WINDOWS SERVER

AUDITS AD

Margaux TANET

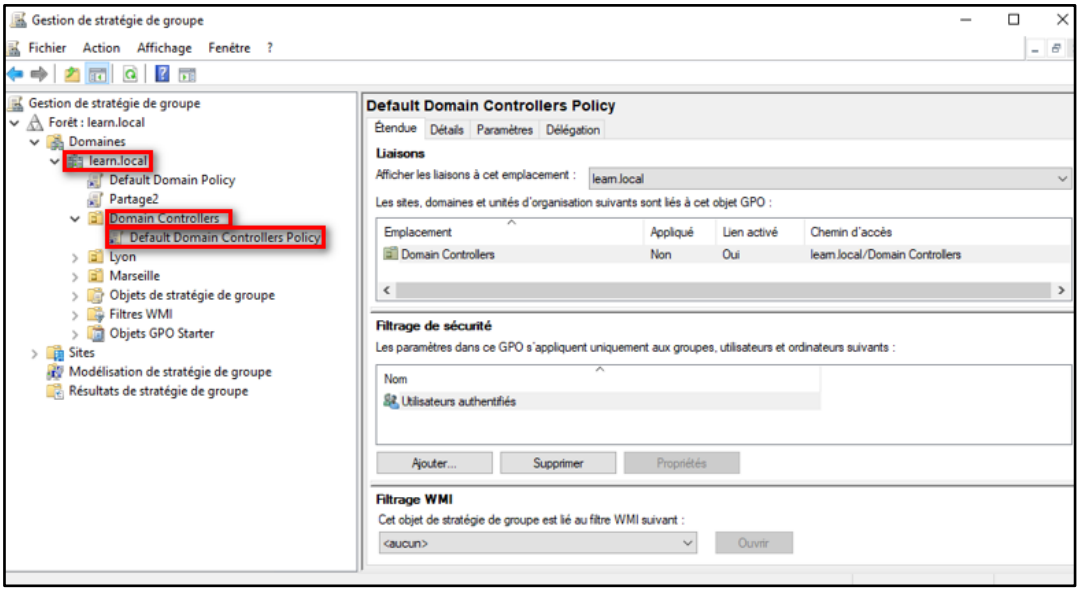
CPI

2024-2025

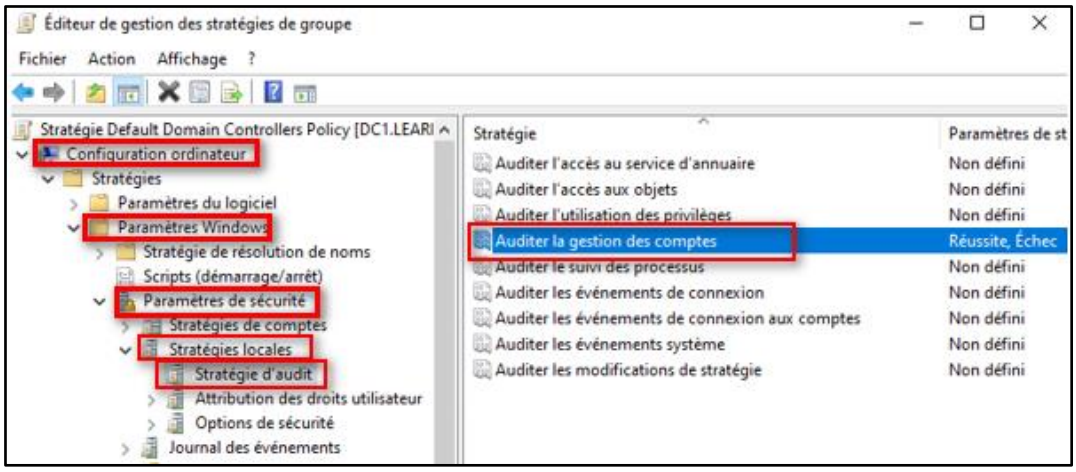
Introduction : Dans ce document, nous allons mettre en place un audit via une GPO pour la gestion de comptes d'AD. Des tests seront réalisés via le journal d'évènement.

I- Création d'une GPO pour activer l'audit

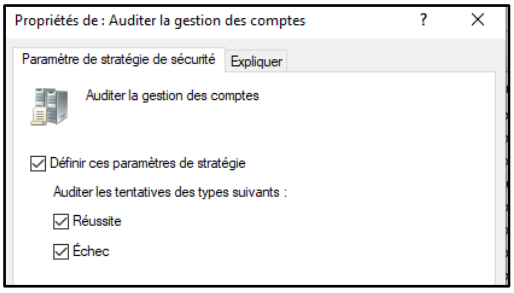
- Se rendre dans **Gestion de stratégie de groupe** > **créer une GPO sur le contrôleur de domaine** > clic droit **Modifier** :



- Dans **l'éditeur de gestion des stratégies de groupe > Configuration ordinateur > Paramètres Windows > Paramètre sécurité > Stratégies locales> Stratégie d'audit> Auditer la gestion des comptes :**



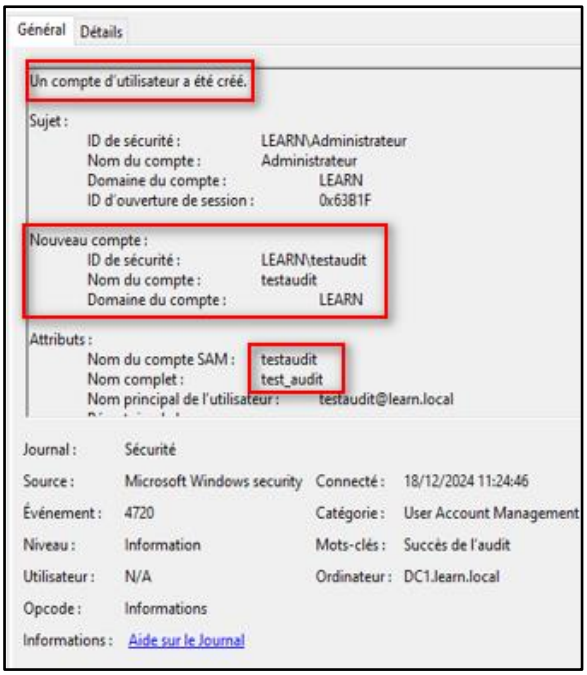
- Dans les **paramètres de stratégie de sécurité**, cocher **Définir ces paramètres de stratégie** et cocher **Réussite et Echec :**



II- Test : journal d'évènement

- Créer un utilisateur dans l'AD. Lors de cette création, grâce à la stratégie mise en place, il est possible de voir la création dans l'observateur d'évènement.

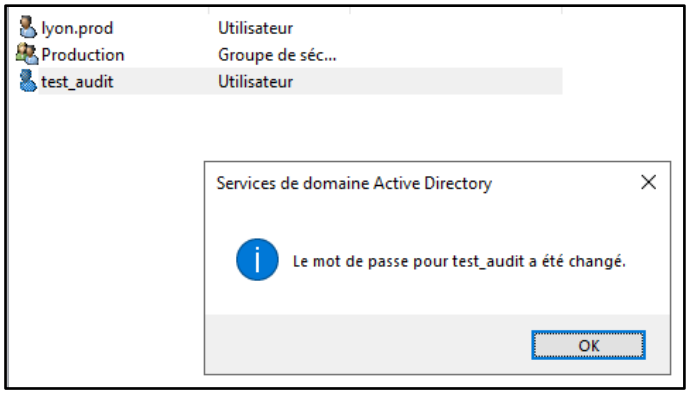
Se rendre dans l'observateur d'évènement et rechercher un évènement 4720 le plus souvent.



III- Audit de modification de mot de passe

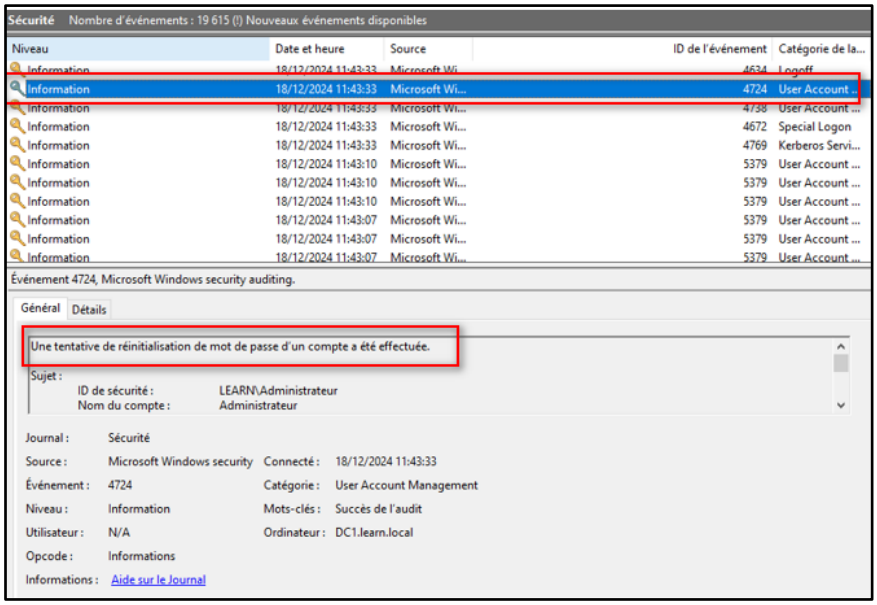
Il n'est pas nécessaire de créer une nouvelle GPO puisque dans la configuration de la GPO précédente, l'option de modification de mot de passe est comprise dans l'audit de gestion de compte utilisateur.

- Changer le mot de passe de l'utilisateur :



IV- Test : journal d'évènement

Dans le journal d'évènement, dans le **journal Windows** > **sécurité**, l'évènement 4724 indique qu'une tentative de réinitialisation de mot de passe a été faite :



Conclusion : Nous avons mis en place un audit activé via GPO qui a permis d'avoir des informations dans le journal d'événement, lors de la création d'un utilisateur ou d'un changement de mot de passe.