

INFRAESTRUCTURA DEL SISTEMA INFORMÀTIC DE L'EDT

BRYAN ALVITRES

ÍNDEX

- **INTRODUCCIÓ**
- **SAMBA-SERVER**
 - Instal·lació de paquets
 - Configuració de IP estàtica
 - Configuracions del sistema
 - Configuració de la sincronització de temps
 - Verificacions i altres comandes
- **WIN-CLIE1_2**
 - Configuració de IP estàtica
 - Connexió al workgroup i comprovacions
- **UBUN-CLIE**
 - Instal·lació de paquets
 - Configuració de IP estàtica
 - Configuració i accés al domini EDT.ORG
 - Unió al domini EDT.ORG
 - Altres configuracions i comprovacions
- **RECURSOS COMPARTITS**
- **CONCLUSIÓ**



INTRODUCCIÓ

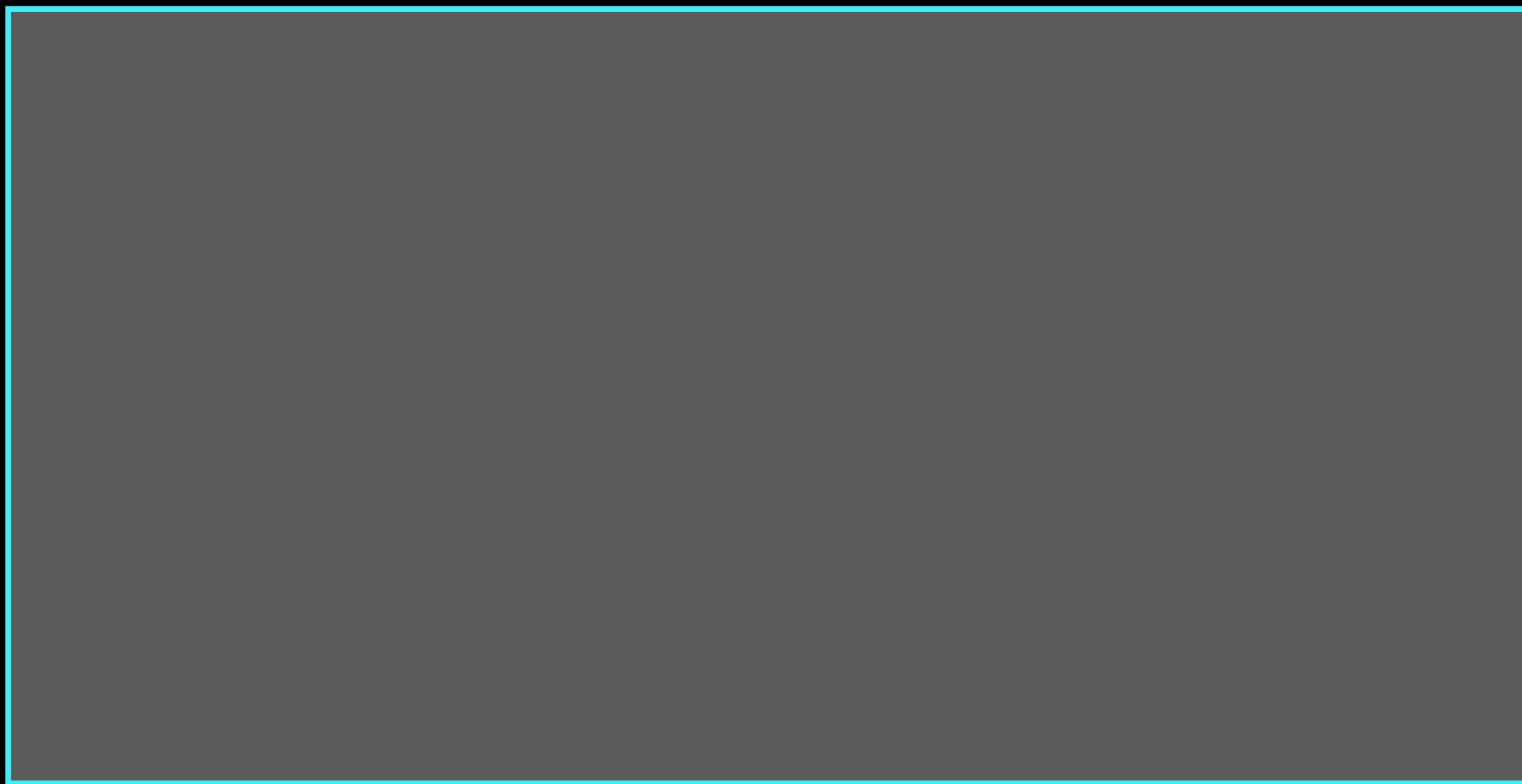
INTRODUCCIÓ



El nostre projecte trimestral té com a objectiu principal la creació d'una infraestructura informàtica de l'Escola del Treball de Barcelona (edt.org). Desenvolupat dins del mòdul M14 d'ASIX aquest projecte abasta una àmplia gamma de coneixements i habilitats clau per a la gestió avançada de sistemes informàtics.

- Implementació de tecnologies com SAMBA-4-AD i FreeIPA per a la integració de sistemes heterogenis i gestió d'identitats.
- Exploració de conceptes avançats com federació d'identitats i delegació de dominis per a millorar l'escalabilitat i flexibilitat del projecte.

VÍDEO RESUM





SAMBA-SERVER

SAMBA-SERVER



imatge ISO: ubuntu-24.04-live-server-amd64.iso

- Adapter1: NAT
- Adapter2: Xarxa Interna
- Adapter3: Adaptador de Pont
- Memoria RAM: 2040 ram
- Processadors: 4 cpus
- Usuari: administrador
- Contrasenya: admin

The image displays three separate windows, each showing the configuration for Adapter 1 of a network adapter. The top window shows Adapter 1 attached to 'NAT'. The middle window shows Adapter 1 attached to 'Internal Network' with the name 'intnet'. The bottom window shows Adapter 1 attached to 'Bridged Adapter' with the name 'Realtek Gaming GbE Family Controller'.

Network

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Enable Network Adapter

Attached to: NAT

Network

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Enable Network Adapter

Attached to: Internal Network

Name: intnet

Network

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek Gaming GbE Family Controller

Instal·lació de paquets



- apt-get update
- apt-get install -y vim acl attr samba samba-dsdb-modules
samba-vfs-modules smbclient winbind libpam-winbind
libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils
chrony net-tools

Configurando la autenticación de Kerberos

Cuando los usuarios intentan usar Kerberos y especifican un nombre principal o de usuario sin aclarar a qué dominio administrativo de Kerberos pertenece el principal, el sistema toma el reino predeterminado. El reino predeterminado también se puede utilizar como el reino de un servicio de Kerberos que se ejecute en la máquina local. Normalmente, el reino predeterminado es el nombre en mayúsculas del dominio del DNS local.

Reino predeterminado de la versión 5 de Kerberos:

EDT.ORG

Configurando la autenticación de Kerberos

Introduzca los nombres de los servidores Kerberos en el reino EDT.ORG de Kerberos, separados por espacios.

Servidores de Kerberos para su reino:

sambac.edt.org

Configurando la autenticación de Kerberos

Introduzca el nombre del servidor administrativo (cambio de contraseña) para el reino EDT.ORG de Kerberos.

Servidor administrativo para su reino de Kerberos:

sambac.edt.org

Configuració de IP estàtica



· ./etc/netplan/00-installer-config.yaml

```
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: false
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
  version: 2
```

· netplan apply

```
root@sambadc:/home/administrador# 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 08:00:27:95:75:3c brd ff:ff:ff:ff:ff:ff
  inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
    valid_lft 86104sec preferred_lft 86104sec
  inet6 fe80::a00:27ff:fe95:753c/64 scope link
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
  link/ether 08:00:27:0d:4c:8c brd ff:ff:ff:ff:ff:ff
  inet 192.168.1.10/24 brd 192.168.1.255 scope global enp0s8
    valid_lft forever preferred_lft forever
  inet6 fe80::a00:27ff:fe0d:4c8c/64 scope link
    valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
  link/ether 08:00:27:8b:70:db brd ff:ff:ff:ff:ff:ff
```

Configuracions del sistema



· /etc/resolv.conf

```
nameserver 192.168.1.10
nameserver 8.8.8.8
search edt.org
```

· /etc/hosts

```
192.168.1.10 sambac sambac.edt.org
192.168.1.10 edt.org edt
```

```
samba-tool domain provision
Realm: Enter (EDT.ORG)
Domain: Enter (EDT)
Server Role: Enter (dc)
DNS backend: Enter (SAMBA_INTERNAL)
DNS forwarder: 8.8.8.8 #o 192.168.1.10 (la que ens mostra per defecte)
```

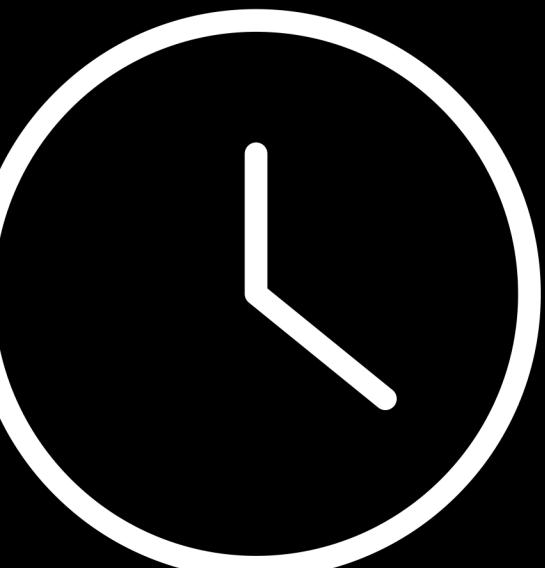
- systemctl start samba-ad-dc
- systemctl status samba-ad-dc

Configuració de la sincronització de temps

- /var/lib/samba/ntp_signd

```
leapsecond right/UTC  
bindcmdaddress 192.168.1.10  
allow 192.168.1.0/24  
ntpsigndsocket /var/lib/samba/ntp_signd
```

- systemctl restart chronyd
- systemctl status chronyd



Verificacions i altres comandes



Verificació de la configuració dels noms de domini

- `host -t A sambac.edt.org`
- `host -t A edt.org`
- `host -t SRV _kerberos._udp.edt.org`
- `host -t SRV _ldap._tcp.edt`

Gestió del servei Chrony

- `systemctl restart chronyd`
- `systemctl status chronyd`

Autenticació i verificació amb Kerberos

- `kinit administrator@EDT.ORG`
 - `1212jupiter@`
- `klist`

Accés a recursos compartits amb SMB

- `smbclient //localhost/netlogon -U 'administrator'`
 - `ls`
- `smbclient -L edt.org`

Nivell del domini i gestió d'usuaris amb Samba

- `samba-tool domain level show`
- `samba-tool user create diego01`
 - `diego01@`
- `samba-tool user create bryan01`
 - `bryan01@`

Verificacions i altres comandes



- samba-tool user list
- samba-tool user delete <nom_user>
- samba-tool computer list
- samba-tool computer delete <nom_pc>
 - samba-tool group add <nom_grup>
 - samba-tool group list
 - samba-tool group listmembers 'Domain Admins'
 - samba-tool group addmembers <nom_grup> <nom_user>
 - samba-tool group removemembers <nom_grup> <nom_user>



WIN-CLIE1_2

WIN-CLIE1_2



imatge ISO: Win10_23H2_es-es_x64.iso

- Adapter1: Xarxa Interna
- Adapter2: Adaptador de Pont
- Memoria RAM: 4080 ram
- Processadors: 4 cpus
- Usuari: WIN-CLIE
- Contrasenya: 1212jupiter@

Three screenshots of network adapter configuration windows, each showing four adapters labeled Adapter 1 through Adapter 4. Each window has an "Enable Network Adapter" checkbox checked.

- The top window shows Adapter 1 selected, attached to "NAT".
- The middle window shows Adapter 1 selected, attached to "Internal Network" and named "intnet".
- The bottom window shows Adapter 3 selected, attached to "Bridged Adapter" and named "Realtek Gaming GbE Family Controller".

Configuració de IP estàtica



Configuració

- Xarxa i Internet, Ethernet
 - o Xarxa
 - o Comfiguració d'IP
 - o IPv4
 - o editar

```
PS C:\Windows\system32> ping edt.org

Haciendo ping a edt.org [192.168.1.10] con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.10:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

IPv4

Activado

Dirección IP

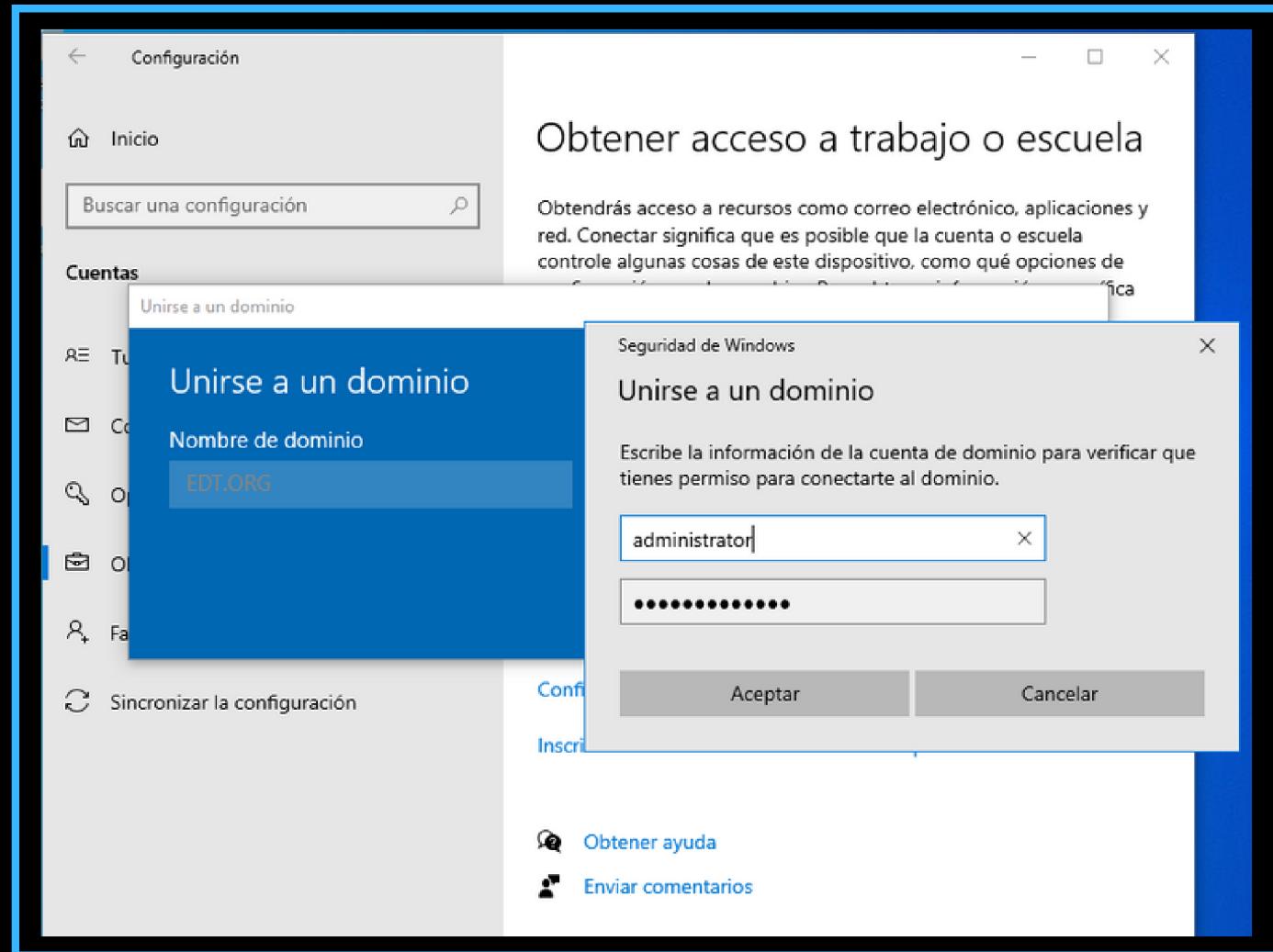
Longitud del prefijo de subred

Puerta de enlace

DNS preferido

DNS alternativo

Connexió al workgroup i comprovacions



Configuració

- Comptes

- Obtindre accessos al treball o escola
 - Connectar
 - Acció alternativa
 - EDT.ORG
 - administrator
 - 1212jupiter@
 - administrator
 - administrador
 - rename-computer WIN-CLIE
 - samba-tool computer list

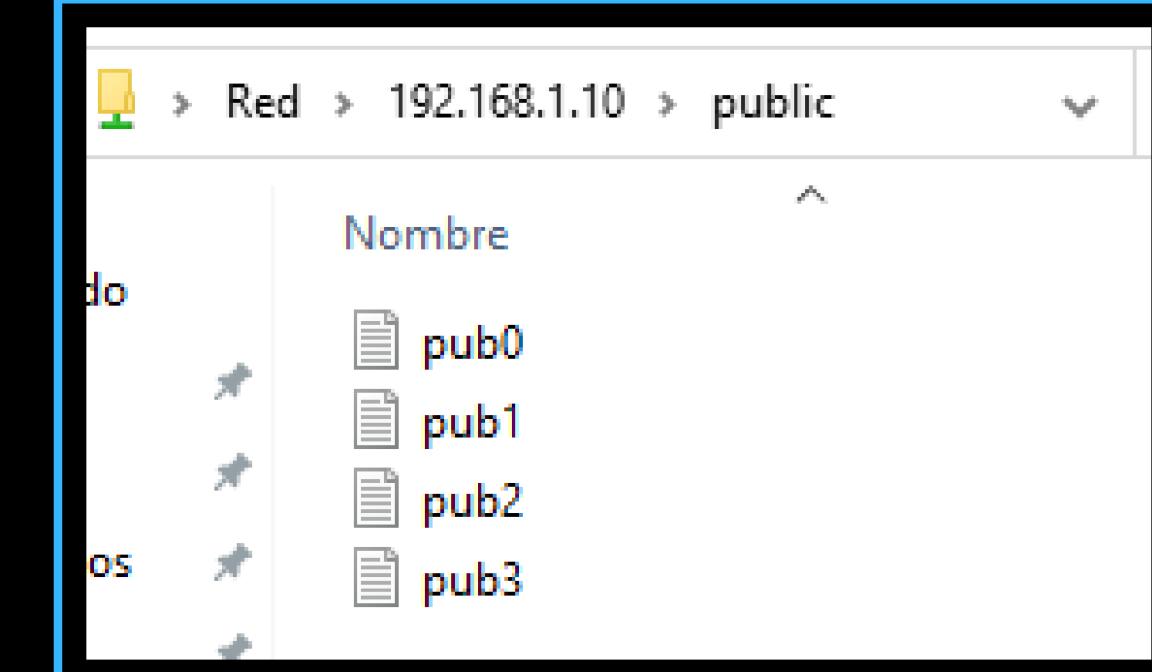
```
root@sambac:/home/administrador# samba-tool computer list
WIN-CLIE$
SAMBAC$
```

Connexió al workgroup i comprovacions

- etc/samba/smb.conf

```
[public]
comment = share public
path = /var/lib/samba/public
browseable = yes
writable = yes
guest ok = yes
[global]
dns forwarder = 192.168.1.10
netbios name = SAMBAC
realm = EDT.ORG
server role = active directory domain controller
workgroup = EDT
[sysvol]
path = /var/lib/samba/sysvol
read only = no
[netlogon]
path = /var/lib/samba/sysvol/edt.org
read only = no
```

- mkdir /var/lib/samba/public
- touch /var/lib/samba/public/pub{0..4}.txt





UBUN-CLIE

UBUN-CLIE



imatge ISO: ubuntu-24.04-desktop-amd64.iso

- Adapter1: Adaptador de Pont
- Adapter1: Xarxa Interna
- Memoria RAM: 2040 ram
- Processadors: 2 cpus
- Usuari: ubun-clie
- Contrasenya: jupiter

The image shows two side-by-side screenshots of network adapter configuration interfaces. Both interfaces have tabs for Adapter 1, Adapter 2, Adapter 3, and Adapter 4, with Adapter 1 selected.

Top Window (Bridged Adapter):

- Enable Network Adapter:** Checked.
- Attached to:** Bridged Adapter.
- Name:** eno1.

Bottom Window (Internal Network):

- Enable Network Adapter:** Checked.
- Attached to:** Internal Network.
- Name:** intnet.

Instal·lació de paquets



- apt-get update
- apt-get install -y vim acl attr samba samba-dsdb-modules
samba-vfs-modules smbclient winbind libpam-winbind
libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils
chrony net-tools

Configurando la autenticación de Kerberos

Cuando los usuarios intentan usar Kerberos y especifican un nombre principal o de usuario sin aclarar a qué dominio administrativo de Kerberos pertenece el principal, el sistema toma el reino predeterminado. El reino predeterminado también se puede utilizar como el reino de un servicio de Kerberos que se ejecute en la máquina local. Normalmente, el reino predeterminado es el nombre en mayúsculas del dominio del DNS local.

Reino predeterminado de la versión 5 de Kerberos:

EDT.ORG

Configurando la autenticación de Kerberos

Introduzca los nombres de los servidores Kerberos en el reino EDT.ORG de Kerberos, separados por espacios.

Servidores de Kerberos para su reino:

sambac.edt.org

Configurando la autenticación de Kerberos

Introduzca el nombre del servidor administrativo (cambio de contraseña) para el reino EDT.ORG de Kerberos.

Servidor administrativo para su reino de Kerberos:

sambac.edt.org

Configuració de IP estàtica



- IPv4 - Manual

The screenshot shows the NetworkManager configuration interface for a 'Wired' connection. The 'IPv4' tab is selected. Under 'IPv4 Method', the 'Manual' option is chosen. In the 'Addresses' section, a new row is configured with the following values:

Address	Netmask	Gateway
192.168.1.30	255.255.255.0	192.168.1.10

Below this, the 'DNS' section shows 'Automatic' selected, with the value '192.168.1.10' listed. A note at the bottom says 'Separate IP addresses with commas'.

- ip a

```
ubun-clie@ubun-clie-VirtualBox:~$ 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 noprefixroute
        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:ba:bd:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.30/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
```

Configuració i accés al domini EDT.ORG



- ./etc/hosts

```
192.168.1.10 sambac sambac.edt.org
192.168.1.10 edt.org edt
```

- kinit administrator@EDT.ORG

- 1212jupiter@

- klist

```
root@ubun-clie-VirtualBox:/home/ubun-clie# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EDT.ORG

Valid starting     Expires            Service principal
06/05/24 18:24:50  07/05/24 04:24:50  krbtgt/EDT.ORG@EDT.ORG
                  renew until 07/05/24 18:24:45
```

- ping sambac.edt.org

```
root@ubun-clie-VirtualBox:/home/ubun-clie# ping sambac.edt.org
PING sambac (192.168.1.10) 56(84) bytes of data.
64 bytes from sambac (192.168.1.10): icmp_seq=1 ttl=64 time=0.252 ms
64 bytes from sambac (192.168.1.10): icmp_seq=2 ttl=64 time=0.212 ms
^C
--- sambac ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.212/0.232/0.252/0.020 ms
```

Unió al domini EDT.ORG



· ./etc/samba/smb.conf

```
[global]
workgroup = EDT
realm = EDT.ORG
netbios name = ubunclie
security = ADS
dns forwarder = 192.168.1.10

idmap config * : backend = tdb
idmap config * : range = 50000-100000

template homedir = /home/%D/%U
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false
winbind nss info = rfc2307
winbind enum users = yes
winbind enum group = yes

vfs objects = acl_xattr
map acl inherit = Yes
store dos attributes = Yes
```

- `systemctl stop samba-ad-dc`
- `systemctl restart smbd nmbd`
- `systemctl enable smbd nmbd`
- `net ads join -U administrator`
 - 1212jupiter@

```
root@sambac:/home/administrador# samba-tool computer list
4IN-CLIE$
JBUN-CLIE$
SAMBAC$
```

Altres configuracions i comprovacions



- ./etc/nsswitch.conf

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

hosts:       files dns
networks:    files

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

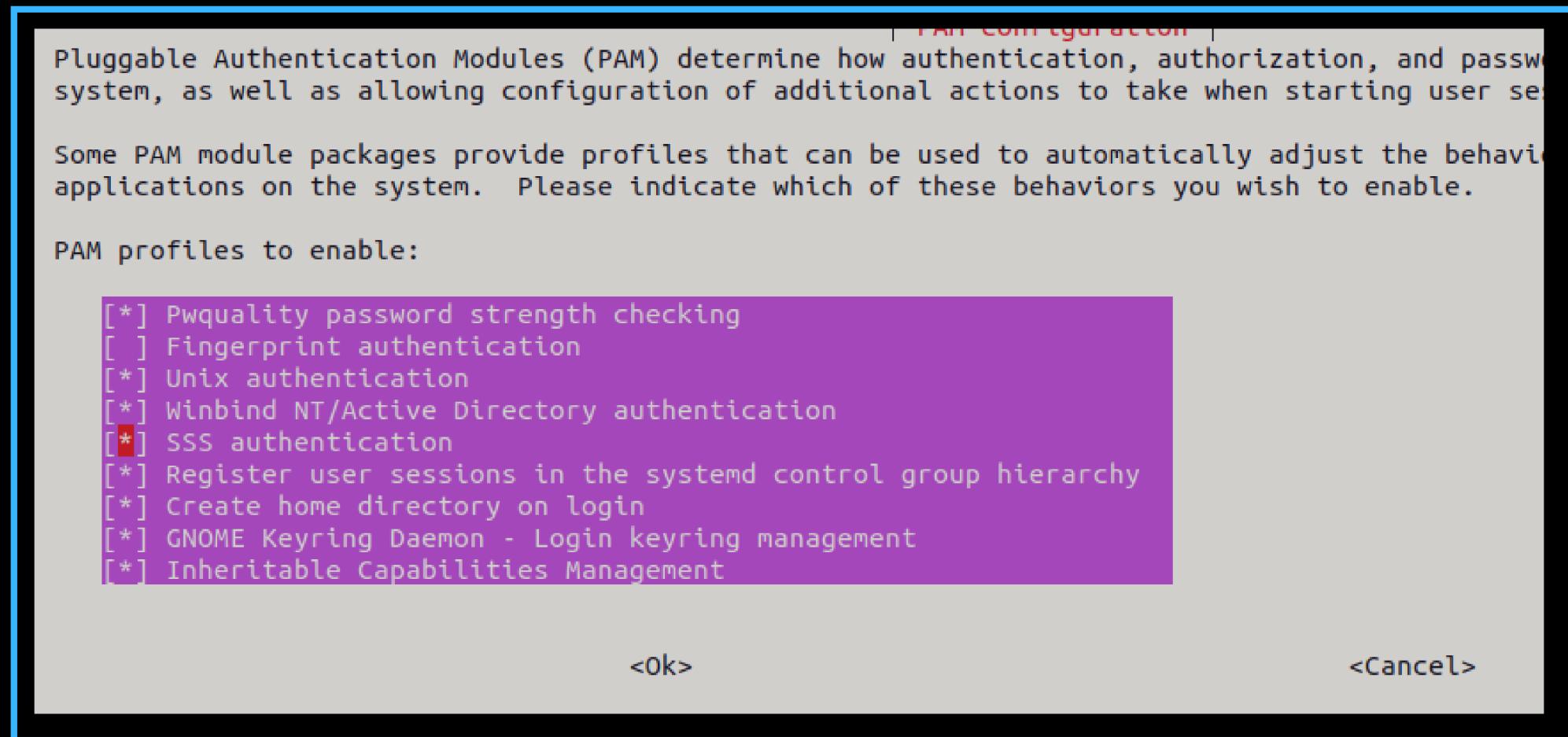
netgroup:    nis  sss
automount:  sss
```

- systemctl restart winbind
- wbinfo -u
- wbinfo -g
- getent passwd | grep administrator
- getent group | grep "domain admins"
- id administrator

Altres configuracions i comprovacions



· pam-auth-update



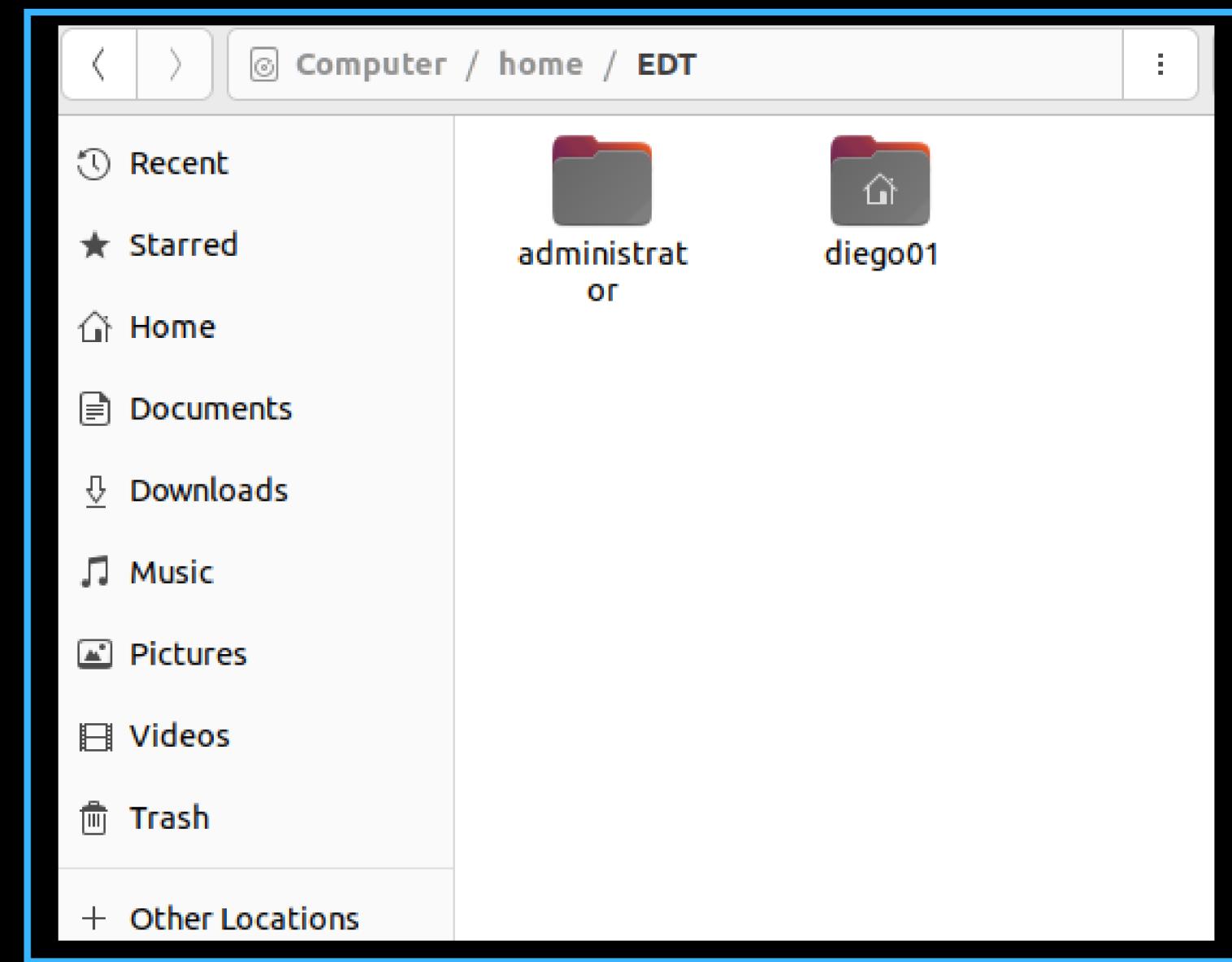
· /etc/pam.d/common-account

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

Altres configuracions i comprovacions



- usermod -aG sudo administrator
- su administrator
 - 1212jupiter@
- sudo su
- su - diego01
 - diego01*
- pwd
 - /home/EDT/diego01





RECURSOS COMAPARTITS

Recursos Compartits

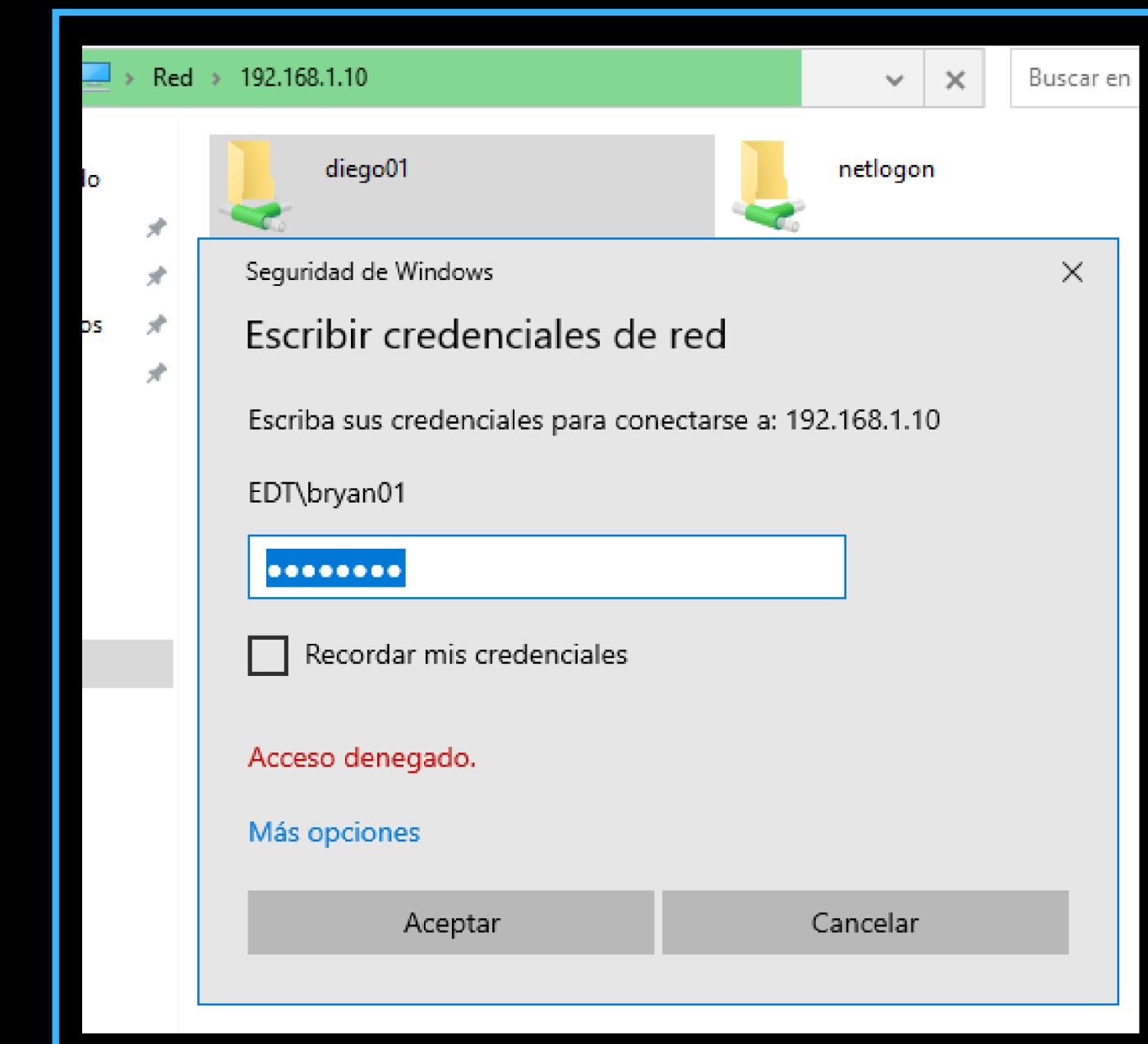
SAMBA-SERVER

- /etc/samba/smb.conf

```
[diego01]
comment = share per a diego01
path = /etc/diego01
valid users = diego01
writable = yes
```

- mkdir /etc/diego01
- chmod 777 /etc/diego01
- systemctl restart samba-ad-dc

WIN-CLIE



Recursos Compartits

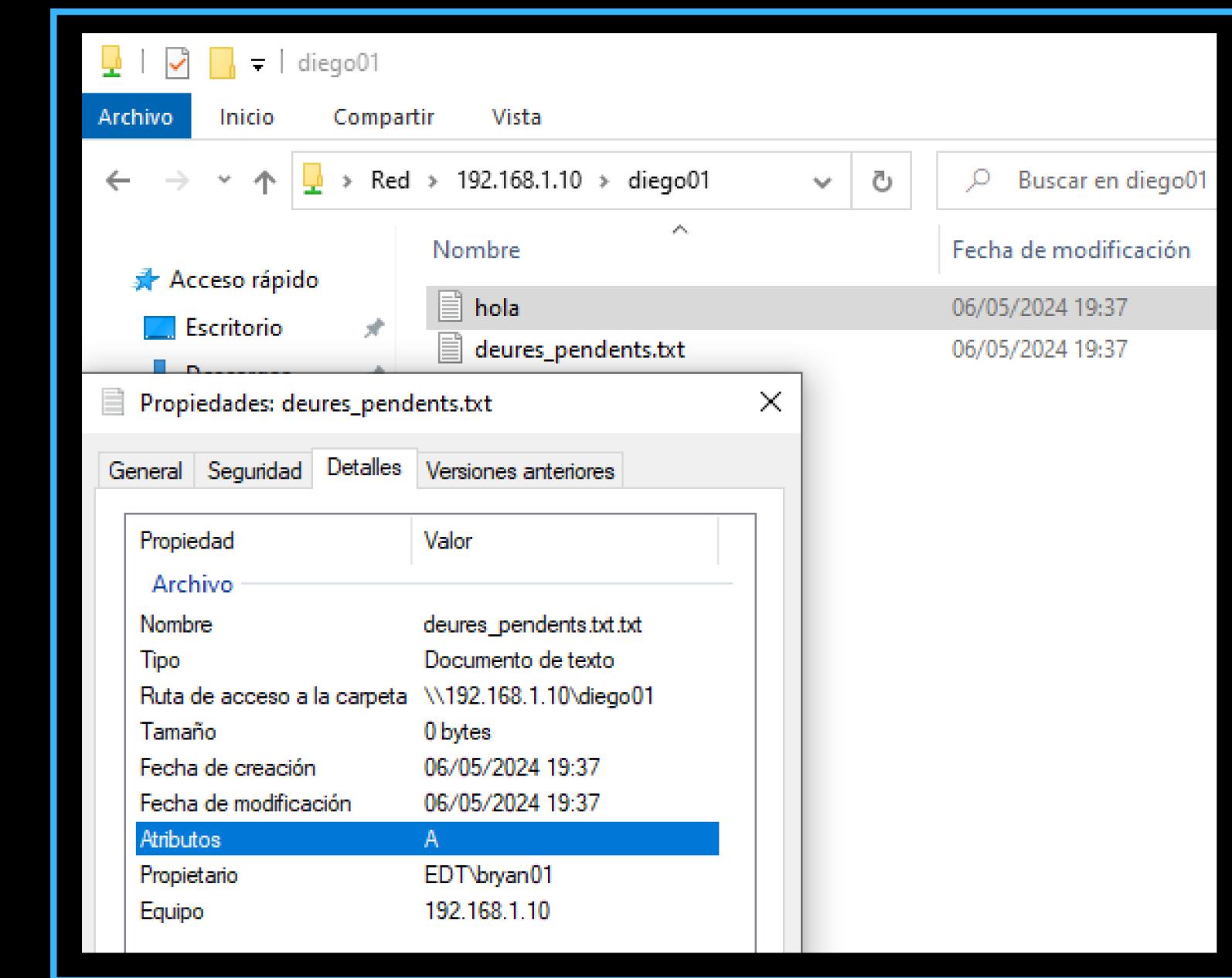
SAMBA-SERVER

- /etc/samba/smb.conf

```
[diego01]
comment = share per a diego01
path = /etc/diego01
browseable = yes
writable = yes
valid users = bryan01, diego01
```

- systemctl restart samba-ad-dc

WIN-CLIE



Recursos Compartits



SAMBA-SERVER

· /etc/samba/smb.conf

```
[diego01]
comment = share per a diego01
path = /etc/diego01
browseable = yes
writable = yes
valid users = bryan01, diego01
```

· systemctl restart samba-ad-dc

SAMBA-SERVER

```
Password for [EDT\bryan01]:
Try "help" to get a list of possible commands.
smb: \> put hola.txt README.md
putting file hola.txt as \README.md (0,0 kb/s) (average 0,0 kb/s)
smb: \> ls
.
..
deures_pendents.txt.txt
README.md
hola.txt
.
11758760 blocks of size 1024. 6499424 blocks available
```

Recursos Compartits

SAMBA-SERVER

- /etc/samba/smb.conf

```
[diego01]
comment = share per a diego01
path = /etc/diego01
browseable = yes
read only = yes
write list = bryan01, diego
```

- systemctl restart samba-ad-dc

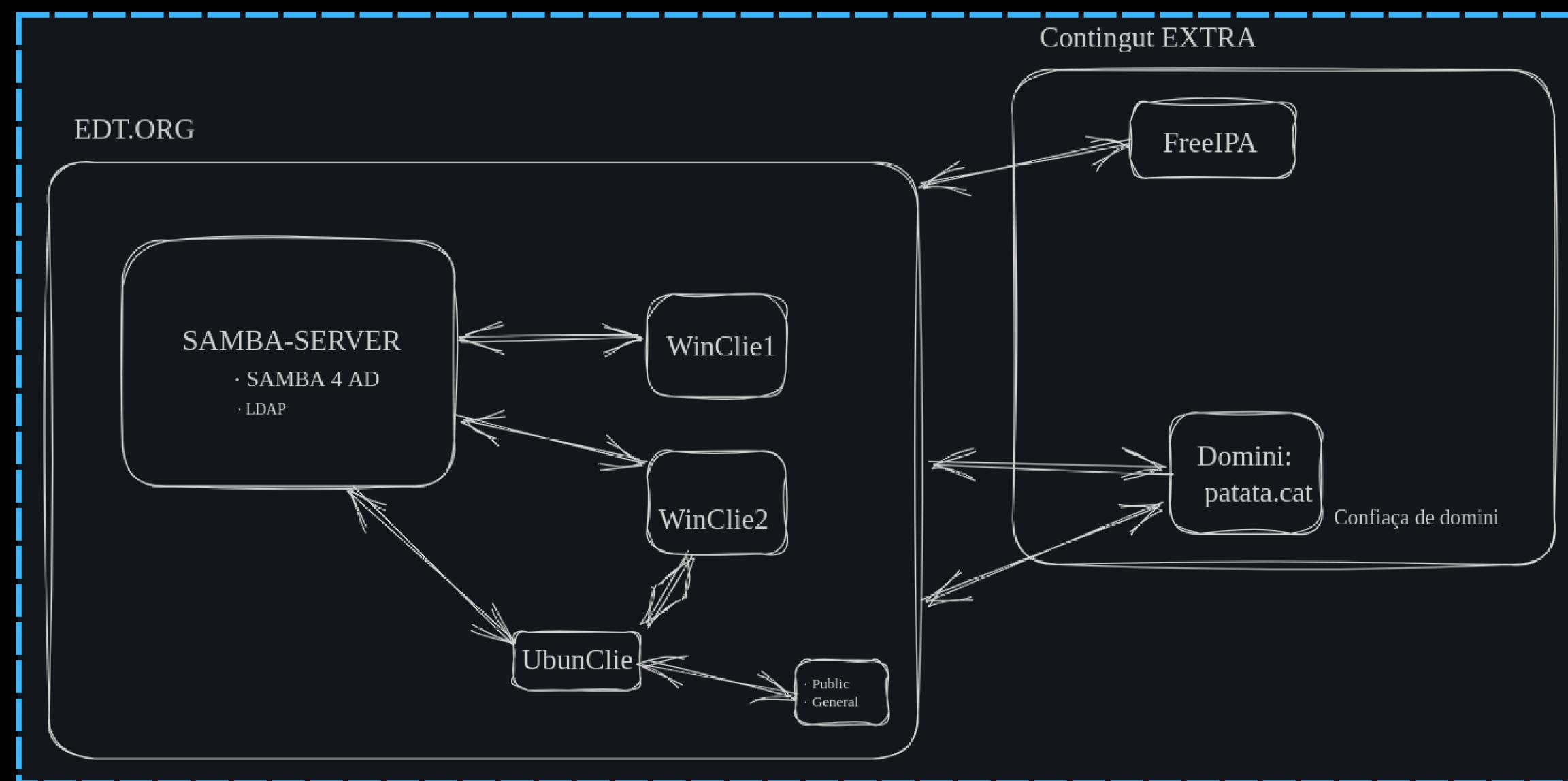
UBUN-CLIE

```
bryan01@ubun-clie-VirtualBox:~$ su - hacker01
Password:
Warning: Your password will expire in 41 days on lun 17 jun 2024 19:43:28
Creando directorio «/home/EDT/hacker01».
hacker01@ubun-clie-VirtualBox:~$ ls
hacker01@ubun-clie-VirtualBox:~$ touch troyan.txt
hacker01@ubun-clie-VirtualBox:~$ smbclient //EDT.ORG/diego01 -U hacker01
Unknown parameter encountered: "winbind enum group"
Ignoring unknown parameter "winbind enum group"
Password for [EDT\hacker01]:
Try "help" to get a list of possible commands.
smb: \> put troyan.txt bromo.txt
NT_STATUS_ACCESS_DENIED opening remote file \bromo.txt
smb: \> q
```



CONCLUSIÓ

CONCLUSIÓ



- Resum dels passos i l'èxit de la configuració
- Reflexió sobre els resultats



**GRÀCIES PER LA
VOSTRA ATENCIÓ**

