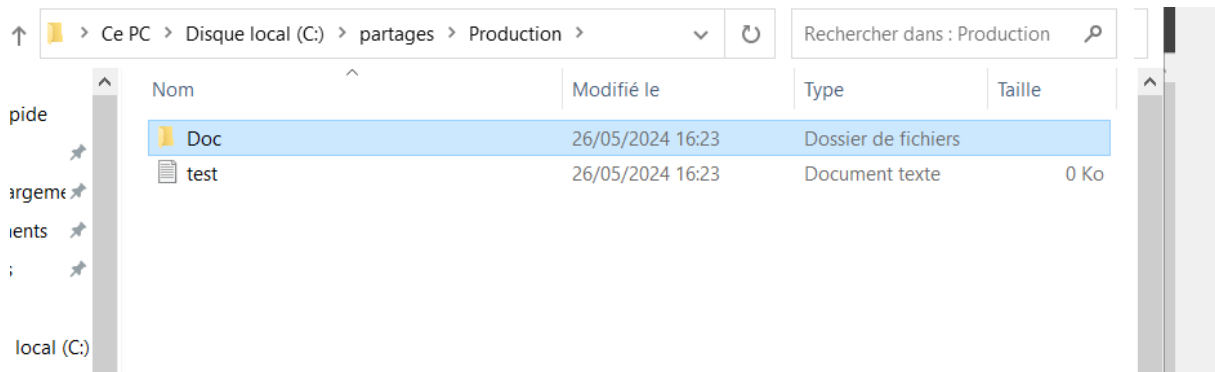
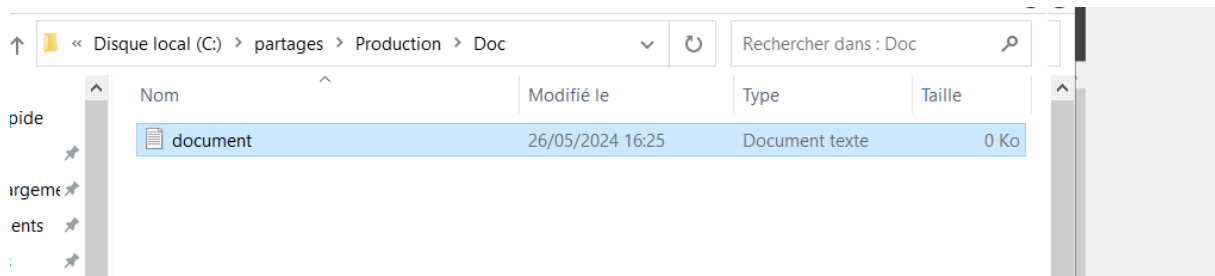


Procédure : Supprimer un fichier

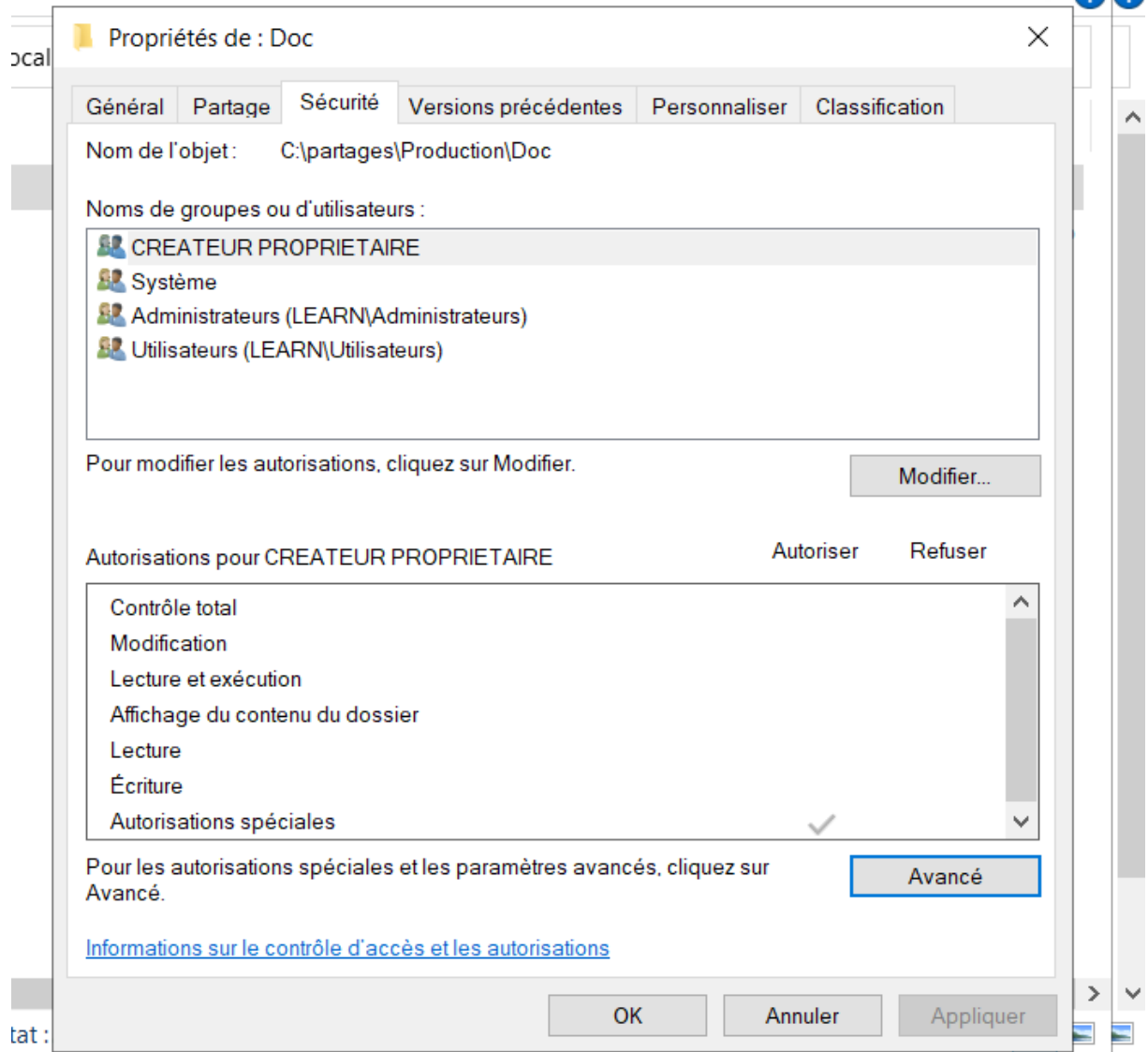
1) En premier je vais sur l'explorateur de fichier de mon serveur puis sur le dossier « partages »
« Production » je crée un dossier Doc .



2) Puis crée un fichier texte « document »



3) Ensuite crée un audit sur ce dossier , dans ce cas je fais un clic droit sur le dossier « Doc »
ensuite « sécurité » puis « Avancé »



4) Je clique sur Audit puis « Ajouter »

Nom : C:\partages\Production\Doc

Propriétaire : Administrateurs (LEARN\Administrateurs) [Modifier](#)

Autorisations | Partage | **Audit** | Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'audit. Pour modifier une entrée d'audit, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'audit :

Type	Principal	Accès	Hérité de	S'applique à
------	-----------	-------	-----------	--------------

[Ajouter](#) [Supprimer](#) [Afficher](#)

[Désactiver l'héritage](#)

☐ Remplacer toutes les entrées d'audit des objets enfants par des entrées d'audit pouvant être héritées de cet objet

[OK](#) [Annuler](#) [Appliquer](#)

5) Je clique sur « Sélectionner un principal »

Audits pour Doc

Principal : [Sélectionnez un principal](#)

Type : Réussite

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations de base : [Afficher les autorisations avancées](#)

- ☐ Contrôle total
- ☐ Modification
- ☒ Lecture et exécution
- ☒ Affichage du contenu du dossier
- ☒ Lecture
- ☐ Écriture
- ☐ Autorisations spéciales

☐ Appliquer ces paramètres d'audit uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur [Effacer tout](#)

Ajoutez une condition pour limiter l'étendue de cette entrée d'audit. Les événements de sécurité ne seront enregistrés que si les conditions sont remplies.

[Ajouter une condition](#)

[OK](#) [Annuler](#)

6) Ensuite « utilisateur du domaine » dans ce cas puis valider

Audits pour Doc

Sélectionnez un utilisateur, un ordinateur, un compte de service ou un groupe

Sélectionnez le type de cet objet:
un utilisateur, un groupe ou Principal de sécurité intégré

A partir de cet emplacement:
learn.local

Entrez le nom de l'objet à sélectionner (exemples):
Utilisateurs du domaine

Types d'objets...
Emplacements...
Vérifier les noms

Avancé... OK Annuler

☒ Affichage du contenu du dossier
☒ Lecture
☐ Écriture
☐ Autorisations spéciales

☐ Appliquer ces paramètres d'audit uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

Afficher les autorisat

7) Je choisis « réussite » puis clique sur « Afficher les autorisations de base » puis cocher sur « Suppression » et « Suppression de sous dossier et fichier »

Audits pour Doc

Principal : Utilisateurs du domaine (LEARN\Utilisateurs du domaine) Sélectionnez un principal

Type : Réussite

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations avancées : Afficher les autorisations de base

<input type="checkbox"/> Contrôle total	<input type="checkbox"/> Attributs d'écriture
<input type="checkbox"/> Parcours du dossier/exécuter le fichier	<input type="checkbox"/> Écriture d'attributs étendus
<input checked="" type="checkbox"/> Liste du dossier/lecture de données	<input checked="" type="checkbox"/> Suppression de sous-dossier et fichier
<input checked="" type="checkbox"/> Attributs de lecture	<input checked="" type="checkbox"/> Suppression
<input checked="" type="checkbox"/> Lecture des attributs étendus	<input type="checkbox"/> Autorisations de lecture
<input type="checkbox"/> Création de fichier/écriture de données	<input type="checkbox"/> Modifier les autorisations
<input type="checkbox"/> Création de dossier/ajout de données	<input type="checkbox"/> Appropriation

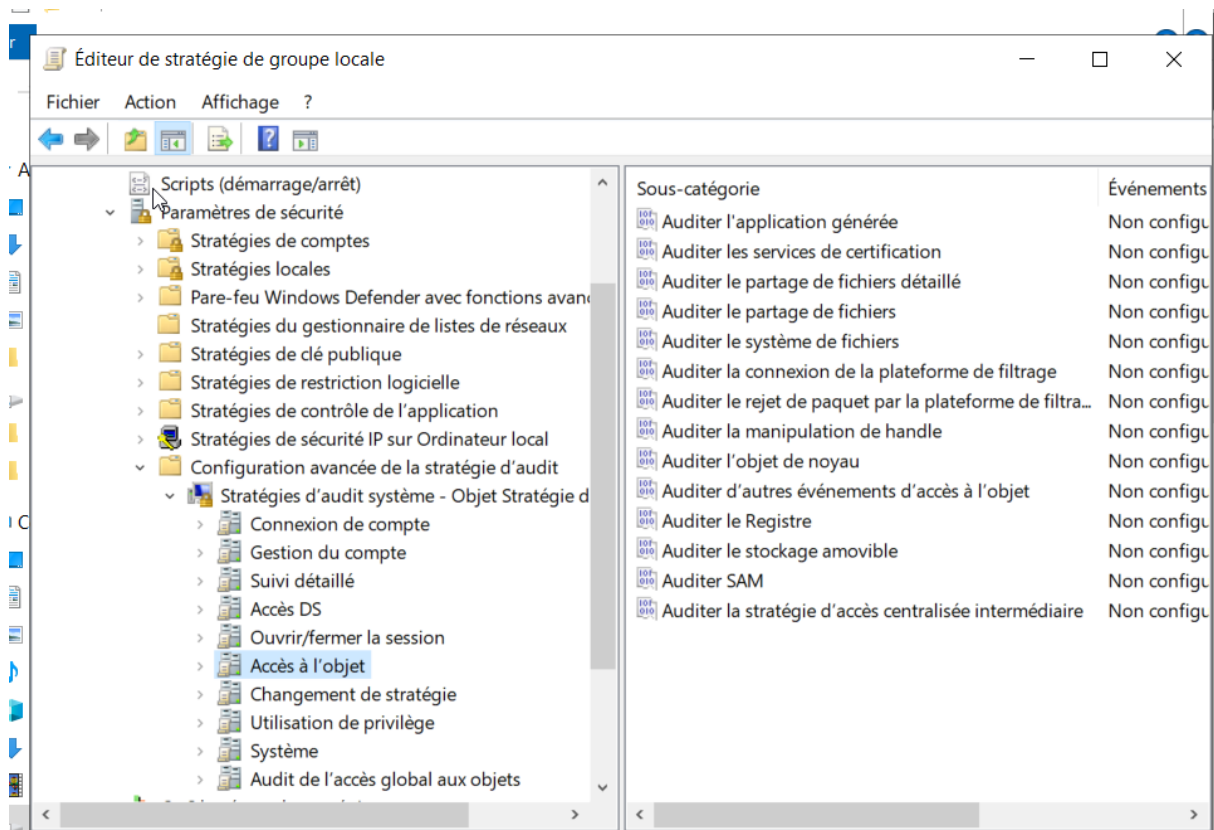
☐ Appliquer ces paramètres d'audit uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur Effacer tout

Ajoutez une condition pour limiter l'étendue de cette entrée d'audit. Les événements de sécurité ne seront enregistrés que si les conditions sont remplies.

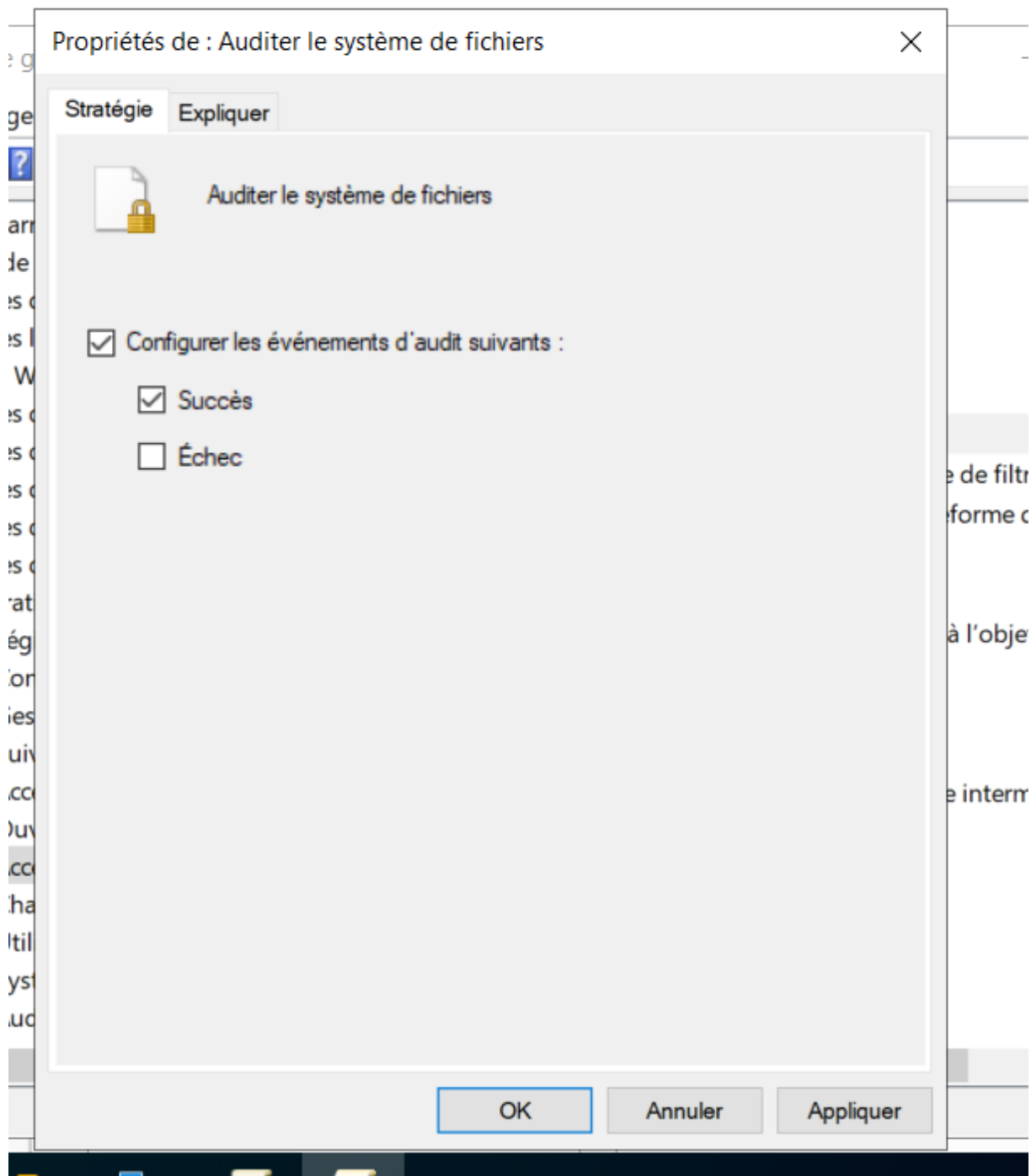
Ajouter une condition

OK Annuler

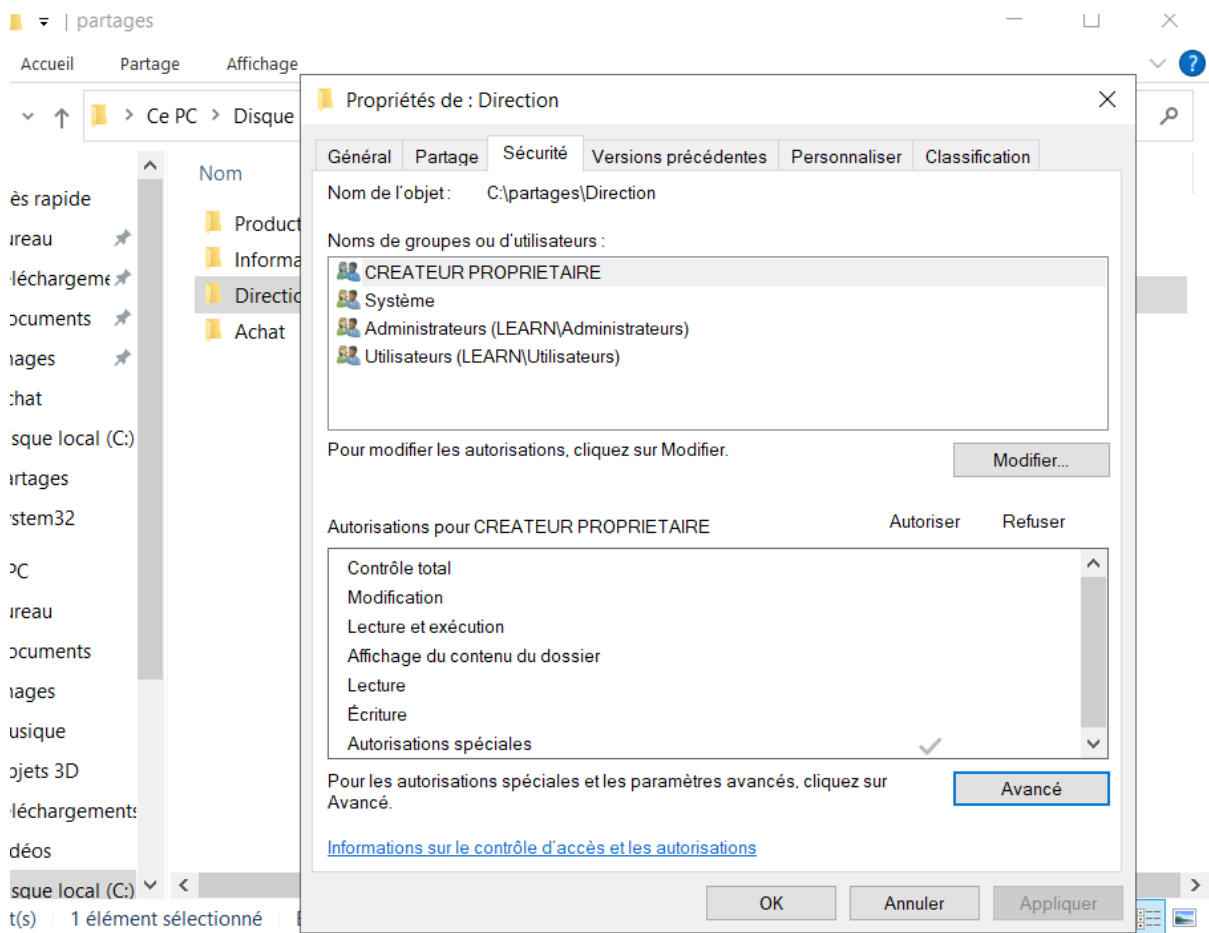
8) Dans la stratégie de groupe, allez dans « Configuration Ordinateur->Paramètres Windows -> Paramètre de sécurité -> Configuration avancée de la stratégie d'audit -> Accès à l'objet -> Auditer le système de fichiers » :



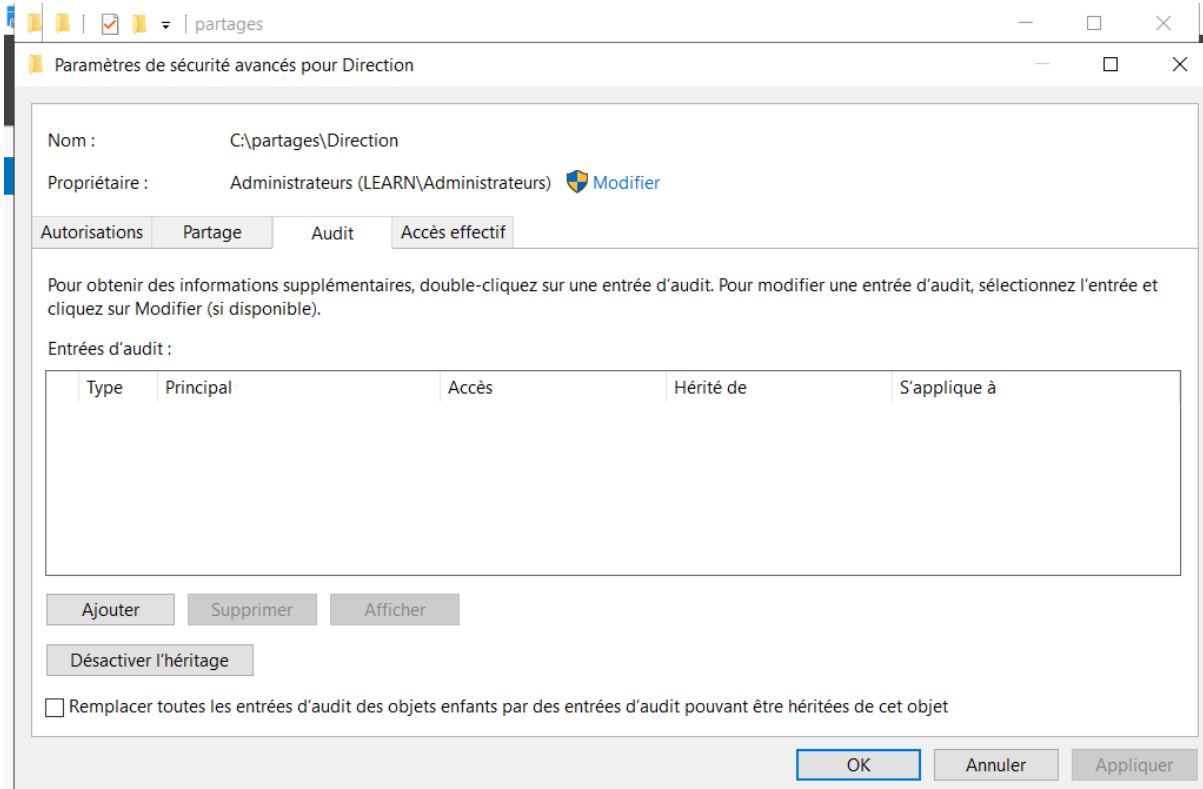
9) Puis je coche les deux cases « Configurer les événements d'audit suivants » puis « Succès »
:Dispose d'un menu contextuel



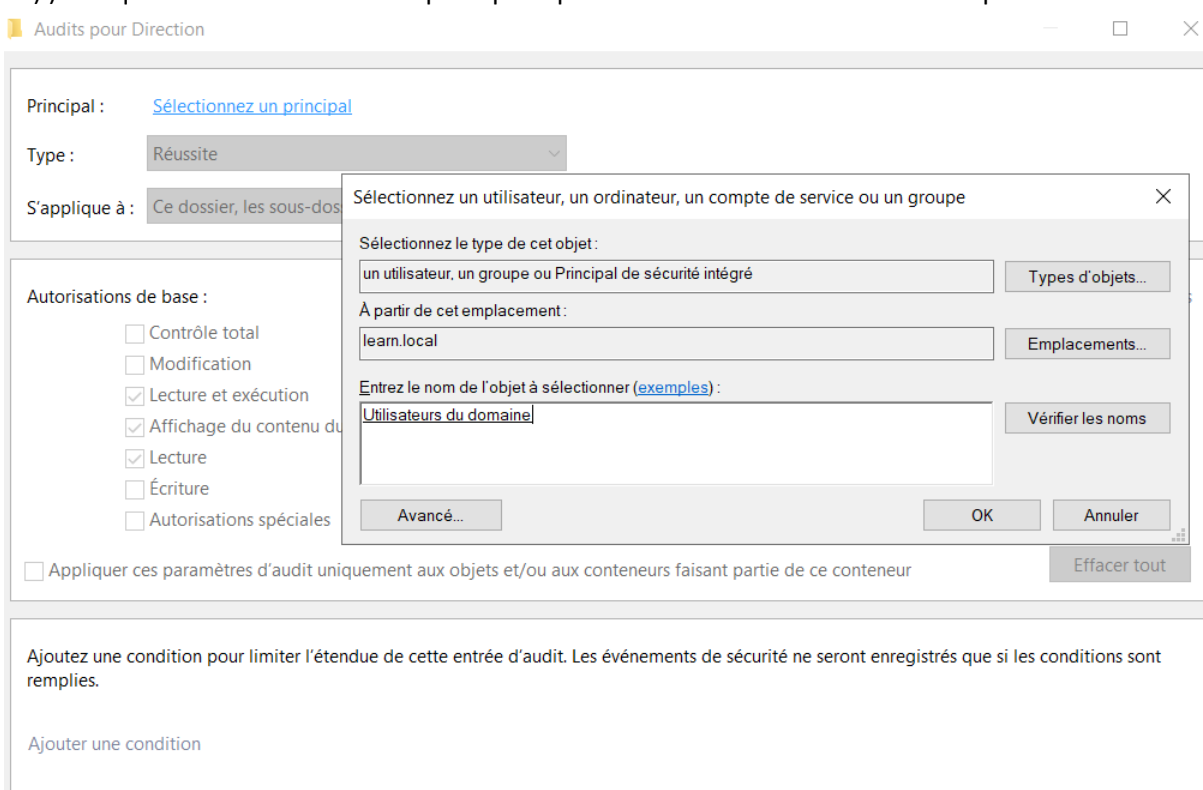
9) je fais un clic droit sur le dossier « Doc » ensuite « sécurité » puis « Avancé »



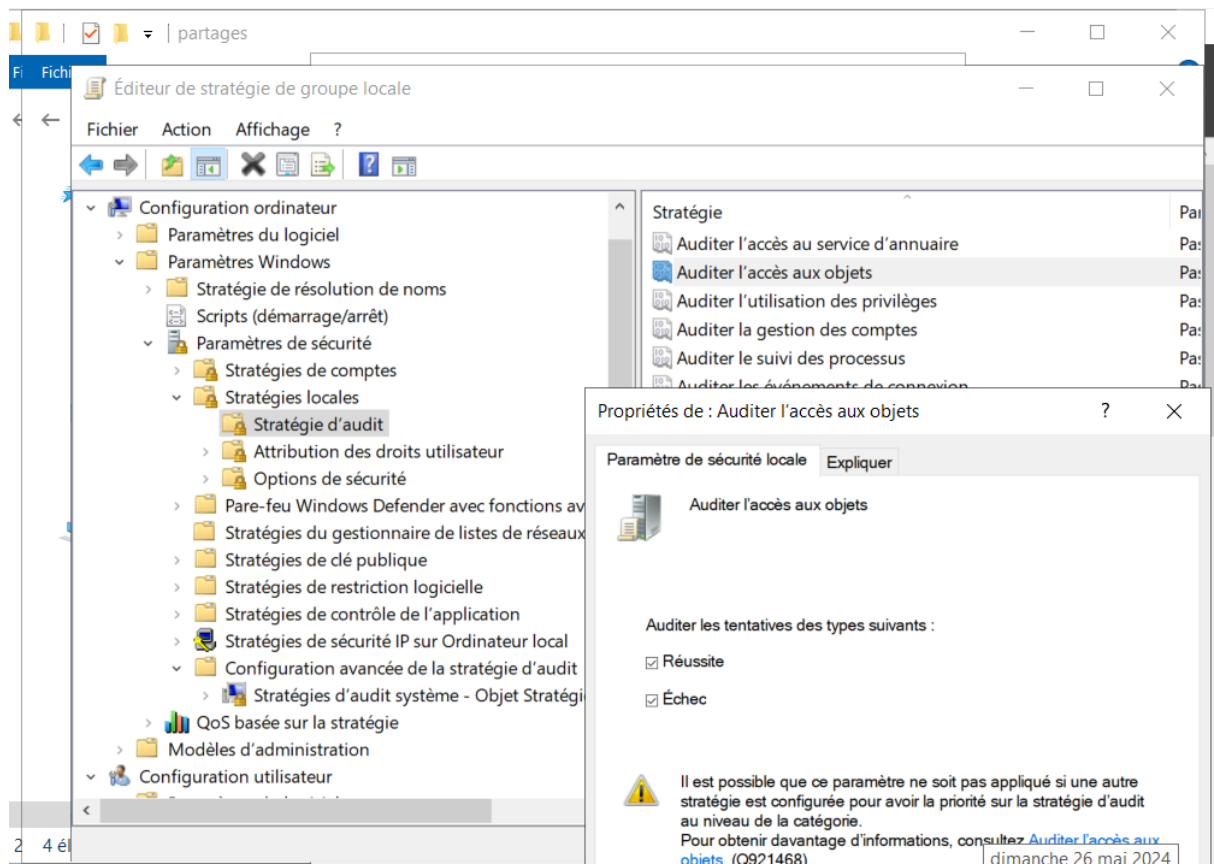
10) Je clic sur Audit puis « Ajouter »



11) Je clique sur « Sélectionner un principal » puis sur « utilisateur du domaine » puis valider



12) Dans la stratégie de groupe, allez dans « Configuration Ordinateur->Paramètres Windows -> Paramètre de sécurité -> stratégie d'audit -> Auditer Accès aux objets -> et cocher « réussite » et « succès »



13) j'ouvre mon journal d'évènement et voici le résultat

Observateur d'événements

Fichier

Propriétés de l'événement - Événement 5145, Microsoft Windows security auditing.

Général Détails

Un objet du partage réseau a été vérifié afin de savoir si l'accès souhaité peut être accordé au client.

Sujet :

ID de sécurité : Système

Nom du compte : WIN\$

Journal : Sécurité

Source : Microsoft Windows security ; Connecté : 26/05/2024 17:48:46

Événement : 5145 Catégorie : Detailed File Share

Niveau : Information Mots-clés : Succès de l'audit

Utilisateur : N/A Ordinateur : win.learn.local

Opcode : Informations

Informations : [Aide sur le Journal](#)

Copier Fermer

Succès... 26/05/2024 17:48:46 Microso... 4719 Audit Po...

Succès... 26/05/2024 17:48:46 Microso... 4719 Audit Po...

Événement 5145, ...

Propriétés d...

Joindre une ...

Copier