



# TP-Backup

---

THOMAS GRZESINSKI

# Procédure / Politique de sauvegarde ?

---

**Qu'est-ce qu'une procédure de sauvegarde ?** Une procédure de sauvegarde aussi appelé plan de sauvegarde est un ensemble de stratégies et de procédures définies pour protéger et préserver les données numériques d'une organisation ou d'un individu en les copiant sur un support physique ou en ligne

**Pourquoi instaurer une politique de sauvegarde ?** Car en cas d'attaque sur le système informatique, la mise en place d'une PRA (Plan de reprise d'activité) vise à assurer la continuité de l'entreprise en cas de sinistre majeur affectant le système informatique. Ce problème peut-être d'origine naturelle (feu, inondation) ou d'origine humaine (on supprime un dossier que l'on ne devait pas, on débranche une chose qu'il ne fallait pas)

# Les stratégies de sauvegardes

---

Les trois méthodes principales de sauvegarde sont :

**Sauvegarde totale (complète)** : Cette méthode consiste à sauvegarder l'intégralité des fichiers à un moment donné (T). Lors de la restauration des données, on prend la sauvegarde la plus récente et tous les fichiers sont restaurés à leur état au jour de la sauvegarde (J). C'est une approche simple mais coûteuse en temps et en espace de stockage.

**Sauvegarde différentielle** : Après une première sauvegarde complète le jour J, les sauvegardes différentielles effectuées les jours suivants ne contiennent que les fichiers modifiés depuis cette sauvegarde complète. Cette approche nécessite moins d'efforts et de temps par rapport à la sauvegarde complète.

**Sauvegarde incrémentielle** : Après une sauvegarde complète initiale, chaque sauvegarde suivante ne contient que les fichiers modifiés depuis la sauvegarde précédente, qu'il s'agisse de la sauvegarde complète ou d'une autre incrémentielle. C'est la méthode la plus économe en temps et en espace, mais elle rend la restauration plus complexe, car plusieurs étapes sont nécessaires pour retrouver l'état d'origine.

# Sauvegarde en ligne ? Comment ?

---

Une sauvegarde en ligne, ou "Stockage Cloud", permet de stocker des données à distance, accessibles via internet. Ce modèle permet aux utilisateurs de consulter leurs fichiers et applications depuis n'importe quel appareil, grâce au stockage sur des serveurs distants dans des datacenters.

Il existe trois types de cloud :

- **Cloud public**: Proposé par des fournisseurs tiers (comme Google Cloud), il offre des ressources de calcul, de stockage et d'applications via internet.
- **Cloud privé**: Utilisé par une seule organisation, il offre plus de sécurité et de contrôle, mais avec des coûts élevés.
- **Cloud hybride** : Combine cloud privé et public, permettant de tirer parti des avantages des deux selon les besoins.

# Pour qui ?

---

Les sauvegardes cloud peuvent être utilisées par tous types d'entreprises (industrielles, hôpitaux, etc.), à condition que les données soient hébergées en Europe, afin de respecter les normes du RGPD. Ce règlement protège les données sensibles, empêchant leur modification ou vente sans autorisation. Par exemple, les hôpitaux doivent stocker leurs données en Europe, bien que la CNIL ait signé un contrat avec Microsoft pour un hébergement sur des serveurs américains. Il est donc recommandé de privilégier des prestataires européens comme OVH ou des acteurs locaux comme le Groupe ASTEN, particulièrement actif en Bretagne, Pays de la Loire, et Normandie.

Source article de la CNLI qui signe avec Microsoft :

[Le Monde informatique](#)

La Cnil a autorisé la création d'un entrepôt de données de santé baptisé EMC2 basé sur le traitement automatisé de données personnelles. Il sera hébergé sur le cloud de Microsoft pour une durée de trois ans. Le régulateur pointe néanmoins les risques d'application de lois américaines à portée extra-territoriale et regrette l'absence de prestataires européens.

# Questions à prendre en compte/Informatique externalisée: qui est responsable de la sauvegarde ?

---

Questions à prendre en compte :

Avant de signer un contrat d'hébergement il faut se poser les questions:

- - Est-ce que mes données sont protégés ?
- - Est-ce que mes applications actuelles sont éligibles au cloud ?
- - Quel prestataire cloud choisir ? Et ou mes données seront-elles stockées ?

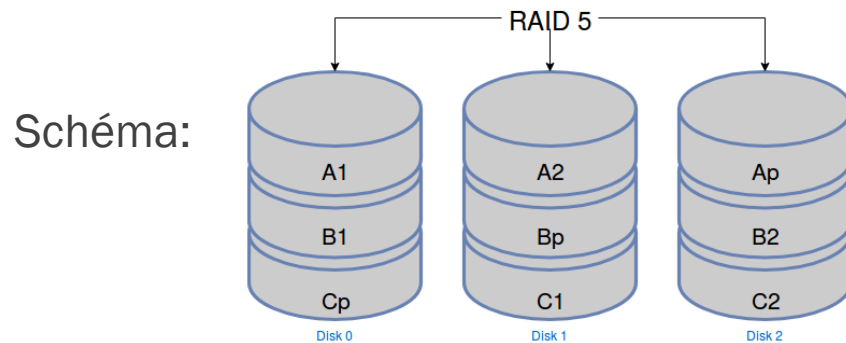
Informatique externalisée: qui est responsable de la sauvegarde ?

- Le responsable des sauvegardes externalisés est donc le prestataire du service. En effet celui-ci doit s'assurer que l'entreprise puisse toujours accéder à ses données quand elle le veut . Il doit donc assurer l'intégrité des données. Et de les protéger

# Sauvegarde de serveurs: Comment et pourquoi ?

---

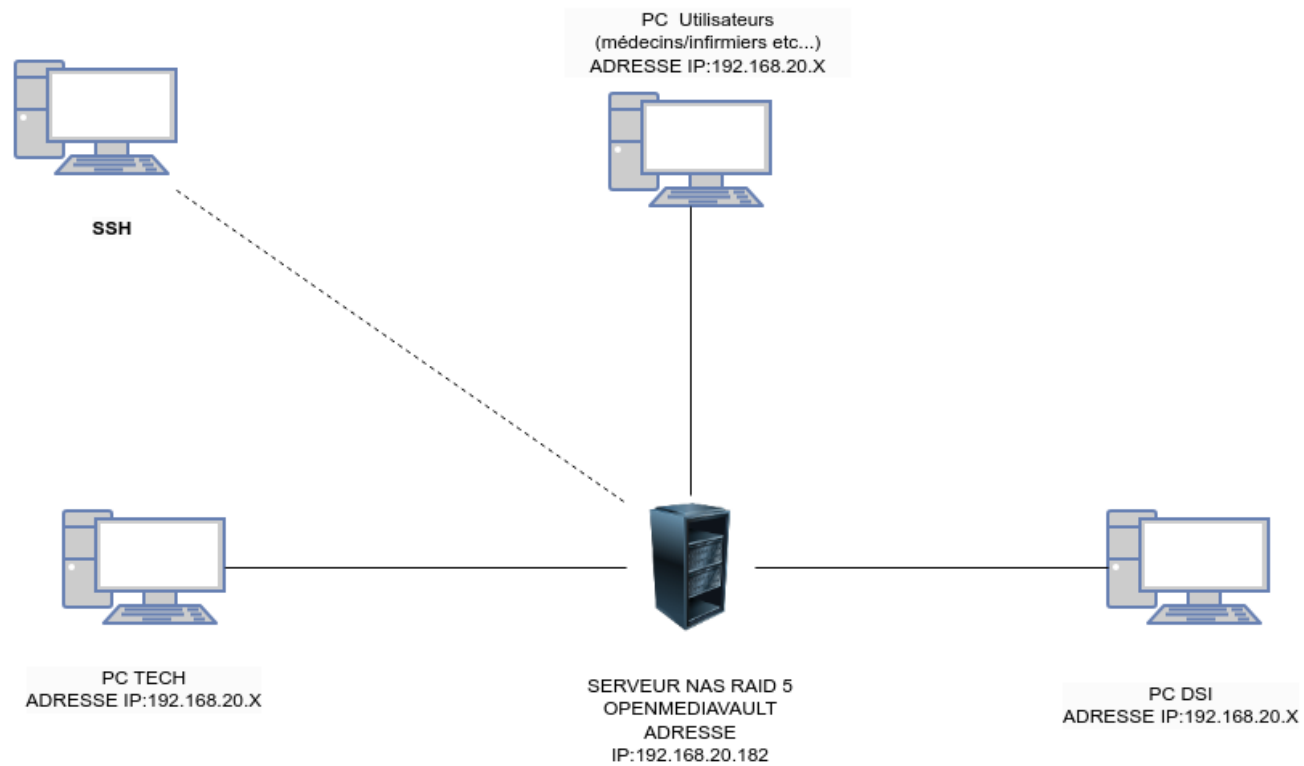
Il existe une stratégie de sauvegarde qui est 3-2-1, elle consiste à créer au moins trois copies de vos données, deux sauvegardes stockées sur des copies de supports différentes et une sauvegarde hors site ou dans le cloud. C'est l'une des meilleures pratiques à l'heure actuelle



Le but de sauvegarder les serveurs est un processus qui garantit la préservation des données et la protection contre la perte d'informations en cas de défaillance du système. Si on ne fait pas ceci de façon régulière, on risque de perdre des fichiers et de perturber l'ensemble du système

# Schéma de l'infrastructure

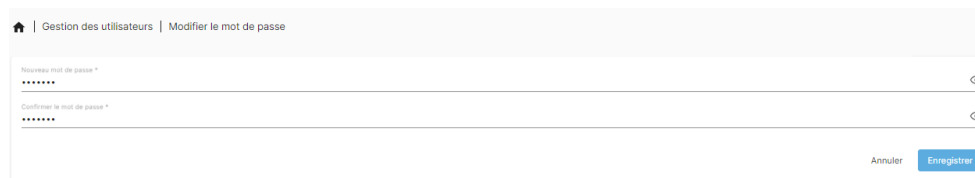
---



# Installation et configuration de OMV

---

- Avoir un iso de préférence OMV version 6.5
- Ajouter trois disques dur SATA a notre VM (2 GO par disque sera nécaissre) pour un RAID 5
- Installer et configurer votre machine
- Ouvrez un navigateur WEB et entrer l'adresse IP de votre machine OMV dans l'url
- le mot de passe par défaut est login: admin mot de passe: openmediavault
- Penser à modifier ce mot de passe dans « Préférences utilisateurs -> modifier mot de passe »



The screenshot shows the 'Gestion des utilisateurs | Modifier le mot de passe' page in the OpenMediaVault web interface. It features two password input fields: 'Nouveau mot de passe \*' and 'Confirmer le mot de passe \*', both with masked characters (dots) and toggle icons. At the bottom right, there are two buttons: 'Annuler' (grey) and 'Enregistrer' (blue).

# Configuration du RAID

Pour notre contexte j'ai préféré utiliser un RAID 5 qui permet d'avoir une configuration plus rapide que un RAID 1, en effet les données sont écrites de la même manière qu'un RAID 0 dans un bloc de données. Le bloc de parité sera ajouté par le contrôle RAID. Le bloc de parité agit comme un système de redondance RAID pour protéger les données sur le disque. Donc si un des disques est défaillant, les données peuvent être reconstituées sur un disque de remplacement grâce au bloc de parité. Voir [TP-Sauvegarde NAS](#)

## Configuration RAID 5 :

- - Aller dans « Stockage -> Disques » Tout vos disques ajoutés à la VM sont censé apparaître
- - Il faut aller ensuite dans « RAID logiciel » et crée un RAID 5
- et sélectionner tous nos disques SATA

Périphérique	Modèle	N° de série	Type	Capacité
sda	QEMU-HARDDISK	04800015	ATA	2,00 GiB
sdb	QEMU-HARDDISK	04800017	ATA	2,00 GiB
sdc	QEMU-HARDDISK	04800019	ATA	2,00 GiB
sdd	QEMU-HARDDISK	04800016	QEMU	10,00 GiB
sddv	QEMU-DVD-ROM	04800013	QEMU	888,80 Mo

Niveau  
RAID 5

Périphériques \*  
QEMU HARDDISK [/dev/sda, 2.00 GiB], QEMU HARDDISK [/dev/sdb, 2.00 GiB], QEMU HARDDISK [/dev/sdc, 2.00 GiB]

Sélectionner les périphériques qui seront utilisés pour créer la grappe RAID. Les périphériques USB ne sont pas affichés (pas assez fiable)

# Configuration du RAID

- Votre RAID 5 est bien mis en place

Périphérique :	État :	Niveau :	Capacité :	Périphériques
/dev/md0	clean	RAID 5	3.99 GiB	<ul style="list-style-type: none"><li>/dev/sda</li><li>/dev/sdb</li><li>/dev/sdc</li></ul>

0 sélectionné / 1 total

- On va maintenant monter un système de fichier qui nous permettra de stocker les informations et de les organiser. Il faut donc aller dans « Systèmes de fichiers » et en créer un avec un format de disque dur EXT 4 et il faudra ensuite monter ce système que l'on a créé

Système de fichiers \*

/dev/md0 [EXT4, 3.99 GiB]

Le système de fichier à monter

Seuil d'avertissement d'utilisation \*

80%

Envoyer une notification quand la capacité du système de fichier utilisé dépasse le seuil spécifié.

Étiquettes

/dev/md0 [EXT4] 3.84 GiB 40.00 KiB ✓ Online

- On va maintenant créer des dossiers partagés que l'on nommera

selon nos besoins

Nom *	Périphérique :	Chemin relatif :	Chemin absolu :	Référence :	Étiquettes :
Patients_semaine_37	/dev/md0	Patients_semaine_37/	/srv/ovs-disk-by-uuid-b75006a-992b-447f-af03-a80748139a09/Patients_semaine_37		
Patients_semaine_38	/dev/md0	Patients_semaine_38/	/srv/ovs-disk-by-uuid-b75006a-992b-447f-af03-a80748139a09/Patients_semaine_38		
RIH	/dev/md0	RIH/	/srv/ovs-disk-by-uuid-b75006a-992b-447f-af03-a80748139a09/RIH		
Sauvegardehopitale	/dev/md0	Sauvegardehopitale/	/srv/ovs-disk-by-uuid-b75006a-992b-447f-af03-a80748139a09/Sauvegardehopitale	✓	

0 sélectionné / 4 total

Nom \*

Sauvegardehopitale

Système de fichiers \*

/dev/md0 [EXT4, 40.00 KiB (1%) used, 3.83 GiB available]

Le système de fichier sur lequel le dossier partagé sera créé.

Chemin relatif \*

Sauvegardehopitale/

Chemin relatif du répertoire à partager. Le répertoire indiqué n'existe pas.

Permissions \*

Administrateur: lect./écriv., Utilisateur: lect./écriv., Autres: lect. seule

Le mode de fichier du chemin de dossier partagé.

Étiquettes

# Configuration RAID (SMB)

- Une fois ceci fait on va donc activer le protocole SMB(Samba) sur notre OVM afin que les utilisateurs puissent accéder à nos dossiers partager

**Activé**

Groupe de travail \*  
**WORKGROUP**

---

Le groupe de travail du serveur qui apparait lors d'interrogation par les clients.

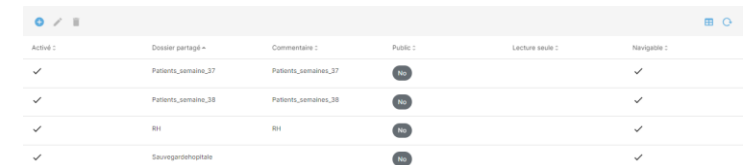
Description \*  
**%h server**

---

Le champ de description NT.

**Serveur de temps**  
Autoriser ce serveur à s'annoncer comme un serveur de temps pour les clients Windows

- On crée ensuite les dossiers que l'on souhaite partagé avec le SMB



Activé :	Dossier partagé :	Commentaire :	Public :	Lecture seule :	Navigable :
✓	Patients_semaine_37	Patients_semaine_37	No		✓
✓	Patients_semaine_38	Patients_semaine_38	No		✓
✓	RH	RH	No		✓
✓	Sauvegardeshopitale		No		✓

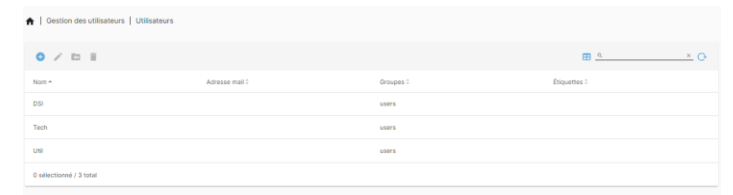
# Configuration RAID(Utilisateurs)

---

- Le soucis maintenant c'est que nos dossiers sont partagés mais on ne peut pas y accéder su la machine cliente comme on le souhaite car il faut s'identifier



- Il faut donc configurer des utilisateurs avec des droits dans « User Managment »



Nom	Adresse mail	Groupes	Etiquettes
DS		users	
Tech		users	
US		users	

0 sélectionné / 3 total

# Configuration RAID (Utilisateurs)

- Pour les droits j'ai décidé d'opérer pour ce genre de choix:
- Pour la tech je lui ai accordé tous les droits comme c'est une configuration, il n'y a encore aucune donnée personnelles et sensibles qui circulent donc il a le droit a tous les accès

Dossier partagé *	Permissions :		
Patients_semaine_37	Read/Write	Read-only	No access
Patients_semaine_38	Read/Write	Read-only	No access
RH	Read/Write	Read-only	No access
Sauvegardehopitale	Read/Write	Read-only	No access

- Pour l'utilisateur je me suis dit que c'était un infirmier ou médecin donc je lui ai attribué tous les droits sur les semaines des patients

Utilisateur	Read/Write	Read-only	No access
Patients_semaine_37	Read/Write	Read-only	No access
Patients_semaine_38	Read/Write	Read-only	No access
RH	Read/Write	Read-only	No access
Sauvegardehopitale	Read/Write	Read-only	No access

- Le DSI n'a donc aucun droit attribué sur les dossiers

Dossier partagé *	Permissions :		
Patients_semaine_37	Read/Write	Read-only	No access
Patients_semaine_38	Read/Write	Read-only	No access
RH	Read/Write	Read-only	No access
Sauvegardehopitale	Read/Write	Read-only	No access

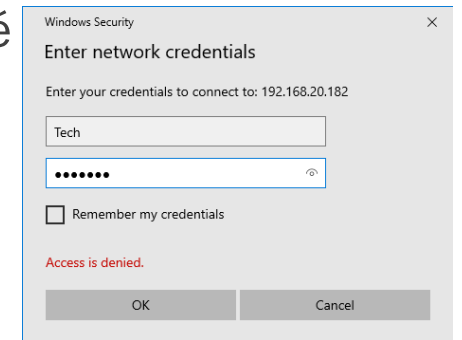
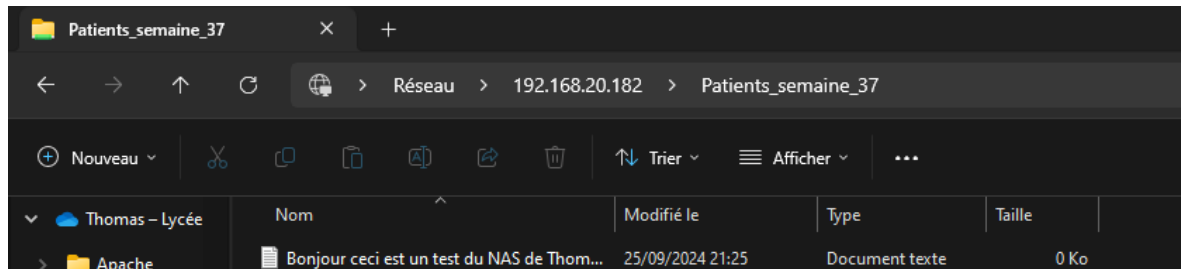
# Configuration RAID (Utilisateurs)

---

- J'ai décidé de vérifier si mes partages fonctionnent correctement avec l'utilisateur Tech pour que ce soit plus simple à vérifier.

La machine vous demandera d'entrer vos identifiants pour des raisons de sécurité

- Test des droits en créant un fichier dans un dossier partagé:



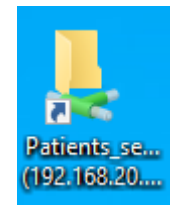
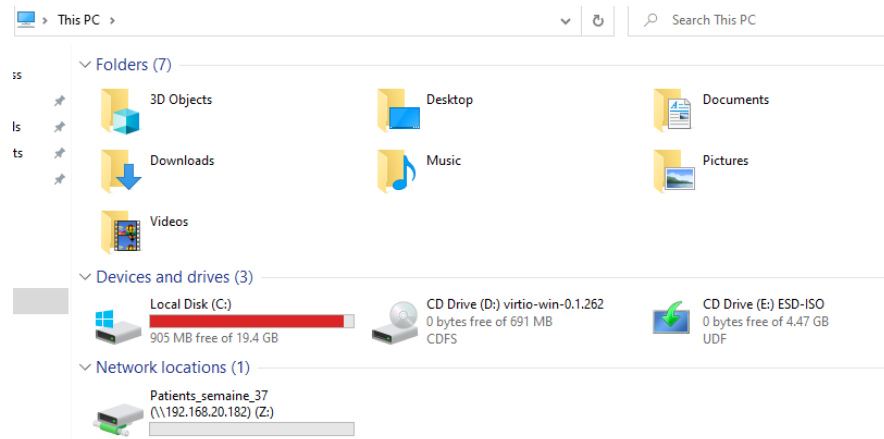
-( Il peut y avoir des erreurs sur Windows sur une VM Windows j'ai un accès refusé tandis que sur ma machine physique j'ai aucun problème)

Source: [Vidéo ShupSi](#)

# Rapidité

---

- Pour que nos utilisateurs puissent sauvegarder rapidement dans leur dossier sans à chaque fois se connecter au réseau du NAS, il suffit de créer un raccourci en faisant un clic droit sur le dossier



# Test de votre NAS

Pour que vos clients puissent enregistrer directement sur le NAS il suffit de créer un raccourci du dossier voulu et vérifier avec une tache simplifié

The image shows a Windows 'Map Network Drive' dialog box on the left and a 'This PC' window on the right. The dialog box is titled 'Map Network Drive' and asks 'What network folder would you like to map?'. It specifies the drive letter 'Z:' and the folder path '\\192.168.20.182\Patients\_semaine\_37'. There are 'Finish' and 'Cancel' buttons at the bottom. The 'This PC' window shows a file explorer view with 'Folders (7)', 'Devices and drives (3)', and 'Network locations (1)'. The 'Network locations' section shows 'Patients\_semaine\_37 (\\192.168.20.182) (Z:)'.

```
Please wait... Syncing </srv/dev-disk-by-uuid-57588aa-92d3-467f-bf03-eab0748139a8/Patients_semaine_37/> to </srv/dev-disk-by-uuid-57588aa-92d3-467f-bf03-eab0748139a8/Sauvegardemepitale/>...
Sending incremental file list
...
Aujourd'hui ceci est un test de NAS de Thomas Grzesinski.txt
...
sent 178 bytes received 38 bytes 432.00 bytes/sec
total size is 0 speedup is 0.00
The synchronization has completed successfully.
...
END OF LINE
```

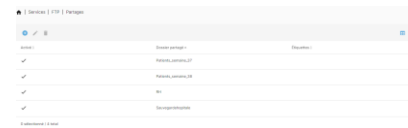
# Mise en place du FTP

---

Maintenant on va mettre en place une solution FTP qui permettrait à nos utilisateurs de pouvoir enregistrer des fichiers à distance sur le serveur NAS

Configuration:

- - Installer l'extension openmediavault FTP-server plugin
- - Vous aurez ensuite le Services FTP qui apparait
- - Activer le serveur FTP
- Partager vos dossiers partagés avec le FTP
- Redémarrer votre machine OMV(pour des raisons de bugs avec le service FTP)



openmediavault-ftp 6.0.7-1  
openmediavault FTP-Server plugin

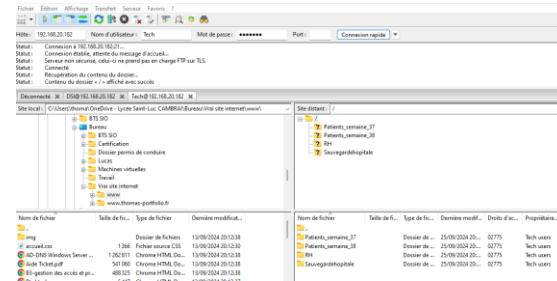
**Installé**

ProFTPD is a powerful modular FTP/SFTP/FTPS server.

Section: Sharing  
Mainteneur: Volker Theile <volker.theile@openmediavault.org>  
Page d'accueil: <http://www.openmediavault.org>  
Dépôt: openmediavault.org archive/shaitan  
Taille: 65.67 KiB

# Mise en place FTP/Automatisation des sauvegardes du NAS

- Tester la fonctionnalité du FTP avec Filezilla par exemple en y entrant l'@IP de OMV et les identifiants d'un utilisateur



- On va maintenant créer un fichier via FTP dans un dossier (ce fichier sera aussi visible sur le réseau partagé) et on va faire en sorte que nos fichiers soient sauvegardés sur le NAS a un instant t précis

- On créer donc notre fichier pas\_sur\_le\_NAS dans notre dossier patients semaine 37

# Automatisation des sauvegardes du NAS

- Une fois le fichier créer on retourne sur notre OMV et on va dans l'onglet Services -> Rsync (remote synchronization, logiciel libre de synchronisation de fichiers), j'ai une préférence d'utiliser Rsync pour l'avoir déjà pu utiliser durant mon TP-Sauvegarde NAS de première année

Donc dans Rsyn, on créer une tâche dans laquelle on définit la source de la sauvegarde et vers qu'elle destination cette source doit arriver.

On a aussi un vaste choix pour choisir a quel instant t on souhaite le sauvegarder (minutes, heures, jours, mois) . J'ai donc moi choisis de sauvegarder les fichiers du dossier Patients\_semaine\_37 tout les dimanches à 20h30 vers la source de sauvegarde principale de notre hôpital qui est le dossier Sauvegarde hopital

Activé

Type  
Local

Source shared folder  
Patients\_semaine\_37 (on /dev/md0, Patients\_semaine\_37)

Destination shared folder  
Sauvegardehopital (on /dev/md0, Sauvegardehopital)

Date d'exécution  
À 20:30, uniquement le dimanche

Minutes \*  
30  Toutes les N minutes

Heures \*  
20  Toutes les N heures

Jour de mois \*  
+  Tous les N jours du mois

Mois \*  
+

Jour de semaine \*  
Dimanche

# Automatisation des sauvegardes du NAS

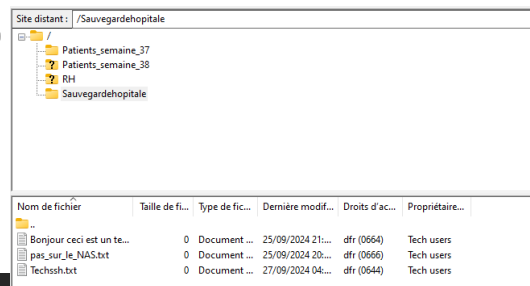
- On va alors ensuite exécuter notre tâche pour des raisons de rapidité et de test et on peut l'observer que notre fichier se sauvegarde correctement dans la sauvegarder de destination

Lancer la tâche rsync

```
Please wait, syncing /srv/dev-disk-by-uuid-675086aa-9826-467f-af43-eab0748139a9/Patients_semaine_37/: to /srv/dev-disk-by-uuid-675086aa-9826-467f-af43-eab0748139a9/Sauvegardehopitale/...
sending incremental file list
./
pas_sur_le_NAS.txt

sent 188 bytes received 38 bytes 352.00 bytes/sec
total size is 9 speedup is 0.69
The synchronisation has completed successfully.
END OF LINE
```

- Si on vient donc à perdre notre fichier dans notre dossier Patients\_SEMAINE\_37, celui-ci se retrouvera donc dans notre dossier Sauvegardehopitale (test effectué en supprimant le fichier de son dossier)



# Accès par SSH

- On voudrait maintenant avoir un accès SSH a nos dossiers distants pour que nos utilisateurs puissent sauvegarder des fichiers à distance.

Configuration:

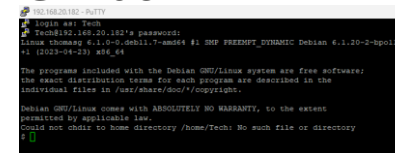
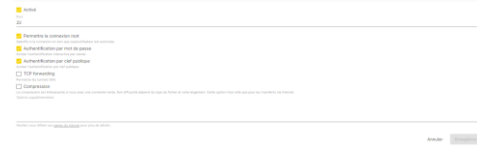
- Il faut tout d'abord sur l'un de nos utilisateurs l'ajouter au groupe SSH(Tech)

- Et activer le protocole SSH

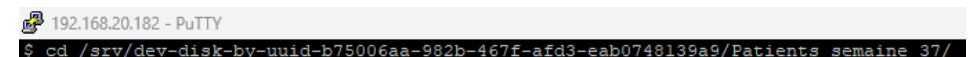
- Ensuite on test notre connectivité avec Putty en y mettant l'@IP de

la VM OMV, et les logs de notre utilisateur (Tech pour nous)

- Ensuite il faut donc se rendre dans le chemin du dossier partagé qui fait référence au chemin absolu dans nos dossier partagés



```
/srv/dev-disk-by-uuid-b75006aa-982b-467f-afd3-eab0748139a9/Patients_semaine_37
```



# Accès par SSH/Crontab

---

- On va ensuite créer un fichier qui nous permettra pour la sauvegardé avec une tâche planifiée

*crontab*

```
$ touch Techssh.txt
$ ls -a
.  ..  'Bonjour ceci est un test du NAS de Thomas Grzesinski.txt'  Techssh.txt
```

- Crontab (cron) est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée à l'avance, ou selon un cycle défini à l'avance

Configuration:

- Sur notre machine OMV ou par SSH en tant que root on va donc créer un fichier sauvegarde\_techssh.sh(ce fichier permet pour l'exécution de notre script)

# Crontab tâche planifié

- Dans ce fichier on va faire en sorte que tous nos fichiers provenant de notre dossier vont se sauvegarder vers notre autre dossier principal de sauvegarde (Sauvegardehopitale)

```
192.168.20.182 - PuTTY
GNU nano 5.4
/root/sauvegarde_techssh.sh *
cp /srv/dev-disk-by-uuid-b75006aa-982b-467f-afd3-eab0748139a9/Patients_semaine_37/Techssh.txt /srv/dev-disk-by-uuid-b75006aa-982b-467f-afd3-eab0748139a9/Sauvegardehopitale
```

- Une fois ceci fait il faut donc rendre script executable

- On va donc ensuite planifié une tâche crontab avec la commande `crontab -e`

```
192.168.20.182 - PuTTY
root@thomasg:~# chmod +x /root/sauvegarde_techssh.sh
```

Dans ce fichier j'ai donc défini que tous les jours  
A 4h du matin mes fichiers présents dans mon  
Dossier Patients\_semaine\_37 soit sauvegardé  
Vers mon dossier Sauvegardehopital

```
192.168.20.182 - PuTTY
GNU nano 5.4
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow  command
0 4 * * * /root/sauvegarde_techssh.sh
```

