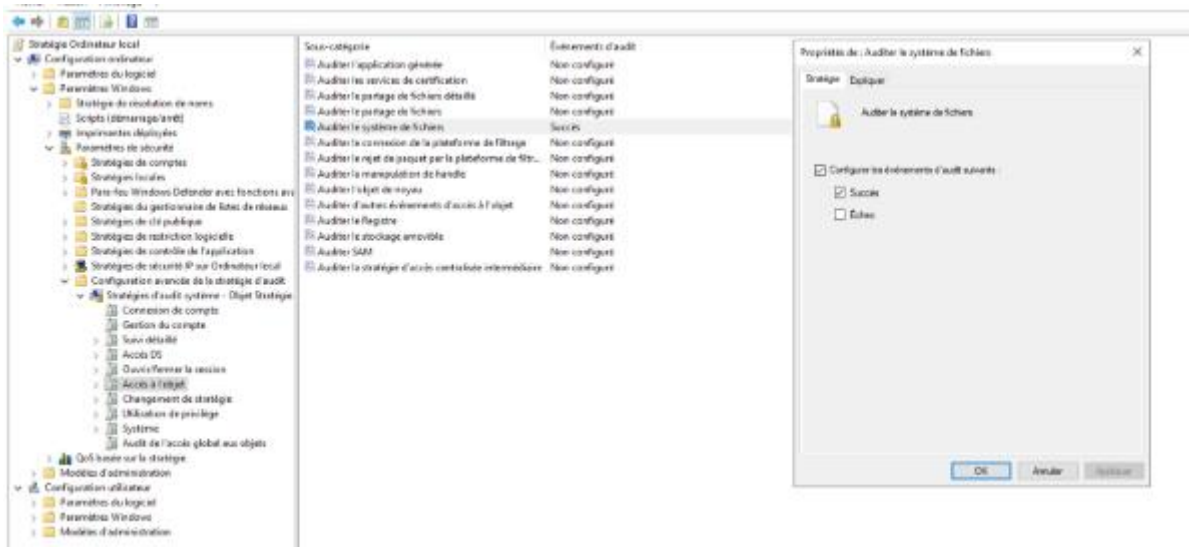
VITAL Louis

Audit des serveurs Windows (système de fichiers)

Pour activer l'audit du système de fichiers sur un serveur Windows, suivez ces étapes :

1. Ouvrez les stratégies de groupes locales et naviguez jusqu'à « Configuration Ordinateur/Paramètres Windows/Paramètres de sécurité/Configuration avancée de la stratégie d'audit/Accès à l'objet/Auditer le système de fichiers ».

2. Cochez la case « Configurer les événements d'audit suivants » et sélectionnez « Succès ».



Pour configurer l'audit sur un fichier spécifique :

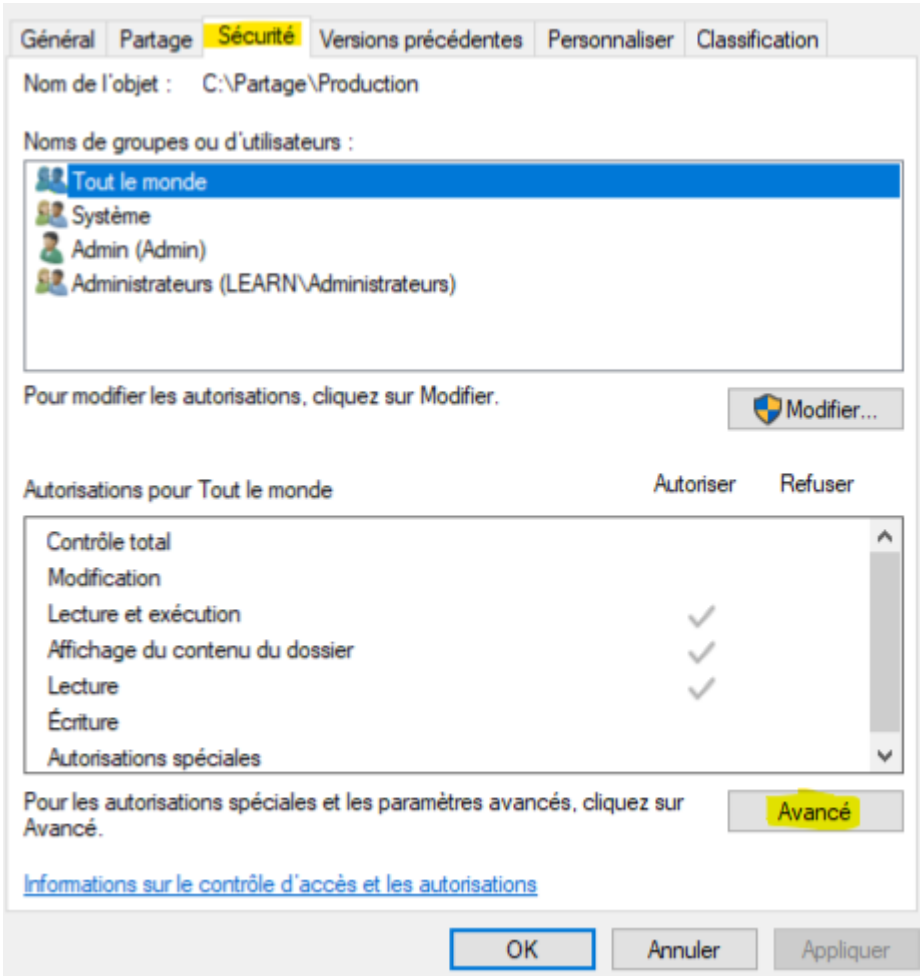
1. Ouvrez les propriétés du dossier contenant le fichier.

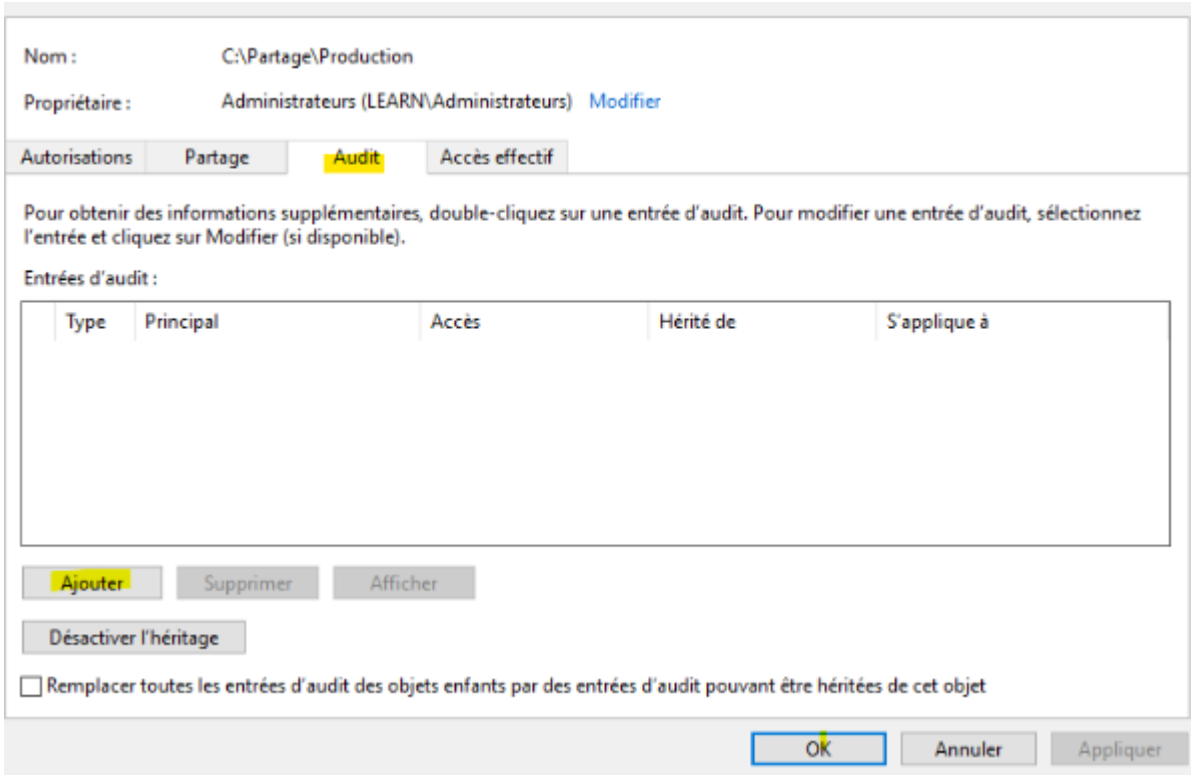
2. Accédez aux paramètres de sécurité avancés et allez à l'onglet « Audit ».

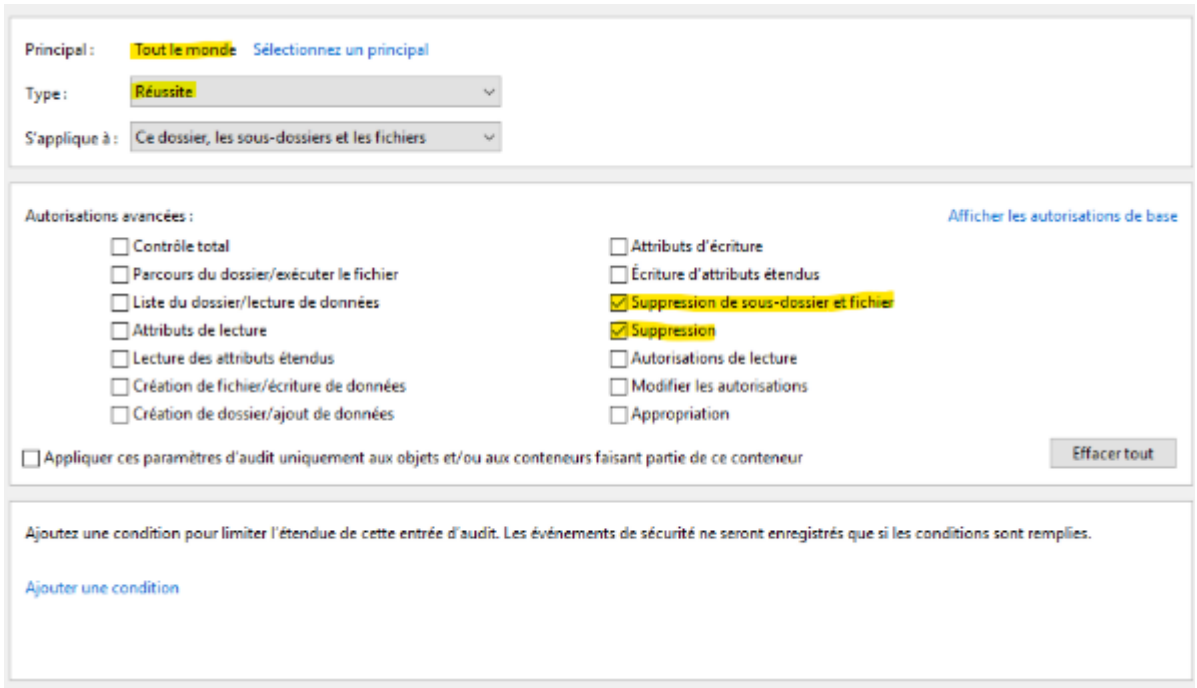
3. Cliquez sur « Ajouter » pour créer une nouvelle règle d'audit.

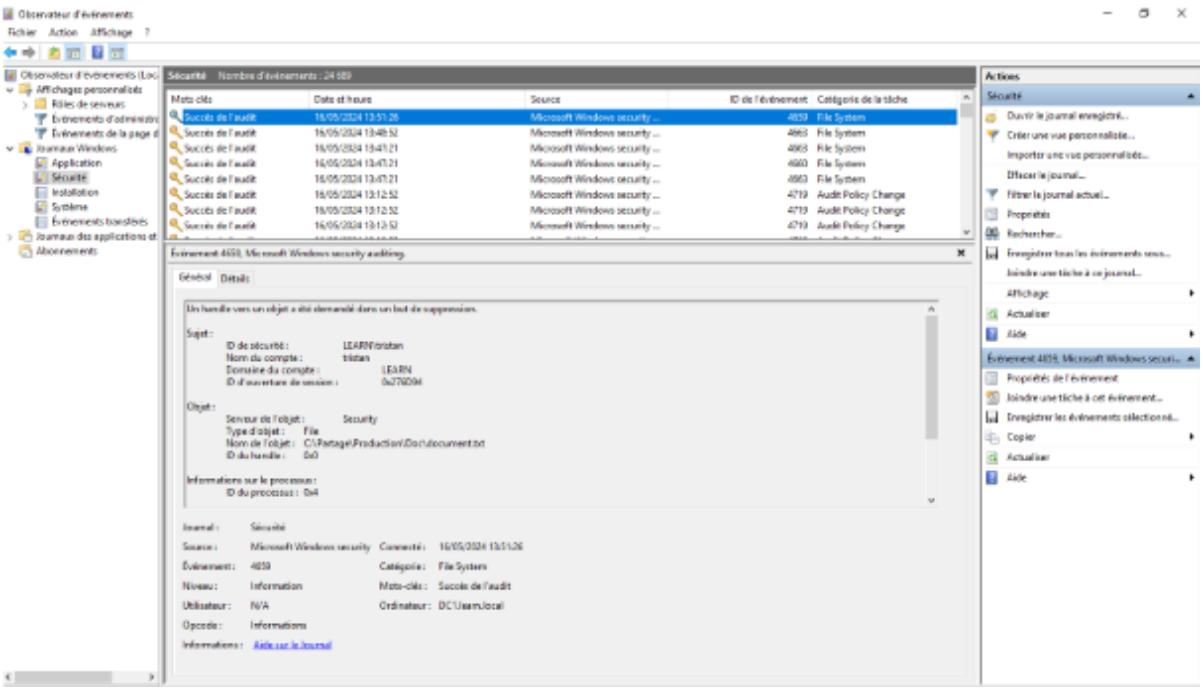
4. Définissez le principal à « Tout le monde » et cochez les options « Supprimer » et « Supprimer les sous-dossiers et les fichiers ».

5. Testez cette configuration en supprimant le fichier « document.txt » depuis un poste client. Vous devriez voir un message d'audit correspondant.




Nom : C:\Partage\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


Principal : Tout le monde Sélectionnez un principal
Type : Réussite
S'applique à : Ce dossier, les sous-dossiers et les fichiers
Autorisations avancées :
Afficher les autorisations de base
Contrôle total
Parcours du dossier/exécuter le fichier
Liste du dossier/lecture de données
Attributs de lecture
Lecture des attributs étendus
Création de fichier/écriture de données
Création de dossier/ajout de données
Attributs d'écriture
Écriture d'attributs étendus
Suppression de sous-dossier et fichier
Suppression
Autorisations de lecture
Modifier les autorisations
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



Pour créer une règle d'audit excluant certains utilisateurs :

1. Créez une nouvelle règle d'audit en excluant les utilisateurs « directeur » et « technicien informatique ».

2. Appliquez cette règle au dossier « direction ».

3. En tentant d'accéder au dossier « Direction », un message approprié devrait apparaître dans le journal d’événements.