

# **Procédure de** **raccordement d'un** **site distant au** **travers d'un VPN.**

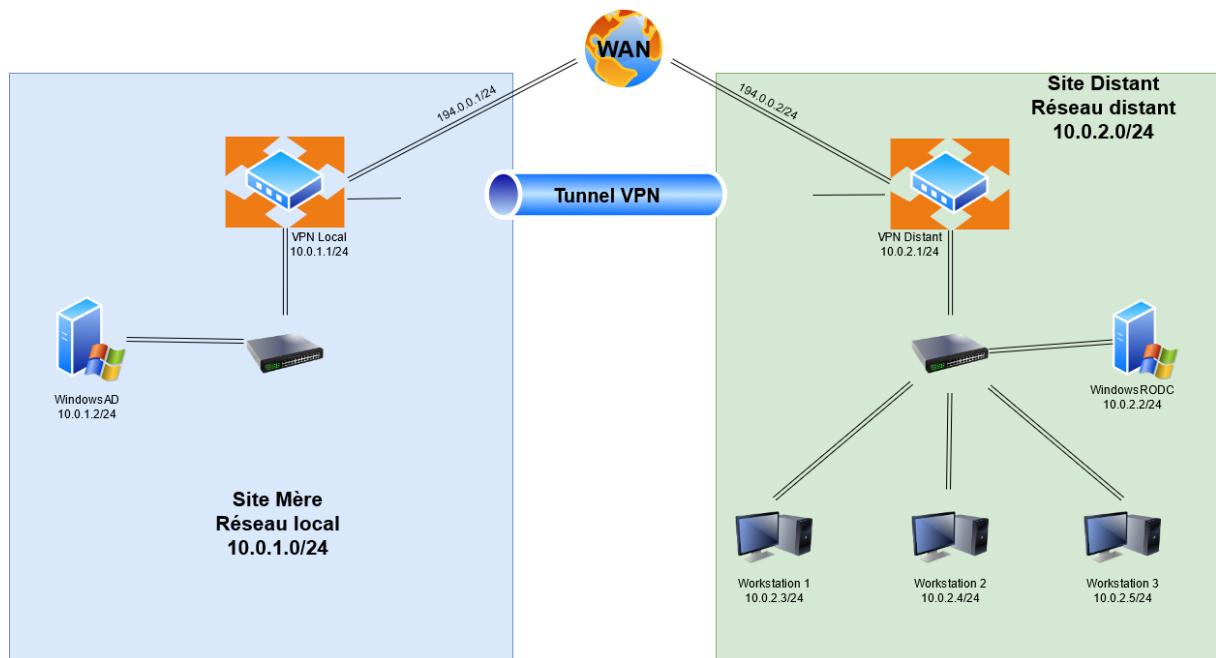
**Gestion des postes client via Active Directory**

|   |    |
|---|----|
| <b>I. Présentation de l'entreprise Afondlinux.</b>                                | 3  |
| A. Topologie et adressage réseau de l'entreprise                                  | 3  |
| B. Infrastructure système des deux sites  | 4  |
| 1. Serveur WindowsAD du site mère : Active Directory                              | 4  |
| 2. Serveur WindowsRODC du site distant : contrôleur de domaine en lecture seul    | 5  |
| 3. VPN Site-to-Site : sécurisation des flux                                       | 6  |
| 4. Principes d'IPsec  | 7  |
| <b>II. Installation et configuration de StrongSwan</b>                            | 8  |
| A. Installation de StrongSwan   | 8  |
| B. Configuration de StrongSwan  | 10 |
| <b>III. Installation et configuration du serveur WindowsAD</b>                    | 13 |
| A. Installation des rôles ADDS et DNS   | 13 |
| B. Promulgation du serveur en contrôleur de domaine                               | 18 |
| C. Création du répertoire partagé SharedCompanyDocs                               | 22 |
| <b>IV. Installation et configuration du serveur WindowsRODC</b>                   | 24 |
| <b>V. Gestion et promulgation en contrôleur de domaine du serveur WindowsRODC</b> | 28 |
| A. Gestion du serveur WindowsRODC   | 28 |
| B. Promulgation en tant que contrôleur de domaine                                 | 29 |
| <b>VI. Mise en place de la réPLICATION inter-sites</b>                            | 34 |
| <b>VII. Déclaration des ressources au sein d'Active Directory</b>                 | 38 |
| A. Unité d'organisation   | 38 |
| B. Création d'utilisateurs  | 40 |
| C. Les groupes  | 42 |
| <b>VIII. Stratégies de groupe ou GPO</b>  | 42 |
| A. GPO Papier peint du bureau   | 43 |
| B. GPO Mot de passe   | 46 |
| C. GPO Pare-feu   | 48 |
| D. GPO Mappage lecteur réseau   | 49 |
| E. Bloquer l'installation de logiciel   | 51 |
| <b>IX. Stratégie de réPLICATION des mots de passe</b>                             | 54 |
| <b>X. Quelques commandes utiles</b>   | 57 |

## I. Présentation de l'entreprise Afondlinux.

L'entreprise Afondlinux dispose d'un site mère à Pau, dont les postes de travail sont gérés par Active Directory. De plus, elle dispose aussi d'un autre site, appelé site distant à Bordeaux, composé de 3 personnes et 3 postes de travail. Le site de Bordeaux est géré à part, sans Active Directory. À ce jour, les employés de l'entreprise Afondlinux présent sur le site de Bordeaux n'ont pas accès à toutes les ressources de la société. Les deux sites sont reliés et communiquent via une connexion VPN.

### A. Topologie et adressage réseau de l'entreprise



|                       | WindowsAD            | VPN Local             | Vpn Distant           | WindowsRODC          |
|-----------------------|----------------------|-----------------------|-----------------------|----------------------|
| <b>IP</b>             | 10.0.1.2             | 195.0.0.1<br>10.0.1.1 | 194.0.0.2<br>10.0.2.1 | 10.0.2.2             |
| <b>Masque Gateway</b> | 255.255.255.0        | 255.255.255.0         | 255.255.255.0         | 255.255.255.0        |
| <b>DNS</b>            | 10.0.1.2<br>10.0.2.2 |                       |                       | 10.0.1.2<br>10.0.2.2 |

## B. Infrastructure système des deux sites

Pour des raisons pratiques, les machines serveurs Windows seront identiques ainsi que les postes clients. Chaque machine serveur sera équipée de la dernière version du système Microsoft Windows Server 2016 à jour.

Chaque poste client sera équipé du système d'exploitation Microsoft Windows 10 dans sa dernière version et à jour.

Concernant les machines VPN, il sera installé StrongSwan sur une distribution Debian.

### 1. Serveur WindowsAD du site mère : Active Directory

Sur le site mère, on installera Windows Server 2016 avec interface graphique. On y retrouvera un annuaire Active Directory. L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, qui contient différents objets, de différents types (utilisateurs, ordinateurs, etc.), l'objectif étant de centraliser deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information.

Administration  
centralisée et  
simplifiée

Unifier  
l'authentification

Identifier les  
objets sur le  
réseau

Référencer les  
utilisateurs et  
ordinateurs

**Administration centralisée et simplifiée** : la gestion des objets, des comptes utilisateurs et ordinateurs est simplifiée, car centralisée dans l'annuaire Active Directory.

**Unifier l'authentification** : un utilisateur authentifié sur une machine, elle-même authentifiée, pourra accéder aux ressources stockées sur d'autres serveurs ou ordinateurs enregistrés dans l'annuaire. Ainsi, une authentification et un seul compte permettront d'accéder à tout un système d'information.

**Identifier les objets sur le réseau** : chaque objet enregistré dans l'annuaire est unique, ce qui permet d'identifier facilement un objet sur le réseau et de le retrouver ensuite dans l'annuaire.

**Référencer les utilisateurs et les ordinateurs** : l'annuaire ressemble à une base de données qui référence les utilisateurs, les groupes et les ordinateurs d'une entreprise permettant de réaliser de nombreuses opérations : authentification, identification, stratégie de groupe, déploiement de logiciels, etc.

On y créera aussi des **GPO**, c'est-à-dire des stratégies de groupe, qui permettent au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques.

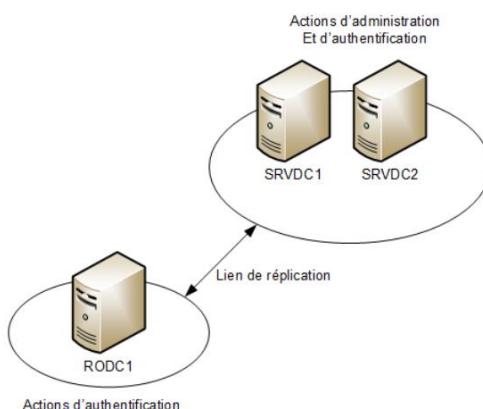
Chaque stratégie dispose de ses propres paramètres, définis par l'administrateur système, et qui seront appliqués ensuite à des postes de travail, des serveurs ou des utilisateurs.

Enfin, un dossier partagé sera créé afin que les utilisateurs du site distant aient accès à certaines ressources de l'entreprise.

## **2. Serveur WindowsRODC du site distant : contrôleur de domaine en lecture seul**

Sur le site distant, on installera Windows Server 2016 en mode Core, c'est à dire sans interface graphique. On y installera par la suite un contrôleur de domaine en lecture seule ou RODC « Read Only Domain Controller ».

L'intérêt est d'avoir un contrôleur de domaine qui contient toutes les informations qu'un contrôleur classique dispose. Ces informations étant stockées en lecture seule aucune modification ne pourra y être réalisée directement dessus. L'intérêt étant de sécuriser le site distant, d'améliorer l'authentification des utilisateurs par la mise en cache des requêtes d'authentification, et d'avoir un rôle de cache DNS ce qui générera moins de trafic sur la liaison WAN et consommera moins de bande passante.



### 3. VPN Site-to-Site : sécurisation des flux

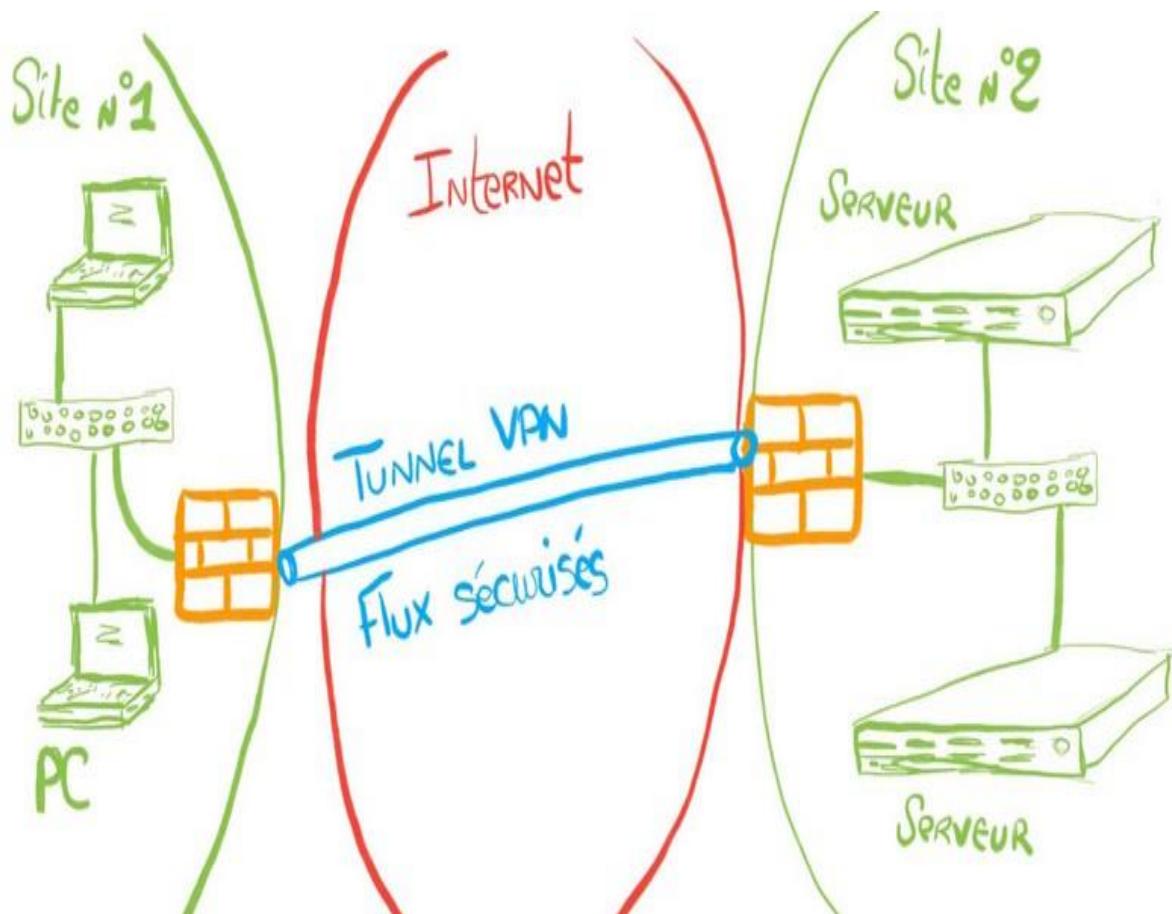
Un **VPN Site-to-Site** est un **VPN** qui permet de joindre deux réseaux de type **LAN** distants de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseau et qu'un simple routeur les séparent.

Le site distant doit pouvoir se connecter aux ressources du site mère de manière transparente malgré leur distance.

L'objectif est de créer un lien virtuel entre le site mère et le site distant, par lequel les données échangées seront sécurisées et isolées du reste du trafic, c'est là tout l'intérêt du **VPN** et cette notion de "**privé**". Le **VPN** permet de créer une extension virtuelle du réseau local jusqu'à un autre réseau ou site ou jusqu'à un poste de travail distant.

On établit une connexion **VPN** à travers le **WAN** afin de joindre les deux réseaux mais également de manière à sécuriser ces flux au travers un chiffrement de bout en bout des données.

Dans notre cas on installera IPSEC qui est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau. IPsec permet de sécuriser les échanges sur un réseau TCP/IP et propose des services de sécurité totalement transparents pour les applications. IPsec assure la confidentialité et la protection contre l'analyse du trafic, mais aussi l'authentification des données (et de leur origine) ainsi que l'intégrité des données.



#### 4. Principes d'IPsec

IPsec n'est pas un protocole unique mais un ensemble de protocoles dont le but est de fournir un haut niveau de sécurité dans l'échange des paquets IP. On se situe donc au niveau de la couche réseau. Les services doivent utiliser la cryptographie et être interopérables. Les points clés sont :

- **Confidentialité** : l'émetteur chiffre les paquets avant de les transmettre sur l'Internet.
- **Intégrité** : le récepteur vérifie que les paquets reçus n'ont pas été altérés lors de la transmission.
- **Authentification** : le récepteur vérifie l'identité de l'émetteur par clés partagées ou certificats numériques signés.
- **Anti rejeu** : le récepteur examine les paquets et rejette les paquets périmés et/ou répétés.

IPsec utilise le protocole IKE (Internet Key Exchange) pour établir un tunnel et utilise aussi la mise en place d'associations de sécurité SA (Security association), en s'appuyant sur le protocole ESP (Encapsulating Security Payload). L'échange de clé Diffie-Hellman est utilisée dans les échanges du protocole IKE pour générer un secret partagé entre les deux extrémités de façon sécurisée. Le secret partagé est utilisé pour calculer une valeur qui sert ensuite aux calculs des clés utilisées dans les phases 1 et 2 du protocole IKE. Des groupes auxquels ont été associé une longueur de clé et une fonction de chiffrement doivent être choisis pour mettre en œuvre l'échange de clés. Plus la clé comprend un nombre de bits important, plus le secret est solide. En contrepartie, le temps de calcul est lui aussi plus important. Cette méthode est appelée à chaque établissement ou renouvellement d'association de sécurité.

L'objectif du mécanisme d'échange IKE, via le protocole ISAKMP, est de permettre aux deux extrémités du tunnel en communication d'établir une association de sécurité. Cette association demande au moins deux étapes.

- **IKE phase 1**, ISAKMP-SA  
Durant cette première phase, il y a établissement d'une session sécurisée ISAKMP entre les deux extrémités que l'on appelle ISAKMP SA.
- **IKE phase 2**, IPsec-SA  
Cette phase ne peut se dérouler que sous la protection du tunnel ISAKMP établi en phase 1. À la différence de la phase 1, on ne parle plus d'une association de sécurité bidirectionnelle utilisant la même clé partagée entre les deux extrémités. Ici, il faut établir deux associations unidirectionnelles entre les mêmes extrémités. Une fois que ces deux SA sont en place, le tunnel IPsec est actif. Les paramètres négociés sont quasiment les mêmes que lors de la phase 1 : algorithme de hachage, algorithme de chiffrement, groupe Diffie Hellman, informations anti rejeu, durée de vie de l'association de sécurité.

## **II. Installation et configuration de StrongSwan**

L'installation des deux machines Linux Debian sera identique. Seule la configuration des adresses IP différera d'un site à l'autre.



### **A. Installation de StrongSwan**

Nous commençons via la commande **apt-get update** par rechercher les mises à jour disponibles pour notre système en se basant sur les sources définies dans **etc/apt/source.list**.

```
Debian GNU/Linux 10 vpn-local tty1
vpn-local login: root
Password:
Linux vpn-local 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@vpn-local:~# apt-get update
Atteint :1 http://security.debian.org/debian-security buster/updates InRelease
Atteint :2 http://deb.debian.org/debian buster InRelease
Atteint :3 http://deb.debian.org/debian buster-updates InRelease
Lecture des listes de paquets... Fait
root@vpn-local:~#
```

Puis nous installons les mises à jour identifiée avec la commande **apt-get upgrade**.

```
root@vpn-local:~# apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@vpn-local:~# _
```

Enfin nous installons **StrongSwan**, un démon **IPsec** open source que nous allons configurer en tant que serveur **VPN**. Nous allons également installer le composant infrastructure de clé publique (ICP) afin que nous puissions créer une autorité de certification pour fournir des identifiants pour notre infrastructure.

```
root@vpnlocal:~# apt-get install strongswan strongswan-pki libcharon-extra-plugins
```

```

Configuration de strongswan-starter

Abandon de l'ancien système de lancement

Les versions précédentes du paquet de strongSwan permettaient de choisir entre trois séquences possibles de lancement au démarrage de la machine. Comme l'organisation générale des scripts de lancement a été profondément modifiée dans le système, cela n'est désormais plus utile. Pour toutes les nouvelles installations, ainsi que pour les anciennes qui fonctionnaient selon un des trois modes prédéfinis, une séquence de lancement sûre va être mise en place. Si vous effectuez une mise à jour et avez modifié les paramètres de lancement de strongSwan, veuillez consulter le fichier NEWS.Debian pour trouver les informations qui vous permettront d'adapter vos réglages.

<OK>

```

```

Disabling opportunistic encryption (OE) in config file ... Created symlink /etc/systemd/system/multi-user.target.wants/strongswan.service → /lib/systemd/system/strongswan.service.
Paramétrage de strongswan-libcharon (5.7.2-1) ...
Paramétrage de strongswan-charon (5.7.2-1) ...
Paramétrage de strongswan-pki (5.7.2-1) ...
Paramétrage de libstrongswan-extra-plugins (5.7.2-1) ...
Paramétrage de libstrongswan-standard-plugins (5.7.2-1) ...
Paramétrage de strongswan (5.7.2-1) ...
Traitement des actions différentes (<> triggers <>) pour man-db (2.8.5-2) ...
Traitement des actions différentes (<> triggers <>) pour systemd (241-7~deb10u7) ...
root@vpnlocal:~#

```

L'étape suivante consiste à la création d'une autorité de certification pour notre serveur VPN.

Un serveur IKEv2 requiert un certificat pour s'identifier auprès de ses clients. Pour créer le certificat requis, le paquet **strongswan-pki** est livré avec un utilitaire appelé **pki** pour générer une autorité de certification et des certificats serveurs.

L'idée est d'avoir autorité de certification qui signera les certificats pour les deux serveurs **VPN**.

Nous allons donc créer **une clé privée** pour **l'autorité de certification** et signer le certificat de l'autorité de certification avec la clé privée. Puis on distribuera le certificat aux deux serveurs **VPN**. Ensuite, on créera une clé privée pour le serveur **VPN local** et on signera le certificat. On fera de même pour le serveur **VPN distant**.

Il est recommandé d'avoir une autorité de certification sur un serveur distinct, mais nous utiliserons ici le serveur VPN Local pour créer les certificats.

Nous commençons par créer un répertoire appelé **certs** dans lequel nous stockerons les certificats et l'on se déplace à l'intérieur.

```

root@vpn-local:~# mkdir /certs && cd /certs
root@vpn-local:/certs# _

```

Puis on crée la clé privée pour l'autorité de certification appelée **caKey.der**.

```

root@vpn-local:/certs# pki --gen > caKey.der
root@vpn-local:/certs#

```

Ensuite, je crée un certificat CA et le signe avec ma clé privée que je viens de créer.

```

root@vpn-local:/certs# pki --self --in caKey.der --dn "C=FR, O=dbreton, CN=afondlinux" --ca > caCert.der

```

Seul le certificat (pas la clé privée) devra être stocké dans le répertoire **/etc/ipsec.d/cacerts** sur les deux hôtes.

```
root@vpn-local:/certs# /bin/cp -rf caCert.der /etc/ipsec.d/cacerts
root@vpn-local:/certs# scp caCert.der root@194.0.0.2:/etc/ipsec.d/cacerts_
```

L'étape suivante consiste à créer une clé privée et un certificat pour host1 et à laisser l'autorité de certification les signer.

On crée d'abord une clé privée pour le serveur **vpn-local**.

```
root@vpn-local:/certs# pk1 --gen > vpn-local.der
```

On crée un certificat signé pour le serveur **vpn-local**.

```
root@vpn-local:/certs# pk1 --pub --in vpn-local.der | pk1 --issue --cacert caCert.der --cakey caKey.
der --dn "C=FR, O=dreton, CN=vpn-local.afondlinux" > vpn-localCert.der
```

La clé privée du serveur **vpn-local** va dans **/etc/ipsec.d/private** et le certificat va dans **/etc/ipsec.d/certs/**.

```
root@vpn-local:/certs# /bin/cp -rf vpn-localCert.der /etc/ipsec.d/certs/
root@vpn-local:/certs# /bin/cp -rf vpn-local.der /etc/ipsec.d/private
```

Nous allons effectuer la même chose pour le serveur **vpn-distant** depuis le serveur **vpn-local** et déplacerons les différents certificats et clés sur le serveur **vpn-distant**.

Maintenant que les certificats sont en place, nous pouvons configurer les fichiers de configuration.

## B. Configuration de StrongSwan

**StrongSwan** dispose d'un fichier de configuration par défaut, mais nous allons devoir faire la plupart de la configuration.

Tout d'abord, nous allons demander à **StrongSwan** d'enregistrer les états des démons pour le débogage et d'autoriser les connexions en double.

```
config setup
    charondebug="all"
    uniqueids=no
```

Ensuite nous renseignons la partie générale du fichier de configuration

```
conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    authby=pubkey
    keyexchange=ikev2
    mobike=no
    type=tunnel
```

- **Ikelifetime**= durée de connexion avant renégociation
- **Authby**= méthode d'authentification
- **Keyingtries**= nombre de tentative pour initier une connexion
- **Mobike**= active le protocole IKEv2 MOBIKE.
- **Keyexchange**= méthode d'échange de clés, quel protocole doit être utilisé pour initialiser la connexion.
- **Type**= type de connexion

Puis la partie liée à notre tunnel VPN.

```
conn vpn
    left=194.0.0.1
    leftcert=host1Cert.der
    leftid="C=FR, O=dbreton, CN=host1.afondlinux.org"
    leftsubnet=10.0.1.0/24
    right=194.0.0.2
    rightid="C=FR, O=dbreton, CN=host2.afondlinux.org"
    rightsubnet=10.0.2.0/24
    ike=aes256-sha2_256-modp2048!
    esp=aes256-sha2_256!
    auto=start
```

- **left**= fait référence à l'identification du serveur vpn-local que l'on configure.
- **leftid**= Cette option contrôle le nom que le serveur présente aux clients. Combiné à l'option **leftcert**, l'option **leftid** garantit que le nom configuré du serveur et le nom distinctif (DN) contenus dans le certificat public correspondent.
- **leftcert**= Cette option est le chemin d'accès au certificat public pour le serveur. Sans celui-ci, le serveur ne pourra pas s'authentifier lui-même auprès des clients, ou terminer de négocier la configuration d'IKEv2.
- **leftsubnet**= Indique les sous réseaux qui sont accessibles derrière le serveur.

Il en va de même pour la partie droite. Les deux dernières lignes spécifient les différents algorithmes d'échange de clés, de hachage, d'authentification et de cryptage que **StrongSwan** permettra à différents clients d'utiliser.

Le fichier final ressemblera à cela et sera configuré de la même manière sur le serveur **vpn-distant**.

```
config setup
    charondebug="all"
    uniqueids=no

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    authby=pubkey
    keyexchange=ikev2
    mobike=no
    type=tunnel

conn vpn
    left=194.0.0.1
    leftcert=host1Cert.der
    leftid="C=FR, O=dbreton, CN=host1.afondlinux.org"
    leftsubnet=10.0.1.0/24
    right=194.0.0.2
    rightid="C=FR, O=dbreton, CN=host2.afondlinux.org"
    rightsubnet=10.0.2.0/24
    ike=aes256-sha2_256-modp2048!
    esp=aes256-sha2_256!
    auto=start
```

Nous allons indiquer à **StrongSwan** où trouver notre clé privée :

```
root@vpn-local:~# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created private key
include /var/lib/strongswan/ipsec.secrets.inc
: RSA host1.der
```

Notre serveur VPN est maintenant configuré. Nous pouvons établir le tunnel avec la commande suivante :

```
root@vpn-local:~# ipsec start
Starting strongSwan 5.7.2 IPsec [starter]...
charon is already running (/var/run/charon.pid exists) -- skipping daemon start
starter is already running (/var/run/starter.charon.pid exists) -- no fork done
```

Ou encore avoir des informations sur le tunnel avec la commande suivante :

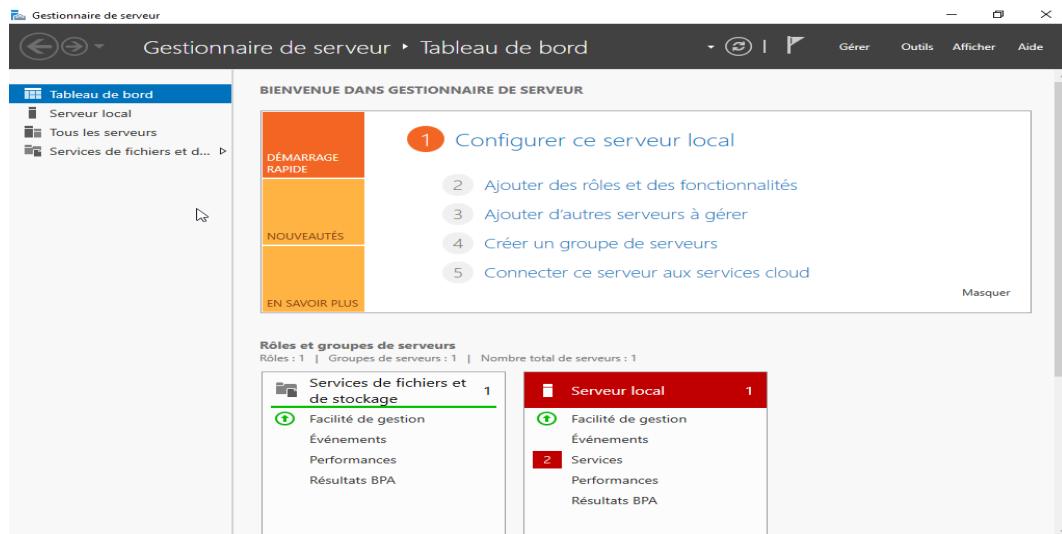
```
root@vpn-local:~# ipsec statusall
Status of IKE charon daemon (strongSwan 5.7.2, Linux 4.19.0-16-amd64, x86_64):
  uptime: 6 hours, since May 27 19:08:08 2021
  malloc: sbrk 1757184, mmap 0, used 1035648, free 721536
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints p
ubkey pkcs1 pkcs7 pkcs8 pkcs12 ppg dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr k
ernel-netlink resolve socket-default commark farp stroke updown eap-identity eap-aka eap-md5 eap-gt
c eap-mschapv2 eap-radius eap-tls eap-ttls eap-tnc xauth-generic xauth-eap xauth-pam tnc-tnccs dhcp
lookup error-notify certexpire led addrblock unity counters
Listening IP addresses:
  194.0.0.1
  10.0.1.1
Connections:
  vpn: 194.0.0.1...194.0.0.2 IKEv2
  vpn: local: [C=FR, O=dbreton, CN=host1.afondlinux.org] uses public key authentication
  vpn: cert: "C=FR, O=dbreton, CN=host1.afondlinux.org"
  vpn: remote: [C=FR, O=dbreton, CN=host2.afondlinux.org] uses public key authentication
  vpn: child: 10.0.1.0/24 === 10.0.2.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
  vpn[9]: ESTABLISHED 34 minutes ago, 194.0.0.1[C=FR, O=dbreton, CN=host1.afondlinux.org]...1
  94.0.0.2[C=FR, O=dbreton, CN=host2.afondlinux.org]
    vpn[9]: IKEv2 SPIs: ad0768aafdb4960e_i* c832adbc5a885a28_r, public key reauthentication in
    18 minutes
    vpn[9]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
    vpn{32}: INSTALLED, TUNNEL, reqid 8, ESP SPIs: c8c3f505_i c5334224_o
    vpn{32}: AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 12 minutes
    vpn{32}: 10.0.1.0/24 === 10.0.2.0/24
```

### **III. Installation et configuration du serveur WindowsAD**

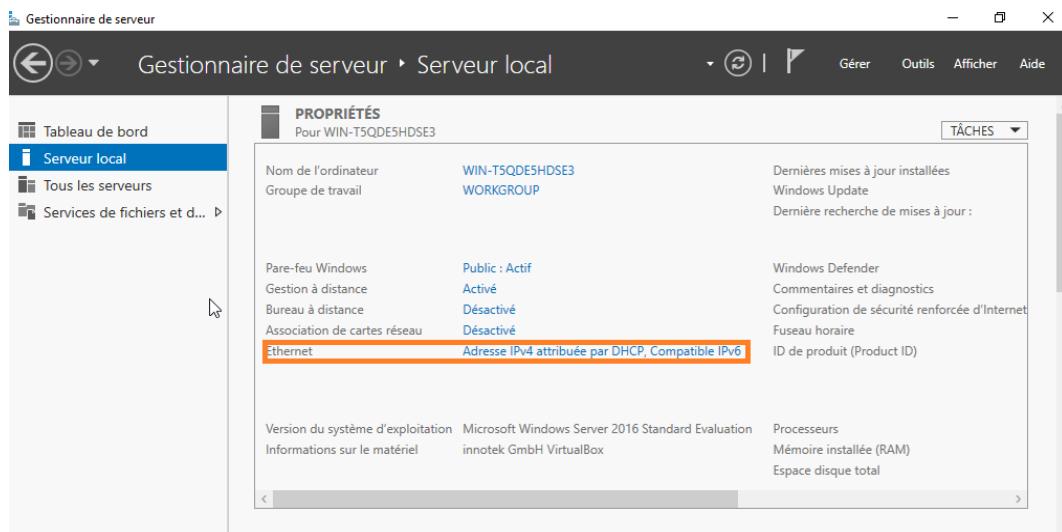
Pour rappel, un annuaire **Active Directory** c'est le service dédié entreprise proposé par Microsoft qui permet de centraliser et gérer des ressources, et qui se base sur le protocole **LDAP** (Lightweight Directory Access Protocol). L'objectif d'**Active Directory** est de fournir des services centralisés d'identification et d'authentification à un réseau informatique en se basant sur une organisation hiérarchisée des ressources d'une entreprise. La machine sur laquelle AD sera installé deviendra un contrôleur de domaine.

#### **A. Installation des rôles ADDS et DNS**

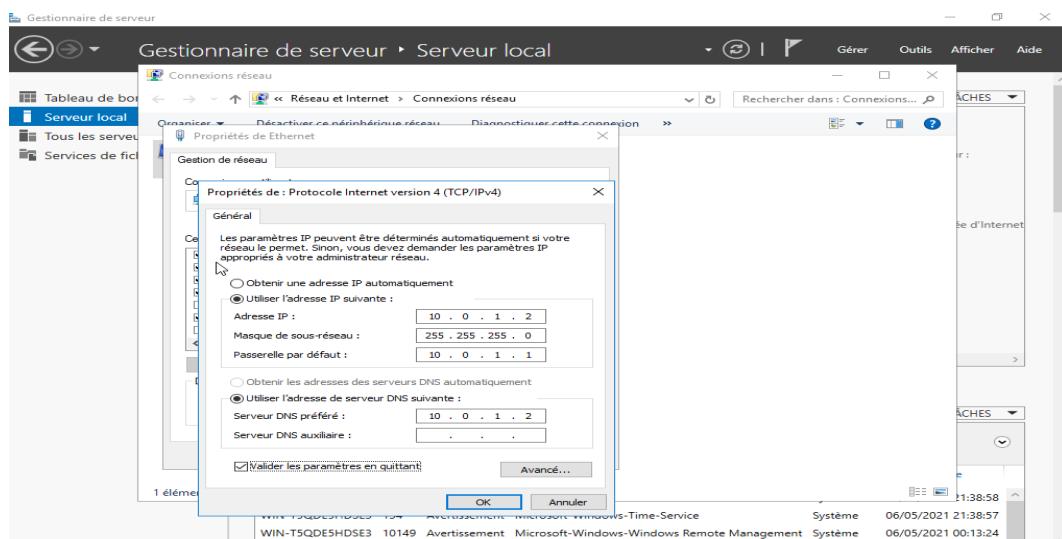
Suite à l'installation de Windows Server 2016 et après redémarrage de la machine, nous arrivons sur l'interface **Tableau de bord du Gestionnaire de serveur** :



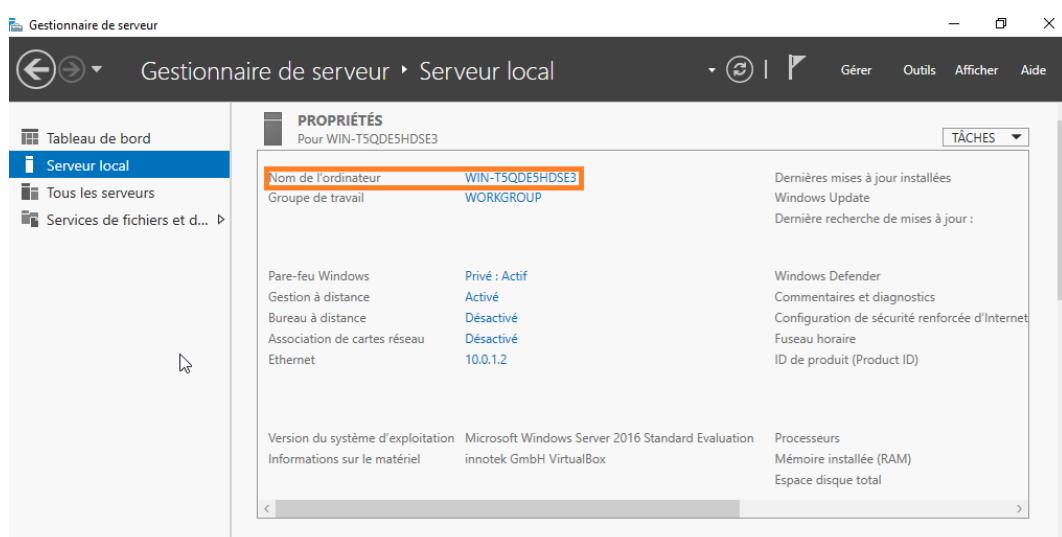
Nous allons ensuite nous rendre sur la partie **Serveur local du Gestionnaire de serveur** afin d'avoir les propriétés de celui-ci, il faut que ce serveur possède une adresse IP fixe et qu'il soit son propre serveur DNS principal. Nous modifions l'adresse en cliquant sur le lien **Ethernet** :

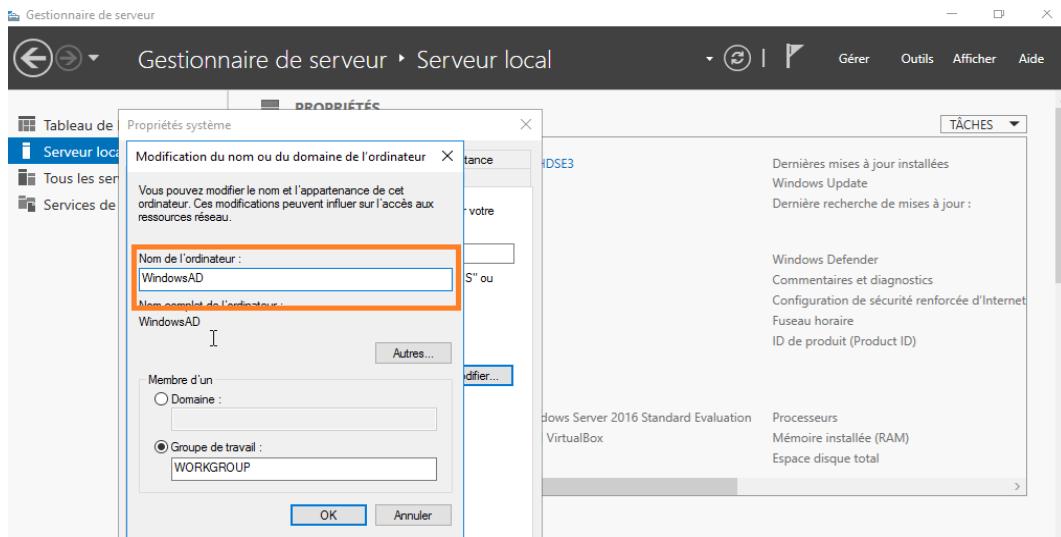


Et l'on modifie l'adresse IP, le masque, la passerelle et les DNS comme suit :

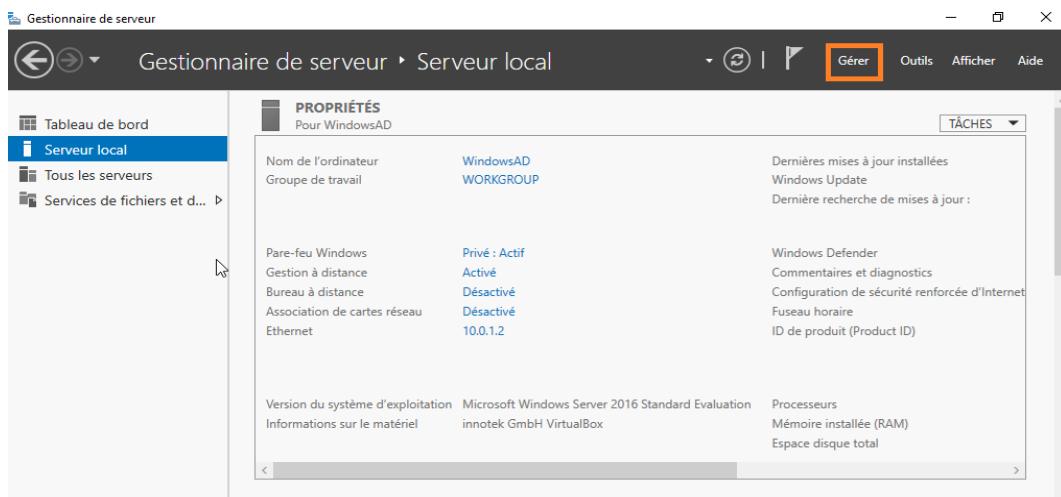


Afin que notre serveur ait un nom reconnaissable, on modifie celui-ci en cliquant sur le lien **Nom de l'ordinateur** comme suit :

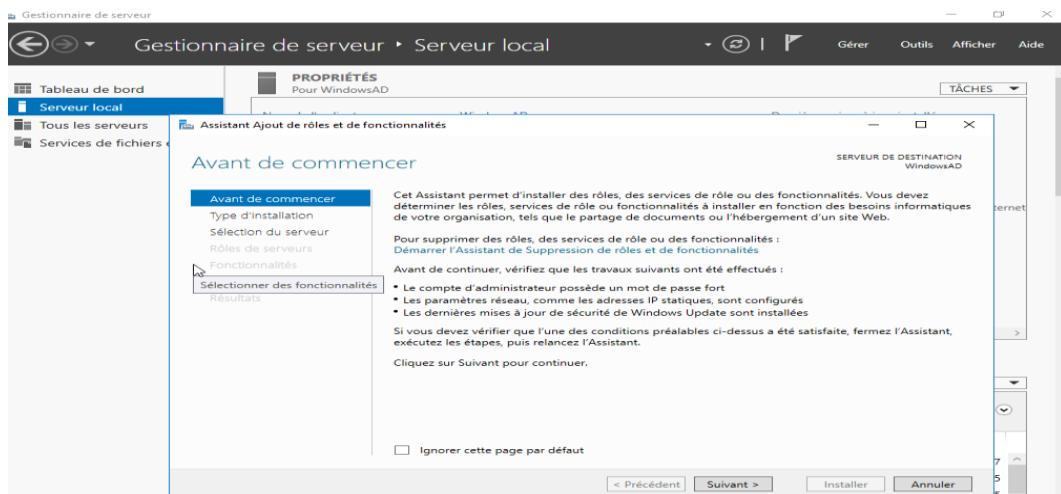




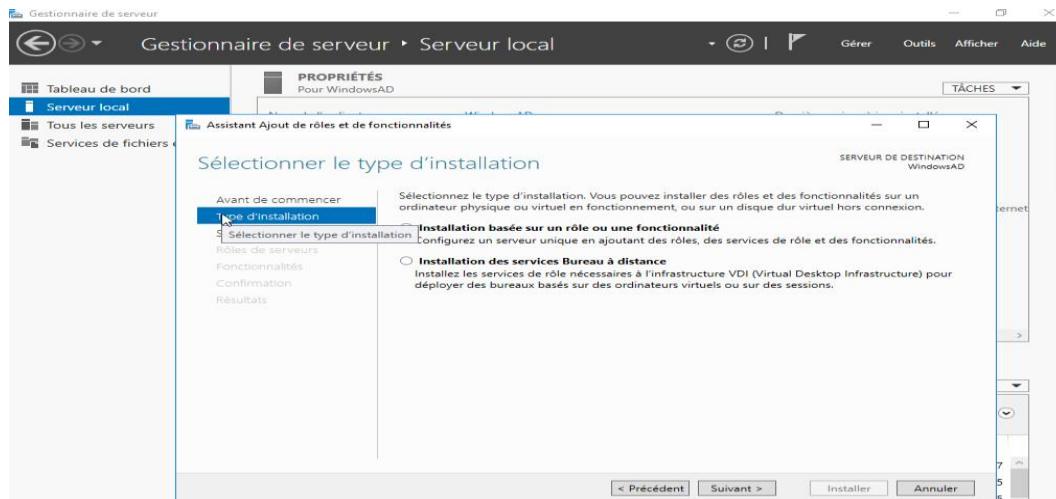
Une fois cela fait, nous allons installer les rôle **ADDS** et **DNS**, pour cela nous allons sur **Gérer puis ajout de rôle et fonctionnalité** :



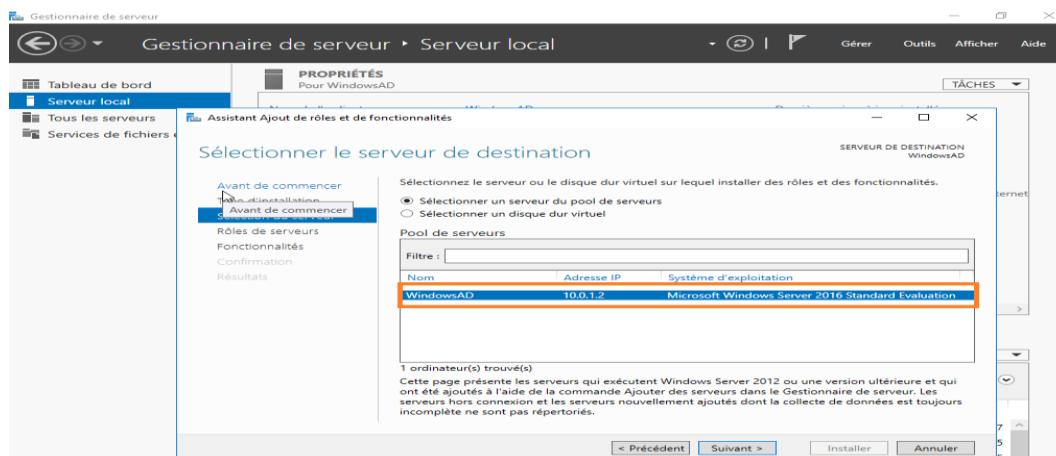
L’assistant d’ajout de rôles et de fonctionnalités va alors s’ouvrir. Cliquez sur **Suivant**.



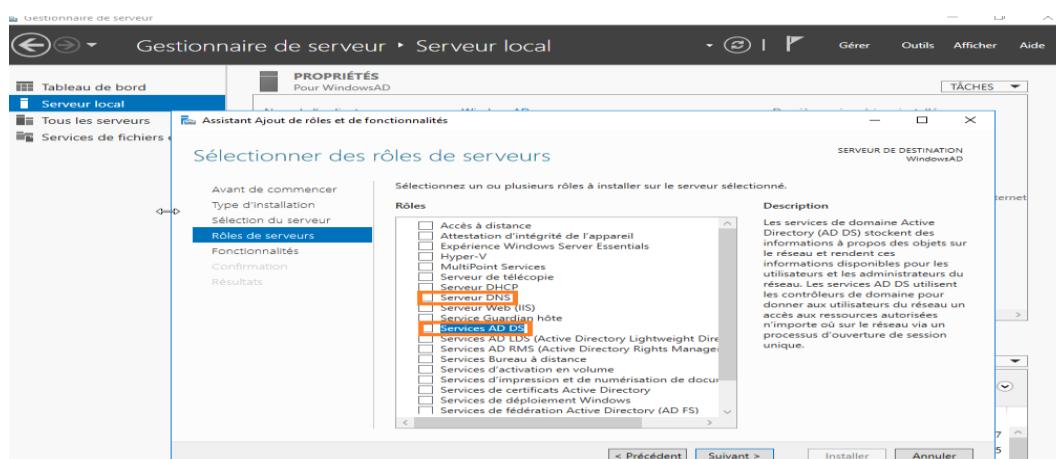
Sélectionnez le type d'**installation basée sur un rôle ou une fonctionnalité** et cliquer sur **Suivant**.



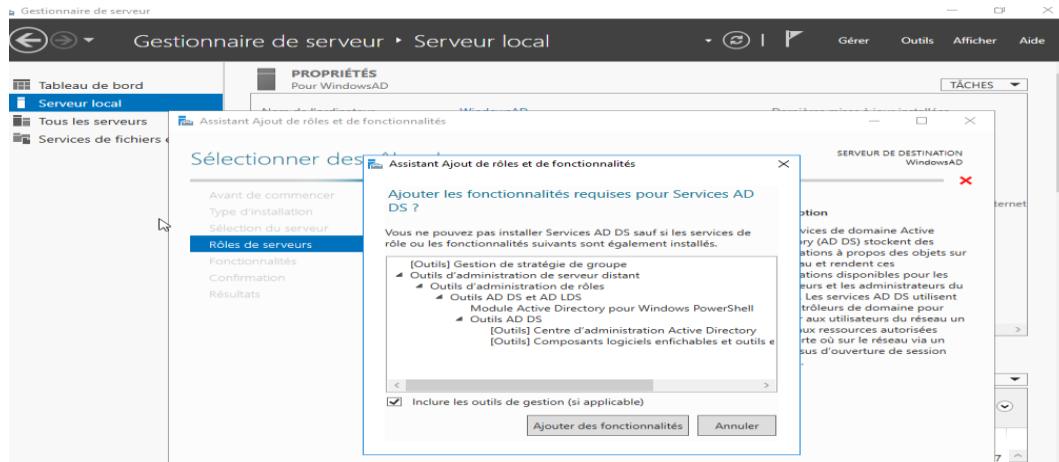
Ensuite, on sélectionne dans le pool, le serveur de destination c'est à dire le serveur sur lequel on souhaite installer le rôle AD.



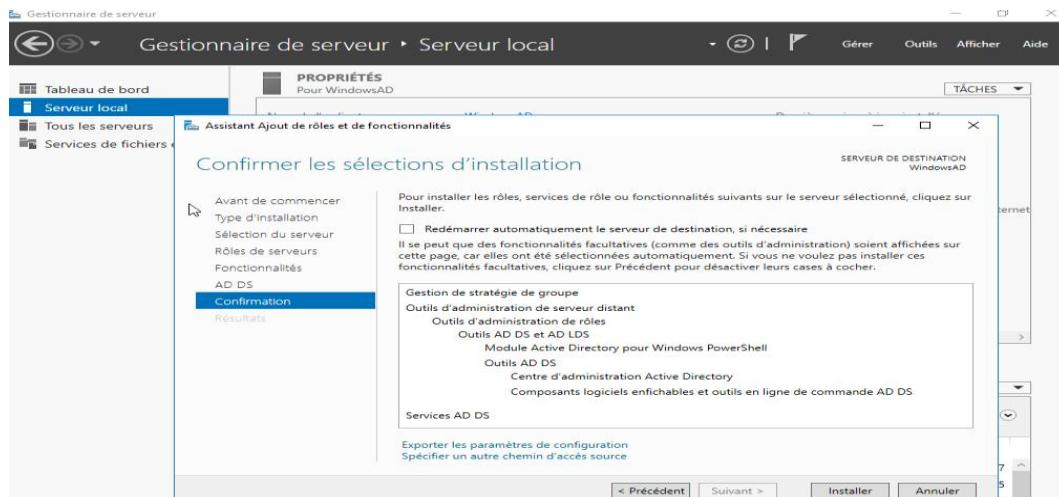
On va maintenant installer les rôles **Active Directory** et **DNS** sur notre serveur. Dans la liste des rôles, on coche les cases correspondant aux Services AD DS et Serveur DNS :

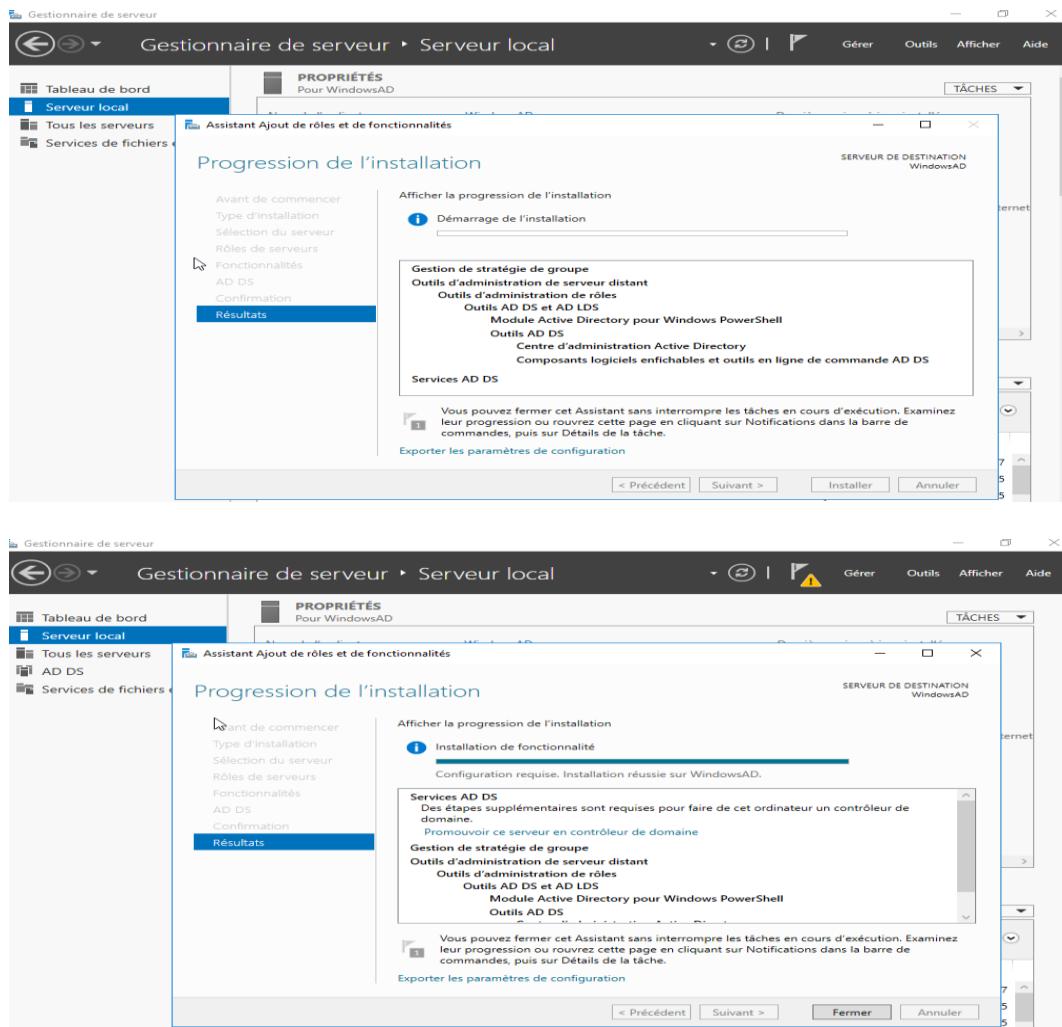


Lorsque l'on coche la case d'un rôle, l'assistant s'ouvre et propose d'installer les fonctionnalités nécessaires au service que vous avez choisi. Sans ces fonctionnalités, le rôle ne pourra pas être déployé. On clique sur **Ajoutez des fonctionnalités**.



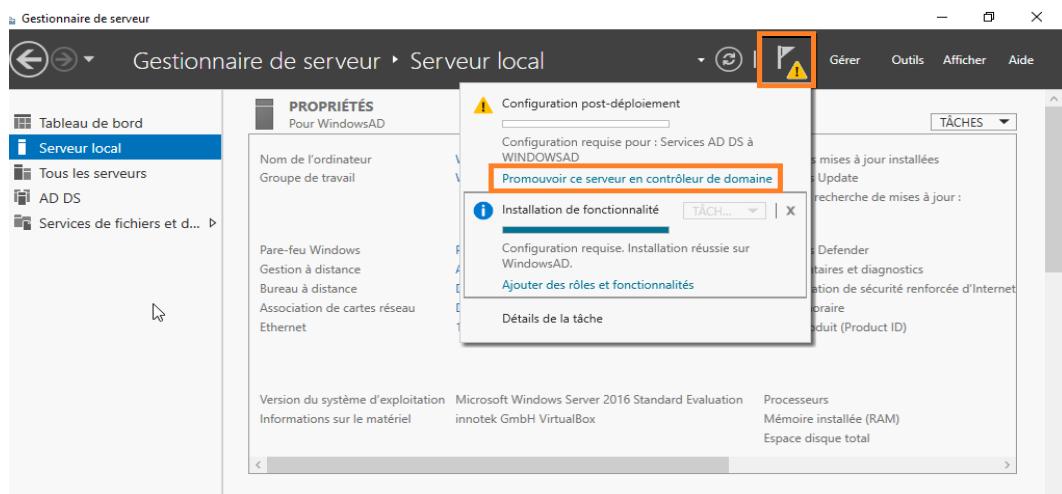
Une fois les deux rôles sélectionnés, on clique sur **Suivant**. Les fonctionnalités dont nous avons besoin ont automatiquement été sélectionnées. On ne modifie rien dans la fenêtre de sélection des fonctionnalités, et on clique sur **Suivant**. L'assistant affichera les informations des services AD DS. On clique sur **Suivant**. De même pour le service DNS. L'installation des rôles débute :





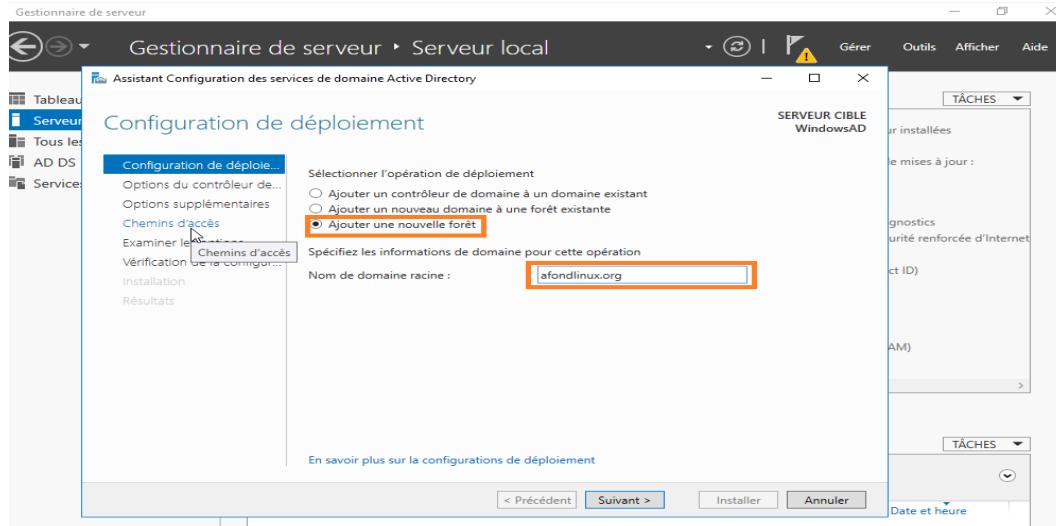
## B. Promulgation du serveur en contrôleur de domaine

Une fois le service AD installé, on déclare le serveur comme contrôleur de domaine. On clique sur **Promouvoir ce serveur en contrôleur de domaine**.



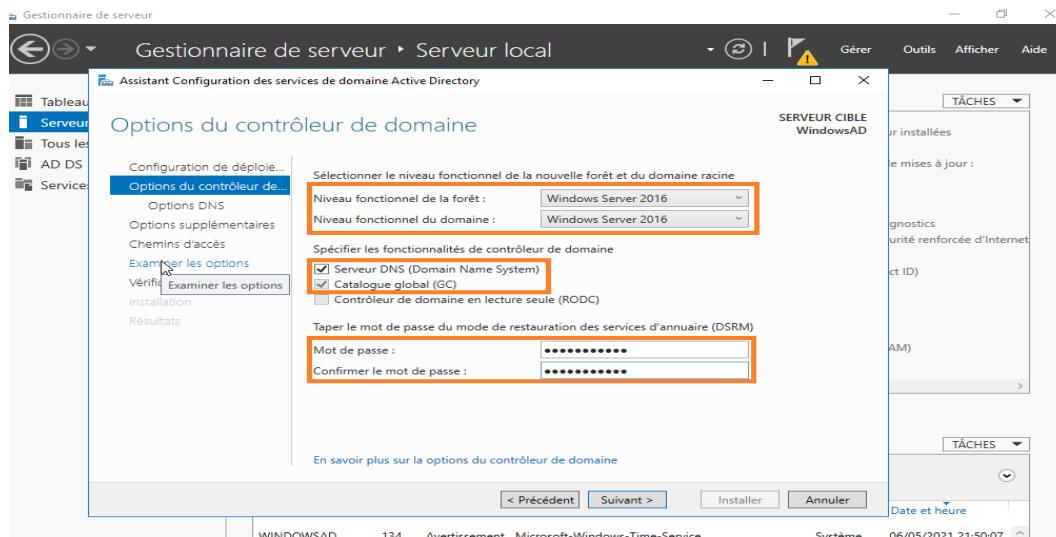
Nous allons maintenant configurer les services **Active Directory**. Je crée un nouveau domaine dans une nouvelle forêt. Ce domaine sera le domaine racine de l'entreprise.

On coche **Ajouter une nouvelle forêt** et enregistre le nom complet de notre domaine ici, **afondlinux.org**.



On choisit ensuite les options du contrôleur de domaine, le niveau fonctionnel de la forêt et du domaine sur la version par défaut. Comme c'est le 1<sup>er</sup> contrôleur de domaine de la nouvelle forêt, il est obligatoirement **serveur DNS** et **Catalogue Global**.

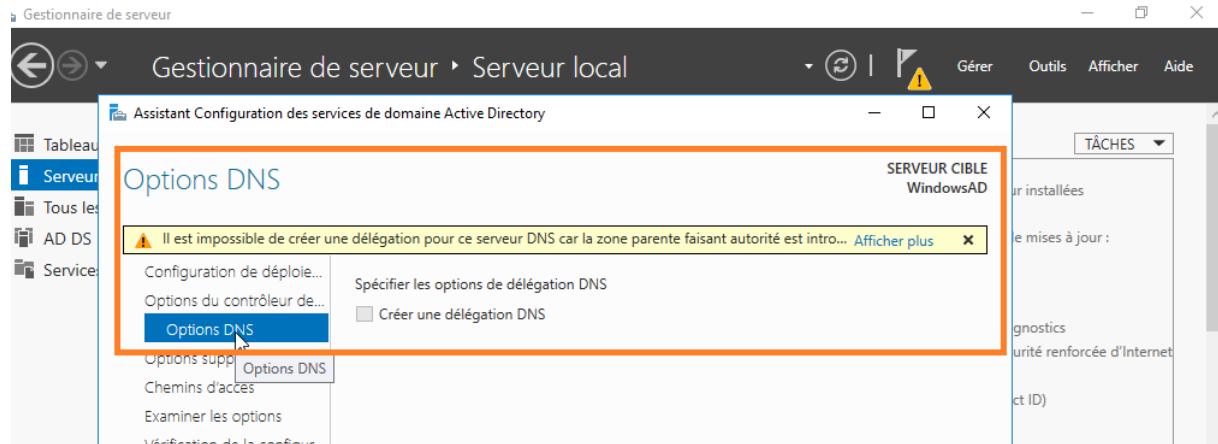
On enregistre un mot de passe afin de restaurer les services d'annuaire en cas de problème et on clique sur **Suivant**.



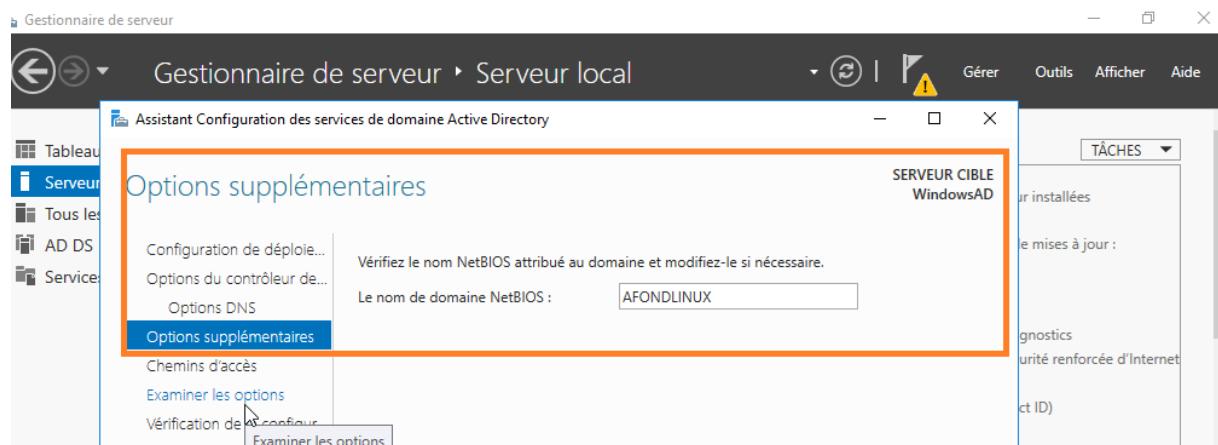
Le niveau fonctionnel est ce qui permet de délimiter les fonctionnalités de l'AD au sein d'un domaine ou d'une forêt et de s'assurer de la compatibilité des versions des contrôleurs de domaine. Le catalogue global est l'index de toute la forêt.

L'assistant nous indique une erreur du service DNS, il ne faut pas en tenir compte, ni cocher la case de délégation, puis cliquer sur **Suivant**.

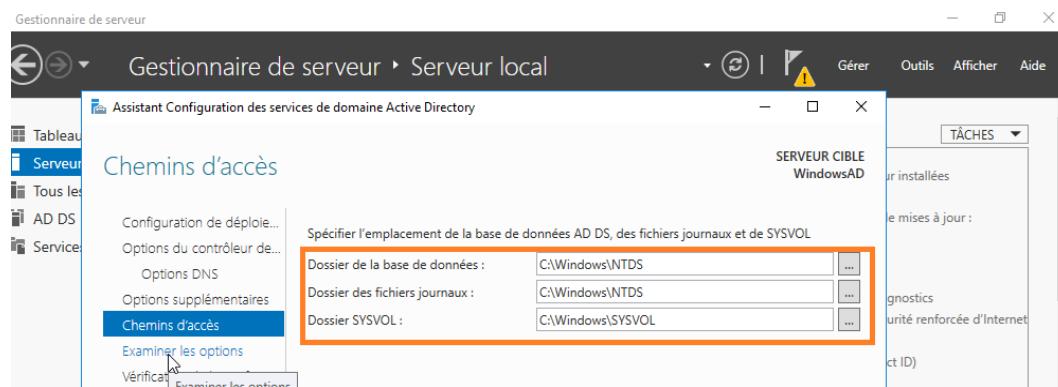
La zone faisant autorité est en fait le serveur DNS gestionnaire de la zone. Elle sera créée sur le serveur DNS à la fin de la configuration des services AD.



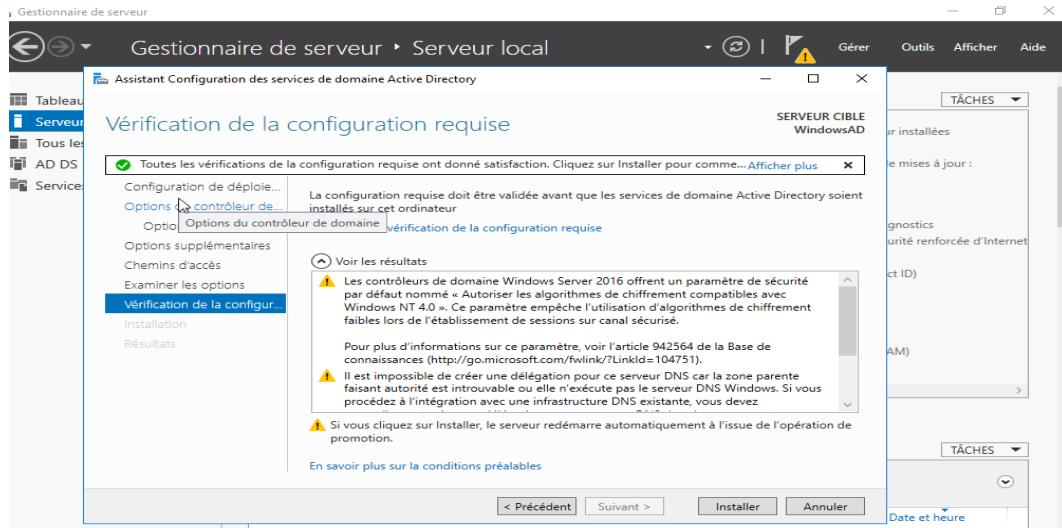
On définit ensuite le nom NetBIOS du domaine. On laisse le nom attribué par défaut.



On définit les répertoires suivants : l'emplacement de stockage de la base de données de **l'Active Directory**, les fichiers de logs et le dossier **SYSVOL**. Le dossier **SYSVOL** est un répertoire partagé qui sera répliqué sur **WindowsRODC** par la suite. Il contient les stratégies de groupes appliquées sur le domaine et les différents scripts pouvant être utilisés. Les scripts sont accessibles dans un partage appelé **NETLOGON**.



Une vérification de la configuration est faite avant de pouvoir débuter l'installation. Une fois les vérifications validées, cliquez sur **Installer**. Suite à cela, le serveur devient contrôleur de domaine, et la machine redémarre automatiquement pour effectuer les dernières configurations. Après le redémarrage, l'écran de connexion avec le nom NetBIOS du domaine et le compte Administrateur apparaît.

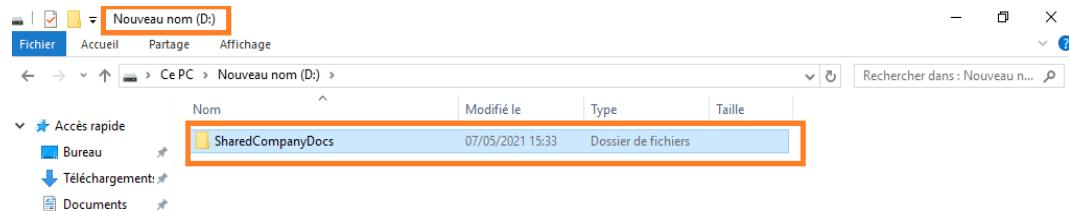


Le compte administrateur local de la machine est devenu le compte administrateur du domaine. Pour ouvrir une session sur le domaine, on saisit soit **AFOND LINUX\Administrateur** soit **Administrateur@afondlinux.org**

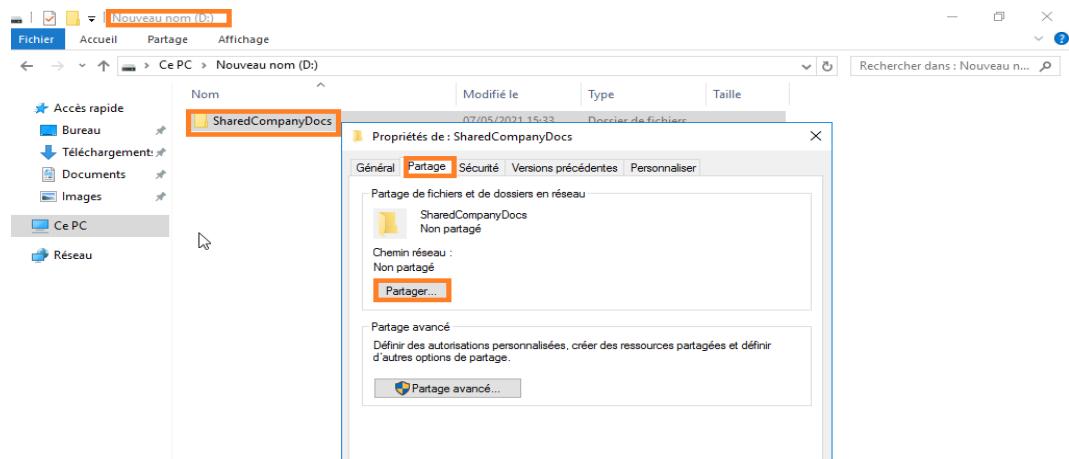
Notre contrôleur de domaine est maintenant installé, nous allons pouvoir passer à l'installation du serveur **WindowsRODC** du site distant.

## C. Création du répertoire partagé SharedCompanyDocs

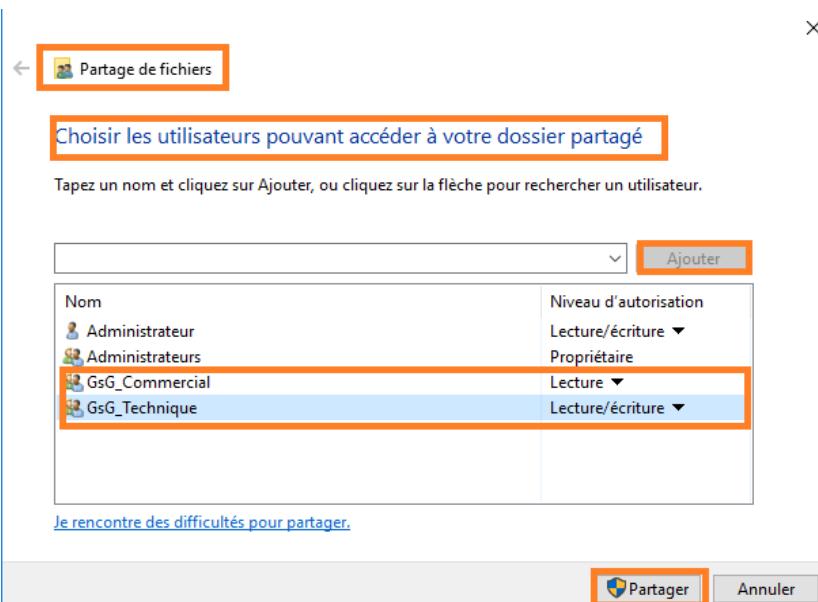
Afin que tous les employés de l'entreprise puissent avoir un dossier partagé, nous allons créer ce dossier dans une seconde partition sur le serveur WindowsAD. Sur la partition D:, nous allons créer un dossier nommé **SharedCompanyDocs**.



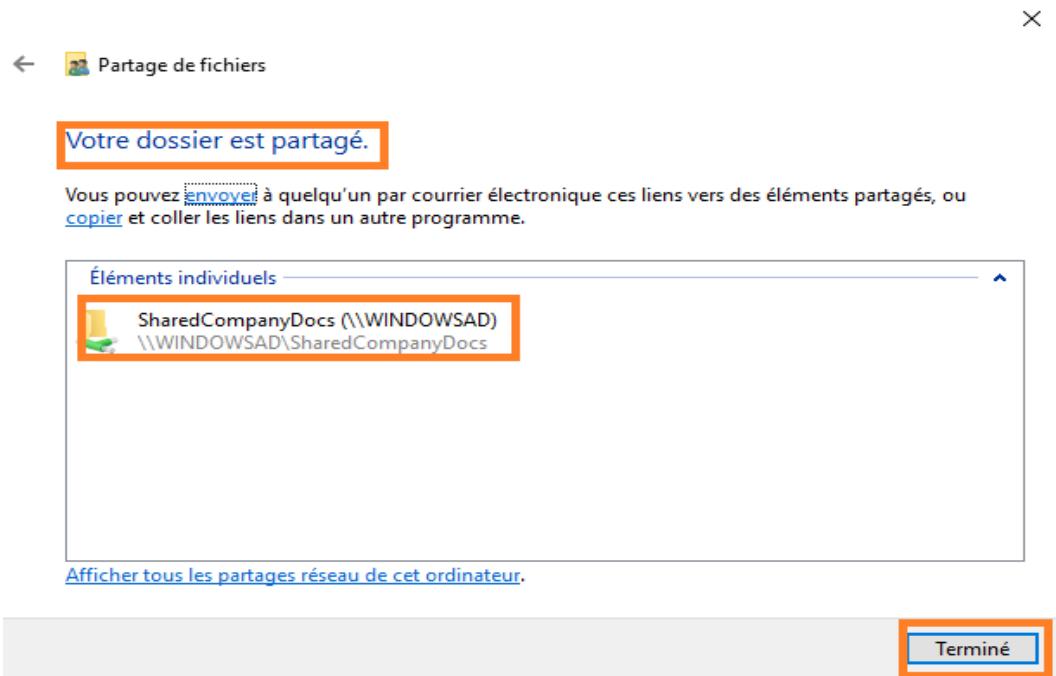
On clique droit sur le dossier pour accéder aux propriétés de celui-ci et l'on se rend sur l'onglet **Partage**.



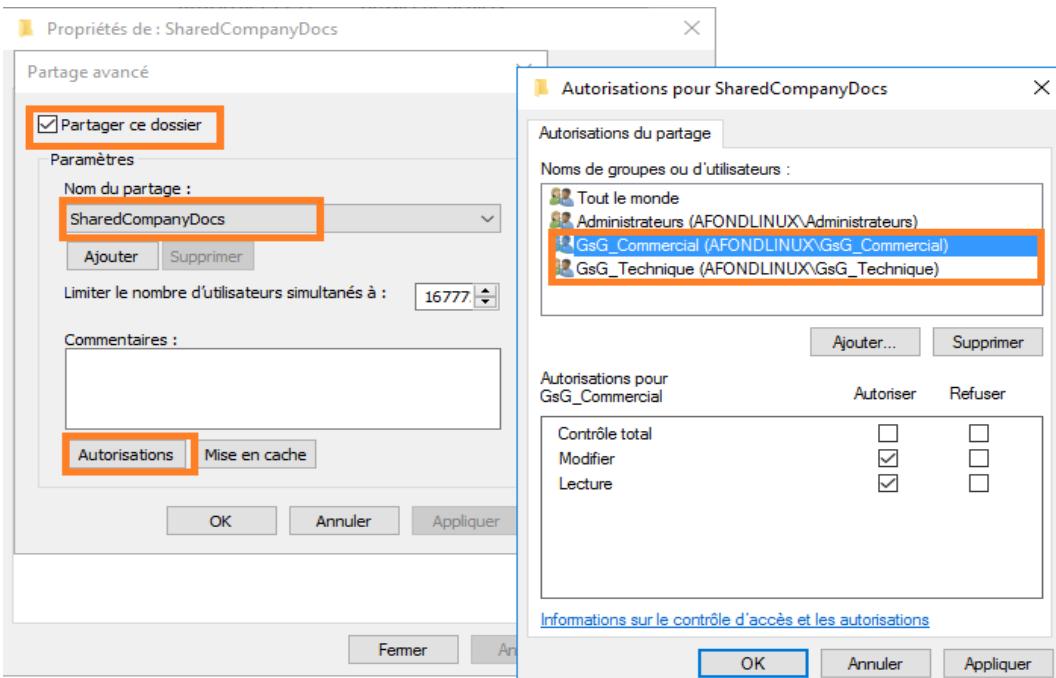
Nous allons maintenant choisir avec quels utilisateurs ou groupe d'utilisateur sera partagé ce dossier et quels seront leur droit en cliquant sur le bouton **Partager**.



On obtient alors les informations suivantes dans la nouvelle fenêtre qui s'ouvre : le dossier est bien partagé et l'adresse réseau du partage. On peut fermer cette fenêtre et retourner sur la fenêtre précédente des propriétés du dossier.



Nous allons cliquer sur le bouton **Partage avancé**, et dans la nouvelle fenêtre, on coche la case **Partager ce dossier**, on donne un nom au partage et l'on peut vérifier et/ou modifier les autorisations sur le dossier **SharedCompanyDocs**.



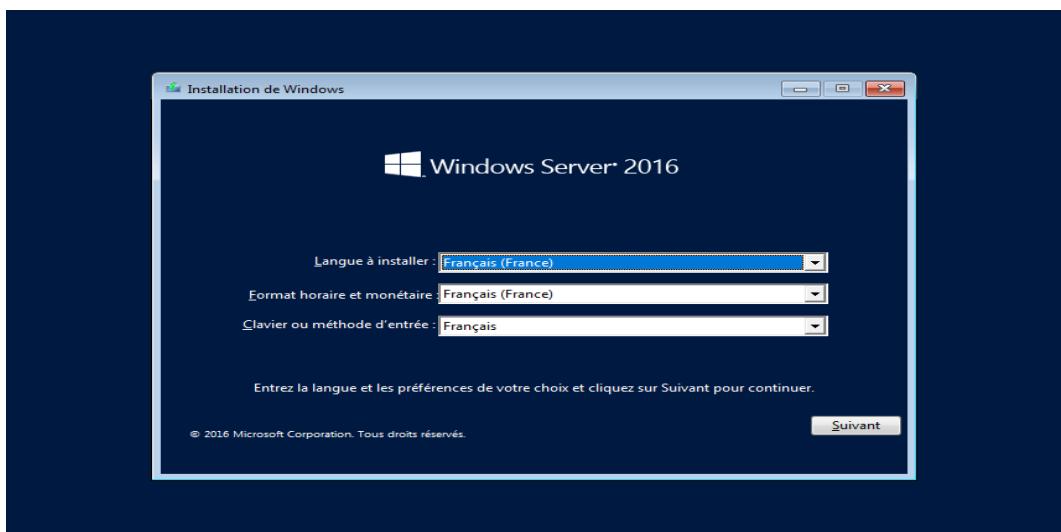
## **IV. Installation et configuration du serveur WindowsRODC**

Le but de l'installation du serveur **WindowsRODC** est que les 3 employés du site distant puissent accéder aux ressources fournies par le site local. Une liaison VPN existe déjà entre les 2 sites. En cas de coupure de la liaison entre les deux sites, les utilisateurs du site distant pourront s'authentifier sur le domaine de l'entreprise Afondlinux.

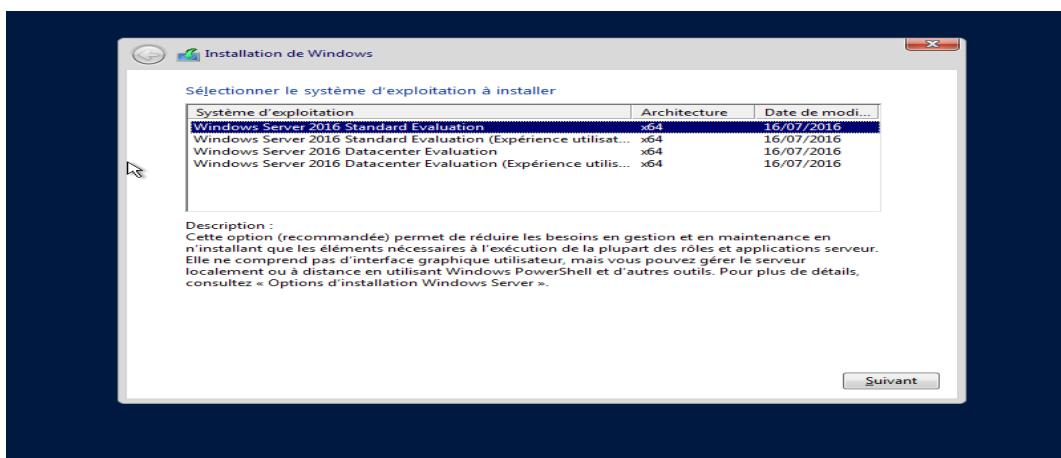
Un serveur jouant le rôle de contrôleur de domaine pour le domaine **afondlinux.org** doit donc être installé sur le site distant. La particularité de ce contrôleur de domaine est qu'il y sera impossible d'administrer **Active Directory** car il sera en lecture seule. C'est ce qu'on appelle un **RODC : Read Only Domain Controller**.

Il ne servira qu'à authentifier les postes et les utilisateurs et appliquera également les stratégies de groupe.

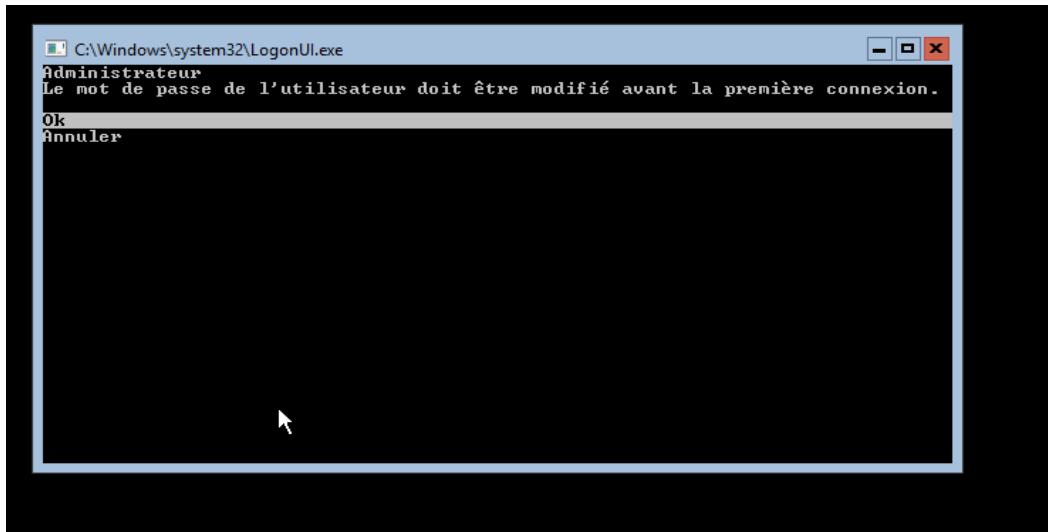
Passons maintenant à l'installation et la configuration du serveur **WindowsRODC**. Nous commençons par installer le système d'exploitation Windows Server 2016.



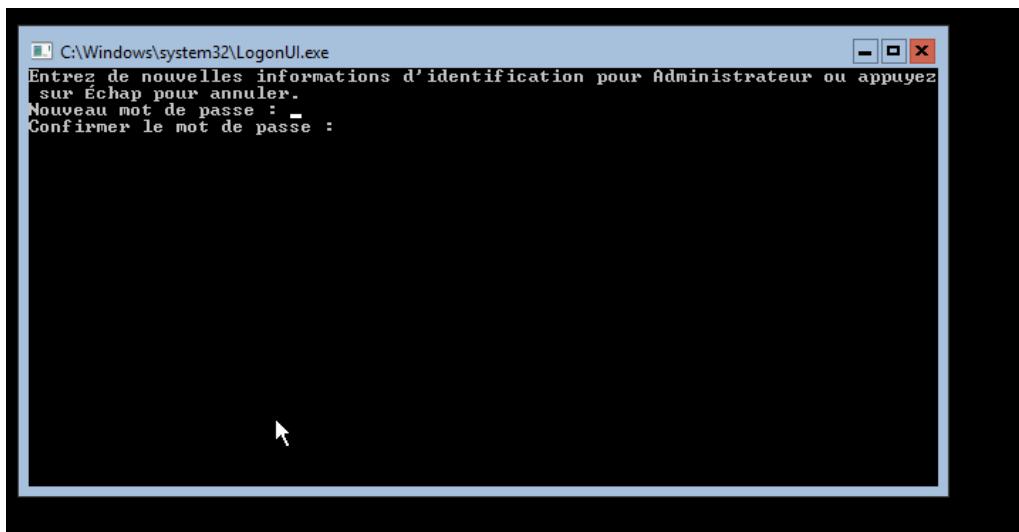
Nous allons choisir la version Standard sans expérience utilisateur, c'est à dire sans mode graphique pour optimiser les ressources.



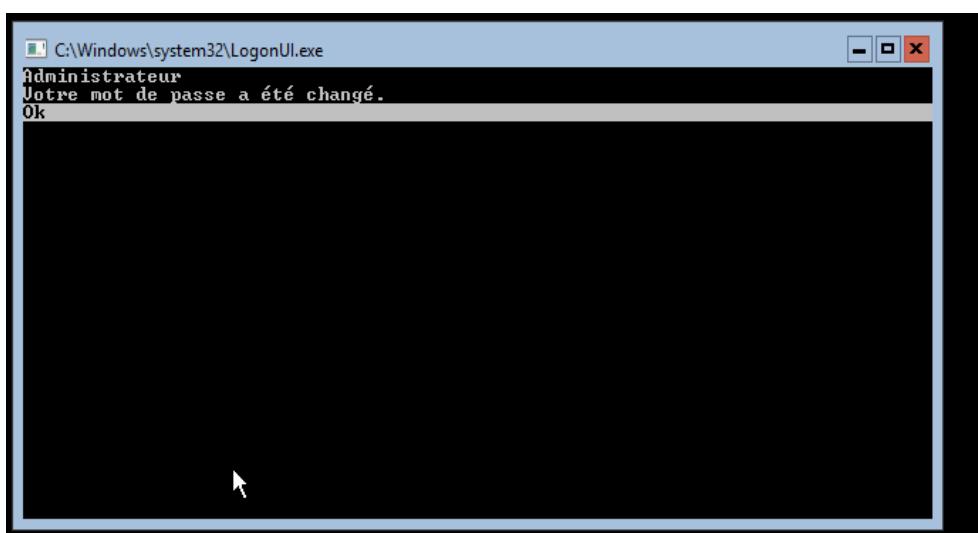
A la fin de l'installation, il faut modifier le mot de passe avant la première connexion.



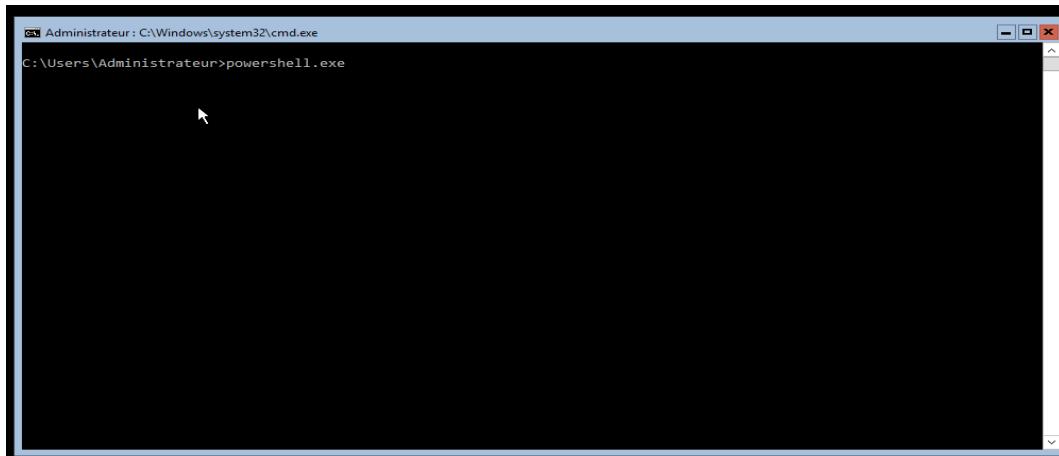
On tape notre nouveau mot de passe et le confirmons une seconde fois.



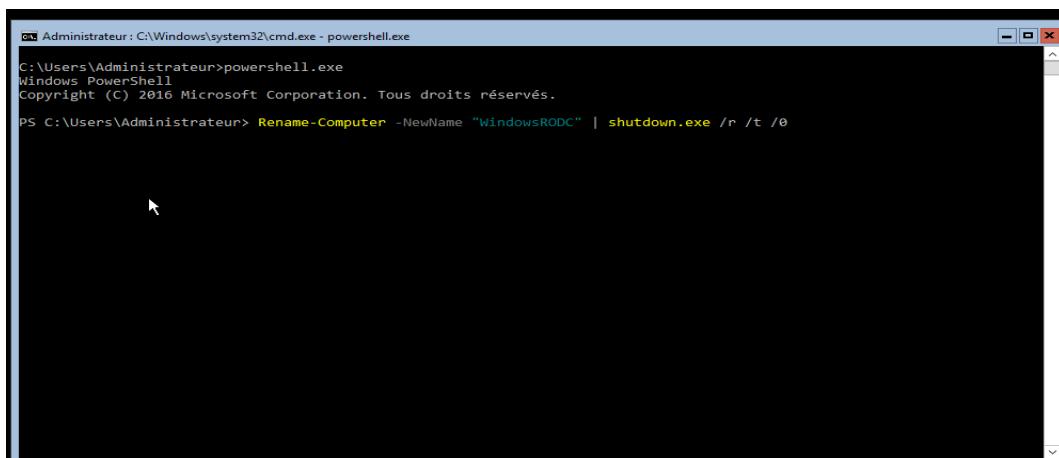
Confirmation du changement de mot passe.



On ouvre par la suite une console **PowerShell** avec la commande powershell.exe



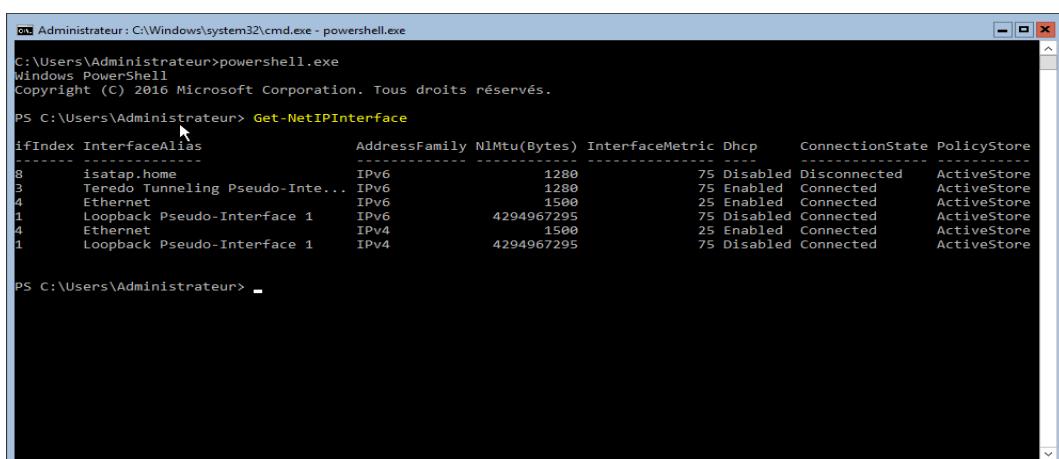
Nous allons renommer notre serveur avec la commande **Rename-Computer**



Le serveur va redémarrer, on se relogue de nouveau en administrateur et on ouvre une console **PowerShell**.

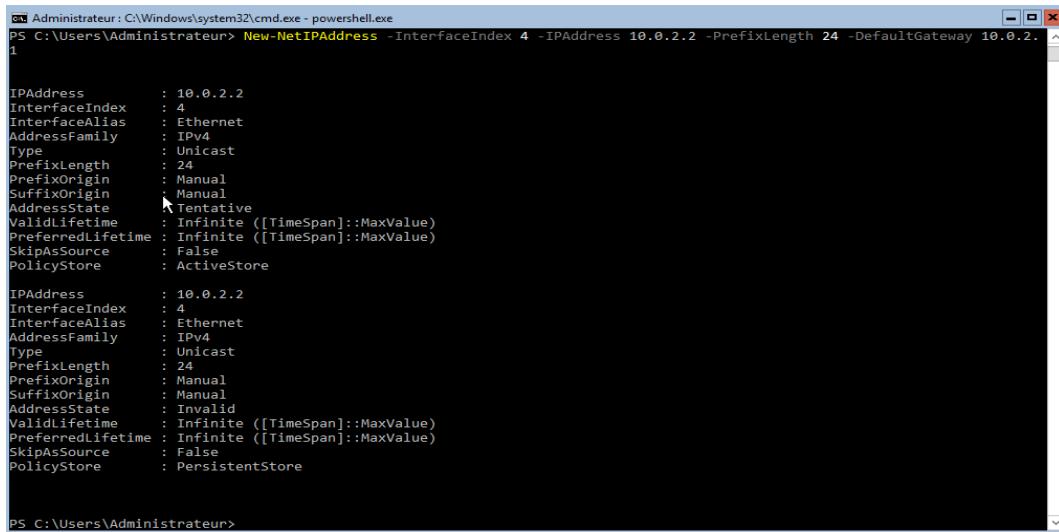
On va maintenant attribuer une adresse IP à notre serveur **WindowsRODC**.

Avec la commande **Get-NetIPInterface** on récupère le numéro de l'interface réseau à configurer.



Ici l'interface qui nous intéresse est la n°4 dans la colonne **ifIndex**, Ethernet0.

On va définir une adresse IP dans le réseau du site distant, un masque et une adresse de passerelle avec la commande **New-NetIPAddress** :



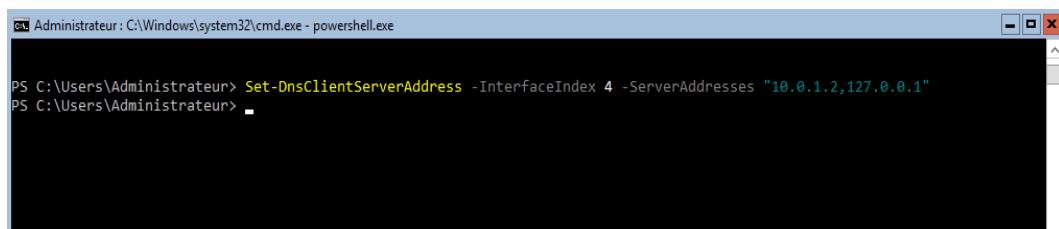
```
Administrator : C:\Windows\system32\cmd.exe - powershell.exe
PS C:\Users\Administrateur> New-NetIPAddress -InterfaceIndex 4 -IPAddress 10.0.2.2 -PrefixLength 24 -DefaultGateway 10.0.2.1
1

IPAddress      : 10.0.2.2
InterfaceIndex : 4
InterfaceAlias : Ethernet
AddressFamily   : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState   : Tentative
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore

IPAddress      : 10.0.2.2
InterfaceIndex : 4
InterfaceAlias : Ethernet
AddressFamily   : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState   : Invalid
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : PersistentStore

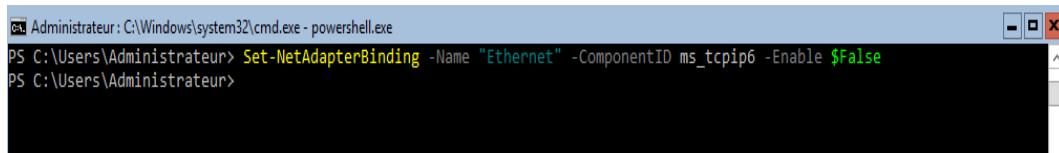
PS C:\Users\Administrateur>
```

L'adresse IP de la passerelle par défaut devra être celle de votre de l'interface Lan de **Pfsense**. Ensuite, on va configurer l'adresse des serveurs DNS. Nous allons lui donner pour adresses de DNS, l'adresse IP du serveur **WindowsAD** situé sur le site local mais également sa propre adresse IP :



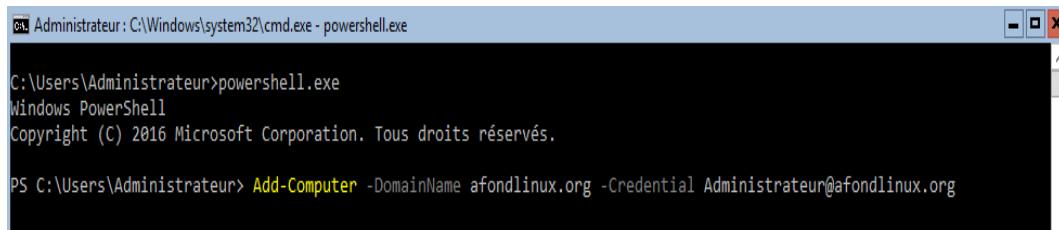
```
Administrator : C:\Windows\system32\cmd.exe - powershell.exe
PS C:\Users\Administrateur> Set-DnsClientServerAddress -InterfaceIndex 4 -ServerAddresses "10.0.1.2,127.0.0.1"
PS C:\Users\Administrateur>
```

Pour des raisons pratiques on désactive l'ipv6 :



```
Administrator : C:\Windows\system32\cmd.exe - powershell.exe
PS C:\Users\Administrateur> Set-NetAdapterBinding -Name "Ethernet" -ComponentID ms_tcpip6 -Enable $False
PS C:\Users\Administrateur>
```

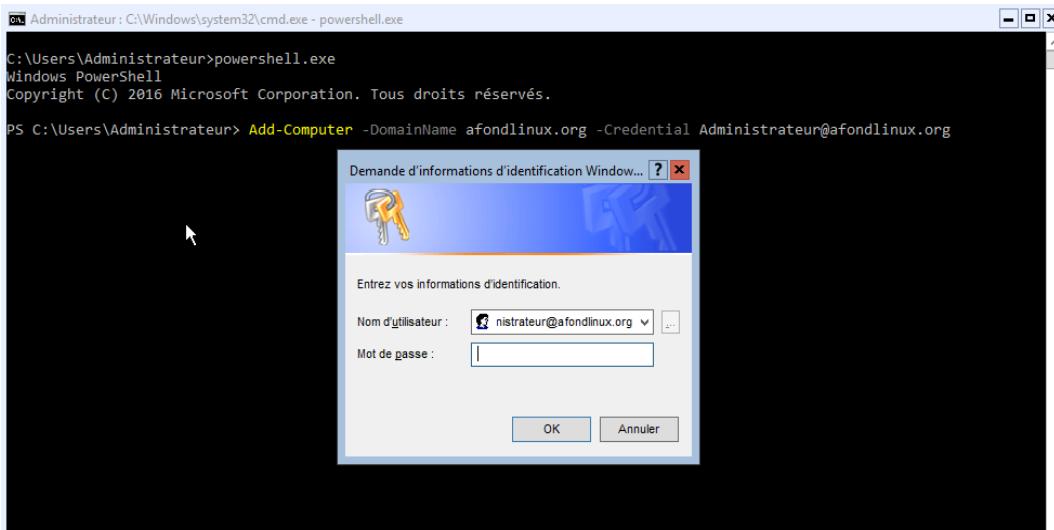
Pour terminer, on va ajouter le serveur **WindowsRODC** au domaine **afondlinux.org** de l'entreprise avec la commande suivante :



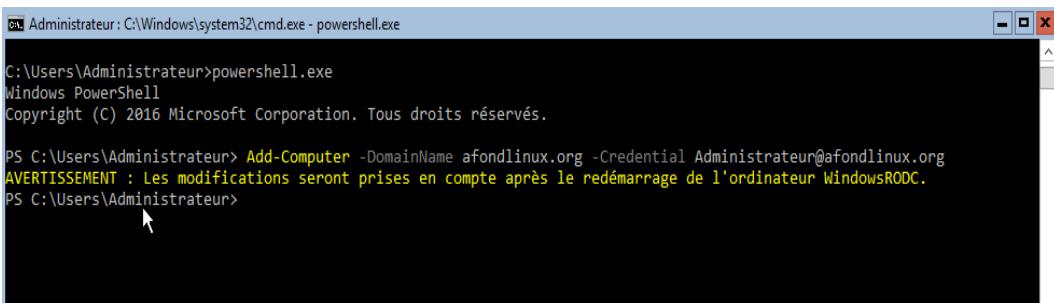
```
C:\Administrator: C:\Windows\system32\cmd.exe - powershell.exe
C:\Users\Administrateur>powershell.exe
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Add-Computer -DomainName afondlinux.org -Credential Administrateur@afondlinux.org
```

À la fenêtre d'authentification, saisir le mot de passe du compte Administrateur du domaine.



Redémarrer une fois encore le serveur avec la commande **shutdown.exe /r** pour appliquer la modification.

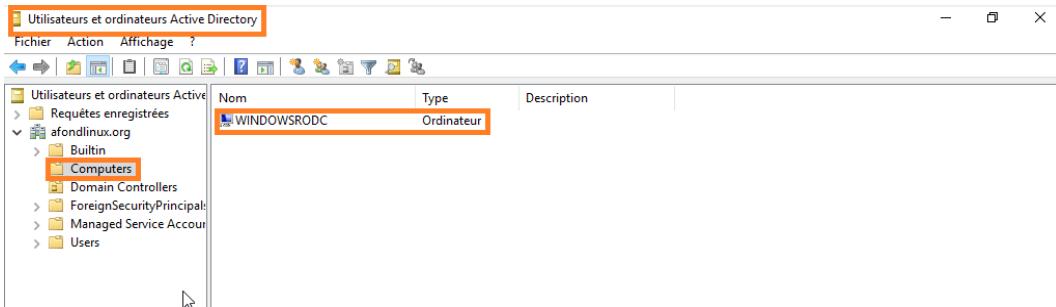


À partir de maintenant, nous n'utiliserons plus le serveur **WindowsRODC** directement.

## V. Gestion et promulgation en contrôleur de domaine du serveur WindowsRODC

### A. Gestion du serveur WindowsRODC

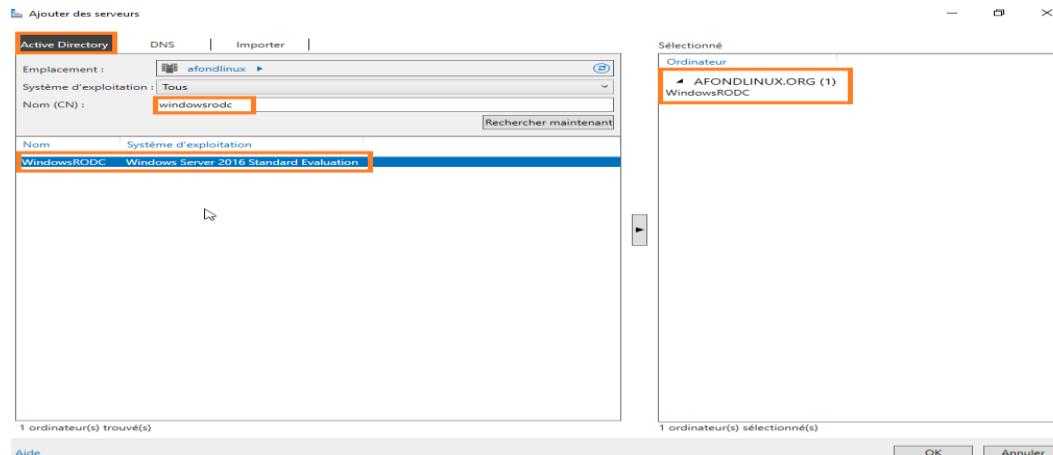
Nous allons contrôler le serveur **WindowsRODC** depuis le serveur **WindowsAD**. On va vérifier que le nouveau serveur est bien membre du domaine. On se rend sur la console **Utilisateurs et ordinateurs Active Directory** et on vérifie que le serveur **WindowsRODC** se trouve dans l'unité d'organisation **Computers**.



On va maintenant promouvoir notre serveur **WindowsRODC** en contrôleur de domaine. On se rend sur le tableau de bord du **Gestionnaire de serveur**.

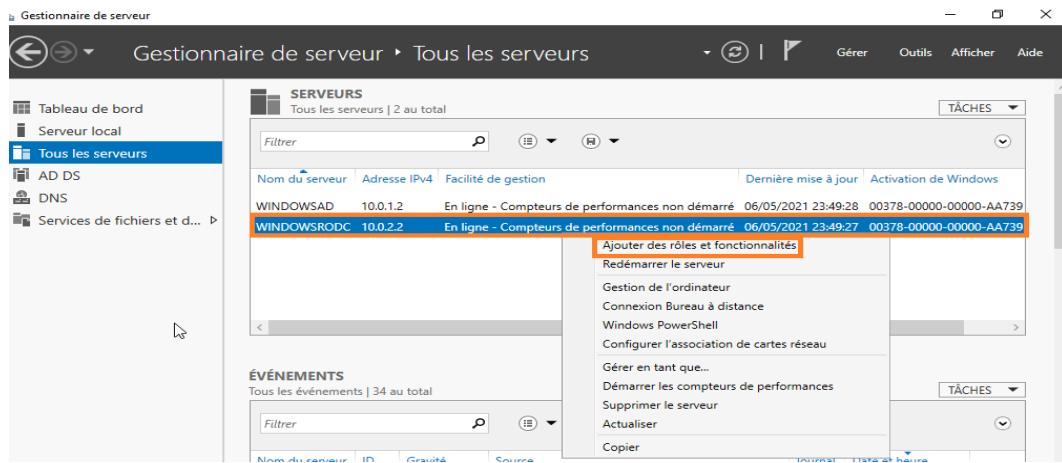


Dans l'onglet **Active Directory**, on recherche le serveur **WindowsRODC** et on clique sur la flèche pour qu'il apparaisse sur la droite. Une fois le serveur sélectionné, cliquez sur **OK**.

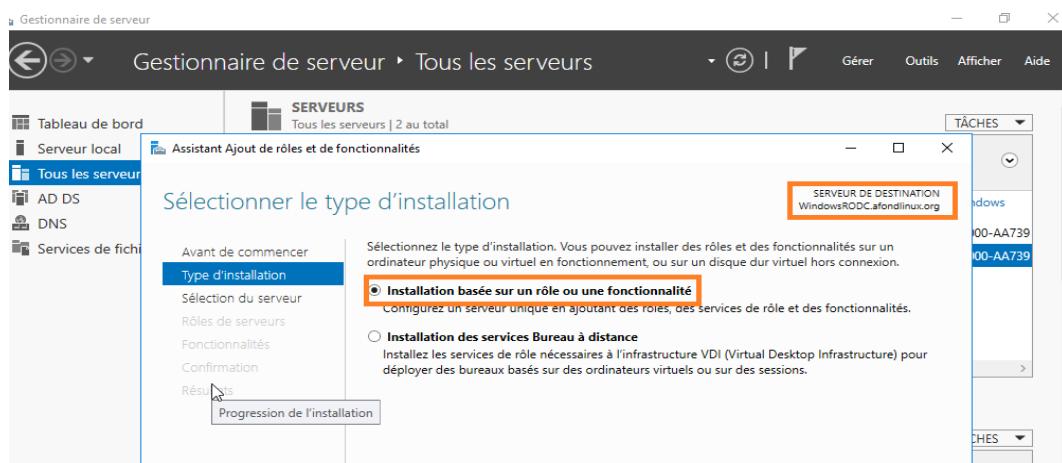


## B. Promulgation en tant que contrôleur de domaine

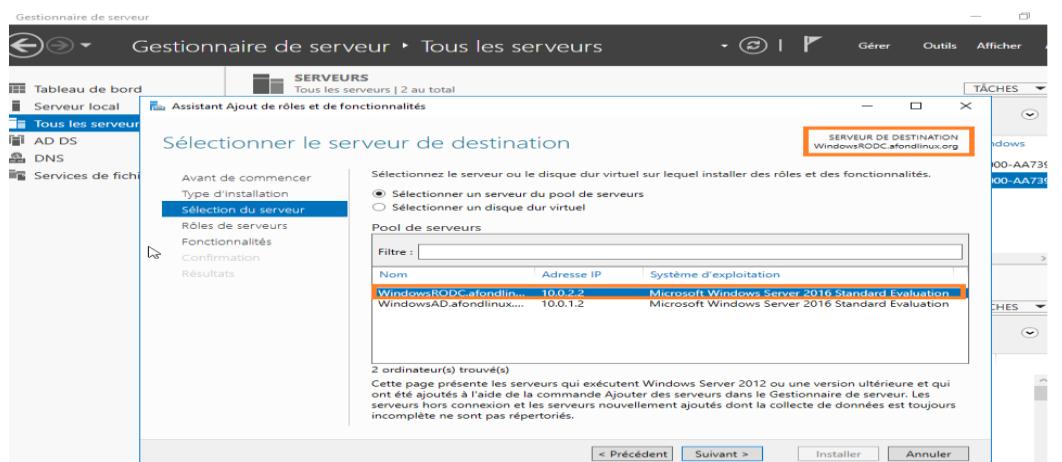
Sur la gauche de la console, on clique sur **Tous les serveurs**. Le serveur **WindowsRODC** peut être configuré depuis ce point. On clique droit sur le serveur **WindowsRODC** et on clique sur **Ajouter des rôles et fonctionnalités**.



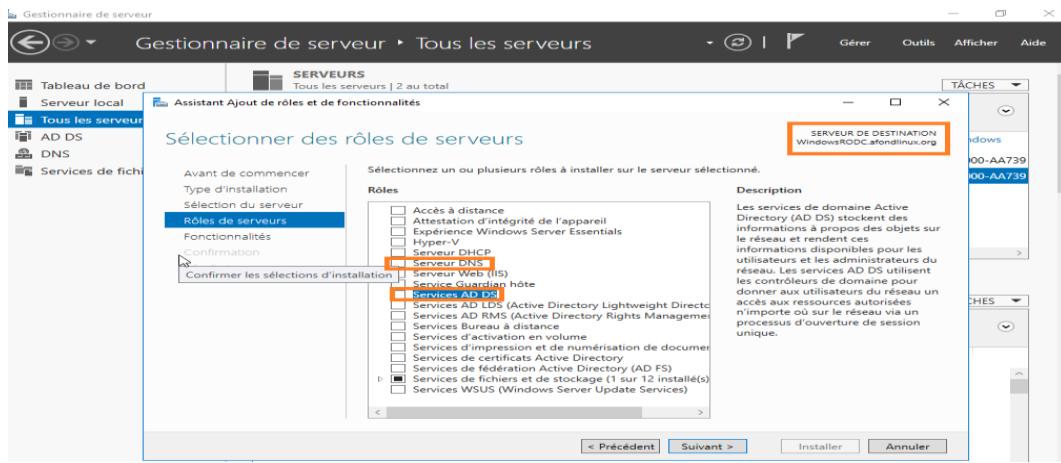
On choisit **Installation basée sur un rôle ou une fonctionnalité** et l'on vérifie que le serveur de destination est bien **WindowsRODC**.



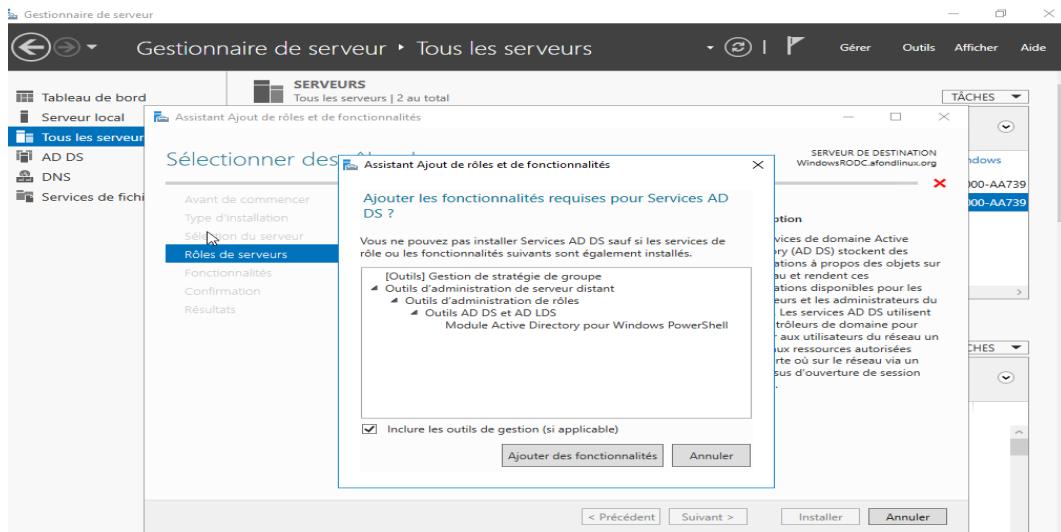
On choisit le serveur **WindowsRODC** dans le pool des serveurs et on clique sur **Suivant**.



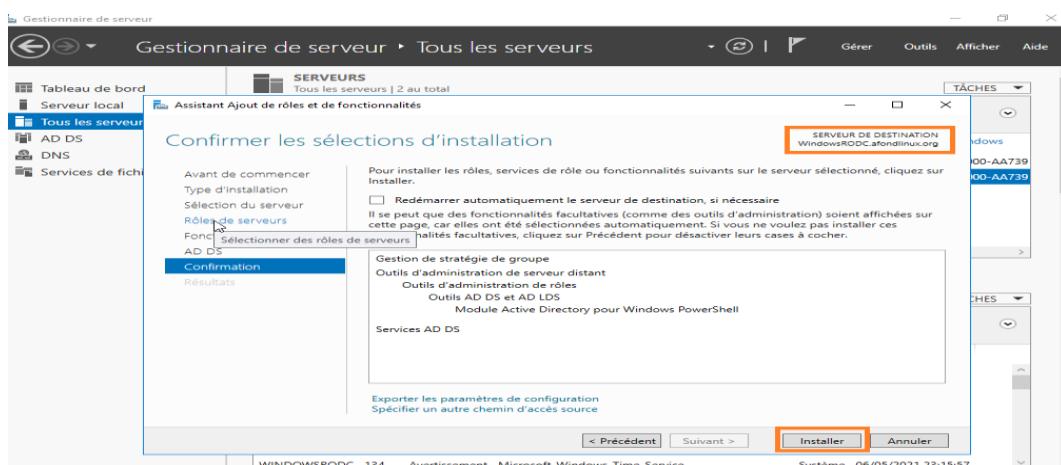
Dans la page de sélection des rôles, on coche les rôles **Services AD DS** et **Serveur DNS**.



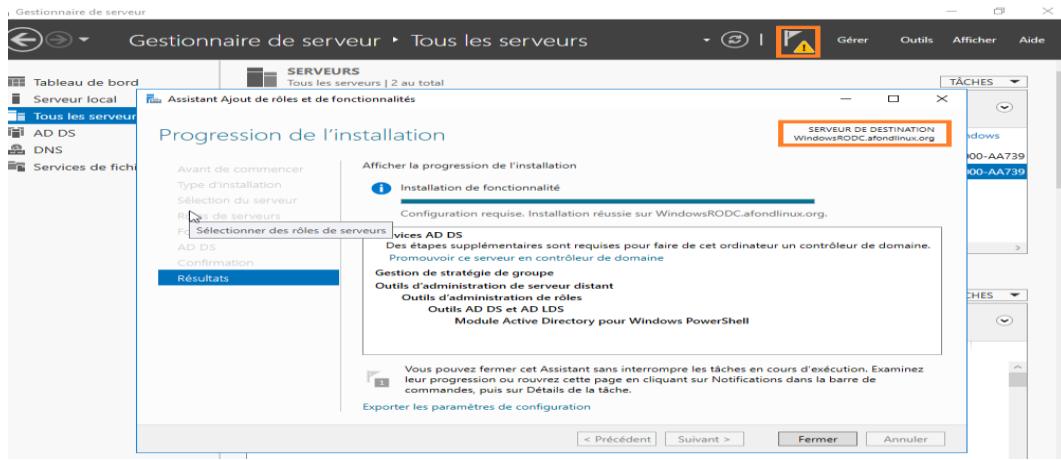
Pour chacun des rôles cochés, on clique sur **Ajouter des fonctionnalités** et on ne modifie rien dans la partie suivante des fonctionnalités vues qu'elles ont déjà été sélectionnées automatiquement.



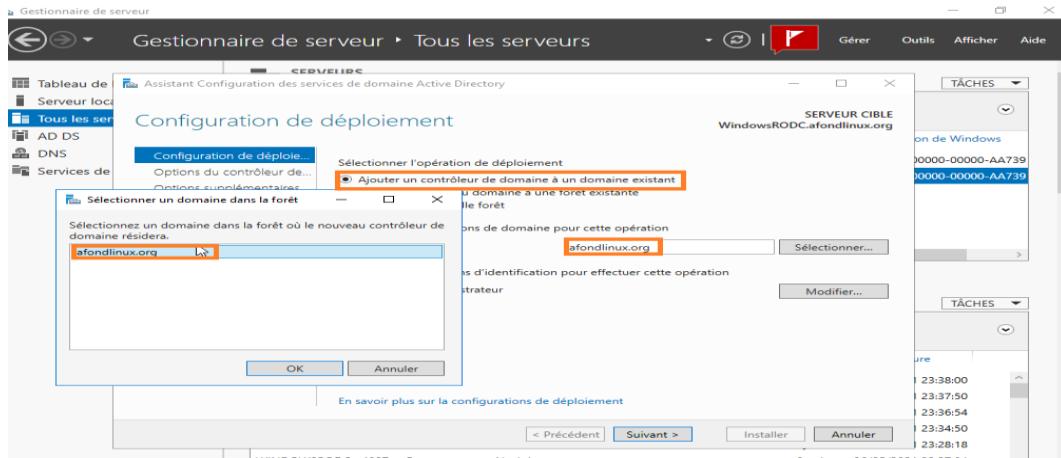
On vérifie les paramètres d'installation et on clique sur **Installer**.



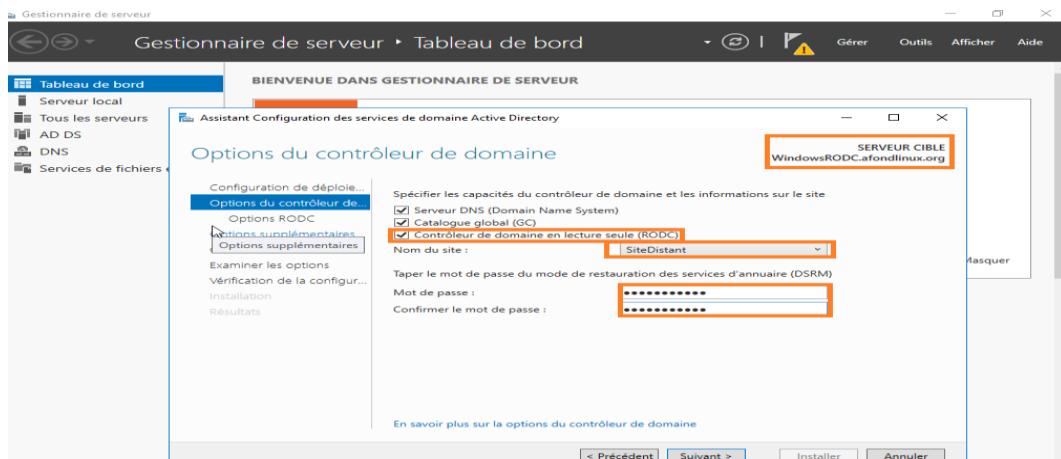
On clique sur **Promouvoir ce serveur en contrôleur de domaine**.



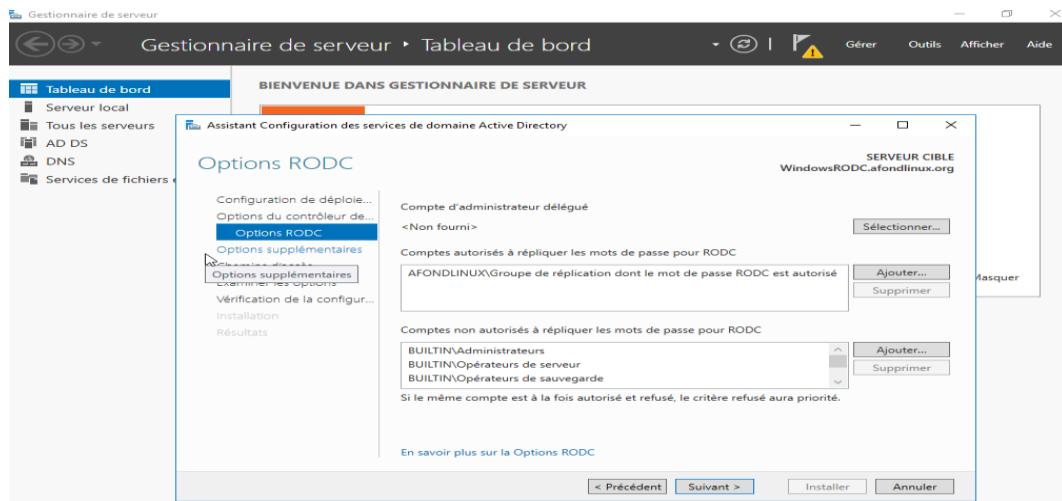
La forêt ainsi que le domaine existent déjà on coche **Ajouter un contrôleur de domaine à un domaine existant**. On renseigne le nom du domaine afondlinux.org et on clique sur **Modifier** pour fournir les informations d'identification du compte **Administrateur du domaine**.



Dans les options de contrôleur de domaine, on coche **Catalogue global** et **Contrôleur de domaine en lecture seule (RODC)**. On sélectionne le site **SiteDistant** et on définit un mot de passe pour la restauration des services d'annuaires.



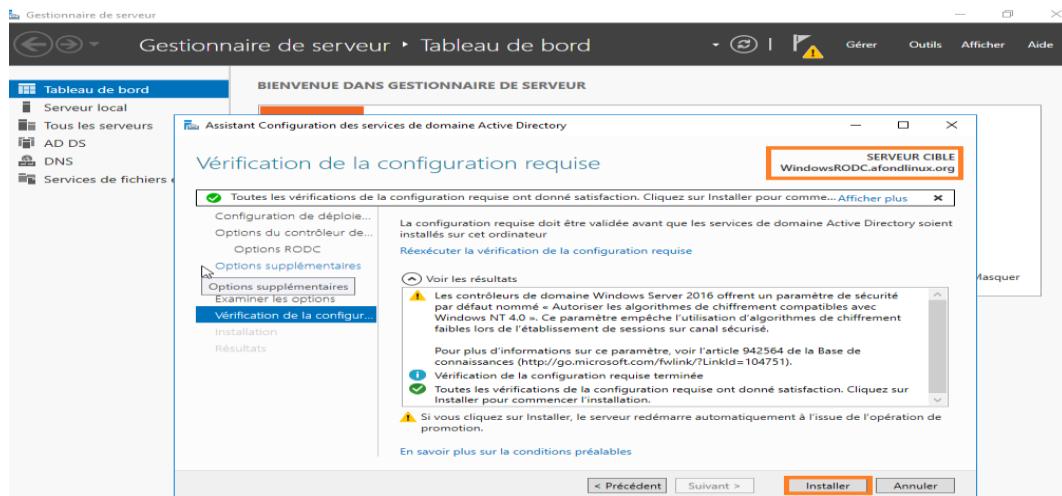
On laisse les options RODC par défaut. **Le groupe de réPLICATION DES MOTS DE PASSE EST ESSENTIEL** pour la suite.



On sélectionne le contrôleur de domaine depuis lequel répliquer les informations autorisées, ici le serveur WindowsAD du site local.



Une série de tests pour vérifier que l'installation est possible, on clique sur **Installer**. Puis le serveur WindowsRODC va redémarrer automatiquement.

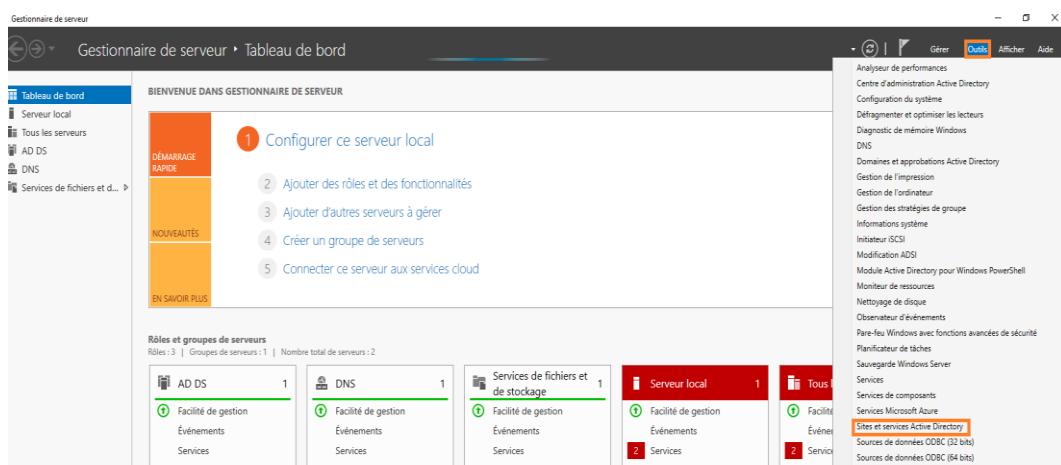


Dans la console **Utilisateurs et Ordinateurs Active Directory**, le serveur **WindowsRODC** a été placé automatiquement dans l'unité d'organisation **Domain Controllers**.

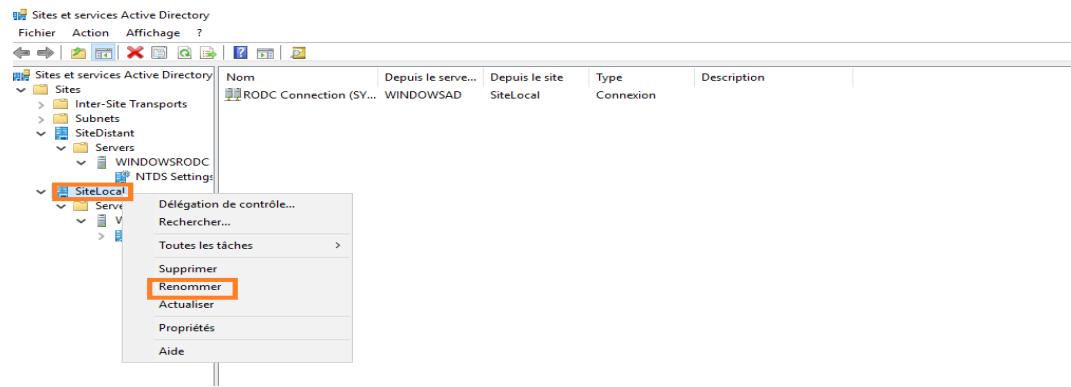
## VI. Mise en place de la réPLICATION inter-sites

La réPLICATION d'**Active Directory** est la méthode de transfert et de mise à jour des objets Active Directory d'un contrôleur de domaine à un autre. Les connexions entre les contrôleurs de domaine sont établies en fonction de leur emplacement dans une forêt et un site. Chaque site d'**Active Directory** contient un ou plusieurs sous-réseaux, qui identifient la plage des adresses IP associées à ce site. En établissant une correspondance entre l'adresse IP d'un contrôleur de domaine et un sous-réseau, **Active Directory** sait quels contrôleurs de domaine se trouvent dans quel site. Des connexions sont configurées entre les différents sites pour garantir que les objets **Active Directory** sont répliqués d'un site à l'autre. La durée de réPLICATION par défaut pour les connexions de site à site est de 180 minutes. Une durée minimale de 15 minutes peut être configurée dans l'interface graphique, et une durée encore plus courte peut être obtenue en modifiant le registre.

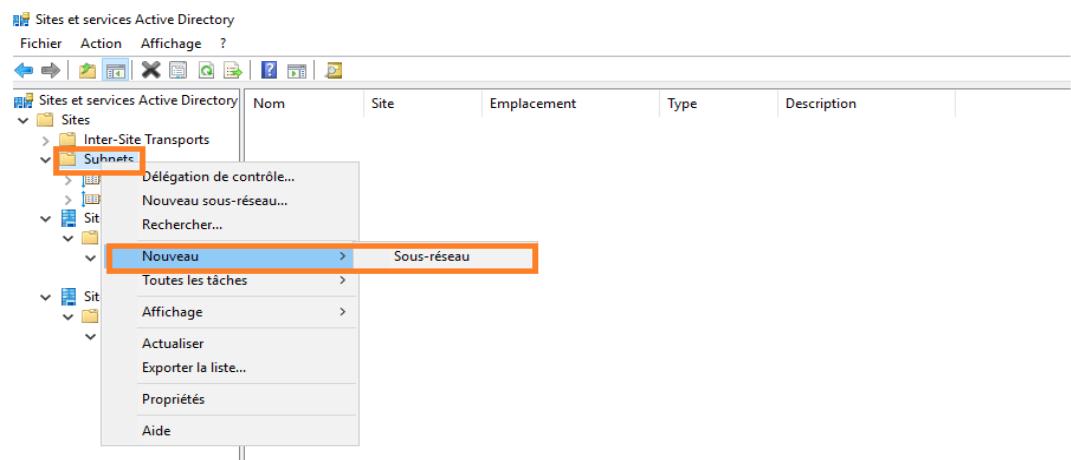
Pour configurer la réPLICATION inter-sites nous nous rendons dans la console **Sites et services Active Directory**



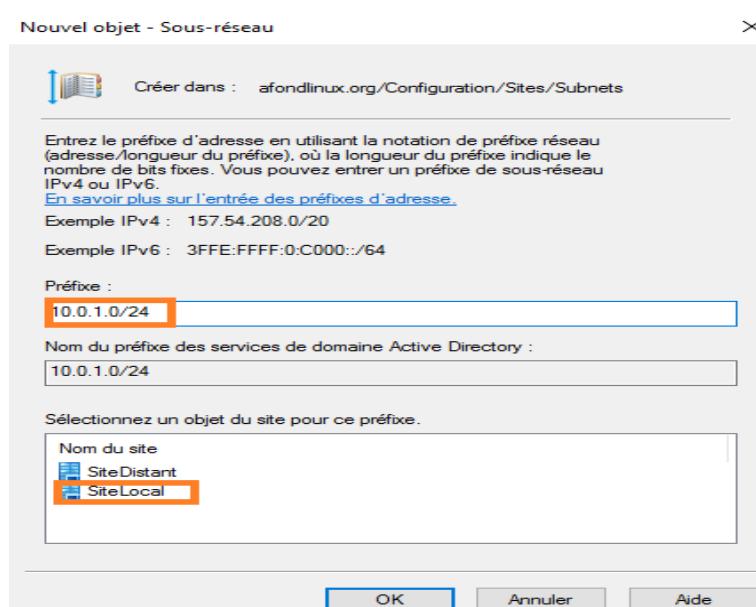
Lors de la création du domaine **Active Directory**, un site par défaut est créé (**Default-First-Site-Name**), la première étape consiste à renommer le site. Pour cela faire un clic droit sur le nom du site et cliquer sur **Renommer**



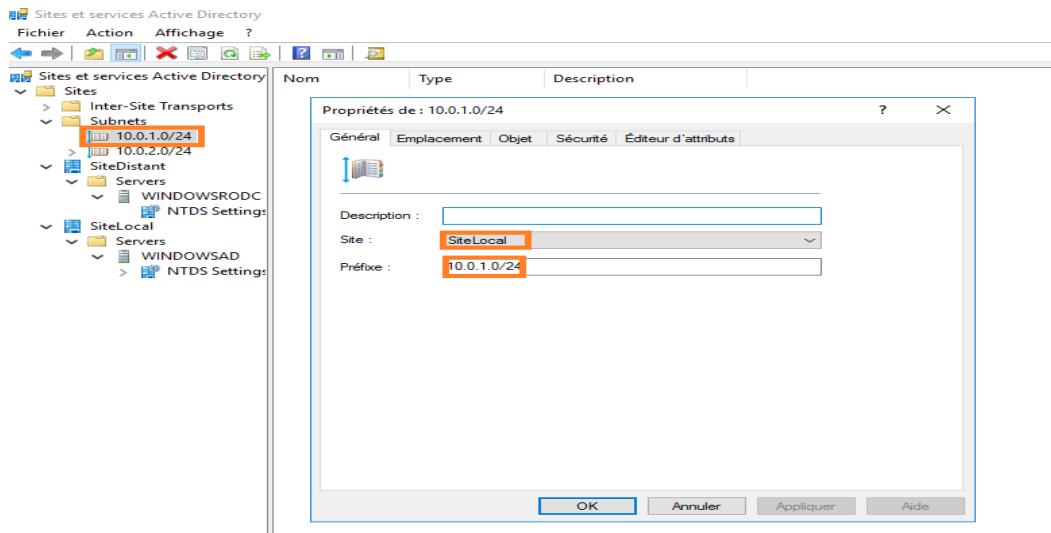
Maintenant que le site est nommé correctement, nous pouvons lui déclarer un réseau IP. La déclaration des réseaux permet de placer automatiquement les serveurs dans le bon site en fonction de son IP. Pour se faire, clic droit sur **Subnets** et on clique sur **Nouveau sous-réseau**.



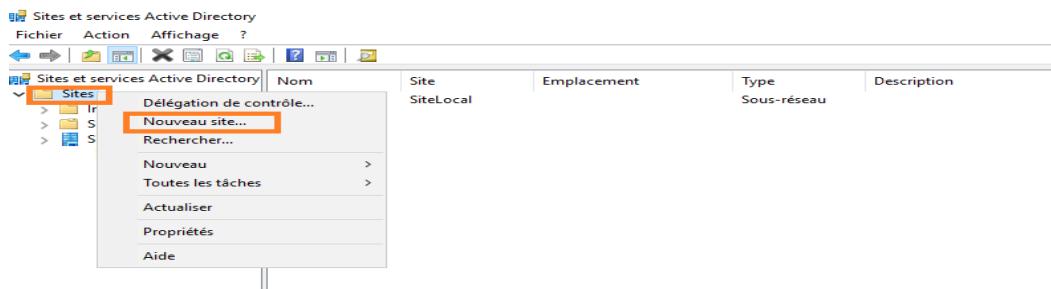
On enregistre l'adresse du réseau du site local et on sélectionne le site local. On valide en cliquant sur **OK** pour ajouter le sous-réseau.



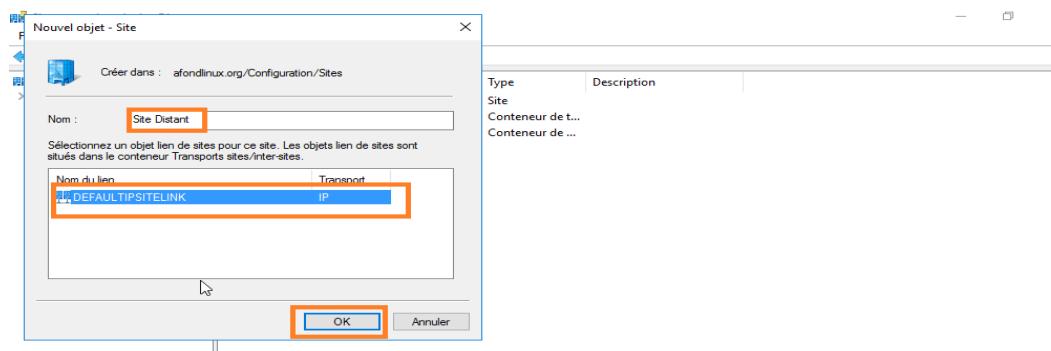
Le sous-réseau est ajouté. On peut également voir dans les propriétés du site local le sous-réseau qui lui est attribué.



On va maintenant ajouter notre site distant. Depuis la console, on fait un clic droit sur **Sites** puis on clique sur **Nouveau site**.



On renseigne le nom du site distant, on sélectionne un objet lien de réplication et on clique sur **OK**



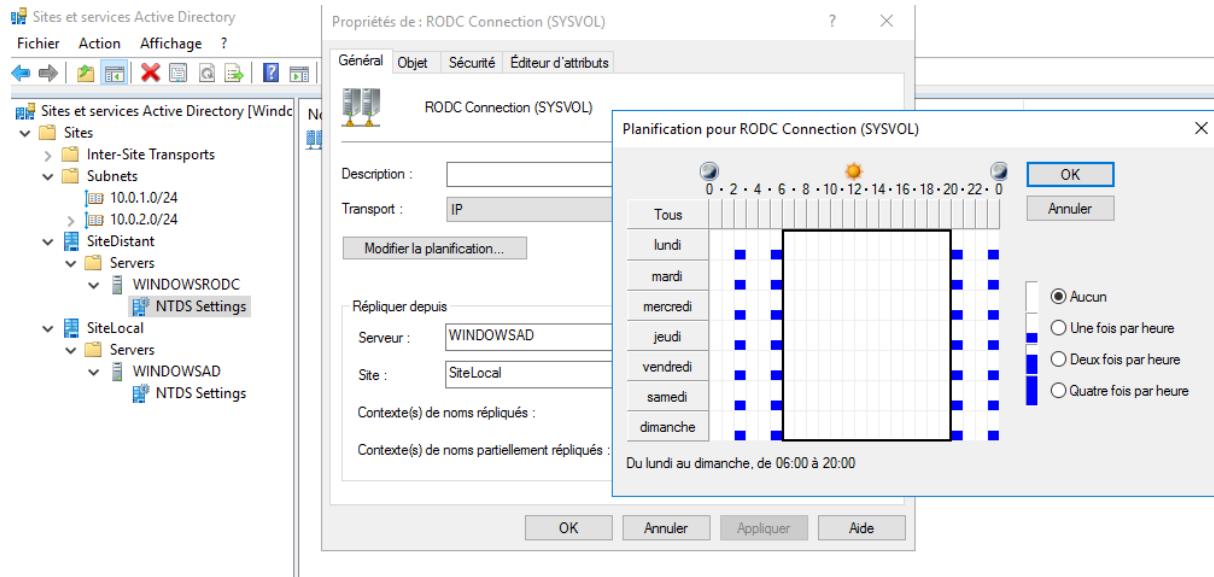
Un message de confirmation s'affiche, on clique sur **OK** pour le fermer. Le site est ajouté et disponible dans la console **Sites et services Active Directory**.

| Nom         | Site        | Emplacement | Type        | Description |
|-------------|-------------|-------------|-------------|-------------|
| 10.0.1.0/24 | SiteLocal   |             | Sous-réseau |             |
| 10.0.2.0/24 | SiteDistant |             | Sous-réseau |             |

Maintenant que les 2 sites ainsi que leur sous-réseau sont créés, on développe le serveur **WindowsRODC** et on clique droit sur **NTDS Settings**. Un lien de réplication du serveur **WindowsAD** a été ajouté pour le serveur **WindowsRODC**. On peut dès à présent forcer la réplication en faisant un clic droit sur **RODC Connection** et cliquer sur **Répliquer maintenant**.

| Nom                     | Depuis le serveur | Depuis le site | Type      | Description          |
|-------------------------|-------------------|----------------|-----------|----------------------|
| RODC Connection (SY...) | WINDOWSAD         | SiteLocal      | Connexion | Répliquer maintenant |

La fréquence de réplication se configure en fonction du type de lien (Inter ou Intra site). On ouvre les propriétés de cette connexion et on vérifie que le type de Transport soit bien **IP**. On clique sur **Modifier la planification**.



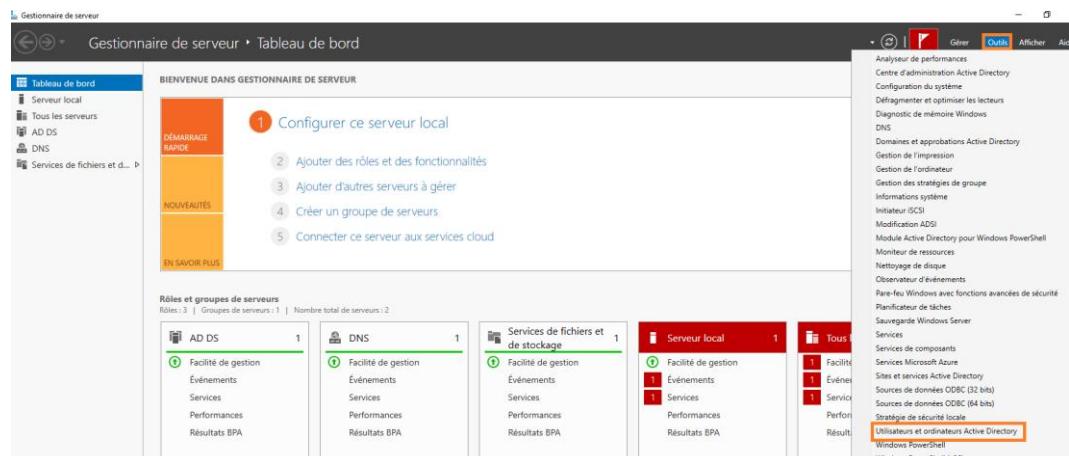
Actuellement, la réPLICATION s'effectue 1 fois toutes les 2 heures tous les jours de 21 heures à 6 heures. Cette planification ne perturbera pas le trafic pendant les heures de bureau.

## VII. Déclaration des ressources au sein d'Active Directory

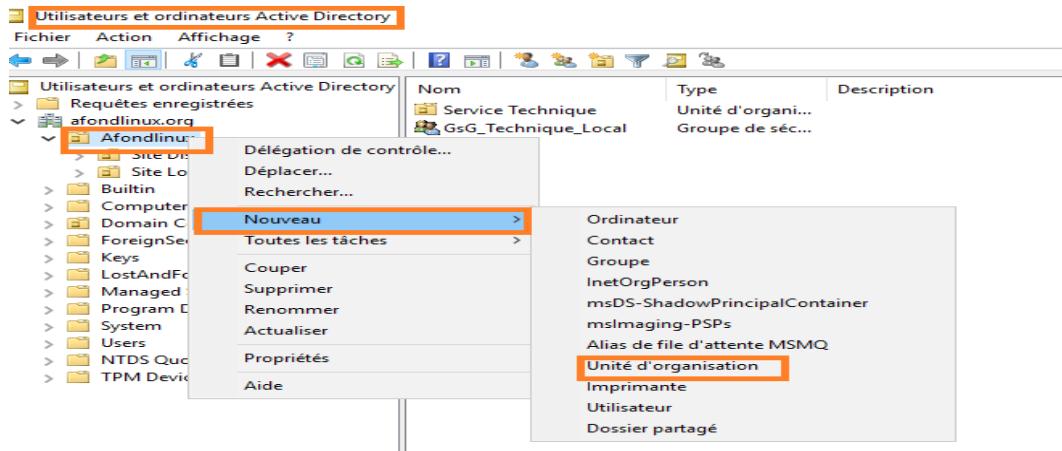
### A. Unité d'organisation

Une **unité d'organisation** ou **OU** est un conteneur dans un domaine **Active Directory** qui peut contenir des utilisateurs, des groupes et des ordinateurs. Il est la plus petite unité et permet de créer une arborescence et organiser les objets.

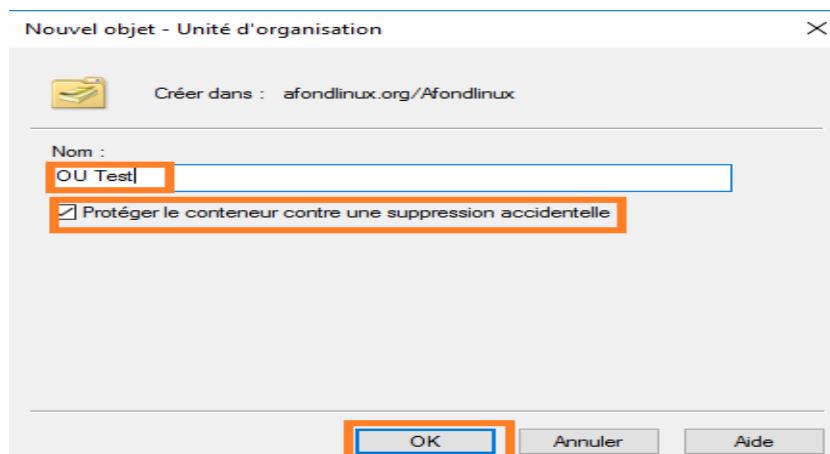
Pour créer des OU, il faut se rendre dans la console **Utilisateurs et Ordinateurs Active Directory**.



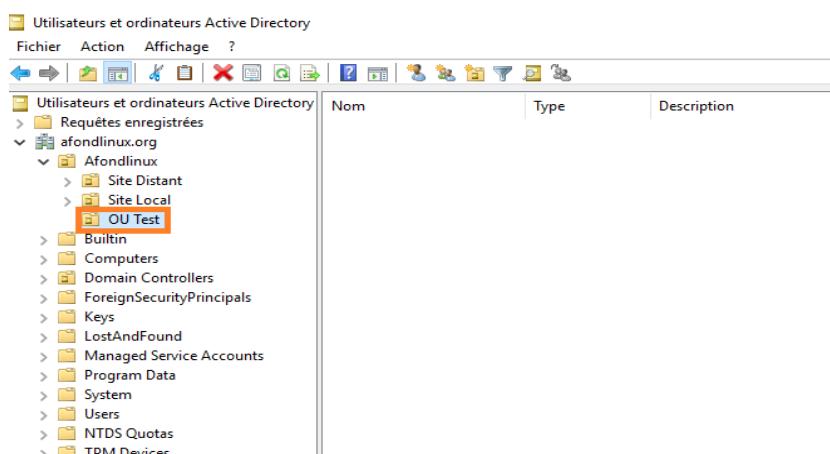
Dans la console **Utilisateurs et ordinateurs Active Directory**, on clique droit à l'endroit où l'on souhaite créer l'OU puis **Nouveau** puis **Unité d'organisation**.



On donne un nom à notre OU, ici OU test, on coche la case **Protéger le conteneur contre une suppression accidentelle** et on valide avec **OK**.

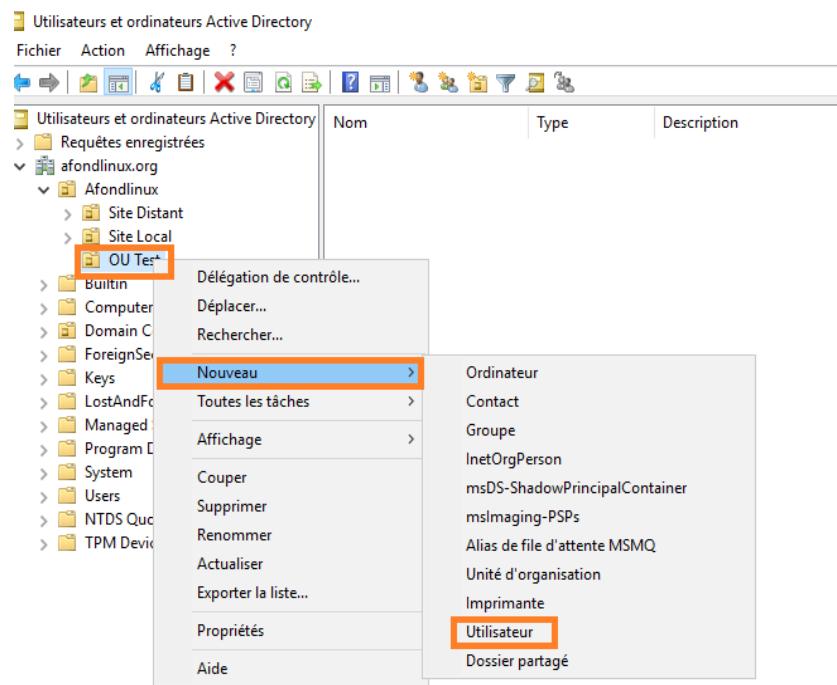


La nouvelle OU apparaît dans l'arborescence de la console **Utilisateurs et ordinateurs d'Active Directory**.



## B. Création d'utilisateurs

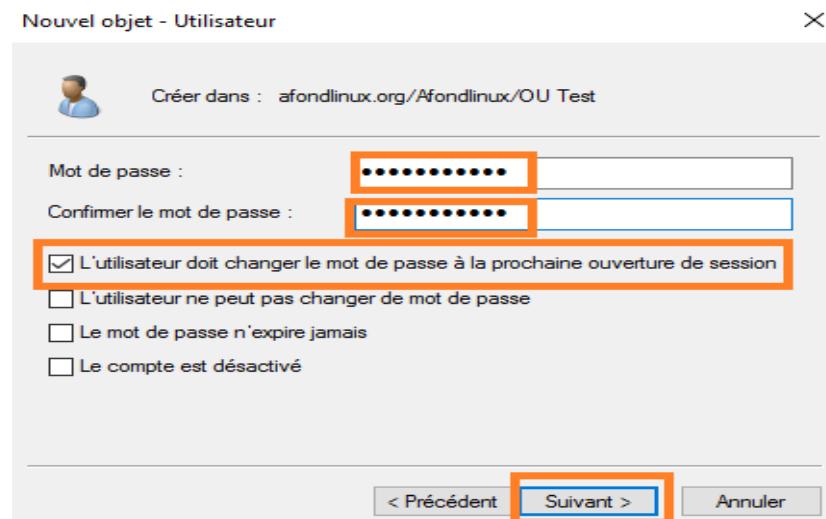
De la même manière, nous allons pouvoir créer via la même console des comptes utilisateurs qui permettent de s'authentifier sur le domaine, et accéder aux ressources, aux ordinateurs. Pour se faire, on clique droit sur l'OU test créée précédemment, puis **Nouveau** et **Utilisateurs**.



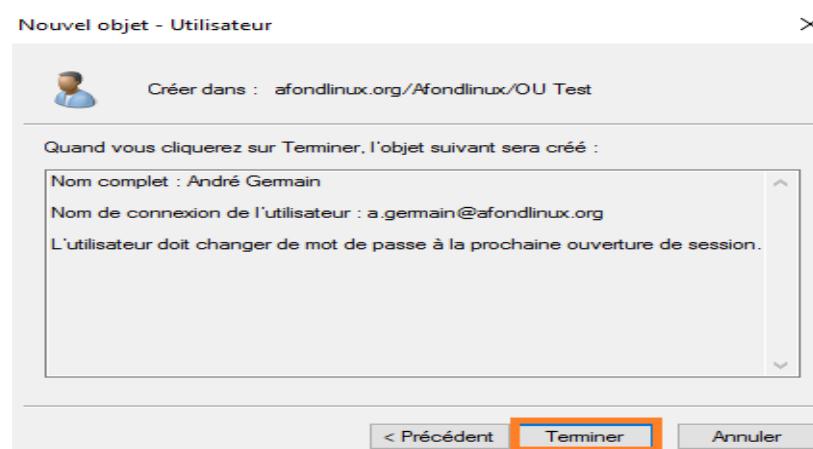
Dans la nouvelle fenêtre, on renseigne le prénom, le nom, et le nom d'ouverture de session du nouvel utilisateur. On valide avec **Suivant**.

The screenshot shows the 'Nouvel objet - Utilisateur' dialog box. The 'Créer dans' field is set to 'afondlinux.org/Afondlinux/OU Test'. The user information fields are filled as follows: Prénom : André, Nom : Germain, Nom complet : André Germain. The 'Nom d'ouverture de session de l'utilisateur' field contains 'a.germain@afondlinux.org'. The 'Suivant >' button at the bottom right is highlighted with a red box.

Dans la nouvelle fenêtre, on enregistre un mot de passe, et on coche la case L'utilisateur doit changer le mot de passe à la prochaine ouverture de session puis **Suivant**.



On accède à un récapitulatif de création de l'utilisateur et on clique sur **Terminer**.



Nous venons de créer un objet de type utilisateur dans l'OU test dans l'annuaire d'**Active Directory**.

| Nom           | Type        | Description |
|---------------|-------------|-------------|
| André Germain | Utilisateur |             |

## C. Les groupes

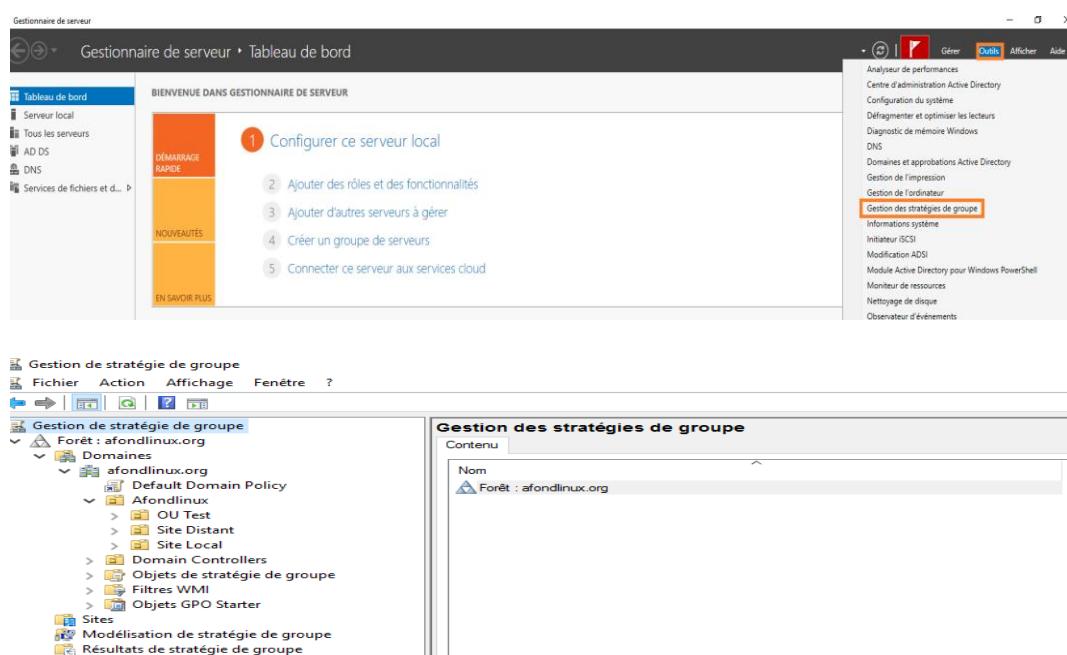
Les groupes permettent de regrouper des objets au sein d'un groupe, notamment pour simplifier l'administration (attribution de droits à un service qui correspond à un groupe nommé).

Il existe trois étendues différentes de groupe qui correspondent à sa portée au niveau de l'arborescence **d'Active Directory** : **Domaine local** utilisé uniquement dans le domaine dans lequel il est créé, **Globale** qui peut être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base et enfin **Universelle** qui a une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.

## VIII. Stratégies de groupe ou GPO

Une stratégie de groupe est un ensemble d'outils intégrés à Windows Server qui permet de centraliser la gestion de l'environnement utilisateur et la configuration des ordinateurs grâce à l'application de politiques. Chaque stratégie dispose de ses propres paramètres qui seront appliqués ensuite à des ordinateurs, des serveurs ou des utilisateurs. Grâce aux stratégies de groupe, il est possible d'avoir une configuration homogène entre les différents ordinateurs, mais aussi au niveau de l'environnement utilisateur. En effet, une stratégie de groupe peut servir à appliquer des paramètres sur Windows, mais aussi à l'utilisateur directement via sa session, ou les deux.

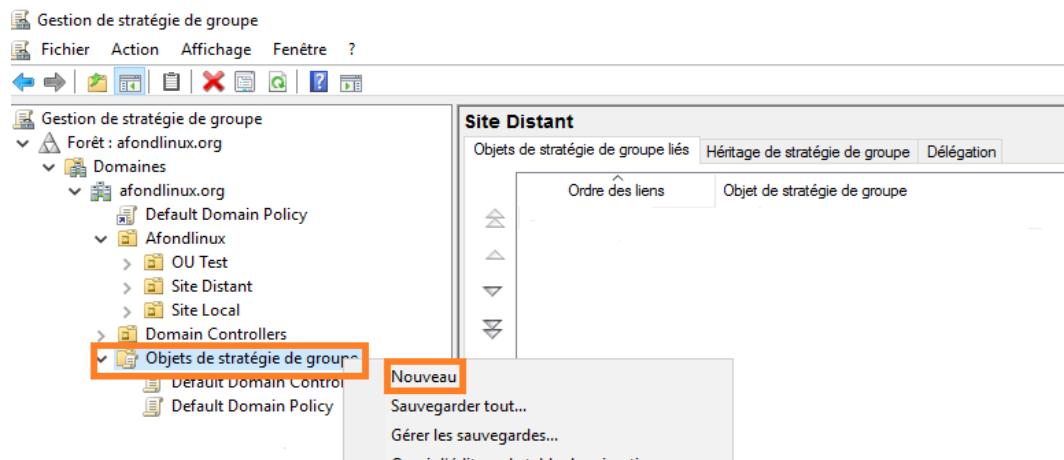
Depuis le Tableau de bord du gestionnaire de serveur, on clique sur Outils puis Gestion des stratégies de groupe.



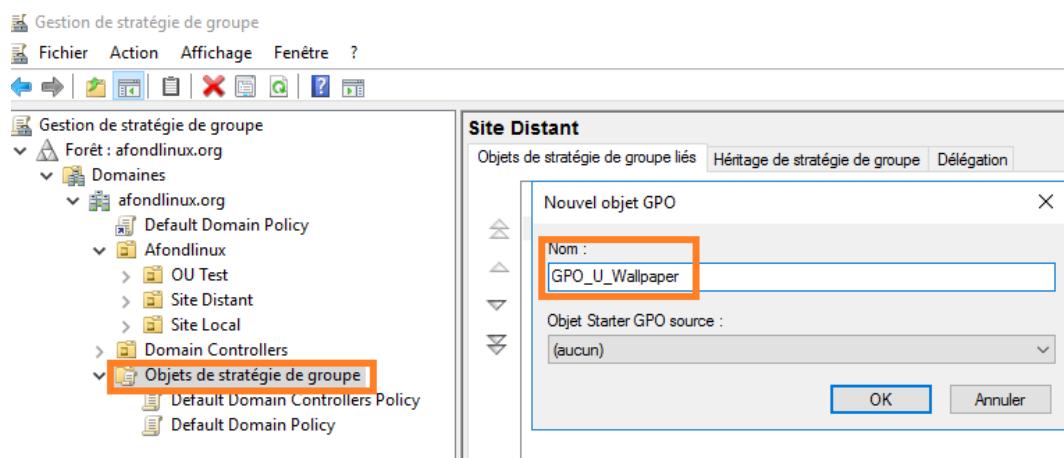
## A. GPO Papier peint du bureau

Tous les employés de l'entreprise Afondlinux doivent avoir le fond d'écran officiel de l'entreprise. Au préalable nous allons placer l'image que nous souhaitons déployer comme fond d'écran dans un dossier partagé sur le réseau de l'entreprise, dans notre cas il s'agira du chemin suivant : \\WINDOWSRODC\\netlogon\\tux.jpg

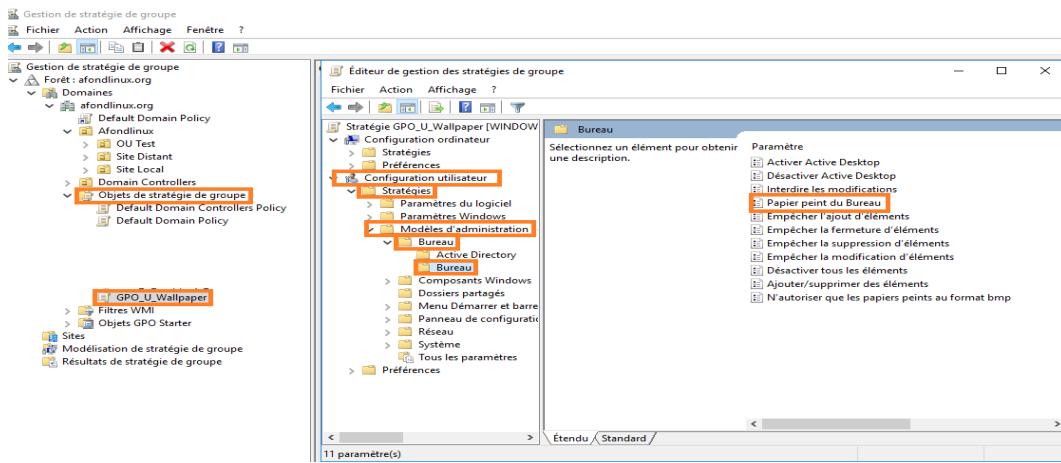
Puis dans la console **Gestion des stratégies de groupe**, on clique droit sur **Objet de stratégie de groupe**, puis **Nouveau**.



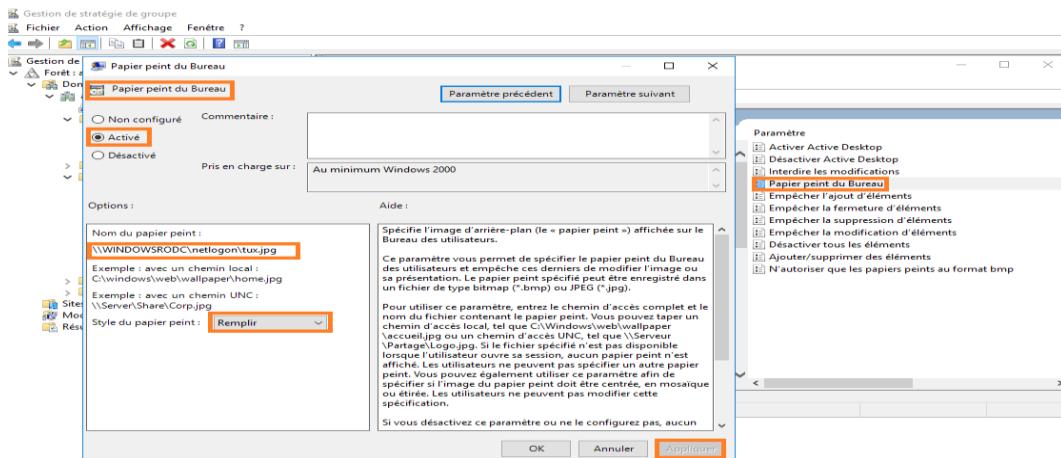
On nomme notre **GPO**, ici comme il s'agit d'une **GPO** qui s'applique sur les utilisateurs, j'utilise un nommage du type GPO\_U et le nom que l'on souhaite donner à notre **GPO**.



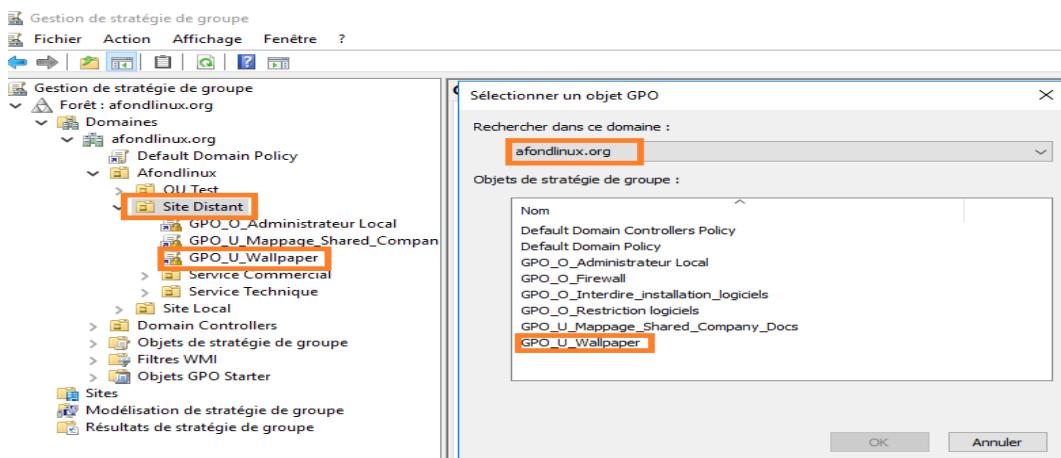
Toujours dans la console **Gestion des stratégies de groupe**, on développe le dossier nommé **Objets de stratégie de groupe**. On clique avec le bouton droit sur l'objet stratégie de groupe que l'on vient de créer et on sélectionne **Modifier**. L'éditeur de gestion de stratégies de groupe apparaît. On développe **Configuration utilisateur**, puis **Stratégies, Modèles d'administration, Bureau**. Sur la partie droite de l'éditeur on ouvre **Papier peint du Bureau**.



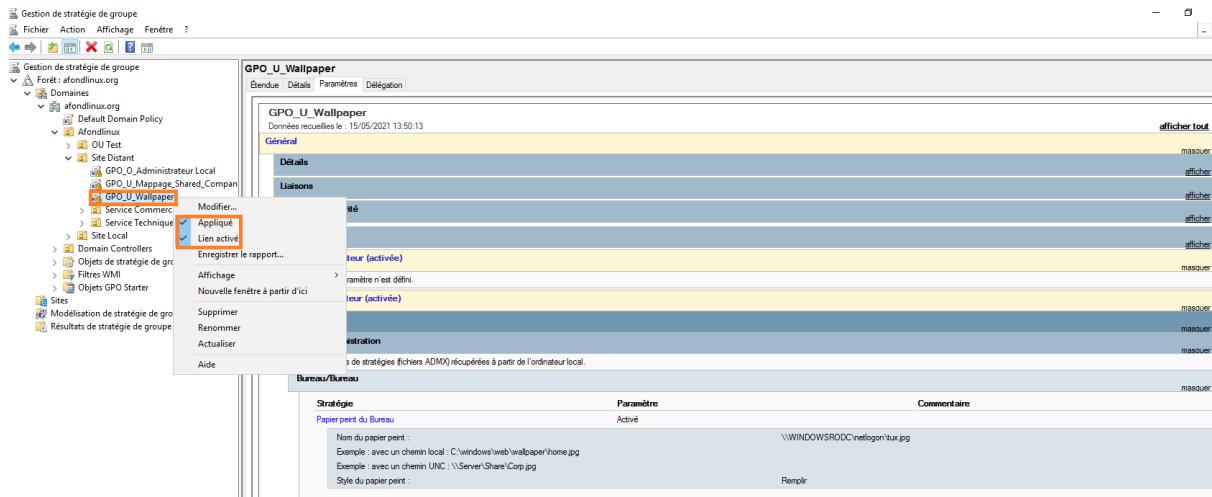
On coche **Activé**, on renseigne l'adresse du dossier partagé à laquelle se trouve l'image que l'on souhaite déployer comme fond d'écran et le type de remplissage puis on clique sur **Appliquer**.



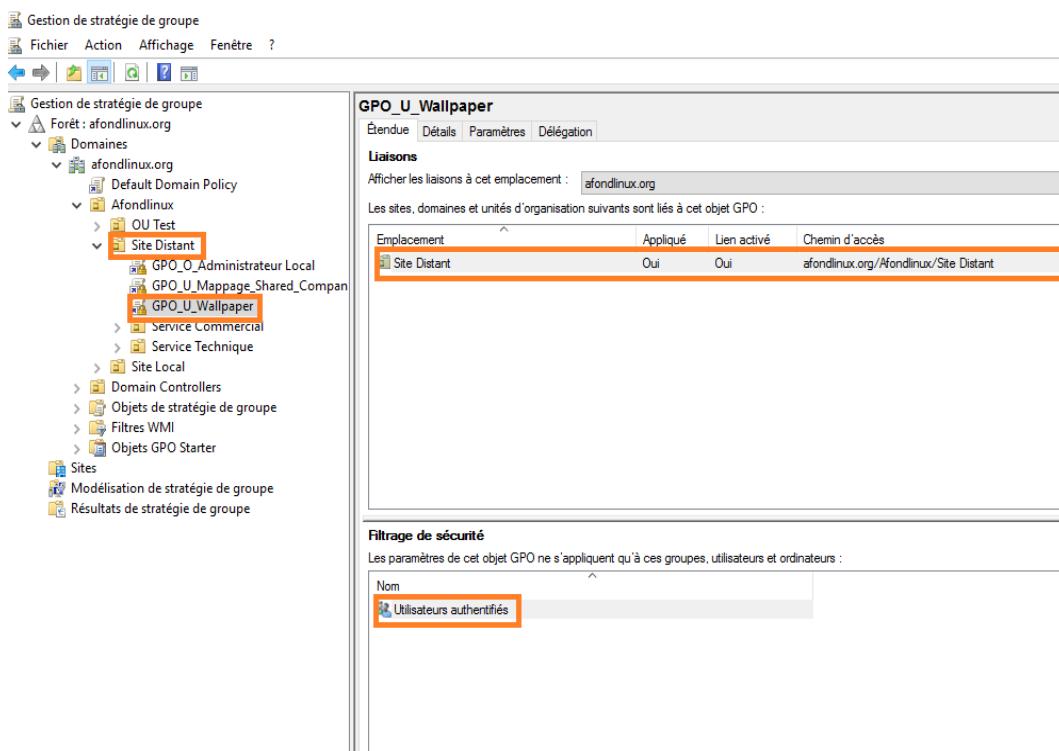
Dans la console **Gestion des stratégies de groupe**, on clique avec le bouton droit sur l'unité organisationnelle sur laquelle on souhaite appliquer la **GPO**, une nouvelle fenêtre apparait, on choisit le domaine, la **GPO\_U\_Wallpaper** puis on valide avec **OK**.



Notre **GPO** est maintenant liée avec l'unité organisationnelle voulue, il nous faut l'appliquer en cliquant droit sur l'objet **GPO\_U\_Wallpaper**, puis **Appliqué**. Sur la partie droite, nous avons un récapitulatif des paramètres de notre **GPO**. Après l'application de l'objet, on doit attendre 10 à 20 minutes pour que notre **GPO** soit appliquée sur les postes client. Pendant ce temps, la **GPO** sera répliquée sur le contrôleur de domaine **RODC**.



Nous voyons au niveau de l'**étendue**, que notre **GPO** est bien activée et appliquée sur l'unité organisationnelle **Site Distant** et qu'elle s'applique aux **Utilisateurs authentifiés sur le domaine**.



Sur un poste client, on ouvre une console CMD, et l'on exécute la commande **gpupdate /force** pour forcer la mise à jour des **GPO**. On voit que la mise à jour des **GPO** s'est déroulée sans erreur.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19042.985]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\c.henri>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

C:\Users\c.henri>
```

En exécutant la commande **gpresult /r**, on voit que la **GPO** a bien été appliquée.

```
Données RSOP pour AFOND LINUX\c.henri sur WORKSTATION1 : mode journalisation
-----
Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.19042
Nom du site..... : N/A
Profil itinérant : N/A
Profil local..... : C:\Users\c.henri
Connexion via une liaison lente ? : Non

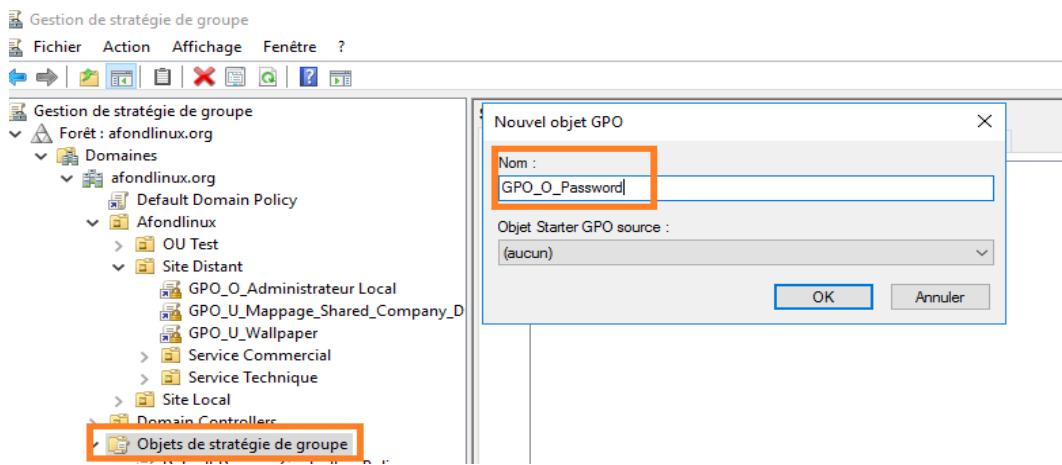
PARAMÈTRES UTILISATEURS
-----
CN=Christophe Henri,OU=Utilisateurs,OU=Service Technique,OU=Site Distant,OU=Afondlinux,DC=afondlinux,DC=org
Heure de la dernière application de la stratégie de groupe : 15/05/2021 à 17:00:36
Stratégie de groupe appliquée depuis : WindowsRDC.afondlinux.org
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : AFOND LINUX
Type de domaine : Windows 2008 ou contrôleur de domaine en lecture seule ultérieur

Objets Stratégie de groupe appliqués
-----
GPO_U_Mappage_Shared_Company_Docs
GPO_U_Wallpaper
```

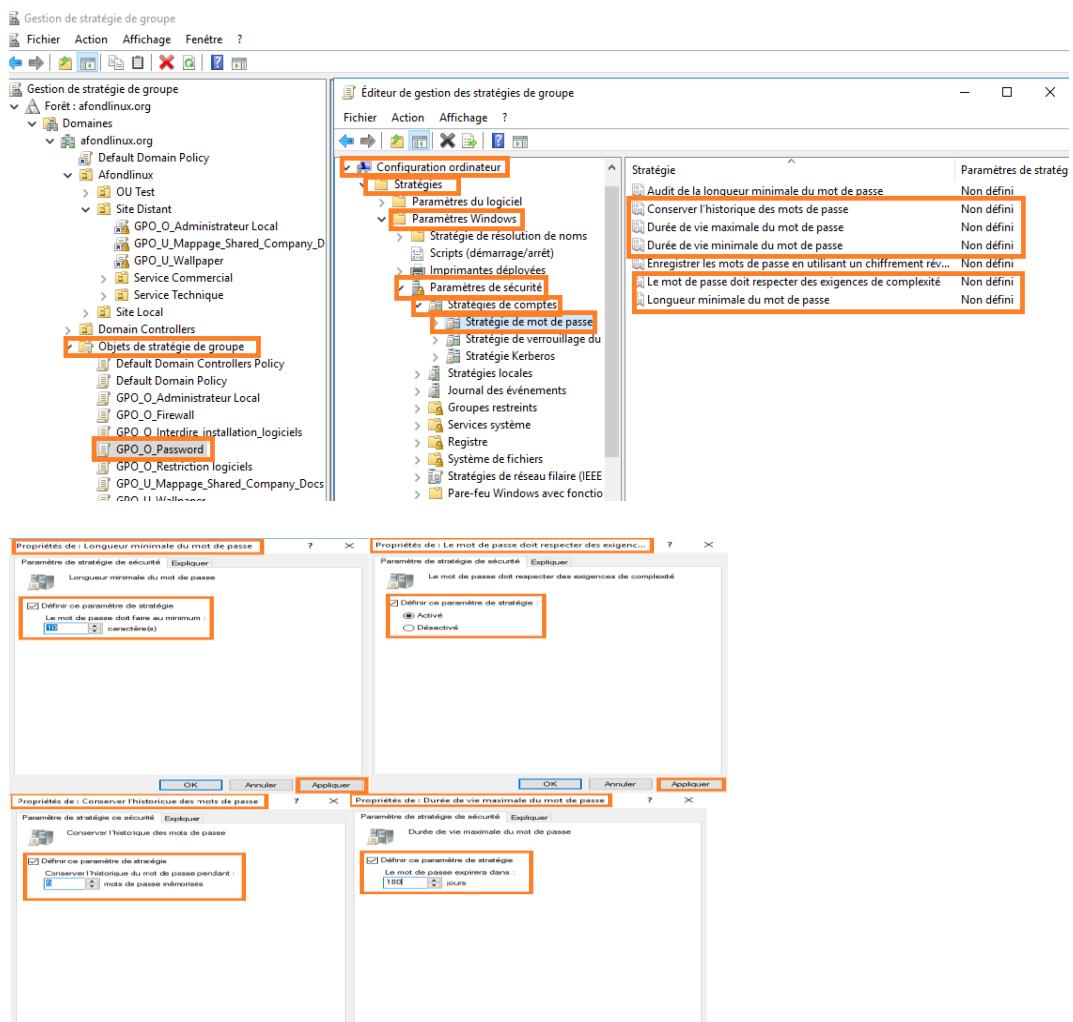
## B. GPO Mot de passe

Tous les employés de l'entreprise afondlinux.org doivent avoir un mot de passe fort et le changer tous les six mois. Même si la **GPO** par défaut du domaine positionne déjà des valeurs, il convient de ne pas y toucher et de créer une nouvelle **GPO** dédiée à votre politique de sécurisation. Ces paramètres se situent dans la configuration ordinateur car ils vont être gérés de la même façon pour tous les utilisateurs d'un ordinateur. Un mot de passe fort est idéalement long et contient des lettres, des signes de ponctuation, des symboles et des chiffres. Il contient au moins huit caractères ou plus. On doit éviter d'utiliser des mots de passe où les signes se succèdent dans l'ordre habituel ou des séquences ou des caractères répétés ni mentionner des informations personnelles.

Pour mettre en place cette **GPO**, nous allons procéder de la même manière que précédemment et créer un nouvel objet de stratégie de groupe appelé **GPO\_O\_Password**.



Dans l'éditeur de gestion des stratégies de groupe, on développe **Configuration ordinateur**, **Stratégies**, **Paramètres de sécurité**, **Stratégies de comptes**, **Stratégies de mot de passe** et on active les stratégies suivantes : **Longueur minimale du mot de passe**, **Le mot de passe doit respecter des exigences de complexité**, **Conserver l'historique des mots de passe** et **Durée de vie maximale du mot de passe**.

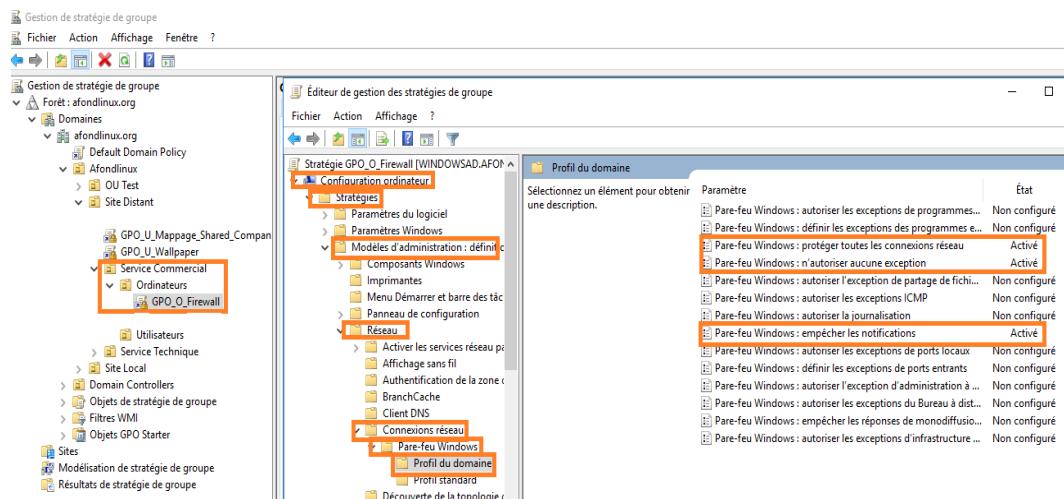


On lie notre **GPO** à l'unité organisationnelle que l'on souhaite et on l'applique.

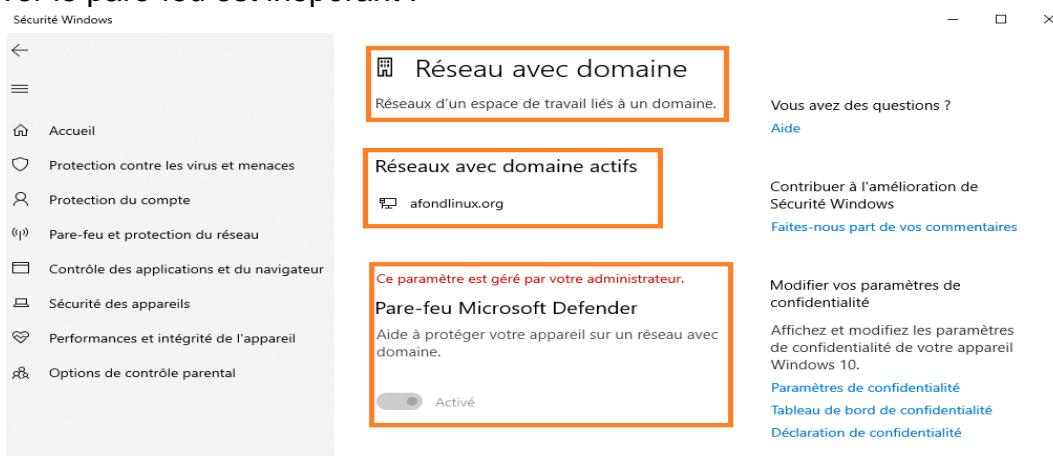
## C. GPO Pare-feu

Aucun employé de l'entreprise ne doit pouvoir désactiver le pare-feu Windows. Par défaut les utilisateurs authentifiés n'ont pas les droits nécessaires de le faire mais un administrateur local possédant des droits administrateurs pourra désactiver le pare-feu.

Pour que cela ne soit pas possible nous allons créer la **GPO** suivante. Celle-ci sera nommée **GPO\_O\_Firewall**, car elle s'applique non pas aux utilisateurs authentifiés mais aux ordinateurs. On l'appliquera aux unités organisationnelles voulues.



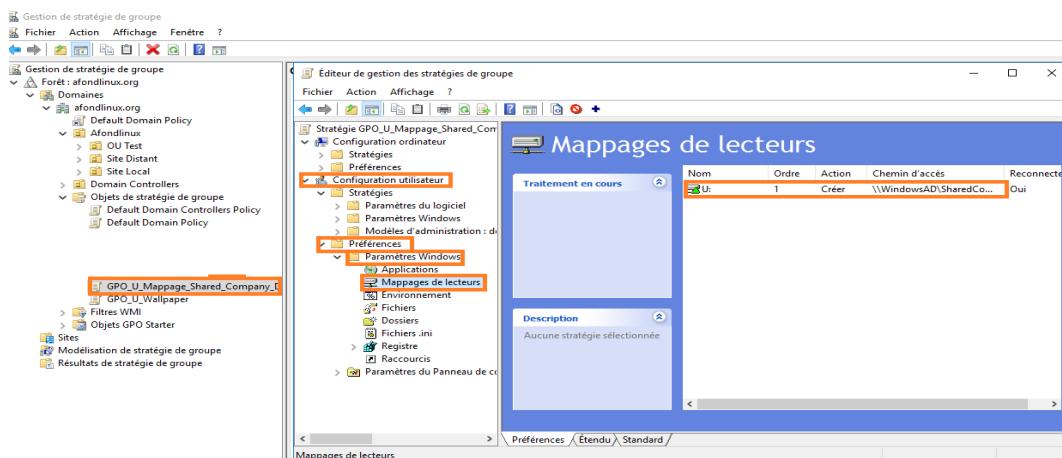
On peut vérifier l'application de la GPO sur un poste client, le bouton pour désactiver / activer le pare-feu est inopérant :



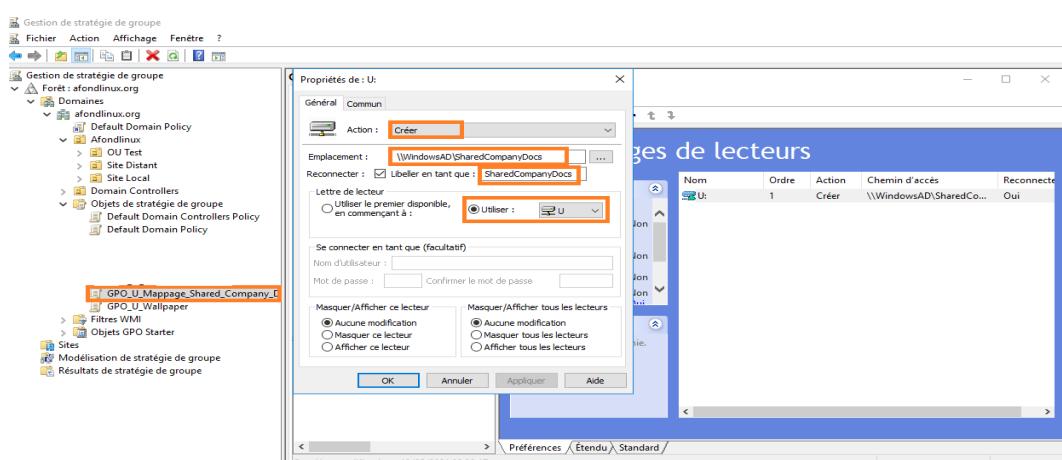
## D. GPO Mappage lecteur réseau

Tous les employés de l'entreprise Afondlinux doivent avoir accès en lecture-écriture au répertoire partagé **SharedCompanyDocs**. De la même manière que précédemment, nous créons un nouvel objet dans **Objet de stratégie de groupe**.

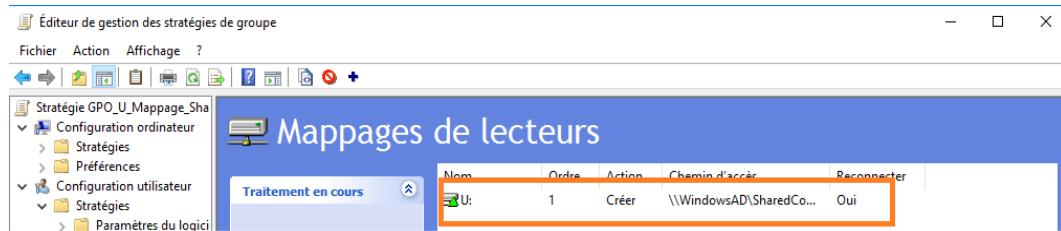
On nomme notre **GPO**, ici comme il s'agit d'une **GPO** qui s'applique sur les utilisateurs, je la nomme **GPO\_U\_Mappage\_Shared\_Company\_Docs**. Dans **l'éditeur de gestion des stratégies de groupe**, je développe **Configuration utilisateur**, **Préférences**, **Paramètres Windows**, **Mappages de lecteurs**. Au niveau de la fenêtre **Mappages de lecteurs**, je clique droit, puis **Nouveau** et enfin **Lecteur mappé**.



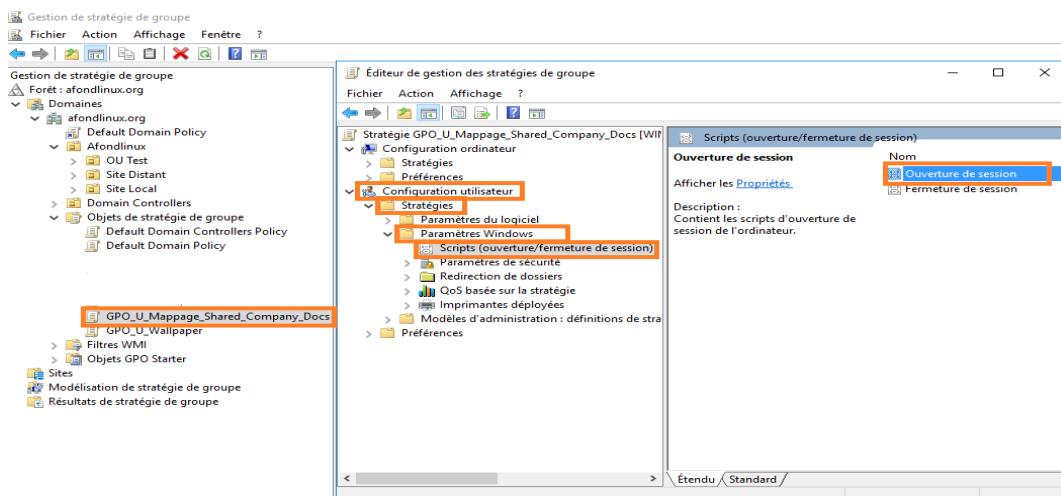
On remplit le formulaire, en saisissant comme action **Créer**, puis l'emplacement du partage réseau, le libellé du partage et la lettre utilisée. On valide avec **OK**.



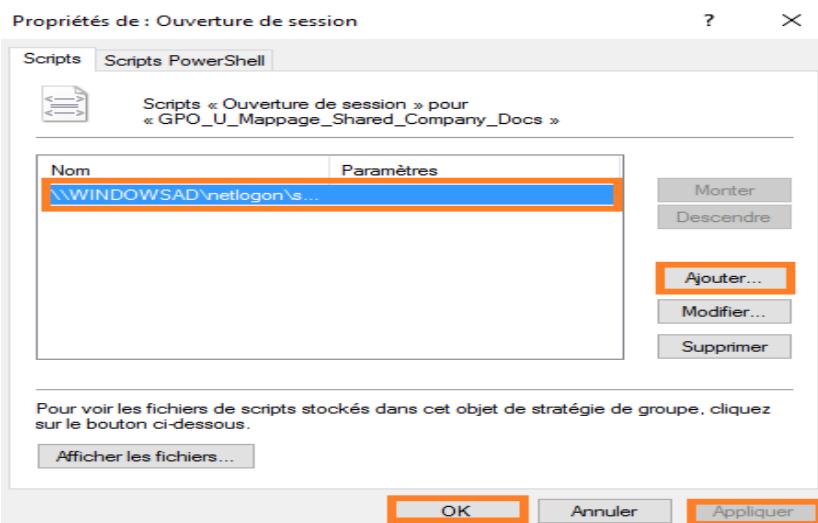
Le lecteur doit être visible dans Mappages de lecteurs.



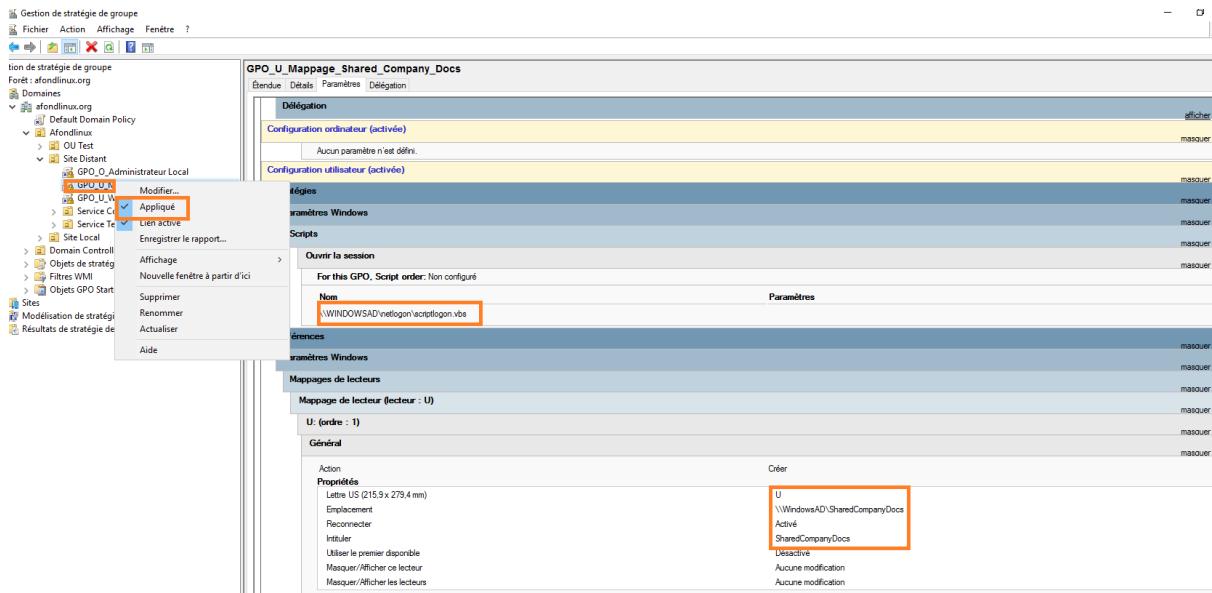
Afin que le lecteur mappé se monte à l'ouverture de session de l'utilisateur, nous allons créer un script qui sera placé dans le dossier partagé NETLOGON qui contient les scripts de démarrage. Nous allons créer une nouvelle GPO pour l'exécution de script.



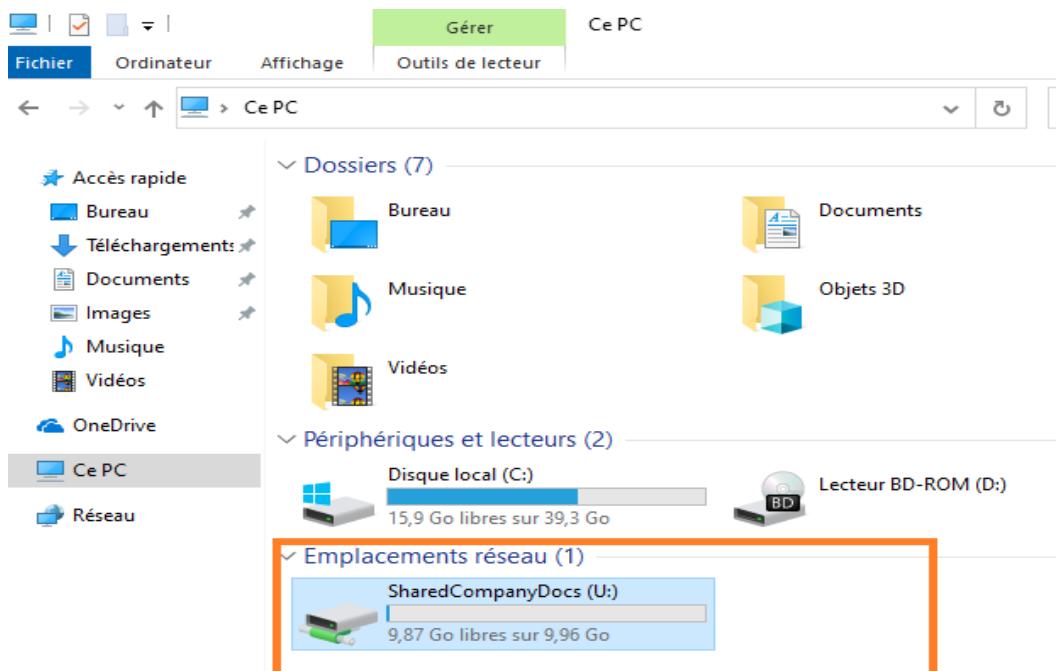
On ouvre en double cliquant sur **Ouverture de session**. On clique sur **Ajouter**. Dans le champ **Nom du script** : on indique le chemin du script de démarrage et on clique sur **OK**. On vérifie que le script est bien sélectionné, puis on clique sur **Appliquer** et sur **OK**.



De la même manière que précédemment, on lie et applique notre GPO à l'unité organisationnelle voulue. On peut vérifier les paramètres ainsi que l'étendue.

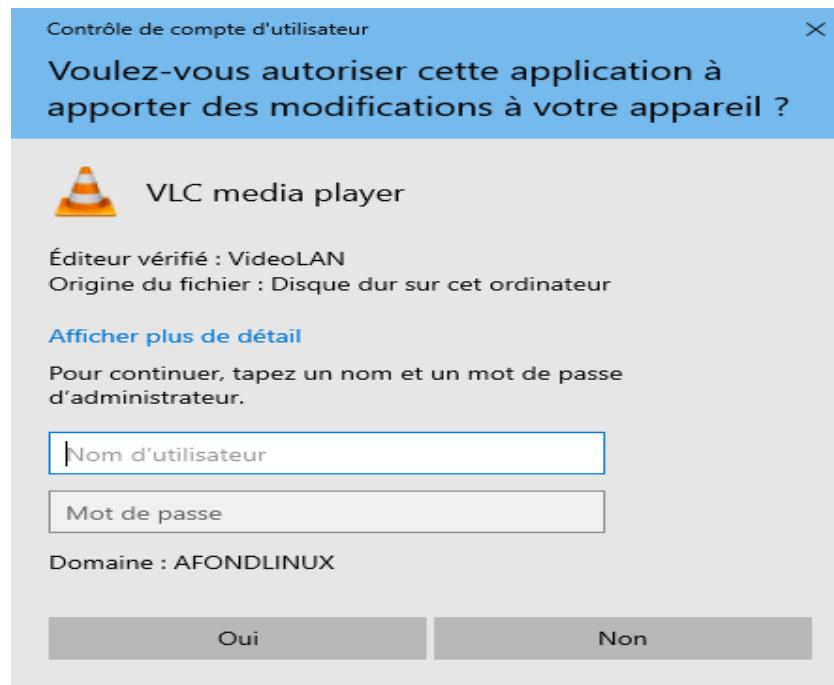


On vérifie sur un poste client que le dossier partagé est bien monté :



## E. Bloquer l'installation de logiciel

Aucun employé de l'entreprise Afondlinux ne peut installer de logiciels sauf les membres du service technique. Il faut savoir que par défaut les utilisateurs authentifiés sur le domaine n'ont pas les droits nécessaires pour installer des logiciels.

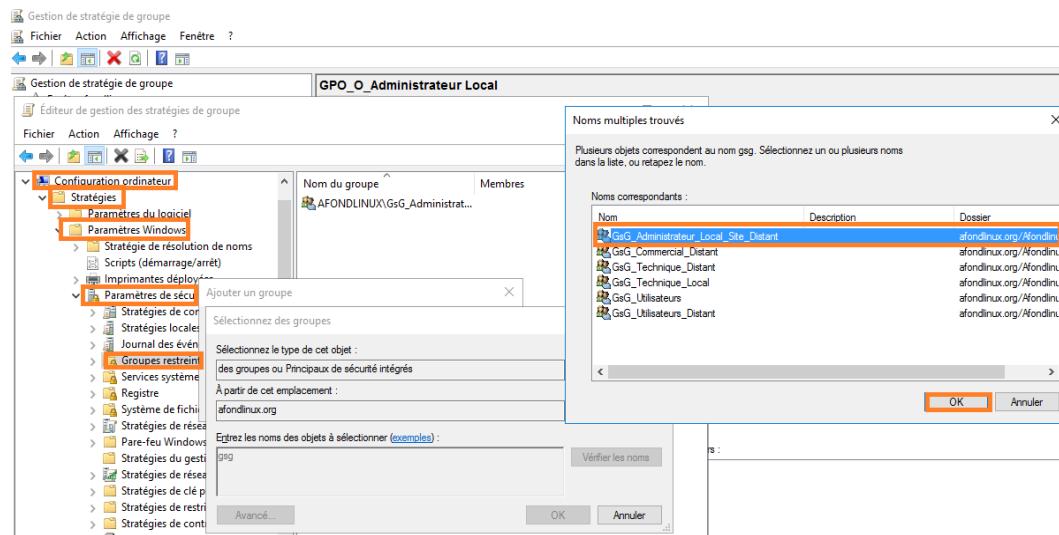


Pour qu'un utilisateur du service technique puisse installer des logiciels, il faut qu'il ait les droits administrateurs. Nous allons donc créer une **GPO** pour que l'utilisateur **c.henri** ait soit **administrateur local** du site distant et puisse installer des logiciels.

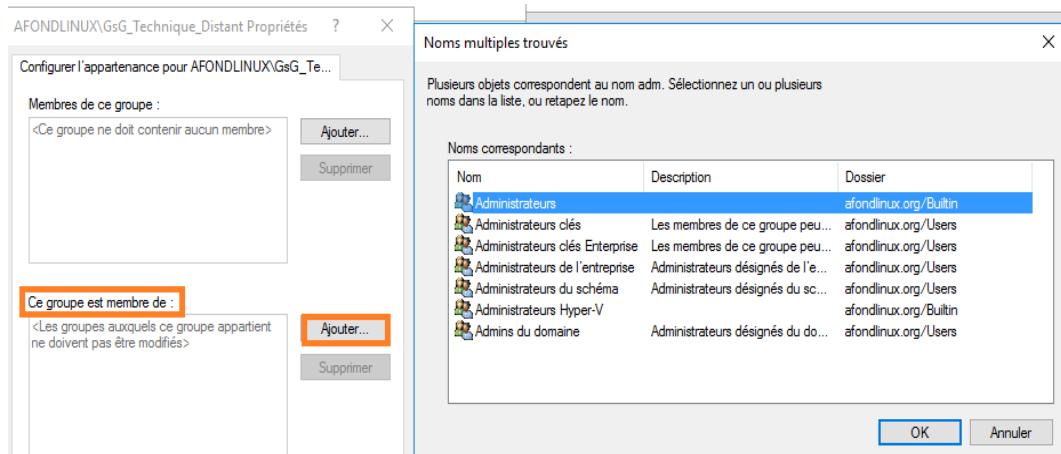
Au préalable, on aura créé un **groupe de Sécurité Globale Administrateur local** qui aura pour membre l'utilisateur **c.henri**.

De la même manière que précédemment, on crée un objet dans **Objet de stratégie de groupe** que l'on appellera **GPO\_O\_Administrateur local**. On clique droit sur notre objet, puis **Modifier**, et on développe **Configuration ordinateur**, **Stratégies**, **Paramètres Windows** et **Groupes restreints**.

On clique droit sur **Groupes restreints** et **Ajouter un groupe**. Un assistant s'ouvre, on clique sur **Parcourir** pour ajouter notre groupe de sécurité globale **Administrateur local** que nous avons créé dans **l'Active Directory**.

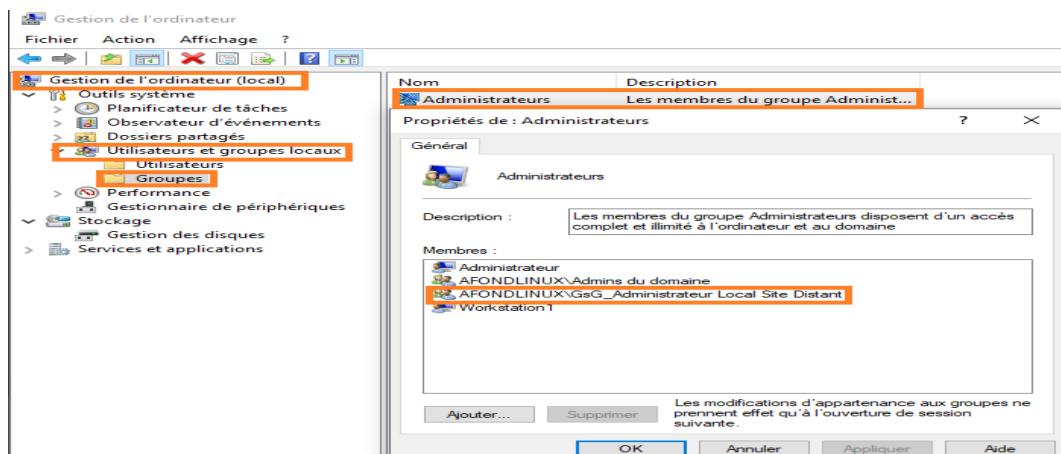


Ensuite, on clique sur **Ajouter** au niveau de **Ce groupe est membre de** puisque l'on veut que notre groupe soit membre de **Administrateurs**. On recherche le groupe **Administrateurs** et on valide.

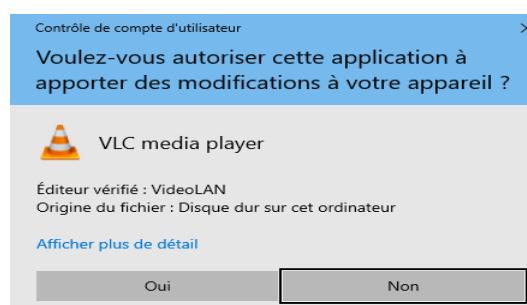


On peut alors lier et appliquer notre **GPO** à l'unité organisationnelle voulue. Et vérifier côté client que notre utilisateur fait bien partie du groupe **Administrateur local** et peut installer des logiciels.

Sur le poste client de **c.henri**, on clique droit sur le bouton **Démarrer** puis **Gestion de l'ordinateur**. Sous **Outils système**, on clique sur **Utilisateurs et groupes locaux**, puis **Groupes**, on ouvre **Administrateurs**, le groupe de sécurité globale contenant notre utilisateur **c.henri** y est présent.

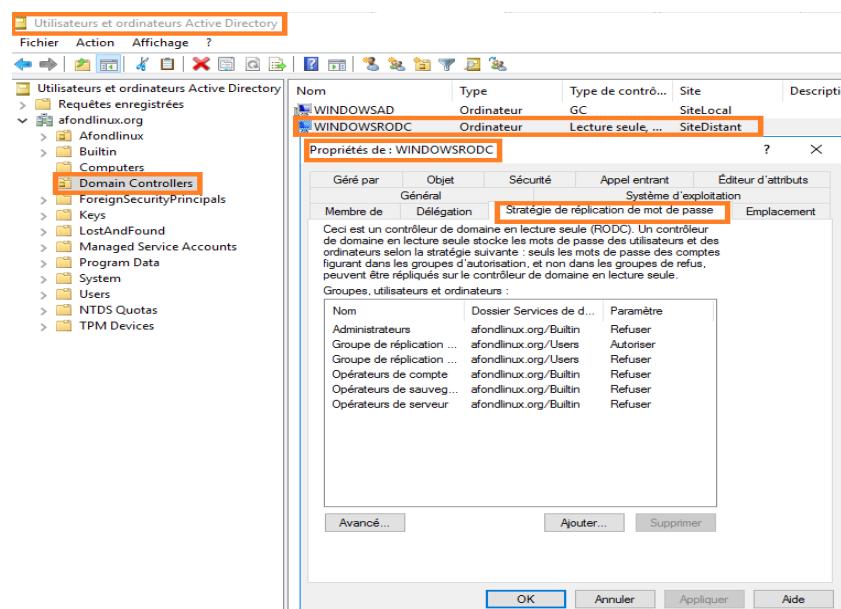


Notre utilisateur **c.henri** du service technique peut maintenant installer des logiciels.

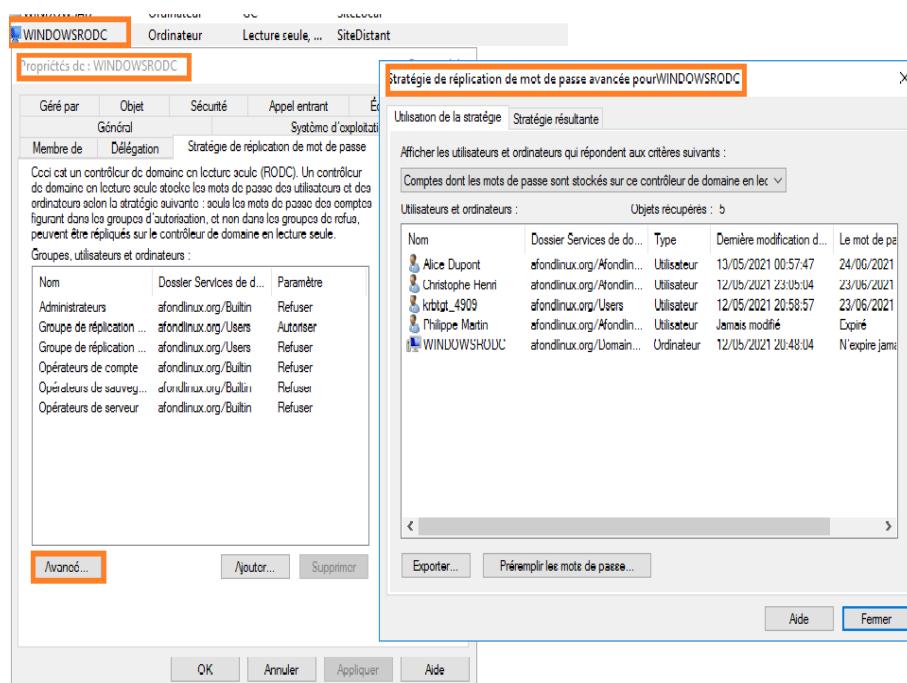


## **IX. Stratégie de réPLICATION des mots de passe**

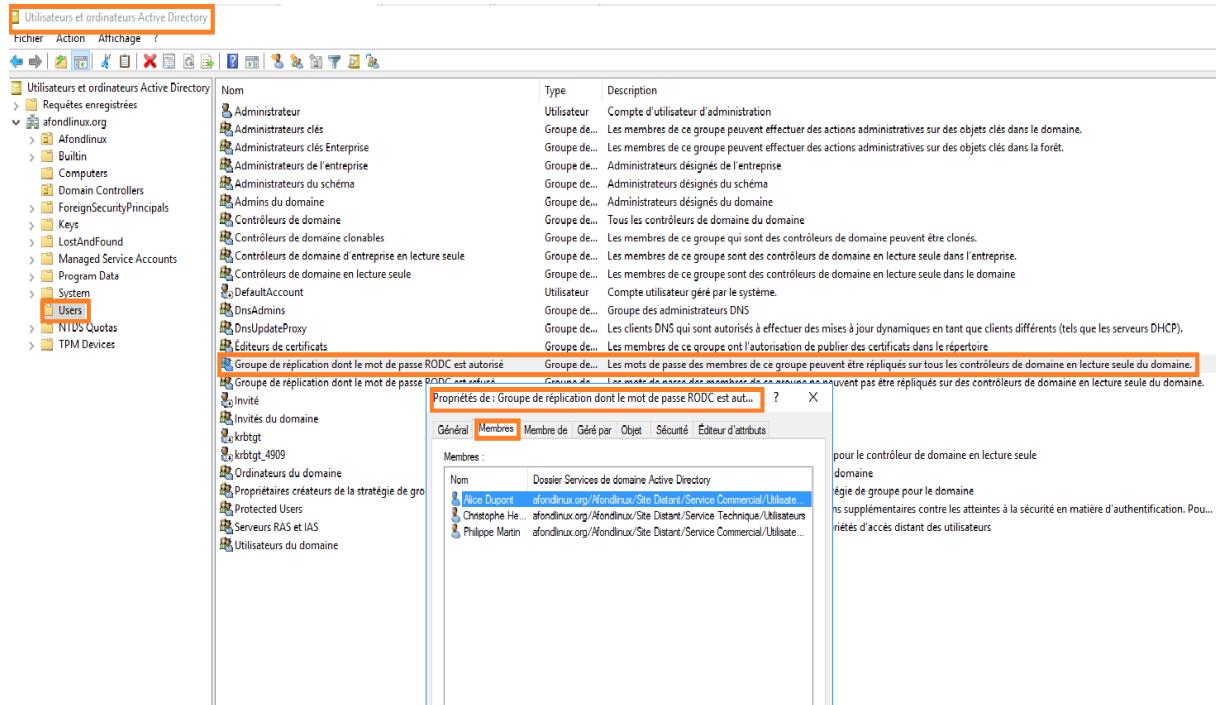
Maintenant que nos utilisateurs et groupes sont créés, nous allons voir comment administrer le contrôleur RODC. Sur le serveur **WindowsAD**, nous ouvrons la console **Utilisateur et ordinateur Active Directory** et entrons dans l'unité organisationnelle **Domain Computer**. Puis ouvrons les propriétés du serveur **WindowsRODC** et allons sur **Stratégie de réPLICATION de mot de passe**, on peut alors voir les groupes **Autorisés** et **Refusés** :



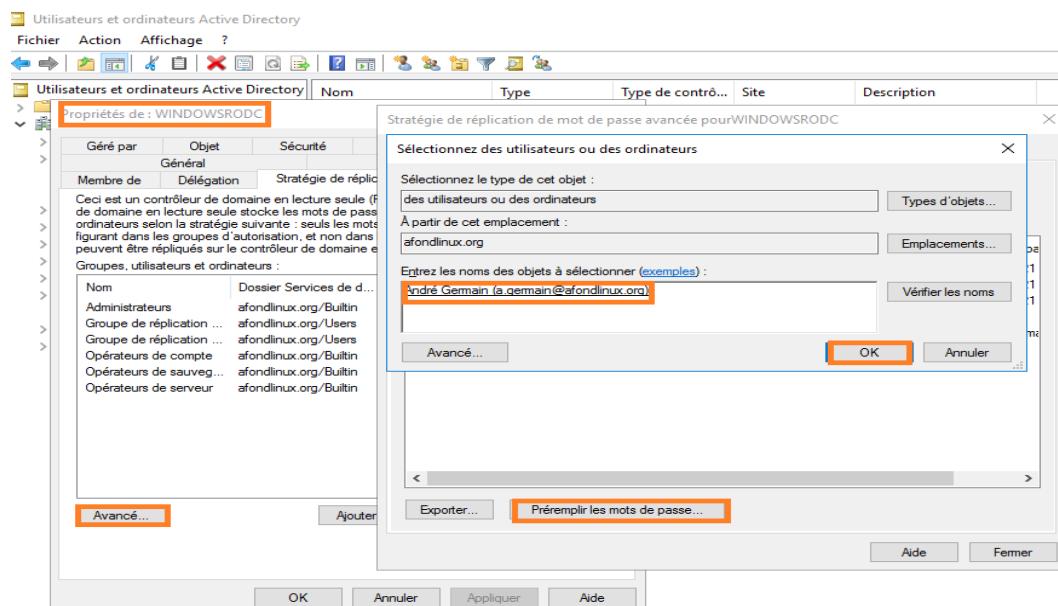
En cliquant sur le bouton **Avancé**, on peut voir les objets dont le mot de passe est répliqué et les utilisateurs ayant une session ouverte sur le **contrôleur RODC**.



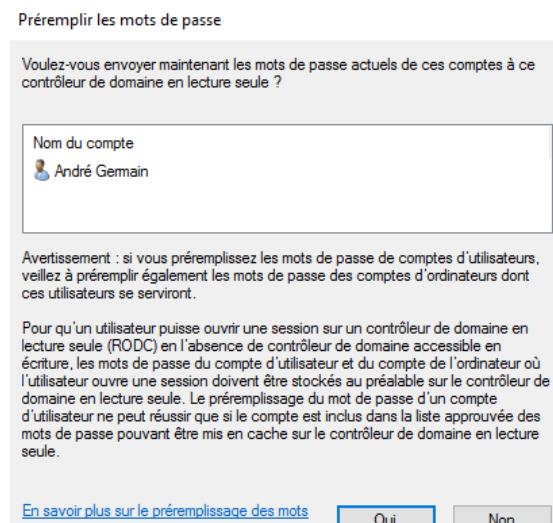
Dans la console **Utilisateurs et ordinateurs Active Directory**, nous entrons dans le conteneur **Users**. Ici, on trouve tous les groupes enregistrés. Nous cliquons droit sur le **Groupe de réPLICATION dont le mot de passe RODC est autorisé** pour accéder aux propriétés. Dans l'onglet **Membres** nous pouvons ajouter nos utilisateurs.



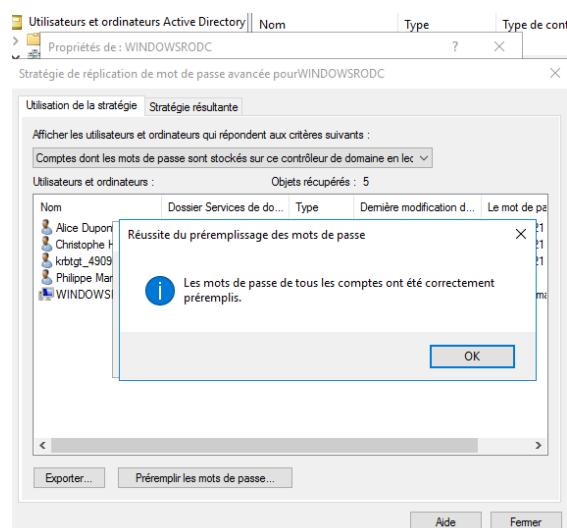
Maintenant que cela est fait, nous nous rendons à nouveau dans les propriétés du serveur **WindowsRODC** dans le conteneur **Domain Controller**. Puis **Stratégie de réPLICATION de mot de passe et Avancé**. Dans la nouvelle fenêtre, on clique sur **Préremplir les mots de passe**. On ajoute l'utilisateur qu'on autorise à s'authentifier via le serveur WindowsRODC.



On confirme en cliquant sur **OK**.



De nouveau **Ok**



Puis **Ok** de nouveau.

L'utilisateur est maintenant ajouté aux comptes qui ont le mot de passe répliqué.

| Stratégie de réplication de mot de passe avancée pourWINDOWSRODC  |                            |                      |                            |                  |  |  |  |  |  |
|---|----------------------------|----------------------|----------------------------|------------------|--|--|--|--|--|
| Utilisation de la stratégie   |                            | Stratégie résultante |                            |                  |  |  |  |  |  |
| Afficher les utilisateurs et ordinateurs qui répondent aux critères suivants :  |                            |                      |                            |                  |  |  |  |  |  |
| Comptes dont les mots de passe sont stockés sur ce contrôleur de domaine en lect...<br>Utilisateurs et ordinateurs : Objets récupérés : 6 |                            |                      |                            |                  |  |  |  |  |  |
| Nom   | Dossier Services de do...  | Type                 | Dernière modification d... | Le mot de pa...  |  |  |  |  |  |
| Alice Dupont  | afondlinux.org/Afondlin... | Utilisateur          | 13/05/2021 00:57:47        | 24/06/2021       |  |  |  |  |  |
| André Germain   | afondlinux.org/Afondlin... | Utilisateur          | Jamais modifié             | Expiré           |  |  |  |  |  |
| Christophe Henri  | afondlinux.org/Afondlin... | Utilisateur          | 12/05/2021 23:05:04        | 23/06/2021       |  |  |  |  |  |
| krbtgt_4909   | afondlinux.org/Users       | Utilisateur          | 12/05/2021 20:58:57        | 23/06/2021       |  |  |  |  |  |
| Philippe Martin   | afondlinux.org/Afondlin... | Utilisateur          | Jamais modifié             | Expiré           |  |  |  |  |  |
| WINDOWSRODC   | afondlinux.org/Domain...   | Ordinateur           | 12/05/2021 20:48:04        | N'expire jama... |  |  |  |  |  |

## X. Quelques commandes utiles

**echo %logonserver%** : Indique sur quel serveur l'utilisateur est authentifié.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19042.985]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\a.dupont echo %logonserver%
\\WINDOWSRODC
```

**nltest /sc\_query:afondlinux.org** : Indique le contrôleur de domaine le plus proche

```
C:\Users\a.dupont nltest /sc_query:afondlinux.org
Indicateurs : 30 HAS_IP HAS_TIMESERV
Nom du contrôleur de domaine approuvé \\WindowsRODC.afondlinux.org
Statut de la connexion du contrôleur de domaine approuvé Status = 0 0x0 NERR_Success
La commande a été correctement exécutée
```

**nltest /DSGETDC:afondlinux.org** : Indique le contrôleur de domaine utilisé

```
C:\Users\a.dupont nltest /DSGETDC:afondlinux.org
Contrôleur de domaine : \\WindowsRODC.afondlinux.org
Adresse : \\10.0.2.2
GUID dom : 719cdecc-58cf-4392-b9c4-9339e148843c
Nom dom : afondlinux.org
Nom de la forêt : afondlinux.org
Nom de site du contrôleur de domaine : SiteDistant
Nom de notre site : SiteDistant
Indicateurs : GC DS LDAP KDC TIMESERV DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE PARTIAL_SECRET
KEYLIST
La commande a été correctement exécutée
```

**nltest /DSGETDC:afondlinux.org /GC** : Pour trouver le contrôleur de domaine global utilisé

```
C:\Users\a.dupont nltest /DSGETDC:afondlinux.org /GC
Contrôleur de domaine : \\WindowsRODC.afondlinux.org
Adresse : \\10.0.2.2
GUID dom : 719cdecc-58cf-4392-b9c4-9339e148843c
Nom dom : afondlinux.org
Nom de la forêt : afondlinux.org
Nom de site du contrôleur de domaine : SiteDistant
Nom de notre site : SiteDistant
Indicateurs : GC DS LDAP KDC TIMESERV DNS_DC DNS_DOMAIN DNS_FOREST
KEYLIST
La commande a été correctement exécutée
```

## **dcdiag /test:replications** : Pour exécuter un test de réPLICATION

```
Administrator : C:\Windows\system32\cmd.exe
C:\Users\Administrateur dcdiag /test:replications
Diagnostic du serveur d'annuaire

Exécution de l'installation initiale :
Tentative de recherche de serveur associé...
Serveur associé : WindowsAD
* Forêt AD identifiée.
Collecte des informations initiales terminée.

Exécution des tests initiaux nécessaires

Test du serveur : SiteLocal\WINDOWSAD
Démarrage du test : Connectivity
..... Le test Connectivity
de WINDOWSAD a réussi

Exécution des tests principaux

Test du serveur : SiteLocal\WINDOWSAD
Démarrage du test : Replications
..... Le test Replications
de WINDOWSAD a réussi

Exécution de tests de partitions sur ForestDnsZones
Exécution de tests de partitions sur DomainDnsZones
Exécution de tests de partitions sur Schema
Exécution de tests de partitions sur Configuration
Exécution de tests de partitions sur afondlinux
Exécution de tests d'entreprise sur afondlinux.org
```

## **dcdiag /test :dns** : Pour exécuter un test DNS

```
Administrator : C:\Windows\system32\cmd.exe
Exécution de tests de partitions sur afondlinux
Exécution de tests d'entreprise sur afondlinux.org
C:\Users\Administrateur dcdiag /test:dns
Diagnostic du serveur d'annuaire

Exécution de l'installation initiale :
Tentative de recherche de serveur associé...
Serveur associé : WindowsAD
* Forêt AD identifiée.
Collecte des informations initiales terminée.

Exécution des tests initiaux nécessaires

Test du serveur : SiteLocal\WINDOWSAD
Démarrage du test : Connectivity
..... Le test Connectivity
de WINDOWSAD a réussi

Exécution des tests principaux

Test du serveur : SiteLocal\WINDOWSAD
Démarrage du test : DNS
Les tests DNS sont en cours d'exécution et ne sont pas arrêtés.
..... Le test DNS
de WINDOWSAD a réussi

Exécution de tests de partitions sur ForestDnsZones
Exécution de tests de partitions sur DomainDnsZones
Exécution de tests de partitions sur Schema
Exécution de tests de partitions sur Configuration
Exécution de tests de partitions sur afondlinux
Exécution de tests d'entreprise sur afondlinux.org
Démarrage du test : DNS
..... Le test DNS
de afondlinux.org a réussi
```

REPADMIN est un outil dédié au diagnostic des problèmes de réPLICATIONS entre les contrôleurS de domaine.

**repadmin /replsummary** : déclenche une collecte de données afin d'afficher un résumé de la réPLICATION au niveau de la forêt

```
Administrator : C:\Windows\system32\cmd.exe
    de afondlinux.org a réussi

C:\Users\Administrateur repadmin /replsummary
Heure de début du résumé de la réPLICATION : 2021-05-16 13:49:01

Début de la collecte des données pour le résumé de la réPLICATION ;
cette opération peut prendre un certain temps :
    .....

DSA source      différence max      nb échecs %%   erreur
WINDOWSAD        01m:27s       0 /     5     0

DSA de destination      différence max      nb échecs %%   erreur
WINDOWSRODC        01m:27s       0 /     5     0
```

**repadmin /showrepl** : permet d'afficher l'état de la réPLICATION lorsque le contrôleur de domaine a tenté une réPLICATION entrante pour la dernière fois

```
PS C:\Users\Administrateur.AFONDLINUX> repadmin /showrepl
Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
SiteDistant\WINDOWSRODC
Options DSA : IS_GC DISABLE_OUTBOUND_REPL IS_RODC
Options de site : (none)
GUID de l'objet DSA : 1de395ed-6214-43be-8bd0-a98f5e0ee251
ID de l'invocation DSA : 8dc1d1b7-862d-4d3a-99c8-ab0c1543a9cd

==== INSTANCES VOISINES ENTRANTES =====
DC=afondlinux,DC=org
    SiteLocal\WINDOWSAD via RPC
        GUID de l'objet DSA : 010c2433-2872-4fcf-bfd3-472aba471bc9
        La dernière tentative, le 2021-05-16 13:47:34, a réussi.

CN=Configuration,DC=afondlinux,DC=org
    SiteLocal\WINDOWSAD via RPC
        GUID de l'objet DSA : 010c2433-2872-4fcf-bfd3-472aba471bc9
        La dernière tentative, le 2021-05-16 13:47:34, a réussi.

CN=Schema,CN=Configuration,DC=afondlinux,DC=org
    SiteLocal\WINDOWSAD via RPC
        GUID de l'objet DSA : 010c2433-2872-4fcf-bfd3-472aba471bc9
        La dernière tentative, le 2021-05-16 13:47:34, a réussi.

DC=DomainDnsZones,DC=afondlinux,DC=org
    SiteLocal\WINDOWSAD via RPC
        GUID de l'objet DSA : 010c2433-2872-4fcf-bfd3-472aba471bc9
        La dernière tentative, le 2021-05-16 13:47:34, a réussi.

DC=ForestDnsZones,DC=afondlinux,DC=org
    SiteLocal\WINDOWSAD via RPC
        GUID de l'objet DSA : 010c2433-2872-4fcf-bfd3-472aba471bc9
        La dernière tentative, le 2021-05-16 13:47:34, a réussi.
```