



SOLUTION INFORMATIQUE

DOCUMENTATION TECHNIQUE

Epreuve E6 : Administration des systèmes et des réseaux

DATE

02/06/2025

RÉDACTEUR

Nohan BROCHARD

07 80 40 96 63

83 Rue André Le Notre, 30900 Nîmes, France

Sommaire

Sommaire.....	2
Présentation Générale	3
Mise en situation.....	3
Contexte et Objectifs	3
Serveur Windows Server 2022 / AD DS / DNS / DHCP	4
Installation du système d'exploitation	4
Configuration du Mot de passe Administrateur.....	6
Configuration du nom de serveur	6
Configuration Réseau en IP Fixe	8
Installation du rôle AD DS / DNS	9
Configuration du redirecteur DNS	13
Installation du rôle DHCP	15
Création et attribution des GPO	18
Affichage d'un fond d'écran personnalisé.....	19
Définir un raccourci GLPI sur le Bureau	21
Configuration du protocole RDP	22
Serveur Active Directory Redondant.....	25
Configuration réseau en IP Fixe	25
Rejoindre le domaine du contrôleur de domaine	26
Installation de la redondance Active Directory	27
Rejoindre le domaine du contrôleur de domaine	27
Promouvoir le serveur en contrôleur de domaine ADDS	29
Vérification de l'opération	32
Configuration du DHCP en basculement	33
Routeur PFSense	34
Installation de PFSense	34
Configuration du LAN & WAN	37
Configuration de PFSense (Interface WEB).....	37
Debian / GLPI	41
Installation du système d'exploitation	41
Installation de GLPI	45
Création d'un utilisateur.....	48
Client Windows 10	49
Installation du système d'exploitation	49
Configuration réseau	52
Rejoindre le domaine AD.....	53



Présentation Générale

Mise en situation

Ayant rejoint l'entreprise **NBRD Corporation**, une entreprise spécialisée dans les solutions informatiques pour les PME, j'ai pu mettre en évidence une infrastructure réseau **vieillissante et à risque**.

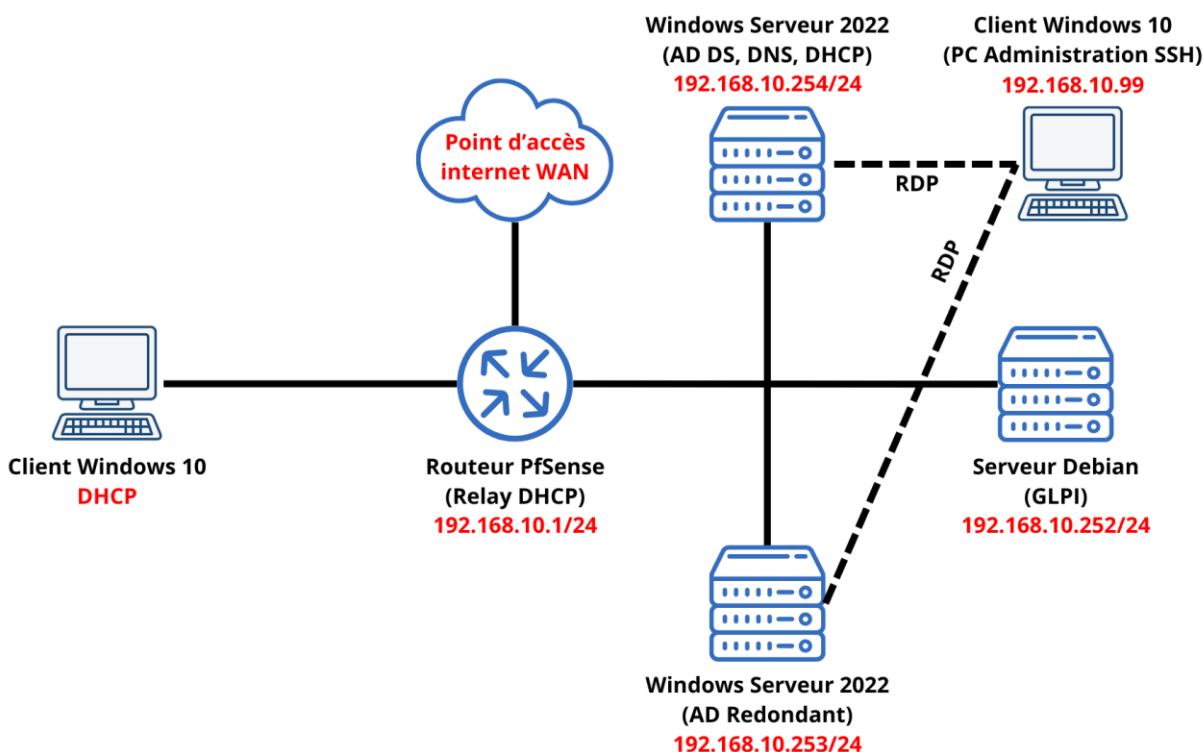
Actuellement, l'équipe chargé de la Hotline fonctionne sur un serveur sous **Windows Server 2008 R2** (*pour le logiciel de ticketing développer en interne*) ainsi qu'un autre Windows Server 2008 R2 (*Pour l'Active Directory, DHCP et DNS*), entraînant des ralentissements et une **fin de support de Microsoft** eu lieu le 14 janvier 2020.

Après quelques recherches, nous avons pu constater que notre serveur Windows Server 2008 R2 utilisé pour l'Active Directory était exposé sur internet et que les pings de l'extérieur n'étaient pas bloqués.

Une **modernisation complète** de l'infrastructure et une sécurisation s'impose pour améliorer les performances, renforcer la sécurité et assurer une redondance en cas d'incident.

Contexte et Objectifs

Ce projet vise à moderniser l'infrastructure réseau de **NBRD Corporation** en mettant en place une architecture entièrement virtualisée. Les principaux composants incluent :



- Un serveur GLPI pour la gestion centralisée des incidents techniques.
- Un contrôleur de domaine sous Windows Server 2022 intégrant AD DS, GPO, DNS et DHCP.
- Une solution de routage et de sécurité PFsense pour protéger le réseau.
- Une haute disponibilité assurée par un contrôleur de domaine redondant
- Une infrastructure virtualisée comprenant Windows Server 2022, Windows 10, Debian et PFsense.
- Un ordinateur Administration avec un accès directe sur le contrôleur de domaine via une connexion SSH.

Cette nouvelle infrastructure garantit flexibilité, sécurité et haute disponibilité des services tout en optimisant la gestion des ressources.

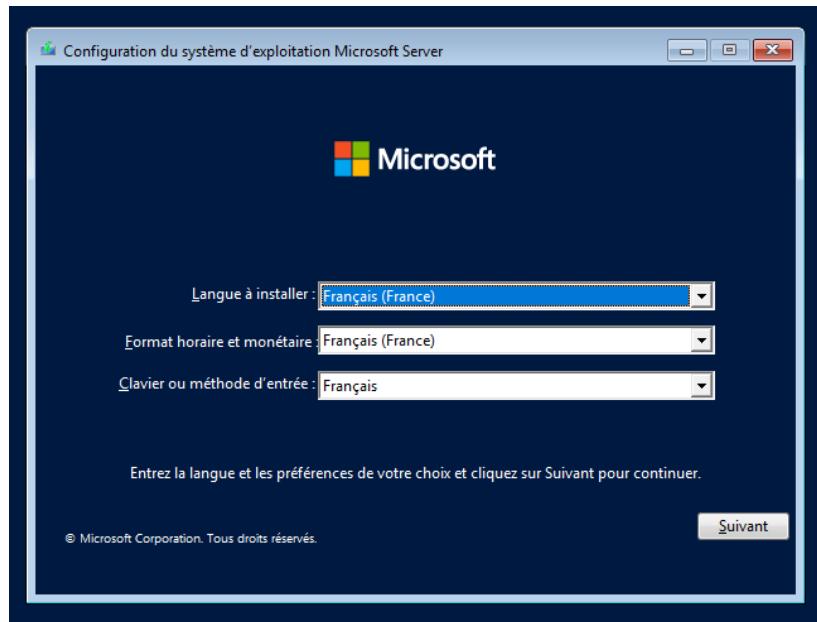


Serveur Windows Server 2022 / AD DS / DNS / DHCP

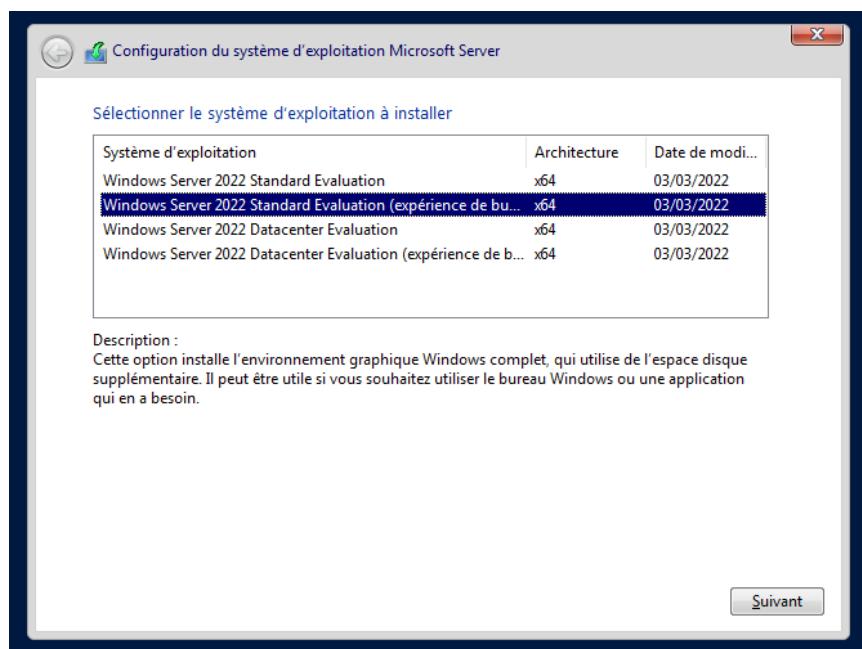
Je vais configurer un **Windows Server 2022** qui comprendra un service **DNS et DHCP** ainsi qu'un rôle **Active Directory (AD DS)**. Ce serveur sera utilisé pour gérer plusieurs utilisateurs organisés dans des Unités d'Organisation (UO) correspondant à leurs services métier, tel que RH, Technicien, Comptabilité, et Direction, ce qui remplacera l'ancien serveur Windows 2008 R2 de l'entreprise.

Installation du système d'exploitation

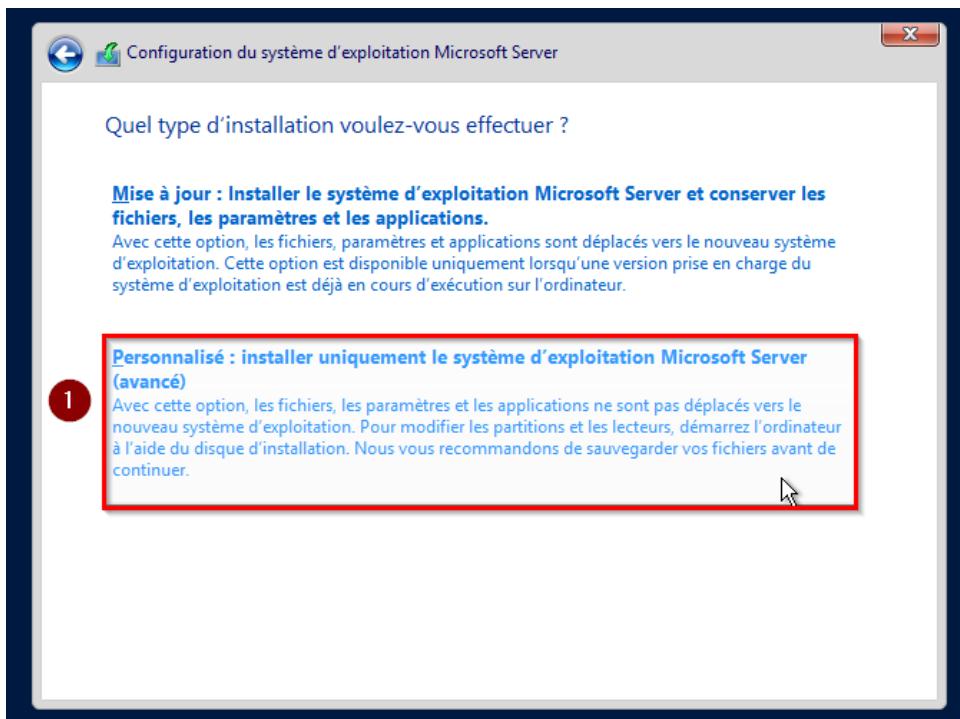
Une fois la **machine virtuelle** lancée, j'ouvre la console pour accéder à l'**interface graphique** de la VM. Pour la première configuration, je sélectionne la langue par défaut.



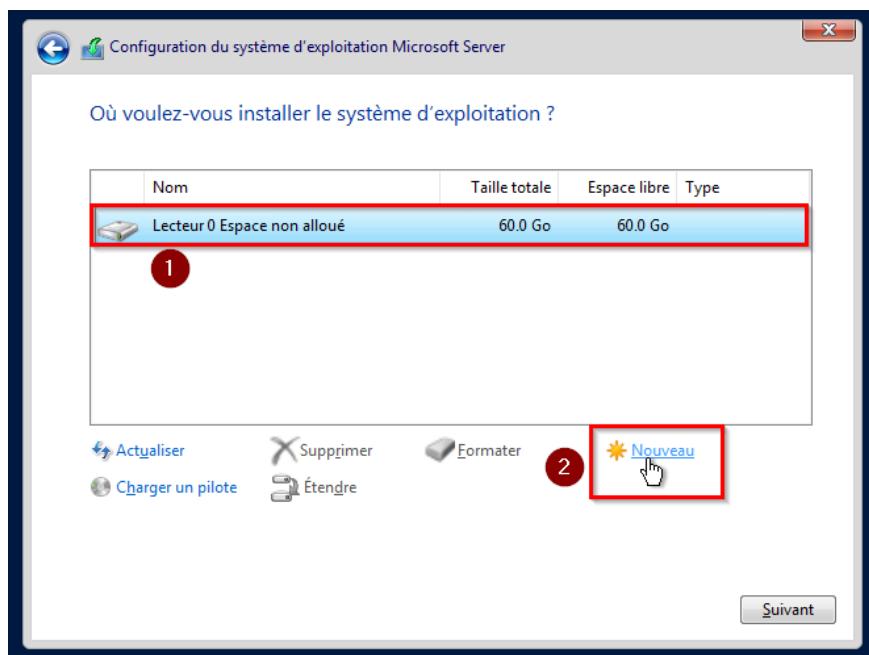
Afin de simplifier la configuration et la gestion, je sélectionne ma préférence entre la version graphique ou la ligne de commande. Dans ce cas, j'opte pour la **version graphique** qui est plus intuitif que la version en ligne de commande.



Ensuite, je choisis le type d'installation, avec le choix entre mise à jour et personnalisé. Dans ce cas, j'opte pour l'installation personnalisée, puis je sélectionne le lecteur 0 qui sera le disque dur système.



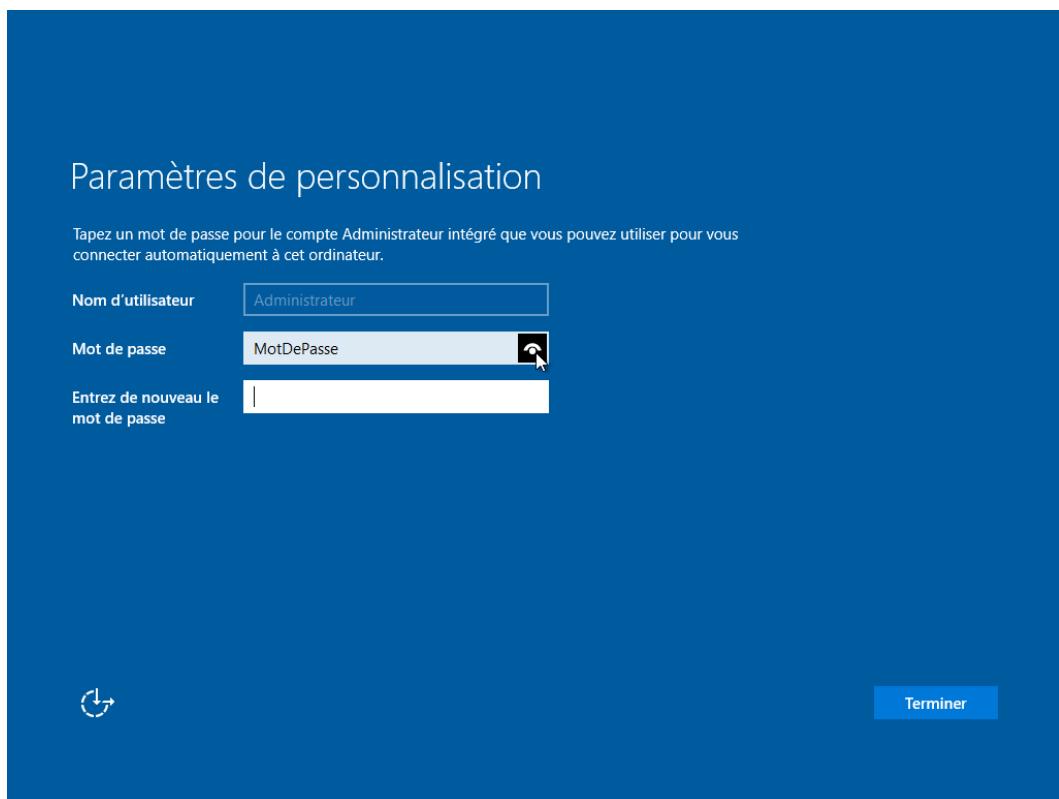
Pour sélectionner le lecteur 0, il faut **cliquer dessus**, ensuite aller dans **Nouveau** et faire **suivant**, cela allouera tous l'espace disque disponible sur celui-ci.



Une fois cette étape passée j'attends la **fin de l'installation**, la machine virtuelle **redémarra à la fin de l'installation**. Une fois toutes c'est étape faite, on peut passer à la configuration

Configuration du Mot de passe Administrateur

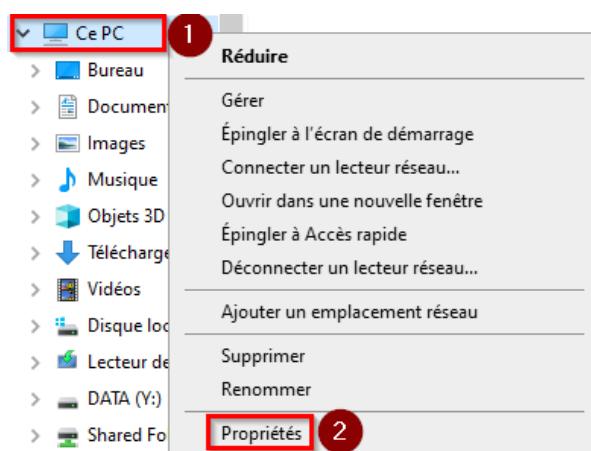
Une fois que le système d'exploitation redémarré, la prochaine étape consiste à saisir le mot de passe pour le **compte administrateur**.



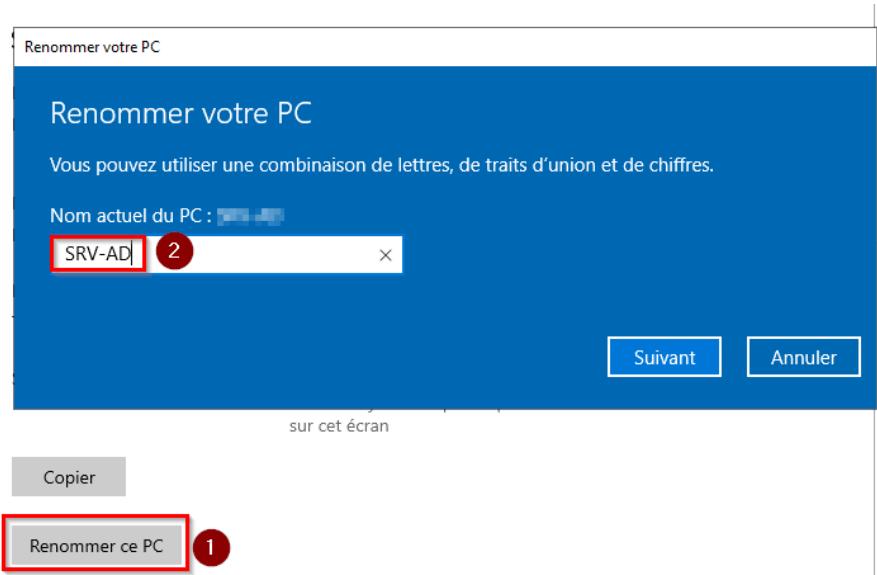
Une fois cette étape terminée, j'aurai la possibilité de **me connecter au compte administrateur local** du serveur.

Configuration du nom de serveur

Une fois connecté au compte administrateur local du serveur, nous allons dans un premier temps renommer le serveur. Pour cela, je me rends dans l'Explorateur de fichiers Windows, puis dans « **Ce PC** ». Ensuite je vais dans **propriétés** pour modifier le nom de la machine sous Windows Server 2022.



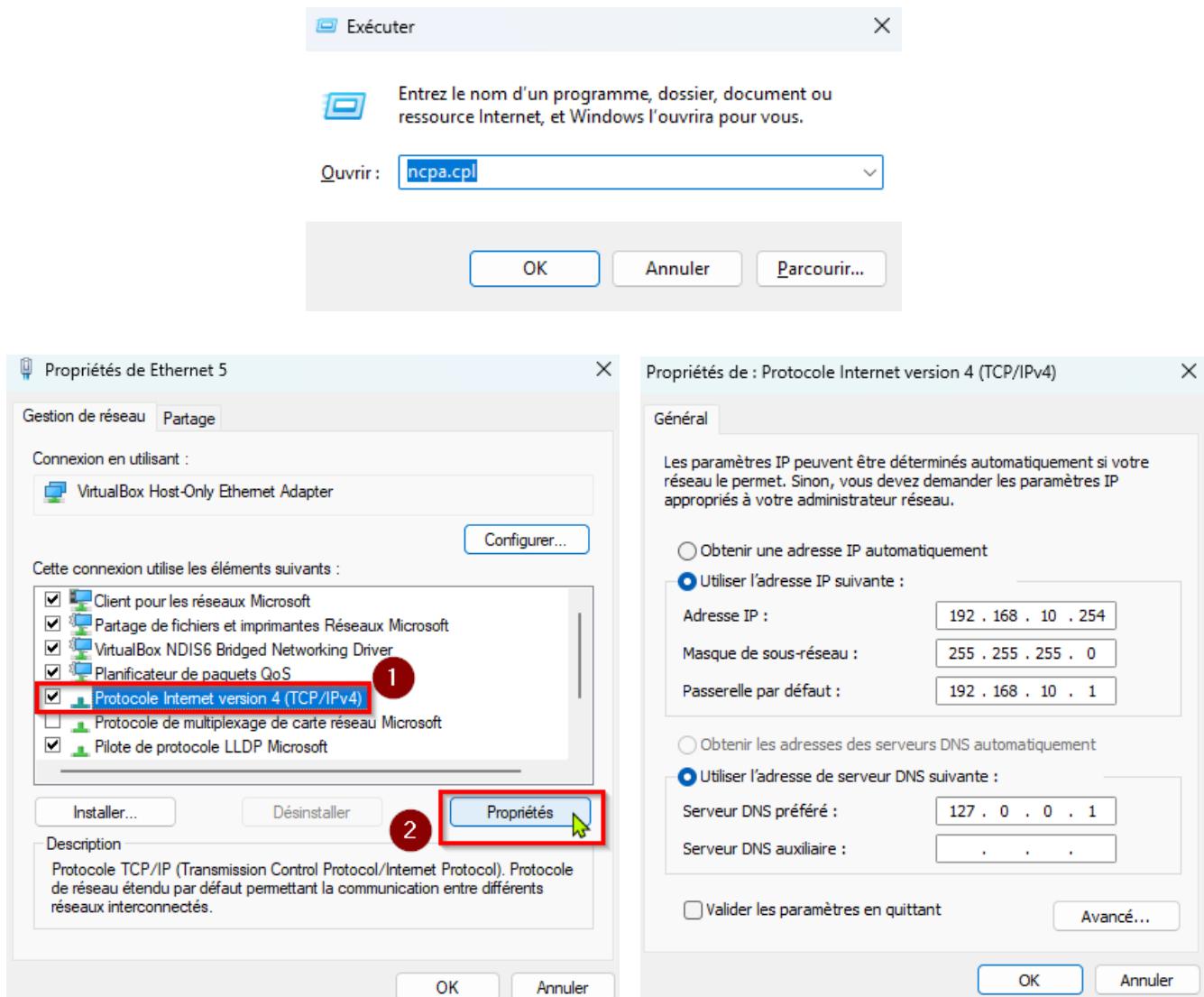
Une fois dans les propriétés, je clique sur « Renommer ce PC », puis j'insère le nom « SRV-AD » pour indiquer que le serveur est le contrôleur de domaine (DC).



Enfin, un **redémarrage sera requis** pour que les modifications prennent effet sur la machine Windows.

Configuration Réseau en IP Fixe

Je vais configurer l'adresse IP du serveur **Active Directory** sur **192.168.10.254**, qui se situe à la fin de ma plage d'adresses statiques, sur l'adaptateur **Ethernet 0**. Les machines virtuelles en **DHCP** auront des adresses allant de **192.168.1.10** à **192.168.1.200**.

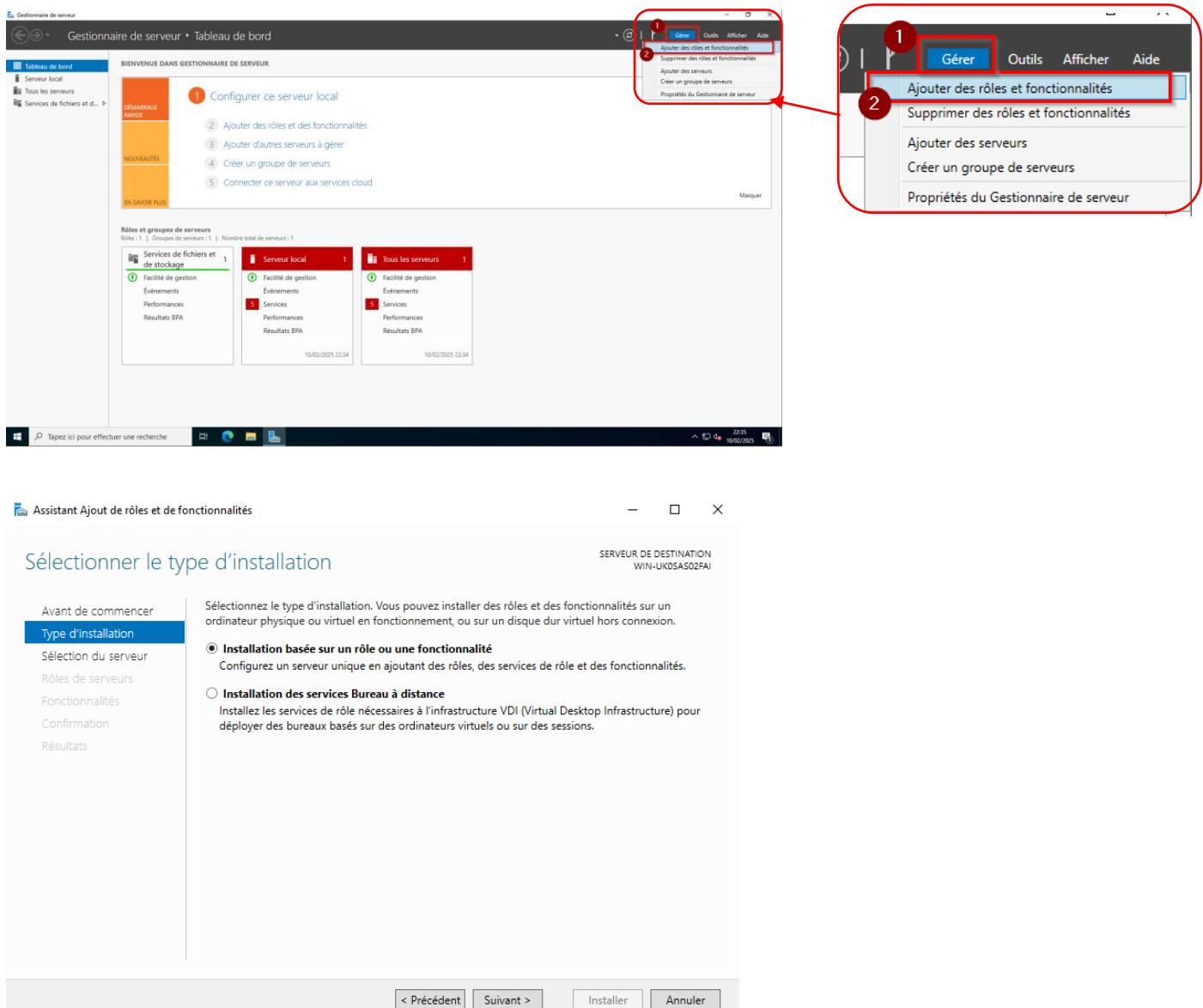


La **passerelle par défaut** est l'adresse IP configurée sur le **routeur PfSense** sur l'interface **LAN**. Pour le **serveur DNS préféré**, nous utilisons **127.0.0.1**, l'adresse IP **localhost**, car le serveur **AD** fait également office de **serveur DNS**. Nous pouvons également rajouter **8.8.8.8** en serveur DNS auxiliaire si nécessaire.

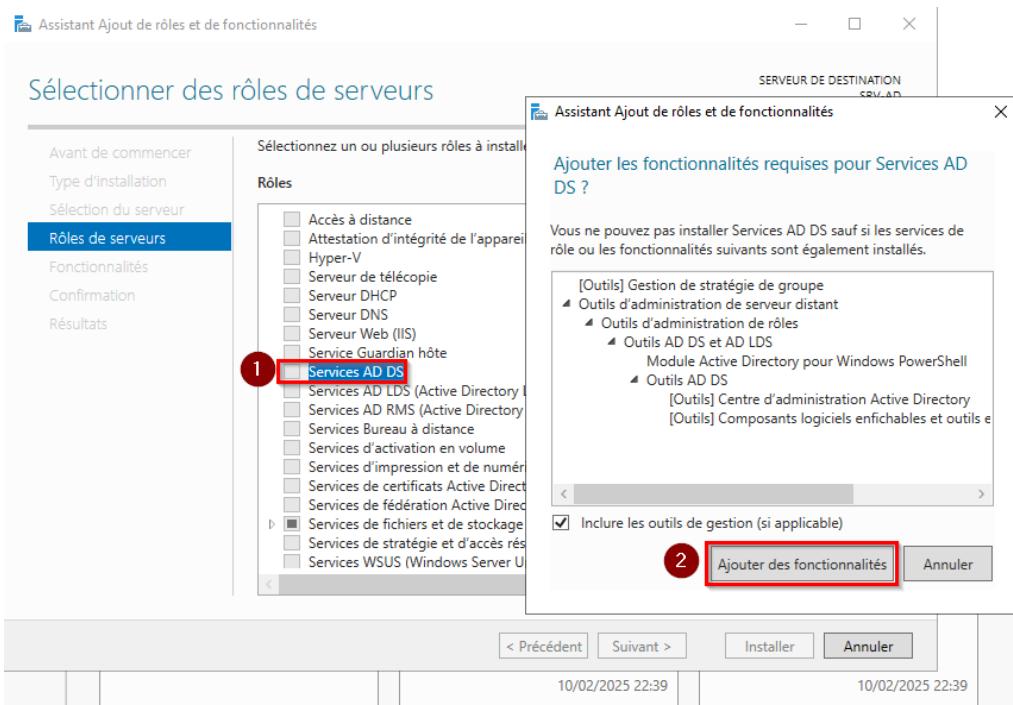


Installation du rôle AD DS / DNS

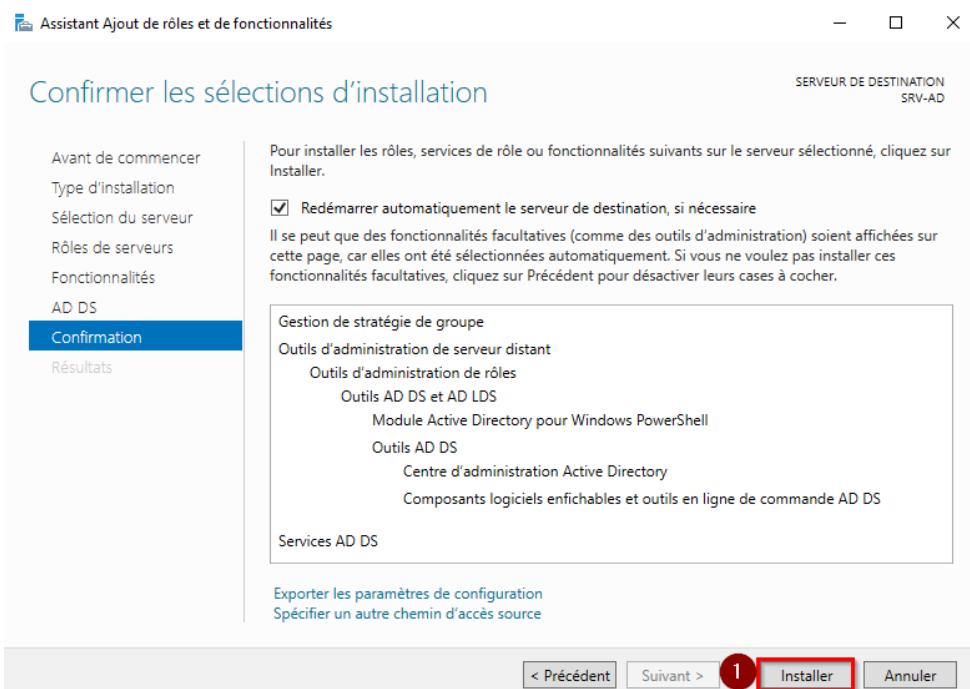
Je commence par ouvrir le « **Gestionnaire de serveur** », puis je clique sur « **Gérer** » et je sélectionne « **installer des rôles et fonctionnalités** » afin d'ajouter le rôle « **Services AD DS** ». Je passe l'étape « **Avant de commencer** » et je choisis « **Installation basée sur un rôle ou une fonctionnalité** » comme « **Type d'installation** ».



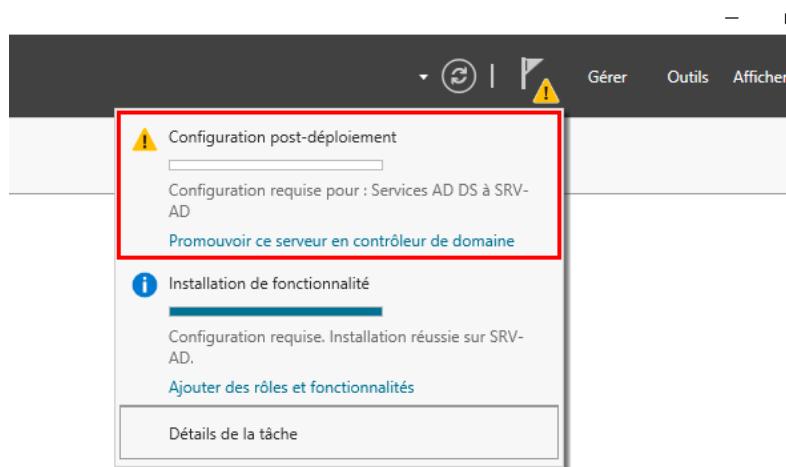
Je passe l'étape « **Sélection du serveur** » puisque j'agis sur le **serveur local**. Lorsque l'étape « **Rôles de serveurs** » s'affiche, je coche le rôle « **Services AD DS** » et je valide en cliquant sur « **Ajouter des fonctionnalités** » pour m'assurer que tout est installé, y compris les consoles de gestion.



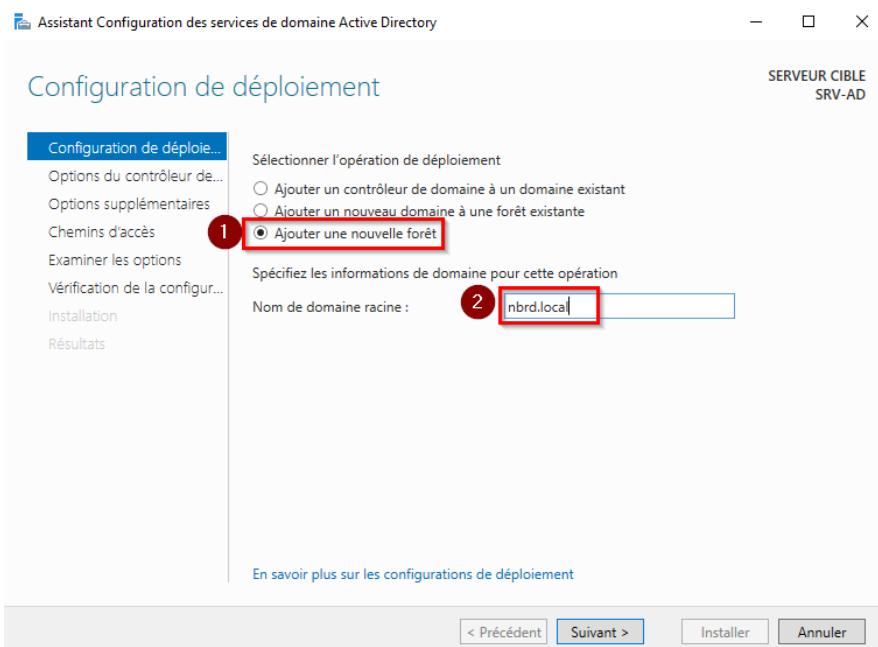
Je poursuis jusqu'à l'étape « **Confirmation** » et je clique sur « **Installer** ». Ensuite, je patiente un instant...



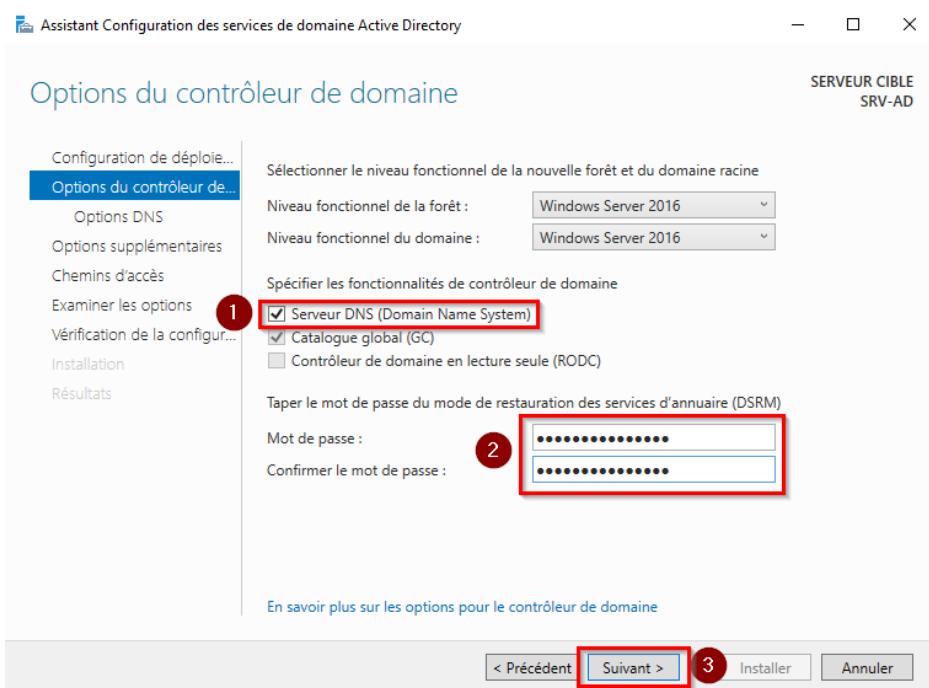
Une fois l'installation du rôle terminée, un **avertissement** s'affiche dans le Gestionnaire de serveur. Par curiosité, je clique dessus pour continuer et j'utilise le bouton « **Promouvoir ce serveur en contrôleur de domaine** ».



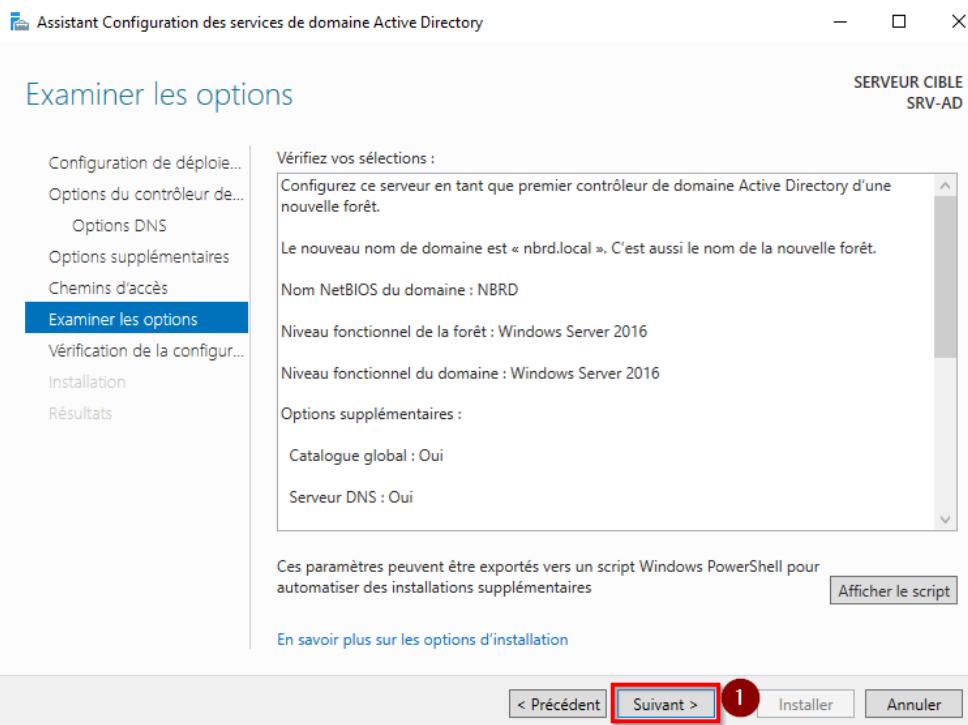
Un nouvel assistant s'exécute. Je sélectionne « **Ajouter une nouvelle forêt** » et je spécifie le nom du domaine, qui est « **nbrd.local** ».



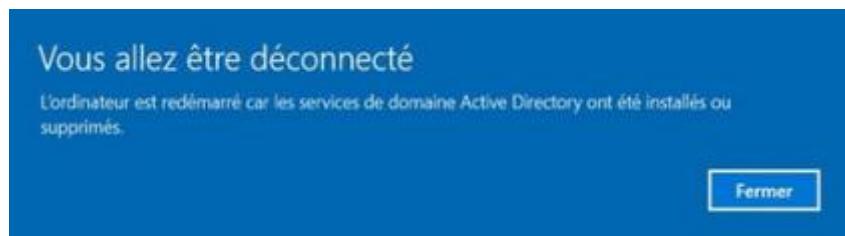
À l'étape suivante, je sélectionne les options pour ce contrôleur de domaine. Je coche « **Serveur DNS** » et j'indique un **mot de passe complexe** pour la restauration des services d'annuaire.



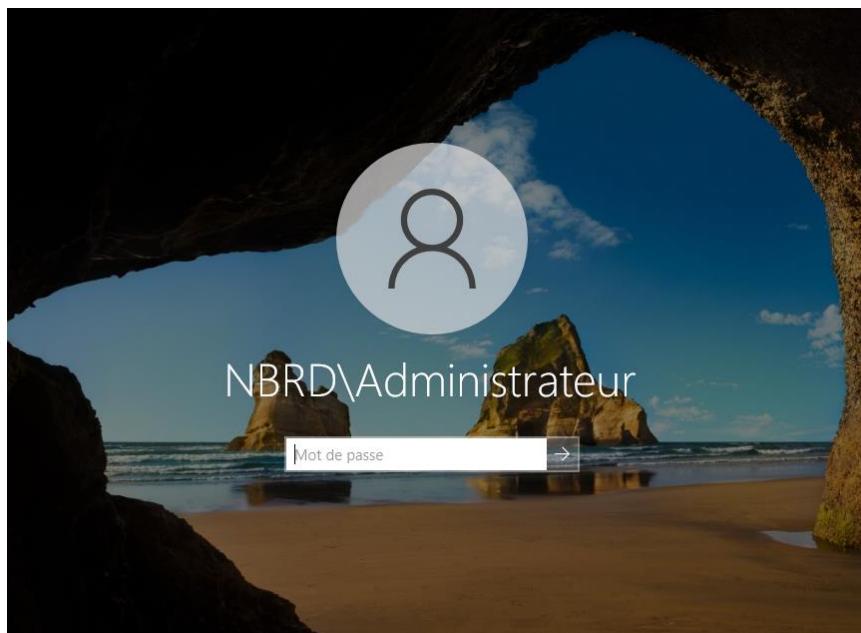
Ensuite, Je laisse le nom **NetBIOS** par défaut, qui sert à identifier le serveur sur le réseau dans les environnements Windows. Par la suite, l'étape de vérification de la configuration s'affiche. Si tout est en ordre, comme dans l'exemple ci-dessous, je clique sur « **Installer** ».



Lorsque l'**opération est terminée**, le serveur redémarre automatiquement dans la minute pour appliquer les modifications et finaliser la configuration du rôle de contrôleur de domaine.



Après le redémarrage, le serveur est devenu un **contrôleur de domaine Active Directory** ! Nous pouvons le vérifier grâce au **nom d'affichage** qui indique le **nom de domaine** et le **nom d'utilisateur**. Il est désormais configuré comme un **annuaire centralisé**, servant à gérer et centraliser les informations sur les **utilisateurs**, les **groupes**, et les **ressources** du réseau.



Je peux également constater dans l'**annuaire Active Directory** des utilisateurs et ordinateurs, que notre contrôleur de domaine, apparaît avec le nom de notre serveur « SRV-AD ».

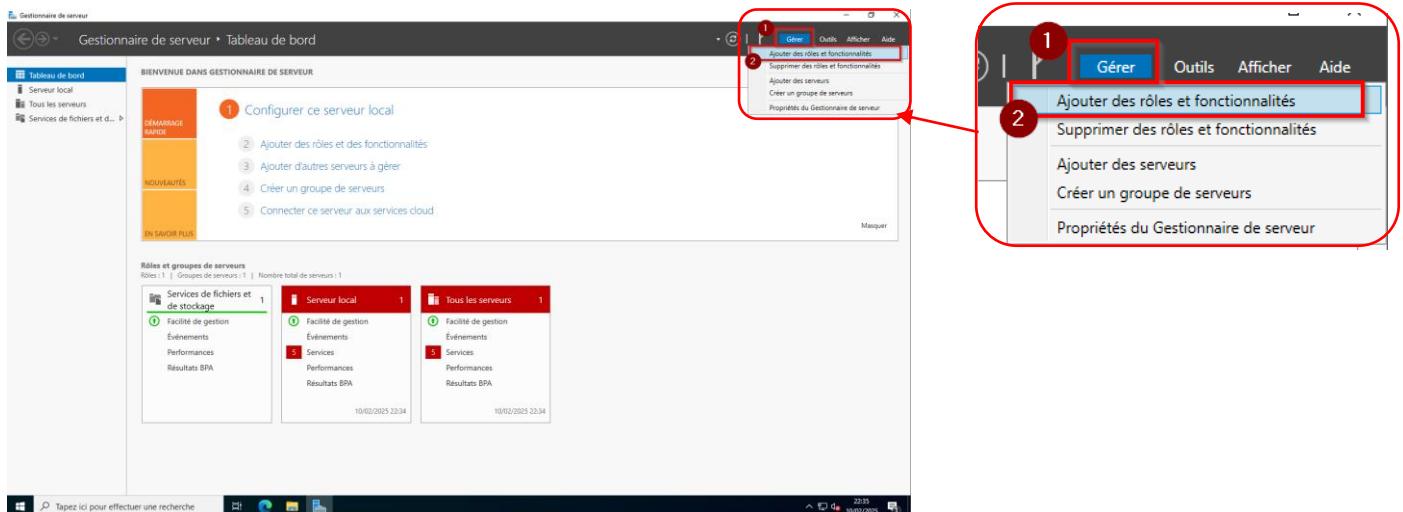
Nom	Type	Type de contrô...	Site	Descript
SRV-AD	Ordinateur	GC	Default-First-Si...	
SRV-AD-PRA	Ordinateur	GC	Default-First-Si...	



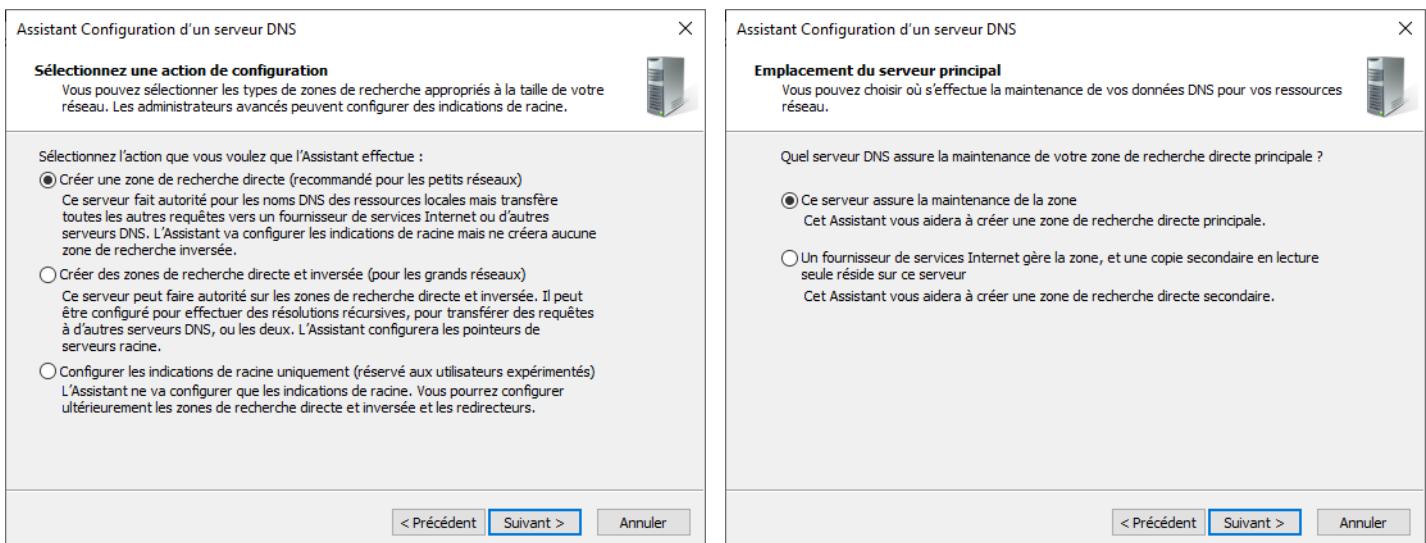
Configuration du redirecteur DNS

Actuellement, après l'installation du rôle **AD DS**, mon serveur communique uniquement avec le réseau interne. Pour permettre la résolution des noms de domaine externes, nous allons ajouter et configurer le rôle DNS avec un **re-directeur externe** tel que **8.8.8.8** (DNS de Google).

Je commence par ouvrir le **Gestionnaire de serveur**, sélectionner « **Installer des rôles et fonctionnalités** », choisir « **Serveur DNS** » comme rôle à installer, puis cliquer sur « **Ajouter des fonctionnalités** ».



Une fois l'installation terminée, je vais dans la section DNS du **Gestionnaire de serveur**, à gauche, où je peux voir tous les rôles activés ainsi que le tableau de bord.



Assistant Configuration d'un serveur DNS

Selectionnez une action de configuration
Vous pouvez sélectionner les types de zones de recherche appropriés à la taille de votre réseau. Les administrateurs avancés peuvent configurer des indications de racine.

Créer une zone de recherche directe (recommandé pour les petits réseaux)
Ce serveur fait autorité pour les noms DNS des ressources locales mais transfère toutes les autres requêtes vers un fournisseur de services Internet ou d'autres serveurs DNS. L'Assistant va configurer les indications de racine mais ne créera aucune zone de recherche inversée.

Créer des zones de recherche directe et inversée (pour les grands réseaux)
Ce serveur peut faire autorité sur les zones de recherche directe et inversée. Il peut être configuré pour effectuer des résolutions récursives, pour transférer des requêtes à d'autres serveurs DNS, ou les deux. L'Assistant configurera les pointeurs de serveurs racine.

Configurer les indications de racine uniquement (réservé aux utilisateurs expérimentés)
L'Assistant ne va configurer que les indications de racine. Vous pourrez configurer ultérieurement les zones de recherche directe et inversée et les redirecteurs.

< Précédent Suivant > Annuler

Assistant Configuration d'un serveur DNS

Emplacement du serveur principal
Vous pouvez choisir où s'effectue la maintenance de vos données DNS pour vos ressources réseau.

Ce serveur assure la maintenance de la zone
Cet Assistant vous aidera à créer une zone de recherche directe principale.

Un fournisseur de services Internet gère la zone, et une copie secondaire en lecture seule réside sur ce serveur
Cet Assistant vous aidera à créer une zone de recherche directe secondaire.

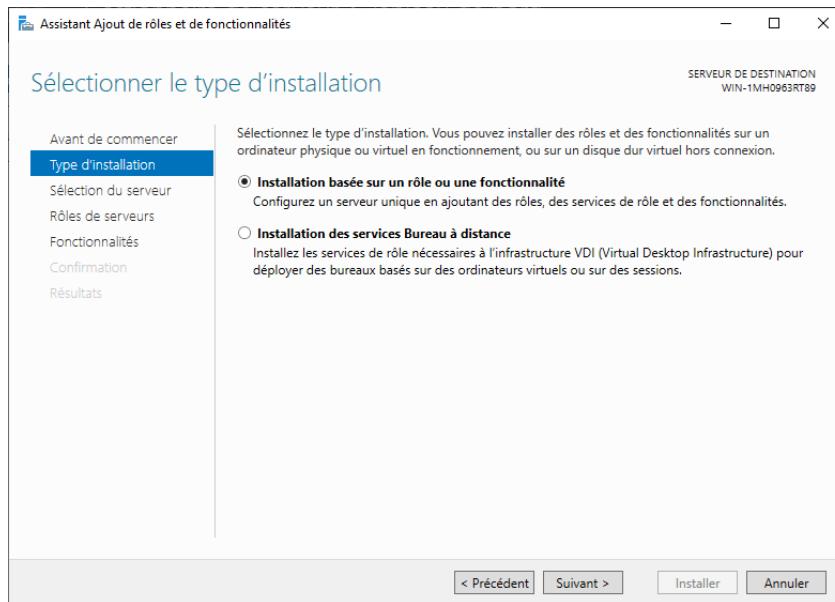
< Précédent Suivant > Annuler

Nous allons ensuite configurer le rôle **DNS**, une fois dans l'assistant **Configuration d'un serveur DNS**, nous allons sélectionner « **Créer une zone de recherche directe** » et on va ensuite choisir « **Ce serveur assure la maintenance de la zone** ».

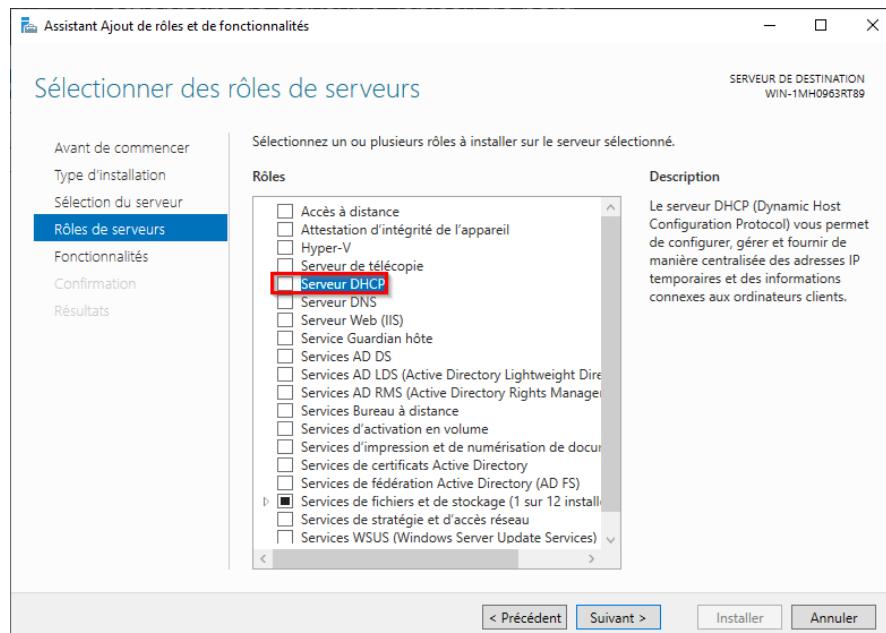


Installation du rôle DHCP

Je lance le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et fonctionnalités**, puis cochez **Serveur DHCP** et installez.

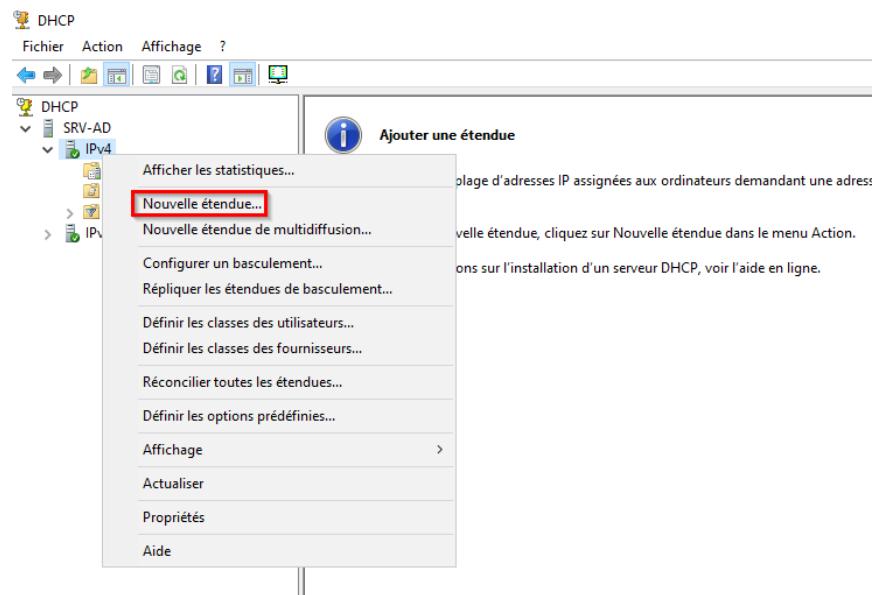


Je passe l'étape « **Sélection du serveur** » puisque j'agis sur le **serveur local**. Lorsque l'étape « **Rôles de serveurs** » s'affiche, je coche le rôle « **Serveur DHCP** » et je valide en cliquant sur « **Ajouter des fonctionnalités** » pour m'assurer que tout est installé, y compris les consoles de gestion.

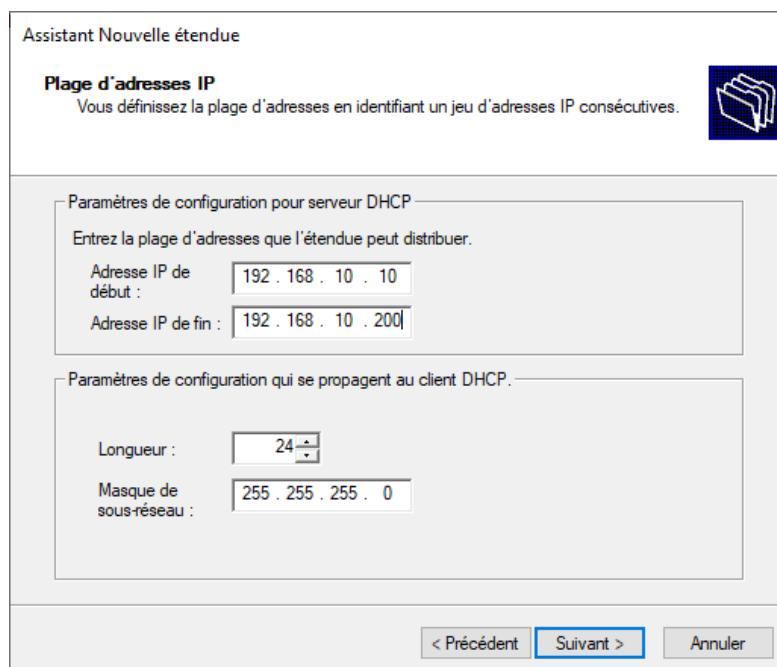


Je poursuis jusqu'à l'étape « Confirmation » et je clique sur « Installer ». Ensuite, je patiente un instant... Une fois l'installation terminée, je clique sur **Configurer l'autorisation DHCP** dans la notification sur le Tableau de bord du serveur, je sélectionne le compte administrateur. Je clique sur « **Suivant** » jusqu'à ce que la configuration soit terminée et que le serveur soit opérationnel.

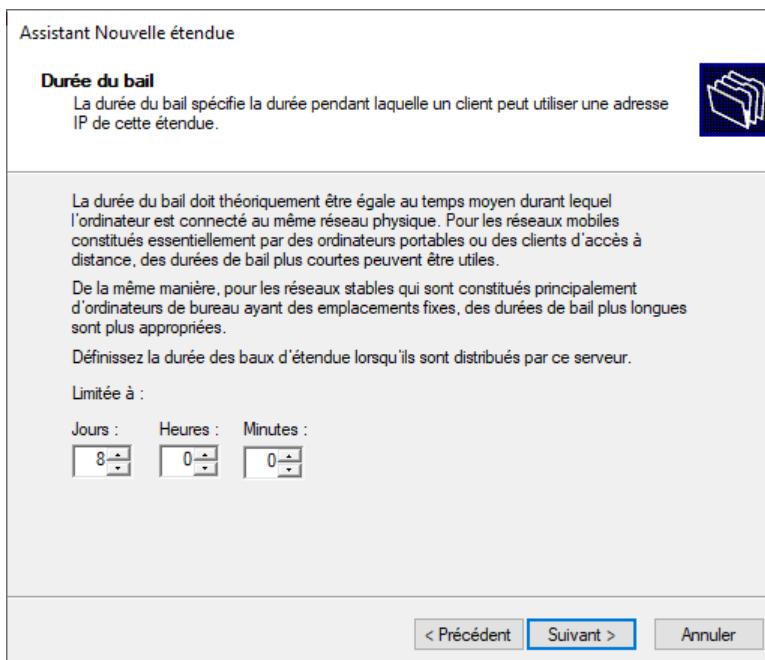
Je me rends dans **DHCP** via le menu Windows, je clique sur « **IPv4** », puis je crée une nouvelle étendue DHCP.



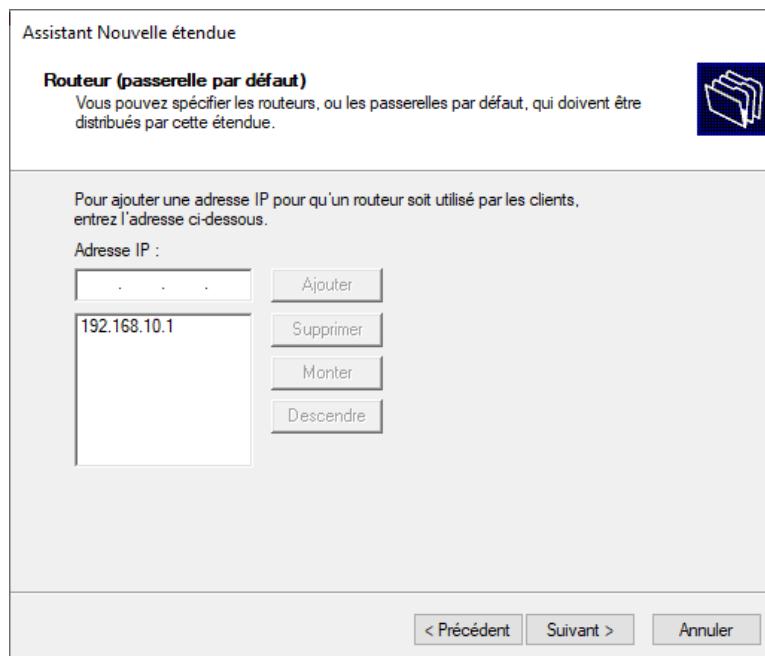
Je renseigne un nom pour l'étendue lorsqu'il est demandé, puis je clique sur « **Suivant** ». Par la suite, je renseigne l'adresse IP de début et de fin de mon étendue DHCP, en choisissant des adresses IP appartenant au réseau de ma carte réseau créée auparavant (192.168.10.0/24).



Je définis une durée de bail de **8 jours**, sans aucune expulsion ni retard, puis je poursuis la configuration.



Je sélectionne « **Oui, je veux configurer les options maintenant** », puis je clique sur « **Suivant** ». Dans la section Passerelle par défaut, j'insère l'adresse IP mon interface LAN de mon PFSense (192.168.10.1).



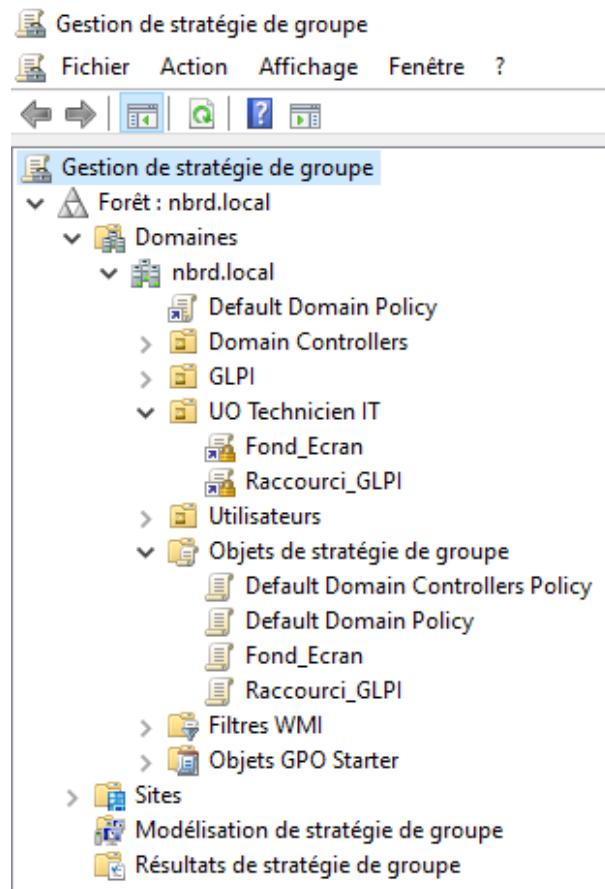
Le **DHCP** est configuré et fonctionne correctement, il attribuera automatiquement des adresses IP aux machines qui se connectent au réseau.



Création et attribution des GPO

J'ai mis en place les GPO (Group Policy Objects) suivantes pour **automatiser** l'implémentation de raccourci et de mise en place d'un fond d'écran commun sur les **postes informatiques** :

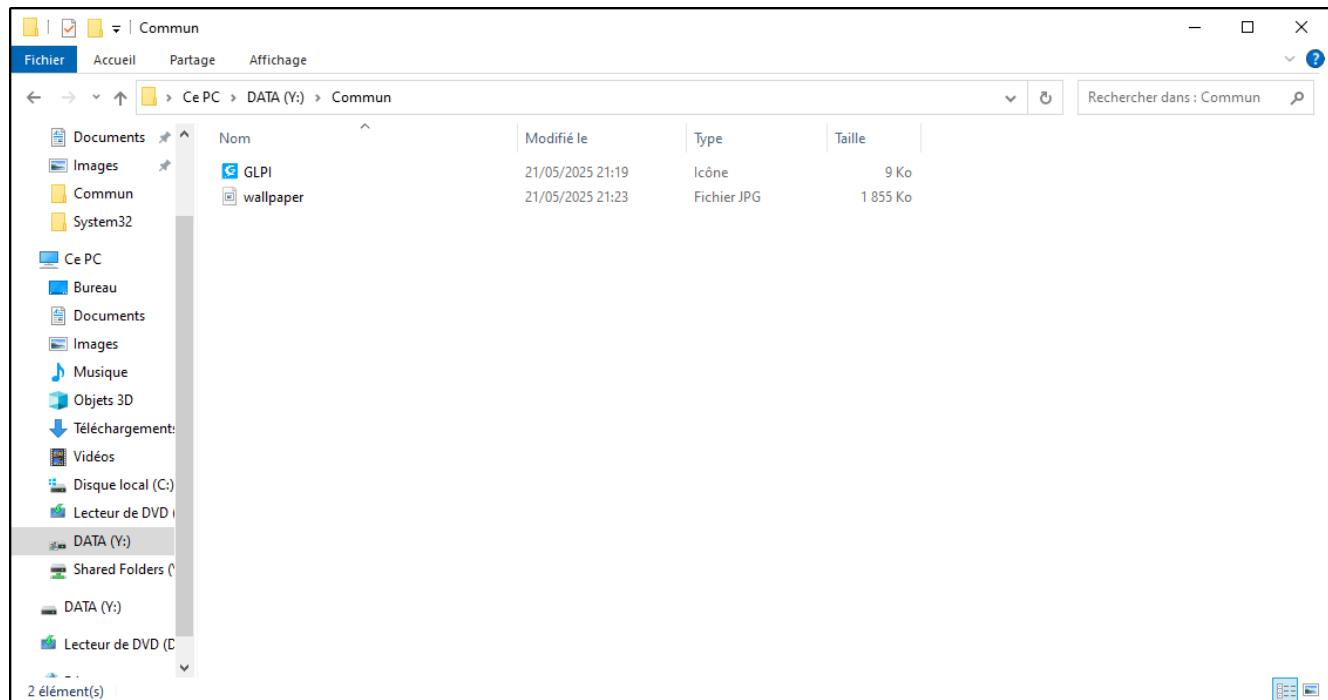
- Une GPO pour définir automatiquement un fond d'écran,
- Une GPO pour définir un raccourci GLPI sur le bureau



Affichage d'un fond d'écran personnalisé

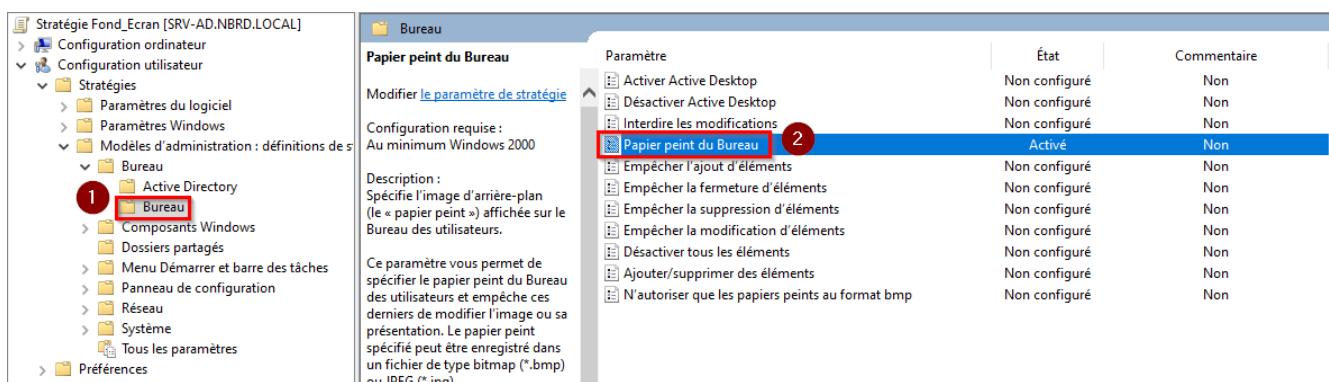
Je commence par la création de la **GPO** (*Group Policy Object*). Ensuite, je récupère auprès du service RH de **NBRD Corporation** le **fond d'écran** que l'entreprise souhaite déployer automatiquement sur les postes de travail des collaborateurs. Pour cela, je place le fichier image (.png) dans un dossier partagé sur le réseau de mon serveur Active Directory, accessible par les collaborateurs.

Cela permet à la GPO de récupérer et appliquer l'image automatiquement sur leurs écrans.



Je dois activer un paramètre spécifique nommé « Papier peint du Bureau ». Pour ce faire, je navigue vers Configuration utilisateur > Modèles d'administration > Bureau > Bureau.

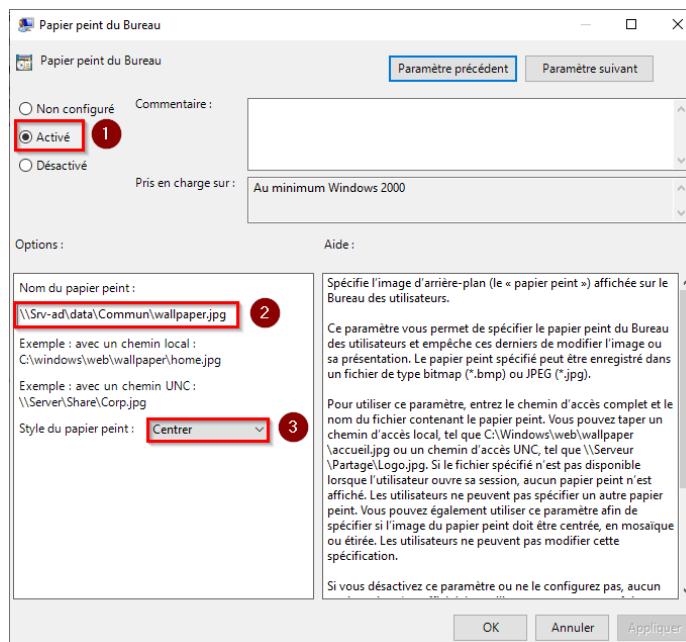
En activant ce paramètre, je définis le chemin de l'image de fond d'écran qui doit s'afficher sur les postes de travail des collaborateurs.



	État	Commentaire
Activer Active Desktop	Non configuré	Non
Désactiver Active Desktop	Non configuré	Non
Interdire les modifications	Non configuré	Non
Papier peint du Bureau	Activé	Non
Empêcher l'ajout d'éléments	Non configuré	Non
Empêcher la fermeture d'éléments	Non configuré	Non
Empêcher la suppression d'éléments	Non configuré	Non
Empêcher la modification d'éléments	Non configuré	Non
Désactiver tous les éléments	Non configuré	Non
Ajouter/supprimer des éléments	Non configuré	Non
N'autoriser que les papiers peints au format bmp	Non configuré	Non

Comme pour chaque GPO, une fois dans l'interface de ma GPO pour le papier peint du bureau, je coche « Activé », puis j'insère le chemin d'accès vers l'image à afficher automatiquement : « **Fichier partage\Wallpaper\wallpaper.png** ». J'ajoute également le nom de la GPO en commentaire pour faciliter son identification et sa gestion future.

Ensuite, j'applique la règle en cliquant sur « Appliquer » pour que les paramètres prennent effet et que le fond d'écran soit déployé automatiquement sur les postes de travail des collaborateurs.

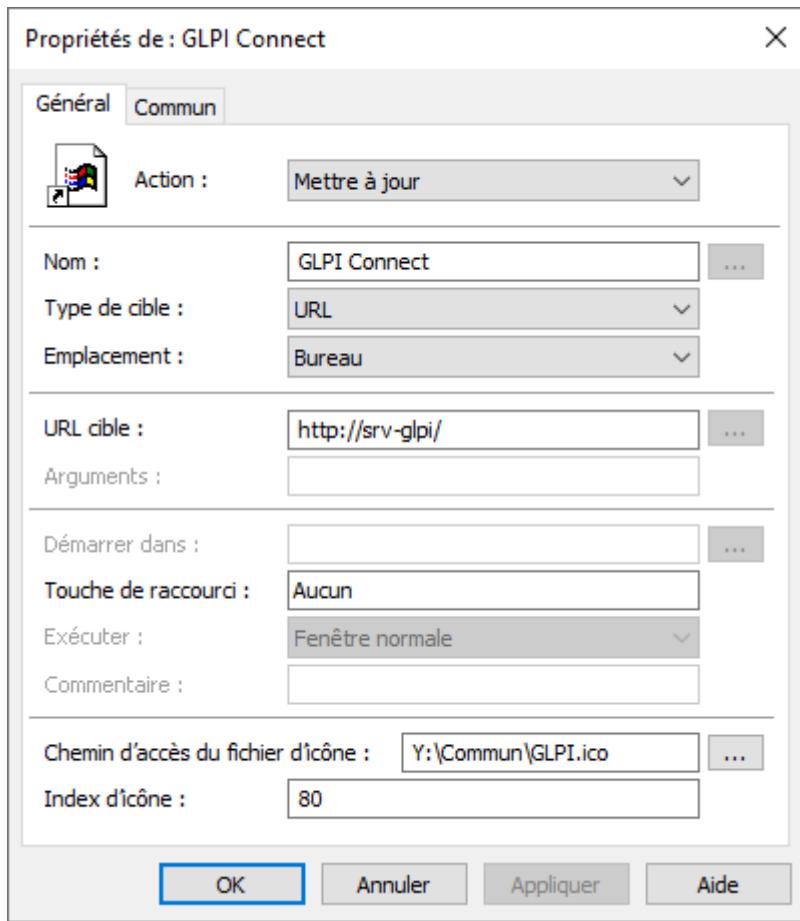


Définir un raccourci GLPI sur le Bureau

Après avoir créé et nommé la GPO, je me rends dans **Configuration utilisateur > Paramètres Windows > Ressources de bureau > Raccourcis**. Ensuite, je clique avec le bouton droit et sélectionne « Nouveau » > « Raccourci » pour créer un nouveau raccourci.

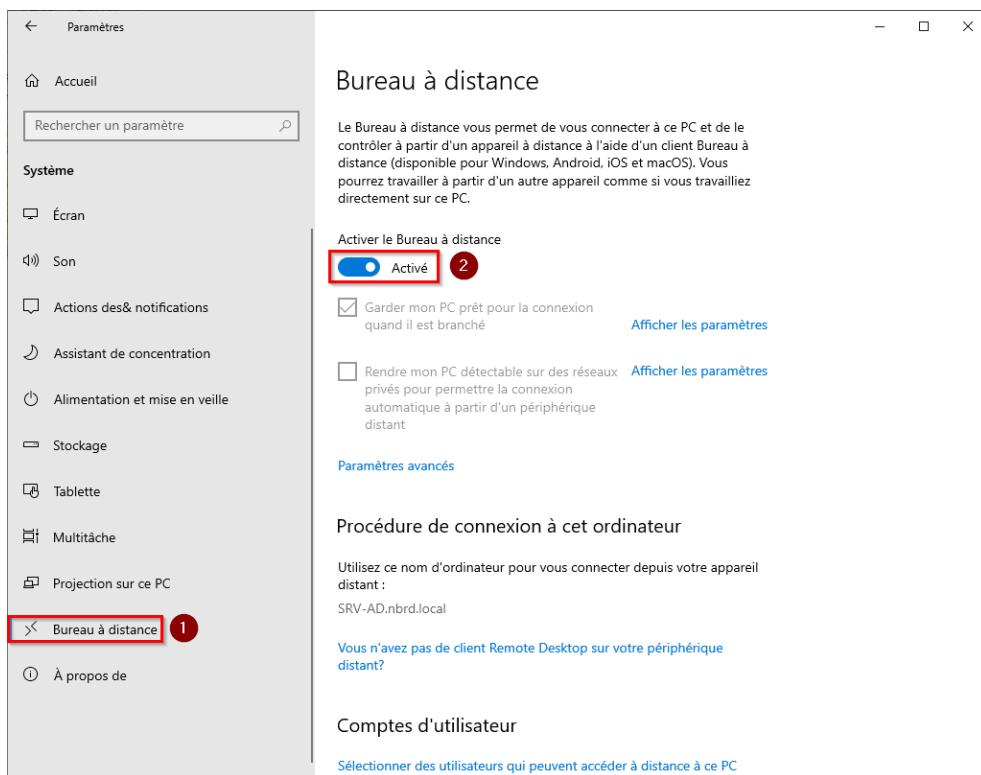


Une fois dans l'interface de création d'un nouveau raccourci, je sélectionne l'action « **Mettre à jour** » pour configurer le raccourci. Ensuite, je définis le nom du raccourci comme « **GLPI Connect** » pour qu'il soit intuitif lors de la formation interne de **NBRD Corporation** sur l'utilisation de GLPI. Je choisis « **Bureau** » comme emplacement pour que le raccourci soit facilement accessible pour les collaborateurs, puis je renseigne l'**adresse d'accès à l'interface web de GLPI**.



Configuration du protocole RDP

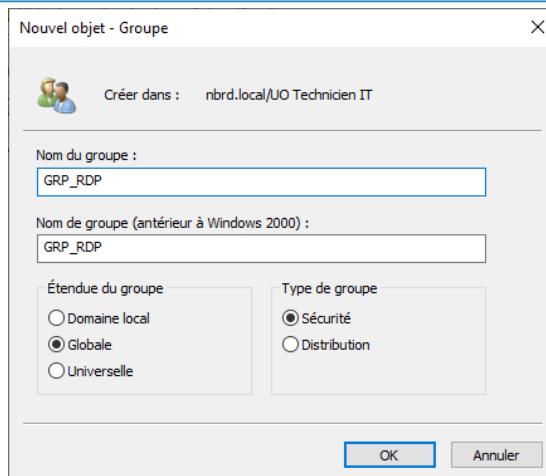
Pour pouvoir prendre la **main à distance** sur le **contrôleur de domaine** et sur l'**Active Directory**, je vais activer le « **Bureau à distance** » dans les **Paramètres Windows** sur le **SRV-AD**.



Par la suite, je vais créer un groupe « **GRP_RDP** » dans l'**Active Directory** afin qu'il y ait que les utilisateurs de ce groupe qui puise accéder au RDP.

The screenshot shows the Active Directory Users and Computers (ADUC) interface. The left pane shows the domain structure. The right pane shows a user account ('Nohan BROCHARD'). A context menu is open over the user account, with the 'Nouveau' option highlighted with a red box. A secondary context menu is displayed, with the 'Groupe' option highlighted with a red box.





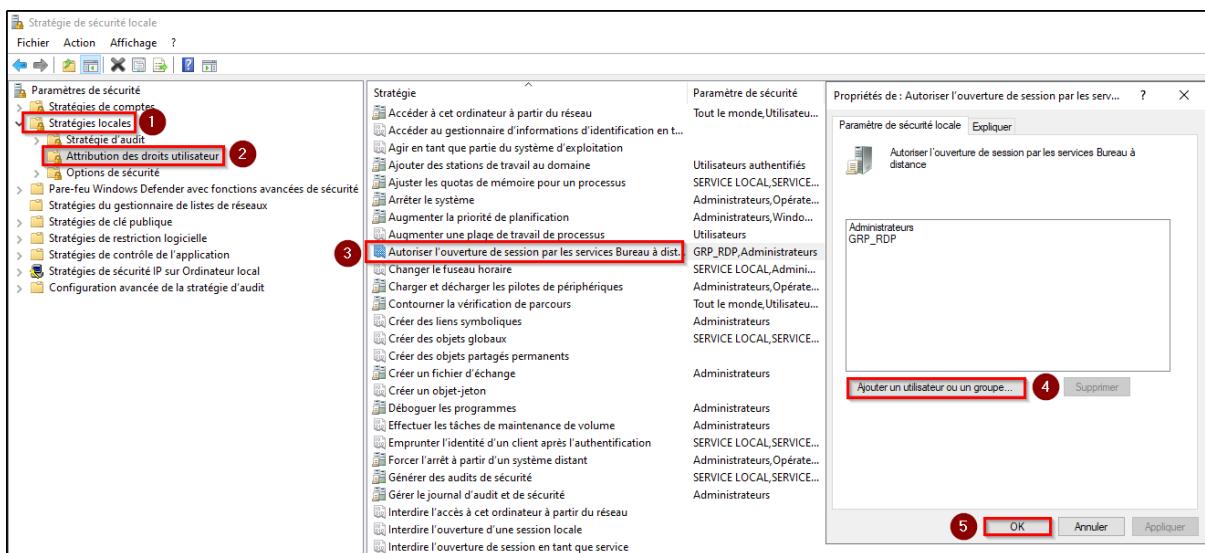
Ensute j'ajoute l'utilisateur dans le groupe « **GRP_RDP** » qui doit avoir **accès à la connexion à distance** sur l'**Active Directory**.

Nom	Type	Description
GRP_RDP	Groupe de sécurité	
Nohan BROCHARD	Utilisateur	



Pour pouvoir ouvrir une session sur le serveur distant, nous allons devoir ajouter dans les stratégies de sécurité locale, l'autorisation pour le groupe « GRP_RDP » d'ouvrir une session par les services Bureau à distance.

Pour cela, nous allons ouvrir « **secpol.msc** » > **Stratégies locales > Attribution des droits utilisateurs > Autoriser l'ouverture de session par les services Bureau à distance**, et ajouter « **GRP_RDP** ».



Une fois cela fait, nous pouvons désormais ouvrir une session sur le serveur distant.

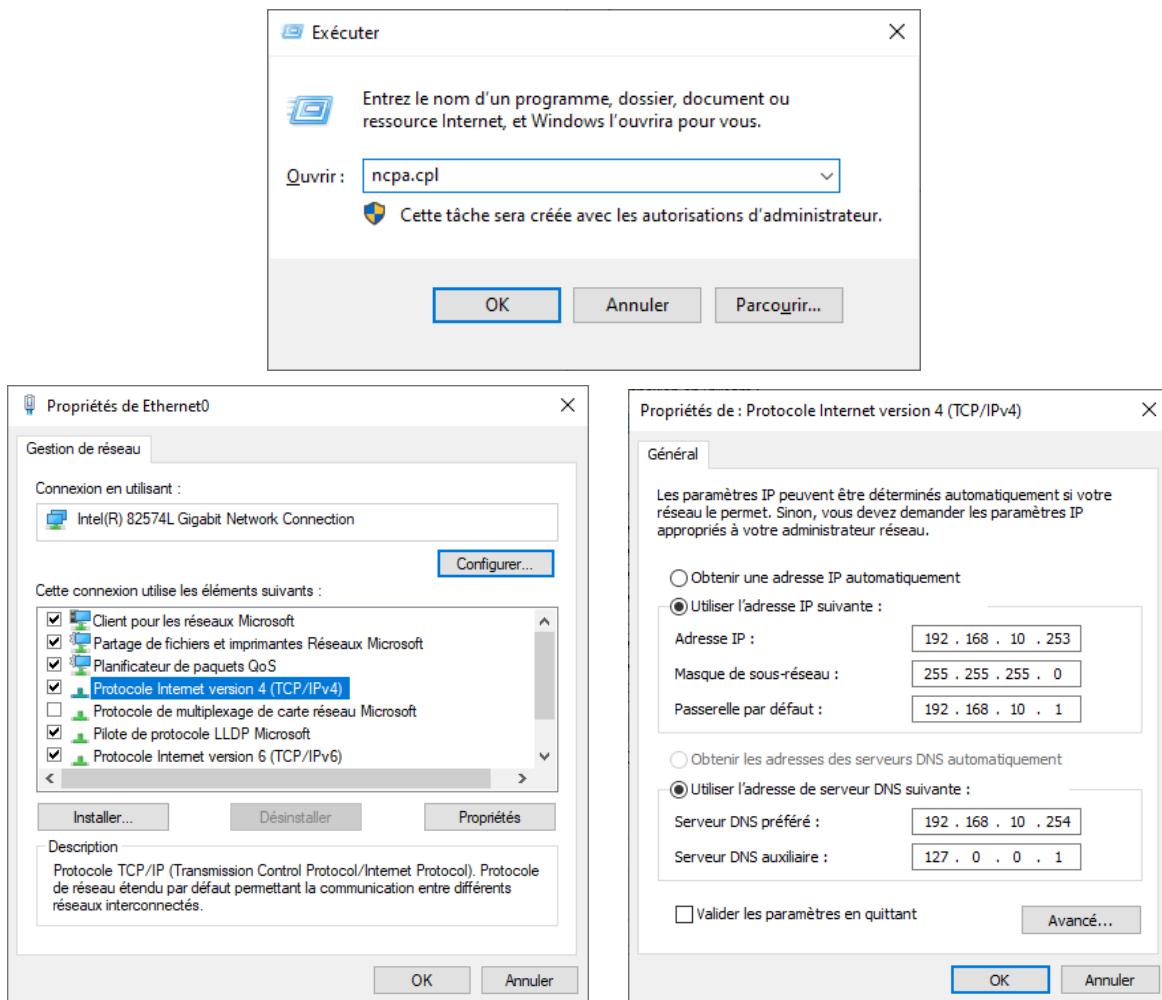


Serveur Active Directory Redondant

Un **Active Directory en redondance** est une configuration où plusieurs **contrôleurs de domaine** sont déployés pour assurer la disponibilité et la continuité des services d'annuaire, même **en cas de panne d'un contrôleur**. J'ai effectué l'installation du système d'exploitation sur le serveur afin de pouvoir procéder à la configuration de l'**Active Directory en redondance**.

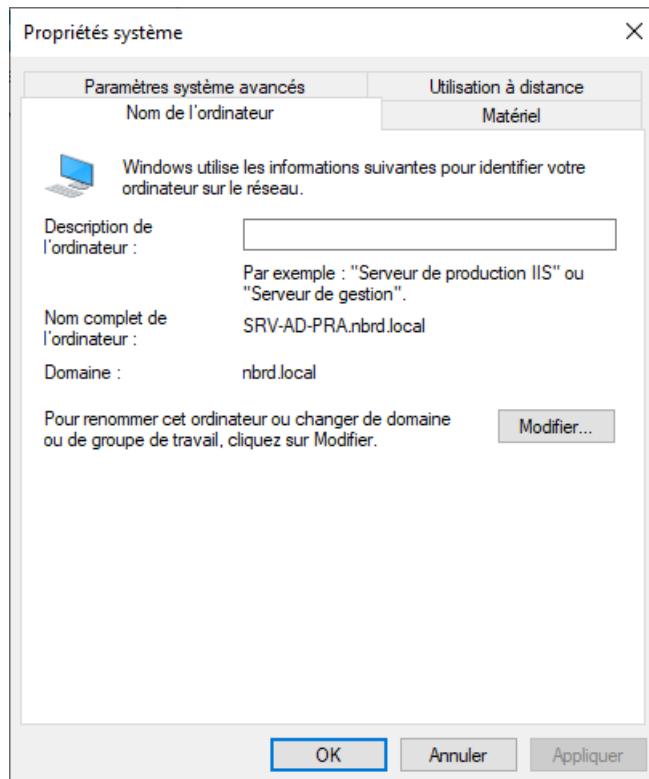
Configuration réseau en IP Fixe

Ensuite, je vais attribuer **l'adresse IP 192.168.1.71** au serveur **AD redondant**, située à la fin de ma plage d'adresses statiques, juste avant celle de mon serveur **AD principal**, sur l'adaptateur Ethernet 0. Je configure également **l'adresse DNS** en spécifiant celle de mon serveur **AD principal**, qui héberge le domaine « **nbrd.local** ».



Rejoindre le domaine du contrôleur de domaine

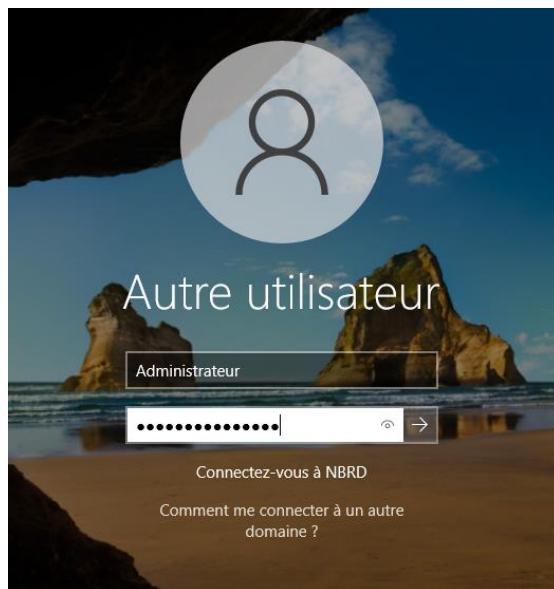
Une fois la configuration terminée, je vais dans l'**explorateur de fichiers**, effectue un clic droit sur « **Ce PC** », puis sélectionne l'option « **Modifier** » pour accéder aux paramètres nécessaires.



Par la suite, une demande d'identifiants apparaît. J'entre alors le **nom d'utilisateur** et le **mot de passe** de l'administrateur du serveur **Active Directory** pour finaliser l'intégration au domaine.

Le poste redémarre. Lors de la reconnexion, je choisis un autre utilisateur, puis je renseigne le nom de domaine suivi du nom d'utilisateur LDAP souhaité (**NBRD\Administrateur**).

Dans ce cas, j'utilise les identifiants de l'**administrateur** créé dans l'annuaire **LDAP** de mon **Active Directory**, afin que la configuration de l'**AD redondant** soit administrée par cet utilisateur.

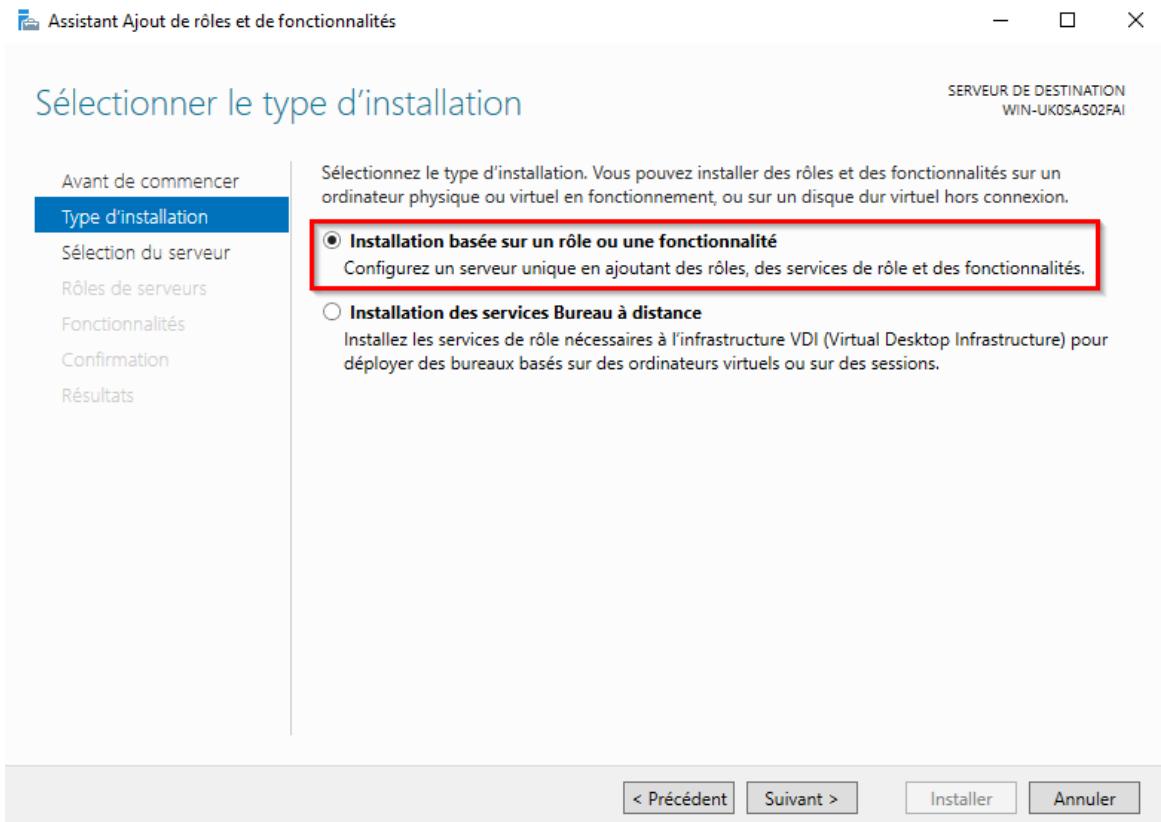


Installation de la redondance Active Directory

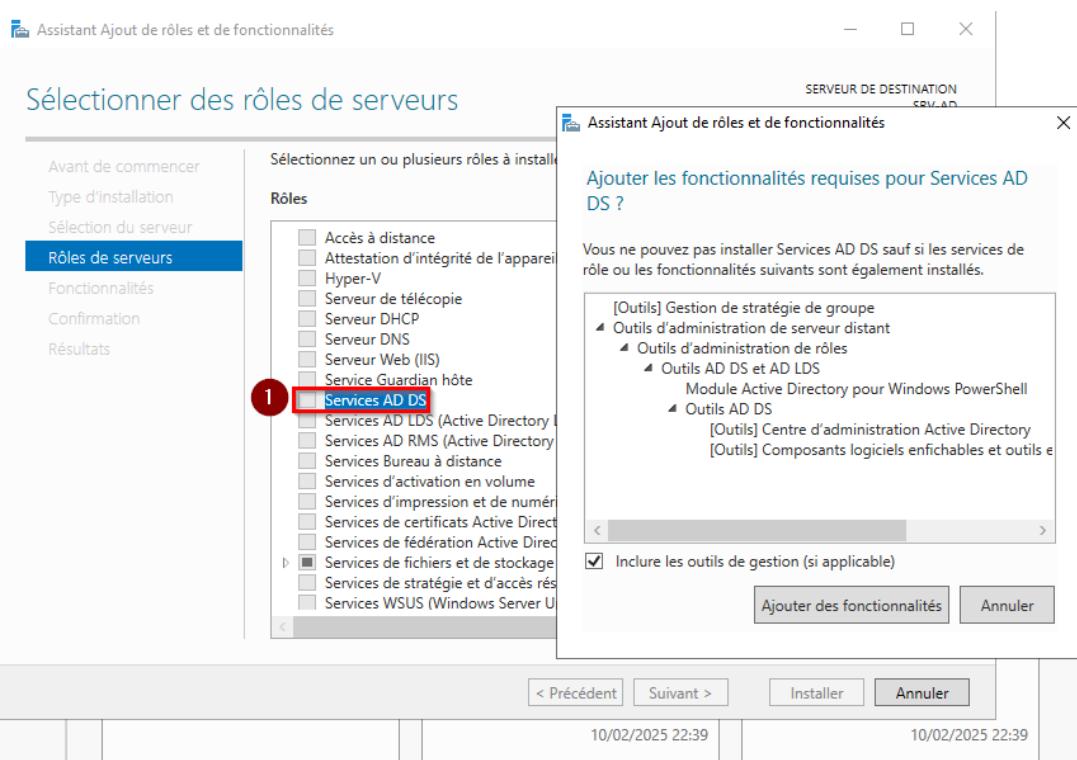
Rejoindre le domaine du contrôleur de domaine

Je commence par ouvrir le « **Gestionnaire de serveur** », puis je clique sur « **Gérer** » et je sélectionne « **Installer des rôles et fonctionnalités** » afin d'ajouter le rôle « **Services AD DS** ».

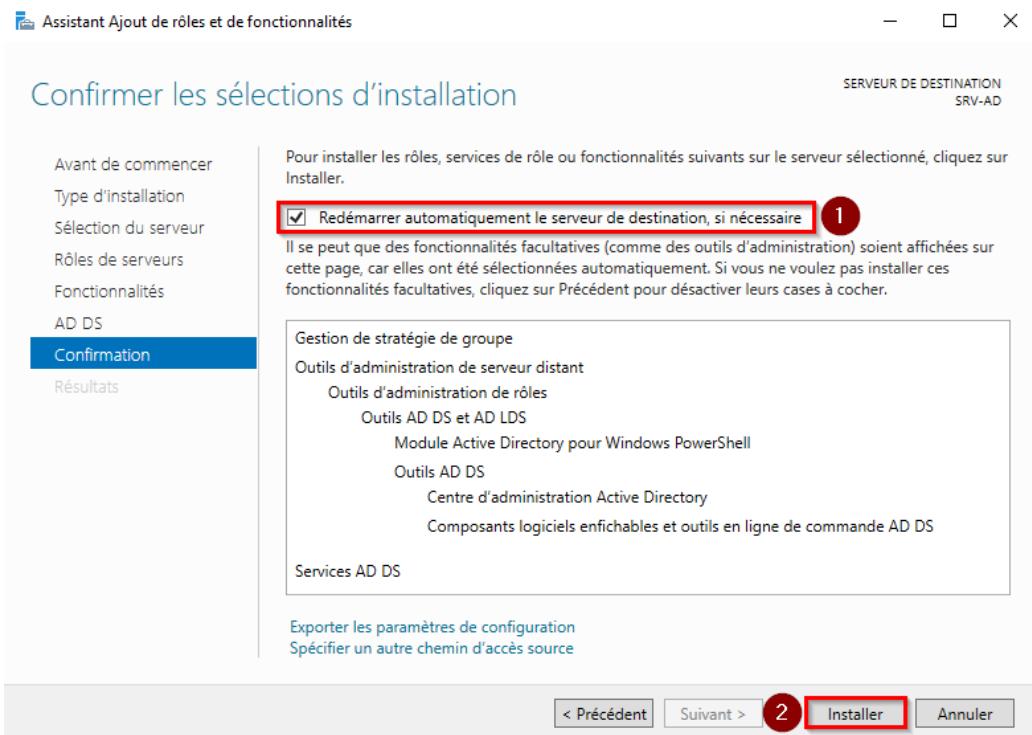
Je passe l'étape « **Avant de commencer** » et je choisis « **Installation basée sur un rôle ou une fonctionnalité** » comme « **Type d'installation** ».



Je passe l'étape « **Sélection du serveur** » puisque j'agis sur le serveur local. Lorsque l'étape « **Rôles de serveurs** » s'affiche, je coche le rôle « **Services AD DS** » et je valide en cliquant sur « **Ajouter des fonctionnalités** » pour m'assurer que tout est installé, y compris les consoles de gestion.

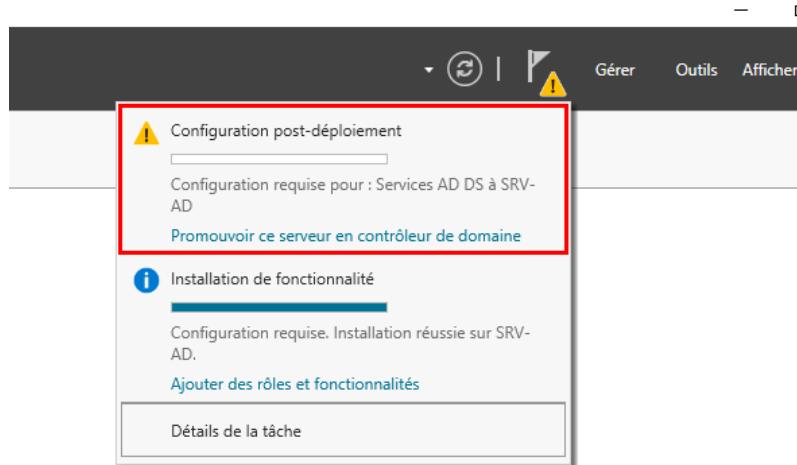


Je poursuis jusqu'à l'étape « **Confirmation** » et je coche « **Redémarrer automatiquement le serveur** » avant de cliquer sur « **Installer** ». Ensuite, je patiente un instant...

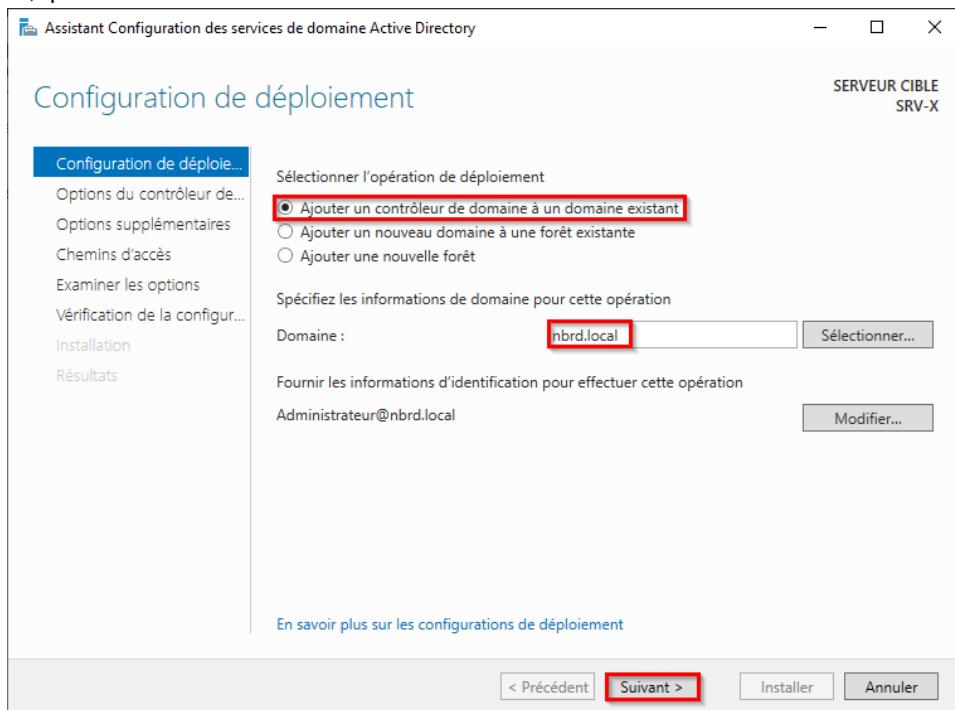


Promouvoir le serveur en contrôleur de domaine ADDS

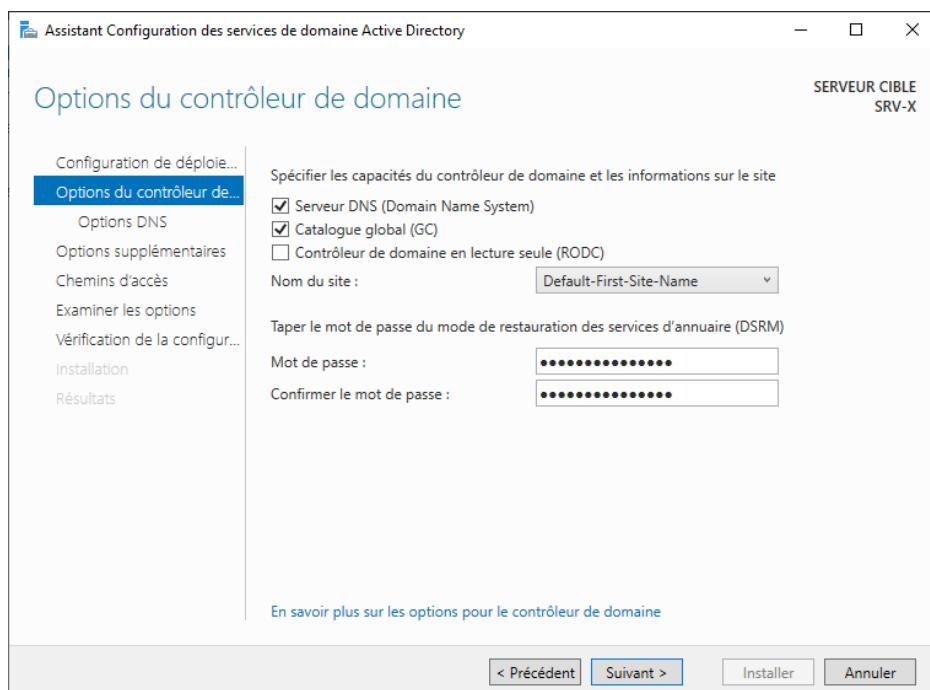
Une fois l'installation du rôle terminée, un **avertissement** s'affiche dans le Tableau de bord du gestionnaire de serveur. Par curiosité, je clique dessus pour continuer et j'utilise le bouton « **Promouvoir ce serveur en contrôleur de domaine** ».



Un nouvel assistant s'exécute. Je sélectionne « **Ajouter un contrôleur de domaine à un domaine existant** » et je spécifie le nom du domaine, qui est « **nbrd.local** ».

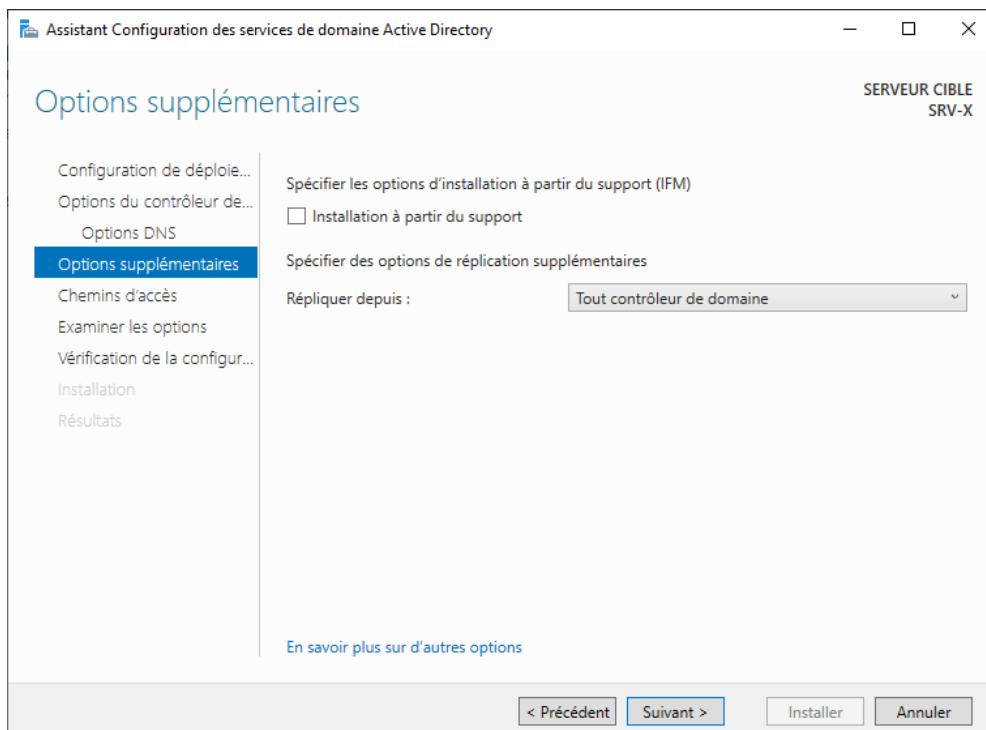


À l'étape suivante, je sélectionne les options pour ce contrôleur de domaine. Je coche « **Serveur DNS** » et j'indique un **mot de passe complexe** pour la restauration des services d'annuaire.

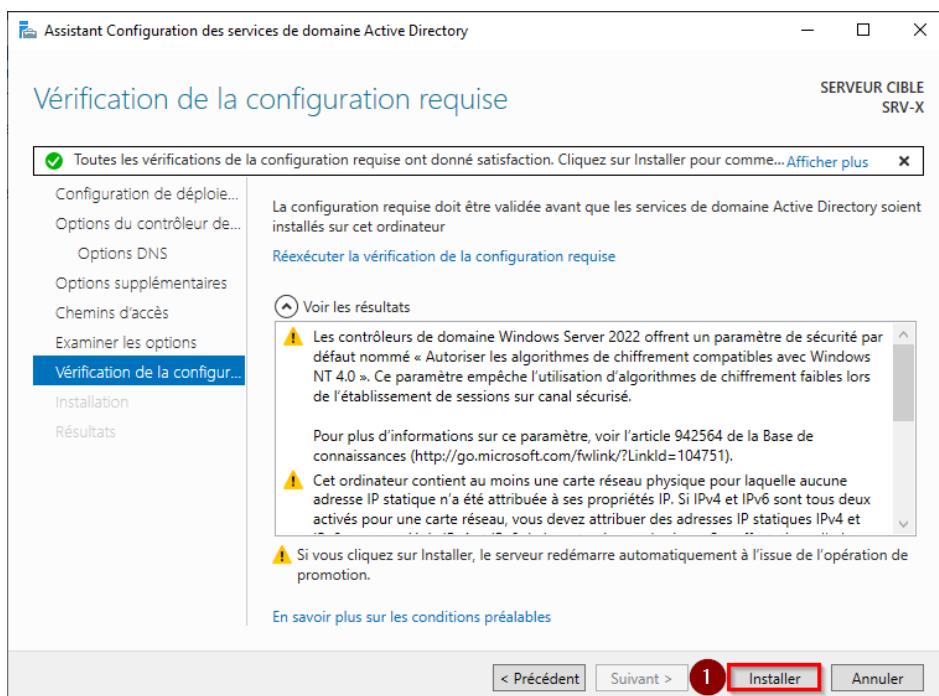


Ensuite, dans les options supplémentaires, je choisis l'option « **Répliquer depuis tout contrôleur de domaine** ».

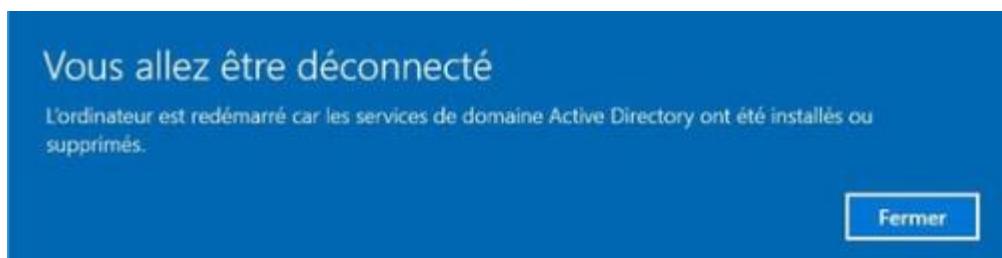
Toutefois, si je souhaite utiliser un **DC spécifique** pour répliquer les données sur ce nouveau **DC**, je peux le choisir ici (ce qui est utile lorsque plusieurs DC existent sur différents sites géographiques). Dans cet exemple, étant donné qu'il n'y a qu'un seul **DC**, il n'est pas nécessaire de s'attarder sur cette option.



L'étape de vérification de la configuration s'affiche. Si tout est en ordre, comme dans l'exemple ci-dessous, je clique sur « Suivant » puis « Installer ».



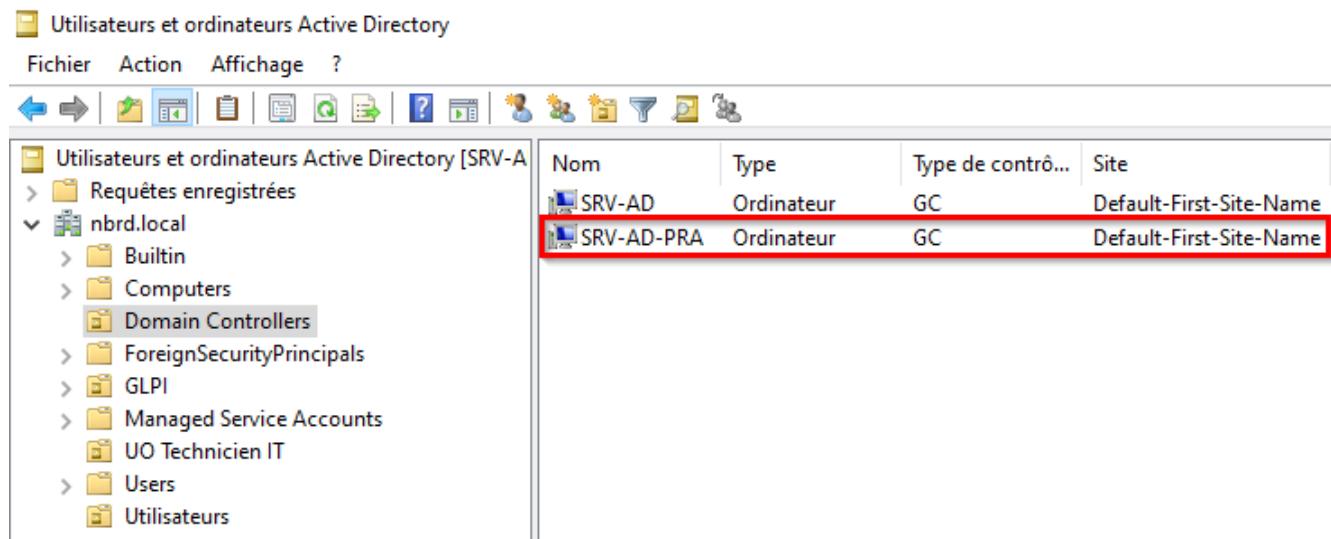
Lorsque l'**opération est terminée**, le serveur redémarre automatiquement dans la minute pour appliquer les modifications et finaliser la configuration du rôle de contrôleur de domaine.



Après le redémarrage, le serveur devient un **contrôleur de domaine Active Directory redondant** ! Ce serveur assure désormais la redondance de l'annuaire centralisé, utilisé pour gérer les utilisateurs, les groupes et les ressources réseau, tout en offrant une tolérance aux pannes.

Vérification de l'opération

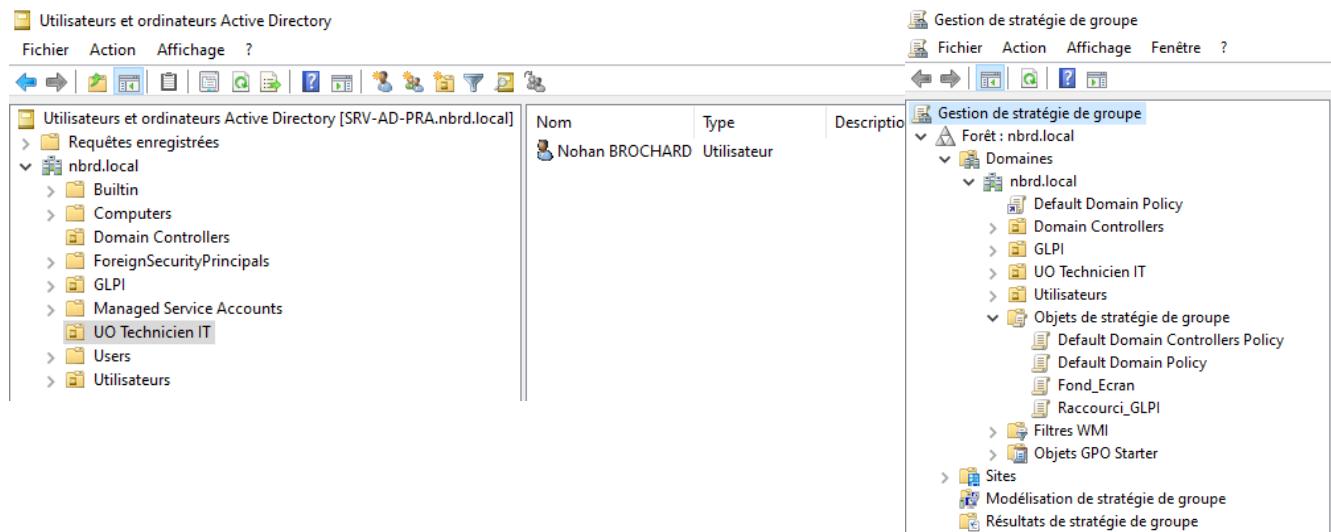
Comment vérifier que l'opération a été réussie ? Tout d'abord, dans la console « Utilisateurs et ordinateurs Active Directory », l'OU « Domain Controllers » devrait désormais afficher deux objets ordinateurs, comme illustré ci-dessous :



The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' console. On the left, the navigation pane shows the tree structure: 'Utilisateurs et ordinateurs Active Directory [SRV-A]' -> 'Requêtes enregistrées' -> 'nbrd.local' -> 'Domain Controllers'. On the right, a table lists objects:

Nom	Type	Type de contrôleur	Site
SRV-AD	Ordinateur	GC	Default-First-Site-Name
SRV-AD-PRA	Ordinateur	GC	Default-First-Site-Name

Une autre manière de vérifier est de se rendre dans la console « Gestion des stratégies de groupe (GPO) ». Je peux vérifier que la réplication est bien effectuée en consultant les stratégies appliquées sur les contrôleurs de domaine. De plus, je peux vérifier la synchronisation des utilisateurs et des groupes entre les deux contrôleurs de domaine.



The screenshot shows the 'Gestion de stratégie de groupe' console. On the left, the navigation pane shows the tree structure: 'Utilisateurs et ordinateurs Active Directory [SRV-AD-PRA.nbrd.local]' -> 'Requêtes enregistrées' -> 'nbrd.local' -> 'Domain Controllers'. On the right, the main pane displays the 'Gestion de stratégie de groupe' interface, showing the structure of policies applied to the domain.

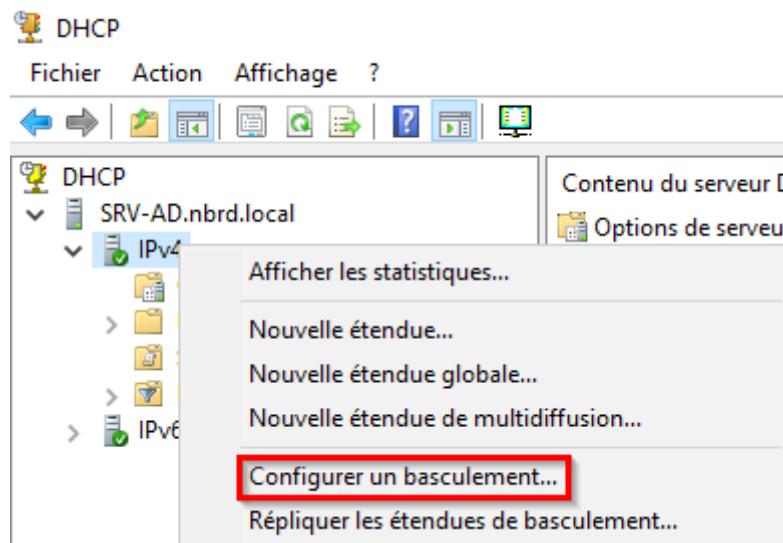
L'**Active Directory en redondance** est devenu en quelque sorte une copie du **contrôleur principal**. Il réplique en continu les informations de l'annuaire, comme les utilisateurs, les groupes et autres objets, afin d'assurer une **haute disponibilité** et une **tolérance aux pannes**. Si le contrôleur principal tombe en panne, le contrôleur redondant peut prendre le relais sans interruption du service.



Configuration du DHCP en basculement

Pour configurer le DHCP en basculement de mon Active Directory principal vers mon Active Directory redondant, voici les étapes détaillées :

Dans un premier temps, je me rends sur le serveur AD principal et ouvre le Gestionnaire du rôle DHCP via le menu Windows, je clic droit sur « IPv4 », puis je clique sur « Configurer un basculement ».



Une fenêtre s'ouvre et je sélectionne mon **AD redondant (SRV-AD-PRA)** comme serveur de basculement.

Ajouter un serveur

Selectionnez un serveur que vous voulez ajouter à votre console.

Ce serveur :

Ce serveur DHCP autorisé :

Nom	Adresse IP
srv-ad.nbrd.local	192.168.1.254

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existante, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :
 Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

Pour finaliser, je configure le **serveur partenaire** en mode **veille** avec **15%** d'adresses réservées sur la plage d'adresses de mon DHCP, afin qu'il prenne le relais en cas de défaillance du serveur principal.



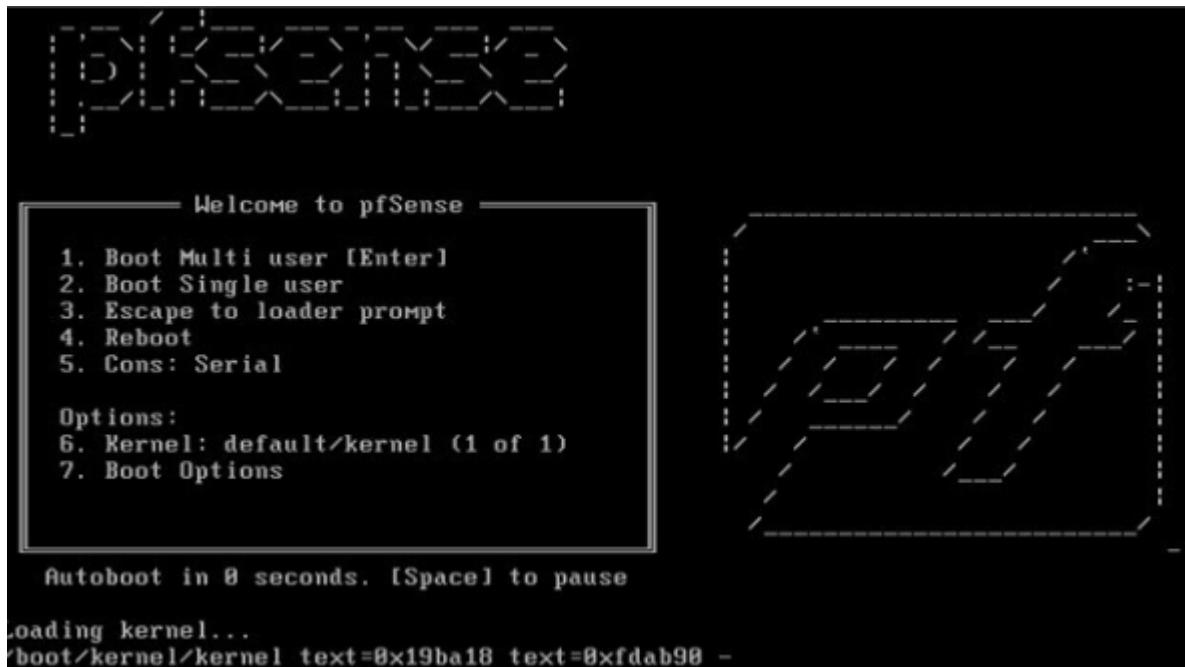
Routeur PFSense

PFsense est un système d'exploitation open-source basé sur **FreeBSD**, conçu pour agir comme pare-feu et routeur. Il propose une **interface web** pour configurer et gérer les fonctionnalités de sécurité et de réseau, telles que le filtrage de paquets, la gestion VPN, et le support multi-WAN. Sa modularité permet d'ajouter des fonctionnalités via des **packages supplémentaires**.

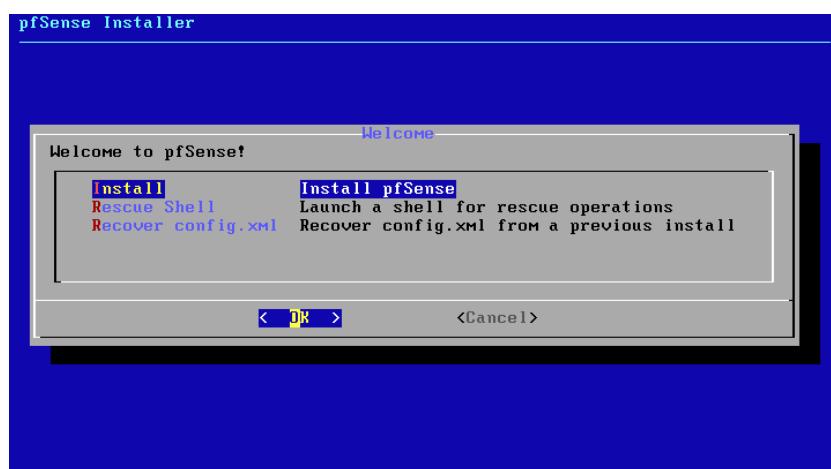
Installation de PFSense

J'ai choisi **PFSense** car il fait partie du cursus de mon BTS SIO, ce qui m'a permis de me familiariser avec ses fonctionnalités et son utilisation. Cette expérience m'a donné la confiance nécessaire pour l'installer et le configurer efficacement dans le cadre de ce projet.

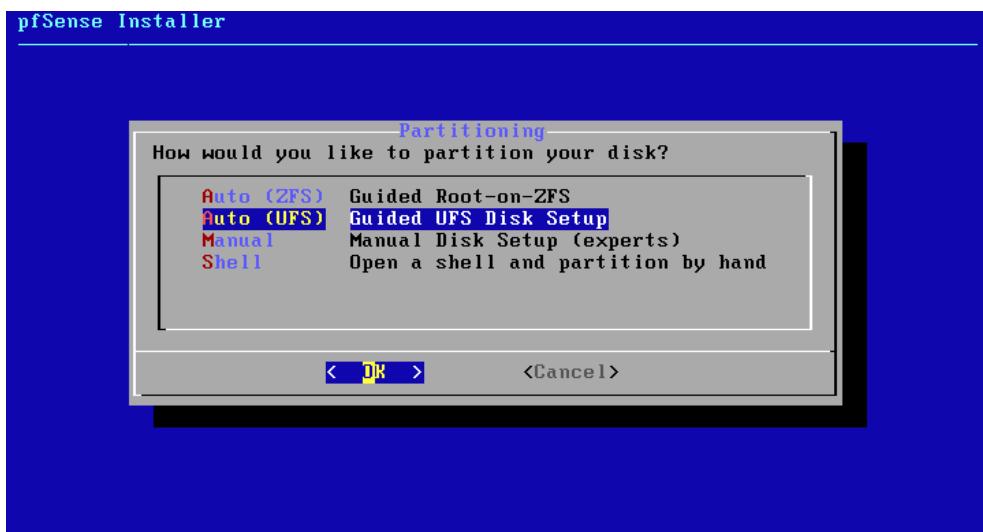
Je commence immédiatement l'installation de **PFSense**. Après avoir inséré l'ISO de **PFSense** dans la VM dédiée, je démarre la machine. Le **setup** se lancera automatiquement après quelques secondes.



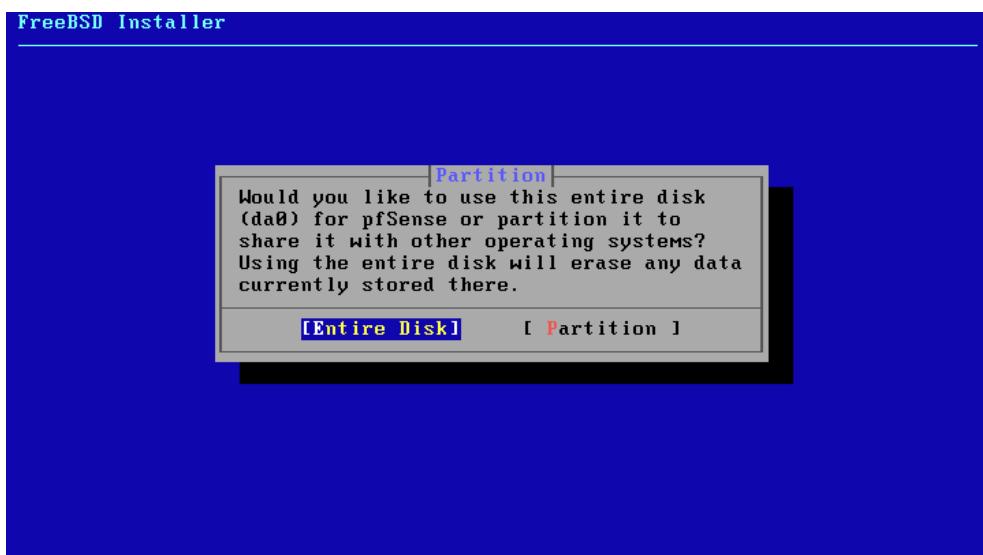
Ensuite, je vérifie que l'option « **Install** » est bien sélectionnée (elle doit apparaître en **bleu foncé** comme sur l'image ci-dessous). Si ce n'est pas le cas, je me déplace avec les **flèches** de mon clavier et j'appuie sur « **Entrée** » pour valider.



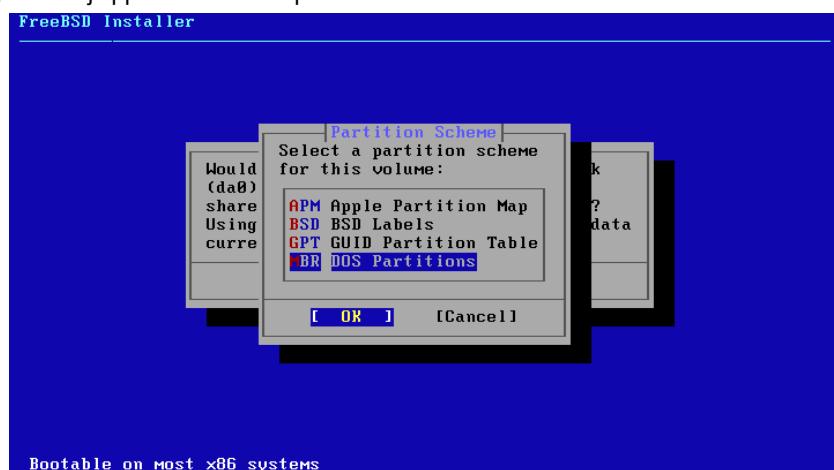
Je procède maintenant au partitionnement du disque de stockage de la machine en optant pour l'option « **Auto (UFS)** », choisie pour sa **fiabilité** et sa **facilité d'utilisation**.



Par la suite, je confirme que je souhaite utiliser le disque entier pour l'installation du système d'exploitation. Je sélectionne donc l'option « **Entire Disk** » et j'appuie sur **Entrée**.



Ici, on choisit « **MBR DOS Partitions** » comme partition pour sa compatibilité étendue sur une large gamme de systèmes d'exploitation et de logiciels et j'appuie sur Entrée pour valider.



Une fois l'installation terminée, la machine virtuelle va redémarrer. Au démarrage, **PFSense** se lance, teste et configure les services nécessaires. Par exemple, dans l'image ci-dessous, on peut voir que **PFSense** a testé et configuré l'interface **WAN** (indiqué par « Configuring WAN interface...done. »), de même que l'interface **LAN**. Il a également lancé le service **DNS** pour la résolution des noms de domaine (ligne "Configuring DNS Resolver...").

```

Starting device manager (devd)...2023-08-14T16:36:43.739744+00:00 - php-fpm 372
-- /rc.linkup: DHCP Client not running on wan (em0), reconfiguring dhclient.
2023-08-14T16:36:43.768898+00:00 - php-fpm 371 -- /rc.linkup: Ignoring link event during boot sequence.
done.
Loading configuration....done.
Updating configuration.....Migrating System Memory RRD file to new format
.done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Configuring LAN interface...done.
Configuring WAN interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Setting up static routes...done.
Setting up DNSs...
Starting DNS Resolver...■

```

Une fois que le démarrage est finalisé, j'aurai la vue suivante sur la machine, affichant les **options de configuration** ainsi que la **configuration actuelle des interfaces LAN et WAN**.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: a86f287011fe9e1cd7a2

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 10.128.0.1/8
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

Sur cette image, je remarque clairement nos deux **interfaces réseaux** (WAN et LAN). L'**interface WAN** a récupéré avec succès une **adresse IP** automatiquement via un serveur **DHCP** (l'adresse IP publique). Quant au LAN, par défaut, il attribue l'adresse **statique 192.168.1.1**, que nous allons modifier.



Configuration du LAN & WAN

Je clique sur l'option « **Set interface IP Address** » sur PFsense pour modifier l'adresse IP de mon **interface LAN**. Je sélectionne **l'interface LAN**, puis j'insère l'adresse IP et le **masque 255.255.255.0**, tout en refusant l'intégration de l'IPv6 et du DHCP.

Par la suite, en validant la modification, l'adresse IP de **l'interface LAN** est mise à jour à **192.168.10.1**, qui devient la **passerelle par défaut (gateway)** de mon réseau local, permettant aux périphériques du réseau de router leurs requêtes via cette adresse.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.nbrd) (ttyv0)

VMware Virtual Machine - Netgate Device ID: bdc293576f6520e26537

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0          -> v4/DHCP4: 192.168.118.150/24
LAN (lan)      -> le1          -> v4: 192.168.10.1/24

 0) Logout (SSH only)          9) pfTop
 1) Assign Interfaces          10) Filter Logs
 2) Set interface(s) IP address 11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults   13) Update from console
 5) Reboot system               14) Enable Secure Shell (sshd)
 6) Halt system                 15) Restore recent configuration
 7) Ping host                   16) Restart PHP-FPM

Enter an option: ■

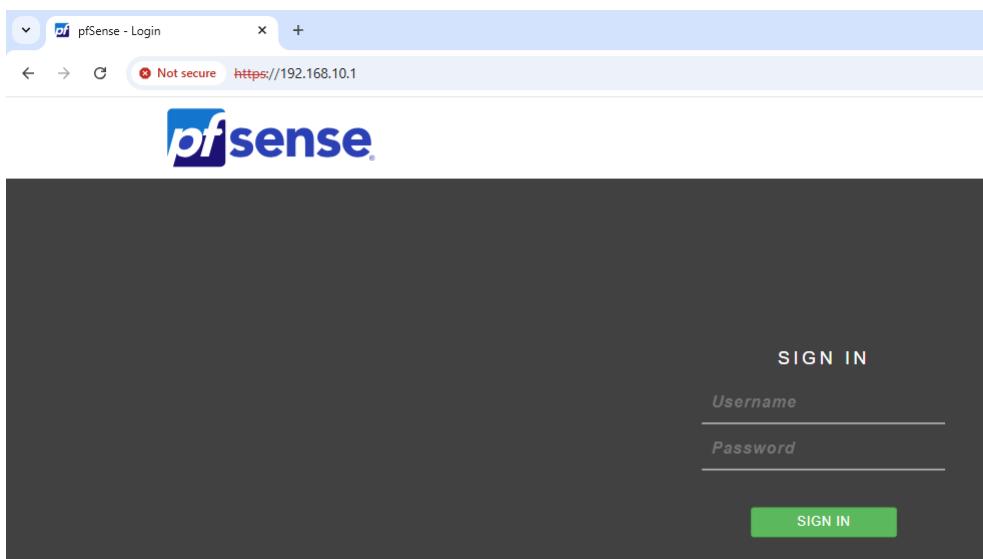
```

Pour **l'interface WAN**, nous ne faisons aucune modification, car dans le cadre de mon projet, mon ordinateur hôte changera régulièrement de connexion.

Il est donc préférable de laisser l'interface WAN en **DHCP** afin qu'elle fonctionne correctement sur n'importe quel réseau.

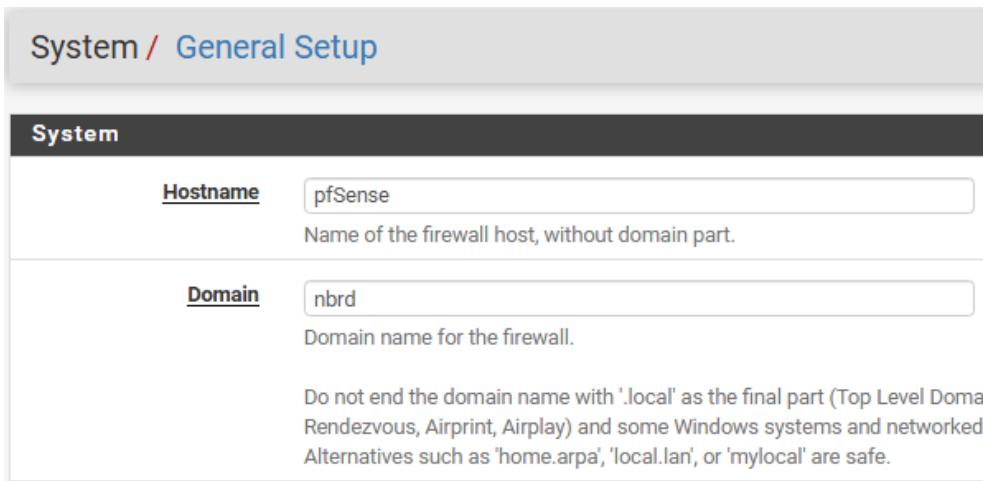
Configuration de PFsense (Interface WEB)

Pour accéder à **PFsense** via l'interface web maintenant que la VM est installée et configurée, je me rends sur le **serveur AD** et entre l'adresse IP de **l'interface LAN** de PFsense dans un navigateur web. Cela me permettra d'accéder à **l'interface de gestion web** de PFsense pour effectuer les configurations nécessaires.



Je me connecte à l'interface de gestion de **PFSense** en utilisant les identifiants génériques par défaut : le **nom d'utilisateur** est « **admin** » et le **mot de passe** est « **pfsense** ».

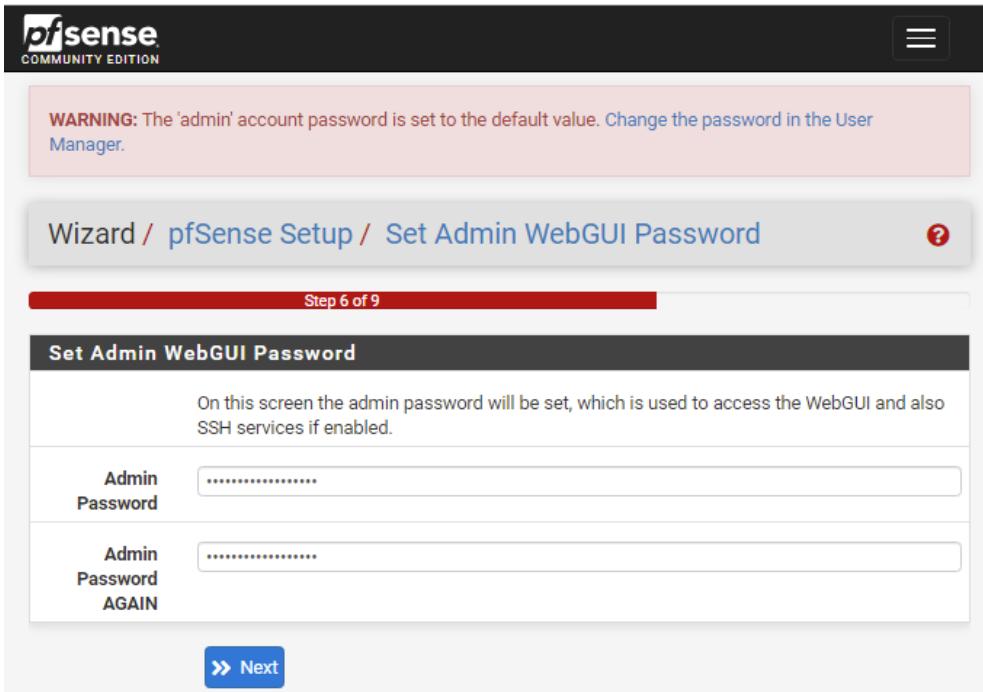
Ensuite, dans la section des **informations générales**, je modifie le **nom du pare-feu** et déclare le **nom de domaine** de mon réseau, configuré au préalable sur le **serveur AD**.



The screenshot shows the 'System / General Setup' interface. Under the 'System' tab, there are two main fields: 'Hostname' set to 'pfSense' with the note 'Name of the firewall host, without domain part.' and 'Domain' set to 'nbrd' with the note 'Domain name for the firewall. Do not end the domain name with '.local' as the final part (Top Level Domain Rendezvous, Airprint, Airplay) and some Windows systems and networked Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.'

Je choisis « **Europe/Paris** » comme fuseau horaire et je poursuis. Ensuite, nous arrivons à la **configuration de l'interface WAN**, qui a été configurée dans les étapes précédentes, tout comme le **LAN**. Je ne modifie donc aucune information et clique sur « **Suivant** ».

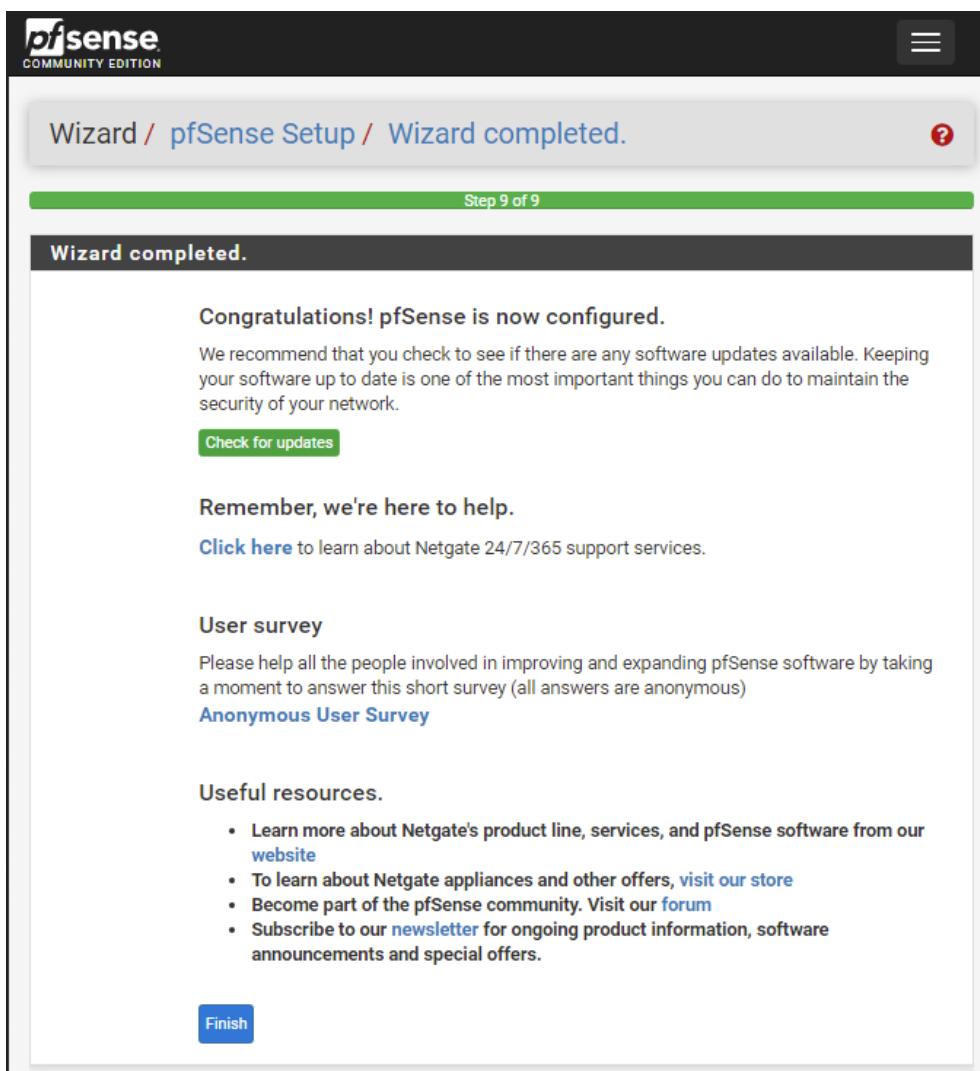
Durant l'étape **6** de la configuration, il m'est demandé de **modifier les identifiants par défaut** du compte **admin** de PFSense.



The screenshot shows the 'Wizard / pfSense Setup / Set Admin WebGUI Password' screen, Step 6 of 9. It displays a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, it says 'Set Admin WebGUI Password'. It explains that the admin password will be set for access to the WebGUI and SSH services. Two password fields are shown: 'Admin Password' and 'Admin Password AGAIN', both containing masked entries. A 'Next' button is at the bottom.



Les étapes finales consistent à cliquer sur « **Reload** » pour **recharger PFSense**, attendre que la page se recharge automatiquement, puis cliquer sur « **Finish** » pour **compléter la configuration**.



Une fois ceci fait, j'arrive sur le **tableau de bord de PFsense**, où je trouve des informations sur l'utilisation des ressources de la machine, ses différentes **adresses IP**, sa **version**, ainsi que les **mises à jour éventuelles**.

Status / Dashboard

System Information	
Name	pfSense.nbrd
User	admin@192.168.10.254 (Local Database)
System	VMware Virtual Machine Netgate Device ID: bdc293576f6520e26537
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT
<small>The system is on the latest version. Version information updated at Sun May 25 18:13:40 CEST 2025</small>	
CPU Type	AMD Ryzen 7 7800X3D 8-Core Processor 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	02 Hours 46 Minutes 50 Seconds
Current date/time	Sun May 25 18:22:09 CEST 2025
DNS server(s)	<ul style="list-style-type: none"> • 127.0.0.1 • 192.168.118.2 • 192.168.10.254 • 8.8.8.8
Last config change	Fri May 23 13:49:52 CEST 2025
State table size	0% (38/198000) Show states
MBUF Usage	0% (1016/1000000)
Load average	0.46, 0.36, 0.30

Netgate Services And Support

Retrieving support information 



Interfaces

	WAN		autoselect 192.168.118.150
	LAN		autoselect 192.168.10.1



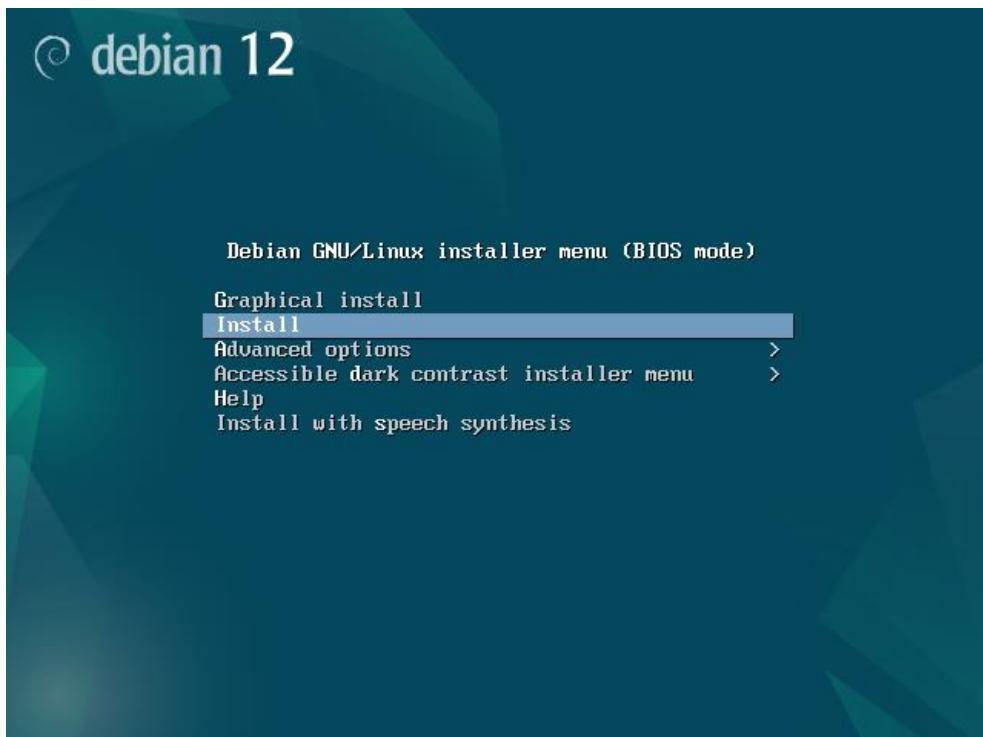
Debian / GLPI

Debian est un système d'exploitation open-source basé sur Linux, connu pour sa stabilité et flexibilité. Il peut héberger un serveur **GLPI**, un logiciel **open-source** de gestion des services informatiques.

GLPI permet de centraliser la gestion des incidents, demandes, et interventions via un système de tickets, où chaque problème ou requête est enregistré, suivi, et résolu de manière organisée, assurant une gestion efficace des ressources et du support technique.

Installation du système d'exploitation

Pour installer Debian, je commence par lancer l'**ISO** du système d'exploitation. Après avoir téléchargé l'image ISO Debian, je la démarre pour débuter l'installation.



Après avoir lancé l'**ISO** Debian, je commence l'installation en sélectionnant la **langue de l'OS** et du **clavier**. Je choisis le **français** pour l'interface du système d'exploitation, puis je configure le clavier en mode **AZERTY** pour correspondre à mon clavier français.

debian 12

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	- 中文(简体)
Chinese (Traditional)	- 中文(繁體)
Croatian	- Hrvatski
Czech	- Čeština
Danish	- Dansk
Dutch	- Nederlands
Dzongkha	- གློང་ཁ
English	- English
Esperanto	- Esperanto
Estonian	- Eesti
Finnish	- Suomi
French	- Français
Galician	- Galego
Georgian	- ქართველი
German	- Deutsch

Screenshot **Go Back** **Continue**

debian 12

Configurer le clavier

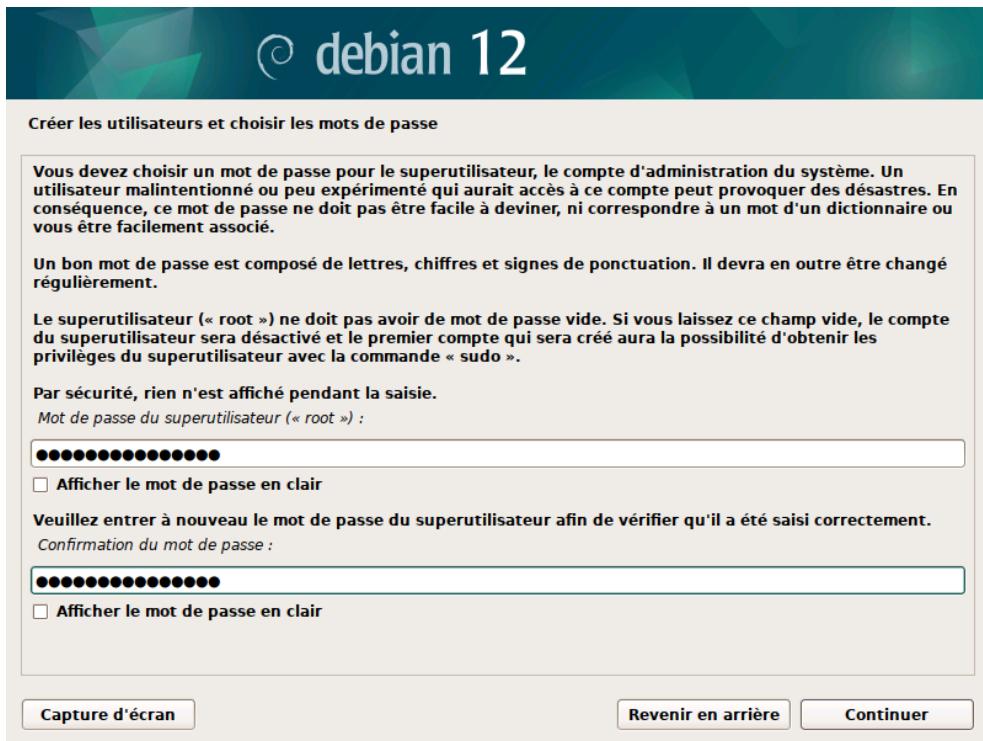
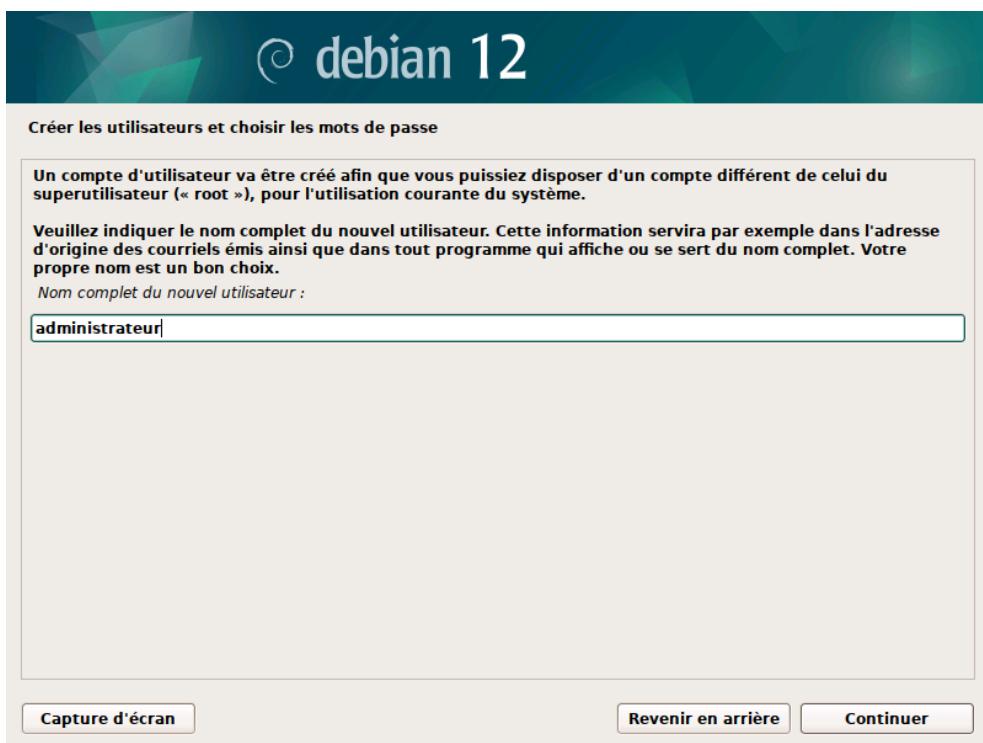
Disposition de clavier à utiliser :

Danois
Néerlandais
Dvorak
Dzongkha
Espéranto
Estonien
Éthiopien
Finnois
Français
Géorgien
Allemand
Grec
Gujarati
Gourmoukhî
Hébreu
Hindi
Hongrois

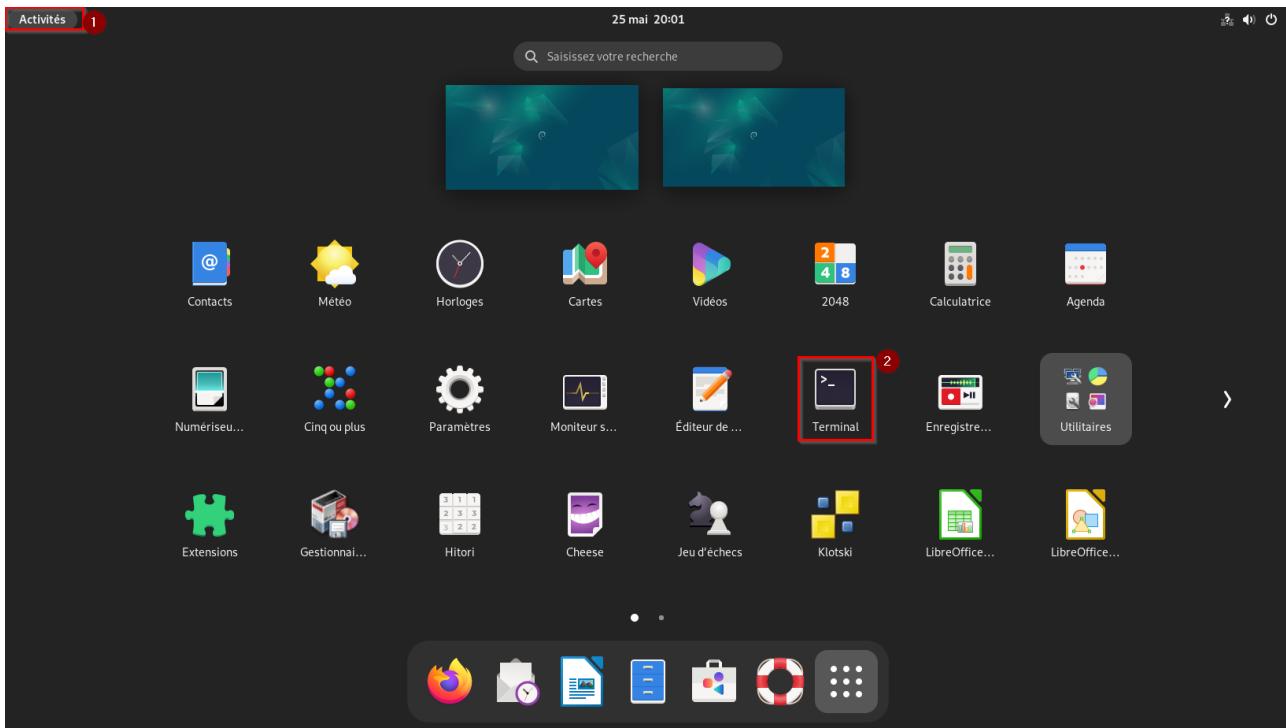
Capture d'écran **Revenir en arrière** **Continuer**



Ensuite, je dois entrer le **nom de l'ordinateur**, le **nom d'utilisateur** et le **mot de passe**. Ces informations sont nécessaires pour créer un compte administrateur sécurisé et garantir l'accès contrôlé au système une fois l'installation terminée.



Après cela, j'ai l'accès au bureau Ubuntu via la **session administrateur**, j'ouvre donc le terminal et j'exécute la commande « **sudo apt update** » et « **sudo apt upgrade** ».



`sudo apt update && upgrade`

Ensuite, nous allons fixer l'**adresse IP** sur **192.168.10.252** avec comme **passerelle** **192.168.10.1 (PFSense)**, et en **Serveur DNS** **192.168.10.254 (Serveur ADDS)**, pour cela, nous allons utiliser la commande suivante :

`sudo nano /etc/network/interfaces`

```
GNU nano 7.2                               /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
```

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto ens33
iface ens33 inet static
    address 192.168.10.252
    netmask 255.255.255.0
    gateway 192.168.10.1
    dns-nameservers 192.168.10.254
```

[Lecture de 12 lignes]
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

J'ai donc terminé l'installation de Debian 12 et effectué les mises à jour nécessaires. Le système est désormais configuré et prêt à accueillir GLPI pour une gestion optimale des incidents.

Installation de GLPI

J'ai préparé une série de commandes que je vais exécuter via l'**invite de commande** pour procéder à l'**installation de GLPI**. J'ai effectué les étapes nécessaires pour installer **Apache2**, **PHP**, **MariaDB**, ainsi que les **modules complémentaires** requis pour assurer le bon fonctionnement de GLPI. Voici la **liste des commandes** que j'ai configurées pour **optimiser** cette installation et garantir que tout soit correctement configuré.

```
# Mise à jour des paquets et mise à niveau
sudo apt-get update
sudo apt-get upgrade

# Installation d'Apache2 et de PHP
sudo apt-get install -y apache2 php libapache2-mod-php

# Installation des extensions PHP nécessaires pour GLPI
sudo apt-get install -y php-imap php-ldap php-curl php-xmlrpc php-gd php-mysql php-cas
php-intl php-mbstring php-json php-xml

# Installation de MariaDB et sécurisation
sudo apt-get install -y mariadb-server
sudo mysql_secure_installation

# Installation des modules complémentaires pour GLPI
sudo apt-get install apcupsd php-apcu

# Redémarrage des services Apache2 et MariaDB
/etc/init.d/apache2 restart ou sudo systemctl restart apache2
/etc/init.d/mysql restart ou sudo systemctl restart mysql

# Création de la base de données GLPI et de l'utilisateur
sudo mysql -u root -p
CREATE DATABASE glpidb;
GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost' IDENTIFIED BY 'votre-mot-de-passe';
QUIT;

# Installation de phpMyAdmin
sudo apt-get install -y phpmyadmin
sudo ln -s /usr/share/phpmyadmin /var/www/html/phpmyadmin

# Activation du module rewrite pour Apache
sudo a2enmod rewrite sudo systemctl restart apache2

# Téléchargement et installation de GLPI version 10.0.7
wget https://github.com/glpi-project/glpi/releases/download/10.0.7/glpi-10.0.7.tgz
tar xvf glpi-10.0.7.tgz
sudo mv glpi /var/www/html/glpi

# Ajustement des permissions pour GLPI
sudo chown -R www-data:www-data /var/www/html/glpi

# Redémarrage final du service Apache
systemctl restart apache2
```

Pour accéder à l'interface graphique de **GLPI**, je récupère l'adresse IP locale du serveur en exécutant « **ip a** » dans le terminal. Ensuite, je saisis cette adresse IP dans la barre d'URL de mon navigateur (par exemple, <http://192.168.10.252>) et je me connecte avec les **identifiants GLPI administrateur par défaut**.

Le mot de passe par défaut pour l'utilisateur administrateur de GLPI est souvent **admin**. Le nom d'utilisateur par défaut est généralement **glpi**. Après avoir saisi l'adresse IP de GLPI dans mon navigateur, une **interface web** s'ouvre me demandant de **sélectionner la langue**. Je choisis la langue souhaitée dans le menu déroulant pour continuer.

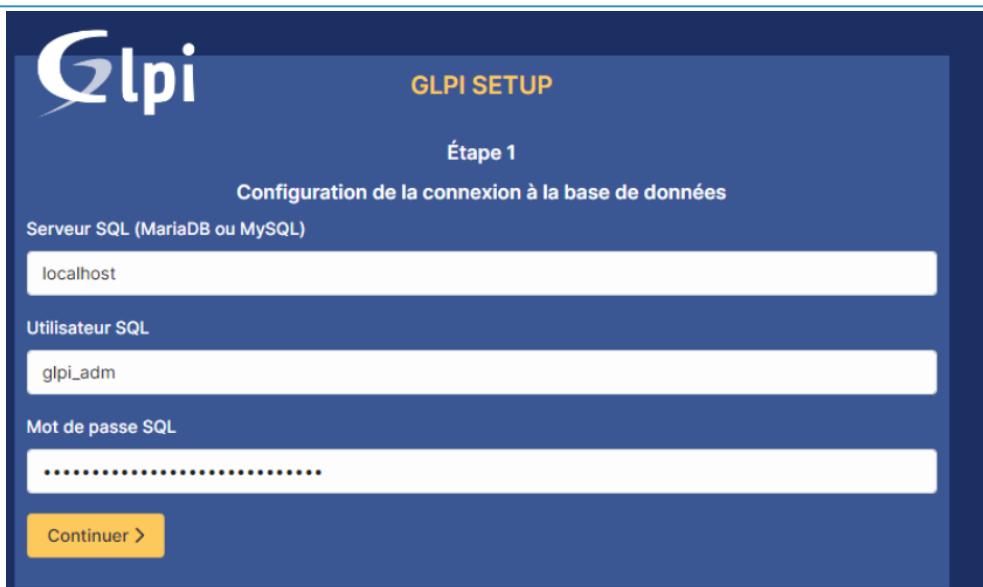




Ensuite, je clique sur le bouton « Installation » pour commencer le processus d'installation de GLPI. Une fois l'installation terminée, une page affiche les **extensions**, **protocoles** et **permissions** nécessaires, en indiquant si chacun est « **Validé** » ou « **Échoué** » selon les **prérequis**. Dans mon cas, avec les commandes d'installation préalablement exécutées, tout est correctement installé.

TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysqli extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <small>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</small>	✓
Requis gd extension <small>Requis pour le traitement des images.</small>	✓
Requis intl extension <small>Requis pour l'internationalisation.</small>	✓
Requis zlib extension <small>Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.</small>	✓
Requis Libsodium ChaCha20-Poly1305 constante de taille <small>Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.</small>	✓
Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓
Suggéré Version de PHP supportée <small>Une version officiellement supportée de PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues.</small>	✓
Suggéré Configuration sécurisée du dossier racine du serveur web <small>La configuration du dossier racine du serveur web devrait être '/var/www/glpi/public' pour s'assurer que les fichiers non publics ne peuvent pas être accédés.</small>	✓
Suggéré Configuration de sécurité pour les sessions <small>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.</small>	✓

Après avoir passé la page des prérequis, je configure la **base de données** en entrant « **localhost** » puisque la base est stockée sur le **serveur local**. Je renseigne également l'utilisateur et le mot de passe que j'ai définis lors de la configuration de la base de données pendant l'installation.



Je sélectionne ensuite ma base de données « **glpidb** » et, une fois les informations de connexion renseignées, il ne me reste plus qu'à valider l'étape pour poursuivre la configuration.

Pour les étapes **3 à 5**, je clique simplement sur « **Suivant** » car elles ne sont pas pertinentes pour ce projet spécifique. Une fois arrivé à la **dernière étape**, je clique sur « **Utiliser GLPI** » pour finaliser l'installation.

Cela me redirige vers le tableau de bord d'administration de GLPI, où je peux commencer à gérer l'application.



L'installation de GLPI étant réussie, nous pouvons immédiatement commencer à configurer la **gestion des actifs et des utilisateurs**, ainsi qu'à **créer et gérer des tickets d'assistance**.

Grâce à GLPI, nous pouvons **centraliser les demandes et intervenir** rapidement pour résoudre les problèmes, optimisant ainsi notre réactivité et efficacité dans la gestion des ressources et du support technique au sein de **NBRD Corporation**.

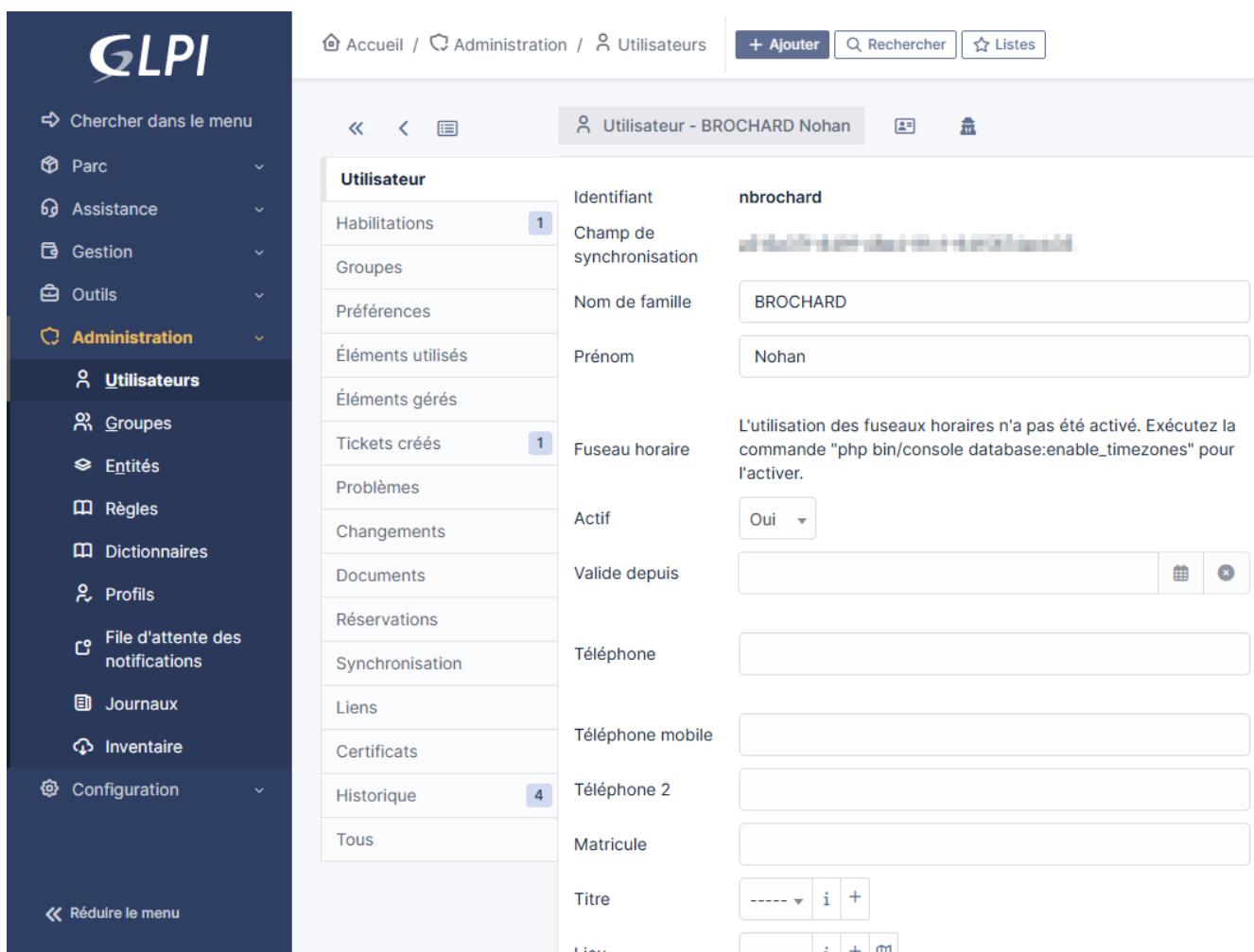
Création d'un utilisateur

Pour finir, je vais créer un utilisateur sur la base de données créée précédemment dans GLPI.

Je vais accéder à l'interface de GLPI, puis naviguer vers Administration > Utilisateurs et cliquer sur « Ajouter utilisateur ». Ensuite, je rempli les informations suivantes pour créer l'utilisateur :

Dans l'exemple qui va suivre, on va créer le technicien Nohan BROCHARD.

- **Identifiant** (pour se connecter sur l'interface GLPI) : nbrochard
- **Nom de famille** : BROCHARD
- **Prénom** : Nohan
- **Mot de passe** : Mot de passe complexe de préférence
- **Actif** : Oui
- **Profil** : Admin (Car le technicien nbrochard doit avoir les permissions administrateur)



Champ	Valeur
Identifiant	nbrochard
Champ de synchronisation	
Nom de famille	BROCHARD
Prénom	Nohan
Fuseau horaire	L'utilisation des fuseaux horaires n'a pas été activé. Exécutez la commande "php bin/console database:enable_timezones" pour l'activer.
Actif	Oui
Validé depuis	
Téléphone	
Téléphone mobile	
Téléphone 2	
Matricule	
Titre	-----
Lieu	

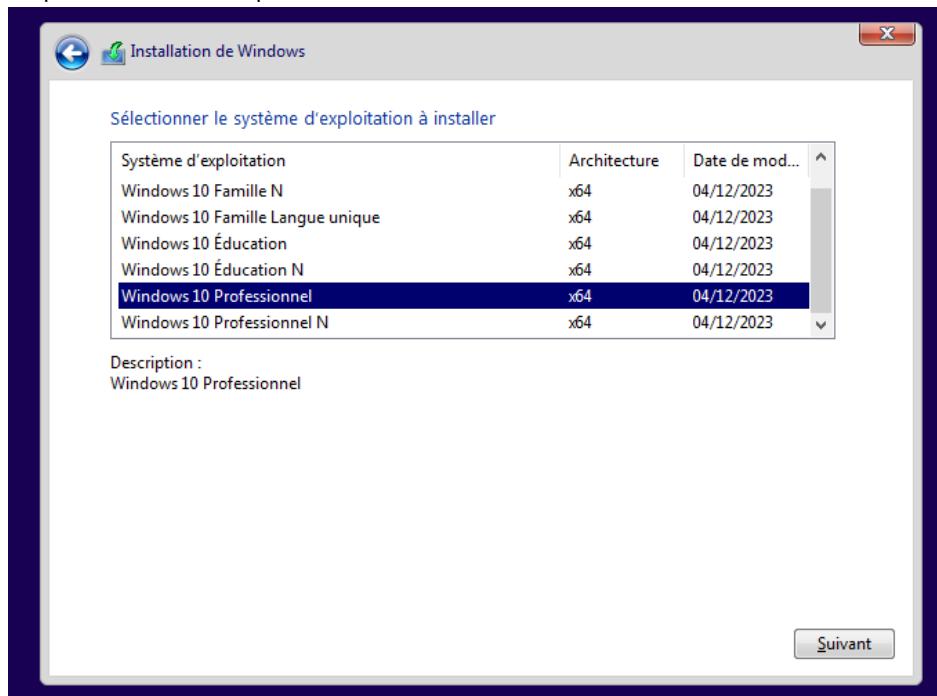


Client Windows 10

Installation du système d'exploitation

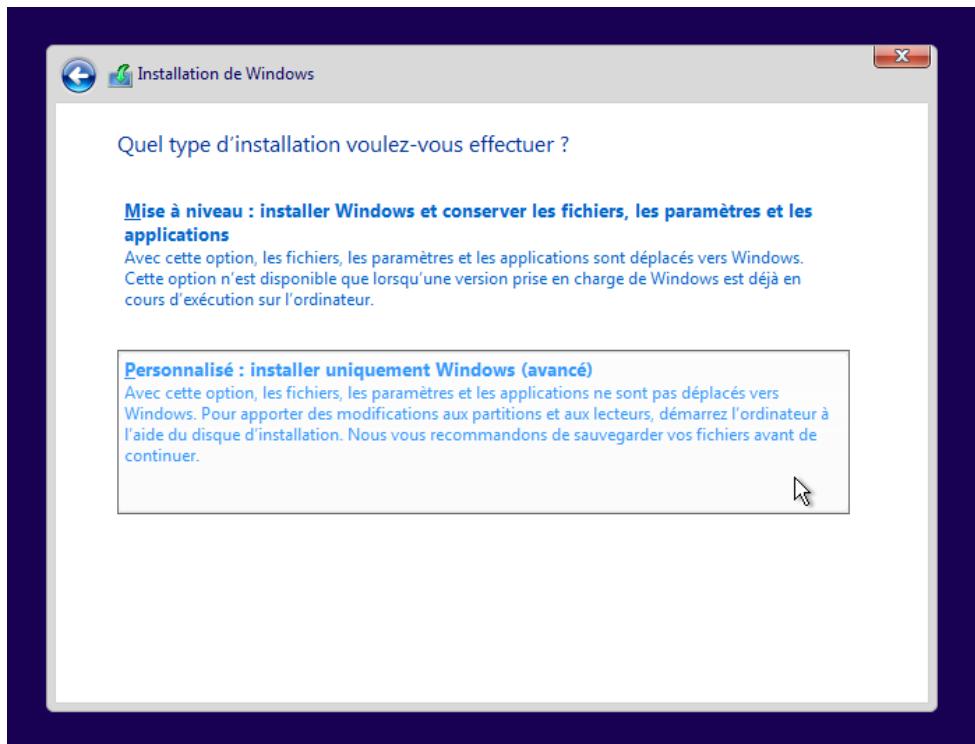
Une fois que j'ai récupéré le **fichier ISO** de Windows 10, je démarre le processus d'installation. Je commence par **boot** sur le fichier ISO pour accéder à l'écran initial, qui me permet de choisir les préférences régionales telles que la langue, le format de l'heure et la devise, ainsi que la disposition du clavier.

Ensuite, je sélectionne la version de Windows 10 qui me convient, dans mon cas, **Windows 10 Professionnel**. Une fois la version choisie, je clique sur « **Suivant** » pour continuer avec l'installation.

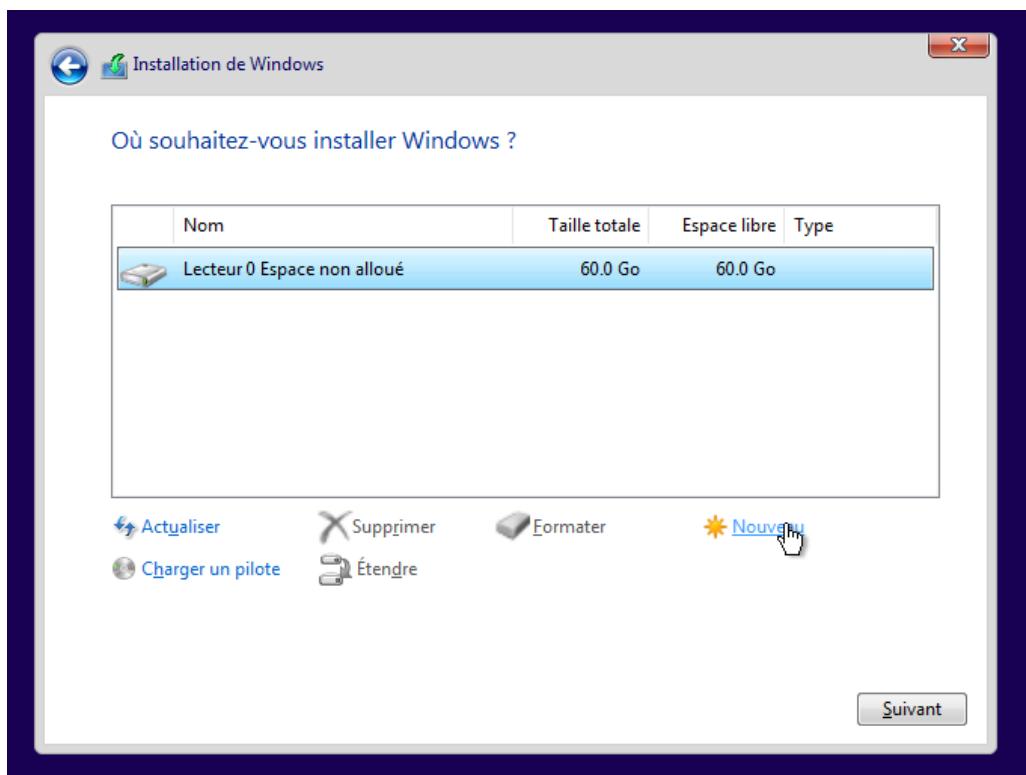


Je coche ensuite la case pour **accepter les termes du contrat de licence Microsoft**, puis je clique sur « **Suivant** » pour continuer l'installation.

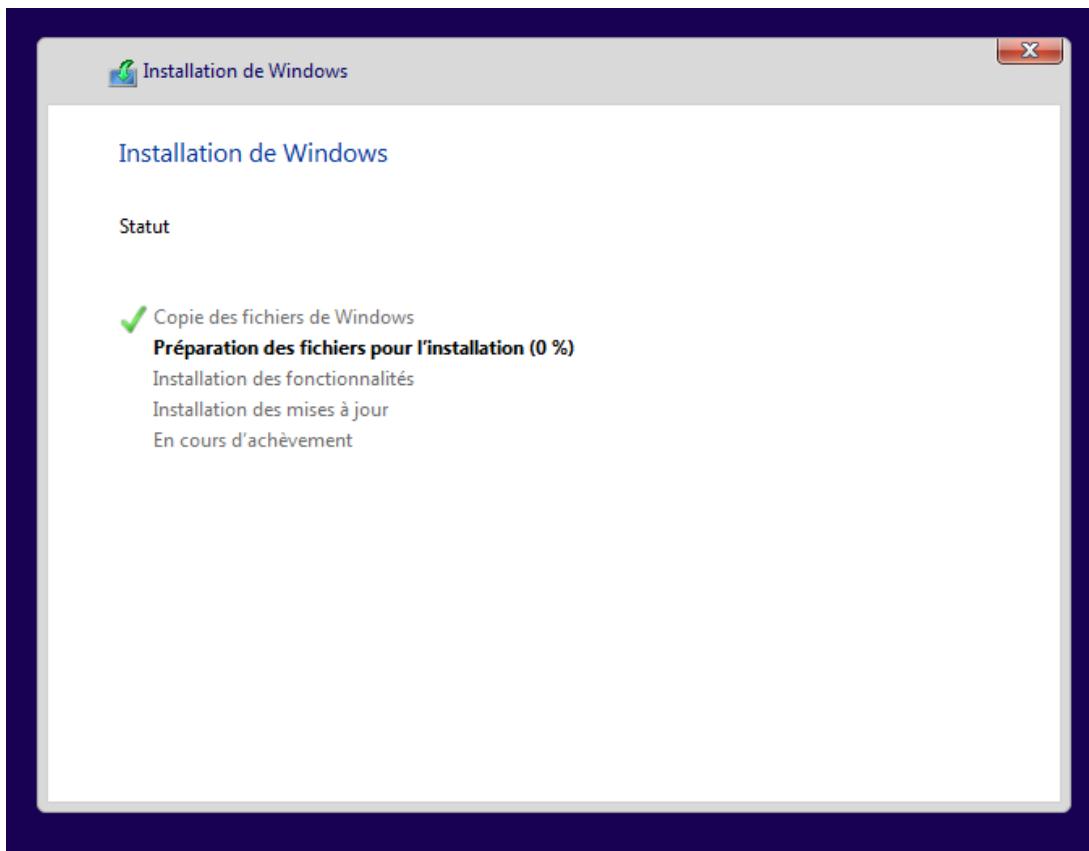
Comme il s'agit d'une nouvelle installation, je choisis l'option « **Personnalisé > Installer uniquement Windows (avancé)** ». Cette option me permet de gérer la configuration de l'installation, comme sélectionner et formater la partition du disque dur, offrant ainsi un contrôle total sur le processus d'installation.



Dans mon cas, l'installation se fait sur un **disque spécifique déjà formaté**. Je sélectionne simplement le **disque concerné**, puis je clique sur « **Suivant** ».



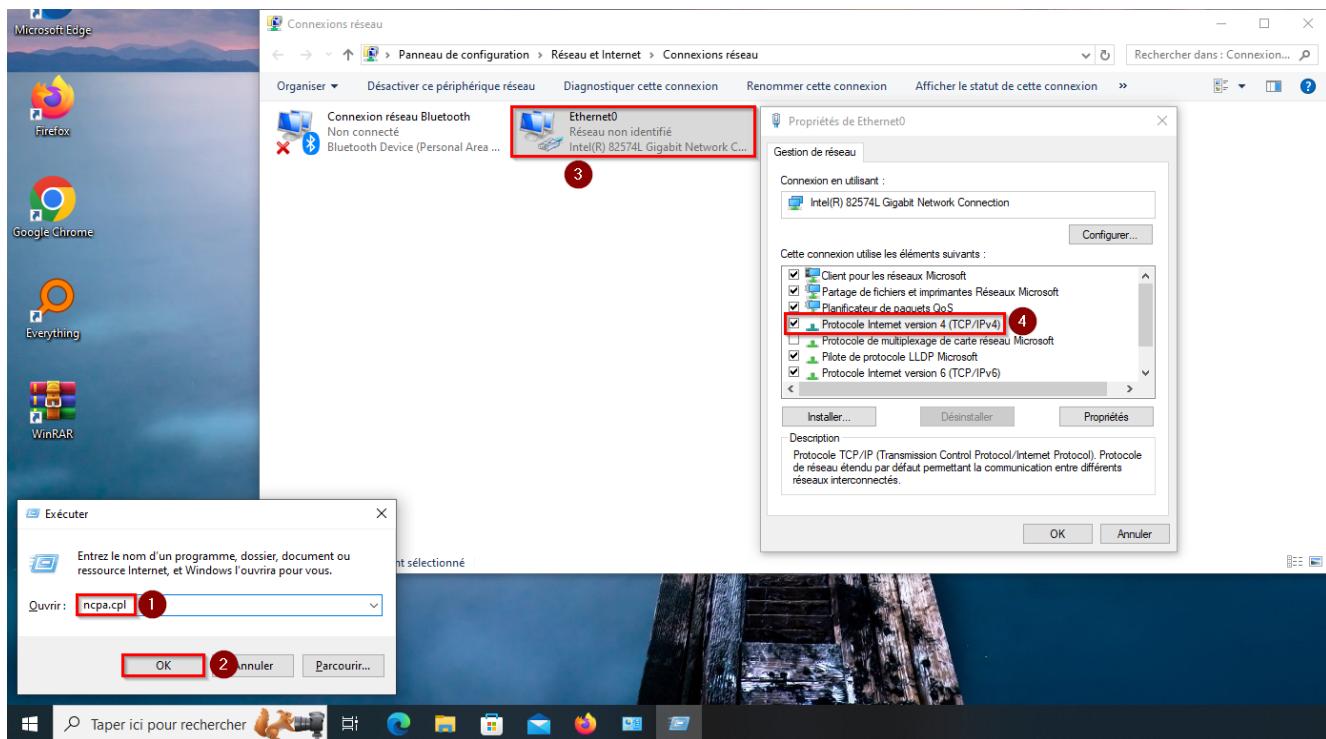
Ensuite, l'installation se poursuit avec la **copie des fichiers nécessaires**, comme ceux du dossier **System32**, sur le disque sélectionné. Ce processus inclut l'extraction et l'**installation des fichiers système essentiels** pour préparer **Windows 10** au premier démarrage.



Une fois l'installation terminée, il ne me reste plus qu'à **configurer le système pour le connecter au réseau**. Cela me permettra d'intégrer l'ordinateur au **domaine Active Directory**, afin de pouvoir me connecter avec un compte utilisateur du domaine depuis l'annuaire.

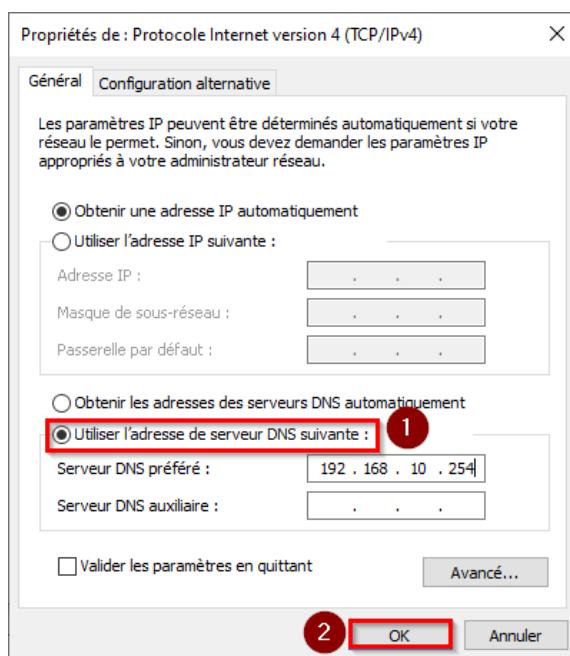
Configuration réseau

Je me rends d'abord dans le menu Exécuter en appuyant sur **WIN + R**, puis je saisis la commande **ncpa.cpl** pour accéder au menu « Connexions réseau ». Ensuite, je fais un clic droit sur ma connexion réseau et sélectionne « Propriétés ». Dans les propriétés, je clique sur « Protocole Internet version 4 (TCP/IPv4) » et je renseigne les informations réseau nécessaires, afin d'assurer la communication correcte avec le serveur AD DS.



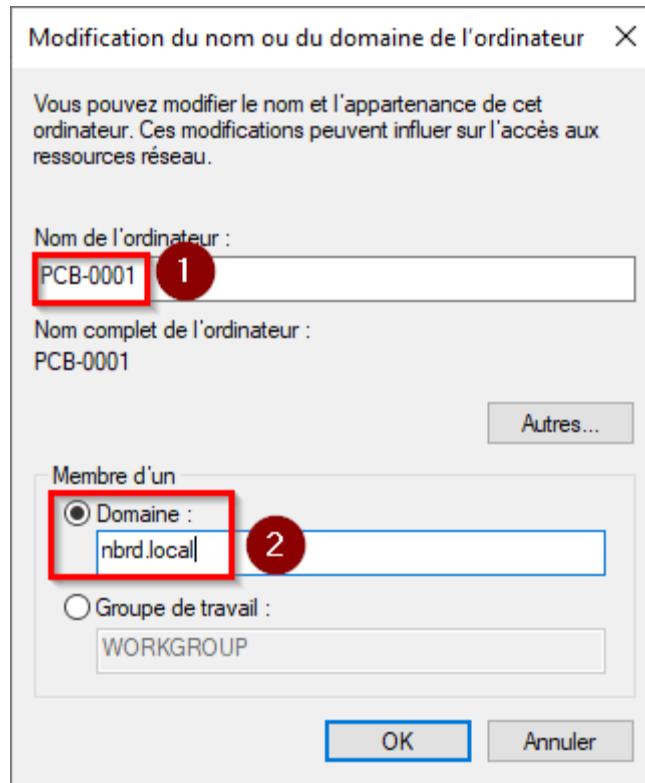
Une fois dans cette interface, je laisse la connexion en mode **DHCP** car c'est mon **PFSense (routeur)** qui me communique automatiquement l'**adresse IP**, le **masque** et la **passerelle**.

Je dois seulement modifier le **serveur DNS préféré** en entrant l'adresse IP fixe de mon serveur **AD**, soit **192.168.1.73**, afin d'établir une connexion entre les deux machines.



Rejoindre le domaine AD

Sur le PC Windows 10, je vais dans **Paramètres > Système > À propos**, je renomme l'ordinateur en « **PCB-0001** » (**PC Bureau**), puis je clique sur **Rejoindre un domaine**. J'entre le **nom de domaine** et je clique sur **Suivant**.



Ensuite, je devrai redémarrer le PC pour terminer le processus d'intégration dans le domaine. Une fois le poste redémarré, je peux vérifier que je me connecte correctement au domaine « **NBRD** ». Par la suite, je n'ai plus qu'à me connecter avec un utilisateur de l'AD, dans mon cas, il s'agit de **Nohan BROCHARD**.

