VALDIVIA Mattéo
SAVIC César
JOURDAN Alix

AP .3
Cas entreprise GSB (Lot 1)

2024/2025

Sommaire :

MODÈLE DE DIAGRAMME DE GANTT

TITRE DU PROJET	Entreprise GSB (lot 1)
CHEF DE PROJET	Alix

NUMÉRO	TITRE DE LA TÂCHE	PROPRIÉTAIRE DE LA TÂCHE	DATE DE DÉBUT	DATE LIMITE	DURÉE (en jours)	TÂCHE TERMINÉE (EN %)	Temps prévu	Temps réel		
							Semaine 1, 2, 3	Semaine 1	Semaine 2	Semaine 3
							J	J 05/09	J 12/09	J 19/09
1	LOT 1 - Equipement des visiteurs médicaux									
1	Distribution des tâches	Mattéo	05/09/24	19/09/24	14j	100 %	60 min	60 min	ABS	
1.1	Proposer des solutions correspondant au cahier des charges, parties a), b), c) et d)	Alix	05/09/24	19/09/24	14j	100 %	60 min	105 min		
1.2	Mettre en place la maquette selon le *document 3*	Mattéo	05/09/24	19/09/24	14j	100 %	60 min		ABS	60 min
1.3	Choisir une mise en place de la masteurisation des postes avec l'environnement choisi, en établissant une méthodologie de préparation des postes avant la création de l'image puis de post-configuration apès la descente des images (partie e)),	César	05/09/24	19/09/24	14j	100 %	180 min		180 min	
1.4	Choisir une configuration/préparation du master selon les choix et préconisation effectués au point précédent	César & Alix	05/09/24	19/09/24	14j	100 %	60 min		60 min	
1.5	Etablir la charte demandée dans la partie f),	César	05/09/24	19/09/24	14j	100 %	60 min	60 min		
							360 min			

Solutions correspondent au cahier des charge :

a , b) : equipement visiteur :

Acer Aspire 5 :
 	
• **Écran** : 15,6 pouces Full HD
• **Processeur** : Intel Core i5 (11e génération) ou AMD Ryzen 5
• **Mémoire vive (RAM)** : 8 Go (extensible à 16 Go)
• **Stockage** : SSD 512 Go
• **Connectivité** :
  ○ **Réseau filaire** : Port Ethernet RJ-45
  ○ **Réseau sans fil** : Wi-Fi 6 et Bluetooth 5.0
• **Autonomie** : Environ 8 heures
• **Prix estimé** : Entre **600€ et 700€**
	IdeaPad Slim 3 Gen 8 (14" AMD)
	
	Écran : 14 pouces Full HD
	
	Processeur : AMD Ryzen 5 5500U ou Intel Core i5
	
	Mémoire vive (RAM) : 8 Go
	
	Stockage : SSD 512 Go
	
	Connectivité :
	
	• Réseau filaire : Port Ethernet via adaptateur USB-C (adaptateur parfois inclus)
	• Réseau sans fil : Wi-Fi 6 et Bluetooth 5.0
	
	Autonomie : Jusqu'à 10 heures
	
	Prix estimé : Entre 650€ et 490
		Inspiron 15
		Processeur : Intel® Core™ i5-1235U, 12e génération (10 cœurs, jusqu'à 4,40 GHz)
		
		Système d'exploitation : Windows 11 Famille (options multilingues)
		
		Carte graphique : Intel® UHD
		
		Écran : 15,6" FHD (1920 x 1080), 120 Hz, IPS, non tactile,
		
		Mémoire : 8 Go DDR4 à 2 666 MHz
		
		Stockage : SSD 512 Go, PCIe NVMe
		
		prix estimé : 600 et 480

Pour les visiteurs, je propose l'**IdeaPad Slim 3 Gen 8 (14" AMD)**, qui respecte parfaitement le cahier des charges. Il est capable de supporter le travail demandé et offre un prix raisonnable.

c) :
Les logiciels que je recommande d'installer au préalable sont **Gmail**, **Google Drive**, ainsi que l'activation de **l'antivirus Windows**. Il y a aussi **Excel**, **Word**, et **Microsoft Visio**.

d) : Chaque PC de l'entreprise sera nommé en fonction de la catégorie de travail et de la salle correspondante. Ensuite, les PC seront nommés selon l'utilisateur auquel ils sont attribués avec son nom . Le bureau sera organisé par applications et logiciels, rangés dans des dossiers spécifiques qui seront communs gpo .

e) :

Clonezilla Server Édition	Fog Projects	DRBLS
permet de cloner plusieurs machines en même temps via le réseau. Voici ses principales caractéristiques : • Déploiement en réseau : Clonage simultané de plusieurs PC via SSH, Samba ou NFS. • Support de systèmes de fichiers : Compatible avec ext2/3/4, NTFS, FAT32, HFS+, XFS, JFS. • Création et restauration d'images : Sauvegarde et récupération de disques. • Automatisation : Processus de clonage automatisés pour déploiements en masse. • Gestion des partitions : Redimensionnement et gestion des partitions. • Support RAID : Compatible avec les configurations RAID. • Sécurité : Cryptage des données pour les sauvegardes. • Interface en ligne de commande : Configuration via CLI.	• **Déploiement en réseau** : Permet d'installer et de cloner des systèmes d'exploitation sur plusieurs ordinateurs via le réseau. • **Gestion d'images** : Crée, stocke et déploie des images disque pour la récupération et la sauvegarde. • **Support de divers systèmes** : Compatible avec Windows, Linux et autres systèmes d'exploitation. • **Interface web** : Administration via une interface web facile à utiliser pour gérer les tâches de clonage et déploiement. • **Automatisation** : Automatise les déploiements grâce à des scripts et des tâches programmées. • **Gestion des tâches** : Prend en charge le déploiement automatique de logiciels, mises à jour et configurations. • **Support PXE** : Utilise le protocole PXE pour démarrer les ordinateurs à partir du réseau lors du déploiement. • **Gratuit** : Solution open source, donc sans coût de licence.	**Démarrage sans disque** : Permet aux ordinateurs de démarrer et de fonctionner sans disque dur local, en utilisant une image système stockée sur un serveur. **Support de clients multiples** : Gère de nombreux clients simultanément via le réseau. **Déploiement de systèmes** : Clonage et déploiement de systèmes d'exploitation sur plusieurs machines. **Support de divers systèmes** : Compatible avec Linux et, avec des outils complémentaires, peut également fonctionner avec Windows. **Gestion des images** : Crée et déploie des images système sur les clients. **Interface web** : Administration via une interface web pour faciliter la gestion des tâches. **Support PXE** : Utilise le protocole PXE pour démarrer les ordinateurs à partir du réseau. **Gratuit** : Solution open source sans coût de licence.

Je choisis Clonezilla SE car c'est une solution gratuite et qu'elle est facilement manipulable sous Linux, offrant une flexibilité idéale pour mon environnement à faible budget.

Mise en place de la maquette :

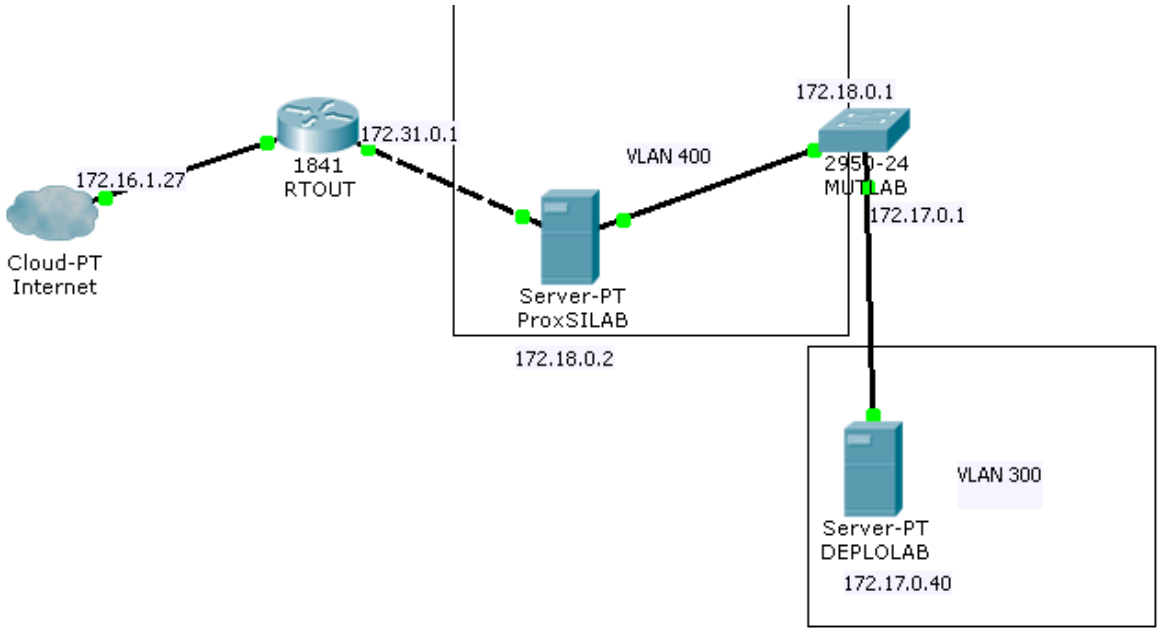


Schéma réseau

Mise en place des vlan et on leur attribue une adresse ip :

```
interface Vlan300
 ip address 172.17.0.1 255.255.0.0
!
interface Vlan400
 ip address 172.18.0.1 255.255.0.0
```

On active l'ip routing disponible sur les commutateur de niveau 3 :

```
no aaa new-model
system mtu routing 1500
ip routing
!
```

Schéma général du processus de déploiement de masterisation et déploiement des machines.

1. **Configurer le poste maître** : Installation du système d'exploitation, des logiciels, et configuration.
2. **Créer une image maître** : Capturer l'état du poste sous forme d'image disque.

3. **Déployer l'image** : Utiliser l'image pour cloner le système sur d'autres postes.
4. **Personnaliser chaque poste** : Ajuster les paramètres uniques à chaque machine.

Charte Informatique pour le Bon Usage de l'Équipement Informatique et la Sécurité des Données d'Entreprise

Préambule : Cette charte a pour objectif de définir les bonnes pratiques à suivre par l'ensemble des employés de l'entreprise en ce qui concerne l'usage de l'équipement informatique, la gestion de la sécurité et la prévention des vols. Les données traitées par l'entreprise sont sensibles, et il est primordial de les protéger, tant pour la sécurité des clients que pour la continuité des opérations de l'entreprise.

1. Objectifs :

- Garantir une utilisation conforme des ressources informatiques mises à disposition.
- Prévenir toute forme d'abus ou d'utilisation inappropriée des outils professionnels.
- Protéger les données sensibles et les systèmes critiques de l'entreprise contre toute forme de fuite, de vol ou d'attaque.
- Assurer la sécurité physique et numérique des infrastructures, y compris la salle des serveurs.

Chapitre 1 : Utilisation des Équipements Informatiques

1.1 Accès et Utilisation

- Chaque employé se voit attribuer des équipements informatiques (ordinateurs, téléphones, tablettes) qui sont la propriété de l'entreprise et ne doivent être utilisés qu'à des fins professionnelles.
- L'utilisation des équipements pour des raisons personnelles doit rester exceptionnelle et limitée à des cas justifiés, tout en respectant les politiques internes en matière de sécurité.
- Tout usage abusif des ressources informatiques à des fins personnelles (ex. téléchargement de contenu illégal, navigation sur des sites non professionnels) est interdit.

1.2 Authentification et Sécurité des Comptes

- Les employés sont responsables de la protection de leurs identifiants (mots de passe, badges, clés sécurisées). Ils doivent utiliser des mots de passe robustes et changer régulièrement ceux-ci.

- En cas de soupçon de compromission des identifiants, il est impératif de le signaler immédiatement à l'équipe de sécurité informatique.
- Les accès aux systèmes internes doivent être sécurisés par une authentification à plusieurs facteurs (ex : lecteur de badge et code PIN).

Chapitre 2 : Sécurité des Données

2.1 Protection des Données Sensibles

- Les données traitées par l'entreprise sont sensibles et leur protection est une priorité. Toute manipulation de ces données doit être réalisée dans le strict respect des procédures internes.
- Il est interdit de transférer ou copier des données professionnelles sensibles sur des supports personnels (ex : clés USB, disques durs externes, plateformes de stockage en ligne non approuvées).

2.2 Transmission des Données

- Les échanges de données sensibles doivent être effectués à l'aide d'outils de communication sécurisés, validés par le département informatique (ex : VPN, messagerie chiffrée).
- Toute fuite ou tentative de fuite de données sera considérée comme une faute grave et entraînera des sanctions disciplinaires, pouvant aller jusqu'au licenciement et à des poursuites judiciaires.

Chapitre 3 : Prévention du Vol et Sécurité Physique

3.1 Accès aux Infrastructures Critiques

- L'accès à la salle des serveurs est strictement limité aux personnes autorisées. Celui-ci est contrôlé par un système de double authentification (clé sécurisée et lecteur de badge).
- Il est interdit de partager ses clés ou badges d'accès avec des collègues non autorisés, ou avec toute autre personne extérieure à l'entreprise.
- Toute anomalie constatée dans les accès physiques (ex : porte laissée ouverte, présence de personnes non autorisées) doit être immédiatement signalée à la sécurité.

3.2 Prévention du Vol d'Équipement

- Les équipements informatiques (ordinateurs portables, téléphones) doivent être surveillés en permanence, notamment lors des déplacements professionnels.
- Tout vol ou perte d’équipement doit être signalé sans délai à l'équipe informatique et

- au service de sécurité pour prendre des mesures appropriées.

Chapitre 4 : Gestion des Risques et Sécurité Numérique

4.1 Mises à jour et Maintenance

- Les employés doivent veiller à ce que les équipements informatiques soient régulièrement mis à jour pour garantir un niveau de sécurité optimal. L'installation de correctifs de sécurité est obligatoire dès leur disponibilité.
- Il est interdit d'installer des logiciels non validés ou non approuvés par le service informatique, car ils peuvent représenter une menace pour la sécurité du réseau.

4.2 Sauvegarde des Données

- Les données sensibles doivent être régulièrement sauvegardées selon les protocoles définis par le département informatique. Toute perte de données due à une mauvaise gestion de ces procédures peut entraîner des sanctions.

Chapitre 5 : Utilisation Personnelle des Outils Professionnels

5.1 Cadre Limité de l'Utilisation Personnelle

- L’utilisation des équipements informatiques à des fins personnelles (mails, navigation internet) doit être limitée et ne doit en aucun cas nuire à la performance des outils professionnels ou à la sécurité des données.
- Les employés ne doivent pas utiliser leur poste de travail pour installer des logiciels ou accéder à des contenus non conformes aux politiques de l'entreprise (ex : contenus illégaux, sites non sécurisés).

5.2 Responsabilité en Cas d’Abus

- Tout abus ou utilisation inappropriée des ressources professionnelles à des fins personnelles sera sanctionné. Les sanctions peuvent inclure des avertissements, des suspensions ou des licenciements en fonction de la gravité de la faute.

Chapitre 6 : Formation et Sensibilisation

6.1 Sessions de Sensibilisation

- Des formations régulières sur les bonnes pratiques de sécurité informatique seront dispensées à l'ensemble des employés. La participation à ces sessions est obligatoire.
- Les employés sont également invités à se tenir informés des nouvelles menaces en matière de cybersécurité et à respecter les consignes qui en découlent.

6.2 Remontée des Incidents

- Toute suspicion de compromission des systèmes ou des données doit être signalée immédiatement à l'équipe informatique via les canaux prévus à cet effet.

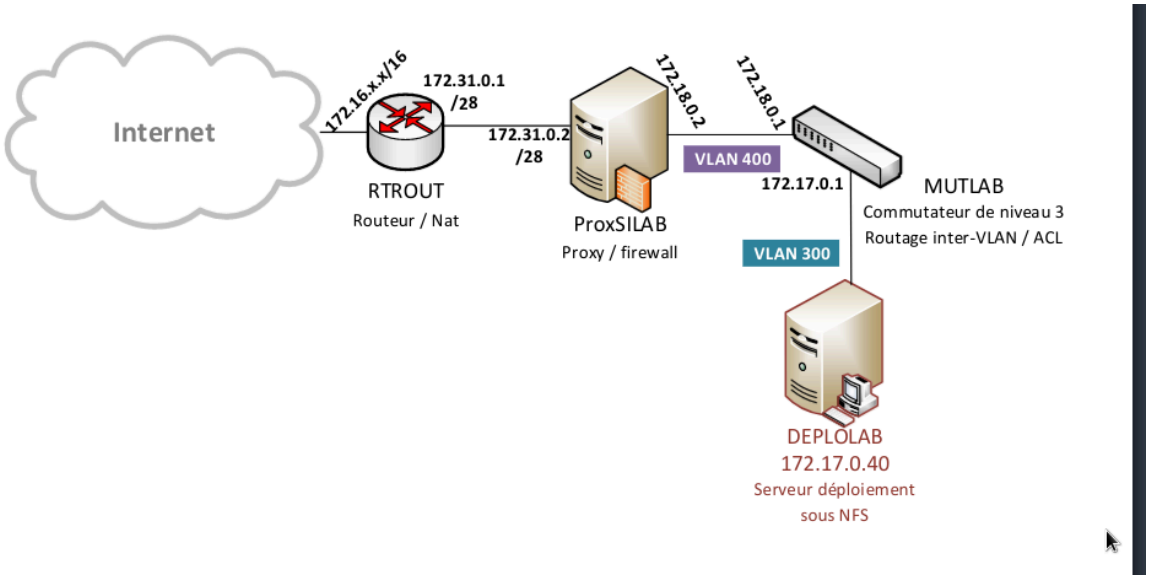
Conclusion :

La bonne utilisation des outils informatiques et la protection des données sont essentielles pour garantir la sécurité et la pérennité de l'entreprise. Tout manquement aux dispositions de cette charte pourra entraîner des sanctions disciplinaires adaptées à la gravité des faits. Chaque employé est invité à prendre cette charte au sérieux et à l'appliquer dans l'intérêt collectif.

Date de mise en application : 7 Septembre 2024

Signature :

Système de partage de fichier Linux-NFS :



Dans un premier temps j'ai créé une machine virtuelle où je vais mettre mon serveur NFS . J'attribue une adresse IP 172.17.0.40

```
# The loopback network interf
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
address 172.17.0.40
netmask 255.255.0.0
gateway 172.17.255.255
```

La commande pour l'installer le serveur :

```
root@Debian-12-Bookworm:/home/partage/Image# apt-get install nfs-kernel-server
```

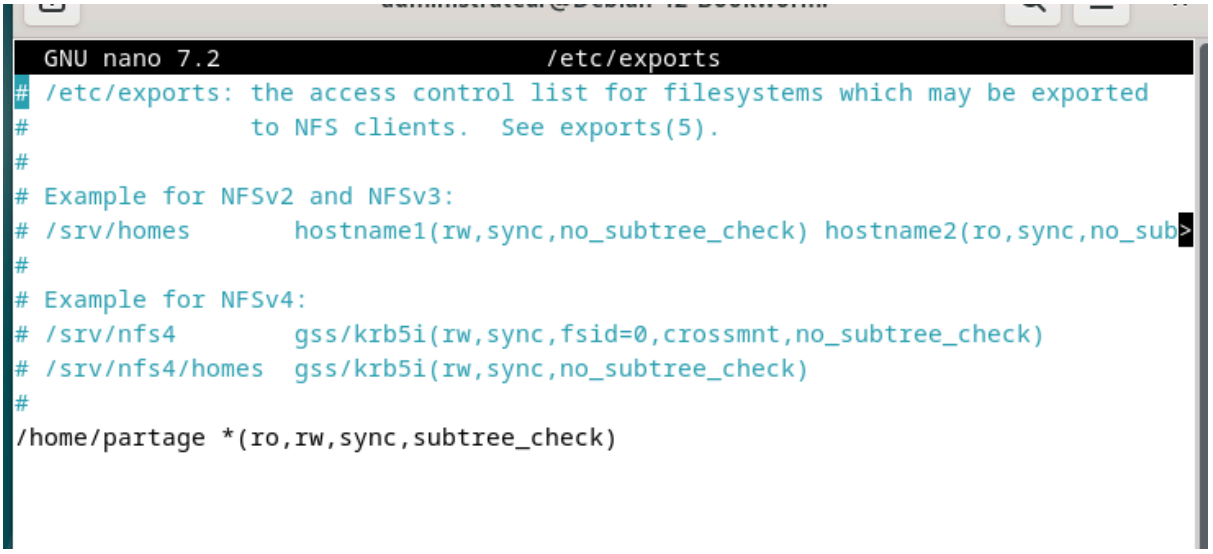
une fois que le serveur et installe il faut l'activité avec la commande :

```
root@Debian-12-Bookworm:/home/partage/Image# sudo systemctl enable nfs-server
```

Quand tout cela est fait, il faut créer le dossier **partage** pour que le client puisse y accéder.

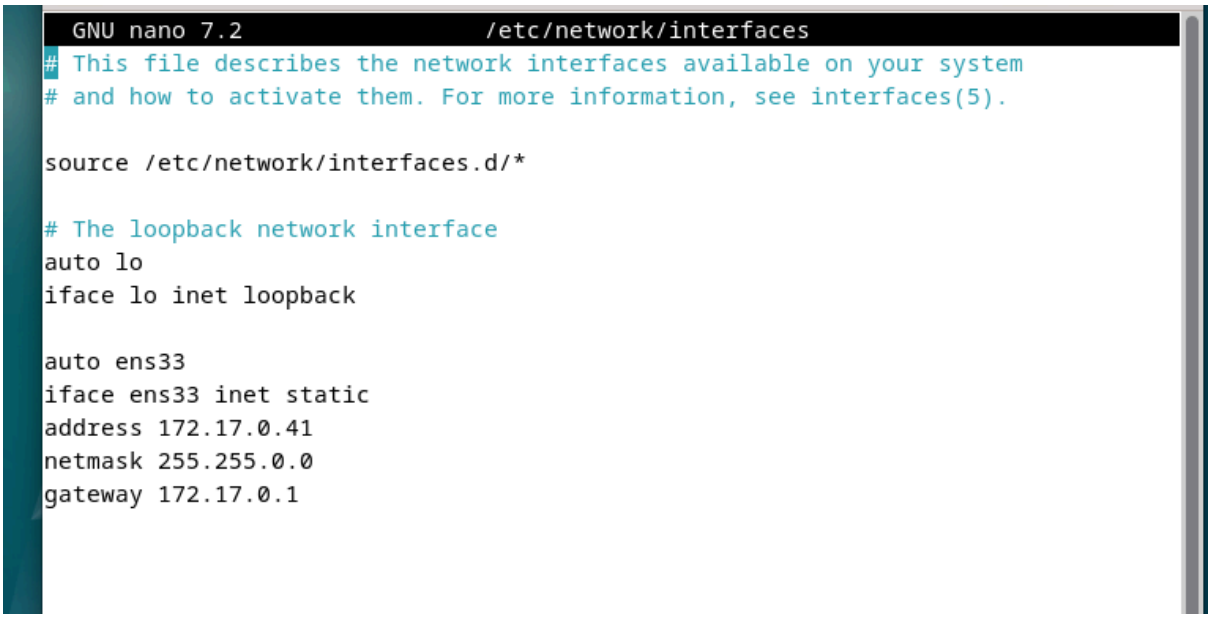
Le dossier **partage** sur le serveur est dans `home/partage/`. Je lui ai attribué les droits 777 `-R` pour que l'utilisateur puisse y accéder.

Ensuite, il faut créer un fichier dans `/etc/exports` pour pouvoir préciser l'emplacement du partage ainsi que l'IP.



ensuite il faut validé l'exportation avec la commande : exportfs -a

Machine client :
Pour la deuxième partie le client a lui aussi son adresse IP



Une fois que cela et fait il faut installer le client serveur nfs

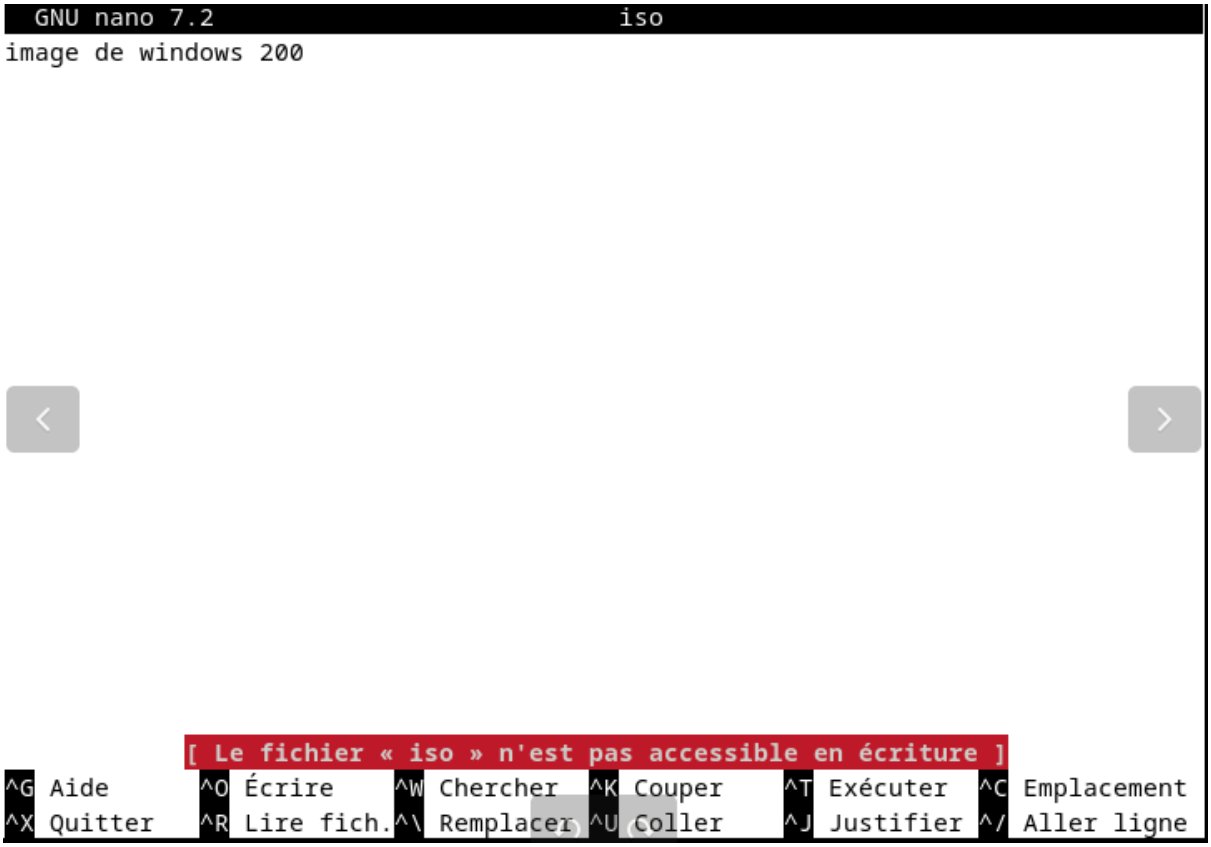
```
root@Debian-12-Bookworm:/media/montage/Image# sudo apt install nfs-common
```

Ensuite il faut créer un répertoire là où le client va pouvoir aller sur le partage comme une clé usb .

```
root@Debian-12-Bookworm:/media/montage/Image# mkdir /media/montage
```

Cette commande et pour préciser au client que le partage et sur le serveur avec son adresse IP et il précise aussi que le client vas voir le partage sur le dossier Media
Quand tout ça est terminé, il faut vérifier dans Media et montage si le client voit bien le partage du serveur nfs .

```
root@Debian-12-Bookworm:/home/administrateur# mount -t nfs 172.17.0.40:/home/partage /media/montage
```



Choix de la mise en place de la masterisation des postes :

- On utilisera un serveur Debian NFS qui est une solution gratuite et open source.

Outils de déploiement dans un serveur Debian NFS :

- PXE (Preboot Execution Environment)
- Cobbler
- Clonezilla Server Édition
- FAI (Fully Automatic Installation)
- Ansible
- FOG Project

Comparaison des outils de déploiement :

Outils	Gratuité	Description de l'outil	Facilité d'utilisation	Coût
PXE	Gratuit	Il permet à un ordinateur d'accéder à un système d'exploitation ou à un dispositif de démarrage au travers d'une connexion réseau, le système étant hébergé sur un serveur distant (NTFS)	Compliqué d'utilisation (compétences requises en réseau - DHCP et configuration réseau)	0 euro
Cobbler	Gratuit	Il sert à centraliser et à automatiser le packaging et le provisioning de logiciels dans l'environnement d'exploitation de l'entreprise	Compliqué d'utilisation (interface en ligne de commande et une API REST)	0 euro
Clonezilla Server Edition	Gratuit	Cela permet de cloner et de déployer des images de systèmes d'exploitation sur plusieurs machines simultanément via un réseau.	Compliqué d'utilisation (interface en ligne de commande, configuration réseau, etc…)	0 euro
FAI	Gratuit	C'est un	Difficile à utiliser	0 euro

		ensemble de scripts Shell et Perl permettant d'installer et de configurer un système d'exploitation Linux complet rapidement sur un grand nombre d'ordinateurs.	(compétences et connaissances des scripts et des principes d'installation Linux) et efficace pour le déploiement (notamment pour les installations en masse)	
Ansible	Gratuit	Cet outil permet d'exécuter des playbooks (fichiers textes écrits en YAML qui contient les tâches à exécuter sur les postes hôtes) sur plusieurs systèmes avec une seule commande.	Simple à utiliser (syntaxe simple en YAML, approche simple et utilise aucun agent ni aucune infrastructure de sécurité personnalisée supplémentaire)	0 euro
FOB Project	Gratuit	FOB Project est un outil pour le déploiement automatisé de systèmes d'exploitation et la gestion de configurations pour les environnements Linux. Il propose des fonctionnalités telles que la gestion des installations à distance, la configuration automatique et la mise à jour des systèmes	Difficile à utiliser (Interface graphique peu intuitive, documentation complexe dû au manque d'informations, configuration nécessite des compétences en réseaux et systèmes ainsi qu'en scripting)	0 euro

Méthodologie post-configuration des postes après la descente des images systèmes:

- Test de démarrage des ordinateurs pour voir si les images iso ont été correctement mises
- Vérification de l'installation des logiciels
- Mise en place du réseau informatique sur les ordinateurs de l'entreprise GSB (adresse IP, masque, passerelle => pour avoir accès à internet)
- Intégration des ordinateurs dans l'Active Directory de GSB
- Dans l'annuaire, créer les utilisateurs et de mots de passe pour tous les salariés de GSB

Choix de configuration/préparation du master :

- Serveur Debian NFS
- Outil de déploiement des images systèmes : Ansible, car il est simple d'utilisation par rapport aux autres outils qui sont plus difficiles à utiliser.

Charte Informatique de l'entreprise GSB :

Charte d'Utilisation du Matériel Professionnel Prêté

Préambule

Cette charte a pour objectif de définir les règles d'utilisation du matériel professionnel prêté par GSB à ses collaborateurs intervenant chez les clients. Le non-respect de ces règles pourra entraîner des sanctions disciplinaires.

1. Champ d'application

Cette charte s'applique à tout collaborateur de l'entreprise GSB amené à utiliser du matériel professionnel prêté par l'entreprise dans le cadre de ses missions.

2. Définitions

- **Matériel professionnel** : Tout équipement (ordinateur portable, tablette, téléphone, outillage, etc.) mis à disposition du collaborateur par l'entreprise pour l'exercice de ses fonctions.
- **Utilisateur** : Tout collaborateur autorisé à utiliser le matériel professionnel.

3. Obligations de l'utilisateur

- **Utilisation conforme** : Le matériel doit être utilisé exclusivement dans le cadre des missions confiées par l'entreprise et conformément à sa destination.
- **Entretien** : L'utilisateur s'engage à prendre soin du matériel et à le conserver en bon état.
- **Sécurité** : L'utilisateur doit respecter les règles de sécurité en vigueur lors de l'utilisation du matériel.

- **Protection des données** : L'utilisateur est responsable de la confidentialité des données traitées sur le matériel et s'engage à respecter les règles de sécurité informatique en vigueur.
- **Inventaire** : L'utilisateur doit participer aux inventaires réguliers du matériel.
- **Retour** : En cas de cessation d'activité ou de changement de poste, l'utilisateur doit restituer le matériel en bon état de fonctionnement.

4. Responsabilité

- **Pertes et vols** : En cas de perte, de vol ou de dégradation du matériel, l'utilisateur peut être tenu responsable financièrement.
- **Réparations** : Les réparations nécessaires suite à une utilisation non conforme ou à une négligence de l'utilisateur seront à sa charge.

5. Sanctions

Le non-respect de cette charte pourra entraîner des sanctions disciplinaires, conformément aux dispositions du règlement intérieur de l'entreprise.

6. Dispositions finales

Cette charte peut être modifiée à tout moment par la direction de l'entreprise.

Points importants à considérer lors de la rédaction de cette charte :

- **Précision des équipements concernés :** Lister les différents types de matériel prêté (ordinateurs, outils spécifiques, etc.).
- **Modalités de prêt et de restitution :** Préciser les conditions de prêt (bon de prêt, inventaire), les modalités de restitution (état des lieux) et les conséquences en cas de non-restitution.
- **Assurances :** Indiquer si une assurance couvre le matériel prêté et dans quelles conditions.
- **Formation :** Prévoir des formations pour les utilisateurs afin de les sensibiliser aux bonnes pratiques d'utilisation.