



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

Déetecter 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.



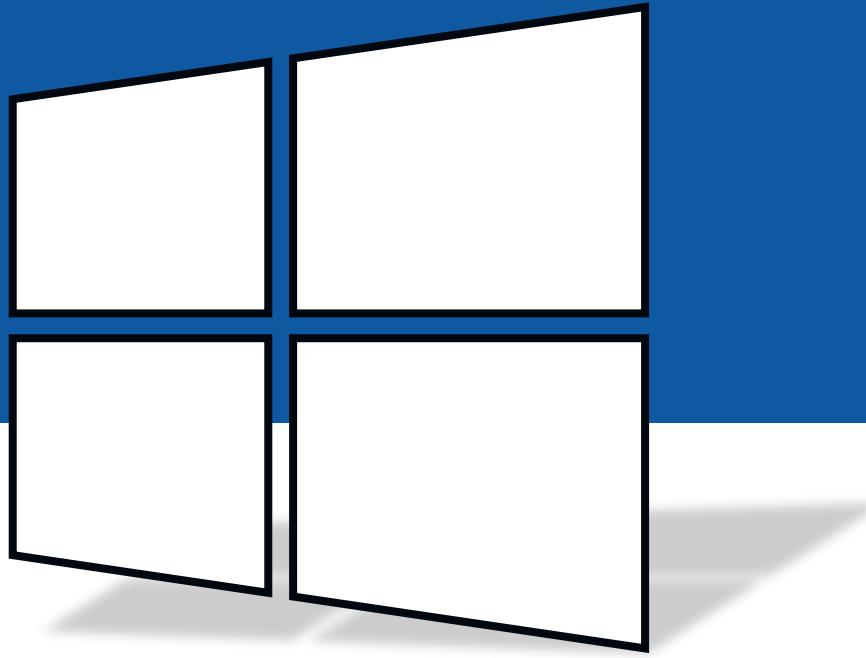
Fichiers log en format texte (rappel)

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

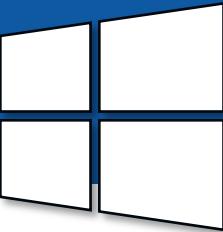
Chaque **événement** occupe généralement **une ligne** de texte

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.

The screenshot shows a Windows File Explorer window titled "CBS". The address bar indicates the path: "Ce PC > Disque local (C:) > Windows > Logs > CBS". The list view displays three files:

Nom	Modifié le	Type	Taille
CBS.log	2019-10-27 15:29	Document texte	1 987 Ko
CbsPersist_20191016014937.cab	2019-10-15 21:32	Fichier CAB	1 379 Ko
CbsP..._20191027155524...	2019-10-27 11:51	Document texte	50 074 Ko

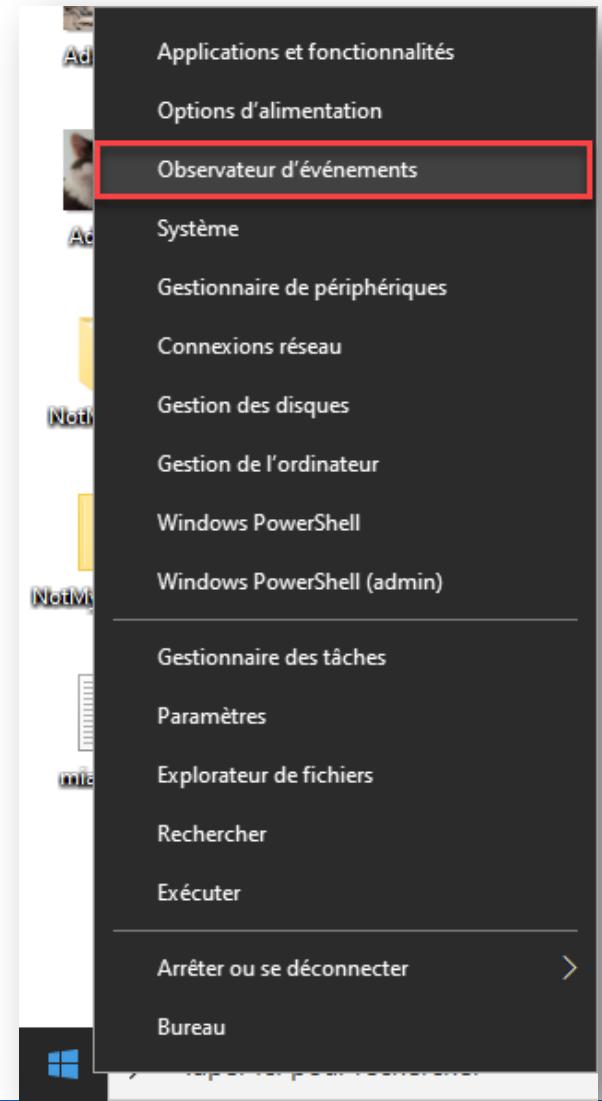
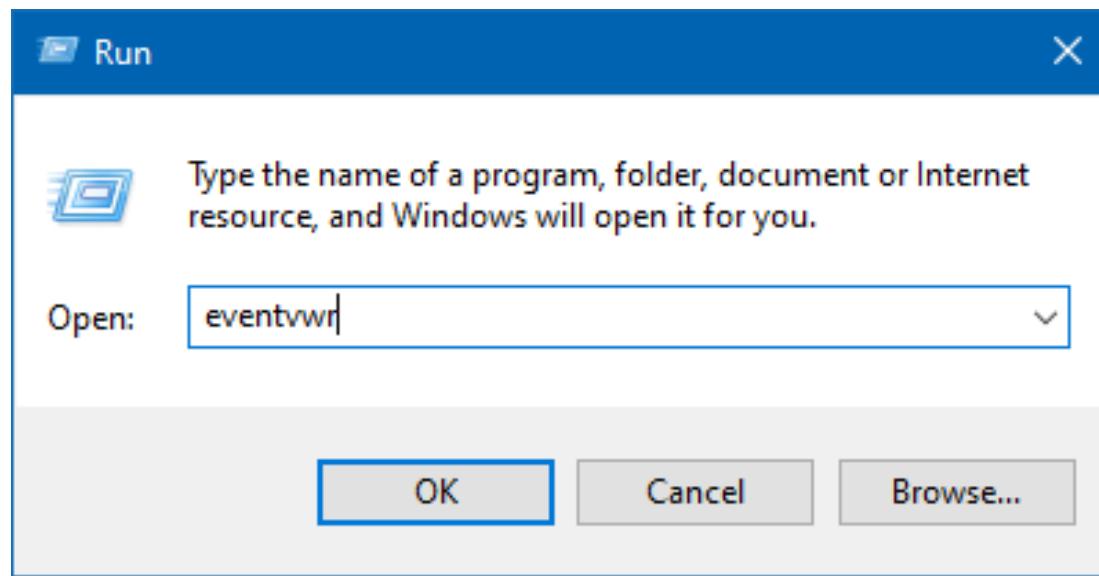
The screenshot shows a Windows Notepad window titled "CBS.log - Bloc-notes". The menu bar includes "Fichier", "Edition", "Format", "Affichage", and "Aide". The content area displays the following log entries:

```
2019-10-27 11:52:11, Info CBS TI: --- Initializing Trusted Installer ---
2019-10-27 11:52:11, Info CBS TI: Last boot time: 2019-10-27 11:46:57.500
2019-10-27 11:52:11, Info CBS Starting TrustedInstaller initialization.
2019-10-27 11:52:11, Info CBS [locks] New lock added: CCbsPublicSession[lock]
```

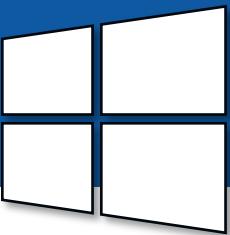
Journaux d'événements



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



Observateur d'évènements



Screenshot of the Windows Event Viewer application window.

The main pane shows a table of events:

Niveau	Date et heure	Source	ID de l'événement	Catégorie
! Erreur	2019-10-27 13:29:21	Application ...	1002 (101)	
Information	2019-10-27 13:28:22	Windows Er...	1001	Aucun
Information	2019-10-27 13:28:21	Windows Er...	1001	Aucun
Information	2019-10-27 13:28:11	Windows Er...	1001	Aucun
Information	2019-10-27 13:19:13	Security-SPP	16384	Aucun

The details pane shows the properties for event ID 1002, titled "Application Hang".

Général

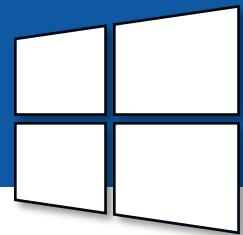
Le programme notmyfault64.exe version 4.20.0.0 a cessé d'interagir avec Windows et a été fermé. Pour voir si plus d'informations sur le problème sont disponibles, vérifiez l'historique des problèmes dans le Panneau de configuration Sécurité et maintenance.
ID de processus : 13e0
Heure de début : 01d58ceb7ca64c6d

Détails

Journal :	Application		
Source :	Application Hang	Connecté :	2019-10-27 13:29:21
Événement :	1002	Catégorie :	(101)
Niveau :	Erreur	Mots-clés :	Classique
Utilisateur :	N/A	Ordinateur :	DESKTOP-4QIGK2J
Opcode :			

Informations : [Aide sur le Journal](#)

Classement des évènements



Information

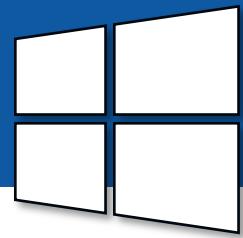
Avertissement

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.

Observateur d'événements

Fichier Action Affichage ?

Application Nombre d'événements : 798 (!) Nouveaux événements disponibles

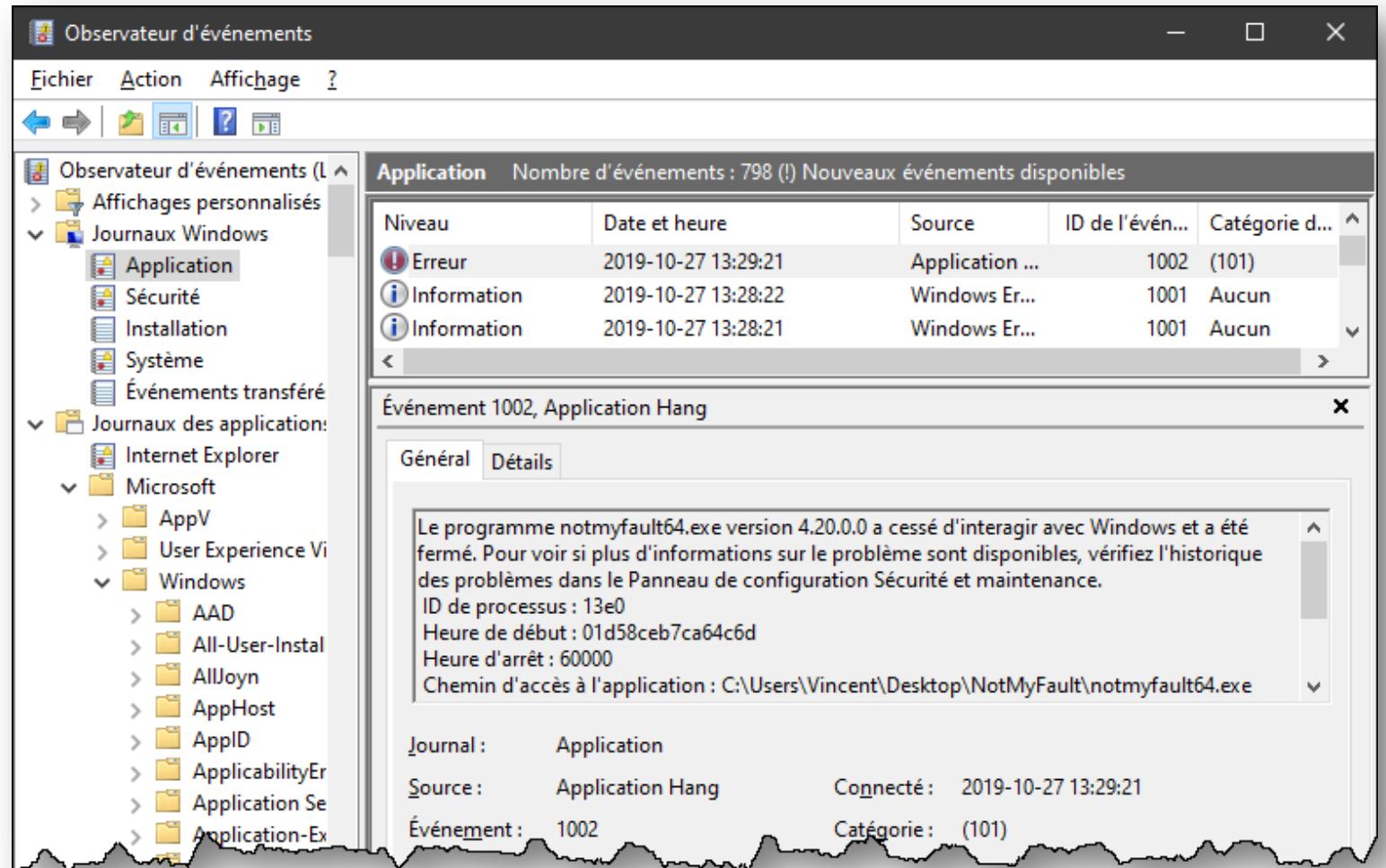
Niveau	Date et heure	Source	ID de l'évén...	Catégorie d...
Erreur	2019-10-27 13:29:21	Application ...	1002	(101)
Information	2019-10-27 13:28:22	Windows Er...	1001	Aucun
Information	2019-10-27 13:28:21	Windows Er...	1001	Aucun

Événement 1002, Application Hang

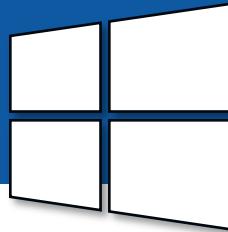
Général Détails

Le programme notmyfault64.exe version 4.20.0.0 a cessé d'interagir avec Windows et a été fermé. Pour voir si plus d'informations sur le problème sont disponibles, vérifiez l'historique des problèmes dans le Panneau de configuration Sécurité et maintenance.
ID de processus : 13e0
Heure de début : 01d58ceb7ca64c6d
Heure d'arrêt : 60000
Chemin d'accès à l'application : C:\Users\Vincent\Desktop\NotMyFault\notmyfault64.exe

Journal : Application
Source : Application Hang Connecté : 2019-10-27 13:29:21
Événement : 1002 Catégorie : (101)



Journal Système

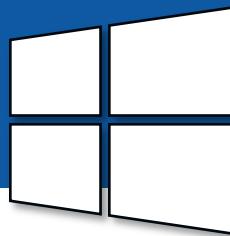


Évènements reliés aux composants internes de Windows et de son noyau.

The screenshot shows the Windows Event Viewer interface. The title bar reads "Observateur d'événements". The menu bar includes "Fichier", "Action", "Affichage", and a question mark icon. Below the menu is a toolbar with icons for back, forward, search, and filters. The left pane displays a navigation tree with "Observateur d'événements (L)", "Affichages personnalisés", "Journaux Windows" (selected), "Application", "Sécurité", "Installation", "Système" (selected), "Événements transféré", "Journaux des applications" (expanded), "Internet Explorer", and "Microsoft". The right pane shows a table titled "Système" with "Nombre d'événements : 1 985". The columns are "Niveau", "Date et heure", "Source", "ID de l'événement", and "Catégorie d'événement". The first two rows are highlighted in blue, indicating selected events. The data is as follows:

Niveau	Date et heure	Source	ID de l'événement	Catégorie d'événement
Avertissement	2019-10-27 14:36:30	DNS Client Events	1014 (1014)	
Avertissement	2019-10-27 14:26:23	DNS Client Events	1014 (1014)	
Information	2019-10-27 14:19:47	Kernel-General	16	Aucun
Information	2019-10-27 14:15:00	Service Control Mana...	7040	Aucun
Information	2019-10-27 14:14:54	WindowsUpdateClient	19	Agent de m...
Information	2019-10-27 14:14:44	WindowsUpdateClient	43	Agent de m...
Information	2019-10-27 14:14:44	WindowsUpdateClient	44	Agent de m...

Journal Installation

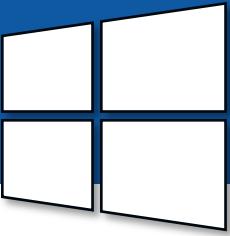


Événements touchant l'installation de composants de Windows tels que les mises à jour du système.

The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with 'Observateur d'événements (Local)', 'Affichages personnalisés', 'Journaux Windows' (selected), containing 'Application', 'Sécurité', 'Installation' (selected), 'Système', and 'Événements transférés'. Below these are 'Journaux des applications et des services' and 'Abonnements'. The right pane shows the 'Installation' log with 35 events. A specific event is selected, showing details: 'Niveau' (Information), 'Date et heure' (2019-10-27 11:48:13), 'Source' (Servicing), 'ID de l'événement' (2 (1)), and 'Catégorie ...'. The event text reads: 'Package KB4523786 was successfully changed to the Installed state.'

Niveau	Date et heure	Source	ID de l'événement	Catégorie ...
Information	2019-10-27 11:48:13	Servicing	2 (1)	
Information	2019-10-27 11:48:13	Servicing	2 (1)	
Information	2019-10-27 11:48:13	Servicing	2 (1)	

Journal de sécurité

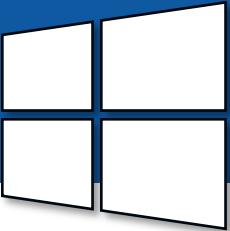


Contient des informations relatives à la sécurité :

- > 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



Sécurité Nombre d'événements : 10 606 (!) Nouveaux événements disponibles

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de l'événement
Succès de l'audit	2019-10-27 14:41:27	Microsoft Windo...	4648	Logon
Échec de l'audit	2019-10-27 14:41:16	Microsoft Windo...	4625	Logon
Échec de l'audit	2019-10-27 14:41:13	Microsoft Windo...	4625	Logon
Succès de l'audit	2019-10-27 14:41:00	Microsoft Windo...	4677	Special Logon

Événement 4648, Microsoft Windows security auditing.

Général Détails

Tentative d'ouverture de session en utilisant des informations d'identification explicites.

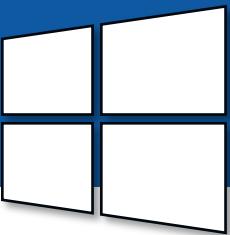
Sujet :

ID de sécurité :	Système
Nom du compte :	DESKTOP-4QIGK2\$
Domaine du compte :	WORKGROUP
ID d'ouverture de session :	0x3E7
GUID d'ouverture de session :	{00000000-0000-0000-0000-000000000000}

Compte dont les informations d'identification ont été utilisées :

Nom du compte :	Ada
Domaine du compte :	DESKTOP-4QIGK2\$
ID d'ouverture de session :	{00000000-0000-0000-0000-000000000000}

Journal de sécurité : échec



Observateur d'événements

Fichier Action Affichage ?

← → | ↗ ↘ | ? |

Sécurité Nombre d'événements : 10 606 (!) Nouveaux événements disponibles

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de l'événement
Success de l'audit	2019-10-27 14:41:27	Microsoft Windo...	4648	Logon
Échec de l'audit	2019-10-27 14:41:16	Microsoft Windo...	4625	Logon
Échec de l'audit	2019-10-27 14:41:13	Microsoft Windo...	4625	Logon
Success de l'audit	2019-10-27 14:41:09	Microsoft Windo...	4672	Special Logon

Événement 4625, Microsoft Windows security auditing.

Général Détails

Échec d'ouverture de session d'un compte.

Sujet :

ID de sécurité :	Système
Nom du compte :	DESKTOP-4QIGK2J\$
Domaine du compte :	WORKGROUP
ID d'ouverture de session :	0x3E7

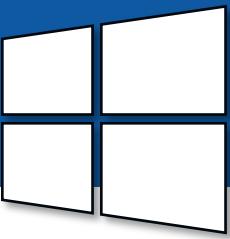
Type d'ouverture de session : 2

Compte pour lequel l'ouverture de session a échoué :

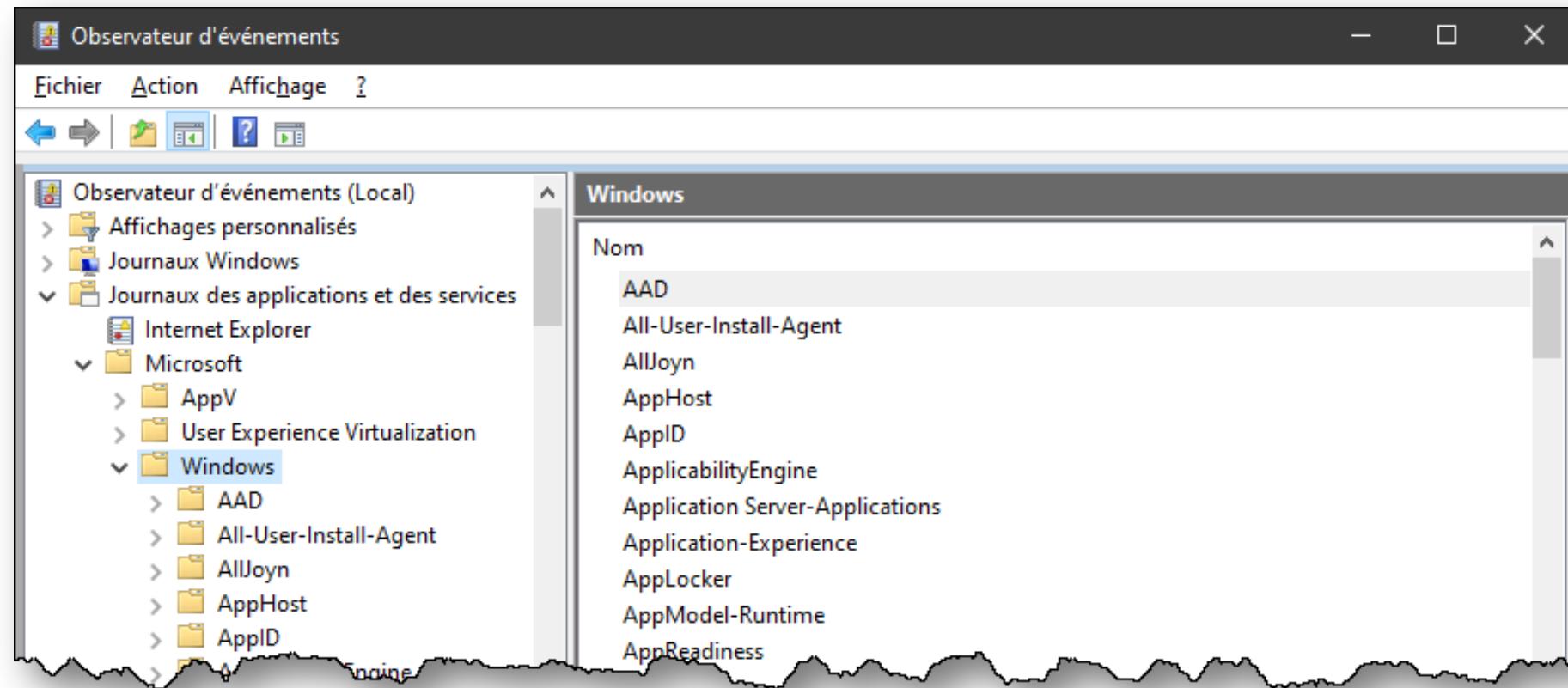
ID de sécurité :	NULL SID
Nom du compte :	Ada
Domaine du compte :	DESKTOP-4QIGK2J

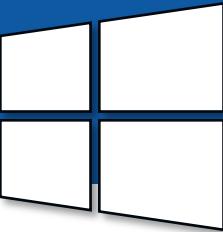
A screenshot of the Windows Event Viewer application. The left pane shows a tree view of logs: 'Affichages personnalisés', 'Journaux Windows' (selected), 'Application', 'Sécurité' (highlighted in yellow), 'Installation', 'Système', 'Événements transférés', and 'Journaux des applications' (expanded) with 'Internet Explorer' and 'Microsoft' (selected). The right pane displays a list of events under 'Sécurité'. The fourth event in the list is highlighted in yellow and has a tooltip 'Échec d'ouverture de session d'un compte.' (Failed logon attempt). The event details show it failed for user 'Ada' (Nom du compte) on domain 'DESKTOP-4QIGK2J' (Domaine du compte) with ID 'NULL SID' (ID de sécurité). The event type is '2' (Type d'ouverture de session).

Journaux spécialisés



Certaines applications et composants de Windows possèdent leur journal spécifique.

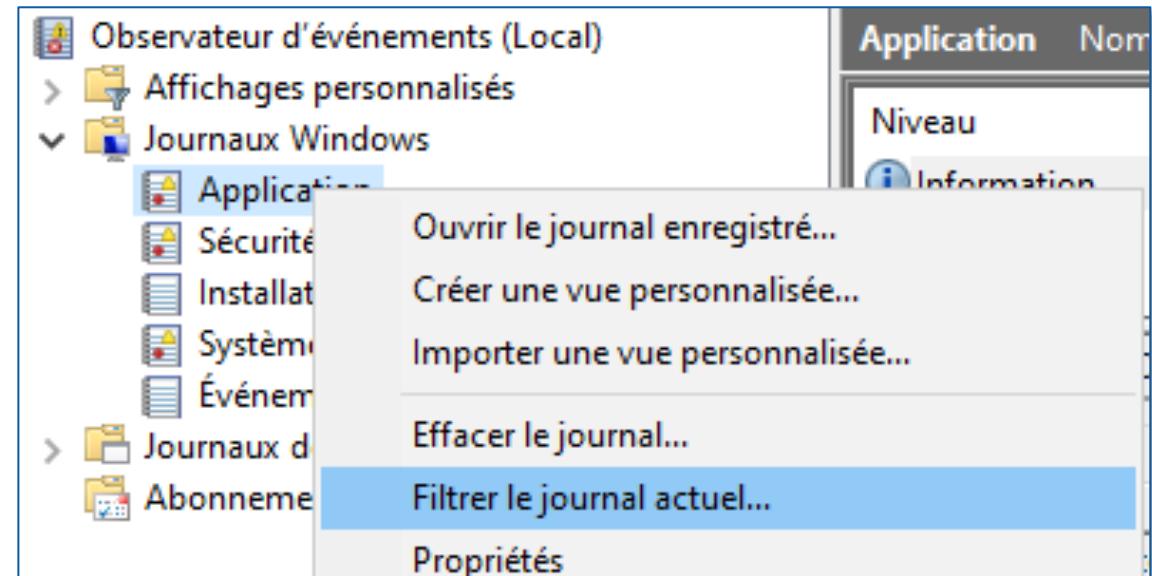




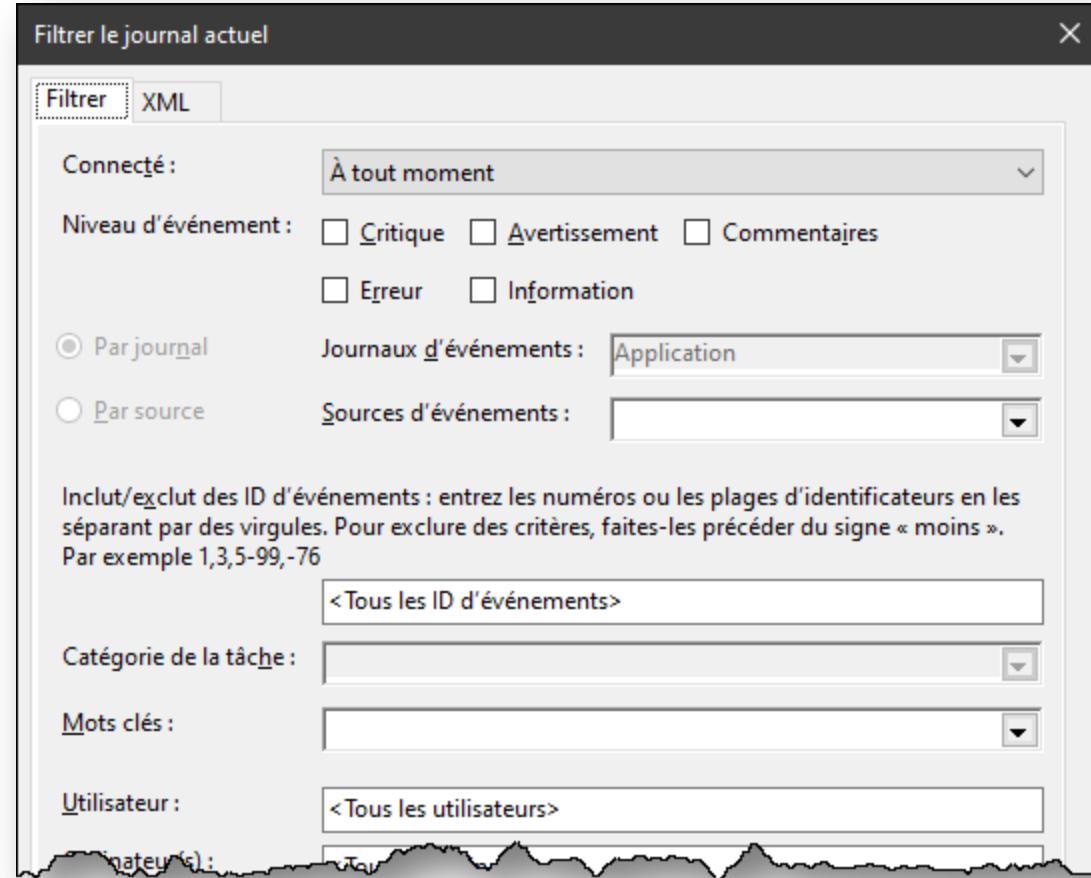
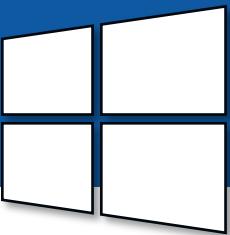
Filtrer le journal

On peut appliquer un filtre pour faire ressortir certains évènements :

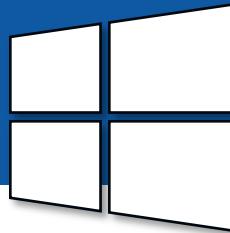
- > Les erreurs seulement
- > Les évènements touchant un composant précis
- > Les évènements survenus depuis une certaine date
- > etc.



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.

