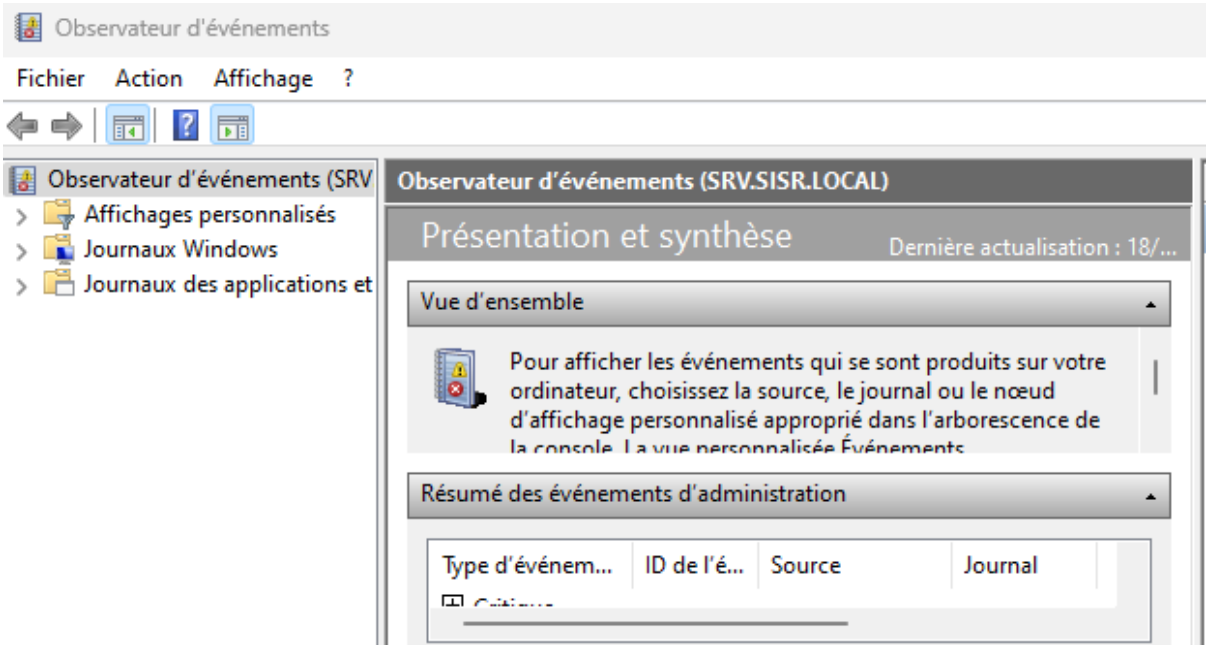
SERPETTE CLEMENT

Gestion des utilisateurs

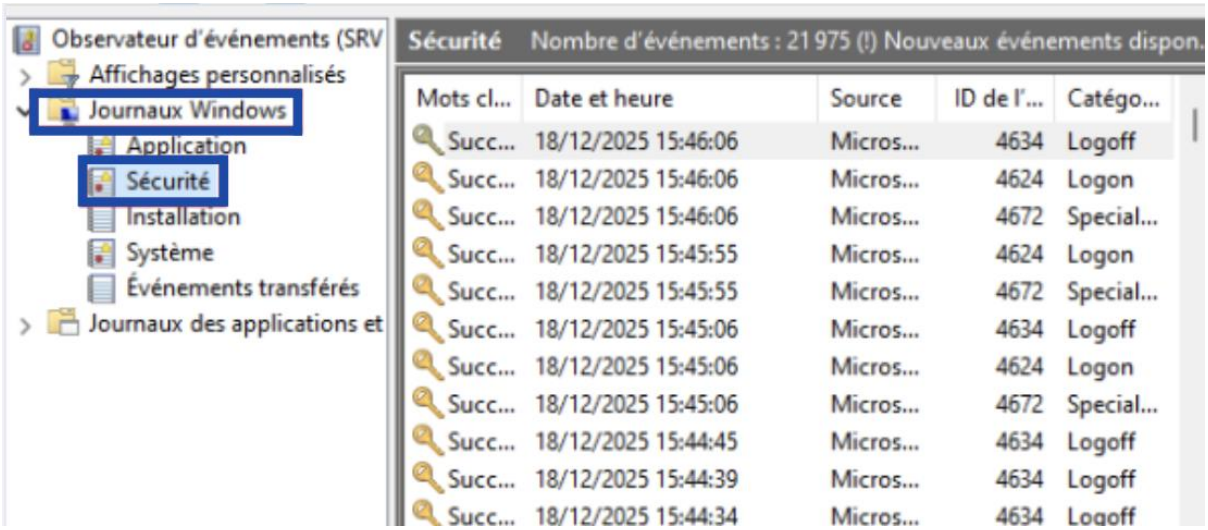
PARTIE 1 – Découverte des journaux d'événements avec l'Observateur d'événements

Étape 1 – Lancement de l'Observateur d'événements

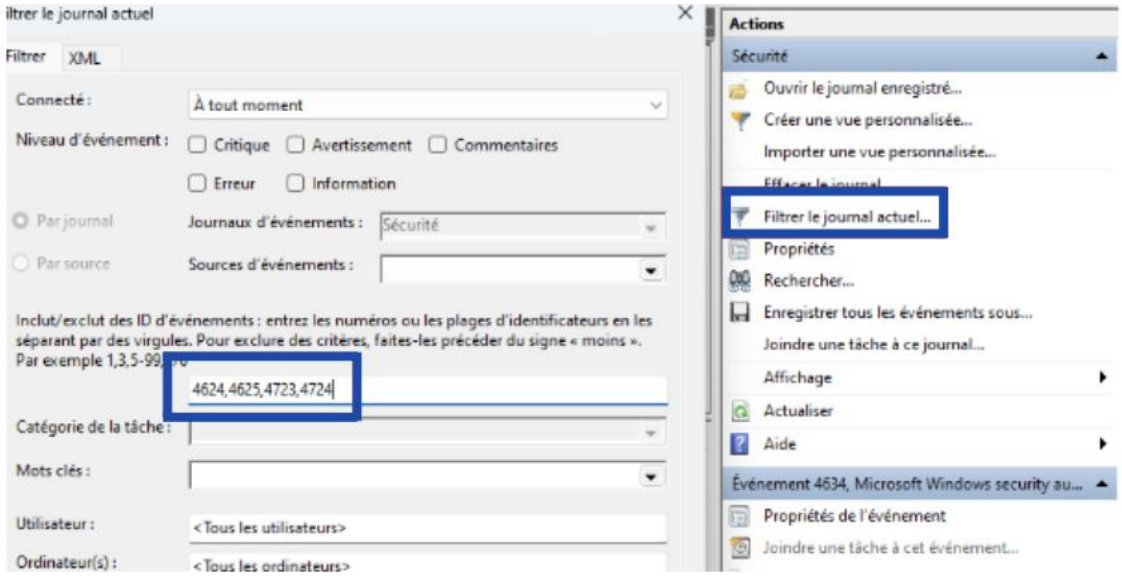
Appuyer sur **Win + R**, puis saisir la commande **eventvwr.msc**.



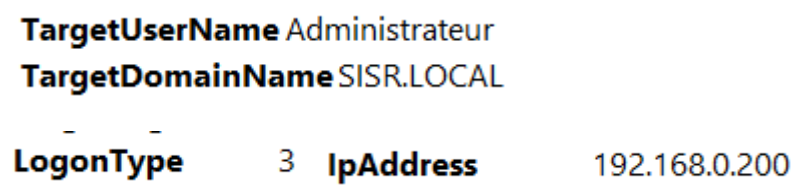
Étape 2 – Localiser le journal Sécurité



Étape 3 – Filtrer les évènements



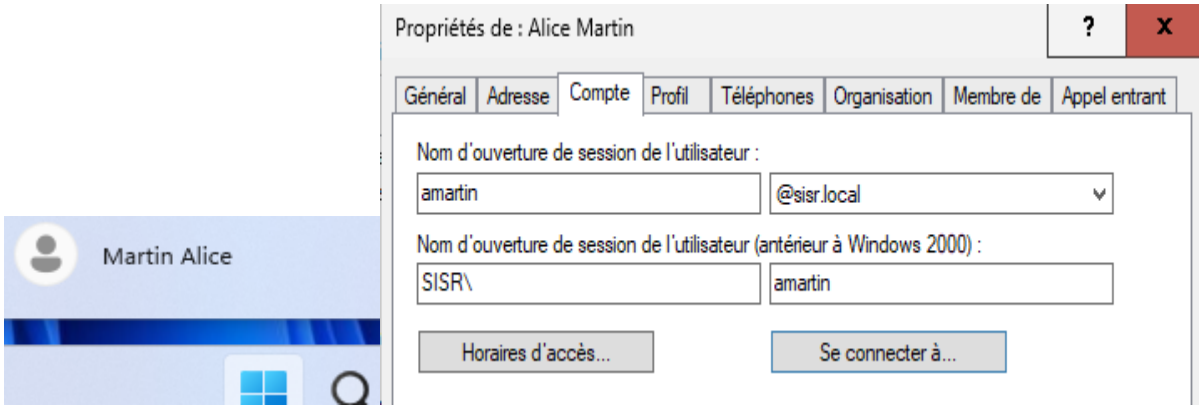
Étape 4 – Ouvrir un évènement 4624 (connexion réussie)



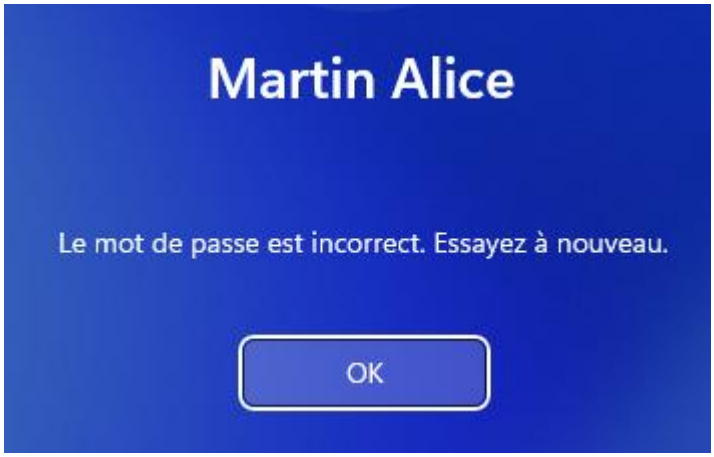
Étape 5 – Ouvrir un évènement 4625 (connexion échouée)

PARTIE 2 – Réaliser des tests de connexion

1. Connexion réussie



2. Connexion échouée

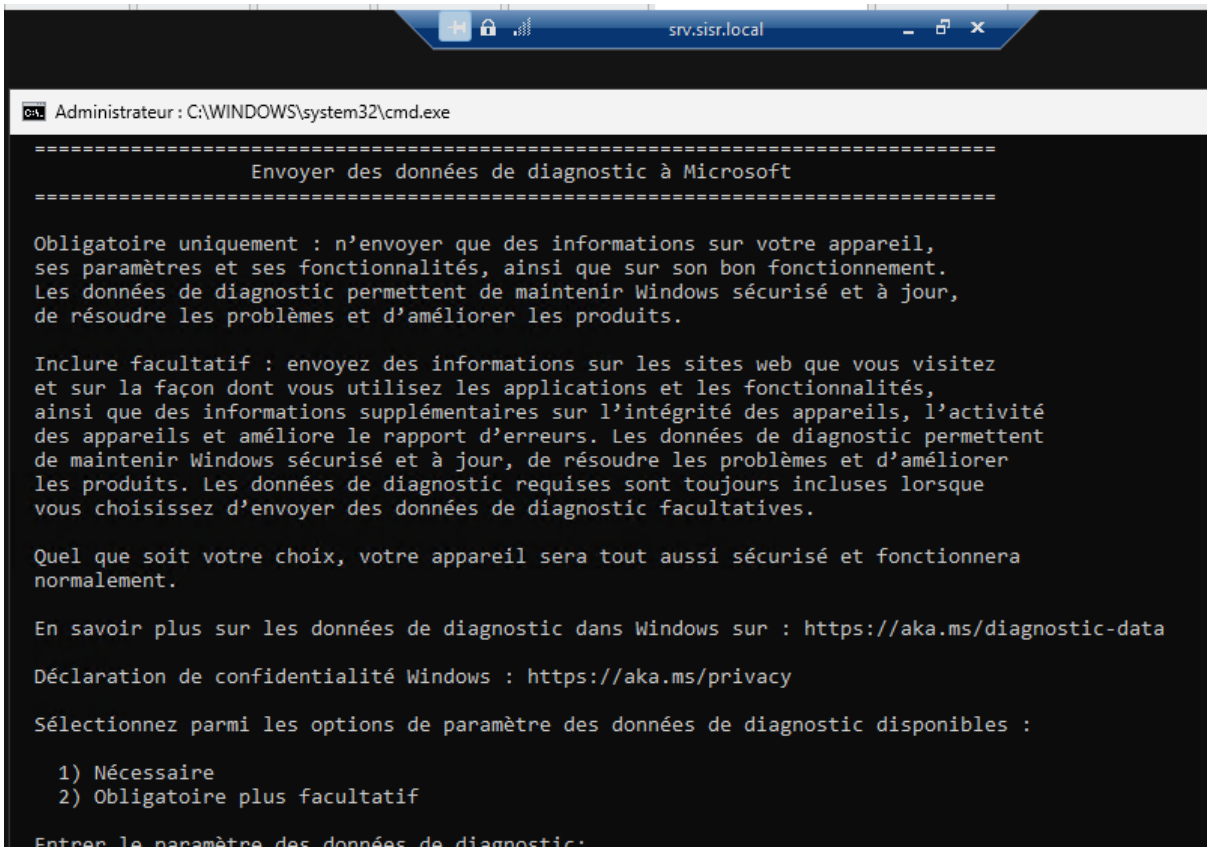


PARTIE 2 – Réaliser des tests de connexion

L'utilisateur Alice Martin est ajouté au groupe « Administrateurs du domaine ».

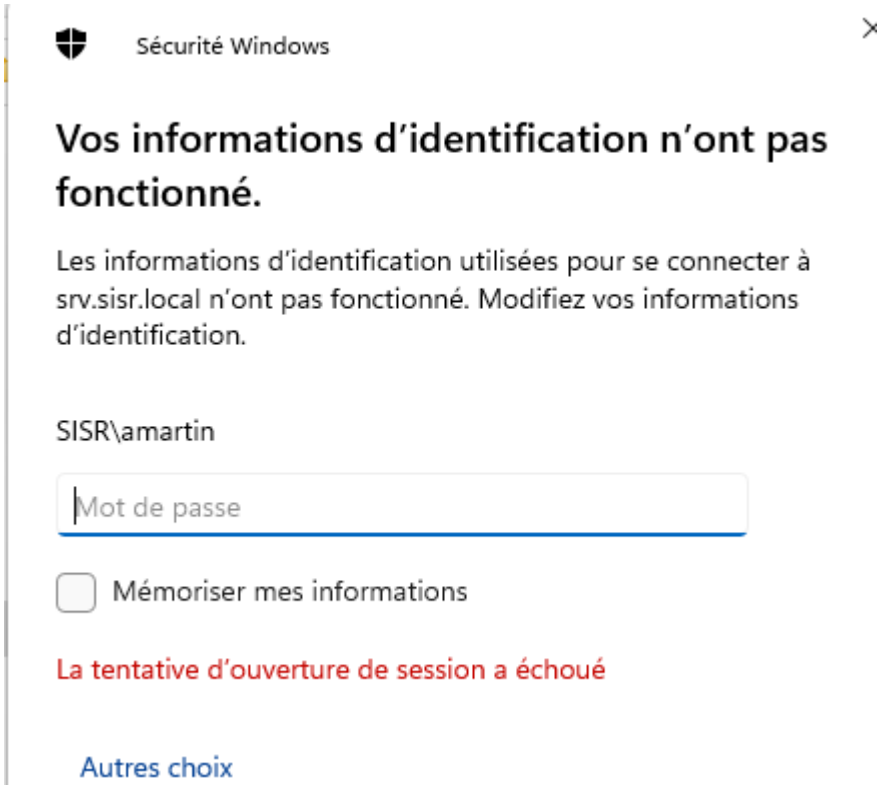
```
PS C:\Users\Administrateur.SISR> Add-ADGroupMember -Identity "Admins du domaine" -Members "amartin"
PS C:\Users\Administrateur.SISR>
```

Connexion au bureau à distance afin d'accéder à l'Active Directory.



4. Tentative de changement de mot de passe (4723)

La même opération est réalisée en utilisant volontairement un mot de passe incorrect.



5. Tentative de réinitialisation de mot de passe (4724)

```
PS C:\Users\Administrateur> Set-ADAccountPassword cpetit -Reset -NewPassword (ConvertTo-SecureString "Test1234!" -AsP
lainText -Force)
```

PARTIE 3 – Analyse avec PowerShell

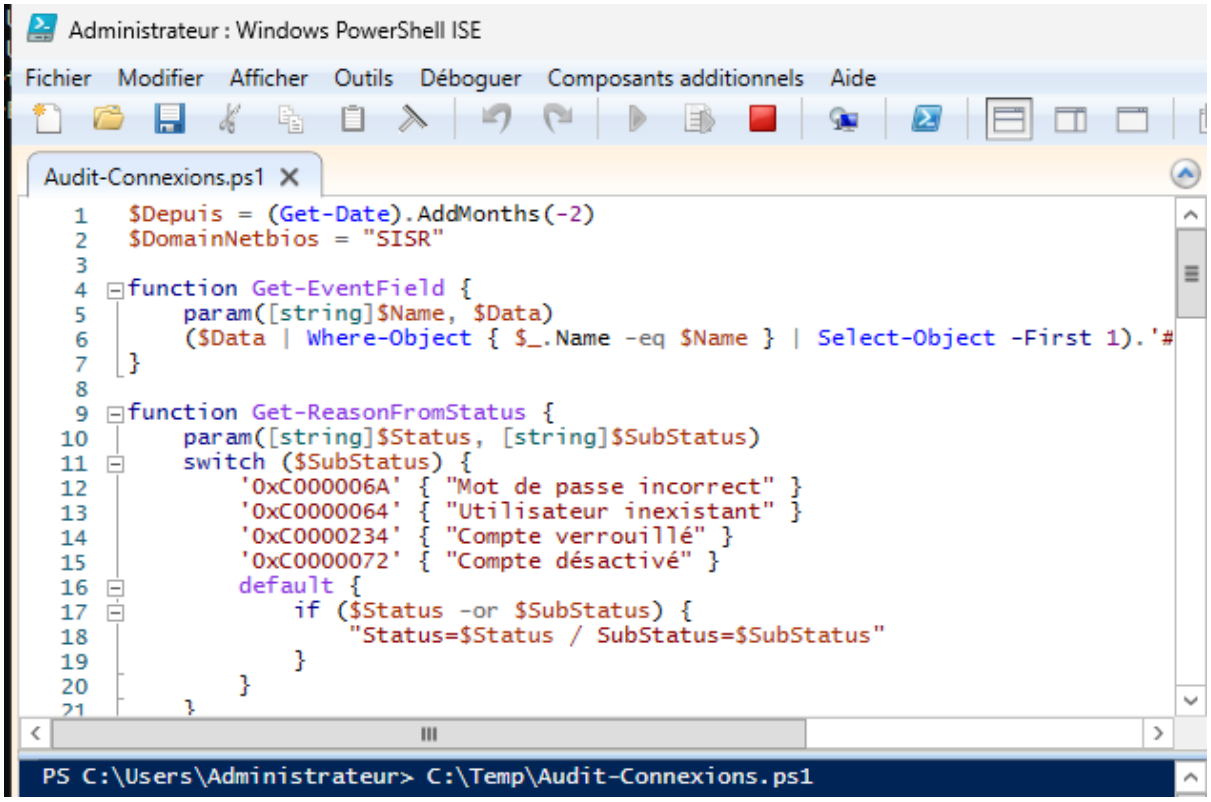
Étape 1 – Lister les 20 derniers évènements du journal Sécurité

```
PS C:\Users\Administrateur> Get-WinEvent -LogName Security -MaxEvents 20 |
>> Select-Object TimeCreated, Id, Message |
>> Format-Table -Wrap

TimeCreated           Id Message
-----------           -- -------
18/12/2025 16:16:06 4634 Fermeture de session d'un compte.

18/12/2025 16:18:06 4624 L'ouverture de session d'un compte s'est correctement déroulée.

18/12/2025 16:14:29 4672 Privilèges spéciaux attribués à la nouvelle ouverture de session.

04/12/2025 14:57:46 4625 Échec d'ouverture de session d'un compte.
```

Étape 2 – Filtrer les évènements du domaine SISR (méthode simple)

Get-WinEvent -LogName Security |
Where-Object { $_.Id -in 4624,4625,4723,4724 } |
Select-Object TimeCreated, Id, Message |
Format-Table -Wrap

PARTIE 4 – Exécution du Script d'Audit



PARTIE 5 – Interprétation et questions guidées

```
06/11/2025 16:56:33    4624 Administrateur SRV2    192.168.0.52  3         N...
06/11/2025 17:02:16    4625 Administrateur SRV     127.0.0.1     7         T...
06/11/2025 17:03:08    4624 Administrateur SRV     127.0.0.1     7         T...
06/11/2025 17:12:36    4624 Administrateur SRV     127.0.0.1     2         I...
06/11/2025 17:22:38    4624 Administrateur SRV2    192.168.0.52  3         N...
06/11/2025 17:22:38    4624 Administrateur SRV2    192.168.0.52  3         N...
06/11/2025 17:22:38    4624 Administrateur SRV2    192.168.0.52  3         N...
06/11/2025 17:22:38    4624 Administrateur SRV2    192.168.0.52  3         N...
20/11/2025 13:33:56    4624 Administrateur SRV     127.0.0.1     2         I...
20/11/2025 13:47:25    4624 Administrateur SRV2    192.168.0.52  3         N...
20/11/2025 13:53:27    4624 Administrateur SRV     127.0.0.1     7         T...
20/11/2025 14:36:47    4624 Administrateur SRV3    192.168.0.53  3         N...
20/11/2025 14:36:47    4624 Administrateur SRV3    192.168.0.53  3         N...
20/11/2025 14:37:03    4624 Administrateur SRV     127.0.0.1     7         T...
20/11/2025 14:54:16    4624 Administrateur SRV3    192.168.0.53  3         N...
20/11/2025 14:54:16    4624 Administrateur SRV3    192.168.0.53  3         N...
20/11/2025 14:54:08    4624 Administrateur SRV3    192.168.0.53  3         N...
20/11/2025 14:54:36    4624 Administrateur SRV3    192.168.0.53  3         N...
20/11/2025 14:55:38    4624 Administrateur SRV     127.0.0.1     7         T...
```

Trouver toutes les connexions RDP:

```
18/12/2025 16:24:18    4624 amartin        SRV     192.168.0.200 10        R...
```

Connexion au compte de amartin à 16:24:18

Trouver les connexions échouées (4625):

```
18/12/2025 16:12:15    4625 Administrateur SRV     127.0.0.1     2         I...
```

Trouver les réinitialisations (4724):

Mot de passe réinitialisé de cpetit

```
04/12/2025 14:25:25    4724 cpetit                                    T...
```

Trouver toutes les IP ayant tenté une connexion :

```
192.168.0.52  3
192.168.0.52  3
127.0.0.1     7
127.0.0.1     7
127.0.0.1     2
192.168.0.52  3
192.168.0.52  3
192.168.0.52  3
192.168.0.52  3
127.0.0.1     2
192.168.0.52  3
127.0.0.1     7
192.168.0.53  3
192.168.0.53  3
127.0.0.1     7
192.168.0.53  3
192.168.0.53  3
192.168.0.53  3
192.168.0.53  3
```

```
Administrateur SRV     127.0.0.1
Administrateur SRV
Administrateur SRV     127.0.0.1
Administrateur SRV
Administrateur SRV     127.0.0.1
Administrateur SRV
amartin
Administrateur SRV     192.168.0.200
Administrateur SRV     192.168.0.200
Administrateur SRV     127.0.0.1
Administrateur SRV     127.0.0.1
cpetit
amartin        SRV     192.168.0.200
Administrateur SRV     127.0.0.1
```

Dans un premier temps, l'Observateur d'événements a été utilisé afin de filtrer les journaux de sécurité correspondant aux identifiants 4624, 4625, 4723 et 4724. Ensuite, des événements ont été volontairement générés en ajoutant un utilisateur au groupe des Administrateurs du domaine et en réalisant des tentatives de connexion, réussies comme échouées. Enfin, l'analyse a été automatisée à l'aide de PowerShell, grâce au script *Audit-Connexions.ps1*, permettant d'extraire les adresses IP ainsi que les causes précises des échecs (mot de passe incorrect, compte verrouillé, etc.).