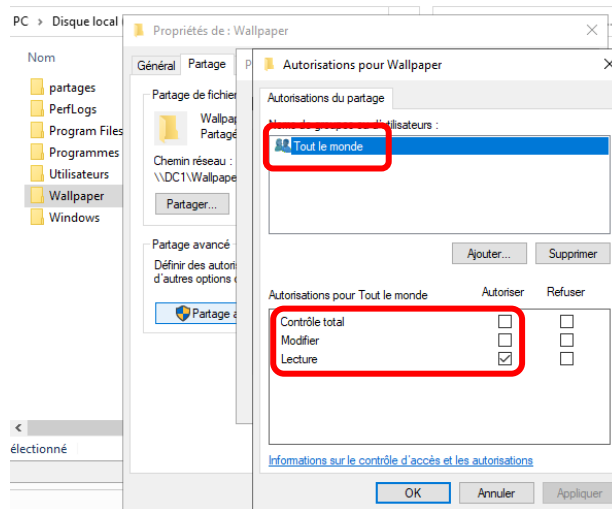
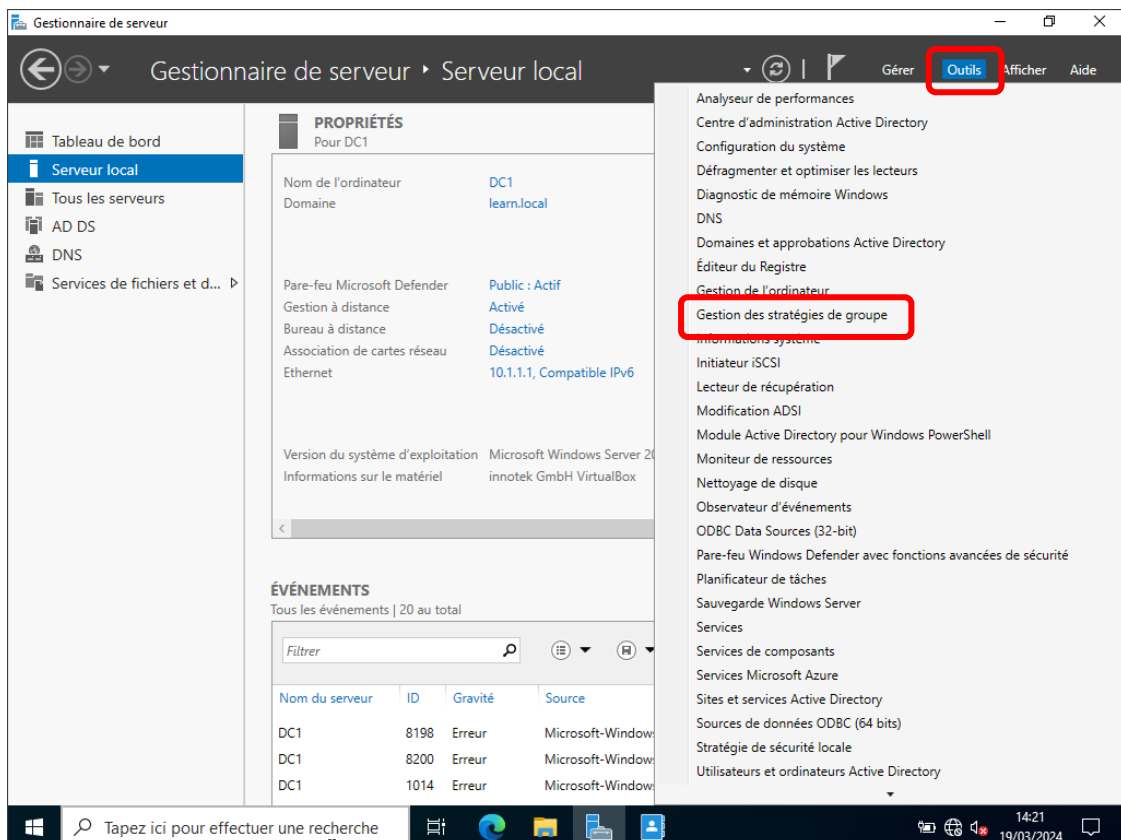


Forcer un fond d'écran avec le GPO

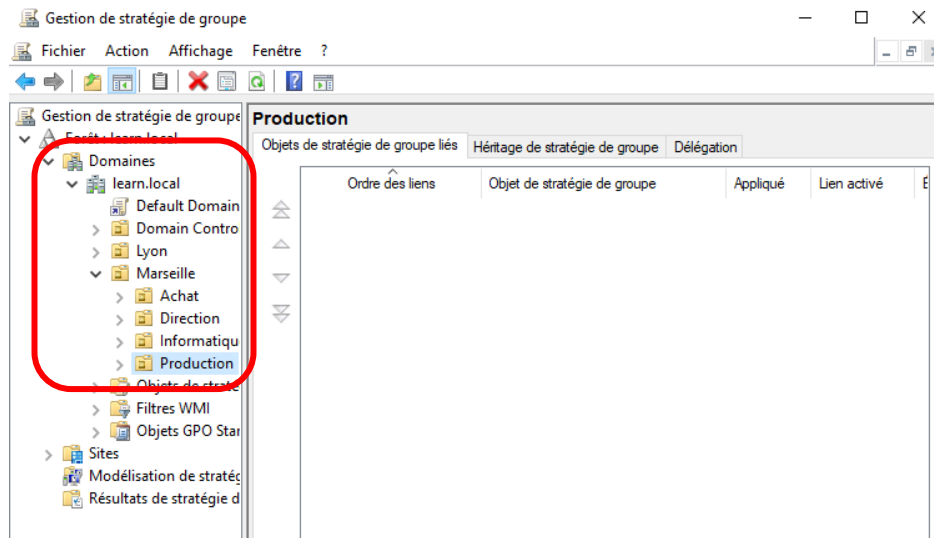
1. Tout d'abord, vous devez créer un dossier partager qui sera accessible à tout le monde en lecture seulement. Dans ce dossier, mettez tous les fonds d'écran que vous voudrez ajouter :



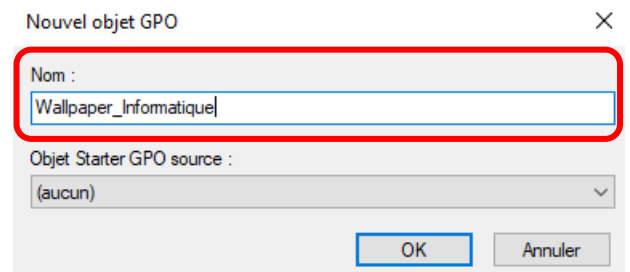
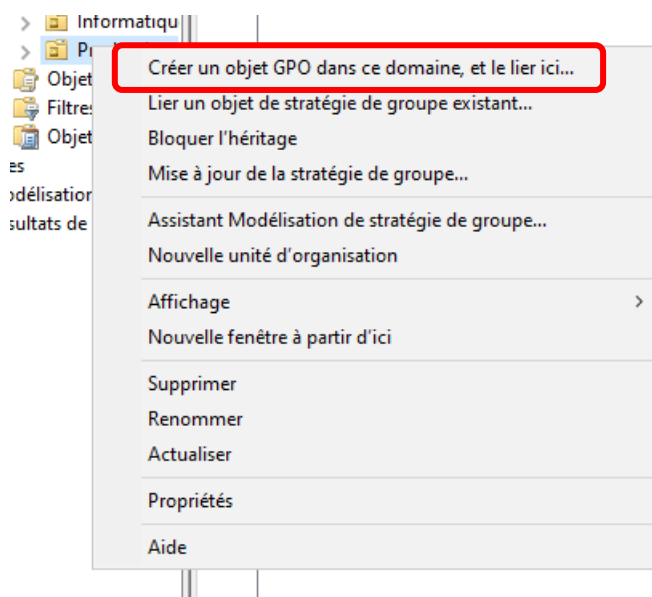
2. Ensuite, ouvrez le Gestionnaire de serveur, en suite cliquez sur « Outils », puis « Gestion des stratégies de groupe » :



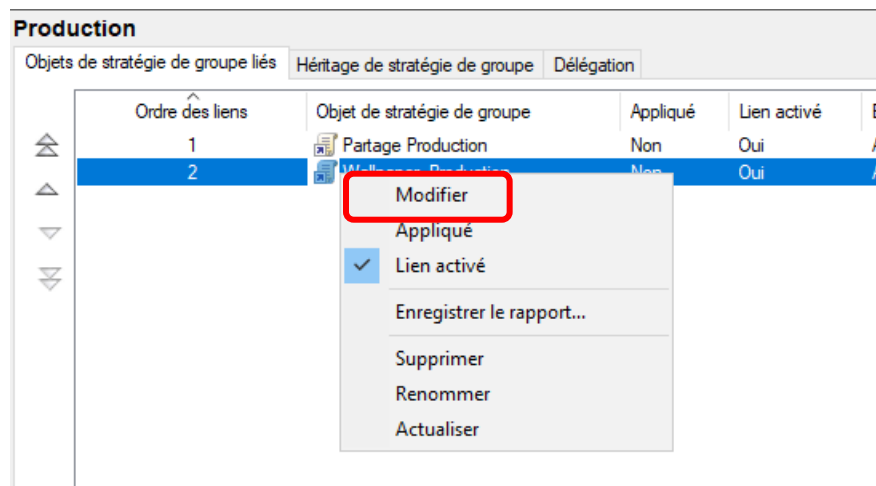
- Une fois la fenêtre ouverte, il faut aller dans « Domaine » puis « learn.local », en suite choisissez l'UO que vous voulez, dans notre cas nous allons prendre « Informatique » dans « Marseille » :



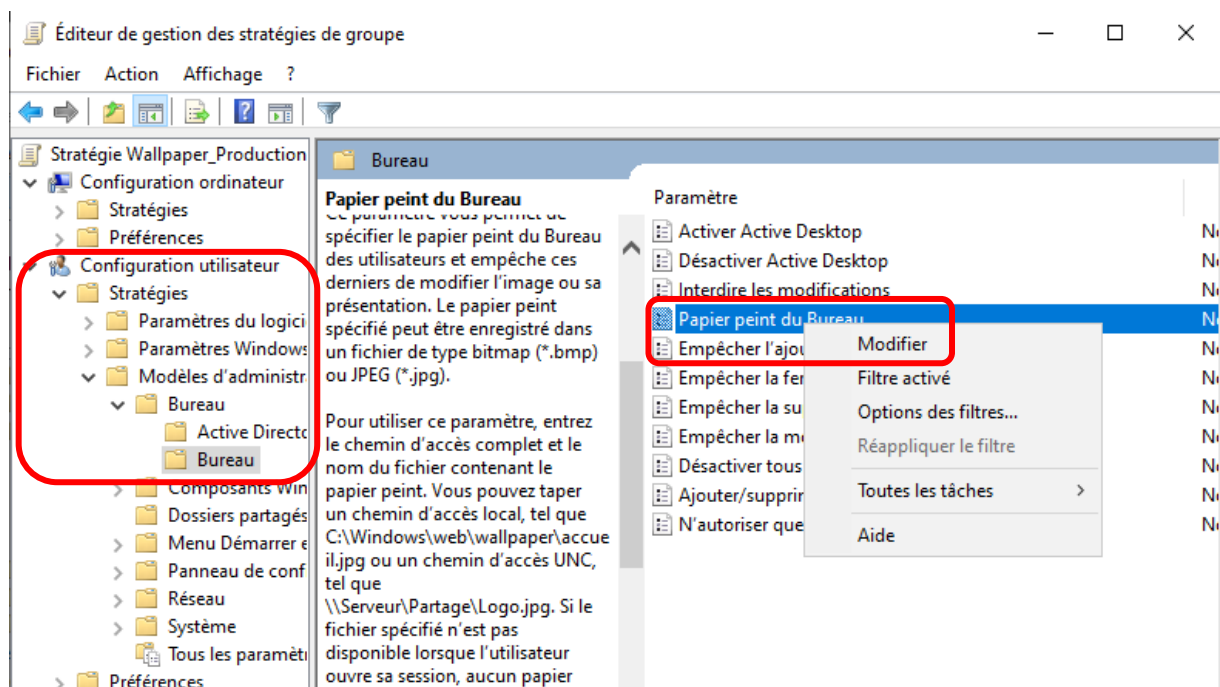
- Ensuite faites un clic droit sur « Informatique » puis « Créer un objet GPO dans ce domaine, et le lier ici... ». Vous pourrez en suite rentrer le nom de votre choix pour le GPO :



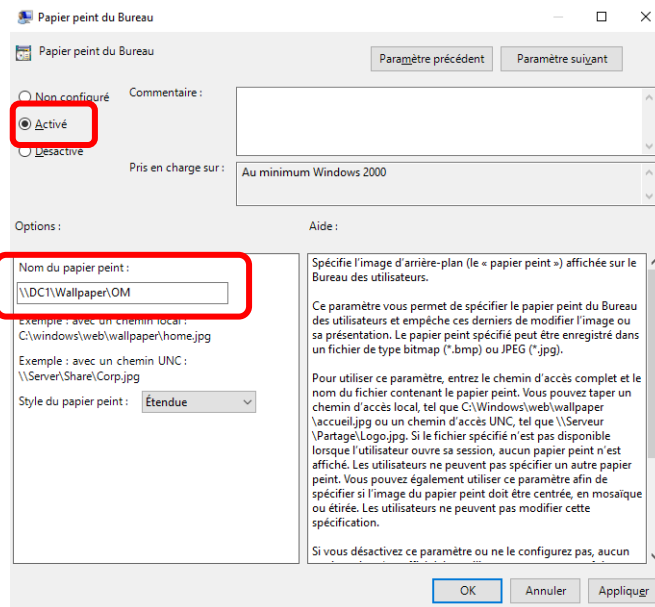
5. Une fois créer, faite modifier :



6. Ensuite, il faut aller dans « Configuration utilisateur », « Stratégie », « Modèles d'administration », « Bureau », « Bureau » puis faire clic droit sur « Papier peint du bureau » et « Modifier » :



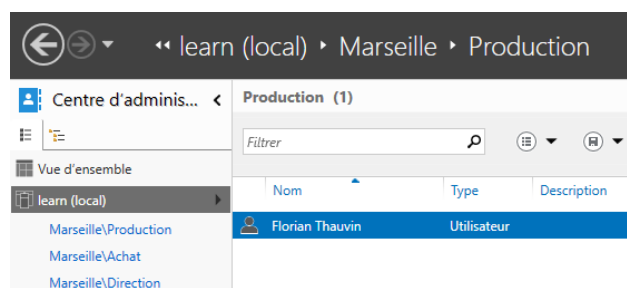
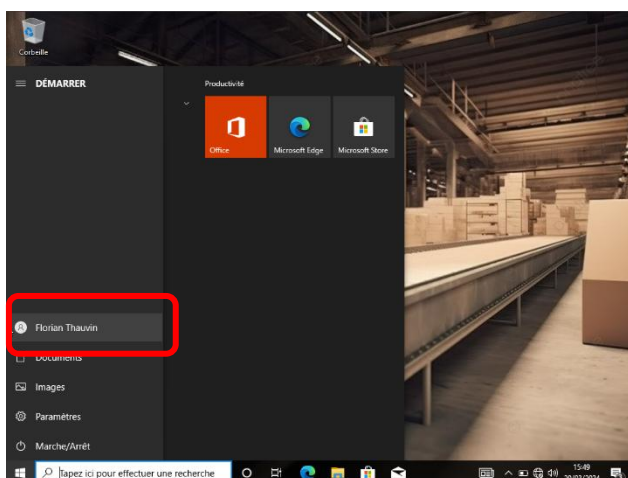
- Une fois sur cette fenêtre, cliquez sur « Activé » puis rentrez le lien vers l'image voulu dans « Nom du papier peint », prenez le lien disponible dans l'onglet partage avancer du dossier suivi de « \NomDeLimage.jpg » (Attention, l'image doit être soit en .JPG soit en .BMP). Pour finir vous pouvez valider et vous rendre sur le client pour vérifier que cela a bien fonctionné :



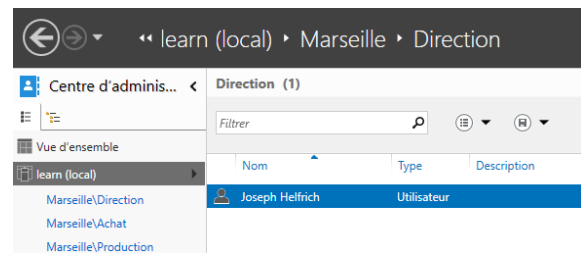
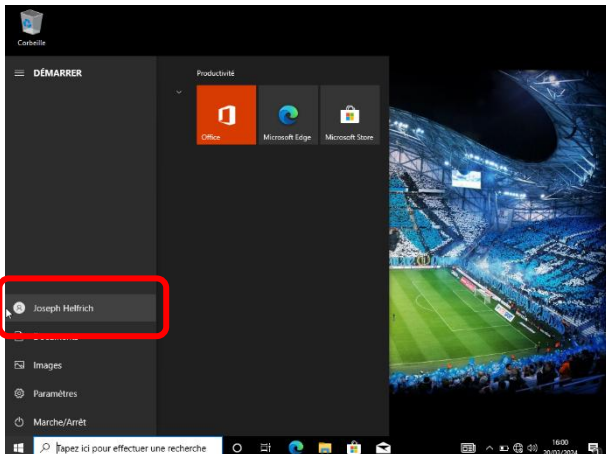
Voici les différents fonds d'écran en fonction de chaque rôle :

- Production :

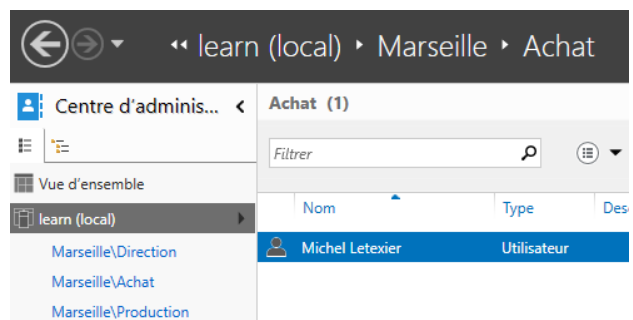
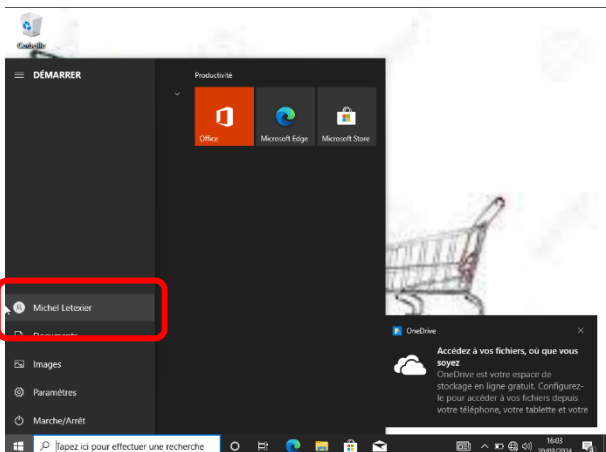
Le fond d'écran de l'utilisateur Florian THAUVIN qui est dans l'UO Production :



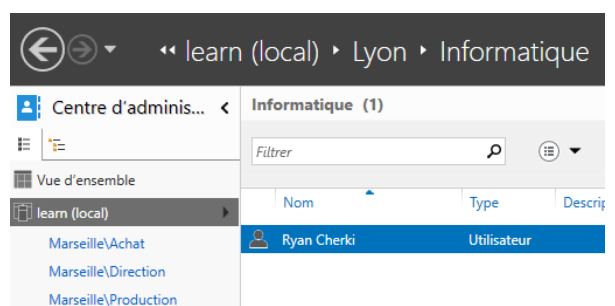
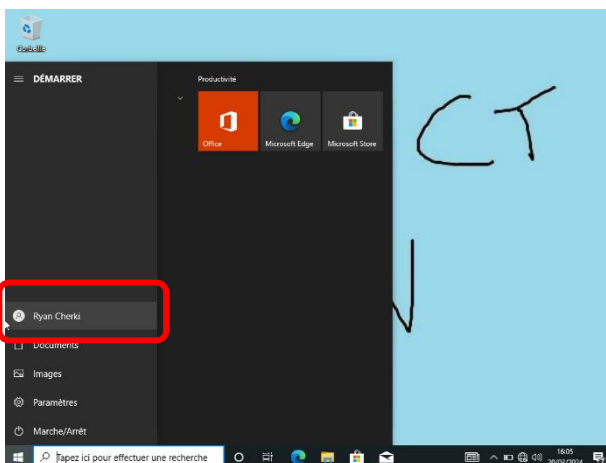
- Direction :



- Achat :



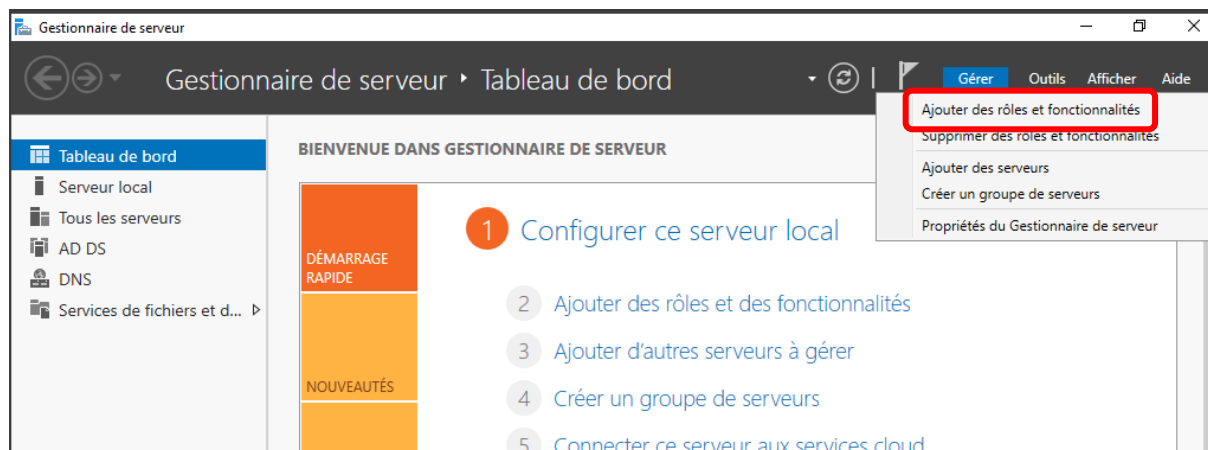
- Informatique :



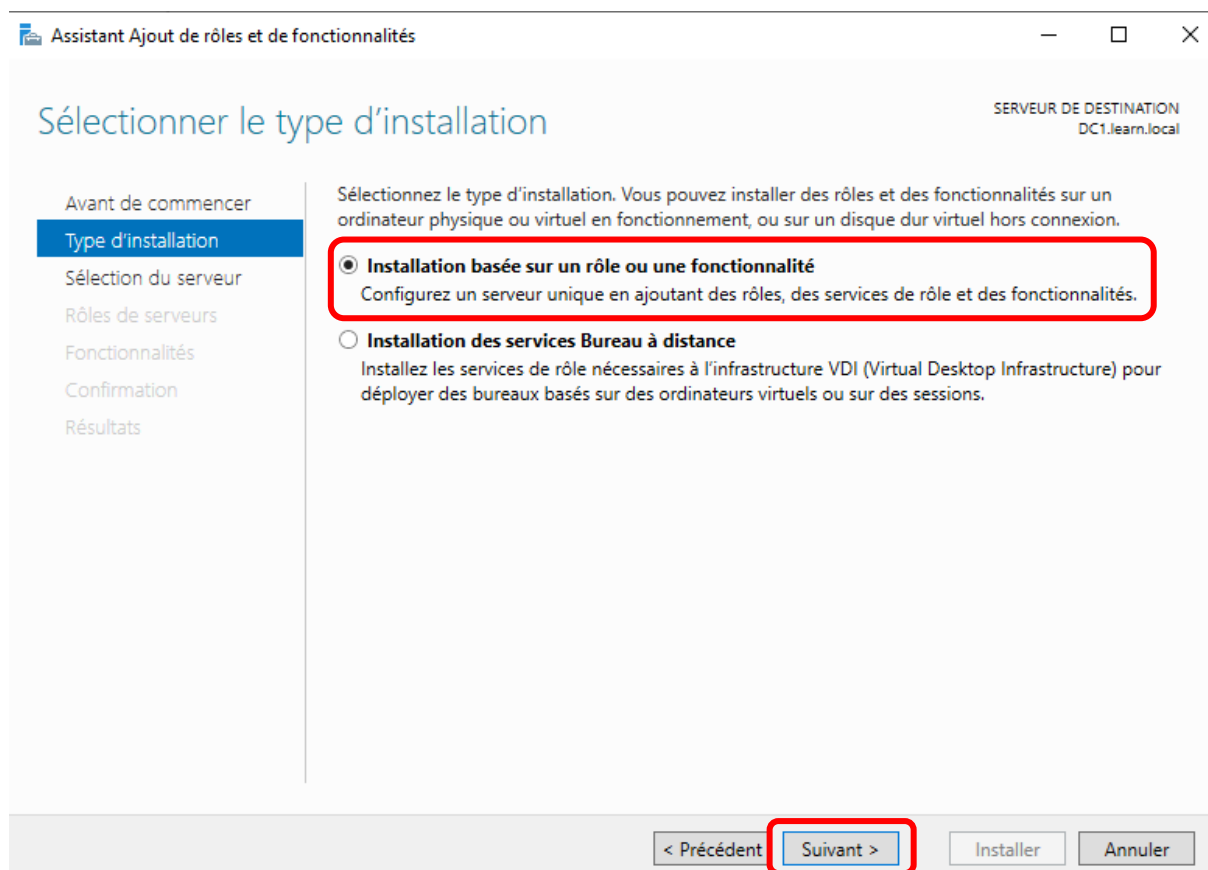
Procédure déduplication

Activer la déduplication :

1. Tout d'abord rendez-vous dans « Ajouter des rôles et fonctionnalités » :



2. Cocher « Installation basée sur un rôle ou une fonctionnalité » puis faite suivant :



3. Choisissez maintenant votre serveur et faite suivent :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
DC1.learn.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
DC1.learn.local	10.1.1.1	Microsoft Windows Server 2022 Standard Evaluation

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

4. Rendez-vous dans « Services de fichiers et de stockage » puis « Services de fichiers et iSCSI » puis cocher « déduplication des données » et faite suivent :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
DC1.learn.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- ☐ Hyper-V
- ☐ Serveur de télécopie
- ☐ Serveur DHCP
- ☒ Serveur DNS (Installé)
- ☐ Serveur Web (IIS)
- ☐ Service Guardian hôte
- ☒ Services AD DS (Installé)
- ☐ Services AD LDS (Active Directory Lightweight Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☐ Services de certificats Active Directory
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (3 sur 12 installés)
 - ☒ Services de fichiers et iSCSI (2 sur 11 installés)
 - ☒ Serveur de fichiers (Installé)
 - ☐ Branchecache pour fichiers réseau
 - ☒ Déduplication des données

Description

La déduplication des données permet d'économiser de l'espace disque en ne stockant qu'une seule copie des données identiques sur le volume.

< Précédent Suivant > Installer Annuler

5. N'installer pas de fonctionnalités faite directement suivant :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des fonctionnalités

SERVEUR DE DESTINATION
DC1.learn.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 sur 7 installé(s))	Les Outils d'administration de serveur distant comprennent des composants logiciels enfichables et des outils en ligne de commande pour la gestion à distance des rôles et des fonctionnalités.
<input checked="" type="checkbox"/> Antivirus Microsoft Defender (Installé)	
<input type="checkbox"/> Assistance à distance	
<input type="checkbox"/> Base de données interne Windows	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Chiffrement de lecteur BitLocker	
<input type="checkbox"/> Client d'impression Internet	
<input type="checkbox"/> Client pour NFS	
<input type="checkbox"/> Client Telnet	
<input type="checkbox"/> Client TFTP	
<input type="checkbox"/> Clustering de basculement	
<input type="checkbox"/> Collection des événements de configuration et de	
<input type="checkbox"/> Compression différentielle à distance	
<input type="checkbox"/> Conteneurs	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Déverrouillage réseau BitLocker	
<input type="checkbox"/> DirectPlay	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Équilibrage de la charge réseau	

< Précédent **Suivant >** Installer Annuler

6. Cocher « Redémarrer automatiquement le serveur de destination » puis « Installer » :

Assistant Ajout de rôles et de fonctionnalités

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
DC1.learn.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☐ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Services de fichiers et de stockage
Services de fichiers et iSCSI
Déduplication des données

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

< Précédent Suivant > **Installer** Annuler

7. Nous allons d'abord analyser le disque. Lancer une invite de commande et taper la commande :
ddpeval (votre lecteur) :

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ddpeval M:
Data Deduplication Savings Evaluation Tool
Copyright (c) 2013 Microsoft Corporation. All Rights Reserved.

Evaluated Target OS: Windows 10.0
Evaluated folder: M:
Evaluated folder size: 705,02 MB
Files in evaluated folder: 8

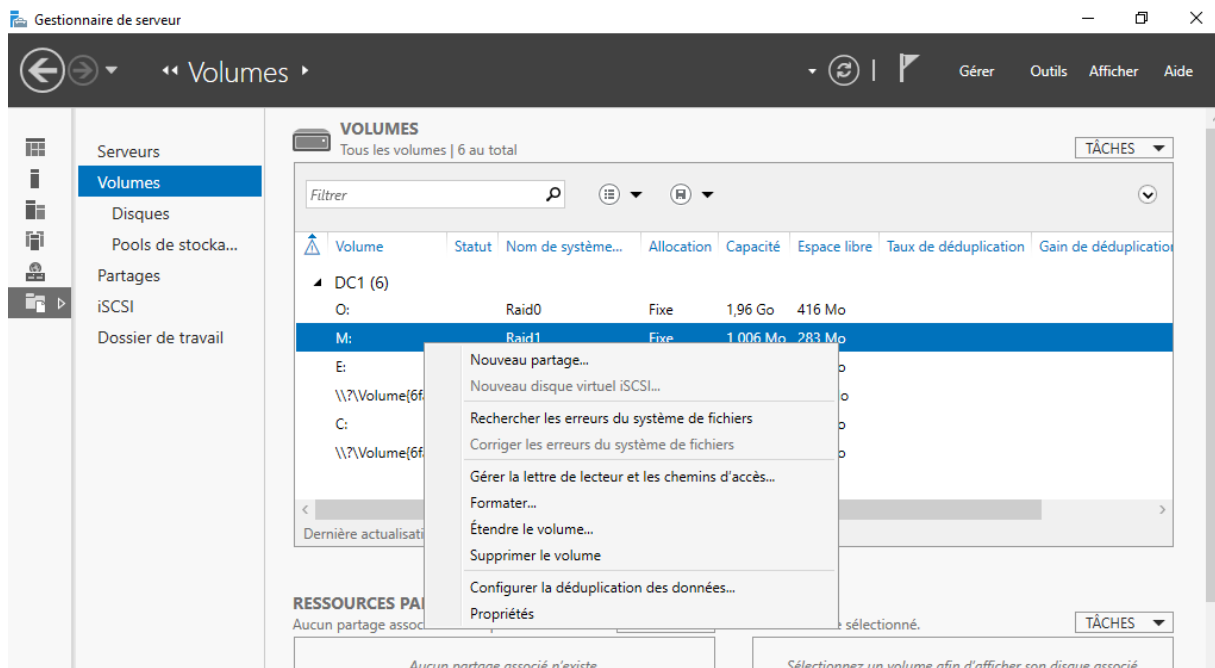
Processed files: 4
Processed files size: 705,02 MB
Optimized files size: 809,53 KB
Space savings: 704,23 MB
Space savings percent: 99

Optimized files size (no compression): 266,13 MB
Space savings (no compression): 438,89 MB
Space savings percent (no compression): 62

Files excluded by policy: 4
    Small files (<32KB): 4
Files excluded by error: 0

C:\Users\Administrateur>
```

8. Maintenant que nous avons analysé le disque, nous allons mettre en place la déduplication du disque.



9. Choisissez « Serveur de fichiers à usage général » et faite « Ok » :

Paramètres de déduplication Raid1 (M:\)

Raid1 (M:\)

Déduplication des données : Serveur de fichiers à usage général

Dédupliquer les fichiers de plus de (en jours) :

Tapez les extensions de fichier que vous souhaitez exclure de la déduplication des données, en séparant les extensions à l'aide d'une virgule. Par exemple : doc,txt,png

Extensions de fichier par défaut à exclure : edb,jrs

Extensions de fichier personnalisées à exclure :

Pour exclure les dossiers sélectionnés (et leur contenu) de la déduplication des données, cliquez sur Ajouter...

Ajouter... Supprimer

Définir la planification de la déduplication...

OK Annuler Appliquer

10. Taper maintenant dans le PowerShell la commande suivante :

Start-DedupJob m : -type Optimization

```
PS C:\Users\Administrateur> Start-DedupJob m: -type Optimization
```

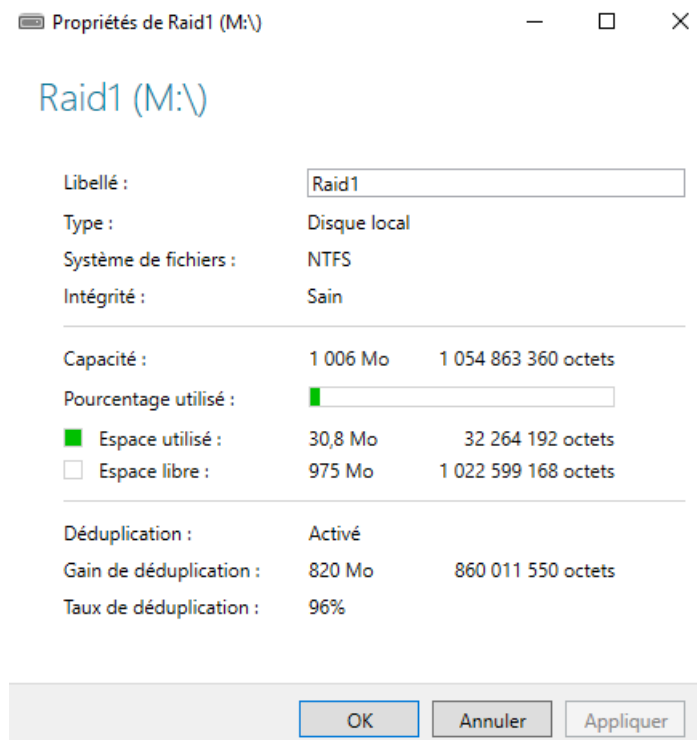
Type	ScheduleType	StartTime	Progress	State	Volume
Optimization	Manual		0 %	Queued	m:

11. Nous avons bien le disque m : de fini :

```
PS C:\Users\Administrateur> Get-DedupJob
```

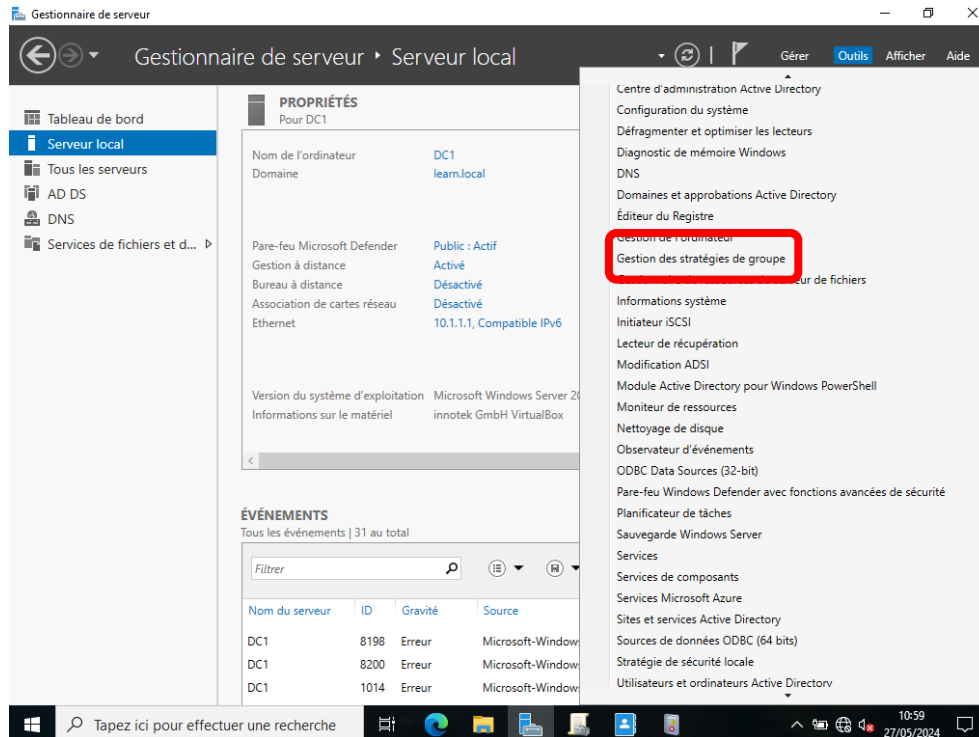
Type	ScheduleType	StartTime	Progress	State	Volume
Optimization	Manual		0 %	Queued	M:
Optimization	Manual		0 %	Queued	M:
Optimization	Manual		0 %	Queued	O:
Optimization	Manual		0 %	Queued	o:
Optimization	Manual	17:10	100 %	Completed	■:

12. Nous pouvons voir que cela a fonctionné :

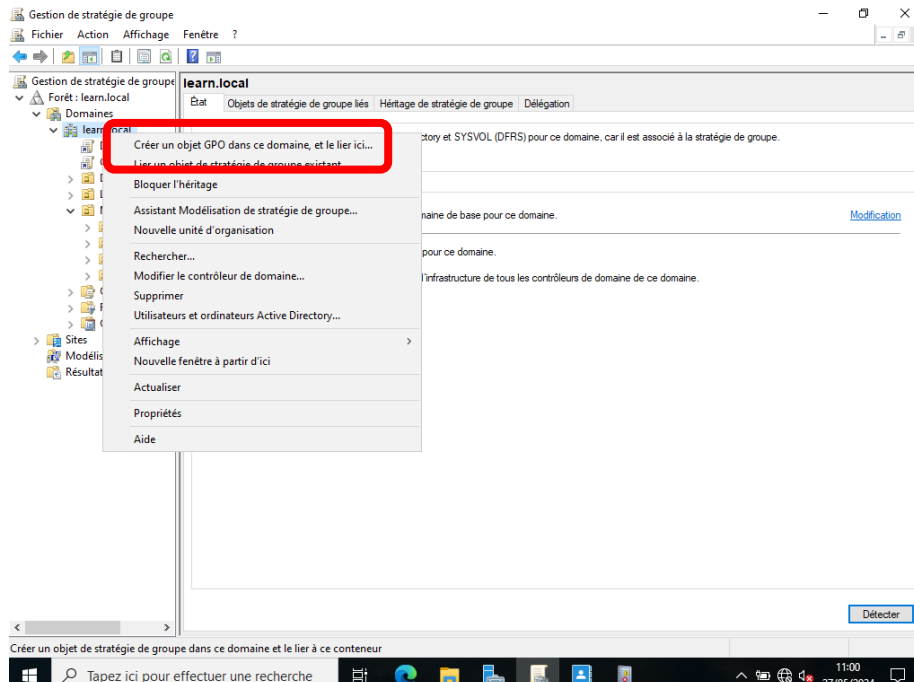


Procédure audit utilisateurs

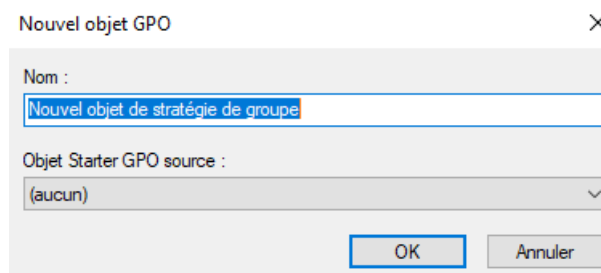
1. Tout d'abord rendez-vous « Gestionnaire des stratégies de groupe » :



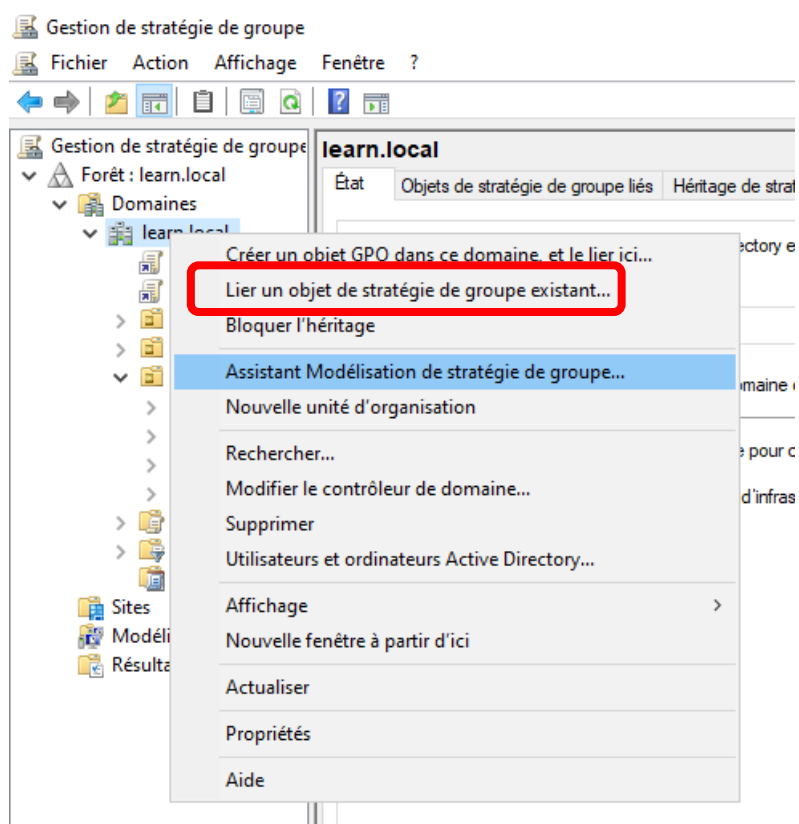
2. Ensuite, allez dans « Domaines » puis faite un clic droit sur « learn.local » et faite « Créer un objet GPO dans ce domaine, et le lier ici... » :



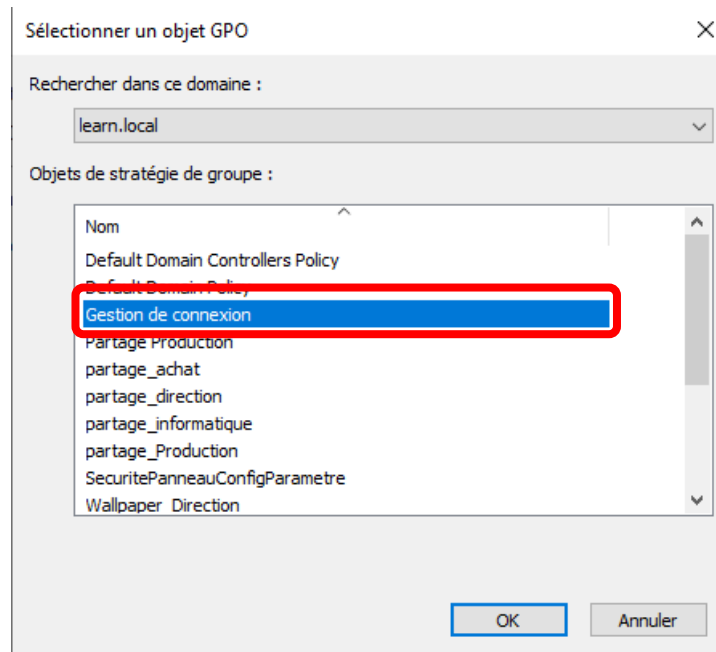
3. Choisissez le nom que vous voulez et valider :



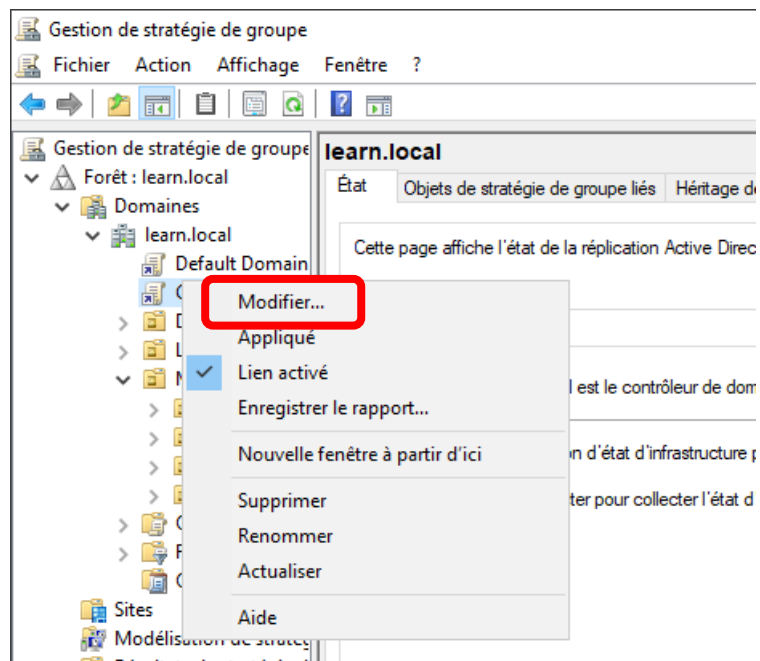
4. En suite refaite un clic droit sur « learn.local » et faite « Lier un objet de stratégie de groupe existant » :



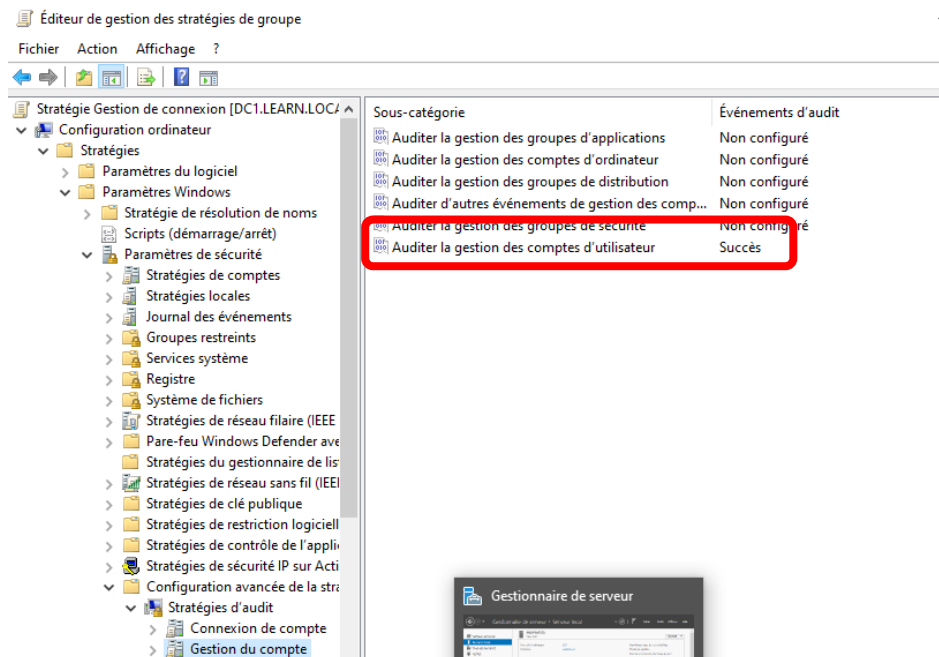
5. Choisissez la stratégie que nous venons de créer, nous faisons ça pour vérifier que la stratégie est bien liée :



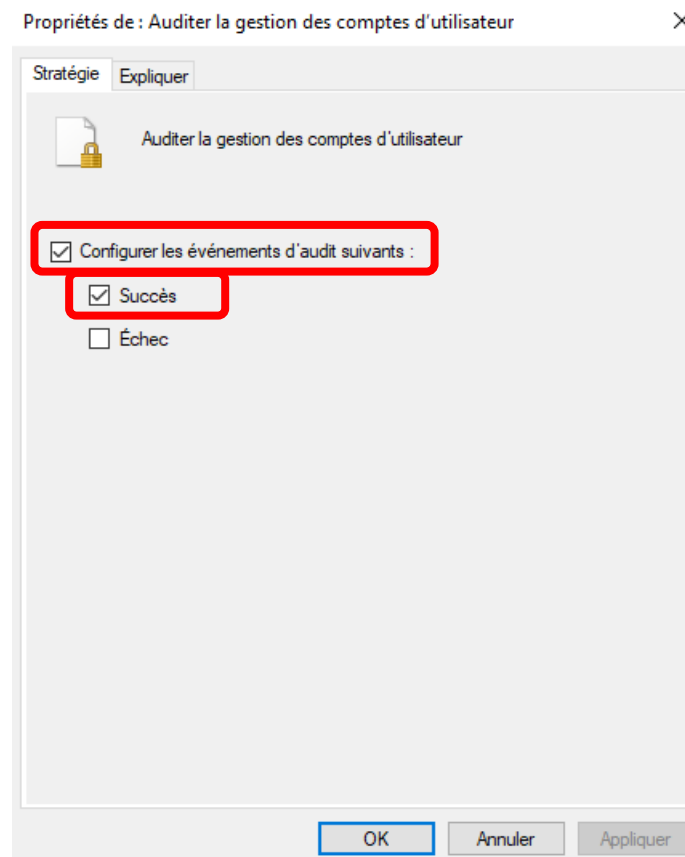
6. En suite faite clique droit sur la stratégie que nous venons de créer, et faite modifier :



7. Maintenant rendez-vous dans « Configuration ordinateur » puis « Paramètres Windows » puis « Paramètres de sécurité » puis « Configuration avancé de la stratégie d'audit » puis « Stratégies d'audit » puis « gestion de compte ». Maintenant faites un clic droit sur « Auditer la gestion des comptes d'utilisateurs ».



8. Maintenant cocher « Configurer les événements d'audit suivants » et en suite « Succès »



9. Ensuite nous créons un compte pour voir si cela apparait dans l'observateur d'événements :

The screenshot shows the 'Compte' (Account) window for 'Jose Garcia'. The 'Compte' tab is active, showing fields for 'Prénom' (Jose), 'Nom' (Garcia), and 'Nom complet' (Jose Garcia). The 'Date d'expiration du con' (Expiration date of the account) is set to 'Jamais' (Never). The 'Options de mot de passe' (Password options) section is expanded, showing 'Autres options de mot de passe' (Other password options) with 'Une carte à puce ou Microsoft Passport est requis pour ouvrir...' (A smart card or Microsoft Passport is required to sign in) checked. The 'Options de chiffrement' (Encryption options) section is also expanded. The 'Organisation' tab is visible below, showing fields for 'Nom complet', 'Bureau', 'Adresse de messagerie', 'Page Web', 'Fonction', 'Service', 'Société', 'Responsable', 'Collaborateurs', 'Adresse', 'Ville', 'Département/Provin...', and 'Code postal'. The 'Informations supplémentaires' (Additional information) link is at the bottom left. The 'OK' and 'Annuler' (Cancel) buttons are at the bottom right.

10. Nous voyons bien un évènement, le 4720 qui nous dis qu'un utilisateur a été créé :

The screenshot shows the 'Observateur d'événements' (Event Viewer) window. The 'Sécurité' (Security) log is selected, showing a list of events. The event 'Succès de l'a...' (Success of the a...) with ID 4720 is highlighted. The details pane shows the event description: 'Un compte d'utilisateur a été créé.' (A user account was created). The details pane also shows the 'Sujet' (Subject) section with the following information:

Propriété	Valeur
ID de sécurité :	LEARN\Administrateur
Nom du compte :	Administrateur
Domaine du compte :	LEARN
ID d'ouverture de session :	0x3AE2A
Nouveau compte :	
ID de sécurité :	LEARN\gjose

The details pane also shows the 'Journal' (Log) section with the following information:

Propriété	Valeur
Journal :	Sécurité
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

The details pane also shows the 'Général' (General) section with the following information:

Propriété	Valeur
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

The details pane also shows the 'Détails' (Details) section with the following information:

Propriété	Valeur
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

The details pane also shows the 'Actions' (Actions) section with the following information:

Propriété	Valeur
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

The details pane also shows the 'Général' (General) section with the following information:

Propriété	Valeur
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

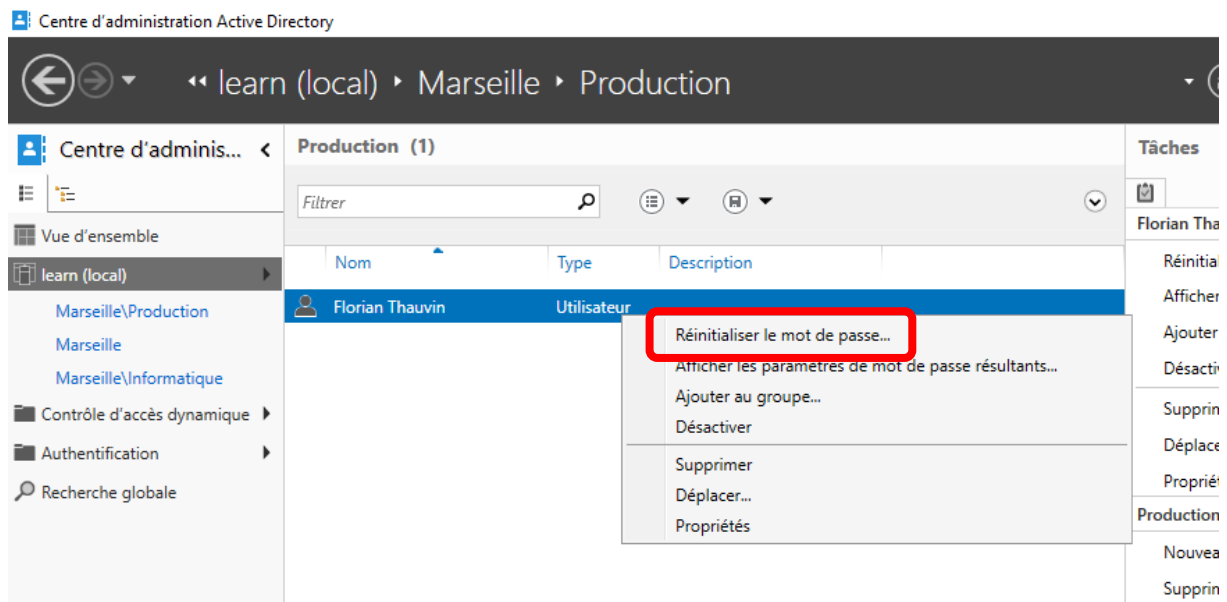
The details pane also shows the 'Détails' (Details) section with the following information:

Propriété	Valeur
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

The details pane also shows the 'Actions' (Actions) section with the following information:

Propriété	Valeur
Source :	Microsoft Windows security
Événement :	4720
Niveau :	Information
Utilisateur :	N/A
Opcode :	Informations
Informations :	Aide sur le Journal

1. Maintenant nous allons modifier le mot de passe d'un utilisateur pour voir si un événement s'affiche. Pour commencer, rendez-vous sur un utilisateur depuis le « Centre d'administration Active Directory », et faite un clic droit sur l'utilisateur, puis « Réinitialiser le mot de passe... » :



2. Maintenant changez le mot de passe :

The screenshot shows the « Réinitialiser le mot de passe » dialog box. It contains two text input fields for « Mot de passe : » and « Confirmation : ». Below these fields are two checkboxes: « ☒ Changer le mot de passe à la prochaine session » and « ☐ Déverrouiller le compte ». At the bottom of the dialog are two buttons: « OK » and « Annuler ».

3. Nous pouvons maintenant aller voir dans l'observateur d'événements :

Nous avons l'évènement 4724 qui nous dit qu'il y a eu une tentative de réinitialisation de mot de passe, suivi du 4738 qui nous dit qu'un utilisateur a été modifié :

The screenshot shows the Windows Event Viewer application. The left pane displays the tree structure with 'Sécurité' (Security) selected under 'Journaux Windows' (Windows Logs). The main pane shows a list of security events. Event 4724, 'Succès de l'audit de la stratégie de mot de passe' (Audit success of password policy), is highlighted with a red rectangle. The details pane for event 4724 is open, showing the message: 'Une tentative de réinitialisation de mot de passe d'un compte a été effectuée.' (A password reset attempt for an account was made). The subject information indicates the user is LEARN\Administrateur and the target is LEARN\lflorian.

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la source
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:58	Microsoft Windows security auditing	5379	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:58	Microsoft Windows security auditing	5379	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:58	Microsoft Windows security auditing	5379	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:57	Microsoft Windows security auditing	4724	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:57	Microsoft Windows security auditing	4724	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:46	Microsoft Windows security auditing	5379	User Account Management

Événement 4724, Microsoft Windows security auditing.

Général Détails

Une tentative de réinitialisation de mot de passe d'un compte a été effectuée.

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x3A8CC

Compte cible :

- ID de sécurité : LEARN\lflorian

Journal : Sécurité

Source : Microsoft Windows security

Connecté : 27/05/2024 11:39:57

Événement : 4724

Catégorie : User Account Management

Niveau : Information

Mots-clés : Succès de l'audit

Utilisateur : N/A

Ordinateur : DC1.learn.local

Opcode : Informations

Informations : [Aide sur le Journal](#)

The screenshot shows the Windows Event Viewer application. The left pane displays the tree structure with 'Sécurité' (Security) selected under 'Journaux Windows' (Windows Logs). The main pane shows a list of security events. Event 4738, 'Succès de l'audit de la stratégie de mot de passe' (Audit success of password policy), is highlighted with a red rectangle. The details pane for event 4738 is open, showing the message: 'Un compte d'utilisateur a été modifié.' (A user account was modified). The subject information indicates the user is LEARN\Administrateur and the target is LEARN\lflorian.

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la source
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:58	Microsoft Windows security auditing	5379	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:58	Microsoft Windows security auditing	5379	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:58	Microsoft Windows security auditing	5379	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:57	Microsoft Windows security auditing	4738	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:57	Microsoft Windows security auditing	4738	User Account Management
Succès de l'audit de la stratégie de mot de passe	27/05/2024 11:39:46	Microsoft Windows security auditing	5379	User Account Management

Événement 4738, Microsoft Windows security auditing.

Général Détails

Un compte d'utilisateur a été modifié.

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x3A8CC

Compte cible :

- ID de sécurité : LEARN\lflorian

Journal : Sécurité

Source : Microsoft Windows security

Connecté : 27/05/2024 11:39:57

Événement : 4738

Catégorie : User Account Management

Niveau : Information

Mots-clés : Succès de l'audit

Utilisateur : N/A

Ordinateur : DC1.learn.local

Opcode : Informations

Informations : [Aide sur le Journal](#)