CAMPUS DE LONGUEUIL
CÉGEP ÉDOUARD MONTPETIT

Journalisation Windows

Gestion de la journalisation sous Windows

Automne 2022

Séance 10C

Contenu

- ✓ Concepts généraux (rappel)
- ✓ Journaux textuels sous Windows
- ✓ Démarrage de l'observateur d'évènements
- ✓ Classement des évènements
- ✓ Principaux journaux : Application, Système, Installation, Sécurité, Journaux spécialisés
- ✓ Filtrage
- ✓ Évènements d'administration

Concepts généraux de la journalisation (logging) (rappel)

Lorsqu'un problème survient dans l'un des processus en arrière-plan, il peut être utile de savoir ce qui s'est passé.

Les systèmes d'exploitation et plusieurs applications gardent une trace des étapes importantes de ce qu'ils font (leur démarrage, les erreurs rencontrées, etc.) dans un journal, ou *log*.

Pourquoi les logs sont importants? (rappel)

Les logs contiennent des informations sur le fonctionnement du système d'exploitation. À quoi servent-ils concrètement?

Auditer le système

Détecter les accès non autorisés

Facturer l'utilisation des ressources

Diagnostiquer les problèmes et les erreurs

etc.

Inconvénients (rappel)

Cependant, la journalisation peut avoir des impacts négatifs.

Réduire les **performances** du système

Utiliser un **espace disque** important

Augmenter le **temps** d'analyse et de traitement des données

Ce n'est donc pas absolument tout qui est journalisé, mais seulement les évènements les plus importants.

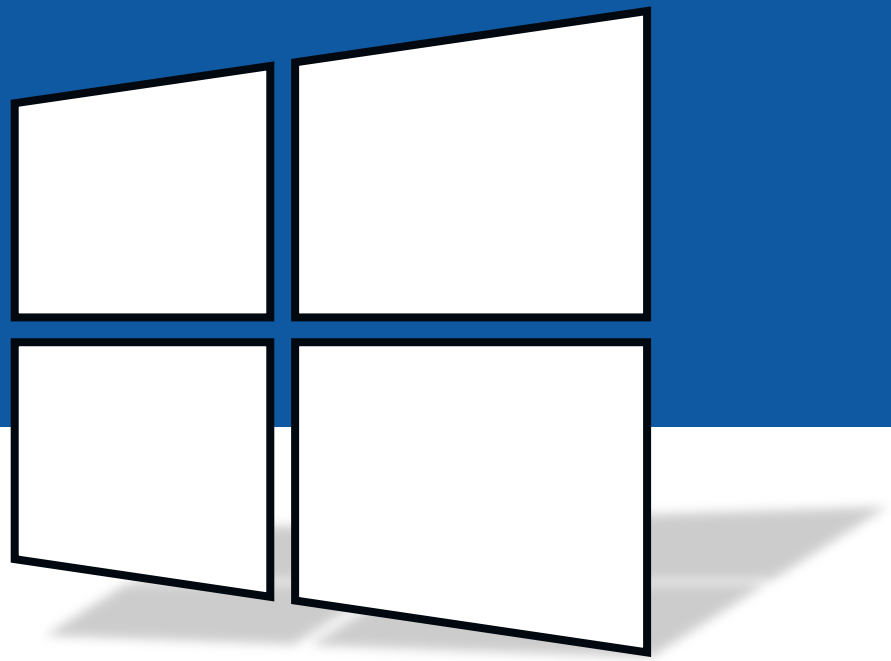
Fichiers log en format texte (rappel)

La forme la plus rudimentaire des journaux prend la forme d'un **fichier texte**, lisible avec des outils de lecture de texte standard.

Chaque **évènement** occupe généralement **une ligne** de texte

Chaque évènement est **horodaté**

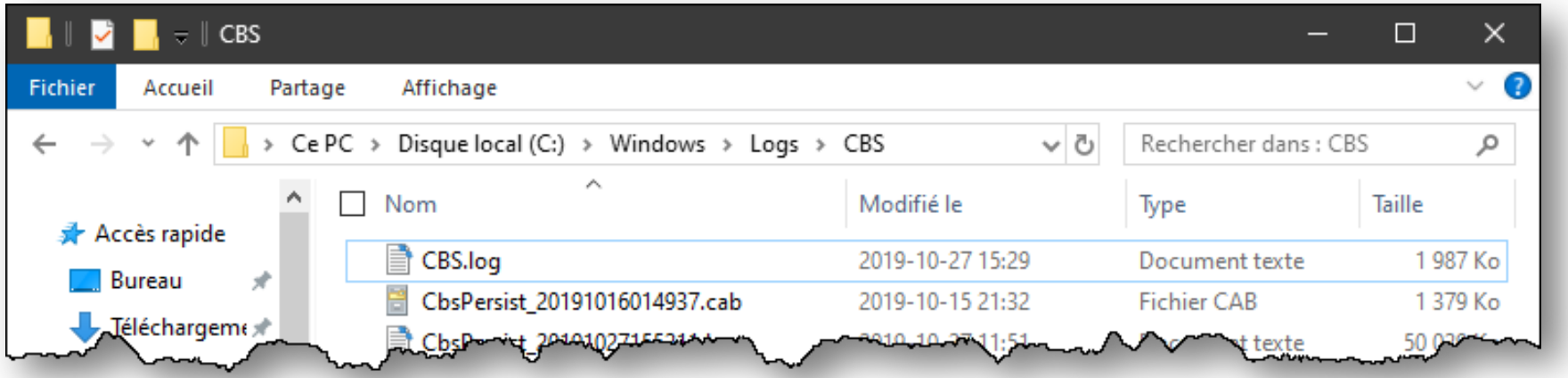
Les évènements sont toujours **ajoutés à la fin du fichier**. Les évènements à la fin du fichier sont donc les plus **récents**.

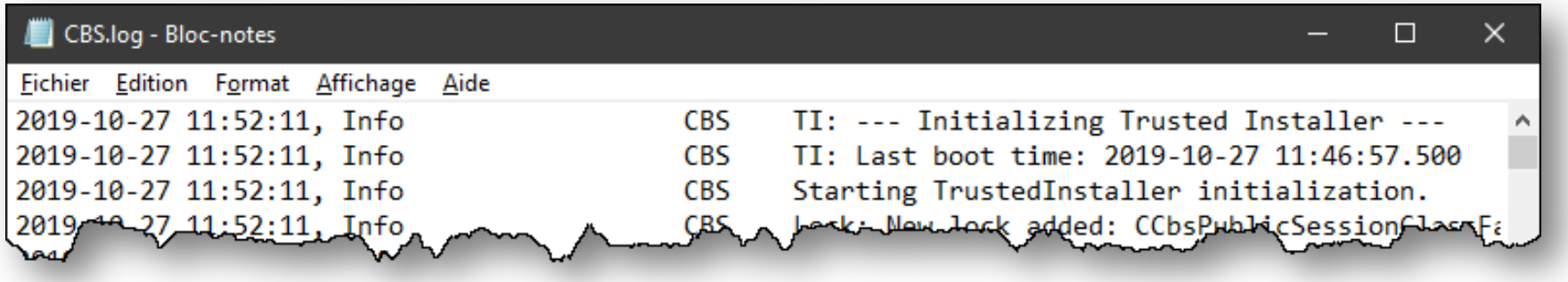


Windows

Journaux textuels

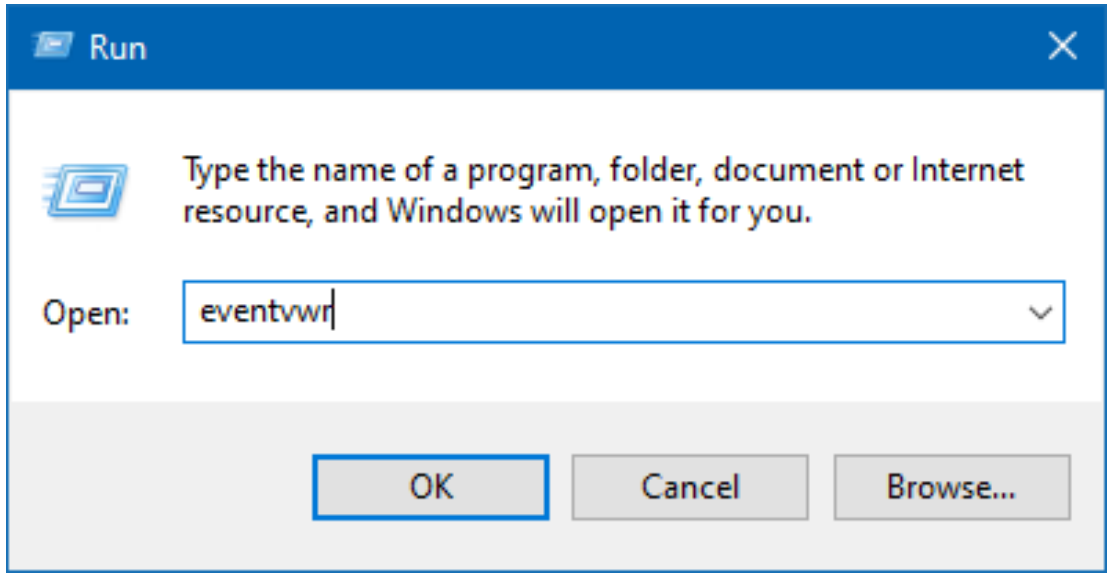
Certaines applications et composants effectuent leur journalisation dans de simples fichiers texte.

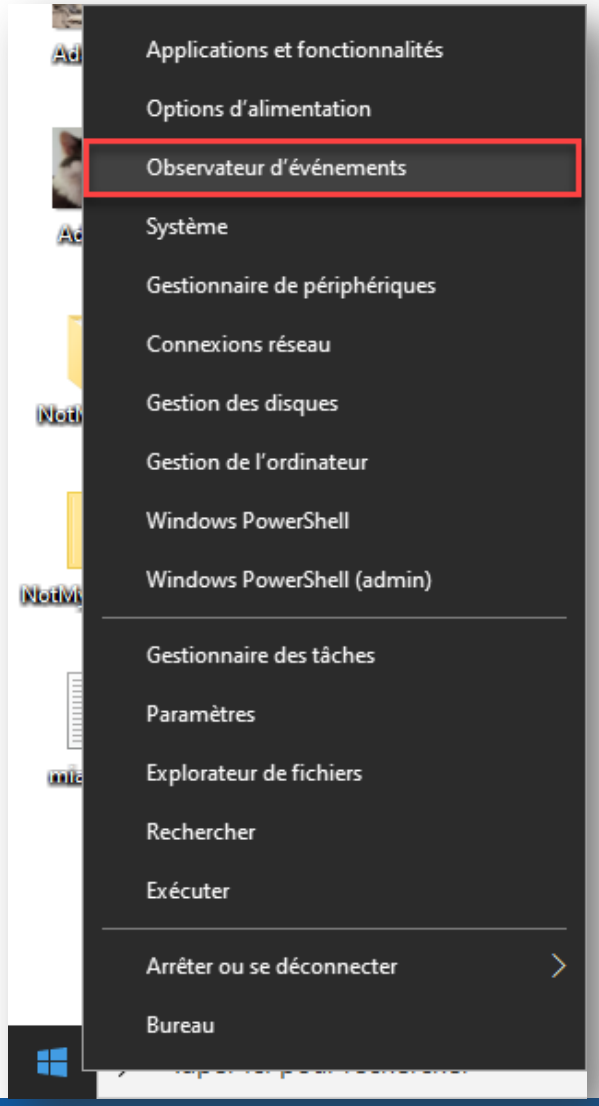




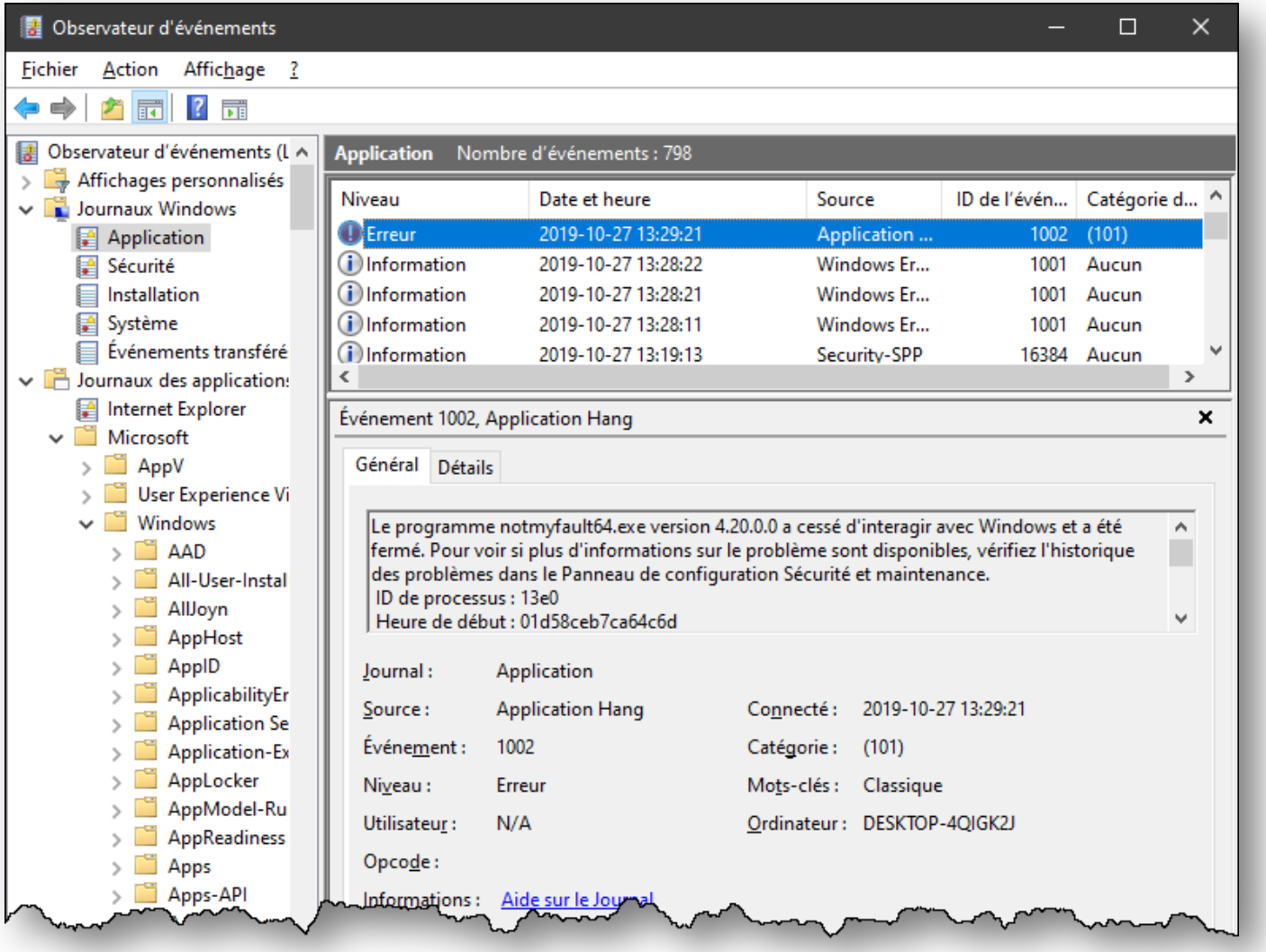
Journaux d'événements

La plupart des événements de journaux rapportés par Windows sont accessibles non pas par des fichiers, mais via l'**observateur d'évènements**.





Observateur d'évènements



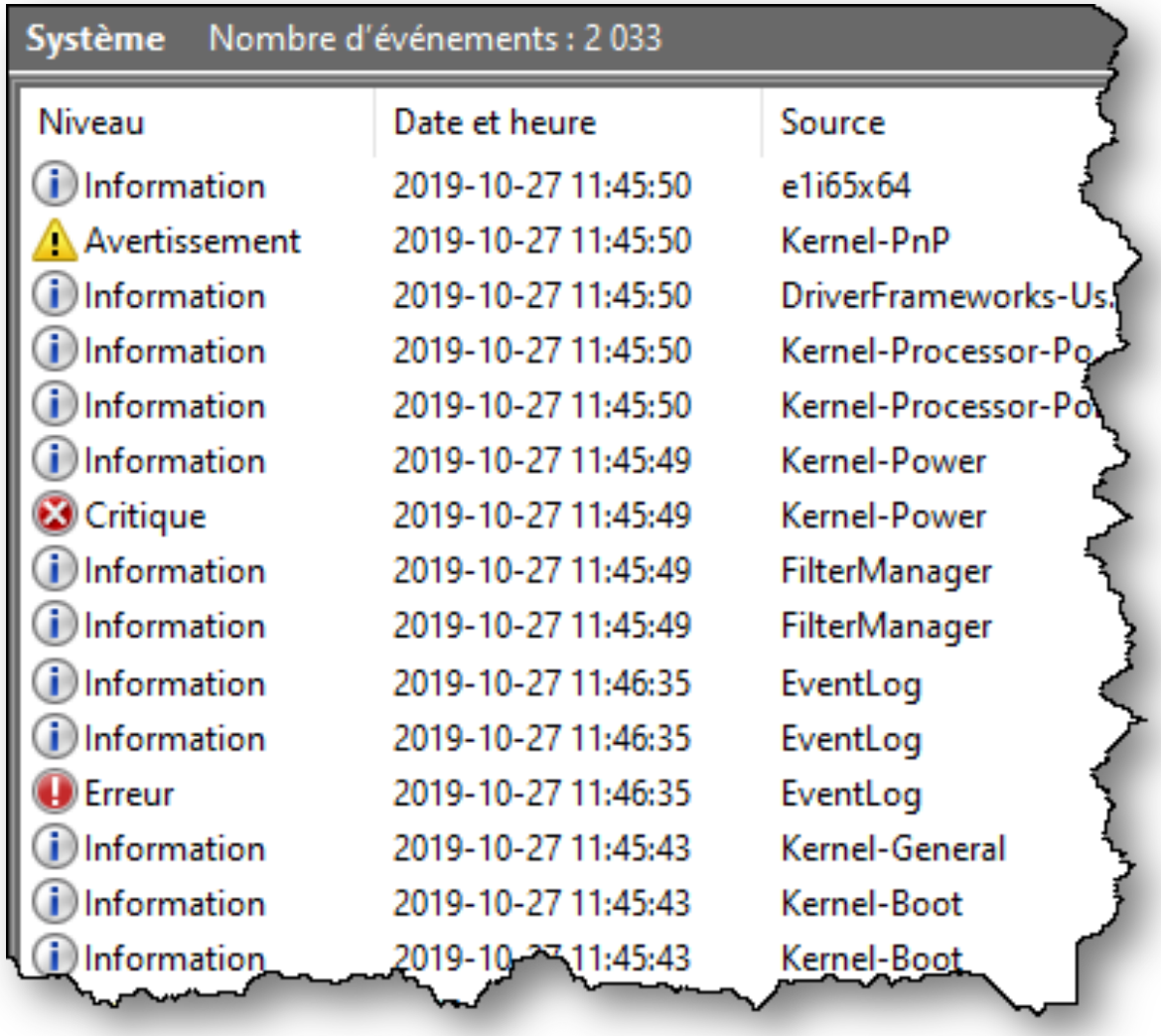
Classement des évènements

Information

Avertissement

Erreur

Critique

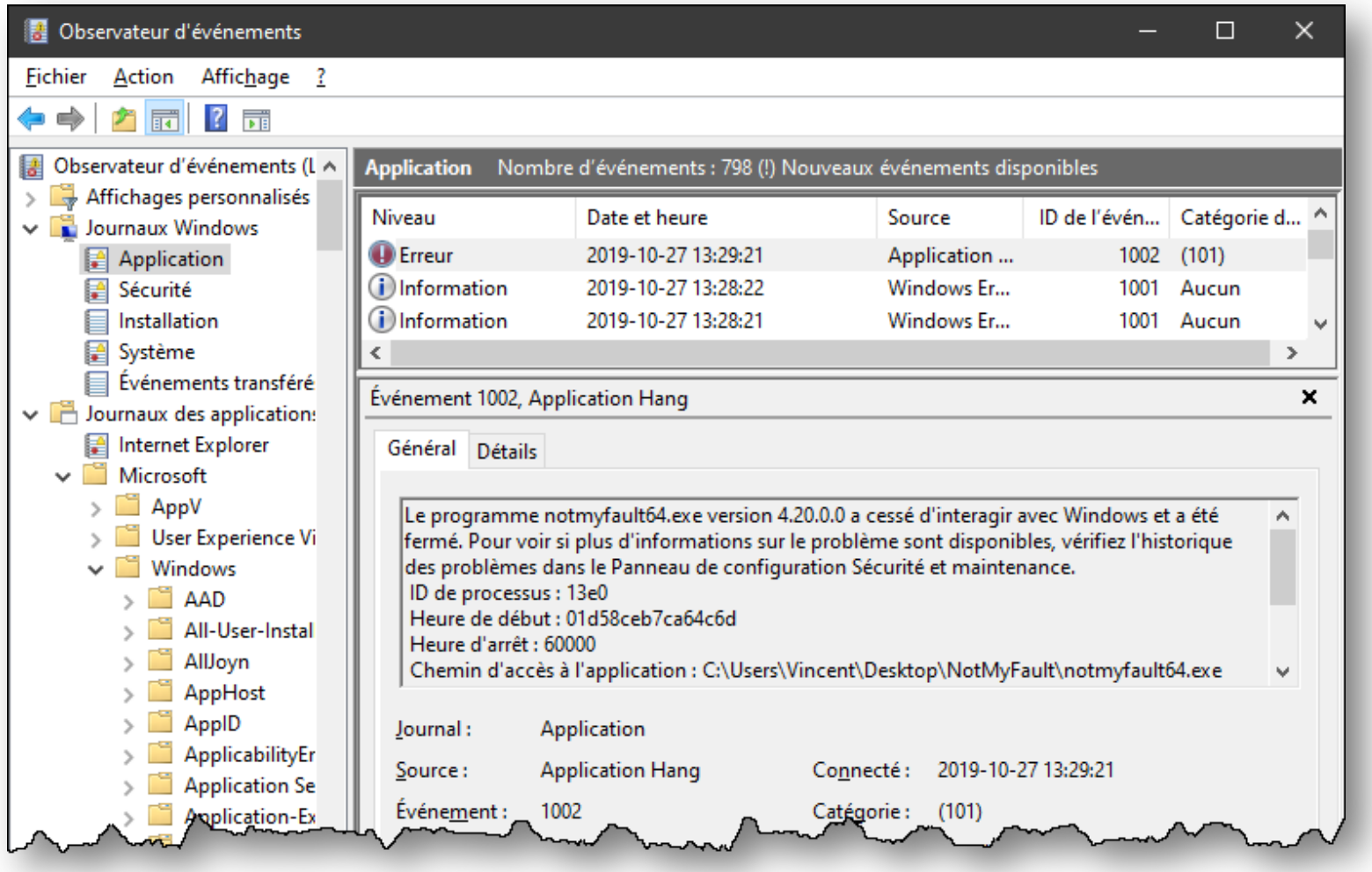


Système Nombre d'événements : 2 033

Niveau	Date et heure	Source
Information	2019-10-27 11:45:50	e1i65x64
Avertissement	2019-10-27 11:45:50	Kernel-PnP
Information	2019-10-27 11:45:50	DriverFrameworks-Us
Information	2019-10-27 11:45:50	Kernel-Processor-Po
Information	2019-10-27 11:45:50	Kernel-Processor-Po
Information	2019-10-27 11:45:49	Kernel-Power
Critique	2019-10-27 11:45:49	Kernel-Power
Information	2019-10-27 11:45:49	FilterManager
Information	2019-10-27 11:45:49	FilterManager
Information	2019-10-27 11:46:35	EventLog
Information	2019-10-27 11:46:35	EventLog
Erreur	2019-10-27 11:46:35	EventLog
Information	2019-10-27 11:45:43	Kernel-General
Information	2019-10-27 11:45:43	Kernel-Boot
Information	2019-10-27 11:45:43	Kernel-Boot

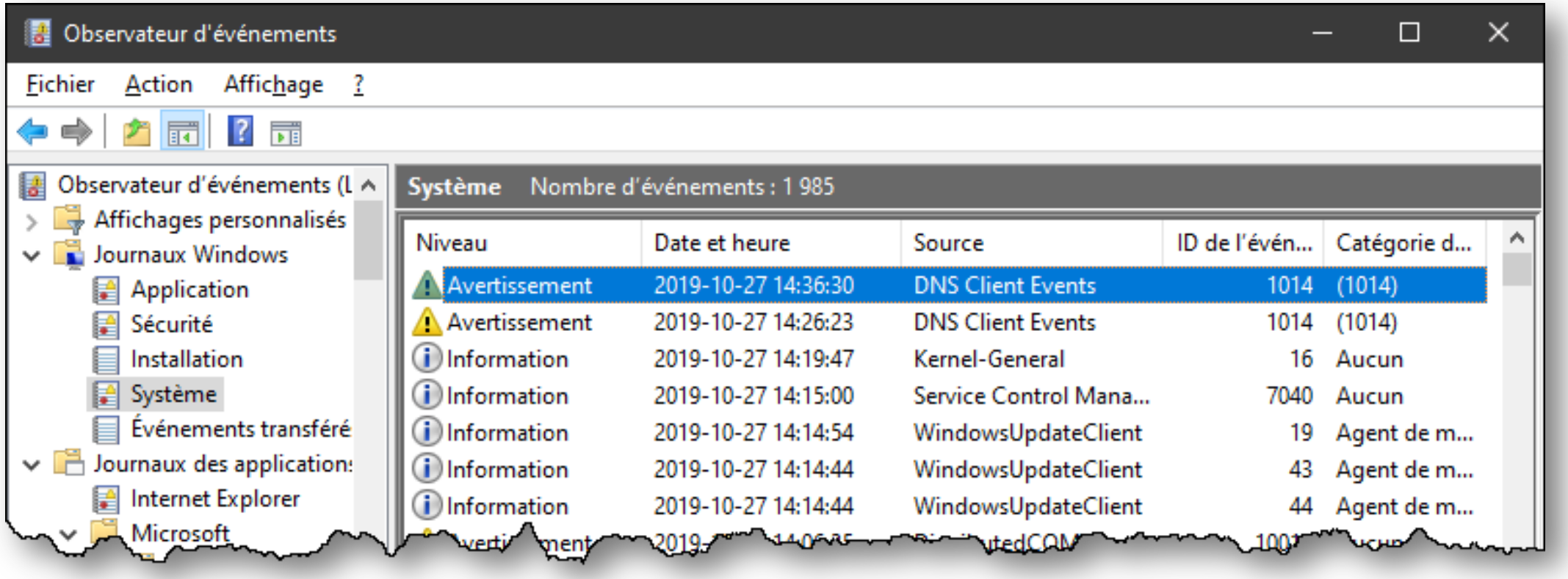
Journal Application

Évènements reliés au fonctionnement d'un programme, d'un pilote ou d'un service.



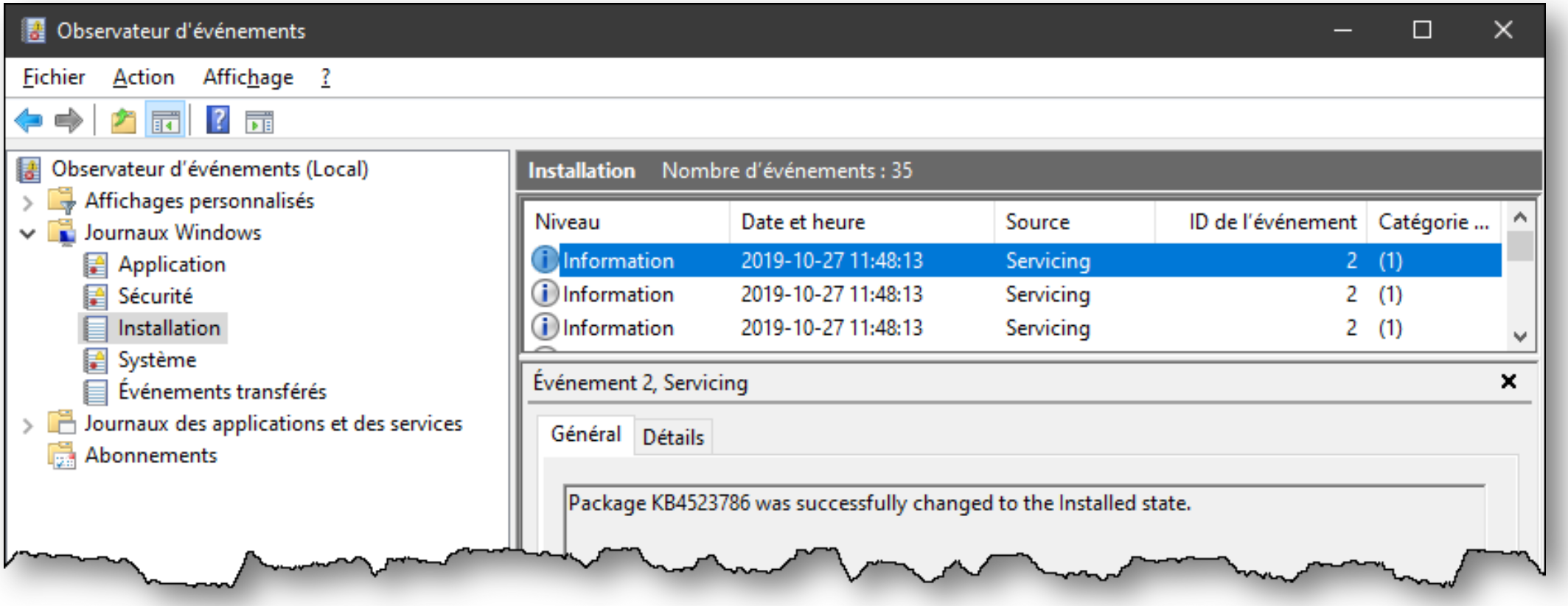
Journal Système

Évènements reliés aux composants internes de Windows et de son noyau.



Journal Installation

Événements touchant l'installation de composants de Windows tels que les mises à jour du système.



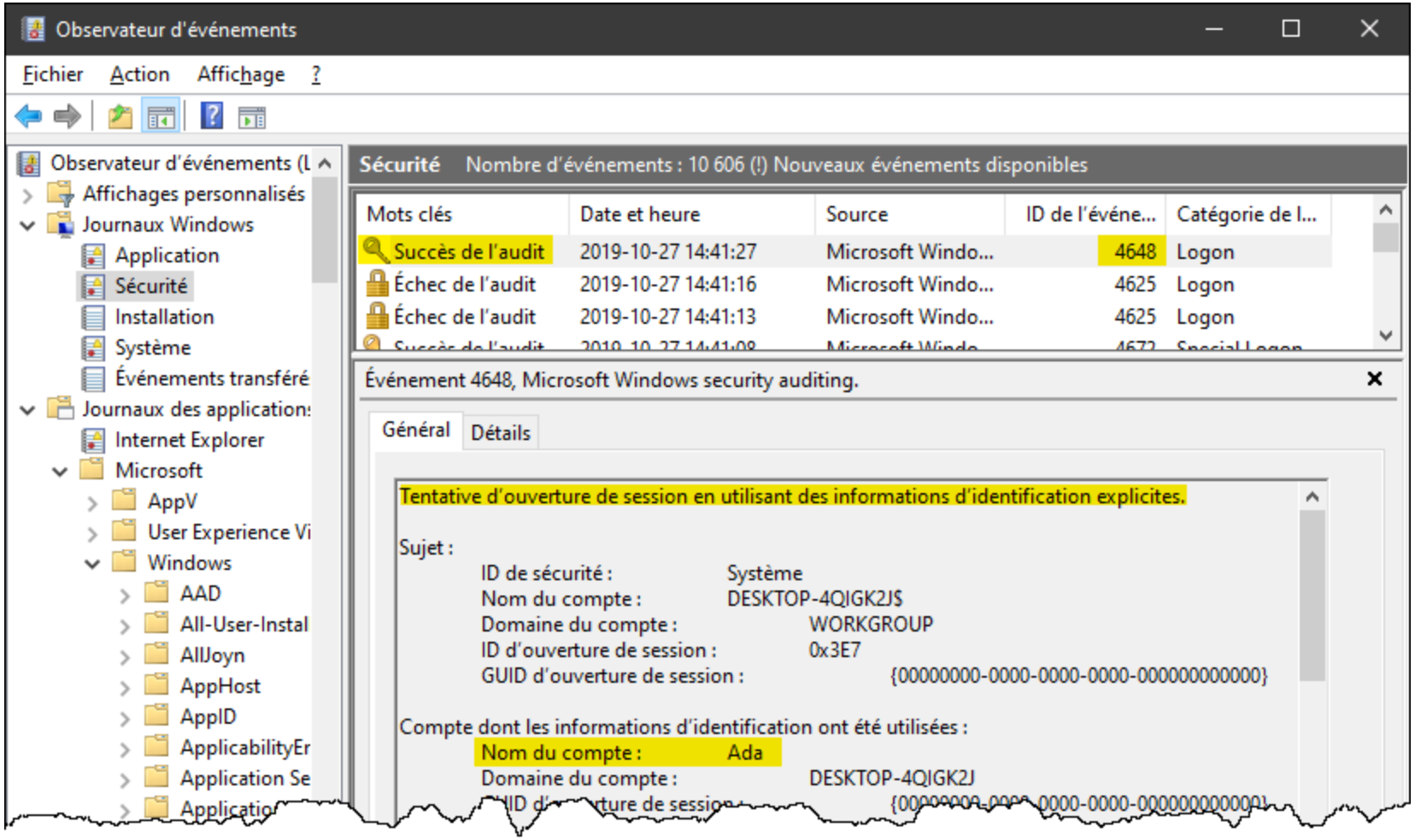
Journal de sécurité

Contient des informations relatives à la sécurité :

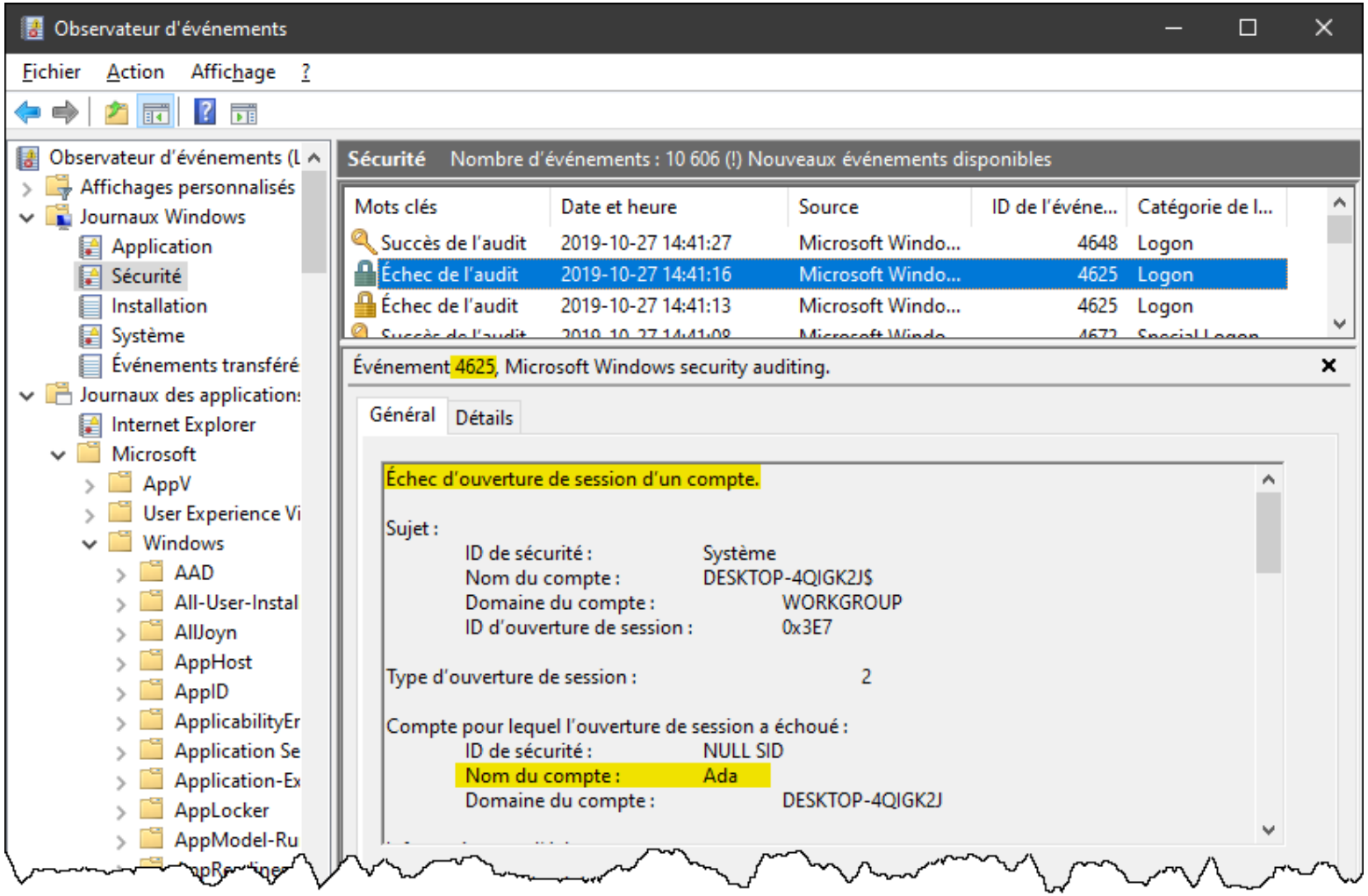
- Tentatives d'ouverture de session
- Accès à des données sensibles
- Échec d'ouverture de session (mauvais mot de passe)
- Élévation de privilèges
- Activation ou désactivation d'éléments de sécurité (pare-feu, antivirus, etc.)

Très utile pour faire des audits de sécurité

Journal de sécurité : succès

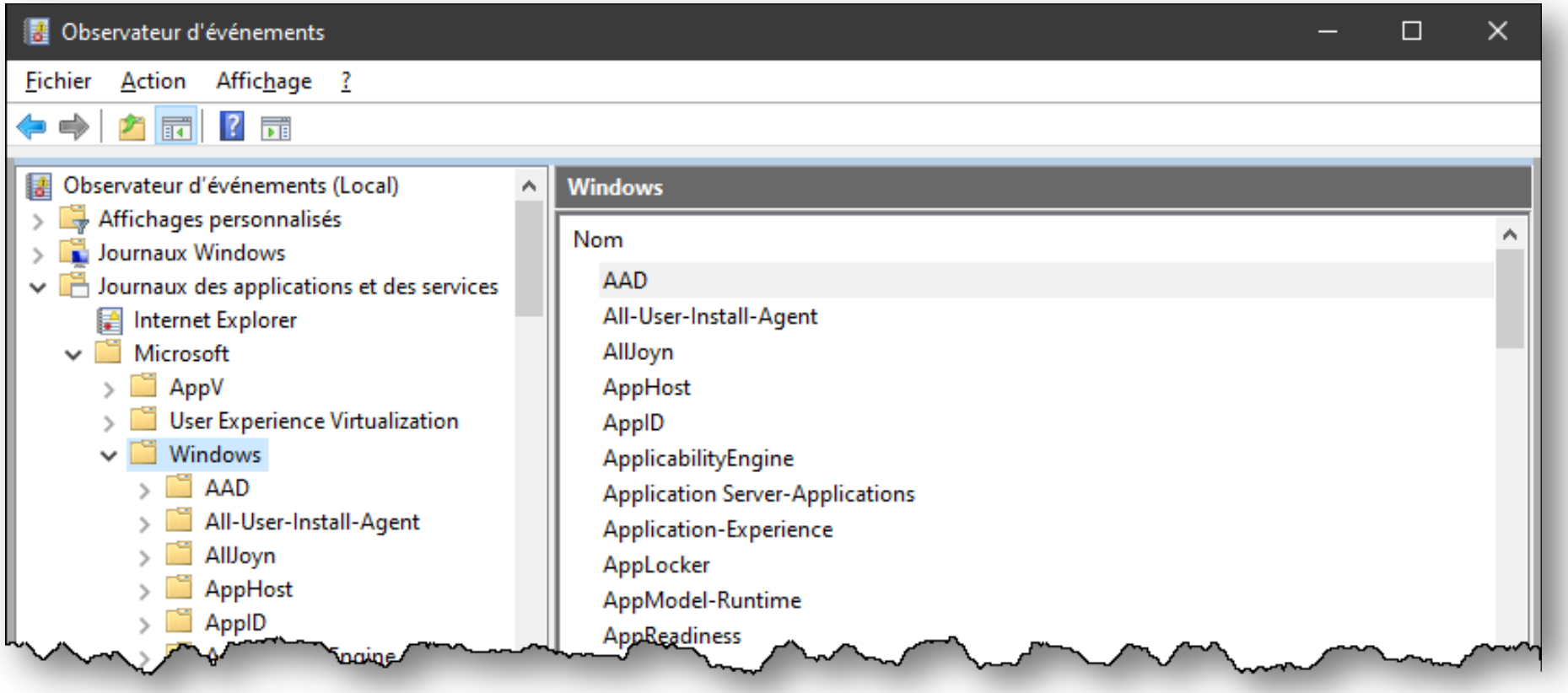


Journal de sécurité : échec



Journaux spécialisés

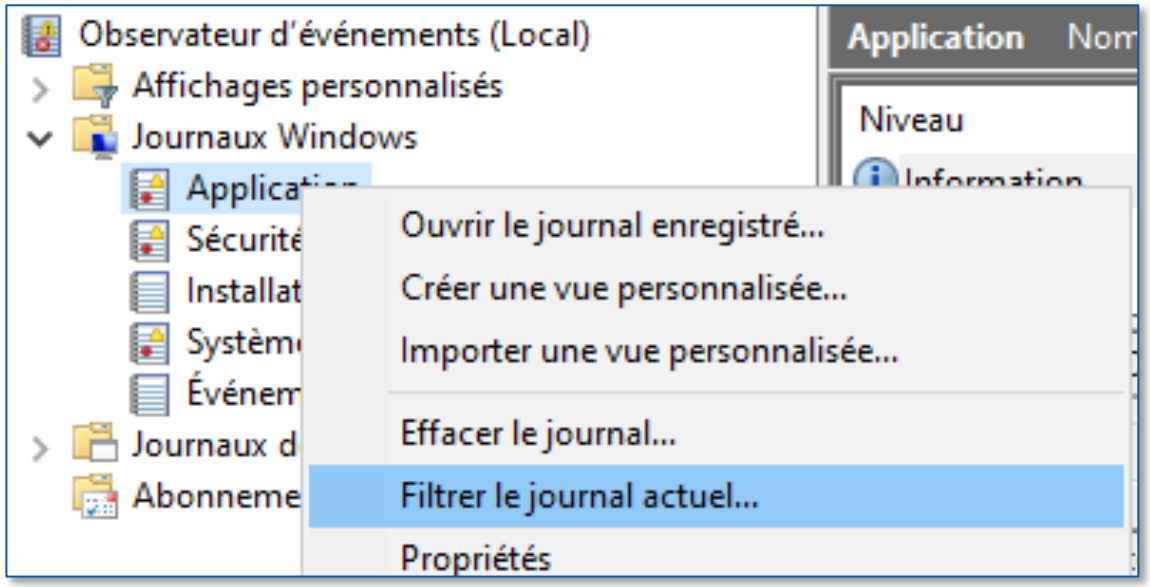
Certaines applications et composants de Windows possèdent leur journal spécifique.



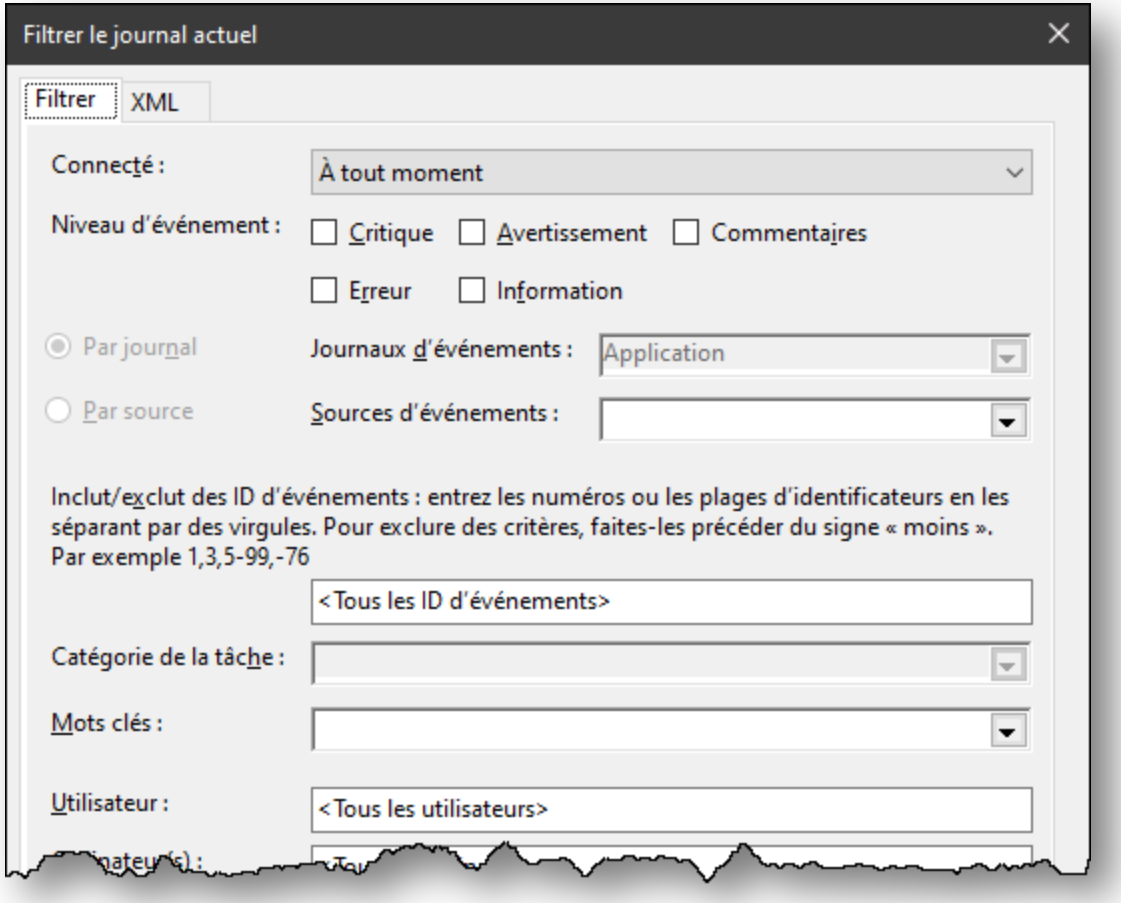
Filtrer le journal

On peut appliquer un filtre pour faire ressortir certains évènements :

- Les erreurs seulement
- Les évènements touchant un composant précis
- Les évènements survenus depuis une certaine date
- etc.



Filtrer le journal



Évènements d'administration

Il s'agit d'un filtre prédéfini, qui montre les évènements critiques, erreurs et avertissements de tous les journaux principaux.