Gestion des journaux de Windows

Contenu

- **Les commandes Get-EventLog et Get-WinEvent**
- **Récupérer des entrées d’un journal d’événements**
- **Ajouter une entrée à un journal d’événement**

Les commandes Get-EventLog et Get-WinEvent

Get-EventLog et Get-WinEvent

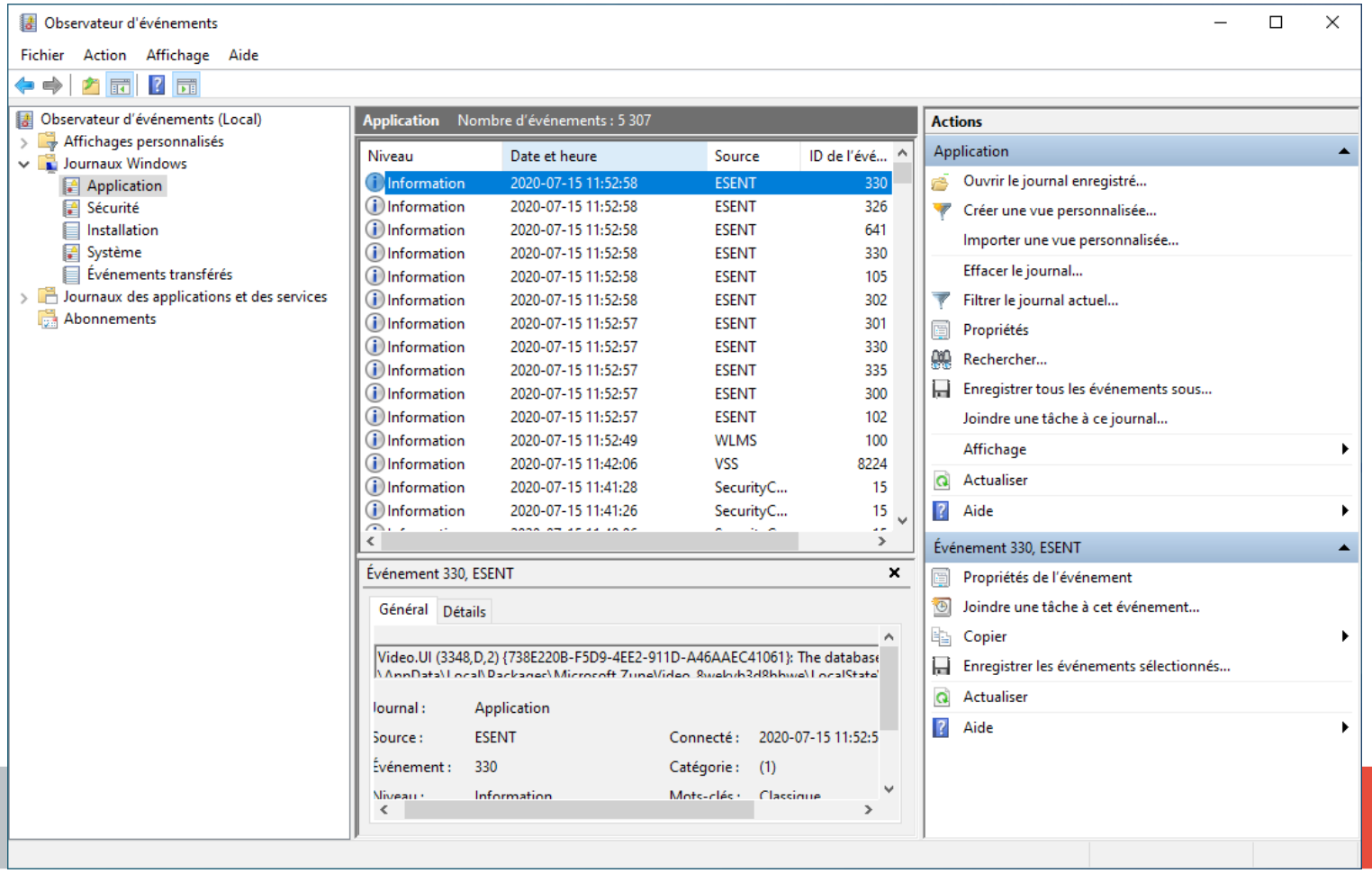
- **Les commandes Get-EventLog et Get-WinEvent permettent de récupérer des événements depuis les journaux (logs) de Windows**
- **Elles peuvent consulter les journaux...**
  - De l'ordinateur local
  - D'un ordinateur distant dont la configuration du pare-feu le permet

Différence ente les deux commandes

- **Get-EventLog permet seulement de consulter les journaux d'événements « classiques »**
- **Get-WinEvent permet aussi de consulter les journaux générés par la *Windows Event Log Technology* introduite avec Windows Vista**

Les événements

- **Les événements pouvant être récupérés apparaissent aussi dans l'Observateur d'événements de Windows**

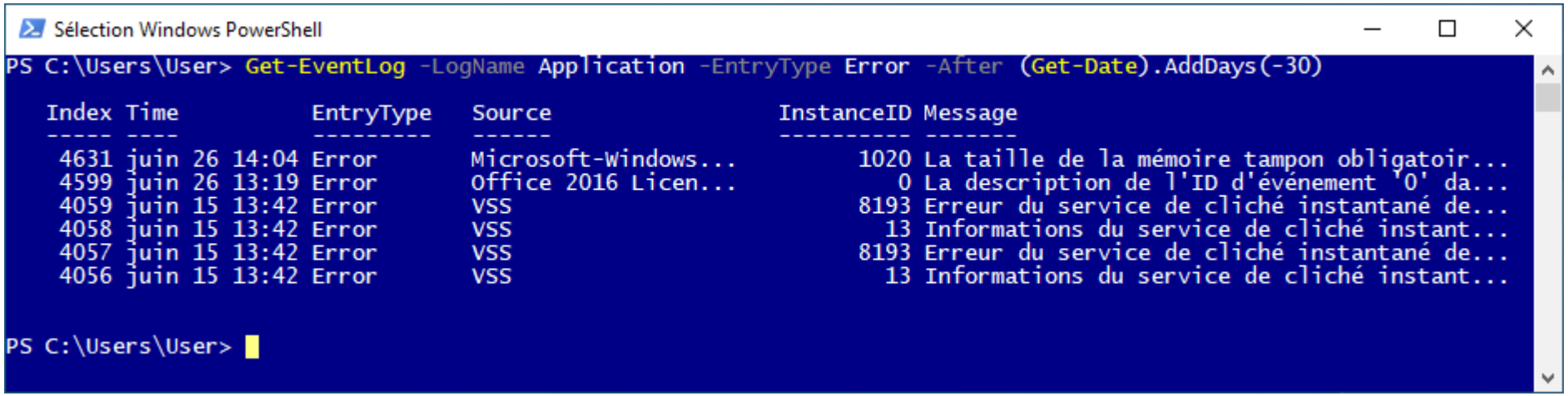


Récupérer des entrées d’un journal d’événements

Avec Get-EventLog

- **Récupérer les entrées de type Erreur du journal Application, créées dans les 30 derniers jours:**
  - **Get-EventLog** -LogName Application -EntryType Error -After (Get-Date).AddDays(-30)
- **Se référer à la documentation de la commande pour les autres paramètres possibles**

Avec Get-EventLog

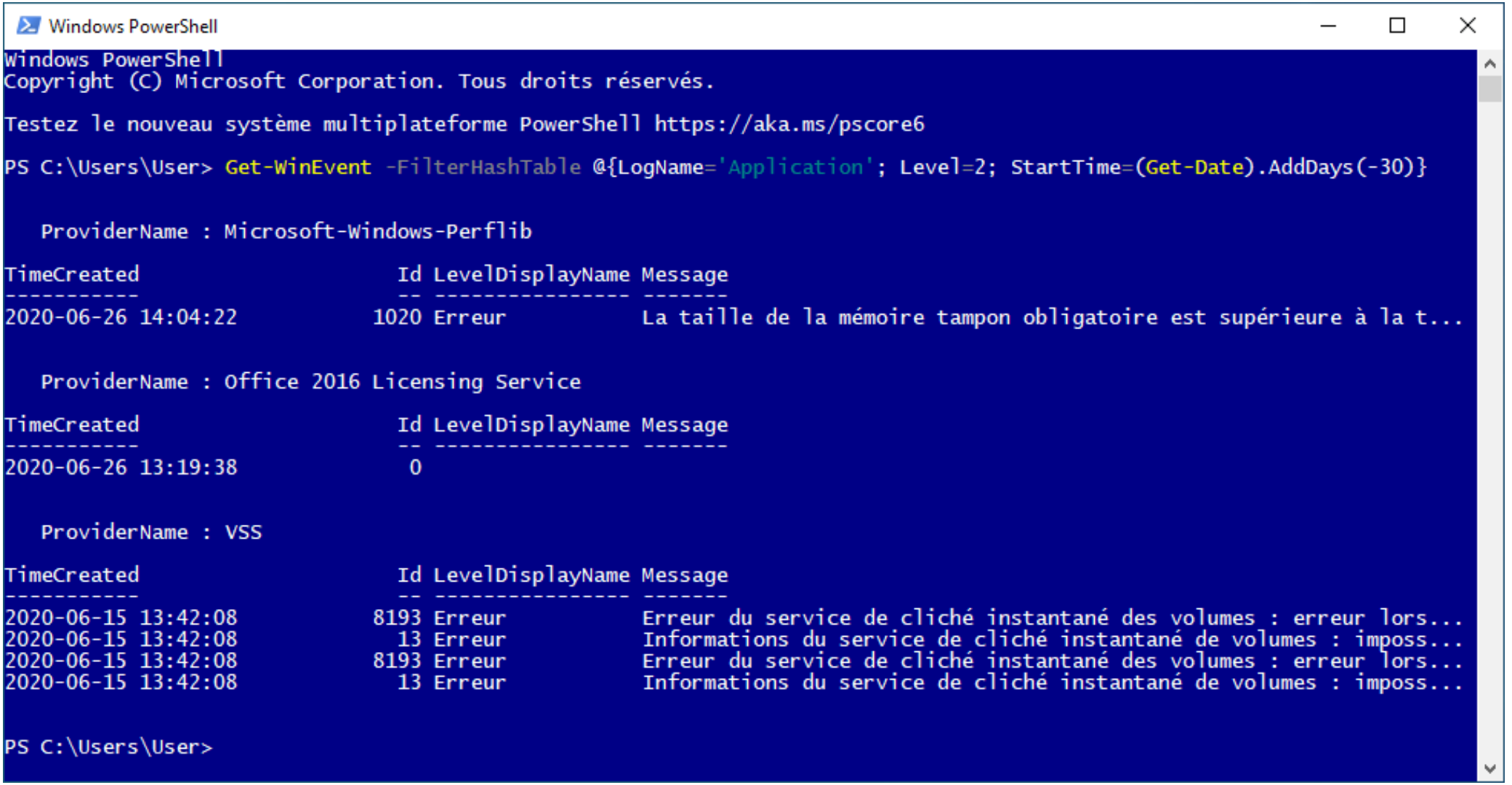


- **Le résultat est un tableau d'objets**
- **Comme d'habitude, Get-Member permet d'obtenir la liste des membres des objets pour savoir comment les utiliser**

Avec Get-WinEvent

- **Récupérer les entrées de type Erreur du journal Application, créées dans les 30 derniers jours:**
  - **Get-WinEvent** -FilterHashTable @{LogName='Application'; Level=2; StartTime=(Get-Date).AddDays(-30)}
- **Se référer à la documentation de la commande pour les autres paramètres possibles**

Avec Get-WinEvent



Ajouter une entrée à un journal d’événements

Ajouter une entrée à un journal d’événements

- **Créer une nouvelle source d’événements (en mode Administrateur)**
  - `New-EventLog -LogName Application -Source "Mon super script"`
- **Ajouter un événement**
  - `Write-EventLog -LogName Application -Source "Mon super script" -EntryType Information -EventId 1 -Message "Je m'amuse avec PowerShell"`

Fin de la présentation

Des questions?

Photo par Emily Morter sur Unsplash