Travaux pratiques : Contrôle et gestion des ressources système

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 avec accès Internet

Instructions

Partie 1 : Observateur d'événements

Dans cette partie, Windows Defender est utilisé pour explorer l'Observateur d'événements lors du changement de l'état d'un service. Windows Defender est le composant antimalware intégré dans Windows.

Étape 1 : Vérifiez que Windows Defender est exécuté.

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

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

b. Pour déterminer si le service Windows Defender est arrêté, cliquez sur **Démarrer**, puis recherchez **Windows Defender**.

Sous Windows 10, cliquez sur **Protection contre les virus et menaces**. Faites défiler l'écran jusqu'à la section **Paramètres de protection contre les virus et menaces**. Cliquez sur **Paramètres de gestion**. Sous l'en-tête Protection en temps réel, vérifiez que cette option est **activée**.

Sous Windows 8.1, dans l'onglet **Accueil**, vérifiez que la protection en temps réel est activée. Si Windows Defender ne s'ouvre pas, accédez au **Centre de notifications** (cliquez sur **Démarrer** et recherchez **Centre de notifications**. Cliquez sur **Activer maintenant** en regard des options Protection contre les logiciels espions et indésirables (Important) et Protection contre les virus (Important).

Sous Windows 7, le message suivant s'affiche : **Ce programme est désactivé**dans la fenêtre Windows Defender. Cliquez sur **Cliquez ici pour l'activer** dans la fenêtre, puis cliquez sur **Fermer** pour continuer.

c. Maintenez Windows Defender ouvert.

Étape 2 : Explorer la Console des services

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 la console **Services** sous Windows 10 et 8.1.

a. Cliquez sur **Démarrer** > **Panneau de configuration**. Dans la vue Petites icônes du panneau de configuration, cliquez sur **Outils d'administration**, puis sur **Gestion de l'ordinateur**. Dans la fenêtre **Gestion de l'ordinateur**, développez **Services et applications**, puis sélectionnez **Services**.

b. Accédez à la fenêtre Gestion de l'ordinateur sous l'en-tête Services pour afficher le service d'inspection du réseau de l'antivirus **Windows Defender** (Windows 10) ou le **service Windows Defender** (Windows 8.1) ou **Window Defender** (Windows 7).

Question :

Quel est l'état de ce service ?

Saisissez vos réponses ici

c. Fermez la fenêtre **Gestion de l'ordinateur**. Revenez à Windows Defender et désactivez-le.

Sous Windows 10, cliquez sur **Protection contre les virus et menaces**. Faites défiler l'écran jusqu'à la section **Paramètres de protection contre les virus et menaces**. Cliquez sur **Paramètres de gestion**. Sous l'en-tête Protection en temps réel, cliquez sur le curseur pour le désactiver. Cliquez sur **Oui** pour autoriser cette application à effectuer des modifications sur votre appareil.

Sous Windows 8.1, dans l'onglet **Paramètres**, sélectionnez l'onglet **Paramètres**. Dans l'onglet Paramètres, sélectionnez **Administrateur**. Cliquez sur **Activer cette application** pour désactiver Windows Defender. Cliquez sur **Enregistrer les modifications** pour désactiver Windows Defender. Cliquez sur **Fermer** dans la fenêtre contextuelle, le cas échéant.

Sous Windows 7, cliquez sur **Outils**. Cliquez sur **Options**. Dans la fenêtre Options, sélectionnez **Administrateur**, puis cliquez sur **Utiliser ce programme**. Cliquez sur **Enregistrer** pour arrêter Windows Defender. Cliquez sur **Fermer** pour continuer lorsqu'un message s'affiche vous informant que vous avez désactivé ce programme.

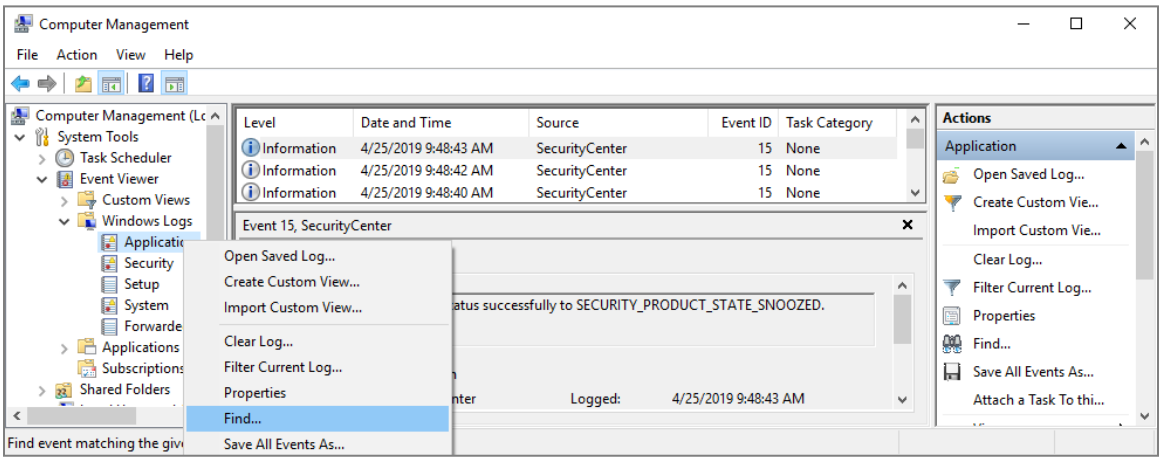
d. Revenez aux services. (**Panneau de configuration** en mode Petites icônes > **Outils d'administration** > **Services**). Cliquez sur **Action**, puis sur **Actualiser**.

Recherchez le **Service Inspection du réseau de l'antivirus Windows Defender** (Windows 10) ou le **Service Windows Defender** (Windows 8.1) ou **Window Defender** (Windows 7). Notez l'état de Windows Defender.

Saisissez vos réponses ici

e. Accédez à l'Observateur d'événements. Dans la fenêtre Gestion de l'ordinateur, développez **Outils système**, développez **Observateur d'événements**, développez **Journaux Windows**, puis sélectionnez **Application** (Windows 10) ou **Système** (Windows 8.1 et 7).

f. Le volet Application ou Système contient les événements les plus récents liés à Windows Defender. Cliquez avec le bouton droit de la souris sur le journal souhaité, puis sélectionnez **Rechercher**. Saisissez **Defender** pour rechercher les entrées associées à Windows Defender.



Dans l'onglet Général, quelle est la source de l'événement ? Quel est le niveau de gravité ?

Saisissez vos réponses ici

g. Accédez à Windows Defender et activez-le. Fermez Windows Defender.

h. Accédez à l'Observateur d'événements pour consulter les entrées d'événements les plus récentes liées à Windows Defender.

Partie 2 : Découverte de l'impact des services

Dans cette partie, vous allez arrêter le service **Spouleur d'impression** et observer l'impact sur le système. Le spouleur d'impression est chargé de la gestion des travaux d'impression et de la gestion de l'interaction avec l'imprimante. Si ce service est désactivé, vous ne pourrez ni imprimer ni afficher vos imprimantes.

Étape 1 : Vérifiez le service d'impression

a. Ouvrez le **Bloc-notes**. Cliquez sur **Démarrer** et recherchez **Bloc-notes**.

b. Dans le **Bloc-notes**, cliquez sur **Fichier** > **Imprimer**. Notez ci-dessous l'une des imprimantes répertoriées. **Remarque** : il n'est pas nécessaire d'installer une imprimante physique.

Saisissez vos réponses ici

c. Cliquez sur **Annuler** pour quitter la boîte de dialogue d'impression.

Étape 2 : Arrêter le spouleur d'impression

a. Ouvrez la Console des services. (Panneau de configuration > Outils d'administration > Services.)

b. Cliquez avec le bouton droit de la souris sur **Spouleur d'impression** et sélectionnez **Arrêter**.

c. Accédez au **Bloc-notes**. Essayez d'imprimer.

Question :

Quel message recevez-vous ? Comment résoudriez-vous ce problème ?

Saisissez vos réponses ici

d. Cliquez sur **OK** ou sur **Non** dans la fenêtre du message et cliquez sur **Annuler** pour quitter la fenêtre d'impression.

Étape 3 : Redémarrer le spouleur d'impression

a. Accédez à la console **Services** et redémarrez le spouleur d'impression. Cliquez avec le bouton droit de la souris sur **Spouleur d'impression** et sélectionnez **Démarrer**.

b. Vérifiez que vous pouvez imprimer.

Étape 4 : Explorer le service client DHCP

Le service client DHCP enregistre et met à jour les adresses IP et les enregistrements DNS de l'ordinateur. Si ce service est arrêté, l'ordinateur ne recevra pas de mises à jour DNS et d'adresses IP dynamiques.

a. Dans la console Services, recherchez le **Client DHCP**. Cliquez avec le bouton droit de la souris sur **Client DHCP** et sélectionnez **Arrêter**.

Question :

Après l'arrêt du client DHCP, quels autres services s'arrêtent-ils également ?

Saisissez vos réponses ici

b. Cliquez sur **Non** dans la fenêtre **Arrêter les autres services**.

Question :

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

Saisissez vos réponses ici

c. Vérifiez que le **Client DHCP** est toujours exécuté.

Partie 3 : Contrôler et enregistrer l'utilisation du système à l'aide des outils d'administration

Vous allez configurer les fonctionnalités avancées des outils d'administration et contrôler l'utilisation des ressources de l'ordinateur.

Étape 1 : Créez un nouvel ensemble de collecteurs de données.

a. Accédez au Panneau de configuration, cliquez sur Outils d'administration, puis cliquez sur Gestion de l'ordinateur et développez les Outils système.

b. Développez **Performances**, développez **Ensembles de collecteurs de données**, dans le volet de gauche cliquez avec le bouton droit de la souris sur **Défini par l'utilisateur**, sélectionnez **Nouveau**, puis cliquez sur **Ensemble de collecteurs de données**.

c. Dans la fenêtre **Créer un nouvel ensemble de collecteurs de données**, tapez **Journaux mémoire** dans le champ Nom. Sélectionnez **Créer manuellement (avancé)**, puis cliquez sur **Suivant** pour continuer.

d. Dans la fenêtre Quel type de données inclure ?, sélectionnez Compteur de performance, puis cliquez sur Suivant.

e. Dans la fenêtre **Quels compteurs de performance enregistrer dans un journal ?**, cliquez sur **Ajouter**. Dans la liste des compteurs disponibles, recherchez et développez **Mémoire**. Sélectionnez **Mégaoctets disponibles > Ajouter**, puis cliquez sur **OK** pour continuer.

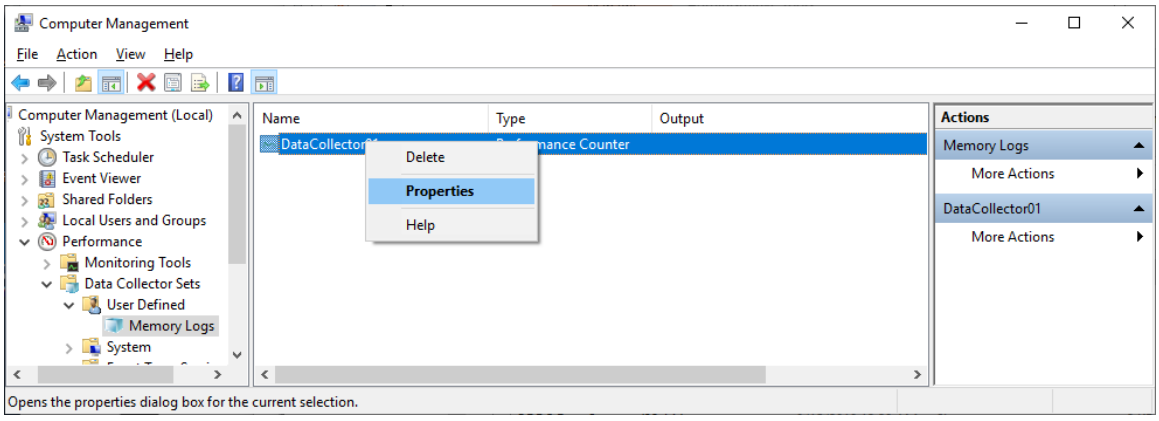
f. Définissez le champ **Intervalle d'échantillonnage** : sur **4** secondes. Cliquez sur **Suivant** pour continuer.

g. Dans la fenêtre Où enregistrer les données ?, cliquez sur Parcourir. Sélectionnez le disque local (C:) et sélectionnez PerfLogs. Cliquez sur OK pour continuer.

h. Vérifiez que le chemin d'accès au répertoire racine correct est affiché (C:\PerfLogs), puis cliquez sur **Terminer** pour continuer.

Étape 2 : Formater l'ensemble de collecteurs de données

a. Développez **Défini par l'utilisateur** et sélectionnez **Journaux mémoire** dans le volet de gauche. Cliquez avec le bouton droit de la souris sur **DataCollector01**, puis choisissez **Propriétés**.



b. Dans la fenêtre Propriétés de DataCollector01, définissez le champ Format du journal : sur **Séparé par une virgule**.

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

Question :

Quel est le nom complet du chemin du fichier exemple ?

Saisissez vos réponses ici

d. Cliquez sur **OK** pour fermer la fenêtre des propriétés.

Étape 3 : Collecter et afficher les données

a. Cliquez sur l'icône **Journaux mémoire** dans le volet de gauche de l'onglet **Gestion de l'ordinateur**. Cliquez avec le bouton droit de la souris sur **Journaux mémoire** et sélectionnez **Démarrer**.

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

c. Cliquez avec le bouton droit de la souris sur **Journaux mémoire** et sélectionnez **Arrêter** pour arrêter l'ensemble de collecteurs de données.

Accédez au **disque local (C:) \PerfLogs**. Cliquez sur **Continuer** dans les messages d'avertissement de Windows.

d. Ouvrez le dossier créé pour stocker le journal mémoire. Cliquez sur **Continuer** dans les messages d'avertissement de Windows. Ouvrez le fichier **DataCollector01.csv**.

Sélectionnez le **Bloc-notes** ou un autre programme capable de lire les fichiers séparés par des virgules (.csv) pour accéder au fichier si le message indiquant que Windows ne peut pas ouvrir le message du fichier s'affiche.

Question :

Qu'indique la colonne située le plus à droite ?

Saisissez vos réponses ici

e. Fermez le fichier DataCollector01.csv.

Étape 4 : Nettoyage

a. Accédez à la fenêtre **Gestion de l'ordinateur**. Sélectionnez **Performance**, cliquez sur **Ensembles de collecteurs de données**, puis cliquez sur **Défini par l'utilisateur**. Cliquez avec le bouton droit de la souris sur **Journaux mémoire** et sélectionnez **Supprimer**. Cliquez sur **Oui** pour confirmer la suppression.

b. Accédez au lecteur local **C: > PerfLogs**. Supprimez le dossier des journaux mémoire stockés (dossier contenant le fichier DataCollector01.csv) créé lors de ces travaux pratiques.

c. Fermez toutes les fenêtres ouvertes.