



Journalisation Windows

Gestion de la journalisation sous Windows

Automne 2022

Séance 10C



- ✓ 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 événements les plus importants.



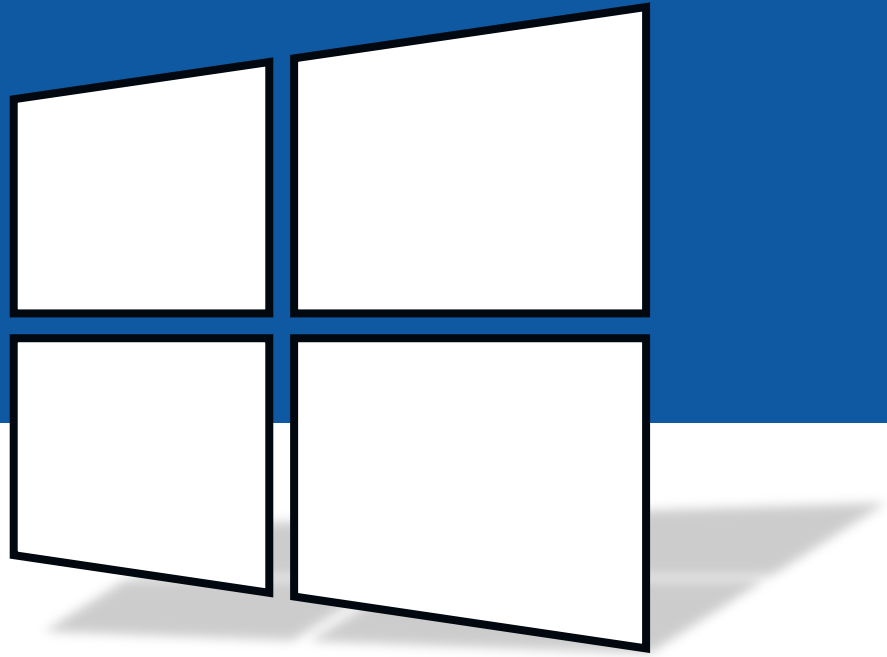
Fichiers log en format texte (rappel)

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

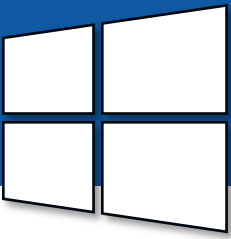
Chaque évènement est **horodaté**

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

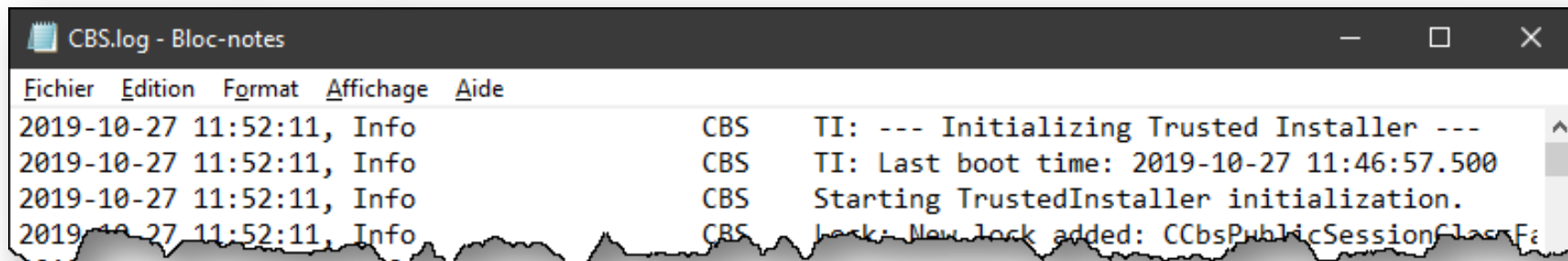
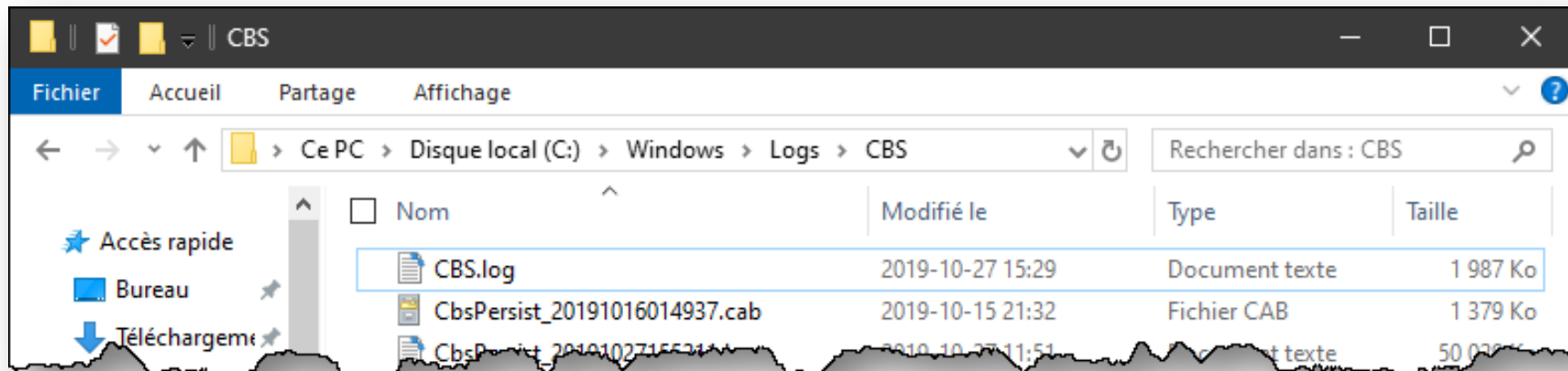


Windows

Journaux textuels



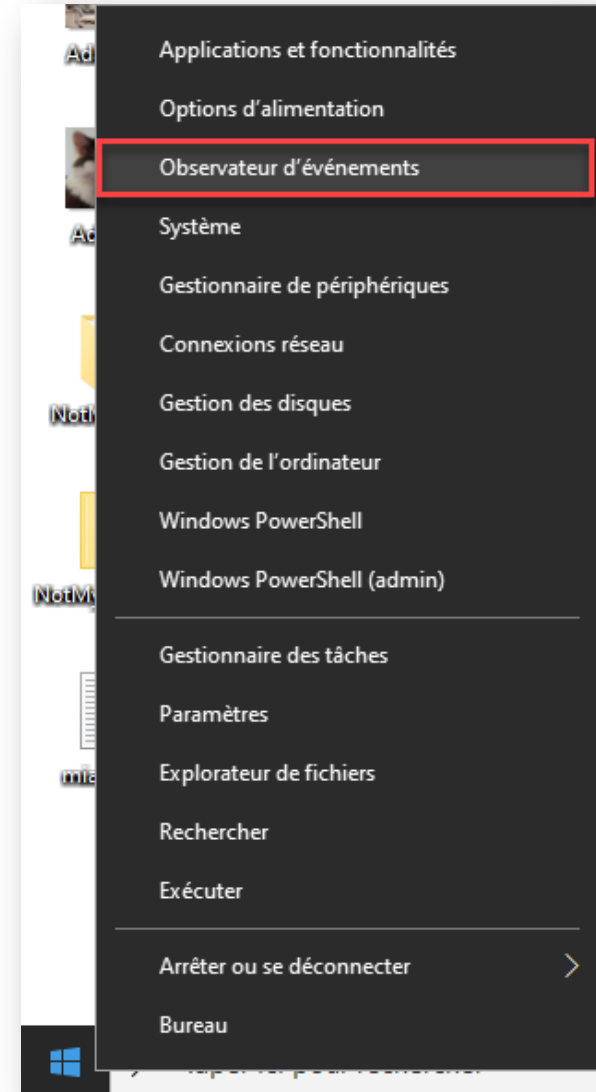
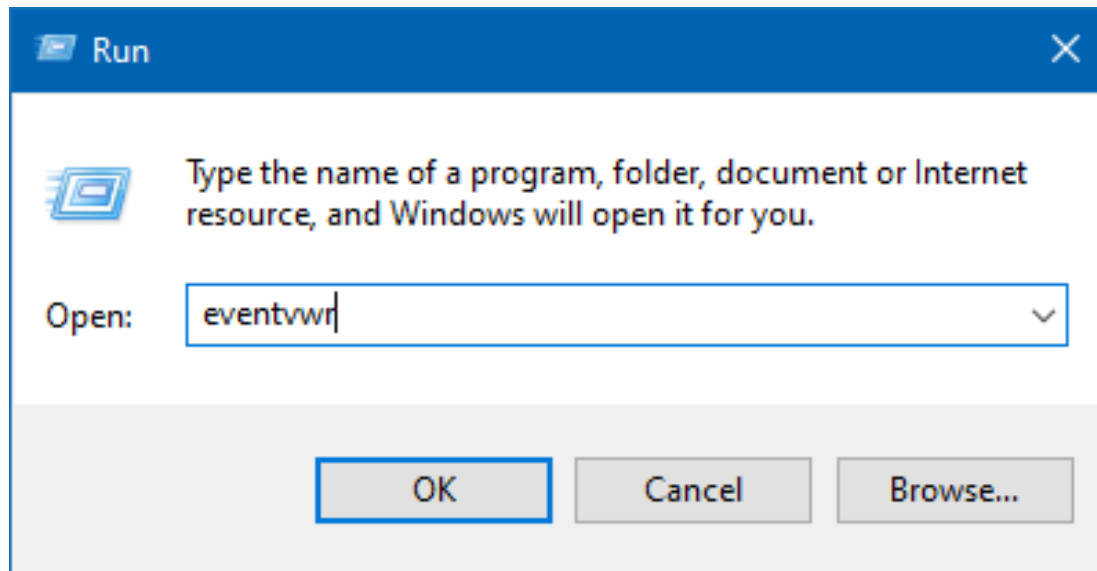
Certaines applications et composants effectuent leur journalisation dans de simples fichiers texte.



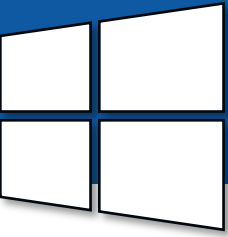
Journaux d'événements



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



Observateur d'évènements



The screenshot shows the Windows Event Viewer application. The left pane displays the tree view with 'Journaux Windows' expanded, showing 'Application' selected. The right pane shows a list of events for the 'Application' log, with event 1002 (Error) selected. Below the list, the details for event 1002 are displayed, including a description of the application hang and various metadata.

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
Information	2019-10-27 13:28:11	Windows Er...	1001	Aucun
Information	2019-10-27 13:19:13	Security-SPP	16384	Aucun

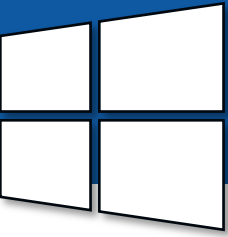
Événement 1002, Application Hang

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

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

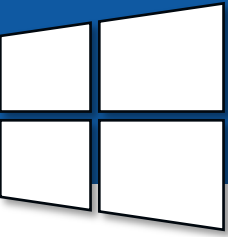
Avertissement

Erreur

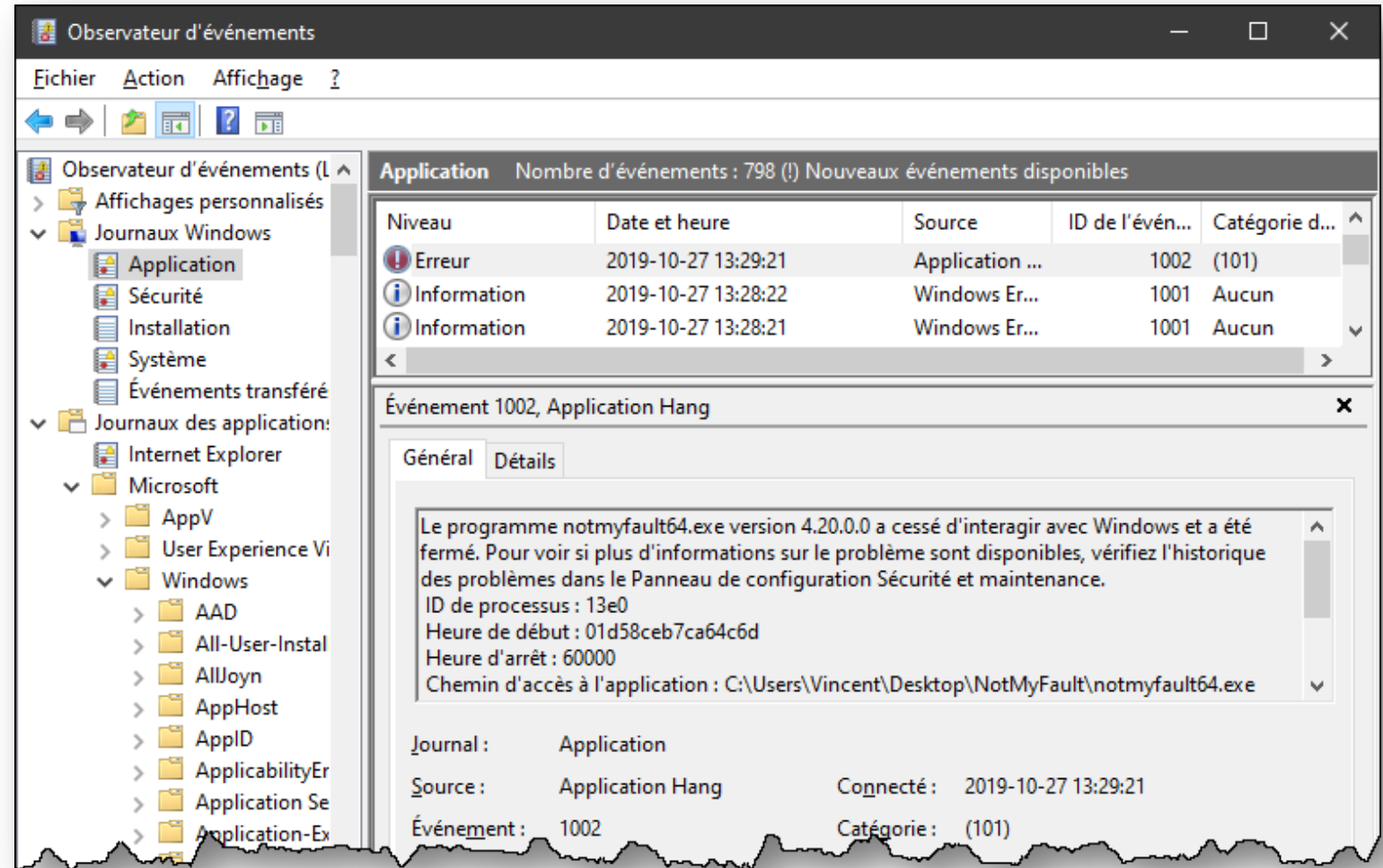
Critique

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

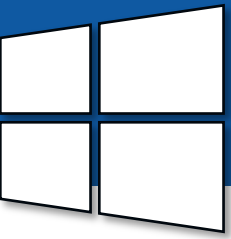
Journal Application



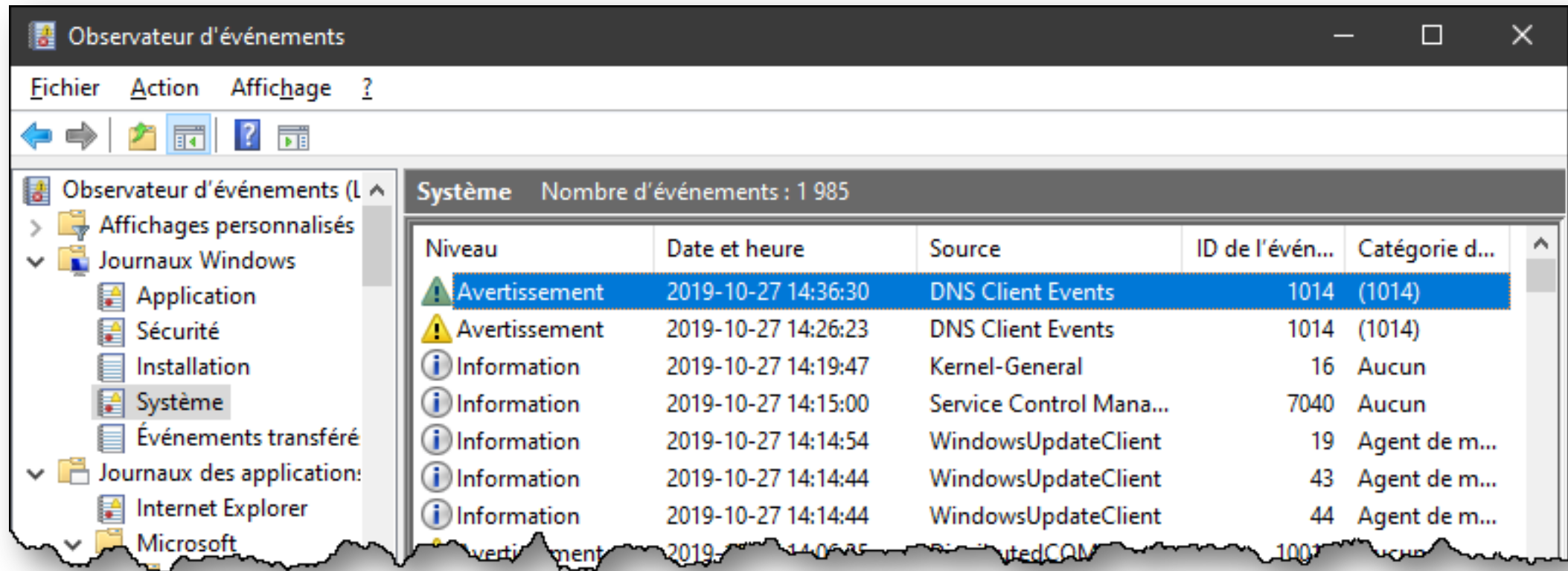
Évènements reliés au fonctionnement d'un programme, d'un pilote ou d'un service.



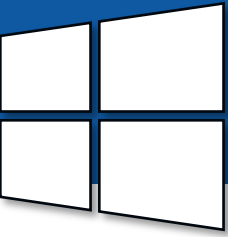
Journal Système



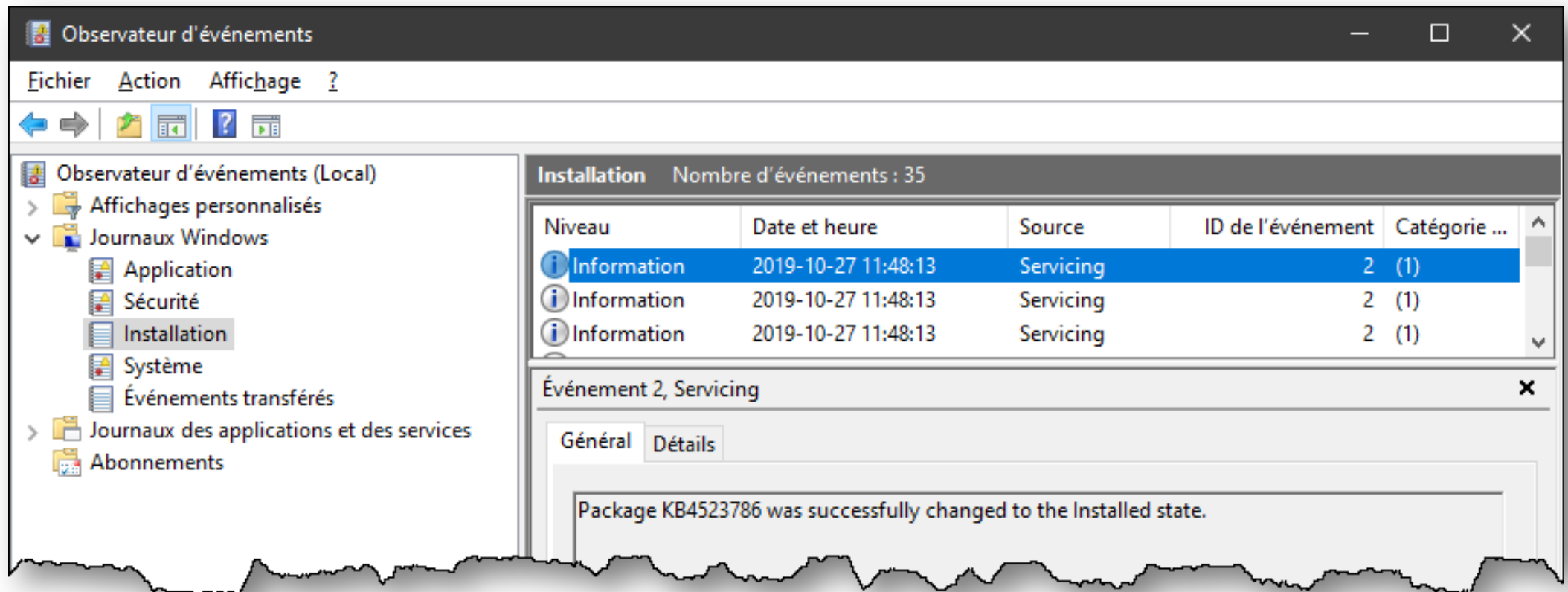
Évènements reliés aux composants **internes** de Windows et de son **noyau**.



Journal Installation



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



Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local)

- Affichages personnalisés
- Journaux Windows
 - Application
 - Sécurité
 - Installation
 - Système
 - Événements transférés
- Journaux des applications et des services
- Abonnements

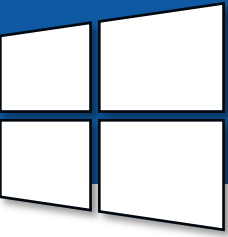
Installation Nombre d'événements : 35

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)	

Événement 2, Servicing

Général Détails

Package KB4523786 was successfully changed to the Installed state.

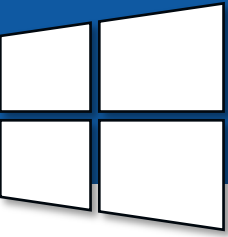


Contient des informations relatives à la sécurité :

- > 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



The screenshot shows the Windows Event Viewer (Observateur d'événements) window. The left pane shows the tree view with 'Journaux Windows' expanded, and 'Sécurité' selected. The right pane shows a list of security events. Event 4648 is highlighted, showing a successful login for user 'Ada'. The details pane for event 4648 is open, showing the 'Général' tab. The event description is 'Tentative d'ouverture de session en utilisant des informations d'identification explicites.' The subject details include the security ID (SYSTEM), account name (DESKTOP-4QIGK2JS), domain (WORKGROUP), session ID (0x3E7), and session GUID. The account used for authentication is 'Ada' on 'DESKTOP-4QIGK2JS'.

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 Windows security auditing	4648	Logon
Échec de l'audit	2019-10-27 14:41:16	Microsoft Windows security auditing	4625	Logon
Échec de l'audit	2019-10-27 14:41:13	Microsoft Windows security auditing	4625	Logon
Succès de l'audit	2019-10-27 14:41:08	Microsoft Windows security auditing	4672	Special Logon

Événement 4648, Microsoft Windows security auditing.

Général Détails

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

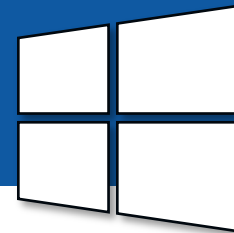
Sujet :

ID de sécurité :	SYSTEM
Nom du compte :	DESKTOP-4QIGK2JS
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-4QIGK2JS
ID d'ouverture de session :	{00000000-0000-0000-0000-000000000000}

Journal de sécurité : échec



Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (L)

- Affichages personnalisés
- Journal Windows
 - Application
 - Sécurité
 - Installation
 - Système
 - Événements transféré
- Journal des applications
 - Internet Explorer
 - Microsoft
 - AppV
 - User Experience Vi
 - Windows
 - AAD
 - All-User-Instal
 - AllJoyn
 - AppHost
 - AppID
 - ApplicabilityEr
 - Application Se
 - Application-Ex
 - AppLocker
 - AppModel-Ru
 - AppRevitiner

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 14:41:08	Microsoft Windo...	4672	Special Logon

Événement 4625, Microsoft Windows security auditing.

Général Détails

Échec d'ouverture de session d'un compte.

Sujet :

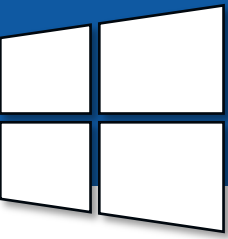
ID de sécurité :	Système
Nom du compte :	DESKTOP-4QIGK2JS
Domaine du compte :	WORKGROUP
ID d'ouverture de session :	0x3E7

Type d'ouverture de session : 2

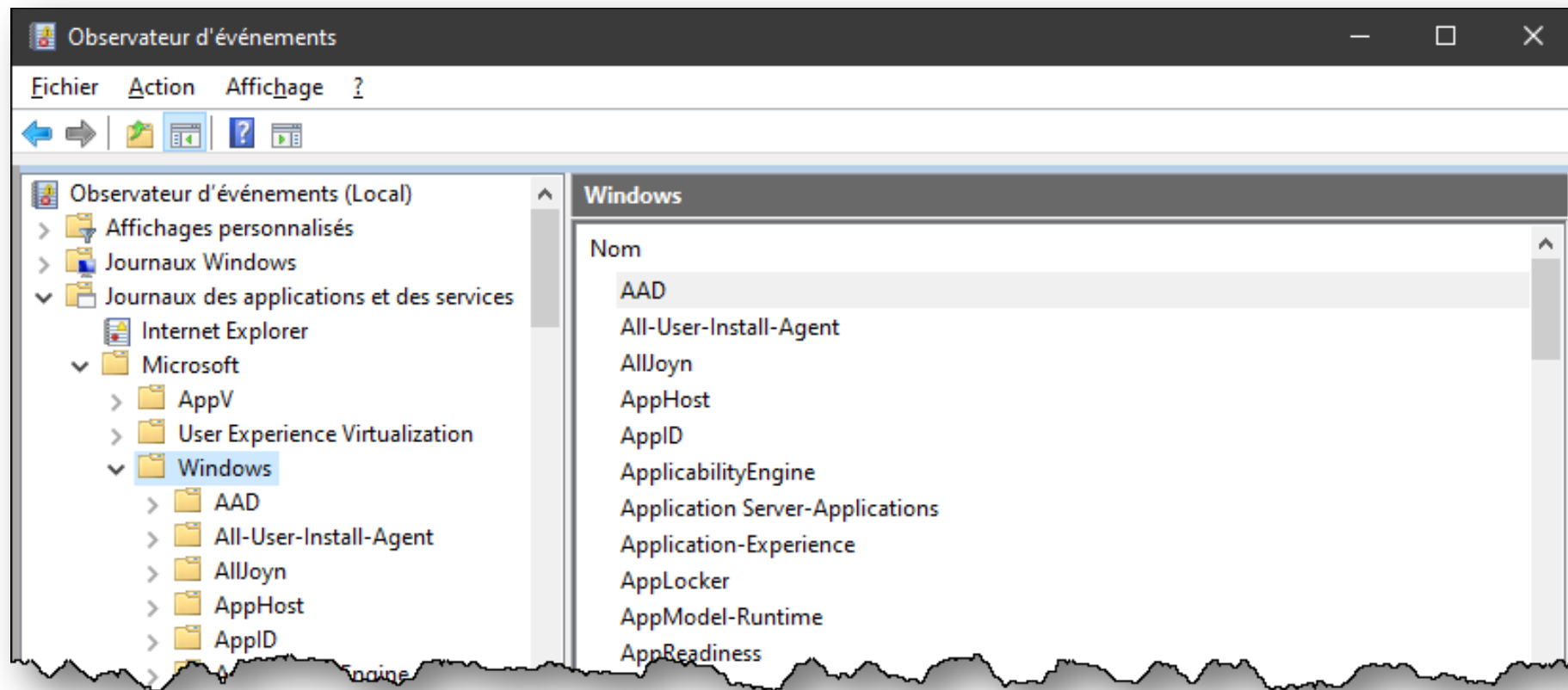
Compte pour lequel l'ouverture de session a échoué :

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

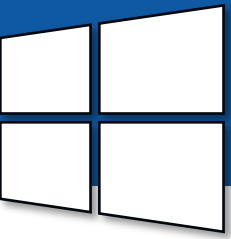
Journaux spécialisés



Certaines applications et composants de Windows possèdent leur journal spécifique.

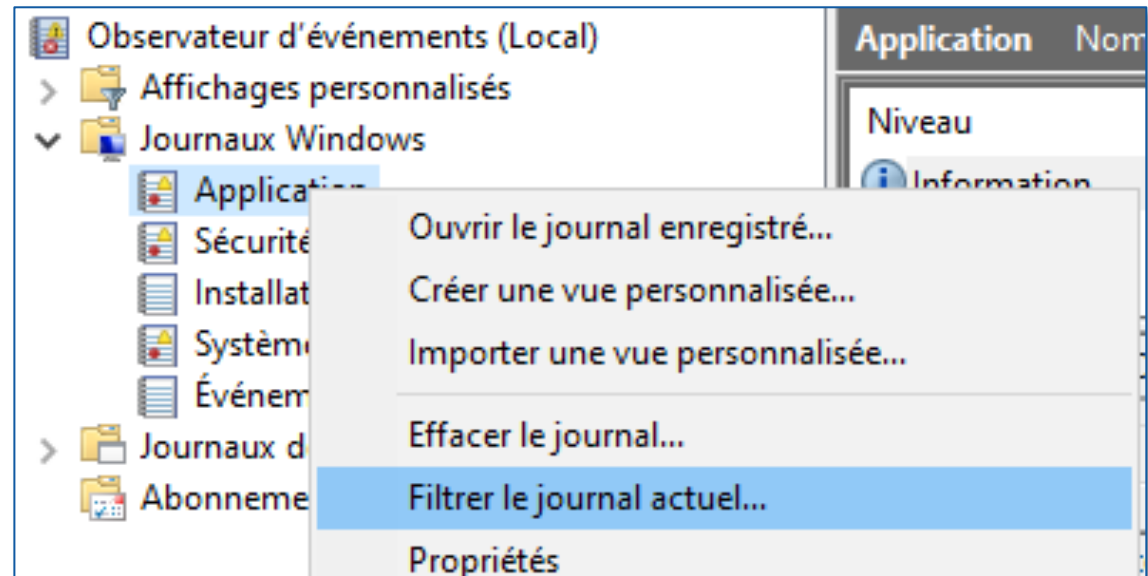


Filtrer le journal

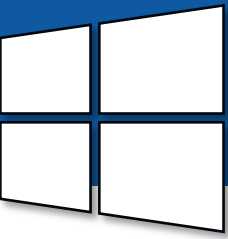


On peut appliquer un filtre pour faire ressortir certains évènements :

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



Filtrer le journal



Filtrer le journal actuel

Filtrer XML

Connecté : À tout moment

Niveau d'événement : ☐ Critique ☐ Avertissement ☐ Commentaires
☐ Erreur ☐ Information

☒ Par journal Journaux d'événements : Application

☐ Par source Sources d'événements :

Inclut/exclut des ID d'événements : entrez les numéros ou les plages d'identificateurs en les séparant par des virgules. Pour exclure des critères, faites-les précéder du signe « moins ». Par exemple 1,3,5-99,-76

<Tous les ID d'événements>

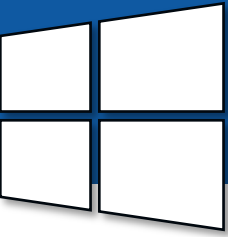
Catégorie de la tâche :

Mots clés :

Utilisateur : <Tous les utilisateurs>

Utilisateur(s) :

Évènements d'administration



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

