ALUMNES: Arturo Aragón Hidalgo, Jesika Jiménez Prado

GRUP: |5012

DOCUMENTACIÓ PRÀCTICA 3 - SESSIÓ 2 - SAMBA

—----------------------------------------------------------------------

Per a aquesta pràctica hem configurat la xarxa amb adaptador en pont i xarxa interna a les màquines client Linux i al servidor. Tant les màquines Linux com el servidor han d’estar configurades amb adaptador en pont.

\*\*\*INSTAL·LACIÓ DE SAMBA\*\*\*

\*\*SERVIDOR\*\*\*

Pel que fa al servidor, el que hem fet ha estat instal·lar Samba amb la comanda següent:  
 apt install samba

També hem configurat el fitxer /etc/network/interfaces per tal que disposi d’una interfície de xarxa en adaptador en pont i una altra per a xarxa interna, de manera que el servidor pugui comunicar-se tant amb clients Windows com amb clients Linux.

Contingut de /etc/network/interfaces:

# Interfície de loopback

auto lo

iface lo inet loopback

# Interfície de xarxa principal

allow-hotplug enp0s3

iface enp0s3 inet dhcp

# Interfície IPv6 automàtica

iface enp0s3 inet6 auto

# Segona interfície de xarxa (xarxa interna)

auto enp0s8

iface enp0s8 inet static

address 10.4.1.3

netmask 255.255.255.0

network 10.4.1.0

broadcast 10.4.1.255

Un cop modificat aquest fitxer, passem a configurar el fitxer /etc/samba/smb.conf, amb l’objectiu de poder crear directoris compartits entre el servidor i els clients (tant Linux com Windows).

Com a configuració bàsica, hem de verificar que dins el fitxer /etc/samba/smb.conf es trobin correctament definits els següents paràmetres:

1 - Verificació de la configuració global

Dins la secció [global] del fitxer de configuració de Samba (smb.conf), cal confirmar que el grup de treball estigui definit correctament:

[global]

workgroup = WORKGROUP

Aquesta línia defineix el nom del grup de treball de Windows/Linux amb el qual els equips del mateix segment de xarxa es poden comunicar. És important que aquest valor coincideixi amb el grup utilitzat per les màquines client.

2 - Configuració de la secció [homes]

Comprovarem que dins la secció [homes] es permeti l'accés en mode lectura i escriptura als directoris personals dels usuaris autenticats:

[homes]

read only = no

Aquesta opció estableix que els directoris "home" dels usuaris no seran de només lectura, permetent així que puguin crear, modificar o esborrar arxius dins la seva pròpia carpeta.

### 3 - Substitució de la secció [print$] per [HOME]

Com que no farem ús compartit de recursos d’impressió, eliminarem la secció [print$] i en el seu lloc crearem una nova secció [HOME], la qual gestionarà la compartició dels directoris personals dels usuaris. La configuració serà la següent:

[HOME]

comment = XXXXXXXXX

path = /home/%u

read only = no

writable = yes

guest ok = no

create mask = 0700

directory mask = 0700

Explicació detallada de cada paràmetre:

comment = XXXXXXXXX: Comentari descriptiu del recurs compartit. Es pot substituir per una breu descripció, com ara "Directori personal de l’usuari".

path = /home/%u: Defineix la ruta al directori personal de cada usuari. %u representa el nom d'usuari amb què s'ha iniciat sessió.

read only = no: Especifica que el recurs no serà de només lectura.

writable = yes: Confirma que els usuaris tenen permisos d'escriptura dins del recurs.

guest ok = no: Indica que els usuaris anònims (sense autenticació) no tenen permès l’accés a aquest recurs compartit.

create mask = 0700: Assigna permisos de lectura, escriptura i execució únicament a l’usuari propietari dels arxius nous. Altres usuaris no tindran cap accés.

directory mask = 0700: Aplica la mateixa política de permisos (lectura/escriptura/executar) però per als directoris que es creïn dins del recurs.

4 - Assignació de permisos al directori personal de l’usuari

Per garantir que només l’usuari propietari pugui accedir al seu directori personal (/home/entel), s’aplicaran permisos restrictius mitjançant la comanda chmod:

# chmod -R 700 /home/entel

Explicació:

L’opció -R aplica els permisos de manera recursiva a tot el contingut del directori. El valor 700 estableix que únicament el propietari del directori tindrà permisos de lectura, escriptura i execució, mentre que altres usuaris no tindran cap accés.

### 5 - Desactivació del servei d’impressió

Atès que no es farà ús del servei de compartició d’impressores, es desactivarà la secció [printers] del fitxer de configuració de Samba (smb.conf) comentant totes les línies que en formen part. Això es pot fer afegint un punt i coma (;) a l’inici de cada línia:

;[printers]

; comment = All Printers

; path = /var/spool/samba

; browseable = no

; guest ok = no

; read only = yes

; printable = yes

Comentant aquestes línies s’evita que Samba carregui o publiqui recursos relacionats amb impressores.

6 - Inclusió d’usuaris al grup sambashare

Per concedir accés als recursos compartits gestionats per Samba, cal afegir els usuaris corresponents al grup del sistema sambashare. Això es pot fer amb la següent comanda:

# adduser usuari sambashare

Per exemple, per afegir l’usuari entel:

# adduser entel sambashare

Verificació:

Per comprovar que l’usuari s’ha afegit correctament al grup, es pot editar el fitxer de grups del sistema amb:

# cat /etc/group

En el nostre cas:

….

systemd-timesync:x:997:

messagebus:x:107:

\_ssh:x:108:

avahi-autoipd:x:109:

bluetooth:x:110:entel

entel:x:1000:

vboxsf:x:996:

vboxdrmipc:x:995:

rdma:x:111:

sambashare:x:994:entel

Un cop dins de l'editor, s’ha de localitzar la línia corresponent al grup sambashare i verificar que l’usuari aparegui a la llista de membres.

7 - Definició de la secció [SAMBA] per a la compartició d’un directori

Afegirem una nova secció al fitxer de configuració de Samba (smb.conf) anomenada [SAMBA], la qual permetrà compartir una carpeta específica entre diversos usuaris. Aquesta secció inclourà la configuració següent:

[SAMBA]

comment = XXXXXXXXX

path = /CompartirSamba

read only = no

writable = yes

guest ok = no

create mask = 0770

directory mask = 0770

force group = sambashare

Descripció de cada paràmetre:

comment = XXXXXXXXX: Comentari descriptiu del recurs compartit. Pot ser, per exemple, "Directori compartit d'usuaris Samba".

path = /CompartirSamba: Ruta absoluta cap al directori físic del sistema que es vol compartir.

read only = no i writable = yes: S’indica explícitament que els usuaris amb accés podran escriure dins el directori compartit.

guest ok = no: Es desactiva l'accés a usuaris no autenticats (convidats), mantenint el recurs restringit a usuaris registrats.

create mask = 0770: Els fitxers creats dins el directori heretaran permisos complets (lectura, escriptura, execució) per a l’usuari propietari i el grup.

directory mask = 0770: Es defineixen permisos idèntics als anteriors però aplicats a nous directoris.

force group = sambashare: Aquesta opció força que qualsevol arxiu o carpeta creada dins el recurs pertanyi automàticament al grup sambashare, independentment del grup principal de l’usuari.

8) Creació i configuració del directori /Samba

Per tal de posar en marxa el directori que serà compartit, cal seguir els passos següents:

a) Creació del directori compartit:

# mkdir /CompartirSamba

Aquest comandament genera el directori físic que allotjarà els fitxers compartits.

b) Assignació del grup al directori:

# chown root:sambashare /CompartirSamba

Amb aquesta instrucció, es defineix root com a propietari i sambashare com a grup del directori, permetent un control centralitzat sobre els accessos.

c) Establiment de permisos:

# chmod 770 CompartirSamba

S’atorguen permisos complets al propietari (root) i als membres del grup sambashare. Altres usuaris del sistema no tindran accés.

### 9) Configuració d’usuaris Samba i activació del servei

a) Afegir l’usuari entel al servei Samba:

# smbpasswd -a entel

Durant el procés, es demanarà definir una contrasenya per a aquest usuari dins del context de Samba. En aquest cas concret, s’ha fet servir la mateixa contrasenya que l’usuari del sistema: letne.

b) Reiniciar el servei Samba per aplicar els canvis:

# service smbd restart

Amb aquesta acció, es recarrega la configuració del servei Samba. A partir d’aquest moment, el servidor estarà operatiu i preparat per acceptar connexions dels usuaris configurats.

### 10) Fitxer smb.conf

S'adjunta el fitxer de configuració smb.conf amb totes les modificacions descrites anteriorment per tal de tenir una visió completa del sistema Samba configurat.

Amb aquests passos, haurem completat la configuració d’un entorn Samba funcional, segur i adaptat a la compartició d’arxius entre usuaris específics.

\*\*\*PROVES DE FUNCIONAMENT\*\*\*

\*\*\*CLIENT LINUX\*\*\*

Para el cliente, lo que hemos hecho ha sido instalar samba con la comanda: **apt install smbclient.**

1) Configuració /etc/network/interfaces

Hemos configurado el /etc/network/interfaces para que tuviera una interfaz en adaptador puente y otra para red interna, ya que de esa manera el servidor puede tener clientes en windows y en linux.

/etc/network/interfaces

# The loopback network interface

auto lo

iface lo inet loopback

auto enp0s3

iface enp0s3 inet static

address 192.168.1.101

netmask 255.255.255.0

gateway 192.168.1.1

dns-nameservers 8.8.8.8 1.1.1.1

auto enp0s8

iface enp0s8 inet static

address 10.4.1.2

netmask 255.255.255.0

network 10.4.1.0

broadcast 10.4.1.255

Per què hem configurat la IP 192.168.1.101 a enp0s3?

Perquè aquesta és la interfície amb adaptador pont, que connecta el client Linux directament a la xarxa física de l’amfitrió. Aquesta configuració permet:

* Que el client Linux es comuniqui directament amb altres dispositius de la xarxa local real (com altres clients Windows).
* Que pugui accedir a internet a través del gateway (192.168.1.1), si és necessari.

- Que estigui a la mateixa subxarxa que el servidor Samba (si aquest també té una interfície en mode pont amb una IP del rang 192.168.1.x).

Això permet fer servir comandes com:

smbclient -L //192.168.1.100 -U usuari

Per què hi ha una segona interfície enp0s8 amb IP 10.4.1.2?

Aquesta és la interfície de xarxa interna (host-only / xarxa privada virtual), configurada per a una xarxa aïllada entre màquines virtuals, sense accés a l’exterior. Es fa servir per:

Connectar el client directament amb el servidor Samba sense passar per la xarxa real.

Simular un entorn controlat on diversos clients (Linux, Windows, etc.) es comuniquin entre ells i amb el servidor.

Permetre que el servidor tingui clients tant a la xarxa interna com a la xarxa pública (pont).

### 2) Llistat de recursos disponibles al servidor Samba

Un cop instal·lat smbclient, podem consultar quins recursos compartits hi ha disponibles en el servidor amb la següent comanda:

# smbclient -L <ip-servidor> -U <usuari>

En el cas pràctic, amb IP 10.4.1.3 i usuari entel, s'utilitzaria:

# smbclient -L 10.4.1.3 -U entel

Un cop executada la comanda, es mostraran tots els directoris compartits pel servidor Samba. Hem d’identificar-hi els recursos anomenats HOME i CompartirSamba, que seran els que utilitzarem posteriorment.

3) Connexió als recursos compartits

Per establir connexió amb un dels directoris compartits, farem ús de la següent sintaxi:

smbclient //<ip-servidor>/<nom\_directori> -U <usuari>

Seguint l’exemple anterior, per connectar-nos al directori personal HOME:

# smbclient //10.4.1.3/HOME -U entel

I per accedir al recurs compartit general Samba:

# smbclient //10.4.1.3/CompartirSamba -U entel

Nota important:

En aquest escenari, el directori Samba està pensat com un espai compartit entre diversos usuaris, però s’ha configurat amb permisos restringits per evitar conflictes. Només l’usuari root tindrà drets d’escriptura complets dins d’aquest recurs.

4) Ús de comandes dins de smbclient

Un cop establerta la connexió, smbclient funciona de manera similar a un client FTP. Aquestes són algunes de les comandes més útils:

get <fitxer>: Descarrega un fitxer del servidor al client.

put <fitxer>: Puja un fitxer del client al servidor.

rm <fitxer>: Elimina un fitxer del servidor.

cd <directori>: Canvia de directori dins del servidor.

ls: Mostra el contingut del directori actual.

?: Llista totes les comandes disponibles dins de smbclient.

5) Requisits addicionals per a muntatge de recursos Samba

Per fer el muntatge permanent dels recursos Samba en el sistema de fitxers local, cal instal·lar alguns paquets addicionals:

# apt install cifs-utils nfs-common

També és necessari crear el grup sambashare, si encara no existeix:

# addgroup sambashare

I afegir els usuaris que necessitin accedir al recurs compartit a aquest grup. Per exemple:

# adduser entel sambashare

# adduser root sambashare # (opcional, només a mode d'exemple)

6) Creació de punts de muntatge

Finalment, crearem els directoris locals que actuaran com a punts de muntatge dels recursos Samba:

# mkdir /HomeSamba

# mkdir /CompartirSamba

7) Muntatge temporal amb cifs

Per muntar recursos Samba de manera temporal (fins al proper reinici), utilitzarem la comanda mount amb el tipus de sistema de fitxers cifs (Common Internet File System), que és el protocol utilitzat per Samba.

Comanda genèrica:

# mount -t cifs //<IP\_SERVIDOR>/<Nom\_recurs> /<Directori\_local> -o rw,username=<usuari\_samba>,password=<contrasenya>,file\_mode=XXXX,dir\_mode=XXXX,uid=<usuari\_local>,gid=<grup\_local>

Las comandes que nosaltres hem fet servir:

# mount -t cifs //10.4.1.3/HOME /HomeSamba -o username=entel,password=letne,file\_mode=0700,dir\_mode=0700,uid=entel,gid=entel

#mount -t cifs //10.4.1.3/SAMBA /CompartirSamba -o username=entel,password=letne,file\_mode=0770,dir\_mode=0770,uid=root,gid=sambashare

Explicació dels paràmetres:

| Opció | Descripció |
| --- | --- |
| -t cifs | Especifica que el tipus de sistema de fitxers és CIFS (per a recursos Samba). |
| //IP/DIRECTORI | Ruta del recurs compartit al servidor Samba. |
| /Directori\_local | Punt de muntatge local al qual es vincularà el recurs. |
| rw | Permet lectura i escriptura. |
| username=... | Usuari Samba utilitzat per autenticar-se. |
| password=... | Contrasenya de l’usuari Samba. |
| file\_mode=0700 | Permisos assignats als fitxers (lectura/escriptura només per l’usuari). |
| dir\_mode=0700 | Permisos per a directoris (lectura/escriptura/exploració només per l’usuari). |
| uid=usuari\_local | Defineix quin usuari local serà el propietari del recurs muntat. |
| gid=grup\_local | Grup local associat com a propietari del recurs muntat. |

## Desmuntatge d’un recurs Samba

Per alliberar un recurs que s’ha muntat prèviament, utilitzarem:

# umount /Directori\_local

## Muntatge persistent amb /etc/fstab

Perquè el sistema monti automàticament els recursos Samba en iniciar-se, podem definir-los dins del fitxer /etc/fstab.

### Pas 1: Crear fitxer de credencials segures

1. Crear el directori de credencials i protegir-ne els permisos:

# mkdir -p /etc/samba/credentials

# chmod 700 /etc/samba/credentials

1. Crear el fitxer de credencials amb les dades d’autenticació:

# nano /etc/samba/credentials/samba.cred

Contingut del fitxer:

username=entel

password=letne

1. Protegir el fitxer de credencials:

# chmod 600 /etc/samba/credentials/samba.cred

### Pas 2: Afegir les entrades a /etc/fstab

Editem el fitxer:

# nano /etc/fstab

I afegim les línies següents:

# Muntatge del directori HOME de Samba

//104.1.3/HOME /HomeSamba cifs credentials=/etc/samba/credentials/samba.cred,file\_mode=0700,dir\_mode=0700,uid=entel,gid=entel 0 0

# Muntatge del directori SAMBA compartit

//10.4.1.3/SAMBA /CompartirSamba cifs credentials=/etc/samba/credentials/samba.cred,file\_mode=0770,dir\_mode=0770,uid=root,gid=sambashare 0 0

### Significat dels darrers dos valors (0 0):

* El primer 0: Indica que no es fa còpia de seguretat (dump) d'aquest sistema de fitxers.
* El segon 0: Especifica que fsck (verificador de sistema de fitxers) no ha de comprovar aquest recurs en l'arrencada.

### Pas 3: Muntar tots els sistemes definits a fstab

Per aplicar i provar que les línies afegides funcionen correctament:

# mount -a

\*\*\*CLIENT WINDOWS\*\*\*

Connexió des de client Windows a un servidor Samba

1 - Activar el protocol SMBv1 (si és necessari)  
 Windows 10 i versions posteriors tenen desactivat per defecte el suport per al protocol SMB 1.0/CIFS per motius de seguretat. Tot i que és recomanable utilitzar SMBv2 o SMBv3, si el servidor Samba utilitza SMBv1, cal activar-lo.

Passos per habilitar SMB 1.0/CIFS:

- Obrir el menú Inici i escrivir: Características de Windows  
- Fer clic a l'opció "Activar o desactivar características de Windows"  
- A la llista que apareix, localitza l’opció "Compatibilidad con el protocolo para compartir archivos SMB 1.0/CIFS"  
- Activa l'opció "Cliente SMB 1.0/CIFS"

(Opcional) També podem activar "Servidor SMB 1.0/CIFS" si aquest ordinador compartirà recursos

Fer clic a Aceptar i reiniciar l'equip per aplicar els canvis

2- Verificació de la IP del servidor Samba

A la màquina Linux, comprovar la IP de la interfície de xarxa (normalment enp0s3 si es tracta d’una màquina virtual de VirtualBox)

Comanda per obtenir-la: ip a show enp0s3  
 Copiar la IP (per exemple: 192.168.1.41), que és la que haurem d’utilitzar des de Windows

3 - Connexió al recurs compartit des de l’Explorador de fitxers

Opció 1: Connexió temporal

- Obrir Explorador de fitxers

- A la barra lateral, seleccionar: Este equipo → Conectar a una unidad de red

-Seleccionar una lletra de la unitat (per exemple Z:)

- Al camp de ruta de la carpeta escriure: \192.168.1.41\Samba  
-Marcar l'opció "Conectar con otras credenciales"  
-Fer clic a Finalizar  
-Introduir les credencials:

Usuari: entel  
Contrasenya: letne

-Si la connexió és correcta, apareixerà el contingut del recurs compartit com una nova unitat

Amb això, ja tindrem accés al directori compartit Samba del servidor Linux des de l'ordinador amb Windows.

Si volem que la connexió sigui permanent (es mantingui després de reiniciar), assegura't de marcar la casella "Reconectar al iniciar sesión" quan muntis la unitat de xarxa.

\*\*\*CONFIGURACIÓ DEL FIREWALL\*\*\*

#!/usr/sbin/nft -f

flush ruleset

table inet firewall {

chains {

input {

type filter hook input priority 0; policy drop;

# Permet connexions establertes i relacionades

ct state established,related accept

# Permet el loopback

iif "lo" accept

# PERMET el servei concret - substitueix segons el port/servei que vulguis

# Exemple per SSH:

tcp dport 22 ct state new accept

# Exemple per HTTP i HTTPS:

# tcp dport {80, 443} ct state new accept

# Permet pings

ip protocol icmp accept

# LOG opcional per regles denegades (últim lloc si vols veure intents bloquejats)

# log prefix "DROP INPUT: " flags all counter

}

forward {

type filter hook forward priority 0; policy drop;

}

output {

type filter hook output priority 0; policy accept;

}

}

}

\*\*\*PROVES DE FUNCIONAMENT\*\*\*

\*\*SERVIDOR SAMBA\*\*

1. Prova de Ports Oberts (prova\_nmap\_server.txt)  
Objectiu: Verificar que els ports essencials per a Samba (139 i 445) estan oberts i accessibles.  
Comanda:  
nmap -p 139,445 10.4.1.3  
Resultats:

139/tcp (netbios-ssn): Obert.

445/tcp (microsoft-ds): Obert.  
Significat:

Els ports necessaris per a SMB/CIFS estan actius, permetent connexions de clients.

Confirma que el servidor està escoltant a les interfícies configurades.

2. Prova de Contingut del Recurs Compartit (prova\_contingut\_samba.txt)  
Objectiu: Validar que el recurs compartit /CompartirSamba existeix i conté fitxers.  
Comandes:  
cd /CompartirSamba  
ls  
Resultats:

Fitxers presents: fichero\_cliente.txt, fichero\_servidor.txt.  
Significat:

El directori compartit està muntat correctament.

Els permisos del grup sambashare permeten veure el seu contingut des del servidor.

3. Estat dels Serveis Samba (prova\_samba\_server.txt)  
Objectiu: Confirmar que els serveis smbd i nmbd estan en execució.  
Comandes:  
systemctl status smbd  
systemctl status nmbd  
Resultats:

smbd: active (running) amb múltiples processos fills.

nmbd: active (running), gestionant resolució NetBIOS.  
Significat:

Els serveis crítics de Samba estan operatius.

No hi ha errors d'inici als logs, la qual cosa indica una configuració vàlida.

4. Verificació del Directori Personal de l'Usuari (prova\_contingut\_entel.txt)  
Objectiu: Comprovar que el directori /home/entel existeix i té contingut.  
Comandes:  
cd /home/entel  
ls  
Resultats:

Fitxer present: prueba.txt.  
Significat:

El recurs HOME està configurat correctament per a l'usuari entel.

Els permisos drwx------ garanteixen que només el propietari té accés.

5. Anàlisi de Connexions Actives i Ports (prova\_funcionament\_server.txt)  
Objectiu: Identificar connexions SMB actives i ports en ús.  
Comandes:  
ss -tp  
ss -tlp  
Resultats:

Connexions actives: Clients des de 10.4.1.2 (xarxa interna) i 192.168.1.134 (xarxa pública).

Ports en escolta: 139/tcp i 445/tcp actius a totes les interfícies (0.0.0.0).  
Significat:

El servidor accepta connexions tant de xarxes internes com externes.

No hi ha ports innecessaris oberts, reduint la superfície d'atac.

6. Xifratge i Signatura de Tràfic (prova\_funcionament\_server.txt)  
Objectiu: Validar que les connexions SMB utilitzen xifratge i signatura de paquets.  
Comanda:  
smbstatus  
Resultats:

Xifratge: AES-128-GCM i AES-128-CCM.

Signatura: AES-128-GMAC i AES-128-CMAC.  
Significat:

El tràfic SMB està protegit contra escoltes i modificacions.

Compleix amb estàndards de seguretat moderns (SMB3)

7. Captura de Tràfic SMB (prova\_funcionament\_server.txt)  
Objectiu: Analitzar el tràfic de xarxa per detectar anomalies.  
Comandes:  
tcpdump -i enp0s8 port 445 or port 139 -w samba\_traffic2.pcap  
tcpdump -r samba\_traffic2.pcap  
Resultats:

Paquets SMB intercanviats entre 10.4.1.3 (servidor) i 10.4.1.2 (client).

Sense retransmissions o paquets corruptes.  
Significat:

Les comunicacions són estables i sense errors.

No hi ha evidència d'atacs (ex.: inundació de paquets).

8. Revisió de Logs de Samba (prova\_funcionament\_server.txt)  
Objectiu: Detectar errors o activitats sospitoses als logs.  
Comanda:  
tail -f /var/log/samba/log.smbd  
Resultats:

Entrades d'inici exitós del servei (smbd version 4.17.12-Debian started).

Sessions d'usuari registrades: session opened for user entel.  
Significat:

No hi ha errors crítics o intents d'accés no autoritzat.

Les operacions d'autenticació es registren correctament.

9. Permisos de Directoris i Grups (prova\_samba\_server.txt)  
Objectiu: Assegurar que els permisos del sistema de fitxers coincideixen amb la configuració de Samba.  
Comandes:  
ls -ld /home/entel  
ls -ld /CompartirSamba  
Resultats:

/home/entel: drwx------ (700) – Només accessible per entel.

/CompartirSamba: drwxrwx--- (770) – Accés per al grup sambashare.  
Significat:

Els permisos del sistema reforcen la seguretat dels recursos compartits.

Coherència entre la configuració de Samba i els permisos UNIX.

\*\*CLIENT WINDOWS\*\*

\*\*1. Configuració de xarxa del client Windows (proves\_client\_windows.txt)

Objectiu: Verificar les interfícies de xarxa i la connectivitat cap al servidor Samba.

Comandes:

ipconfig

Resultats:

Adreça IPv4 de la interfície Wi-Fi: 192.168.1.134.

Adreça del servidor Samba: 192.168.1.141.

Significat:

El client Windows està a la mateixa xarxa que el servidor Samba (192.168.1.0/24).

La configuració de xarxa permet la comunicació SMB a través del port 445.

\*\*2. Accés als recursos compartits des de Windows (proves\_client\_windows.txt)

Objectiu: Validar l'accés als recursos SAMBA i HOME des del client Windows.  
Comandes:

ls Z:\ # On Z: és la unitat mapejada a \\192.168.1.141\SAMBA

ls \\192.168.1.141\home

Resultats:

Recurs SAMBA: Conté fichero\_cliente.txt i fichero\_servidor.txt.

Recurs HOME: Conté prueba.txt.  
Significat:

Els recursos compartits són accessibles des de Windows.

\*\*CLIENT LINUX\*\*

L'usuari entel té permisos per llegir i escriure al directori SAMBA.

\*\*1. Muntatge temporal del recurs SAMBA en Linux (prova\_montar\_temporalment\_arxiu.txt)

Objectiu: Provar el muntatge manual del recurs compartit i la gestió d'arxius.  
Comandes:

mount -t cifs //10.4.1.3/SAMBA /CompartirSamba -o username=entel,password=letne

touch /CompartirSamba/test\_linux.txt

Resultats:

Arxius al directori muntat: fichero\_cliente.txt, fichero\_servidor.txt, test\_linux.txt.  
Significat:

El muntatge temporal funciona correctament.

L'usuari té permisos d'escriptura al compartit SAMBA (pot crear/eliminar arxius).

\*\*2. Llistat de tots els recursos compartits (prova\_listar\_tots\_els\_serveis\_compartits.txt)

Objectiu: Identificar tots els recursos publicats pel servidor Samba.  
Comanda:

smbclient -L //10.4.1.3 -U entel

Resultats:

Recursos detectats:

HOME: Directori personal de l'usuari.

SAMBA: Recurs compartit per al grup.

IPC$: Servei d'intercomunicació de processos.  
Significat:

El servidor publica correctament els recursos configurats a smb.conf.

No hi ha recursos no desitjats exposats.

\*\*3. Transferència d'arxius des del client Linux (prova\_client\_get.txt)

Objectiu: Verificar operacions bàsiques de lectura/escriptura al compartit SAMBA.  
Comandes dins de smbclient:

get fichero\_servidor.txt # Descarrega un arxiu del servidor

put fichero\_cliente.txt # Puja un arxiu al servidor

rm prueba1.txt # Elimina un arxiu

Resultats:

Arxius modificats al servidor:

fichero\_cliente.txt afegit.

prueba1.txt eliminat.  
Significat:

L'usuari té permisos complets (lectura, escriptura, eliminació) al recurs SAMBA.

Les operacions de xarxa es completen sense errors.

\*\*4. Accés al directori personal HOME des de Linux (prova\_entrar\_tots\_usuaris.txt)

Objectiu: Confirmar que l'usuari pot accedir al seu directori privat.

Comandes:

smbclient //10.4.1.3/HOME -U entel

ls

Resultats:

Arxius al directori HOME: prueba.txt, .bashrc, .profile, etc.  
Significat:

L'accés al directori personal està restringit a l'usuari propietari.

Els arxius ocults del sistema (com .bashrc) són visibles però no editables via Samba.

Conclusió General

El client Windows i Linux poden accedir correctament als recursos compartits del servidor Samba:

Recurs SAMBA: Compartit en mode lectura/escriptura per al grup sambashare.

Recurs HOME: Accés restringit a l'usuari propietari.

Encriptació: Les connexions usen xifrat AES-128 (comprovat a les proves anteriors).

Permisos: Coherents amb la configuració de Samba i els permisos UNIX.

BACKUPS

--------------

RSYNC:

Hem creat una MV per a guardar els Backups que farem usant les eines rsync i Borgbackup:  
  
La seva configuració de xarxa és la següent (com s’indica a les instruccions de l'entrega, pertany a la xarxa 10.G.1.0 on G es el nombre del nostre grup, en aquest cas, 4:

source /etc/network/interfaces.d/\*

# The loopback network interface

auto lo

iface lo inet loopback

# The primary network interface

allow-hotplug enp0s3

iface enp0s3 inet dhcp

# This is an autoconfigured IPv6 interface

iface enp0s3 inet6 auto

auto enp0s8

iface enp0s8 inet static

address 10.4.1.10

netmask 255.255.255.0

network 10.4.1.0

broadcast 10.4.1.255

També tenim configurada una xarxa NAT per a poder descarregar paquets en cas de que en necessitem més.

Ara cal que modifiquem la Configuració de SSH a la máquina Backup:

Habilitarem accés root i autenticació per contrasenya:

1. Editar el fitxer de configuració de SSH

Obrim el fitxer /etc/ssh/sshd\_config amb l'editor de text:

$ nano /etc/ssh/sshd\_config

2. Comprovar i configurar els següents paràmetres

- PermitRootLogin yes

(Permet l'accés com a usuari root via SSH)

- PasswordAuthentication yes

(Permet l'autenticació amb contrasenya)

- PermitTTY yes

(Permet la connexió via terminal TTY, útil en alguns casos específics)

3. Desar i sortir de l’editor

Un cop realitzades les modificacions, desem els canvis i sortim de l'editor.

4. Reiniciar el servei SSH

Per aplicar la nova configuració, reiniciem el servei SSH amb la següent comanda:

$ systemctl restart sshd.service

Finalment crearem un directori per guardar els backups amb la comanda:

$ mkdir /backup/backup-rsync

Una vegada acabada la configuració, podem anar a la màquina des d’on volem fer el backup i fer la connexió ssh mitjançant rsync amb la comanda:  
  
$ rsync -avz --delete -e ssh /root root@10.0.4.10:~/backup/backup-rsync

rsync: Eina de línia de comandes per sincronitzar fitxers i directoris.

-a: Mode arxiu (archive mode). Conserva permisos, enllaços simbòlics, dates de modificació, propietaris, etc.

-v: Sortida detallada (verbose), mostra el que està fent durant la sincronització.

-z: Comprimeix les dades durant la transferència per fer-la més ràpida (especialment útil a través de xarxa).

--delete: Esborra del destí els fitxers que ja no existeixen a l’origen.

-e ssh: Indica que es vol utilitzar SSH com a mètode de transport segur per enviar les dades.

/root/: La barra final (/) indica que es volen sincronitzar els continguts del directori /root, i no el directori en si mateix.

root@10.0.4.10:/backup/backup-rsync/: Ruta de destinació a la màquina remota, on es copiaran els fitxers. En aquest cas, es fa com a usuari root a la màquina Backup amb IP 10.0.4.10.

Posem la contrasenya root de la maquina del back up i si es correcta ens sortirà el missatge següent:  
  
sending incremental file list

root/

root/.bash\_history

root/.bashrc

root/.lesshst

root/.profile

root/.selected\_editor

root/139,445

root/backingup.txt

root/prueba2.txt

root/samba\_traffic.pcap

root/servidor\_ssh.pcap

root/status\_samba\_server.txt

root/tcpdump\_server.txt

root/.local/

root/.local/share/

root/.local/share/nano/

root/.ssh/

root/.ssh/known\_hosts

sent 10.359 bytes received 291 bytes 4.260,00 bytes/sec

total size is 34.711 speedup is 3,26

Per comprovar que s’ha fet el backup, a la nostra maquina backup executem:  
  
$ tree

Aquesta comanda ens permet tenir una visió en forma d’arbre de tots els fitxers i directoris del nostre sistema (fitxer “tree-after-backup.txt”):  
  
.

├── backup

│ └── backup-rsync

│ └── root

│ ├── 139,445

│ ├── backingup.txt

│ ├── prueba2.txt

│ ├── samba\_traffic.pcap

│ ├── servidor\_ssh.pcap

│ ├── status\_samba\_server.txt

│ └── tcpdump\_server.txt

└── tree-after-backup.txt

4 directories, 8 files

Si comparem amb el tree de la maquina server (fitxer “tree-server-samba.txt”):  
  
.

├── 139,445

├── backingup.txt

├── prueba2.txt

├── samba\_traffic.pcap

├── servidor\_ssh.pcap

├── status\_samba\_server.txt

├── tcpdump\_server.txt

└── tree-server-samba.txt

1 directory, 8 files

veiem que els continguts a /backup/backup-rsync son exactament iguals.

BORGBACKUP:

Borgbackup, al igual que rsync, es una eina que permet crear copies de seguretat dels nostres fitxers i directoris. A diferència de rsync, brogbackup treballa amb repositoris que es poden encriptar.

Primer instal·larem borgbackup amb l comanda següent:  
  
$ sudo apt install borgbackup

Ara caldrà inicialitzar un repositori de borgbackup. Hi ha dues formes:  
  
- Respositori local, amb enciptació repokey:

$ borg init --encryption=repokey-blake2 /path/repositori

Hi ha d’altres amb encriptació com repokey, repokey-blake o keyfile. Peò la més segura i la recomandada segons forums de borgbackups és la de repokey-blake2 degut a la seva opció per entorns on es vulgui separar la clau del repositori.

- Respositori local, sense encriptació:

$ borg init --encryption=none /path/repositori

L’executem a la carpeta anteriorment creada amb:  
  
$ borg init --encryption=repokey-blake2 /backup/backup-borg

i ens demanarà generar una PASSPHRASE, en el nostre cas és:  
  
seax2025

Aquesta passphrase serà necessaria per accedir a la repo juntament amb la repokey.

Ara, crearem un backup del nostre root amb la comanda:  
  
$ borg create --stat --progress /backup/::nou-backup /root

nou-backup és el nom que li donarem al backup de la repo.

/root es la carpeta de la qual volem fer el backup

Ens demanarà introduir el passphrase que hem configurat abans (seax2025)

root@backup:~# borg create --stat --progress /backup/::nou-backup /root

Enter passphrase for key /root/backup/backup-borg:

Enter passphrase for key /root/backup/backup-borg:

Initializing cache transaction: Reading config

Initializing cache transaction: Reading chunks

Initializing cache transaction: Reading files

Saving files cache

Saving chunks cache

Saving cache config

------------------------------------------------------------------------------

Repository: /root/backup/backup-borg

Archive name: nou-backup

Archive fingerprint: c99b54dfb8a5a741e441d51ebc409cf369dfaf161ef973cd8b171db8e23952bd

Time (start): Tue, 2025-05-20 17:14:38

Time (end): Tue, 2025-05-20 17:14:38

Duration: 0.06 seconds

Number of files: 29

Utilization of max. archive size: 0%

-----------------------------------------------------------------------

Original size Compressed size Deduplicated size

This archive: 38.44 kB 18.20 kB 17.43 kB

All archives: 37.91 kB 17.67 kB 20.16 kB

Unique chunks Total chunks

Chunk index: 25 28

-----------------------------------------------------------------------

root@backup:~# exit

Per comprobar que el backup s’ha fet correctament podem llistar els backups que tenim actualment a la repo:  
  
$ borg list /backup/backup-borg  
  
On podem veure que el backup “nou-backup” s’ha fet correctament (es pot veur eal fitxer adjunt “llistar-backups-borg.txt”):

Enter passphrase for key /root/backup/backup-borg:

nou-backup Tue, 2025-05-20 17:14:38 [c99b54dfb8a5a741e441d51ebc409cf369dfaf161ef973cd8b171db8e23952bd]

AUTOMATITZACIÓ AMB CRON:  
  
Utilitzarem cron per automatitzar els backups segons hores/dates determinades:  
  
Primer modificarem el fitxer crontatb amb:  
  
$ crontab -e  
  
Ens demanarà l’editor que volguem usar, excollim 1 (nano):  
  
I afegim la comanda seguent:  
  
30 18 \* \* \* borg create --stats --progress /backup/backup-borg::auto-$(date +\%Y-\%m-\%d) /root >> /var/log/borg-backup.log 2>&1

Això fa el backup cada dia a les 18:30 i desa l’output i errors a /var/log/borg-backup.log per si volem revisar.

Com estem usantt encriptació (--encryption=repokey-blake2), Borg nst demanarà la passphrase.

Per evitar això en mode cron, hem de posar la passphrase en una variable d'entorn segura:  
  
Creem un script, per exemple a /usr/local/bin/[backup-borg.sh](http://backup-borg.sh):  
  
#!/bin/bash

export BORG\_PASSPHRASE="seax2025"

/usr/bin/borg create --stats --progress /backup/backup-borg::auto-$(date +%Y-%m-%d) /root

Li donem permisos d’execució:  
  
chmod +x /usr/local/bin/backup-borg.sh

I afegim el següent a crontab:  
  
30 18 \* \* \* /usr/local/bin/backup-borg.sh >> /var/log/borg-backup.log 2>&1

Per comprovar que s’ha executat correctament el backup, llistem els backups que tenim actualment:  
  
$ borg list ~/backup/backup-borg

I veurem com el backup automatitzat per a les 18:30 s’ha creat correctament:  
  
root@backup:~# borg list ~/backup/backup-borg

Enter passphrase for key /root/backup/backup-borg:

nou-backup Tue, 2025-05-20 17:14:38 [c99b54dfb8a5a741e441d51ebc409cf369dfaf161ef973cd8b171db8e23952bd]

auto-2025-05-20 Tue, 2025-05-20 18:30:02 [1ce8f6f201ca7f5d24f4df833f67d05493577163158a719b487ad97585de9ac8]

root@backup:~# exit

I per confirmar, podem veure també el contingut dels log creats:  
  
------------------------------------------------------------------------------

Repository: /root/backup/backup-borg

Archive name: auto-2025-05-20

Archive fingerprint: 1ce8f6f201ca7f5d24f4df833f67d05493577163158a719b487ad97585de9ac8

Time (start): Tue, 2025-05-20 18:30:02

Time (end): Tue, 2025-05-20 18:30:02

Duration: 0.06 seconds

Number of files: 32

Utilization of max. archive size: 0%

------------------------------------------------------------------------------

Original size Compressed size Deduplicated size

This archive: 58.68 kB 23.79 kB 6.82 kB

All archives: 96.04 kB 40.92 kB 29.95 kB

Unique chunks Total chunks

Chunk index: 33 60

------------------------------------------------------------------------------

Bibliografia:

<https://serverspace.ca/support/help/configuring-samba-on-debian/>

<https://unix.stackexchange.com/questions/180814/how-to-use-rsync-with-samba-share>

<https://www.youtube.com/watch?v=t18-C6f9y5Q>

<https://download.samba.org/pub/rsync/INSTALL.html>