

# Audit d'un fichier d'accès





# Sommaire

<b>Introduction</b> .....	3
<b>Configuration d'audit d'un fichier d'accès</b> .....	3
<b>Test de l'Audit</b> .....	7
<b>Audit d'autorisation d'accès à un dossier</b> .....	8
<b>Test de l'Audit</b> .....	10
<b>Audit de l'Active Directory</b> .....	12
<b>Test de l'Audit</b> .....	13
<b>Test de l'Audit pour le mot de passe</b> .....	14
<b>Conclusion</b> .....	14

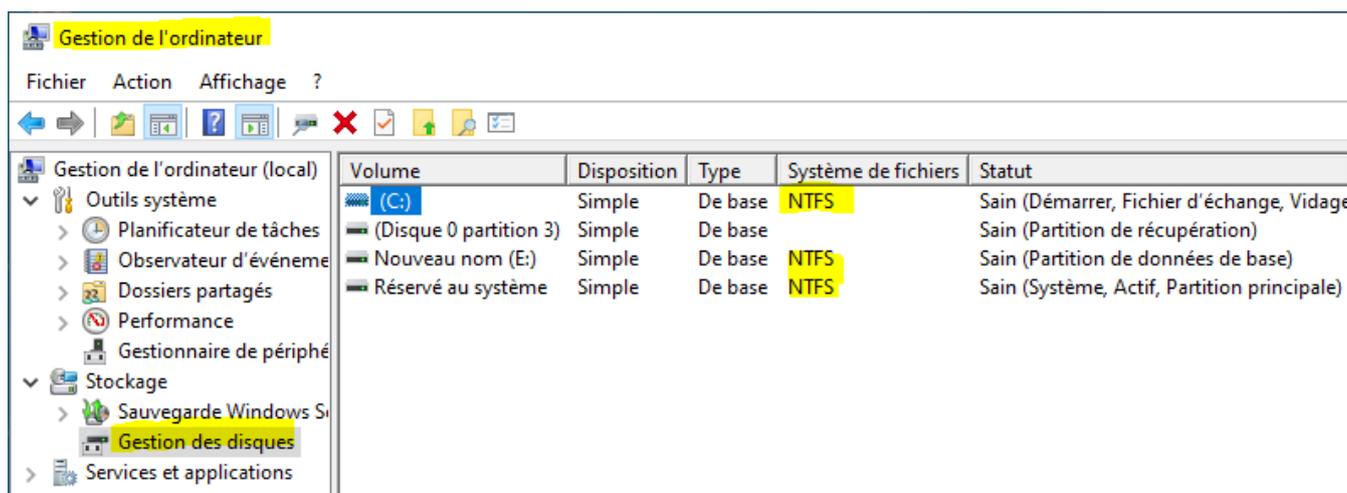
## Introduction

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.

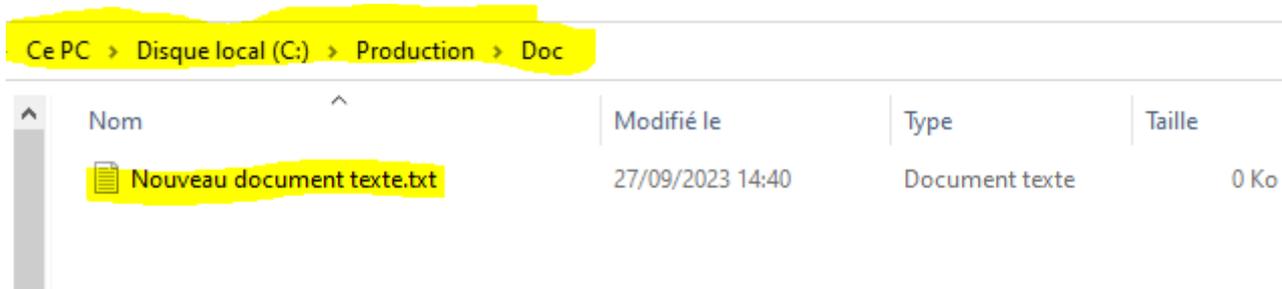
## Configuration d'audit d'un fichier d'accès

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

→ Gestion de l'ordinateur → gestion des disques

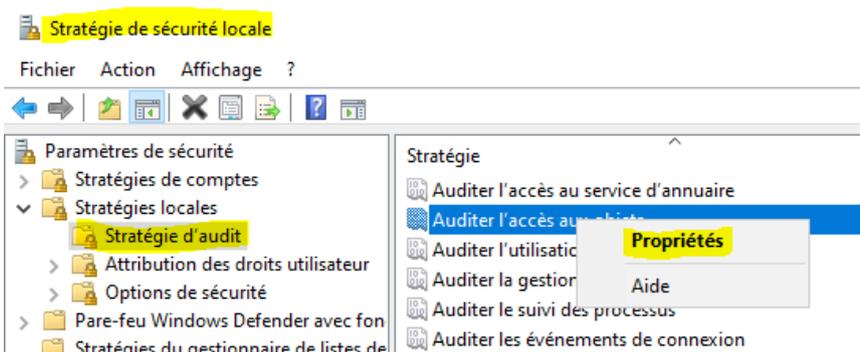


On crée ensuite notre document dans le sous dossier (Doc) du dossier Production

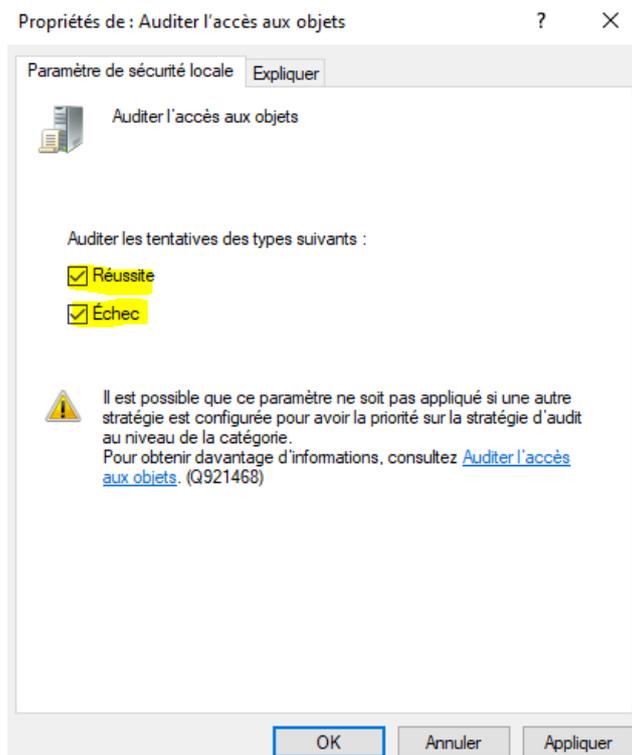


On autorise les audits sur notre serveur.

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

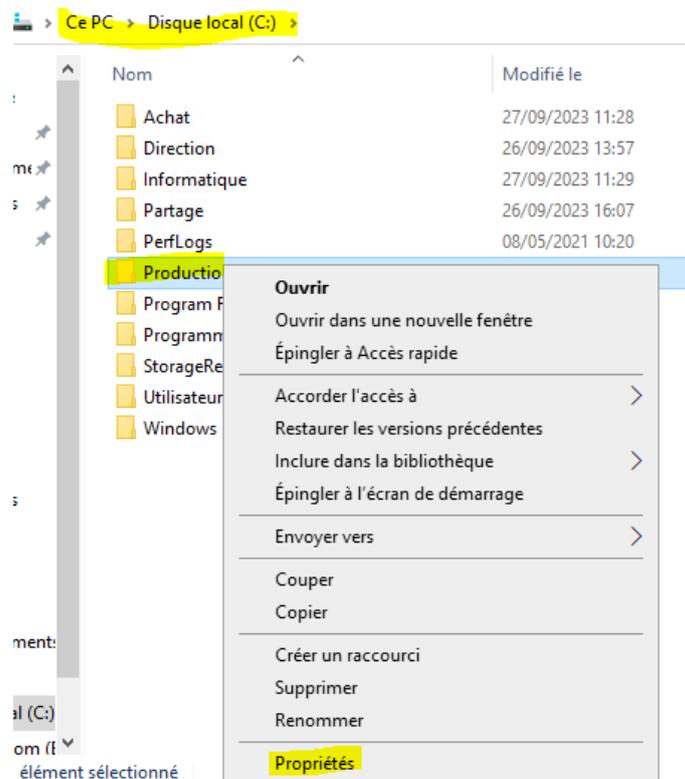


Activer l'audite sur les tentatives en Réussite et en Echec.

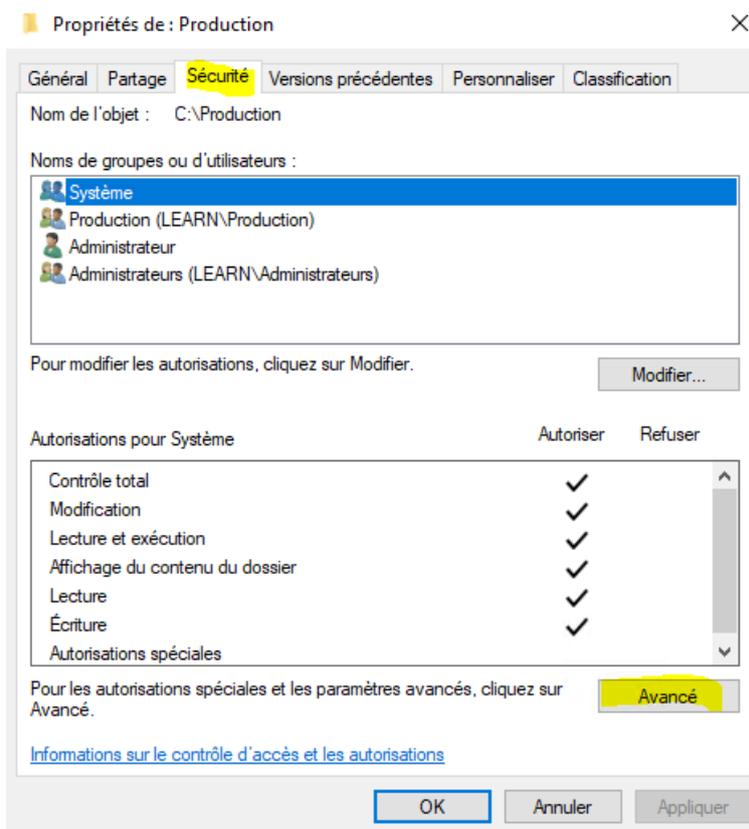


On autorise l'Audit créer sur le dossier Production.

➔ Clic droit sur le dossier Production ➔ Propriétés

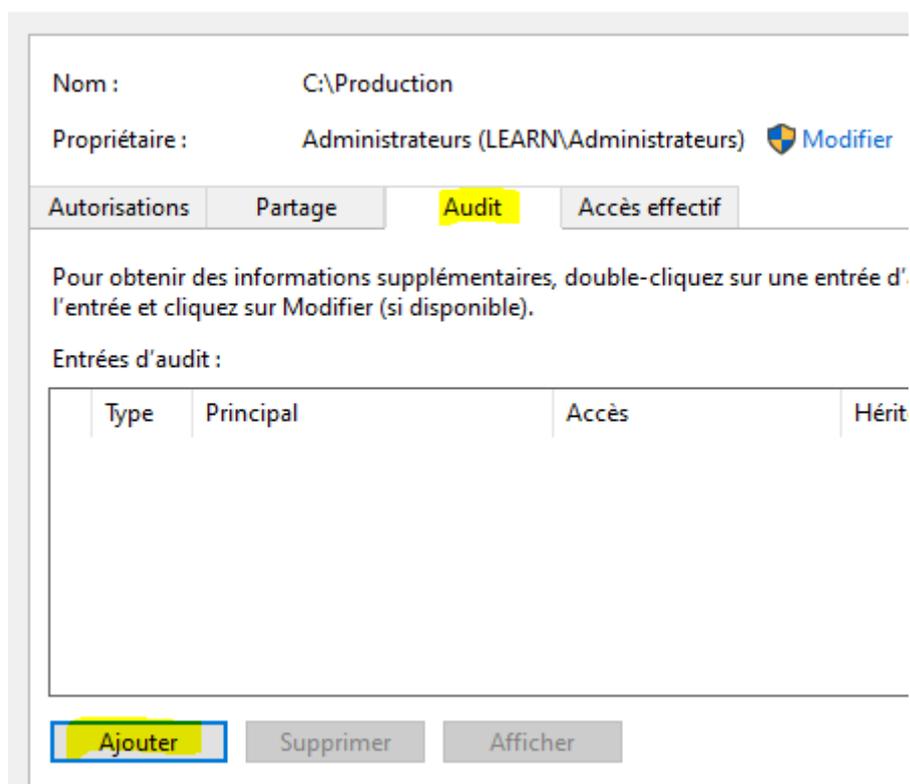


## → Sécurité → Avancé



## → Audit → Ajouter

### Paramètres de sécurité avancés pour Production



On ajoute tout le monde dans l'Audit.

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

**Audits pour Production**

Principal : **Sélectionnez un principal**

Type : Réussite

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

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

À partir de cet emplacement :

leam.local

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

**Tout le monde**

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

Avancé... OK Annuler

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

**Audits pour Production**

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](#)

<input type="checkbox"/> Contrôle total	<input type="checkbox"/> Attributs d'écriture
<input checked="" 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"/> <b>Suppression de sous-dossier et fichier</b>
<input checked="" type="checkbox"/> Attributs de lecture	<input checked="" type="checkbox"/> <b>Suppression</b>
<input checked="" type="checkbox"/> Lecture des attributs étendus	<input checked="" 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

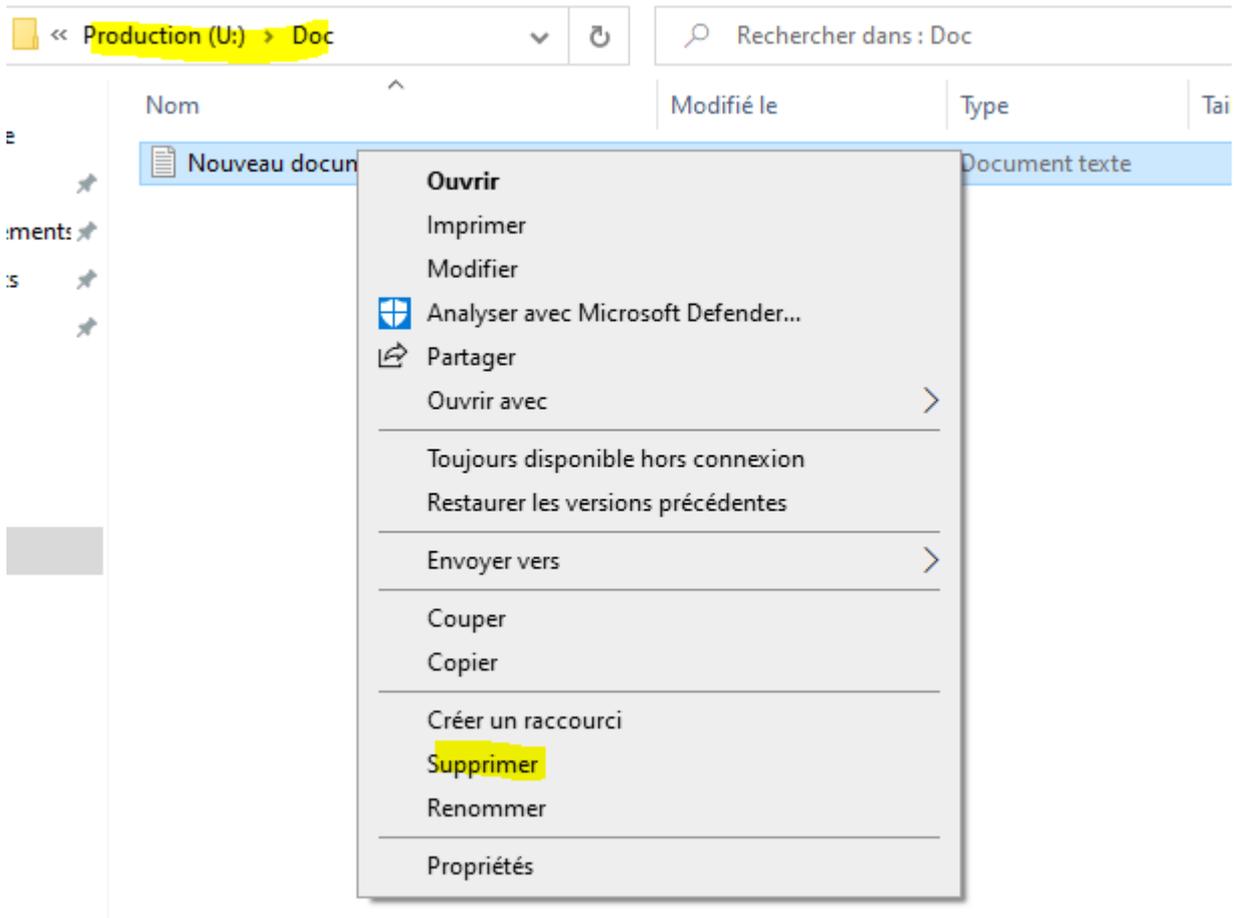
Appliquer ces paramètres d'audit uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

Effacer tout

## 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



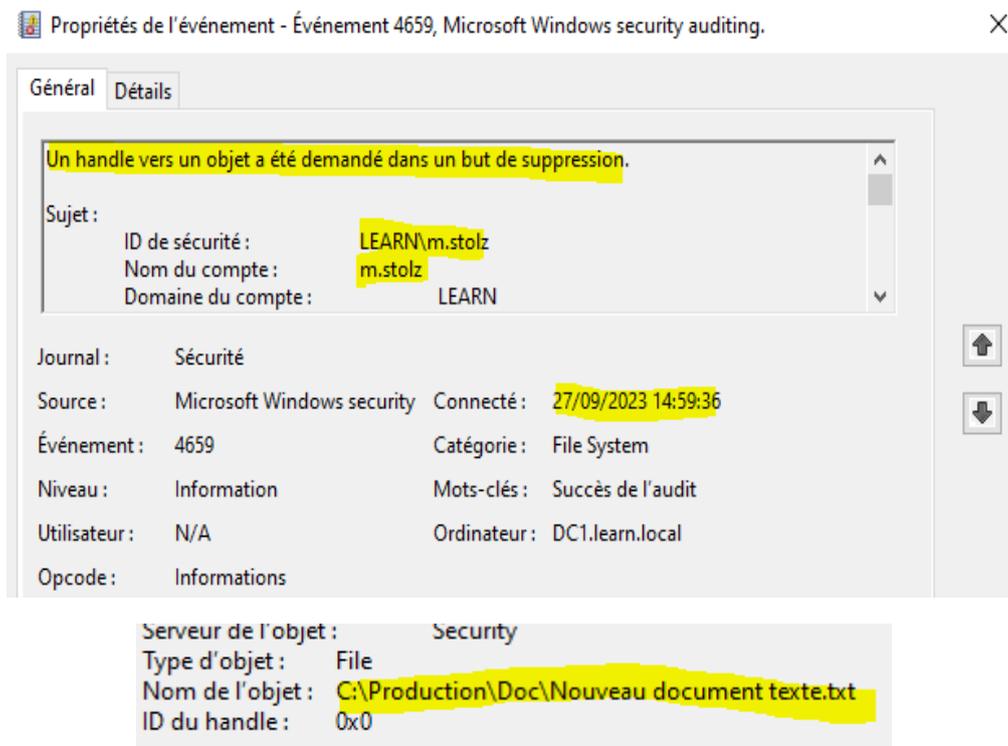
On retourne sur le serveur.

→ Observateur d'événements → Journaux Windows → Sécurité

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

Succès de l'audit	27/09/2023 14:59:36	Microsoft Windows securi...	4659	File System
-------------------	---------------------	-----------------------------	------	-------------

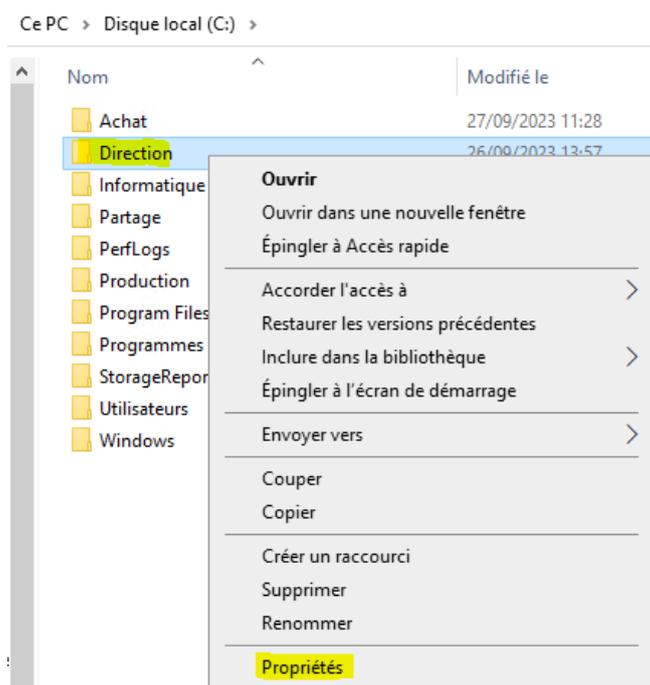
On peut voir l'alerte d'Audit qui nous permet de voir l'utilisateur et quand le document a été supprimer.



## Audit d'autorisation d'accès à un dossier

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

→ Direction → Clic droit → Propriété



→ On clique Sélectionnez un principal

**Audits pour Direction**

Principal : **Sélectionnez un principal**

Type : Réussite

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

**Autorisations de base :**

- 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

→ On ajoute les groupes Production et Achat en échec.

**Paramètres de sécurité avancés pour Direction**

Nom : C:\Direction

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
Échec	Production (LEARN\Producti...	Parcours du dossier/ex...	Aucun	Ce dossier, les sous-dossiers et...
Échec	Achat (LEARN\Achat)	Parcours du dossier/ex...	Aucun	Ce dossier, les sous-dossiers et...

Ajouter | Supprimer | Modifier

→ On coche Parcours du dossier/exécuter le fichier

**Audits pour Direction**

Principal : Tout le monde [Sélectionnez un principal](#)

Type : **Échec**

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

Autorisations avancées :

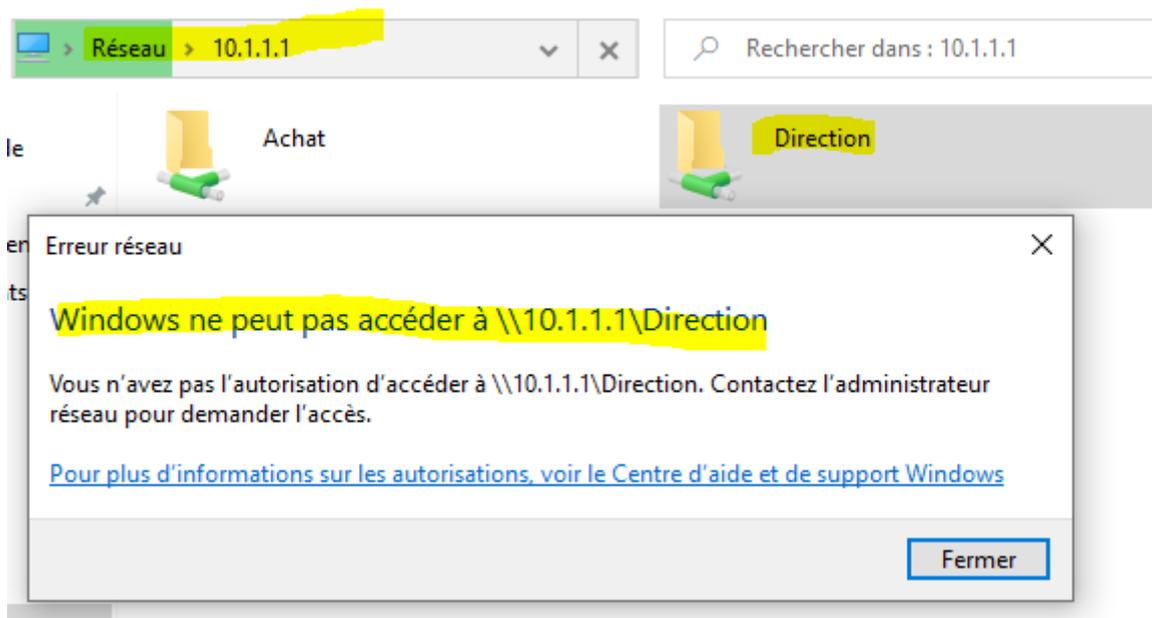
<input type="checkbox"/> Contrôle total	<input type="checkbox"/> Attributs d'écriture
<input checked="" type="checkbox"/> <b>Parcours du dossier/exécuter le fichier</b>	<input type="checkbox"/> Écriture d'attributs étendus
<input type="checkbox"/> Liste du dossier/lecture de données	<input type="checkbox"/> Suppression de sous-dossier et fichier
<input type="checkbox"/> Attributs de lecture	<input type="checkbox"/> Suppression
<input 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

## Test de l'Audit

On se connecte avec un utilisateur du groupe Production ou Achat

→ On tape [\\10.1.1.1](http://10.1.1.1) → On clique sur le dossier Direction



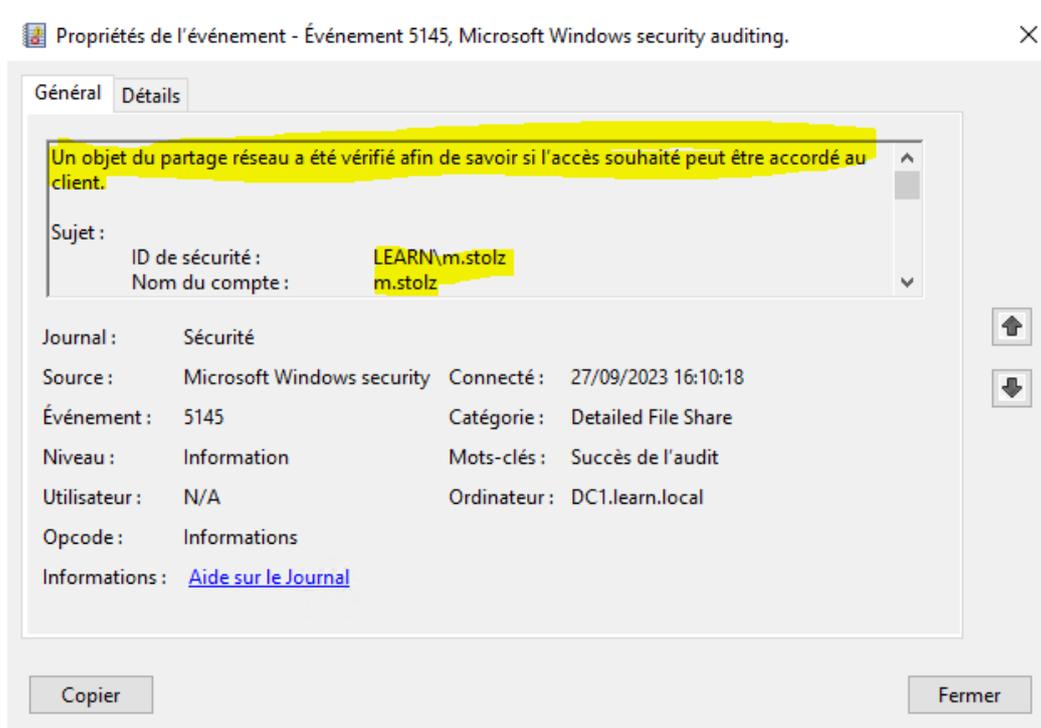
On retourne sur le serveur.

→ 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.

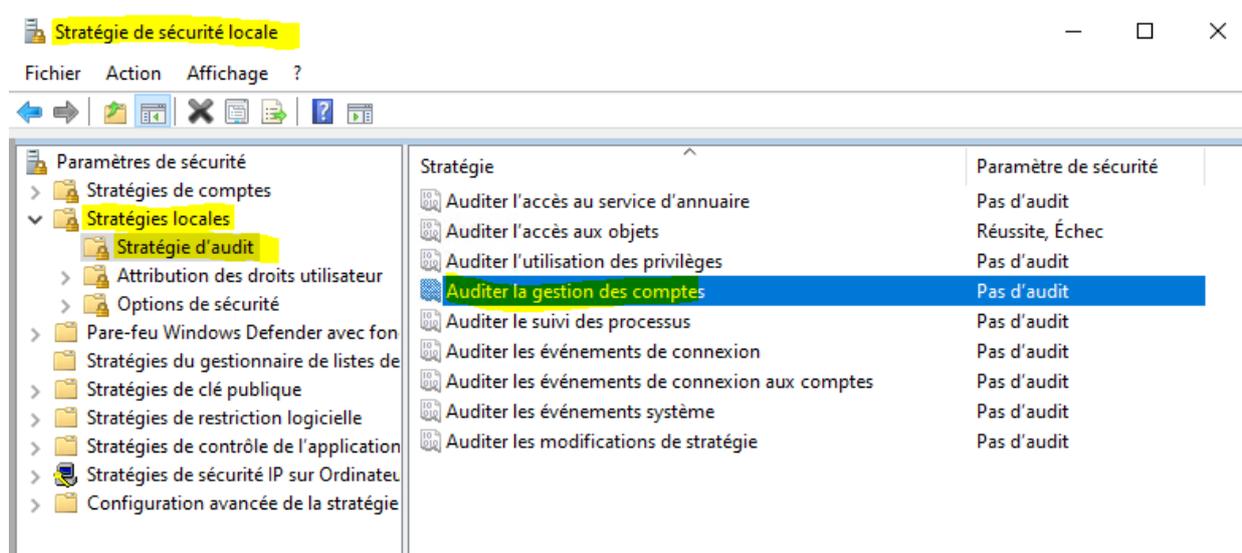
Succès de l'audit      27/09/2023 16:10:18      Microsoft Windows securi...      5145 Detailed File Share



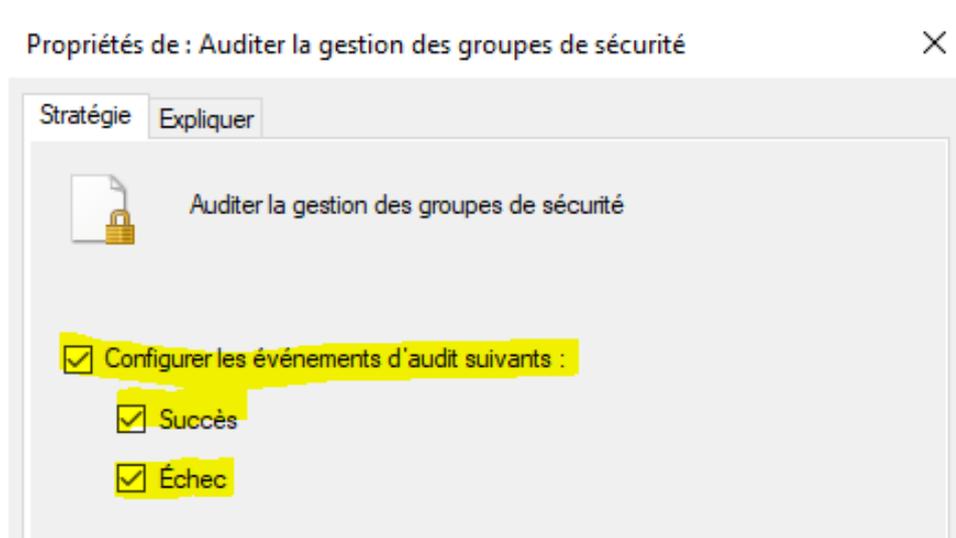
## Audit de l'Active Directory

Cette Audit va nous permettre d'être notifié 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.

Nouvel objet - Utilisateur

Créer dans : leam.local/

Prénom : salut      Initiales :

Nom : salut

Nom complet : salut salut

Nom d'ouverture de session de l'utilisateur :  
 @leam.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent    Suivant >    Annuler

On vérifie les logs.

→ Observateur d'événements → Journaux Windows → Sécurité  
 On voit « Succès de l'audit » 4720, on clique dessus pour voir le contenu.

Succès de l'audit    27/09/2023 17:28:14    Microsoft Windows securi...    4720    User Account Management

Propriétés de l'événement - Événement 4720, Microsoft Windows security auditing.

Général    Détails

Un compte d'utilisateur a été créé.

Sujet :  
 ID de sécurité : LEARN\Administrateur  
 Nom du compte : Administrateur  
 Domaine du compte : LEARN

Journal : Sécurité

Source : Microsoft Windows security    Connecté : 27/09/2023 17:28:14

Événement : 4720    Catégorie : User Account Management

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

Utilisateur : N/A    Ordinateur : DC1.leam.local

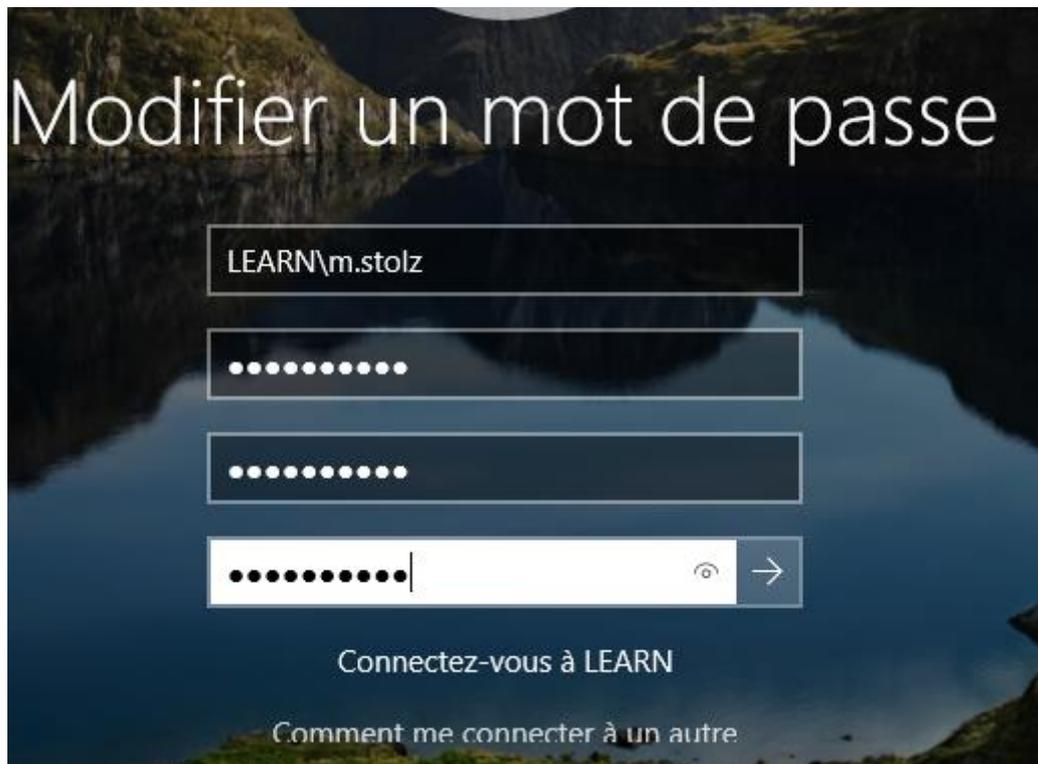
Opcode : Informations

Informations : [Aide sur le Journal](#)

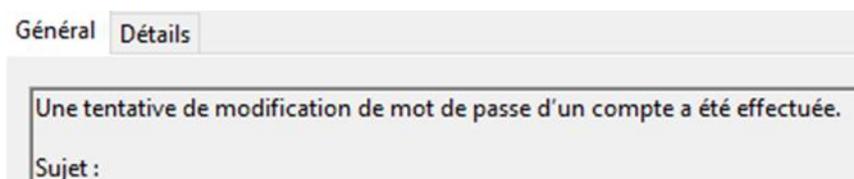
Copier    Fermer

## 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.

