ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Gestion des services et des processus
www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

1. INTRODUCTION

Souvent, on se pose la question : mais pourquoi mon PC rame ?
La première réponse est de savoir quels sont les processus par défaut qui tournent sur votre PC. Parce que c'est souvent ici que l'on remarque la présence d'un virus ou d'un ver qui se promène gentiment dans votre PC.

Donc pour optimiser les performances et la sécurité de votre PC, un petit nettoyage s'impose pour supprimer quelques **services** et **processus** qui ne servent que de temps en temps, voire pas du tout.

2. GESTION DES SERVICES

2.1. Définition de services

Les services sont des processus qui s'exécutent au démarrage de Windows, ils offrent un certain nombre de fonctionnalités et d'assistances à votre système d'exploitation. Par défaut, votre système d'exploitation en démarre un certain nombre (51 sur le SP2) qui ne reflètent pas forcément la configuration de votre machine et son environnement ou votre façon de l'utiliser.

Avoir beaucoup de fonctionnalités, c'est bien, mais beaucoup d'entre elles sont prévues pour l'utilisation d'une station de travail dans une entreprise en réseau, est-ce votre cas ?

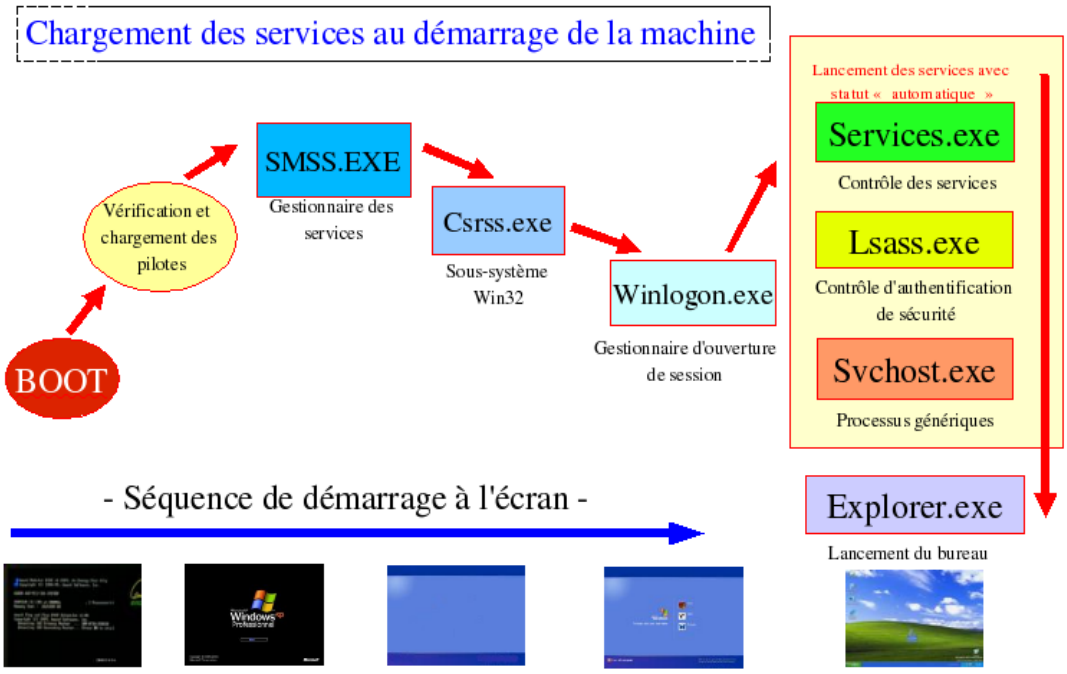
Ils ne sont pas nécessairement utiles pour l'utilisation courante d'un PC dans un environnement domestique, ils prennent de la mémoire et du temps CPU. D'autre part certains services pourraient compromettre la sécurité de votre PC.

Désactiver certains de ces services libère des ressources systèmes et améliore la sécurité de votre PC sur les réseaux...

2.2. Comment fonctionnent les services ?

Pour faire simple, et sans entrer dans les détails techniques, quand votre système démarre, après le chargement des pilotes, les services démarrent les uns à la suite des autres en fonction des indications lues dans la base de registre.

En premier, le gestionnaire des services est lancé, "**smss.exe**" => et la suite s'enchaîne après la vérification de la présence des services démarrés inscrits dans la base de registre, voir figure ci-dessous :



Chaque service démarré sur cette image correspond aux processus obligatoires dont les autres services dépendent, plus vous aurez des services démarrés en automatique, plus le temps de chargement sera long, sans oublier toutes vos applications supplémentaires gérées après l'ouverture du bureau.

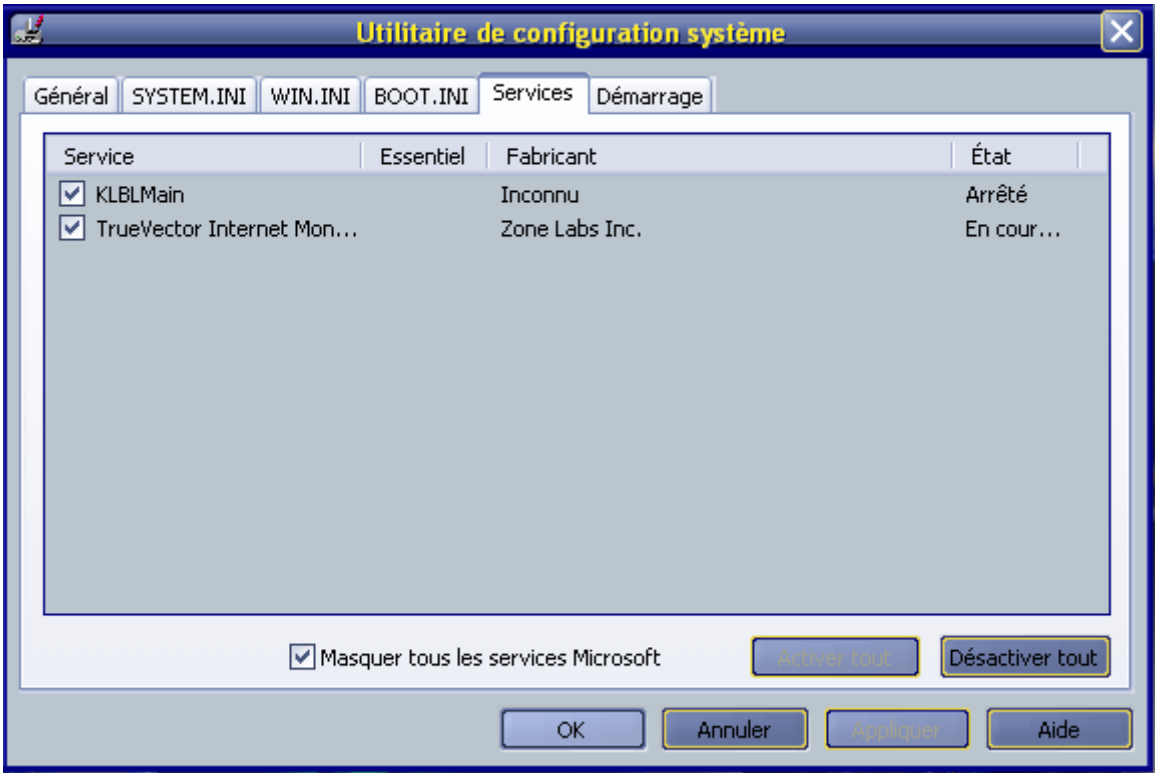
Comme vous pouvez déjà le remarquer, ces processus sont très connus, et sont souvent imités par les virus qui créent des noms proches afin que l'utilisateur se laisse prendre au piège sans s'en apercevoir.

On peut déjà résumer la situation ainsi, **"tous ces services seront toujours présents et indispensables au bon fonctionnement de votre système".** Si un de ces services ne démarre pas, vous risquez de vous retrouver bloqué sur l'écran d'ouverture de session sans pouvoir atteindre votre bureau. Dans ce cas, seule une réparation avec la console de récupération vous permettra de redémarrer le service en question.

Le nombre de services démarrés peut varier d'un PC à l'autre en fonction du matériel (hardware) et de certains logiciels installés (antivirus, firewall, etc...). Ce nombre se situe entre 70 et 85 services uniquement pour Windows. Nous verrons par la suite la liste complète faisant partie du système Windows.

2.3. *Pour connaître les services non-Microsoft*

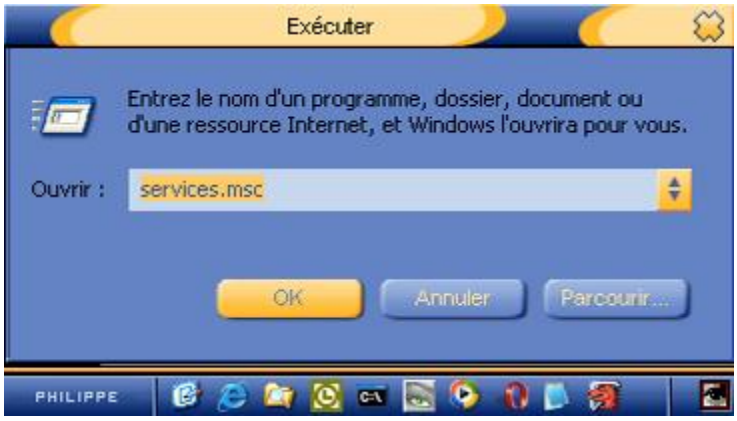
Nous pouvons voir d'un seul coup d'oeil les divers services non-Microsoft grâce à l'utilitaire msconfig
Menu Démarrer ==> Exécuter : **msconfig**
allez à l'onglet services, et activez la case : **Masquer tous les services Microsoft**



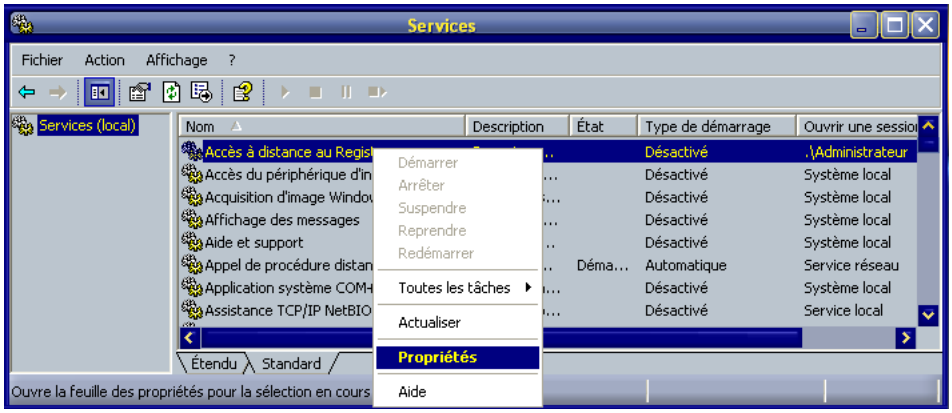
Il est important aussi de connaître les services non-Microsoft, car aujourd'hui de nombreux malwares/virus inscrivent des clés dans la base de registre à propos des services, il est souvent difficile de les identifier car ils reprennent des noms connus en changeant simplement une lettre, le simple fait de faire une vérification périodique avec cette commande vous permet de vous rassurer ou au contraire de vous alerter.

2.4. Accéder aux services

Pour accéder aux services de Windows, il suffit d'aller sur le menu "**Démarrer**" "**Exécuter**" et de taper "**services.msc**" comme sur la photo



La fenêtre suivante va s'ouvrir :



Sur la partie droite de la fenêtre,

Dans la colonne "**Nom**", vous avez la liste complète de l'ensemble des services installés sous Windows.

La colonne "**Description**" vous donne une description complète du service en question.

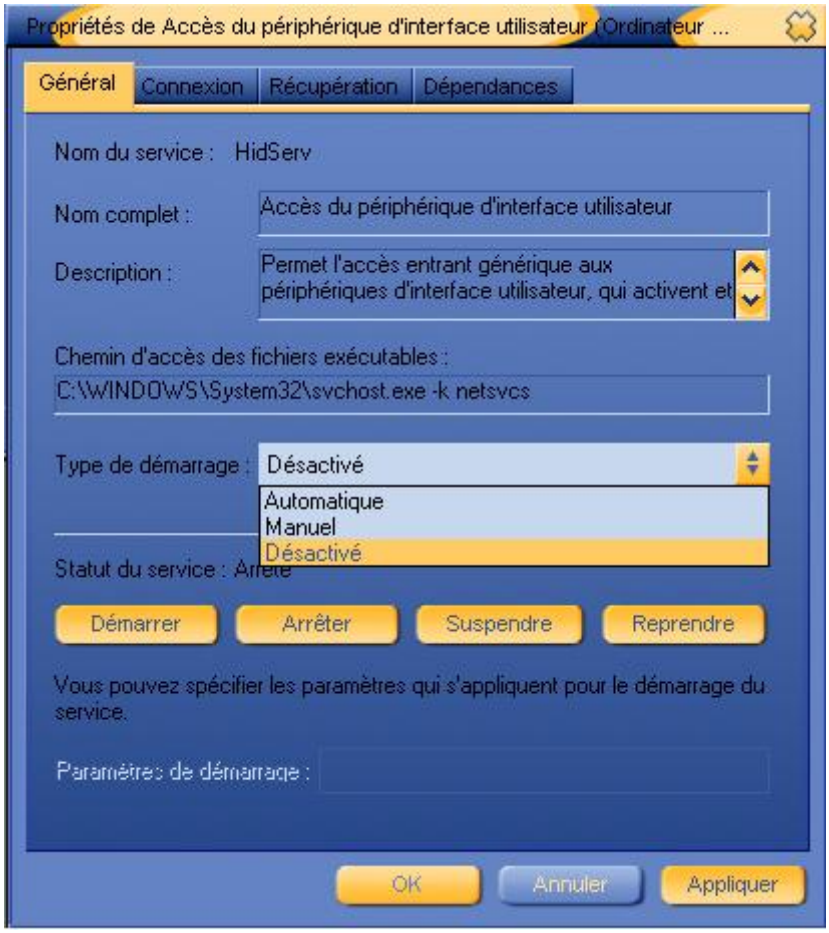
La colonne "**État**" vous indique si ce service est démarré ou non, "c'est à dire s'il a été lancé par Windows au moment où vous affichez les services" Ce lancement ne s'est pas forcément déroulé au démarrage

La colonne "**Type de démarrage**" vous indique si le démarrage de ce service est effectué automatiquement, défini de manière manuelle ou s'il est désactivé.

Pour modifier n'importe lequel de ces services, il suffit de faire un clic droit sur celui que vous voulez modifier, aller sur

"**Propriétés**"

Une nouvelle fenêtre s'ouvre alors :



Trois options sont alors disponibles pour le type de démarrage d'un service :

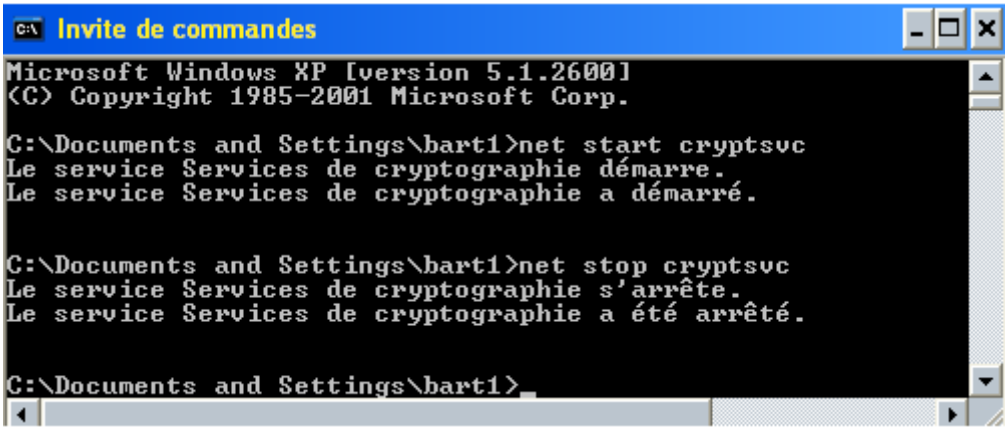
Automatique : *quand vous sélectionnez cette option, le service en question sera automatiquement exécuté au démarrage de Windows. Ceci augmente sensiblement le temps de chargement de Windows mais attention, certains services sont nécessaires à la bonne exécution de Windows XP comme l'Appel de procédure Distante (RPC).*
Des services seront également exécutés par le fait de dépendances (voir dernier onglet), certains services ayant besoin d'autres services pour fonctionner.

Manuel : *cette option permet au service en question de s'exécuter sur requête de l'utilisateur. Il n'est donc pas chargé en mémoire au démarrage du PC mais peut l'être à tout moment si vous en avez le besoin. Cette option sera parfaite pour sauvegarder des ressources systèmes et réduire le temps de boot sans désactiver complètement ces services au cas ou vous en auriez besoin ultérieurement, comme par exemple le Spouleur d'impression.*

Désactivé : *quand cette option est sélectionnée, le service en question n'est pas chargé par Windows et ne pourra l'être même s'il est requis par l'utilisateur. Cette option est idéale pour des questions de sécurité en empêchant complètement l'exécution d'un service donné.*

A l'aide d'une invite de commande
Il est également possible de démarrer ou d'arrêter un service à l'aide de l'invite

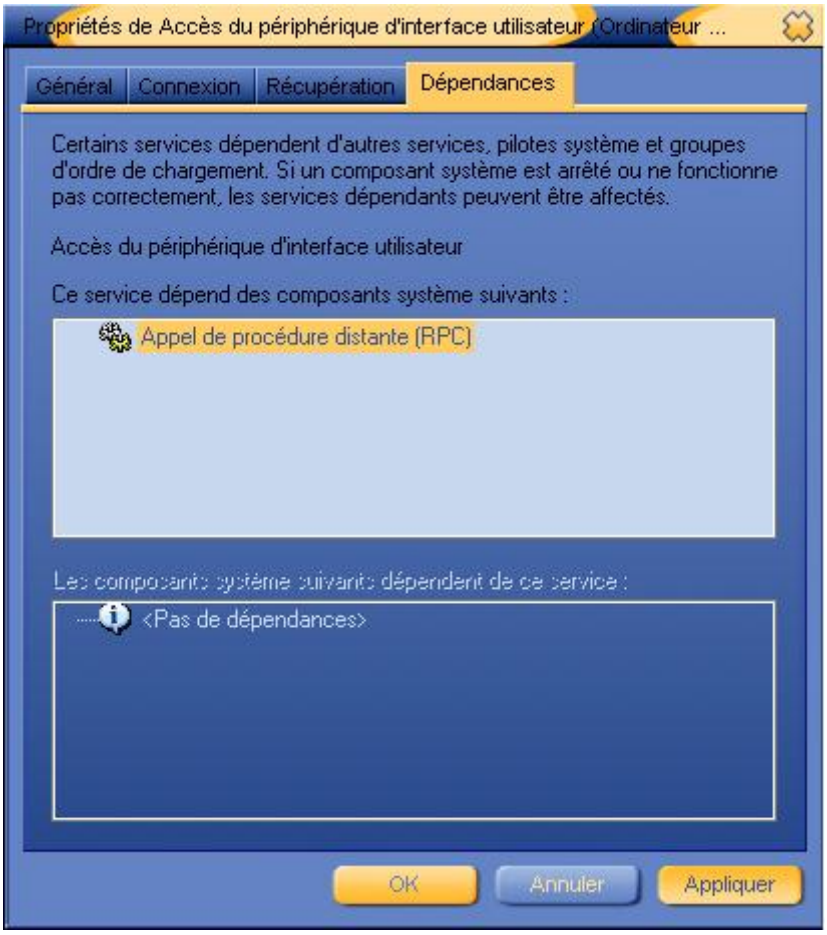
de commande:
Menu Démarrer ==> Exécuter : **cmd**
pour démarrer le service : **net start <nom interne du service>**
pour arrêter le service : **net stop <nom interne du service>**



Attention, cette commande ne fonctionne pas si le service que vous souhaitez démarrer est désactivé, ou si une dépendance dont il a besoin est désactivée.

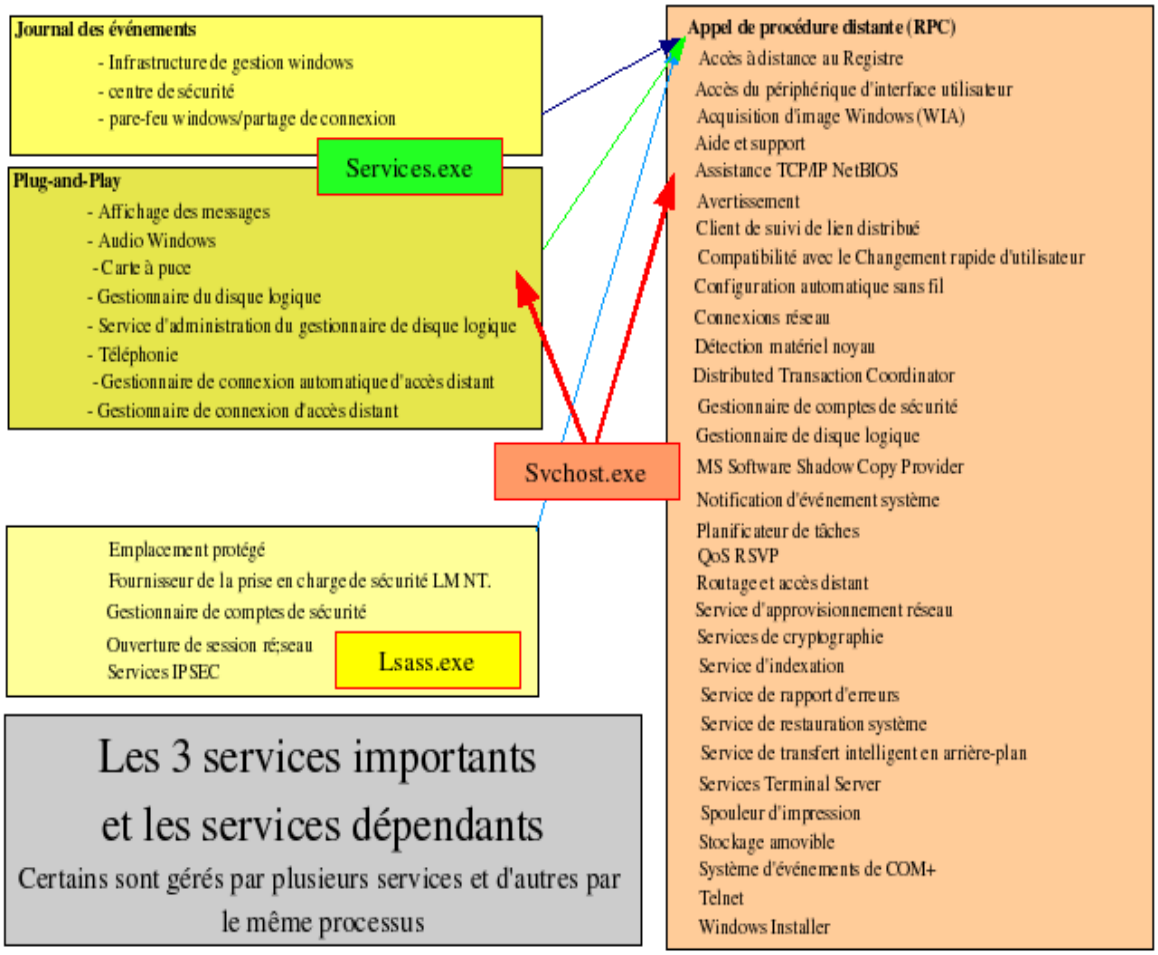
Les dépendances

Passons à l'onglet "**Dépendances**"



La dépendance est une relation qui relie deux ou plusieurs ressources, l'exécution d'un service peut être enchaînée à l'exécution de l'autre, ou inversement. Ainsi, il n'est pas recommandé de désactiver un service mais plutôt de le mettre sur manuel. Ceci empêchera que des services fonctionnent mal ou pas du tout.
Avant de désactiver un service, vérifiez toujours ces dépendances.

Sur cette image : les 3 principaux processus et leurs dépendances :



Comme vous pouvez le constater ici, les processus principaux à savoir :
services.exe - lsass.exe - svchost.exe représentent 4 sous-ensembles importants :
- Journal des évènements
- Plug and Play
- Appel de procédure distante RPC
- et le groupe utilisant lsass.exe
Plusieurs services présents ici dépendent de plusieurs processus, d'où l'inconvénient de ne pas pouvoir donner une configuration idéale

2.5. Les services obligatoires pour le bon fonctionnement de votre système.

Nous verrons par la suite que tous les services utilisant svchost.exe ne sont pas présents ici, mais on remarque déjà que ces services sont obligatoires pour le bon fonctionnement de votre système.

Pour chaque service et pour le besoin de compréhension, j'indique :
Le nom complet du service : indiqué en bleu gras
Nom de l'exécutable : indiqué en vert
Nom interne : indiqué en bleu clair
la description : *du service indiqué en italique par Microsoft*
Il dépend de : indiqué en orange, représente les services qui doivent être

démarrés afin que le service fonctionne
Dépendent de lui : indiqué en violet, représente les services qui dépendent de lui, en principe, ces services sont indispensables
Commentaire : indiqué en bleu pour les services traditionnels, **indiqué en rouge et gras pour les services obligatoires,**

Il est difficile de donner une configuration idéale, tout dépend de l'utilisation de son PC, d'être en réseau local ou pas, de privilégier la sécurité ou de vouloir gagner en efficacité.

Attention, il est possible que certains de ces services ne soient pas présents sur votre système, tout dépend de votre version Windows et des services Packs installés.

Accès à distance au Registre

Nom de l'exécutable : svchost.exe
Nom interne : remote registry
Description : *Permet aux utilisateurs à distance de modifier les paramètres du Registre sur cet ordinateur*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : Bien, voyons, c'est autoriser tout le monde à modifier votre base de registre, ce service est à fermer en priorité, pourquoi le service pack 2 de XP laisse toujours ce service "automatique" par défaut ? - Eux qui combattent les problèmes de sécurité !!!
Pour des raisons évidentes de sécurité, ce service doit être **"Désactivé"**. Ce service n'est pas présent sur XP Home.

Accès du périphérique d'interface utilisateur

Nom de l'exécutable : svchost.exe
Nom interne : HidServ
Description : *Permet l'accès entrant générique aux périphériques d'interface utilisateur, qui activent et maintiennent l'utilisation des boutons actifs prédéfinis sur le clavier, les contrôles à distance, et d'autres périphériques multimédia. Si ce service est arrêté, les boutons actifs contrôlés par ce service ne fonctionneront pas.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : Ce service peut être mis sur **"désactivé"** si vous n'utilisez pas de clavier multimédia, sinon, le laisser en mode **"manuel"**

Acquisition d'image Windows (WIA)

Nom de l'exécutable : svchost.exe
Nom interne : sticvc
Description : *Fournit des services d'acquisition d'images pour les scanneurs et les appareils photo.*
Il dépend de : RPC

Dépendent de lui : aucun
Commentaire : Ce service peut être mis sur **"manuel"** compte tenu que les applications et le matériel (hardware) installés sur votre PC suffisent à assurer leur propre fonctionnalité.

Affichage des messages
Nom de l'exécutable : svchost.exe
Nom interne : Messenger
Description : *Envoie et reçoit les messages des services d'alertes entre les clients et les poste de travails. Ce service n'est pas lié à Windows Messenger. Si ce service est arrêté, les messages d'alertes ne seront pas transmis*
Il dépend de : RPC - Interface NETBIOS - Plug And Play - Station de travail
Dépendent de lui : aucun
Commentaire : Ce service doit être mis sur **"Désactivé"** pour des raisons de sécurité, ce service est maintenant désactivé d'office sur XP SP2

Aide et support
Nom de l'exécutable : svchost.exe
Nom interne : helpsvc
Description: *Permet à l'application Aide et support de fonctionner sur cet ordinateur*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : ce service peut être **"désactivé"** si vous connaissez bien votre système et pour des raisons de sécurité, bon nombre de virus peuvent s'inscrire dans les fichiers d'aide de Windows, sinon vous pouvez le laisser en **"manuel"** pour l'utiliser à l'occasion.

Aide de Windows Media Connect
Nom de l'exécutable : mswmcls.exe
Nom interne : helpsvc
Description:
Il dépend de : RPC
Dépendent de lui : Windows Media Connect (WMC)
Commentaire : pas de commentaire, je ne connais pas encore ce service en rapport avec le service "Windows Media Connect" (voir plus bas)

Appel de procédure distante (RPC)
Nom de l'exécutable : svchost.exe
Nom interne : RpcSs
Description : *Fournit le mappeur du point de sortie et divers services RPC*
Il dépend de : aucun
Dépendent de lui : **une grande partie des services qui utilisent "svchost.exe", soit 31 services à l'heure actuelle sur XP SP2**
Commentaire : **ce service doit être impérativement en "Automatique" pour assurer le bon fonctionnement de tous les services, si vous le**

"désactivez", vous ne pouvez plus revenir en arrière lors de votre session, la communication avec le réseau ne fonctionne plus, etc, et vous êtes obligé de redémarrer ce service à l'aide de la console de récupération ou éventuellement de ré-installer votre OS.
Ce service fait l'objet d'un article rien que pour lui.

Application système COM+

Nom de l'exécutable : dllhost.exe
Nom interne : COMSysApp
Description : *Gère la configuration et le suivi des composants de base COM+ (Component Object Model) .*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : Si le service est "arrêté", la plupart des composants de base COM+ ne fonctionneront pas correctement. Si ce service est "désactivé", les services qui en dépendent de manière explicite ne pourront pas démarrer. Vous pouvez laisser ce service sur **"automatique"** pour assurer un fonctionnement optimal de votre PC. Pour une sécurité renforcée, mettez le en **"manuel"**, ce service sert principalement sur des poste de travails utilisant des composants COM+, pour un particulier, ce service peut être éventuellement **"désactivé"** pour des raison de sécurité.

ASP.NET State Service

Nom de l'exécutable : aspnet_state.exe
Nom interne : aspnet_state
Description : *Assure la prise en charge des états de session out-of-process pour ASP.NET. En cas d'interruption de ce dernier service, les demandes out-of process ne sont pas traitées. En cas de désactivation du service, le démarrage de tout service qui dépend explicitement de ce service est impossible*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : Rien que le nom ne me donne pas confiance, cela me rappelle le compte ASP-NET qui s'installe sur la machine sans rien demander par l'intermédiaire de l'installation d'une imprimante comme HP par exemple, ce service est en mode **"manuel"** d'origine, il correspond à la mise en ligne de service Microsoft avec votre compte "Passport". Si vous n'utilisez pas ce service, il est préférable de le **"désactiver".** Ce service est uniquement "obligatoire" pour les développeurs qui créent des applications ASP.NET.

Assistance TCP/IP NetBIOS

Nom de l'exécutable : svchost.exe
Nom interne : LmHosts
Description : *Permet la prise en charge pour NetBIOS sur un service TCP/IP (NetBT) et la résolution des noms NetBIOS.*
Dépend de : Environnement de prise en charge réseau - NETBIOS sur TCP/IP - pilote du protocole TCP/IP - pilote IPSEC
Dépendent de lui : aucun
Commentaire : Si vous n'êtes pas en réseau local et pour des raisons de sécurité, vous pouvez **"désactiver"** ce service, si vous êtes en réseau local, laissez ce

service en **"automatique"**. Ce service ne gère que votre carte réseau, pas l'interface d'une connexion USB ADSL

Audio Windows
Nom de l'exécutable : svchost.exe
Nom interne : AudioSrv
Description : *Gère les périphériques audio pour les programmes basés sur Windows.*
Dépend de : RPC - Plug and Play
Dépendent de lui : aucun
Commentaire : **ce service doit être sur "automatique" sinon vous ne pourrez pas obtenir de son. Si vous souhaitez désactiver le son sur un PC, mettez ce service sur "manuel" ou "désactivé" (pratique en entreprise !).**

Avertissement
Nom de l'exécutable : svchost.exe
Nom interne : Alerter
Description : *Informe les utilisateurs et les ordinateurs sélectionnés des alertes administratives.*
Il dépend de : Station de travail
Dépendent de lui : aucun
Commentaire : vous pouvez mettre ce service en **"désactivé"** si vous ne souhaitez pas recevoir d'alerte.

Bluetooth Services
Nom de l'exécutable : btwdins.exe
Nom interne : btwdins
Description : aucune
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : ce service est présent sur des ordinateurs portables qui utilisent la technologie Bluetooth, si vous utilisez ce mode de connexion, laissez ce service en **"automatique"**

Carte à puce
Nom de l'exécutable : SCardSvr.exe
Nom interne : SCardSvr
Description : *Gère l'accès aux cartes à puce lues par cet ordinateur. Si ce service est arrêté, cet ordinateur ne pourra plus lire de cartes à puces. Si ce service est désactivé, tout service en dépendant explicitement ne démarrera pas.*
Il dépend de : Plug and Play
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en **"manuel"**; Si nous n'utilisez pas de lecteur de carte à puce (magasin, etc..) vous pouvez **"désactiver"** ce service

Carte de performance WMI
Nom de l'exécutable : wmiapsrv.exe
Nom interne : WmiApSrv
Description : *Fournit des informations concernant la bibliothèque de performance à partir des fournisseurs HiPerf WMI.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en **"manuel"** , sinon, vous pouvez le **"désactiver",** ce service sert principalement aux poste de travails pour l'administration à distance avec des outils dédiés.

Centre de sécurité
Nom de l'exécutable : svchost.exe
Nom interne : wscsvc
Description : *Analyse les paramètres de sécurité et les configurations du système.*
Il dépend de : RPC - Infrastructure de gestion Windows - Journal des évènements
Dépendent de lui : aucun
Commentaire : Présent uniquement sur le service Pack 2 de Windows XP. Ce service gère le firewall du SP2, les mises à jour, et vérifie que vous utilisez un antivirus. Laissez ce service en **"Automatique"** si vous utilisez le firewall du SP2 et les mises à jour automatiques. C'est lui qui lance des alertes de sécurité quand un programme est inconnu, etc...
; Si vous utilisez un autre firewall et un antivirus, il est préférable de **"désactiver"** ce service pour éviter les conflits.

Cliché instantané de volume
Nom de l'exécutable : vssvc.exe
Nom interne : VSS
Description : *Gère et implémente les clichés instantanés de volumes pour les sauvegardes et autres utilisations. Si ce service est arrêté, les clichés instantanés ne seront pas disponibles pour la sauvegarde et la sauvegarde échouera.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en **"manuel"**; Si vous n'utilisez pas le gestionnaire de sauvegarde Windows, vous pouvez **"désactiver"** ce service.

Client de suivi de lien distribué
Nom de l'exécutable : svchost.exe
Nom interne : TrkWks
Description : *Maintient les liens entre les fichiers NTFS au sein d'un ordinateur ou de plusieurs ordinateurs dans un domaine de réseau.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : Ce service ne sert que si vous partagez des fichiers NTFS entre plusieurs ordinateurs; Si vous n'êtes pas en réseau, ce service n'a pas d'intérêt, vous pouvez laisser ce service en mode **"désactivé"**

Client DHCP
Nom de l'exécutable : svchost.exe
Nom interne : Dhcp
Description : *Gère la configuration réseau en inscrivant et en mettant à jour les adresses IP et les noms DNS.*
Il dépend de : NETBIOS sur TCP/IP - Environnement de prise en charge du réseau AFD - Pilote de protocole TCP/IP - Pilote IPSEC
Dépendent de lui : aucun
Commentaire : si vous êtes en réseau et si vous avez configuré vos adresses IP en manuel, vous pouvez laisser ce service sur **"désactivé"** . Ce service n'a pas d'influence pour surfer sur Internet .
Attention, ce service est obligatoire pour les utilisateurs de la FreeBox ou des lignes dégroupées, ainsi que Numericable, dans ce cas, laissez ce service en **"automatique"**

Client DNS
Nom de l'exécutable : svchost.exe
Nom interne : Dnscache
Description : *Résout et met en cache les noms DNS pour cet ordinateur.*
Il dépend de : Pilote de protocole TCP/IP - Pilote IPSEC
Dépendent de lui : aucun
Commentaire : Ce service ne devrait être présent que dans un domaine. Ce service n'a pas d'influence pour surfer sur Internet , si vous utilisez un fichier HOSTS pour votre sécurité, vous devez laisser ce service en mode **"désactivé"**, sinon, vous aurez de la peine à surfer et vous verrez un processus svchost.exe à 99% dans votre gestionnaire des tâches.

Compatibilité avec le Changement rapide d'utilisateur
Nom de l'exécutable : svchost.exe
Nom interne : FastUserSwitchingCompatibity
Description : *Fournit un système de gestion à des applications qui nécessitent de l'Assistance dans un environnement d'utilisateurs multiples.*
Il dépend de : Service Terminal server - RPC
Dépendent de lui : aucun
Commentaire : si vous êtes le seul à utiliser votre PC, vous pouvez **"désactiver"** ce service, cela ne vous empêchera pas de démarrer votre session administrateur, il faudra simplement fermer votre session avant d'en ouvrir une autre. Si vous avez plusieurs sessions, mettez ce service en **"automatique"**. Il faut configurer cette fonctionnalité dans le "panneau de configuration -- >> comptes d'utilisateurs"

Configuration automatique sans fil
Nom de l'exécutable : svchost.exe
Nom interne : WZCSVC
Description : *Fournit la configuration automatique des cartes 802.11*
Il dépend de : RPC - NDIS mode utilisateur E/S protocole
Dépendent de lui : aucun

Commentaire : vous pouvez **"désactiver"** ce service si vous n'utilisez pas de connexion sans fil

Connexion secondaire

Nom de l'exécutable : svchost.exe
Nom interne : seclogon
Description : *Permet le démarrage des processus sous d'autres informations d'identification.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : Ce service est l'équivalent du service RunAs. Il permet d'exécuter des applications avec les privilèges d'un autre utilisateur en faisant un clic droit sur le raccourci de l'application puis "Exécuter en tant que". Cependant ce service apporte un risque de sécurité, mettre ce service sur **"manuel"** laisse ce défaut de sécurité actif, la seule solution étant de le mettre sur **"désactivé"**. A vous de voir si vous utilisez cette commande.

Connexions réseau

Nom de l'exécutable : svchost.exe
Nom interne : Netman
Description : *Prend en charge les objets dans le dossier Connexions réseau et accès à distance, dans lequel vous pouvez afficher à la fois les connexions du réseau local et les connexions à distance.*
Il dépend de : RPC
Dépendent de lui : Pare-feu Windows / partage de connexion internet
Commentaire : vous pouvez laisser ce service en **"manuel"**, sauf si vous utilisez le partage de connexion ou le pare-feu de Windows, dans ce cas ce service doit être en **"automatique"**

DDE réseau

Nom de l'exécutable : netdde.exe
Nom interne : NetDDE
Description : *Fournit le transport en réseau et la sécurité pour l'échange dynamique de données pour les programmes exécutés sur un même ordinateur ou des ordinateurs différents.*
Il dépend de : DSDM réseau
Dépendent de lui : Gestionnaire de l'album
Commentaire : Vous pouvez laisser ce service en mode **"manuel"** si vous êtes en réseau, si vous n'avez pas de réseau local, vous pouvez **"désactiver"** ce service.

Détection matériel noyau

Nom de l'exécutable : svchost.exe
Nom interne : ShellHWDetection
Description : *Fournit des notifications à des évènements matériel de lecture automatique*

Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : pendant longtemps, j'ai pensé que ce service était obligatoire, le mot "noyau" certainement. Finalement, j'ai fait plusieurs tests, et maintenant il est désactivé sur mon PC et XP fonctionne toujours correctement. Vous pouvez laisser ce service en mode **"manuel"**

Distributed Transaction Coordinator
Nom de l'exécutable : msdtc.exe
Nom interne : MSDTC
Description : *Coordonne les transactions qui comportent plusieurs gestionnaires de ressources, tels que des bases de données, des files d'attente de messages net des systèmes de fichiers.*
Il dépend de : RPC - Gestionnaire de comptes de sécurité
Dépendent de lui : aucun
Commentaire : si vous ne partagez pas de base de données ou si votre PC ne fait pas office de poste de travail, vous pouvez mettre ce service en mode **"manuel"** ou carrément le **"désactiver"** pour plus de sécurité.

DSDM DDE réseau
Nom de l'exécutable : netdde.exe
Nom interne : NetDDEdsdm
Description : *Gère l'échange dynamique de données partagées de réseau. Si ce service est arrêté, l'échange dynamique de données partagées de réseau ne sera plus disponible.*
Il dépend de : aucun
Dépendent de lui : DDE réseau - Gestionnaire de l'album
Commentaire : si vous n'avez pas de réseau, vous pouvez mettre ce service en mode **"désactivé"** sinon, si vous partagez des ressources, vous pouvez le mettre en mode **"manuel"**.

Emplacement protégé
Nom de l'exécutable : Lsass.exe
Nom interne : ProtectedStorage
Description : *Fournit un stockage protégé pour les données sensibles, telles que les clés privées, afin d'empêcher l'accès par des services, des processus ou des utilisateurs non autorisés.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : si votre système de fichier est en NTFS et si vous cryptez vos données il est préférable de laisser ce service en mode **"automatique"**. Sinon, vous pouvez le laisser en mode **"manuel"**

Explorateur d'ordinateur
Nom de l'exécutable : svchost.exe
Nom interne : Browser
Description : *Tient à jour une liste des ordinateurs présents sur le réseau et fournit cette liste aux ordinateurs désignés comme navigateurs. Si ce service est*

arrêté, la liste ne sera pas mise ou tenue à jour.
Il dépend de : Serveur - Station de travail
Dépendent de lui : aucun
Commentaire : si vous n'avez pas de réseau domestique, vous pouvez laisser ce service en mode **"manuel"**, si vous êtes en réseau local, laissez le en mode **"automatique"**. Si vous n'avez aucun réseau local et pour préserver la sécurité, vous pouvez **"désactiver"** ce service.

Extensions du pilote WMI
Nom de l'exécutable : svchost.exe
Nom interne : Wmi
Description : *Fournit des informations de gestion du système vers et à partir des pilotes.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : vous pouvez mettre ce service en mode **"manuel"**, ce service **WMI** (Windows Management Instrumentation) est prévu pour gérer des évènements dans un réseau d'entreprise, si vous n'êtes pas dans cas là, vous pouvez **"désactiver"** ce service.

FAX
Nom de l'exécutable : fxssvc.exe
Nom interne : ?
Description : *Fournit des informations de gestion du système vers et à partir des pilotes.*
Il dépend de : RPC, Plug-and-play, Spouleur d'impression, Téléphonie
Dépendent de lui : aucun
Commentaire : vous devez laisser ce service en mode **"automatique"** pour utiliser votre logiciel de FAX, si vous n'utilisez pas de fax, vous pouvez le **"désactiver"**

Fournisseur de la prise en charge de sécurité LM NT
Nom de l'exécutable : lsass.exe
Nom interne : NtLmSsp
Description : *Assure la sécurité des programmes RPC (appels de procédure distante) qui utilisent des transports autres que des canaux nommés.*
Il dépend de : aucun
Dépendent de lui : Telnet
Commentaire : vous pouvez mettre ce service en mode **"manuel"**, si vous n'utilisez pas Telnet, et pour des raisons de sécurité, vous pouvez **"désactiver"** ce service

Gestion d'applications

Nom de l'exécutable : svchost.exe
Nom interne : AppMgmt
Description : *Fournit des services d'installation de logiciels tels que Attribuer, Publier et Supprimer.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : ce service sert principalement dans un réseau afin d'installer des logiciels par cet intermédiaire soit sur d'autres PCs, ce service est utile pour 2000 Server, 2003 Server, si vous n'êtes pas en réseau, vous pouvez **"désactiver"** ce service, il n'a aucune incidence sur l'installation d'un logiciel traditionnel sur votre système.

Gestionnaire de comptes de sécurité
Nom de l'exécutable : Lsass.exe
Nom interne : SamSs
Description : *Stocke les informations de sécurité pour les comptes d'utilisateurs locaux.*
Il dépend de : RPC
Dépendent de lui : Distributed Transaction Coordination
Commentaire : Si vous avez modifié des paramètres de sécurité avec **"gpedit.msc"**, laissez ce service en mode **"automatique"**, sinon, vous pouvez le laisser en mode **"manuel"** , si vous utilisez uniquement XP Home, compte-tenu que "gpedit" n'est pas présent, vous pouvez **"désactiver"** ce service.

Gestionnaire de connexion automatique d'accès distant
Nom de l'exécutable : svchost.exe
Nom interne : RasAuto
Description : *Crée une connexion vers un réseau distant à chaque fois qu'un programme référence un nom ou une adresse DNS ou NetBIOS distant.*
Il dépend de : Gestionnaire de connexion d'accès distant - Téléphonie - RPC - Plug and Play
Dépendent de lui : aucun
Commentaire : Si vous utilisez une connexion Internet par modem vous pouvez laisser ce service en mode **"automatique"**; Si vous utilisez un routeur, vous pouvez le laisser en mode **"manuel"**.

Gestionnaire de connexions d'accès distant
Nom de l'exécutable : svchost.exe
Nom interne : RasMan
Description : *Crée une connexion réseau.*
Il dépend de : Téléphonie - RPC - Plug and Play
Dépendent de lui : Gestionnaire de connexion automatique d'accès distant
Commentaire : si vous utilisez une connexion réseau local ou Internet par USB ADSL ou que vous partagez votre connexion, laissez ce service en mode **"automatique"**, si vous passez par un routeur, vous pouvez le mettre en **"manuel"**.

Gestionnaire de disque logique
Nom de l'exécutable : svchost.exe
Nom interne : dmserver
Description : *Détecte et analyse de nouveaux lecteurs de disque dur et envoie les informations de volume de disque au service gestionnaire administratif de disque logique pour la configuration. Si ce service est arrêté, l'état des disques dynamiques et les informations de configuration peuvent devenir obsolètes.*
Il dépend de : RPC - Plug and Play
Dépendent de lui : Service d'administration de disque logique
Commentaire : Il est préférable de laisser ce service en **"automatique"** si vous utilisez des clés USB ou des disques durs USB.

Gestionnaire de l'Album
Nom de l'exécutable : clipsrv.exe
Nom interne : ClipSrv
Description : *Active le Gestionnaire de l'Album afin de stocker les informations et les partager avec des ordinateurs à distance. Si le service est arrêté, le Gestionnaire de l'Album ne pourra pas partager les informations avec des ordinateurs à distance.*
Il dépend de : DDE réseau - DSDM DDE réseau
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"manuel"**, pour des raisons de sécurité et si vous ne partagez rien avec d'autres ordinateurs à distance ou en réseau local, vous pouvez **"désactiver"** ce service. Le fait de désactiver ce service n'influence pas le partage de dossiers/fichiers sur votre réseau local.

Gestionnaire de session d'aide sur le Bureau à distance
Nom de l'exécutable : sessmgr.exe
Nom interne : RDSessMgr
Description : *Gère et contrôle l'assistance à distance. Si ce service est arrêté, l'assistance à distance n'est pas disponible.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : à moins de vous faire dépanner par un collègue, pour des raisons de sécurité vous pouvez **"désactiver"** ce service, sinon, laissez le en mode **"manuel"**

Gestionnaire de téléchargement
Nom de l'exécutable : svchost.exe
Nom interne : uploadmgr
Description : *Gère les transferts de fichiers synchrones et asynchrones entre les clients et les poste de travails sur le réseau. Si ce service est arrêté, les transferts de fichiers synchrones et asynchrones entre les clients et les poste de travails ne seront pas possibles.*
Il dépend de : aucun

Dépendent de lui : aucun
Commentaire : vous pouvez mettre ce service en mode **"manuel"** ou **"désactiver"** ce service si vous n'êtes pas en réseau ou que votre PC ne fait pas office de poste de travail de fichiers.

Horloge Windows

Nom de l'exécutable : svchost.exe
Nom interne : W32Time
Description : *Conserve la synchronisation de la date et de l'heure sur tous les clients et poste de travails sur le réseau. Si ce service est arrêté, la synchronisation de la date et de l'heure sera indisponible.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : hormis l'envie de toujours vouloir être à l'heure d'Internet, vous pouvez **"désactiver"** ce service, d'autant plus que ce service ne se synchronise qu'une fois par semaine.

Hôte de périphérique universel Plug-and-Play

Nom de l'exécutable : svchost.exe
Nom interne : upnphost
Description : *Offre la prise en charge des périphériques hôtes universels Plug-and-Play.*
Il dépend de : HTTP -Service de découverte SSDP
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"manuel"**; Pour des raisons de sécurité vous pouvez **"désactiver"** ce service si vous n'êtes pas en réseau local.

HTTP SSL

Nom de l'exécutable : svchost.exe
Nom Interne : HTTPFilter
Description : *Ce service implémente le protocole sécurisé HTTPS (Secure HyperText Transfer Protocol) pour le service HTTP, en utilisant la couche SSL (Secure Socket Layer). Si ce service est désactivé, tous les services qui en dépendent de manière explicite échoueront au démarrage.*
Il dépend de : HTTP
Dépendent de lui : aucun
Commentaire : Nouveau service du SP2 XP. Ce service n'est pas en relation avec votre navigateur internet, si vous **"désactivez"** ce service, il n'y aura pas de répercussion sur la visite des sites sécurisés HTTPS (banques, achat en ligne, etc.).

Infrastructure de gestion Windows

Nom de l'exécutable : svchost.exe
Nom interne : winmgmt
Description : *Fournit une interface commune et un modèle objet pour accéder aux informations de gestion du système d'exploitation, des périphériques, des applications et des services. Si ce service est arrêté, la plupart des logiciels sur*

base Windows ne fonctionneront pas correctement.
Il dépend de : RPC - journal des évènements
Dépendent de lui : Centre de sécurité - pare-feu de connexion/partage de connexion
Commentaire : **ce service est obligatoire, vous devez laisser ce service en mode "automatique" , si vous désactivez ce service, vous n'aurez plus accès à aucune boîte de dialogue.**

Journal des événements
Nom de l'exécutable : services.exe
Nom interne : Eventlog
Description : *Active les messages d'événements émis par les programmes fonctionnant sous Windows et les composants devant être affichés dans l'observateur d'événements. Ce service ne peut être arrêté.*
Il dépend de : aucun
Dépendent de lui : Infrastructure de gestion Windows - centre de sécurité - pare-feu Windows/partage de connexion
Commentaire : **ce service est maintenant obligatoire sur XP SP2, laissez ce service en mode "automatique".**

Journaux et alertes de performance
Nom de l'exécutable : smlogsvc.exe
Nom interne : SysmonLog
Description : *Collecte les données de performances des ordinateurs locaux ou distants basés sur des paramètres planifiés pré-configurés, puis écrit les données dans un journal ou déclenche une alerte.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : ce service n'a aucune dépendance, pour des raisons de sécurité, mettez ce service en mode **"désactivé"**, sinon vous pouvez le laisser en mode **"manuel"**

Lanceur de processus poste de travail DCOM
Nom de l'exécutable : svchost.exe
Nom interne : DcomLaunch
Description : *Fournit la fonctionnalité de lancement des services DCOM.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : ce service devrait rester en mode **"automatique"**, c'est un nouveau service du SP2 - XP, qui prend en charge une partie du service "Appel de procédure distante RPC" afin de le sécuriser sur le SP2, si vous désactivez ce service, certaines commandes ne fonctionneront pas comme "tasklist" ou simplement la visualisation des dépendances des services par exemple.

Localisateur d'appels de procédure distante (RPC)
Nom de l'exécutable : locator.exe
Nom interne : RpcLocator
Description : *Gère la base de données du service de nom RPC.*

Il dépend de : Station de travail
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"manuel"** ; Si vous souhaitez plus de sécurité, vous pouvez **"désactiver"** ce service

Machine Debug Manager
Nom de l'exécutable : mdm.exe
Nom interne : MDM
Description : *Débogage de programme avec Visual Studio Debuggers*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : à moins d'être programmeur, vous pouvez **"désactiver"** ce service, cela évite les alertes des bugs des logiciels Windows

Mises à jour automatiques
Nom de l'exécutable : svchost.exe
Nom interne : wuauserv
Description : *Active le téléchargement et l'installation de mises à jour Windows critiques. Si le service est désactivé, le système d'exploitation peut être mis à jour manuellement sur le site Web de Windows Update.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : laissez ce service en **"automatique"** si vous souhaitez laisser faire Windows à votre place ou si le service "centre de sécurité" est activé; Si vous **"désactivez"** ce service, cela ne vous empêche pas de faire des mises à jour sur le site de Microsoft manuellement.

Moniteur infrarouge
Nom de l'exécutable : svchost.exe
Nom interne : Irmon
Description : *Prend en charge les périphériques infrarouge installés sur l'ordinateur et détecte les autres périphériques qui sont dans la même gamme*
Il dépend de : RPC, Protocol IrDa, Terminal Server,
Dépendent de lui : aucun
Commentaire : ce service n'est présent que sur les portables apparemment, laissez ce service en **"automatique"** uniquement si vous utilisez cette fonctionnalité, sinon, laissez-le en manuel

MS Software Shadow Copy Provider
Nom de l'exécutable : dllhost.exe
Nom interne : SwPrv
Description : *Gère les copies logicielles de clichés instantanés de volumes créés par le service de cliché instantané de volumes. Si ce service est arrêté, les copies logicielles de clichés instantanés ne peuvent pas être gérées.*
Il dépend de : RPC
Dépendent de lui : aucun

Commentaire : ce service est utile si vous êtes connecté à un poste de travail Windows.net ou si vous utilisez l'utilitaire de sauvegarde, et encore !!! Sinon mettez ce service en mode **"désactivé"** pour des raisons de sécurité.

NLA (Network Location Awareness)

Nom de l'exécutable : svchost.exe
Nom interne : Nla
Description : *Recueille et stocke les informations de configuration et d'emplacement réseau, et notifie les applications quand ces informations changent.*
Il dépend de : Environnement de prise en charge de réseau AFD - Pilote de protocole TCP/IP - Pilote IPSEC
Dépendent de lui : aucun
Commentaire : laissez ce service en mode **"manuel"** si vous êtes en réseau local, sinon, vous pouvez **"désactiver"** ce service.

Notification d'événement système

Nom de l'exécutable : svchost.exe
Nom interne : SENS
Description : *Scrute les événements système tels que les ouvertures de session Windows et les événements concernant le réseau et l'alimentation. Avertit les abonnés du système d'événements COM+ de ces événements.*
Il dépend de : Système d'évènements de COM + - RPC
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"automatique"** si vous aimez bien regarder le journal des évènements ou si vous comprennez parfaitement les erreurs et le code donné, si vous préférez la sécurité, vous pouvez **"désactiver"** ce service

Numéro de série du média portable

Nom de l'exécutable : svchost.exe
Nom interne : WmdmPmSp
Description : *Lit le numéro de série du baladeur numérique connecté à votre ordinateur*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"manuel"**, si vous n'utilisez aucun lecteur média portable, vous pouvez **"désactiver"** ce service

Onduleur

Nom de l'exécutable : ups.exe
Nom interne : UPS
Description : *Gère un onduleur connecté à l'ordinateur.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : si vous ne possédez pas d'onduleur, vous pouvez **"désactiver"** ce service , si vous utilisez un onduleur, vous devez laisser ce service en mode **"automatique"**, sinon, l'onduleur ne prendra pas le relais en cas de panne de

courant, n'oubliez pas de faire reconnaître votre onduleur dans la "gestion d'alimentation" qui se trouve dans le "panneau de configuration".

Ouverture de session réseau
Nom de l'exécutable : lsass.exe
Nom interne : Netlogon
Description : *Prend en charge l'authentification directe des événements d'ouverture de session du compte pour les ordinateurs dans un domaine.*
Il dépend de : Station de travail
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"manuel"** sauf si vous êtes sur un domaine où vous devez le laisser en **"automatique".** Si vous n'avez pas de réseau du tout, vous pouvez **"désactiver"** le service.

Pare-feu de connexion Internet (ICF) / Partage de connexion Internet (ICS)
ou Pare-feu de connexion
Nom de l'exécutable : svchost.exe
Nom interne : SharedAccess
Description : *Assure la traduction d'adresses de réseau, l'adressage, les services de résolution de noms et/ou les services de prévention d'intrusion pour un réseau de petite entreprise ou un réseau domestique.*
Il dépend de : Connexion réseau - RPC - Infrastructure de gestion Windows - Journal des évènements
Dépendent de lui : aucun
Commentaire : si votre PC partage une connexion internet, vous devez laisser ce service en mode **"automatique"**, si vous utilisez le pare-feu de connexion, vous devez laisser ce service en mode **"automatique"**, sinon, vous pouvez le mettre en **"manuel"** ou carrément le **"désactiver"** si vous utilisez un autre firewall et que vous ne partagez pas votre connexion internet.

Pare-feu de connexion IPV6
Nom de l'exécutable : svchost.exe
Nom interne : Ip6FwHlp
Description : *Fournit un service de prévention d'intrusion pour un réseau domestique ou de petite entreprise.*
Il dépend de : connexion réseau et NLA Network Location Awareness
Dépendent de lui : aucun
Commentaire : Vous pouvez **"désactiver"** ce service pour l'instant, car ce protocole n'est pas encore implémenté par les FAI à ce jour.

Partage de Bureau à distance NetMeeting
Nom de l'exécutable : mnmsrvc.exe
Nom interne : mnmsrvc
Description : *Permet aux personnes autorisées d'accéder à votre Bureau Windows en utilisant NetMeeting.*

Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : pour des raisons de sécurité, vous pouvez **"désactiver"** ce service si vous ne donnez pas l'autorisation de venir sur votre PC à l'aide de ce logiciel.

Planificateur de tâches

Nom de l'exécutable : svchost.exe
Nom interne : Schedule
Description : *Permet à un utilisateur de configurer et de planifier des tâches automatisées sur cet ordinateur. Si ce service est arrêté, ces tâches ne seront pas exécutées à l'heure prévue.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : si vous avez l'habitude de gérer vos tâches régulièrement (nettoyage, défragmentation, etc..) vous pouvez **"désactiver"** ce service, sinon, laissez le sur **"automatique"**.

Plug-and-Play

Nom de l'exécutable : services.exe
Nom interne : PlugPlay
Description : *Permet à l'ordinateur de reconnaître et d'adapter les modifications matérielles avec peu ou pas du tout d'intervention de l'utilisateur. Arrêter ou désactiver ce service provoque une instabilité du système.*
Il dépend de : aucun
Dépendent de lui : **Affichage des messages - Audio Windows - Carte à puce - Gestionnaire du disque logique - Service d'administration du gestionnaire de disque logique - Téléphonie - Gestionnaire de connexion automatique d'accès distant - Gestionnaire de connexion d'accès distant**
Commentaire : **ce service est obligatoire, il faut laisser ce service en mode "automatique" car beaucoup de services dépendent de lui.**

QoS RSVP

Nom de l'exécutable : rsvp.exe
Nom interne : RSVP
Description : *Fournit la signalisation de réseau et la fonctionnalité d'installation du contrôle de trafic local pour les programmes reconnaissant QoS et les applets de contrôle.*
Il dépend de : RPC - Environnement de prise en charge du réseau AFD - Pilote de protocole tCP/IP - Pilote IPSEC
Dépendent de lui : aucun
Commentaire : vous pouvez laisser ce service en mode **"désactivé"**

Routage et accès distant

Nom de l'exécutable : svchost.exe
Nom interne : RemoteAccess

Description : *Offre aux entreprises des services de routage dans les environnements de réseau local ou étendu.*
Il dépend de : RPC - NETBIOS GROUPE - Interface NETBIOS
Dépendent de lui : aucun
Commentaire : pour des questions de sécurité, laissez ce service **"désactivé"**, sauf si vous utilisez le partage de connexion ICS, laissez ce service sur **"automatique"**

Serveur
Nom de l'exécutable : svchost.exe
Nom interne : lanmanserver
Description : *Prend en charge le partage de fichiers, d'impression et des canaux nommés via le réseau pour cet ordinateur. Si ce service est arrêté, ces fonctions ne seront pas disponibles. Si ce service est désactivé, les services qui en dépendent ne pourront pas démarrer.*
Il dépend de : aucun
Dépendent de lui : Explorateur d'ordinateur
Commentaire : vous pouvez **"désactiver"** ce service, sauf si vous partagez des fichiers dans un réseau local ou vous devez le mettre en **"automatique"** .

Service COM de gravage de CD IMAPI
Nom de l'exécutable : imapi.exe
Nom interne : ImapiService
Description : *Gère le gravage des CD via l'interface série IMAPI (Image Mastering Applications Programming Interface). Si ce service est arrêté, cet ordinateur ne pourra plus enregistrer de CD.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : si vous utilisez un autre logiciel de gravure tel que Nero, CDMate, Easy CD,etc.., vous devez **"désactiver"** ce service pour éviter les conflits, si vous désirez graver vos CD avec le logiciel de Windows, laissez le en mode **"automatique"**.

Service d'administration du Gestionnaire de disque logique
Nom de l'exécutable : dmadmin.exe
Nom interne : dmadmin
Description : *Configure les lecteurs de disque dur et les volumes. Le service ne s'exécute que pour les processus de configurations puis s'arrête.*
Il dépend de : RPC - Gestionnaire du disque logique - Plug and Play
Dépendent de lui : aucun
Commentaire : vous devez laisser ce service en mode **"manuel"**

Service d'approvisionnement réseau
Nom de l'exécutable : svchost.exe
Nom interne : xmlprov
Description : *Gère les fichiers de configuration XML en fonction du domaine pour l'approvisionnement réseau automatique.*
Il dépend de : RPC

Dépendent de lui : aucun
Commentaire : Nouveau service présent sur le pack SP2 d' XP, si vous n'êtes pas dans un domaine, vous pouvez **"désactiver"** ce service

Service de découvertes SSDP
Nom de l'exécutable : svchost.exe
Nom interne : SSDPSRV
Description : *Active la découverte de périphériques Plug and Play universels sur votre réseau domestique.*
Il dépend de : HTTP
Dépendent de lui : Hôte de périphérique universel Plug and Play
Commentaire : si votre PC est connecté à des périphériques UPnP, laissez ce service en **"automatique"**, sinon, laissez le en mode **"manuel"**. Le service "Hôte de périphérique universel Plug-and-Play" doit être identique avec ce service. Pour des raison de sécurité vous pouvez **"désactiver"** ces 2 services même si vous êtes en réseau.

Service de numéro de série du lecteur multimedia portable
Nom de l'exécutable : svchost.exe
Nom interne : WmdmPmSN
Description : *Extrait le numéro de série d'un lecteur multimedia connecté à cet ordinateur. Si ce service est interrompu, le contenu protégé risque de ne pas être téléchargé sur le périphérique*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : service présent sur les portables, à confirmer

Service de la passerelle de la couche Application
Nom de l'exécutable : alg.exe
Nom interne : ALG
Description : *Fournit la prise en charge des plugins de protocoles tiers pour le partage de connexion Internet et le pare-feu Internet.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : si vous utilisez le partage de connexion ou le pare-feu Windows, vous devez le mettre en **"automatique"**, sinon laissez ce service en mode **"manuel"**.

Service de rapport d'erreurs
Nom de l'exécutable : svchost.exe
Nom interne : ERSvc
Description : *Active le rapport d'erreurs pour les services et les applications s'exécutant sur des environnements non standard.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : vous pouvez **"désactiver"** ce service, sauf si vous souhaitez

envoyer des rapports d'erreur à Microsoft.

Service de restauration système
Nom de l'exécutable : svchost.exe
Nom interne : srservice
Description : *Effectue des opérations de restauration du système. Pour arrêter ce service, désactivez Restauration du système dans l'onglet Restauration du système des propriétés du Poste de travail.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : Si vous ne souhaitez pas faire de restauration système, vous pouvez laisser ce service en mode **"désactivé"**, sinon, si vous utilisez ce service, laissez-le en mode **"automatique"**

Service de transfert intelligent en arrière-plan
Nom de l'exécutable : svchost.exe
Nom interne : BITS
Description : *Utilise la bande passante réseau inactive pour transférer des données.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : cette fonctionnalité est peu utilisée, vous pouvez laisser ce service en mode **"manuel"**, si vous faites beaucoup de transferts de données dans un réseau local, il est préférable de laisser ce service en mode **"automatique". Attention, ce service doit être démarré pour les mises à jour Windows Update.**

Service d'indexation
Nom de l'exécutable : cisvc.exe
Nom interne : cisvc
Description : *Construit un index des contenus et des propriétés des fichiers sur les ordinateurs locaux et distants ; fournit un accès rapide aux fichiers par le biais d'un langage d'interrogation flexible.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : si vous ne souhaitez pas faire un catalogue de vos données, vous pouvez **"désactiver"** ce service; Sinon, vous pouvez construire votre catalogue dans "Outils d'administration => gestion de l'ordinateur => services et applications => service d'indexation" dans ce cas, vous devez laisser le service en mode **"automatique"**

Services de cryptographie
Nom de l'exécutable : svchost.exe
Nom interne : CryptSvc
Description : *Fournit trois services de gestion : le service de base de données de catalogue, qui confirme la signature des fichiers Windows; le service de racine protégée, qui ajoute et supprime des certificats d'autorité de certification de*

racine approuvés et le service Clé, qui fournit une aide dans l'inscription de cet ordinateur pour les certificats.
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : en principe, vous devez laisser ce service en mode **"automatique"** car il est utilisé pour la mise à jour et l'installation des produits Microsoft et vérifie la validité des packs d'installation. Il sert également à la gestion de cryptage des fichier EFS. Si vous n'utilisez pas la mise à jour automatique, ou si vous ne cryptez pas vos dossiers/fichiers, vous pouvez mettre ce service en mode **"manuel"**

Services IPSEC
Nom de l'exécutable : lsass.exe
Nom interne : PolicyAgent
Description : *Gère la stratégie de sécurité IP et démarre les pilotes de gestion de sécurité IP et ISAKMP/Oakley (IKE).*
Il dépend de : RPC -Pilote de protocole TCP/IP - Pilote IPSEC
Dépendent de lui : aucun
Commentaire : vous pouvez mettre ce service en mode **"manuel"**, parce que de nombreux fournisseurs d'accès Internet n'utilisent pas encore cette fonction.

Services Terminal Server
Nom de l'exécutable : svchost.exe
Nom interne : TermService
Description : *Permet à plusieurs utilisateurs de se connecter en même temps à un ordinateur, tout en affichant les bureaux et les applications sur les ordinateurs distants. Contient les fonctions sous-jacentes de Bureau à distance (y compris le Bureau à distance pour les administrateurs), le Changement rapide d'utilisateur, l'Assistance à distance et le service Terminal Server.*
Il dépend de : RPC
Dépendent de lui : Compatibilité avec le changement rapide d'utilisateur
Commentaire : si vous utilisez le changement rapide d'utilisateur, vous devez laisser ce service en mode **"automatique"**, sinon si vous n'utilisez qu'une seule session et pour plus de sécurité et que n'êtes pas en réseau local, vous pouvez **"désactiver"** ce service.

Spouleur d'impression
Nom de l'exécutable : spoolsv.exe
Nom interne : Spooler
Description : *Charge des fichiers en mémoire pour une impression ultérieure.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : si vous utilisez régulièrement une imprimante, laissez ce service en mode **"automatique"**, si vous utilisez très peu l'imprimante voire pas du tout, mettez-le en mode **"manuel"**, dans ce cas, n'oubliez pas de redémarrer le service avant de lancer une impression.

Station de travail

Nom de l'exécutable : svchost.exe
Nom interne : lanmanworkstation
Description : *Crée et maintient des connexions de réseau client à des poste de travails distants. Si ce service est arrêté, ces connexions ne seront pas disponibles.*
Il dépend de : aucun
Dépendent de lui : Affichage des messages - Avertissement - Explorateur d'ordinateur - Localisateur d'appels de procédure distante RPC - Ouverture de session réseau
Commentaire: **ce service est obligatoire, laissez-le en mode" automatique".**

Stockage amovible

Nom de l'exécutable : svchost.exe
Nom interne : NtmsSvc
Description : *Gère les médias amovible, les lecteurs et les bibliothèques.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : si vous utilisez un lecteur type Ioméga par exemple, laisser ce service en mode **"automatique"**, ou sinon, laissez le en mode **"manuel"**

Système d'événements de COM+

Nom de l'exécutable : svchost.exe
Nom interne : EventSystem
Description : *Prend en charge le service de notification d'événements système (SENS, System Event Notification Service), qui fournit une distribution automatique d'événements aux composants COM (Component Object Model) abonnés. Si le service est arrêté, SENS sera fermé et ne pourra fournir des informations d'ouverture et de fermeture de session. Si ce service est désactivé, le démarrage de tout service qui en dépend explicitement échouera.*
Il dépend de : RPC
Dépendent de lui : Notification d'évènement système
Commentaire : si vous êtes le seul à utiliser le PC, vous pouvez mettre ce service en mode **"manuel"** , sinon laissez ce service en mode **"automatique"**.

Téléphonie

Nom de l'exécutable : svchost.exe
Nom interne : TapiSrv
Description : *Fournit la prise en charge des API de téléphonie (TAPI) pour les programmes contrôlant les périphériques de téléphonie, les connexions vocales basées sur le protocole IP, sur l'ordinateur local, via le réseau local, sur le poste de travail où ce service fonctionne également.*
Il dépend de : RPC - Plug and Play
Dépendent de lui : Gestionnaire de connexion automatique d'accès distant - Gestionnaire de connexion d'accès distant
Commentaire : laissez ce service en mode **"automatique"** si vous utilisez un modem interne, un fax ou un modem USB, si vous utilisez un routeur pour vous connecter, et si vous n'utilisez pas la fonction FAX, vous pouvez **"désactiver"** ce service

Telnet
Nom de l'exécutable : tlntsvr.exe
Nom interne : TlntSvr
Description : *Permet à un utilisateur distant de se connecter au système et d'exécuter des programmes, et prend en charge divers clients Telnet TCP/IP dont les ordinateurs sous UNIX et sous Windows. Si ce service est arrêté, l'utilisateur peut ne plus avoir accès à distance aux programmes. Si ce service est désactivé, les services qui en dépendent explicitement ne pourront pas démarrer.*
Il dépend de : RPC - Fournisseur de la prise en charge de réseau AFD - Pilote de protocole TCP/IP - Pilote IPSEC
Dépendent de lui : aucun
Commentaire : pour des raisons de sécurité, il est préférable de **"désactiver"** ce service

Thèmes
Nom de l'exécutable : svchost.exe
Nom interne : Themes
Description : *Fournit un système de gestion de thème de l'expérience utilisateur.*
Il dépend de : aucun
Dépendent de lui : aucun
Commentaire : laissez ce service en mode **"automatique"** si vous utilisez les thèmes de Windows ou si vous utilisez d'autres thèmes que ceux de Windows, le fait de **"désactiver"** ce service remet par défaut le thème en 2D de Windows 2000, c'est juste une affaire de goût.

WebClient
Nom de l'exécutable : svchost.exe
Nom interne : WebClient
Description : *Permet à un programme fonctionnant sous Windows de créer, modifier et accéder à des fichiers Internet. Si ce service est arrêté, Ces fonctions ne seront pas disponibles.*
Il dépend de : Redirecteur de client WebDav
Dépendent de lui : aucun
Commentaire : pour des raisons de sécurité, il est préférable de **"désactiver"** ce service

Windows Installer
Nom de l'exécutable : msiexec.exe
Nom interne : MSIServer
Description : *Installe, répare et supprime des logiciels selon les instructions contenues dans les fichiers MSI.*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : laissez ce service en mode **"manuel"**, cela vous permet d'installer/désinstaller des programmes fonctionnant avec les fichiers .MSI, si vous souhaitez qu'aucun utilisateur (les enfants, par exemple) n'installe rien de chez Microsoft ou certains programmes demandant cette technologie, vous pouvez **"désactiver"** ce service.

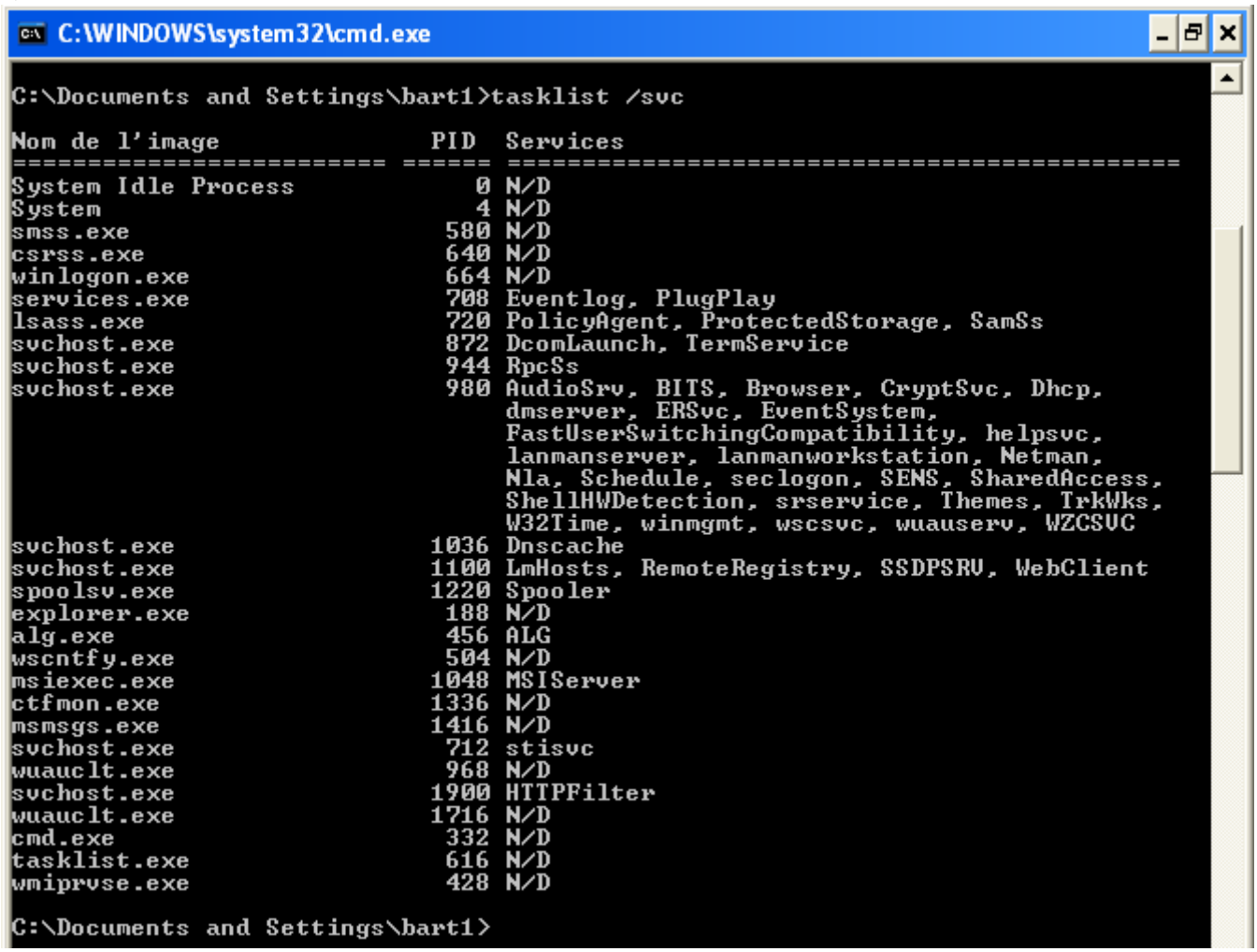
Windows Media Connect (WMC)
Nom de l'exécutable : mswmccds.exe
Nom interne : ?
Description : *permet très simplement à n'importe quel client IP ou pas équipé de la fonction Microsoft* ***PlayForSure*** *de lire le contenu multimédia de votre PC à coup sûr, sans bugs ni incompatibilités.*
Il dépend de : RPC, Aide de Windows Mesia Connect (WMC), Hôte de périphérique universel Plug-and-Play
Dépendent de lui : aucun
Commentaire : Ce service permet de lire le contenu de vos fichiers multimédia à partir de n'importe où, une sorte de P2P à la sauce Microsoft, pas de commentaire personnel, il n'est pas présent sur mon PC

Windows User Mode Driver Framework
Nom de l'exécutable : wdfmgr.exe
Nom interne : UMWdf
Description : *Active les pilotes en mode utilisateur Windows*
Il dépend de : RPC
Dépendent de lui : aucun
Commentaire : Le "Framework .Net" en lui-même n'est rien de plus qu'une machine virtuelle... un peu comme Java, une "CLR" (Common Language Runtime), il est possible que certains logiciels aient besoin de ce service si un de leurs outils a été compilé avec ce type de langage. Mettre ce service sur **"manuel"**

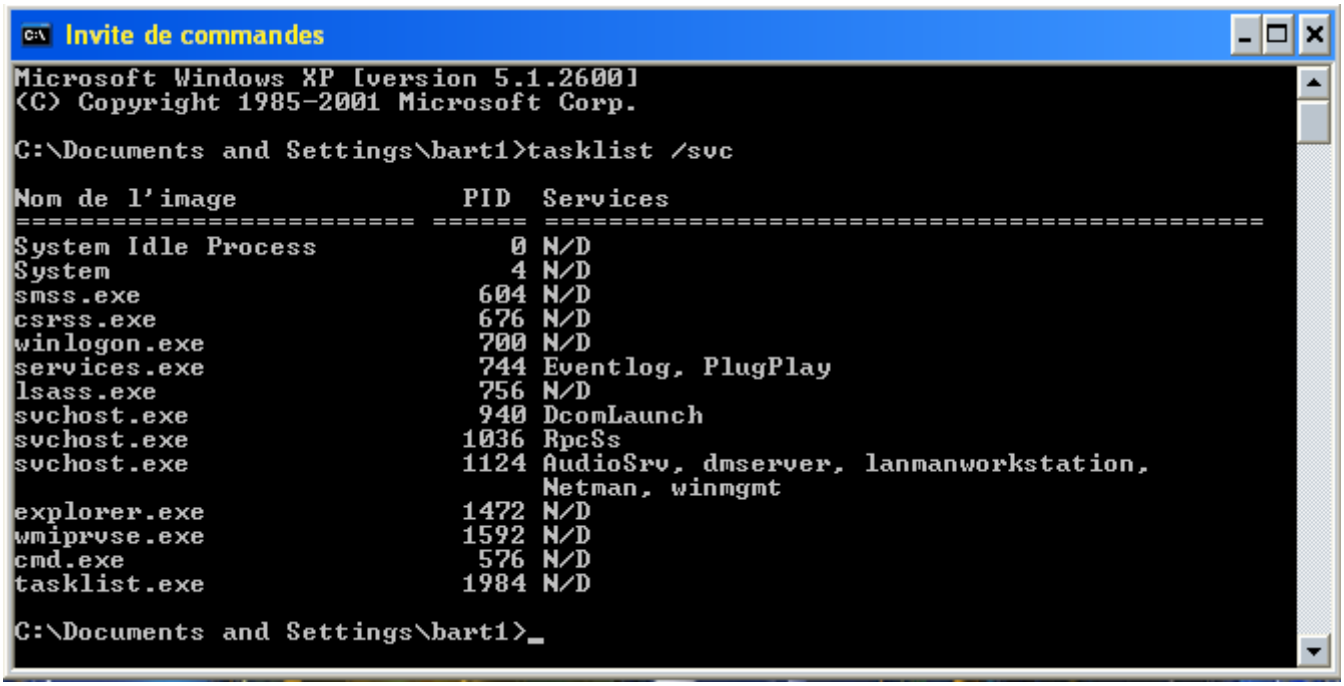
Nous avons fait le tour d'horizon de tous ces services, j'espère que cet article vous permettra de faire un choix judicieux du bien fondé de tel ou tel service démarré sur votre système.

Pour vous donner une idée des résultats possibles, voici 2 copies d'écran : - Un fait avant l'optimisation sur XP SP2 d'origine par défaut, soit 51 services démarrés sur 81 (image ci-dessous)

<



- L'autre fait après optimisation complète des services, sur le même ordinateur, il ne reste plus que 12 services démarrés, ceux qui sont obligatoires pour le bon fonctionnement de votre machine, il ne s'agit en aucun cas de vous faire arriver à cet extrême, ce n'est pas l'objectif, mais avec ces 12 services, Windows fonctionne parfaitement, je peux me connecter au réseau, aller sur internet ou voir les partages de connexion du réseau local, écouter de la musique ou lire un DVD, écrire un courrier, faire des copies d'écrans, etc.. (image ci-dessous)



Avant de vous lancer dans l'aventure d'arrêt de services, je vous recommande de faire un point sur l'utilité ou non du dit service en rapport avec votre façon d'utiliser votre OS et de votre environnement,

3. GESTION DES PROCESSUS

3.1. Définition d'un processus

Un **processus** (en anglais, *process*), en informatique, est défini par :

- un ensemble d'instructions à exécuter (un programme) ;
- un espace mémoire pour les données de travail ;
- éventuellement, d'autres ressources, comme des descripteurs de fichiers, des ports réseau, etc.

Un ordinateur équipé d'un système d'exploitation à temps partagé est capable d'exécuter plusieurs processus de façon « quasi-simultanée ». S'il y a plusieurs processeurs, l'exécution des processus est distribuée de façon équitable sur ces processeurs.

Le sens de processus doit être pris comme quelque chose qui prend du temps, donc qui a un début et (parfois) une fin. Un processus peut-être démarré par un utilisateur par l'intermédiaire d'un périphérique ou bien par un autre processus : les *applications* des utilisateurs sont des (ensembles de) processus.

Le système d'exploitation est chargé d'allouer les ressources (mémoires, temps processeur, entrées/sorties) nécessaires aux processus et d'assurer que le fonctionnement d'un processus n'interfère pas avec celui des autres (isolation). Il

peut aussi fournir une API pour permettre la communication inter-processus (IPC).

Outre le multiplexage des ressources matérielles, le système peut contrôler l'accès des processus aux ressources selon une matrice de droits (permissions d'accès) et également associer les processus aux utilisateurs, qui sont les récipendiaires d'un ensemble de droits d'accès : un processus a les droits de l'utilisateur qui l'a démarré.

La plupart des systèmes offrent la distinction entre processus *lourd* (tels que nous les avons décrits), qui sont a priori complètement isolés les uns des autres, et *processus légers* (*Threads* en anglais), qui ont un espace mémoire (et d'autres ressources) en commun.

Dans le cas de processus comportant plusieurs processus légers (ou suivant l'expression souvent utilisée multi-thread) il existe un état du processeur (un contexte d'exécution) distinct pour chaque processus léger.

3.2. Pour afficher les processus

Il faut utiliser le gestionnaire des Tâches pour afficher les processus qui sont en cours d'exécution sur votre système

Pour accéder au gestionnaire des Tâches :

Clic droit sur la barre des tâches =>**"Gestionnaire des tâches"** Onglet **"Processus"**. - Ou la combinaison des 3 touches **"Ctrl Alt Suppr"**

3.2.1.Le Gestionnaire des tâches

Le Gestionnaire des tâches comporte une vue d'ensemble de l'activité et des performances du système et fournit des informations concernant les programmes et les processus en cours d'exécution sur votre ordinateur. Il indique également le type de mesure des performances du processus le plus utilisé. De plus, vous pouvez l'employer pour une analyse en temps réel.

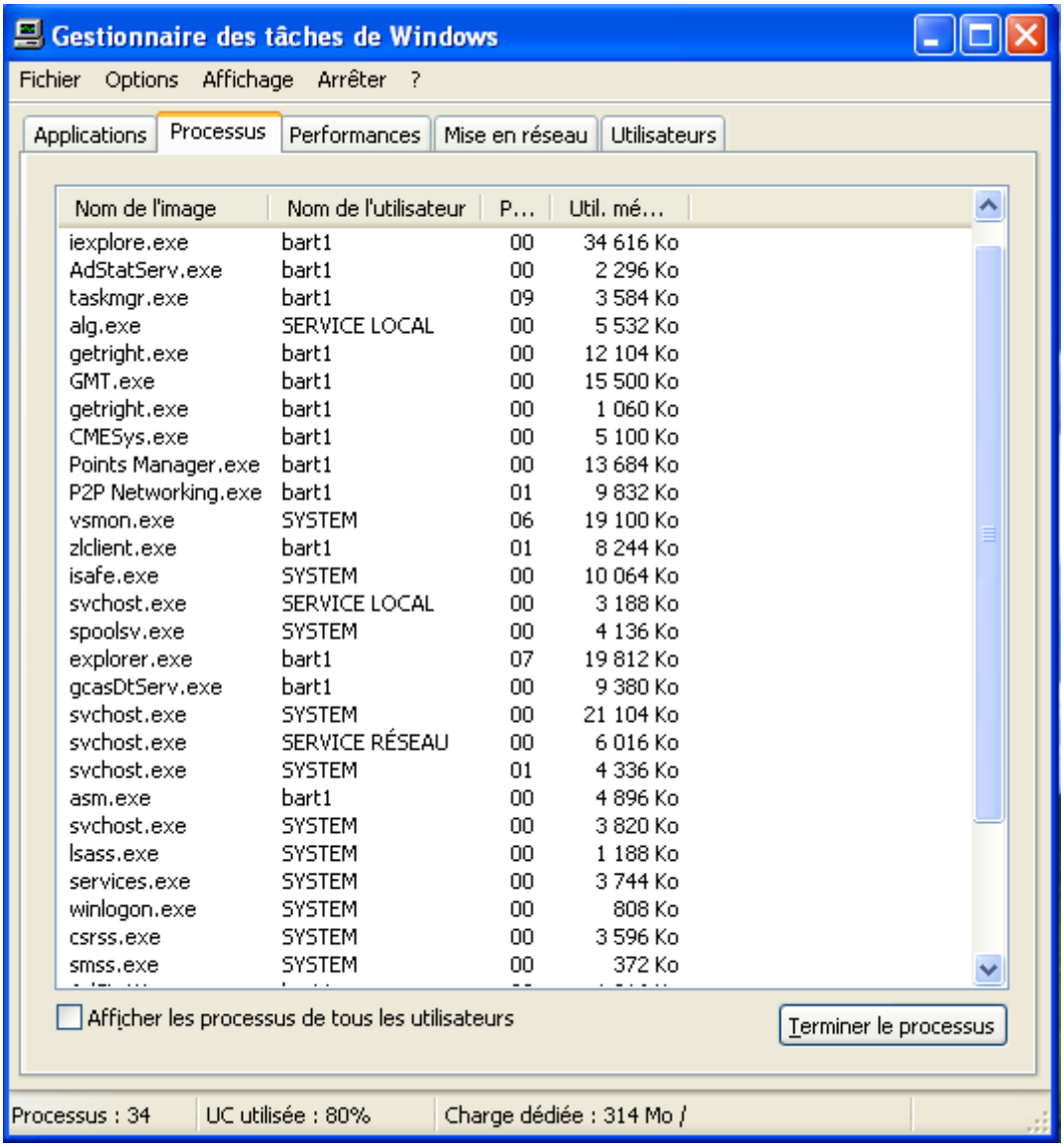
Fonctions du Gestionnaire des tâches

Le Gestionnaire des tâches peut permettre d'analyser les indicateurs clés des performances de votre ordinateur :

- Vous pouvez afficher l'état des programmes en cours d'exécution et terminer ceux qui ne répondent plus.
- L'activité des processus en cours peut être évaluée en utilisant jusqu'à quinze paramètres, et des graphiques ainsi que des données concernant l'utilisation du processeur et de la mémoire peuvent être affichés.
- Si vous êtes connecté à un réseau, vous avez la possibilité d'afficher l'état de ce réseau.
- Si plusieurs utilisateurs sont connectés à votre ordinateur, vous pouvez savoir qui ils sont, quels fichiers sont utilisés et leur envoyer un message.

Le Gestionnaire des tâches comporte cinq onglets qui permettent d'effectuer toutes ces actions.

ONGLET	DESCRIPTION
Applications	Cet onglet affiche l'état des programmes en cours d'exécution sur l'ordinateur. Il offre la possibilité de terminer un programme, d'en ouvrir un ou de basculer vers un autre.
Processus	Cet onglet contient des informations concernant les processus en cours d'exécution sur l'ordinateur. Par exemple, vous pouvez afficher des informations concernant l'utilisation du processeur et de la mémoire, les erreurs de page, le nombre de descripteurs et d'autres paramètres.
Performances	Cet onglet affiche une vue d'ensemble dynamique des performances de votre ordinateur, notamment : ! Des graphiques concernant l'utilisation du processeur et de la mémoire. ! Le nombre de descripteurs, de threads et de processus en cours d'exécution sur l'ordinateur. ! La quantité, en kilo-octets, de mémoire physique, de mémoire pour le noyau et de mémoire utile. La mémoire physique est la mémoire totale, celle pour le noyau est celle utilisée par le noyau du système et les pilotes de périphérique, et la mémoire utile correspond à la quantité de mémoire allouée aux programmes et au système d'exploitation.
Mise en réseau	Cet onglet comporte une représentation graphique des performances du réseau. Il constitue un indicateur qualitatif simple pour connaître l'état du ou des réseaux utilisés sur votre ordinateur. Il n'apparaît que si l'ordinateur dispose d'une carte réseau. Il indique la qualité et la disponibilité de la connexion, que vous soyez connecté à un ou plusieurs des réseaux.
Utilisateurs	Cet onglet indique le nom des utilisateurs pouvant accéder à l'ordinateur ainsi que l'état et le nom de la session. Le champ **Nom du client** indique le nom de l'ordinateur client qui utilise la session, le cas échéant. Le champ **Session** comporte le nom que vous devez utiliser pour effectuer des tâches telles qu'envoyer un message à un autre utilisateur ou vous connecter à une autre session d'utilisateur. L'onglet **Utilisateurs** n'apparaît que si l'option **Bascule rapide utilisateur** est activée sur l'ordinateur que vous utilisez. Ce dernier doit également être autonome ou membre d'un groupe de travail. L'onglet **Utilisateurs** n'est pas disponible sur les ordinateurs membres d'un domaine de réseau. **Onglet Performances** **Onglet Mise en réseau** **Onglet Utilisateurs**



Comme vous pouvez le constater, vous avez un certain nombre de processus qui tournent sur votre PC. Cela peut varier en fonction du nombre de programmes et de services ouverts sur votre machine ainsi que du matériel que vous utilisez. Sur cette image, nous avons même quelques virus/malwares *(essayez de les découvrir)*.

A savoir

Vos onglets ne sont pas visibles.

Il se peut que vous ne voyiez pas les onglets, ni la barre des menus, dans ce cas :

- Double-cliquez sur un des bords de la fenêtre, et vous retrouverez vos onglets.

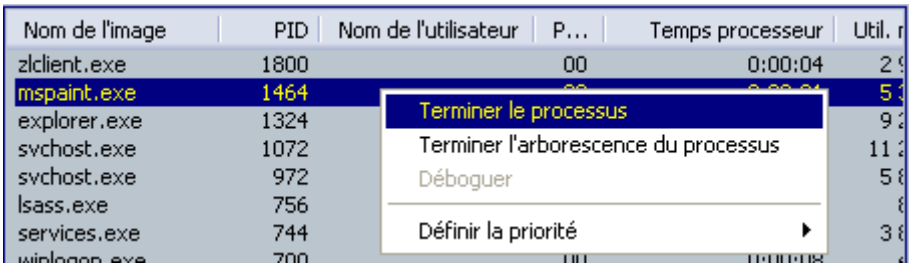
Votre Gestionnaire ne démarre pas.

Ce problème peut être dû à la présence d'un virus qui en interdit l'accés.
Ouvrez votre Explorateur, allez dans l'arborescence du dossier :
C:\Windows\System32\taskmgr.exe
renommez le fichier "taskmgr.exe" en "taskmgr.com" et double-cliquez dessus pour l'ouvrir.

(n'oubliez pas par la suite de faire une analyse antivirale pour corriger le problème)

3.3. Arrêter un processus

- Clic droit sur le processus en question => **Terminer le processus**
-



Certains processus ne peuvent pas être terminés, c'est soit :
- des processus obligatoires

- des services ou des programmes essentiels pour la sécurité (antivirus, pare-feu de connexion).

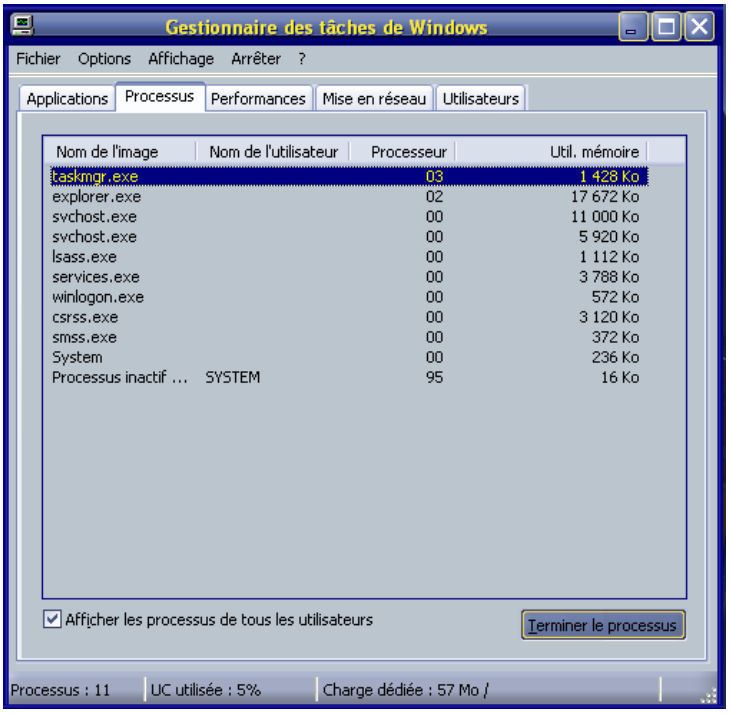
- des virus ou programmes malveillants (très souvent).

Certains processus ne peuvent être arrêtés que par l'intermédiaire des services

3.4. Les processus obligatoires

Pour fonctionner correctement, votre système d'exploitation a besoin d'un certain nombre de processus. Nous allons essayer de reconnaître les services ou processus les plus connus et décortiquer chacun d'entre-eux.

Sur cette image, nous avons le minimum vital pour le bon fonctionnement de votre système, ici Windows XP SP2.



Certains sont présents sur cette image, d'autres non, ils sont référencés par ordre alphabétique.

Alg.exe (Application Layer Gateway Service)

Utilisé pour le partage de connexion internet. Nécessaire en cas d'utilisation d'un firewall.
Ce processus est obligatoire si vous avez une connexion partagée

Csrss.exe(Client Server Runtime Process)

Il s'agit de la portion dite de mode utilisateur du sous-système Win32. Csrss signifie client server run-time subsystem et reste un sous-système essentiel qui doit fonctionner en permanence. Csrss gère les applications consoles, la création et la destruction de threads et quelques parties de l'environnement 16 bits virtuel MS-DOS.
Ce processus est obligatoire

Explorer.exe(Votre bureau)

Il s'agit de l'interface utilisateur, celle qui nous présente le bureau de Windows, la barre des tâches etc... Ce processus n'est pas vital pour le système d'exploitation ; il peut être arrêté et relancé à partir du gestionnaire des tâches (ouvrir puis spécifier explorer.exe). Il peut être remplacé par d'autres solutions si vous changez de bureau par exemple, pour des logiciels comme **"Litestep"** par exemple, Explorer.exe sera ainsi remplacé par litestep.exe
Ce processus est obligatoire si vous voulez avoir le bureau

Lsass.exe(Local Security Authority Service)

Il s'agit du poste de travail local d'authentification de sécurité, il génère le processus responsable de l'authentification des utilisateurs par le service Winlogon. Ce processus est permis par l'utilisation de packages d'authentification comme msgina.dll. Si l'authentification est réussie, Lsass génère le jeton d'accès de l'utilisateur qui est utilisé pour lancer le shell initial. D'autres processus que l'utilisateur peut lancer, vont hériter de ce jeton. Ce processus peut être ouvert par plusieurs types de services dont voici la liste :

- Emplacement protégé
- Fournisseur de la prise en charge de sécurité LM NT
- Gestionnaire de compte de sécurité
- Ouverture de session réseau
- Service IPSEC

Ce processus est obligatoire même si vous n'avez aucun service correspondant démarré.

Services.exe ou Services(Services Control Manager)

Il s'agit du Service Control Manager (gestionnaire de contrôle des services) qui est responsable du démarrage, de l'arrêt et de l'interaction avec les services système.

Smss.exe (Windows NT Session Manager)

Il s'agit du sous-système de gestion de session (session manager subsystem) qui est responsable de démarrer la session utilisateur.
Ce processus est initié par le thread système et est responsable de différentes activités dont le lancement des process Winlogon et Win32 (csrss.exe) et du positionnement des variables système. Après qu'il ait lancé ces processus, il attend que Winlogon ou
Csrss se termine. Si cela se produit normalement, le système s'arrête.

Svchost.exe

Il s'agit d'un processus générique, il fonctionne en tant qu'hôte pour d'autres processus tournant à partir de Dlls, il peut y avoir plusieurs entrées pour ce processus. Afin de voir les processus qui utilisent svchost.exe, il faut utiliser l'utilitaire tasklist.exe

Ces processus sont obligatoires (entre 2 à 8 processus)

System ou System Idle Process Processus inactif du système

Ce process est un thread unique qui fonctionne sur chaque processeur, sa seule fonction est d'occuper le temps processeur
lorsque le système ne fait tourner aucun autre thread.

Winlogon.exe

Il s'agit du processus responsable de gérer l'ouverture et la fermeture de session. Par ailleurs, Winlogon est actif uniquement lorsque l'utilisateur appuie sur CTRL+ALT+DEL, à ce moment il affiche la boîte de sécurité.
Ce processus est obligatoire si vous utilisez le changement rapide d'utilisateur

Taskmgr.exe

C'est le processus pour le gestionnaire des tâches lui-même.
Ce processus ne démarre que lorsque que vous utilisez le gestionnaire de tâches

Winmgmt.exe ou wmiprvse.exe

Winmgmt.exe est un composant noyau de la gestion des clients sous Windows 2000. Ce processus s'initialise lorsque la première application cliente se connecte. Winmgmt.exe correspond au service WMI qui permet de surveiller par exemple des ressources sur la machine (mémoire, disque ...).
Ce processus se nomme wmiprvse.exe sur XP
Ce processus est obligatoire, mais pas toujours présent

3.5. Les processus indispensables

Les processus indispensables correspondent aujourd'hui à votre connexion Internet et la sécurité de votre PC pour accéder au réseau. Cela comprend tous les services et programmes d'antivirus et de pare-feu (firewall). Chaque Editeur ayant des noms spécifiques, il est difficile de faire une liste complète, mais en voici quelques-uns des plus connus par marque :

CnxMon.exe - CnxDslTb.exe

Connexion ADSL USB, elle peut se retrouver sous plusieurs noms différents en fonction de votre fournisseur d'accès internet
Ce processus est obligatoire si vous utilisez une connexion USB ADSL

waol.exe - Shellmon.exe

Pour les possesseurs d'une connexion internet par le FAI AOL
Ces processus sont obligatoires si vous êtes chez AOL version 8

NAVAPW32.EXE - NAVAPSVC.EXE

Correspond à des services de Norton, il peut en exister d'autres à propos de Norton
Ces processus sont obligatoires si vous utilisez Norton

ashDisp.exe - aswUpdSv.exe - ashServ.exe

Correspond à des services Avast
Ces processus sont obligatoires si vous utilisez Avast

Vsmon.exe - Zlclient.exe

Correspond au pare-feu ZoneAlarm
Ce processus est obligatoire si vous utilisez ZoneAlarm

3.6. Les processus utiles mais pas indispensables

Spoolss.exe(Printer Spooler Subsystem)

Le sous-ensemble du spooler d'imprimante Windows despoole les données à imprimer du disque à l'imprimante.

Spoolsv.exe(spooler service)

Le service spooler est responsable de la gestion des travaux d'impression et de fax. Ce process ne peut être arrêté à partir du gestionnaire des tâches. Les autres processus connus par l'intermédiaire de votre imprimante ne sont absolument pas indispensables à la bonne marche de votre imprimante. Seul ce processus est obligatoire si vous utilisez une imprimante.
Ce processus est utile si vous utilisez une imprimante

Ctfmon.exe(CTF Loader)

Ce processus appartient à Windows XP / Office XP et fournit le "Alternate User Text Input Processor" (TIP) et la barre de langage de Microsoft Office. Si vous voulez obtenir quelques ressources en plus, essayez de neutraliser ce processus.

Internat.exe

"Internat.exe" fonctionne au démarrage. Il charge les différents paramètres locaux d'entrée spécifiés par l'utilisateur. Les paramètres sont pris à partir de la clé de registre suivante :
HKEY_USERS\.DEFAULT\Keyboard Layout\Preload
Internat.exe charge l'icône **"FR"** dans le systray, ce qui permet de changer facilement entre différents paramètres régionaux. Cette icône disparaît lorsque le process est arrêté mais les paramètres peuvent toujours être changés via le panneau de configuration.

Mobsync.exe

Il s'agit du "Synchronisation Manager" qui peut se trouver après l'installation du SP2 de Windows 2000
pour le supprimer, allez dans Exécuter et tapez ceci : **regsvr32 /u mobsync.dll**
Il se peut que vous ne le voyiez pas dans les processus actifs, mais vous pouvez le trouver par l'intermédiaire de
Exécuter : **msconfig** => onglet **"Démarrage"**

Mstask.exe

Il s'agit du service de planification de tâches, responsable de lancer des tâches à un instant déterminé par l'utilisateur.
Ce process ne peut être arrêté à partir du gestionnaire des tâches.

Netdde.exe

Fournit le transport en réseau et la sécurité pour l'échange dynamique des données pour les programmes exécutés sur un même ordinateur ou des ordinateurs différents, il est présent par exemple avec ZoneAlarm dans sa Version 4.0.1
il correspond à 2 services **"DDE Réseau" et "DSDM DDE réseau"**

3.7. Les processus inutiles

De nombreux processus sont inutiles au bon fonctionnement de votre machine, ils sont souvent installés par défaut par l'intermédiaire du fabricant du PC, de l'installation d'un nouveau périphérique, etc.. Il n'est pas possible de faire une liste complète tellement il en existe, en voici plusieurs :

aom.exe

Ce processus correspond à un programme de Adobe qui tente de se connecter sur internet pour chercher des mises à jour des produits installés, pour le désactiver il suffit de rechercher le fichier sur votre DD, et de renommer le fichier aom.exe en fichier aom.bak

iTouch.exe

C'est le processus des pilotes de claviers sans fils iTouch. Il crée une icône dans le System tray de Windows qui lance un logiciel de Logitech pour la configuration du clavier. Ce logiciel peut également être lancé à partir du menu Démarrer. Nécessaire aux utilisateurs des claviers Logitech.
Pour empêcher le lancement de ce processus, il faut supprimer la valeur de registre contenue dans :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
et qui a pour valeur : **C:\Program Files\Logitech\iTouch\iTouch.exe**

NeroCheck.exe

Ce processus surveille le **"nerocd2k.sys"** de Nero 5.5 ou supérieur.
Ceci doit empêcher les conflits avec d'autres programme de gravure.
Pour empêcher le lancement de ce processus, il faut supprimer la valeur de registre contenue dans :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
et qui a pour valeur : **C:\WINDOWS\System32\NeroCheck.exe**

Qttask.exe

(Quick Time Tray Icon)
Permet de démarrer Quicktime à partir du System Tray
Pour empêcher le lancement de ce processus, il faut supprimer la clé de registre contenue dans :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
et qui a pour valeur : **"C:\Program Files\QuickTime\qttask.exe" -atboottime**

Realsched.exe

(RealNetworks Scheduler)
Processus de mise-à-jour de RealPlayer. C'est un processus qui prend de la mémoire : vous pouvez l'arrêter.
Installé par RealOne, il est recréé et mis à jour quand RealOne est lancé même si vous essayez de le supprimer.
Pour empêcher le lancement de ce processus, il faut supprimer la valeur de registre contenue dans :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
et qui a pour valeur: **C:\Program Files\Common Files\Real\Update_OB\evntsvc.exe -osboot**

Ca y est nous avons fait un petit tour d'horizon des processus les plus connus, il est temps pour vous d'optimiser le nombre de processus ouverts sur votre machine.
Il faut savoir que Windows gère convenablement le multi-tâches tant qu'il ne dépasse pas 21 processus en cours A vous de faire le choix le plus judicieux afin de tirer partie au mieux des ressources de votre système.

Pour approfondir le sujet....

Consulter le support aide de Microsoft

Sources de référence

SITE TECHNET DE MICROSOFT