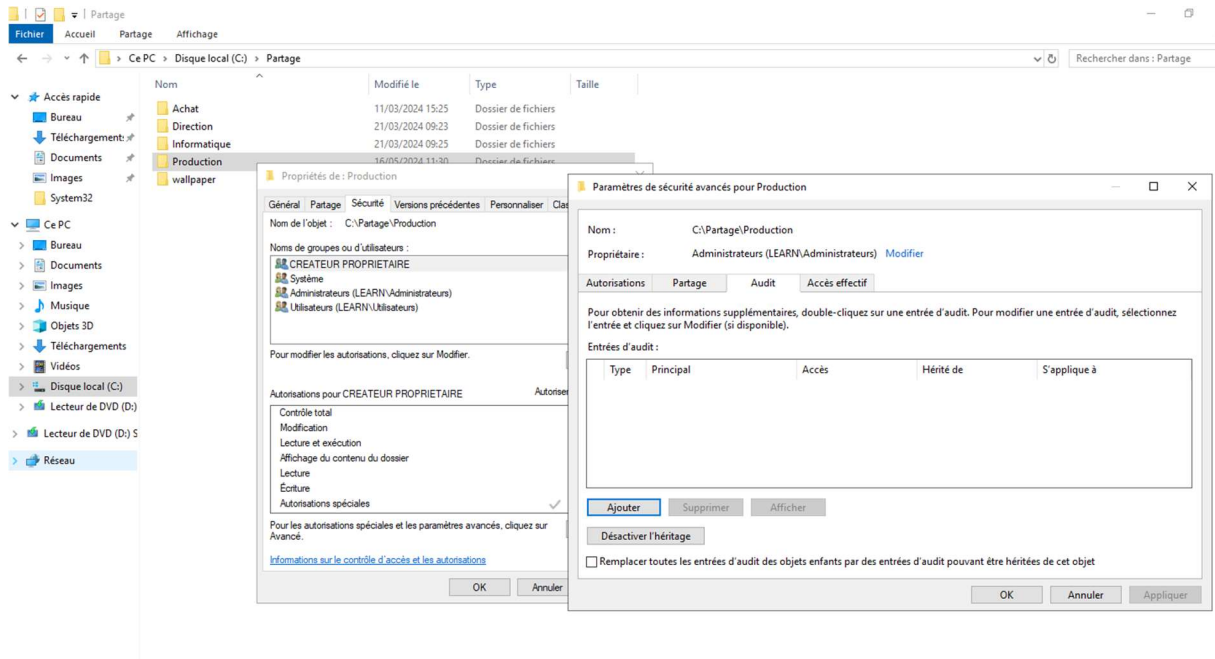


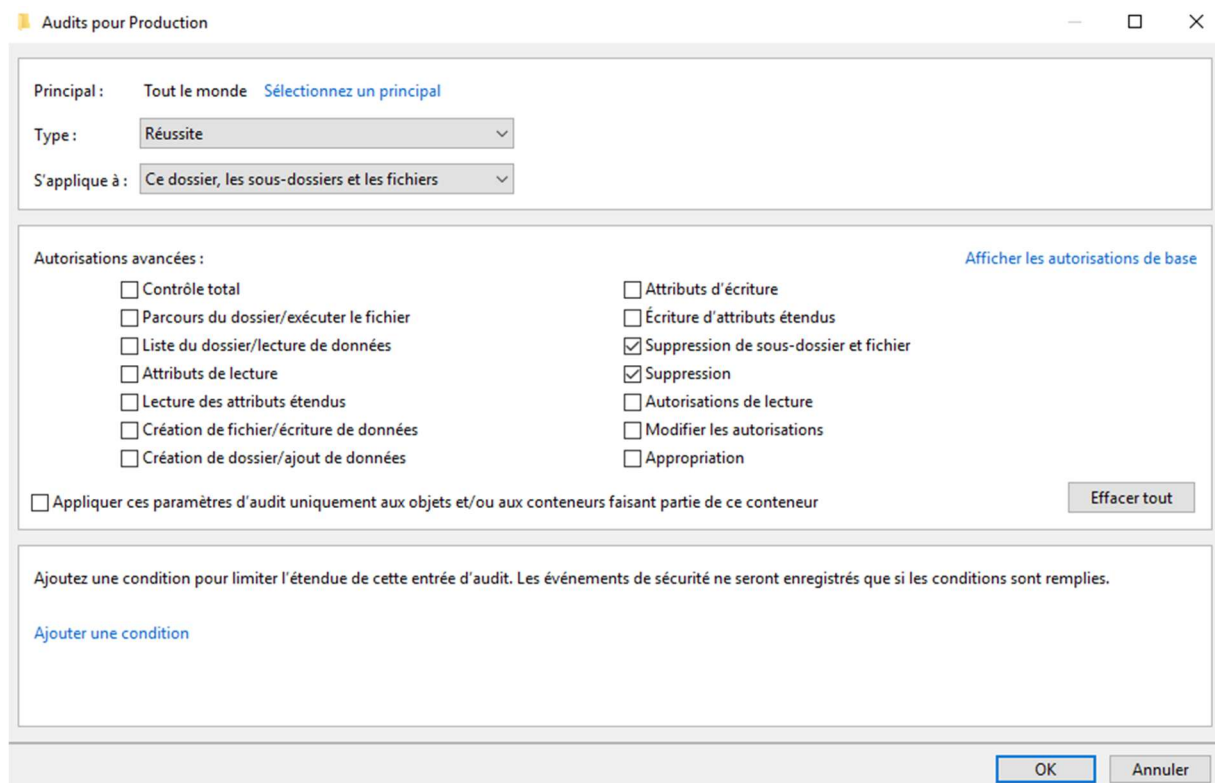
# Procédure : Audit suppression de fichier

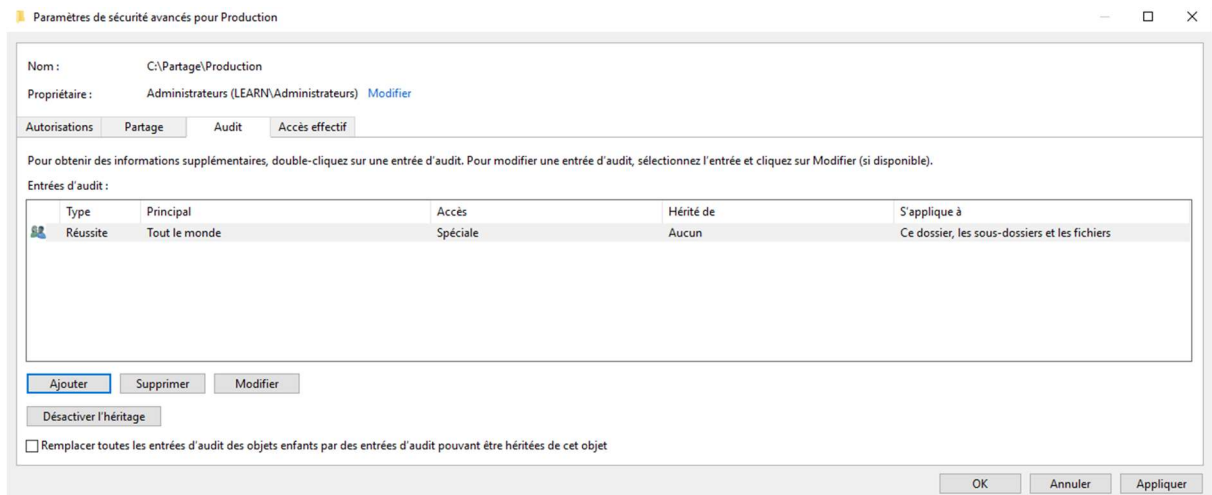
Étape 1 :

Appliquer les paramètres voulu de son audit sur le dossier de son choix.

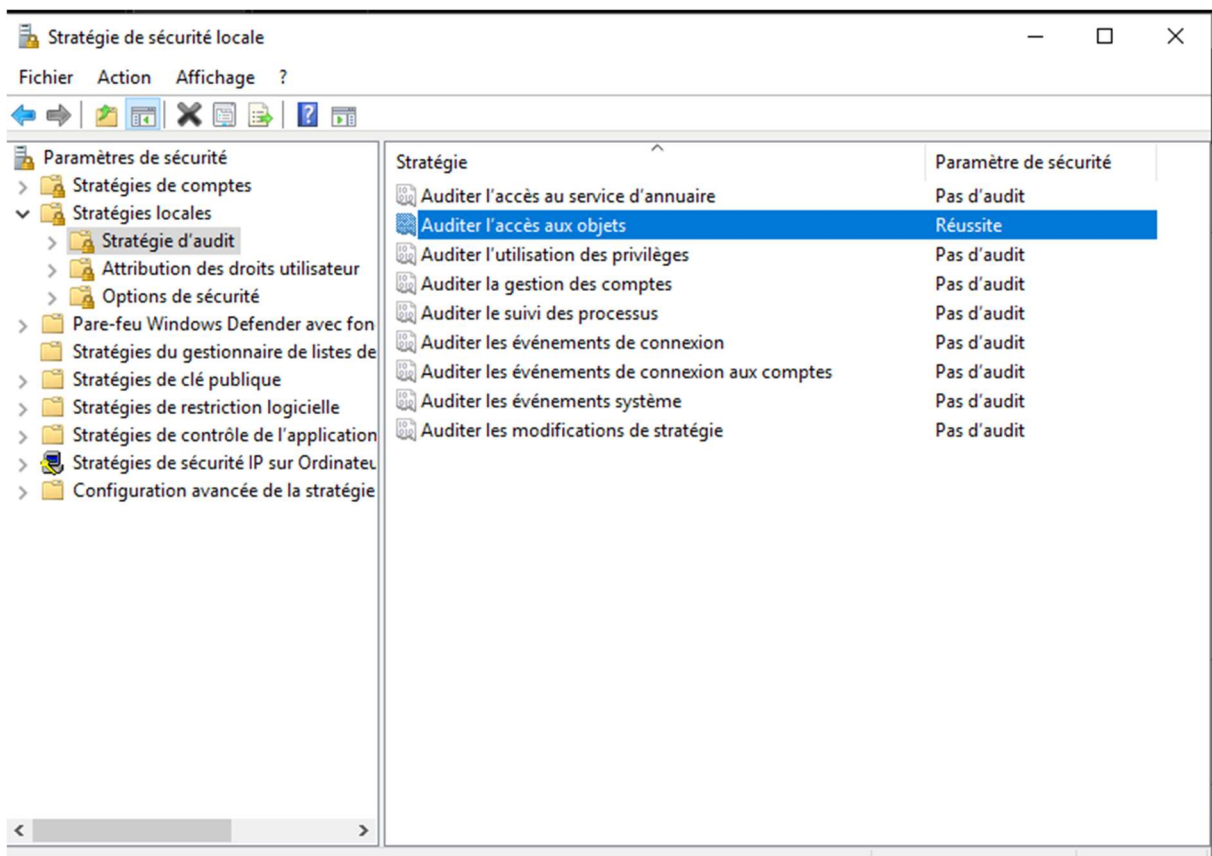


On choisit les paramètres que l'on veut.

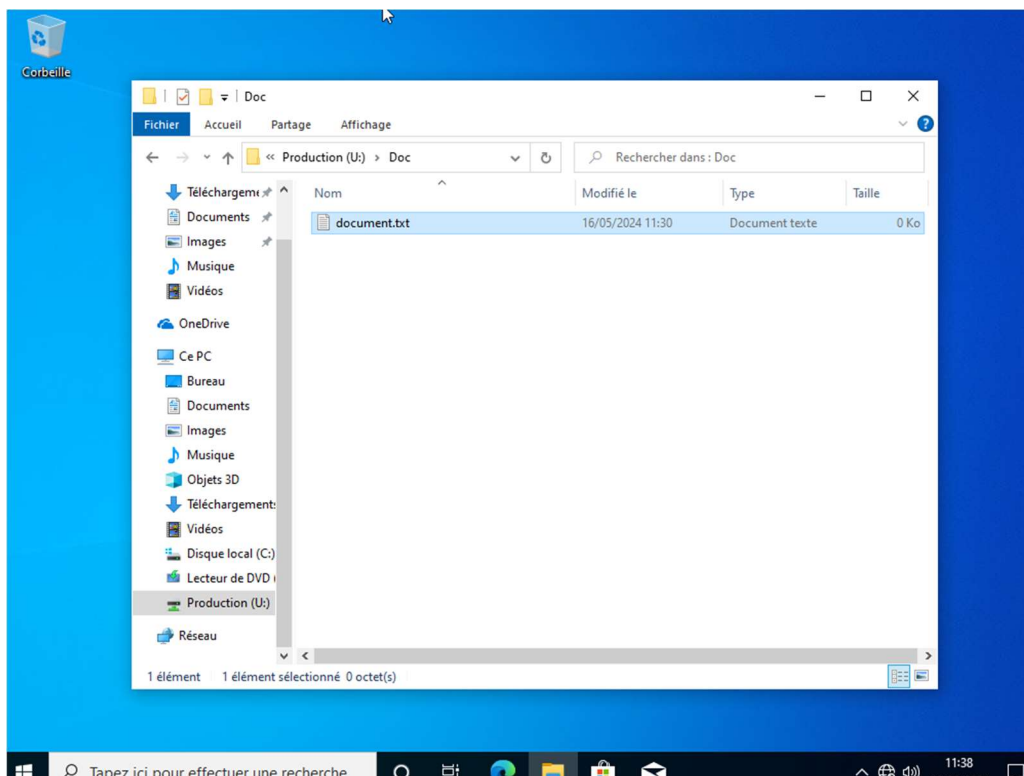




Étape 2 : Activer l'audit dans la stratégie de sécurité locale sur son serveur.

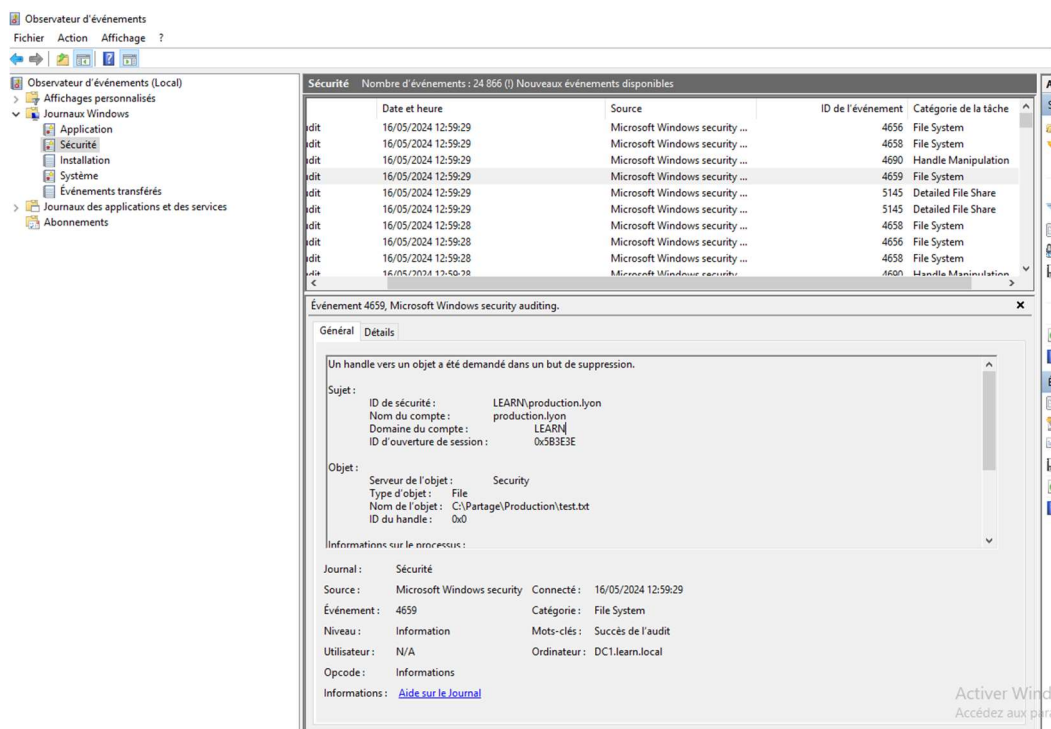


Étape 3 : Créer un fichier test sur son serveur puis le supprimer sur son client.



Étape 4 :

Regarder sur son serveur, dans l'observateur d'événements que l'alerte remonte bien.



Partage

Accueil Partage Affichage

Ce PC > Disque local (C:) > Partage

Nom Modifié le Type

Achat 11/03/2024 15:25 Dos

Direction 21/03/2024 09:23 Dos

Informatique 21/03/2024 09:25 Dos

Production 16/05/2024 12:59 Dos

wallpaper 11/03/2024 17:29 Dos

Propriétés de : Direction

Général Partage Sécurité Versions précédentes Personnaliser Classification

Nom de l'objet : C:\Partage\Direction

Noms de groupes ou d'utilisateurs :

- CREATEUR PROPRIETAIRE
- Système
- Administrateurs (LEARN\Administrateurs)
- Utilisateurs (LEARN\Utilisateurs)

Pour modifier les autorisations, cliquez sur Modifier.

Modifier...

Autorisations pour CREATEUR PROPRIETAIRE

Autoriser Refuser

Contrôle total

Modification

Lecture et exécution

Affichage du contenu du dossier

Lecture

Écriture

Autorisations spéciales

Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.

Informations sur le contrôle d'accès et les autorisations

OK Annuler Appliquer

Paramètres de sécurité avancés pour Direction

Nom : C:\Partage\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
Tout	achat lyon (achat.lyon@learn....	Spéciale	Aucun	Ce dossier seulement

Audits pour Direction

Principal : achat lyon (achat.lyon@learn.local) Sélectionnez un principal

Type : Tout

S'applique à : Ce dossier seulement

Autorisations avancées :

☐ 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

☐ Afficher les autorisations de base

☐ 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

Activer Windows

Accédez aux paramètres pour activer Windows.

OK Annuler

Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local)

Affichages personnalisés

Journaux Windows

- Application
- Sécurité
- Installation
- Système
- Événements transférés

Journaux des applications et des services

Abonnements

Sécurité Nombre d'événements : 25 806 (0) Nouveaux événements disponibles

Date et heure	Source	ID de l'événement	Catégorie de la tâche
16/05/2024 13:35:12	Microsoft Windows security ...	4624	Logon
16/05/2024 13:35:12	Microsoft Windows security ...	4769	Kerberos Service Ticket Oper
16/05/2024 13:35:12	Microsoft Windows security ...	5145	Detailed File Share
16/05/2024 13:35:12	Microsoft Windows security ...	5140	File Share
16/05/2024 13:35:12	Microsoft Windows security ...	4634	Logoff
16/05/2024 13:35:12	Microsoft Windows security ...	4624	Logon
16/05/2024 13:35:12	Microsoft Windows security ...	4672	Special Logon
16/05/2024 13:35:12	Microsoft Windows security ...	5145	Detailed File Share

Événement 5140, Microsoft Windows security auditing.

Général Détails

Un objet du partage réseau a fait l'objet d'un accès.

Sujet :

ID de sécurité : LEARN\achat.lyon

Nom du compte : achat.lyon

Domaine du compte : LEARN

ID d'ouverture de session : 0x87D576

Informations sur le réseau :

Type d'objet : File

Adresses source : 10.1.1.2

Port source : 50590

Informations sur le partage :

Nom du partage : \\.\Direction

Chemin d'accès du partage : \\?\C:\Partage\Direction

Journal : Sécurité

Source : Microsoft Windows security

Connecté : 16/05/2024 13:35:12

Événement : 5140

Catégorie : File Share

Niveau : Information

Mots-clés : Succès de l'audit

Utilisateur : N/A

Ordinateur : DC1.learn.local

Opcode : Informations

Informations : Aide sur le Journal

Activer Wi

Accédez aux

Observateur d'événements

Fichier Action Affichage ?



Observateur d'événements (Local)

- > Affichages personnalisés
- ▼ Journaux Windows
  - Application
  - Sécurité
  - Installation
  - Système
  - Événements transférés
- > Journaux des applications et des services
- Abonnements

Sécurité Nombre d'événements : 25 806 (0) Nouveaux événements disponibles

Date et heure	Source	ID de l'événement	Catégorie de la tâche
16/05/2024 13:35:12	Microsoft Windows security ...	4624	Logon
16/05/2024 13:35:12	Microsoft Windows security ...	4769	Kerberos Service Ticket Oper...
16/05/2024 13:35:12	Microsoft Windows security ...	5145	Detailed File Share
16/05/2024 13:35:12	Microsoft Windows security ...	5140	File Share
16/05/2024 13:35:12	Microsoft Windows security ...	4634	Logoff
16/05/2024 13:35:12	Microsoft Windows security ...	4624	Logon
16/05/2024 13:35:12	Microsoft Windows security ...	4672	Special Logon
16/05/2024 13:35:08	Microsoft Windows security ...	5145	Detailed File Share

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 : LEARN\achat.lyon  
 Nom du compte : achat.lyon  
 Domaine du compte : LEARN  
 ID d'ouverture de session : 0x87D576

Informations sur le réseau :

Type d'objet : File  
 Adresse source : 10.1.1.2  
 Port source : 50588

Informations de partage :

Nom de partage : \\.\IPC\$  
 Chemin d'accès du partage :  
 Nom cible relatif : srvsvc

Journal : Sécurité

Source : Microsoft Windows security Connecté : 16/05/2024 13:35:12

Événement : 5145 Catégorie : Detailed File Share

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

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

Opcode : Informations

Informations : [Aide sur le Journal](#)

Activer W  
Accédez aux