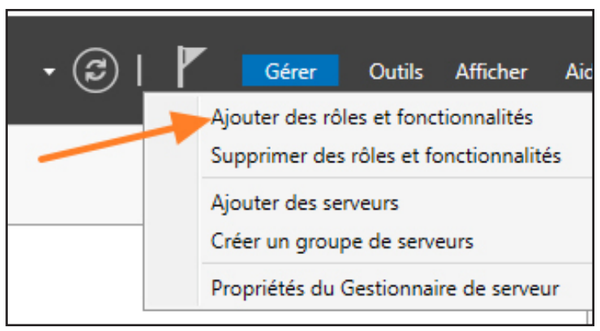
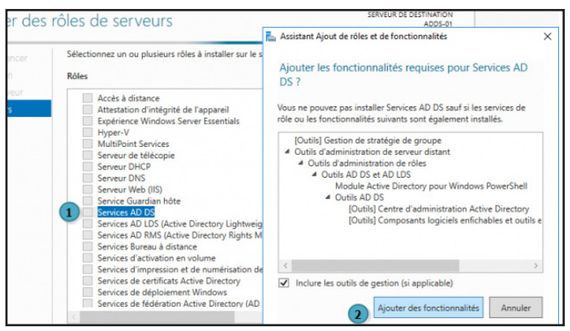
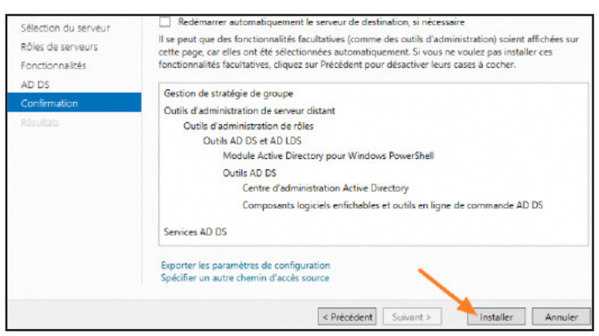
• **Installer et configurer Active Directory et DNS (intégré à AD) ;**

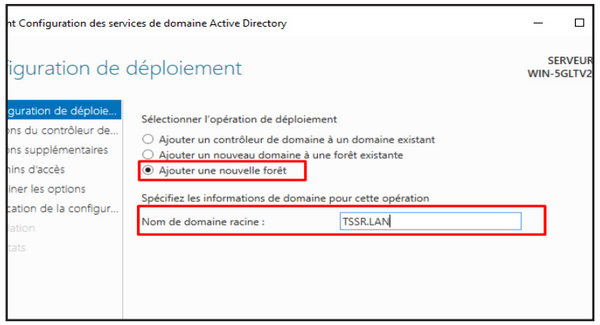
Pour installer Active Directory il faut installer le rôle ADDS, pour cela suivez la procédure suivante:

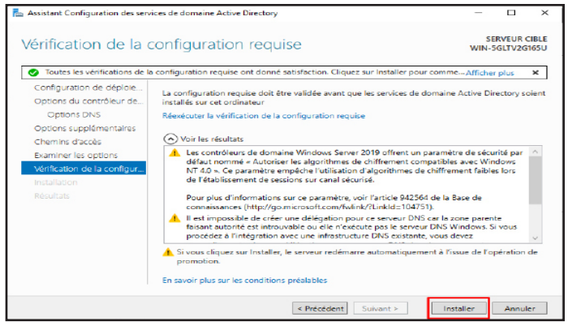






Creation de notre forêt et du domaine (online.tssr pour nous)

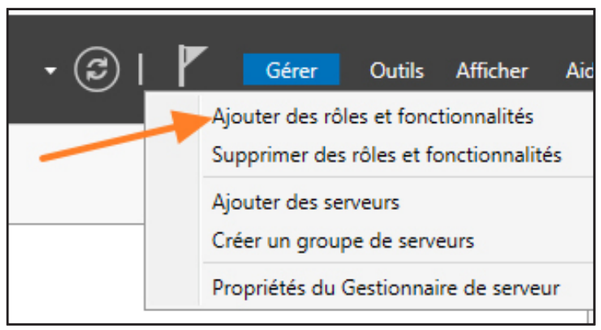


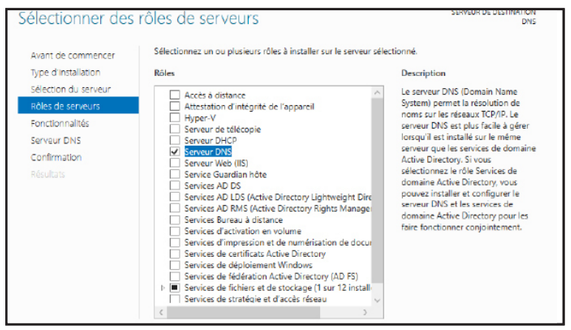


Il faut désormais promouvoir ce serveur en tant que contrôleur de domaine !

Installation du DNS

Pour installer le DNS, il faut ajouter le rôle «DNS» :





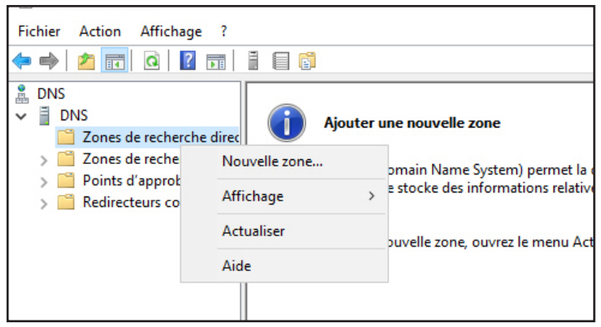
Terminer l'installation en acceptant toutes les propositions

Configurer les différentes zones DNS

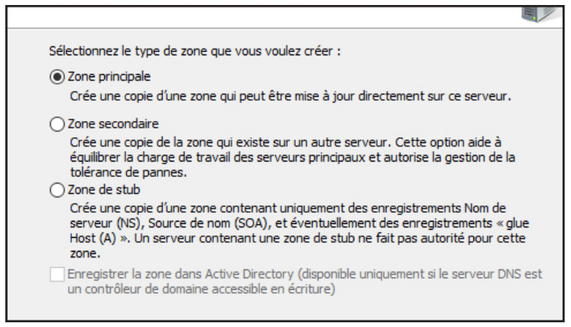
Il existe 2 zones DNS, les zones de recherche **directes** et les zones de recherche **inversées**

La zone de recherche **directe** permet de trouver l'adresse IP correspondant à un nom de domaine, tandis que la zone de recherche **inversée** permet de trouver le nom de domaine correspondant à une adresse IP.

Pour configurer les zones de recherches, RDV dans Outils --> DNS



Créer une Nouvelle Zone directe



Choisir Zone Principale

Ensuite il faut indiquer le nom de domaine de la zone (online.tssr dans notre cas).

Le serveur va alors générer un fichier contenant les informations de la zone. Cliquez simplement sur suivant

Autorisez les mises à jour de votre zone afin que les nouveaux hôtes puissent s'y ajouter.

Terminez la configuration

Configurer les différentes zones DNS

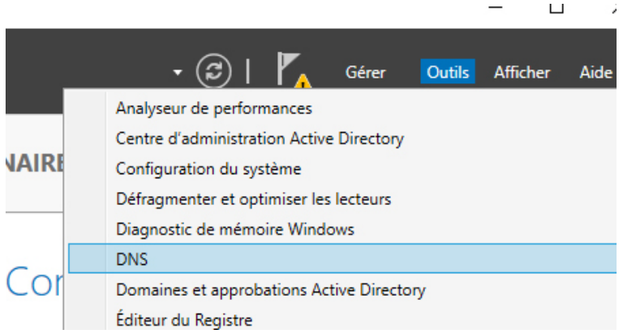
Il existe 2 zones pour le DNS:

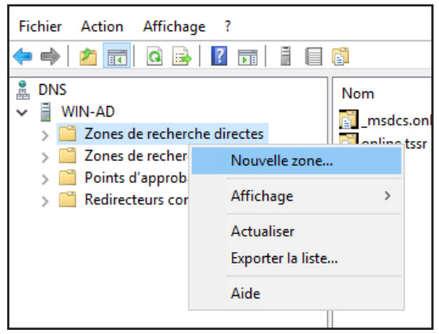
Les zones de recherches directes sont utilisées pour résoudre les noms de domaines en adresses IP. Elles sont constituées d'un ensemble d'enregistrements DNS qui mappent les noms de domaines aux adresses IP.

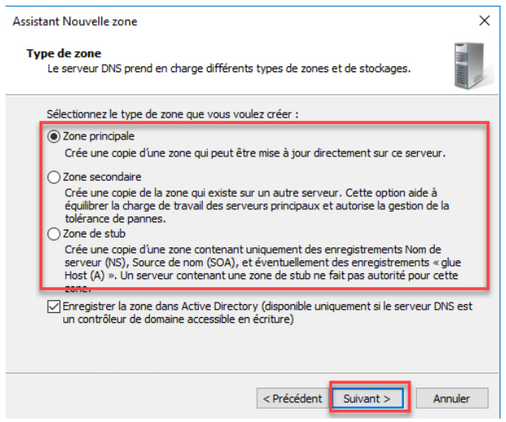
Les zones de recherches inversées sont utilisées pour résoudre les adresses IP en noms de domaines. Elles sont constituées d'un ensemble d'enregistrements DNS qui mappent les adresses IP aux noms de domaines.

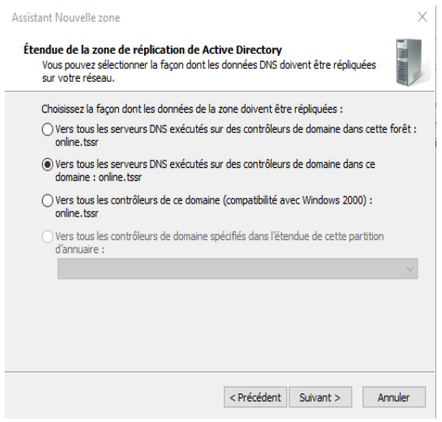
Pour résoudre le nom de domaine www.example.com en adresse IP, le client DNS utilisera une zone de recherche directe. Pour résoudre l'adresse IP 192.168.1.1 en nom de domaine, le client DNS utilisera une zone de recherche inversée.

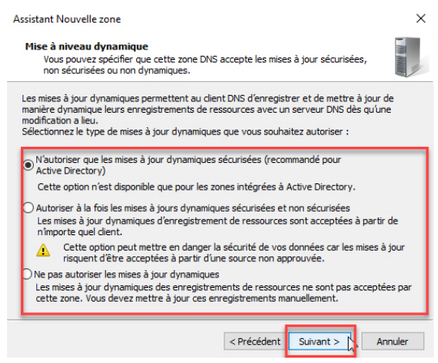
Suivre la configuration pour configurer la zone de recherche directe:









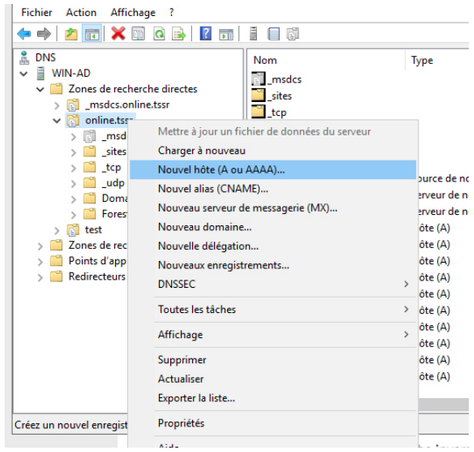


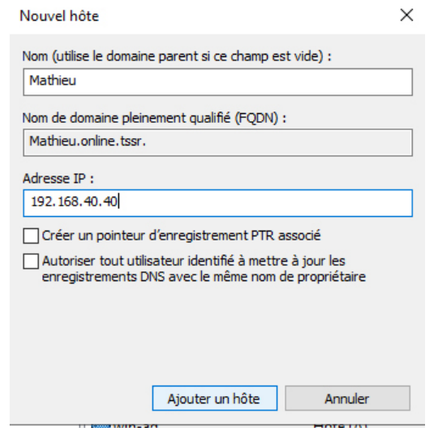
Confirmer la création de la zone DNS

La zone est maintenant créée et disponible dans la console Gestionnaire DNS.

Configuration de la zone de recherche **directe**

Créer un nouvel hôte





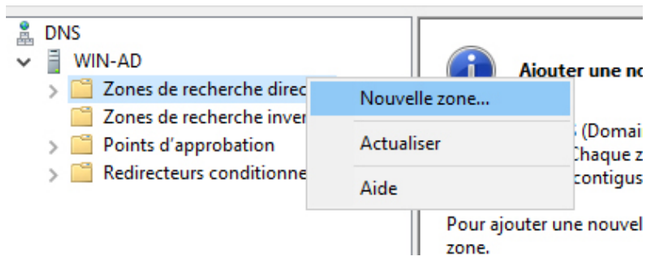
Maintenant l'hôte «Mathieu» a été ajouté, essayons de ping le pc «Mathieu» pour voir si la «traduction» ce fait.
Pour ce faire il faut dans l'invité de commande entrer le nom FQDN de Mathieu soit «Mathieu.online.tssr»

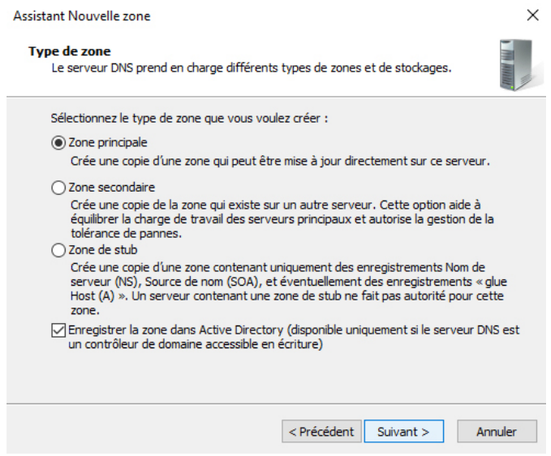
```
C:\Users\Administrateur>ping Mathieu.online.tssr

Envoi d'une requête 'ping' sur Mathieu.online.tssr [192.168.40.40] avec 32 octets de données :
Réponse de 192.168.40.40 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.40.40 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.40.40 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.40.40 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.40.40:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

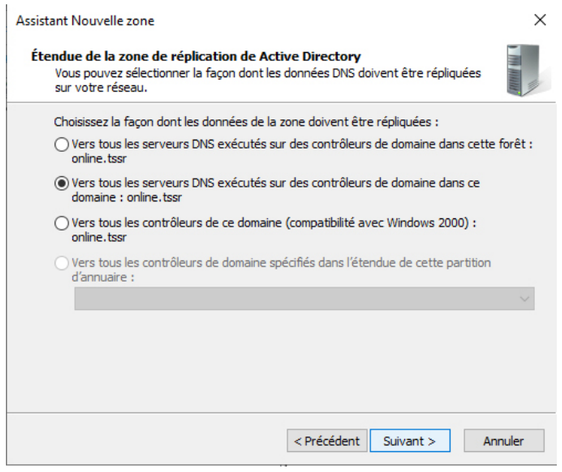
Le ping fonctionne donc la zone de recherche directe du DNS est en place !

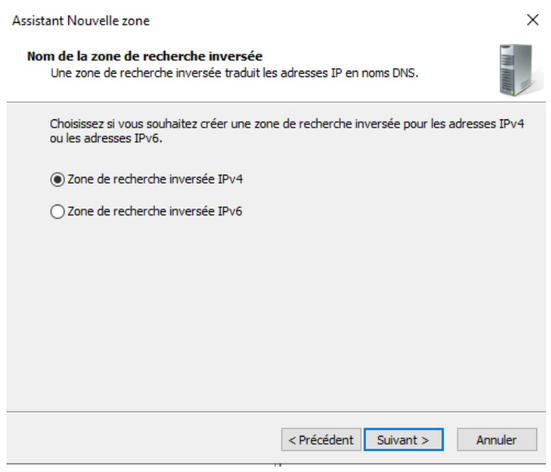
Configuration de la zone de recherche **inversée**

Suivre la configuration pour configurer la zone de recherche inversée:

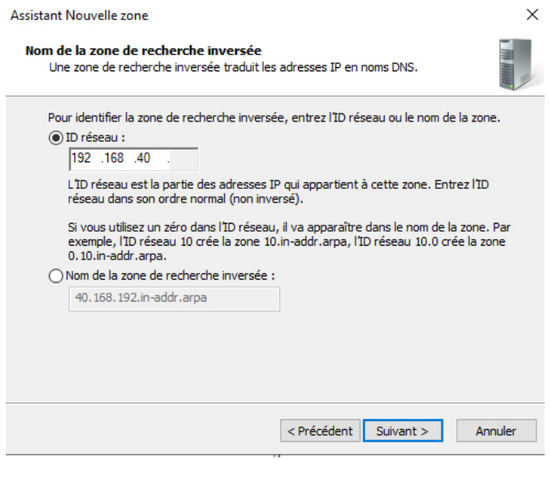


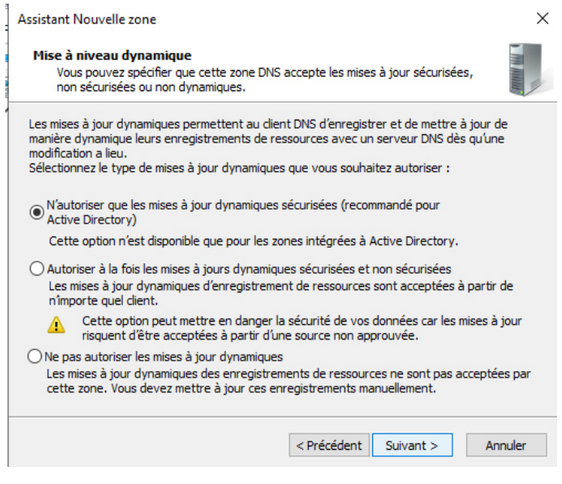




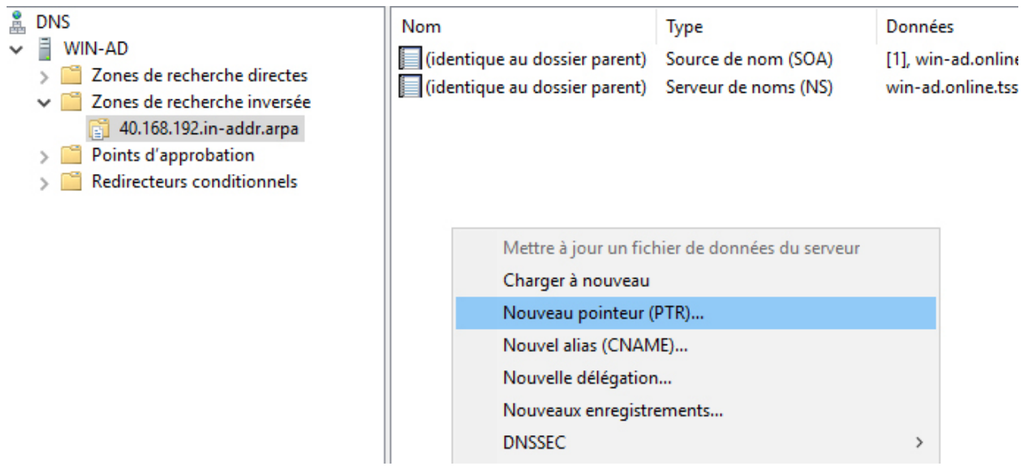


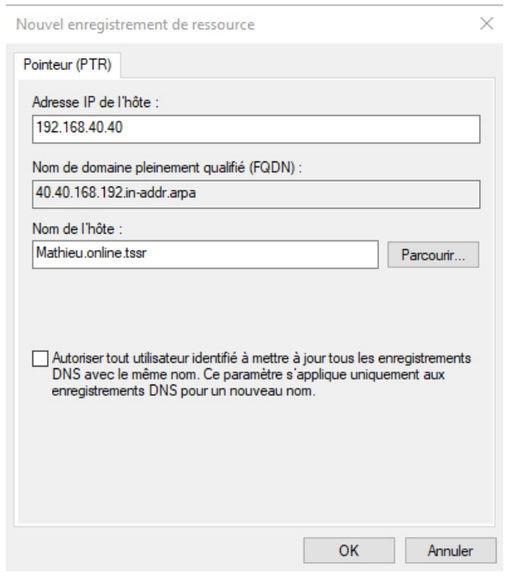
Entrez l'ip de votre partie réseau:



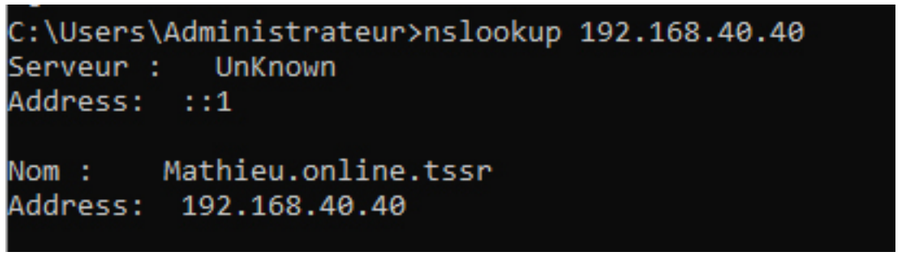


Création d'un nouveau pointeur (PTR)





Veillez à bien entrer le bon nom FQDN de l'hôte concerné, normalement la config en place on peut faire la commande «nslookup 192.168.40.40» pour trouver le nom du pc qui a l'ip 192.168.40.40



Ca marche !

Créer les 91 utilisateurs et les ajouter aux groupes correspondant grâce à un script en PowerShell

Voila notre script powershell:

```
$CSVFile = "C:\Utilisateurs.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding Default

Foreach($Utilisateurs in $CSVData){
 $UtilisateursPrénom = $Utilisateurs.Prénom
 $UtilisateursNom = $Utilisateurs.Nom
 $UtilisateursLogin = ($UtilisateursPrénom).Substring(0,1).ToLower() + "." + $UtilisateursNom.ToLower()
 $UtilisateursEmail = "$UtilisateursLogin@online.tssr"
 $UtilisateursMotDePasse = "TSSR01234"
 $UtilisateursSecteur = $Utilisateurs.Secteur

    if (Get-ADUser -filter {SamAccountName -eq $UtilisateursLogin})
    {
        write-warning "Vas te faire, il existe déjà"
    }
    else
Script pour créer des utilisateurs en masse sur Active Directory

    {
        New-ADUser  -Name "$UtilisateursNom $UtilisateursPrénom"
                    -DisplayName "$UtilisateurNom $UtilisateursPrénom"
                    -GivenName $UtilisateursPrénom
                    -Surname $UtilisateursNom
                    -SamAccountName $UtilisateursLogin
                    -UserPrincipalName "$UtilisateursLogin@online.tssr"
                    -EmailAddress $UtilisateursEmail
                    -Title $UtilisateursSecteur
                    -AccountPassword(ConvertTo-SecureString $UtilisateursMotDePasse -AsPlainText -Force)
                    -ChangePasswordAtLogon $true
                    -Enabled $true

        Write-Output "Création de l'utilisateur : $UtilisateursLogin ($UtilisateursNom $UtilisateursPrénom)"
    }

}
```

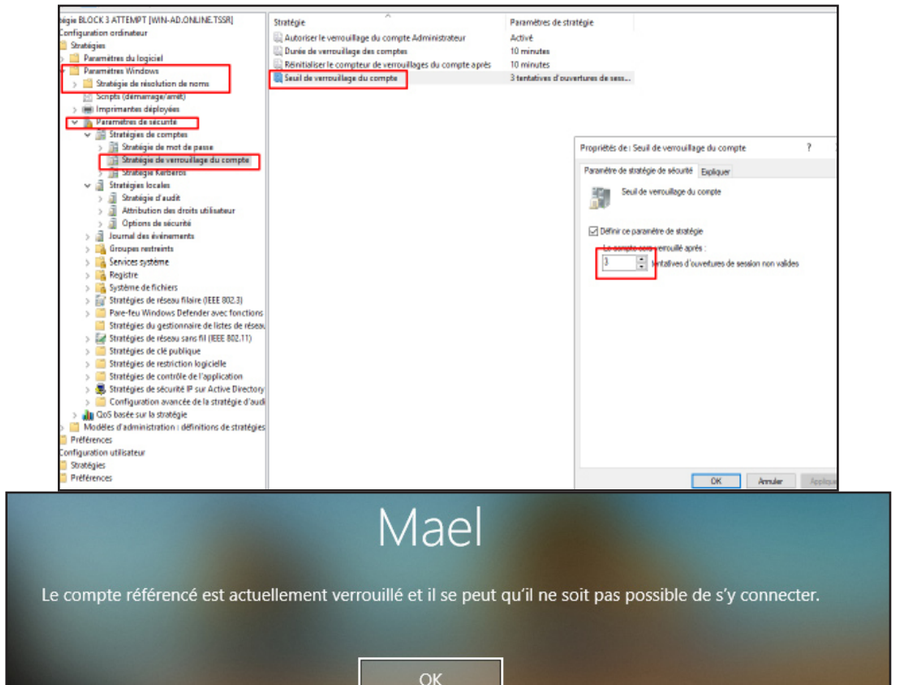
Basé sur ce fichier csv

```
Prénom;Nom;Secteur
Ethan;Ahmed;Ingénieur P1
Hayden ;Kent;Ingénieur P1
Spencer;Bradley;Ingénieur P1
Charlie;Epps;Ingénieur P1
Gregory;Ashton;Ingénieur P1
Emma;Rowe;Ingénieur P1
Kian;Heney;Ingénieur P1
Sophie;Laurent;Ingénieur P1
Lola;Diesel;Ingénieur P1
Léo;Daguant;Ingénieur P2
Kim;Kardachiante;Ingénieur P2
Frederic;Molas;Ingénieur P2
Abdou;Abdou;Ingénieur P2
Antoine ;Daniel;Ingénieur P2
Horty;Capique;Ingénieur P2
Bob;L'éponge;Ingénieur P2
Oui;Oui;Ingénieur P2
Jimmy;Neutron;Ingénieur P2
Vin;Gasouale ;Ingénieur P2
Mathieu;Coutinho;Service Informatique
Benjamin;Brun;Service Informatique
Elon;Musk;Service Informatique
Elliot ;Alderson;Service Informatique
Denis ;Echeverri;Directeur Général
```

Réduire Utilisateurs.csv 1 Ko

Un compte doit être bloqué au bout de 3 tentatives de connexion échoués

Pour bloquer un compte au bout de 3 tentatives de connexions échoués, il faut créer 1 GPO. Cette GPO ce trouve ici: (il est préferable d'appliquer cette GPO sur le domaine entier comme ça tous les postes sont répertorié car la GPO s'applique sur les ordinateurs)

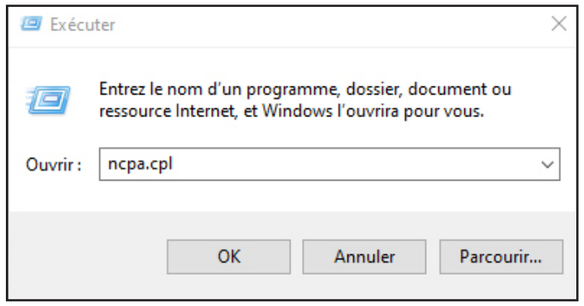


(Voir la suite du doc pour appliqué des GPO)

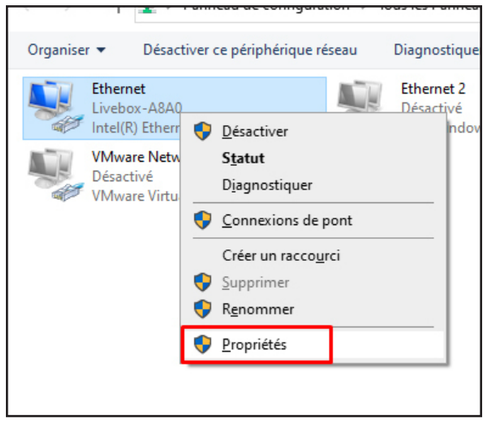
Intégrer un poste client au domaine

Pour intégrer un poste au domaine, il faut d'abord aller dans les paramètres réseaux pour changer son DNS et mettre celui de l'AD.

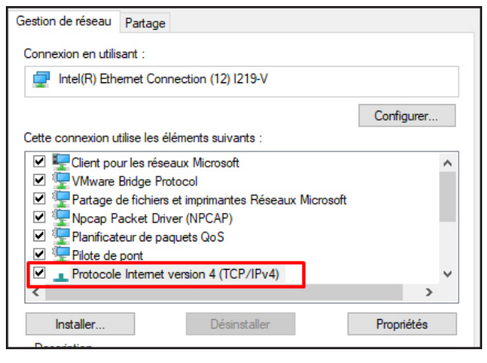
Pour cela tapez le raccourci Touche Windows + R et tapez ncpa.cpl

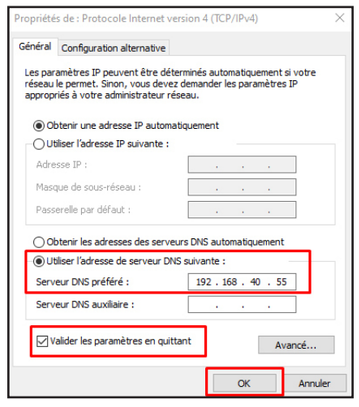


Sélectionner votre carte réseau et faites propriétés



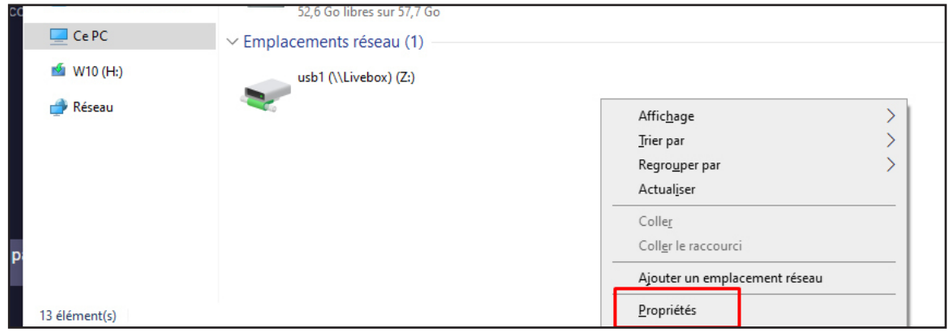
Double cliquer sur la zone rouge



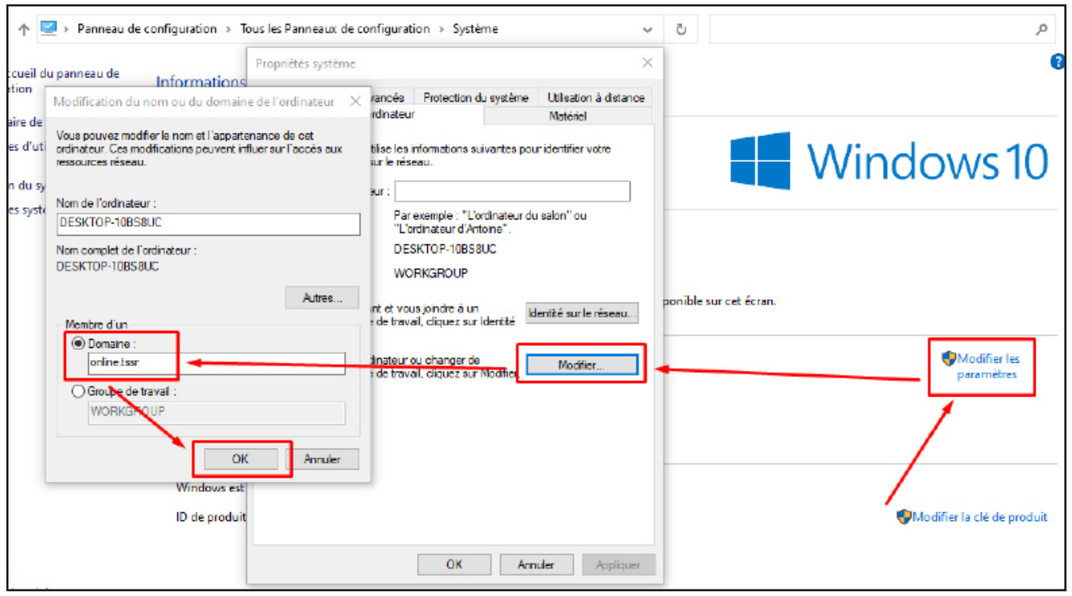


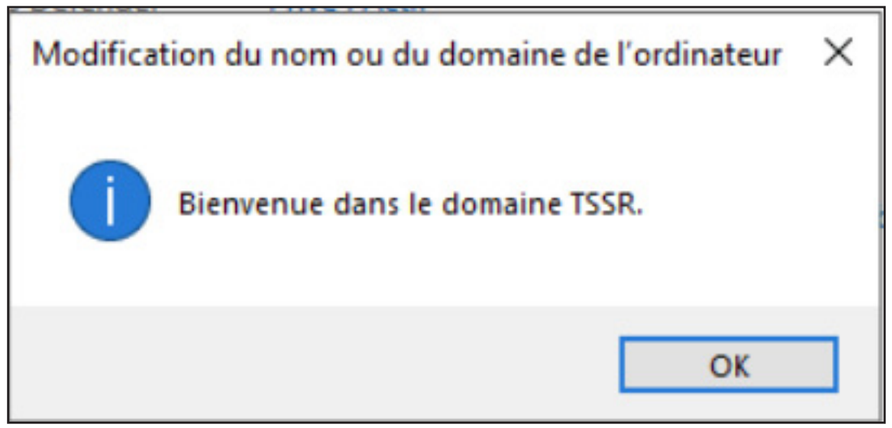
Entrez l'IP du contrôleur de domaine (dans le cas ou c'est lui qui est DNS) dans la partie DNS puis validez

Ensuite ouvrez l'Explorateur de fichiers puis Ce PC et faites un clique droit dans la partie blanche puis Propriétés:



Suivre la capture d'écran ci-dessous



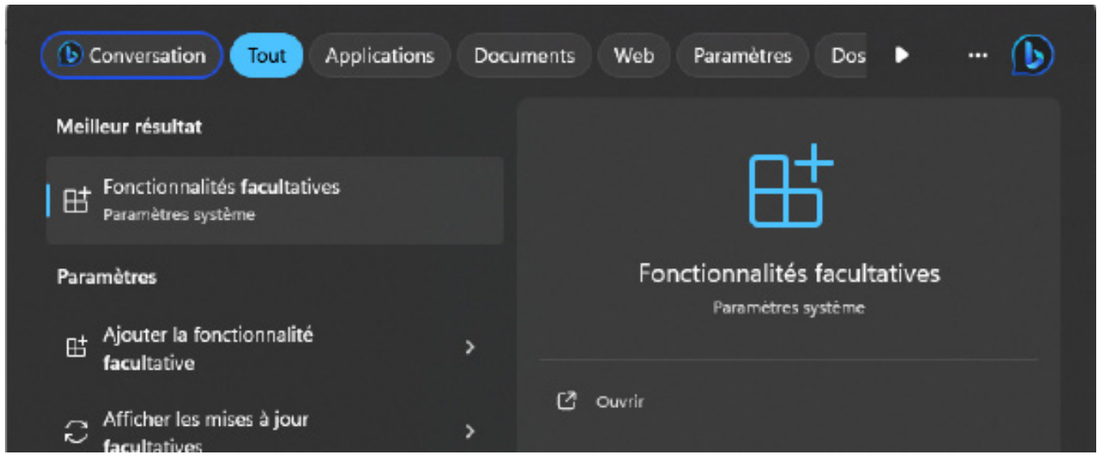


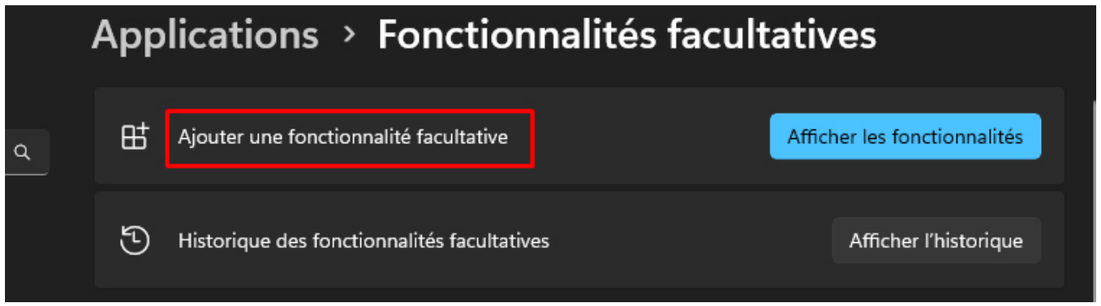
ET VOILA !!

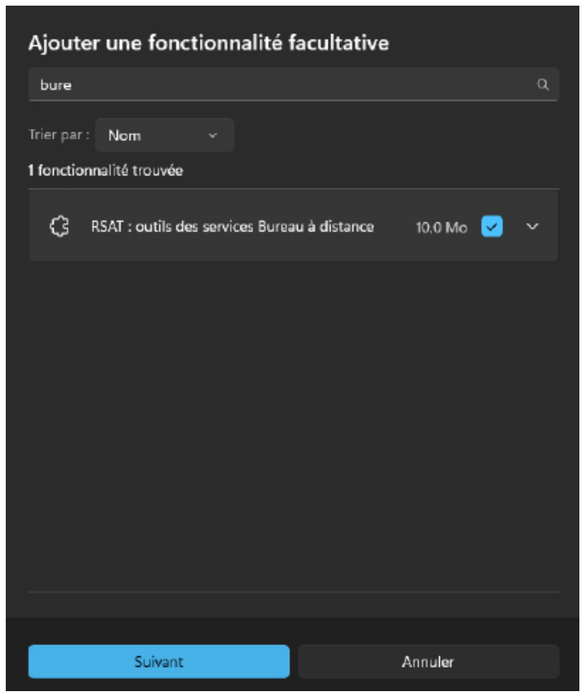
Installer les outils RSAT sur un poste client afin de pouvoir gérer vos serveurs à distance

Pour installer les Outils RSAT, il faut une version de Windows Pro ou Enterprise

Allez dans Fonctionnalités facultatives







Installer et configurer un serveur DHCP avec PowerShell

Installer la fonctionnalitée DHCP pour cela entrer la commande suivante:

Install-WindowsFeature DHCP -IncludeManagementTools

Autoriser le DHCP au niveau de l'AD

Add-DHCPServerInDC -DNSName WIN-AD.online.tssr

Création de l'option du DNS Server ainsi que la Passerelle par défaut qui sera attribué

Set-DhcpServerv4OptionValue -DNSServer 192.168.40.55 -DNSDomain online.tssr -Router 192.168.40.254

Création du Pool «vlan40»:

Add-DhcpServerv4Scope -Name «LAB-vlan40» -StartRange 192.168.40.190 -EndRange 192.168.40.200 -SubnetMask 255.255.255.0 -Description «Plage DHCP vlan40»

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Install-WindowsFeature DHCP -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Serveur DHCP, Outils du serveur DHCP}


PS C:\Users\Administrateur> Add-DHCPServerInDC -DNSName WIN-AD.online.tssr
AVERTISSEMENT : Le serveur DHCP win-ad.online.tssr avec l'adresse IP 10.10.10.1 est déjà autorisé dans Active
Directory. La vérification d'autorisation a été engagée sur le serveur DHCP.
PS C:\Users\Administrateur> Set-DhcpServerv4OptionValue -DNSServer 192.168.40.55 -DNSDomain online.tssr -Router 192.168.
40.254
PS C:\Users\Administrateur> Add-DhcpServerv4Scope -Name "LAB-vlan40" -StartRange 192.168.40.190 -EndRange 192.168.40.200
 -SubnetMask 255.255.255.0 -Description "Plage DHCP vlan40"
Add-DhcpServerv4Scope : Échec de l'ajout de l'étendue 192.168.40.0 au serveur DHCP WIN-AD.
Au caractère Ligne:1 : 1
+ Add-DhcpServerv4Scope -Name "LAB-vlan40" -StartRange 192.168.40.190 - ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (192.168.40.0:root/Microsoft/...cpServerv4Scope) [Add-DhcpServerv4Scope]
   , CimException
    + FullyQualifiedErrorId : DHCP 20052,Add-DhcpServerv4Scope

PS C:\Users\Administrateur> Add-DhcpServerv4Scope -Name "LAB-vlan40" -StartRange 192.168.40.190 -EndRange 192.168.40.200
 -SubnetMask 255.255.255.0 -Description "Plage DHCP vlan40"
PS C:\Users\Administrateur>
```

Le DHCP est bien configuré avec un Pool pour notre VLAN40, si on veut utiliser le DHCP pour qu'il puisse attribuer des adresses aux hôtes, il faut sur pfSense indiquer le serveur comme DHCP Relay !

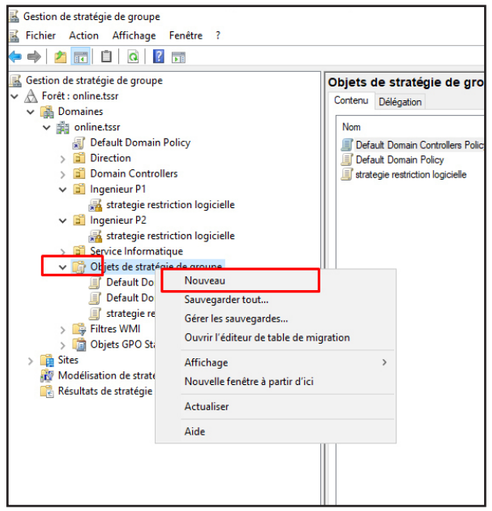
Stratégies spécifiques :

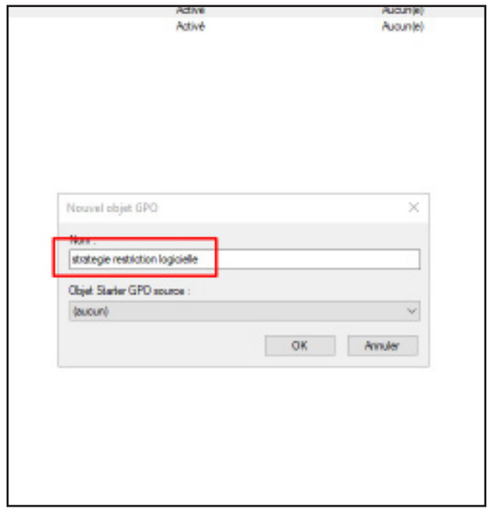
- En dehors de la direction et du service informatique, personne ne peut installer de logiciels sur sa machine ni modifier l'heure ;

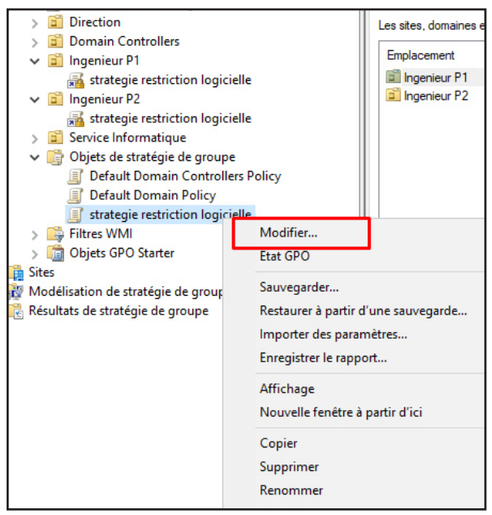
Dans notre cas, pour que seuls la direction et le service informatique puissent installer des logiciels, il faut créer une GPO qui interdit l'installation de logiciels sur les UO «Ingenieur P1» et «Ingenieur P2»

Afin d'éviter toute mauvaise application de la stratégie de groupe, on va la créer dans conteneur Objets de stratégie de groupe et ensuite la lier à l'OU que l'on souhaite l'appliquer.

Depuis la console Gestion de stratégie de groupe, faire un clic droit sur le dossier Objets de stratégie de groupe et cliquer sur Nouveau et suivre les étapes suivantes:

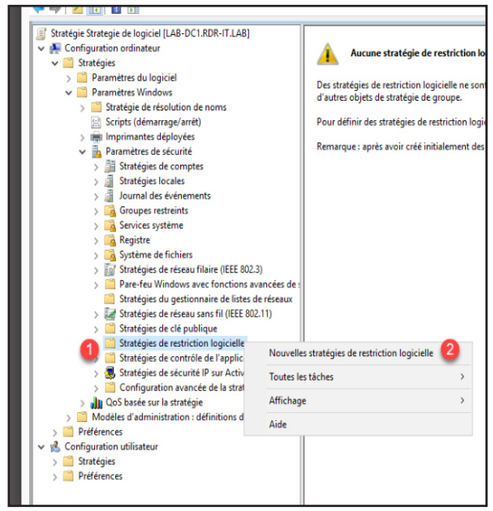


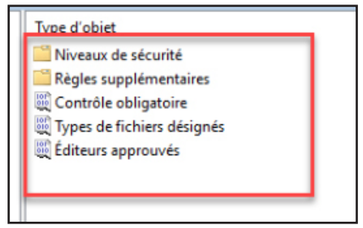




Configuration de la stratégie de restriction logicielle

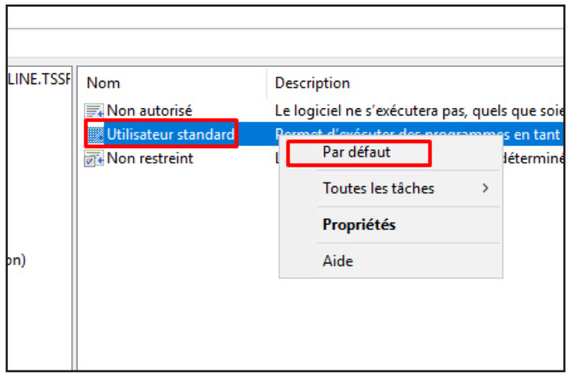
Depuis l'éditeur de gestion des stratégies de groupe, aller à l'emplacement : Configuration utilisateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de restriction logicielle et créer une Nouvelles stratégies de restriction logicielles





Après avoir cliqué sur Nouvelles stratégies de restriction logicielle, on peut voir que des éléments ont été ajoutés dans la stratégie.

Sur niveau de sécurité , on retrouve le comportement de la stratégie de restriction logicielle, par défaut la configuration est non restreint (on peut voir la sélection en bas à gauche sur l'icône). Ce que l'on va faire c'est passer en Utilisateur standard pour activer le blocage.

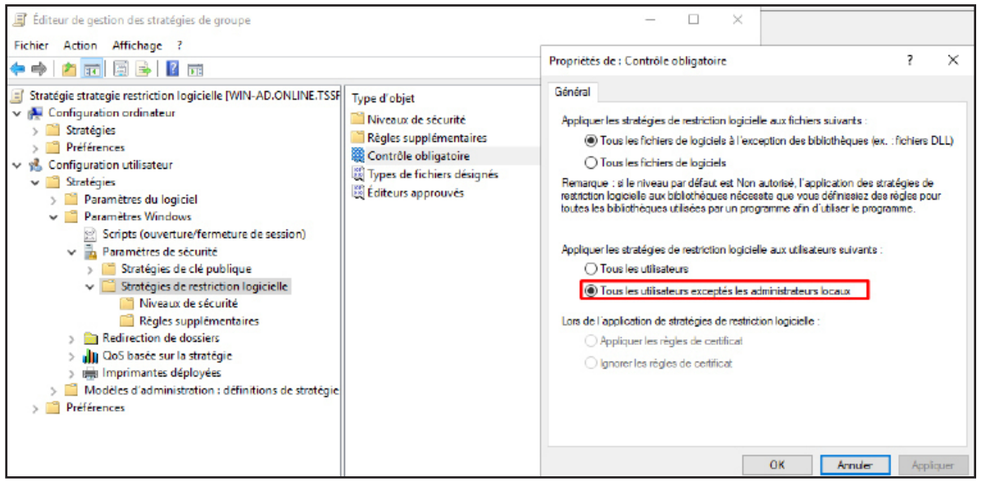


Maintenant que le blocage est activé, deux exceptions ont été créé pour permettre l'exécution des programmes dans le dossier Règles supplémentaires (normalement on a pas besoin d'y toucher mais si on rencontrez des problèmes pour lancer des programmes lors des tests, ajouter les chemins suivant :

– C:\Program Files (x86)
– C:\Program Files
– C:\Windows

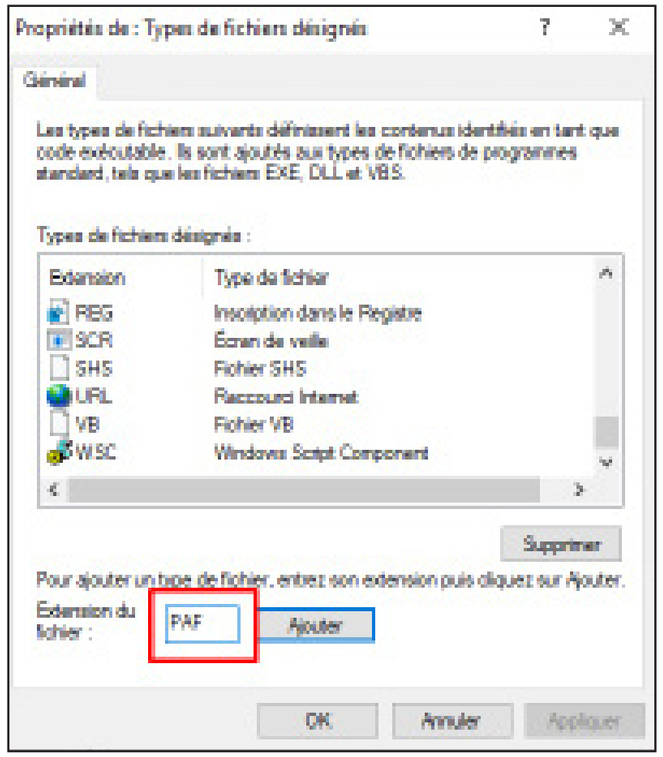
Retourner sur le dossier Stratégies de restriction logicielle, on va continuer d'affiner la configuration.

Cliquer sur Contrôle obligatoire, on va exclure les administrateurs locaux de la stratégie



Ouvrir ensuite la propriété : Types de fichiers désignés.

Ici on peut configurer les extensions des fichiers bloqués.



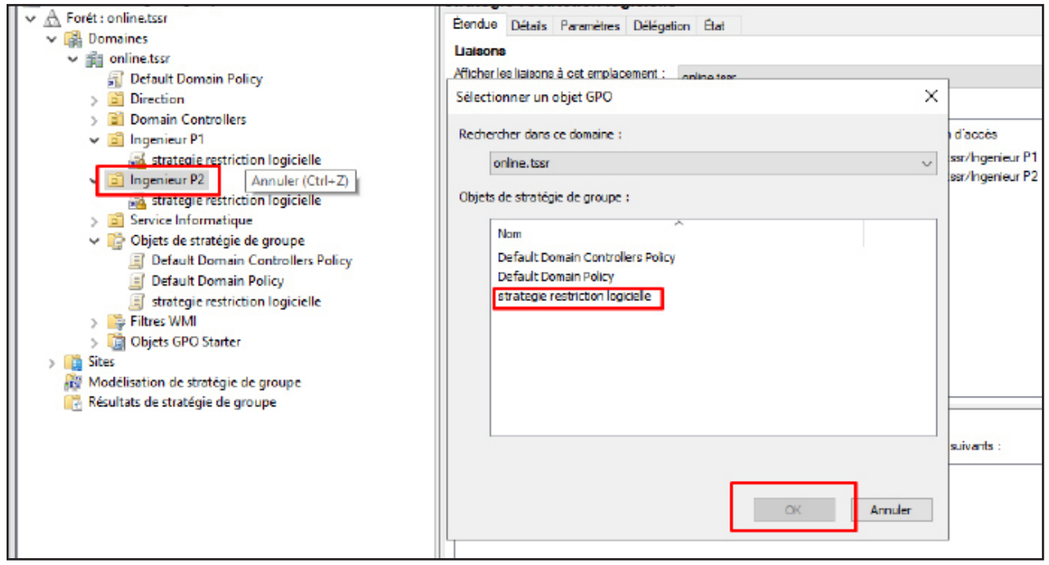
Bloquer l'extension .PAF permet d'empêcher l'exécution d'application portable

La stratégie de groupe est prête.

Lier la stratégie de groupe à l'OU

Maintenant il ne reste plus qu'à lier la stratégie de groupe à UE où celle-ci doit s'appliquer.

Dans Gestion de stratégies de groupes faire un clic droit sur l'UE Ingenieur P1 et Ingenieur P2 et cliquer sur Lier un objet de stratégie de groupe existant et choisir la GPO «stratégie de restriction logicielle»

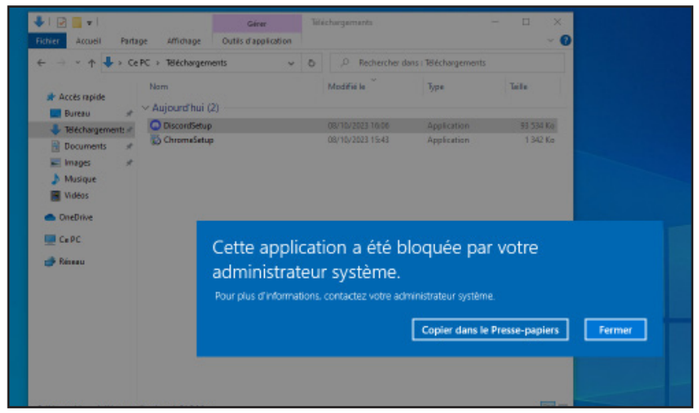


Pour rappel, la stratégie a été configurée au niveau Utilisateur, je lie donc la stratégie à une OU qui contient les utilisateurs.

Ne pas oublier d'activer la GPO (clique droit -> Activé)

Tester la stratégie de restriction logicielle

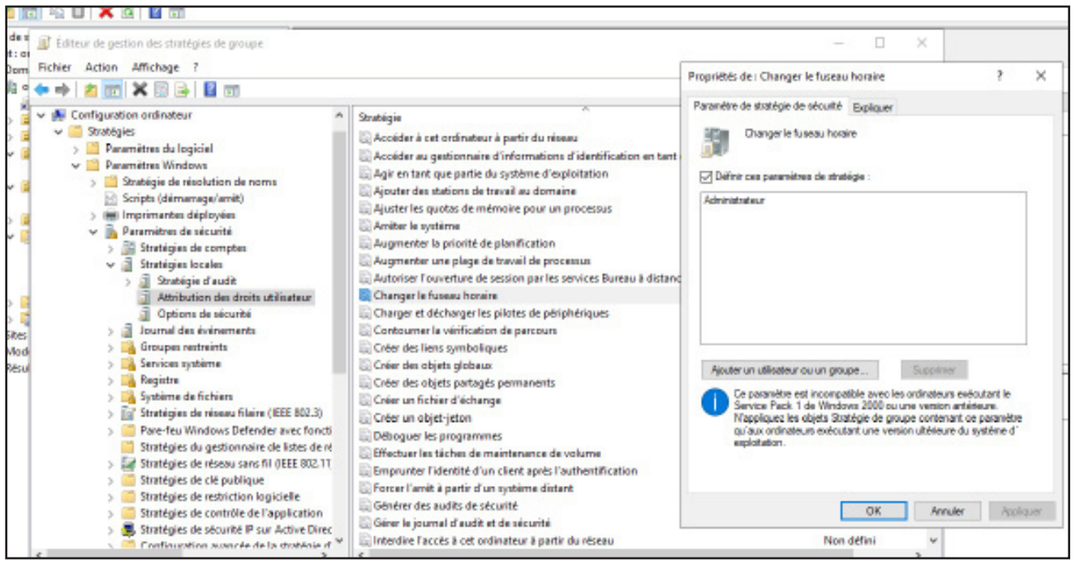
Pour tester je vais simplement me connecter à un utilisateur de l'UE «Ingénieur P1» et tenter d'installer une application



Voilà, il est impossible d'exécuter un fichier ce qui veut dire que la GPO s'applique bien.

Pour empêcher les utilisateur des 2 UO de modifier l'heure il faut simplement ajouter une option à la GPO qui indique que personne ne peut modifier l'heure pour cela suivez la procédure:

Dans gestion des stratégies de groupe, développez Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attributions des droits d'utilisateurs
Double-cliquez sur Changer le fuseau horaire
Dans la fenêtre cocher le paramétre «Définir ces paramètres de stratégies» et ajouter uniquement l'Administrateur pour qu'il soit le seul autorisé à modifier l'heure.



Vue que c'est une GPO qui concerne la configuration de l'ordinateur, il est nécessaire d'ajouter les postes sur lesquels seront les utilisateurs de l'UE pour que cela fonctionne.

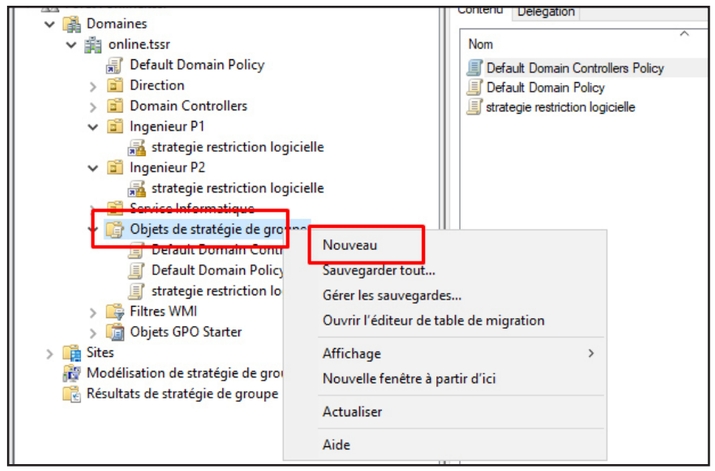
A savoir, pour appliquer un GPO instantanément pensez à la commande gpupdate /force

Les lecteurs CD et USB sont désactivés sur tous les postes informatiques, sauf pour le service informatique

Maintenant que nous avons déjà fais une première GPO ensemble je vais moins détailler la procédure.

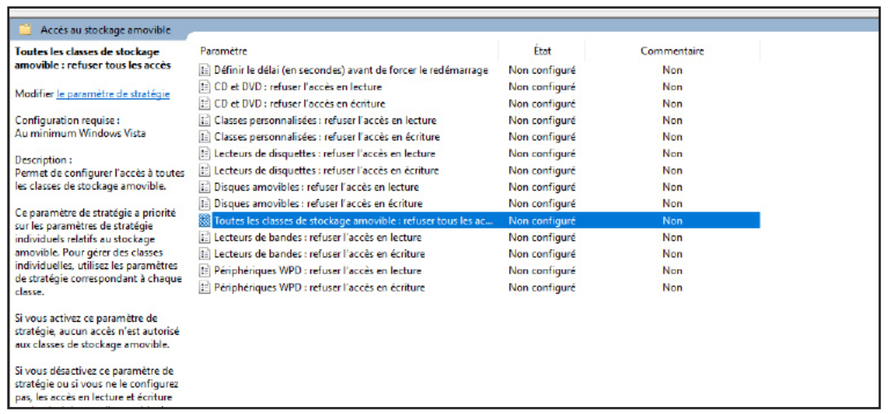
Notre GPO sera appliquée sur les UO Ingenieur P1 et P2 ainsi que la direction.

Pour créer la GPO Rendez-vous dans la Gestion de stratégies de groupes et créer une nouvelle stratégie et la nommer «BLOCK USB CD»



Pour paramétrer la GPO, Suivre le chemin suivant: Configuration utilisateur -> Stratégies -> Modèles d'administration -> Système -> Accès au stockage amovible

Choisir cette option et activez là:



Normalement tous les types de stockages amovibles ne sont pas autorisé et la GPO fonctionne.

Pour tester connecter une clé usb sur un pc d'un utilisateur des UO concernées et devrait apparaître une erreur

Le panneau de configuration ne doit pas être accessible sur le poste des salariés qui ne font pas partie du service informatique

Maintenant que le principe des GPO est bien assimilée, je vais juste me concentrer sur le paramètre des GPO.

Nous allons agir sur les UO suivantes: Ingenieur P1 et P2 et la Direction.

Il faut créer une nouvelle GPO puis parcourez les paramètres comme ceci : Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration.

Et là il faut choisir le paramètre «Interdire l'accès au Panneau de configuration et l'application Paramètres du PC»

Il suffit de double-cliquer sur ce paramètre et de l'activer.

Il suffit juste de lier la GPO sur les UO concernées

Si la GPO s'applique voilà le message qui est censé apparaître

Seul les membres du service informatique doivent être « Administrateur Local » de la machine

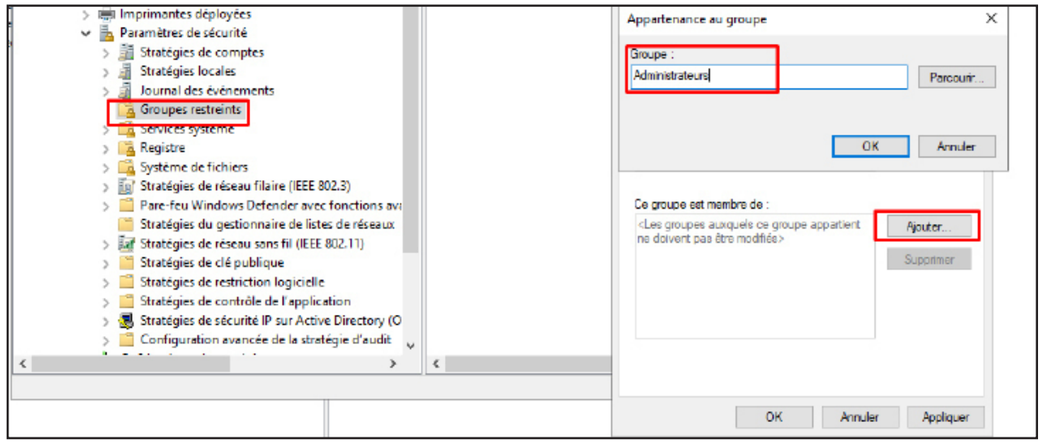
Pour cette GPO, il faut que les postes des utilisateurs soient bien répertoriés dans les UO, car elle agit sur la configuration de l'ordinateur.

Les UO concerné par cette GPO seront Ingenieur P1 et P2 ainsi que la Direction.

Pre-requis: créer un groupe dans l'UE du service informatique et la nommez Admin locaux

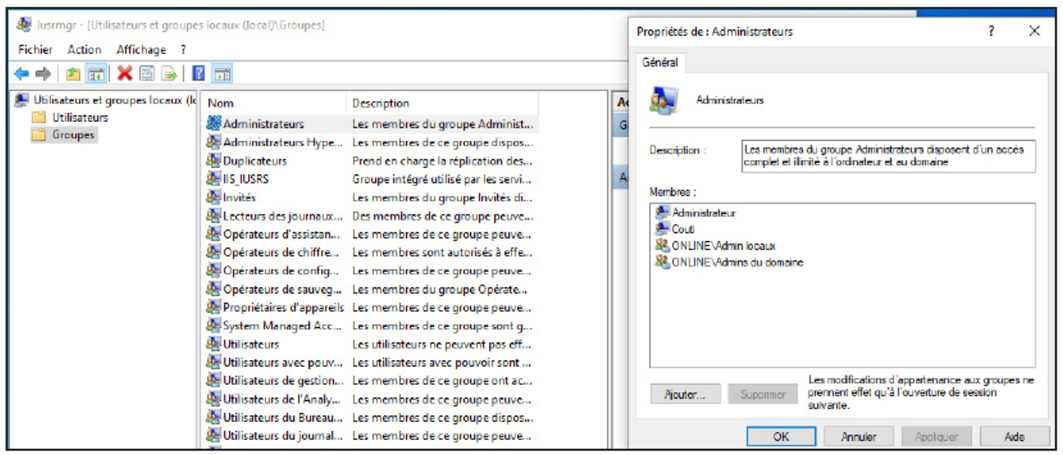
Il faut créer une nouvelle GPO puis parcourez les paramètres comme ceci : Configuration de l'Ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Groupes restreints puis Ajouter un groupe

Ajouter le groupe crée précédemment et spécifié que ce groupe est membre du groupe Adminstrateurs NE PAS OUBLIER LE «S» (pour faire simple le groupe qu'on a crée sera Administrateur local des postes)



La stratégie est terminée maintenant il faut la lier aux UO concernées

Après ça on verifie sur un utilisateur d'une UO concernées:



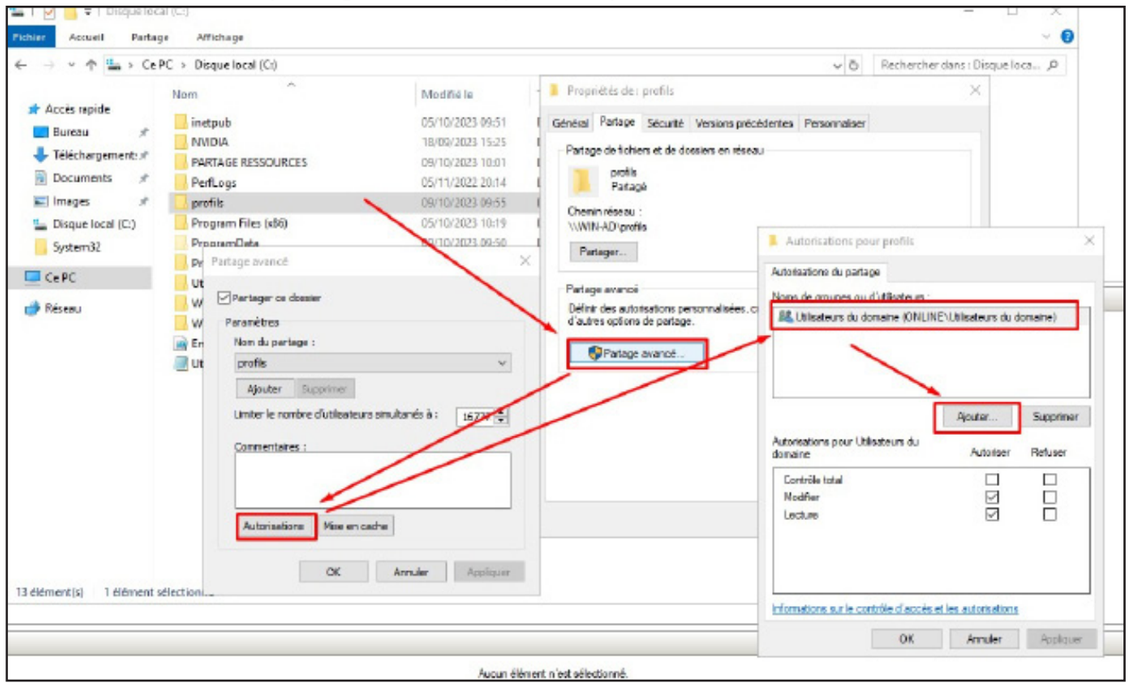
Dans le groupe Administrateur du poste ce trouve bien le groupe Admin locaux du domaine qu'on à crée. Pour que seuls le groupe du domaine soit Administrateur Local, il suffit de supprimer les compte Administrateur local de la machine et de ne laisser que ce qui concerne le domaine pour une meilleur protection.

Le dossier local « Mes Documents » doit être redirigé vers un emplacement de votre choix sur le serveur

Pour rediriger le dossier «Mes Documents» des utilisateurs du Domaine, il faut préalablement créer un dossier partagé sur le controleur de domaine. C'est dans ce dossier que seront stocké les dossiers «Mes Documents» des utilisateurs.

Création du dossier partagé

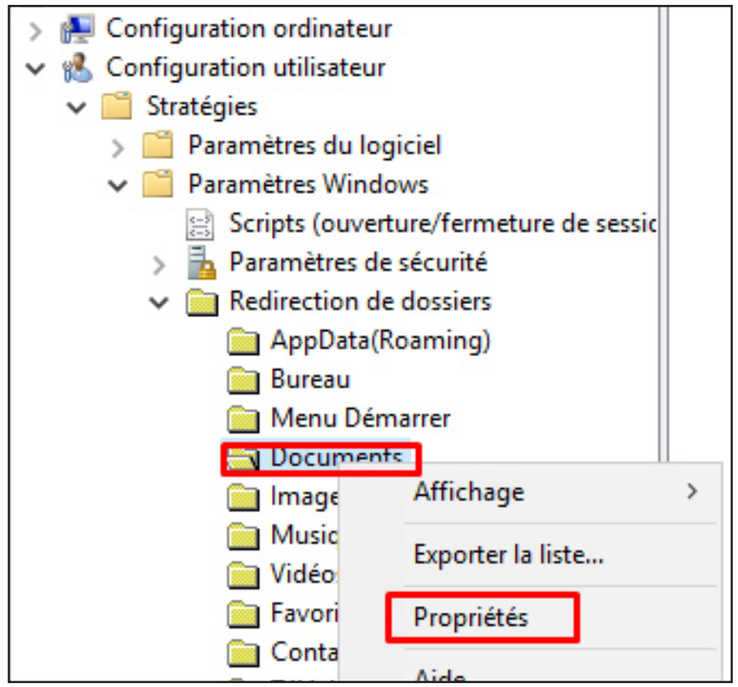
On va créer un dossier partagé nommé «profils», pour cela suivre la procédure:



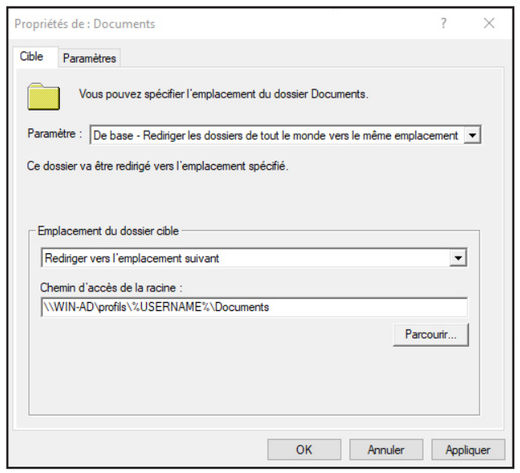
Création de la GPO:

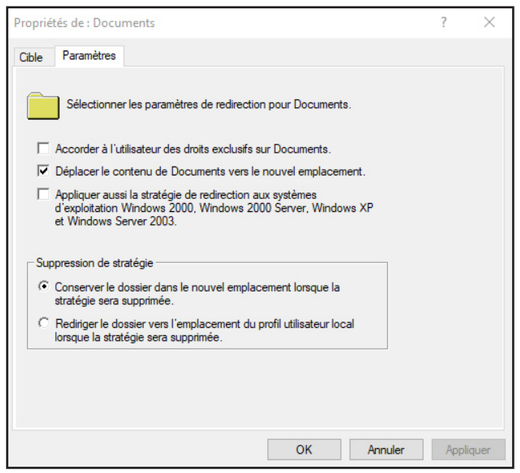
Rendez-vous dans l'outil Gestion de strategies de groupes depuis le menu démarrer

Créer la GPO, et suivre le chemin suivant Configuration utilisateur / Stratégies / Paramètres Windows / Redirection de dossiers puis sélectionner Documents et faites un click droit -> Propriétés



Mettre en place les paramètres suivants:





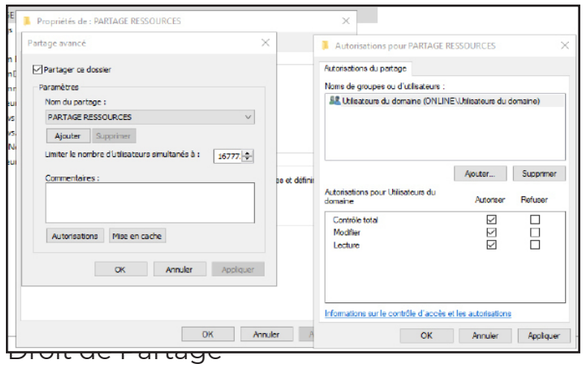
Normalement tous fonctionne après ça, il suffit de se connecter à un utilisateur du domaine et son dossier «Documents» apparaîtra dans le dossier partagé (bien appliquer la régle aux UO)

Vous devez déployer le logiciel « 7zip » et « Google Chrome » pour le service « comptabilité »

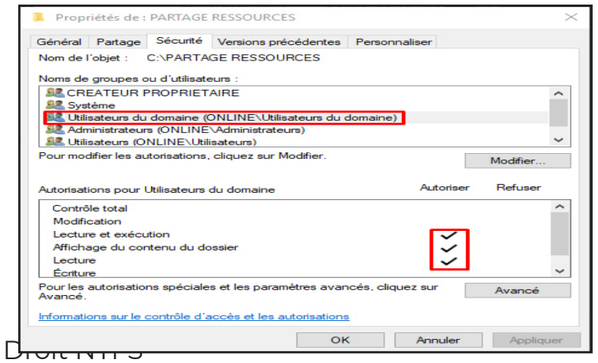
Dans notre cas, le deploiement des logiciels ce fera sur le service Informatique.

Pour réaliser la GPO, il faut préalablement créer un dossier partagé dans le domaine qui hebergera les éxecutables de Chrome et 7zip. (les executables doivent être au format .msi)

Le dossier partagé est configuré comme ceci:



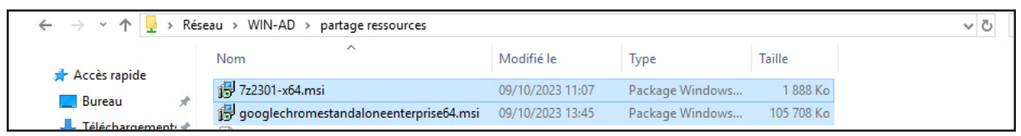
Droit de Partage



Droit NTFS

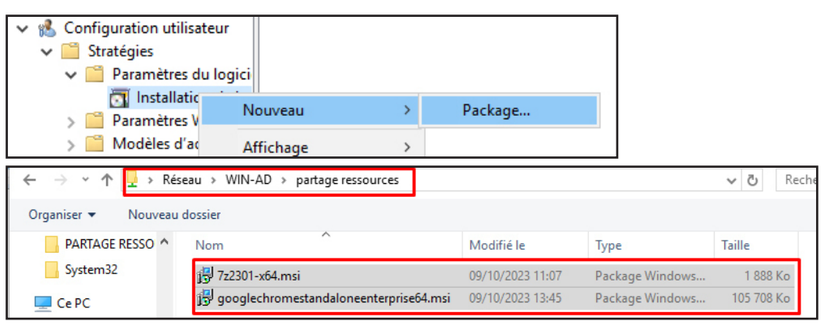
Partage accessible via ce chemin: \\Win-ad\partage ressources

Il faut désormais insérer les .msi des 2 logiciels

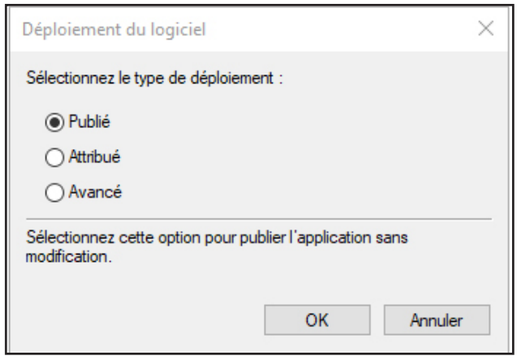


Création de la GPO sur l'UO Service Informatique

Suivre le chemin suivant: Configuration utilisateur > Stratégies > Paramètres du logiciel > Installation de logiciel puis:



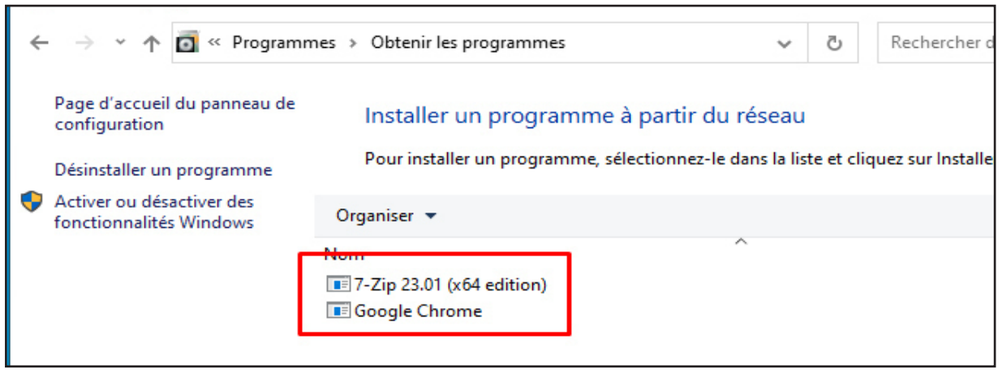
Si on choisit l'option Publié ça laisse le choix à l'utilisateur d'installer ou non le logiciel, si la GPO agissait sur l'ordinateur, nous aurions dû choisir Attribué pour que les logiciels soient installer AUTOMATIQUEMENT sur les postes



Installation de Chrome et 7zip pour les utilsateurs

Il suffit de se connecter sur un utilisateur du service informatique et d'installer manuellement les logiciels.

Pour cela rendez-vous ici: Panneau de Configuration -> Programmes -> Programmes et Fonctionnalités puis Installer un programme à partir du réseau



On peut voir que les 2 logiciels sont bien déployés pour les utilisateurs du service informatique.

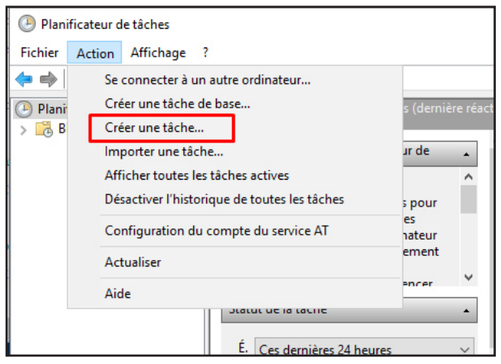
Vous devez sauvegarder les GPO grâce à un script PowerShell vers un endroit sécurisé (utiliser une tâche planifiée pour lancer le script tous les jours à 16h00)

Pour sauvegarder les GPO, il nous faut créer un script Powershell et planifier une tâche qui s'exécutera tous les jours à 16h.

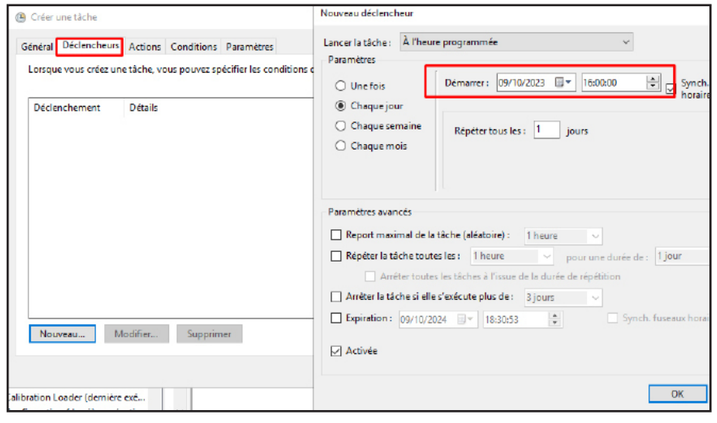
Voilà le script qu'on utilisera:

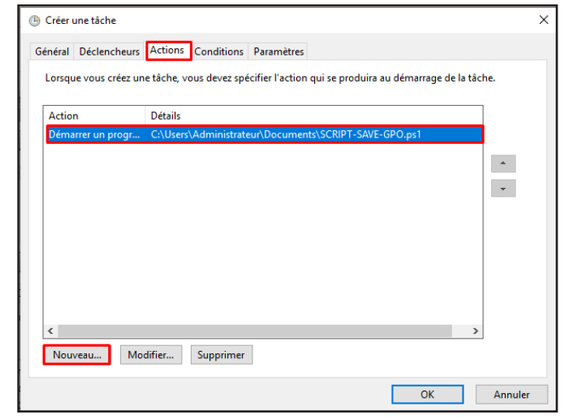
```powershell
$BackupShare = "C:\BACKUP-GPO" # partage pour la sauvegarde
$date = get-date -format yyyy.M.d #Date du jour
$Jour = 15 # Nombre de jour a conserver
$Backup = $BackupShare+"\"+$date #Dossier journalier de sauvegarde

#Création du dossier du jour
New-Item -Name $date -ItemType Directory -Path $BackupShare

#Suppression des anciennes GPO de plus de $jour
Get-ChildItem $BackupShare -Directory | ?{$_.CreationTime -lt (get-date).AddDays(-$Jour)} | %{Remove-Item $_.FullName -Force -Recurse}

#Sauvegarde des stratégies
Backup-Gpo -All -Path $Backup
```

Maintenant il faut planifier le lancement du script chaque jour à 16h.
Pour cela, Ouvrir le Planificateur de Tâches et créer une nouvelle tâche.

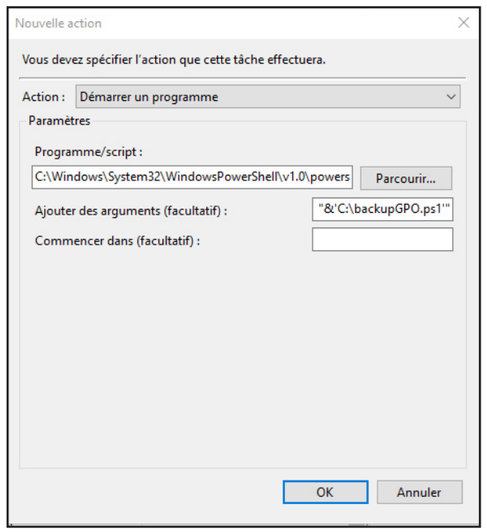


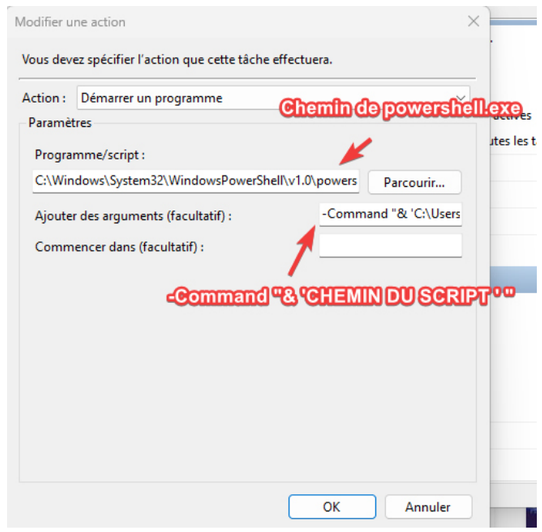
Choisir Déclencheur, puis suivre les captures d'écrans ci-joint



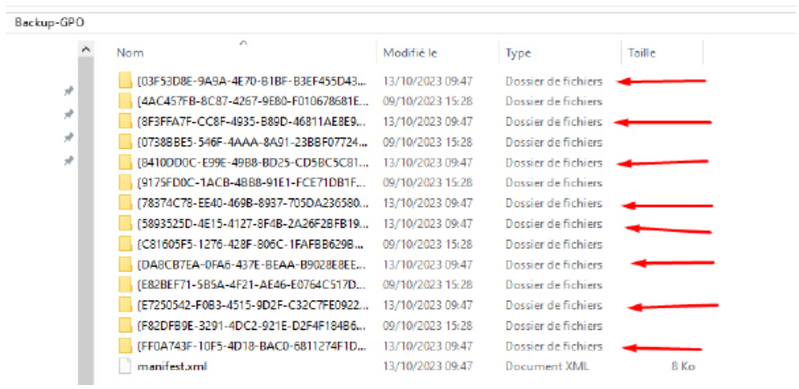


Explication





On a planifié la tâche pour 16h, mais on a crée une autre tâche (la même) pour ne pas attendre 16h... l'autre tâche est planifiée à 9h47.



Conclusion: Tout fonctionne

Le script s'est bien lancé, les GPo ont été sauvegardées à 9h47

(Les flèches rouges indiquent les GPO sauvegardées lors du script)

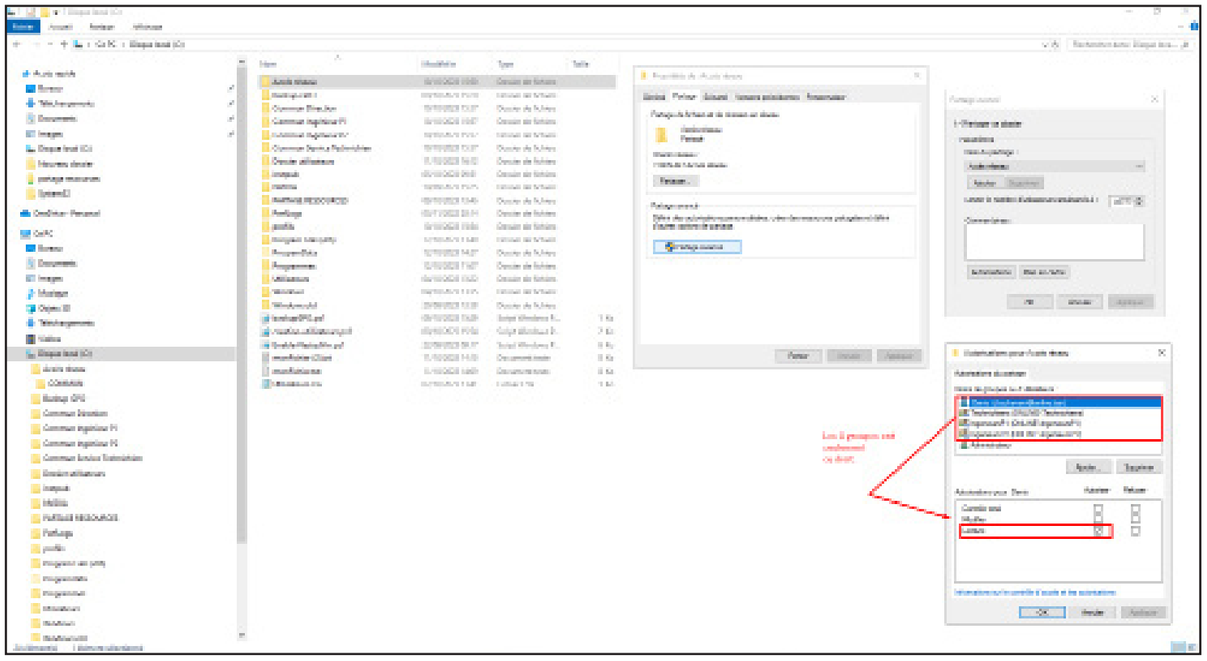
Un dossier « Commun » doit être partagé. Le contenu doit être disponible en lecture – écriture – modification pour tous les services. Le dossier « Commun » ne peut pas être supprimé sauf par le service informatique.

Si on décompose étapes par étapes :

- Un dossier « Commun » doit être partagé.
On a créé un dossier racine, dossier dans lequel on a mis un dossier nommé « Commun »
Pour la raison que si on avait mis le dossier « Commun » comme premier dossier « racine » il aurait été impossible de réaliser la partie de la consigne qui stipule : Le dossier « Commun » ne peut pas être supprimé sauf par le service informatique parce que même le service informatique n'aurait pas pu. Voilà pourquoi on va partager le dossier Commun par le biais de son dossier racine que l'on a nommé «Accès réseau».

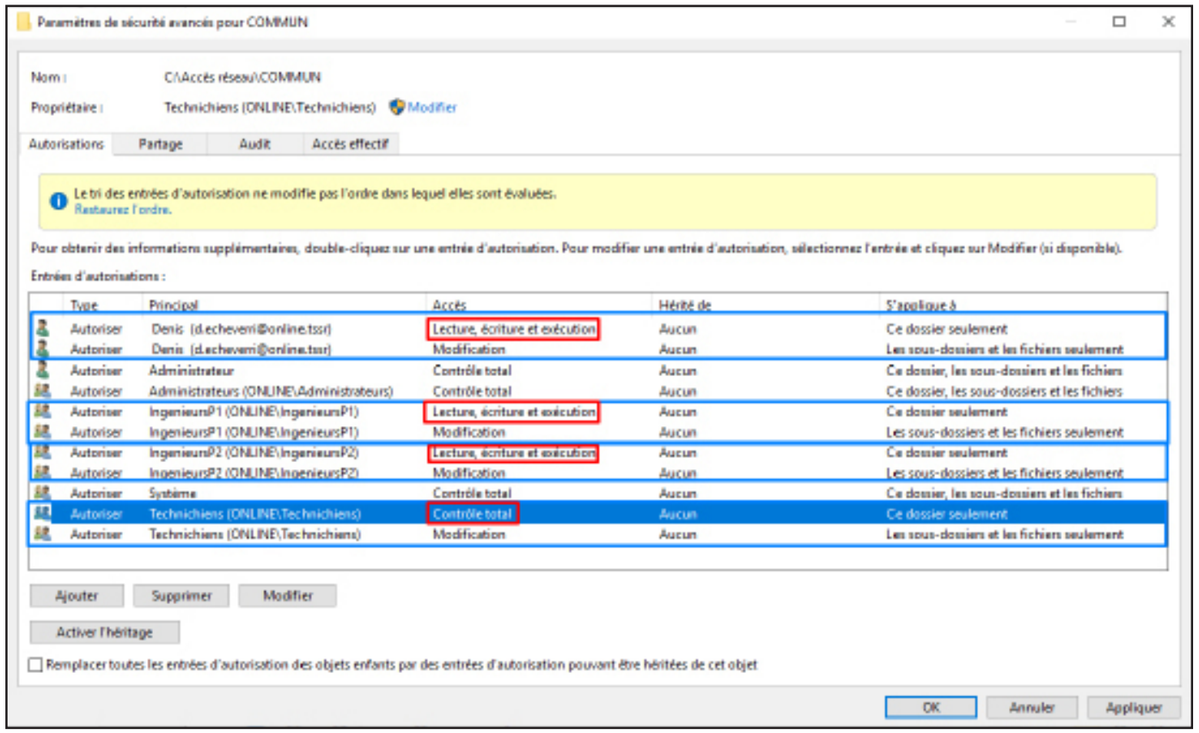
TLDR : On a partagé le dossier commun par le biais de son dossier racine.

Voilà les droits de Partage du dossier:



Le contenu doit être disponible en lecture – écriture – modification pour tous les services &
Le dossier « Commun » ne peut pas être supprimé sauf par le service informatique.

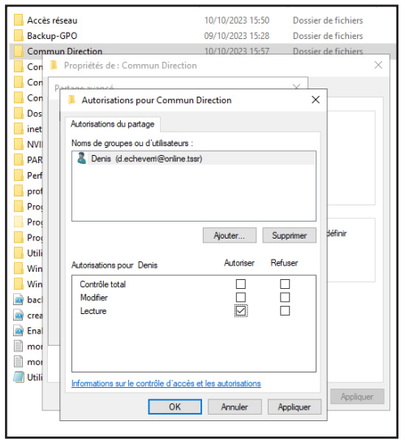
Voici les paramètres NTFS du dossier:



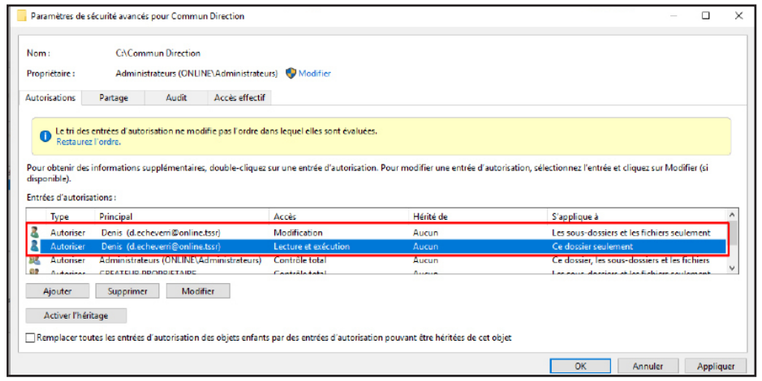
Chaque service doit avoir un répertoire partagé nommé « Commun_nom_du_service » qui sera attribué à chacun des salariés lors de sa connexion réseau (permissions en lecture – écriture - modification des sous dossiers mais pas du dossier « racine »)

On a crée 4 dossiers pour nos 4 services à savoir: Direction, Technichiens, IngenieurP1 et P2

Dossier Commun **Direction**

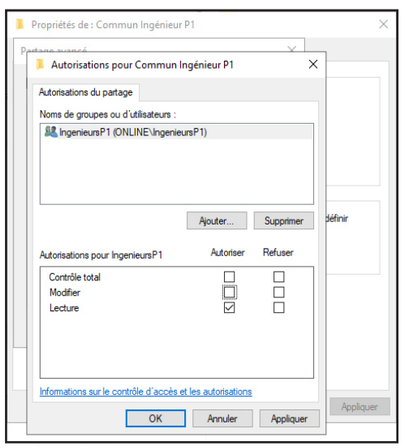


Droits de Partage

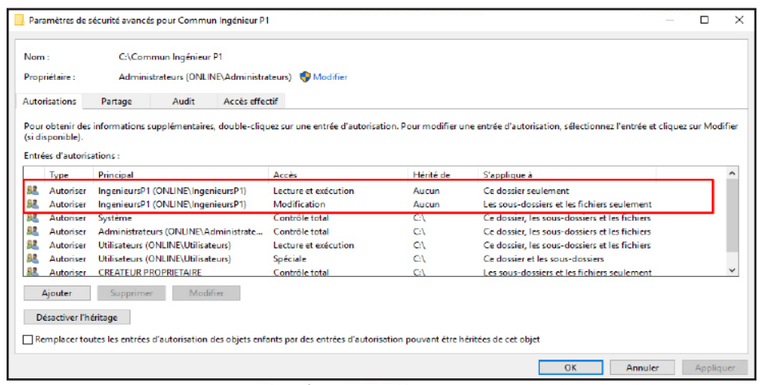


Droits NTFS

Dossier Commun IngenieurP1

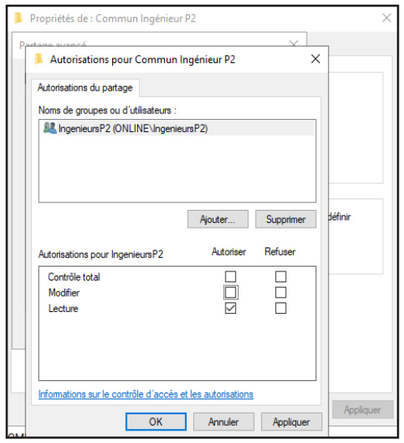


Droits de Partage

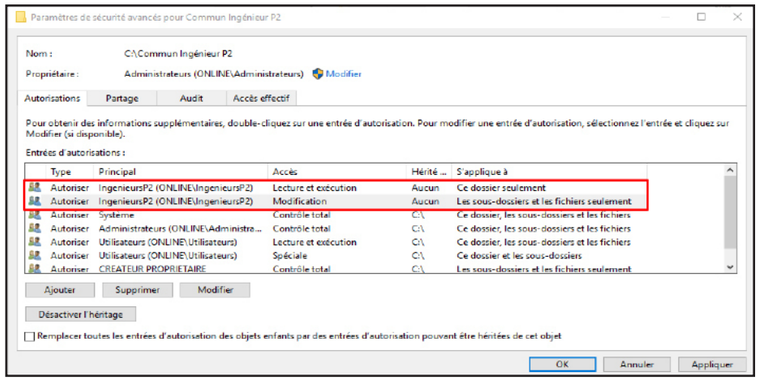


Droits NTFS

Dossier Commun **IngenieurP2**

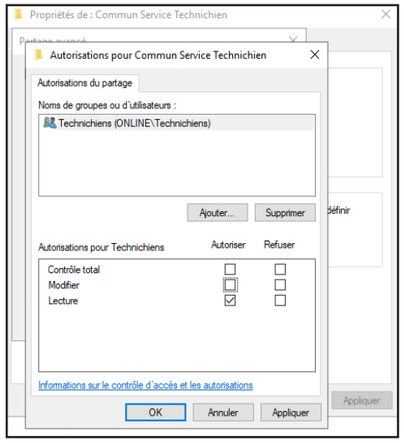


Droits de Partage

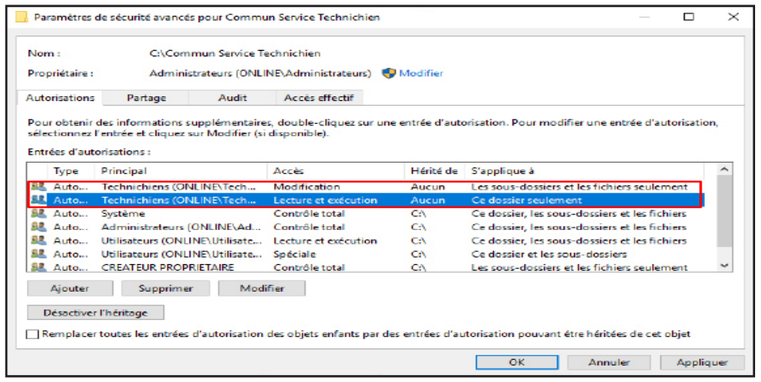


Droits NTFS

Dossier Commun **Technichiens**



Droits de Partage



Droits NTFS

On a autorisé seulement le service concerné à accéder aux partages qui les concernent, pour les droits NTFS on a fait ça en 2 parties, la première qui indique que le service est autorisé à lire le dossier mais ne peut écrire / faire des modifications.
Par contre pour ce qui concerne les sous-dossiers et fichiers qui seront crées dans le dossier, on autorise au service concerné à faire des modifications / écrire / lire.

Vous devez créer un dossier partagé personnel « caché » pour chaque salarié (contrôle total sur celui-ci et aucun accès sur ceux des collègues) et configurer un lecteur réseau associé

Tout d'abord nous allons créer un dossier «Général» sur le serveur qui regroupera par la suite les dossiers utilisateurs.

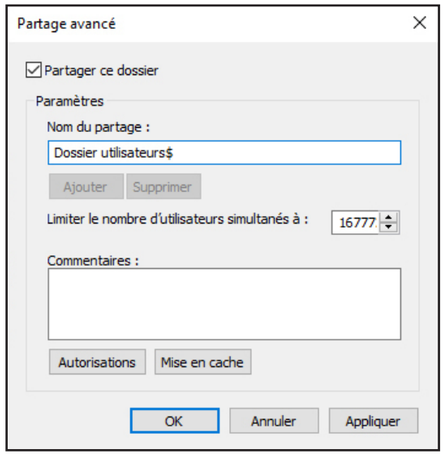
Le dossier crée, il faut le paramétrer comme ceci:

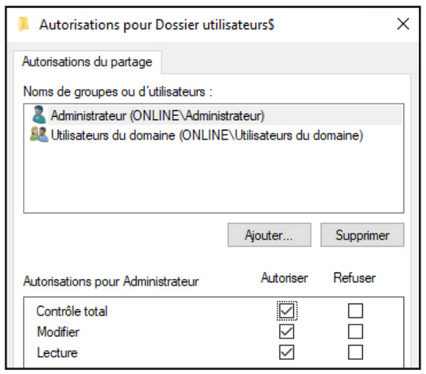
Faites un clic droit sur ce dossier et cliquez sur« Propriétés »

• Cliquez l'onglet « Partage » et cliquez sur « Partage avancé »

• Cliquez la case « Partager ce dossier » et indiquez le nom de partage : ici « Dossier utilisateurs$ ». Attention le signe $ permet de cacher le partage sur le réseau

• Cliquez ensuite sur « Autorisations » et spécifiez les autorisations suivantes :





On ajoute les « Utilisateurs du domaine » et les « Administrateurs » avec un « Contrôle total » pour chacun.

- Cliquez, ensuite, sur l'onglet « Sécurité » et cliquez sur le bouton « Avancé » en bas pour affecter des autorisations NTFS particulières :

• Désactivez les héritages (bouton en bas à gauche) et supprimez toutes les autorisations

• Ajoutez ensuite les groupes et utilisateurs suivants : Administrateurs, CREATEUR PROPRIETAIRE, système, Utilisateurs du domaine

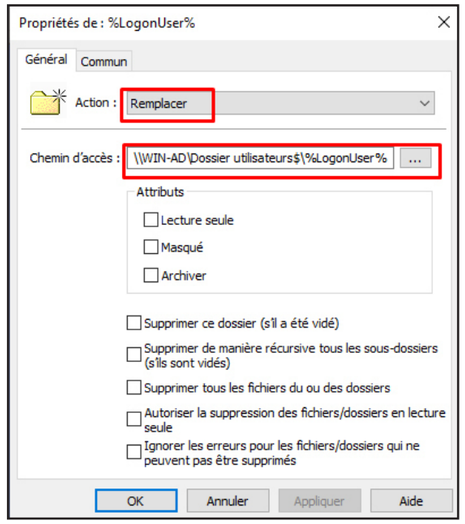
• Accorder les paramètres suivants:

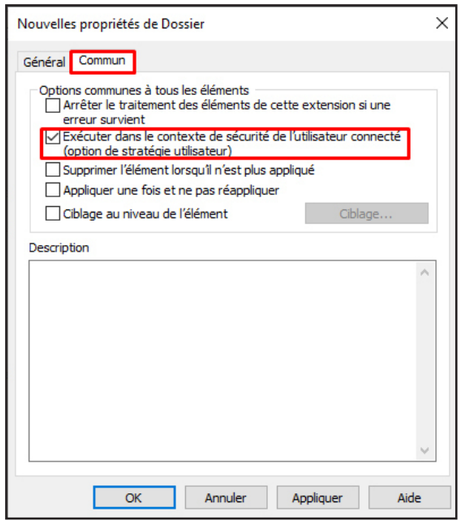
Administrateurs – Ce dossier : Contrôle total
Système – Ce dossier, les sous-dossiers et les fichiers : Contrôle total
CREATEUR PROPRIETAIRE – Les sous-dossiers et les fichiers seulement : Contrôle total
Utilisateurs du domaine – Ce dossier, les sous-dossiers et les fichiers : **Contrôle total**

CREATION DE LA GPO PERMETTANT DE CREER AUTOMATIQUEMENT LE DOSSIER PERSONNEL DE L'UTILISATEUR

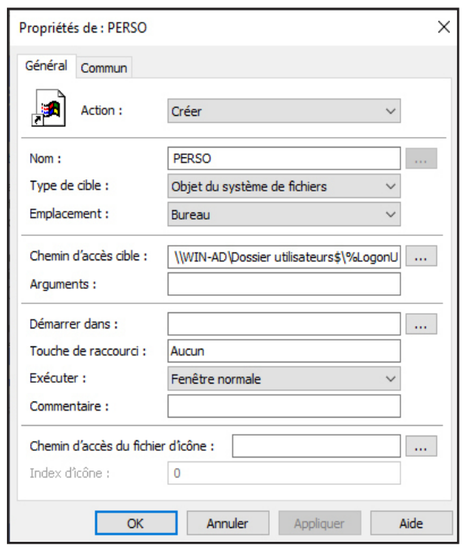
Ouvrez la fenêtre « Gestionnaire de serveur » et cliquez « Outils » - « Gestion des stratégies de groupe »
• Créer un objet GPO à la racine de votre domaine (clic droit – « Créer un objet GPO… »)
• Nommez-le « Création dossier perso user »

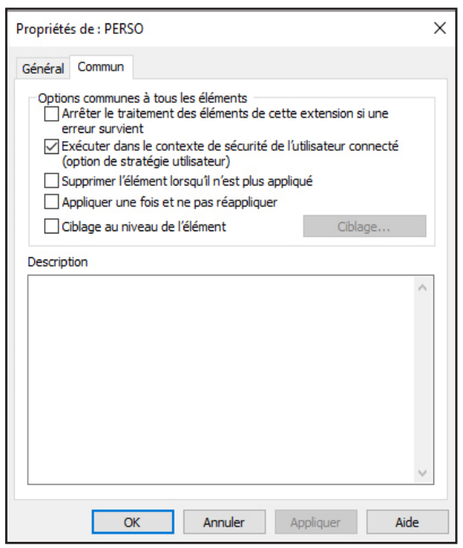
Faites un clic droit sur l'objet GPO et cliquez sur « Modifier »
• Dans le volet de gauche, développez « Configuration utilisateur » - « Préférences » - « Paramètres Windows »
• Cliquez sur « Dossiers » :
• Faites un clic droit dans la fenêtre de droite et cliquez « Nouveau » - « Dossier »DD





Il est possible de créer un raccourci sur le Bureau pour les utilisateurs, pour cela dans Paramètres Windows, faites un click droit sur Raccourcis et paramétrer comme ceci:

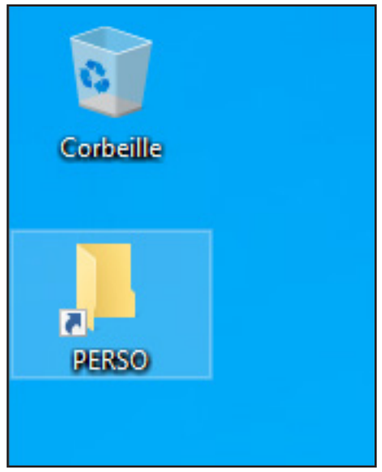


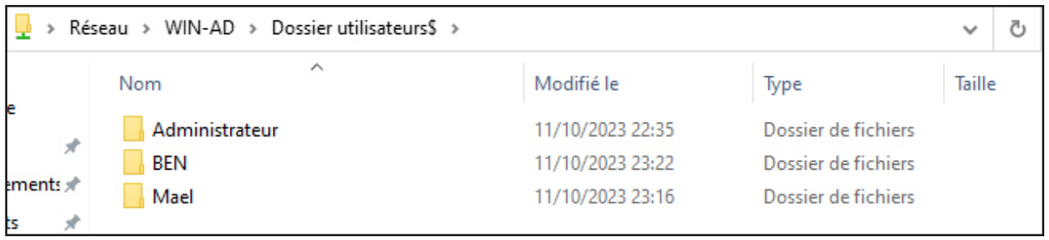


Connection sur un poste utilisateur

Bien penser à faire un gpupdate /force sur le serveur !

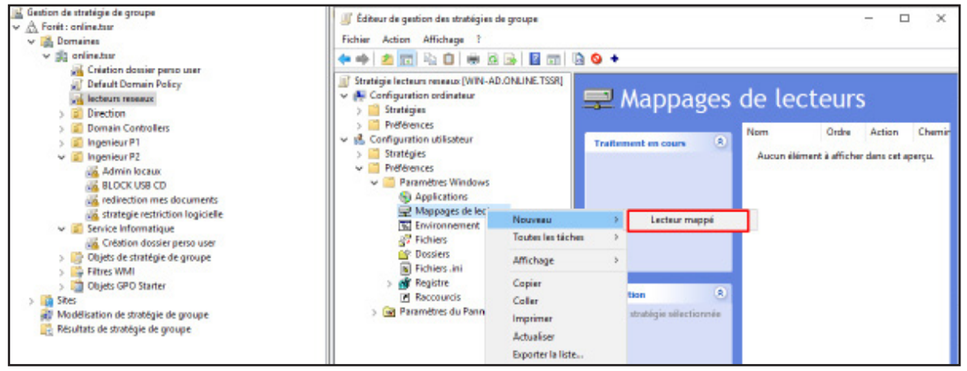
Si tout est bien configurer, à la connexion il devrait apparaître le fumeux dossier personnel de l'utilisateurs, si il s'avère qu'il n'est pas présent entrer le chemin réseau ou est stocké le dossier «général» \\WIN-AD\Dossier utilisateurs$ dans notre cas



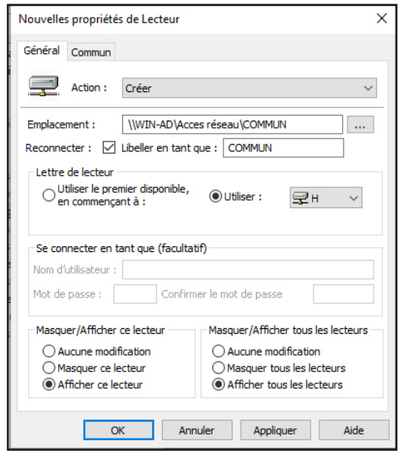


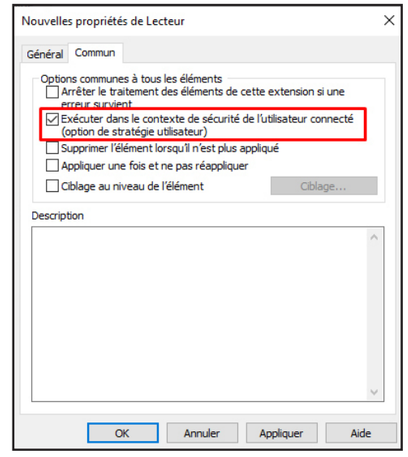
Déployer les lecteurs réseaux nécessaires au bon fonctionnement de l'entreprise (pour chacune des ressources nécessaires aux salariés – Dossier « COMMUN », « SERVICE » et « PERSO »

Il nous faut créer une GPO «lecteurs réseaux» et ensuite redirigé le lecteur réseau vers la ressource souhaité.

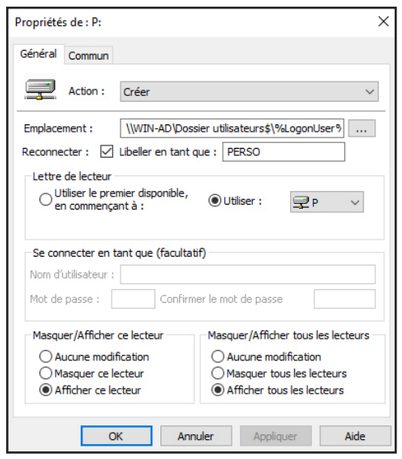


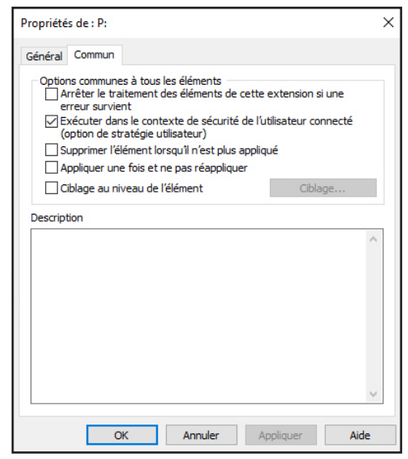
LECTEUR COMMUN



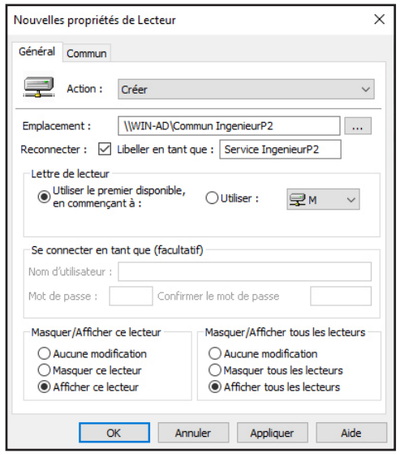


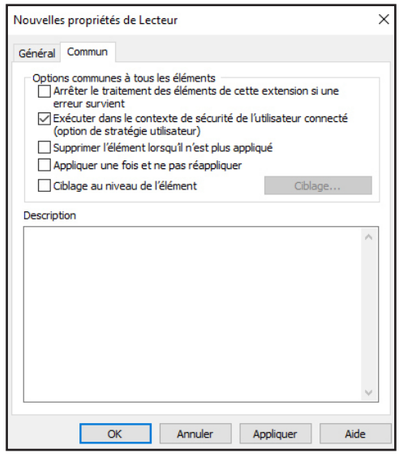
LECTEUR PERSO



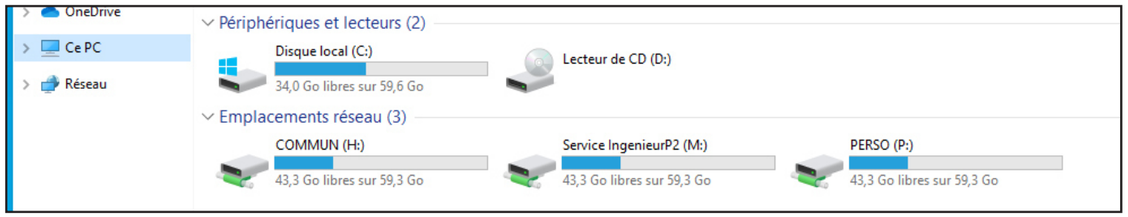


LECTEUR SERVICE





C'est un exemple pour le service «Ingenieur P2» mais la logique reste la même, sauf qu'il faut choisir l'emplacement qui redirige vers le dossier Commun du service concerné.



Voici un utilisateur du service «IngenieurP2» et il a bien accès aux lecteurs qu'il faut !

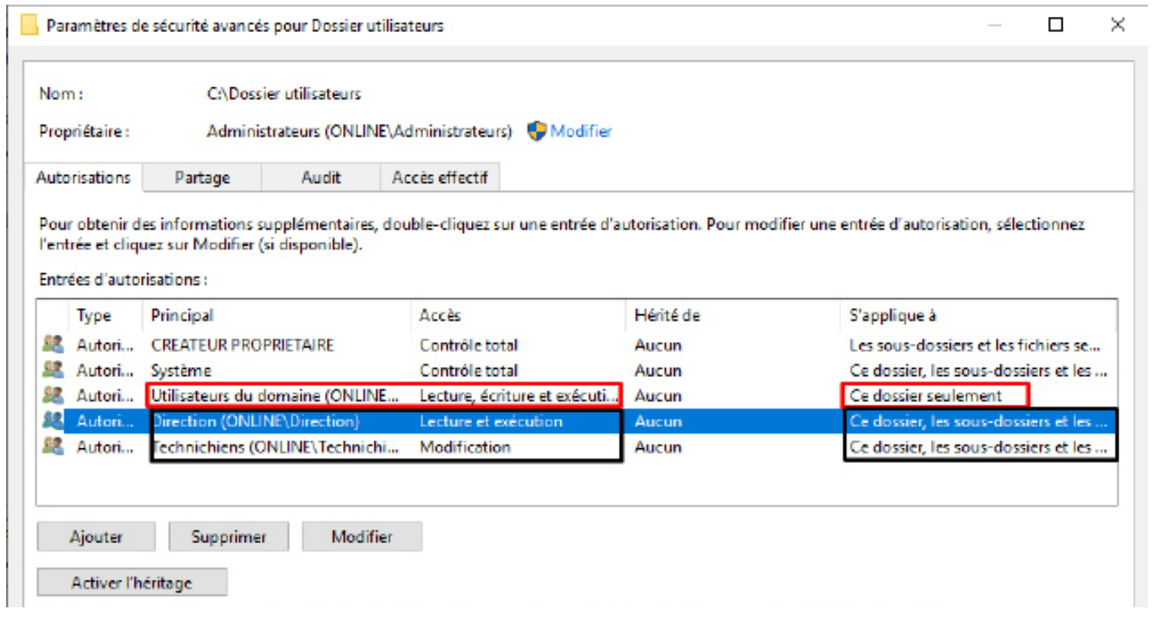
Seuls la direction et l'informatique peuvent accéder au dossier personnel des salariés (juste « lecture » pour la direction)

Pour faire cela il faut configurer les droits NTFS de façon à ce que tous les utilisateurs du domaine soient en Lécture, éxécution, écriture pour **uniquement le dossier racine** qui accueil les dossiers personnels. Cette règle est là pour que les dossier perso des utilisateurs puissent être crées. Les utilisateurs ont donc le droit de Lécture, éxécution, écriture mais sur ce dossier uniquement mais pas sur les sous-dossiers et fichiers, ce qui leurs empêche d'accéder aux dossiers des autres utilisateurs.

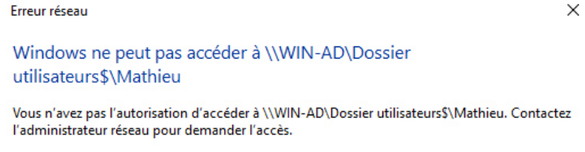
Ensuite il faut créer une deuxième règle pour le service «Direction» qui s'applique sur C**e dossier, les sous-dossiers et les fichiers** et qui autorise le groupe à Lire et éxecuter uniquement

Enfin il faut créer une troisième règle pour le service informatique (Technichiens) qui s'applique également sur **Ce dossier, les sous-dossiers et les fichiers** et qui autorise le groupe à Lire et éxecuter et modifier les dossiers personnels.

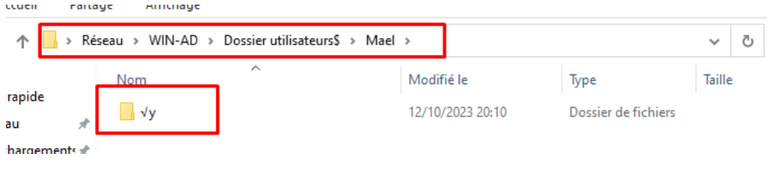
Configuration:



POV Utilisateur Mael (IngenieurP1)



POV Utilisateur Ramazan (Technichien)



Seul le service Info peut accéder au dossier perso des utilisateurs

Déployer au moins un lecteur réseau grâce à un script (BAT ou POWERSHELL) sur ces dossiers

```powershell
# Spécifiez le chemin UNC du dossier partagé
$sharedFolder = "\\Win-ad\testps"

# Spécifiez la lettre de lecteur à utiliser
$driveLetter = "y"

# Créez le lecteur réseau
New-PSDrive -Name $driveLetter -PSProvider FileSystem -Root $sharedFolder -Persist

# Obtenez l'objet de sécurité du lecteur réseau
$acl = Get-Acl $driveLetter":\"

# Obtenez l'identité du groupe Administrateurs
$administratorsGroup = [System.Security.Principal.WindowsBuiltInRole]::Administrator

# Créez une règle d'autorisation pour le groupe Administrateurs
$permission = "$($administratorsGroup)\FullControl"
$rule = New-Object System.Security.AccessControl.FileSystemAccessRule($administratorsGroup,"FullControl","Allow")

# Ajoutez la règle d'autorisation au lecteur réseau
$acl.SetAccessRule($rule)
Set-Acl $driveLetter":\" $acl
```

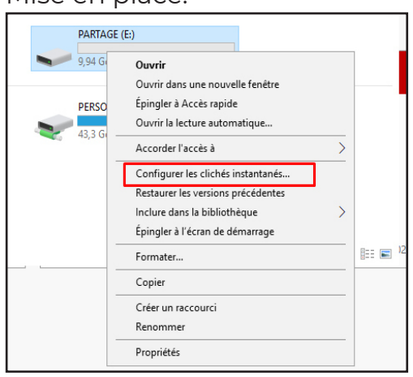
```
Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
y                  16,01         43,39 FileSystem    \\Win-ad\testps
```

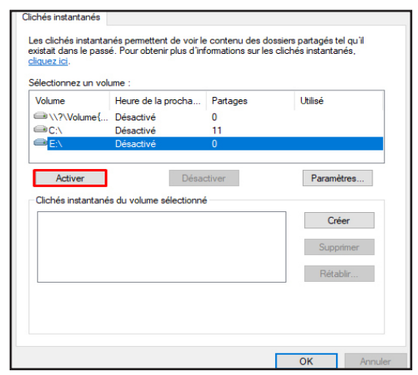
Configurer les clichés instantanés sur un disque (ou est présent votre partage) et tester cette fonctionnalité.

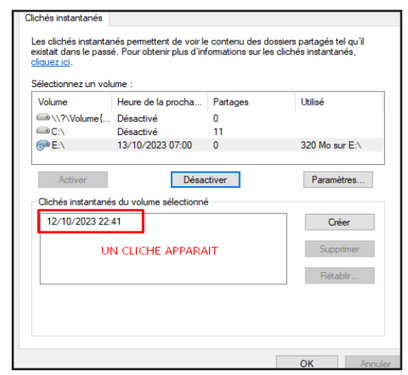
C'est quoi les clichés instantanés ?

Les clichés instantanés sont une fonctionnalité de stockage de données de Windows qui permet de créer une image instantanée de l'état des données à un moment donné. Ils peuvent être utilisés pour récupérer des données supprimées accidentellement ou pour créer des sauvegardes des données importantes.

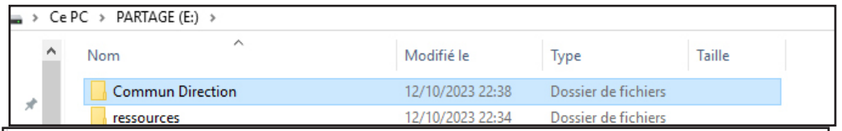
Mise en place:

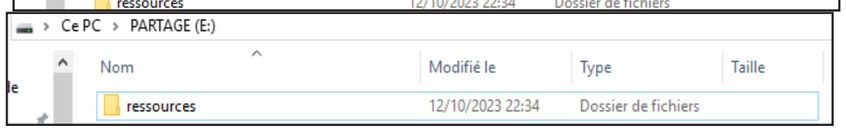




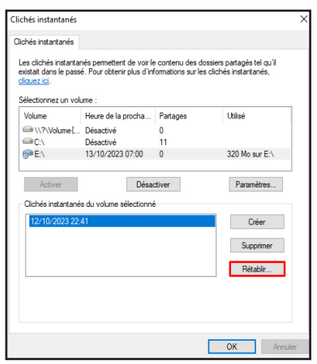


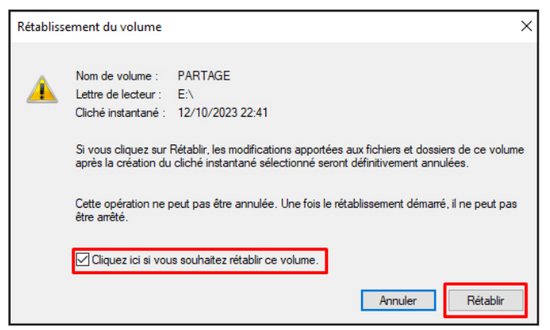
On a crée un cliché qui stocke les données présentes au jour et à l'heure indiqué. Maintenant il faut supprimer le dossier «Commun Direction» pour vérifier si lorsqu'on tente une récupération à partir de cette «image» nos données sont bien récupérées.

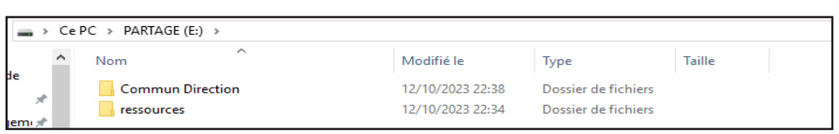




Le dossier supprimé on tente de restaurer le disque:







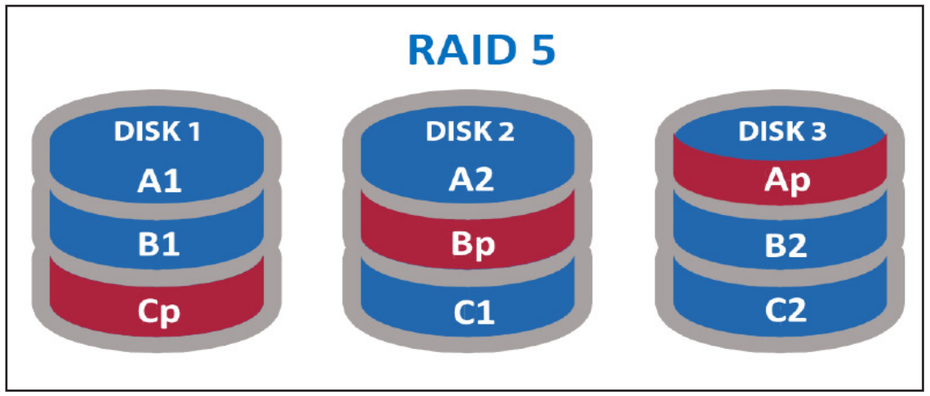
Le dossier «Commun Direction» est bien réapparue !

Ajouter des disques virtuels à votre serveur de fichier et configurer un « POOL de stockage en RAID 5. Créer un dossier partagé seulement pour la direction

Il faut d'abord ajouter nos 3 disques virtuelles au minimum pour faire notre RAID 5. (Sur votre VM ou en Physique)

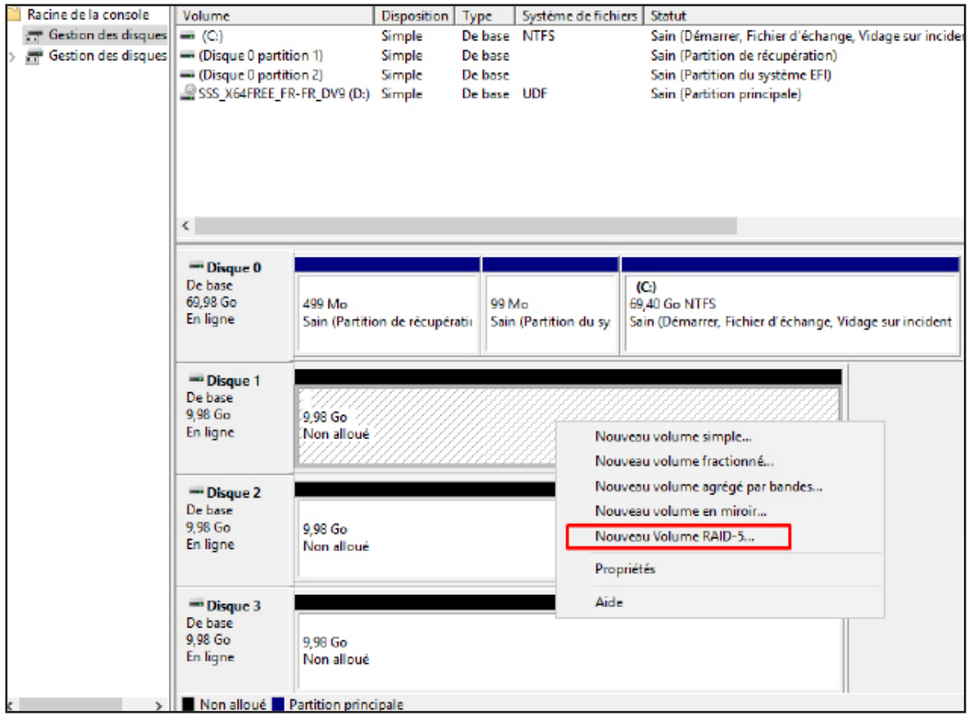
Rappel RAID 5:

Le RAID 5 répartit les données sur plusieurs disques et stocke une valeur de parité sur un ou desdisques différents. En cas de panne d'un disque, les données peuvent être reconstituées à partir des données des disques restants et de la valeur de parité.

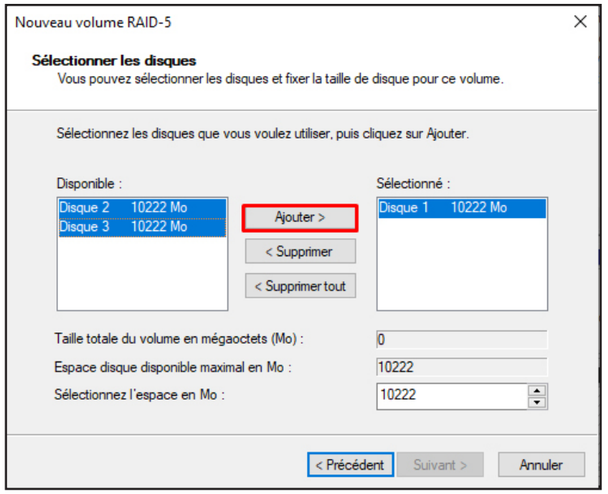


Ouvrir la console mmc via Windows + R et entrez «mmc» et ajouter le composant «Gestion des disques»

Choisir un des 3 disques non alloué et click droit «Nouveau volume Raid5»

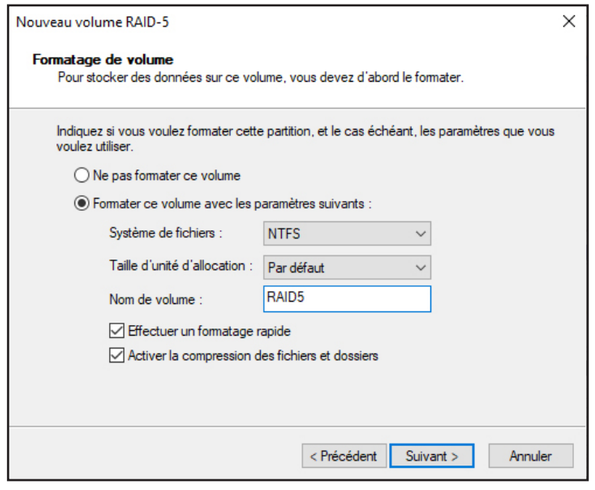


Séléctionner les 2 autres disques qui vont composer notre RAID 5

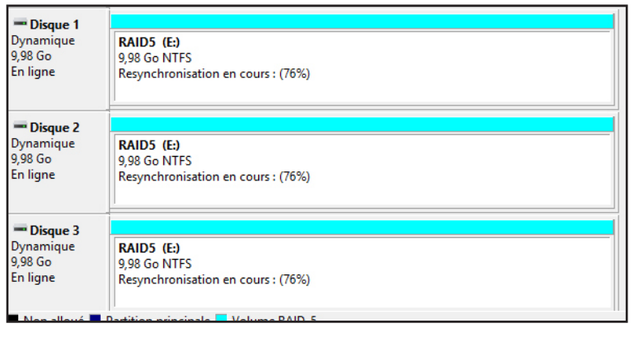


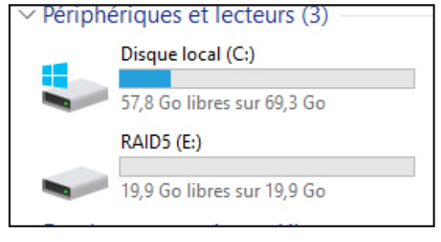
Puis choisir une lettre à attribuer au lecteur, «E» dans mon cas

Formater le volume en NTFS et donnez lui comme nom «RAID5»



Après ça les disques vont ce synchroniser et passer officiellement en RAID5.

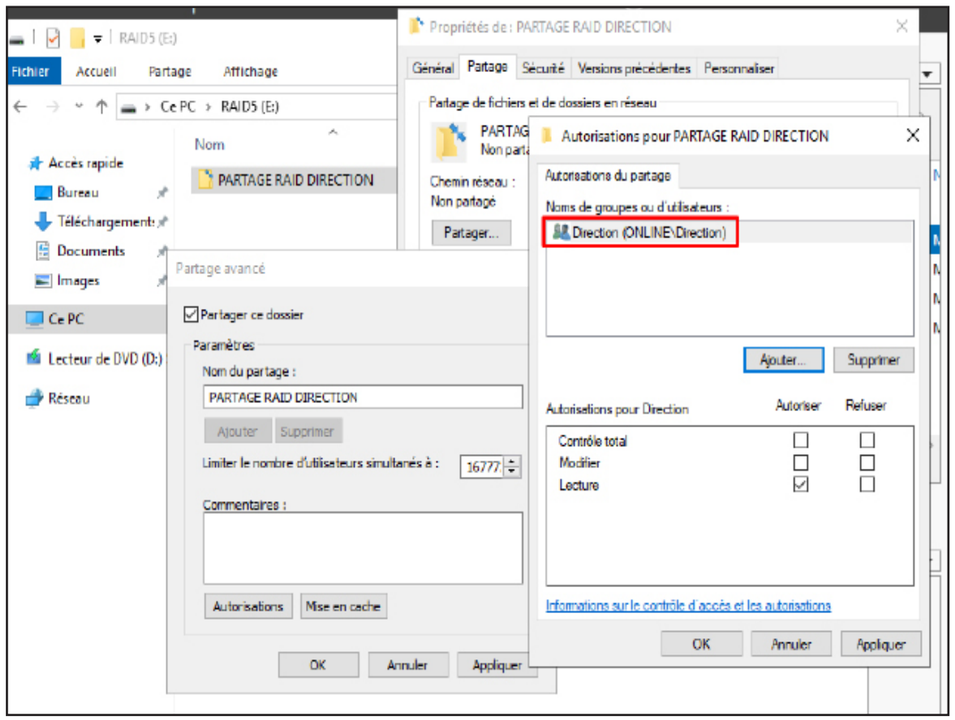




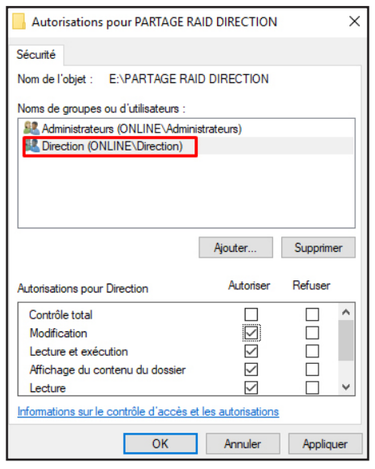
Le disque «RAID5» apparaît bien, on va passer à la création d'un dossier partagé pour la Direction.

Création du dossier partagé pour la Direction sur le Volume en RAID5

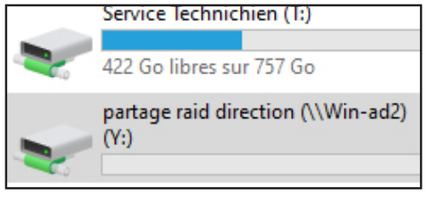
Se rendre dans le volume E:\ t créer un dossier «PARTAGE RAID DIRECTION» et le partager comme ici:



Droits NTFS:



Côté utilisateur de la Direction le dossier partagé est bien accessible



Partie 5 : Autres Services du serveur Windows

- Installation et configuration de serveurs Windows:

Serveur de déploiement d'images – WDS (Rapprochez-vous du DAF)

Qu'est-ce que WDS?

Source: https://it-connect.fr/overview-mdt-wds-winpe/

WDS (Windows Deployment Services)

C'est Le service de déploiement Windows. Autrement dit un «rôle» facultatif disponible sur toutes les versions Windows Server depuis 2003R2. (Pour la petite histoire, son ancêtre se dénommait RIS pour «Remote Installation Service») - En quelques mots, ce service assure 2 fonctions majeures : Le déploiement des images WIM pour les systèmes d'exploitation Windows et La fourniture d'images de démarrage (via PXE) pour l'initialisation des processus d'installation (ou de réparation).

Quels sont les prérequis pour pouvoir utiliser un serveur WDS dans votre environnement d'entreprise ?

Les pré-requis pour pouvoir utiliser un serveur WDS dans un environnement d'entreprise sont les suivants :

- **Un serveur Windows Server 2016 ou version ultérieure.** Le serveur WDS doit être un serveur physique ou virtuel exécutant Windows Server 2016 ou version ultérieure.

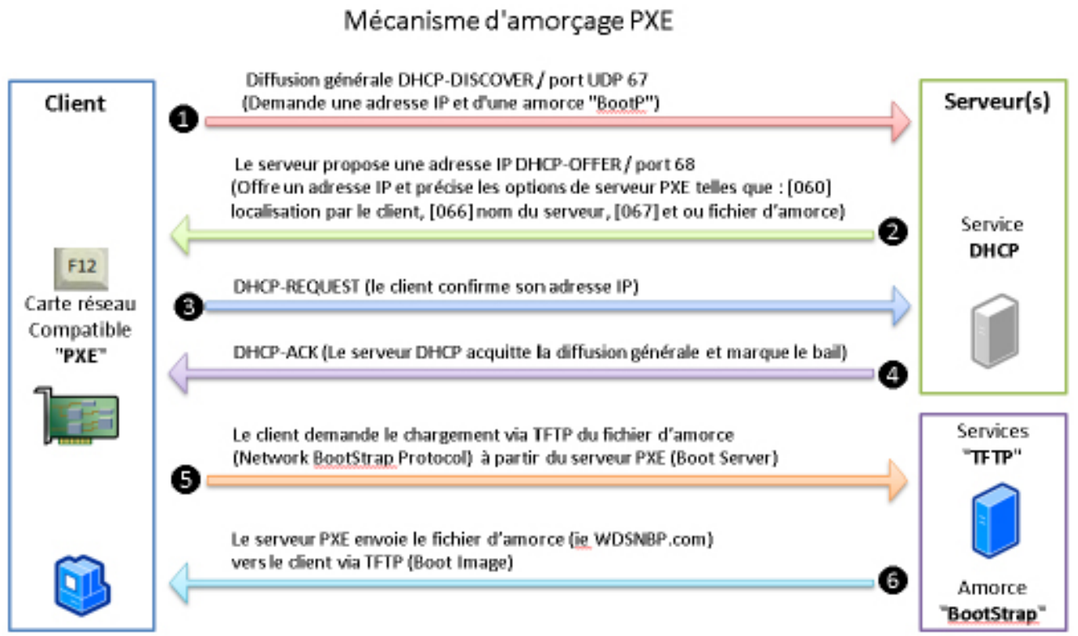
- **Un rôle Active Directory**. Le serveur WDS doit être membre d'un domaine Active Directory ou d'un contrôleur de domaine pour un domaine Active Directory.

- **Un serveur DHCP.** Le serveur WDS doit avoir accès à un serveur DHCP pour attribuer des adresses IP aux ordinateurs clients.

- **Un serveur TFTP**. Le serveur WDS doit avoir accès à un serveur TFTP pour stocker les images de démarrage et d'installation.

- **Une image de démarrage.** Une image de démarrage est une image de démarrage de Windows qui est nécessaire pour démarrer les ordinateurs clients en mode PXE.

- **Une image d'installation**. Une image d'installation est une image complète de Windows qui est utilisée pour installer le système d'exploitation sur les ordinateurs clients.



Quelles sont les alternatives (libres ou non) à cette solution ?

Source: 10 Best WDS Alternatives 2023 (rigorousthemes.com)

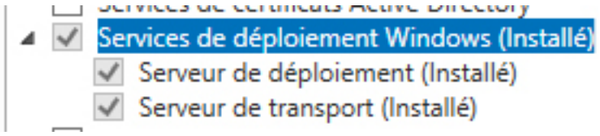
- SmartDeploy
- AOMEI Image Deploy
- Clonezilla
- ManageEngine OS Deployer
- Kace Systems Deployment Appliance
- The FOG Project
- Ghost Solution Suite
- Acronis Snap Deploy
- Ivanti
- SmartImager

Installer et configurer WDS pour déployer des images sur vos postes clients (utilisez les ressources nécessaires sur l'ISO de Windows 10 PRO)

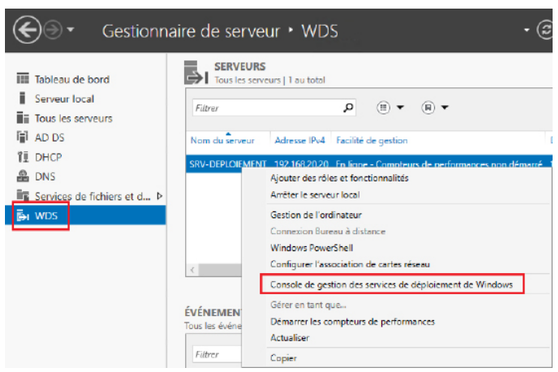
Sources:
https://neptunet.fr/mdt-deploy/

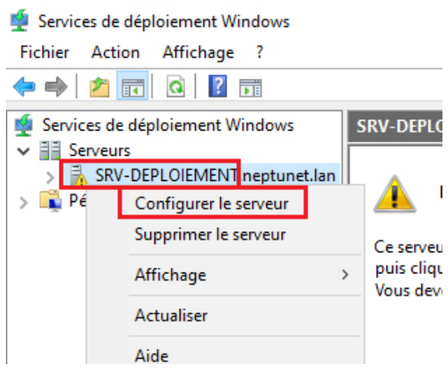
Avant de commencer il faut bien veiller à ce que le DHCP ait bien une étendue active sur le contrôleur de domaine

On commence par installer le rôle WDS

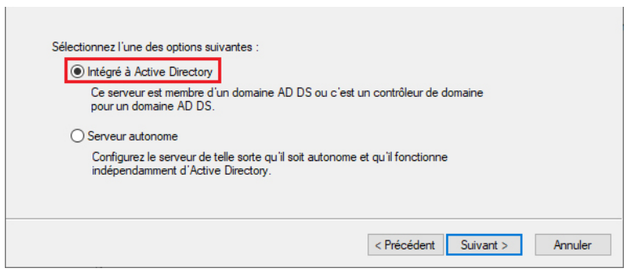


Configuration de WDS

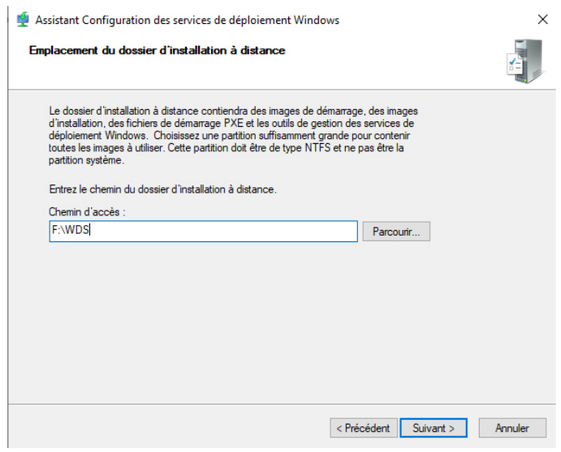




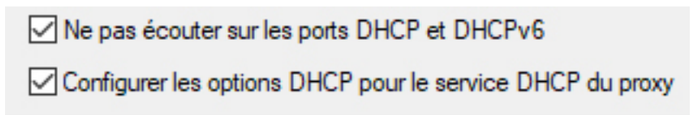
Indiquer que ce serveur est membre d'un domaine ADDS ou que c'est un contrôleur de domaine dans notre cas c'est un contrôleur de domaine



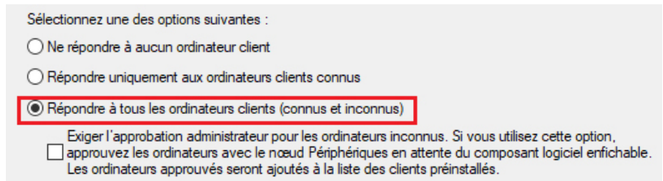
L'emplacement du dossier d'installation de WDS est important. Comme n'importe quel service, il est préférable de ne pas l'installer sur la même partition que le système d'exploitation. De mon côté, j'ai prévu un second disque de stockage monté sur la lettre E, je vais donc indiquer « E:\WDS » comme emplacement.



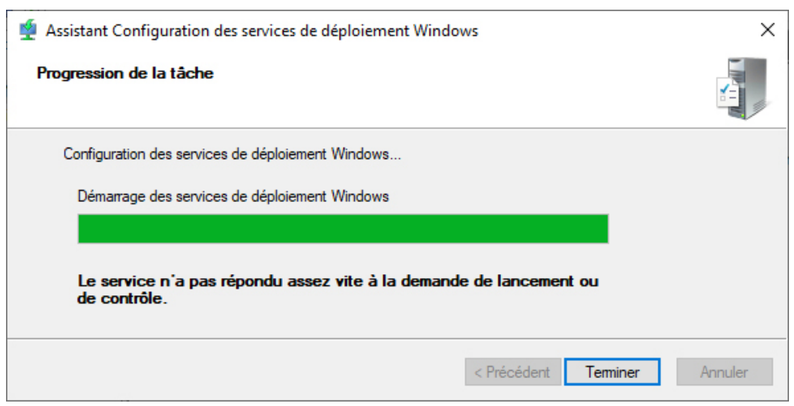
Je ne touche à rien dans la configuration du DHCP car mon serveur dispose du service DHCP déjà configuré, les options nécessaires seront ajoutées automatiquement, veillez juste à ce que les 2 cases soient bien cochées.



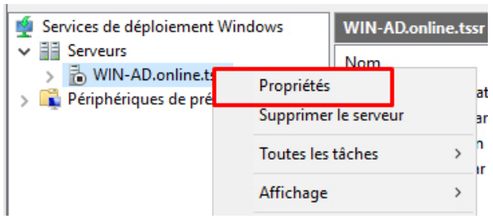
Ensuite cocher que cette option



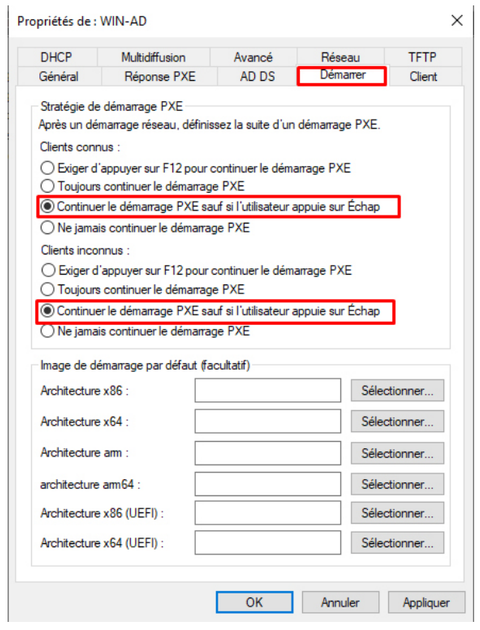
La configuration du service est terminée. Le service ne démarre pas c'est normal, cliquez sur Terminer



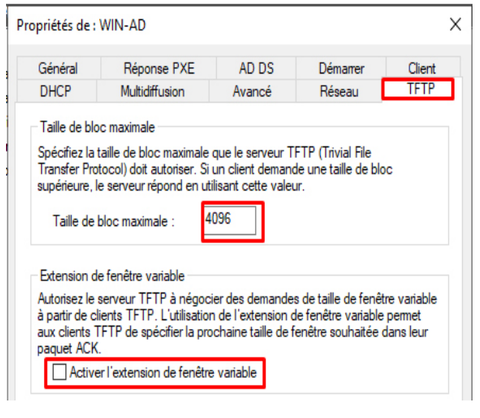
Ensuite clique droit -> Propriétés



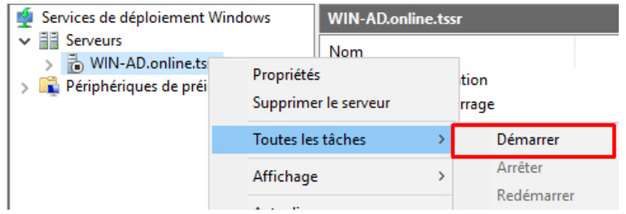
Dans l'onglet « Démarrer », cochez les deux points disant « Continuer le démarrage PXE sauf si l'utilisateur appuie sur Echap », cela permettra de ne pas avoir à appuyer sur F12 pour lancer le boot PXE sur les postes clients.



Ensuite, allez dans l'onglet « TFTP » pour décocher la case « Activer l'extension de fenêtre variable » et dans la partie « Taille maximale de bloc », vous pouvez mettre 2048 ou 4096 par exemple. Cette configuration permettra d'éviter une erreur bien connue (erreur 0x000000c1) lors du démarrage en réseau



Appliquer les modifications et cliquer sur OK et fermez les propriétés, on peut désormais démarrer le service.



Un message vous confirme le bon démarrage du service. Cliquez sur OK et fermez la console WDS, nous n'en avons plus besoin pour le moment et il n'y a pas à cette étape d'images de démarrage ou d'installation à ajouter.

4. Installation des outils ADK et MDT

Pour que notre infra fonctionne correctement, nous aurons besoin d'installer tous les outils nécessaires, à savoir **ADK**, **PE** et **MDT.**

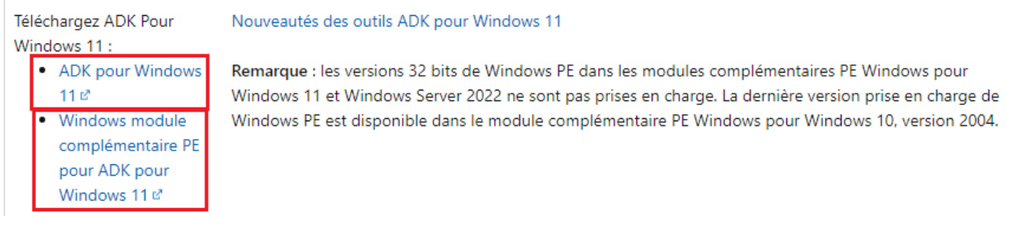
Pour rappel, ADK (le kit d'installation automatisée Windows, en français dans le texte), est une suite d'outils fournie gratuitement par Microsoft pour aider au déploiement d'OS Windows.

PE (ou WinPE) est une extension de l'outil ADK qui fonctionne de pair avec lui. C'est une sorte de « mini-OS » qui est lancé lors de l'installation de Windows ou lors de la capture d'un master entre autres. Le PE est la partie qui permet d'installation un OS sur un disque dur, c'est également par le PE qu'on peut réparer une image d'installation de Windows par exemple.

Petite mise en garde cependant ! Je ne télécharge jamais les versions données en haut de page qui sont censées être les dernières car à chaque fois je me retrouve avec des bugs relous qui me font juste perdre du temps

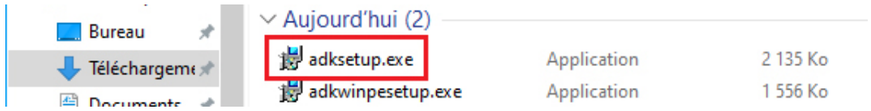
Pour récupérer le kit ADK et module PE rdv sur https://learn.microsoft.com/fr-fr/windows-hardware/get-started/adk-install

Dans mon cas, je vais prendre le kit ADK et le module PE pour Windows 11 mais ça fonctionnera également pour Windows 10. Vous n'avez qu'à cliquer sur les 2 liens en bleus pour télécharger les exécutables sur votre serveur.



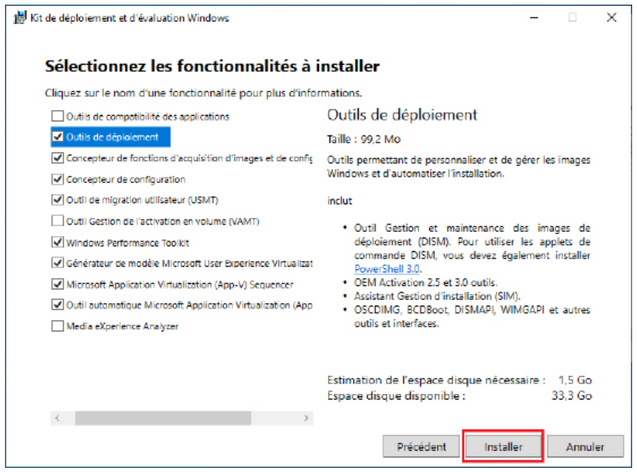
Installation de ADK et WinPE

Normalement on se retrouve avec les 2 exécutables d'ADK et de WinPE



On exécute ADK

Vous pouvez cliquer sur le bouton « Suivant » tout le long. Sauf si vous êtes certains de ne pas avoir besoin à un moment d'une fonctionnalité spécifique d'ADK, vous pouvez tout laisser cocher par défaut et cliquer sur le bouton « Installer ».

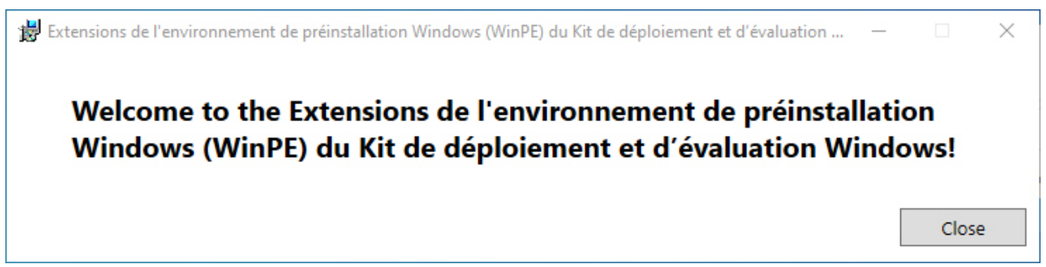


Laisser l'installation se faire

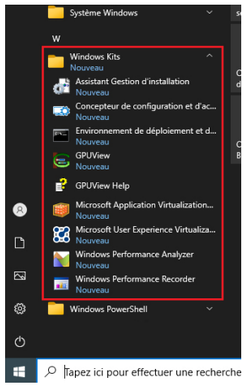
Une fois terminée, vous pouvez fermer la fenêtre et lancer l'exécutable « **adkwinpesetup** ».

Pour le module PE de ADK, l'installation est similaire, laissez tout **par défaut**.

Une fois l'installation terminée, vous pouvez fermer la fenêtre du setup de WinPE.



Vous pourrez retrouver tout ce que contient ADK dans le menu démarrer du serveur, dossier « Windows Kits ».

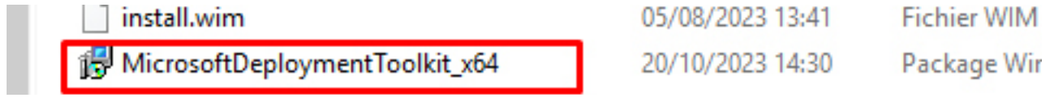


Installation de MDT

Vous pouvez le télécharger sur la page suivante : https://www.microsoft.com/en-us/download/details.aspx?id=54259

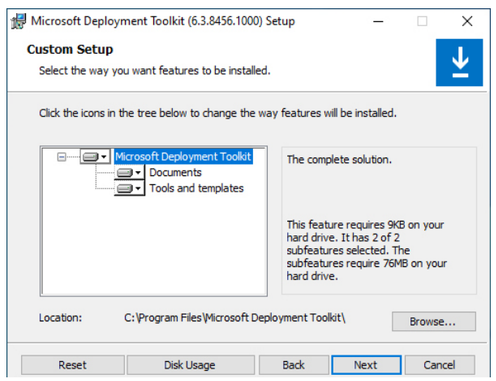
Choisissez la version **x64** après avoir cliquer sur le bouton rouge « **Download** ».

Double-cliquez sur le fichier « MicrosoftDeploymentToolkit_x64 » pour lancer l'installation de MDT sur votre serveur.



L'installation est vraiment très simple. Commencez par cliquer sur Next puis accepter le contrat d'utilisation

On va choisir d'installer la solution complète du produit donc on ne touche à rien et on clique sur Next.



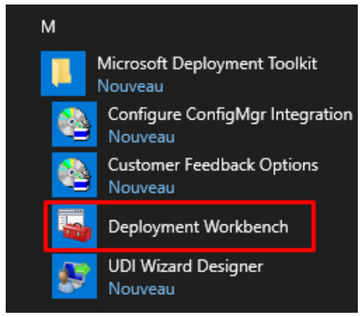
Choisissez ou non d'envoyer des infos à Microsoft sur votre utilisation du produit et cliquez de nouveau sur Next.

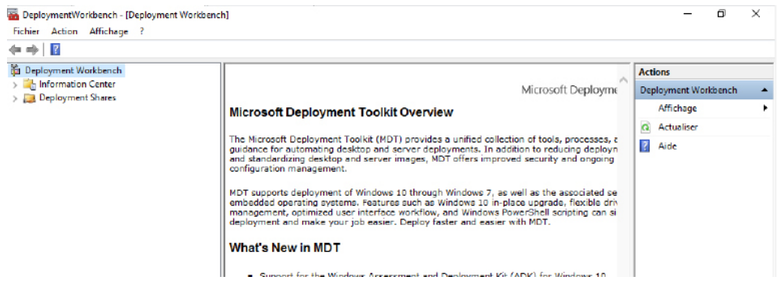
Et enfin, cliquez sur « Install ».

Voilà MDT est installé ! Vous pouvez retrouver les outils que MDT embarque dans le menu démarrer du serveur, partie « Microsoft Deployment Toolkit ».

Première configuration de MDT via la console Deployment Workbench

Ouvrir la console «Deployment Workbench»

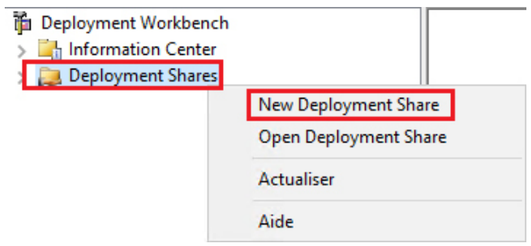




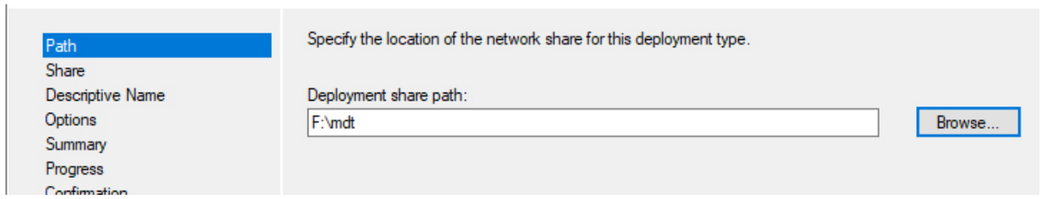
Cette console mmc va centraliser toutes les données dont on aura besoin dans des partages appelés « Deployment Shares » (en haut à gauche de la console).

Dans ces partages, nous trouverons par exemple les fichiers d'images d'installation des OS, les fichiers d'images de démarrage également (le PE, que nous utiliserons sur WDS dans le cadre de ce tuto pour booter en réseau), les fichiers de réponses, les applications, les scripts, les séquences de tâches... tout en fait ! C'est le point névralgique pour vos déploiements à l'aide de MDT.

Notre première mission ici est donc de créer un 1er « deployment share ». Pour cela, faites un clic droit sur la partie « Deployment Shares » en haut à gauche de la console et ensuite sur « New ... ».



La première fenêtre vous demande la localisation de ce futur partage sur le serveur. Je vous conseille fortement de ne pas le mettre sur le même disque que l'OS. J'ai donc crée un disque F: dédié à WDS et MDT (il faut que le dossier « MDT » existe dans le lecteur F sinon vous aurez une erreur, pensez bien de le créer en amont).

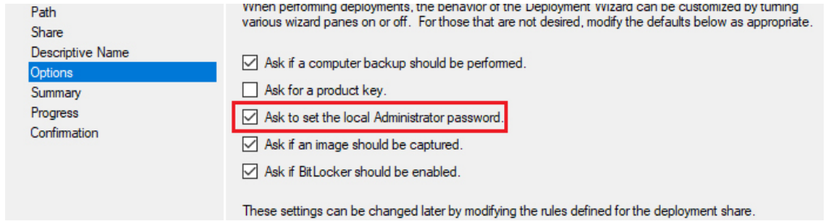


Vous pouvez ensuite changer le nom du partage. Je vais laisser par défaut.

Vous pouvez ensuite ajouter si besoin une petite description

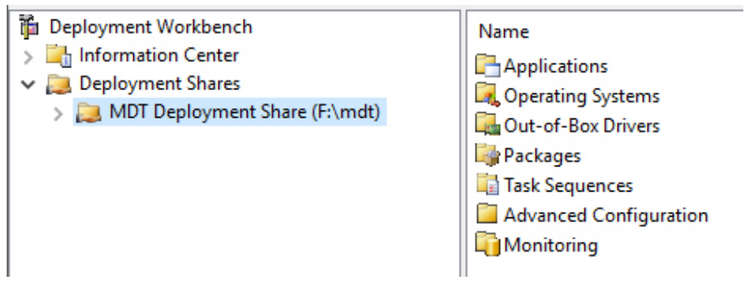
Ensuite il faudra sélectionner des options qui seront vues ou non pendant le déploiement avec MDT, les options ici sont les suivantes :

- Demande si une sauvegarde doit avoir lieu
- Demande de saisir une clé de licence
- Demande de définir le mot de passe de l'administrateur local de la future machine
- Demande si une image de capture doit être faite de la machine avant déploiement
- Demande si bitlocker doit être activé
- Dans cette partie, je coche la case concernant le mot de passe de l'administrateur local en plus des 3 autres déjà cochées par défaut

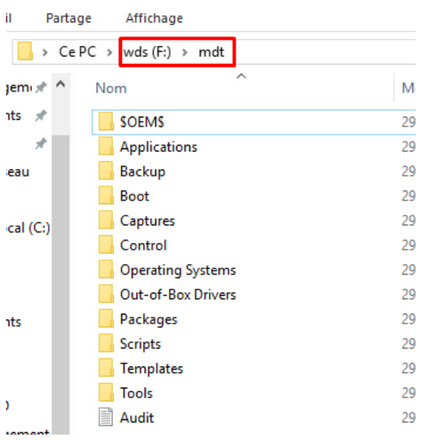


Vous avez ensuite un petit récap de l'ensemble, cliquez sur Next pour lancer la création du partage de déploiement.

Le nouveau partage de déploiement sera disponible dans la console Deployment Workbench.



Si vous allez voir le contenu du partage sur le serveur, vous aurez cette arborescence



C'est dans ce dossier partagé que seront stockés les fichiers de configurations, les séquences de tâches, les images d'installation et de démarrage, les applications... ouais bon bref tout quoi

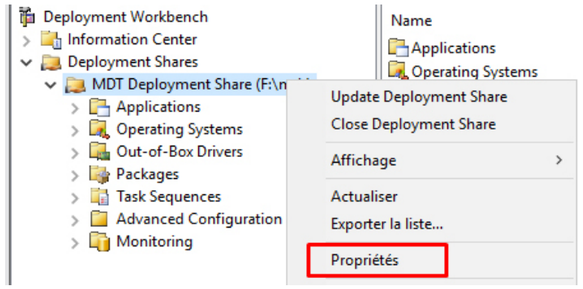
Il est conseillé de créer un utilisateur dans mon AD dédié au Déploiement mais dans mon cas ce sera l'administrateur du domaine qui gère ça

Si c'était un utilisateur dans l'AD autre que l'administrateur alors il faut lui donner les droits sur le partage « deploymentshare» pour que cet utilisateur puisse lire les infos du déploiement dans le dossier. Dans notre cas l'administrateur à les droits de lecture par défaut

Voir précision sur neptunet: https://neptunet.fr/mdt-deploy/

Une fois ceci fait, nous pouvons retourner sur la console DeploymentWorkbench.

Faites un clic droit sur le nom de votre Deployment Share et allez dans ses propriétés.



Dans l'onglet Général, partie « Platforms Supported », je vais décocher x86 car je n'aurais pas d'architecture en 32 bits.

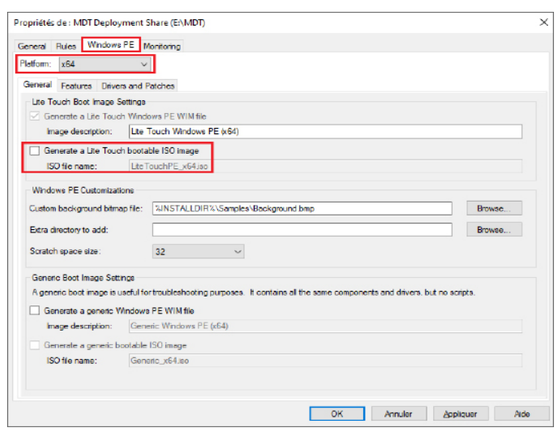
Dans l'onglet « **Rules** », vous pourrez **automatiser tout ou parties de vos déploiements**. Cela se fait grâce à deux fichiers de configuration essentiels de MDT nommés respectivement :

- **Bootstrap.ini**, qui sert surtout à l'initialisation du déploiement via MDT pour accéder au deploymentshare
- **Customsettings.ini**, qui va permettre de pré-remplir ou passer complètement les questions de base telles que le nom du PC, l'ajout à un domaine, le fuseau horaire, le mot de passe administrateur local, la conservation des données…

Ne modifiez rien dans ces 2 parties.

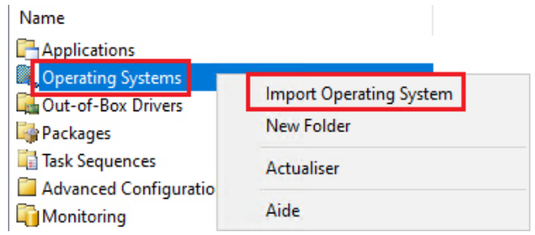
Dans l'onglet « Windows PE », on va pouvoir gérer la création de la partie PE du déploiement, l'équivalent du fichier « boot.wim » dispo sur les ISO de Windows.

Dans cet onglet, je vais juste aller dans la partie « Platform x64 » et décocher la case « Generate a Lite Touch bootable ISO image » car je ne veux pas un ISO bootable mais seulement un fichier .wim que j'ajouterai en tant qu'image de démarrage sur WDS.

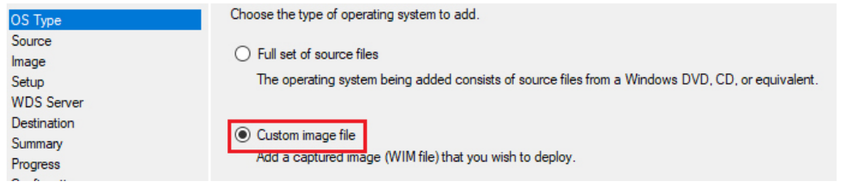


Ajout de Windows 10 ou 11 et de sa séquence de tâches

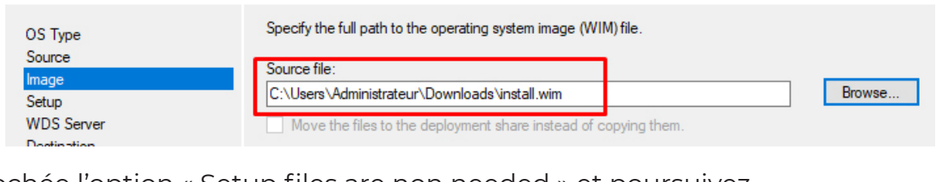
On va ajouter une image d'installation de Windows 10 qui sera déployée via MDT, je vais prendre le fichier « install.wim » tout fait dispo dans l'ISO officielle de Windows 11 Entreprise pour ce tuto.



Choisissez la seconde option, à savoir « Custom image file » pour importer un fichier .wim.



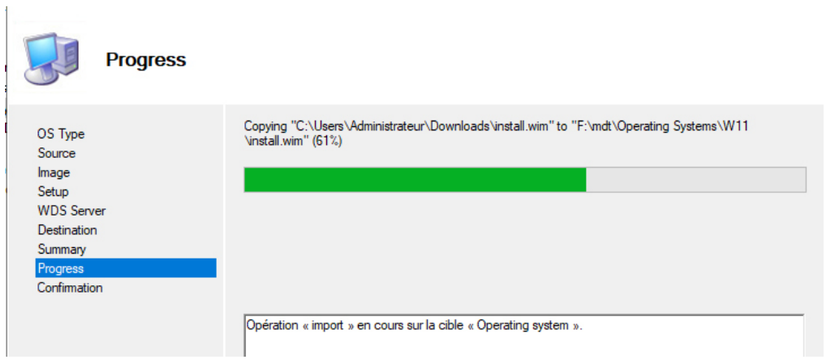
Choisissez la source où se trouve votre fichier .wim



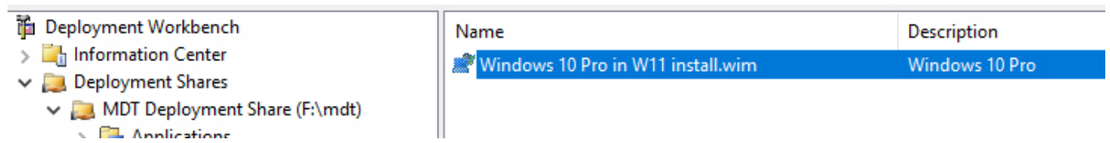
Laissez cochée l'option « Setup files are non needed » et poursuivez.

Définissez ensuite le nom du dossier qui sera créé et contiendra l'image de Windows 11.

Finissez l'installation

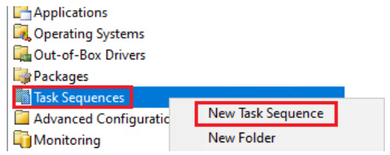


Vous retrouverez l'image de l'OS Windows 10 disponible dans la console de déploiement, partie « Operating Systems ».

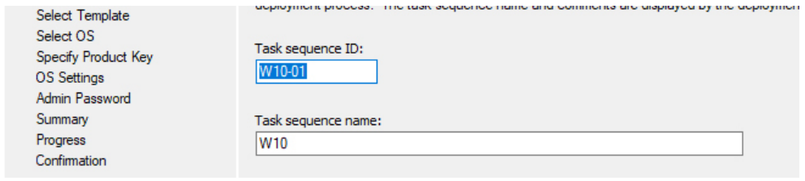


Nous allons maintenant créer une séquence de tâches. Pour faire simple, c'est une suite de tâches, d'actions, qui seront ou pourront être exécutées au besoin lors du déploiement (et même après) et qui sont personnalisables. Par exemple sur quel disque doit avoir lieu l'installation d'un OS, est-ce que si c'est une capture d'un master on fait un sysprep, est-ce qu'il faut exécuter tel ou tel script etc...

Pour créer cette séquence, faites un clic droit sur « Task Sequences » et cliquez sur « New Task Sequence ».

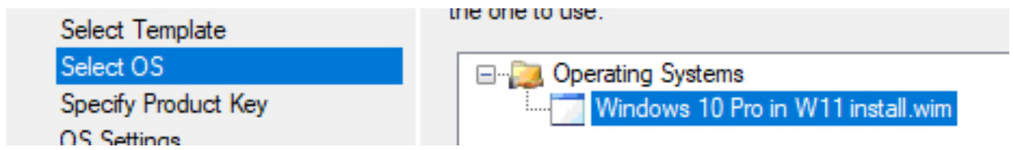


Définissez un ID (identifiant) pour cette séquence de tâche (vous pouvez mettre 01, 001, 999,truc1, etc...) et un nom également. Le nom sera vu dans MDT, veillez donc à mettre des noms assez parlant pour se repérer dans le cas où vous avez plusieurs séquences de tâches.



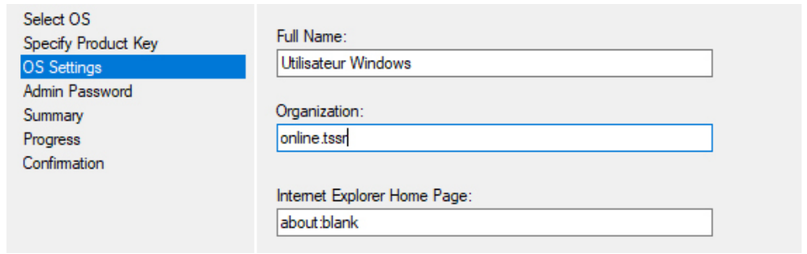
Ensuite on laisse par défaut sur « Standard Client Task Sequence » car ce qu'on veut c'est faire une simple installation complète d'un OS et on poursuit.

Vous devez choisir quel OS sera déployé via cette séquence de tâches. Ici je n'en ai qu'un donc c'est simple, je clique sur Windows 10 Pro et je continue

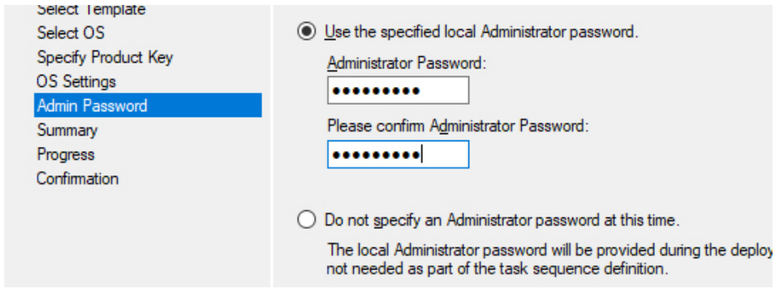


Après Laissez l'option « Do not specify a produit key at this time » qui est cochée par défaut et poursuivez.

Définissez le nom complet d'un utilisateur et l'organisation (vous pouvez laisser par défaut et juste mettre le nom de votre entreprise, ça n'a pas vraiment d'importance).

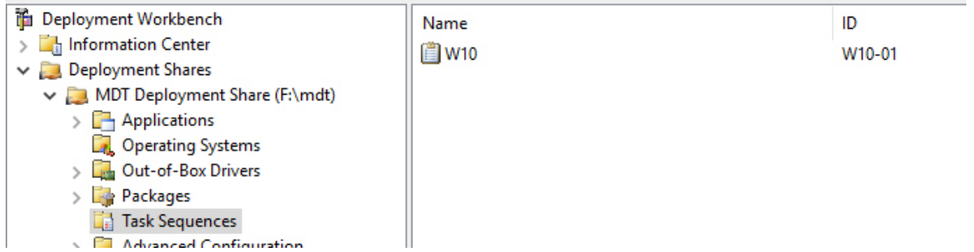


Définir ensuite le mdp du compte Administrateur local des postes aux déploiements



Quand c'est OK, on peut fermer en cliquant sur Finish.

On retrouve bien la séquence. Allons voir ses propriétés en faisant un clic droit sur son nom.

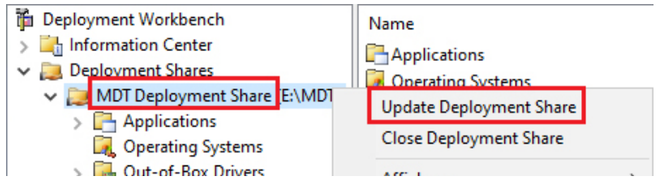


Dans l'onglet « OS Info », ce qui est intéressant c'est le bouton « Edit Unattend.xml » car il va nous permettre de voir et d'éditer le fichier de réponses qui est utilisé pour cette séquence de tâches. Mais dans notre cas on ne crée pas de fichier de réponse personnalisé donc on peut passer

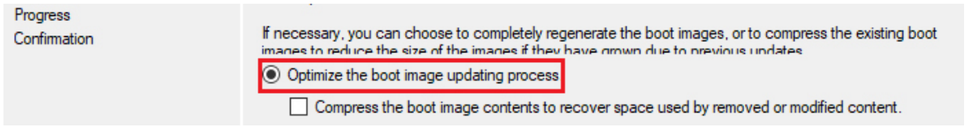
Génération de l'image de démarrage Lite Touch et ajout à WDS

Pour booter, nous avons besoin d'une image de démarrage appelée ici « Lite Touch PE ». Une fois qu'on a terminé nos configurations de déploiement, on doit générer cette image.

Faites un clic droit sur votre partage de déploiement dans la console Deployment Workbench et cliquez sur « Update Deployment Share ».



Le menu va proposer 2 options, à savoir générer une image de boot complète ou alors mette à jour une existante. Vous pouvez ici laisser l'option « Optimize the boot image updating process » car il s'agit ici de la première génération de l'image de boot donc elle sera forcément complète dans tous les cas.

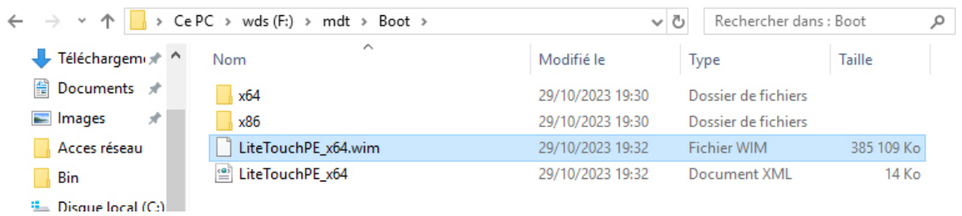


Info ++ : Certaines modifications dans votre deployment share nécessiteront la mise à jour de ce dernier, il faudra penser à refaire cette manipulation et remettre la future image .wim générée dans WDS sinon ça ne fonctionnera pas comme vous vous y attendez.

Faîtes suivant pour les fenêtres suivantes

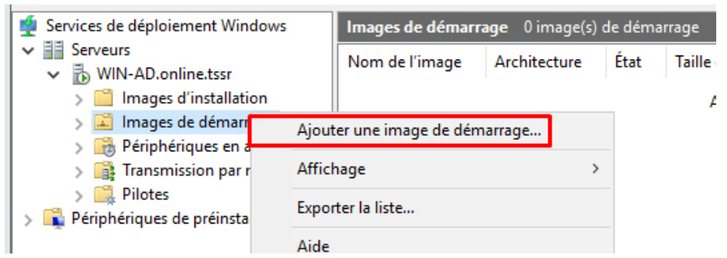
Une fois que la fenêtre vous indique que c'est terminé, vous pouvez cliquer sur Finish.

Le fichier « LiteTouchPE_x64.wim » généré sera stockée dans le dossier « Boot » de votre DeploymentShare (qui chez moi se trouve dans F:\mdt).



Il ne nous reste plus qu'à mettre ce fichier dans les images de démarrage du service WDS.

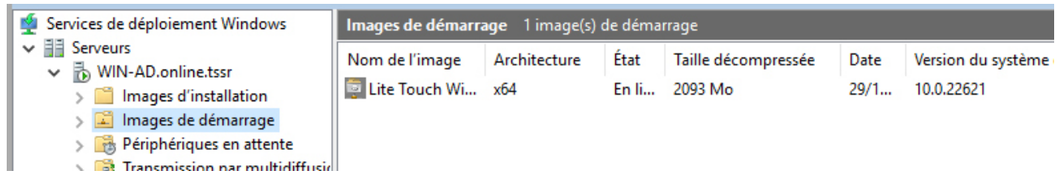
Ouvrez la **console de gestion des services de déploiement Windows.** Fait un clic droit « Images de démarrage » et cliquez sur « Ajouter une image de démarrage ».



Dans le champ concernant l'emplacement du fichier, vous pouvez cliquer sur Parcourir et allez chercher le fichier « LiteTouchPE_x64.wim ».

Faîtes suivants sur les fenêtres suivantes et une fois fini, cliquez sur Terminer.

L'image de boot qui sera utilisée par MDT est disponible dans WDS. En démarrant sur le réseau, les futurs postes à déployer chargeront et utiliseront cette image de démarrage.



Notre déploiement de base de Windows 10 via MDT et WDS et désormais prêt !

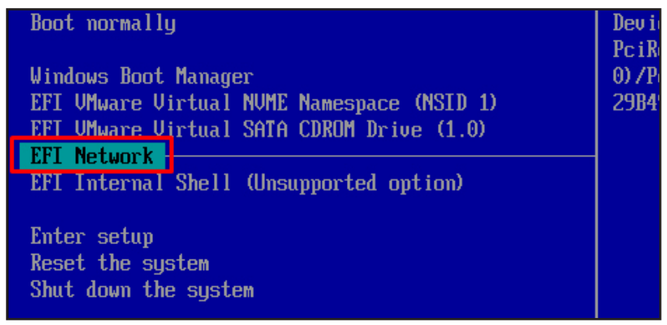
Test de déploiement de Windows 10 via le réseau

Pour ce faire il suffit de brancher notre pc à notre VLAN 40 et de boot via le réseau

*Si nous sommes sur une VM, il faut bien vérifier que les 2 VM à savoir Windows server et le client soient bien sur le même réseau virtuel (bah oui sinon ça ne va pas communiquer ce n'est pas magique...).

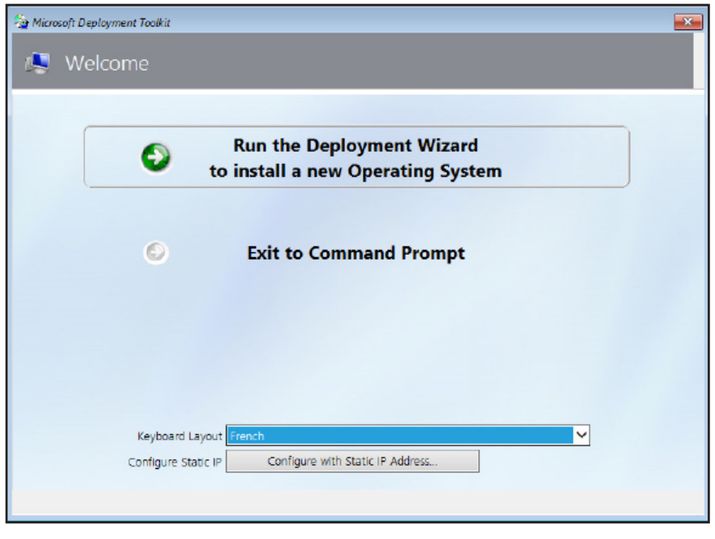
Info ++ : N'oubliez pas que si vous bossez en physique ou avec un hyperviseur, vous n'aurez pas forcément les mêmes écrans que moi donc il faudra s'adapter, l'idée reste de faire un boot PXE, la suite sera similaire.

Choisir le boot via le réseau

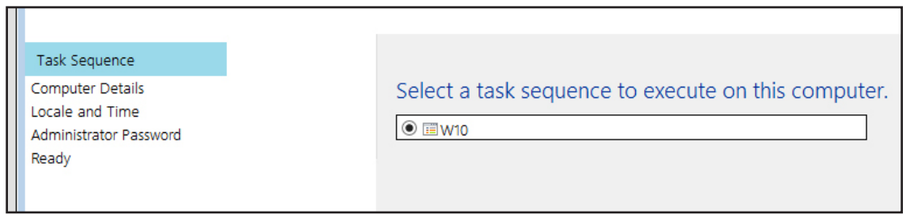


Le pc client communique avec le serveur WDS

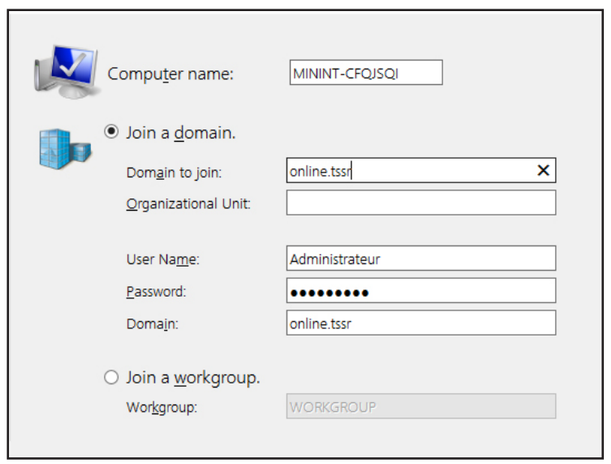
On arrive sur MDT, il suffit de suivre ce qu'on nous demande ce n'est pas bien compliqué



Choix de la séquence

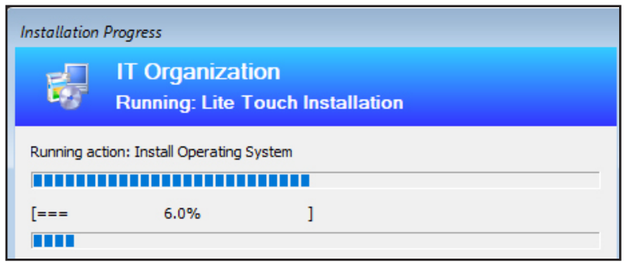


Rejoindre le domaine

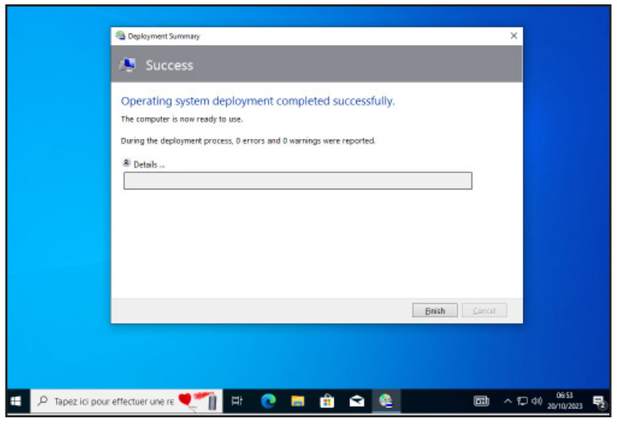


Continuer en validant / entrant les autres paramètres

Ensuite l'installation de l'OS ce fait (ça prend un peu de temps)



Après ça c'est terminé, l'installation d'un poste via le réseau fonctionne



Serveurs de mises à jour – WSUS (Rapprochez-vous du DAF)

Qu'est-ce que WSUS?

WSUS (Windows Server Update Services) permet aux administrateurs informatiques de déployer les dernières mises à jour de produits Microsoft. Grâce à WSUS, vous pouvez gérer entièrement la distribution des mises à jour publiées par Microsoft Update sur les ordinateurs de votre réseau.

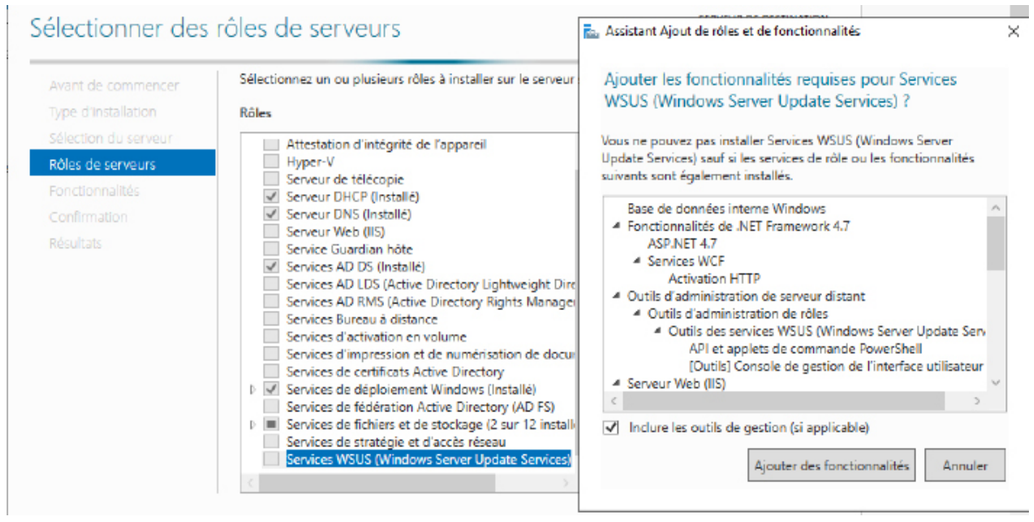
Installer et configurer WSUS dans votre infrastructure

Source: https://www.it-connect.fr/chapitres/installation-de-wsus-sur-windows-server-2022/

Installation du rôle WSUS

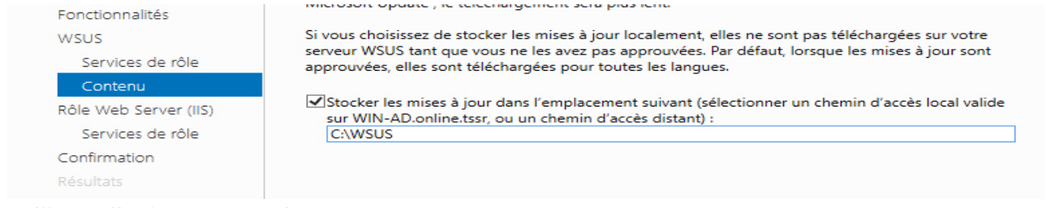
Ouvrez le « Gestionnaire de serveur », cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».

Puis choisir «Windows Server Update Services»



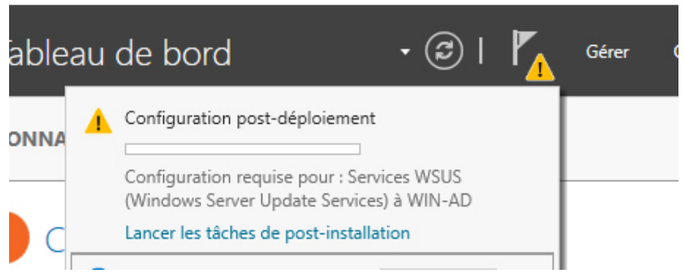
Continuer l'installation sans rien modifier jusqu'à la sélection de l'emplacement du contenu

Indiquez l'emplacement des données WSUS, notamment les fichiers de mises à jour.



Finissez l'installation normalement

En temps normal, l'installation ne prend que quelques minutes, mais elle ne s'arrête pas là. Au sein du « Gestionnaire de serveur », nous pouvons remarquer un avertissement en haut à droite : il faut démarrer les tâches de post-installation de WSUS en cliquant sur le lien.

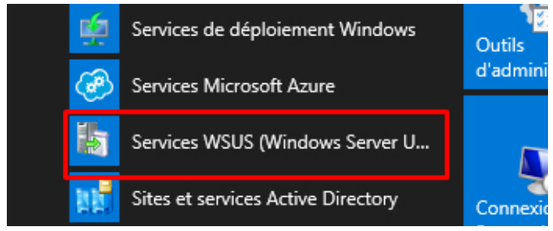


Patientez pendant ce temps : WSUS crée la base de données. Si vous obtenez une erreur lors de ces étapes de post-installation, je vous invite à regarder les logs à cet emplacement :

C:\Users\<utilisateur>\AppData\Local\Temp\WSUS_PostInstall_<date>.log

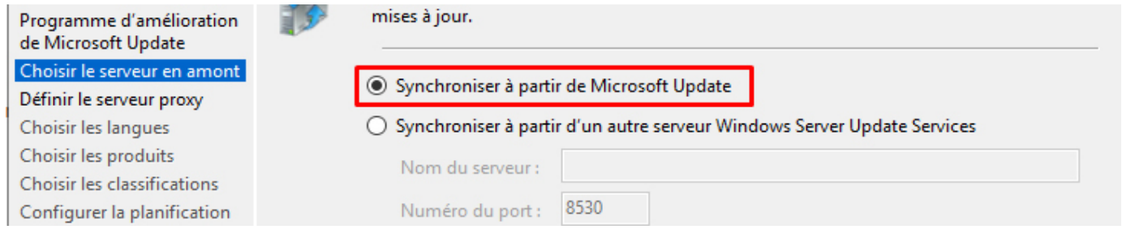
Configuration de base de WSUS

WSUS est installé sur notre serveur et la base de données est créée, désormais, nous pouvons lancer la console « Services WSUS » afin d'effectuer la configuration de base.



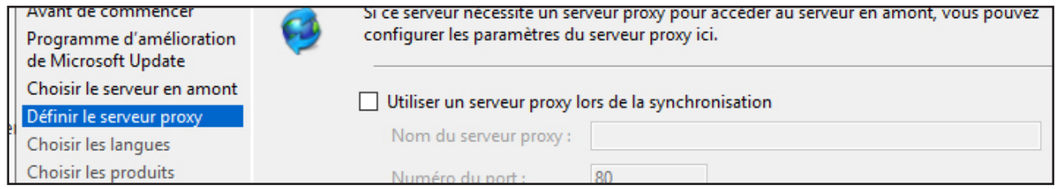
Au lancement Cliquez sur « Suivant » / « Next » pour commencer. ensuite si vous souhaitez participer du programme d'amélioration de Microsoft Update, cochez l'option, sinon décochez cette option. Poursuivez.

Sur quelle source notre serveur WSUS doit-il s'appuyer pour se synchroniser et obtenir les nouvelles mises à jour ? Deux options : à partir des serveurs de Microsoft Update (Synchronize from Microsoft Update) ou à partir d'un autre serveur WSUS (Synchronize from another Windows Server Update Services server).



Si vous utilisez un proxy pour accéder à Internet et qu'il doit être déclaré, c'est le moment. Sinon, poursuivez sans cocher l'option.

Note : les communications avec les serveurs de Microsoft Update s'effectuent en HTTPS avec le port 443. Veillez à autoriser ce flux au sein de votre réseau.



Cliquez sur « Démarrer la connexion » / « Start Connecting » pour que notre serveur WSUS se connecte sur les serveurs Microsoft Update. Cela va lui permettre de récupérer la liste des systèmes d'exploitation et logiciels pris en charge, les types de mises à jour, et les langages disponibles.

La prochaine étape consiste à choisir les langues de mises à jour. Si vous utilisez seulement des systèmes d'exploitation en français pour vos postes de travail et vos serveurs, vous pouvez choisir « Français » (ou « French »).

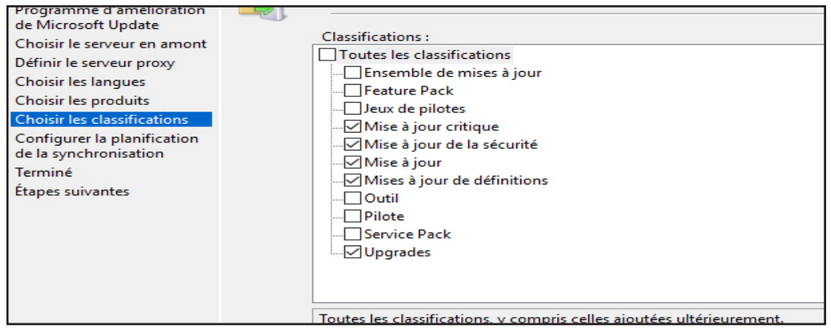
Si vous utilisez Windows en FR sur les postes de travail et en version EN pour les serveurs, choisissez également « Anglais » (ou « English »).

Ensuite, nous devons sélectionner les produits pour lesquels nous souhaitons synchroniser les mises à jour. La liste est très longue et très complète (Exchange, Office, Edge, SQL Ser ver, etc…), vous devez cocher les produits correspondants à ceux que vous utilisez !

Pour plus de détails rendre-vous sur le site d'itconnect, nous ce qu'on va faire c'est de recevoir les mises à jour pour Windows Server 2019 et tous les Windows car c'est ce que j'ai besoin

L'étape suivante concerne la classification des mises à jour, c'est-à-dire les types de mises à jour qu'il faut synchroniser sur le serveur WSUS. Les catégories « Mises à jour critique », « Mise à jour de la sécurité » et « Mise à jour » permettent d'obtenir les mises à jour mensuelles publiées par Microsoft, tandis que la catégorie « Mises à jour de définitions » correspond aux mises à jour Windows Defender.

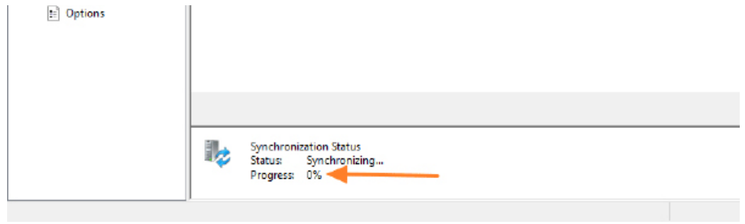
Dans un environnement où il y a la volonté de distribuer les mises à niveau de Windows via **WSUS**, il sera nécessaire de cocher l'option « **Upgrades ».**



Cochez l'option « Commencer la synchronisation initiale » / « Begin initial synchronization » si vous souhaitez réaliser une première synchronisation dès maintenant.

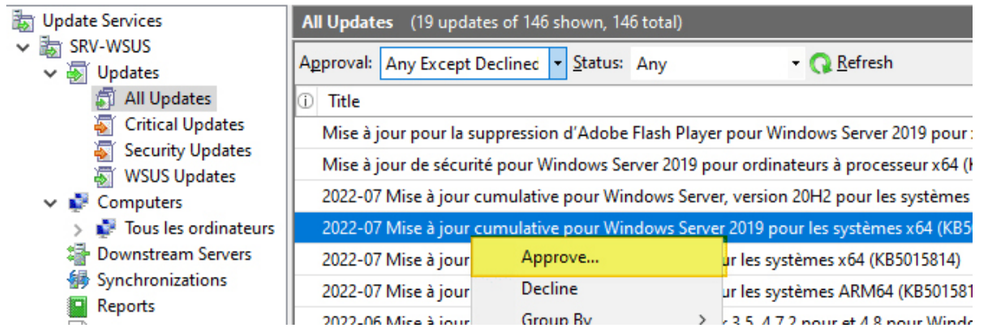
Continuer l'installation sans rien modifié à partir de là et Cliquez sur « Terminer » / « Finish » : l'initialisation de WSUS est terminée !

Dans la console WSUS, si l'on clique sur la section « Synchronisations » à gauche, nous pouvons voir que la synchronisation est en cours puisqu'elle est sur l'état « En cours » / « Running ».

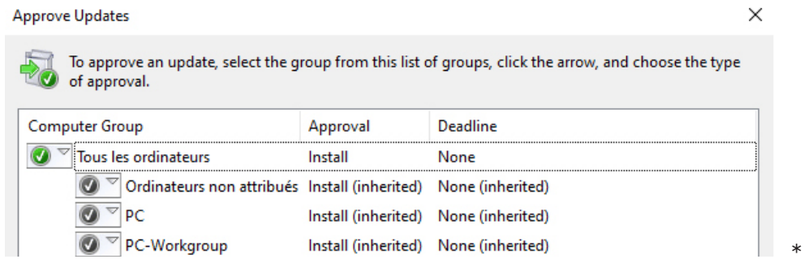


Vous devez approuvez certaines mises à jour avant de les appliquer sur un « pool » d'ordinateurs critiques de l'atelier

Pour cela il faut sélectionner une mise à jour et faire une clique droit dessus et «Approuver»



Après avoir cliqué sur le bouton, une seconde fenêtre va s'ouvrir. Par défaut, il vous sera proposé d'approuver la mise à jour pour « Tous les ordinateurs » donc cela s'appliquera à tous les groupes de votre serveur WSUS (par héritage). Mais il est possible de ne pas approuver aussi.



La mise à jour est approuvé, WSUS téléchargera les sources d'installation depuis les serveurs de Microsoft et commencera le deploiement sur les postes
* Screen d'illustration, en vrai on a un groupe de PC «Critique» et c'est lui qu'il faut sélecionner

Serveur de clients légers – RDS (Rapprochez-vous du DAF)

Qu'est-ce que RDS?

Les serveurs RDS « Remote Desktop Services », autrefois appelés TSE, dits « Terminal Server Edition » sont un ensemble de composants de Microsoft Windows qui permettent à un utilisateur d'accéder à des applications ou des données stockées sur un ordinateur distant, au moyen d'une connexion réseau dite « Connexion Bureau à distance ». Lorsque les connexions à distance à votre PC sont autorisées, cet appareil peut être utilisé pour accéder à l'ensemble des applications, fichiers et ressources réseau comme si vous étiez assis à votre bureau.

Comment dimensionner un serveur RDS (quelles sont les configurations techniques minimales à respecter pour accueillir les sessions de vos utilisateurs ?

Le dimensionnement d'un serveur RDS est important pour garantir les performances et la disponibilité du service. Les configurations techniques minimales à respecter pour accueillir les sessions de vos utilisateurs dépendent de plusieurs facteurs, notamment :

- Le nombre d'utilisateurs simultanés
- Les applications et les ressources utilisées par les utilisateurs
- La bande passante disponible

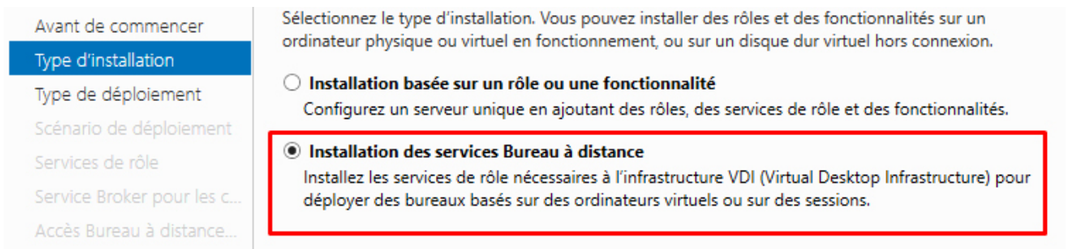
Il est impossible de savoir les configurations techniques minimales si on a pas les paramètres ci-dessus.

Vous devez commencer par déployer un serveur RDS et quelques applications Remote APP (NotePad, calculatrice) – Faites valider par votre formateur

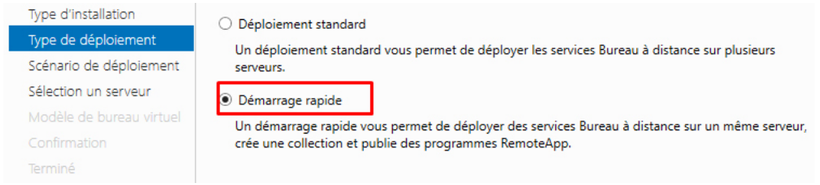
Installation du rôle RDS

Source: https://www.it-connect.fr/deploiement-rapide-dun-serveur-rds-avec-windows-server-2016/

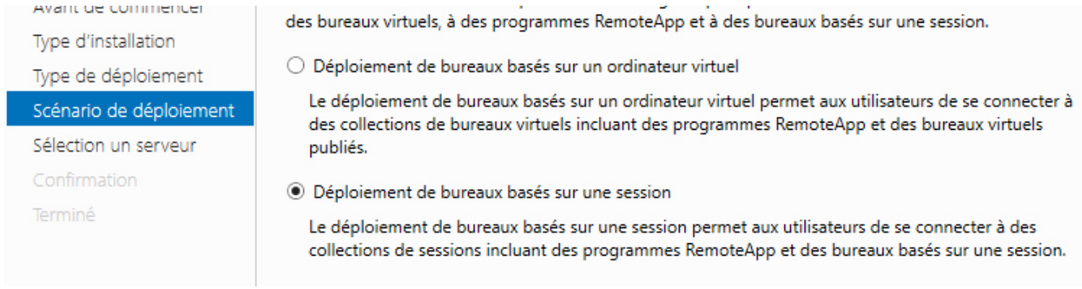
Alors que vous avez surement l'habitude de prendre le premier choix au lancement de cet assistant, cette fois-ci, sélectionnez «Installation des services Bureau à distance». Poursuivez.



.Choisir démarrage rapide

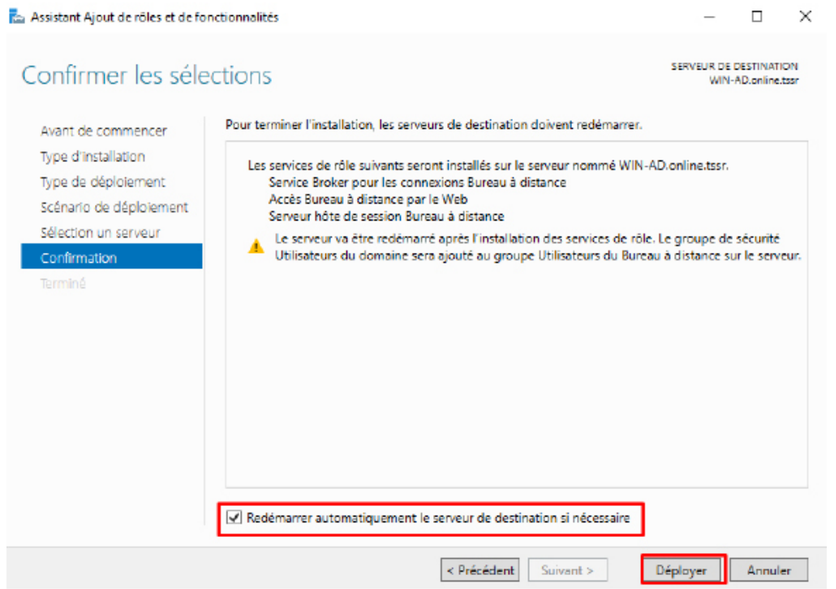


Maintenant, nous avons le choix entre un scénario de déploiement basé sur des sessions ou des ordinateurs virtuels, nous partirons sur la méthode basée sur les sessions. Choisissez «Déploiement de bureaux basés sur une session».

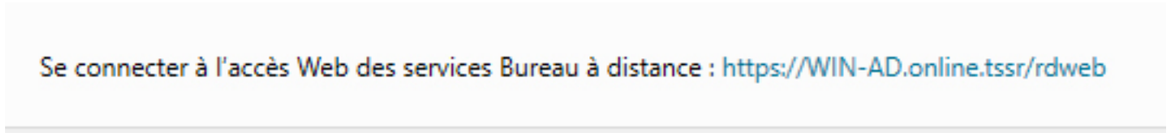


Sélectionner votre serveur

Pour commencer l'installation des rôles, cochez la case «Redémarrer automatiquement le serveur de destination si nécessaire» et cliquez sur «Déployer».



Après l'installation, On peut voir dans le bas de la fenêtre l'url pour accéder au portail Web des RemoteApp.

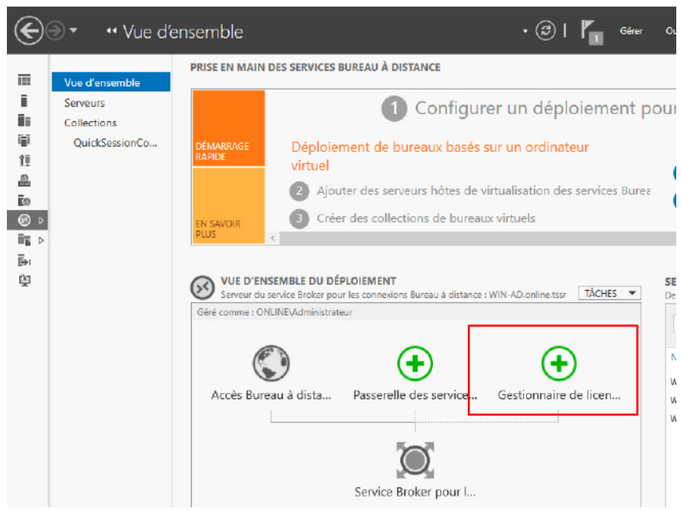


Configuration du serveur RDS

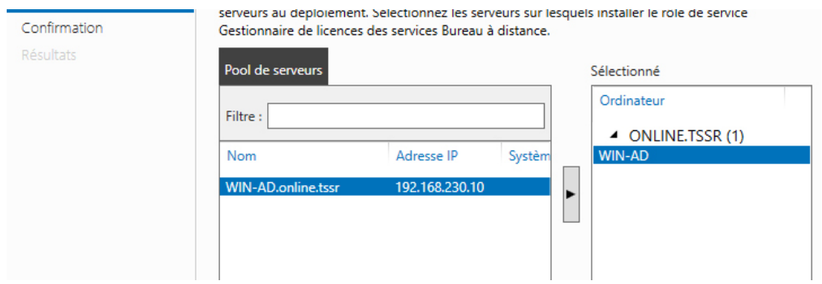
Dans notre cas on va garder la configuration de base, elle suffit (itconnect explique pour configurer)

Installation et configuration du serveur de licences

Dans Gestionnaire de serveur\Services Bureau à distance\Vue d'ensemble cliquer sur Gestionnaire de licences pour lancer l'assistant d'installation



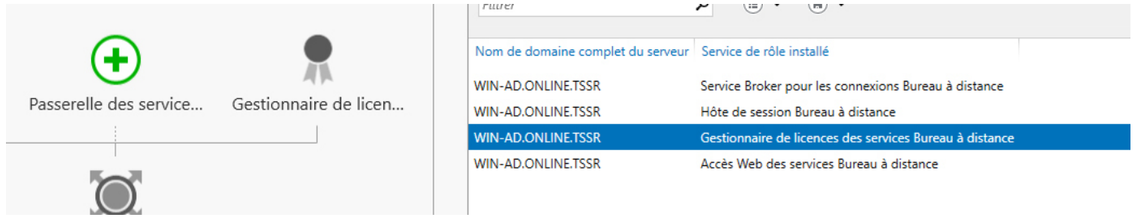
Sélectionner le serveur RDS et suivant



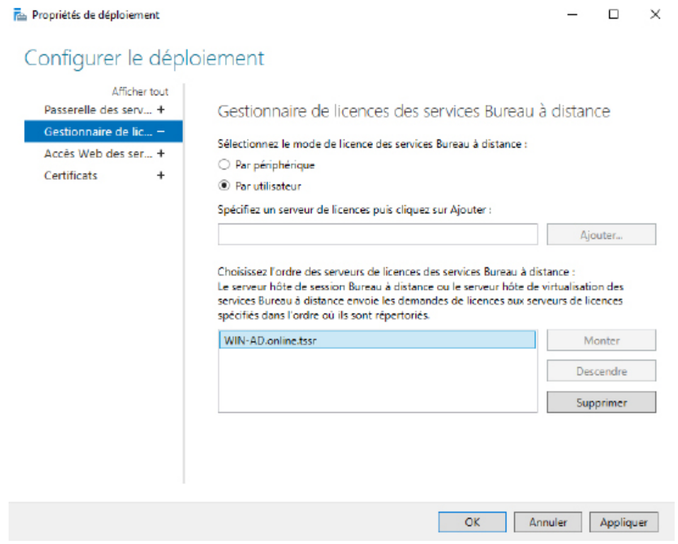
Ensuite Confirmer l'installation du serveur de licences en cliquant sur Ajouter

L'installation terminée, quitter l'assistant en cliquant sur Fermer

Dans le schéma de déploiement RDS, le gestionnaire de licence est disponible et on peut voir que celui-ci est installé sur le serveur WIN-AD

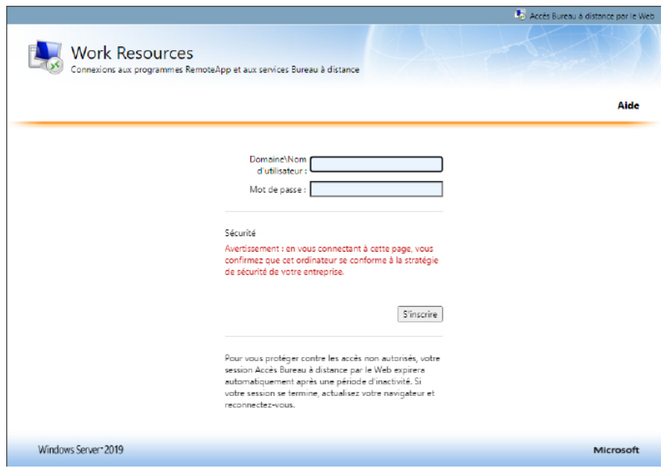


Il faut maintenant configurer le mode de licences? Cliquer sur TACHES et cliquer sur Modifier les propriétés de déploiement et entrer ces paramètres



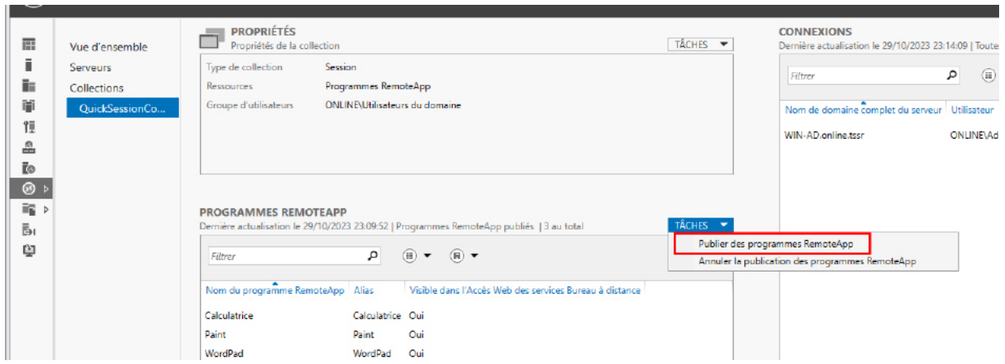
Voilà RDS est installé et configurer, il reste plus qu'a se connecter via un utilisateur en connexion en mode bureau à distance

Pour le remote App sur un navigateur rentrez l'URL suivante: https://WIN-AD.online.tssr/rdweb

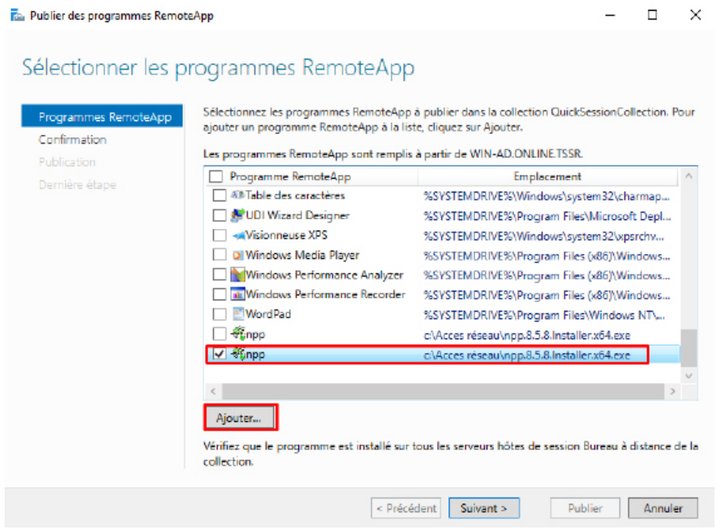


Ajouter des application Remote App

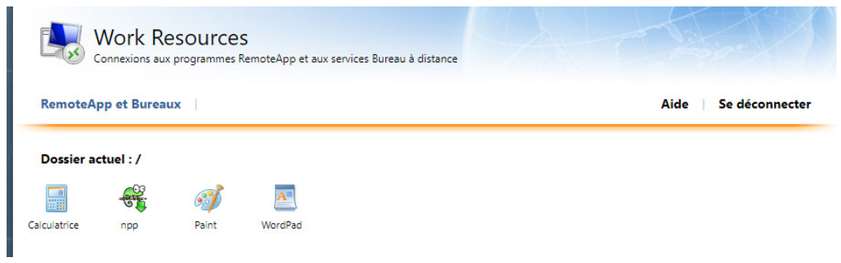
Dans Gestionnaire de serveur\Services Bureau à distance\Collections\QuickSessionCollection cliquez sur TACHES puis «Publier des programmes RemoteApp»



Ensuite on nous propose des programmes par défaut mais moi je veux installer Notepad++ donc je dois Ajouter un programme suffit de cliquer sur Ajouter et d'aller chercher l'exécutable de Notepad++ (il faut que le chemin soit un chemin UNC avec ce format \\Win-ad.online.tssr\c$\Acces réseau)



Il suffit de terminer la publication et c'est bon !



Notepad++ est bien là !