

**Laboratoire 10 : Processus, services et Journalisation Windows**

# CORRIGÉ

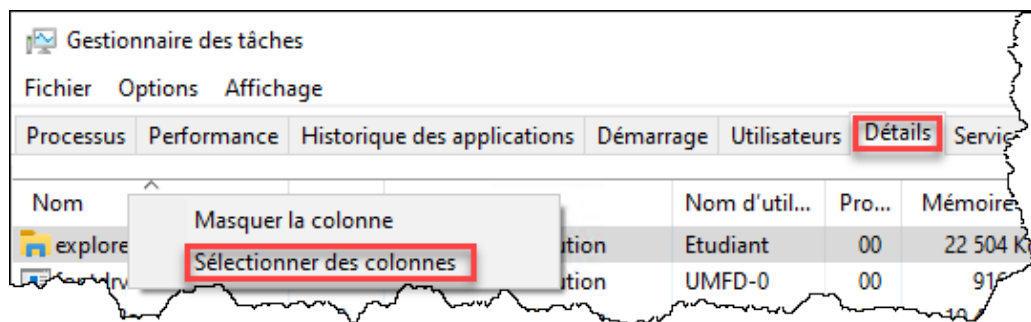
**Partie 1 : Processus**

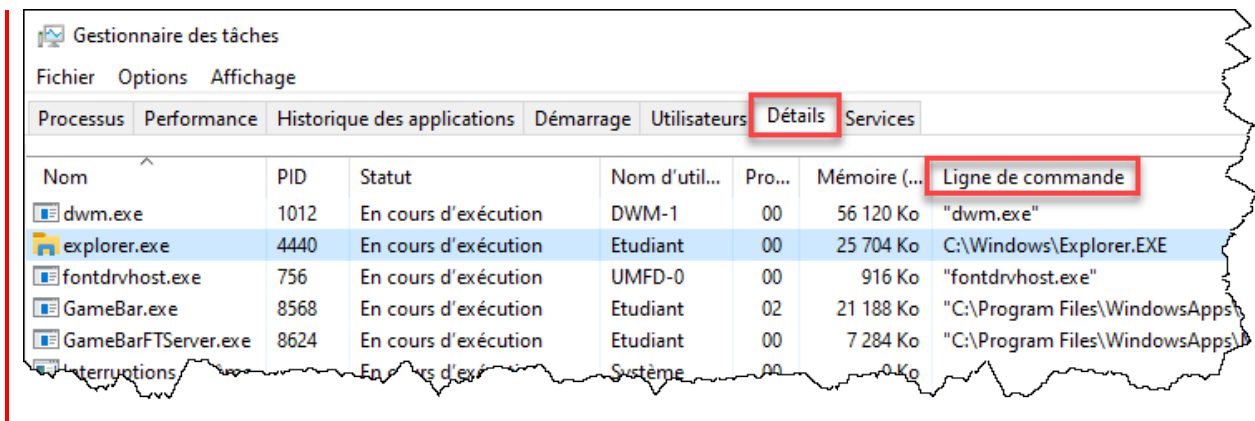
Les manipulations de cette section doivent être effectuées dans votre machine virtuelle Windows 10, à moins d'indications contraires.

Les processus représentent les programmes en cours d'exécution. Chaque fois qu'on exécute un programme (un fichier exécutable), un processus est créé, et un numéro lui est attribué. Le système d'exploitation alloue à ce processus des ressources système, telles que du temps de processeur et de la mémoire réservée, et s'assure de faire en sorte que les autres processus ne puissent pas empiéter les uns sur les autres. Lorsqu'on ferme l'application, le processus est automatiquement détruit.

- Q1 Sur votre machine virtuelle Windows 10, démarrez le gestionnaire des tâches et localisez le processus **explorer.exe**.
- a) Quel est le chemin complet vers le fichier de programme **explorer.exe**? Trouvez l'information dans le gestionnaire de tâches.

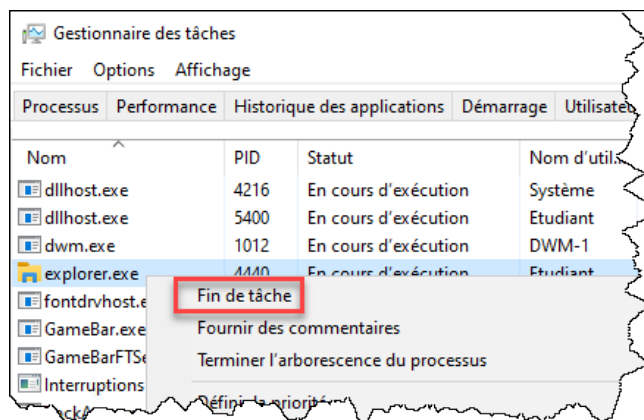
C:\Windows\Explorer.EXE



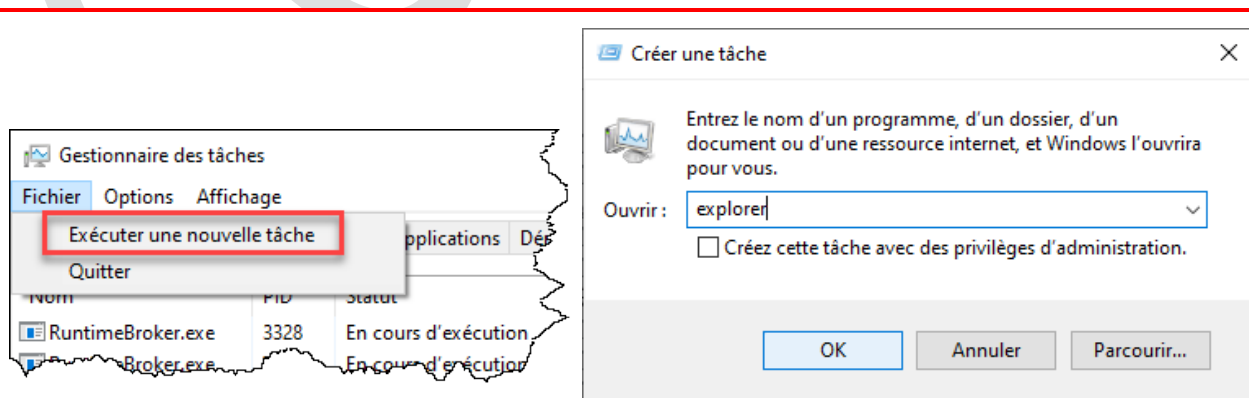


- b) Mettez fin au processus **explorer.exe** (ou à tous les processus **explorer.exe**, s'il y en a plus d'un).  
Que constatez-vous?

Le bureau devient vide; les icônes, le menu Démarrer et la barre de tâches disparaissent.



- c) Essayez de repartir **explorer.exe** à l'aide du gestionnaire de tâches. Comment vous y êtes-vous pris?



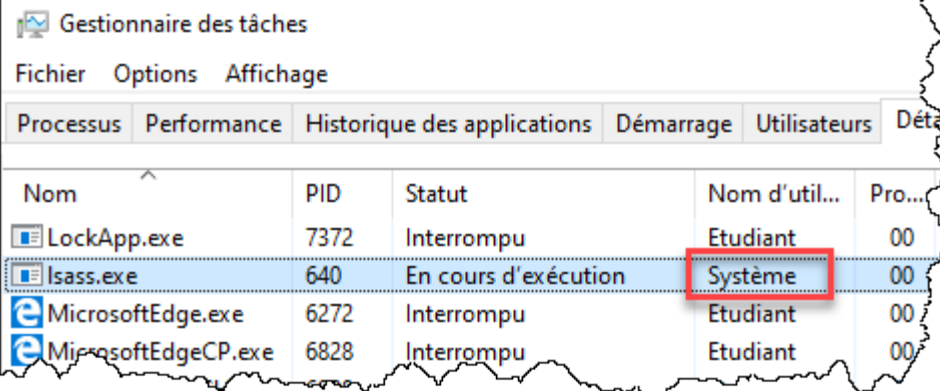
Q2 Toujours sur votre machine virtuelle Windows 10, dans le gestionnaire de tâches, localisez le processus **lsass.exe**

a) Selon vous, quel est le rôle de ce processus? (Vous pouvez vous aider de Google)

C'est le processus responsable de l'identification des utilisateurs et de la validation de leur mot de passe. Si ce processus n'existait pas, il serait impossible de démarrer une session sous Windows car le système serait incapable de valider leur identité. Il s'agit d'un processus système très important, essentiel au bon fonctionnement de Windows.

b) Ce processus appartient à quel utilisateur?

Le compte système.



Gestionnaire des tâches					
Fichier Options Affichage					
Processus Performance Historique des applications Démarrage Utilisateurs Détails					
Nom	PID	Statut	Nom d'util...	Pro...	
LockApp.exe	7372	Interrompu	Etudiant	00	
lsass.exe	640	En cours d'exécution	Système	00	
MicrosoftEdge.exe	6272	Interrompu	Etudiant	00	
MicrosoftEdgeCP.exe	6828	Interrompu	Etudiant	00	

c) Mettez fin à ce processus. Que se passe-t-il?

Windows n'aime vraiment pas ça. Il redémarre automatiquement après une minute, en avertissant l'utilisateur à l'écran.

Q3 Sur votre VM Windows 10, démarrez l'outil bloc-notes (notepad.exe). Puis, démarrez une ligne de commandes.

- a) Dans la ligne de commandes, obtenez la liste des processus en cours et localisez le bloc-notes. Quel est son numéro d'identification (PID)?

2220 dans mon cas. Il est différent à chaque fois, voici comment le trouver :

```
C:\Windows\system32\cmd.exe

C:\Users\Etudiant>tasklist

Nom de l'image          PID Nom de la sessio Numéro de s Utilisation
=====
System Idle Process      0 Services          0      8 Ko
System                   4 Services          0     144 Ko
Registry                 88 Services          0    19 264 Ko
smss.exe                 328 Services          0      1 188 Ko
csrss.exe                 420 Services          0      5 200 Ko
wininit.exe              500 Services          0      6 936 Ko
csrss.exe                 516 Console          1      5 012 Ko

SearchUI.exe             5592 Console          1    142 976 Ko
MicrosoftEdgeCP.exe      6416 Console          1      26 612 Ko
smartscreen.exe           6284 Console          1     22 256 Ko
notepad.exe               2220 Console          1     15 488 Ko
cmd.exe                   3240 Console          1      4 008 Ko
conhost.exe               1388 Console          1     18 988 Ko
tasklist.exe              3580 Console          1      8 604 Ko

C:\Users\Etudiant>
```

Ou encore avec un filtre pour simplifier la recherche :

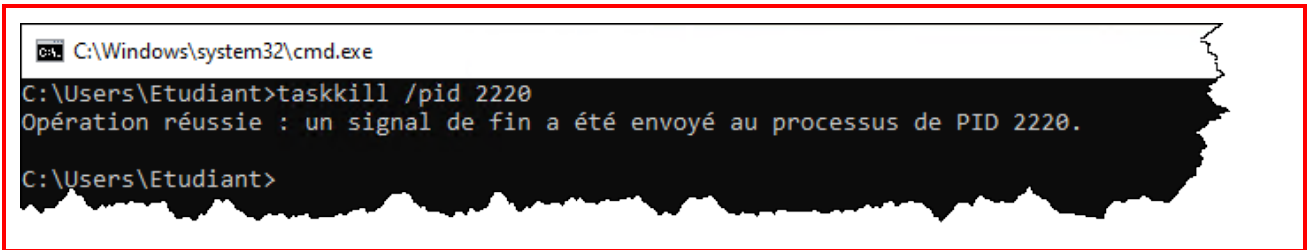
```
C:\Windows\system32\cmd.exe

C:\Users\Etudiant>tasklist /fi "IMAGENAME eq notepad.exe"

Nom de l'image          PID Nom de la sessio Numéro de s Utilisation
=====
notepad.exe             2220 Console          1     15 524 Ko

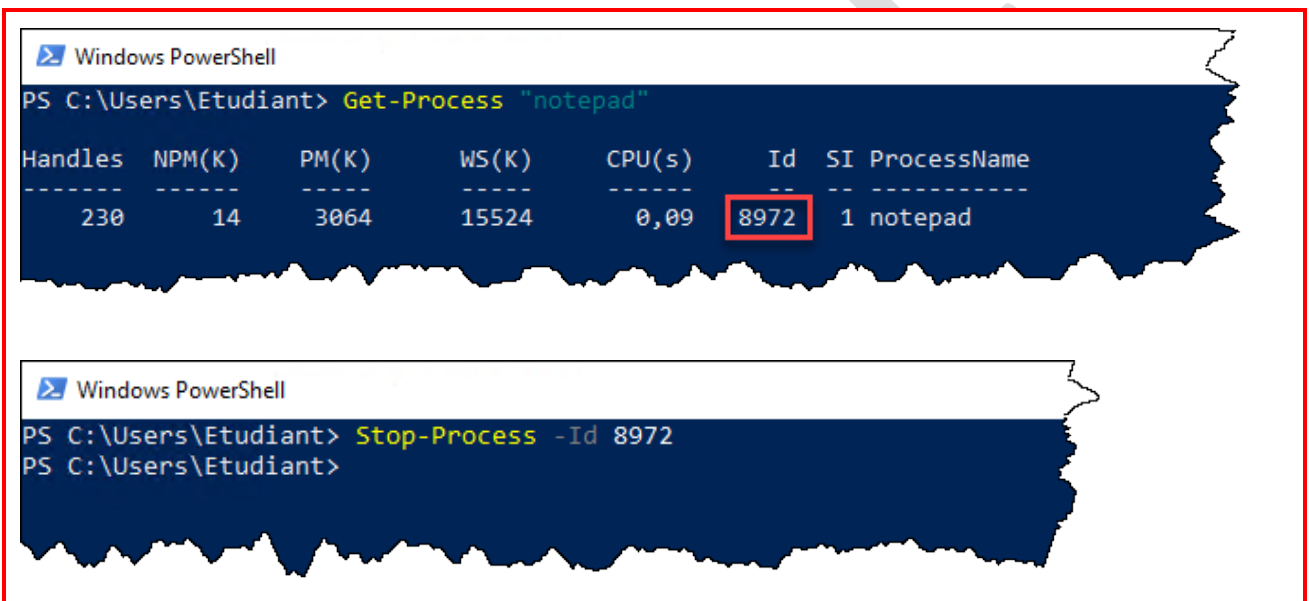
C:\Users\Etudiant>_
```

b) Mettez fin à ce processus. Insérez une capture d'écran.



```
C:\Windows\system32\cmd.exe
C:\Users\Etudiant>taskkill /pid 2220
Opération réussie : un signal de fin a été envoyé au processus de PID 2220.
C:\Users\Etudiant>
```

c) Faites la même chose en PowerShell. Insérez des captures d'écran.



```
Windows PowerShell
PS C:\Users\Etudiant> Get-Process "notepad"

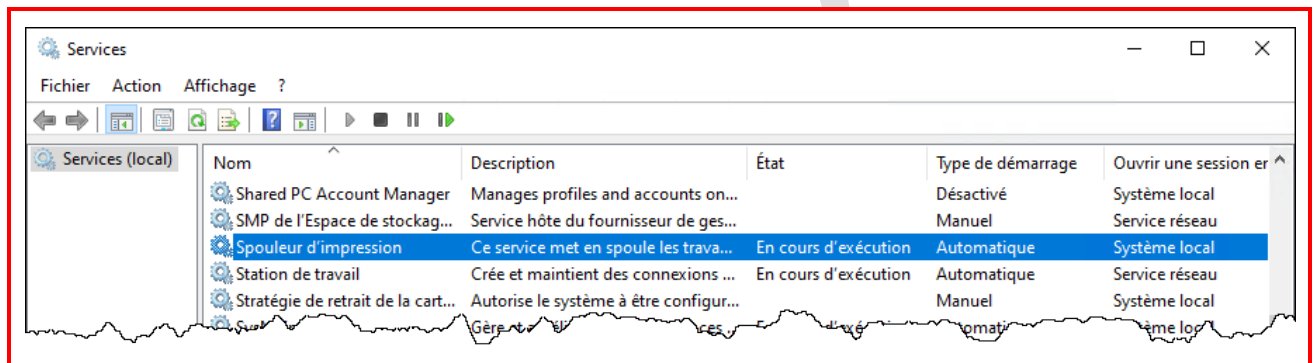
Handles  NPM(K)  PM(K)  WS(K)  CPU(s)  Id  SI ProcessName
-----  -
230      14      3064   15524   0,09    8972  1 notepad

Windows PowerShell
PS C:\Users\Etudiant> Stop-Process -Id 8972
PS C:\Users\Etudiant>
```

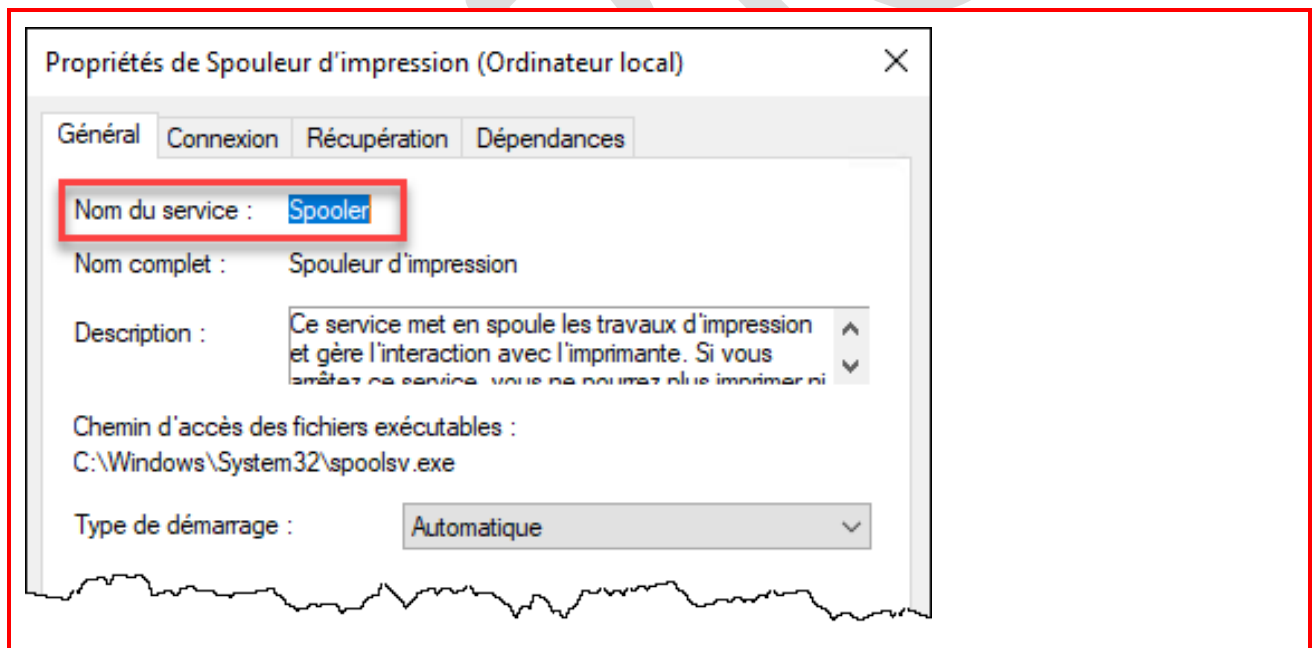
## Partie 2 : Services

Q4 Localisez le service qui se nomme « Spouleur d'impression » dans la console des services (services.msc).

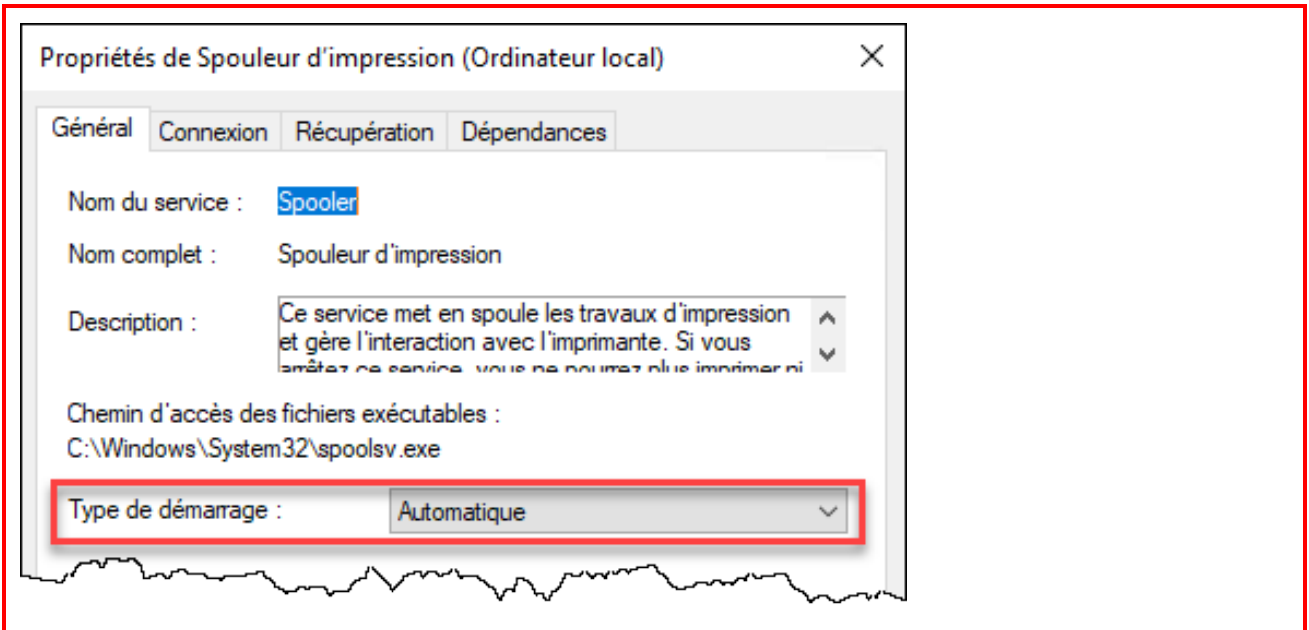
a) Insérez une capture d'écran.



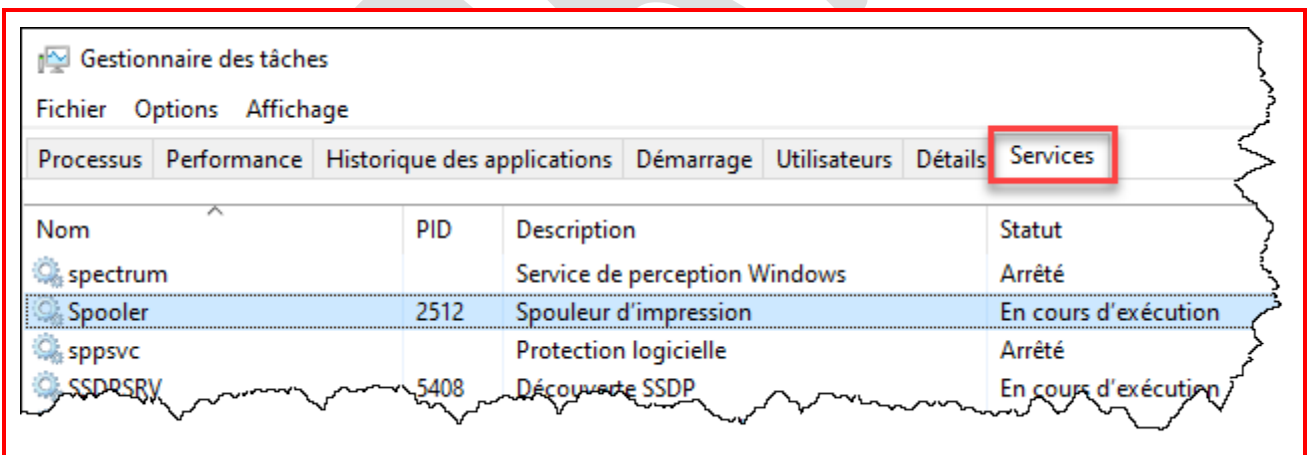
b) Quel est le véritable nom de ce service? Vous pouvez le trouver dans les propriétés de ce service.



c) Quel est le mode de démarrage de ce service?

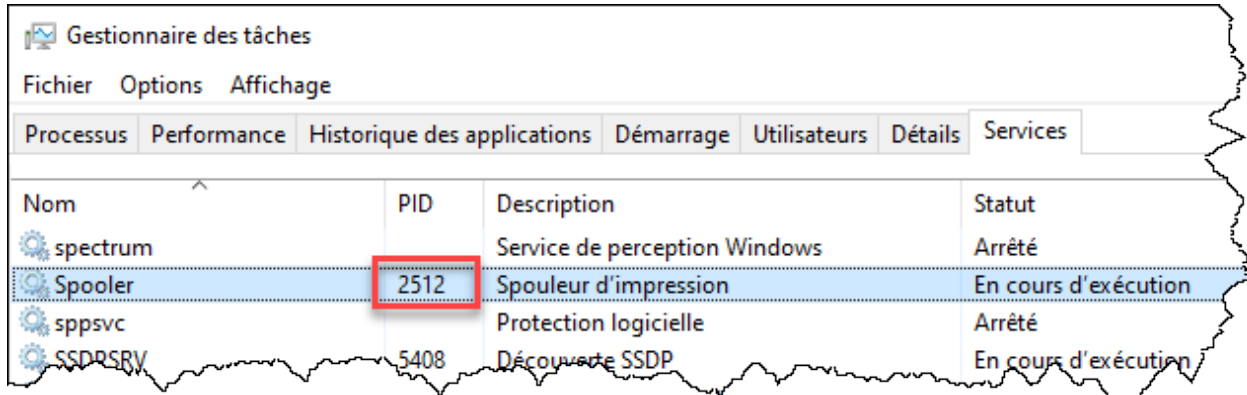


d) Dans l'onglet Services du gestionnaire de tâches, trouvez ce service. Insérez une capture d'écran.



e) Ce service opère via quel processus? Trouvez le PID de ce processus.

Le PID change à chaque fois.



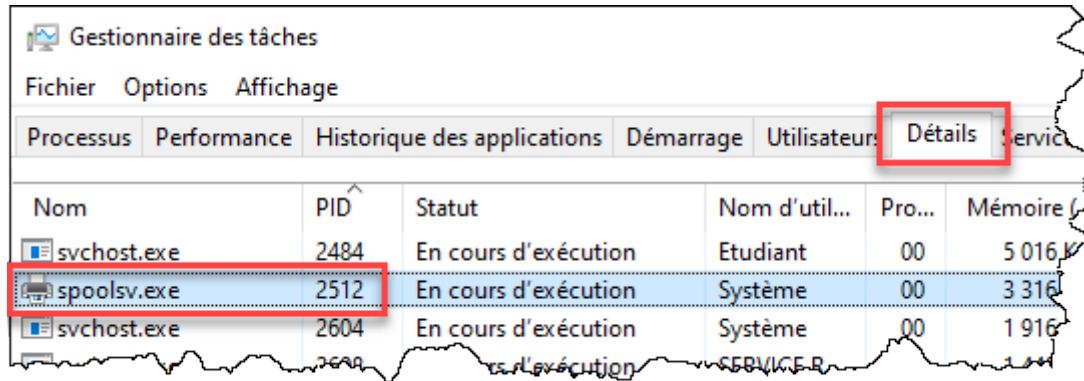
Gestionnaire des tâches

Fichier Options Affichage

Processus Performance Historique des applications Démarrage Utilisateurs Détails Services

Nom	PID	Description	Statut
spectrum		Service de perception Windows	Arrêté
Spooler	2512	Spouleur d'impression	En cours d'exécution
sppsvc		Protection logicielle	Arrêté
SSDP.SRV	5408	Découverte SSDP	En cours d'exécution

Et comme de fait, il y a un processus associé à ce service.



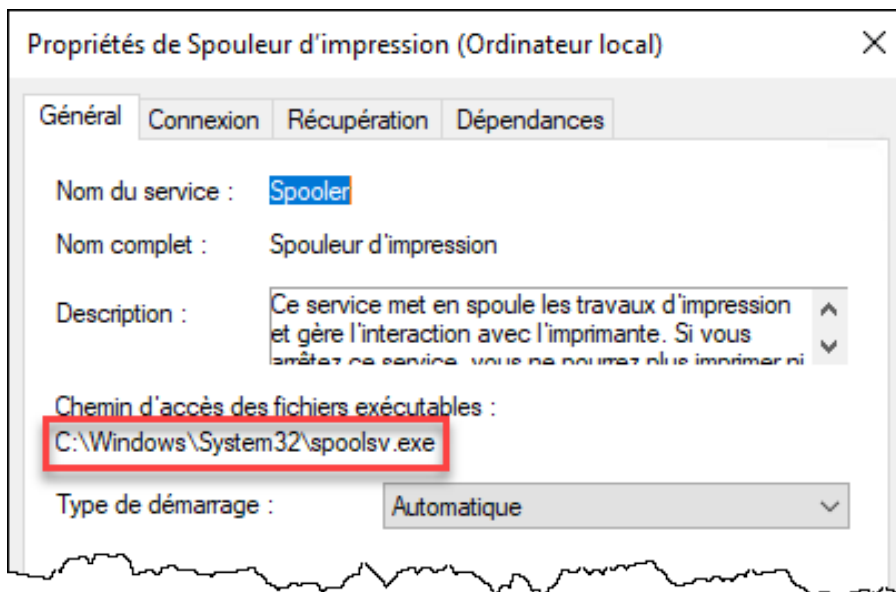
Gestionnaire des tâches

Fichier Options Affichage

Processus Performance Historique des applications Démarrage Utilisateurs Détails Services

Nom	PID	Statut	Nom d'util...	Pro...	Mémoire (K)
svchost.exe	2484	En cours d'exécution	Etudiant	00	5 016 K
spoolsv.exe	2512	En cours d'exécution	Système	00	3 316 K
svchost.exe	2604	En cours d'exécution	Système	00	1 916 K

C'est exactement cet exécutable, spoolsv.exe, qui est configuré dans le service.



Propriétés de Spouleur d'impression (Ordinateur local)

Général Connexion Récupération Dépendances

Nom du service : Spooler

Nom complet : Spouleur d'impression

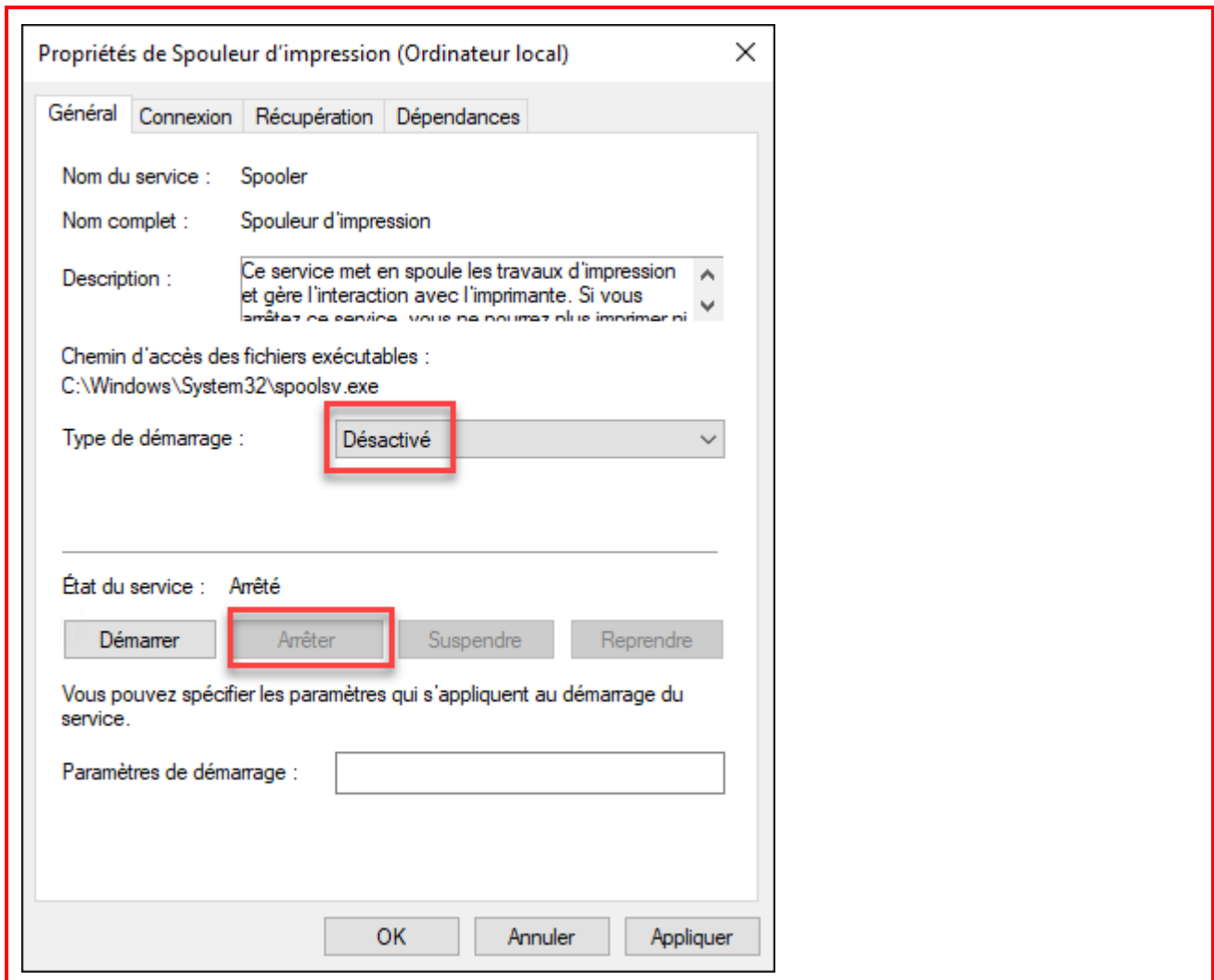
Description : Ce service met en spoule les travaux d'impression et gère l'interaction avec l'imprimante. Si vous arrêtez ce service, vous ne pourrez plus imprimer ni...

Chemin d'accès des fichiers exécutables : C:\Windows\System32\spoolsv.exe

Type de démarrage : Automatique



- f) Arrêtez le service et faites en sorte qu'il ne puisse plus démarrer. Comment vous y êtes-vous pris?



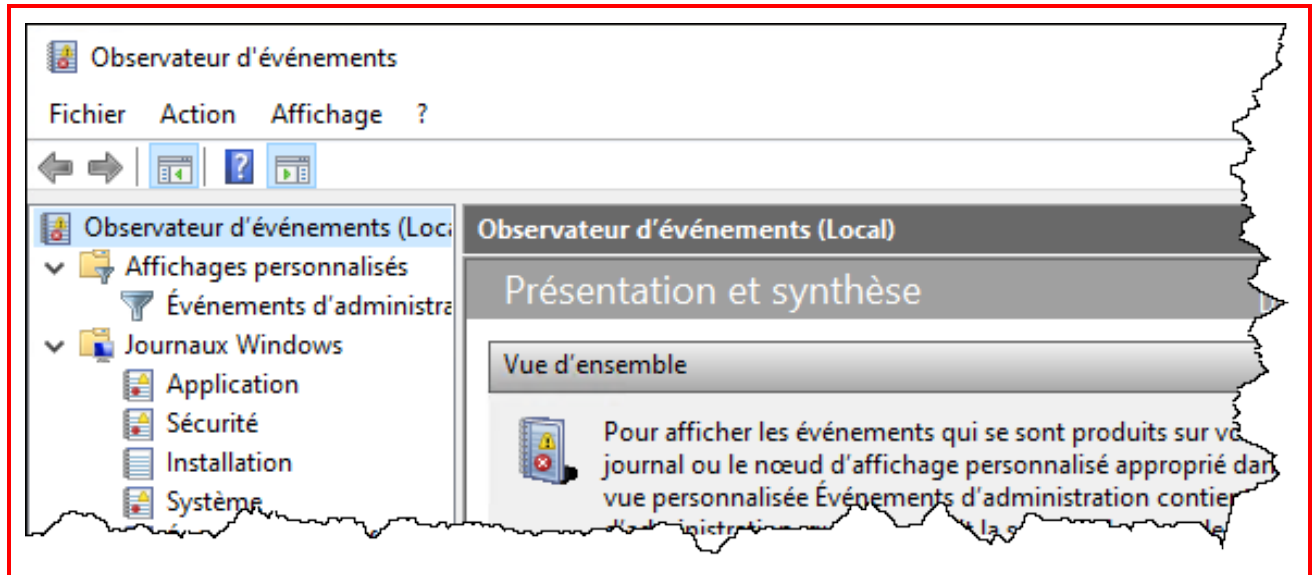
### Partie 3 : Journal d'événements

Les manipulations de cette section doivent être effectuées dans votre machine virtuelle Windows 10, à moins d'indications contraires.

- Q5 Dans quelles situations pourriez-vous avoir besoin d'utiliser l'observateur d'événements?

Une erreur s'est produite et on veut comprendre ce qui s'est passé;  
On veut savoir qui a tenté de se connecter au système dernièrement

Q6 Accédez à l'observateur d'événements. Faites une capture d'écran de l'observateur ouvert.



Q7 Comment pouvez-vous accéder à l'observateur d'événements par la ligne de commandes? Indiquez quelle commande utiliser.

Eventvwr (ou eventvwr.exe)

```
C:\Windows\system32\cmd.exe
C:\Users\Etudiant>eventvwr
C:\Users\Etudiant>
```

Q8 Expliquez (dans vos propres mots) ce que contiennent les différents journaux Windows de l'observateur d'événements.

a) Application

Ce journal contient des événements et des erreurs survenues dans les applications et les composants de Windows.

b) Sécurité

Ce journal contient des événements concernant la sécurité, tels que les démarrages de session et les tentatives d'accès au système.

c) Système

Ce journal contient les événements relatifs au noyau de Windows, tels que le démarrage et la mise sous tension du système d'exploitation, les erreurs globales du système (écrans bleus), etc.

Q9 Trouvez un exemple d'événement pour chaque niveau de sévérité

a) Information

The screenshot displays the Windows Event Viewer interface. At the top, a header bar indicates 'Application' and 'Nombre d'événements : 4 081'. Below this is a table of events. The second row is selected, showing an 'Information' level event from 'VMTools' with ID '105' and category 'Aucun'. The event description is 'The service was started.' Below the table, the 'Événement 105, VMTools' window is open, showing the 'Général' tab. This tab displays the event details: Journal: Application, Source: VMTools, Connecté: 2020-11-13 13:26:57, Événement: 105, Catégorie: Aucun, Niveau: Information, Mots-clés: Classique, Utilisateur: N/A, Ordinateur: DESKTOP-6GGOFCD, Opcode: , and Informations: [Aide sur le Journal](#).

Niveau	Date et heure	Source	ID de l'événement	Catégorie de ...
Information	2020-11-13 13:26:58	Security-SPP	900	Aucun
Information	2020-11-13 13:26:57	VMTools	105	Aucun
Information	2020-11-13 13:26:56	WMI	5617	Aucun
Information	2020-11-13 13:26:56	WMI	5615	Aucun

Événement 105, VMTools

Général Détails

The service was started.

Journal : Application

Source : VMTools Connecté : 2020-11-13 13:26:57

Événement : 105 Catégorie : Aucun

Niveau : Information Mots-clés : Classique

Utilisateur : N/A Ordinateur : DESKTOP-6GGOFCD

Opcode :

Informations : [Aide sur le Journal](#)

## b) Avertissement

The screenshot displays the Windows Event Viewer interface. At the top, a header bar indicates 'Application' and 'Nombre d'événements : 4 081'. Below this is a table listing events. The first three rows are warnings (yellow triangle icon) from the 'ESENT' source, all occurring on 2020-09-09 at 16:30:49, with IDs 640, 636, and 640 respectively, and a 'Général' category. The fourth row is an information event (blue 'i' icon) from 'EventSystem' at 16:30:48, with ID 4625 and 'Aucun' category. The fifth row is partially visible, showing an information event from 'User Profile' at 16:30:47, with ID 1521 and 'Aucun' category.

The 'Événement 640, ESENT' window is open, showing the 'Général' tab. The main text area contains the following message:

Catalog Database (1300,D,35) Catalog Database: Erreur -1919 lors de la validation de la page d'en-tête dans le fichier de mappage de vidage « C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb.jfm ». Le fichier de mappage de vidage sera invalidé.  
Informations supplémentaires : [SignDbHdrFromDb:Create time:00/00/1900 00:00:00.000 Rand:0]

Below the message, the following details are listed:

Journal :	Application		
Source :	ESENT	Connecté :	2020-09-09 16:30:49
Événement :	640	Catégorie :	Général
Niveau :	Avertissement	Mots-clés :	Classique
Utilisateur :	N/A	Ordinateur :	DESKTOP-6GGOFCD
Opcode :			
Informations :	<a href="#">Aide sur le Journal</a>		

## c) Erreur

**Système** Nombre d'événements : 2 605

Niveau	Date et heure	Source	ID de l'événe...	Catégorie de ...
Information	2020-11-10 07:18:10	Time-Service	37	Aucun
Erreur	2020-11-10 03:56:31	DistributedC...	10010	Aucun
Erreur	2020-11-09 15:57:46	DistributedC...	10010	Aucun
Information	2020-11-09 15:43:19	Kernel-Gener...	16	Aucun
Information	2020-11-09 14:24:01	Service Cont...	7040	Aucun

**Événement 10010, DistributedCOM**

Général Détails

Le serveur Microsoft.SkypeApp\_15.65.78.0\_x86\_kzf8qxf38zg5c!App.AppXtvmqn4em5r5dpafgj4t4yyxgjfe0hr50.mca ne s'est pas enregistré sur DCOM avant la fin du temps imparti.

Journal : Système

Source : DistributedCOM Connecté : 2020-11-10 03:56:31

Événement : 10010 Catégorie : Aucun

Niveau : Erreur Mots-clés : Classique

Utilisateur : DESKTOP-6GGOFCD\Etudiar Ordinateur : DESKTOP-6GGOFCD

Opcode : Informations

Informations : [Aide sur le Journal](#)

## d) Critique

The screenshot displays the Windows Event Viewer interface. At the top, a summary bar indicates 'Système' with 'Nombre d'événements : 2 605'. Below this is a table of events. The event with ID 41 is highlighted, showing a 'Critique' (Critical) level. The description of this event states: 'Le système a redémarré sans s'arrêter correctement au préalable. Cette erreur peut survenir si le système ne répond plus, s'est bloqué ou n'est plus alimenté de façon inattendue.' Below the description, the 'Général' (General) tab is active, showing details such as 'Journal : Système', 'Source : Kernel-Power', 'Événement : 41', 'Niveau : Critique', 'Utilisateur : Système', 'Opcode : Informations', and 'Informations : [Aide sur le Journal](#)'.

Niveau	Date et heure	Source	ID de l'événe...	Catégorie de ...
Information	2020-11-11 14:08:49	Kernel-Power	172	(203)
Critique	2020-11-11 14:08:49	Kernel-Power	41	(63)
Information	2020-11-11 14:08:49	FilterManager	6	Aucun
Information	2020-11-11 14:08:49	e1i65x64	32	Aucun
Information	2020-11-11 14:08:49	Kernel-Power	55	(17)

Événement 41, Kernel-Power

Général Détails

Le système a redémarré sans s'arrêter correctement au préalable. Cette erreur peut survenir si le système ne répond plus, s'est bloqué ou n'est plus alimenté de façon inattendue.

Journal : Système  
Source : Kernel-Power  
Événement : 41  
Niveau : Critique  
Utilisateur : Système  
Opcode : Informations  
Informations : [Aide sur le Journal](#)

Connecté : 2020-11-11 14:08:49  
Catégorie : (63)  
Mots-clés : (70368744177664),(2)  
Ordinateur : DESKTOP-6GGOFCD

Q10 Fermez votre session puis essayez de la rouvrir avec un mauvais mot de passe (un seul essai suffit). Donnez ensuite le bon mot de passe et ouvrez l'observateur d'événements. À quel endroit allez-vous chercher pour voir l'information sur l'échec de l'ouverture de session?

Dans le journal de sécurité

Q11 L'avez-vous trouvé? Insérez une capture d'écran de l'événement témoignant de l'échec d'ouverture de session.

**Sécurité** Nombre d'événements : 20 211 (1) Nouveaux événements disponibles

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la
Succès de l'audit	2020-11-13 14:55:34	Microsoft Windo...	4648	Logon
Échec de l'audit	2020-11-13 14:55:29	Microsoft Windo...	4625	Logon
Succès de l'audit	2020-11-13 14:55:26	Microsoft Windo...	4634	Logoff
Succès de l'audit	2020-11-13 14:55:26	Microsoft Windo...	4634	Logoff

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-6GGOFCD\$
- 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 : Etudiant
- Domaine du compte : DESKTOP-6GGOFCD

Informations sur l'échec :

- Raison de l'échec : Nom d'utilisateur inconnu ou mot de passe incorrect.
- État : 0xC000006D
- Sous-état : 0xC000006A

Informations sur le processus :

- ID du processus de l'appelant : 0x504
- Nom du processus de l'appelant : C:\Windows\System32\svchost.exe

Journal : Sécurité

Source : Microsoft Windows security Connecté : 2020-11-13 14:55:29

Événement : 4625 Catégorie : Logon

Niveau : Information Mots-clés : Échec de l'audit

Utilisateur : N/A Ordinateur : DESKTOP-6GGOFCD

Opcode : Informations

Informations : [Aide sur le Journal](#)

# Fin du laboratoire!