Travaux pratiques - Contrôle et gestion des ressources système sous Windows 8

Introduction

Au cours de ces travaux pratiques, vous allez utiliser des outils d'administration pour contrôler et gérer les ressources système.

Équipements recommandés

- Un ordinateur équipé de Windows 8 avec accès Internet

Étape 1 : Arrêtez et démarrez un service sous Windows.

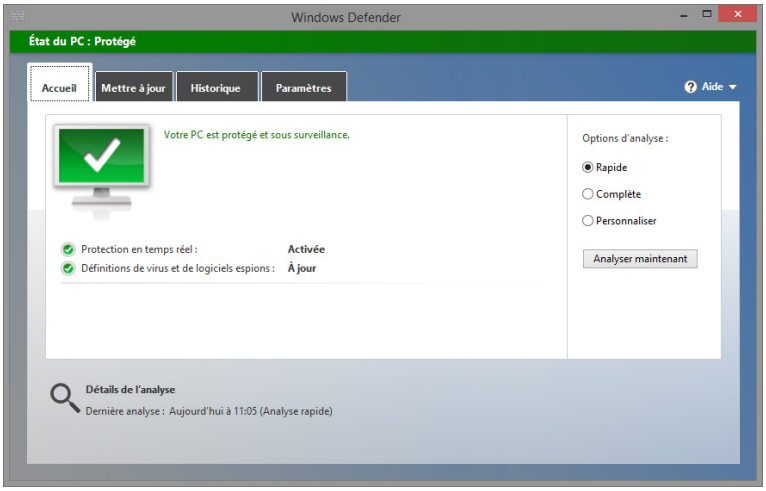
Vous allez observer ce qui se produit lorsqu'un service est arrêté, puis démarré.

a. Ouvrez une session Windows en tant qu'administrateur.

Remarque : certains logiciels antivirus ou anti-espion doivent être désinstallés pour que Windows Defender fonctionne.

b. Pour savoir si Windows Defender est désactivé, cliquez sur **Démarrer** dans le champ **Rechercher les programmes et fichiers**, tapez **Defender** et sélectionnez **Windows Defender**. **Windows Defender** doit être en cours d'exécution.

Remarque : sous Windows 8.0, cliquez sur **Rechercher**, tapez **Defender**, puis sélectionnez **Windows Defender**.

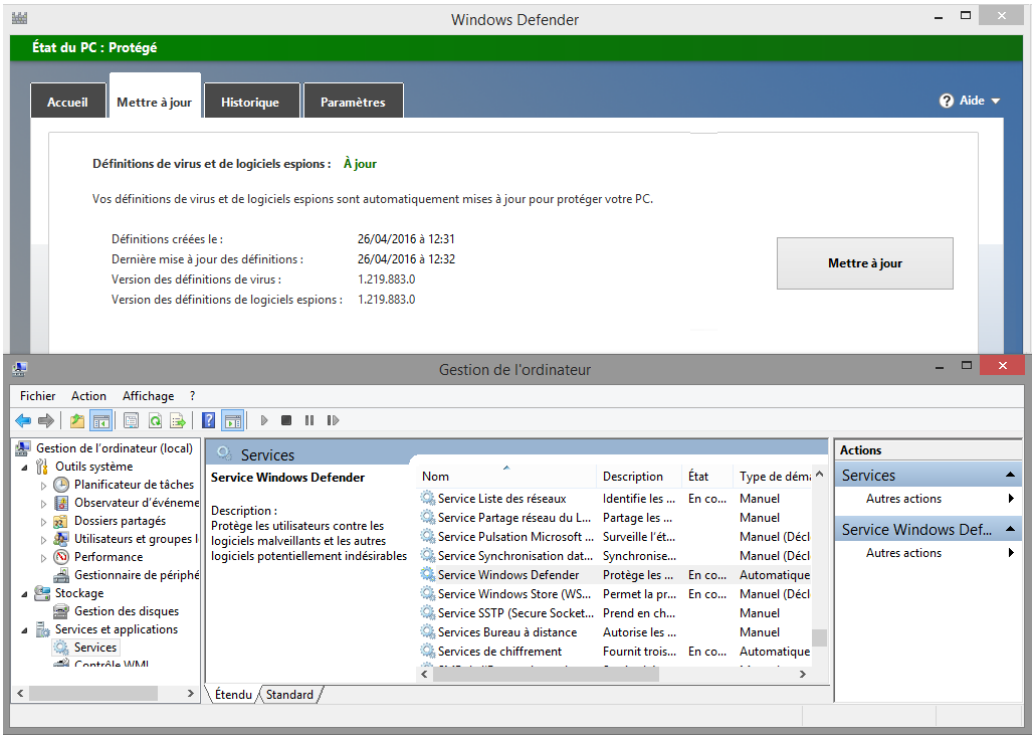


Remarque : si **Windows Defender** n'est pas en cours d'exécution, une fenêtre d'avertissement s'ouvre et **Windows Defender** ne démarre pas. Pour démarrer Windows Defender, cliquez sur **Panneau de configuration > Centre de maintenance**. Dans la section **Protection antivirus (Important)** de la fenêtre **Centre de maintenance**, cliquez sur **Activer maintenant**.

c. Sans fermer **Windows Defender,** ouvrez la console **Services**. Cliquez sur **Panneau de configuration > Outils d'administration > Gestion de l'ordinateur**.

d. La fenêtre **Gestion de l'ordinateur** s'affiche. Sous Services et applications, sélectionnez **Services**.

e. Fermez la fenêtre **Windows Explorer**, mais laissez ouvertes les fenêtres **Windows Defender** et **Gestion de l'ordinateur**. Redimensionnez et positionnez les deux fenêtres de manière à pouvoir les consulter en même temps.



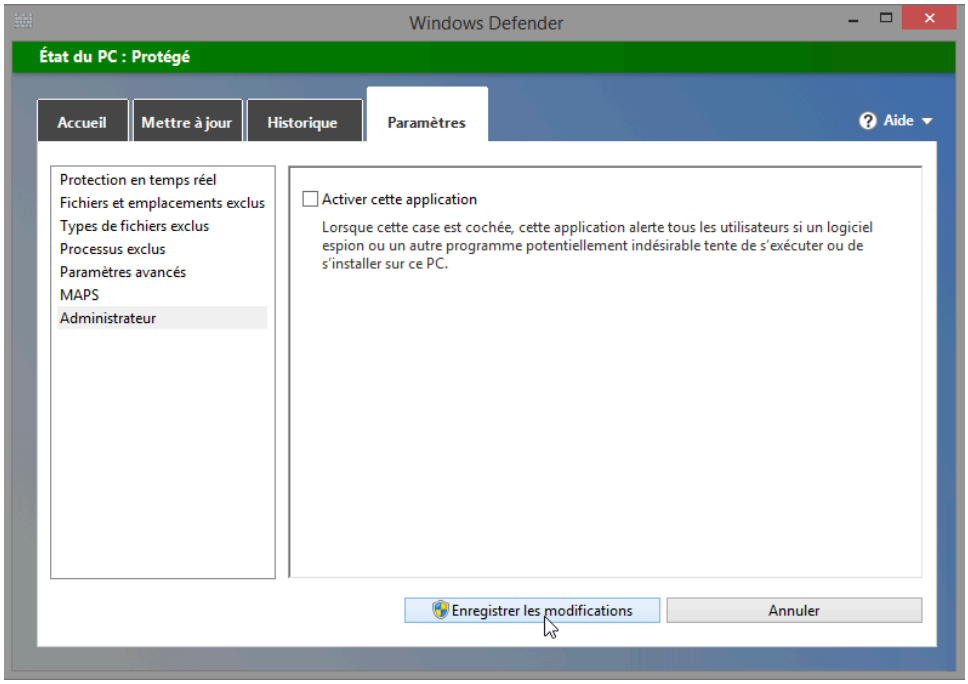
L'application Windows Defender peut-elle rechercher des mises à jour ? (Consultez l'onglet **Mettre à jour** pour répondre à la question)

f. Faites défiler le contenu de la fenêtre **Gestion de l'ordinateur** de manière à voir le **service Windows Defender**.

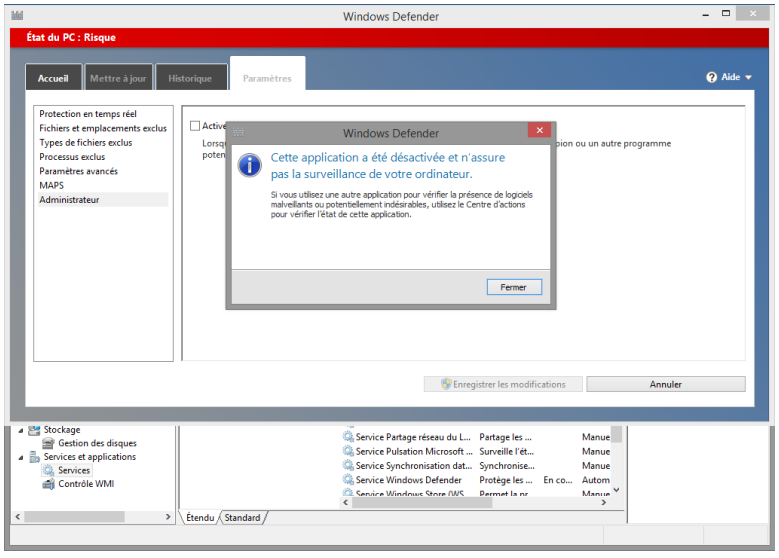
Quel est l'état de ce service ?

Remarque : alors que la plupart des services Windows peuvent être gérés via la console Services, il n'est pas possible d'arrêter **Windows Defender** depuis cette dernière sous Windows 8.

g. Pour que vous puissiez désactiver **Windows Defender**, la fenêtre **Windows Defender** doit être active. Sélectionnez l'onglet **Paramètres** et cliquez sur **Administrateur**. Décochez la case **Activer cette application**, puis cliquez sur **Enregistrer les modifications**.



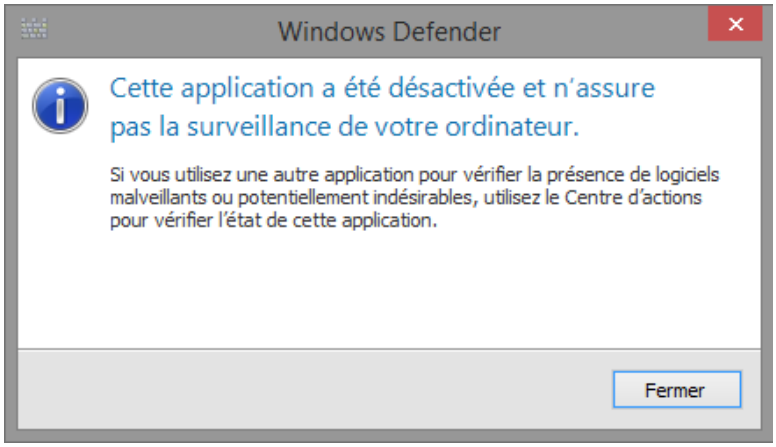
h. Une fenêtre d'avertissement s'ouvre. Cliquez sur **Fermer**. Notez que l'application **Windows Defender** se ferme complètement.



Remarque : vous arrêtez ce service tout simplement pour voir les conséquences de cette action. Lorsque vous arrêtez un service afin de libérer les ressources système qu'il utilise, vous devez bien comprendre en quoi cela affecte le fonctionnement global du système.

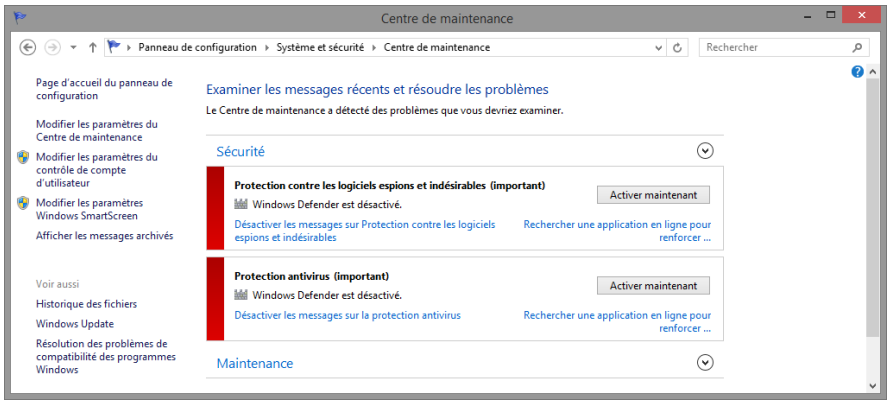
Remarque : bien que le service Windows Defender ne puisse pas être contrôlé via la fenêtre **Gestion de l'ordinateur**, l'état de Windows Defender continue d'être géré et de s'afficher. Pour actualiser la fenêtre **Gestion de l'ordinateur**, appuyez sur **F5**.

i. À présent que le service **Windows Defender** est arrêté, essayez d'exécuter de nouveau **Windows Defender** en cliquant sur **Rechercher**. Tapez **Defender**, puis sélectionnez **Windows Defender**.

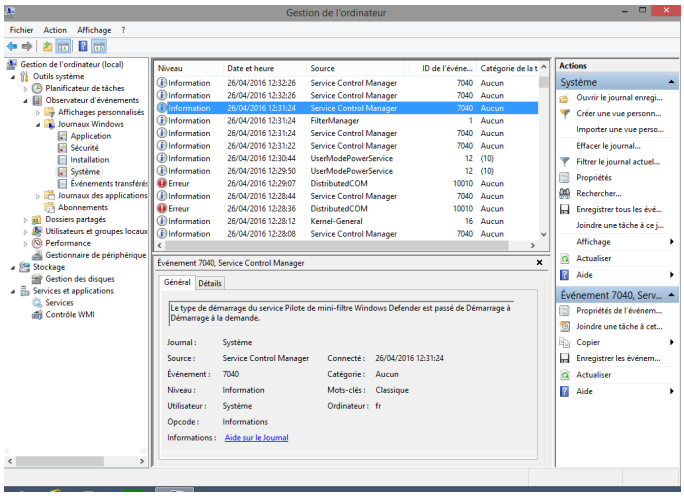


Que faut-il faire pour que Windows Defender puisse s'exécuter ?

j. Démarrez le service Windows Defender dans le **Centre de maintenance**. Cliquez sur **Panneau de configuration > Centre de maintenance**. Dans la section **Protection antivirus (Important)**, cliquez sur **Activer maintenant**.



k. La fenêtre **Windows Defender** s'ouvre et le service doit être de nouveau en cours d'exécution. Fermez la fenêtre **Windows Defender** et assurez-vous que la fenêtre Gestion de l'ordinateur est ouverte.

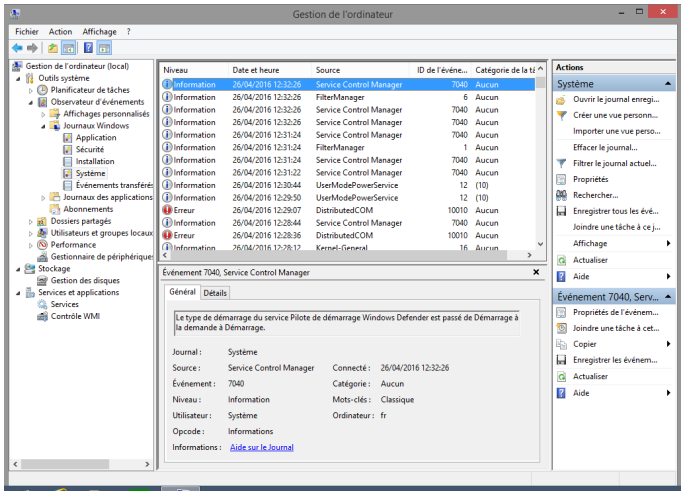


l. Sélectionnez **Observateur d'événements > Journaux Windows > Système**.

m. Sélectionnez le deuxième événement **Gestionnaire de contrôle des services** de la liste.

Regardez dans l'onglet Général et expliquez ce qu'il est advenu du service Windows Defender.

n. Cliquez sur la flèche vers le haut sur le clavier ou sélectionnez l'événement situé juste au-dessus de celui que vous venez de consulter.



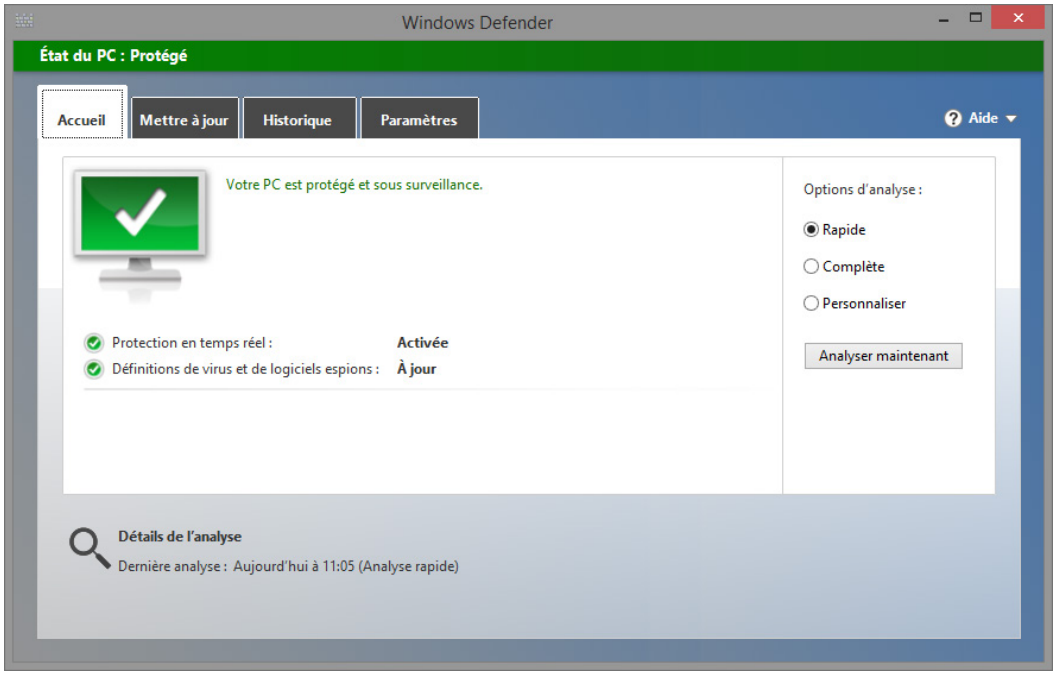
Regardez dans l'onglet Général et expliquez ce qu'il est advenu du service Windows Defender.

o. Fermez toutes les fenêtres ouvertes.

Étape 2 : Découvrez l'impact des services.

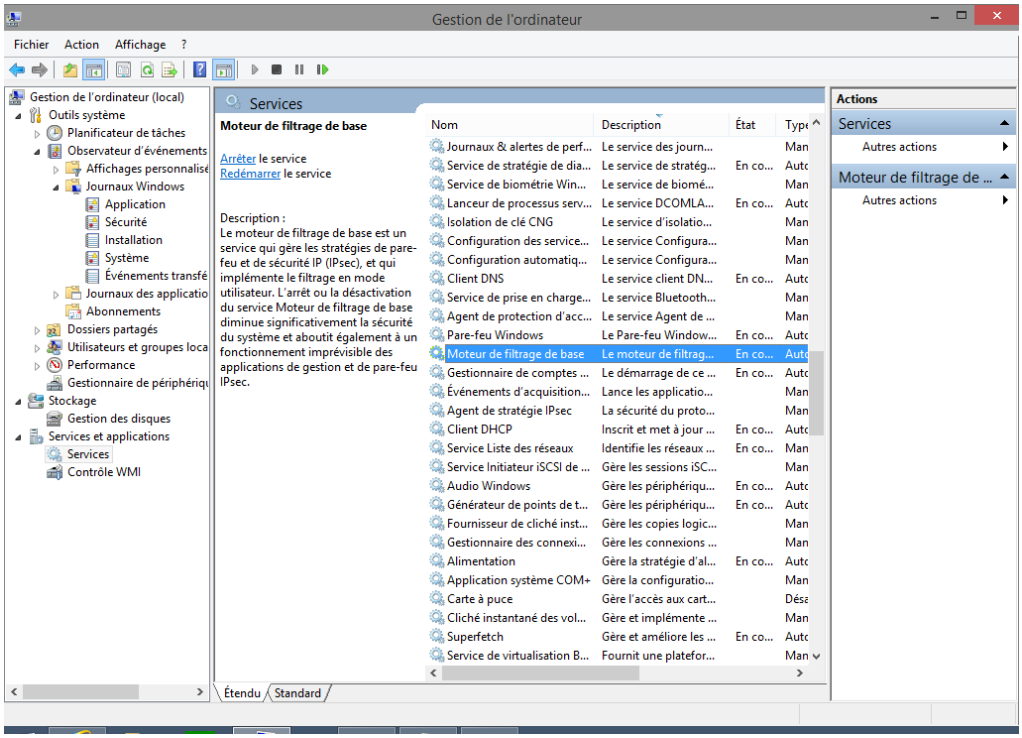
Dans cette section, vous allez arrêter le **Moteur de filtrage de base Windows (Base Filtering Engine, BFE)**, analyser l'impact sur le système, puis redémarrer le BFE. Le BFE assure la gestion du pare-feu et d'autres stratégies de sécurité sous Windows. Il constitue un service Windows important, car de nombreux autres services en dépendent.

a. Vérifiez que **Windows Defender** est en cours d'exécution en cliquant sur **Panneau de configuration > Windows Defender**.

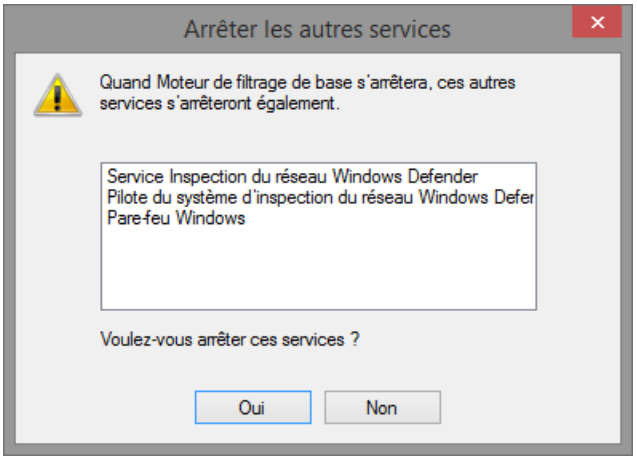


b. Ouvrez l'utilitaire Gestion de l'ordinateur. Cliquez sur **Panneau de configuration > Outils d'administration > Gestion de l'ordinateur**. Sélectionnez **Service** et recherchez le service **Moteur de filtrage de base**.

c. Arrêtez le service BFE en cliquant avec le bouton droit, puis en sélectionnant **Arrêter**. Vous pouvez également cliquer sur le bouton d'arrêt de la barre d'outils supérieure de la **Console des services** alors que le BFE est sélectionné.



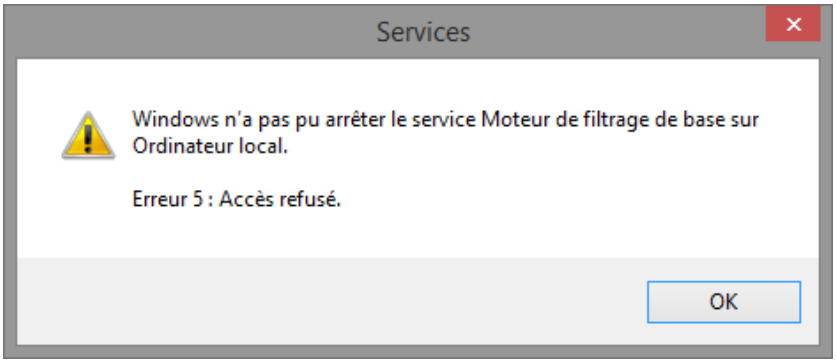
d. Windows affiche un message d'avertissement indiquant l'ensemble des services qui dépendent du BFE. Cliquez sur **Oui** pour arrêter le BFE et les services dépendants.



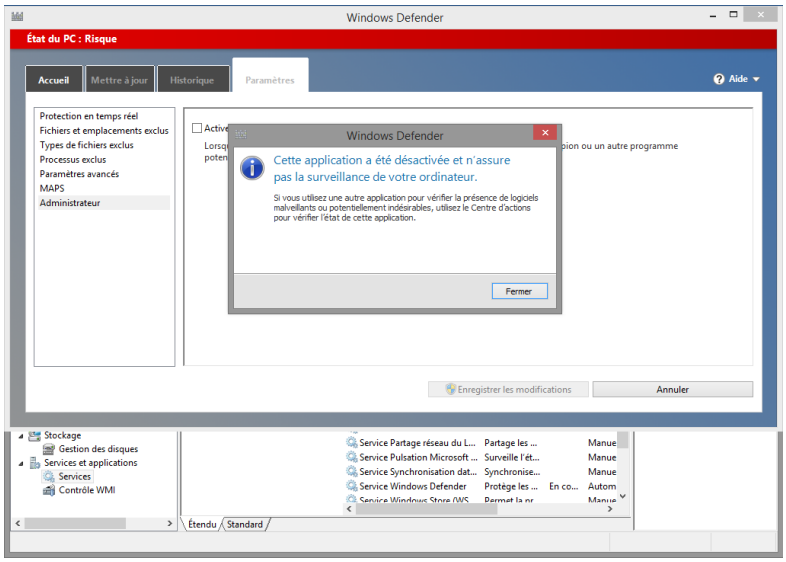
Remarque : les services répertoriés peuvent différer de ceux contenus dans le message d'avertissement.

e. Windows ne devrait pas vous laisser arrêter le BFE si le service **Windows Defender** s'affiche dans la fenêtre **Arrêter les autres services**. **Windows Defender** ne pouvant pas être arrêté via la **Console des services**, le BFE ne peut pas non plus l'être.

Remarque : si cette fenêtre d'erreur ne s'affiche pas, passez à la **sous-étape h**.



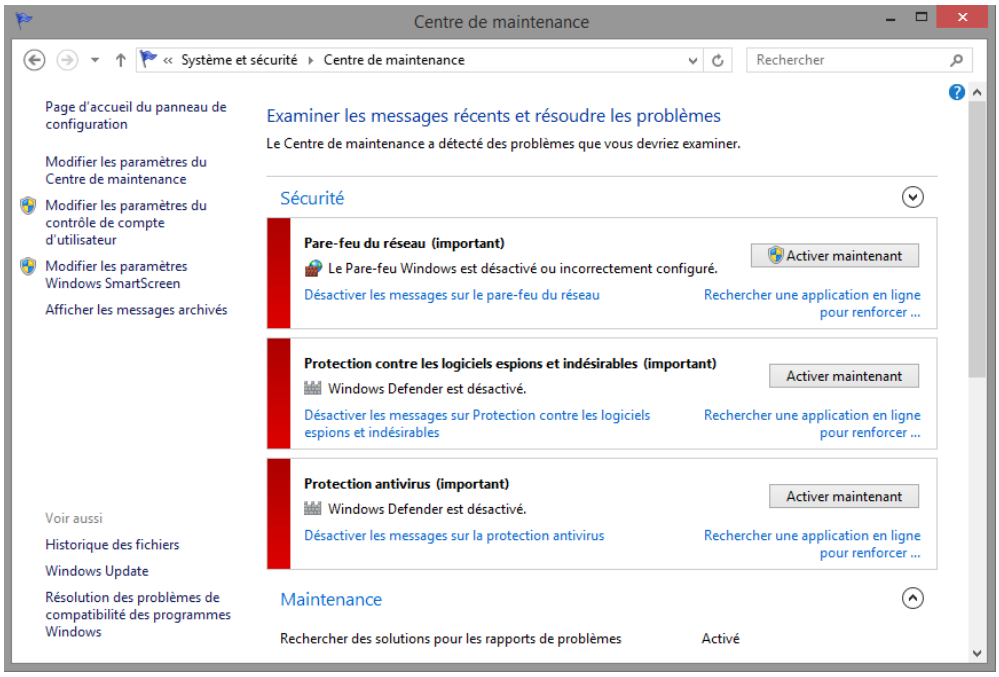
f. Pour arrêter le BFE, vous devez d'abord arrêter **Windows Defender**. Ouvrez **Windows Defender**, puis cliquez sur **Arrêter** dans l'onglet **Paramètres**. Reportez-vous au début de ces travaux pratiques pour plus de détails.



g. Une fois **Windows Defender** arrêté, ouvrez la **Console des services**, puis arrêtez le BFE. Cliquez avec le bouton droit sur le service BFE, puis sélectionnez **Arrêter**.

Qu'indique la colonne d'état de la **Console de services** pour le service BFE ?

h. Étant donné que plusieurs services de sécurité dépendent du BFE, des alertes sont émises qui peuvent être consultées dans le **Centre de maintenance**.



Remarque : les problèmes répertoriés peuvent différer de ceux contenus dans ce message d'avertissement.

Pourquoi est-ce important d'être très attentif lors de la gestion des services ?

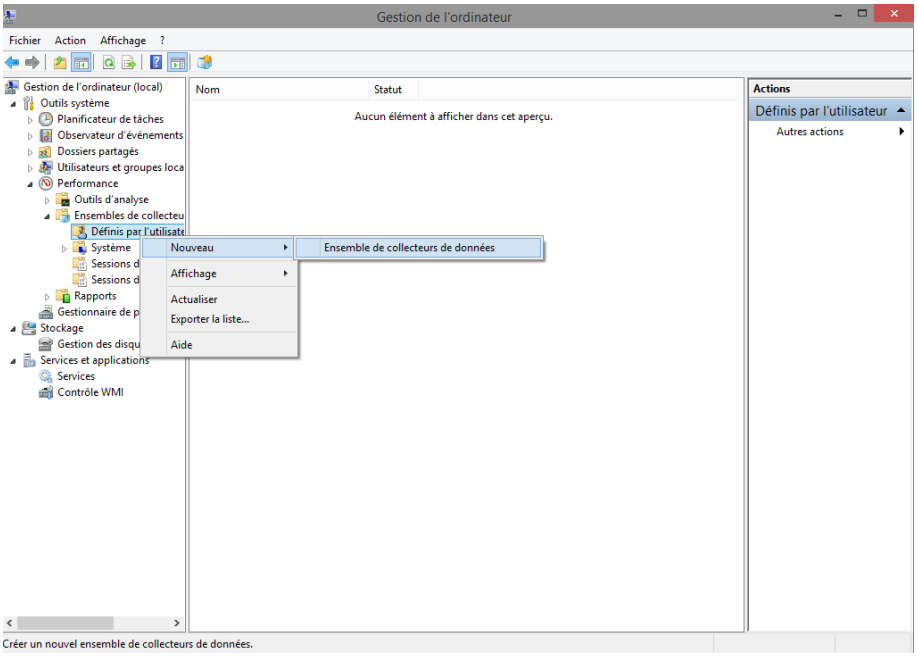
i. Pour redémarrer un service arrêté à partir du **Centre de maintenance**, sélectionnez-le et cliquez sur **Activer maintenant**.

Étape 3 : Configurez les fonctionnalités avancées dans les outils d'administration.

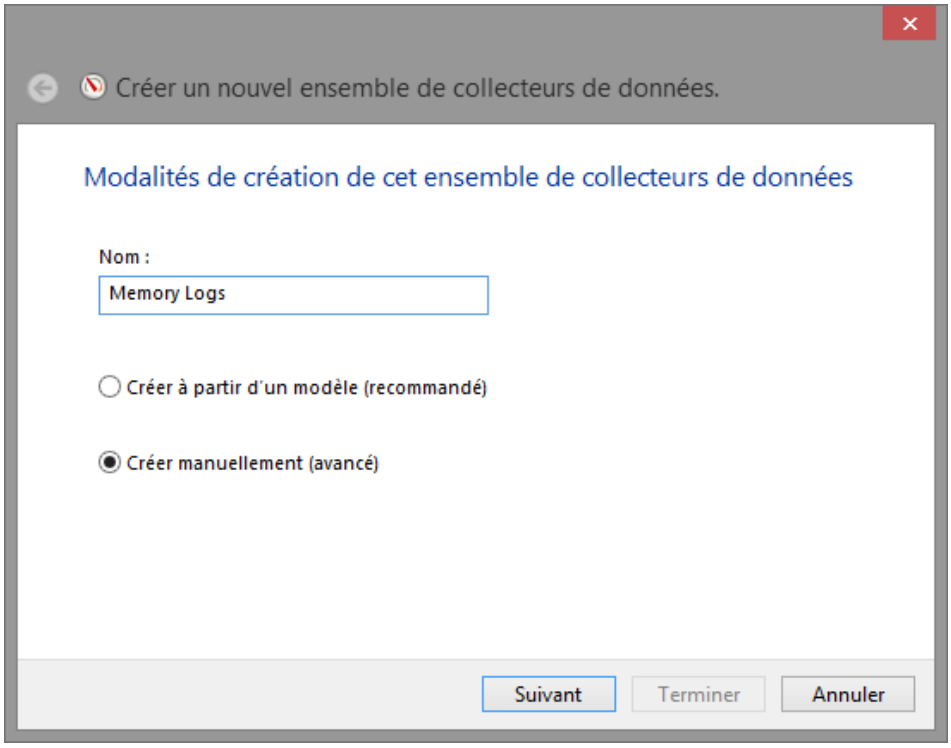
Pour la suite de ces travaux pratiques, vous allez configurer les fonctionnalités avancées de l'outil d'administration et contrôler l'impact sur l'ordinateur.

a. À partir de l'**Explorateur Windows**, cliquez avec le bouton droit sur **Ce PC** et sélectionnez **Gérer**. La fenêtre **Gestion de l'ordinateur** s'affiche.

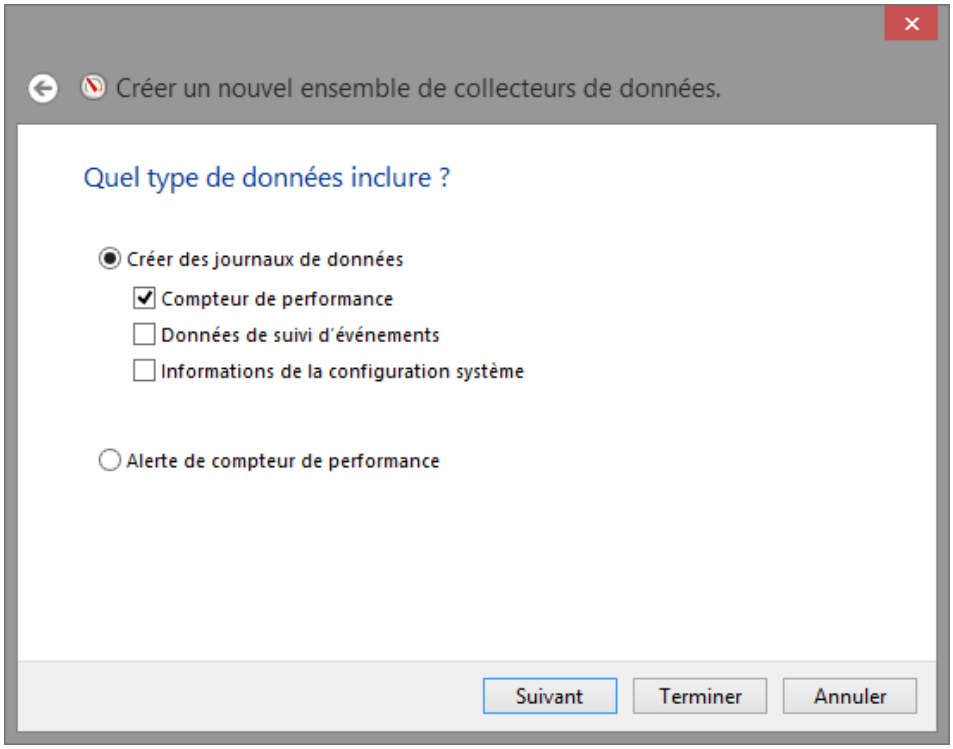
b. Allez dans **Outils système > Performances > Ensembles de collecteurs de données**. Cliquez avec le bouton droit sur **Définis par l'utilisateur**, puis cliquez sur **Nouveau > Ensemble de collecteurs de données**.



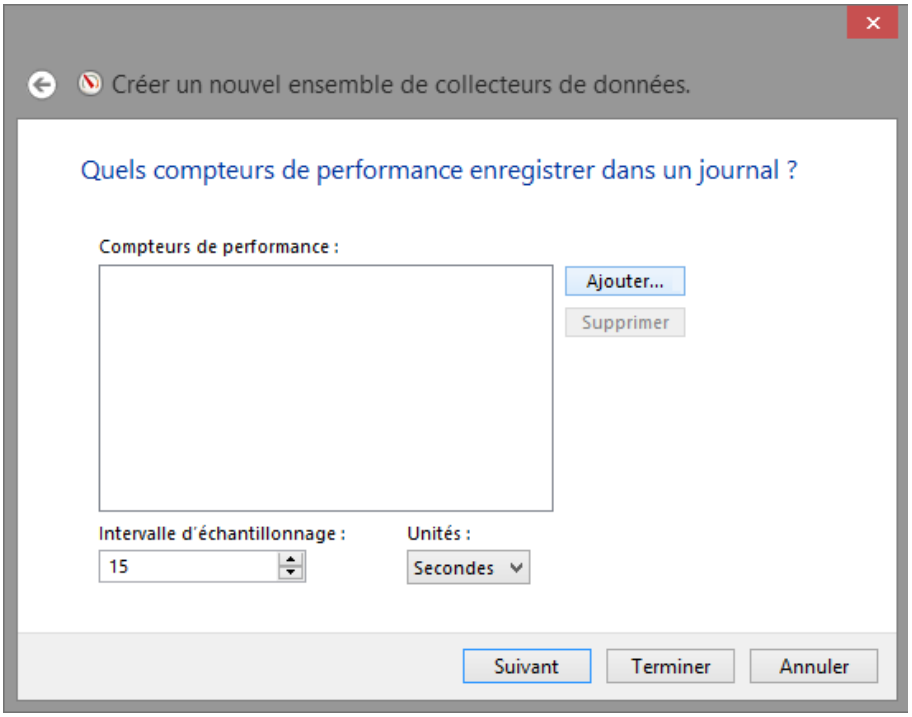
c. La fenêtre **Créer un nouvel ensemble de collecteurs de données** s'affiche. Dans le champ Nom, tapez **Journaux de mémoire**. Activez le bouton radio **Créer manuellement (avancé)**, puis cliquez sur **Suivant**.



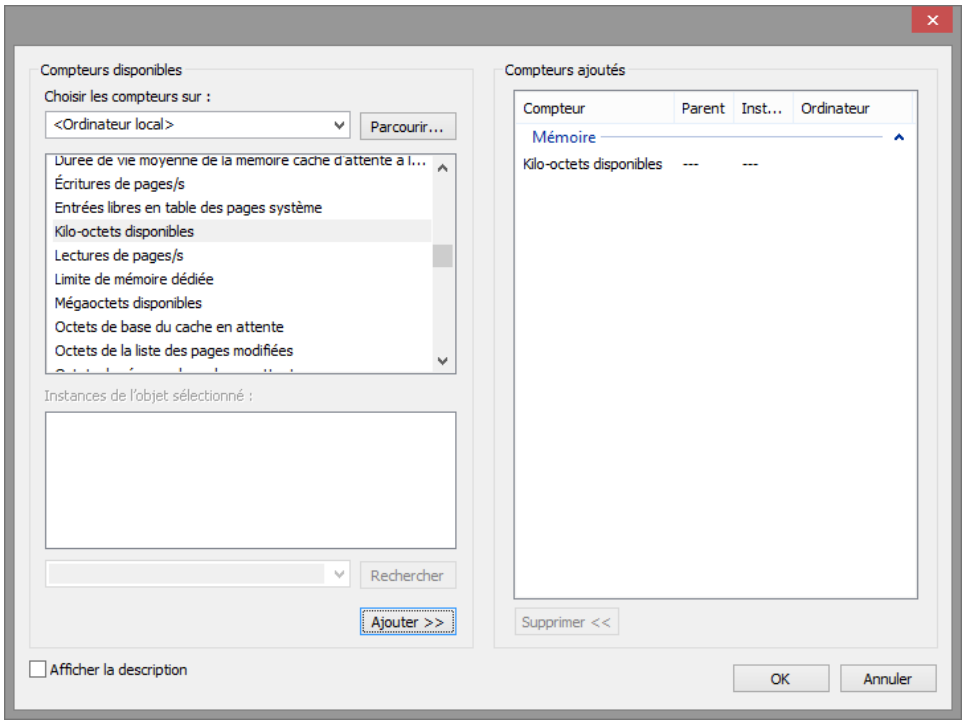
d. La fenêtre **Quel type de données inclure ?** s'affiche. Cochez la case **Compteur de performance**, puis cliquez sur **Suivant**.



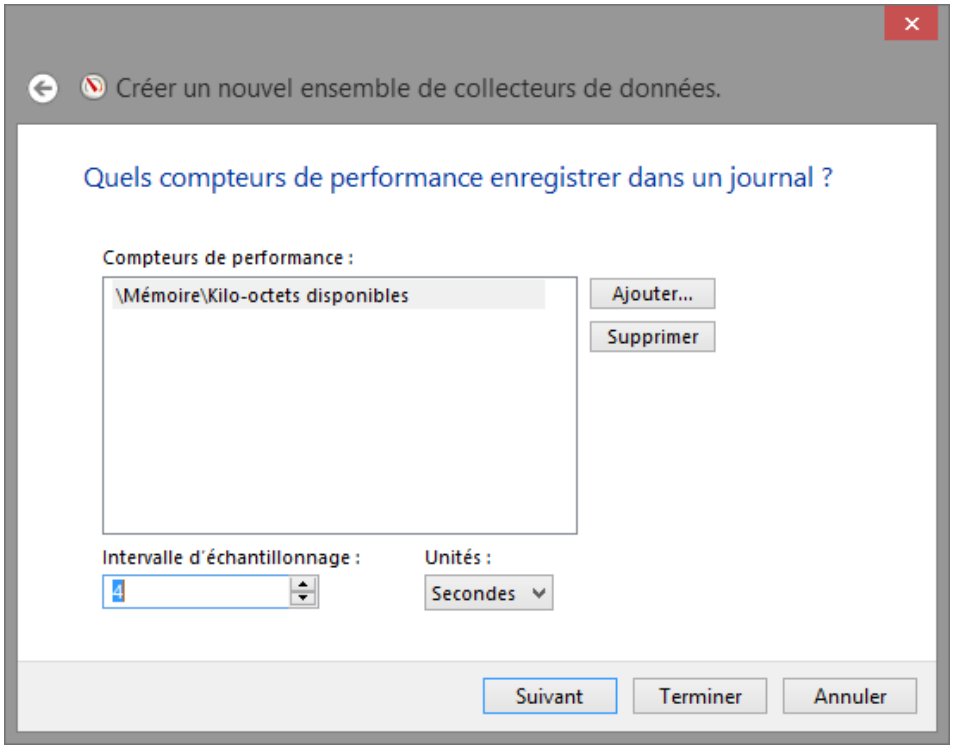
e. La fenêtre **Quels compteurs de performance enregistrer dans un journal ?** s'affiche. Cliquez sur **Ajouter**.



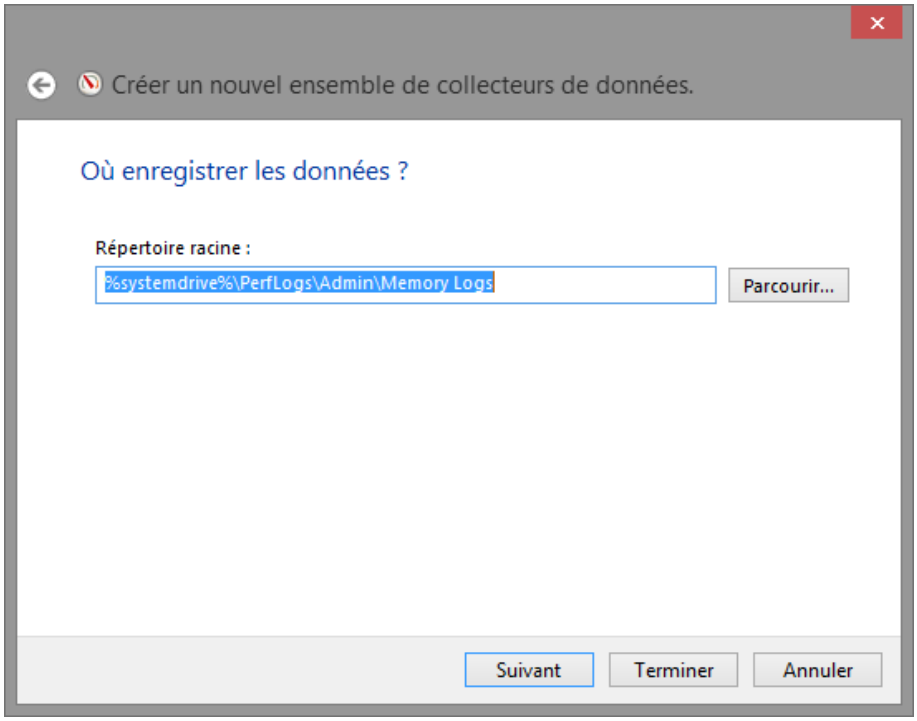
f. Dans la liste des compteurs disponibles, recherchez et développez **Mémoire**. Sélectionnez **Mégaoctets disponibles > Ajouter**, puis cliquez sur **OK**.



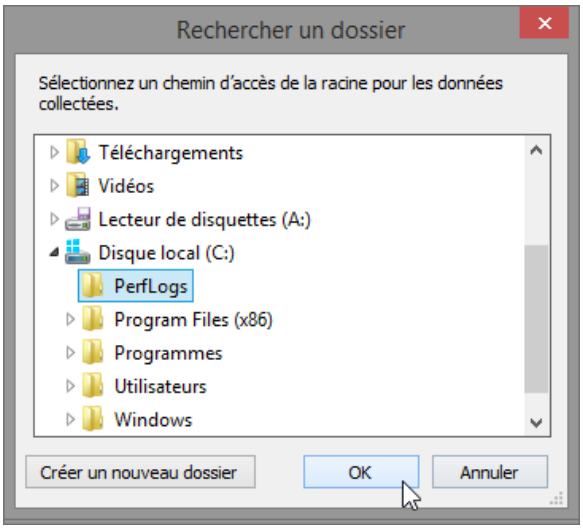
g. Définissez le champ **Intervalle d'échantillonnage** sur **4** secondes. Cliquez sur **Suivant**.



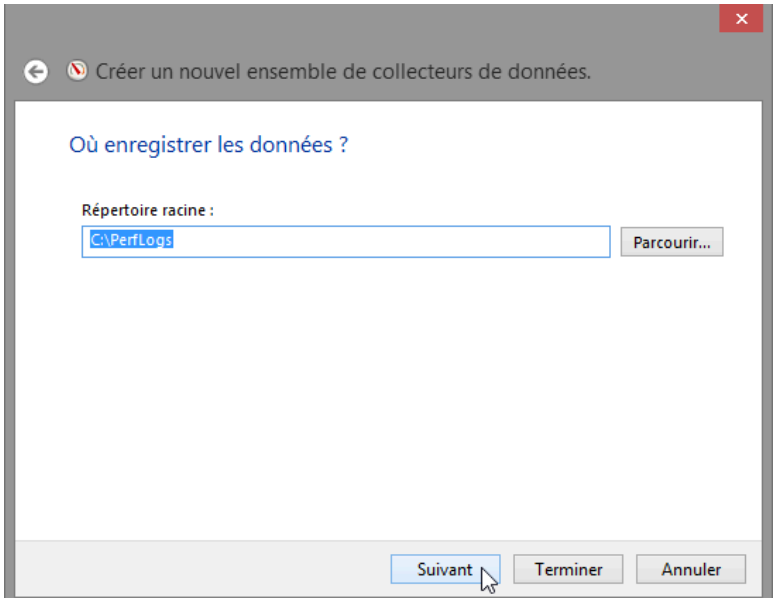
h. La fenêtre **Où enregistrer les données ?** s'affiche. Cliquez sur **Parcourir...**.



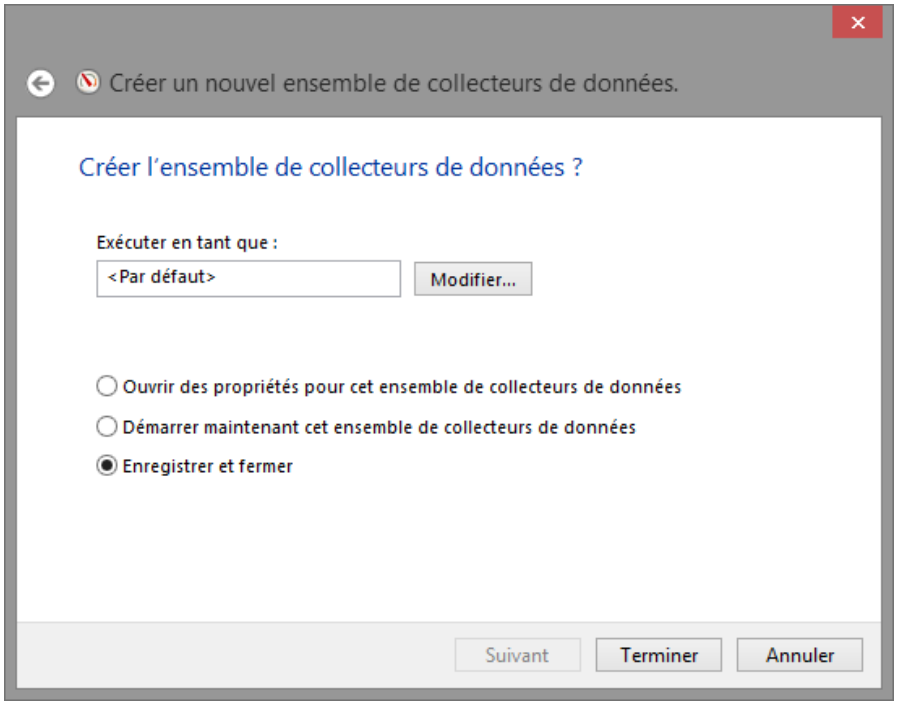
i. Sélectionnez le disque local **(C:)**, puis sélectionnez le dossier **\PerfLogs**. Cliquez sur **OK**.



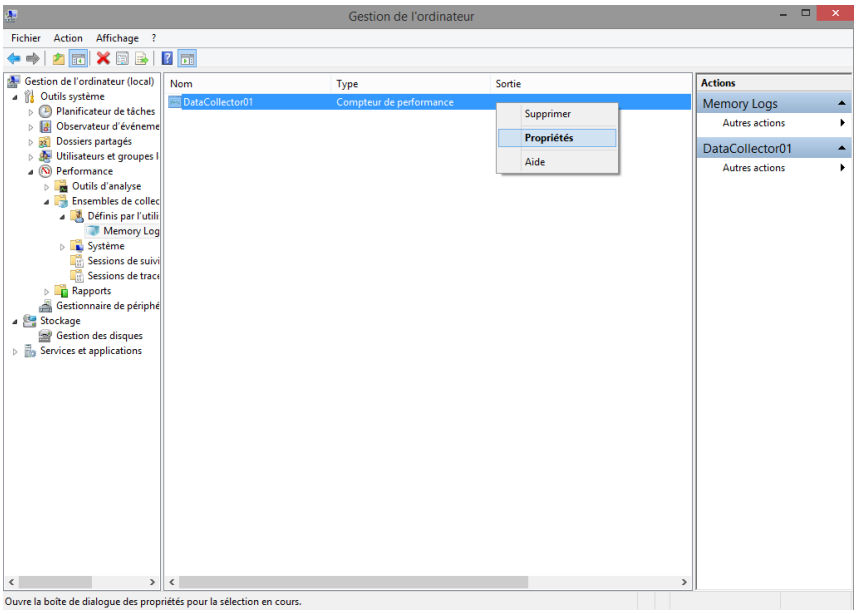
j. Vérifiez le chemin du répertoire racine, puis cliquez sur **Suivant**.



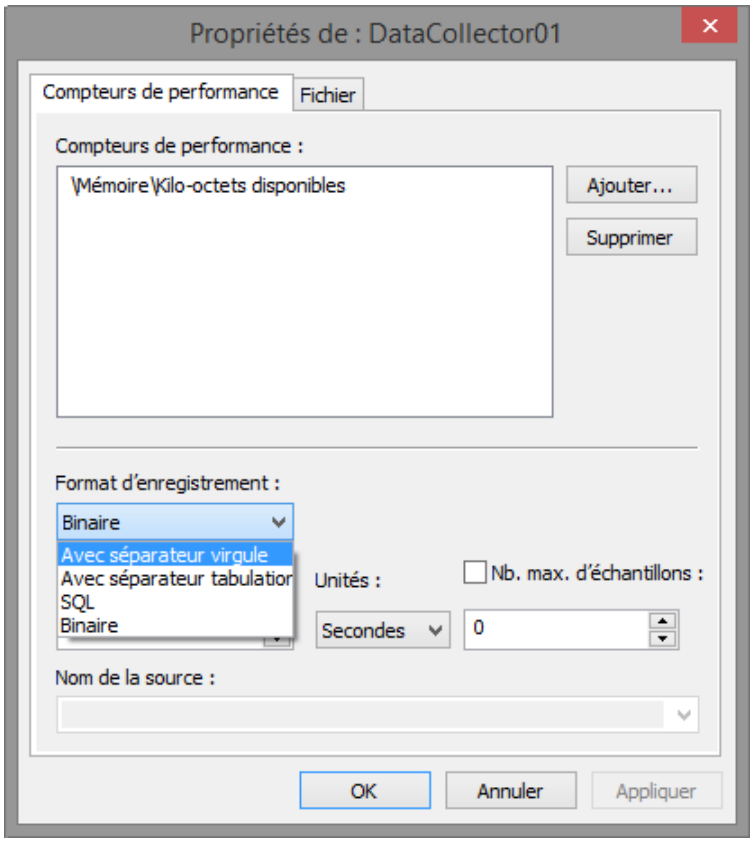
k. La fenêtre **Créer l'ensemble de collecteurs de données ?** s'affiche. Cliquez sur **Terminer**.



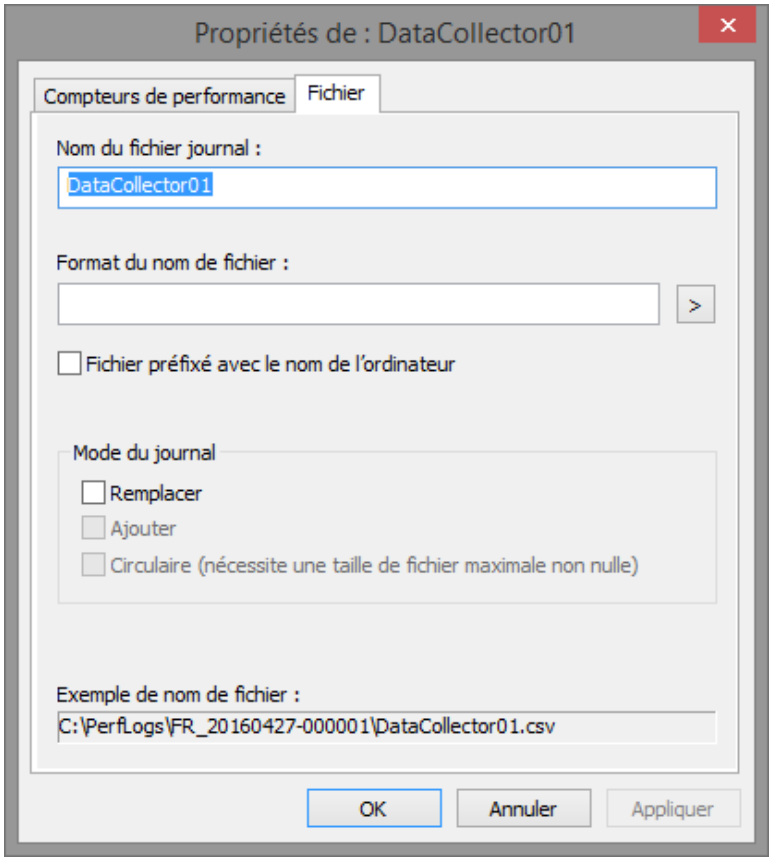
l. Développez **Définis par l'utilisateur** et sélectionnez **Journaux de mémoire**. Cliquez avec le bouton droit sur **Data Collector01**, puis sélectionnez **Propriétés**.



m. La fenêtre **Propriétés de DataCollector01** s'affiche. Définissez le champ **Format d'enregistrement :** sur **Séparé par une virgule**.



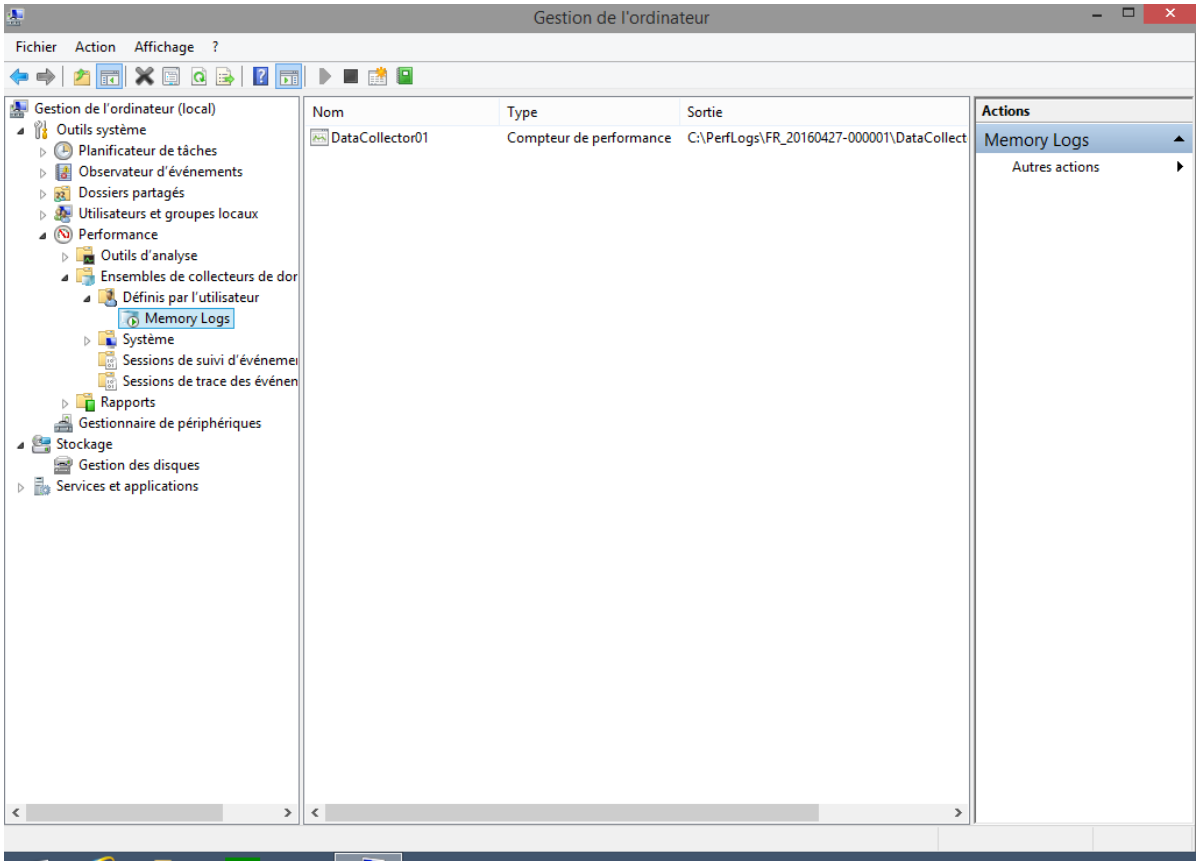
n. Cliquez sur l'onglet **Fichier**.



Quel est le nom complet du chemin du fichier exemple ?

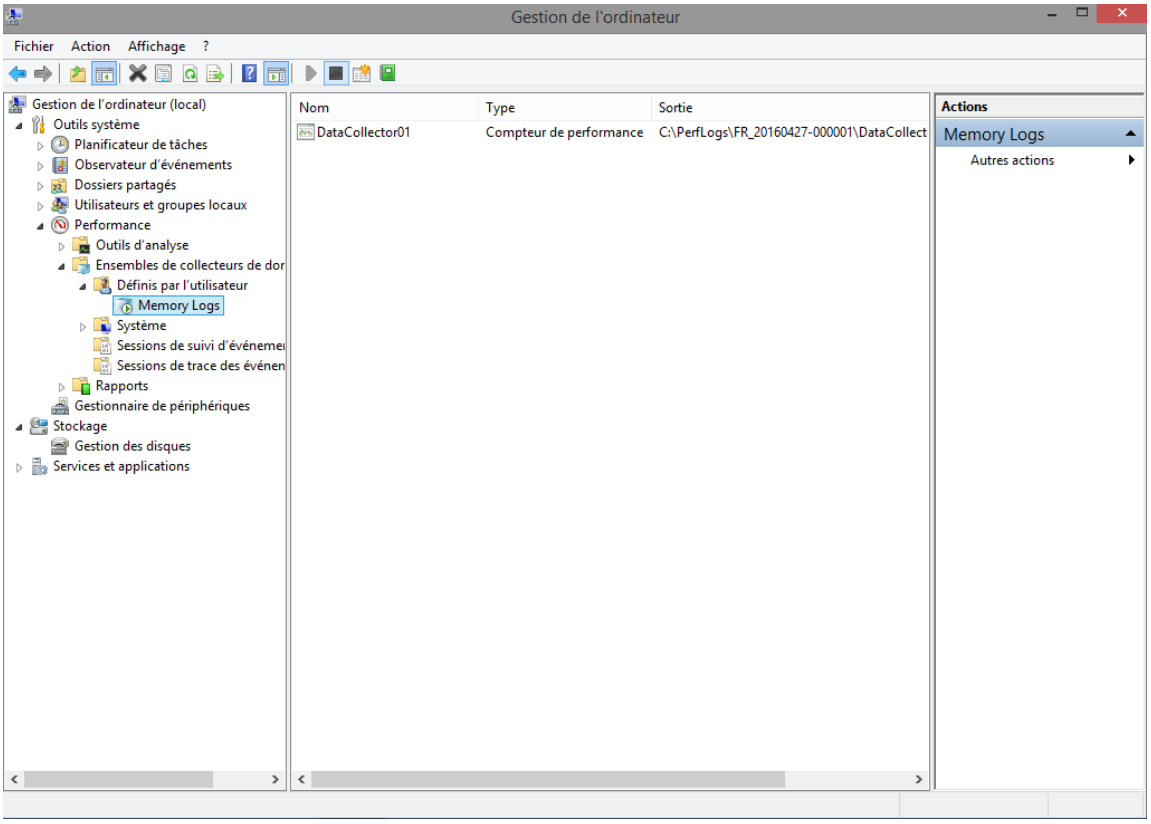
o. Cliquez sur **OK**.

p. Cliquez sur l'icône **Journaux de mémoire** dans le volet de gauche de l'onglet **Analyseur de performances**. Cliquez sur la **flèche verte** pour démarrer l'ensemble de collecte de données. Notez qu'une flèche verte est placée au-dessus de l'icône **Journaux de mémoire**.



q. Pour forcer l'ordinateur à utiliser une partie de la mémoire disponible, ouvrez et fermez un navigateur.

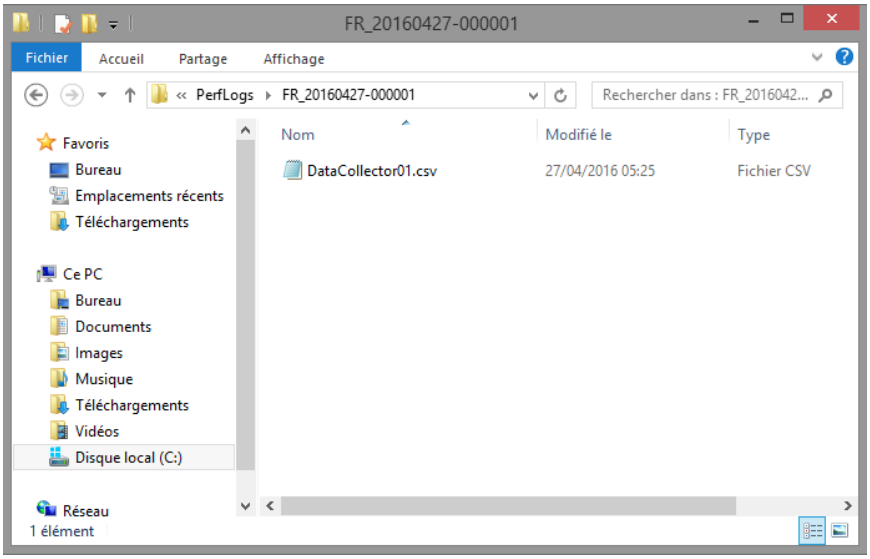
r. Cliquez sur le **carré noir** pour démarrer l'ensemble de collecte de données.



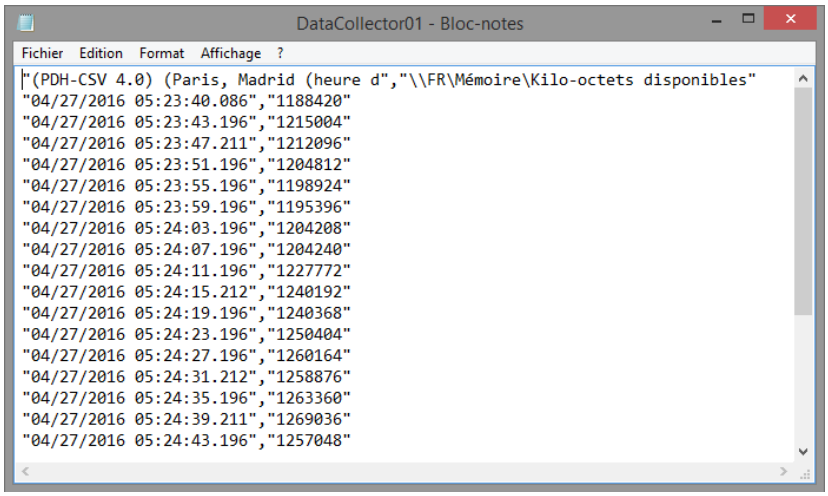
Quel changement remarquez-vous à propos de l'icône Journaux de mémoire ?

s. Ouvrez **Windows Defender**, puis cliquez sur **Disque local (C:) > PerfLogs**. Cliquez sur le dossier créé pour stocker le journal de mémoire et double-cliquez sur le fichier **DataCollector01.csv**.

Remarque : cliquez sur **Continuer** à chaque message d'avertissement de Windows.



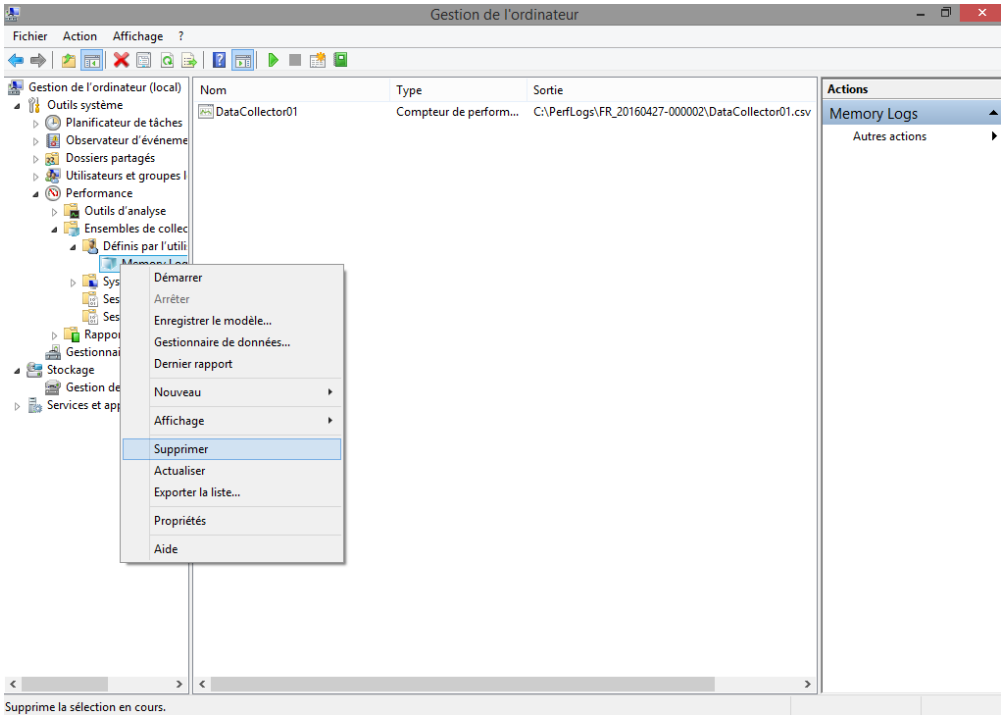
t. Si le message **Windows ne peut pas ouvrir ce fichier** s'affiche, activez le bouton radio **Sélectionner un programme dans la liste des programmes installés > OK > Bloc-notes > OK**.



Qu'indique la colonne située le plus à droite ?

u. Fermez le fichier **DataCollector01.csv** et l'**Explorateur Windows**.

v. Sélectionnez la fenêtre **Analyseur de performances**.



w. Cliquez avec le bouton droit sur **Journaux de mémoire > Supprimer**, puis cliquez sur **Oui**.

x. Ouvrez l'**Explorateur Windows**, puis cliquez sur **Disque local (C:) > PerfLogs**. Cliquez avec le bouton droit sur le dossier créé pour stocker les journaux de mémoire, puis sur **Supprimer**.

y. Fermez toutes les fenêtres ouvertes.