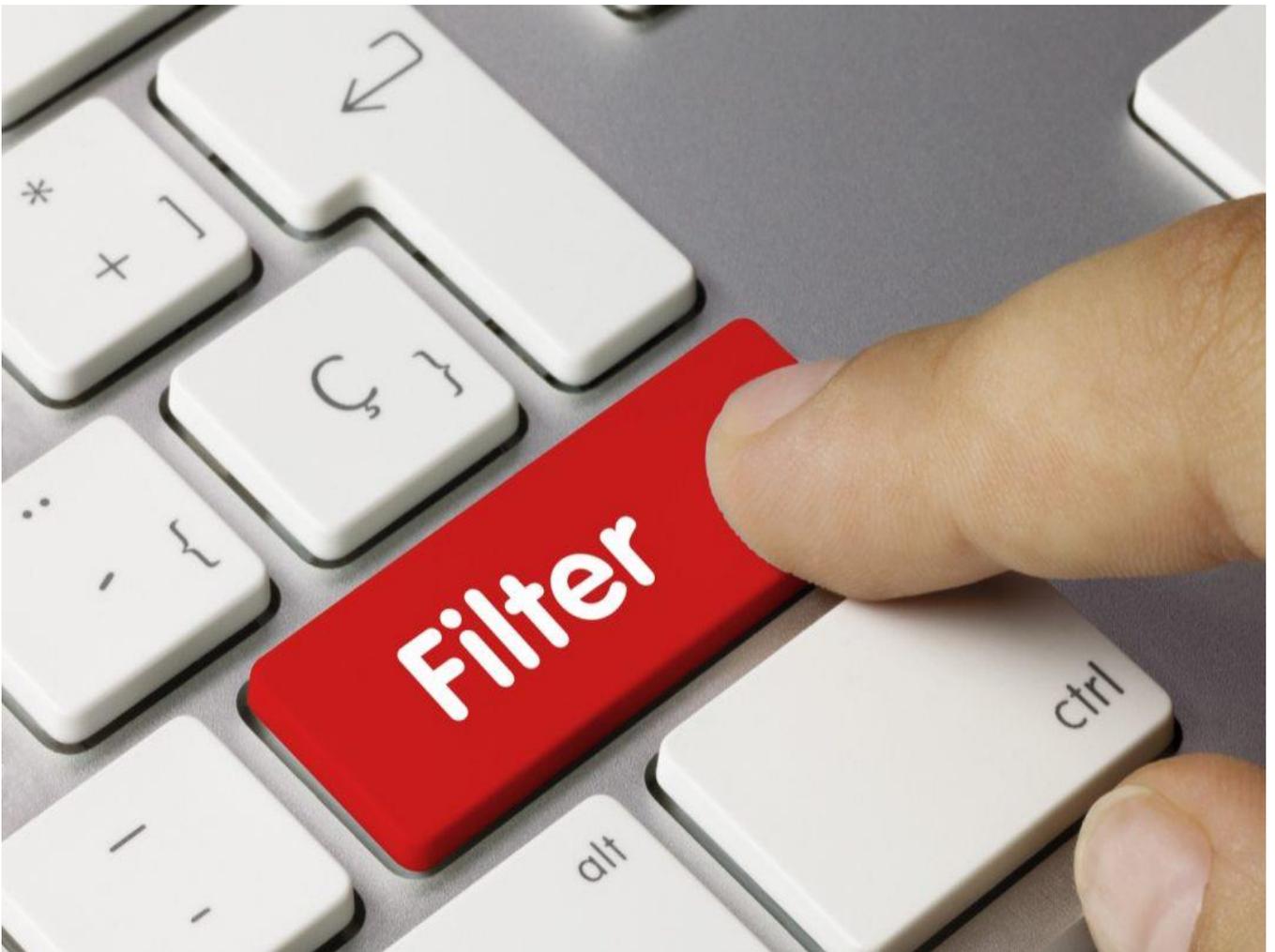


Créer un modèle de filtre pour bloquer des fichiers vidéo





Sommaire

Table des matières

Introduction	3
Création d'un filtre pour bloquer des fichiers vidéo	3
Configuration du filtre vidéo	6
Test du filtre	7
Création de filtre pour se protéger de Ransomware	8
Test du filtre	12
Conclusion	13

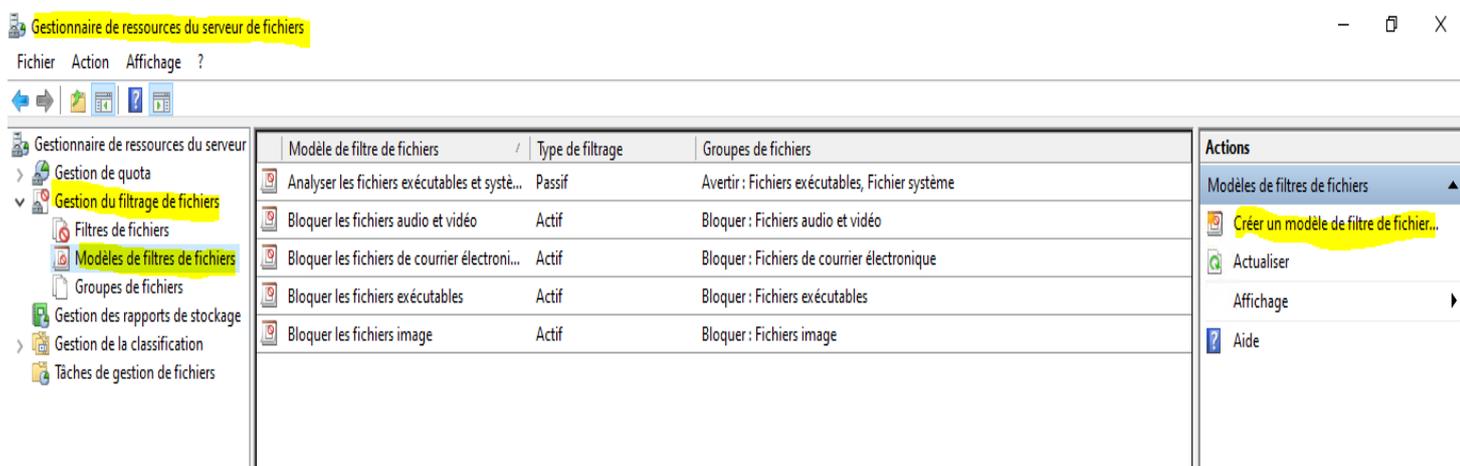
Introduction

Les services de fichiers vous permettent de bloquer les extensions dans les dossiers souhaités. Par conséquent, les fichiers avec des extensions de filtre ne peuvent pas être ajoutés.

Création d'un filtre pour bloquer des fichiers vidéo

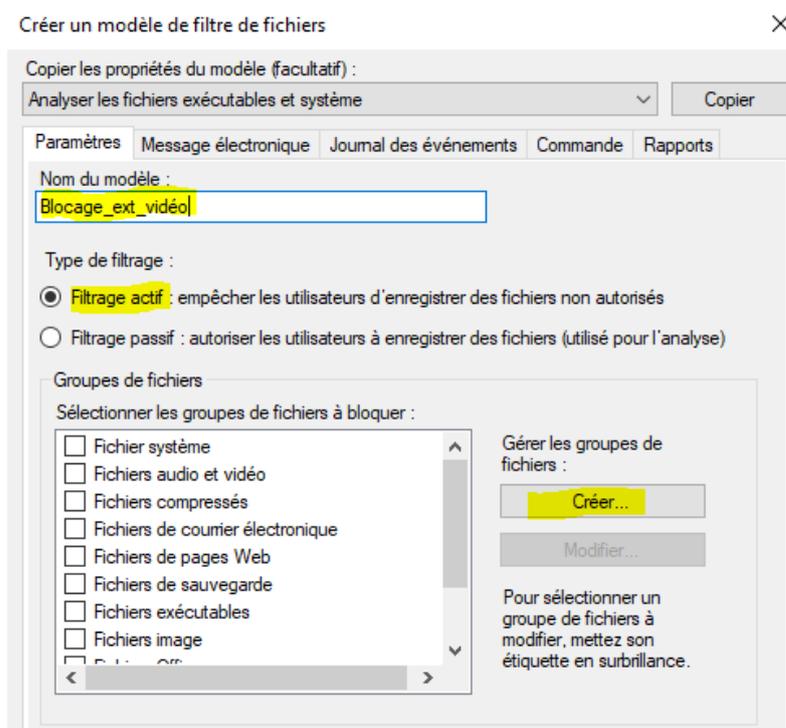
Tout d'abord, créez un modèle qui filtre les extensions vidéo.

➔ Gestionnaire de ressources du serveur de fichiers ➔ Gestion des filtres de fichiers et sélectionnez Modèles de filtre de fichiers ➔ « Créer un modèle de filtre de fichiers ».



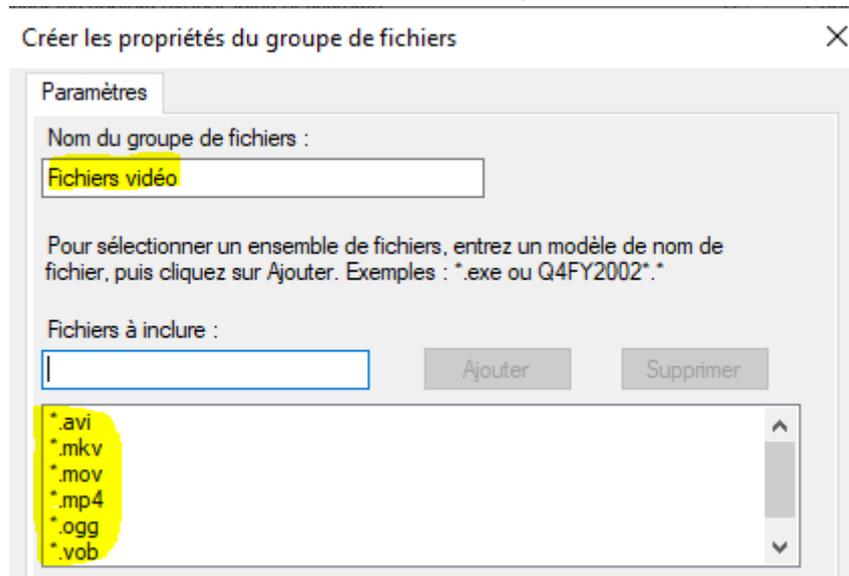
Donner un nom à votre modèle

➔ Nom du modèle ➔ Filtre actif ➔ Gérer les groupes de fichiers ➔ Créer...



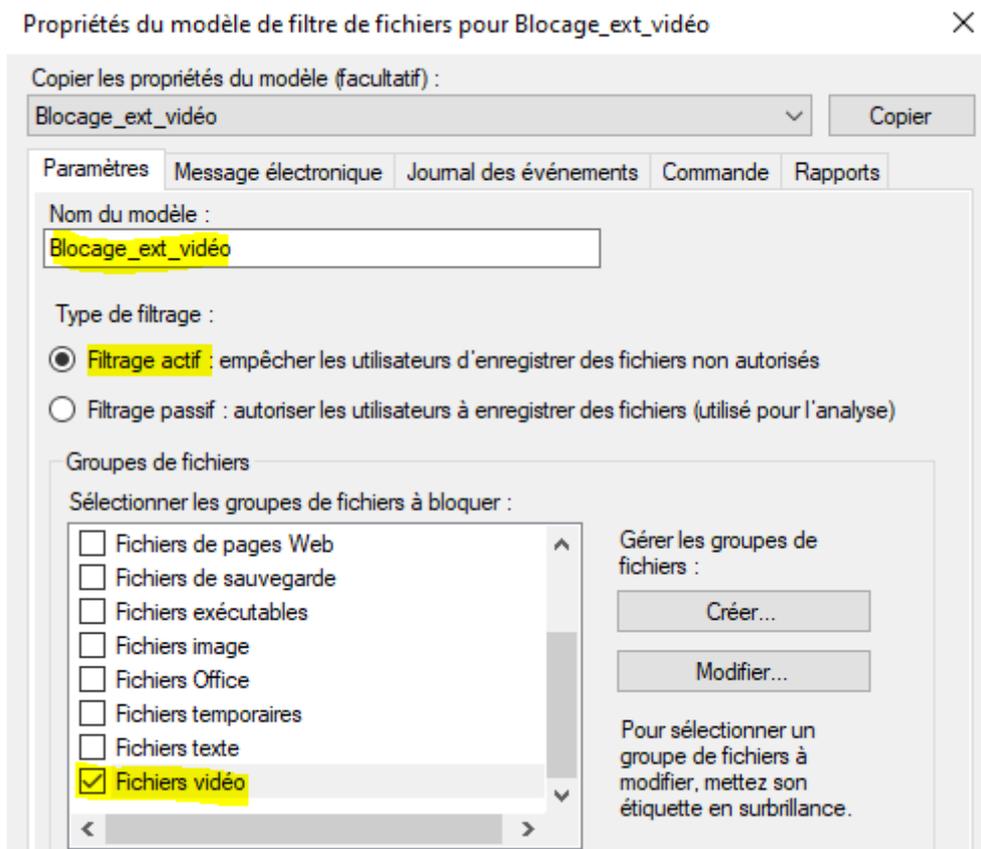
Donner un nom à votre groupe de fichiers

→ Nom du fichier → ajouter les extensions dans filtre à inclure → *.mp4 (Ne pas oublier l'étoile avant le point) → Ok



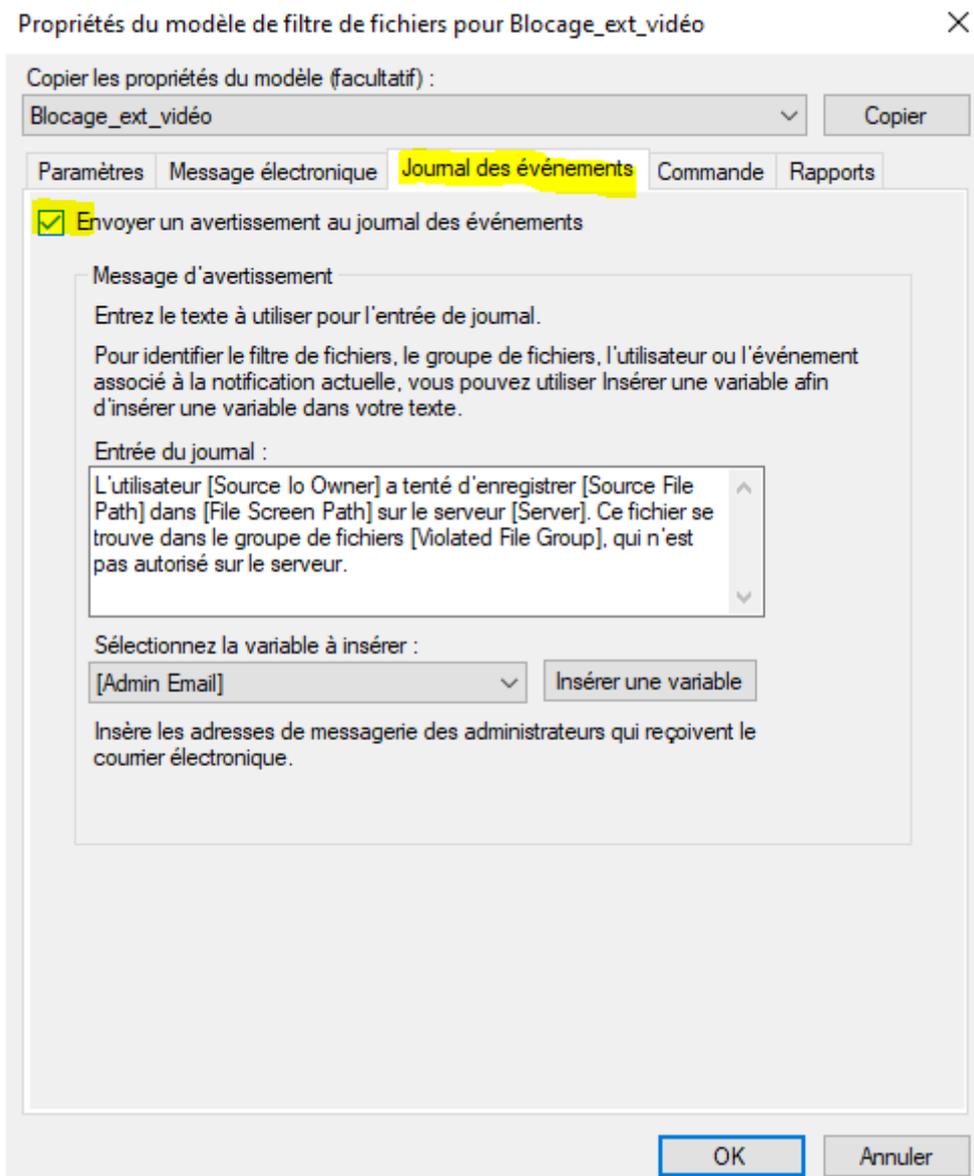
Cocher le groupe de fichier que vous avez créer

→ Sélectionner les groupes de fichiers à bloquer → Fichiers vidéo → Ok



Activer les notifications du journal d'événement

→ Cliquer sur le filtre créer → Journal d'événement → Envoyer un avertissement au journal des événements → Ok



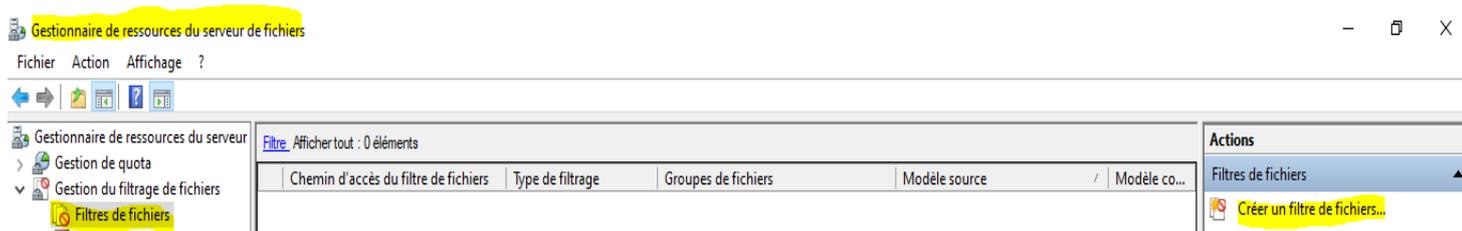
On peut voir que le filtre apparaît dans la liste de modèle.

Modèle de filtre de fichiers	Type de filtrage	Groupes de fichiers
Analyser les fichiers exécutables et systè...	Passif	Avertir : Fichiers exécutables, Fichier système
Blocage_ext_vidéo	Actif	Bloquer : Fichiers vidéo

Configuration du filtre vidéo

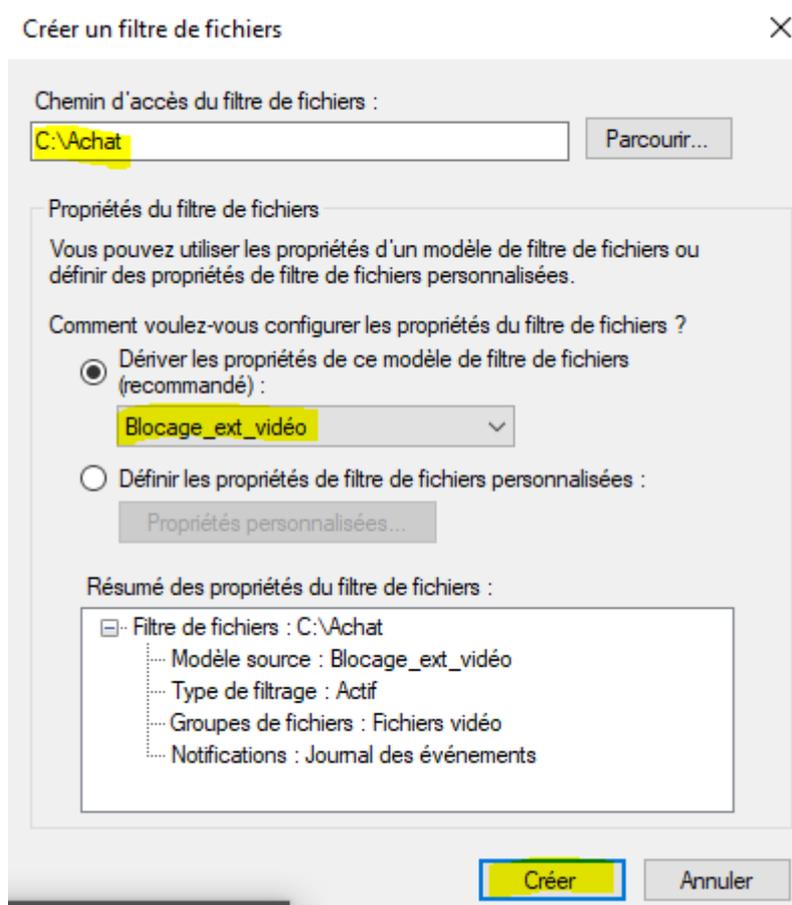
Pour configurer le filtre

➔ Gestionnaire de ressources du serveur de fichiers ➔ Filtres de fichiers ➔ Créer un filtre de fichiers...



Comme pour la création du quota, on indique le chemin d'accès sur les dossiers et on sélectionne le modèle du filtre vidéo. On applique le même filtre pour les dossiers Achat, Informatique et Production.

➔ Chemin d'accès du filtre de fichiers ➔ Dériver les propriétés de ce modèle de filtre de fichiers (recommandé) ➔ Sélectionner le filtre crée ➔ Créer

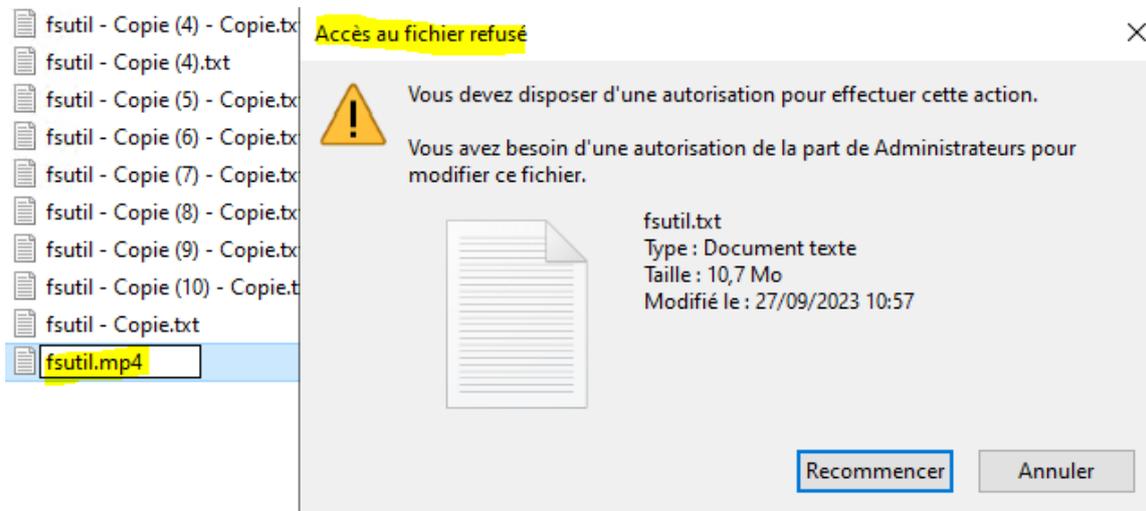


On voit ici les trois filtres créés.

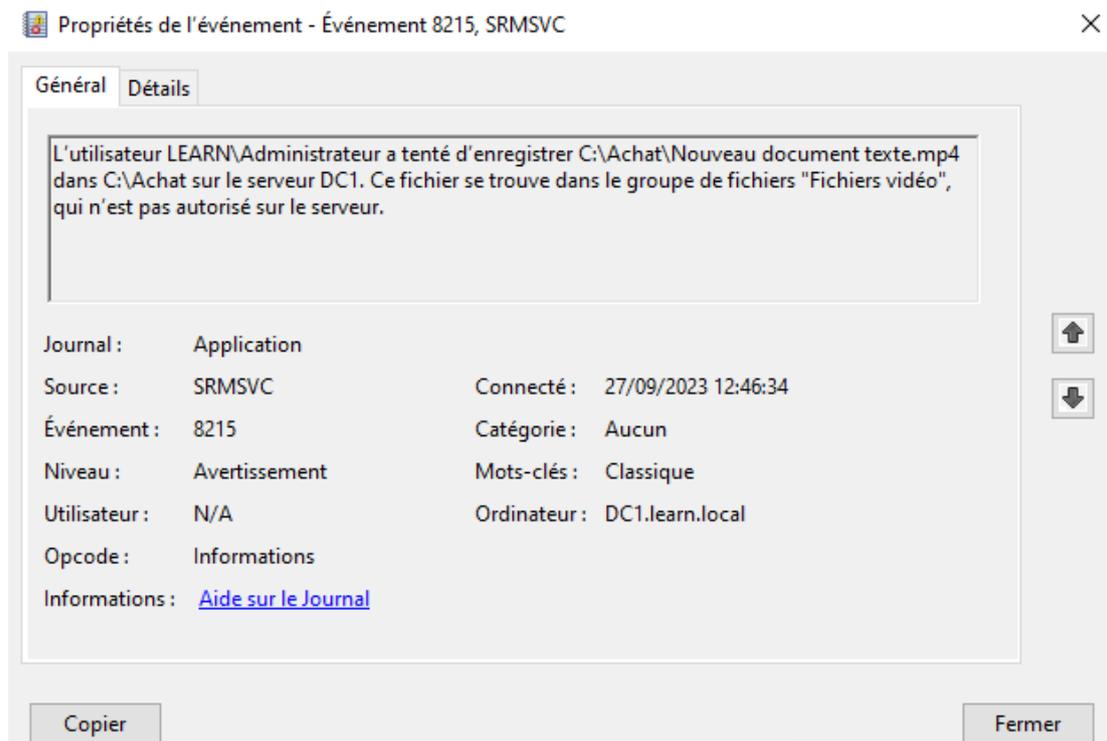
Modèle source : Blocage_ext_vidéo (3 éléments)					
	C:\Achat	Actif	Bloquer : Fichiers vidéo	Blocage_ext_vidéo	Oui
	C:\Informatique	Actif	Bloquer : Fichiers vidéo	Blocage_ext_vidéo	Oui
	C:\Production	Actif	Bloquer : Fichiers vidéo	Blocage_ext_vidéo	Oui

Test du filtre

On va dans le dossier Achat, Informatique ou Production et on teste en essayant de mettre un fichier en MP4 etc. On effectue le test avec un PC dans le domaine (Client ou Serveur)



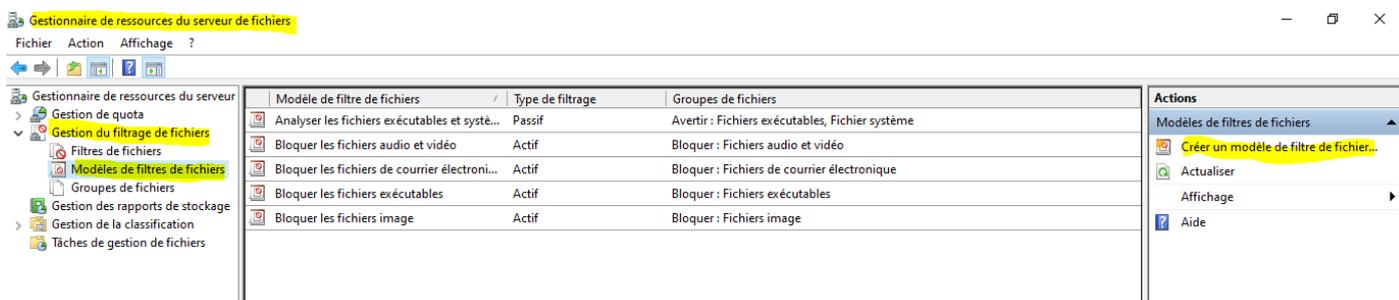
Dans le journal des événements on peut voir qu'on reçoit la notification indiquant le problème.



Création de filtre pour se protéger de Ransomware

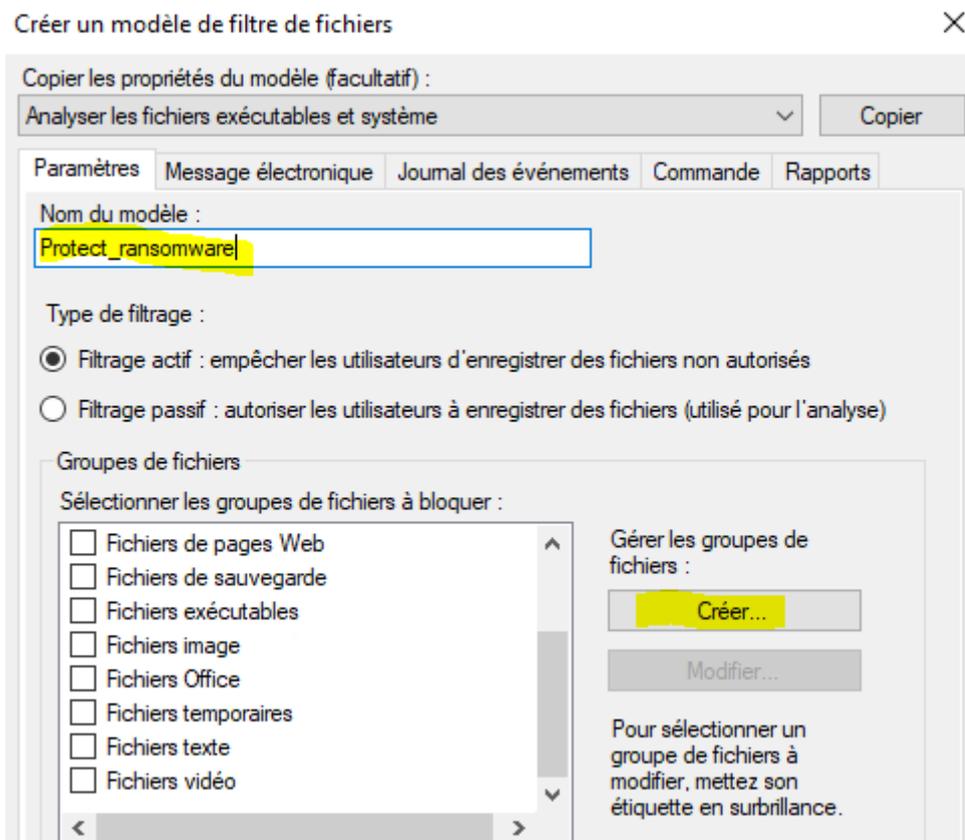
On procède de la même manière que la création du modèle vidéo.

- Gestionnaire de ressources du serveur de fichiers → Gestion des filtres de fichiers et sélectionnez Modèles de filtre de fichiers → « Créer un modèle de filtre de fichiers ».



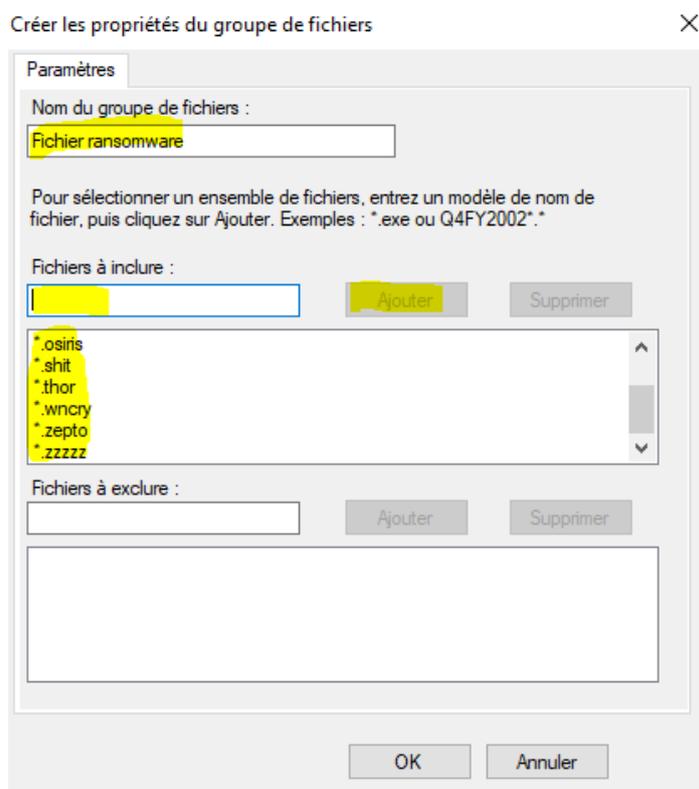
Donner un nom à votre modèle

Nom du modèle → Filtre actif → Gérer les groupes de fichiers → Créer...



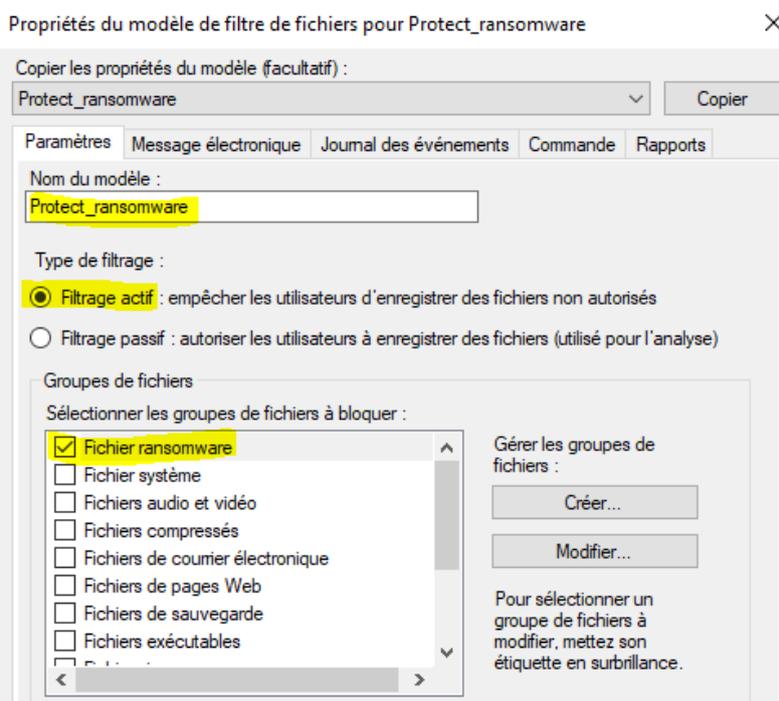
Donner un nom à votre groupe de fichiers

→ Nom du fichier → ajouter les extensions dans filtre à inclure → *.wncry (Ne pas oublier l'étoile avant le point) → Ok



Cocher le groupe de fichier que vous avez créer

→ Sélectionner les groupes de fichiers à bloquer → Fichiers ransomware → Ok

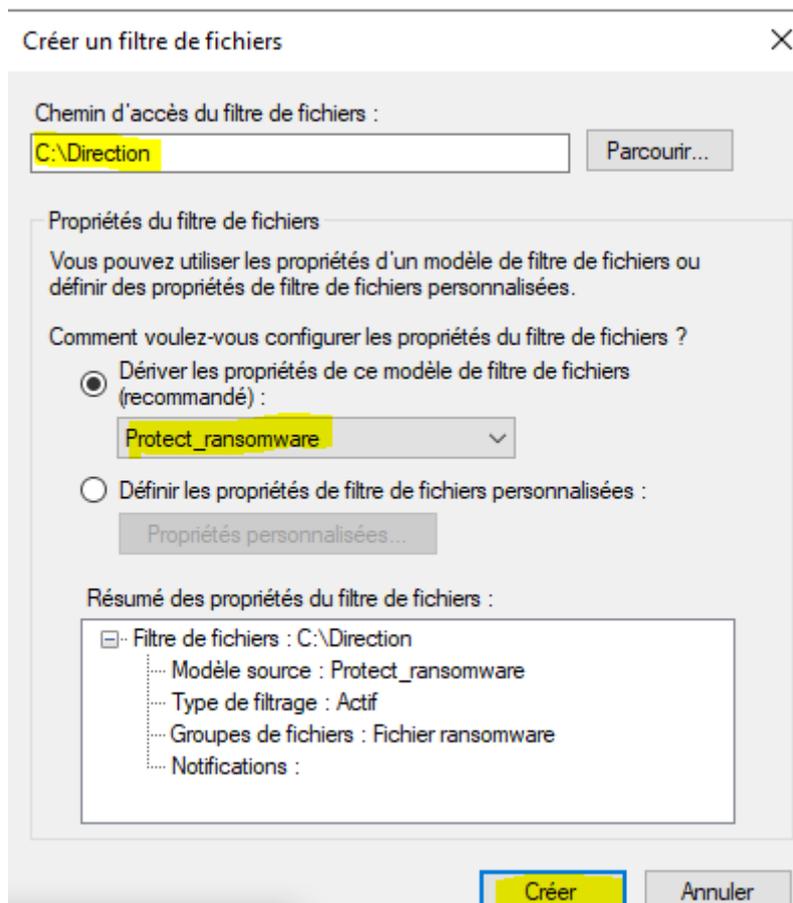


On peut voir que notre filtre est actif.

 Protect_ransomware	Actif	Bloquer : Fichier ransomware
--	-------	------------------------------

Comme pour la création du quota, on indique le chemin d'accès sur les dossiers et on sélectionne le modèle du filtre vidéo. On applique le filtre pour le dossier Direction

→ Chemin d'accès du filtre de fichiers → Dériver les propriétés de ce modèle de filtre de fichiers (recommandé) → Sélectionner le filtre crée → Créer



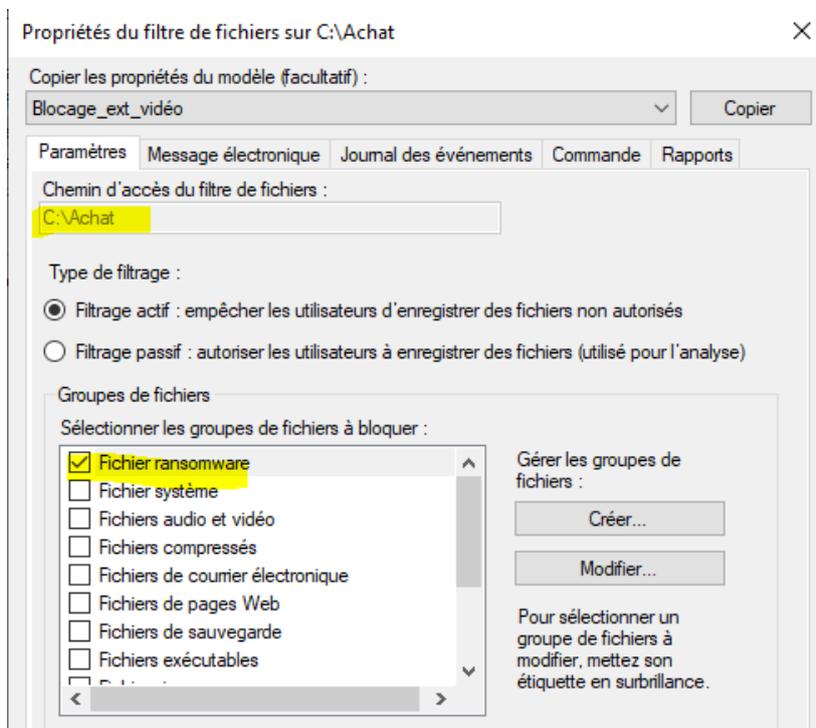
On peut appliquer qu'un seul filtre par fichier, donc pour les dossiers Achat, Informatique et Production on va leurs ajouter le groupe « Fichier ransomware »

→ Clic droit sur les filtres de fichier déjà mise en place → Modifier les propriétés du filtre de fichiers...

 C:\Achat	Actif	Bloquer : Fichiers vidéo	Blocage_ext_vidéo	Oui
 C:\Informatique			Blocage_ext_vidéo	Oui
 C:\Production			Blocage_ext_vidéo	Oui
 Modèle source : Protect_ransomware				
 C:\Direction			Protect_ransomware	Oui

On ajoute le groupe de fichier à bloquer pour le dossier Achat, Informatique et Production

→ Sélectionner les groupes de fichiers à bloquer → Fichier ransomware

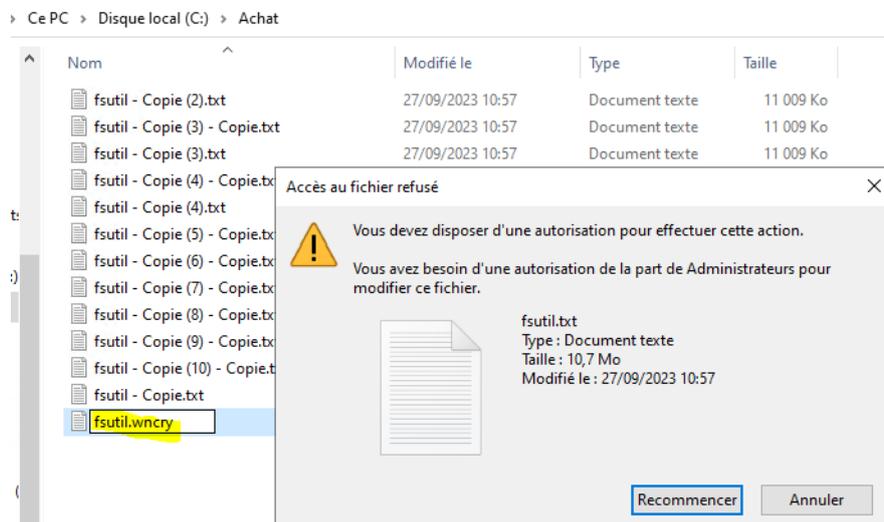


Voici les deux filtre mise en place pour les dossiers Achat, Informatique et Production et le filtre créer pour le dossier Direction.

Modèle source : Blocage_ext_vidéo (3 éléments)				
C:\Achat	Actif	Bloquer : Fichier ransomware, Fichiers...	Blocage_ext_vidéo	Non
C:\Informatique	Actif	Bloquer : Fichier ransomware, Fichiers...	Blocage_ext_vidéo	Non
C:\Production	Actif	Bloquer : Fichier ransomware, Fichiers...	Blocage_ext_vidéo	Non
Modèle source : Protect_ransomware (1 élément)				
C:\Direction	Actif	Bloquer : Fichier ransomware	Protect_ransomware	Oui

Test du filtre

On va dans le dossier Achat, Informatique, Production ou Direction et on test en essayant de mettre un fichier en extension wncry etc. On effectue le test avec un PC dans le domaine (Client ou Serveur).



Dans le journal des événements on peut voir qu'on reçoit la notification indiquant le problème.



Conclusion

Dans cette procédure, nous avons vu les avantages que peuvent apporter les filtres mises en place. Cela permet dans une infrastructure d'avoir des solutions de sécurité pousser.