



Windows Client Avancé

Cours 1 : Dépannage et analyse du Système et du matériel

JACQUEMIN Mathieu

Maîtriser les fonctions avancées du système d'exploitation Windows sur les postes clients d'une entreprise

- **Installer, optimiser et dépanner les postes sous Windows dans un environnement réseau**
 - **Déployer des postes de travail sous Windows**
 - **Analyser les performances d'un poste de travail sous Windows**
 - **Être capable de protéger et récupérer un système Windows**

Chaque séance sera composée de cours, entremêlé de TP, dans lesquels vous rédigerez un compte-rendu sous forme de tutoriel expliquant vos faits et gestes afin de répondre à la problématique du TP

Tirez des conclusions sur ce que vous venez de découvrir, documentez votre compte-rendu. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration (capture d'écran)...

Le contexte

- 1 Utilisateur
- 1 Ordinateur Windows Client

Les souhaits de la direction

- Déterminer et diagnostiquer rapidement une panne sur un poste utilisateur et savoir la réparer

Quelles solutions ?

→ Comment répondre au besoin ?

Connaitre les outils à utiliser en cas de panne et savoir où regarder

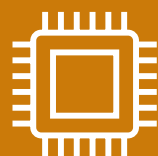
→ Quelles préconisations supplémentaires en tant que technicien informatique ?

Mise en place d'une supervision





Analyse des
ressources et
performance



Diagnostic
système et
matériel



Optimiser
l'utilisation de
votre
ordinateur



Bonnes
Pratiques et
Sécurisations



Travaux
Pratiques

1. Analyse des ressources et performance

Le Gestionnaire des Tâches

- C'est dans le gestionnaire des tâches que l'on va fouiller dans le cas de :
 - Ralentissement de l'ordinateur
 - Ralentissement d'un programme
 - Bug d'un programme
 - Vérification du matériel de l'ordinateur
 - Vérification des services qui tournent
 - Etc.

- Pour y accéder : « Clic droit dans la barre des tâches », puis « Gestionnaire des tâches »

Le Gestionnaire des Tâches : Processus

Le Gestionnaire des Tâches : Processus

Le premier réflexe à avoir, quand un ordinateur est trop lent, est de vérifier ici qu'une application ou un programme n'utilise pas une ressource de manière disproportionnée.

Si c'est bien le cas, il est fort possible que cette application ait un problème. Dans ce cas, il vous est possible de la « tuer » en la sélectionnant et en cliquant sur « Fin de tâche » en bas à droite.

Une autre explication possible est que l'ordinateur n'a pas suffisamment de ressources pour cette application. Dans ce cas, il n'y a pas d'autre solution que de changer de matériel.

Le Gestionnaire des Tâches : Performance

L'onglet Performances : vous permet de voir l'état d'une ressource plus en profondeur, mais sans prendre en compte les applications

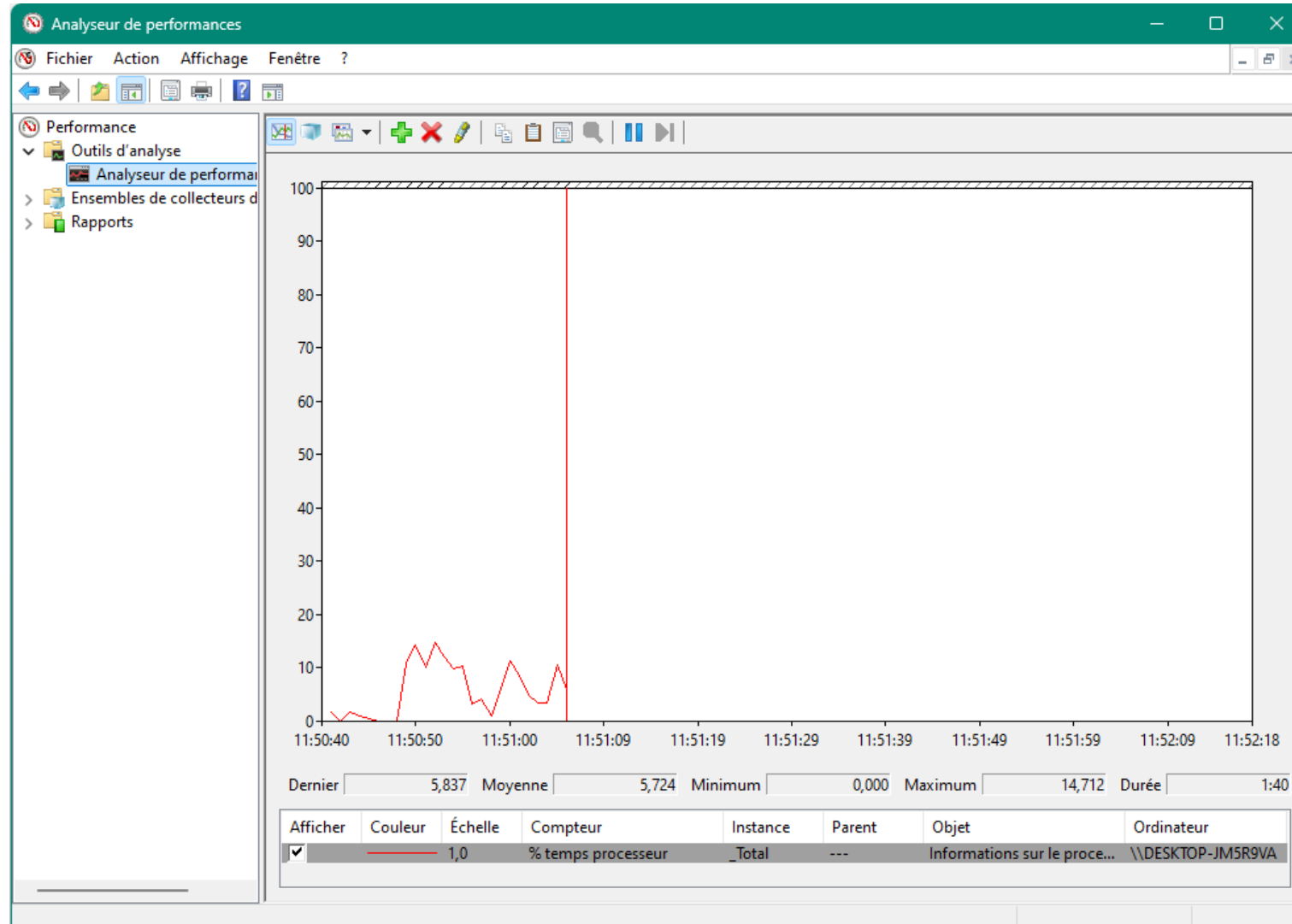
Vous pouvez vérifier, l'état du processeur, la mémoire RAM, l'utilisation du disque dur, les cartes réseau, le Bluetooth et la carte graphique.

Il permet également de voir les références et la puissance maximale de chaque composant

L'analyseur de performances

- L'analyseur de performances permet d'affiner les recherches. Par exemple, dans le cas du processeur, des dizaines d'indicateurs sont possibles. Vous pouvez, entre autres, regarder le taux d'inactivité de votre processeur, mais aussi des moyennes.
- Pour ajouter un indicateur à votre Analyseur de Performances, il vous suffit de :
 - Cliquer sur le bouton + (vert)
 - Sélectionner un compteur (c'est-à-dire un type : processeur, processus, RAM, etc.)
 - Sélectionner une instance, ou plusieurs (c'est-à-dire un sous-type encore plus précis).
- Dans notre cas, « Processus », « % temps processeur » et ensuite le processus voulu

L'analyseur de performances



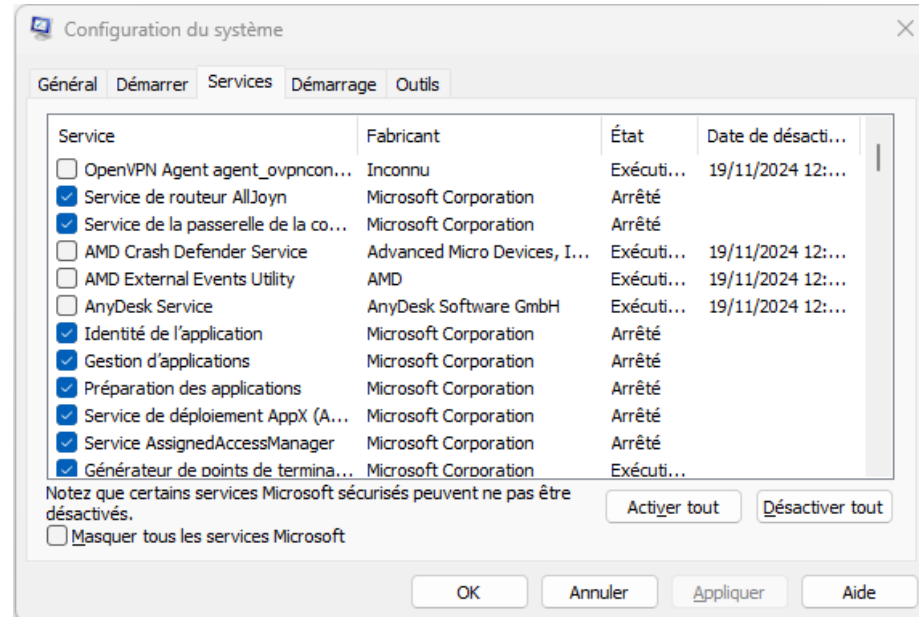
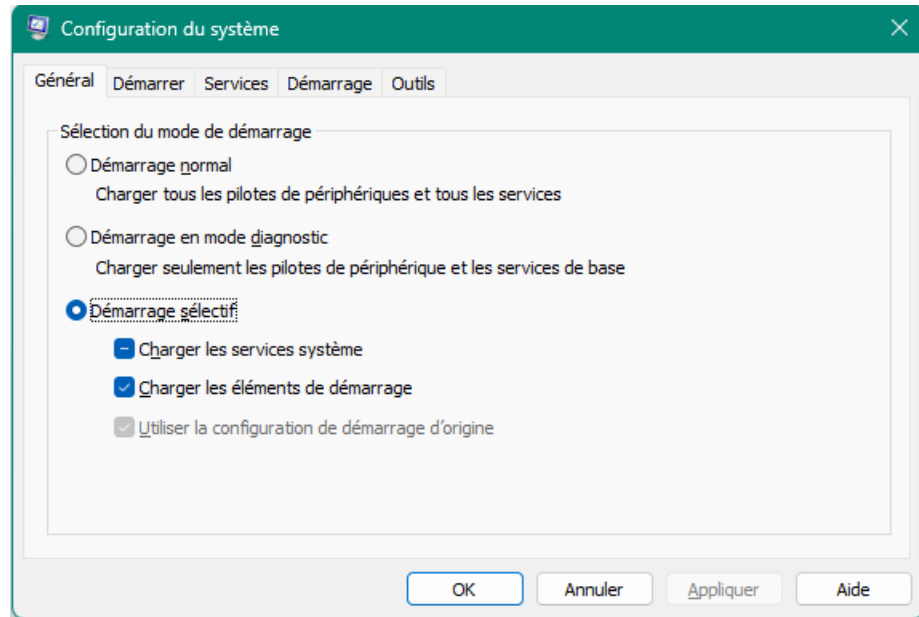
Démarrage Sélectif

- Si l'une de vos applications ne fonctionne pas normalement, comme l'application métier de votre entreprise par exemple, il se peut que ce ne soit pas elle directement qui soit à mettre en cause mais plutôt la configuration de Windows. Autrement dit, ce qui est installé sur l'ordinateur et leurs paramètres.
- Pour savoir si votre application est la cause du dysfonctionnement ou non, vous allez devoir redémarrer Windows en « mode sélectif ». Ce mode vous permet de redémarrer Windows en ne sélectionnant que les services de base, et donc d'éliminer ceux qui seraient susceptibles de vous poser problème.

Démarrage Sélectif

- Pour cela, rendez-vous dans « Configuration du système » (ou en tapant « msconfig ») :
 - Cochez « Démarrage sélectif » dans le 1^{er} onglet
 - Dans l'onglet « Services »
 - Cochez « Masquer tous les services Windows »
 - Cliquez sur « Désactiver tout »
 - Cochez le service portant le nom de votre application (si votre application n'a pas de service associé, vous pourrez la lancer au démarrage)
 - Redémarrez Windows

Démarrage Sélectif



Pour rappel, un service n'est ni plus ni moins qu'un programme s'exécutant en arrière-plan. C'est-à-dire que vous ne le voyez pas forcément et qu'il ne dispose pas non plus d'interface graphique montrant son exécution. Pour son fonctionnement, Windows lance une multitude de services au démarrage. Beaucoup d'applications que vous installerez exécuteront un service sur votre ordinateur Windows. Il se peut qu'ils soient la cause d'un problème

Si, au redémarrage de Windows, votre application fonctionne correctement, vous savez qu'il s'agit d'un problème lié à votre configuration. Il vous reste donc à trouver les modifications que vous avez effectuées sur votre ordinateur et qui empêchent votre application de fonctionner correctement. Dans le cas contraire, il ne vous reste plus qu'à contacter les développeurs de l'application.

L'un de vos collègues rencontre des problèmes de performance sur son PC depuis votre tout premier jour. L'ordinateur met très longtemps à s'allumer chaque matin, les applications comme Microsoft Edge s'exécutent lentement et il reçoit régulièrement des alertes sur son écran sur le manque de mémoire RAM de l'ordinateur. À cause de tout cela, il lui est difficile d'accomplir son travail au quotidien.

Vous avez accepté de bloquer deux heures cette semaine pour analyser l'ordinateur et identifier le problème.

Ce que vous devez faire : Utilisez les outils suivants pour analyser la performance de votre ordinateur et en déduire le problème (à simuler car le TP se fera sur vos postes respectifs) :

1. Gestionnaire des tâches
2. Analyseur de performances
3. Démarrage sélectif

2. Diagnostic système et matériel

Mode sans échec

Le mode sans échec correspond à un mode de démarrage de Windows dans sa version minimaliste, ce qui signifie que seuls quelques fichiers et pilotes essentiels sont chargés lorsque le PC démarre.

Le mode sans échec permet d'effectuer un diagnostic rapide de l'appareil en écartant certaines causes possibles liées aux paramètres par défaut, aux pilotes de périphériques et aux logiciels installés. Car si le problème ne survient pas lorsque Windows démarre en mode sans échec, c'est que son origine ne se trouve pas au niveau du système en lui-même, mais ailleurs.

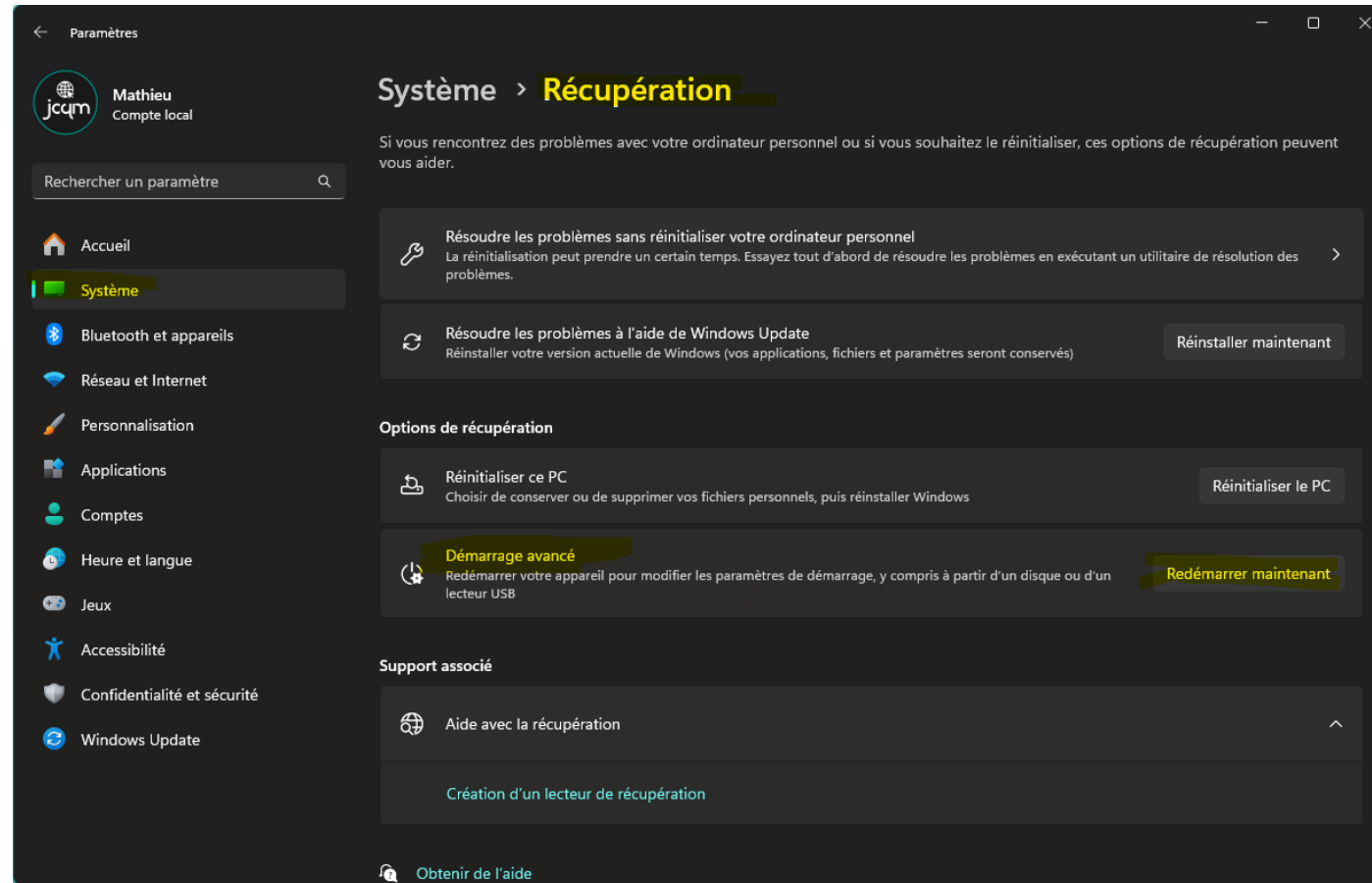
Le mode sans échec correspond à un mode de démarrage de Windows dans sa version minimaliste, ce qui signifie que seuls quelques fichiers et pilotes essentiels sont chargés lorsque le PC démarre.

Mode sans échec

→ Il existe différents moyens d'accéder au mode sans échec :

- Depuis les Paramètres : Rendez-vous dans « Système », puis sélectionnez « Récupération » dans la liste. Ensuite dans « Démarrage avancé », cliquez sur « Redémarrer maintenant ». Une fois redémarré, sélectionnez « Dépannage », « Options avancées », « Paramètres », puis « Redémarrer ». Différentes options sont affichées : Appuyez sur 4 pour le mode sans échec et 5 pour la prise en charge du réseau
- Si votre PC plante et qu'il devient impossible d'accéder aux Paramètres, essayez de retourner à l'écran de connexion de Windows puis maintenez la touche Maj (Shift) enfoncée tout en cliquant sur « Redémarrer » dans le menu Démarrer. Une fois fait, vous pouvez suivre les manipulations de la solution précédente, une fois le 1^{er} redémarrage effectué
- Si vous n'avez plus accès à rien et que votre ordinateur ne veut rien savoir, vous pouvez également lancer le mode sans échec lorsque vous allumez votre PC. Il vous suffira de rester appuyer sur la touche F8 tout en démarrant votre ordinateur via le bouton power. Puis de nouveau suivre les mêmes instructions qu'au dessus

Mode sans échec



Mode sans échec

← Options avancées



Restauration du système

Utiliser un point de restauration sur votre PC pour restaurer Windows



Invite de commandes

Utiliser l'invite de commandes pour un dépannage avancé



Récupération de l'image système

Récupérer Windows à l'aide d'un fichier image système spécifique



Paramètres

Changer le comportement de Windows au démarrage



Outil de redémarrage système

Corriger les problèmes qui empêchent le chargement de Windows



Rétrograder vers la version précédente

Mode sans échec

Paramètres de démarrage

Appuyez sur un chiffre pour sélectionner l'une des options ci-dessous :

Utilisez les touches numériques ou les touches de fonction F1 à F9.

- 1) Activer le débogage
- 2) Activer la journalisation du démarrage
- 3) Activer la vidéo basse résolution
- 4) Activer le mode sans échec
- 5) Activer le mode sans échec avec prise en charge réseau
- 6) Activer le mode sans échec avec invite de commandes
- 7) Désactiver le contrôle obligatoire des signatures de pilotes
- 8) Désactiver la protection du logiciel anti-programme malveillant à lancement anticipé
- 9) Désactiver le redémarrage automatique en cas d'échec

L'observateur d'événements est le journal d'activité de Windows et de ses applications.

Il enregistre donc toute l'activité de Windows et des applications dans des journaux d'évènements consultables par l'utilisateur. Cela peut aller de la simple information, à l'enregistrement d'évènements critiques ou d'erreurs lié à des plantages de Windows ou de logiciels.

Ainsi l'observateur d'évènements de Windows est un formidable outil pour savoir tout ce qui se passe dans le système d'exploitation

L'observateur d'évènements

The screenshot displays the Windows Event Viewer application. The left pane shows the tree structure with 'System' selected under 'Windows Logs'. The main pane shows a list of system events. The selected event is 'Error 20' from 'WindowsUpdateClient', which occurred on 19/11/2024 at 12:53:33. The details pane shows the error message: 'Échec de l'installation : l'installation de la mise à jour suivante a échoué avec l'erreur 0x80073D02 : 9MSSGKG348SP-MicrosoftWindows.Client.WebExperience.' The right pane shows the 'Actions' menu with options like 'Open the log', 'Create a custom view', etc.

Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local)

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

Système Nombre d'événements : 37331

Niveau	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Information	19/11/2024 13:23:48	DriverFramework...	10000	Installation or up...
Information	19/11/2024 13:22:20	Kernel-Power	566	(268)
Information	19/11/2024 12:56:00	Kernel-Power	566	(268)
Information	19/11/2024 12:53:34	WindowsUpdate...	19	Agent de mise à j...
Erreur	19/11/2024 12:53:33	WindowsUpdate...	20	Agent de mise à j...
Information	19/11/2024 12:53:33	WindowsUpdate...	43	Agent de mise à j...

Événement 20, WindowsUpdateClient

Général Détails

Échec de l'installation : l'installation de la mise à jour suivante a échoué avec l'erreur 0x80073D02 : 9MSSGKG348SP-MicrosoftWindows.Client.WebExperience.

Journal : Système

Source : WindowsUpdateClient Connecté : 19/11/2024 12:53:33

Événement : 20 Catégorie : Agent de mise à jour automatique Windows Update

Niveau : Erreur Mots-clés : Échec, Installation

Utilisateur : Système Ordinateur : DESKTOP-JM5R9VA

Opcode : Installation

Informations : [Aide sur le Journal](#)

Actions

Système

- Ouvrir le journal enregistré...
- Créer une vue personnalisée...
- Importer une vue personnalisée...
- Effacer le journal...
- Filtrer le journal actuel...
- Propriétés
- Rechercher...
- Enregistrer tous les événements...
- Joindre une tâche à ce journal...
- Affichage
- Actualiser
- Aide

Événement 20, WindowsUpdateCli...

- Propriétés de l'événement
- Joindre une tâche à cet événement...
- Copier
- Enregistrer les événements sélectionnés...
- Actualiser
- Aide

L'un de vos collègues rencontre un problème sur son PC, il n'arrive même plus à accéder à sa session et au système d'exploitation.

Il ne peut donc pas du tout utiliser son poste actuellement.

C'est à vous que revient la tâche d'identifier le problème et tant qu'à faire, de le résoudre !

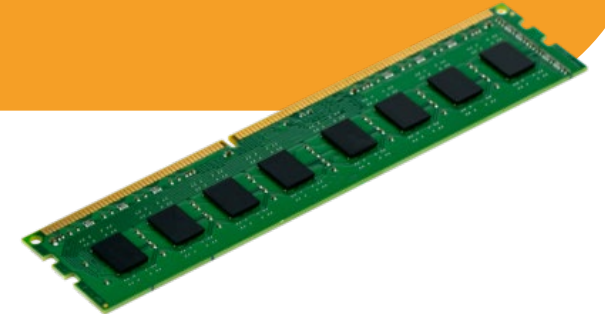
Ce que vous devez faire :

1. Démarrer le poste en mode sans échec
2. Déterminer si un programme peut empêcher le démarrage
3. Regarder si il y a des erreurs

PC qui plante, écran bleu, Ceci peut être dû à un problème de barrette mémoire. Ce composant est souvent utilisé et très fragile, c'est pourquoi Windows propose un outil de diagnostic vous permettant de connaître l'état de votre RAM

Un autre outil plus puissant (mais non intégré à Windows) vous permet de tester votre mémoire vive en lui appliquant une série de tests (13 algorithmes de test de RAM différents sont disponibles). Il est beaucoup plus puissant et il est suivi et mis à jour régulièrement par son éditeur :

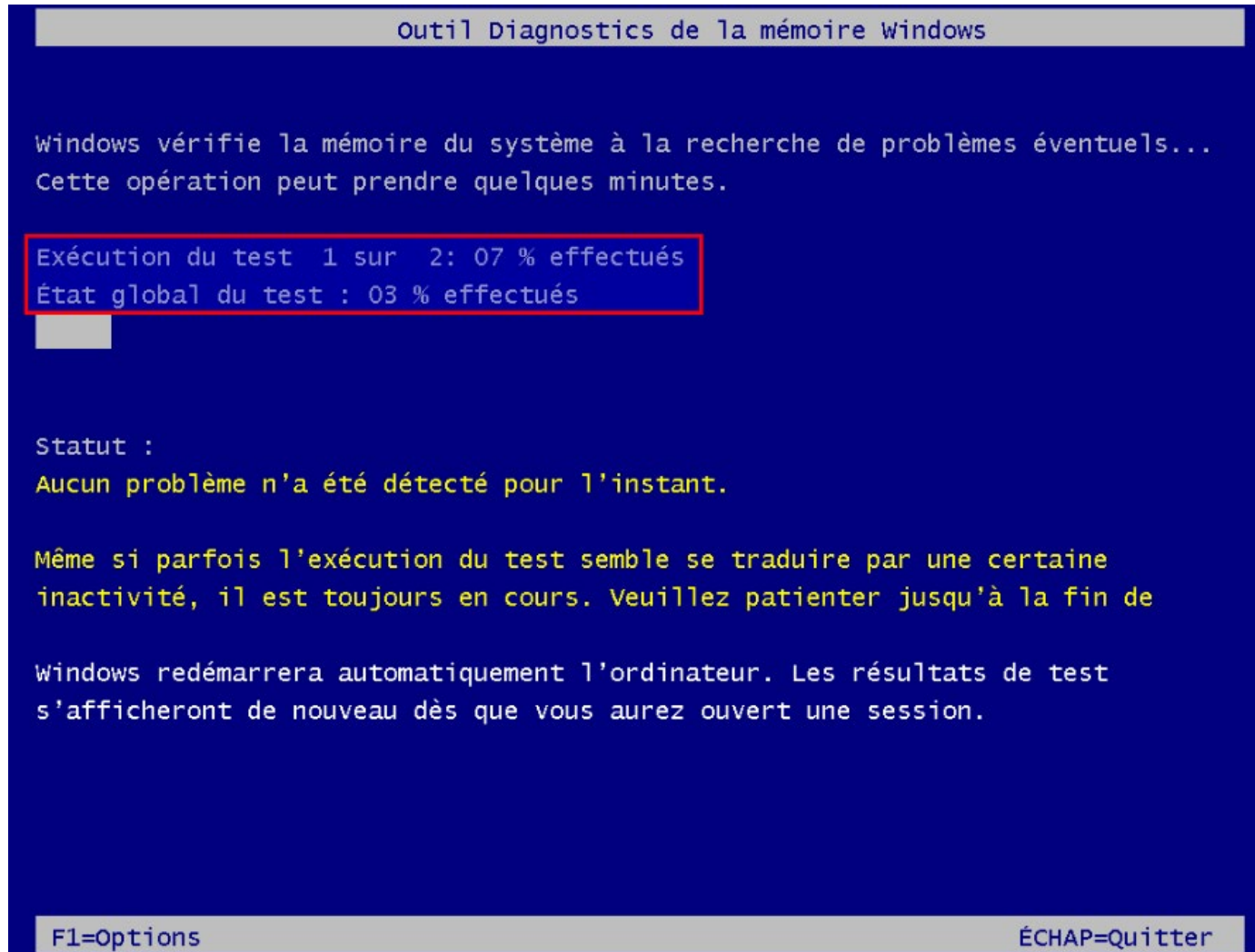
MemTest86



Diagnostic de la mémoire vive Windows

- Ouvrir « Diagnostic de mémoire Windows »
- Deux choix s'offrent à vous : redémarrer tout de suite l'ordinateur afin d'effectuer le diagnostic, ou effectuer le diagnostic au prochain redémarrage
- Une fois sur l'écran du diagnostic, vous pouvez presser la touche F1 afin d'effectuer un test approfondi
- Choisissez « cache : actif » (il s'agit de la mémoire intégrée à votre CPU)
- Choisissez la valeur cinq pour le nombre de passe (plus la panne est rare, plus il est difficile de la trouver ; en faisant plusieurs passes, vous avez plus de chances de trouver la panne).

Diagnostic de la mémoire vive Windows



Diagnostic de la mémoire vive Windows

```
Memtest-86 v4.0a      Intel(R) Core(TM) i7 CPU           870  @ 2.93GHz
CPU Clk : 2927 MHz      : Pass 6% ##
L1 Cache: 64K 63626 MB/s : Test 38% #####
L2 Cache: 256K 33641 MB/s : Test #3 [Moving inversions, 1s & 0s] Sequential
L3 Cache: 8192K 225138 MB/s : Testing: 260K - 2048M 2048M of 2048M
Memory : 2048M 33656 MB/s : Pattern: 00000000
-----
CPU: 0 1 2 3          : CPUs_Started: 4  CPU_Select: All
State: W : W W        : CPUs_Active: 1  CPUs_Found: 4
-----
Time 0:00:27  Iterations: 2  Test_Sel: Std  Pass: 0  Errors: 0

-

(ESC)exit (c)configuration (SP)scroll_lock (CR)scroll_unlock
```


Les disques durs sont depuis plusieurs années équipés de systèmes SMART (Self-Monitoring, Analysis, and Reporting Technology) qui vous permettent d'avoir des indications concernant leur état de santé. C'est important car, quand un disque dur tombe en panne, vous perdez généralement ses données.

Le principe est simple : chaque fois que le disque dur va rencontrer un problème, il ne va pas vous le dire, mais il va mettre à jour sa liste d'incidents. On appelle ces informations les informations "SMART".



Diagnostic du disque dur

- Voici quelques tests possibles pour les disques durs :
 - Avec WMIC (Windows Management Instrumentation Command-line)
"wmic diskdrive get status, model, size, mediatype"
cette méthode est ultra-simple mais aussi ultra-limitée
 - Pour avoir plus d'informations sur l'état de santé d'un disque dur, il faut se tourner vers des logiciels tiers comme :
 - CrystalDiskInfo
 - Hard Disk Sentinel
 - HD Tune
 - Etc.

Diagnostic du disque dur

CrystalDiskInfo 9.4.4 x64

FichierÉditionFonctionsThèmeDisqueAideLangue(Language)

Bon
33 °C
C:

INTEL SSDPEKNW512GZL : 512,1 GB

État de santé
Bon
96 %
Température
33 °C

Firmware	C01C	Total lecture hôte	30388 GB
Numéro de série	BTKA22610P23512A	Total écriture hôte	19730 GB
Interface	NVM Express	Vitesse de rotation	---- (SSD)
Mode de transfert	PCIe 3.0 x4 PCIe 3.0 x4	Nombre d'allumages	3713 fois
Lettre de lecteur	C:	heures de fonctionnement	3034 heures
Standard	NVM Express 1.4		
Fonctionnalités	S.M.A.R.T., TRIM, VolatileWriteCache		

ID	Nom d'attribut	Valeurs brutes
01	Avertissement critique	0000000000000000
02	Température composite	000000000000132
03	Cellules de rechange disponibles	000000000000064
04	Seuil de cellules de rechange disponibles	00000000000000A
05	Pourcentage utilisé	000000000000004
06	Unités de données lues	00000003CC7082
07	Unités de données écrites	00000002776073
08	Commandes de lecture de l'hôte	0000002A888180
09	Commandes d'écriture de l'hôte	000000218111DB
0A	Temps occupé du contrôleur	00000000002F40
0B	Cycles d'alimentation	000000000000E81
0C	Heures de mise sous tension	000000000000BDA
0D	Arrêts dangereux	00000000000001B
0E	Erreurs d'intégrité des médias et des données	000000000000000
0F	Nombre d'entrées du journal d'informations sur les erreurs	000000000000001

HD Tune Pro 3.00 - Hard Disk Utility

WDC WD360GD-00FLA2 (37 GB) 27°C

Folder UsageEraseFile BenchmarkDisk monitorAAM

BenchmarkInfoHealthError Scan

Start

Read

Write

Transfer rate

Minimum
43.4 MB/sec

Maximum
62.7 MB/sec

Average:
55.8 MB/sec

Access time:
7.9 ms

Burst rate
95.7 MB/sec

CPU usage
7.3%

MB/sec

ms

70

60

50

40

30

20

10

0

0

10

20

30

40

50

60

70

80

90

100%

Medicat, l'outil magique !

Medicat, est un utilitaire bootable qui inclut une suite d'outils pour dépanner et analyser un ordinateur facilement à la manière de Hiren's Boot CD, mais beaucoup plus complet.

- Utilitaires de récupérations de données
 - Live USB : Mini Windows 10
- Outils de disques : Acronis Disk Director, DiskGenius, EaseUS Partition Master
 - Outils de sauvegarde et de récupération de fichiers
 - Outils de réparation du démarrage
 - Outils de diagnostics : Memtest86+, TestDisk
 - Analyses antivirus
 - Stress Test
- Réinitialiser et suppression de mots de passe Windows



Votre collègue se plaint de grosse lenteur sur son poste au démarrage ou à l'ouverture de programmes.

Effectuez et citez le test par lequel vous commenceriez à regarder

Grâce aux isos fournis, expérimentez avec les outils vus précédemment

3. Optimiser l'utilisation de votre ordinateur

Gestion des disques

- Le « Gestionnaire de disque dur » est l'outil de Microsoft qui vous permet de gérer un disque. Cet outil vous sera donc utile pour :
 - Ajouter un nouveau disque
 - Partitionner un disque dur, pour diviser un disque physique en plusieurs disques logiques
 - Formater un disque dur
- Lors d'une réinstallation de Windows, cet outil vous sera présenté d'une façon un peu différente mais les étapes resteront les mêmes. Vous aurez ainsi la possibilité de formater vos disques durs à l'installation de Windows

Gestion des disques

Gestion des disques

Fichier Action Affichage ?

Navigation icons: back, forward, refresh, help, search, delete, copy, paste, link, unlink, etc.

Volume	Disposition	Type	Système de ...	Statut	Capacité	Espace li...	% libres
(C:)	Simple	De base	NTFS	Sain (Dém...	476,06 Go	122,55 Go	26 %
(Disque 0 partition...	Simple	De base		Sain (Parti...	100 Mo	100 Mo	100 %
(Disque 0 partition...	Simple	De base		Sain (Parti...	781 Mo	781 Mo	100 %

Disque 0
De base
476,92 Go
En ligne

100 Mo Sain (Partition du système)	(C:) 476,06 Go NTFS Sain (Démarrer, Fichier d'échange, Image mémoire après incident, Partition de d	781 Mo Sain (Partition de récupération)
---------------------------------------	---	--

■ Non alloué ■ Partition principale

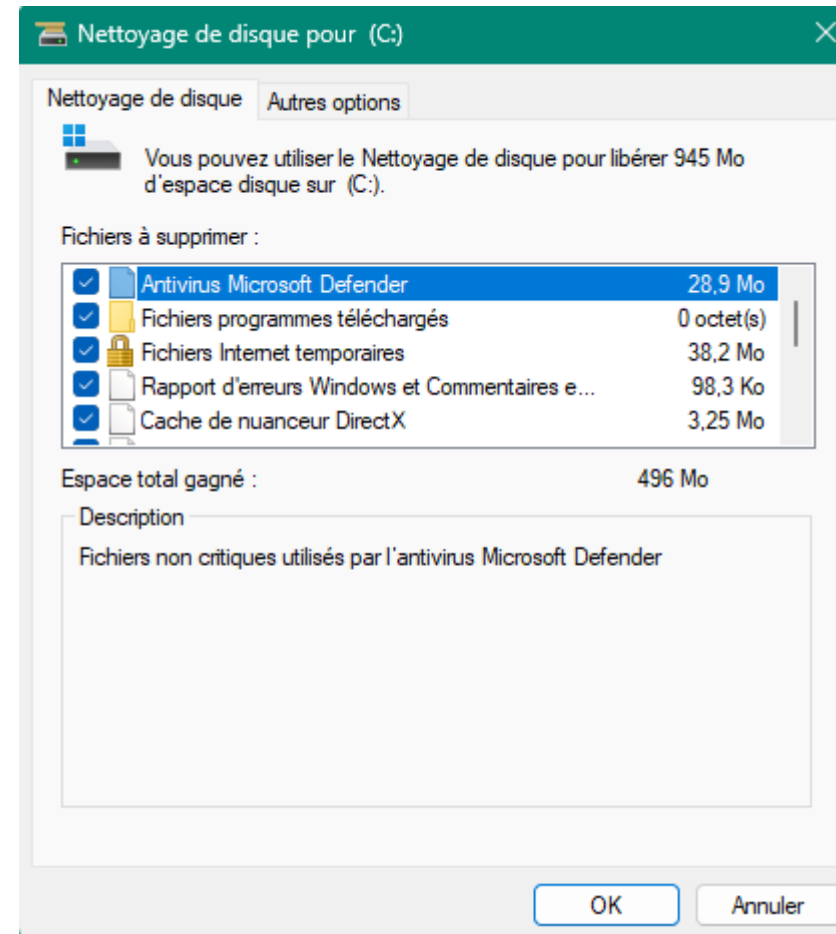
Nettoyage des disques

Votre ordinateur doit être nettoyé comme on nettoie une pièce. Il faut que l'utilisateur range ses fichiers dans les bons dossiers, tout comme nous rangeons nos affaires dans les placards, et qu'il supprime tout ce qui traîne, c'est-à-dire tout ce qui doit aller à la poubelle

Encore une fois, Windows met à votre disposition un outil vous permettant d'effectuer cette tâche.
Cet outil s'appelle « Nettoyage de disque ».

Son utilisation est très simple : il suffit de cocher les fichiers à supprimer et d'appuyer sur « OK

Nettoyage des disques



Pour automatiser une tâche, Windows met à votre disposition un outil appelé :
« Planificateur de tâches »

Le « Planificateur de tâches » vous permet de lancer un programme à une certaine fréquence. Dans le cas du nettoyeur de disque, vous pourrez donc lancer le nettoyage du disque tous les lundis par exemple

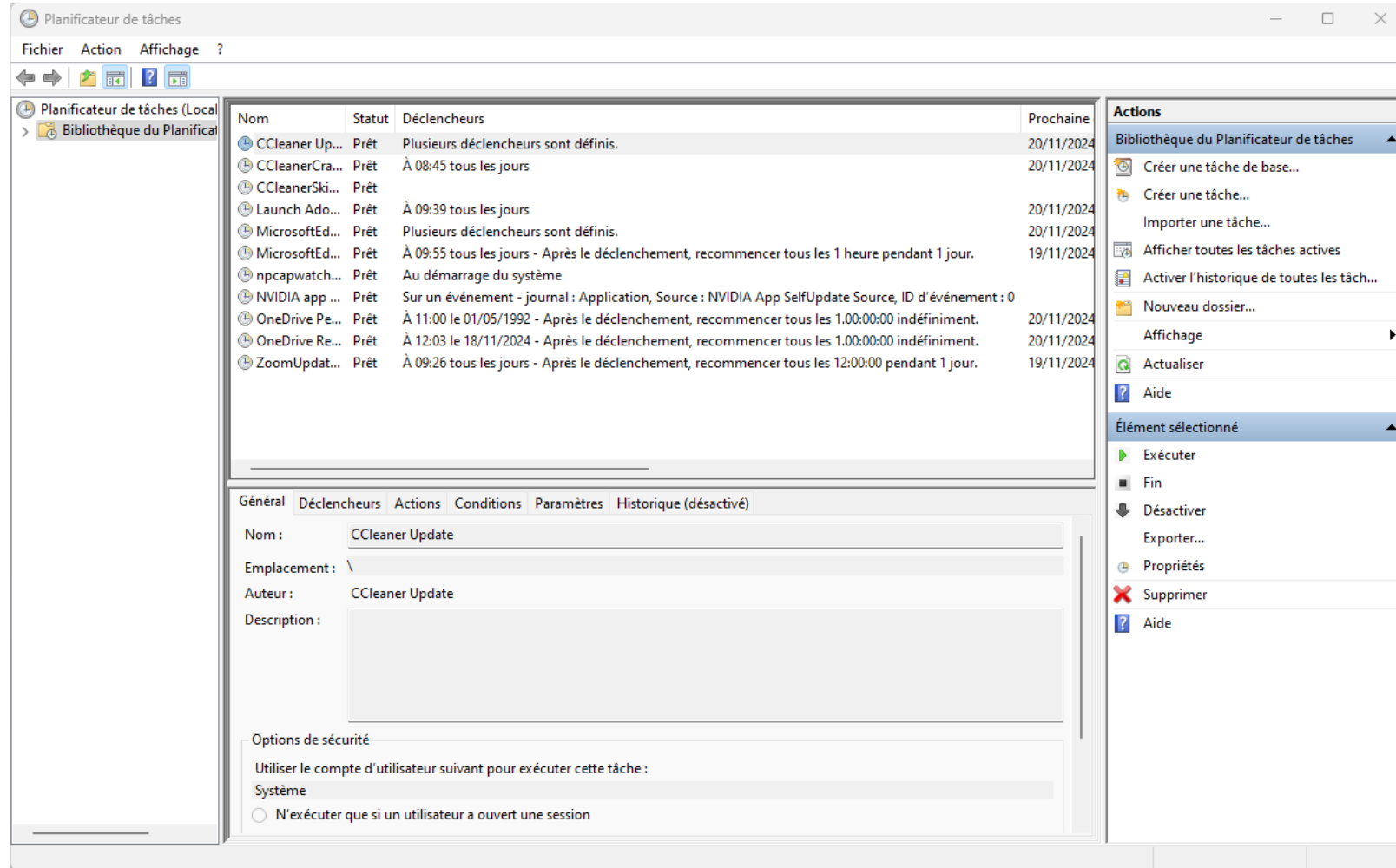
Automatiser une tâche

- Ouvrez un CMD et entrez la commande « `cleanmgr /c /sageset:1` »
- `cleanmgr` c'est donc le nettoyeur, `/c` vous permet de spécifier le disque (vous pouvez aussi choisir un autre disque), `/sageset:1` va ouvrir le nettoyeur de disque, afin que vous puissiez cocher les dossiers que vous souhaitez nettoyer. Une fois fermé, le numéro 1 (vous pouvez en choisir un autre) aura retenu votre configuration
- Entrez la commande « `cleanmgr /c /sagerun:1` », `/sagerun:1` va cette fois-ci lancer le nettoyeur de disque, avec les paramètres spécifiés correspondant au numéro 1, c'est-à-dire ce que vous avez renseigné juste avant.

Automatiser une tâche

- Créez un fichier exécutable avec l'extension « .bat » contenant la commande du dessus
- Ouvrez le « Planificateur de tâches »
- Sur la droite, sélectionnez « Créer une tâche de base »
- Donnez un nom, une description, une fréquence à votre tâche
- Sélectionnez le script en « .bat » créé précédemment

Automatiser une tâche



L'application de comptabilité de votre entreprise est utilisée pour générer un rapport financier hebdomadaire tous les vendredis à 17 heures.

Ce rapport est détaillé et peut atteindre 300 MB ! Il est essentiel que le rapport soit sauvegardé chaque semaine. Pour vous assurer qu'il y a assez d'espace disponible sur l'ordinateur, vous décidez d'exécuter un nettoyage de disque régulier. Cette opération supprimera tous les documents inutiles et garantira que seuls les fichiers importants sont sauvegardés sur l'ordinateur.

Ce que vous devez faire :

1. Créez une tâche planifiée chaque jeudi à 16 heures pour exécuter un nettoyage du disque supprimant tous les fichiers inutiles.

