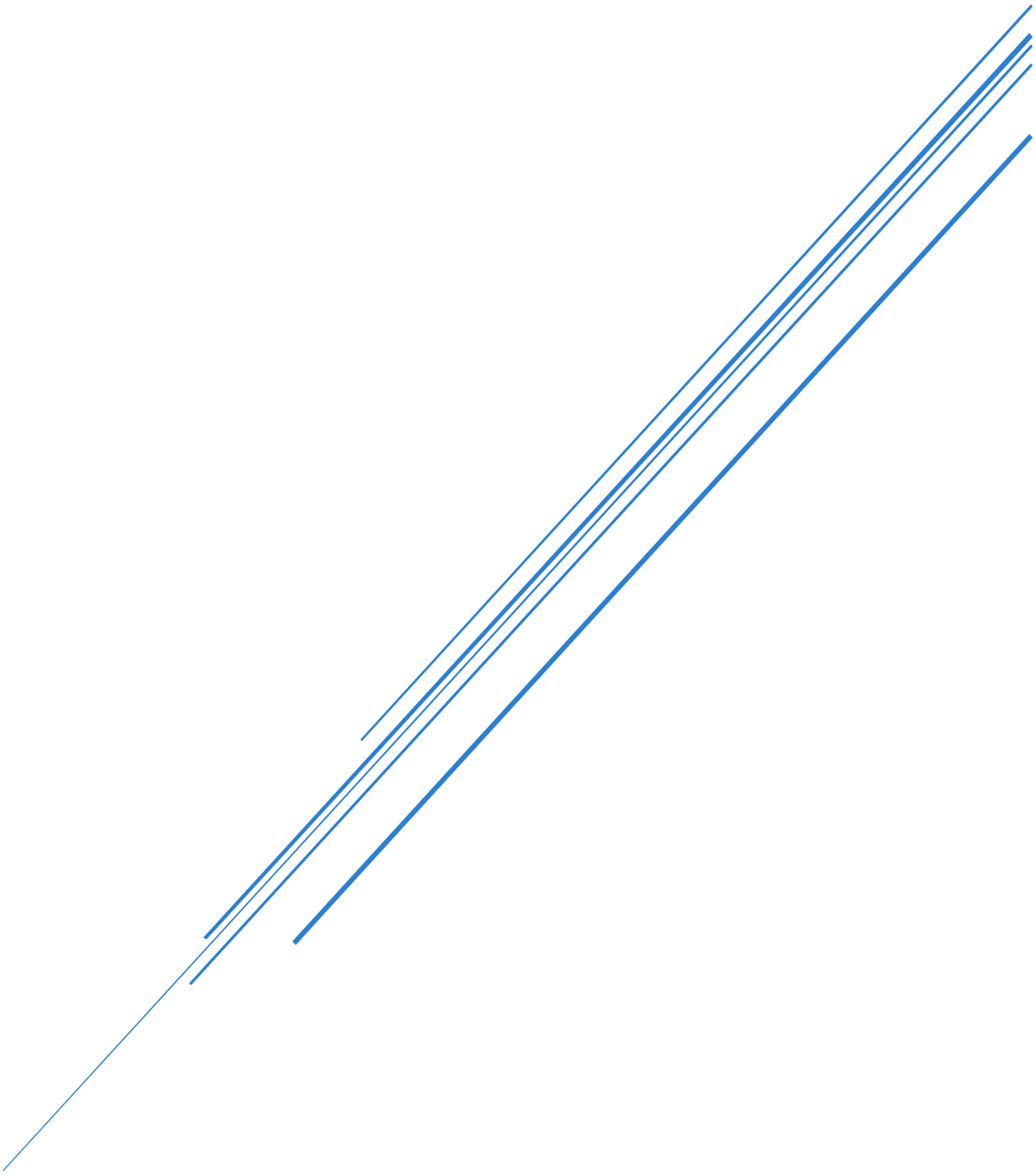
TD HOPITAL

14/06/2024



WARTH Victor
TD

Table des matières

1. Analyse de risques 3
1.1. Détails des Risques et Solutions 3
Risque R1 : Version obsolète de Windows Server 2008 R2 3
Risque R2 : Pas de redondance du contrôleur de domaine 3
Risque R3 : Version obsolète de Windows 7 Pro sur les postes clients 3
Risque R4 : Absence de firewall entre les segments réseau 4
Risque R5 : Utilisation d'un routeur simple 4
Risque R6 : Pas de sauvegarde fiable 4
Risque R7 : Absence de surveillance continue 5
1.2. Tableau d'analyse de risques 1
1.3. Cartographie des risques 1
1.4. Synthèse des actions à réaliser 1
2. Etude comparative 2
2.1. Services d’annuaires et d’authentification 2
2.2. Services DNS et DHCP 4
2.3. Service de fichiers 6
2.4. Conclusion 7
3. Maquettage 1
3.1. Schéma réseau de ma maquette : 1
3.2. Paramétrage clé de mes VM 1
3.2.1. Paramétrage clé du premier Windows Serveur 1
3.2.2. Paramétrage clé du deuxième Windows Serveur 6
3.3. Vérification du fonctionnement 9

1. Analyse de risques

Tout d'abord, nous allons analyser l'ensemble des risques qui sont liées à notre périmètre d'intervention.

1.1. Détails des Risques et Solutions

Risque R1 : Version obsolète de Windows Server 2008 R2

Description : Les deux serveurs utilisent une version de Windows Server qui n'est plus supportée par Microsoft, ce qui les rend vulnérables aux nouvelles attaques.

Gravité : Risque élevé d'exploitation des vulnérabilités connues.

Vraisemblance : Élevée, car ces versions sont fréquemment ciblées par les attaques.

Mesures Correctives : Migrer vers Windows Server 2019 ou 2022, appliquer les mises à jour de sécurité régulièrement.

Statut de la Couverture **:** Total, après migration et mise à jour.

Risque R2 : Pas de redondance du contrôleur de domaine

Description **:** Un seul serveur gère plusieurs rôles critiques, y compris AD DS, DHCP, DNS, et DFS, ce qui crée un point de défaillance unique.

Gravité **:** Perte de disponibilité et de gestion de l'authentification et des services réseau en cas de panne.

Vraisemblance **:** Élevée, en raison de l'absence de redondance.

Mesures Correctives **:** Ajouter un deuxième contrôleur de domaine pour assurer la continuité des services en cas de défaillance.

Statut de la Couverture **:** Total, après ajout d'un deuxième contrôleur.

Risque R3 : Version obsolète de Windows 7 Pro sur les postes clients

Description **:** Les postes de travail utilisent Windows 7 Pro, qui ne reçoit plus de mises à jour de sécurité.

Gravité **:** Exposition aux attaques exploitant des vulnérabilités non corrigées.

Vraisemblance **:** Élevée, car bien que les postes soient moins critiques en tant que tels, ils sont d'important vecteur d'attaque.

Mesures Correctives **:** Mettre à niveau les postes vers Windows 10 ou 11, utiliser des solutions antivirus et appliquer les mises à jour de sécurité.

Statut de la Couverture **:** Total, après migration et sécurisation.

Risque R4 : Absence de firewall entre les segments réseau

Description **:** Les segments réseau critique (production) et administratif ne sont pas séparés par un firewall, ce qui augmente le risque de propagation d'une attaque.

Gravité **:** Très élevé, car une attaque sur le segment administratif pourrait affecter le segment critique.

Vraisemblance **:** Élevée, car les réseaux ne sont pas isolés.

Mesures Correctives **:** Installer des firewalls pour isoler les segments réseau critiques des autres, appliquer des règles de sécurité strictes. N'autoriser que le flux nécessaire au bon fonctionnement du segment critique.

Statut de la Couverture **:** Total, après installation et configuration des firewalls.

Risque R5 : Utilisation d'un routeur simple

Description **:** Les différents segments réseau sont connectés par un simple routeur, sans fonctionnalités de sécurité avancées.

Gravité **:** Élevé, car il y a peu de contrôle sur le trafic entre les segments.

Vraisemblance **:** Moyenne, car le routeur simple est moins efficace pour protéger contre les menaces modernes.

Mesures Correctives **:** Remplacer le routeur par un Next-Generation Firewall (NGFW) capable de gérer et de sécuriser les segments réseau.

Statut de la Couverture **:** Total, après remplacement par un NGFW.

Risque R6 : Pas de sauvegarde fiable

Description **:** L'absence de sauvegarde fiable des données critiques expose l'hôpital à des pertes de données importantes en cas de ransomware ou de défaillance système.

Gravité **:** Très élevé, car la perte de données pourrait affecter gravement les opérations de l'hôpital.

Vraisemblance **:** Élevée, sans stratégie de sauvegarde appropriée.

Mesures Correctives **:** Mettre en place une stratégie de sauvegarde régulière avec des copies hors site et des tests de restauration.

Statut de la Couverture **:** Total, après mise en œuvre d'une stratégie de sauvegarde.

Risque R7 : Absence de surveillance continue

Description **:** Il n'y a pas de surveillance continue des activités réseau et systèmes, ce qui empêche la détection précoce des incidents de sécurité.

Gravité : Élevé, car les incidents peuvent passer inaperçus et causer des dommages importants.

Vraisemblance **:** Moyenne, en l'absence de surveillance.

Mesures Correctives **:** Implémenter un système de surveillance continue (SIEM) pour détecter et répondre rapidement aux incidents.

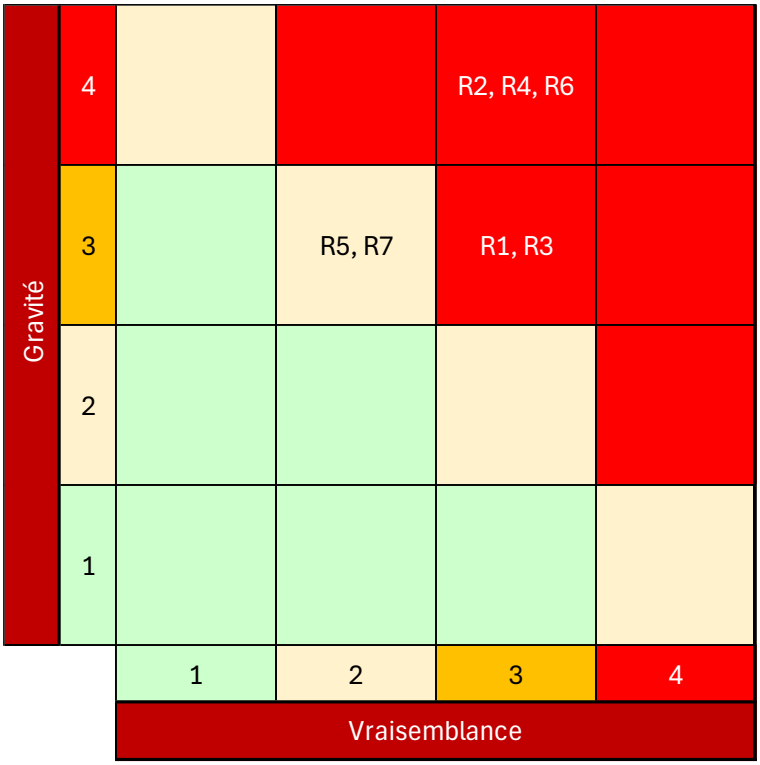
Statut de la Couverture **:** Partiel, car la mise en œuvre peut nécessiter du temps et des ressources.

1.2. Tableau d'analyse de risques

ID	Risque	Description	Gravité	Vraisemblance	Niveau de Risque	Mesures Correctives	Statut de la Couverture
R1	Version obsolète de Windows Server 2008 R2	Les serveurs utilisent une version obsolète de Windows Server, vulnérable aux attaques récentes.	3	3	INNACEPTABLE	Migrer vers une version supportée de Windows Server (2019 ou 2022), appliquer les mises à jour de sécurité.	Total
R2	Pas de redondance du contrôleur de domaine	Un seul contrôleur de domaine avec plusieurs rôles critiques.	4	3	INNACEPTABLE	Ajouter un deuxième contrôleur de domaine pour redondance, répartir les rôles critiques entre plusieurs serveurs.	Total
R3	Version obsolète de Windows 7 Pro	Les postes clients utilisent Windows 7 Pro, qui n'est plus supporté, ce qui expose à des vulnérabilités non corrigées.	3	3	INNACEPTABLE	Migrer les postes clients vers Windows 10 ou 11, appliquer des correctifs de sécurité et des outils de protection.	Total
R4	Pas de firewall entre les segments réseau	Absence de firewall entre les segments réseau administratif et de production.	4	3	INNACEPTABLE	Installer des firewalls pour segmenter les réseaux critiques et administratifs, appliquer des règles strictes de contrôle d'accès.	Total
R5	Utilisation d'un routeur simple	Un simple routeur relie les différents segments réseau sans mécanismes avancés de sécurité.	3	2	VIGILANCE	Remplacer le routeur par un dispositif de sécurité avancé (NGFW - Next-Generation Firewall) capable de gérer et segmenter les différents réseaux efficacement.	Total
R6	Pas de sauvegarde fiable	Les données critiques ne sont pas sauvegardées de manière fiable et sécurisée.	4	3	INNACEPTABLE	Mettre en place une stratégie de sauvegarde régulière et fiable, avec des copies hors site et des tests réguliers de restauration.	Total
R7	Absence de surveillance continue	Pas de surveillance continue des activités réseau et systèmes.	3	2	VIGILANCE	Implémenter un système de surveillance continue (SIEM) pour détecter et réagir rapidement aux incidents de sécurité.	Partiel

1.3. Cartographie des risques

Voici la cartographie des risques d'après le modèle du club EBIOS :



1.4. Synthèse des actions à réaliser

Voici une liste des actions les plus importantes à réaliser :

- Migration des systèmes : Mettre à jour les versions obsolètes de Windows Server et des postes clients.
- Implémentation de la redondance : Ajouter des serveurs pour assurer la redondance et répartir les rôles critiques.
- Sécurisation des réseaux : Installer des firewalls entre les segments réseau et remplacer les routeurs simples par des NGFW.
- Mise en place de sauvegardes : Établir une stratégie de sauvegarde régulière et fiable.
- Surveillance continue : Mettre en place des outils de surveillance continue pour détecter les incidents en temps réel.

2. Etude comparative

L'étude comparative ci-dessous va permettre de comparer la solution actuellement mise en place mais dans l'une des dernières versions (Windows Serveur 2019/2022) avec une solution alternative.

2.1. Services d'annuaires et d'authentification

Options comparées :

1. Active Directory (AD) sur Windows Server 2019/2022
2. Azure Active Directory (AAD)
3. FreeIPA sur Linux

Comparaison :

- **Active Directory sur Windows Server 2019/2022 :**

  AD est une solution éprouvée, bien intégrée dans les environnements Windows, qui offre une gestion centralisée des identités et des ressources.

  - Avantages :
    - Intégration native avec les systèmes Windows.
    - Support complet pour les politiques de groupe (GPO).
    - Large support communautaire et documentation.
  - Inconvénients :
    - Coûts de licence et maintenance élevés.
    - Complexité dans la gestion de la migration à partir des versions plus anciennes comme Windows Server 2008 R2.
  - Adaptabilité : Parfait pour les environnements déjà basés sur Windows, avec des besoins en gestion centralisée de sécurité.

- **Azure Active Directory :**

  AAD est une solution de gestion des identités basée sur le cloud, offrant des fonctionnalités avancées de sécurité et de gestion.

  - Avantages :
    - Accès à des fonctionnalités de sécurité avancées comme l'authentification multifacteur (MFA) et la gestion des accès conditionnels.
    - Intégration native avec les services cloud de Microsoft.
    - Réduction des coûts d'infrastructure et de maintenance.

  - Inconvénients :
    - Peut nécessiter une connectivité Internet constante pour certaines fonctionnalités.
    - Complexité dans l'intégration avec les systèmes on-premises existants.
  - Adaptabilité : Idéal pour les organisations cherchant à intégrer ou migrer vers le cloud avec des besoins de gestion modernes.

- **FreeIPA sur Linux :**

  FreeIPA est une solution open-source pour la gestion des identités et la politique d'authentification.

  - Avantages :
    - Open-source, donc sans coûts de licence.
    - Bonne intégration avec les environnements Linux et les services open-source.
    - Support pour les protocoles LDAP et Kerberos.
  - Inconvénients :
    - Courbe d'apprentissage plus raide pour les équipes non familier avec Linux.
    - Moins de support natif pour les environnements Windows.
  - Adaptabilité : Convient aux organisations avec une forte infrastructure Linux ou une expertise en open-source.

Recommandation : Pour l'hôpital, en tenant compte de la migration depuis Windows Server 2008 R2 et la probable prépondérance des environnements Windows, migrer vers Active Directory sur Windows Server 2019/2022 serait le plus approprié. Cela garantit la continuité et une intégration fluide avec les systèmes existants. Pour les futures expansions, l'intégration avec Azure AD pourrait être envisagée pour bénéficier de fonctionnalités cloud avancées.

2.2. Services DNS et DHCP

Options comparées :

1. Microsoft DNS et DHCP sur Windows Server 2019/2022
2. BIND DNS avec ISC DHCP sur Linux
3. Cisco Umbrella

Comparaison :

- **Microsoft DNS et DHCP sur Windows Server 2019/2022 :**

  Solutions intégrées dans l'écosystème Windows Server pour la gestion DNS et DHCP.

  - Avantages :
    - Intégration étroite avec Active Directory.
    - Gestion simplifiée dans des environnements Windows.
    - Support pour la haute disponibilité et la redondance.
  - Inconvénients :
    - Coûts de licence.
    - Dépendance à l'infrastructure Windows.
  - Adaptabilité : Idéal pour les environnements Windows, particulièrement ceux avec Active Directory.

- **BIND DNS avec ISC DHCP sur Linux :**

  Solutions open-source largement utilisées pour la gestion DNS et DHCP.

  - Avantages :
    - Open-source, sans coûts de licence.
    - Haute flexibilité et capacité de personnalisation.
    - Large communauté de support et documentation.
  - Inconvénients :
    - Administration et configuration plus complexes pour ceux non familiers avec Linux.
    - Support natif limité pour l'intégration avec Windows AD.
  - Adaptabilité : Convient aux environnements mixtes ou Linux avec des besoins spécifiques en personnalisation.

- **Cisco Umbrella :**

  Solution DNS basée sur le cloud, offrant une sécurité améliorée avec une approche de filtrage DNS.

  - Avantages :
    - Protection avancée contre les menaces avec une surveillance continue du trafic DNS.
    - Pas besoin de gestion d'infrastructure sur site.
    - Intégration facile avec d'autres services de sécurité Cisco.
  - Inconvénients :
    - Dépendance à une connexion internet fiable.
    - Moins de contrôle granulaire sur les configurations locales.
  - Adaptabilité : Idéal pour les organisations cherchant une solution de sécurité DNS basée sur le cloud.

Recommandation : Pour l'hôpital, Microsoft DNS et DHCP sur Windows Server 2019/2022 est recommandé en raison de sa compatibilité avec l'environnement Active Directory existant et sa facilité d'intégration. Pour des options de sécurité DNS améliorée, Cisco Umbrella pourrait être une solution complémentaire en fournissant une protection contre les menaces en ligne.

2.3. Service de fichiers

Options Comparées :

1. DFS (Distributed File System) sur Windows Server 2019/2022
2. Ceph
3. Azure File Storage

Comparaison :

- **DFS sur Windows Server 2019/2022 :**

  Solution native de Windows pour la gestion distribuée des fichiers et des dossiers.

  - Avantages :
    - Intégration étroite avec l'Active Directory.
    - Support pour la réplication de fichiers et la tolérance aux pannes.
    - Facilité de gestion dans les environnements Windows.
  - Inconvénients :
    - Nécessite une infrastructure Windows.
    - Coûts de licence associés.
  - Adaptabilité : Parfait pour les organisations utilisant majoritairement Windows, nécessitant une gestion centralisée des fichiers.

- **Ceph :**

  Solution open-source de stockage distribué, offrant des fonctionnalités de stockage en bloc, de fichiers et d'objets.

  - Avantages :
    - Hautement évolutif et résilient.
    - Support pour la réplication des données et la haute disponibilité.
    - Compatible avec différents types de stockage (bloc, fichier, objet).
  - Inconvénients :
    - Complexité d'installation et de gestion.
    - Exige une infrastructure et des ressources significatives.
  - Adaptabilité : Convient aux organisations nécessitant une solution de stockage distribué robuste avec des besoins de haute disponibilité et de scalabilité.

- **Azure File Storage :**

  Solution de stockage de fichiers sur le cloud de Microsoft, offrant un accès via le protocole SMB.

  - Avantages :
    - Facilité de gestion et de déploiement dans le cloud.
    - Évolutif à la demande, avec des coûts basés sur l'utilisation.
    - Support natif pour les environnements Windows.
  - Inconvénients :
    - Dépendance à une connexion Internet fiable.
    - Coûts récurrents en fonction de l'utilisation et du stockage.
  - Adaptabilité : Idéal pour les organisations cherchant à réduire les coûts d'infrastructure sur site et nécessitant une solution de stockage évolutive.

Recommandation : Pour l'hôpital, DFS sur Windows Server 2019/2022 est recommandé car il s'intègre bien avec Active Directory et offre des fonctionnalités robustes pour la gestion et la réplication des fichiers dans un environnement Windows. Pour des options de stockage additionnel ou pour des besoins de haute disponibilité et de scalabilité, Ceph ou Azure File Storage peuvent être considérés comme des solutions complémentaires ou futures.

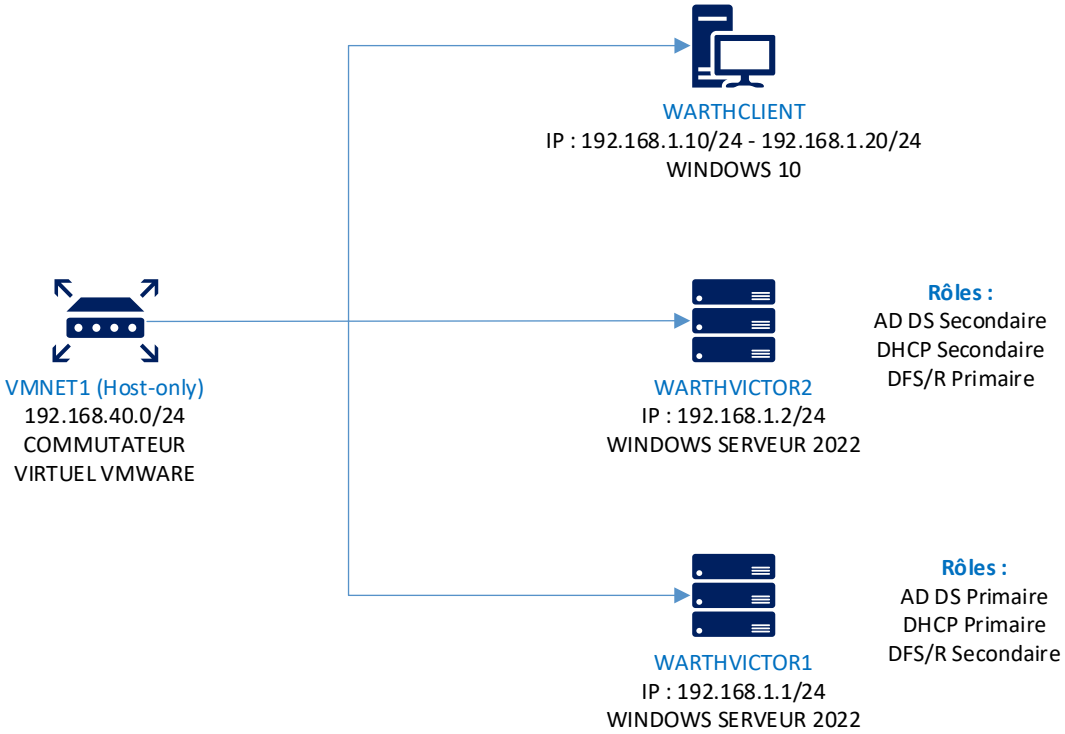
2.4. Conclusion

Après cette analyse comparative, les solutions les plus adaptées pour l'hôpital sont :

1. **Active Directory sur Windows Server 2019/2022** pour les services d'annuaires et d'authentification, avec une éventuelle extension vers **Azure AD** pour les fonctionnalités avancées.
2. **Microsoft DNS et DHCP sur Windows Server 2019/2022** pour la gestion DNS et DHCP, avec **Cisco Umbrella** pour améliorer la sécurité DNS.
3. **DFS sur Windows Server 2019/2022** pour les services de fichiers, avec **Ceph** ou **Azure File Storage** comme options futures pour une scalabilité ou une flexibilité supplémentaire.

3. Maquettage

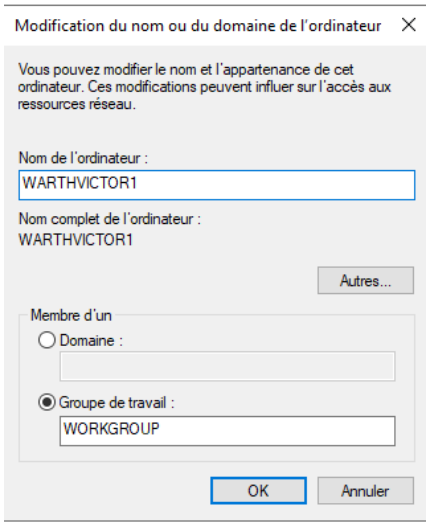
3.1. Schéma réseau de ma maquette :



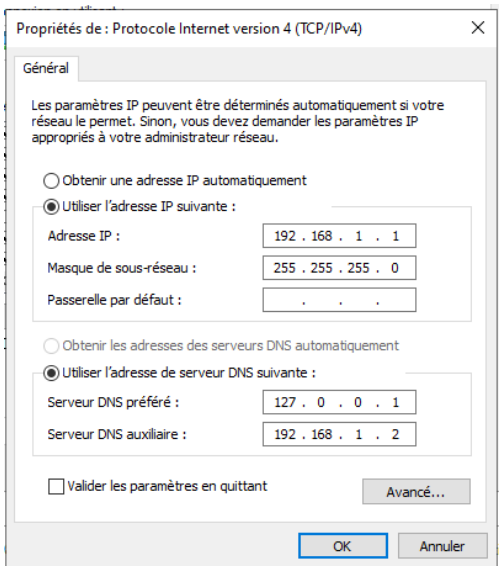
3.2. Paramétrage clé de mes VM

3.2.1. Paramétrage clé du premier Windows Serveur

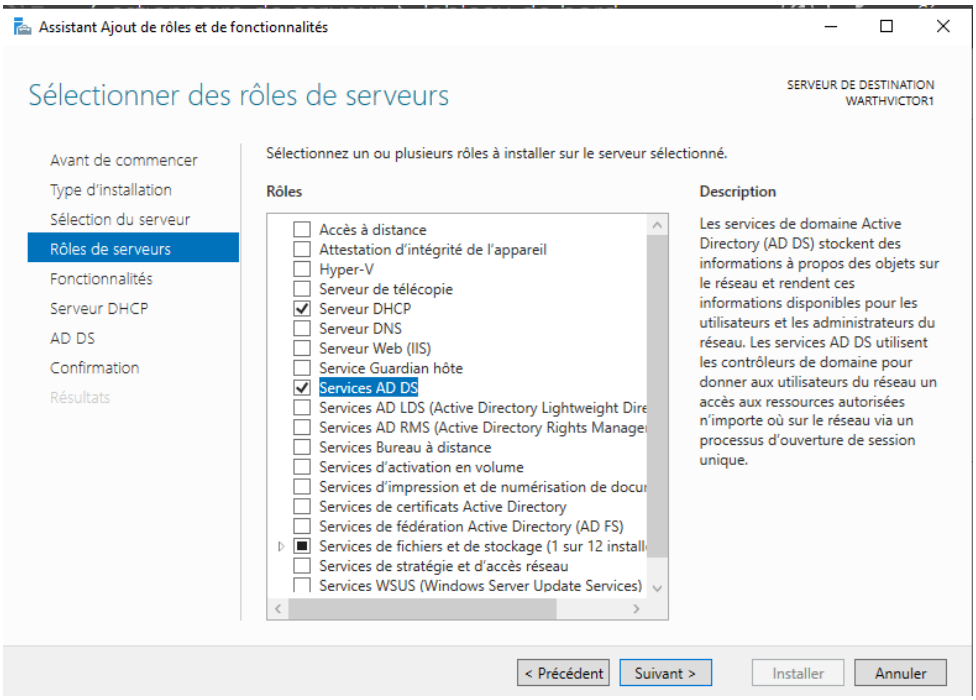
Modification du nom de mon serveur :



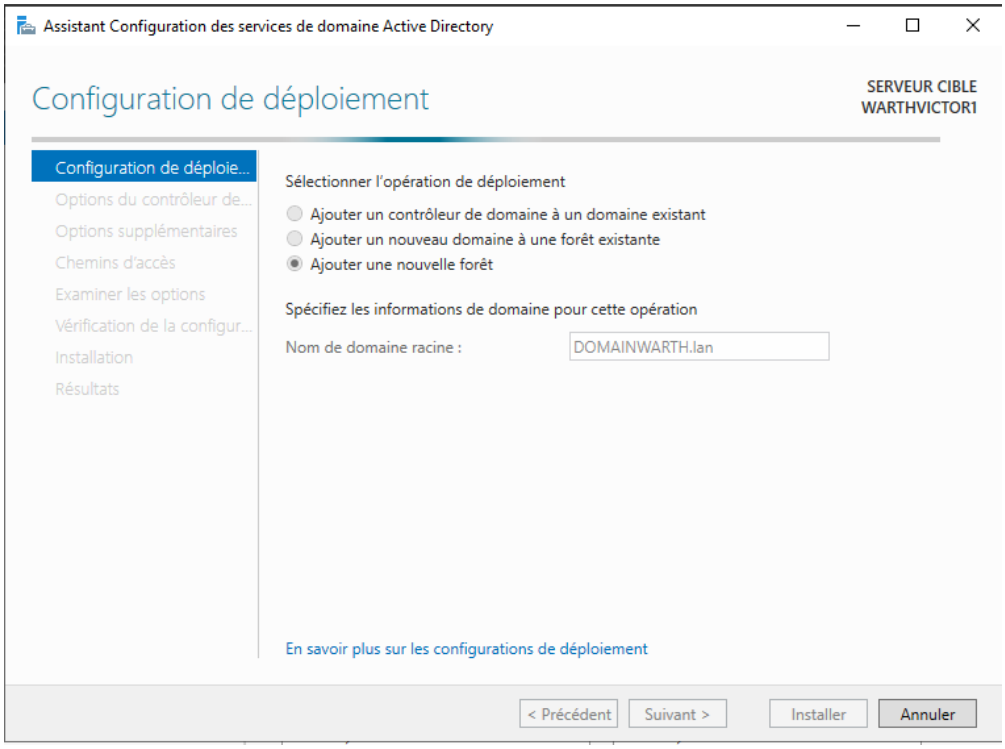
Mise en place d'une adresse IPv4 fixe avec les serveurs DNS appropriés :



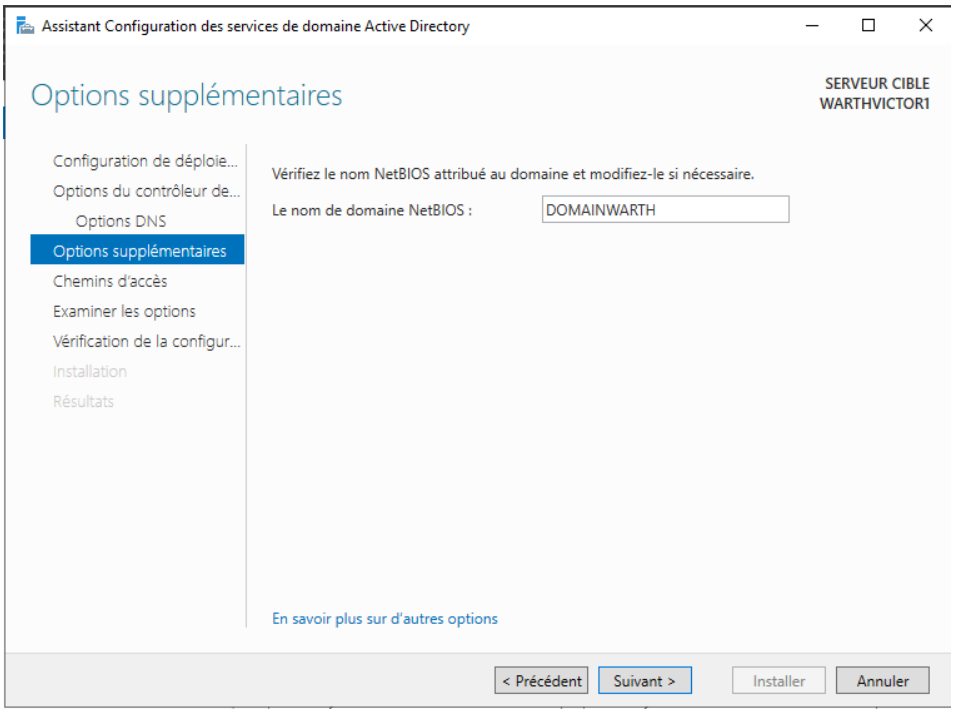
On installe l'AD DS et le DHCP sur ce serveur :



On créé une nouvelle forêt :

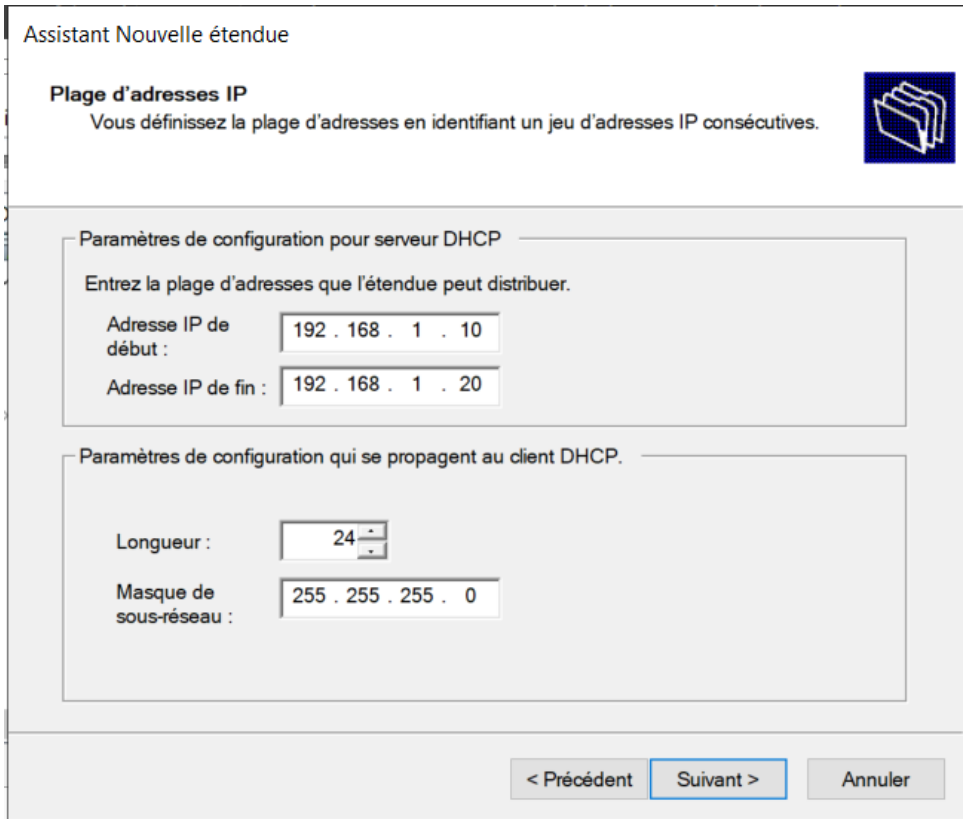


On vérifie le nom NetBIOS :

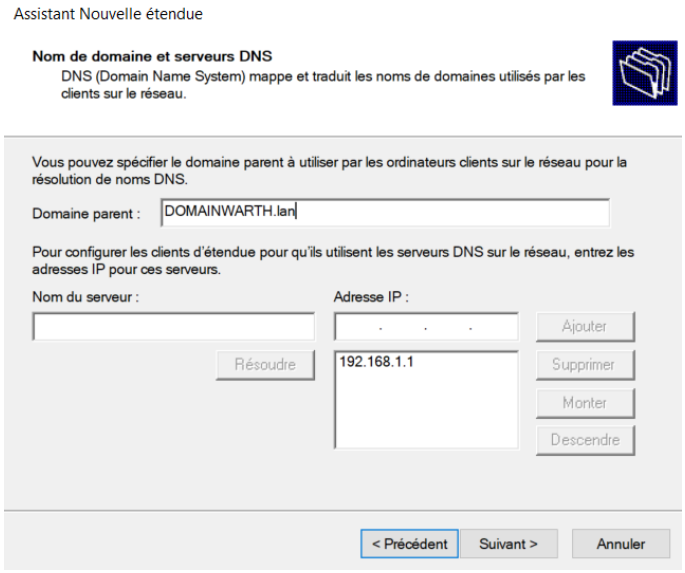


Ensuite, il faut terminer la config DHCP (laisser les options par défaut)

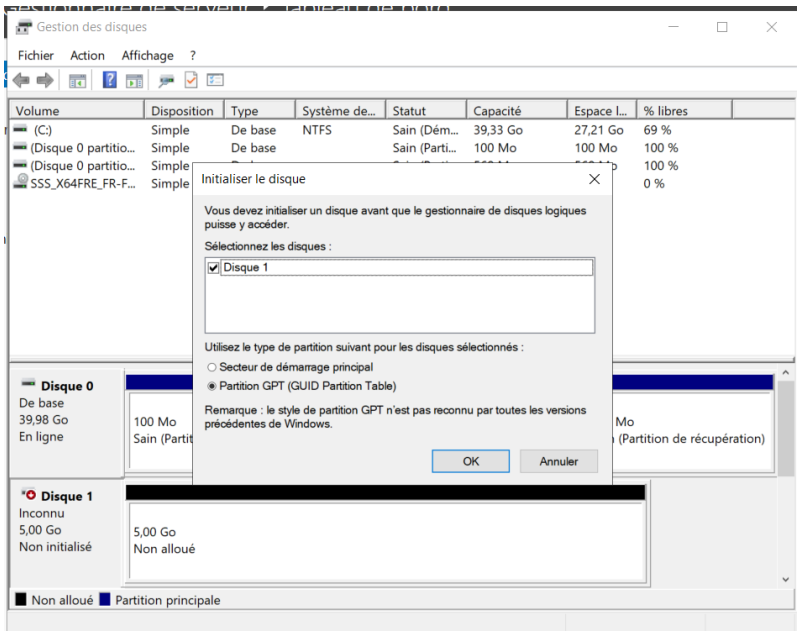
On configure une nouvelle étendue DHCP pour respecter le plan d'adressage :



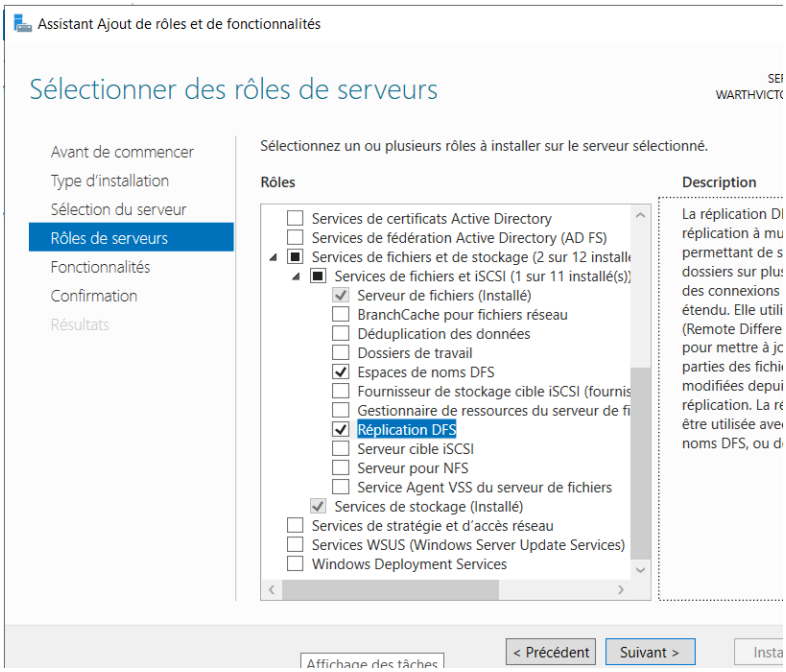
On configure dans un premier temps un seul serveur DNS (car pas encore de redondance) :



Ensuite on va installer DFS/R, on va déjà formater le disque correctement :

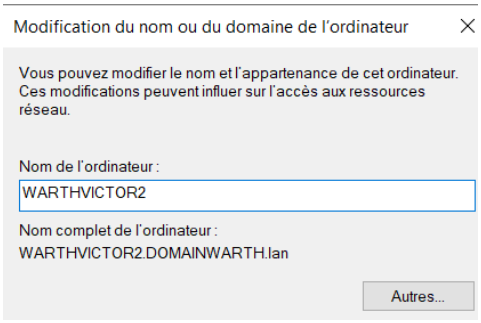


On ajoute les rôles Espaces de noms DFS et Réplication DFS

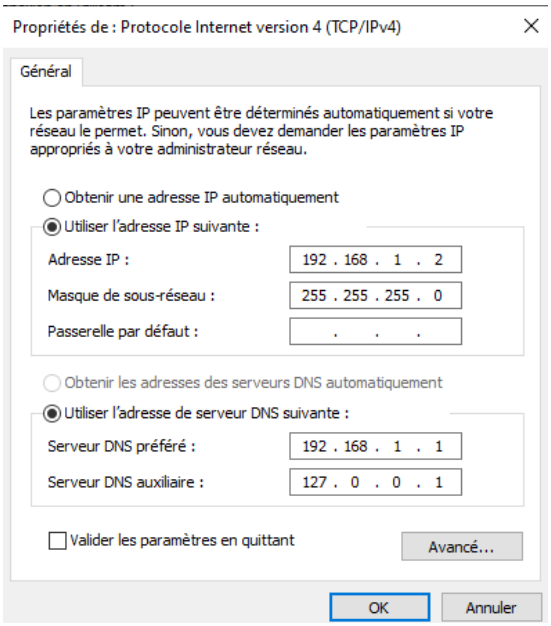


3.2.2. Paramétrage clé du deuxième Windows Serveur

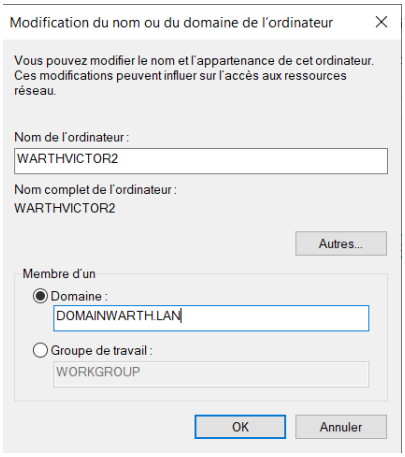
Modification du nom de mon serveur :



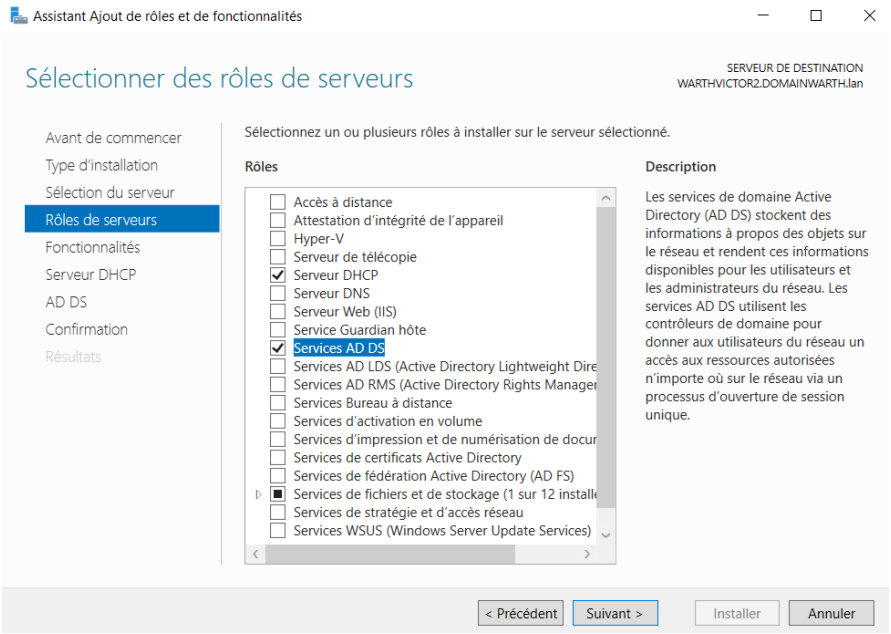
Mise en place d'une adresse IPv4 fixe avec les serveurs DNS appropriés :



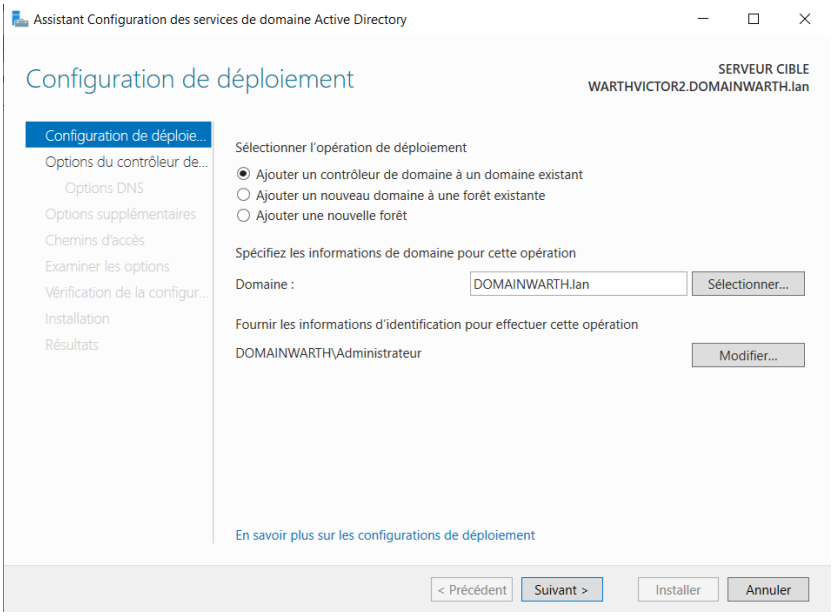
On ajoute le serveur au domaine :



On ajoute les rôles au deuxième serveur :

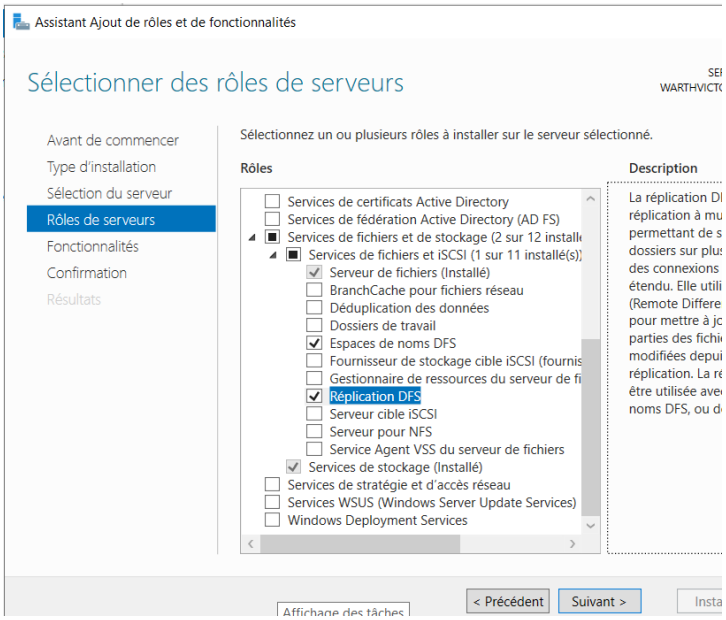


On configure l'AD DS en ajoutant le contrôleur de domaine au domaine précédemment créé

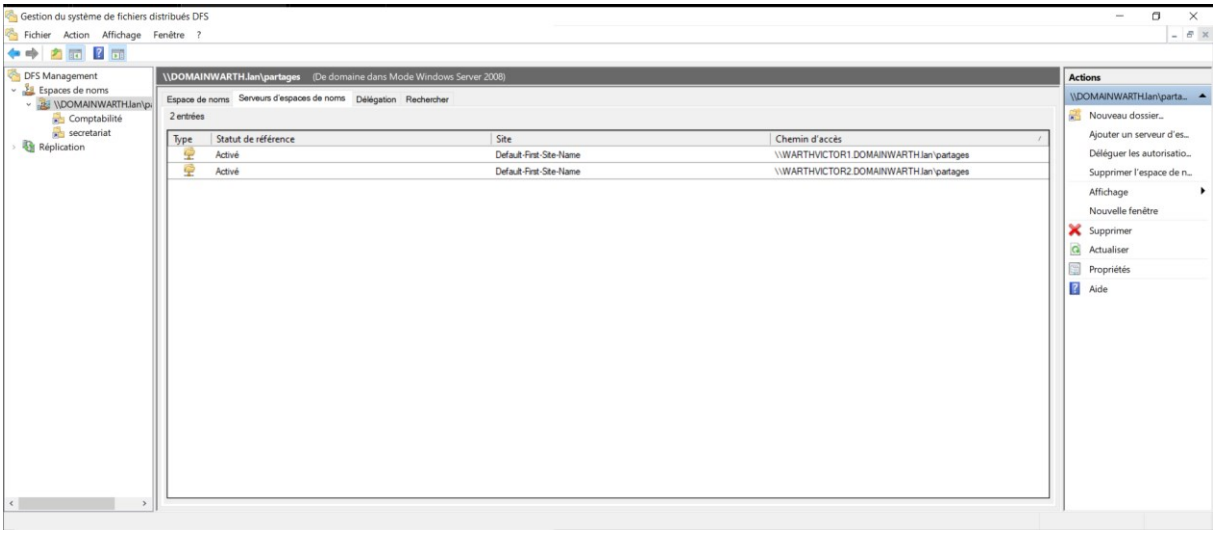


On laisse les options par défaut pour finir la config DHCP.

On ajoute les rôles Espaces de noms DFS et Réplication DFS

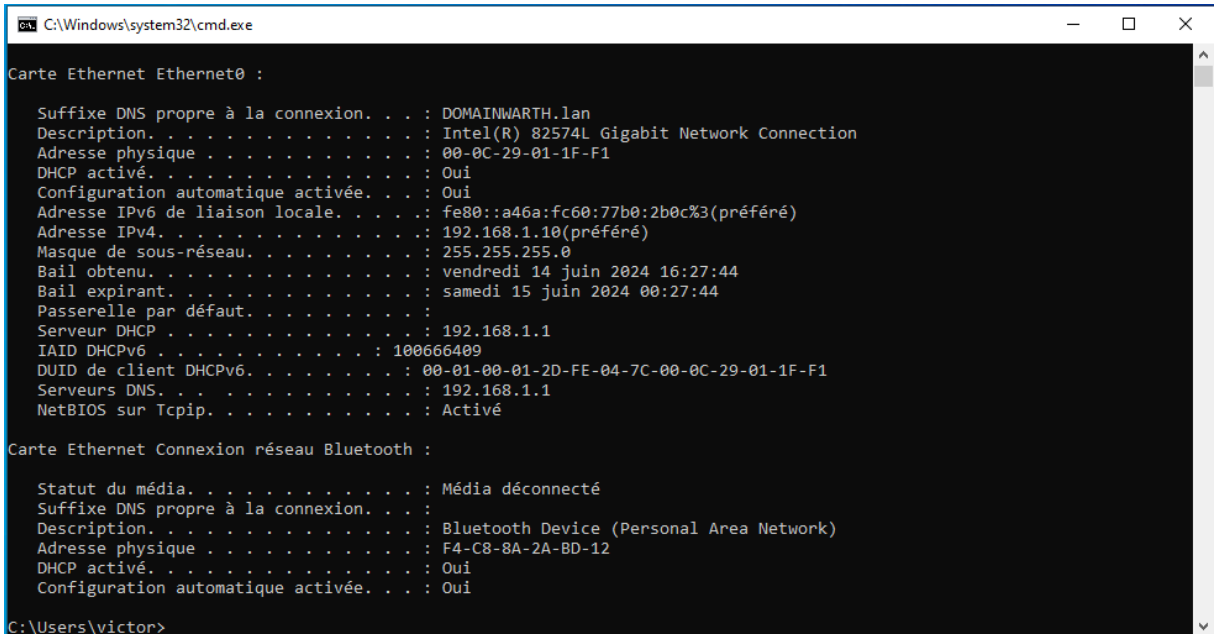


On configure l'espace de noms et les dossiers partagés :



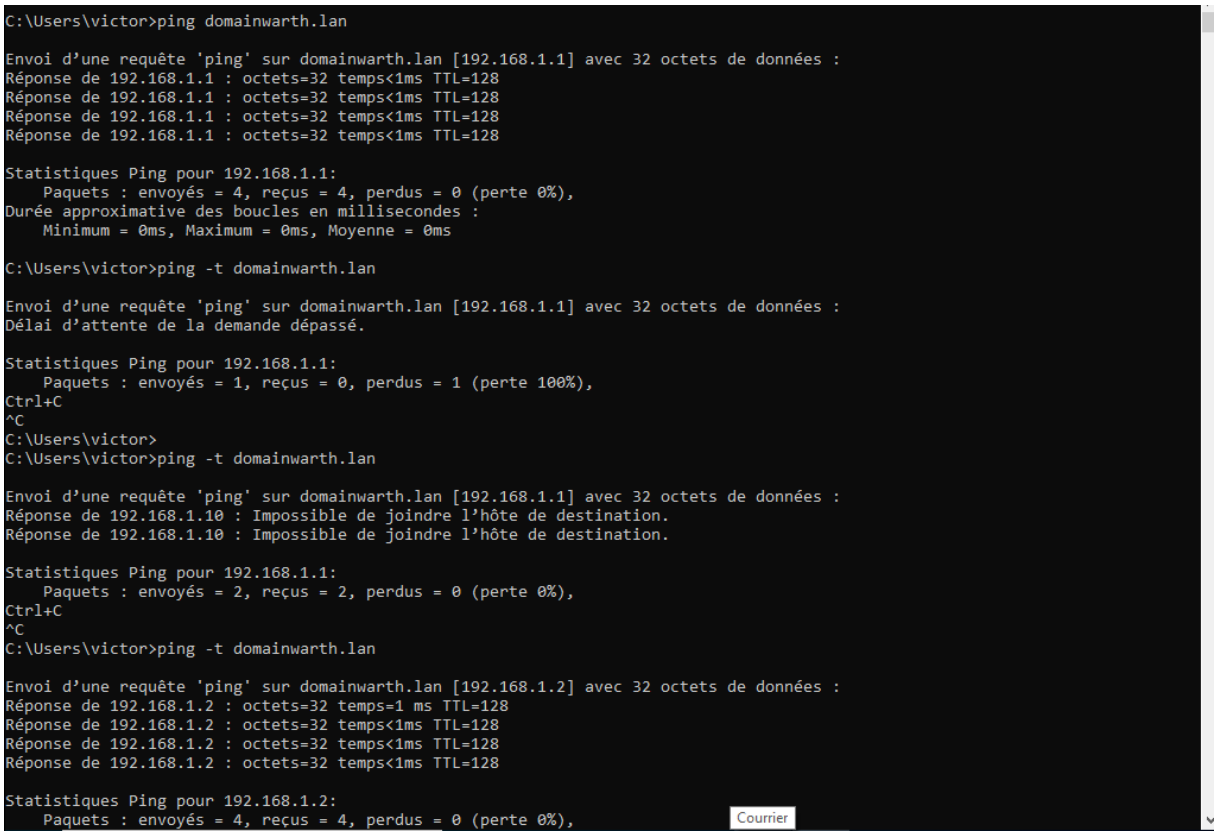
3.3. Vérification du fonctionnement

Le service DHCP fonctionne, on peut le voir en joignant un poste sur le réseau :

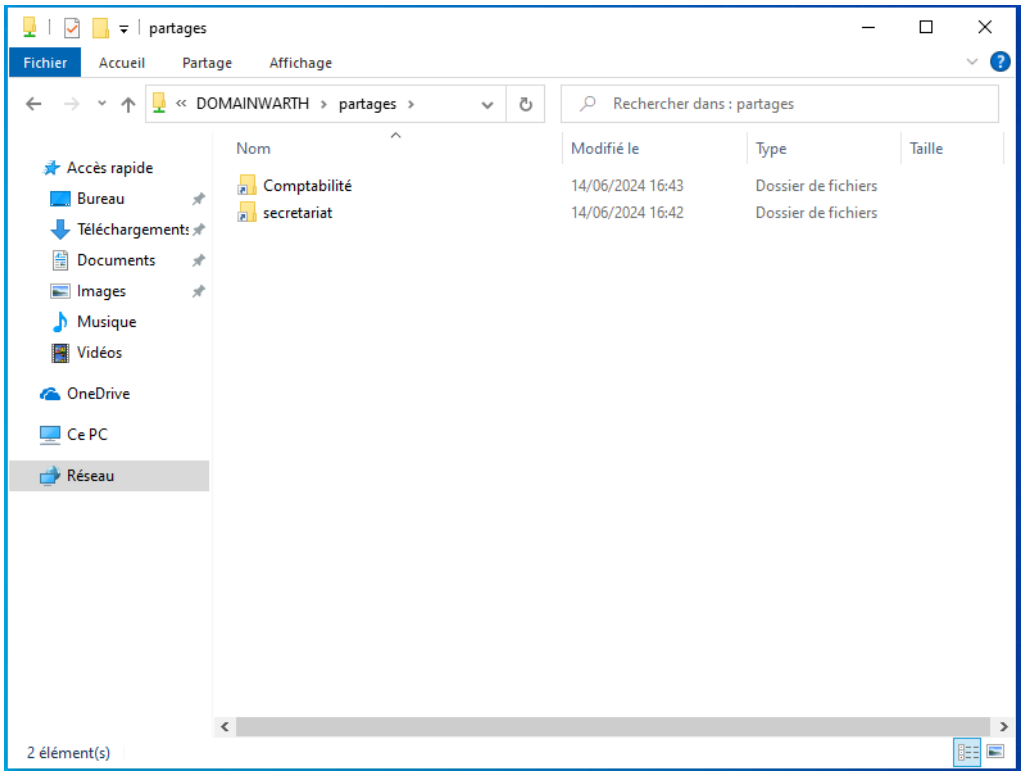


La bonne adresse IP est attribuée automatiquement, les serveurs DHCP et DNS remontent bien.

La redondance fonctionne correctement (on peut voir que le deuxième serveur prends bien le relais) :



Le DFS fonctionne correctement :


partages
Fichier
Accueil
Partage
Affichage
DOMAINWARTH › partages ›
Rechercher dans : partages
Accès rapide
Bureau
Téléchargements
Documents
Images
Musique
Vidéos
OneDrive
Ce PC
Réseau
Nom
Modifié le
Type
Taille
Comptabilité
14/06/2024 16:43
Dossier de fichiers
secretariat
14/06/2024 16:42
Dossier de fichiers
2 élément(s)