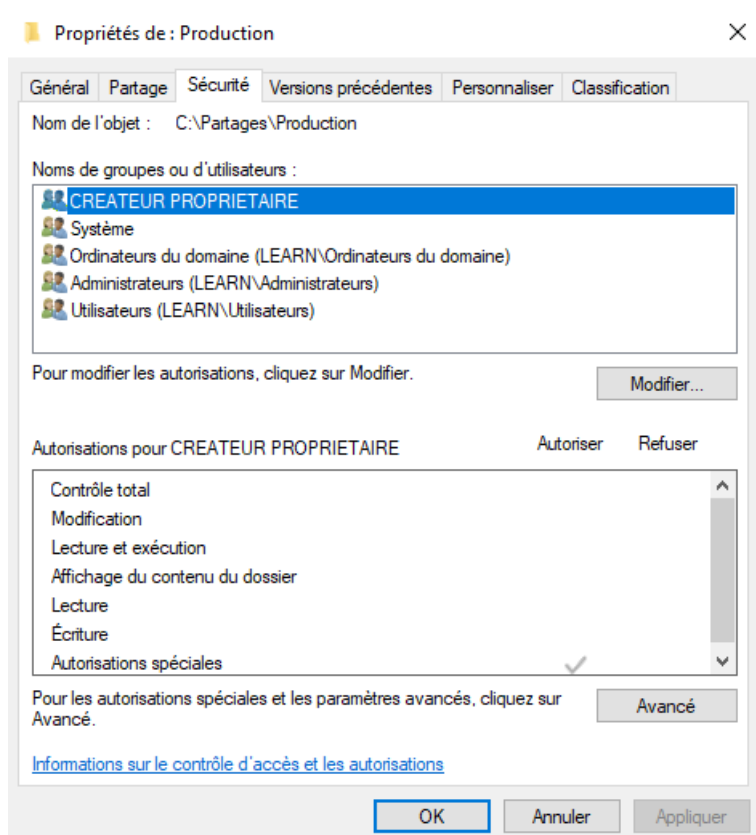


## Procédures

Pour commencer, créer un sous-dossier « Doc » dans le dossier Production.

Ensuite rendez-vous dans l'onglet sécurité du dossier Production.



Ensuite cliqué sur « Avancé » en bas. Et rendez-vous dans Audit.

Paramètres de sécurité avancés pour Production

Nom : C:\Partages\Production

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

Ce qui nous ramène à cette page.

En haut de cette page sélectionner **utilisateurs du domaine**, ensuite de type « Réussite » puis donner les autorisations nécessaires. Cliquez ensuite sur *Afficher les autorisations avancées*. Et cochez les cases « suppressions » et « suppressions de sous-dossier et fichier » Puis valider tout ça en cliquant sur ok.

Audits pour Production

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 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

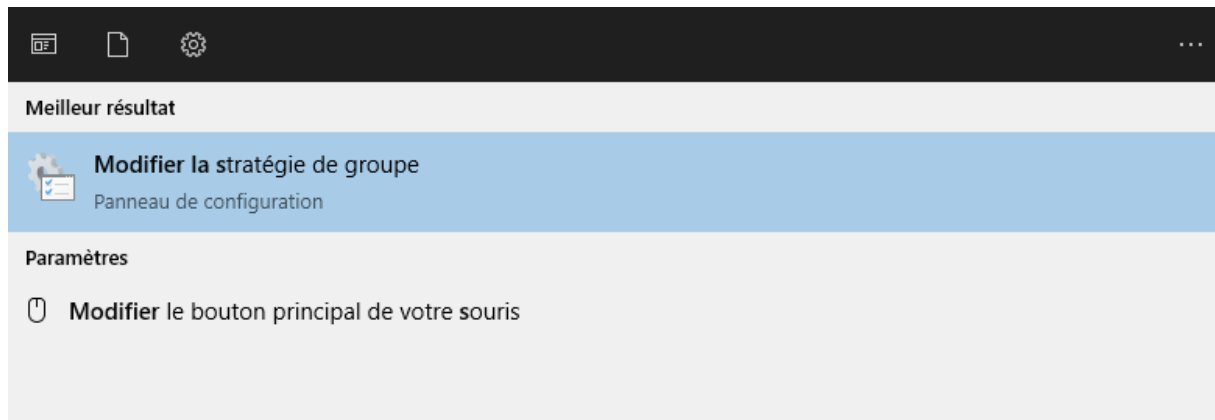
Effacer tout

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.

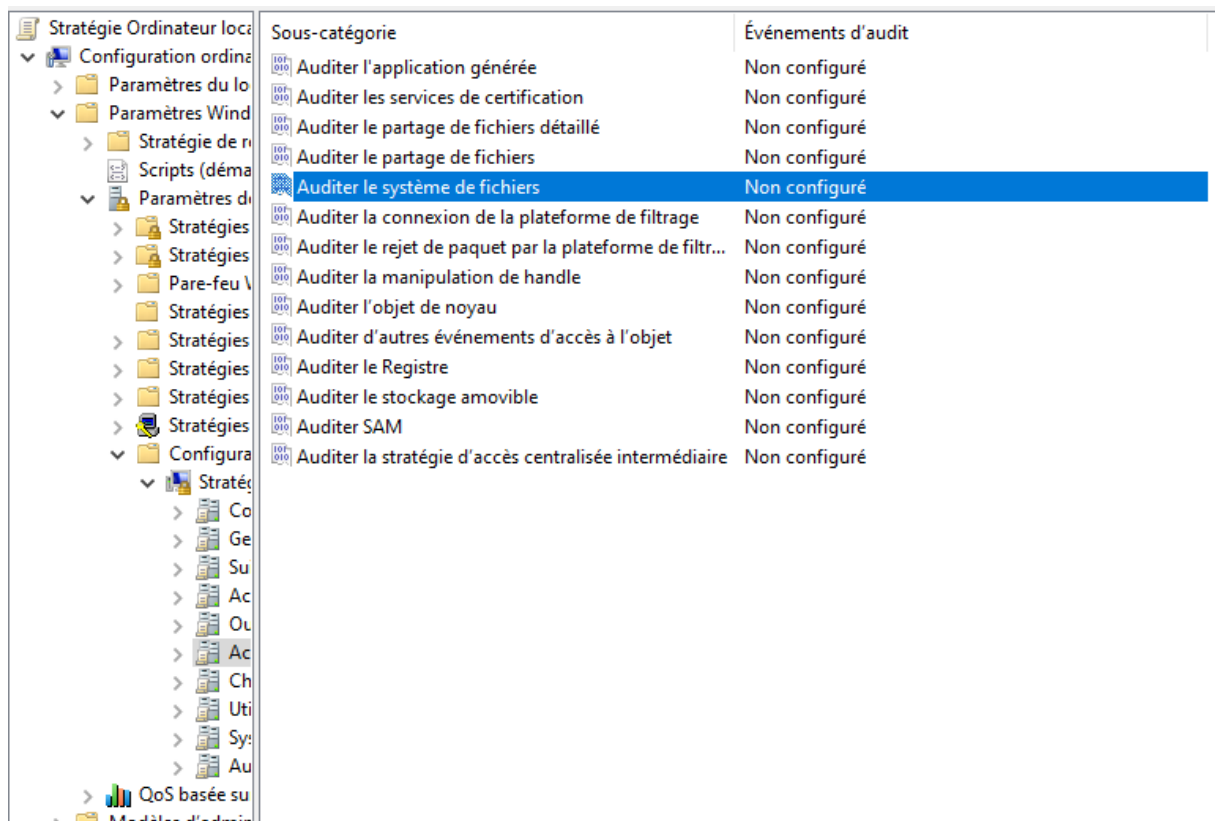
[Ajouter une condition](#)

OK Annuler

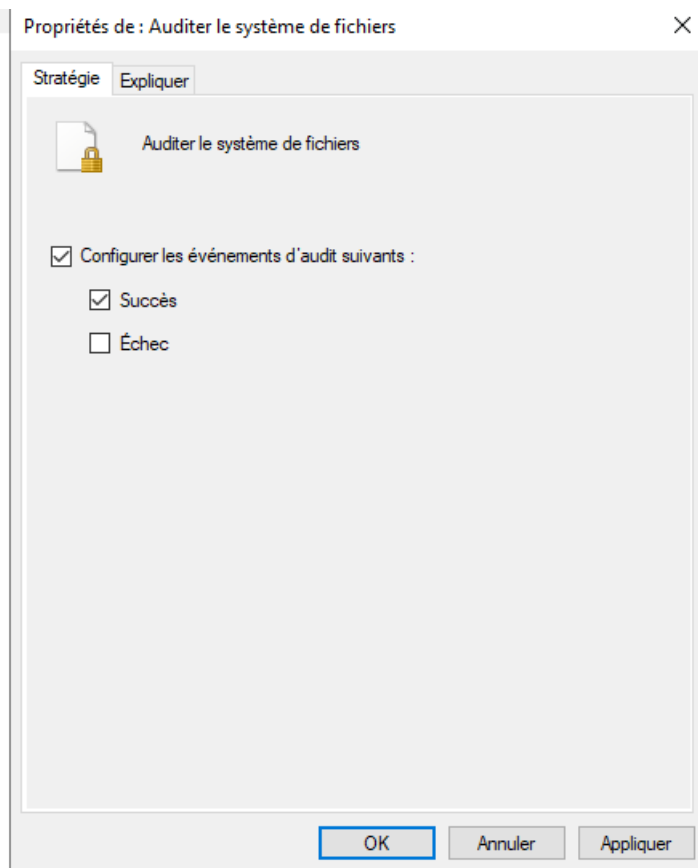
Ensuite rendez-vous dans le bureau et tapez dans la barre de recherche : *Modifier la stratégie de groupe*.



Une fois dedans cliquez sur *paramètre Windows* -> *paramètre de sécurité* -> *configuration avancée de la stratégie de l'audit* -> *Stratégie d'audit système* puis *accès à l'objet*. Ensuite cliquez sur *auditer le système de fichiers*.

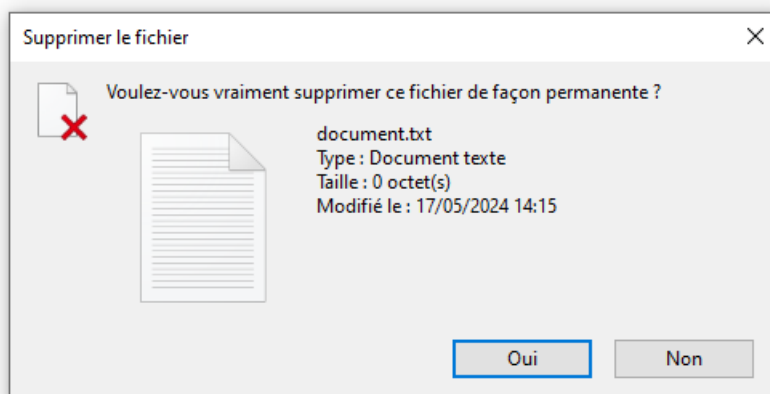


Puis cochez la case *configurer les événements d'audits suivants* puis *succès*. Et validé

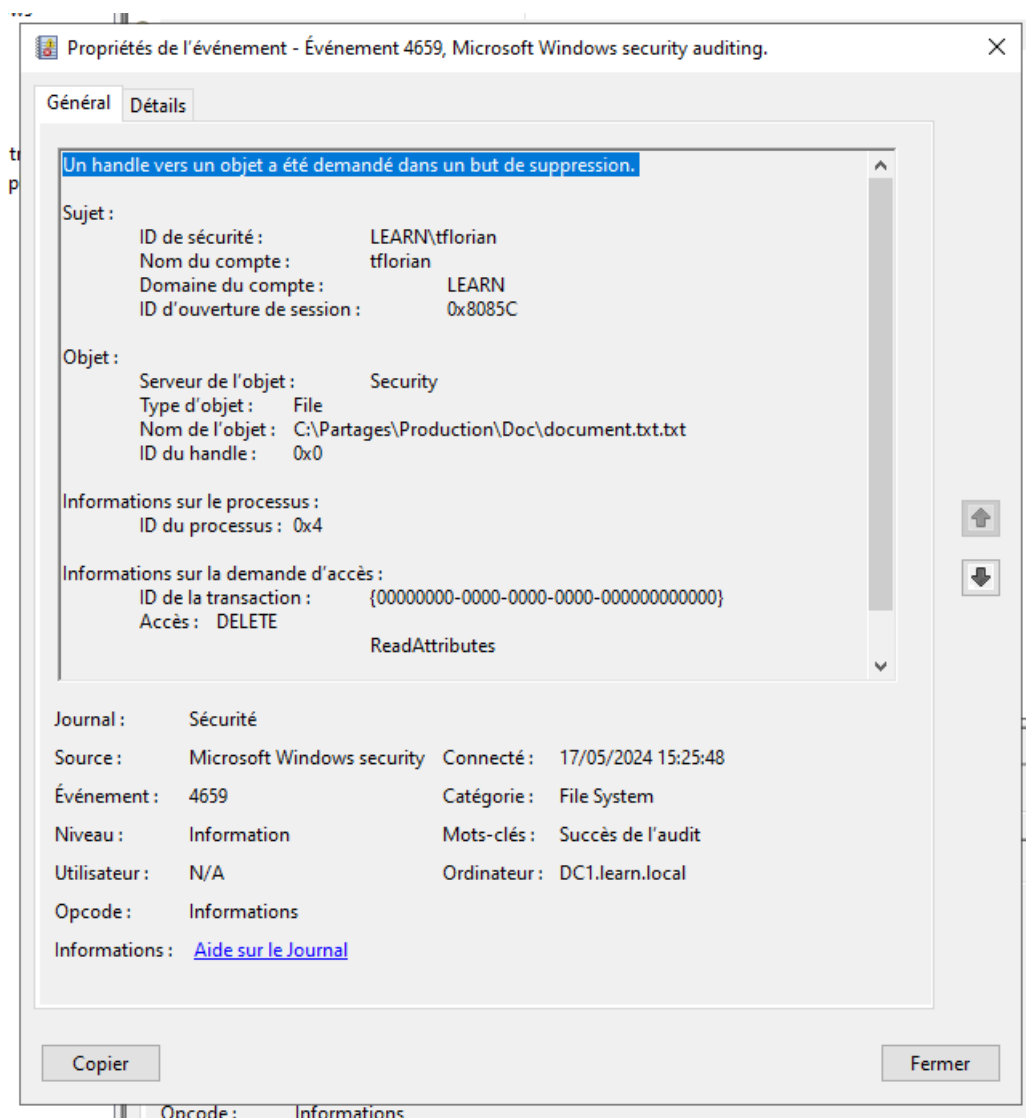


Tout est bon nous pouvons maintenant essayer du coté clients.

Rendez-vous du cote client, essaye de supprimé le doc créer au paravent.

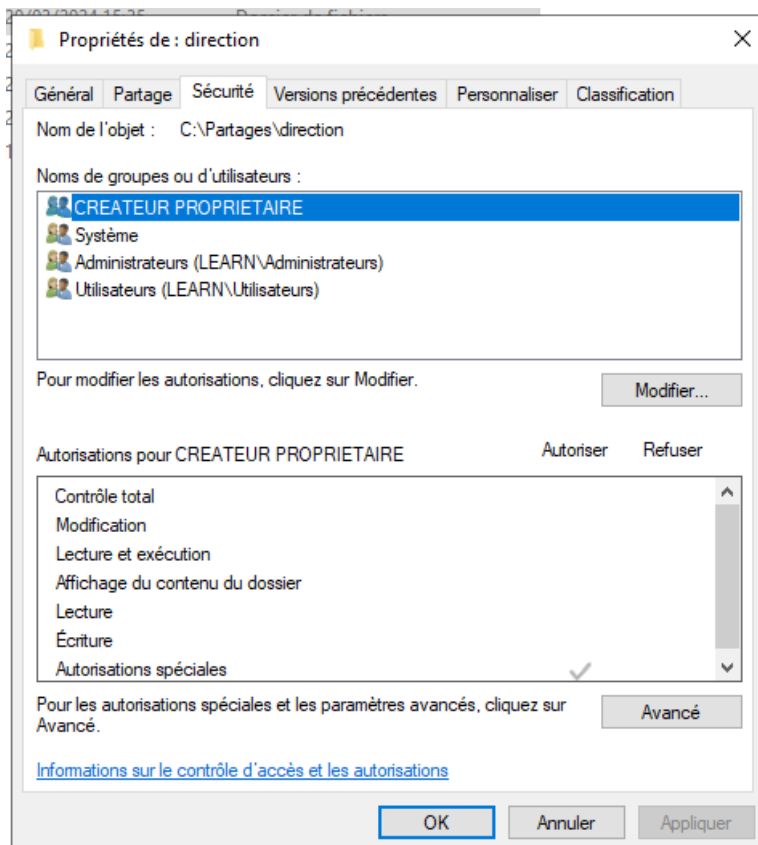


Une fois supprimé lancé dans Windows server, lancé l'observateur d'événements, et si les choses sont bien faites , un message de ce type apparait :

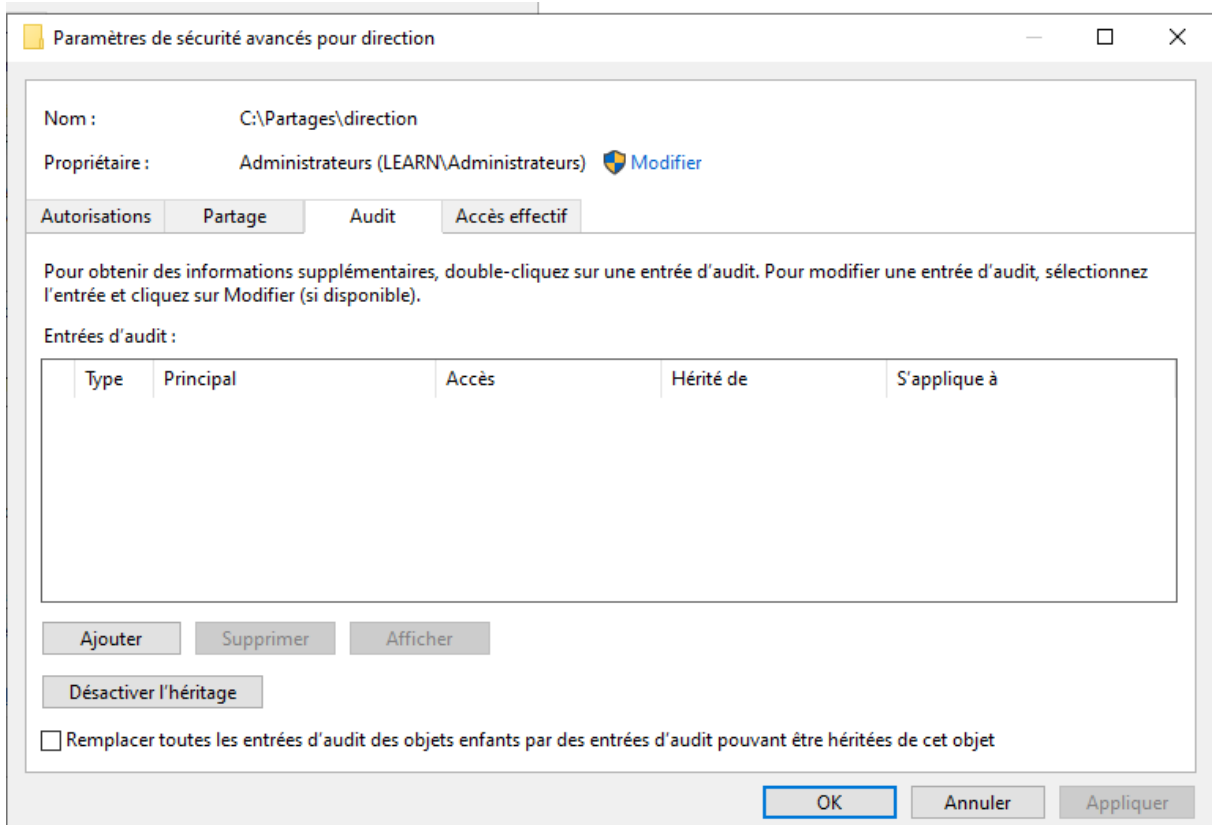


Procédure suivante :

Rendez-vous dans l'onglets sécurité du dossier Production.



Ensuite cliqué sur « Avancé » en bas. Et rendez-vous dans Audit.

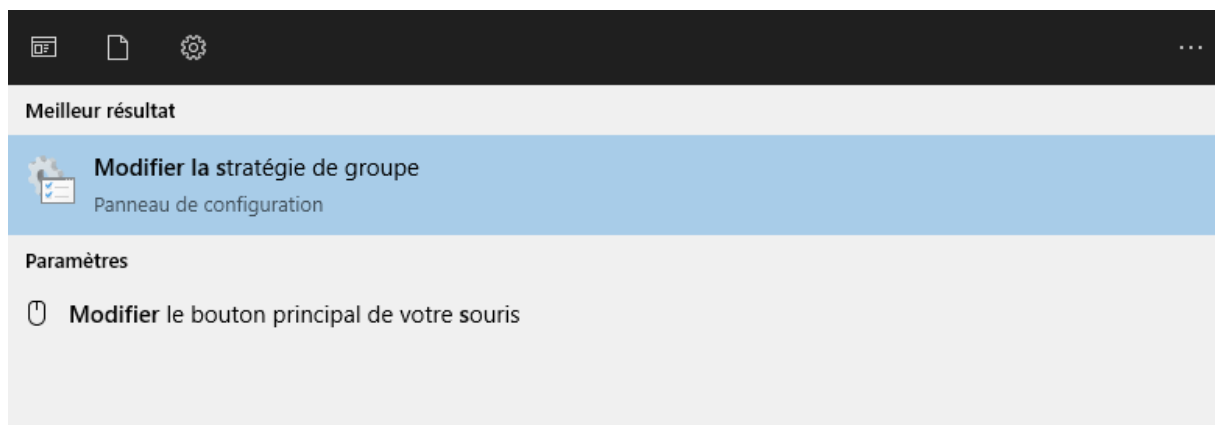


Ce qui nous ramène à cette page.

En haut de cette page sélectionner **utilisateurs du domaine**, ensuite de type « Réussite » puis donner les autorisations nécessaires. Cliquez ensuite sur *Afficher les autorisations avancées*. Et cochez la case « *approbations et autorisations de lecture* » et cliquez ensuite sur ok.

- ☐ Attributs d'écriture
- ☐ Écriture d'attributs étendus
- ☐ Suppression de sous-dossier et fichier
- ☐ Suppression
- ☐ Autorisations de lecture
- ☐ Modifier les autorisations
- ☒ Appropriation

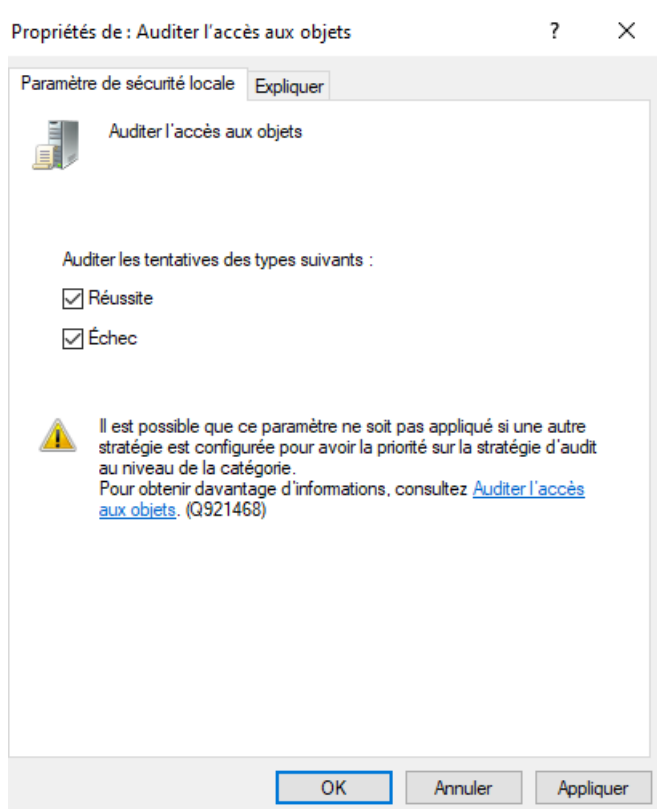
Ensuite rendez-vous dans le bureau et tapez dans la barre de recherche : *Modifier la stratégie de groupe*.



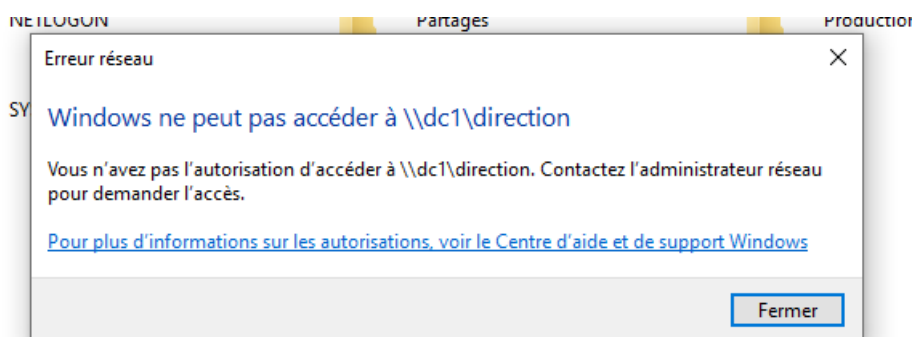
Une fois dedans cliquez sur *paramètre Windows* -> *paramètre de sécurité* -> *configuration avancée de la stratégie de l'audit* -> *Stratégie d'audit système* puis *accès à l'objet*. Ensuite cliquez sur *auditer le système de fichiers*.

Stratégie	Paramètre de sécurité
Auditer l'accès au service d'annuaire	Pas d'audit
Auditer l'accès aux objets	Pas d'audit
Auditer l'utilisation des privilèges	Pas d'audit
Auditer la gestion des comptes	Pas d'audit
Auditer le suivi des processus	Pas d'audit
Auditer les événements de connexion	Pas d'audit
Auditer les événements de connexion aux comptes	Pas d'audit
Auditer les événements système	Pas d'audit
Auditer les modifications de stratégie	Pas d'audit

Puis cochez la case *configurer les événements d'audits suivants* puis *succès et échec*. Et validez



Maintenant, du côté client essayer d'accéder au dossier direction,



Une fois cette étape faites lancer dans Windows server l'*observateurs d'événements* de commande l'onglet *paramètre Windows* puis *sécurité*.

Puis l'évènements 5145.



