WINDOWS SERVER

AUDITS

Margaux TANET

CPI

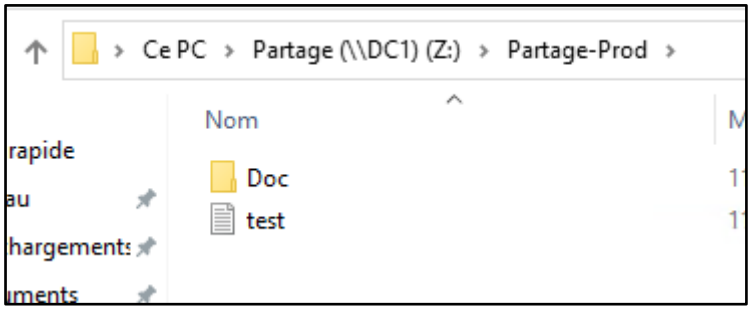
2024-2025

Introduction : Dans ce document, nous allons créer un dossier **Doc** dans le dossier **Production** et y créer un fichier texte **document.txt**. Nous créerons un audit sur le dossier Production pour que tous les utilisateurs ne puissent pas supprimer de fichier ni de sous-dossier. Un test sera réalisé lors d'une suppression de ce fichier sur le client et nous regarderons le journal d'événement sur le serveur. Nous ferons la même chose pour le dossier **Direction**, avec la connexion d'un utilisateur qui ne fait pas partie de Direction pour voir s'il y a accès et si un message d'information apparaît dans le journal d'événement.

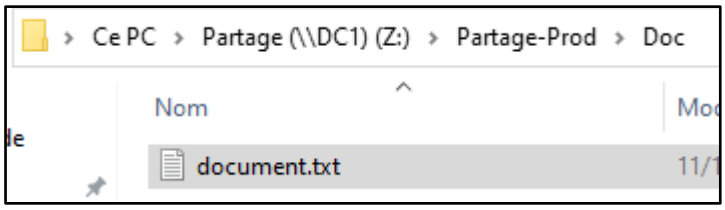
L'audit permet de suivre les activités d'un utilisateur, d'un serveur, etc. En configurant un audit, il est possible de spécifier quelles tâches peuvent être recensé et retrouvés par la suite dans le journal d'événement. Des informations tel que les actions effectuées, l'utilisateur qui a effectué ces actions ainsi que la réussite ou l'échec de l'événement sont des éléments visibles dans l'observateur d'événement.

I- Création des différents documents

➢ Création du fichier **doc** dans le partage **production** :



➢ Création du fichier texte **document.txt** dans le dossier partage :

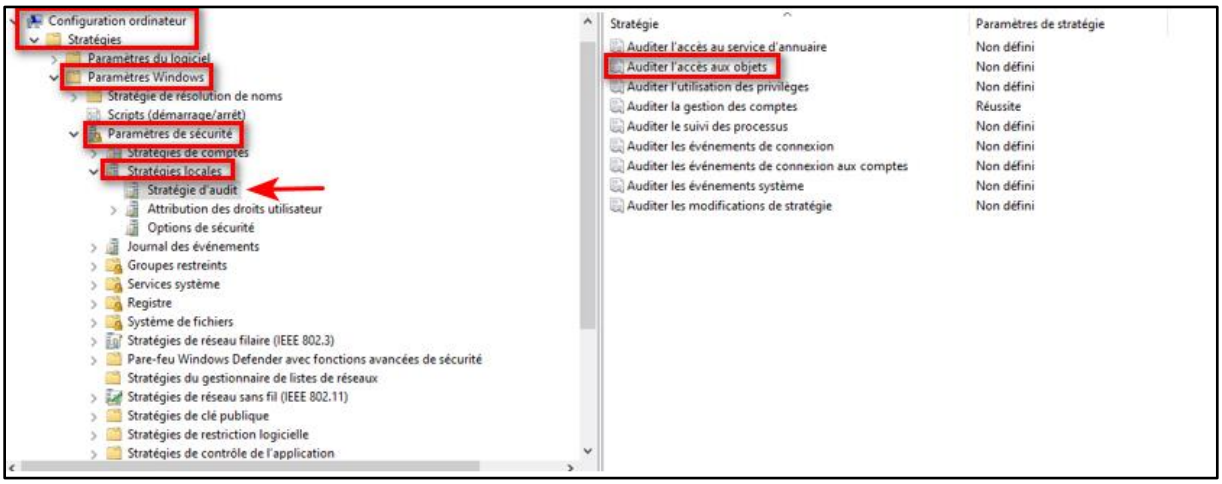


II- Configuration pour l'audit des objets sur le dossier Production

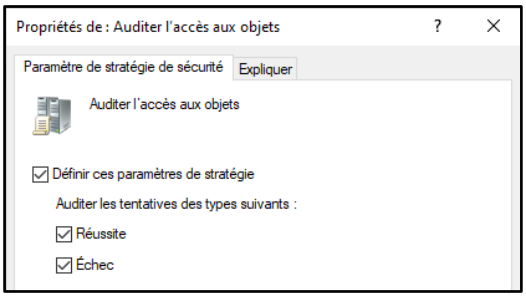
Nous allons activer l'audit des objets via **les stratégies locales ou de groupe** :

Pour cela il faut se rendre dans l'**Éditeur de stratégie de groupe locale**

➢ Aller dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit** :

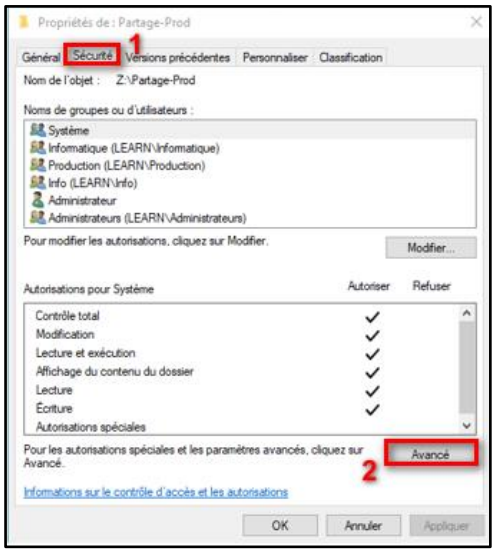


- Dans l'onglet « **paramètre des stratégies de sécurité** », activer **définir ces paramètres de stratégie** et auditer ces tentatives que ce soit pour **Succès** ou **Échec :**

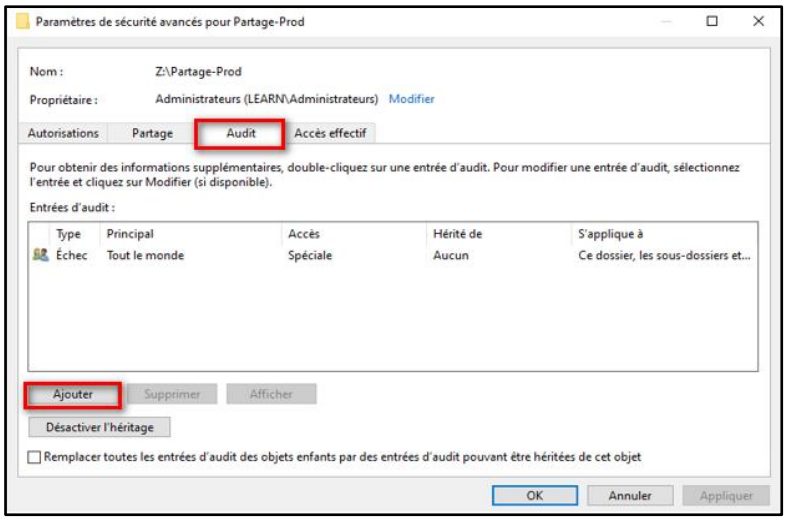


III- Configuration de l'audit sur le dossier Production

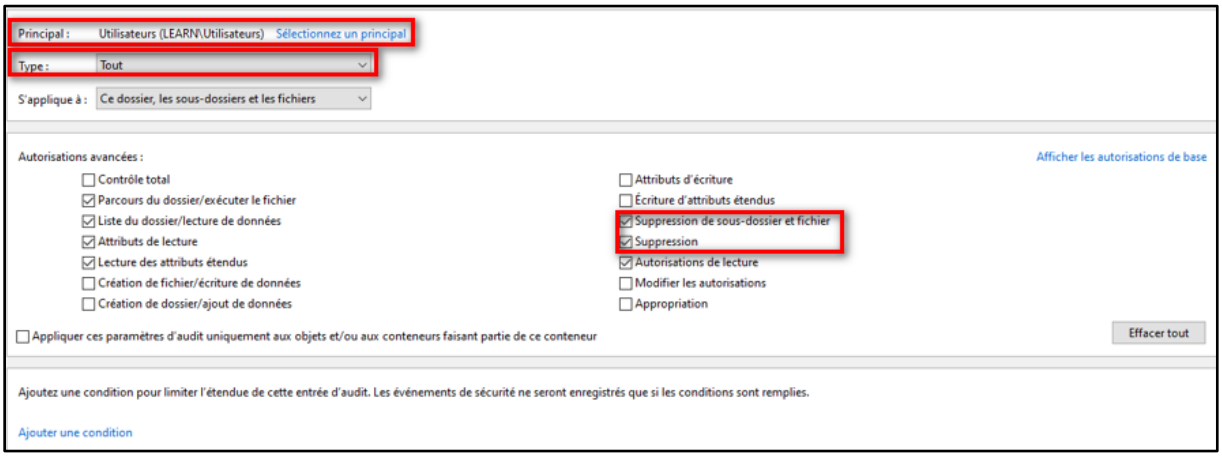
- Se rendre dans l'explorateur de fichier et faire un clic droit sur le dossier Production. Se rendre ensuite dans les **Propriétés** puis l'**onglet Sécurité**. Se rendre dans **Avancé**.



Dans l'onglet **Audit,** cliquer sur Ajouter.



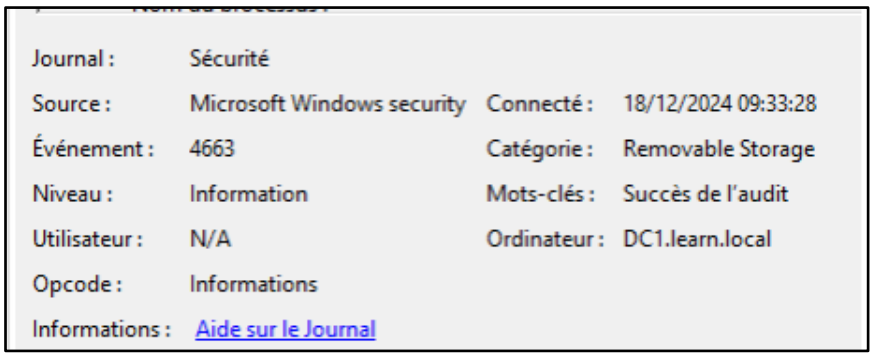
- Pour **principal**, indiquer **Utilisateurs**.
- Pour **type** : **Succès** et **Échec**.
- Pour les **autorisations**, cocher **Suppression** et **Suppression de sous-dossier et fichier**.



IV- Test : journal d'évènement

Lorsque nous essayons de supprimer le fichier texte depuis le client, il est impossible de le faire ce qui est normal. Sur notre serveur, si l'audit fonctionne, il doit y avoir une information liée à notre test réalisé juste avant.

Dans le journal d'évènement, on perçoit le message 4663 « **tentative d'accès à un objet a été effectuée** ».

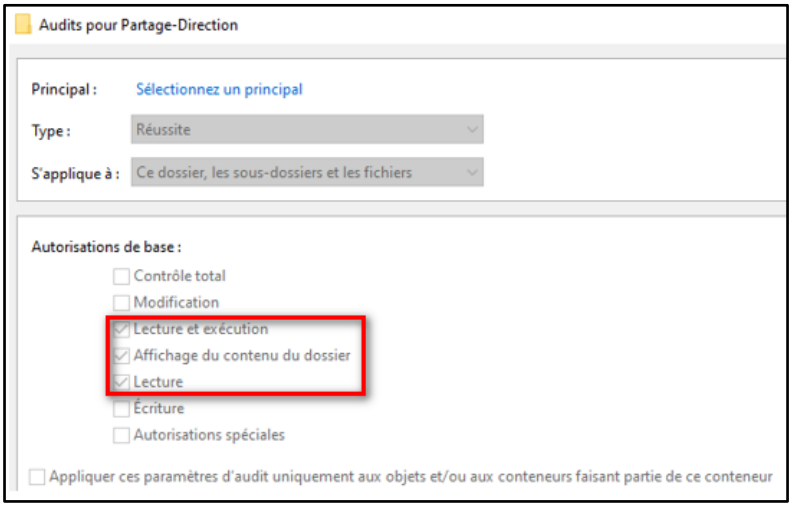


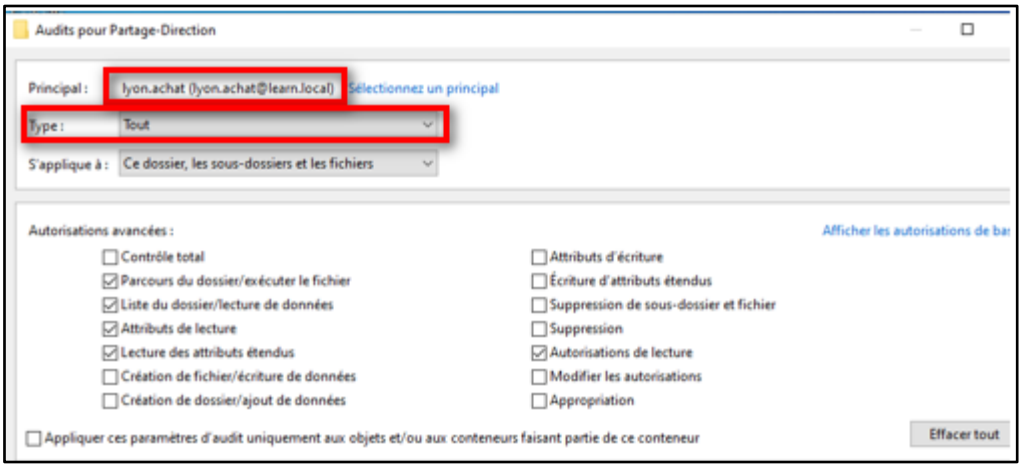
V- Configuration de l'audit sur le dossier Direction

De la même manière qu'a été réalisé l'audit sur le dossier **Production**, les mêmes actions vont être réalisées sur le dossier **Direction**.

- Faire un clic droit sur le dossier **Direction** puis **Propriétés** > **Onglet Sécurité**.

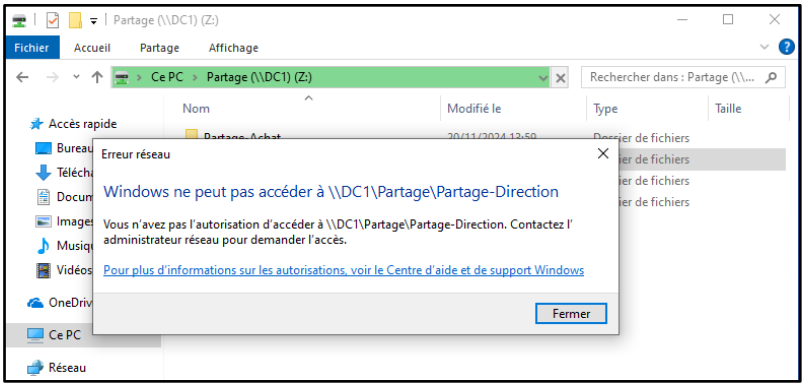
- Se rendre dans **Avancé** puis aller dans l'onglet **Audit**.
- Cliquer sur **ajouter** puis dans principal mettre un utilisateur autre qu'Informatique ou Direction. Par exemple, ici il a été mis lyon.achat. Pour le **type**, mettre **Tout**.
- Pour les autorisations : **Lecture**, **Affichage du contenu du dossier et lecture et exécution.**



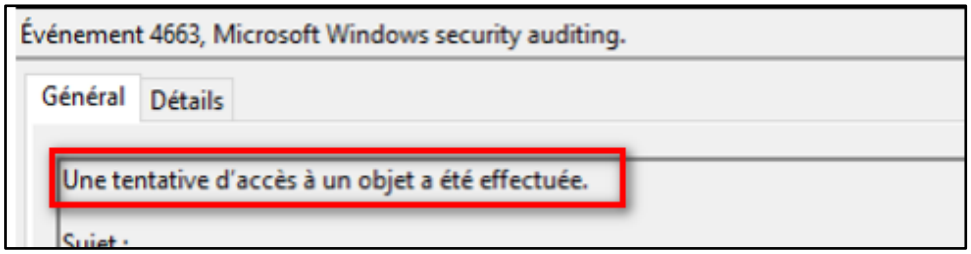


VI- Test : journal d'évènement

- Se connecter sur son utilisateur (ici achat) et essayer d'accéder au dossier de Direction :



Dans le journal d'évènement, se rendre dans l'onglet **journaux Windows** puis **Sécurité**. Il faut rechercher un message qui indiquerait qu'un utilisateur accède au dossier. Ici on peut voir qu'une tentative d'accès à un dossier a été effectuée :



Conclusion : Nous avons mis en place différents audits sur différents dossiers et nous avons pu constater que ces audits fonctionnent grâce aux différents messages dans le journal d'événement.