SOMMAIRE

I-Préparation de l'environnement

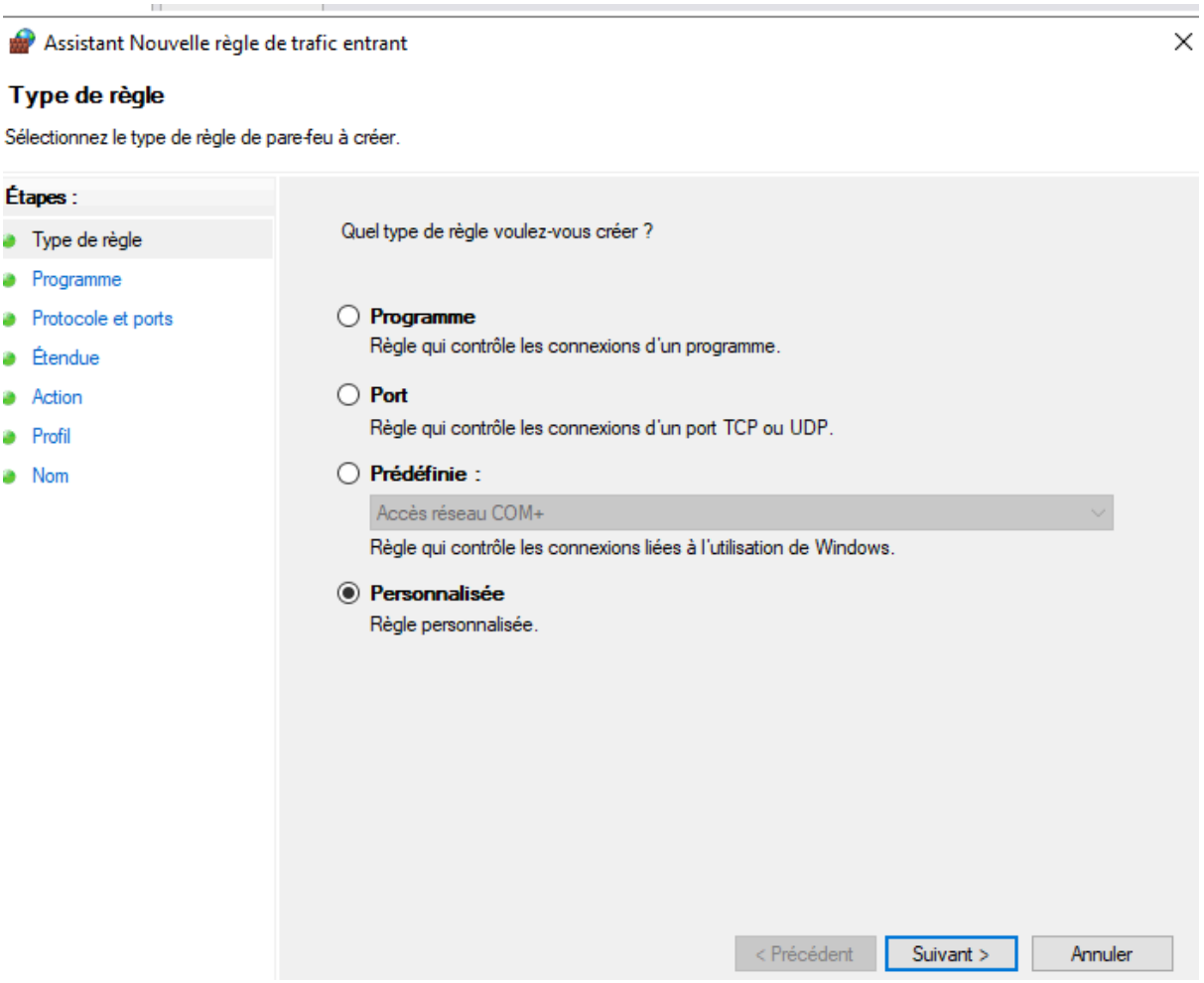
Après la création de mes trois machines à savoir deux serveurs et un client. Chaque poste du parc a été configuré avec une **carte réseau en mode DHCP**, permettant l'attribution automatique d'une adresse IP.
La plage d'adresses utilisée est **192.168.145.0/24**, assurant ainsi une gestion centralisée et cohérente des configurations réseau.Pour les noms des serveurs, j'ai choisi de rester dans la simplicité : **SRVAD1** et **SRVAD2** ; pour le client, **PCFIXE01**.

Test de connectivité

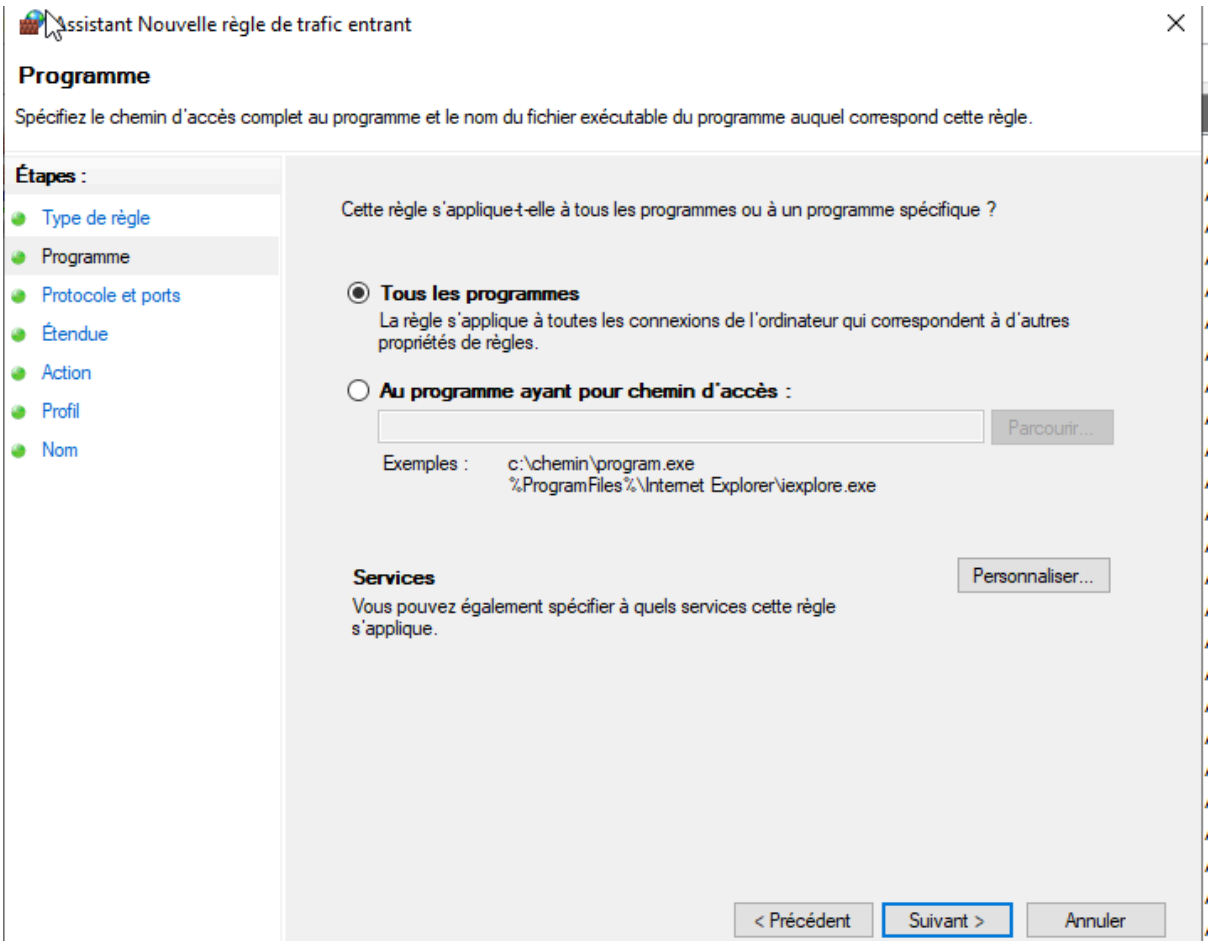
Pour réaliser un test de connectivité (ping) entre les machines, et vérifier qu'elles peuvent communiquer, il faut d'abord ajouter une nouvelle règle icmpv4 parce que par défaut windows bloque tous les ping . Pour le faire suivez ces étapes suivantes.

allez dans pare-feu windows defender puis cliquez sur règle de trafic entrant puis nouvelle règle

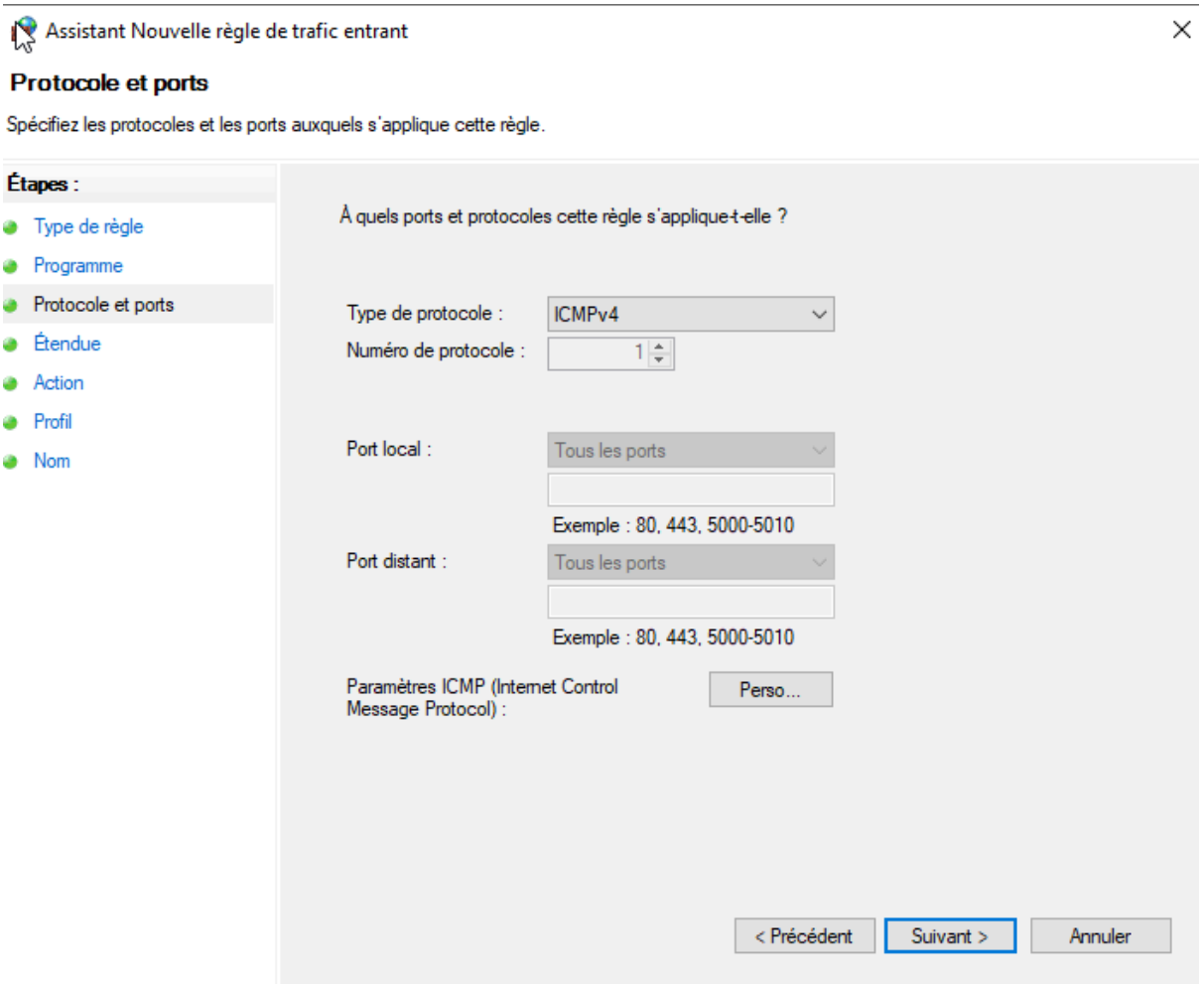
comme type de règle choisir personnalisée puis suivant



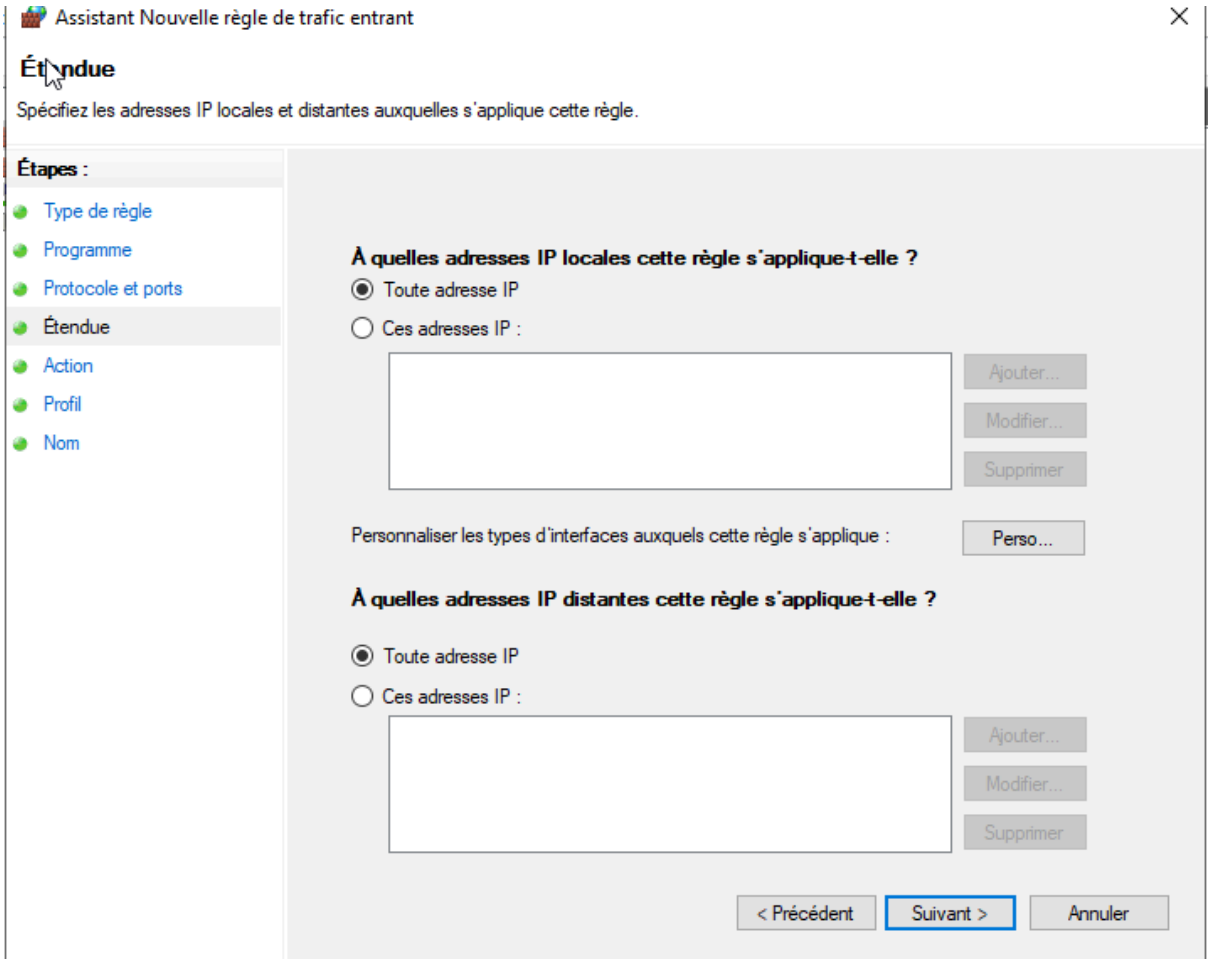
Spécifier le chemin d'accès j'ai laissé par défaut tous les programmes suivant



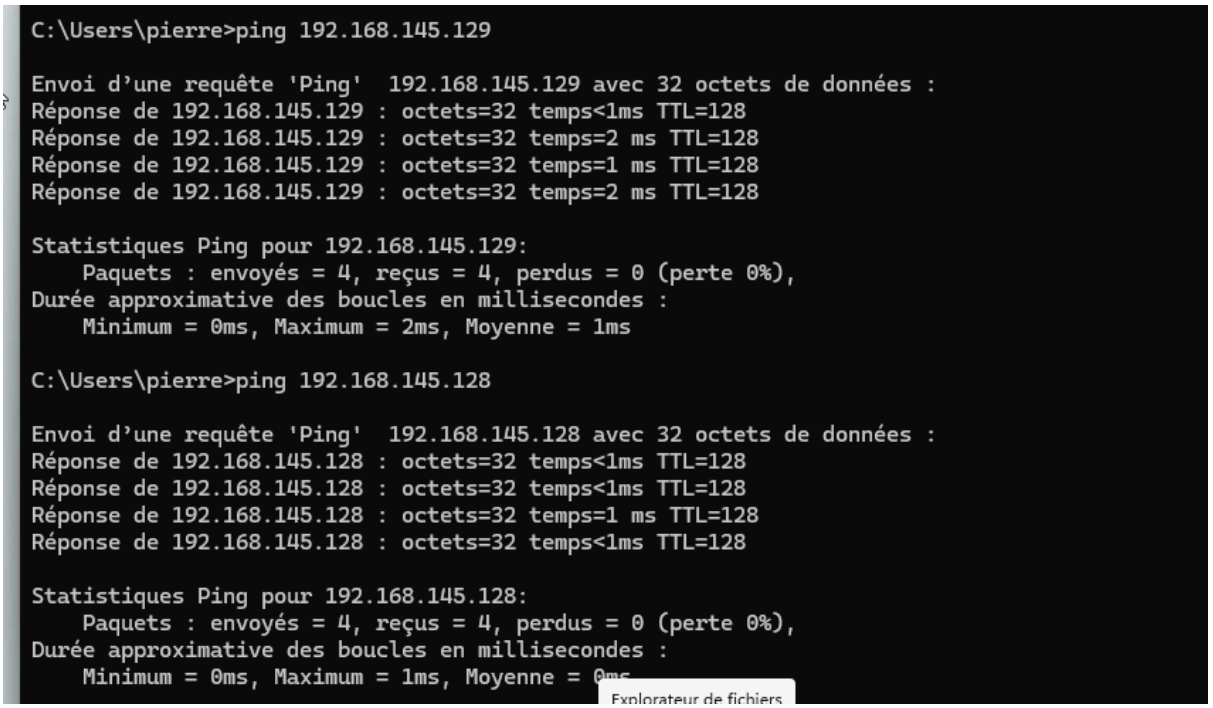
ensuite spécifiez le type de protocole dans notre cas icmpv4



Définir l'adresse IP sur laquelle la règle s'applique dans notre cas j'ai laissé toute adresse



ensuite faire suivant , suivant puis nommé la règle et terminer maintenant nous pouvons effectuer les tests de connectivités entre nos différents machine

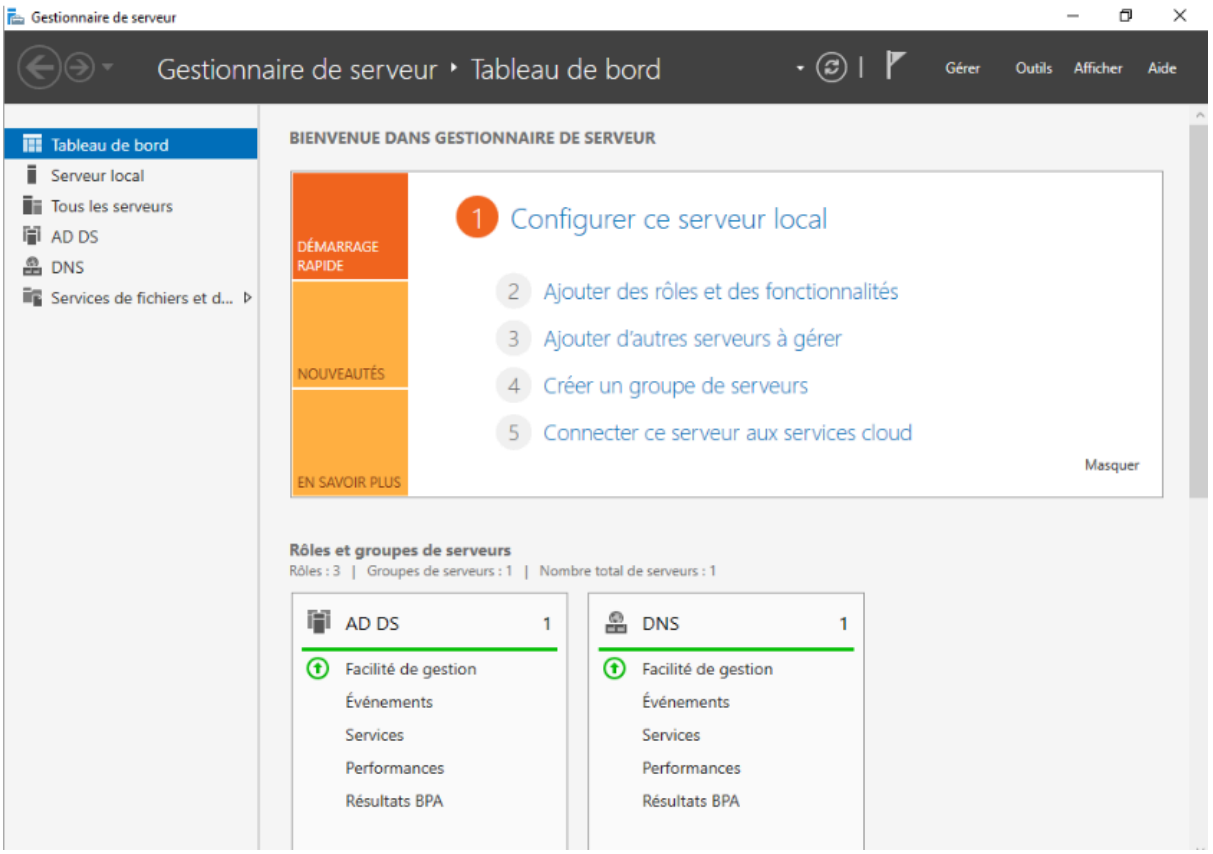


Comme le montre l'image ci-dessus depuis le PCFIXE01 j'arrive à joindre les deux serveurs.Maintenant que le réseau est configuré, il ne reste qu'à installer les services dont vous aurez besoin. Active Directory se base sur le service de noms de domaines pour fonctionner. Vos serveurs auront donc besoin du rôle de serveur DNS en plus du rôle des services Active Directory Domain Services.

Si toutefois vous oubliez d'installer le rôle DNS, il sera mis en œuvre automatiquement par Microsoft lors de la promotion de votre serveur en contrôleur de domaine.

Préparation des serveurs

Pour cela, il faut vous rendre dans le gestionnaire de serveurs :

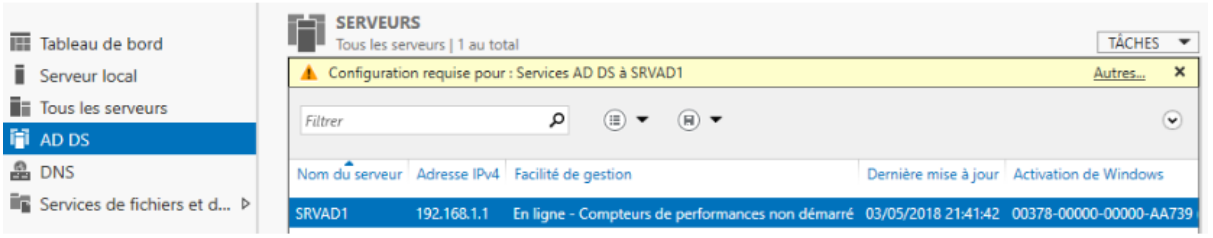


Cliquez sur **Ajouter des rôles et des fonctionnalités**. Validez la première étape de l'assistant en cliquant sur **Suivant**. Sélectionnez **Installation basée sur un rôle ou une fonctionnalité** et sélectionnez le nom du serveur dans la liste, cochez **Service AD DS** et lancez l'installation.

Configuration de notre premier contrôleur de domaine

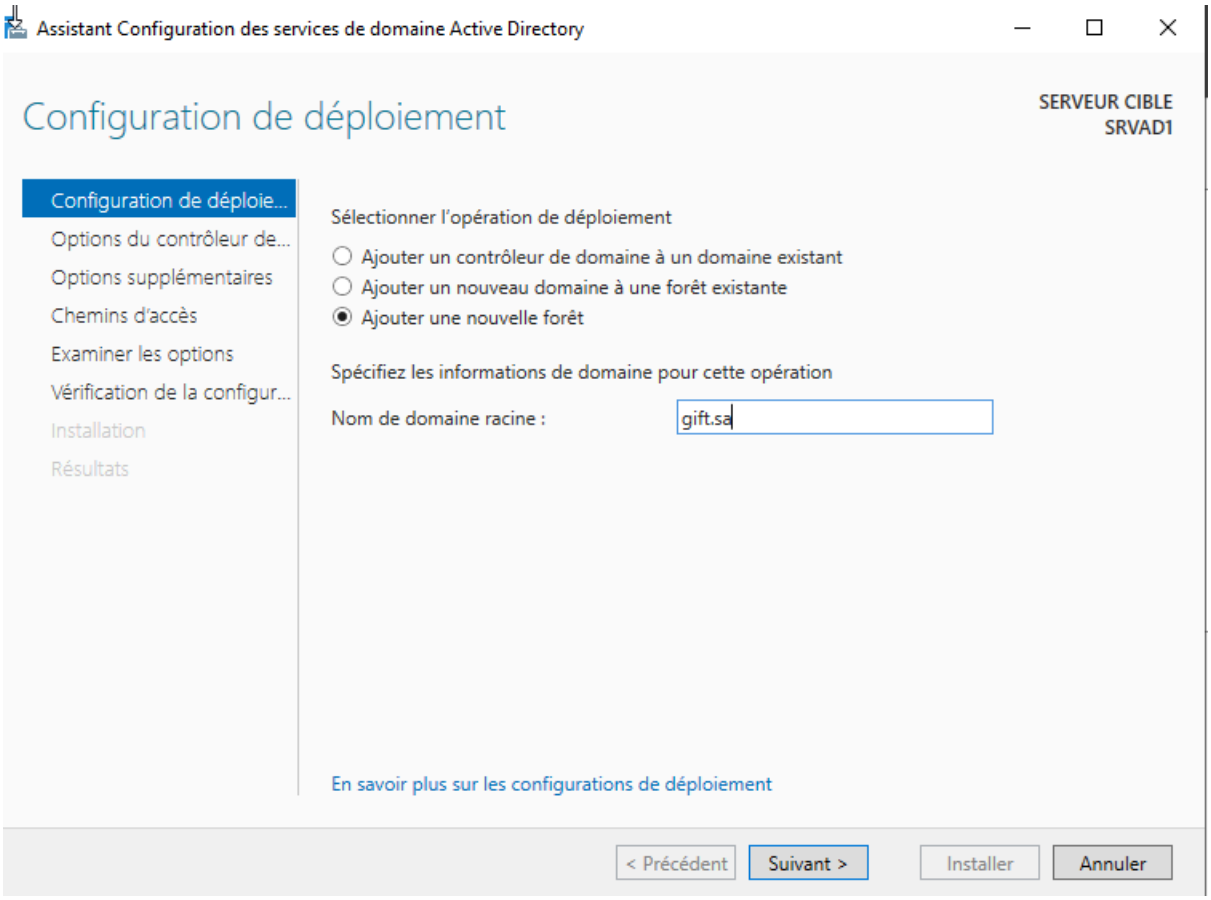
Pour mettre en œuvre un premier contrôleur de domaine, suivez ces étapes suivantes:

Tout d'abord, rendez-vous à nouveau dans le gestionnaire de serveur, et cliquez sur le service AD DS dans la liste sur la gauche du gestionnaire.

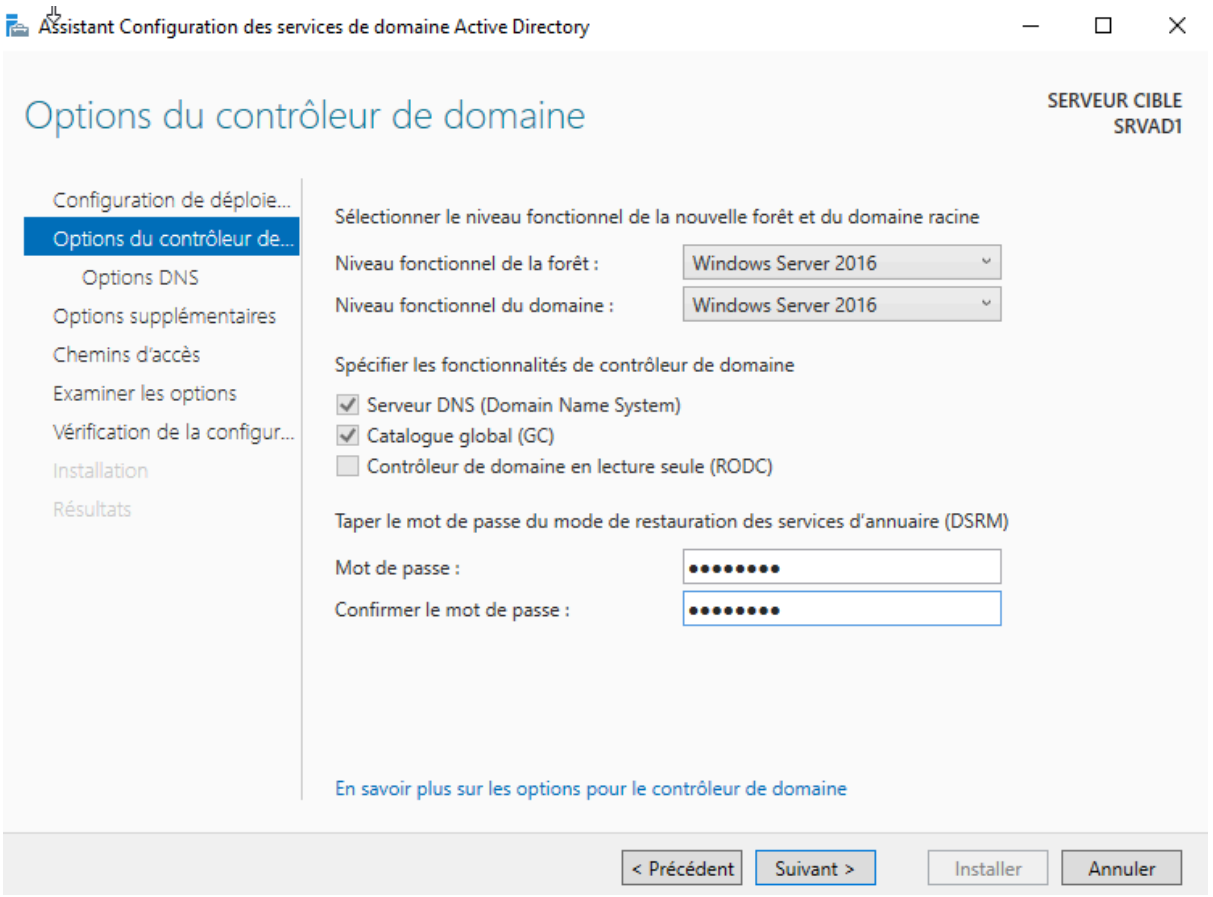


Puis cliquez sur le bouton **Autres** présent sur la bande jaune. Cliquez ensuite sur **Promouvoir ce serveur en contrôleur de domaine** ! L'assistant vous propose

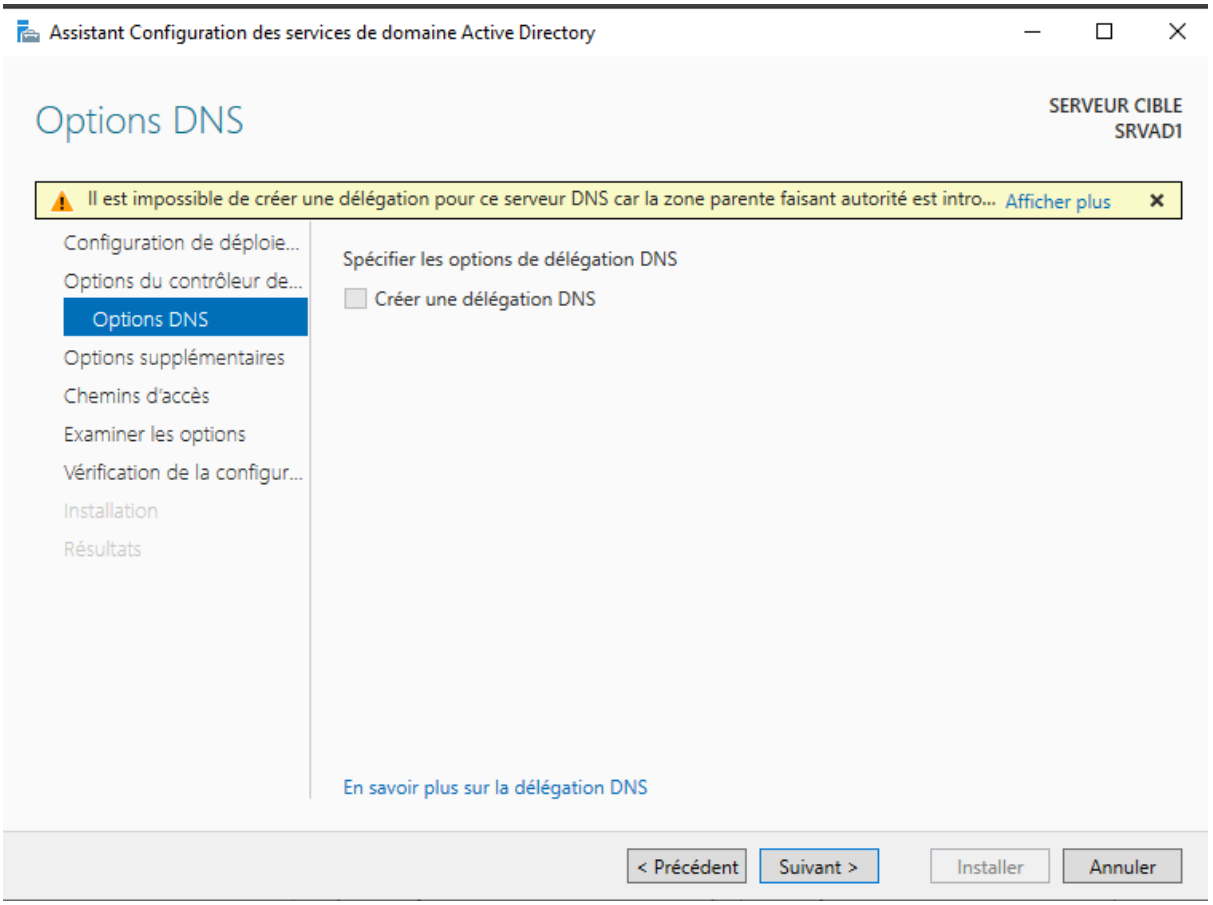
alors d’ajouter une nouvelle forêt, et de définir le domaine racine dans notre situation j’ai choisi gift.sa



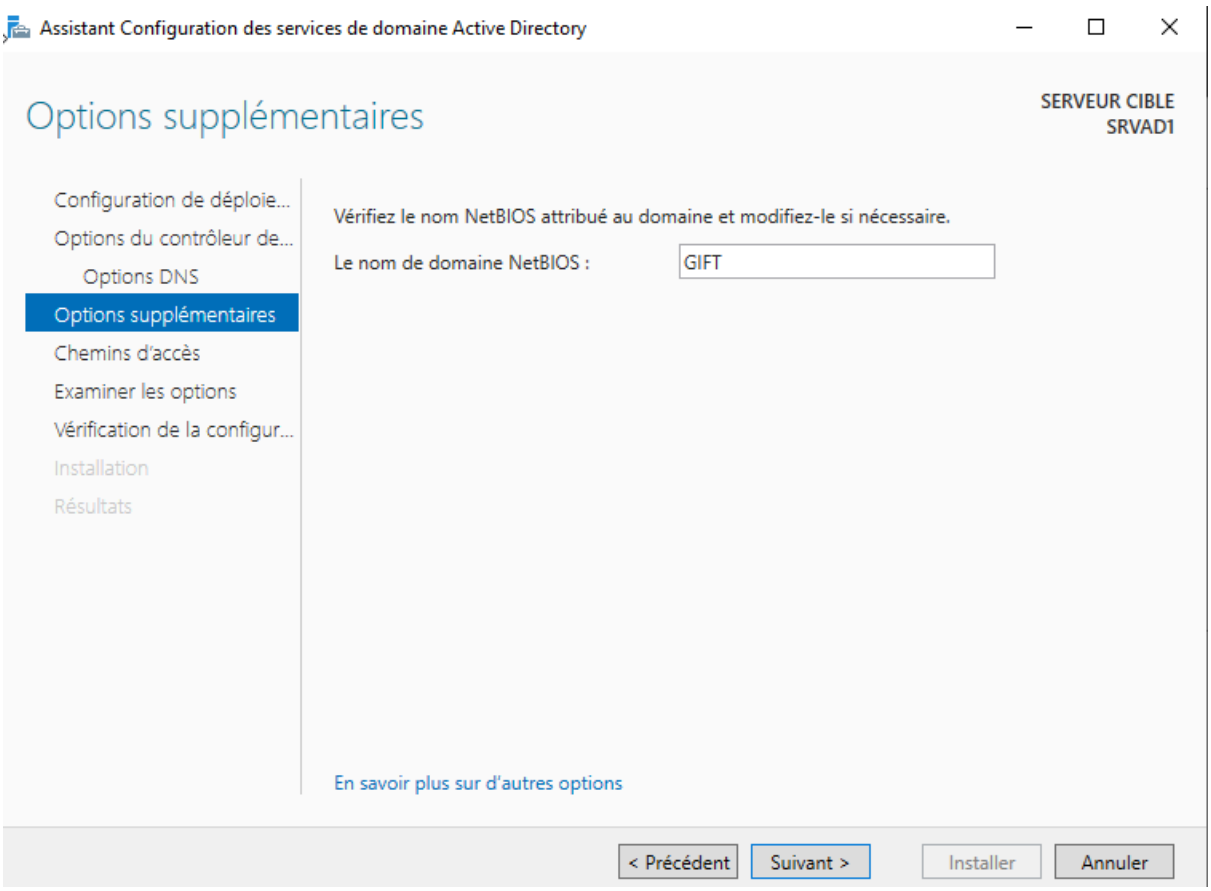
Ensuite, vous avez un choix à faire sur le **niveau fonctionnel** du domaine et de la forêt.
Le niveau fonctionnel permet de limiter les fonctionnalités dans le cas où un contrôleur de domaine d’une version inférieure serait mis en place (Windows 2008, 2008R2, 2012, 2012R2).



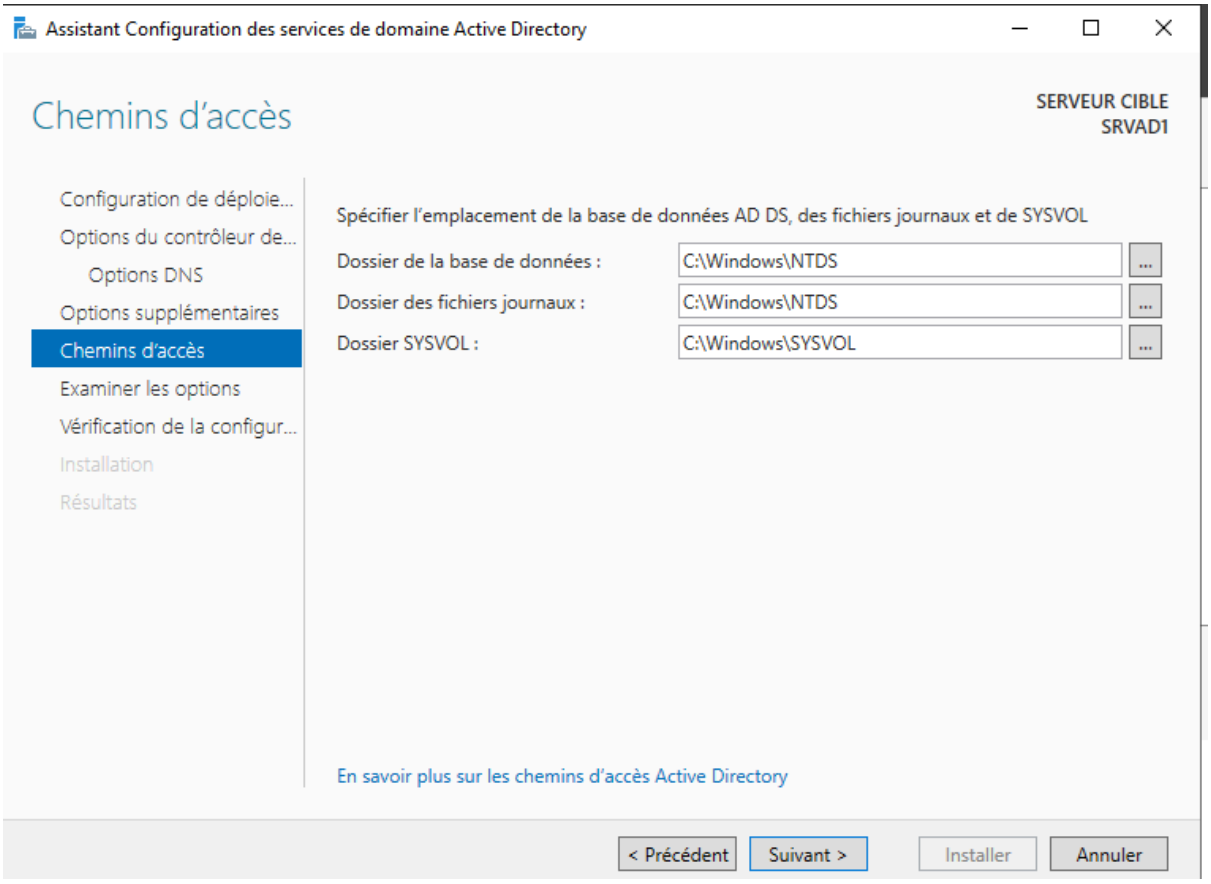
A cette étape vue que le serveur dns n’est rattaché à aucun serveur c’est normal d’avoir ce message laissé par défaut et faire suivant



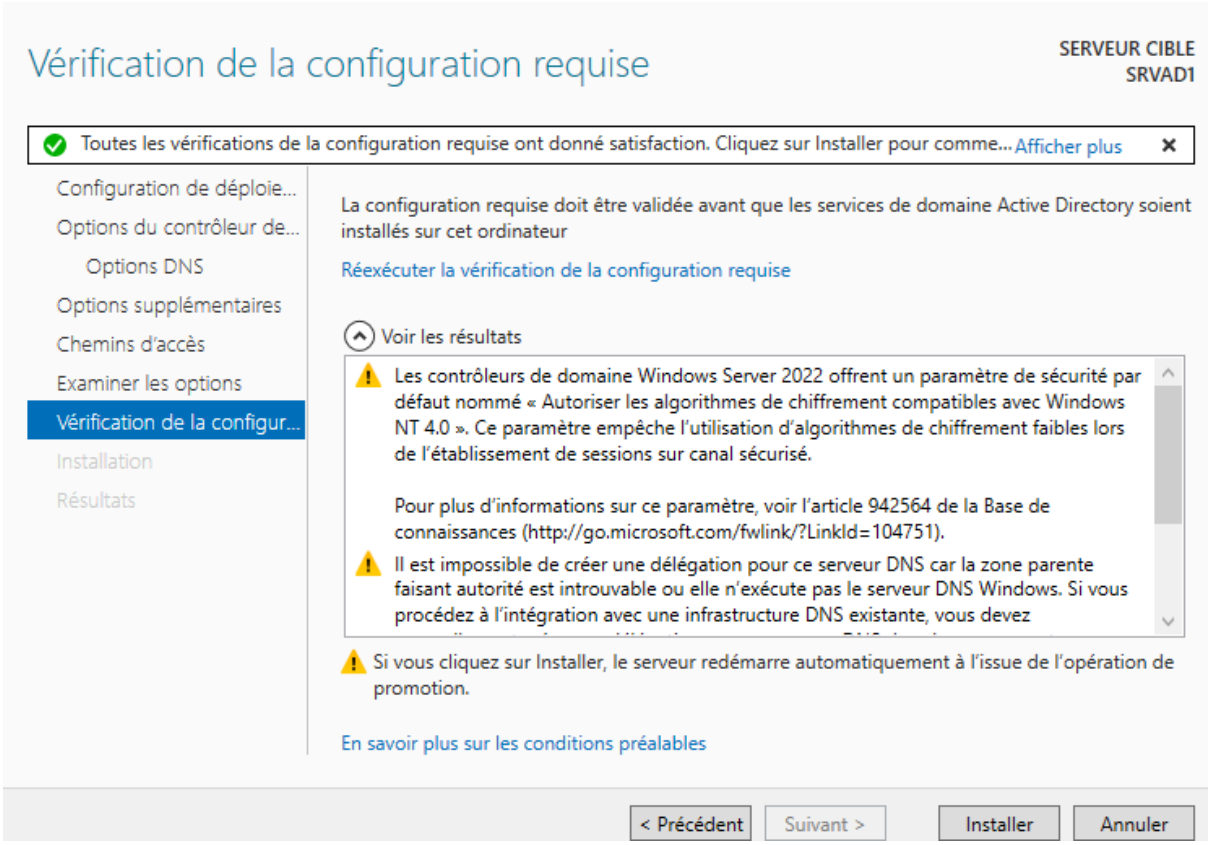
la machine va ensuite détecté le nom par défaut attribué à notre serveur netBIOS faire suivant



ensuite laisser par défaut et faire suivant

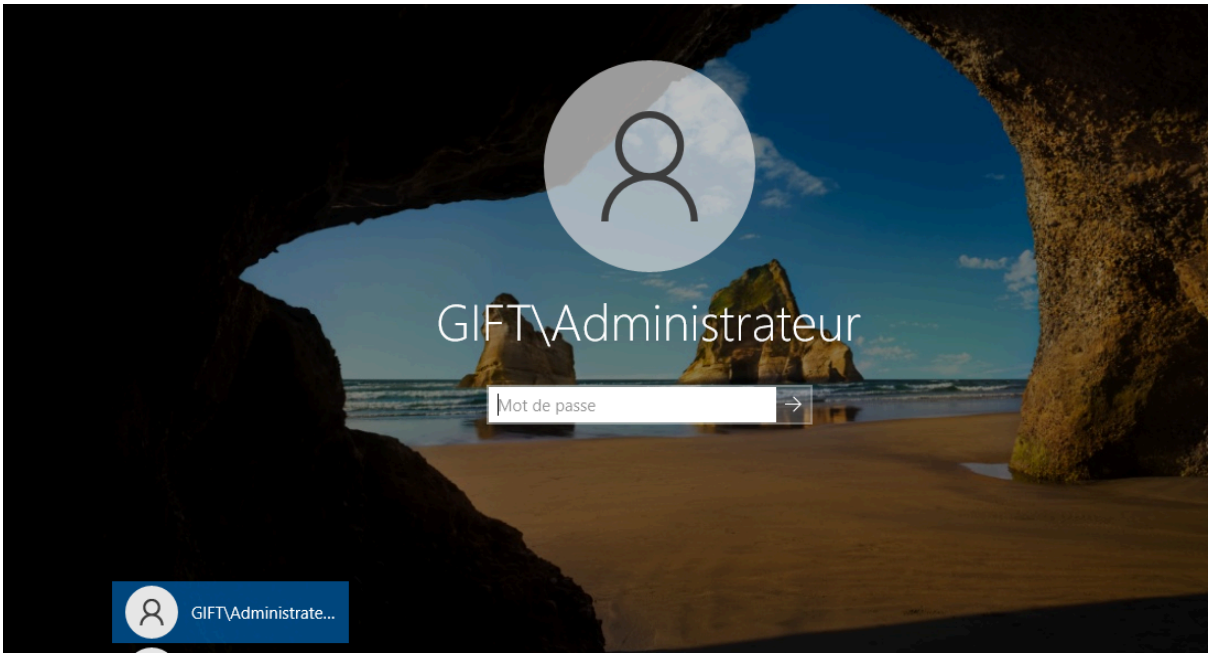


ensuite nous pouvons voir un petit récapitulatif des étapes faire installer



La génération de l'annuaire va commencer dès que vous validerez ces choix. Cela peut prendre quelques minutes. Il est obligatoire de redémarrer le serveur après cette opération.

Au redémarrage, vous pouvez observer qu'il vous est proposé de vous authentifier avec un nom de domaine avant votre nom d'utilisateur, GIFT\Administrateur :



Configuration de notre second contrôleur de domaine

Maintenant, je vous propose de reproduire ces opérations sur le second serveur. Cette fois, vous allez choisir d'ajouter votre serveur à un domaine existant.

Attention, le deuxième serveur ne sera capable de retrouver la configuration du domaine existant que si vous avez réalisé correctement sa configuration réseau. La paramètre important à ne pas oublier est de lui spécifier que ses serveurs DNS primaire et secondaire sont 192.168.145.128 et 192.168.145.129.

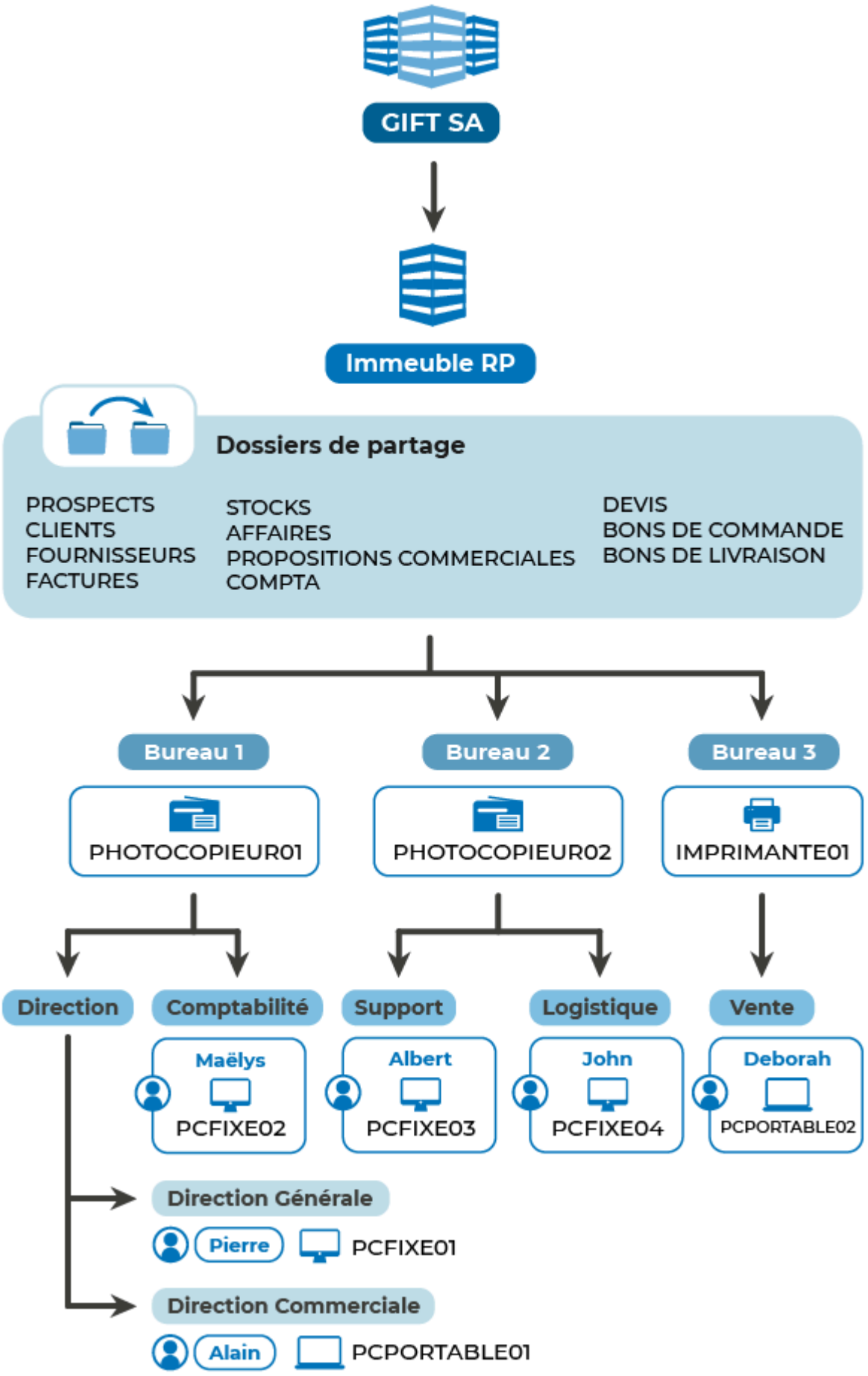
Les choix sont plus restreints, car les paramètres propres au domaine et à la forêt sont déjà stockés dans la base de données présente sur le premier contrôleur de domaine. Après avoir terminé cette étape, il faut également redémarrer le serveur. Au redémarrage, vous observez à nouveau le nom de domaine avant votre nom d'utilisateur : GIFT\Administrateur.

Le serveur est donc déclaré comme contrôleur de domaine, et a été inclus dans votre domaine.

Mettre en place l’arborescence de notre active directory

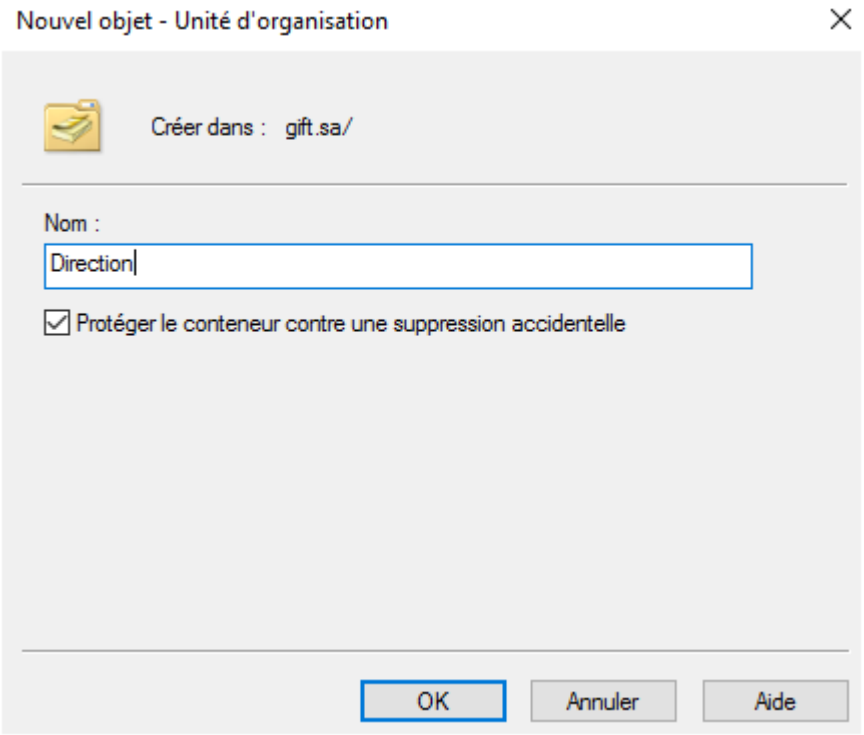
Déclaration des ressources

Notre domaine est maintenant créé. Ce qui signifie qu’on dispose d’un annuaire, mais presque vide. Il vous faut donc maintenant créer les ressources que ous avons identifiées au sien de notre entreprise pour mieux connaître de quoi il s’agit je vous invite à vous référez de l’organigramme suivante:

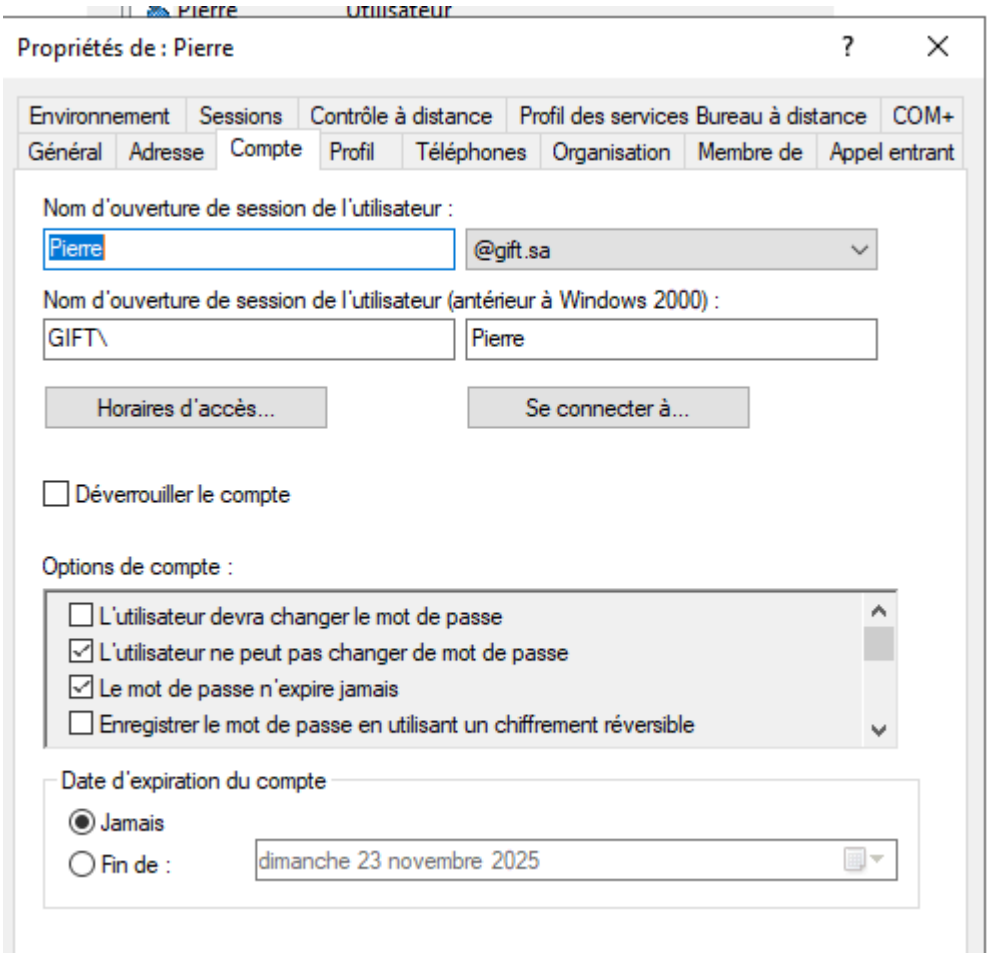

GIFT SA
Immeuble RP
Dossiers de partage
PROSPECTS
CLIENTS
FOURNISSEURS
FACTURES
STOCKS
AFFAIRES
PROPOSITIONS COMMERCIALES
COMPTA
DEVIS
BONS DE COMMANDE
BONS DE LIVRAISON
Bureau 1
Bureau 2
Bureau 3
PHOTOCOPIEUR01
PHOTOCOPIEUR02
IMPRIMANTE01
Direction
Comptabilité
Support
Logistique
Vente
Maëlys
PCFIXE02
Albert
PCFIXE03
John
PCFIXE04
Deborah
PCPORTABLE02
Direction Générale
Pierre
PCFIXE01
Direction Commerciale
Alain
PCPORTABLE01

Création des premiers objets

Je vous propose d'utiliser l'outil **Utilisateurs et ordinateurs Active Directory** ; il est, encore aujourd'hui, le plus utilisé en entreprise. Il est très simple d'utilisation : pour créer une unité organisationnelle pour la direction, il vous suffit de cliquer sur le nom du domaine et de sélectionner « **nouveau** » puis « **Unité d'organisation** », et de fournir un nom. Vous avez sûrement remarqué qu'il est possible de cocher une option lors de ce processus. Elle permet de mettre en place une **protection contre la suppression accidentelle**.
Sans cette option, un geste de travers, la touche suppr est appuyée et c'est le drame ! Toutes les UO sont supprimées !

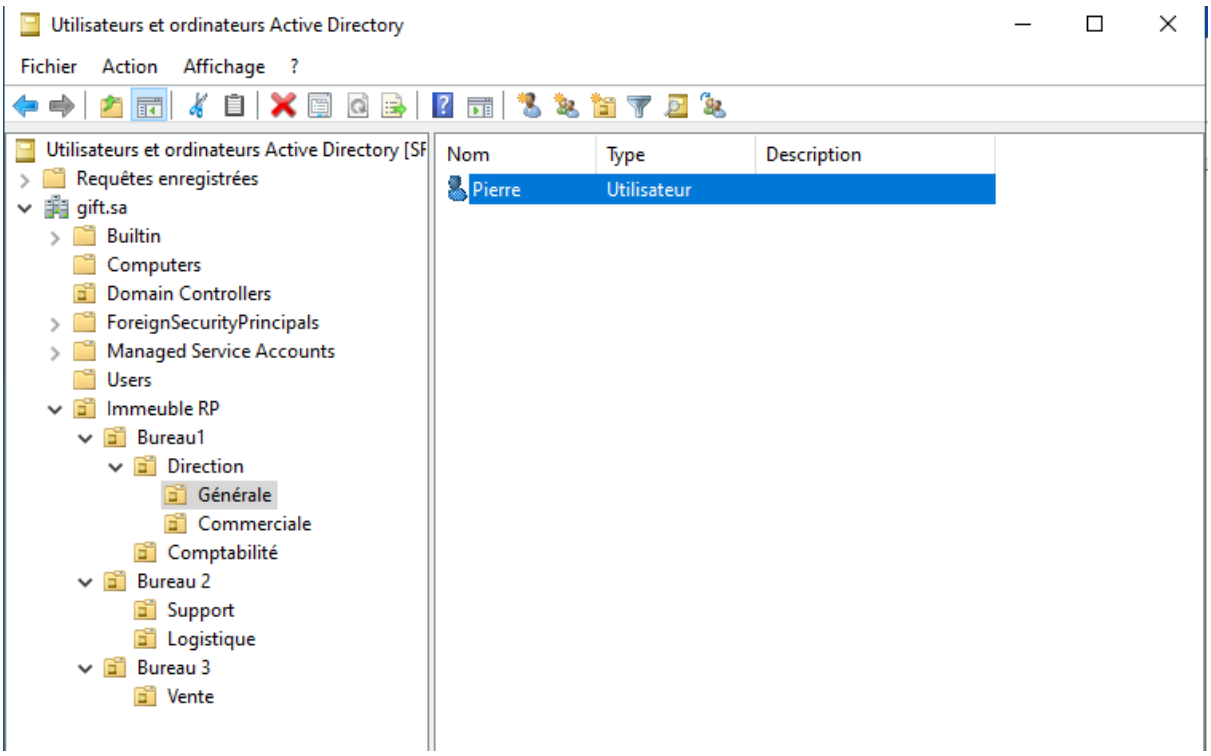


Pour créer un objet utilisateur, là aussi rien de plus simple : cliquez sur le nom de l'unité organisationnelle dans laquelle vous souhaitez ajouter un utilisateur, puis sélectionnez « **Nouveau** » et enfin « **Utilisateur** ». Sur ce type d'objet, il faut remplir une fiche d'identification qui permet de fournir les informations complètes sur un utilisateur

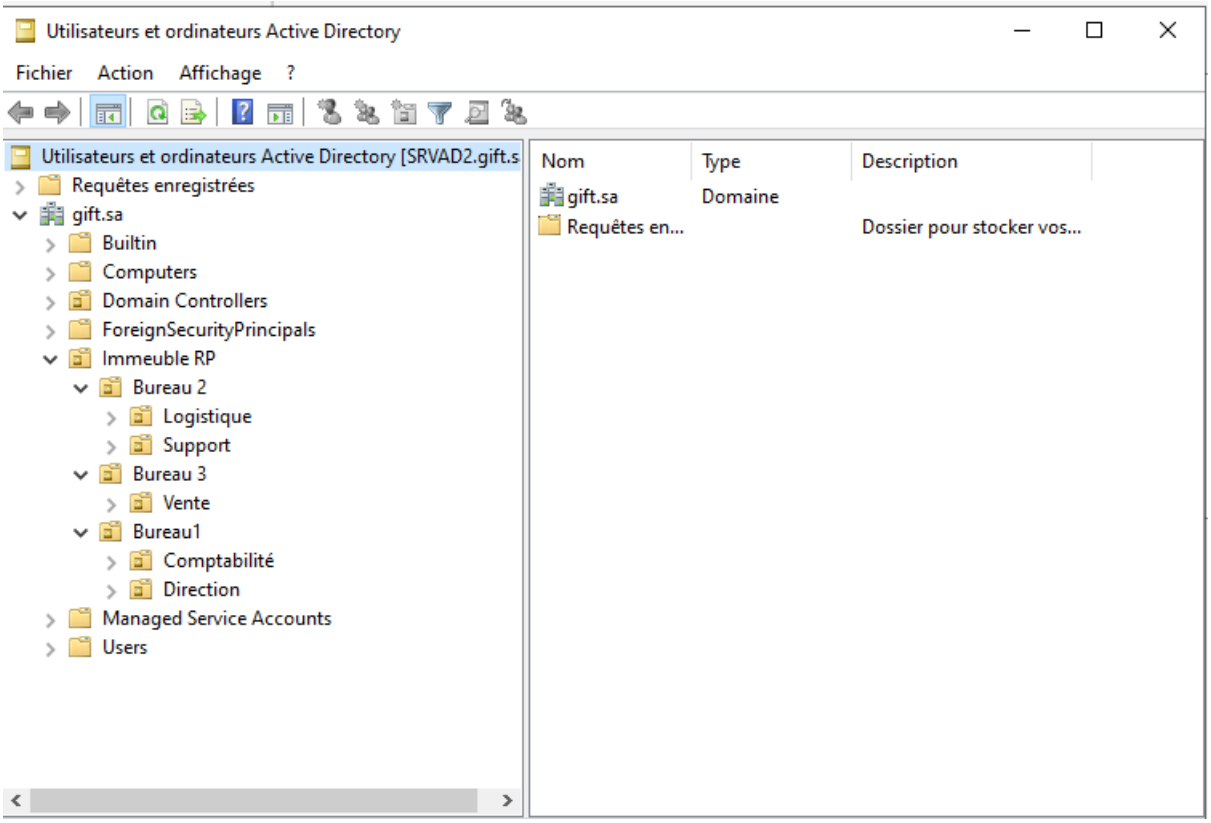


Vous noterez que pour les utilisateurs, vous devez ajouter plus d'informations avec notamment un nom d’ouverture de session, et dans la fenêtre suivante, un mot de passe.

voici la structure de notre annuaire avec les différentes OU et objets types utilisateurs



on peut voir ci-dessus le fonctionnement de la réplication sur notre serveur SRAD2



Intégration des postes clients au domaine

L’intégration d’un poste client à un domaine consiste à l’enregistrer comme une ressource au sein de l’annuaire du réseau. Cette démarche permet au poste de communiquer en permanence avec les contrôleurs de domaine et de s’insérer dans l’architecture organisationnelle définie.

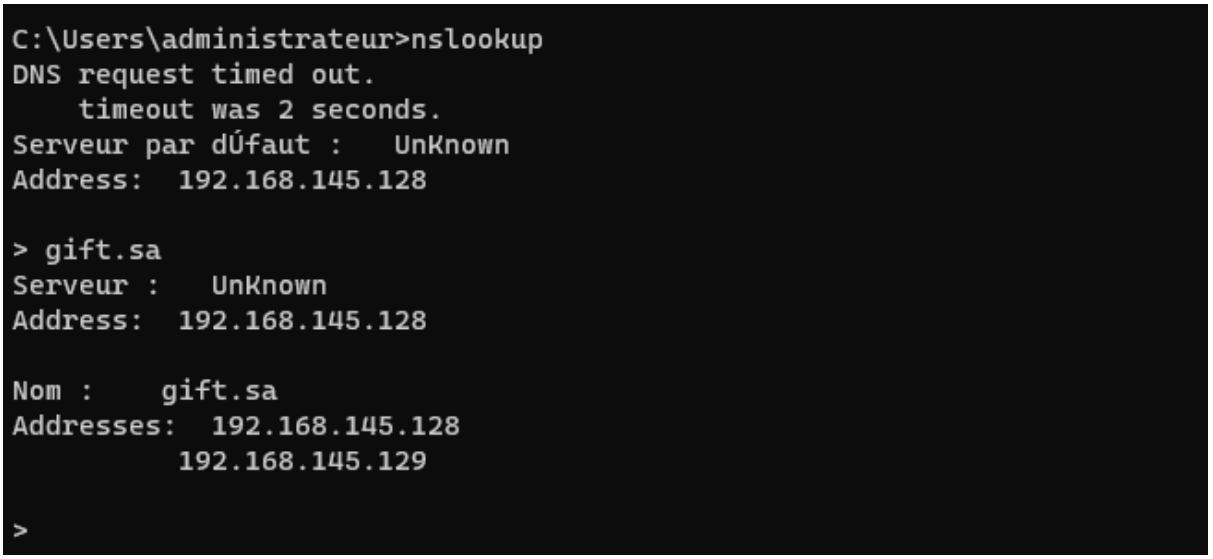
Enjeux pour l’entreprise :

- **Inventaire et gestion centralisée** : Chaque poste intégré est répertorié et peut être classé selon la structure hiérarchique de l’annuaire.
- **Configuration simplifiée** : Les stratégies et paramètres sont déployés de manière homogène et centralisée depuis les contrôleurs de domaine.
- **Sécurité et cohérence** : Les postes clients deviennent des éléments reconnus et supervisés, facilitant le contrôle d’accès et la conformité du parc informatique.

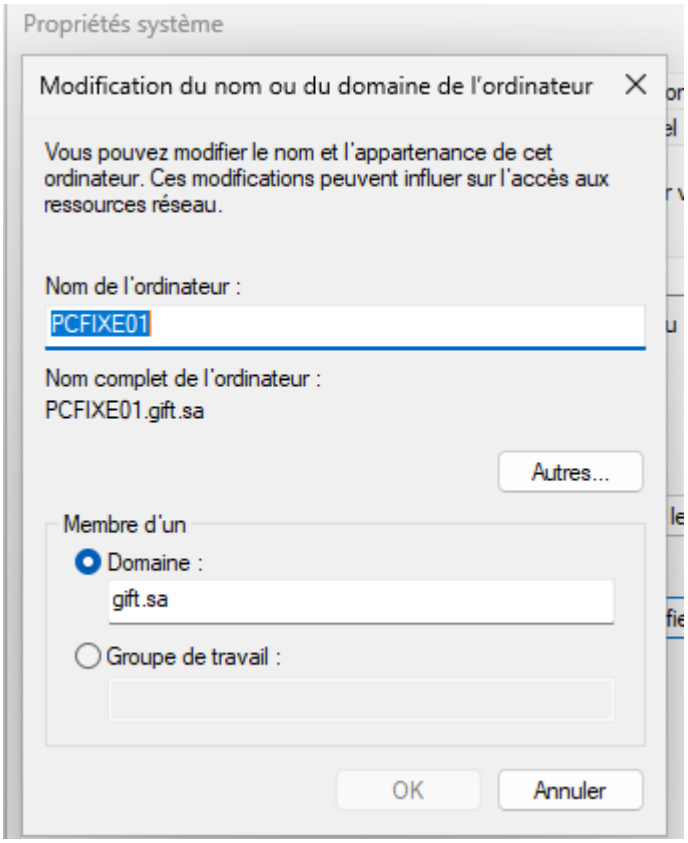
Cette intégration est une étape clé pour administrer efficacement un réseau d’entreprise et en assurer la cohérence.

Voyons justement, étape par étape, comment ajouter un poste client dans notre AD :

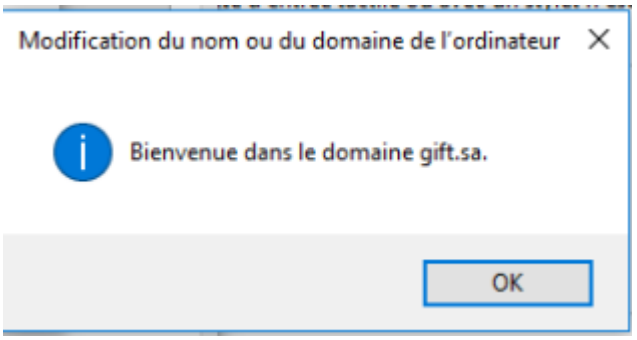
au niveau de notre client (PCFIXE01) ouvrir l’invite de commande pou voir au niveau DNS tout fonctionne normalement avec l'outil nslookup on peut voir que notre DNS reconnait bien notre domaine



Maintenant pour intégrer la machine au domaine il faut il faut aller dans les propriétés du système dans l'onglet à propos cliquez sur renommer ce pc puis modifiez et mettre le nom du domaine

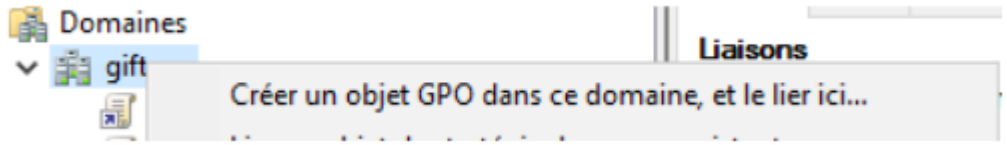


après vous verrez un message de bienvenue au domaine une fois que la machine ait redémarrer il fait partie du domaine

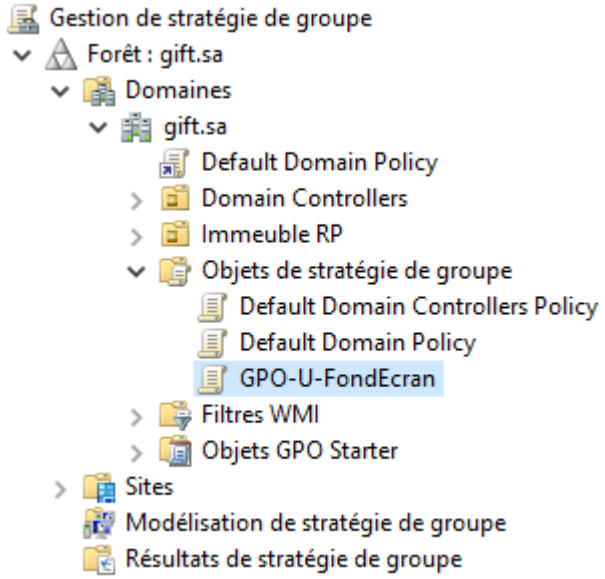


Mise en place des stratégies de groupes

Pour créer notre premier GPO au niveau du gestionnaire de serveur à l'onglet outil choisir **gestion des stratégies de groupe** vous allez donc créer un nouvel objet GPO en cliquant sur le nom de votre domaine

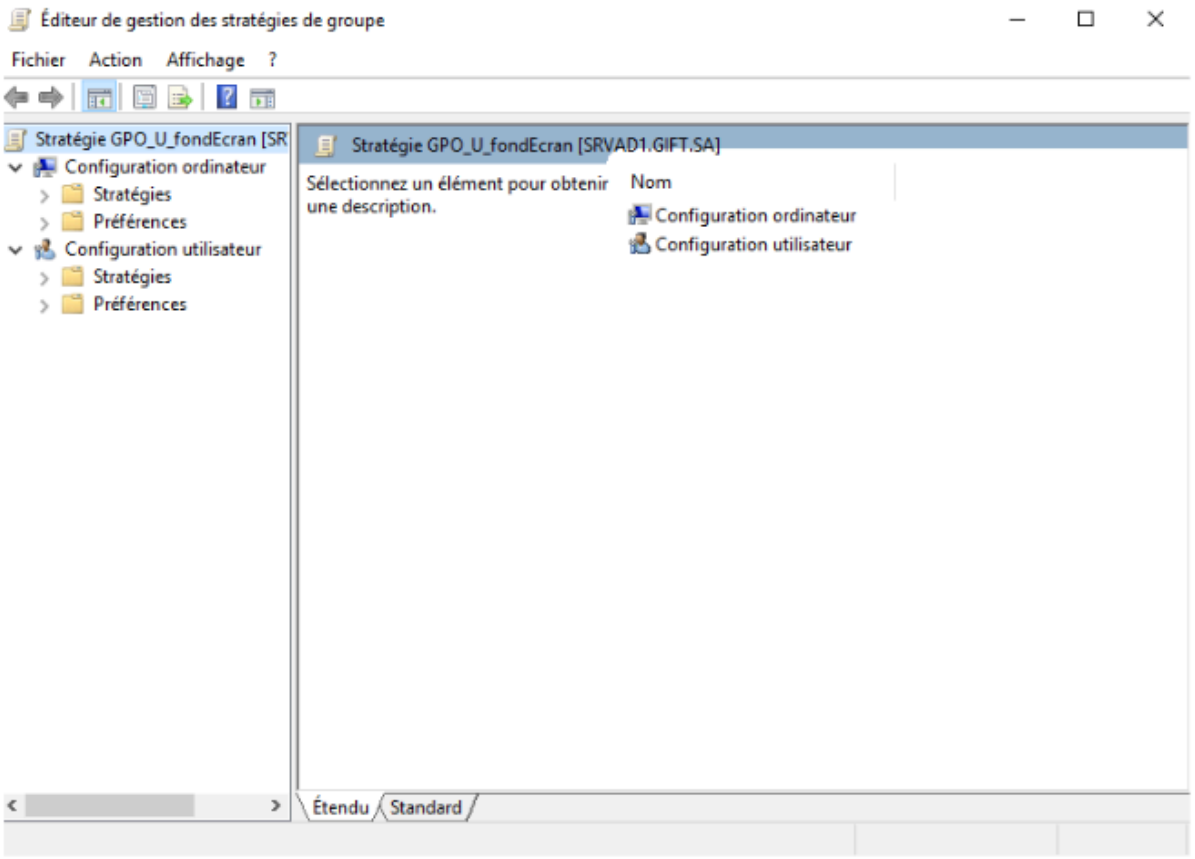


Nous allons le nommer GPO-U-FondEcran. Cela permet de savoir qu'il s'agit d'un objet GPO avec des paramètres utilisateur concernant le fond d'écran.

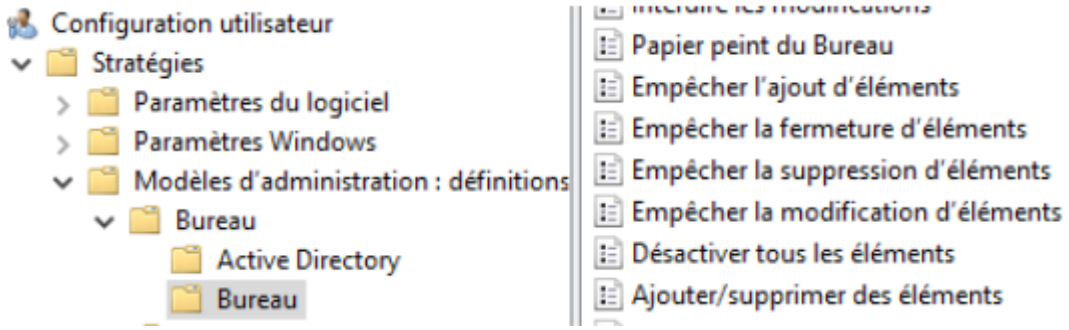


En effet, le lien sur le domaine fait apparaître l'objet GPO sous le nom du domaine, et cet objet se retrouve listé avec les autres objets GPO existants.

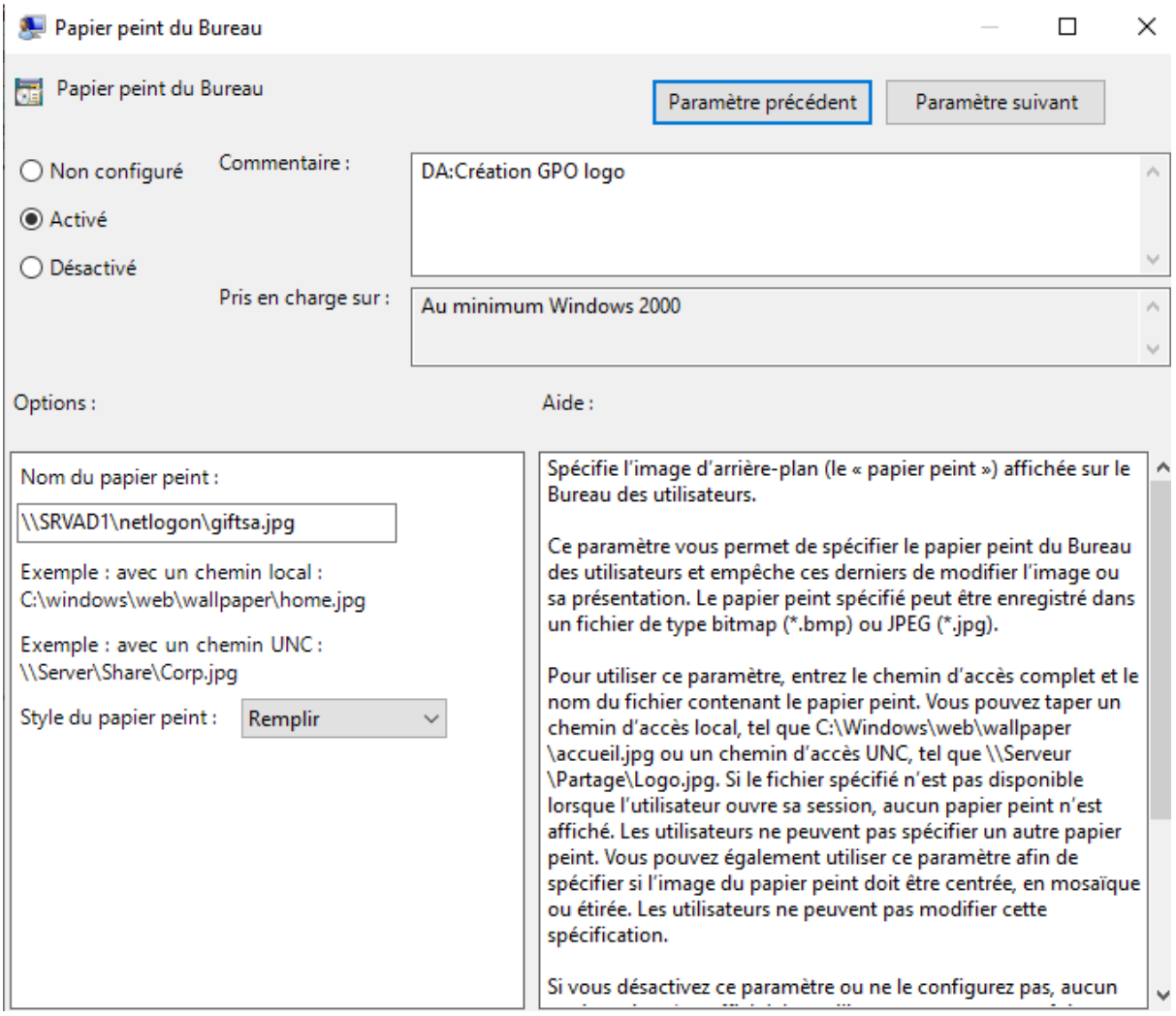
Faites un **clic gauche** sur le nom de votre GPO et sélectionnez **Modifier**. Vous arrivez dans la fenêtre de personnalisation de la GPO :



Rendez-vous dans la partie Configuration utilisateur, Stratégies, Modèle d'administration puis dans Bureau, et Bureau à nouveau :

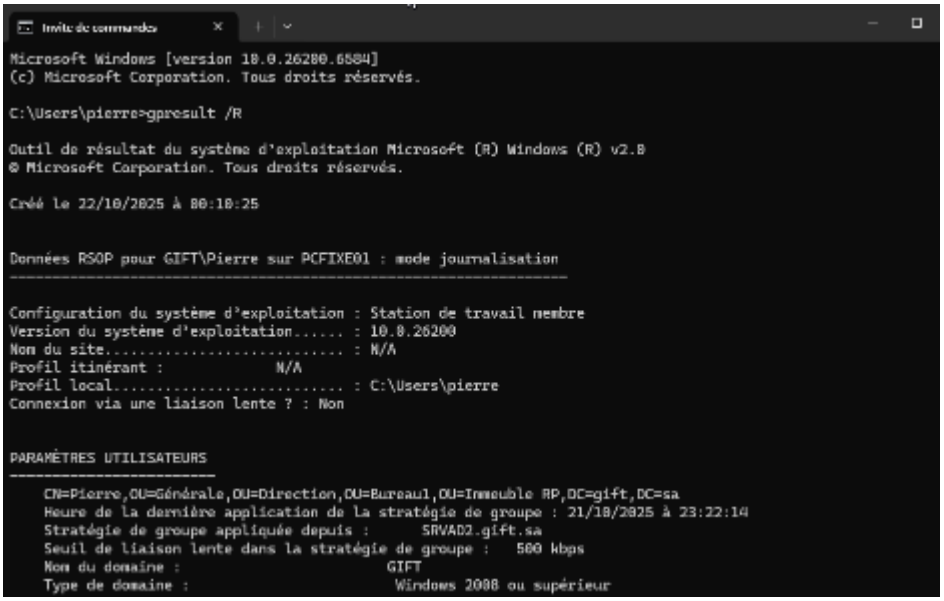


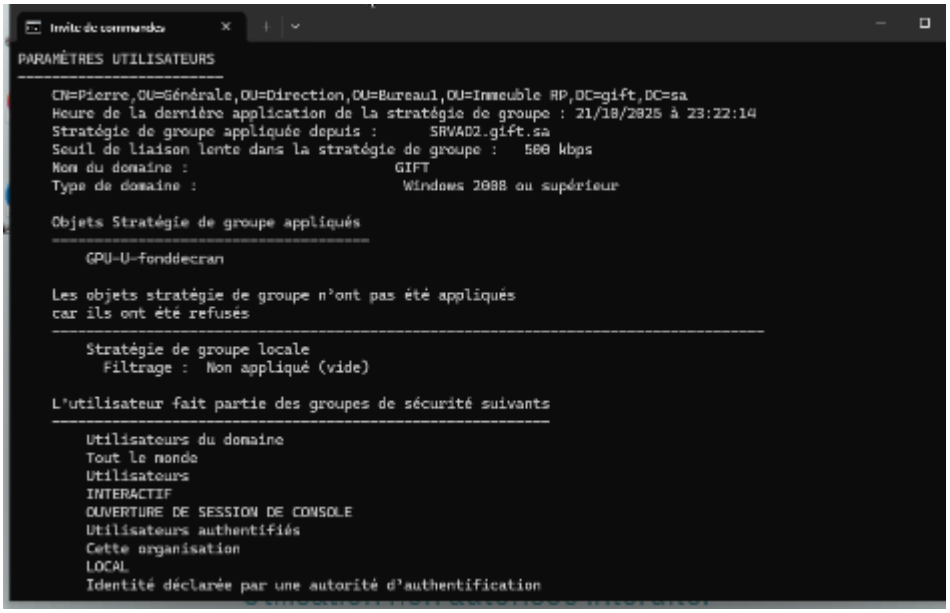
sur la partie de droite la liste des paramètres modifiables. Vous allez modifier le paramètre Papier peint du Bureau. Cliquez sur ce paramètre, et vous obtenez **la page de configuration**.



j'ai activé ce paramètre en cochant **Activé**, et de remplir les champs disponibles puis appliquer et cocher ok. Nous allons tester le fonctionnement sur notre client **PCFIXE01** en utilisant un compte utilisateur vous pouvez voir le résultat ci-dessous :

Nous pouvons aussi vérifier l'application de cette GPO avec la commande **gpresult**, permet d'afficher les informations sur l'application des stratégies à partir d'un poste et pour l'utilisateur courant.Par exemple, je suis connecté avec l'utilisateur Pierre sur le PCFIXE01. Voici le résultat de la commande avec le commutateur /R





Mise en place d’une politique de mot de passe affinée

Afin d’améliorer la sécurité des comptes utilisateurs au sein du domaine **GIFT.SA**, j’ai mis en place une politique de mot de passe affinée

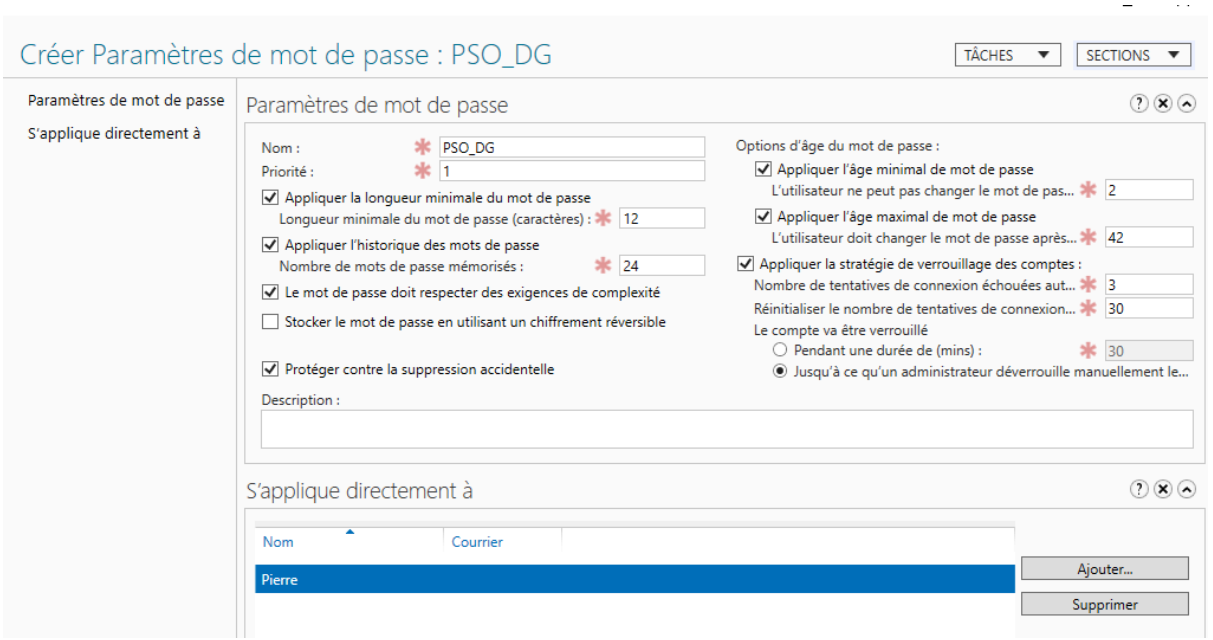
Contrairement à la stratégie de mot de passe classique qui s’applique à l’ensemble du domaine, cette fonctionnalité permet de définir des règles différentes selon les groupes d’utilisateurs.

J’ai créé une politique spécifique via la console **Active Directory Administrative Center**, en définissant notamment la longueur minimale du mot de passe à 12 caractères, l’obligation de complexité.

Cette politique a ensuite été liée à un compte de sécurité spécifique c’est celui du directeur général Pierre , afin d’imposer un niveau de sécurité plus élevé pour ce compte critique.

Cette configuration garantit une meilleure protection contre les attaques par force brute ou par dictionnaire, tout en laissant la possibilité d’appliquer des règles plus souples à d’autres catégories d’utilisateurs. Voici le lien d’IT-Connect pour la configuration : Mise en place d'une Politique de mot de passe

Au final, j'obtiens la configuration suivante :



Si vous désirez voir quelle stratégie s'applique à un utilisateur,avec PowerShell et le cmdlet "**Get-ADUserResultantPasswordPolicy**" puisqu'il suffit de préciser l'identifiant du user :

```
PS C:\Users\Administrateur> Get-ADUserResultantPasswordPolicy -Identity pierre


AppliesTo                   : {CN=Pierre,OU=Générale,OU=Direction,OU=Bureau1,OU=Immeuble RP,DC=gift,DC=sa}
ComplexityEnabled           : True
DistinguishedName           : CN=PSO_DG,CN=Password Settings Container,CN=System,DC=gift,DC=sa
LockoutDuration             : 00:00:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 3
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 2.00:00:00
MinPasswordLength           : 12
Name                        : PSO_DG
ObjectClass                 : msDS-PasswordSettings
ObjectGUID                  : 1c1184f3-05b1-481b-b9d5-d08c97b9e132
PasswordHistoryCount        : 24
Precedence                  : 1
ReversibleEncryptionEnabled : False
```

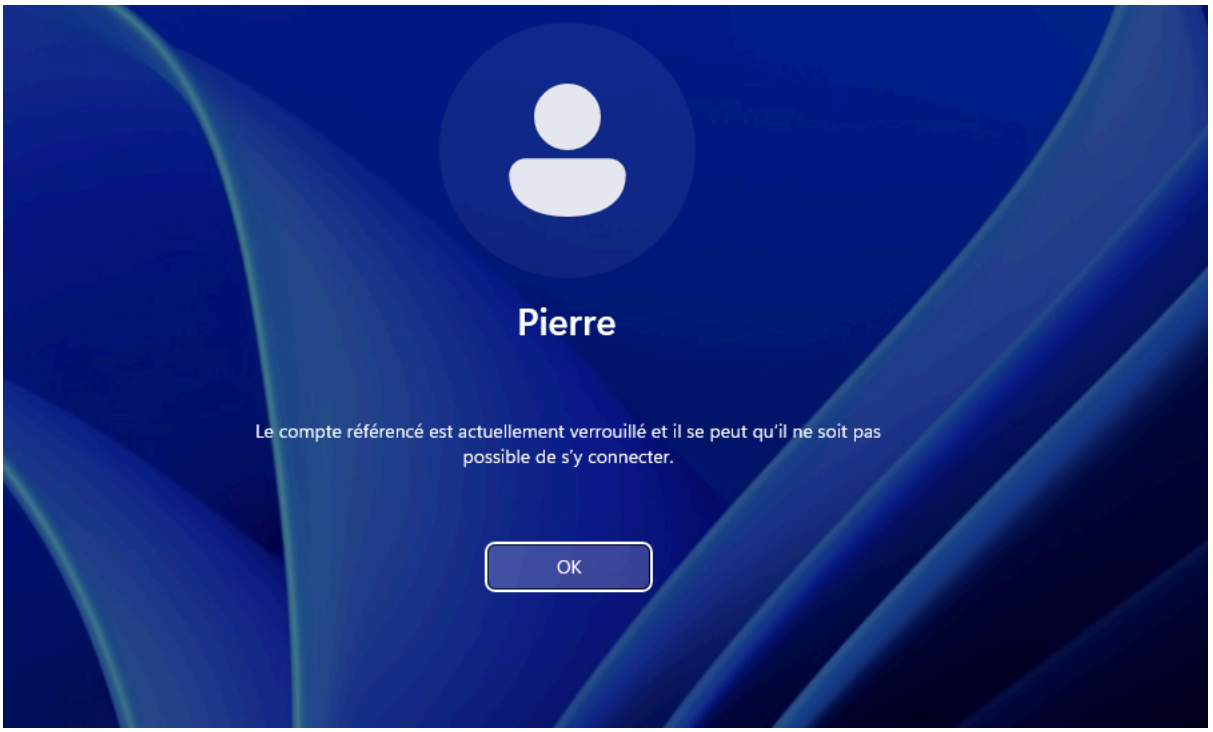
Vérification du fonctionnement de la politique de mot de passe affinée

Pour vérifier l'efficacité de la politique de mot de passe affinée mise en place, j'ai effectué un test pratique sur le compte utilisateur concerné (**pierre)**.

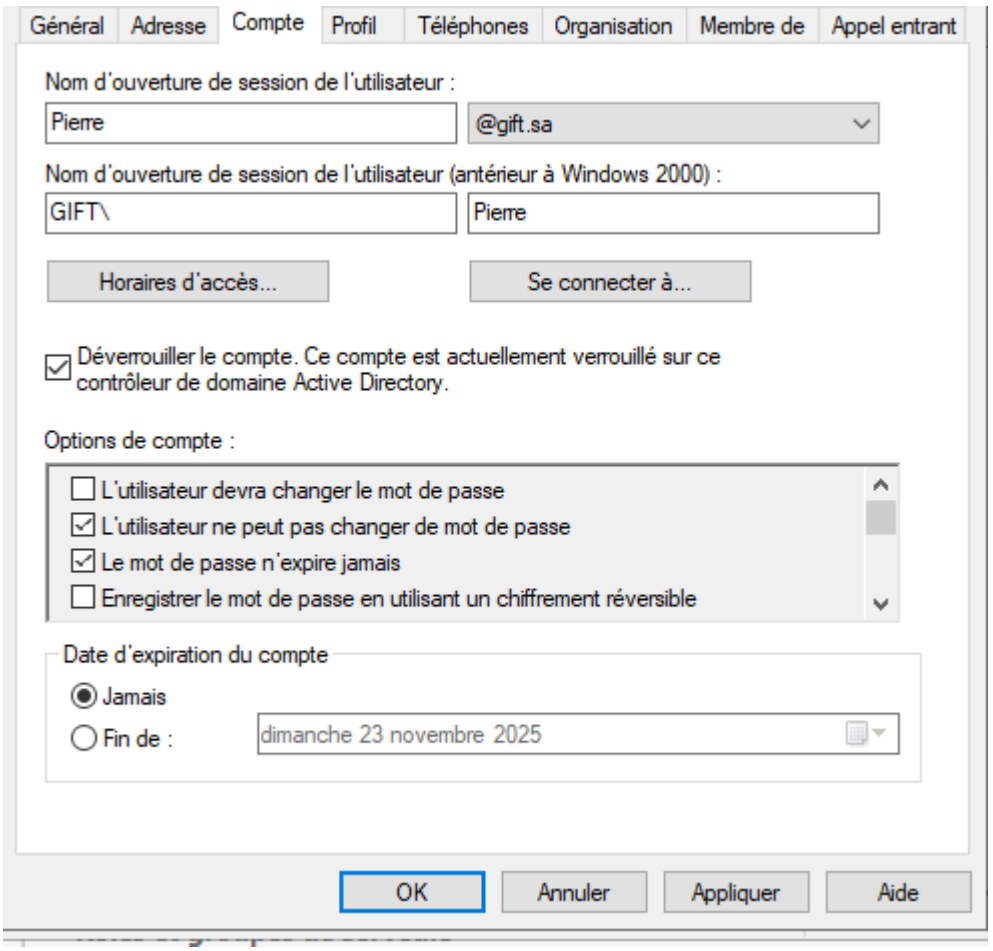
Lors de la saisie de **trois mots de passe incorrects consécutifs**, le compte a été **automatiquement verrouillé**, conformément aux paramètres de sécurité définis dans la stratégie (seuil de verrouillage configuré).

Ce comportement confirme que la politique est **correctement appliquée et opérationnelle**.

Le compte ne peut être utilisé à nouveau qu'après **déverrouillage manuel par un administrateur**, garantissant ainsi une **meilleure protection contre les tentatives d'accès non autorisées** ou les attaques par force brute. ci-dessous le message



Pour la déverrouiller il faut aller dans les propriétés du compte et cochez la case **déverrouiller le compte il est actuellement verrouillé sur ce contrôleur de domaine Active Directory** appliquer puis ok.



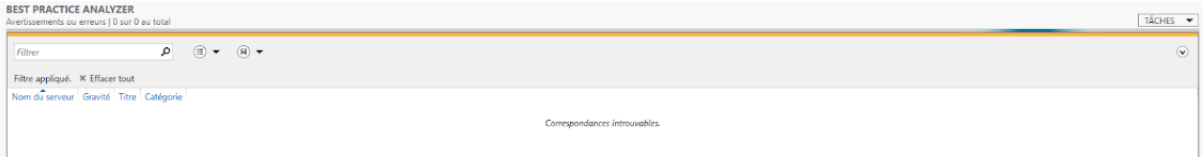
II- Analysons la sécurité de notre architecture

l'annuaire Active Directory se trouve au centre de la **sécurité d'un système d'information**. En règle générale, un domaine correctement sécurisé permet de s'assurer que le système d'information ne permet pas d'accéder aux données sensibles, ou même aux postes d'administration, trop simplement. Une gestion des droits trop permissive au sein de l'AD permettrait de prendre rapidement le contrôle d'un système d'information.

Utilisons l'outil d'analyse des bonnes pratiques Microsoft

Microsoft se soucie de son image et à ce titre, fournit des outils permettant de s'assurer de la bonne configuration de ses services ou logiciels. Au sein du gestionnaire de serveur, sous le rôle AD DS, Microsoft fournit un outil d'analyse des bonnes pratiques de configuration de tous les rôles qu'il propose.

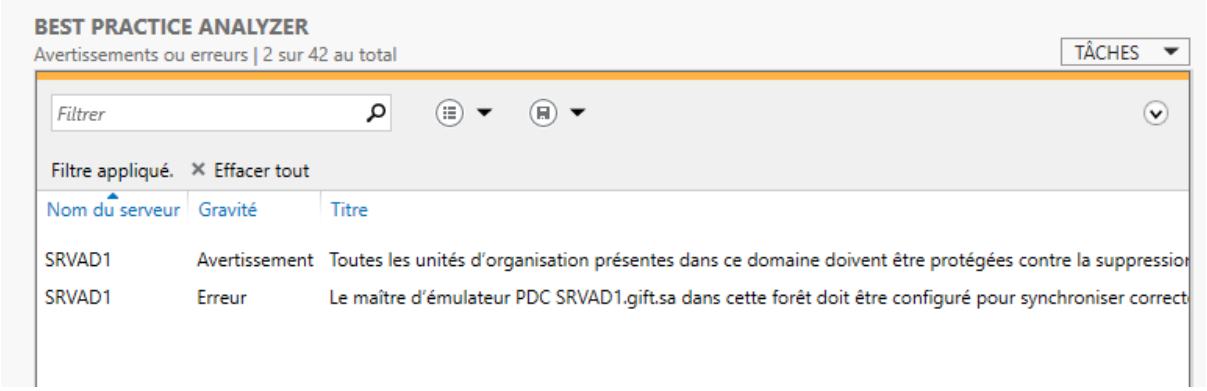
C’est notamment le cas du rôle AD DS. L’outil **Best Practice Analyzer (BPA)** se présente simplement par une zone dans le gestionnaire de serveur :



Analyseur des bonnes pratiques de configuration d’AD DS

Après Analyse nous avons deux Avertissements ou erreurs , le premier nous indique que tous les OU doivent être protégées contre la suppression accidentelle. En effet, l’unité organisationnelle *Domain Controllers* n’est pas **protégée contre la suppression accidentelle** . Après avoir protégé l’UO *Domain Controllers* contre la suppression, relancez l'analyse, cet avertissement disparaît .

voir ci-dessous les avertissements



Fiabilisation de l’architecture locale

La disponibilité de l’Active Directory est indispensable au bon fonctionnement du système d’information. Il en va de la capacité des utilisateurs à se connecter, du bon fonctionnement des services ou encore de l’accès aux partages de fichiers par exemple. Je vais utiliser deux techniques pour assurer la bonne accessibilité de ces services au sein de l’entreprise GIFT.SA. La première consiste à organiser les différents sites géographiques et la seconde à mettre en place un contrôleur de domaine en lecture seule (**RODC**).

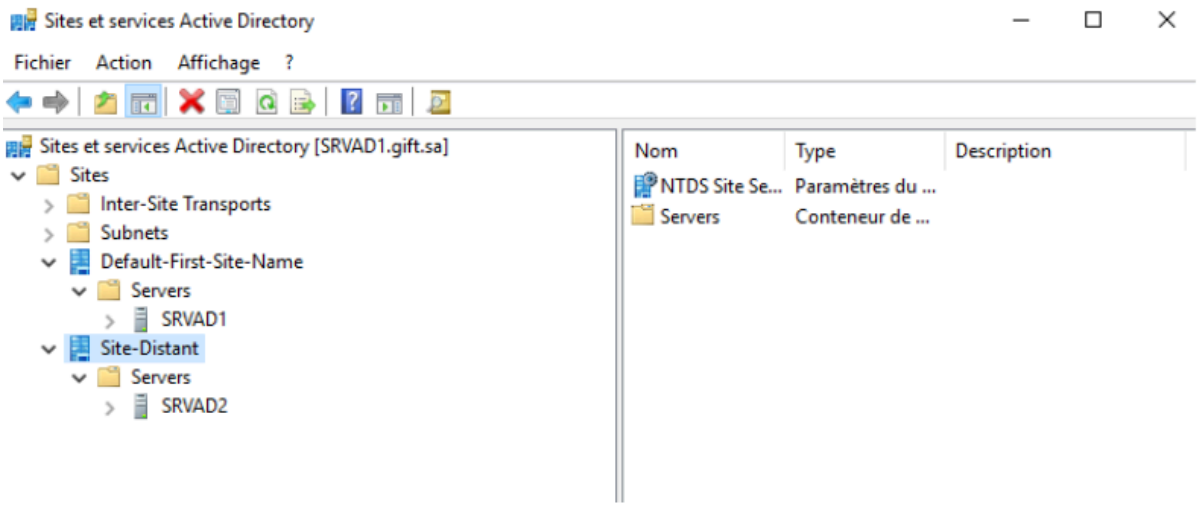
Organisation des différents sites géographiques

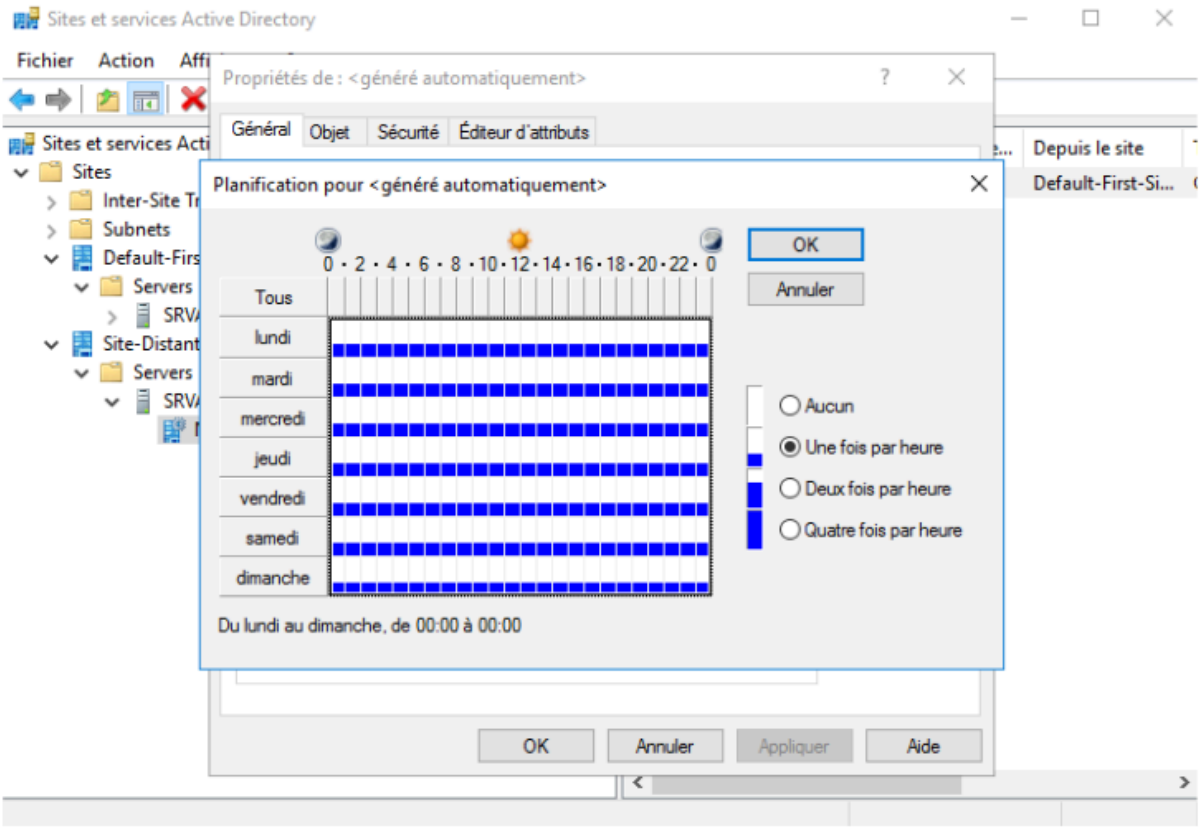
L’entreprise étant répartie sur plusieurs **sites géographiques distants**, il est essentiel d’assurer une **réplication efficace et maîtrisée** des données Active Directory entre ces sites.

Pour répondre à ce besoin, Microsoft propose la fonctionnalité **“Sites et services Active Directory”**, permettant de **distribuer les contrôleurs de domaine** selon la topologie réseau de l’entreprise.

J’ai donc créé **deux sites distincts**, chacun représentant un emplacement physique isolé du point de vue réseau, tout en maintenant un **routage inter-sites** pour garantir la communication entre eux.

Enfin, j’ai configuré un **calendrier de réplication** afin d’optimiser la synchronisation des données d’annuaire entre les contrôleurs de domaine, en limitant la consommation de bande passante tout en assurant la **cohérence des informations dans l’ensemble du domaine**. vous pouvez suivre ce lien pour [configuration-multi sites-sous-réseau]





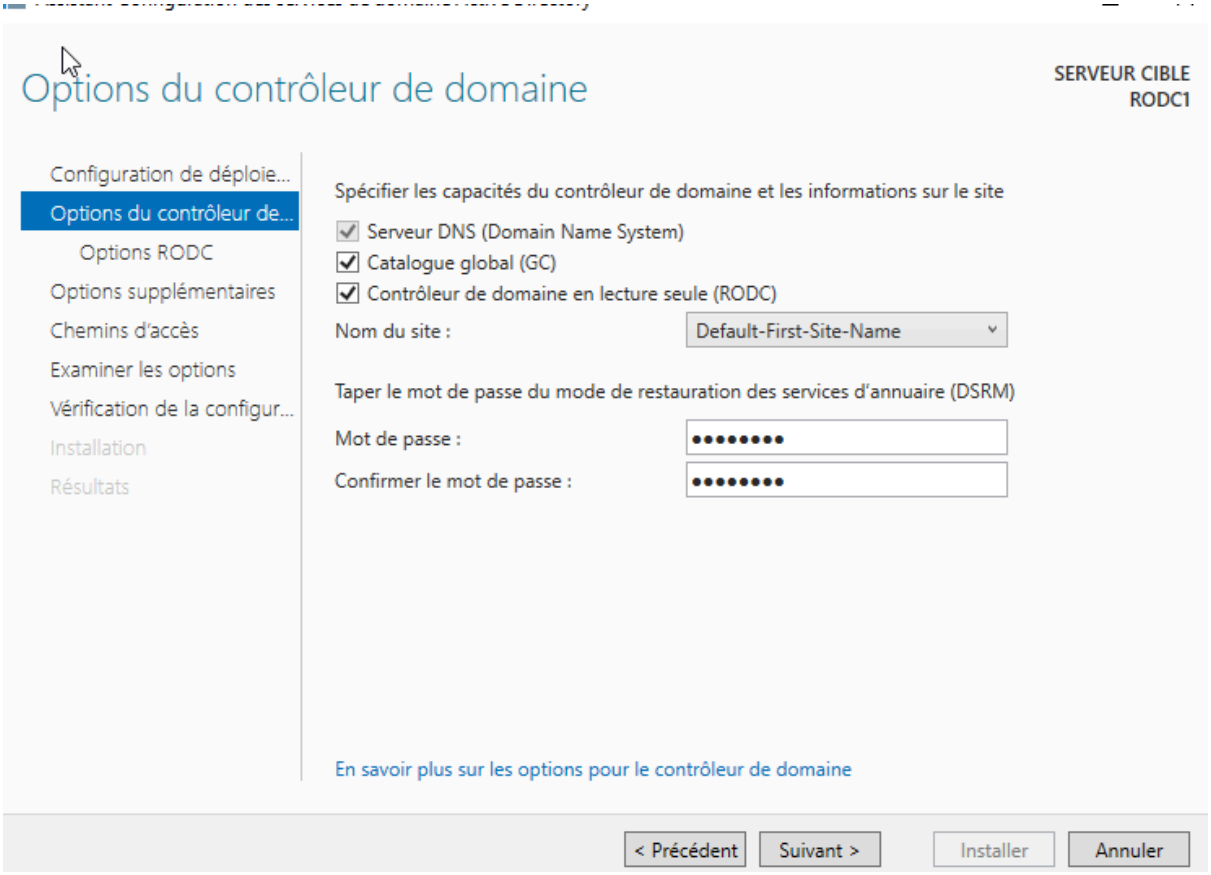
Mise en place d'un contrôleur de domaine en lecture seule (RODC)

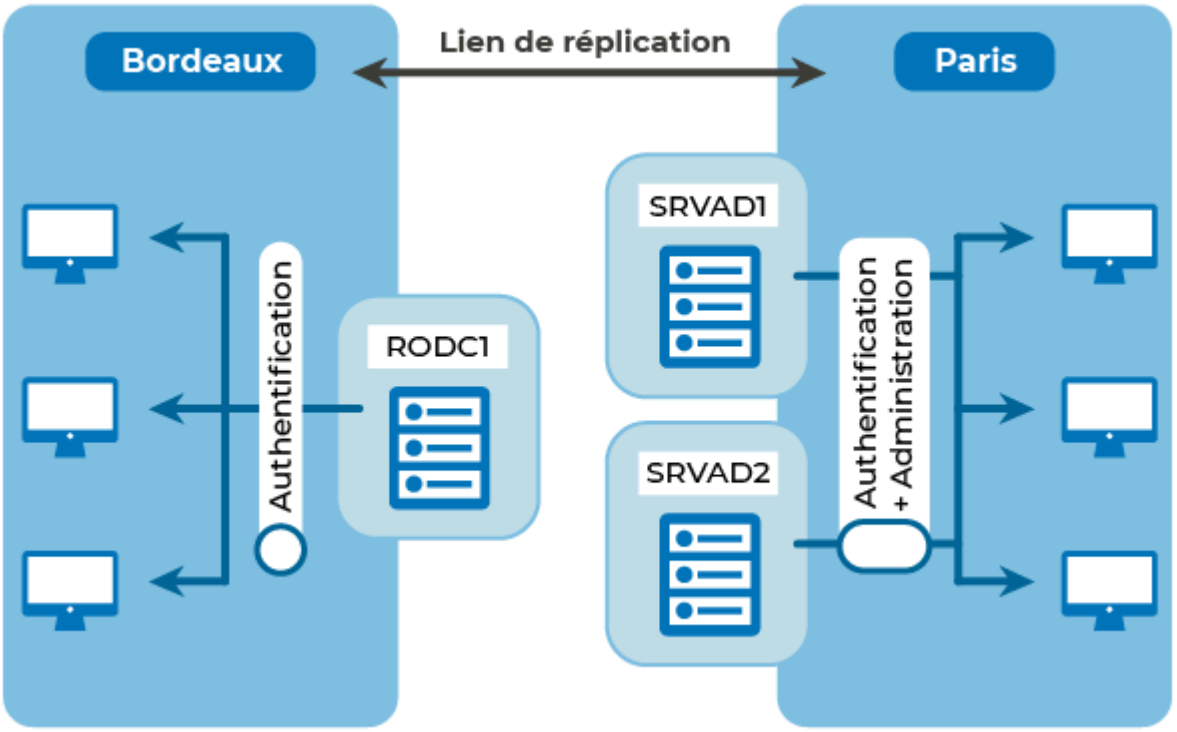
Dans le cadre du déploiement du domaine **GIFT.SA**, j'ai mis en place un **contrôleur de domaine en lecture seule (RODC)** destiné au **site distant de Bordeaux**.

Ce choix répond à un **objectif de sécurité** : dans les sites éloignés du siège principal, où les conditions de sécurité physique ou réseau peuvent être moins maîtrisées, le RODC permet de **limiter les risques d'attaques ou de compromission**.

Contrairement à un contrôleur de domaine classique, le RODC **ne stocke pas les informations sensibles d'authentification** (mots de passe) et ne permet pas de modifications directes de la base Active Directory.

Ainsi, même en cas de vol, de piratage ou de panne locale, les données critiques du domaine restent **protégées sur le site principal**, tout en assurant une **authentification rapide et fiable** pour les utilisateurs du site de Bordeaux.


Options du contrôleur de domaine
SERVEUR CIBLE
RODC1
Configuration de déploie...
Options du contrôleur de...
Options RODC
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier les capacités du contrôleur de domaine et les informations sur le site
Serveur DNS (Domain Name System)
Catalogue global (GC)
Contrôleur de domaine en lecture seule (RODC)
Nom du site :
Default-First-Site-Name
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
Mot de passe :
Confirmer le mot de passe :
En savoir plus sur les options pour le contrôleur de domaine
< Précédent
Suivant >
Installer
Annuler



Configuration d’un domaine sur plusieurs sites avec un RODC

III-Sécuriser le parc informatique grâce à Active Directory

La sécurité du système d’information est un enjeu majeur pour toute entreprise. Afin de renforcer la protection du domaine **GIFT.SA**, j’ai choisi de mettre en place trois actions clés : **auditer et restreindre les accès entrants** afin d’identifier les tentatives de connexion infructueuses, le **filtrage des flux réseau** pour limiter les accès non autorisés, et la **restriction de l’exécution des logicielles non autorisées**.

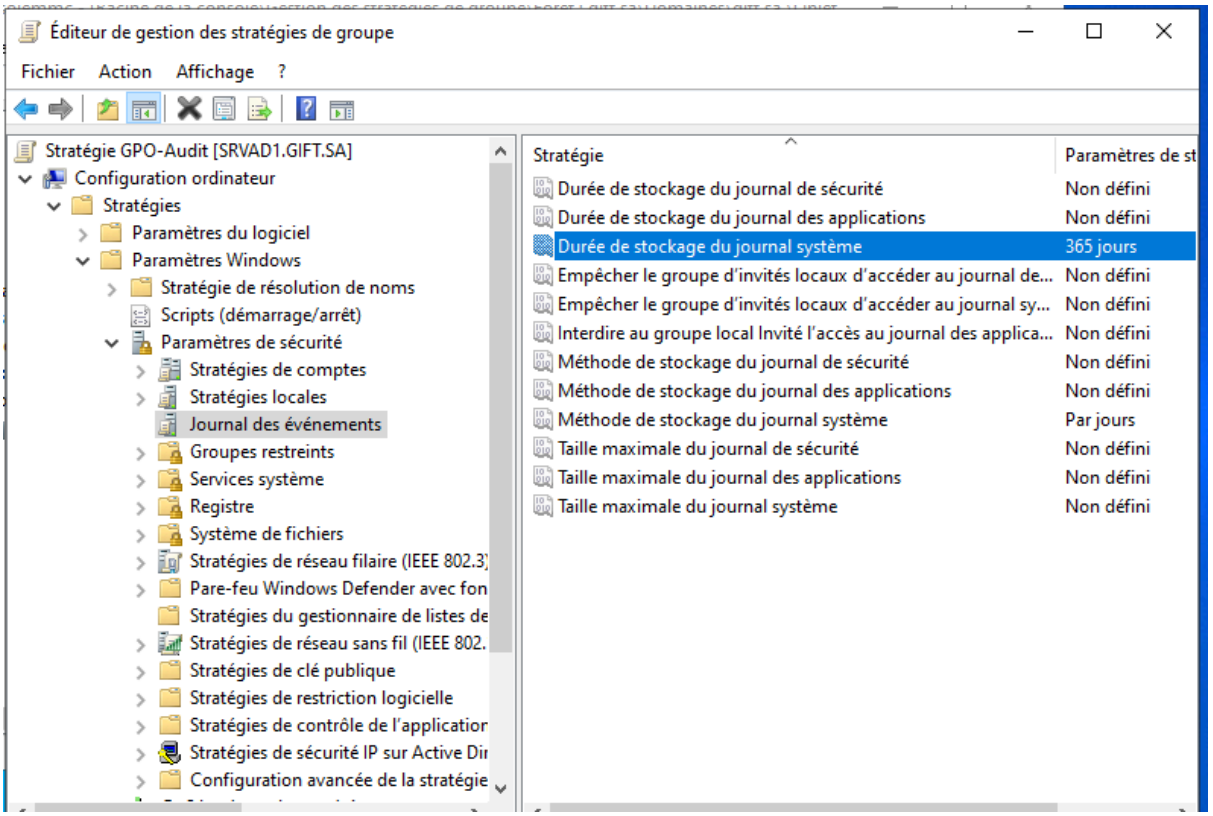
Ces mesures visent à **améliorer la fiabilité, la cohérence et la sécurité** de l’infrastructure Active Directory.

a)Audit et restriction des accès entrants

Afin de renforcer la sécurité, d'assurer la conformité et de permettre la détection de comportements anormaux, une stratégie d'audit a été initiée pour surveiller,

enregistrer et analyser les interactions avec les objets et les ressources du domaine (utilisateurs, groupes, fichiers, etc.).

Dans le cadre du renforcement de la traçabilité des accès au sein de l'Active Directory, une **Stratégie de Groupe (GPO)**, nommée **GPO-Audit**, a été créée et configurée spécifiquement pour activer la journalisation des événements d'audit, permettant ainsi à Active Directory de répertorier tous les accès aux objets, qu'ils soient initiés par des postes appartenant au domaine ou par des postes externes (hors domaine). Simultanément, pour garantir une rétention suffisante des informations pour l'analyse de sécurité et la conformité à long terme, la durée de stockage du **journal système** a été définie et paramétrée à **365 jours**.



Restriction des Options de Connexion (Accès Réseau)

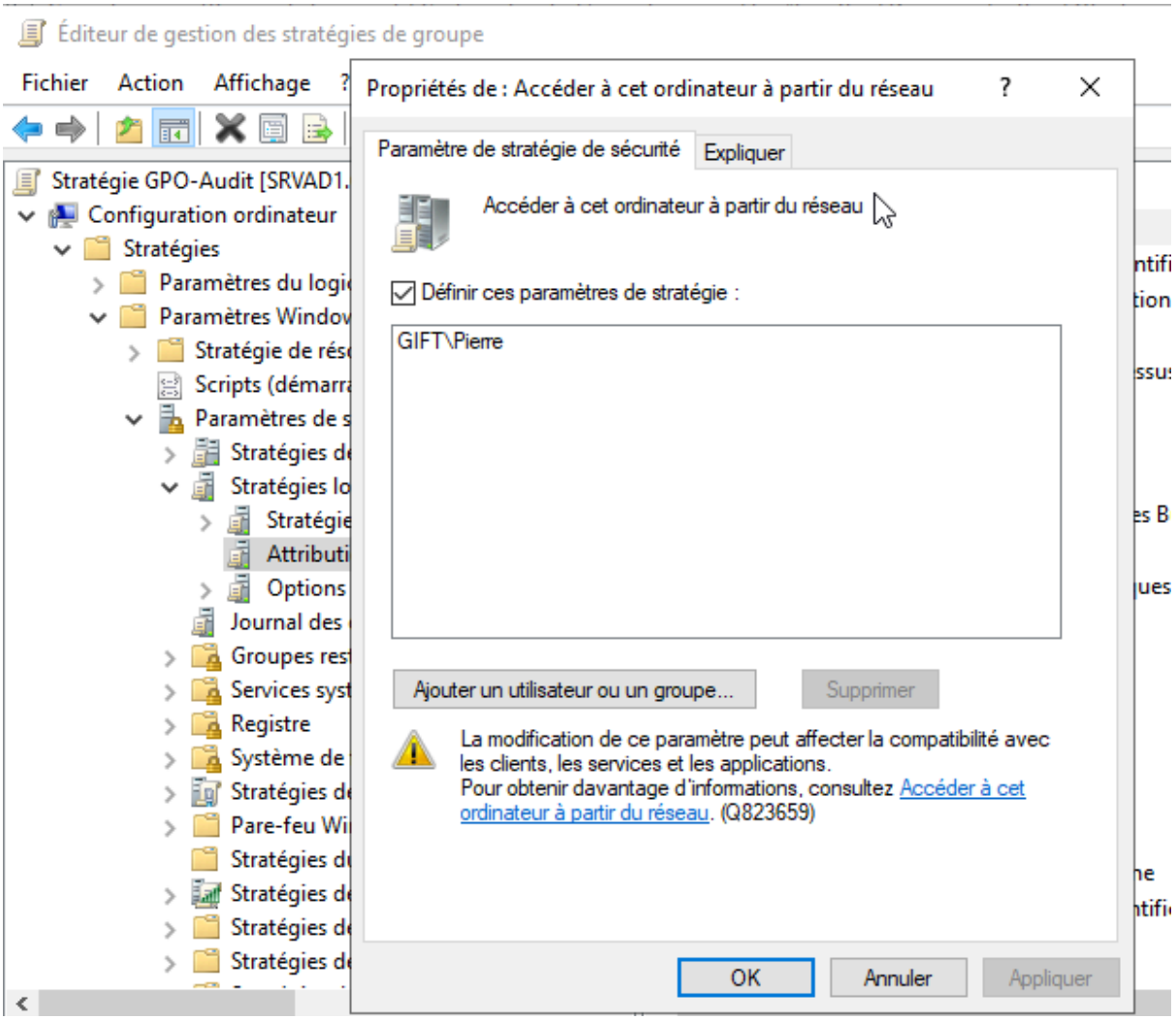
Parallèlement à l'audit, des mesures spécifiques ont été prises pour restreindre les connexions réseau, limitant ainsi l'accès aux ressources sur un poste ciblé.

Configuration de la Restriction d'Accès

- **Niveau d'application :** La restriction a été appliquée via les **Stratégies Locales** du poste cible.
- **Droit utilisateur ciblé :** La modification a porté sur l'attribution du droit utilisateur **"Accéder à cet ordinateur à partir du réseau"** (*Access this computer from the network*).
- **Mise en place :** La politique a été définie pour n'autoriser que des utilisateurs spécifiques.

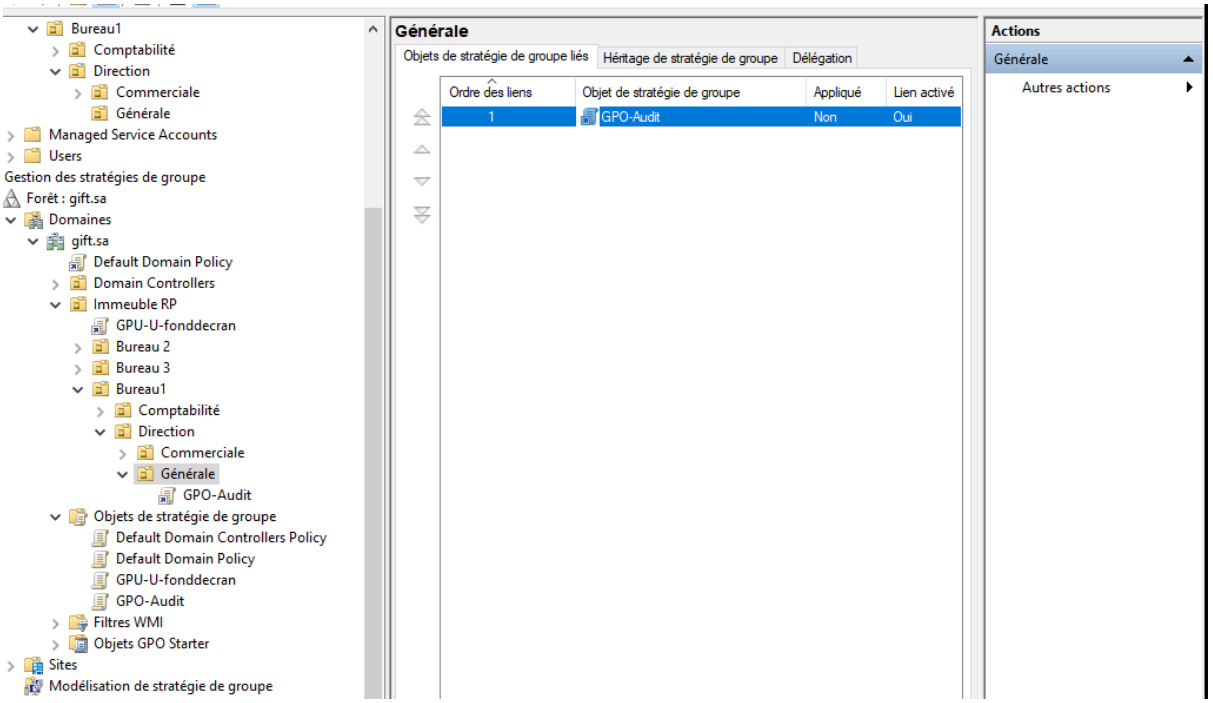
Attribution des Droits

- **Utilisateur désigné :** L'utilisateur **"Pierre" (Directeur Général)** a été explicitement ajouté à cette politique, restreignant de fait l'accès réseau à cet ordinateur aux seuls comptes autorisés, incluant celui du Directeur Général.



Déploiement de la Stratégie de Groupe

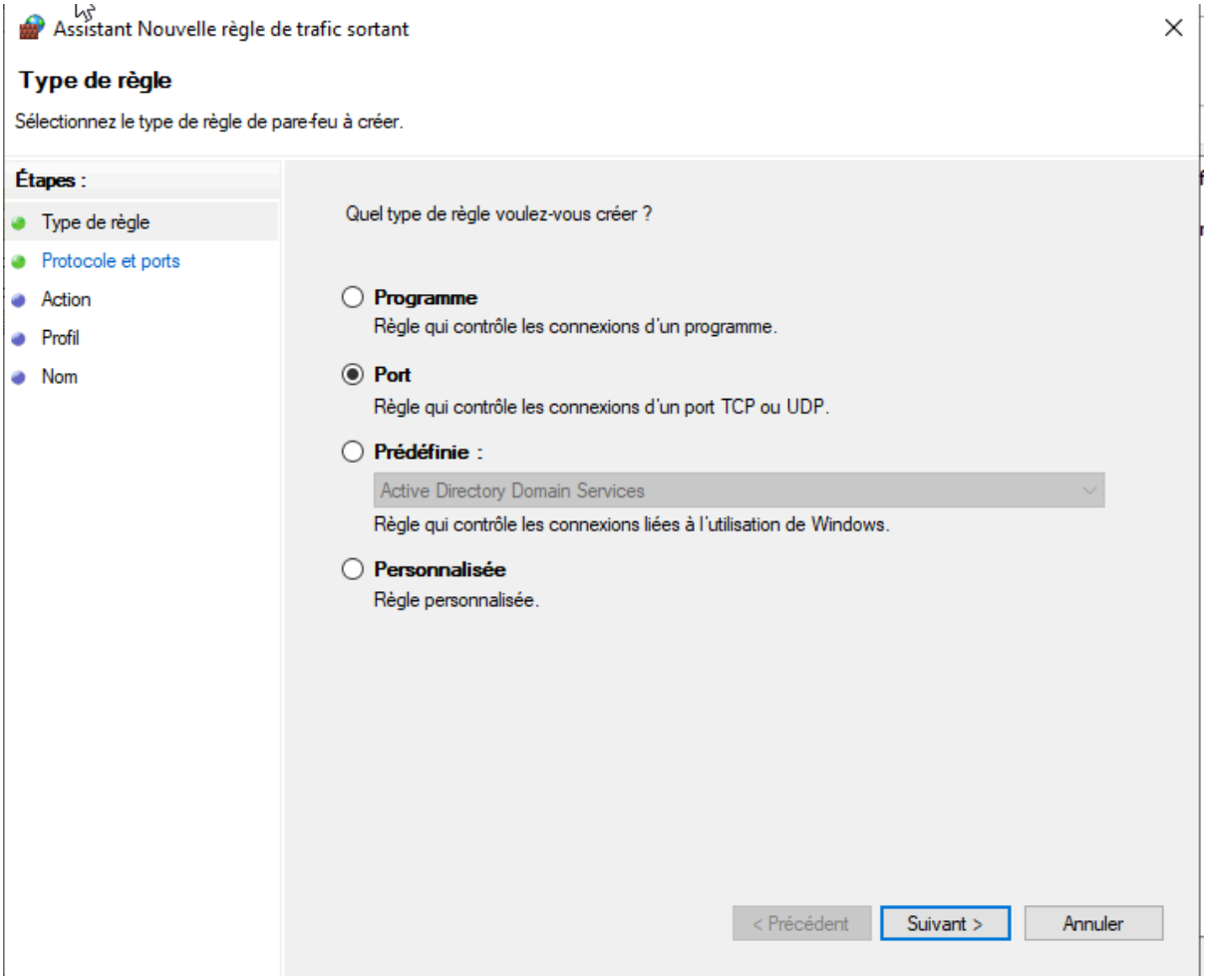
- **Liaison de la GPO :** La **Stratégie de Groupe (GPO)** configurée (GPO de restriction/attribution des droits) a été liée à l'**Unité d'Organisation (OU)** nommée **Direction**, garantissant que les paramètres de restriction des accès s'appliquent correctement aux utilisateurs et/ou ordinateurs membres de cette unité.



b) Filtrage des flux réseau

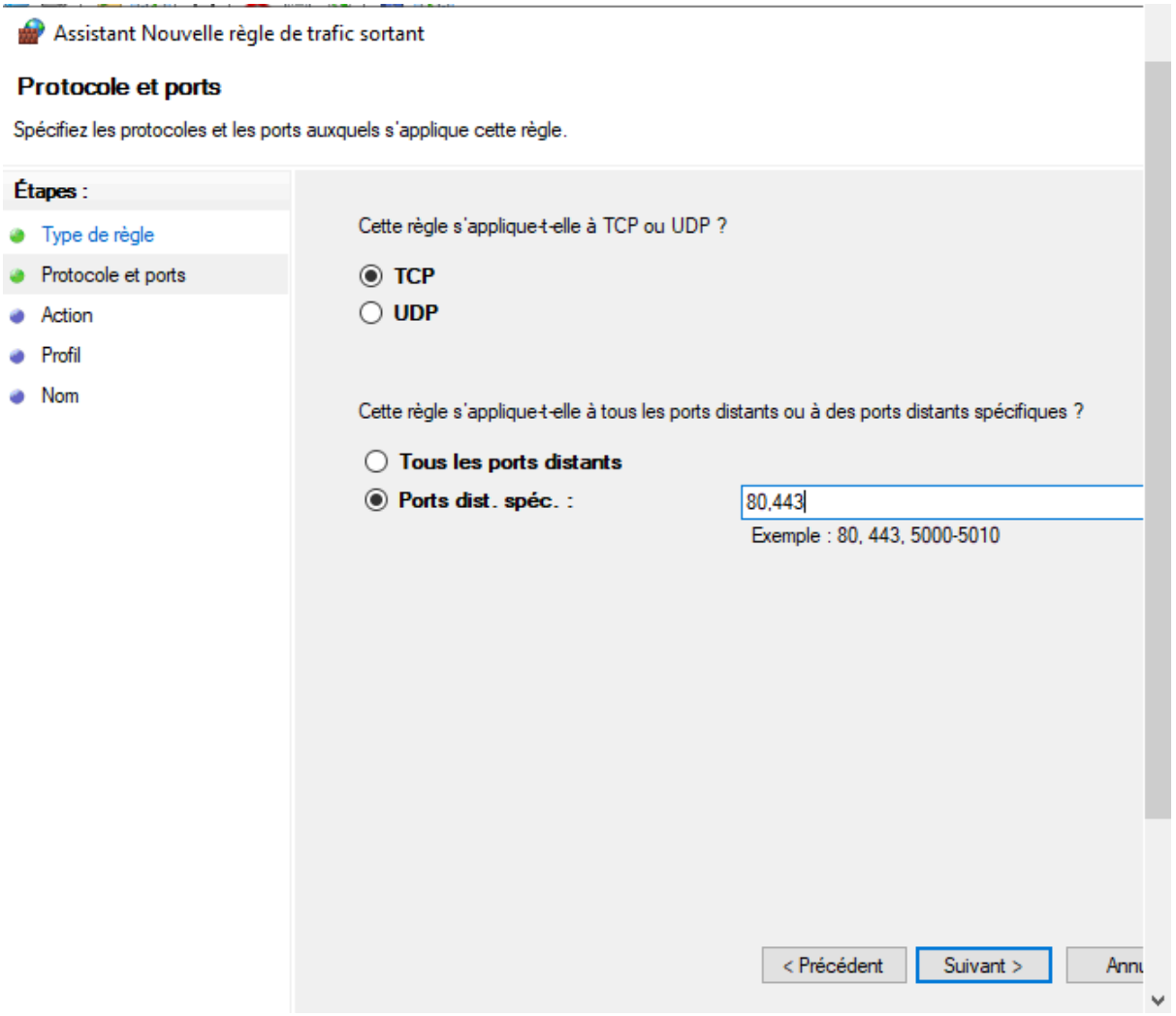
Afin de renforcer la sécurité du réseau interne, un filtrage des flux a été mis en place pour contrôler les communications sortantes et limiter les accès non nécessaires à Internet. Cette mesure vise à réduire la surface d’exposition du parc informatique tout en assurant un meilleur contrôle des connexions établies par les postes et serveurs.

l’objectif est de bloquer l'accès internet aux utilisateurs donc je vais bloquer les ports spécifiés au trafic web , cocher port puis suivant

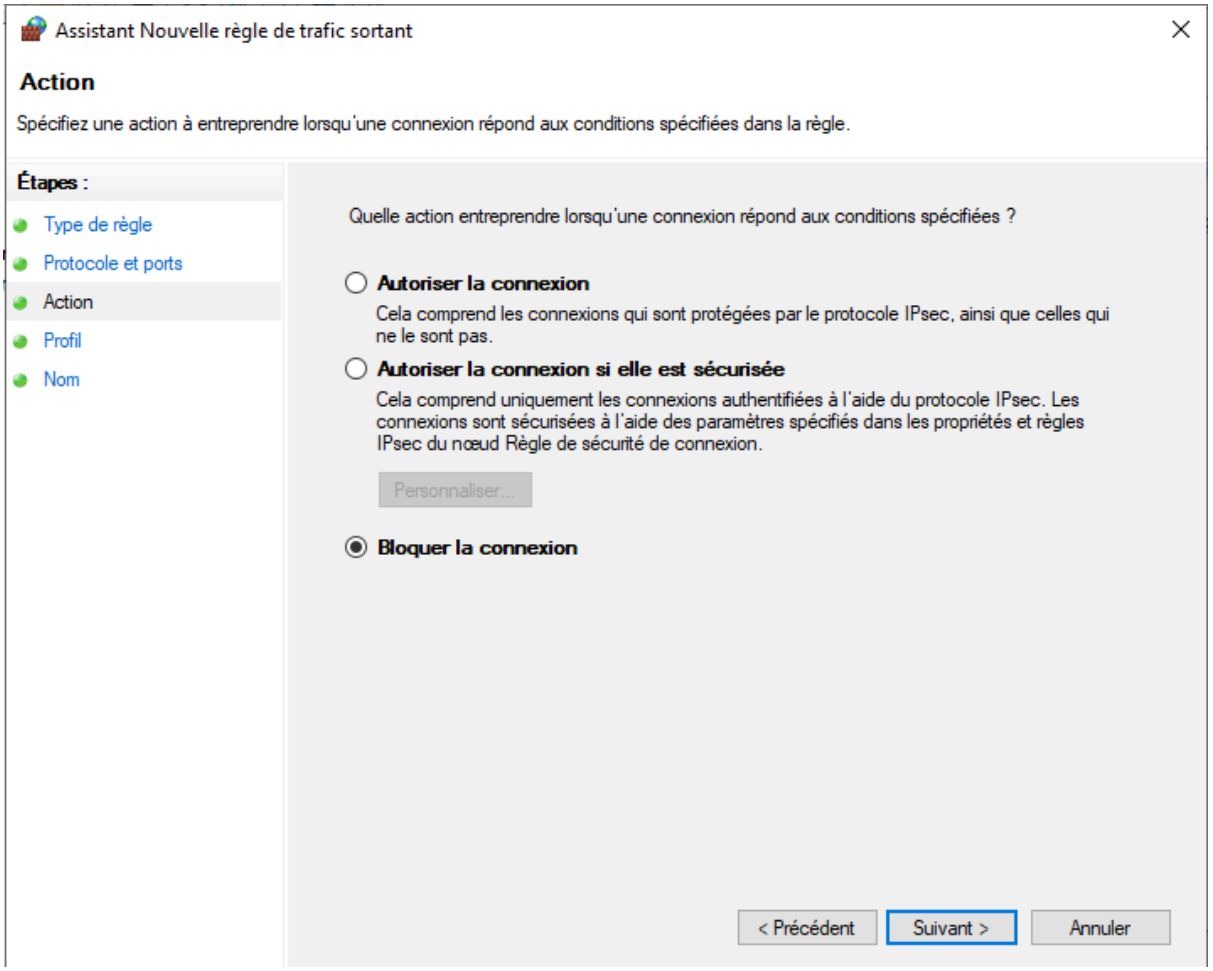


Spécifier le protocole ici TCP et le ou les ports correspondant ici les ports (80,443)

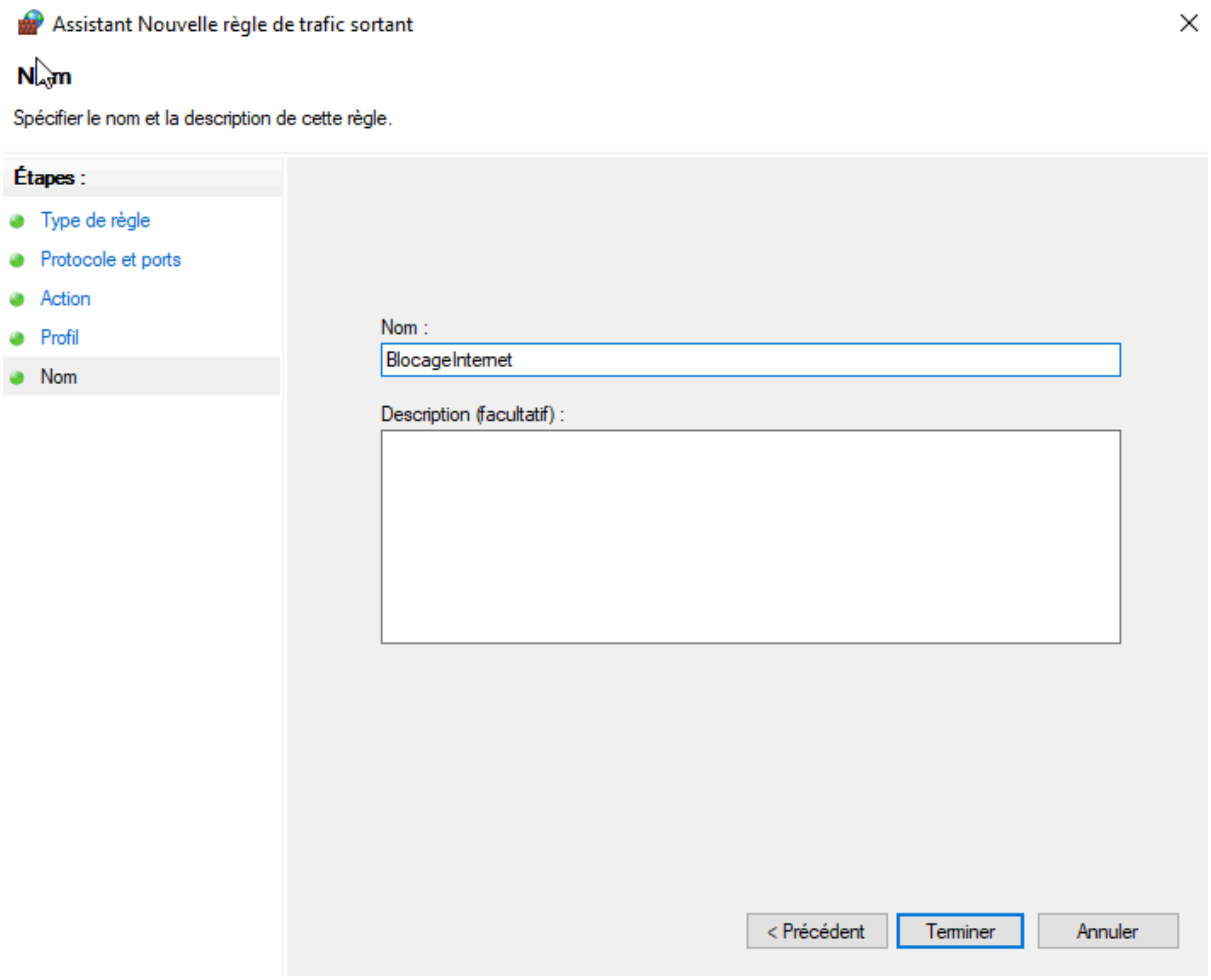
faire suivant ,

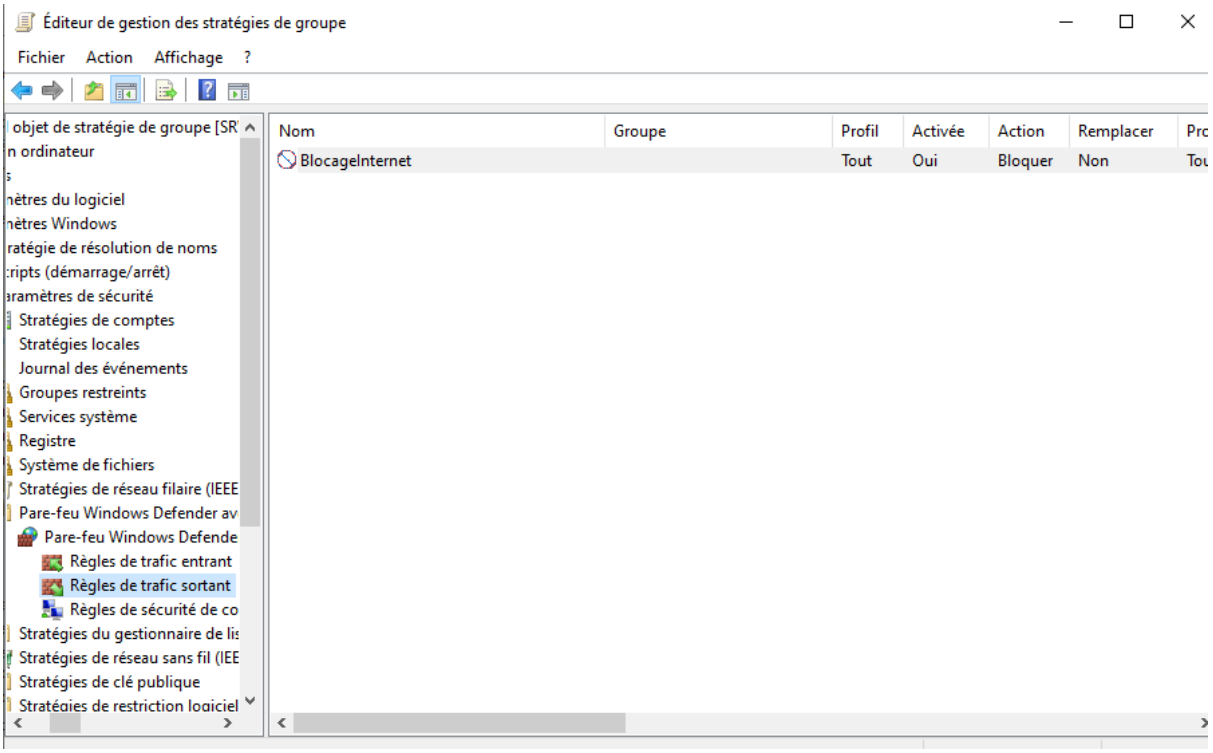


ensuite cocher bloquer la connexion

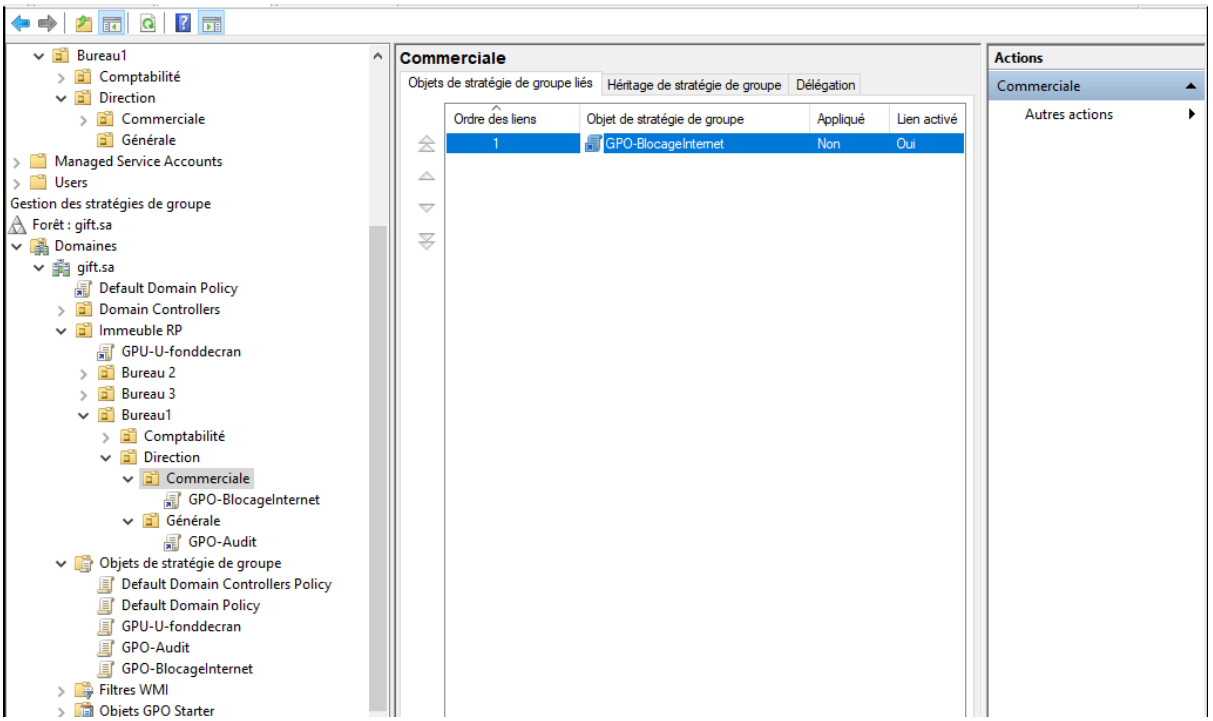


Nommé la règle et terminer


Assistant Nouvelle règle de trafic sortant
Nom
Spécifier le nom et la description de cette règle.
Étapes :
Type de règle
Protocole et ports
Action
Profil
Nom
Nom :
BlocageInternet
Description (facultatif) :
< Précédent
Terminer
Annuler

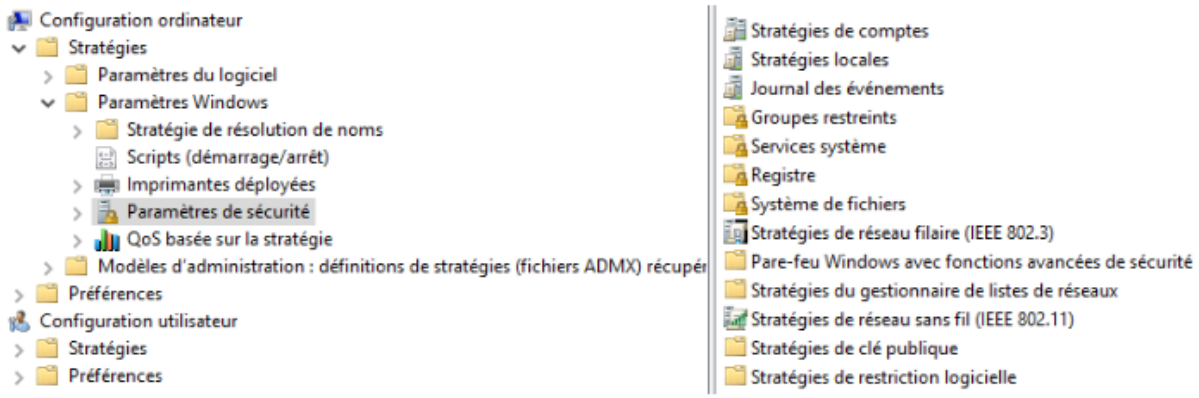


Après avoir créé la GPO je l'ai déplacé vers l'OU Direction , Commerciale

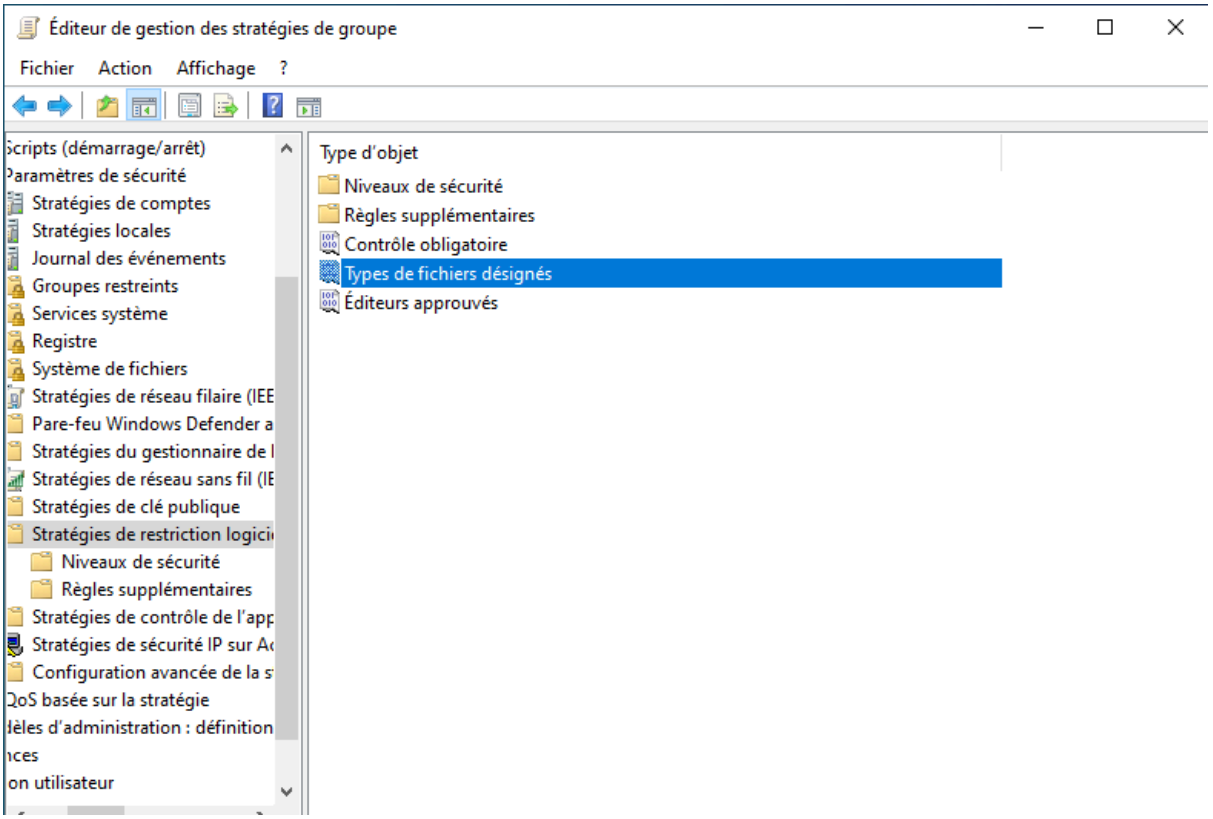


c) restriction de l’exécution de logicielles non autorisées

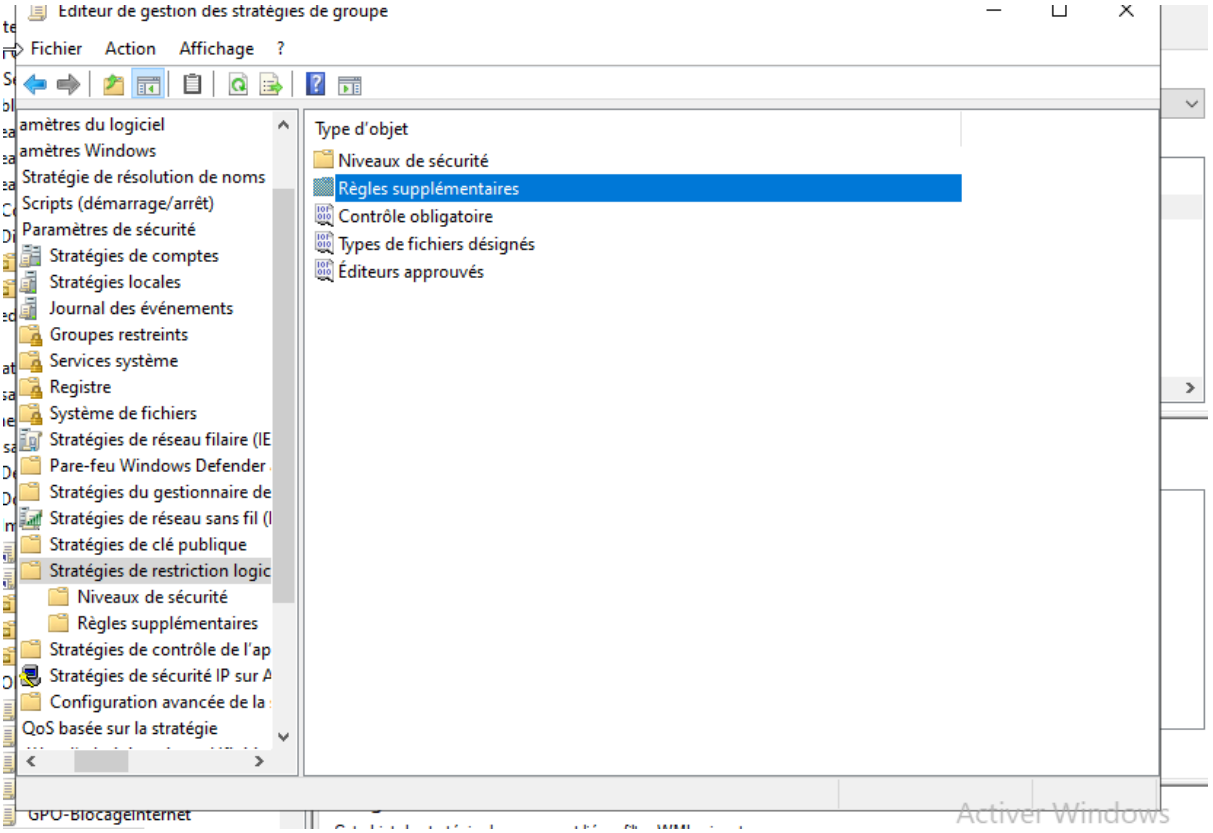
Il est possible de mettre en œuvre simplement une **stratégie de restriction logicielle**, appelée **SRP**, via les GPO. Pour cela il vous faut créer une GPO, et vous rendre dans la partie **Configuration ordinateur**, puis **Paramètres de sécurité**, comme ceci :



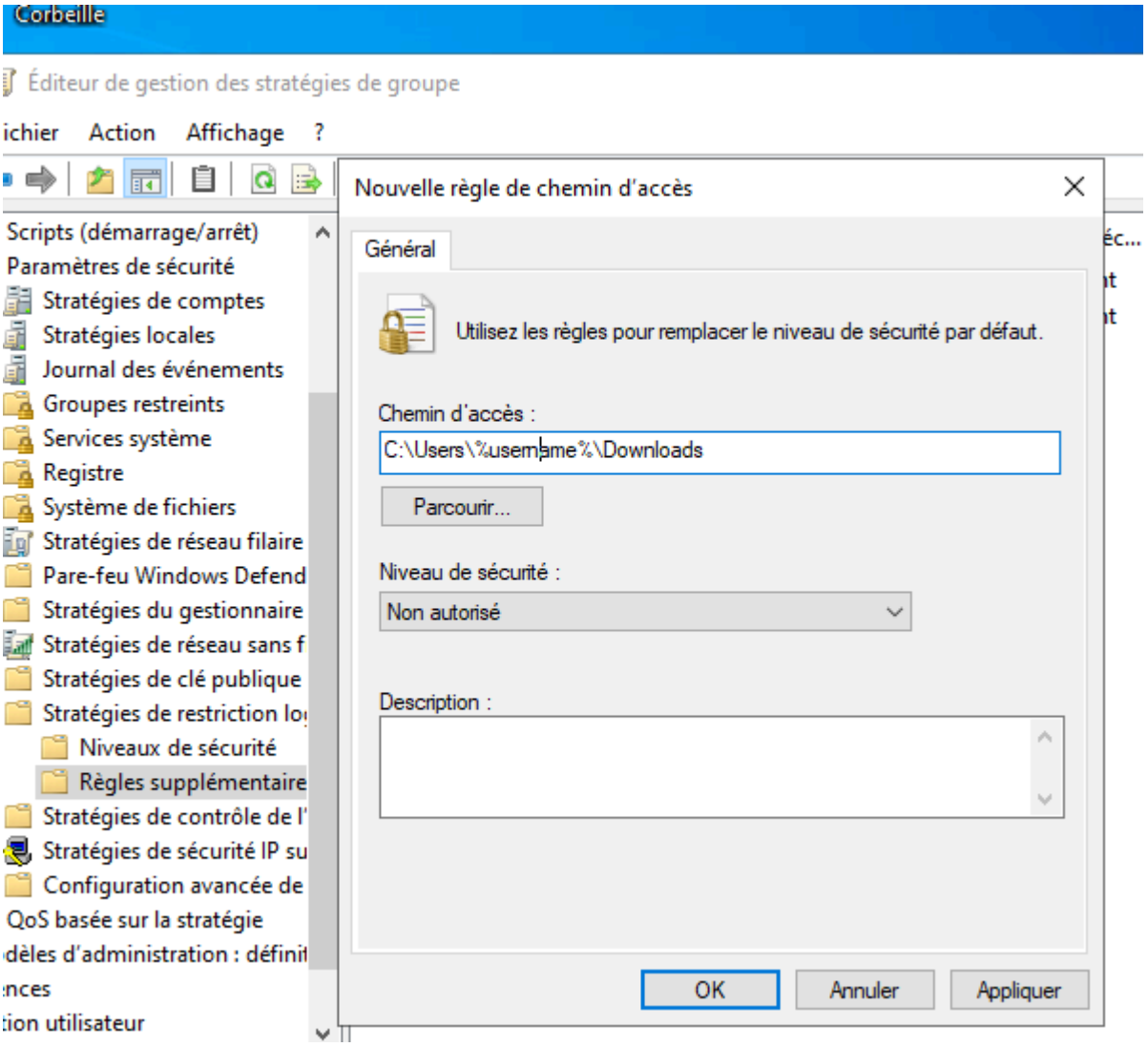
effectuez un clic droit sur le dossier Stratégies de restriction logicielle puis désignez le type de fichiers j’ai choisi les fichiers EXE et MSI



Après avoir défini les fichiers j'ai défini l'emplacement où est interdit l'exécution au niveau de règles supplémentaires voir ci-dessous



puis spécifié le chemin



VI-Sauvegarde de la base de données

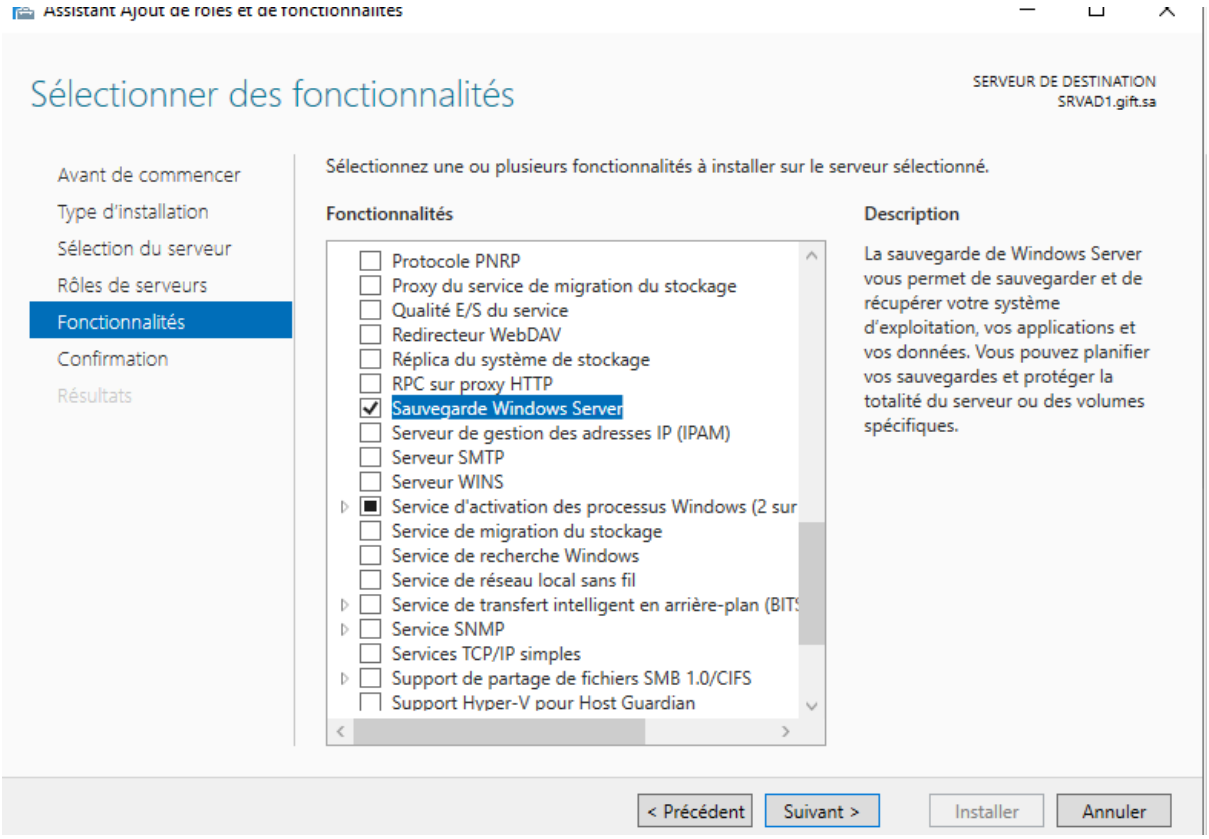
Active Directory est, comme nous l'avons vu précédemment, une véritable base de données. Son emplacement a été défini lors de la promotion du serveur en contrôleur de domaine.

Comme toute base de données essentielle au fonctionnement du système d'information, il est indispensable de la sauvegarder correctement afin de garantir la restauration du service en cas d'incident.

Pour cela, Microsoft fournit un outil dédié : Sauvegarde Windows Server.
Cet utilitaire peut être utilisé de deux manières : soit graphiquement via le Gestionnaire de serveur, soit en ligne de commande pour des sauvegardes automatisées et planifiées.

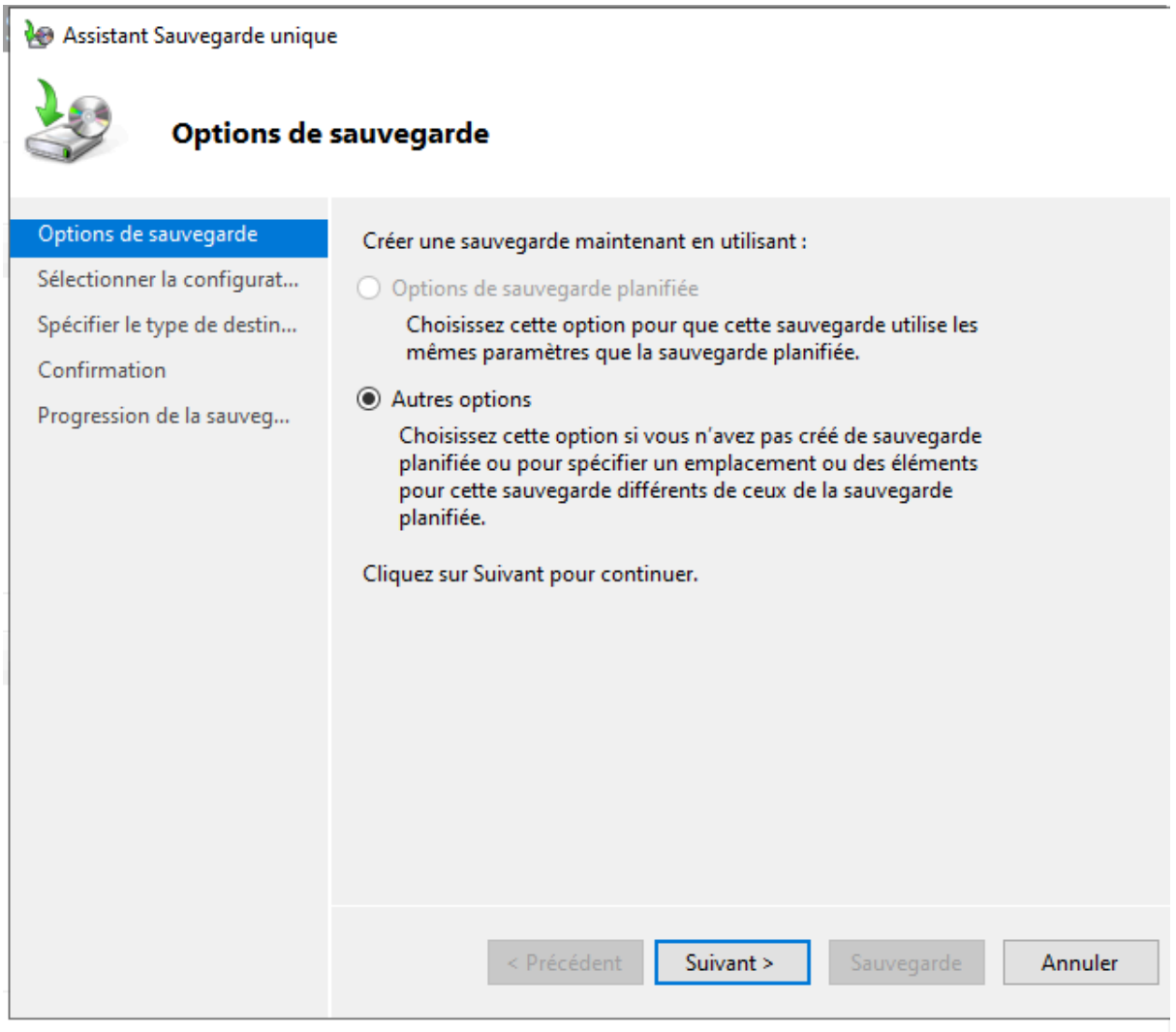
Voici les différentes étapes pour installer l'outil (et donc la fonctionnalité) :

- ouvrez le **Gestionnaire de serveur** et cliquez sur **Ajouter des rôles et fonctionnalités** ;
- sur l'assistant, **Ajouter des rôles et fonctionnalités** puis cliquez sur **Suivant** ;
- laissez la valeur par défaut : **Installation basée sur un rôle ou une fonctionnalité**, et cliquez sur **Suivant** ;
- **sélectionnez votre serveur** et cliquez sur **Suivant** ;
- sur l'écran des rôles, cliquez sur **Suivant** ;
- sur l'écran des fonctionnalités, sélectionnez **Sauvegarde de Windows Server** et cliquez sur **Suivant** ;

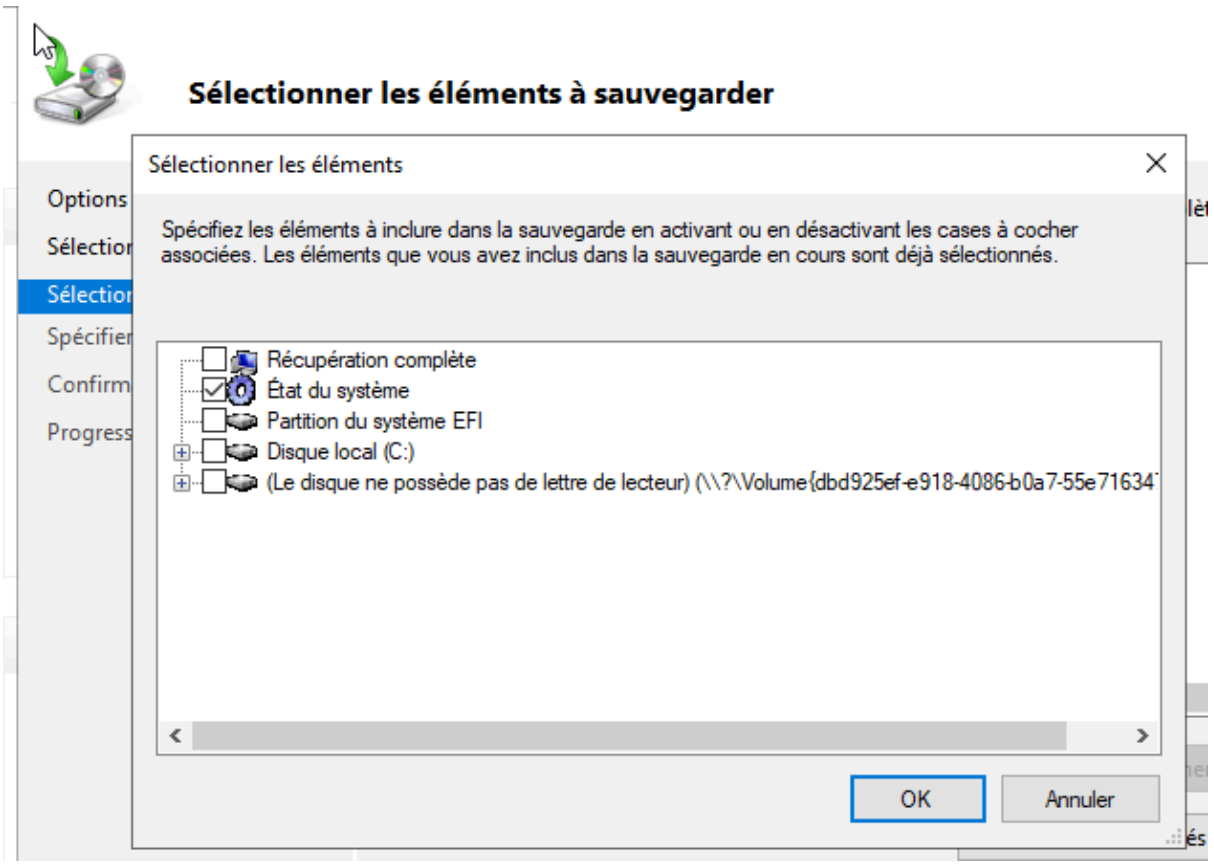


- cliquez sur **Installer** ;
- une fois l'installation terminée, cliquez sur **Fermer**.

- lancez l'outil ;
- cliquez sur **Sauvegarde locale** (si ce n’est pas déjà sélectionné) ;
- sur le menu Action, cliquez sur **Sauvegarde unique** ;
- dans Assistant sauvegarde unique, cliquez sur **Différentes options**, puis cliquez sur **Suivant** ;

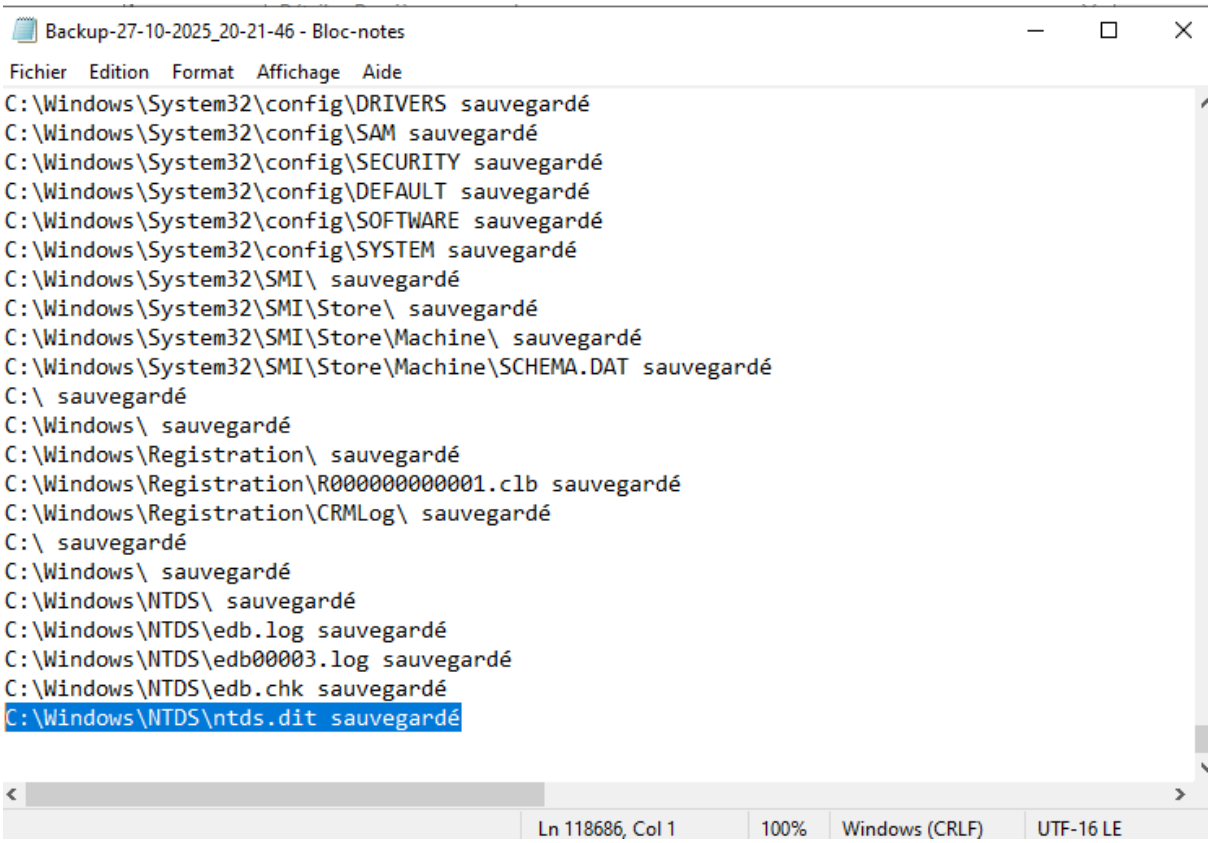


- sélectionnez l'**état du système**, puis cliquez sur **Suivant** ;



- spécifiez le **type de destination** (lecteurs locaux ou dossier partagé distant) puis cliquez sur Suivant ;
- enfin, cliquez sur **Sauvegarde**.

Après la sauvegarde, il est possible d'afficher les détails et de consulter les fichiers sauvegardés. Le fichier qui retiendra particulièrement notre attention est **NTDS.dit**, car il contient l'intégralité de l'annuaire.


Backup-27-10-2025_20-21-46 - Bloc-notes
Fichier Edition Format Affichage Aide
C:\Windows\System32\config\DRIVERS sauvegardé
C:\Windows\System32\config\SAM sauvegardé
C:\Windows\System32\config\SECURITY sauvegardé
C:\Windows\System32\config\DEFAULT sauvegardé
C:\Windows\System32\config\SOFTWARE sauvegardé
C:\Windows\System32\config\SYSTEM sauvegardé
C:\Windows\System32\SMI\ sauvegardé
C:\Windows\System32\SMI\Store\ sauvegardé
C:\Windows\System32\SMI\Store\Machine\ sauvegardé
C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT sauvegardé
C:\ sauvegardé
C:\Windows\ sauvegardé
C:\Windows\Registration\ sauvegardé
C:\Windows\Registration\R000000000001.clb sauvegardé
C:\Windows\Registration\CRMLog\ sauvegardé
C:\ sauvegardé
C:\Windows\ sauvegardé
C:\Windows\NTDS\ sauvegardé
C:\Windows\NTDS\edb.log sauvegardé
C:\Windows\NTDS\edb00003.log sauvegardé
C:\Windows\NTDS\edb.chk sauvegardé
C:\Windows\NTDS\ntds.dit sauvegardé
Ln 118686, Col 1
100%
Windows (CRLF)
UTF-16 LE