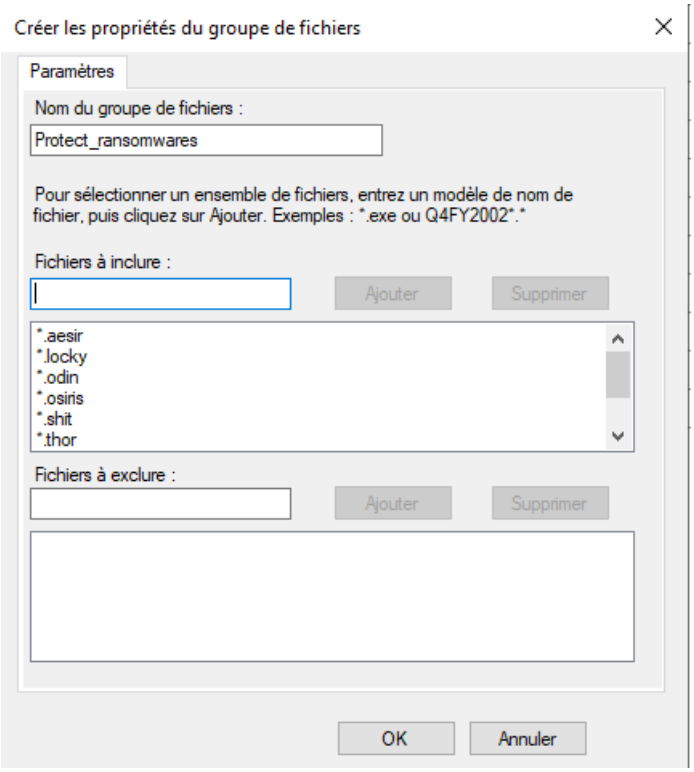
Comment créer un modèle de filtre ?

Pour commencer lancer le Gestionnaire de serveurs de fichier.

Rendez-vous dans Gestion du filtrage des fichiers, ensuite deux options vous pouvez utilisez les listes d'extensions prédéfinis mais pour ma part je vais créer ma liste personnalisée.

Pour ce faire, cliquez sur Groupe de fichier une fois dedans faites un clic droite pour créer un nouveau groupe de fichier.

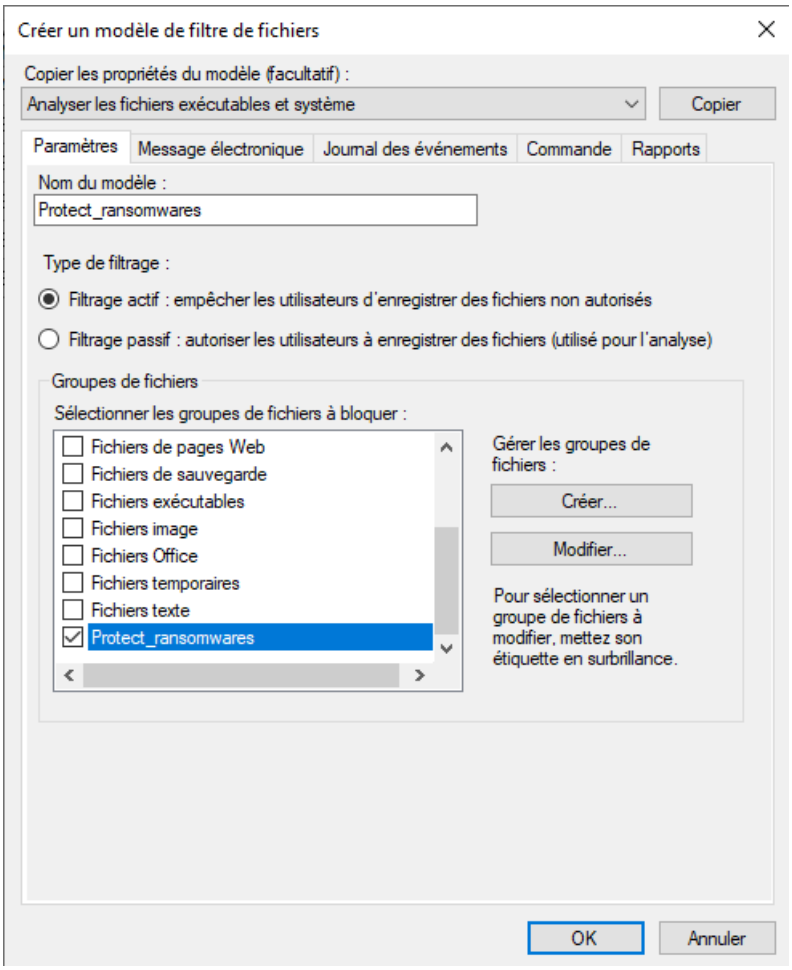


Remplissez dans fichier à inclure les fichiers que vous ne souhaites pas utiliser écrivez *. *Extensions*

. Cela englobe tout le reste des fichiers. Finissez par lui donner un nom. Et validé.

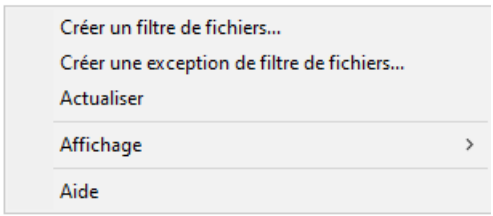
Nous allons maintenant créer un modèle de filtre :

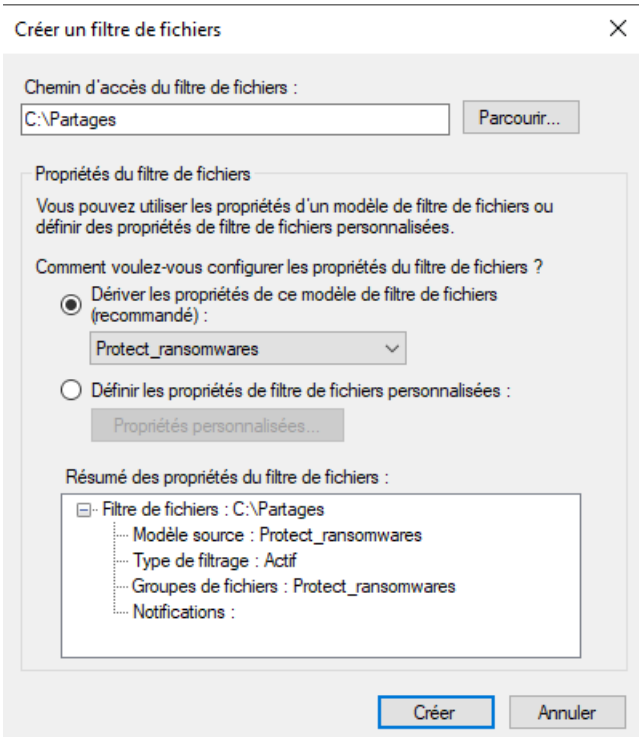
Pour ce faire cliquez sur créer un modèle de filtre de fichiers une fois dedans faites un clic droit dedans pour crée un modèle de filtre de fichiers.



Saisissez un nom, dans type de filtrage renseigner actif, sélectionné le groupe de fichier a bloqué que vous avait créer au paravent. Pour recevoir une alerte rendez-vous dans journal d'événements. Et cochez la case Envoyer un avertissement au journal des événements.

Créer ensuite un filtre de fichiers.





Renseignez le chemin d'accès, sélectionné bien votre modèle de filtre créer aux préalables. Puis appuyiez ensuite sur crées.

Les filtres sont maintenant créés, nous allons maintenant les tester.

Grâce à la commande :

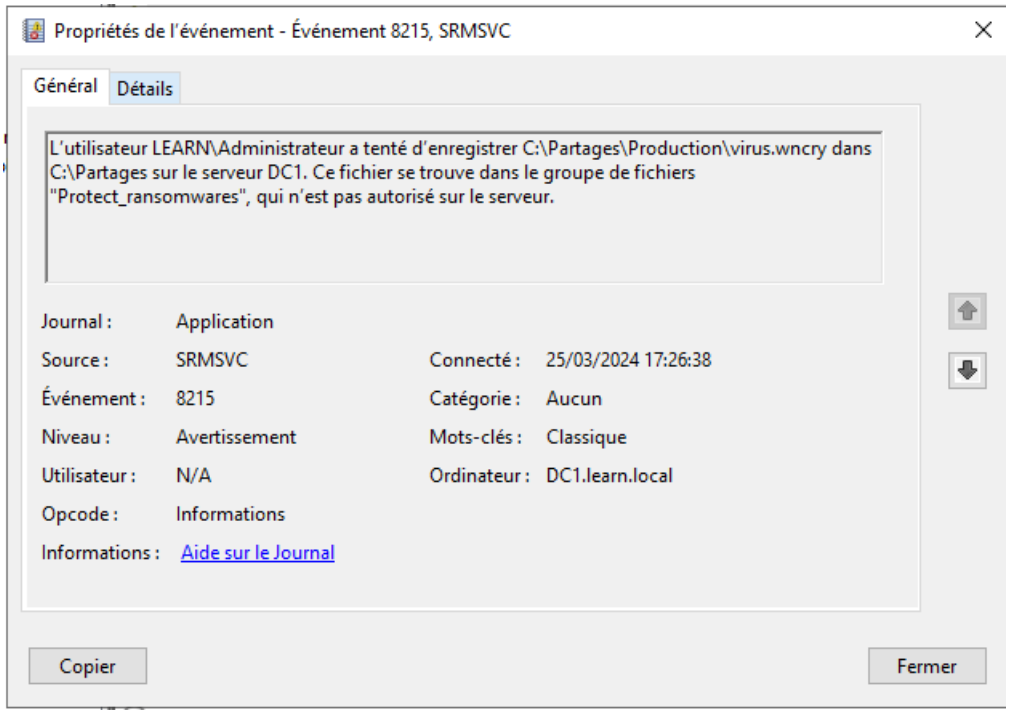
Fsutil file createnew \\nom_du_serveur\nom_du_dossier\mon_fichier.extensions 8940000

Directement dans l'invite de commande, si les filtres sont bien opérationnels un message d'erreur devrait s'afficher ainsi qu'un avertissement dans l'observateurs d'évènement devrais apparaitre.

```
C:\Users\Administrateur>fsutil file createnew \\DC1\Partages\Production\virus.wncry 4000
Erreur :  Accès refusé.

C:\Users\Administrateur>
```

Nous voyons bien que si nous essayons de créer un fichier.mp4 alors l'accès seras refusé ainsi qu'un avertissement est visibles dans l'observateur d'événements.



Nous voilà maintenant protégé de certains ransomwares.