

Documentation raccordement site distant

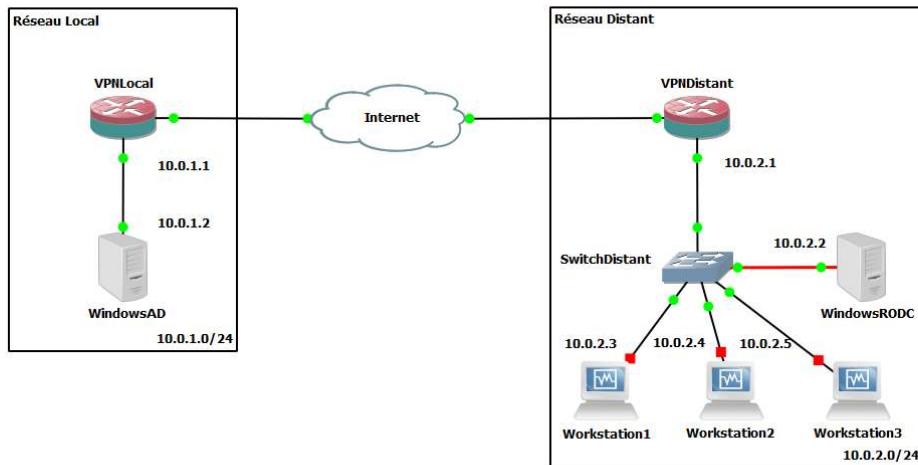
Procédure pas à pas du raccordement site distant

Procédure rédigée par : KEVIN SOUSA

Sommaire

I -Topologie du réseau.....	p-3
II -Configuration des routeurs IPFire.....	p-4
III -Raccordement de WindowsAD et WindowsRODC.....	p-6
IV -Liaison VPN.....	p-8
V -Installation d'Active Directory sur WindowsAD.....	p-15
VI - Promotion du serveur WindowsAD comme contrôleur de domaine.....	p-24
VII -Installation et raccordement du WindowsRODC.....	p-31
VIII -Création des utilisateurs.....	p-32
IX -Mise en place des GPO.....	p-35
A- Politique concernant les fonds d'écran.....	p-38
B- Politique concernant la gestion des firewalls.....	p-45
C- Politique concernant la gestion des mots de passe.....	p-46
D- Politique concernant la gestion des logiciels installés.....	p-47
E- Politique concernant le mappage lecteur réseau.....	p-52

I -Topologie du réseau



WindowsAD :

Serveur Windows Active Directory maître
Adresse 10.0.1.2

WindowsRODC :

Serveur Windows Active Directory miroir
Adresse 10.0.2.2

VPNLocal :

Routeur IPFire utilisant IPSec avec clé partagé pour la liaison VPN
Adresse LAN : 10.0.1.1
Adresse WAN : 192.168.122.194 (DHCP)

VPNDistant :

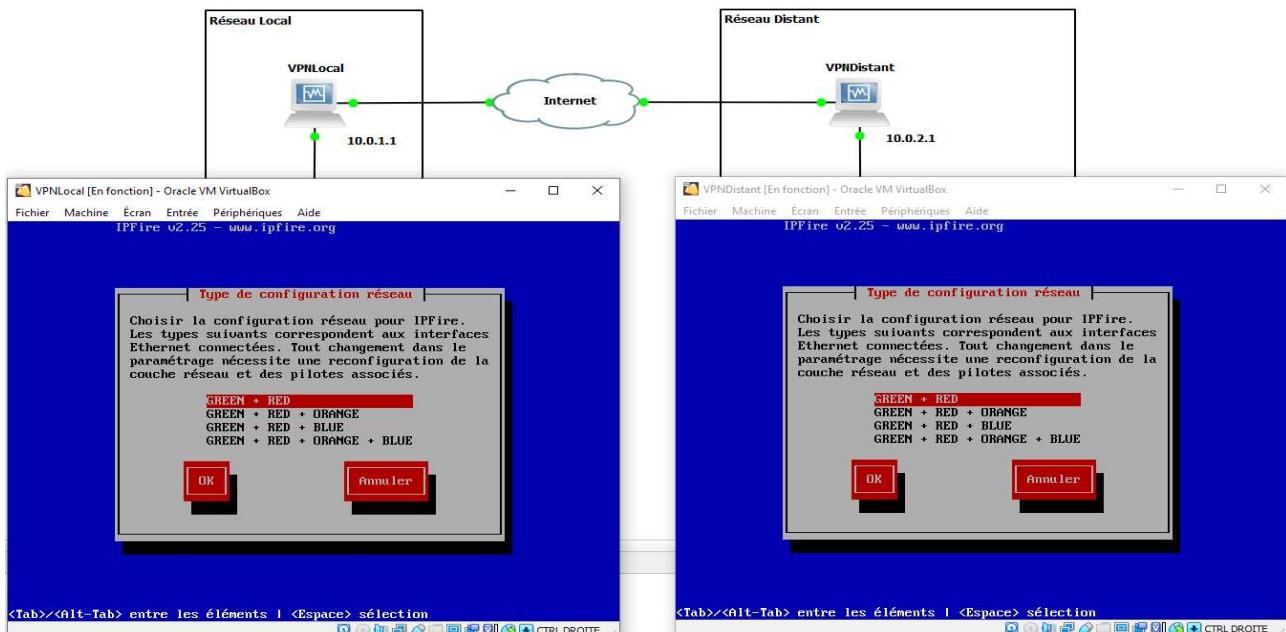
Routeur IPFire utilisant IPSec avec clé partagé pour la liaison VPN
Adresse LAN : 10.0.2.1
Adresse WAN : 192.168.122.175 (DHCP)

Workstation1/Workstation2/Workstation3 :

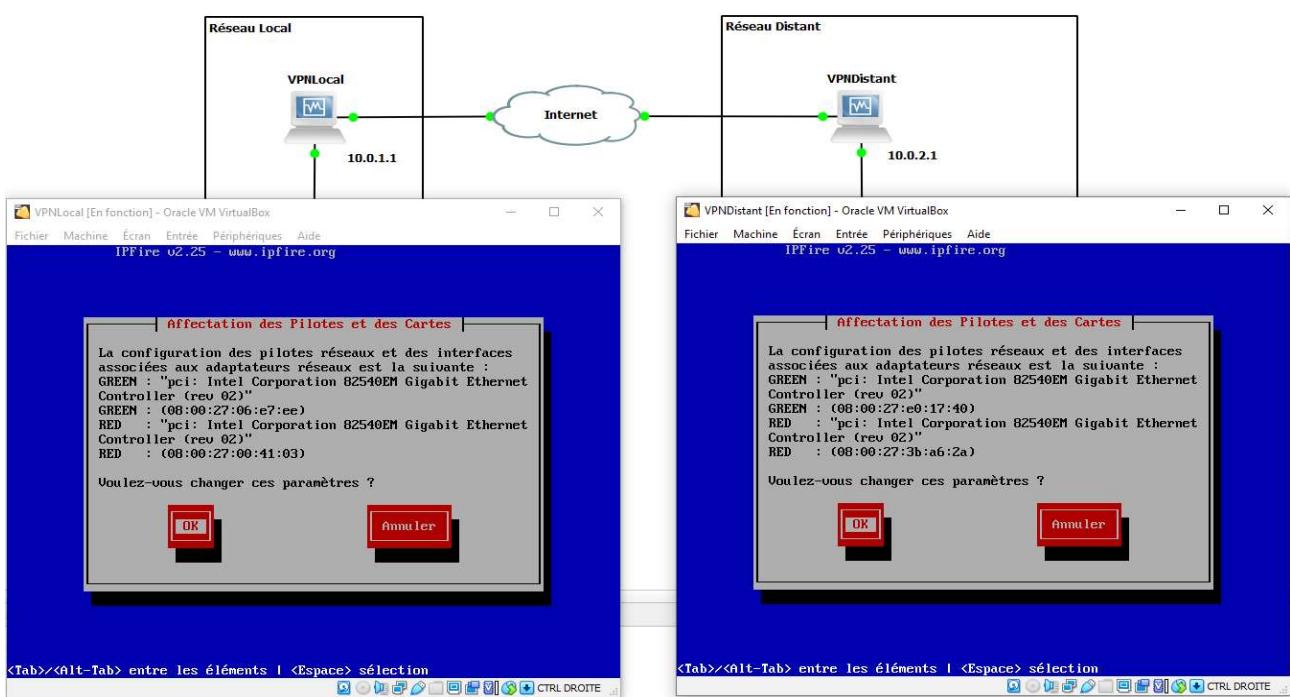
Clients Windows 10
Adresses : 10.0.2.3 / 10.0.2.4 / 10.0.2.5

II -Configuration des routeurs IPFire et de la liaison VPN

Tout d'abord on configure le type de configuration réseau utilisé via la console avec la commande "Setup", ici LAN Green et WAN (Red).

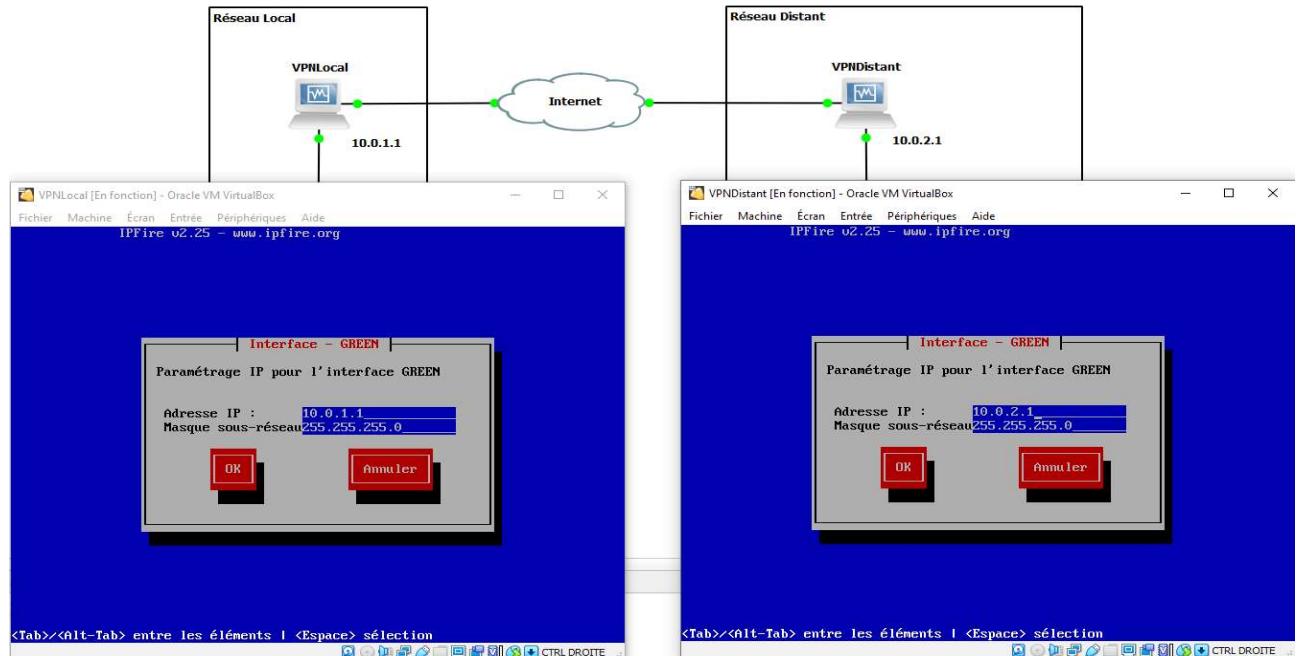


Ensuite on associe les interfaces aux adaptateurs réseaux.

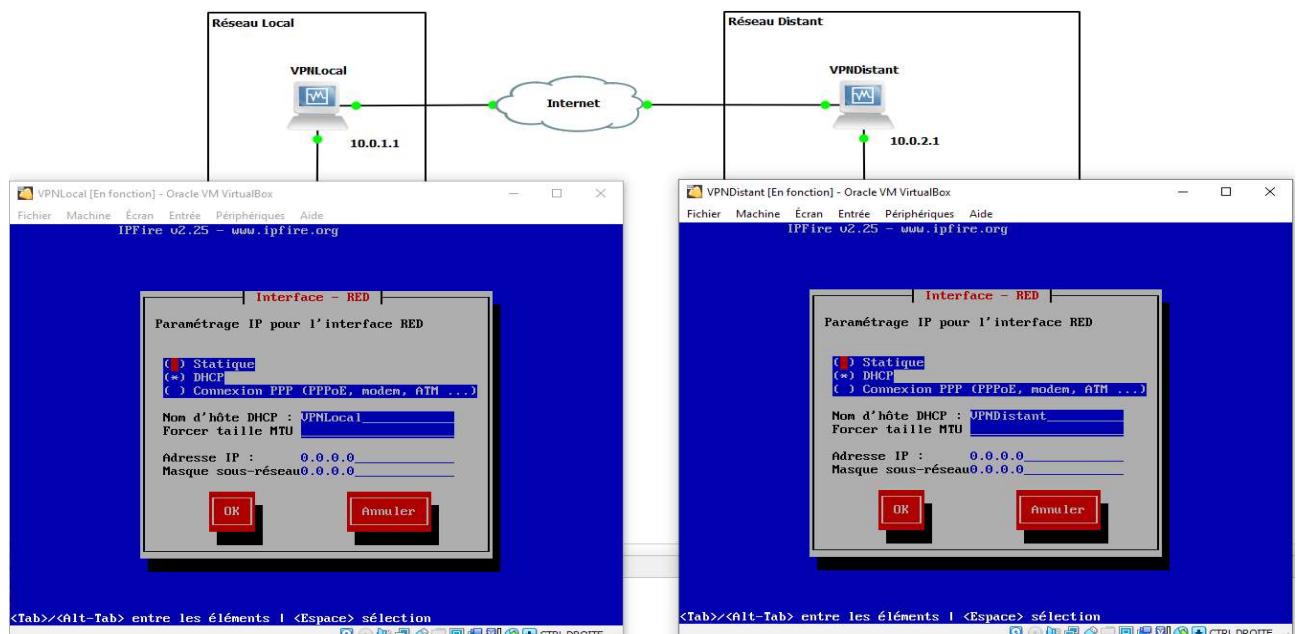


Puis on configure les différentes interfaces.

GREEN



RED

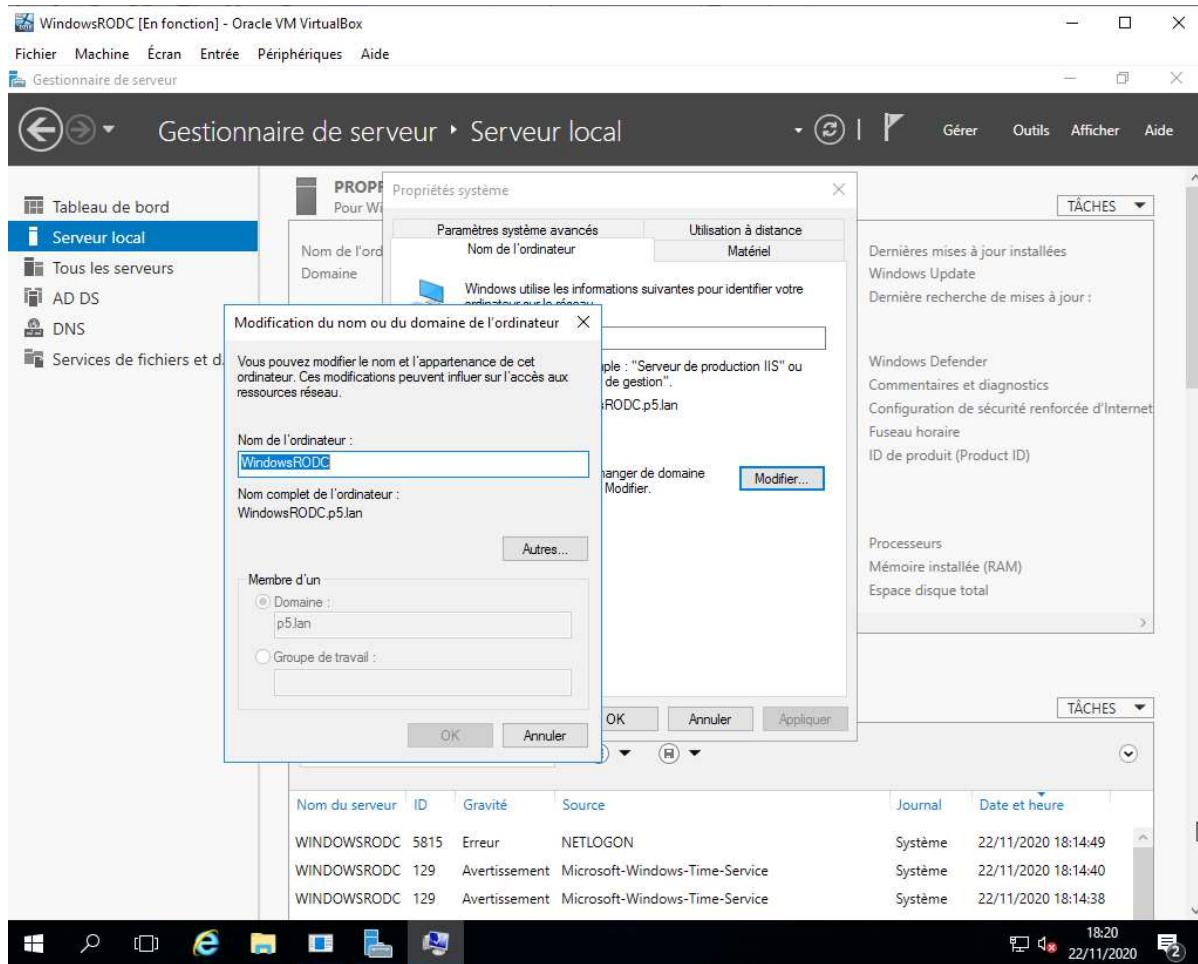


III -Raccordement de WindowsAD et WindowsRODC

Une fois les IPFIREs configurés, on procède à l'installation des différents serveurs windows sur chacun des réseaux privés afin d'utiliser l'interface Web des IPFIREs pour établir la liaison VPN.

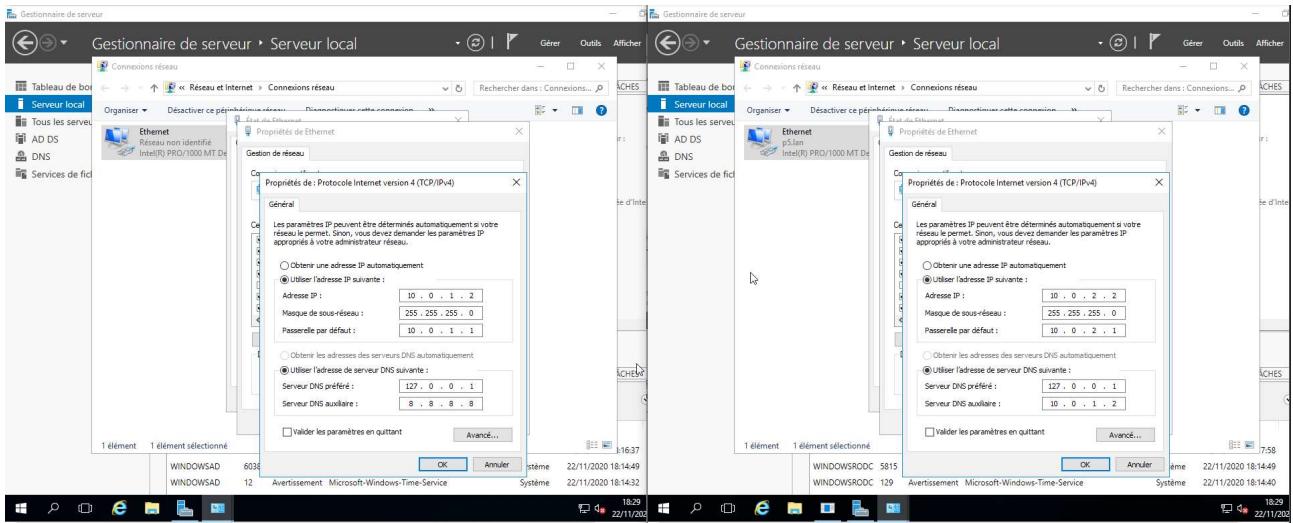
Après l'installation faite, mettre à jour le serveur et modifier le nom de celui.

Pour changer le nom : Serveur Local → double cliquez sur le nom de l'ordinateur → modifier



Faire la manipulation sur les 2 serveurs windows.

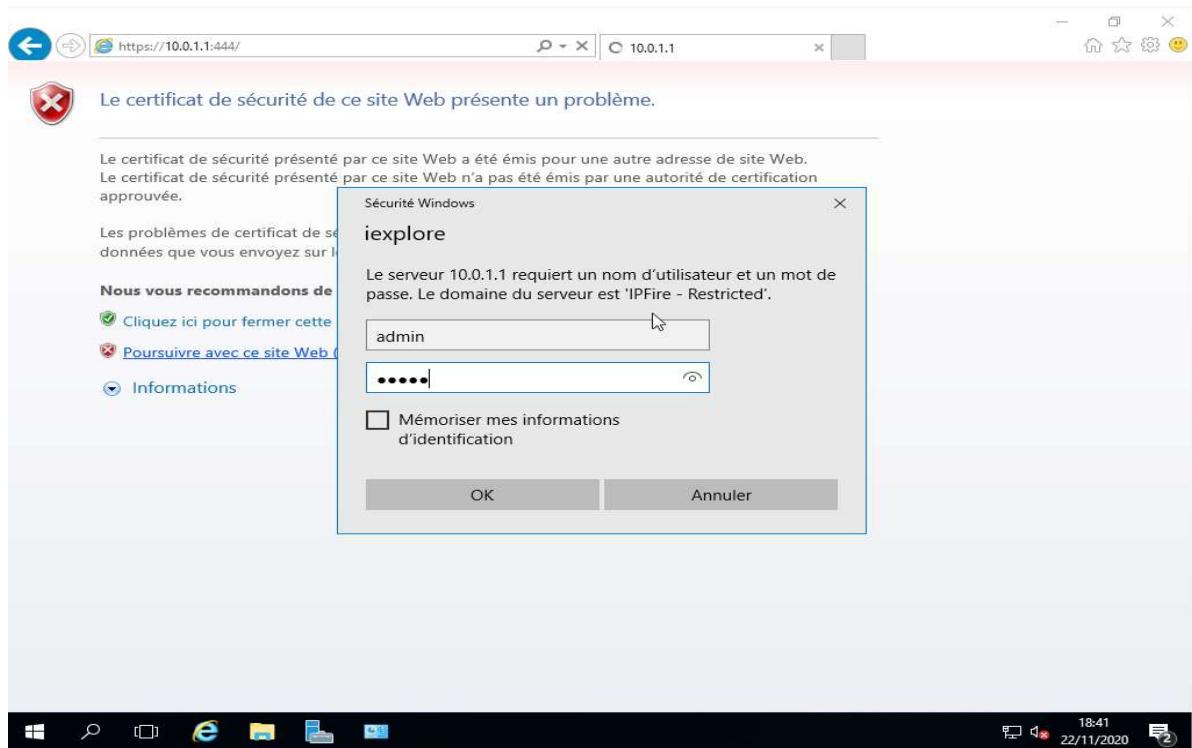
Depuis les serveurs windows, ouvrir le centre de partage et réseaux / Modifier les paramètres de la carte, puis dans les propriétés de la carte, double cliquez sur protocole internet version 4 et rentrez les informations propres au réseau.



Une fois les adresses ip configurées, nous pouvons procéder à la liaison VPN afin de relier les sites entre eux.

IV -Liaison VPN

On configure la connexion IPSec sur chaque routeur IPFire via l'interface Web de chacun des IPFIRE depuis les serveurs windows. Pour cela rentrez l'URL des IPFIREs dans un navigateur web:
Exemple: <https://10.0.1.1:444/> (IPFIRE site local)



Entrez l'utilisateur admin précédemment configurer lors de l'installation des IPFIREs. Ce qui nous donne accès à l'interface web.

The screenshot shows the IPFire web interface at <https://10.0.1.1:444/cgi-bin/index.cgi>. The title bar indicates an SSL certificate error. The main page displays network status and a VPN connection.

Network Status:

Réseau	Adresse IP	Statut
INTERNET	192.168.122.194 VPNLocal.p5.lan 192.168.122.1	Connecté - (30m 35s)
LAN	10.0.1.1/24	Proxy éteint
IPsec		Online

VPN:

Réseau IPsec	Adresse IP	Statut
VPNLocal	10.0.2.0/24	CONNECTÉ

Bottom status bar: IPFire 2.25 (x86_64) - Core Update 149, IPFire.org • Soutenez le projet IPFire avec votre don, 18:45, 22/11/2020.

Nous pouvons donc maintenant faire la liaison VPN. Pour cela, allez dans Services → Ipsec

- Dans configuration générale cocher la case Activé.
- Dans Etat et contrôle de connexion, cliquez sur Ajouter.

The screenshot shows a web-based IPsec configuration interface with the following sections:

- Configuration générale:** Shows the "Activé" (Enabled) checkbox checked, and the "Réseau privé virtuel (VPN) de l'hôte au réseau (client nomade)" field set to "VPNDistant.p5.lan - IPsec". A "Sauvegarder" (Save) button is visible.
- Etat et contrôle de connexion :** A table listing connections:

Nom	Type	Nom courant	Remarque	Statut	Action
VPNDistant	Réseau (PSK) ikev2			CONNECTÉ	<input checked="" type="checkbox"/>

Legend: Activé (déscocher pour désactiver) Afficher le certificat Modifier Enlever
 Désactivé (cocher pour activer) Télécharger le certificat Relancer

A "Ajouter" (Add) button is located at the bottom right.
- Autorité de certification:** A table listing certificate authorities:

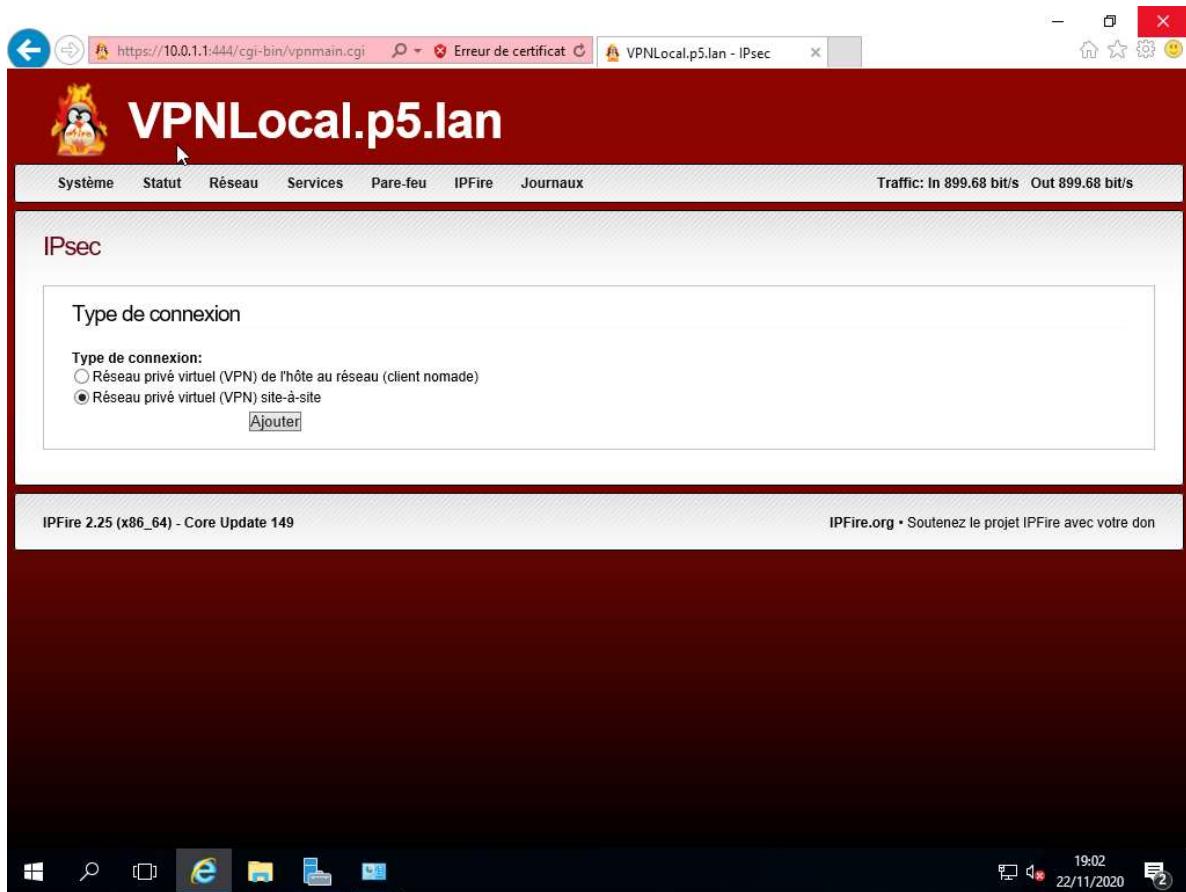
Nom	Sujet	Action
Certificat root	C = FR O = MyVPN CN = MyVPN CA	
Certificat hôte	C = FR O = MyVPN CN = VPNDistant.p5.lan	

Legend: Afficher le certificat Télécharger le certificat

Fields: Nom CA : * Parcourir...

Note: La réinitialisation de la configuration VPN va supprimer le CA root, le certificat hôte et tous les certificats basés sur les connexions :

- Dans type de connexion, selectionnez Réseau privé virtuel (VPN) site-à-site, puis Ajouter.



Puis configurer la connexion selon vos machines et réseaux.

The screenshot shows the configuration interface for the VPNLocal.p5.lan device. The main window title is "VPNLLocal.p5.lan". The top menu bar includes "Système", "Statut", "Réseau", "Services", "Pare-feu", "IPFire", and "Journaux". The status bar at the bottom indicates "Traffic: In 479.49 bit/s Out 479.49 bit/s".

Connexion: VPNLLocal

Activé :

Adresse IP locale:

Sous-réseau local : *

ID Local:

Hôte/IP distant: *

Sous-réseau distant : *

ID distant:

Remarque :

Paramètres IPsec

Mode:

Mode d'interface:

MTU:

Adresse IP /Masque de sous-réseau:

Authentification :

Utiliser une clé pré-partagée :

Connexion: VPNDistant

Activé :

Adresse IP locale:

Sous-réseau local : *

ID Local:

Hôte/IP distant: *

Sous-réseau distant : *

ID distant:

Remarque :

Paramètres IPsec

Mode:

Mode d'interface:

MTU:

Adresse IP /Masque de sous-réseau:

Authentification :

Utiliser une clé pré-partagée :

Sauvegarder **Avancé** **Annuler**

The screenshot shows the configuration interface for the VPNDistant.p5.lan device. The main window title is "VPNDistant.p5.lan". The top menu bar includes "Système", "Statut", "Réseau", "Services", "Pare-feu", "IPFire", and "Journaux". The status bar at the bottom indicates "Traffic: In 483.57 bit/s Out 483.57 bit/s".

Connexion: VPNDistant

Activé :

Adresse IP locale:

Sous-réseau local : *

ID Local:

Hôte/IP distant: *

Sous-réseau distant : *

ID distant:

Remarque :

Paramètres IPsec

Mode:

Mode d'interface:

MTU:

Adresse IP /Masque de sous-réseau:

Authentification :

Utiliser une clé pré-partagée :

Sauvegarder **Avancé** **Annuler**

On s'assure que la liaison est activé.

VPNLocal.p5.lan

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 0.00 bit/s Out 0.00 bit/s

IPsec

Configuration générale

Activé : Réseau privé virtuel (VPN) de l'hôte au réseau (client nomade) : Sauvegarder

Etat et contrôle de connexion :

Nom	Type	Nom courant	Remarque	Statut	Action
VPNLocal	Réseau (PSK) ikev2			CONNECTÉ	

Légende : Activé (décocher pour désactiver) Afficher le certificat Modifier Enlever
 Désactivé (cocher pour activer) Télécharger le certificat Relancer Ajouter

VPNDistant.p5.lan

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 245.88 bit/s Out 245.88 bit/s

IPsec

Configuration générale

Activé : Réseau privé virtuel (VPN) de l'hôte au réseau (client nomade) : Sauvegarder

Etat et contrôle de connexion :

Nom	Type	Nom courant	Remarque	Statut	Action
VPNDistant	Réseau (PSK) ikev2			CONNECTÉ	

Légende : Activé (décocher pour désactiver) Afficher le certificat Modifier Enlever
 Désactivé (cocher pour activer) Télécharger le certificat Relancer Ajouter

On procède à une vérification du trafic avec Wireshark

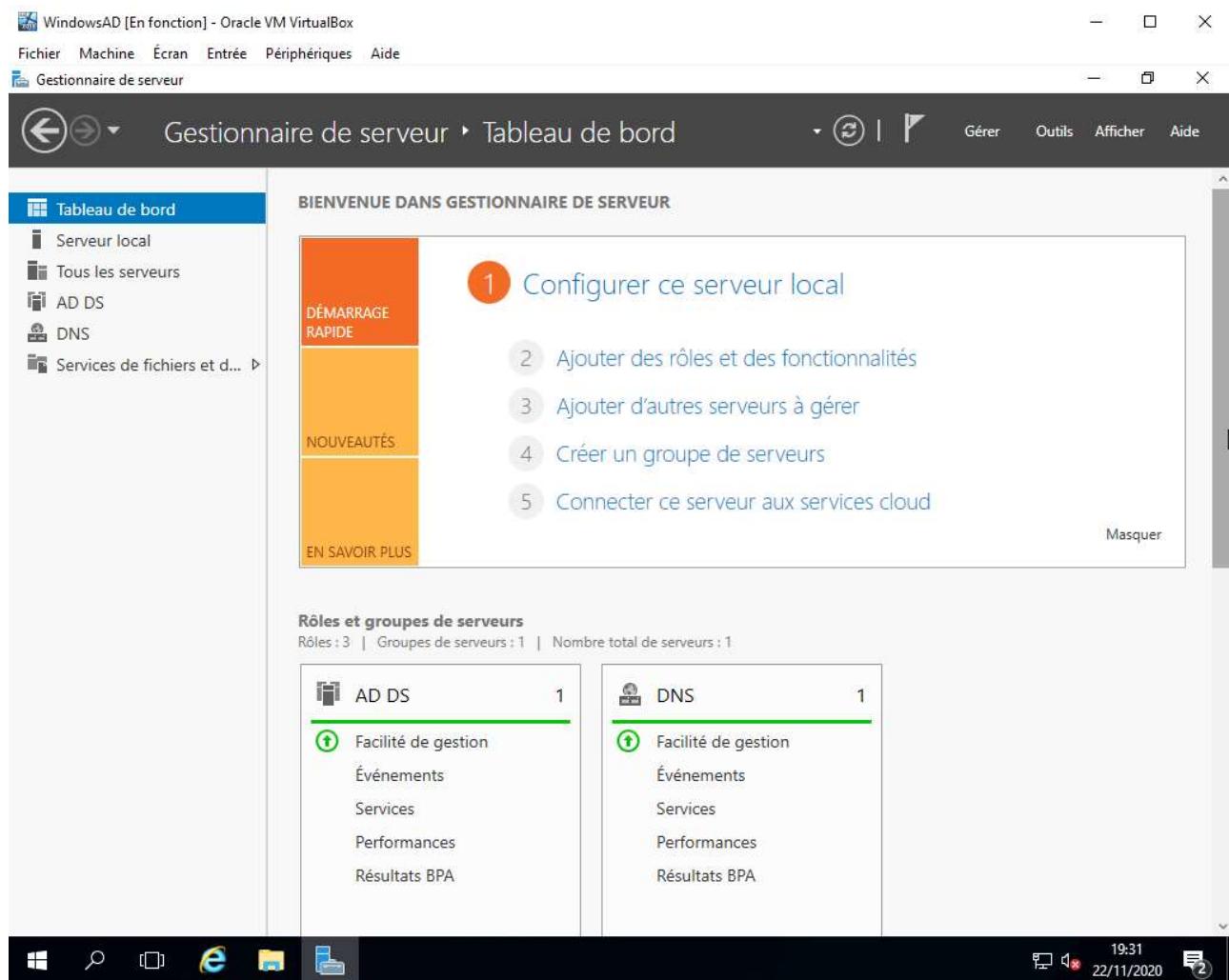
On constate que tous les paquets transitant entre nos 2 réseaux privés sont chiffrés via le protocole ESP

The screenshot shows the Wireshark interface with the following details:

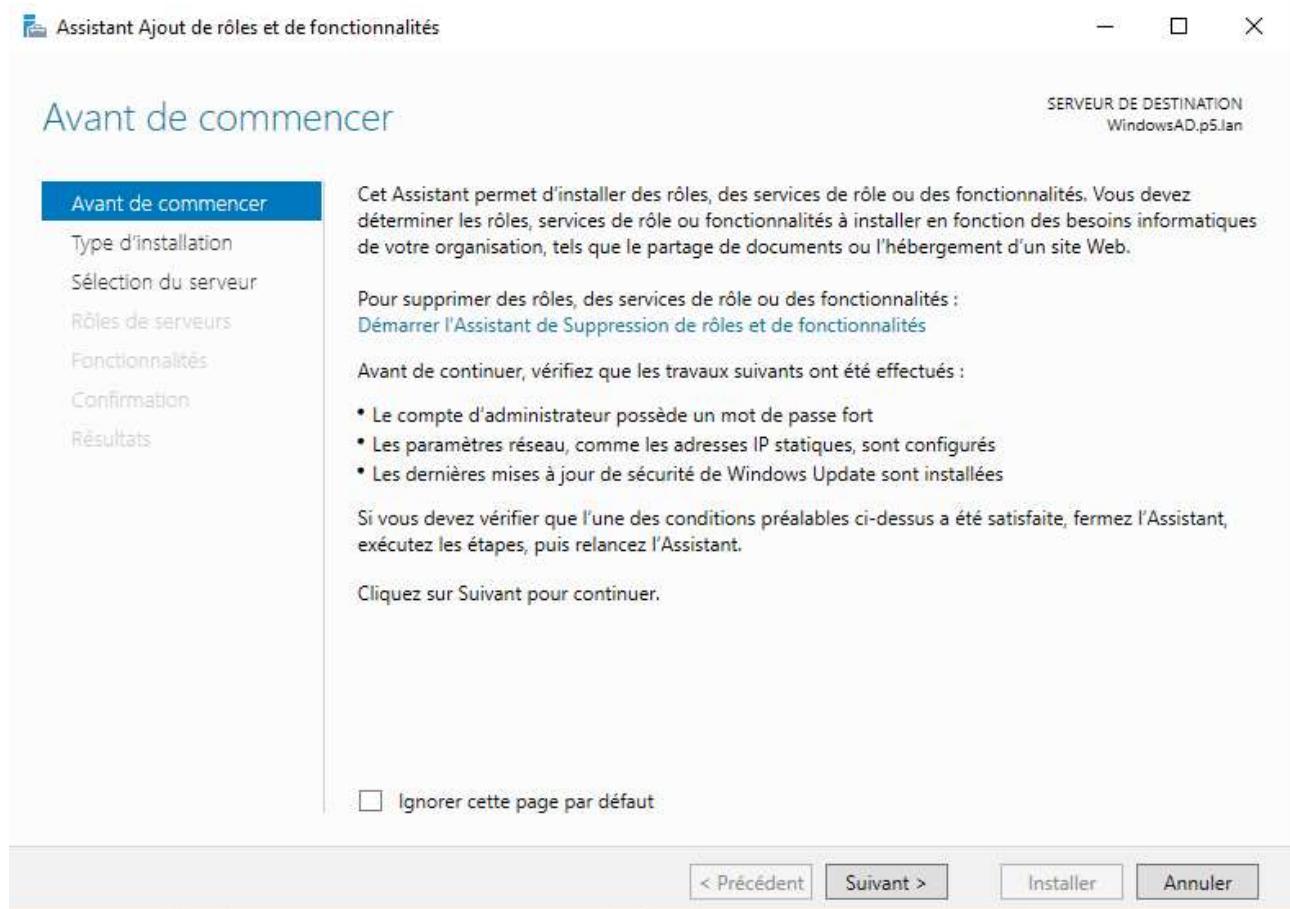
- Title Bar:** *-[VPNDistant Ethernet0 to Internet nat0]
- Menu Bar:** Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Téléphonie, Sans fil, Outils, Aide
- Toolbar:** Includes icons for file operations, search, and analysis.
- Search Bar:** Apply a display filter ... <Ctrl-/>
- Table:** Displays network traffic in a tabular format with columns: No., Time, Source, Destination, Protocol, Length, Info.
- Data:** The table shows several rows of traffic, with row 9 highlighted in grey. The "Info" column for row 9 indicates an ESP (Encapsulating Security Payload) packet with SPI values 0xc9910cd5 and 0xc9fb5ffd.
- Bottom Panel:** Shows expanded details for selected frame 9, including:
 - Frame 9: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface -, id 0
 - Ethernet II, Src: PcsCompu_3b:a6:2a (08:00:27:3b:a6:2a), Dst: PcsCompu_00:41:03 (08:00:27:00:41:03)
 - Internet Protocol Version 4, Src: 192.168.122.175, Dst: 192.168.122.194
 - Encapsulating Security Payload

V -Installation d'Active Directory sur WindowsAD

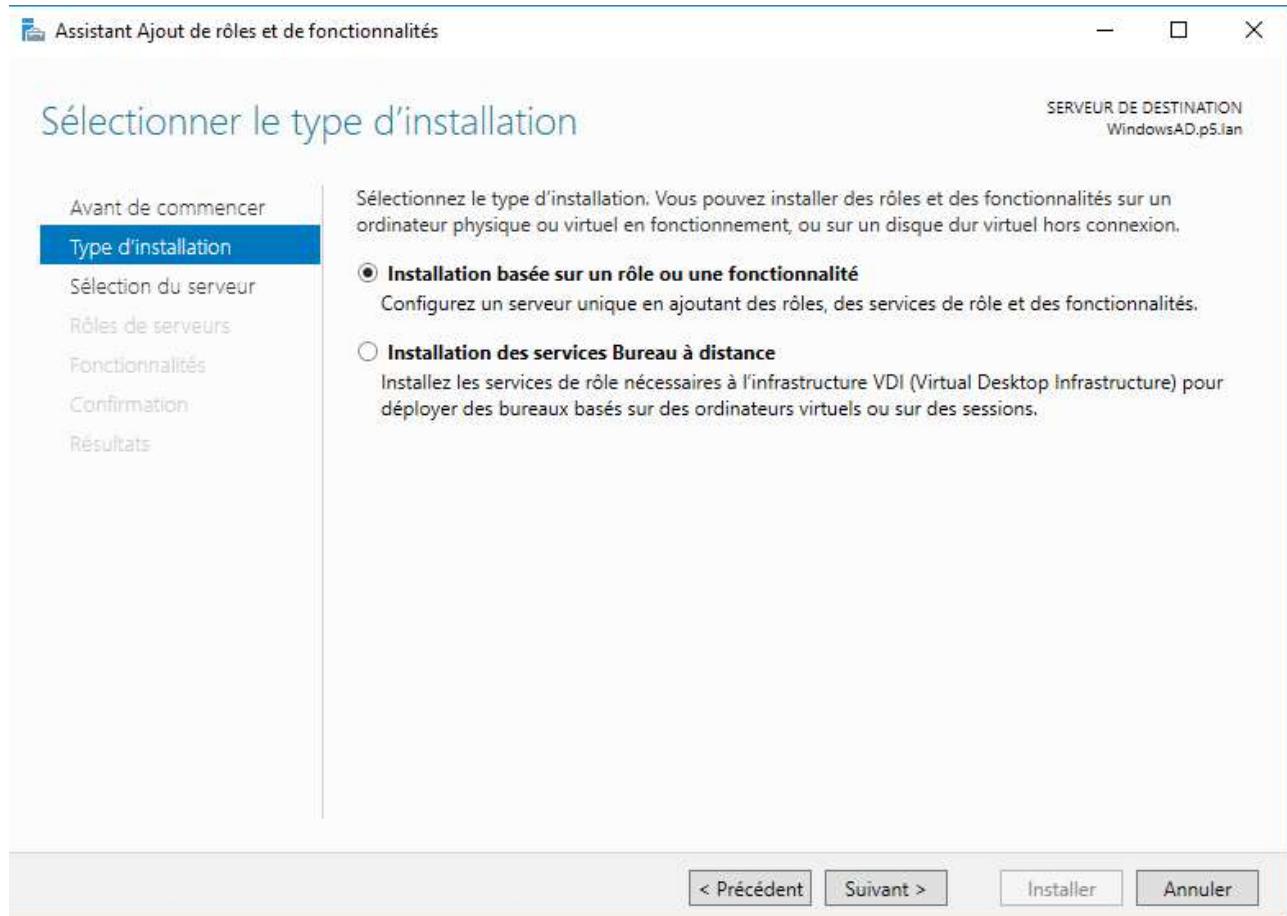
Sur WindowsAD, ouvrir le gestionnaire de serveur et cliquez sur Ajouter des rôles et des fonctionnalités.



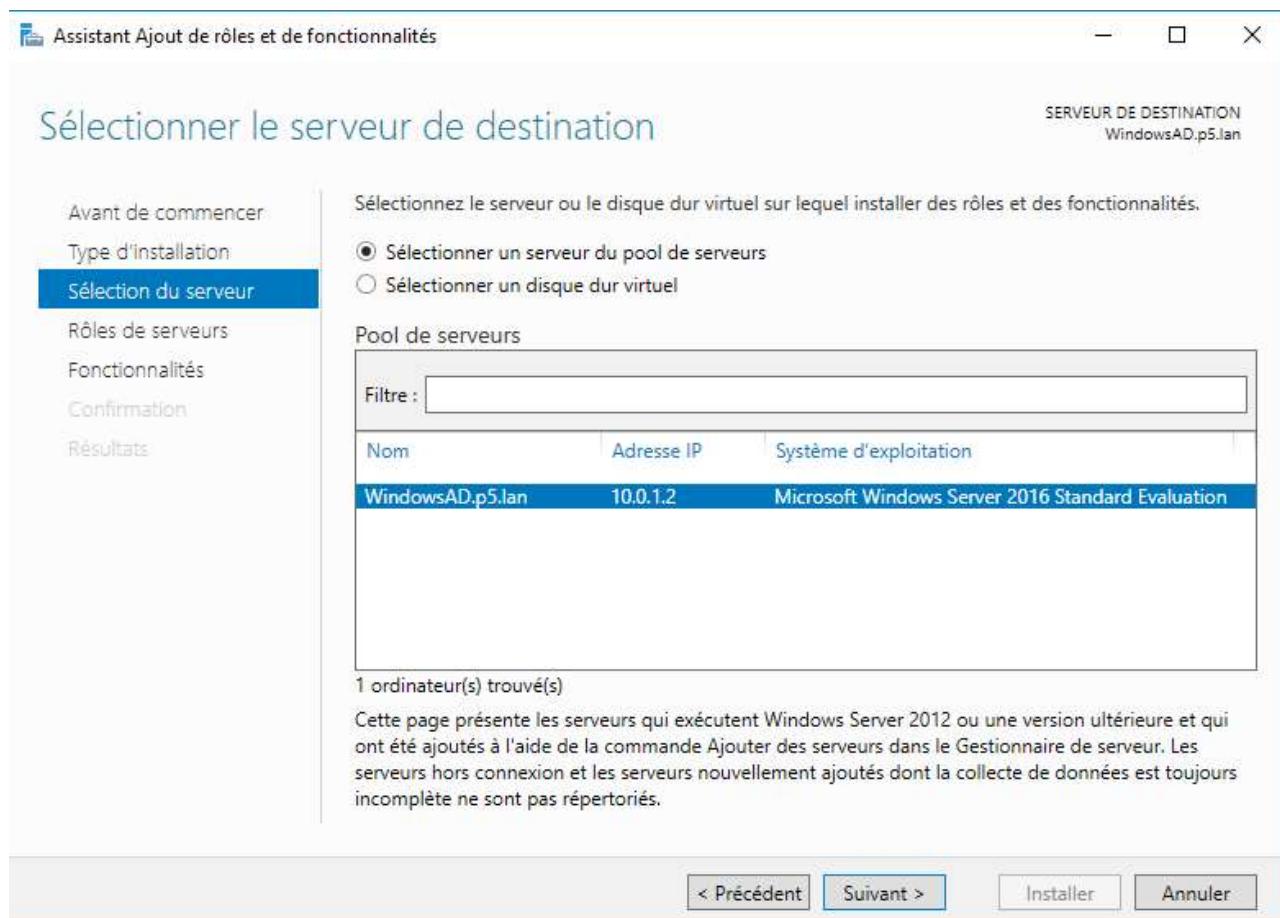
Au lancement de l'assistant, cliquez sur "Suivant"



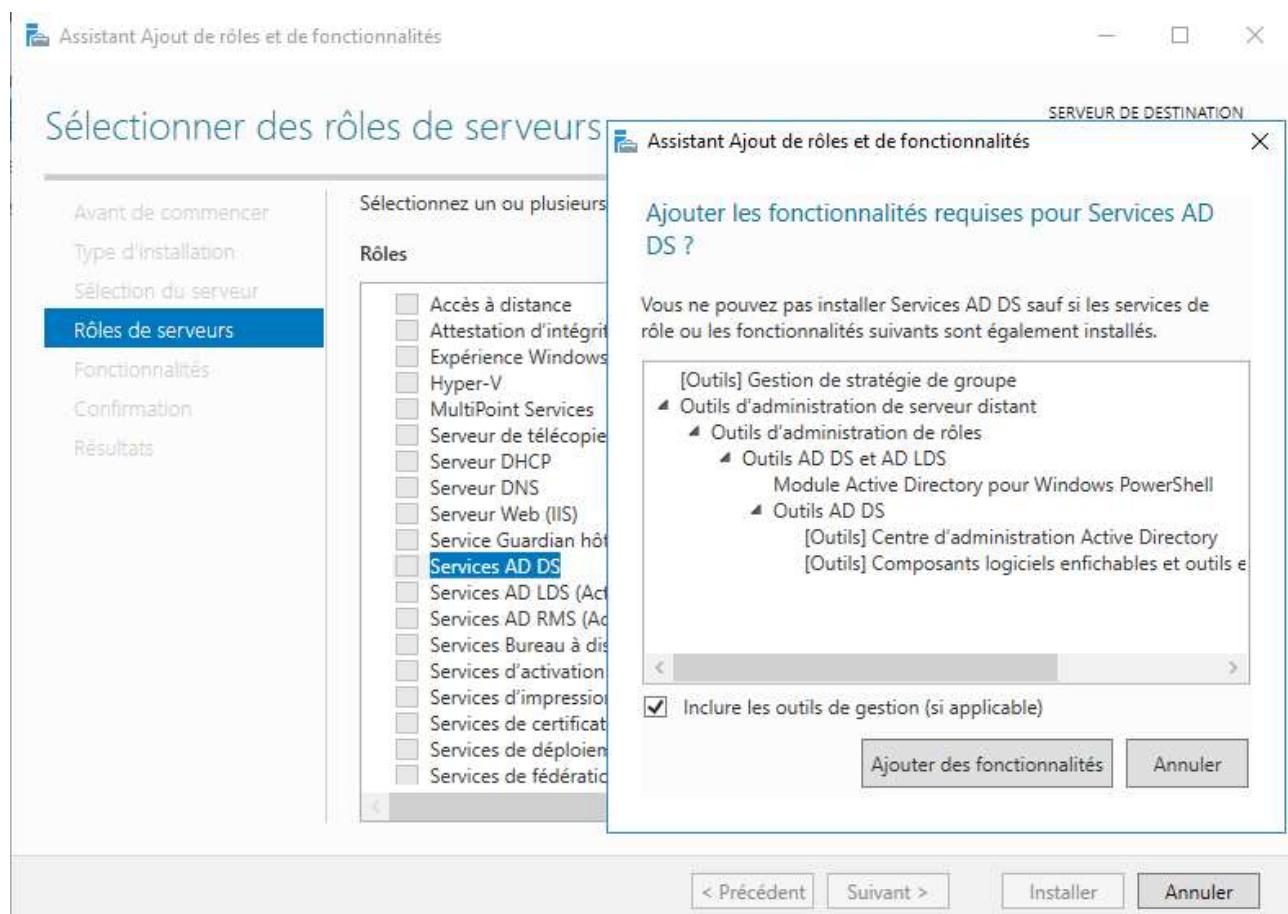
Sélectionnez Installation basée sur un rôle ou une fonctionnalité et cliquez sur “Suivant”



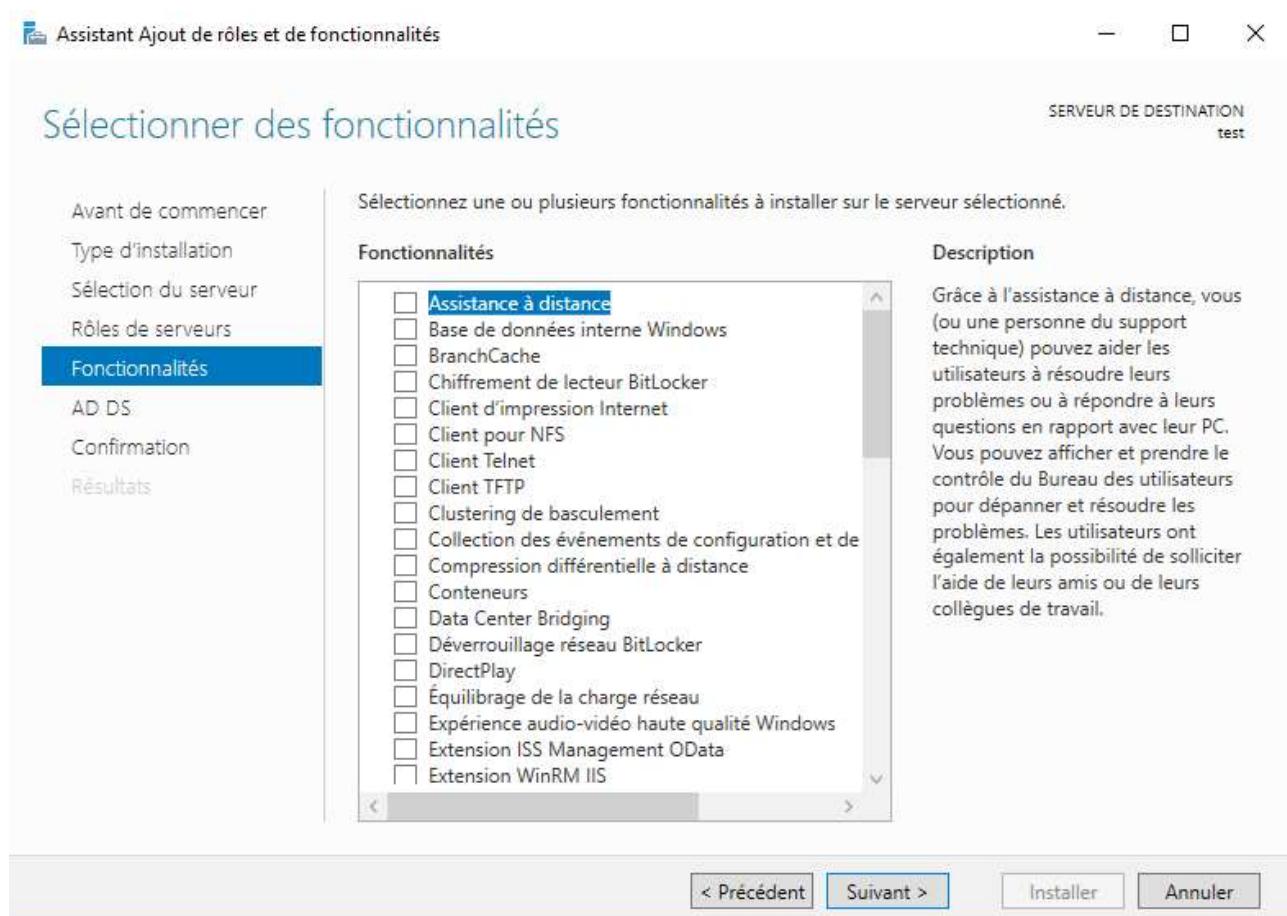
Choisir le serveur où le rôle AD DS va être installé et cliquez sur “Suivant”.



Dans la liste des rôles, cocher la case Service AD DS et ajoutez les fonctionnalités.



Passez la liste des fonctionnalités en cliquant sur “Suivant”.



Le résumé du rôle AD DS s'affiche, cliquez sur "Suivant"

Assistant Ajout de rôles et de fonctionnalités

Services de domaine Active Directory

SERVEUR DE DESTINATION
test

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs.

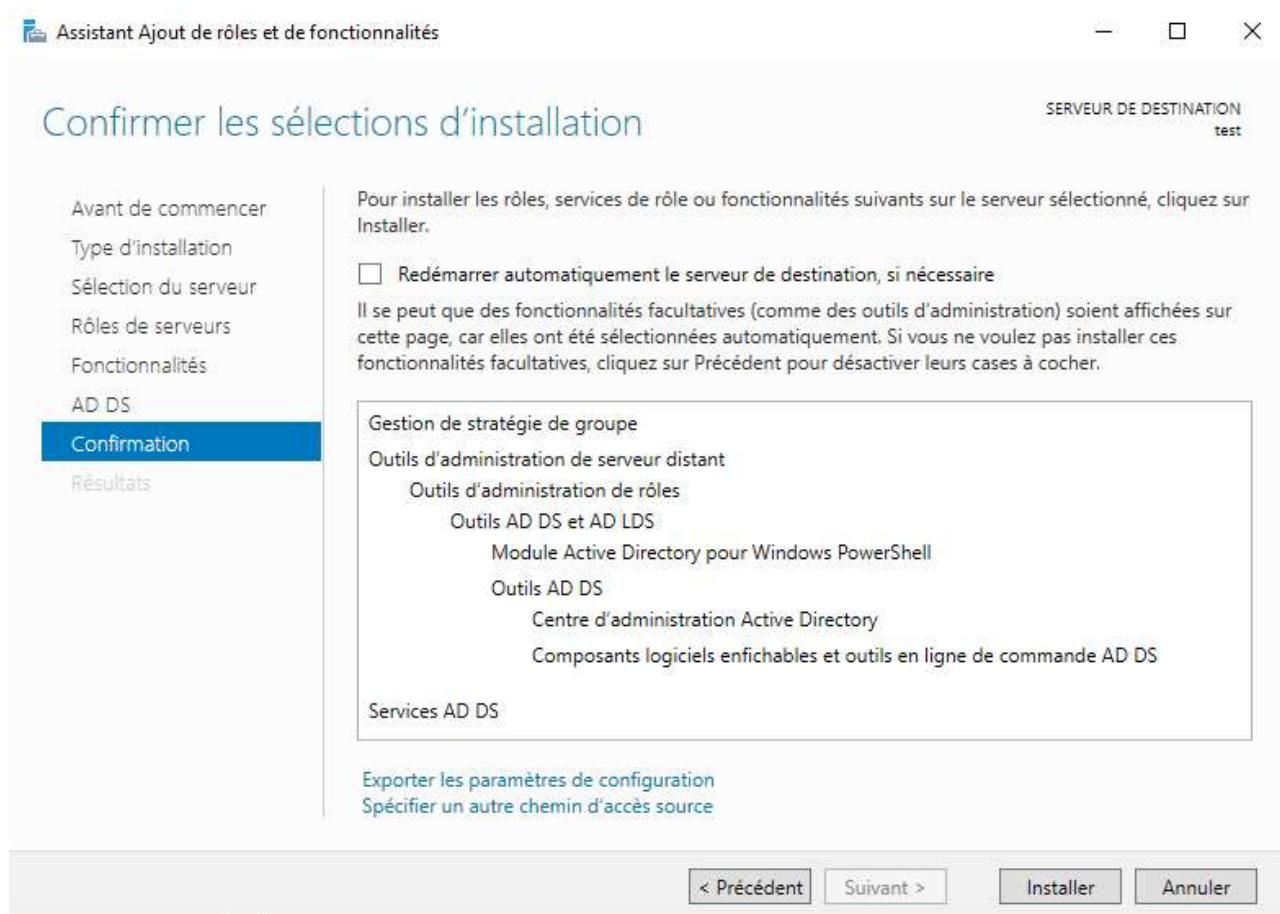
À noter :

- Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
- Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.

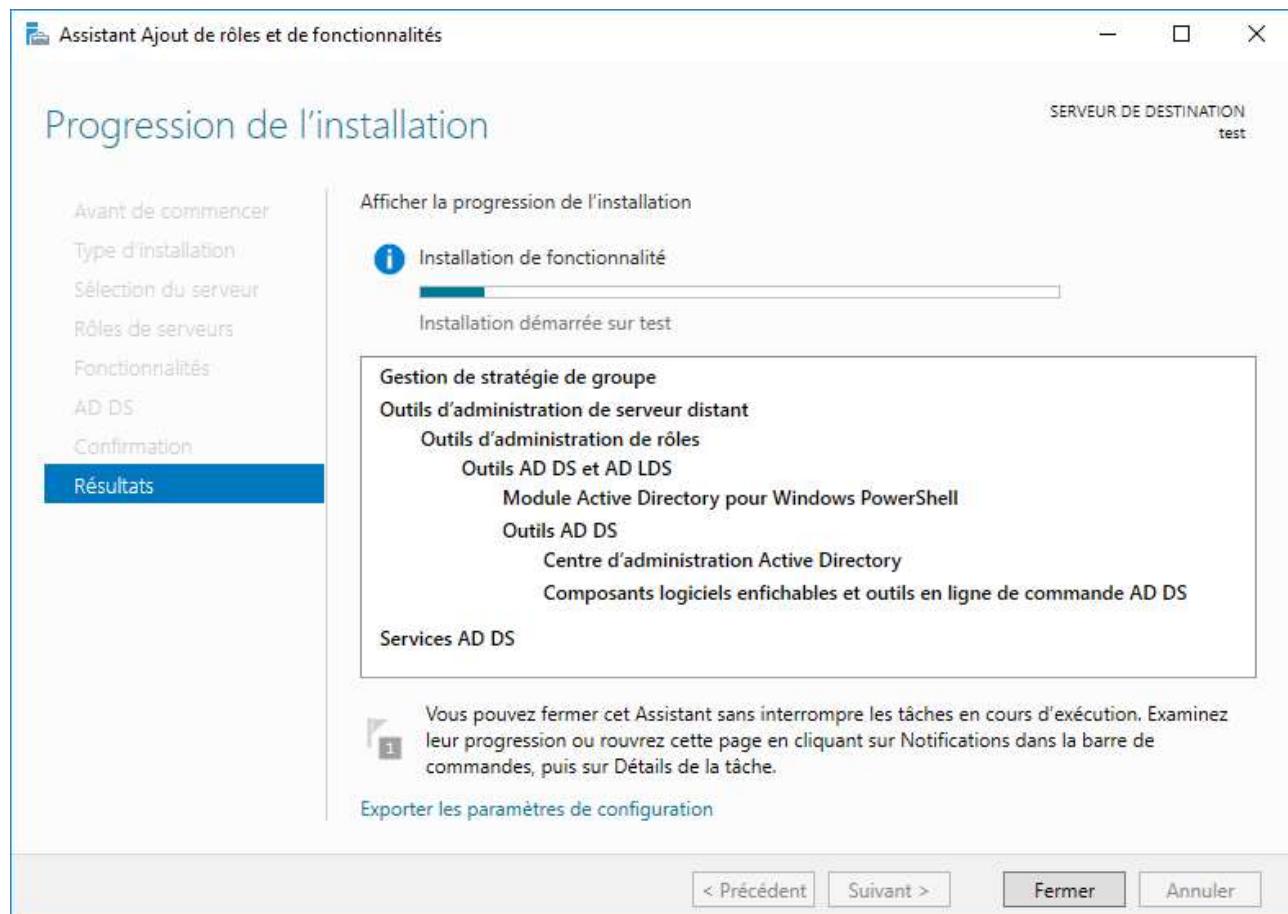
Azure Active Directory, un service en ligne distinct, peut fournir une gestion simplifiée des identités et des accès, des rapports de sécurité et une authentification unique aux applications web dans le cloud et sur site.
[En savoir plus sur Azure Active Directory](#)
[Configurer Office 365 avec Azure Active Directory Connect](#)

< Précédent Suivant > Installer Annuler

Confirmez l'installation en cliquant sur "Installer".

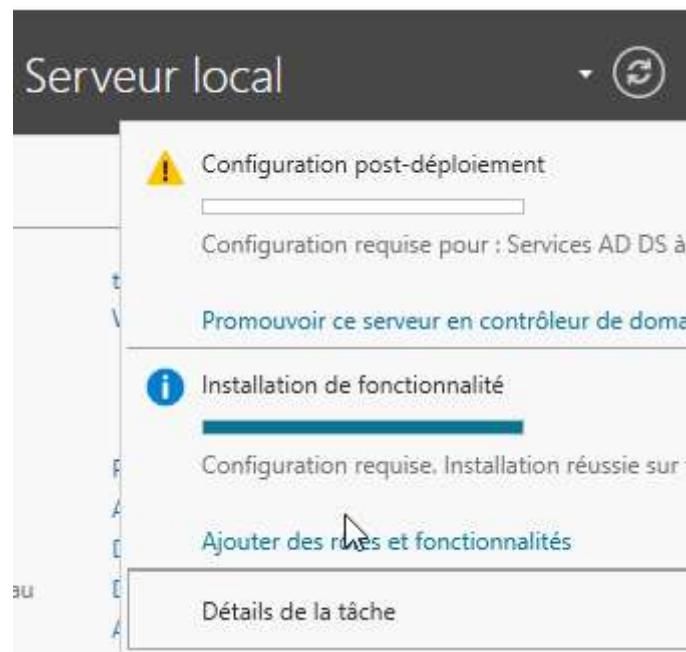


L'installation terminée, quittez l'assistant en cliquant sur "Fermer".



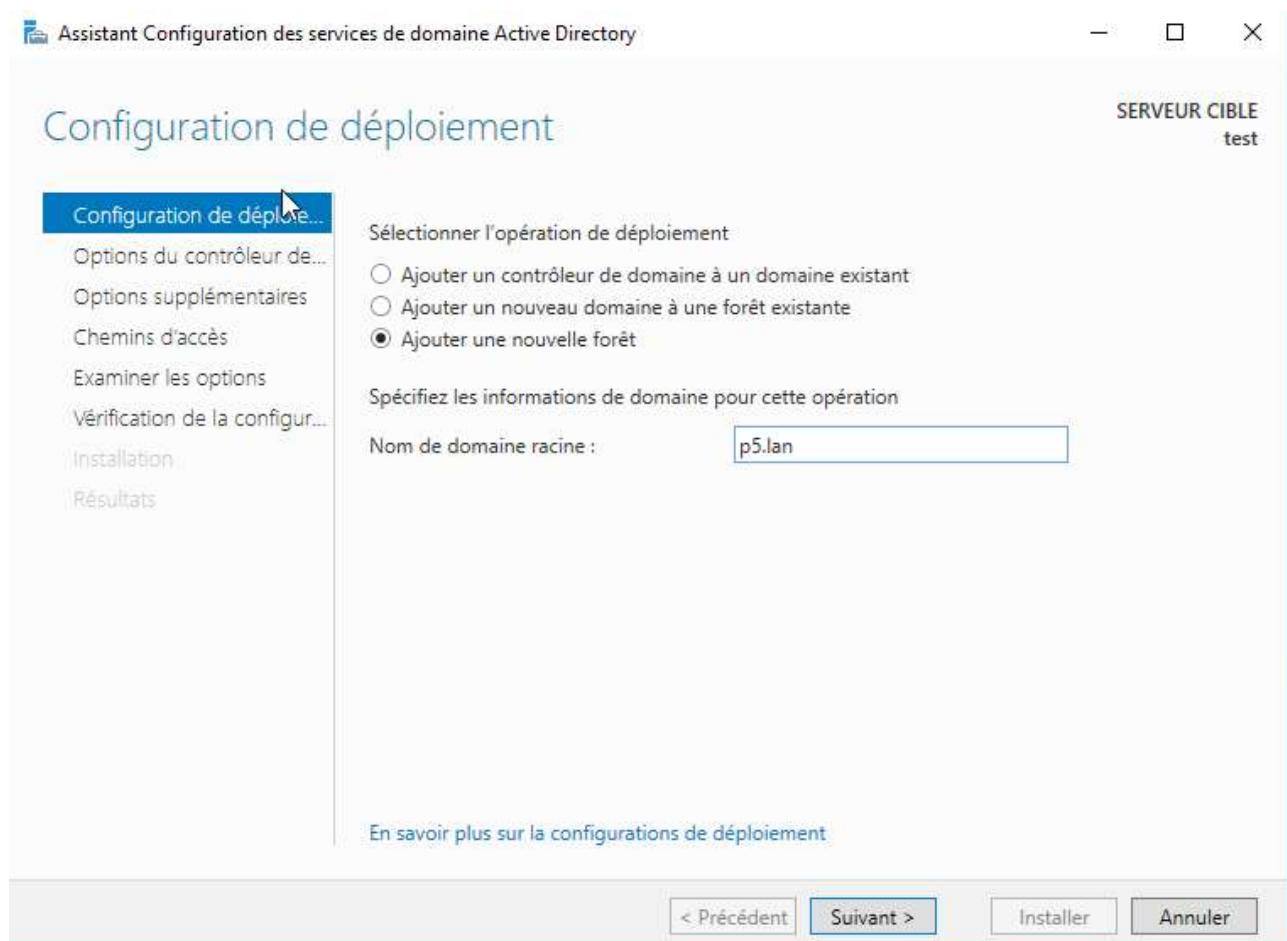
VI - Promotion du serveur WindowsAD comme contrôleur de domaine

Depuis le gestionnaire de serveur on remarque l'apparition d'une icône à côté du drapeau, cliquez dessus "Promouvoir ce serveur comme contrôleur de domaine".



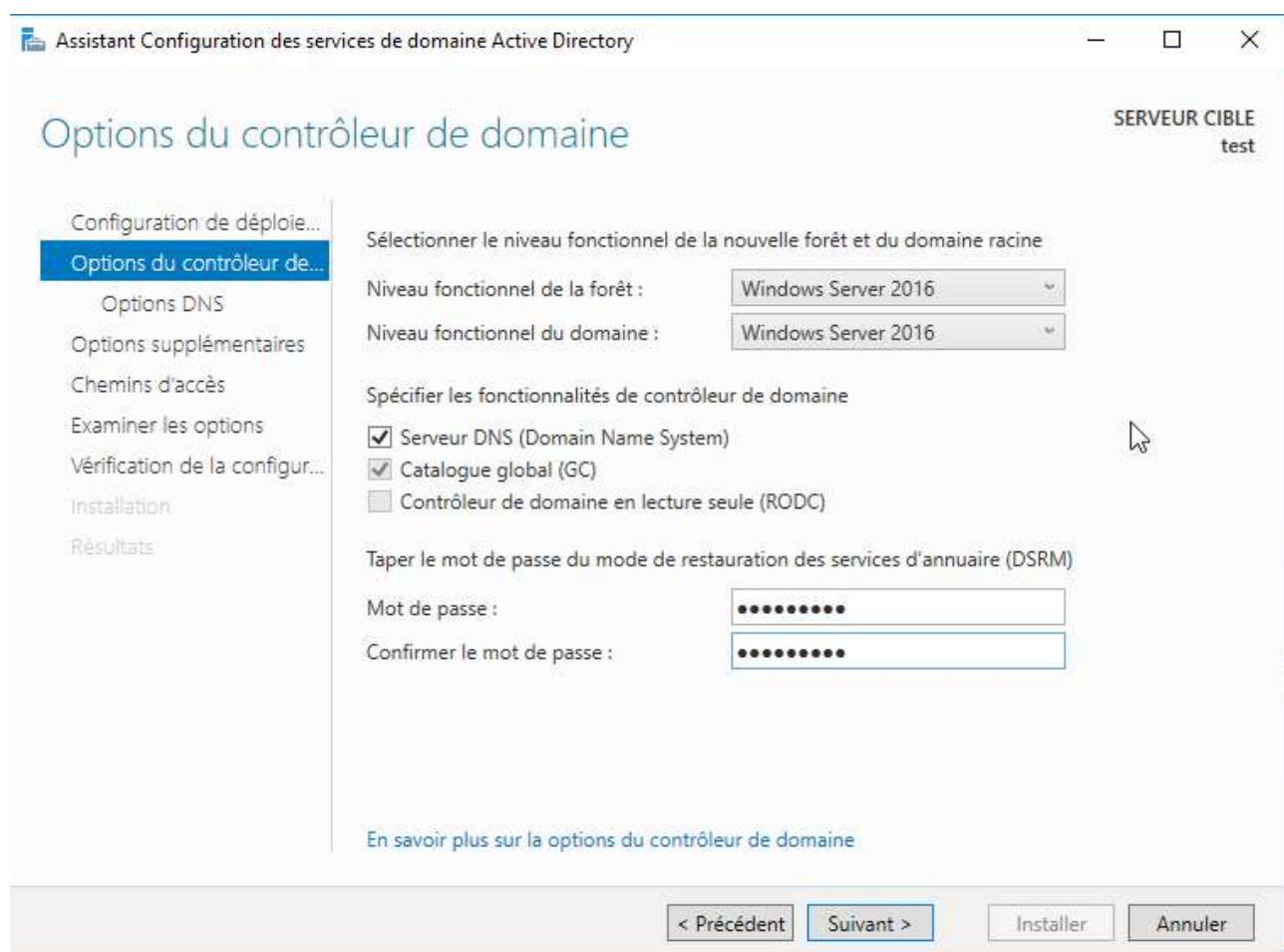
Cela aura pour effet l'ouverture de l'assistant de configuration.

Ici nous allons ajouter une nouvelle forêt et lui donner un nom de racine.

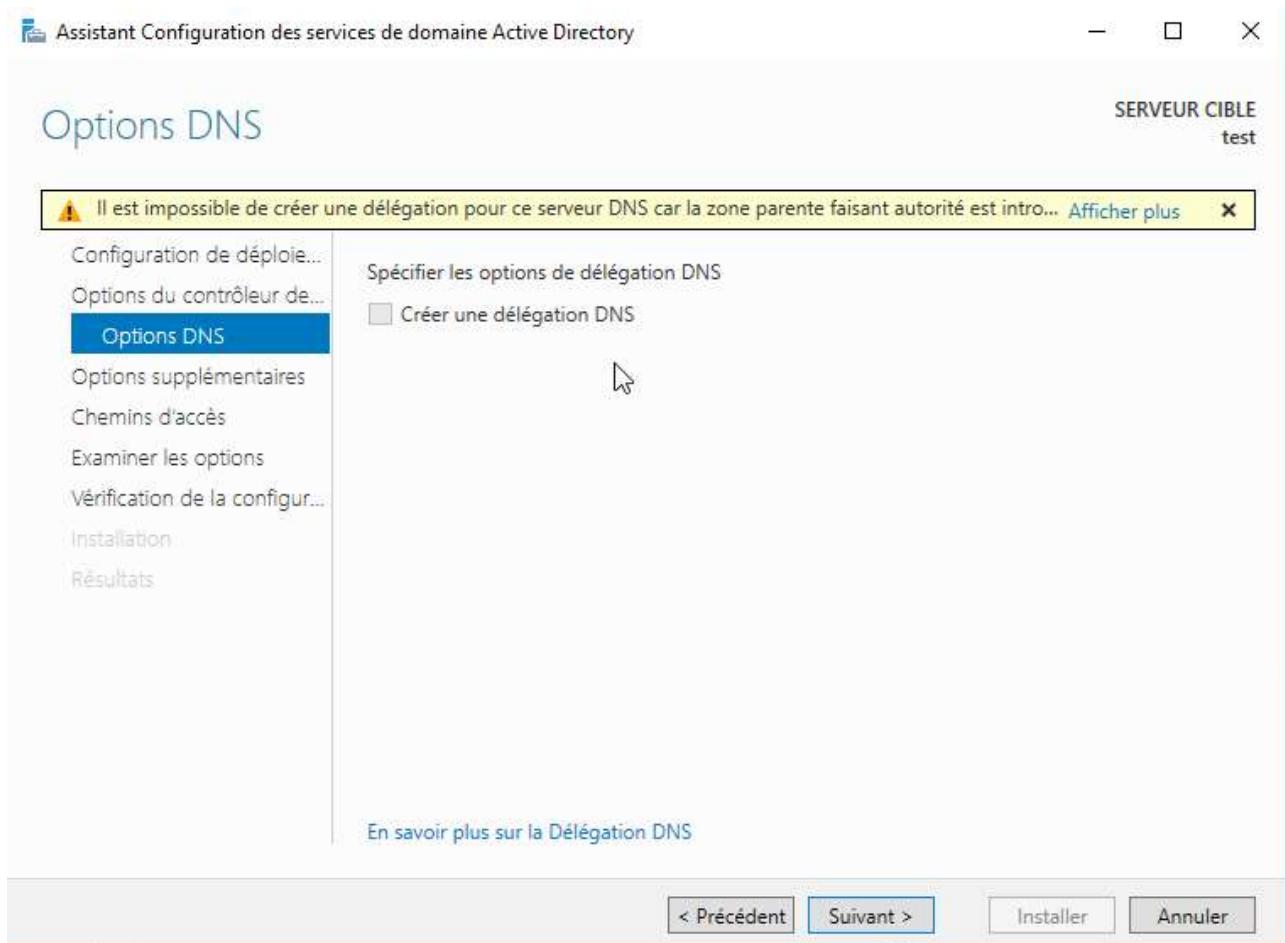


L'étape suivante consiste à définir quelques options du contrôleur de domaine.

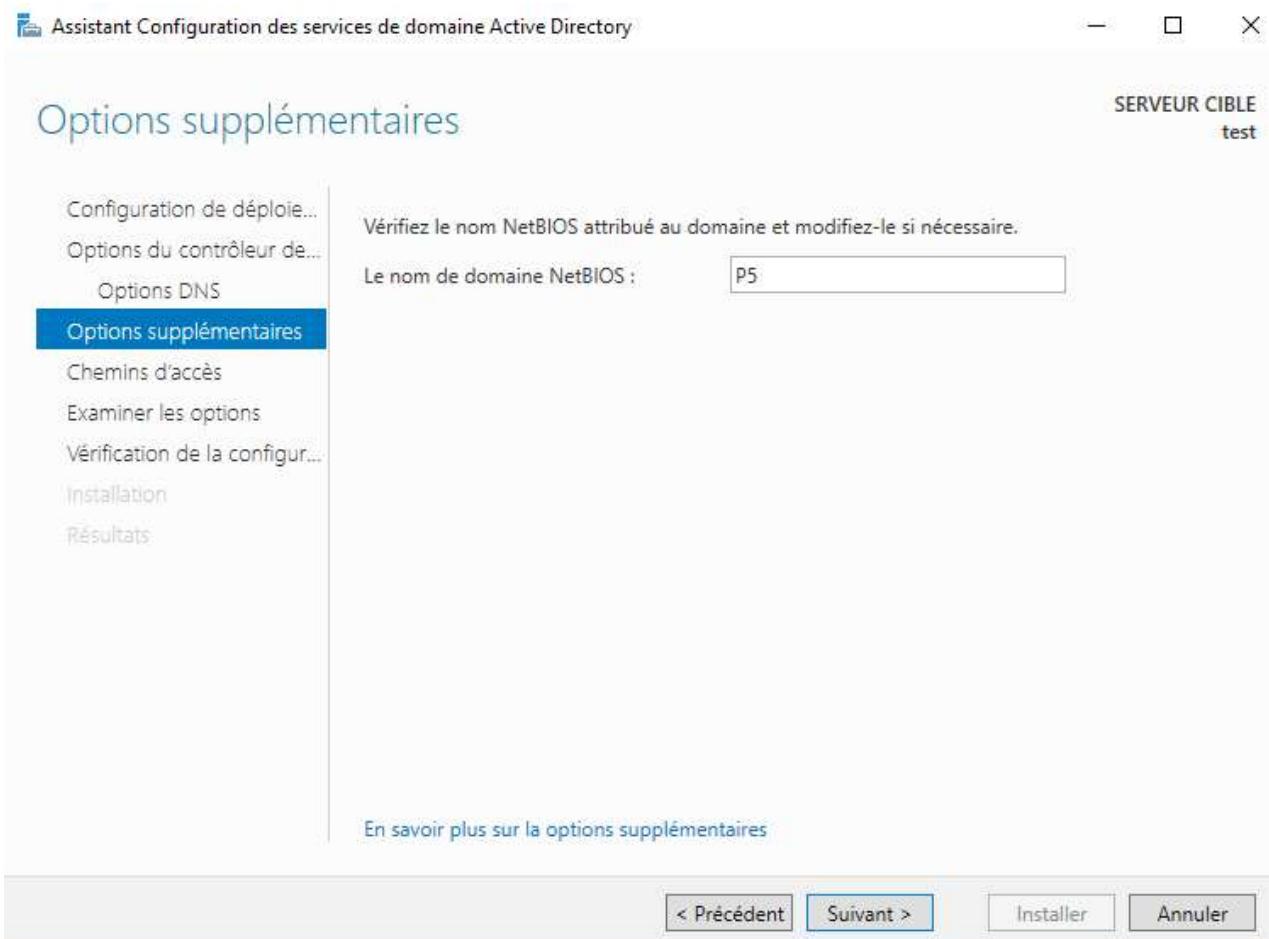
Les niveaux de domaine et de forêt permettent d'activer des fonctionnalités à l'échelle d'un domaine ou d'une forêt dans l'environnement de vos services de domaine Active Directory (AD DS).



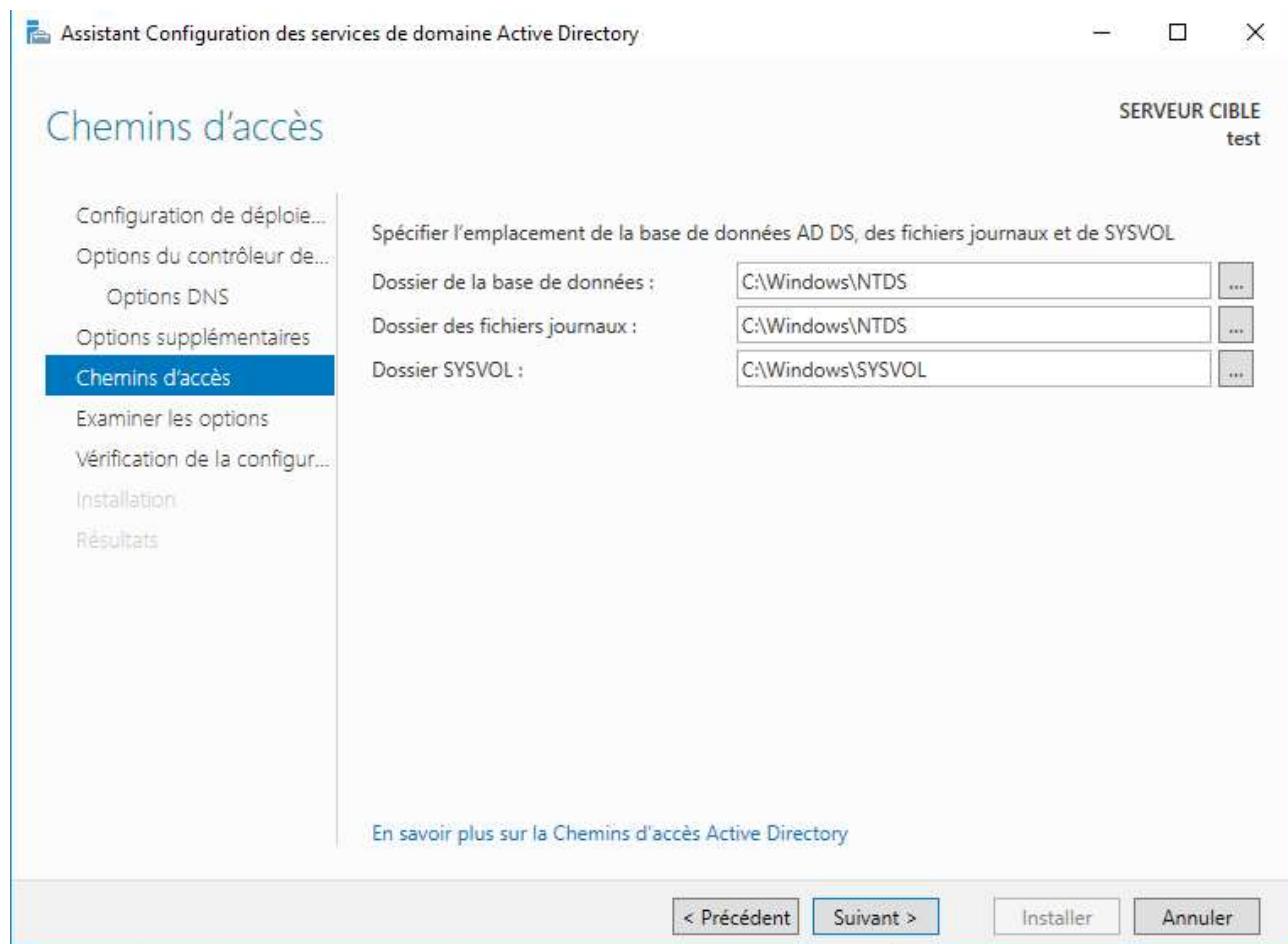
Un avertissement apparaît à cet écran car aucun serveur DNS n'est installé sur la machine, ce qui n'aura aucune influence négative sur la suite de notre configuration, cliquez sur "Suivant".



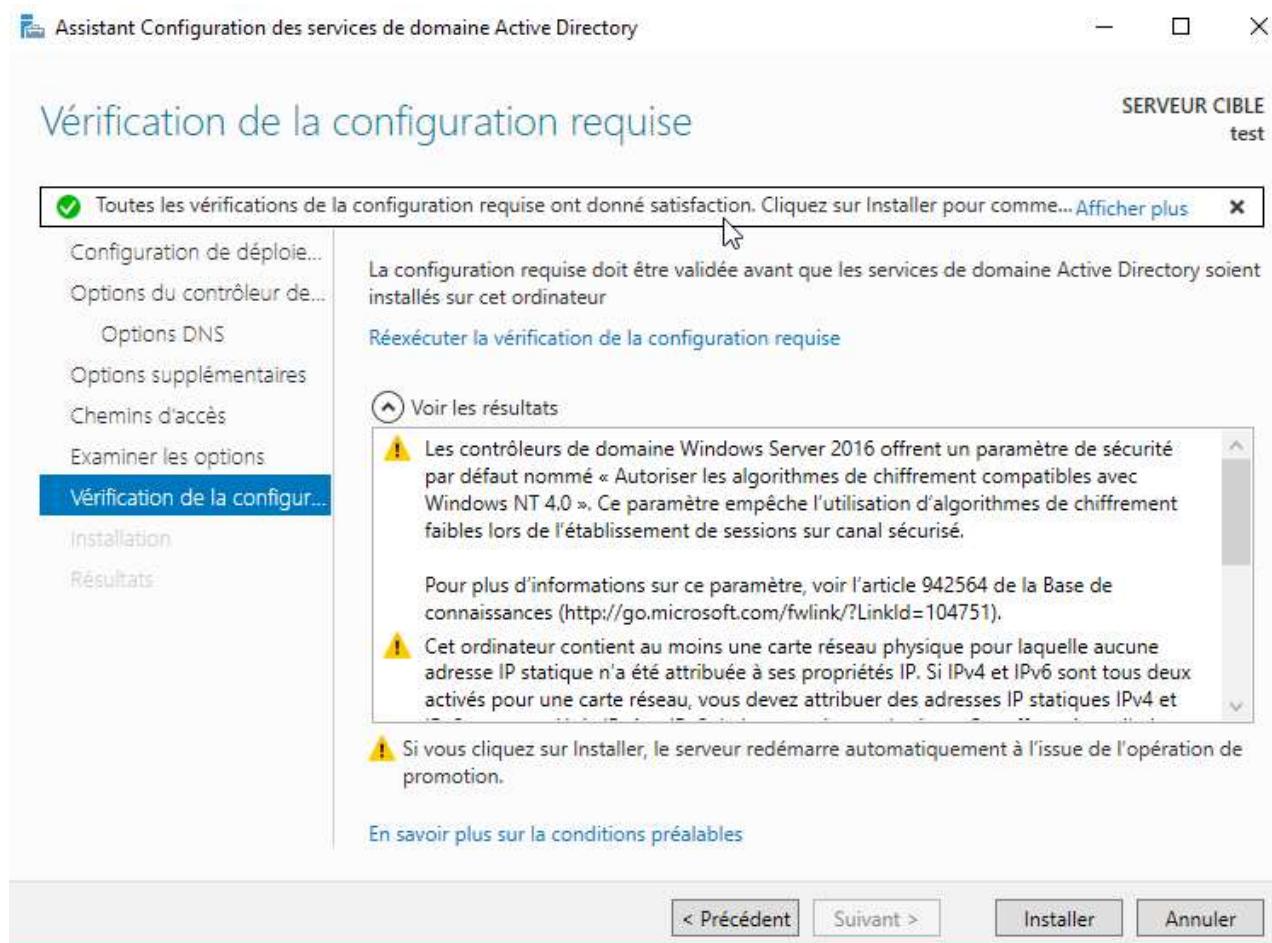
Laissons ici le nom NetBIOS déjà présent par défaut puis “Suivant”.



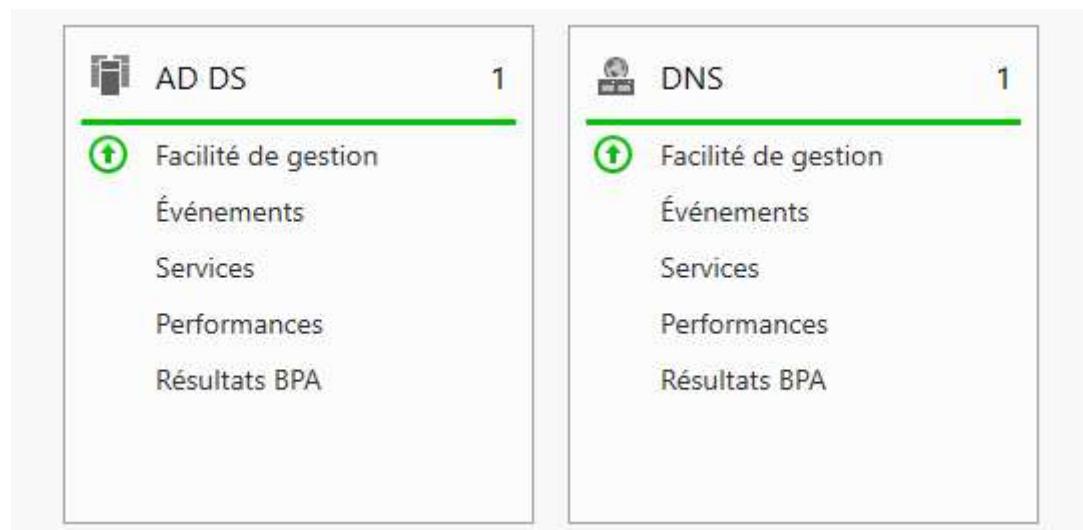
Laissons ici aussi les valeurs par défaut et cliquons sur “Suivant”.



Après vérification de la configuration, cliquez sur "Installer".

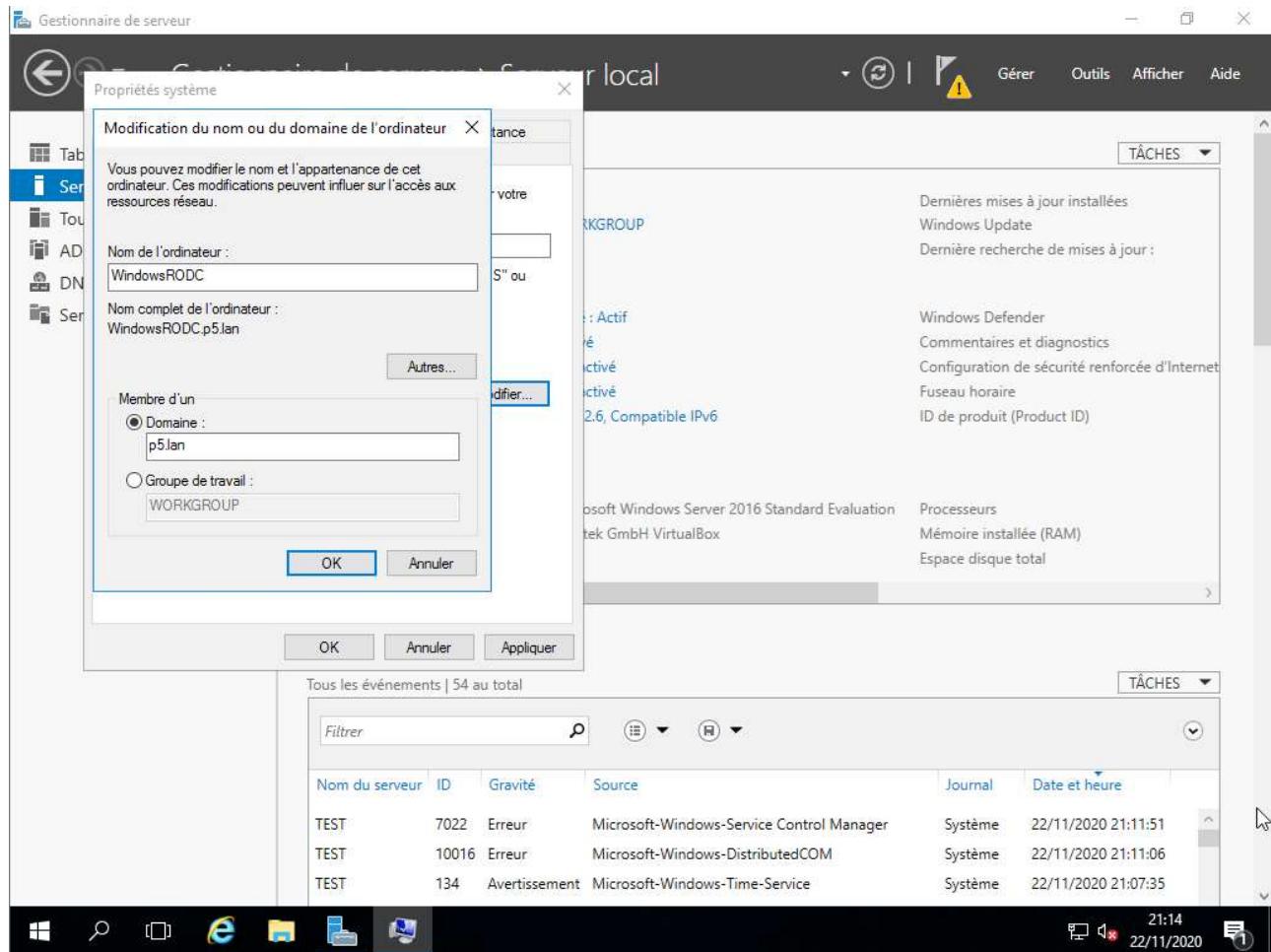


Une fois l'installation fini, les rôles sont opérationnels.



VII -Installation et raccordement du WindowsRODC

Changez l'option Groupe de travail pour Domaine et tapez le nom du domaine créé sur WindowsAD (ici p5.lan)



Reprenez l'installation vu précédemment :

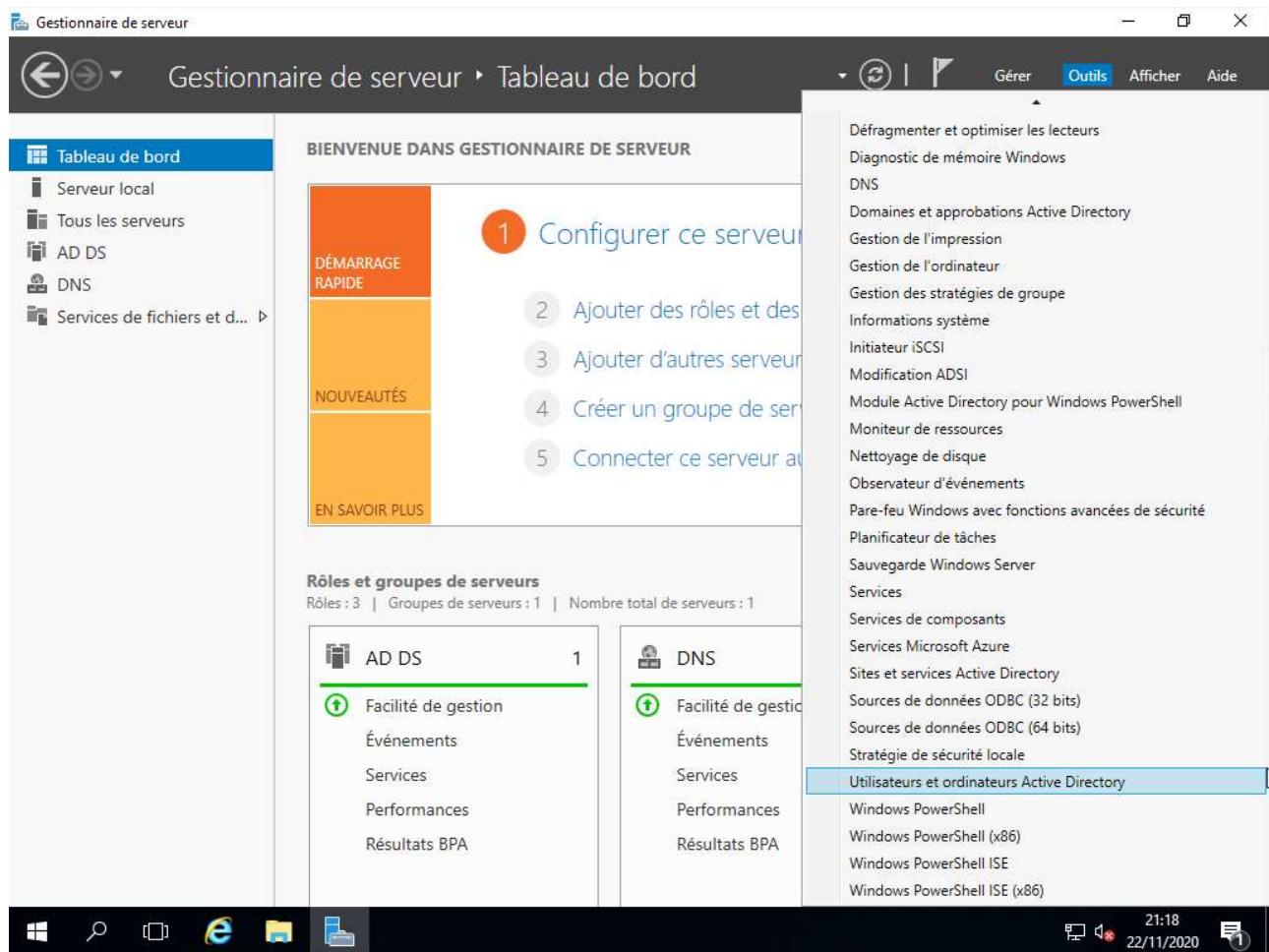
“3. Promotion sur serveur WindowsAD comme Contrôleur de domaine”

Mais en précisant :

- D'ajouter le nouveau contrôleur à un domaine existant
- Puis dans les options d'installation cochez “Contrôleur de domaine en lecture seul (RODC)”

VIII -Création des utilisateurs

Pour la création d'utilisateurs, rendez-vous depuis le gestionnaire de serveur dans le menu Outils en haut à droite et sélectionnez Utilisateurs et ordinateurs Active Directory

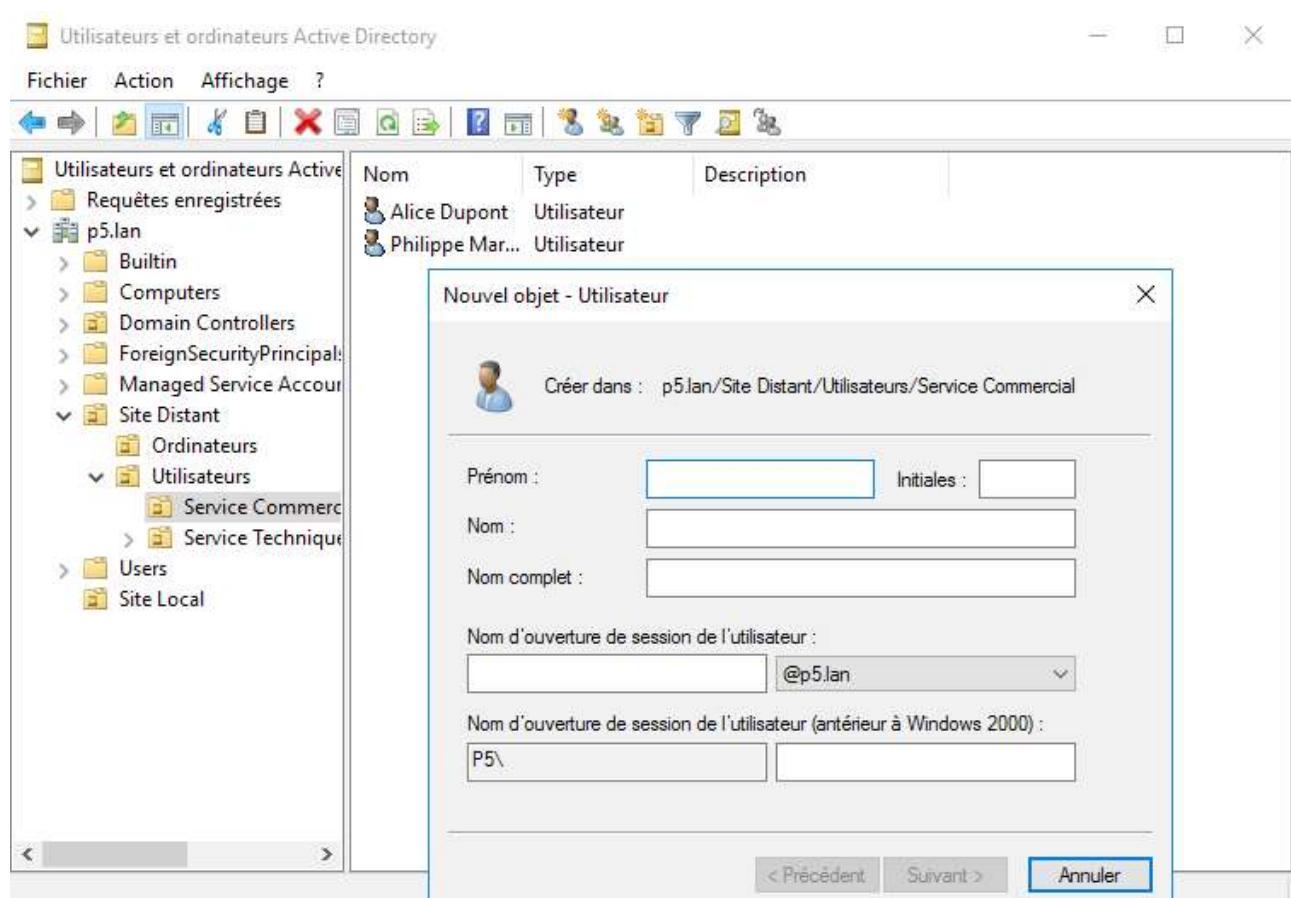


Dans le volet gauche cliquez sur le domaine et créez une OU.

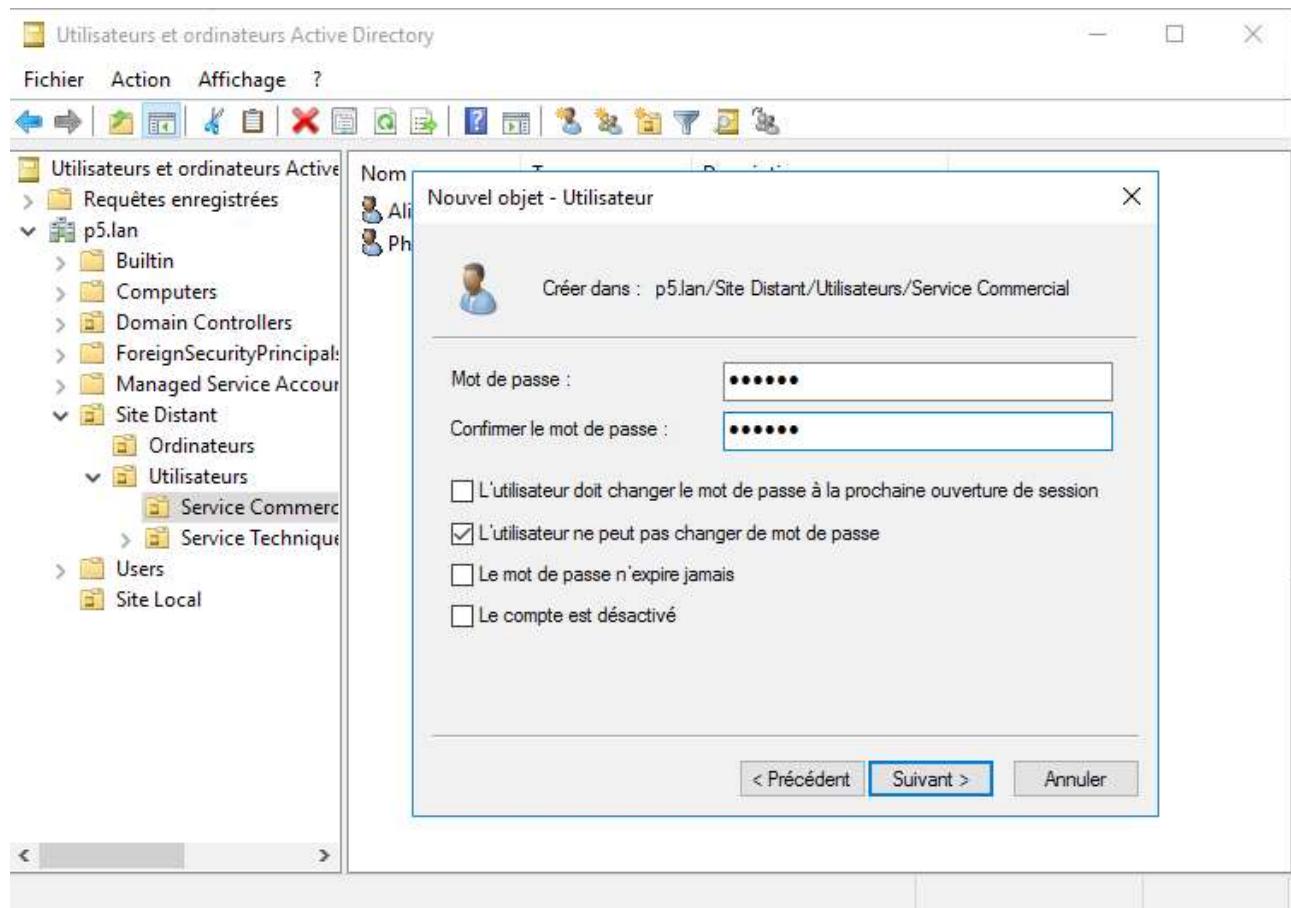
Dans notre cas l'arbre se limite au Site Local et au Site Distant comprenant les ordinateurs et les utilisateurs dans les service commercial et technique.

Pour ajouter un utilisateur à un certain niveau du domaine, cliquez sur le niveau souhaité (ici le service commercial) et cliquez sur ajouter un nouvel utilisateur dans la barre de menu

On créer donc nos 3 utilisateurs.

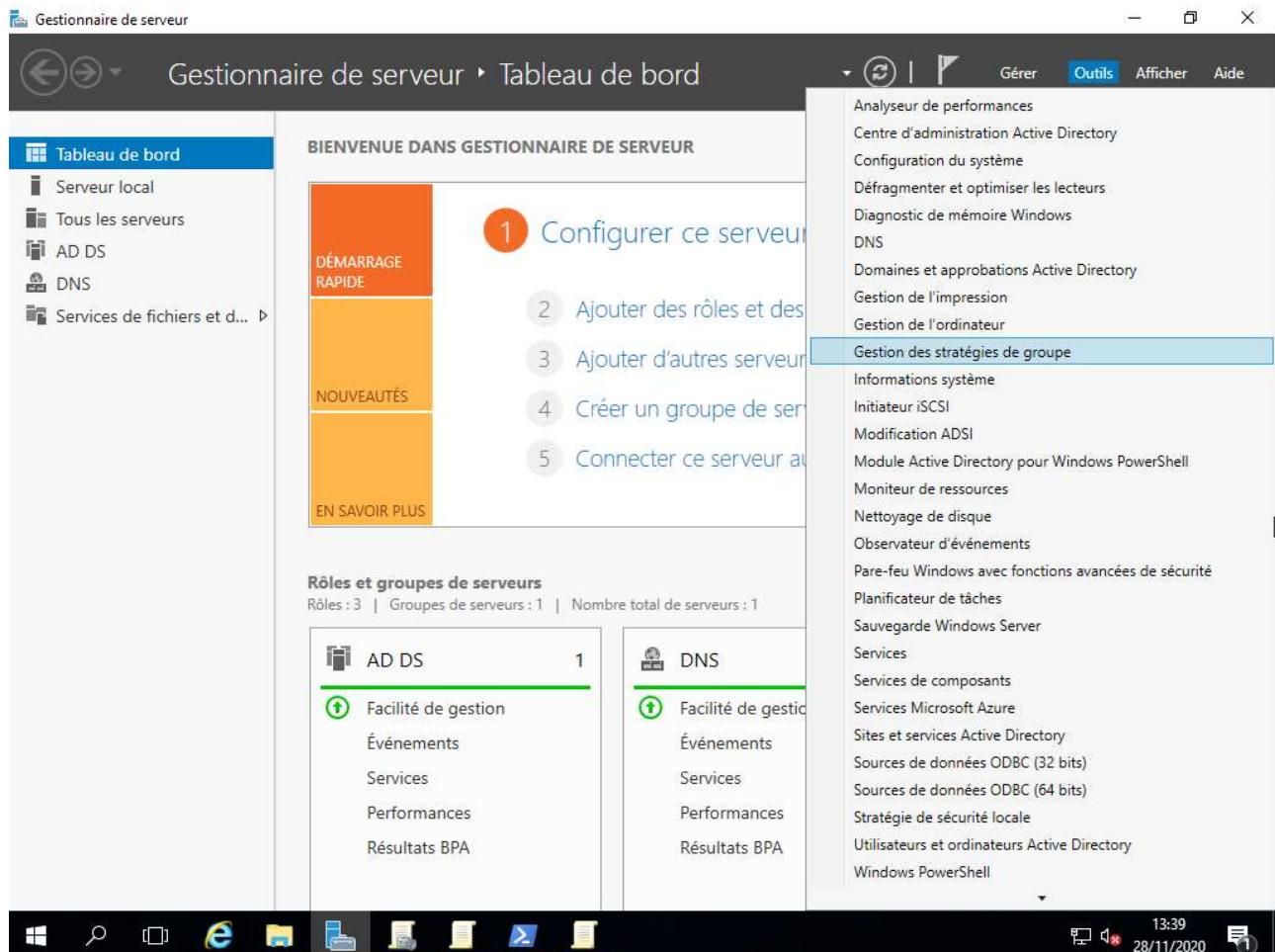


Remplissez les informations demandées sans oublier de préciser que l'utilisateur ne peut pas changer son mot de passe



IX -Mise en place des GPO

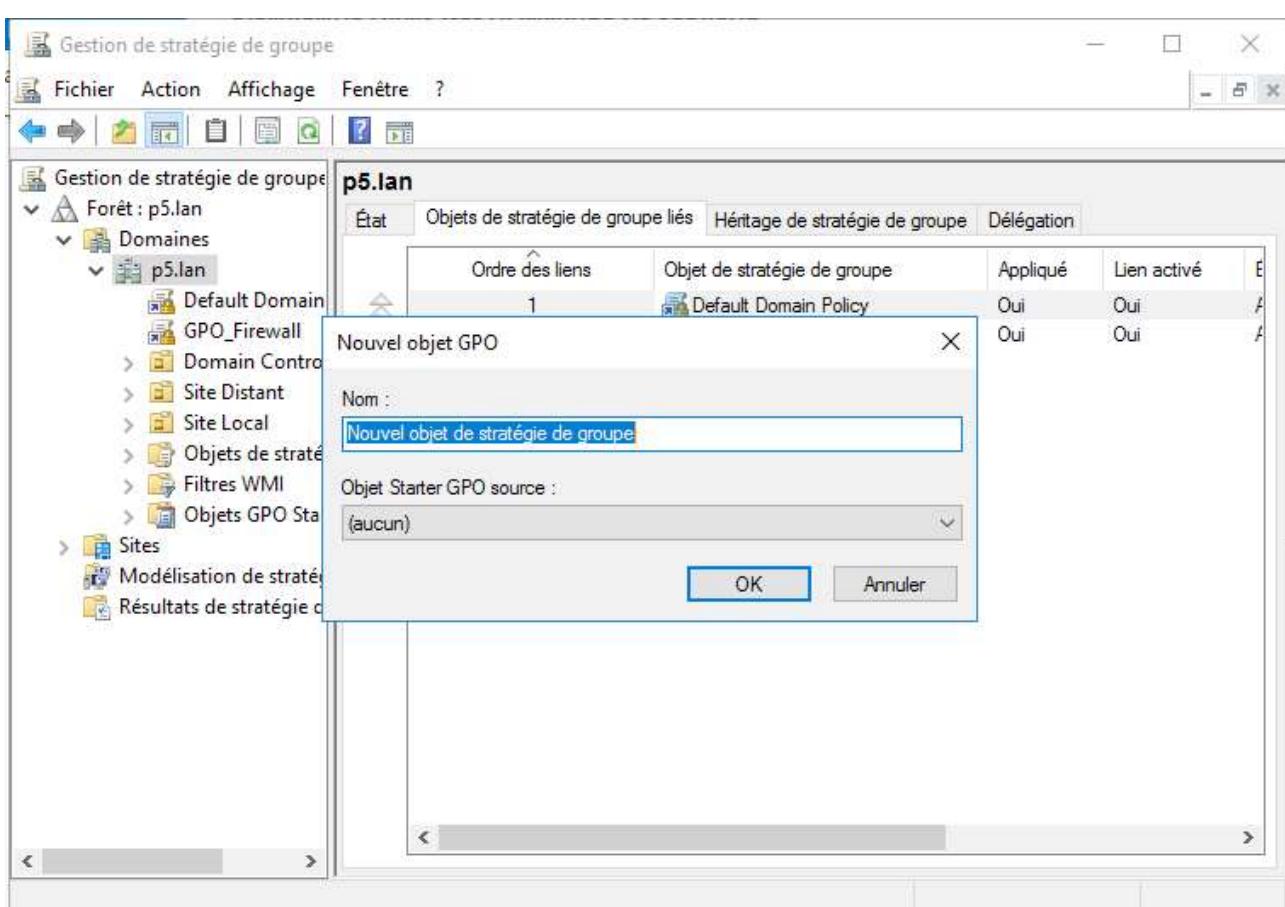
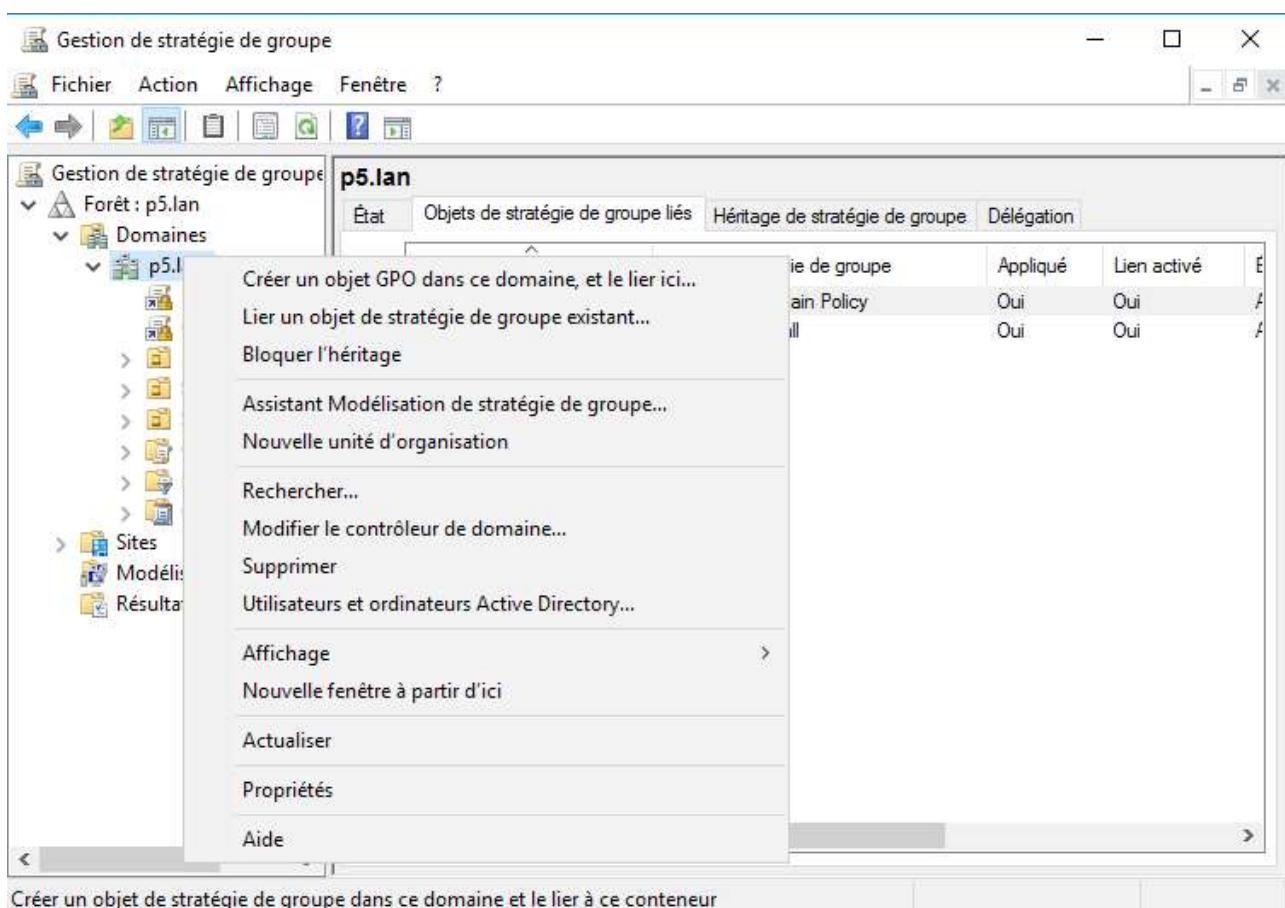
Pour la mise en place des Group Policy Object, rendez-vous depuis le gestionnaire de serveur dans le menu Outils en haut à droite et sélectionnez Gestion des stratégies de groupe.

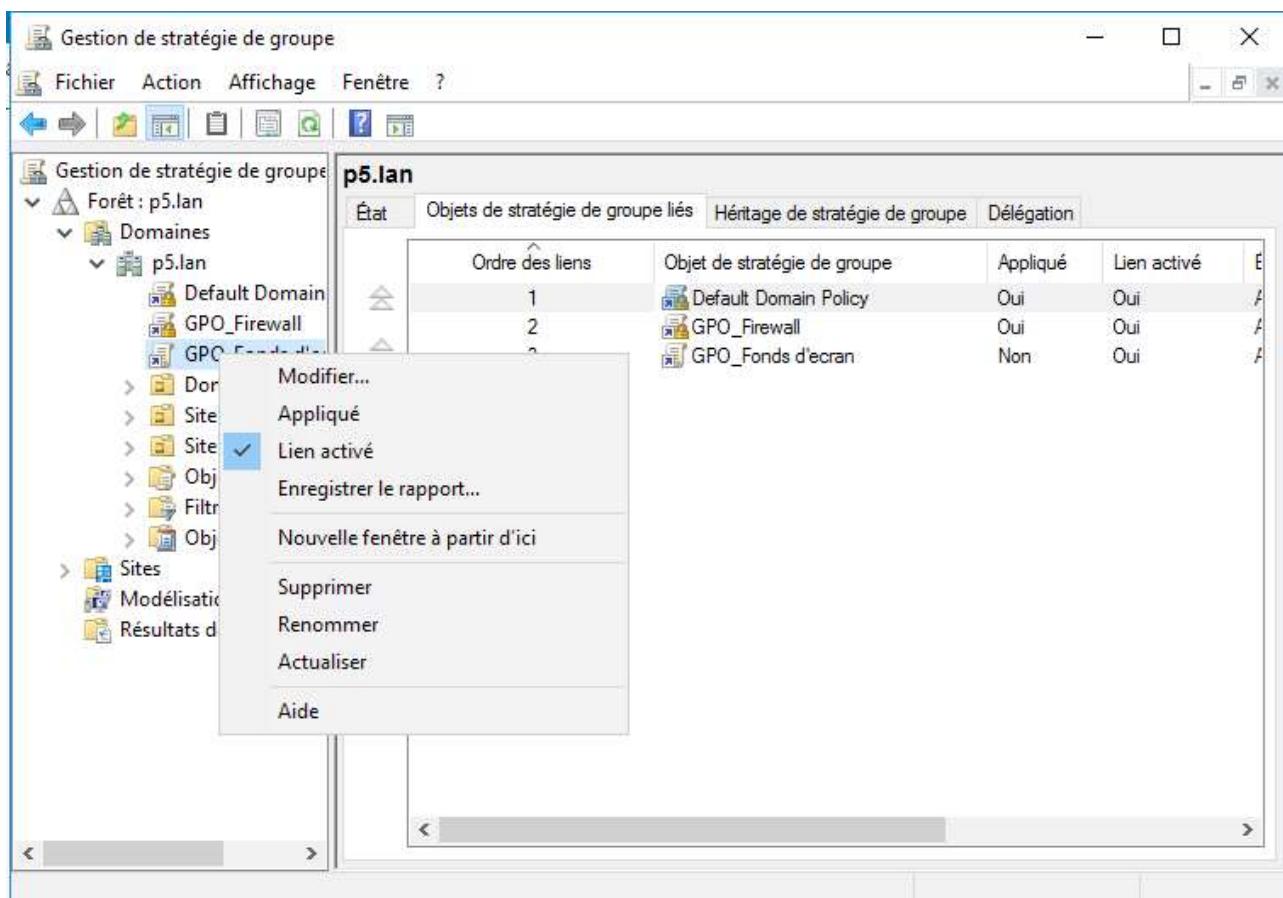


Dans notre cas on peut distinguer 5 GPO :

- Un GPO pour la gestion des fonds d'écran
- Un GPO pour la gestion des firewalls
- Un GPO pour la gestion des mots de passe
- Un GPO pour la gestion des logiciels installés
- Mappage Lecteur réseau « ShareCompanyDocs »

Pour créer un nouveau GPO au niveau du domaine, effectuez un clique droit sur le domaine et cliquez sur Créez un objet GPO dans ce domaine puis donnez lui un nom. Pour lui affecter des actions faites clique droit sur le GPO nouvellement créé et cliquez sur Modifier



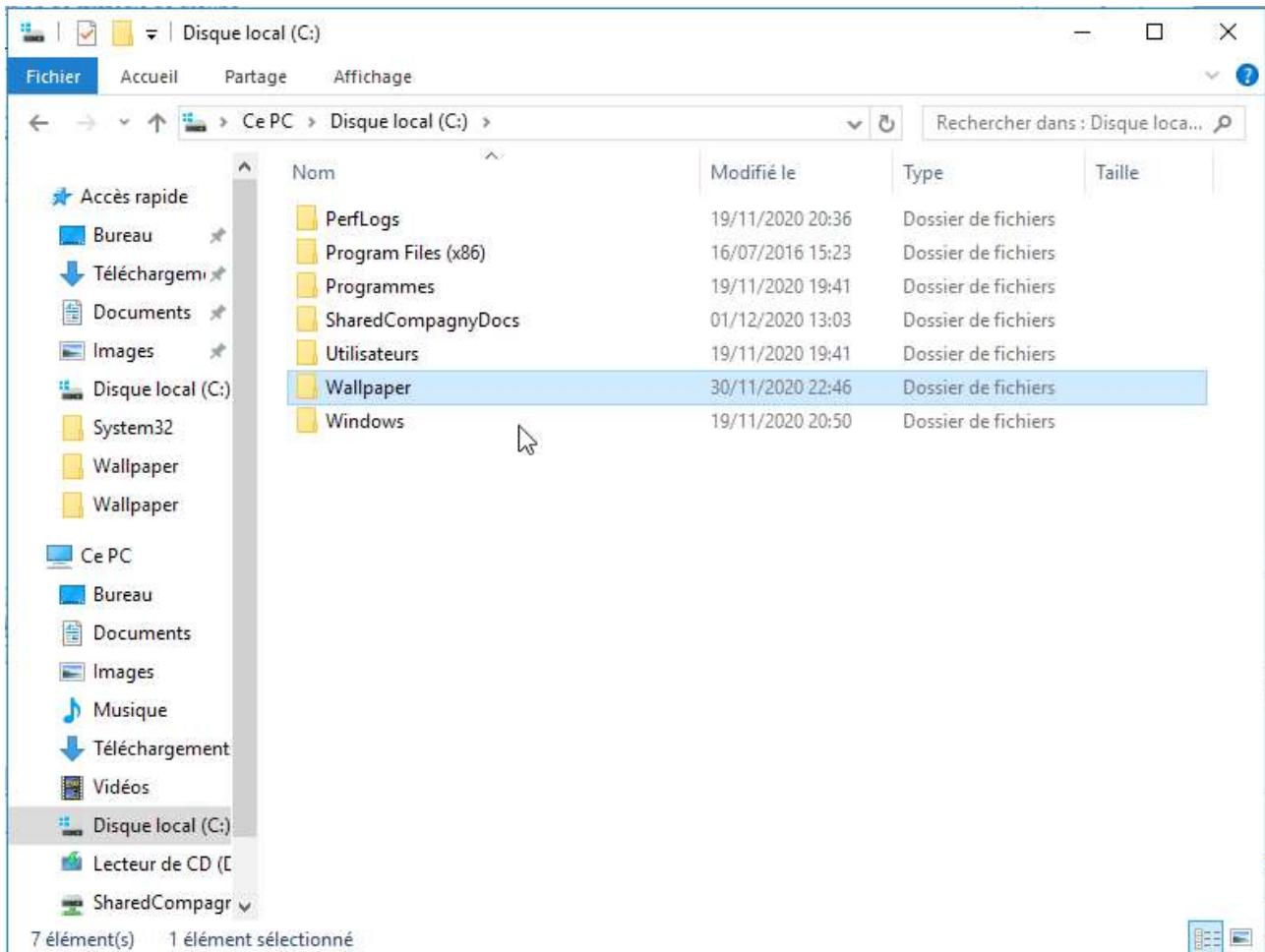


A- Politique concernant les fond d'écran :

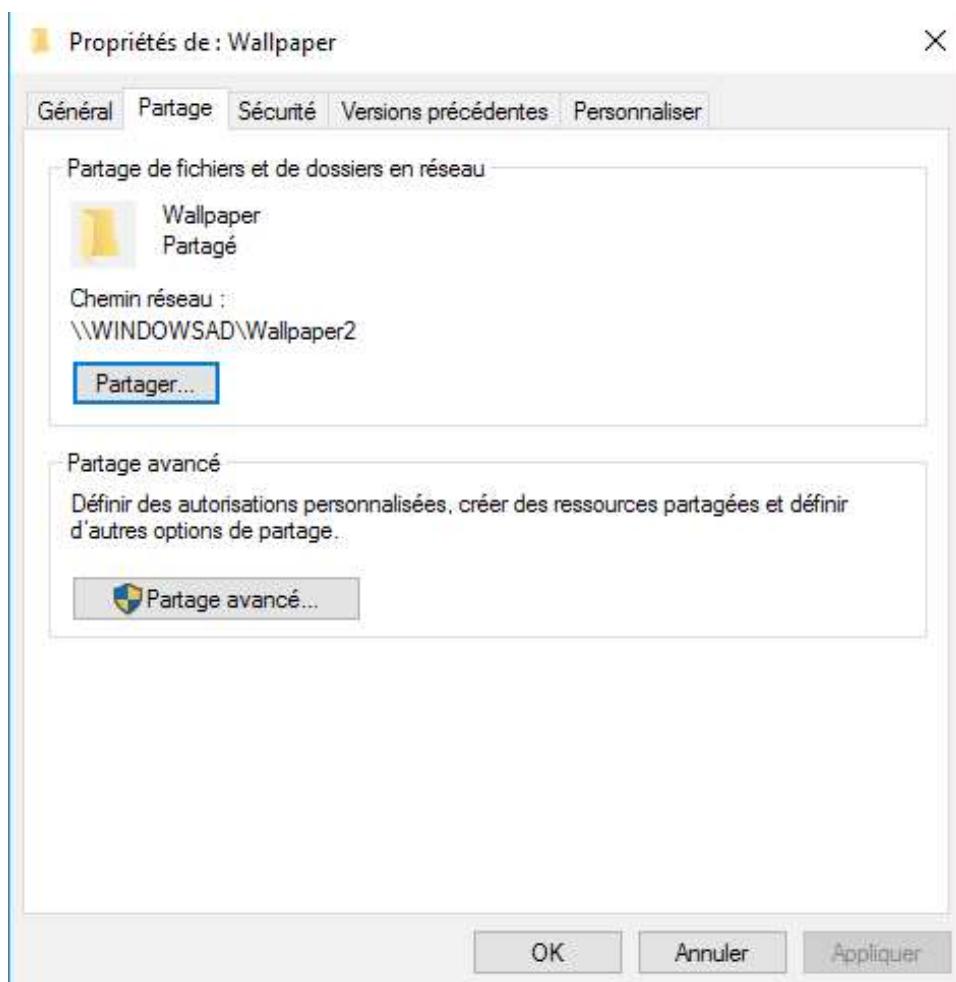
Il s'agit ici d'imposer un fond d'écran unique pour l'ensemble des machines du domaine.

Premièrement, nous débutons par créer un partage pour héberger le fichier du fond d'écran, il doit être accessible par le réseau par les postes clients.

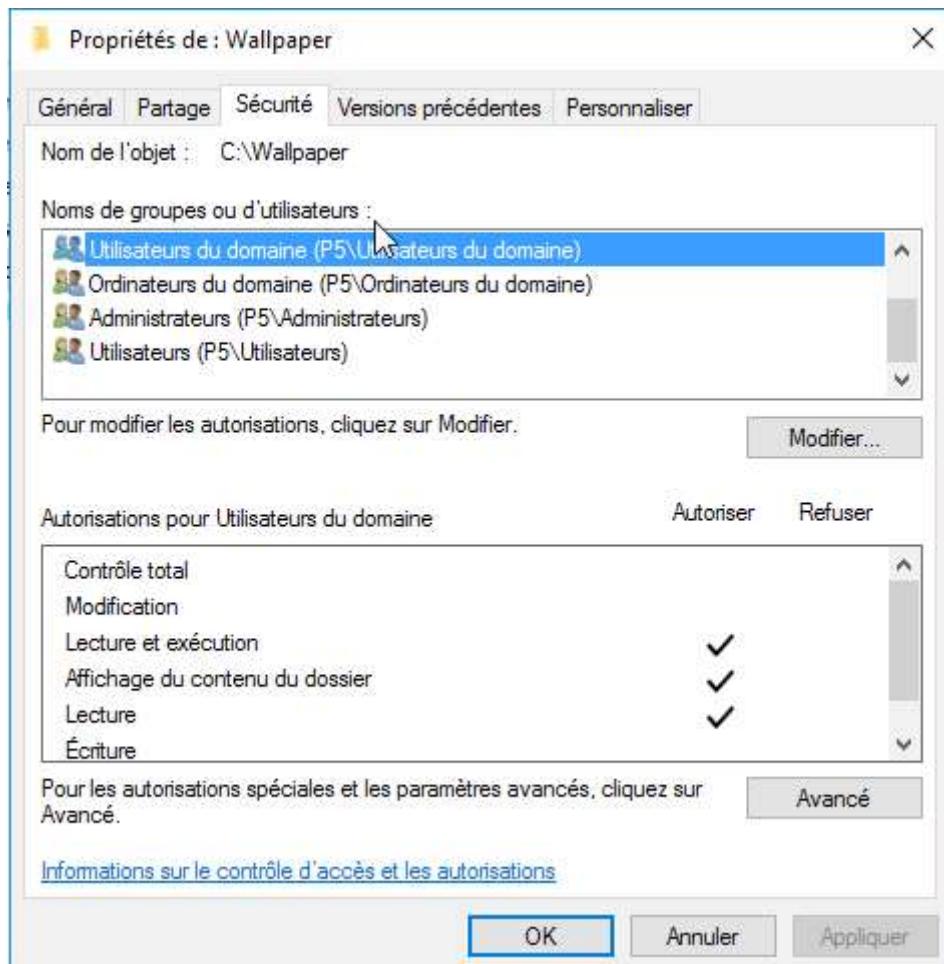
Notre choix sera de créer ce répertoire partagé à la racine du lecteur C: du contrôleur de domaine.



Nous partagerons ce répertoire pour le rendre accessible par nos postes utilisateurs.



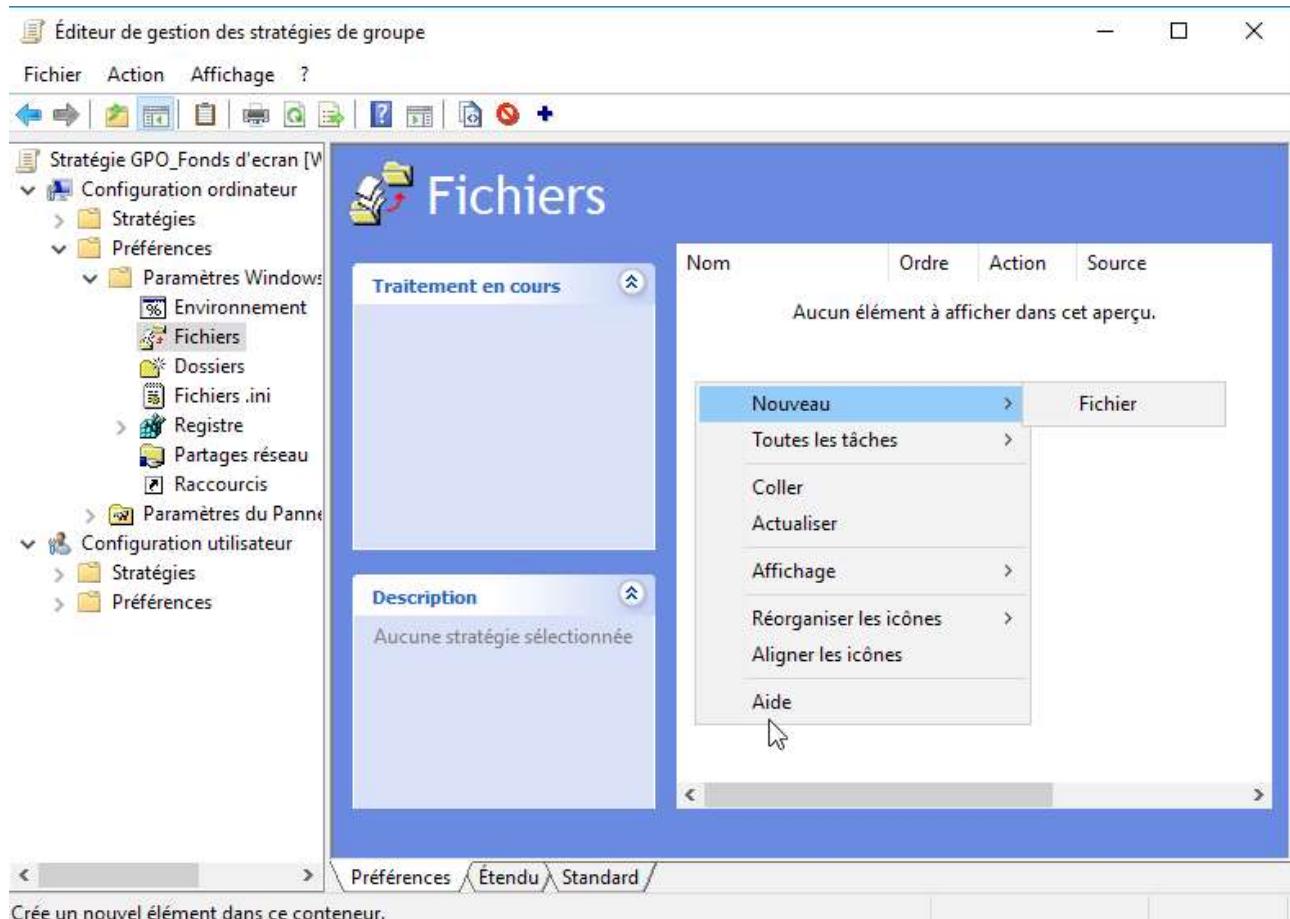
Nous attribuerons les droits de lecture au groupe «*Ordinateurs du domaine*» pour qu'il puisse venir chercher le fichier, car il s'agit d'une stratégie de type «*Ordinateur*».



Nous pouvons maintenant créer la GPO.

Commençons par créer un paramètre de préférence pour que le fichier image du fond d'écran soit copié sur les ordinateurs distants. On va créer un nouveau fichier.

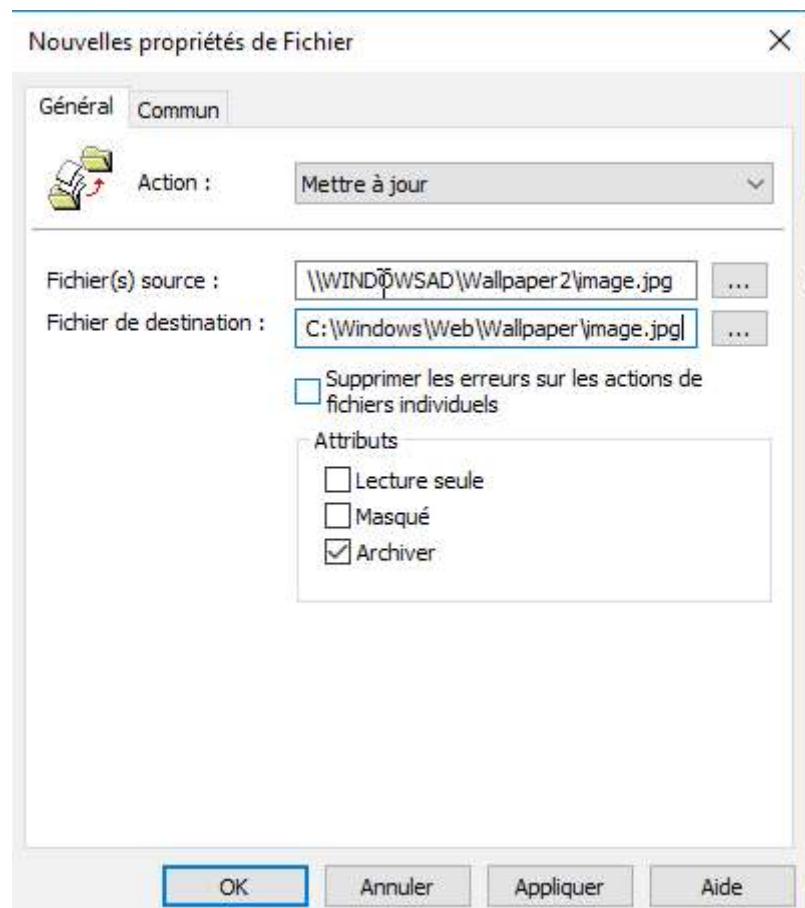
Configuration ordinateur / Préférences / Paramètres Windows / Fichier



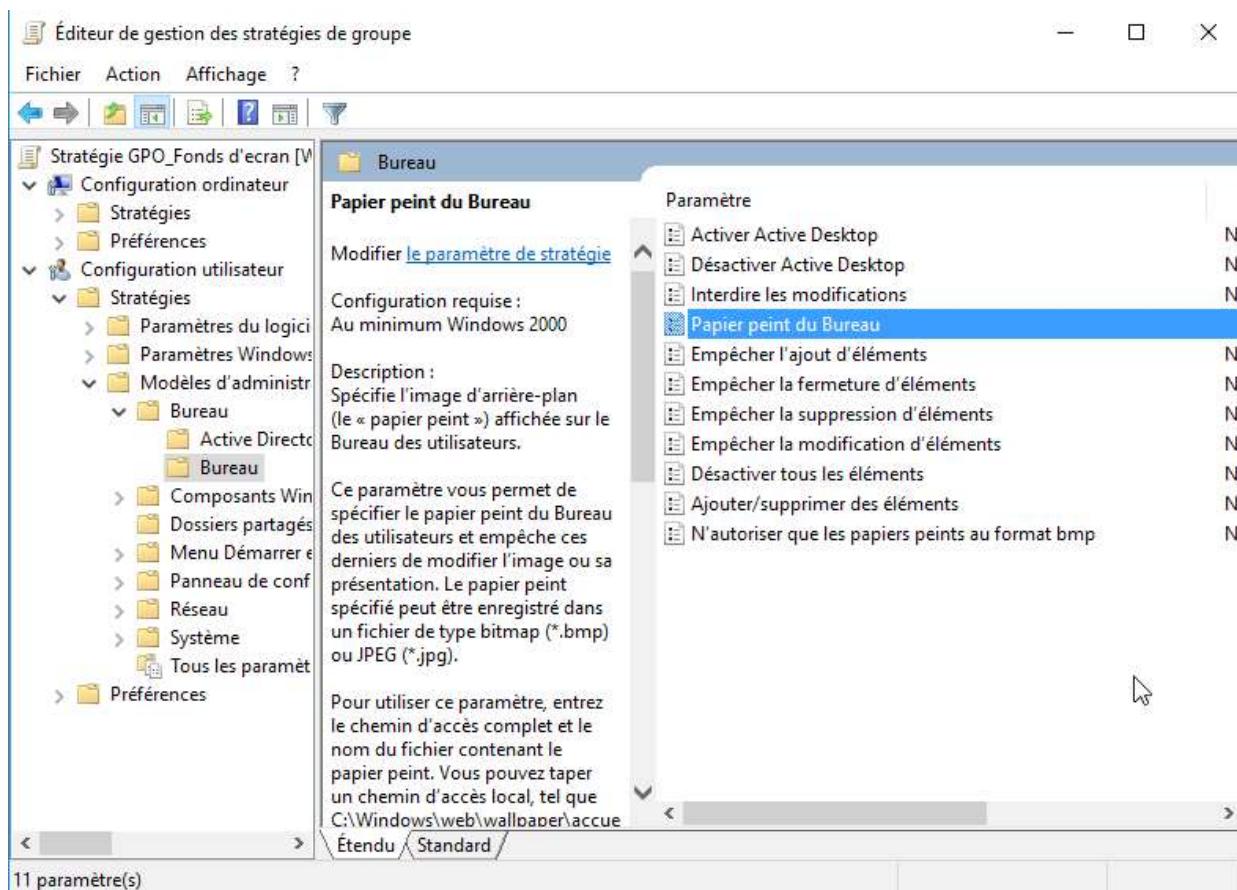
Le champs «fichier(s) source» permet de préciser le chemin menant au stockage de l'image sur votre serveur (*du type: \\WINDOWSAD\wallpaper\image.jpg*).

Pour conclure la configuration, le champs «fichier de destination» stocke le lieu où vous souhaitez copier le fichier sur l'ordinateur, en local évidemment.

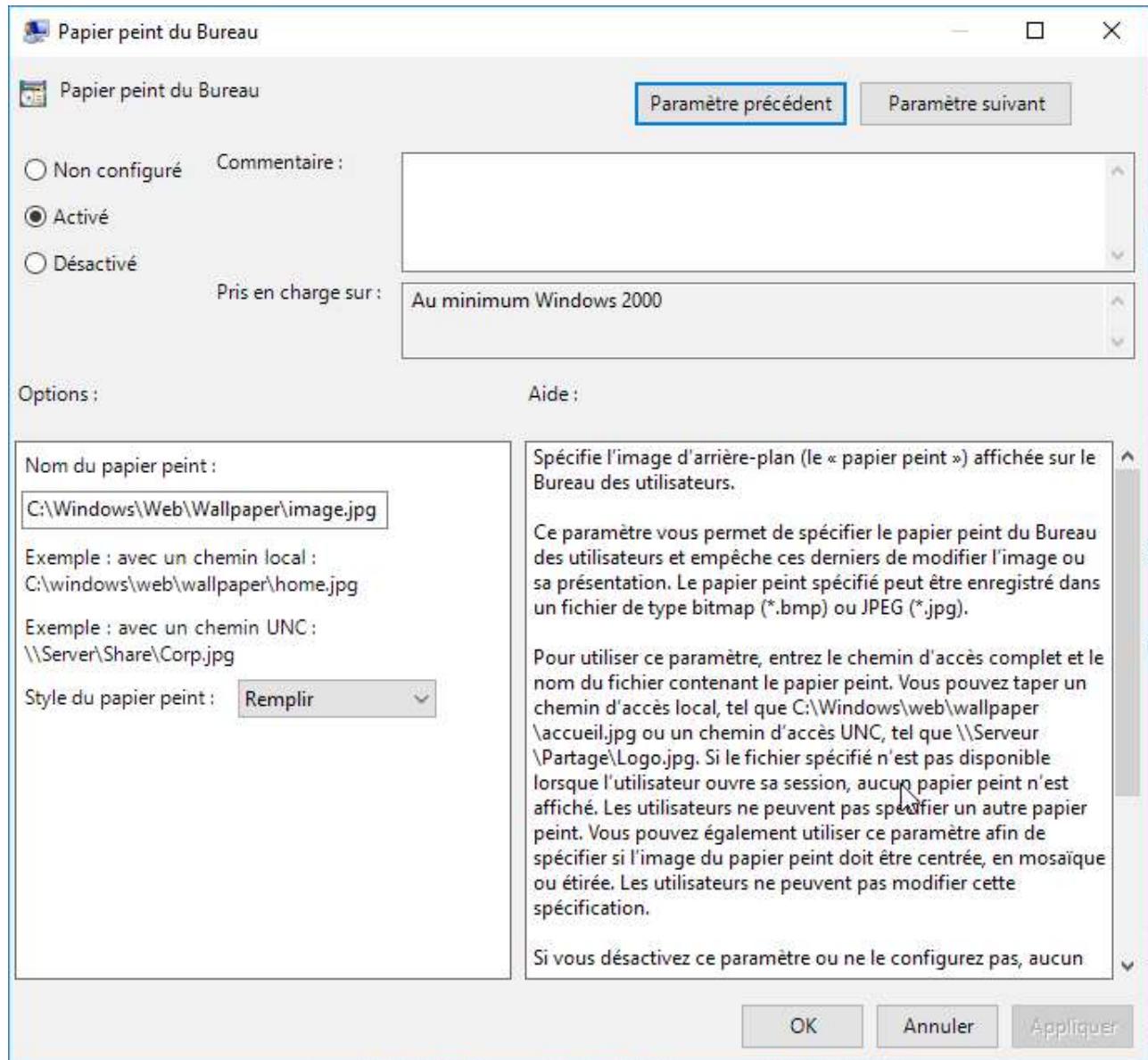
Pour ma part, j'indique «C:\\Windows\\Web\\Wallpaper\\image.jpg» pour le copier dans le répertoire où Windows stocke par défaut l'ensemble des fonds d'écran.



Dans l'éditeur de GPO cherchez via le volet d'exploration à gauche
Configuration utilisateur / Modèle d'administration / Bureau / Bureau



Puis double cliquez sur Papier peint du Bureau
Indiquez le chemin du fichier utilisé, le style d'affichage puis cliquez sur appliquer.



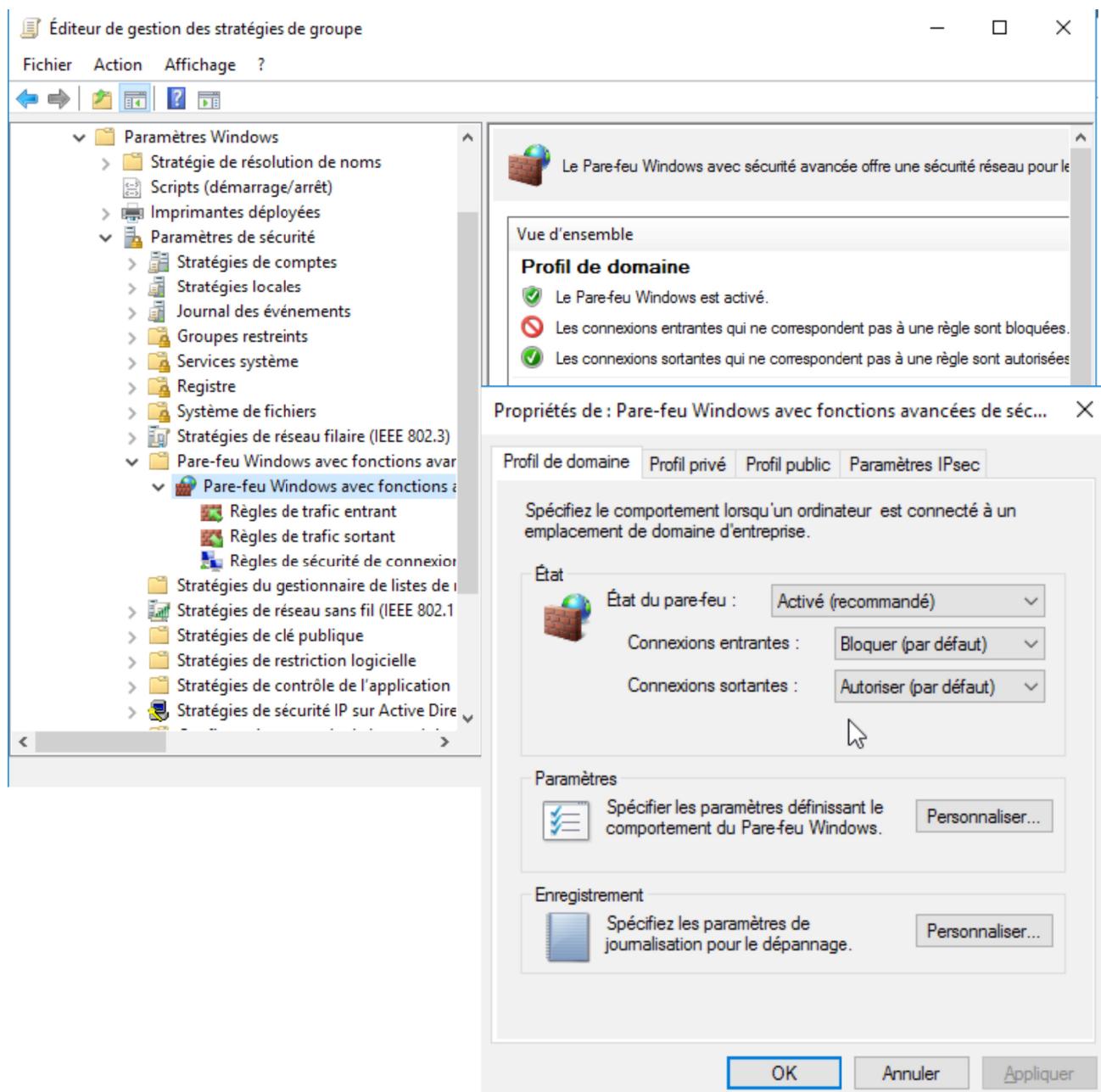
B- Politique concernant les firewalls :

Il s'agit ici d'imposer une configuration des firewalls pour les postes clients sans que les utilisateurs ne puissent la modifier.

Après avoir créé un nouveau GPO, accédez à l'éditeur de GPO et cherchez

Configuration ordinateur / Paramètre Windows / Paramètre de sécurité / Pare-feu Windows avec fonction avancées de sécurité

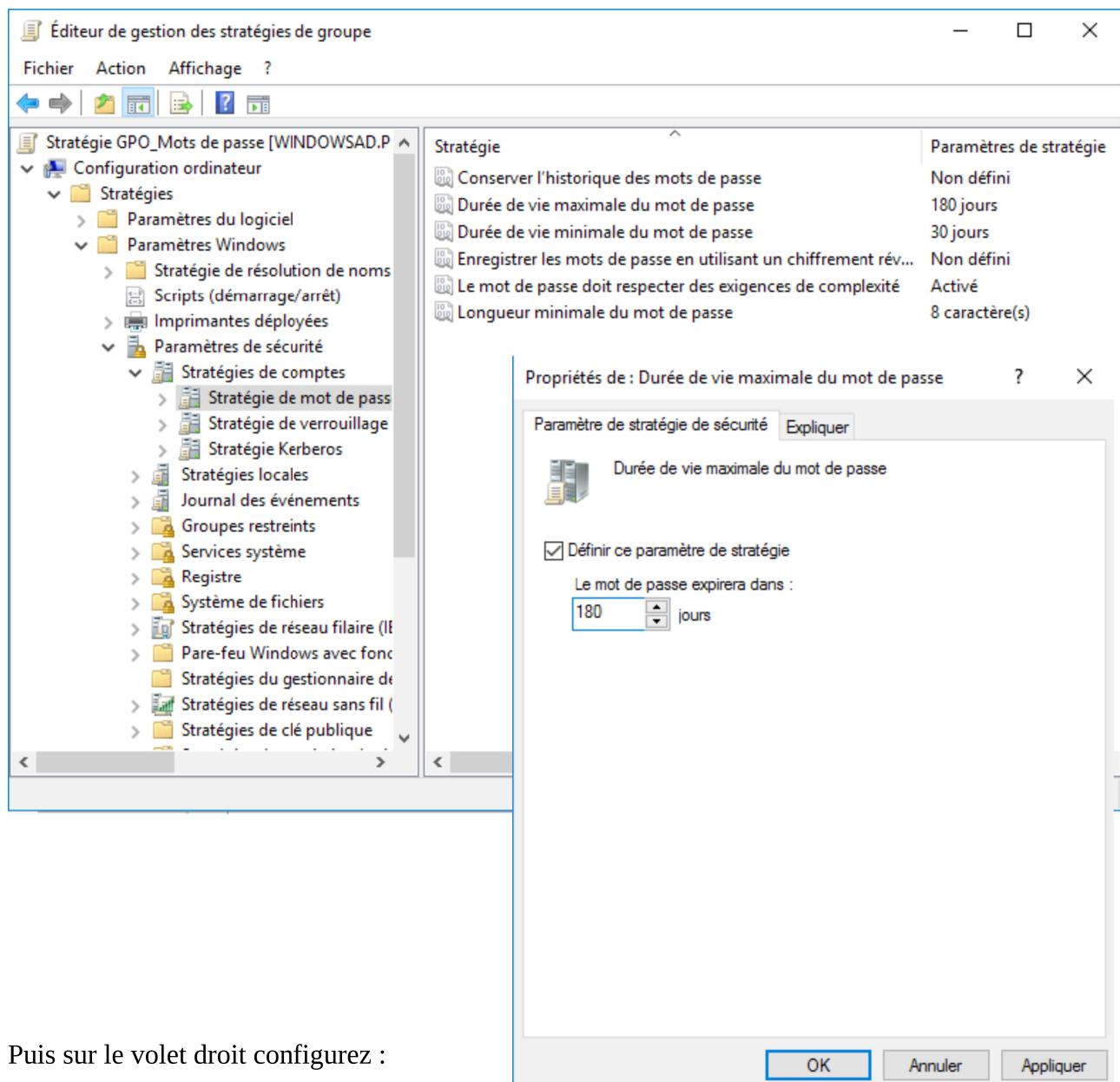
Puis sur le volet droit cliquez sur Propriété du Pare-feu Windows



C- Politique concernant les mots de passe :

Il s'agit ici d'imposer des règles sur la gestion des mots de passes utilisateurs
Après avoir créé un nouveau GPO, accédez à l'éditeur de GPO et cherchez

Configuration ordinateur / Paramètre Windows / Paramètre de sécurité / Stratégies des comptes / Stratégies de mots de passe



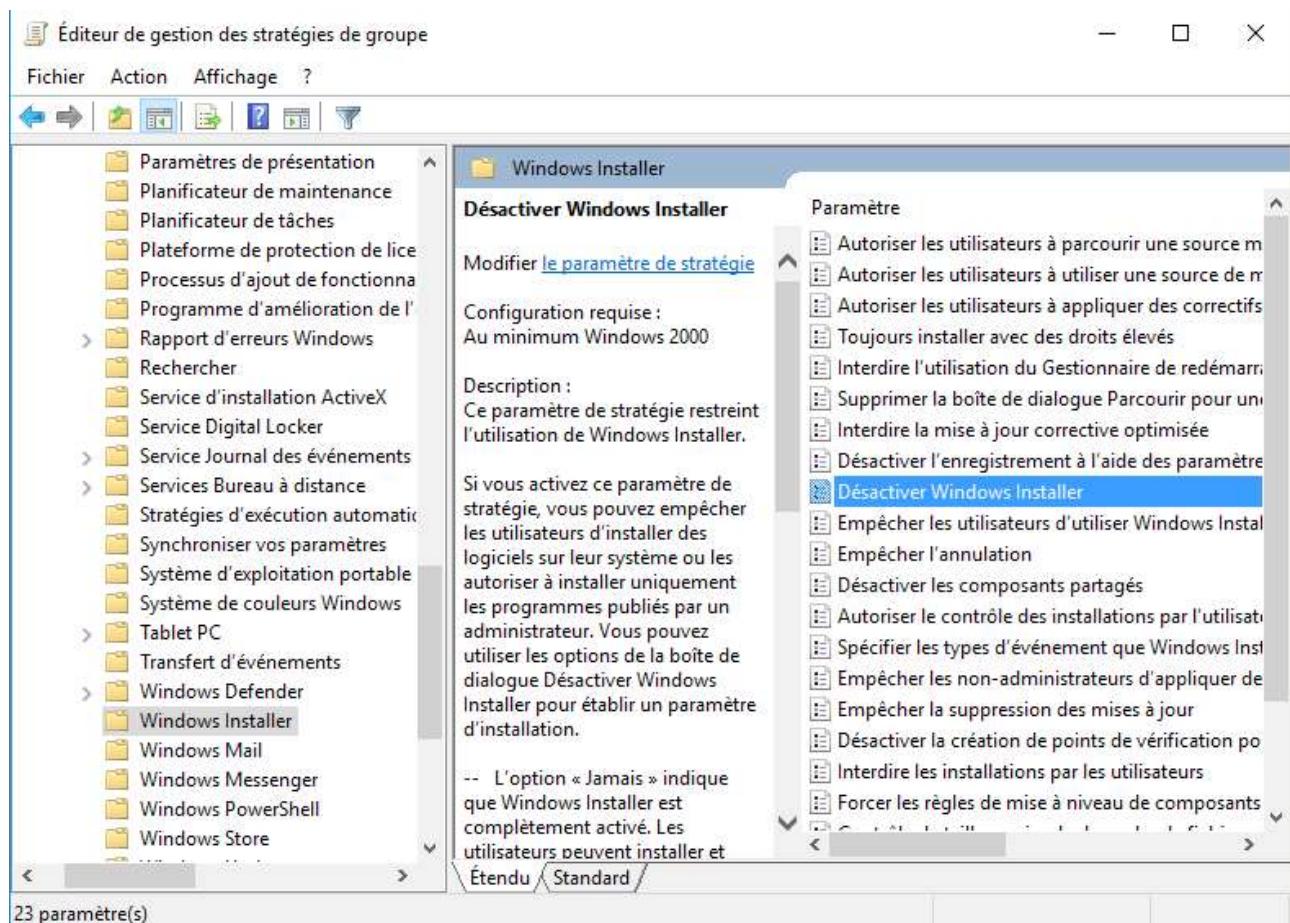
Puis sur le volet droit configurez :

- Durée de vie maximales du mots de passe
- Le mots de passe doit respecter des exigences de complexité
- Longueur minimale de mots de passe

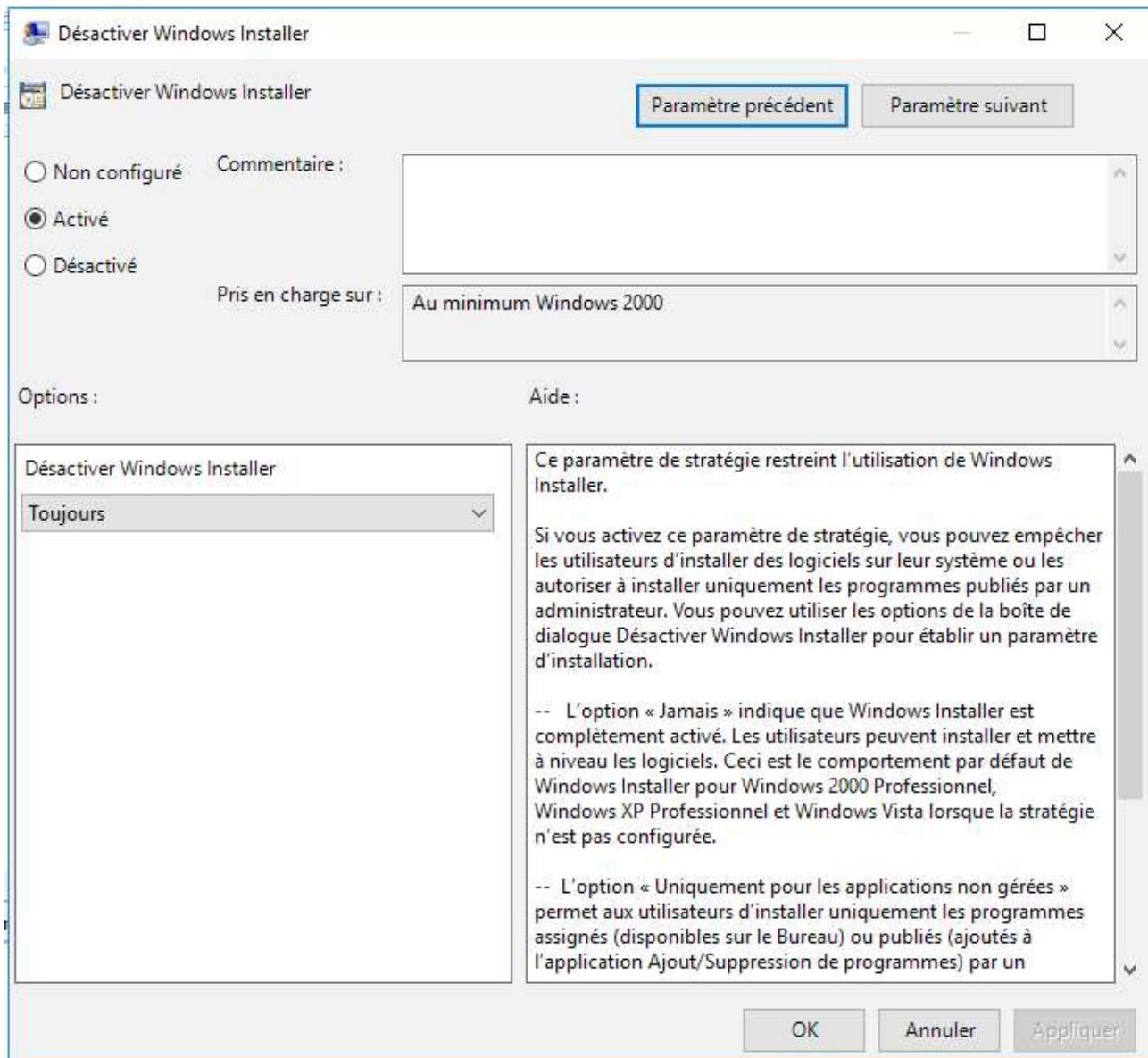
D- Politique concernant les logiciels installés :

Il s'agit ici de limiter l'installation de logiciel tiers par l'utilisateur
Après avoir créé un nouveau GPO, accédez à l'éditeur de GPO et cherchez

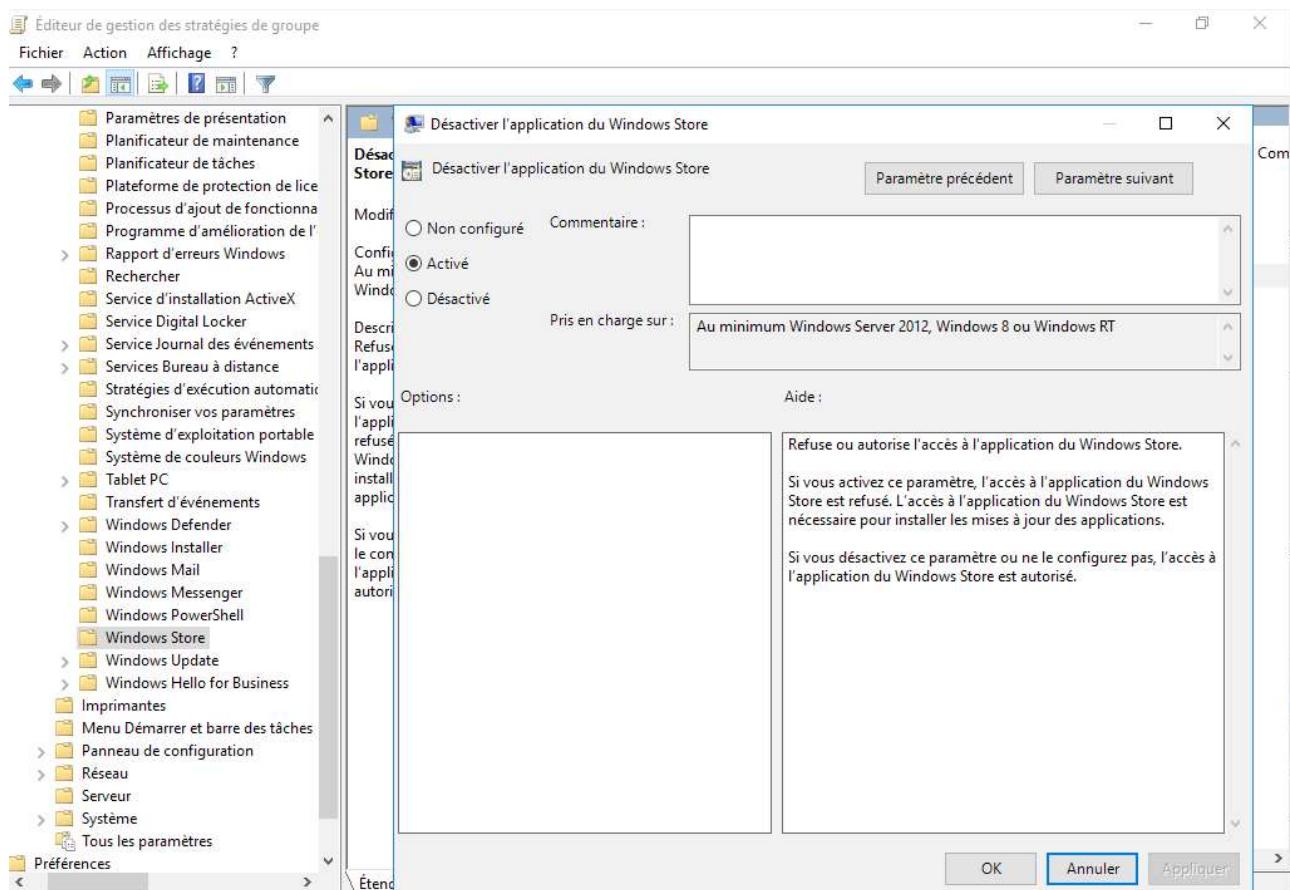
Configuration ordinateur / Stratégies / Modèle d'administration / Composant Windows / Windows installer



Puis sur le volet droit cliquez sur Désactiver Windows Installer.
Ceci aura pour effet d'interdire l'installation de logiciels tiers qui ne sont pas publiés par les administrateurs.



Nous pouvions également interdire l'usage du windows store



Nous pouvions interdire le téléchargement de fichier depuis le navigateur IE
 Configuration ordinateur \ Modèles d'administration \ Composants Windows \ Internet Explorer \ Panneau de configuration Internet \ Page de sécurité \ Zone Internet \ Autoriser les téléchargements de fichiers

The screenshot shows the 'Éditeur de gestion des stratégies de groupe' (Group Policy Management Editor) window. The left pane displays a navigation tree with various policy categories. The right pane shows the configuration details for the 'Zone Internet' policy.

Autoriser les téléchargements de fichiers

Description :
 Ce paramètre de stratégie permet d'indiquer si les téléchargements de fichiers sont autorisés depuis la zone. Cette option est définie par la zone de la page contenant le lien qui lance le téléchargement, et non pas la zone depuis laquelle le fichier est envoyé.

Si vous activez ce paramètre de stratégie, les fichiers peuvent être téléchargés depuis la zone.

Si vous désactivez ce paramètre de stratégie, les fichiers ne peuvent pas être téléchargés depuis la zone.

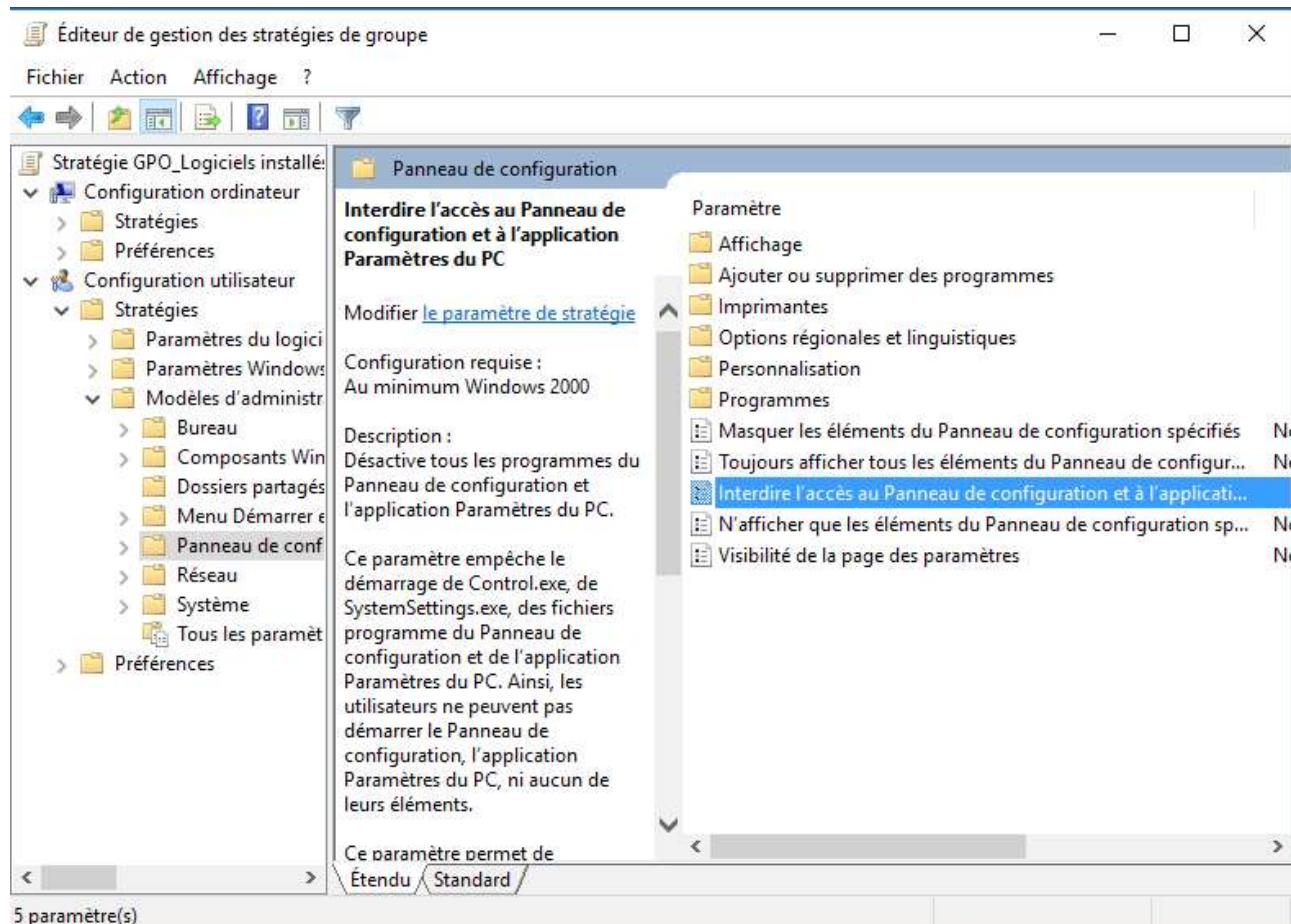
Si vous ne configurez pas ce paramètre de stratégie, les fichiers peuvent être téléchargés depuis la zone.

Paramètre	État
Accès aux sources de données sur plusieurs domaines	Non configuré
Autoriser les scripts actifs	Non configuré
Autoriser l'actualisation des métacharactères	Non configuré
Autoriser les opérations couper, copier ou coller dans le Pres...	Non configuré
Autoriser uniquement les domaines approuvés à utiliser le c...	Non configuré
Ne pas exécuter de logiciels anti-programme malveillant sur...	Non configuré
Autoriser les comportements des fichiers binaires et des scri...	Non configuré
Utiliser le bloqueur de fenêtres publicitaires	Non configuré
Afficher un contenu mixte	Non configuré
Télécharger les contrôles ActiveX signés	Non configuré
Télécharger les contrôles ActiveX non signés	Non configuré
Permettre de faire glisser du contenu entre les domaines da...	Non configuré
Permettre de faire glisser du contenu entre des domaines da...	Non configuré
Autoriser le glisser-déplacer ou le copier-colle des fichiers	Non configuré
Autoriser les téléchargements de fichiers	Désactivé
Autoriser les téléchargements de polices	Non configuré
Autoriser l'installation des éléments du Bureau	Non configuré
Autorisations Java	Non configuré
Lancement des applications et des fichiers dans un cadre IF...	Non configuré
Options d'ouverture de session	Non configuré
Activer la détection MIME	Non configuré
Naviguer dans des fenêtres et des cadres sur différents dom...	Non configuré
Autoriser le contenu actif sur des protocoles restreints à acc...	Non configuré
Ne pas proposer la sélection d'un certificat client lorsqu'il n'...	Non configuré
Demander confirmation pour les contrôles ActiveX	Non configuré
Demander confirmation pour les téléchargements de fichiers	Non configuré
Autoriser uniquement les domaines approuvés à utiliser les ...	Non configuré
Effectuer le rendu des filtres hérités	Non configuré

Mais aussi celui du panneau de configuration

Configuration utilisateur / Stratégies / Modèle d'administration / Panneau de configuration

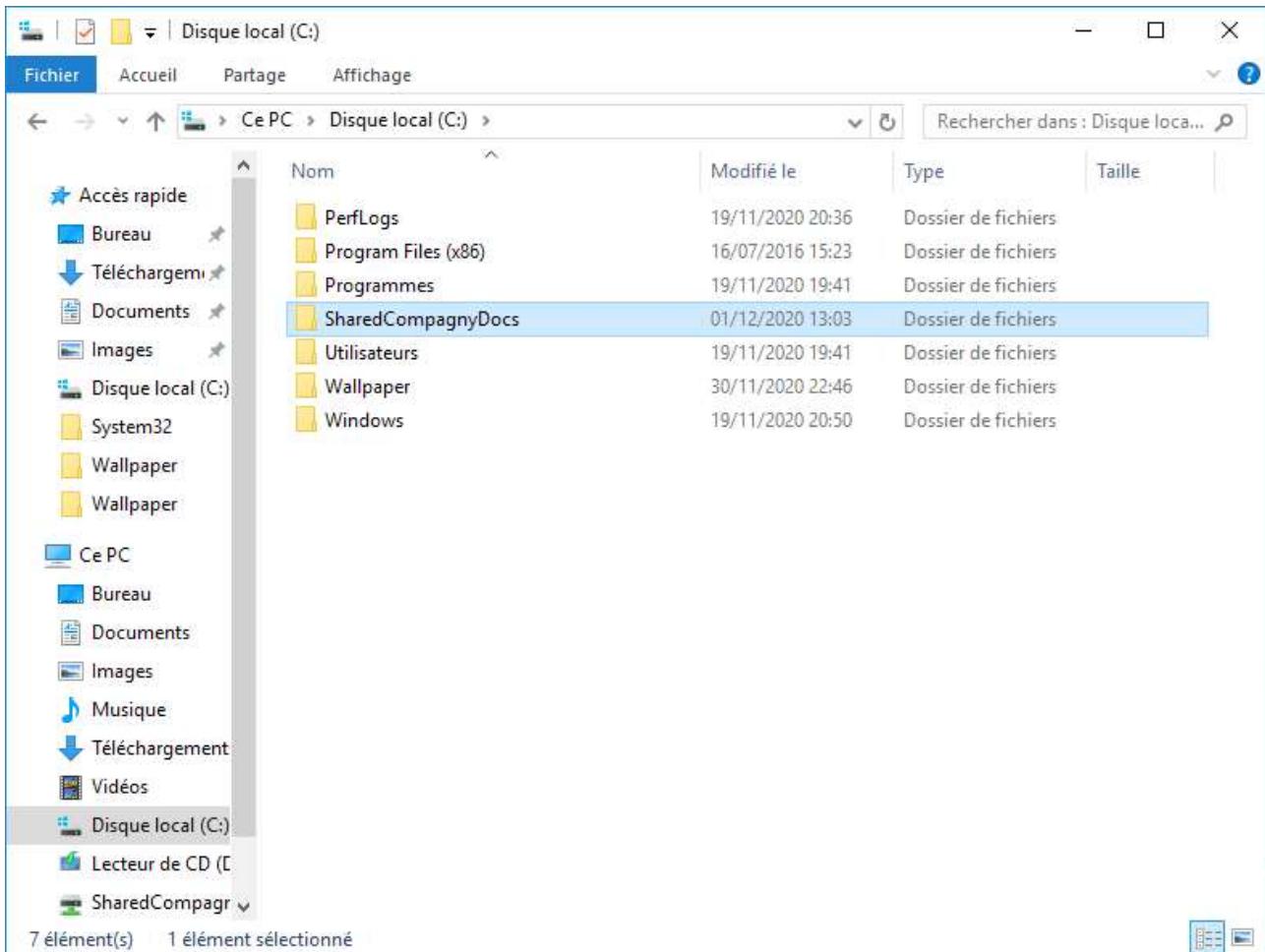
Cliquez sur Interdire l'accès au Panneau de configuration et à l'application paramètre windows



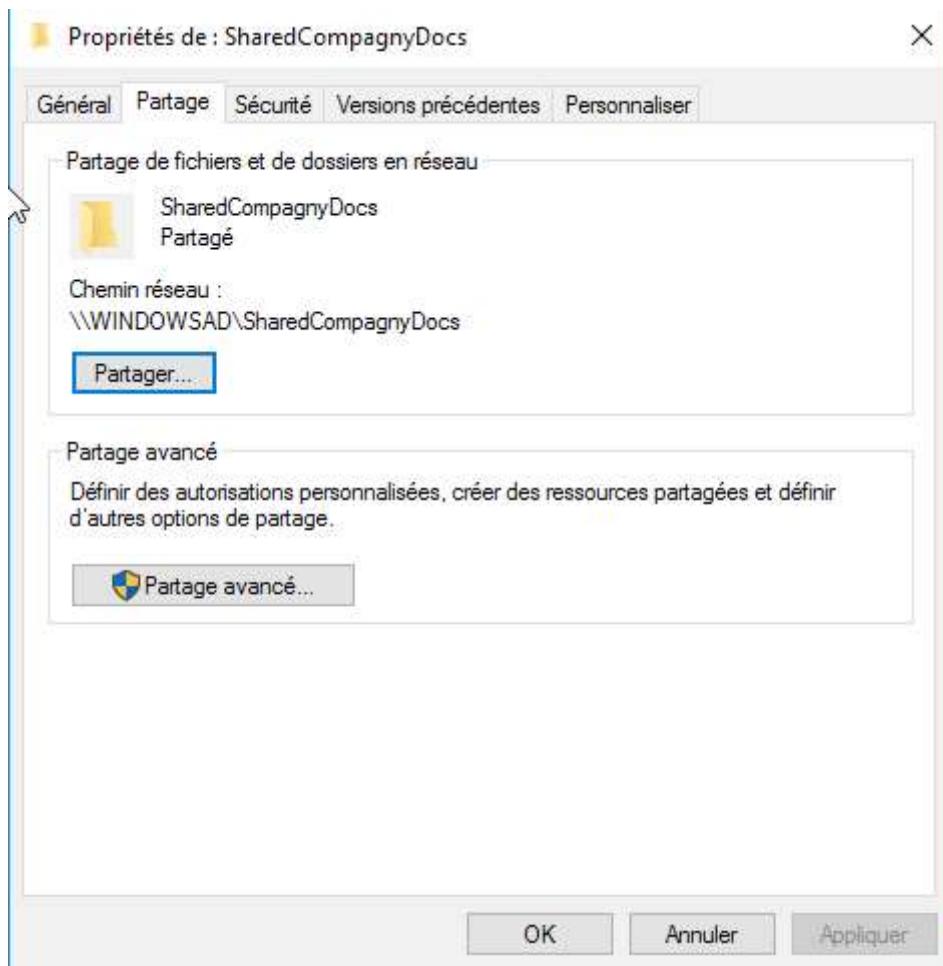
E- Politique concernant le mappage lecteur réseau :

Il s'agit de mapper un lecteur réseau afin que les utilisateurs puissent partager des fichiers sur le domaine.

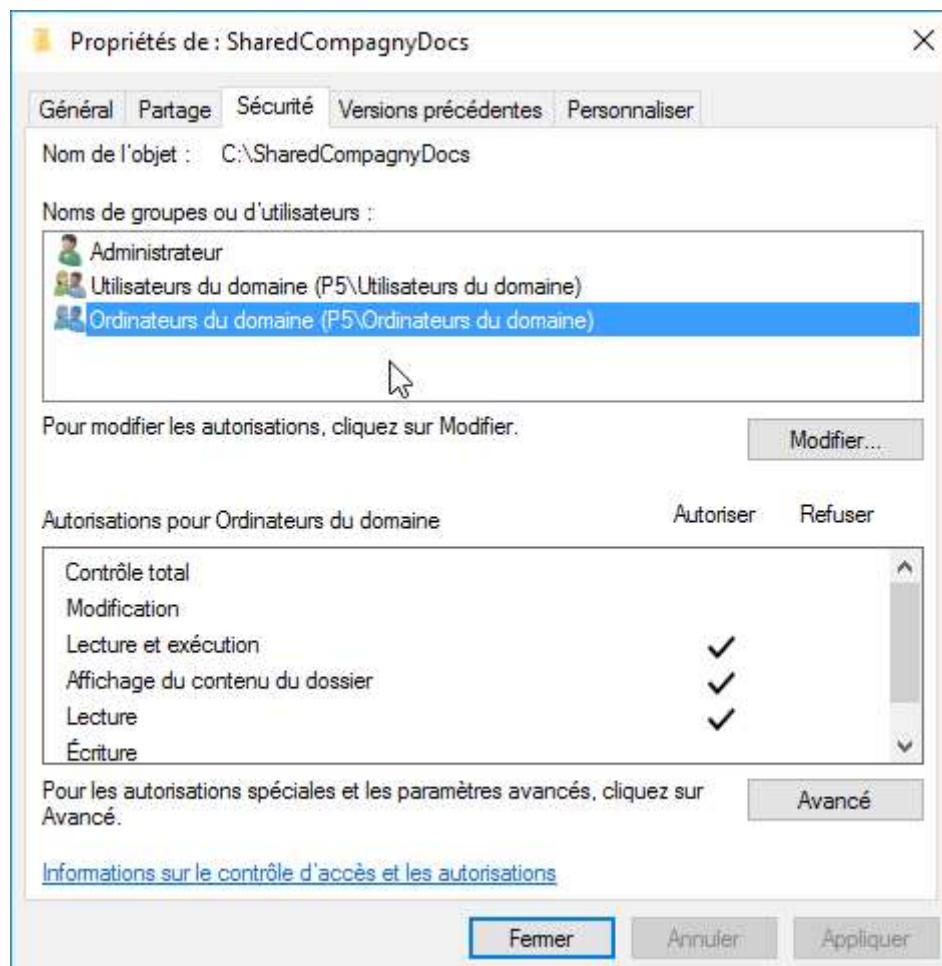
Tout d'abord, créer le dossier ShareCompagnyDocs. Notre choix sera de créer ce répertoire partagé à la racine du lecteur C: du contrôleur de domaine.



Nous partagerons ce répertoire pour le rendre accessible par nos postes utilisateurs.

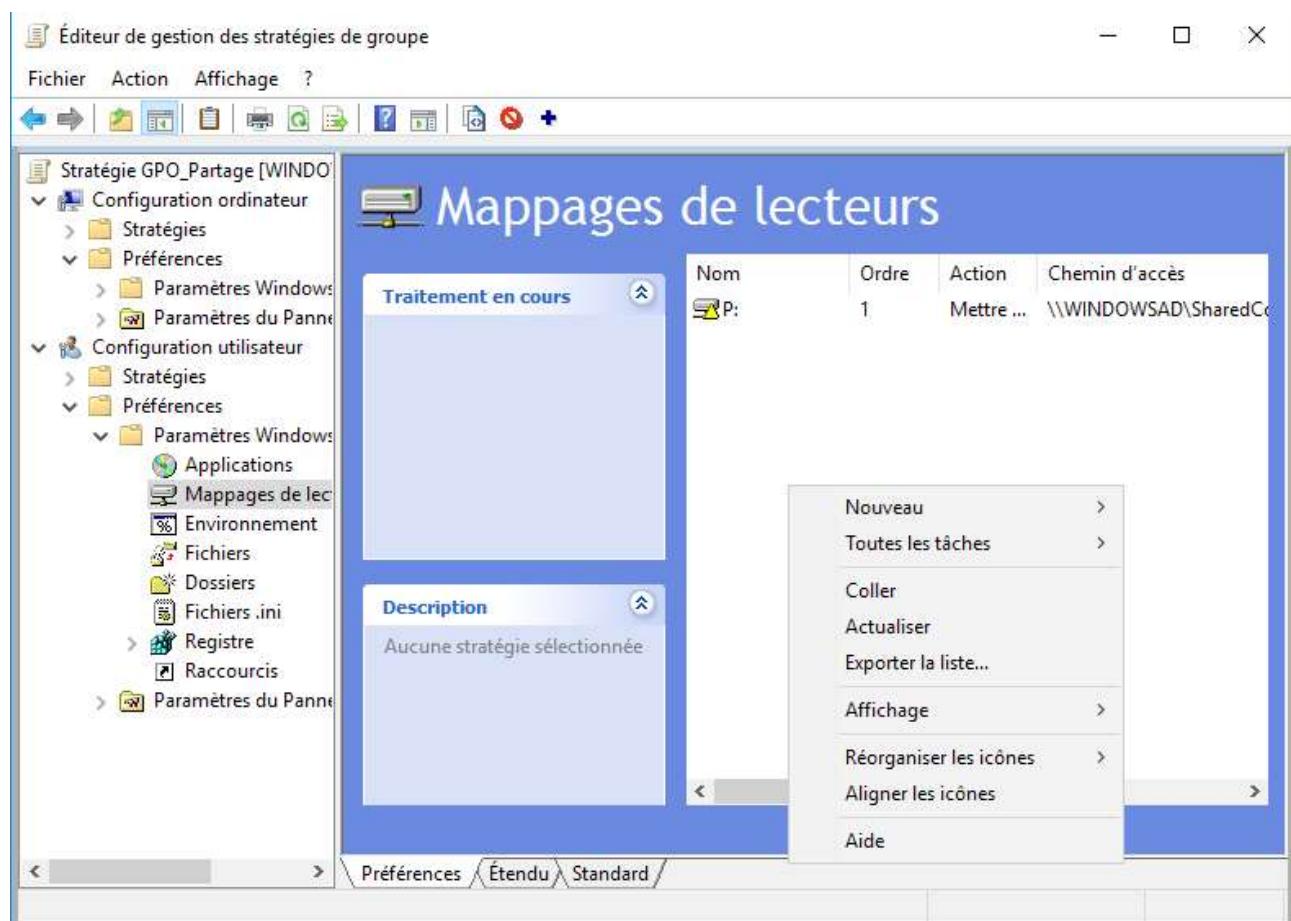


Nous attribuerons les droits de lecture au groupe «utilisateur du domaine» pour qu'il puisse venir chercher le fichier, car il s'agit d'une stratégie de type «Utilisateur».

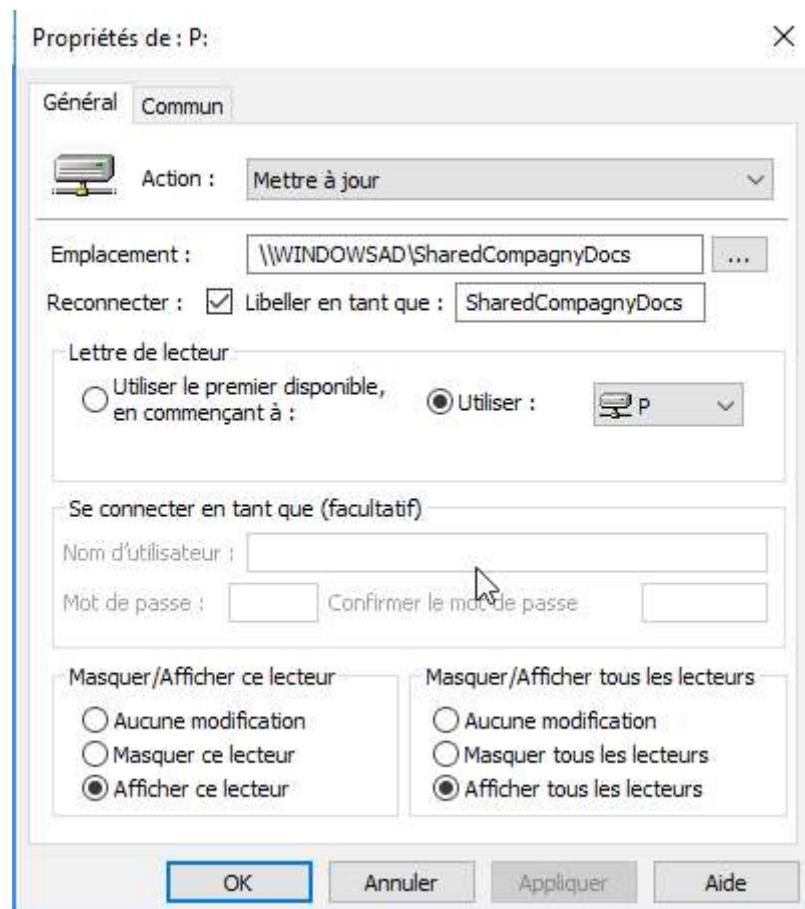


Nous pouvons maintenant créer la GPO.
On va créer un nouveau mappage de lecteur.

Configuration utilisateur / Préférences / Paramètres Windows / Mappages de lecteur



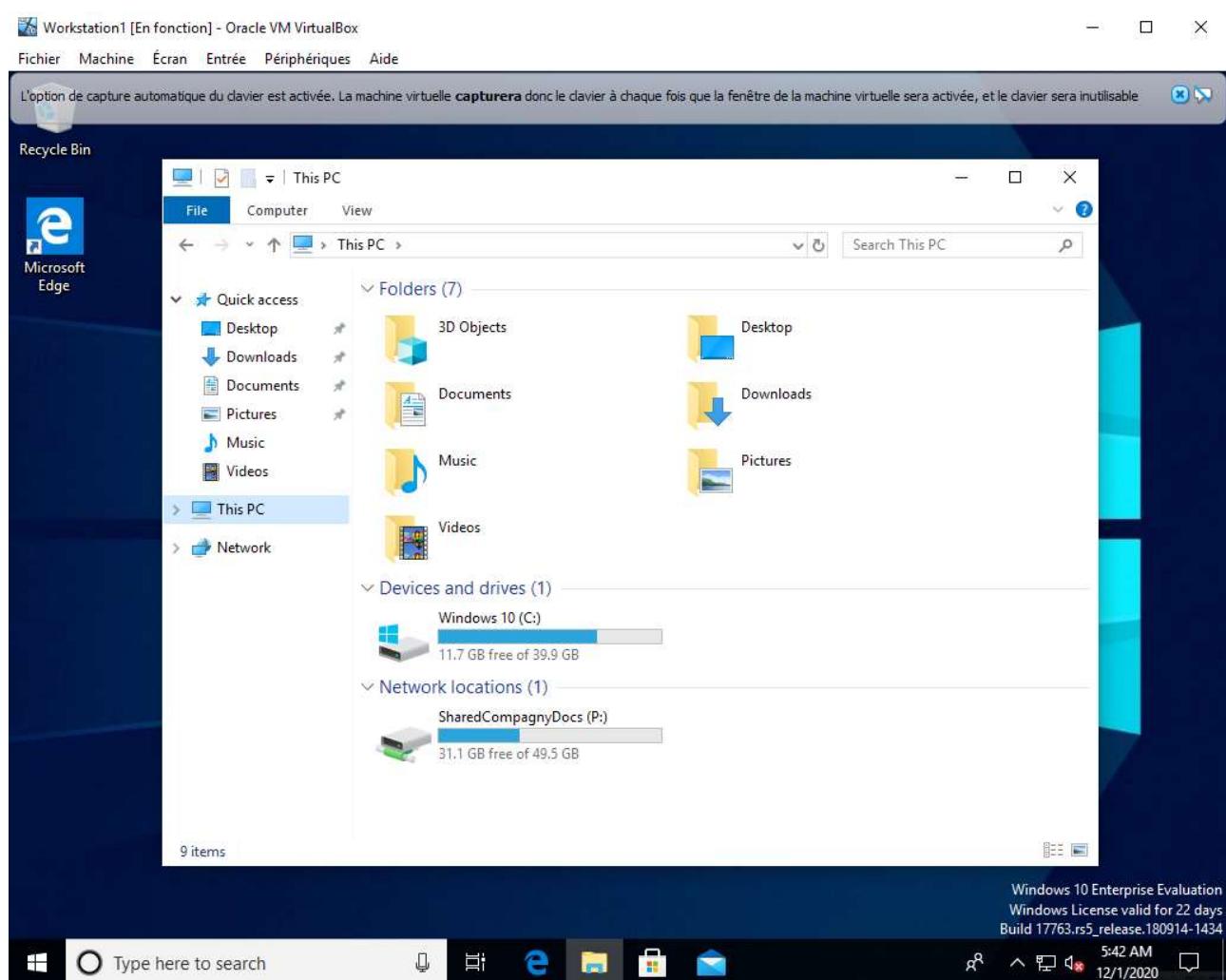
Prenons l'exemple suivant : je souhaite réaliser le mappage du partage "\\\WINDOWSAD\\SharedCompagnyDocs" sur les sessions de mes utilisateurs, de façon persistante, en le nommant "SharedCompagnyDocs" et utilisant la lettre "P". Ce qui donne :



Après validation, le lecteur réseau va apparaître dans la GPO. Il est possible de configurer plusieurs actions de mappages de lecteurs dans la même GPO.

Mappages de lecteurs					
	Nom	Ordre	Action	Chemin d'accès	Reconnecter
Traitement en cours	P:	1	Mettre ...	\\\\WINDOWSAD\\\\SharedCo... Oui	

Sur un poste du domaine vérifiez si le lecteur est visible.



Une fois tous les GPO configurés, ne pas oubliez de les activer en faisant un clique droit sur chacun et sélectionner «Appliqué»

