REPUBLIQUE DU SENEGAL

Un Peuple - Un But - Une Foi

Ministère de l'Enseignement Supérieur de la Recherche et de l'innovation

Direction Générale de l'Enseignement Supérieur Privé

ISI INSTITUT SUPERIEUR D'INFORMATIQUE

L'institut de référence dans les TIC

Gestionnaire de ressources du serveur de fichiers – FSRM – Filtre de fichiers

Sous Windows Server 2022

Présenté Par :

Mr. LAMINE DABO

Professeur :

Mr. Massamba LO

Sommaire

I. Présentation

Dans ce tutoriel, nous allons apprendre à configurer FSRM sur notre serveur de fichiers de manière à déployer une première barrière de protection contre les ransomwares.

Pour rappel, un ransomware, en français rançongiciel, est un logiciel malveillant qui va chiffrer vos données et vous demander de payer une rançon si vous souhaitez obtenir la clé de déchiffrement dans le but de récupérer vos données. Dans certains cas, les données sont également exfiltrées dans le but d'être divulguées ou revendues.

II. L'intérêt de cette protection

Avec le filtrage de fichiers de FSRM, on va pouvoir bannir certaines extensions de fichiers (et noms de fichiers) sur notre serveur de fichiers Windows Server. En bloquant les extensions associées aux ransomwares, on empêchera le ransomware de chiffrer les fichiers, car il ne pourra pas enregistrer le fichier dans son nouveau format.

Prenons un exemple. L'extension ".locky" associée au ransomware Locky. S'il est e S'il est exécuté par un pirate sur votre serveur de fichiers, il ne pourra pas chiffer vos données, car l'extension ".locky" est bloquée sur les volumes/dossiers où sont situées vos données grâce à la règle mise en place et déployée via le script PowerShell.

III. Présentation du gestionnaire de ressources du serveur de fichiers

Le Gestionnaire de ressources du serveur de fichiers (**File Server Ressource Manager FSRM**) est une fonctionnalité du rôle Serveur de fichiers.

FSRM permet plusieurs choses au niveau des serveurs de fichiers :

- Application de quota sur un dossier
- Taches automatiques sur les dossiers et fichiers (archivage automatique des fichiers non ouvert depuis xxxx)
- Rapport sur le stockage (Volumétrie par groupe de fichiers, doublons...)
- Filtrer les fichiers, ce que nous allons voir dans ce tutoriel
- ...

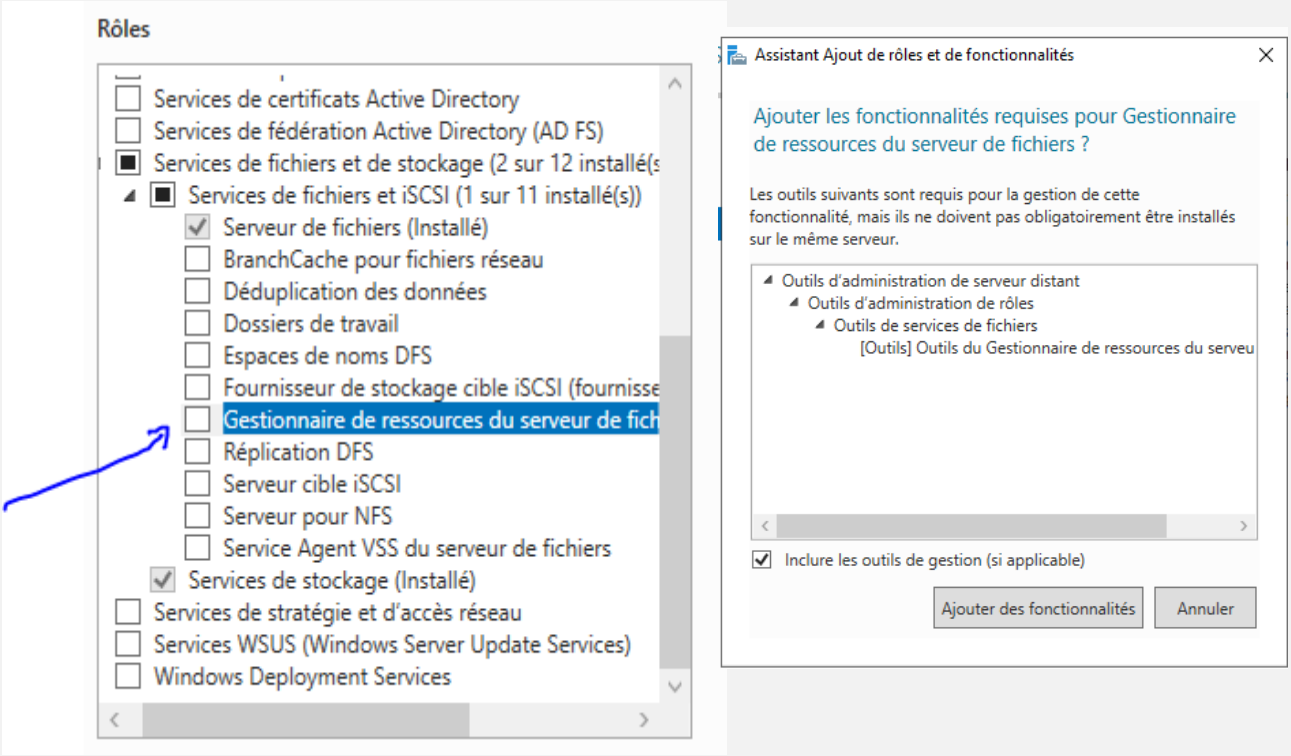
Par ailleurs, on peut aussi **configurer un message d'erreur spécifique lorsqu'un utilisateur fait face à un accès refusé** pour accéder à un dossier, en lui proposant d'envoyer une demande d'assistance par e-mail, le tout à partir de l'Explorateur de fichiers Windows.

IV. Installation de FSRM sur Windows Server 2022

A. Avec l'interface graphique

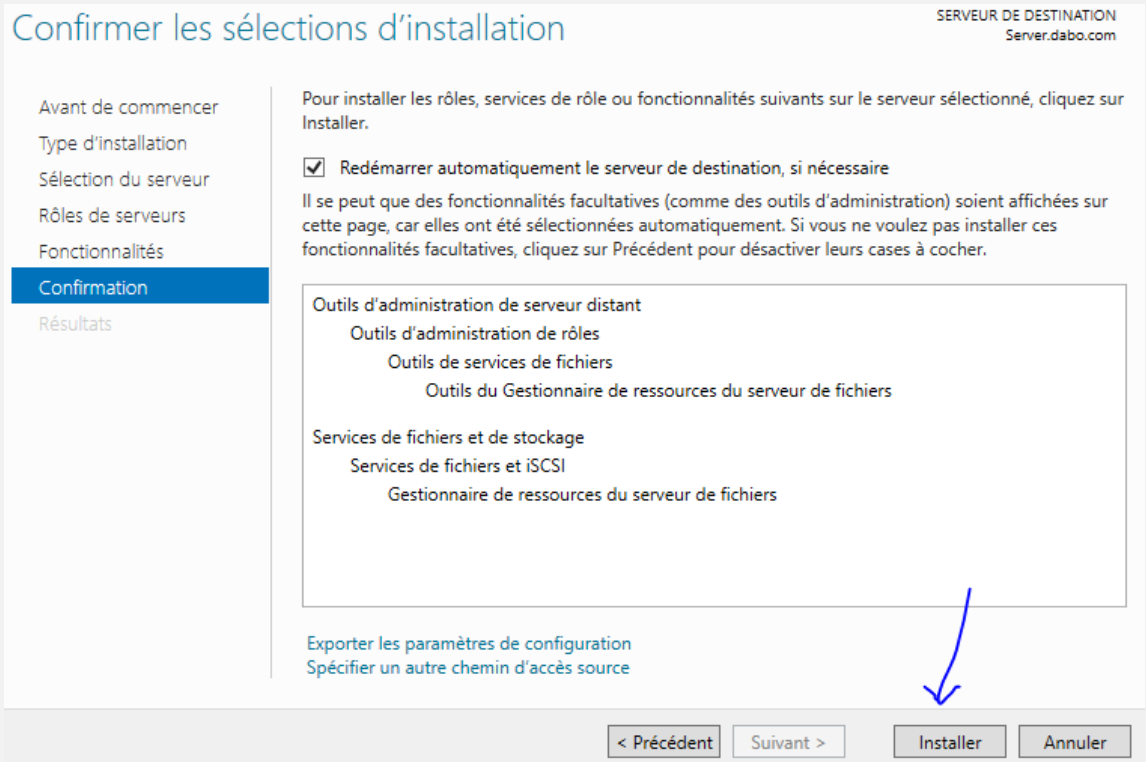
Cette installation est réalisée à partir du Gestionnaire de serveur. Cliquez sur "**Gérer**" puis "**Ajouter des rôles et fonctionnalités**". Passez la première étape... Avancez jusqu'à l'étape "**Rôles de serveur**".

Dans la liste des rôles, aller à Services de fichiers et de stockage > Service de fichiers et iSCSI> puis cocher **Gestionnaire de ressources du serveur de fichiers**.

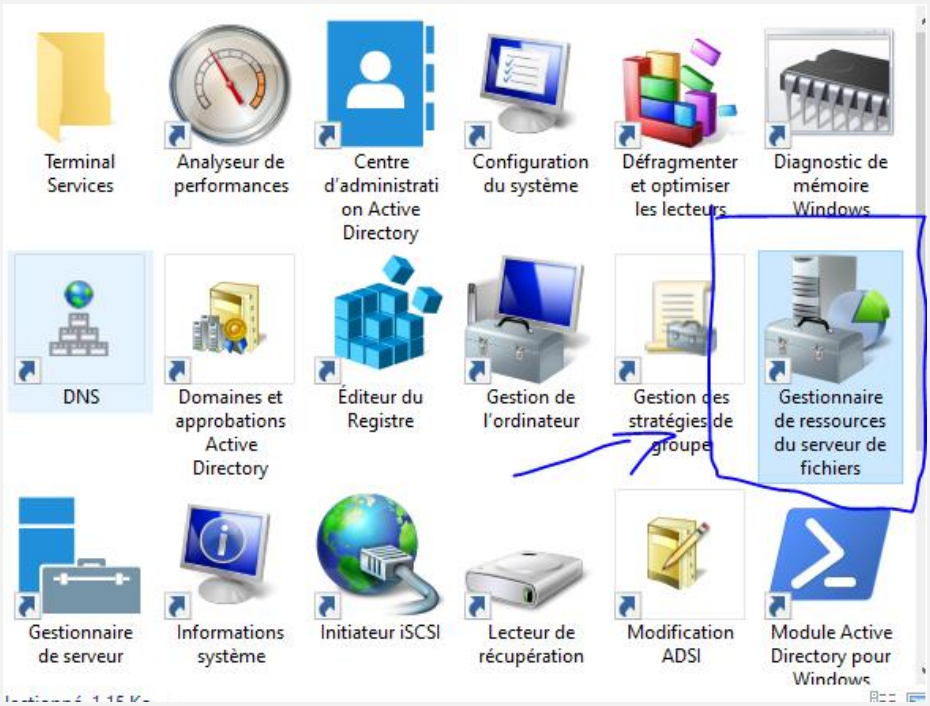


Validez aussi lorsque l'assistant vous propose d'installer les outils de gestion.

Poursuivez jusqu'à la fin de l'installation... Il n'y a rien de spécial à effectuer pour cette installation.



Une fois l'installation réalisée, dans les outils d'administration du serveur, vous devez trouver une nouvelle console nommée "**Gestionnaire de ressources du serveur de fichiers**" qui sera utile pour configurer toutes les fonctions relatives à FSRM.



B. Avec PowerShell

Pour effectuer l'installation en ligne de commande à partir d'une console PowerShell, la commande est la suivante :

```
Install-WindowsFeature -Name FS-Resource-Manager, RSAT-FSRM-Mgmt
```

Cette commande installe à la fois le rôle et la console de management FSRM.

V. Quotas d'annuaires et FSRM

À compter de Windows Server® 2003 R2, file server Resource Manager (FSRM) offre une gestion avancée des quotas et des répertoires. Le système de quota peut désormais être basé sur des répertoires, plutôt que défini par un utilisateur Windows. Cela permet de limiter rapidement et facilement la quantité de contenu chargé dans le répertoire racine d'un site Web, plutôt que de le configurer par utilisateur.

- Procédure d'Installation, de création et de définition de quotas

Sur le nœud **Gestion de quota** du composant logiciel enfichable MMC (Microsoft® Management Console) des outils de gestion de ressources pour serveur de fichiers, vous pouvez effectuer les tâches suivantes :

- Créer des quotas afin de limiter l'espace autorisé pour un volume ou un dossier et de générer des notifications quand les limites de quota sont approchées ou dépassées.
- Générer des quotas automatiques qui s'appliquent à tous les sous-dossiers existants d'un volume ou dossier et à tous les sous-dossiers créés par la suite.

- Définir des modèles de quota qui peuvent être facilement appliqués à de nouveaux volumes ou dossiers, puis utilisés au sein d'une organisation.

Par exemple, vous pouvez :

- Placer une limite de 200 mégaoctets (Mo) sur les dossiers de serveur personnel des utilisateurs, avec une notification par e-mail envoyée à vous-même et à l'utilisateur quand le volume de 180 Mo de stockage a été dépassé.
- Définir un quota flexible de 500 Mo sur le dossier partagé d'un groupe. Quand cette limite est atteinte, tous les utilisateurs du groupe sont avertis par e-mail que le quota de stockage a été temporairement augmenté à 520 Mo, pour leur permettre de supprimer les fichiers inutiles et de revenir dans les limites de stratégie de quota initiale de 500 Mo.
- Recevoir une notification quand un dossier temporaire atteint 2 gigaoctets (Go) d'utilisation, sans toutefois limiter le quota de ce dossier, car il est nécessaire pour un service s'exécutant sur votre serveur.

❖ Créer un quota basé sur un modèle

Les quotas peuvent être créés à partir d'un modèle ou avec des propriétés personnalisées. La procédure suivante décrit comment créer un quota basé sur un modèle (recommandé).

Lorsque vous créez un quota, vous choisissez un chemin d'accès de quota, c'est-à-dire un volume ou un dossier auquel s'applique la limite de stockage. Sur un chemin d'accès de quota donné, vous pouvez utiliser un modèle pour créer l'un des types de quota suivants :

- Quota unique qui limite l'espace pour l'intégralité d'un volume ou d'un dossier.
- Un quota d'application automatique, qui affecte le modèle de quota à un dossier ou à un volume.

Notes :

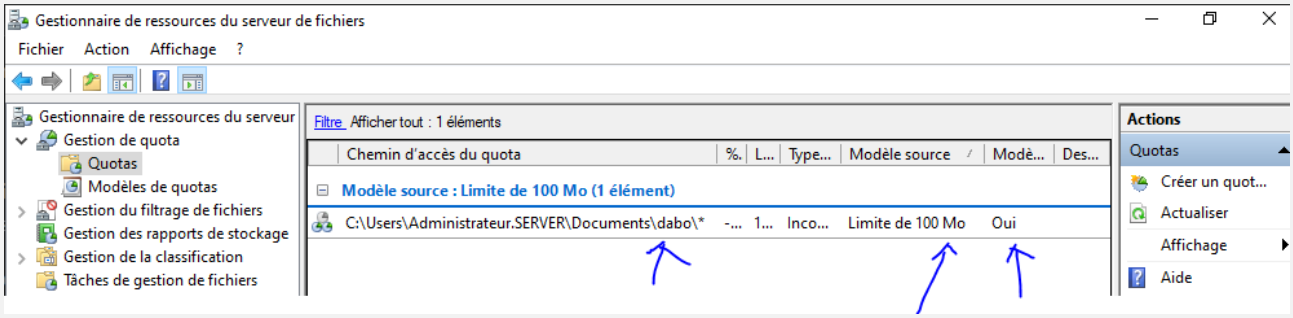
En créant des quotas exclusivement à partir de modèles, vous pouvez gérer vos quotas de manière centralisée en mettant à jour les modèles au lieu des quotas individuels. Ensuite, vous pouvez appliquer des modifications à tous les quotas basés sur le modèle modifié. Cette fonctionnalité simplifie l'implémentation des modifications de stratégie de stockage en fournissant un point central où toutes les mises à jour peuvent être effectuées.

Procédure :

1. Dans gestion de quota, cliquez sur le **nœud quotas**.
2. Cliquez avec le bouton droit sur **quotas**, puis cliquez sur créer un **quota** (ou sélectionnez créer un quota dans le volet actions). La boîte de dialogue créer un quota s'ouvre.
3. Sous **chemin d'accès du quota**, tapez le nom ou accédez au dossier parent auquel le profil de quota s'applique. Le quota d'application automatique sera appliqué à chacun des sous-dossiers (actuel et futur) dans ce dossier.

4. Cliquez sur **appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux**.
5. Sous **dériver les propriétés à partir de ce modèle de quota**, sélectionnez le modèle de quota que vous souhaitez appliquer dans la liste déroulante. Notez que les propriétés de chaque modèle sont affichées sous **Résumé des propriétés de quota**.
6. Cliquez sur Créer.

Exemple :

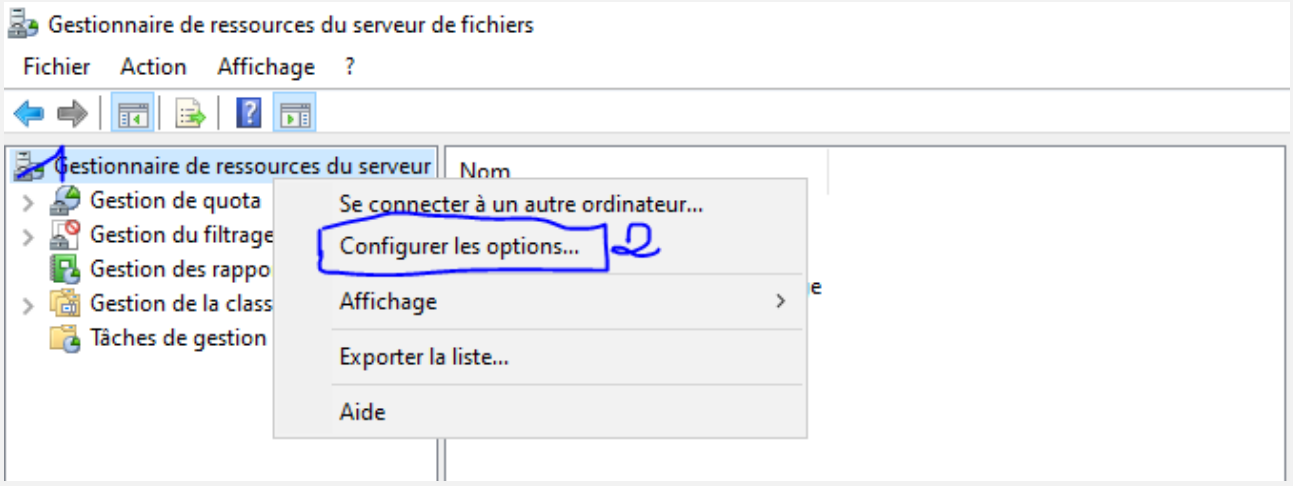


Pour en savoir plus : [Gestion des quotas | Microsoft Learn]

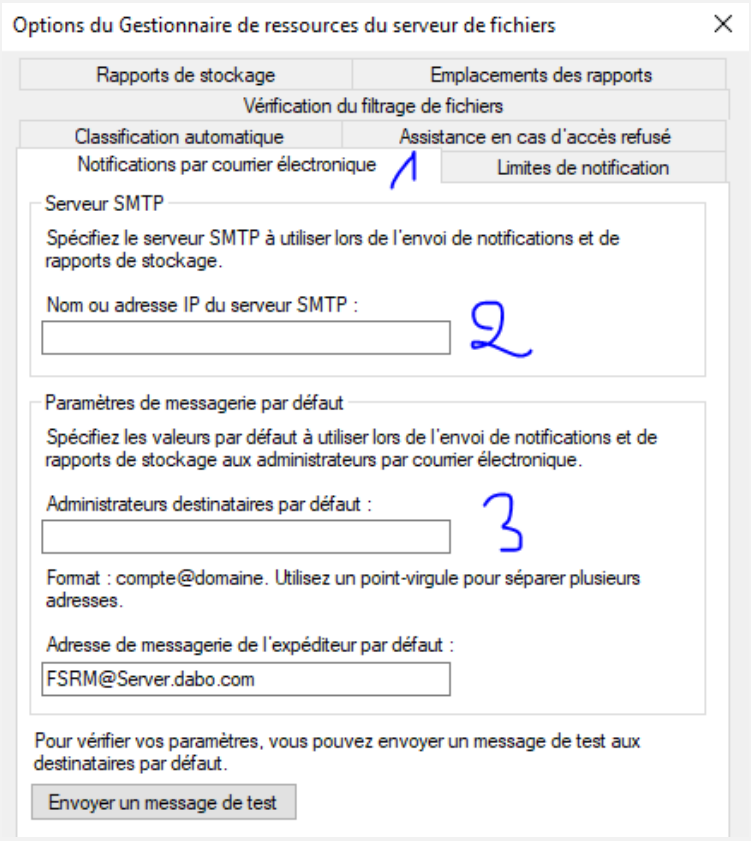
VI. Configurer les notifications par email dans FSRM

La configuration du serveur SMTP permet de recevoir un email lors qu'un fichier interdit essaie d'être copié sur le serveur ou d'avertir lors de l'approche de la limite du quota …

Depuis la console faire un clic droit sur le **Gestionnaire de ressources du serveur de fichiers 1** et cliquer sur Configurer les options **2**.

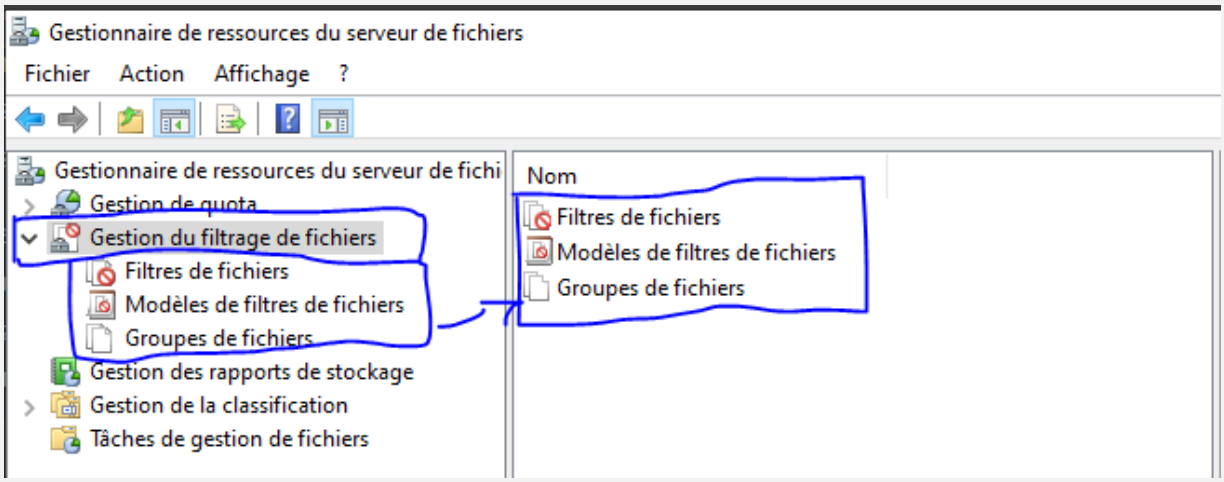


Aller sur l'onglet Notification par courrier électronique **1**, entrer le serveur SMTP **2** et un destinataire **3**. Il est possible de tester la configuration **A**. Cliquer sur OK pour valider.



VII. Gestion du filtrage de fichiers

Sur le nœud **gestion du filtrage des fichiers** du serveur de fichiers gestionnaire des ressources composant logiciel enfichable MMC,



Vous pouvez effectuer les tâches suivantes :

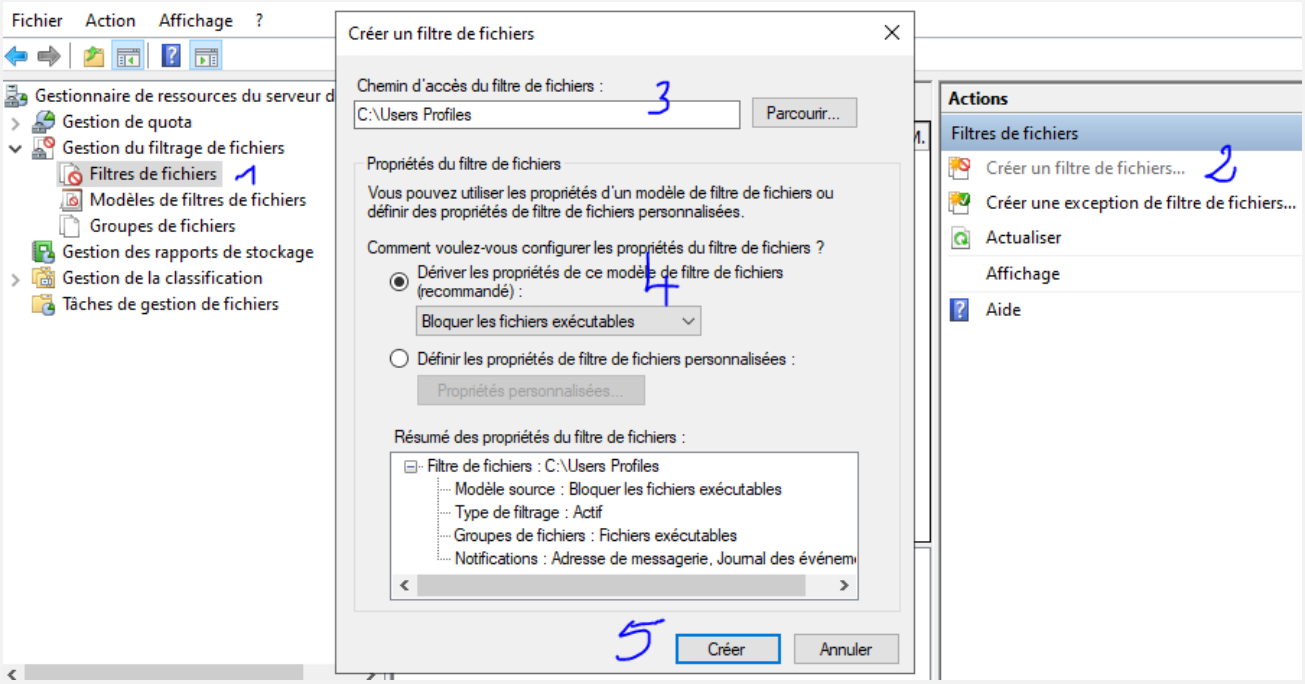
- Créer des filtres de fichiers pour contrôler les types de fichiers que les utilisateurs peuvent enregistrer et générer des notifications lorsque les utilisateurs essaient d'enregistrer des fichiers non autorisés.
- Définissez les modèles de filtrage de fichiers qui peuvent être appliqués aux nouveaux volumes ou dossiers et qui peuvent être utilisés dans une organisation.

- Créez des exceptions de filtrage de fichier qui étendent la flexibilité des règles de filtrage de fichiers.

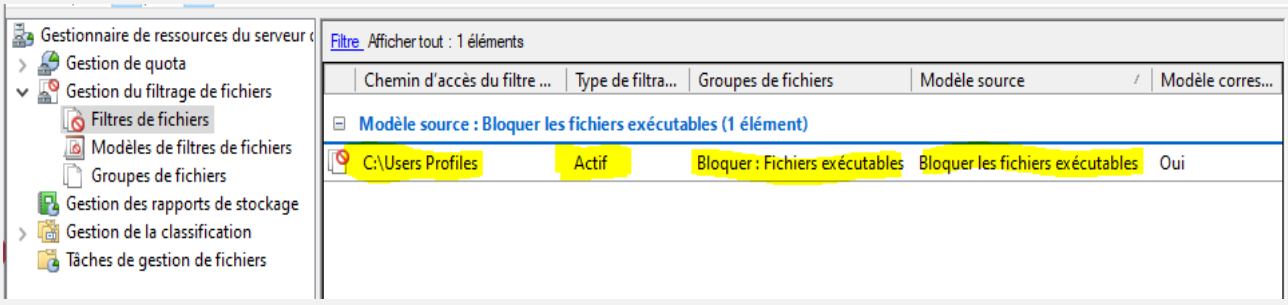
A. Utiliser un filtre prédéfini

Dans cette partie, nous allons voir comment ajouter un filtre de fichier prédéfini (bloquer les fichiers exécutables) sur le répertoire qui contient les profils utilisateurs.

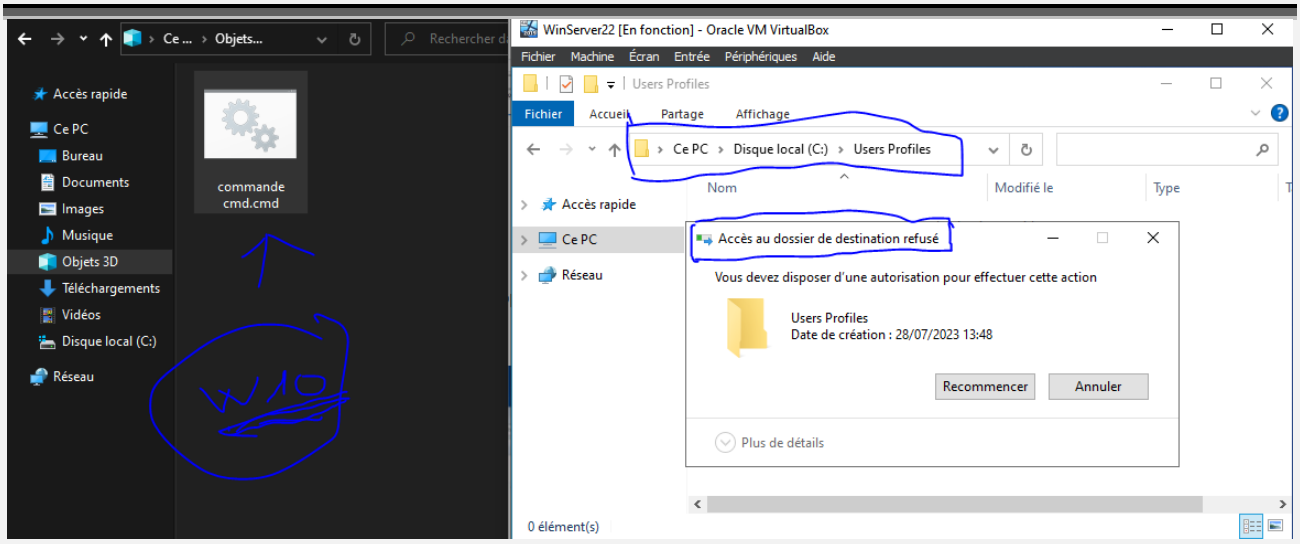
Depuis la console, aller sur **Gestion du filtrage de fichiers** > **Filtre de fichiers** 1 et cliquer sur **Créer un filtre de fichier...** 2. Sélectionner ou entrer le chemin **3** du dossier où le filtre doit être appliqué. Sélectionner le filtre 4 (Bloquer les fichiers exécutables) et cliquer sur le bouton Créer 5.



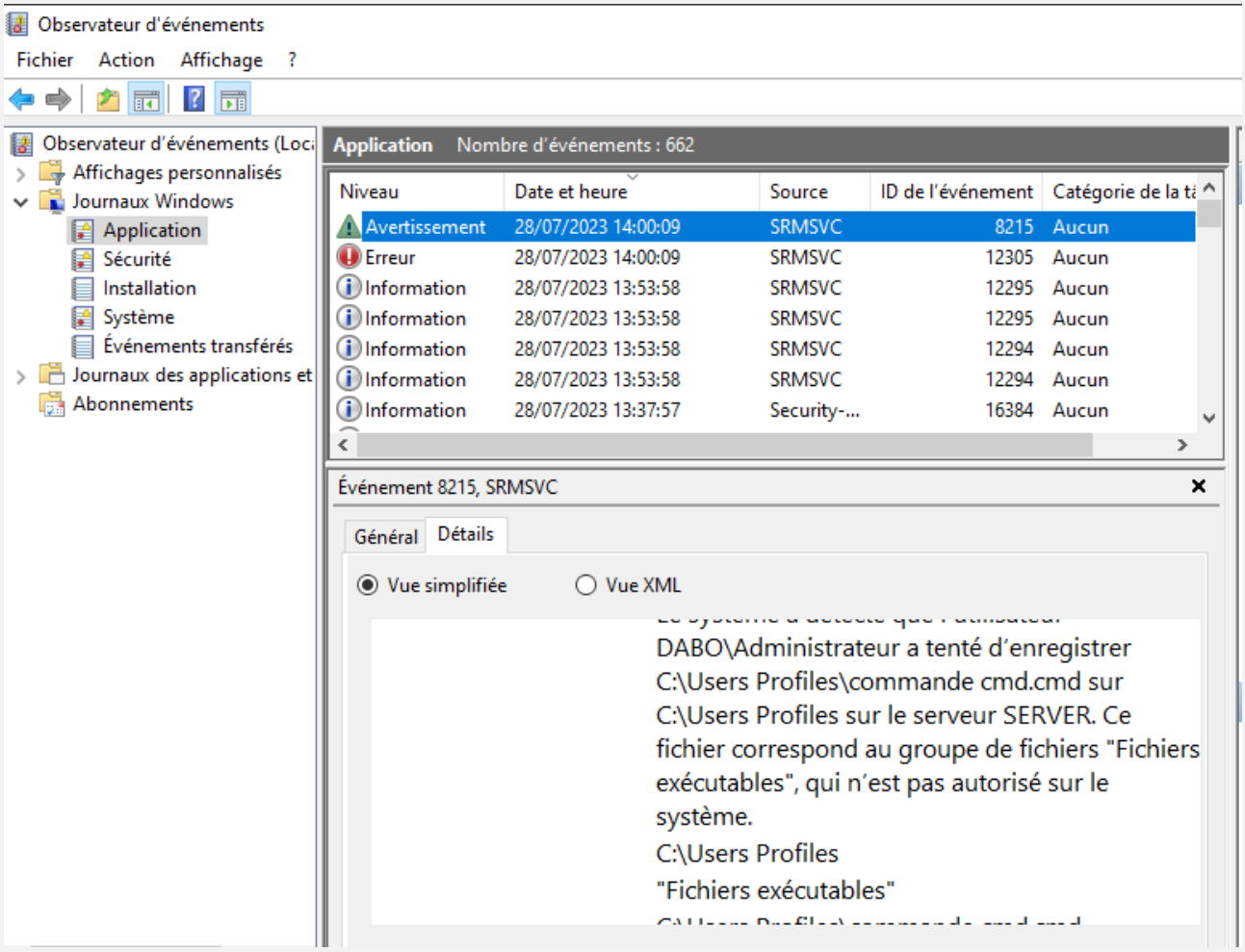
Le filtre est actif :



Depuis un **poste client Windows10**, j'ai copié un exécutable (**.cmd**) dans le dossier **''Users Profiles''**. Voici le message qui s'affiche :



Depuis l'observateur d'événement il est également possible de voir le message FSRM sous l'ID **8215.**



Si un serveur SMTP est configuré, un email est envoyé pour notifier l'action.

B. Utiliser un filtre personnalisé (cas ransomware)

Pour illustrer cette partie, nous allons créer un groupe de fichiers qui contient les extensions connus des cryptolocker, puis créer un modèle de filtrage et ensuite l'appliquer à un lecteur.

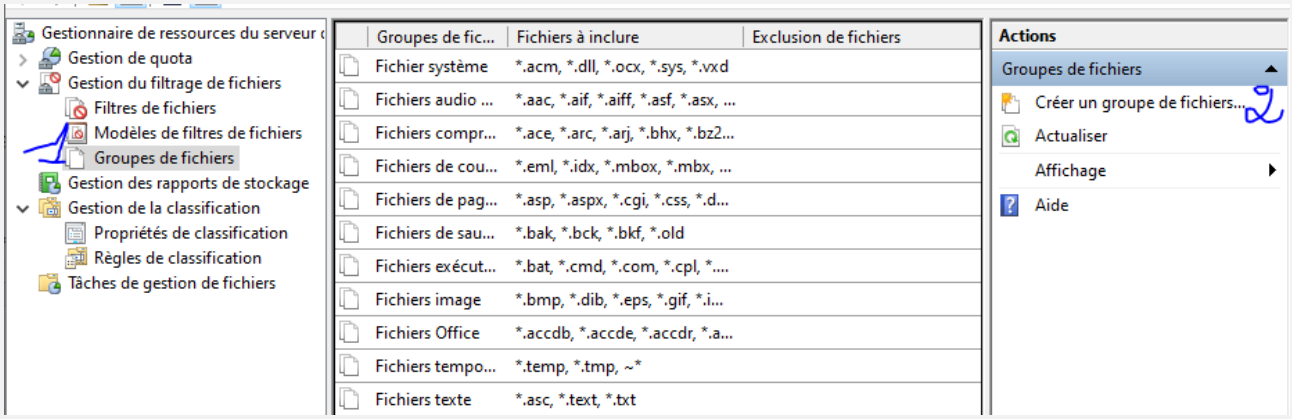
Avec ce filtre, il ne sera pas possible au virus d'écrire les fichiers cryptés sur le serveur.

L'utilisation d'un filtre personnalisé passe par 3 étapes :

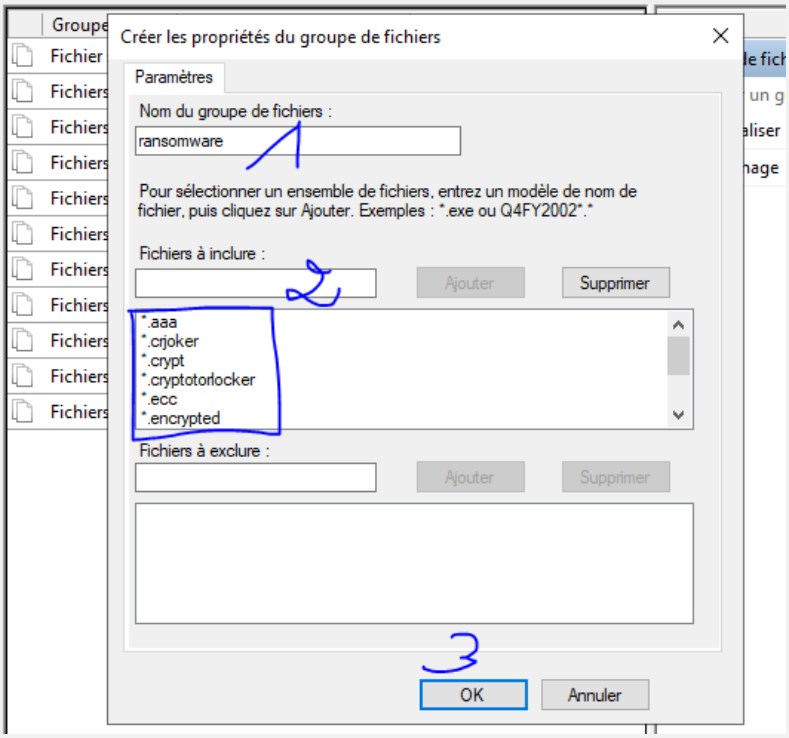
- La création d'un groupe de fichiers, qui va contenir l'ensemble des extensions des cryptolockers. Les groupes peuvent être utilisés dans plusieurs modèles.
- Un modèle de filtre de fichiers, qui a pour but de choisir le type de filtrage (actif/passif) ainsi que la configuration des notifications.
- Un filtre de fichiers, qui est l'application du modèle à un emplacement sur le serveur.

1. Création d'un groupe de fichiers

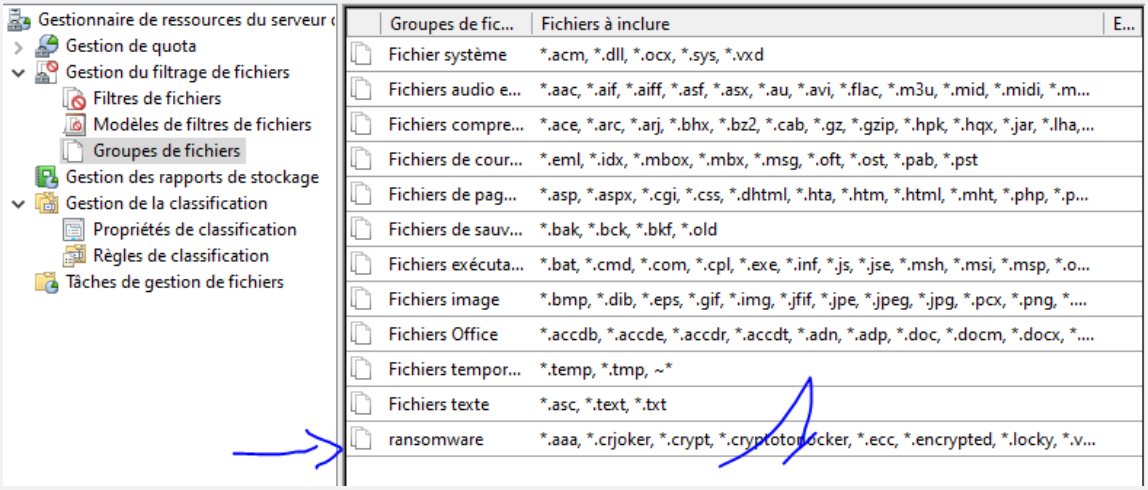
Depuis la console, aller sur **Gestion du filtrage de fichiers > Groupe de fichiers** 1. Faire un clic droit dans la zone centrale et cliquer sur **Créer un groupe de fichiers...** 2 ou passer par le menu Actions.



Nommer le groupe 1, entrer les extensions des fichiers à bloquer sous la forme *.extension 2 et cliquer sur le bouton OK 3.

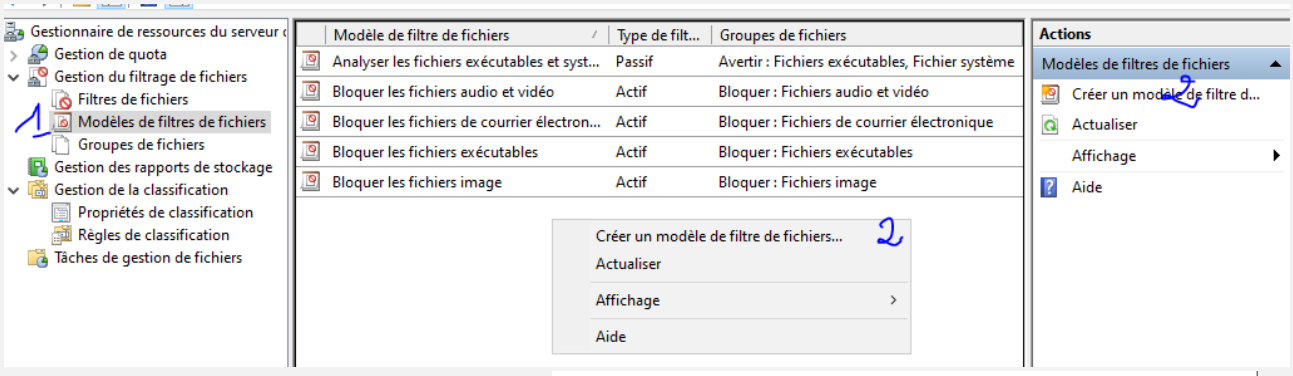


Le groupe est ajouté **1**.

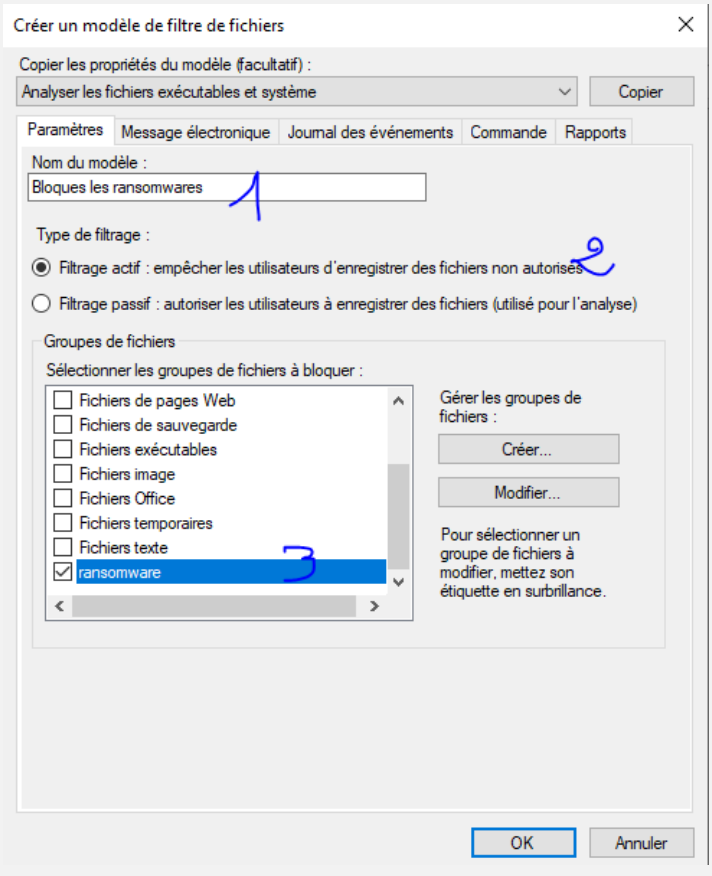


2. Création du modèle de filtre de fichiers

Aller sur Modèle de filtres de fichiers 1, faire clic droit puis cliquer sur **Créer un modèle de filtre de fichiers ...** 2 ou passer par le menu Actions.

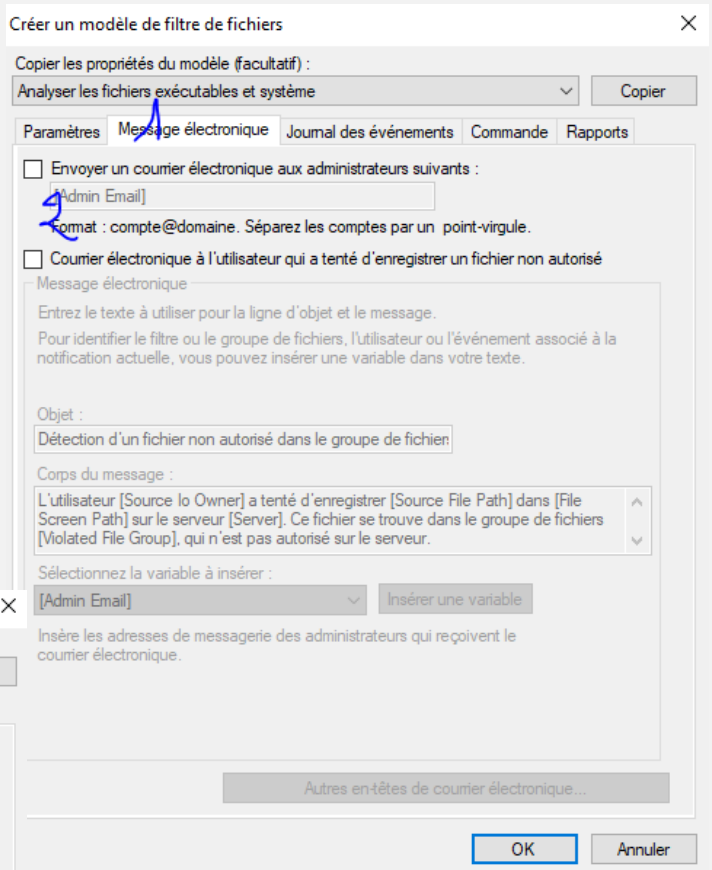


Nommer le modèle 1, choisir comment le filtre est appliqué* 2 puis sélectionner le/les groupes de fichiers 3 qui compose le modèle.

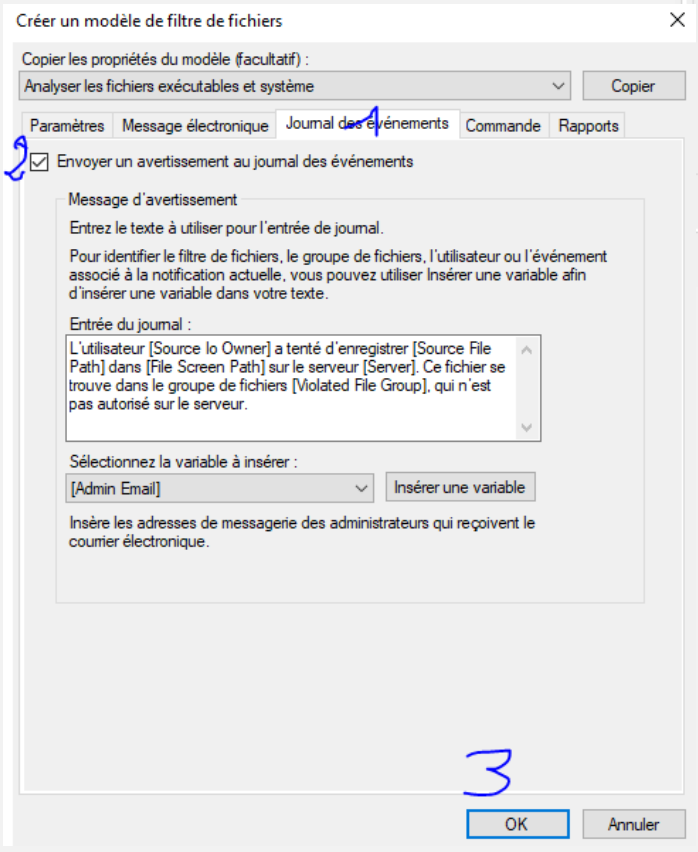


Note :

** Il y a deux types de filtrage, le filtre **actif** va empêcher l'écriture du type de fichiers, le mode **passif** est utilisé à des fins d'audit.*

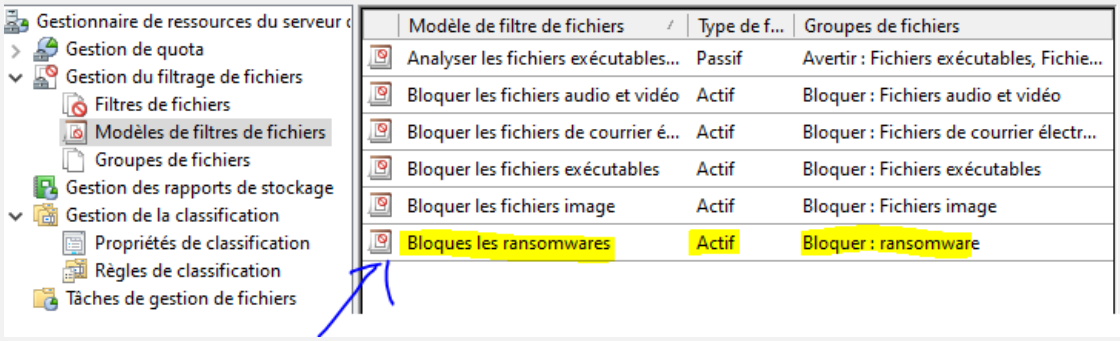


Passer sur l'onglet Message électronique 1 et cocher 2 les alertes e-mail si besoin.



Aller sur l'onglet Journal des événements et cocher la case Envoyer un avertissement au journal des événements 2. Cliquer sur le bouton OK 3 pour valider la création du modèle.

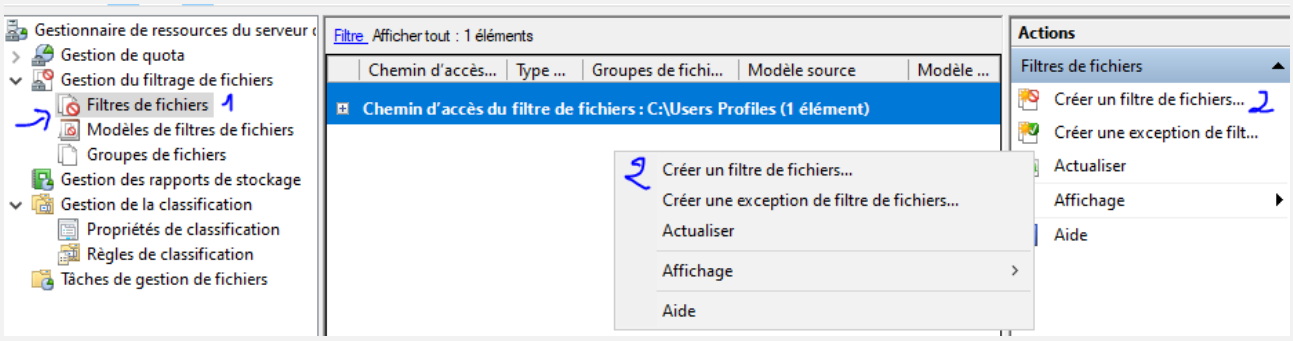
Le modèle **1** est disponible dans la liste.



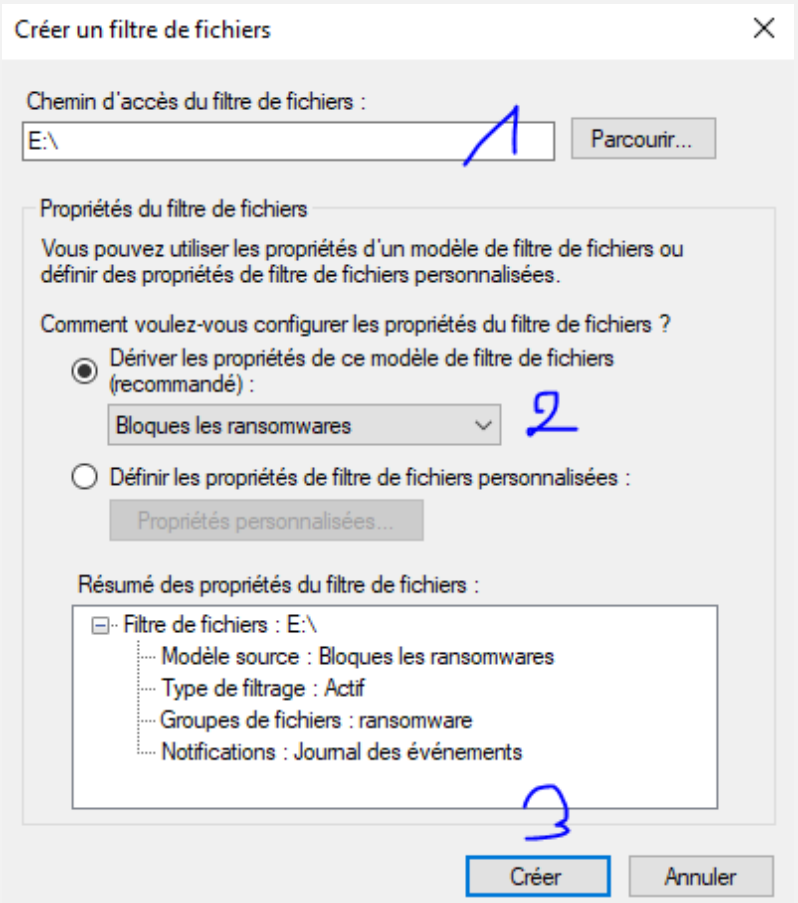
3. Appliquer un filtre de fichiers

Dans cette partie, nous allons voir comment appliquer un filtre de fichiers en utilisant le groupe créer précédemment.

Aller sur Filtres de fichiers 1 et créer en un nouveau 2.



Indiquer le chemin racine où doit être appliqué le filtre 1, sélectionner le filtre 2 et cliquer sur Créer 3.



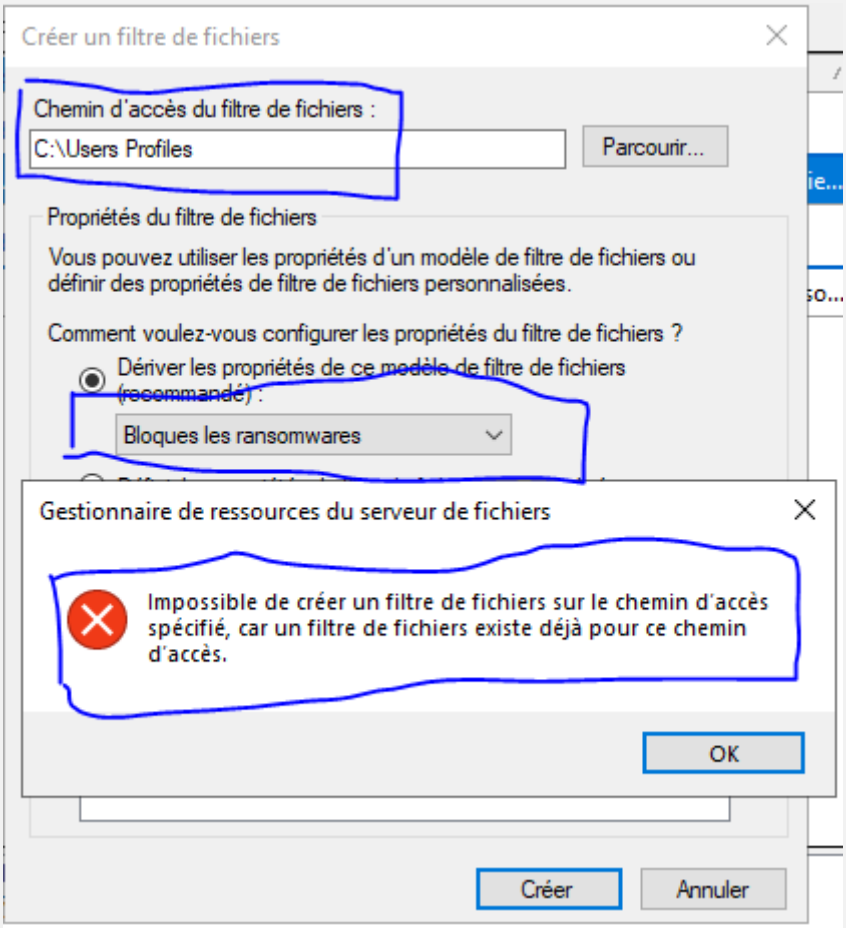
Le filtre est créé, de cette manière la création de fichiers cryptés est bloquée sur la partition D du serveur.

VIII. Troubleshooting

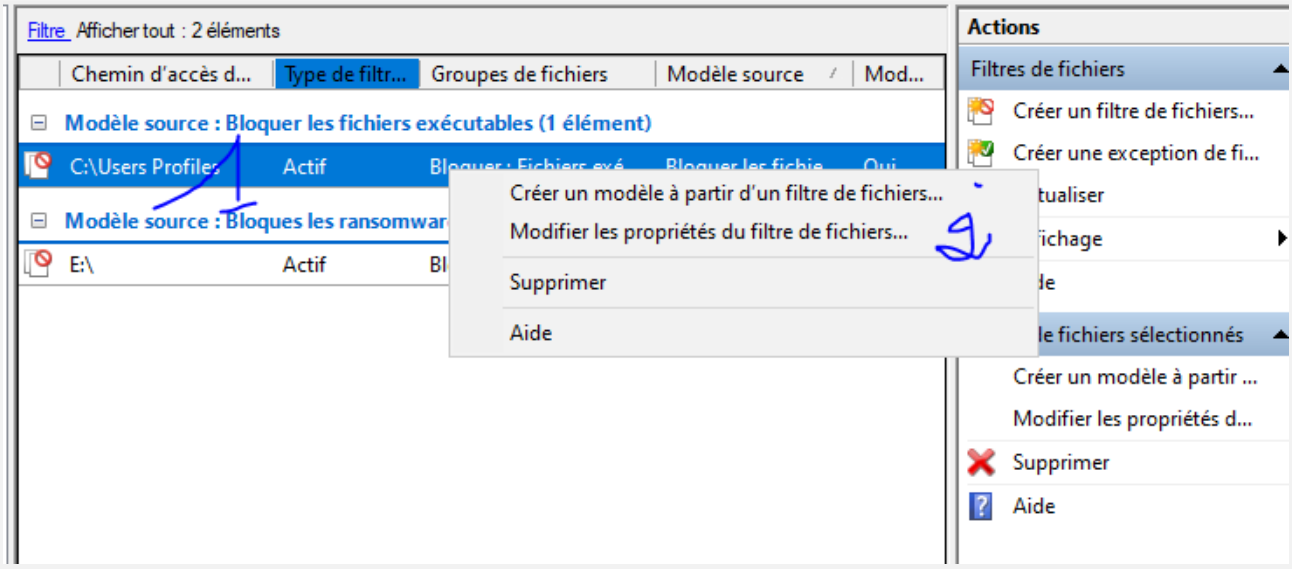
Appliquer plusieurs filtres sur un même dossier

Il n'est pas possible de créer plusieurs filtres différents sur un même dossier.

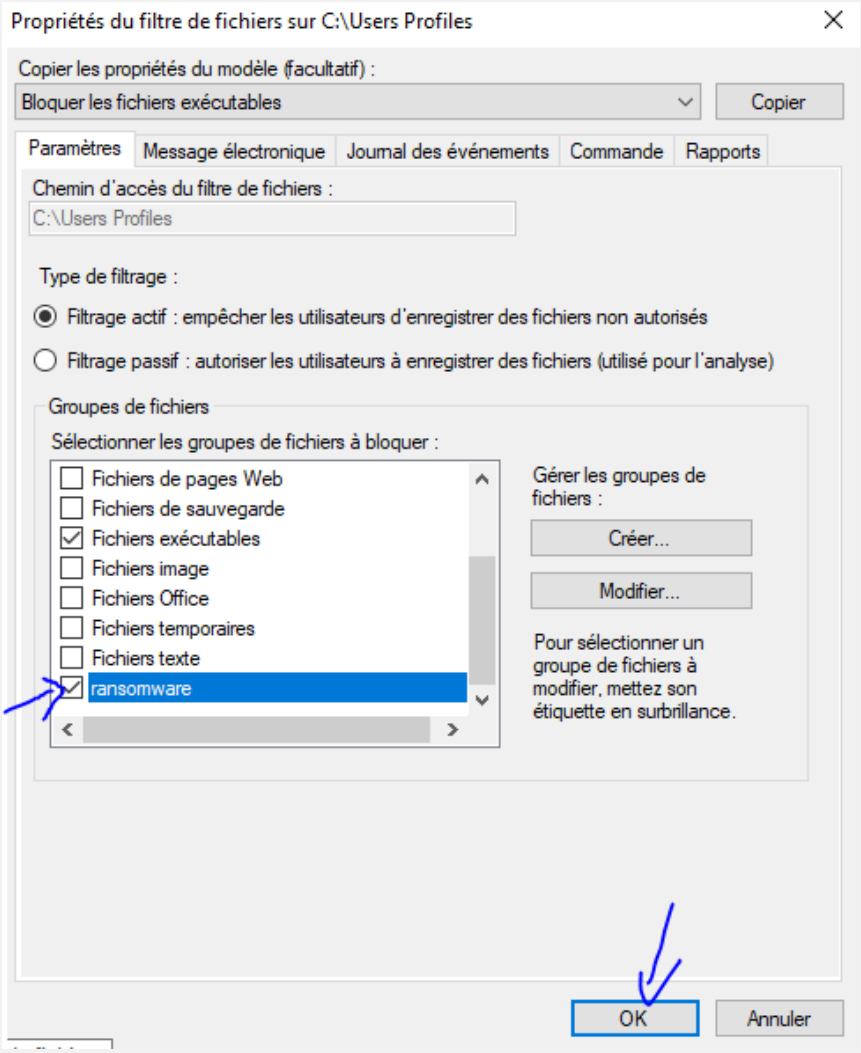
Voici le message d'erreur que vous aurez : *Impossible de créer un filtre de fichiers sur le chemin d'accès spécifié, car un filtre de fichier existe déjà pour ce chemin d'accès.*



Pour ajouter le blocage des ransomwares sur le dossier '**Users Profiles'**, Sélectionner le filtre **1** et faire un clic droit dessus puis cliquer sur *Modifier les propriétés du filtre de fichiers…*



Cocher les groupes que vous souhaitez filtrer. Dans notre cas c'est le groupe **'ransomware'** et cliquer sur OK.



Depuis la liste, on voit que le filtre est appliqué sur plusieurs groupes de fichiers