Audit d’un fichier d’accès

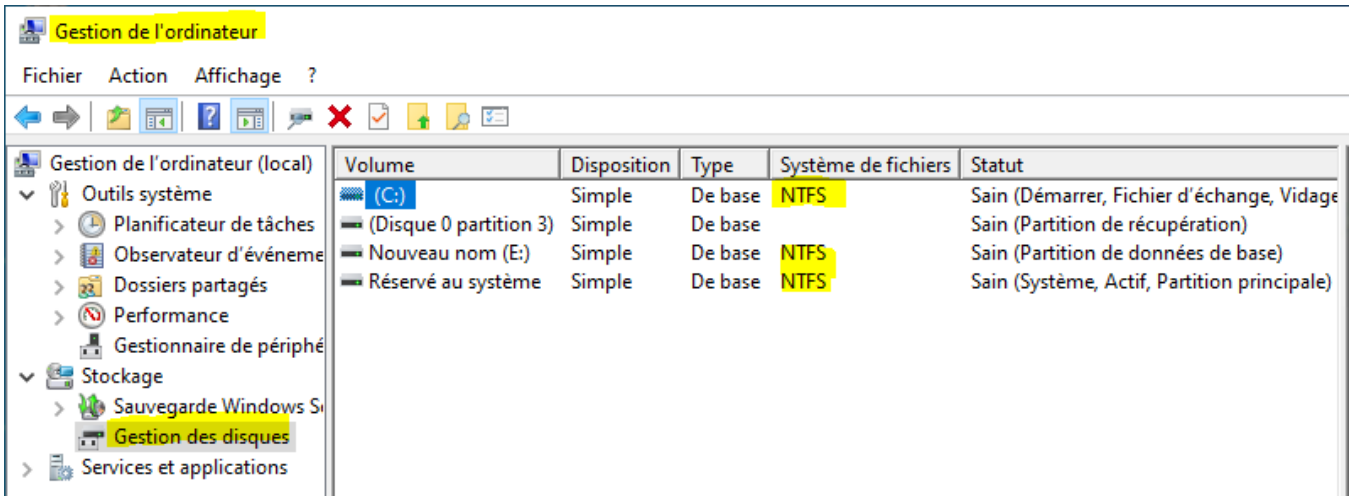
Introduction

Les audits permettent de surveiller les activités d'un dossier, cela permet de renforcer de savoir exactement par qui et quand a été supprimé modifier le document.

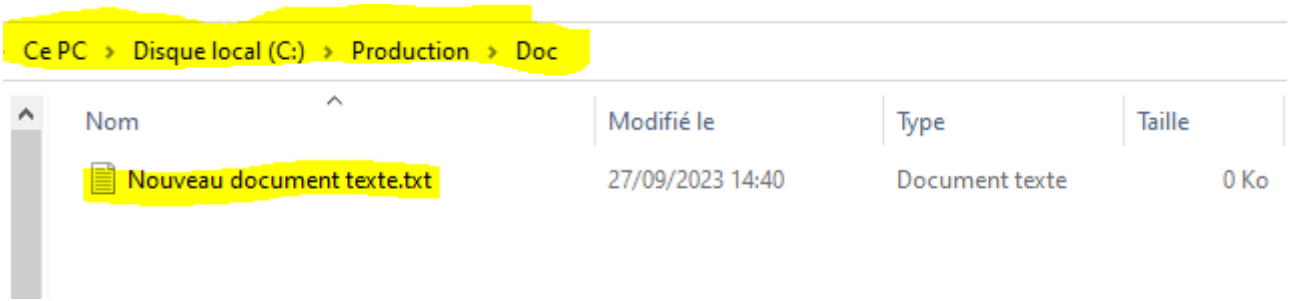
Configuration d'audit d'un fichier d'accès

On vérifie d'abord si nos disques sont au format NTFS.

➔ Gestion de l'ordinateur → gestion des disques

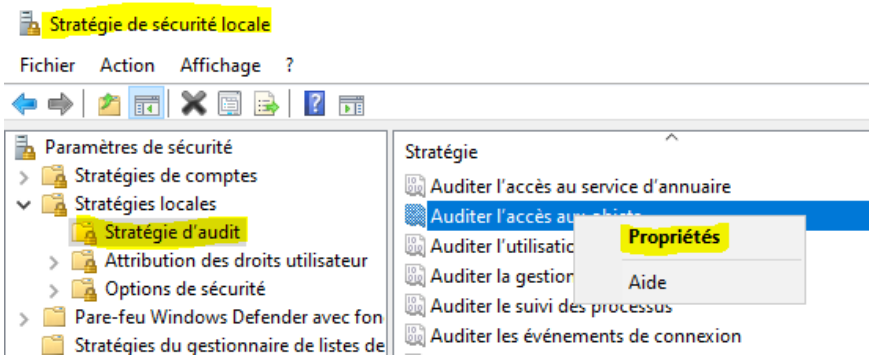


On crée ensuite notre document dans le sous dossier (Doc) du dossier Production

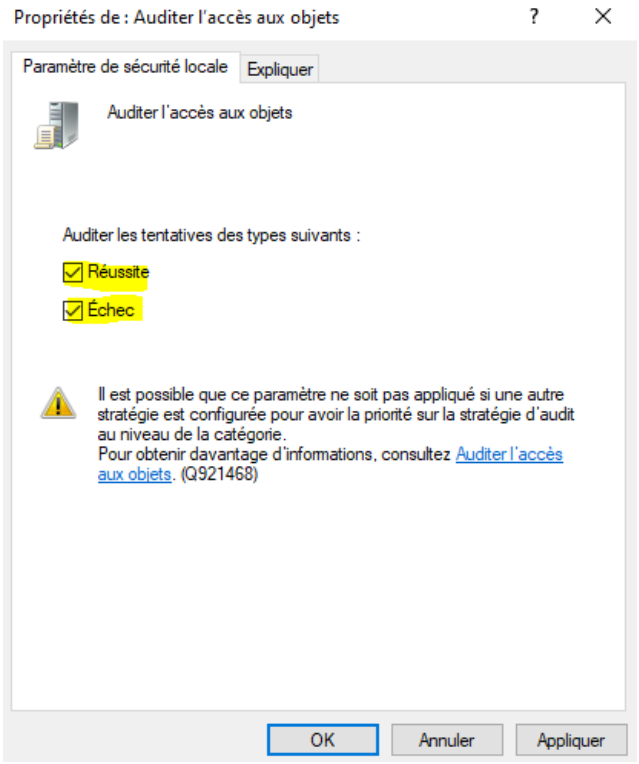


On autorise les audits sur notre serveur.

➔ Stratégie de sécurité locale → Stratégie locale → Stratégie d'audit → Audit l'accès aux objets → Propriétés

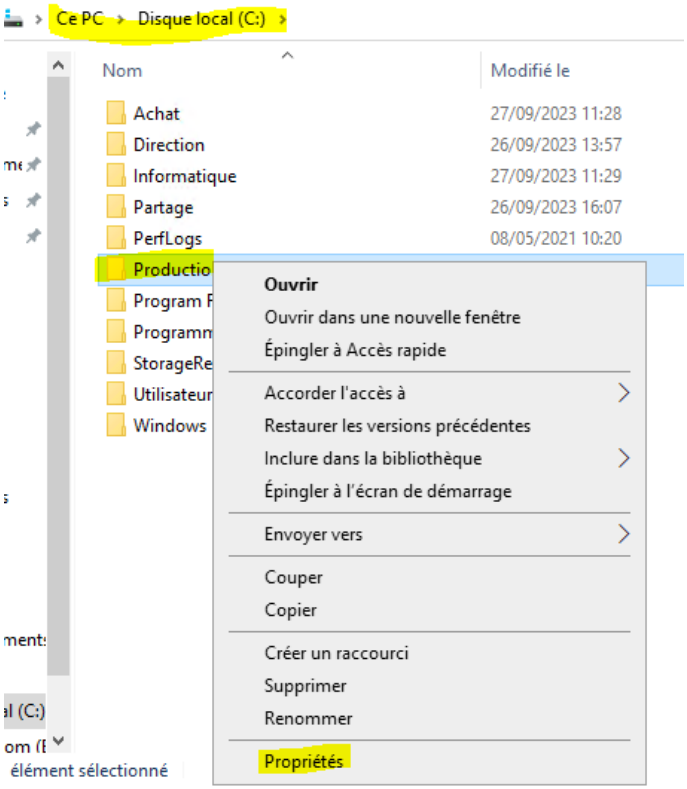


Activer l'audite sur les tentatives en Réussite et en Echec.

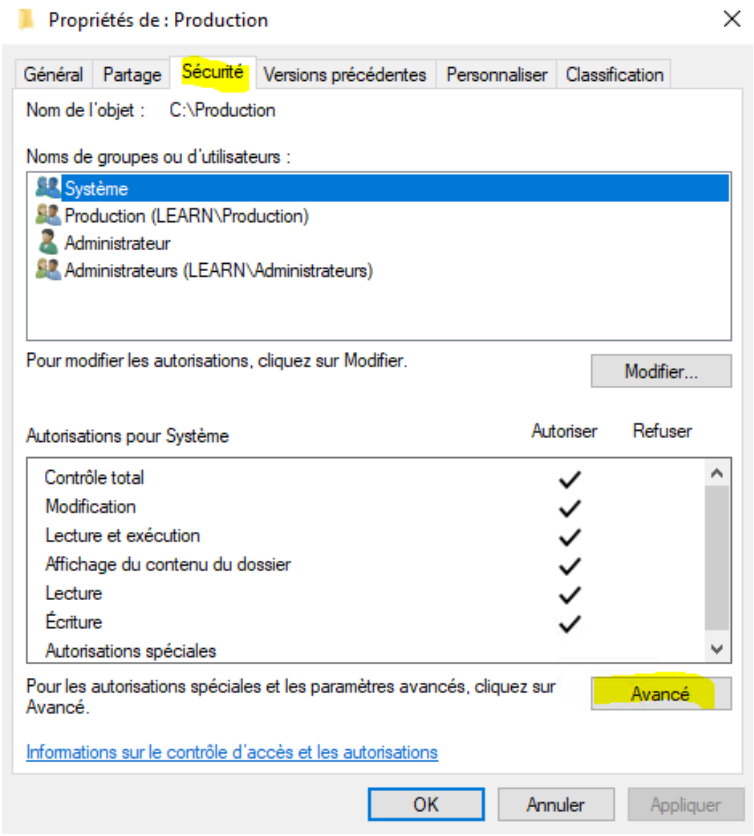


On autorise l'Audit créer sur le dossier Production.

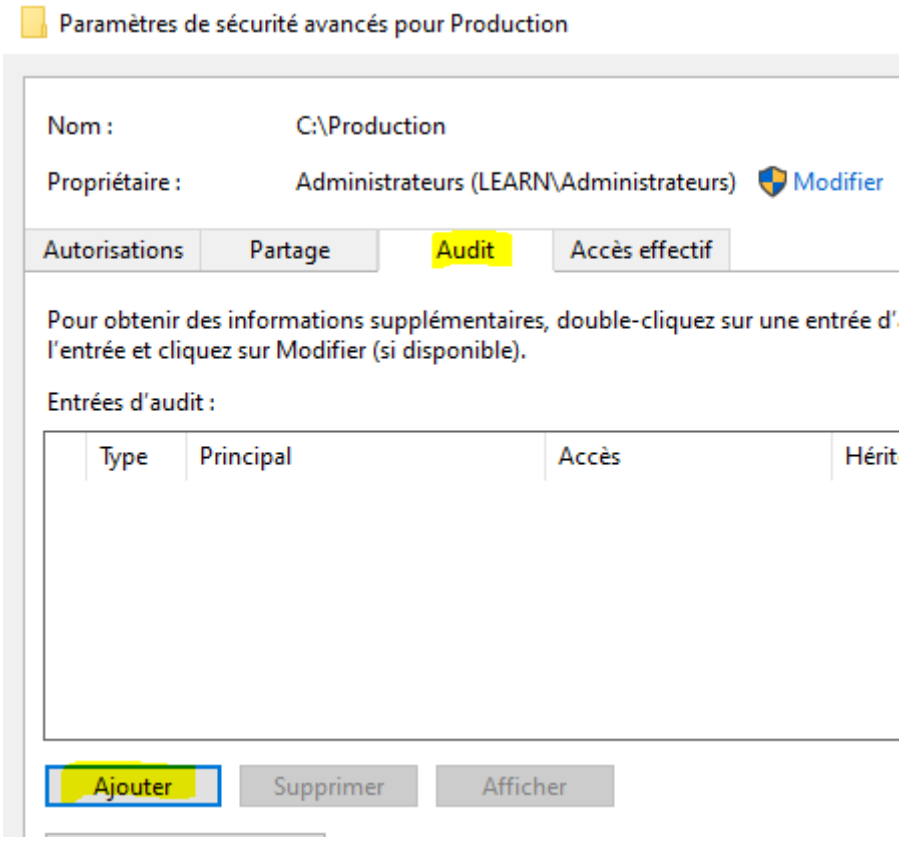
➔ Clic droit sur le dossier Production → Propriétés



➔ Sécurité → Avancé

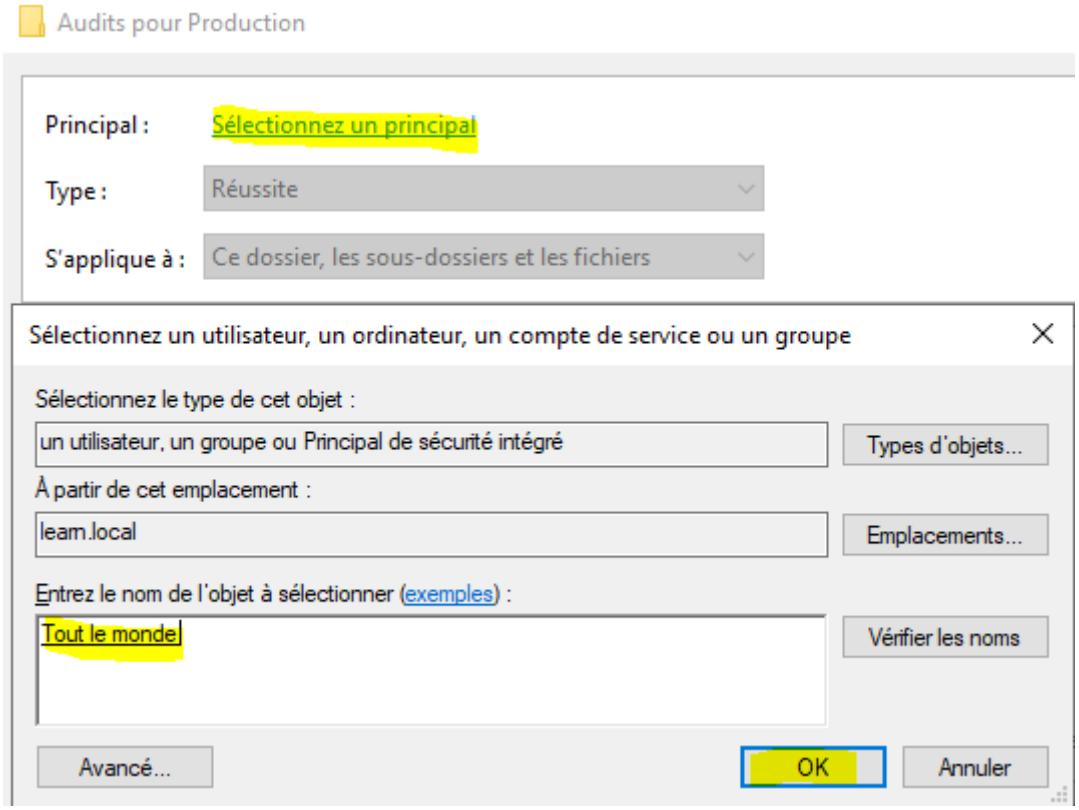


➔ Audit → Ajouter

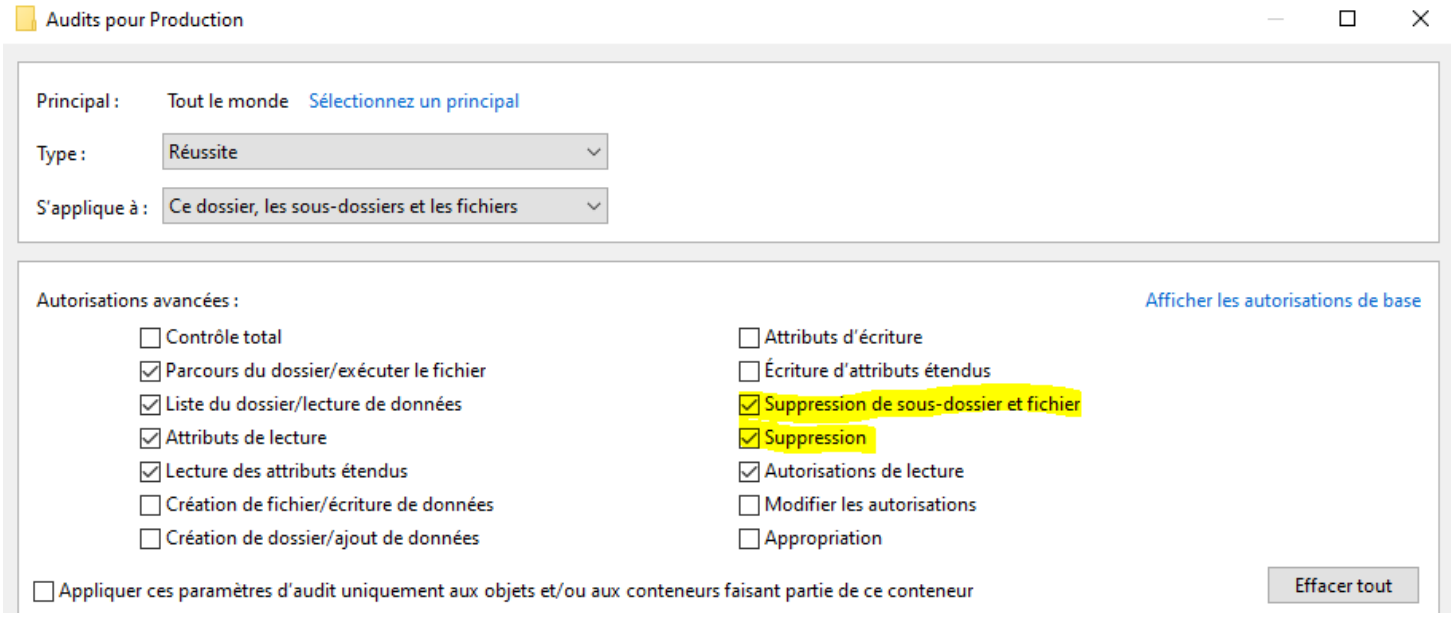


On ajoute tout le monde dans l'Audit.

➔ Sélectionnez un principal → Entrez le nom de l'objet à sélectionner → Tout le monde → Ok



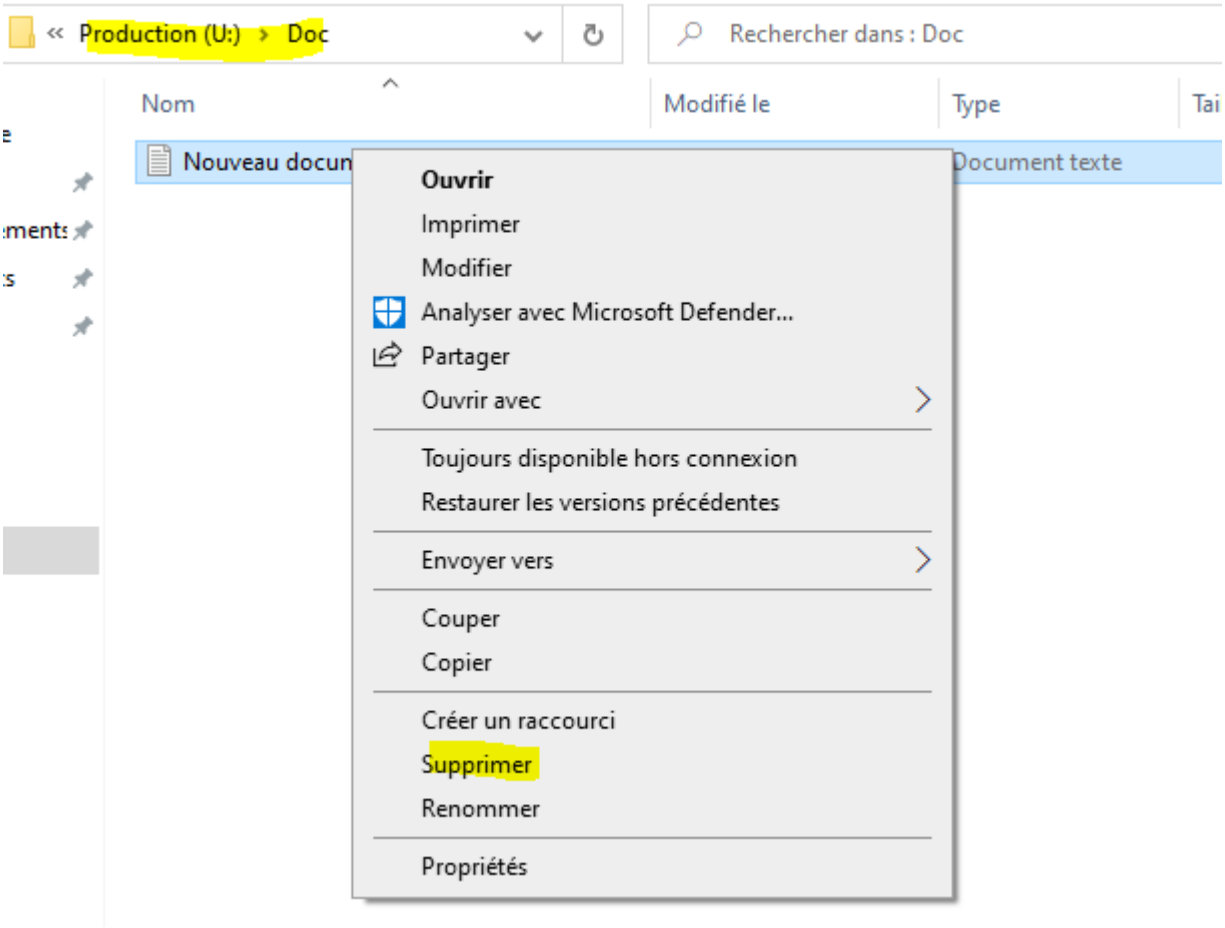
➔ Afficher les autorisations avancées →Cocher suppression de sous-dossier et fichier → Cocher suppression



Test de l'Audit

On se connecte avec un utilisateur qui est dans le groupe Production et on test l'Audit.

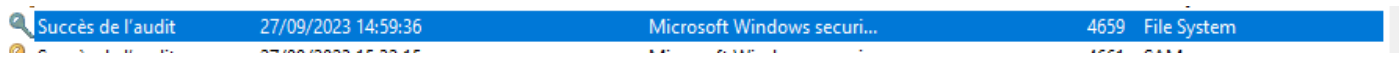
➔ Ouvrir le dossier Production → On supprime le dossier



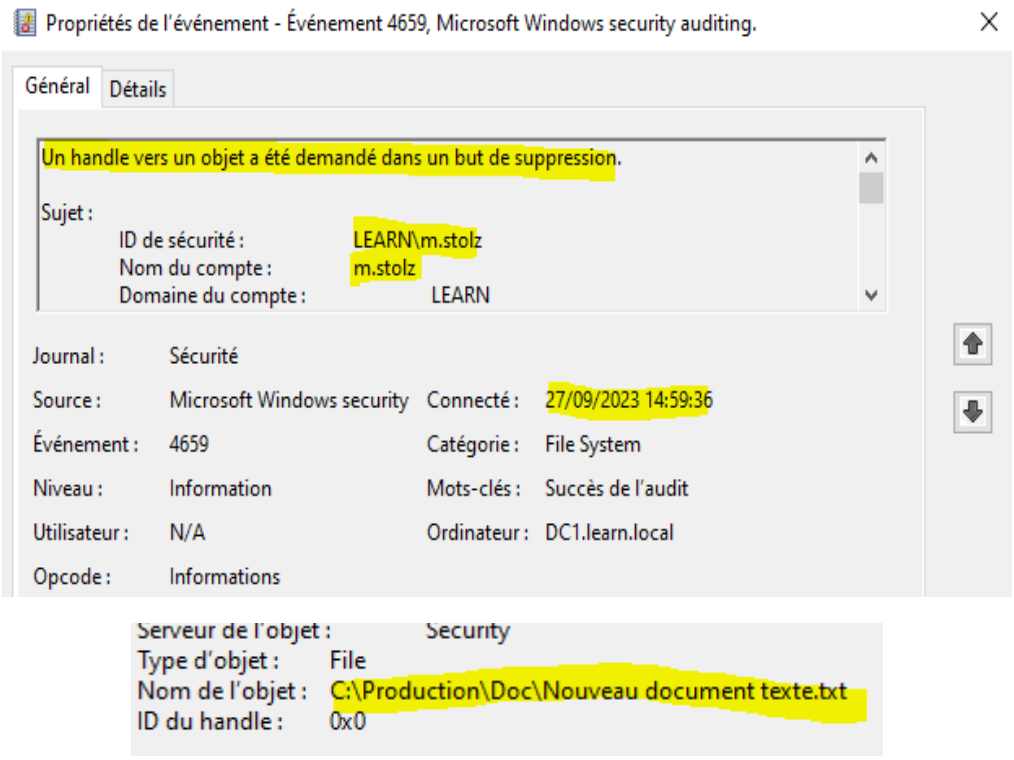
On retourne sur le serveur.

➔ Observateur d'événements →Journaux Windows → Sécurité

On voit « Succès de l'audit » 4659, on clique dessus pour voir le contenu



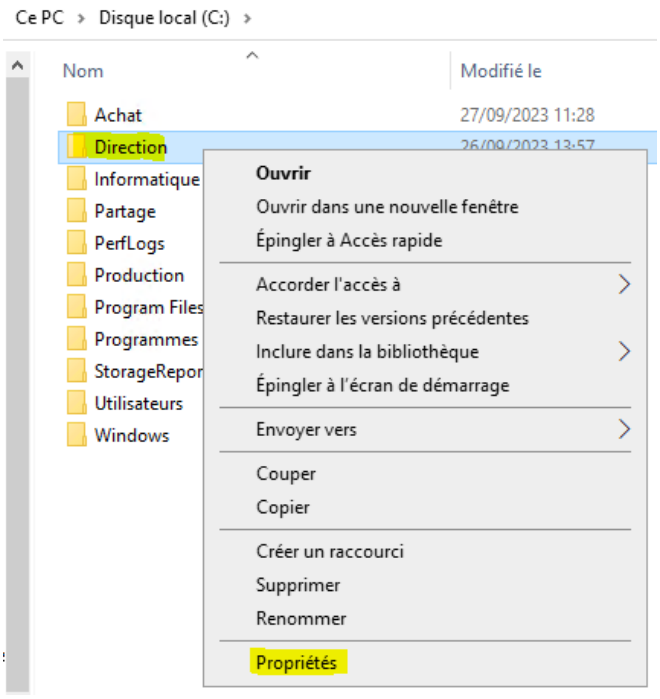
On peut voir l'alerte d'Audit qui nous permet de voir l'utilisateur et quand le document a été supprimer.



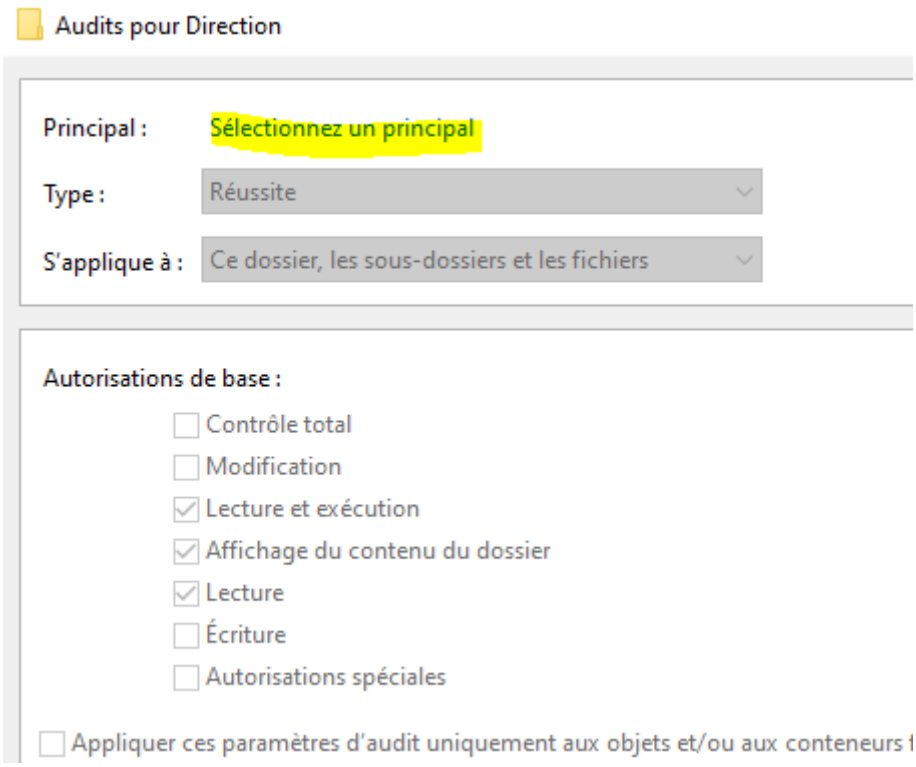
Audit d'autorisation d'accès à un dossier

Pour cette Audit, nous allons surveiller les personnes n'aillant pas les droits et qui cherche à ouvrir le dossier Direction.

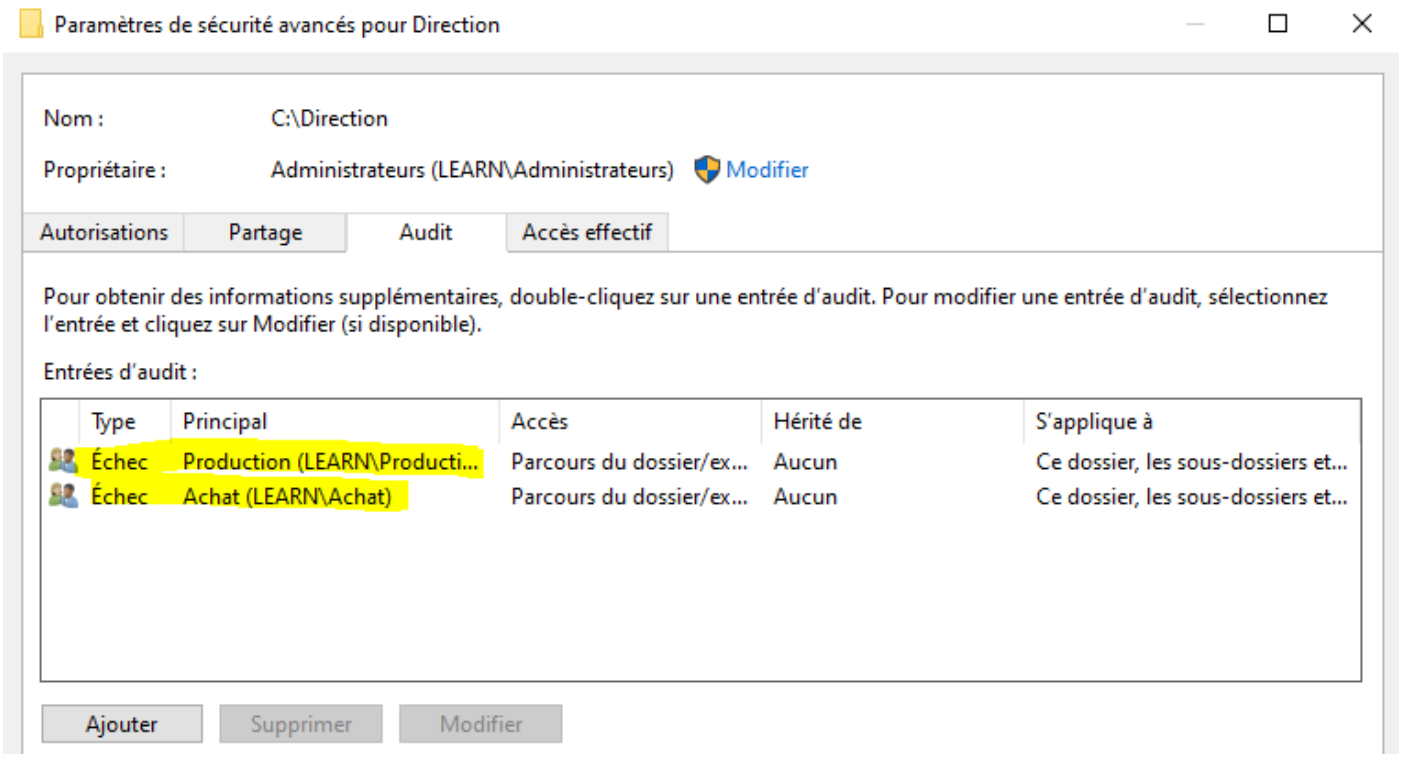
➔ Direction → Clic droit → Propriété



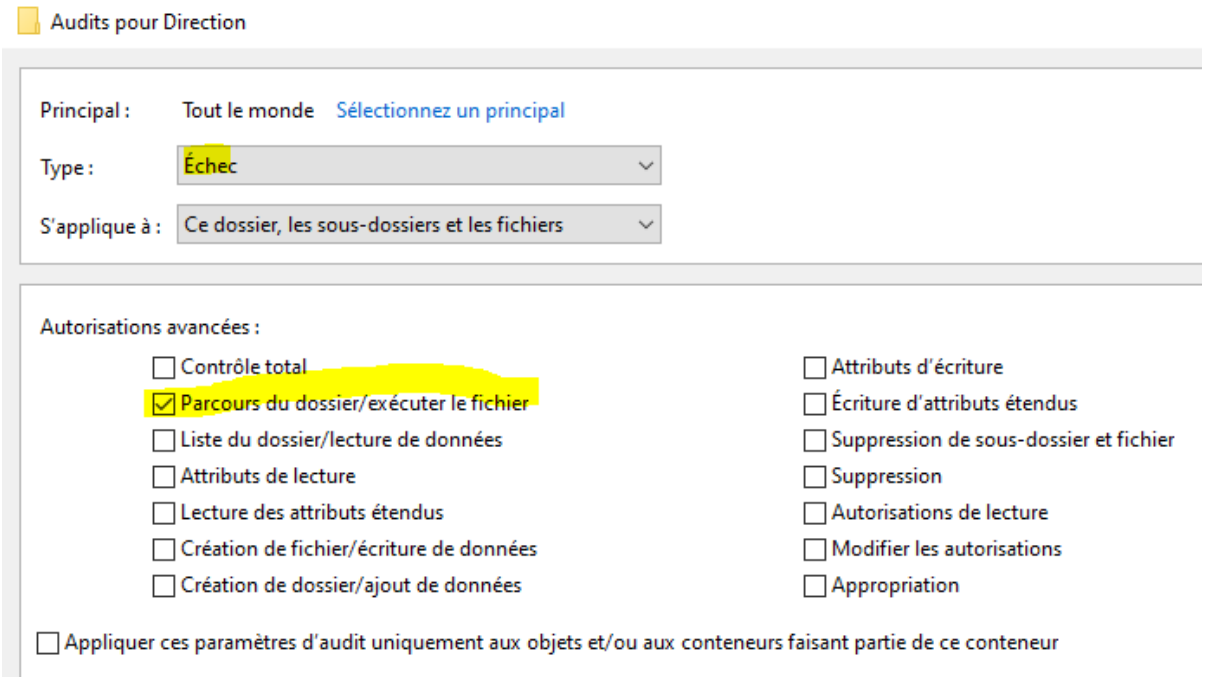
➔ On clique Sélectionnez un principal



➔ On ajoute les groupes Production et Achat en échec.



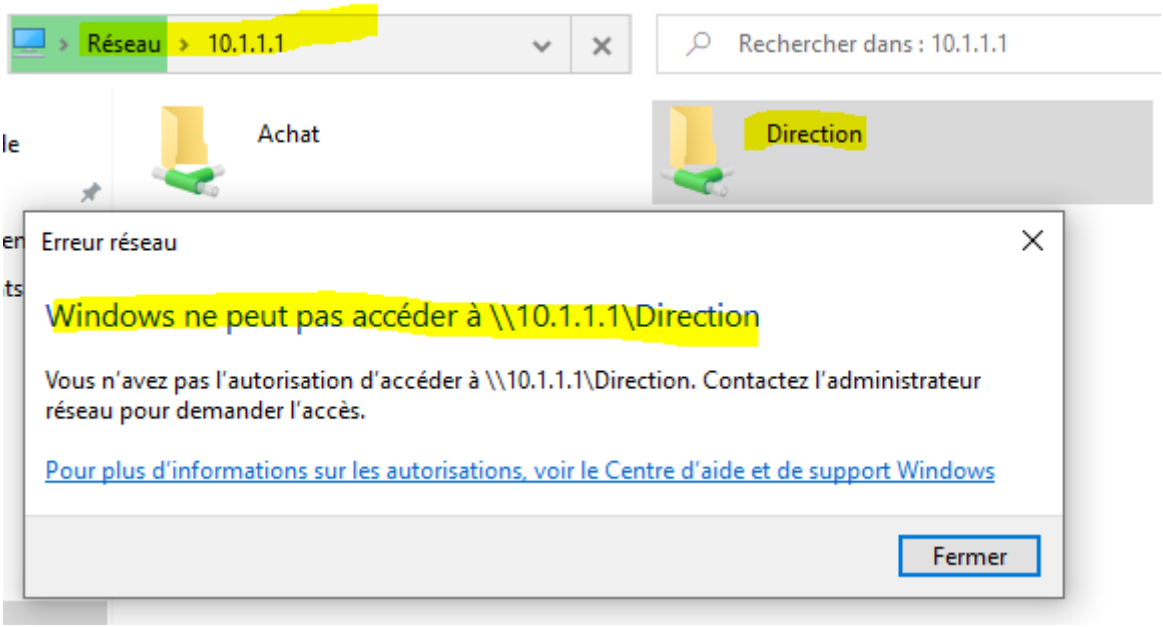
➔ On coche Parcours du dossier/exécuter le fichier



Test de l'Audit

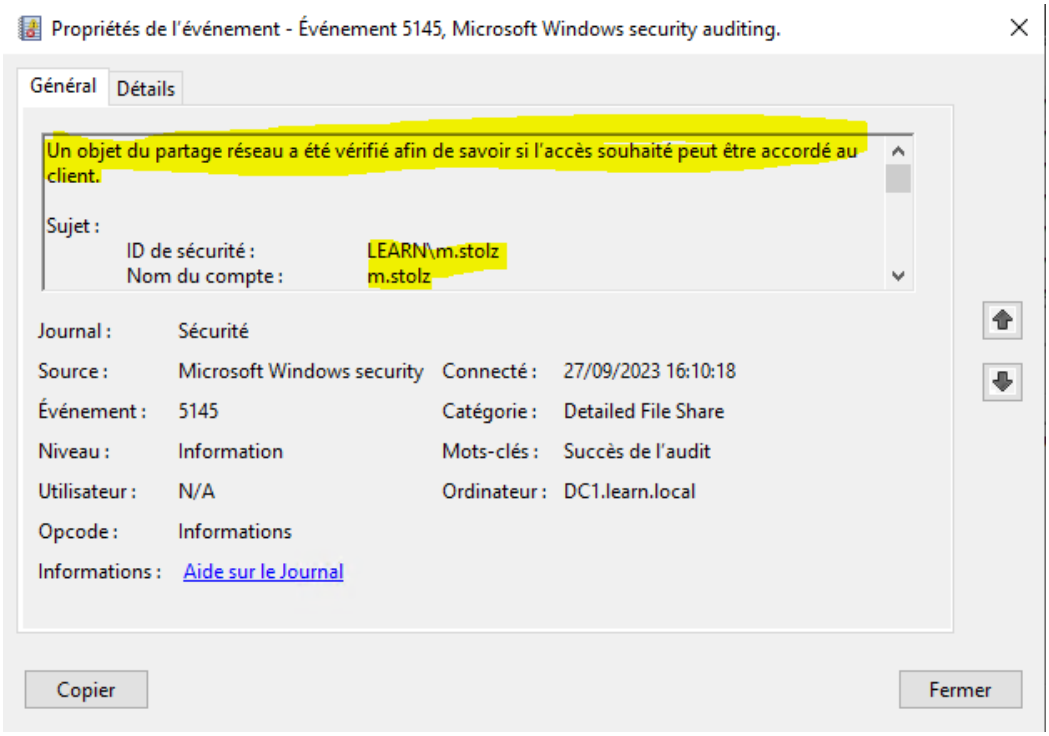
On se connecte avec un utilisateur du groupe Production ou Achat

➔ On tape \\10.1.1.1 → On clique sur le dossier Direction



On retourne sur le serveur.

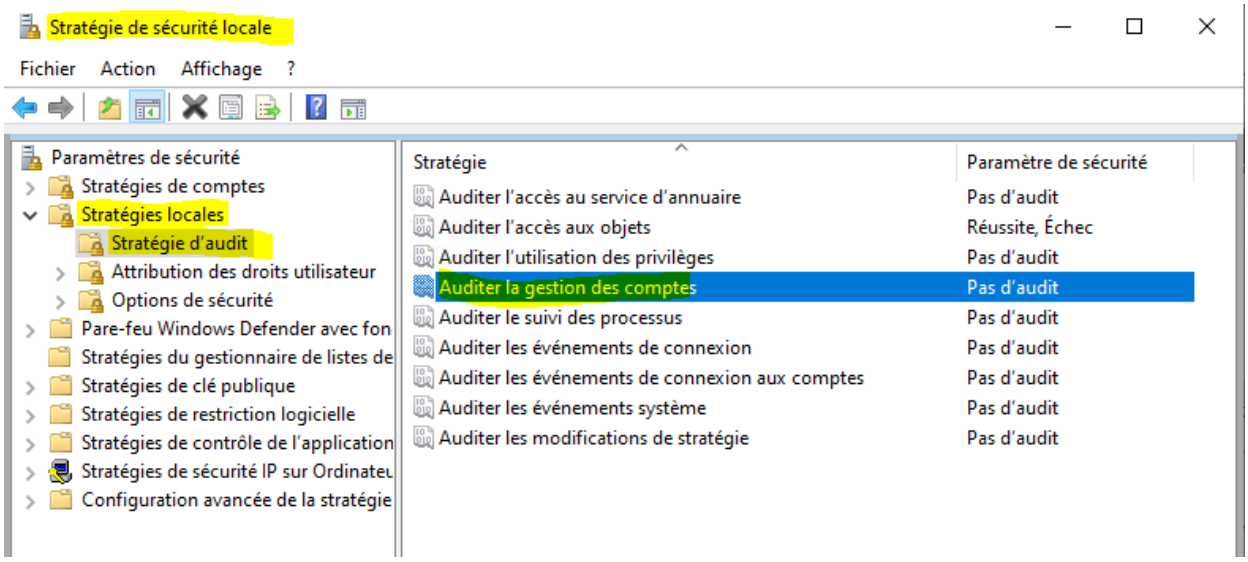
➔ Observateur d'événements →Journaux Windows → Sécurité
On voit « Succès de l'audit » 5145, on clique dessus pour voir le contenu.
On peut voir l'utilisateur qui a tenté d'ouvrir le dossier et l'heure exacte de la tentative.



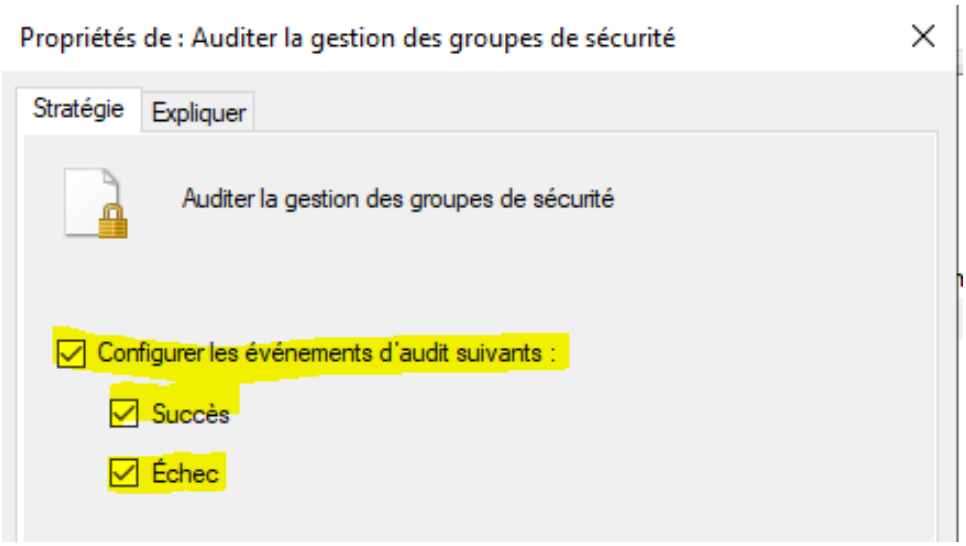
Audit de l'Active Directory

Cette Audit va nous permettre d'être notifier lors de création ou modification d'un utilisateur.

➔ Stratégie de sécurité locale → Stratégie locales → Stratégie d'audit → Auditer la gestion des comptes

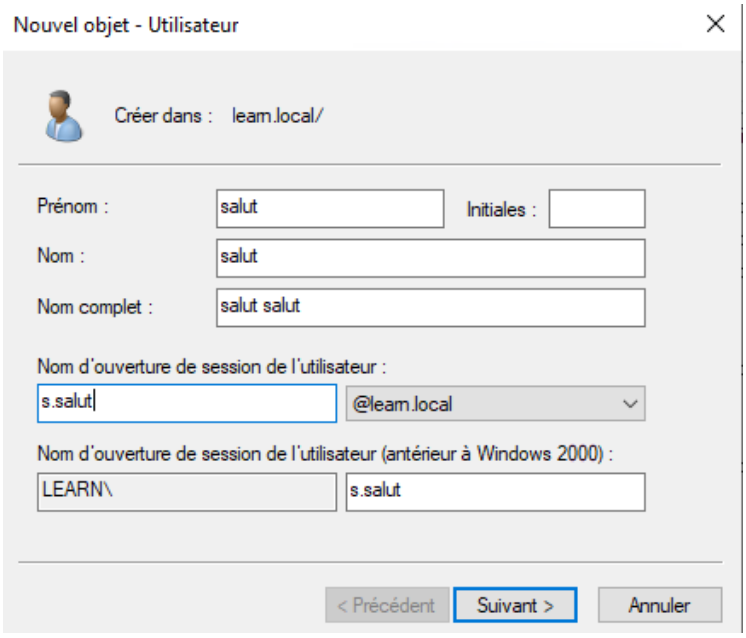


On configure les événements d'audit suivants :



Test de l'Audit

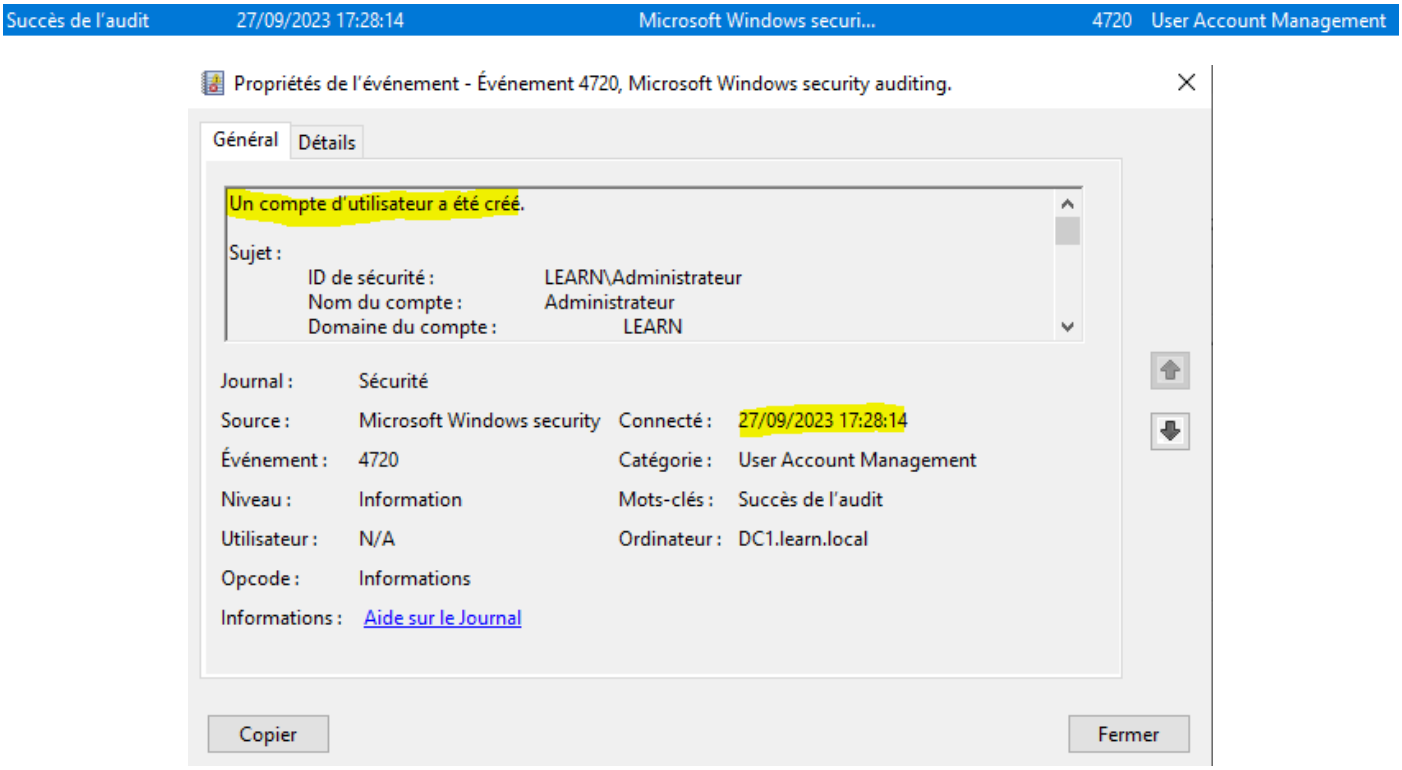
On créer un utilisateur dans l'AD.



On vérifie les logs.

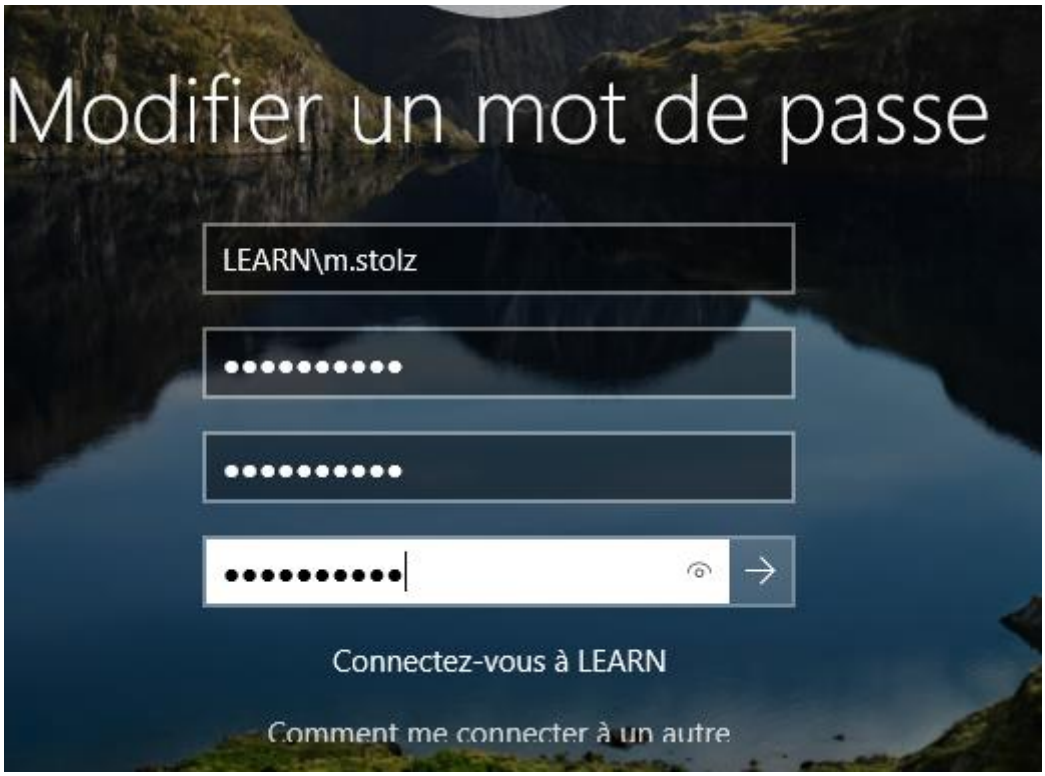
➔ Observateur d'événements →Journaux Windows → Sécurité

On voit « Succès de l'audit » 4720, on clique dessus pour voir le contenu.



Test de l'Audit pour le mot de passe

On modifie le mot de passe d'un utilisateur du domaine.



➔ Observateur d'événements →Journaux Windows → Sécurité

On voit « Succès de l'audit » 4723, on clique dessus pour voir le contenu.

Conclusion

L'audit permet d'avoir une couche de sécurité supplémentaire sur votre infrastructure.