WINDOWS SERVER

MISE EN PLACE DE FILTRES

Margaux TANET

CPI

2024-2025

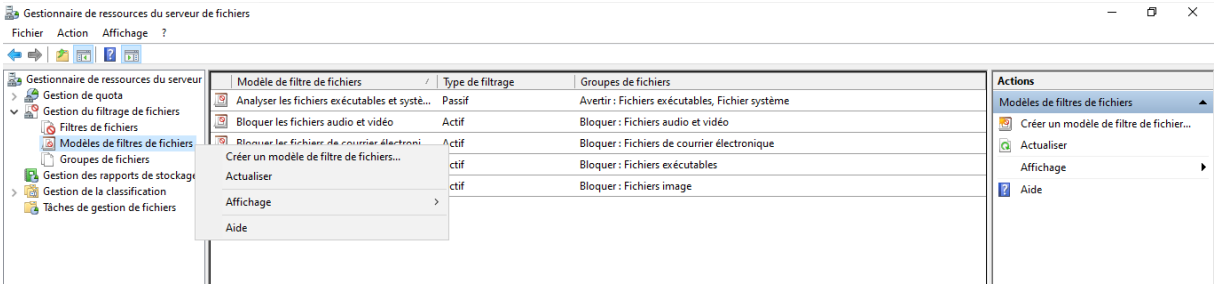
Introduction : Dans ce document, nous allons voir comment il est possible de mettre en place différents filtres pour refuser l'accès à certains types de fichiers par extension. Les différents filtres mis en place bloqueront certains types de fichiers vidéo et des fichiers pour des ransomware. A la fin nous pourront constater si ces filtres marchent en effectuant des tests.

Prérequis : Avoir installer FSRM

I- Création du modèle de filtre vidéo

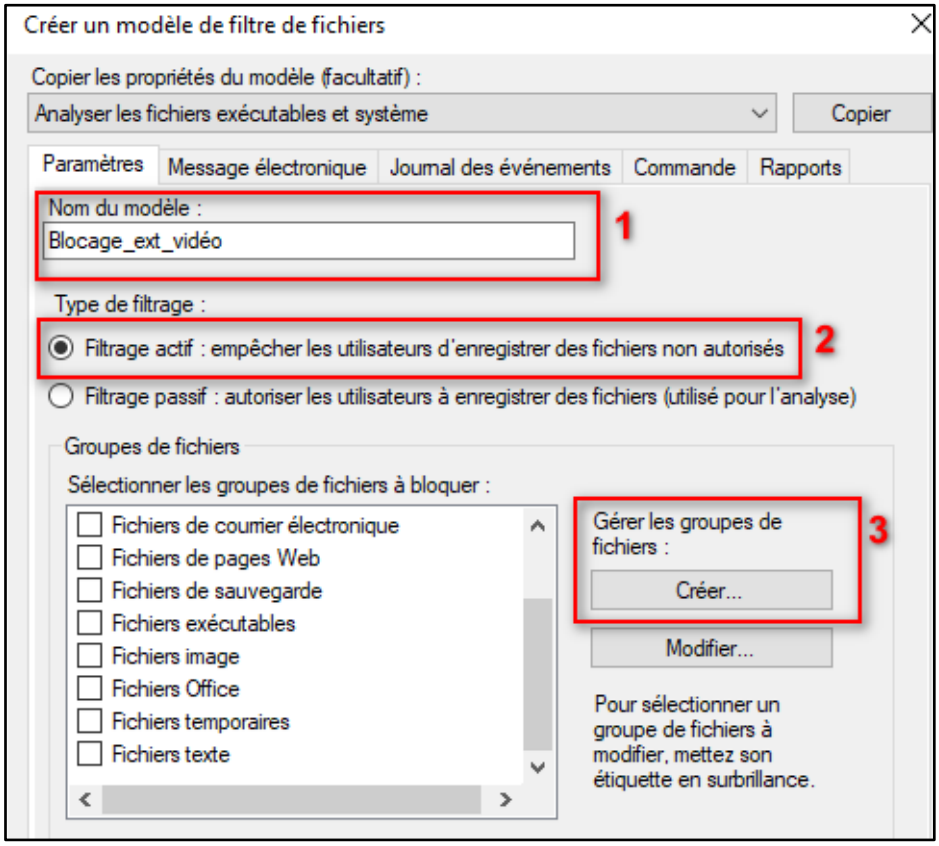
Se rendre dans le gestionnaire de ressources du serveur de fichiers.

- Créer un modèle de filtre de fichiers :
  Clic droit puis *créer un modèle de fichier de filtre de fichier :*

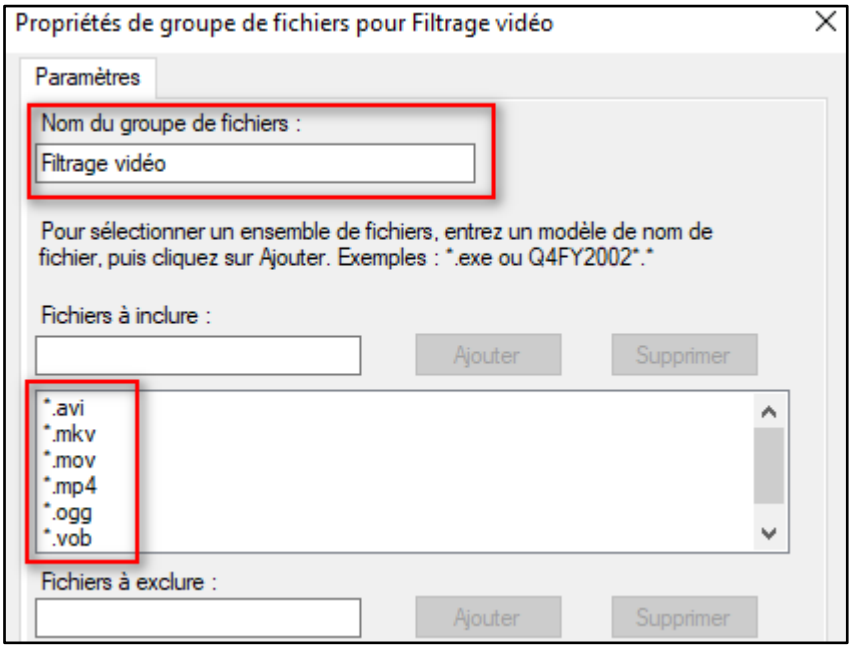


- Mettre le nom du modèle, choisir un filtrage actif puis cliquer sur créer dans la zone de groupe de fichier :

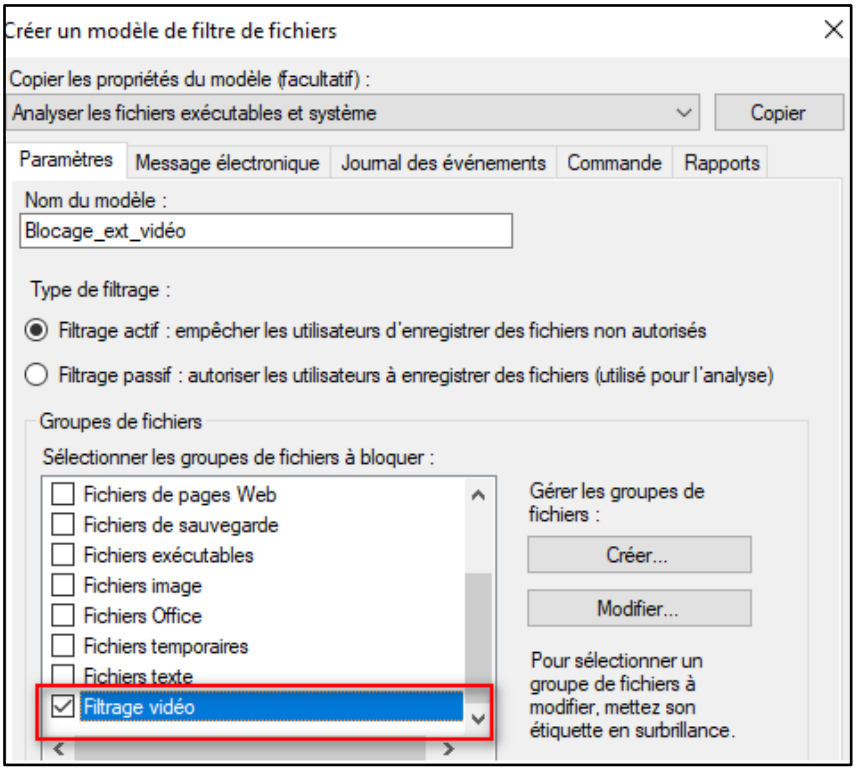
Un filtrage actif permet d'intercepter les requêtes faites au système de fichiers. Il empêche ainsi les utilisateurs d'enregistrer des fichiers qui ne sont pas autorisés.



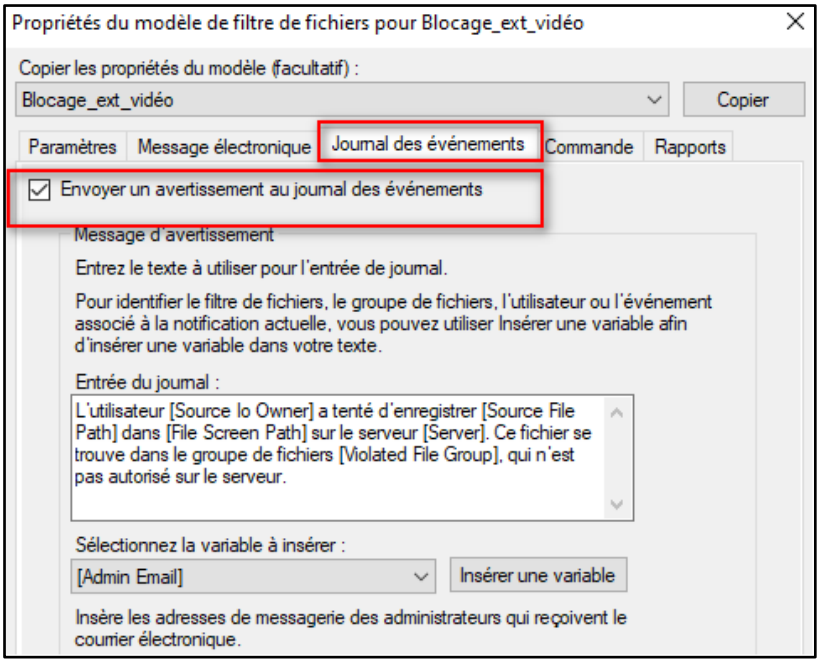
- Après avoir cliqué sur « créer » dans le groupe de fichier, il faut mettre le nom du groupe de fichier et renseigner les extensions des vidéos qui seront bloquées (.avi .mp4 .mkv .mov .ogg .vob .wmv). L'astérisque permet de sélectionner l'entièreté des fichiers.



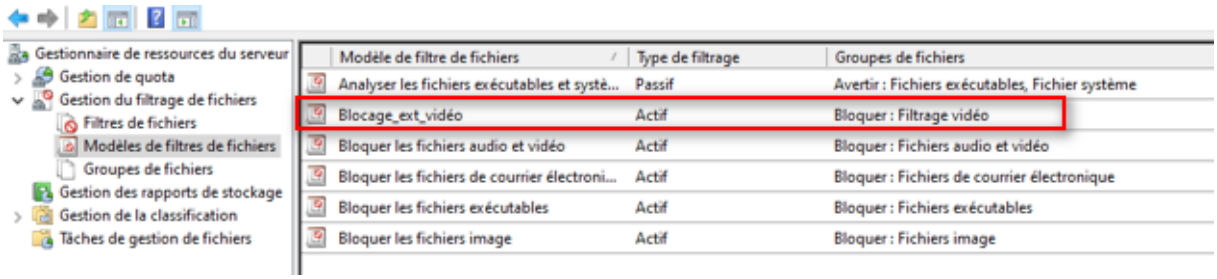
Confirmer la modification et sélectionner le groupe de fichier créer précédemment :



Important : Dans l'onglet journal d'évènement, cocher la case « *envoyer un avertissement au journal d'évènement* » pour être informé et recevoir une alerte.

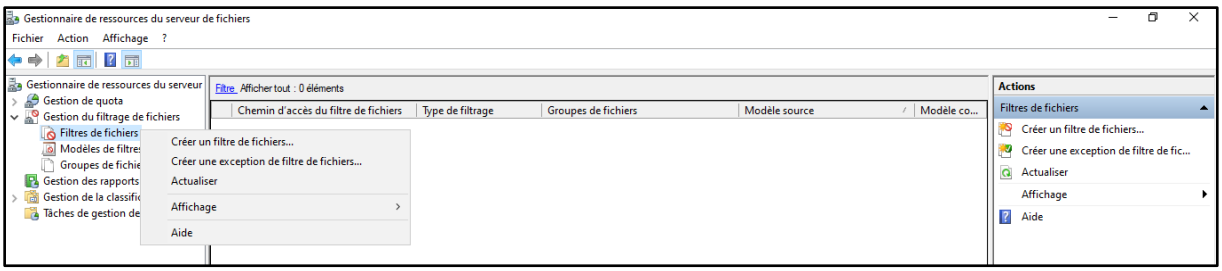


Le modèle de filtre créé précédemment :



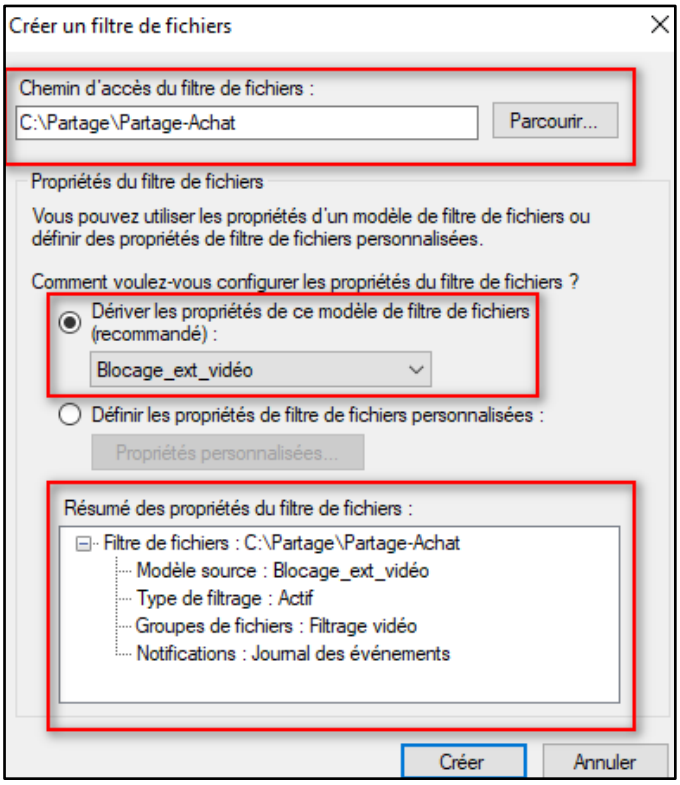
II- Création du filtre de fichier vidéo

- Se rendre dans « filtres de fichiers » et cliquer sur créer un filtre de fichier :

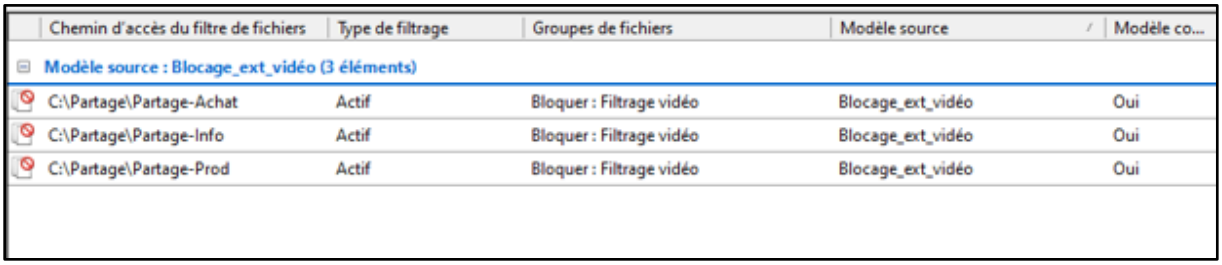


- Le filtre doit s'appliquer uniquement sur les dossiers du partage Achat, Production et Informatique. Dans le chemin d'accès à indiquer sélectionner le chemin correspondant aux différents dossiers sur lequel sera appliquer le filtre. Dans les propriétés de ce modèle, saisir le modèle créer juste avant « blocage_ext_vidéo » :

Ici dans l'exemple a été fait que pour le dossier partage Achat.



On peut constater les trois filtres mis en place pour les différents dossiers de partage :



III- Test pour le filtre de vidéo

Voici les tests réalisés pour les différents dossiers avec la commande fsutil en créant un fichier dont l'extension (.mp4) doit être refusée.

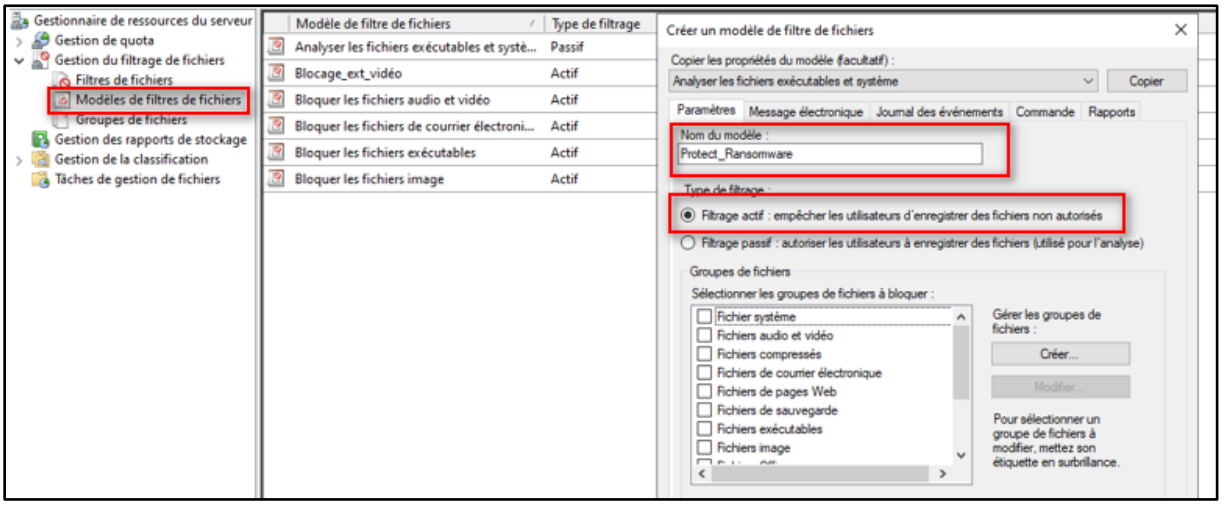
```
C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Info\video.mp4 100
Erreur :  Accès refusé.

C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Achat\video.mp4 100
Erreur :  Accès refusé.

C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Prod\video.mp4 100
Erreur :  Accès refusé.

C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Direction\video.mp4 100
Le fichier C:\Partage\Partage-Direction\video.mp4 est créé
```

IV- Création d'un modèle de filtre de fichiers ransomware

Ce qu'il nous a été demandé :

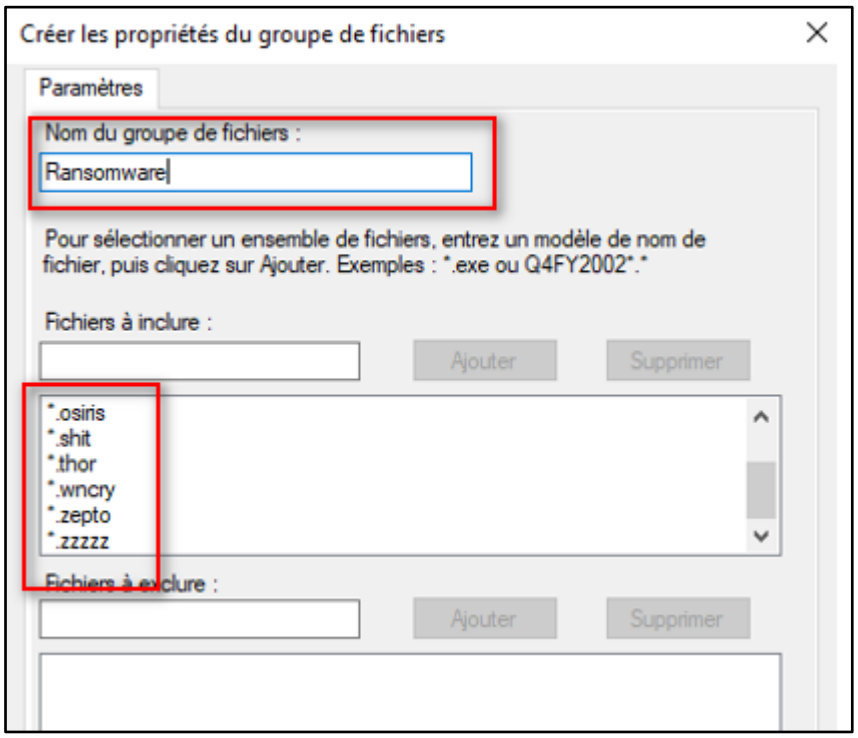
- DC1 : Créer un filtre afin de vous protéger de deux ransomwares :
  - Nom : Protect_ransomware
  - *Bloquer : « .locky / .zepto / .osiris / .odin / .zzzzz / .aesir / .thor / .shit / .wncry »*
  - Alerte dans le journal d'évènement
- DC1 : Appliquer le modèle de filtre à tous les dossiers
- Créer un fichier ayant pour extension .wncry dans un des dossiers et tester votre configuration
  - *Prendre screenshot du message dans le journal d'évènement*

➢ Clic droit pour créer un modèle de filtre appelé *Protect_Ransomware*. Choisir le filtrage actif.

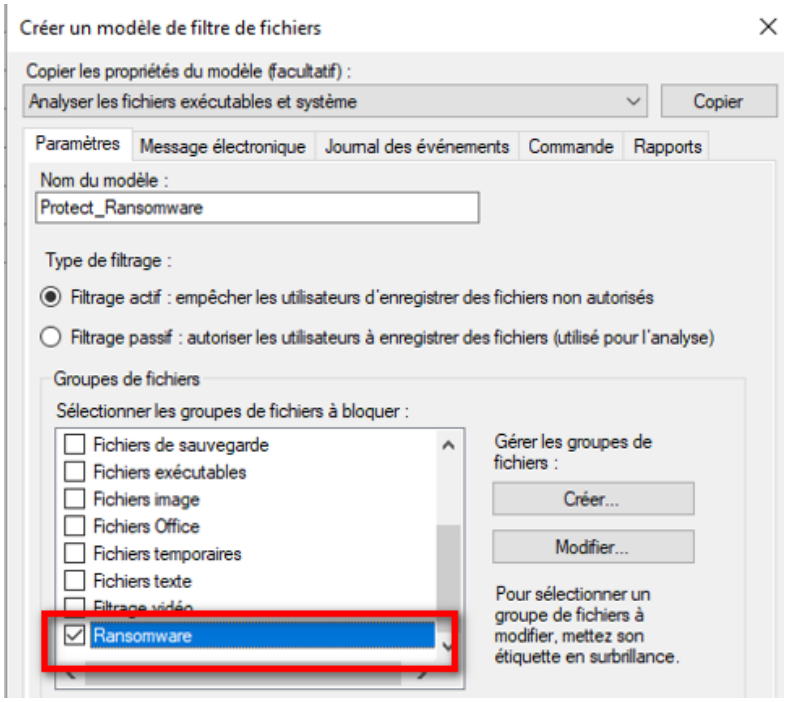


- Appuyer sur « créer » pour ajouter des extensions de fichiers à bloquer avec pour nom de groupe de fichiers « Ransomware » :

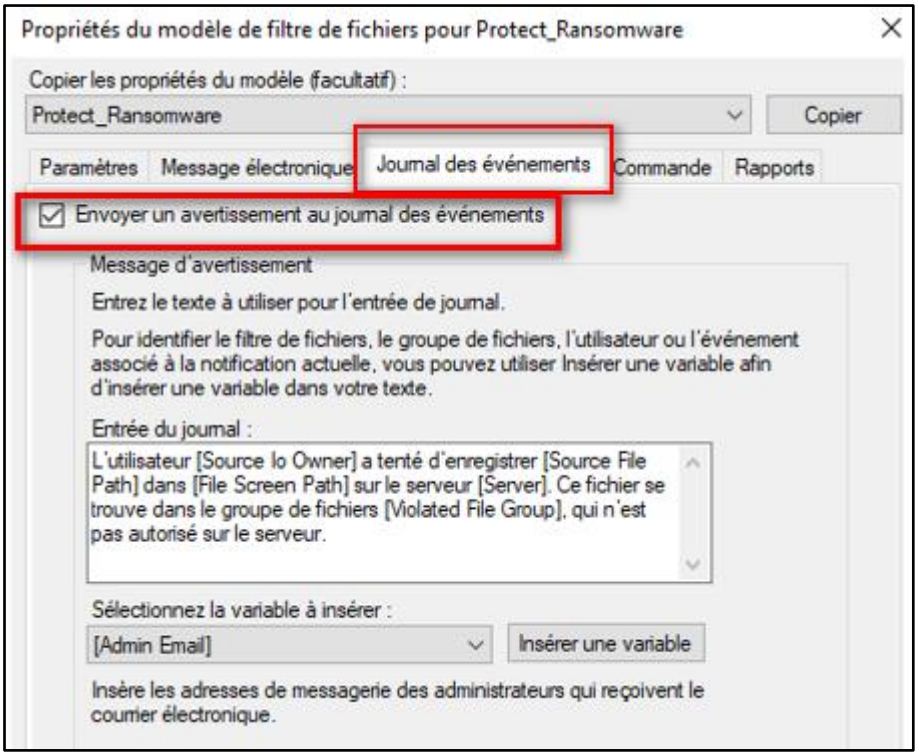
  Ici il a été ajouté les extensions *.thor, *.zzzzz, *.aesir, etc



- On sélectionne ensuite le groupe de fichier créer juste avant contenant les extensions et on fait « ok » :

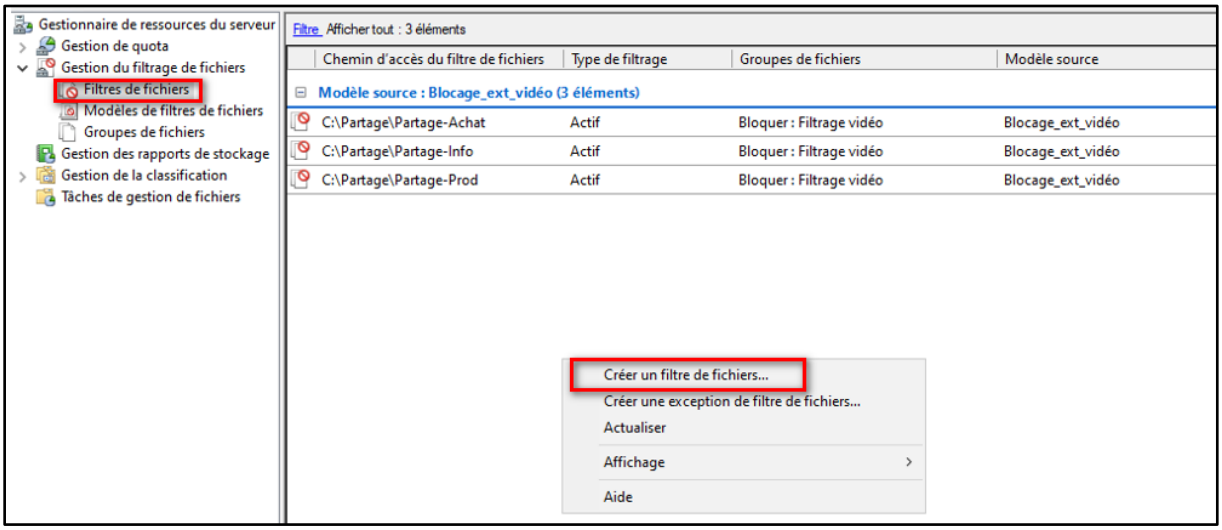


➢ **Important :** Bien penser à activer le journal d'évènement pour recevoir les alertes dans l'onglet « journal d'évènements » :

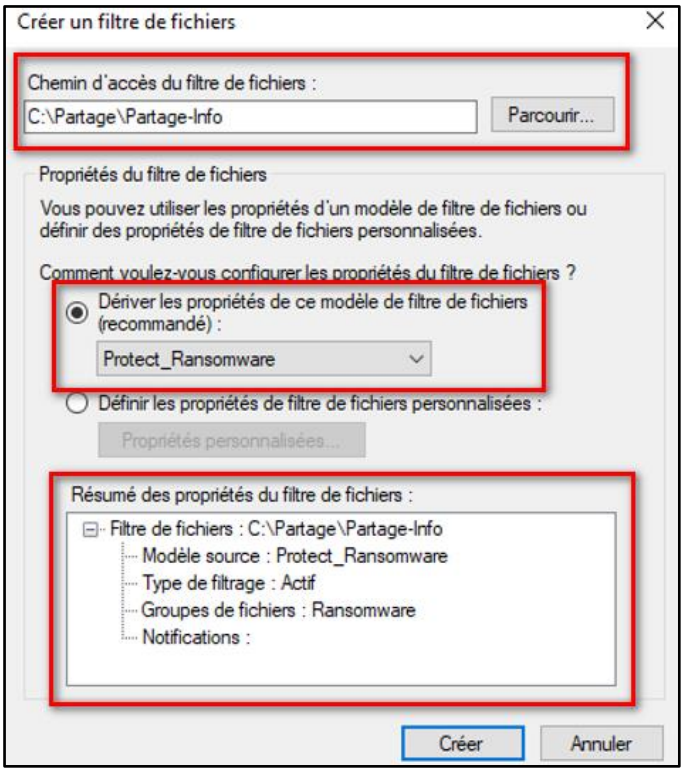


V- Création du filtre fichier pour ransomware

➢ Créer un filtre de fichier en faisant clic droit :



- Création du filtre pour chaque direction comme l'exemple sur la partie Informatique en reprenant le modèle de filtre créer précédemment (Protect_ransomware) :



Voici tous les filtres crées pour chaque partage :

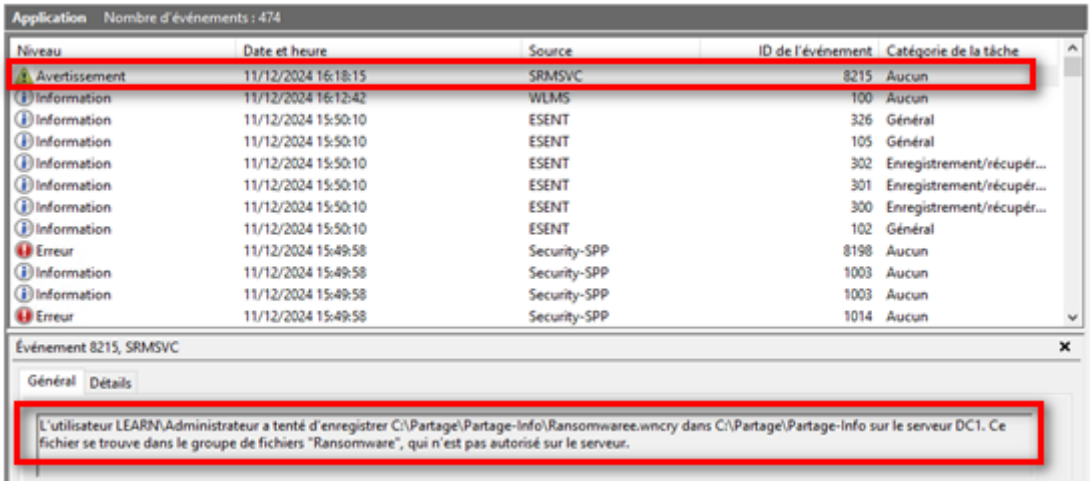
Chemin d'accès du filtre de fichiers	Type de filtrage	Groupes de fichiers	Modèle source	Modèle co...
Modèle source : Protect_Ransomware (4 éléments)				
C:\Partage\Partage-Achat	Actif	Bloquer : Ransomware	Protect_Ransomware	Oui
C:\Partage\Partage-Direction	Actif	Bloquer : Ransomware	Protect_Ransomware	Oui
C:\Partage\Partage-Info	Actif	Bloquer : Ransomware	Protect_Ransomware	Oui
C:\Partage\Partage-Prod	Actif	Bloquer : Ransomware	Protect_Ransomware	Oui

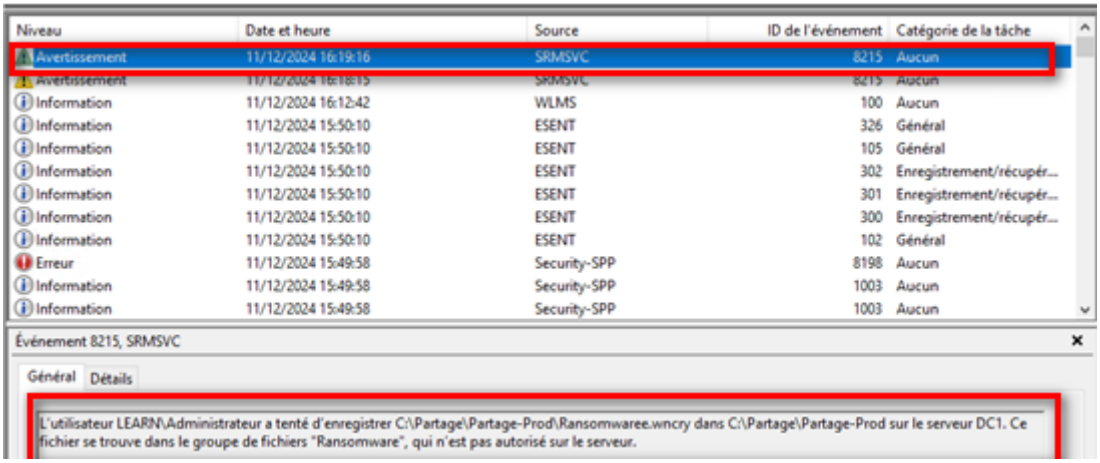
VI- Tests avec extension .wncry

Un test est réalisé avec la création d'un fichier dans une des directions avec comme extension .wncry qui est censé être bloquée :

```
C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Info\Ransomware.wncry 100000
Erreur :  Accès refusé.

C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Achat\Ransomware.wncry 100000
Erreur :  Accès refusé.

C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Direction\Ransomware.wncry 100000
Erreur :  Accès refusé.

C:\Users\Administrateur>fsutil file createnew C:\Partage\Partage-Prod\Ransomware.wncry 100000
Erreur :  Accès refusé.
```

Et voici les messages d'alertes dans le journal d'évènement après l'essai de création de ces fichiers :





Conclusion : Nous avons mis en place plusieurs types de filtre de fichiers : sur les extensions de vidéo et l'autre sur l'extension de fichier ransomware. Nous avons constaté que les filtres étaient bien appliqués puisqu'on recevait bien les alertes et l'accès été refusé.