

20
Juin
2025

Documentation Technique

MINILAB

- Création d'un minilab pour organiser le système d'une association.
- Déploiement d'un serveur général, d'un Master et d'un Slave
- Organisation du système de fichiers et des utilisateurs (poste de travail)



Pauline / Samet / Silvia / Noa

Compétences visées

- Administration et sécurité systèmes
- Administration et sécurité réseaux
- Privileged Access Management (PAM)
- LDAP
- Réseau

I. Cahier des charges

A. L'architecture réseau de l'infrastructure

- **VM SERVEUR** : 2 CPU - 1Go RAM - 8G disk + 4*8Go pour le Raid
- Comprenant les **services suivants**:
 - Passerelle Internet (2 cartes réseau: WAN / LAN)
 - Authentification PAM-LDAP
 - Serveur NFS (monté sur les disques en Raid5 et avec le protocole NFS)
 - pare-feu
 - VPN

⇒ **EN PLUS**, nous pouvons installer et configurer le logiciel **Load Balancing** (= répartition de charge), offrant une meilleure fiabilité/disponibilité des données et de meilleures performances.

- **2 VMs SERVEURS** : 1 CPU - 1Go RAM - 8Go Disk
- Comprenant les **services suivants**:
 - DHCP
 - DNS
 - LDAP

⇒ Puis, mettre en place '**Master/Slave**' pour le DHCP, DNS, LDAP et une IP en '**failover**'

- Au moins **2 VMs CLIENTES**: debian 12 bureau MATE / 1 CPU - 1Go Ram - 16Go Disk
- Permettant:
 - L' authentification PAM-LDAP pour la gestion des utilisateurs
 - Le montage du /home depuis le serveur NFS
- **CONTRAINTE**: L'asso impose les IPs suivantes:
 - **NFS Server** : 192.168.15.254
 - **DHCP1** : 192.168.15.253
 - **DHCP2** : 192.168.15.252
 - **FAILOVER** 192.168.15.250
 - **DCHP Range** : 192.168.15.100 - 192.168.15.150
 - **domaine** : linuxisgood.local

II. Sécurisation

Une fois l'architecture mise en place, passons à la sécurisation.

- A.** Depuis l'extérieur, seul le VPN sera accessible
- B.** Sécuriser LDAP
- C.** Script MaJ de l'ensemble des machines connectées
- D.** Interface (UI) pour la gestion de l'ensemble des services = NFS / LDAP / DNS / DHCP
- E.** MFA pour les utilisateurs

III. Documentation pour l'association

- A.** Gestion de l'ensemble du parc informatique
- B.** Procédures de mises à jour
- C.** PRA / PCA

IV. Évolution / Scalabilité

À présent, le système est opérationnel, il est temps de penser aux divers axes d'évolutions possibles au travers d'une documentation.

- A.** Un gestionnaire d'impression centralisé
- B.** Sauvegardes des configurations
- C.** Duplication des données du serveur NFS (NAS, Cloud...)

I. Cahier des charges

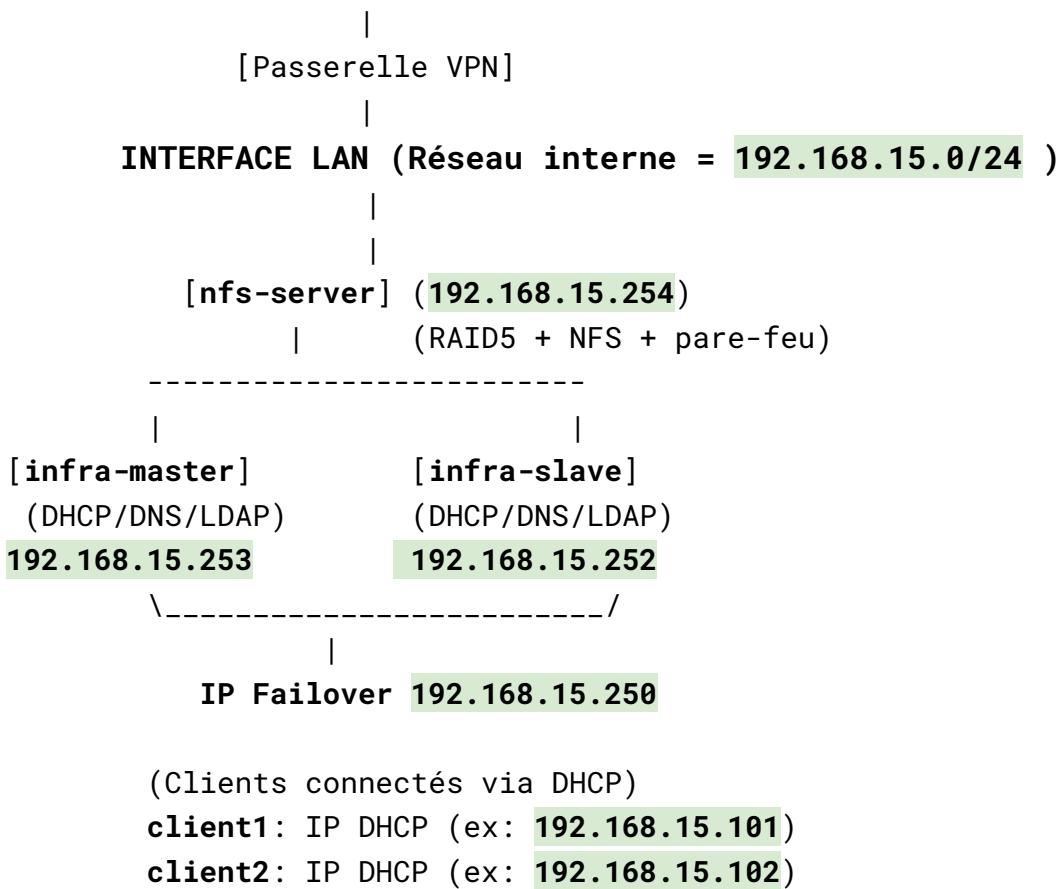
A. L'architecture réseau de l'infrastructure

Résumé des rôles des machines et de leur IP

Rôle	Nom suggéré	IP Fixe attribuée	Fonction principale
Serveur principal	nfs-serv er	192.168.15.2 54	RAID, NFS, pare-feu, VPN, passerelle, PAM-LDAP
Serveur secondaire (Master)	infra-ma ster	192.168.15.2 53	DHCP, DNS, LDAP (Master)
Serveur secondaire (Slave)	infra-sl ave	192.168.15.2 52	DHCP, DNS, LDAP (Slave)
IP Failover	infra-fa ilover	192.168.15.2 50	IP flottante pour redondance
Plage DHCP	-	192.168.15.1 00-150	Adressage automatique clients
Clients Debian MATE	client-0 1, etc	IPs dynamiques DHCP	Utilisation LDAP/NFS

Schéma global de l'architecture réseau

[Internet]



Pourquoi cette architecture ?

- Centraliser la sécurité et la gestion des accès sur le main-server (pare-feu, VPN, authentification réseau).
- Permettre aux serveurs Master/Slave de se concentrer sur les services critiques LDAP/DNS/DHCP avec redondance.
- Faciliter la maintenance et l'extension (ajout d'autres services si besoin).

{Interface LAN = 192.168.15.254

- C'est l'**interface locale** côté réseau de l'association.
- Tous les clients et autres serveurs y sont connectés.
- C'est sur cette interface que tournent les services **NFS, LDAP, etc.**
- C'est l'**IP imposée dans le cahier des charges.**}

{Interface WAN = IP vers l'extérieur

- Elle permet au serveur de se connecter à **Internet** (et de le partager avec les clients via NAT).
- Mettre ici une **IP sur une autre plage**, typiquement :

1. Cas en environnement virtuel local (test/lab) :

- Brancher cette interface sur un **réseau NAT (VirtualBox ou VMware)**
- IP possible : **10.0.2.15**, ou quelque chose du genre, attribuée par VirtualBox (NAT par défaut).

2. Cas en environnement réel :

- L'IP WAN serait attribuée par le **FAI** ou la box (ex: **192.168.1.50** ou une IP publique si dispo).

Services à installer: explications et utilité

PAM-LDAP

- **PAM** = Pluggable Authentication Modules
 - ⇒ Permet de gérer l'authentification des utilisateurs (login, sudo, etc.)
- **LDAP** = base de données hiérarchique contenant les comptes utilisateurs
 - ⇒ Les clients s'authentifient sur le serveur LDAP, pas localement

NFS (Network File System)

- Permet aux clients de monter un dossier réseau (ici **/home**)
 - ⇒ Chaque utilisateur retrouve **son environnement personnel** sur n'importe quel client.

RAID5

- 4 disques de 8Go = 32Go (RAID5 ⇒ capacité utile = 24Go)
 - ⇒ Redondance + performance (si un disque tombe en panne, les données ne sont pas perdues)

DNS / DHCP

- **DNS** : Résolution de noms de domaine (ex: `linuxisgood.local`)
- **DHCP** : Attribution automatique d'adresses IP aux clients

Master / Slave + Failover

- **Master** = serveur principal
- **Slave** = serveur secondaire, prêt à prendre la relève
- **Failover IP (192.168.15.250)** :
 - IP virtuelle qui pointe **soit vers le Master, soit vers le Slave** selon l'état
 - Permet de garder les services **accessibles même si le Master tombe**

VPN + Pare-feu

- **VPN** : Crée un tunnel sécurisé depuis l'extérieur vers l'infrastructure
- **Pare-feu** : Règles de sécurité (blocage des ports non autorisés)
- Il vient en complément du LAN:
 - permet à des machines **hors du LAN** (à distance) de **se connecter comme si elles étaient dans le LAN**.
 - créer une **interface virtuelle** (ex: `tun0`) avec une **plage d'adresses dédiée** (par exemple `10.8.0.0/24` si on utilise OpenVPN).

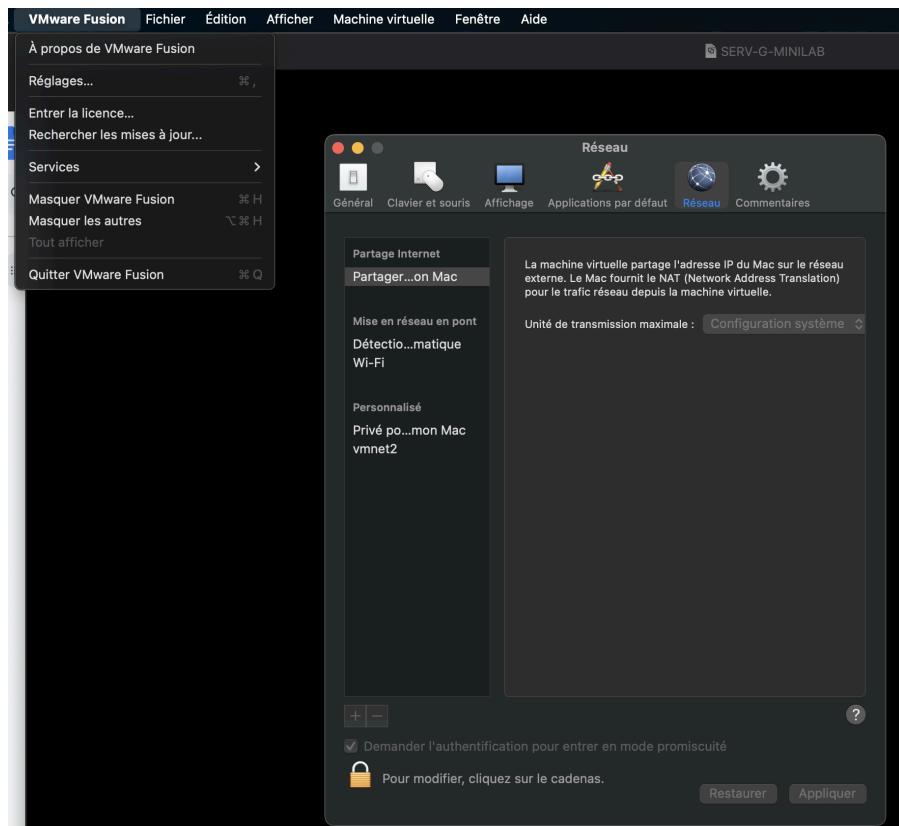
→ Les clients VPN qui se connectent verront le réseau interne (`192.168.15.0/24`) via ce tunnel.

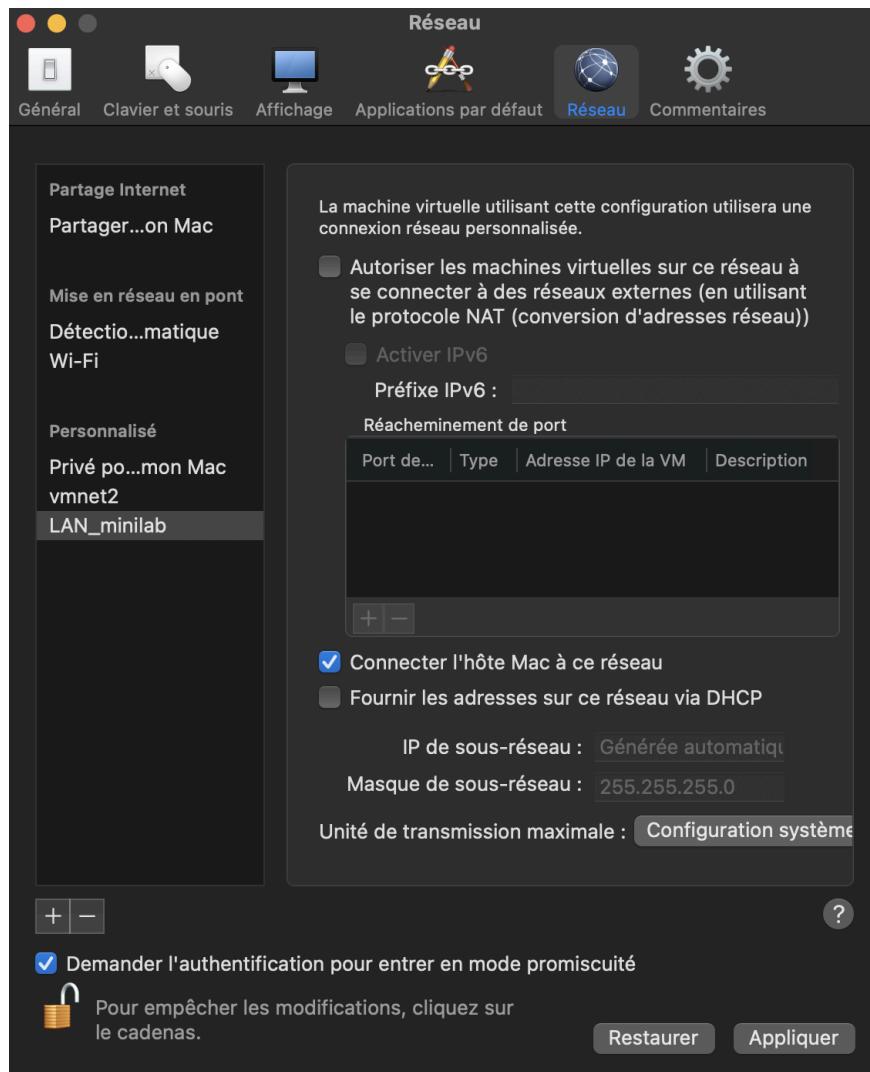
B. Configuration des VMs

1. VM “main-server”

a. Configuration des interfaces réseaux:

- Définir la **1ere interface réseau en NAT**
 - Définir un IP statique
 - DNS nameservers : Dans un premier temps, indiquer les DNS 1.1.1.1 et 8.8.8.8 puis dans un second temps, quand nous aurons configuré le service DNS sur les 2 serveurs "Master/Slave", nous modifierons cette ligne pour y renseigner l'IP des serveurs DNS.
- Définir la **2ème interface en "Custom"** pour personnaliser le réseau interne selon le cahier des charges
 - Définir une IP statique
 - Définir le masque de sous-réseau





- Décocher :

"Autoriser les machines virtuelles sur ce réseau..." puisque les serveurs Master/Slave serviront de DHCP.

"Fournir les adresses sur ce réseau via DHCP" puisque nous aurons le service DHCP configuré sur les serveurs Master/Slave.

- Configurer le fichier **/etc/network/interfaces**

```

GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
interfaces *

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#Interface WAN (vers NAT/Internet)
auto ens33
iface ens33 inet static
    address 172.16.104.180
    netmask 255.255.255.0
    gateway 172.16.104.2
    dns-nameservers 8.8.8.8 1.1.1.1

#Interface LAN (réseau interne minilab)
auto ens34
iface ens34 inet static
    address 192.168.15.254
    netmask 255.255.255.0

```

- Vérifier les nouvelles configurations

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:99:6c:21 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.104.180/24 brd 172.16.104.255 scope global ens33
        valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:fe99:6c21/64 scope link
            valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:3f:61:0e brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 192.168.15.254/24 brd 192.168.15.255 scope global ens34
        valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fe3f:610e/64 scope link
            valid_lft forever preferred_lft forever
root@main-server:/etc/network# ip route show
default via 172.16.104.2 dev ens33 onlink
172.16.104.0/24 dev ens33 proto kernel scope link src 172.16.104.180
192.168.15.0/24 dev ens34 proto kernel scope link src 192.168.15.254
```

- Test de connectivité avec ping

```
root@main-server:/etc/network# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=13.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=8.42 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 8.420/11.011/13.467/2.062 ms
root@main-server:/etc/network# ping 172.16.104.2
PING 172.16.104.2 (172.16.104.2) 56(84) bytes of data.
64 bytes from 172.16.104.2: icmp_seq=1 ttl=128 time=0.483 ms
64 bytes from 172.16.104.2: icmp_seq=2 ttl=128 time=0.662 ms
64 bytes from 172.16.104.2: icmp_seq=3 ttl=128 time=0.747 ms
^C
--- 172.16.104.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.483/0.630/0.747/0.110 ms
root@main-server:/etc/network# ping 192.168.15.254
PING 192.168.15.254 (192.168.15.254) 56(84) bytes of data.
64 bytes from 192.168.15.254: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 192.168.15.254: icmp_seq=2 ttl=64 time=0.051 ms
64 bytes from 192.168.15.254: icmp_seq=3 ttl=64 time=0.050 ms
^C
--- 192.168.15.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.031/0.044/0.051/0.009 ms
```

- Mettre en place l'IP Forwarding et le NATiptables

A FAIRE = CF la NOTE "MINILAB"

b. Configuration du RAID5:

- Ajouter des Disques via VMware

Pour simuler un RAID, nous ajoutons plusieurs disques virtuels dans VMware. Cela peut être fait en modifiant les paramètres de la machine virtuelle et en ajoutant des disques supplémentaires.

- **Installation de MDADM** (*MDADM est un outil pour gérer les volumes RAID sous Linux.*)

Mettre à jour et installer MDADM :

```
sudo apt update && sudo apt upgrade -y  
sudo apt install mdadm
```

```
[admin_minilab@main-server:~$ sudo apt install mdadm  
[sudo] Mot de passe de admin_minilab :  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  bsd-mailx exim4-base exim4-config exim4-daemon-light libevent-2.1-7  
  libgnutls-dane0 libidn12 libblockfile1 libunbound8 psmisc  
Paquets suggérés :  
  exim4-doc-html | exim4-doc-info eximon4 SPF-tools-perl swaks  
  dns-root-data dracut-core  
Les NOUVEAUX paquets suivants seront installés :  
  bsd-mailx exim4-base exim4-config exim4-daemon-light libevent-2.1-7  
  libgnutls-dane0 libidn12 libblockfile1 libunbound8 mdadm psmisc  
0 mis à jour, 11 nouvellement installés, 0 à enlever et 0 non mis à jour.  
Il est nécessaire de prendre 4 009 ko dans les archives.
```

```
Created symlink /etc/systemd/system/timers.target.wants/exim4-base.timer →  
/lib/systemd/system/exim4-base.timer.  
exim4-base.service is a disabled or a static unit, not starting it.  
Paramétrage de libunbound8:amd64 (1.17.1-2+deb12u2) ...  
Paramétrage de libgnutls-dane0:amd64 (3.7.9-2+deb12u4) ...  
Paramétrage de exim4-daemon-light (4.96-15+deb12u7) ...  
Paramétrage de bsd-mailx (8.1.2-0.20220412cvs-1) ...  
update-alternatives: utilisation de « /usr/bin/bsd-mailx » pour fournir « /  
usr/bin/mailx » (mailx) en mode automatique  
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12  
u10) ...  
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...  
Traitement des actions différées (« triggers ») pour initramfs-tools (0.142  
+deb12u3) ...  
update-initramfs: Generating /boot/initrd.img-6.1.0-37-amd64
```

- Création du RAID5

Créer un tableau RAID5 (possibilité d'ajouter un disque SPARE = **de secours**, il n'est pas utilisé directement par le RAID. Il reste en attente. Si un des disques actifs meurt, le RAID utilise automatiquement le spare pour reconstruire la grappe et maintenir l'intégrité des données.

```
sudo mdadm --create --verbose /dev/md0 --level=5 --raid-devices=4  
/dev/sdb /dev/sdc /dev/sdd /dev/sde
```

```
admin_minilab@main-server:~$ sudo mdadm --create --verbose /dev/md0 --level=5 --raid-devices=4 /dev/sdb /dev/sdc /dev/sdd /dev/sde
[sudo] Mot de passe de admin_minilab :
mdadm: layout defaults to left-symmetric
mdadm: layout defaults to left-symmetric
mdadm: chunk size defaults to 512K
mdadm: size set to 8379392K
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
```

- Vérifier l'état

```
cat /proc/mdstat
```

```
[admin_minilab@main-server:~$ cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid5 sde[4] sdd[2] sdc[1] sdb[0]
      25138176 blocks super 1.2 level 5, 512k chunk, algorithm 2 [4/4] [UUUU]

unused devices: <none>
```

- Création du Système de Fichiers

Créer un système de fichiers ext4 sur le volume RAID :

```
sudo mkfs.ext4 /dev/md0
```

```
[admin_minilab@main-server:~$ sudo mkfs.ext4 /dev/md0
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 6284544 4k blocks and 1572864 inodes
Filesystem UUID: 950a61f6-3602-47f1-a681-70094f8c4c96
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
      4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

- Montage du Volume RAID

Créer un répertoire pour le montage :

```
sudo mkdir -p /mnt/raid5
```

Monter le RAID :

```
sudo mount /dev/md0 /mnt/raid5
```

```
[admin_minilab@main-server:~$ sudo mkdir -p /mnt/raid5
[admin_minilab@main-server:~$ sudo mount /dev/md0 /mnt/raid5
```

- Ajouter le RAID au fichier fstab pour un montage automatique

Obtenez l'UUID du RAID :

```
sudo blkid /dev/md0
```

```
[admin_minilab@main-server:~$ sudo blkid /dev/md0
/dev/md0: UUID="950a61f6-3602-47f1-a681-70094f8c4c96" BLOCK_SIZE="4096" TYPE="ext4"
[admin_minilab@main-server:~$ nano /etc/fstab
```

Ajouter l'entrée au fichier **/etc/fstab** :

```
UUID=<UUID_du_RAID> /mnt/md0 ext4 defaults nobfail 0 2
```

```
#UUID du raid5 pour le montage automatique
UUID=950a61f6-3602-47f1-a681-70094f8c4c96 /mnt/raid5 ext4 defaults,nofail 0 2
```

- Tester le montage automatique sans redémarrer

```
sudo umount /mnt/raid5
```

```
sudo mount -a (= remonter les systèmes de fichiers selon la nouvelle config)
```

```
root@main-server:~# sudo umount /mnt/raid5
root@main-server:~# sudo mount -a
montage : (astuce) votre fstab a été modifié mais systemd utilise encore
          l'ancienne version ; utilisez « systemctl daemon-reload » pour recharger.
root@main-server:~# sudo systemctl daemon-reload
root@main-server:~# sudo mount -a
root@main-server:~# exit
déconnexion
```

→ Le message “montage : (astuce) votre fstab a été modifié mais systemd utilise encore l'ancienne version ; utilisez « systemctl daemon-reload » pour recharger.”

= Le service **systemd** (qui gère les montages et plein d'autres trucs) utilise encore une ancienne version de la config en mémoire.

= Il conseille de faire un **reload** de la configuration pour prendre en compte les changements = **sudo systemctl daemon-reload**

- Sauvegarder la config RAID

Pour que Debian détecte automatiquement le RAID au boot

```
sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf
```

```
[admin_minilab@main-server:~$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf
ARRAY /dev/md0 metadata=1.2 name=main-server:0 UUID=01caacc4:1c19efdf:b426e9f5:dc02be83
```

- Mettre à jour initramfs

Mettre à jour initramfs pour garantir que le RAID est monté au démarrage

```
sudo update-initramfs -u
```

```
[admin_minilab@main-server:~$ sudo update-initramfs -u
update-initramfs: Generating /boot/initrd.img-6.1.0-37-amd64
```

- Vérifications du RAID avec diverses commandes

Vérifier l'état du RAID :

```
sudo mdadm --detail /dev/md0
```

```
[admin_minilab@main-server:~$ sudo mdadm --detail /dev/md0
[[sudo] Mot de passe de admin_minilab :
/dev/md0:
      Version : 1.2
      Creation Time : Tue Jun 24 13:08:09 2025
      Raid Level : raid5
      Array Size : 25138176 (23.97 GiB 25.74 GB)
      Used Dev Size : 8379392 (7.99 GiB 8.58 GB)
      Raid Devices : 4
      Total Devices : 4
      Persistence : Superblock is persistent

      Update Time : Tue Jun 24 13:34:11 2025
                  State : clean
      Active Devices : 4
      Working Devices : 4
      Failed Devices : 0
      Spare Devices : 0

      Layout : left-symmetric
      Chunk Size : 512K

      Consistency Policy : resync

              Name : main-server:0  (local to host main-server)
              UUID : 01caacc4:1c19efdf:b426e9f5:dc02be83
              Events : 18

      Number  Major  Minor  RaidDevice State
          0      8      16        0  active sync  /dev/sdb
          1      8      32        1  active sync  /dev/sdc
          2      8      48        2  active sync  /dev/sdd
          4      8      64        3  active sync  /dev/sde
```

Vérifier les disques ajoutés pour le RAID:

```
lsblk
```

```
[admin_minilab@main-server:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda     8:0    0   8G  0 disk
└─sda1  8:1    0   7G  0 part   /
└─sda2  8:2    0   1K  0 part
└─sda5  8:5    0 975M 0 part   [SWAP]
sdb     8:16   0   8G  0 disk
└─md0   9:0    0 24G  0 raid5 /mnt/raid5
sdc     8:32   0   8G  0 disk
└─md0   9:0    0 24G  0 raid5 /mnt/raid5
sdd     8:48   0   8G  0 disk
└─md0   9:0    0 24G  0 raid5 /mnt/raid5
sde     8:64   0   8G  0 disk
└─md0   9:0    0 24G  0 raid5 /mnt/raid5
sr0    11:0   1 631M 0 rom
```

OU

```
sudo fdisk -l
```

```
[admin_minilab@main-server:~$ sudo fdisk -l
Disque /dev/sda : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VMware Virtual 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 : 0x7d79e9f6

Périphérique Amorçage      Début      Fin Secteurs Taille Id Type
/dev/sda1      *          2048 14776319 14774272    7G 83 Linux
/dev/sda2            14778366 16775167 1996802   975M 5 Étendue
/dev/sda5            14778368 16775167 1996800   975M 82 partition d'éch
```

```
Disque /dev/sdb : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VMware Virtual 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
```

```
Disque /dev/sdc : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VMware Virtual 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
```

```
Disque /dev/sdd : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VMware Virtual 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
```

```
Disque /dev/sde : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VMware Virtual 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
```

```
Disque /dev/md0 : 23,97 GiB, 25741492224 octets, 50276352 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 524288 octets / 1572864 octets
```

```
mount | grep /mnt/raid5
```

```
[admin_minilab@main-server:~$ mount | grep /mnt/raid5
/dev/md0 on /mnt/raid5 type ext4 (rw,relatime,stripe=384)
```

```
df -h /mnt/raid5
```

```
[admin_minilab@main-server:~$ df -h /mnt/raid5/
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/md0          24G      24K    23G   1% /mnt/raid5
```

c. Configuration NFS & Intégration PAM/LDAP

Configuration du serveur NFS pour partager le RAID /mnt/raid avec les autres machines du réseau.

Configurer **main-server comme serveur NFS**, afin que les machines clientes puissent accéder au répertoire RAID /mnt/raid comme un dossier local.

Installer le serveur NFS:

```
apt update
```

```
apt install nfs-kernel-server -y
```

Modifier le fichier /etc(exports

```
root@nfs-server:~# cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#           to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes    hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4      gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
#/export/home 192.168.15.0/24(rw,sync,no_subtree_check,no_root_squash)
root@nfs-server:~# exportfs -v
/export/home 192.168.15.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all_squash)
root@nfs-server:~# showmount -e localhost
Export list for localhost:
/export/home 192.168.15.0/24
root@nfs-server:~# |
```

La commande **exportfs -v** montre bien le partage pour **192.168.15.0/24**

Le service **NFS** écoute bien sur le **port 2049**

```
root@debian:/home/server1# exportfs -v
/mnt/raid/partage_nfs
          192.168.15.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all
_squash)
root@debian:/home/server1# ss -tulpn | grep nfs
root@debian:/home/server1# nano /etc/exports
root@debian:/home/server1# exportfs -ra
root@debian:/home/server1# systemctl restart nfs-kernel-server
root@debian:/home/server1# exportfs -v
/mnt/raid/partage_nfs
          192.168.15.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,no_root_squash,no_all
_squash)
root@debian:/home/server1# ss -tulpn | grep 2049
tcp    LISTEN  0        64          0.0.0.0:2049        0.0.0.0:*
tcp    LISTEN  0        64          [::]:2049          [::]::*;

root@debian:/home/server1# |
```

```
root@nfs-server:~# systemctl status nfs-kernel-server --no-pager
● nfs-server.service - NFS server and services
  Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; preset: enabled)
  Drop-In: /run/systemd/generator/nfs-server.service.d
            └─order-with-mounts.conf
    Active: active (exited) since Fri 2025-07-04 18:48:03 CEST; 16h ago
      Main PID: 1036 (code=exited, status=0/SUCCESS)
        CPU: 10ms

juil. 04 18:48:03 nfs-server systemd[1]: Starting nfs-server.service - NFS server and services...
juil. 04 18:48:03 nfs-server systemd[1]: Finished nfs-server.service - NFS server and services.
root@nfs-server:~# systemctl status rpcbind --no-pager
● rpcbind.service - RPC bind portmap service
  Loaded: loaded (/lib/systemd/system/rpcbind.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-07-04 18:48:01 CEST; 16h ago
TriggeredBy: ● rpcbind.socket
    Docs: man:rpcbind(8)
  Main PID: 554 (rpcbind)
    Tasks: 1 (limit: 1061)
   Memory: 2.1M
     CPU: 86ms
    CGroup: /system.slice/rpcbind.service
             └─554 /sbin/rpcbind -f -w

juil. 04 18:48:01 nfs-server systemd[1]: Starting rpcbind.service - RPC bind portmap service...
juil. 04 18:48:01 nfs-server systemd[1]: Started rpcbind.service - RPC bind portmap service.
root@nfs-server:~# |
```

nfs-kernel-server a démarré et fonctionne.

Configuration NFS sur server2, server3, et client Debian

Chaque fois qu'on veut qu'une **machine cliente** (serveur ou poste utilisateur) **accède à un partage NFS**, il faut faire un minimum de configuration côté client, car :

Le NFS ne fonctionne pas automatiquement comme un partage visible.

Il faut :

1. Installer les outils nécessaires (**nfs-common**)
2. Créer un dossier local pour monter le partage (ex : **/mnt/partage_nfs**)
3. Monter le partage distant (**mount**)
4. Configurer **/etc/fstab** pour monter automatiquement au démarrage

Pourquoi ?

Parce que le **noyau Linux** n'accède pas au réseau pour monter un dossier tout seul.

Le montage NFS est **volontairement explicite**, car ça touche directement le système de fichiers.

En plus : c'est une bonne pratique en cybersécurité

Cela oblige à :

- Contrôler quelle machine accède à quoi
- Appliquer des règles précises (ex : montage en lecture seule, UID/GID...)
- Restreindre l'accès dans **/etc(exports** sur le serveur
- Limiter certaines IP ou plages dans **/etc(exports**, comme on l'a déjà fait (192.168.15.0/24).

server2 et **server3** seront les serveurs DHCP/DNS/LDAP master et slave, avec une IP statique chacun.

Ils doivent avoir une IP fixe pour que tous les autres clients et services puissent s'y connecter de manière fiable.

Les adresses IP à respecter

- DHCP1 (master) : 192.168.15.253 → server2 (par exemple)
- DHCP2 (slave) : 192.168.15.252 → server3 (par exemple)
- Failover : 192.168.15.250 (adresse virtuelle pour failover entre les deux serveurs DHCP)

Config. server2 (DHCP1 master):

nano /etc/network/interfaces

allow-hotplug ens33

```

iface ens33 inet static
    address 192.168.15.253
    netmask 255.255.255.0
    gateway 192.168.15.254
    dns-nameservers 192.168.15.253 8.8.8.8

```

- address : l'IP statique attribuée à server2 (ici DHCP1 : 192.168.15.253)
- gateway : IP de la passerelle (du server1 à 192.168.15.254). La passerelle (gateway) sera toujours 192.168.15.254 (server1, la passerelle)
- dns-nameservers : en premier le serveur DNS local (server2), puis un DNS public (8.8.8.8) en fallback.
- DNS pointent sur eux-mêmes d'abord (car ils font aussi DNS), puis vers un DNS public

Server2:

```

GNU nano 7.2
/etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.15.253
    netmask 255.255.255.0
    gateway 192.168.15.254
    dns-nameservers 192.168.15.253 8.8.8.8

```

Config pour server3 (DHCP2 slave), idem avec l'IP 192.168.15.252 :

```

sudo nano /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet static
    address 192.168.15.252
    netmask 255.255.255.0
    gateway 192.168.15.254
    dns-nameservers 192.168.15.252 8.8.8.8

```

Server3:

```
GNU nano 7.2                               /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.15.252
    netmask 255.255.255.0
    gateway 192.168.15.254
    dns-nameservers 192.168.15.252 8.8.8.8
```

Configuration NSF client/user

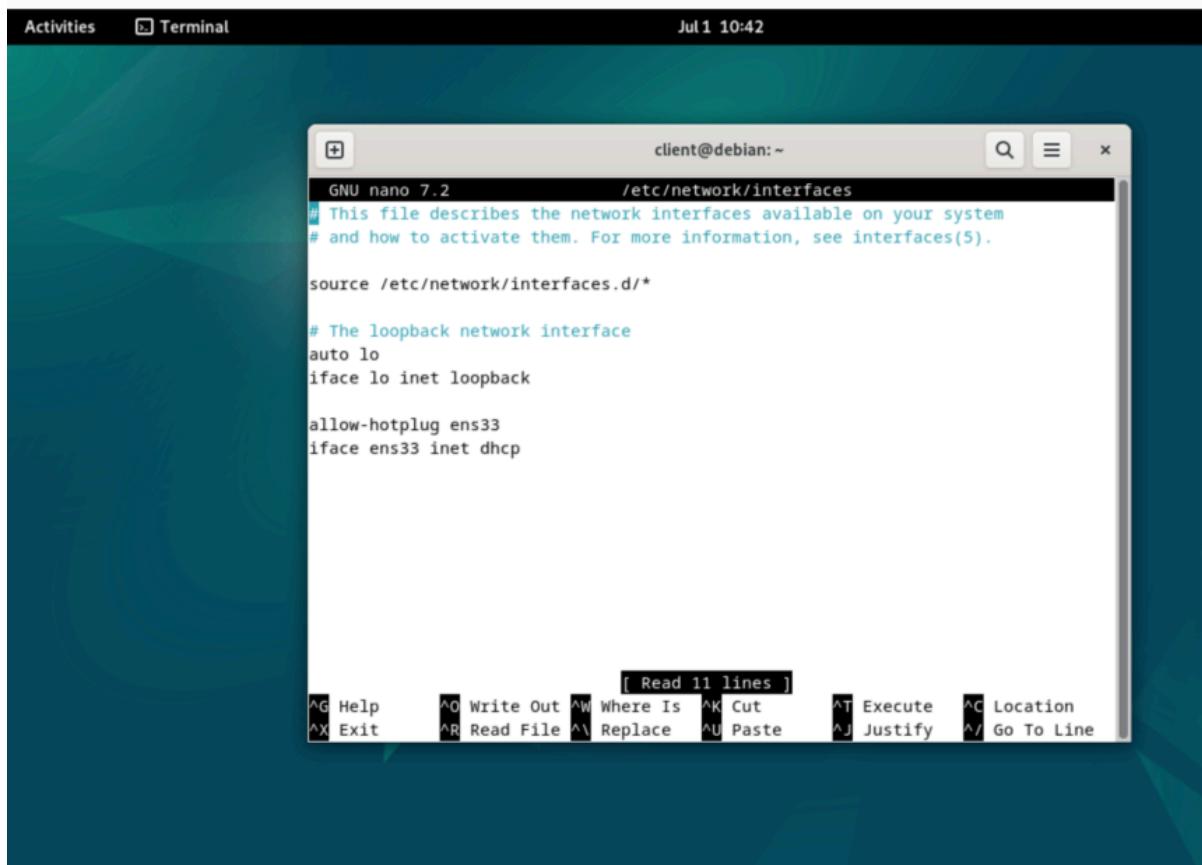
Installer les outils NFS côté client:

```
sudo apt update
sudo apt install nfs-common -y
```

Créer le point de montage local

Dossier où on va monter le partage NFS, par exemple `/mnt/nfs_home` :

```
sudo mkdir -p /mnt/nfs_home
```



Ping depuis server2 vers server1

```

root@debian:/home/server2# 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ee:6e:56 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.15.10/24 brd 192.168.15.255 scope global ens33
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:feee:6e56/64 scope link
            valid_lft forever preferred_lft forever
root@debian:/home/server2# ping 192.168.15.254
PING 192.168.15.254 (192.168.15.254) 56(84) bytes of data.
64 bytes from 192.168.15.254: icmp_seq=1 ttl=64 time=0.700 ms
64 bytes from 192.168.15.254: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.15.254: icmp_seq=3 ttl=64 time=1.77 ms
64 bytes from 192.168.15.254: icmp_seq=4 ttl=64 time=1.28 ms
64 bytes from 192.168.15.254: icmp_seq=5 ttl=64 time=1.89 ms
64 bytes from 192.168.15.254: icmp_seq=6 ttl=64 time=1.41 ms
64 bytes from 192.168.15.254: icmp_seq=7 ttl=64 time=2.40 ms
64 bytes from 192.168.15.254: icmp_seq=8 ttl=64 time=0.730 ms
64 bytes from 192.168.15.254: icmp_seq=9 ttl=64 time=1.76 ms
64 bytes from 192.168.15.254: icmp_seq=10 ttl=64 time=0.817 ms
64 bytes from 192.168.15.254: icmp_seq=11 ttl=64 time=1.85 ms
64 bytes from 192.168.15.254: icmp_seq=12 ttl=64 time=1.25 ms
64 bytes from 192.168.15.254: icmp_seq=13 ttl=64 time=1.57 ms

```

État du montage NFS et accès au répertoire personnel dans le client

```

root@nfs-server:~# ls -la /export/home/
total 40
drwxr-xr-x  7 root      root      4096  1 juil. 14:47 .
drwxr-xr-x  3 root      root      4096 19 juin   11:26 ..
drwxr-xr-x 13 admin1   admin1   4096  2 juil. 15:51 client1
drwxr-xr-x 14 admin1   admin1   4096  1 juil. 15:02 client2
drwx----- 2 root      root     16384 19 juin   11:26 lost+found
drwxr-xr-x  2 nobody   nogroup  4096 19 juin   11:29 test-user
drwxr-xr-x  7 10001   users   4096  4 juil. 21:38 testuser

```

```

root@nfs-server:~# ls -la /export/home/testuser/
total 72
drwxr-xr-x  7 10001  users  4096  4 juil. 21:38 .
drwxr-xr-x  7 root      root   4096  1 juil. 14:47 ..
-rw-----  1 10001 10001 1121  4 juil. 21:42 .bash_history
-rw-r--r--  1 10001  users   220  1 juil. 13:09 .bash_logout
-rw-r--r--  1 10001  users  3526  1 juil. 13:09 .bashrc
drwx----- 3 10001 10001 4096  1 juil. 14:49 .cache
drwx----- 4 10001 10001 4096  1 juil. 14:49 .config
drwxr-xr-x  3 10001 10001 4096  4 juil. 21:37 documents
-rw-r--r--  1 10001 10001    42  4 juil. 21:38 e2e-integration-test.txt
-rw-r--r--  1 10001 10001    55  4 juil. 21:37 e2e-test-from-client.txt
-rw-r--r--  1 10001  users  5290  1 juil. 13:09 .face
lrwxrwxrwx  1 10001  users     5  1 juil. 13:09 .face.icon -> .face
-rw-r--r--  1 10001 10001    67  1 juil. 13:10 final-integration-test.txt
-r-----  1 10001 10001   169  3 juil. 09:37 .google_authenticator
drwxr-xr-x  2 10001 10001 4096  1 juil. 14:49 .icons
-rw-r--r--  1 10001  users   807  1 juil. 13:09 .profile
-rw-r--r--  1 10001 10001    35  1 juil. 13:10 test-integration.txt
drwxr-xr-x  2 10001 10001 4096  1 juil. 14:49 .themes
root@nfs-server:~#

```

```

root@client1:~# mount | grep nfs
192.168.15.254:/export/home on /home type nfs4 (rw,relatime,vers=4.2,rsize=131072,wszie=131072,namlen=255,hardtimeo=600,retrans=2,sec=sys,clientaddr=192.168.15.125,local_lock=none,addr=192.168.15.254)
192.168.15.254:/export/home on /mnt/nfs-test type nfs4 (rw,relatime,vers=4.2,rsize=131072,wszie=131072,namlen=255,hardtimeo=600,retrans=2,sec=sys,clientaddr=192.168.15.125,local_lock=none,addr=192.168.15.254)
root@client1:~# df -h | grep nfs
root@client1:~# ls -la /home/testuser/
total 72
drwxr-xr-x 7 testuser users 4096 4 juil. 21:38 .
drwxr-xr-x 7 root root 4096 1 juil. 14:47 ..
-rw----- 1 testuser users 1160 5 juil. 11:06 .bash_history
-rw-r--r-- 1 testuser users 220 1 juil. 13:09 .bash_logout
-rw-r--r-- 1 testuser users 3526 1 juil. 13:09 .bashrc
drwx----- 3 testuser users 4096 1 juil. 14:49 .cache
drwx----- 4 testuser users 4096 1 juil. 14:49 .config
drwxr-xr-x 3 testuser users 4096 4 juil. 21:37 documents
-rw-r--r-- 1 testuser users 42 4 juil. 21:38 e2e-integration-test.txt
-rw-r--r-- 1 testuser users 55 4 juil. 21:37 e2e-test-from-client.txt
-rw-r--r-- 1 testuser users 5290 1 juil. 13:09 .face
lrwxrwxrwx 1 testuser users 5 1 juil. 13:09 .face.icon -> .face
-rw-r--r-- 1 testuser users 67 1 juil. 13:10 final-integration-test.txt
-r----- 1 testuser users 169 3 juil. 09:37 .google_authenticator
drwxr-xr-x 2 testuser users 4096 1 juil. 14:49 .icons
-rw-r--r-- 1 testuser users 807 1 juil. 13:09 .profile
-rw-r--r-- 1 testuser users 35 1 juil. 13:10 test-integration.txt
drwxr-xr-x 2 testuser users 4096 1 juil. 14:49 .themes
root@client1:~#

```

Authentification PAM/LDAP (point d'entrée d'authentification réseau)

```

root@dhcp1:~# systemctl status slapd --no-pager
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
             └─slapd-remain-after-exit.conf
     Active: active (running) since Fri 2025-07-04 18:48:03 CEST; 15h ago
       Docs: man:systemd-sysv-generator(8)
   Process: 826 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
   Tasks: 4 (limit: 1065)
  Memory: 30.4M
    CPU: 343ms
   CGroup: /system.slice/slapd.service
           └─877 /usr/sbin/slapd -h "ldap:/// ldapi://" -g openldap -u openldap -F /etc/ldap/slapd.d

juil. 04 21:36:36 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 04 21:36:36 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 04 22:56:47 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 04 22:56:47 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 05 09:12:34 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 05 09:20:54 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 05 09:20:56 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 05 09:20:56 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 05 10:22:37 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
juil. 05 10:22:37 dhcp1 slapd[877]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203..66.5.16
Hint: Some lines were ellipsized, use -l to show in full.
root@dhcp1:~# ss -tlnp | grep 389
LISTEN 0      2048          0.0.0.0:389          0.0.0.0:*      users:(("slapd",pid=877,fd=8))

LISTEN 0      2048          [::]:389          [::]:*      users:(("slapd",pid=877,fd=9))

root@dhcp1:~#

```

Montrer le système d'authentification LDAP et la gestion des utilisateurs

LDAP directory structure (organization, people, groups)

```
root@dhcp1:~# slapcat
dn: dc=linuxisgood,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: linuxisgood.local
dc: linuxisgood
structuralObjectClass: organization
entryUUID: ae7d9c28-e2e7-103f-8dad-132d1c49207e
creatorsName: cn=admin,dc=linuxisgood,dc=local
createTimestamp: 20250621123330Z
entryCSN: 20250621123330.056112Z#000000#000#000000
modifiersName: cn=admin,dc=linuxisgood,dc=local
modifyTimestamp: 20250621123330Z

dn: ou=people,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: people
structuralObjectClass: organizationalUnit
entryUUID: 0d6cd88e-e3a1-103f-9d31-f56b66eadf0f
creatorsName: cn=admin,dc=linuxisgood,dc=local
createTimestamp: 20250622104026Z
entryCSN: 20250622104026.224719Z#000000#000#000000
modifiersName: cn=admin,dc=linuxisgood,dc=local
modifyTimestamp: 20250622104026Z

dn: ou=groups,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: groups
structuralObjectClass: organizationalUnit
entryUUID: 0d6d56f6-e3a1-103f-9d32-f56b66eadf0f
creatorsName: cn=admin,dc=linuxisgood,dc=local
createTimestamp: 20250622104026Z
entryCSN: 20250622104026.228056Z#000000#000#000000
modifiersName: cn=admin,dc=linuxisgood,dc=local
modifyTimestamp: 20250622104026Z
```

```
dn: ou=groups,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: groups
structuralObjectClass: organizationalUnit
entryUUID: 0d6d56f6-e3a1-103f-9d32-f56b66eadf0f
creatorsName: cn=admin,dc=linuxisgood,dc=local
createTimestamp: 20250622104026Z
entryCSN: 20250622104026.228056Z#000000#000#000000
modifiersName: cn=admin,dc=linuxisgood,dc=local
modifyTimestamp: 20250622104026Z

dn: uid=testuser,ou=people,dc=linuxisgood,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser
sn: User
givenName: Test
cn: Test User
displayName: Test User
uidNumber: 10001
gidNumber: 10001
gecos: Test User
loginShell: /bin/bash
homeDirectory: /home/testuser
structuralObjectClass: inetOrgPerson
entryUUID: 1f000ed6-e3a1-103f-9d33-f56b66eadf0f
creatorsName: cn=admin,dc=linuxisgood,dc=local
createTimestamp: 20250622104055Z
userPassword:: e1NTSEF9djNMUjFjZTVJQzJjZ2QxcUMxY1o0RWVLMUwwLzBQNwIk=
entryCSN: 20250701104555.017530Z#000000#000#000000
modifiersName: cn=admin,dc=linuxisgood,dc=local
modifyTimestamp: 20250701104555Z

dn: cn=users,ou=groups,dc=linuxisgood,dc=local
objectClass: posixGroup
cn: users
gidNumber: 10001
```

LDAP search results (testuser, groups)

```
root@dhcp1:~# ldapsearch -x -LLL -b "dc=linuxisgood,dc=local"
dn: dc=linuxisgood,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: linuxisgood.local
dc: linuxisgood

dn: ou=people,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: groups

dn: uid=testuser,ou=people,dc=linuxisgood,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser
sn: User
givenName: Test
cn: Test User
displayName: Test User
uidNumber: 10001
gidNumber: 10001
gecos: Test User
loginShell: /bin/bash
homeDirectory: /home/testuser

dn: cn=users,ou=groups,dc=linuxisgood,dc=local
objectClass: posixGroup
cn: users
gidNumber: 10001
memberUid: testuser

root@dhcp1:~#
```

Résolution d'utilisateurs LDAP dans le client

```
root@client1:~# getent passwd testuser
testuser:x:10001:10001:Test User:/home/testuser:/bin/bash
root@client1:~# id testuser
uid=10001(testuser) gid=10001(users) groupes=27(sudo),10001(users)
root@client1:~# groups testuser
testuser : users sudo
root@client1:~# |
```

Réussie avec l'utilisateur LDAP

```
root@client1:~# su - testuser
testuser@client1:~$ whoami
testuser
testuser@client1:~$ pwd
/home/testuser
testuser@client1:~$ ls -la /home/testuser/
total 72
drwxr-xr-x 7 testuser users 4096 4 juil. 21:38 .
drwxr-xr-x 7 root root 4096 1 juil. 14:47 ..
-rw----- 1 testuser users 1121 4 juil. 21:42 .bash_history
-rw-r--r-- 1 testuser users 220 1 juil. 13:09 .bash_logout
-rw-r--r-- 1 testuser users 3526 1 juil. 13:09 .bashrc
drwx----- 3 testuser users 4096 1 juil. 14:49 .cache
drwx----- 4 testuser users 4096 1 juil. 14:49 .config
drwxr-xr-x 3 testuser users 4096 4 juil. 21:37 documents
-rw-r--r-- 1 testuser users 42 4 juil. 21:38 e2e-integration-test.txt
-rw-r--r-- 1 testuser users 55 4 juil. 21:37 e2e-test-from-client.txt
-rw-r--r-- 1 testuser users 5290 1 juil. 13:09 .face
lrwxrwxrwx 1 testuser users 5 1 juil. 13:09 .face.icon -> .face
-rw-r--r-- 1 testuser users 67 1 juil. 13:10 final-integration-test.txt
-r----- 1 testuser users 169 3 juil. 09:37 .google_authenticator
drwxr-xr-x 2 testuser users 4096 1 juil. 14:49 .icons
-rw-r--r-- 1 testuser users 807 1 juil. 13:09 .profile
-rw-r--r-- 1 testuser users 35 1 juil. 13:10 test-integration.txt
drwxr-xr-x 2 testuser users 4096 1 juil. 14:49 .themes
testuser@client1:~$
```

2. VM “Master” & VM “Slave”

Configuration DHCP Master/Slave et le système de basculement et Active DHCP leases

```
root@dhcp1:~# systemctl status isc-dhcp-server --no-pager
● isc-dhcp-server.service - LSB: DHCP server
  Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
  Active: active (running) since Sat 2025-07-05 10:20:16 CEST; 3min 14s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 14168 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Tasks: 1 (limit: 1065)
  Memory: 4.2M
    CPU: 87ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─14180 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens33

juil. 05 10:20:14 dhcp1 dhcpcd[14180]: balancing pool 564b490dc2d0 192.168.15.0/24 total 51 fre...(+/-)5
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: balanced pool 564b490dc2d0 192.168.15.0/24 total 51 free...sbal 7
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: Sending updates to dhcp-failover.
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: failover peer dhcp-failover: peer moves from communication...normal
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: failover peer dhcp-failover: Both servers normal
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: bind update on 192.168.15.127 from dhcp-failover rejected:...expired
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: bind update on 192.168.15.125 from dhcp-failover rejected:...expired
juil. 05 10:20:14 dhcp1 dhcpcd[14180]: bind update on 192.168.15.126 from dhcp-failover rejected:...expired
juil. 05 10:20:16 dhcp1 isc-dhcp-server[14168]: Starting ISC DHCPv4 server: dhcpcd.
juil. 05 10:20:16 dhcp1 systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
Hint: Some lines were ellipsized, use -l to show in full.
root@dhcp1:~# systemctl status keepalived --no-pager
● keepalived.service - Keepalive Daemon (LVS and VRRP)
  Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-07-04 21:51:41 CEST; 12h ago
    Docs: man:keepalived(8)
          man:keepalived.conf(5)
          man:genhash(1)
          https://keepalived.org
 Main PID: 7961 (keepalived)
  Tasks: 2 (limit: 1065)
 Memory: 1.9M
    CPU: 3.094s
   CGroup: /system.slice/keepalived.service
           ├─7961 /usr/sbin/keepalived --dont-fork
           └─7962 /usr/sbin/keepalived --dont-fork

juil. 04 21:51:42 dhcp1 Keepalived_vrrp[7962]: (VI_1) received lower priority (100) advert from 1...rding
juil. 04 21:51:43 dhcp1 Keepalived_vrrp[7962]: (VI_1) received lower priority (100) advert from 1...rding
```

```

root@dhcp2:~# systemctl status isc-dhcp-server --no-pager
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Fri 2025-07-04 18:48:09 CEST; 15h ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 1065)
   Memory: 7.8M
      CPU: 1.962s
     CGroup: /system.slice/isc-dhcp-server.service
             └─886 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens33

juil. 05 10:18:43 dhcp2 dhcpcd[886]: DHCPACK on 192.168.15.125 to 00:0c:29:03:7c:88 (client1) via ens33
juil. 05 10:19:39 dhcp2 dhcpcd[886]: DHCPREQUEST for 192.168.15.127 from 00:0c:29:03:f2:61 (Client2) via ens33
juil. 05 10:19:39 dhcp2 dhcpcd[886]: DHCPACK on 192.168.15.127 to 00:0c:29:03:f2:61 (Client2) via ens33
juil. 05 10:20:14 dhcp2 dhcpcd[886]: failover peer dhcp-failover: peer moves from normal to normal
juil. 05 10:20:14 dhcp2 dhcpcd[886]: failover peer dhcp-failover: I move from communications-int... normal
juil. 05 10:20:14 dhcp2 dhcpcd[886]: failover peer dhcp-failover: Both servers normal
juil. 05 10:20:14 dhcp2 dhcpcd[886]: balancing pool 55683ff65eb0 192.168.15.0/24 total 51 free... (+/-)5
juil. 05 10:20:14 dhcp2 dhcpcd[886]: balanced pool 55683ff65eb0 192.168.15.0/24 total 51 free ...isbal 7
juil. 05 10:21:18 dhcp2 dhcpcd[886]: DHCPREQUEST for 192.168.15.126 from 00:0c:29:03:7c:88 (client1) via ens33
juil. 05 10:21:18 dhcp2 dhcpcd[886]: DHCPACK on 192.168.15.126 to 00:0c:29:03:7c:88 (client1) via ens33
Hint: Some lines were ellipsized, use -l to show in full.
root@dhcp2:~# systemctl status keepalived --no-pager
● keepalived.service - Keepalive Daemon (LVS and VRRP)
   Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-07-04 18:48:07 CEST; 15h ago
     Docs: man:keepalived(8)
           man:keepalived.conf(5)
           man:genhash(1)
           https://keepalived.org
   Main PID: 847 (keepalived)
      Tasks: 2 (limit: 1065)
     Memory: 6.0M
        CPU: 2.114s
     CGroup: /system.slice/keepalived.service
             ├─847 /usr/sbin/keepalived --dont-fork
             └─860 /usr/sbin/keepalived --dont-fork

```

```

GNU nano 7.2                               /etc/dhcp/dhcpd.conf *
# Domain config
option domain-name "linuxisgood.local";
option domain-name-servers 192.168.15.253, 192.168.15.252;

# Failover config (primary)
failover peer "dhcp-failover" {
    primary;
    address 192.168.15.253;
    port 647;
    peer address 192.168.15.252;
    peer port 647;
    max-response-delay 60;
    max-unacked-updates 10;
    mclt 3600;
    split 128;
    load balance max seconds 3;
}

# Subnet config
subnet 192.168.15.0 netmask 255.255.255.0 {
    pool {
        failover peer "dhcp-failover";
        range 192.168.15.100 192.168.15.150;
    }
    option routers 192.168.15.254;
    option broadcast-address 192.168.15.255;
}

# Host reservations
host nfs-server {
    hardware ethernet 00:0c:29:5c:3b:45;
}

```

```

GNU nano 7.2                                     /etc/dhcp/dhcpd.conf *
mclt 3600;
split 128;
load balance max seconds 3;
}

# Subnet config
subnet 192.168.15.0 netmask 255.255.255.0 {
    pool {
        failover peer "dhcp-failover";
        range 192.168.15.100 192.168.15.150;
    }
    option routers 192.168.15.254;
    option broadcast-address 192.168.15.255;
}

# Host reservations
host nfs-server {
    hardware ethernet 00:0c:29:5c:3b:45;
    fixed-address 192.168.15.254;
}

host dhcp1 {
    hardware ethernet 00:0c:29:ee:70:56;
    fixed-address 192.168.15.253;
}

host dhcp2 {
    hardware ethernet 00:0c:29:a7:d0:fb;
    fixed-address 192.168.15.252;
}

^G Aide      ^O Écrire     ^W Chercher   ^K Couper      ^T Exécuter   ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^\ Remplacer   ^U Coller      ^J Justifier  ^/ Aller ligne M-E Refaire

```

```

root@dhcp1:~# nano /etc/dhcp/dhcpd.conf
root@dhcp1:~# ip addr show | grep -A 2 -B 2 192.168.15.250
    inet 192.168.15.253/24 brd 192.168.15.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.15.250/32 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feee:7056/64 scope link
root@dhcp1:~# cat /etc/keepalived/keepalived.conf
vrrp_instance VI_1 {
    state MASTER
    interface ens33
    virtual_router_id 51
    priority 110
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass linuxproject
    }
    virtual_ipaddress {
        192.168.15.250
    }
}
root@dhcp1:~#

```

```

root@dhcp1:~# tail -20 /var/lib/dhcp/dhcpd.leases
    atsfp 6 2025/07/05 08:44:39;
    cltt 5 2025/07/04 19:40:03;
    binding state active;
    next binding state expired;
    hardware ethernet 00:0c:29:03:f2:61;
    uid "\001\000\014)\003\362a";
    client-hostname "Client2";
}
lease 192.168.15.126 {
    starts 6 2025/07/05 08:29:48;
    ends 6 2025/07/05 08:39:48;
    tstamp 5 2025/07/04 19:56:06;
    tsfp 6 2025/07/05 08:44:48;
    atsfp 6 2025/07/05 08:44:48;
    cltt 5 2025/07/04 19:41:06;
    binding state active;
    next binding state expired;
    hardware ethernet 00:0c:29:03:7c:88;
    client-hostname "client1";
}
root@dhcp1:~#

```

```

root@dhcp1:~# dhclient -l 2>/dev/null || echo "Active DHCP leases shown above"
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC           IP             hostname      valid until   manufacturer
=====
00:0c:29:03:7c:88 192.168.15.125  client1       2025-07-05 08:33:43 -NA-
00:0c:29:03:f2:61 192.168.15.127  Client2       2025-07-05 08:34:39 -NA-
root@dhcp1:~#

```

Montrer le système de haute disponibilité et les processus de basculement automatique

- Propriété virtuelle de l'IP de DHCP1 (durée normale)
- Arrêt de Keepalived et perte d'IP dans DHCP1
- Héritage d'IP virtuelles dans DHCP2
- Récupération de service et récupération d'IP dans DHCP1

```

root@dhcp2:~# systemctl status keepalived --no-pager
● keepalived.service - Keepalive Daemon (LVS and VRRP)
  Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-07-04 18:48:07 CEST; 17h ago
    Docs: man:keepalived(8)
          man:keepalived.conf(5)
          man:genhash(1)
          https://keepalived.org
   Main PID: 847 (keepalived)
     Tasks: 2 (limit: 1065)
    Memory: 6.0M
      CPU: 2.538s
     CGroup: /system.slice/keepalived.service
             └─847 /usr/sbin/keepalived --dont-fork
                  ├─860 /usr/sbin/keepalived --dont-fork

juil. 04 20:17:14 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
juil. 04 20:43:49 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
juil. 04 20:43:49 dhcp2 Keepalived_vrrp[860]: (VI_1) Master received advert from 192.168.15.253 ...rs 100
juil. 04 20:43:49 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
juil. 04 21:43:05 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
juil. 04 21:51:45 dhcp2 Keepalived_vrrp[860]: (VI_1) Master received advert from 192.168.15.253 ...rs 100
juil. 04 21:51:45 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
juil. 05 10:12:05 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
juil. 05 10:13:34 dhcp2 Keepalived_vrrp[860]: (VI_1) Master received advert from 192.168.15.253 ...rs 100
juil. 05 10:13:34 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
Hint: Some lines were ellipsized, use -l to show in full.
root@dhcp2:~#

```

```

root@dhcp1:~# ip addr show | grep -A 3 -B 3 192.168.15.250
    altname enp2s1
    inet 192.168.15.253/24 brd 192.168.15.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.15.250/32 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feee:7056/64 scope link
        valid_lft forever preferred_lft forever
root@dhcp1:~# systemctl status keepalived --no-pager
● keepalived.service - Keepalive Daemon (LVS and VRRP)
   Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-07-04 21:51:41 CEST; 15h ago
       Docs: man:keepalived(8)
              man:keepalived.conf(5)
              man:genhash(1)
              https://keepalived.org
     Main PID: 7961 (keepalived)
        Tasks: 2 (limit: 1065)
      Memory: 1.9M
         CPU: 4.708s
      CGroup: /system.slice/keepalived.service
              └─7961 /usr/sbin/keepalived --dont-fork
                  ├─7962 /usr/sbin/keepalived --dont-fork

juil. 04 21:51:44 dhcp1 Keepalived_vrrp[7962]: (VI_1) received lower priority (100) advert from 1...rding
juil. 04 21:51:45 dhcp1 Keepalived_vrrp[7962]: (VI_1) received lower priority (100) advert from 1...rding
juil. 04 21:51:45 dhcp1 Keepalived_vrrp[7962]: (VI_1) Entering MASTER STATE
juil. 04 22:15:14 dhcp1 Keepalived_vrrp[7962]: A thread timer expired 2.800714 seconds ago
juil. 04 23:27:56 dhcp1 Keepalived_vrrp[7962]: A thread timer expired 2.674854 seconds ago
juil. 05 08:57:20 dhcp1 Keepalived_vrrp[7962]: A thread timer expired 2.097329 seconds ago
juil. 05 10:13:34 dhcp1 Keepalived_vrrp[7962]: A thread timer expired 2.972710 seconds ago
juil. 05 10:13:34 dhcp1 Keepalived_vrrp[7962]: (VI_1) Received advert from 192.168.15.252 with location
juil. 05 11:38:27 dhcp1 Keepalived_vrrp[7962]: A thread timer expired 2.067092 seconds ago
juil. 05 12:06:27 dhcp1 Keepalived_vrrp[7962]: A thread timer expired 2.522954 seconds ago
Hint: Some lines were ellipsized, use -l to show in full.
root@dhcp1:~# |

```

```

root@dhcp1:~# systemctl stop keepalived
root@dhcp1:~# sleep 5
root@dhcp1:~# ip addr show | grep 192.168.15.250
root@dhcp1:~# |

```

```

root@dhcp2:~# ip addr show | grep -A 3 -B 3 192.168.15.250
    altname enp2s1
    inet 192.168.15.252/24 brd 192.168.15.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.15.250/32 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fea7:d0fb/64 scope link
        valid_lft forever preferred_lft forever
root@dhcp2:~# systemctl status keepalived --no-pager | tail -10
juil. 04 20:43:49 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
juil. 04 20:43:49 dhcp2 Keepalived_vrrp[860]: (VI_1) Master received advert from 192.168.15.253 with higher priority 110, ours 100
juil. 04 20:43:49 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
juil. 04 21:43:05 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
juil. 04 21:51:45 dhcp2 Keepalived_vrrp[860]: (VI_1) Master received advert from 192.168.15.253 with higher priority 110, ours 100
juil. 04 21:51:45 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
juil. 05 10:12:05 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
juil. 05 10:13:34 dhcp2 Keepalived_vrrp[860]: (VI_1) Master received advert from 192.168.15.253 with higher priority 110, ours 100
juil. 05 10:13:34 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering BACKUP STATE
juil. 05 13:50:15 dhcp2 Keepalived_vrrp[860]: (VI_1) Entering MASTER STATE
root@dhcp2:~# |

```

```

root@dhcp1:~# systemctl start keepalived
root@dhcp1:~# sleep 5
ip addr show | grep -A 3 -B 3 192.168.15.250root@dhcp1:~#
root@dhcp1:~# ip addr show | grep -A 3 -B 3 192.168.15.250
    altname enp2s1
    inet 192.168.15.253/24 brd 192.168.15.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.15.250/32 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feee:7056/64 scope link
        valid_lft forever preferred_lft forever
root@dhcp1:~# |

```

Configuration DNS Master/Slave et les fichiers de zone

```
root@dhcp1:~# systemctl status bind9 --no-pager
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-07-04 18:48:03 CEST; 15h ago
       Docs: man:named(8)
   Main PID: 825 (named)
     Status: "running"
        Tasks: 8 (limit: 1065)
      Memory: 39.1M
        CPU: 1.237s
      CGroup: /system.slice/named.service
              └─825 /usr/sbin/named -f -u bind

juil. 04 20:58:11 dhcp1 named[825]: network unreachable resolving 'deb.debian.org/A/IN': 2001:5::f#:53
juil. 04 20:58:11 dhcp1 named[825]: network unreachable resolving 'deb.debian.org/AAAA/IN': 2001:f::f#:53
juil. 04 20:58:11 dhcp1 named[825]: network unreachable resolving 'deb.debian.org/A/IN': 2001:5::e#:53
juil. 04 20:58:11 dhcp1 named[825]: network unreachable resolving 'deb.debian.org/AAAA/IN': 2001:8::e#:53
juil. 04 20:58:21 dhcp1 named[825]: timed out resolving '_http._tcp.deb.debian.org/SRV/IN': 8.8.8.8#:53
juil. 04 20:58:22 dhcp1 named[825]: timed out resolving '_http._tcp.deb.debian.org/SRV/IN': 8.8.4.4#:53
juil. 04 20:58:22 dhcp1 named[825]: network unreachable resolving '_http._tcp.deb.debian.org/SR...0::b#:53
juil. 04 21:43:04 dhcp1 named[825]: network unreachable resolving '_http._tcp.deb.debian.org/SR...2::c#:53
juil. 04 21:51:45 dhcp1 named[825]: no longer listening on 192.168.15.250#:53
Hint: Some lines were ellipsized, use -l to show in full.
```

DNS Zone Configuration: Forward zone, Reverse Zone fichiers, DNS Resolution Test

```
GNU nano 7.2                                     /etc/bind/named.conf.local
// DNS Master Configuration for linuxisgood.local
// 

// Forward zone
zone "linuxisgood.local" {
    type master;
    file "/etc/bind/db.linuxisgood.local";
    allow-update { none; };
    allow-transfer { 192.168.15.252; };
    notify yes;
    also-notify { 192.168.15.252; };
};

// Reverse zone (192.168.15.x)
zone "15.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.15";
    allow-update { none; };
    allow-transfer { 192.168.15.252; };
    notify yes;
    also-notify { 192.168.15.252; };
};
```

```
GNU nano 7.2                                     /etc/bind/db.linuxisgood.local
$TTL    604800
@       IN      SOA     dhcp1.linuxisgood.local. admin.linuxisgood.local. (
                      2                   ; Serial
                      604800            ; Refresh
                      86400             ; Retry
                     2419200           ; Expire
                      604800            ; Negative Cache TTL
@       IN      NS      dhcp1.linuxisgood.local.

; Host records
dhcp1          IN      A       192.168.15.253
nfs-server     IN      A       192.168.15.254
gateway        IN      A       192.168.15.254
```

```

GNU nano 7.2                                     /etc/bind/db.192.168.15
$TTL    604800
@      IN      SOA    dhcp1.linuxisgood.local. admin.linuxisgood.local. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )     ; Negative Cache TTL

@      IN      NS     dhcp1.linuxisgood.local.

; PTR Records
253    IN      PTR    dhcp1.linuxisgood.local.
254    IN      PTR    nfs-server.linuxisgood.local.

```

```

root@client1:~# nslookup dhcp1.linuxisgood.local
Server:      192.168.15.253
Address:     192.168.15.253#53

Name:   dhcp1.linuxisgood.local
Address: 192.168.15.253

root@client1:~# nslookup nfs-server.linuxisgood.local
Server:      192.168.15.253
Address:     192.168.15.253#53

Name:   nfs-server.linuxisgood.local
Address: 192.168.15.254

root@client1:~# dig @192.168.15.253 linuxisgood.local

;; <>> DiG 9.18.33-1~deb12u2-Debian <>> @192.168.15.253 linuxisgood.local
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34948
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 997fb08bb161e095010000006868e49dd129379921eb62da (good)
;; QUESTION SECTION:
;linuxisgood.local.      IN      A

;; AUTHORITY SECTION:
linuxisgood.local.    604800  IN      SOA    dhcp1.linuxisgood.local. admin.linuxisgood.local. 2 604800 86
604800

```

3. VMs "Clients"

Test de vérification que tous les systèmes fonctionnent ensemble et que le workflow client est réussi

- **Test de résolution DNS (forward/reverse)**

```
root@client1:~# nslookup dhcp1.linuxisgood.local
Server:      192.168.15.253
Address:     192.168.15.253#53

Name:   dhcp1.linuxisgood.local
Address: 192.168.15.253

root@client1:~# nslookup nfs-server.linuxisgood.local
Server:      192.168.15.253
Address:     192.168.15.253#53

Name:   nfs-server.linuxisgood.local
Address: 192.168.15.254

root@client1:~# nslookup 192.168.15.253
253.15.168.192.in-addr.arpa      name = dhcp1.linuxisgood.local.

root@client1:~# ping -c 3 dhcp1.linuxisgood.local
PING dhcp1.linuxisgood.local (192.168.15.253) 56(84) bytes of data.
64 bytes from dhcp1.linuxisgood.local (192.168.15.253): icmp_seq=1 ttl=64 time=0.385 ms
64 bytes from dhcp1.linuxisgood.local (192.168.15.253): icmp_seq=2 ttl=64 time=0.717 ms
64 bytes from dhcp1.linuxisgood.local (192.168.15.253): icmp_seq=3 ttl=64 time=0.661 ms
--- dhcp1.linuxisgood.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.385/0.587/0.717/0.145 ms
root@client1:~# |
```

- **Récupération automatique de l'IP à partir du DHCP dans le client**

```
root@client1:~# dhclient ens33
RTNETLINK answers: File exists
root@client1:~# ip addr show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:03:7c:88 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.15.125/24 brd 192.168.15.255 scope global dynamic noprefixroute ens33
        valid_lft 377sec preferred_lft 377sec
    inet 192.168.15.126/24 brd 192.168.15.255 scope global secondary dynamic ens33
        valid_lft 567sec preferred_lft 567sec
    inet6 fe80::20c:29ff:fe03:7c88/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@client1:~#
root@client1:~# |
```

- **Authentification LDAP par session utilisateur**

```
root@client1:~# getent passwd testuser
testuser:x:10001:10001:Test User:/home/testuser:/bin/bash
root@client1:~# su - testuser
testuser@client1:~$ whoami && pwd && id
testuser
/home/testuser
uid=10001(testuser) gid=10001(users) groupes=10001(users),27(sudo)
testuser@client1:~$ |
```

- Utilisation du répertoire personnel NFS et opérations sur les fichiers

```
testuser@client1:~$ ls -la /home/testuser/
total 120
drwxr-xr-x 16 testuser users 4096 5 juil. 14:18 .
drwxr-xr-x 7 root      root  4096 1 juil. 14:47 ..
-rw----- 1 testuser users 1160 5 juil. 11:06 .bash_history
-rw-r--r-- 1 testuser users  220 1 juil. 13:09 .bash_logout
-rw-r--r-- 1 testuser users 3526 1 juil. 13:09 .bashrc
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Bureau
drwx----- 5 testuser users 4096 5 juil. 14:18 .cache
drwx----- 7 testuser users 4096 5 juil. 14:18 .config
drwxr-xr-x 3 testuser users 4096 4 juil. 21:37 documents
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Documents
-rw-r--r-- 1 testuser users   42 4 juil. 21:38 e2e-integration-test.txt
-rw-r--r-- 1 testuser users   55 4 juil. 21:37 e2e-test-from-client.txt
-rw-r--r-- 1 testuser users 5290 1 juil. 13:09 .face
lrwxrwxrwx 1 testuser users   5 1 juil. 13:09 .face.icon -> .face
-rw-r--r-- 1 testuser users   67 1 juil. 13:10 final-integration-test.txt
-r----- 1 testuser users 169 3 juil. 09:37 .google_authenticator
drwxr-xr-x 2 testuser users 4096 1 juil. 14:49 .icons
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Images
drwx----- 3 testuser users 4096 5 juil. 14:18 .local
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Modèles
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Musique
-rw-r--r-- 1 testuser users  807 1 juil. 13:09 .profile
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Public
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Téléchargements
-rw-r--r-- 1 testuser users   35 1 juil. 13:10 test-integration.txt
drwxr-xr-x 2 testuser users 4096 1 juil. 14:49 .themes
drwxr-xr-x 2 testuser users 4096 5 juil. 14:18 Vidéos
-rw----- 1 testuser users   52 5 juil. 14:18 .Xauthority
-rw----- 1 testuser users 4360 5 juil. 14:18 .xsession-errors
testuser@client1:~$ |
```

- État final de tous les services du système

```
root@nfs-server:~# systemctl status nfs-kernel-server openvpn-server@server --no-pager
● nfs-server.service - NFS server and services
  Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; preset: enabled)
  Drop-In: /run/systemd/generator/nfs-server.service.d
            └─order-with-mounts.conf
    Active: active (exited) since Fri 2025-07-04 18:48:03 CEST; 19h ago
      Main PID: 1036 (code=exited, status=0/SUCCESS)
        CPU: 10ms

juil. 04 18:48:03 nfs-server systemd[1]: Starting nfs-server.service - NFS server and services...
juil. 04 18:48:03 nfs-server systemd[1]: Finished nfs-server.service - NFS server and services.

● openvpn-server@server.service - OpenVPN service for server
  Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-07-04 20:32:48 CEST; 18h ago
    Docs: man:openvpn(8)
          https://community.openvpn.net/openvpn/wiki/OpenVPN24ManPage
          https://community.openvpn.net/openvpn/wiki/HOWTO
    Main PID: 1694 (openvpn)
    Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 1061)
     Memory: 1.4M
        CPU: 354ms
      CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
               └─1694 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --supp...

juil. 04 20:32:48 nfs-server systemd[1]: Stopped openvpn-server@server.service - OpenVPN service for server.
juil. 04 20:32:48 nfs-server systemd[1]: Starting openvpn-server@server.service - OpenVPN service for server...
juil. 04 20:32:48 nfs-server systemd[1]: Started openvpn-server@server.service - OpenVPN service for server.
Hint: Some lines were ellipsized, use -l to show in full.
root@nfs-server:~#
```

II. Sécurisation

Une fois l'architecture mise en place, passons à la sécurisation.

A. Depuis l'extérieur, seul le VPN sera accessible

- Règles du pare-feu du serveur NFS (politique DROP, règles d'autorisation)

```
root@nfs-server:~# iptables -L INPUT -v --line-numbers
Chain INPUT (policy DROP 163 packets, 32586 bytes)
num  pkts bytes target  prot opt in     out    source        destination
1    197 12348 ACCEPT   all  --  lo      any    anywhere     anywhere
2    28180 6989K ACCEPT  all  --  any    any    anywhere     anywhere          state RELATED,ESTABLISHED
3      0    0 ACCEPT   udp  --  any    any    anywhere     anywhere
4    520 40883 ACCEPT  all  --  any    any    192.168.15.0/24 anywhere
5      0    0 ACCEPT   all  --  any    any    10.8.0.0/24  anywhere
root@nfs-server:~# iptables -L FORWARD -v --line-numbers
Chain FORWARD (policy DROP 0 packets, 0 bytes)
num  pkts bytes target  prot opt in     out    source        destination
1    1622 5962K ACCEPT  all  --  ens33  ens34  anywhere     anywhere          state RELATED,ESTABLISHED
2    1739 137K ACCEPT  all  --  ens34  ens33  anywhere     anywhere
3      0    0 ACCEPT   all  --  ens34  ens33  anywhere     anywhere
4      0    0 ACCEPT   all  --  ens33  ens34  anywhere     anywhere          state RELATED,ESTABLISHED
5      0    0 ACCEPT   all  --  tun0   any    anywhere     anywhere
6      0    0 ACCEPT   all  --  tun0   ens34  anywhere     anywhere
7      0    0 ACCEPT   all  --  ens34  tun0   anywhere     anywhere
8      0    0 ACCEPT   all  --  ens34  ens33  anywhere     anywhere
9      0    0 ACCEPT   all  --  ens33  ens34  anywhere     anywhere          state RELATED,ESTABLISHED
10     0    0 ACCEPT   all  --  tun+   any    anywhere     anywhere
11     0    0 ACCEPT   all  --  tun+   eth0   anywhere     anywhere          state RELATED,ESTABLISHED
12     0    0 ACCEPT   all  --  eth0   tun+   anywhere     anywhere          state RELATED,ESTABLISHED
root@nfs-server:~# |
```

```
root@dhcp2:~# iptables -L | grep -E "(DROP|ACCEPT)"
Chain INPUT (policy DROP)
ACCEPT  all  --  anywhere           anywhere
ACCEPT  all  --  anywhere           anywhere          state RELATED,ESTABLISHED
ACCEPT  all  --  192.168.15.0/24   anywhere
ACCEPT  all  --  192.168.0.0/24   anywhere
ACCEPT  tcp  --  anywhere           anywhere          tcp dpt:ssh
ACCEPT  tcp  --  anywhere           anywhere          tcp dpt:domain
ACCEPT  udp  --  anywhere           anywhere          udp dpt:domain
ACCEPT  tcp  --  anywhere           anywhere          tcp dpt:ldap
ACCEPT  udp  --  anywhere           anywhere          udp dpt:bootps
ACCEPT  udp  --  anywhere           anywhere          udp dpt:bootpc
ACCEPT  tcp  --  anywhere           anywhere          tcp dpt:647
ACCEPT  all  --  10.8.0.0/24       anywhere
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
root@dhcp2:~# |
```

- Règles et politiques du pare-feu DHCP2

```

root@dhcp2:~# iptables -L | grep -E "(DROP|ACCEPT)"
Chain INPUT (policy DROP)
ACCEPT    all  --  anywhere             anywhere
ACCEPT    all  --  anywhere             anywhere           state RELATED,ESTABLISHED
ACCEPT    all  --  192.168.15.0/24      anywhere
ACCEPT    all  --  192.168.0.0/24      anywhere
ACCEPT    tcp  --  anywhere             anywhere           tcp dpt:ssh
ACCEPT    tcp  --  anywhere             anywhere           tcp dpt:domain
ACCEPT    udp  --  anywhere             anywhere           udp dpt:domain
ACCEPT    tcp  --  anywhere             anywhere           tcp dpt:ldap
ACCEPT    udp  --  anywhere             anywhere           udp dpt:bootps
ACCEPT    udp  --  anywhere             anywhere           udp dpt:bootpc
ACCEPT    tcp  --  anywhere             anywhere           tcp dpt:647
ACCEPT    all  --  10.8.0.0/24        anywhere
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
root@dhcp2:~# |

```

- **État et configuration du service OpenVPN / État de l'interface VPN et certificats des clients**

```

root@nfs-server:~# systemctl status openvpn-server@server --no-pager
● openvpn-server@server.service - OpenVPN service for server
   Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-07-04 20:32:48 CEST; 15h ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 1694 (openvpn)
      Status: "Initialization Sequence Completed"
        Tasks: 1 (limit: 1061)
       Memory: 1.4M
          CPU: 296ms
        CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
                  └─1694 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --sup

juil. 04 20:32:48 nfs-server systemd[1]: Stopped openvpn-server@server.service - OpenVPN service for server.
juil. 04 20:32:48 nfs-server systemd[1]: Starting openvpn-server@server.service - OpenVPN service for server.
juil. 04 20:32:48 nfs-server systemd[1]: Started openvpn-server@server.service - OpenVPN service for server.
Hint: Some lines were ellipsized, use -l to show in full.
root@nfs-server:~# |

root@nfs-server:~# ip addr show tun0
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
  link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
      valid_lft forever preferred_lft forever
    inet6 fe80::450:7438:782e:bc0b/64 scope link stable-privacy
      valid_lft forever preferred_lft forever
root@nfs-server:~# cat /etc/openvpn/openvpn-status.log
OpenVPN CLIENT LIST
Updated,2025-07-04 20:30:56
Common Name,Real Address,Bytes Received,Bytes Sent,Connected Since
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
GLOBAL STATS
Max bcast/mcast queue length,0
END
root@nfs-server:~# ls -la /etc/openvpn/easy-rsa/pki/issued/
total 24
drwx----- 2 root root 4096  3 juil. 00:30 .
drwx----- 7 root root 4096  3 juil. 00:30 ..
-rw----- 1 root root 4494  3 juil. 00:30 client1.crt
-rw----- 1 root root 4609 20 juin 11:20 server.crt
root@nfs-server:~# |

```

- **Services de sécurité et ports ouverts**

```

root@nfs-server:~# ss -tlnp | grep -E "(22|53|67|68|111|2049|389|636|4444)"
LISTEN 0      64          0.0.0.0:2049        0.0.0.0:*
LISTEN 0      128         0.0.0.0:22          0.0.0.0:*
users:(("sshd",pid=2871,fd=3))
LISTEN 0      4096        0.0.0.0:111         0.0.0.0:*
users:(("rpcbind",pid=554,fd=4),("systemd",pid=1,fd=105))
LISTEN 0      4096        0.0.0.0:53825       0.0.0.0:*
users:(("rpc.statd",pid=1031,fd=9))
LISTEN 0      64          [:]:2049           [:]:*
LISTEN 0      128         [:]:22             [:]:*
users:(("sshd",pid=2871,fd=4))
LISTEN 0      4096        [:]:111            [:]:*
users:(("rpcbind",pid=554,fd=6),("systemd",pid=1,fd=107))
root@nfs-server:~# ps aux | grep -E "(openvpn|sshd|dhcpd|named)"
nobody   1694  0.0  0.9  13720  8844 ?          Ss   06:42  0:00 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-timestamps --config server.conf
root    2871  0.0  0.9  15864  9436 ?          Ss   09:41  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-1
00 startups
root    2929  0.0  1.1  18412  10892 ?          Ss   10:07  0:00 sshd: admin1 [priv]
admin1  2936  0.0  0.7  18672  6648 ?          Ss   10:07  0:00 sshd: admin1@pts/0
root    3022  0.0  1.1  18412  10908 ?          Ss   11:12  0:00 sshd: admin1 [priv]
admin1  3029  0.0  0.6  18672  6508 ?          Ss   11:12  0:00 sshd: admin1@pts/1
root    3104  0.0  1.1  18412  10948 ?          Ss   11:39  0:00 sshd: admin1 [priv]
admin1  3111  0.0  0.6  18672  6636 ?          Ss   11:39  0:00 sshd: admin1@pts/2
root    3150  0.0  0.2  6488   2368 pts/2        S+   11:49  0:00 grep -E (openvpn|sshd|dhcpd|named)
root@nfs-server:~#

```

B. Sécuriser LDAP

- Comparaison des règles de pare-feu multi-serveurs

```

root@nfs-server:~# iptables -L INPUT --line-numbers | head -15
Chain INPUT (policy DROP)
num  target     prot opt source          destination
1    ACCEPT     all  --  anywhere        anywhere
2    ACCEPT     all  --  anywhere        anywhere
3    ACCEPT     udp  --  anywhere        anywhere          state RELATED,ESTABLISHED
4    ACCEPT     all  --  192.168.15.0/24   anywhere
5    ACCEPT     all  --  10.8.0.0/24     anywhere
root@nfs-server:~# echo "==" DHCP2 Firewall ==="
== DHCP2 Firewall ==
root@nfs-server:~# ssh root@192.168.15.252 "iptables -L INPUT --line-numbers | head -10"
The authenticity of host '192.168.15.252 (192.168.15.252)' can't be established.
ED25519 key fingerprint is SHA256:0a0QPZFFTYVLIGf51oEU+OtcQONks/ixb0haejWRyes.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.15.252' (ED25519) to the list of known hosts.
root@192.168.15.252's password:
Chain INPUT (policy DROP)
num  target     prot opt source          destination
1    ACCEPT     all  --  anywhere        anywhere
2    ACCEPT     all  --  anywhere        anywhere          state RELATED,ESTABLISHED
3    ACCEPT     all  --  192.168.15.0/24   anywhere
4    ACCEPT     all  --  192.168.0.0/24   anywhere
5    ACCEPT     tcp  --  anywhere        anywhere          tcp dpt:ssh
6    ACCEPT     tcp  --  anywhere        anywhere          tcp dpt:domain
7    ACCEPT     udp  --  anywhere        anywhere          udp dpt:domain
8    ACCEPT     tcp  --  anywhere        anywhere          tcp dpt:ldap
root@nfs-server:~|

```

- Paramètres de sécurité et certificats VPN

```

root@nfs-server:~# cat /etc/openvpn/server/server.conf | grep -E "(cipher|auth|tls|ca|cert)"
ca /etc/openvpn/easy-rsa/pki/ca.crt
cert /etc/openvpn/easy-rsa/pki/issued/server.crt
tls-auth /etc/openvpn/easy-rsa/ta.key 0
push "dhcp-option DOMAIN linuxisgood.local"
cipher AES-256-CBC
auth SHA256
tls-version-min 1.2
# Kullanıcı ayrıcalıkları
root@nfs-server:~# ls -la /etc/openvpn/easy-rsa/pki/issued/
total 24
drwx----- 2 root root 4096 3 juil. 00:30 .
drwx----- 7 root root 4096 3 juil. 00:30 ..
-rw----- 1 root root 4494 3 juil. 00:30 client1.crt
-rw----- 1 root root 4609 20 juin 11:20 server.crt
root@nfs-server:~# cat /etc/openvpn/openvpn-status.log
OpenVPN CLIENT LIST
Updated, 2025-07-04 20:30:56
Common Name,Real Address,Bytes Received,Bytes Sent,Connected Since
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
GLOBAL STATS
Max bcast/mcast queue length,0
END
root@nfs-server:~# |

```

● Services de sécurité et matrice des ports

```

root@nfs-server:~# echo "=== Security Services Overview ==="
== Security Services Overview ==
root@nfs-server:~# ss -tlnp | grep -E "(22|53|67|389|647|2049|4444)" | sort -n
LISTEN 0      128          0.0.0.0:22          0.0.0.0:*      users:(("sshd",pid=2871,fd=3))

LISTEN 0      128          [::]:22           [::]:*        users:(("sshd",pid=2871,fd=4))

LISTEN 0      4096         0.0.0.0:53825       0.0.0.0:*      users:(("rpc.statd",pid=1031,fd=9))

LISTEN 0      64           0.0.0.0:2049       0.0.0.0:*      *

LISTEN 0      64           [::]:2049         [::]:*        *

root@nfs-server:~# echo "=== Running Security Processes ==="
== Running Security Processes ==
root@nfs-server:~# ps aux | grep -E "(sshd|openvpn|iptables)" | grep -v grep
nobody    1694  0.0   0.9  13720  8844 ?          Ss   08:21  0:00 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-timestamps --config server.conf
root     2871  0.0   0.9  15864  9436 ?          Ss   11:19  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-1
00 startups
root     3022  0.0   1.1  18412  10908 ?          Ss   12:50  0:00 sshd: admin1 [priv]
admin1   3029  0.0   0.6  18672  6508 ?          S    12:51  0:00 sshd: admin1@pts/1
root     3104  0.0   1.1  18412  10948 ?          Ss   13:18  0:00 sshd: admin1 [priv]
admin1   3111  0.0   0.6  18672  6636 ?          S    13:18  0:00 sshd: admin1@pts/2
root     3175  0.0   1.1  18412  10872 ?          Ss   13:45  0:00 sshd: admin1 [priv]
admin1   3182  0.0   0.6  18672  6612 ?          S    13:45  0:00 sshd: admin1@pts/3
root@nfs-server:~# |

```

● LDAP authentication via SSH access logs

```

root@dhcp1:~# echo "=== LDAP Security ==="
== LDAP Security ==
root@dhcp1:~# ldapsearch -x -LLL -b "dc=linuxisgood,dc=local" | grep -E "(dn:|uid:|gidNumber)"
dn: dc=linuxisgood,dc=local
dn: ou=people,dc=linuxisgood,dc=local
dn: ou=groups,dc=linuxisgood,dc=local
dn: uid=testuser,ou=people,dc=linuxisgood,dc=local
uid: testuser
gidNumber: 10001
dn: cn=users,ou=groups,dc=linuxisgood,dc=local
gidNumber: 10001
root@dhcp1:~# echo "=== SSH Access Logs ==="
== SSH Access Logs ==
root@dhcp1:~# journalctl -u ssh --since "1 hour ago" --no-pager | tail -5
-- No entries --
root@dhcp1:~# last | head -10
admin1 pts/1      192.168.15.1      Sat Jul  5 13:45  still logged in
admin1 pts/0      192.168.15.1      Sat Jul  5 11:40 - 14:04  (02:24)
admin1 pts/1      192.168.15.1      Sat Jul  5 10:19 - 11:59  (01:40)
admin1 pts/0      192.168.15.1      Sat Jul  5 09:34 - 10:38  (01:03)
root  pts/2      192.168.15.253    Fri Jul  4 21:48 - 22:53  (01:05)
root  pts/0      192.168.15.1      Fri Jul  4 21:41 - 22:53  (01:11)
root  pts/2      192.168.15.1      Fri Jul  4 21:08 - 21:25  (00:17)
admin1 pts/1      192.168.15.1      Fri Jul  4 20:52 - 22:54  (02:01)
admin1 pts/0      192.168.15.1      Fri Jul  4 19:01 - 21:12  (02:10)
admin1 ttym1          Fri Jul  4 18:48  gone - no logout
root@dhcp1:~# |

```

C. Script MaJ de l'ensemble des machines connectées

```

#!/bin/bash

# Met à jour la liste des paquets
apt update

# Met à jour tous les paquets installés sans interaction
apt upgrade -y

# Nettoie les paquets inutiles
apt autoremove -y

# Redémarre les services critiques si besoin (exemple)
systemctl restart nslcd
systemctl restart nfs-common

echo "Mise à jour terminée sur $(hostname)"

```

Ce script est exécuté régulièrement via **cron** ou manuellement à partir d'un serveur de gestion.

D. Interface (UI) pour la gestion de l'ensemble des services = NFS / LDAP / DNS / DHCP

Pour la gestion des serveurs, nous avons créé un **dashboard** sur-mesure, qui couvre l'**opérationnalité de chaque service** de manière claire et visuelle.

The screenshot displays a web-based dashboard with the following sections:

- Server Status:** A table listing four servers with their details:

Server	IP Address	Status	Uptime	Load	Memory	Disk	Actions
DHCP1/LDAP/DNS Master dhcp1	192.168.15.253	Online	up 8 hours, 30 minutes	0.00 0.03 0.02	471Mi/925Mi	2.1G/19G (12%)	
DHCP2/DNS Slave dhcp2	192.168.15.252	Online	SSH Failed	N/A	N/A	N/A	
Client with MFA (SSH Limited) client2	192.168.15.127	Online	SSH Failed	N/A	N/A	N/A	
NFS Server (SSH Limited) nfs-server	192.168.15.254	Online	SSH Failed	N/A	N/A	N/A	
- Quick Actions:** Buttons for running updates, checking services, and viewing logs.
- System Management:** Links to DHCP Config, DNS Config, and VPN Status.
- System Overview:** A summary section.

E. MFA pour les utilisateurs

Activer le MFA pour renforcer la sécurité

- Utilisation de Google Authenticator ⇒ Télécharger l'application mobile

1. Installer Google Authenticator sur le serveur

```
sudo apt update  
sudo apt install libpam-google-authenticator
```

2. Créer un utilisateur sur le système Linux du serveur (ou via LDAP??)

```
sudo adduser testuser-openvpn
```

3. Se connecter en tant que testuser-openvpn sur le serveur

```
sudo su - testuser-openvpn
```

Puis exécuter: **google-authenticator**

4. Configurer Google Authenticator pour cet utilisateur



Scanner le QR code affiché avec l'appli Google Authenticator sur iPhone.

Bien lire les informations de paramétrages et répondre par y/n

```
Your new secret key is: IIVGIAYQ4LWE4NDLT5GPH2QNBQ
Enter code from app (-1 to skip): 632 242
Code incorrect (correct code 632242). Try again.
Enter code from app (-1 to skip): 632242
Code confirmed
Your emergency scratch codes are:
27751692
25844856
47101608
13579757
49546342
```

```
Do you want me to update your "/home/cli1-openvpn/.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 minute
s
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
```

5. Activation du 'nologin' pour les clients

Une fois le MFA activé, retirer la possibilité à l'utilisateur de se connecter en SSH en désactivant son shell:

```
sudo usermod -s /usr/sbin/nologin cli1-openvpn)
```

III. Documentation pour l'association

CF → Document annexe “*Gestion du parc informatique et procédures de mises à jour*”

Sommaire

1. Introduction
2. Glossaire
3. Présentation de l'architecture réseau
4. Gestion des utilisateurs et profils itinérants
5. Procédures de mise à jour des machines
6. Sécurisation de l'infrastructure
7. Interface de gestion centralisée
8. Plan de Reprise d'Activité (PRA) et Plan de Continuité d'Activité (PCA)
9. Annexes et ressources

IV. Évolution / Scalabilité

CF → Document annexe “*Axes d'Évolution et Scalabilité de l'Infrastructure*”

Sommaire

Introduction

1. Gestion centralisée de l'impression

- Choix du gestionnaire (CUPS)
- Intégration avec LDAP
- Sécurité et contrôle d'accès
- Suivi et quotas d'impression

2. Sauvegarde des configurations critiques

- Éléments à sauvegarder

- Outils recommandés (Rsync, BorgBackup, Rdiff-backup, Ansible)
- Stratégie de sauvegarde (locale, distante, chiffrée)
- Planification et automatisation

3. Duplication des données utilisateur (NFS)

- RéPLICATION locale (NAS)
- RéPLICATION distante (cloud, site distant)
- Outils et solutions (Rsync, Nextcloud, Ceph, GlusterFS)
- Surveillance et intégrité des données

4. Supervision et monitoring

- Outils de supervision (Zabbix, Grafana, Prometheus)
- Centralisation des logs (Graylog, ELK)
- Alerting et visualisation

5. Interface de gestion centralisée

- Cockpit, Ansible AWX
- Accès restreint et audit des actions
- Scénarios d'automatisation

6. Sécurité avancée et authentification

- Intégration SSO (ex: Keycloak)
- Authentification multifacteur (MFA)
- Gestion des accès et des rôles via LDAP

7. Plan de montée en charge

- Ajout de clients ou de services
- RéPLICATION de serveurs critiques
- Mise en cluster (DNS, LDAP, NFS)

Conclusion

SOURCES

<https://indico.in2p3.fr/event/12779/contributions/11231/attachments/9505/11873/JI-2016-keepalived.pdf>

<https://www.napsis.fr/cloud-lexique/pr-a-pca/>

<https://en.wikipedia.org/wiki/Slapd>

<https://en.wikipedia.org/wiki/DHCPD>

<https://eole.ac-dijon.fr/documentations/2.5/partielles/HTML/ClientsGnuLinux/co/10-IntroClientsLinux.html>

<https://en.wikipedia.org/wiki/OpenLDAP>