

Active directory (Windows Server)

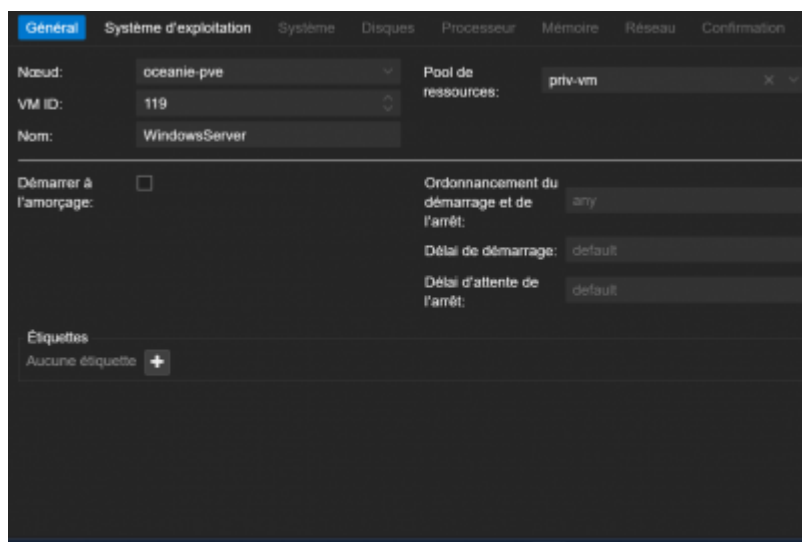
Tout d'abord on récupère une image .iso de Windows 11, d'un Windows Server et du driver virtio dans sa dernière version stable. On se rend sur notre interface web Proxmox (10.31.208.1:8006). On clique à droite sur 'oceanie-pve' puis sur 'local' puis sur 'Image ISO', et on ajoute les fichiers .iso.

Windows Server

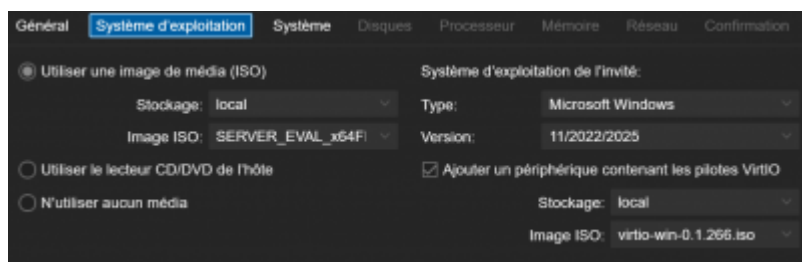
Installation

Sur Proxmox on crée une VM :

- Général :
 - Nom : WindowsServer
 - Pool : priv-vm



- OS :
 - Image ISO : SERVER_EVAL_x64FRE_fr-fr.iso
 - Type : Microsoft Windows
 - Version : 11/2022/2025
 - Ajouter un périphérique contenant les pilotes VirtIO
 - Image ISO : virtio-win-0.1.266.iso



- Système :
 - Stockage EFI : local-lvm

- Contrôleur SCSI : VirtIO SCSI
- Agent QEMU
- Stockage TPS : local-lvm

The screenshot shows the 'Système' tab in the QEMU configuration window. The 'Contrôleur SCSI' is set to 'VirtIO SCSI'. The 'Agent QEMU' checkbox is checked. The 'BIOS' is set to 'OVMF (UEFI)'. The 'Ajouter un disque EFI' checkbox is checked. The 'Stockage EFI' is set to 'local-lvm'. The 'Format' is set to 'Image disque brute (raw)'. The 'Clé de préinscription' checkbox is checked.

- Disques :
 - Taille du disque : <32
 - Cache : Write back

The screenshot shows the 'Disques' tab in the QEMU configuration window. The 'Bus/périphérique' is set to 'SCSI'. The 'Cache' is set to 'Write back'. The 'Contrôleur SCSI' is set to 'VirtIO SCSI'. The 'Stockage' is set to 'local-lvm'. The 'Taille du disque (Gio)' is set to '64'. The 'Format' is set to 'Image disque brute (r)'. The 'Émulation de SSD' checkbox is unchecked. The 'En lecture seule' checkbox is unchecked. The 'Sauvegarde' checkbox is checked. The 'Passer la réplication' checkbox is unchecked. The 'E-S asynchrones' is set to 'Par défaut (io_uring)'.

- Processeur :
 - Cœurs : 2

The screenshot shows the 'Processeur' tab in the QEMU configuration window. The 'Supports de processeur' is set to '1'. The 'Cœurs' is set to '2'. The 'Type' is set to 'x86-64-v2-AES'. The 'Total de cœurs' is set to '2'. The 'Processeurs virtuels' is set to '2'. The 'Unités processeur' is set to '100'. The 'Limite d'utilisation processeur' is set to 'Illimité'. The 'Activer NUMA' checkbox is unchecked. The 'Affinité processeur' is set to 'Tous les cœurs'.

Configuration de l'installation

Une fois créé on lance la VM et l'installation de Windows.

On choisit la langue. Puis dans la sélection du disque on clique sur "Charger le pilote" on accède au lecteur CD sur lequel on a monté le pilote VirtIO on sélectionne le dossier "vioscsi\2k22\amd64" puis sur le fichier "Red Hat VirtIO SCSI pass-through controller". On clique sur 'suivant'.

On répète l'opération avec le fichier "NetKVM\2k19\amd64\Redhat VirtIO Ethernet Adapter" et "Balloon\2k19\amd64\VirtIO Balloon Driver".

On valide et l'installation de la configuration se fait.

Configuration du serveur

On se rend dans les Paramètres réseau et internet, dans Modifier les options d'adaptateur, dans Ethernet, dans Propriétés, puis Double clic sur ipv4

Adresse IP : 10.31.208.200 Masque de sous-réseau : 255.255.252.0 (pour /22) Passerelle par défaut : 10.31.211.254 Serveur DNS préféré : 127.0.0.1

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

☐ Valider les paramètres en quittant

Avancé...

On se rend dans le gestionnaire de serveur, sur Serveur local, changez le nom puis activez le bureau à distance pour l'administrateur uniquement.

Modification du nom ou du domaine de l'ordinateur ✕

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :

Nom complet de l'ordinateur :

WSOceanie.oceanie.lan

Autres...

Membre d'un



Domaine :



Groupe de travail :

OK

Annuler

Propriétés système ✕

Nom de l'ordinateur

Matériel

Paramètres système avancés

Utilisation à distance

Assistance à distance

☐ Autoriser les connexions d'assistance à distance vers cet ordinateur

Options avancées...

Bureau à distance

Choisissez une option, puis spécifiez qui peut se connecter.

☐ Ne pas autoriser les connexions à distance à cet ordinateur

☒ Autoriser les connexions à distance à cet ordinateur

☒ N'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (recommandé)

[Comment choisir ?](#)

Sélectionnez des utilisateurs...

OK

Annuler

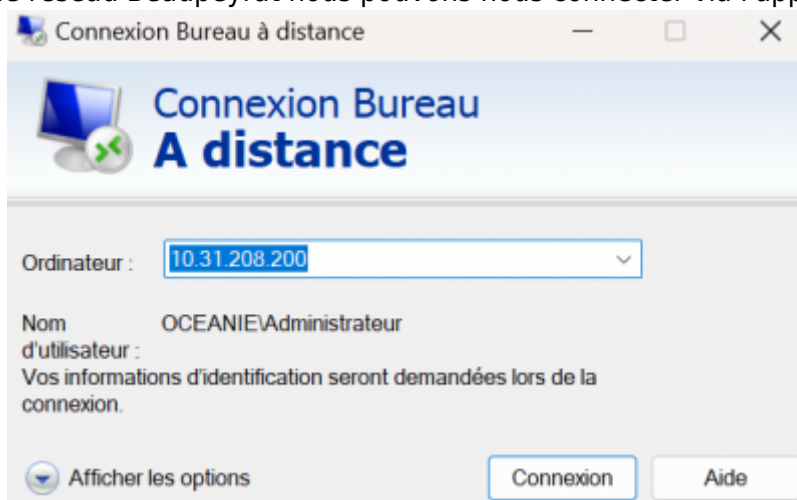
Appliquer

Et on ajoute le compte Administrateur comme pouvant être le compte auquel on se connecte.

Pour se connecter au bureau à distance il faut autoriser la connexion à travers le parefeu en rajoutant une règle sur le routeur :

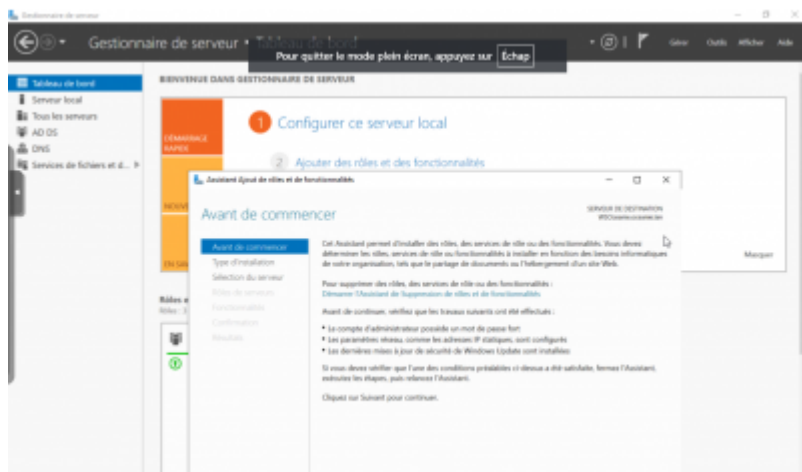
Source	Destination	Port	Protocole
BeaupNET	10.31.208.200	3389	TCP/UDP

Maintenant depuis le réseau Beaupeyrat nous pouvons nous connecter via l'application Connexion



Bureau à distance :

Maintenant connecté, on va aller dans le gestionnaire de serveur, sur le tableau de bord, sur « Ajouter des rôles et des fonctionnalités » :



Type d'installation : Installation basée sur un rôle ou une fonctionnalité
Suivant

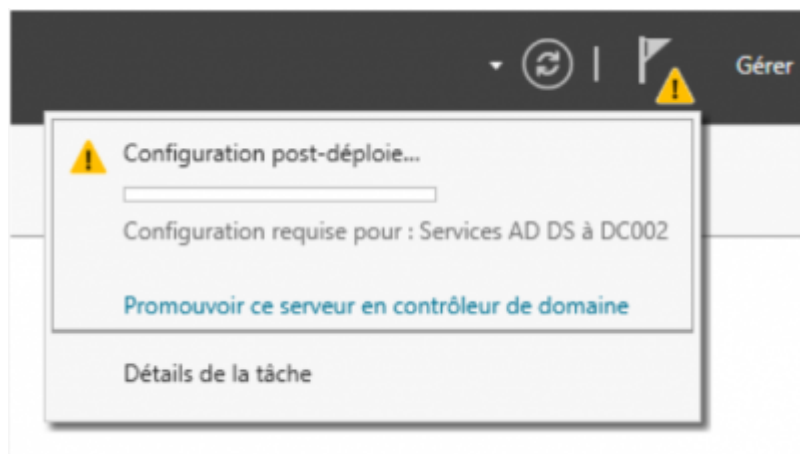
Sélection du serveur : on sélectionne notre serveur
Suivant

Rôle de serveurs : on sélectionne Serveur DNS et Serveur AD DS
Suivant

On termine la configuration et on reboot la machine.

De retour sur notre machine, on retourne sur le gestionnaire de serveurs, en haut à gauche un sigle

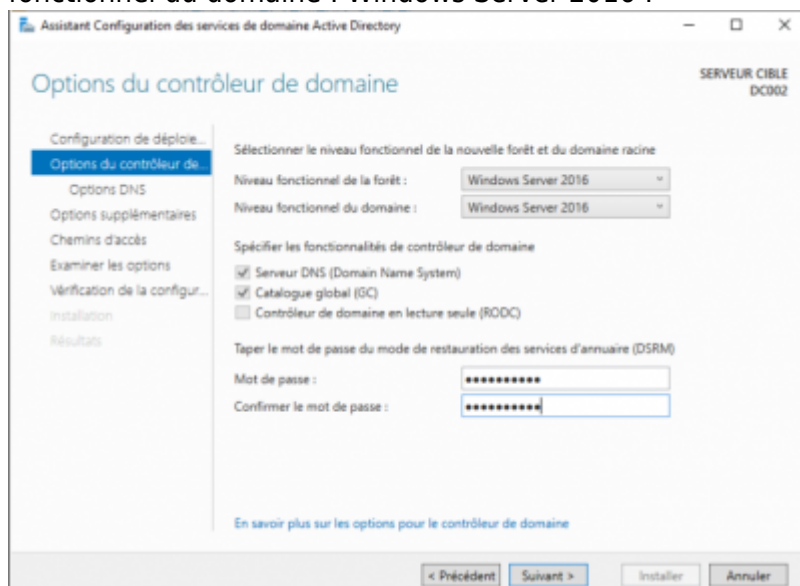
'attention' est apparu :



On clique sur “Promouvoir ce serveur en contrôleur de domaine”

Configuration du déploiement : on clique sur “Ajouter une nouvelle forêt”, on ajoute le nom de domaine racine : “oceanie.lan”

Option du contrôleur de domaine : Niveau fonctionnel de la forêt : Windows Server 2016; Niveau fonctionnel du domaine : Windows Server 2016 :



On fait suivant et on installe, le serveur reboot.

On doit maintenant créer des utilisateurs. On va dans “Utilisateurs et ordinateurs Active Directory”. On clique droit sur oceanie.lan, puis sur “nouveau”, puis sur “Unité d'organisation”. On lui donne le nom de 'Employés'.

On fait clique droit sur le répertoire 'Employés' maintenant apparu, clique sur nouveau, puis sur utilisateur et on crée quelques utilisateurs.

Windows Client

Pour vérifier notre configuration de Windows Server nous devons créer deux machines clientes sous Windows 10, une sur le LAN, l'autre sur la DMZ.

Il faut créer les VMs dans Proxmox, pour cela on télécharge l'ISO de Windows 10. Puis on procède de la même manière que pour l'installation de Windows Server à l'exception qu'on va mettre l'image ISO de Windows 10.

ATTENTION à bien mettre Windows 10 Professional !

Pour la machine sur la DMZ nous allons ajouter des règles de parefeu du côté DMZ :

Source	Destination	Port	Protocole
10.31.216.201	10.31.208.200	53	TCP/UDP
10.31.216.201	10.31.208.200	389	TCP/UDP
10.31.216.201	10.31.208.200	88	TCP
10.31.216.201	10.31.208.200	445	TCP
10.31.216.201	10.31.208.200	135	TCP
10.31.216.201	10.31.208.200	49152-65535	TCP

On se connecte avec le compte admin créé lors de l’installation : Login → admin ; Password → password

On modifie les paramètres IP de la machine :

LAN

Adresse IP : 10.31.208.201

Masque de sous-réseaux : 255.255.252.0

Passerelle par défaut : 10.31.211.254

Serveur DNS préféré : 10.31.208.200

DMZ

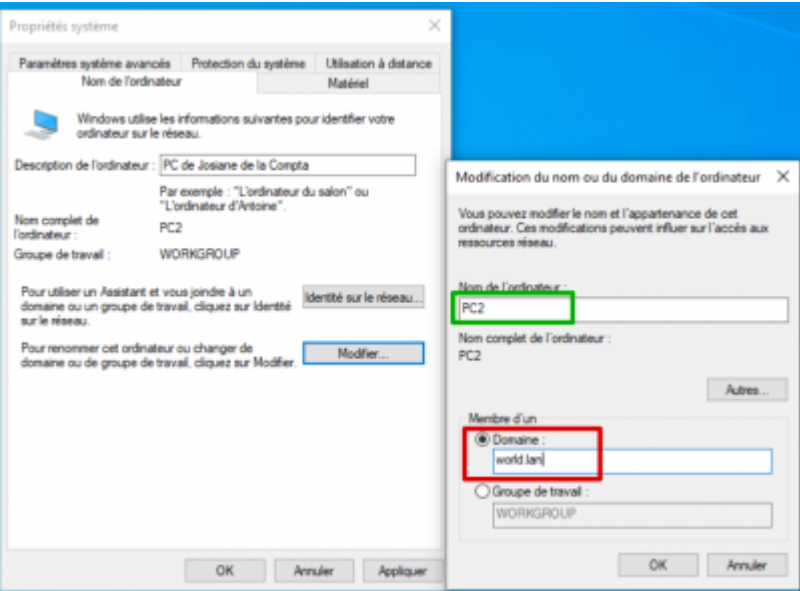
Adresse IP : 10.31.216.201

Masque de sous-réseaux : 255.255.252.0

Passerelle par défaut : 10.31.219.254

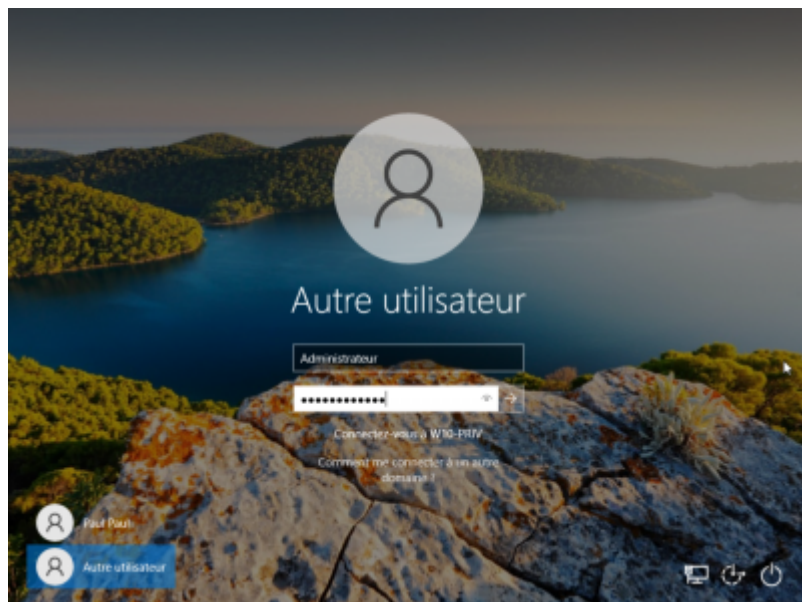
Serveur DNS préféré : 10.31.208.200

On change le nom de la machine ainsi que son nom de domaine :



On utilise le compte Administrateur de l’Active Directory pour autoriser l’ordinateur à se connecter au domaine.

Après reboot, sur l'interface d'authentification, on clique en bas à gauche sur “Autre utilisateur” et :



On entre les identifiants du compte Administrateur.

BRAVO !

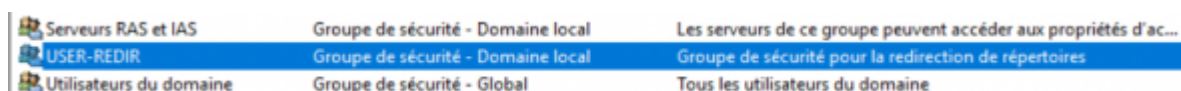
On peut faire la même chose avec les utilisateurs créés précédemment.

GPO

Nous allons mettre en place une solution GPO.

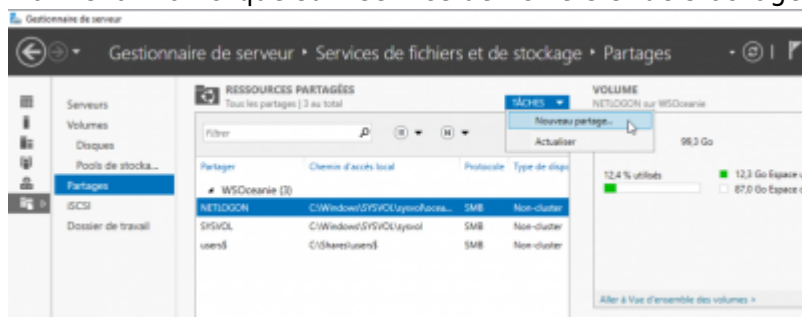
Sur le serveur on va créer des groupes de sécurité :

```
New-ADGroup -Name "USER-REDIR" `
-SamAccountName "USER-REDIR" `
-GroupCategory Security -GroupScope DomainLocal `
-Description "Groupe de sécurité pour la redirection derépertoires"
```



On ajoute les utilisateurs à ce groupe.

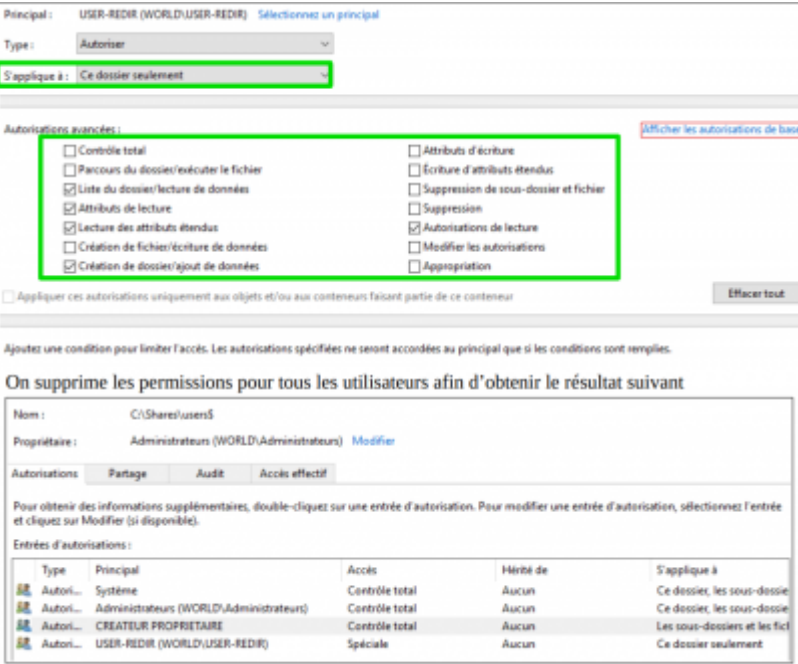
Maintenant on clique sur "service de fichiers et de stockage" puis sur "Partages" :



On clique sur SMB rapide, Nom du partage : users\$ et on ne modifie pas les chemins. On coche "Activer l'énumération basée sur l'accès", pour masquer les dossiers pour lesquels l'utilisateur n'a aucune permission.

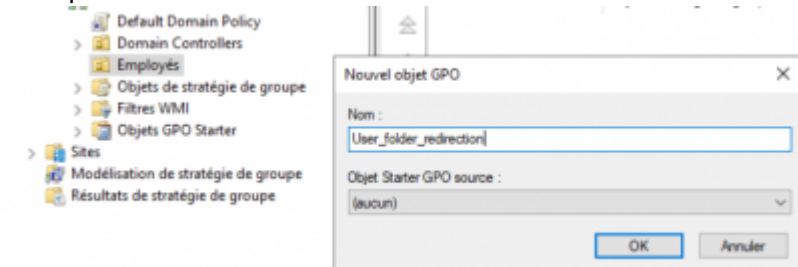
Ensuite on clique sur personnalisé les autorisations, puis sur désactiver l'héritage.

Ensuite on ajoute le groupe USER-REDIR :

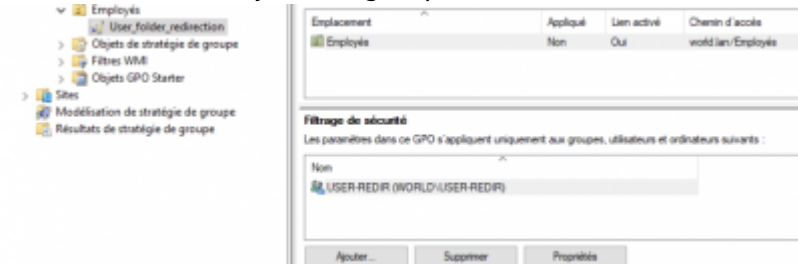


Suivant → Créer → Fermer

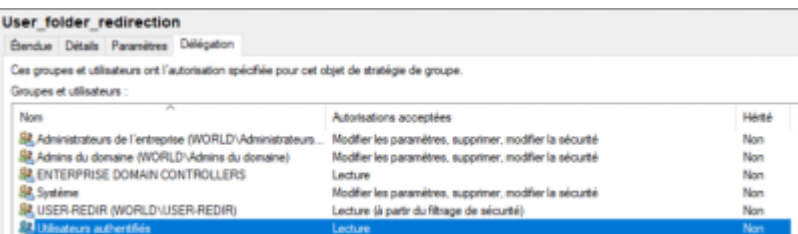
On ouvre maintenant l'application « Gestion de stratégie de groupe » Sur 'Employés' on fait clic droit pour créer une GPO :



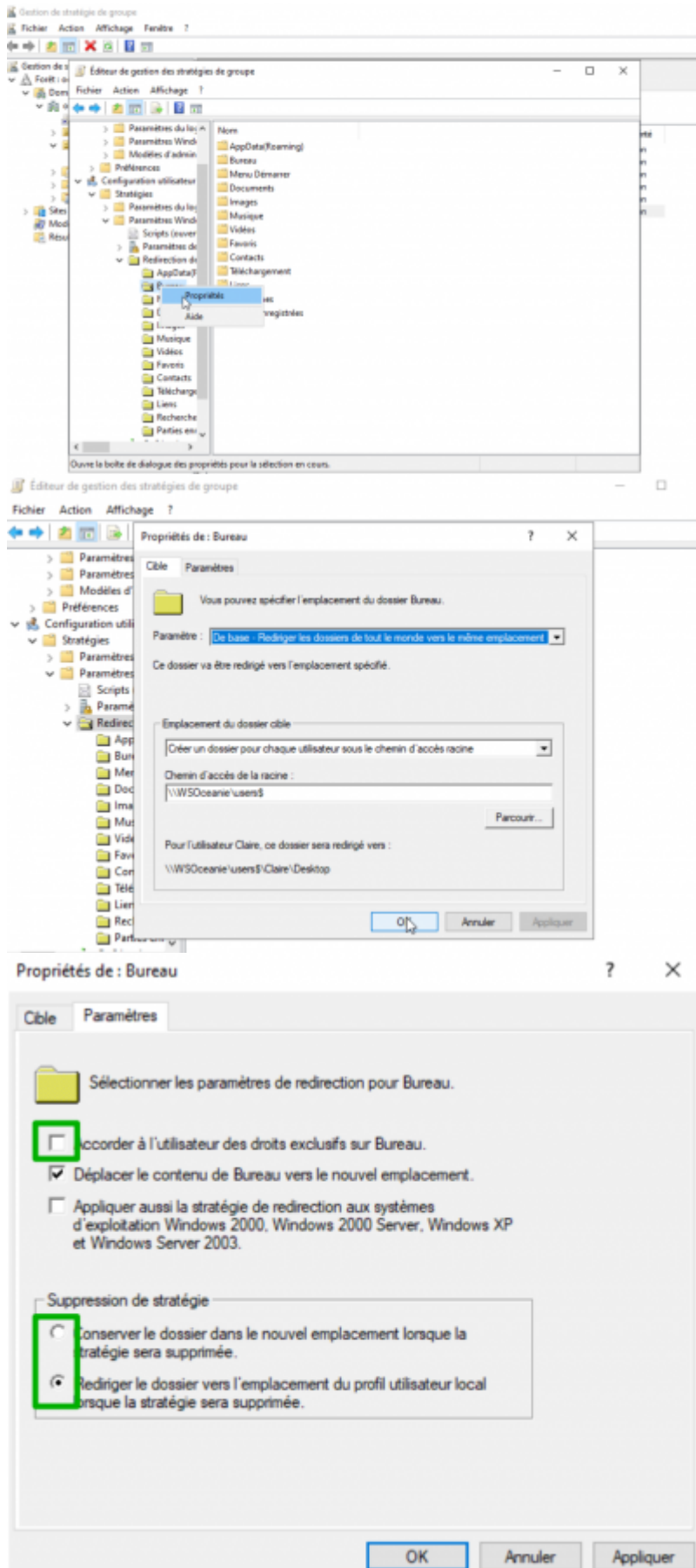
On Double-clique sur la GPO créée. Dans la zone « Filtrage de sécurité » on supprime les Utilisateurs authentifiés et on ajoute le groupe USER-REDIR :



On passe ensuite à l'onglet Délégation, on ajoute "Utilisateurs authentifiés" en "Lecture" uniquement :



Clic droit sur la GPO - Modifier, Utilisateurs → Stratégie → Paramètres Windows → Redirection de dossiers, Clic droit sur Bureau → Propriétés :



Cela permettra d'accéder à tout les fichiers et répertoires présent sur le bureau des utilisateurs.

Test

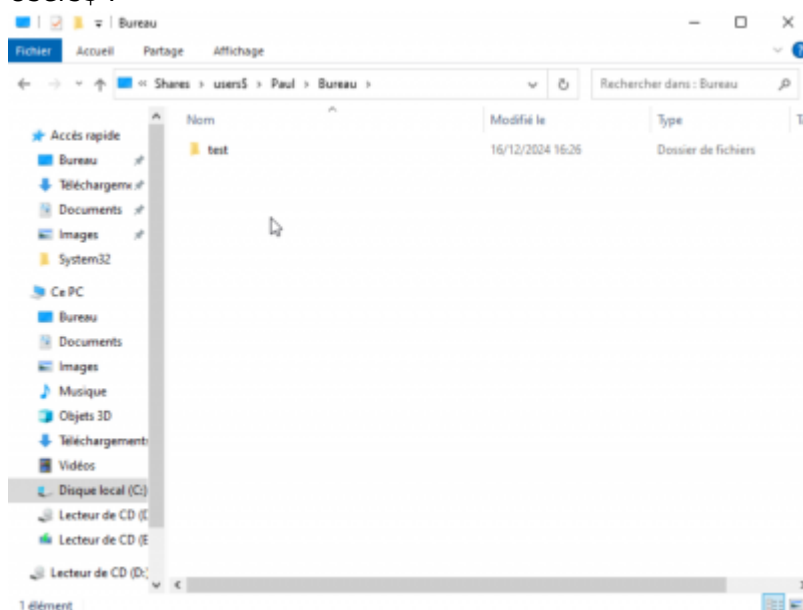
Sur un client on se connecte avec un compte utilisateur, on lance PowerShell :

```
gpupdate /force
```

On ferme la session, on se reconnecte, on crée un dossier sur le bureau :



On se rend sur notre serveur, on dans le gestionnaire de fichier. Ce PC → Disque local (C:) → Share → Users\$:



CELA MARCHE !

From:

<https://sisr2.beaupeyrat.com/> - **Documentations SIO2 option SISR**

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:mission14>

Last update: **2024/12/19 10:26**



