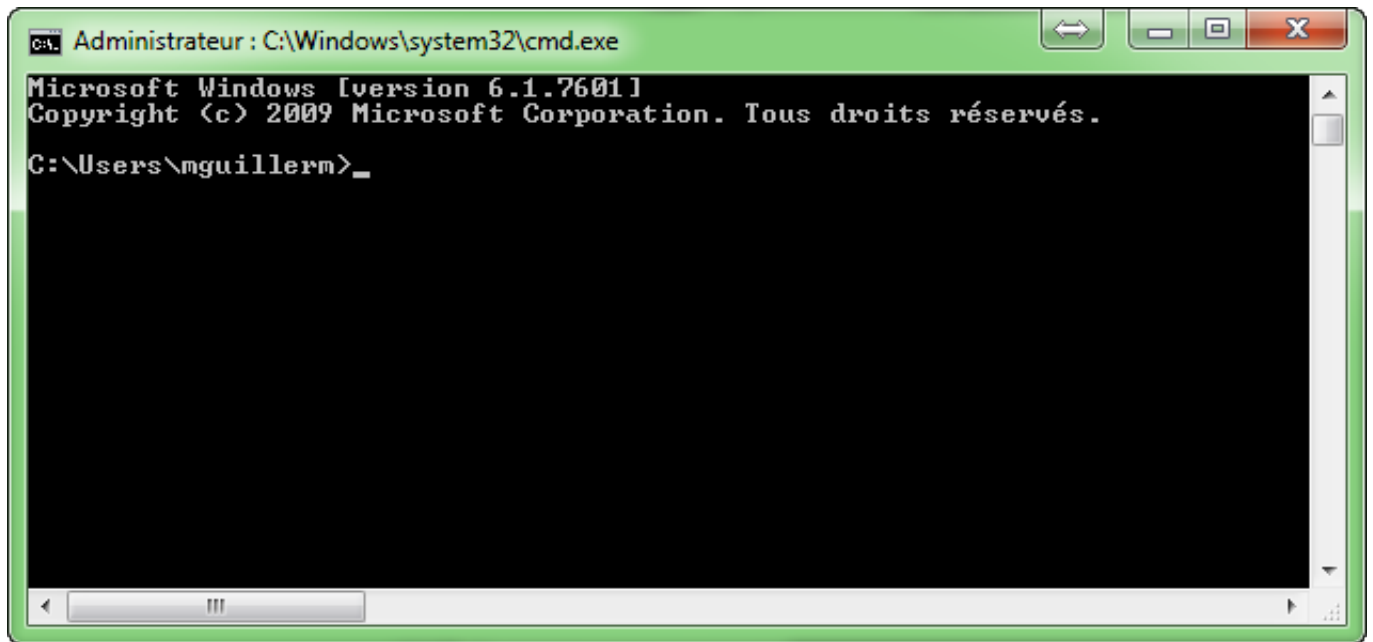


# Les commandes Windows à connaître



Même sur [Windows](#), il y a beaucoup de choses que l'on peut faire à partir de **ligne de commande**, et c'est souvent plus rapide, voire même plus efficace que via l'interface graphique. Certains n'ont même pas d'équivalent en graphique, c'est pourquoi il peut être bon de rappeler quelques commandes que j'utilise au quotidien pour diagnostiquer ou réparer les pc de mes clients.

Bien évidemment, je ne vais pas mettre toutes les commandes ici, mais seulement celle qui me semble les plus utiles. Si j'en oublie ou si vous pensez que certaines devraient avoir leurs places ici alors n'hésitez pas, **les commentaires sont là pour ça !**

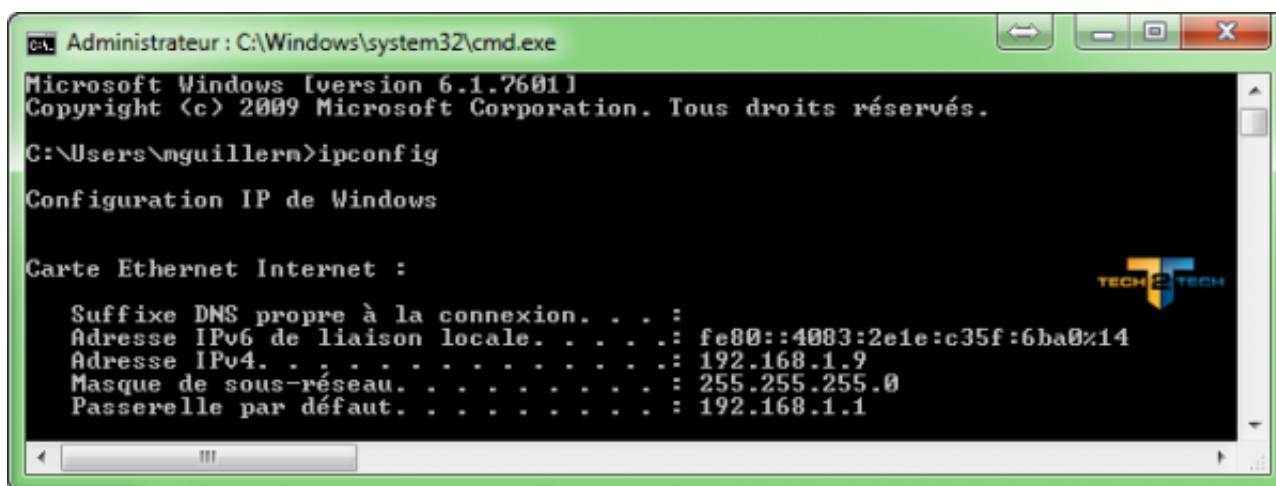
## **ipconfig – retrouvez rapidement votre adresse ip**

Il est possible de **trouver son adresse ip** via le panneau de configuration, mais il y a beaucoup plus rapide. La commande **ipconfig** est un moyen rapide de **déterminer l'adresse IP de votre ordinateur** et d'autres informations, telles que l'adresse de sa passerelle par défaut – utile par exemple si vous voulez connaître l'adresse IP de votre routeur.

Pour utiliser la commande, il suffit de taper **ipconfig** dans une fenêtre d'invite de commande. Vous verrez alors une liste de toutes les connexions réseau de votre ordinateur utilisé avec leurs adresses respectives.

Et si vous souhaitez avec encore plus de détails, alors utiliser la commande "**ipconfig /all**" qui vous donnera encore plus d'informations telle que l'adresse MAC de la carte réseau. (Mais il existe encore d'autre argument très utile à la commande ipconfig,

comme “ipconfig /release” et “ipconfig /renew” pour relancer une requête DHCP par exemple.)



```
Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\mguillerm>ipconfig

Configuration IP de Windows

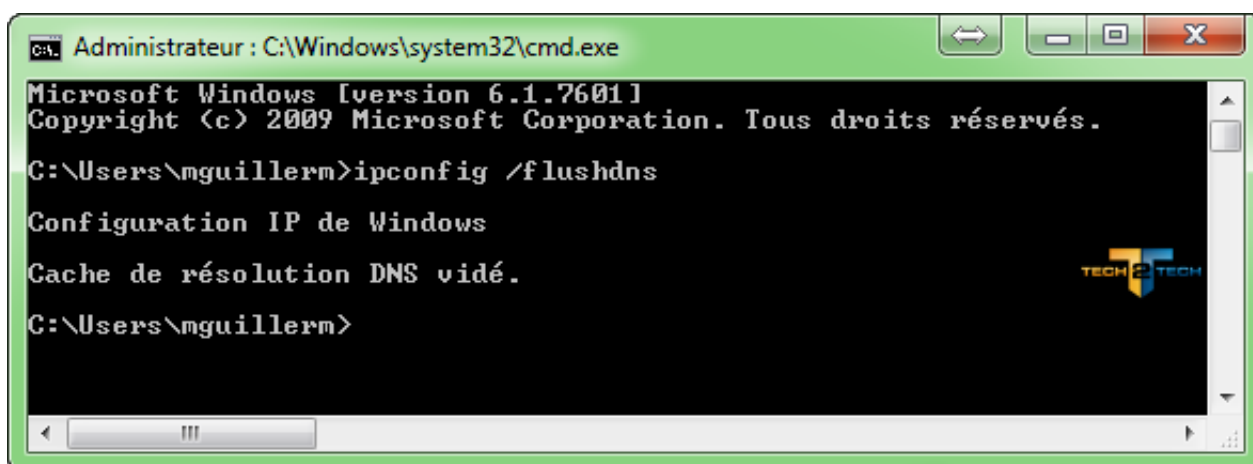
Carte Ethernet Internet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::4083:2e1e:c35f:6ba0%14
    Adresse IPv4. . . . . : 192.168.1.9
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.1
```

## ipconfig / flushdns – Vider votre cache de résolution DNS

Vide et réinitialise le contenu du cache de résolution du client DNS.

Par exemple, si vous **changez vos serveurs DNS** , les effets ne seront pas toujours immédiatement. En effet, Windows utilise un cache pour les entrées DNS. C’est ce cache que nous allons vider avec la commande “ipconfig /flushdns”.



```
Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\mguillerm>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

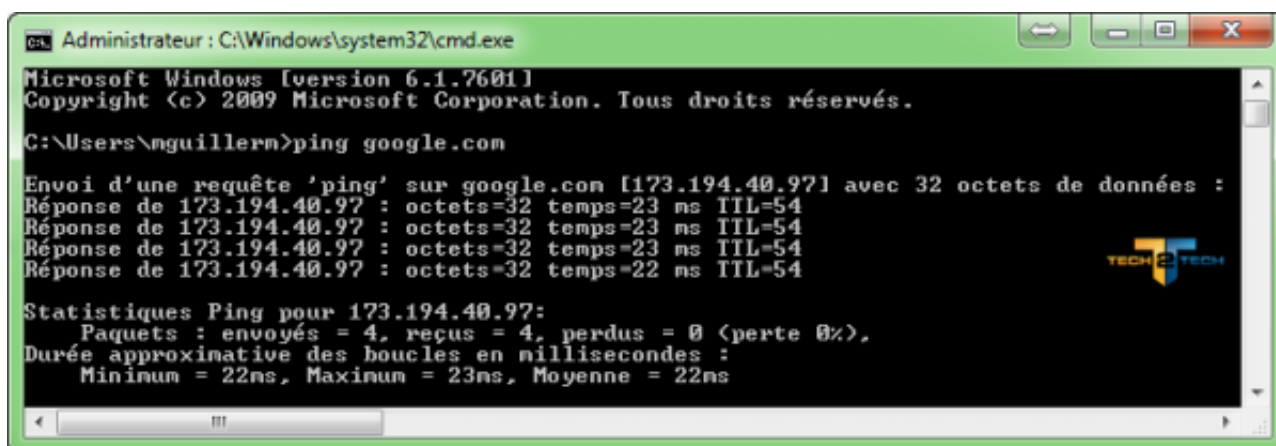
C:\Users\mguillerm>
```

## ping – Tester sa connexion réseau

Si vous **rencontrez des problèmes de connexion** à un site Web ou d’autres problèmes de connexion réseau, Windows a des outils que vous pouvez utiliser pour identifier les problèmes.

Tout d’abord, il y a la commande ping. Par exemple **ping google.com** ou ping 192.168.1.1 pour savoir si la connexion entre votre ordinateur et l’adresse distante fonctionne. Windows va envoyer des paquets à Google.com. Google va réagir et vous faire savoir qu’il a reçu. Si des paquets ne circulent pas correctement, alors vous serez

en mesure de le voir directement depuis votre console. Vous verrez également combien de temps il vous a fallu joindre l'adresse distante. Pour aller un peu plus loin, il faut utiliser la commande "tracert"



```
Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

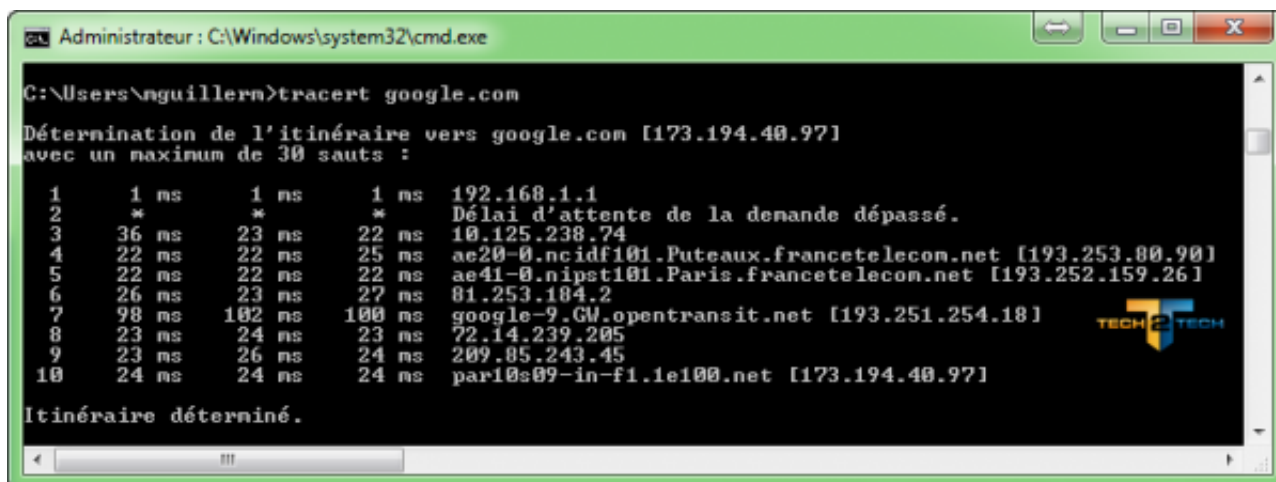
C:\Users\nguillern>ping google.com

Envoi d'une requête 'ping' sur google.com [173.194.40.97] avec 32 octets de données :
Réponse de 173.194.40.97 : octets=32 temps=23 ms TTL=54
Réponse de 173.194.40.97 : octets=32 temps=23 ms TTL=54
Réponse de 173.194.40.97 : octets=32 temps=23 ms TTL=54
Réponse de 173.194.40.97 : octets=32 temps=22 ms TTL=54

Statistiques Ping pour 173.194.40.97:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 22ms, Maximum = 23ms, Moyenne = 22ms
```

## tracert – Résoudre les problèmes de connexion réseau

La commande **tracert**, permet de **retracer l'itinéraire** qu'il faut pour un paquet avant d'atteindre une destination. Par exemple, si vous exécutez **tracert google.com** vous verrez alors le chemin de votre paquet avant d'atteindre Google. Si vous rencontrez des problèmes de connexion réseau, la commande tracert peut vous permettre de comprendre où bloque la connexion réseau ; si c'est chez vous, ou sur l'un des serveurs / routeurs qui se trouve après votre propre routeur.



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

C:\Users\nguillern>tracert google.com

Détermination de l'itinéraire vers google.com [173.194.40.97]
avec un maximum de 30 sauts :

  1    1 ms    1 ms    1 ms    192.168.1.1
  2    *      *      *      Délai d'attente de la demande dépassé.
  3   36 ms   23 ms   22 ms   10.125.238.74
  4   22 ms   22 ms   25 ms   ae20-0.ncidf101.Puteaux.francetelecom.net [193.253.80.90]
  5   22 ms   22 ms   22 ms   ae41-0.nipst101.Paris.francetelecom.net [193.252.159.26]
  6   26 ms   23 ms   27 ms   81.253.184.2
  7   98 ms  102 ms  100 ms  google-9.GW.opentransit.net [193.251.254.18]
  8   23 ms   24 ms   23 ms   72.14.239.205
  9   23 ms   26 ms   24 ms   209.85.243.45
 10   24 ms   24 ms   24 ms   pari0s09-in-f1.1e100.net [173.194.40.97]

Itinéraire déterminé.
```

## netstat-an – Liste des connexions réseau et des ports

La commande **netstat** est très utile, en utilisant certaines options, cette commande s'avère très puissante. Par exemple l'une des options les plus intéressantes de netstat est **netstat -an**, qui permet d'afficher la liste de toutes les connexions réseau ouvertes sur l'ordinateur, ainsi que les ports utilisés et les adresses IP externes sur lesquelles le pc est connecté. Lorsque vous avez un virus (de type cheval de Troie par exemple), vous pouvez voir l'adresse où est connecté le virus.

```

ca. Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\nguillerm>netstat -an

Connexions actives

Proto  Adresse locale          Adresse distante        État
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
TCP    0.0.0.0:443              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    0.0.0.0:902              0.0.0.0:0               LISTENING
TCP    0.0.0.0:912              0.0.0.0:0               LISTENING
TCP    0.0.0.0:2869             0.0.0.0:0               LISTENING
TCP    0.0.0.0:8081             0.0.0.0:0               LISTENING
TCP    0.0.0.0:17500            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49152            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49153            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49154            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49156            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49157            0.0.0.0:0               LISTENING
TCP    0.0.0.0:53138            0.0.0.0:0               LISTENING
TCP    127.0.0.1:5939           0.0.0.0:0               LISTENING
TCP    127.0.0.1:5939           127.0.0.1:56014        ESTABLISHED
TCP    127.0.0.1:8307           0.0.0.0:0               LISTENING
TCP    127.0.0.1:19872          127.0.0.1:60358        ESTABLISHED
TCP    127.0.0.1:49155          0.0.0.0:0               LISTENING
TCP    127.0.0.1:51538          0.0.0.0:0               LISTENING
TCP    127.0.0.1:56012          127.0.0.1:56013        ESTABLISHED
TCP    127.0.0.1:56013          127.0.0.1:56012        ESTABLISHED
TCP    127.0.0.1:56014          127.0.0.1:5939         ESTABLISHED
TCP    127.0.0.1:60358          127.0.0.1:19872        ESTABLISHED
TCP    169.254.146.205:139     0.0.0.0:0               LISTENING
TCP    192.168.1.9:139         0.0.0.0:0               LISTENING
TCP    192.168.1.9:50848        173.194.40.213:443     ESTABLISHED
TCP    192.168.1.9:50849        173.194.67.106:443     CLOSING
TCP    192.168.1.9:50858        173.194.40.166:443     ESTABLISHED
TCP    192.168.1.9:50859        173.194.78.125:5222    ESTABLISHED
TCP    192.168.1.9:50861        108.160.162.112:80     ESTABLISHED
TCP    192.168.1.9:50865        37.252.229.2:5938      ESTABLISHED
TCP    192.168.1.9:50872        37.59.60.169:21        ESTABLISHED
TCP    192.168.1.9:50885        173.194.40.127:443     ESTABLISHED
TCP    192.168.1.9:50890        37.59.60.169:80        CLOSING
TCP    192.168.1.9:50897        37.59.60.169:80        CLOSING
TCP    192.168.1.9:50906        66.96.147.117:80       TIME_WAIT
TCP    192.168.1.9:50914        37.59.60.169:80        LAST_ACK
TCP    192.168.1.9:50917        199.47.217.177:443     ESTABLISHED
TCP    192.168.1.9:50918        37.59.60.169:21        ESTABLISHED
TCP    192.168.1.9:50920        37.59.60.169:42964     ESTABLISHED
TCP    192.168.1.9:50921        37.59.60.169:80        ESTABLISHED
TCP    192.168.1.9:50923        93.88.241.128:80       TIME_WAIT
TCP    192.168.1.9:50924        37.59.60.169:21        ESTABLISHED
TCP    192.168.1.9:50926        93.88.241.128:80       LAST_ACK
TCP    192.168.1.9:50927        93.88.241.128:80       ESTABLISHED
TCP    192.168.1.9:50931        66.96.147.117:80       ESTABLISHED
TCP    192.168.1.9:50933        37.59.60.169:44628     ESTABLISHED
TCP    192.168.1.9:50934        66.96.147.117:445     SYN_SENT
TCP    192.168.152.1:139       0.0.0.0:0               LISTENING
TCP    192.168.217.1:139       0.0.0.0:0               LISTENING
TCP    [::]:135                 [::]:0                   LISTENING

```

## cipher – Supprimer définitivement et écraser un répertoire

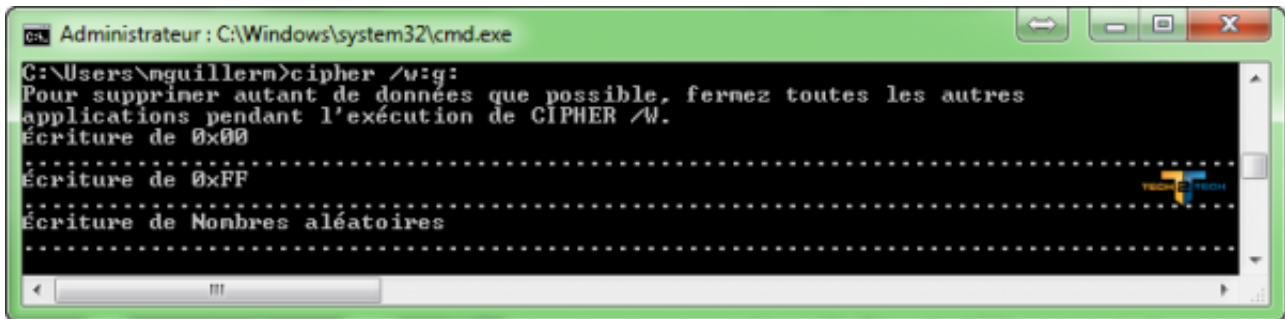
La commande “**cipher**” permet le chiffrement des données, mais pas que ! En effet, elle permet également d’écrire des données aléatoires sur un disque. Pourquoi faire me direz vous ? Et bien par exemple si vous souhaitez vendre un disque dur, le formater ne suffit pas, sachez qu’après un formatage, vos données ne sont pas visibles directement sur le disque, mais pourtant sont bel et bien là ! Il suffira alors



d'un [logiciel de récupération de données](#) pour récupérer toutes vos données. C'est ce que va empêcher la commande **cipher**.

Pour utiliser la commande, spécifier le lecteur que vous souhaitez effacer comme ceci par exemple :

*cipher /w:g: ou cipher /w:e:*

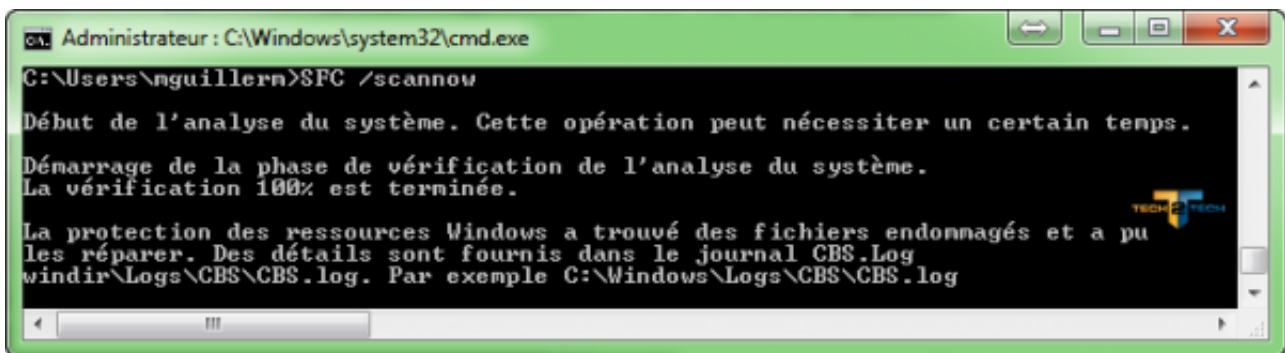


```
Administrateur : C:\Windows\system32\cmd.exe
C:\Users\nguillern>cipher /w:g:
Pour supprimer autant de données que possible, fermez toutes les autres
applications pendant l'exécution de CIPHER /W.
Écriture de 0x00
.....
Écriture de 0xFF
.....
Écriture de Nombres aléatoires
.....
```

## Scanner les fichiers système pour vérifier leur intégrité – SFC / scannow

Windows inclut un outil de vérification du système de fichiers qui scanne les fichiers système et cherche des problèmes. Si les fichiers système sont manquants ou endommagés, le vérificateur des fichiers système (SFC : System Files Check) va les réparer. Cela peut résoudre certains problèmes des systèmes Windows.

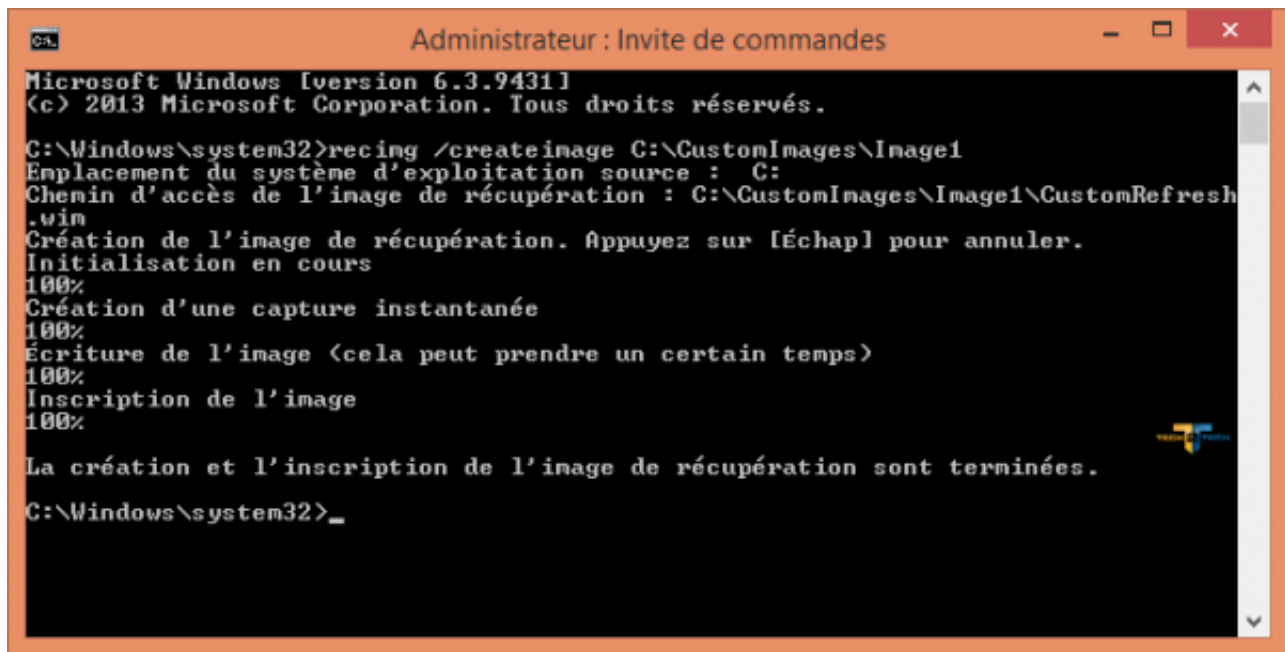
Pour utiliser cet outil, ouvrez une fenêtre d'invite de commande en tant qu'administrateur et exécutez la commande : **SFC / scannow**



```
Administrateur : C:\Windows\system32\cmd.exe
C:\Users\nguillern>SFC /scannow
Début de l'analyse du système. Cette opération peut nécessiter un certain temps.
Démarrage de la phase de vérification de l'analyse du système.
La vérification 100% est terminée.
La protection des ressources Windows a trouvé des fichiers endommagés et a pu
les réparer. Des détails sont fournis dans le journal CBS.Log
windir\Log\CBS\CBS.log. Par exemple C:\Windows\Log\CBS\CBS.log
```

## recimg – créer des images de récupération personnalisée

La [fonction Actualiser votre PC sur Windows 8](#) vous permet de restaurer l'état du système de votre ordinateur à son état d'origine. Vous pouvez créer vos propres images de récupération personnalisées, mais cette fonctionnalité est cachée – vous pouvez le faire grâce à la commande **recimg**. Cela vous permet de supprimer les images installées par défaut par le constructeur, mais surtout de créer vos propres images de récupération avec vos programmes et icônes préinstallés.



```
Administrateur : Invite de commandes
Microsoft Windows [version 6.3.9431]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>recimg /createimage C:\CustomImages\Image1
Emplacement du système d'exploitation source : C:
Chemin d'accès de l'image de récupération : C:\CustomImages\Image1\CustomRefresh
.win
Création de l'image de récupération. Appuyez sur [Échap] pour annuler.
Initialisation en cours
100%
Création d'une capture instantanée
100%
Écriture de l'image (cela peut prendre un certain temps)
100%
Inscription de l'image
100%

La création et l'inscription de l'image de récupération sont terminées.
C:\Windows\system32>_
```

J'avais déjà détaillé un peu plus cette fonction dans un article, [vous pouvez y faire un tour si vous souhaitez un peu plus de détails.](#)

Cette fonction existe seulement pour Windows 8, mais si vous souhaitez [créer vos propres images de récupération sur Windows 7, il y a aussi un article pour ça ici.](#)

## **wbAdmin start backup – Créer une sauvegarde du système**

L'arrivée de Windows 8.1 annonce la suppression de l'interface de sauvegarde de Windows 7. Elle permettait entre autres de créer des images de sauvegarde du système. Ces images système contiennent tout le contenu de votre disque, elles sont donc différentes des images de récupération que l'on a pu voir ci-dessus.

Bien que l'interface graphique ait été supprimée, les admins peuvent toujours créer des sauvegardes d'image système en **exécutant la commande wbadmin dans PowerShell**. Contrairement à toutes les autres commandes ici, **cet outil en ligne de commande doit être exécuté à partir de PowerShell (en admin)**, et non via l'invite de commande.

```
Administrateur : Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

PS C:\Windows\system32>
PS C:\Windows\system32> wbAdmin start backup -backupTarget:e: -include:c: -allCritical
wbAdmin 1.0 - Outil en ligne de commande de sauvegarde
(C) Copyright 2013 Microsoft Corporation. Tous droits réservés.

Récupération des informations de volume...
Cette opération va sauvegarder Réserve au système (350.00 Mo), (C:) sur e:.
Voulez-vous démarrer l'opération de sauvegarde ?
[O] Oui [N] Non O

L'opération de sauvegarde sur E: démarre.
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'une sauvegarde du volume Réserve au système (350.00 Mo) en cours, (7%) copiés.
Création d'une sauvegarde du volume Réserve au système (350.00 Mo) en cours, (99%) copiés.
La sauvegarde du volume Réserve au système (350.00 Mo) a abouti.
Création d'une sauvegarde du volume (C:) en cours, (0%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (2%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (3%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (4%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (5%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (7%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (8%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (9%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (11%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (12%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (13%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (15%) copiés.
```

D'autres idées de commande à intégrer à cet article ? Les commentaires sont là pour ça 😊