

Infrastructure & Système d'information

Lucas Gerard -Jordan Milleville

Documentation projet SI "Partage Réseau et Annuaire"

Contexte et Objectifs :

Le projet "Partage Réseau + Annuaire" vise à créer un système de partage de fichiers sécurisé et efficace au sein d'un réseau local. Il a pour but de mettre en place un réseau permettant aux utilisateurs un accès centralisé et contrôlé aux ressources partagées, tout en assurant des sauvegardes régulières des données.

Objectifs Principaux

Centralisation des Ressources :

Établir un dossier partagé accessible à tous les utilisateurs autorisés, favorisant la collaboration et simplifiant la gestion des fichiers au sein du réseau. Cela permet à chacun d'accéder facilement aux documents nécessaires sans avoir à les chercher sur divers appareils.

Sécurité des Données :

Configurer des permissions d'accès rigoureuses pour chaque utilisateur afin de sécuriser les données sensibles. Ceci garantit que seules les personnes autorisées peuvent accéder aux fichiers et répertoires critiques, renforçant ainsi la confidentialité et la protection contre les intrusions non autorisées.

Automatisation des Sauvegardes :

Développer et déployer un script de sauvegarde automatique pour assurer une protection continue des données stockées dans le répertoire partagé. Cette automatisation régulière minimise le risque de perte de données et offre une tranquillité d'esprit en cas de sinistre ou de défaillance du système.

Gestion Efficace des Utilisateurs :

Utiliser des outils tels que Samba et Webmin pour simplifier la gestion quotidienne des utilisateurs et de leurs permissions. Ces solutions facilitent l'administration du réseau en centralisant la gestion des comptes, des accès aux fichiers et des autorisations, optimisant ainsi les opérations administratives.

Étapes de Réalisation

Le projet est structuré en plusieurs étapes, détaillées dans cette documentation, afin de guider l'administrateur système à travers la configuration et la mise en œuvre de la solution :

1. Installation de la Machine Virtuelle (VM)

Objectif : Configurer une machine virtuelle avec VMware Workstation sous Linux, en utilisant Ubuntu comme distribution, pour servir de serveur.

Paramètres pour la VM :

- **Choix de l'hyperviseur :** [VMware Workstation](#)
- **Système d'exploitation choisi :** Ubuntu Server 24.04

Étapes d'installation :

1. **Téléchargement de l'ISO :**
 - Téléchargez l'image ISO d'Ubuntu Server depuis le site officiel [Ubuntu](#).
2. **Création de la VM :**
 - Ouvrez VMware Workstation.
 - Cliquez sur "Create a New Virtual Machine".
 - Sélectionnez "Installer disc image file (iso)" et choisissez l'ISO téléchargé.
 - Suivez les instructions pour configurer les différents paramètres de la VM.
3. **Installation d'Ubuntu :**
 - Démarrez la VM.
 - Suivez les instructions à l'écran pour installer Ubuntu Server.
4. **Configuration du réseau en mode Bridge :**
 - Allez dans les paramètres de la VM.
 - Sous "Network Adapter", sélectionnez "Bridged : Connected directly to the physical network".

Explication :

Pour ce projet, nous devons changer le type de connexion réseau par défaut de NAT à Bridge.

- **NAT (Network Address Translation) :** Les VMs partagent l'adresse IP de l'hôte et ne sont pas accessibles depuis le réseau externe. Ce mode convient pour les tests simples ou lorsque les VMs n'ont pas besoin de communiquer avec le réseau local.
- **Bridge :** Chaque VM obtient une adresse IP unique du réseau local, permettant une communication directe avec les autres machines. Ce mode est choisi pour une interaction fluide avec le réseau local.

• 2. Configuration du réseau

Objectif : Configurer le réseau de la machine virtuelle pour permettre une communication fluide et directe entre la VM Ubuntu et les autres dispositifs du réseau local en utilisant le mode Bridge.

1. Vérification des adresses IP :

- **Windows :**
 - Ouvrez une invite de commande et tapez : ipconfig
 - Notez l'adresse IP.
- **Linux (Ubuntu) :**
 - Installez net-tools grâce à la commande : `sudo apt-get install net-tools`
 - Tapez : `ifconfig`
 - Notez l'adresse IP.

2. Test de communication :

- **Depuis Windows :** `ping <IP_Ubuntu>`
- **Depuis Linux :** `ping <IP_Windows>`

```

Microsoft Windows [version 10.0.22631.3737]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\lucas>ipconfig

Carte réseau sans fil Wi-Fi :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6. . . . . :
    Adresse IPv6 temporaire. . . . . :
    Adresse IPv6 de liaison locale. . . . . :
    Adresse IPv4. . . . . : 192.168.1.168
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : fe80::de00:b0ff:fe60:3310%12
                                     192.168.1.254
  
```

Récupération de l'adresse IP de la machine sous Windows

```

C:\Users\lucas>ping 192.168.1.86

Envoi d'une requête 'Ping' 192.168.1.86 avec 32 octets de données :
Réponse de 192.168.1.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.86 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.86:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
  
```

Test de communication de Windows à Linux (VM)

```

lucas@lucas-VMware-Virtual-Platform: ~$ sudo apt-get install net-tools
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
net-tools est déjà la version la plus récente (2.10-0.1ubuntu4).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 3 non mis à jour.
lucas@lucas-VMware-Virtual-Platform:~$
  
```

Installation de l'outil net-tools afin de récupérer l'adresse IP plus facilement

```

lucas@lucas-VMware-Virtual-Platform: ~$ ping 192.168.1.168
PING 192.168.1.168 (192.168.1.168) 56(84) bytes of data:
64 bytes from 192.168.1.168: icmp_seq=1 ttl=128 time=0.628 ms
64 bytes from 192.168.1.168: icmp_seq=2 ttl=128 time=0.594 ms
64 bytes from 192.168.1.168: icmp_seq=3 ttl=128 time=0.697 ms
64 bytes from 192.168.1.168: icmp_seq=4 ttl=128 time=0.778 ms
^C
--- 192.168.1.168 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3085ms
rtt min/avg/max/mdev = 0.584/0.651/0.778/0.100 ms
lucas@lucas-VMware-Virtual-Platform:~$
  
```

Test de communication de Linux (VM) à Windows

```

lucas@lucas-VMware-Virtual-Platform: ~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.86 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2a01:e0a:c0a:68a0:9d76:6f31:35e0:1f10 prefixlen 64 scopeid 0x0<global>
    inet6 2a01:e0a:c0a:68a0:20c:29ff:feef:4e94 prefixlen 64 scopeid 0x0<global>
  
```

Récupération de l'adresse IP de la machine sous Linux (VM)

3. Installation et configuration de [Samba](#) pour le partage de fichiers

Objectif : Installer et configurer Samba sur la machine virtuelle Ubuntu afin de permettre le partage de fichiers avec d'autres ordinateurs du réseau local de manière sécurisée et efficace.

Introduction à Samba :

Samba est une suite de logiciels open source qui permet aux systèmes d'exploitation de type Unix/Linux de partager des fichiers et des imprimantes avec des ordinateurs exécutant Windows.

Il implémente le protocole SMB/CIFS (Server Message Block / Common Internet File System), largement utilisé dans les environnements réseau hétérogènes pour le partage de ressources entre différents systèmes d'exploitation.

Server Message Block (SMB) :

- Le SMB est un protocole de communication réseau, il permet le partage de fichiers, d'imprimantes, de ports série et d'autres ressources entre des ordinateurs sur un réseau local.
- Il facilite l'accès aux fichiers et services réseau en permettant à un client de demander des ressources sur un serveur et de gérer les opérations de fichiers à distance.

Common Internet File System (CIFS) :

- Le CIFS est une version améliorée et plus moderne du protocole SMB, fournissant une sécurité accrue et une compatibilité améliorée avec les systèmes d'exploitation non-Windows.
- Il prend en charge des fonctionnalités telles que l'authentification Kerberos, la compression des données.

Fonctionnement du SMB/CIFS :

- **Partage de Fichiers :** Un serveur SMB partage des dossiers et des fichiers avec des clients sur le réseau. Les clients peuvent monter ces partages comme s'ils étaient des disques locaux, leur permettant d'accéder et de manipuler les fichiers comme s'ils étaient sur leur propre système.
- **Authentification :** Le protocole SMB/CIFS utilise des mécanismes d'authentification pour vérifier l'identité des utilisateurs qui accèdent aux partages. Cela peut inclure l'authentification par nom d'utilisateur/mot de passe, ou des méthodes plus avancées comme l'authentification Kerberos.
- **Gestion des Sessions :** Il gère les sessions utilisateur en attribuant des identifiants de session uniques aux clients qui se connectent aux ressources partagées. Cela permet une gestion efficace des connexions et des transferts de données.

1. Vérification des mises à jour Ubuntu :

- Exécutez la commande suivante pour mettre à jour le système



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

Effectuer régulièrement les mises à jour sur Ubuntu est essentiel pour maintenir le système sécurisé et optimisé. L'utilisation de `sudo` avant la commande confère temporairement des privilèges administratifs, assurant que les modifications système peuvent être apportées en toute sécurité.

La commande commence par mettre à jour la liste des paquets disponibles avec `apt update`, garantissant ainsi que le système dispose des informations les plus récentes sur les versions disponibles et les dépendances logicielles. Ensuite, `apt upgrade -y` permet de mettre à jour automatiquement tous les paquets installés sans nécessiter d'intervention de l'utilisateur pour chaque mise à jour individuelle.

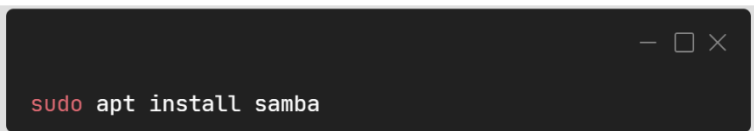
`apt` est l'outil principal de gestion des paquets sous Ubuntu, assurant une gestion cohérente des installations, des mises à jour et des suppressions de logiciels.

L'opérateur `&&` permet d'exécuter plusieurs commandes en séquence dans un seul appel, assurant une exécution efficace des tâches système.

Le paramètre `-y` indique à `apt` d'accepter automatiquement toutes les modifications proposées sans nécessiter de confirmation manuelle de l'utilisateur, ce qui est particulièrement utile pour les tâches d'automatisation ou lorsqu'on veut éviter les prompts interactifs.

2. Installation de Samba :

- Exécutez la commande suivante pour installer samba

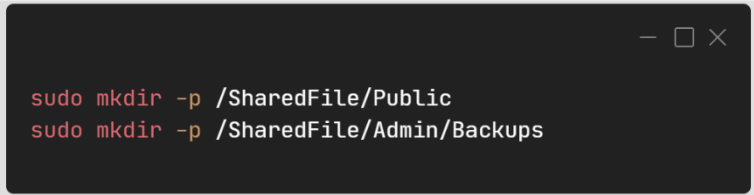


```
sudo apt install samba
```

Cette commande installe les paquets nécessaires pour le logiciel Samba.

3. Création des répertoires de partage :

- Exécutez la commande suivante pour permettre la création des différents fichiers de partage



```
sudo mkdir -p /SharedFile/Public  
sudo mkdir -p /SharedFile/Admin/Backups
```

Ces commandes créent les répertoires avec le chemin en paramètre sur le système de fichiers. On utilise `mkdir` pour créer des répertoires. L'option `-p` est utilisée pour créer tous les répertoires nécessaires. Cela évite les erreurs si des répertoires parents nécessaires n'existent pas encore. La création de répertoire est essentielle pour préparer l'espace de stockage où les fichiers seront partagés et utilisés ultérieurement dans les configurations de partage de fichiers, facilitant ainsi l'organisation et la gestion des données partagées sur le réseau.

4. Configuration de Samba :

- Exécutez la commande suivante pour modifier le fichier `smb.conf` :



```
sudo nano /etc/samba/smb.conf
```

Cette commande est utilisée pour éditer le fichier de configuration principal de Samba, situé à `/etc/samba/smb.conf`. Il contient toutes les instructions nécessaires pour configurer les partages de fichiers et autres paramètres importants de Samba. L'utilisation de `sudo` garantit que nous avons les permissions nécessaires pour modifier ce fichier, tandis que `nano` est l'éditeur de texte en ligne de commande que nous utilisons pour effectuer les modifications directement dans le terminal.

- Ajoutez les sections suivantes à la fin du fichier :

```
[Public]
comment = Dossier de partage
path = /SharedFile/Public
browseable = yes
writable = yes
guest ok = yes
valid users = @GRPUsers, @GRPadmins

[Admin]
comment = Dossier Administrateur
path = /SharedFile/Admin
browseable = yes
writable = yes
guest ok = no
valid users = @GRPadmins
```

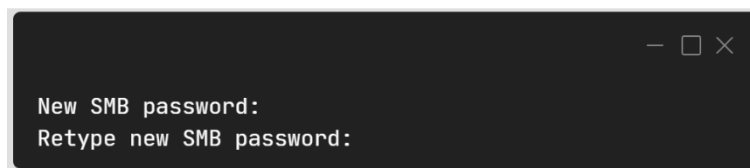
L'ajout de ses sections permet l'ajout des documents partagés, les lignes path, browseable, writable, guest ok et valid users sont utilisées pour configurer chaque partage. Par exemple, path définit le chemin du répertoire partagé, browseable contrôle la visibilité du partage, writable autorise l'écriture de fichiers, guest ok permet l'accès en tant qu'invité, et valid users spécifie les utilisateurs autorisés, y compris les groupes avec @group-name.

5. Création des utilisateurs Samba :

```
sudo smbpasswd -a user
sudo smbpasswd -a admin
```

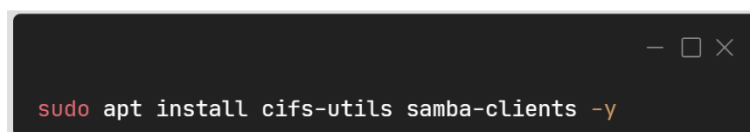
Cette commande est spécifique à Samba. Elle est utilisée pour ajouter un utilisateur au système d'authentification de Samba, en lui permettant d'accéder aux partages réseau configurés via Samba. L'option -a indique à smbpasswd d'ajouter un nouvel utilisateur.

6. Remplir les informations demandées pour la création des utilisateurs



Samba demande "New SMB password", elle sollicite l'utilisateur à saisir le nouveau mot de passe qu'il souhaite définir pour cet utilisateur. Cette étape est essentielle pour sécuriser l'accès aux partages de fichiers Samba. Ensuite, elle demande de "Retype new SMB password" pour confirmer le mot de passe en le saisissant à nouveau. Cette double saisie permet de s'assurer qu'il n'y a pas eu d'erreur de frappe lors de la définition du nouveau mot de passe.

7. Exécuté la commande afin de finaliser l'installation et configuration de Samba et de ses fonctionnalités



Cette commande est utilisée pour installer les utilitaires nécessaires à la gestion des partages de fichiers SMB/CIFS et pour interagir avec les serveurs Samba sous Ubuntu. Le paramètre -y permet d'accepter automatiquement toutes les modifications proposées par la commande sans confirmation manuelle de l'utilisateur.

8. Vérifiez les règles du pare-feu

- Assurez-vous que le pare-feu sur votre serveur permet les connexions Samba :



Cette commande vérifie les règles actuelles du pare-feu UFW (Uncomplicated Firewall), affichant quelles connexions sont actuellement autorisées ou bloquées. Cela est essentiel pour s'assurer que les ports nécessaires pour Samba sont ouverts.


- Pour permettre les connexions Samba, utilisez :



```
sudo ufw allow 'Samba'
```

Cette commande configure UFW pour autoriser le trafic nécessaire pour les services Samba, permettant ainsi les connexions réseau pour le partage de fichiers. Cela ouvre les ports requis par Samba pour fonctionner correctement.

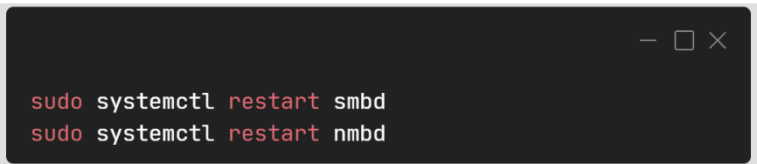
9. Redémarrez le serveur



```
sudo reboot
```

Cette commande redémarre le serveur, ce qui peut aider à appliquer toutes les modifications de configuration et résoudre les problèmes qui pourraient ne pas être pris en compte sans un redémarrage complet. Cela garantit que tous les services, y compris ceux de Samba, redémarrent avec les nouvelles configurations.

10. Redémarrage de Samba :



```
sudo systemctl restart smbd  
sudo systemctl restart nmbd
```

La commande `systemctl restart` est essentielle sous `systemd`, le gestionnaire d'initiation de Linux. Elle est utilisée pour redémarrer les services, notamment `smbd` pour la gestion des partages de fichiers et d'imprimantes via Samba, ainsi que `nmbd` pour la résolution des noms NetBIOS sur les réseaux locaux. Ce redémarrage est crucial après toute modification de configuration afin d'appliquer les changements effectués sur le système.

4. Installation et configuration de [Webmin](#) pour le partage de fichiers

Objectif : Installer les paquets nécessaires pour ajouter des dépôts externes et télécharger des fichiers via le protocole HTTPS.

Introduction à Webmin :

Webmin est un outil d'administration système basé sur le web pour Unix. Il permet aux administrateurs de gérer les utilisateurs, les groupes, les disques, les services et bien d'autres aspects du système à partir d'une interface web conviviale. Webmin simplifie la gestion des serveurs et des services, évitant ainsi la nécessité de maîtriser les commandes en ligne de commande.

Technologie Utilisée :

Webmin est écrit en Perl et fonctionne comme un service web. Il utilise le protocole HTTPS pour sécuriser les communications entre le serveur et le navigateur de l'administrateur. Webmin repose sur une architecture modulaire, permettant l'extension de ses fonctionnalités via des modules supplémentaires pour différents services et applications.

- **Interface Web :** Permet l'administration via un navigateur web, accessible à partir de n'importe quel système sur le réseau.
- **Modules :** Chaque service ou fonctionnalité est géré par un module spécifique, rendant Webmin très extensible.
- **Protocole HTTPS :** Sécurise les communications pour protéger les données transmises entre le client (navigateur) et le serveur Webmin.

Alternatives à Webmin :

- **phpMyAdmin :** Pour la gestion de bases de données MySQL/MariaDB.
- **Cockpit :** Un autre outil d'administration système avec une interface web moderne, souvent utilisé pour gérer des serveurs Linux.
- **cPanel/WHM :** Solution commerciale largement utilisée pour la gestion de serveurs web et de services d'hébergement.

1. Vérification des mises à jour Ubuntu :

- Exécutez la commande suivante pour mettre à jour le système



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

Effectuer régulièrement les mises à jour sur Ubuntu est essentiel pour maintenir le système sécurisé et optimisé. L'utilisation de `sudo` avant la commande confère temporairement des privilèges administratifs, assurant que les modifications système peuvent être apportées en toute sécurité.

2. Installation des paquets requis

- Exécutez la commande suivante installer les paquets nécessaires pour ajouter des dépôts externes et télécharger des fichiers via le protocole HTTPS.

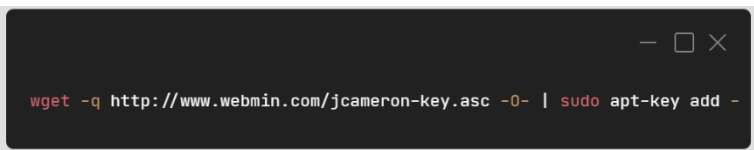


```
sudo apt install software-properties-common apt-transport-https wget -y
```

Effectuer cette commande installe `software-properties-common`, `apt-transport-https` et `wget`, qui sont essentiels pour gérer les sources de paquets, permettre les téléchargements via HTTPS, et récupérer des fichiers depuis des URL. Le paramètre `-y` assure que toutes les confirmations nécessaires sont automatiquement acceptées.

3. Ajouter la clé de dépôt de Webmin

- Ajouter la clé GPG de Webmin pour garantir l'authenticité des paquets téléchargés.



```
wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
```

Cette commande télécharge la clé GPG (GNU Privacy Guard) de Webmin, une clé cryptographique utilisée pour sécuriser les communications et vérifier l'authenticité des données. Pour l'ajouter au système pour vérifier l'authenticité des paquets lors de leur installation.

4. Ajouter le dépôt Webmin

- Ajouter le dépôt Webmin à la liste des sources de paquets.




```
sudo add-apt-repository "deb [arch=amd64] http://download.webmin.com/download/repository sarge contrib"
```

Cette commande ajoute le dépôt officiel de Webmin à la liste des sources de paquets d'APT, permettant ainsi au système de télécharger et d'installer Webmin directement depuis ce dépôt.

5. Mettre à jour les paquets

- Mettre à jour la liste des paquets pour inclure le dépôt Webmin.



```
sudo apt update
```

Exécuter cette commande met à jour la liste des paquets disponibles en incluant les nouveaux dépôts ajoutés, y compris celui de Webmin.

6. Installer Webmin

- Installer Webmin sur le système.




```
sudo apt install webmin -y
```

Cette commande installe Webmin, un outil d'administration système basé sur le web, avec toutes les dépendances nécessaires. Le paramètre -y permet une installation sans confirmation manuelle.

7. Vérifier le statut du service Webmin

- Vérifier que le service Webmin est actif et en cours d'exécution.



```
sudo systemctl status webmin.service
```

Cette commande affiche le statut actuel du service Webmin, confirmant s'il est actif, inactif, ou rencontre des problèmes.

8. Vérifier l'état du pare-feu

- Vérifier l'état actuel du pare-feu UFW (Uncomplicated Firewall).



```
sudo ufw status
```

Cette commande affiche l'état actuel du pare-feu UFW, indiquant quelles règles sont appliquées et si le pare-feu est activé ou non.

9. Autoriser le port Webmin dans le pare-feu

- Ouvrir le port 10000 pour permettre l'accès à Webmin.

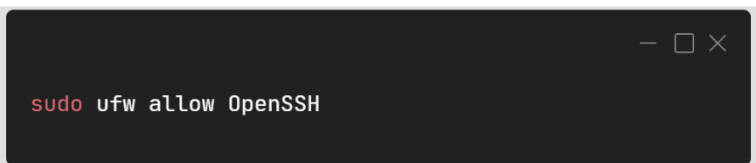


```
sudo ufw allow 10000
```

Cette commande configure UFW pour autoriser le trafic entrant sur le port 10000, qui est le port par défaut utilisé par Webmin pour l'accès web.

10. Autoriser les connexions SSH

- Ouvrir le port SSH pour permettre l'administration à distance.



```
sudo ufw allow OpenSSH
```

Cette commande permet les connexions SSH en ajoutant une règle à UFW pour autoriser le trafic entrant sur le port 22, facilitant ainsi l'administration à distance.

11. Activer le pare-feu UFW

- Activer le pare-feu UFW pour appliquer les règles définies.

```
sudo ufw enable
```

Cette commande active le pare-feu UFW, appliquant toutes les règles configurées et renforçant ainsi la sécurité du système en contrôlant le trafic réseau.

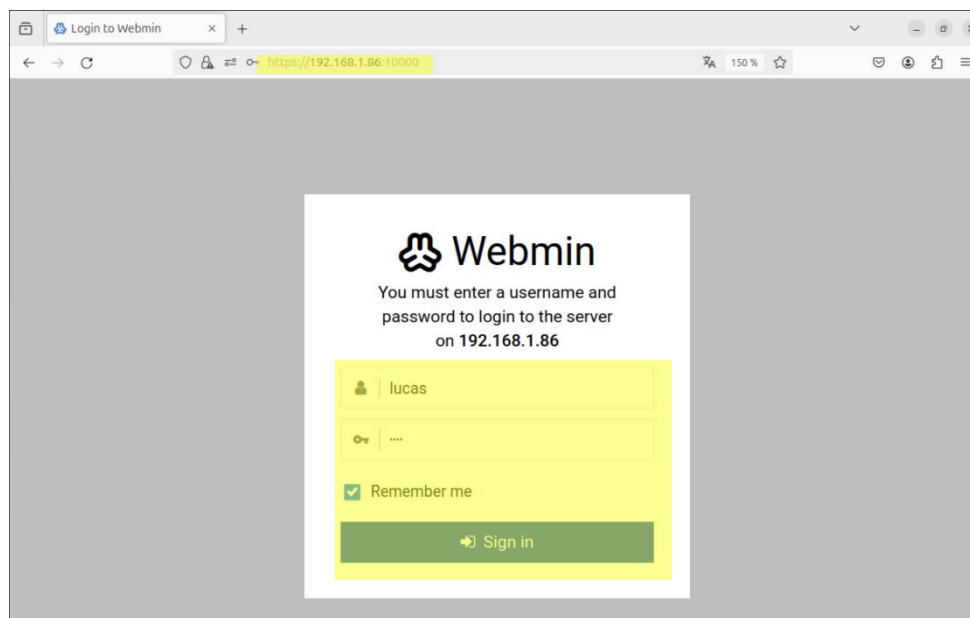
Paramétrage de [Webmin](#) et configuration des partages Samba

Objectif : Configurer Webmin pour gérer facilement les utilisateurs et les partages Samba, permettant une administration simplifiée du serveur.

1. Accéder à Webmin

- Accéder à l'interface Webmin via un navigateur pour gérer le serveur.

Ouvrez votre navigateur et tapez l'adresse suivante : <adresse du serveur> :10000



Page de connexion Webmin

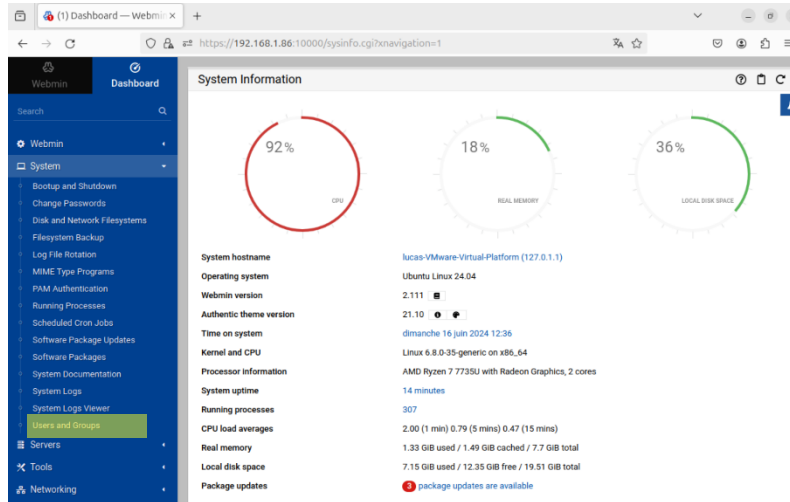
Webmin utilise le port 10000 par défaut. Cette interface web permet d'administrer le serveur Ubuntu et les services associés, comme Samba, via une interface graphique conviviale. Vous devrez vous connecter avec un utilisateur ayant des privilèges administratifs pour accéder et configurer les services.

2. Ajouter un Utilisateur Linux Local

- Créer un nouvel utilisateur local sur le système via Webmin.

Étapes

1. Dans Webmin, allez dans System > Users and Groups.



Dashboard du logiciel Webmin

2. Cliquez sur Create a new user.

The screenshot shows the 'Users and Groups' page in Webmin. It displays a table of local users and groups. The table has columns for Username, User ID, Group, Real name, Home directory, and Shell. A 'Create a new user' button is visible at the top right of the table.

Username	User ID	Group	Real name	Home directory	Shell
root	0	root	root	/root	/bin/bash
daemon	1	daemon	daemon	/usr/sbin	/usr/sbin/n
bin	2	bin	bin	/bin	/usr/sbin/n
sys	3	sys	sys	/dev	/usr/sbin/n
sync	4	nogroup	sync	/bin	/bin/lynx
games	5	games	games	/usr/games	/usr/sbin/n
man	6	man	man	/var/cache/man	/usr/sbin/n
lp	7	lp	lp	/var/spool/lpd	/usr/sbin/n
mail	8	mail	mail	/var/mail	/usr/sbin/n
news	9	news	news	/var/spool/news	/usr/sbin/n
uucp	10	uucp	uucp	/var/spool/uucp	/usr/sbin/n
proxy	13	proxy	proxy	/bin	/usr/sbin/n
www-data	33	www-data	www-data	/var/www	/usr/sbin/n
backup	34	backup	backup	/var/backups	/usr/sbin/n
list	38	list	Mailing List Manager	/var/test	/usr/sbin/n
irc	39	irc	irc	/run/ircd	/usr/sbin/n
_apt	42	nogroup	nobody	/nonexistent	/usr/sbin/n
nobody	65534	nogroup	nobody	/nonexistent	/usr/sbin/n
systemd-network	998	systemd-network	systemd Network Management	/	/usr/sbin/n
systemd-timesync	996	systemd-timesync	systemd Time Synchronization	/	/usr/sbin/n
dhcpd	100	nogroup	DHCP Client Daemon	/usr/lib/dhcpd	/bin/false

Page de gestion des utilisateurs et groupes locaux

3. Renseignez les informations requises, telles que le nom d'utilisateur, le mot de passe, et le groupe.

Formulaire des informations à la création d'un utilisateur

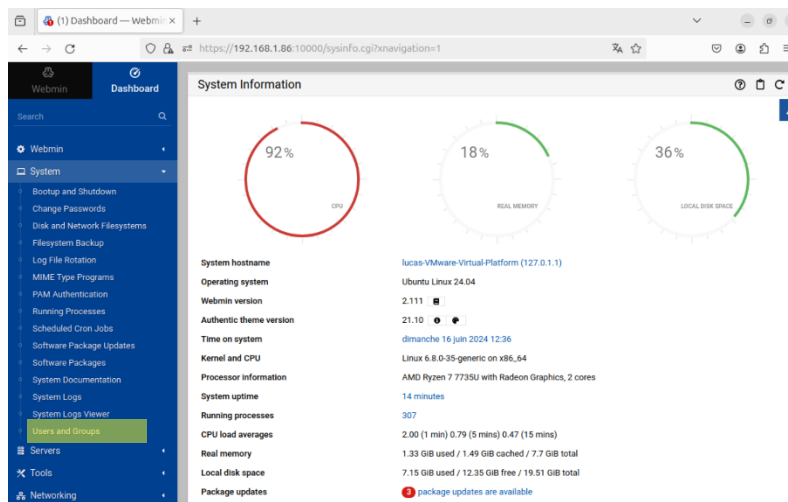
L'ajout d'un utilisateur local permet de définir les utilisateurs qui pourront accéder aux ressources partagées et se connecter au serveur.

3. Ajouter un Groupe Linux Local

- Créer un nouveau groupe local pour organiser les utilisateurs.

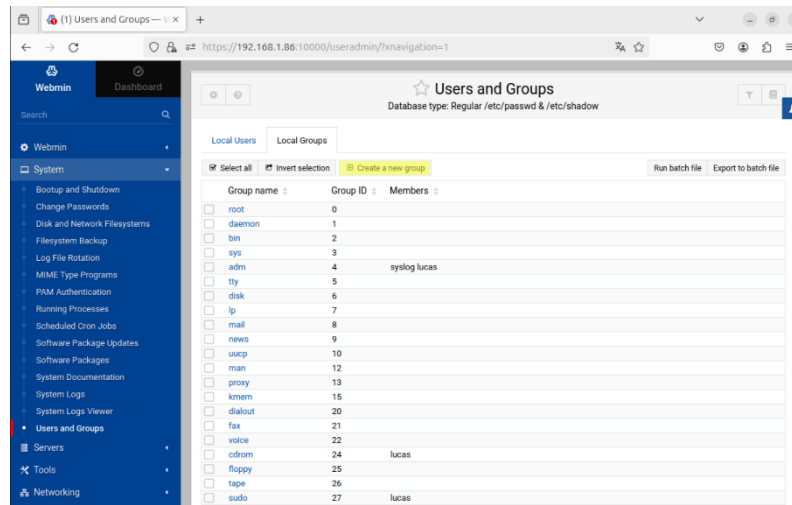
Étapes

1. Dans Webmin, allez dans System > Users and Groups.



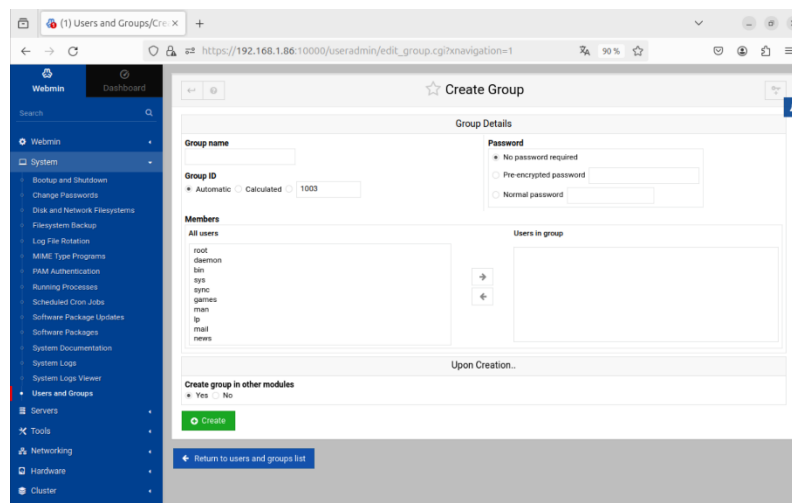
Dashboard du logiciel Webmin

2. Cliquez sur Local Groups > Create a new group.



Page de gestion des utilisateurs et groupes locaux

3. Donnez un nom au groupe et ajoutez des utilisateurs existants au groupe.



Formulaire des informations à la création d'un groupe

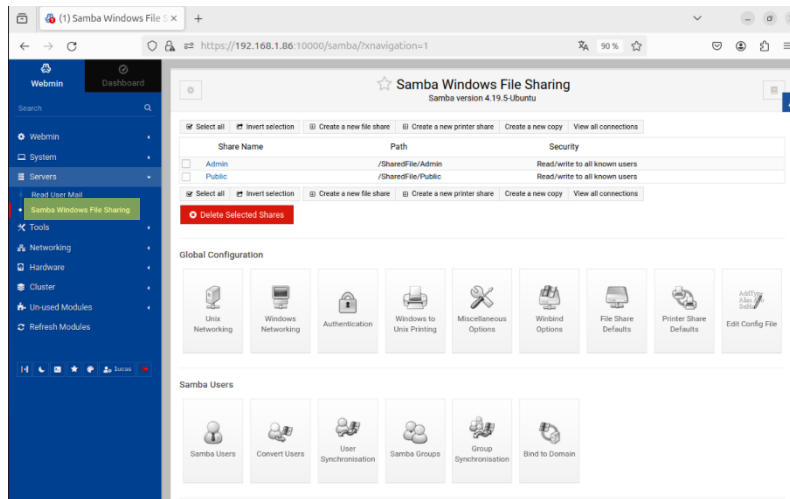
Les groupes permettent de gérer les permissions de manière plus efficace, en appliquant des règles de sécurité à plusieurs utilisateurs en même temps.

4. Convertir les Utilisateurs Linux en Utilisateurs Samba

- Permettre aux utilisateurs Linux de se connecter aux partages Samba.

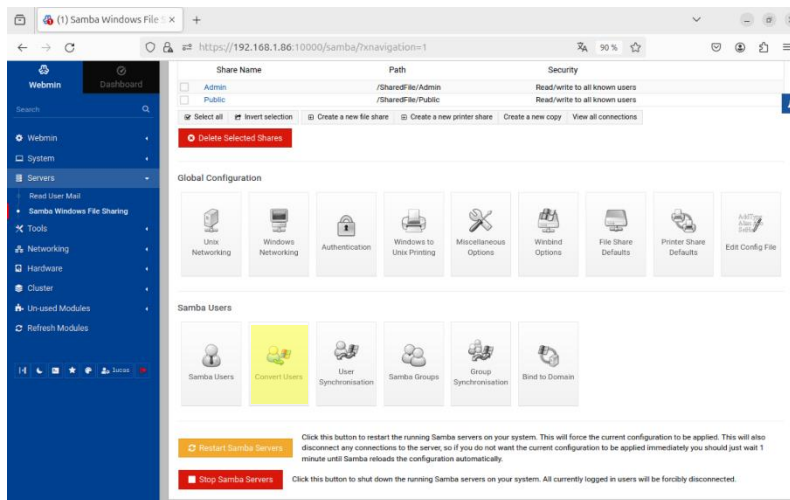
Étapes

1. Dans Webmin, allez dans Servers > Samba Windows File Sharing.



Page de la gestion de Samba via Webmin

2. Cliquez sur Convert Users.



Page de la gestion de Samba via Webmin

- Sélectionnez les utilisateurs via son IUD que vous souhaitez convertir, sélectionnez les paramètres souhaités et cliquez sur Convert.

The screenshot shows the 'Convert Users' page in Webmin. The left sidebar has 'Servers' > 'Samba Windows File Sharing' selected. The main content area has the title 'Convert Users'. Below the title, there is a text block explaining the purpose of the form. Then, there are three main sections: 'Unix users to convert' with radio buttons for 'Only listed users or UID ranges' (selected) and 'All except listed users and UID ranges'; 'Update existing Samba users from their Unix details' with radio buttons for 'Yes' (selected) and 'No'; and 'Delete Samba users who do not exist under Unix' with radio buttons for 'Yes' (selected) and 'No'. There is a 'Convert Users' button and a 'Return to share list' button. On the right, there is a section 'For newly created users, set the password to:' with radio buttons for 'No password' (selected), 'Account locked', and 'Use this password' with an input field.

Formulaire des informations à la conversion d'un utilisateur local à Samba

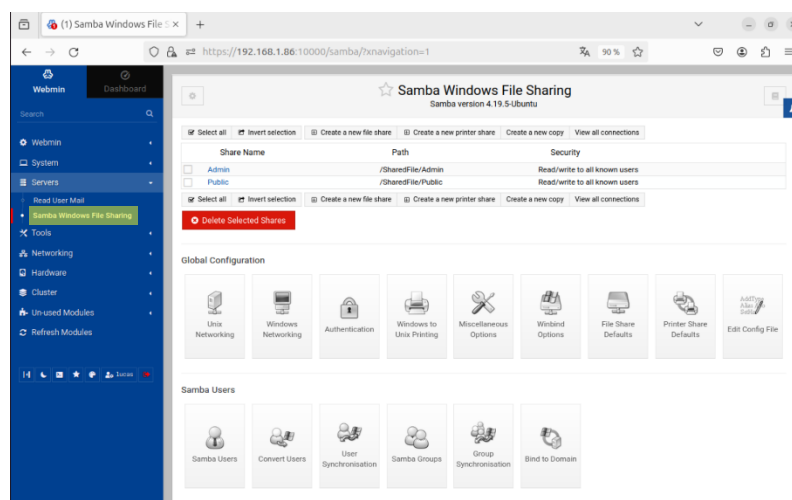
Cette conversion est nécessaire pour que les utilisateurs Linux puissent accéder aux partages Samba avec les mêmes identifiants.

5. Créer un Dossier de Partage et le Paramétrer

- Créer un dossier partagé accessible via Samba avec des permissions spécifiques.

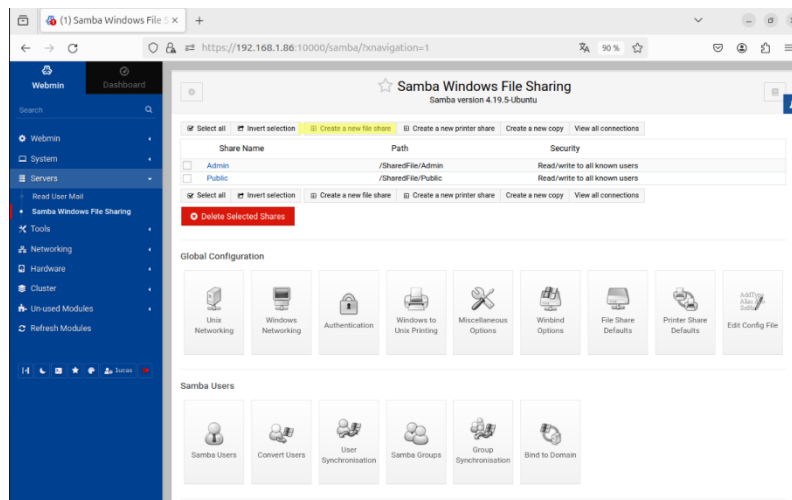
Étapes

- Dans Webmin, allez dans Servers > Samba Windows File Sharing.



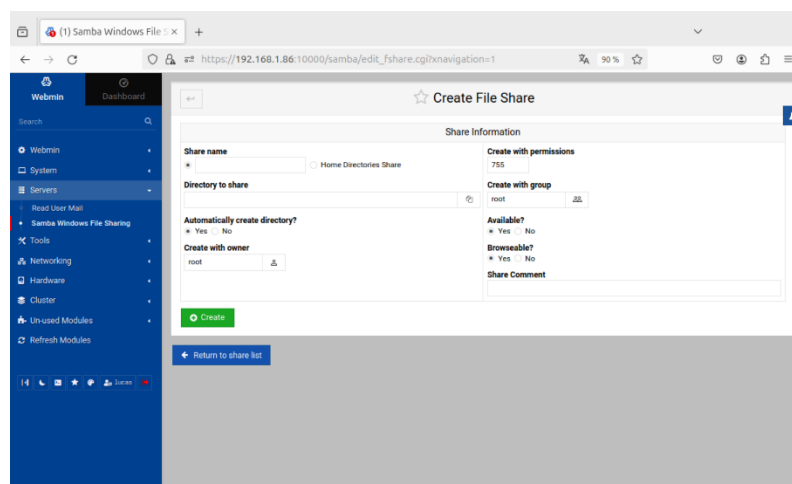
Page de la gestion de Samba via Webmin

2. Cliquez sur Create a new file share.



Page de la gestion de Samba via Webmin

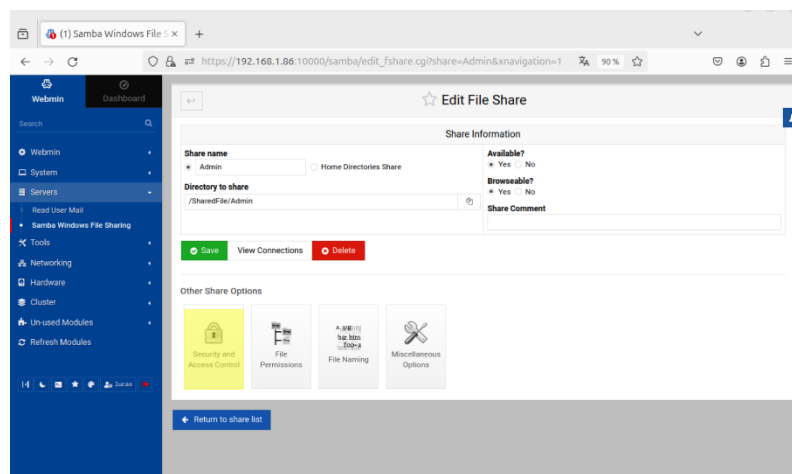
3. Configurer les paramètres de base du partage :



Formulaire des informations à la création d'un fichier de partage

4. Configurer les paramètres avancés du partage :

- Cliquez sur Security et Acces Control.



Page de la gestion d'un dossier de partage

5. Configurez les paramètres du partage :

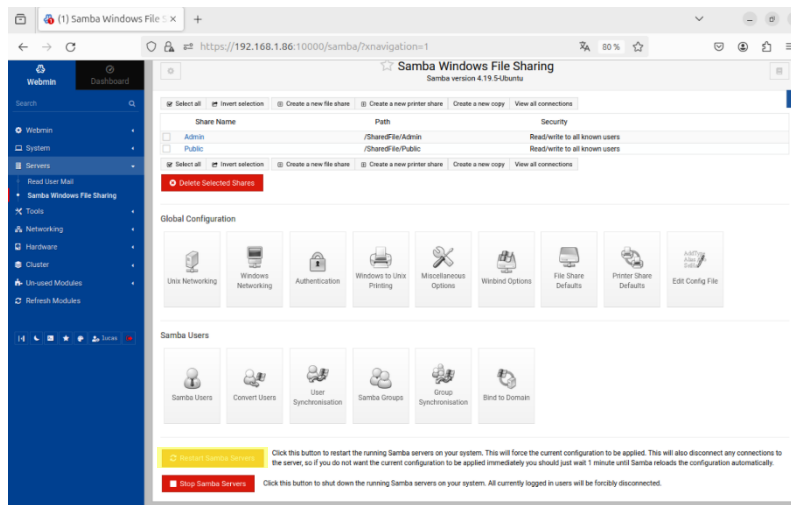
- Share name: Nom du partage.
- Directory to share: Chemin du dossier à partager.
- Writable: Cochez cette option si le partage doit être modifiable.
- Allowed users: Spécifiez les utilisateurs ou groupes (grâce à @ avant le nom du groupe) qui peuvent accéder au partage.
- Valid users: Liste des utilisateurs autorisés.
- Guest access: Permettre ou non l'accès invité.

The screenshot shows the 'Edit Security' interface for a Samba share named 'Admin'. The left sidebar contains a navigation menu with options like Webmin, System, Services, Read/Write Mail, Samba Windows File Sharing, Tools, Networking, Hardware, Cluster, Unused Modules, and Refresh Modules. The main content area is titled 'Edit Security' and 'For share Admin'. It includes sections for 'Security and Access Control' with options for 'Writable?' (Yes/No), 'Guest Access?' (None/Yes/Guest only), 'Guest Unix user' (nobody), 'Limit to possible list?' (Yes/No), 'Hosts to allow' (All/Only allow), and 'Hosts to deny' (None/Only deny). There are also fields for 'Possible users', 'Possible groups', and 'Read only users'. On the right, there are sections for 'Revalidate users?' (Yes/No), 'Valid users' (admin), 'Valid groups' (GPPAdmin), 'Invalid users', 'Invalid groups', 'Read only groups', 'Read/write users', and 'Read/write groups'. A green 'Save' button is at the bottom left, and 'Return to file share' and 'Return to share list' buttons are at the bottom.

Formulaire des paramètres avancé pour le dossier de partage

Créer et paramétrer un partage permet de définir quels utilisateurs et groupes peuvent accéder au dossier, et si ces utilisateurs peuvent modifier les fichiers dans le partage.

6. Redémarrage de Samba :



```
sudo systemctl restart smbd
sudo systemctl restart nmbd
```

Page de la gestion de Samba via Webmin

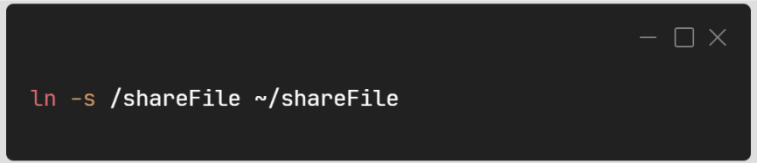
Le redémarrage de Samba est essentiel afin de prendre les derniers ajouts et paramètres en compte. Il peut se réaliser grâce à l'interface de Webmin. Ou directement dans la console avec la commande `systemctl restart`. Elle est utilisée pour redémarrer les services, notamment `smbd` pour la gestion des partages de fichiers et d'imprimantes via Samba, ainsi que `nmbd` pour la résolution des noms NetBIOS sur les réseaux locaux. Ce redémarrage est crucial après toute modification de configuration afin d'appliquer les changements effectués sur le système.

5. Mise en place de fichiers de sauvegardes

Objectif : Mettre en place un script de sauvegarde automatique et le planifier pour qu'il s'exécute à intervalles réguliers. Les sauvegardes doivent être sécurisées et non modifiables pour garantir l'intégrité des données.

1. Créer un lien symbolique pour un accès simplifié au dossier partagé depuis le répertoire personnel de l'administrateur :


- Exécutez la commande suivante pour créer d'un lien symbolique



```
ln -s /shareFile ~/shareFile
```

Pour éviter les conflits entre utilisateurs et gérer les accès de manière centralisée, le dossier partagé est situé à la racine du système. En créant un lien symbolique, on facilite l'accès à ce dossier depuis le répertoire personnel de l'administrateur. La commande suivante crée un lien symbolique nommé shareFile dans le répertoire personnel de l'utilisateur (~/.shareFile), pointant vers le répertoire /shareFile. Cela permet un accès rapide et facile au contenu de /shareFile depuis le répertoire personnel.

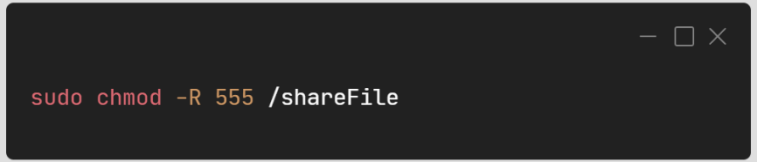
- Changement de Propriétaire



```
sudo chown -R admin:admin /shareFile
```

Cette commande change le propriétaire et le groupe du répertoire /shareFile et de tous ses sous-répertoires et fichiers pour admin. Cela donne à l'utilisateur admin la propriété complète sur ce répertoire.


- Modification des Permissions



```
sudo chmod -R 555 /shareFile
```

Cette commande modifie les permissions du répertoire /shareFile et de tout son contenu pour qu'ils soient en lecture et exécution seulement (r-xr-xr-x). Les fichiers de sauvegarde peuvent être lus et copiés, mais ne peuvent pas être supprimés ou modifiés. Même l'utilisateur administrateur ne peut pas modifier ces fichiers, ce qui protège les données contre les modifications non autorisées. Pour effectuer des modifications, il faudra le faire directement depuis le serveur.

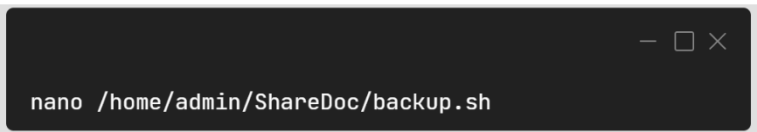
2. Installation de l'Outil tree



```
sudo apt-get install tree -y
```

Cette commande installe l'outil tree, qui affiche les répertoires et fichiers dans une structure arborescente qu'on utilisera pour le fichier de logs des sauvegardes. L'option -y permet de répondre automatiquement "oui" à toutes les invites, simplifiant ainsi l'installation.

3. Création du Script de Sauvegarde



```
nano /home/admin/ShareDoc/backup.sh
```

Cette commande ouvre l'éditeur de texte nano pour créer ou modifier le fichier backup.sh dans le répertoire /home/admin/ShareDoc. Le script de sauvegarde sera écrit et sauvegardé dans ce fichier.

- Intégrer le code permettant la sauvegarde :

```
#!/bin/bash

# Chemin vers le répertoire Public et Admin/Backups
SRC_DIR="/ShareFile/Public"
DEST_DIR="/ShareFile/Admin/Backups"

# Timestamp pour le nom des backups avec les deux derniers chiffres de l'année et des /
TIMESTAMP=$(date +"%d-%m-%y_%H:%M")
BACKUP_DIR="$DEST_DIR/Backup-$TIMESTAMP"
LOG_FILE="$BACKUP_DIR/backup.log"

# Print debug information
echo "Debug: SRC_DIR=$SRC_DIR"
echo "Debug: DEST_DIR=$DEST_DIR"
echo "Debug: TIMESTAMP=$TIMESTAMP"
echo "Debug: BACKUP_DIR=$BACKUP_DIR"
echo "Debug: LOG_FILE=$LOG_FILE"

# Créer le répertoire de destination s'il n'existe pas
mkdir -p "$BACKUP_DIR"
echo "Debug: Created backup directory $BACKUP_DIR"

# Copier récursivement tout le contenu du répertoire source vers le répertoire de destination
rsync -av --delete "$SRC_DIR/" "$BACKUP_DIR/"
echo "Debug: Rsync copy completed"

# Générer le fichier de log
echo "Copie de $SRC_DIR à $BACKUP_DIR réussie, $TIMESTAMP" > "$LOG_FILE"
echo "" >> "$LOG_FILE"

# Ajouter l'arborescence du répertoire Public dans le log
echo "Arborescence du répertoire Public :" >> "$LOG_FILE"
tree "$SRC_DIR" >> "$LOG_FILE"


# Print completion message
echo "Debug: Backup script completed"
```

4. Rendre le Script Exécutable

```
chmod +x /home/Lucas/ShareDoc/backup.sh
```

Cette commande modifie les permissions du script de sauvegarde pour qu'il soit exécutable. Cela permet au script d'être exécuté directement comme une commande.

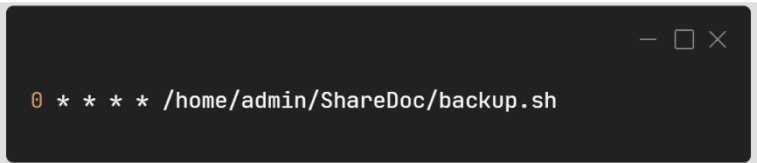
5. Planification du Script de Sauvegarde



```
crontab -e
```

Cette commande ouvre l'éditeur de tâches cron pour l'utilisateur actuel. Vous pouvez ajouter une nouvelle tâche cron pour exécuter le script de sauvegarde à intervalles réguliers.

- Intégrer la tâche cron:



```
* * * * * /home/admin/ShareDoc/backup.sh
```

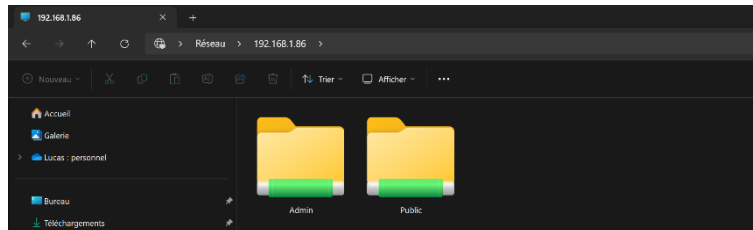
Cette ligne ajoute une tâche cron qui exécute le script de sauvegarde (/home/admin/ShareDoc/backup.sh) toutes les heures. Le format de la tâche cron est minute heure jour_mois mois jour_semaine commande.

Utilisation et Démonstration

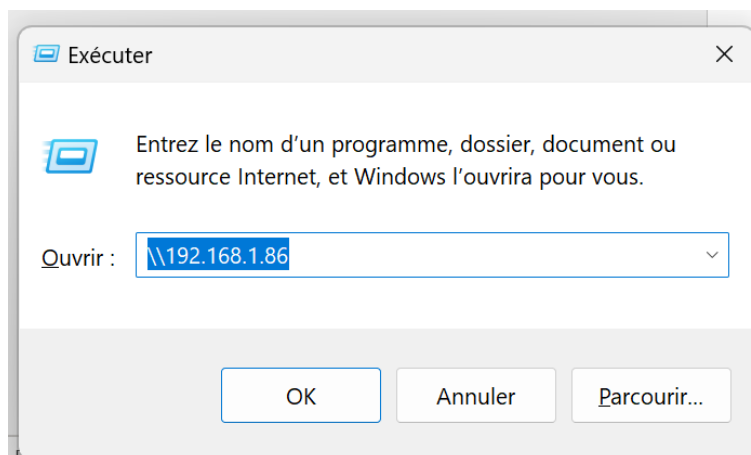
- **Accès au Dossier Partagé depuis un Client Windows**

1. Ouvrir l'Explorateur de Fichiers :

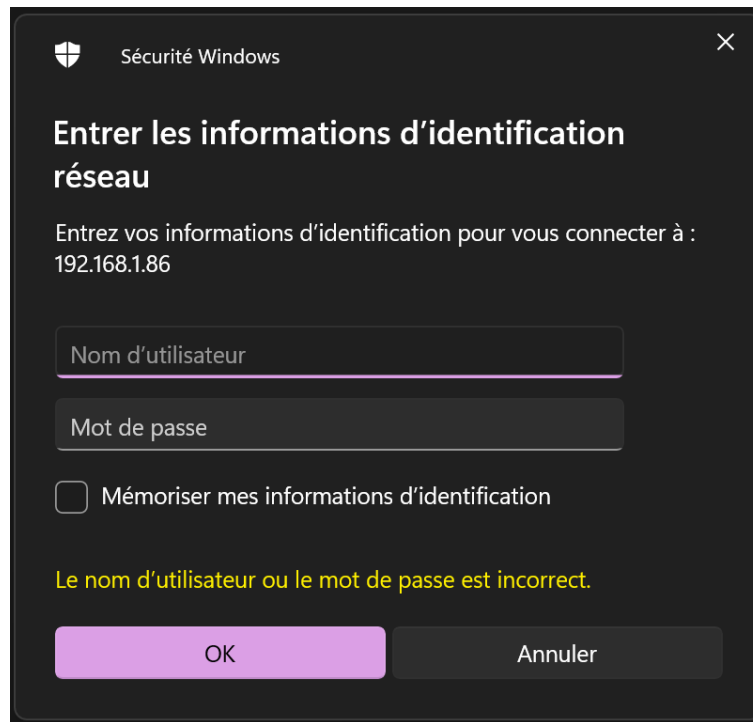
- Cliquez sur l'icône de l'Explorateur de fichiers dans la barre des tâches utilisez le raccourci clavier Win + E.
- Accéder au Dossier Partagé : Dans la barre d'adresse de l'Explorateur de fichiers, tapez \\<IP_du_Serveur_Linux> et appuyez sur Entrée.



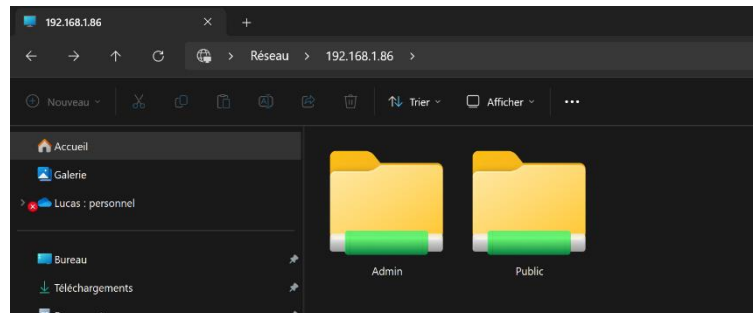
- Utilisez le raccourci clavier Win + E et tapez \\<IP_du_Serveur_Linux> et appuyez sur Entrée ou OK.



- Une fenêtre de connexion s'ouvrira, entrer les informations demandées



- Vous avez accès aux fichiers selon votre status



- **Supprimer les informations d'identification enregistrées**

Ouvrir le Gestionnaire des identifiants :

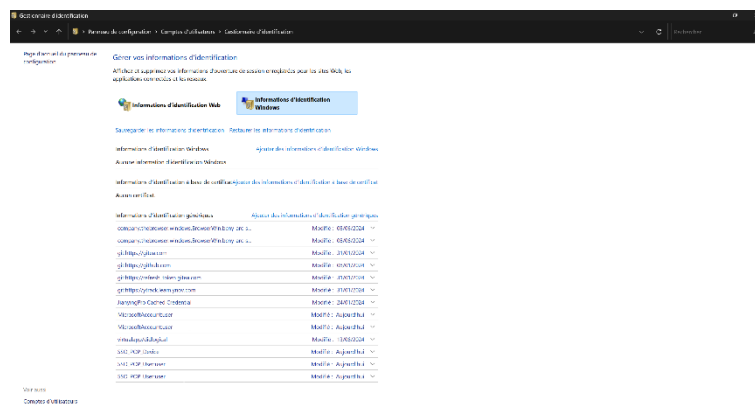
- Cliquez sur le menu Démarrer et tapez "Gestionnaire des identifiants".
- Sélectionnez "Gestionnaire des identifiants".

Supprimer les informations d'identification enregistrées :

- Dans le Gestionnaire des identifiants, cliquez sur "Identifiants Windows".
- Recherchez l'entrée correspondant à l'adresse IP ou au nom du serveur Linux (par exemple, \\192.168.1.86).
- Cliquez sur la flèche à droite de l'entrée pour l'agrandir.
- Cliquez sur "Supprimer".

Confirmer la suppression :

- Confirmez que vous souhaitez supprimer les informations d'identification.



Ou via l'invite de commande :

- Cliquez sur le menu Démarrer, tapez "cmd", faites un clic droit sur "Invite de commandes" et sélectionnez "Exécuter en tant qu'administrateur".

Supprimer les informations d'identification :

- Dans l'invite de commande, tapez la commande suivante et appuyez sur Entrée :

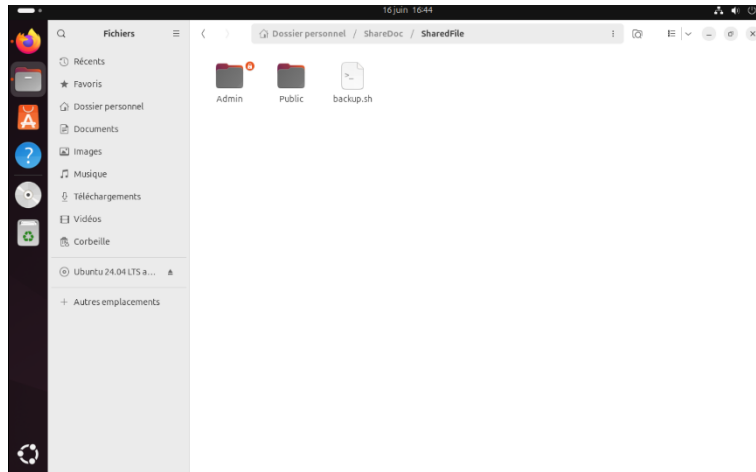


Cette commande supprimera toutes les connexions réseau actives et les informations d'identification enregistrées.

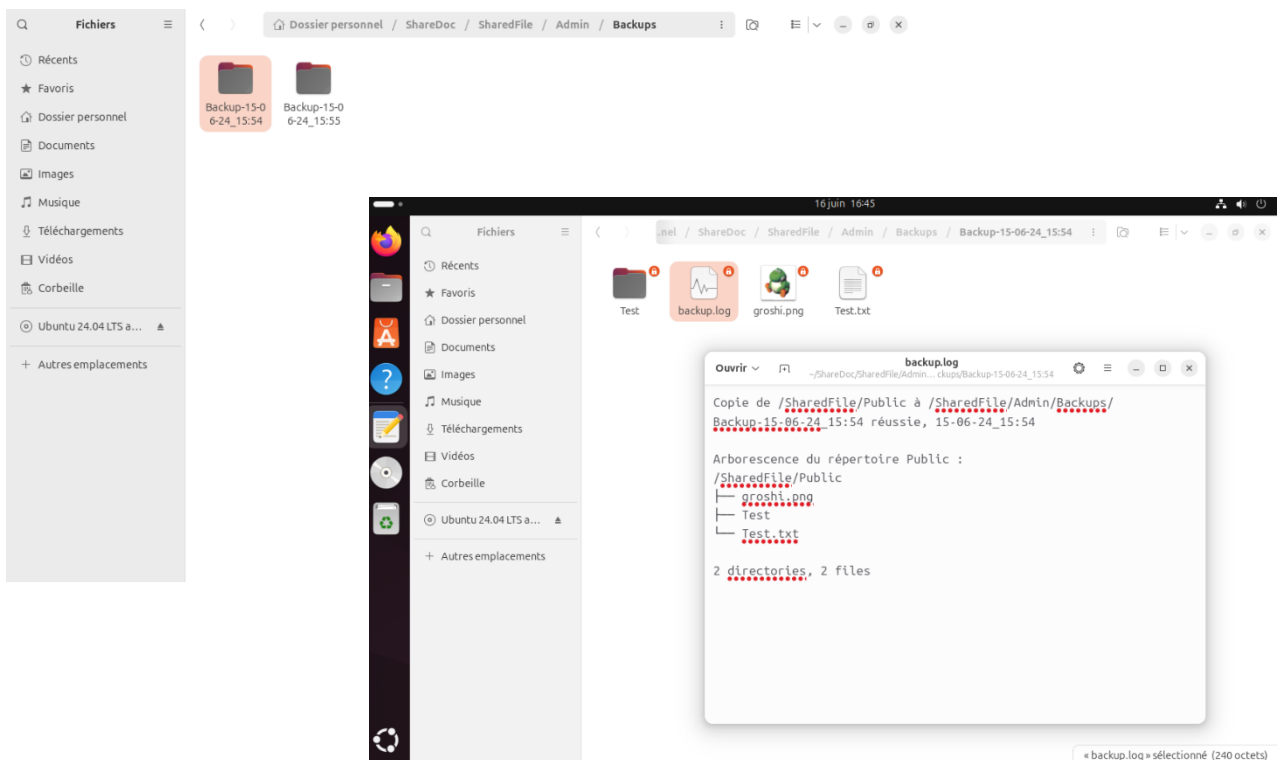
- **Accès au Dossier Partagé depuis le serveur Linux (Ubuntu)**

1. Ouvrir l'Explorateur de Fichiers :

- Se rendre dans le chemin d'accès des fichiers de partage



- Vous accédez aux dossiers d'administrateur si vous avez les droits



Remarque :

Vous avez les mêmes accès si vous êtes connecté en tant qu'admin du côté client de Windows.