Les journaux d'événements

1. Gérer et utiliser les journaux d'événements

L'**Observateur d'événements** est un des outils les plus couramment utilisés par les administrateurs système pour analyser l'activité courante d'un poste Windows. L'Observateur d'événements collecte les informations issues du système, mais également des services et applications.

Cet outil se révèle souvent indispensable pour aider à la définition d'un diagnostic et déterminer l'origine d'une erreur. Il permet de visualiser l'activité du système et de trouver des codes d'erreur liés à des articles de la base de connaissances Microsoft.

Windows 10 dispose de différents journaux d'événements pour stocker le suivi des informations du système d'exploitation et des applications et services Windows. Pour prendre rapidement connaissance de l'état d'un système, vous pouvez consulter les journaux Windows. Si le problème rencontré concerne par exemple un service particulier, vous pouvez consulter les journaux des services Windows. Chaque service dispose de son propre journal d'événements.

Les journaux d'événements sont stockés sous forme de fichiers de type *.evtx situés dans le répertoire %SystemRoot%\System32\Winevt\Logs\.

Depuis Windows 7, l'utilisation de l'Observateur d'événements ne se limite plus à la collecte des événements. Vous pouvez, par exemple, utiliser les journaux d'événements Windows pour des actions de remédiation comme par exemple déclencher une tâche planifiée sur un événement de type erreur.

- Pour lancer l'Observateur d'événements, à partir du menu **Démarrer**, tapez **eventvwr.msc** dans la zone de recherche, puis appuyez sur la touche [Entrée].

  Vous pouvez également afficher l'Observateur d'événements à partir des outils d'administration accessibles dans la section **Système et sécurité** du **Panneau de configuration**.

L'utilitaire **wevtutil.exe** permet de gérer les journaux d'événements via une invite de commandes.

Vous disposez aussi de cmdlets PowerShell pour gérer et accéder aux journaux d'événements comme par exemple la commande `Show-Eventlog`.

2. Filtrer les événements de type erreur

Le processus de filtrage est le même quel que soit le journal sélectionné. Pour afficher les événements générés par les composants système de Windows, dans l'Observateur d'événements, sélectionnez **Journaux Windows - Système**.

- Pour filtrer ce journal afin d'obtenir uniquement les événements de type erreur et avertissement pour les 7 derniers jours, dans le volet **Actions**, sélectionnez l'option **Filtrer le journal actuel**.
- Renseignez les règles de filtrage :
  - Dans la rubrique **Connecté**, sélectionnez **Les 7 derniers jours**.
  - Dans la rubrique **Niveau d'événements**, cliquez sur **Erreur** et **Avertissement**.
- Cliquez sur le bouton **OK** pour activer la règle de filtrage.

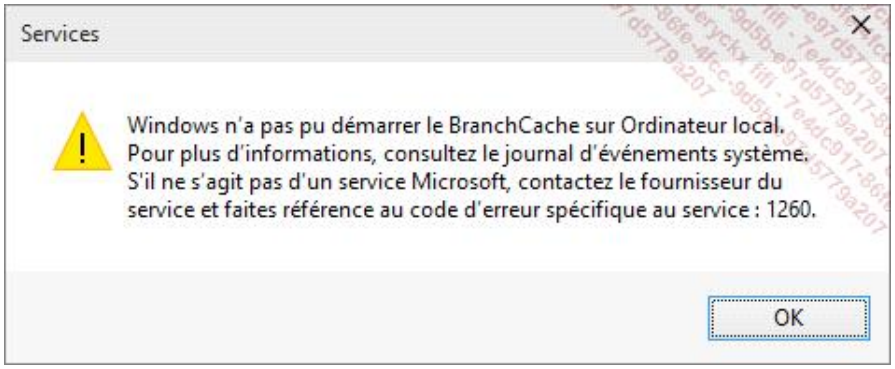
Vous pouvez exporter ou archiver ce journal filtré au format *.evtx ou *.csv, par exemple pour l'exploiter dans un

outil tiers, avec le menu **Enregistrer le fichier journal sous**.

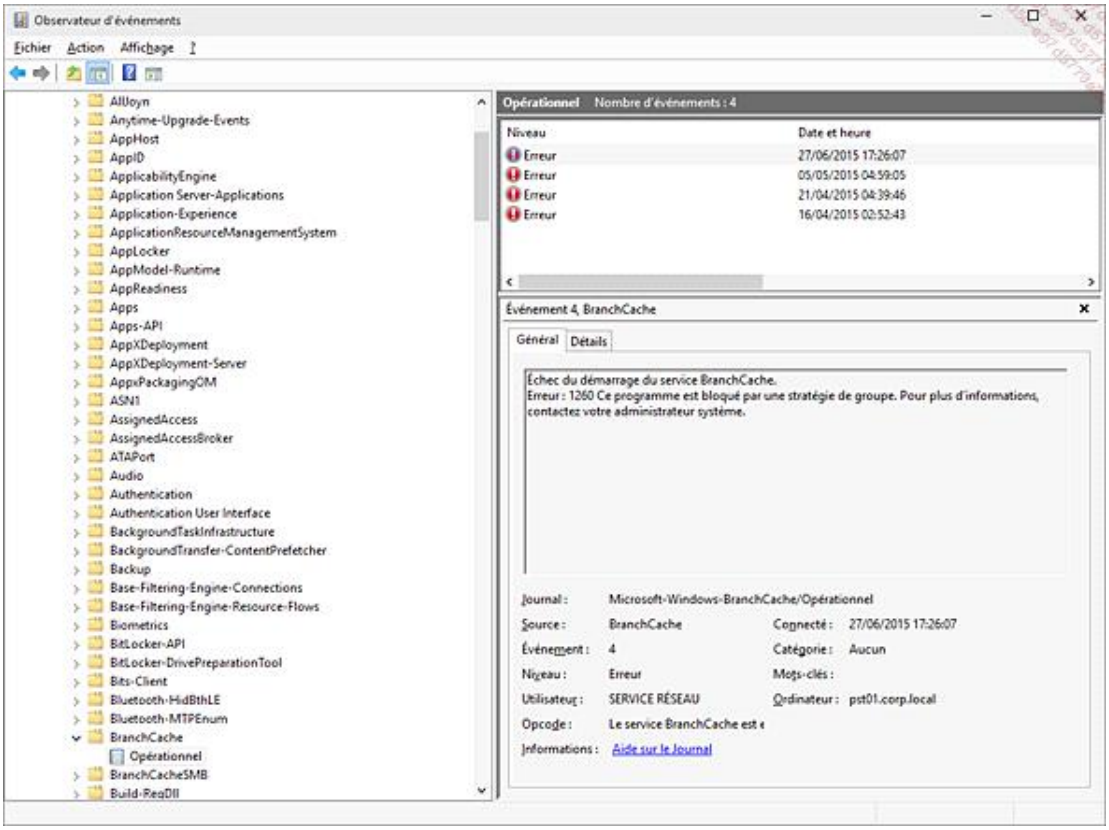
3. Diagnostiquer les erreurs de démarrage de service

Lorsqu'un service ne démarre pas, le message d'erreur indique le code d'erreur relevé et vous invite à consulter le journal d'événements **Système**.

Prenons par exemple le service **BranchCache** sur un poste de travail autonome, c'est-à-dire qu'il n'appartient pas à un domaine. Essayez de démarrer ce service via la console de gestion des services Windows, vous remarquez que le service ne démarre pas.

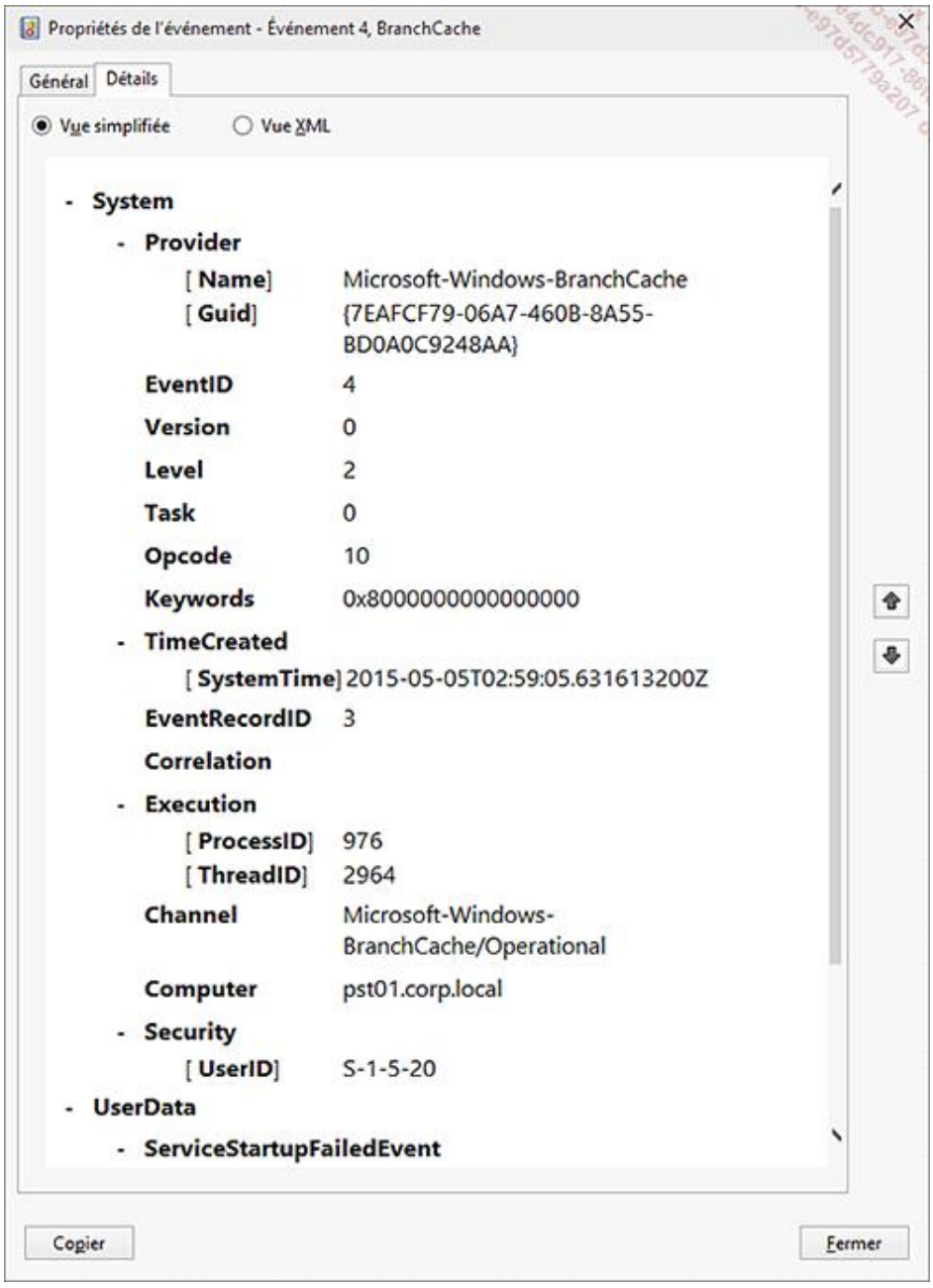


Si vous ouvrez le journal relatif au service **BranchCache** (dans **Journaux des applications et services - Microsoft - Windows**), vous visualisez les messages d'erreur générés par les actions de démarrage successif du service Windows.



Sélectionnez un événement de type erreur puis accédez aux propriétés de cet événement. Vous visualisez dans

l'onglet **Détails** les informations qui permettent de qualifier l'erreur analysée. Vous pouvez, par exemple, voir le SID (*Security Identifier*) correspondant au compte utilisateur utilisé dans ce contexte, ici le compte **SERVICE RESEAU**. C'est ce compte qui est positionné par défaut comme compte de démarrage de service.



Dans le cas du service BranchCache, le message d'erreur indique que le programme est bloqué par une stratégie de groupe. Cette stratégie est effectivement requise pour la mise en œuvre de la fonctionnalité.

Attention, certains journaux ne sont pas actifs par défaut. Si vous désirez par exemple résoudre des problèmes liés au service d'impression, vous devrez activer le journal de type **Opérationnel** du service **PrintService** via le lien **Activer le journal** dans le volet **Actions**.