Mise en place d'un réseau sécurisé pour un projet d'école

Objectif du projet :

L’entreprise fictive "TechSolutions", une start-up de 5 employés spécialisée dans le développement web et mobile, souhaite moderniser son infrastructure informatique pour améliorer la sécurité et la performance de son réseau. En raison de contraintes budgétaires, elle veut limiter les coûts tout en adoptant les bonnes pratiques recommandées par l’ANSSI (Agence nationale de la sécurité des systèmes d'information).

L'objectif principal est de concevoir une infrastructure à la fois sécurisée et résiliente, capable de répondre aux besoins actuels tout en préparant le réseau à des éventuelles évolutions futures. Pour ce faire, quatre axes stratégiques ont été déterminés : la mise en place d'une architecture Active Directory répliquée, l'installation d'un service DNS et DHCP et l'installation d'un pare-feu sur DynFI, Voir schéma réseau annexe 1.

Afin de limiter l'impact financier, l'entreprise utilisera des solutions accessibles et des technologies bien éprouvées.

Pour ce faire, trois éléments clés sont mis en place :

- Un Active Directory répliqué permettant une gestion centralisée des utilisateurs et des ressources avec de bonnes pratiques de sécurité.
- Un service DNS et DHCP assurant une résolution efficace des noms de domaine internes et une distribution automatisée des adresses IP.
- Un pare-feu DynFI en réplication avec une adresse IP virtuelle pour garantir la continuité de service et sécuriser l’ensemble du réseau.

Infrastructure Active Directory avec DNS et DHCP

L’Active Directory (AD) sera déployé sur deux serveurs Windows Server 2022 afin d’assurer une haute disponibilité et une gestion centralisée des utilisateurs, des groupes et des ressources partagées. L’objectif est de garantir une administration fluide et un accès sécurisé aux services de l’entreprise.

Le premier serveur, AD01 (192.168.100.1/24), sera installé avec une interface graphique pour faciliter la gestion des objets Active Directory. Il servira de point principal pour les tâches administratives, notamment la gestion des utilisateurs, des stratégies de groupe (GPO) et des ressources réseau.

Le second serveur, AD02 (192.168.100.2/24), sera déployé en mode Core, une version allégée de Windows Server sans interface graphique. Ce choix technique repose sur plusieurs avantages significatifs. Premièrement, il réduit la surface d'attaque en limitant l'exposition aux vulnérabilités de l'interface utilisateur. Ensuite, il améliore la performance globale du serveur en libérant des ressources système qui peuvent être utilisées pour les tâches essentielles comme la réplication Active Directory et la gestion des requêtes réseau.

Les deux contrôleurs de domaine seront configurés pour assurer une réplication automatique et bidirectionnelle des données Active Directory. En cas de panne d'AD01, AD02 prendra immédiatement le relais pour éviter toute interruption des services. De plus, la répartition des rôles FSMO (Flexible Single Master Operation) entre les deux serveurs garantira une meilleure tolérance aux pannes et une gestion optimale des opérations critiques d'Active Directory.

Fonctionnalités essentielles : DNS et DHCP

Le service DNS sera installé sur les deux contrôleurs de domaine afin de permettre la résolution des noms de domaine internes de manière rapide et efficace. Cette configuration assure également une réplication automatique des enregistrements DNS, garantissant ainsi une continuité de service même en cas de défaillance d'un des serveurs. Le DNS est indispensable au bon fonctionnement d'Active Directory, car il permet aux machines du réseau de localiser les contrôleurs de domaine et d'accéder aux ressources partagées sans difficultés.

Le DHCP, quant à lui, sera mis en place sur AD01 pour attribuer automatiquement les adresses IP aux postes clients et aux équipements du réseau. Une configuration de secours sur AD02 permettra d'assurer la continuité du service en cas d'indisponibilité du serveur principal. Des règles de réservation d'adresses IP seront définies pour les équipements critiques comme les serveurs et les pare-feu afin d'éviter toute interruption de service.

Afin d'optimiser la sécurité et la gestion des postes de travail, des bonnes pratiques Active Directory seront appliquées. Cela inclut :

- Création de multiples Unités Organisationnelles (OU) afin d'organiser les objets Active Directory de manière structurée (Utilisateurs, Groupes, Ordinateurs, Serveurs). Cette séparation facilite la gestion et l'application des stratégies de sécurité.
- Activation de la corbeille Active Directory, permettant de restaurer facilement des objets supprimés par erreur sans nécessiter de restauration complète du serveur.
- Désactivation de la délégation des comptes administrateurs afin de limiter les accès critiques et d'éviter qu'un utilisateur malveillant puisse escalader ses privilèges.
- Suppression des permissions d'ajout automatique dans le DNS pour empêcher les utilisateurs non autorisés d'introduire des enregistrements DNS pouvant compromettre le bon fonctionnement du réseau.

- Changement du nom par défaut de "Default-First-Site-Name", une modification essentielle pour personnaliser l’environnement Active Directory et mieux organiser la gestion des sites AD.
- Déclaration des sous-réseaux utilisés afin d’optimiser la gestion des sites Active Directory et d’améliorer la découverte des contrôleurs de domaine par les clients.
- Désactivation du spouleur d’impression afin de limiter les risques liés aux vulnérabilités de ce service.
- Séparation des rôles FSMO (Flexible Single Master Operation) entre les deux contrôleurs de domaine pour répartir la charge et éviter tout point de défaillance unique.

Active Directory repose sur cinq rôles FSMO essentiels à son bon fonctionnement. Ces rôles sont répartis sur les contrôleurs de domaine pour assurer une redondance et éviter tout point unique de défaillance. Voici les cinq rôles FSMO et leur importance :

Schema Master : Responsable des modifications du schéma AD, ce rôle doit être unique dans la forêt.

Domain Naming Master : Gère l'ajout et la suppression de domaines dans la forêt AD.

RID Master : Fournit des identifiants uniques aux objets créés dans le domaine.

PDC Emulator : Assure la synchronisation des horloges, la gestion des mots de passe et le support des anciennes versions de Windows.

Infrastructure Master : Maintient les relations inter-domaines et met à jour les références entre objets.

Sécurisation du réseau avec DynFI

La mise en place d’un pare-feu performant est indispensable pour protéger l’entreprise contre les menaces extérieures et contrôler le trafic réseau. Pour ce projet, la solution open source française Dynfi a été retenue en raison de sa robustesse, de sa facilité de gestion et de ses fonctionnalités avancées en matière de filtrage et de détection d’intrusions.

Dynfi n’est pas seulement un simple pare-feu, mais un UTM (Unified Threat Management), c’est-à-dire une solution de sécurité tout-en-un qui regroupe plusieurs fonctionnalités avancées pour protéger l’infrastructure informatique de TechSolutions. Contrairement à un pare-feu classique qui se limite à filtrer le trafic réseau, un UTM comme Dynfi intègre plusieurs couches de protection pour détecter, analyser et bloquer les menaces en temps réel.

Les principales fonctionnalités de DynFI incluent :

1. Filtrage du trafic réseau : Blocage des connexions non autorisées, limitation des flux indésirables et application de politiques de sécurité strictes pour contrôler les accès internes et externes.
2. Gestion des VPN : Il permet de sécuriser les connexions à distance des employés en télétravail ou des prestataires en utilisant des tunnels chiffrés.
3. Contrôle applicatif : Possibilité de restreindre l'utilisation de certaines applications ou services en fonction des règles établies.
4. Journalisation et supervision avancée : DynFI fournit des logs détaillés sur toutes les activités réseau, facilitant l'analyse des incidents de sécurité et le suivi des performances.
5. Filtrage web et protection contre les malwares : Capacité d'empêcher l'accès à des sites malveillants et de limiter l'exposition aux logiciels malveillants.

Dans l'architecture de TechSolutions, DynFI joue un rôle essentiel en tant que barrière de sécurité entre le réseau interne et Internet, en filtrant et en surveillant toutes les connexions entrantes et sortantes.

Architecture du pare-feu DynFI

L'un des aspects les plus critiques de la cybersécurité est la haute disponibilité. Un seul point de défaillance, comme un pare-feu unique, peut rendre l'entreprise vulnérable en cas de panne ou d'attaque. C'est pourquoi il est indispensable de mettre en place deux instances DynFI en réplication, garantissant ainsi une continuité de service sans interruption.

- DynFI-01 (192.168.100.253/24) sera le pare-feu principal, connecté à la fois au réseau interne (LAN), au réseau utilisateurs (OPT1) et à Internet (WAN).
- DynFI-02 (192.168.100.252/24) sera son serveur de secours, en réplication constante avec le premier.
- Une adresse IP virtuelle en CARP (192.168.100.254/24) sera mise en place pour permettre une bascule automatique entre les deux pare-feux en cas de panne.

Le protocole CARP (Common Address Redundancy Protocol) est un protocole réseau qui permet à plusieurs machines sur un même réseau local de partager une adresse IP virtuelle

L'utilisation d'une adresse IP virtuelle CARP est cruciale pour garantir la continuité du service. Grâce à cette configuration, tous les équipements du réseau interne continueront d'accéder à Internet et aux services de l'entreprise sans interruption, même si l'un des pare-feux tombe en panne. Cette approche évite également de devoir modifier la configuration réseau des clients en cas de changement du pare-feu actif.

Fonctionnalités de sécurité

Les pare-feux DynFI seront configurés pour bloquer toutes les connexions par défaut. Seules celles nécessaires au bon fonctionnement du réseau seront ouvertes, garantissant ainsi une sécurité renforcée

Conclusion

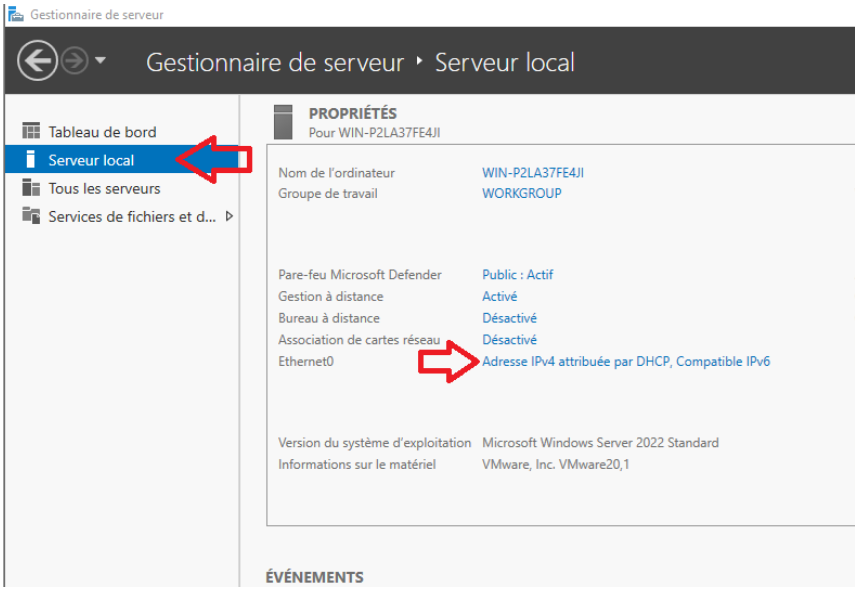
Avec cette infrastructure, TechSolutions bénéficiera d'un réseau performant, sécurisé et évolutif. L'Active Directory permettra une gestion centralisée et sécurisée des utilisateurs et des ressources, tandis que l'architecture DNS et DHCP assurera une distribution efficace des adresses IP et une résolution rapide des noms de domaine internes. L'ajout des UTM DynFI, avec leur configuration redondante et leur IP virtuelle, garantira une protection optimale du réseau contre les cybermenaces et assurera la continuité des services en cas de panne.

Cette mise en place représente un équilibre optimal entre sécurité, résilience et coût maîtrisé, garantissant ainsi une infrastructure fiable et pérenne pour l'entreprise.

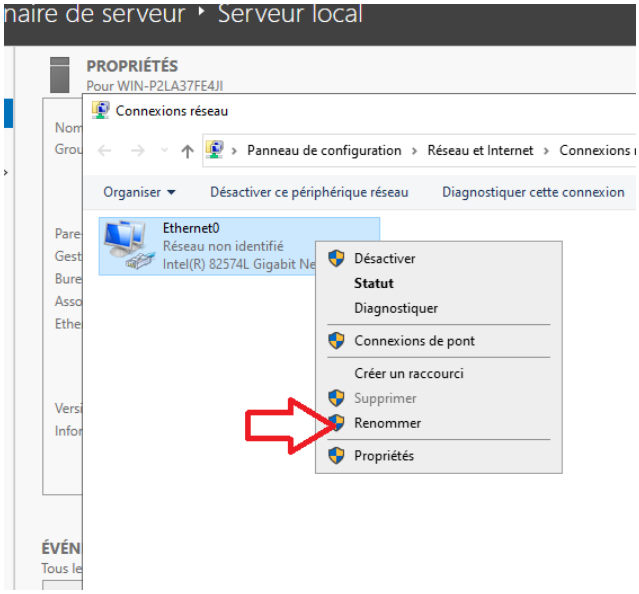
Installation et configuration de l'AD01

Après avoir injecté l'ISO de Windows Server 2022 sur un hyperviseur et lancé l'installation, nous arrivons sur une page permettant de sélectionner la langue du système.

Une fois cette étape validée, nous cliquons sur "Suivant", puis sur "Reporter à plus tard" avant de définir le mot de passe du compte administrateur du contrôleur de domaine. Une fois connecté au serveur, nous accédons au Gestionnaire de serveur afin de configurer la carte réseau, notamment en modifiant son nom et en définissant une adresse IP statique. Pour ce faire, nous suivons le chemin permettant d'accéder aux paramètres d'adressage IP du serveur.

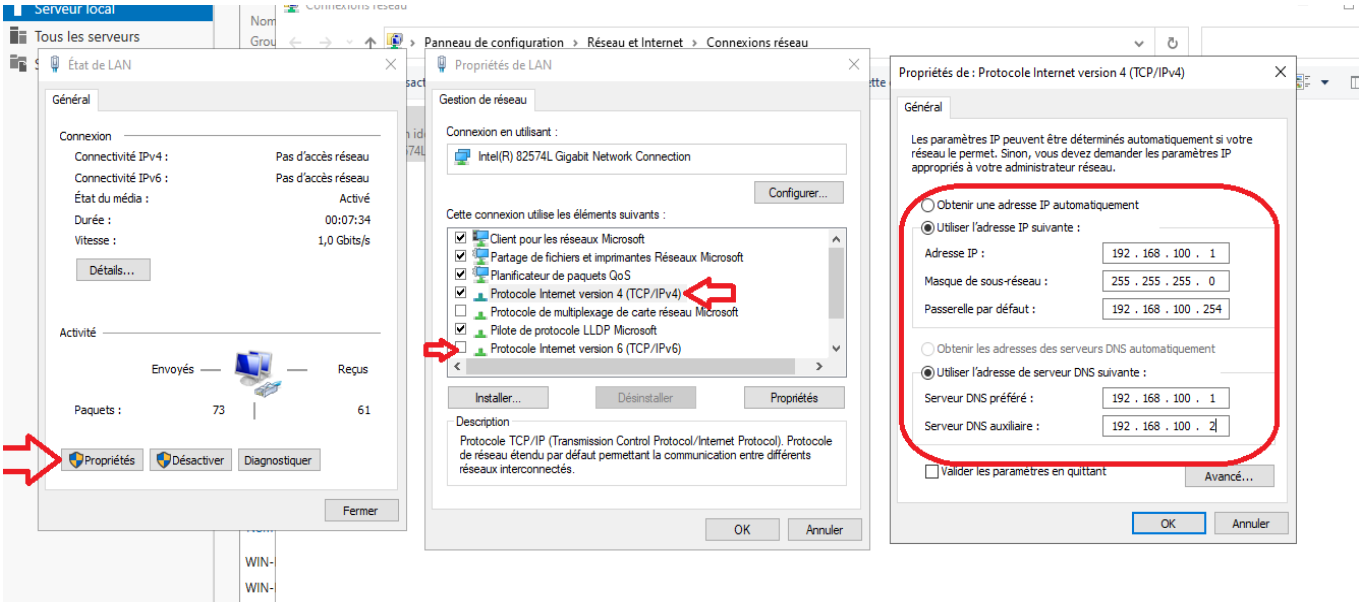


La première étape consiste à renommer la carte réseau en "LAN" pour une identification plus claire.

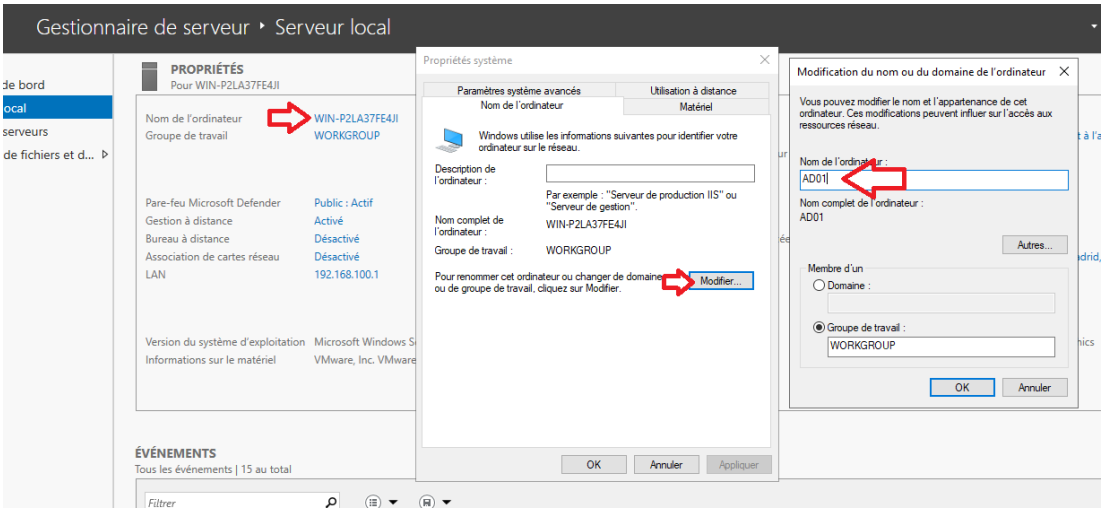


Nous procéderons ensuite à la configuration de l'adresse IP en la définissant sur 192.168.100.1/24. La passerelle par défaut sera fixée à 192.168.100.254, correspondant à l'adresse de nos pare-feu.

Concernant les serveurs DNS, nous utiliserons 127.0.0.1 (localhost) et 192.168.100.2, qui représenteront les deux contrôleurs de domaine responsables de la réplication DNS.

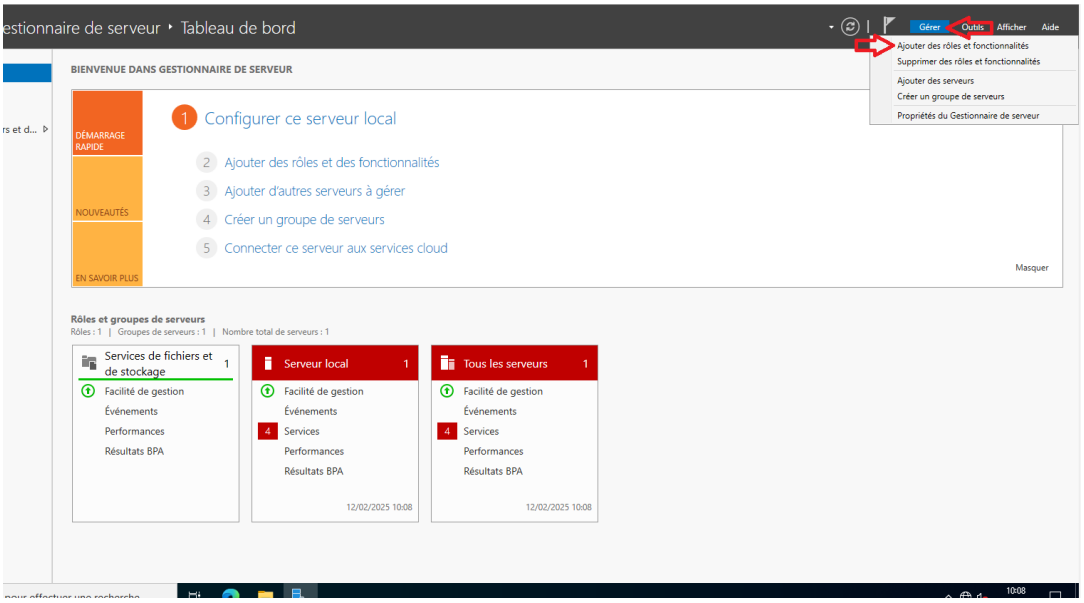


Une fois ces modifications appliquées, nous rouvrirons le Gestionnaire de serveur, puis nous accéderons à la section "Serveur local" afin de renommer la machine.

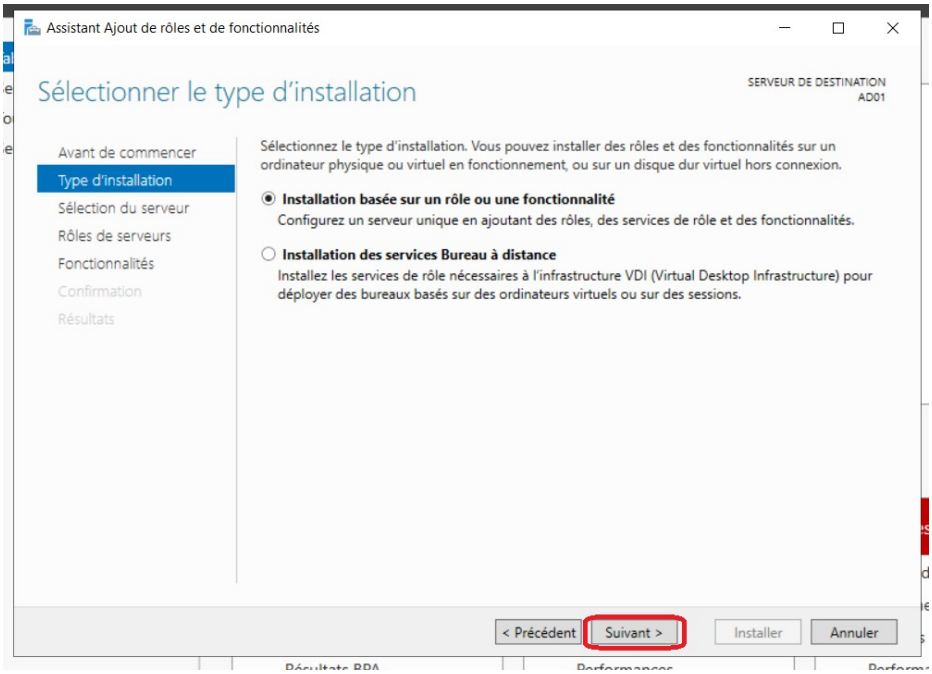


Il suffira alors de cliquer sur "Modifier", d'entrer le nouveau nom, puis de valider en cliquant sur "OK". Pour que le changement de nom soit pris en compte, un redémarrage du serveur est nécessaire.

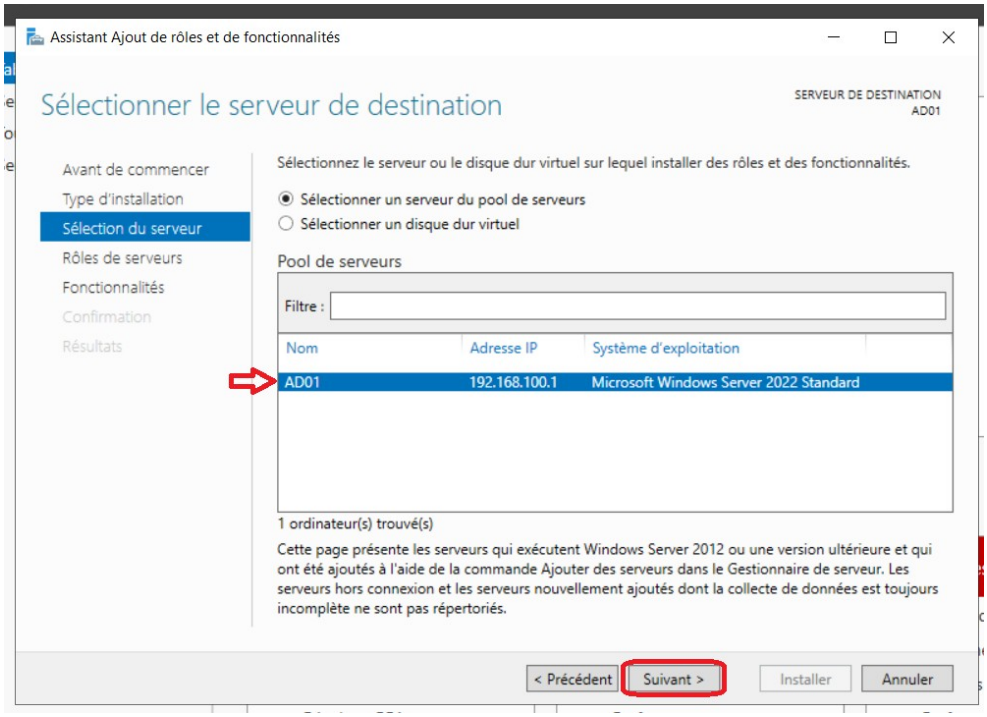
Afin d'ajouter des rôles et des fonctionnalités au serveur, nous devons retourner dans le Gestionnaire de serveur. En haut à droite de la fenêtre, nous cliquerons sur "Gérer", puis sélectionnerons l'option "Ajouter des rôles et fonctionnalités".



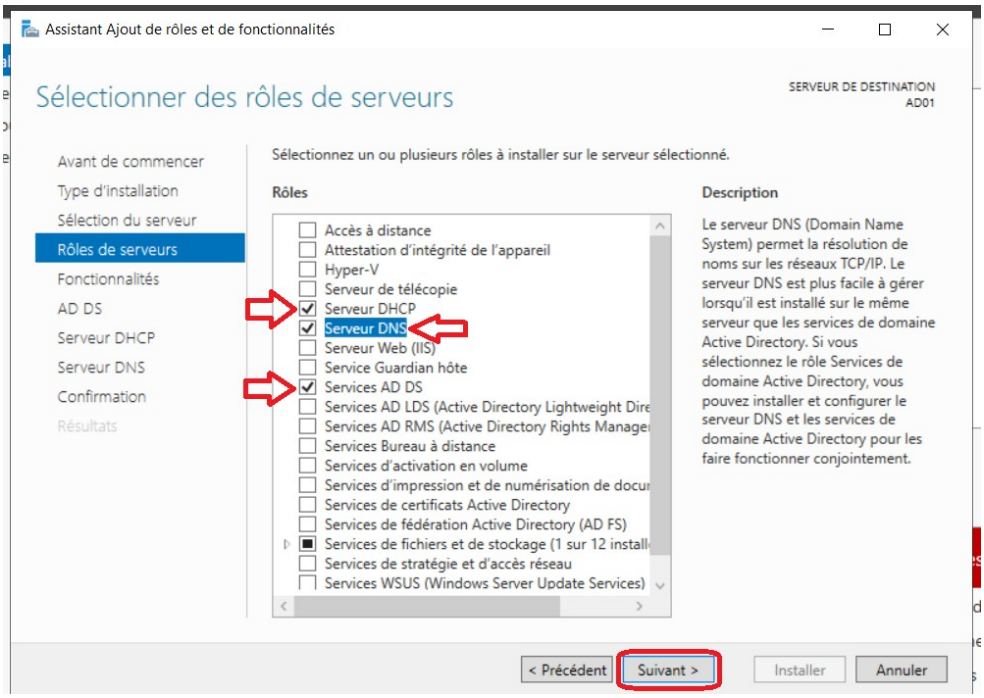
Une fois l'assistant d'installation lancé, nous cliquerons sur "Suivant" pour poursuivre le processus. Nous choisirons ensuite l'option "Installation basée sur un rôle ou une fonctionnalité" afin de configurer les services nécessaires.



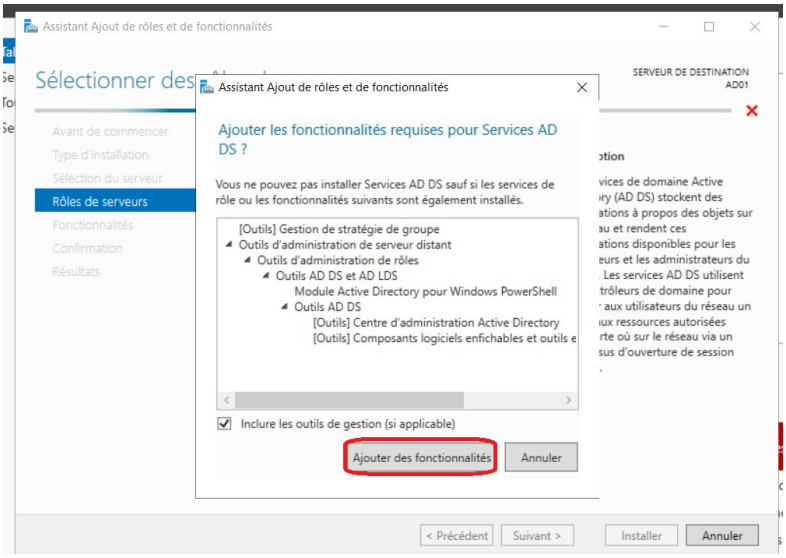
Puis nous sélectionnerons le serveur concerné.



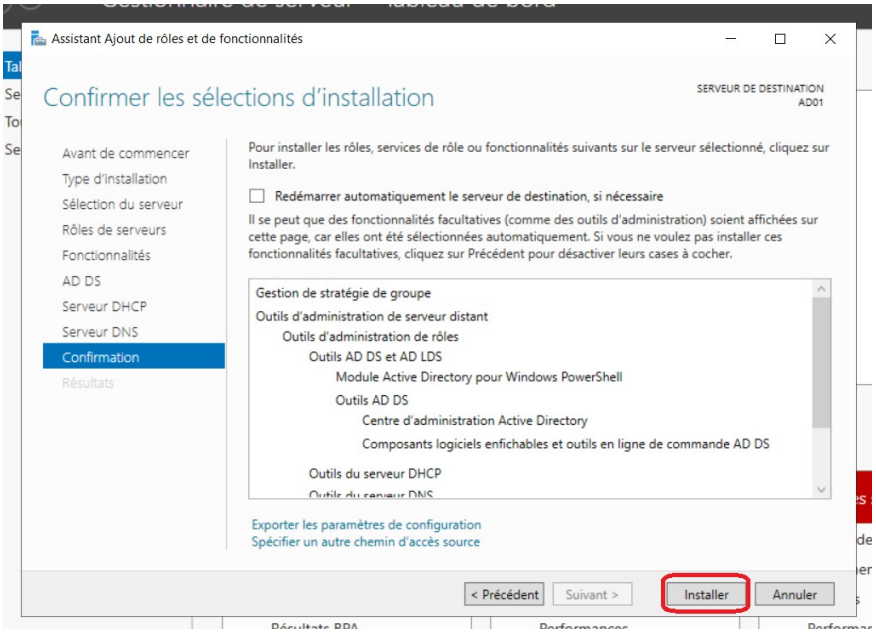
À l’étape de sélection des rôles et fonctionnalités, nous ajouterons ceux nécessaires au bon fonctionnement de notre infrastructure. AD DS, DHCP et DNS



Une fenêtre s’affichera alors, proposant d’ajouter des fonctionnalités complémentaires. Il suffira de cliquer sur "Ajouter des fonctionnalités" pour valider cette étape.

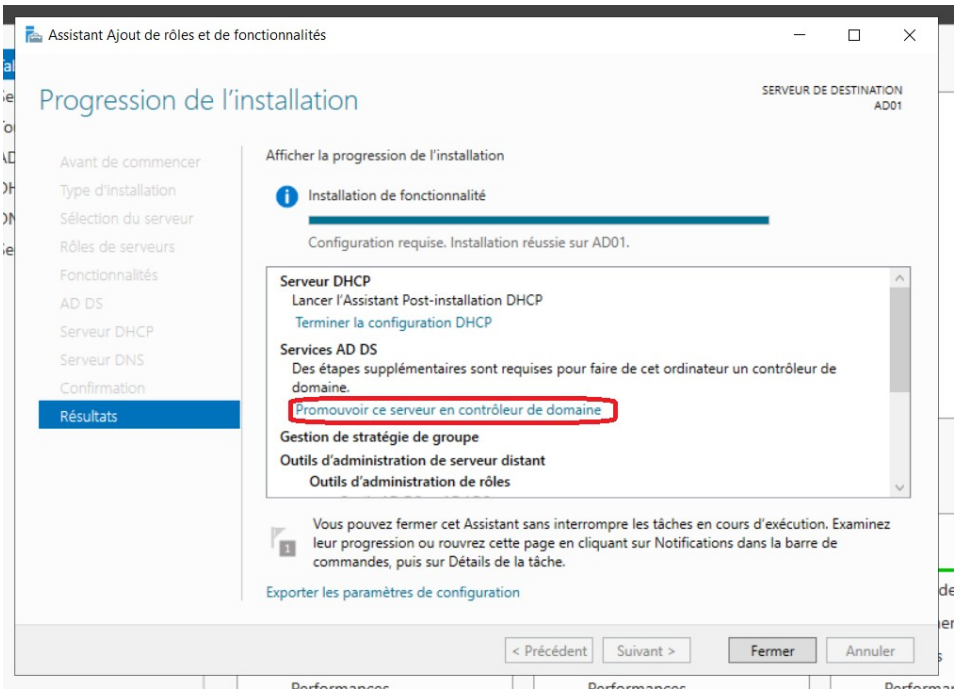


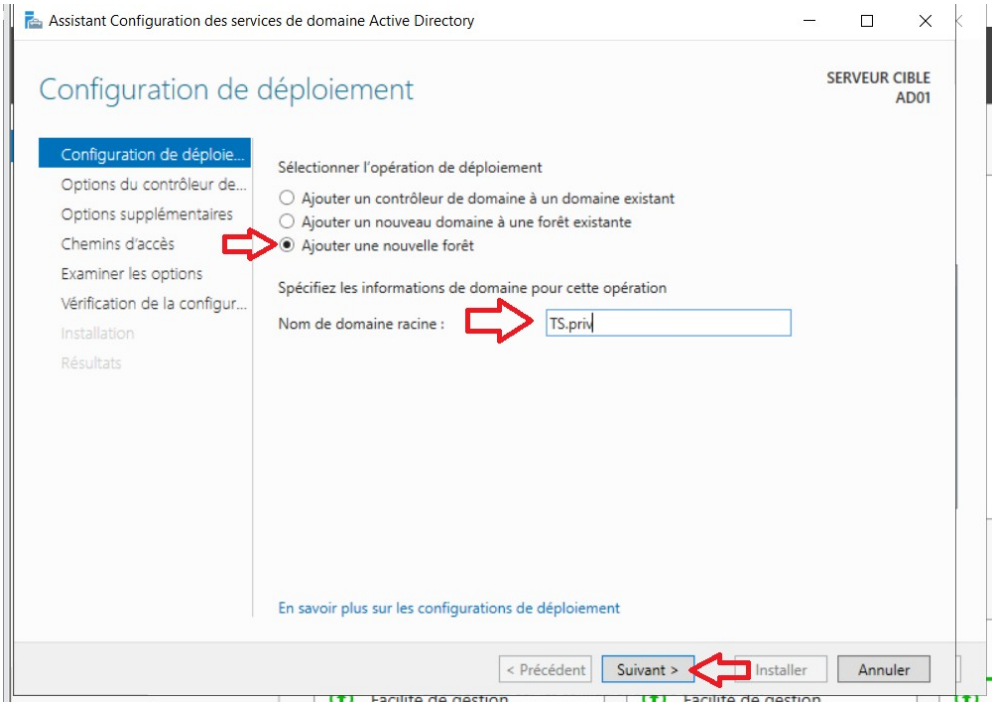
Les quatre écrans suivants de l'assistant d'installation seront validés en cliquant sur "Suivant" jusqu'à l'affichage de la page récapitulative. Une fois les rôles et fonctionnalités confirmés, nous pourrons lancer l'installation.



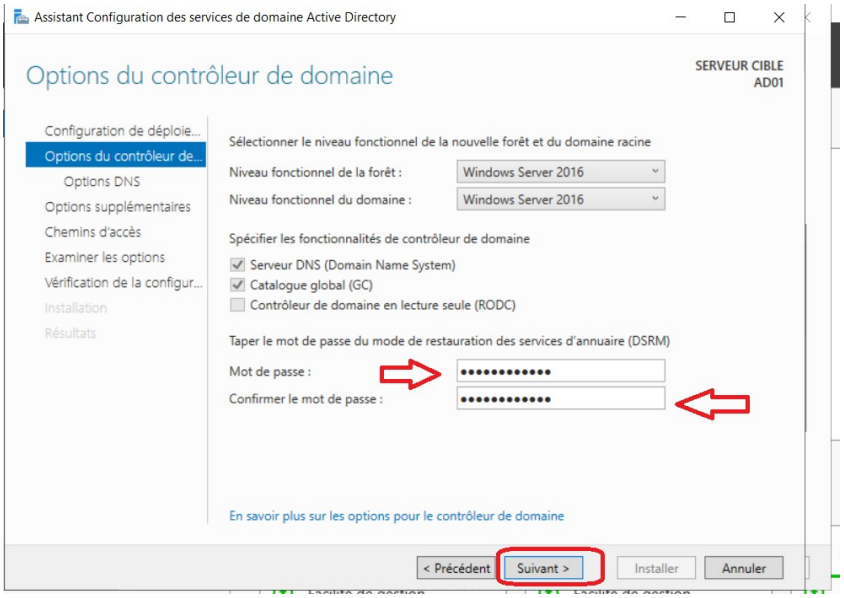
Une fois l'installation terminée, nous allons promouvoir ce serveur en tant que contrôleur de domaine.

Configuration de l'Active Directory :

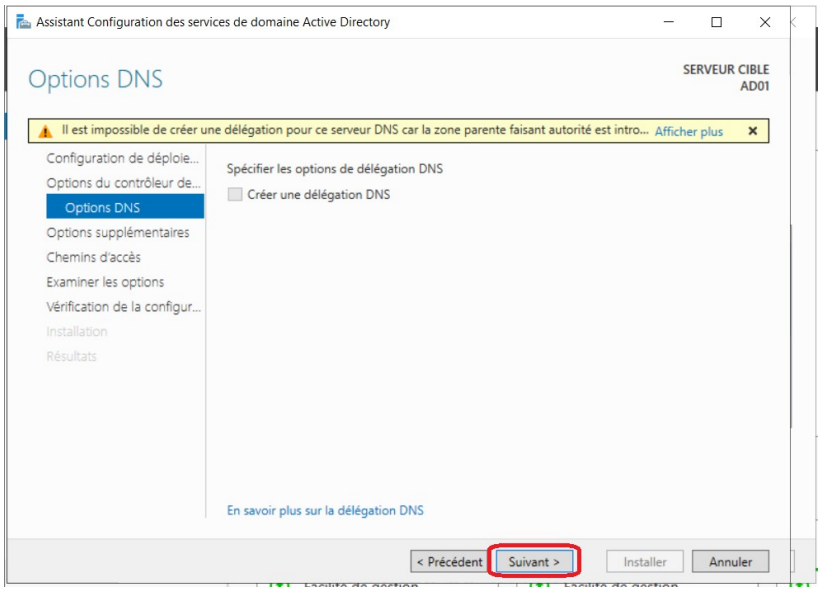




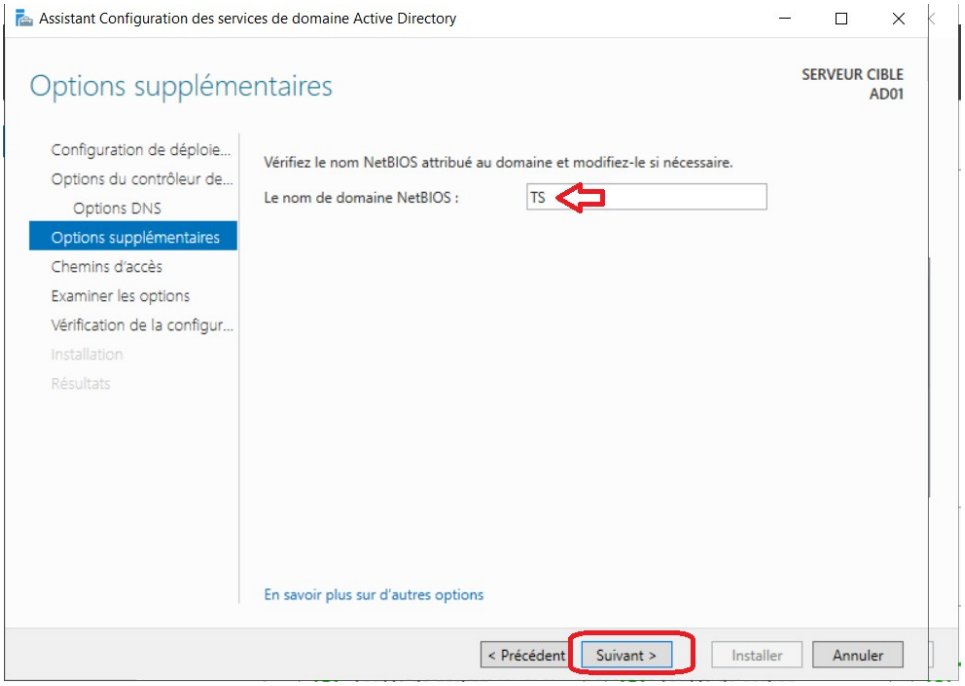
Dans la fenêtre qui s'affiche, nous sélectionnerons l'option "Ajouter une nouvelle forêt" et définirons le nom de domaine, qui sera "TS.priv" dans notre cas pour "**T**ech**S**olutions". Ensuite, nous saisirons un mot de passe pour le mode de restauration.



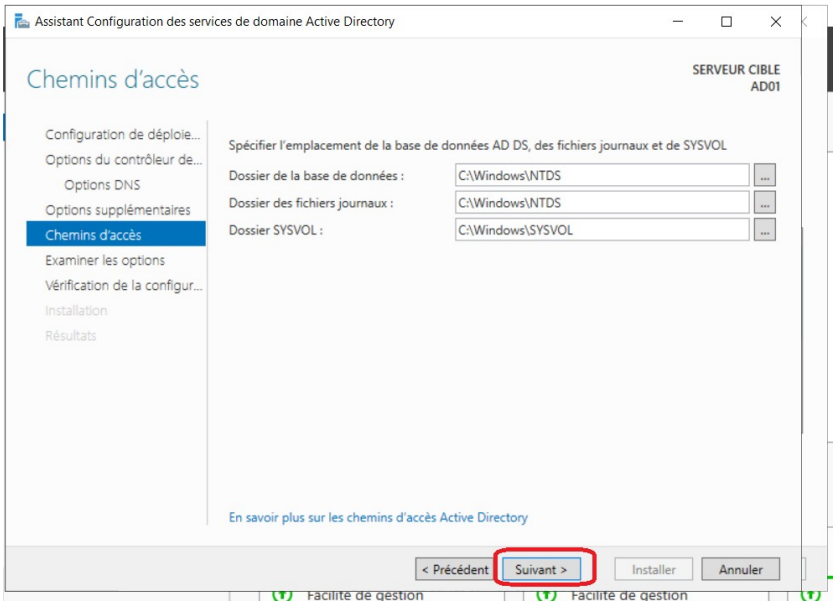
Pour la configuration DNS, nous choisirons de ne pas créer de délégation DNS.



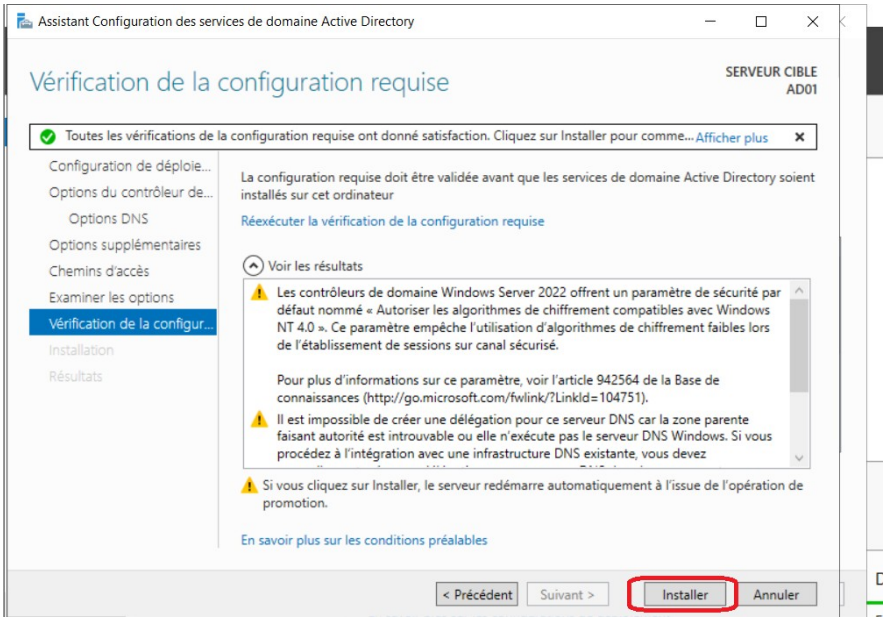
Dans les options supplémentaires, nous pourrons vérifier que le nom NetBIOS est pré-rempli. Dans notre cas, nous le laisserons tel quel, sous la forme "TS".



Concernant les fichiers d'installation, pour une meilleure organisation et clarté, nous allons modifier l'emplacement des journaux dans "C:\Windows\journaux", on clique sur Suivant



Une page récapitulative affichera l'ensemble des configurations effectuées avant de nous permettre de lancer l'installation.



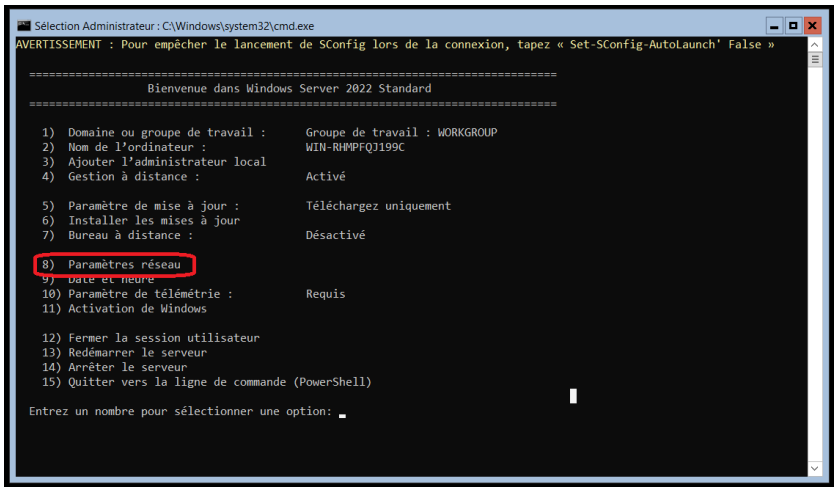
Une fois le processus achevé, le serveur redémarrera automatiquement.

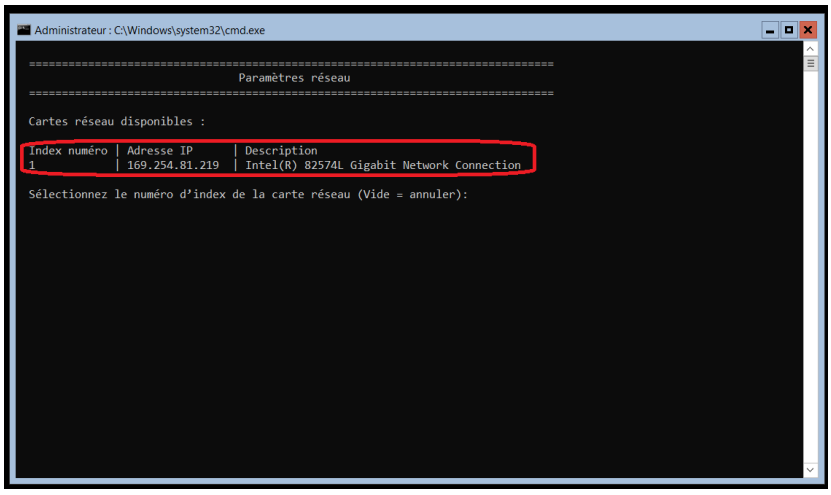
Une fois le serveur redémarré, une notification apparaîtra dans le Gestionnaire de serveur sous le drapeau de notification. Avant de procéder à la configuration du DHCP, nous allons créer un second contrôleur de domaine, "AD02", en mode CORE et le mettre en réplication avec "AD01".

Pour cela, nous installerons la version de Windows Server sans interface graphique. Une fois l'installation terminée, nous accéderons à l'interface Sconfig.

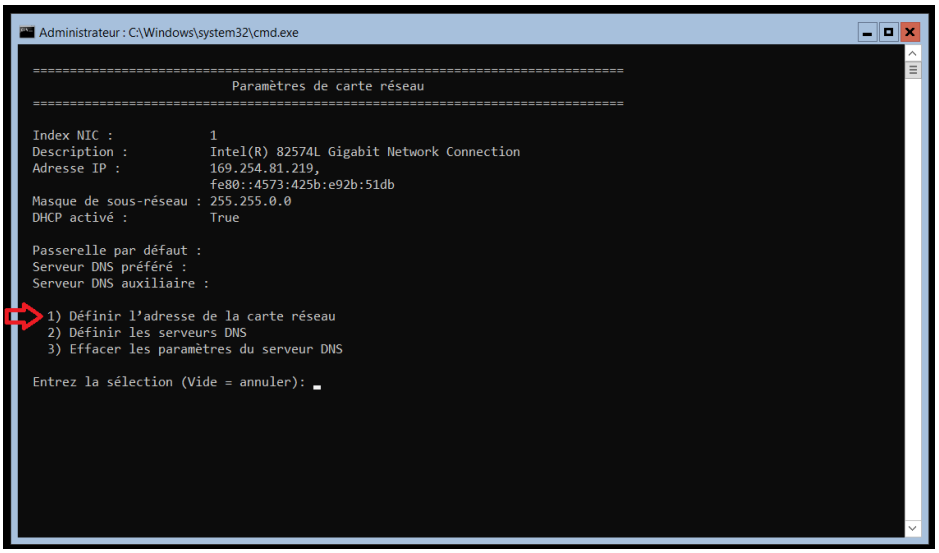
Configuration de l'AD02 en mode CORE et mise en réplication sur AD01 :

Nous allons commencer par configurer l'adresse IP du serveur en accédant au menu de configuration et en sélectionnant l'option 8. Cette étape est essentielle, car elle nous permettra de joindre le serveur au domaine afin de pouvoir configurer AD02 sur AD01.

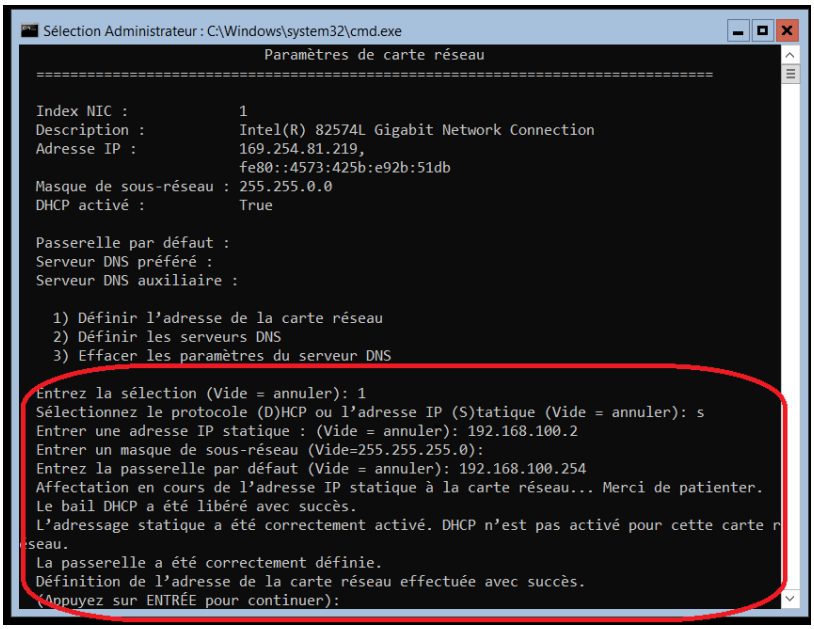




Dans notre cas, une seule carte réseau est disponible, nous veillerons donc à sélectionner le bon index correspondant à cette carte. Une fois cette sélection effectuée.



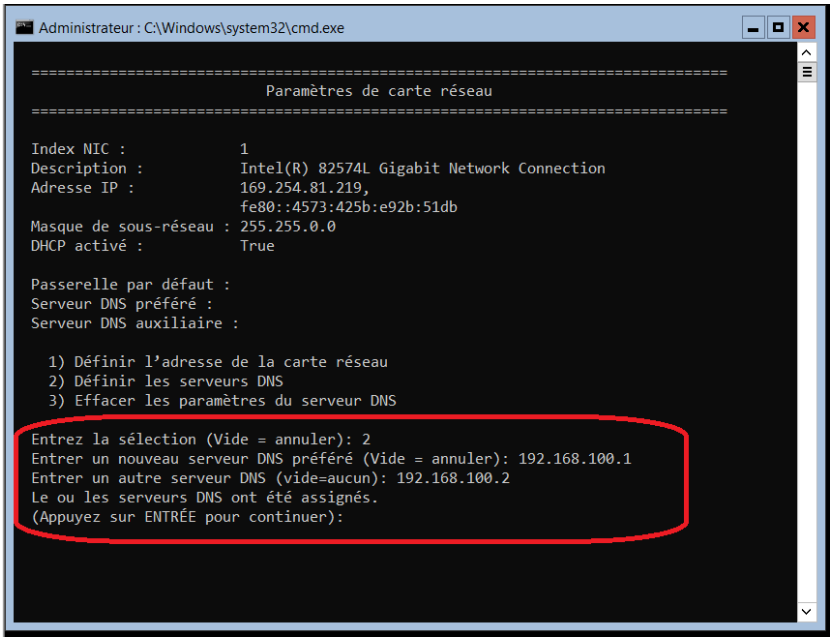
Nous choisirons l'option 1 afin de définir l'adresse IP du serveur.



Nous attribuerons ensuite une adresse IP statique au serveur. L'adresse choisie sera 192.168.100.2, tandis que le masque de sous-réseau sera laissé vide, correspondant par défaut à 255.255.255.0. La passerelle sera définie sur 192.168.100.254, correspondant à nos pare-feu.

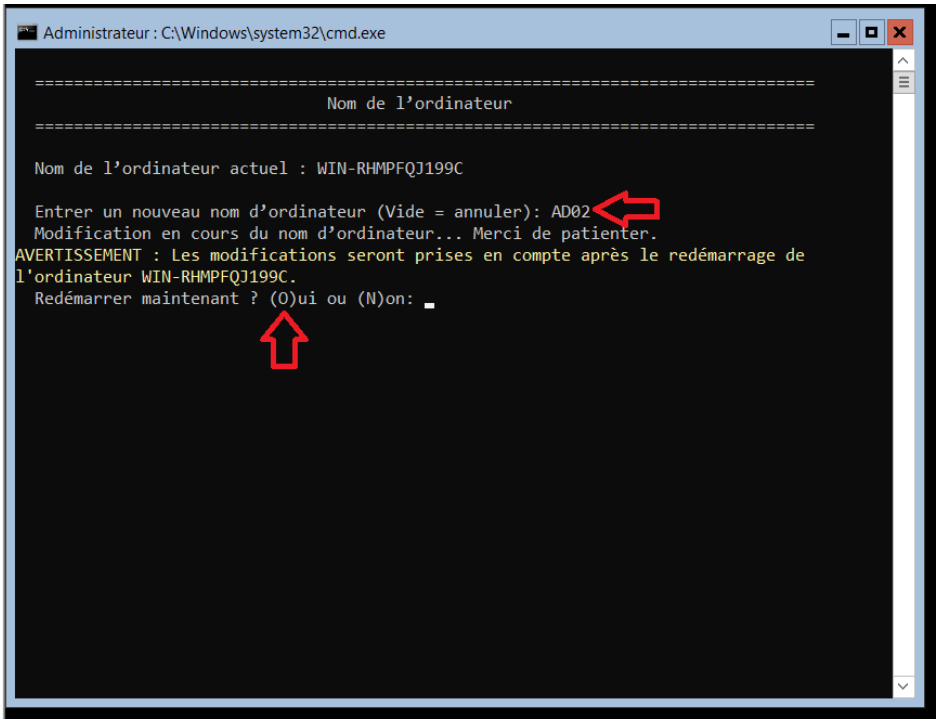
Une fois ces paramètres appliqués, nous vérifierons que la configuration a bien été prise en compte et qu'aucune erreur n'est signalée.

Nous procéderons ensuite à la pré configuration des serveurs DNS en utilisant les adresses 192.168.100.1 et 127.0.0.1. Pour cela, nous retournerons dans la configuration de la carte réseau et sélectionnerons l'option 2, qui permet de définir manuellement les adresses DNS.



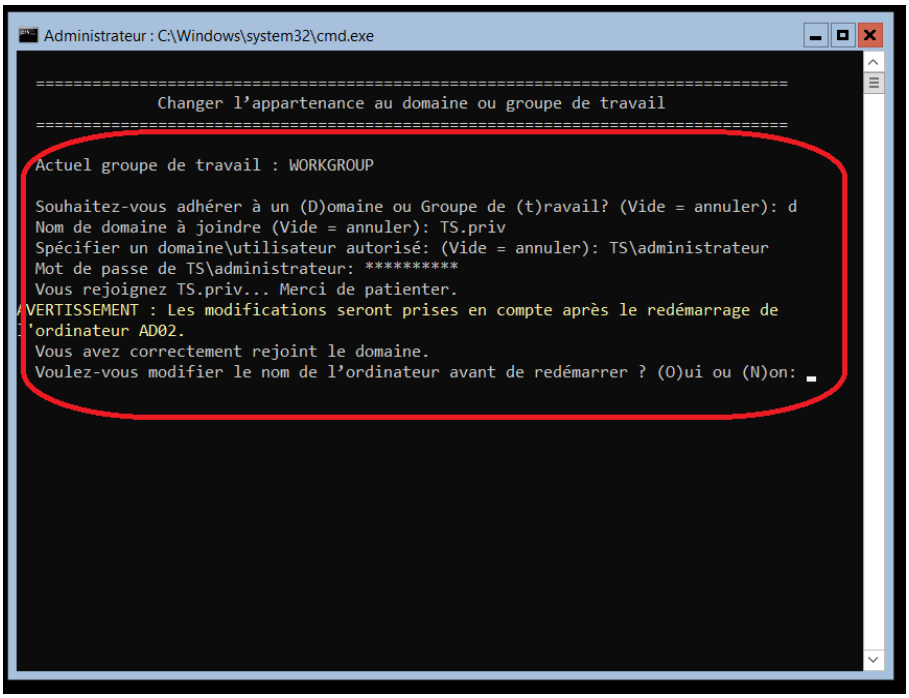
L'étape suivante consiste à modifier le nom du serveur afin de respecter notre convention de nommage. Pour cela, nous retournerons dans Sconfig et sélectionnerons l'option 2 pour changer le nom de l'hôte. Nous remplacerons alors le nom actuel du serveur par AD02.

Comme pour AD01, cette modification nécessitera un redémarrage du serveur afin qu'elle soit prise en compte.

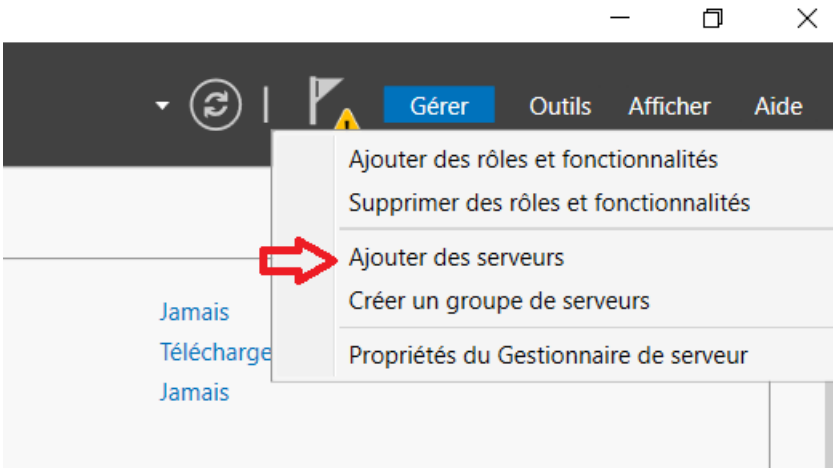


Une fois le serveur redémarré, nous pourrons l'intégrer au domaine. Pour ce faire, nous retournerons dans Sconfig et sélectionnerons l'option 1. Nous choisirons ensuite l'option D pour adhérer à un domaine.

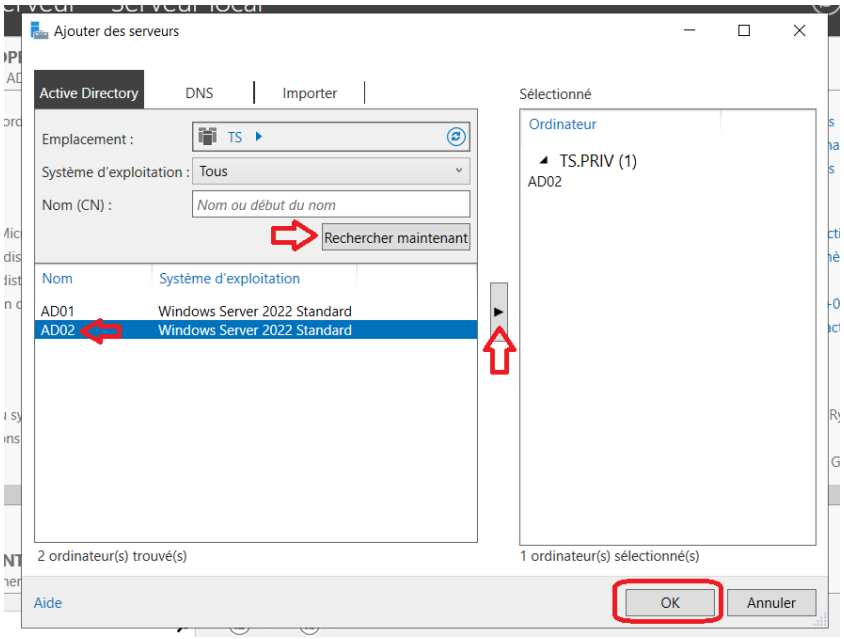
Nous serons alors invités à saisir le nom du domaine auquel nous souhaitons joindre le serveur, qui dans notre cas est TS.priv. Ensuite, nous entrerons les identifiants d'un utilisateur disposant des droits d'administration nécessaires pour autoriser l'adhésion au domaine.



Une fois l'adhésion au domaine effectuée et le serveur redémarré, nous pourrons accéder au Gestionnaire de serveurs sur AD01. Cela nous permettra d'intégrer AD02 à AD01 afin de simplifier sa gestion. Pour ce faire, nous nous rendrons dans l'onglet "Gérer", puis sélectionnerons "Ajouter des serveurs".

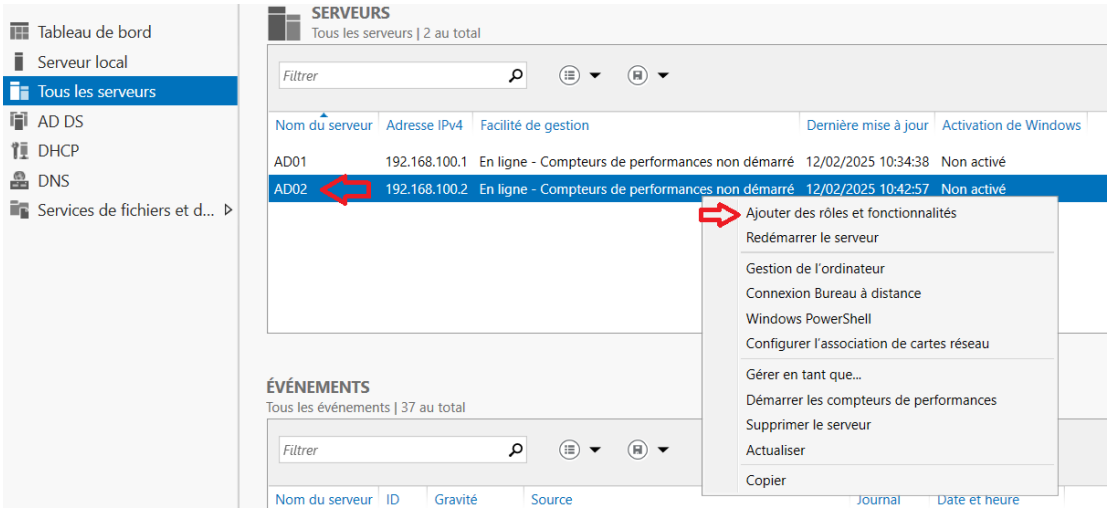


Ensuite, si le paramétrage a été correctement effectué, un clic sur "Rechercher maintenant" permettra d'afficher AD02 dans la liste située en dessous. Il suffira alors de le sélectionner, puis de cliquer sur la flèche au centre de la fenêtre pour l'ajouter.

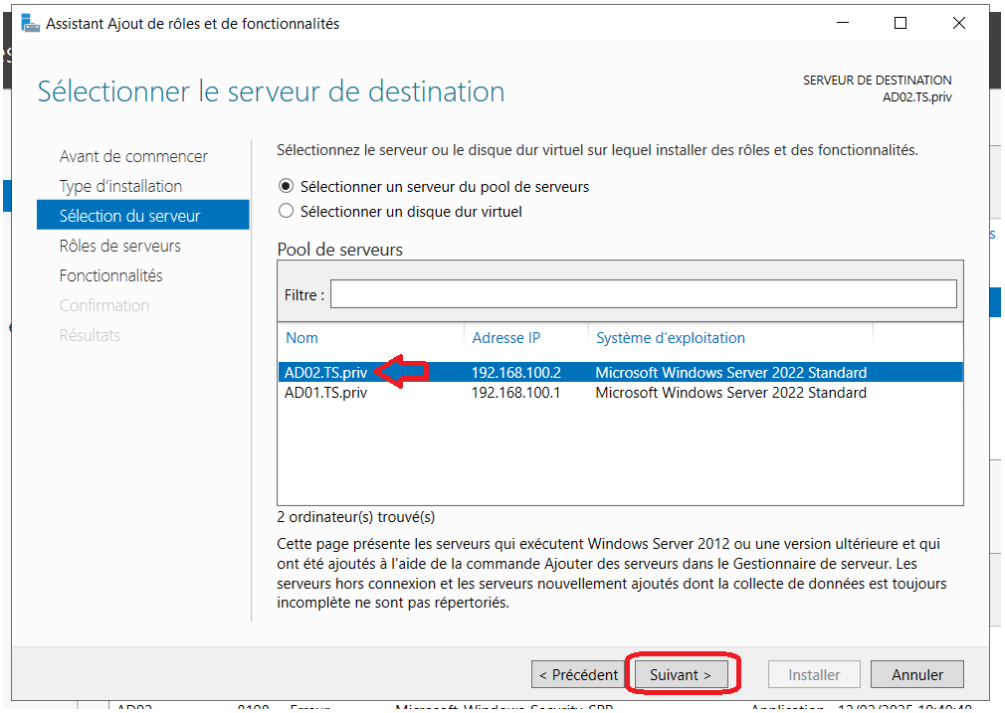


Maintenant qu'AD02 a été ajouté, il apparaît dans la liste des serveurs du Gestionnaire de serveurs, sous l'onglet "Tous les serveurs".

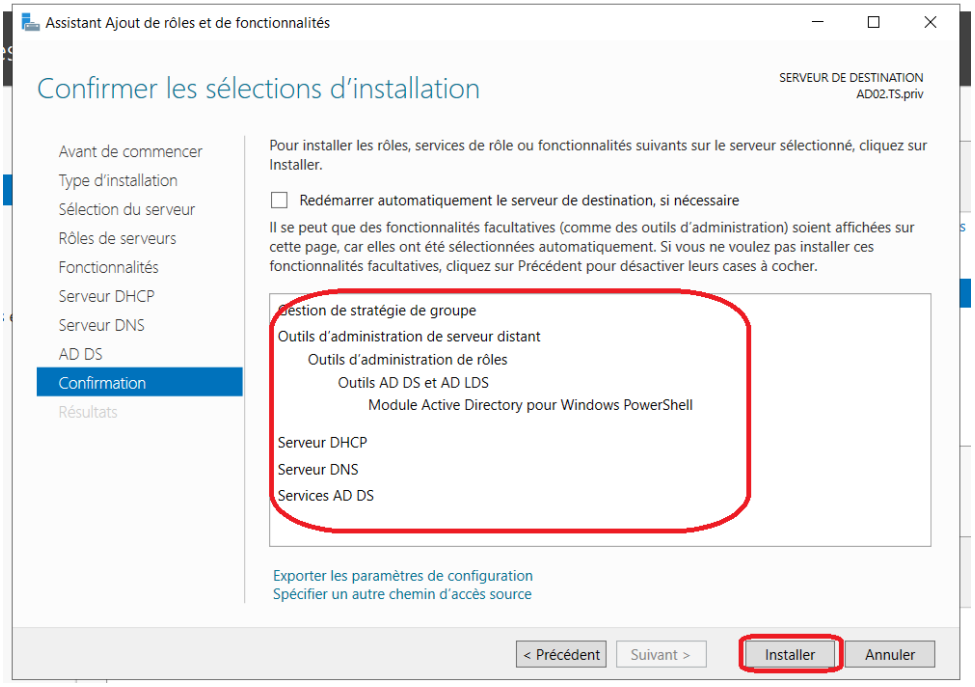
Nous allons donc procéder à sa configuration en tant que contrôleur de domaine depuis AD01. Pour ce faire, nous effectuerons un clic droit sur AD02, puis sélectionnerons "Ajouter des rôles et fonctionnalités".



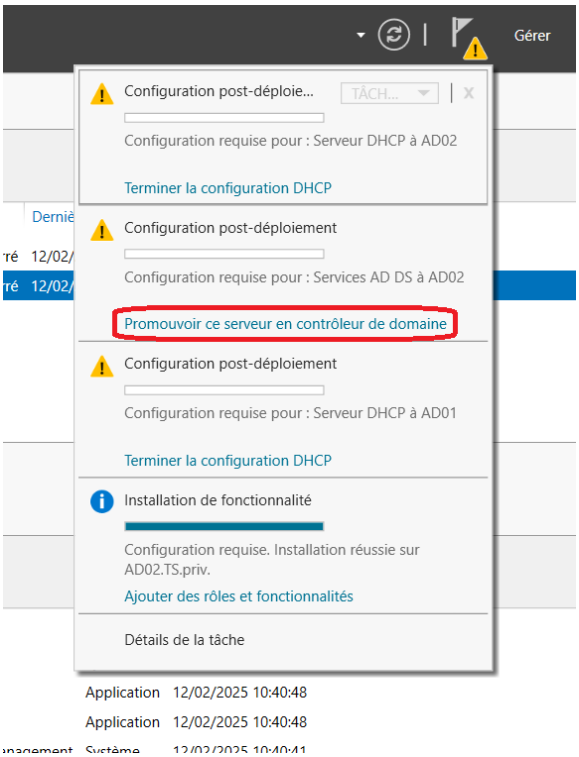
Nous veillerons à bien sélectionner AD02 dans la fenêtre suivante avant de poursuivre l'installation des rôles et fonctionnalités.



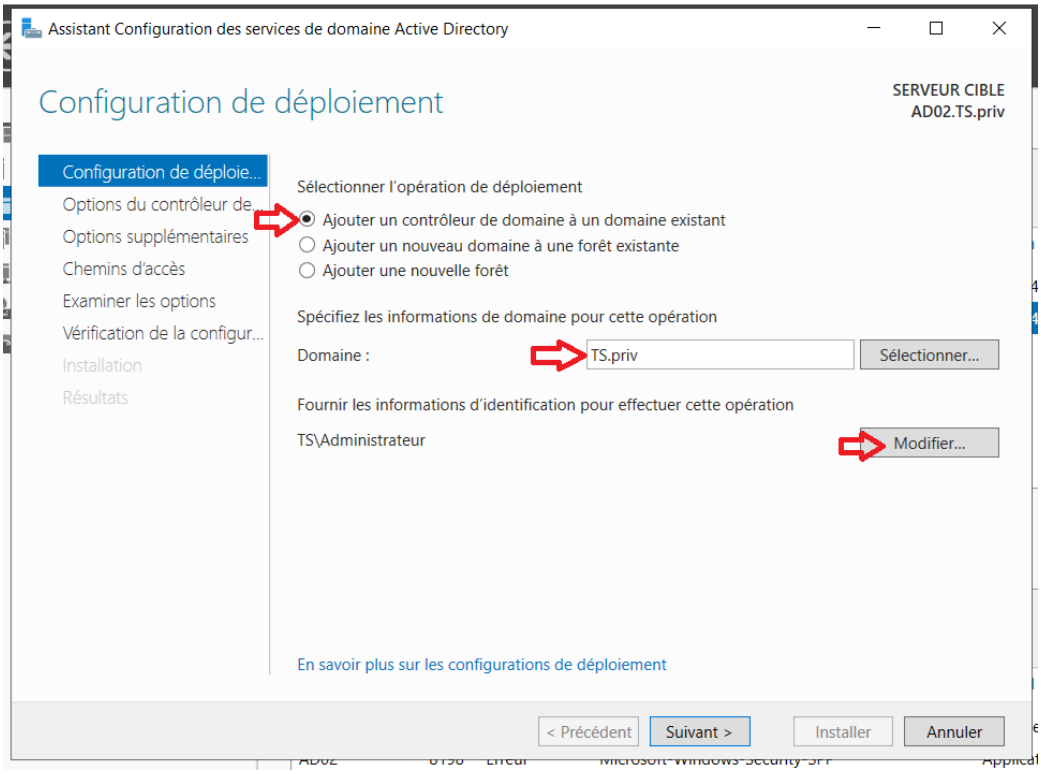
Dans la fenêtre suivante, nous sélectionnerons et installerons les mêmes rôles que sur AD01, à savoir AD DS, DHCP et DNS.



Une fois l'installation terminée, nous procéderons à la promotion d'AD02 en tant que contrôleur de domaine.



Nous choisirons l'option "Ajouter un contrôleur de domaine à un domaine existant", puis nous renseignerons le domaine, qui dans notre cas est TS.priv. Ensuite, nous fournirons les identifiants d'un utilisateur disposant des droits administratifs nécessaires pour effectuer cette opération.



Dans les fenêtres suivantes, nous définirons un mot de passe pour la restauration des services, choisirons de ne pas créer de délégation DNS et, dans l'onglet de réplication, sélectionnerons "Tout contrôleur de domaine".

Nous modifions l'emplacement des journaux dans "C:\Windows\journaux", puis lancerons l'installation. Une fois AD02 configuré, il sera en réplication avec AD01, ce qui signifie que toute action effectuée sur AD01 sera directement copiée sur AD02.

Nous procéderons ensuite à la configuration des services DNS et DHCP.

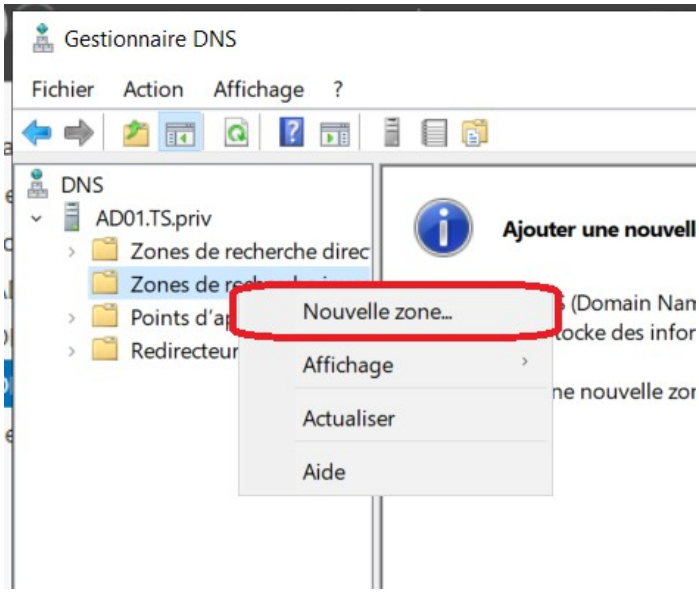
Configuration du DNS :

Nous allons maintenant configurer le service DNS en réalisant deux paramétrages essentiels :

- Créer la zone inverse
- Ajouter un enregistrement PTR pour les serveurs

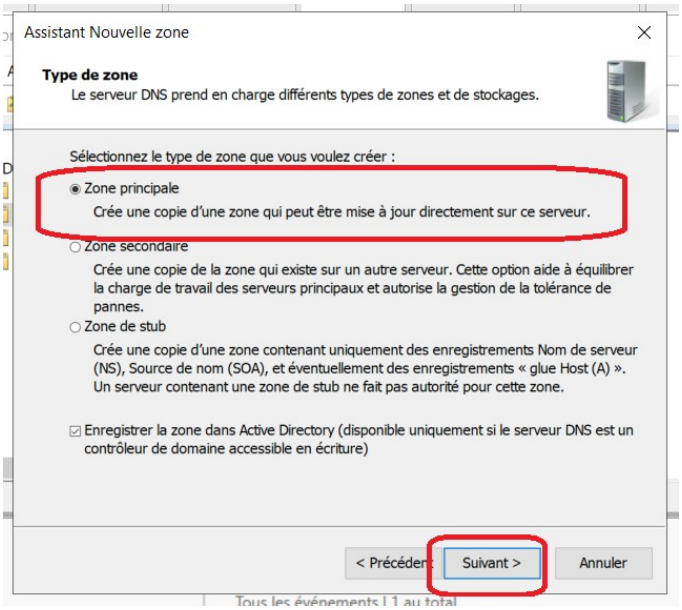
Pour commencer, nous devons nous rendre dans le Gestionnaire de serveur sur AD01, puis accéder à la section DNS. Ensuite, nous effectuerons un clic droit sur AD01, puis sélectionnerons Gestionnaire DNS.

Dans la fenêtre qui s'affiche, nous verrons deux types de zones : une zone directe et une zone inverse. Nous effectuerons un clic droit sur la zone inverse, puis choisirons Nouvelle zone pour lancer l'assistant de création.

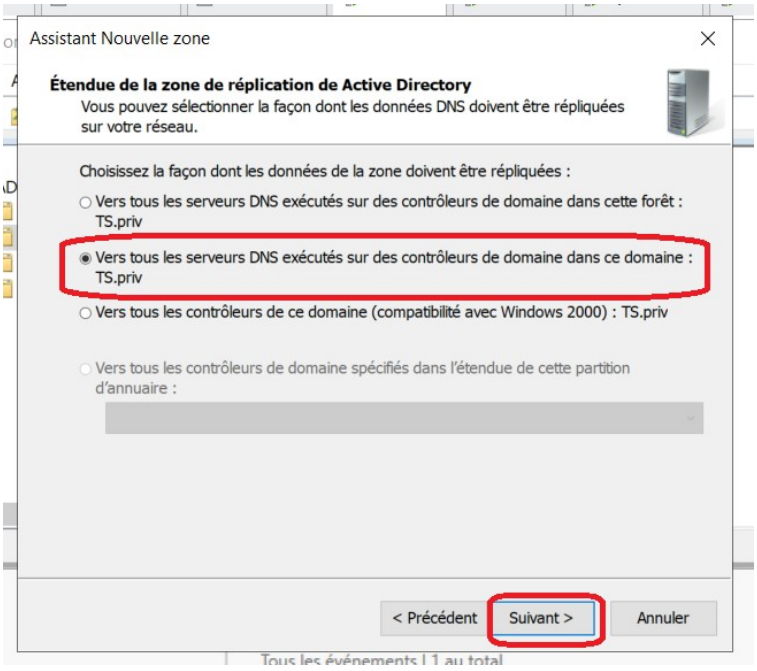


La première fenêtre affichée est celle de bienvenue, que nous pouvons passer directement pour accéder à l’étape suivante.

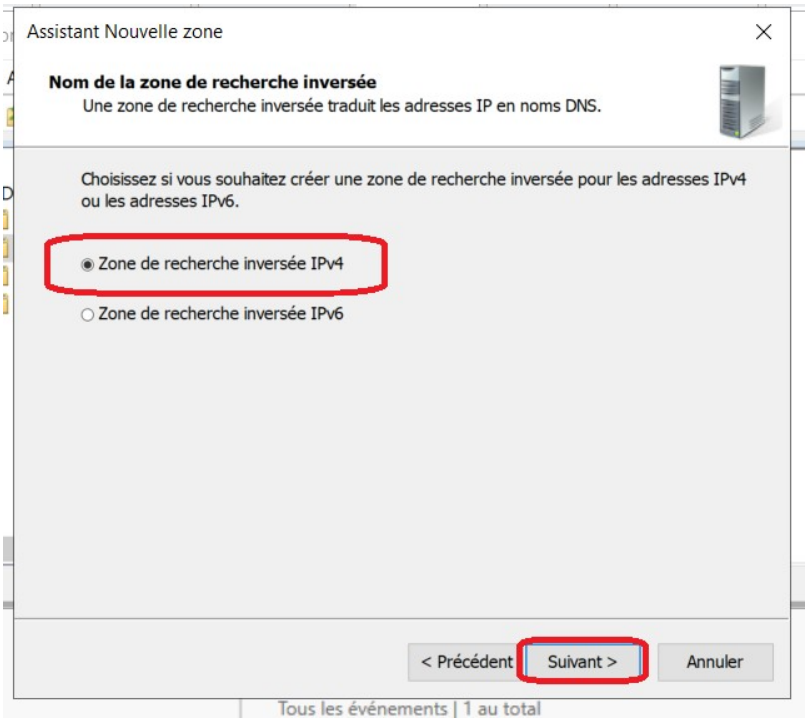
À cette étape, il nous sera demandé de sélectionner le type de zone. Dans notre cas, nous choisirons une zone principale, car elle sera stockée et gérée directement sur notre serveur DNS principal.



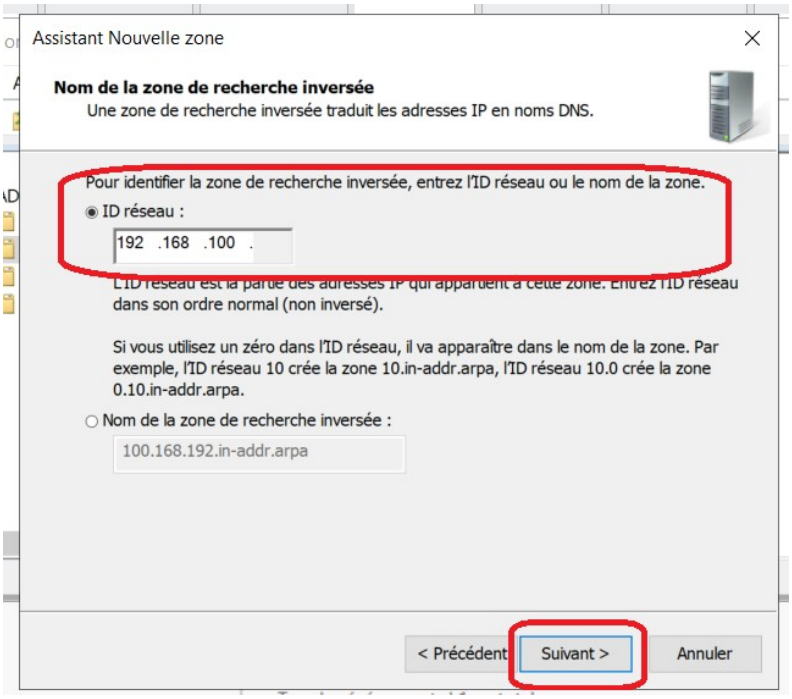
À l’étape suivante, nous devrons configurer l’étendue de la réplication de la zone. Nous choisirons l’option "Tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : TS.priv" afin de garantir la disponibilité de la zone DNS sur l’ensemble des contrôleurs de domaine du domaine TS.priv.



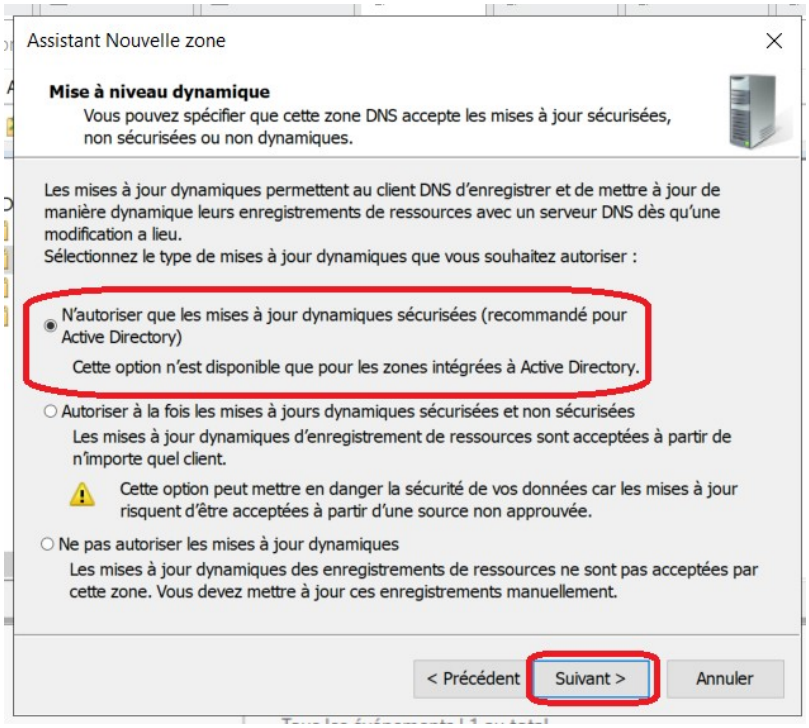
À cette étape, il nous sera demandé de choisir le type d'adresse pour la zone inverse. Deux options sont disponibles : IPv4 et IPv6. Nous sélectionnerons IPv4, car notre infrastructure utilise ce protocole pour l'adressage réseau.



Il nous sera demandé de renseigner l'ID réseau afin d'identifier la zone inverse. Nous entrerons les trois premiers octets de notre plage d'adresses IP, soit 192.168.100, afin de définir la zone de résolution inverse pour ce sous-réseau.

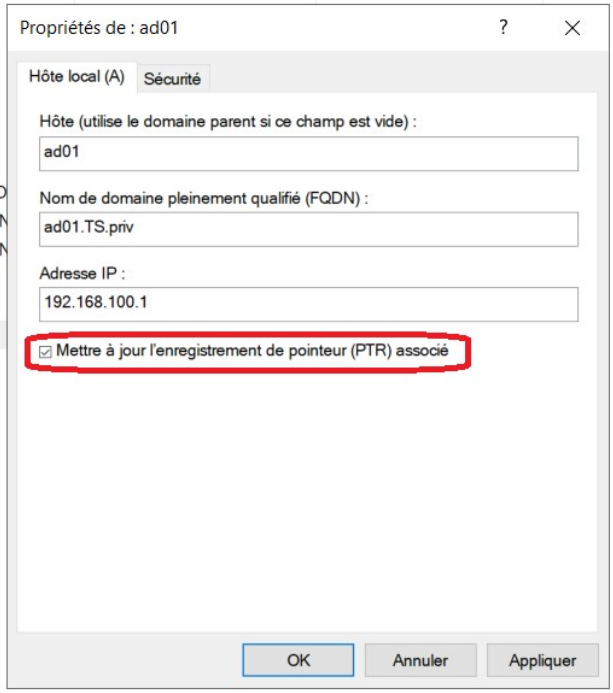


Nous choisirons d’autoriser uniquement les mises à jour dynamiques sécurisées afin de garantir que seuls les enregistrements autorisés puissent être modifiés.



Enfin, un récapitulatif des configurations s’affichera, et nous pourrons cliquer sur "Terminer" pour finaliser la création de la zone inverse.

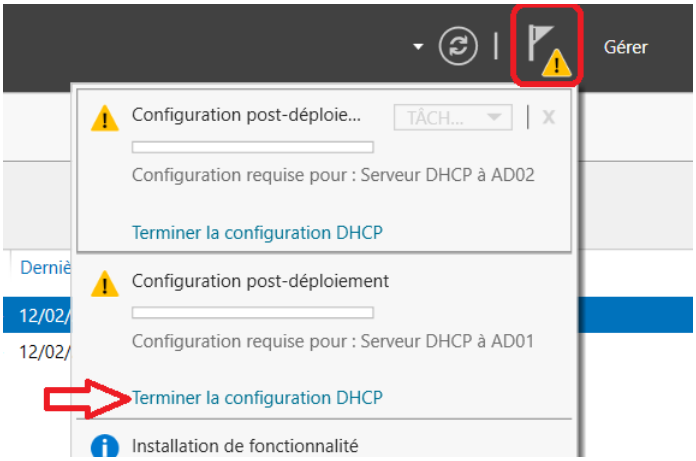
Nous allons maintenant passer à la deuxième étape, qui consiste à ajouter le pointeur PTR sur les serveurs. Pour cela, nous nous rendrons dans la zone directe, puis nous ferons un clic droit sur chaque serveur, sélectionnerons "Propriétés" et cocherons la case PTR. Cette opération devra être répétée pour tous les serveurs du domaine afin d’assurer la résolution inverse des adresses IP.



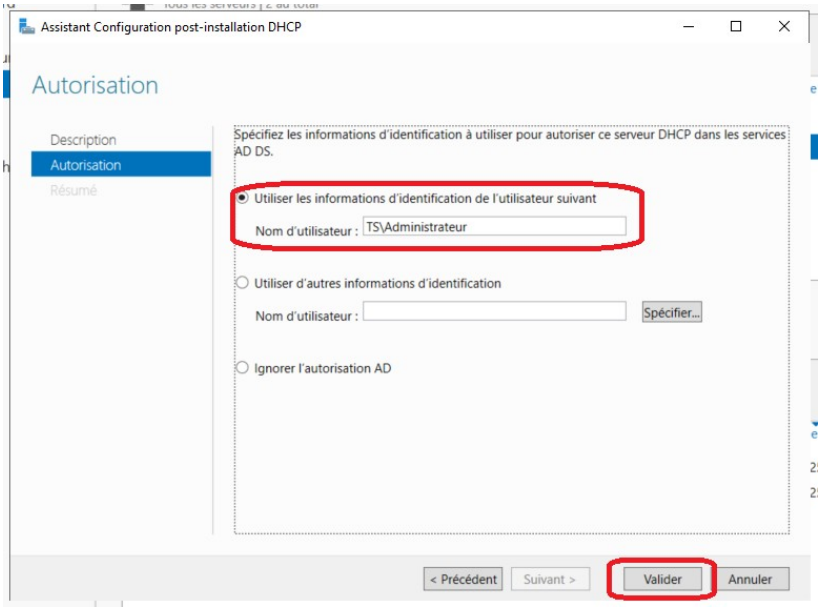
Configuration du DHCP :

Comme mentionné dans l'introduction, le rôle du DHCP est de distribuer automatiquement les adresses IP aux postes clients, évitant ainsi une configuration manuelle sur chaque machine. Nous allons maintenant procéder à sa configuration.

Nous commencerons par la post-installation en cliquant sur le drapeau de notification dans le Gestionnaire de serveur, puis sur "Terminer la configuration DHCP".



Dans les fenêtres suivantes, nous cliquerons simplement sur "Suivant" jusqu'à l'étape où il nous sera demandé de spécifier les informations d'identification. Nous fournirons alors les identifiants d'un utilisateur disposant des droits nécessaires pour autoriser le service DHCP à communiquer avec Active Directory.



Nous allons maintenant configurer la plage d’adresses IP pour notre réseau utilisateur. Les postes auront des adresses comprises entre 192.168.110.50 et 192.168.110.150, soit un pool de 100 adresses. Cette plage est largement suffisante pour les besoins actuels de l’entreprise ainsi que pour son évolution future.

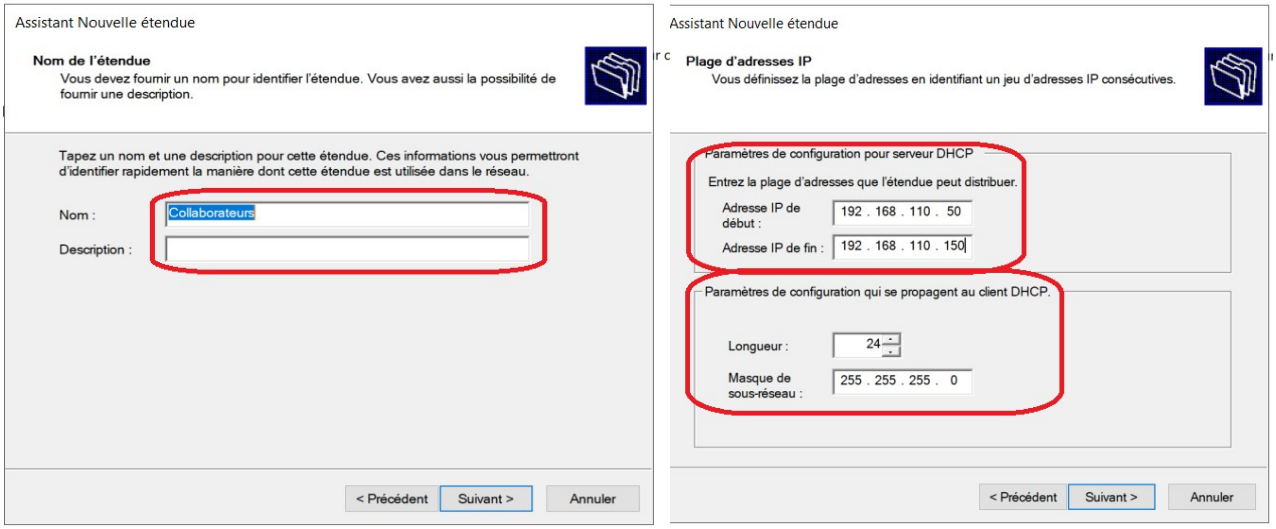
Pour configurer cette plage, nous nous rendrons dans le Gestionnaire de serveur, puis dans la section DHCP afin d’accéder au Gestionnaire DHCP. Nous ferons un clic droit sur Étendu, puis sélectionnerons Créer une nouvelle étendue.

L’assistant nous demandera d’abord de renseigner un nom et une description. Comme cette étendue est destinée aux utilisateurs standard, nous la nommerons Collaborateurs.

À l’étape suivante, nous définirons la plage d’adresses que le serveur DHCP pourra attribuer, soit 192.168.110.50 à 192.168.110.150, avec un masque de sous-réseau 255.255.255.0.

L’assistant nous demandera ensuite de renseigner les adresses à exclure, c'est-à-dire les adresses comprises dans la plage mais réservées pour des appareils configurés en IP statique. Dans notre cas, nous n’avons aucune adresse à exclure, donc nous passerons cette étape.

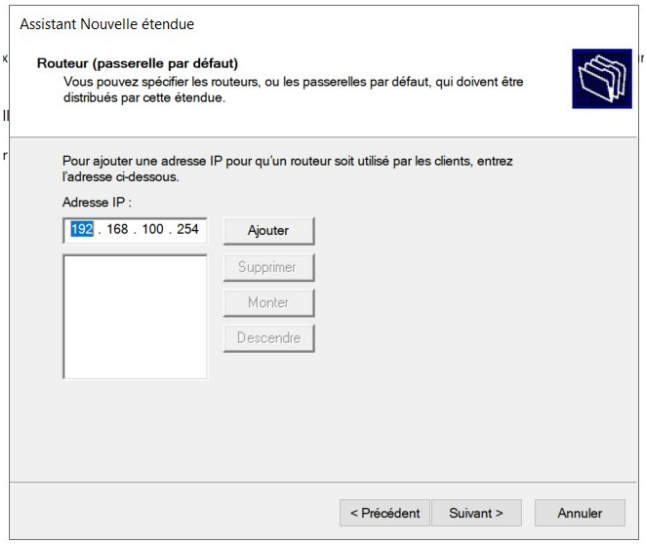
Enfin, nous configurerons la durée du bail, c'est-à-dire la période pendant laquelle une adresse IP est réservée pour une machine. Nous avons décidé de fixer cette durée à 5 jours.

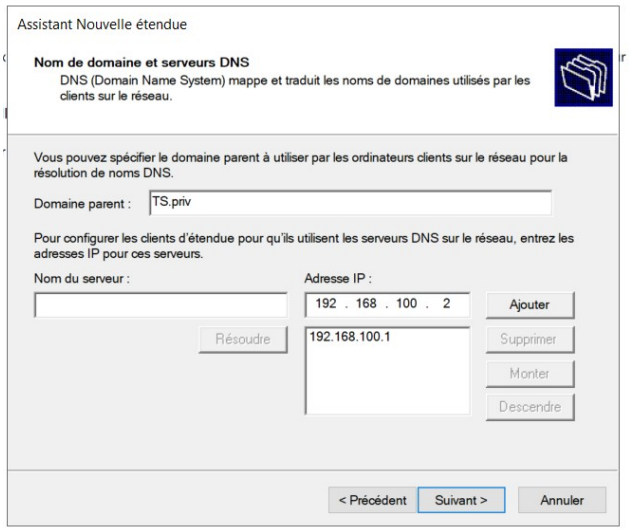


Après la configuration de la plage d’adresses, l’assistant nous demandera si nous souhaitons configurer les options complémentaires. Nous choisirons de les renseigner immédiatement.

La première option demandée est la passerelle par défaut. Dans notre cas, il s’agit de l’adresse 192.168.110.254, qui correspond à l’IP virtuelle de notre cluster DynFi.

Une fois la passerelle renseignée, nous passerons à la configuration des serveurs DNS. Nous entrerons les adresses de nos contrôleurs de domaine, soit 192.168.100.1 et 192.168.100.2, afin que les postes clients puissent effectuer correctement la résolution de noms.

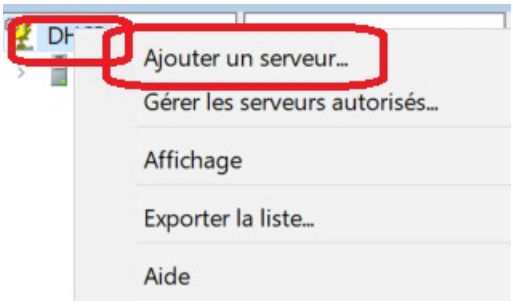




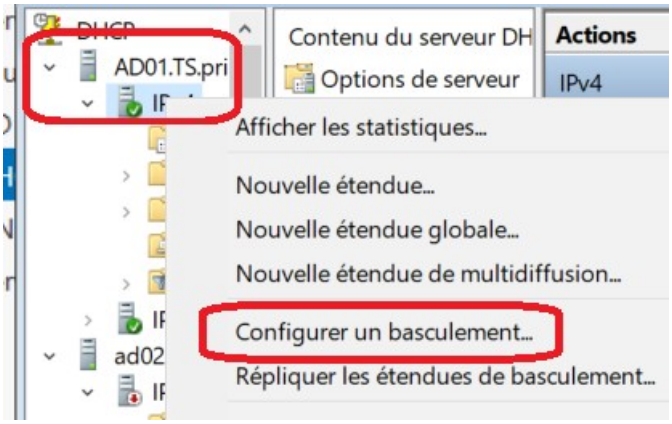
Après cette étape, l'assistant nous demandera de renseigner l'adresse du serveur WINS. Étant donné que nous n'en avons pas sur notre réseau, nous laisserons ce champ vide. Enfin, nous activerons l'étendue pour que le DHCP commence à distribuer les adresses IP aux postes clients.

Passons maintenant à la mise en place de la réplication du service DHCP.

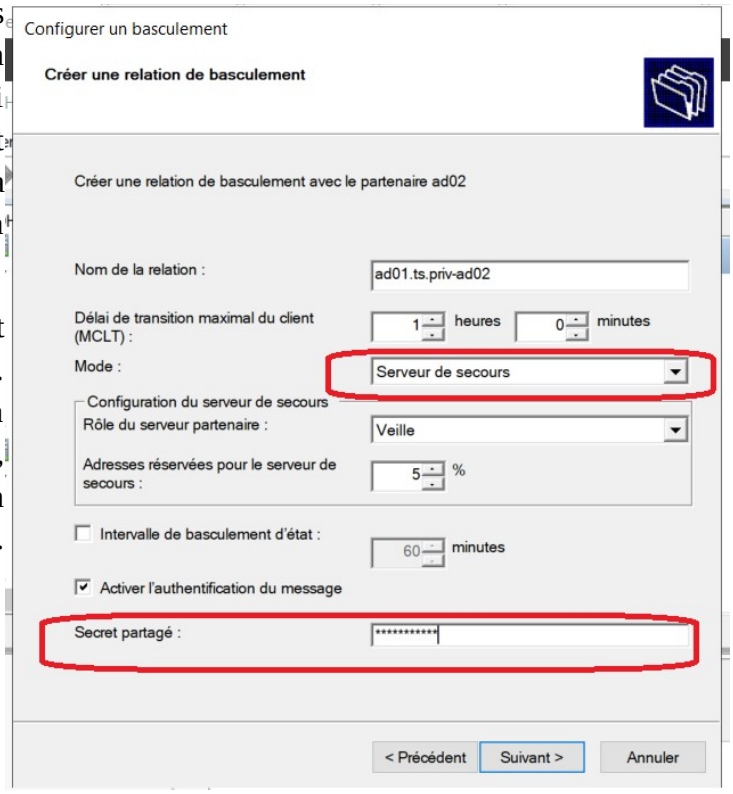
Pour commencer, ouvrons le Gestionnaire DHCP, effectuons un clic droit sur DHCP, puis sélectionnons Ajouter un serveur afin d'ajouter AD02.



Ensuite, dans la section IPv4 du serveur AD01, faisons un clic droit et choisissons Configurer un basculement. Nous sélectionnons AD02 comme serveur partenaire.



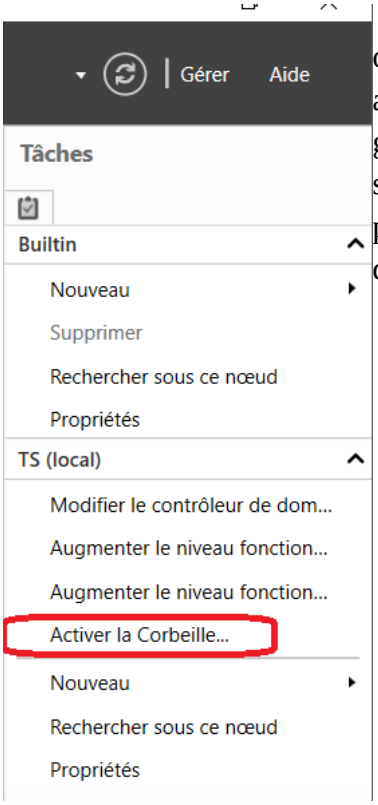
Lors de la configuration, ajustons les paramètres " d'équilibrage de charge" en " serveur de secours". De cette manière, si le service DHCP sur AD01 devient indisponible, AD02 prendra automatiquement le relais pour assurer la continuité du service.



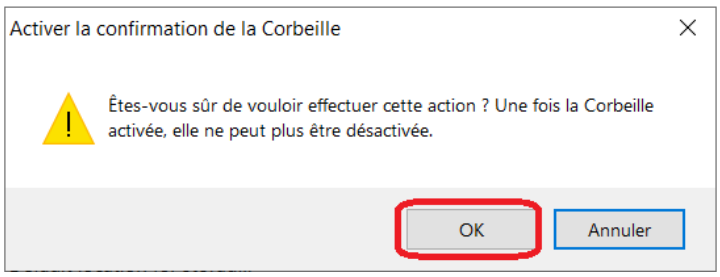
Il nous faut ensuite définir un secret partagé, qui agit comme un mot de passe. Ce secret permet de sécuriser et valider la réplication entre les deux serveurs, garantissant ainsi que la communication entre AD01 et AD02 est bien authentifiée.

Une fois cette configuration terminée, nous allons mettre en place des bonnes pratiques sur Active Directory afin de renforcer la sécurité.

Bonnes pratiques Active Directory

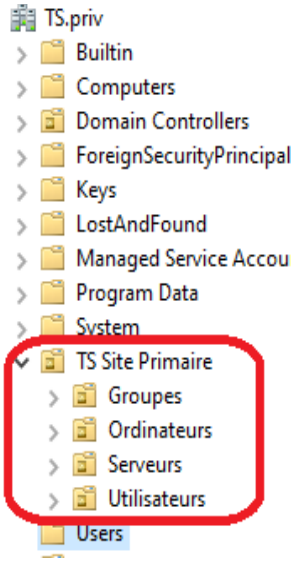


Nous commencerons par activer la corbeille Active Directory, ce qui offrira une protection supplémentaire contre la suppression accidentelle d'objets. Pour cela, nous nous rendrons dans le gestionnaire de serveur sur AD01, puis dans la section outils, où nous sélectionnerons Centre d'administration Active Directory. Dans la partie droite de l'interface, nous trouverons l'option permettant d'activer la corbeille.



Nous allons maintenant structurer Active Directory en créant des unités d'organisation, des utilisateurs et des groupes.

Pour cela, nous nous rendrons dans la section outils du gestionnaire de serveur, puis sélectionnerons Utilisateurs et ordinateurs Active Directory. Dans la colonne de gauche, nous ferons un clic droit, puis choisirons Nouveau > Unité d'organisation.

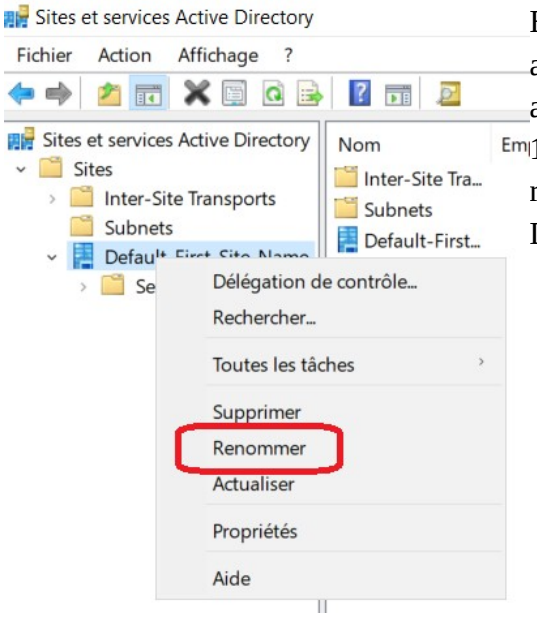


L'architecture de notre Active Directory sera organisée par site, avec une première unité d'organisation nommée TS Site Primaire. À l'intérieur de celle-ci, nous créerons plusieurs unités d'organisation pour classer les objets de manière structurée : Serveurs, Groupes, Utilisateurs et Ordinateurs. Toutes ces unités d'organisation seront protégées contre la suppression accidentelle.

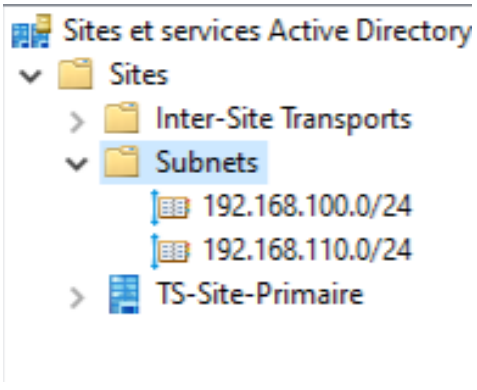
Chaque objet sera placé dans l'unité d'organisation appropriée. Les groupes seront créés en fonction des besoins de l'entreprise, et en cas d'ajout de nouveaux serveurs ou ordinateurs, ils seront déplacés dans les unités d'organisation correspondantes. De même, les nouveaux utilisateurs seront directement créés dans la bonne unité d'organisation.

Nous allons poursuivre l'organisation de l'Active Directory en renommant le site par défaut "Default-First-Site-Name" en "TS-Site-Primaire".

Pour cela, nous ouvrirons le gestionnaire de serveurs, puis nous nous rendrons dans l'onglet outils et sélectionnerons Sites et services Active Directory. Une fois dans l'interface, nous localiserons "Default-First-Site-Name", puis nous le renommerons en "TS-Site-Primaire" pour correspondre à notre architecture réseau.

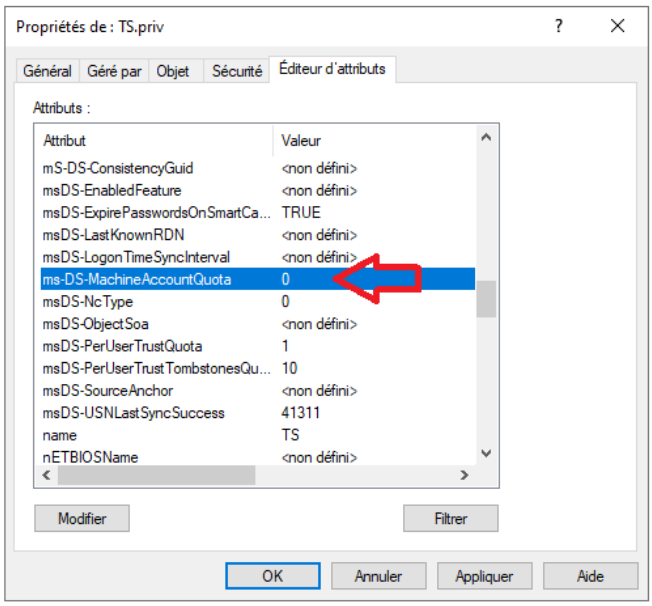


Ensuite, nous renseignerons les différents sous-réseaux afin de les associer à notre site. Dans notre cas, nous avons deux sous-réseaux : 192.168.100.0 et 192.168.110.0. Pour cela, nous ajouterons ces sous-réseaux dans la configuration de Sites et services Active Directory et les associerons au site "TS-Site-Primaire".



Nous allons maintenant ajouter une délégation pour permettre uniquement à certains utilisateurs d'ajouter des ordinateurs dans le domaine, tout en supprimant cette permission pour tous les autres utilisateurs.

Tout d'abord, pour supprimer l'ajout automatique des ordinateurs par n'importe quel utilisateur, nous nous rendrons dans Active Directory, puis dans les propriétés du domaine TS.priv. Ensuite, dans l'onglet éditeur d'attributs, nous chercherons l'attribut "ms-DS-MachineAccountQuota". Par défaut, cette valeur est fixée à 10, ce qui signifie que chaque utilisateur peut ajouter jusqu'à 10 machines dans le domaine. Nous modifierons cette valeur à 0 afin d'empêcher tout ajout d'ordinateurs par des utilisateurs standards.

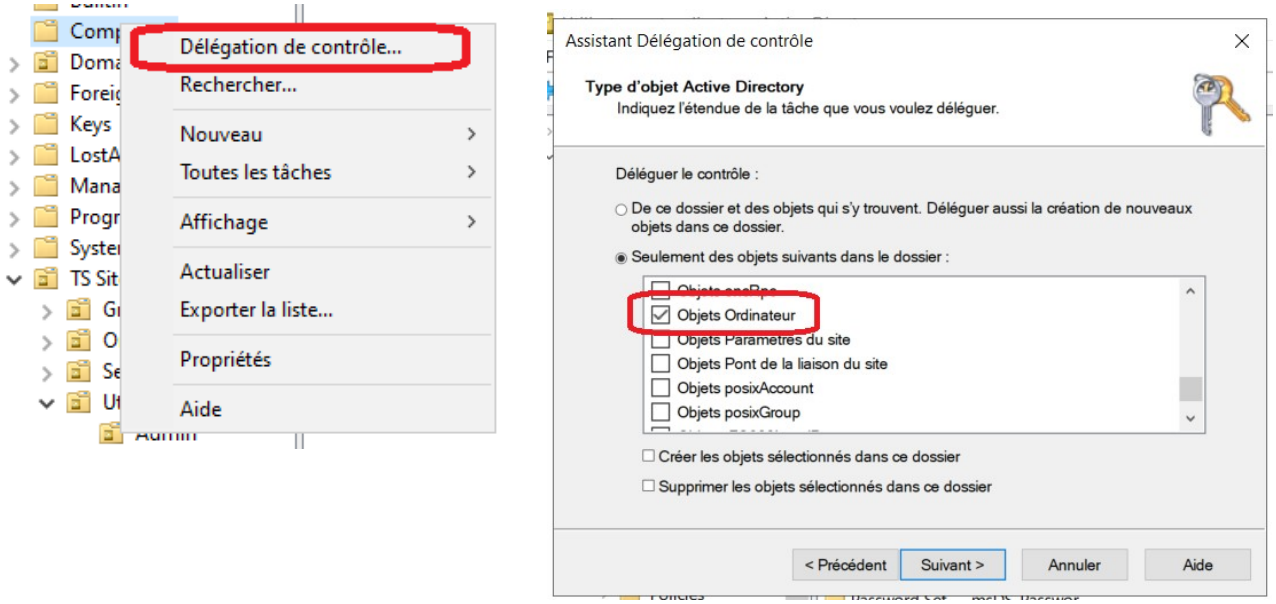


Après avoir appliqué ce paramètre, nous allons créer une délégation pour autoriser un groupe spécifique à ajouter des machines dans le domaine. Pour cela, nous nous rendrons dans Active Directory, puis dans l'unité d'organisation Computers. Nous ferons un clic droit dessus, puis sélectionnerons Délégation de contrôle.

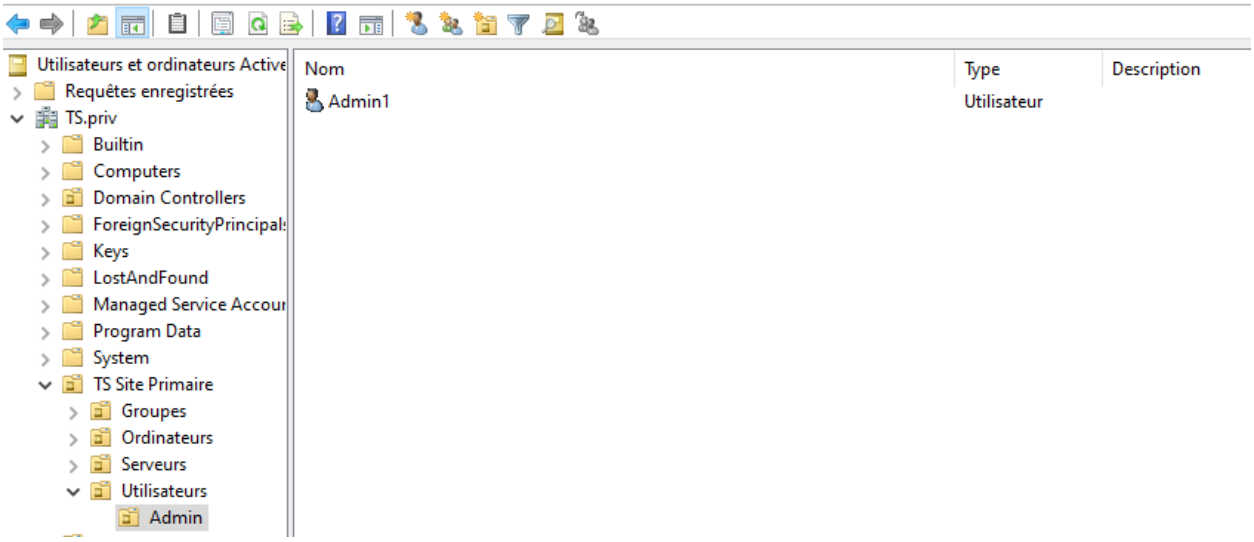
Dans l'assistant de délégation de contrôle, nous ajouterons l'utilisateur ou le groupe qui sera autorisé à ajouter des machines au domaine. Dans notre cas, nous sélectionnerons Admin du domaine comme exemple car il dispose déjà des droits pour adhérer des PC au domaine.

Ensuite, nous créerons une nouvelle tâche et spécifierons que cette délégation s'applique aux objets de type Ordinateur. Enfin, nous accorderons les permissions nécessaires en activant l'autorisation de Création et suppression d'objets enfants.

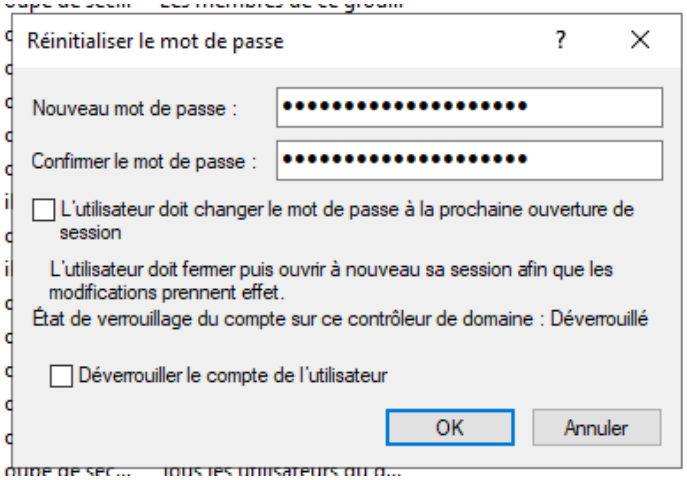
Après validation, les administrateurs du domaine pourront ajouter des ordinateurs sans restriction, tout en empêchant les utilisateurs standards d'effectuer cette opération.



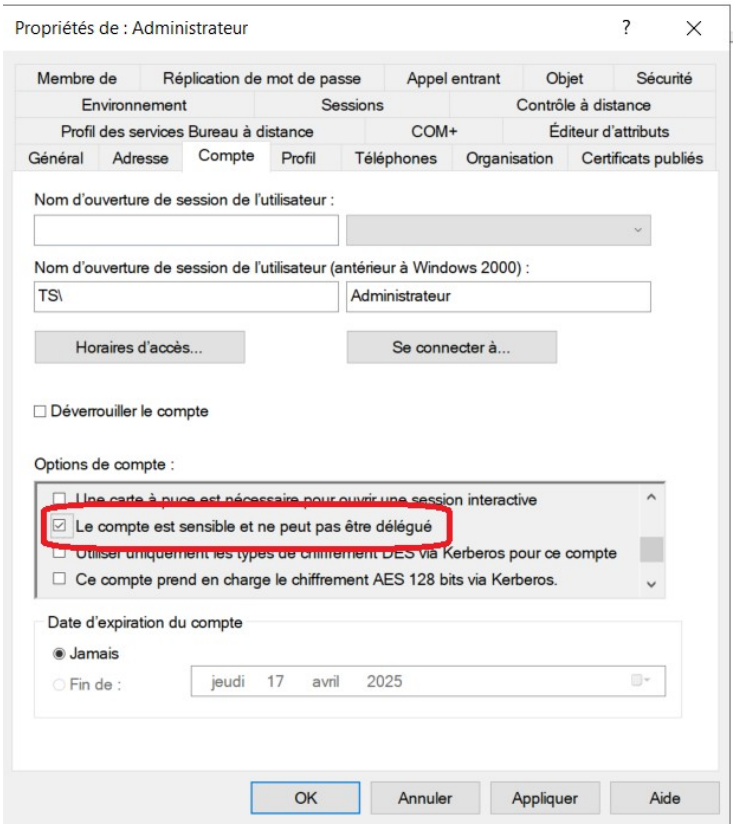
Pour renforcer la sécurité du domaine, nous créerons un compte admin1 avec un mot de passe sécurisé et l'ajouterons aux groupes Administrateurs du domaine, Administrateurs et Administrateurs de l'entreprise. Ce compte sera utilisé pour la gestion quotidienne, limitant ainsi l'usage du compte Administrateur aux cas exceptionnels. Ensuite, pour sécuriser l'administration du domaine, nous allons modifier le mot de passe du compte Administrateur en utilisant un mot de passe complexe généré par KeePass. Ensuite.



Pour changer le mot de passe du compte Administrateur, nous nous rendons dans l'OU Users, faisons un clic droit sur le compte, puis sélectionnons Réinitialiser le mot de passe. Nous entrons ensuite le mot de passe complexe généré par KeePass et décochons l'option obligeant la modification du mot de passe à la première connexion.



Pour interdire la délégation des comptes administrateurs, nous devons modifier les propriétés de chaque compte administrateur. Il suffit de se rendre dans les Propriétés de chaque compte, puis dans l'onglet Compte, où nous trouverons l'option "Le compte est sensible et ne peut pas être délégué". En cochant cette option, nous empêchons la délégation de ces comptes administrateurs.



Pour la séparation des rôles FSMO, on utilise l'outil ntdsutil. On ouvre une invite de commandes en administrateur et on saisit la commande ntdsutil. Une fois dans le prompt, on entre "roles" pour passer en mode FSMO maintenance, qui permet de transférer ou de forcer le déplacement des rôles en cas de problème avec la commande "seize".

Les rôles seront déplacés vers AD02. Pour cela, on tape "connects", puis "connect to server AD02" pour établir la connexion avec le serveur cible. Une fois connecté, on quitte le mode connexion en tapant "q" et on revient en mode FSMO maintenance. Enfin, on transfère les rôles avec la commande "transfer" suivie du nom du rôle à déplacer. Pour nous ce sera :

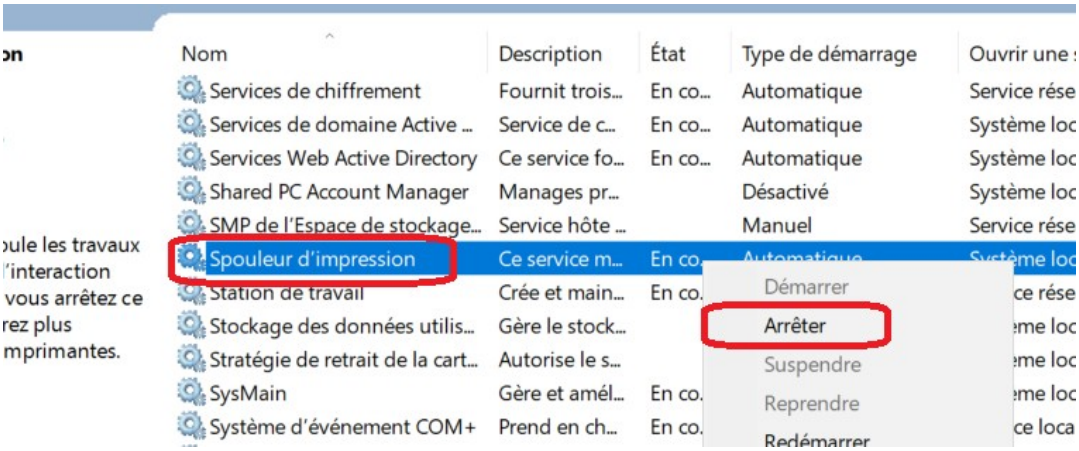
-"transfer domain naming master" pour le Maître d'attribution des noms de domaine
-"transfer rid master" pour le Maître RID

Une fois le transfert effectué, il est recommandé de vérifier que les rôles sont bien en place sur AD02. Avec la commande "NETDOM QUERY /Domain:TS.priv FSMO"

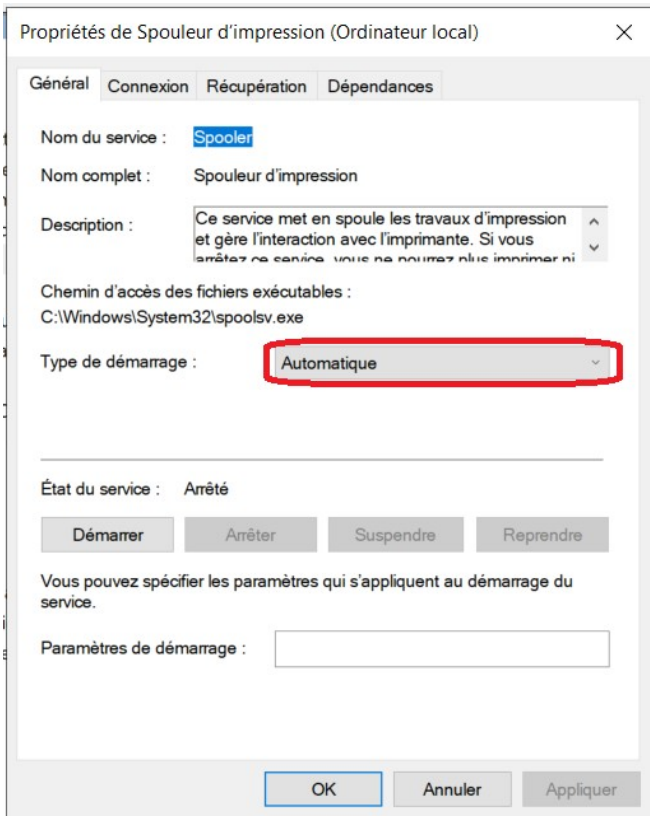
```
C:\Users\admin1>NETDOM QUERY /Domain:TS.priv FSMO
Contrôleur de schéma        AD01.TS.priv
Maître des noms de domaine  AD02.TS.priv
Contrôleur domaine princip. AD01.TS.priv
Gestionnaire du pool RID    AD02.TS.priv
Maître d'infrastructure     AD01.TS.priv
L'opération s'est bien déroulée.
```

Pour renforcer la sécurité de notre Active Directory, nous allons désactiver le spouleur d'impression afin de limiter les risques liés aux vulnérabilités potentielles de ce service.

Sur AD01, nous accédons à Services et recherchons le service Spouleur d'impression. Si celui-ci est en cours d'exécution, nous cliquons sur Arrêter.



Ensuite, en effectuant un clic droit sur le service, nous sélectionnons Propriétés et modifions son type de démarrage en Désactivé.



Cela arrêtera immédiatement le service et l'empêchera de redémarrer automatiquement au prochain démarrage du serveur. Cette mesure permet de réduire les risques d'exploitation des vulnérabilités associées au spouleur d'impression.

Voilà, toutes les bonnes pratiques ont été appliquées. Cela permet de renforcer la sécurité de notre Active Directory tout en assurant une meilleure organisation. Grâce à ces configurations, nous avons sécurisé les services essentiels, contrôlé les accès et amélioré la gestion des rôles et des comptes. L'ensemble des paramètres appliqués garantit une gestion plus sécurisée et structurée de l'Active Directory, tout en limitant les risques d'accès non autorisé et de vulnérabilités.

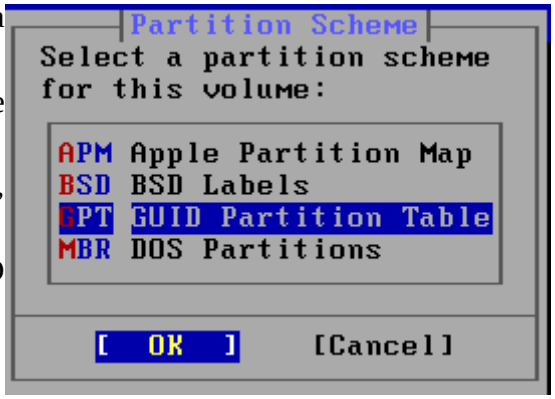
Installation et configuration DynFi

Pour installer DynFi avec une adresse IP virtuelle, nous commençons par injecter l'ISO sur une VM. Une fois lancé, nous procédons à l'installation de DynFi01, puis répétons l'opération sur une seconde VM. Sur le premier écran, nous sélectionnons Install pour une installation standard. Ensuite, nous choisissons le clavier AZERTY français afin d'éviter toute confusion avec un clavier QWERTY.

Nous sélectionnons ensuite le type de système de fichiers et optons pour « Auto (UFS) Guided UFS Disk Setup » afin de laisser l'installation gérer automatiquement le partitionnement du disque. Une fois cette étape validée, l'installateur procède au formatage et à la création des partitions nécessaires au bon fonctionnement de DynFi.

Après, on nous demande le partitionnement du disque. Pour nous, l'utilisation de l'intégralité du disque est ce qui est recommandé, mais attention, le disque sera formaté. La prochaine option concerne le choix du partitionnement. Nous aurons le choix entre plusieurs options de formatage :

- APM : Apple Partition Map (peu d'intérêt à choisir ce mode).
- BSD : BSD Labels (utilise exclusivement le partitionnement BSD).
- GPT : GUID Partition Table (choix par défaut, sauf pour les anciens BIOS).
- MBR : DOS Partitions (à utiliser si GPT et BSD ne fonctionnent pas).



L'option recommandée par défaut est GPT, que nous sélectionnerons également.

L'installation du système débute alors et sera répliquée sur le second serveur DynFi. Une fois terminée, nous devons configurer les interfaces réseau et leur attribuer des adresses IP.

Avant cela, nous devons nous authentifier avec les identifiants par défaut, qui seront modifiés ultérieurement :

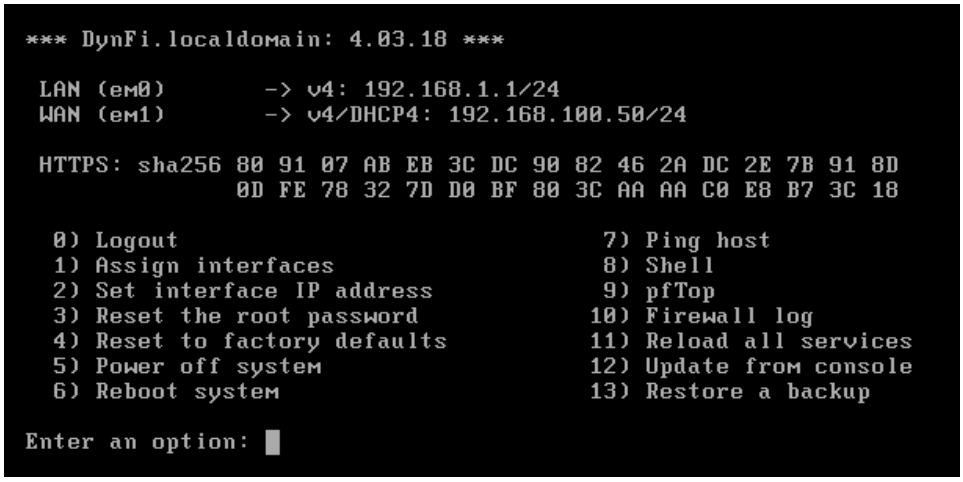
- Login : root
- Mot de passe : dynfi

Chaque instance de DynFi disposera de trois interfaces réseau :

Interfaces	@MAC	@IP	Sous-Réseaux	UTM
Em0 = vmbr0	BC:24:11:76:4C:E9	10.1.0.x	WAN	DynFI01
Em1 = vmbr101	BC:24:11:A5:BC:C2	192.168.100.253/24	LAN	DynFI01
Em2 = vmbr102	BC:24:11:60:9D:02	192.168.110.253/24	LAN USER	DynFI01
Em0 = vmbr0	BC:24:11:8C:28:17	10.1.0.x	WAN	DynFI02
Em1 = vmbr101	BC:24:11:ED:88:60	192.168.100.252/24	LAN	DynFI02
Em2 = vmbr102	BC:24:11:A0:2A:D9	192.168.110.252/24	LAN USER	DynFI02

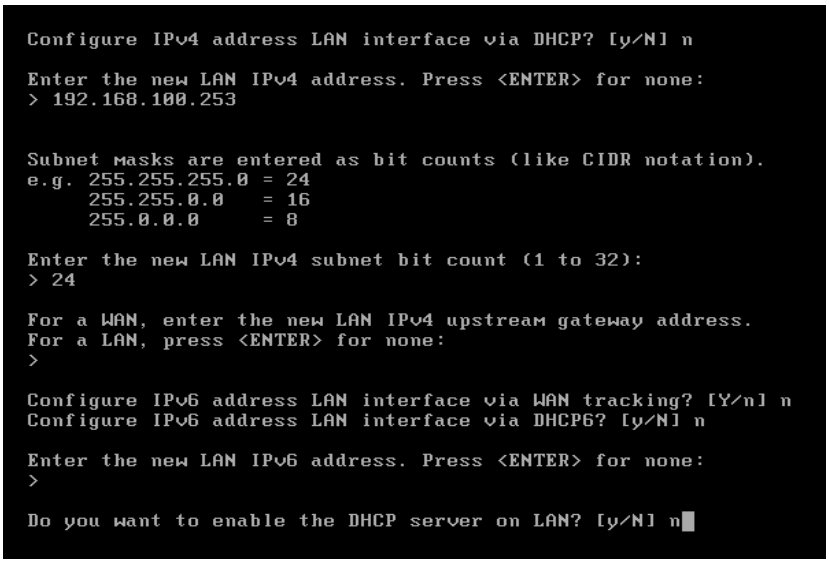
Nous débutons par la configuration des interfaces réseau en définissant les rôles de chaque interface WAN, LAN et LAN USERS.

Dans le menu sconfig de DynFi, plusieurs options s'affichent. Nous sélectionnons l’option 1 : "Assign Interfaces" pour attribuer chaque interface à son usage spécifique.



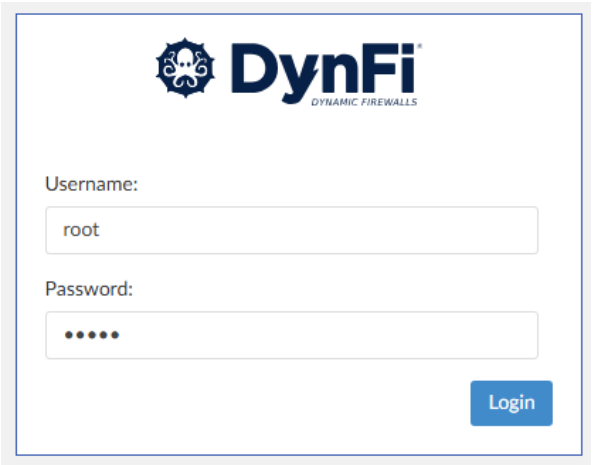
Nous allons maintenant attribuer les interfaces réseau dans l’ordre demandé : WAN, LAN et OPT1 (qui correspond au LAN USERS). Pour cela, nous devons respecter le tableau de configuration défini précédemment.

Une fois les interfaces assignées, nous allons leur attribuer leurs adresses IP respectives. Lorsqu'on nous demande si l'interface doit être configurée en DHCP, nous sélectionnons non afin de définir une adresse IP manuelle. Nous indiquons ensuite l'adresse IP de l'interface ainsi que son masque en /24. Une fois cette étape réalisée, plusieurs autres options sont proposées, mais elles ne sont pas utiles dans notre configuration, nous les refusons donc systématiquement.

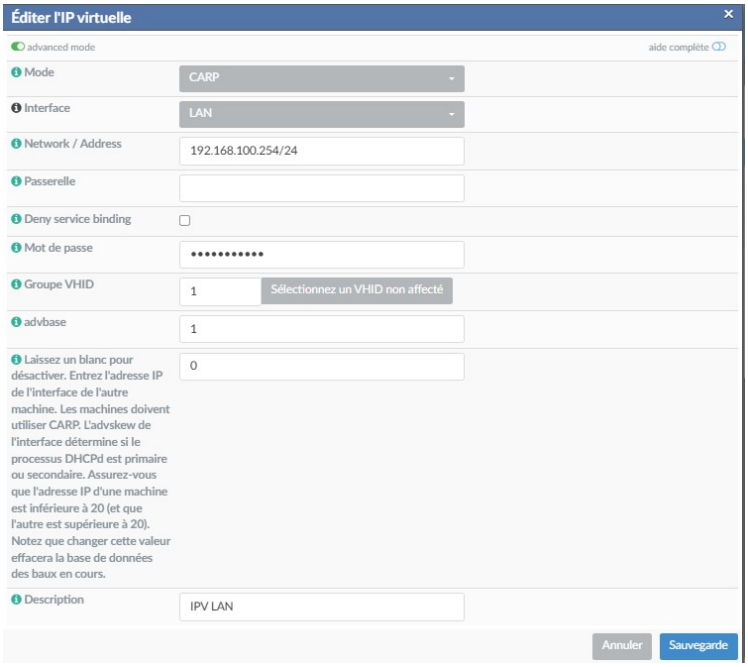


Nous répétons l'opération pour la seconde interface OPT1 (LAN USERS) en lui attribuant l'adresse 192.168.110.253/24. Comme pour l'installation précédente, nous réalisons cette configuration sur le second DynFi, en adaptant les adresses IP : 192.168.100.252 pour LAN et 192.168.110.252 pour OPT1 (LAN USERS).

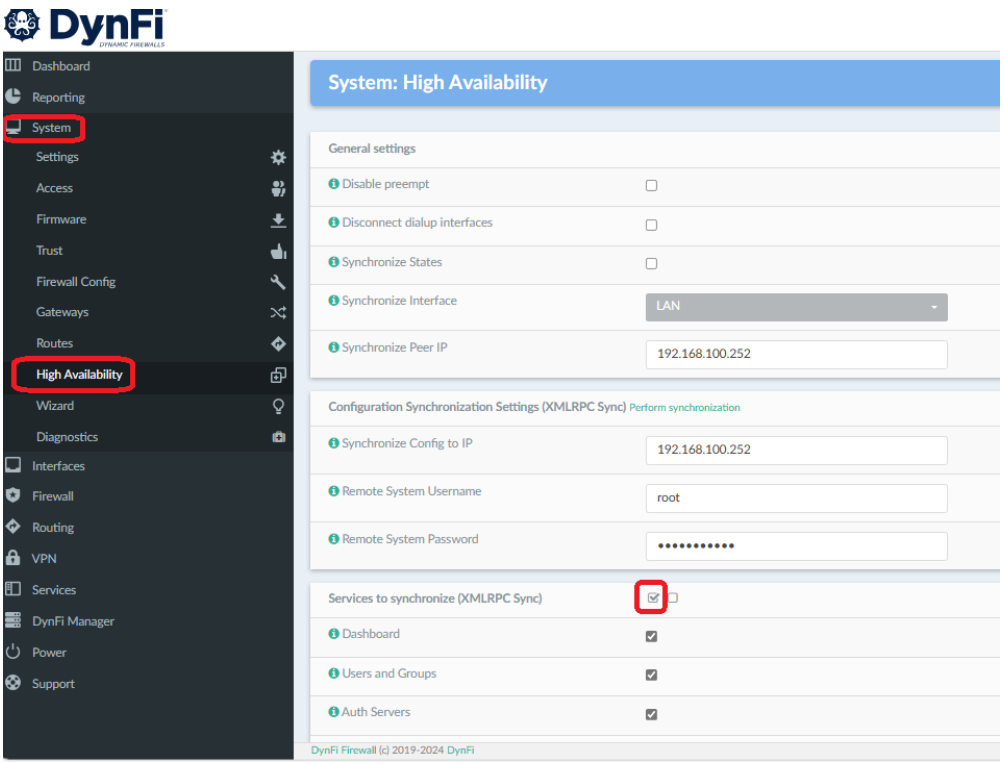
Une fois toutes les configurations effectuées, nous nous rendons sur Edge depuis AD01 pour poursuivre la configuration. En entrant 192.168.100.253 dans la barre d'adresse, nous accédons à la page de connexion du DynFi01. Nous nous connectons à l'aide des identifiants par défaut. Une fois connectés, une configuration de base nous est demandée : paramétrage du WAN, réglage de l'heure, puis modification du mot de passe par défaut afin de renforcer la sécurité.



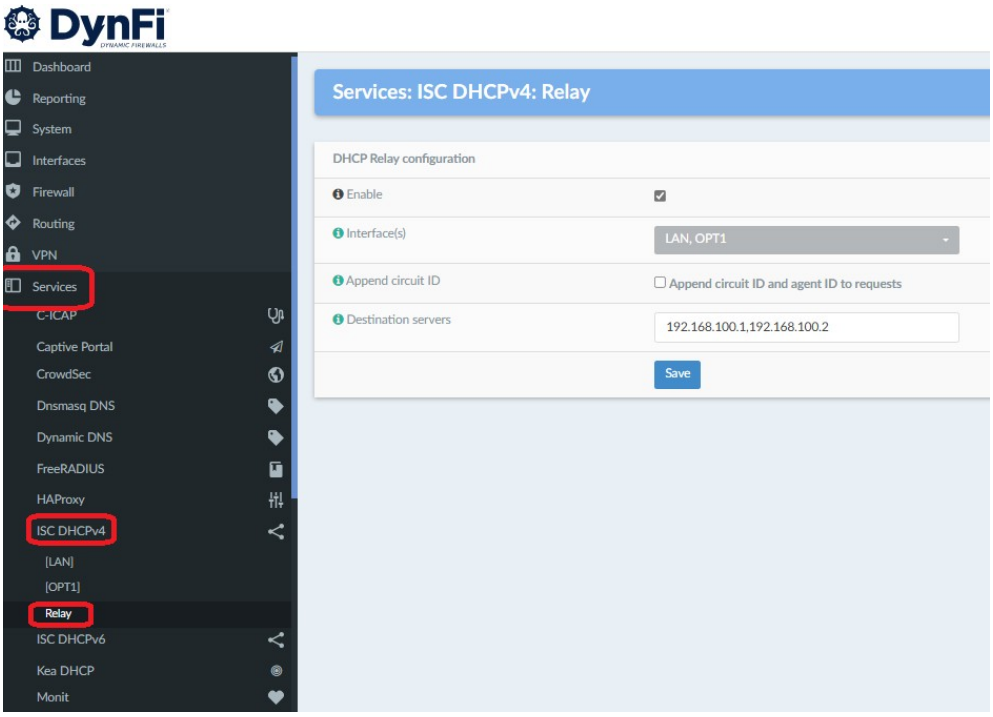
Pour configurer la réplication HA entre les deux DynFi, il est nécessaire de créer des adresses IP virtuelles. Ces adresses seront 192.168.100.254/24 et 192.168.110.254/24. Pour cela, il faut se rendre dans l'onglet Interfaces, puis IP virtuelles, et ajouter ces deux adresses en mode CARP sur l'interface LAN et OPT1. Lors de la création, il faut renseigner l'adresse IP, un mot de passe sécurisé, le VHID qui sera défini sur 1, l'AdvBase sur 1 également, et enfin la priorité qui doit être réglée sur 0 pour le primaire et 100 pour le secondaire. Une fois ces paramètres configurés, il ne reste plus qu'à ajouter une description, comme IPV LAN pour l'adresse du LAN et IPV LAN USERS pour l'autre.



Pour configurer la réplication entre les deux DynFi, il faut se rendre dans l'onglet Système, puis dans la section Haute Disponibilité. Dans le champ Synchronize Peer IP, il faut renseigner l'adresse IP de DynFi02. Ensuite, il faut activer le protocole XMLRPC Sync, entrer à nouveau l'adresse IP de DynFi02, ainsi que les identifiants (utilisateur et mot de passe) nécessaires pour assurer une synchronisation correcte. Enfin, il ne reste plus qu'à sélectionner les éléments à synchroniser, et dans notre cas, nous choisirons l'ensemble des paramètres pour une réplication complète.

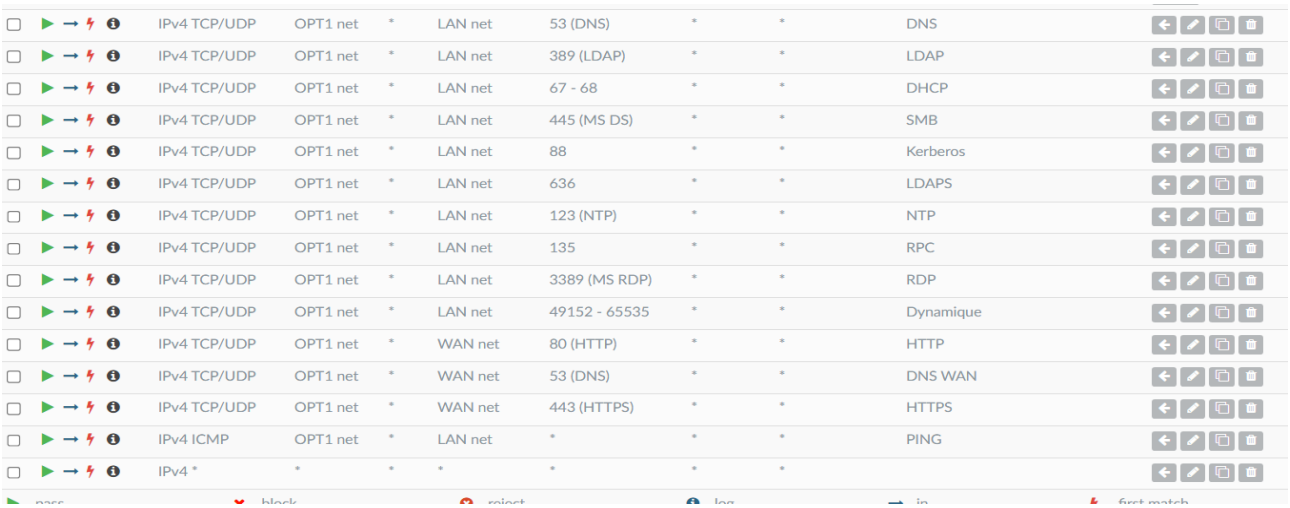


Il reste à activer le DHCP Relay, un service permettant aux postes du réseau LAN USERS de recevoir une adresse IP depuis le serveur DHCP situé sur le LAN. Pour cela, il faut se rendre dans Services > DHCPv4 > Relay, puis configurer les interfaces en sélectionnant LAN et OPT1. Enfin, il suffit d'indiquer l'adresse du serveur DHCP et d'enregistrer la configuration.



Il reste à configurer le NAT Outbound en le réglant sur "Hybrid Outbound NAT Rule Generation". Cette option permet de mieux contrôler la traduction des adresses IP internes en adresses IP publiques lorsqu'elles sortent du réseau local.

Ensuite, nous configurerons les règles du firewall. La stratégie consiste à tout bloquer par défaut, puis à autoriser uniquement les flux nécessaires. Par exemple, sur l'interface OPT1 (LAN USERS), voici les règles autorisées :



IPv4 TCP/UDP	OPT1 net	*	LAN net	53 (DNS)	*	*	DNS
IPv4 TCP/UDP	OPT1 net	*	LAN net	389 (LDAP)	*	*	LDAP
IPv4 TCP/UDP	OPT1 net	*	LAN net	67 - 68	*	*	DHCP
IPv4 TCP/UDP	OPT1 net	*	LAN net	445 (MS DS)	*	*	SMB
IPv4 TCP/UDP	OPT1 net	*	LAN net	88	*	*	Kerberos
IPv4 TCP/UDP	OPT1 net	*	LAN net	636	*	*	LDAPS
IPv4 TCP/UDP	OPT1 net	*	LAN net	123 (NTP)	*	*	NTP
IPv4 TCP/UDP	OPT1 net	*	LAN net	135	*	*	RPC
IPv4 TCP/UDP	OPT1 net	*	LAN net	3389 (MS RDP)	*	*	RDP
IPv4 TCP/UDP	OPT1 net	*	LAN net	49152 - 65535	*	*	Dynamique
IPv4 TCP/UDP	OPT1 net	*	WAN net	80 (HTTP)	*	*	HTTP
IPv4 TCP/UDP	OPT1 net	*	WAN net	53 (DNS)	*	*	DNS WAN
IPv4 TCP/UDP	OPT1 net	*	WAN net	443 (HTTPS)	*	*	HTTPS
IPv4 ICMP	OPT1 net	*	LAN net	*	*	*	PING
IPv4 *	*	*	*	*	*	*	

Conclusion

Ce projet fournit une infrastructure réseau robuste et adaptée aux besoins de TechSolutions. En adoptant les recommandations de l'ANSSI et des outils open source performants, l'entreprise bénéficie d'un réseau performant et économique, tout en préservant un bon niveau de sécurité.