

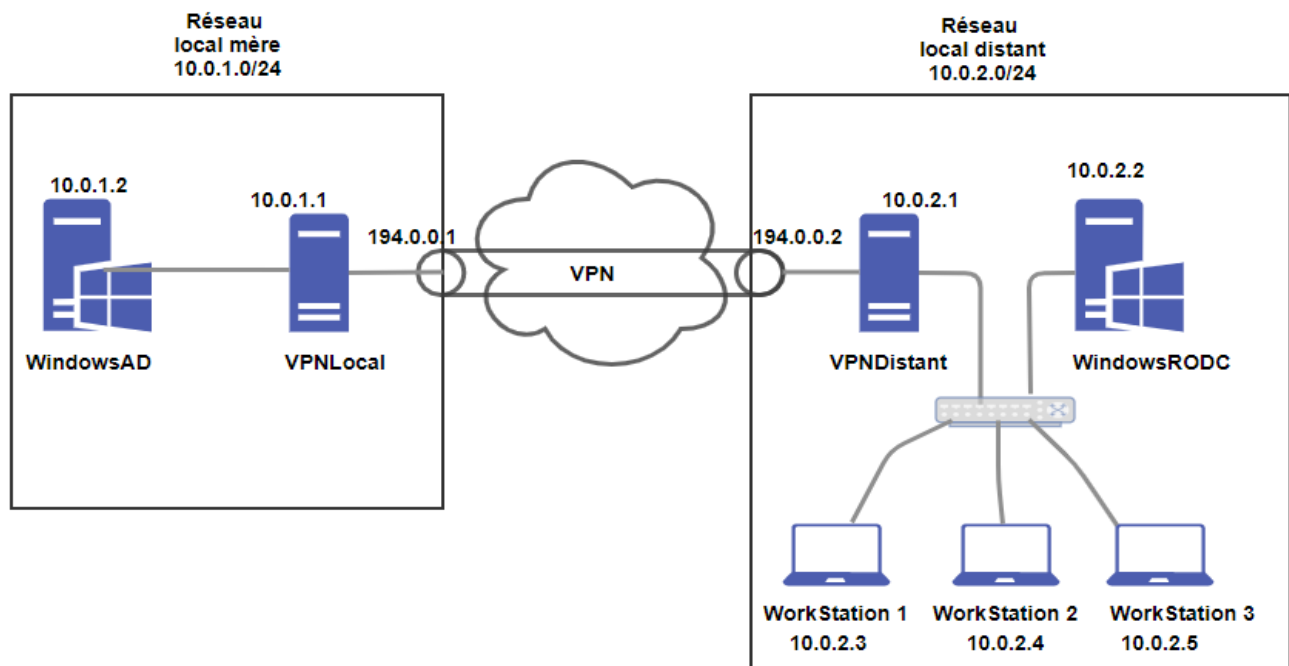
# Documentation du projet 5

Procédure rédigée par : CHERIF Ahmed

## Table des matières

I -Schéma réseau de l'architecture du réseau :.....	2
II -Installation et configuration de l'infrastructure:.....	3
II.1 – Configuration du VPNLocal :.....	3
II.2 -Configuration du VPNDistant: .....	5
II.3 -Configuration de WindowsAD: .....	6
II.4 -Configuration du WindowsRODC: .....	6
II.2 -Configuration d'une VM windows:.....	7
III -Installation et configuration de openvpn dans VPNLocal et VPNDistant :.....	7
III.1 - VPNLocal :.....	7
III.2 -VPNDistant : .....	13
III.4 – Tester le fonctionnement du VPN :.....	14
IV -Installation et configuration du AD: .....	16
IV.1 -Installation et configuration du contrôleur du domaine DC:.....	16
IV.2 -Installation et configuration d'un RODC: .....	21
V -Utilisation de l'AD :.....	26
V.1 – Créer des comptes AD:.....	26
V.2 - Accéder à un utilisateur AD à partir d'un poste client pour la première fois: .....	26
V.3 -Création des GPO: .....	28
V.4 -Réduire le trafic pendant les horaires de bureau:.....	40
V.5 - Vérifiez que lorsque la liaison VPN est coupée, les utilisateurs peuvent s'authentifier sur le Domaine mais pas changer leur mot de passe.: .....	42

## I-\ Schéma réseau de l'architecture du projet



## II-\ Installation et configuration de l'infrastructure :

### 1-\ Configuration de VPNLocal

#### La configuration des adresses réseaux

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

# The loopback network interface
auto lo
iface lo inet loopback

# interface externe
auto ens33
iface ens33 inet static
    address 194.0.0.1
    netmask 255.255.255.0

# interface interne
auto ens34
iface ens34 inet static
    address 10.0.1.1
    netmask 255.255.255.0

# on place la route vers 10.0.2.0 statique
up ip route add 10.0.2.0/24 via 194.0.0.2 dev ens33

# interface bridge se connecter en ssh
auto ens38
iface ens38 inet static
    address 192.168.0.30
    netmask 255.255.255.0
    gateway 192.168.0.1
```

### **Activer le routage et le rendre permanent:**

```
nano /etc/sysctl.conf
```

Eliminer # dans cette ligne :

```
net.ipv4.ip_forward=1
```

### **Redémarrer le service :**

```
sudo systemctl restart procps
```

### **Activer le nat entre les cartes (eth0 ==> carte externe)**

```
iptables -A POSTROUTING -t nat -o ens33 -j MASQUERADE
```

### **Installer iptables-persistent pour rendre les changements d'iptables persistants**

```
apt-get install iptables-persistent
```

### **Sauvegarder de façon permanente les règles**

```
iptables-save > /etc/iptables/rules.v4
```

### **Afficher le contenu de fichier rulesv4 de iptables**

```
cat /etc/iptables/rules.v4
```

### **Placer une route statique vers 10.0.2.0**

```
nano /etc/network/interfaces
```

```
up ip route add 10.0.2.0/24 via 194.0.0.2 dev ens33
```

### **Afficher les routes disponibles:**

```
ip route
```

## 2-\ Configuration de VPNDistant

La même configuration que VPNLocal avec quelques modifications dans l'adressage

### La configuration des adresses réseaux

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

# The loopback network interface
auto lo
iface lo inet loopback

# interface externe
auto ens33
iface ens33 inet static
    address 194.0.0.2
    netmask 255.255.255.0

auto ens34
iface ens34 inet static
    address 10.0.2.1
    netmask 255.255.255.0

# on place la route statique vers 10.0.1.0
up ip route add 10.0.1.0/24 via 194.0.0.1 dev ens33

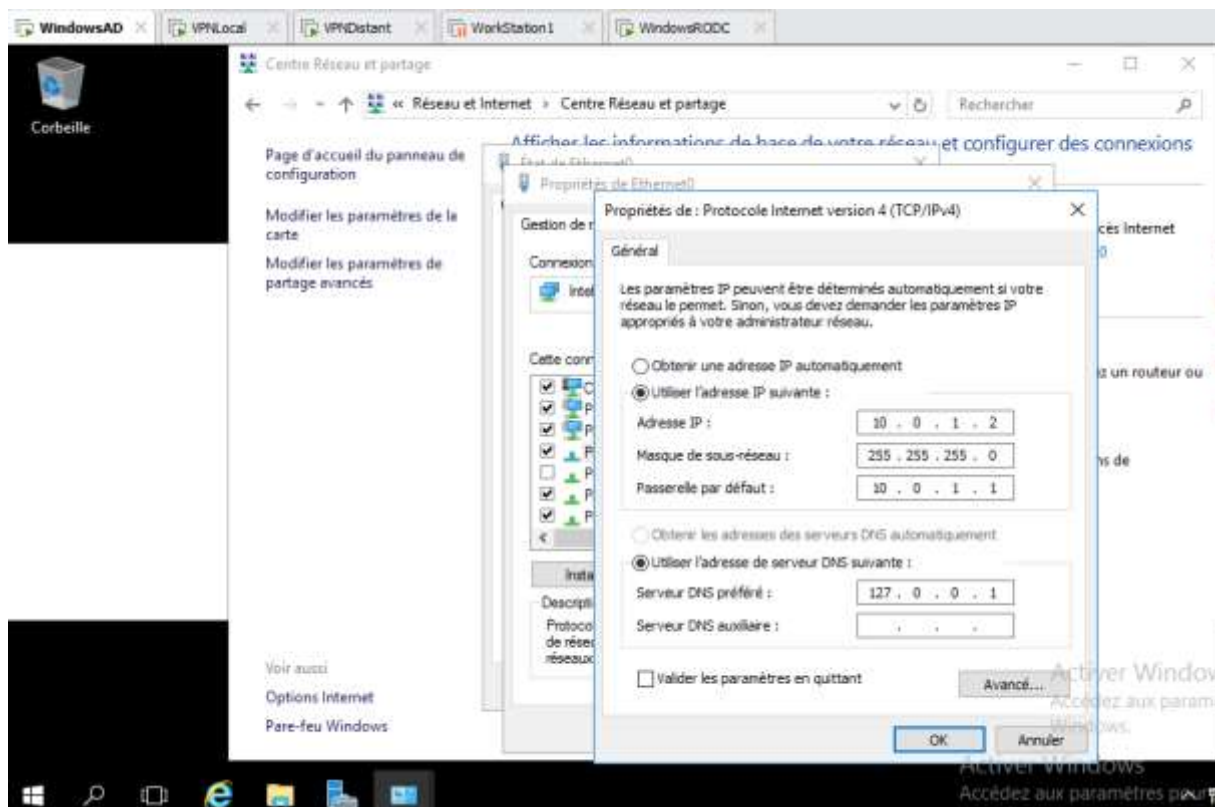
auto ens38
iface ens38 inet static
    address 192.168.0.40
    netmask 255.255.255.0
    gateway 192.168.0.1
```

### Placer une route statique vers 10.0.1.0

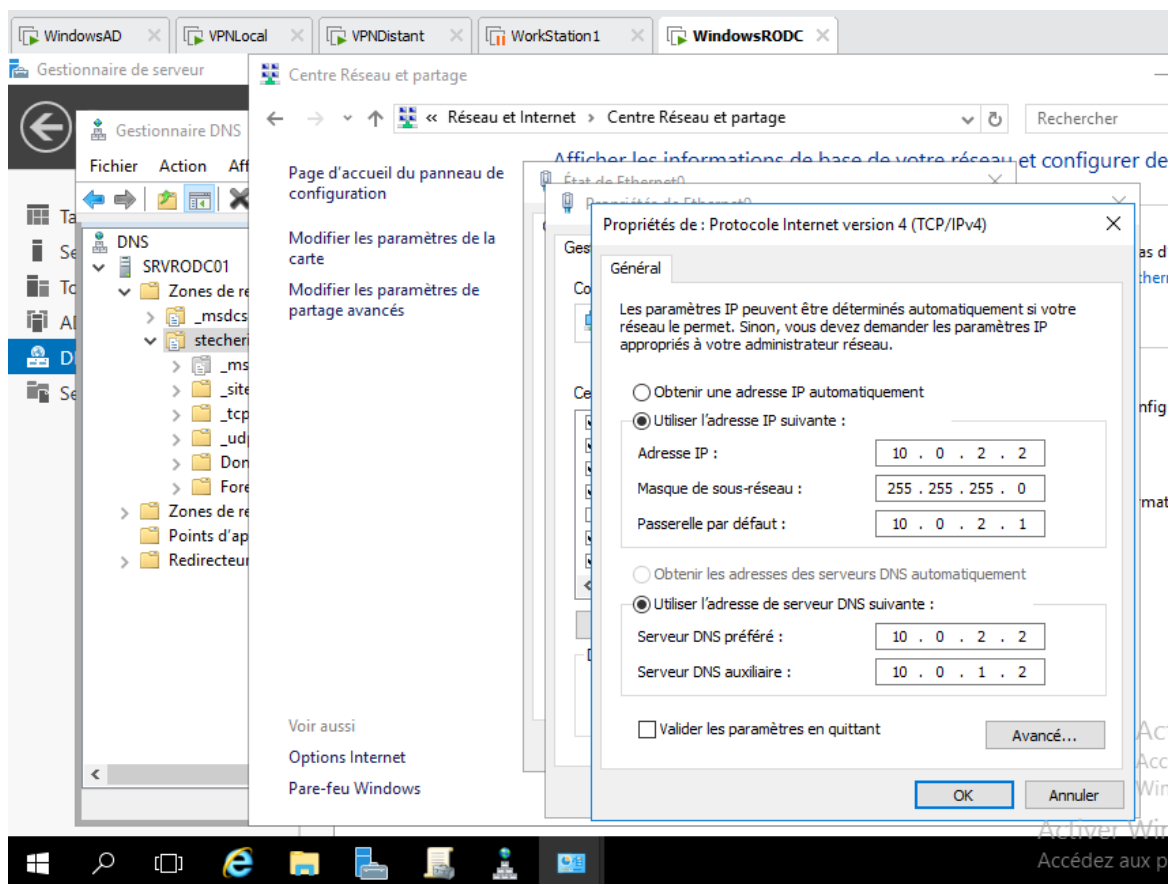
```
nano /etc/network/interfaces

up ip route add 10.0.1.0/24 via 194.0.0.1 dev ens33
```

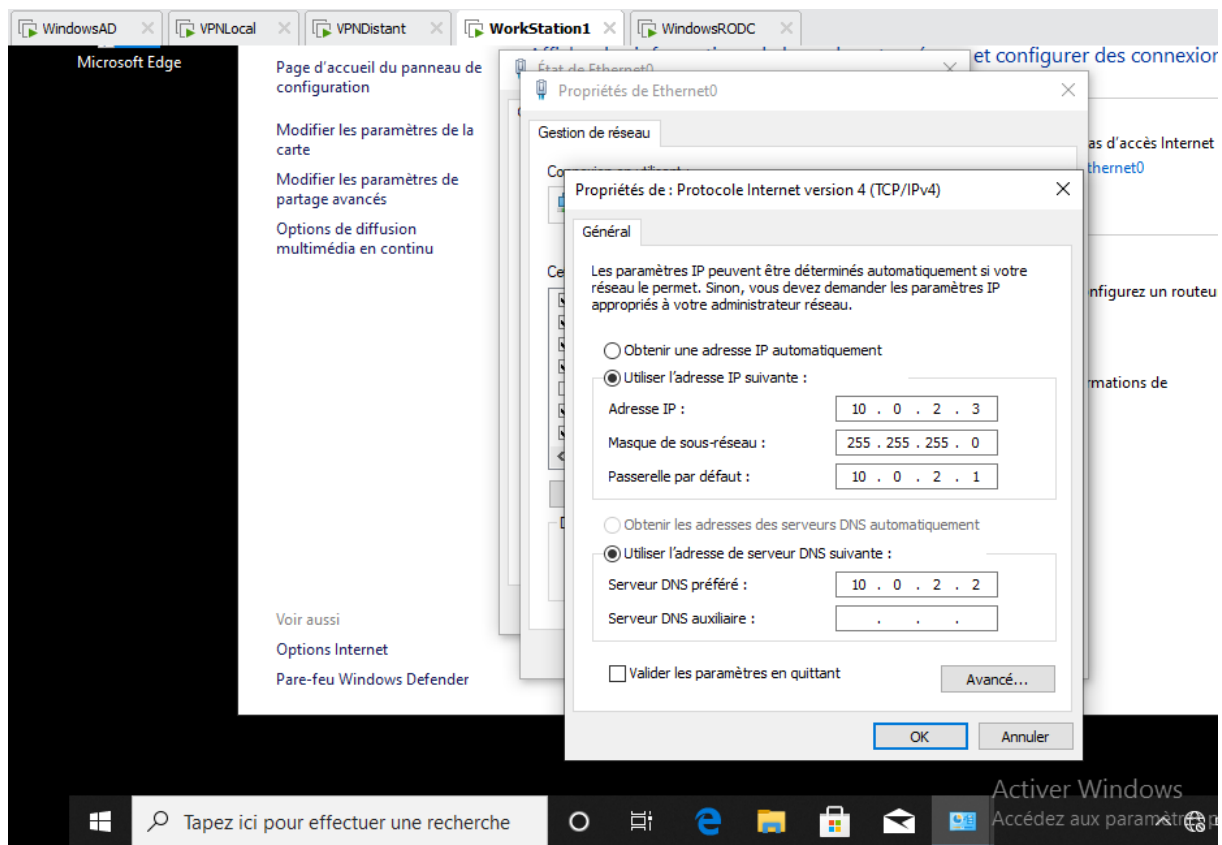
### 3- Configuration de WindowsAD



### 4- Configuration de WindowsRODC



## 5-\ Configuration d'une VM Windows (WorkStation1)



## III-\ Installation et configuration de openvpn dans VPNLocal et VPNDistant :

### 1-\ VPNLocal:

```
apt-get install openvpn
```

```
root@VPNLocal:~# ls /etc/openvpn/  
client scripts server update-resolv-conf  
root@VPNLocal:~# ls /usr/share/easy-rsa/  
easyrsa openssl-easyrsa.cnf pki vars vars.example x509-types
```

Créer le fichier vars a partir vars.example

```
cp /usr/share/easy-rsa/vars.example /usr/share/easy-rsa/vars
```

Configurer ce fichier :

```
nano /usr/share/easy-rsa/vars
```

```
set_var EASYRSA "${0%/*}"
set_var EASYRSA_PKI      "$PWD/pki"
set_var EASYRSA_DN      "cn_only"
set_var EASYRSA_REQ_COUNTRY  "FR"
set_var EASYRSA_REQ_PROVINCE "Ile de france"
set_var EASYRSA_REQ_CITY    "Paris"
set_var EASYRSA_REQ_ORG     "Copyleft Certificate Co"
set_var EASYRSA_REQ_EMAIL   "ahmedcherif3232@gmail.com"
set_var EASYRSA_REQ_OU      "infra"
set_var EASYRSA_KEY_SIZE    2048
set_var EASYRSA_ALGO        rsa
set_var EASYRSA_CA_EXPIRE   3650
set_var EASYRSA_CERT_EXPIRE 1080
set_var EASYRSA_NS_SUPPORT  "no"
set_var EASYRSA_EXT_DIR "$EASYRSA/x509-types"
set_var EASYRSA_SSL_CONF    "$EASYRSA/openssl-easyrsa.cnf"
set_var EASYRSA_DIGEST      "sha256"
```

Changer la permission de ce fichier

```
chmod +x vars
```

## PKI (Public key Infrastructure)

- **Mettre en place du pki**

```
root@host:~# /usr/share/easy-rsa/easyrsa clean-all
```

```
root@host:~# /usr/share/easy-rsa/easyrsa init-pki
```



- Entrer yes pour démarrer l'initialisation :

```
Type the word 'yes' to continue, or any other input to
abort.
```

```
Confirm removal: yes
```

- Créer un certificate authority dans /etc/openvpn/pki/ca.crt

```
root@host:~# /usr/share/easy-rsa/easyrsa build-ca nopass
```

- Ne pas tenir compte du message concernant le random number generator :

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Common Name (eg: your user, host, or server name) [Easy-RSA
CA]: openvpn-host
```

```
CA creation complete and you may now import and sign cert
requests.
```

```
Your new CA certificate file for publishing is at:
/etc/openvpn/pki/ca.crt
```

## Certificats Serveur

- Créer le certificat et la clé privé pour le serveur

```
root@host:~# /usr/share/easy-rsa/easyrsa build-server-full vpn
server2 nopass
```

## Générer des paramètres Diffie Hellman dans /etc/openvpn/pki/dh.pem

```
root@host:~# /usr/share/easy-rsa/easyrsa gen-dh
```

## Certificats Client

- Créer un certificat client01 :

```
root@host:~# /usr/share/easy-rsa/easyrsa build-client-full client01 nopass
```

## Déplacer les clés et les certificats dans le repertoire /etc/openssl/server/

```
root@VPNLocal:/etc/openssl/server# cp /usr/share/easy-rsa/pki/private/ca.key /etc/openssl/server/
root@VPNLocal:/etc/openssl/server# cp /usr/share/easy-rsa/pki/private/vpnserver2.key /etc/openssl/server/
root@VPNLocal:/etc/openssl/server# cp /usr/share/easy-rsa/pki/issued/vpnserver2.crt /etc/openssl/server/
root@VPNLocal:/etc/openssl/server# ls /etc/openssl/server/
ca.crt  ca.key  vpnserver2.crt  vpnserver2.key
root@VPNLocal:/etc/openssl/server# ls
ca.crt  ca.key  vpnserver2.crt  vpnserver2.key
root@VPNLocal:/etc/openssl/server# cp /usr/share/easy-rsa/pki/issued/vpnserver2.crt /etc/openssl/server/
root@VPNLocal:/etc/openssl/server#
root@VPNLocal:/etc/openssl/server# cp /usr/share/easy-rsa/pki/dh.pem /etc/openssl/server/
root@VPNLocal:/etc/openssl/server# ls
ca.crt  ca.key  dh.pem  vpnserver2.crt  vpnserver2.key
```

Créer le répertoire temporaire /srv/openssl/tmp ==> indispensable au démarrage du serveur (voir les logs)

```
mkdir /srv/openssl/tmp
```

S'assurer que les fichiers de log seront accessibles

```
touch /var/log/openssl-status.log
touch /var/log/openssl.log
chmod 777 /var/log/openssl-status.log
chmod 777 /var/log/openssl.log
```

Créer le fichier de configuration /etc/openssl/server.conf (voir "man openssl" pour les infos)

# On crée le fichier "server.conf"

```
nano /etc/openssl/server/server.conf
```

```
GNU nano 3.2 /etc/openvpn/server/server.conf
# Serveur
proto udp
port 1194
dev tun
#
# Clés et certificats
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/vpnserver2.crt
key /etc/openvpn/server/vpnserver2.key
dh /etc/openvpn/server/dh.pem
#tls-auth /etc/openvpn/server/ca.key 0
#cipher AES-256-CBC
#
# Réseau
server 10.0.1.0 255.255.255.0 # Réseau interne
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
#
# Sécurité
user nobody
group nogroup
chroot /srv/openvpn
persist-key
persist-tun
comp-lzo
#
# Log
verb 3
mute 20
status /var/log/openvpn-status.log
log-append /var/log/openvpn.log
```

```
# Serveur
proto udp
port 1194
dev tun
#
# Clés et certificats
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/vpnserver2.crt
key /etc/openvpn/server/vpnserver2.key
dh /etc/openvpn/server/dh.pem
#tls-auth /etc/openvpn/server/ca.key 0
#cipher AES-256-CBC
#
# Réseau
server 10.0.1.0 255.255.255.0 # Réseau interne
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
#
# Sécurité
user nobody
```

```
group nogroup
chroot /srv/openvpn
persist-key
persist-tun
comp-lzo
#
# Log
verb 3
mute 20
status /var/log/openvpn-status.log
log-append /var/log/openvpn.log
```

## Déplacer les clés et les certificats dans le repertoire /etc/openvpn/client/

```
root@VPNLocal:~# cp /usr/share/easy-rsa/pki/private/client01.key /etc/openvpn/client/
root@VPNLocal:~# cp /usr/share/easy-rsa/pki/issued/client01.crt /etc/openvpn/client/
root@VPNLocal:~# systemctl restart openvpn.service
root@VPNLocal:~# systemctl status openvpn.service
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sun 2021-08-01 16:00:20 CEST; 11s ago
     Process: 1497 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 1497 (code=exited, status=0/SUCCESS)

août 01 16:00:20 VPNLocal systemd[1]: Starting OpenVPN service...
août 01 16:00:20 VPNLocal systemd[1]: Started OpenVPN service.
root@VPNLocal:~# cp /usr/share/easy-rsa/pki/ca.crt /etc/openvpn/client/
root@VPNLocal:~# ls /etc/openvpn/client/
ca.crt  client01.crt  client01.key
root@VPNLocal:~# nano /etc/openvpn/client/client.conf
```

Créer le fichier client.conf

```
GNU nano 3.2 /etc/openvpn/client/client01.conf

client
dev tun
proto udp
# adresse ip serveur
remote 194.0.0.1 1194
resolv-retry infinite

#
# Clés
ca /etc/openvpn/client/ca.crt
cert /etc/openvpn/client/client01.crt
key /etc/openvpn/client/client01.key

#
# Sécurité
nobind
persist-key
persist-tun
comp-lzo
verb 3
```

client

```
dev tun
proto udp
# adresse ip serveur
remote 194.0.0.1 1194
resolv-retry infinite
#
# Clés
ca /etc/openvpn/client/ca.crt
cert /etc/openvpn/client/client01.crt
key /etc/openvpn/client/client01.key
#
# Sécurité
nobind
persist-key
persist-tun
comp-lzo
verb 3
```

- **Se déplacer dans le dossier `/etc/openvpn/` :**

```
root@host:~# cd /etc/openvpn/
```

- **Activer OpenVPN au démarrage :**

```
root@host:~# sed -i 's/#AUTOSTART="all"/AUTOSTART="all"/' /etc
/default/openvpn
```

- **Activer le service OpenVPN :**

```
root@host:~# systemctl enable openvpn@.service
```

- **Redémarrer le service OpenVPN :**

```
root@host:~# systemctl restart openvpn.service
```

## 2- \ VPN Distant:

```
apt-get install openvpn
```

## Revenir au VPNLocal et envoyer les certificats et la cle et le fichier de configuration vers VPNDistant

```
root@VPNLocal:/etc/openvpn/client# scp /etc/openvpn/client/* root@192.168.0.40:/etc/openvpn/client/
```

```
root@VPNLocal:/etc/openvpn/client# scp /etc/openvpn/client/* root@192.168.0.40:/etc/openvpn/client/
root@192.168.0.40's password:
ca.crt                                100% 1208      2.2MB/s   00:00
ca.key                                100% 1675      2.3MB/s   00:00
clien01.conf                          100% 351       710.5KB/s 00:00
client01.crt                          100% 4500      7.1MB/s   00:00
client01.key                          100% 1708      3.7MB/s   00:00
```

### 3- Tester le fonctionnement du VPN

#### Coté VPNLocal:

```
root@VPNLocal:~# openvpn --config /etc/openvpn/server/server.conf
```

```
root@VPNLocal:~# openvpn --config /etc/openvpn/server/server.conf
```

#### Coté VPNDistant

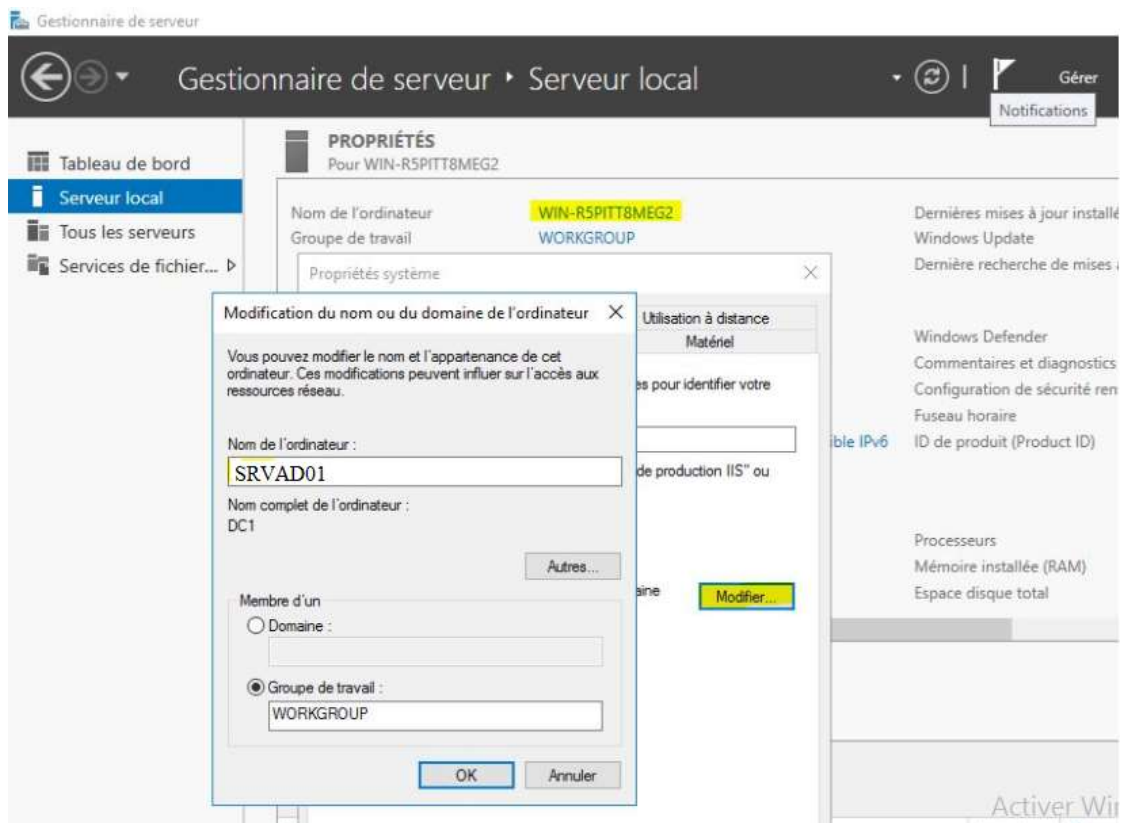
```
root@VPNDistant:/etc/openvpn/client# openvpn --config /etc/openvpn/client/clien01.conf
```

```
root@VPNDistant:/etc/openvpn/client# openvpn --config /etc/openvpn/client/clien01.conf
Sun Aug  1 23:42:25 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
[EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 28 2021
Sun Aug  1 23:42:25 2021 library versions: OpenSSL 1.1.1d 10 Sep 2019, LZO 2.10
Sun Aug  1 23:42:25 2021 WARNING: No server certificate verification method has been en
abled. See http://openvpn.net/howto.html#mitm for more info.
Sun Aug  1 23:42:25 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]194
.0.0.1:1194
Sun Aug  1 23:42:25 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Sun Aug  1 23:42:25 2021 UDP link local: (not bound)
Sun Aug  1 23:42:25 2021 UDP link remote: [AF_INET]194.0.0.1:1194
Sun Aug  1 23:42:25 2021 TLS: Initial packet from [AF_INET]194.0.0.1:1194, sid=7bd217b1
441302f6
```

```
Mon Aug  2 13:13:59 2021 VERIFY OK: depth=1, CN=openvpn-host
Mon Aug  2 13:13:59 2021 VERIFY OK: depth=0, CN=vpnsrvr2
Mon Aug  2 13:13:59 2021 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
Mon Aug  2 13:13:59 2021 [vpnsrvr2] Peer Connection Initiated with [AF_INET]194.0.0.1:1194
Mon Aug  2 13:14:00 2021 SENT CONTROL [vpnsrvr2]: 'PUSH_REQUEST' (status=1)
Mon Aug  2 13:14:00 2021 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,route 10.0.1.1,topology net30,ping 10,ping-restart 120,ifconfig 10.0.1.6 10.0.1.5,peer-id 0,cipher AES-256-GCM'
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: timers and/or timeouts modified
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: --ifconfig/up options modified
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: route options modified
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: peer-id set
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: adjusting link_mtu to 1625
Mon Aug  2 13:14:00 2021 OPTIONS IMPORT: data channel crypto options modified
Mon Aug  2 13:14:00 2021 Data Channel: using negotiated cipher 'AES-256-GCM'
Mon Aug  2 13:14:00 2021 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Mon Aug  2 13:14:00 2021 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Mon Aug  2 13:14:00 2021 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=ens38 HWADDR=00:0c:29:b6:8d:83
Mon Aug  2 13:14:00 2021 TUN/TAP device tun0 opened
Mon Aug  2 13:14:00 2021 TUN/TAP TX queue length set to 100
Mon Aug  2 13:14:00 2021 /sbin/ip link set dev tun0 up mtu 1500
Mon Aug  2 13:14:00 2021 /sbin/ip addr add dev tun0 local 10.0.1.6 peer 10.0.1.5
Mon Aug  2 13:14:00 2021 /sbin/ip route add 194.0.0.1/32 via 192.168.0.1
Mon Aug  2 13:14:00 2021 /sbin/ip route add 0.0.0.0/1 via 10.0.1.5
Mon Aug  2 13:14:00 2021 /sbin/ip route add 128.0.0.0/1 via 10.0.1.5
Mon Aug  2 13:14:00 2021 /sbin/ip route add 10.0.1.1/32 via 10.0.1.5
Mon Aug  2 13:14:00 2021 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Mon Aug  2 13:14:00 2021 Initialization Sequence Completed
```

## IV-\ Installation et configuration du AD

### 1-\ Installation et configuration d'un contrôleur de domaine (DC)



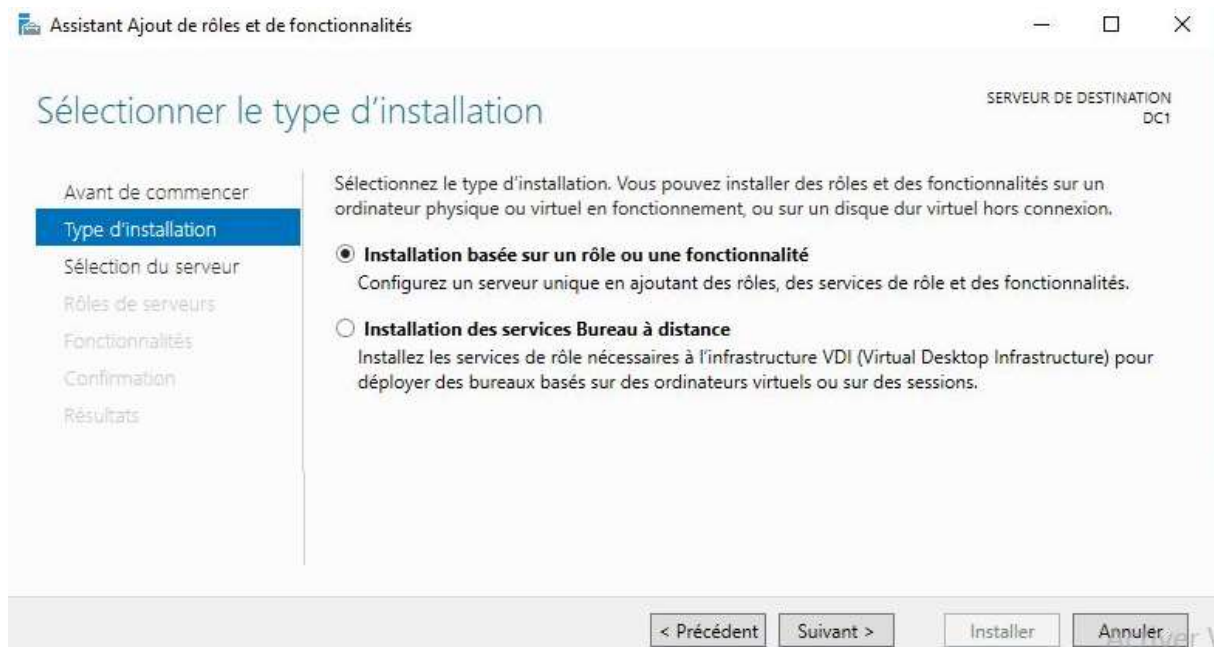
### REDÉMARRER

A partir du Gestionnaire de serveur, cliquer sur « **Gérer** » puis « **Ajouter des rôles et fonctionnalités** »

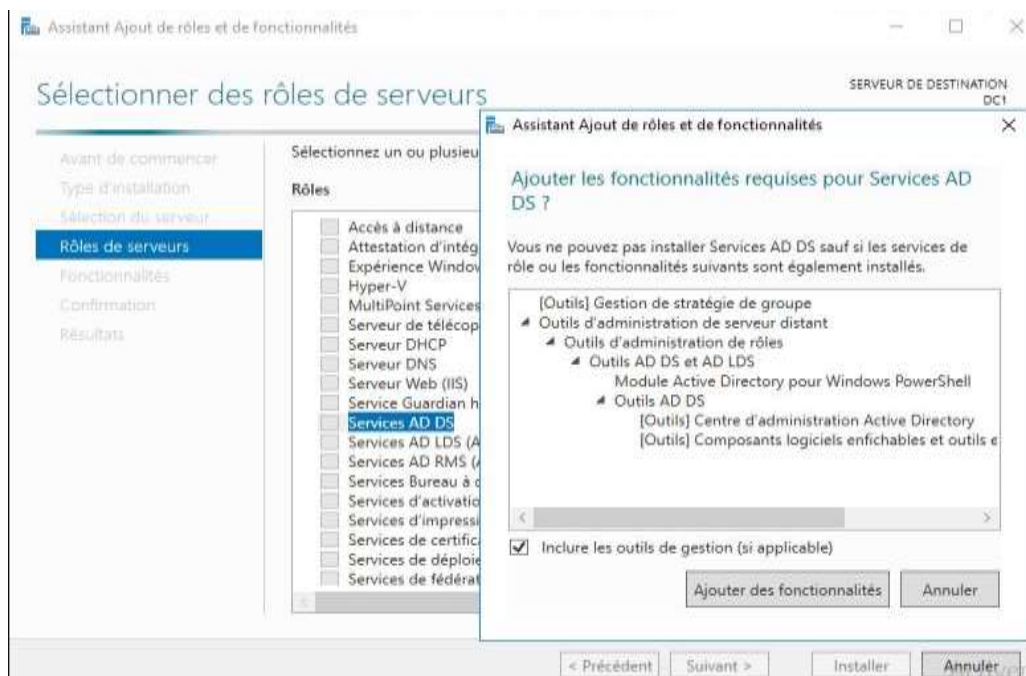


Cliquer sur « **Installation basée sur un rôle ou une fonctionnalité** »

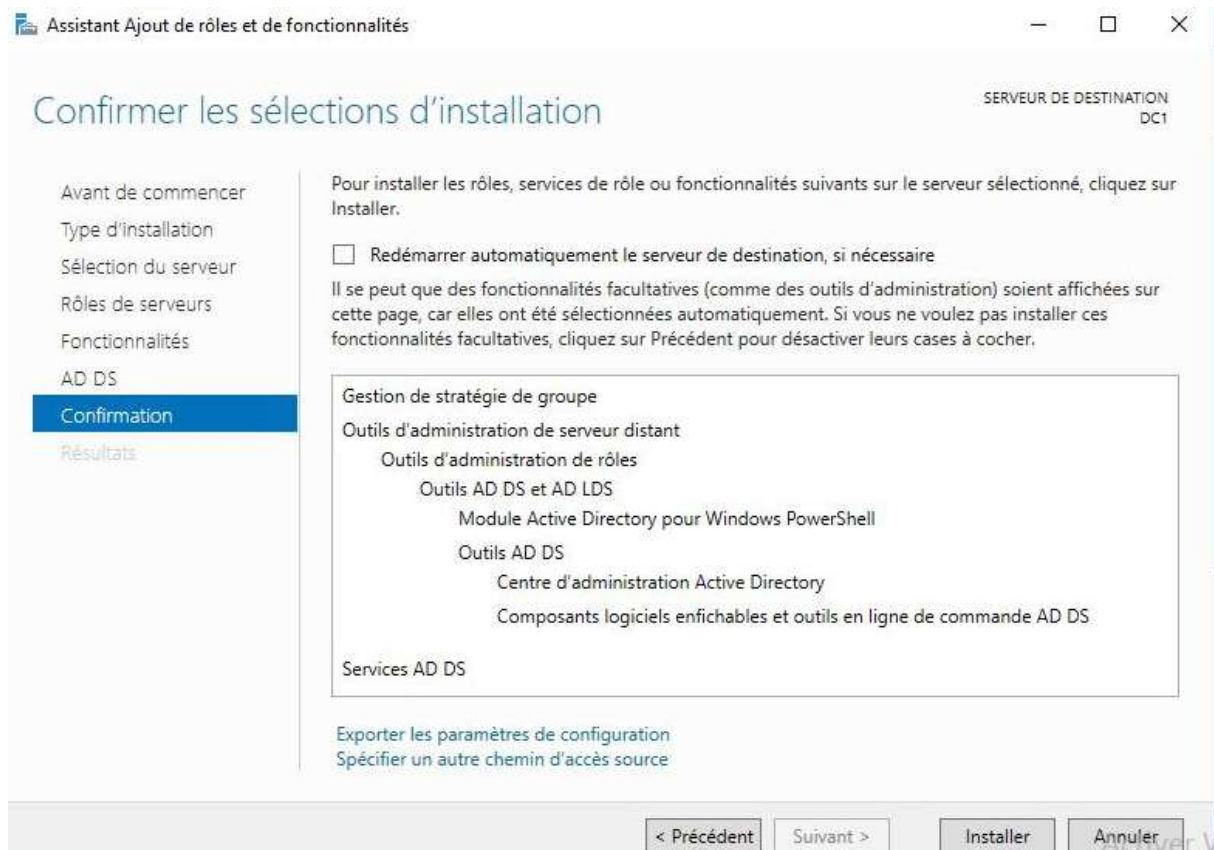




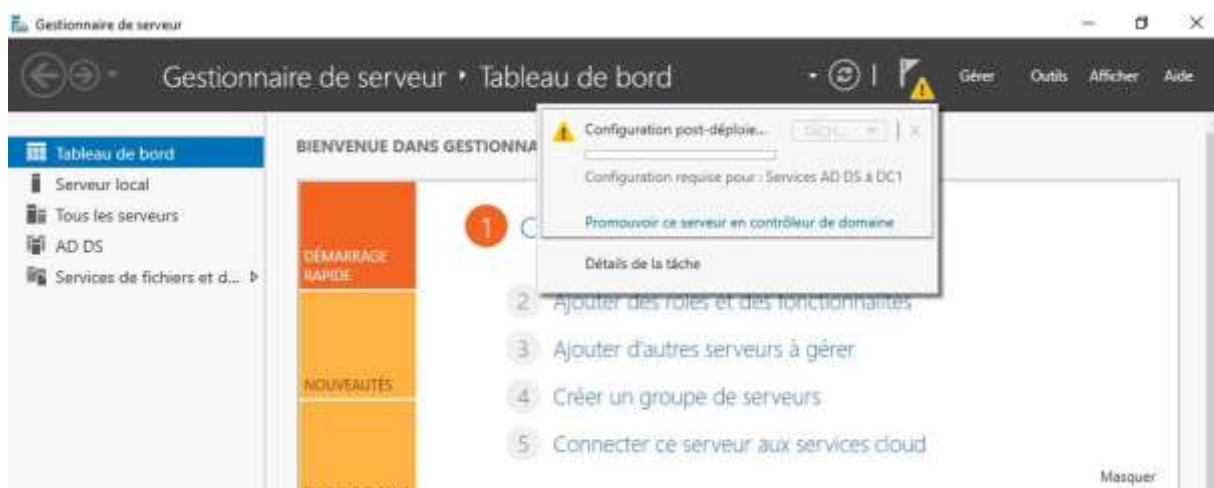
Choisir d'installer « **Services AD DS** » qui requiert également l'installation de plusieurs outils d'administration de ce rôle. Cliquer sur « **Ajouter des fonctionnalités** » puis sur « **Suivant** ».



Cliquer encore suivant, puis cliquez sur le bouton « **Installer** » pour exécuter l'installation après avoir vérifié le résumé. Puis cliquer « **Fermer** » a la fin. Puis Redémarrer le Serveur.



Cliquer sur l'icône du drapeau puis sur « **Promouvoir ce serveur en contrôleur de domaine** »



Sélectionner :

- Ajouter un contrôleur de domaine à un domaine existant (créer un contrôleur supplémentaire)
- Ajouter un nouveau domaine à un forêt existant (créer un domaine enfant associé à un domaine parent dans une même forêt)

- Ajouter un nouveau foret (aucune foret et domaine n'existe)

Donner un NOM au Domaine (Exemple : STECHERIF.local)

Assistant Configuration des services de domaine Active Directory

## Configuration de déploiement

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

☐ Ajouter un contrôleur de domaine à un domaine existant  
☐ Ajouter un nouveau domaine à une forêt existante  
☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

[En savoir plus sur la configurations de déploiement](#)

Nom NETBIOS pour le domaine (Exemple : STECHERIF)

Assistant Configuration des services de domaine Active Directory

## Options supplémentaires

Configuration de déploie...

Options du contrôleur de...

Options DNS

**Options supplémentaires**

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

SERVEUR C

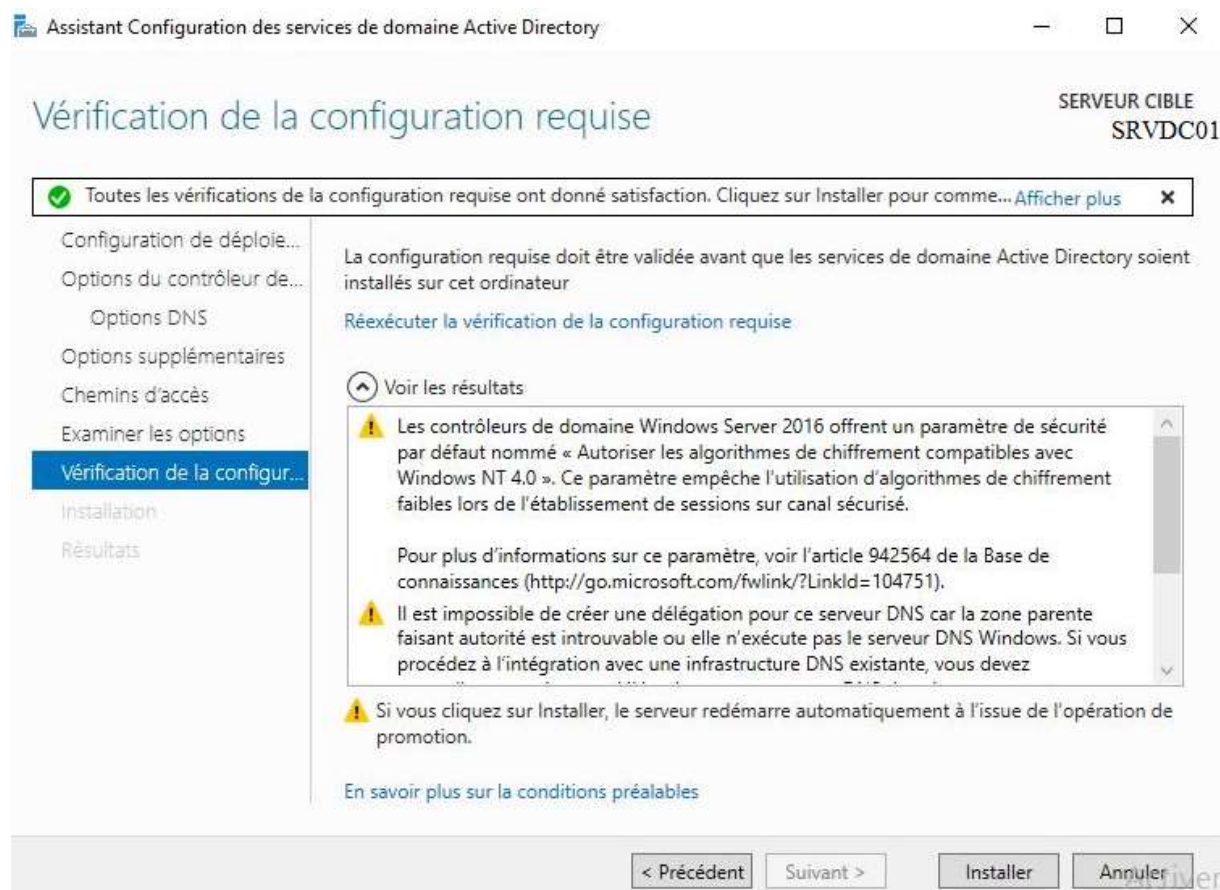
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

[En savoir plus sur la options supplémentaires](#)

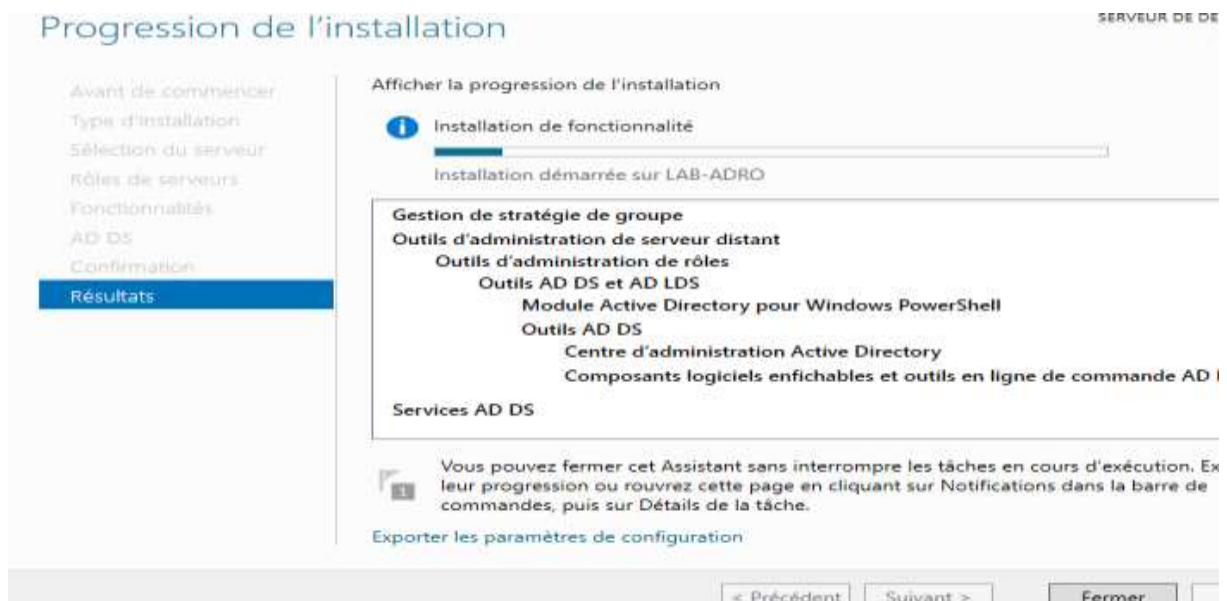
Les vérifications avant configuration montrent que la configuration requise a donné satisfaction.

Il suffit de lancer l'installation et d'attendre la fin de l'exécution.

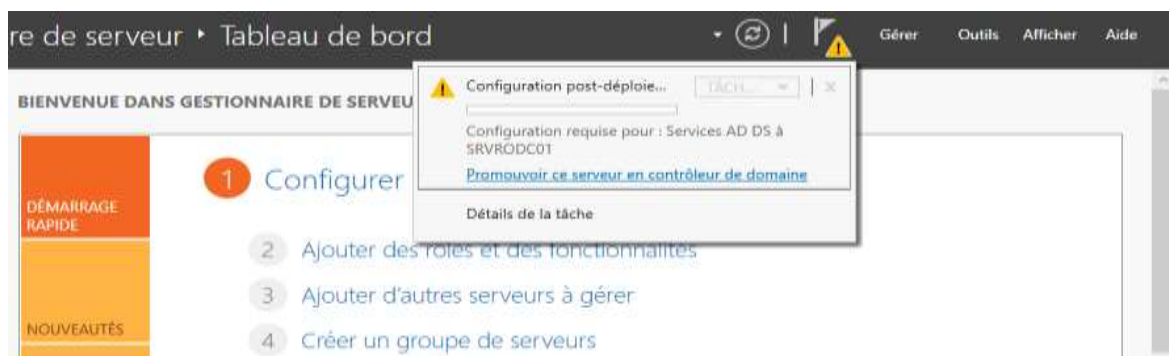


## 2-\ Installation et configuration d'un RODC

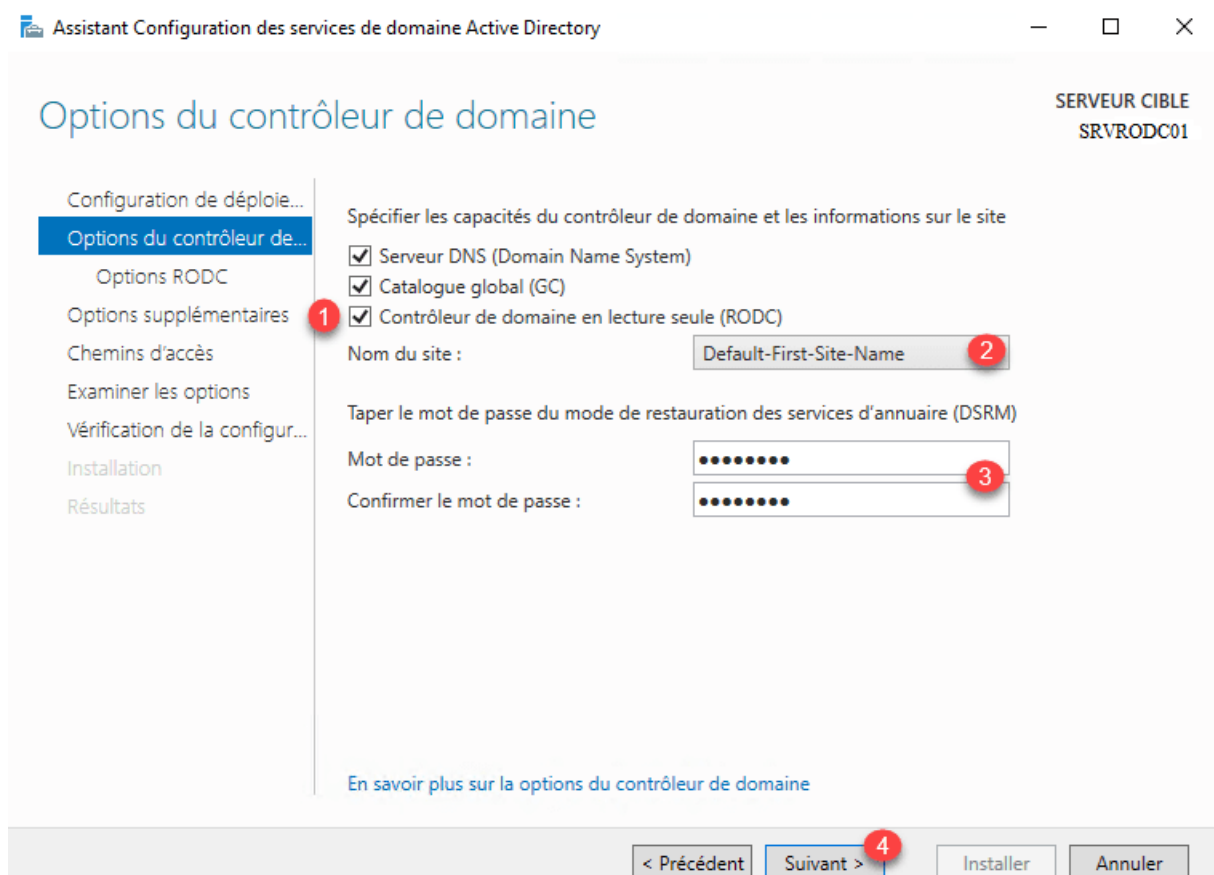
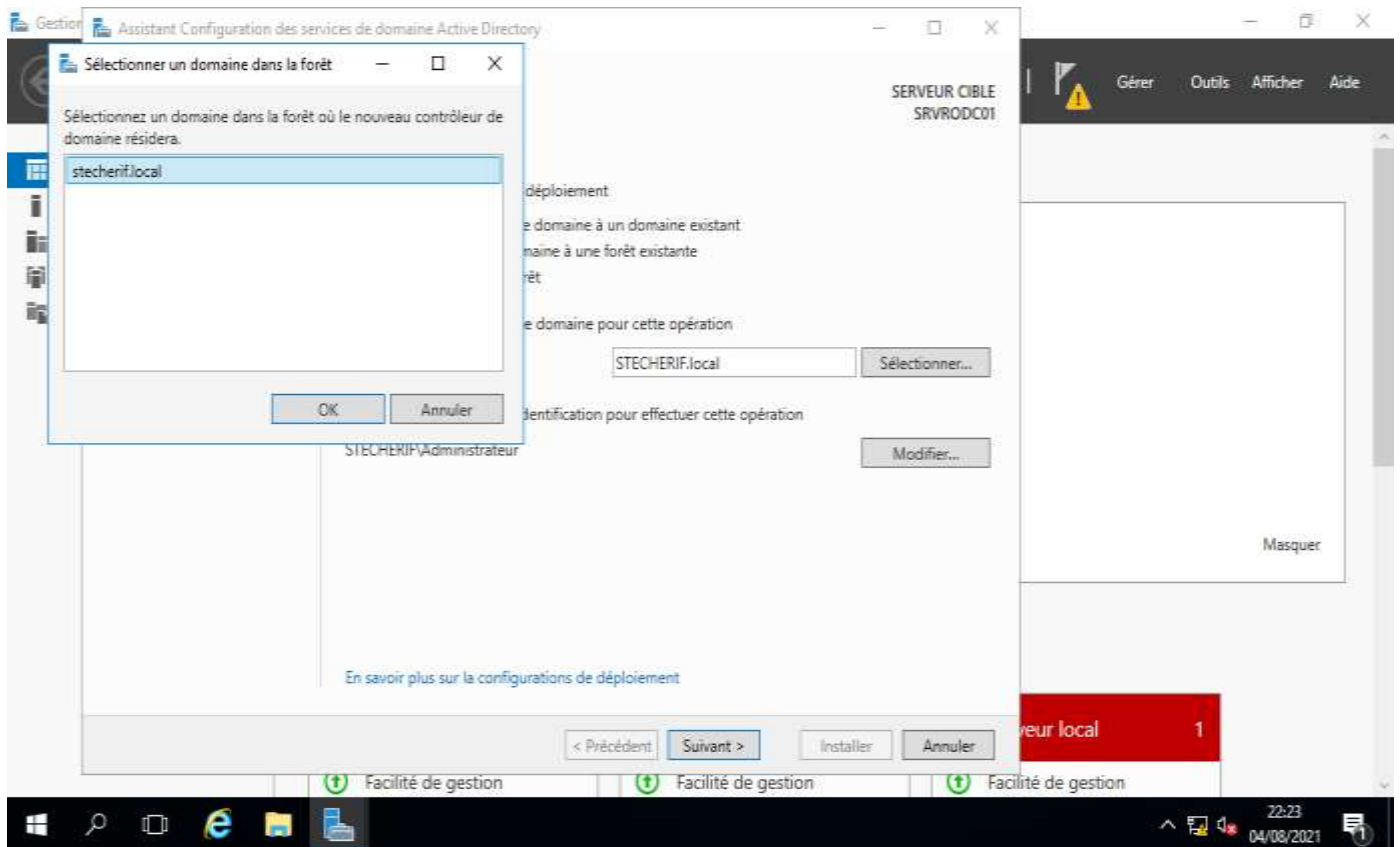
### Installation du AD



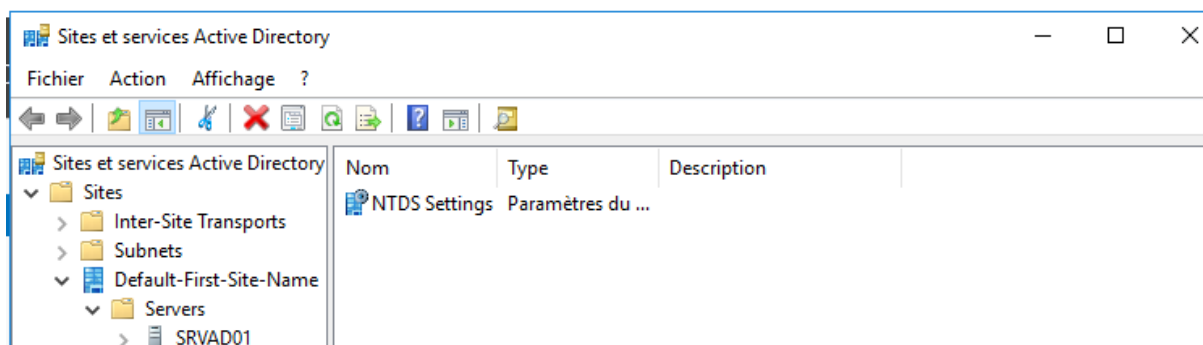
Associez le serveur au domaine, puis configurez le serveur comme contrôleur de domaine.



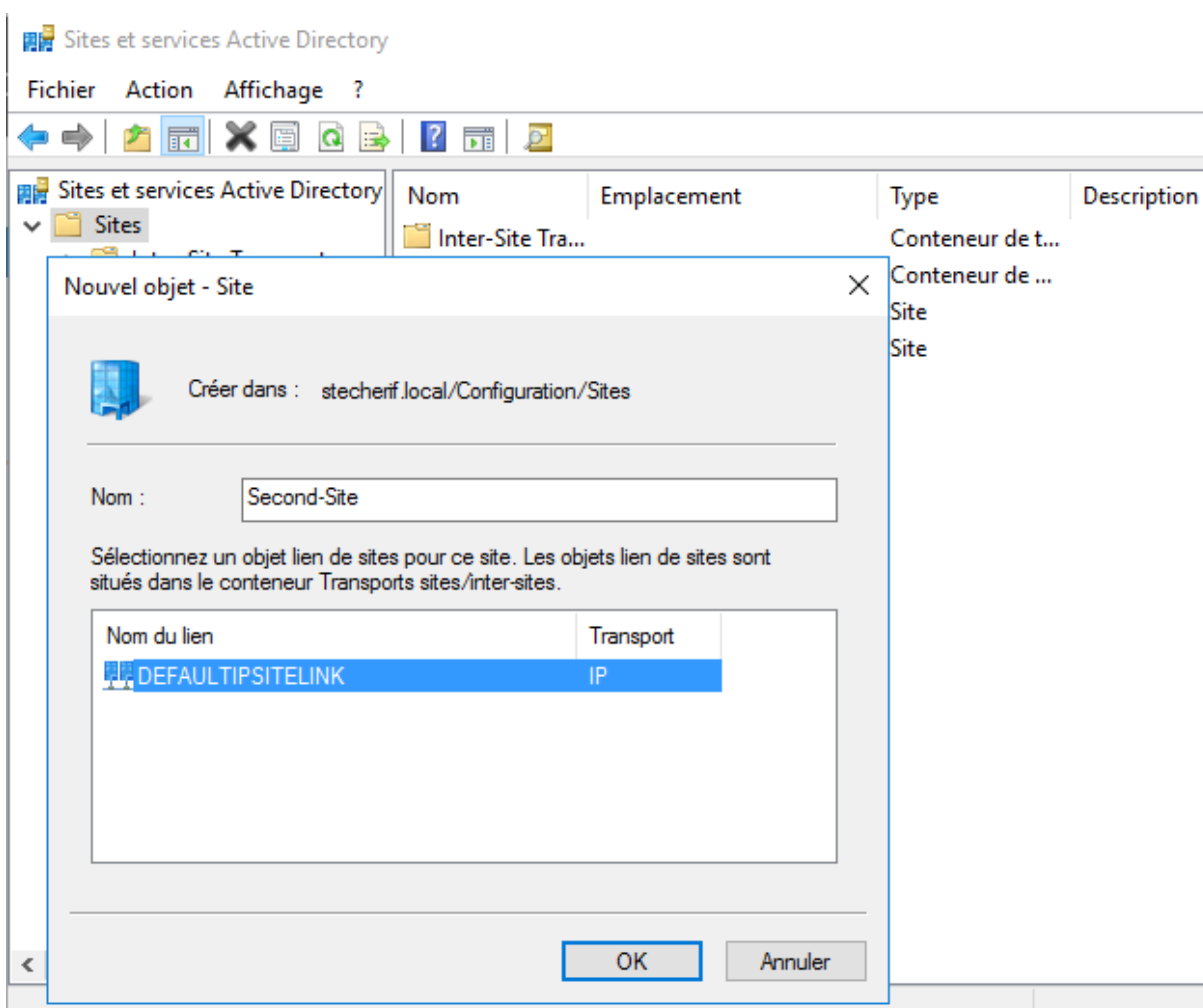




Ouvrir la console **Sites et services Active Directory** depuis les outils d'administration



Faire un clic droit sur **Sites** et créer un « **Nouveau site** ». Nommer le site « **Second-Site** » et sélectionnez le **transport par IP**.



Faire un clic droit sur « **Subnets** » et créer un « **Nouveau sous-réseau** ».  
Renseignez l'**adresse réseau du site distant**, 10.0.2.0/24 et sélectionnez le site correspondant.

Nouvel objet - Sous-réseau

Créer dans : stecherif.local/Configuration/Sites/Subnets

Entrez le préfixe d'adresse en utilisant la notation de préfixe réseau (adresse/longueur du préfixe), où la longueur du préfixe indique le nombre de bits fixes. Vous pouvez entrer un préfixe de sous-réseau IPv4 ou IPv6.  
[En savoir plus sur l'entrée des préfixes d'adresse.](#)

Exemple IPv4 : 157.54.208.0/20

Exemple IPv6 : 3FFE:FFFF:0:C000::/64

Préfixe :

10.0.2.0/24

Nom du préfixe des services de domaine Active Directory :

10.0.2.0/24

Sélectionnez un objet du site pour ce préfixe.

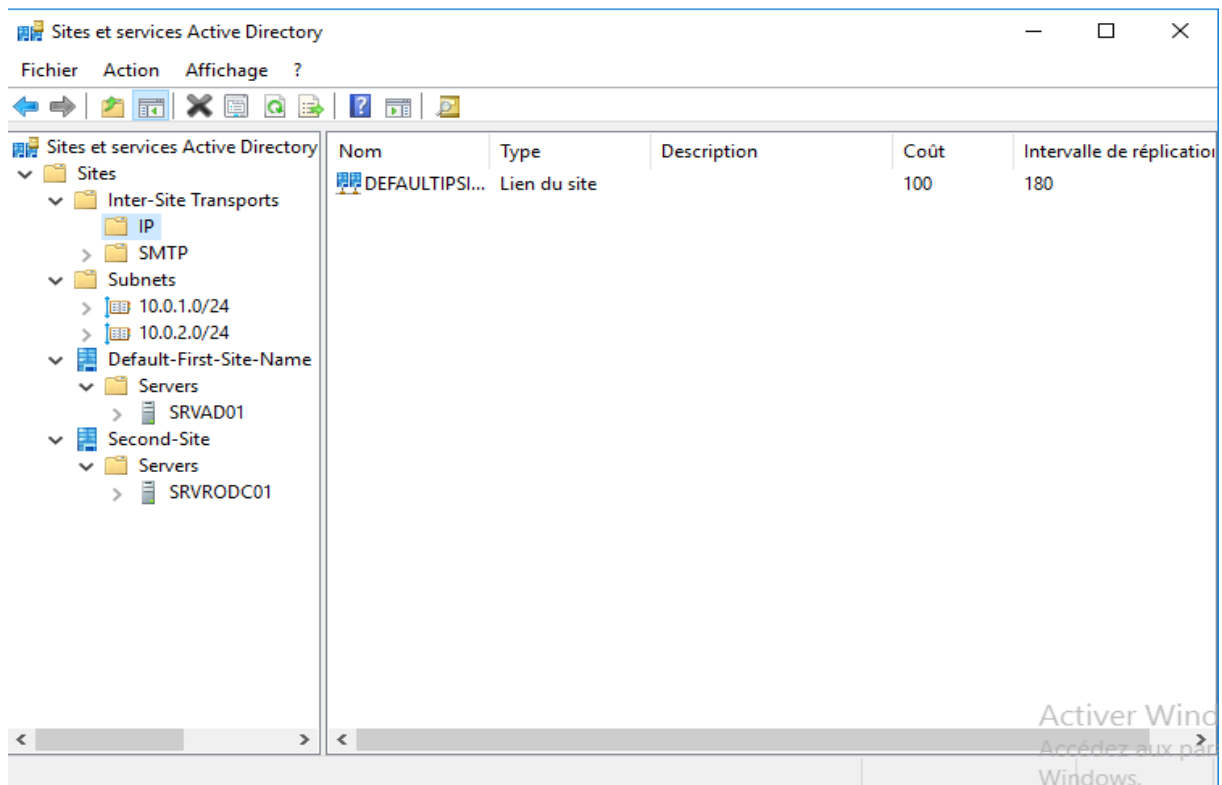
Nom du site

- Default-First-Site-Name
- Second-Site**

OK Annuler Aide

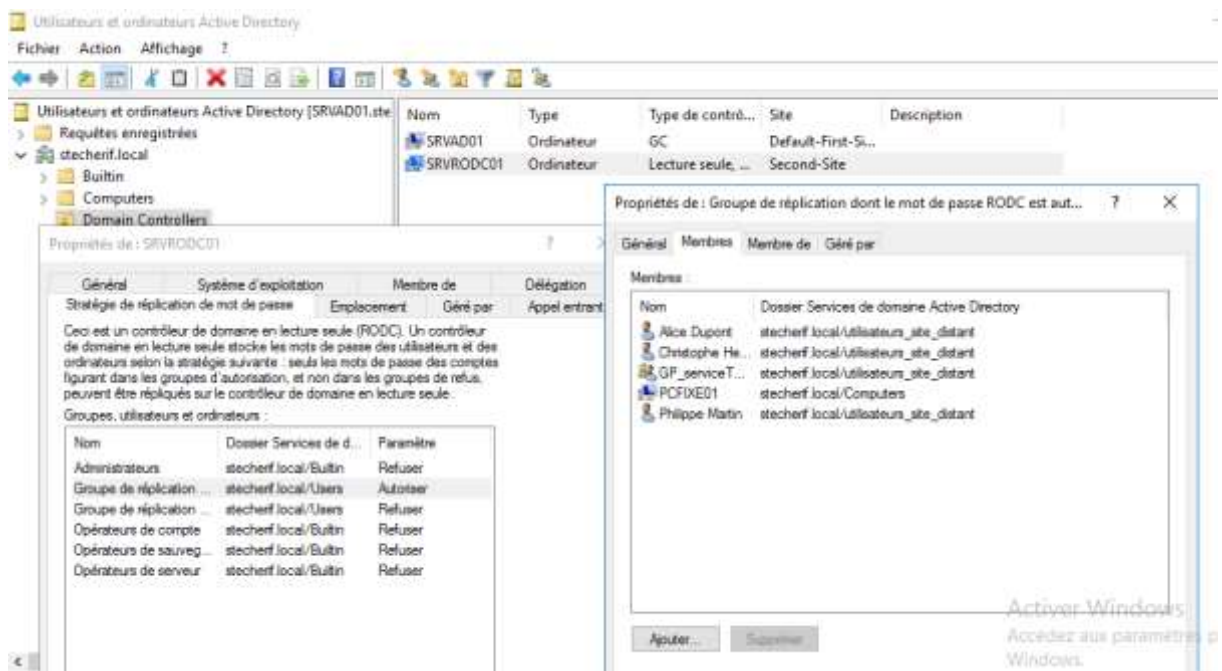
Déplacer le serveur SRVRODC01 sous « **Second-Site** » pour obtenir le résultat suivant





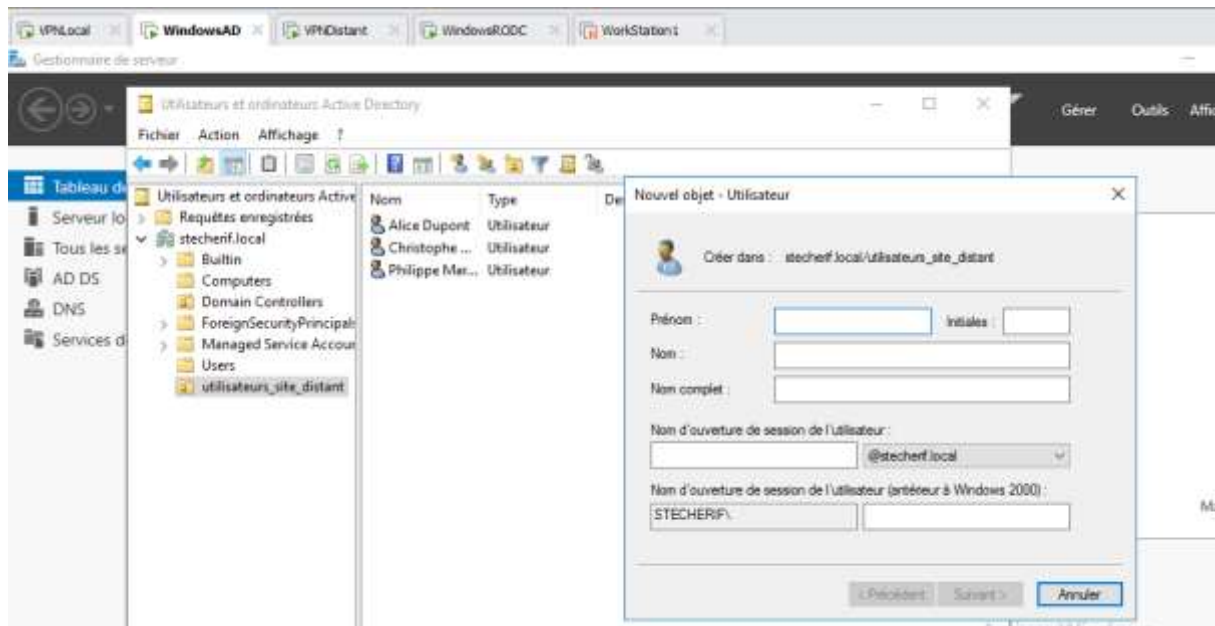
Pour permettre l'authentification des utilisateurs du Second site sur le RODC il suffit d'ouvrir « **Utilisateur et ordinateurs Active Directory** » aller sous « **Domain Controllers** » et cliquer droit sur « **SRVRODC01** » puis choisir propriétés

Il faut ajouter les utilisateurs du Second-Site au groupe explicitement autoriser à répliquer leurs mots de passe sur le RODC



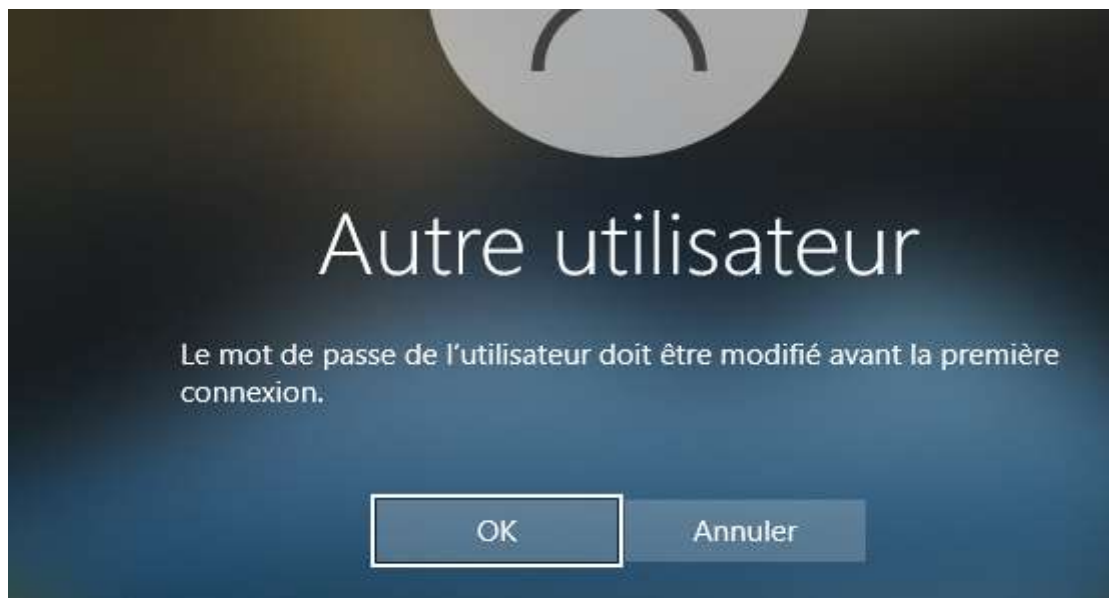
## V- Utilisation de l'AD

### 1- Créer les comptes AD des trois utilisateurs du site distant



### 2- Accéder à un utilisateur AD à partir d'un poste client pour la première fois

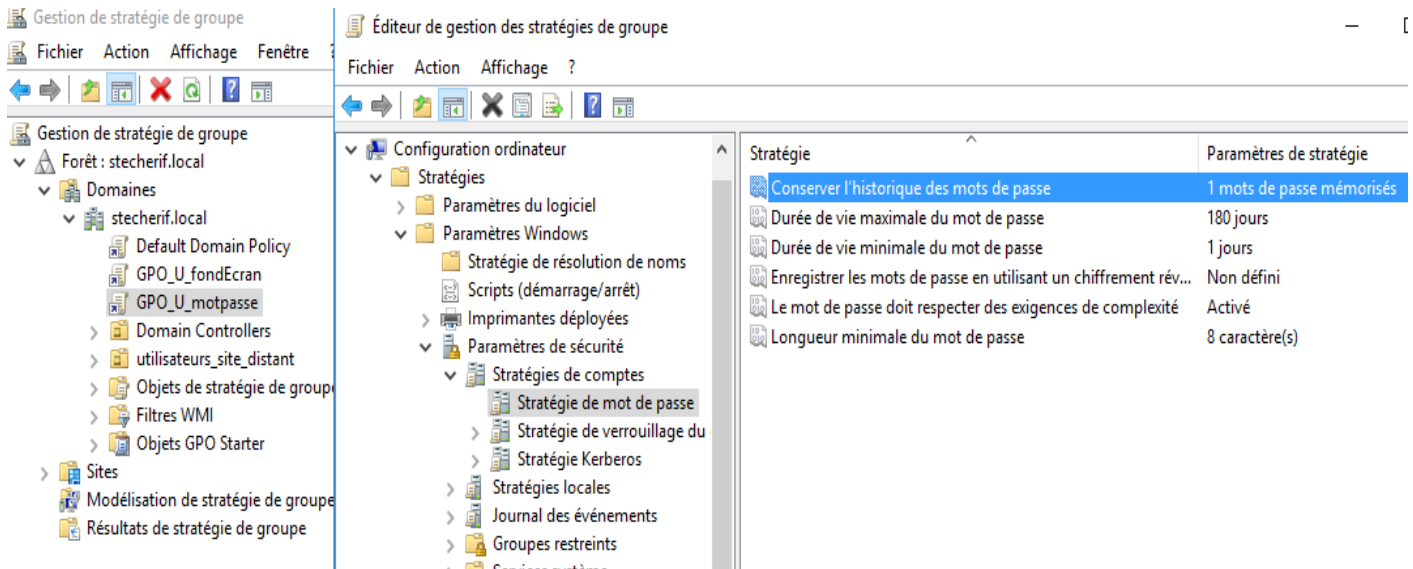




### 3-\ Création des GPO

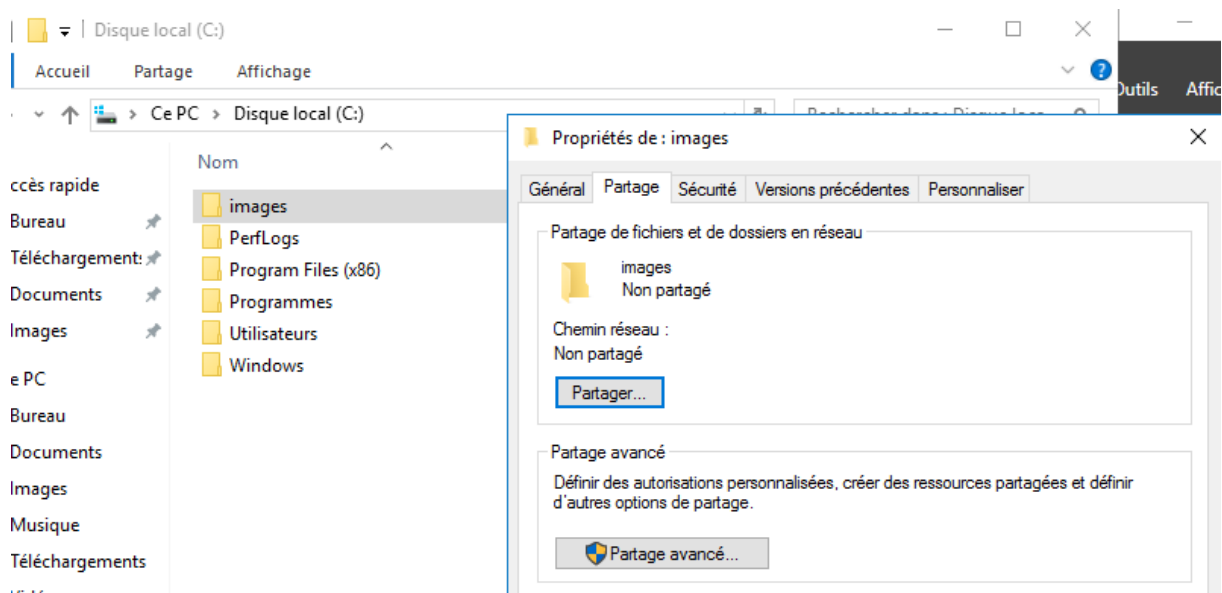
#### 1-\ Tous les employés doivent avoir un mot de passe fort et le changer tous les six mois

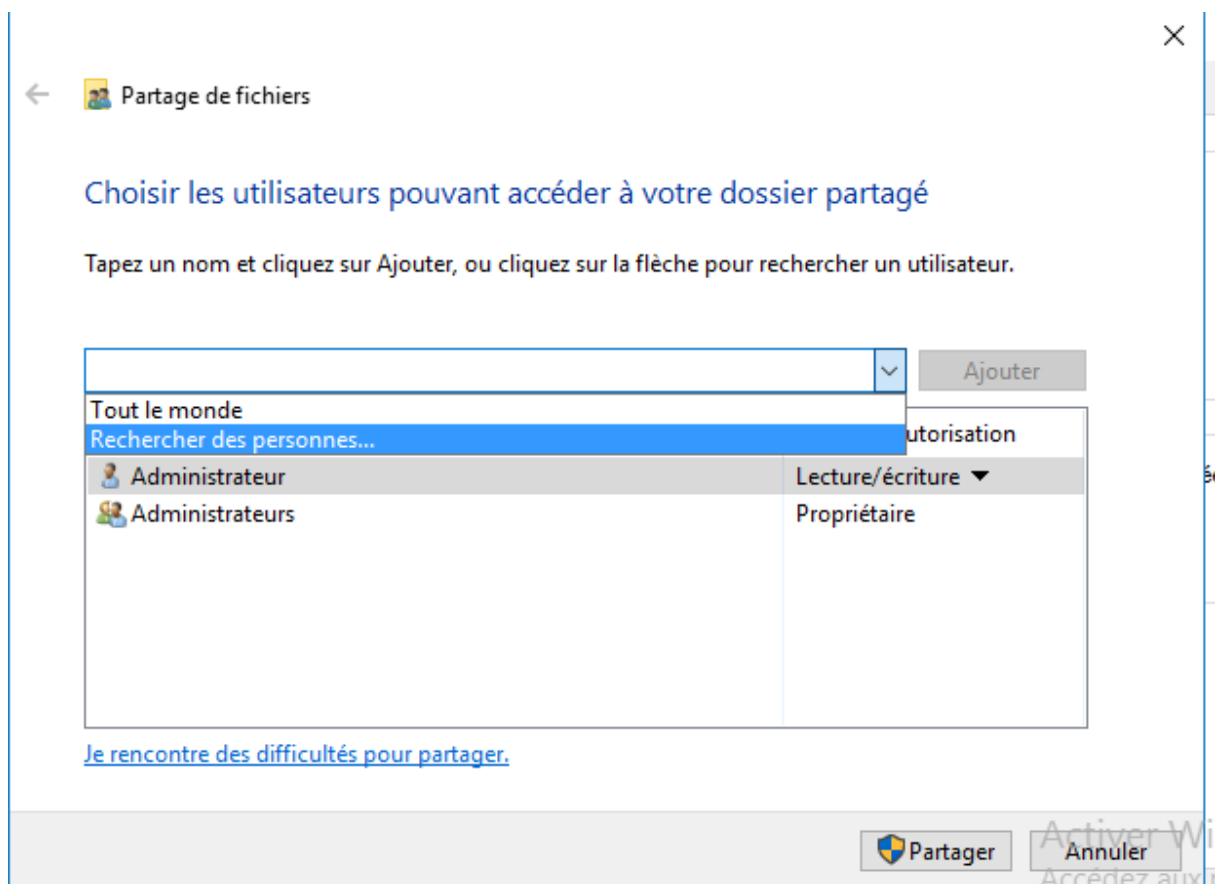
Outil → gestion des stratégies de groupe



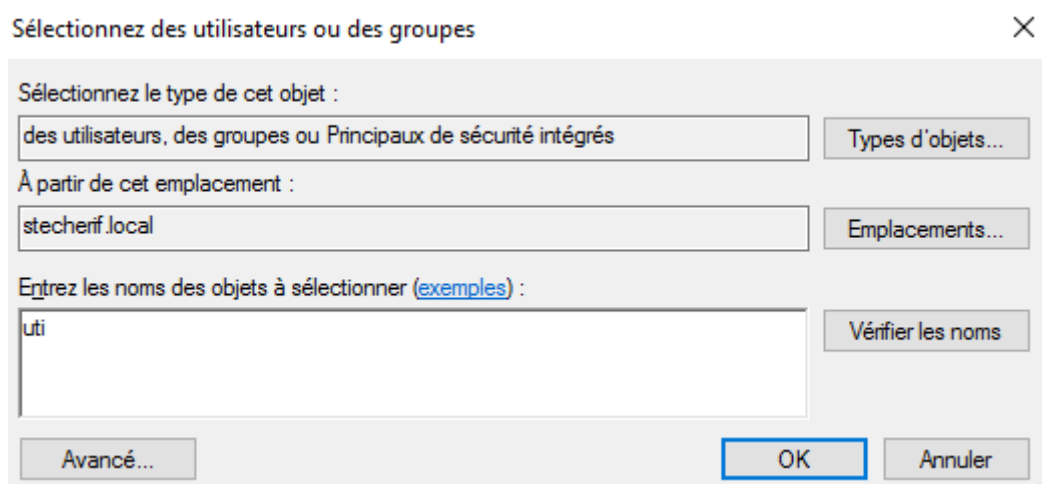
#### 2-\ Tous les employés doivent avoir le fond d'écran officiel de la société

**Création d'un dossier de partage pour placer l'image de fond de l'écran**





Saisir uti et cliquer sur vérifier les noms



Sélectionner utilisateurs authentifiés

Noms multiples trouvés

×

Plusieurs objets correspondent au nom uti. Sélectionnez un ou plusieurs noms dans la liste, ou retapez le nom.

Noms correspondants :

Nom	Nom d'ouverture ...	Adresse de mess...	Description	Dossier ^
UTILISATEUR TERMINAL ...				
Utilisateurs	Utilisateurs			steche
Utilisateurs authentifiés				
Utilisateurs de gestion à dist...	Utilisateurs de ge...			steche
Utilisateurs de l'Analyseur d...	Utilisateurs de l'A...			steche
Utilisateurs du Bureau à dist...	Utilisateurs du B...			steche
Utilisateurs du domaine	Utilisateurs du do...		Tous les utilisate...	steche
Utilisateurs du journal de per...	Utilisateurs du jo...			steche
Utilisateurs du modèle COM ...	Utilisateurs du m...			steche v

OK

Annuler

## Valider

Sélectionnez des utilisateurs ou des groupes

×

Sélectionnez le type de cet objet :

des utilisateurs, des groupes ou Principaux de sécurité intégrés
 

Types d'objets...

À partir de cet emplacement :

stecherif.local
 

Emplacements...

Entrez les noms des objets à sélectionner (exemples) :

Utilisateurs authentifiés
 

Vérifier les noms




Avancé...

OK


Annuler

## Choisir les utilisateurs pouvant accéder à votre dossier partagé

Tapez un nom et cliquez sur Ajouter, ou cliquez sur la flèche pour rechercher un utilisateur.

Nom	Niveau d'autorisation
 Administrateur	Lecture/écriture ▼
 Administrateurs	Propriétaire
 Utilisateurs authentifiés	Lecture ▼

[Je rencontre des difficultés pour partager.](#)


 Partager

Annuler

## Cliquer Partager

## Votre dossier est partagé.

Vous pouvez [envoyer](#) à quelqu'un par courrier électronique ces liens vers des éléments partagés, ou [copier](#) et coller les liens dans un autre programme.

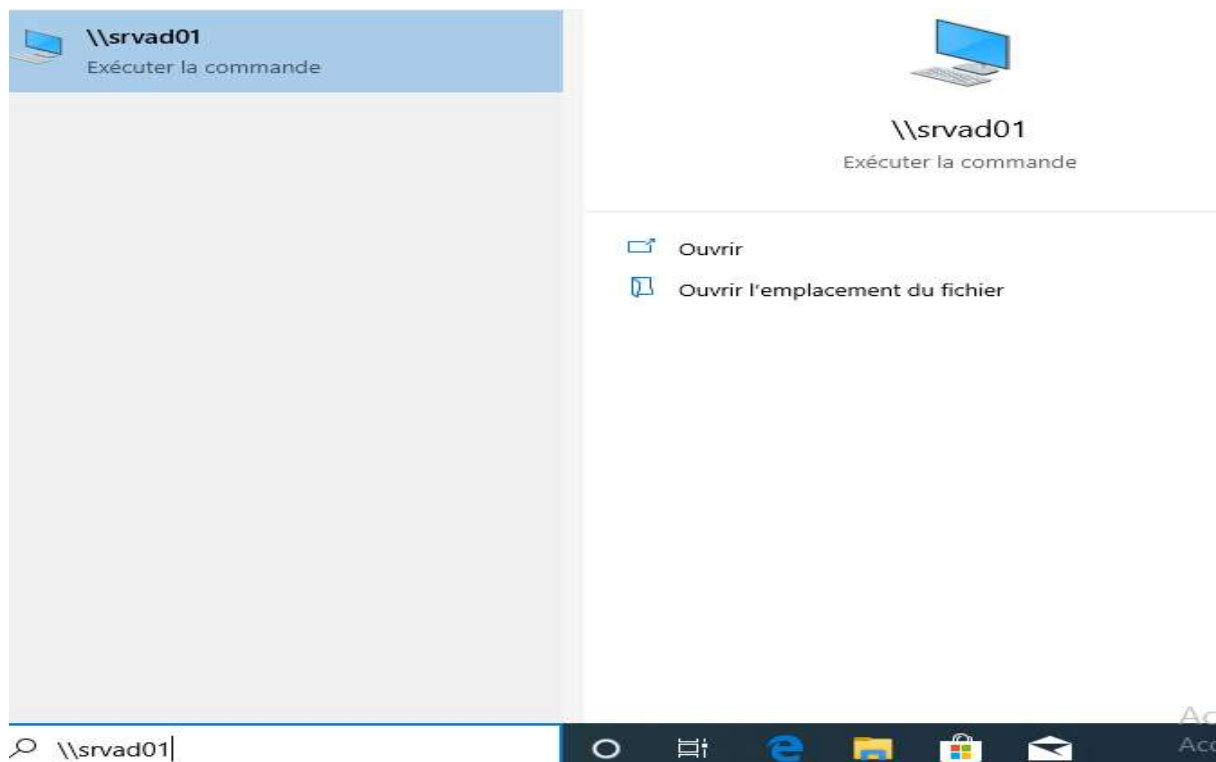
Éléments individuels	
	images (\\SRVAD01) \\SRVAD01\images

[Afficher tous les partages réseau de cet ordinateur.](#)

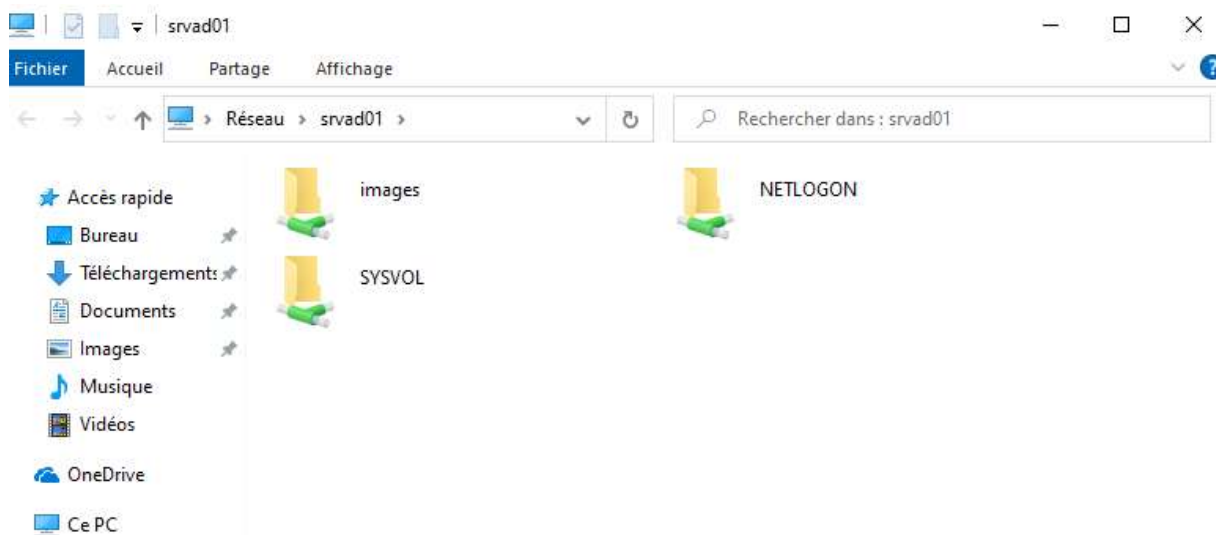
Terminé

Terminer → fermer

Voir les dossiers partager

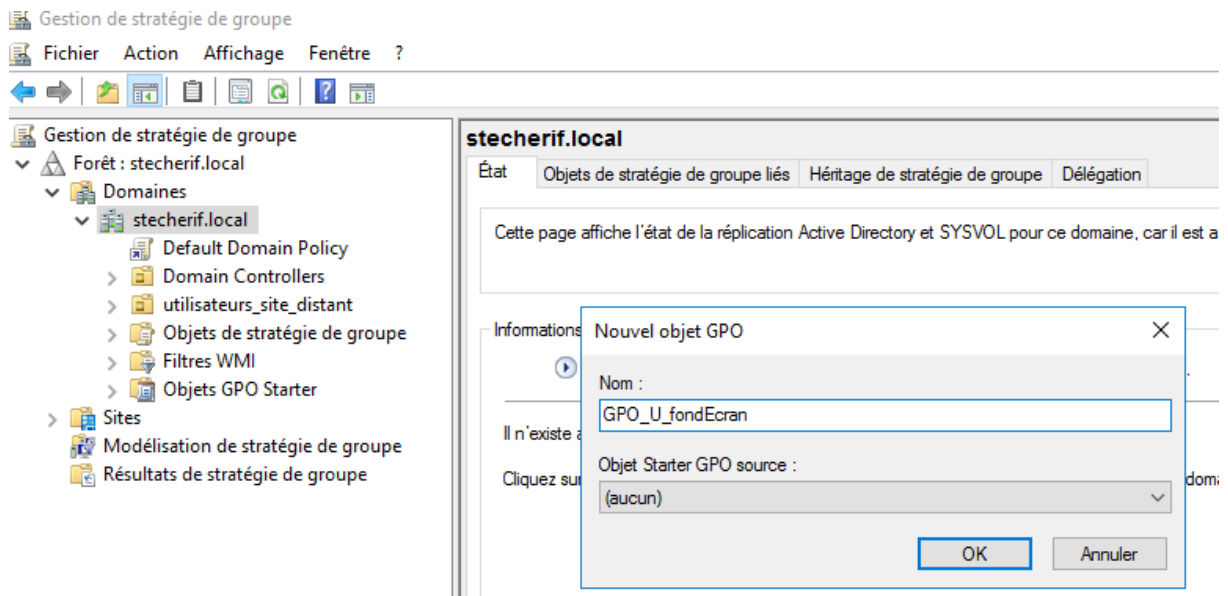


Cliquer sur ouvrir

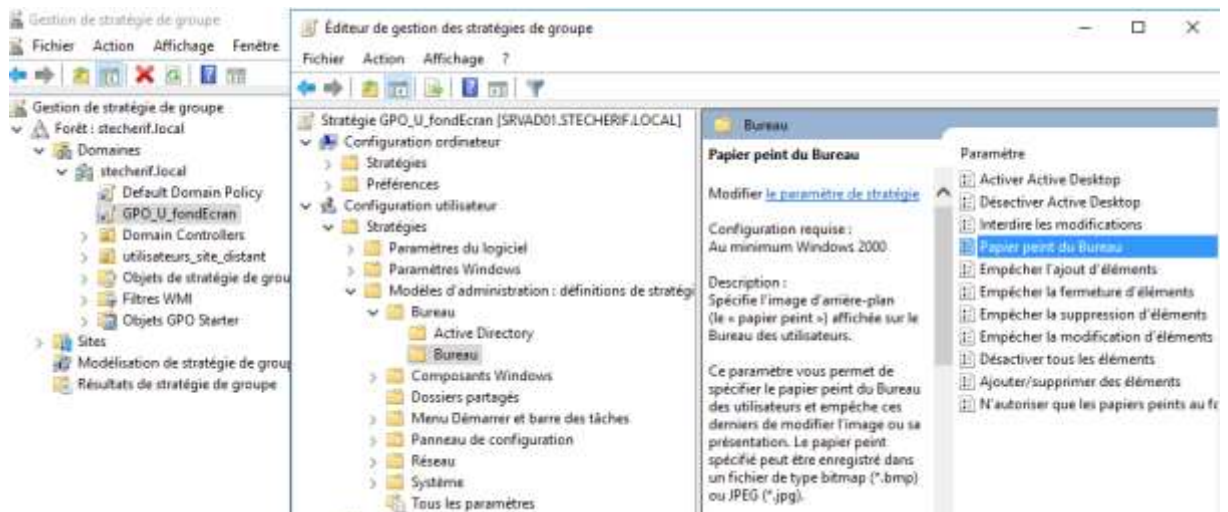




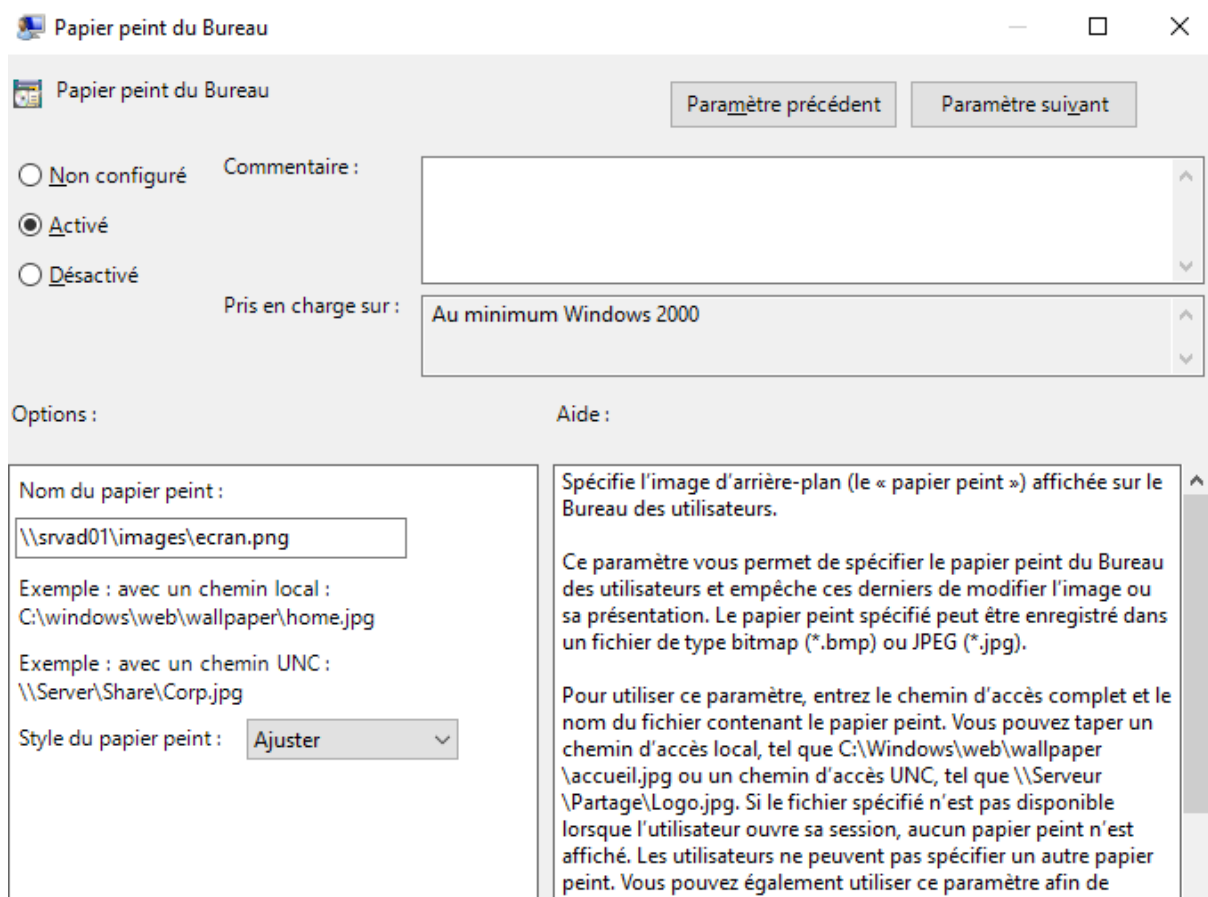
## Création du GPO « GPO\_fondEcran »



Cliquer sur le bouton droite du GPO\_U\_fondEcran → modifier

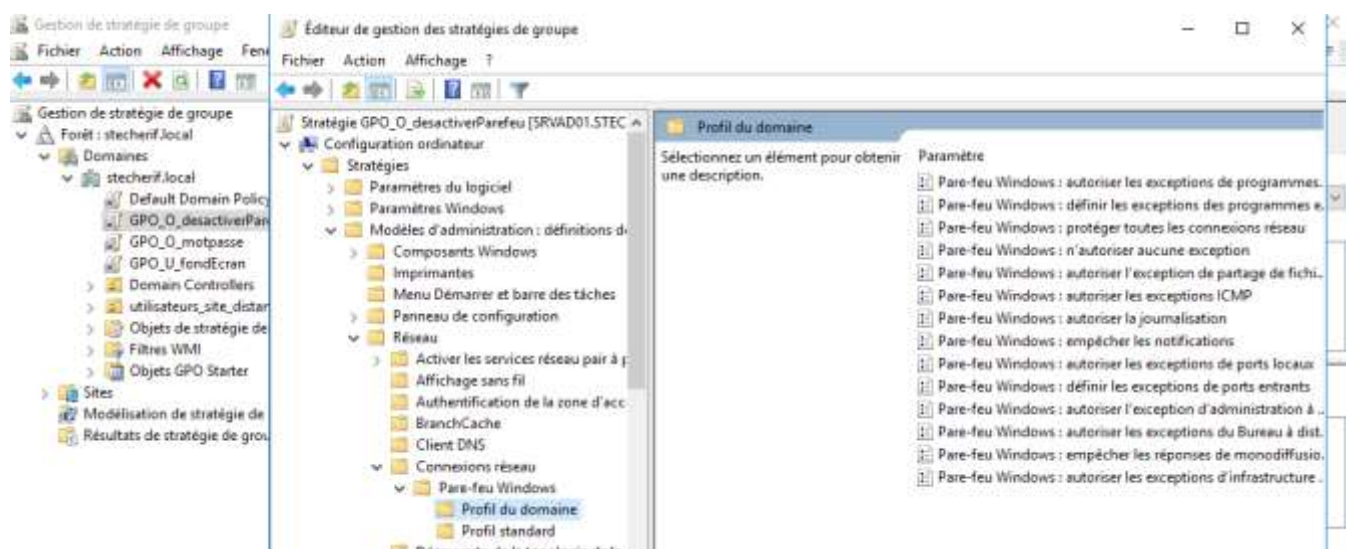


Cliquer sur papier peint du bureau



Saisir le nom du papier peint et son chemin et activer le GPO et valider en cliquant sur ok

### 3- \Aucun employé ne peut désactiver le parefeu Windows



Pare-feu Windows : protéger toutes les connexions réseau

Pare-feu Windows : protéger toutes les connexions réseau Paramètre précédent Paramètre suivant

☐ Non configuré    Commentaire :   
☒ **Activé**   
☐ Désactivé

Pris en charge sur : **Au minimum Windows XP Professionnel avec SP2**

Options : Aide :

Active le Pare-feu Windows.

Si vous activez ce paramètre de stratégie, le Pare-feu Windows s'exécutera en ignorant le paramètre de stratégie « Configuration ordinateur\Modèles d'administration\Réseau\Connexions réseau\Interdire l'utilisation de pare-feu de connexion Internet sur le réseau de votre domaine DNS ».

Si vous désactivez ce paramètre, le Pare-feu Windows ne

## Tester ce GPO sur la machine client

VPNDistant x WindowsRODC x **WorkStation1** x

Page d'accueil du panneau de configuration

Autoriser une application ou une fonctionnalité via le Pare-feu Windows Defender

Modifier les paramètres de notification  
 Activer ou désactiver le Pare-feu Windows Defender  
 Paramètres par défaut  
 Paramètres avancés  
 Dépanner mon réseau

### Protégez votre ordinateur avec le Pare-feu Windows Defender

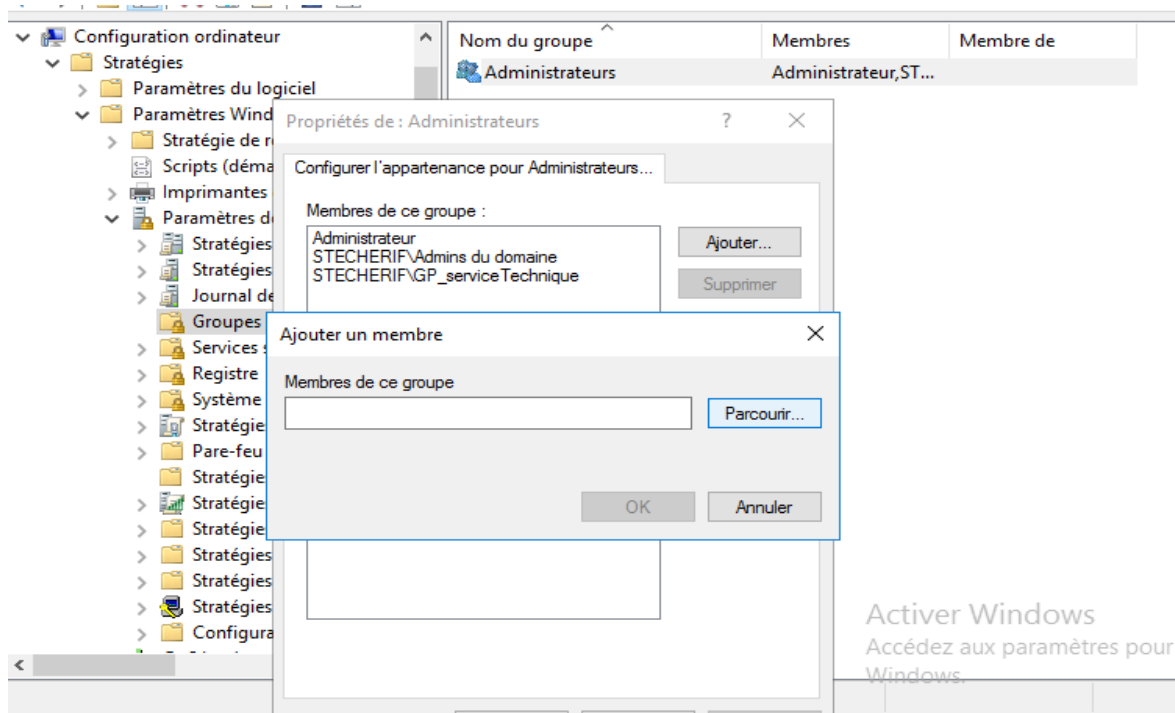
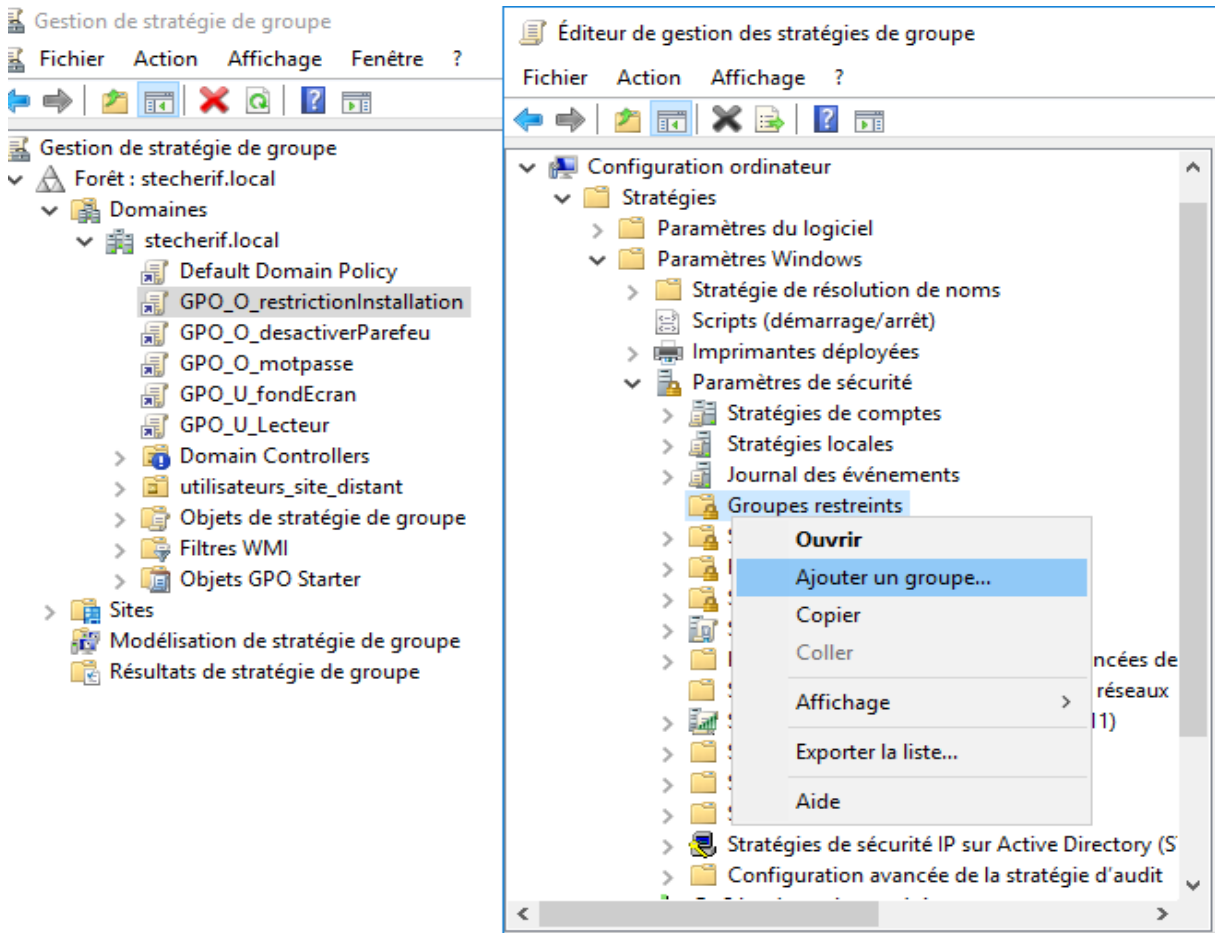
Le Pare-feu Windows Defender a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.

**i** Par sécurité, certains paramètres sont gérés par l'administrateur système.

<b>Réseaux avec domaine</b> <span>Connecté ^</span>	
Réseaux en entreprise, qui appartiennent à un domaine	
État du Pare-feu Windows Defender :	Activé
Connexions entrantes :	Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées
Réseaux avec domaine actifs :	stecherif.local
État de notification :	M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application


<b>Réseaux privés</b>	Non connecté v
<b>Réseaux publics ou invités</b>	Non connecté v

#### 4-\ Aucun employé ne peut installer de logiciels sauf les membres du service technique






**5- Tous les employés ont accès en lecture-écriture au répertoire partagé “SharedCompanyDocs” hébergé sur le DC Active Directory : vous devrez donc d’abord créer et partager ce dossier puis le mapper en tant que lecteur réseau pour tous les employés.**

**Creation du repertoire de partage « SharedCompanyDocs »**


←  Partage de fichiers

Choisir les utilisateurs pouvant accéder à votre dossier partagé

Tapez un nom et cliquez sur Ajouter, ou cliquez sur la flèche pour rechercher un utilisateur.

Nom	Niveau d'autorisation
 Administrateur	Lecture/écriture ▼
 Administrateurs	Propriétaire
 Utilisateurs authentifiés	Lecture/écriture ▼


[Je rencontre des difficultés pour partager.](#)

←  Partage de fichiers

Votre dossier est partagé.

Vous pouvez [envoyer](#) à quelqu'un par courrier électronique ces liens vers des éléments partagés, ou [copier](#) et coller les liens dans un autre programme.

Éléments individuels

 SharedCompanyDocs (\\SRVAD01)  
\\SRVAD01\\SharedCompanyDocs

[Afficher tous les partages réseau de cet ordinateur.](#)

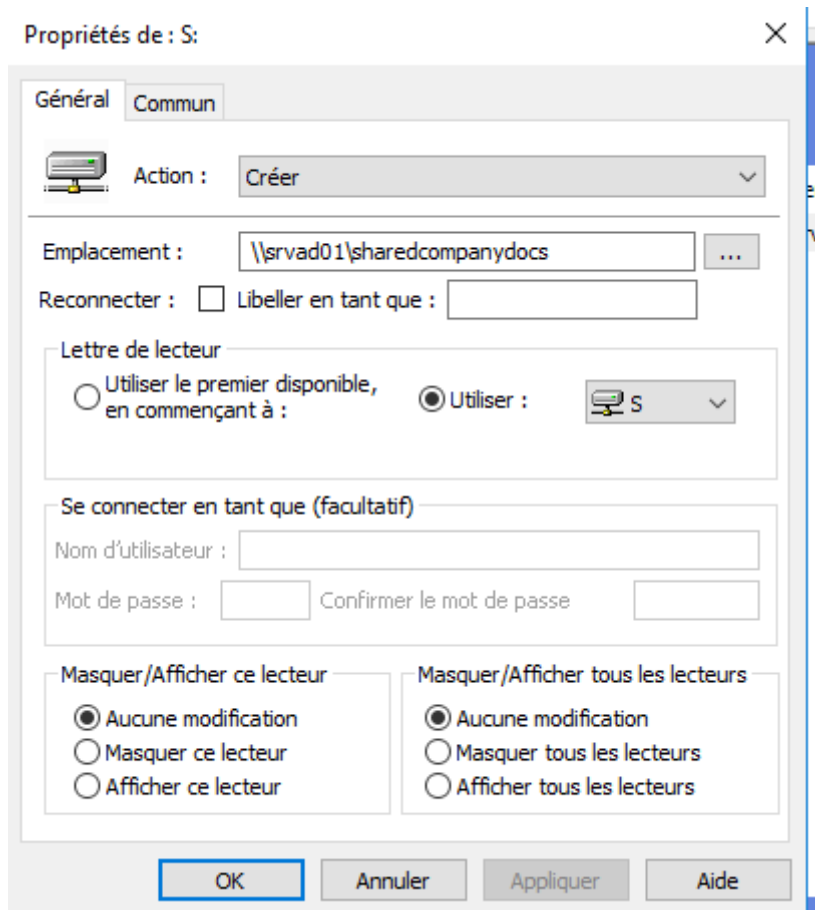
## Creation du GPO « GPO U Lecteur »

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

The screenshot shows the Group Policy Editor window. The left pane displays the hierarchy: Configuration ordinateur > Stratégies > Préférences > Configuration utilisateur > Stratégies > Préférences > Paramètres Windows > Mappages de lecteurs. The right pane shows the 'Mappages de lecteurs' policy with a table header: Nom, Ordre, Action. The table contains one entry: 'Traitement en cours' with a status of 'Auc'. Below the table is a 'Description' section stating 'Aucune stratégie sélectionnée'.

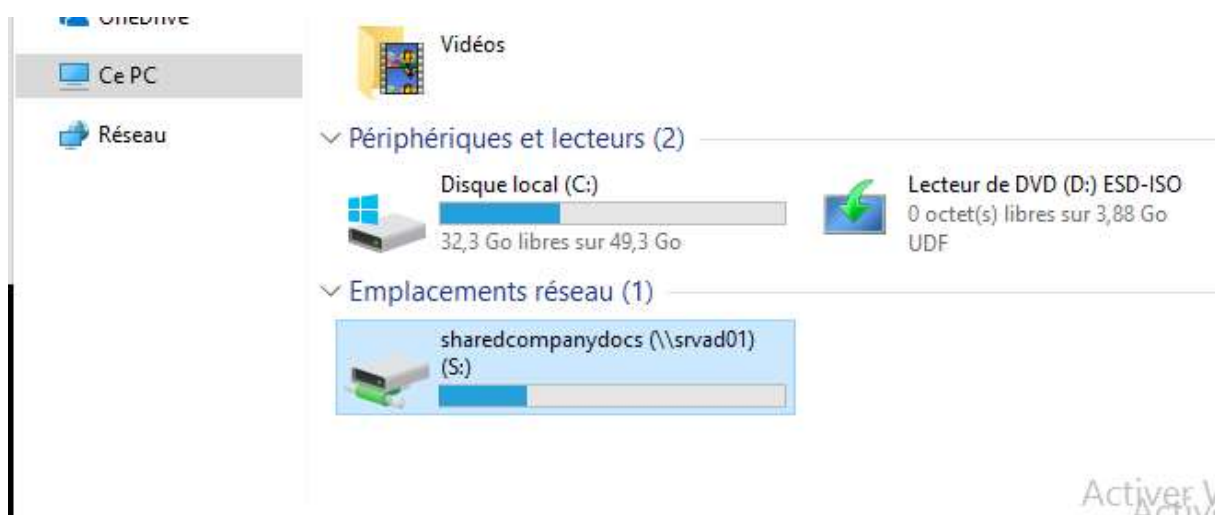
The screenshot shows the 'Mappages de lecteurs' control panel window. It has a table with columns: Nom, Ordre, Action, Chemin d'accès, and Reconnecter. The table is empty, with the message 'Aucun élément à afficher dans cet aperçu.' below it. A context menu is open over the 'Lecteur mappé' header, showing options: Nouveau, Toutes les tâches, Actualiser, Affichage, Réorganiser les icônes, Aligner les icônes, and Aide.



Tester ce GPO sur la machine client

```
C:\Users\adupont>
C:\Users\adupont>gpupdate /force
Mise à jour de la stratégie...

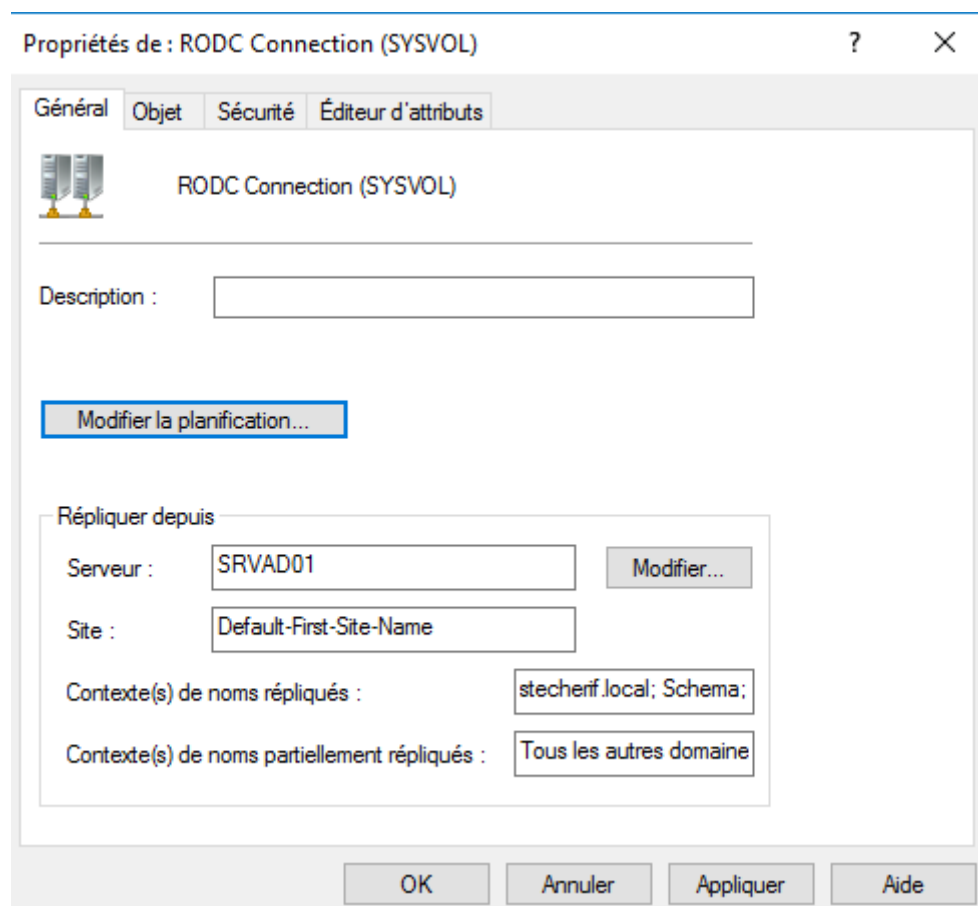
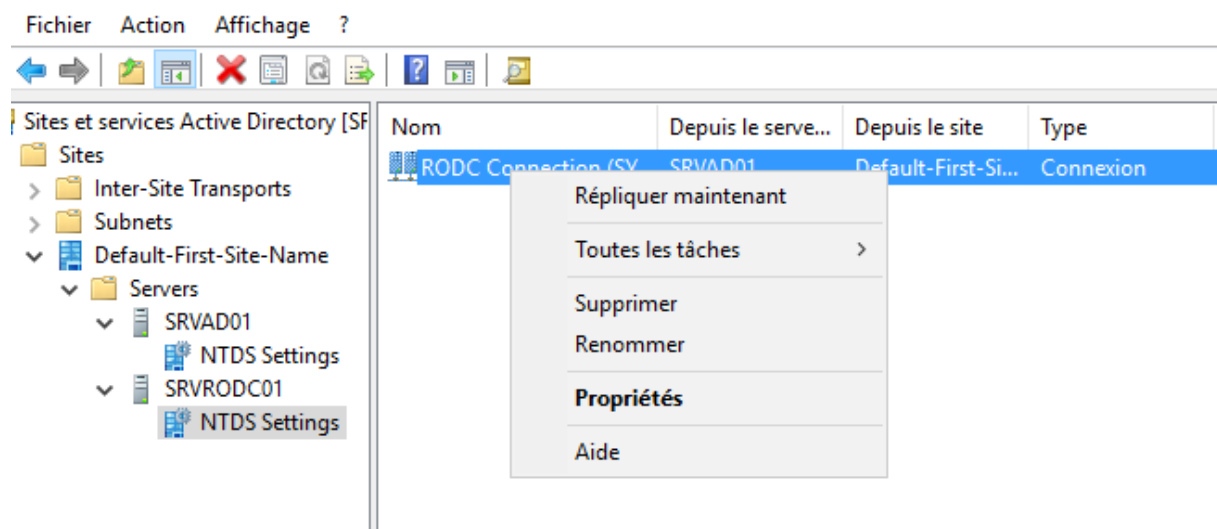
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```



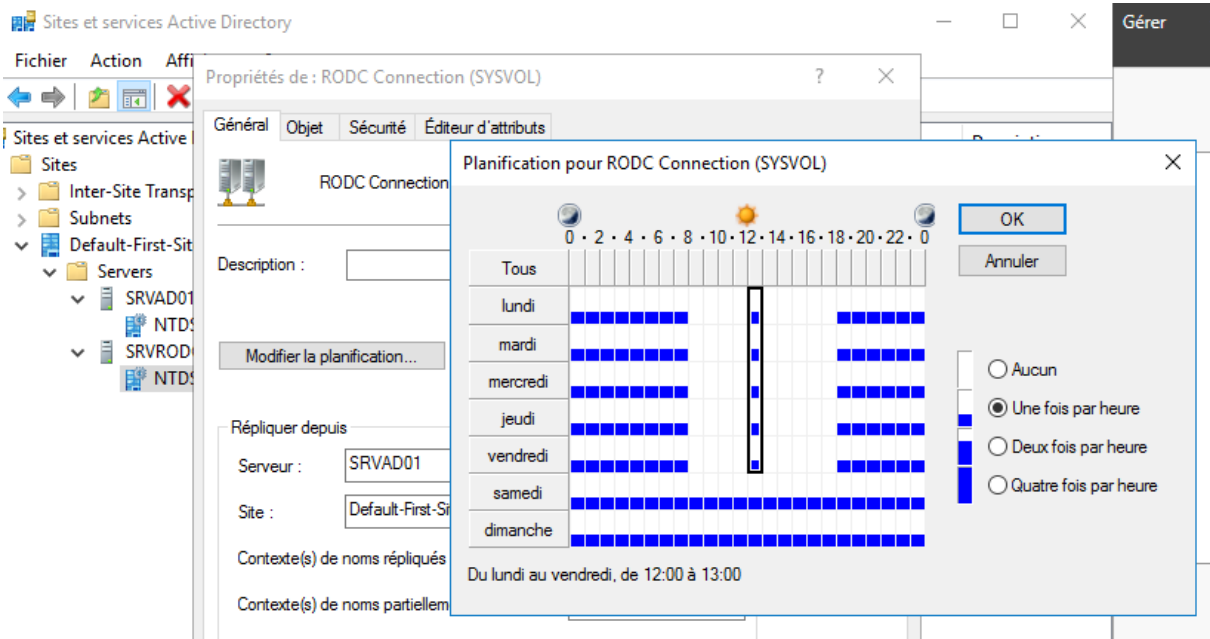


## 4-\ Réduire le trafic pendant les horaires de bureau

Outil → sites et services Active Directory

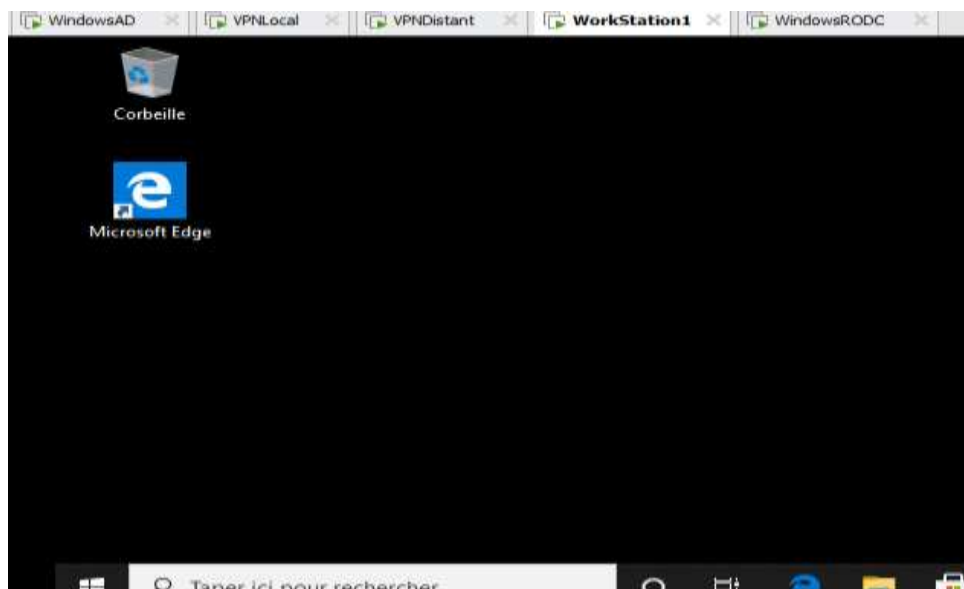






**5-\ Vérifiez que lorsque la liaison VPN est coupée, les utilisateurs peuvent s'authentifier sur le Domaine mais pas changer leur mot de passe.**

**Authentification de Alice Dupont avec coupure du VPN**



**Alice dupont n'a pas pu changer son mot de passe**



**Commande pour vérifier le contrôleur de domaine disponible pour authentifier Alice Dupont**

```
C:\Users\adupont>nlttest /whowill:STECHERIF adupont
[13:15:35] Message 0 envoyé correctement (\MAILSLOT\NET\GETDCEA94FAF4)
[13:15:35] Réponse 0 : NetpDcAllocateCacheEntry: new entry 0x0000018CD528BA10 -> DC:SRVRODC01 DnsDomName:(null) Flags:0x
0
S :SRVRODC01 D :STECHERIF A :adupont (Acte trouvé)
La commande a été correctement exécutée
C:\Users\adupont>
```

## Webography

### **Partie : Installation et configuration de openvpn :**

[https://shebangthedolphins.net/fr/vpn\\_openvpn\\_buster.html](https://shebangthedolphins.net/fr/vpn_openvpn_buster.html)

<https://www.youtube.com/watch?v=BqdHUjH1nwU>

<https://matoski.com/article/site-to-site-openvpn-firewalld-debian/>

<https://www.rosehosting.com/blog/how-to-set-up-an-openvpn-server-on-debian-10/>

<https://www.howtoforge.com/tutorial/how-to-install-openvpn-server-and-client-with-easy-rsa-3-on-centos-8/>

### **Partie : Installation et configuration d'un AD**

<https://www.pc2s.fr/installation-dun-controleur-de-domaine-windows-serveur-2019-2016-2012-r2/>

<https://neptunet.fr/rodc/>

<https://rdr-it.com/mise-en-place-controleur-domaine-lecture-seule-rodc/>

<https://fr.linkedin.com/learning/windows-server-2019-active-directory-et-les-strategies-de-groupe/deployer-des-lecteurs-reseau-a-l-aide-des-preferences?resume=false>