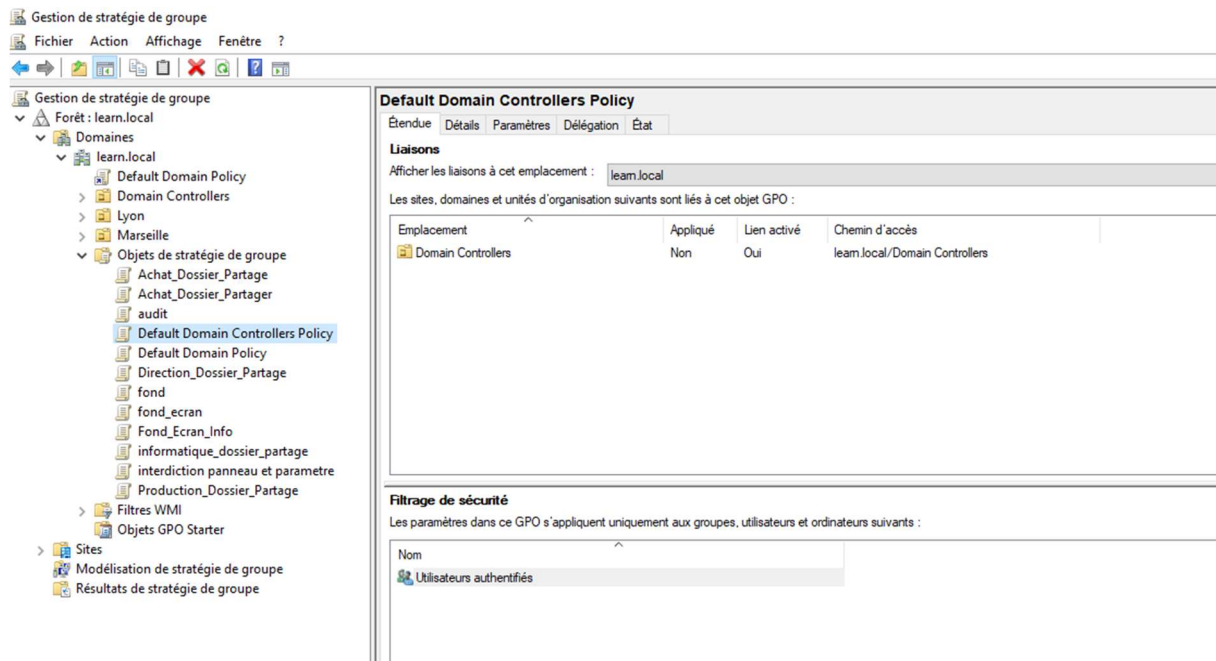


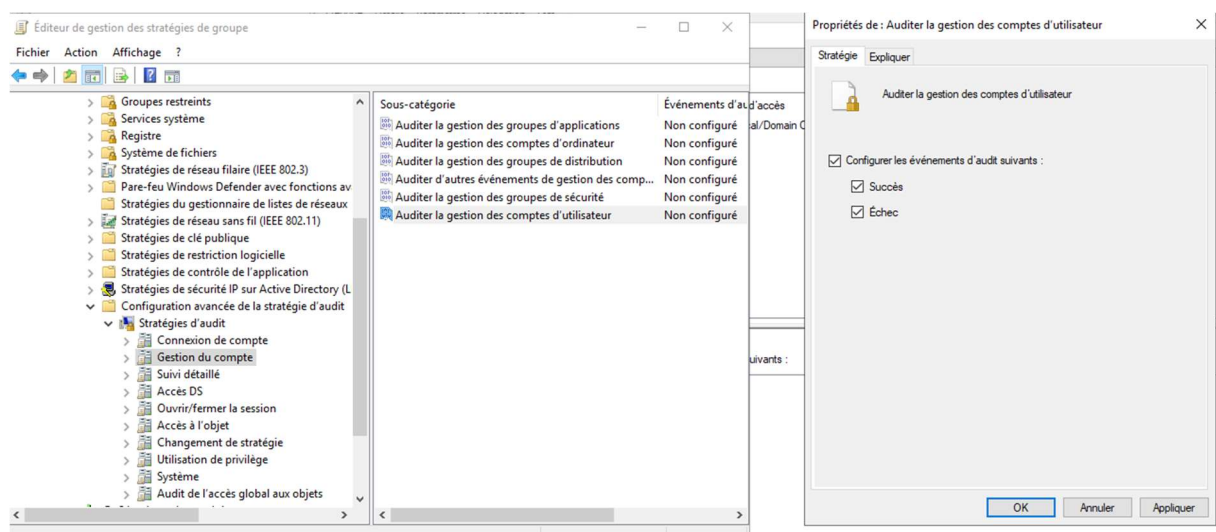
Procédure : Créer un audit pour la gestion de compte utilisateur AD sur le DC

Étape 1 :

Modifier la GPO, Default Domain Controller Policy.



Étape 2 : Dérouler jusqu'à Stratégies d'audit puis activer l'audit de la gestion des comptes d'utilisateurs.



Étape 3 :

Je vérifie en créant un utilisateur dans l'AD, un log remonte bien.

The screenshot shows the Windows Event Viewer application. The left pane displays the tree structure with 'Sécurité' selected under 'Journaux Windows'. The right pane shows a list of security events, with event 4720 highlighted. Below the list, the details of event 4720 are displayed, indicating that a user account was created.

Événement 4720, Microsoft Windows security auditing.

Général Détails

Un compte d'utilisateur a été créé.

Sujet :

- ID de sécurité : LEARN\admin.lucas
- Nom du compte : admin.lucas
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x8DDBA

Nouveau compte :

- ID de sécurité : LEARN\eezq
- Nom du compte : eezq
- Domaine du compte : LEARN

Attributs :

- Nom du compte SAM : eezq
- Nom complet : test audit
- Nom principal de l'utilisateur : eezqa@learn.local

Journal : Sécurité

Source : Microsoft Windows security **Connecté :** 16/05/2024 16:41:20

Événement : 4720 **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](#)

Étape 4 : Vérifier pour la réinitialisation d'un mot de passe d'un compte utilisateur via l'ad

The screenshot shows the Windows Event Viewer application. The left pane displays the tree structure with 'Sécurité' selected under 'Journaux Windows'. The right pane shows a list of security events, with event 4724 highlighted. Below the list, the details of event 4724 are displayed, indicating that a password reset attempt was successful.

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\admin.lucas
- Nom du compte : admin.lucas
- Domaine du compte : LEARN
- ID d'ouverture de session : 0xC284EC

Compte cible :

- ID de sécurité : LEARN\production.lyon
- Nom du compte : production.lyon
- Domaine du compte : LEARN

Journal : Sécurité

Source : Microsoft Windows security **Connecté :** 16/05/2024 17:00:57

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](#)