

Henry Astafieff

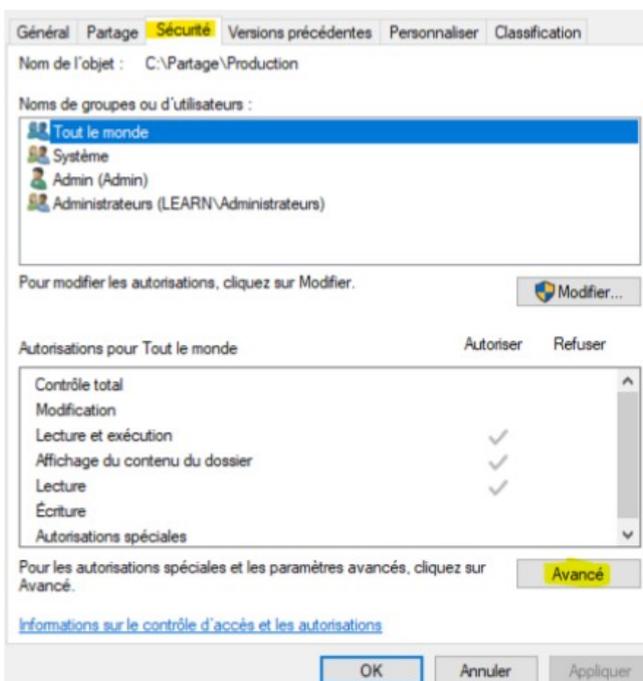
Audit des serveurs windows

Suivre les étapes suivantes :

1. Ouvrez les stratégies de groupes locales, configuration ordinateur, paramètres windows, paramètres de sécurité, configuration avancée de la stratégie d'audit, accès à l'objet puis auditer le système de fichiers .
2. Cochez : Configurer les événements d'audit suivants et sélectionnez « Succès »

Configurer l'audit sur un fichier spécifique :

1. Ouvrez les propriétés du dossier avec le fichier
2. Allez paramètres de sécurité avancés et allez à l'onglet « Audit ».
3. Ajouter pour créer une nouvelle règle.
4. Définissez le principal à « Tout le monde » et cochez « Supprimer » et « Supprimer les sous-dossiers et les fichiers ».
5. Testez en supprimant le fichier « document.txt » depuis un poste client. Un message d'audit correspondant devrait apparaître.



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

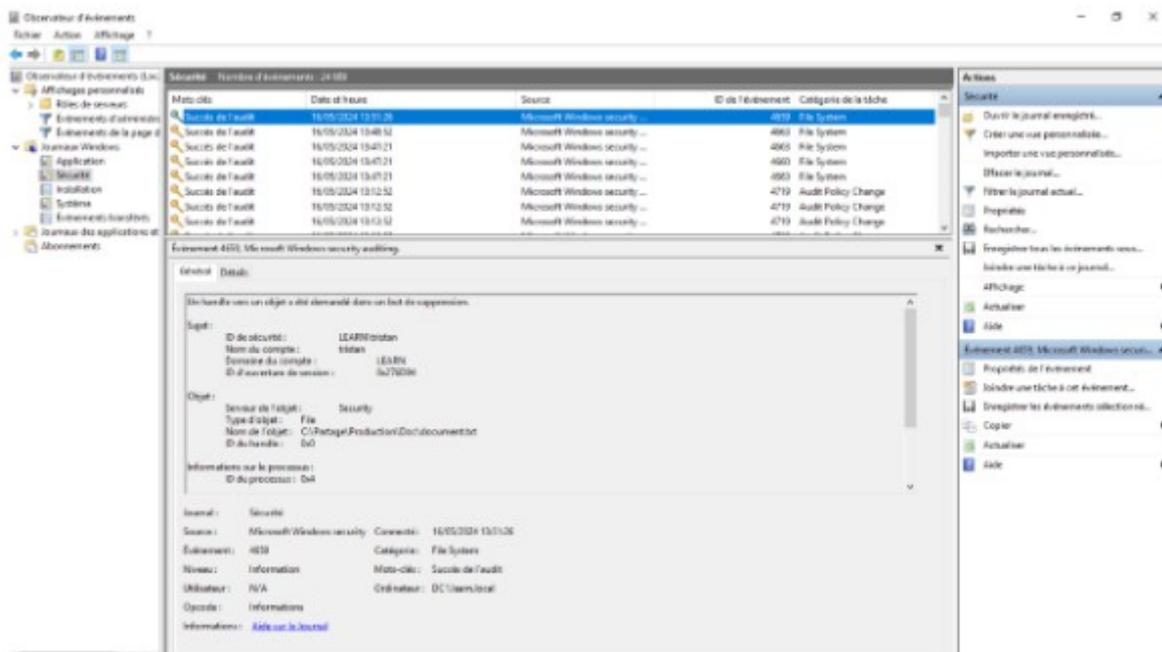
Autorisations avancées : [Afficher les autorisations de base](#)

<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 type="checkbox"/> Liste du dossier/lecture de données	<input checked="" type="checkbox"/> <b>Suppression de sous-dossier et fichier</b>
<input type="checkbox"/> Attributs de lecture	<input checked="" type="checkbox"/> <b>Suppression</b>
<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 **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 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 doit apparaître dans le journal d'événements.