

SOMMAIRE

| | |
|---|-----------|
| SOMMAIRE..... | 1 |
| I-Préparation de l'environnement..... | 1 |
| Préparation des serveurs..... | 6 |
| Configuration de notre premier contrôleur de domaine..... | 7 |
| Configuration de notre second contrôleur de domaine..... | 13 |
| Mettre en place l'arborescence de notre active directory..... | 14 |
| Déclaration des ressources..... | 14 |
| Création des premiers objets..... | 16 |
| Intégration des postes clients au domaine..... | 18 |
| Mise en place d'une politique de mot de passe affinée..... | 25 |
| Vérification du fonctionnement de la politique de mot de passe affinée..... | 26 |
| II- Analysons la sécurité de notre architecture..... | 28 |
| Utilisons l'outil d'analyse des bonnes pratiques Microsoft..... | 28 |
| Fiabilisation de l'architecture locale..... | 29 |
| Organisation des différents sites géographiques..... | 29 |
| Mise en place d'un contrôleur de domaine en lecture seule (RODC)..... | 31 |
| III-Sécuriser le parc informatique grâce à Active Directory..... | 33 |
| a) Audit et restriction des accès entrants..... | 33 |
| Restriction des Options de Connexion (Accès Réseau)..... | 34 |
| Configuration de la Restriction d'Accès..... | 34 |
| Attribution des Droits..... | 35 |
| Déploiement de la Stratégie de Groupe..... | 36 |
| c) restriction de l'exécution de logicielles non autorisées..... | 42 |
| VI-Sauvegarde de la base de données..... | 44 |

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

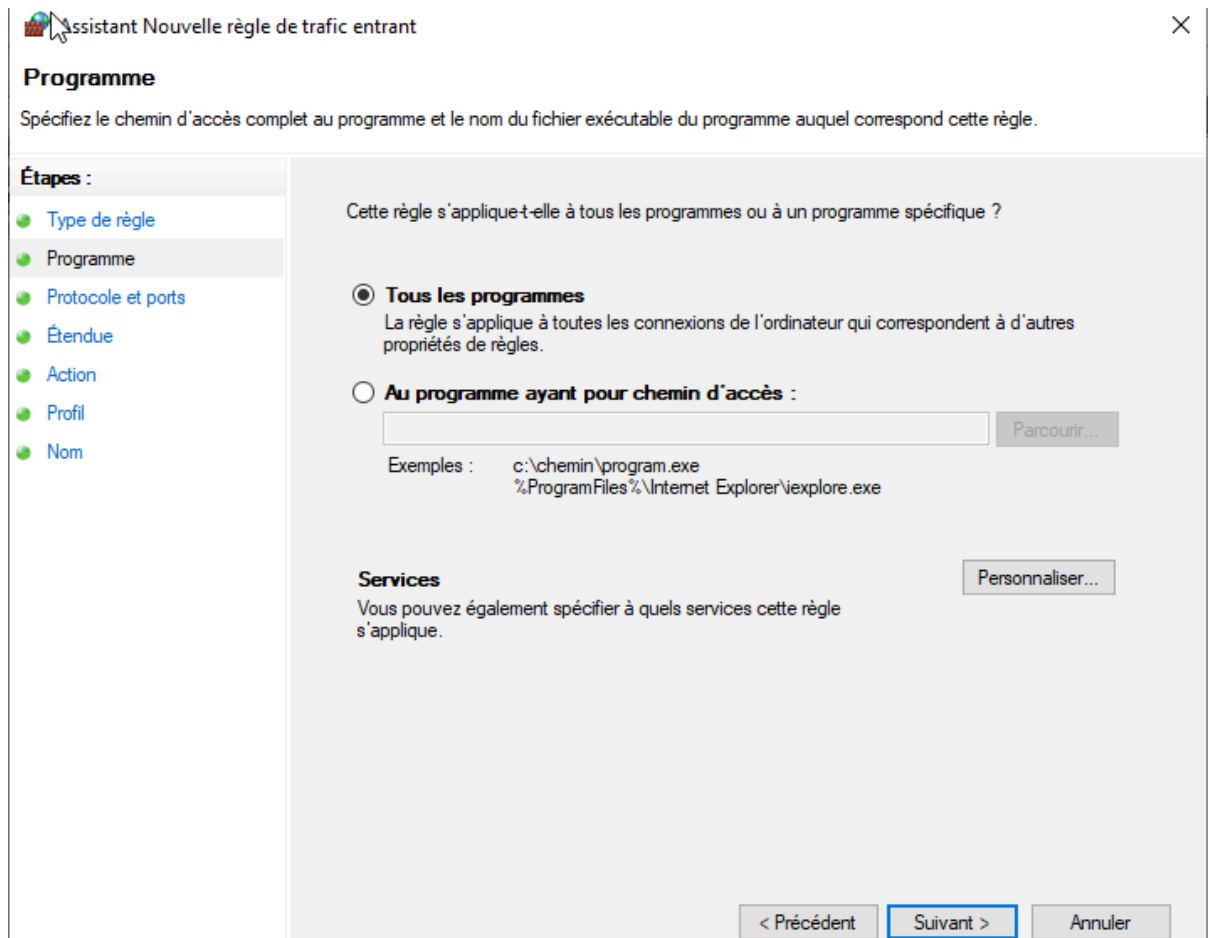
Pour réaliser un test de connectivité (ping) entre les machines, et vérifier qu'elles peuvent communiquer, il faut d'abord ajouter une nouvelle règle icmpv4 parce que par défaut windows bloque tous les ping . Pour le faire suivez ces étapes suivantes.

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


comme type de règle choisir personnalisée puis suivant

The screenshot shows the 'Assistant Nouvelle règle de trafic entrant' (New Inbound Rule Wizard) window. The title bar includes a close button (X). The main heading is 'Type de règle' (Rule Type), with the instruction 'Sélectionnez le type de règle de pare-feu à créer.' (Select the type of firewall rule to create.). On the left, a sidebar titled 'Étapes :' (Steps) lists the wizard's steps: 'Type de règle' (selected), 'Programme', 'Protocole et ports', 'Étendue', 'Action', 'Profil', and 'Nom'. The main area asks 'Quel type de règle voulez-vous créer ?' (What type of rule do you want to create?). It offers four options: 'Programme' (Rule that controls connections from a program), 'Port' (Rule that controls connections from a TCP or UDP port), 'Prédéfinie :' (Predefined), and 'Personnalisée' (Custom, selected). The 'Prédéfinie' dropdown menu is open, showing 'Accès réseau COM+' (Network COM+ access). At the bottom, there are three buttons: '< Précédent' (Previous), 'Suivant >' (Next, highlighted with a blue border), and 'Annuler' (Cancel).

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



ensuite spécifiez le type de protocole dans notre cas icmpv4

 Assistant Nouvelle règle de trafic entrant

×

Protocole et ports

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

Étapes :

- Type de règle
- Programme
- Protocole et ports**
- Étendue
- Action
- Profil
- Nom

À quels ports et protocoles cette règle s'applique-t-elle ?

Type de protocole :

Numéro de protocole :

Port local :

Exemple : 80, 443, 5000-5010

Port distant :

Exemple : 80, 443, 5000-5010

Paramètres ICMP (Internet Control Message Protocol) :

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

Assistant Nouvelle règle de trafic entrant

Étendue

Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.

Étapes :

- Type de règle
- Programme
- Protocole et ports
- Étendue**
- Action
- Profil
- Nom

À quelles adresses IP locales cette règle s'applique-t-elle ?

☒ Toute adresse IP

☐ Ces adresses IP :

Ajouter...
Modifier...
Supprimer

Personnaliser les types d'interfaces auxquels cette règle s'applique : Perso...

À quelles adresses IP distantes cette règle s'applique-t-elle ?

☒ Toute adresse IP

☐ Ces adresses IP :

Ajouter...
Modifier...
Supprimer

< Précédent Suivant > Annuler

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

```
C:\Users\pierre>ping 192.168.145.129

Envoi d'une requête 'Ping' 192.168.145.129 avec 32 octets de données :
Réponse de 192.168.145.129 : octets=32 temps<1ms TTL=128
Réponse de 192.168.145.129 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.145.129 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.145.129 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 192.168.145.129:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\pierre>ping 192.168.145.128

Envoi d'une requête 'Ping' 192.168.145.128 avec 32 octets de données :
Réponse de 192.168.145.128 : octets=32 temps<1ms TTL=128
Réponse de 192.168.145.128 : octets=32 temps<1ms TTL=128
Réponse de 192.168.145.128 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.145.128 : octets=32 temps<1ms TTL=128

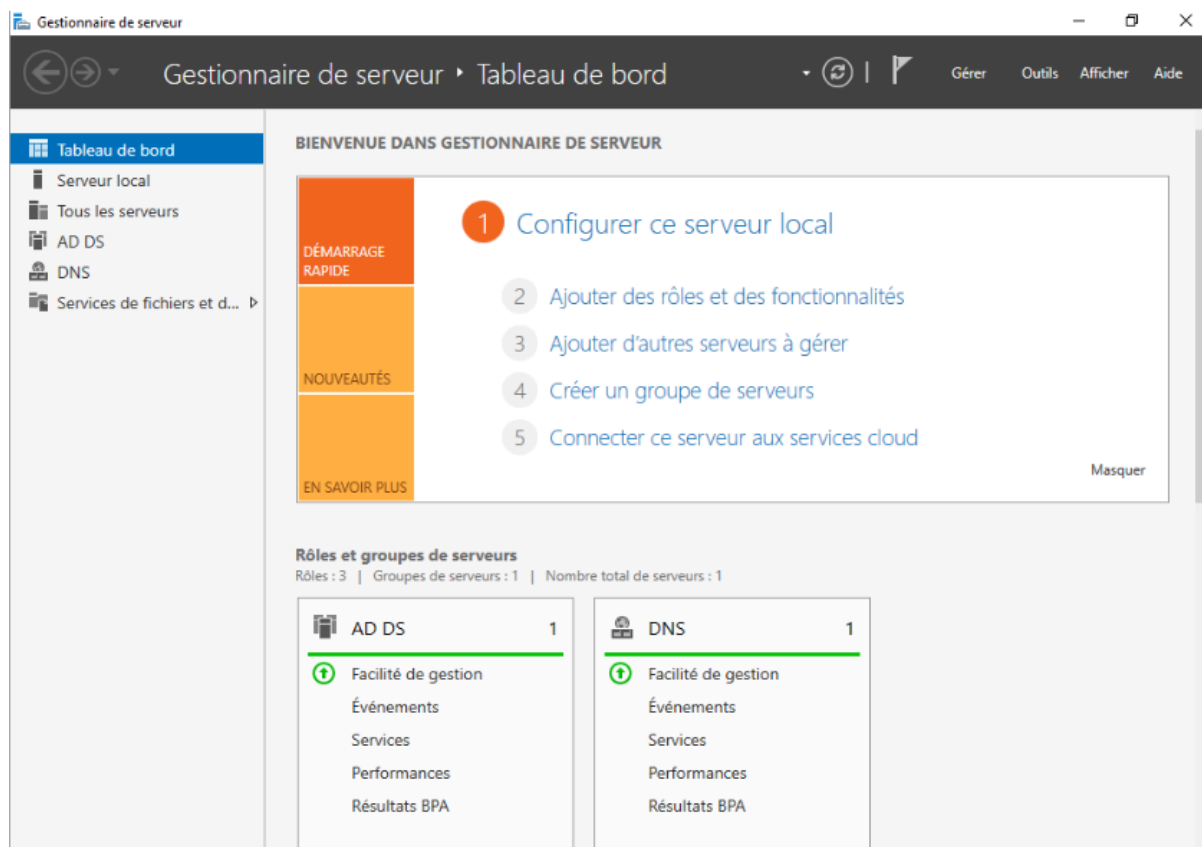
Statistiques Ping pour 192.168.145.128:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

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 :

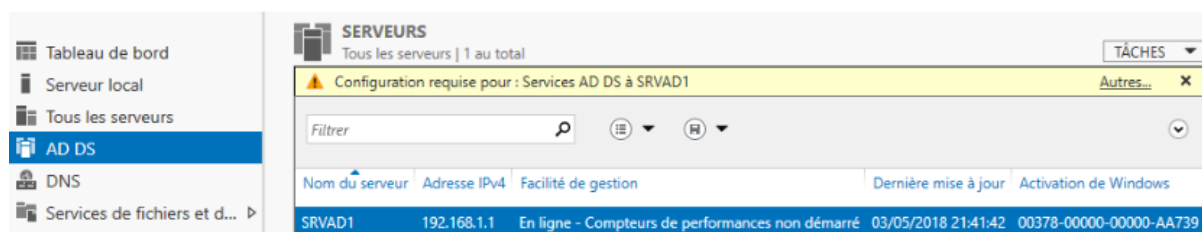


Cliquez sur **Ajouter des rôles et des fonctionnalités**. Validez la première étape de l'assistant en cliquant sur **Suivant**. Sélectionnez **Installation basée sur un rôle ou une fonctionnalité** et sélectionnez le nom du serveur dans la liste, cochez **Service AD DS** et lancez l'installation.

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

The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar indicates the target server is 'SRVAD1'. The main heading is 'Configuration de déploiement'. On the left, a sidebar lists the steps: 'Configuration de déploiement...', 'Options du contrôleur de...', 'Options supplémentaires', 'Chemins d'accès', 'Examiner les options', 'Vérification de la configur...', 'Installation', and 'Résultats'. The main area is titled 'Sélectionner l'opération de déploiement' and contains three radio buttons: 'Ajouter un contrôleur de domaine à un domaine existant', 'Ajouter un nouveau domaine à une forêt existante', and 'Ajouter une nouvelle forêt' (which is selected). Below this, it says 'Spécifiez les informations de domaine pour cette opération' and has a text box for 'Nom de domaine racine : ' with 'gift.sa' entered. At the bottom, there are buttons for '< Précédent', 'Suivant >', 'Installer', and 'Annuler'. A link 'En savoir plus sur les configurations de déploiement' is also present.

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).

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
SRVAD1

Configuration de déploiement
Options du contrôleur de domaine
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration
Installation
Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Domain Name System)
☒ Catalogue global (GC)
☐ Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

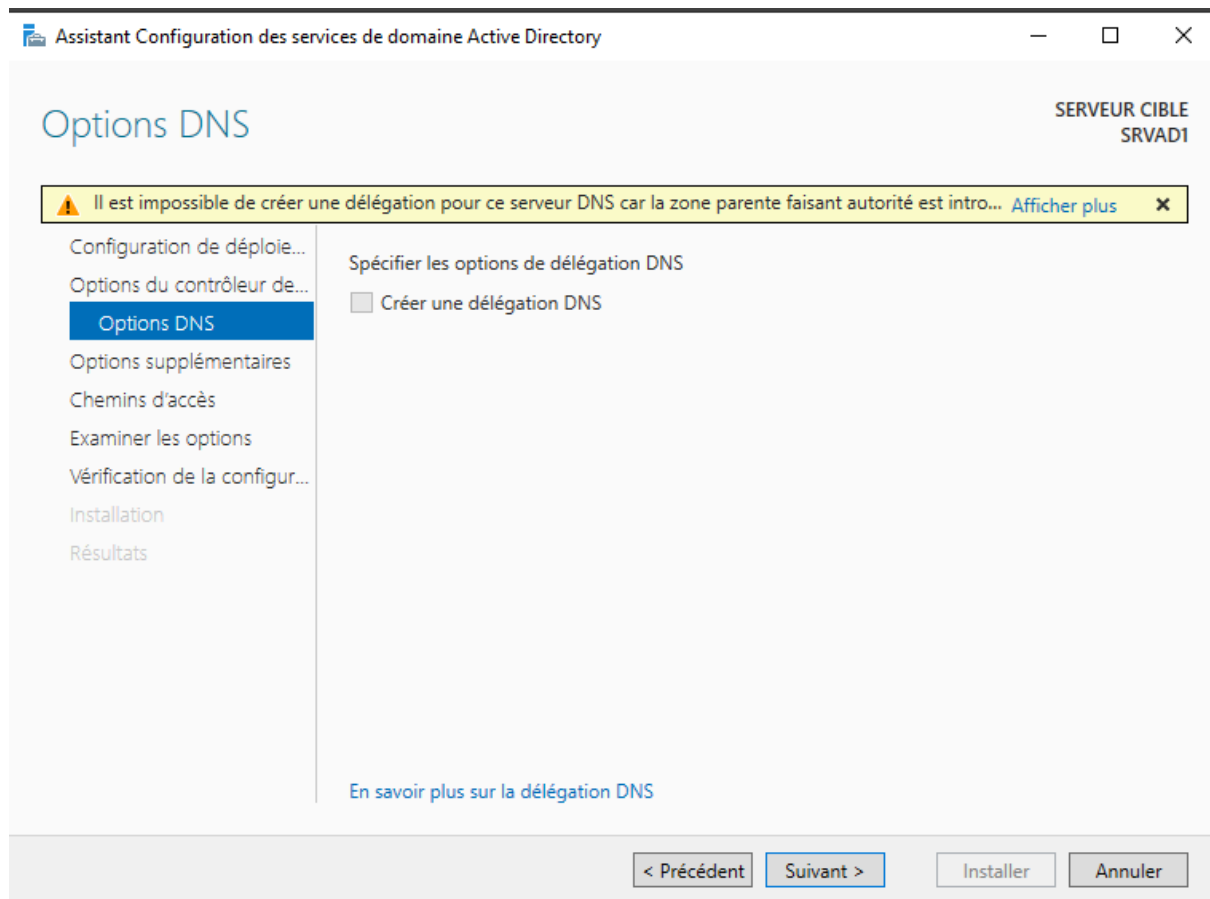
Mot de passe :

Confirmer le mot de passe :

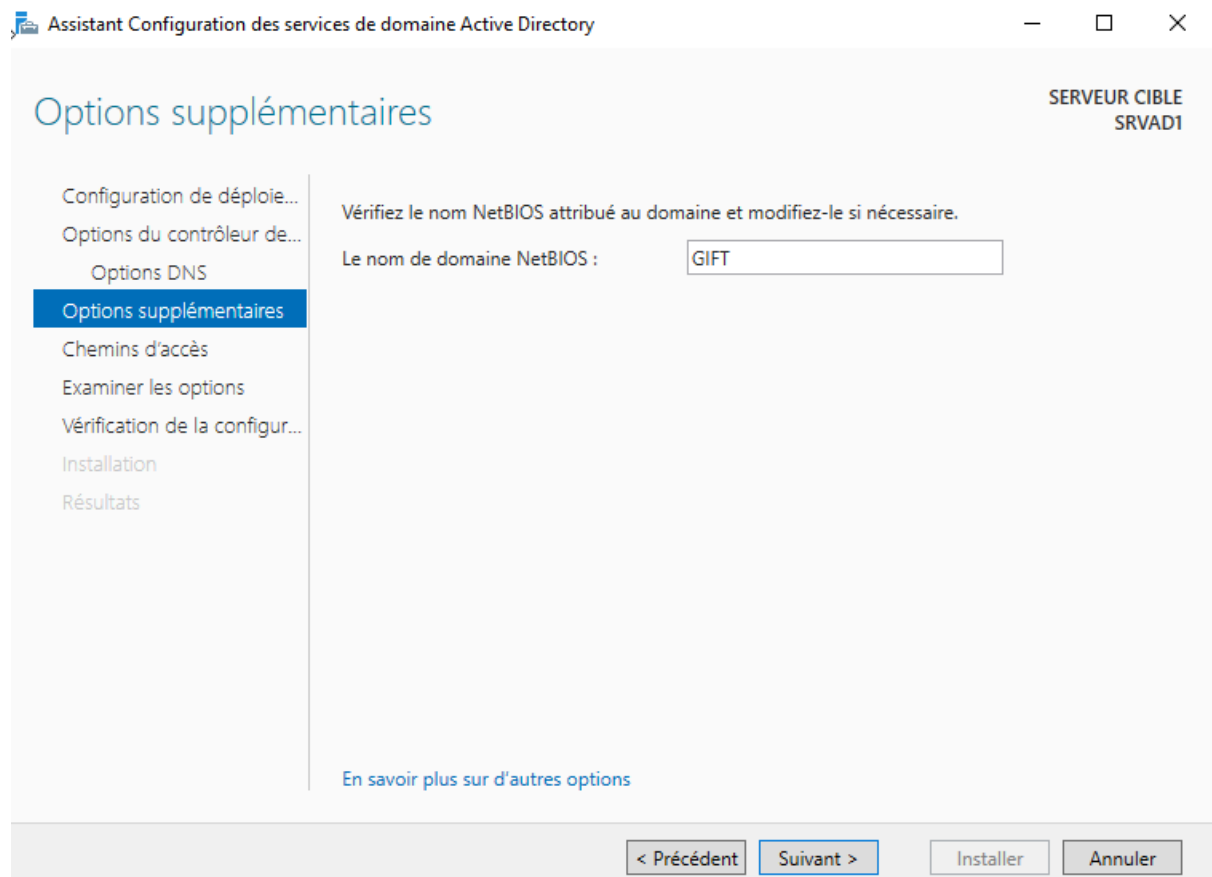
[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

A cette étape vu 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

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE
SRVAD1

Chemins d'accès

Configuration de déploiement...
Options du contrôleur de domaine...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration...
Installation
Résultats

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données : C:\Windows\NTDS

Dossier des fichiers journaux : C:\Windows\NTDS

Dossier SYSVOL : C:\Windows\SYSVOL

[En savoir plus sur les chemins d'accès Active Directory](#)

< Précédent Suivant > Installer Annuler

ensuite nous pouvons voir un petit récapitulatif des étapes à faire installer

Vérification de la configuration requise

SERVEUR CIBLE
SRVAD1

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation. [Afficher plus](#)

Configuration de déploiement...
Options du contrôleur de domaine...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration requise
Installation
Résultats

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

⬆ Voir les résultats

⚠ Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez

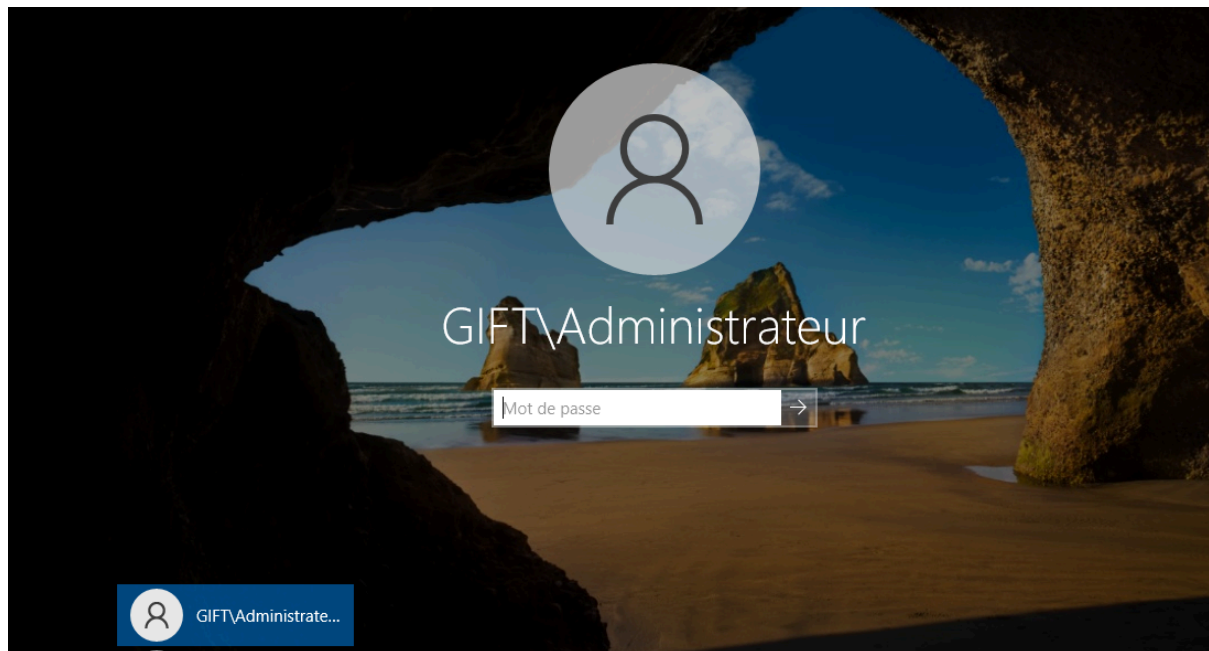
⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur les conditions préalables](#)

< Précédent Suivant > Installer Annuler

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.

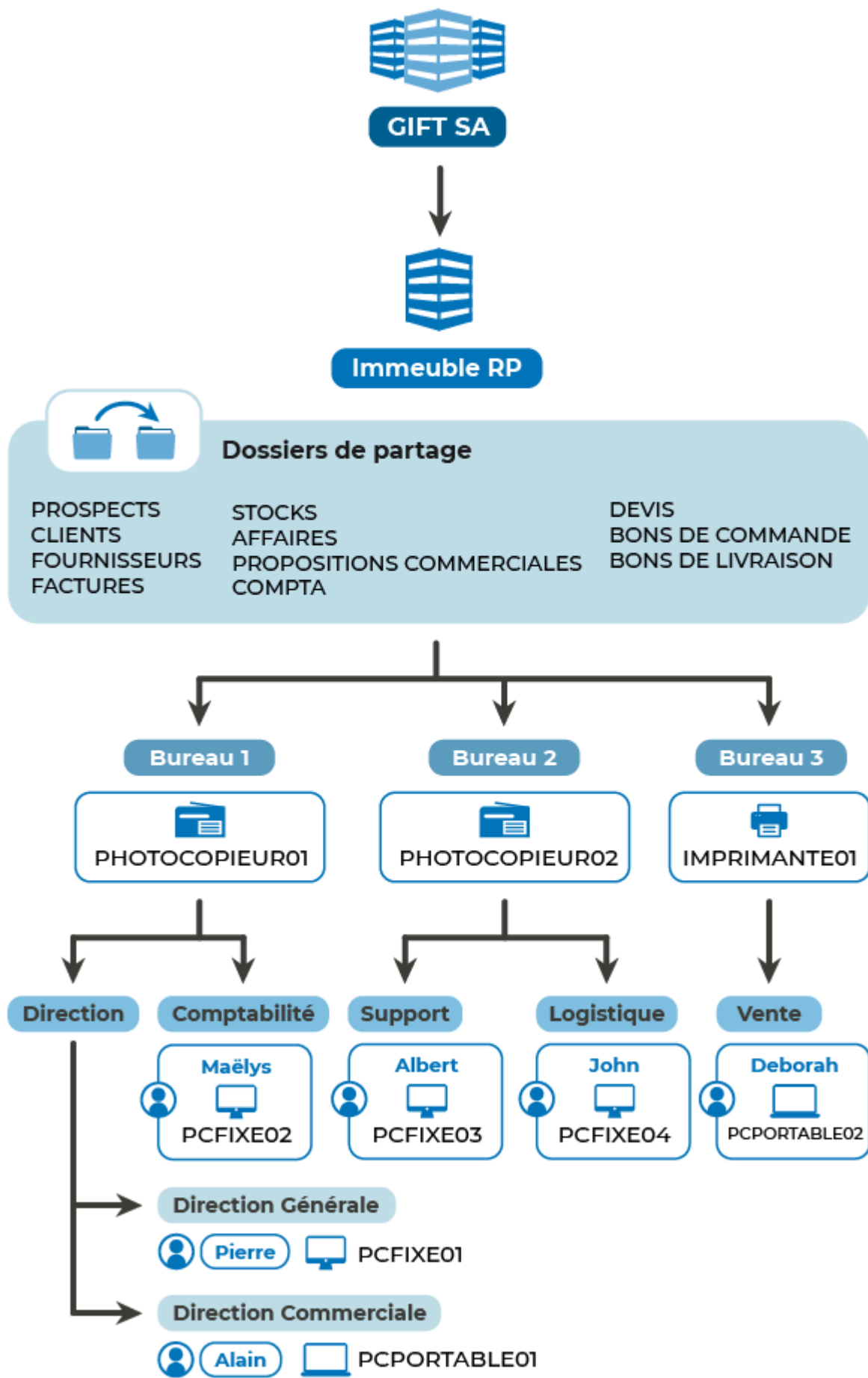
Les choix sont plus restreints, car les paramètres propres au domaine et à la forêt sont déjà stockés dans la base de données présente sur le premier contrôleur de domaine. Après avoir terminé cette étape, il faut également redémarrer le serveur. Au redémarrage, vous observez à nouveau le nom de domaine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

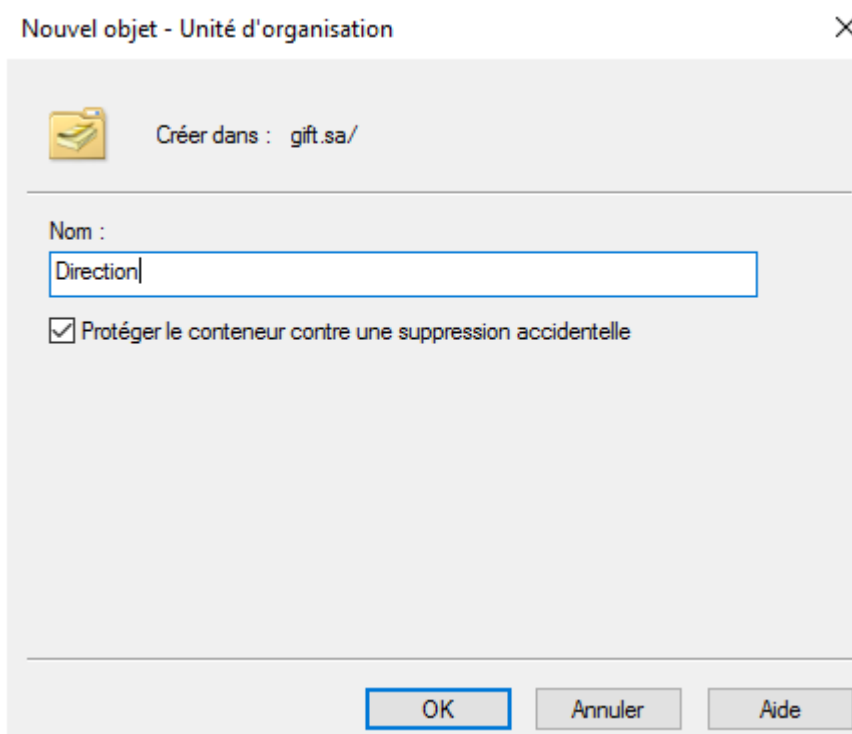
Notre domaine est maintenant créé. Ce qui signifie qu'on dispose d'un annuaire, mais presque vide. Il vous faut donc maintenant créer les ressources que nous avons identifiées au sein de notre entreprise pour mieux connaître de quoi il s'agit je vous invite à vous référer de l'organigramme suivante:



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 !



Nouvel objet - Unité d'organisation

Créer dans : gift.sa/

Nom :
Direction

☒ Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

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

Pierre Utilisateur

Propriétés de : Pierre ? X

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+
Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Nom d'ouverture de session de l'utilisateur :
 @gift.sa

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

☐ Déverrouiller le compte

Options de compte :

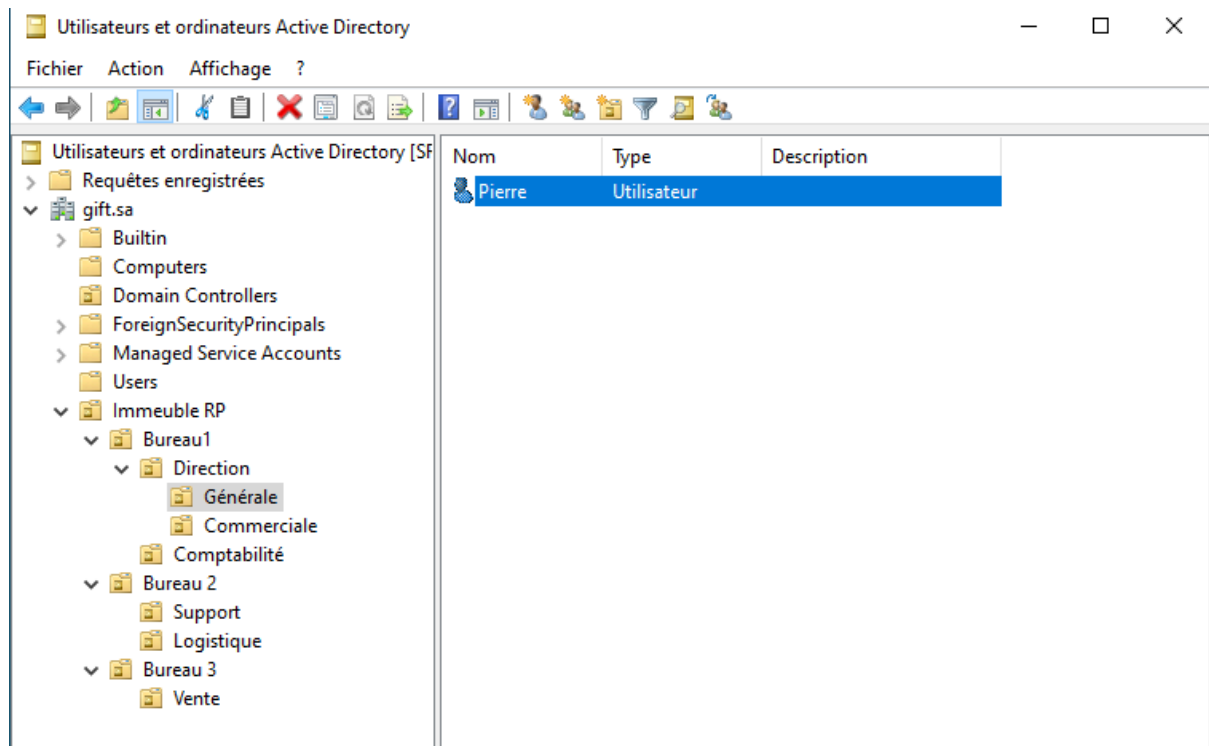
☐ L'utilisateur devra changer le mot de passe
☒ L'utilisateur ne peut pas changer de mot de passe
☒ Le mot de passe n'expire jamais
☐ Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

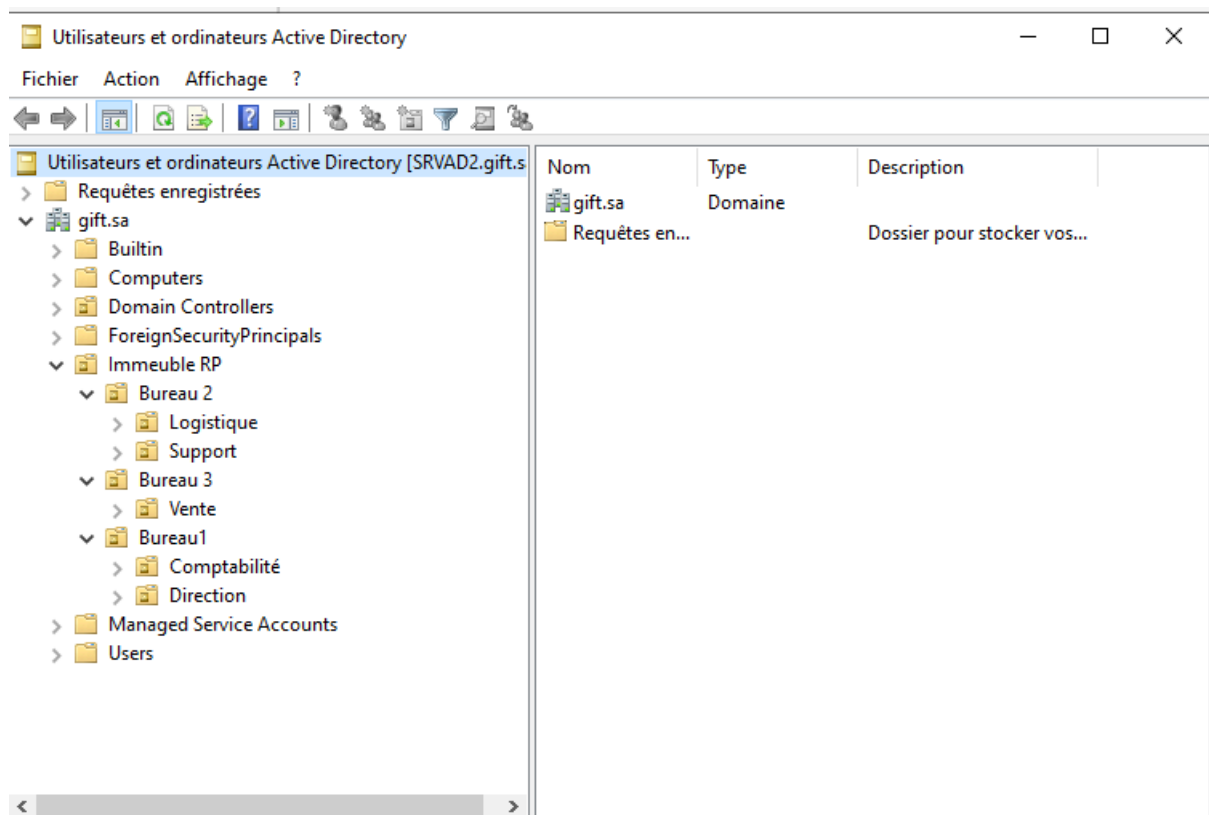
☒ Jamais
☐ Fin de :

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 pour voir au niveau DNS tout fonctionne normalement avec l'outil nslookup on peut voir que notre DNS reconnaît bien notre domaine

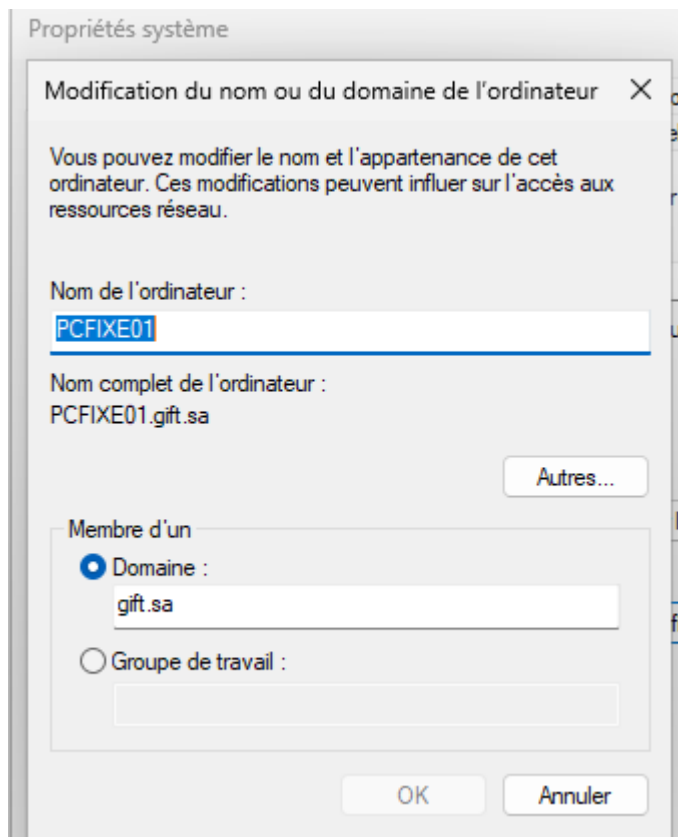
```
C:\Users\administrateur>nslookup
DNS request timed out.
    timeout was 2 seconds.
Serveur par défaut :   UnKnown
Address:  192.168.145.128

> gift.sa
Serveur :   UnKnown
Address:  192.168.145.128

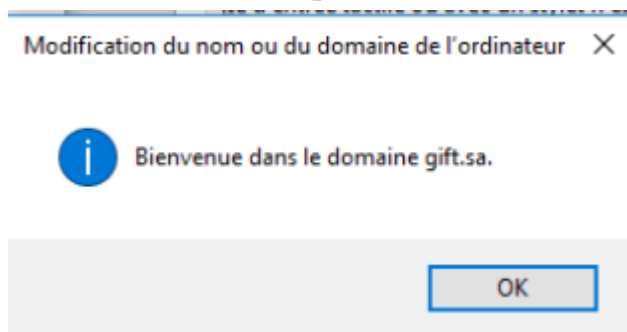
Nom :      gift.sa
Addresses: 192.168.145.128
           192.168.145.129

>
```

Maintenant pour intégrer la machine au domaine 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

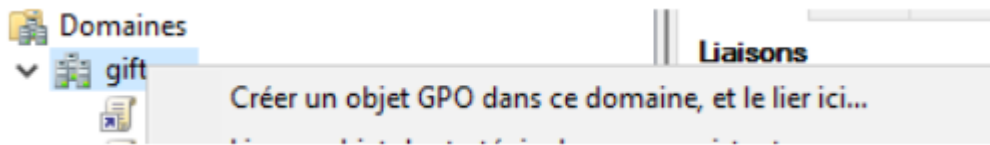


après vous verrez un message de bienvenue au domaine une fois que la machine ait redémarrer il fait partie du domaine

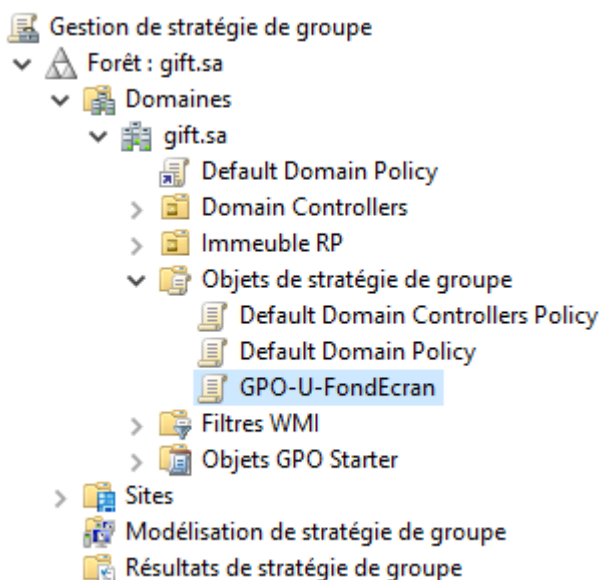


Mise en place des stratégies de groupes

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

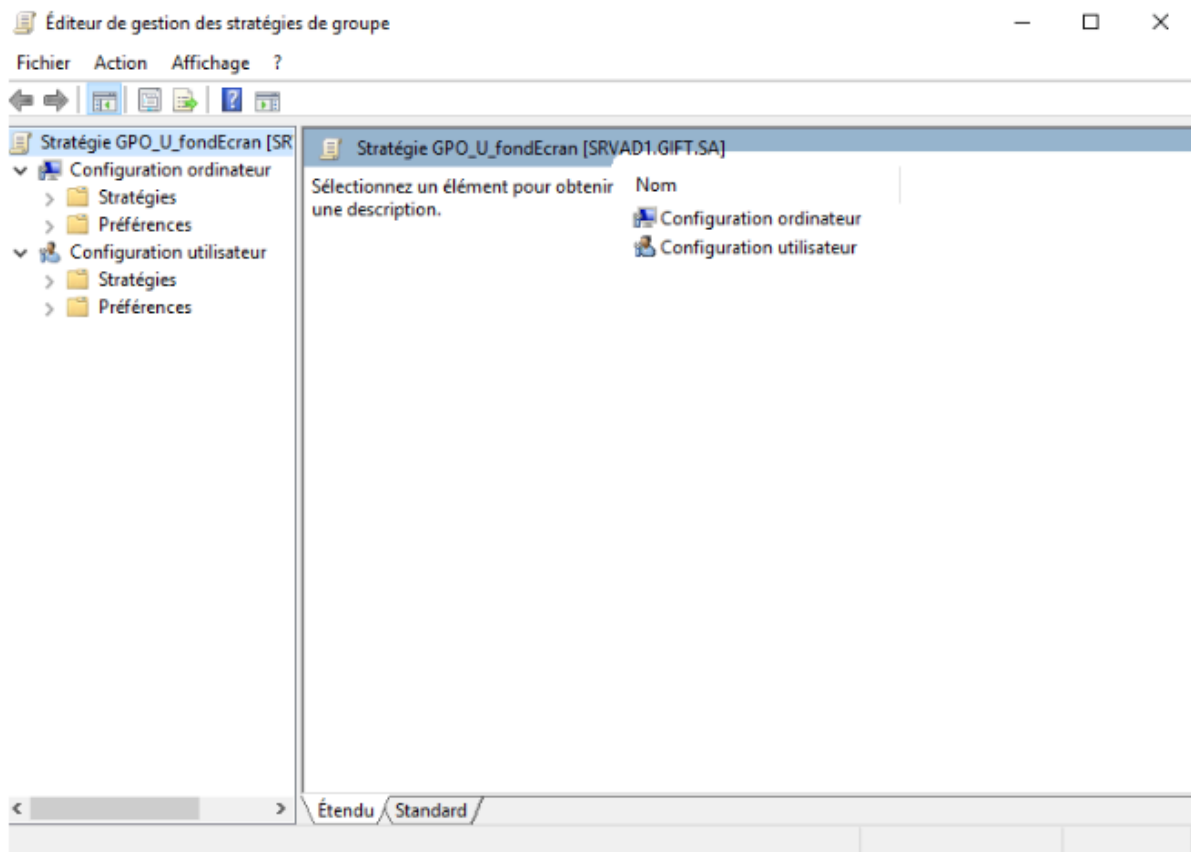


Nous allons le nommer *GPO-U-FondEcran*. Cela permet de savoir qu'il s'agit d'un objet GPO avec des paramètres utilisateur concernant le fond d'écran.

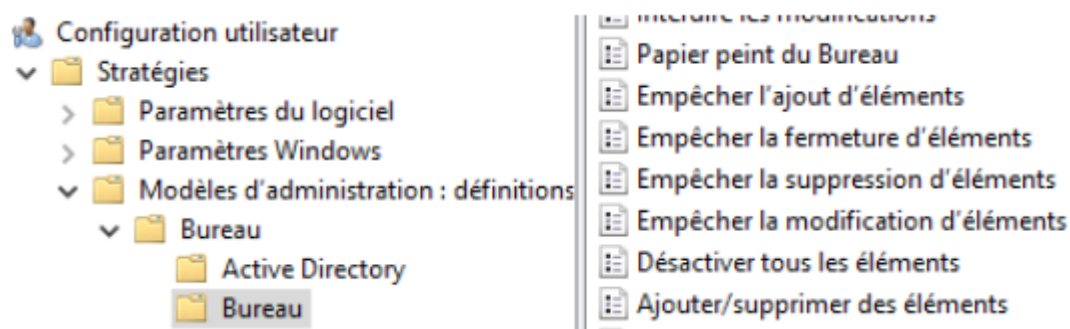


En effet, le lien sur le domaine fait apparaître l'objet GPO sous le nom du domaine, et cet objet se retrouve listé avec les autres objets GPO existants.

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**.

Papier peint du Bureau

Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire : DA:Création GPO logo
☒ **Activé**
☐ Désactivé

Pris en charge sur : Au minimum Windows 2000

Options : Aide :

Nom du papier peint :

Exemple : avec un chemin local :
 C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC :
 \\Server\Share\Corp.jpg

Style du papier peint : Remplir

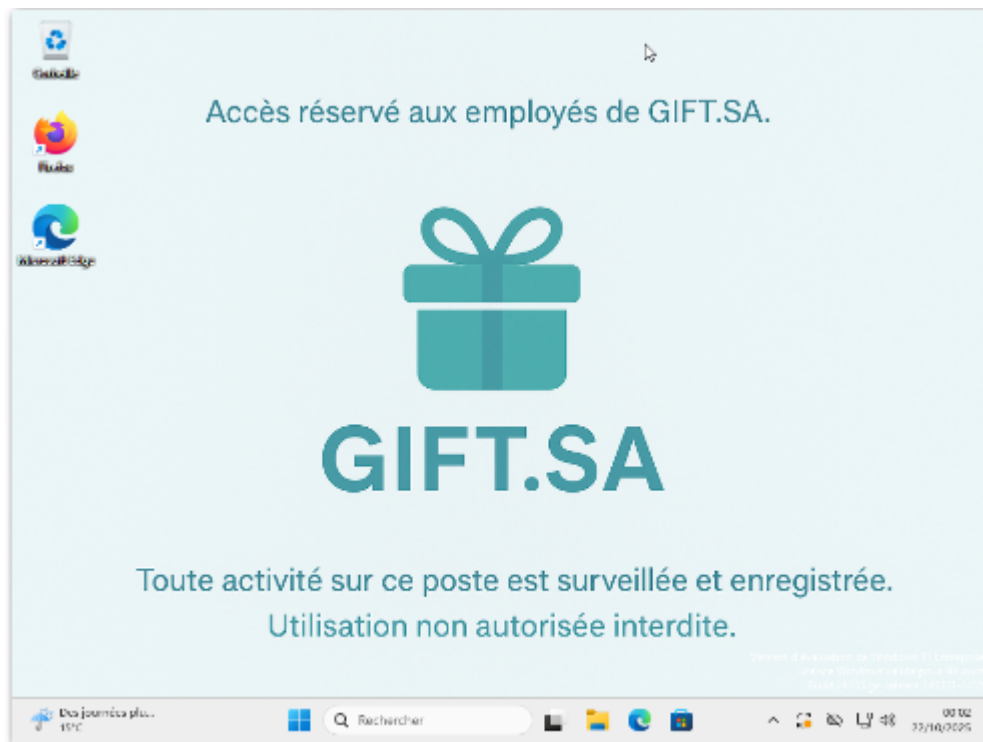
Spécifie l'image d'arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.

Ce paramètre vous permet de spécifier le papier peint du Bureau des utilisateurs et empêche ces derniers de modifier l'image ou sa présentation. Le papier peint spécifié peut être enregistré dans un fichier de type bitmap (*.bmp) ou JPEG (*.jpg).

Pour utiliser ce paramètre, entrez le chemin d'accès complet et le nom du fichier contenant le papier peint. Vous pouvez taper un chemin d'accès local, tel que C:\Windows\web\wallpaper\accueil.jpg ou un chemin d'accès UNC, tel que \\Serveur\Partage\Logo.jpg. Si le fichier spécifié n'est pas disponible lorsque l'utilisateur ouvre sa session, aucun papier peint n'est affiché. Les utilisateurs ne peuvent pas spécifier un autre papier peint. Vous pouvez également utiliser ce paramètre afin de spécifier si l'image du papier peint doit être centrée, en mosaïque ou étirée. Les utilisateurs ne peuvent pas modifier cette spécification.

Si vous désactivez ce paramètre ou ne le configurez pas, aucun

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**

```
Invité de commande
Microsoft Windows [version 10.0.26280.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\pierre>gpresult /R

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.8
© Microsoft Corporation. Tous droits réservés.

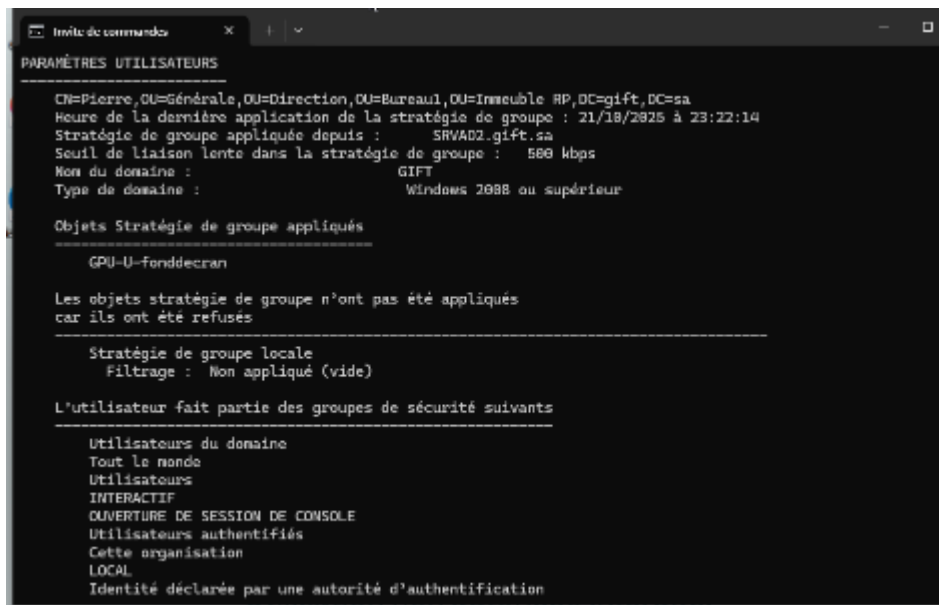
Créé le 22/10/2025 à 00:10:25

Données RSOP pour GIFT\Pierre sur PCFIXE01 : mode journalisation
-----

Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.26280
Nom du site..... : N/A
Profil itinérant : N/A
Profil local..... : C:\Users\pierre
Connexion via une liaison lente ? : Non

PARAMÈTRES UTILISATEURS
-----

CN=Pierre,OU=Générale,OU=Direction,OU=Bureau,OU=Immeuble RP,DC=gift,DC=sa
Heure de la dernière application de la stratégie de groupe : 21/10/2025 à 23:22:14
Stratégie de groupe appliquée depuis : SRVAD2.gift.sa
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : GIFT
Type de domaine : Windows 2008 ou supérieur
```

```
Invite de commande

PARAMÈTRES UTILISATEURS

CN=Pierre,OU=Générale,OU=Direction,OU=Bureau1,OU=Immeuble RP,DC=gift,DC=sa
Heure de la dernière application de la stratégie de groupe : 21/10/2025 à 23:22:14
Stratégie de groupe appliquée depuis : SRVAD2.gift.sa
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : GIFT
Type de domaine : Windows 2008 ou supérieur

Objets Stratégie de groupe appliqués

GPU-U-fonddecran

Les objets stratégie de groupe n'ont pas été appliqués
car ils ont été refusés

Stratégie de groupe locale
Filtrage : Non appliqué (vide)

L'utilisateur fait partie des groupes de sécurité suivants

Utilisateurs du domaine
Tout le monde
Utilisateurs
INTERACTIF
OUVERTURE DE SESSION DE CONSOLE
Utilisateurs authentifiés
Cette organisation
LOCAL
Identité déclarée par une autorité d'authentification
```

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 :

Créer Paramètres de mot de passe : PSO_DG

TÂCHES ▼ SECTIONS ▼

Paramètres de mot de passe

S'applique directement à

Nom : * PSO_DG

Priorité : * 1

☒ Appliquer la longueur minimale du mot de passe

Longueur minimale du mot de passe (caractères) : * 12

☒ Appliquer l'historique des mots de passe

Nombre de mots de passe mémorisés : * 24

☒ Le mot de passe doit respecter des exigences de complexité

☐ Stocker le mot de passe en utilisant un chiffrement réversible

☒ Protéger contre la suppression accidentelle

Description :

Options d'âge du mot de passe :

☒ Appliquer l'âge minimal de mot de passe

L'utilisateur ne peut pas changer le mot de pas... * 2

☒ Appliquer l'âge maximal de mot de passe

L'utilisateur doit changer le mot de passe après... * 42

☒ Appliquer la stratégie de verrouillage des comptes :

Nombre de tentatives de connexion échouées aut... * 3

Réinitialiser le nombre de tentatives de connexion... * 30

Le compte va être verrouillé

☐ Pendant une durée de (mins) : * 30

☒ Jusqu'à ce qu'un administrateur déverrouille manuellement le...

S'applique directement à

Nom Courrier

Pierre

Ajouter...

Supprimer

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
```

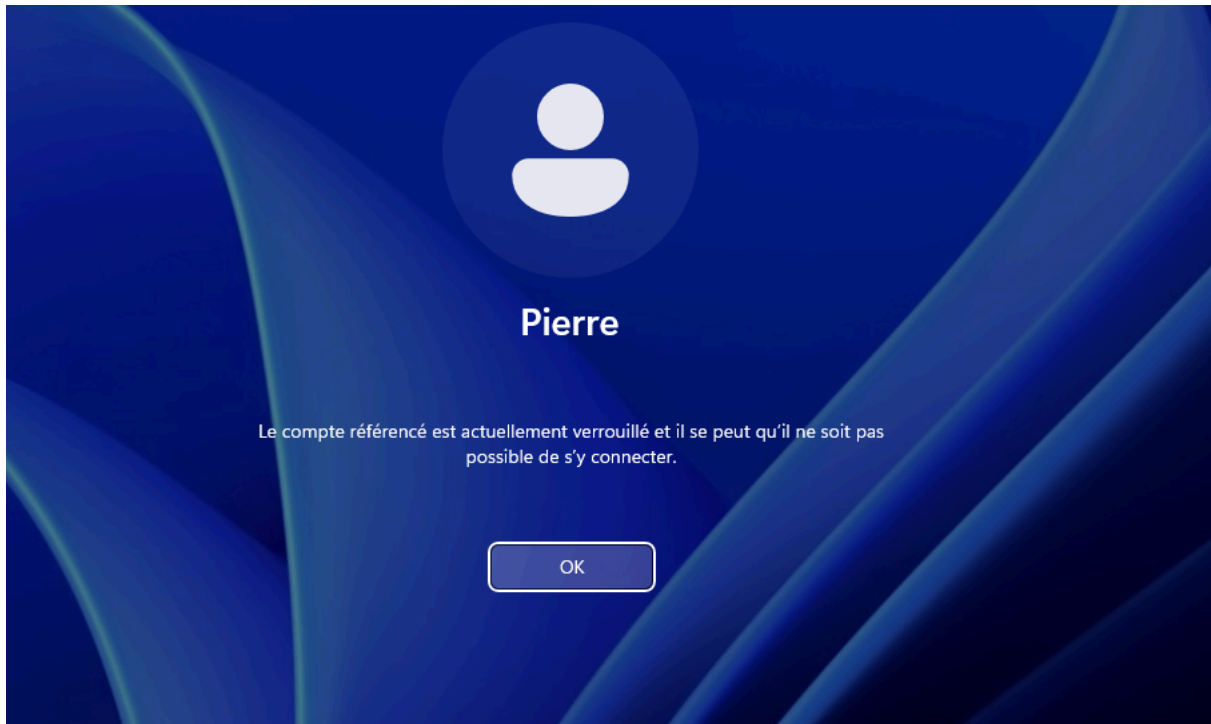
Vérification du fonctionnement de la politique de mot de passe affinée

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.

Général Adresse **Compte** Profil Téléphones Organisation Membre de Appel entrant

Nom d'ouverture de session de l'utilisateur :
Pierre @gift.sa

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
GIFT\ Pierre

Horaires d'accès... Se connecter à...

☒ Déverrouiller le compte. Ce compte est actuellement verrouillé sur ce contrôleur de domaine Active Directory.

Options de compte :

- ☐ L'utilisateur devra changer le mot de passe
- ☒ L'utilisateur ne peut pas changer de mot de passe
- ☒ Le mot de passe n'expire jamais
- ☐ Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

☒ Jamais

☐ Fin de : dimanche 23 novembre 2025

OK Annuler Appliquer Aide

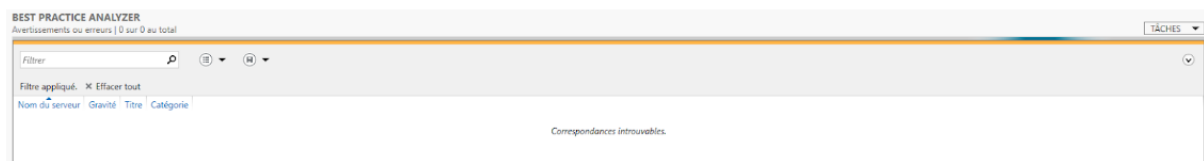
II- Analysons la sécurité de notre architecture

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.

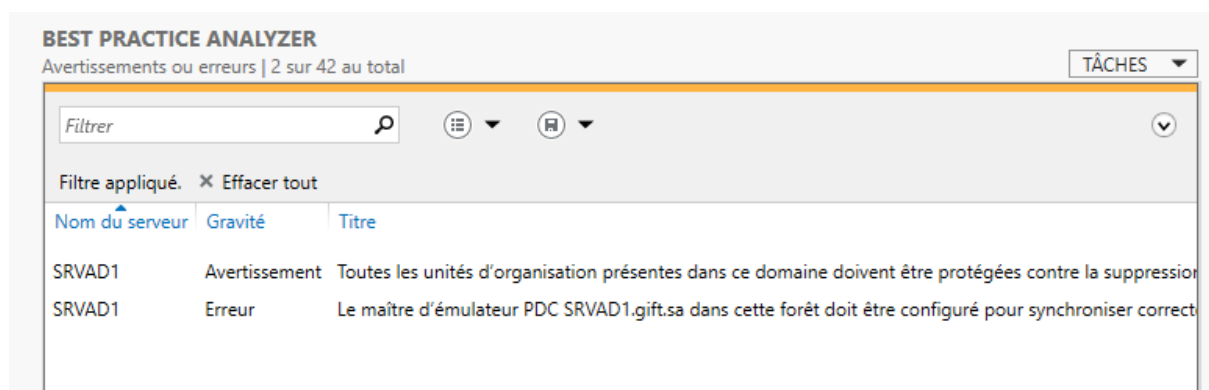
C'est notamment le cas du rôle AD DS. L'outil **Best Practice Analyzer (BPA)** se présente simplement par une zone dans le gestionnaire de serveur :



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**).

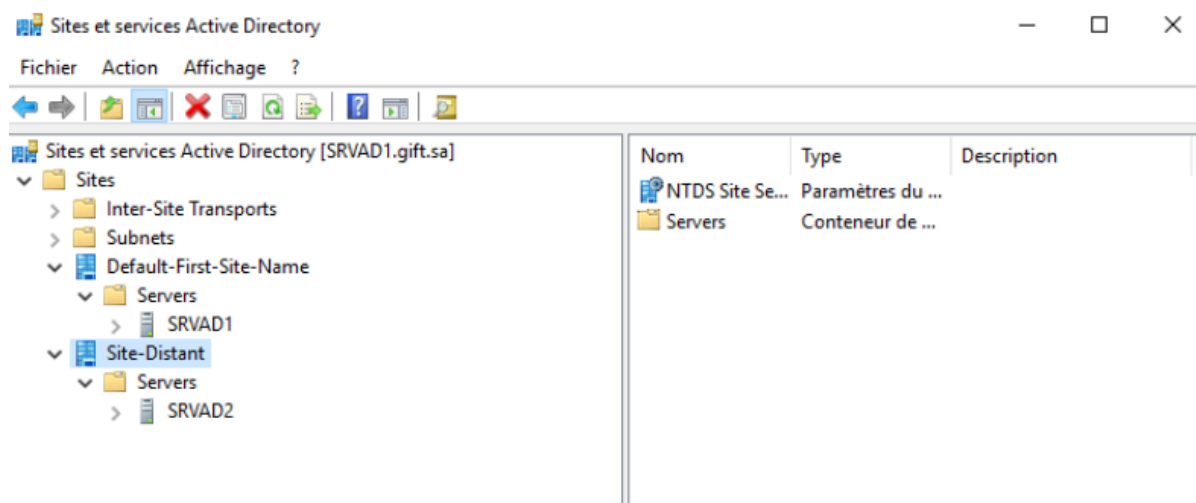
Organisation des différents sites géographiques

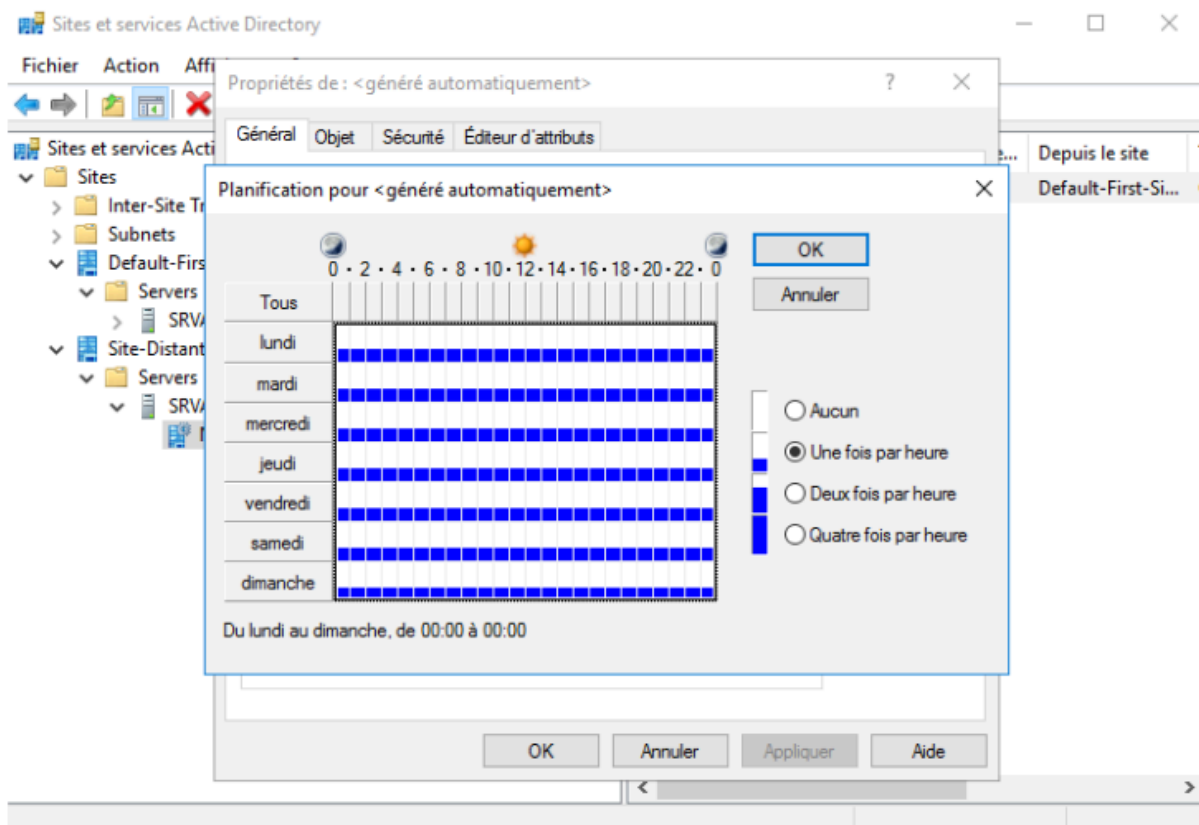
L'entreprise étant répartie sur plusieurs **sites géographiques distants**, il est essentiel d'assurer une **réplication efficace et maîtrisée** des données Active Directory entre ces sites.

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 **roulage 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 déploiement...

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 :

••••••••

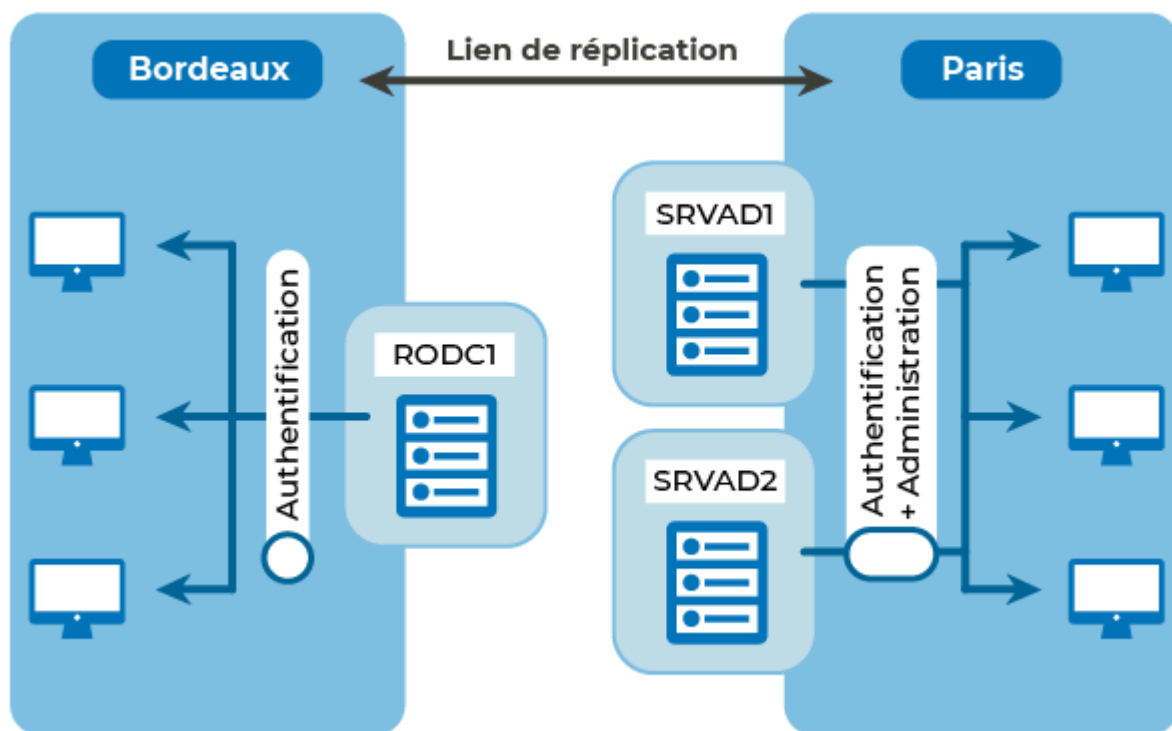
[En savoir plus sur les options pour le contrôleur de domaine](#)

< 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**.

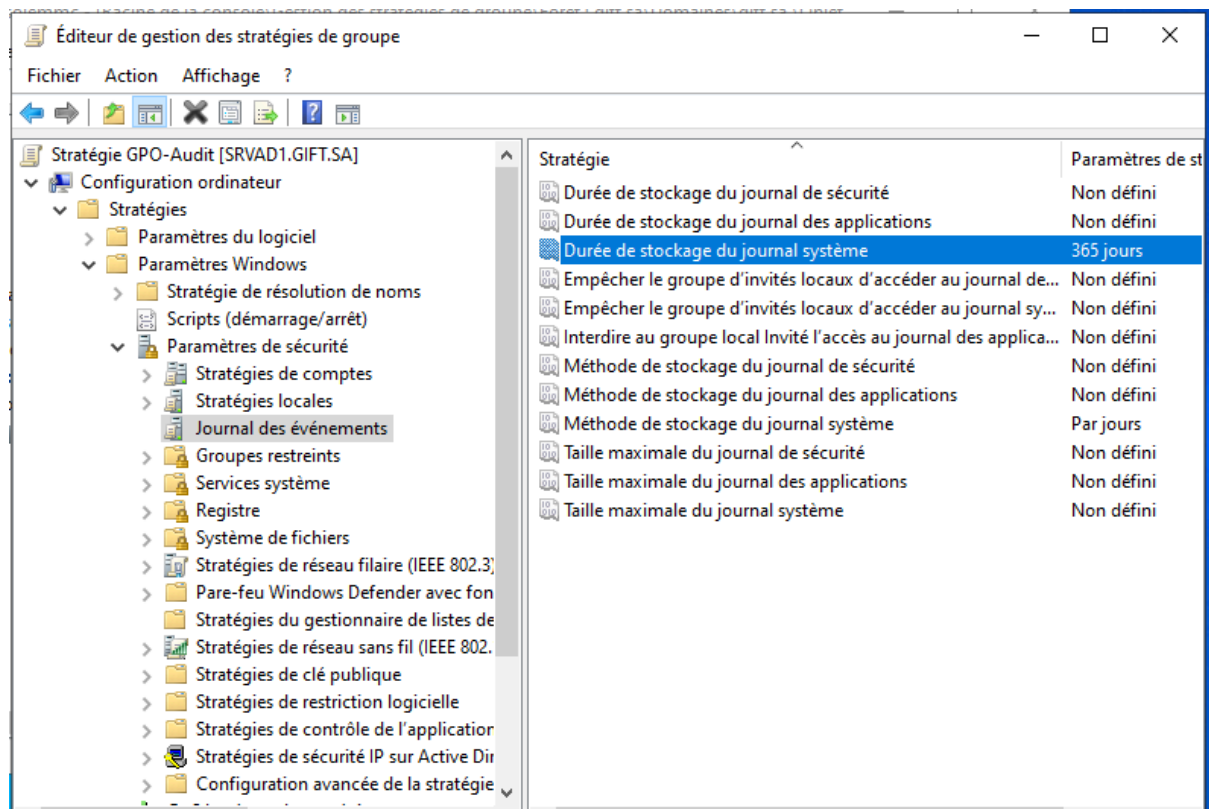
Ces mesures visent à **améliorer la fiabilité, la cohérence et la sécurité** de l'infrastructure Active Directory.

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)

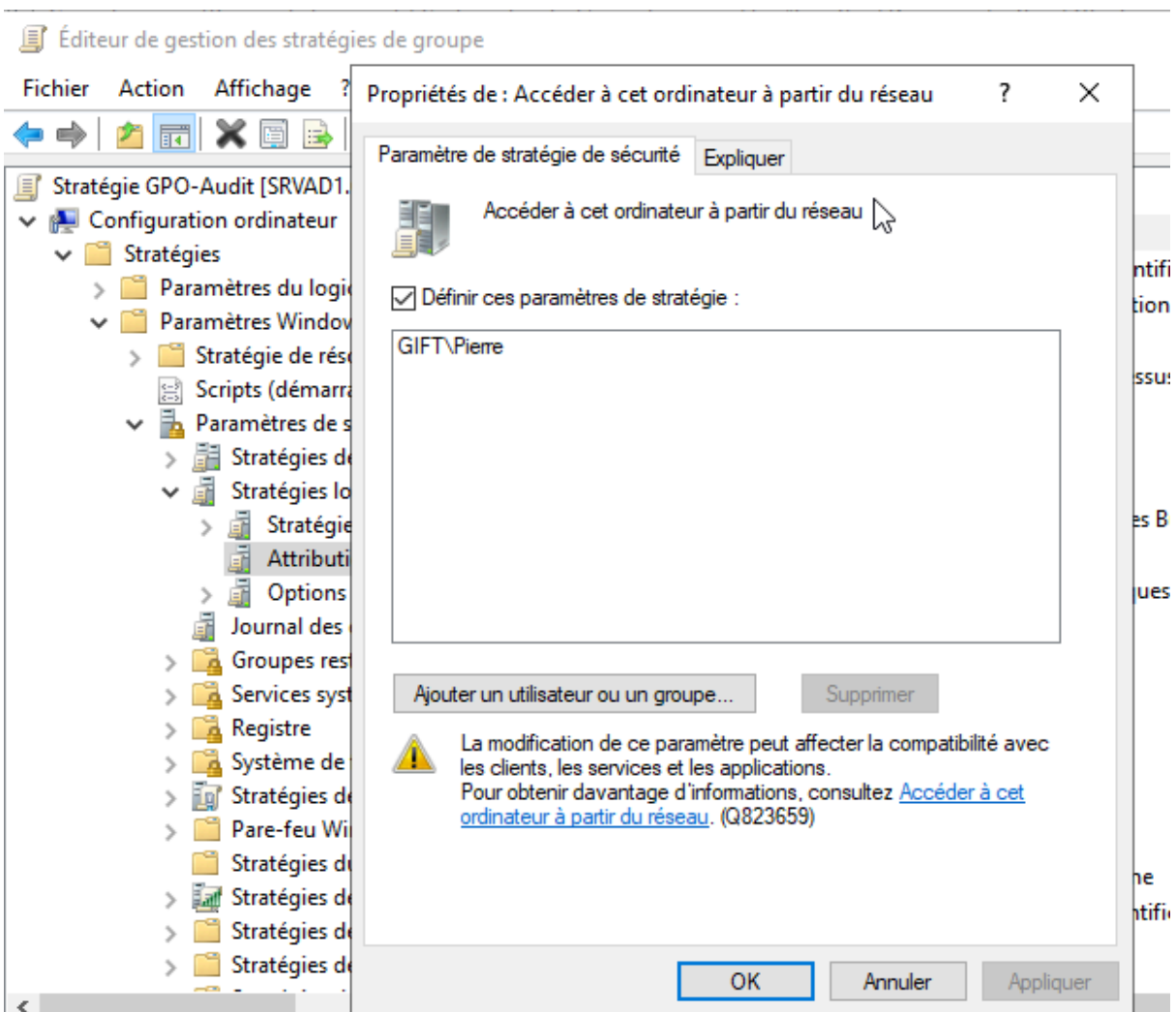
Parallèlement à l'audit, des mesures spécifiques ont été prises pour restreindre les connexions réseau, limitant ainsi l'accès aux ressources sur un poste ciblé.

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.

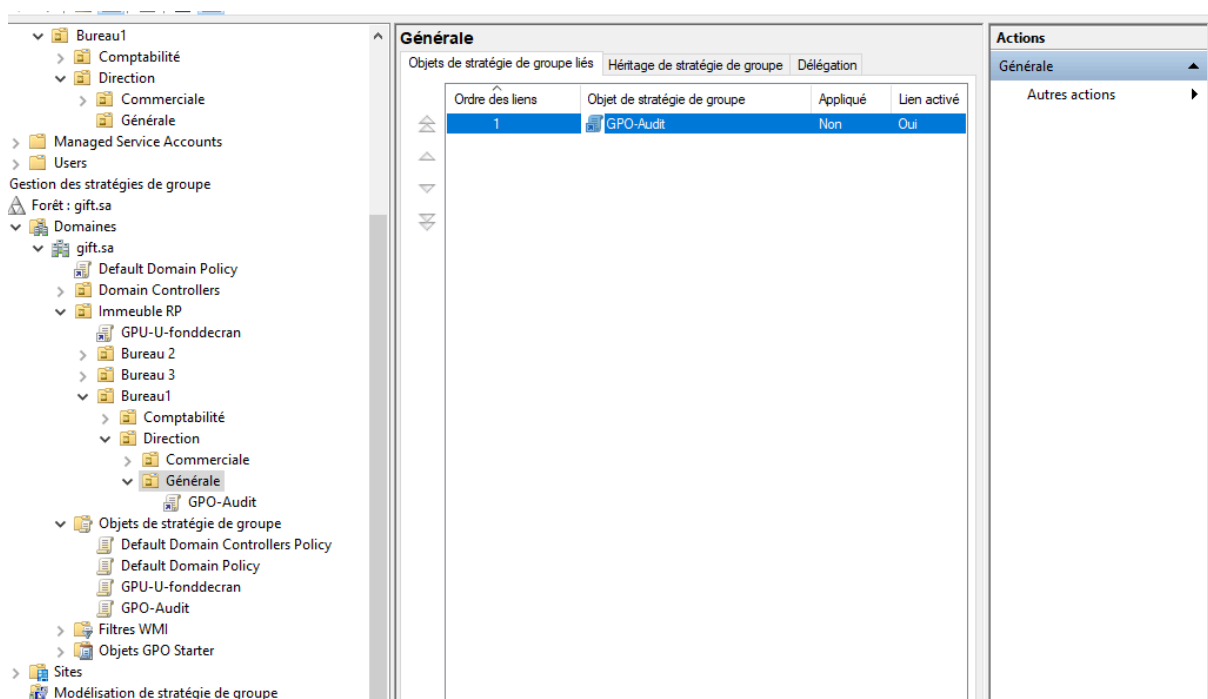
Attribution des Droits

- **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

The screenshot shows the 'Assistant Nouvelle règle de trafic sortant' (New Outgoing Traffic Rule Wizard) in Windows Firewall. The title bar includes the Windows logo and a close button. The main heading is 'Type de règle' (Rule Type), with a subtitle 'Sélectionnez le type de règle de pare-feu à créer.' (Select the type of firewall rule to create.).

On the left, a sidebar titled 'Étapes :' (Steps) lists the wizard's steps: 'Type de règle' (selected with a green dot), 'Protocole et ports' (blue dot), 'Action' (blue dot), 'Profil' (blue dot), and 'Nom' (blue dot).

The main area asks 'Quel type de règle voulez-vous créer ?' (What type of rule do you want to create?). It offers four options:

- ☐ **Programme**
Règle qui contrôle les connexions d'un programme.
- ☒ **Port**
Règle qui contrôle les connexions d'un port TCP ou UDP.
- ☐ **Prédéfinie :**
A dropdown menu shows 'Active Directory Domain Services'. Below it, the text reads: 'Règle qui contrôle les connexions liées à l'utilisation de Windows.'
- ☐ **Personnalisée**
Règle personnalisée.

At the bottom right, there are three buttons: '< Précédent' (disabled), 'Suivant >' (highlighted with a blue border), and 'Annuler' (disabled).

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

faire suivant ,

Assistant Nouvelle règle de trafic sortant

Protocole et ports

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

Étapes :

- Type de règle
- Protocole et ports**
- Action
- Profil
- Nom

Cette règle s'applique-t-elle à TCP ou UDP ?

☒ **TCP**

☐ **UDP**

Cette règle s'applique-t-elle à tous les ports distants ou à des ports distants spécifiques ?

☐ **Tous les ports distants**

☒ **Ports dist. spéc. :**

Exemple : 80, 443, 5000-5010

< Précédent **Suivant >** Annuler

ensuite cocher bloquer la connexion

Assistant Nouvelle règle de trafic sortant

×

Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :

Type de règle

Protocole et ports

Action

Profil

Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

☐ Autoriser la connexion

Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ Autoriser la connexion si elle est sécurisée

Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

Personnaliser...

☒ Bloquer la connexion

< Précédent

Suivant >

Annuler

Nommé la règle et terminer

Nom

Spécifier le nom et la description de cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Nom :

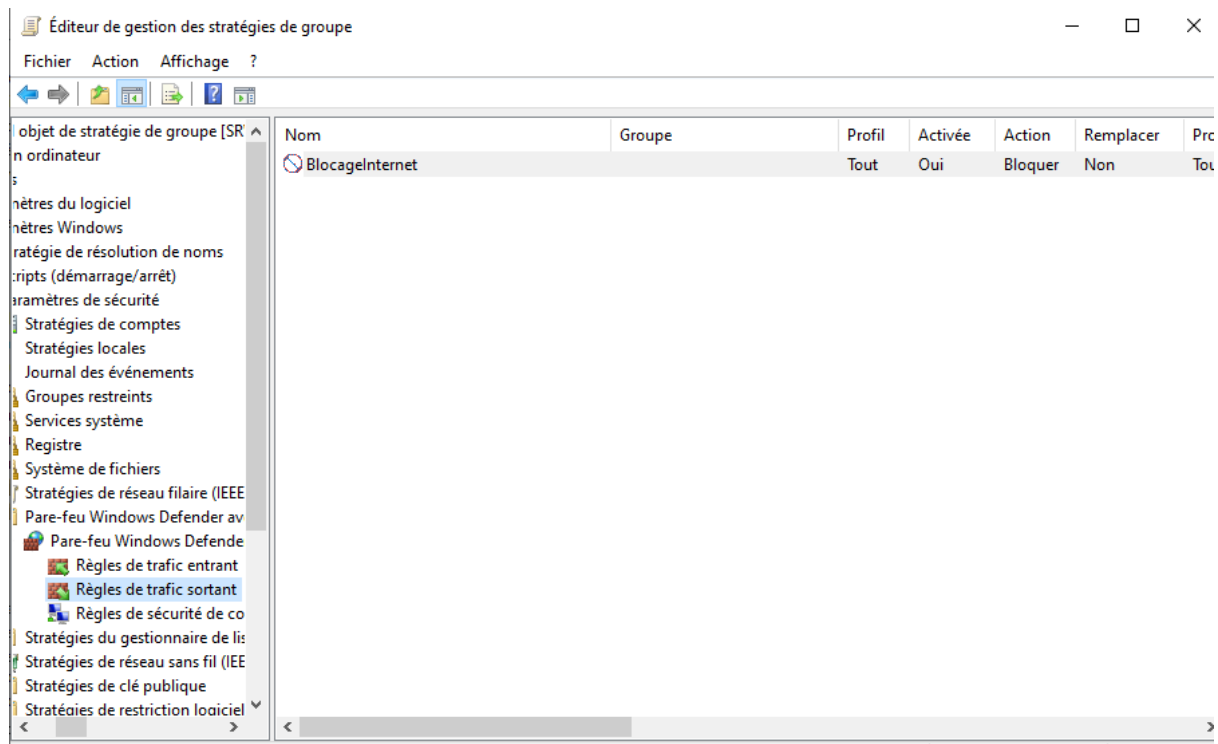
BlocageInternet

Description (facultatif) :

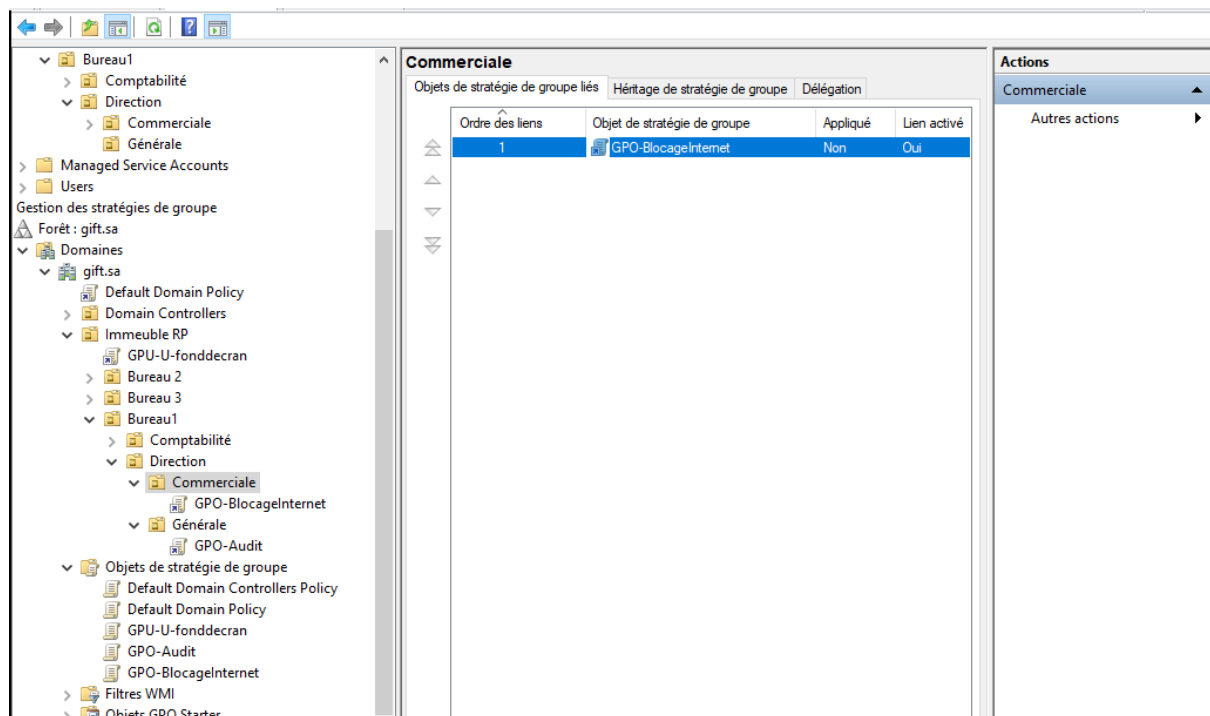
< Précédent

Terminer

Annuler

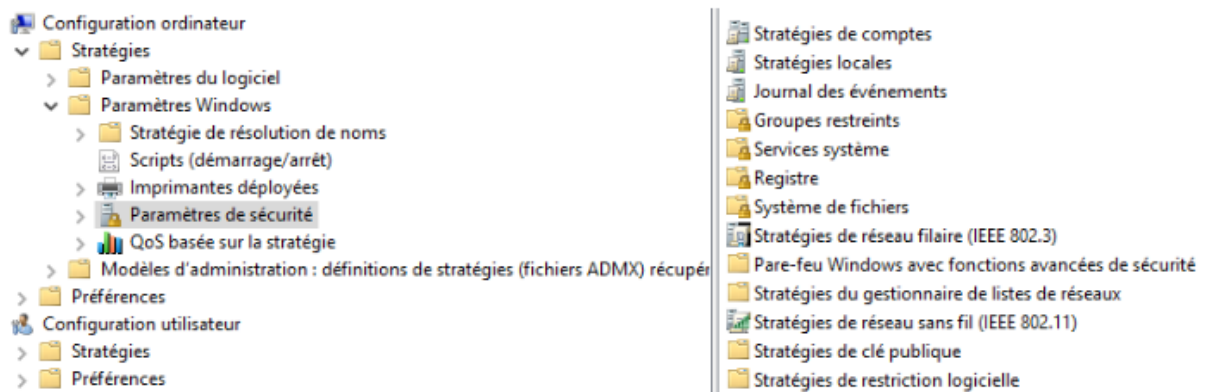


Après avoir créé la GPO je l'ai déplacé vers l'OU Direction , Commerciale

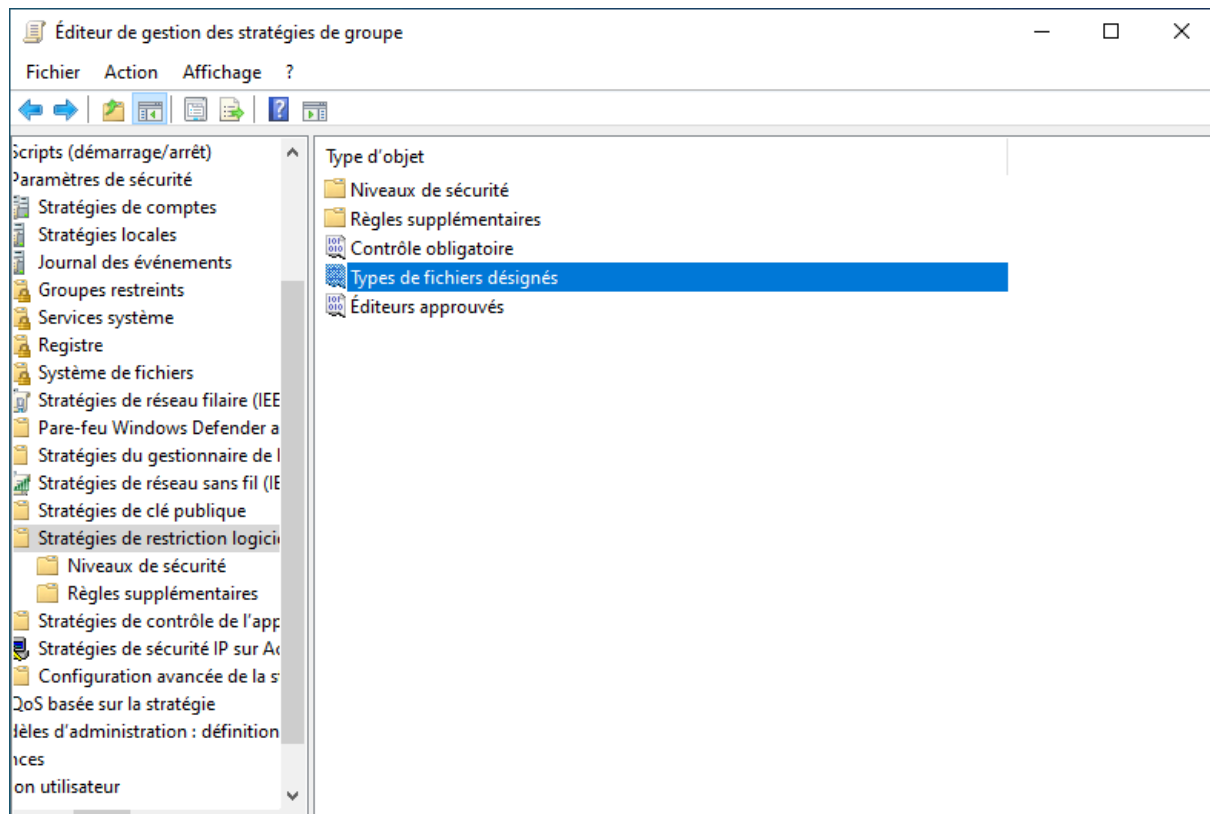


c) restriction de l'exécution de logiciels non autorisées

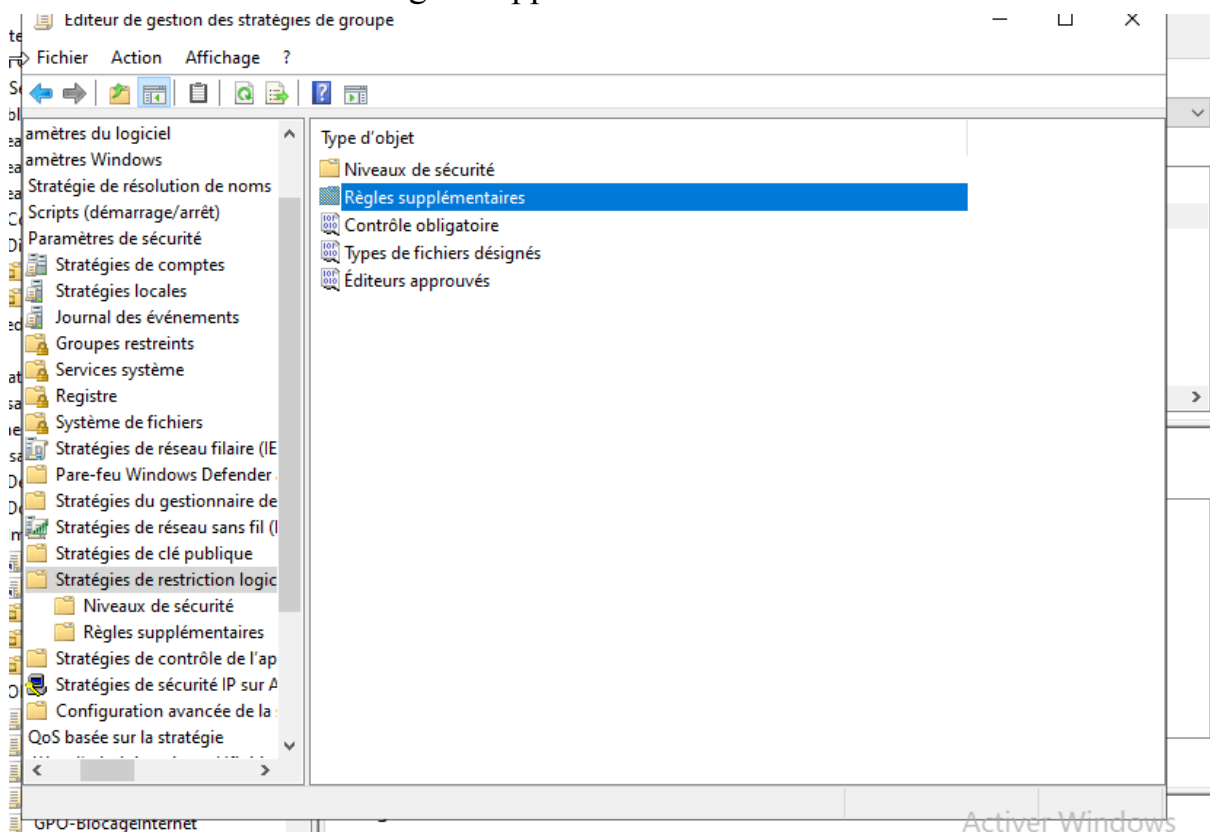
Il est possible de mettre en œuvre simplement une **stratégie de restriction logicielle**, appelée **SRP**, via les GPO. Pour cela il vous faut créer une GPO, et vous rendre dans la partie **Configuration ordinateur**, puis **Paramètres de sécurité**, comme ceci :



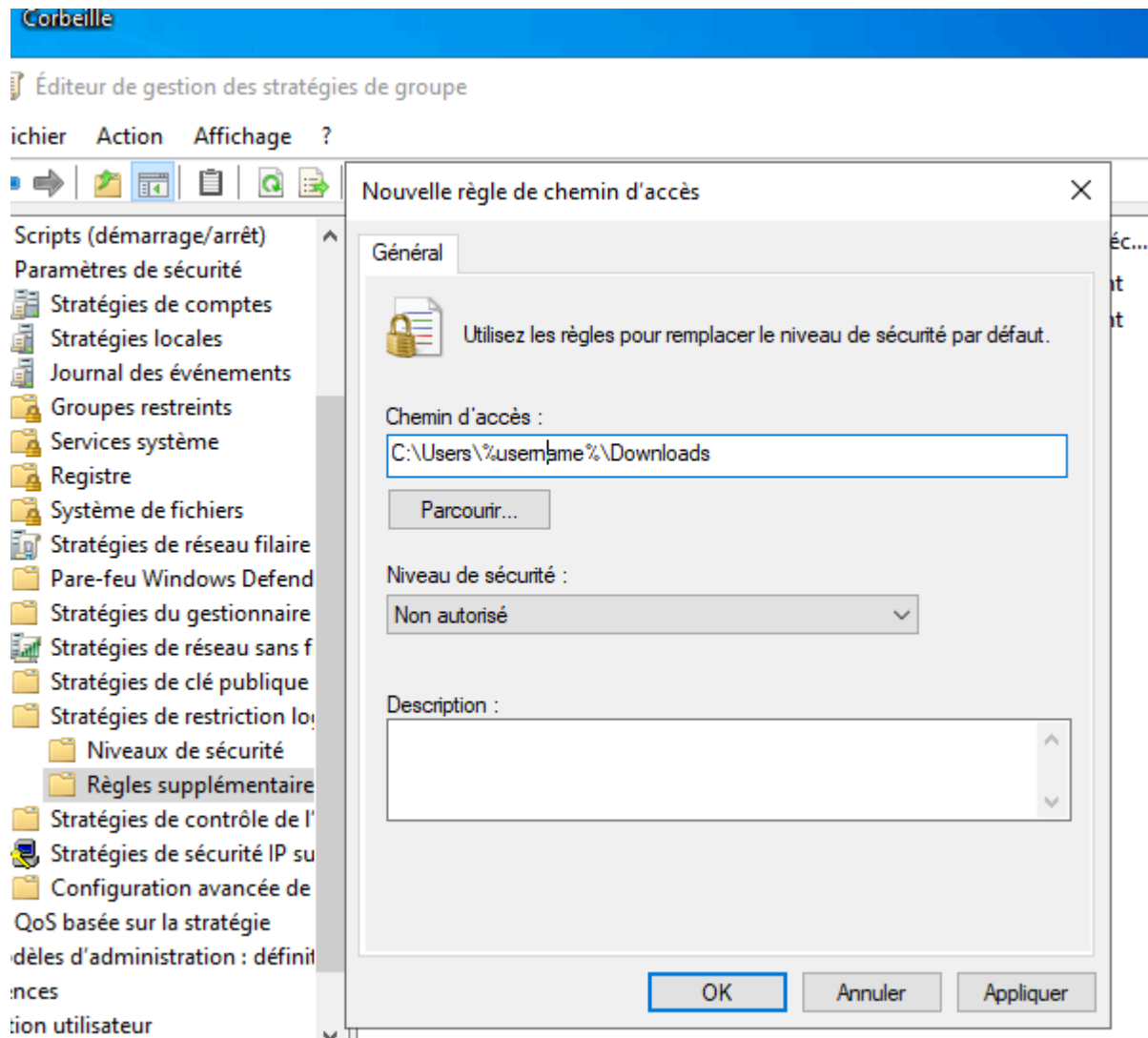
effectuez un clic droit sur le dossier Stratégies de restriction logicielle puis désignez le type de fichiers j'ai choisi les fichiers EXE et MSI



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

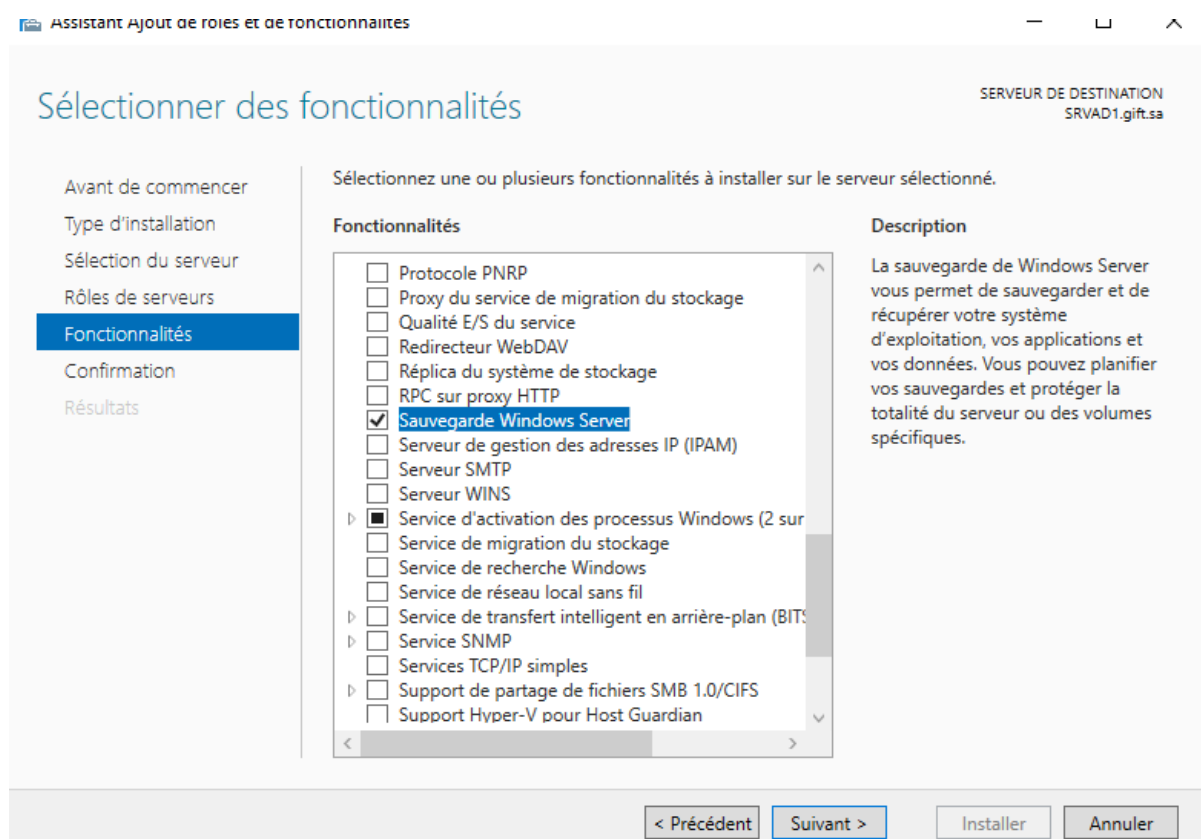
Active Directory est, comme nous l'avons vu précédemment, une véritable base de données. Son emplacement a été défini lors de la promotion du serveur en contrôleur de domaine.

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.

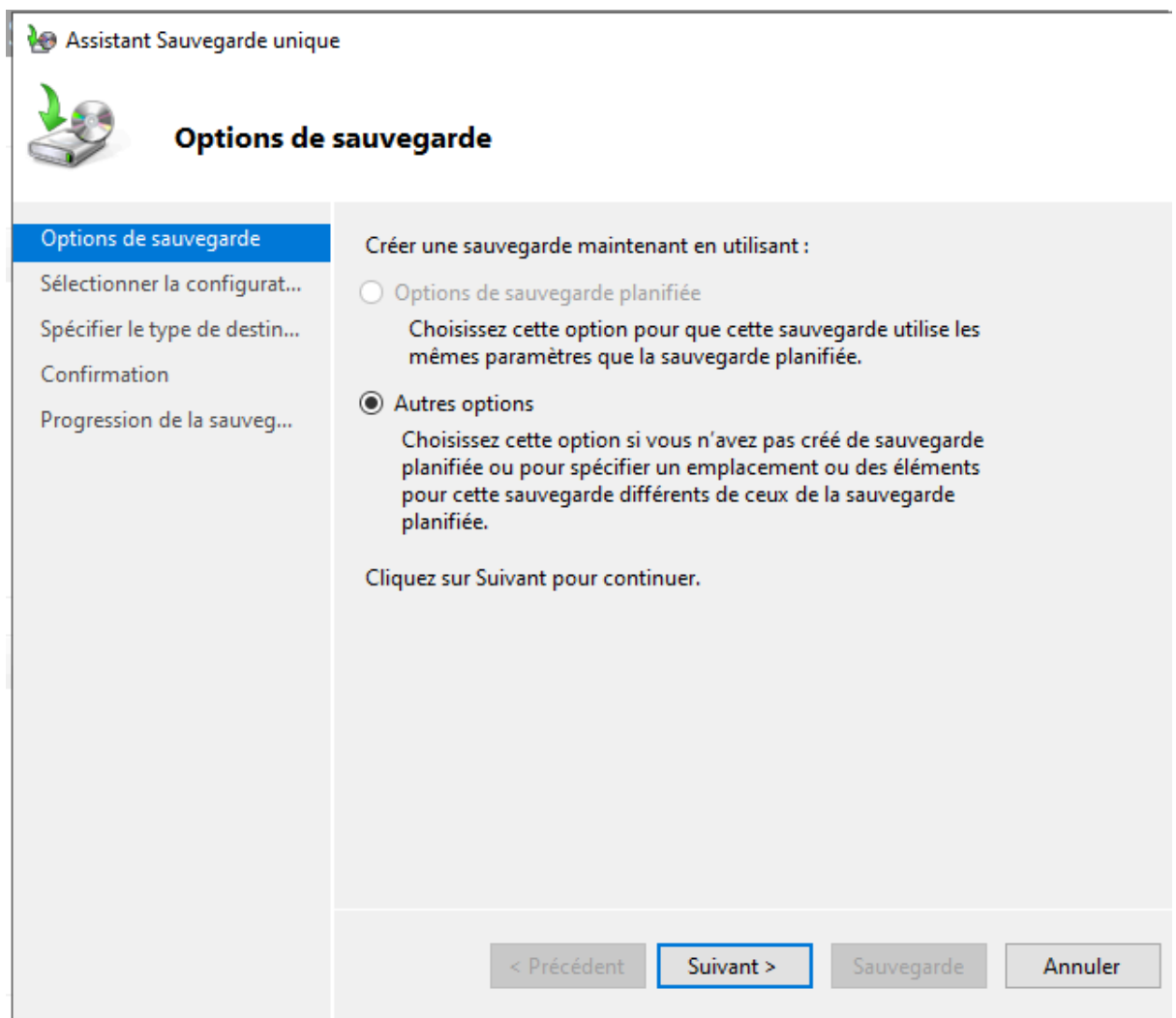
Voici les différentes étapes pour installer l'outil (et donc la fonctionnalité) :

- 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** ;

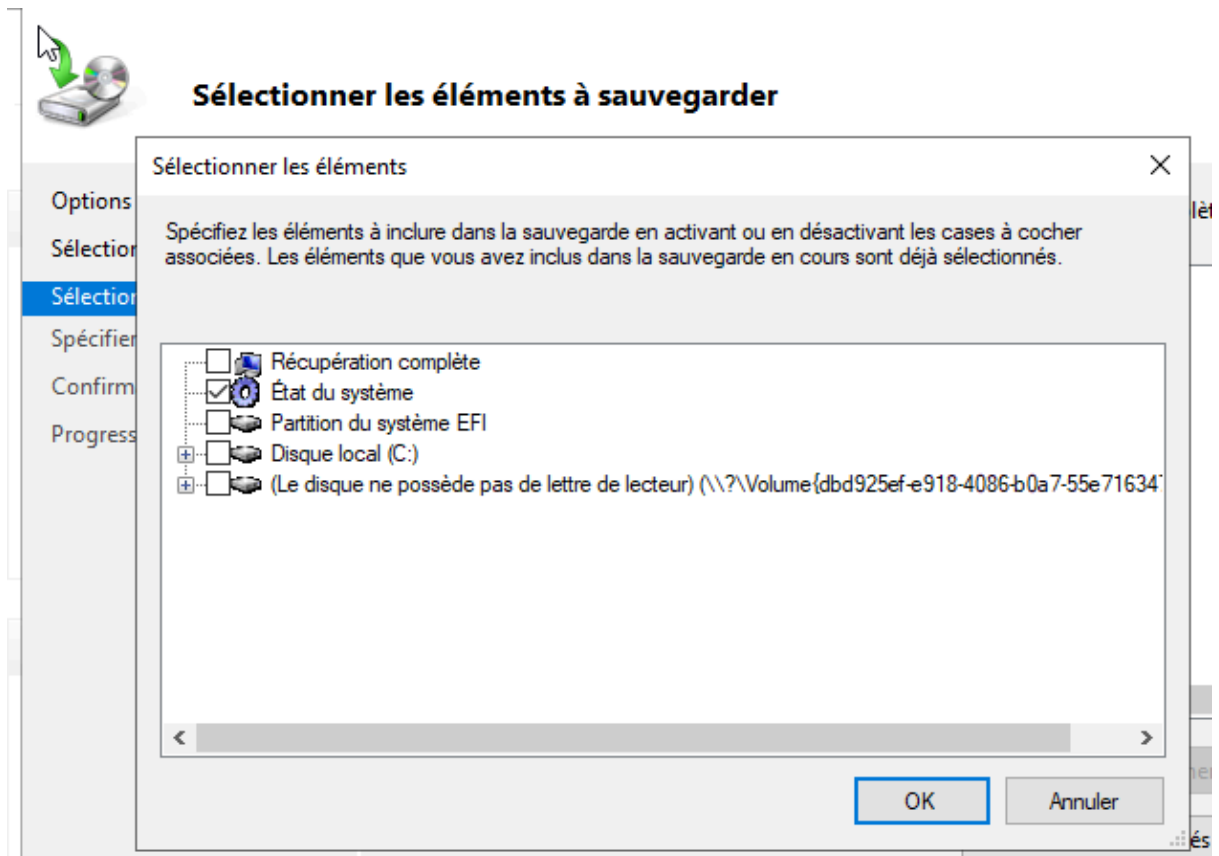


- cliquez sur **Installer** ;
- une fois l'installation terminée, cliquez sur **Fermer**.

- 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