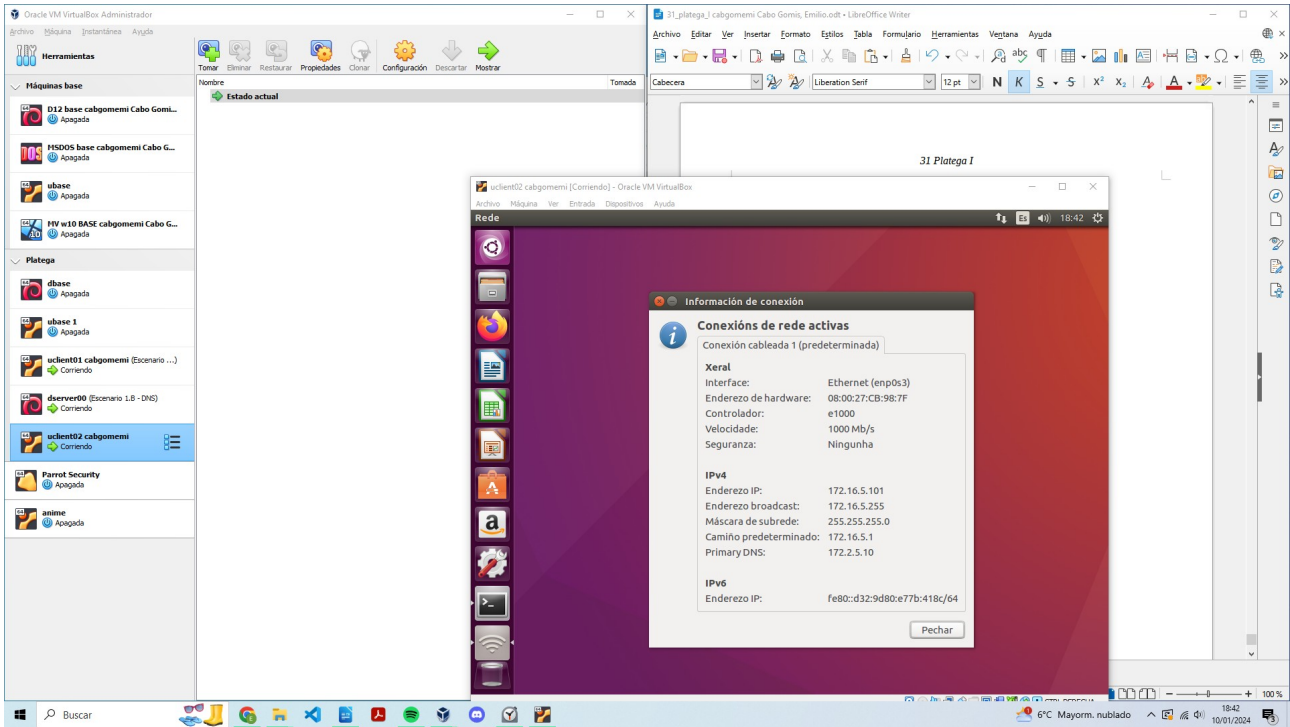


Virtualbox.

Al refrescar la MAC al crear la máquina se ha creado una conexión de red nueva. Es la que está en gallego.

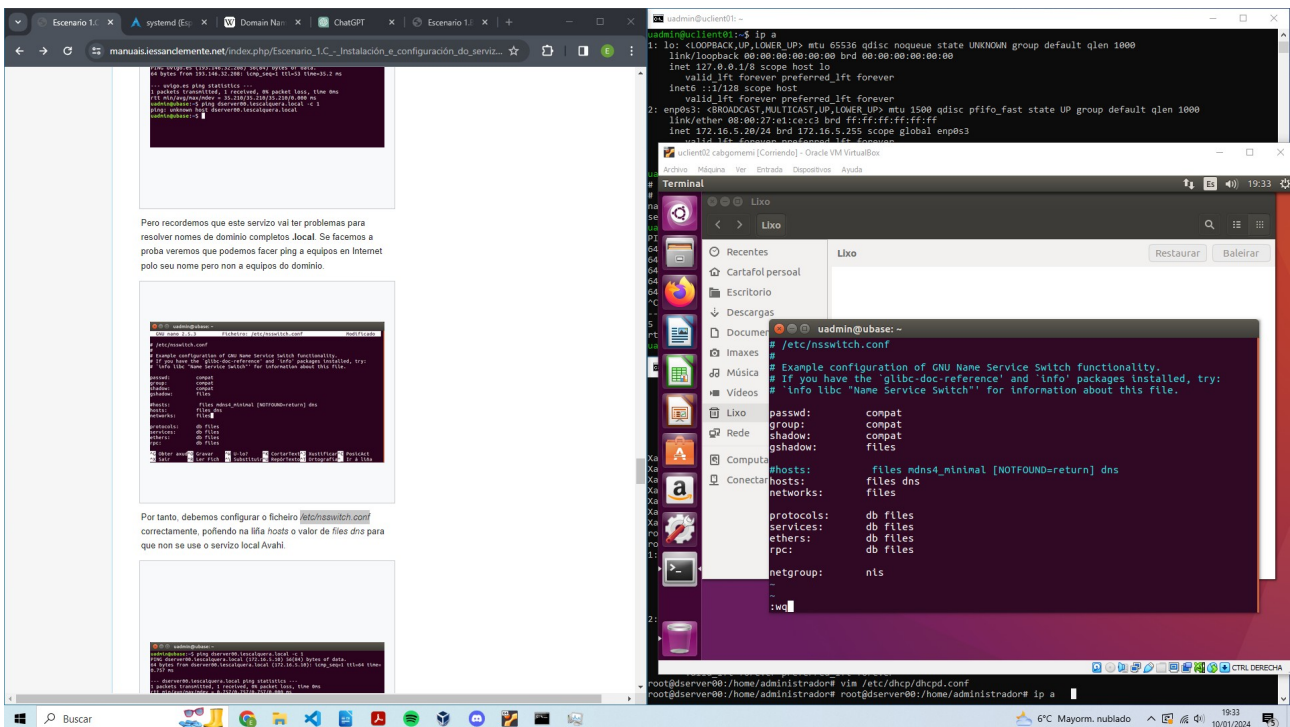
Hacemos click en el menú de información de conexión para comprobar los datos que el cliente ha recopilado del servidor DHCP.

51 *Platega* I_II_III



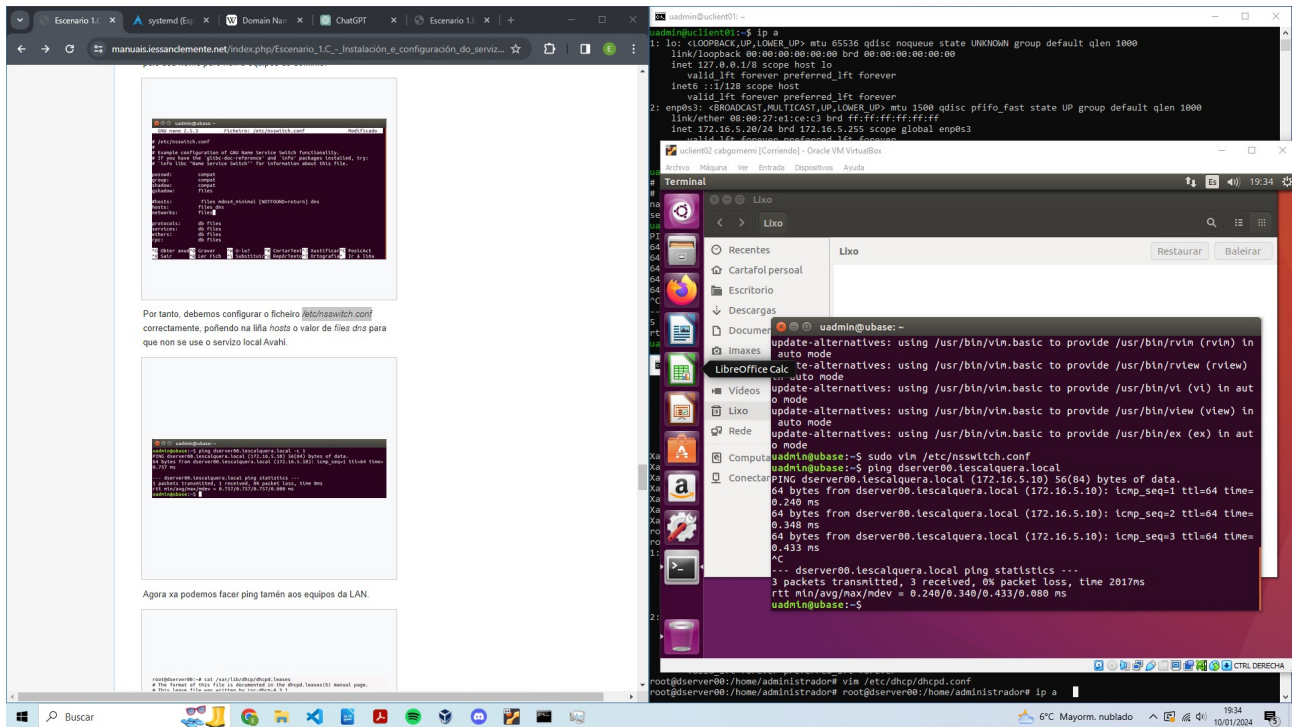
Información de conexión.

Editamos el fichero `/etc/nsswitch.conf` para que no use el servicio local Avahi. Así es como quedaría el fichero editado.



Fichero /etc/nsswitch.conf.

Ahora podremos hacer ping a equipos en la red local mediante su nombre completo.



Ping.

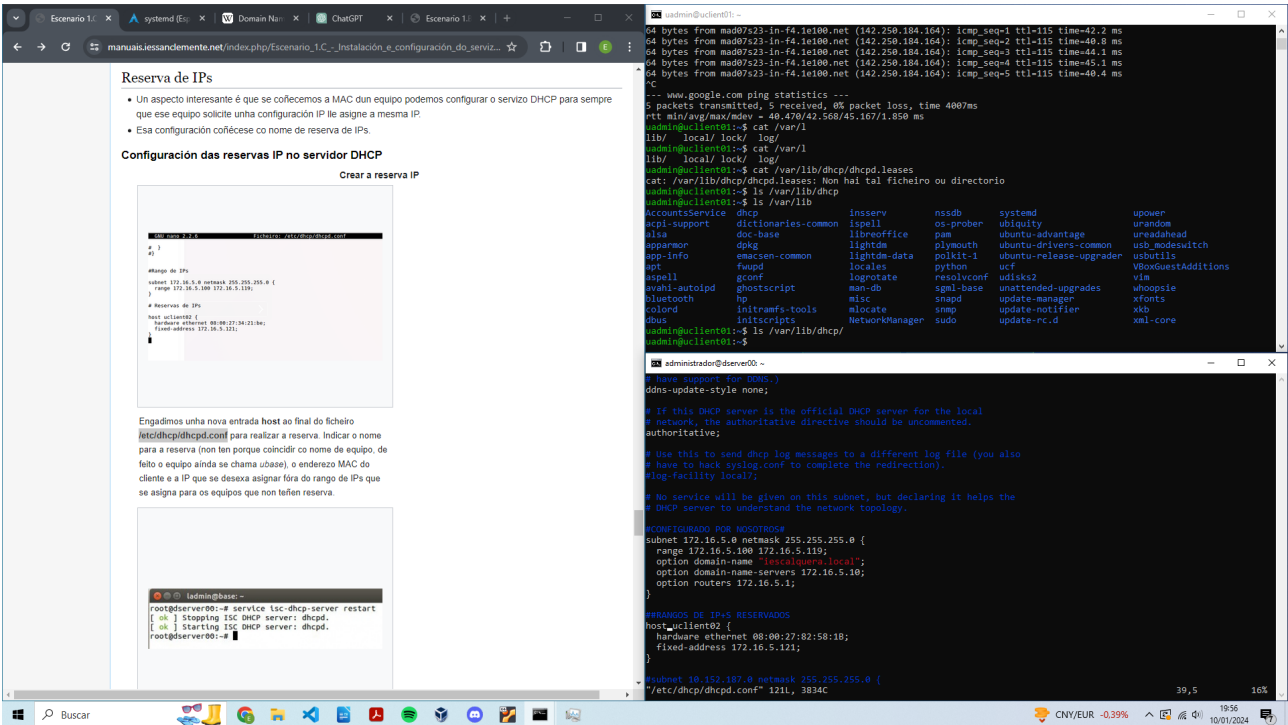
Reserva de IPs

Configuración de reservas de IP en dserver00

Editamos el fichero `/etc/dhcp/dhcpd.conf`

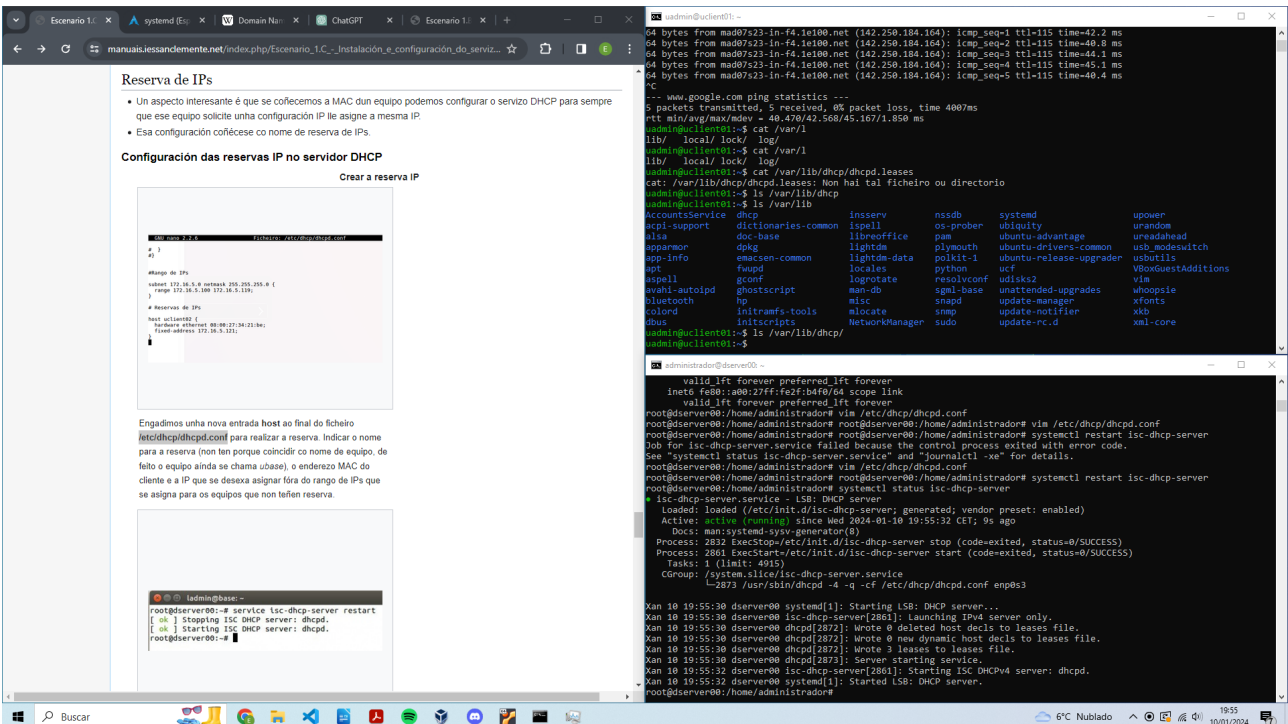
Si buscamos la palabra “fixed” dentro del fichero de configuración nos aparecerán ejemplos de direcciones IP reservadas.

51 *Platega* I_II_III



```
/etc/dhcp/dhcpd.conf
```

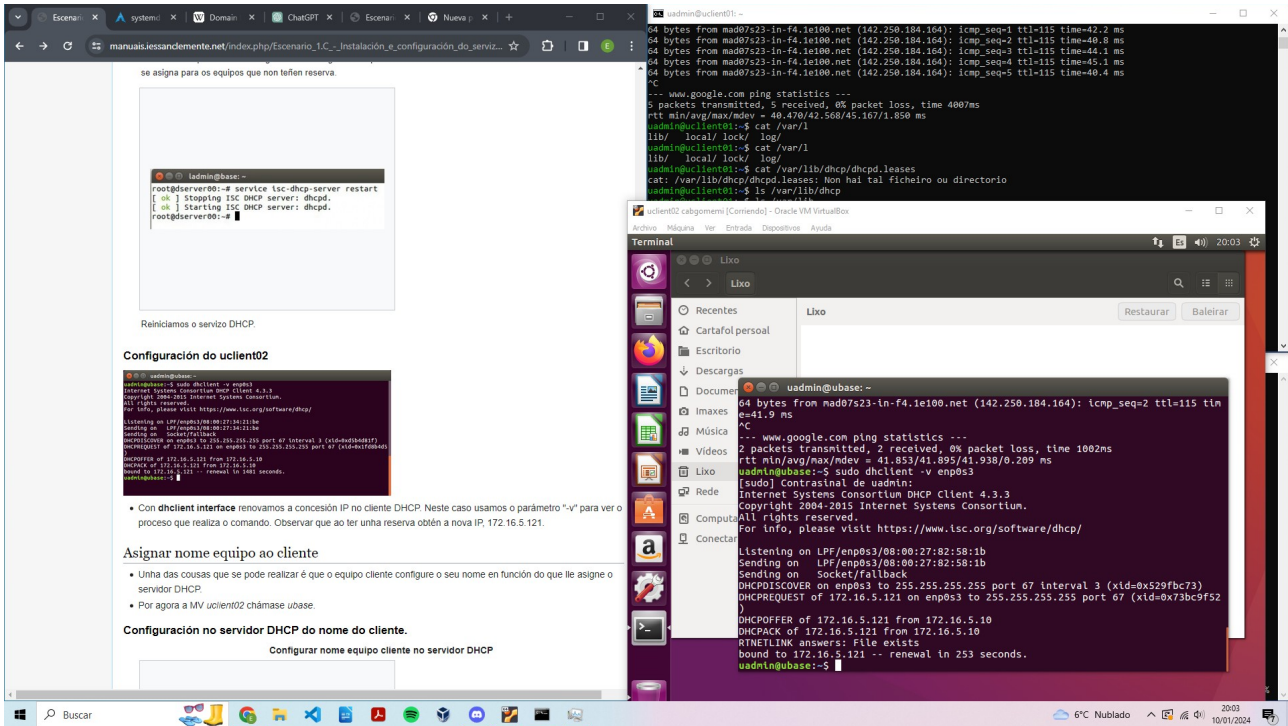
Reiniciamos el servicio de DHCP y comprobamos que se encuentra activo.



Comprobación de reinicio de servicio DHCP.

Configuración de uclient02

Mediante el comando **sudo dhclient -v enp0s3** renovamos la concesión de IP por parte del servidor DHCP.



“**sudo dhclient -v enp0s3**”

Asignación automática de hostname

Configuración en el servidor DHCP

Aplicaremos la siguiente configuración al archivo `/etc/dhcp/dhcpd.conf` :

Tendremos que añadir la entrada “**option host-name "uclient02";**” en la sección dónde se encuentran las IP reservadas.

[illegible]

```
/etc/dhcp/dhcpd.conf
```

Configuración en el cliente para configurar su nome de equipo mediante el servidor DHCP

Crearemos el fichero. `/etc/NetworkManager/dispatcher.d/99hostname` con el siguiente contenido.

```

1  #!/bin/sh
2
3  ### Script para configurar o nome do equipo
4  ### a partir dos datos enviados polo servidor DHCP
5
6
7  case "$2" in
8
9      up|dhcp4-change)
10         # Non facemos nada se o servidor
11         # non nos deu a variable adecuada
12         if [ -z "$DHCP4_HOST_NAME" ]
13         then
14             exit 0
15         else
16             hostname $DHCP4_HOST_NAME
17             echo $DHCP4_HOST_NAME > /etc/hostname
18         fi
19     ;;
20 esac

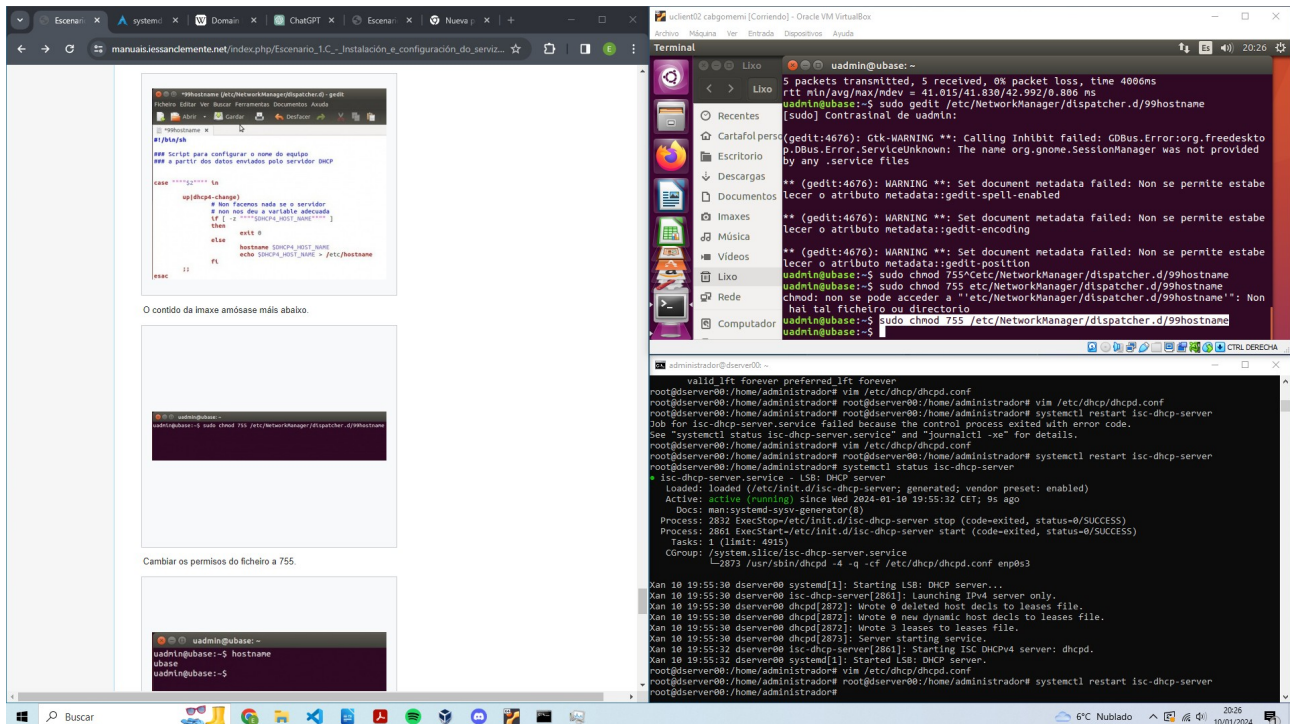
```

Contenido `/etc/NetworkManager/dispatcher.d/99hostname`

Cambiamos los permisos del archivo que acabamos de crear mediante el siguiente comando.

`sudo chmod 755 /etc/NetworkManager/dispatcher.d/99hostname`

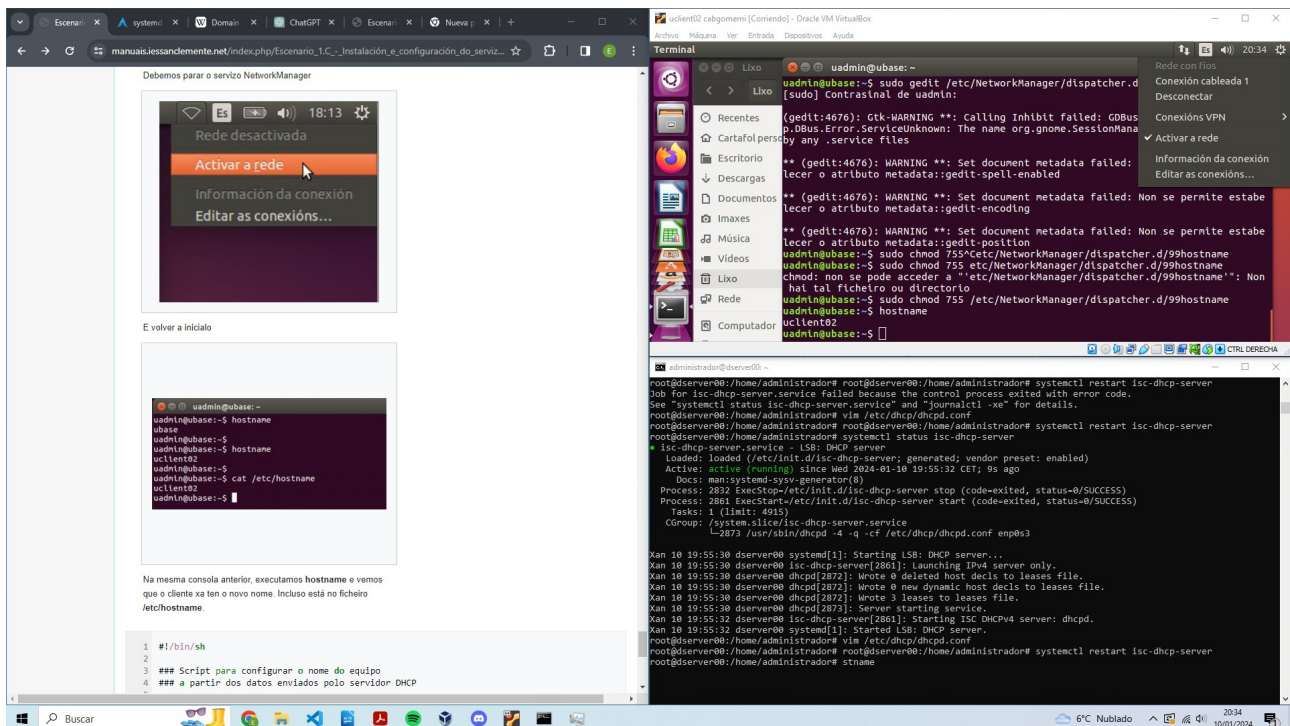
output `sudo chmod 755 /etc/NetworkManager/dispatcher.d/99hostname`



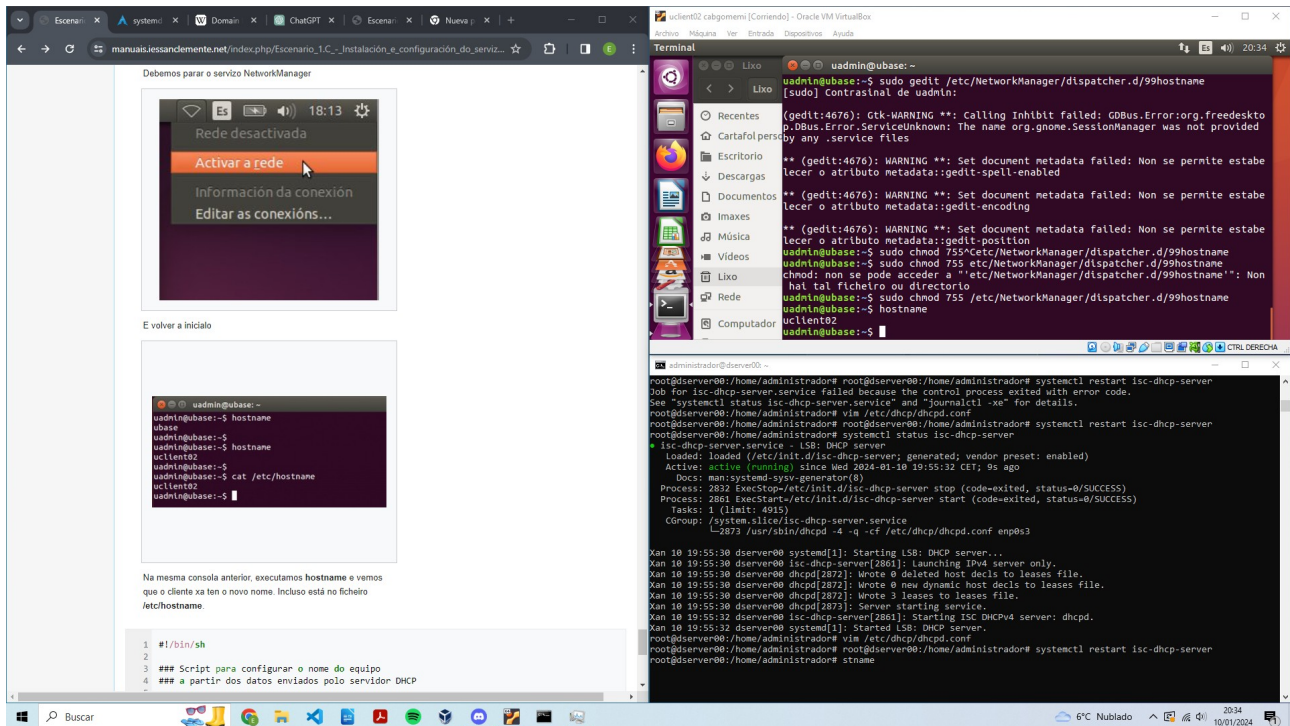
output sudo chmod 755 /etc/NetworkManager/dispatcher.d/99hostname

Reiniciamos el servicio NetworkManager

Al hacer click en Activar a Rede se desactiva, al volver a hacer click se reiniciará la red.



Ejecutamos el comando **hostname**.



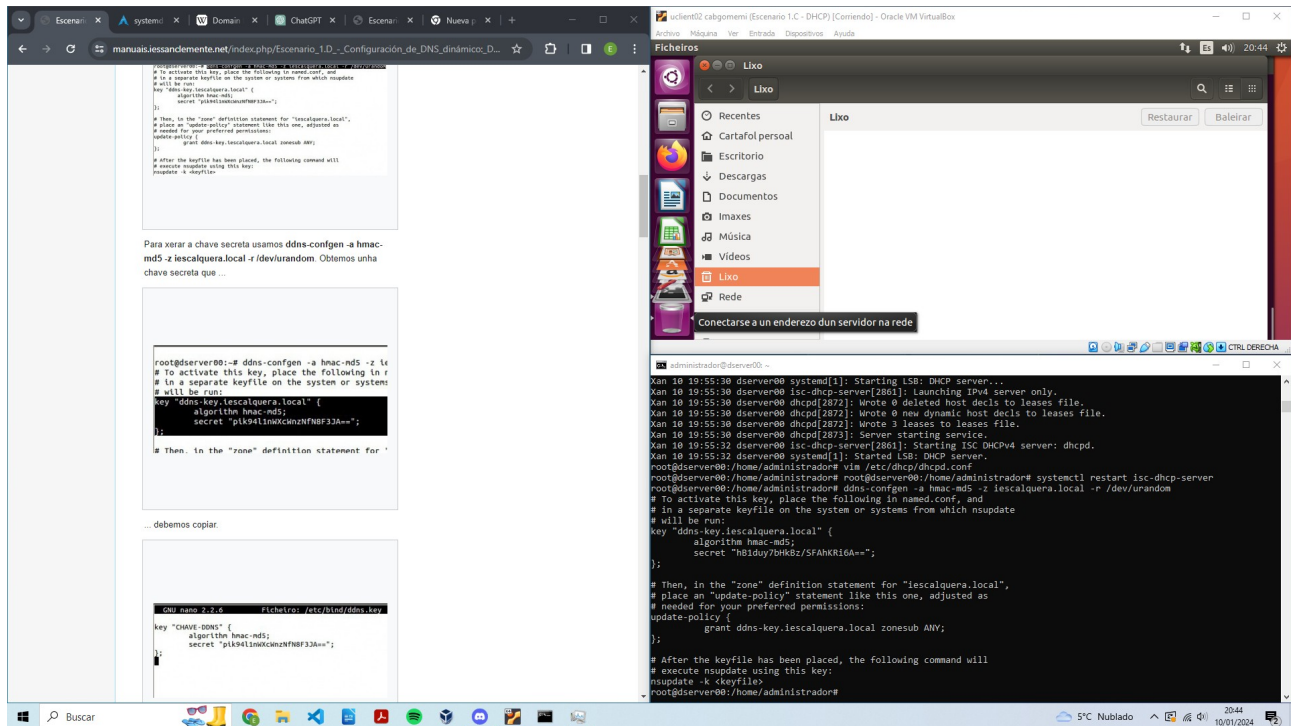
Output hostname.

Tal y como podemos comprobar se ha cambiado el contenido del /etc/hostname. Todo mediante el servidor DHCP.

Escenario 1.D - Configuración de DNS dinámico: DDNS

Configuración de DDNS en dserver00

Mediante el comando **ddns-confgen -a hmac-md5 -z iescalquera.local -r /dev/urandom**.
 Generaremos una clave secreta que deberemos copiar.

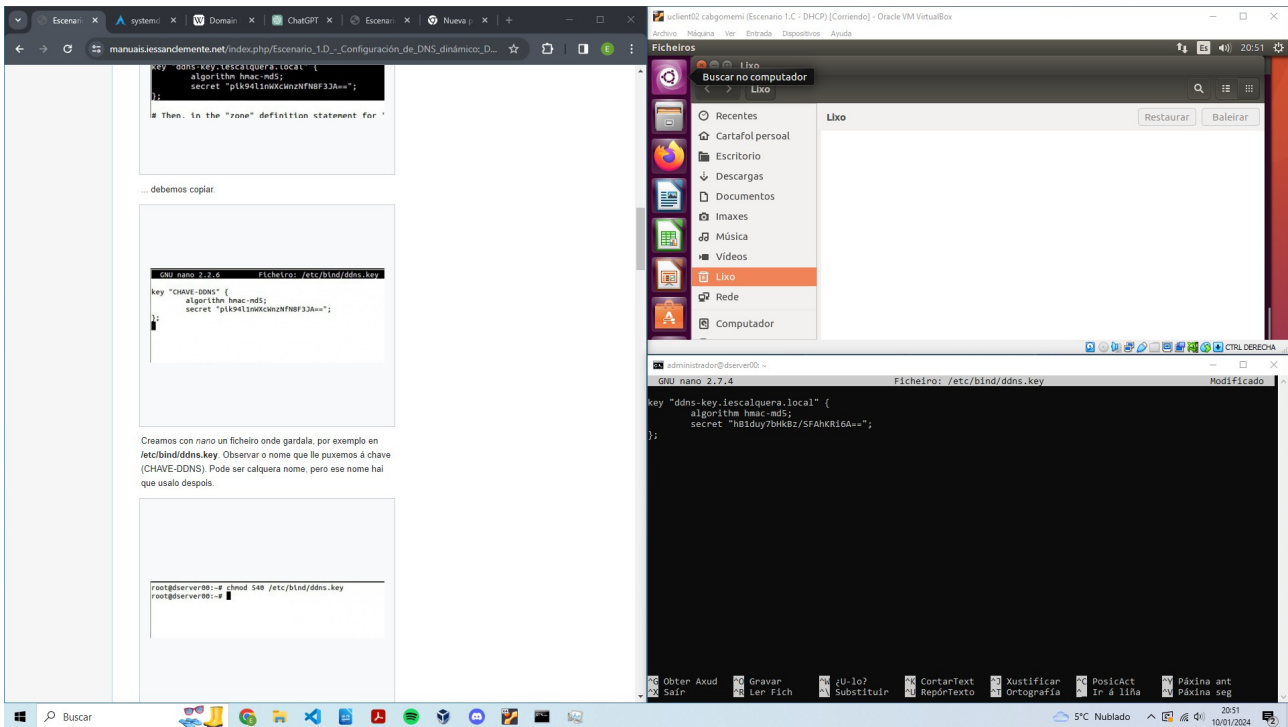


ddns-confgen -a hmac-md5 -z iescalquera.local -r /dev/urandom

Tal y como nos indica la shell podríamos copiar esta sección en el named.conf o podremos hacerlo de la siguiente manera.

Crearemos el siguiente fichero.

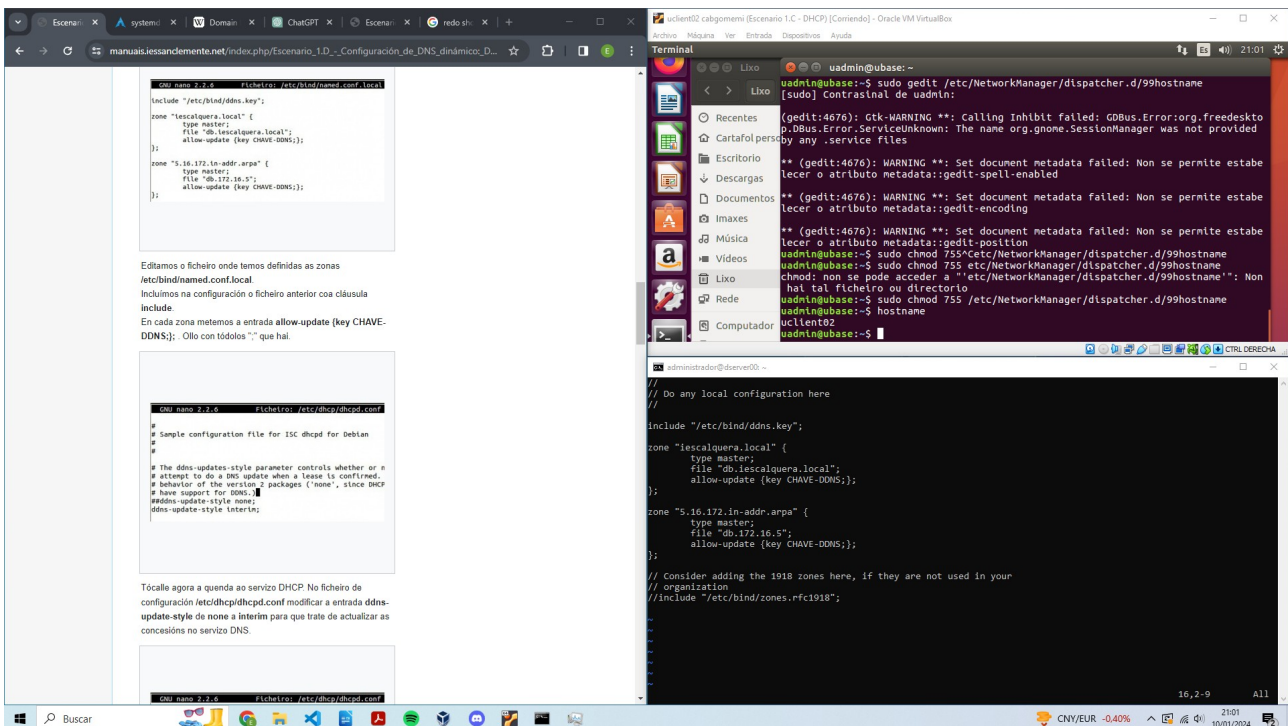
51 Platega I_II_III



Le asignaremos permisos mediante el siguiente comando.

chmod 540 /etc/bind/ddns.key

Añadiremos los siguientes cambios al archivo de configuración `/etc/bind/named.conf.local`

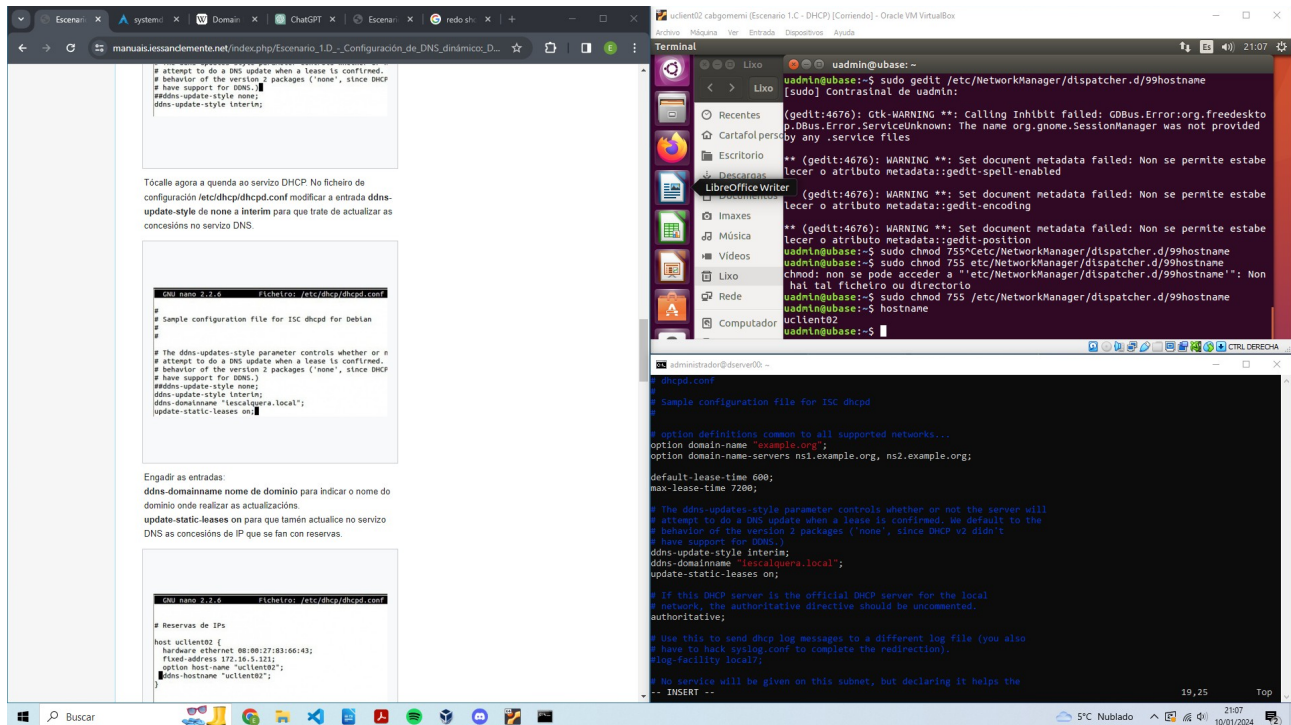


Contenido `/etc/bind/named.conf.local`

51 Platega I_II_III

Ahora editaremos el fichero de configuración `/etc/dhcp/dhcpd.conf`

Cambiaremos el update style de DDNS de none a interim además de otros cambios. (Revisar cambios en la imagen).



`/etc/dhcp/dhcpd.conf`

En el mismo archivo añadiremos la línea en la sección de reserva de IP para configurar el nombre aplicado por el DDNS.

ddns-hostname "uclient02";

The screenshot shows a web browser window on the left displaying a manual for configuring dynamic DNS. The manual includes instructions on how to configure the `ddns-hostname` parameter in the `/etc/dhcp/dhcpd.conf` file. It also shows a terminal window on the right with the following configuration:

```
# The ddns-updates-style parameter controls whether or not
# attempt to do a DNS update when a lease is confirmed,
# behavior of the version 3 packages (none, since dnsmasq
# have support for DNS.)
ddns-updates-style none;
ddns-update-style interim;
ddns-domainname "lescalquera.local";
update-static-leases on;
```

The terminal window also shows the configuration of the `uclient02` host in the `/etc/dhcp/dhcpd.conf` file:

```
host uclient02 {
    hardware ethernet 08:00:27:18:10:64;
    fixed-address 172.16.5.121;
    option host-name "uclient02";
    ddns-hostname "uclient02";
}
```

/etc/dhcp/dhcpd.conf

Además añadiremos las siguientes líneas al final del archivo de configuración.

The screenshot shows a web browser window on the left displaying a manual for configuring dynamic DNS. The manual includes instructions on how to configure the `ddns-hostname` parameter in the `/etc/dhcp/dhcpd.conf` file. It also shows a terminal window on the right with the following configuration:

```
# The ddns-updates-style parameter controls whether or not
# attempt to do a DNS update when a lease is confirmed,
# behavior of the version 3 packages (none, since dnsmasq
# have support for DNS.)
ddns-updates-style none;
ddns-update-style interim;
ddns-domainname "lescalquera.local";
update-static-leases on;
```

The terminal window also shows the configuration of the `uclient02` host in the `/etc/dhcp/dhcpd.conf` file:

```
host uclient02 {
    hardware ethernet 08:00:27:18:10:64;
    fixed-address 172.16.5.121;
    option host-name "uclient02";
    ddns-hostname "uclient02";
}
```

/etc/dhcp/dhcpd.conf

```
include "/etc/bind/ddns.key";

zone iescalquera.local. {
    primary 172.16.5.10;
    key CHAVE-DDNS;
}

zone 5.16.172.in-addr.arpa. {
    primary 172.16.5.10;
    key CHAVE-DDNS;
}
```

Contenido /etc/dhcp/dhcpd.conf

Reiniciamos ambos servicios.

Configuración client-side

Realizamos una nueva solicitud al DHCP mediante el comando

Sudo dhclient enp0s3

The screenshot shows a web browser on the left displaying a tutorial for DHCP configuration. The tutorial includes a code block for the /etc/bind/ddns.key file and instructions for configuring the DHCP client. On the right, a terminal window shows the execution of various commands to configure and restart the DHCP service. The terminal output includes the following commands and their results:

```
uadmin@ubase:~$ sudo chnod 755 /etc/NetworkManager/dnsmasq.d/99hostname
chnod: non se pode acceder a "/etc/NetworkManager/dnsmasq.d/99hostname"
ou directorio
uadmin@ubase:~$ sudo chnod 755 /etc/NetworkManager/dnsmasq.d/99hostname
uadmin@ubase:~$ hostname
uadmin@ubase:~$ sudo dhclient -v enp0s3
sudo: unable to resolve host uadmin: A conexión espirou
[sudo] Contraseña de uadmin:
Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:82:58:1b
Sending on LPF/enp0s3/08:00:27:82:58:1b
Sending on Socket/fallback
DHCPREQUEST of 172.16.5.121 on enp0s3 to 255.255.255.255 port 67 (xid=0x43bd547)
DHCPOFFER of 172.16.5.121 from 172.16.5.10
RTNETLINK answers: File exists
bound to 172.16.5.121 -- renewal in 298 seconds.
uadmin@ubase:~$
```

The terminal also shows the output of the systemctl command, indicating that the isc-dhcp-server service is failed with the result 'exit-code'. The administrator then restarts the service, and the output shows that the service is now active and running.

Output

Finalización

Saldremos de ambas shells remotas.

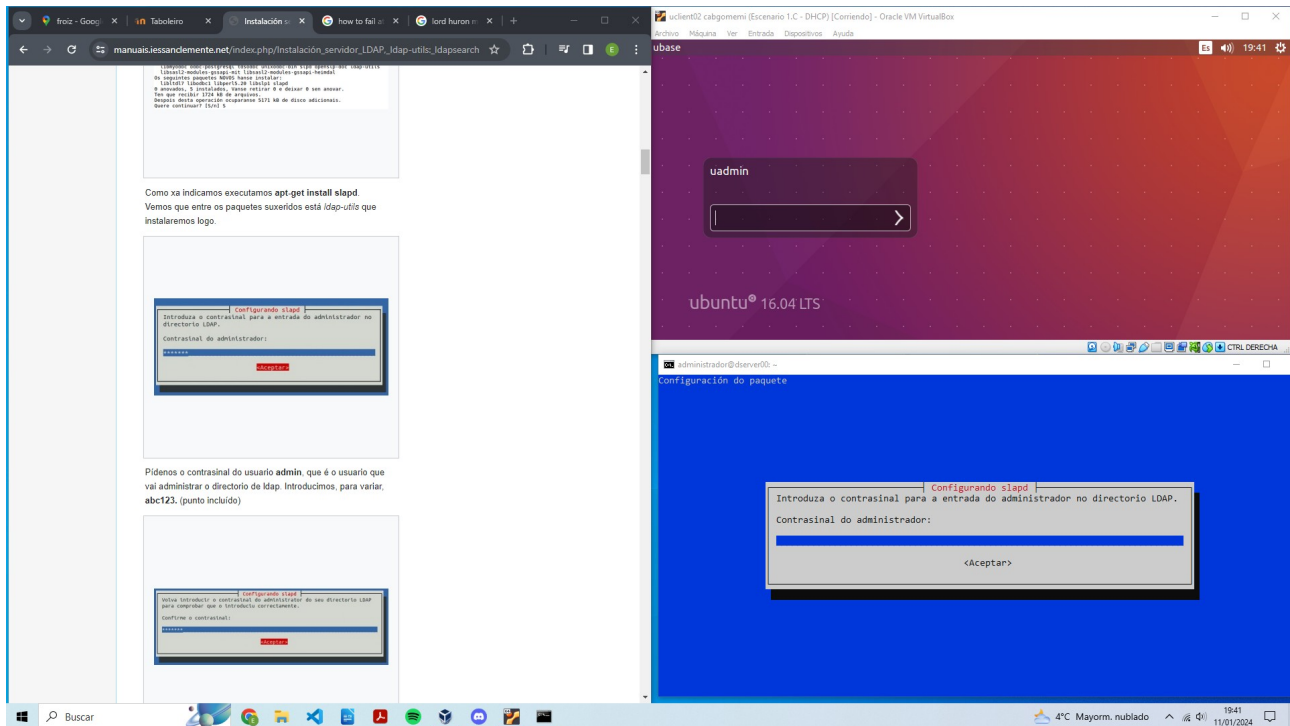
Tomaremos una instantánea de ambas máquinas dado que hemos terminado el ejercicio.

Platega II

Instalar y configurar slapd

Instalamos slapd en la máquina dserver00

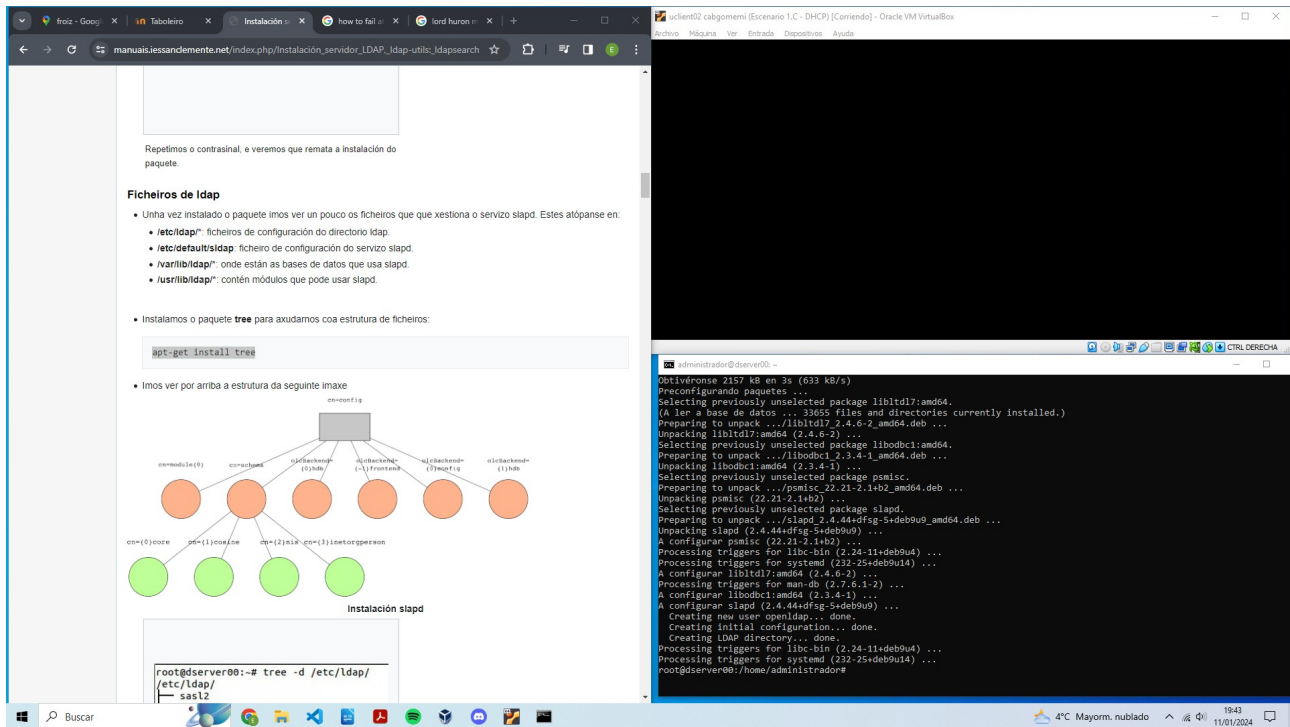
Una vez instalado se nos abrirá la siguiente pantalla.



Loginscreen.

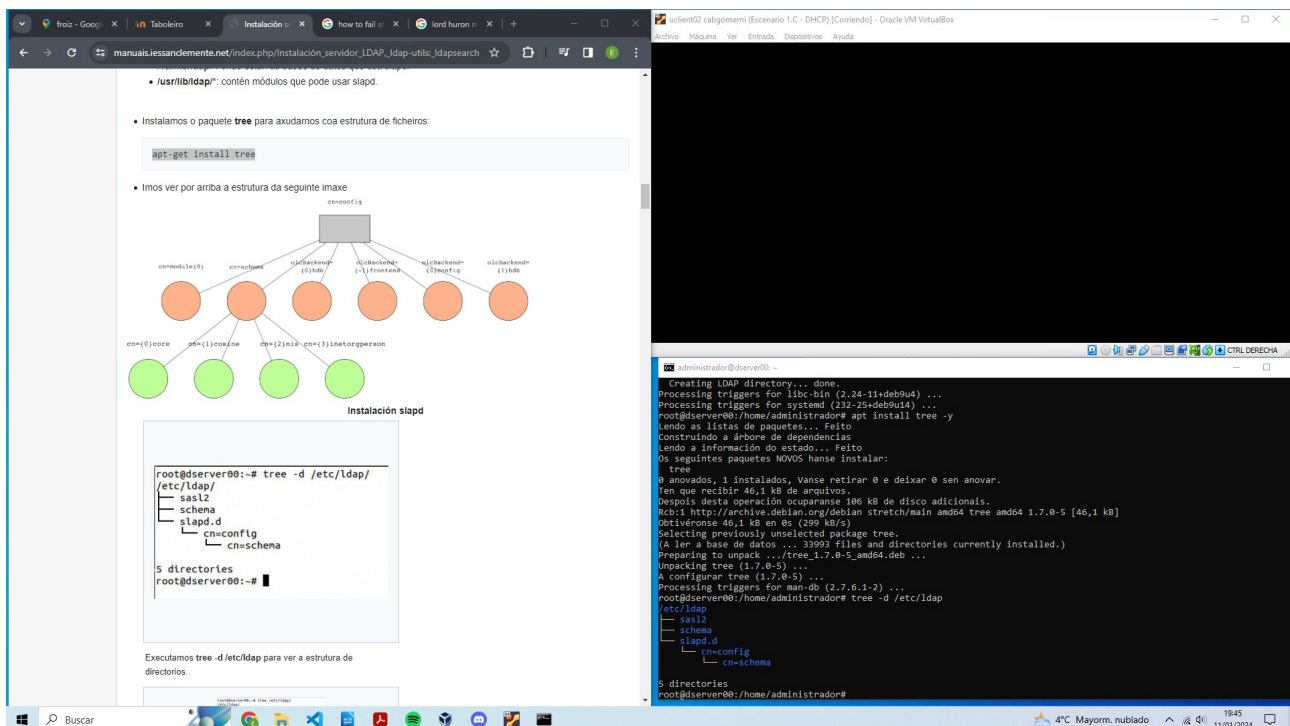
Introduciremos la contraseña del usuario administrador. En nuestro caso de seguir las instrucciones será abc123.

Ahora el sistema ldap estará instalado.



Mediante el siguiente comando instalaremos el paquete tree para ayudarnos a visualizar mejor la estructura de directorios.

apt-get install tree

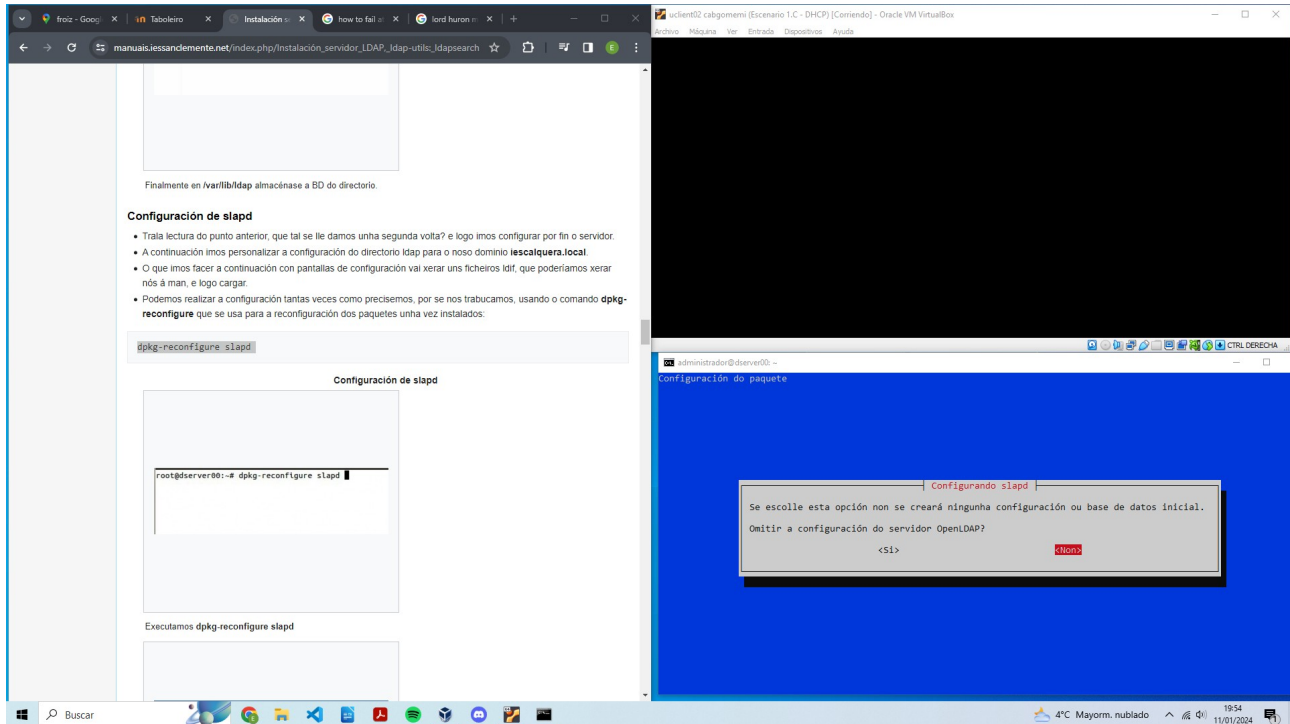


Visualización del sistema de directorios.

Ejecutamos el siguiente comando.

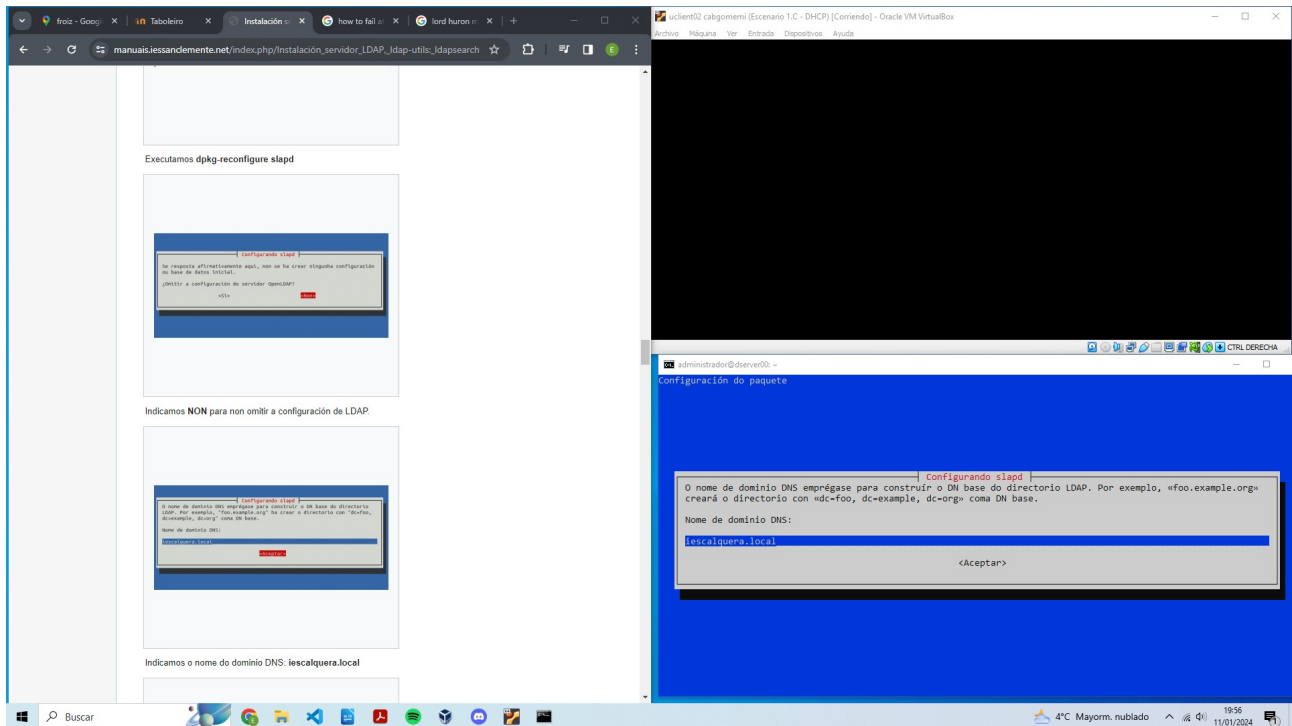
dpkg-reconfigure slapd

Seleccionamos No



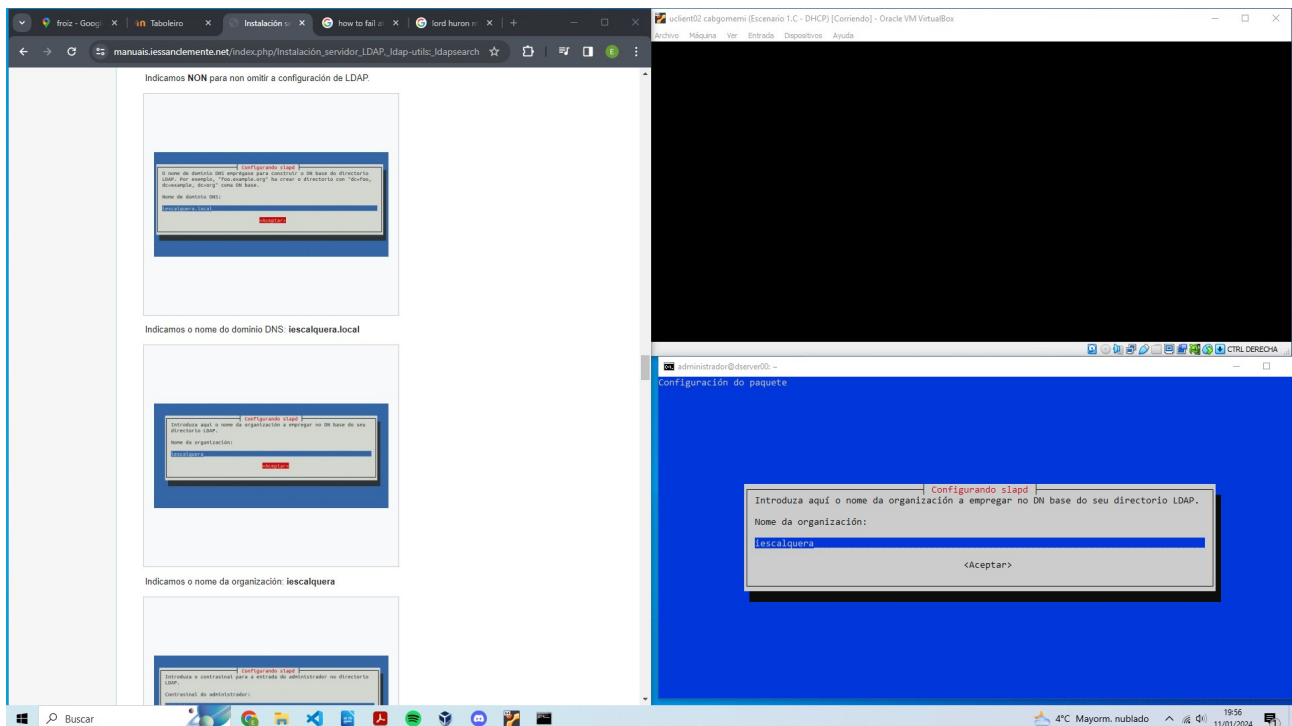
Menú de configuración OPENLDAP

Introducimos el siguiente dominio.



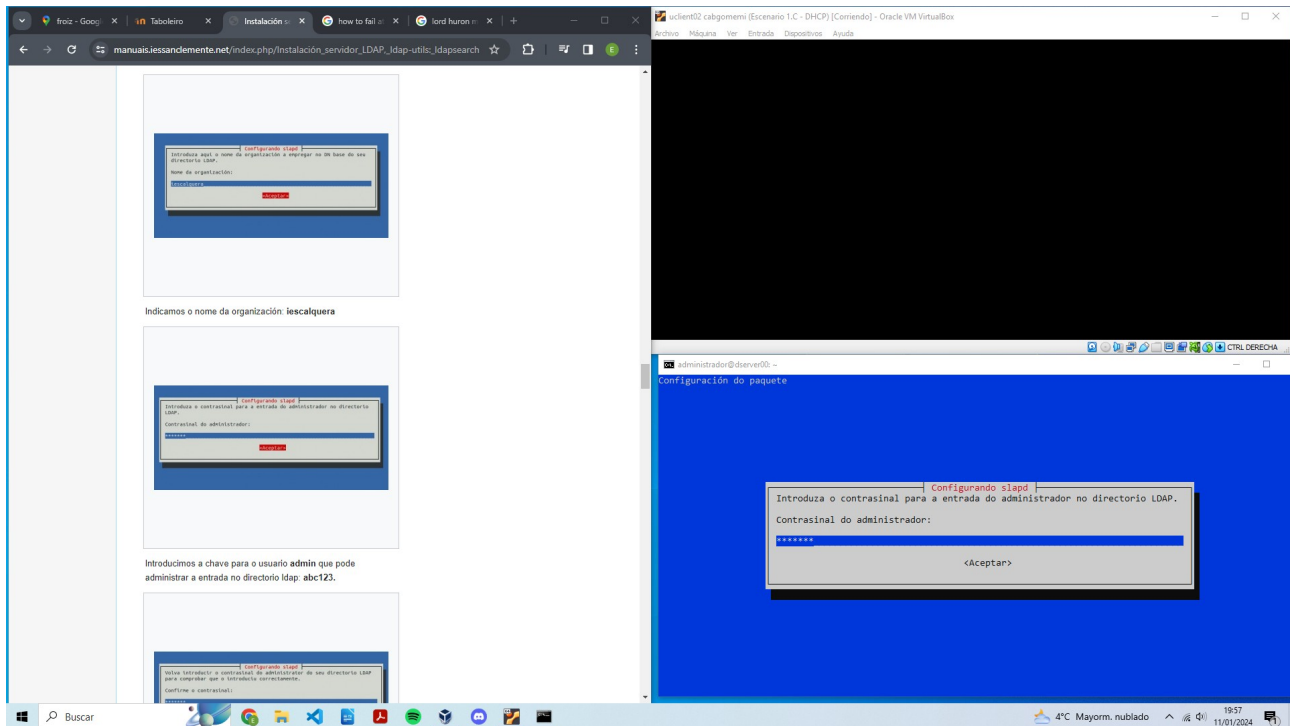
Menú de configuración OPENLDAP

Introducimos iescalquera como nombre de organización.



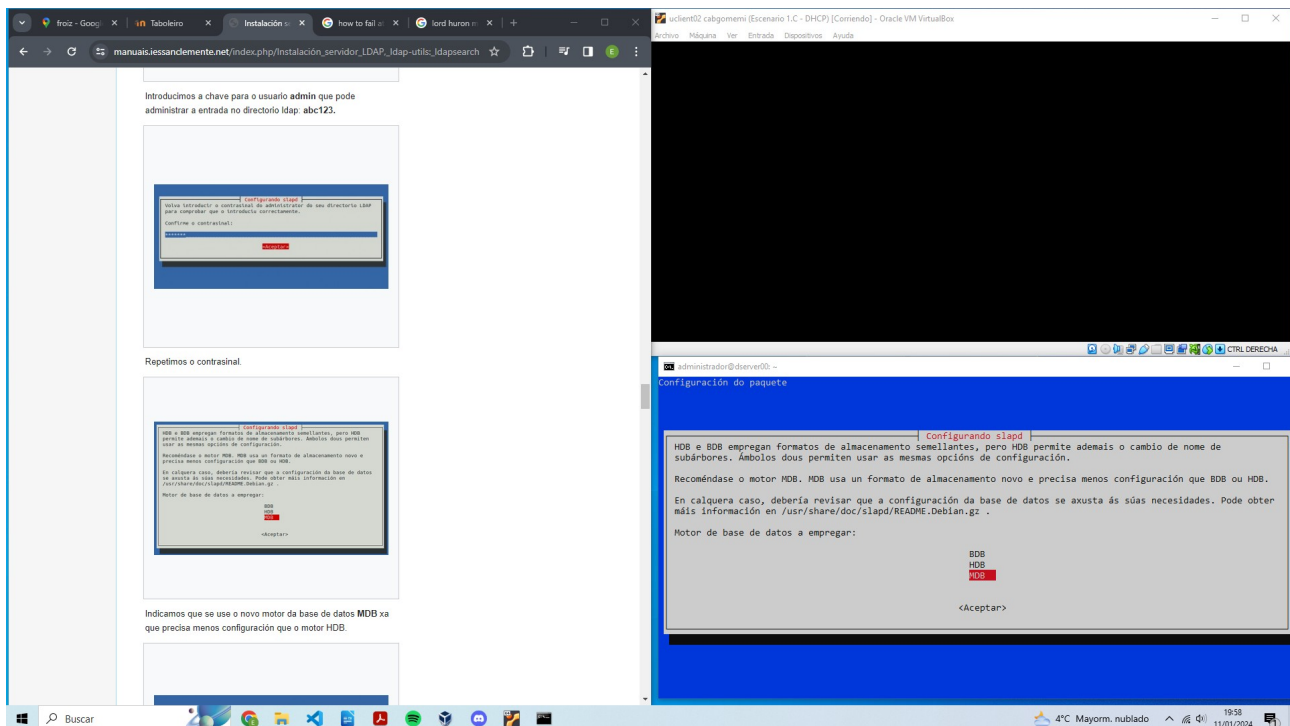
Menú de configuración OPENLDAP

Introducimos la contraseña.



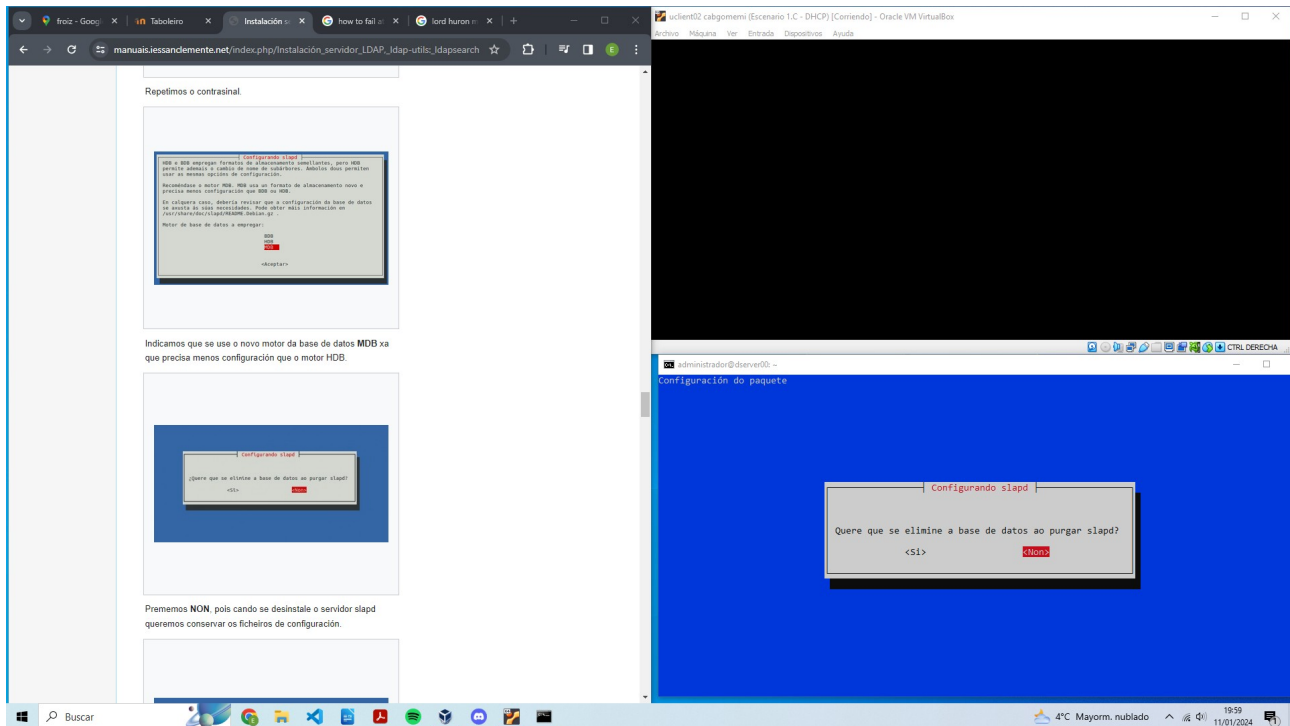
Menú de configuración OPENLDAP

Seleccionamos MBD (requiere de menos configuración).



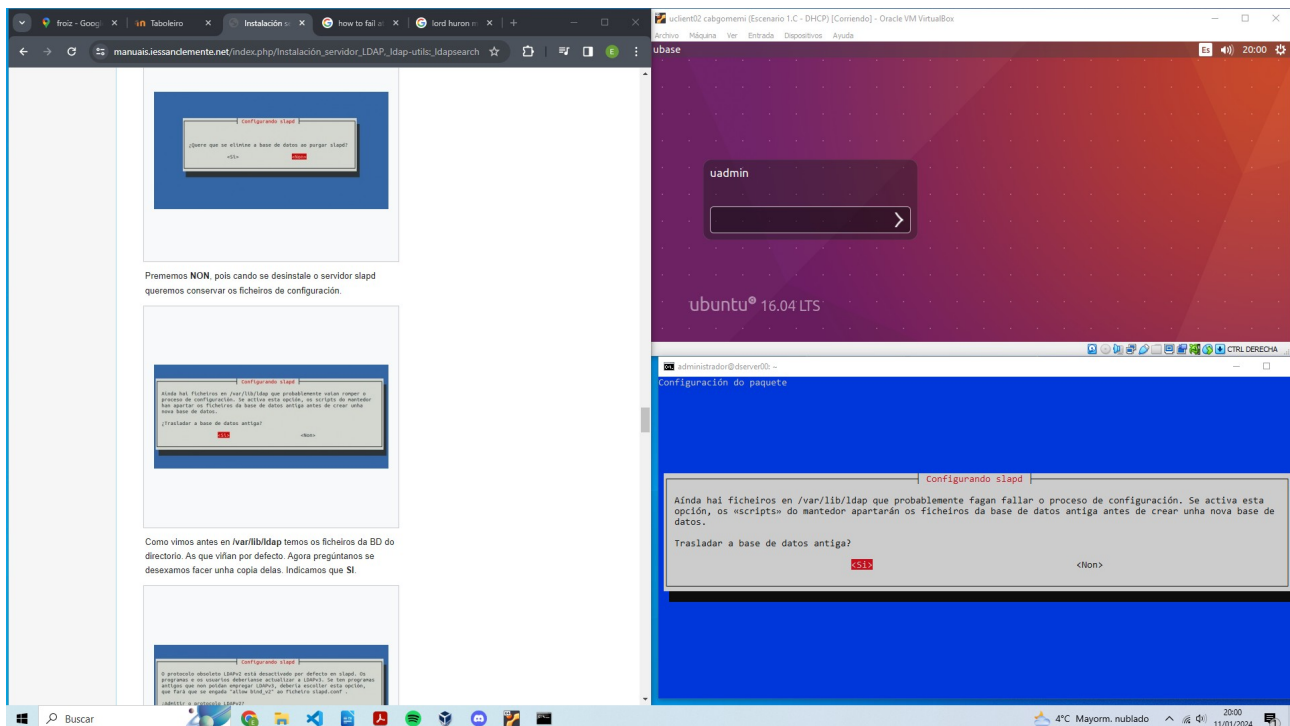
Menú de configuración OPENLDAP

Seleccionamos NON



Menú de configuración OPENLDAP

Seleccionamos SI



Menú de configuración OPENLDAP

Utilidades ldap: paquete ldap-utils

Instalación y comprobación de funcionamiento

Instalamos las utilidades mediante el comando

```
apt install ldap-utils -y
```

Comprobamos que las utilidades han sido instaladas correctamente mediante la emisión del comando.

```
root@dserver00:~# ldapsearch -x -b '' -s base objectclass=* namingcontexts
```

The screenshot shows a terminal window on the left and a diagram on the right. The terminal displays the output of the command `ldapsearch -x -b '' -s base objectclass=* namingcontexts`, showing the search result for the `namingContexts` attribute. The diagram, titled "Estrutura LDAP: Ponto de vista da xeraquia LDAP", shows a hierarchical tree structure of LDAP objects. The root is `dc=iescalquera,dc=local`, which branches into `ou=usuarios`, `ou=grupos`, and `ou=maquinas`. Under `ou=usuarios` are `cn=profes`, `cn=alumnos`, `cn=usuarios`, `cn=profes`, `cn=alum`, and `cn=bas01`. Under `ou=grupos` are `cn=profes`, `cn=alumnos`, `cn=usuarios`, `cn=profes`, `cn=alum`, and `cn=bas01`. Under `ou=maquinas` is `cn=bas01`. The terminal output shows the search result for the `namingContexts` attribute, indicating that the search was successful and returned one entry.

Output: `root@dserver00:~# ldapsearch -x -b '' -s base objectclass=* namingcontexts`

Consultamos la rama creada en el anterior paso mediante el siguiente comando.

```
ldapsearch -x -b 'dc=iescalquera,dc=local'
```

51 Platega I_II_III

The screenshot displays a Windows desktop environment with three main windows:

- Left Window (PDF Viewer):** Shows a document titled "Instalación servidor LDAP. ldap-utils: ldapsearch". It contains instructions in Spanish for consulting objects in the `dc=iescalquera,dc=local` branch and performing an `ldapsearch` command. The command is: `root@dserver00:~# ldapsearch -x -b 'dc=iescalquera,dc=local'`.
- Right Window (Diagram):** Titled "Estrutura LDAP: Punto de vista da xeraquia LDAP", it shows a hierarchical tree structure. The root is `dc=iescalquera,dc=local`, which branches into `ou=usuarios`, `ou=grupos`, and `ou=maquinas`. `ou=usuarios` further branches into `ou=profes`, `ou=alumnos`, `cn=profes`, `cn=alumnos`, `cn=profes`, `cn=alumnos`, and `ou=maquinas`. `ou=maquinas` branches into `cn=maquina01` and `cn=maquina02`.
- Bottom Window (Terminal):** Shows the output of the `ldapsearch` command. The output lists LDAPv3 search details and the structure of the LDAP tree, including the root `dc=iescalquera,dc=local` and its children `ou=usuarios`, `ou=grupos`, and `ou=maquinas`.

Output: `ldapsearch -x -b 'dc=iescalquera,dc=local'`

Mediante el siguiente comando comprobaremos que podemos acceder a la administración del servidor LDAP.

ldapsearch -Y EXTERNAL -H ldapi:// -b 'dc=iescalquera,dc=local'

Atención mediante la utilización de la opción -H ldapi:// indicamos que estamos realizando la conexión al servidor LDAP mediante una conexión local. Teniendo en cuenta que estamos trabajando en la máquina que corre el servidor LDAP esto es perfectamente normal.

De querer trabajar desde una ubicación de red tendríamos que introducir un nombre conocido o una dirección válida.

Output: `ldapsearch -Y EXTERNAL -H ldapi:// -b 'dc=iescalquera,dc=local'`

Mediante el siguiente comando comprobaremos que podemos acceder a la administración del servidor LDAP mediante el comando.

Finalización

Saldremos de ambas `shells` remotas.

Tomaremos una instantánea de ambas máquinas dado que hemos terminado el ejercicio.

ldapsearch -Y EXTERNAL -H ldapi:// -b 'dc=iescalquera,dc=local'

Atención mediante la utilización de la opción -H ldapi:// indicamos que estamos realizando la conexión al servidor LDAP mediante una conexión local. Teniendo en cuenta que estamos trabajando en la máquina que corre el servidor LDAP esto es perfectamente normal.

De querer trabajar desde una ubicación de red tendríamos que introducir un nombre conocido o una dirección válida.

```

root@server08: /home/administrador# ldapsearch -Y EXTERNAL -H ldapi:// -b 'dc=iescalquera,dc=local'
SASL/EXTERNAL authentication started
SASL username: gidNumber=0uidnumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
# extended LDIF
#
# LDAPv3
# base <dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# iescalquera.local
dn: dc=iescalquera,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: iescalquera
dc: iescalquera

# admin, iescalquera.local
dn: cn=admin,dc=iescalquera,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# usuarios, iescalquera.local
dn: ou=usuarios,dc=iescalquera,dc=local

```

Output: `ldapsearch -Y EXTERNAL -H ldapi:// -b 'dc=iescalquera,dc=local'`

En el anterior ejemplo de utilización de **ldapsearch** habíamos empleado la autenticación SASL implícita. En el siguiente ejemplo especificaremos la autenticación deseada.

ldapsearch -D cn=admin,dc=iescalquera,dc=local -w abc123. -H ldap://localhost -b 'dc=iescalquera,dc=local'

The screenshot shows a terminal window with the following output:

```
search: 2
result: 0 Success
# numResponses: 3
# numEntries: 2

• Indicando o usuario e contrasinal co que nos conectamos
• Observar a liña 24, pois como somos o usuario admin cnsinanos o hash asociado ao seu contrasinal.
• Observar como con -D indicamos o usuario e con -w o contrasinal.
• Nesta ocasión como uri usamos ldap://localhost, pero podería ser ldap://dserver00, ldap://dserver00.iescalquera.local (consultarase o DNS), etc.

root@dserver00:~# ldapsearch -D cn=admin,dc=iescalquera,dc=local -w abc123. -H ldap://localhost -b 'dc=iescalquera,dc=local'
# extended LDIF
#
# LDAPv3
# base <dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# iescalquera.local
dn: dc=iescalquera,dc=local
objectClass: top

Instalación servidor LDAP, ldap-utils: ldapsearch 140

objectClass: dcObject
objectClass: organization
o: iescalquera
dc: iescalquera

# admin, iescalquera.local
dn: cn=admin,dc=iescalquera,dc=local
objectClass: simpleSecurityObject
```

On the right, there is a diagram titled "Estrutura LDAP: Punto de vista da xeraquia LDAP" showing the hierarchy of the LDAP directory. The root is "dc=iescalquera,dc=local", which branches into "ou=usuarios", "ou=grupos", and "ou=equipamentos". "ou=usuarios" further branches into "ou=profes", "ou=alumnos", "ou=usuarios", "ou=profes", "ou=alum", and "ou=asoci". "ou=profes" branches into "cn=prof", "cn=prof", "ou=prof1", and "ou=prof2". "ou=alumnos" branches into "cn=alun", "cn=alun", "ou=alun1", and "ou=alun2". "ou=equipamentos" branches into "cn=equip", "cn=equip", "ou=equip1", and "ou=equip2".

Below the diagram, there is a terminal window showing the output of the command:

```
root@dserver00:/home/administrador# abc123. -H ldap://localhost -b 'dc=iescalquera,dc=local'
bash: abc123.: command not found
root@dserver00:/home/administrador# ldapsearch -D cn=admin,dc=iescalquera,dc=local -w abc123. -H ldap://localhost -b 'dc=iescalquera,dc=local'
# extended LDIF
#
# LDAPv3
# base <dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# iescalquera.local
dn: dc=iescalquera,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: iescalquera
dc: iescalquera

# admin, iescalquera.local
dn: cn=admin,dc=iescalquera,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: e1ntSEf9N6WvzAvU10BQzArZ1R3U2oxbNzDNHjYQ1tZEZF52c=

# usuarios, iescalquera.local
dn: ou=usuarios,dc=iescalquera,dc=local
```

Output: ldapsearch -D cn=admin,dc=iescalquera,dc=local -w abc123. -H ldap://localhost -b 'dc=iescalquera,dc=local'

Ahora emplearemos como URI **ldap://dserver00**

ldapsearch -D cn=admin,dc=iescalquera,dc=local -W -H ldap://dserver00 -b 'dc=iescalquera,dc=local'

51 Platega I_II_III

The screenshot shows a terminal window on the left and a diagram on the right. The terminal displays the output of an LDAP search command: `ldapsearch -x -b 'dc=iescalquera,dc=local' -s one`. The output shows a search result for the entry `cn=admin,dc=iescalquera,dc=local` with object classes `simpleSecurityObject` and `organizationalRole`. The diagram on the right, titled "Estrutura LDAP: Ponto de vista da xeraquia LDAP", shows a hierarchical tree structure. The root is `dc=iescalquera,dc=local`, which branches into `ou=usuarios`, `ou=grupos`, and `ou=maquinas`. Under `ou=usuarios` are `cn=profes` and `cn=alumnos`. Under `ou=grupos` are `cn=profes` and `cn=alum`. Under `ou=maquinas` is `cn=maqui01`. The terminal also shows the output of a search for `objectClass=*` which returns the same entry.

`ldapsearch -D cn=admin,dc=iescalquera,dc=local -W -H ldap://dserver00 -b 'dc=iescalquera,dc=local'`

Ahora realizaremos una búsqueda a un nivel de profundidad mediante el comando:

`ldapsearch -x -b 'dc=iescalquera,dc=local' -s one`

Mediante la opción “-s one” especificamos el nivel de profundidad de búsqueda.

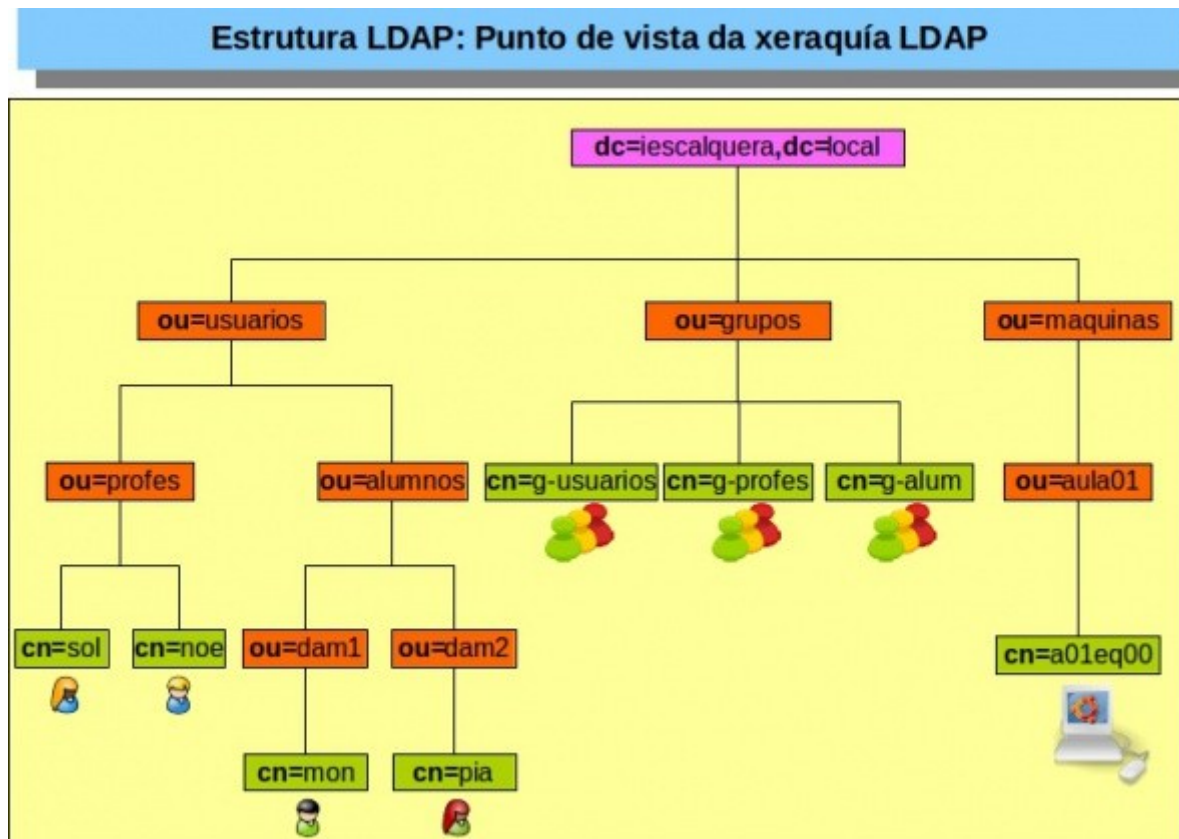
The screenshot shows a terminal window on the left and a diagram on the right. The terminal displays the output of an LDAP search command: `ldapsearch -x -b 'dc=iescalquera,dc=local' -s one`. The output shows a search result for the entry `cn=admin,dc=iescalquera,dc=local` with object classes `simpleSecurityObject` and `organizationalRole`. The diagram on the right, titled "Estrutura LDAP: Ponto de vista da xeraquia LDAP", shows a hierarchical tree structure. The root is `dc=iescalquera,dc=local`, which branches into `ou=usuarios`, `ou=grupos`, and `ou=maquinas`. Under `ou=usuarios` are `cn=profes` and `cn=alumnos`. Under `ou=grupos` are `cn=profes` and `cn=alum`. Under `ou=maquinas` is `cn=maqui01`. The terminal also shows the output of a search for `objectClass=*` which returns the same entry.

`ldapsearch -x -b 'dc=iescalquera,dc=local' -s one`

Administración de unidades organizativas, usuarios e grupos en LDAP con ldap-utils

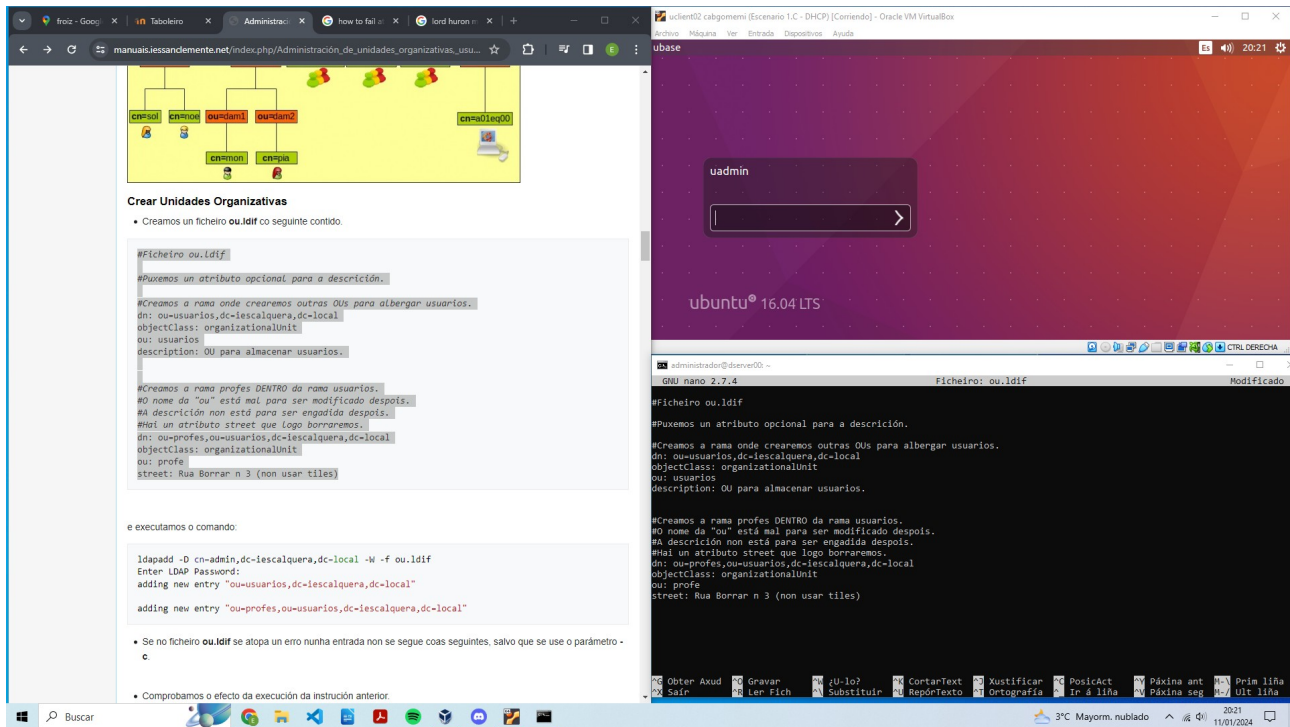
Creación de unidades organizativas

Crearemos la siguiente estructura



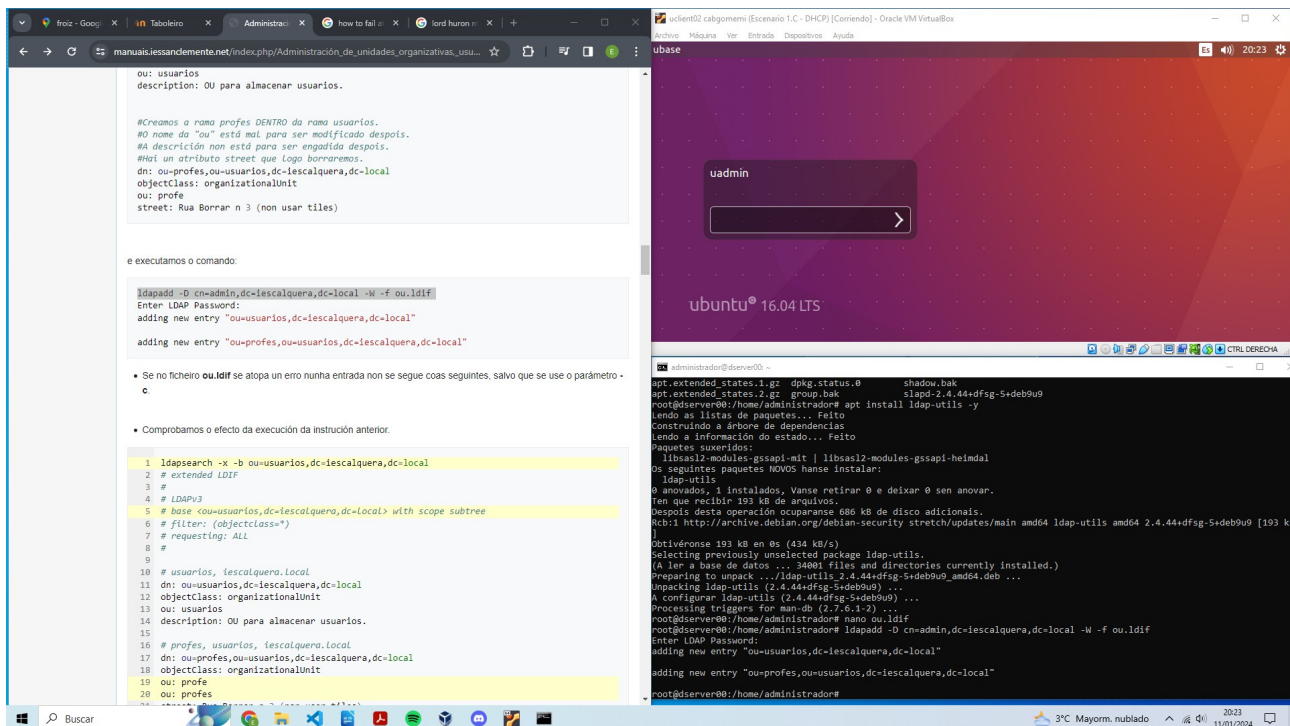
Fuente: Platega

Creamos el fichero ou.ldif



ficheiro ou.ldif

Ejecutamos el comando **ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou.ldif**



ficheiro ou.ldif

Comprobamos que las entradas se han añadido correctamente mediante la emisión del comando.

ldapsearch -x -b ou=usuarios,dc=iescalquera,dc=local

The screenshot shows a terminal window with the following content:

```

street: Rua Borrar n 3 (non usar tiles)
e executamos o comando:

Administración de unidades organizativas, usuarios e grupos en LDAP con ldap-utils 150

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=iescalquera,dc=local"
adding new entry "ou=profes,ou=usuarios,dc=iescalquera,dc=local"

• Se no ficheiro ou.ldif se atopa un erro nunha entrada non se segue coas seguintes, salvo que se use o parámetro -e.
• Comprobamos o efecto da execución da instrución anterior.

ldapsearch -x -b ou=usuarios,dc=iescalquera,dc=local
# extended LDIF
#
# LDAPv3
# base <ou=usuarios,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# usuarios, iescalquera.local
dn: ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: usuarios
description: OU para almacenar usuarios.

# profes, usuarios, iescalquera.local
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: profes
description: OU para almacenar profes.

# search result
search: 2
result: 0 Success
# numResponses: 3
# numEntries: 2
root@dserv00:/home/administrador#

```

On the right, there is a diagram titled "Estrutura LDAP: Punto de vista da xeraquía LDAP" showing a hierarchy starting from "dc=iescalquera,dc=local" and branching into "ou=usuarios", "ou=profes", and "ou=profes,ou=usuarios".

ldapsearch -x -b ou=usuarios,dc=iescalquera,dc=local

Tal y cómo podemos comprobar en la línea señalada nos hemos equivocado y hemos creado la **ou** **profe**. (Últimas dos líneas del ou.ldif).

Modificación de unidades organizativas

Creamos el fichero ou_modif.ldif

En el modificaremos la ou profe a profes, le añadiremos una descripción. Esto solventará el error cometido en el anterior paso.

Además, eliminar street.

El contenido del archivo será el siguiente.


```
#Ficheiro ou_modif.ldif

#Indicamos o obxecto que desexamos modificar
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
changetype: modify
replace: ou|
ou: profes|
-|
add: description|
description: OU para almacenar usuarios profes.
-|
delete: street
```

fichero ou_modif.ldif

The screenshot displays a web browser window with a document titled "42platega 1516_2 parte I-II LDAP". The document contains instructions for creating and modifying an LDAP entry. The instructions include creating a file named "ou_modif.ldif" and executing the "ldapadd" command to create the entry. The entry details are as follows:

- dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
- changetype: modify
- replace: ou
- ou: profes
- add: description
- description: OU para almacenar usuarios profes.
- delete: street

The terminal window shows the execution of the "ldapadd" command, which successfully creates the entry. The output of the "ldapssearch" command is also shown, confirming the entry's creation:

```
# extended LDIF
#
# LDAPv3
# base <ou=profes,ou=usuarios,dc=iescalquera,dc=local> with scope subtree
# filter: (objectClass=*)
# requesting: ALL
#
# profes, usuarios, iescalquera.local
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: profes
description: OU para almacenar usuarios profes.
```

fichero ou_modif.ldif

Ejecutamos el comando

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_modif.ldif

The screenshot displays a terminal window with the following content:

```
#Creamos un ficheiro ou_modif.ldif co seguinte contido.
#Imos realizar operacións na OU profes.
# Cambiar o valor do atributo ou
# Engadirle unha descrición
# Eliminar a unha rúa.

#Ficheiro ou_modif.ldif

#Indicamos o obxecto que desexamos modificar
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
changetype: modify
replace: ou
ou: profes
-|
add: description
description: OU para almacenar usuarios profes.
-|
delete: street

• Executamos o seguinte comando:

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_modif.ldif
Enter LDAP Password:
modifying entry "ou=profes,ou=usuarios,dc=iescalquera,dc=local"

• Observamos o efecto da instrución anterior.
• Observar que só temos un atributo ou, que non está o atributo street e si description.

ldapsearch -x -b ou=profes,ou=usuarios,dc=iescalquera,dc=local
# extended LDIF
#
# LDAPv3
# base <ou=profes,ou=usuarios,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# profes, usuarios, iescalquera.local
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: profes
description: OU para almacenar usuarios profes.
# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@dsrver00:/home/administrador# nano ou_modif.ldif
root@dsrver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_modif.ldif
Enter LDAP Password:
modifying entry "ou=profes,ou=usuarios,dc=iescalquera,dc=local"
root@dsrver00:/home/administrador#
```

On the right, a diagram titled "Estrutura LDAP: Punto de vista da xeraquia LDAP" shows the hierarchy:

- dc=iescalquera,dc=local
 - ou=usuarios
 - ou=profes
 - cn=prof1
 - cn=prof2
 - ou=prof1
 - cn=prof1
 - cn=prof2
 - ou=profes
 - cn=prof1
 - cn=prof2
 - ou=profes
 - cn=prof1
 - cn=prof2
 - ou=usuarios
 - cn=prof1
 - cn=prof2
 - ou=usuarios
 - cn=prof1
 - cn=prof2

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_modif.ldif

Comprobamos que el error ha quedado resuelto mediante el comando.

ldapsearch -x -b ou=profes,ou=usuarios,dc=iescalquera,dc=local

The screenshot shows a Linux desktop environment. On the left, a web browser displays a document titled "Estrutura LDAP: Ponto de vista da xeraquia LDAP". The document contains a hierarchical diagram of an LDAP directory structure. The root is "dc=iescalquera,dc=local", which branches into "ou=usuarios", "ou=profes", and "ou=grupos". Under "ou=usuarios", there are "ou=profes" and "ou=usuarios". Under "ou=profes", there are "ou=profes" and "ou=usuarios". Under "ou=usuarios", there are "ou=profes" and "ou=usuarios". The diagram also shows "ou=profes" and "ou=usuarios" under "ou=profes".

On the right, a terminal window shows the output of the command `ldapsearch -x -b ou=profes,ou=usuarios,dc=iescalquera,dc=local`. The output is as follows:

```
# extended LDIF
#
# LDAPv3
# base <ou=profes,ou=usuarios,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# profes, usuarios, iescalquera.local
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: profes
description: OU para almacenar usuarios profes.

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@dserv00:/home/administrador# nano ou_modif.ldif
root@dserv00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_modif.ldif
Enter LDAP Password:
modifying entry "ou=profes,ou=usuarios,dc=iescalquera,dc=local"

root@dserv00:/home/administrador# ldapsearch -x -b ou=profes,ou=usuarios,dc=iescalquera,dc=local
# extended LDIF
#
# LDAPv3
# base <ou=profes,ou=usuarios,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# profes, usuarios, iescalquera.local
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: profes
description: OU para almacenar usuarios profes.

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
root@dserv00:/home/administrador#
```

ldapsearch -x -b ou=profes,ou=usuarios,dc=iescalquera,dc=local

Eliminar Unidades Organizativas

Comando ldapadd

Crearemos el fichero ou_borrar1.ldif

```
#Ficheiro ou_borrar1.ldif

#Debemos borrar antes os obxectos fillos que o pai.
#Non o imos facer para propiciar un erro

#dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
#changetype: delete

dn: ou=usuarios,dc=iescalquera,dc=local
changetype: delete
```

Eliminar Unidades Organizativas

- Para eliminar unidades organizativas podemos usar:
 - ldapadd**, onde lle pasamos o ficheiro cos DN's dos obxectos e a función a realizar con eles (eliminar).
 - ldapdelete**, onde lle podemos pasar o ficheiro directamente cos DN's dos obxectos a eliminar ou mesmo podemos indicarllos por consola.
- Exemplo 1: ldapadd**

```
#Ficheiro ou_borrar1.ldif

#Debemos borrar antes os obxectos fillos que o pai
#Non o imos facer para propiciar un erro

dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
#changeltype: delete

dn: ou=usuarios,dc=iescalquera,dc=local
#changeltype: delete
```

 - Executamos o seguinte comando e vemos que non nos borra a ou=usuarios porque contén fillos.
 - Se descomentamos as liñas anteriores referentes a ou=profes o resultado sería positivo.

```
ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_borrar1.ldif
Enter LDAP Password:
deleting entry "ou=usuarios,dc=iescalquera,dc=local"
ldap_delete: Operation not allowed on non-leaf (66)
additional info: subordinate objects must be deleted first
```
- Exemplo 2: ldapdelete**
 - Podemos crear un ficheiro semellante ao seguinte onde só indicamos os DN's dos obxectos a borrar.
 - Igual que antes hai que indicar os obxectos fillos ante ca o pai.
 - Se se usa o parámetro **-r** podemos indicar só o pai e vai borrar os obxectos fillos en modo recursivo.

```
#Ficheiro ou_borrar2.ldif

#Debemos borrar antes os obxectos fillos que o pai.
#Non o imos facer para propiciar un erro

dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
dn: ou=usuarios,dc=iescalquera,dc=local
```

ou_borrar1.ldif

Ejecutamos el comando. **ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_borrar1.ldif**

```
Seleccin administrador@dserver00: ~
# LDAPv3
# base <ou=profes,ou=usuarios,dc=iescalquera,dc=local> with scope baseObject
# filter: (objectclass=*)
# requesting: ALL
#
# profes, usuarios, iescalquera.local
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: profes
description: OU para almacenar usuarios profes.

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
root@dserver00:/home/administrador# ls
ou.ldif ou_modif.ldif
root@dserver00:/home/administrador# ou_borrar1.ldif
bash: ou_borrar1.ldif: non se atopou a orde
root@dserver00:/home/administrador# nano ou_borrar1.ldif
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f ou_borrar1.ldif
Enter LDAP Password:
deleting entry "ou=usuarios,dc=iescalquera,dc=local"
ldap_delete: Operation not allowed on non-leaf (66)
additional info: subordinate objects must be deleted first
root@dserver00:/home/administrador#
```

Tal y como podemos comprobar primero **deberemos eliminar los objetos subordinados**. Por el momento, profes se encuentra dentro de usuarios. Por lo que nos es imposible eliminar usuarios.

ATENCION ATENCION ATENCION

El fichero que emplearemos en el comando ldapadd será el anterior puesto que si aplicamos el fichero a continuación. Eliminará el trabajo hecho.

```
#Ficheiro ou_borrar2.ldif

#Debemos borrar antes os obxectos fillos que o pai.
#Non o imos facer para propiciar un erro

dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
dn: ou=usuarios,dc=iescalquera,dc=local
```

Cómo podemos ver el fichero elimina primero la unidad organizacional profes y luego usuarios.

Comando Idapdelete

En la siguiente sección crearemos la estructura de 0.

A continuación eliminaremos toda la estructura.

```
ldapdelete -D cn=admin,dc=iescalquera,dc=local -W "ou=usuarios,dc=iescalquera,dc=local" -r
```

Administración de unidades organizativas, usuarios y grupos en LDAP con ldap-utils

153

Unidades Organizativas: ejercicio para o/a lector/a

- Todo o visto até agora é aplicable a calquera tipo de obxecto do LDAP (usuarios, grupos, etc)
- Agora o lector ou lectora debe ser quen de crear un ficheiro **ou_final.ldif** coas unidades organizativas seguintes:
 - dn: ou=usuarios,dc=iescalquera,dc=local
 - dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
 - dn: ou=grupos,dc=iescalquera,dc=local
 - dn: ou=alumn,ou=usuarios,dc=iescalquera,dc=local
 - dn: ou=daml,ou=alumn,ou=usuarios,dc=iescalquera,dc=local

Recorte y anotación

154

Estructura LDAP: Punto de vista da xeraquía LDAP

```

dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
dn: ou=usuarios,dc=iescalquera,dc=local

# Necesita ocasión non imos usar o ficheiro anterior, que se cargaría con -f igual que en ldapadd.
# Imos borrar todo á árbore de usuarios en modo recursivo (-x) coa instrución:
ldapdelete -x cn=admin,dc=iescalquera,dc=local -W "ou=usuarios,dc=iescalquera,dc=local" -r
Enter LDAP Password:

```

```

root@dserv00:/home/administrador# ls
ou.ldif ou_modif.ldif
root@dserv00:/home/administrador# ou_borrar1.ldif
bash: ou_borrar1.ldif: non se atopou a orde
root@dserv00:/home/administrador# nano ou_borrar1.ldif
Enter LDAP Password:
deleting entry "ou=usuarios,dc=iescalquera,dc=local"
ldap_delete: Operation not allowed on non-leaf (66)
additional info: subordinate objects must be deleted first

root@dserv00:/home/administrador# ldapdelete -x cn=admin,dc=iescalquera,dc=local -W "ou=usuarios,dc=iescalquera,dc=local" -r
Enter LDAP Password:
root@dserv00:/home/administrador#

```

```
ldapdelete -D cn=admin,dc=iescalquera,dc=local -W "ou=usuarios,dc=iescalquera,dc=local" -r
```

Unidades Organizativas: ejercicio para o/a lector/a

Luego de eliminar crearemos el archivo ou_final.ldif.

Deberá tener el siguiente contenido.

- dn: ou=usuarios,dc=iescalquera,dc=local
- dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
- dn: ou=grupos,dc=iescalquera,dc=local
- dn: ou=alum,ou=usuarios,dc=iescalquera,dc=local
- dn: ou=dam1,ou=alum,ou=usuarios,dc=iescalquera,dc=local

Una vez hemos creado el fichero con el siguiente contenido.

```
administrador@diervo0:~$ cat ou_final.ldif
# Creamos un atributo opcional para la descripción.
dn: ou=usuarios,dc=iescalquera,dc=local
objectclass: organizationalunit
ou: usuarios
description: OU para almacenar usuarios.

# Creamos a rama profes DENTRO de rama usuarios.
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectclass: organizationalunit
ou: profes
description: OU para almacenar usuarios/as profes.

# Creamos la rama Grupos dentro de el dc iescalquera.local
dn: ou=grupos,dc=iescalquera,dc=local
objectclass: organizationalunit
ou: grupos
description: OU para almacenar los grupos.

# Creamos la rama alum dentro de el dc iescalquera.local
dn: ou=alum,ou=usuarios,dc=iescalquera,dc=local
objectclass: organizationalunit
ou: alum
description: OU para almacenar los alumnos.

# Creamos la rama dam1 dentro de el dc iescalquera.local
dn: ou=dam1,ou=alum,ou=usuarios,dc=iescalquera,dc=local
objectclass: organizationalunit
ou: dam1
description: OU para almacenar los alumnos de DAM1.
```

Ejecutamos el comando **ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f ou_final.ldif**

51 Platega I_II_III

```
administrador@dserv00 -  
shell returned 16  
Press ENTER or type command to continue  
[No write since last change]  
No manual entry for DAM1  
shell returned 16  
Press ENTER or type command to continue  
root@dserv00:/home/administrador# ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f ou_  
ou_borrar1.ldif ou_borrar2.ldif ou_final.ldif ou_modif.ldif  
root@dserv00:/home/administrador# ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f ou_  
ou_borrar1.ldif ou_borrar2.ldif ou_final.ldif ou_modif.ldif  
root@dserv00:/home/administrador# ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f ou_  
ou_borrar1.ldif ou_borrar2.ldif ou_final.ldif ou_modif.ldif  
root@dserv00:/home/administrador# ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f ou_final.ldif  
Enter LDAP Password:  
adding new entry "ou-usuarios,dc=iescalquera,dc=local"  
adding new entry "ou-profes,ou-usuarios,dc=iescalquera,dc=local"  
adding new entry "ou-grupos,dc=iescalquera,dc=local"  
adding new entry "ou-alum,ou-usuarios,dc=iescalquera,dc=local"  
adding new entry "ou-dam1,ou-alum,ou-usuarios,dc=iescalquera,dc=local"  
root@dserv00:/home/administrador# vim ou_final.ldif  
root@dserv00:/home/administrador# root@dserv00:/home/administrador#
```

Para comprobar el resultado de el añadido ejecutamos el comando:

Atención, es un comando distinto que el indicado en el platega, para que nos aparezcan los grupos.

ldapsearch -x -b dc=iescalquera,dc=local

```
administrador@dserv00 -  
root@dserv00:/home/administrador# root@dserv00:/home/administrador# ldapsearch -x -b ou-usuarios,dc=iescalquera,dc=local  
root@dserv00:/home/administrador# ldapsearch -x -b dc=iescalquera,dc=local  
# extended LDIF  
#  
# LDAPv3  
# base <dc=iescalquera,dc=local> with scope subtree  
# filter: (objectclass=*)  
# requesting: All  
#  
# iescalquera.local  
dn: dc=iescalquera,dc=local  
objectclass: top  
objectclass: dcObject  
objectclass: organization  
o: iescalquera  
dc: iescalquera  
# admin, iescalquera.local  
dn: cn=admin,dc=iescalquera,dc=local  
objectclass: simpleSecurityObject  
objectclass: organizationalRole  
cn: admin  
description: LDAP administrator  
# usuarios, iescalquera.local  
dn: ou=usuarios,dc=iescalquera,dc=local  
objectclass: organizationalUnit  
ou: usuarios  
description: OU para almacenar usuarios.  
# profes, usuarios, iescalquera.local  
dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local  
objectclass: organizationalUnit  
ou: profes  
description: OU para almacenar usuarios/as profes.  
# grupos, iescalquera.local  
dn: ou=grupos,dc=iescalquera,dc=local  
objectclass: organizationalUnit  
ou: grupos  
description: OU para almacenar os grupos.  
# alum, usuarios, iescalquera.local  
dn: ou=alum,ou=usuarios,dc=iescalquera,dc=local  
objectclass: organizationalUnit  
ou: alum  
description: OU para almacenar os alumnos.  
# dam1, alum, usuarios, iescalquera.local  
dn: ou=dam1,ou=alum,ou=usuarios,dc=iescalquera,dc=local  
objectclass: organizationalUnit  
ou: dam1  
description: OU para almacenar os alumnos de DAM1.  
# search result  
search: 2  
result: 0 Success  
# numResponses: 8  
# numEntries: 7  
root@dserv00:/home/administrador#
```

Administración de grupos

Creamos el siguiente archivo para introducir los grupos.

grupos_final.ldif

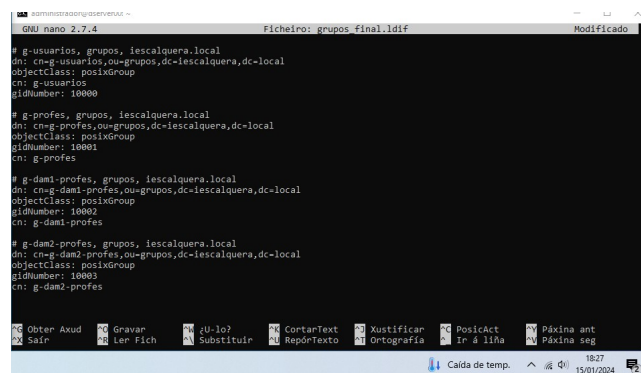
Este tendrá el siguiente contenido:

dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local

dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local

dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local

dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local



```

# g-usuarios, grupos, iescalquera.local
dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
cn: g-usuarios
gidNumber: 10000

# g-profes, grupos, iescalquera.local
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidNumber: 10001
cn: g-profes

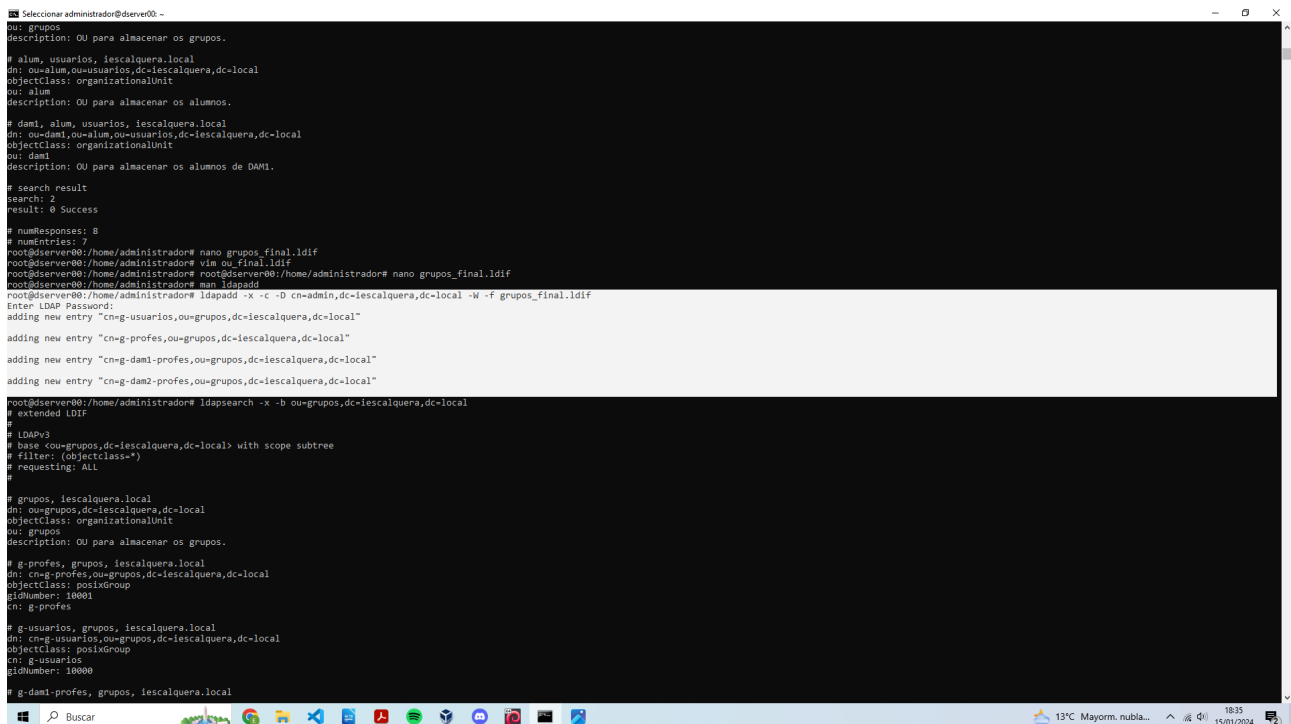
# g-dam1-profes, grupos, iescalquera.local
dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidNumber: 10002
cn: g-dam1-profes

# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidNumber: 10003
cn: g-dam2-profes

```

Ejecutamos el siguiente comando para hacer efectivos los cambios.

ldapadd -x -c -D cn=admin,dc=iescalquera,dc=local -W -f grupos_final.ldif



```

Selección administrador@dserv00: ~
ou: grupos
description: OU para almacenar los grupos.

# alum, usuarios, iescalquera.local
dn: ou=alum,ou=usuarios,dc=iescalquera,dc=local
objectclass: organizationalUnit
ou: alum
description: OU para almacenar los alumnos.

# dam1, alum, usuarios, iescalquera.local
dn: ou=dam1,ou=alum,ou=usuarios,dc=iescalquera,dc=local
objectclass: organizationalUnit
ou: dam1
description: OU para almacenar los alumnos de DAM1.

# search result
search: 2
result: 0 Success

# numResponses: 8
# numEntries: 7
root@dserv00:/home/administrador# nano grupos_final.ldif
root@dserv00:/home/administrador# vim ou_final.ldif
root@dserv00:/home/administrador# root@dserv00:/home/administrador# nano grupos_final.ldif
root@dserv00:/home/administrador# man ldapadd
root@dserv00:/home/administrador# ldapadd -x -c -D cn=admin,dc=iescalquera,dc=local -W -f grupos_final.ldif
Enter LDAP Password:
adding new entry "cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local"
adding new entry "cn=g-profes,ou=grupos,dc=iescalquera,dc=local"
adding new entry "cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local"
adding new entry "cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local"

root@dserv00:/home/administrador# ldapsearch -x -b ou=grupos,dc=iescalquera,dc=local
extended LDIF
#
# LDAPv3
# base <ou=grupos,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# grupos, iescalquera.local
dn: ou=grupos,dc=iescalquera,dc=local
objectclass: organizationalUnit
ou: grupos
description: OU para almacenar los grupos.
#
# g-profes, grupos, iescalquera.local
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidNumber: 10001
cn: g-profes
#
# g-usuarios, grupos, iescalquera.local
dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
cn: g-usuarios
gidNumber: 10000
#
# g-dam1-profes, grupos, iescalquera.local

```

Ejecutamos el siguiente comando para comprobar que las entradas se han añadido correctamente.

ldapsearch -x -b ou=grupos,dc=iescalquera,dc=local

```
Seleccionar administrador@server00: -
adding new entry "cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local"
adding new entry "cn=g-profes,ou=grupos,dc=iescalquera,dc=local"
adding new entry "cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local"
adding new entry "cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local"
root@server00:/home/administrador# ldapsearch -x -b ou=grupos,dc=iescalquera,dc=local
# extended LDIF
#
# LDAPv3
# base <ou=grupos,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# grupos, iescalquera.local
dn: ou=grupos,dc=iescalquera,dc=local
objectclass: organizationalunit
ou: grupos
description: OU para almacenar os grupos.
# g-profes, grupos, iescalquera.local
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidnumber: 10001
cn: g-profes
# g-usuarios, grupos, iescalquera.local
dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
cn: g-usuarios
gidnumber: 10000
# g-dam1-profes, grupos, iescalquera.local
dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidnumber: 10002
cn: g-dam1-profes
# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectclass: posixGroup
gidnumber: 10003
cn: g-dam2-profes
# search result
search: 2
result: 0 Success
# numResponses: 6
# numEntries: 5
root@server00:/home/administrador#
```

Administración de usuarios

Creamos el archivo usuarios.ldif con el siguiente contenido.

```

administrador@dserver00: ~
GNU nano 2.7.4                               Ficheiro: usuarios.ldif          Modificado
#Ficheiro usuarios.ldif

#Observar onde se poñen tiles e onde non. Non é preciso poñelas
#Observar tamén que se indica o gid do grupo primario (10000 -> g-usuarios)
#Finalmente indicase que o contrasinal nunca expira.

dn: uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: sol
sn: Lúa
cn: Profe - Sol Lúa
givenName: Sol
displayName: Profe - Sol Lúa
uidNumber: 10000
gidNumber: 10000
userPassword: abc123.
gecos: Profe - Sol Lua
loginShell: /bin/bash
homeDirectory: /home/sol
mail: sol@iescalquera.local
initials: SL
shadowExpire: -1

```

Ejecutamos el siguiente comando para configurar correctamente la entrada.

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f usuarios.ldif

```

Seleccíonador administrador@dserver00: ~
gidNumber: 10000

# g-dam1-profes, grupos, iescalquera.local
dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10002
cn: g-dam1-profes

# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10003
cn: g-dam2-profes

# search result
search: 2
result: 0 Success

# numResponses: 6
# numEntries: 5
root@dserver00:/home/administrador# nano usuarios.ldif
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f usuarios.ldif
Enter LDAP Password:
adding new entry "uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local"

root@dserver00:/home/administrador#

```

Añadir usuarios a los grupos secundarios

Crearemos el fichero **grupos_secundarios.ldif** con el siguiente contenido:

```

administrador@dserver00: ~
GNU nano 2.7.4 Fichero: grupos_secundarios.ldif Modificado
#Fichero grupos_secundarios.ldif
#Observar que os grupos sepáranse por unha liña en branco
#Se tivéramos máis usuarios para un grupo seguiríamos poñendo: memberUid: usuario
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
add: memberUid
memberUid:sol

dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
add: memberUid
memberUid:sol

dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
add: memberUid
memberUid:sol

Grava-lo buffer modificado? (Respondendo "Non" descartará os cambios).
S Si
N Non  C Cancelar

```

Ejecutamos el comando para hacer efectivas las entradas.

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f grupos_secundarios.ldif -c

```

administrador@dserver00: ~
gidNumber: 10002
cn: g-dam1-profes

# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10003
cn: g-dam2-profes

# search result
search: 2
result: 0 Success

# numResponses: 6
# numEntries: 5
root@dserver00:/home/administrador# nano usuarios.ldif
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f usuarios.ldif
Enter LDAP Password:
adding new entry "uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local"

root@dserver00:/home/administrador# nano grupos_secundarios.ldif
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f grupos_secundarios.ldif -c
Enter LDAP Password:
modifying entry "cn=g-profes,ou=grupos,dc=iescalquera,dc=local"

modifying entry "cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local"

modifying entry "cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local"

root@dserver00:/home/administrador#

```


Eliminar/modificar usuarios

Tomaremos una instantánea para poder retornar al proceso anterior.

Crearemos el siguiente fichero para eliminar el usuario recientemente creado.

Recordemos que deberemos eliminar el usuario de todos los subgrupos creados.

```
administrador@dserv03 ~$
# fichero usuarios_borrar.ldif
# En este fichero modificaremos las entradas del fichero para que se eliminen las entradas de usuarios
# que se crearon anteriormente.

dn: cn=profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
delete: memberuid
memberuid:sol

dn: cn=dam1-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
delete: memberuid
memberuid:sol

dn: cn=dam2-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
delete: memberuid
memberuid:sol

usuarios_borrar.ldif* 19L, 488C
```

Ejecutaremos el comando

ldapmodify -D cn=admin,dc=iescalquera,dc=local -W -f usuarios_borrar.ldif

Comprobaremos que los usuarios se han eliminado correctamente mediante el comando

ldapsearch -x -b ou=grupos,dc=iescalquera,dc=local

51 Platega I_II_III

```
Seleccionar administrador@dserv00: ~
memberUid: sol
root@dserv00:/home/administrador# vim usuarios_borrar.ldif
root@dserv00:/home/administrador# root@dserv00:/home/administrador# ldapmodify -D cn=admin,dc=iescalquera,dc=local -W -f usuarios_borrar.ldif
Enter LDAP Password:
modifying entry "cn=g-profes,ou=grupos,dc=iescalquera,dc=local"
modifying entry "cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local"
modifying entry "cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local"

root@dserv00:/home/administrador# ldapsearch -x -b ou=grupos,dc=iescalquera,dc=local
# extended LDIF
#
# LDAPv3
# base <ou=grupos,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# grupos, iescalquera.local
dn: ou=grupos,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: grupos
description: OU para almacenar os grupos.

# g-profes, grupos, iescalquera.local
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10001
cn: g-profes

# g-usuarios, grupos, iescalquera.local
dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
cn: g-usuarios
gidNumber: 10000

# g-dam1-profes, grupos, iescalquera.local
dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10002
cn: g-dam1-profes

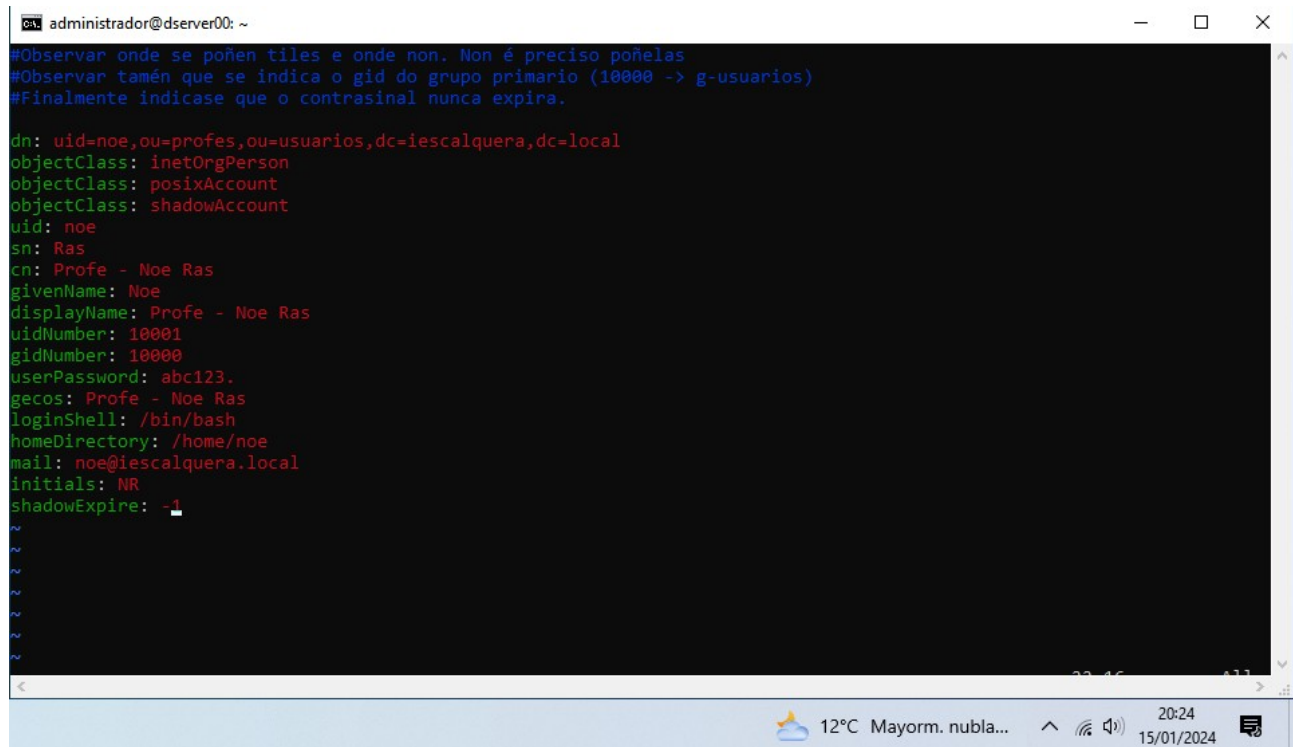
# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10003
cn: g-dam2-profes

# search result
search: 2
result: 0 Success

# numResponses: 6
# numEntries: 5
root@dserv00:/home/administrador#
```

Usuarios: ejercicio para el lector

Crearemos el fichero para añadir a la usuaria noe con el siguiente contenido.



```
administrador@dserver00: ~  
#Observar onde se poñen tiles e onde non. Non é preciso poñelas  
#Observar tamén que se indica o gid do grupo primario (10000 -> g-usuarios)  
#Finalmente indicase que o contrasinal nunca expira.  
  
dn: uid=noe,ou=profes,ou=usuarios,dc=iescalquera,dc=local  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
uid: noe  
sn: Ras  
cn: Profe - Noe Ras  
givenName: Noe  
displayName: Profe - Noe Ras  
uidNumber: 10001  
gidNumber: 10000  
userPassword: abc123.  
gecos: Profe - Noe Ras  
loginShell: /bin/bash  
homeDirectory: /home/noe  
mail: noe@iescalquera.local  
initials: NR  
shadowExpire: -1
```

Ejecutamos el comando para hacer efectivas las entradas.

```
ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f usuarios_final.ldif
```

Crearemos el archivo para modificar los grupos.

```

#Ficheiro grupos_secundarios_final.ldif

#Observar que os grupos sepáranse por unha liña en branco
#Se tivéramos máis usuarios para un grupo seguiríamos poñendo: memberUid: usuario
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
add: memberUid
memberUid: noe

dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
changetype: modify
add: memberUid
memberUid: noe

"grupos_secundarios_final.ldif" 14L, 391C written

```

Ejecutamos el comando para hacer efectivas las entradas.

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f grupos_secundarios.ldif -c

```

Seleccionar administrador@dserver00: ~
Permission denied, please try again.
administrador@192.168.1.40's password:
Linux dserver00 4.9.0-19-amd64 #1 SMP Debian 4.9.320-2 (2022-06-30) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 15 19:33:25 2024 from 192.168.1.40
administrador@dserver00:~$ su
Password:
root@dserver00:/home/administrador# ls
grupos_final.ldif      ou_borrar1.ldif  ou.ldif           usuarios_final.ldif
grupos_secundarios_final.ldif  ou_borrar2.ldif  ou_modif.ldif     usuarios.ldif
grupos_secundarios.ldif  ou_final.ldif    usuarios_borrar.ldif
root@dserver00:/home/administrador# vim grupos_secundarios
grupos_secundarios_final.ldif grupos_secundarios.ldif
root@dserver00:/home/administrador# vim grupos_secundarios_final.ldif
root@dserver00:/home/administrador# root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=^Ccal l
cldif -cpos_secundarios_fina.ldif -c
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f grupos_secundarios_final.ldif -
c
Enter LDAP Password:
modifying entry "cn=g-profes,ou=grupos,dc=iescalquera,dc=local"

modifying entry "cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local"

root@dserver00:/home/administrador#

```

Comprobamos que los cambios se han efectuado correctamente mediante el comando.

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f grupos_secundarios_final.ldif -c

51 Platega I_II_III

```
administrador@dserver00: ~
grupos_secundarios.ldif      ou_final.ldif      usuarios_borrar.ldif
root@dserver00:/home/administrador# vim grupos_secundarios
grupos_secundarios_final.ldif grupos_secundarios.ldif
root@dserver00:/home/administrador# vim grupos_secundarios_final.ldif
root@dserver00:/home/administrador# root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=^Ccal l
cldif -cpos_secundarios_fina.ldif -c
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f grupos_secundarios_final.ldif -
c
Enter LDAP Password:
modifying entry "cn=g-profes,ou=grupos,dc=iescalquera,dc=local"

modifying entry "cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local"

root@dserver00:/home/administrador# ldapsearch -x -b ou=grupos,dc=iescalquera,dc=local
# extended LDIF
#
# LDAPv3
# base <ou=grupos,dc=iescalquera,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# grupos, iescalquera.local
dn: ou=grupos,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: grupos
description: OU para almacenar os grupos.

# g-profes, grupos, iescalquera.local
dn: cn=g-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10001
cn: g-profes
memberUid: sol
memberUid: noe

# g-usuarios, grupos, iescalquera.local
dn: cn=g-usuarios,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
cn: g-usuarios
gidNumber: 10000

# g-dam1-profes, grupos, iescalquera.local
dn: cn=g-dam1-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10002
cn: g-dam1-profes
memberUid: sol

# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10003
cn: g-dam2-profes
memberUid: sol
memberUid: noe

# search result
search: 2
result: 0 Success

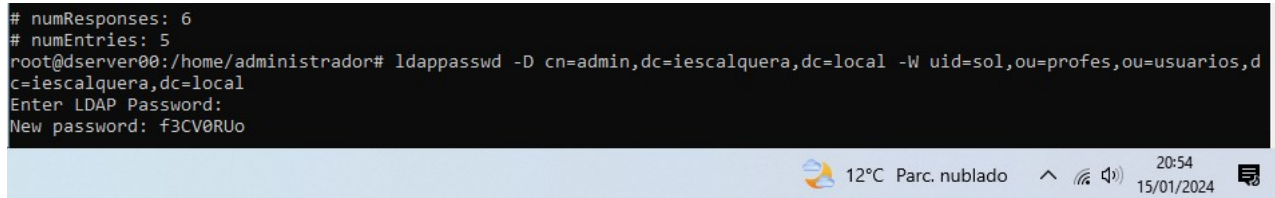
# numResponses: 6
# numEntries: 5
```

Cambiar la contraseña de un usuario

Si no le proveemos de ninguna contraseña provee una contraseña aleatoria.

**ldappasswd -D cn=admin,dc=iescalquera,dc=local -W
uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local**

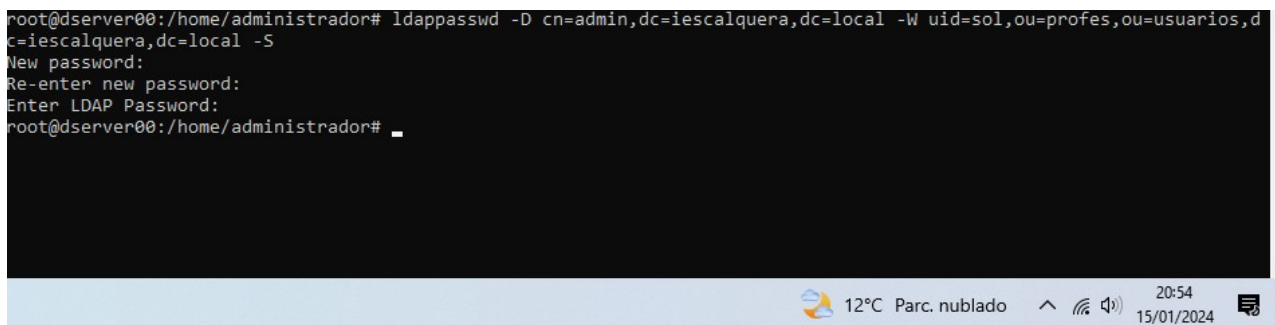
```
# numResponses: 6
# numEntries: 5
root@dserver00:/home/administrador# ldappasswd -D cn=admin,dc=iescalquera,dc=local -W uid=sol,ou=profes,ou=usuarios,d
c=iescalquera,dc=local
Enter LDAP Password:
New password: f3CV0RUo
```

A terminal window with a black background and white text. The prompt is 'root@dserver00:/home/administrador#'. The command entered is 'ldappasswd -D cn=admin,dc=iescalquera,dc=local -W uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local'. The output shows 'Enter LDAP Password:' followed by a blank line, and 'New password: f3CV0RUo'. The window has a taskbar at the bottom with a weather icon (12°C, Parc. nublado), network and volume icons, and a clock showing 20:54 on 15/01/2024.

Mediante la opción -S nos promptea a escribir una nueva contraseña.

**ldappasswd -D cn=admin,dc=iescalquera,dc=local -W
uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local -S**

```
root@dserver00:/home/administrador# ldappasswd -D cn=admin,dc=iescalquera,dc=local -W uid=sol,ou=profes,ou=usuarios,d
c=iescalquera,dc=local -S
New password:
Re-enter new password:
Enter LDAP Password:
root@dserver00:/home/administrador#
```

A terminal window with a black background and white text. The prompt is 'root@dserver00:/home/administrador#'. The command entered is 'ldappasswd -D cn=admin,dc=iescalquera,dc=local -W uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local -S'. The output shows 'New password:', 'Re-enter new password:', and 'Enter LDAP Password:' followed by a blank line. The window has a taskbar at the bottom with a weather icon (12°C, Parc. nublado), network and volume icons, and a clock showing 20:54 on 15/01/2024.

Podemos modificar la contraseña de un usuario mediante un archivo de modificación *.ldif

51 Platega I_II_III

```
administrador@dserver00: ~
GNU nano 2.7.4                               Ficheiro: password_sol.ldif      Modificado
dn: uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local
changetype: modify
replace: userPassword
userPassword:novo contrasinal

Grava-lo buffer modificado? (Respondendo "Non" descartará os cambios).
S Si
N Non      ^C Cancelar
```

Ejecutamos el comando para hacer efectivas las entradas.

ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f password_sol.ldif

```
administrador@dserver00: ~
# g-dam2-profes, grupos, iescalquera.local
dn: cn=g-dam2-profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
gidNumber: 10003
cn: g-dam2-profes
memberUid: sol
memberUid: noe

# search result
search: 2
result: 0 Success

# numResponses: 6
# numEntries: 5
root@dserver00:/home/administrador# ldappasswd -D cn=admin,dc=iescalquera,dc=local -W uid=sol,ou=profes,ou=usuarios,d
c=iescalquera,dc=local
Enter LDAP Password:
New password: f3CV0RUo
root@dserver00:/home/administrador# ldappasswd -D cn=admin,dc=iescalquera,dc=local -W uid=sol,ou=profes,ou=usuarios,d
c=iescalquera,dc=local -S
New password:
Re-enter new password:
Enter LDAP Password:
root@dserver00:/home/administrador# nano password_sol.ldif
root@dserver00:/home/administrador# ldapadd -D cn=admin,dc=iescalquera,dc=local -W -f password_sol.ldif
Enter LDAP Password:
modifying entry "uid=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local"

root@dserver00:/home/administrador#
```

Herramientas incluidas con el servidor LDAP

Slapindex este comando puede ser muy útil en caso de apagones accidentales del servidor LDAP, ya que es posible que los índices utilizados para acceder a la información del directorio se corrompan, lo que puede provocar errores en la búsqueda o inserción de información en el directorio e incluso que el servidor LDAP no pueda arrancar. **La función del comando es regenerar los índices a partir de la información almacenada en el directorio**, creando así de nuevo las estructuras necesarias para que el servicio LDAP funcione correctamente.

¿Cómo realizar la secuencia de comandos necesarias para realizar un Slapindex?

```
service slapd stop
su - openldap -s /bin/bash
/usr/sbin/slapindex -v
service slapd start
```

```
root@dserver00:/home/administrador# service slapd stop
root@dserver00:/home/administrador# su - openldap -s /bin/bash
openldap@dserver00:~$ /usr/sbin/slapindex -v
indexing id=00000001
indexing id=00000002
indexing id=00000003
indexing id=00000004
indexing id=00000005
indexing id=00000006
indexing id=00000007
indexing id=00000008
indexing id=00000009
indexing id=0000000a
indexing id=0000000b
indexing id=0000000c
indexing id=0000000d
openldap@dserver00:~$ exit
logout
root@dserver00:/home/administrador# service slapd start
root@dserver00:/home/administrador# _
```

12°C Parc. nublado 21:08 15/01/2024

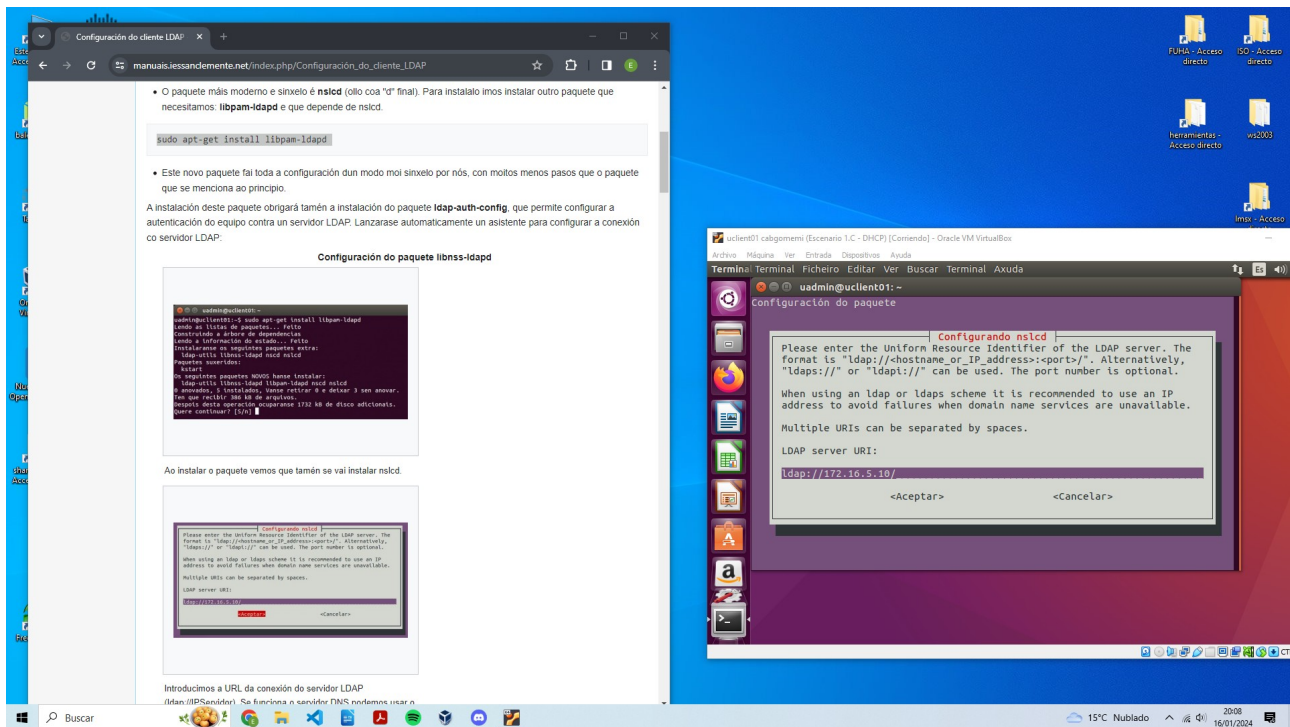
Configuración del cliente LDAP

Instalar los paquetes necesarios

Empleamos el siguiente comando.

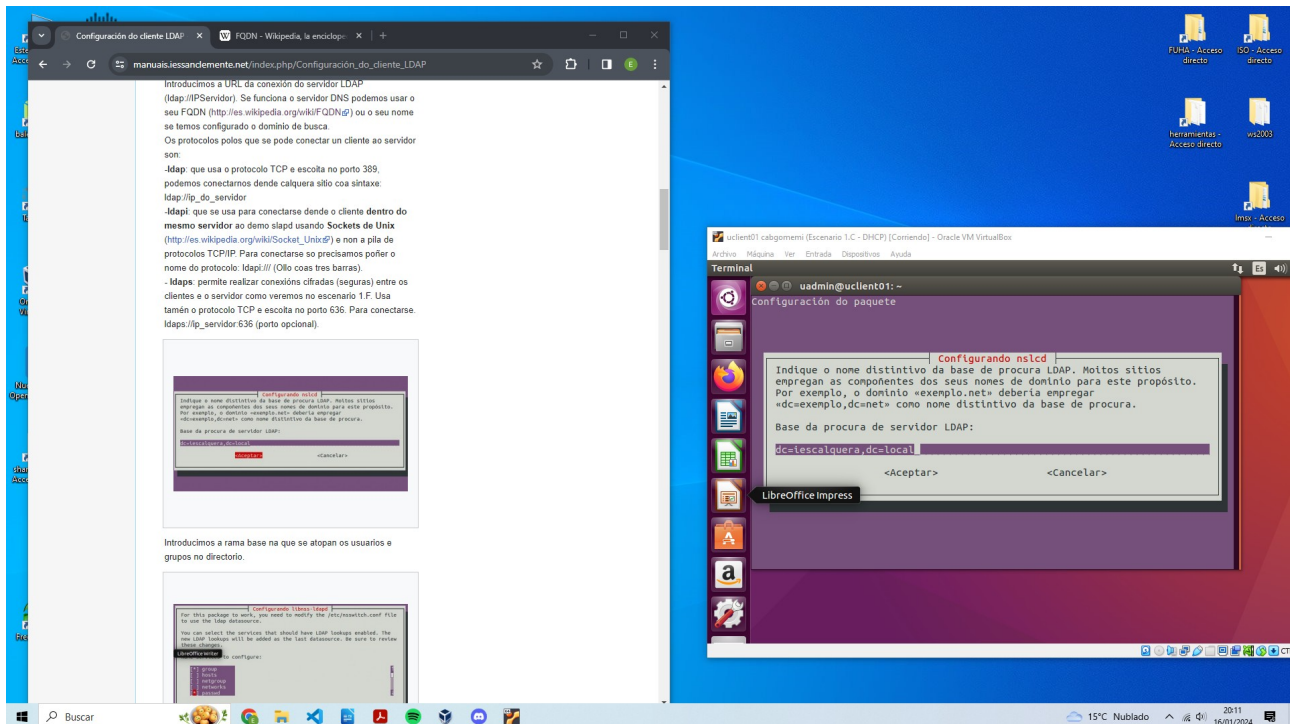
```
sudo apt-get update -y && sudo apt install libpam-ldapd -y
```

Introducimos la IP del dserver00.

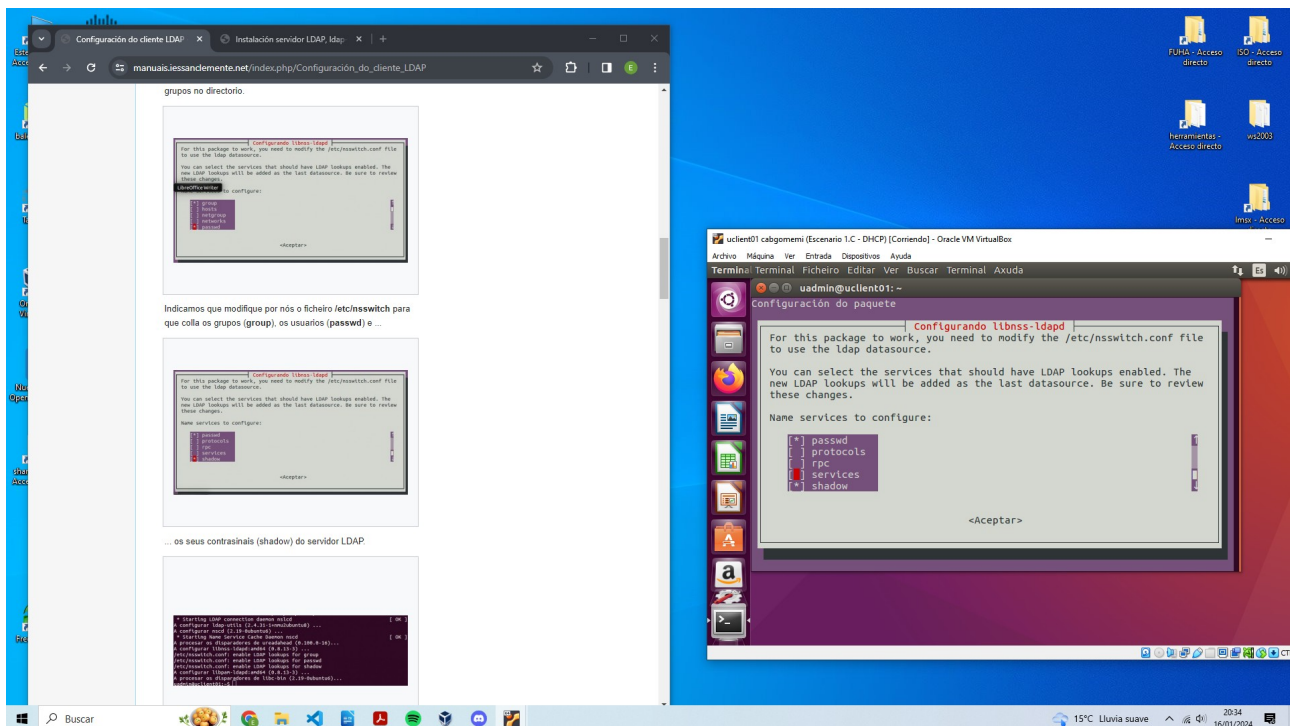


Introducimos la rama base creada anteriormente.

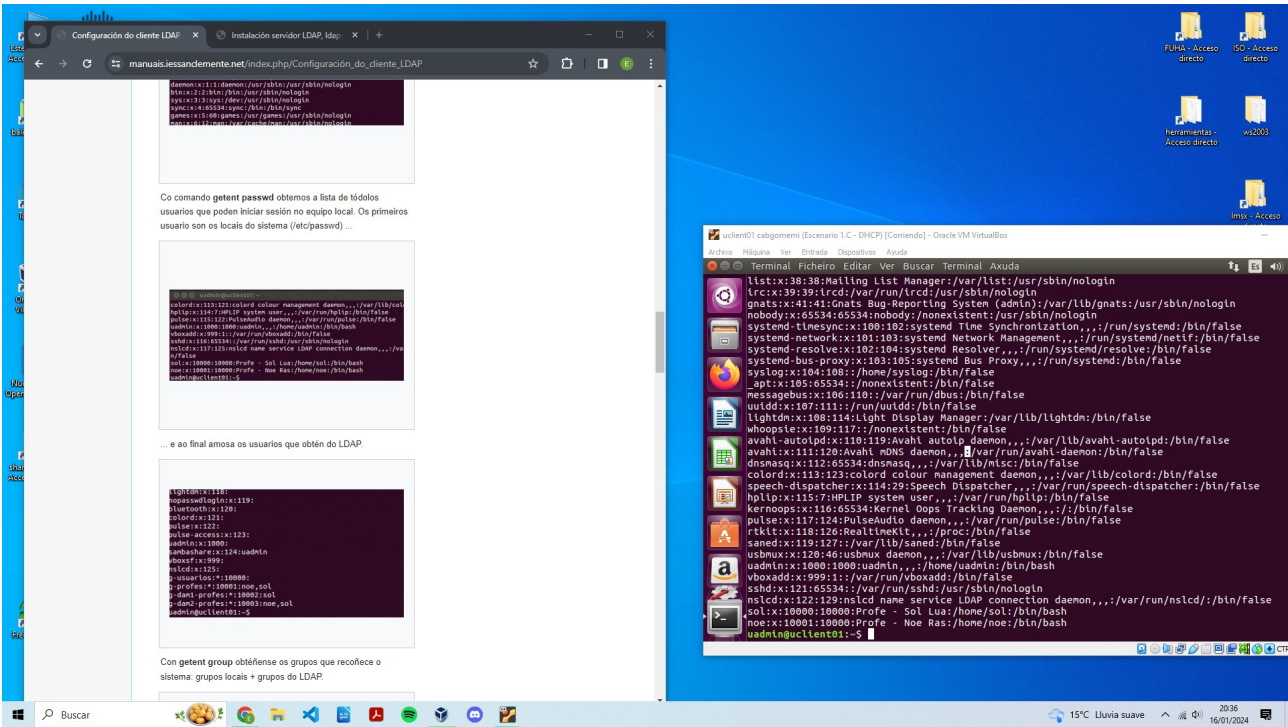
51 Platega I_II_III



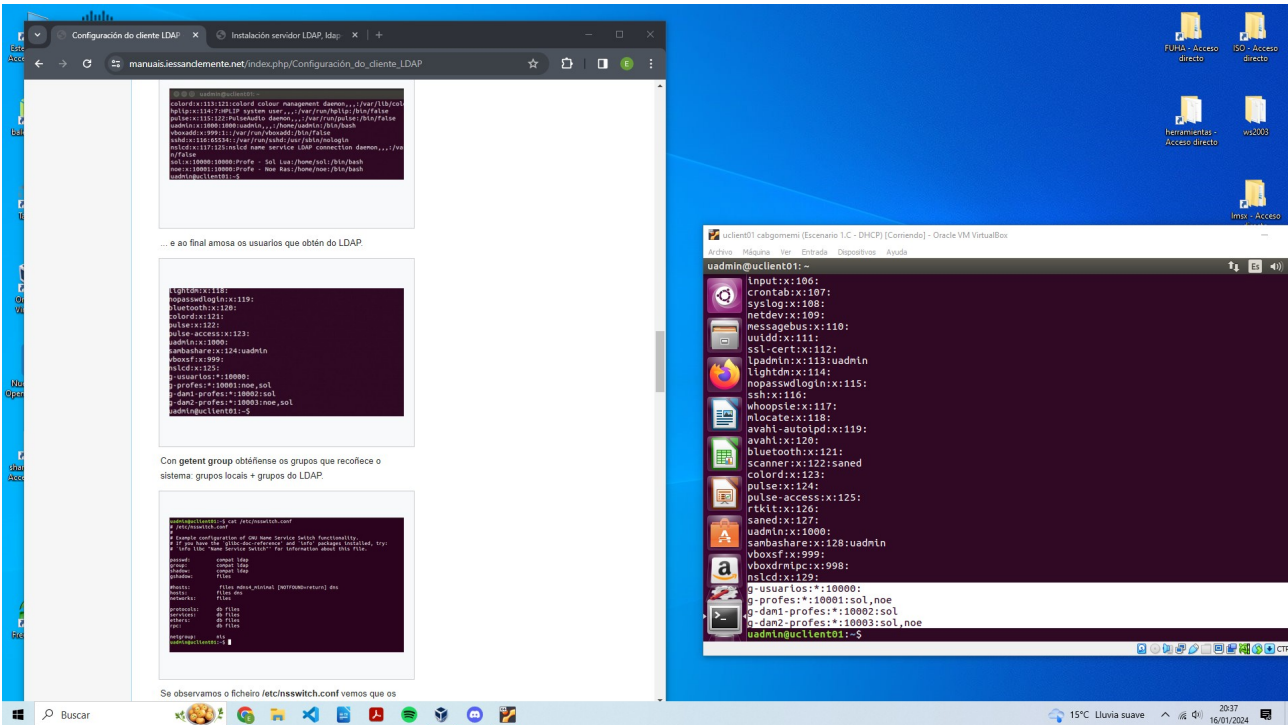
Seleccionamos passwd, group y shadow.



Mediante el comando **getent passwd** podemos ver al final los usuarios que pueden conectarse al sistema.

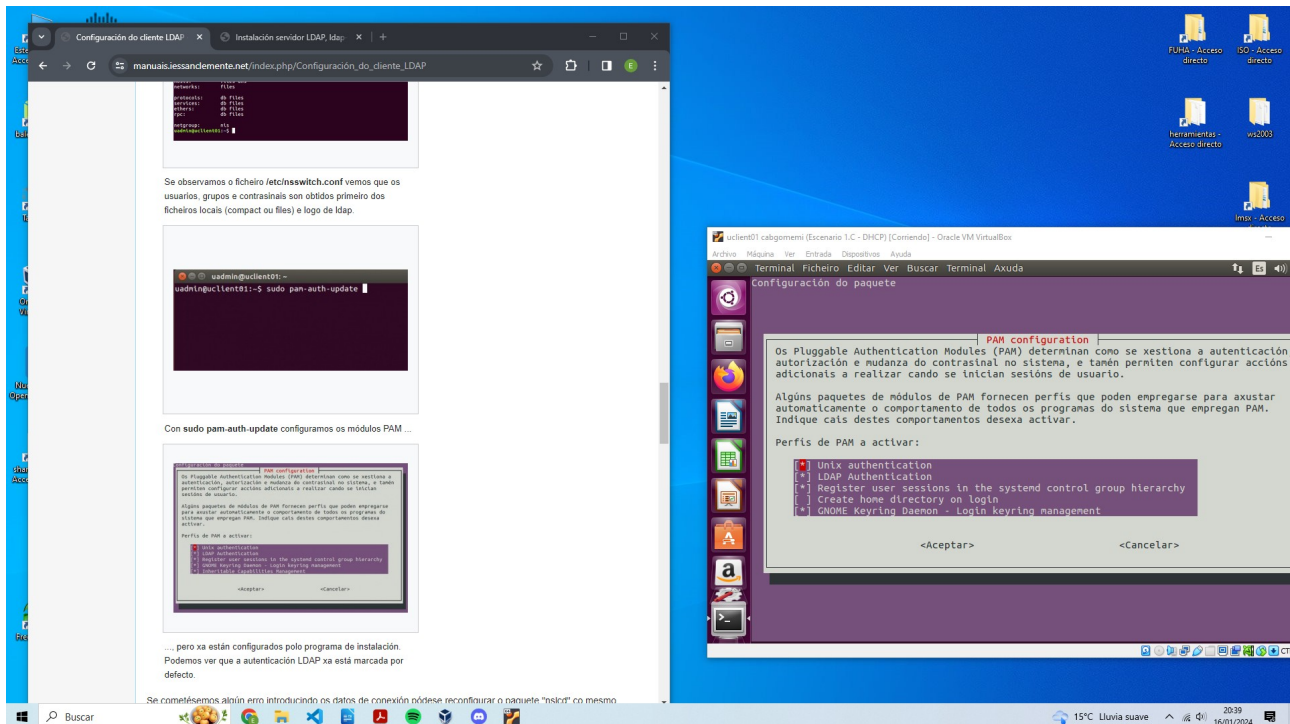
51 *Platega I_II_III*

Mediante el comando **getent group** podemos ver al final los grupos y sus miembros.



Mediante el comando `sudo pam-auth-update`

Configuramos los módulos PAM, donde podemos ver las configuraciones en materia de contraseñas.



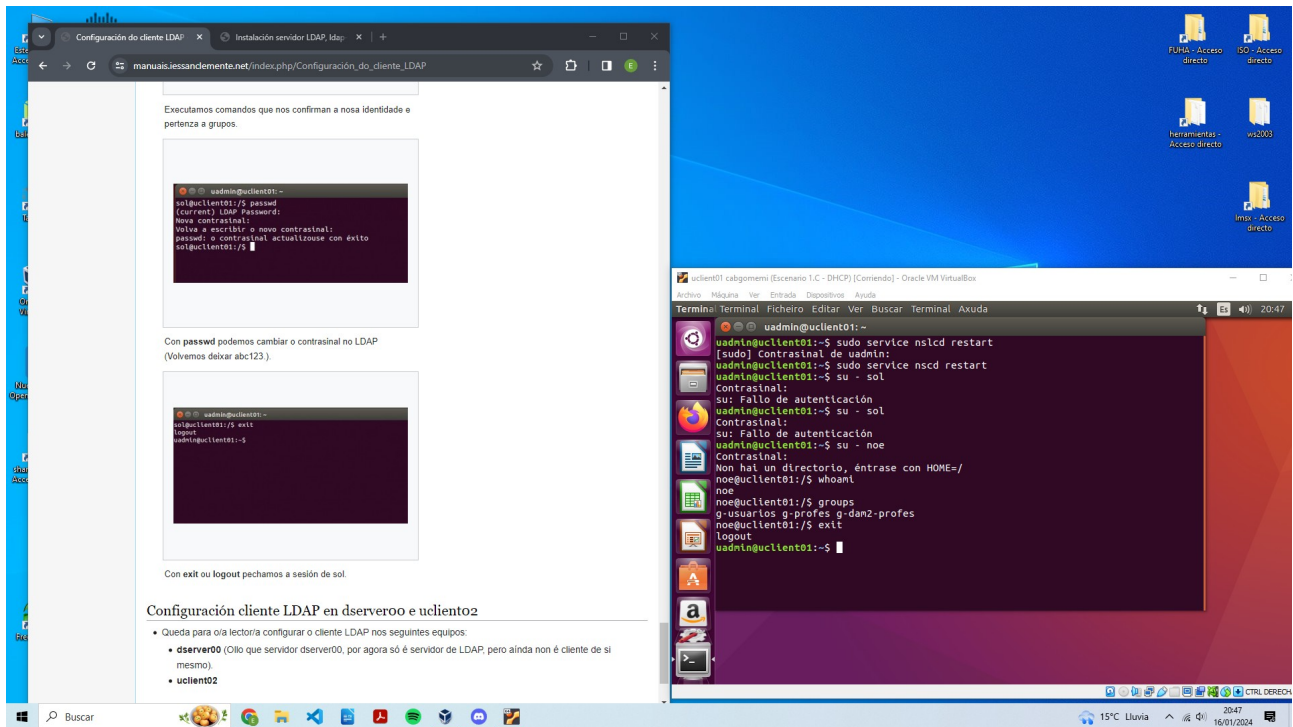
Reiniciamos el equipo para poder comprobar que lo cambios se han aplicado correctamente.

sudo service nslcd restart

sudo service nscd restart

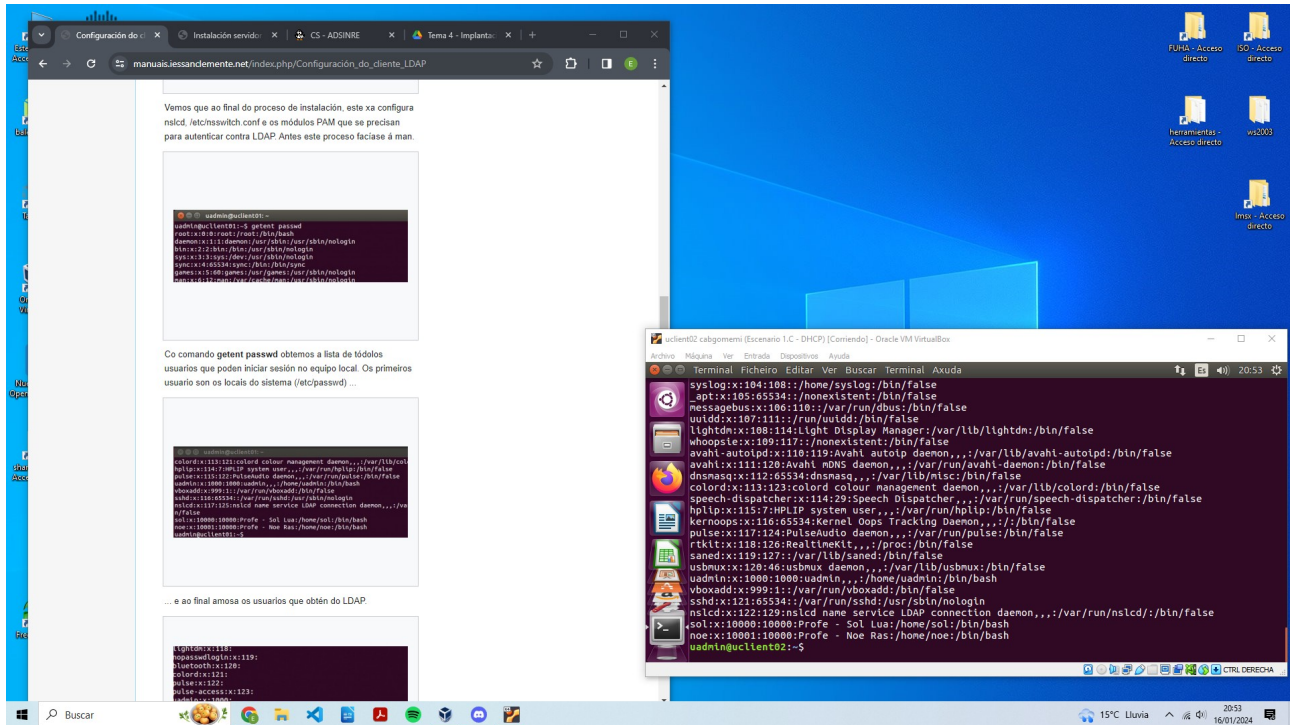
Ejecutamos el comando. `su - noe` para iniciar cómo noe.

Ejecutamos los siguientes comandos para comprobar el funcionamiento.

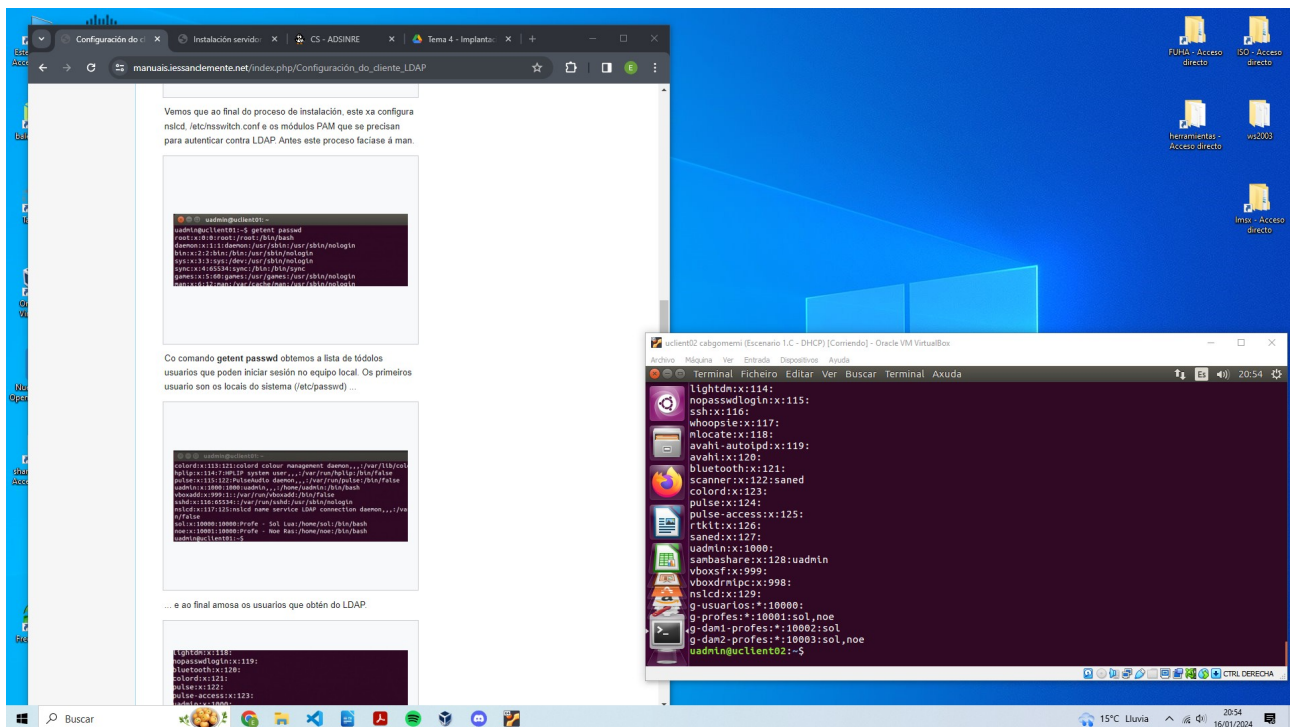


Configuración cliente LDAP en `dserver00` e `ucient02`

Configuración de cliente LDAP en uclient02

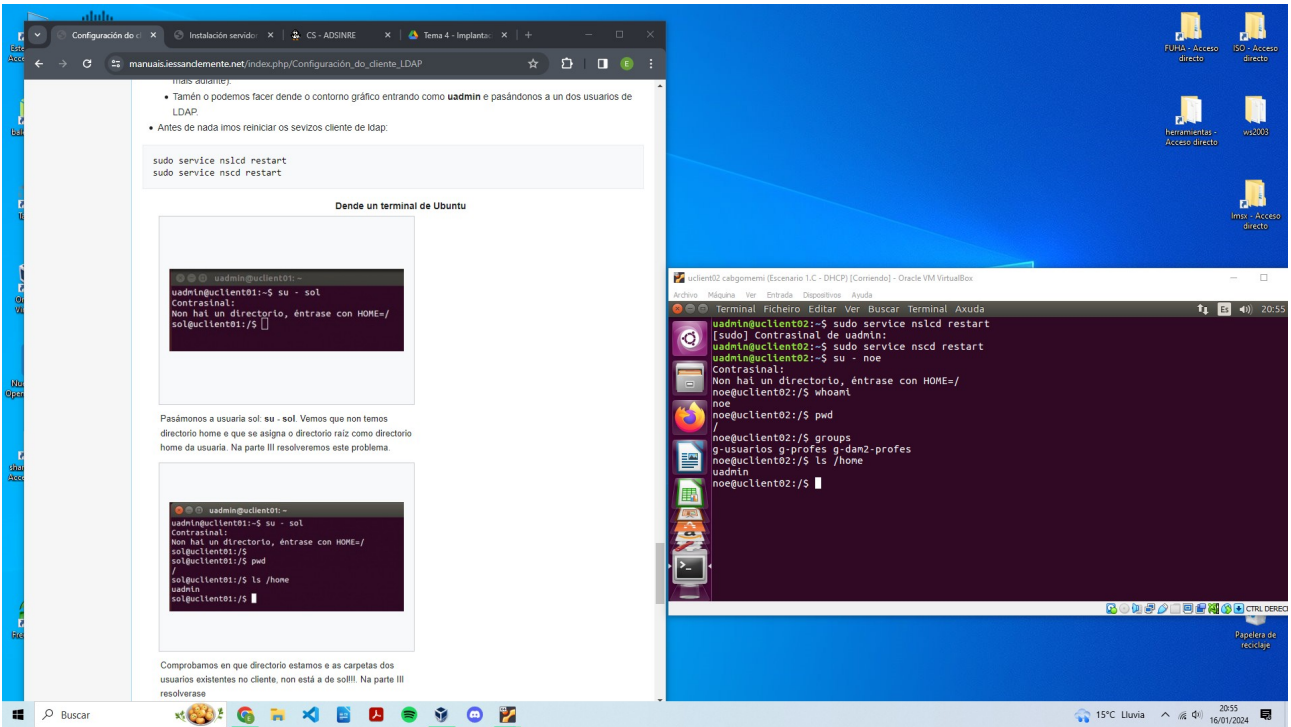


Comprobación



Comprobación

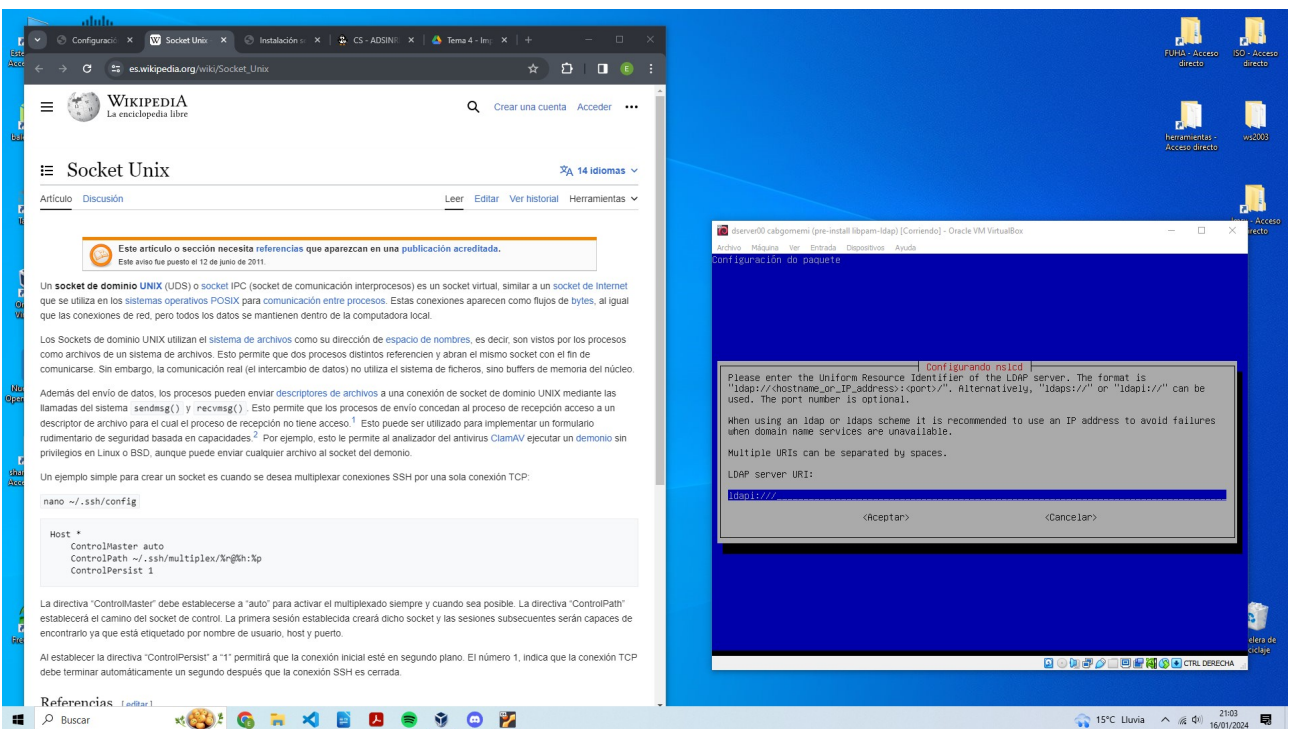
51 Platega I_II_III



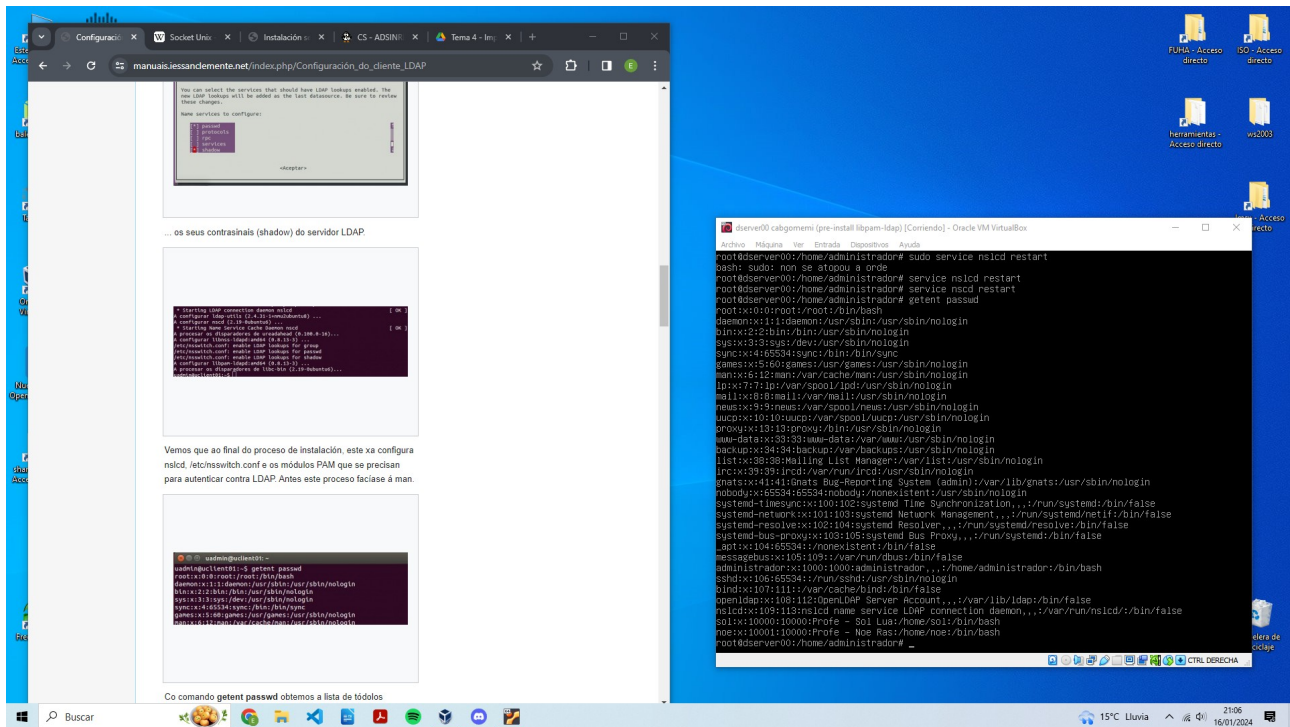
Comprobación

Configuración de cliente LDAP en dserver00

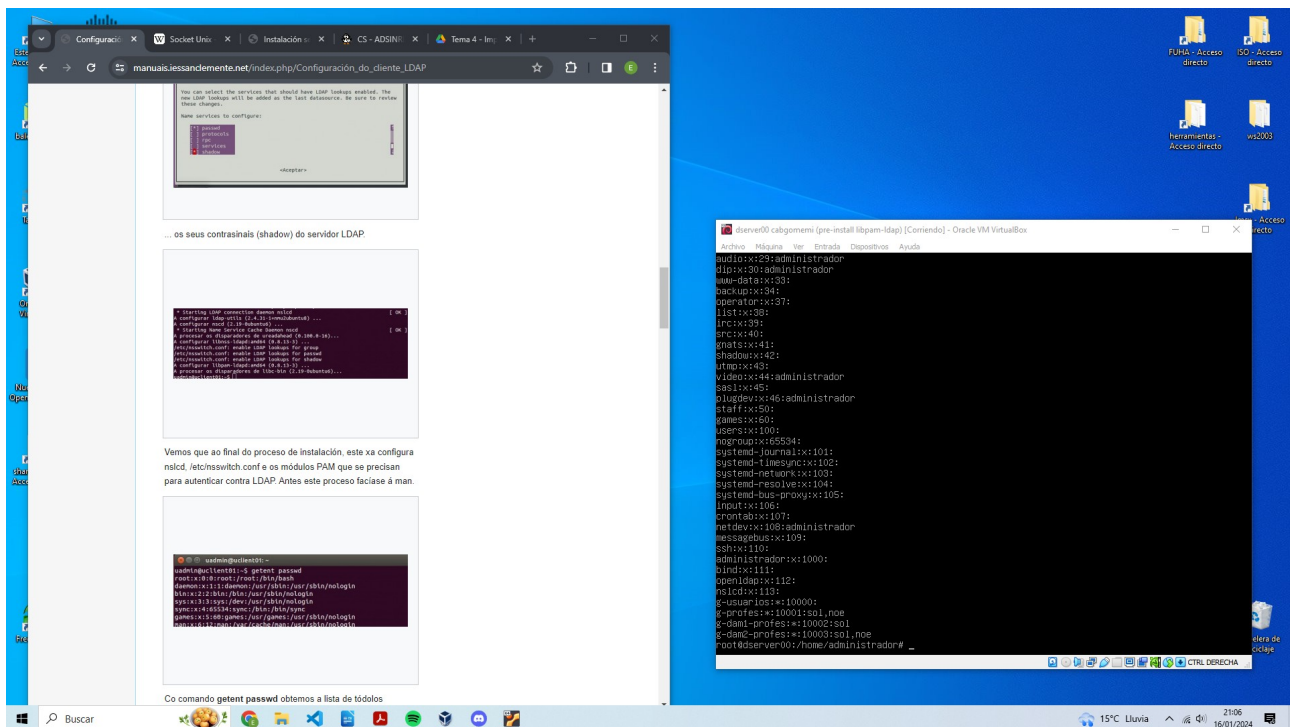
Dejamos esto en blanco, dado que no sabemos el puerto que debemos configurar.



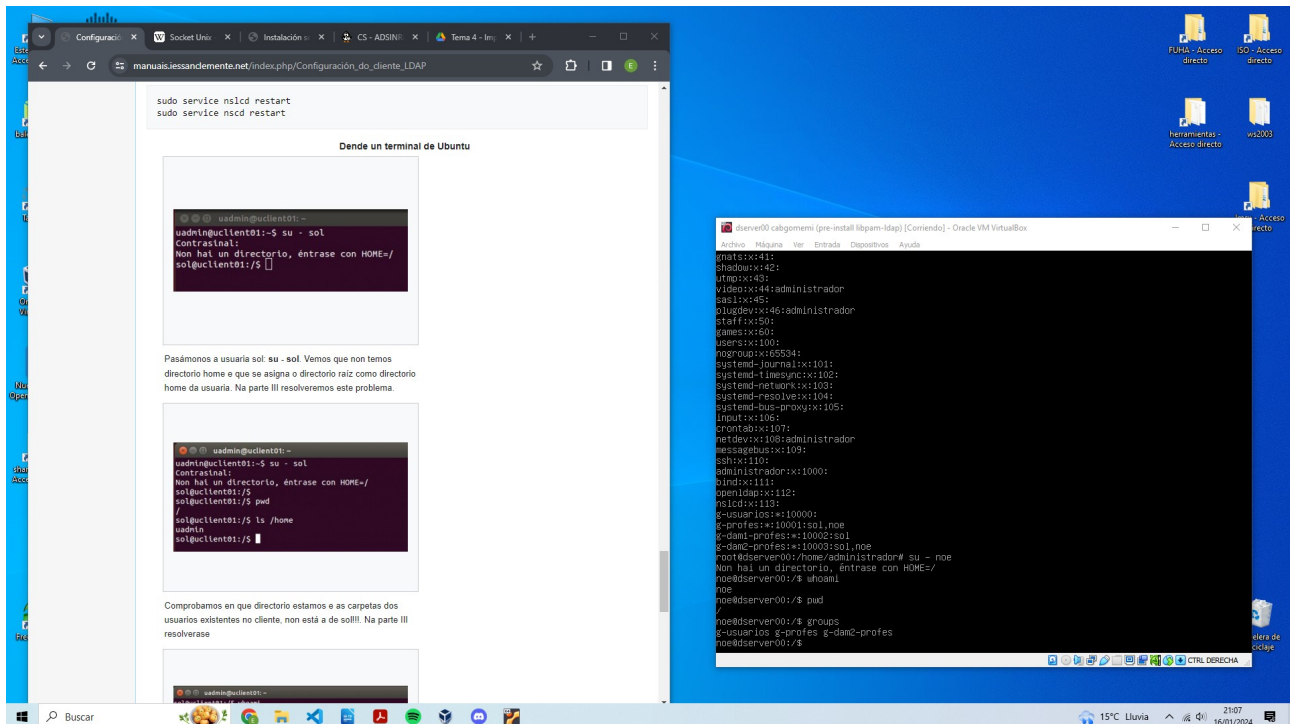
51 Platega I_II_III



Comprobación



Comprobación



Comprobación

Herramientas para administración de LDAP: Idapscripts, LDAP Account Manager (LAM) y Jxplorer

Administración mediante scripts

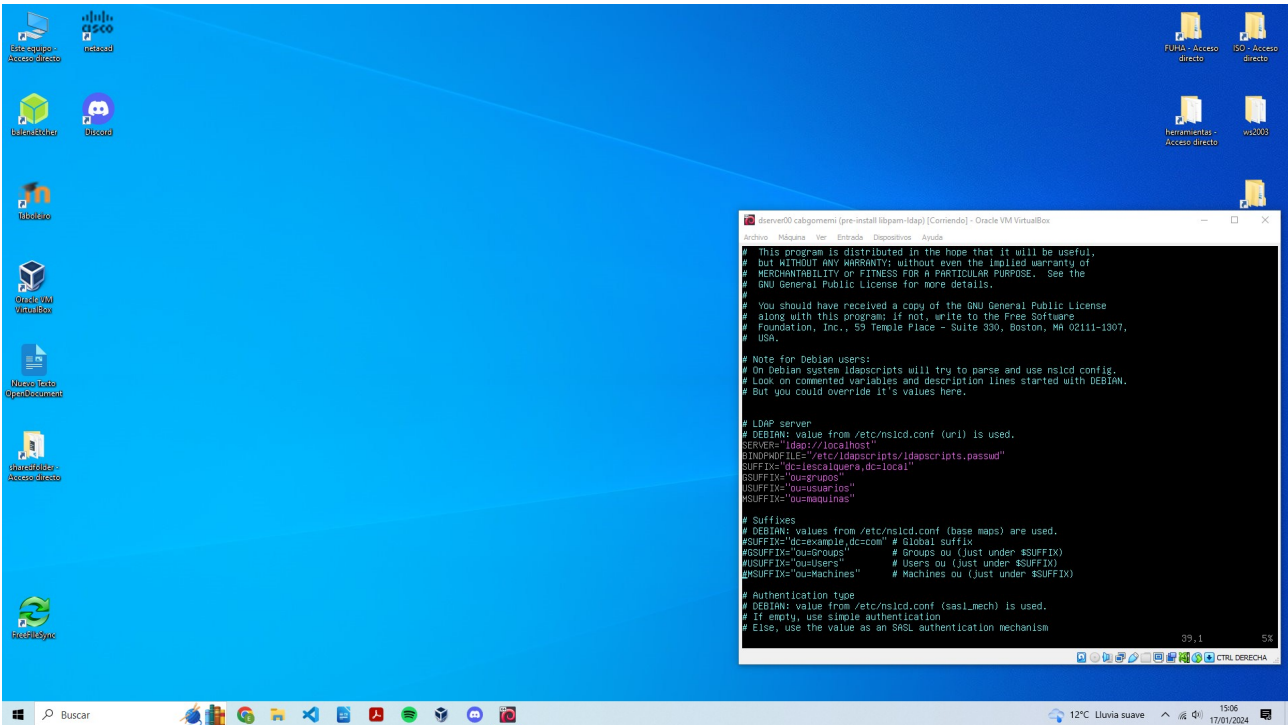
Instalamos el paquete en la máquina **dserver00**

```
apt-get install ldapscrip
```

Editamos el siguiente archivo para que incluya los siguientes ajustes.

/etc/ldapscrip

```
SERVER="ldap://localhost"
BINDPWDFILE="/etc/ldapscrip/ldapscrip.passwd"
SUFFIX="dc=iescalquera,dc=local"
GSUFFIX="ou=grupos"
USUFFIX="ou=usuarios"
MSUFFIX="ou=maquinas"
...
BINDDDN="cn=admin,dc=iescalquera,dc=local"
BINDPWDFILE="/etc/ldapscrip/ldapscrip.passwd"
...
CREATEHOMES="yes"
```

Ahora crearemos el fichero especificado en la línea **BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"** dónde almacenaremos la contraseña, mediante el comando.

```
sh -c "echo -n 'abc123.' > /etc/ldapscripts/ldapscripts.passwd"
```

```
chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

manuais.essandemente.net/index.php/Ferramentas_para_administracão_do_LDAP/ldapscrip...

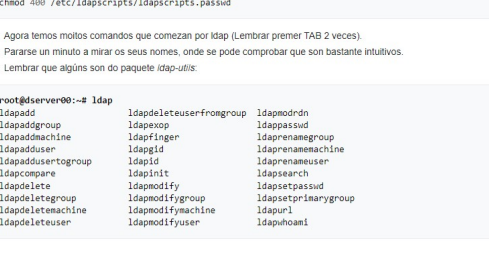
```
chmod 400 /etc/ldapscrip/ldapscrip.passwd
```

- Agora temos muitos comandos que começam por ldap (Lembrar premer TAB 2 vezes).
- Parase um minuto a mirar os seus nomes, onde se pode comprobar que son bastante intuitivos.
- Lembrar que alguns son do paquete ldap-utils:

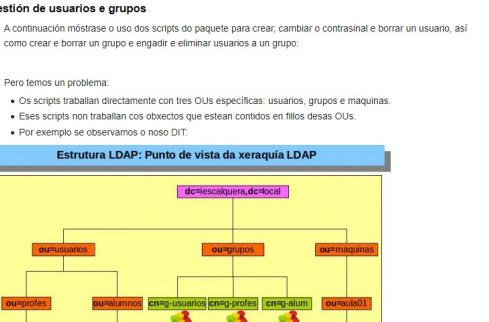
```
root@server00:~# ldap
ldapadd      ldapdeleteuserfromgroup  ldapmodrdn
ldapaddgroup ldapexop                    ldapasswd
ldapaddmachine ldapfinger                ldaprenamegroup
ldapadduser    ldapgid                    ldaprenamemachine
ldapaddusertogroup ldapid                    ldaprenameuser
ldapcompare    ldapinit                    ldapsearch
ldapdelete     ldapmodify                ldapsetpasswd
ldapdeletemachine ldapmodifygroup            ldapsetprimarygroup
ldapdeleteuser  ldapmodifyuser          ldaphuami
```

Gestión de usuarios e grupos

- A continuación móstrase o uso dos scripts do paquete para crear, cambiar o contrasinal e borrar un usuario, así como crear e borrar un grupo e engadir e eliminar usuarios a un grupo:
- Pero temos un problema:
 - Os scripts traballan directamente con tres OUs específicas: usuarios, grupos e máquinas.
 - Esos scripts non traballan con obxectos que estean contidos en fillos das OUs.
 - Por exemplo se observamos o noso DIT:



Estrutura LDAP: Punto de vista da xeraquia LDAP



```
root@server00:~# ldap
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
# USA.
#
# Note for Debian users:
# On Debian system ldapscrip will try to parse and use nsicd config.
# Look on commented variables and description lines started with DEBIAN.
# But you could override it's values here.
#
# LDAP server
# DEBIAN: value from /etc/nsicd.conf (url) is used.
SERVER="ldap://localhost"
BINDINGURL="/etc/ldapscrip/ldapscrip.passwd"
$SUFFIX="dc=example,dc=local"
$SUFFIX="ou=groups"
$SUFFIX="ou=users"
$SUFFIX="ou=machines"
# Suffixes
# DEBIAN: values from /etc/nsicd.conf (base maps) are used.
$SUFFIX="dc=example,dc=com" # Global suffix
$SUFFIX="ou=groups" # Groups ou (just under $SUFFIX)
$SUFFIX="ou=users" # Users ou (just under $SUFFIX)
$SUFFIX="ou=machines" # Machines ou (just under $SUFFIX)
# Authentication type
# DEBIAN: value from /etc/nsicd.conf (sasl_mech) is used.
# If empty, use simple authentication
# Else, use the value as an sasl authentication mechanism
root@server00:/home/administrador# sh -c "echo -n 'abc123.' > /etc/ldapscrip/ldapscrip.passwd"
root@server00:/home/administrador# chmod 400 /etc/ldapscrip/ldapscrip.passwd
root@server00:/home/administrador#
```

Gestión de usuarios y grupos.

Añadimos el grupo alumnos mediante el comando.

ldapaddgroup g-alum

The screenshot shows a web browser window on the left displaying a page titled "Estrutura LDAP: Punto de vista da xeraquia LDAP". The page contains a hierarchical diagram of an LDAP structure. The root is "dc=escala,dc=local", which branches into "ou=usuarios", "ou=grupos", and "ou=máquinas". Under "ou=usuarios", there are "ou=profes" and "ou=alumnos". "ou=profes" contains "cn=prof1", "cn=prof2", and "cn=prof3". "ou=alumnos" contains "cn=al1", "cn=al2", and "cn=al3". Under "ou=grupos", there is "cn=profes" and "cn=alumnos". Under "ou=máquinas", there is "cn=profes" and "cn=alumnos".

Below the diagram, there is a list of bullet points in Galician:

- Pero temos un problema:
- Os scripts traballan directamente con tres OUs específicas: usuarios, grupos e máquinas.
- Eses scripts non traballan cos obxectos que estean contidos en fillos desas OUs.
- Por exemplo se observamos o noso DIT:

The diagram shows the following structure:

```

graph TD
    Root["dc=escala,dc=local"] --> OUUsuarios["ou=usuarios"]
    Root --> OUGrupos["ou=grupos"]
    Root --> OUMaquinas["ou=máquinas"]
    OUUsuarios --> OUProfes["ou=profes"]
    OUUsuarios --> OUAlumnos["ou=alumnos"]
    OUGrupos --> CNProfes["cn=profes"]
    OUGrupos --> CNAlumnos["cn=alumnos"]
    OUMaquinas --> CNProfes
    OUMaquinas --> CNAlumnos
    OUProfes --> CNProf1["cn=prof1"]
    OUProfes --> CNProf2["cn=prof2"]
    OUProfes --> CNProf3["cn=prof3"]
    OUAlumnos --> CNAl1["cn=al1"]
    OUAlumnos --> CNAl2["cn=al2"]
    OUAlumnos --> CNAl3["cn=al3"]
  
```

Below the diagram, there is a list of bullet points in Galician:

- Vemos que non podemos dar usuarios de alta nas OUs profes, dam1 e dam2, só os podemos dar de alta con estes scripts na OU usuarios.
- Estes scripts vellen ben cando se trata de organizacións pequenas que non teñen clasificados os usuarios e todos están xuntos na OU usuarios.
- O mesmo pasa coas máquinas.
- En cambio cos grupos, neste caso, si que podemos dar de alta. Neste caso o grupo **g-alum**. Non confundir coa OU alumnos.

Below the list, there is a terminal window showing the execution of the **ldapaddgroup g-alum** command. The output is:

```

ldapaddgroup g-alum
Successfully added group g-alum to LDAP

A continuación ponse a modo de exemplo unha ficticia xestión de usuarios, que vai traballar coa OU usuarios
(supondo que previamente creamos no LDAP os grupos grupo1-ficticio e grupo2-ficticio con ldapaddgroup):

ldapadduser pepe grupo1.ficticio
Successfully added user pepe to LDAP
Successfully set password for user pepe
Successfully created home directory for user pepe
  
```

The terminal window also shows the output of the **ldapaddgroup g-alum** command, which is:

```

# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
# USA.

# Note for Debian users:
# On Debian system ldapscripts will try to parse and use nsldap config.
# Look on commented variables and description lines started with DEBIAN.
# But you could override it's values here.

# LDAP server
# DEBIAN: value from /etc/nsldap.conf (uri) is used.
SERVER="ldap://localhost"
BINDINGFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX="dc=escala,dc=local"
GSUFFIX="ou=grupos"
USUFFIX="ou=usuarios"
MSUFFIX="ou=máquinas"

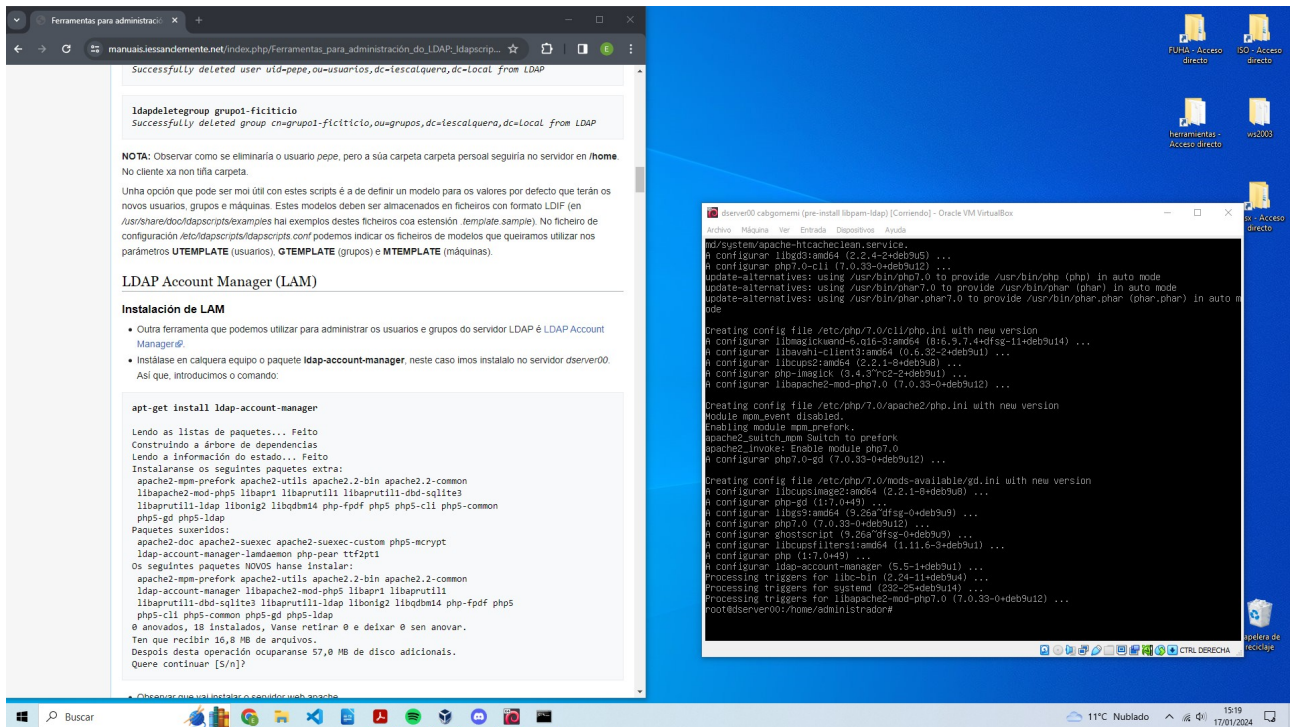
# Suffixes
# DEBIAN: values from /etc/nsldap.conf (base maps) are used.
MSUFFIX="dc=example,dc=com" # Global suffix
USUFFIX="ou=groups" # Groups ou (Just under $SUFFIX)
MSUFFIX="ou=users" # Users ou (Just under $SUFFIX)
MSUFFIX="ou=Machines" # Machines ou (Just under $SUFFIX)

# Authentication type
# DEBIAN: value from /etc/nsldap.conf (sasl_mech) is used.
# If empty, use simple authentication.
# Else, use the value as an SASL authentication mechanism
root@server00:/home/administrador# sh -c "echo -n 'abc123:' > /etc/ldapscripts/ldapscripts.passwd"
root@server00:/home/administrador# chmod 400 /etc/ldapscripts/ldapscripts.passwd
root@server00:/home/administrador# ldapaddgroup g-alum
Successfully added group g-alum to LDAP
root@server00:/home/administrador#
  
```

LDAP Account Manager (LAM)

Instalamos el LAM

apt-get install ldap-account-manager



Comprobamos que están instaladas el servidor apache.

Reiniciamos el servicio apache.

service apache2 restart

Configuración de LAM

Iniciamos la máquina **uclient01**

Introducimos en la barra del navegador la siguiente dirección:

<http://dserver00.iescalquera.local/lam>

En caso de no tener correctamente configurado el dns (platega I) poner la IP.

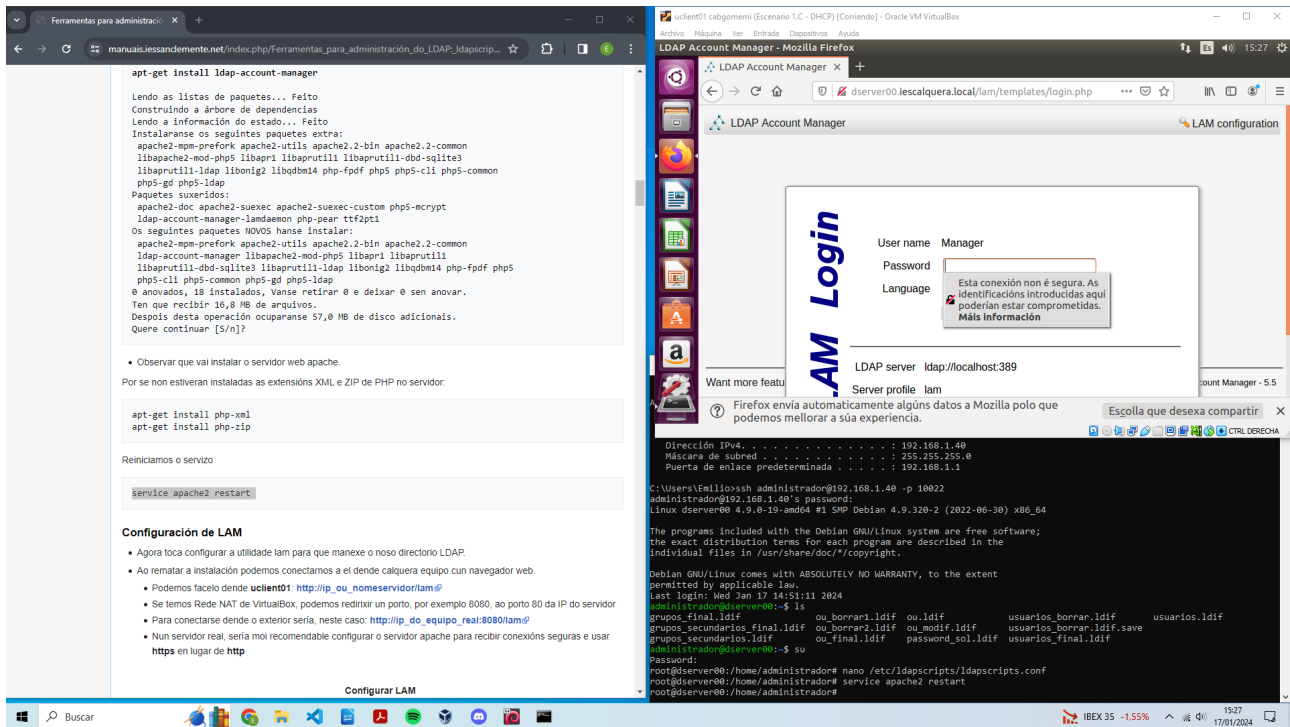
Si al intentar administrar el LDAP mediante LAM nos da error PHP y ZIP.

apt-get install php-xml

apt-get install php-zip

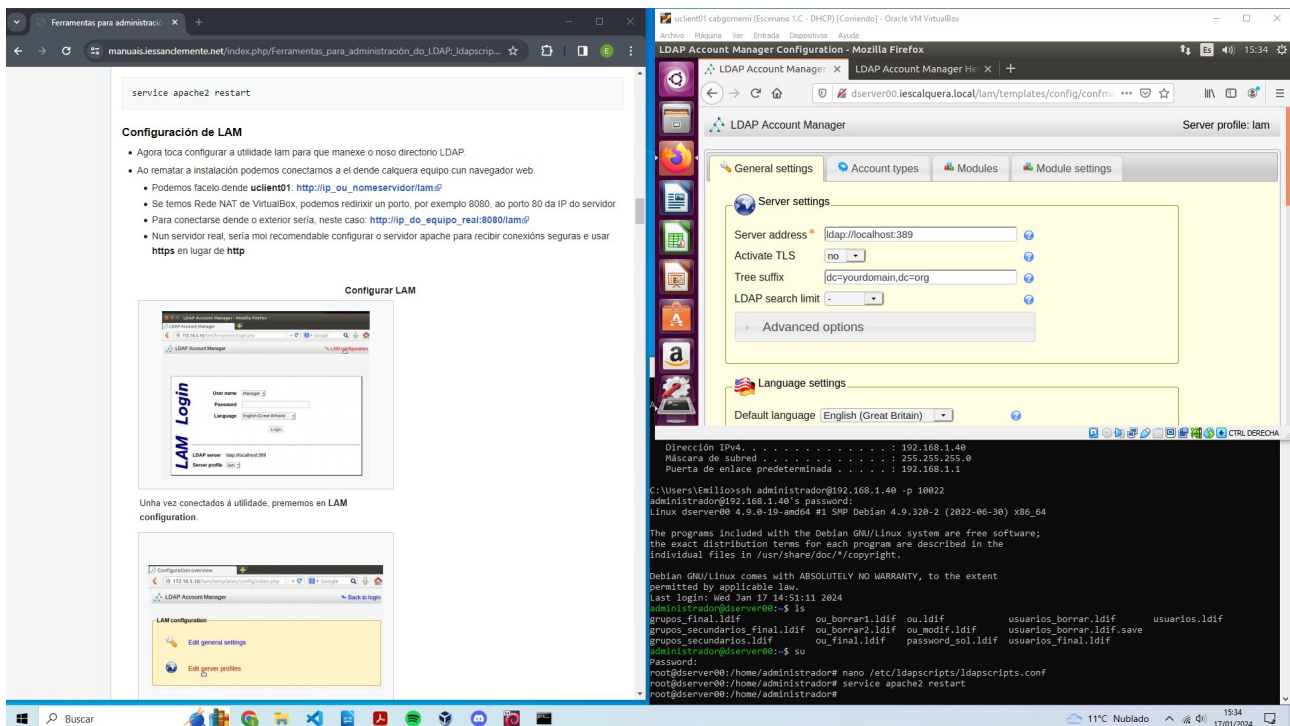
service apache2 restart

51 Platega I_II_III

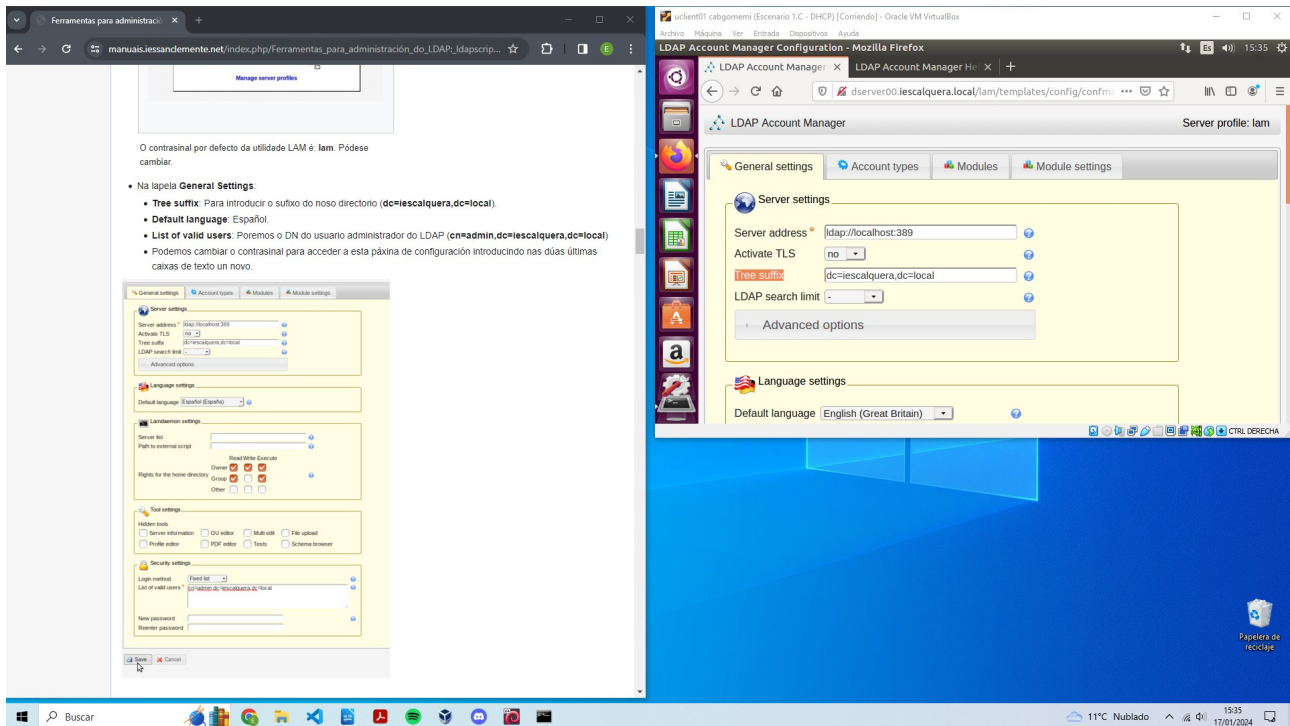


Iremos a lam configurations > Server settings.

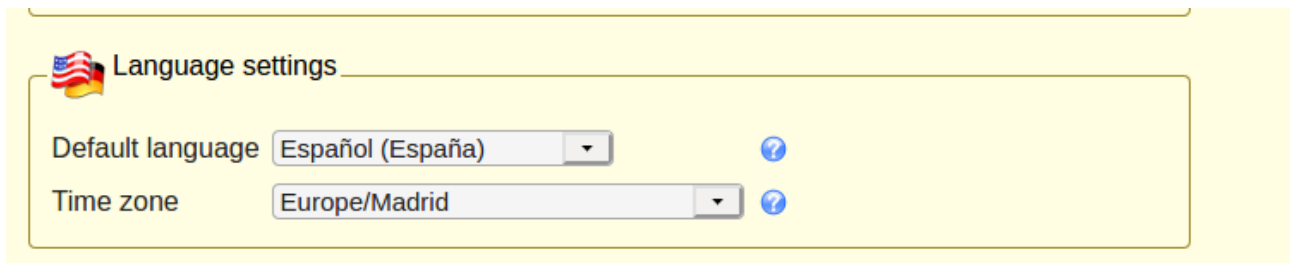
Si es la primera vez que iniciamos sesión entraremos como contraseña lam.



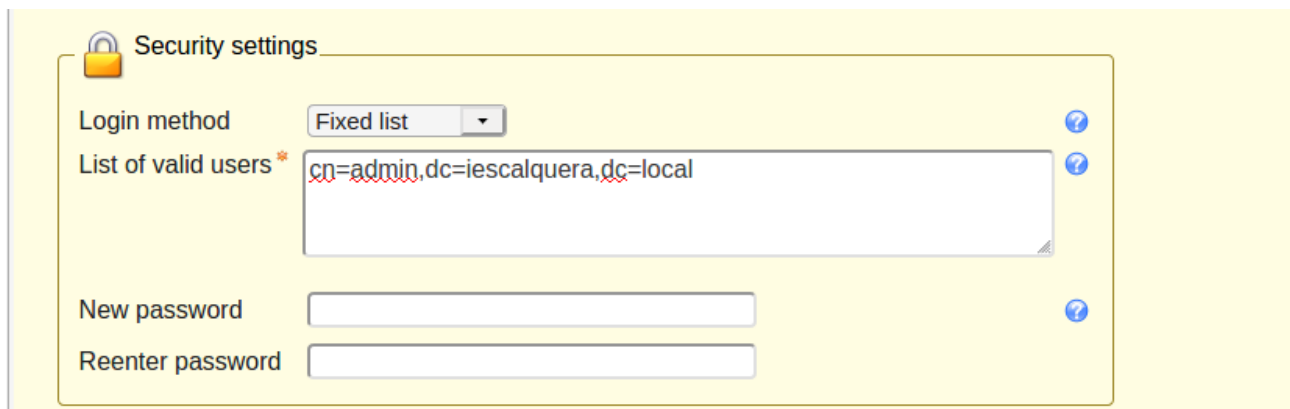
Introducimos el siguiente contenido en el apartado “tree-suffix”.



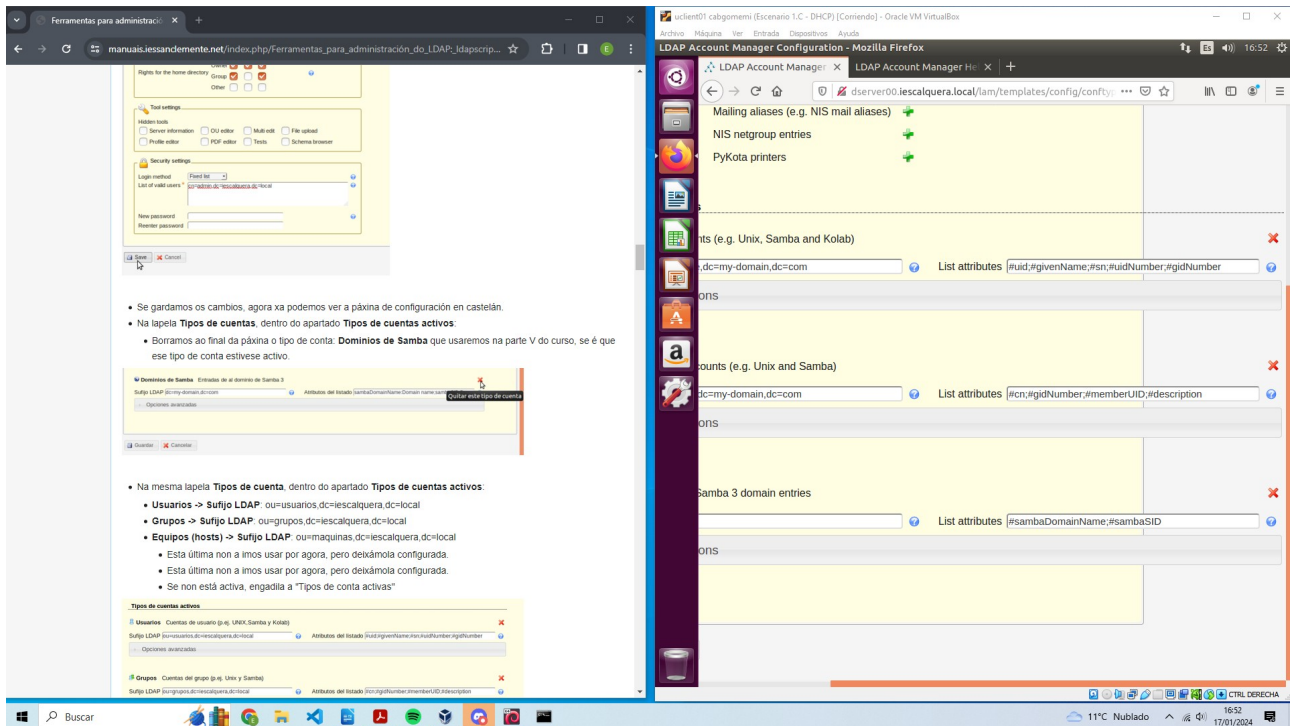
Configuramos la zona horaria.



Configuramos los usuarios válidos.



Eliminamos el dominio de samba3 haciendo click en la x al final del menú.



Configuramos en la misma pestaña la lista de equipos activos de la siguiente manera.

Active account types

Users User accounts (e.g. Unix, Samba and Kolab)

DAP suffix List attributes

Advanced options

Groups Group accounts (e.g. Unix and Samba)

DAP suffix List attributes

Advanced options

Hosts Host accounts (e.g. Samba)

DAP suffix List attributes

Advanced options

Save

Haremos click en guardar.

En la pestaña de modules deberá quedar configurado de la siguiente manera.

51 Platega I_II_III

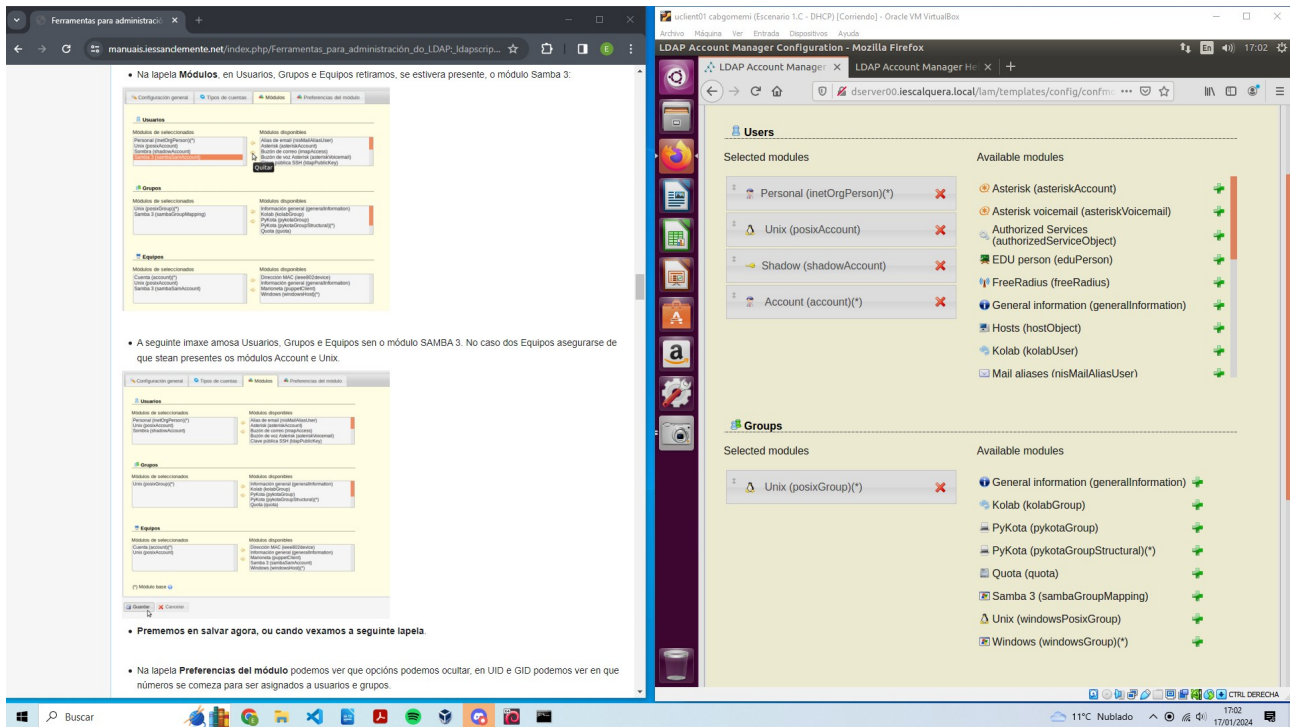
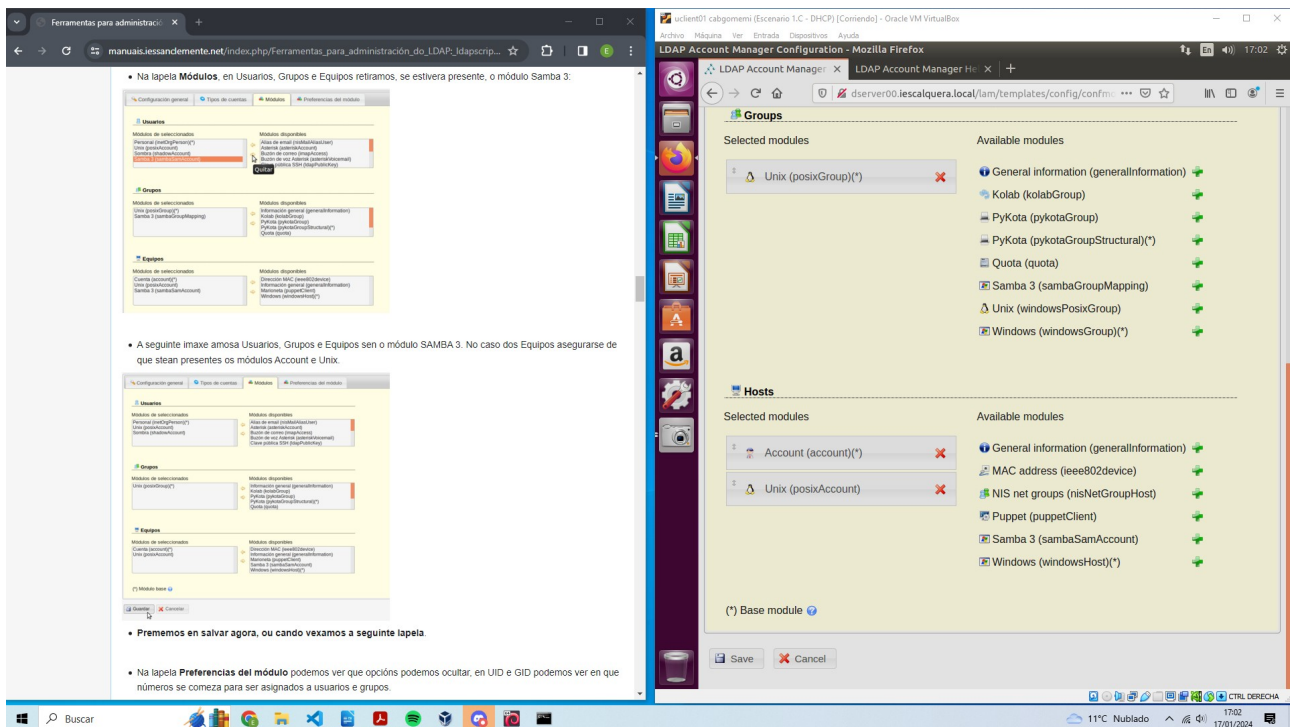


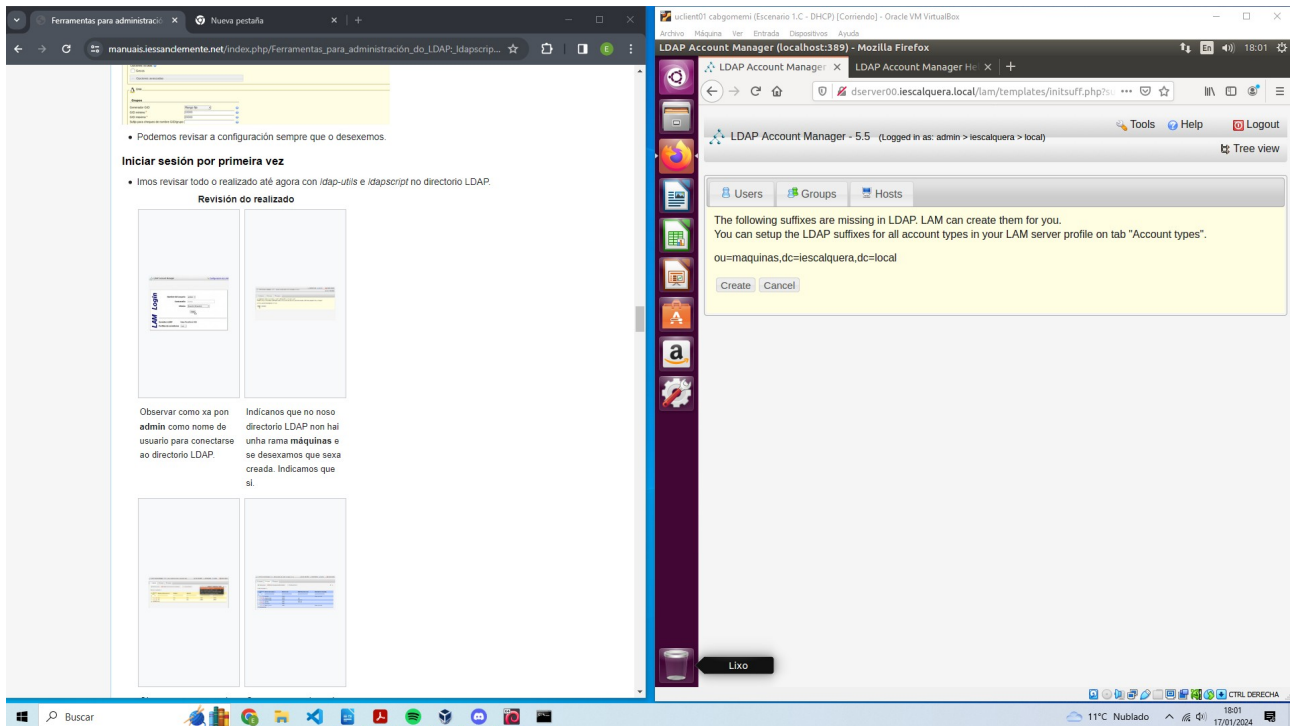
Foto 1



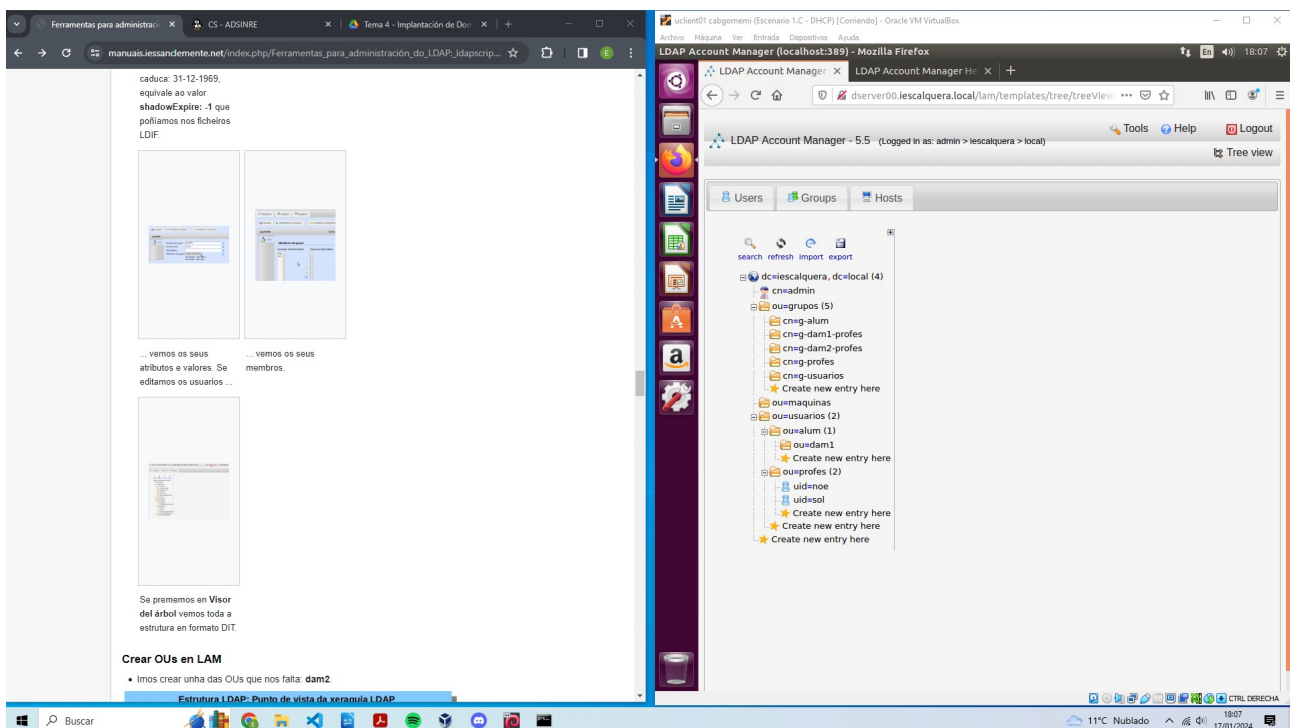
Haremos click en guardar.

Iniciar sesión por primera vez

Hacemos click en create



Podemos ver el visor de árbol



Creamos una nueva entrada en alumno.

The screenshot shows two windows. The left window is a web browser displaying the 'Manuais' website. It shows a file upload interface for 'Archivo:DI 2014 lam 20.jpeg'. The right window is the LDAP Account Manager interface, showing a tree view of the directory structure. A 'Create new entry here' button is highlighted in the tree view.

Indicamos que es una entrada genérica.

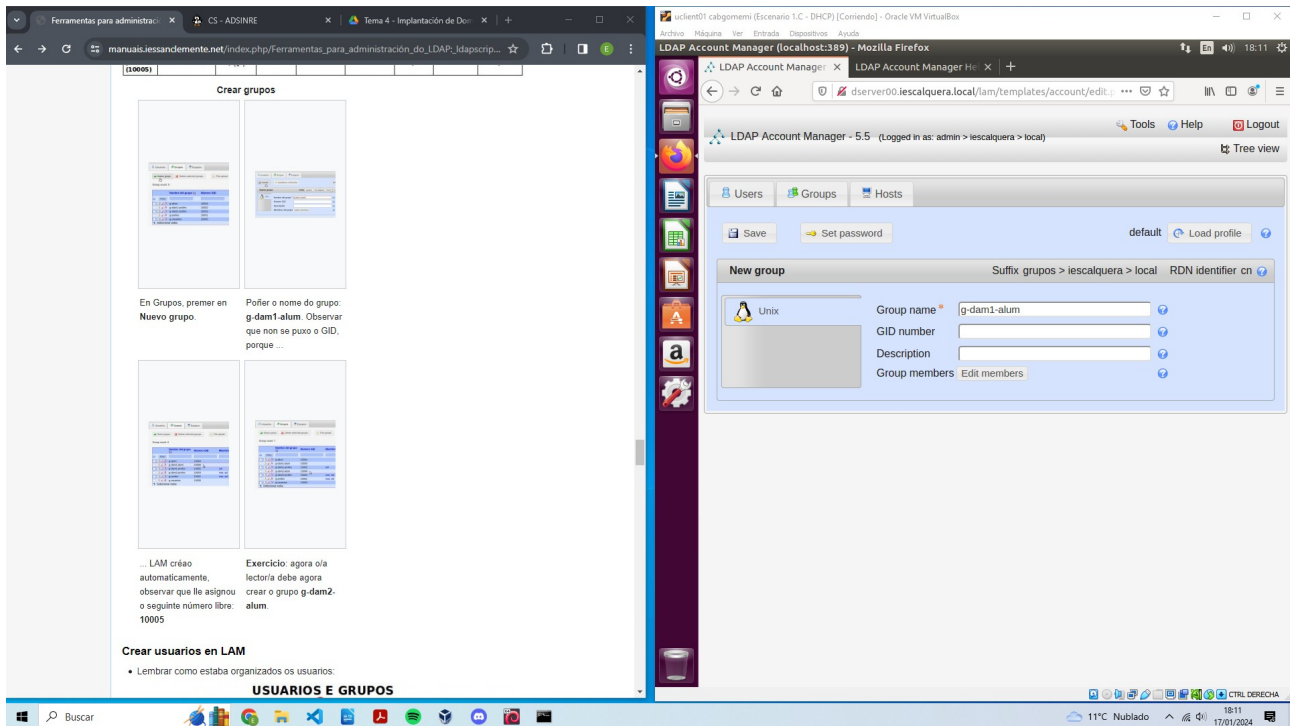
Indicamos que el nombre es dam².

The screenshot shows the LDAP Account Manager 'Create object' form. The form is titled 'New Organisational Unit (Step 1 of 1)'. It shows the 'Organisational Unit' field with the name 'dam2' entered. The 'Create object' button is visible at the bottom of the form.

Guardamos la entrada.

Crear grupos en LAM. Ejercicio

Creamos el grupo g-dam1-alum



Hacemos lo mismo con g-dam2-alum

Crear usuarios en LAM

Después de exportar el archivo.csv lo importamos. Para que los cambios tengan efecto.

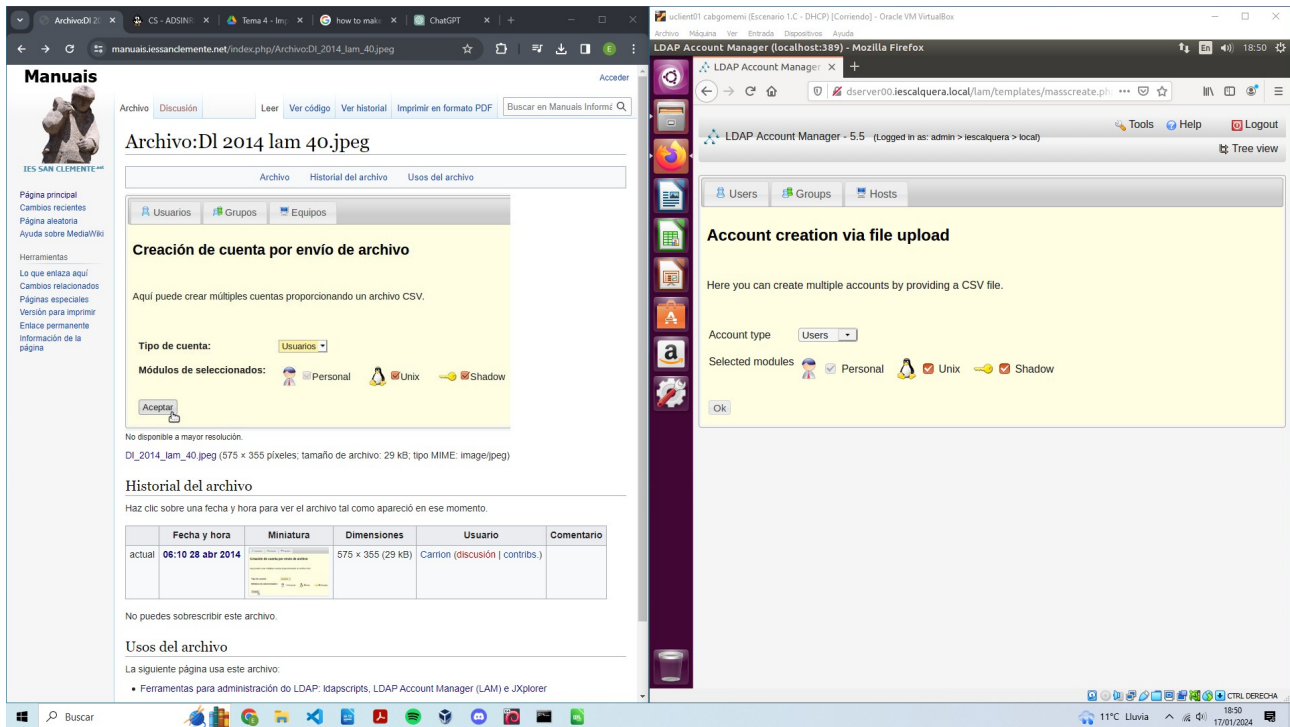
Atención: Debemos checkear el formato de los elementos incluídos, en el archivo sample.

Por ejemplo: La fecha el formato es dd-mm-yy

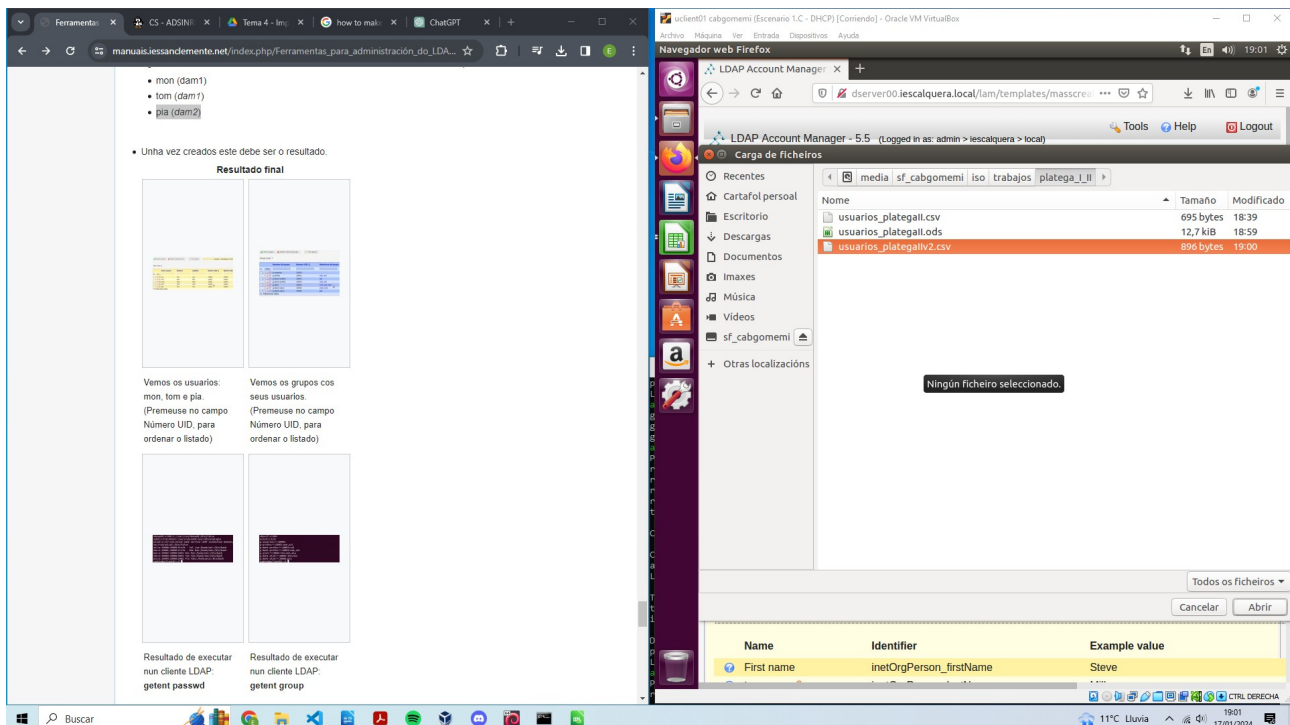
Hacemos click en file upload.

Hacemos click en aceptar.

51 Platega I_II_III

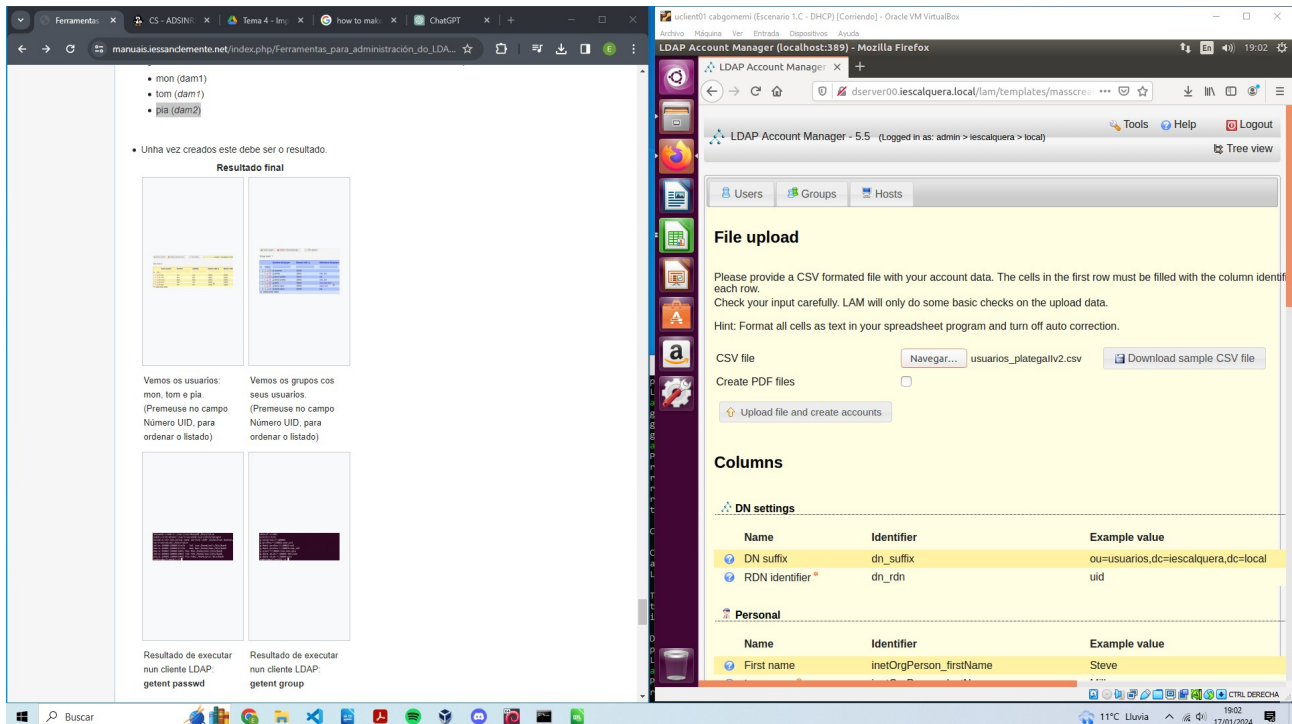


Hacemos click en navegar y seleccionamos el fichero *.csv

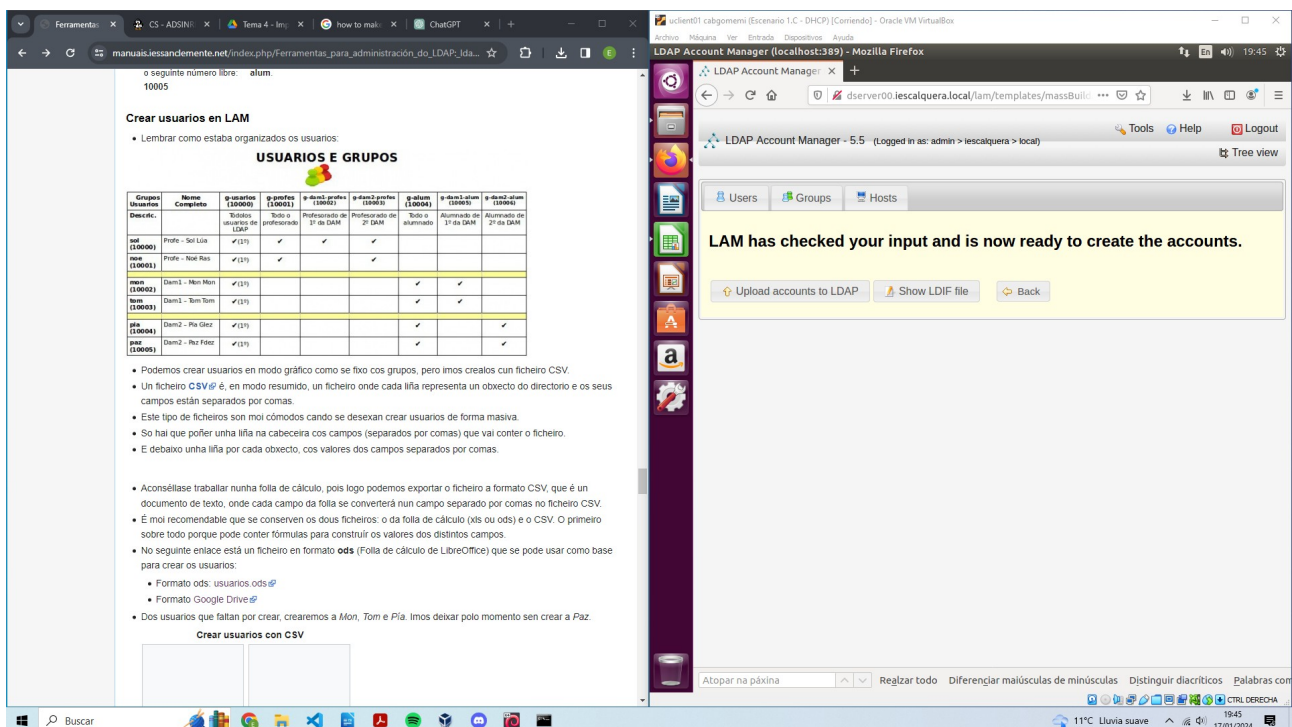


Seleccionamos upload file and create accounts.

51 Platega I_II_III



Hacemos click en upload acc to LDAP.



Realizamos las comprobaciones.

Podemos si click en las cabezeras de las tablas ordenar por id.

51 Platega I_II_III

The screenshot shows a web browser with two tabs. The left tab is 'manuais.iesandemete.net/index.php/Archivo:DI_2014_lam_60.jpeg'. The right tab is 'LDAP Account Manager (localhost:389) - Mozilla Firefox'. The 'Manuais' website shows a file upload interface for 'Archivo:DI_2014_lam_60.jpeg'. The 'LDAP Account Manager' interface shows a list of users and groups.

Nombre del grupo	Número GID	Miembros del grupo
g-usuarios	10000	
g-profes	10001	noe; sol
g-dam1-profes	10002	sol
g-dam2-profes	10003	noe; sol
g-alum	10004	mon; pia; tom
g-dam1-alum	10005	mon; tom
g-dam2-alum	10006	pia

User name	First name	Last name	UID number	GID num
sol	Sol	Lúa	10000	10000
noe	Noe	Ras	10001	10000
mon	Mon	Mon	10002	10000
tom	Tom	Tom	10003	10000
Pia	Pia	Pia	10004	10000

Realizamos las comprobaciones.

The screenshot shows a web browser with two tabs. The left tab is 'manuais.iesandemete.net/index.php/Archivo:DI_2014_lam_60.jpeg'. The right tab is 'LDAP Account Manager (localhost:389) - Mozilla Firefox'. The 'Manuais' website shows a file upload interface for 'Archivo:DI_2014_lam_60.jpeg'. The 'LDAP Account Manager' interface shows a list of groups and their members.

Nombre del grupo	Número GID	Miembros del grupo
g-usuarios	10000	
g-profes	10001	noe; sol
g-dam1-profes	10002	sol
g-dam2-profes	10003	noe; sol
g-alum	10004	mon; pia; tom
g-dam1-alum	10005	mon; tom
g-dam2-alum	10006	pia

Group name	GID number	Group members	Group description
g-usuarios	10000		
g-dam1-alum	10005	mon; tom	
g-profes	10001	noe; sol	
g-dam2-profes	10003	noe; sol	
g-alum	10004	Pia; mon; tom	Group account
g-dam2-alum	10006	Pia	
g-dam1-profes	10002	sol	

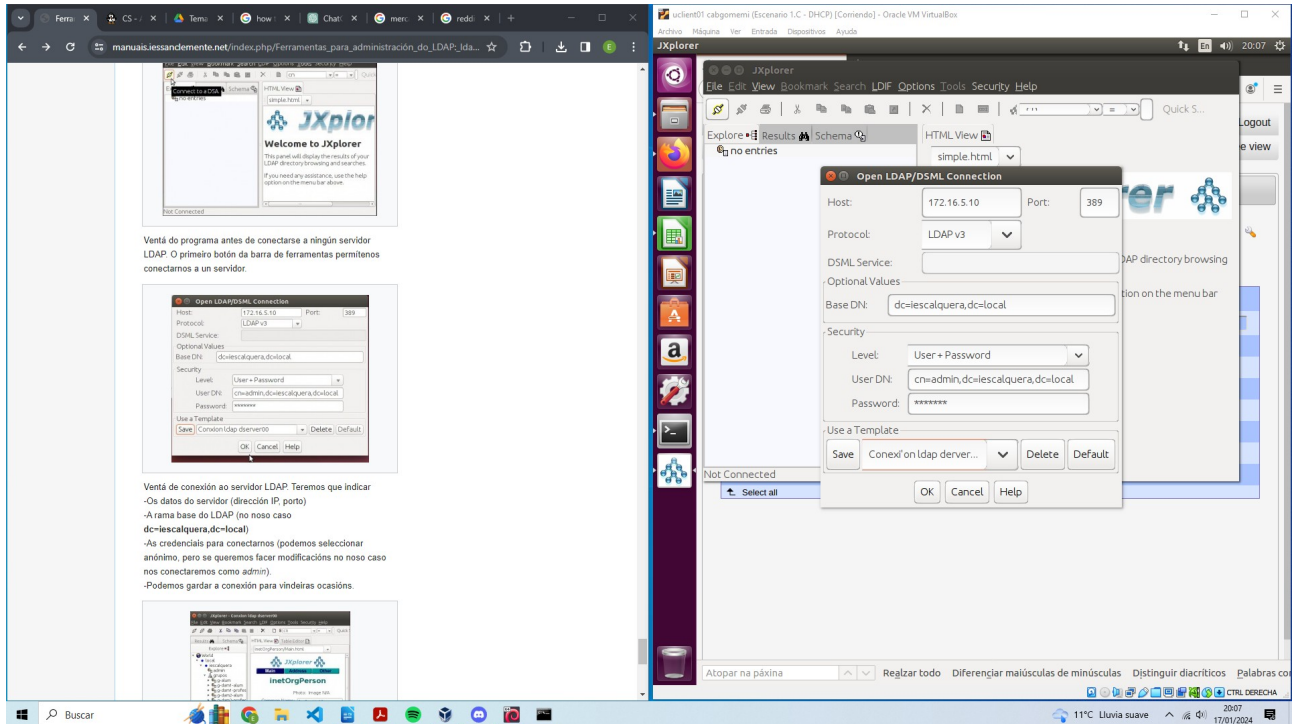
Jxplorer

Instalaremos esta herramienta para el manejo de información almacenada en el servidor ldap.

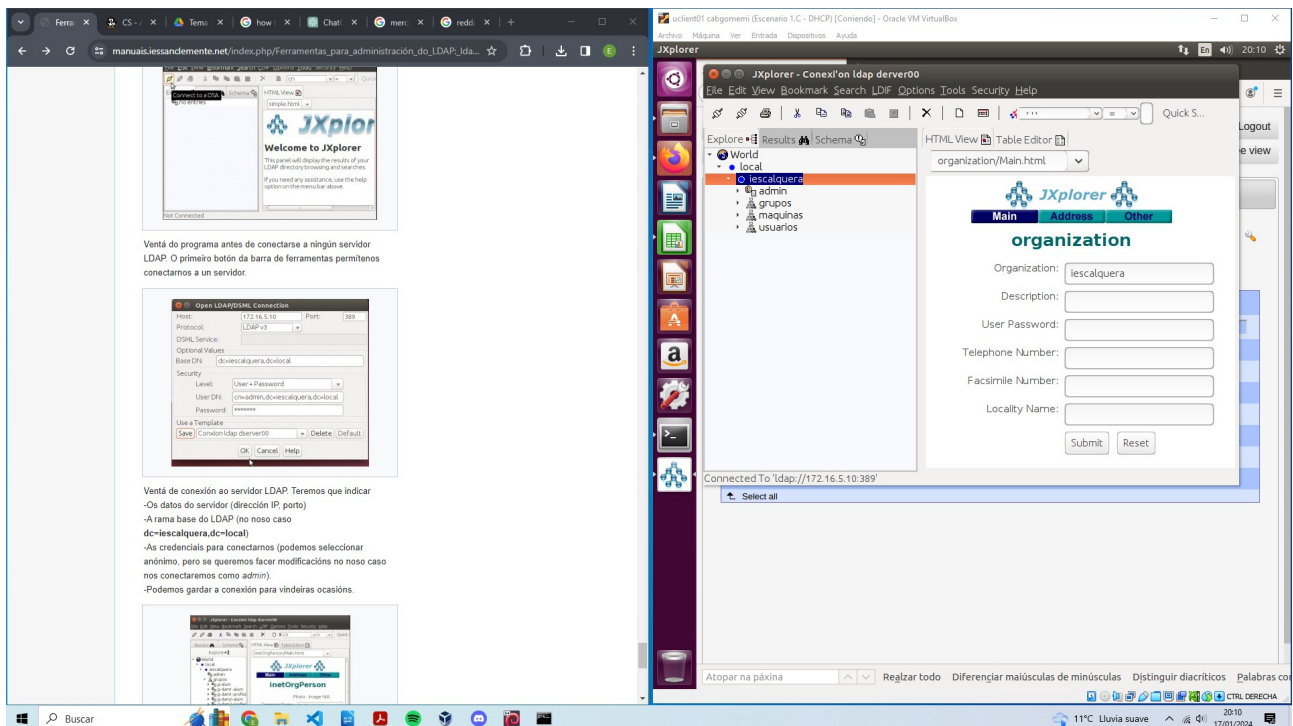
sudo apt-get install jxplorer

Abrimos el programa mediante la interfaz gráfica de ubuntu.

Introducimos los siguientes datos.



Hacemos click en guardar.

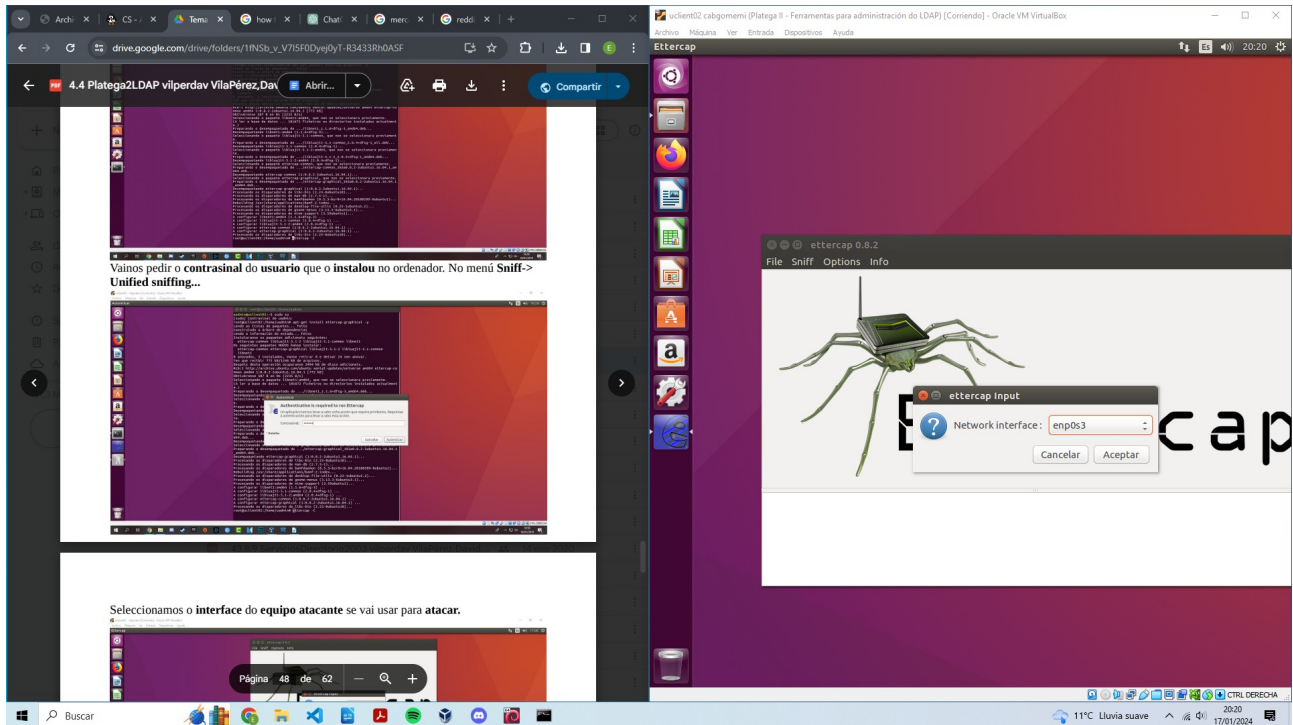


Ya podemos administrar el servidor LDAP mediante JXPLOER.

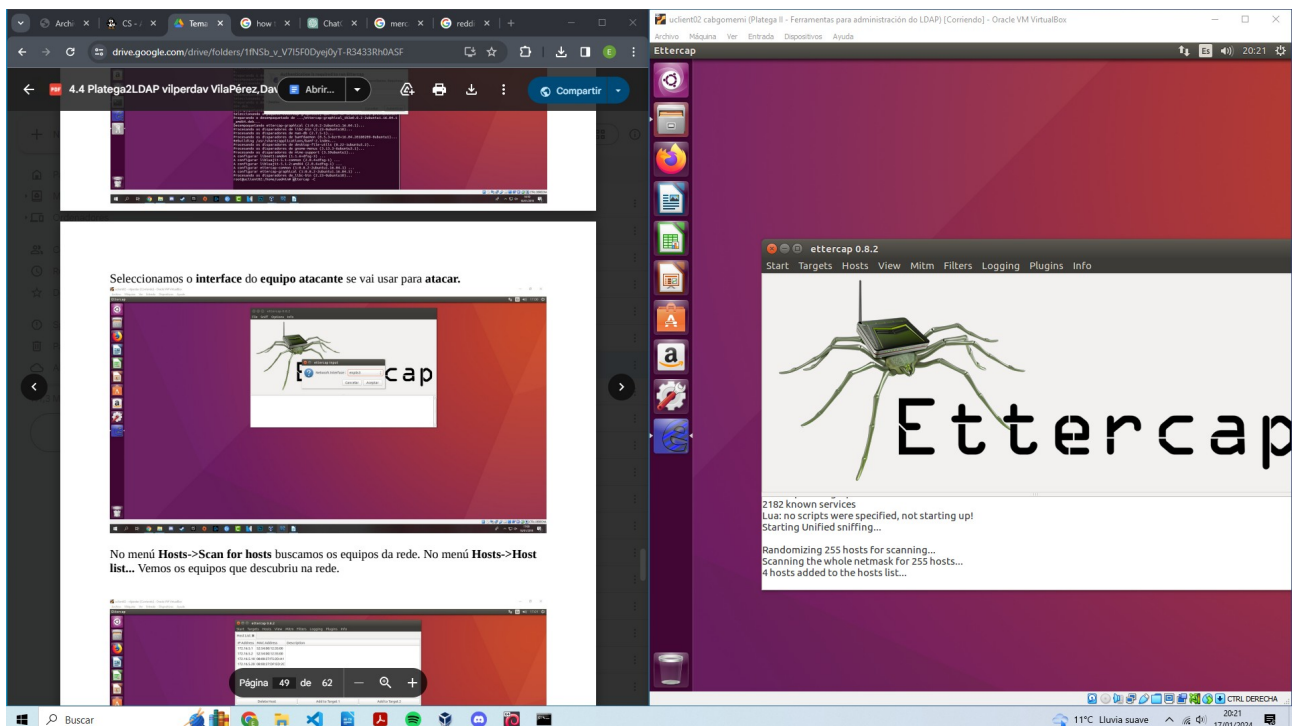
Autenticación segura contra LDAP. Uso de TLS/SSL: LDAPS

Instalamos en uclient02 el programa ettercap

En la pestaña sniff, seleccionamos unified sniffing y la interfaz de red que queramos.



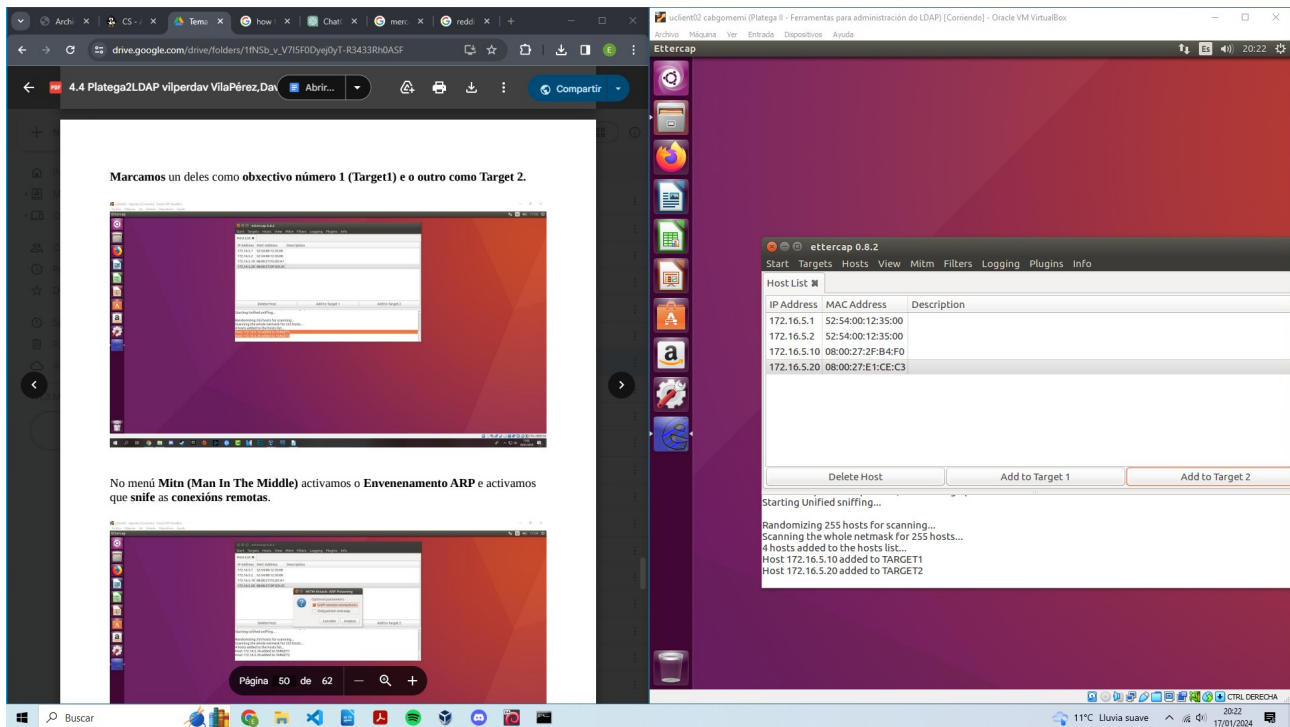
Hosts > scan for hosts



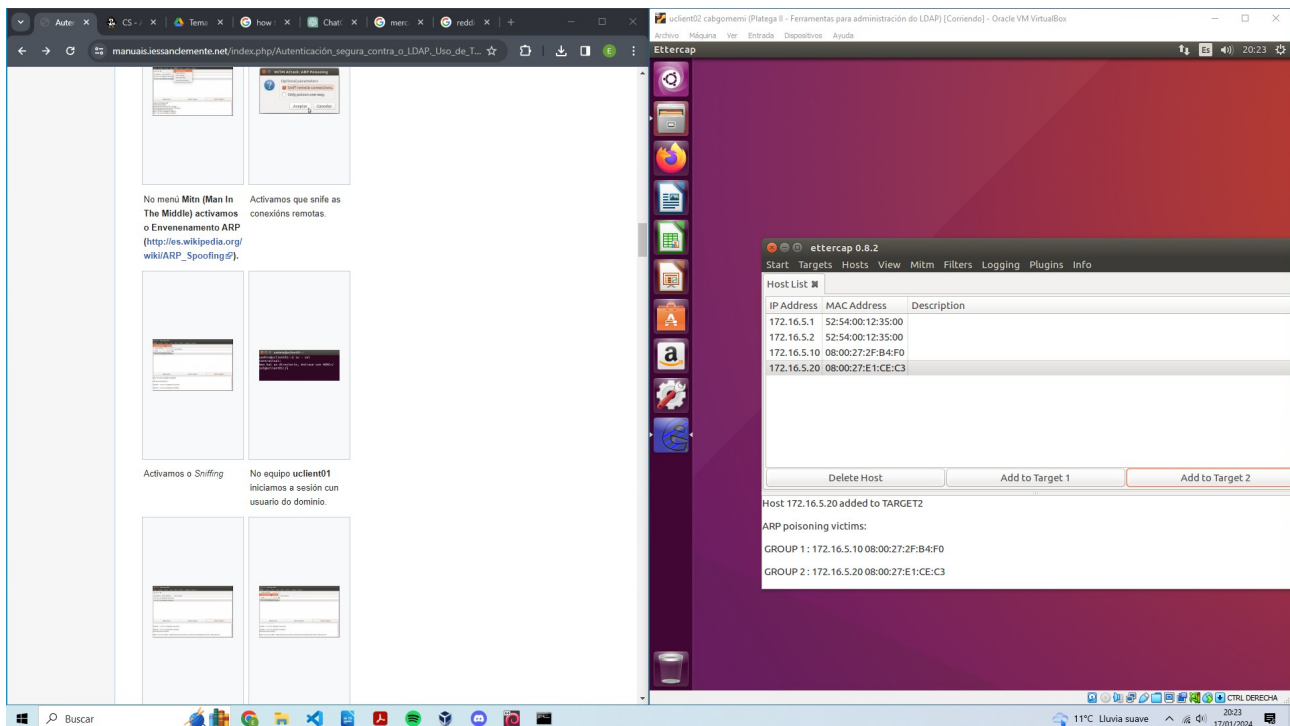
51 Platega I_II_III

Entramos al menú hosts > hosts list.

Seleccionamos uno como target 1 y otro como target 2



En pestaña mtim activamos el sniff de conexiones remotas.



51 Platega I_II_III

Iniciamos sesión en el equipo uclient01 con el usuario de dominio.

The screenshot shows a Windows desktop environment. On the left, a web browser window displays the 'Manuais' website, specifically the page for 'Archivo:DI 2014 ldaps_15.jpeg'. The page includes a sidebar with navigation links and a main content area with a table of hosts and a 'Historial del archivo' section. On the right, a terminal window titled 'uclient01 cabgomei (Platega II - Herramientas para administración de LDAP) [Conenido] - Oracle VM VirtualBox' is open. The terminal shows a command prompt for 'uadmin@uclient01:~' and a series of commands being executed, including 'update-alternatives', 'A configurar default-jre-headless', 'A configurar openjdk-8-jre:amd64', 'A configurar default-jre (2:1.8-56ubuntu2)', 'A configurar javahelp2 (2.0.0s.ds1-8)', 'Procesando os dsparadores de ca-certificates', 'Updating certificates in /etc/ssl/certs...', 'A added, 0 removed; done.', 'Running hooks in /etc/ca-certificates/update.d...', 'done.', 'done.', 'A configurar jxplorer (3.3.2+dfsg-2)', 'Procesando os dsparadores de libc-bin (2.23-8ubuntu11.3)...', 'uadmin@uclient01:~\$ su - noe', 'Contraseña:', 'Non hai un directorio, entrase con HOME=/', 'noe@uclient01:/\$'.

Aquí podemos ver los usuarios y las contraseñas capturadas.

The screenshot shows a Windows desktop environment. On the left, a web browser window displays the 'Manuais' website, specifically the page for 'Archivo:DI 2014 ldaps_15.jpeg'. The page includes a sidebar with navigation links and a main content area with a table of hosts and a 'Historial del archivo' section. On the right, a terminal window titled 'uclient02 cabgomei (Platega II - Herramientas para administración de LDAP) [Conenido] - Oracle VM VirtualBox' is open. The terminal shows a command prompt for 'uadmin@uclient02:~' and a series of commands being executed, including 'update-alternatives', 'A configurar default-jre-headless', 'A configurar openjdk-8-jre:amd64', 'A configurar default-jre (2:1.8-56ubuntu2)', 'A configurar javahelp2 (2.0.0s.ds1-8)', 'Procesando os dsparadores de ca-certificates', 'Updating certificates in /etc/ssl/certs...', 'A added, 0 removed; done.', 'Running hooks in /etc/ca-certificates/update.d...', 'done.', 'done.', 'A configurar jxplorer (3.3.2+dfsg-2)', 'Procesando os dsparadores de libc-bin (2.23-8ubuntu11.3)...', 'uadmin@uclient02:~\$ su - noe', 'Contraseña:', 'Non hai un directorio, entrase con HOME=/', 'noe@uclient02:/\$'.

Paramos el sniffing.

Creación de los certificados digitales

Creación de la autoridad de certificación

Creamos directorios.

mkdir /etc/ssl/CA

mkdir /etc/ssl/newcerts

Creamos dos ficheros necesarios para el CA

touch /etc/ssl/CA/index.txt

sh -c "echo '01' > /etc/ssl/CA/serial"

The screenshot shows a web browser on the left displaying a tutorial for creating a Certificate Authority (CA). The tutorial includes the following steps and commands:

- Crear a Autoridade de Certificação (CA)**: En dserver00, primeiro, creamos os directorios para almacenar os certificados da CA e os ficheiros relacionados:


```
mkdir /etc/ssl/CA
mkdir /etc/ssl/newcerts
```
- Creamos dous ficheiros para manter un número de serie que lle asignará a cada certificado e almacenar os certificados emitidos:


```
touch /etc/ssl/CA/index.txt
sh -c "echo '01' > /etc/ssl/CA/serial"
```
- No ficheiro de configuración da CA `/etc/ssl/openssl.cnf`, modificaremos os seguintes parámetros dentro da sección `[CA_default]`:


```
dir = /etc/ssl # Where everything is kept
...
database = $dir/CA/index.txt # database index file.
...
certificate = $dir/certs/cacert.pem # The CA certificate
serial = $dir/CA/serial # The current serial number
```
- Creamos o certificado raíz para a propia CA, que será firmado por si mesma:


```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```
- Teremos que introducir un contrasinal para a CA (podemos poñer `abc123`), e os datos do certificado.
 - A continuación móstrase un exemplo para estes datos.
 - É importante ter en conta que o que poñamos en **Organization Name**, deberá ser o mesmo valor que togo poñamos neste mesmo campo no certificado do servidor.
- Generating a 1024 bit RSA private key


```
.....+++++
.....+++++
unable to write 'random state'
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
```

On the right, a terminal window shows the execution of these commands on a system named `uclient01` (Debian 4.9.320-2):

```
administrador@dserver00:~$ su
root@dserver00:/home/administrador# nano /etc/ldscripts/ldscripts.conf
root@dserver00:/home/administrador# service apache2 restart
root@dserver00:/home/administrador# vim /etc/ldscripts/ldscripts.conf
root@dserver00:/home/administrador# root@dserver00:/home/administrador# client_loop: send disconnect: Connection reset
C:\Users\Emilio>ssh administrador@192.168.1.40 -p 10022
C:\Users\Emilio>ssh administrador@192.168.1.40 -p 10022
administrador@192.168.1.40's password:
Linux dserver00 4.9.0-19-amd64 #1 SMP Debian 4.9.320-2 (2022-06-30) x86_64

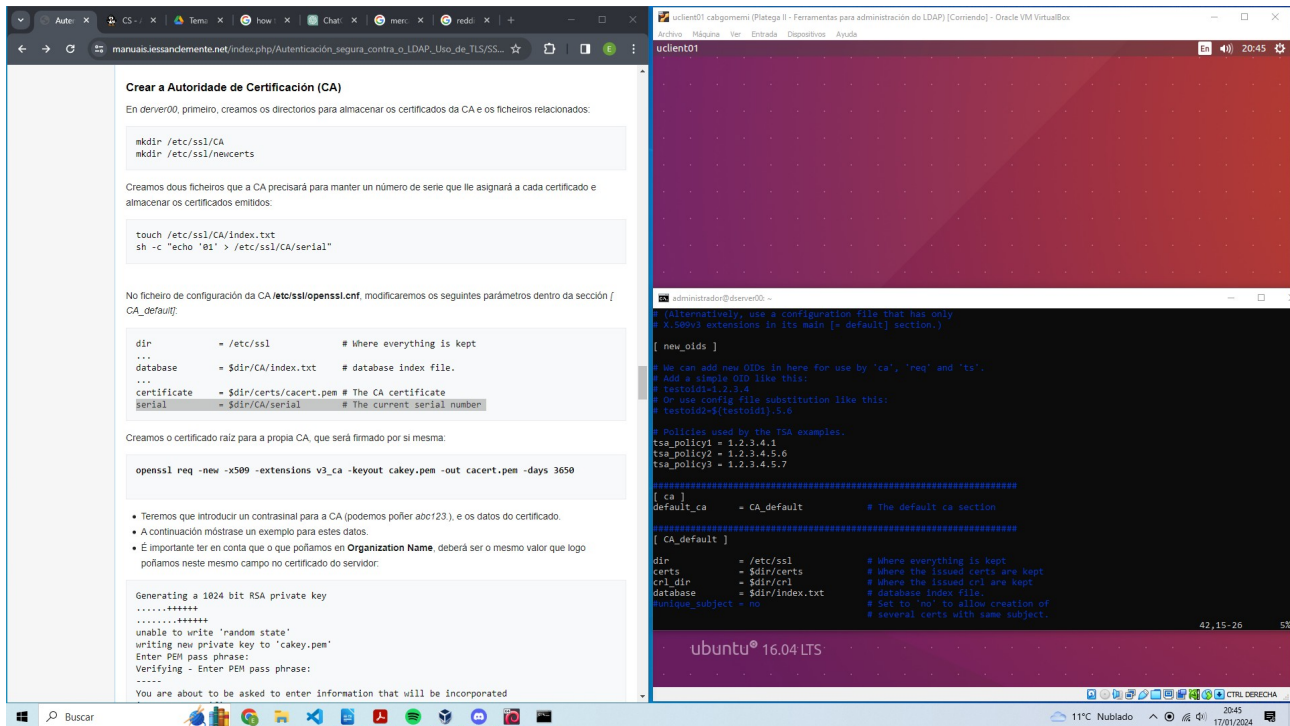
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 17 15:00:29 2024 from 192.168.1.40
administrador@dserver00:~$ su
Password:
root@dserver00:/home/administrador# mkdir /etc/ssl/CA
root@dserver00:/home/administrador# mkdir /etc/ssl/newcerts
root@dserver00:/home/administrador# touch /etc/ssl/CA/index.txt
root@dserver00:/home/administrador# sh -c "echo '01' > /etc/ssl/CA/serial"
root@dserver00:/home/administrador# n
```

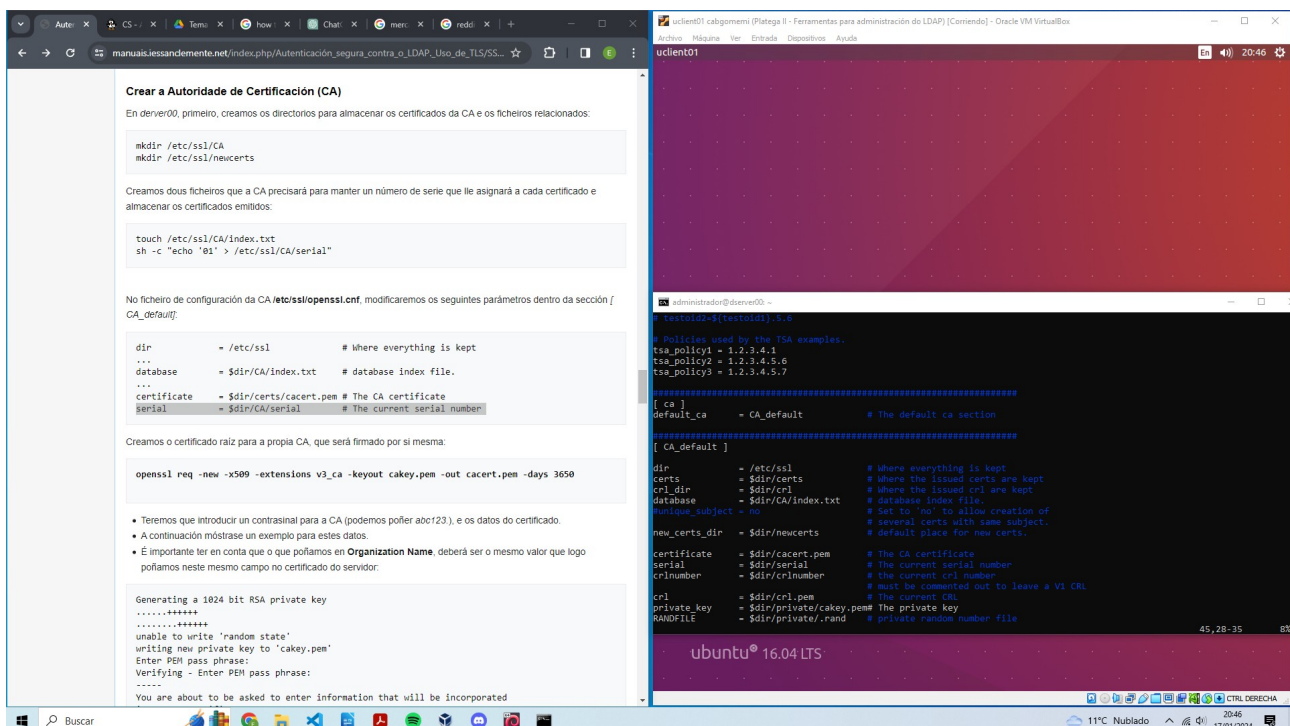
Editamos el fichero de configuración para que contenga lo siguientes ajustes:

51 Platega I_II_III

dir = /etc/ssl # Where everything is kept

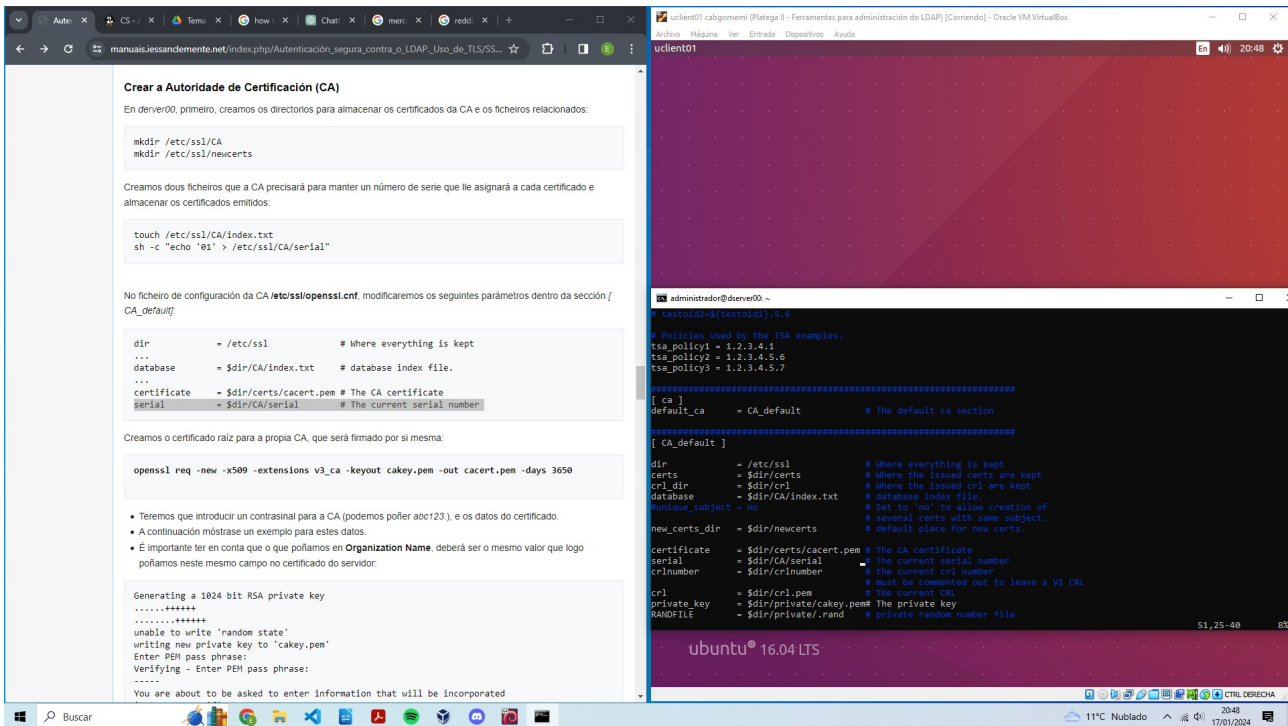


database = \$dir/CA/index.txt # database index file.



certificate = \$dir/certs/cacert.pem # The CA certificate

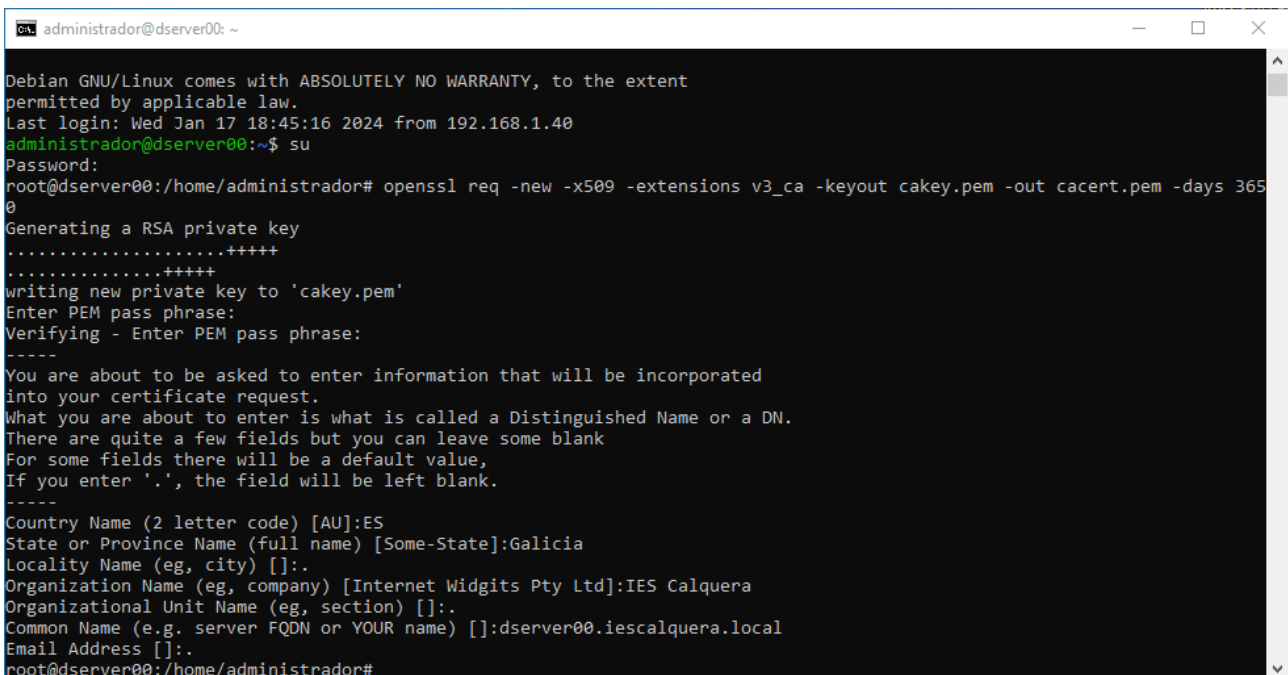
serial = **\$dir/CA/serial** # The current serial number



Creamos el certificado para la CA que será firmado por ella misma.

openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650

Responderemos a las preguntas de la siguiente manera.



Estos datos es importante tomar nota de ellos.

Movemos a los directorios creados anteriormente tanto la clave privada como el certificado mediante el comando:

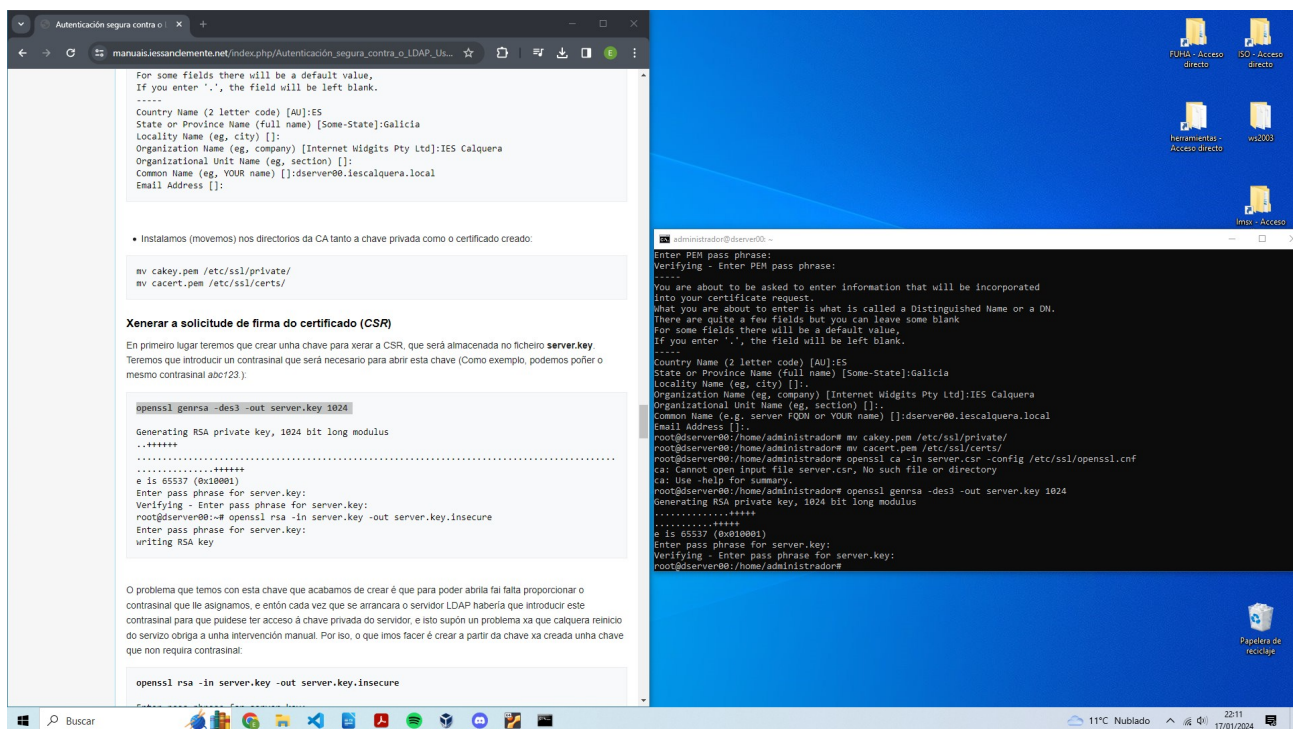
```
mv cakey.pem /etc/ssl/private/
```

```
mv cacert.pem /etc/ssl/certs/
```

Generar la solicitud de firma del certificado (CSR)

Introducimos el comando:

```
openssl genrsa -des3 -out server.key 1024
```

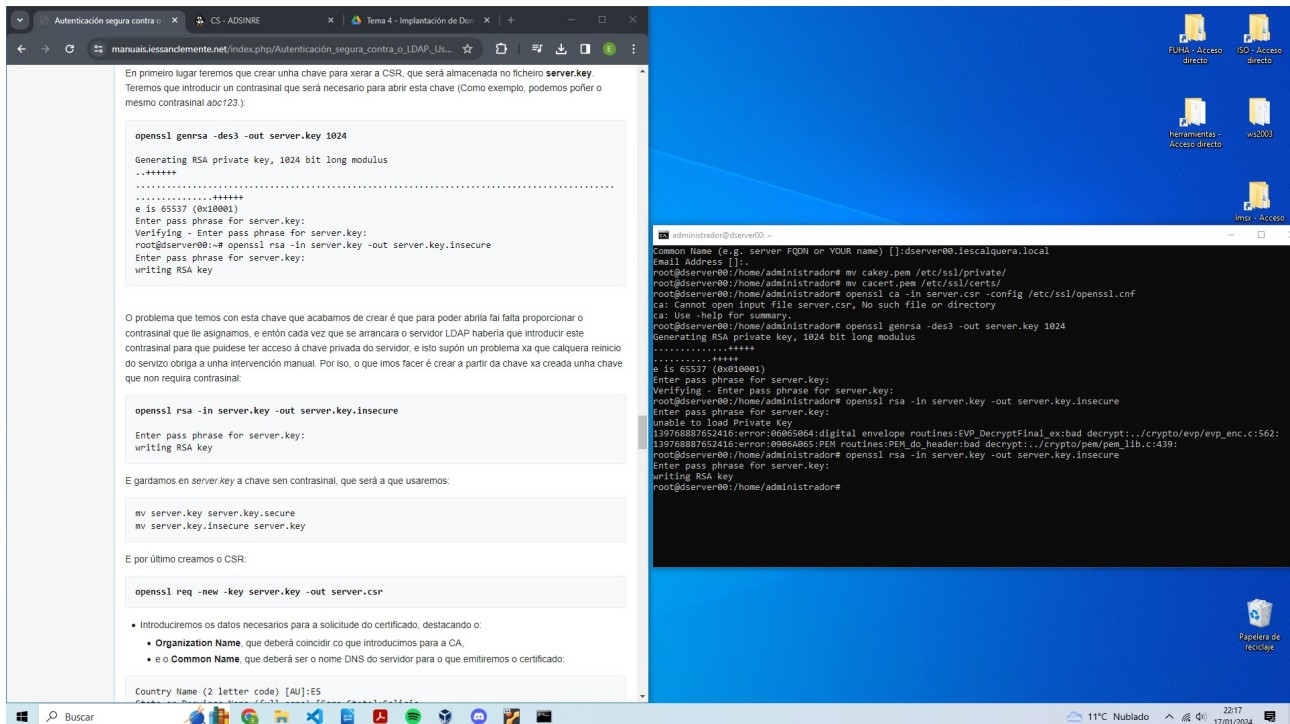


He introducido la contraseña que estamos acostumbrados a emplear.

Generaremos a partir de la clave que acabamos de generar, otra que no requiera de contraseña siempre que reiniciamos el servicio ldap.

```
openssl rsa -in server.key -out server.key.insecure
```


51 Platega I_II_III



Guardamos la clave sin contraseña mediante los siguientes comandos.

Creamos el CSR

Empleamos el siguiente comando.

openssl ca -in server.csr -config /etc/ssl/openssl.cnf

```
root@dserver00:/home/administrador# openssl req -new -key server.key -out server.csr
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]:Galicia
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Calquera
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:dserver00.iescalquera.local
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123.
An optional company name []:abc123.
root@dserver00:/home/administrador#
```

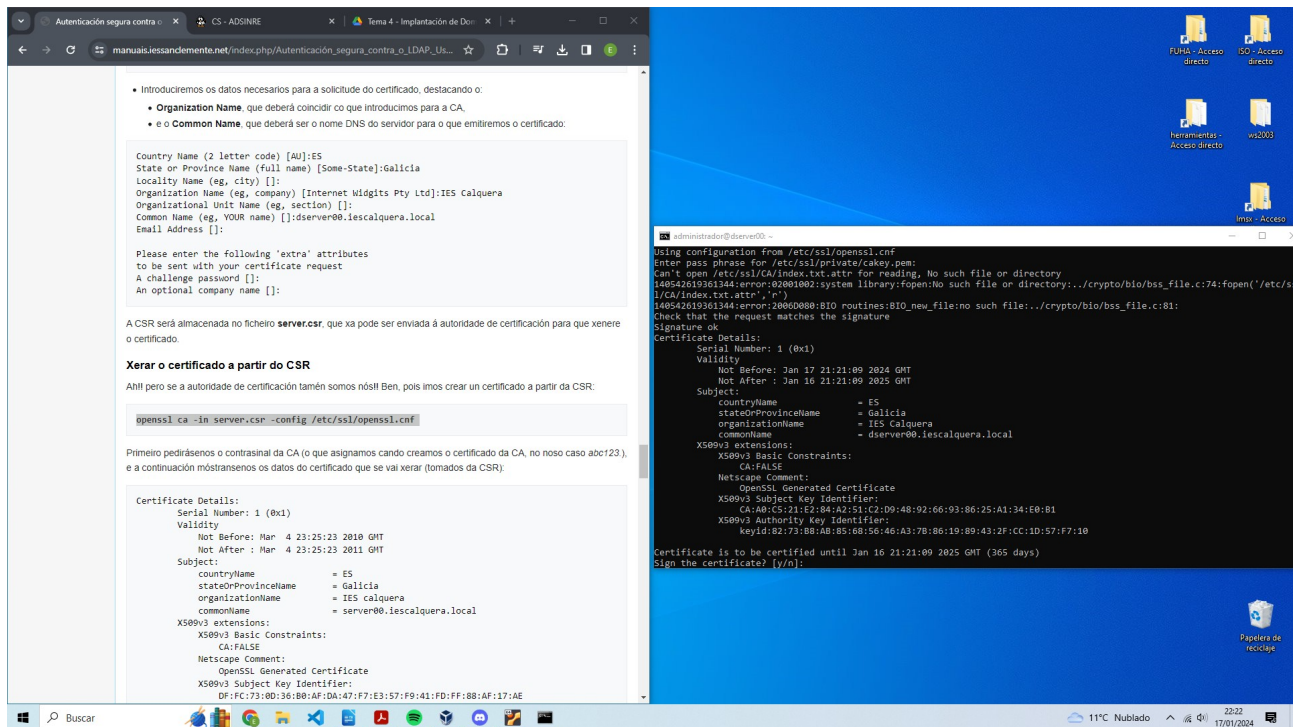
Fijarse en los elementos introducidos.

Generar el certificado a partir do CSR

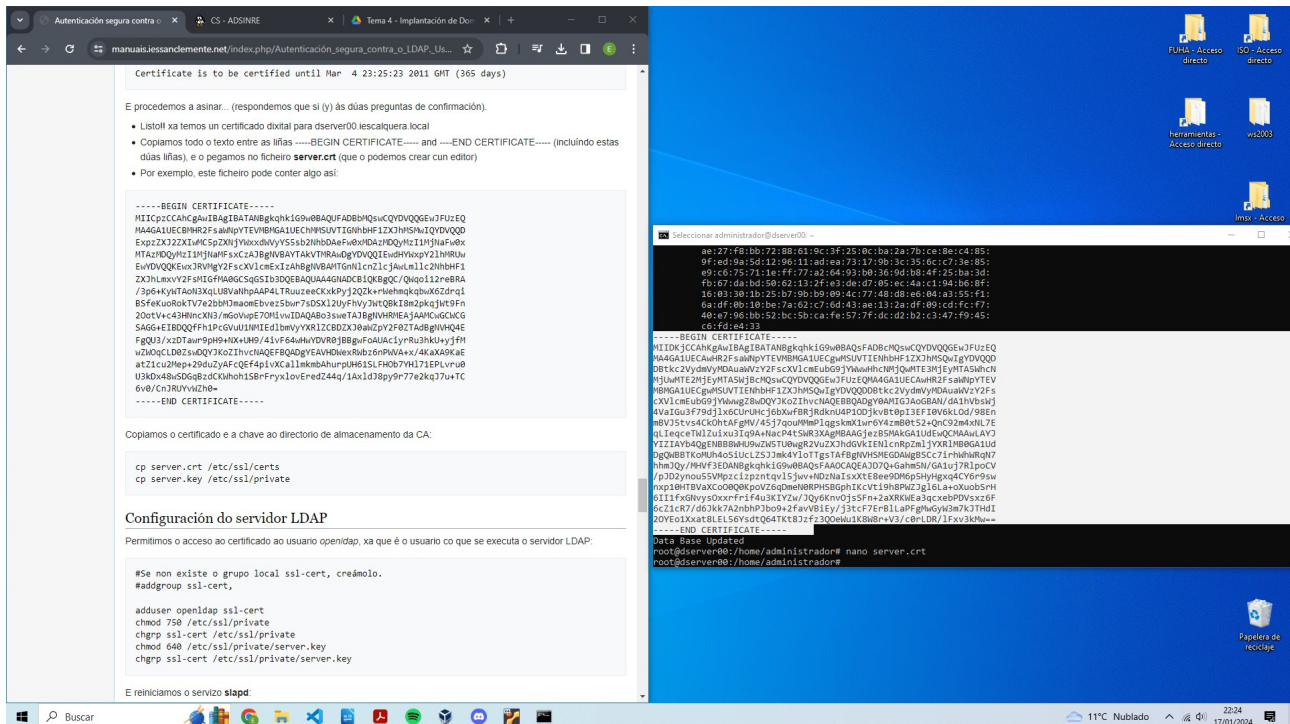
Empleamos el comando:

openssl ca -in server.csr -config /etc/ssl/openssl.cnf

Comprobamos que los datos son correctos.



Copiamos el contenido del output que se encuentra entre las líneas BEGIN CERTIFICATE Y END CERTIFICATE (ambas estas líneas incluídas) en un archivo que llamaremos server.crt



Copiamos la clave al directorio de almacenamiento.

cp server.crt /etc/ssl/certs

cp server.key /etc/ssl/private

Configuración do servidor LDAP

Permitimos el acceso al certificado al usuario openldap (que crearemos ahora) .

Groups para comprobar los grupos que están creados. Sino esta creado, emitiremos el comando.

addgroup ssl-cert,

En mi caso ya lo tenía creado por eso me dio el mensaje de error que vimos en pantalla.

Mediante este comando añadimos al usuario openldap al grupo.

adduser openldap ssl-cert

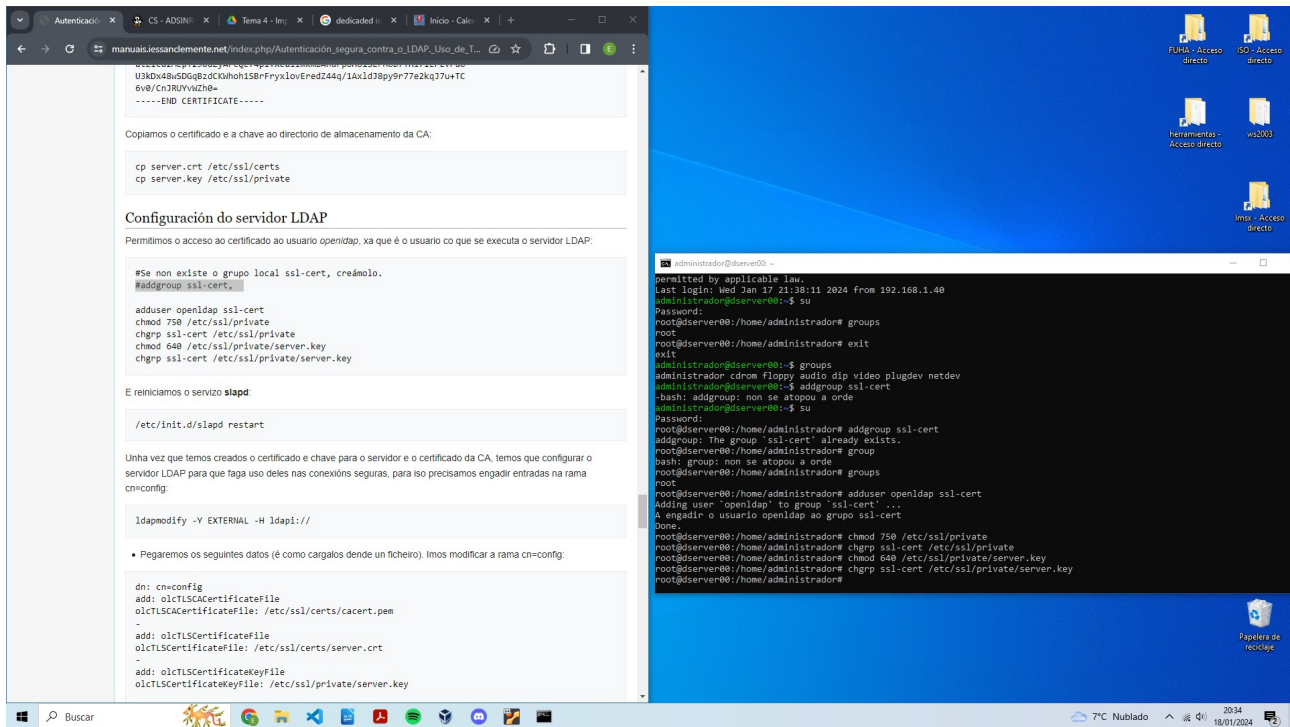
chmod 750 /etc/ssl/private

chgrp ssl-cert /etc/ssl/private

chmod 640 /etc/ssl/private/server.key

chgrp ssl-cert /etc/ssl/private/server.key

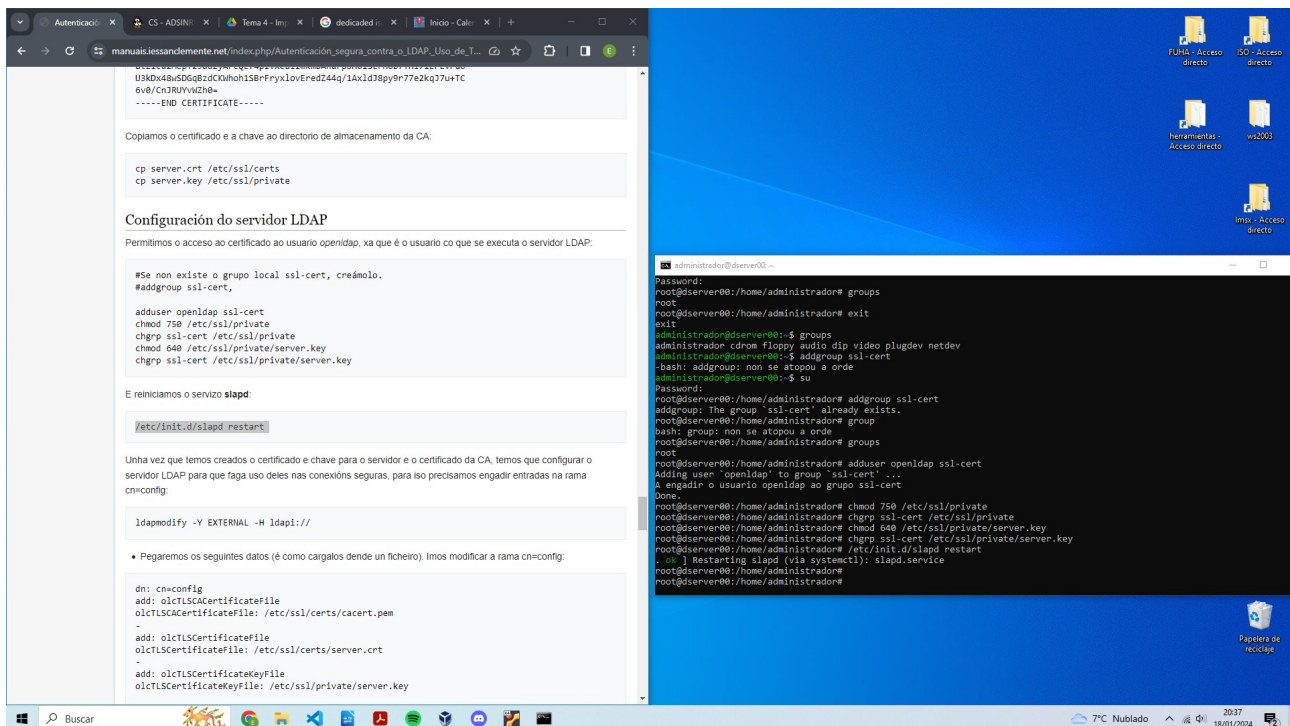
51 Platega I_II_III



Reiniciamos el servicio Ldapsearch

/etc/init.d/slapd restart

(Es posible que tarde unos segundos en reiniciar).



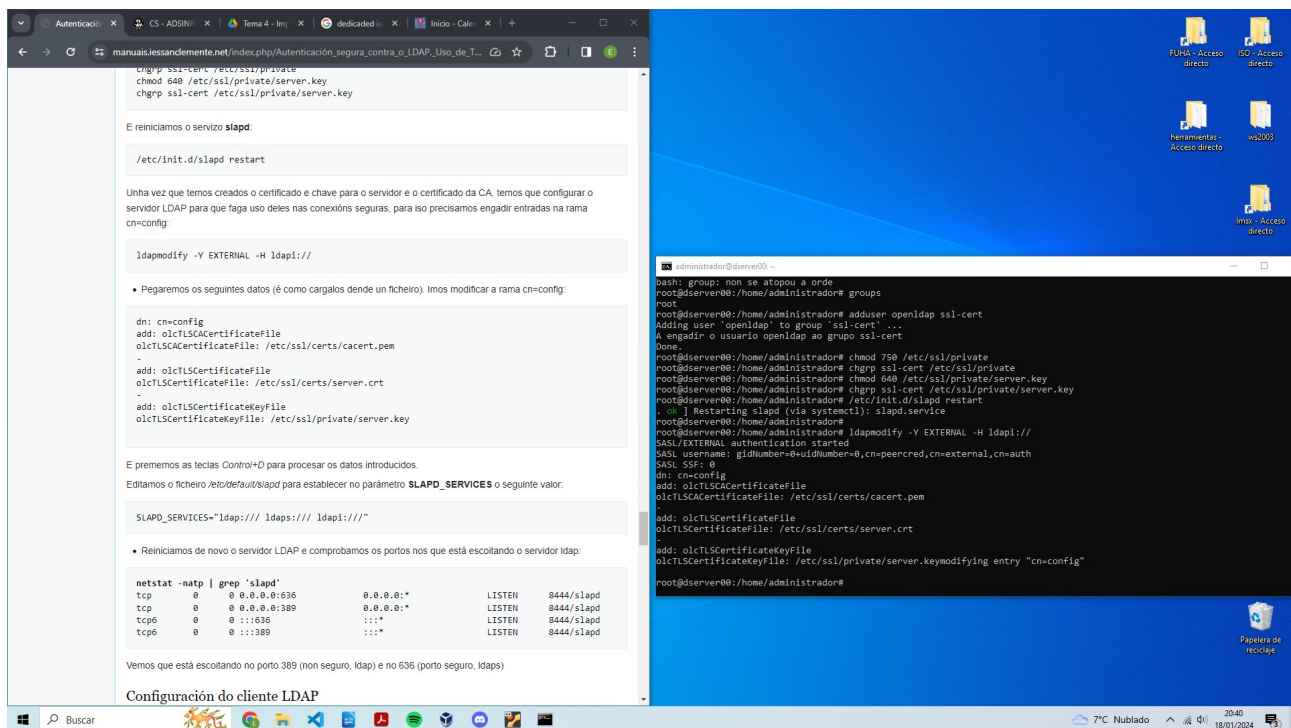
Ahora emitiremos el comando.

ldapmodify -Y EXTERNAL -H ldapi://

Pegaremos las siguientes líneas en el terminal. Al pegar las líneas presionaremos las teclas ctrl + d para cargar las entradas.

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/server.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/server.key
```

Terminal



Editamos el archivo /etc/default/slapd e introducimos el valor:

SLAPD_SERVICES="ldap:/// ldaps:/// ldapi:///"

Recomiendo usar la función de búsqueda de el editor de texto de su elección.

51 Platega I_II_III

The screenshot shows a Linux desktop with a blue background. On the left, a web browser displays a tutorial for configuring slapd. The tutorial includes instructions for setting permissions, restarting the service, and configuring the slapd.conf file. It also shows the output of the netstat command, which indicates that slapd is listening on ports 389 and 636. On the right, a terminal window shows the same configuration steps being executed. The terminal output includes the commands for setting permissions, restarting the service, and editing the slapd.conf file. It also shows the output of the netstat command, which confirms that slapd is listening on the correct ports.

manuais.essandamente.net/index.php/Autenticación_segura_contra_o_LDAP_Uso_de_T...

```
chmod 640 /etc/ssl/private/server.key
chgrp ssl-cert /etc/ssl/private/server.key
```

Reiniciamos o servizo slapd:

```
/etc/init.d/slapd restart
```

Unha vez que temos creados o certificado e chave para o servidor e o certificado da CA, temos que configurar o servidor LDAP para que faga uso deles nas conexións seguras, para iso precisamos engadir entradas na rama cn=config:

```
ldapmodify -Y EXTERNAL -H ldapi:///
```

- Pegaremos os seguintes datos (é como cargalos dende un ficheiro). Imos modificar a rama cn=config:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/server.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/server.key
```

E prememos as teclas **Control+D** para procesar os datos introducidos.

Editamos o ficheiro `/etc/default/slapd` para establecer no parámetro **SLAPD_SERVICES** o seguinte valor:

```
SLAPD_SERVICES="ldap:/// ldaps:/// ldapi:///"
```

- Reiniciamos de novo o servidor LDAP e comprobamos os portos nos que está escoitando o servidor ldap:

```
netstat -natp | grep 'slapd'
```

Protocol	Local Address	Foreign Address	State	Process
tcp	0.0.0.0:636	0.0.0.0:*	LISTEN	8444/slapd
	0.0.0.0:389	0.0.0.0:*	LISTEN	8444/slapd
tcp6	:::636	:::*	LISTEN	8444/slapd
	:::389	:::*	LISTEN	8444/slapd

Vemos que está escoitando no porto 389 (non seguro, ldap) e no 636 (porto seguro, ldaps)

Configuración do cliente LDAP

```
# Empty line the compiled-in default (/etc/ldap/slapd.d with a fallback to
# /etc/ldap/slapd.conf).
# System account to run the slapd server under. If empty the server
# will run as root.
# SLAPD_USER="openldap"
# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
# SLAPD_GROUP="openldap"
# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf by
# default)
# SLAPD_PIDFILE=
# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://197.0.0.1:389/ ldaps:/// ldapi:///"
# SLAPD_SERVICES="ldap:/// ldaps:/// ldapi:///"
# If SLAPD_WD_START is set, the init script will not start or restart
# slapd (but stop will still work). Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
```

Para comprobar que servicios tenemos activos podemos emplear el comando:

systemctl list-units --type=service --state=active | grep la | less

```

administrador@dserv00: ~
cron.service                                loaded active running Regular
background program processing daemon
keyboard-setup.service                     loaded active exited Set the
console keyboard layout
slapd.service                              loaded active running LSB: Ope
nLDAP standalone server (Lightweight Directory Access Protocol)
systemd-tmpfiles-setup.service              loaded active exited Create V
olatile Files and Directories
(END)

```

Reiniciamos el servicio ldap mediante el comando.

systemctl restart slapd

The screenshot shows a desktop environment with a blue background. On the left, a web browser displays the ProgramaMe website, which is for a programming competition. The website has a navigation bar with 'ProgramaMe', 'Información general', 'Problemas', 'Regionales', and 'Ediciones anteriores'. Below the navigation bar, there's a large banner with 'ProgramaMe' and 'Concurso de Programación para Ciclos Formativos'. A sidebar on the left lists various sections like 'Inicio', 'Reglamento', 'Fechas importantes', 'Inscripción', 'Equipos participantes', 'Entrenamiento', 'Desarrollo del concurso', and 'Centro organizador'. The main content area features a 'Calentamiento pre-navideño' section for December 18, 2023, organized by IES Serra Perenxisa.

On the right, a terminal window is open, showing the output of the command `systemctl list-units --type=service --state=active | grep la | less`. The output lists various services and their states, including `cron.service`, `background program processing daemon`, `keyboard-setup.service`, `console keyboard layout`, `slapd.service`, `nLDAP standalone server (Lightweight Directory Access Protocol)`, `systemd-tmpfiles-setup.service`, and `volatile Files and Directories`. The terminal also shows the command `systemctl restart slapd` being executed.

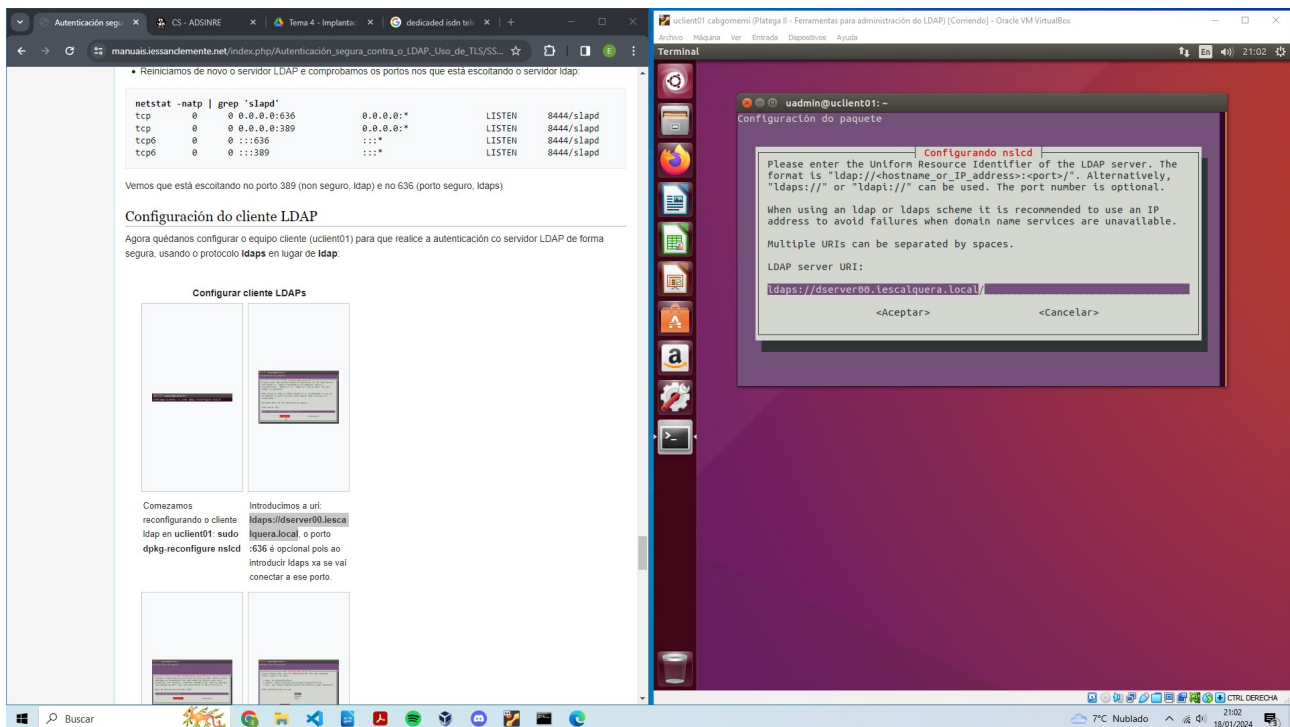
Configuración del cliente.

Reconfiguramos el cliente.

Introducimos el comando:

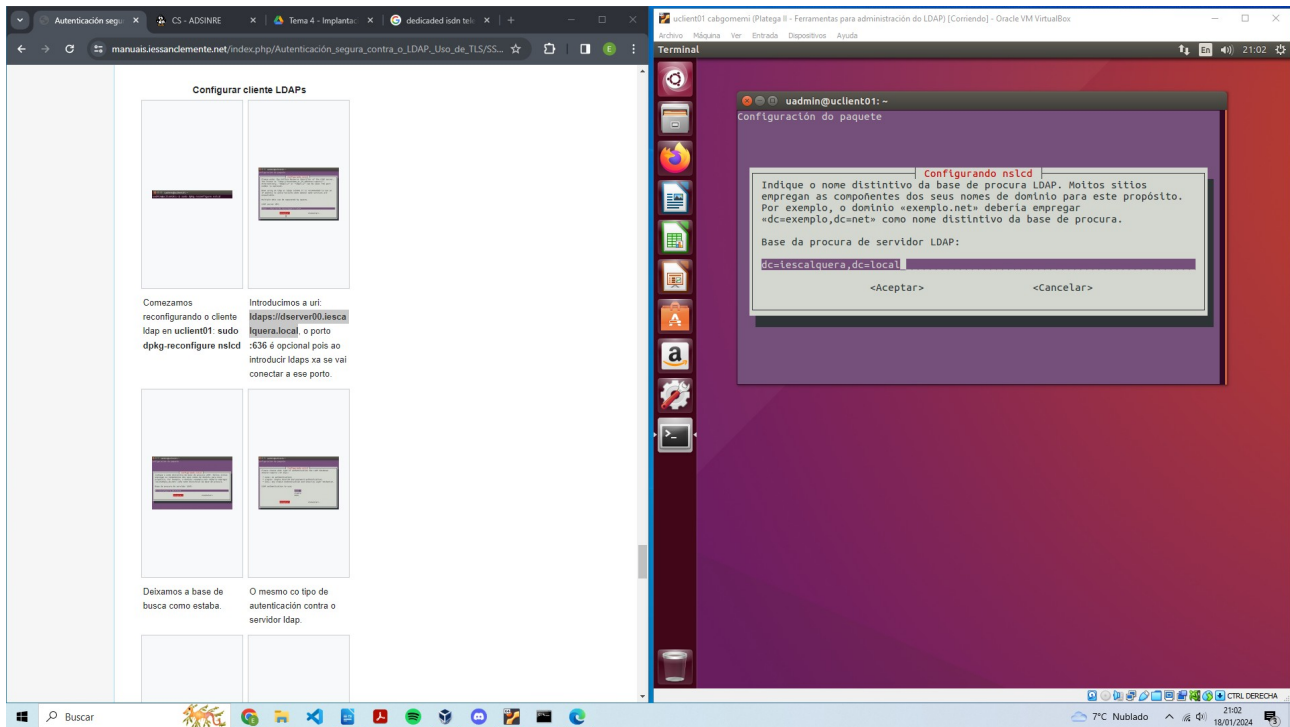
sudo dpkg-reconfigure nslcd

Introducimos la URI, ldaps://dserver00.iescalquera.local

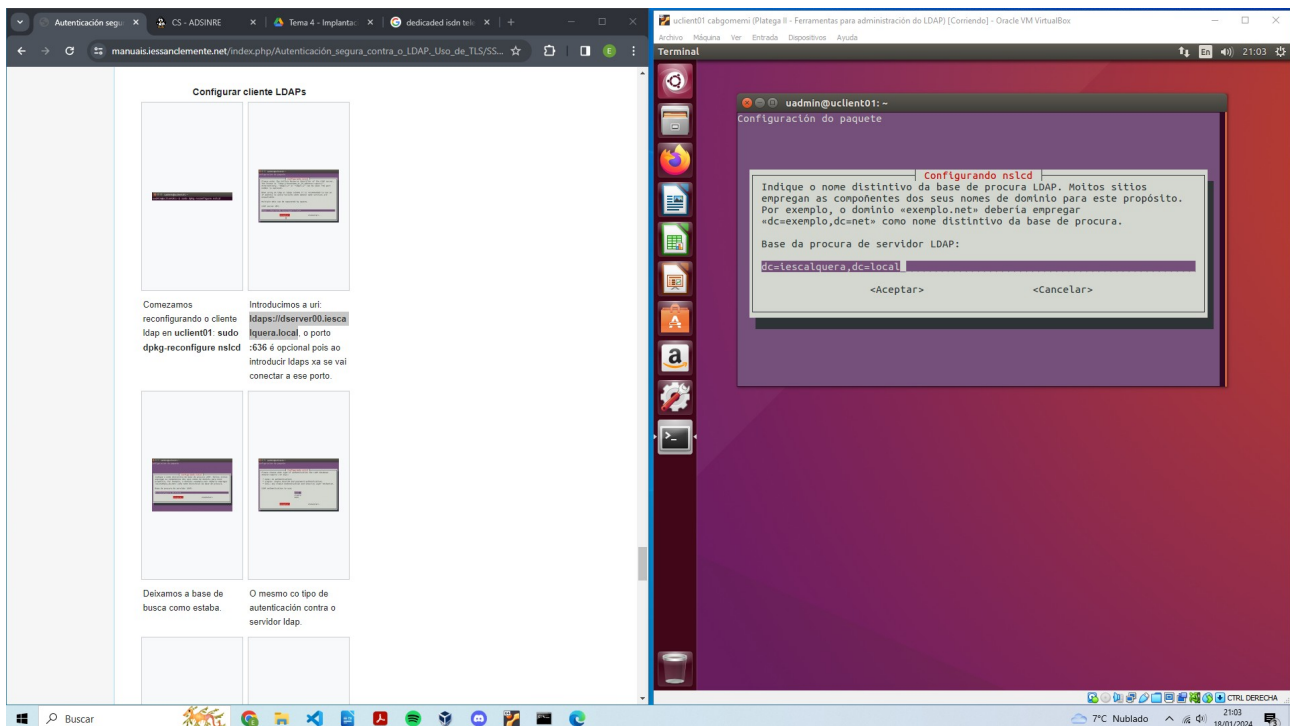


Dejamos este ajuste tal y como estaba

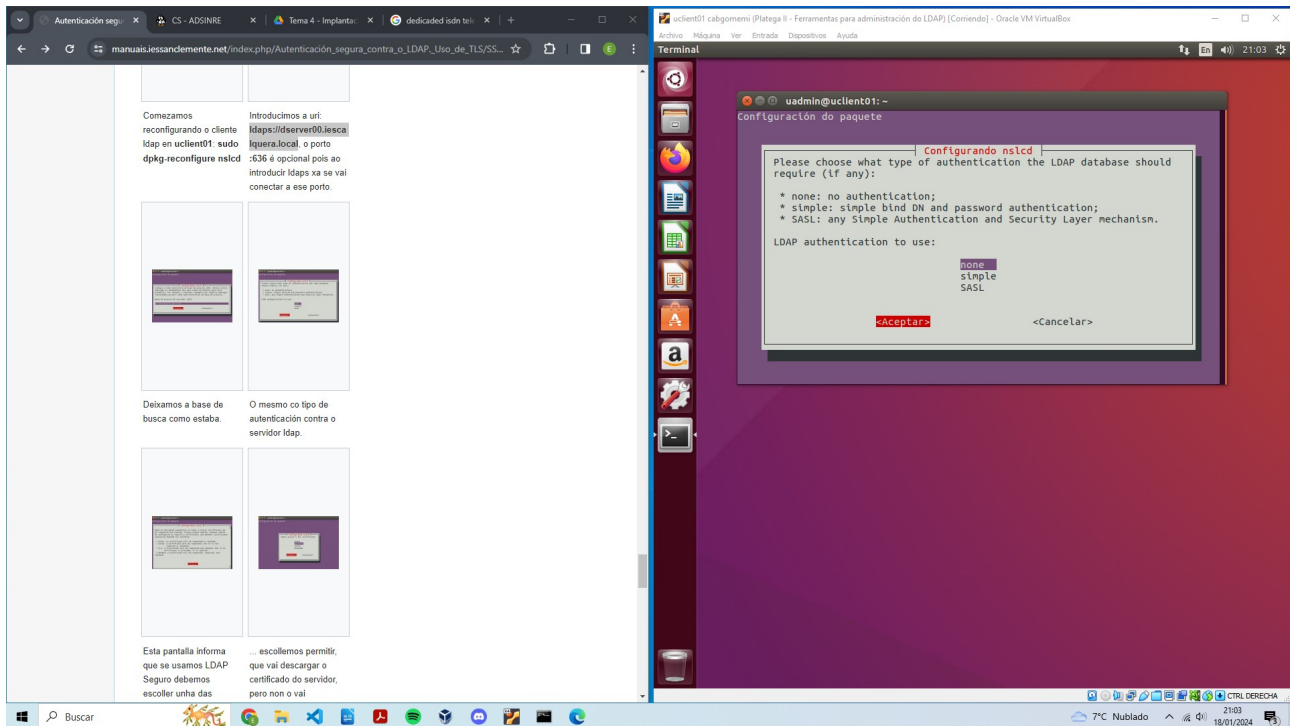
51 Platega I_II_III



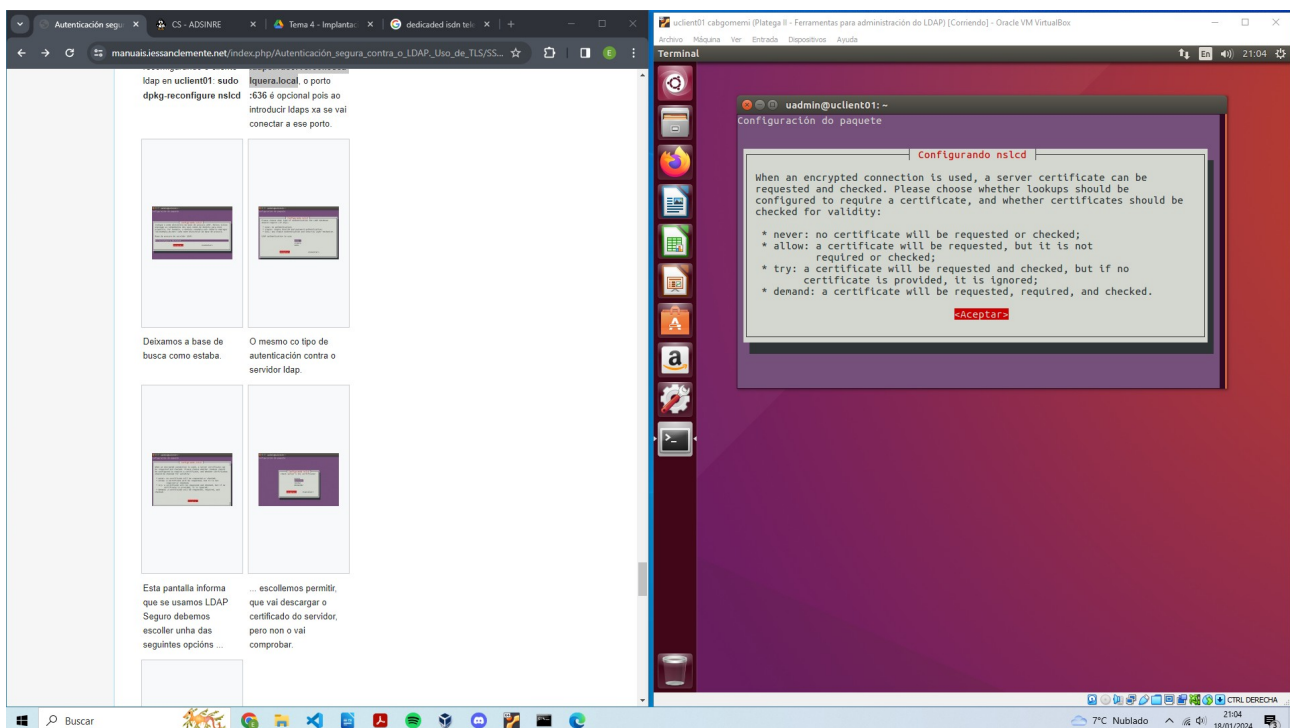
Dejamos este ajuste tal y como estaba



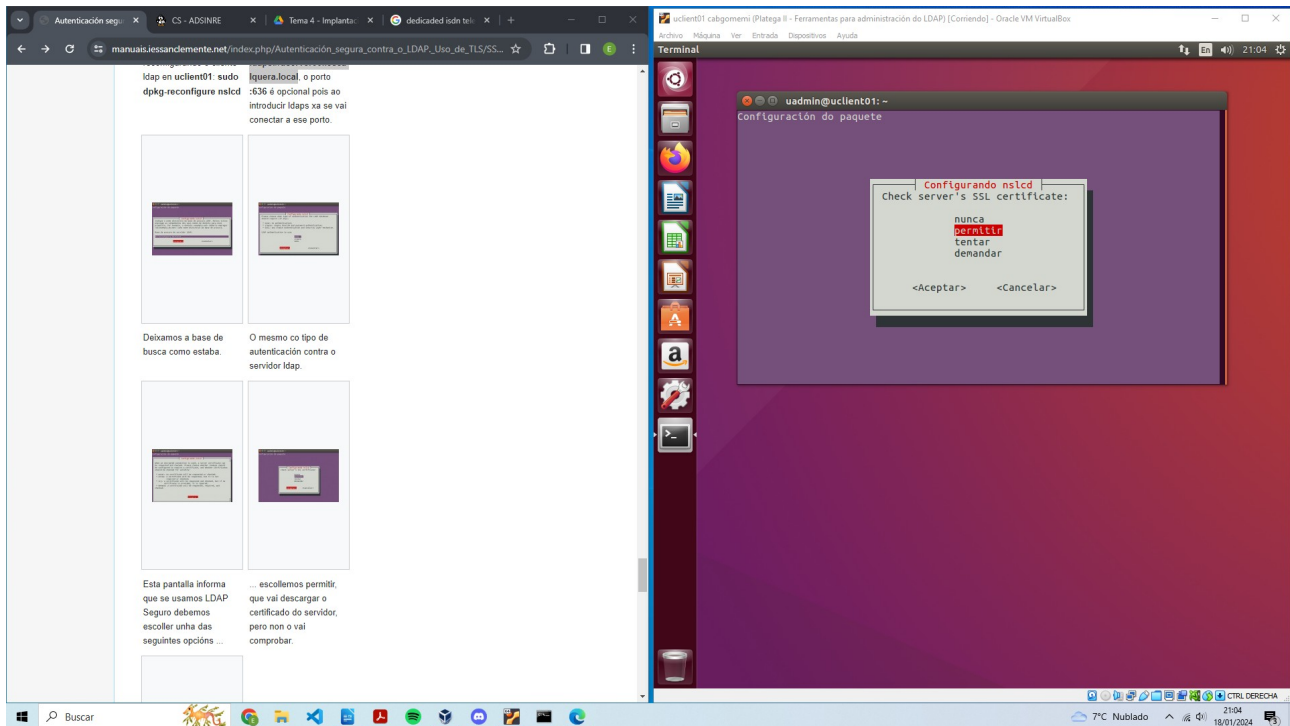
Dejamos este ajuste tal y como estaba



Aceptar

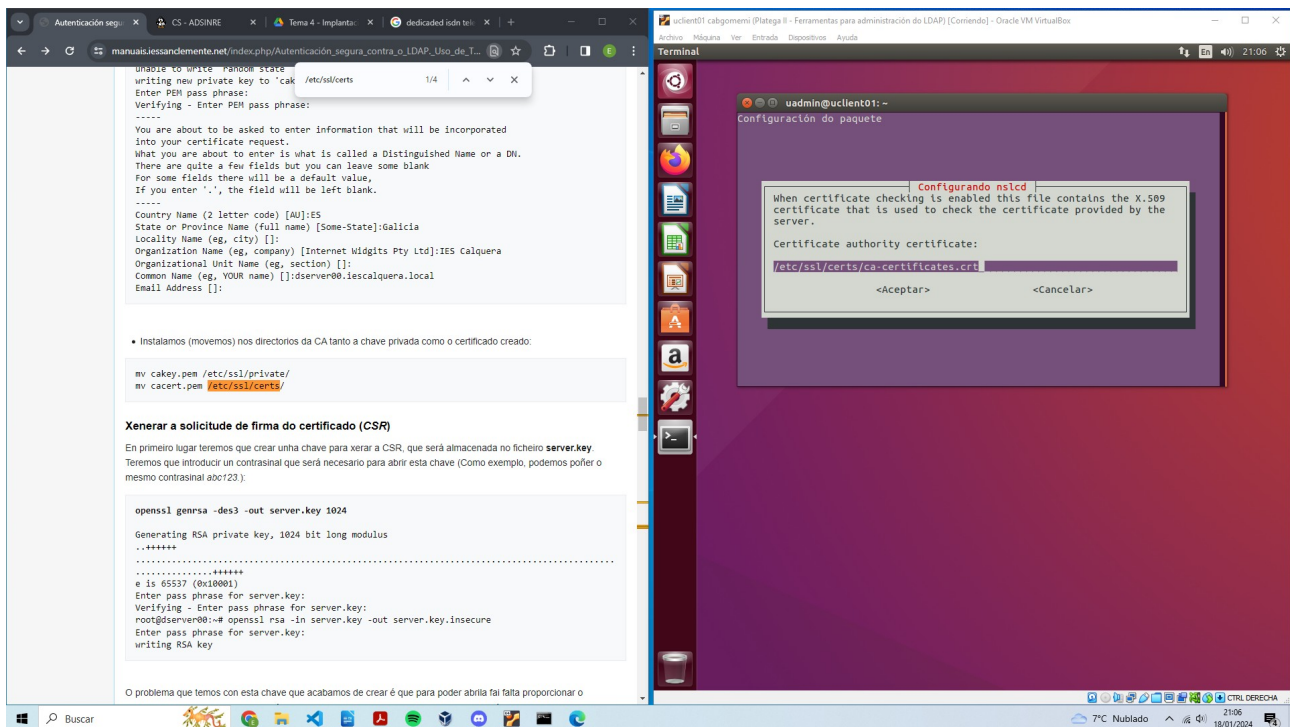


Seleccionamos PERMITIR



Dejamos este ajuste tal y como estaba y comprobamos que el directorio dónde hemos almacenado las claves con anterioridad.

/etc/ssl/certs/



Comprobación mediante ettercap

La conexión está encriptada por lo que las credenciales de acceso no son visibles en clear text.

The screenshot shows a desktop environment with a web browser and the Ettercap 0.8.2 interface. The browser displays a webpage with instructions on how to use Ettercap for LDAP authentication. The Ettercap interface shows a list of connections, including one to 172.16.5.10:636, which is identified as an Anonymous Bind connection.

Webpage Content:

```

30
31
32 # The search scope.
33 #scope sub
  
```

Instructions:

- Sempre podemos modificar o ficheiro a man e logo reiniciar o servizo manualmente:

```
sudo service nslcd restart
```

- Por exemplo na liña 12 podemos poñer `uri ldap://dserv00.iescalquera.local`, reiniciariamos nslcd e xa non teriamos ldap seguro.

Comprobación con Ettercap

- Agora loca revisar se o usuario e o contrasinal viañan cifrados entre uclient01 e dserv00
- Temos activado o Ettercap en uclient02 como ao principio desta sección.

Comprobación LDAPs

Iniciamos sesión en uclient01 ...

En Ettercap, no menú View > Connections. Aquelas conexións que teñen un asterisco á esquerda son nas que o programa atopou información relevante. Neste caso imos ver a liña que ten o estado *killed*, que é onde se realizou a autenticación ...

Ettercap 0.8.2 Interface:

Connections: 172.16.5.20:44124, 172.16.5.10:636

Log output:

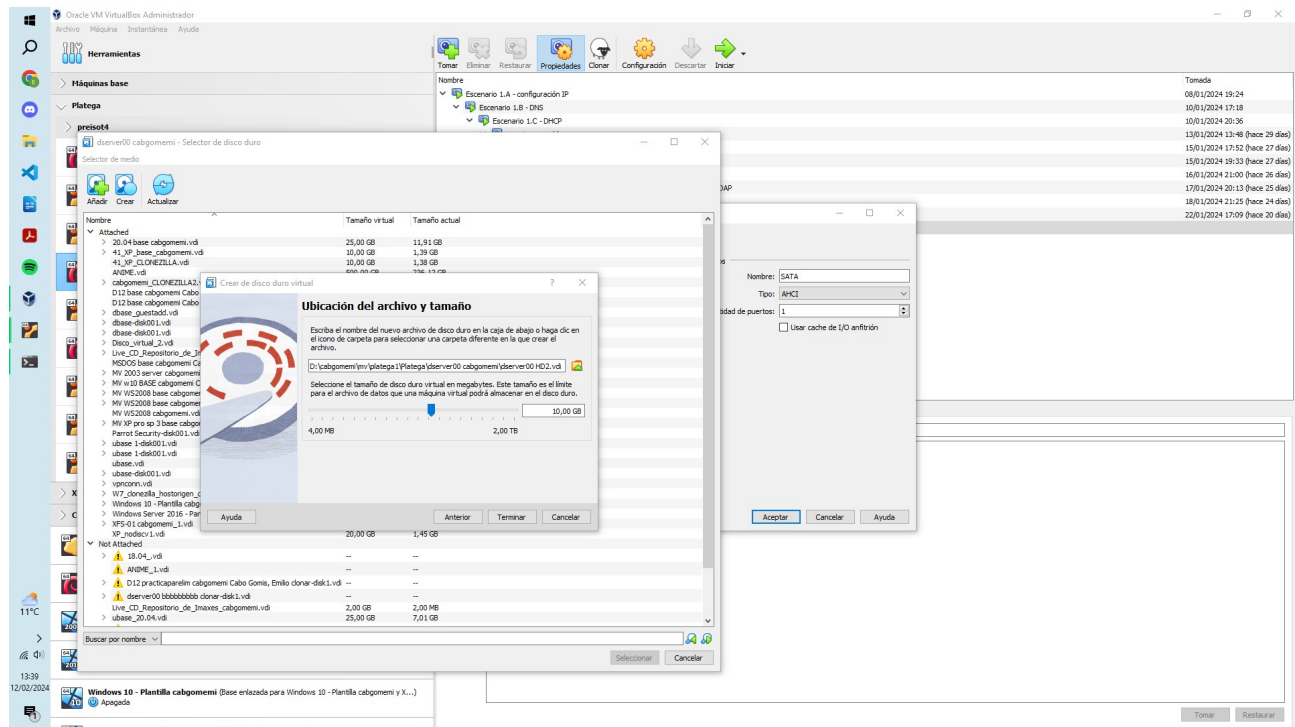
```

LDAP: 172.16.5.10:636 -> Anonymous Bind
LDAP: 172.16.5.10:636 -> Anonymous Bind
LDAP: 172.16.5.10:636 -> Anonymous Bind
LDAP: 172.16.5.10:636 -> Anonymous Bind
LDAP: 172.16.5.10:636 -> Anonymous Bind
LDAP: 172.16.5.10:636 -> Anonymous Bind
  
```

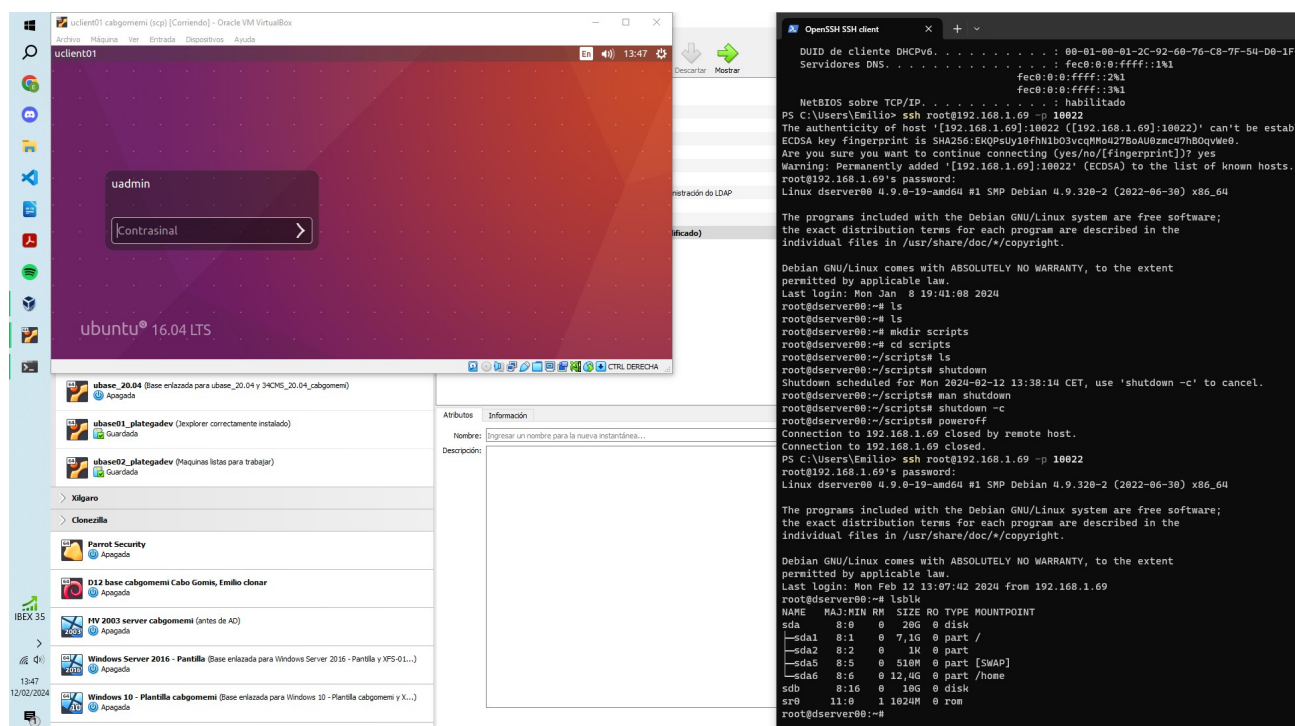
Platega III

Creación y configuración del esqueleto de la estructura de carpetas.

Añadiremos un nuevo disco a dserver00.



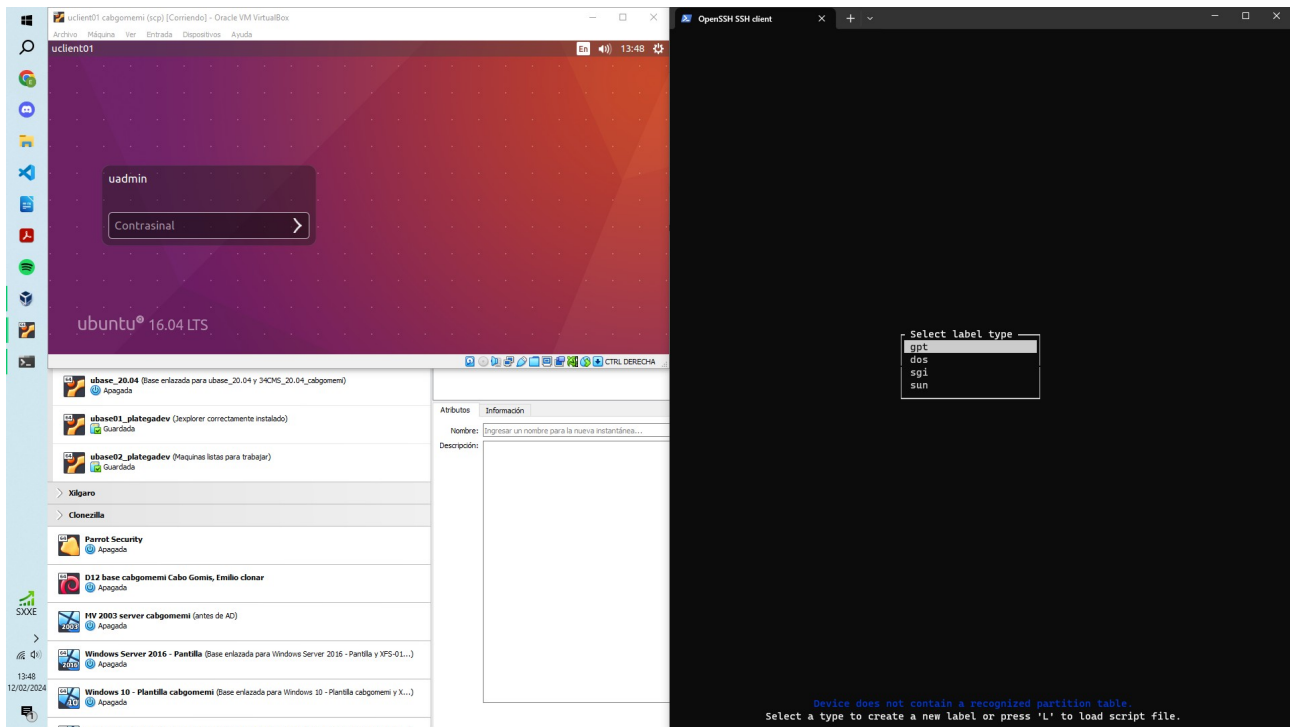
Comprobamos que el hardware es detectado.



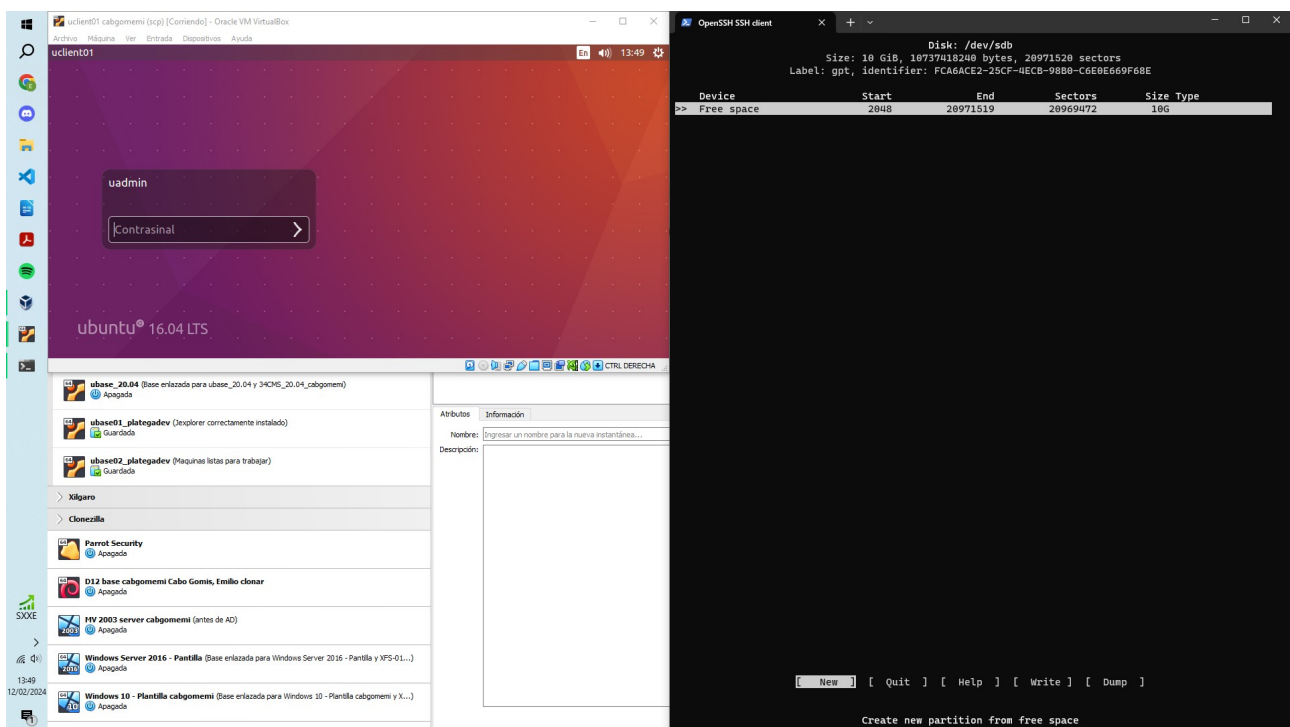
51 Platega I_II_III

Crearemos particiones y formatearemos el disco.

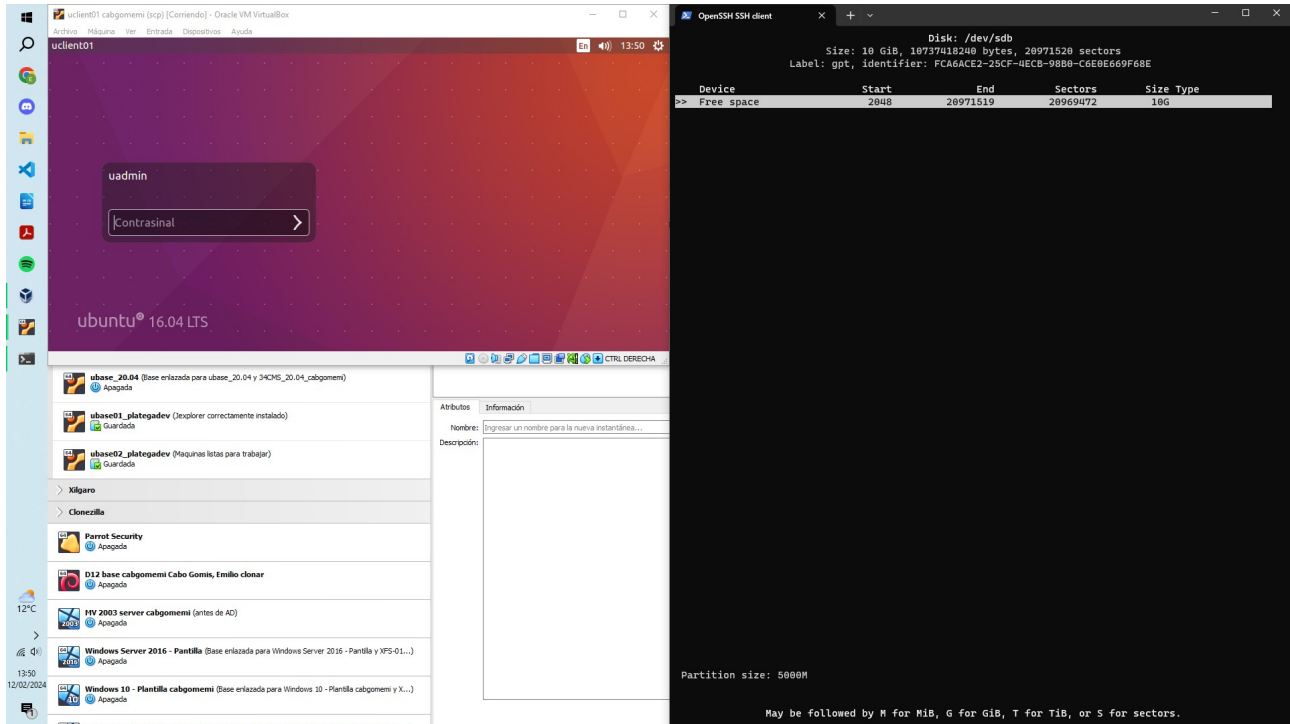
cfdisk /dev/sdb para particionar el disco.



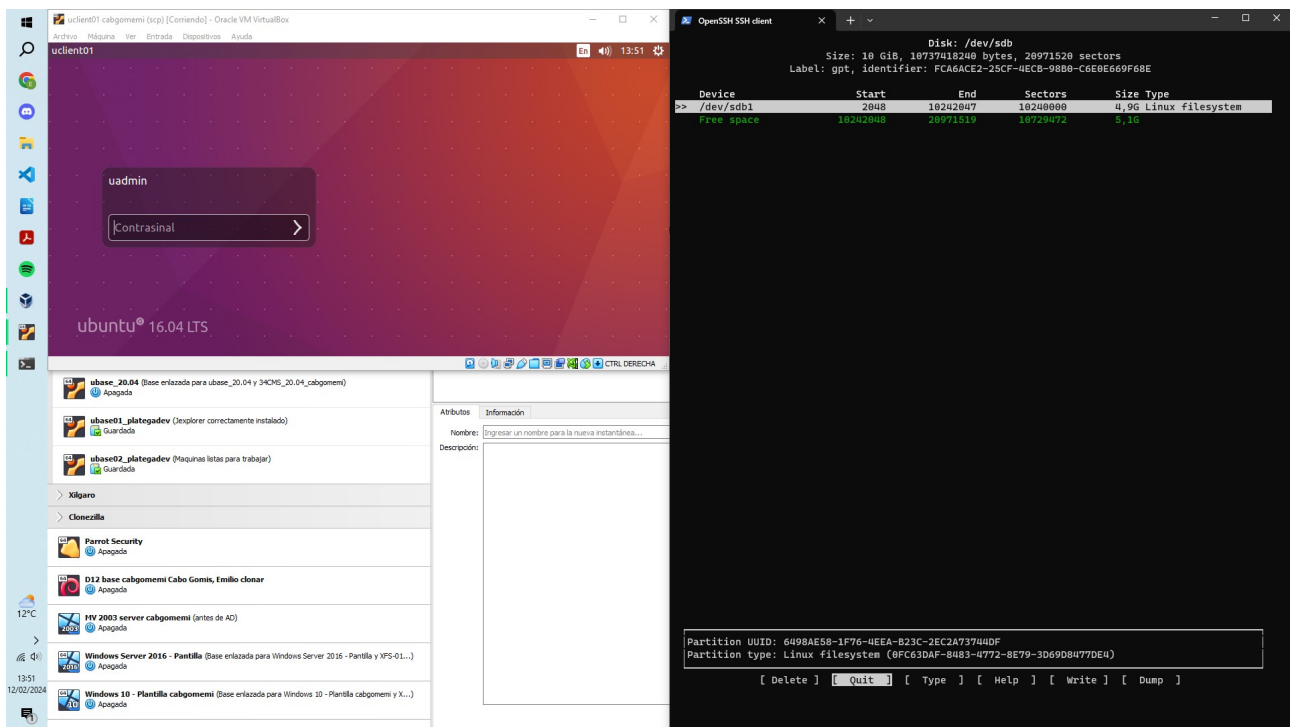
Escogemos gpt



Seleccionamos new > Primary > 5000M

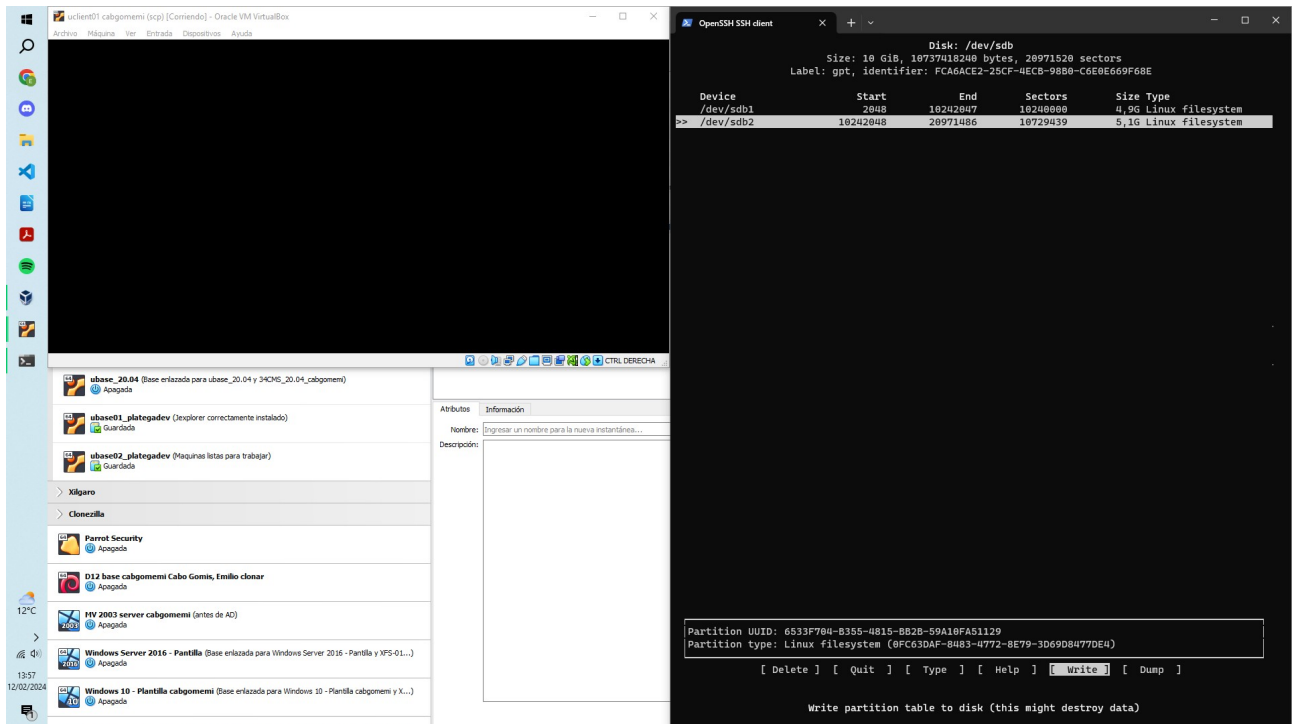


Partición creada con éxito.

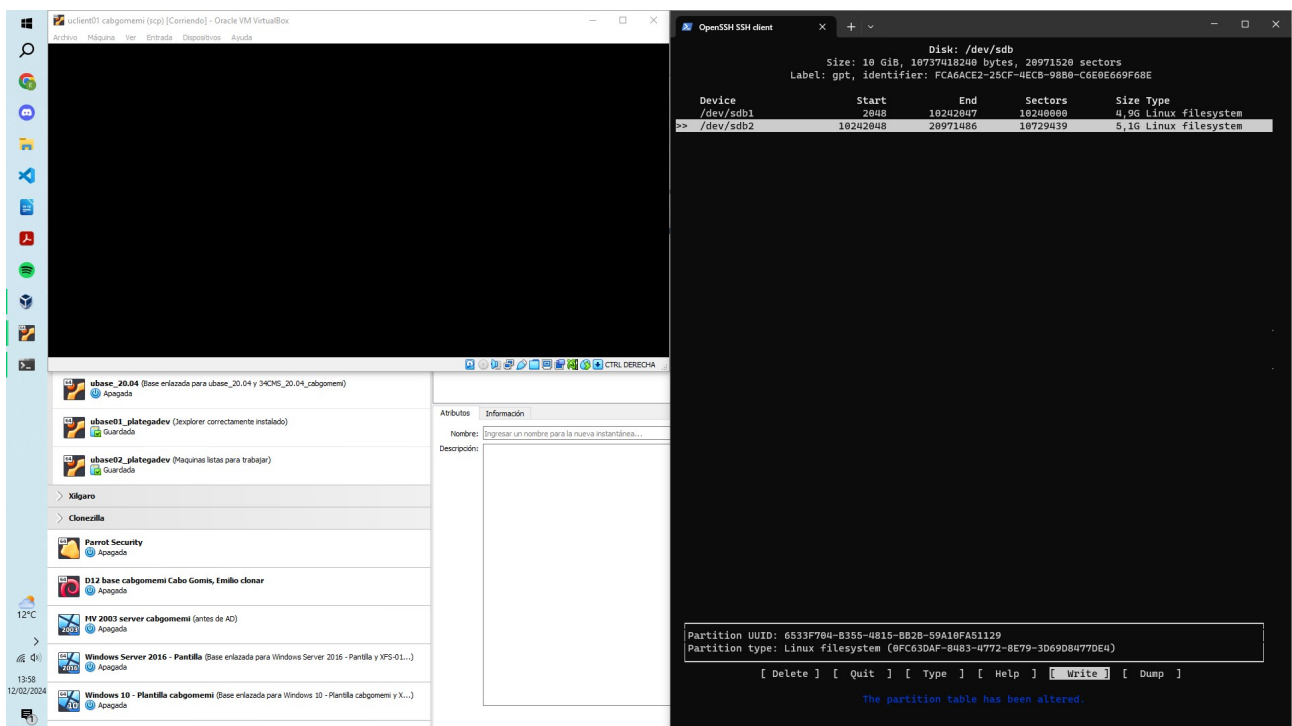


51 Platega I_II_III

Con el resto del espacio crearemos una partición /Común dónde almacenar los usuarios.

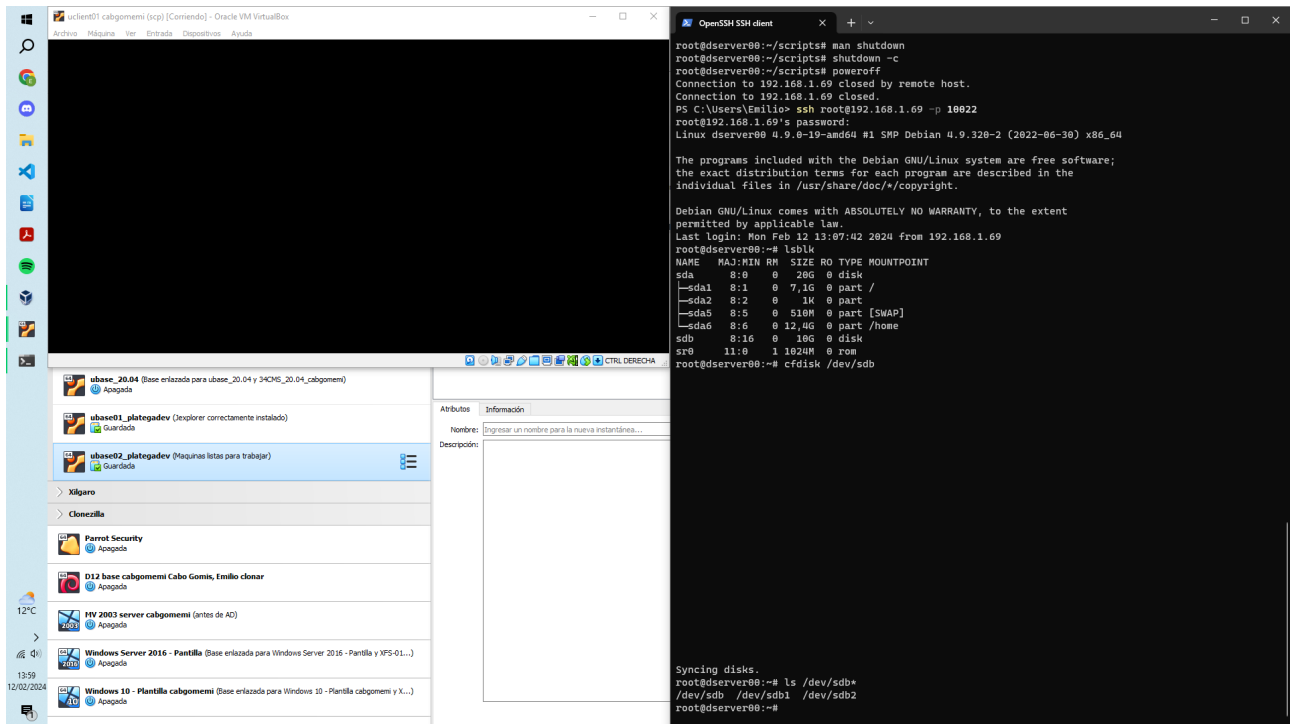


Escribimos los cambios al disco.



Checkeo de la creación de las particiones.

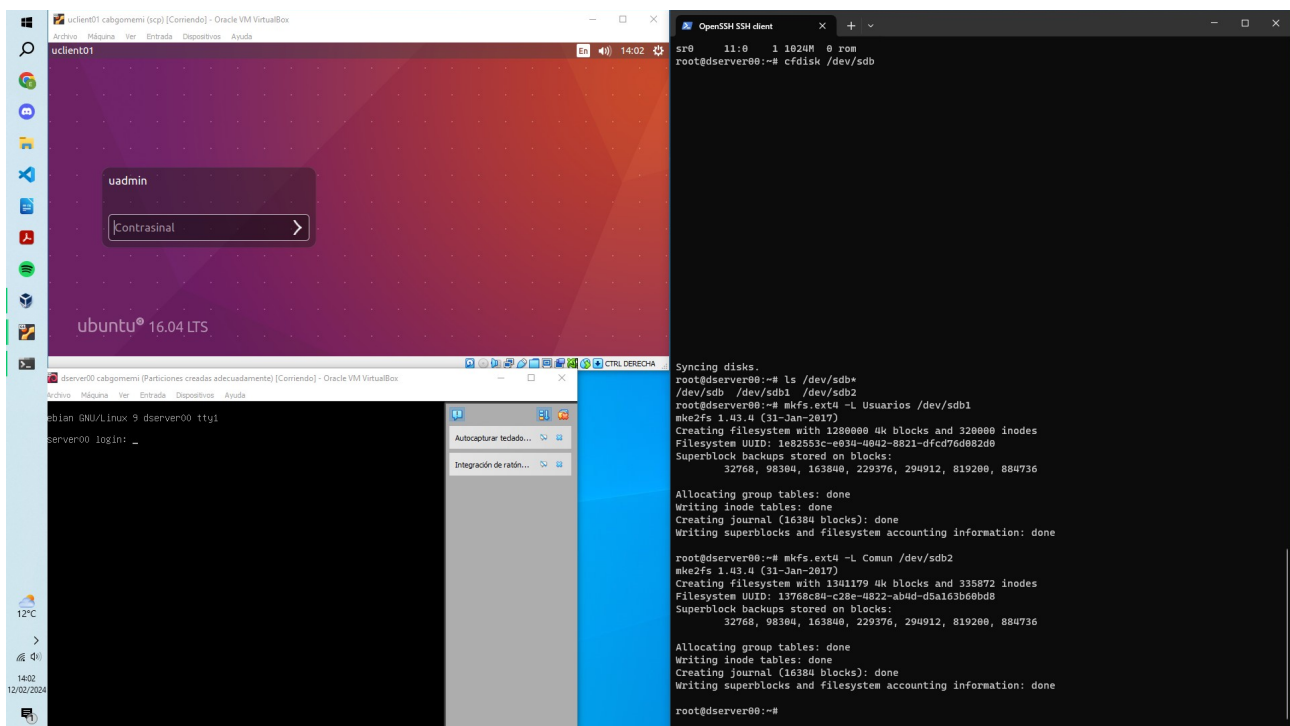
Ls /dev/sdb*



Formateado de las particiones.

mkfs.ext4 -L Usuarios /dev/sdb1

mkfs.ext4 -L Comun /dev/sdb2

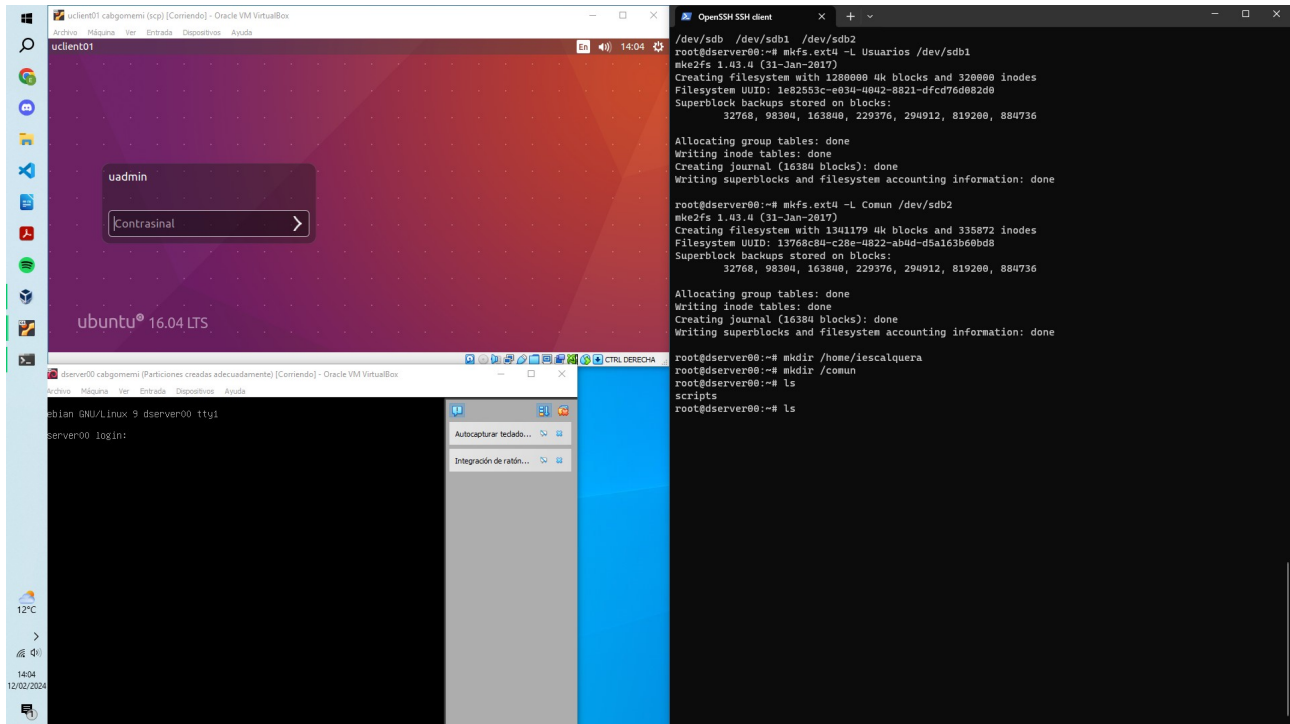


Montado de las particiones

Creamos las carpetas dónde se van a realizar los puntos de montaje.

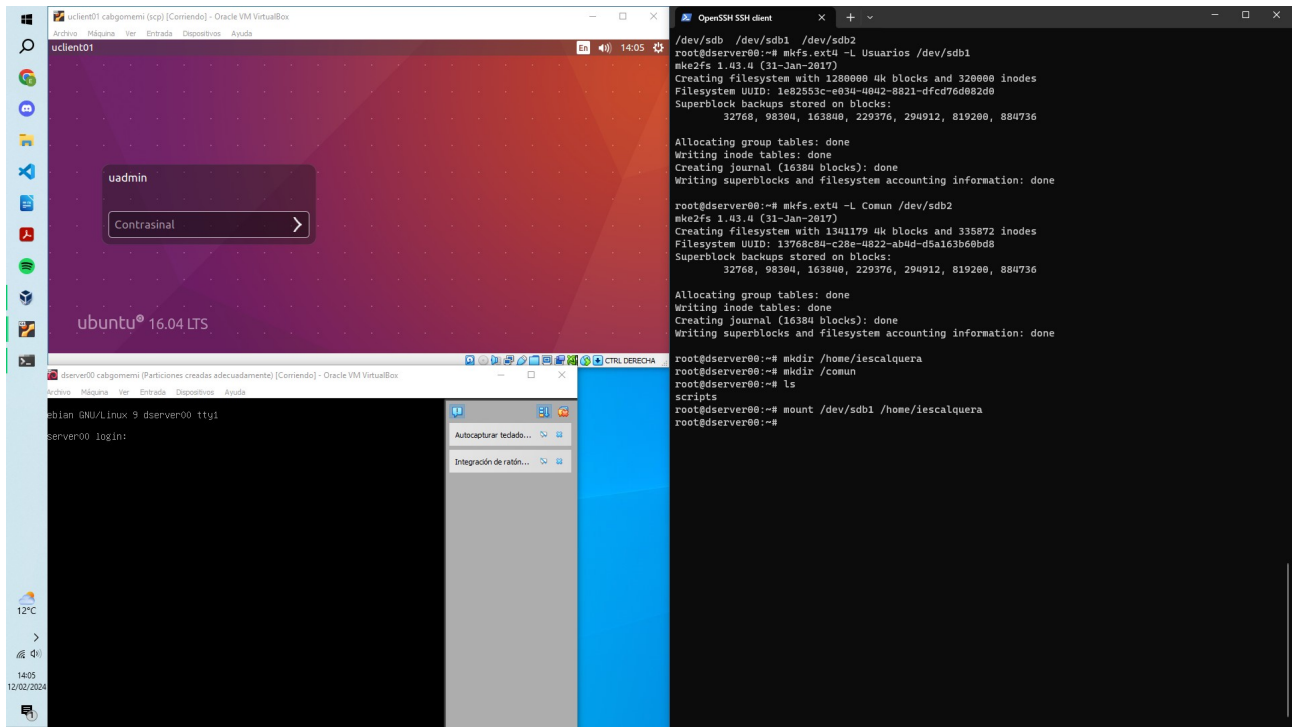
```
mkdir /home/iescalquera
```

```
mkdir /comun
```

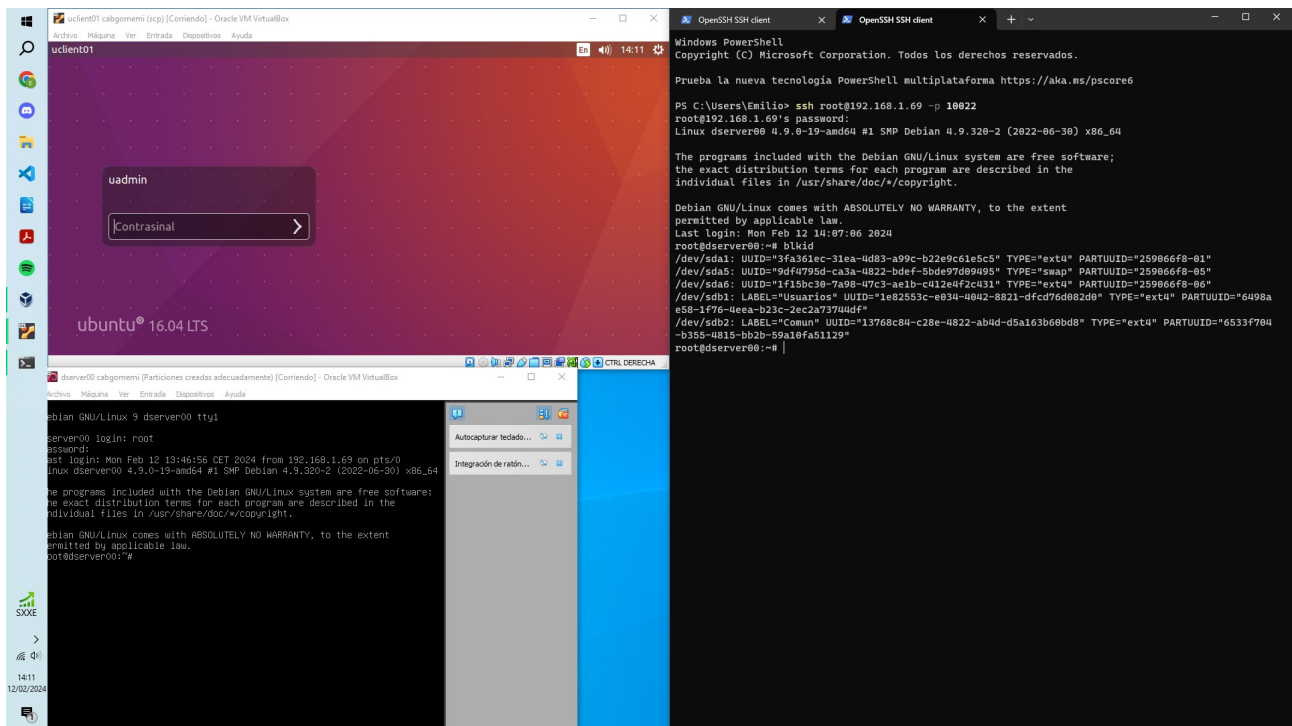


```
mount /dev/sdb1 /home/iescalquera
```

51 Platega I_II_III

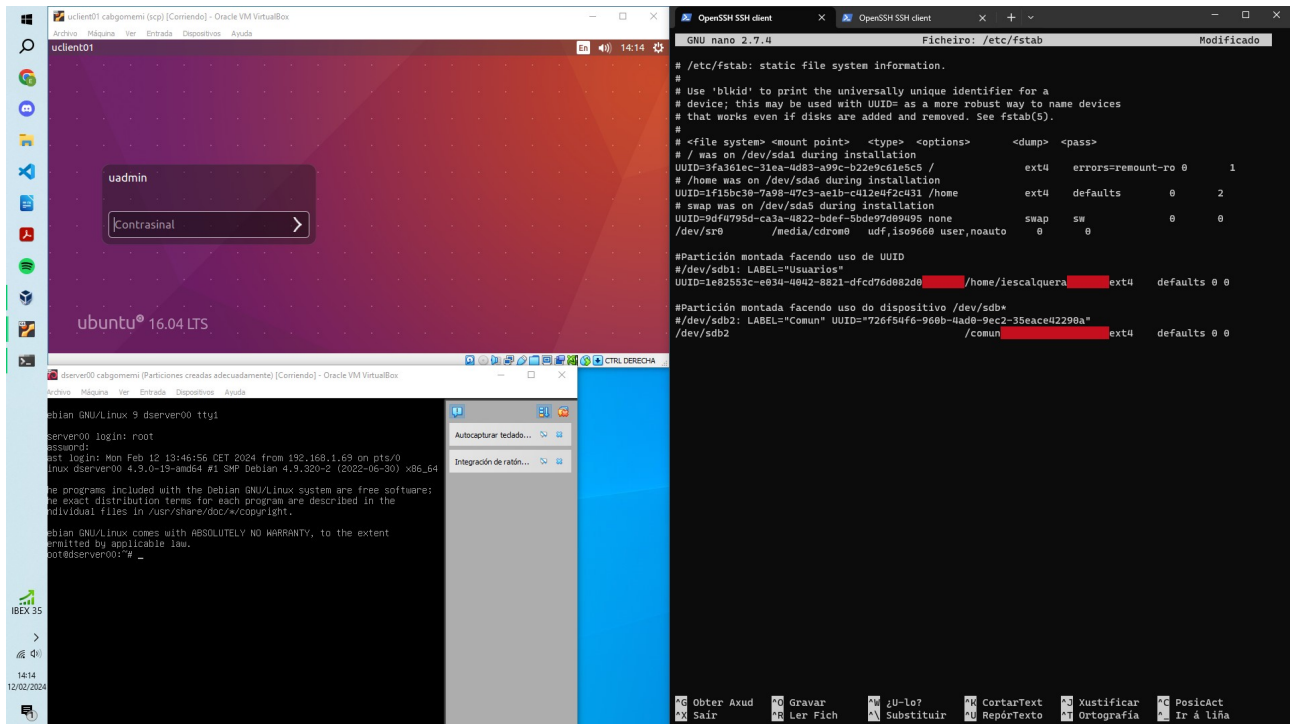


Deberemos tomar nota del UUID del dispositivo. **Blikid**

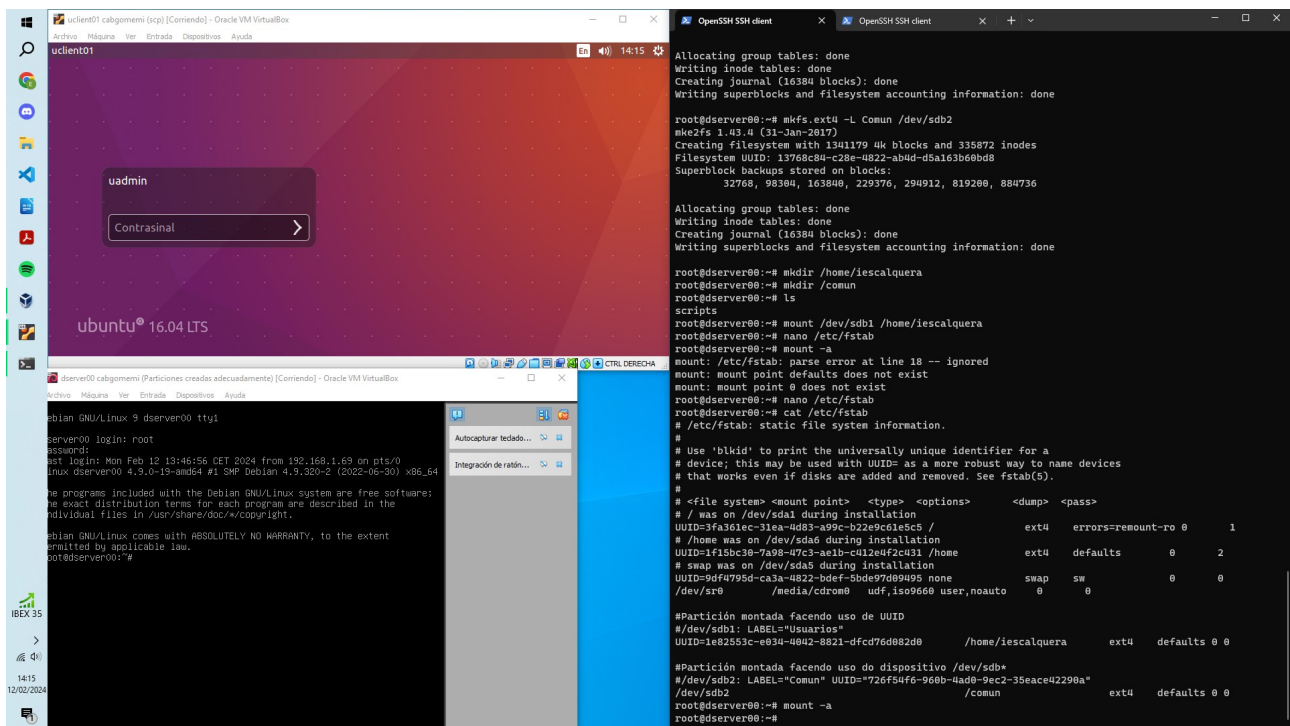


Editamos el fichero `/etc/fstab` para añadir los puntos de montaje

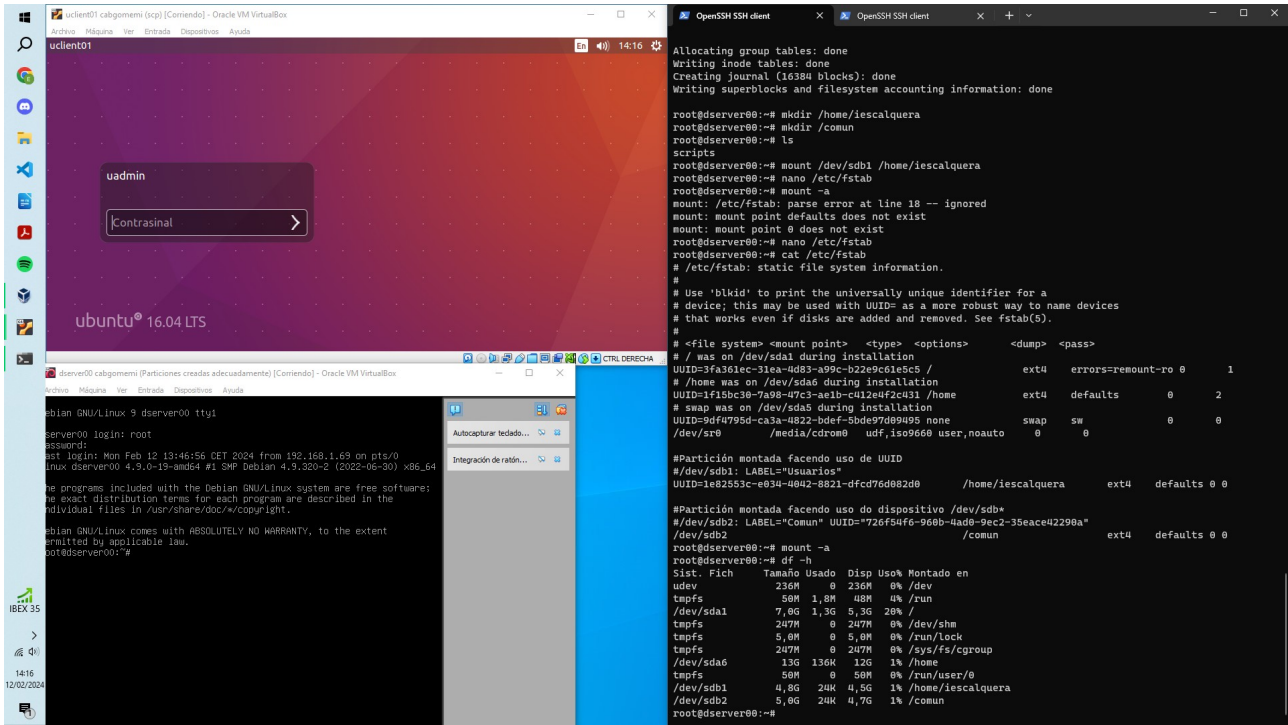
El mío tiene el siguiente contenido. **Atención tened cuidado con los UUID.**



Mediante el comando **mount -a** se lee el fichero /etc/fstab y se montan aquellos archivos que no hayan sido montados anteriormente.



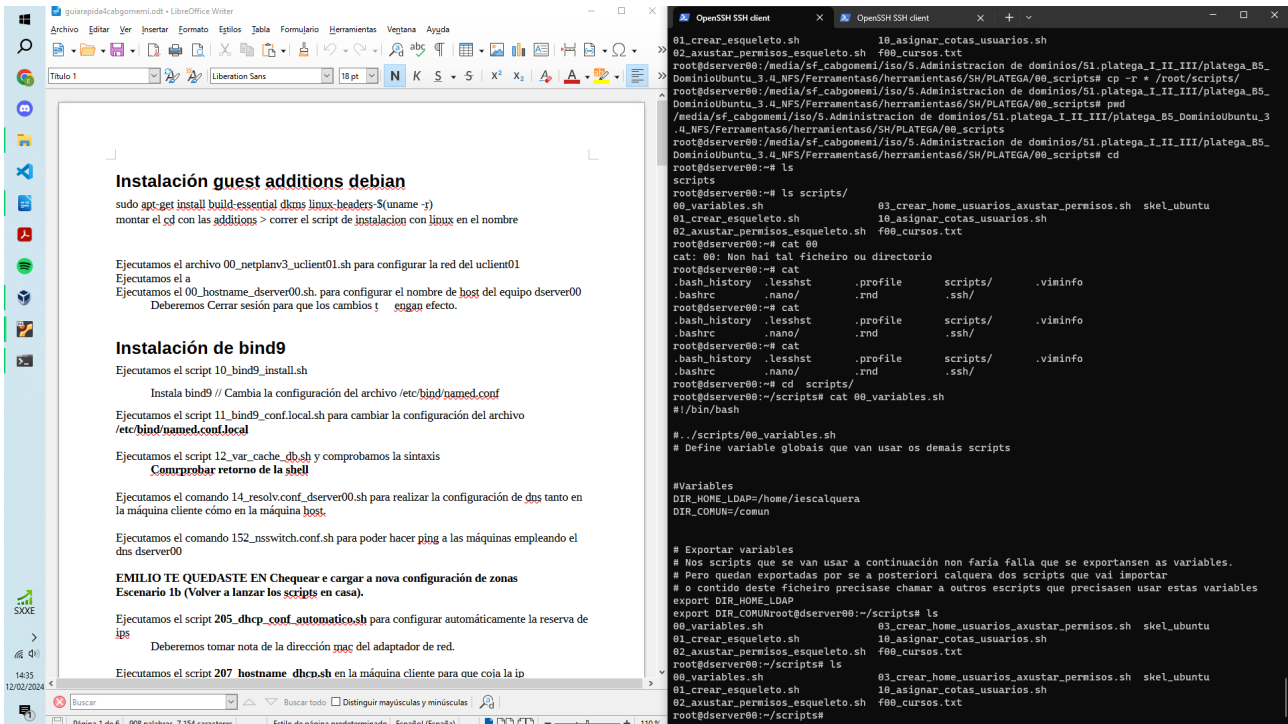
Df -h para ver las particiones sdb* montadas.



Creado del esqueleto

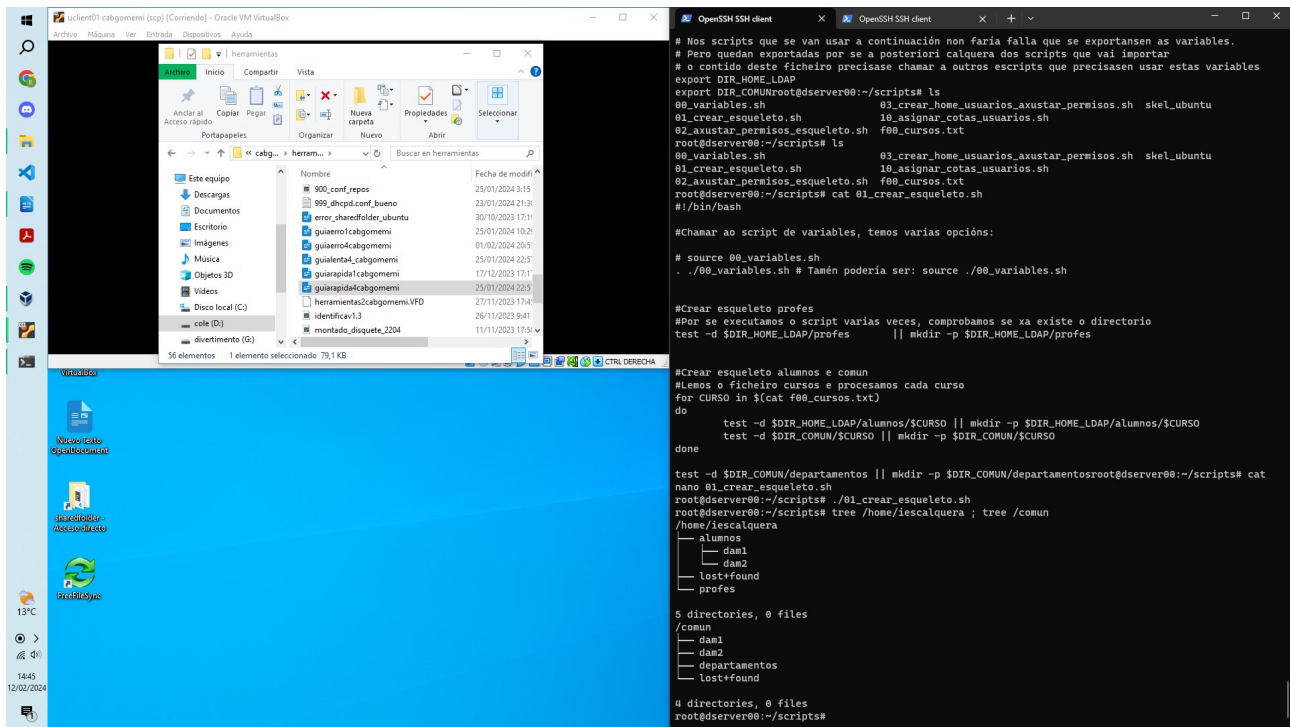
Cambiamos al directorio /root/scripts

Creamos los siguientes scripts.



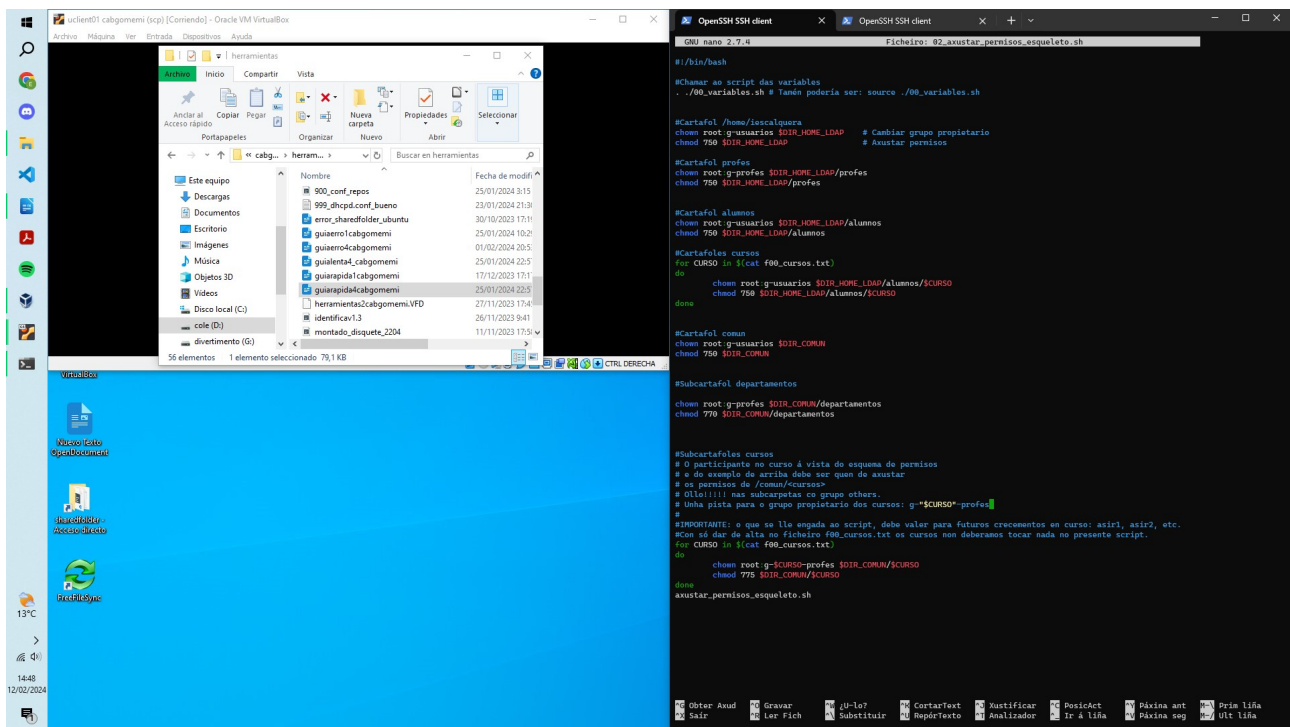
Ejecutamos el script → **01_crear_esqueleto.sh**

Comprobamos su ejecución mediante el comando → `tree /home/iescalquera ; tree /comun`

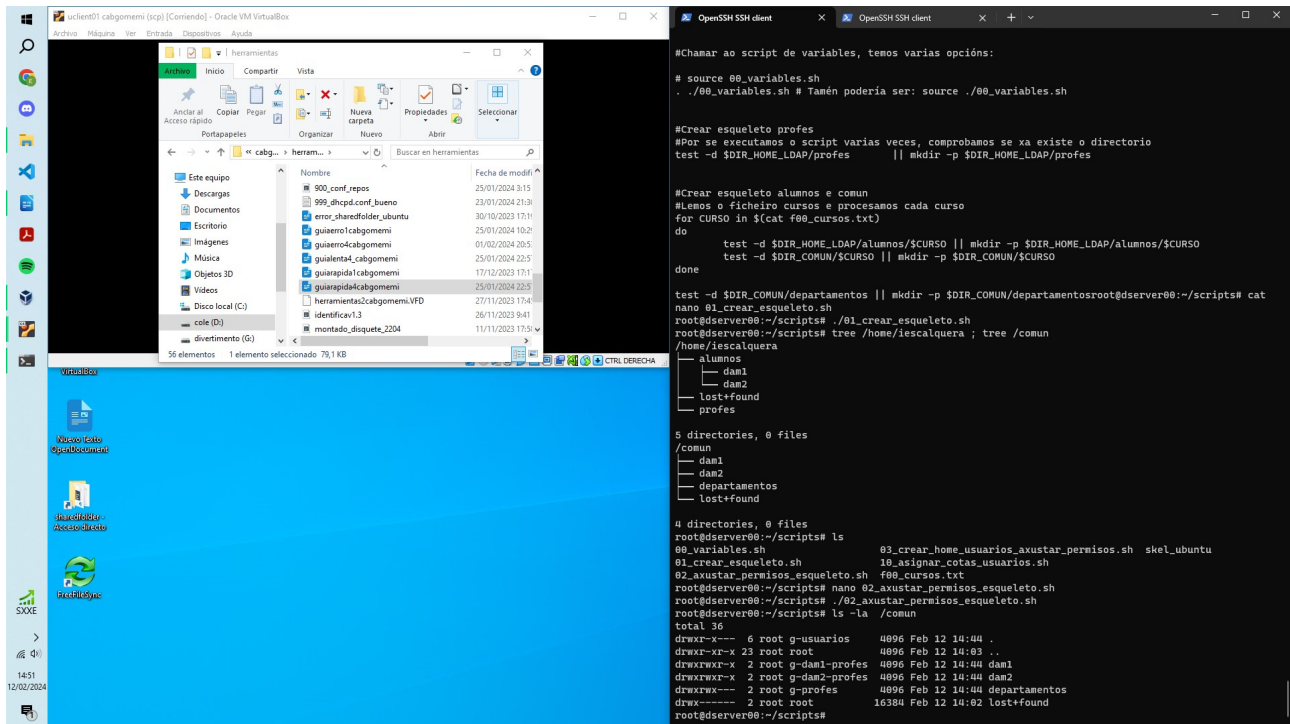


Ejecutamos el siguiente script. → **02_axustar_permisos_esqueleto.sh**

Este es el contenido que debería tener el script.



Comprobamos resultados: **ls -la /comun**



Cambiado de ruta de directorio

Deberán quedar los directorios hasta que queden de la siguiente manera.

getent passwd | tail -n 5

```
sol:x:10000:10000:Profe - Sol Lua:/home/iescalquera/profes/sol:/bin/bash
noe:x:10001:10000:Profe - Noe Ras:/home/iescalquera/profes/noe:/bin/bash
mon:x:10002:10000:DAM1 Mon Mon:/home/iescalquera/alumnos/dam1/mon:/bin/bash
tom:x:10003:10000:DAM1 Tom Tom:/home/iescalquera/alumnos/dam1/tom:/bin/bash
pia:x:10004:10000:DAM2 Pia Fdez:/home/iescalquera/alumnos/dam2/pia:/bin/bash
```

Abrimos LAM para realizar estos ajustes.

Realizaremos este ajuste en todos los usuarios hasta tenerlo todo correctamente configurado.

51 Platega I_II_III

The image shows two side-by-side screenshots. The left screenshot is a web browser displaying a manual for LDAP configuration. The right screenshot shows the LDAP Account Manager web interface.

Manual Content:

- Diagrama de estructura de usuarios:

```

graph TD
    profesores --> sol
    profesores --> noe
    profesores --> dam1
    profesores --> dam2
    profesores --> departamentos
    alumnos --> mon
    alumnos --> tom
    alumnos --> pia
    alumnos --> piaz

```

- Pero se nos fixamos no que temos no ldap, para os nosos usuarios indicase que as carpetas persoais deberan estar en `/home`
- getent passwd | tail -n 5
- Pero `/home` non vai ser o cartafol que valiamos exportar á rede (compartir) senón `/home/iescalquera`.
- E dentro de `/home/iescalquera` a carpeta de cada usuario está nun directorio en función do curso/grupo ao que pertence.
- Agora temos que cambiar no ldap a ruta aos cartafoles home de cada usuario.
- O aconsellable é no momento de dar de alta o usuario indicarlle cal é a ruta correcta á súa carpeta persoal.
- IMPORTANTE: Agora por calquera dos métodos (consola, LAM, JXplorer) cambiamos o home de cada usuario, con moito tempo, para facelo ben á primeira. Para que quede así:
- getent passwd | tail -n 5
- Fixase ben que cada quen ten o cartafol onde lle corresponde, porque senón logo van fallar os scripts de creación das súas carpetas persoais e de anuste de permisos.
- Se por exemplo se fixera a creación dos usuarios con LAM e se usa unha folia de cálculo para crear o ficheiro CSV, o ideal é usar unhas columnas base (nome, apelidos, grupo, etc) para construír as outras columnas (OUs, home, anupos, etc) coa función das follas de cálculo concatenar. Logo importárase como

LDAP Account Manager Interface:

- LDAP Account Manager (localhost:389) - Mozilla Firefox
- LDAP Account Manager - 5.5 (Logged in as: admin > iescalquera > local)
- Users Groups Hosts
- Save Reset changes Set password default Load profile
- LibreOffice Impress Suffix dam1 > alum > usuarios > iescalquera > loca RDN identifier uid
- mon@iescalquera.local
- Personal User name mon Common name DAM1 - Mon Mon UID number 10002 Gecos DAM1 Mon Mon Primary group g-usuarios Additional groups Edit groups Home directory /home/iescalquera/alumnos/dam1/mon Login shell /bin/bash Password Lock password Remove password

Una vez realizados correctamente todos los ajustes deberán quedar así.

The image shows two side-by-side screenshots. The left screenshot is a file explorer window showing the directory structure. The right screenshot is a terminal window showing the execution of scripts to create the LDAP structure.

File Explorer Content:

- herramientas
- Este equipo
- Descargas
- Documentos
- Escritorio
- Imágenes
- Música
- Objetos 3D
- Videos
- Disco local (C:)
- cole (D:)
- divertimento (G:)
- 56 elementos 1 elemento seleccionado 79,1 KB

Terminal Content:

```

#Crear esqueleto alumnos e comun
#Lemos o ficheiro cursos e procesamos cada curso
for CURSO in $(cat f08_cursos.txt)
do
    test -d $DIR_HOME_LDAP/alumnos/$CURSO || mkdir -p $DIR_HOME_LDAP/alumnos/$CURSO
    test -d $DIR_COMUN/$CURSO || mkdir -p $DIR_COMUN/$CURSO
done

test -d $DIR_COMUN/departamentos || mkdir -p $DIR_COMUN/departamentosroot@server00:~/scripts# cat
nano 01_crear_esqueleto.sh
root@server00:~/scripts# ./01_crear_esqueleto.sh
root@server00:~/scripts# tree /home/iescalquera ; tree /comun
/home/iescalquera
├── alumnos
│   ├── dam1
│   ├── dam2
│   └── lost+found
└── profes

5 directories, 0 files
/comun
├── dam1
├── dam2
├── departamentos
└── lost+found

4 directories, 0 files
root@server00:~/scripts# ls
00_variables.sh                                03_crear_home_usuarios_axustar_permisos.sh  skel_ubuntu
01_crear_esqueleto.sh                          10_asignar_cotas_usuarios.sh
02_axustar_permisos_esqueleto.sh                f08_cursos.txt
root@server00:~/scripts# nano 02_axustar_permisos_esqueleto.sh
root@server00:~/scripts# ./02_axustar_permisos_esqueleto.sh
root@server00:~/scripts# ls -la /comun
total 36
drwxr-xr-x  6 root g-usuarios 4096 Feb 12 14:44 .
drwxr-xr-x 23 root root        4096 Feb 12 14:03 ..
drwxrwxr-x  2 root g-dam1-profes 4096 Feb 12 14:44 dam1
drwxrwxr-x  2 root g-dam2-profes 4096 Feb 12 14:44 dam2
drwxrwxr-x  2 root g-profes      4096 Feb 12 14:44 departamentos
drwx----- 2 root root        16384 Feb 12 14:02 lost+found
root@server00:~/scripts# getent passwd | tail -n 5
sol:x:10000:10000:Profe - Sol Lua:/home/sol:/bin/bash
noe:x:10001:10000:Profe - Noe Ras:/home/noe:/bin/bash
mon:x:10002:10000:DAM1 Mon Mon:/home/mon:/bin/bash
tom:x:10003:10000:DAM1 Tom Tom:/home/tom:/bin/bash
pia:x:10004:10000:DAM2 Pia Glez:/home/pia:/bin/bash
root@server00:~/scripts# getent passwd | tail -n 5
sol:x:10000:10000:Profe - Sol Lua:/home/iescalquera/profes/sol:/bin/bash
noe:x:10001:10000:Profe - Noe Ras:/home/iescalquera/profes/noe:/bin/bash
mon:x:10002:10000:DAM1 Mon Mon:/home/iescalquera/alumnos/dam1/mon:/bin/bash
tom:x:10003:10000:DAM1 Tom Tom:/home/iescalquera/alumnos/dam1/tom:/bin/bash
pia:x:10004:10000:DAM2 Pia Glez:/home/iescalquera/alumnos/dam2/pia:/bin/bash
root@server00:~/scripts#

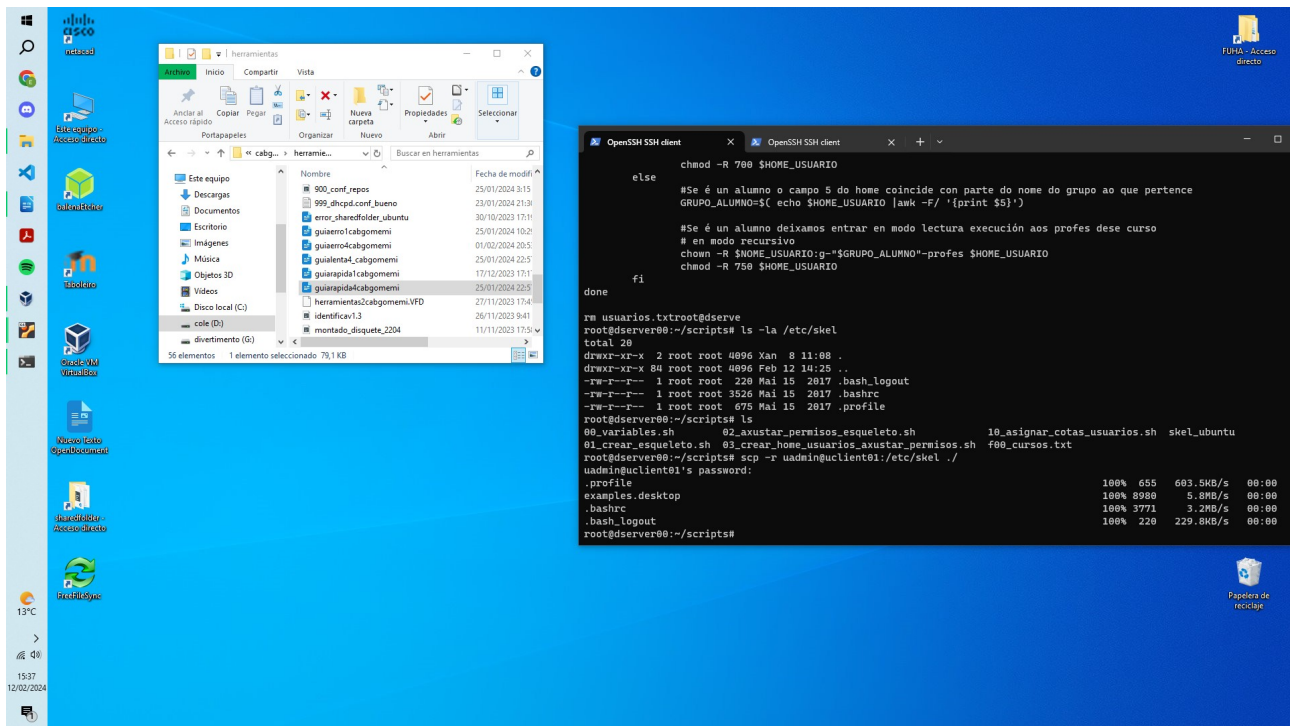
```


Copiado del /etc/skel ./

Para comprobar el contenido de este directorio ejecutamos el comando `ls -la /etc/skel`

Ahora copiaremos el contenido del directorio el el cliente uclient01 mediante el comando

`scp -r uadmin@uclient01:/etc/skel ./`

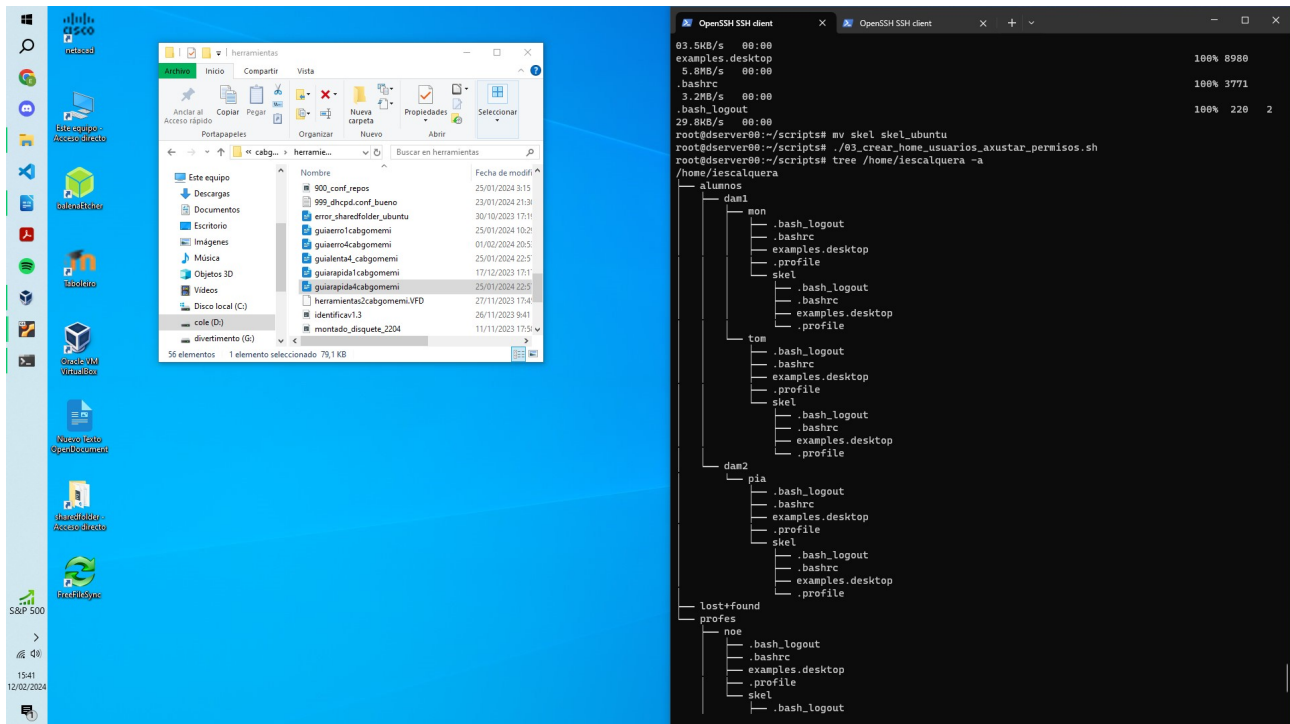


Lo renombramos mediante el comando `mv skel skel_ubuntu`

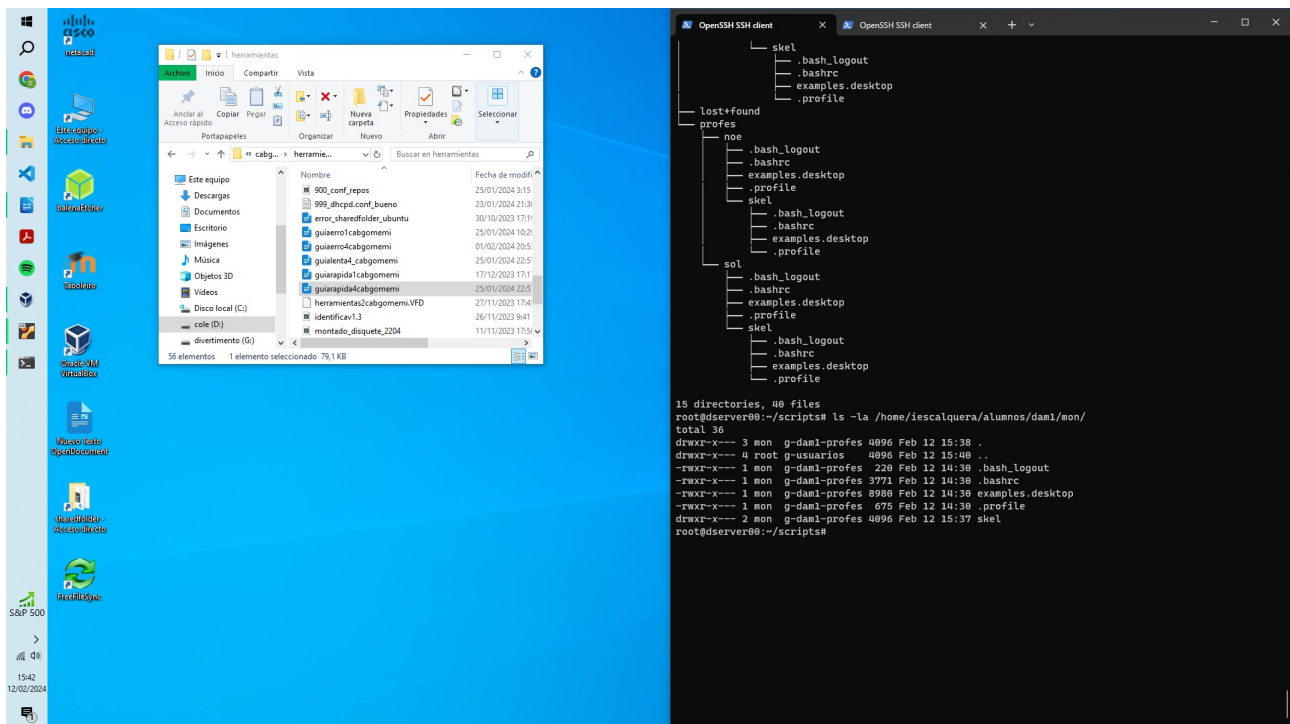
Ejecutamos el script `03_crear_home_usuarios_axustar_permisos.sh`

Realizamos la comprobación de la ejecución del script mediante el comando `tree /home/iescalquera -a`

51 Platega I_II_III

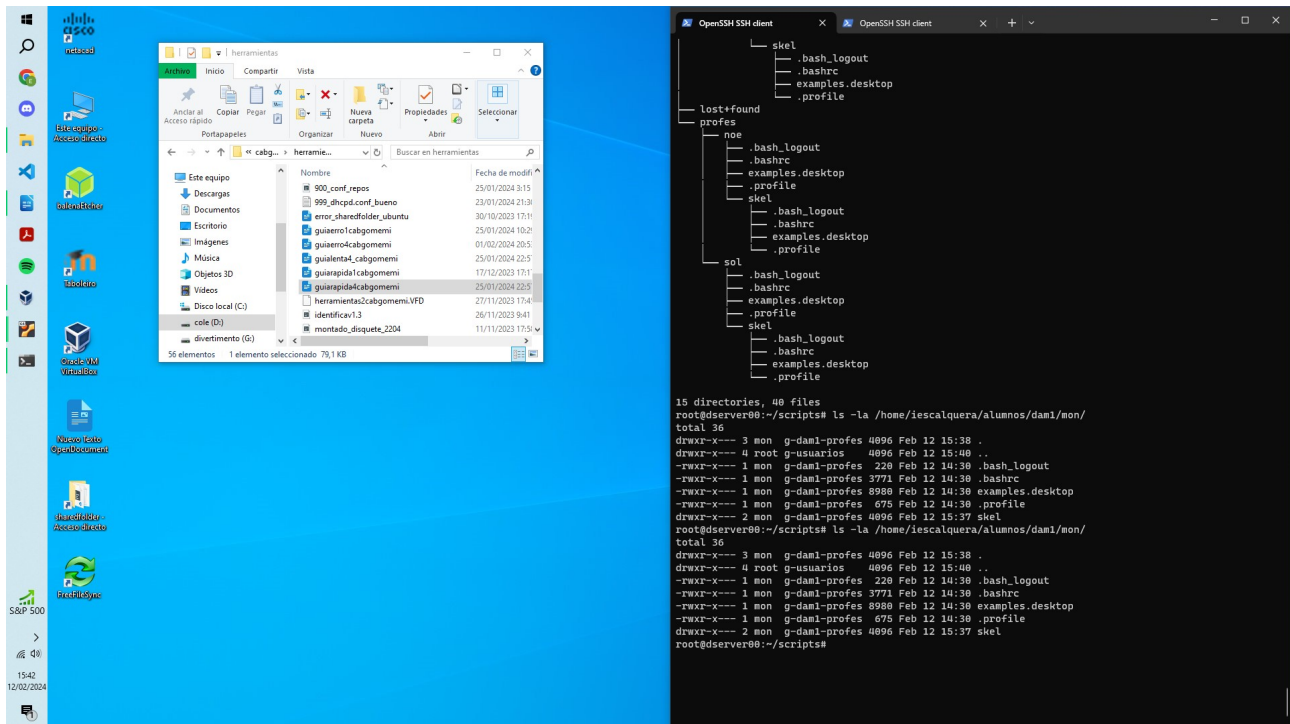


ls -la /home/iescalquera/alumnos/dam1/mon/



ls -la /home/iescalquera/alumnos/dam1/mon/

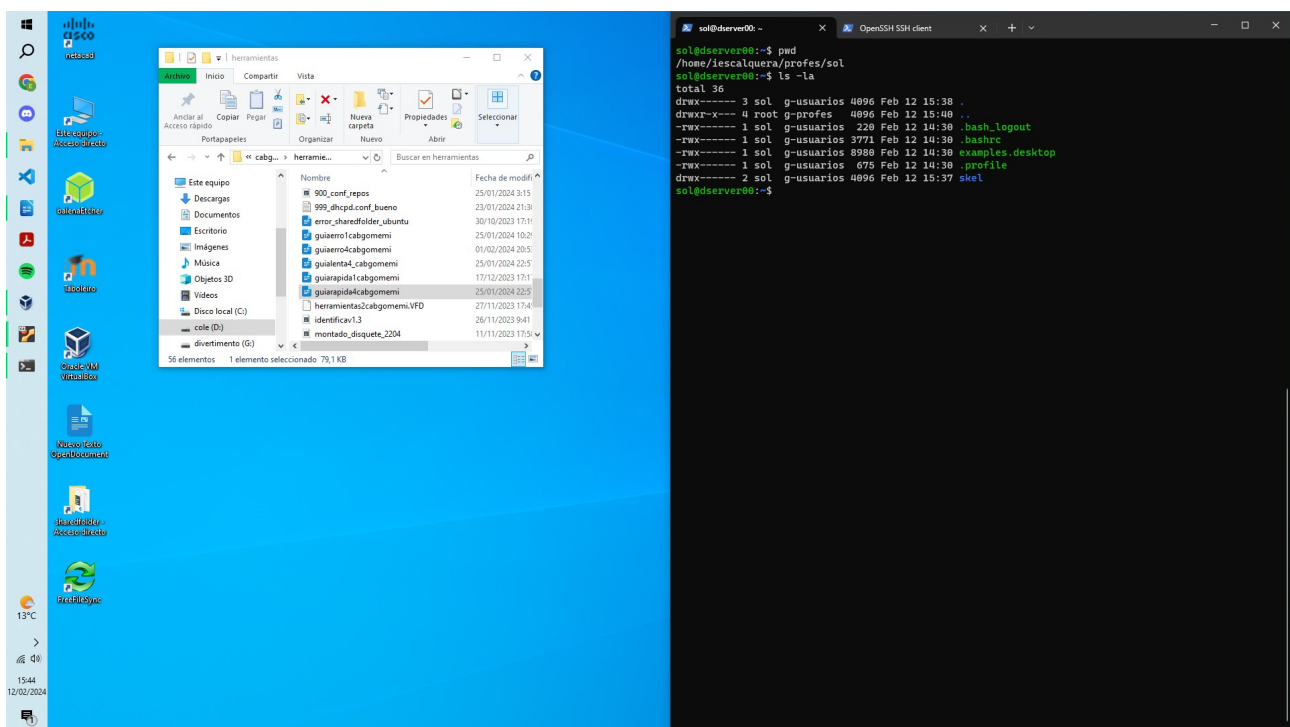
51 Platega I_II_III



iniciamos sesión como sol y comprobamos los ficheros que se encuentran en su disrectorio.

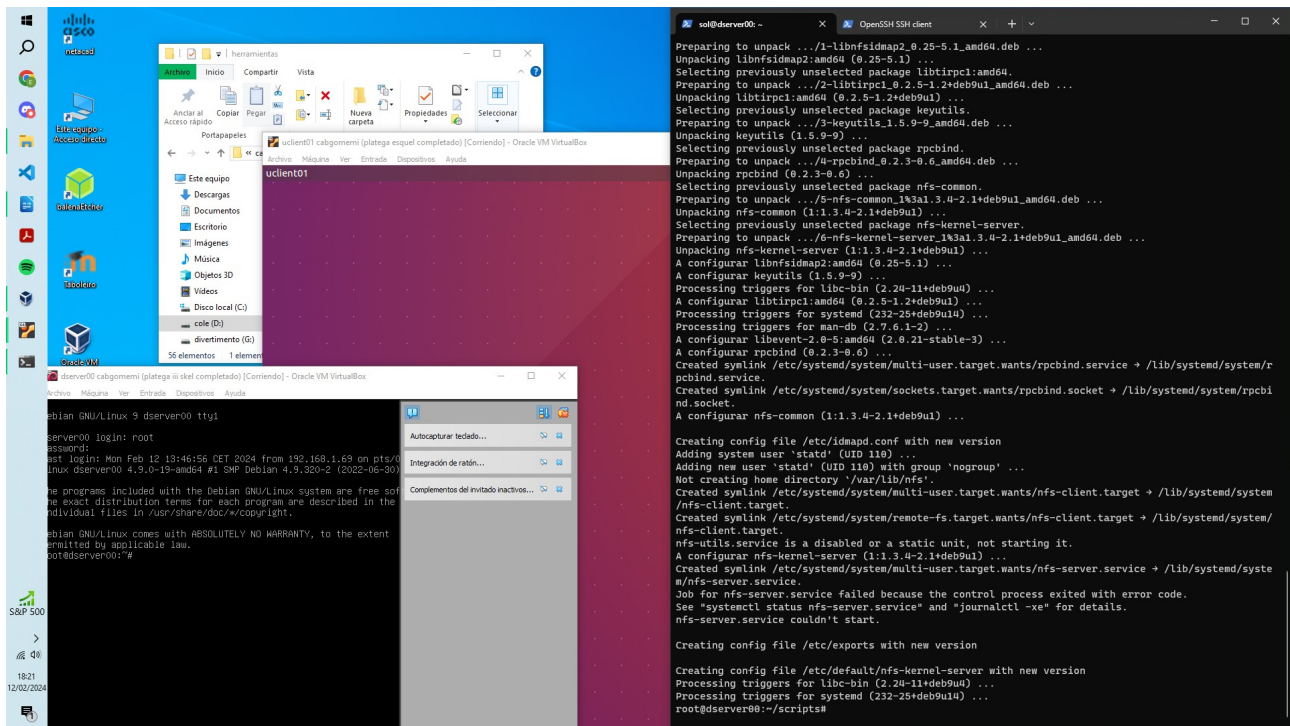
Pwd

ls -la



Instalación del servidor NFS. Exportaciones

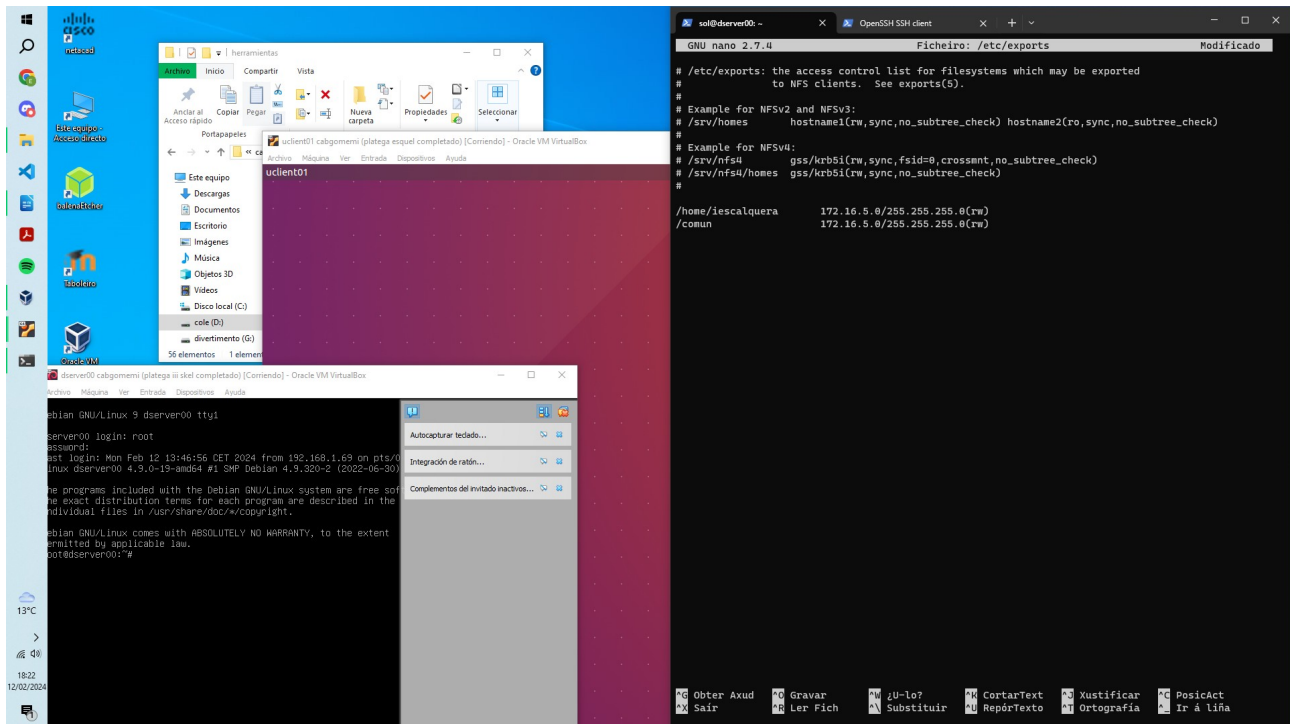
Instalamos el paquete de servidor nfs mediante el comando **apt-get install nfs-kernel-server -y**



Editamos el archivo `/etc/exports` y añadimos las siguientes líneas.

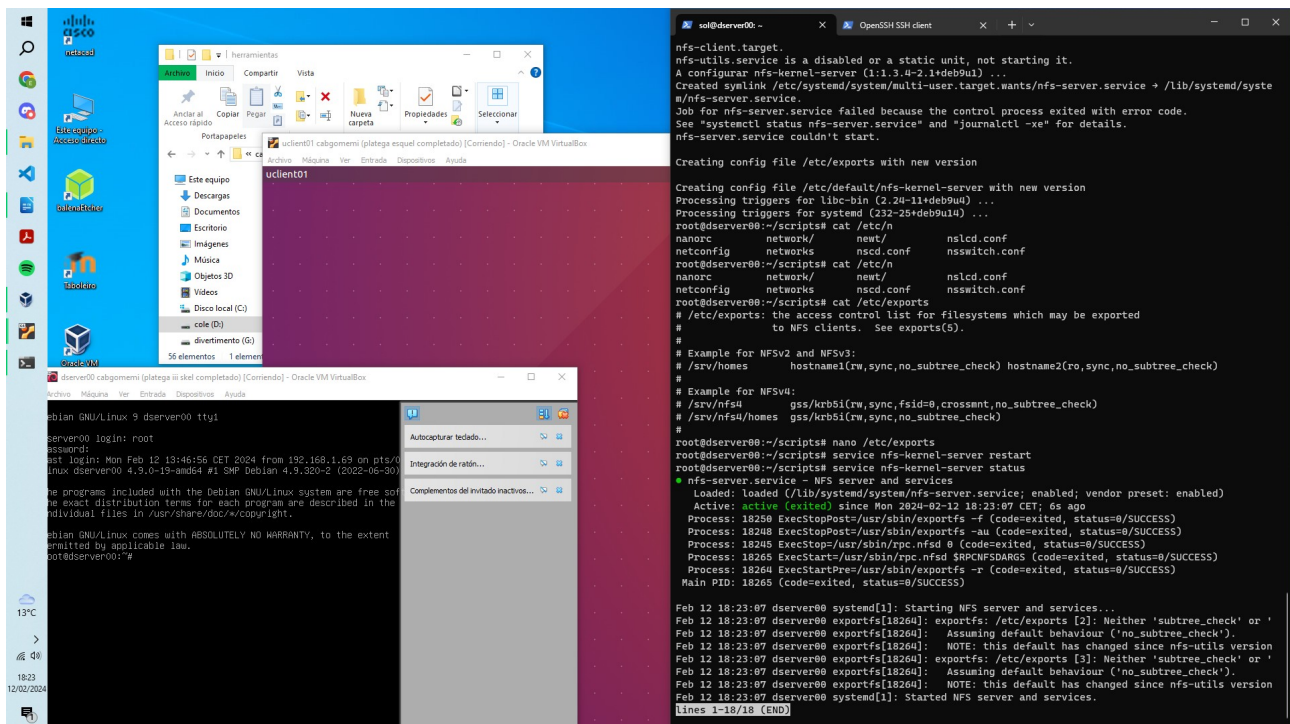
`/home/iescalquera 172.16.5.0/255.255.255.0(rw)`

`/comun 172.16.5.0/255.255.255.0(rw)`



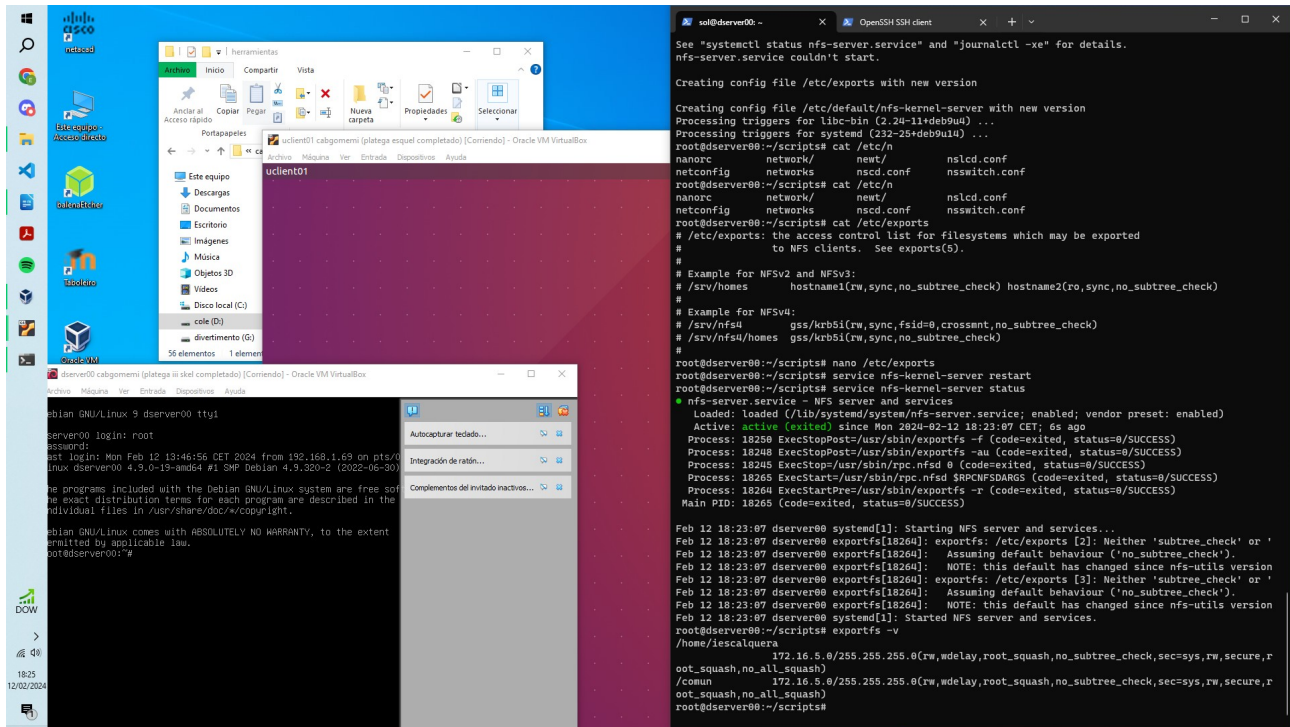
Reiniciamos el servicio

service nfs-kernel-server restart



Comprobamos lo que está exportando el servidor.

Exportfs -v



PLATEGA IV Cuotas de disco y copias de seguridad