Compte rendu stage 2 juin

Aujourd'hui, mon premier jour j'ai découvert mon environnement de travail ainsi que la tâche importante qui va porter sur un projet de renouvellement des serveurs des écoles.

Sommaire

Installation debian 13 :
Nom des écoles : srv-ecole
domaine : exterieur
mdp root : Nadir&73200
Nom utilisateur : ntic
mdp : Nadir&73200
methode de partitionnement : disque dur entier
disque dur : PNY 250 gb
partition de disques : Partition /home, /var et /tmp séparées
logiciels sélectionné par default :

- utilitaires usuel

logiciels rajouté :

- serveur SSH

Fin d'installation.

Addresse ip fixe : 10.61.0.254/16

Configuration des vlan sur le serveur.

Sur ma machine j'ai suivi ces étapes :

```
sudo apt install vlan
sudo modprobe 8021q
sudo ip link add link eth0 name eth0.36 type vlan id 36
sudo ip addr add 10.61.0.10/24 dev eth0.36
sudo ip link set dev eth0.36 up
```

sur le serveur :

```
apt install vlan
modprobe était introuvable j'ai du installer le paquet locate  :
apt install locate
updatedb
locate modprobe
/usr/sbin/modprobe 8021q
```

Configuration de l'interface du serveur :

interface école

```
rename enp4s0=int-ecole ou
allow-hotplug int-ecole
iface int-ecole inet static
      address 10.61.0.254
      netmask 255.255.0.0
      up ifup int-internet
```

interface externe

```
rename enp4s0.2=int-internet
auto int-internet
iface int-internet inet dhcp
   pre-up ip link add link int-ecole name int-internet type vlan id 2
   up ip link set dev int-internet up
   down ip link set dev int-internet down
   post-down ip link delete int-internet
```

pour les test j'ai arreter et redemarrer les interface avec les commandes

- ifdown int-ecole = arreter les interfaces int école et internet car c'est la même interface physique.
- ifup int-ecole = redémarre seulement ecole
- ifup int-internet = permet de redémarrer l'interface internet aussi.

comment mettre en place le dhcp et dns

installation des paquet nécessaires

sudo apt update
sudo apt install dnsmasq resolvconf dnsutils

création des fichiers

touch /etc/dnsmasq-dhcphosts
touch /etc/dnsmasq-hosts

copie de sécurité dans un autre fichier

cp /etc/dnsmasq.conf /etc/dnsmasq.conf.bak

Configuration
nano /etc/dnsmasq.d/debnas.conf
Configuration file for dnsmasq.

By default, dnsmasq will send queries to any of the upstream
servers it knows about and tries to favour servers to are known
to be up. Uncommenting this forces dnsmasq to try each query
with each server strictly in the order they appear in
/etc/resolv.conf
strict-order

# Add local-only domains here, queries in these domains are answered
# from /etc/hosts or DHCP only.
local=/ecole/

Set this (and domain: see below) if you want to have a domain
automatically added to simple names in a hosts-file.
expand-hosts

# Set the domain for dnsmasq. this is optional, but if it is set, it
# does the following things.
# 1) Allows DHCP hosts to have fully qualified domain names, as long
# as the domain part matches this setting.
# 2) Sets the "domain" DHCP option thereby potentially setting the
# domain of all systems configured by DHCP
# 3) Provides the domain part for "expand-hosts"
domain=ecole

# interfaces autorisé pour dns LAN ecole
interface=enp4s0
#interface=tun0

Resolution de nom propre à dnsmarq
resolv-file=/etc/dnsmasq-dns.conf

Extra options

```
cache-size=500
neg-ttl=60

# never forward plain names
domain-needed

# never forward addresses in the non-routed address spaces
bogus-priv
filterwin2k

# query with each server strictly in the order in resolv.conf
strict-order


#dhcp-option=252,http://wpad.ecole/wpad.dat

dhcp-range=10.61.1.0,10.61.1.255,255.255.0.0,8h
dhcp-option=option:router,10.61.0.254
dhcp-hostsfile=/etc/dnsmasq-dhcphosts

dhcp-option=option:domain-search,ecole,public.albertville.fr
dhcp-option=15,"ecole"
dhcp-option=option:ntp-server,10.61.0.254
dhcp-option=6,10.61.0.254
```

DNS Configuration manuel

```
host-record=srv-ecole.ecole,10.61.0.254
cname=eevr.ecole,srv-ecole.ecole
```

/etc/dnsmasq-dns.conf

```
 Voir quel DNS :
# OpenDNS pour la famille =
#    208.67.222.123
#    208.67.220.123
# DNS Cloudflare sans blocage :
#    DNS primaire: 1.1.1.1
#    DNS secondaire: 1.0.0.1
# DNS Cloudflare, bloquant uniquement les logiciels malveillants :
#    DNS primaire: 1.1.1.2
#   DNS secondaire: 1.0.0.2
# DNS Cloudflare, blocage des logiciels malveillants et du contenu pour adultes :
#    DNS primaire: 1.1.1.3
#    DNS secondaire: 1.0.0.3
nameserver 192.168.192.253
```

cat /var/lib/misc/dnsmasq.leases

ln -s /var/lib/misc/dnsmasq.leases /etc/dnsmasq.leases

interface école

```
rename enp4s0=int-ecole
allow-hotplug int-ecole
iface int-ecole inet static
      address 10.61.0.254
      netmask 255.255.0.0
      up ifup int-internet
```

interface externe

```
rename enp4s0.2=int-internet
auto int-internet
iface int-internet inet dhcp
   pre-up ip link add link int-ecole name int-internet type vlan id 2
   up ip link set dev int-internet up
   down ip link set dev int-internet down
   post-down ip link delete int-internet
```

ipv6

nano /etc/sysctl.d/local.conf

et.ipv6.conf.all.disable_ipv6 = 1

net.ipv6.conf.default.disable_ipv6 = 1

net.ipv4.ip_forward=1

test en ecrivant les regles au niveau systeme

echo "1" > /proc/sys/net/ipv4/ip_forward

nftables

apt install nftables

systemctl enable nftables.service

nano /root/nftables.ruleset.sh

```
#!/usr/sbin/nft -f

# # Exécution :
# /root/nftables.ruleset.sh
#
# # vérification
# nft list ruleset
#
# # Sauvegarde : NON, ne pas utiliser, erreur au démarrage
# nft list ruleset > /etc/nftables.conf
# lancer dans /etc/network/interfaces

flush ruleset

table inet filter {
        chain input {
                type filter hook input priority 0;
                                policy drop;

                                # connexions établies
                                ct state established accept

                                # looback interface
                                iifname lo accept

                                # icmp
                                ip protocol icmp accept
```

```
                # services réseau ouverts pour SSH, HTTP, HTTPS
                # port 53 ouvert car serveur dns et dhcp et ntp pour LAN ecole
                # port 1194 pour openvpn
                tcp dport {ssh, 53, http, https} ct state new accept
                udp dport {53, ntp,1194} ct state new accept
                # Serveur DHCP
                iifname int-ecole udp sport 68 udp dport 67 ct state new accept
                # Serveur samba
                #iifname int-ecole ct state new accept
                iifname != int-internet tcp dport {445, 139} ct state new accept
                #iifname != int-internet udp dport {137,138} ct state new accept
    }
    chain forward {
        type filter hook forward priority 0;
                policy drop;
# connexions établies
                ct state established accept

                # icmp
                ip protocol icmp accept

                # services réseau utilisés DNS, NTP, HTTP, HTTPS, mail smtp
                tcp dport {53, http, https, 25, 587, 993, 995} ct state new accept
                udp dport {53, ntp} ct state new accept

                                # VPN mairie
                ip daddr 154.45.230.174/32 udp dport {1190-1199} ct state new accept

                                # Autoriser SSH et TighVNC
                                iifname tun0 tcp dport {22,5900-5909} ct state new accept
    }
    chain output {
        type filter hook output priority 0;
```

```
                policy drop;

                # connexions établies
                ct state established accept

                # looback interface
                oifname lo accept

                # icmp
                ip protocol icmp accept

                # services réseau utilisés SSH, DNS, NTP, HTTP, HTTPS, mail smtp,
proxyecole(3128)
                tcp dport {ssh,53, http, https, 25, 587, 993, 995, 3128} ct state new accept
                udp dport {53, ntp} ct state new accept
                # Serveur DHCP
                oifname int-ecole ip saddr 10.61.0.254/32 udp sport 67 udp dport 68 ct state
new accept
        }
}
table ip nat {
chain prerouting {
        type nat hook prerouting priority 0; policy accept;
        }

        chain postrouting {
                type nat hook postrouting priority 0; policy accept;
                masquerade
                #ip saddr 10.61.0.0/24 oifname int-internet snat to 192.168.192.253
                ip saddr 10.61.0.0/24 oifname int-internet snat to 192.168.192.175
        }
}
```

Mise à jour auto

Lien utile : https://wiki.debian.org/fr/unattended-upgrades

Installation de unattended-upgrades
sudo apt-get install unattended-upgrades

nano /etc/apt/apt.conf.d/50unattended-upgrades
Unattended-Upgrade::Origins-Pattern {
"origin=Debian,codename=${distro_codename},label=Debian";
"origin=Debian,codename=${distro_codename},label=Debian-Security";
"origin=Debian,codename=${distro_codename}-security,label=Debian-Securi>
"o=*";

Unattended-Upgrade::Package-Blacklist {

Unattended-Upgrade::Mail "root";

Unattended-Upgrade::Remove-Unused-Dependencies "true";

Unattended-Upgrade::Automatic-Reboot "true";

Unattended-Upgrade::Automatic-Reboot-Time "02:00";

nano /etc/apt/apt.conf.d/02periodic
// Control parameters for cron jobs by /etc/cron.daily/apt //

// Enable the update/upgrade script (0=disable)
APT::Periodic::Enable "1";

// Do "apt-get update" automatically every n-days (0=disable)
APT::Periodic::Update-Package-Lists "1";

// Do "apt-get upgrade --download-only" every n-days (0=disable)
APT::Periodic::Download-Upgradeable-Packages "1";

// Run the "unattended-upgrade" security upgrade script
// every n-days (0=disabled)
// Requires the package "unattended-upgrades" and will write
// a log in /var/log/unattended-upgrades
APT::Periodic::Unattended-Upgrade "1";

// Do "apt-get autoclean" every n-days (0=disable)
APT::Periodic::AutocleanInterval "21";

voir les logs

less /var/log/unattended-upgrades/unattended-upgrades.log

less /var/log/unattended-upgrades/unattended-upgrades-dpkg.log

Postfix

apt-get install postfix logwatch

dpkg-reconfigure postfix

postfix :

choisir système satelite

nom de courrier = ecole.XXX ou XXX et l'ecole ex: ecole.EEPC

serveur relais smtp = mail3.albertville.fr:587

destinataire des courrier root = ntic.albertville.fr

Autre destinations = vide

faut t'il forcer les maj synchronisées = non

réseau interne :127.0.0.1

ipv4

/etc/postfix/main.cf

compatibility_level = 3.9

smtpd_banner = $myhostname ESMTP $mail_name (Debian)

inet_protocols = all

mynetworks_style = host

mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

mydestination = $myhostname, localhost.albertville.fr, localhost

mailbox_size_limit = 0

mailbox_command =

alias_maps = hash:/etc/aliases

alias_database = hash:/etc/aliases

biff = no

recipient_delimiter = +

relayhost = smtp2.albertville.fr:587

cyrus_sasl_config_path = /etc/postfix/sasl

smtpd_tls_key_file = /etc/ssl/private/ssl-cert-snakeoil.key

smtpd_tls_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem

smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

smtp_tls_CApath = /etc/ssl/certs

smtp_sasl_auth_enable = yes

smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd

smtp_sasl_security_options = noanonymous

smtp_sasl_mechanism_filter =

smtp_tls_security_level = encrypt

smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination

myhostname = srv-ecole.ecole.albertville.fr

inet_interfaces = loopback-only

smtp_generic_maps = hash:/etc/postfix/generic

append_dot_mydomain = no

readme_directory = no

nano /etc/postfix/sasl/sasl_passwd

smtp2.albertville.fr:587 stagesi:Nadir&73200

revoir chmod et owner pour /etc/postfix/sasl/sasl_passwd

chmod o-r /etc/postfix/sasl/sasl_passwd

postmap /etc/postfix/sasl/sasl_passwd

Pour la translation du courriel, on crée le fichier /etc/postfix/generic et on y place :

mettre utilisateur@hostname.domainname du serveur

root@srv-ecole.ecole stagesi@albertville.fr

root@srv-ecole.ariane.intra stagesi@albertville.fr

myserver# postmap hash:/etc/postfix/generic

et n'autoriser que root lui-même à y accéder en lecture et écriture :

chmod -R 600 /etc/postfix/sasl

Il ne reste plus qu'à redémarrer le serveur Postfix pour qu'il prenne les nouveaux paramètres :

systemctl restart postfix

Test d’envoi de mail

echo "test d'envoi" |mail stagesi@albertville.fr --subject='Test postfix'

Openvpn

apt install openvpn

pkiDir="/etc/openvpn/easy-rsa-pki"

vars="/etc/openvpn/vars"

mkdir ${pkiDir}

easyrsaDir="/usr/share/easy-rsa"

cd ${easyrsaDir}

vi /etc/openvpn/easy-rsa-pki/vars

set_var EASYRSA_CA_EXPIRE 7300

set_var EASYRSA_CERT_EXPIRE 7300

set_var EASYRSA_CRL_DAYS 7300

set_var EASYRSA_REQ_COUNTRY "FR"

set_var EASYRSA_REQ_PROVINCE "FRANCE"

set_var EASYRSA_REQ_CITY "Albertville"

set_var EASYRSA_REQ_ORG "albertville.fr"

set_var EASYRSA_REQ_EMAIL "ntic@albertville.fr"

set_var EASYRSA_REQ_OU "Commune"

<eof>

mkdir /etc/openvpn/private

mkdir /etc/openvpn/certs

mkdir -p /etc/openvpn/easy-rsa-pki

cd /usr/share/easy-rsa

./easyrsa --batch=0 --pki-dir=/etc/openvpn/easy-rsa-pki --vars=/etc/openvpn/easy-rsa-pki/vars init-pki

openvpn --genkey secret /etc/openvpn/private/vpn-ta.key

EasyRSA Version Information

Version: 3.2.2

Generated: Sat Feb 1 07:22:55 CST 2025

SSL Lib: OpenSSL 3.5.0 8 Apr 2025 (Library: OpenSSL 3.5.0 8 Apr 2025)

Git Commit: 8de63429e6c70e4c573aad291fb0ca3cdba763bd

Source Repo: https://github.com/OpenVPN/easy-rsa

Host: 3.2.2 | nix | Linux | /bin/bash

Etape non réussie : # Generate ta.key for additional security beyond SSL/TLS, protects from UDP flood.

Openvpn tuto youtube

https://www.youtube.com/watch?app=desktop&v=BqdHUjH1nwU&t=866s

Création des certificats

ln -s /usr/share/easy-rsa /etc/openvpn/scripts

nano /etc/openvpn/vars

set_var EASYRSA_CA_EXPIRE 7300

set_var EASYRSA_CERT_EXPIRE 7300

set_var EASYRSA_CRL_DAYS 7300

set_var EASYRSA_REQ_COUNTRY "FR"

set_var EASYRSA_REQ_PROVINCE "FRANCE"

set_var EASYRSA_REQ_CITY "Albertville"

set_var EASYRSA_REQ_ORG "albertville.fr"

set_var EASYRSA_REQ_EMAIL "ntic@albertville.fr"

set_var EASYRSA_REQ_OU "Commune"

On renomme on on fait une lien vers le dernier certicat "ssl" (le plus récent) en openssl.cnf ex:
ln -s /etc/openvpn/scripts/openssl-1.0.0.cnf /etc/openvpn/scripts/openssl.cnf

On génère les certificats (attention au message 'clean-all'
cd /etc/openvpn/scripts
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
openvpn --genkey --secret keys/ta.key

Private-Key and Public-Certificate-Request files created.

Your files are:

* req: /etc/openvpn/easy-rsa/pki/reqs/serveur.req

* key: /etc/openvpn/easy-rsa/pki/private/serveur.key

Installer les paquets nécessaires
apt update

apt install openvpn easy-rsa -y

Préparer Easy-RSA

mkdir -p /etc/openvpn/easy-rsa

cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/

cd /etc/openvpn/easy-rsa/

Corriger le fichier vars (important)

Ouvre /etc/openvpn/easy-rsa/vars avec un éditeur (nano par exemple) :

nano vars

set_var EASYRSA_CA_EXPIRE 7300

set_var EASYRSA_CERT_EXPIRE 7300

set_var EASYRSA_CRL_DAYS 7300

set_var EASYRSA_REQ_COUNTRY "FR"

set_var EASYRSA_REQ_PROVINCE "FRANCE"

set_var EASYRSA_REQ_CITY "Albertville"

set_var EASYRSA_REQ_ORG "albertville.fr"

set_var EASYRSA_REQ_EMAIL "ntic@albertville.fr"

set_var EASYRSA_REQ_OU "Commune"

./easyrsa init-pki

./easyrsa build-ca nopass

Common name : srv-ecole-ca

./easyrsa gen-req serveur nopass

./easyrsa sign-req server serveur

./easyrsa gen-dh

openvpn --genkey secret ta.key

mkdir -p /etc/openvpn/server

cp pki/ca.crt /etc/openvpn/server/

cp pki/issued/serveur.crt /etc/openvpn/server/

cp pki/private/serveur.key /etc/openvpn/server/

cp pki/dh.pem /etc/openvpn/server/

cp ta.key /etc/openvpn/server/

nano /etc/openvpn/server/server.conf

port 1194

proto udp

dev tun

ca ca.crt

cert serveur.crt

key serveur.key

dh dh.pem

tls-auth ta.key 0

cipher AES-256-CBC

auth SHA256

topology s ubnet

server 10.8.0.0 255.255.255.0

```
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"

keepalive 10 120
persist-key
persist-tun

user nobody
group nogroup

status /run/openvpn/server.status
log-append /var/log/openvpn.log
verb 3

explicit-exit-notify 1



# Activer et démarrer OpenVPN
systemctl daemon-reload
systemctl enable openvpn-server@server
systemctl start openvpn-server@server
systemctl status openvpn-server@server

# Créer un certificat client
./easyrsa gen-req client01 nopass
./easyrsa sign-req client client01

nano /etc/openvpn/client01.ovpn
lient
dev tun
proto udp
remote 10.61.0.254 1194
```

resolv-retry infinite

nobind

persist-key

persist-tun

remote-cert-tls server

cipher AES-256-CBC

auth SHA256

key-direction 1

verb 3

<ca>

Colle ici le contenu de /etc/openvpn/server/ca.crt

-----BEGIN CERTIFICATE-----

MIIDTjCCAjagAwIBAgIUPNwuJuWRJWS8+rP3El0cS+As7lAwDQYJKoZIhvcNAQEL

BQAwFzEVMBMGA1UEAwwMc3J2LWVjb2xlLUNBMB4XDTI1MDYxMjA4MTQ1MVoXDT
Q1

MDYwNzA4MTQ1MVowFzEVMBMGA1UEAwwMc3J2LWVjb2xlLUNBMIIBIjANBgkqhkiG

9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxx7LvjnMmk2HAoxIUYHGjxhE2KbRGPaNuk3E

H7c1KMn0cqtdLHPd+wTmYS+IyO3ZVRe73y+fi1vGXkGgao/uASX8gzfZDK00vt40

QdcgEmcBpGHzwK/jXnCehalDUCUVC1lRABoBQ6JxaTcRRqUGG/Tt/mi1zk3iA9U6

fk87RIUjosg04srRIld+aTpKq5DD+iFMtLNk2XhSUg5nrwMS8a/rvysGlJe7TfGB

g3CuoirRqu/Yv9exwJI6b1O1qs8QCar2is8PKNtkGmtmRWY17DHXgByWv0maH8VK

3yKIxMsOK+RJThMJWjiXJXbdrTdKKVnq7ZFktclvi819+5GvpwIDAQABo4GRMIGO

MAwGA1UdEwQFMAMBAf8wHQYDVR0OBBYEFJRJWaOUAQ1DxcErQoR1OkYvIX1TMFI
G

A1UdIwRLMEmAFJRJWaOUAQ1DxcErQoR1OkYvIX1ToRukGTAXMRUwEwYDVQQDDAxz

cnYtZWNvbGUtQ0GCFDzcLiblkSVkvPqz9xJdHEvgLO5QMAsGA1UdDwQEAwIBBjAN

BgkqhkiG9w0BAQsFAAOCAQEALGQDY0pRw6gcGD0dmojJz5XYKB+uX1xPC38dq3XN

7is0tIMVMXU0dSfTlOwq8NA0LYAuwDNS1rxifkS+HhKJtiR+xQW1Dz/5V+VmrjiA

7KMc/Etva0VAeyqSsauxJphSwX0o4jIu9WfX1Uq8/4xknlJ9uYhjcRaAxL/OIySH

rFIL2tPAEql3VdjVy5A8im4UVMS+y4r/dr34lV7pzuKNLIXBRkB4Vu7ZgiJgRsIt

yj9p+2RXRW6GLBdDLaY0jxwcwsKoVDUPdt80Hi46nYXqUEjts7sfXYpSTN0ggR+8

wR4FJQVggCxBG3YFxFaTrVWK+xDGxh0qolcelc9VrauVfA==

-----END CERTIFICATE-----

</ca>

<cert>

Colle ici le contenu de /etc/openvpn/client1.crt

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

42:49:8c:4d:e8:23:92:e6:6b:07:2b:bb:18:1d:bd:c5

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=srv-ecole-CA

Validity

Not Before: Jun 12 08:34:14 2025 GMT

Not After : Jun 7 08:34:14 2045 GMT

Subject: CN=client01

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c0:65:7d:d6:13:b8:bc:89:2b:28:99:a6:cd:81:

88:85:60:cb:41:37:aa:26:76:7d:1b:6f:96:0a:6c:

3e:b9:24:9a:86:4d:af:51:5d:1b:93:7d:60:56:8c:

e0:ff:1b:86:2c:9c:1b:e4:c0:57:e2:fe:9b:aa:55:

a8:90:11:05:d6:be:ca:b3:e1:69:00:a4:bb:cb:ae:

51:3d:84:45:27:17:4a:c0:06:3b:df:6e:e3:c1:f3:

8b:7b:c1:76:ab:d9:5f:e3:11:9f:d2:44:70:19:9b:

55:a4:cb:ba:09:53:32:2d:a4:a5:4e:65:26:57:e2:

85:cc:20:ad:23:e5:c3:2f:1d:0e:75:ad:61:2d:6b:

69:7f:d2:ce:ce:1b:36:48:fe:99:d5:b2:71:45:80:

eb:ad:79:64:1b:45:18:7e:81:3c:99:b8:5f:98:ff:

eb:f1:1f:a3:2f:98:71:9a:ac:96:33:2e:75:1e:af:

f2:f8:74:ca:83:0e:c1:3c:30:3e:18:e7:89:5c:bd:

32:ae:7e:27:5a:fa:4b:93:2b:11:af:ea:23:b7:7c:

55:e8:18:0f:ab:4c:99:ac:53:04:64:92:7d:e7:15:

b8:ad:21:85:4c:d4:4a:5d:0c:16:7e:92:d3:7c:49:

ab:26:dd:83:28:4d:e1:b8:fe:9c:22:f0:58:78:a4:

4a:f9

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Subject Key Identifier:

0A:8B:DB:70:3F:28:0A:E8:5A:06:2E:79:7F:6E:C0:25:AA:70:C3:55

X509v3 Authority Key Identifier:

keyid:94:49:59:A3:94:01:0D:43:C5:C1:2B:42:84:75:3A:46:2F:21:7D:53

DirName:/CN=srv-ecole-CA

serial:3C:DC:2E:26:E5:91:25:64:BC:FA:B3:F7:12:5D:1C:4B:E0:2C:EE:50

X509v3 Extended Key Usage:

TLS Web Client Authentication

X509v3 Key Usage:

Digital Signature

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

1b:20:44:ad:83:8a:e5:13:12:80:f4:cc:55:a7:a8:af:b0:2d:

71:29:69:d2:03:05:9c:cf:68:1b:f1:9e:3e:6f:6c:3d:d7:a4:

85:46:c1:98:33:19:d6:7f:3c:88:70:3d:62:88:c6:cd:3b:c4:

24:bc:b2:0a:03:49:57:f6:40:60:b2:f4:92:f7:54:93:b7:fe:

b4:16:bc:19:b0:a0:7e:dc:9a:64:39:61:f1:fd:c9:c0:26:f7:

ee:23:01:58:30:5a:df:e1:85:c0:06:f7:f8:78:ed:a1:f5:a9:

d3:ec:37:22:49:50:61:1c:91:5f:3e:26:6f:36:ba:53:70:51:

92:cf:c0:45:b4:de:90:90:d8:31:12:8e:0f:35:88:bd:85:24:

83:36:e1:39:40:8d:ff:46:1e:15:cd:ea:87:51:88:1f:5e:a5:

28:e1:b5:41:49:80:76:32:78:b4:26:60:21:28:2b:27:01:b1:

37:5e:3a:f5:85:db:e1:89:ec:78:4e:f0:b9:b7:7f:10:e8:a7:

64:33:4b:ee:ec:7a:3a:46:c3:0d:f1:2d:3c:96:29:6b:c6:45:

96:d2:69:24:bd:70:16:45:4e:6d:7b:ec:e2:d3:74:61:f8:18:

a5:d4:b4:cb:94:3c:56:6a:48:7f:a4:a9:ea:90:78:4b:1b:c2:

1b:fb:2e:ca

-----BEGIN CERTIFICATE-----

MIIDWDCCAkCgAwIBAgIQQkmMTegjkuZrByu7GB29xTANBgkqhkiG9w0BAQsFADAX

MRUwEwYDVQQDDAxzcnYtZWNvbGUtQ0EwHhcNMjUwNjEyMDgzNDE0WhcNNDUwNjA
3

MDgzNDE0WjATMREwDwYDVQQDDAhjbGllbnQwMTCCASIwDQYJKoZIhvcNAQEBBQA
D

ggEPADCCAQoCggEBAMBlfdYTuLyJKyiZps2BiIVgy0E3qiZ2fRtvlgpsPrkkmoZN

r1FdG5N9YFaM4P8bhiycG+TAV+L+m6pVqJARBda+yrPhaQCku8uuUT2ERScXSsAG

O99u48Hzi3vBdqvZX+MRn9JEcBmbVaTLuglTMi2kpU5lJlfihcwgrSPlwy8dDnWt

YS1raX/Szs4bNkj+mdWycUWA6615ZBtFGH6BPJm4X5j/6/Efoy+YcZqsljMudR6v

8vh0yoMOwTwwPhjniVy9Mq5+J1r6S5MrEa/qI7d8VegYD6tMmaxTBGSSfecVuK0h

hUzUSl0MFn6S03xJqybdgyhN4bj+nCLwWHikSvkCAwEAAaOBozCBoDAJBgNVHRME

AjAAMB0GA1UdDgQWBBQKi9twPygK6FoGLnl/bsAlqnDDVTBSBgNVHSMESzBJgBSU

SVmjlAENQ8XBK0KEdTpGLyF9U6EbpBkwFzEVMBMGA1UEAwwMc3J2LWVjb2xlLUNB

ghQ83C4m5ZElZLz6s/cSXRxL4CzuUDATBgNVHSUEDDAKBggrBgEFBQcDAjALBgNV

HQ8EBAMCB4AwDQYJKoZIhvcNAQELBQADggEBABsgRK2DiuUTEoD0zFWnqK+wLXEp

adIDBZzPaBvxnj5vbD3XpIVGwZgzGdZ/PIhwPWKIxs07xCS8sgoDSVf2QGCy9JL3

VJO3/rQWvBmwoH7cmmQ5YfH9ycAm9+4jAVgwWt/hhcAG9/h47aH1qdPsNyJJUGEc

kV8+Jm82ulNwUZLPwEW03pCQ2DESjg81iL2FJIM24TlAjf9GHhXN6odRiB9epSjh

tUFJgHYyeLQmYCEoKycBsTdeOvWF2+GJ7HhO8Lm3fxDop2QzS+7sejpGww3xLTyW

KWvGRZbSaSS9cBZFTm177OLTdGH4GKXUtMuUPFZqSH+kqeqQeEsbwhv7Lso=

-----END CERTIFICATE-----

</cert>

<key>

Colle ici le contenu de /etc/openvpn/private/client1.key

-----BEGIN PRIVATE KEY-----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDAZX3WE7i8iSso

mabNgYiFYMtBN6omdn0bb5YKbD65JJqGTa9RXRuTfWBWjOD/G4YsnBvkwFfi/puq

VaiQEQXWvsqz4WkApLvLrlE9hEUnF0rABjvfbuPB84t7wXar2V/jEZ/SRHAZm1Wk

y7oJUzItpKVOZSZX4oXMIK0j5cMvHQ51rWEta2l/0s7OGzZI/pnVsnFFgOuteWQb

RRh+gTyZuF+Y/+vxH6MvmHGarJYzLnUer/L4dMqDDsE8MD4Y54lcvTKufida+kuT

KxGv6iO3fFXoGA+rTJmsUwRkkn3nFbitIYVM1EpdDBZ+ktN8Sasm3YMoTeG4/pwi
8Fh4pEr5AgMBAAECggEAD2jRkFDaDfeqhkDwNCt4xL4A6YNM1HHPCWCBkuoih++f
lLwqG4kqiUCUc7oq1yPcNjx2m3awU1TzIMxliMxkPFPhplCaeVu4UtLuXM/4Pe5G
pWSabQXTphgchtfy6kapwGUL+OpUVCi1zlIm31JThYZXWxUM4iMZdkTzuRlQ7bfx
fShodX//fB6VKjwlhyDL35dPTxGMrwONnmMgXMCBIy5eHQ/LRFzwgP+zmXjfibR8
JtLF65kh7fAWSnX82jS8N4llOmvuBn/H2lkl+/Ho87oZ91GN7lz8JyHhIEMH625T
UWAyYs2DtQ+JtufyNFSEEYZEh7Uzapr+tJfHcCRtkQKBgQDkI2Fih9rLB5VFFuWo
FUFFWI5tvGacNyA8NqJFGqamVOnUVEKq5ctN9yMPYdNVMW3JJs0or+172hRwyTS/
a1kEA5JIyCGV9CixEzKZZ/rsVFfYABp9XAb4z7enqcu+eQUe+gRH27UNWndSeX+P
/ydfXWeRtE6aeWs3FGFCCg7xhQKBgQDX5KoLVOyBM4S64sui0aUXNpvM/aw+8z1f
ya2RT57MhIawjrrMqyR+rdc9AEy+XpAmwla7V1o3igHc1a6Ew9EGMER7MrrFqdb/
/Ig7KofTkgJRdIYR5iyVZREuSuM4pxEAuBBTx3OvZjVt0cjVWZfpqEeoGjj39LEh
SPaUHoHz5QKBgEfRV3vkFp1pgrUgMyXJoyWIbjXfZFHzDKPH8ydb73BXNNERwXb5
JhoiHZhfDF86UzxKibUwRMuDaIHk5UUJLxmTYj6lOeVx2kl8KKagVB6HoqutxKkI
Cm3TPhZ63lfU0ybgP+67HHDatMty0hRrl2JvDgaRQ1lftb++G6vlbLTdAoGBALXX
Q+KHhSzN194RaLObIRKMTG48u/fJqMgldqwOBBL/DPNpRK1e+T457jDTL9ColYIP
7j2dNb/R3f/De1sYE9bCkOuzrt0OUKkMazJqgD0TniA9pS8uUB8FIZN8QCZXkVqp
rhbix+3UiOwW5rHM5MdJlhFhBNrUnt0KN6ZKi+qBAoGAf0KHq6XKwFyGplT58+Wg
YD06Y1RwKsCplFUK8jnXpf3vKW8a5zJps7tqf8UeIMGYRmQHfya9J15I59iA+egk
ylD+7WdUlXWSICfLRotauDCgedzgxs1mkJd9xZzHQjdMRpM8S5dQRHoFpUpKxmq8
zu43j4iEK/DjgFs+K7LdpaE=
-----END PRIVATE KEY-----
</key>
<tls-auth>
Colle ici le contenu de /etc/openvpn/server/ta.key
-----BEGIN OpenVPN Static key V1-----
0ce72b04856adefe8bca6c6bc3e0759b
f467f4d877423cef16a104084e719fdb
7eb275cdde4eed44115567762b31bb32
a6ce863a7a10589dc27e546c2365f332
4ead4d4c8ecc8e00e269ecb4fda8ce1b
3311cf905b3f1f7b395259d00f0bc75c
9d32f1a67d56d64f244468c976d54607

000da26f6554731104359e4626f674e1

b9c512bdabaf751aa3ea584e94dfac24

3e55f0263e21e29d8b83be29fe7b65d8

ed9d43dc9790b19b7ba4468c901ff315

95b8d0ec247bb021c777dbddfe0efa7e

0b68a9c602fcb1a99d531cb42e7469f0

588c4f92ebc3170dbcee2fd2706eda72

79b364f532dcf58cda642bf390f91fd6

18591a2be6fdeec5e859f96da03fb612

-----END OpenVPN Static key V1-----

</tls-auth>

transferer vers le client01

Chroot pour Openvpn

nano /etc/openvpn/server/server.conf

Test

A vérifier, il me semble que les service fonctionnel est openvpn.service

Activer et démarrer OpenVPN
systemctl daemon-reload

systemctl enable openvpn-server@server

systemctl start openvpn-server@server

systemctl status openvpn-server@server

authentification totp

Installation de totp

apt install libpam-google-authenticator -y

Configuration du compte utilisateur

adduser vpnuser

su - vpnuser

google-authenticator

Nouveau mot de passe :

Retapez le nouveau mot de passe :

passwd : mot de passe mis à jour avec succès

Modifier les informations associées à un utilisateur pour vpnuser

Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut

NOM []: client01

Numéro de chambre []:

Téléphone professionnel []:

Téléphone personnel []:

Autre []:

Is the information correct? [Y/n] yes

exit pour revenir en mode admin

Do you want authentication tokens to be time-based (y/n) y

https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/root@srv-ecole%3Fsecret%3DCBH6F47BW4YULR7EAMRZ67VK4U%26issuer%3Dsrv-ecole

clé

Your new secret key is: CBH6F47BW4YULR7EAMRZ67VK4U

Enter code from app (-1 to skip): -1

Code confirmation skipped

Your emergency scratch codes are:

54707307

93526015

30087504

26956700

30947765

configuration de Pam pour openvpn

nano /etc/pam.d/openvpn

auth required pam_google_authenticator.so

Modifier la configuration OpenVPN pour utiliser PAM

nano /etc/openvpn/server/server.conf

plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so openvpn

client-cert-not-required

username-as-common-name

redemarrer

systemctl restart openvpn-server@server

configurer les alarmes d’un onduleur

authentification google

mkdir /etc/google-auth
apt-get install libpam-google-authenticator

google-authenticator

Your new secret key is: CTLNWHOY7VODGI7L6PVE46OX7A

Enter code from app (-1 to skip): 796532

Code confirmed

Your emergency scratch codes are:

31416433

57530015

92798300

33720609

14158571

Do you want me to update your "/root/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.

Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.

Do you want to enable rate-limiting? (y/n) y

mv ~/.google_authenticator /etc/google-auth/some_username

adduser openvpn

Nouveau mot de passe :

Retapez le nouveau mot de passe :

passwd : mot de passe mis à jour avec succès

Modifier les informations associées à un utilisateur pour openvpn

Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut

NOM []: client01

Numéro de chambre []:

Téléphone professionnel []:

Téléphone personnel []:

Autre []:

Is the information correct? [Y/n] y

su - openvpn

openvpn@srv-ecole:~$ exit

déconnexion

chown -R openvpn /etc/google-auth

nano /etc/pam.d/openvpn
auth requisite /lib/x86_64-linux-gnu/security/pam_google_authenticator.so secret=/etc/google-auth/some_username user=openvpn

account required pam_permit.so

sur la machine client faire sur le fichier client01.ovpn

```
auth-user-pass
  auth-nocache
  reneg-sec 0
```

Btrfs

Définition : système de gestion de fichiers qui journalise et permet les snapshot.

root@srv-ecole:~# fdisk -l

Disque /dev/sdb : 232,89 GiB, 250059350016 octets, 488397168 secteurs

Modèle de disque : Samsung SSD 870

Unités : secteur de 1 × 512 = 512 octets

Taille de secteur (logique / physique) : 512 octets / 512 octets

taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/sdc : 232,89 GiB, 250059350016 octets, 488397168 secteurs

Modèle de disque : Samsung SSD 870

Unités : secteur de 1 × 512 = 512 octets

Taille de secteur (logique / physique) : 512 octets / 512 octets

taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/sda : 232,89 GiB, 250059350016 octets, 488397168 secteurs

Modèle de disque : PNY 250GB SATA S

Unités : secteur de 1 × 512 = 512 octets

Taille de secteur (logique / physique) : 512 octets / 512 octets

taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Type d'étiquette de disque : dos

Identifiant de disque : 0x9cbeaf7e

Périphérique Amorçage Début Fin Secteurs Taille Id Type

/dev/sda1 * 2048 2000895 1998848 976M 83 Linux

/dev/sda2 2002942 488396799 486393858 231,9G f Étendue W95 (LBA)

/dev/sda5 2002944 488396799 486393856 231,9G 8e LVM Linux

Disque /dev/mapper/srv--ecole--vg-root : 18,04 GiB, 19365101568 octets, 37822464 secteurs

Unités : secteur de 1 × 512 = 512 octets

Taille de secteur (logique / physique) : 512 octets / 512 octets

taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/mapper/srv--ecole--vg-var : 6,47 GiB, 6945767424 octets, 13565952 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/mapper/srv--ecole--vg-swap_1 : 7,89 GiB, 8472494080 octets, 16547840 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/mapper/srv--ecole--vg-tmp : 2,77 GiB, 2969567232 octets, 5799936 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/mapper/srv--ecole--vg-home : 196,73 GiB, 211237732352 octets, 412573696 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets

apt install -y btrfs-progs

root@srv-ecole:~# mkfs.btrfs -d raid1 -m raid1 /dev/sdb /dev/sdc
btrfs-progs v6.14
See https://btrfs.readthedocs.io for more information.

Performing full device TRIM /dev/sdb (232.89GiB) ...

Performing full device TRIM /dev/sdc (232.89GiB) ...

NOTE: several default settings have changed in version 5.15, please make sure
this does not affect your deployments:
- DUP for metadata (-m dup)
- enabled no-holes (-O no-holes)
- enabled free-space-tree (-R free-space-tree)

Label: (null)
UUID: f59955a1-bc6d-4920-896f-7d989ca4772f
Node size: 16384
Sector size: 4096 (CPU page size: 4096)
Filesystem size: 465.77GiB
Block group profiles:
Data: RAID1 1.00GiB
Metadata: RAID1 1.00GiB
System: RAID1 8.00MiB
SSD detected: yes
Zoned device: no
Features: extref, skinny-metadata, no-holes, free-space-tree
Checksum: crc32c
Number of devices: 2
Devices:
ID SIZE PATH
1 232.89GiB /dev/sdb
2 232.89GiB /dev/sdc

Définir un label pour notre stockage

btrfs filesystem label /dev/XXX <label>
btrfs filesystem label /dev/XXX <label>

Label: NasVol1
UUID: 9285d260-4b2f-49cc-9e03-0f27e45a7281
Node size: 16384
Sector size: 4096 (CPU page size: 4096)

```
Filesystem size:    465.77GiB
Block group profiles:
  Data:             RAID1            1.00GiB
  Metadata:         RAID1            1.00GiB
  System:           RAID1            8.00MiB
SSD detected:       yes
Zoned device:       no
Features:           extref, skinny-metadata, no-holes, free-space-tree
Checksum:           crc32c
Number of devices:  2
Devices:
   ID        SIZE  PATH
    1   232.89GiB  /dev/sdb
    2   232.89GiB  /dev/sdc
```

Monter par label

mount -L NasVol1 /storage

Vérifier le raid de disques

btrfs filesystem usage /storage

```
Overall:
    Device size:                 465.77GiB
    Device allocated:              4.02GiB
    Device unallocated:          461.76GiB
    Device missing:                0.00B
    Device slack:                  0.00B
    Used:                        288.00KiB
    Free (estimated):            231.88GiB      (min: 231.88GiB)
    Free (statfs, df):           231.88GiB
    Data ratio:                       2.00
    Metadata ratio:                   2.00
    Global reserve:                5.50MiB      (used: 0.00B)
    Multiple profiles:                  no
```

Data,RAID1: Size:1.00GiB, Used:0.00B (0.00%)

/dev/sdb 1.00GiB

/dev/sdc 1.00GiB

Metadata,RAID1: Size:1.00GiB, Used:128.00KiB (0.01%)

/dev/sdb 1.00GiB

/dev/sdc 1.00GiB

System,RAID1: Size:8.00MiB, Used:16.00KiB (0.20%)

/dev/sdb 8.00MiB

/dev/sdc 8.00MiB

Unallocated:

/dev/sdb 230.88GiB

/dev/sdc 230.88GiB

installer ubuntu sur le raid1 /storage pour voir la réaction du raid1 pour sa telecharger ensuite transferer sur le serveur et sur le répertoire /storage avec scp.

Partage

Volume école

btrfs subvolume create /storage/vol.ecole

Dossier école

mkdir /storage/dir.ecole.shadow

mkdir /storage/vol.ecole/share

mkdir /storage/vol.ecole/recycle

Volume enseignant

btrfs subvolume create /storage/vol.enseignant

Dossier enseignant

mkdir /storage/dir.enseignant.shadow

mkdir /storage/vol.enseignant/share

mkdir /storage/vol.enseignant/recycle

Activation des quotas

btrfs quota enable /storage/vol.ecole/

btrfs quota enable /storage/vol.enseignant/

Automatisation d'accès au démarrage la partition filesystem avec acl

nano /etc/fstab

ajouter la ligne :

LABEL=NasVol1 /storage btrfs defaults,acl 0 2

#LABEL=NasVol1 /storage btrfs rw,relatime,compress=lzo,space_cache

tester avec le démontage et le montage avec

- umount
- mount

Ajout des utilisateurs et des groupes

Groupes

groupadd ecole

groupadd enseignant

Utilisateurs

Les élèves :

useradd -m -G ecole -s /bin/bash eleve1

useradd -m -G ecole -s /bin/bash eleve2

enseignant :

useradd -m -G enseignant -s /bin/bash prof1

useradd -m -G enseignant -s /bin/bash prof2

Getfacl

getfacl /storage

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage

owner: root

group: root

user::rwx

group::r-x

other::r-x

getfacl /storage/vol.ecole/

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/vol.ecole/

owner: root

group: root

user::rwx

group::r-x

other::r-x

getfacl /storage/vol.enseignant/

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/vol.enseignant/

owner: root

group: root

user::rwx

group::r-x

other::r-x

getfacl /storage/vol.ecole/share/

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/vol.ecole/share/

owner: root

group: ecole

user::rwx

group::rwx

other::---

getfacl /storage/vol.ecole/recycle/

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/vol.ecole/recycle/

owner: root

group: root

user::rwx

group::rwx

other::---

getfacl /storage/vol.enseignant/share

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/vol.enseignant/share

owner: root

group: root

user::rwx

group::rwx

other::---

getfacl /storage/vol.enseignant/recycle

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/vol.enseignant/recycle

owner: root

group: root

user::rwx

group::rwx

other::---

chmod 755 /storage/dir.enseignant.shadow

root@srv-ecole:~# getfacl /storage/dir.enseignant.shadow

getfacl : suppression du premier « / » des noms de chemins absolus

file: storage/dir.enseignant.shadow

owner: root

group: root

user::rwx

group::r-x

other::r-x

Créer le partage dans Samba

/etc/samba/smb.conf

[global]

server role = standalone server

  workgroup = WORKGROUP

  server string = %h server

  dns proxy = no

  log level = 2

  log file = /var/log/samba/log.%m

  max log size = 1000

  logging = syslog

  panic action = /usr/share/samba/panic-action %d

  encrypt passwords = true

  passdb backend = tdbsam

  obey pam restrictions = no

  unix password sync = no

  passwd program = /usr/bin/passwd %u

  passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .

  pam password change = yes

  socket options = TCP_NODELAY IPTOS_LOWDELAY

  guest account = nobody

  load printers = no

```
   disable spoolss = yes
   printing = bsd
   printcap name = /dev/null

   unix extensions = yes
   wide links = no
   create mask = 0777
   directory mask = 0777
   use sendfile = yes
   aio read size = 16384
   aio write size = 16384
   local master = yes
   time server = yes
   wins support = yes

# ======================= Partages =======================

[enseignant.corbeille]
   path = /storage/vol.enseignant/recycle
   guest ok = no
   read only = yes
   browseable = yes
   inherit acls = yes
   ea support = no
   store dos attributes = no
   printable = no
   create mask = 0664
   force create mode = 0664
   directory mask = 0775
   force directory mode = 0775
   hide special files = yes
   follow symlinks = yes
   hide dot files = yes
```

```
[ecole.corbeille]
   path = /storage/vol.ecole/recycle
   guest ok = no
   read only = yes
   browseable = yes
   inherit acls = yes
   ea support = no
   store dos attributes = no
   printable = no
   create mask = 0664
   force create mode = 0664
   directory mask = 0775
   force directory mode = 0775
   hide special files = yes
   follow symlinks = yes
   hide dot files = yes

[enseignant]
   path = /storage/vol.enseignant/share
   guest ok = no
read only = no
   browseable = yes
   inherit acls = yes
   ea support = no
   store dos attributes = no
   printable = no
   create mask = 0664
   force create mode = 0664
   directory mask = 0775
   force directory mode = 0775
   hide special files = yes
   follow symlinks = yes
```

```
   hide dot files = yes
   vfs objects = btrfs shadow_copy2 recycle
   btrfs: manipulate snapshots = yes
   shadow:basedir = /storage/vol.enseignant
   shadow:snapdir = /storage/dir.enseignant.shadow
   shadow:format = @GMT-%Y.%m.%d-%H.%M.%S-%w
   recycle:repository = /storage/vol.enseignant/recycle
   recycle:keeptree = yes
   recycle:versions = yes
   recycle:exclude = ?~$*,~$*,*.tmp,*.temp,*.TMP

[ecole]
   path = /storage/dir.ecole/share
   guest ok = no
   read only = no
   browseable = yes
   inherit acls = yes
   ea support = no
   store dos attributes = no
   printable = no
   create mask = 0664
   force create mode = 0664
   directory mask = 0775
   force directory mode = 0775
   hide special files = yes
   follow symlinks = yes
hide dot files = yes
   vfs objects = btrfs shadow_copy2 recycle
   btrfs: manipulate snapshots = yes
   shadow:basedir = /storage/vol.ecole
   shadow:snapdir = /storage/dir.ecole.shadow
   shadow:format = @GMT-%Y.%m.%d-%H.%M.%S-%w
   recycle:repository = /storage/vol.ecole/recycle
```

recycle:keeptree = yes

recycle:versions = yes

recycle:exclude = ?~$*,~$*,*.tmp,*.temp,*.TMP

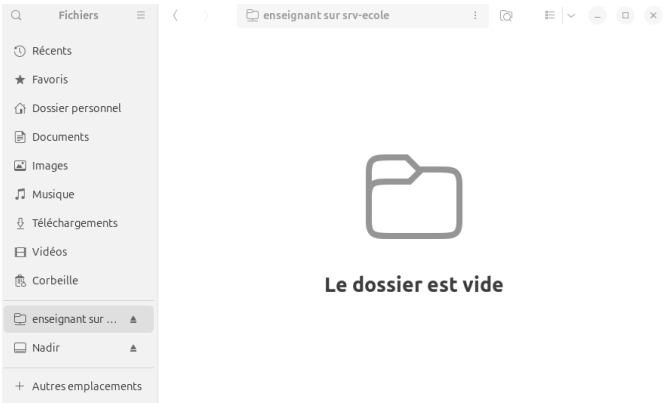
Création de mot de passe samba

Création pour l'utilisateur enseignant :

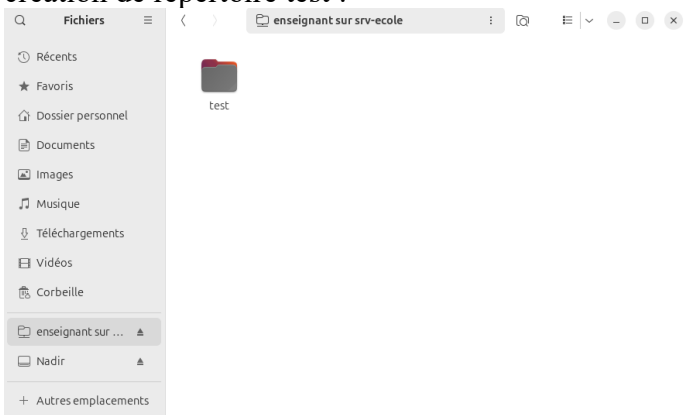
smbpasswd -a enseignant

vérification samba

Afin de vérifier on vérifie dans fichiers en créant un nouveau emplacement :
smb://WORKGROUP;enseignant@srv-ecole/enseignant Enseignant
on se connecte en utilisant le mot de passe que l'on a crée pour l'utilisateur



création de répertoire test :



ls -l /storage/vol.enseignant/share/
total 0
drwxrwx---+ 1 enseignant enseignant 28 20 juin 11:02 test
comme on peut voir le dossier s'est bien crée.

Programmation des sauvegardes et des restaurations

/root/purge-btrfs-snap.sh

```
#!/bin/bash
#
# Script pour supprimer en fonction de l'ages, des snapshots  des sous-volumes BTRFS
# Paramètres : purge-btrfs-snap.sh path
# path = chemin absolu. ex:/storage/dir.ecole.shadow

# afficher la date avec un décalage de x jour avant : date --date '7 days ago' +%Y.%m.%d-%H.%M.%S
# comparet le nom du fichier et non la date du fichier : if [[ "@GMT-2020.04.10-08.18.36" > "@GMT-2020.04.10-08.18.37" ]]; then echo OK; fi

# Max Age of snapshots dayly in days
maxday="7"

# Max Age of snapshot weekly in months
maxweek="4"

# Chemin des snapshots (si non renseigné)
#pathsnap="/storage/dir.ecole.shadow"
pathsnap=""

# Log
logfile="/var/log/snap.log"

# Gestion du chemin en paramètre
if [ "${1}" ] ; then
  #echo "paramètre ${1} existe"
  if [ -d "${1}" ] ; then
    #echo "dossier ${1} existe"
    pathsnap="${1}"
```

```
  else
    echo "Erreur : paramètre path n'est pas un répertoire. fin d'execution" > ${logfile}
    exit 1
  fi
else
  echo "Erreur : paramètre path non renseigné. fin d'execution" > ${logfile}
  exit 1
fi

#echo "maxday=${maxday}"
#echo "maxweek=${maxweek}"
#echo "pathsnap=${pathsnap}"

export logfile
echo "" > ${logfile}

# Gestion de la date limite dans le nom du fichier à comparer
maxdatedayly="${pathsnap}/@GMT-$(date --date """${maxday} days ago""" 
+%Y.%m.%d-%H.%M.%S-%w)"

maxdateweekly="${pathsnap}/@GMT-$(date --date """${maxweek} months ago""" 
+%Y.%m.%d-%H.%M.%S-%w)"

#
# Fonction de suppression de snapshots plus vieux qu'une date donnée.
# fichier = $1
# date limite = $2
#
fDeleteOlderSnapshoThan() {
  pFile="${1}"
  pLimitDay="${2}"

  #echo "pFile = ${1}"
```

```
  #echo "pLimitDay = ${2}"

  # Si nom du fichier plus petit (vieux)  que référence quotidien
  #echo "${pFile} test" >> $logfile
  if [[ "${pFile}"  < "${pLimitDay}" ]] ; then
    # snapshot à supprimer
    echo "${pFile} < ${pLimitDay} à supprimer" >> $logfile
    btrfs subvolume delete "${pFile}"
  else
    echo "${pFile} > ${pLimitDay} conservé" >> $logfile
  fi
}
# export pour utilisation dans le bash lancé par find
export -f fDeleteOlderSnapshoThan

# Recherche des snapshots quotidiens et suppression si plus vieux que maxdatedayly
find $pathsnap -name "@GMT-*-[1-6]" -exec bash -c "fDeleteOlderSnapshoThan {}
${maxdatedayly}" \;

# Recherche des snapshots hebdomadaires et suppression si plus vieux que maxdateweekly
find $pathsnap -name "@GMT-*-[07]" -exec bash -c "fDeleteOlderSnapshoThan {}
${maxdateweekly}" \;

#cat $logfile
<EOF>

/root/take-btrfs-snap.sh
#!/bin/bash
#
# Script pour prendre un snapshot des sous-volumes BTRFS
#
#Paramètre : CheminSubVolume cheminSnapShot
# CheminSubVolume = sous-volum devant être sauvegarder
```

```
# cheminSnapShot = dossier ou stocket les snapshots

# Gestion du chemin en paramètre
if [ "${1}" ] && [ "${2}" ] ; then
  #echo "paramètres ${1} et ${2} existes"
  if [ -d "${1}" ] && [ -d "${2}" ] ; then
    #echo "dossiers  existes"
    pathsubvol="${1}"
    pathsnap="${2}"
  else
    echo "Erreur : un ou les paramètres ne sont pas un répertoire. fin d'execution" > ${logfile}
    exit 1
  fi
else
  echo "Erreur : problème sur paramètre non renseigné. fin d'execution" > ${logfile}
  exit 1
fi

#pathsubvol="/storage/vol.ecole"
#pathsnap="/storage/dir.ecole.shadow"
snapname="$(TZ=GMT date +@GMT-%Y.%m.%d-%H.%M.%S-%w)"

btrfs subvolume snapshot -r "${pathsubvol}" "${pathsnap}/${snapname}"



<EOF>

/root/list-btrfs-vol.sh
#!/bin/bash
#
# Script pour lister les sous-volumes BTRFS et snapshots
#
pathsubvol="/storage"
```

btrfs subvolume list $pathsubvol

<EOF>

Rendre executable les scripts

chmod 700 /root/*.sh

Test snapshot

/root/take-btrfs-snap.sh /storage/vol.ecole /storage/dir.ecole.shadow

pour vérifier on exécute la commande

/root/list-btrfs-vol.sh

ID 256 gen 61 top level 5 path vol.ecole

ID 257 gen 59 top level 5 path vol.enseignant

ID 258 gen 61 top level 5 path dir.ecole.shadow/@GMT-2025.06.24-06.55.52-2

simulation de purge :

/root/purge-btrfs-snap.sh /storage/dir.ecole.shadow

voir le journal :

cat /var/log/snap.log

/storage/dir.ecole.shadow/@GMT-2025.06.24-06.55.52-2 > /storage/dir.ecole.shadow/@GMT-2025.06.17-10.39.03-2 conservé

Configuration de l’onduleur

Apcupsd

nano /etc/apcupsd/apcupsd.conf

#Un nom pour identifier le serveur (optionnel)
UPSNAME nom_de_votre_choix
#Onduleur connecté en USB :
UPSCABLE usb
UPSTYPE usb
#Mettre DEVICE en commentaire
#DEVICE /dev/ttyS0
#Définit en tant que serveur (pensez à ouvrir le port TCP 3551 de votre firewall
NETSERVER on
NISIP 192.168.2.254
#Port par défaut du serveur (si vous le changer, il faudra le changer aussi sur les clients)
NISPORT 3551
#On arrête le serveur en cas de niveau de batterie <20% ou s'il reste moins de 5mn de vie de batterie
BATTERYLEVEL 20
MINUTES 5
#Optionnel, si sur batterie le temps maximum à attendre avant d'éteindre l'ordinateur (utile si l'onduleur est vieux et que le temps restant de batterie devient faux)
TIMEOUT 900

Test

Afin de tester on va débrancher l’onduleur et on va vérifier dans les mails si on reçoit un mail d’alerte ressemblant a celui-là.