

INFRA RÉSEAUX



l'école d'ingénierie
informatique



l'école [tech]
de l'expertise digitale

Participants :

Thibault ROYER
Annalia PRIEUR
Tom CLEMENT
Noa RODRIGUES

Préparation et présentation d'une infra réseaux - Première Année, 2025

EPSI — Ecole de l'ingénierie
informatique, Arras

Projet encadré par :

Briki Rachid

Contexte

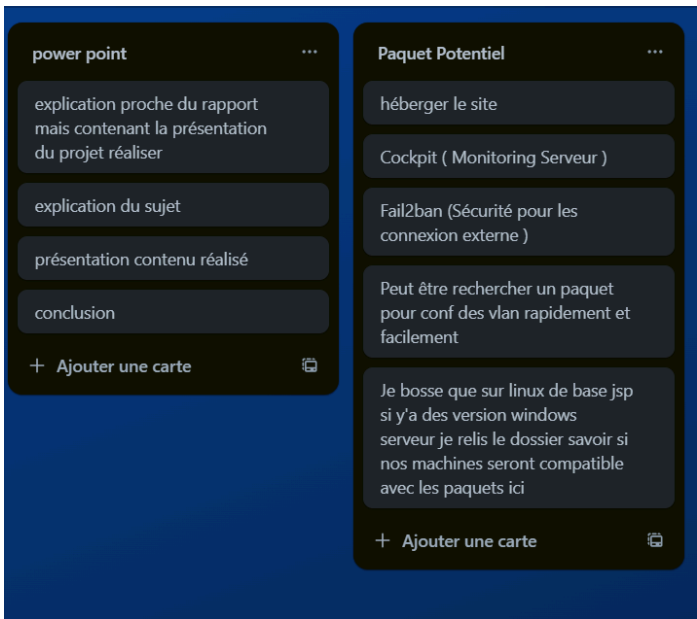
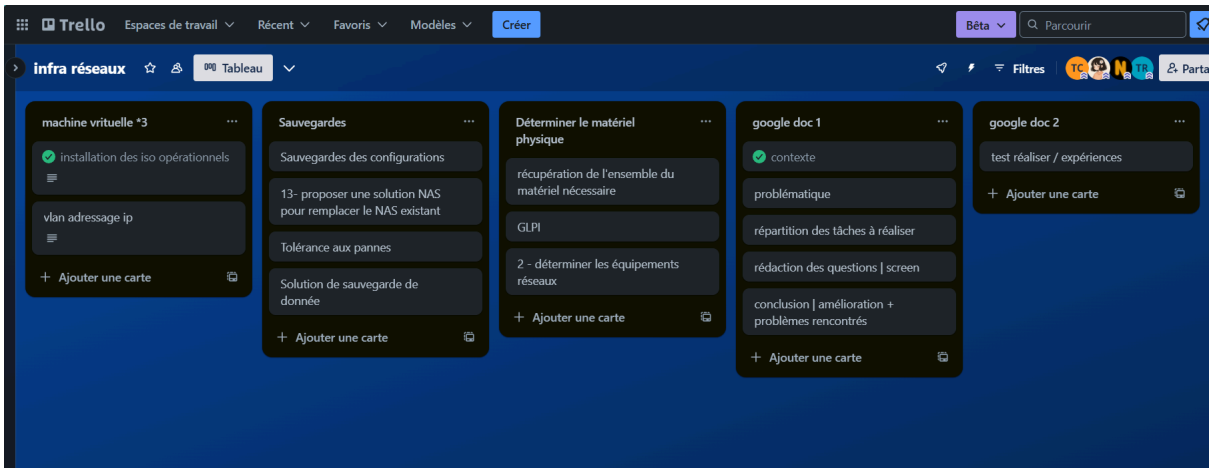
Dans le cadre du déploiement du nouveau réseau informatique du centre de recherche GenHealth, il est primordial de concevoir une infrastructure à la fois performante, sécurisée et adaptée aux besoins métier de l'entreprise.

GenHealth regroupe plusieurs pôles fonctionnels (laboratoire, bureaux administratifs, open-space, accueil, Salle serveurs, salle de réunion, espace libre.) ayant des usages réseau bien distincts. Une segmentation logique de l'infrastructure s'impose donc pour :

- Améliorer les performances du réseau,
- Renforcer la sécurité en isolant les différentes zones,
- Faciliter l'administration et la gestion des flux de données.

Répartition des tâches :

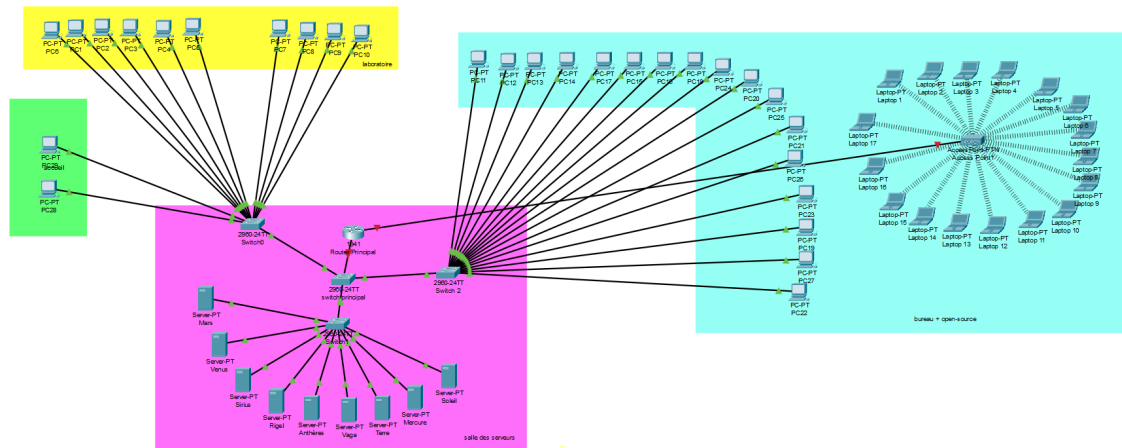
Nous avons tout d’abord mis en place un trelo pour analyser les différentes tâches auxquelles nous serons confrontés.



Suite à ces différentes tâches nous nous sommes selon les membres réparties les missions :

Membres	Tâches associés
Annalia PRIEUR	Doc, Déploiement, packet tracer et hébergement du site web, gestion réseau
Tom CLEMENT	Doc, GLPI, Trello, Gestion réseau, packet tracer
Thibault ROYER	Doc, sauvegarder, Gestion réseau
Noa RODRIGUES	Doc, GLPI , Slide , Gestion réseau

Pour répondre au sujet nous avons réalisé un schéma du plan de l'architecture de notre déploiement de notre réseau informatique :



Afin de répondre à ces enjeux, nous avons opté pour une organisation en VLANs (Virtual LANs), permettant de séparer virtuellement les différents services sur une même infrastructure physique.

1) On associe a chaque zone un Vlan / Nom de Vlan et une adresse IP

Zone	Vlan	Nom Vlan
Laboratoire	10	Vlan-Labo
Open-Space, Bureau	20	Vlan-OB
Accueil, salle de réunion	30	Vlan-AR
Serveur Interne	40	Vlan-Serv
Serveur DMZ	50	Vlan-DMZ
Guest (WIFI)	60	Vlan-Wifi

2) Pour répondre à cette nouvelle question nous avons élaboré la liste des équipements réseaux à partir du logiciel GLPI (Gestionnaire Libre de Parc Informatique).

- 29 pc fixes
- 17 laptops
- 3 switchs
- 3 points d'accès
- 9 serveurs

Liste de notre Parc :



Les pcs et laptops :

<input type="checkbox"/>	Laptop1	HP	GenHealth	2025-04-09 16:36
<input type="checkbox"/>	Laptop10	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop11	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop12	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop13	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop14	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop15	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop16	HP	GenHealth	2025-04-09 16:40
<input type="checkbox"/>	Laptop17	HP	GenHealth	2025-04-09 16:40
<input type="checkbox"/>	Laptop2	HP	GenHealth	2025-04-09 16:37
<input type="checkbox"/>	Laptop3	HP	GenHealth	2025-04-09 16:37
<input type="checkbox"/>	Laptop4	HP	GenHealth	2025-04-09 16:37
<input type="checkbox"/>	Laptop5	HP	GenHealth	2025-04-09 16:38
<input type="checkbox"/>	Laptop6	HP	GenHealth	2025-04-09 16:38
<input type="checkbox"/>	Laptop7	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop8	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	Laptop9	HP	GenHealth	2025-04-09 16:39
<input type="checkbox"/>	PC1	HP	GenHealth	2025-04-09 16:17

Les serveurs, switchs, routeur, point d'accès :

<input type="checkbox"/> NOM ▲	STATUT	FABRICANT	LIEU	TYPE	MODÈLE	FIRMWARE	DERNIÈRE MODIFICATION
<input type="checkbox"/> Anthères		DELL	GenHealth	serveur			2025-04-09 16:48
<input type="checkbox"/> Mars		DELL	GenHealth	serveur			2025-04-09 16:46
<input type="checkbox"/> mercure		DELL	GenHealth	serveur			2025-04-09 16:45
<input type="checkbox"/> point d'accès			GenHealth	point d'accès			2025-04-09 17:05
<input type="checkbox"/> Rigel		DELL	GenHealth	serveur			2025-04-09 16:47
<input type="checkbox"/> routeur principal		DELL	GenHealth	routeur			2025-04-09 16:44
<input type="checkbox"/> Sirius		DELL	GenHealth	serveur			2025-04-09 16:47
<input type="checkbox"/> soleil		DELL	GenHealth	serveur			2025-04-09 16:46
<input type="checkbox"/> switch 1			GenHealth	switch			2025-04-16 15:00
<input type="checkbox"/> switch principal			GenHealth	switch			2025-04-16 14:59
<input type="checkbox"/> switch2			GenHealth	switch			2025-04-09 17:04
<input type="checkbox"/> switch3			GenHealth	switch			2025-04-09 17:04
<input type="checkbox"/> Terre		DELL	GenHealth	serveur			2025-04-09 16:46
<input type="checkbox"/> Vaga		DELL	GenHealth	serveur			2025-04-09 16:48
<input type="checkbox"/> Venus		DELL	GenHealth	serveur			2025-04-09 16:46

3)

Adressage ip pour les différents Vlan afin de séparer les différents services pour limiter la propagation d'éventuelles attaques internes :

- Vlan-Labo : 172.168.10.X
- Vlan-OB : 172.168.20.X
- Vlan-AR : 172.168.30.X
- Vlan-Serv : 172.168.40.X
- Vlan-DMZ : 172.168.50.X
- Vlan-Wifi : 172.168.60.X

Pour les configurer suivre les informations ci-dessous :

switch (config)#

- vlan 10
- name ""
- vlan 20
- name ""
- enable

Switch#

- show vlan (voit toutes les vlan)

switch#

- conf
- entrer

switch (config)#

- int range F0/1-12 (permet de sélectionner les 12 premiers ports)

switch (config-if-range)#

- sw ac vlan 10
- int range f0/13-24
- sw ac vlan 20

réaliser la manipulation pour tous les vlans et les associer dans les différents switch en fonction des services.

Il faut aussi faire une sécurisation des équipements réseau (switchs, routeurs, etc.)

- Changer les identifiants d'administration par défaut.
- Désactiver les services inutiles (ex : Telnet au profit de SSH).
- Mettre à jour le firmware régulièrement pour corriger les failles de sécurité.
- Limiter l'accès à l'interface d'administration (par IP ou via VPN uniquement).




De plus la sécurisation des réseaux est importante

- Créer un réseau invité séparé du réseau interne pour les visiteurs.
- Filtrer les accès par adresse MAC ou par authentification captive.
- Réduire la portée du signal pour limiter les risques d'écoute à l'extérieur. Il faut accéder à l'interface administrateur du routeur ou celle du point d'accès, chercher un point "transmit Power" ou "TX Power" et réduire le pourcentage de diffusion du signal.

5) Pour sauvegarder les diverses configurations des équipements réseau tel que les switch, il est conseillé de faire un serveur TFTP afin de permettre de stocker et de trier toutes les configurations sur une autre machine. Envoyée en fichier texte, il est conseillé de les sauvegarder sur un disque NTFS qui permettra de gérer plus facilement les permissions d'accès à chaque fichier.

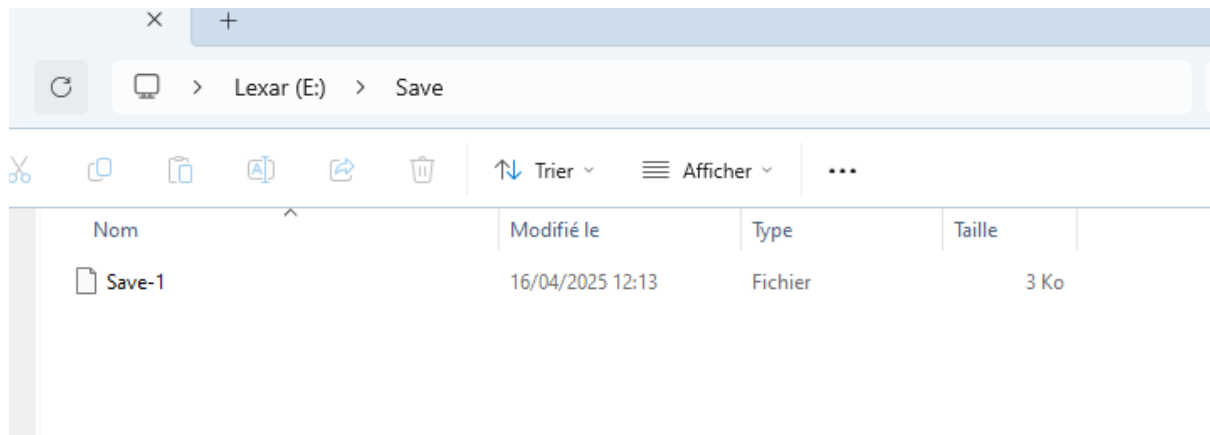
Afin de tester si tout fonctionnait nous avons dû sauvegarder la configuration du switch sur un serveur distant TFTP, pour ce faire nous avons utilisé PuTTY (logiciel permettant d'accéder au switch et le configurer) et tftpd64 (logiciel de tftp par microsoft)

Tout d'abord nous avons téléchargé les logiciels et créé un dossier dans lequel les sauvegardes seront déposées.

Nom	Modifié le	Type	Taille
 Save	16/04/2025 11:55	Dossier de fichiers	
 Tftpd64	16/04/2025 11:55	Dossier de fichiers	
 Tftpd64-4.64-setup.exe	27/03/2025 10:43	Application	634 Ko

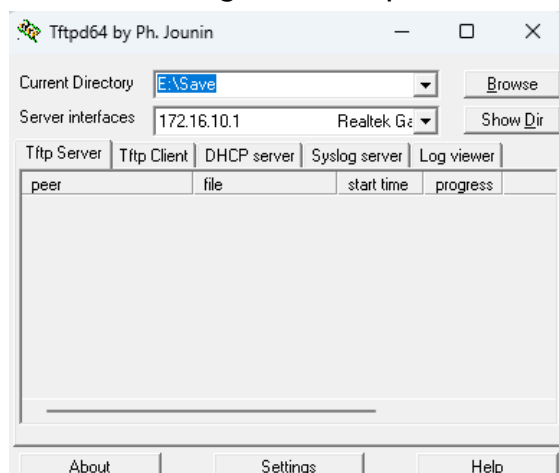
(il n'est pas obligatoire de le mettre au même endroit que la sauvegarde ! Il est juste que pour plus de praticité nous l'avons mis dans le même disque amovible.)

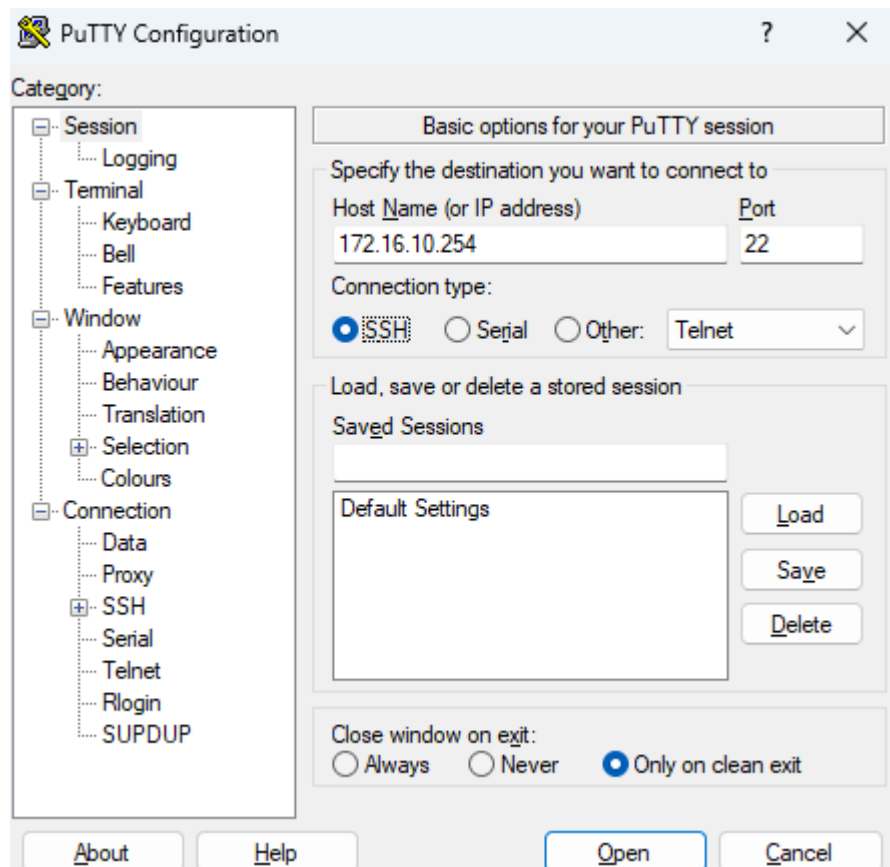
Maintenant pour récupérer la sauvegarde nous allons sur le switch grâce à pUTTY et taper la commande “copy run tftp” afin de pouvoir sauvegarder la configuration du switch sur le serveur tftp ainsi que lui donner un nom approprié



En cas de problème et de perte de la config dans le switch, il est possible d'uploader la configuration dans le switch avec la commande “copy tftp run”

Interface configurée de tftpd64





interface de PuTTY
pour accéder au switch.

Ici nous sommes connecté en telNet car nous ne passons pas par d'autres réseau et donc crypter le flux n'est pas utile

```
User Access Verification

Password:
SwitchCentral>en
Password:
SwitchCentral#copy run tftp
Address or name of remote host []? 172.16.10.1
Destination filename [switchcentral-config]? save-2
!!
2560 bytes copied in 1.233 secs (2076 bytes/sec)
SwitchCentral#
```

commandes utilisées pour enregistrer la configuration.

```
SwitchCentral#copy tftp run
Address or name of remote host []? 172.16.10.1
Source filename []? save-1
Destination filename [running-config]?
Accessing tftp://172.16.10.1/save-1...
Loading save-1 from 172.16.10.1 (via Vlan1): !
[OK - 2560 bytes]
```

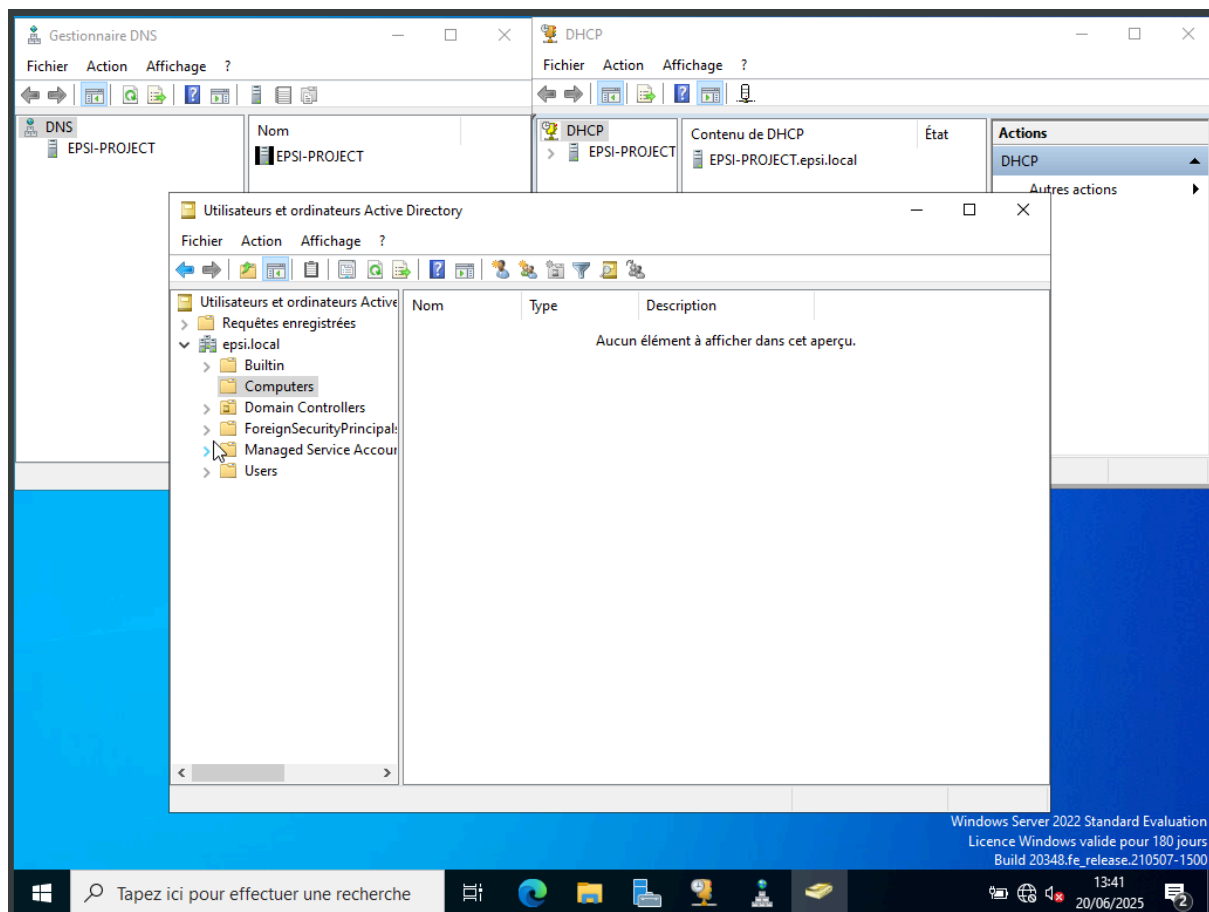

Et ici pour envoyer la config au switch.

8)

Afin de répondre au besoins d'une gestion des utilisateurs nous avons penser à cette solution :

1. Mise en place d'un serveur Active Directory (AD)

- Installer un serveur Windows Server et le promouvoir en tant que contrôleur de domaine.
- Créer une arborescence d'unités d'organisation pour structurer les utilisateurs (ex. : par service ou fonction).
- Gérer les droits d'accès, groupes et stratégies de sécurité depuis une console centrale.



2. Avantages de l'Active Directory

- Centralisation des comptes utilisateurs (création, suppression, modification).

- Authentification unique: les utilisateurs n'ont qu'un seul identifiant/mot de passe.
- Application des stratégies de groupe: contrôle des paramètres utilisateurs et machines à distance.
- Sécurité renforcée : contrôle précis des accès aux fichiers, imprimantes, logiciels. Ça permet de protéger les données sensibles en associant des autorisations d'accès à certains fichiers.

3. Intégration des postes clients

- Les postes Windows doivent être rejoints au domaine. Cela permet l'application automatique des règles et politiques définies dans l'AD

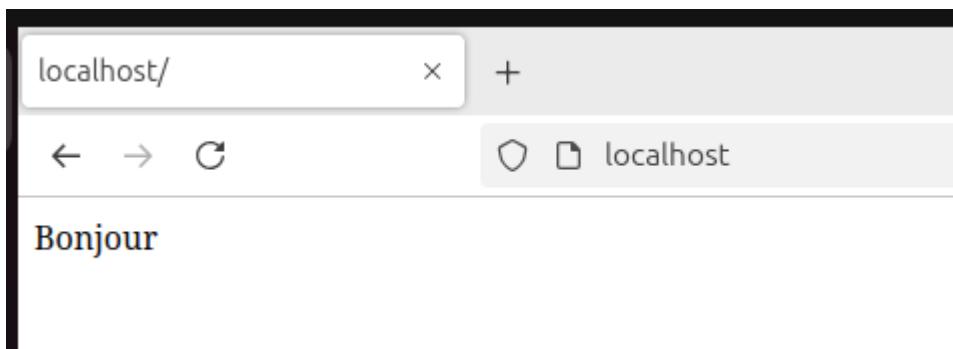
9) Amélioration de la tolérance aux pannes

Pour améliorer la tolérance aux pannes des sauvegardes il peut être recommandé de faire des sauvegardes sur deux serveurs différents. Ainsi si jamais un tombe, l'autre prendra le relais et les données ne seront pas perdues. De plus, un serveur de stockage coupé du réseau peut aussi être d'une grande aide pour éviter les menaces de rançon. Le seul bémol d'avoir ces plusieurs sauvegardes c'est que cela peut mener à un temps d'attente du téléchargement de l'ancienne version plutôt long. De plus, avoir au moins un deuxième serveur permettra de ne pas couper les services, l'autre prenant directement le flux de l'autre en cas de panne.

10) Pour les sauvegardes, si il est possible de le faire sur de multiples serveurs, il pourrait être conseillé de sauvegarder chaque jour de la semaine 10% du travail effectué et des données, et, le week-end ou lorsque personne ne travaille, faire un téléchargement complet de toutes les modifications (donc une sauvegarde différentielle) sur le serveur coupé du réseau et sur le second serveur.

11) Installation d'apache2 sur une vm Ubuntu (sudo apt install apache2). Modifications du fichier /var/www/html/index.html et on a entré l'adresse "localhost" dans mon navigateur. Ensuite nous avons programmé apache pour qu'il s'allume automatiquement au démarrage de la VM (sudo systemctl enable apache2).

```
annalia@annalia-VMware-Virtual-Platform:~$ sudo systemctl enable apache2
[sudo] password for annalia:
Synchronizing state of apache2.service with SysV service script with /usr/lib/sy
stemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
```



12)

Dans le cas d'un remplacement de 30 postes, le meilleur plan pour configurer les postes serai :

1. Création d'une image système

- Préparer une machine de référence avec le système d'exploitation, les pilotes, logiciels et configurations nécessaires.
- Utiliser un outil de capture d'image (par exemple acronis)

2. déploiement par réseaux

- L'image sera sauvegardée sur un serveur (PXE) relié aux ordinateurs par un câble rj45 sur un switch. Le serveur aura un outil WDS (Windows Deployment Services) qui va permettre de déployer l'image sur chaque poste.

3. Automatisation de la configuration

- Prévoir une configuration automatique des noms de machine et de l'adressage IP via DHCP.

4. Contrôle

- Vérifier sur 1 ou 2 postes que l'ensemble de la configuration est un succès avant de l'effectuer sur les autres postes.

Pourquoi le plan que nous proposons est une bonne idée ?

- **Gain de temps important** : déploiement simultané ou en série sans intervention manuelle répétitive.
- **Uniformité** : toutes les machines auront la même configuration.
- **Facilité de maintenance** : plus simple à gérer dans le futur. leurs images seront gardées et stockées dans les disques du serveur PXE.

13) Pour changer le NAS il faut déjà déterminer le nombre de données qui vont être à stocker dans les prochaines années afin de proposer la meilleure des solutions de stockage.

1 an	5
2 ans	6
3 ans	7
4 ans	9
5 ans	11
6 ans	13
7 ans	15
8 ans	18
9 ans	21
10 ans	25
11 ans	29

Ici on pourrait notamment conseiller une configuration RAID 5 avec 3 disques de 8To, donnant ainsi un total de 16 To de stockage et une redondance de 8To en cas de panne.

Pour respecter ces demandes et pour qu'il puisse durer le plus longtemps, le QNAP TS-453E-8G est des plus optimal. Car il bénéficie de suffisamment de ram (8Go) pour un serveur NAS et d'un Intel Celeron J6412.,

15)

Mise en place d'un pare-feu (Firewall)

- Définir des règles de filtrage : autoriser uniquement le trafic nécessaire (HTTP, HTTPS, DNS...)
- Bloquer les ports non utilisés
- Surveiller le trafic sortant pour empêcher l'accès à des sites dangereux ou non professionnels

16)

Afin de mettre en place une tolérance aux pannes de la liaison internet, l'utilisation d'un multi lien internet serait intéressant. Le principe est de souscrire à deux abonnements Internet auprès de fournisseurs différents (ex. : Orange + SFR). En cas de défaillance du lien principal, le trafic bascule automatiquement vers le second lien.

Pour réaliser la conception de la tolérance du au pannes internet, il nous faudrait donc un serveur ou un pare-feu compatible avec un multi-WAN. Le serveur va permettre de répartir le trafic sur les deux connexions et de basculer tous sur un des réseaux en cas de panne.

Il faudra aussi une configuration des règles de routage (IP publique DNS)

Il est possible aussi de prévoir une clé 4G ou 5G si les deux lignes de réseaux tombent en panne simultanément.

Les avantages de notre solution son multiple cela permet de réduire les pannes de courants donc de fluidifier le travail et faire en sorte que tous les VPN, Cloud ect reste en marche même lors du panne lié au réseau.

Question 4/6/7 voir cisco

- Positionnement du routage
- adressage ip en DHCP
- DNS

