

# 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

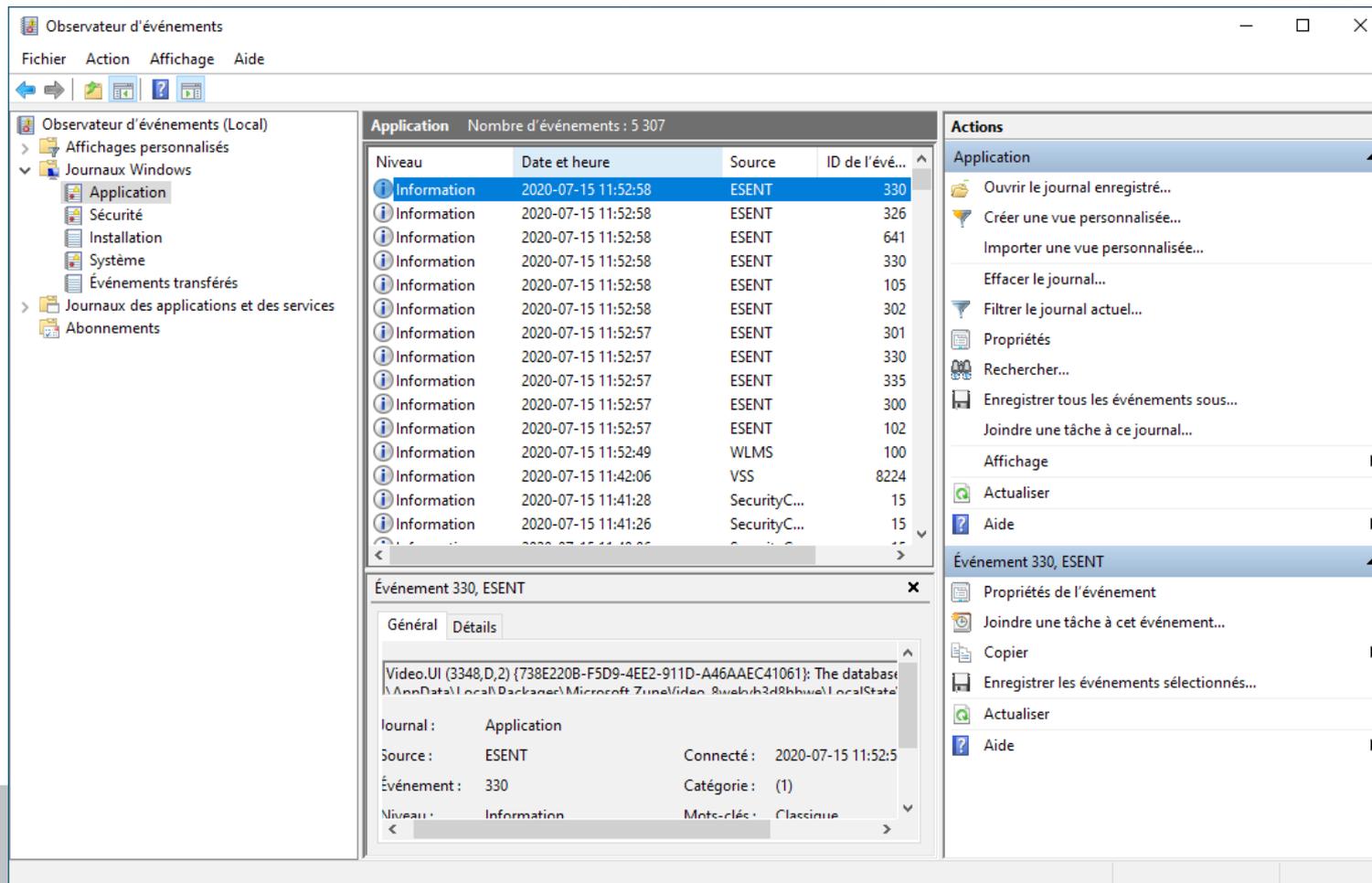
- Les commandes **Get-EventLog** et **Get-WinEvent** permettent de récupérer des événements depuis les journaux (logs) de Windows
- Elles peuvent consulter les journaux...
  - De l'ordinateur local
  - D'un ordinateur distant dont la configuration du pare-feu le permet

# Différence entre 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

```
Sélection Windows PowerShell
PS C:\Users\User> Get-EventLog -LogName Application -EntryType Error -After (Get-Date).AddDays(-30)

Index Time           EntryType Source                InstanceID Message
-----
4631 juin 26 14:04 Error Microsoft-Windows... 1020 La taille de la mémoire tampon obligatoir...
4599 juin 26 13:19 Error Office 2016 Licen... 0 La description de l'ID d'événement '0' da...
4059 juin 15 13:42 Error VSS 8193 Erreur du service de cliché instantané de...
4058 juin 15 13:42 Error VSS 13 Informations du service de cliché instant...
4057 juin 15 13:42 Error VSS 8193 Erreur du service de cliché instantané de...
4056 juin 15 13:42 Error VSS 13 Informations du service de cliché instant...

PS C:\Users\User> █
```

- 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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\User> Get-WinEvent -FilterHashTable @{LogName='Application'; Level=2; StartTime=(Get-Date).AddDays(-30)}

    ProviderName : Microsoft-Windows-Perflib

TimeCreated          Id LevelDisplayName Message
-----
2020-06-26 14:04:22  1020 Erreur          La taille de la mémoire tampon obligatoire est supérieure à la t...

    ProviderName : Office 2016 Licensing Service

TimeCreated          Id LevelDisplayName Message
-----
2020-06-26 13:19:38      0

    ProviderName : VSS

TimeCreated          Id LevelDisplayName Message
-----
2020-06-15 13:42:08  8193 Erreur          Erreur du service de cliché instantané des volumes : erreur lors...
2020-06-15 13:42:08    13 Erreur          Informations du service de cliché instantané de volumes : imposs...
2020-06-15 13:42:08  8193 Erreur          Erreur du service de cliché instantané des volumes : erreur lors...
2020-06-15 13:42:08    13 Erreur          Informations du service de cliché instantané de volumes : imposs...

PS C:\Users\User>
```

# 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