

# Infrastructure d'une PME avec deux sites distants



*Fontana Andrea  
Av. de la Gare 14  
1450, Ste-Croix*

**cpnv**  
Centre professionnel du Nord vaudois  
Haute école d'ingénierie

SI-CA2a

*07.04.2025*

## Table des matières

1	Analyse préliminaire .....	4
1.1	Introduction.....	4
1.2	Organisation.....	4
1.3	Objectifs.....	4
1.4	Méthode de travail.....	5
1.5	Planification initiale.....	6
1.6	Structure du dossier .....	7
1.7	Gestion des versions et sauvegarde du travail .....	7
2	Analyse.....	8
2.1	Cahier des charges détaillé .....	8
2.1.1	Définition du contenu et des fonctionnalités.....	12
2.1.2	Situation actuelle.....	12
2.1.3	Utilisateurs cibles .....	12
2.1.4	Présentation des solutions matérielles et logiciels .....	12
2.2	Etude de faisabilité .....	14
2.3	Stratégie de test.....	14
2.4	VPN IPsec .....	15
3	Conception.....	16
3.1	Plans topologiques .....	16
3.1.1	Topologie Hybride Logique/physique.....	16
3.1.2	Conventions de dénomination et d'adressage .....	16
3.1.3	Structures logiques et arborescences.....	17
3.2	Mise en place de la Sécurité.....	19
4	Réalisation et mise en service.....	20
4.1	Description des tâches effectuées.....	20
4.1.1	Rufus .....	20
4.1.2	Putty .....	21
4.1.3	Poste fixe .....	22
4.1.4	Imprimante Bullet.....	22
4.1.5	Switch Bullet .....	22
4.1.6	Routeur Bullet.....	23
4.1.7	Firewall .....	26

4.1.8	Premier serveur .....	28
4.1.9	Serveur redondant .....	33
4.1.10	Nas.....	35
4.1.11	Access Point Bullet.....	36
4.1.12	Laptop.....	38
4.1.13	Routeur Lausanne .....	38
4.1.14	Imprimante Lausanne .....	41
4.1.15	Switch Lausanne .....	41
4.1.16	Access Point Lausanne.....	43
4.2	Description des tests effectués .....	45
4.3	Problèmes rencontrés .....	46
4.3.1	PrintNightmare.....	46
4.3.2	Délégation DFS.....	46
4.4	Erreurs restantes .....	49
4.5	Liste des documents fournis et dossier d'archivage .....	50
5	Conclusions .....	50
5.1	Comparaison entre la conception et la réalisation.....	50
5.2	Etat actuel du projet.....	50
5.3	Améliorations possibles .....	50
5.4	Ressenti sur le projet .....	51
6	Annexes .....	51
6.1	Sources – Bibliographie.....	51
6.1.1	Intelligences Artificielles : .....	51
6.1.2	Sites internet : .....	52
6.1.3	Personnes extérieures au projet : .....	52
6.2	Glossaire .....	53
6.3	Table des illustrations.....	53
6.4	Journal de bord.....	53

# **1 Analyse préliminaire**

## **1.1 Introduction**

Ce projet a pour objectif de concevoir et de mettre en place une infrastructure informatique complète pour une petite entreprise fictive Kicroit basée à Bullet. L'entreprise cherche à se développer et veut repenser toute son infrastructure réseau pour incorporer une succursale à Lausanne. La sécurité des données est une prérogative pour l'entreprise.

Le choix de sujet s'explique par mon intérêt marqué pour l'administration des systèmes et réseaux. Ce projet me permet d'approfondir mes compétences techniques dans un contexte concret et d'acquérir une expérience précieuse dans la mise en œuvre de solutions informatiques adaptées aux besoins spécifiques d'une organisation. De plus, il constitue une opportunité d'appliquer mes connaissances actuelles en réseau (Lan, Vlan, VPN, ...), en gestion des services Windows Server (Active Directory, DNS, DHCP, ...) et en configuration de solutions de stockage centralisé comme le NAS.

Pour l'école ce projet permet de mettre en application ce qui m'a été enseigné. Il permet également de valoriser la formation en illustrant la mise en œuvre de solutions modernes et adaptées aux exigences du marché du travail.

L'infrastructure proposée comprendra la mise en place d'un réseau structuré autour d'un serveur Windows en assurant les services de bases tels que l'authentification des utilisateurs (AD), la gestion des ressources réseau (DHCP, DNS), la gestion de fichier et un pool d'impression. La sauvegarde des données sera sécurisée via un NAS Synology. De plus la sécurité sera assurée par un Firewall. Enfin la connexion VPN site à site se fera par l'intermédiaire de deux routeur Sisco.

Ainsi, ce projet permettra d'approfondir mes compétences en gestion d'infrastructure IT tout en répondant aux besoins concrets de l'entreprise, en proposant une solution adaptée, sécurisée et évolutive.

## **1.2 Organisation**

**Élève :** Fontana Andrea, [andrea.fontana@eduvaud.ch](mailto:andrea.fontana@eduvaud.ch), 078 635 58 59

**Chef de projet :** Vitor Coval, [vitor.coval@eduvaud.ch](mailto:vitor.coval@eduvaud.ch), 079 784 52 81

**Expert 1:** Daniel Berney, [daniel.berney@heig-vd.ch](mailto:daniel.berney@heig-vd.ch), 079 209 87 93

**Expert 2:** Cédric Schaffter, [cedric\\_schaffter@outlook.com](mailto:cedric_schaffter@outlook.com), 076 822 41 27

## **1.3 Objectifs**

Les objectifs à atteindre durant ce projet sont les suivants :

Installer et configurer l'infrastructure réseau d'une petite entreprise.

- Installer deux routeurs
- Installer un firewall
- Installer un serveur : DHCP, DNS, AD, Serveur d'impression, Serveur de fichier.

- Installer un serveur pour la redondance
- Configurer deux imprimantes
- Configurer trois postes de travail
- Installer deux Access Point
- Installer un serveur de Back up sur un NAS.
- Installer deux Switchs PoE
- Connecter deux routeurs distants et les appareils qui en découlent via VPN

Critères de validation des objectifs :

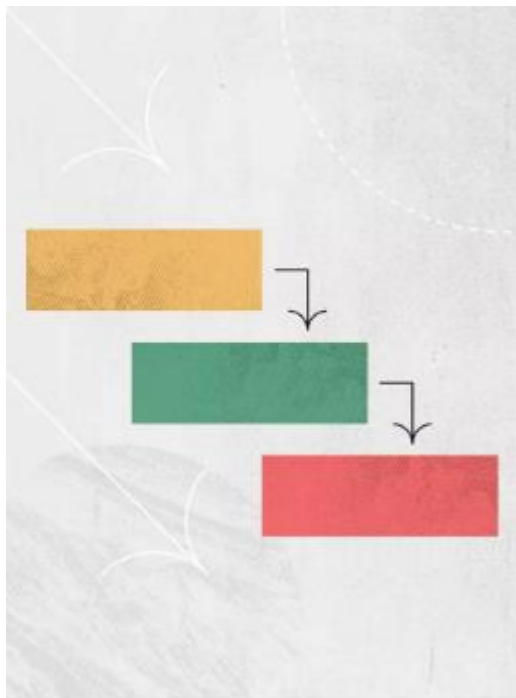
- Le schéma de l'infrastructure réseau doit être complet et explicite.
- Les services AD, DNS, DHCP, FS et impression doivent être fonctionnels et redondants.
- Le tunnel IPSEC doit être fonctionnel et son installation doit être précisément documentée.
- Le firewall doit respecter les règles de sécurité de base.
- Les access point doivent être correctement configurés.
- Le NAS doit effectuer un back up des données contenues sur le serveur complet et un back up incrémentiel. L'installation doit être clairement documentée.
- Les appareils ne doivent pas pouvoir communiquer entre eux que lorsque que c'est nécessaire.
- Les imprimantes doivent être installées et visibles sur le réseau.

#### **1.4 Méthode de travail**

Pour ce projet la méthode de travail Waterfall<sup>1</sup> est la plus adaptée. C'est une méthodologie de gestion de projet séquentielle, organisée en plusieurs phases, où chaque phase dépend de la dernière.

---

<sup>1</sup> <https://asana.com/fr/resources/waterfall-project-management-methodology>



**Figure 1 Schéma Waterfall**

Ce projet applique ce processus. En effet il n'est pas possible de réaliser la mise en place de l'infrastructure si l'analyse préliminaire n'a pas été faite. De même il n'est pas possible d'effectuer des tests si la réalisation n'est pas encore effectuée. Cette méthode est donc la plus adaptée au projet. Cependant toutes les étapes d'un Waterfall « classique » ne sont pas nécessaires. Voici donc les étapes qui seront appliquées ici :

#### **Définition des besoins**

Durant cette phase le cahier des charges est analysé pour en ressortir les objectifs et les difficultés.

#### **Conception de l'infrastructure**

Durant cette phase les moyens déployés pour répondre aux objectifs sont définis. Les solutions apportées sont référencées et explicitées.

#### **Mise en œuvre**

Durant cette phase l'infrastructure réseau est mise en place conformément à la conception.

#### **Tests**

Durant cette phase les différents tests imaginés durant la conception sont réalisés et les erreurs potentielles sont documentées et corrigées.

Il est à noter que pour faciliter la résolution de problèmes certains tests seront réalisés durant la phase de mise en œuvre afin de limiter l'impacte sur le reste de la réalisation. Cependant les tests ne pouvant être fait qu'après la mise en service de l'appareil la chronologie est respectée.

### **1.5 Planification initiale**

## **1.6 Structure du dossier**

Ce dossier est structuré en fonction des différentes étapes du projet. Il débute par une introduction qui présente les grandes lignes du projet. Ensuite vient l'analyse qui développe les solutions envisagées ainsi que les objectifs du projet. La conception apporte des éléments concrets qui correspondent aux besoins identifiés durant l'analyse. La réalisation est l'étape qui décrit les tâches effectuées, les problèmes rencontrés et les problèmes persistants. Enfin la conclusion vient résumer le dossier et apporte une ouverture sur les améliorations possibles du projet.

## **1.7 Gestion des versions et sauvegarde du travail**

Afin de garantir l'intégrité des données, la règle du 3-2-1 est mise en place. Cette règle recommande d'avoir au moins trois copies des données dans deux lieux de stockages différents et une copie hors site. Les documents produits sont sauvegardés en trois points distincts. Le premier est l'ordinateur de travail présent à Sainte-Croix, le deuxième est une clé USB présente aussi à Sainte-Croix et le troisième est un repository GitHub<sup>2</sup>. Chaque fichier est sauvegardé en local après modification et une sauvegarde complète du dossier est effectuée durant la dernière période de chaque journée sur la clé USB et push sur GitHub.

---

<sup>2</sup><https://github.com/andreafont/TPI-Infrastrucutre-d-une-PME-avec-deux-sites-distants/tree/main>

## 2 Analyse

### 2.1 Cahier des charges détaillé

#### 1 INFORMATIONS GENERALES

Candidat :	Nom : <b>FONTANA</b>	Prénom : <b>ANDREA</b>
	✉ : <a href="mailto:andrea.fontana@eduvaud.ch">andrea.fontana@eduvaud.ch</a>	☎ : 078 635 58 59
Lieu de travail :	<input type="checkbox"/> CPNV, Rue de la Gare 14, 1450 Sainte-Croix	
Orientation :	<input type="checkbox"/> 88601 Développement d'application	
	<input type="checkbox"/> 88602 Informatique d'entreprise	
	<input type="checkbox"/> 88603 Technique des systèmes	
	<input checked="" type="checkbox"/> 88614 Informaticienne d'entreprise CFC	
Chef de projet :	Nom : COVAL	Prénom : Vitor
	✉ : <a href="mailto:vitor.coval@eduvaud.ch">vitor.coval@eduvaud.ch</a>	☎ : 079 784 52 81
Expert 1 :	Nom : BERNEY	Prénom : Daniel
	✉ : <a href="mailto:daniel.berney@heig-vd.ch">daniel.berney@heig-vd.ch</a>	☎ : 079 209 87 93
Expert 2 :	Nom : SCHAFFTER	Prénom : Cédric
	✉ : <a href="mailto:cedric.schaffter@outlook.com">cedric.schaffter@outlook.com</a>	☎ : 076 822 41 27
Période de réalisation :	Du <b>lundi 7 avril 2025 à 8h15</b> au <b>mercredi 14 mai 2025 à 10h40</b>	
Horaire de travail :	Lundi	08h15-12h30    13h20-15h50
	Mardi	08h15-10h50    13h20-16h40
	Mercredi	08h15-12h30    13h20-15h50
	Jeudi	08h15-12h30    -
	Vendredi	08h15-11h40    -
	<i>Toutes les demi-journées ont une pause obligatoire de 15 minutes le matin et de 10 minutes l'après-midi, sauf si elles commencent à 10h05 ou si elles se terminent à 14h55. Les vacances scolaires auront lieu du 12 avril 2025 au 27 avril 2025.</i>	
Nombre d'heures :	90 heures	
Planning (en H ou %)	Analyse 20%, Implémentation 40%, Tests 15%, Documentation 25%	
Présentation :	Dates retenues : 27 ou 28 mai 2025	

#### 2 PROCÉDURE

Le candidat réalise un travail personnel sur la base d'un cahier des charges reçu le 1er jour.

Le cahier des charges est approuvé par les deux experts. Il est en outre présenté, commenté et discuté avec le candidat. Par sa signature, le candidat accepte le travail proposé.

Le candidat a connaissance de la feuille d'appréciation avant de débiter le travail.

Le candidat est entièrement responsable de la sécurité de ses données.

En cas de problèmes graves, le candidat avertit au plus vite les deux experts et son CdP.

Le candidat a la possibilité d'obtenir de l'aide, mais doit le mentionner dans son dossier.

A la fin du délai imparti pour la réalisation du TPI, le candidat doit transmettre par courrier électronique le dossier de projet aux deux experts et au chef de projet. En parallèle, une copie papier du rapport doit être fournie sans délai en trois exemplaires (L'un des deux experts peut demander à ne recevoir que la version électronique du dossier). Cette dernière doit être en tout point identique à la version électronique.

Figure 2 Cahier des charges 1



### 3 TITRE

Infrastructure d'une PME avec deux sites distants

### 4 MATÉRIEL ET LOGICIEL À DISPOSITION

- 2 Routeurs Cisco 1921
- 1 Firewall Fortinet FG-50E
- 1 Serveur HP Proliant MicroServer Gen10
- 1 Serveur redondant HP Proliant MicroServer Gen10
- 1 NAS Synology DS923+
- 2 AP Cisco Aironet AIR-SAP2602I-E-K9
- 3 Ordinateurs (1 poste client fixe DELL Optiplex 9020 et deux mobiles DELL Latitude E6520)
- 2 Imprimantes DCP-L8400CDN
- 2 Switchs Cisco Catalyst 3560

### 5 PRÉREQUIS

Avoir suivi les modules 117, 123, 126, 127, 129, 143, 146, 159, 182, 304, 305.

Le candidat maîtrise les divers concepts réseau et système, a déjà utilisé divers outils de sauvegarde

### 6 DESCRIPTIF DU PROJET

La société Kicroit (société fictive) est une petite entreprise familiale basée à Bullet.

Son activité principale nécessitant la proximité d'un centre urbain, de nouveaux locaux ont été acquis en ville de Lausanne.

N'ayant pas de parc informatique – les employés utilisaient les fichiers sur leurs ordinateurs et se les partageaient par email – il faut créer toute l'infrastructure réseau.

Sur le site de Bullet il faut installer un serveur avec les services AD, DNS, DHCP, FS (sur le NAS) et impression. Une solution de sauvegarde doit être effectuée sur le NAS (complète les samedis 01h00 et incrémentielle du Mardi au Vendredi 01h00). Les utilisateurs doivent avoir accès à Internet. Un serveur de redondance/backup des services AD, DNS, DHCP, FS et impression doit aussi être installé.

Les employés sur le site de Lausanne doivent pouvoir accéder aux services proposés à Bullet. Ils accèdent aux mêmes serveurs à travers une connexion sécurisée (VPN).

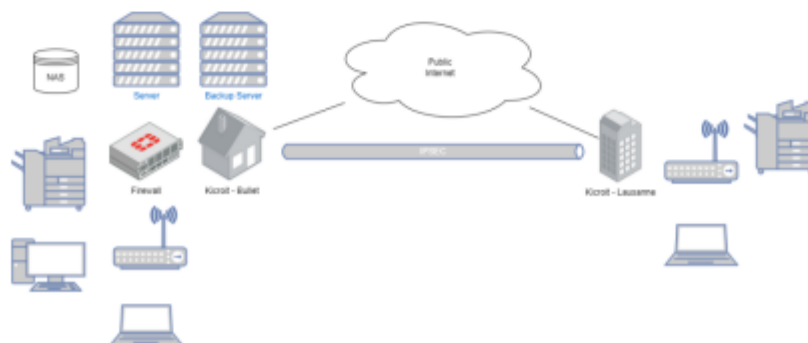


Figure 3 Cahier des charges 2

- o Une copie papier aux experts du rapport de travail.

## 8 POINTS TECHNIQUES ÉVALUÉS SPÉCIFIQUES AU PROJET

La grille d'évaluation définit les critères généraux selon lesquels le travail du candidat sera évalué (documentation, journal de travail, respect des normes, qualité, ...).

En plus de cela, le travail sera évalué sur les 7 points spécifiques suivants (Point A14 à A20):

1. Schéma de l'infrastructure réseau :
  - 3 points = schéma complet (routes, adresses, masques, noms, ...)
  - 2 points = manque 1 élément ou schéma non conventionnel
  - 1 point = schéma incomplet
  - 0 points = pas fait
2. Explication de la mise en place du tunnel IPSEC
  - 3 points = explication claire et précise
  - 2 points = manque 1 élément
  - 1 point = explication incomplète
  - 0 points = pas fait
3. Les services AD, DNS, DHCP, FS et impression sont redondants
  - 3 points = tous les services sont redondants
  - 2 points = manque 1 service
  - 1 point = manque plusieurs services
  - 0 points = pas fait
4. Configuration du firewall
  - 3 points = toutes les règles de base (sécurité minimum) sont configurées
  - 2 points = manque 1 règle de base
  - 1 point = manque plusieurs règles de base
  - 0 points = pas fait
5. Configuration de l'AP
  - 3 points = configuration complète
  - 2 points = manque la configuration d'un élément
  - 1 point = manque la configuration de plusieurs éléments
  - 0 points = pas fait
6. Explication installation serveur de backup
  - 3 points = explication claire et précise
  - 2 points = manque 1 élément
  - 1 point = beaucoup d'éléments manquent
  - 0 points = pas fait
7. Installation des imprimantes
  - 3 points = les imprimantes sont installées et vues dans le réseau
  - 2 points = les imprimantes sont installées mais quelques bugs persistent
  - 1 point = une imprimante n'est pas installée
  - 0 points = pas fait

**Figure 4 Cahier des charges 3**

Schéma modèle comprenant le matériel à disposition. Le schéma de l'infrastructure finale sera créé par le candidat.

### 6.1 La partie du projet que le candidat doit développer est la suivante

- Infrastructure réseau à Bullet :
  - o Serveur (AD, DNS, DHCP, FS et impression)
  - o Serveur redondant (AD, DNS, DHCP, FS et impression)
  - o Firewall
  - o Routeur
  - o Switch
  - o NAS
  - o AP
  - o Imprimante
  - o Poste client fixe
- Infrastructure réseau à Lausanne :
  - o Router
  - o Switch
  - o AP
  - o Imprimante
- Utilisateurs
  - o Jean Dupont – [jean.dupont@kicroit.ch](mailto:jean.dupont@kicroit.ch) – groupe Marketing
  - o Marie Martin – [marie.martin@kicroit.ch](mailto:marie.martin@kicroit.ch) – groupe Marketing
  - o Pierre Lefevre – [pierre.lefevre@kicroit.ch](mailto:pierre.lefevre@kicroit.ch) – groupe Marketing
  - o Sophie Durand – [sophie.durand@kicroit.ch](mailto:sophie.durand@kicroit.ch) – groupe Finances
  - o Lucie Bernard – [lucie.bernard@kicroit.ch](mailto:lucie.bernard@kicroit.ch) – groupe Finances
- Divers
  - o Les deux PC portables doivent pouvoir avoir accès au réseau et ses ressources depuis les deux sites

Le candidat connectera les deux routeurs ensemble par un câble Ethernet, afin de ne pas ajouter la complexité du FAI et ainsi protéger son travail d'éventuelles attaques informatiques pouvant surgir de l'extérieur.

## 7 LIVRABLES

Le candidat est responsable de livrer à son chef de projet et aux deux experts :

- Une planification initiale
- Un rapport de projet
- Un journal de travail
- A la fin du TPI (14 mai 2025 à 10h40)
  - o Le rapport de travail sous forme électronique
  - o Le journal de travail sous forme électronique
  - o Une archive contenant tous les scripts et fichiers de configuration utilisés/créés

Figure 5 Cahier des charges 4

### **2.1.1 Définition du contenu et des fonctionnalités**

L'entreprise Kicroit souhaite moderniser son infrastructure informatique afin de mieux gérer ses ressources, optimiser la collaboration entre ses membres, assurer la sécurité des données et permettre aux deux sites d'accéder aux mêmes ressources.

Pour pouvoir faire fonctionner et sécuriser l'infrastructure un firewall faisant la liaison entre les différentes parties du réseau est nécessaire. De plus un tunnel VPN site à site fera la liaison entre le site de Bullet où se trouvent les serveurs et le site de Lausanne. Les utilisateurs de Lausanne doivent avoir accès aux services des serveurs de Bullet et pouvoir se connecter au domaine

Il est nécessaire de mettre en place un contrôleur de domaine basé sur un micro-serveur, avec une gestion centralisée des utilisateurs et des permissions. L'installation d'un AD, d'un DNS et d'un DHCP est requis. Le serveur devra aussi offrir un service d'impression et service de fichier. De plus pour plus de sécurité un serveur redondant proposant les mêmes services sera installé.

Il faut également installer un NAS le Back up des données. Ainsi que définir et appliquer les groupes de sécurité pour restreindre l'accès aux différentes ressources.

Enfin, L'entreprise veut un wifi pour ces employés. Il faudra sécuriser les deux Access Point pour éviter tout risque d'intrusion.

### **2.1.2 Situation actuelle**

Actuellement la société n'a pas d'installation Informatique viable. Ils n'ont pas de parc informatique, chaque utilisateur travaille sur son poste personnel et les fichiers étaient transmis par email. Cette solution n'est, en effet, pas suffisante pour l'ouverture d'une succursale. Les données ne sont pas sauvegardées, les utilisateurs impriment via le logiciel HP classique ce qui ne permet pas de gérer efficacement les imprimantes et n'ayant pas de serveur il n'est pas possible d'avoir un domaine permettant à chacun de se connecter sur tous les postes.

### **2.1.3 Utilisateurs cibles**

L'objectif est de fournir une infrastructure clé en main pour que l'entreprise puisse travailler sans avoir à se soucier du réseau. A ce titre, et comme l'entreprise n'a pas d'IT à proprement parler, ils n'auront pas accès aux comptes administrateurs pour éviter toute complication.

### **2.1.4 Présentation des solutions matérielles et logiciels**

#### **Présentation des solutions matérielles**

Le point critique de ce projet se situe au niveau de la structure du réseau. La présence de deux sites crée plusieurs problèmes. Premièrement, le site de Lausanne n'ayant pas de DHCP il doit utiliser celui de Bullet. Deuxièmement, l'imprimante de Lausanne doit être accessible par le serveur de Bullet mais elle doit aussi être sécurisée. Troisièmement, les ordinateurs de Lausanne doivent avoir accès aux fichiers et services de Bullet. Il existe plusieurs solutions pour répondre à ce problème.

Pour régler ces problèmes il faut les prendre d'abord individuellement. Pour l'imprimante il n'y a pas beaucoup de solutions, le plus simple et efficace est de séparer l'imprimante dans un réseau dédié. Ainsi elle ne peut pas communiquer librement avec les autres appareils et il est possible de mettre en place des règles de

firewall spécifiques pour ne laisser transiter que les protocoles d'impression. Il serait aussi possible de bloquer manuellement les requêtes de la machine en se basant sur son IP et donc de la laisser dans le même réseau mais cela laisse plus de place à l'erreur et cela implique de le refaire si une autre imprimante est ajoutée.

Pour le problème du DHCP et des ressources une première solution serait de mettre toutes les adresses IP en statique à Lausanne. En faisant cela il n'y a plus le problème du DHCP. Le tunnel VPN permettrait d'accéder aux ressources de l'entreprise. Cette solution est la plus simple dans le cadre de cet exercice mais la plus laide et la moins efficace dans un cas concret. En effet elle implique de devoir configurer manuellement chaque appareil ce qui est une perte de temps conséquente et laisse place aux erreurs. Comme personne à Kicroit n'est IT cela implique aussi un suivi constant de la part de notre entreprise.

Une deuxième solution serait de créer le même réseau sur les deux sites. Si le réseau est identique alors le DHCP pourra fonctionner et donner les adresses des deux côtés. Après discussion avec monsieur Varela cette technique comporte cependant un risque. Comme le réseau est le même de part et d'autre du routeur il ne sait pas où il doit envoyer le paquet ou risque de l'envoyer par défaut toujours au même endroit. Il est possible de contrecarrer ce problème en utilisant le NAT pour spécifier dans quelle partie du réseau les routeurs doivent envoyer les requêtes. Cette solution fonctionne mais complexifie considérablement le projet.

Une troisième solution serait de créer deux réseaux séparés et d'utiliser un relai DHCP. Sur le service DHCP du serveur il faudrait créer deux étendues distinctes et suivant qui fait la requête le DHCP donnerait une adresse d'une plage ou de l'autre. Cette solution demande de mettre en place sur le routeur de Lausanne un relai DHCP en unicast qui redirige sur le serveur. Elle est relativement simple à mettre en place et répond à tous les problèmes posés par les deux sites.

### **Solution Choisie**

Pour répondre aux contraintes de sécurité les imprimantes de Lausanne seront dans leur propre réseau. L'idée est d'utiliser deux Vlan pour séparer la partie imprimantes et la partie utilisateurs sur le site. Pour répondre aux contraintes d'accès aux ressources deux étendues seront créées dans le DHCP et un relai DHCP sera mis en place sur le routeur de Lausanne. La combinaison de ces solutions offre un bon niveau de sécurité puisque les connexions seront gérées par le firewall et permettent de gérer facilement le parc de Lausanne avec le serveur de Bullet.

### **Présentation des solutions logicielles.**

Dans ce projet il est demandé d'utiliser le Nas pour faire un backup des fichiers en respectant certaines contraintes. Une sauvegarde complète doit être faite le samedi à 1h toutes les semaines et une sauvegarde incrémentielle doit être faite du mardi au vendredi à 1h.

La première solution est d'utiliser Active backup business<sup>3</sup>. C'est un paquet téléchargeable qui s'insère directement sur le Nas via le centre de paquet ou via une clé USB. Il a l'avantage d'être facile à utiliser, il permet de faire des backups en ayant uniquement l'adresse IP et les identifiants du serveur. Cependant il ne permet une grande personnalisation des sauvegardes, par exemple il n'est pas possible de choisir le type de sauvegarde elles sont toujours complètes. Il ne répond donc pas complètement au cahier des charges.

---

<sup>3</sup> <https://www.synology.com/fr-fr/dsm/feature/active-backup-business/pc>



Le Nas Synology n'est pas directement équipé d'une application pour faire des backups et le centre de paquets n'offrent pas de solution convenable non plus. La deuxième possibilité imaginée repose sur L'ISCI. En connectant le Nas en ISCI au serveur il est possible d'utiliser des outils comme les Sauvegardes Windows ou des logiciels tiers. Handy Backup<sup>4</sup> est un logiciel qui permet de paramétrer les sauvegardes pour les ordinateurs et les serveurs. Il est facile d'utilisation et peut faire tout type de sauvegardes.

### **Solution Choisie**

Pour répondre aux contraintes de backup j'ai choisi la solution Handy Backup en utilisant le Nas en ISCI. L'application permet de faire des backups complets et différentiels poussés sans difficulté et mettre le Nas en ICSI évite beaucoup de complications potentielles.

## **2.2 Etude de faisabilité**

La principale contrainte de ce projet est le temps. 90 heures pour mettre en place une infrastructure complète est très serré. Chaque tâche n'est pas très complexe mais un problème qui entrainerait une perte de temps est à prendre très au sérieux.

Une autre contrainte est la contrainte technique. En effet je n'ai que peu travaillé avec un firewall. Mettre en place comme je le désire ce service risque donc de prendre du temps et le résultat n'est pas garanti. Je n'ai jamais configuré de sauvegarde incrémentielle avec un NAS. Même si la configuration demandée n'est pas très poussée les recherches risquent de prendre du temps.

## **2.3 Stratégie de test**

Pour ce projet les tests se feront sur chaque appareil installé. L'ordre des tests suivra l'ordre d'installation des appareils dans sa globalité (Routeur, Firewall, PC 1 et 2, Serveur, Switch, Imprimante, Access point, NAS, Serveur redondant, Routeur Lausanne, PC 1 Lausanne, Imprimante Lausanne, Access point Lausanne, Connexion VPN). Cependant comme certaines parties des configurations se feront après avoir mis en place le reste des infrastructures les tests se feront à ce moment-là. Par exemple il n'est pas possible de tester le service d'impression avant d'avoir installé l'imprimante mais on peut quand même tester les autres fonctionnalités et le fonctionnement du serveur.

Les tests ne demandent pas de matériel supplémentaire. Ils fonctionnent de la manière suivante :

- Quel appareil ou service ?
- Qu'est ce qui est testé ?
- Quel est le résultat attendu ?
- Est-ce que le test est une réussite ou un échec ?
- Remarques supplémentaires.

Les tests ont pour objectifs d'être exhaustifs et d'assurer du bon fonctionnement de l'infrastructure. Ils seront tous réalisés par la personne qui met en place l'infrastructure.

---

<sup>4</sup>[https://www.handybackup.net/?srsId=AfmBOop\\_AP8EptB7n39ocP-PicG2xVfuZEj2bPiA6Vq-i6be3v9uZmHN](https://www.handybackup.net/?srsId=AfmBOop_AP8EptB7n39ocP-PicG2xVfuZEj2bPiA6Vq-i6be3v9uZmHN)

## **2.4 VPN IPsec**

Pour ce projet L'entreprise doit pouvoir lier ses deux sites distincts grâce à un VPN pour permettre aux utilisateurs d'accéder aux ressources de l'entreprise en travaillant sur le site distant.

Le VPN est un réseau virtuel permettant de créer une connexion sécurisée entre différents sites ou utilisateurs à travers internet. Un VPN chiffre les données et masque l'adresse IP ce qui garantit la confidentialité des données. Il existe plusieurs types de VPN mais celui que nous allons mettre en place pour cette entreprise est un VPN site-à-site. Il permet de connecter deux réseaux distincts avec un lien qui n'est pas limité dans le temps et permet le partage de ressources comme si les sites étaient physiquement connectés.

Il existe plusieurs protocoles pour les VPN, nous allons utiliser IPsec. C'est une suite de protocoles qui visent à sécuriser les communications sur un réseau IP. Il se compose de 3 parties.

1. AH (Authentication Header) qui assure l'authenticité et l'intégrité des paquets sans chiffrement des données.
2. ESP (Encapsulating Security Payload) qui assure l'authenticité et l'intégrité des paquets grâce au chiffrement des données.
3. IKE (Internet Key Exchange) qui gère l'établissement des connexions sécurisées et l'échange des clés de chiffrement

Le Fonctionnement du Tunnel IPsec se déroule en trois phases :

1. Négociation IKE

Les deux parties établissent une connexion sécurisée en utilisant un algorithme d'échange de clés. Les protocoles de sécurité et les algorithmes de chiffrement sont négociés

2. Etablissement du Tunnel IPsec

Le tunnel sécurisé est créé entre les deux sites. Les données circulent de manière chiffrée au travers du tunnel

3. Transfert de données

Les paquets IP originaux sont encapsulés dans des paquets IPsec avant d'être envoyés à travers le tunnel

Les différents phases seront explicitées durant la réalisation

### 3 Conception

#### 3.1 Plans topologiques

##### 3.1.1 Topologie Hybride Logique/physique

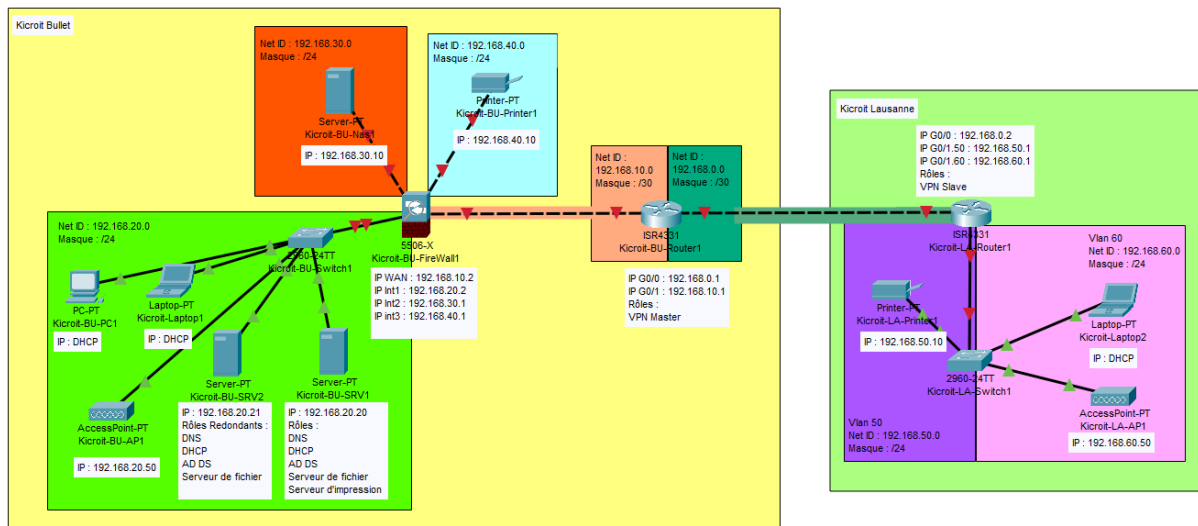


Figure 6 Schéma logique/physique

La topologie a été faite avec le logiciel Cisco Packet Tracer<sup>5</sup>. Cette représentation est le schéma logique/physique réel du projet. Si c'était un cas pratique le Net ID 192.168.0.0 n'existerait pas. Les deux routeurs seraient reliés à internet via le FAI et un tunnel VPN serait fait entre les deux.

##### 3.1.2 Conventions de dénomination et d'adressage

A des fins d'unicité et de clarté, tous les appareils présents dans les réseaux suivent une dénomination commune. Elle prend la forme suivante : Kicroit- « abréviation du site » - « type d'appareil » « numéro de l'appareil ». Par exemple le premier ordinateur fixe installé à Bullet s'appellera : Kicroit-BU-PC1. Le numéro dépend aussi des sites, si un ordinateur fixe était installé à Lausanne il s'appellerait : Kicroit-LA-PC1 et non Kicroit-LA-PC2. Avec cette dénomination il est possible de savoir immédiatement de quelle machine on parle et sur quel site. Les tables d'adressages sont les suivantes.

<sup>5</sup> <https://www.netacad.com/cisco-packet-tracer>



Table d'adressage						
Nom	Rôle	IP	Masque	Passerelle	DNS	DNS secondaire
Kicroit-Laptop1	Ordinateur portable	DHCP	255.255.255.0	192.168.20.2	192.168.20.20	192.168.20.21
Kicroit-Laptop2	Ordinateur portable	DHCP	255.255.255.0	192.168.60.1	192.168.20.20	192.168.20.21
Kicroit-BU-PC1	Poste de travail	DHCP	255.255.255.0	192.168.20.2	192.168.20.20	192.168.20.21
Kicroit-BU-Server1	Contrôleur de domaine, DHCP, DNS, serveur de fichier et d'impression	192.168.20.20	255.255.255.0	192.168.20.2	127.0.0.1	192.168.20.21
Kicroit-BU-Server2	Serveur redondant	192.168.20.21	255.255.255.0	192.168.20.2	127.0.0.1	192.168.20.20
Kicroit-BU-AP1	Access point Bullet	192.168.20.50	255.255.255.0	192.168.20.2	192.168.20.20	192.168.20.21
Kicroit-BU-Nas1	Serveur de backup	192.168.30.10	255.255.255.0	192.168.30.1	-	-
Kicroit-BU-Printer1	Imprimante Bullet	192.168.40.10	255.255.255.0	192.168.40.1	-	-
Kicroit-LA-Printer1	Imprimante Lausanne	192.168.50.10	255.255.255.0	192.168.50.1	-	-
Kicroit-LA-AP1	Access point Lausane	192.168.60.50	255.255.255.0	192.168.60.1	192.168.20.20	192.168.20.21

Figure 7 Table d'adressage

Table d'adressage Firewall				
Interface	Role	IP	Masque	Passerelle
Ian1	Réseau de l'entreprise	192.168.20.2	255.255.255.0	192.168.10.2
Ian2	Réseau du serveur de backup	192.168.30.1	255.255.255.0	192.168.10.2
Ian3	Réseau des imprimantes	192.168.40.1	255.255.255.0	192.168.10.2
Wan1	Connexion au routeur	192.168.10.2	255.255.255.252	192.168.10.1

Figure 8 Table d'adressage firewall

Table d'adressage Routeurs					
Nom	Interface	Role	IP	Masque	Passerelle
Kicroit-BU-Router1	G0/0	Connexion Lausanne	192.168.0.1	255.255.255.252	192.168.0.2
Kicroit-BU-Router1	G0/1	Connexion firewall	192.168.10.1	255.255.255.252	192.168.0.2
Kicroit-LA-Router1	G0/0	Connexion Bullet	192.168.0.2	255.255.255.252	192.168.0.1
Kicroit-LA-Router1	G0/1.50	Vlan imprimantes LA	192.168.50.1	255.255.255.0	192.168.0.1
Kicroit-LA-Router1	G0/1.60	Vlan utilisateurs	192.168.60.1	255.255.255.0	192.168.0.1

Figure 9 Table d'adressage routeurs

### 3.1.3 Structures logiques et arborescences

Cette rubrique présente le fonctionnement de l'entreprise fictive, les différents groupes et employés ainsi que les permissions qui leur seront accordées.

## ORGANIGRAMME GROUPES ET EMPLOYES

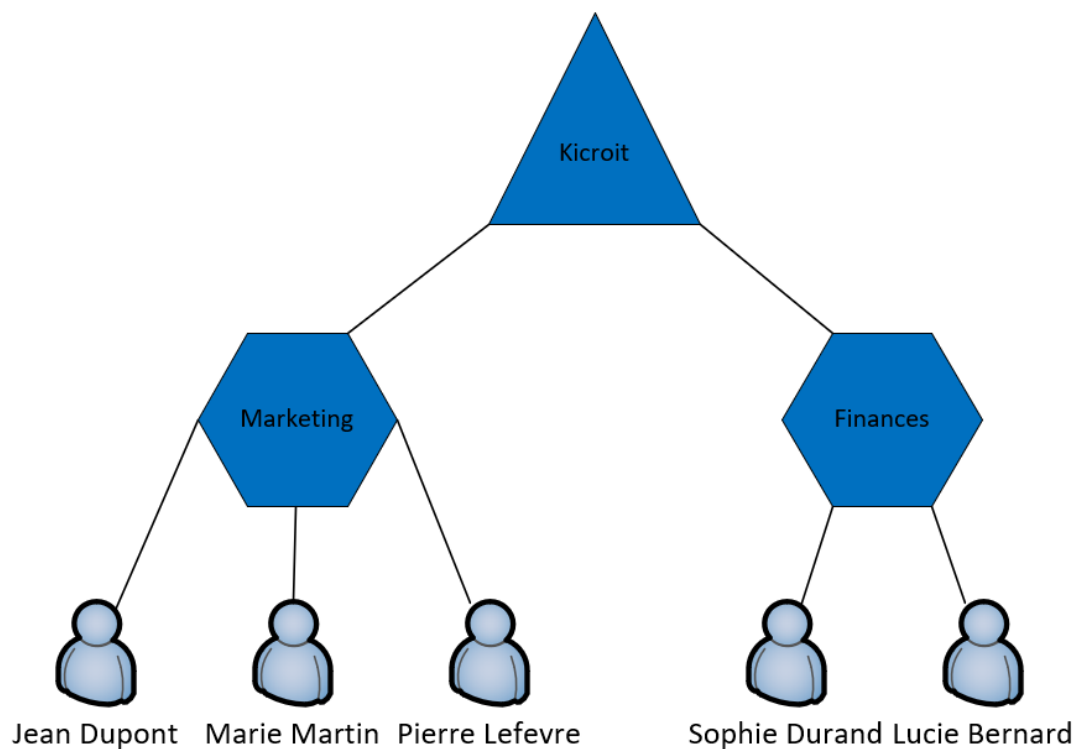


Figure 10 Organigramme Kicroit

Permissions NTFS				
Dossier		Groupes		
		Admins du domaine	Marketing	Finances
F:\		CT		
	\Marketing	CT	M	
	\Finances	CT		M

CT	Contrôle total
M	Modification
LX	Lecture et exécution

Figure 11 Tableau des permissions NTFS

Utilisateurs & Groupes				
Groupes	Admins du domaine	Utilisateurs du domaine	Marketing	Finances
Utilisateurs				
admin	X	X		
Jean Dupont		X	X	
Marie Martin		X	X	
Pierre Lefevre		X	X	
Sophie Durand		X		X
Lucie Bernard		X		X

Figure 12 Tableau des utilisateurs et groupes

### 3.2 Mise en place de la Sécurité

La mise en place de la sécurité se fait directement à la configuration des différents appareils de l'infrastructure. Les mots de passes seront soit générés par un gestionnaire de mot de passe soit fonctionneront via un code par exemple Kicroit24-[Nom de l'appareil]\_MdP\$ ce qui garantit une bien meilleure sécurité.

Les Switchs, le routeur et les access point doivent avoir un mot de passe pour passer en mode Enable. Les lignes Vty doivent être sécurisées et l'accès via le port console doit avoir un mot de passe. De plus les ports non utilisés des switchs doivent être verrouillés manuellement pour éviter toute intrusion sur le réseau. Les Wifis fournis par les Access Points doivent avoir un mot de passe crypté. Les ordinateurs et le serveur doivent avoir un mot de passe. Pour les utilisateurs les permissions NTFS permettent de limiter les données auxquelles ils auront accès afin de limiter les fuites.

Le firewall s'occupe de la sécurité des connexions. Chaque réseau est par défaut séparé. Le réseau principal ne doit pouvoir communiquer qu'avec le réseau du routeur, celui de l'imprimante et celui du NAS et les deux réseaux de Lausanne. Uniquement les protocoles utilisés par ces derniers sont autorisés. Ainsi le Réseau principal ne peut pas ping les autres par exemple. Les réseaux des imprimantes ne peuvent communiquer qu'avec le réseau principal, de même pour le réseau du NAS. Enfin des règles concernant le trafic entrant scannent les emails et des règles concernant le trafic limitent les sites auxquels les internautes peuvent accéder.

Pour ce projet comme le GitHub est public les mots de passes sont gérés grâce à keepass<sup>6</sup> pour éviter de donner accès aux mots de passes au monde entier. L'application est portable, il suffit de télécharger le fichier et elle est directement utilisable. Elle crée une base de données contenant les mots de passes des différents appareils. Le mot de passe de la database a été transmis par mail aux experts et au chef de projet.

<sup>6</sup> <https://keepass.info/>

## 4 Réalisation et mise en service

### 4.1 Description des tâches effectuées

La réalisation de ce projet s'est faite en plusieurs parties entremêlées. En effet certains éléments ont vu leur configuration changer au fur et à mesure des avancées du projet. Par exemple le firewall a été installé une première fois puis sa configuration a été modifiée pour permettre aux autres éléments de l'infrastructure de fonctionner correctement. Pour des raisons de clarté les éléments rapportés dans ce rapport sont structurés suivant le type d'appareil qui est mis en service et non de manière chronologique. Les différentes procédures d'installation seront mises à jour au fur et à mesure. Cette rubrique contient donc l'installation et la configuration des routeurs, du firewall, des serveurs, des switchs, des pcs, des imprimantes, du nas et des access point.

#### 4.1.1 Rufus

Rufus<sup>7</sup> est un outil gratuit qui permet de faire des clés bootables avec une image iso à choix. Il n'exige pas d'avoir accès à l'image iso au préalable. Après avoir vérifié qu'il n'y a rien d'important sur la clé USB et téléchargé l'image iso il suffit de sélectionner le périphérique sur lequel créer l'image de boot et de sélectionner l'iso à mettre dessus. Rufus fait lui-même les checks de faisabilité. En cliquant sur démarrer l'image la clé est créée. Cette opération détruit toutes les données déjà existantes sur la clé.

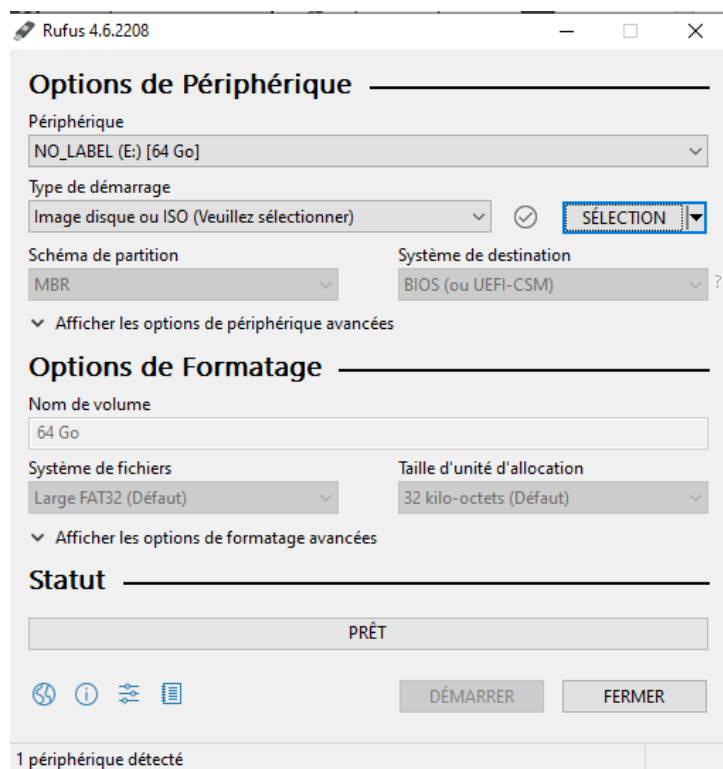


Figure 13 Création d'une clé bootable via RUFUS

<sup>7</sup> [https://rufus.ie/fr/#google\\_vignette](https://rufus.ie/fr/#google_vignette)

### 4.1.2 Putty

Putty<sup>8</sup> est une application qui permet de se connecter en SSH ou via un câble Serial à un appareil. Dans le projet il est utilisé à de multiples reprises pour la configuration de différents appareils. Pour ne pas avoir à expliquer à chaque fois les manipulations effectuées voici une marche à suivre pour se connecter à un appareil.

Via SSH :

Lors de l'ouverture de Putty il faut entrer l'adresse IP de la machine cible et le port 22 (port par défaut pour le ssh) puis appuyer sur « open ».

Via Serial :

Vérifier que le câble sériel soit bien connecté à la machine à configurer, sélectionner l'option sériel et cliquer sur « open ».

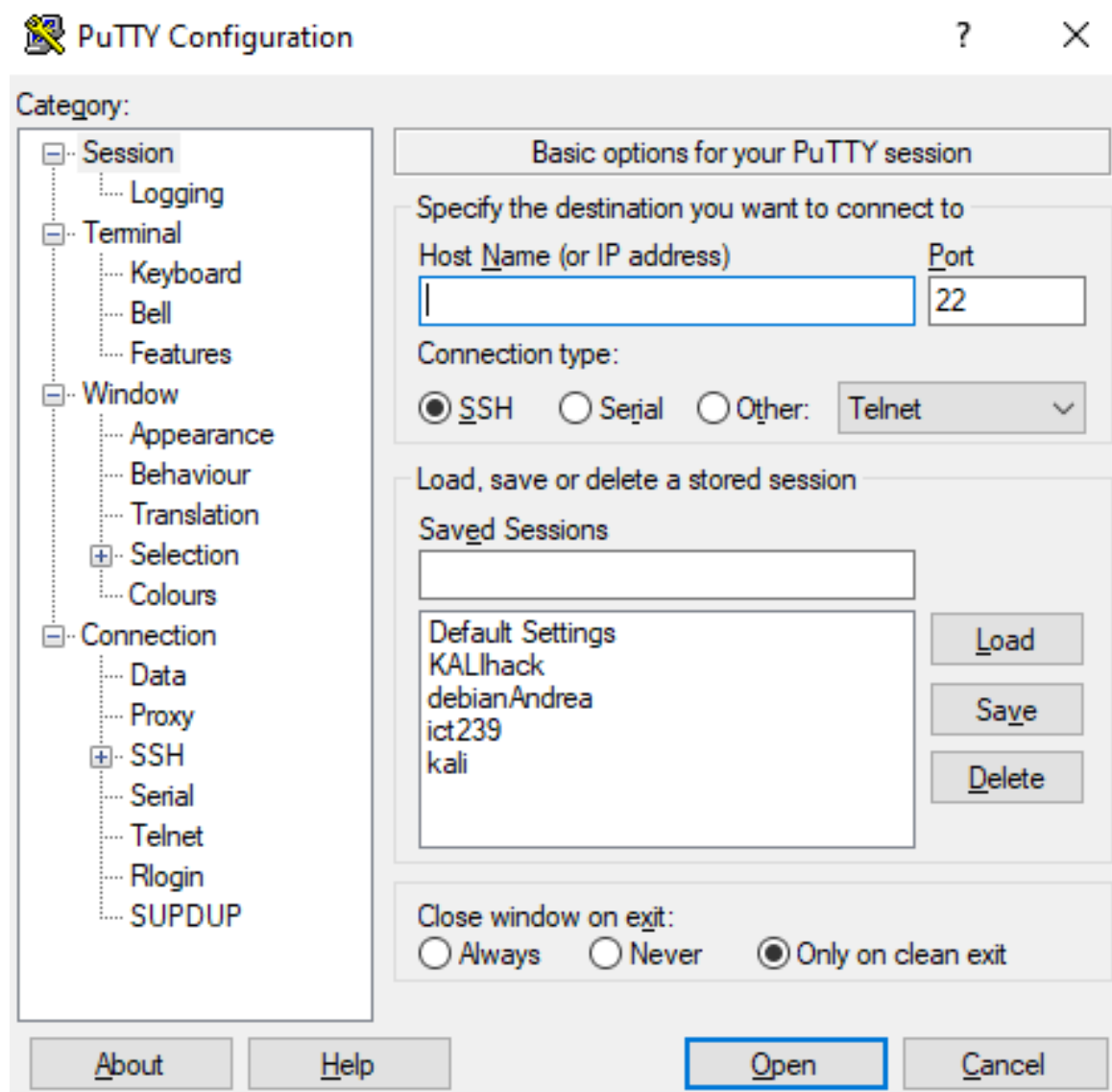


Figure 14 Connexion avec PUTTY

<sup>8</sup> <https://www.putty.org/>

### 4.1.3 Poste fixe

Pour ce projet un poste fixe est fourni. Il faut premièrement installer l'os. En connectant la clé bootable et en la sélectionnant dans le boot menu on accède à l'installation classique de Windows. Pour ce projet il n'y a pas de clé de produit, la région à sélectionner est france et les disques doivent être complètement formatés pour repartir à zéro. Une fois l'installation initiale effectuée l'ordinateur redémarre et on passe à la configuration du Windows. Attention à bien sélectionner le clavier suisse et à dire non à toutes les options que propose windows. Enfin il faut créer un premier utilisateur que l'on va nommer Admin avec comme mot de passe Pa\$\$wOrd. Une fois le serveur installé il faut rentrer l'ordinateur dans le domaine et modifier le nom de l'ordinateur. Pour ce faire il faut aller dans « Renommer ce PC avancé>Nom de l'ordinateur>modifier ». Après avoir écrit le nouveau nom de l'ordinateur selon la convention de nommage il faut redémarrer l'ordinateur et revenir au même endroit pour sélectionner « membre d'un domaine », écrire le nom de domaine « Kikroit.com » et se connecter via un compte présent dans l'AD. Finalement il faut vérifier que les paramètres IPv4 soient bien sur DHCP via centre de réseau et *partage>modifier les options d'adaptateur> (sur la carte réseau) propriétés>Protocol internet ipv4*. Putty doit aussi être installé pour pouvoir configurer les prochains appareils

### 4.1.4 Imprimante Bullet

La configuration de l'imprimante se fait sous *network>Wired Lan>TCP/IP*. Il faut mettre une adresse en statique : 192.168.40.10/24 gateway : 192.168.40.1. Le nom de l'imprimante doit aussi être changé sous « node name » pour correspondre aux conventions de nommages (Kicroit-BU-Printer1). L'imprimante ne demande pas plus d'installation.

### 4.1.5 Switch Bullet

La configuration de switch se fait via le port sérial. La première étape est de remettre à zéro le switch. Pour se faire il suffit de maintenir le bouton de reset pendant 10 secondes au démarrage du switch.

Voici la configuration du switch 1 qui interconnecte les ordinateurs et le serveur :

```
ena

conf t

hostname Kicroit-BU-Switch1

enable secret Kicroit24-Switch1_MdP$

Line console 0
password Kicroit24-Switch1_MdP$
Login
exit
```

```
line vty 0 4
password Kicroit24-Switch1_MdP$
login
transport input ssh
exit

service password-encryption

no ip domain-lookup

banner motd # Switch Kicroit acces interdit aux personnes non autorises #

int range fa0/6-8
shutdown
end
write
```

#### 4.1.6 Routeur Bullet

Premièrement on remet le routeur à zéro. Comme je possède les accès au mode privilégié il est possible d'utiliser « write erase » pour supprimer la configuration de démarrage et « reload » pour valider les changements.

Une fois cela fait voici les commandes pour configurer le routeur en respectant l'analyse faite :

```
enable

conf t

hostname Kicroit-BU-Router1

enable secret Kicroit24-Router1_MdP$

Line console 0
```

```
password Kicroit24-Router1_MdP$
Login
exit

line vty 0 15
password Kicroit24-Router1_MdP$
login
transport input ssh
exit

service password-encryption

no ip domain-lookup

banner motd # Routeur Kicroit acces interdit aux personnes non autorises #

! configuration des routes statiques
ip route 192.168.20.0 255.255.255.0 192.168.10.2
ip route 192.168.50.0 255.255.255.0 192.168.0.2
ip route 192.168.60.0 255.255.255.0 192.168.0.2

! phase 1 configuration de l'IKE
crypto isakmp policy 10
encr aes                        ! algorithme de chiffrement AES
hash sha                       ! algorithme de hachage SHA
authentication pre-share
group 2                         ! Groupe Diffie-Hellman
lifetime 86400
exit
```



```
! clé pré-partagée pour l'authentification de la Phase 1
crypto isakmp key VPN_KEY address 192.168.0.2

! Phase 2 Création du tunnel
crypto ipsec transform-set TRANS esp-aes esp-sha-hmac
exit

! Phase 2 association du transform set à une crypto map
crypto map VPNMAP 10 ipsec-isakmp
set peer 192.168.0.2
set transform-set TRANS
match address 101
exit

int G0/0
ip address 192.168.0.1 255.255.255.252
crypto map VPNMAP
no shutdown
exit

int g0/1
ip address 192.168.10.1 255.255.255.252
no shutdown
exit

! Liste de contrôle d'accès définissant le trafic chiffré
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.60.0 0.0.0.255 192.168.20.0 0.0.0.255
end
write
```

#### 4.1.7 Firewall

En premier il faut remettre à zéro le firewall. Comme on possède déjà les identifiants de connexion du firewall il est possible de le remettre à zéro avec des lignes de commandes en mode privilégié. « Exécute factoryreset » permet d'effacer toute la configuration et « execute reboot » redémarre le firewall. Lorsque le firewall est remis à zéro la configuration peut commencer. Le nouvel identifiant est admin et il n'y a pas de mot de passe. La configuration se fera via l'interface visuelle mais il faut pour cela configurer une adresse ip<sup>9</sup> sur un port pour pouvoir se connecter via un navigateur au firewall. Voici les commandes à utiliser :

```
config system interface
edit wan1
set mode static
set ip 192.168.10.2 255.255.255.252
set allowaccess ping https ssh http
next
end

config router static
edit 1
set gateway 192.168.10.1
set device wan1
next
end

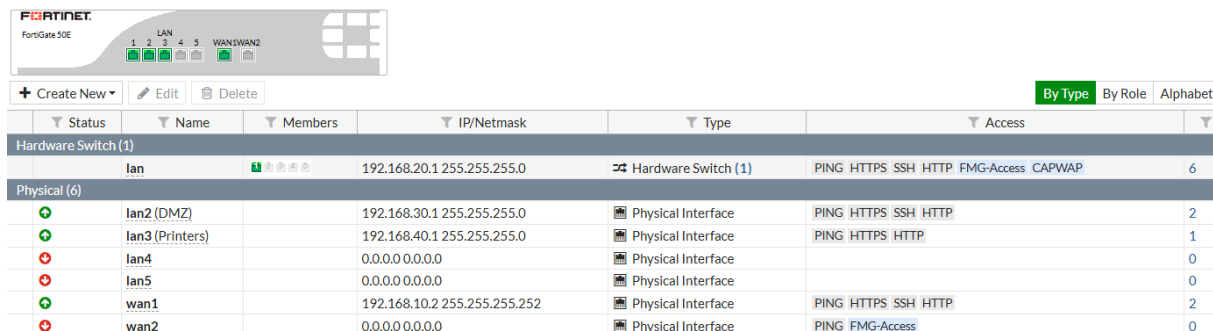
config system global
set hostname Kicroit-BU-Firewall1
end
```

Si la configuration a bien été effectuée il est maintenant possible de se connecter grâce à un navigateur et à l'adresse IP du Wan1. La première chose à faire lors de la connexion est de modifier l'utilisateur principale sous *System>Administrateur>create new*. Le nom est Kicroit, le mot de passe respecte la convention de mot de passe et il doit être super admin. De plus, l'ancien admin doit être supprimé pour éviter de laisser une faille béante dans la sécurité.

---

<sup>9</sup> [https://help.fortinet.com/fdb/5-0-0/html/source/tasks/t\\_network\\_configuration\\_cli.html](https://help.fortinet.com/fdb/5-0-0/html/source/tasks/t_network_configuration_cli.html)

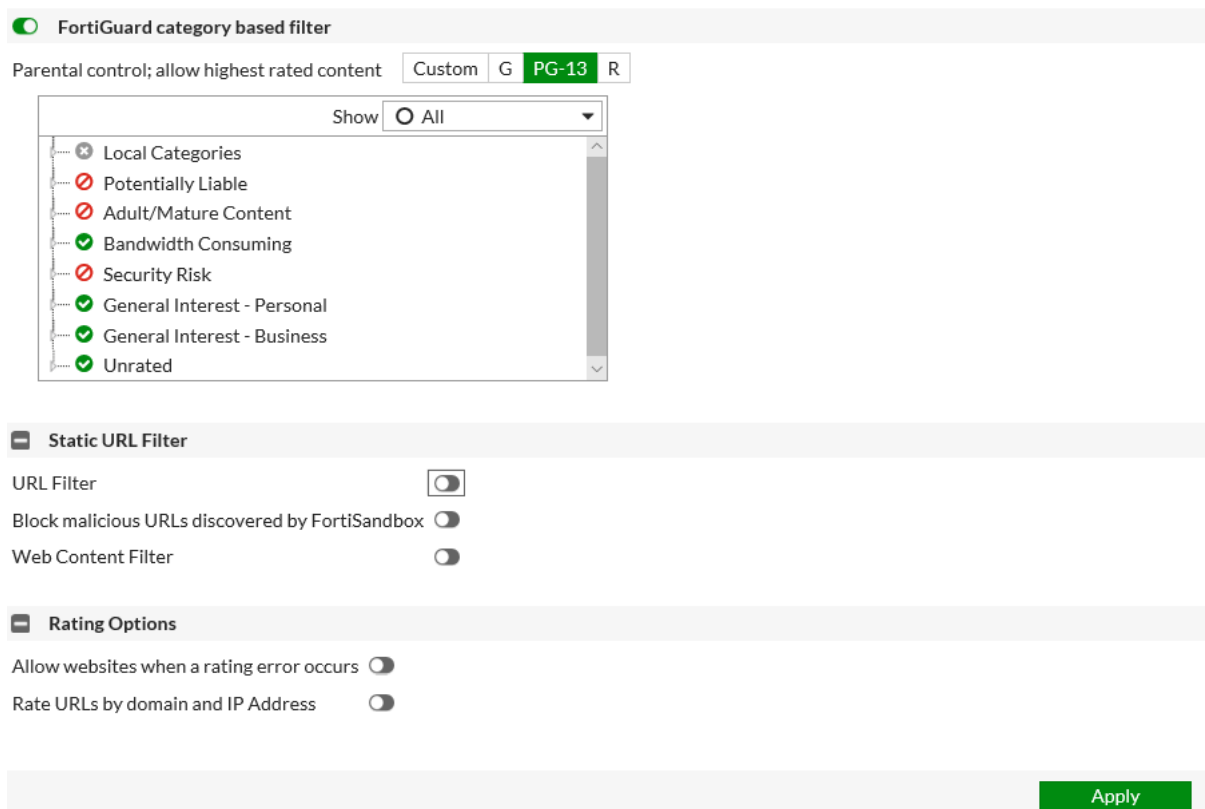
Maintenant que les utilisateurs sont gérés il faut configurer les interfaces sous *Network>interfaces* selon le plan d'adressage. Pour chacune d'entre elle il faut renseigner : Le nom et l'alias, les interfaces membres, l'ip, le masque et les protocoles qu'elles acceptent. Attention au protocole, s'il n'est pas présent aucune police d'aucune sorte ne permettra d'effectuer l'action voulue. La configuration finale donne ce résultat :



Status	Name	Members	IP/Netmask	Type	Access	
<b>Hardware Switch (1)</b>						
	lan		192.168.20.1 255.255.255.0	Hardware Switch (1)	PING HTTPS SSH HTTP FMG-Access CAPWAP	6
<b>Physical (6)</b>						
+	lan2 (DMZ)		192.168.30.1 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	2
+	lan3 (Printers)		192.168.40.1 255.255.255.0	Physical Interface	PING HTTPS HTTP	1
-	lan4		0.0.0.0 0.0.0.0	Physical Interface		0
-	lan5		0.0.0.0 0.0.0.0	Physical Interface		0
+	wan1		192.168.10.2 255.255.255.252	Physical Interface	PING HTTPS SSH HTTP	2
-	wan2		0.0.0.0 0.0.0.0	Physical Interface	PING FMG-Access	0

Figure 15 Résumé des interfaces

Il est aussi important de mettre en place les filtres par catégorie pour limiter l'accès à certains sites au sein de l'entreprise. Ils se trouvent sous *Security profiles>Web Filter* :



☒ FortiGuard category based filter

Parental control; allow highest rated content   Custom   G   **PG-13**   R

Show: ☐ All

- Local Categories
  - ☒ Potentially Liable
  - ☒ Adult/Mature Content
  - ☒ Bandwidth Consuming
  - ☒ Security Risk
  - ☒ General Interest - Personal
  - ☒ General Interest - Business
  - ☒ Unrated

**Static URL Filter**

URL Filter: ☐

Block malicious URLs discovered by FortiSandbox: ☐

Web Content Filter: ☐

**Rating Options**

Allow websites when a rating error occurs: ☐

Rate URLs by domain and IP Address: ☐

**Apply**

Figure 16 filtres pour le WEB

La dernière étape de la configuration du firewall concerne les polices. Sans elles le trafic entre les différents réseaux ne peut pas se faire ou il se fait très mal. Actuellement les polices sont basiques et ne visent qu'à permettre tout le trafic sans faire de distinction entre les protocoles. Pour ajouter une police il faut aller sous *Policy and Object>IPv4 Policies>new*. Il faut ensuite renseigner les champs : nom, incoming

interface, outgoing interface, source, destination, Service et Action. Dans ce projet source Destination et service sont tous sur All. Voici le résultat :

+ Create New Edit Delete Q Policy Lookup Q Search										Interface Pair View	By Ser
Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	
DMZ (lan2) - lan (1 - 1)											
1	dmztolan	all	all	always	ALL	ACCEPT	Enabled	UTM		212.02 kB	
lan - DMZ (lan2) (2 - 2)											
2	DMZ	all	all	always	ALL	ACCEPT	Enabled	UTM		1.09 GB	
lan - Printers (lan3) (3 - 3)											
3	Connexion imprimantes	all	all	always	ALL	ACCEPT	Enabled	UTM		2.51 MB	
lan - wan1 (4 - 4)											
4		all	all	always	ALL	ACCEPT	Enabled	UTM		147.08 kB	
Implicit (5 - 5)											
5	Implicit Deny	all	all	always	ALL	DENY	Disabled			10.45 kB	

**Figure 17 Règles du pare-feu**

### 4.1.8 Premier serveur

Le serveur étant un point conséquent de l'installation il sera séparé en sous catégories suivant les services installés. Pour l'installation d'un nouveau service la démarche étant toujours la même elle est décrite ici pour éviter la redondance.

Pour installer un nouveau service ou rôle sur windows serveur 2022 il faut aller dans rôle et fonctionnalité > sous « rôles de serveurs » sélectionner le rôle ou la fonctionnalité voulue et vérifier qu'il s'installe sur le bon serveur. Il n'y a pas de spécificité dans l'installation. Après avoir installé le rôle il faut redémarrer le serveur.

#### Installation de Windows Serveur 2022

Pour pouvoir installer l'iso il faut une clé bootable avec l'iso dessus que l'on fait via Rufus. Après avoir sélectionné l'option de boot sur usb l'installation de Windows serveur se fait sans particularité. Si les disques ne sont pas vierges il faut les formater.

Pour la configuration ip la procédure est la même que pour le pc fixe mais l'adresse ip doit être fixe : 192.168.20.20/24, gateway 192.168.20.1.

Il faut ensuite créer un disque F : sous « créer et formater des partitions de disque dur » > créer un nouveau volume simple de 1 To.

#### DNS

Pour le DNS il n'y a pas grand-chose à faire. Après avoir installé le rôle la zone directe et indirecte se feront toute seule une fois l'AD installé.

#### DHCP

Après avoir installé le rôle on crée une nouvelle étendue en allant sur gestionnaire DHCP>nouvelle étendue ipv4. Les informations entrées sont les suivantes

Nom : Kicroit-Bullet

Pool d'adresses : 192.168.20.100 - 192.168.20.254 avec un masque 255.255.255.0

Gateway : 192.168.20.1

Serveur DNS : 192.168.20.20 et 192.168.20.21

Nom de domaine DNS : Kicroit.com

On crée une autre étendue DHCP pour le site de Lausanne avec les informations suivantes

Nom : Kicroit-Lausanne

Pool d'adresses : 192.168.60.100 - 192.168.60.254 avec un masque 255.255.255.0

Gateway : 192.168.60.1

Serveur DNS : 192.168.20.20 et 192.168.20.21

Nom de domaine DNS : Kicroit.com

## AD DS

Après avoir installé le rôle on configure le Domain contrôleur, il faut donc promouvoir ce serveur en contrôleur de domaine. Lors de la configuration de déploiement, sélectionner Ajouter une nouvelle forêt>nom de domaine racine Kicroit.com. Sous « Options du contrôleur de domaine il faut ajouter le mot de passe Pa\$\$w0rd pour le mode de restauration des services d'annuaires. Le reste de la configuration n'est pas nécessaire il suffit de cliquer sur suivant. Une fois le redémarrage fait il faut accepter le DHCP dans le domaine et « UP » l'étendue ipv4 pour qu'il puisse à nouveau donner des Adresses IP.

Lorsque le domaine est créé on ajoute les différents groupes et utilisateurs prévus par la conception. Sous « Utilisateurs et ordinateurs Active Directory » il faut cliquer droit « ajouter » dans user et choisir soit groupe soit utilisateur. Pour les utilisateurs voici un exemple de paramétrage, ils suivent tous la même logique et le mot de passe est Pa\$\$w0rd.

The image shows two side-by-side screenshots of the 'Nouvel objet - Utilisateur' (New Object - User) dialog box in Windows Server. Both windows are titled 'Créer dans : Kicroit.com/Users'.

The left window shows the following fields filled out:

- Prénom : Marie
- Initiales : (empty)
- Nom : Martin
- Nom complet : Marie Martin
- Nom d'ouverture de session de l'utilisateur : Marie.Martin
- Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : KICROIT\Marie.Martin

The right window shows the following fields and options:

- Mot de passe : (masked with dots)
- Confirmer le mot de passe : (masked with dots)
- Options (all unchecked):
  - ☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
  - ☐ L'utilisateur ne peut pas changer de mot de passe
  - ☐ Le mot de passe n'expire jamais
  - ☐ Le compte est désactivé

Both windows have navigation buttons at the bottom: '< Précédent', 'Suivant >', and 'Annuler'.

**Figure 18** Création d'un utilisateur

Voici la création d'un groupe, on en fait de même pour Marketing.

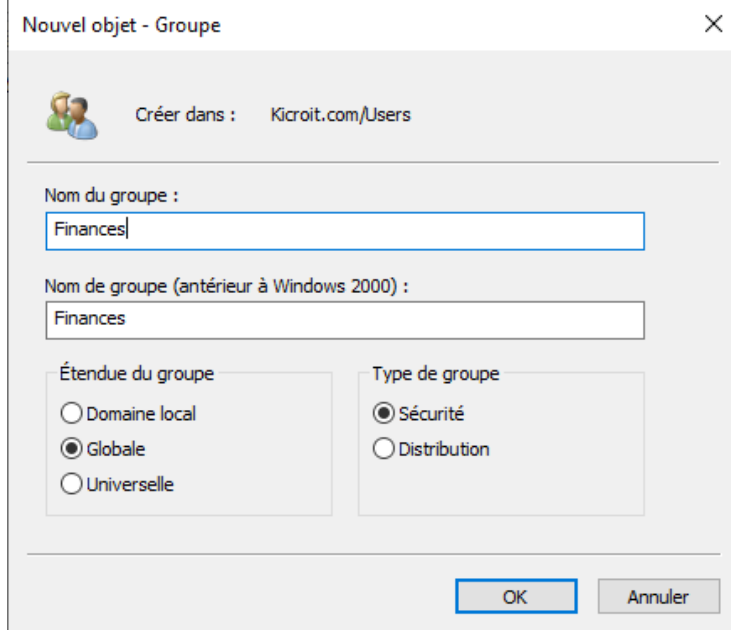


Figure 19 Création d'un groupe

La dernière étape consiste à mettre les utilisateurs dans les groupes comme suit :

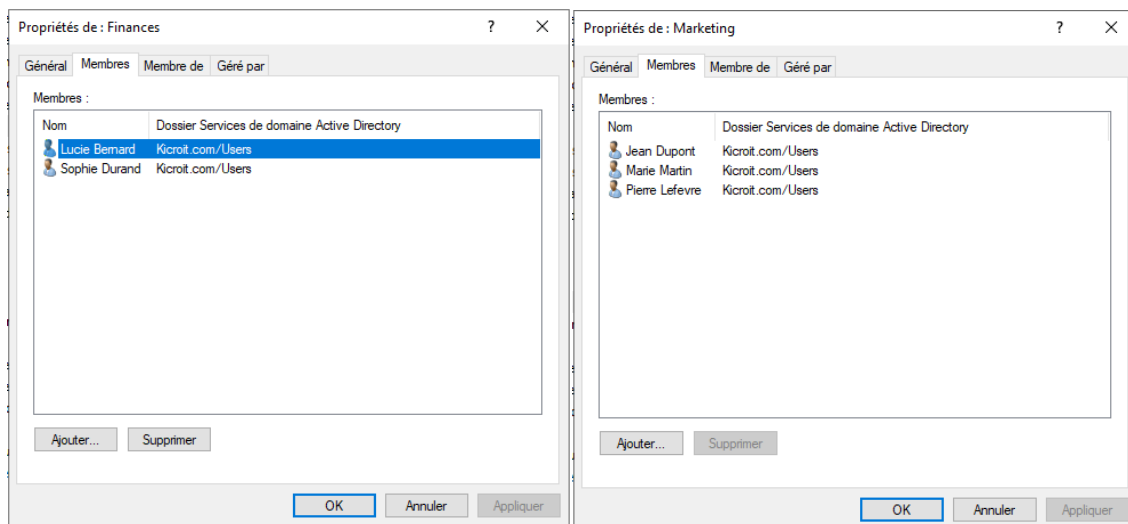
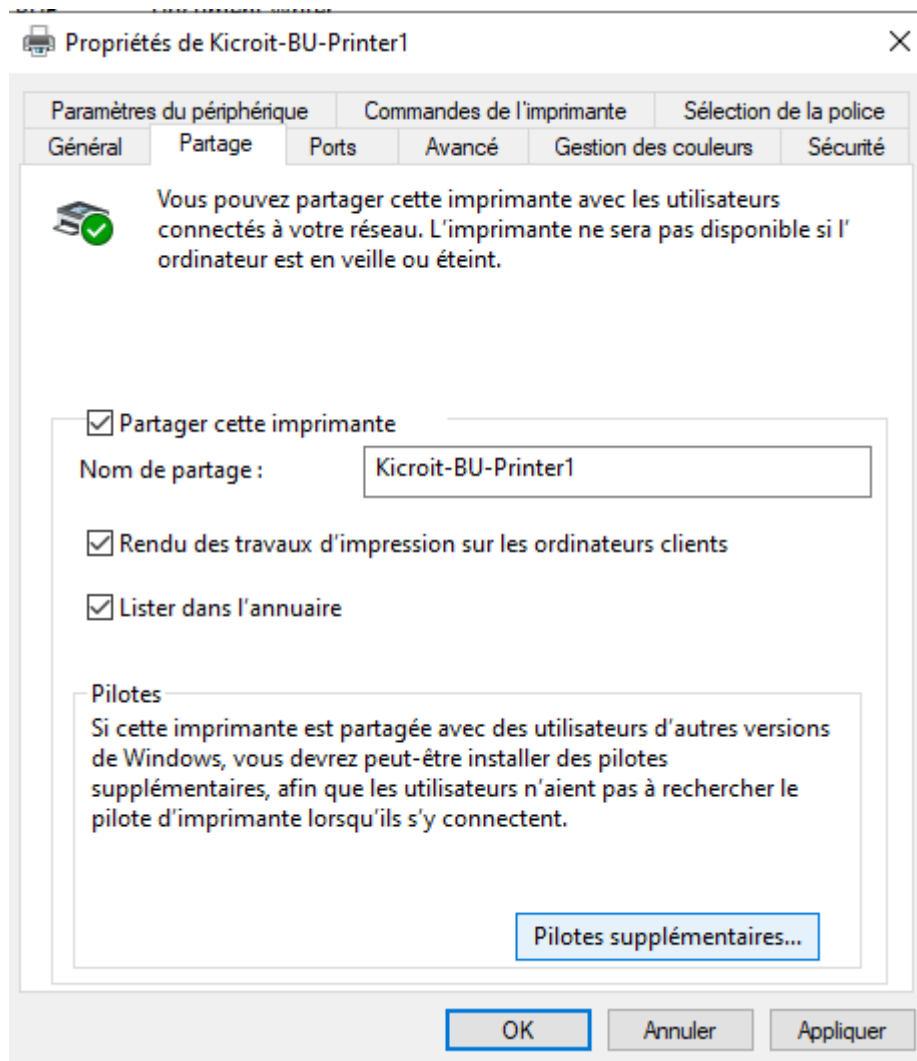


Figure 20 Utilisateurs dans les groupes

Après avoir installé les services d'impression il faut installer l'imprimante Via le panneau de configuration>périphériques et imprimantes>imprimantes>nouvelle imprimante en rentrant l'adresse ipv4 de l'imprimante. Comme l'imprimante assez ancienne il faut impérativement installer les drivers. Ils sont téléchargeables sur le site de Brother<sup>10</sup> en sélectionnant le modèle de l'imprimante (DCP-L8400CDN). Au moment d'ajouter l'imprimante il suffit alors de sélectionner disque fourni et de prendre les drivers téléchargés.

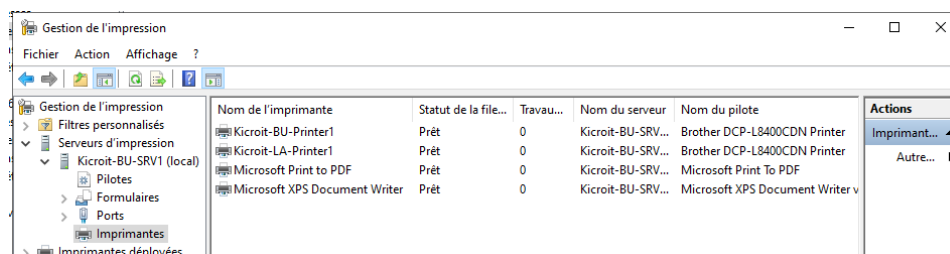
<sup>10</sup><https://www.brother.ch/fr-ch/support/dcp-l8400cdn/downloads?srsId=AfmBOoqwRtN1MVaA4cSWpiNEBUx-pzJqTl9Vpo4oOZZwUyKT-yRHsCV3>

Lorsque l'imprimante est installée elle apparaît dans « gestion de l'impression ». Il faut donc la partager comme suit :



**Figure 21 Partage imprimante**

Une fois cela fait on vérifie dans services d'impression que l'imprimante apparaît bien et que les drivers sont aussi dans le partage. La procédure est la même pour l'imprimante de Lausanne. Voici le résultat final



**Figure 22 Service d'impression fini**

## Serveur de Fichier

Dans le lecteur F : on crée un dossier « Serveur de fichier » à l'intérieur duquel on crée deux dossiers « Marketing » et « Finances ». Il y a plusieurs possibilités pour configurer le partage des fichiers et les permissions, on a choisi de passer par l'explorateur de fichier Windows. Sur « Serveur de fichier » > propriétés > partage > Partage avancé on

gère les autorisations de partage. On ne laisse que « admins du domaine » qui auront accès au contrôle total et « utilisateurs du domaine » qui auront modifier + lecture. Sur les trois dossiers il faut maintenant gérer les permissions NTFS sous propriétés>sécurité en se référant à la conception. Voici le résultat.

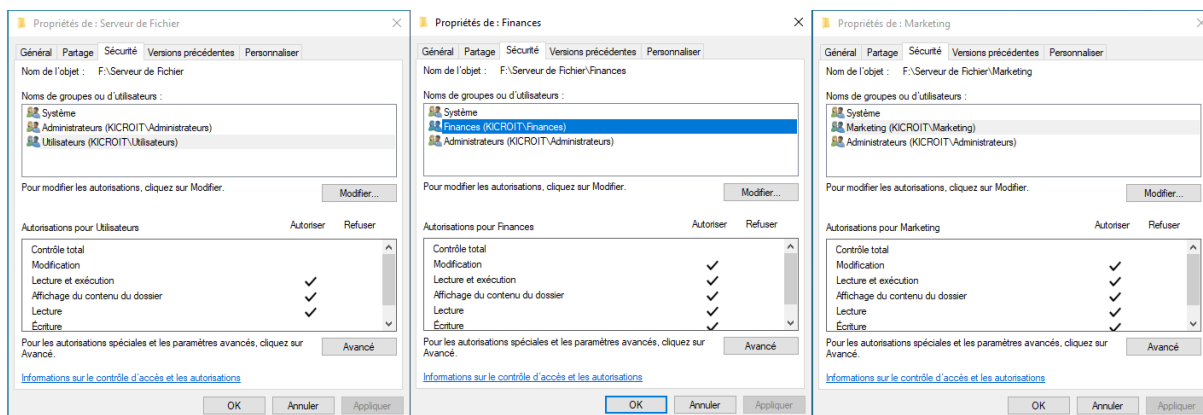


Figure 23 Permissions NTFS

Système et Administrateurs ont le contrôle total sur les dossiers. Après cela le partage est déjà accessible pour les utilisateurs mais il faut encore configurer un lecteur mappé pour éviter aux utilisateurs de devoir aller le chercher via le chemin ou sous réseau. Pour cette partie la délégation DFS détaillée sous serveur redondant est déjà en place. Sous Gestion des Stratégies de groupes > Kicroit.com on crée une nouvelle GPO qu'on lie à Kicroit.com. Dans celle-ci sous Configuration utilisateur > Préférences > Paramètres Windows> mapper des lecteurs on crée un nouveau mappage comme ceci :

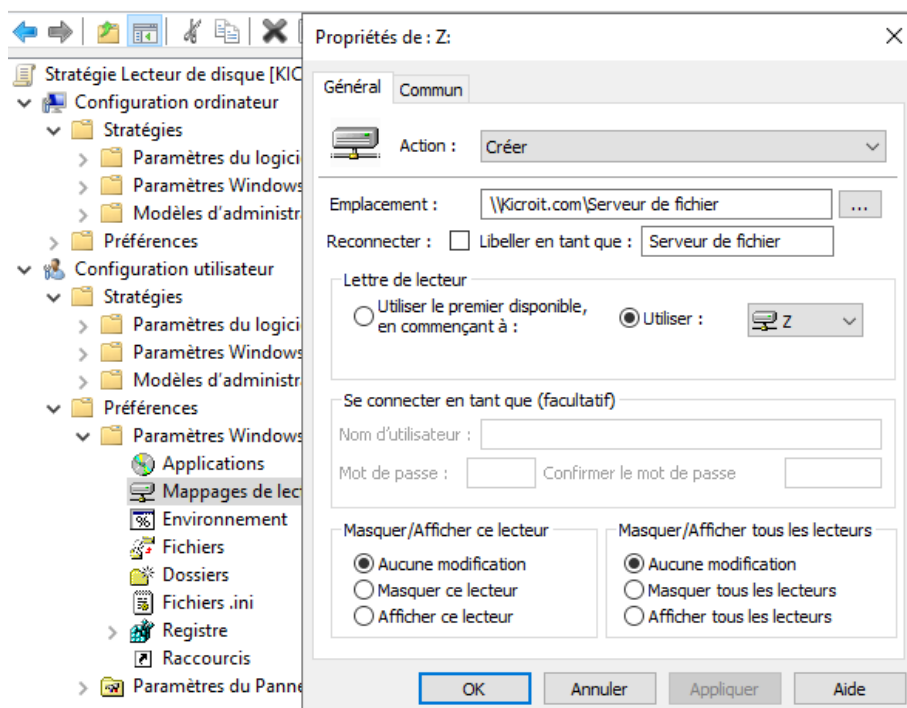


Figure 24 GPO disque

Après cela un lecteur Z : apparaît sous chaque poste connecté au domaine.



#### 4.1.9 Serveur redondant

L'installation initiale se fait de la même manière que pour le premier serveur. L'adresse IPv4 fixe à renseigner est la 192.168.20.21 avec 192.168.20.1 pour passerelle et 127.0.0.1 / 192.168.20.20 comme DNS. Attention à bien désactiver la deuxième interface pour éviter de recevoir un APIPA et de risquer des effets de bords. Sous « renommer ce pc avancé » on le renomme Kicroit-BU-SRV2 et on l'insère dans le domaine avec un compte administrateur.

#### Redondance des services

Le premier rôle à installer est l'AD DS en suivant toujours la même procédure. Après l'avoir installé on le configure en sélectionnant « Ajouter un contrôleur de domaine à un domaine existant » et en renseignant Administrateur Pa\$\$w0rd pour l'identifiant. Le serveur va encore demander le mot de passe de restauration des services d'annuaire (Pa\$\$w0rd) et pour le reste cliquer suivant est suffisant. Une fois cela fait le rôle AD DS et DNS se configurent tout seuls en répliquant le premier contrôleur de domaine.

Pour le rôle DHCP on configure un basculement DHCP. Après avoir installé le rôle sur le serveur redondant il faut les configurer sur le premier serveur. Sous chaque étendue DHCP il faut sélectionner « configurer un Basculement DHCP » et sélectionner comme serveur partenaire le serveur redondant kicroit-bu-srv2. Pour le reste de la configuration on peut laisser tel quel le nom de la relation, le mode équilibrage de la charge et les pourcentages. On renseigne le Secret partagé Pa\$\$w0rd et si tout à été configuré correctement on obtient ce résultat :

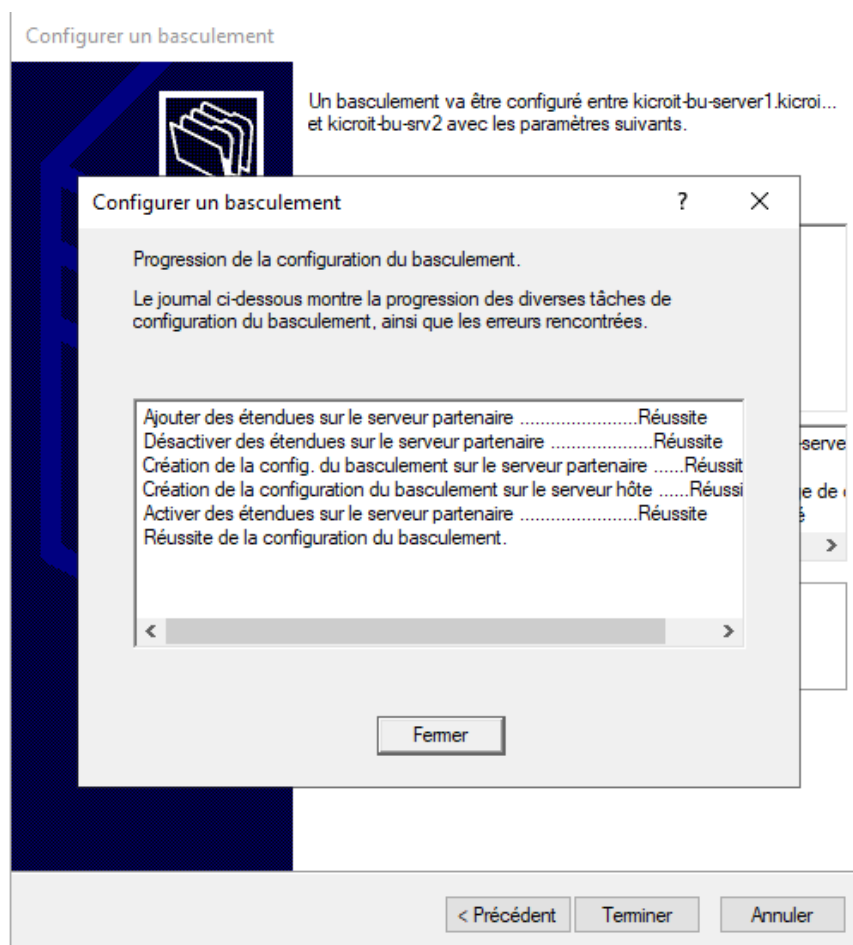
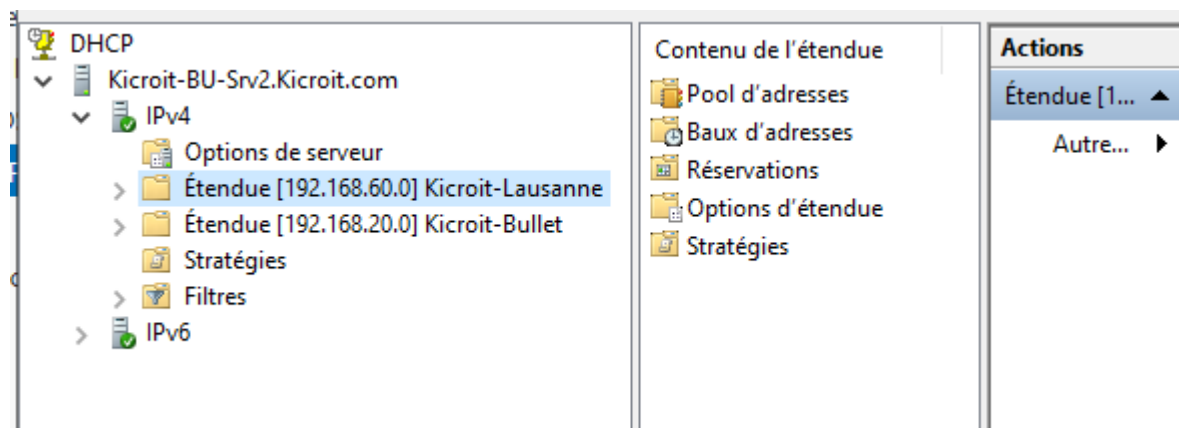


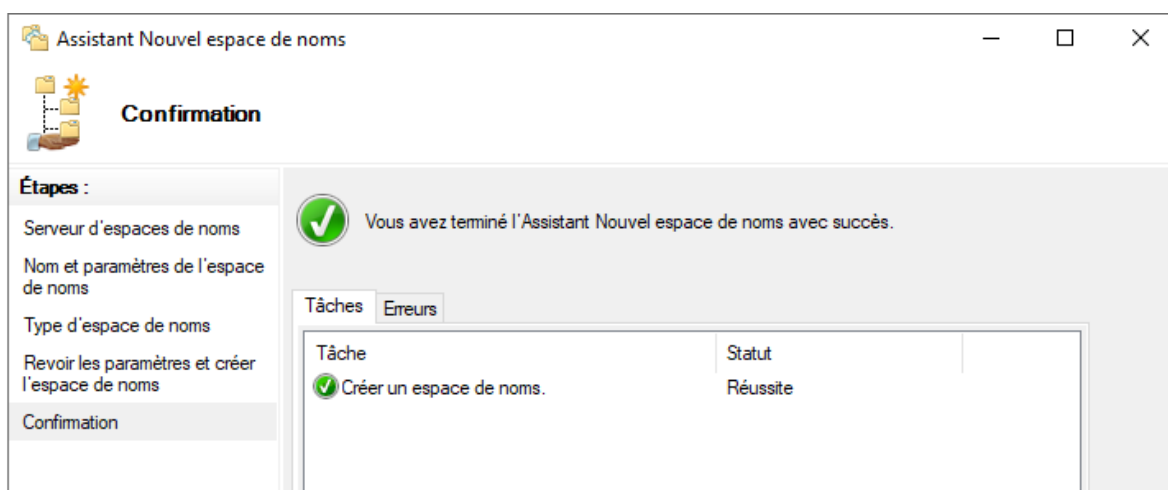
Figure 25 Basculement DHCP

Lorsque les deux étendues sont faites voici le résultat sur le serveur redondant :



**Figure 26 Etendue DHCP serveur redondant**

Pour le rôle de serveur de fichier la configuration se fait sur le premier serveur. Dans les rôles sous « services de fichiers et isCSI » on installe « Espaces de nom DFS » et « réplication DFS ». L'espace de nom permet de créer un pointeur unique qui pointe les deux serveurs et la réplication permet de synchroniser les dossiers en temps réel sur les deux serveurs. Lorsque les rôles sont installés L'outil d'administration Gestion des fichiers partagés DFS est disponible. Dedans on crée un nouvel espace de nom sur le serveur kicroit-bu-srv1. On renseigne le nom de l'espace de nom comme étant « serveur de fichier » ce qui permet de garder les droits précédemment faits. Il faut s'assurer que l'espace de nom est géré par l'active directory et on peut valider la création :

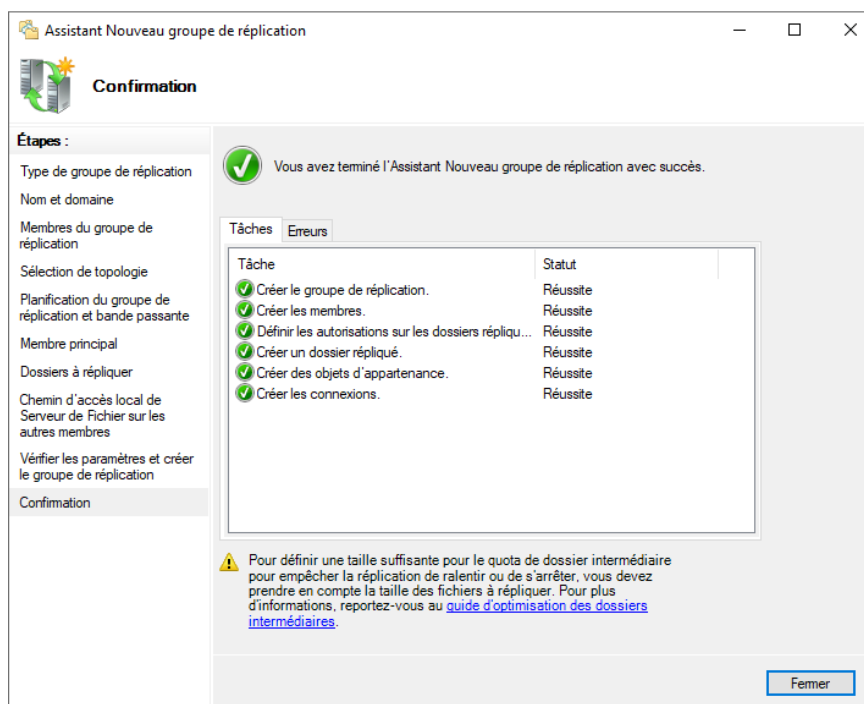


**Figure 27 Création espace de nom**

Une fois l'espace de nom créé, sous « actions », on ajoute le deuxième serveur via « ajouter un serveur d'espace de noms » en renseignant l'adresse du serveur kicroit-bu-srv2. Cette action crée le dossier « serveur de fichier » dans le serveur redondant mais il faut encore modifier les options de partages pour le faire correspondre au dossier présent sur le serveur 1.

Pour assurer la synchronisation des données contenue dans notre dossier on crée une réplication DFS. Sous « Réplication DFS » on en fait une nouvelle. On renseigne le nom du groupe, ici « Serveur de fichier », et on ajoute les deux serveurs au groupe de réplication. La topologie est en maille pleine comme on a que deux serveurs. Pour la

planification on choisit de répliquer en continu comme les serveurs sont en local. Le membre principal est le serveur de fichier 1. On choisit ensuite les noms de dossiers à répliquer donc F:\Serveur de fichier sur le serveur 1 et on sélectionne l'endroit où le répliquer donc le dossier créé via l'espace de nom sur le serveur 2. Lorsque l'on crée voici ce qu'on obtient :



**Figure 28 Création réplication DFS**

Après quelques minutes pour la synchronisation les dossiers « Marketing » et « Finances » sont répliqués sur le serveur de backup et s'ils sont modifiés d'un côté comme de l'autre la modification se transmet aux deux.

Il n'est malheureusement pas possible de répliquer le rôle du serveur d'impression sans utiliser de virtualisation pour mettre les serveurs en HA. Le rôle ne sera donc pas redondant

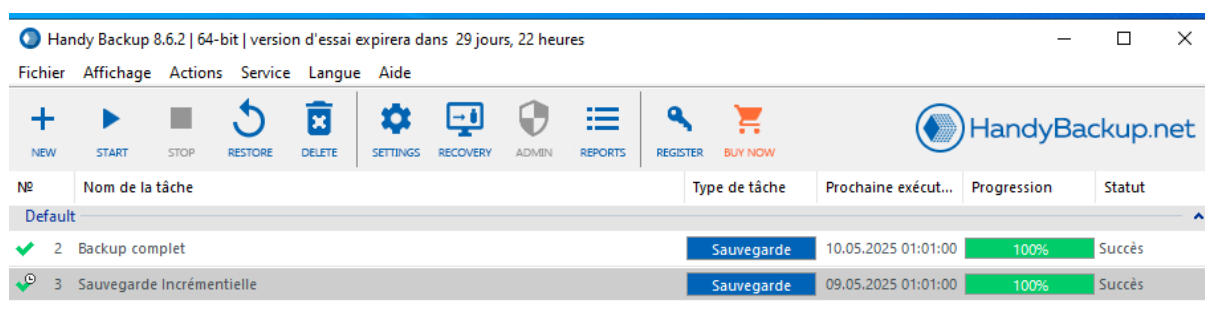
#### 4.1.10 Nas

Pour installer et configurer le NAS nous aurons besoin de l'intégrer dans un premier temps au réseau du serveur pour pouvoir lui donner une adresse via DHCP. Le NAS possède deux ports Ethernet, nous allons pouvoir connecter le premier directement au firewall dans le port dédié et le deuxième au switch du réseaux du serveur ainsi nous allons pouvoir le configurer via l'interface web. En premier lieu il faut remettre à zéro le NAS. Pour se faire il suffit de cliquer sur le bouton reset jusqu'à entendre un bip puis de recliquer sur ce même bouton jusqu'à entendre 3 bips. Ensuite, en utilisant le Wizard, on fait la première installation. On crée un utilisateur Nommé Kicroit (mdp : Pa\$\$wOrd) et on renomme le NAS Kicroit-BU-Nas1. On configure l'adresse IPv4 de l'autre interface avec l'IP fixe 192.168.30.10 et on peut débrancher le câble relié au serveur. Il faut ensuite initialiser les disques en raid 5. Pour ce faire : Gestionnaire de stockage>volume>nouveau volume et sélectionner la totalité de l'espace disponible.

Une fois les volumes initialisés il faut configurer la cible iSCSI pour pouvoir connecter le disque au serveur. On va dans gestionnaire de stockage>iSCSI LUN>créer. On le nomme iSCSI Nas, on sélectionne le volume précédemment créé et on sélectionne « créer un nouveau iSCSI target ». On laisse l'IQN classique et on peut valider la

création du LUN. Sur l'ordinateur on utilise l'initiateur ISCI avec l'IP du NAS pour pouvoir connecter le disque. Une fois cela fait on met le disque en ligne et on l'initialise le disque dans Gestionnaire de disque. On crée ensuite un nouveau volume simple avec la lettre E:.

La dernière étape est de télécharger et installer Handy Backup pour pouvoir organiser les sauvegardes. Une fois l'application lancée on crée une nouvelle règle en cliquant sur « new ». On sélectionne « tâche de sauvegarde » et dans l'onglet « sélectionner les données » on prend le dossier Serveur de fichier. Pour l'emplacement où sauvegarder les données on sélectionne le disque E : ajouté précédemment. On choisit ensuite le type de sauvegarde pour la première règle « complète ». On finit par activer la planification, on sélectionne samedi 00 : 01 : 00 et on nomme la tâche backup complet. La tâche s'exécute immédiatement ce qui permet de vérifier si elle fonctionne correctement. On répète le processus avec une nouvelle sauvegarde de type incrémentielle qui se fait du mardi au vendredi à 00 : 01 : 00 et qui se nomme Sauvegarde Incrémentielle.



**Figure 29 Résumé tâches de backup**

Avec cette configuration les sauvegardes s'effectuent sur le NAS en respectant le cahier des charges.

#### 4.1.11 Access Point Bullet

La configuration de l'access point se fait via câble sériel. Premièrement on reset la configuration en débranchant puis rebranchant l'alimentation PoE tout en maintenant le bouton reset. Voici la configuration de l'access point.

```
ena

conf t

hostname Kicroit-BU-AP1

enable secret Kicroit24-Ap1_MdP$

Line console 0
password Kicroit24-Ap1_MdP$
Login
```

```
exit

Line vty 0 4
password Kicroit24-Ap1_MdP$
Login
exit

service password-encryption

banner motd # AccessPoint Kicroit acces interdit aux personnes non
autorisees #

no ip domain-lookup

int bv1
ip address 192.168.20.50 255.255.255.0
exit

ip default-gateway 192.168.20.1

dot11 ssid KicroitBU_Wifi2.4
auth open
auth key wpa ver 2
wpa-psk ascii Pa$$w0rd
guest-mode
exit

int d0
encryption mode ciphers aes
ssid KicroitBU_Wifi2.4
channel 1
channel least-congested
```

```
no shutdown  
  
end  
  
write
```

#### 4.1.12 Laptop

Le Laptop ne demande pas de configuration particulière. Avec la même clé que pour le pc fixe on installe windows en faisant attention à supprimer tous les disques déjà existants. Une fois Windows installé on renomme le PC Kicroit-Laptop1 sous « renommer ce pc avancé » et on l'insère dans le domaine. Au redémarrage il suffit de se connecter avec un compte présent dans l'AD pour avoir accès aux ressources du domaine.

#### 4.1.13 Routeur Lausanne

Premièrement on remet le routeur à zéro. Comme je possède les accès au mode privilégié il est possible d'utiliser « write erase » pour supprimer la configuration de démarrage et « reload » pour valider les changements.

Une fois cela fait voici les commandes pour configurer le routeur en respectant l'analyse faite :

```
enable  
  
conf t  
  
hostname Kicroit-LA-Router1  
  
enable secret Kicroit24-Router2_MdP$  
  
Line console 0  
password Kicroit24-Router2_MdP$  
Login  
exit  
  
line vty 0 4  
password Kicroit24-Router2_MdP$  
login  
transport input ssh  
exit
```

```
service password-encryption

no ip domain-lookup

banner motd # Routeur Kicroit acces interdit aux personnes non autorises #

ip routing

! Liste de contrôle d'accès définissant le trafic chiffré
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 102 permit ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 102 permit ip 192.168.60.0 0.0.0.255 192.168.20.0 0.0.0.255

! configuration des routes statiques
ip route 192.168.10.0 255.255.255.0 192.168.0.1
ip route 192.168.20.0 255.255.255.0 192.168.0.1

! phase 1 configuration de l'IKE
crypto isakmp policy 10
encr aes
hash sha
authentication pre-share
group 2
lifetime 86400
exit

! clé pré-partagée pour l'authentification de la Phase 1
crypto isakmp key VPN_KEY address 192.168.0.1

! Phase 2 Création du tunnel
```

```
crypto ipsec transform-set TRANS esp-aes esp-sha-hmac
exit

! Phase 2 association du transform set à une crypto map
crypto map VPNMAP 10 ipsec-isakmp
set peer 192.168.0.1
set transform-set TRANS
match address 102
exit

int G0/0
ip address 192.168.0.2 255.255.255.252
crypto map VPNMAP
no shutdown
exit

int g0/1
no shutdown

int g0/1.50
encapsulation dot1Q 50
ip address 192.168.50.1 255.255.255.0
exit

int g0/1.60
encapsulation dot1Q 60
ip address 192.168.60.1 255.255.255.0
ip helper-address 192.168.20.20
exit

end
```



```
write
```

#### 4.1.14 Imprimante Lausanne

La configuration de l'imprimante se fait sous network>Wired Lan> TCP/IP. Il faut mettre une adresse en statique : 192.168.50.10/24 gateway 192.268.50.1. On change aussi le node name en Kicroit-LA-Printer1.

#### 4.1.15 Switch Lausanne

La configuration du switch se fait par le port sérial. Premièrement on le remet à zéro avec les commandes write erase et reload. Dans ce switch les Vlans doivent être créés pour pouvoir séparer le réseau des imprimantes du réseau des utilisateurs. Voici la configuration du switch.

```
enable

conf t

hostname Kicroit-LA-Switch1

enable secret Kicroit24-Switch2_MdP$

Line console 0
password Kicroit24-Switch2_MdP$
Login
exit

line vty 0 4
password Kicroit24-Switch2_MdP$
login
transport input ssh
exit

service password-encryption

no ip domain-lookup
```

```
banner motd # Switch Kicroit acces interdit aux personnes non autorisees #

vlan 50
name VLAN50

vlan 60
name VLAN60

int fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 50,60
no shutdown

int fa0/2
switchport mode access
switchport access vlan 60
no shutdown
exit

int fa0/3
switchport mode access
switchport access vlan 50
no shutdown
exit

int range fa0/4-8
shutdown
end
write
```

#### 4.1.16 Access Point Lausanne

La configuration de l'accès point se fait via câble sériel. Premièrement on reset la configuration en débranchant puis rebranchant l'alimentation PoE tout en maintenant le bouton reset. Voici la configuration de l'accès point.

```
ena

conf t

hostname Kicroit-LA-AP1

enable secret Kicroit24-Ap2_MdP$

Line console 0
password Kicroit24-Ap2_MdP$
Login
exit

Line vty 0 4
password Kicroit24-Ap2_MdP$
Login
exit

service password-encryption

banner motd # AccessPoint Kicroit acces interdit aux personnes non
autorisees #

no ip domain-lookup

int bv1
ip address 192.168.60.50 255.255.255.0
exit
```

```
ip default-gateway 192.168.60.1

dot11 ssid KicroitLA_Wifi2.4
auth open
auth key wpa ver 2
wpa-psk ascii Pa$$w0rd
guest-mode
exit

int d0
encryption mode ciphers aes
ssid KicroitLA_Wifi2.4
channel 1
channel least-congested
no shutdown
end

write
```

## 4.2 Description des tests effectués

Appareil ou service testé	Quoi	Résultat Attendu	Réussite/échec	Commentaire
Routeur BU	Allumage du routeur	Le routeur s'allume et démarre correctement	Réussite	
Routeur BU	Configuration initiale	La configuration initiale du routeur est correctement effectuée (nom, adresse)	Réussite	
Routeur BU	Sécurité	Le routeur demande un mot de passe pour pouvoir se connecter en Vty et avec un câble console	Réussite	
Routeur BU	Connexion avec le fire wall	le routeur doit pouvoir ping l'interface wan du fire wall	Réussite	
Routeur BU	VPN	Le routeur assure son rôle de VPN master	Réussite	
Fire wall	Allumage du fire wall	Le fire wall s'allume correctement	Réussite	
Fire wall	Configuration initiale	La configuration initiale du fire wall est correctement effectuée et il est possible d'y accéder via un navigateur web	Réussite	
Fire wall	Compte admin	Un compte admin propre à Kicroit existe et possède tous les droits	Réussite	
Fire wall	Connexion avec le réseau 1	les appareils du réseau lan 1 doivent pouvoir ping l'interface 1	Réussite	
Fire wall	Connexion avec le réseau 2	les appareils du réseau lan 1 doivent pouvoir ping l'interface 2	Réussite	
Fire wall	Connexion avec le réseau 3	les appareils du réseau lan 1 doivent pouvoir ping l'interface 3	Réussite	
Fire wall	Configuration des polices	Les sites webs sont filtrés suivant des filtres pertinents pour une entre prise	Réussite	
Fire wall	Routes statiques	interconnectés	Réussite	
Fire wall	Règles fire wall	Les règles fire wall bloquent le trafic de manière précise entre les réseaux	Echec	Actuellement les règles fire wall ne bloquent rien du
Serveur 1	Allumage du serveur	le serveur s'allume et démarre correctement	Réussite	
Serveur 1	Installation initiale	Windows serveur 2022 est correctement installé sur le serveur	Réussite	
Serveur 1	Ping	Le serveur peut ping les appareils du réseau	Réussite	
DHCP	Livraison d'adresse BU	Le DHCP donne des adresses suivant la plage sélectionnée	Réussite	
DHCP	Livraison d'adresse Lausanne	Le DHCP donne des adresses suivant la plage sélectionnée	Réussite	
DNS	Inscription DNS	Le DNS inscrit dans ses registres les adresses ip avec les appareils correspondants	Réussite	
AD DS	Le service est fonctionnel	Le domaine Kicroit.ch existe et il est possible de s'y connecter	Réussite	
AD DS	Utilisateurs et groupes	Les utilisateurs et groupes sont créés conformément à la planification	Réussite	
Serveur de fichier	Arborescence	Les dossiers de l'arborescence existent conformément à la planification	Réussite	
Serveur de fichier	Partage	Le partage fonctionne	Réussite	
Serveur de fichier	GPO	Les Gpo permettent le déploiement automatique du partage	Réussite	
Serveur de fichier	DNS	Les permissions NTFS existent conformément à la planification	Réussite	
Serveur d'impression	Imprimante	Le serveur d'impression liste les imprimantes et les pilotes	Réussite	
Serveur d'impression	GPO	Le serveur d'impression distribue l'imprimante via GPO	Echec	Les GPO pour les imprimantes ne fonctionnent pas mais ne sont pas nécessaires actuellement
Serveur redondant	Allumage du serveur	le serveur s'allume et démarre correctement	Réussite	
Serveur redondant	Installation initiale	Windows serveur 2022 est correctement installé sur le serveur	Réussite	
Serveur redondant	Ping	Le serveur peut ping les appareils du réseau	Réussite	
DHCP	Basculement DHCP	Le DHCP donne des adresses suivant la plage sélectionnée	Réussite	
DHCP	Basculement DHCP	Le DHCP donne des adresses suivant la plage sélectionnée	Réussite	
DNS	Inscription DNS	Le DNS inscrit dans ses registres les adresses ip avec les appareils	Réussite	
AD DS	Le service est fonctionnel	Le domaine Kicroit.ch existe et il est possible de s'y connecter	Réussite	
AD DS	Réplication	Le serveur est bien contrôleur de domaine et la réplication depuis le main s'est faite correctement	Réussite	
Serveur de fichier	Réplication DFS	Les dossiers sont répliqués correctement	Réussite	
Serveur de fichier	Réplication DFS	Le serveur reprend le rôle de l'autre s'il n'est plus en ligne	Réussite	
Serveur d'impression	Imprimante	Le serveur d'impression possède l'imprimante	Echec	Le service d'impression ne peut pas être redondant sans Virtualisation ce qui change toute l'infrastructure du réseau
Serveur d'impression	GPO	Le serveur d'impression distribue l'imprimante via GPO	Echec	Le service d'impression ne peut pas être redondant sans Virtualisation ce qui change toute l'infrastructure du réseau
Serveur redondant	Redondance	Le serveur reprend le rôle de l'autre s'il n'est plus en ligne	Réussite	
PC fixe Bullet	Installation initiale	Windows 10 pro est installé sur le pc	Réussite	
PC fixe Bullet	Putty	Putty est installé et permet de se connecter aux appareils	Réussite	
PC fixe Bullet	Domaine	Le pc fait partie du domaine	Réussite	
PC fixe Bullet	Ping	le PC peut ping les appareil du réseau	Réussite	
PC portables	Installation initiale	Windows 10 pro est installé sur les deux pc	Réussite	
PC portables	Putty	Putty est installé et permet de se connecter aux appareils	Réussite	
PC portables	Domaine	Les pc font partie du domaine	Réussite	
PC portables	Ping	les pc peuvent ping les appareil du réseau	Réussite	
Imprimantes	Configuration initiale	La configuration initiale des imprimantes est correctement effectuée(ip	Réussite	
Imprimantes	Impression	L'impression depuis les postes de travail fonctionne	Réussite	
Switch Bullet	Configuration initiale	La configuration initiale de switch est correctement effectuée	Réussite	
Switch Bullet	Sécurité	Les principes de sécurités élémentaires sont respectés	Réussite	
Switch Lausanne	Configuration initiale	La configuration initiale de switch est correctement effectuée	Réussite	
Switch Lausanne	Sécurité	Les principes de sécurités élémentaires sont respectés	Réussite	
Switch Lausanne	Vlan	Le switch gère correctement les Vlans	Réussite	
AP Bullet	Configuration initiale	La configuration initiale des AP est correctement effectuée	Réussite	
AP Bullet	Distribution adresse IP	L'AP donne des adresses et elles sont référencées dans le DHCP	Réussite	
AP Lausanne	Configuration initiale	La configuration initiale des AP est correctement effectuée	Réussite	
AP Lausanne	Distribution adresse IP	L'AP donne des adresses et elles sont référencées dans le DHCP	Réussite	
NAS	Configuration initiale	La configuration initiale du NAS permet de se connecter via WEB	Réussite	
NAS	Raid	Les disques sont initialisés en raid 5	Réussite	
NAS	Stratégie de backup	Les stratégies de backup sont fonctionnelles et représentent les choix fait pendant la conception	Réussite	
NAS	Ping	Le serveur ne peut rien ping	Echec	Du aux règles fire wall actuellement le Nas peut ping
Routeur Lausanne	Allumage du routeur	Le routeur s'allume et démarre correctement	Réussite	
Routeur Lausanne	Configuration initiale	La configuration initiale du routeur est correctement effectuée (nom, adresse)	Réussite	
Routeur Lausanne	Sécurité	Le routeur demande un mot de passe pour pouvoir se connecter en Vty et avec un câble console	Réussite	
Routeur Lausanne	VPN	Le routeur remplit son rôle de VPN slave	Réussite	
Routeur Lausanne	Vlans	Le routeur gère correctement les Vlans	Réussite	

Figure 30 Résultats des tests

## **4.3 Problèmes rencontrés**

### **4.3.1 PrintNightmare**

Le premier grand problème que j'ai rencontré avec le projet s'est produit lors de l'installation du serveur d'impression. A cette étape du projet l'ordinateur fixe et le laptop sont déjà installés, le serveur principal est en marche avec AD DNS et DHCP et l'imprimante de Bullet est configurée. J'ai pu intégrer assez facilement l'imprimante dans les périphériques du serveur et ma GPO pour les imprimantes est déployée.

Maintenant arrive le problème, lorsque je veux récupérer l'imprimante depuis mon poste fixe c'est impossible. J'obtiens l'erreur 283<sup>11</sup>, elle fait référence à une mauvaise gestion des pilotes d'impression tiers. En effet les imprimantes qui m'ont été fournies sont vieilles, il faut donc des pilotes anciens qui se trouvent sur le site de Brother. Si ces pilotes sont installés manuellement via une clé USB et en mode administrateur ça ne pose pas de problème mais pour le déploiement automatique ça coince.

J'ai essayé plusieurs choses. Modifier les GPO pour autoriser l'installation de pilotes sans le compte administrateur. Installer l'imprimante depuis partage. Installer en administrateur. Réinstaller l'imprimante sans les pilotes. Réinstaller l'ordinateur. Aucune de ses solutions ne donnais de résultats satisfaisants.

Chose étonnante en testant avec le Portable j'ai réussi à installer correctement l'imprimante. En effectuant des recherches <sup>12</sup>et avec l'aide de monsieur Fazola nous avons trouvé le problème. La version de Windows 10 que j'avais récupéré sur le partage de l'école était en 17.09 et n'était donc pas patchée pour le PrintNightmare<sup>13</sup>. Il s'agit d'un bug de pilotes qui est apparu après des patches de Microsoft en 2021 pour corriger une faille de sécurité.

Il existe deux possibilités pour corriger la panne. Réinstaller une version plus à jour de windows ou modifier la valeur de la clé de registre HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint. J'ai choisi la première option pour avoir une infrastructure propre et éviter des bugs futurs. Après la réinstallation de la machine il est possible de connecter sans problème les imprimantes sur le PC.

### **4.3.2 Délégation DFS**

Lorsque j'ai mis en place le serveur redondant j'ai dû mettre en place une délégation DFS pour pouvoir assurer le relai du serveur de fichier si le serveur principal tombait. Je n'avais jamais mis en place ce rôle. Je ne saurais pas exactement expliquer quelle erreur j'ai fait mais lors de la création DFS, au moment de la validation, le serveur n'a pas réussi à le faire. Il a ressorti des erreurs globales mais la quand même créé. Malheureusement je ne pouvais plus interagir avec la délégation. Lorsque je voulais la supprimer ou la modifier toutes les options disparaissaient et un message indiquant qu'il était impossible de contacter le serveur RPC<sup>14</sup> apparaissait.

---

<sup>11</sup> <https://learn.microsoft.com/en-us/answers/questions/1334580/linking-printers-gives-an-error-error-283>

<sup>12</sup> <https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>

<sup>13</sup> <https://en.wikipedia.org/wiki/PrintNightmare>

<sup>14</sup> <https://www.ionos.fr/digitalguide/serveur/configuration/serveur-rpc-nest-pas-disponible/>

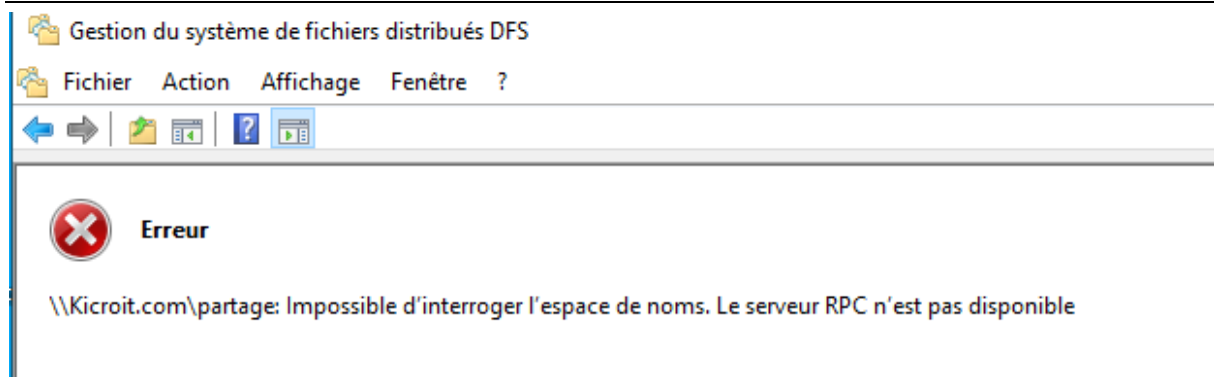


Figure 31 Bug DFS

Même après avoir redémarré le serveur il est impossible de se débarrasser de cette réplication. J'ai donc essayé de désinstaller le rôle DFS du serveur mais malheureusement quand le serveur fait partie d'une réplication il est impossible de supprimer le rôle.

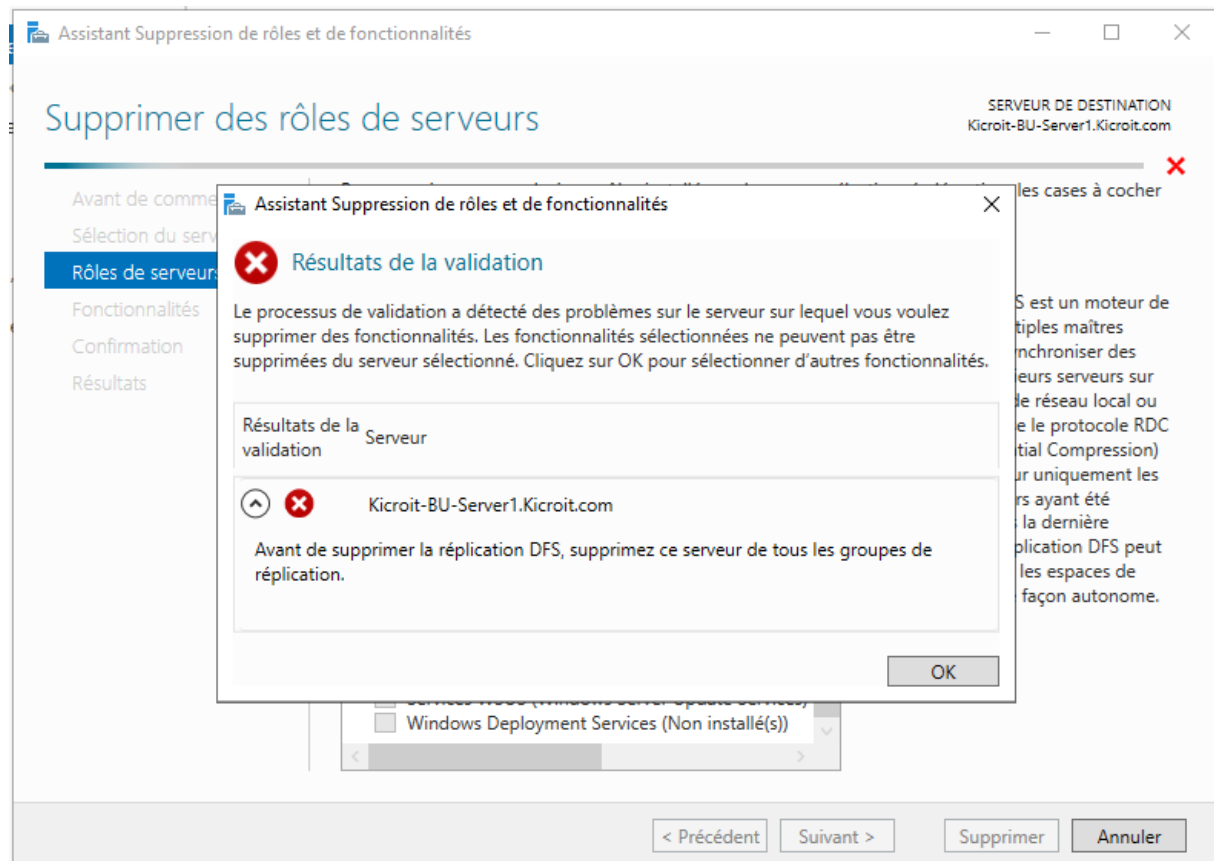


Figure 32 Suppression Role DFS

Après plusieurs tentatives en Powershell Chatgpt m'a donné ce code qui supprime le rôle :

```
# ===== CONFIGURATION =====
$regPath = "HKLM:\SYSTEM\CurrentControlSet\Services\DFSR"
$dfsFolder = "C:\System Volume Information\DFSR"
```

```
# ===== 1. Désinstallation du rôle =====

Write-Host "`nTentative de désinstallation de FS-DFS-Replication..." -
ForegroundColor Cyan

try {

    Uninstall-WindowsFeature -Name FS-DFS-Replication -Remove -ErrorAction
Stop -Verbose

    Write-Host "✓ Rôle DFS-R désinstallé avec succès." -ForegroundColor
Green

} catch {

    Write-Host "X Échec de la désinstallation propre. On passe au
nettoyage manuel..." -ForegroundColor Yellow

}

# ===== 2. Suppression du registre DFSR =====

if (Test-Path $regPath) {

    try {

        Write-Host "Suppression de la clé registre DFSR..." -
ForegroundColor Cyan

        Remove-Item -Path $regPath -Recurse -Force

        Write-Host "✓ Clé registre supprimée." -ForegroundColor Green

    } catch {

        Write-Host "X Impossible de supprimer la clé registre :
$(($_.Exception.Message))" -ForegroundColor Red

    }

} else {

    Write-Host "Aucune clé registre DFSR trouvée." -ForegroundColor Yellow

}

# ===== 3. Suppression du dossier système DFSR =====

if (Test-Path $dfsrFolder) {

    try {

        Write-Host "Tentative de suppression du dossier DFSR..." -
ForegroundColor Cyan

    }
```



```
# Prendre possession

takeown /F "$dfsrFolder" /A /R /D Y | Out-Null

icacls "$dfsrFolder" /grant Administrateurs:F /T | Out-Null


# Supprimer le dossier

Remove-Item "$dfsrFolder" -Recurse -Force

Write-Host "✓ Dossier DFSR supprimé." -ForegroundColor Green
} catch {

    Write-Host "X Impossible de supprimer le dossier DFSR :
$(($_.Exception.Message))" -ForegroundColor Red

}
} else {

    Write-Host "Aucun dossier DFSR trouvé." -ForegroundColor Yellow
}

# ===== 4. Redémarrage =====

Write-Host "`nRedémarrage du serveur dans 10 secondes..." -ForegroundColor Cyan

Start-Sleep -Seconds 10

Restart-Computer -Force
```

Grâce à ça le service a effectivement été supprimé mais certains fichiers importants aussi. Je ne pouvais, par exemple, plus créer de GPO pour mapper les disques. J'ai donc choisi de réinstaller entièrement le serveur plutôt que de trainer des problèmes potentiels sur le reste du projet. Après la réinstallation le service DFS a fonctionné sans problème.

#### 4.4 Erreurs restantes

Le projet a été rigoureusement testé et ne présente actuellement aucune erreur technique ou fonctionnelle. L'unique « erreur » se situe au niveau des GPO pour les imprimantes ou l'imprimante ne se supprime pas automatiquement des ordinateurs si elle est supprimée du pool d'impression. Elle n'est juste plus accessible.

#### 4.5 Liste des documents fournis et dossier d'archivage

## 5 Conclusions

### 5.1 Comparaison entre la conception et la réalisation

Il n'y a pas beaucoup de modifications faites entre la conception et la réalisation. Dans cette version finale le schéma logique a été mis à jour en corrigeant les quelques erreurs qu'il comportait. Par exemple le rôle redondant Service d'impression a été supprimé parce qu'il n'a pas pu être fait et les IP ont été corrigées lorsque mal faites. Hormis le service d'impression il n'y avait que des petites erreurs d'inattention, la structure complète du schéma était saine et il a été possible de la mettre en œuvre complètement.

La deuxième différence par rapport à la conception se situe au niveau du serveur de fichier. En effet, dans la conception, j'avais prévu de créer les dossier Marketing et Finances directement à la racine du lecteur F:. Cependant cette méthode me demande de partager tout le lecteur F: ou de séparer en deux partages distincts les dossiers. La première n'est jamais une bonne pratique et la deuxième est très rigide et demanderait de refaire un partage pour chaque nouveau dossier créé dans le F: ce qui n'est pas une bonne pratique non plus. J'ai donc créé un dossier supplémentaire « Serveur de fichier ». Voici le graphe adapté :

Permissions NTFS					
Dossier		Groupes	Admins du domaines	Marketing	Finances
F:\Serveur de Fichiers			CT		
	\Marketing		CT	M	
	\Finances		CT		M

CT	Contrôle total
M	Modification
LX	Lecture et exécution

Figure 33 Permissions NTFS Mises à jour

### 5.2 Etat actuel du projet

Le projet, tel qu'il se présente actuellement, peut être considéré comme pleinement concluant. Tous les objectifs initiaux ont été pleinement atteints et parfois même consolidés par des ajustements visant à garantir une efficacité optimale. L'infrastructure mise en place est entièrement opérationnelle et stable. De plus, l'ensemble des points techniques ont été traités.

### 5.3 Améliorations possibles

Les principales améliorations possibles se trouvent au niveau des règles du firewall. En effet, à l'heure actuelle le firewall laisse passer tout le trafic en interne. Il n'a pas été

demandé de sécuriser ces différentes liaisons mais pour plus de sécurité et de pertinence il faudrait limiter les services et protocoles qui passent au strict nécessaire.

#### 5.4 Ressenti sur le projet

J'ai pris beaucoup de plaisir à faire ce projet. La durée limitée était un défi qui m'a poussé à donner le meilleur de moi-même et je suis fier du résultat que j'ai obtenu. J'ai pu développer mes compétences en pratiquant des éléments nouveaux pour moi comme le VPN ou la réplication FDS. Je regrette de ne pas avoir eu le temps de peaufiner les règles du trafic pour le firewall mais ça n'entache en rien la réussite de ce projet.

## 6 Annexes

### 6.1 Sources – Bibliographie

#### 6.1.1 Intelligences Artificielles :

Pour les cas d'utilisation de l'IA le prompt et le problème auquel il répond sont spécifiés.

Grok :

Prompt	Problème sous-jacent
Fais-moi le logo d'une entreprise fictive qui s'appelle Kicroit.	Créer le logo pour la page de garde.

Chat GPT 4o :

Prompt	Problème sous-jacent
Pour mon travail de fin de CFC je dois créer un réseau pour une petite entreprise. L'entreprise est sur deux sites distincts (Bullet et Lausanne) et je dois les interconnecter avec un VPN site à site. Mon problème est le suivant : J'ai un serveur Windows 2022 qui fait service d'impression mais j'ai une imprimante à Bullet et une à Lausanne. Pour sécuriser mon infrastructure je ne veux pas que les imprimantes soient dans le même réseau que les serveurs et les utilisateurs. Pour Bullet le site est équipé d'un firewall du coup je pensais faire un réseau distinct et limiter le trafic via des règles mais je ne sais pas comment sécuriser les deux imprimantes de manière logique	Il faut connecter l'imprimante de Lausanne en tenant compte de la sécurité. Elle ne doit donc pas pouvoir communiquer avec les autres appareils du réseau mais doit quand même être accessible pour que le serveur d'impression puisse l'intégrer.
J'ai un firewall fortigate 50e. je dois sécuriser les différents LAN qu'il interconnecte. Quel sont les protocoles utilisés par les imprimantes ? quels sont les protocoles utilisés par un NAS ?	Afin de limiter le trafic il faut identifier les différents protocoles et les ports utilisés pour les services d'impression et de sauvegarde. Comme ça il est possible de n'autoriser qu'eux

Sur mon Windows serveur 2022 j'ai ajouté le rôle réplication DFS. J'ai mal fait une configuration ce qui fait planter le tout. Je veux pouvoir supprimer ce rôle et recommencer. Problème je ne peux pas il me dit " avant de supprimer la réplication dfs supprimez ce serveur de tous les groupes de réplication"	Le Service DFS plante sur le serveur principal. J'ai demandé à chat GPT une solution pour pouvoir supprimer le rôle.

### 6.1.2 Sites internet :

<https://asana.com/fr/resources/waterfall-project-management-methodology>

<https://github.com/andreafont/TPI-Infrastrucutre-d-une-PME-avec-deux-sites-distants/tree/main>

<https://neptunet.fr/relais-dhcp/>

<https://www.netacad.com/cisco-packet-tracer>

<https://keepass.info/>

[https://rufus.ie/fr/#google\\_vignette](https://rufus.ie/fr/#google_vignette)

<https://www.putty.org/>

[https://help.fortinet.com/fdb/5-0-0/html/source/tasks/t\\_network\\_configuration\\_cli.html](https://help.fortinet.com/fdb/5-0-0/html/source/tasks/t_network_configuration_cli.html)

<https://www.brother.ch/fr-ch/support/dcp-l8400cdn/downloads?srsId=AfmBOoqwRtN1MVaA4cSWpiNEBUx-pzJqTI9Vpo4oOZZwUyKT-yRHsCV3>

<https://learn.microsoft.com/en-us/answers/questions/1334580/linking-printers-gives-an-error-error-283>

<https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>

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

<https://www.ionos.fr/digitalguide/serveur/configuration/serveur-rpc-nest-pas-disponible/>

### 6.1.3 Personnes extérieures au projet :

Grégory Renaud

Francis Varela

Sylvain Fazola

**6.2 Glossaire**

**6.3 Table des illustrations**

Aucune entrée de table d'illustration n'a été trouvée.

**6.4 Journal de bord**