Les solutions spécialisées

Dans cette partie sont regroupés différents types de solutions qui vont vous permettre de résoudre des problèmes en apparence compliqués. Ils ont tous un point commun : les manipulations décrites nécessitent de l'attention et beaucoup de méthode. Ces solutions ont été testées des centaines de fois. Elles sont donc toutes efficaces !

1. Procédure de dépannage générique

Suite à l'installation d'un nouveau périphérique ou d'un nouveau programme, vous ne pouvez accéder à Windows : démarrez en mode WinRE puis utilisez l'outil de restauration du système.

Si vous pouvez démarrer ou travailler en mode sans échec, le problème est a priori d'ordre logiciel : un pilote de périphérique dont il faut faire la mise à jour, un programme à désinstaller ou à mettre à jour ou encore à désactiver en utilisant l'éditeur de configuration système.

Dans les autres cas, c'est plutôt un problème matériel : mise à jour du BIOS (UEFI), paramétrage du BIOS (UEFI) sur les options par défaut ou vérification de chaque composant présent dans votre ordinateur (barrettes mémoire, processeur, carte mère, cartes PCI ou AGP, périphériques de stockage et de lecture).

Les erreurs STOP peuvent être suivies d'un nom de fichier. Lancez une recherche sur ce fichier puis accédez à ses propriétés. Les informations qui y figurent vous permettent de voir si le fichier en cause fait partie du système d'exploitation Windows ou est rattaché à un programme ou un pilote de périphérique. Dans ce dernier cas, désactivez le périphérique ou désinstallez le programme ou mieux procédez à sa mise à jour.

Dans le Gestionnaire de périphériques, désactivez un à un chaque périphérique que vous pouvez considérer comme suspect.

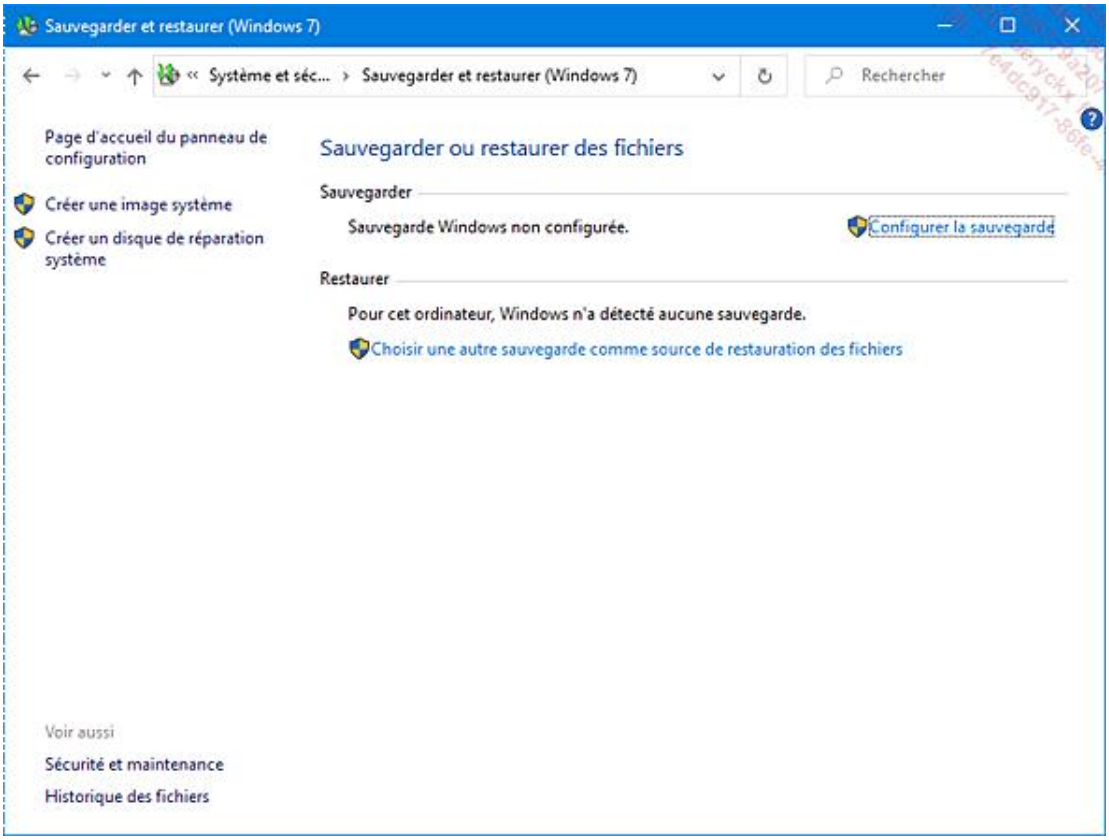
Respectez l'ordre suivant : ports, modem et rubriques attachées (modem énumérateur, par exemple), cartes réseau, contrôleurs audio, vidéo et jeu, contrôleurs de bus USB, périphériques USB, périphériques infrarouges. Une fois que le pilote de périphérique défectueux sera identifié, il vous faudra alors effectuer une mise à jour de ce dernier (et supprimer le profil matériel que vous avez créé).

Si votre souci date d'une mise à jour d'un de vos périphériques, revenez à la version précédente du pilote.

2. Créer un disque de réparation système

Cette option de Windows permet de créer un disque de réparation système avec les fonctionnalités WinRE si vous n'avez plus votre disque d'installation de Windows. Avec ce disque vous pourrez réparer votre installation à partir des points de restauration du système.

- Ouvrez une invite de commandes en mode administrateur.
- Exécutez la commande suivante : `sdclt`. Vous pouvez aussi accéder à cet utilitaire depuis le **Panneau de configuration** dans la section **Système et sécurité**, puis **Sauvegarder et restaurer (Windows 7)**.



- Cliquez sur **Créer un disque de réparation système**. Il faudra obligatoirement disposer d'un graveur de DVD.
- À la fin de l'opération de création du disque, cliquez sur le bouton **Fermer** puis sur le bouton **OK**. Le disque de réparation système est prêt.

En cas de problème, démarrez votre poste sur ce disque de réparation afin de pouvoir accéder aux fonctionnalités WinRE.

3. Réinitialiser les paramètres de sécurité par défaut

Cette manipulation peut, par exemple, vous permettre de résoudre une erreur Windows Update 0x8007f004 (Droits insuffisants) ou un problème d'accès à une ressource partagée sur un réseau local. Avant toute manipulation, prenez la précaution de faire un point de restauration système. Les commutateurs pour la commande `Secedit` sont les suivants :

- `/configure` : le fichier *Secedit.exe* devra définir les paramètres de sécurité du système.
- `/db Nom_Fichier` : indique le chemin d'une base de données qui contient le modèle de sécurité à appliquer. Bien que cet argument soit obligatoire, le fichier de base de données peut ne pas exister.
- `/cfg Nom_Fichier` : il s'agit du chemin du modèle de sécurité qui sera importé dans la base de données puis appliqué au système. Si vous ne spécifiez pas cet argument, le modèle qui est déjà stocké dans la base de données sera appliqué. Cet argument n'est possible que si vous l'utilisez avec le commutateur `/DB`.
- `/overwrite` : indique si le modèle de sécurité défini à la suite du commutateur `/CFG` écrase le modèle stocké dans la base de données, au lieu d'ajouter les résultats dans ce même modèle (c'est l'option par défaut). Cet argument n'est possible que si vous l'utilisez avec le commutateur `/DB`.
- `/areas Zones_Sécurité` : définit les zones de sécurité qui doivent être appliquées.

Les valeurs permises sont les suivantes :

- **SECURITYPOLICY** : stratégies des comptes et les attributions des droits des utilisateurs.
- **GROUP_MGMT** : paramètres des restrictions pour les groupes qui sont spécifiés dans le modèle de sécurité.
- **USER_RIGHTS** : autorisations d'ouverture de session de l'utilisateur et octroi de privilèges.
- **REGKEYS** : modèles de sécurité pour les clés locales du Registre.
- **FILESTORE** : sécurité pour le stockage local des fichiers.
- **SERVICES** : sécurité de tous les services définis.

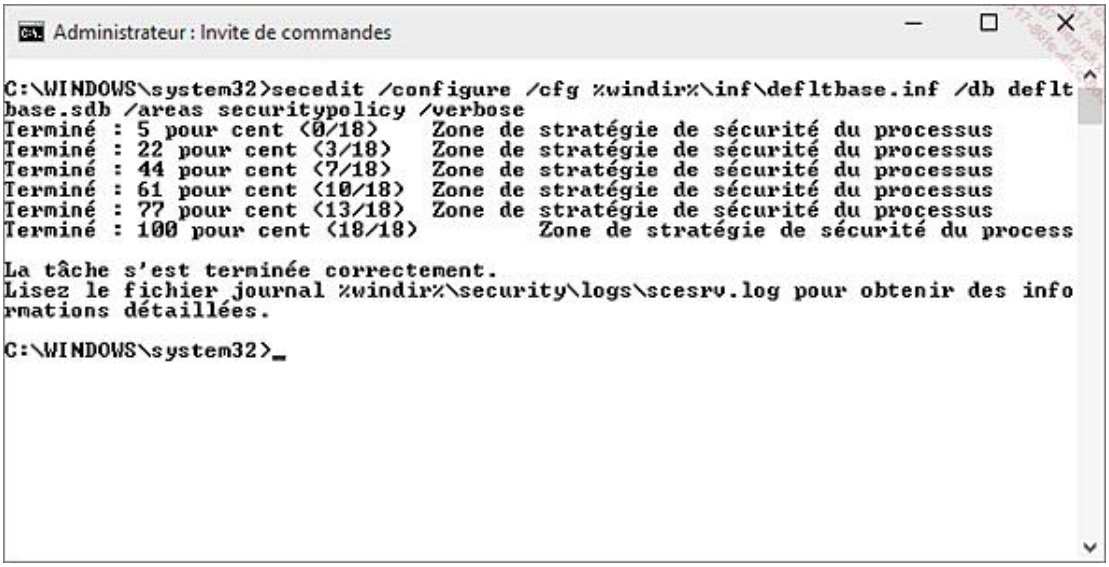
Voici les autres commutateurs :

- `/log Chemin_Fichier_Journal` : permet de définir l'emplacement du fichier journal qui retrace le suivi des modifications.
- `/verbose` : permet d'afficher des informations plus détaillées.
- `/quiet` : réduit le volume des informations affichées à l'écran ainsi que celles qui seront consignées dans le fichier journal.

Vous devez exécuter `Secedit` à partir de l'invite de commandes.

Par exemple, afin de configurer sur les paramètres d'origine les stratégies sur les comptes d'utilisateurs, saisissez cette commande :

```
secedit /configure /cfg %windir%\inf\defltbase.inf /db
defltbase.sdb /areas securitypolicy /verbose
```



La liste des entrées du Registre qui auront été réécrites sera visible en éditant le fichier *Scesrv.log* placé dans \WINDOWS\security\logs.

La configuration des privilèges utilisateur s'opère en saisissant cette commande :

```
secedit /configure /cfg %windir%\inf\defltbase.inf /db
```

```
defltbase.sdb /areas user_rights /verbose
```

Vous pouvez redéfinir les autorisations définies dans le Registre en saisissant cette commande :

```
secedit /configure /cfg %windir%\inf\defltbase.inf /db
defltbase.sdb /areas regkeys /verbose
```

La configuration des permissions liées aux fichiers et aux répertoires se force en saisissant cette commande :

```
secedit /configure /cfg %windir%\inf\defltbase.inf /db
defltbase.sdb /areas filestore /verbose
```

Voici maintenant un exemple d'utilisation : il vous est impossible d'ouvrir une session interactive sur un poste. Ce problème est lié à une stratégie locale de sécurité endommagée. Vous avez deux solutions :

- Créez un script de démarrage utilisant **Secedit** afin de vous permettre de réinitialiser les paramètres de sécurité par défaut.
- Utilisez conjointement **Psexec** (outil Systernals, cf. chapitre Les outils système, section Les outils Sysinternals) et **Secedit** afin d'exécuter ce type de commande :

```
psExec \\Nom_Serveur -u Nom_Administrateur -p Mot_De_Passe
secedit /configure /cfg %windir%\inf\defltbase.inf /db
defltbase.sdb /areas user_rights /verbose
```

4. Réparer les permissions NTFS dans le Registre Windows

Cette solution vous permet, par exemple, de résoudre les problèmes suivants :

- Plusieurs boîtes de dialogue sont vides.
- Il y a des dysfonctionnements uniquement sur un des comptes d'utilisateurs.
- Windows Media Player ne peut pas démarrer.
- Il est impossible de définir un "Player" comme étant le programme par défaut.
- Les fichiers EXE ne sont plus reconnus.
- Les programmes utilisant Windows Installer ne peuvent plus s'installer correctement (Code d'erreur n°10 ou message de type "Accès refusé").
- Vous avez des erreurs de type "code 5" ou "0x5" ou 0x80070005".
- Certains paramètres de la Barre des tâches ne sont pas mémorisés.
- Des associations de fichiers ne fonctionnent plus.

Vous pouvez résoudre assez facilement ce problème en utilisant un outil appelé SubInAcl et qui est téléchargeable séparément à partir de cette page : http://www.microsoft.com/en-us/download/details.aspx?id=23510

Procédez ensuite à l'installation du fichier MSI. SubInACL.exe est un outil d'invite de commandes qui vous permet de manipuler le jeu des permissions NTFS des fichiers, dossiers, clés du Registre et des services.

- Créez un nouveau document appelé *registre.cmd* (le nom n'a pas d'importance).

Seul point indispensable : ce fichier doit avoir l'extension *.cmd* (ou *.bat*). Afin de vous faciliter la tâche, enregistrez ce fichier dans le même répertoire que celui dans lequel réside *SubInACL*.

- Copiez ensuite le contenu suivant :

```
subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=
administrators=f subinacl /subkeyreg HKEY_CURRENT_USER
/grant=administrators=f subinacl /subkeyreg
HKEY_CLASSES_ROOT /grant=administrators=f subinacl
/subdirectories %SystemDrive% /grant=administrators=f
subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=system=f
subinacl /subkeyreg HKEY_CURRENT_USER /grant=system=f
subinacl /subkeyreg HKEY_CLASSES_ROOT /grant=system=f
subinacl /subdirectories %SystemDrive% /grant=system=f
```

- Ouvrez une fenêtre d'invite de commandes.
- En utilisant la commande `cd`, déplacez-vous dans le répertoire contenant votre fichier de commande.
- Saisissez ceci : `registre.cmd`.

Patientez de longues minutes avant de pouvoir redémarrer votre ordinateur.