

Commande cmd

-
- Gestion des fichiers et des dossiers (cmd,fc,replace....)
 - Command Line Setup(Timeout.....)
 - System Information and Configurations(date.time.....)
 - Applications and Processes(shutdown,tasklist)
 - Network(ipconfig,ip)
 - Tutoriel pour Doskey
 - Carte mental

Exemple 1 : COMP

1. Aide en ligne

Dans l'invite de commandes (cmd) :

```
D:\>COMP /?
Compare le contenu de deux fichiers ou ensembles de fichiers.

COMP [data1] [data2] [/D] [/A] [/L] [/N=chiffre] [/C] [/OFF[LINE]] [/M]

data1    Spécifie l'emplacement et le(s) nom(s) du (des) premier(s) fichier(s) à comparer.
data2    Spécifie l'emplacement et le(s) nom(s) des deuxièmes fichiers à comparer.
/D       Affiche les différences au format décimal.
/A       Affiche les différences en caractères ASCII.
/L       Affiche les numéros de ligne pour les différences.
/N=chiffre Compare uniquement le premier nombre de lignes spécifié dans chaque fichier.
/C       Ignore le cas des lettres ASCII lors de la comparaison de fichiers.
/OFF[LINE] N'ignorez pas les fichiers avec un ensemble d'attributs hors connexion.
/M       Ne pas demander de comparer d'autres fichiers.

Pour comparer des ensembles de fichiers, utilisez des caractères génériques dans les paramètres data1 et data2.
```

Cela affiche la syntaxe, les paramètres optionnels, et des explications d'usage.

2. Fonctionnement

La commande **COMP** compare le contenu de deux fichiers (ou deux ensembles de fichiers) octet par octet. Elle indique les différences (position et nombre d'octets différents). Utile pour vérifier que deux fichiers sont identiques ou repérer où ils divergent.

3. Exemple d'utilisation

```
D:\>COMP texte.txt texte2.txt
Comparaison de texte.txt et texte2.txt...
Les fichiers sont de taille différente.

Comparer d'autres fichiers (O/N) ? N
```

Exemple 2 : FC

1. Aide en ligne

```
D:\>FC /?
Compare deux fichiers ou ensembles de fichiers et affiche les différences
entre eux.

FC [/A] [/C] [/L] [/LBn] [/N][OFF[LINE]][/T] [/U] [/W] [/nnnn]
  [lect1:][chemin1]fichier1 [lect2:][chemin2]fichier2
FC /B [lect1:][chemin1]fichier1 [lect2:][chemin2]fichier2

  /A      Affiche la 1ère et dernière ligne de chaque ensemble de
           différences.
  /B      Effectue une comparaison binaire.
  /C      Ignore la casse.
  /L      Compare les fichiers en tant que texte ASCII.
  /LBn    Définit le nombre maximal de différences consécutives comme égal
           au nombre de lignes spécifié.
  /N      Affiche les numéros de ligne pour une comparaison ASCII.
  /OFF[LINE] Ne pas ignorer les fichiers dont l'attribut hors connexion a été
           réglé.
  /T      Ne convertit pas les tabulations en espaces.
  /U      Compare les fichiers en tant que fichiers texte UNICODE.
  /W      Comprime les blancs (tabulations et espaces) pour la comparaison.
  /nnnn   Spécifie le nombre de lignes consécutives qui doivent
           correspondre après une différence.
  [lect1:][chemin1]fichier1
           Spécifie le premier fichier ou ensemble de fichiers à comparer.
  [lect2:][chemin2]fichier2
           Spécifie le second fichier ou ensemble de fichiers à comparer.
```

2. Fonctionnement

FC (File Compare) compare deux fichiers texte (ou fichiers binaires) et affiche les différences ligne par ligne (pour les fichiers texte). Il est plus orienté “diff” que byte par byte (même s’il peut aussi comparer des fichiers binaires selon les options).

3. Exemple

```
D:\>FC texte.txt texte2.txt
Comparaison des fichiers texte.txt et TEXTE2.TXT
***** texte.txt

***** TEXTE2.TXT
dfqsefgijoeufsehjÛsfqzÛXavier
*****
```

Si les fichiers sont identiques, il affiche “aucune différence”. Sinon, il montre les sections différentes avec les numéros de lignes.

Exemple 3 : REPLACE

1. Aide en ligne

```
D:\>replace /?
Remplace des fichiers.

REPLACE [lect1:][chemin1]fichier [lect2:][chemin2] [/A] [/P] [/R] [/W]
REPLACE [lect1:][chemin1]fichier [lect2:][chemin2] [/P] [/R] [/S] [/W] [/U]

[lect1:][chemin1]fichier Spécifie le ou les fichiers source.
[lect2:][chemin2]       Spécifie le répertoire dont les fichiers
                        sont à remplacer.
/A                       Ajoute nouveaux fichiers au répertoire destination.
                        Inutilisable avec les commutateurs /S ou /U.
/P                       Demande confirmation avant de remplacer un fichier
                        ou d'ajouter un fichier source.
/R                       Remplace les fichiers en lecture seule ainsi que
                        les fichiers non protégés.
/S                       Remplace les fichiers dans tous les sous-répertoires
                        du répertoire destination. Ne peut pas être utilisé
                        avec le commutateur /A.
/W                       Attend insertion d'une disquette avant de commencer.
/U                       Remplace (met à jour) les fichiers plus anciens
                        que les fichiers source. Inutilisable avec /A.
```

2. Fonctionnement

REPLACE permet de remplacer des fichiers dans une arborescence par des fichiers du même nom, venant d'un autre dossier. En gros, “copier / mettre à jour” les fichiers de destination avec les versions plus récentes de la source.

3. Exemple

```
D:\>REPLACE D:\texte\texte.txt D:\remplace
Remplacement de D:\remplace\texte.txt
```

Cela va remplacer les fichiers `.txt` dans `D:\texte` par ceux de `D:\remplace` si les fichiers de la source sont plus récents, ou les copies si elles n'existent pas.

Exemple 4 : ROBOCOPY

1. Aide en ligne

```
D:\>ROBOCOPY /?

-----
ROBOCOPY  ::  Copie de fichiers robuste pour Windows
-----

Début : lundi 29 septembre 2025 13:51:30
Syntaxe :: ROBOCOPY source destination [fichier
           [fichier]...] [options]

           source :: répertoire source (lecteur:\chemin ou
                    \\serveur\partage\chemin).
           destination :: rép. de destination (lecteur:\chemin ou
                    \\serveur\partage\chemin).
           fichier :: fichier(s) à copier (noms/caractères
                    génériques : valeur par défaut "*.*").

::
:: Options de copie :
::
           /S :: copie les sous-répertoires non vides
                uniquement.
           /E :: copie les sous-répertoires, y compris les
                vides.
           /LEV:n :: copie uniquement les n premiers niveaux de
                    l'arborescence source.

           /Z :: copie les fichiers en mode de redémarrage.
           /B :: copie les fichiers en mode de sauvegarde.
           /ZB :: utilise le mode de redémarrage ; si
                  l'accès est refusé, utilise le mode de
                  sauvegarde.
           /J :: copier à l'aide d'E/S non mises en mémoire
                  tampon (recommandé pour les fichiers
                  volumineux).
           /EFSRAW :: copie tous les fichiers chiffrés en mode
                    EFS RAW.
```

2. Fonctionnement

ROBOCOPY (Robust File Copy) est un utilitaire très puissant pour copier des fichiers et arborescences de dossiers, avec des options avancées (copie incrémentielle, reprise, filtrage, options de journalisation, etc.). Il est plus fiable que **xcopy** dans certains cas.

3. Exemple

```
D:\>ROBOCOPY D:\texte D:\remplace /E

-----
ROBOCOPY  ::  Copie de fichiers robuste pour Windows
-----

Début : lundi 29 septembre 2025 13:54:51
Source : D:\texte\
Dest   : D:\remplace\

Fichiers : *.*

Options : *.* /S /E /DCOPY:DA /COPY:DAT /R:1000000 /W:30

-----
100%      Nouveau fichier      2      D:\texte\      30      texte2.txt
          Nouveau rép.        0      D:\texte\
-----

          Total      Copié      IgnoréDiscordance      ÉCHEC      Extras
Rép :           2           1           1           0           0           0
Fichiers :       2           1           1           0           0           0
Octets :       52          30          22           0           0           0
Heures:  0:00:00   0:00:00                                0:00:00   0:00:00

Débit :                1666 Octets/sec.
Débit :                0.095 Méga-octets/min.
Fin : lundi 29 septembre 2025 13:54:51
```

Le paramètre **/E** indique d'inclure les sous-dossiers (y compris les vides).

XCOPY

1. Aide en ligne

Dans l'invite de commandes :

```
D:\>XCOPY /?
Copie des fichiers et des arborescences de répertoires.

XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]
                                [/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]
                                [/K] [/N] [/O] [/X] [/Y] [/Y] [/Z] [/B] [/J]
                                [/EXCLUDE:fich1[+fich2][+fich3]...]

source      Spécifie le ou les fichiers à copier.
destination Spécifie l'emplacement et/ou le nom de nouveaux fichiers.
/A          Copie uniquement les fichiers ayant l'attribut archive, ne
            modifie pas l'attribut.
/M          Copie uniquement les fichiers ayant l'attribut archive,
            désactive l'attribut archive.
/D:j-m-a    Copie les fichiers modifiés à partir de la date spécifiée.
            Si aucune date n'est donnée, copie uniquement les fichiers dont
            l'heure source est plus récente que l'heure de destination.
/EXCLUDE:fich1[+fich2][+fich3]...
            Spécifie une liste de fichiers contenant des chaînes. Chaque
            chaîne doit être placée sur une ligne dans le fichier.
            Lorsque l'une des chaînes est trouvée dans le chemin d'accès
            absolu du fichier devant être copié, ce fichier est exclu de la
            copie. Par exemple, spécifier une chaîne telle que \obj\
            ou .obj exclura respectivement tous les fichiers situés sous
            le répertoire obj ou tous les fichiers dont l'extension
            est .obj.
/P          Confirmer la création de chaque fichier
            de destination.
/S          Copie les répertoires et sous-répertoires à l'exception des
            répertoires vides.
/E          Copie les répertoires et sous-répertoires, y compris les
            répertoires vides.
            Identique à /S /E. Peut être utilisé pour modifier /T.
/V          Vérifie la taille de chaque nouveau fichier.
/W          Vous demande d'appuyer sur une touche avant la copie.
/C          Continuer la copie même si des erreurs se produisent.
/I          Si la destination n'existe pas et que plus d'un fichier est
            copié, considérer la destination comme devant être
            un répertoire.
/Q          N'affiche pas les noms de fichiers lors de la copie.
```

XCOPY (eXtended Copy) est une commande permettant de copier des fichiers, des répertoires et leurs sous-dossiers, y compris les fichiers système et cachés. C'est une version plus avancée de la commande **COPY**.

```
D:\>XCOPY D:\texte D:\texte3
Remplacer D:\texte3 (Oui/Non/Tous)? O
D:\texte\texte.txt
Remplacer D:\texte3 (Oui/Non/Tous)? o
D:\texte\texte2.txt
2 fichier(s) copié(s)
```

TIMEOUT

2. Aide en ligne

Dans l'invite de commandes :

```
D:\>timeout /?

TIMEOUT [/T] délai_d'attente [/NOBREAK]

Description :
    Cet utilitaire accepte un paramètre de délai d'attente qui définit la
    période de temps d'attente (en secondes) ou jusqu'à ce qu'une frappe de
    touche se produise. Il accepte également un paramètre pour ignorer
    l'utilisation d'une touche.

Liste de paramètres :
    /T          délai_maximal Spécifie le nombre de secondes d'attente.
                    La plage valide est comprise entre
                    -1 et 99999 secondes.

    /NOBREAK      Ignorer l'utilisation des touches et attendre le
                    temps indiqué.

    /?           Affiche ce message d'aide.

Remarque : une valeur de délai d'attente égale à -1 signifie qu'une
            frappe de touche est attendue.

Exemples :
    TIMEOUT /?
    TIMEOUT /T 10
    TIMEOUT /T 300 /NOBREAK
    TIMEOUT /T -1
```

Activer Windows
Accédez aux paramètres pour activer Windo

TIMEOUT interrompt temporairement l'exécution d'une commande ou d'un script batch pendant un nombre de secondes donné.

Options :

- **/T [secondes]** : Définit la durée d'attente

```
D:\>TIMEOUT /T 5

Attendre 0 secondes, appuyez sur une touche pour continuer...
```

COLOR

3. Aide en ligne

Dans l'invite de commandes :

```
D:\>color /?
Change les couleurs par défaut du premier plan et de l'arrière-plan de la console.

COLOR [attr]

    attr    Spécifie les attributs de couleurs de l'apparence de la console

Les attributs de couleurs sont spécifiés par DEUX chiffres hexadécimaux -- le
premier correspond à l'arrière-plan, le second au premier plan. Chaque chiffre
peut prendre n'importe quelle de ces valeurs :

    0 = Noir          8 = Gris
    1 = Bleu          9 = Bleu clair
    2 = Vert          A = Vert clair
    3 = Bleu-gris     B = Cyan
    4 = Rouge         C = Rouge clair
    5 = Violet        D = Violet clair
    6 = Jaune         E = Jaune clair
    7 = Blanc         F = Blanc brillant

Si aucun argument n'est donné, cette commande restaure les couleurs
sélectionnées au moment où CMD.EXE a été ouvert. Cette valeur vient soit de la
fenêtre de la console, du commutateur en ligne de commande /T, ou de la valeur
DefaultColor du registre.

La commande COLOR met ERRORLEVEL à 1 si vous tentez de l'exécuter
avec la même couleur pour l'arrière et le premier plan.

Exemple : « COLOR fc » affiche du rouge sur du blanc
```

Activer Windows
Accédez aux paramètres pour activer Windows.

resultat

```
D:\>color a
```

COLOR modifie la couleur du texte et du fond dans la console.

DATE

Aide en ligne

```
D:\>date /?
Affiche ou modifie la date.

DATE [date]

Entrez DATE sans paramètres pour afficher la date système et être invité à la
modifier. Appuyez sur ENTRÉE pour conserver la même date.

Si les extensions de commandes sont activées, la commande DATE prend en charge
le commutateur /T qui fait que la commande n'indique que la date, sans
demander d'en entrer une nouvelle.
Accédez aux paramètres pour activer Windows Defender.
```

DATE permet d'afficher ou de modifier la date du système.

```
D:\>date
La date du jour est : 29/09/2025
Entrez la nouvelle date : (jj-mm-aa) 30-09-2025
```

TIME

Aide en ligne

```
D:\>time /?
Affiche ou modifie l'heure système.

TIME [/T | heure]

TIME sans paramètres affiche l'heure en cours et demande une nouvelle heure.
Appuyez sur ENTRÉE pour conserver la même heure.

Si les extensions de commandes sont activées, la commande TIME prend en charge
le commutateur /T qui fait que la commande n'indique que l'heure, sans
demander d'en entrer une nouvelle.
```

TIME permet d'afficher ou de modifier l'heure système.

```
D:\>time
L'heure actuelle est : 14:24:15,40
Entrez la nouvelle heure : 15
```

DRIVERQUERY

Aide en ligne

```
D:\>driverquery /?
```

DRIVERQUERY [/S système [/U nom_utilisateur [/P [mot_passe]]]]
 [/FO format] [/NH] [/SI] [/V]

Description :
 Permet à un administrateur d'afficher la liste des pilotes de périphériques installés.

Liste de paramètres :

/S	système	Spécifie le système distant auquel se connecter.
/U	[domaine\]utili.	Spécifie le contexte utilisateur dans lequel la commande doit être exécutée.
/P	[mot_passe]	Spécifie le mot de passe pour le contexte utilisateur donné.
/FO	format	Spécifie le type de sortie à afficher. Les valeurs autorisées avec le commutateur sont "TABLE", "LIST" et "CSV".
/NH		Spécifie que l'"en-tête de colonne" ne doit pas être affichée. Valide pour les formats "TABLE" et "CSV" uniquement.
/SI		Affiche des informations sur les pilotes signés.
/V		Affiche les sorties détaillées. Non valide sur les pilotes signés.
/?		Affiche ce message d'aide.

Exemples :

```
DRIVERQUERY
DRIVERQUERY /FO CSV /SI
DRIVERQUERY /NH
DRIVERQUERY /S adresse_IP /U utilisateur /V
DRIVERQUERY /S système /U domaine\utilisateur /P mot_passe /FO LIST
```

Activer Windows
 Activer Windows
 Activer Windows

DRIVERQUERY liste tous les pilotes installés sur le système, avec leurs noms, types, dates de lien, modules utilisés.

```
D:\>driverquery
```

Nom du module	Nom complet	Type de pilote	Link Date
1394ohci	Contrôleur d'hôte comp	Kernel	
3ware	3ware	Kernel	19/05/2015 00:28:03
ACPI	Pilote ACPI Microsoft	Kernel	
AcpiDev	Pilote d'appareils ACP	Kernel	
acpiex	Microsoft ACPIEx Drive	Kernel	
acpipagr	Pilote d'agrégation de	Kernel	
AcpiPmi	Jauge d'alimentation A	Kernel	
acpitime	Pilote d'alarme de sor	Kernel	
ADP80XX	ADP80XX	Kernel	09/04/2015 22:49:48
AFD	Pilote de fonction con	Kernel	
afunix	afunix	Kernel	
ahcache	Application Compatibil	Kernel	
amdgpio2	AMD GPIO Client Driver	Kernel	11/03/2020 12:15:48
amdgpio3	AMD GPIO Client Driver	Kernel	14/03/2016 11:19:36
AmdK8	Pilote de processeur A	Kernel	
amdkmdag	amdkmdag	Kernel	16/08/2019 17:57:18

HOSTNAME

Aide en ligne

```
D:\>hostname /?

Affiche le nom de l'hôte actuel.

hostname
```

HOSTNAME affiche le nom de l'ordinateur (nom de la machine).

```
D:\>hostname
DESKTOP-AJBUS26
```

SYSTEMINFO

Aide en ligne

```
D:\>systeminfo /?
```

SYSTEMINFO [/S système [/U utilisateur [/P mot_de_passe]] [/FO format] [/NH]

Description :

Cet outil affiche les informations de configuration du système d'exploitation pour un ordinateur local ou distant, y compris les niveaux de Service Pack.

Liste de paramètres :

/S	système	Spécifie le système distant auquel se connecter.
/U	[domaine\]utili.	Spécifie le contexte utilisateur sous lequel la commande doit s'exécuter.
/P	[mot_de_passe]	Spécifie le mot de passe pour le contexte utilisateur donné. Est demandé s'il est omis.
/FO	format	Spécifie le format dans lequel la sortie doit être affichée. Valeurs autorisées : "TABLE", "LIST", "CSV".
/NH		Spécifie que les en-têtes de colonnes ne doivent pas apparaître dans la sortie. Valide uniquement pour les formats TABLE et CSV.
/?		Affiche ce message d'aide.

Exemples :

```
SYSTEMINFO
SYSTEMINFO /?
SYSTEMINFO /S système
SYSTEMINFO /S système /U utilisateur
SYSTEMINFO /S système /U domaine\utilisateur /P mot_de_passe /FO TABLE
SYSTEMINFO /S système /FO LIST
SYSTEMINFO /S système /FO CSV /NH
```

Activer Windows
Accédez aux paramètres pour activer Windows.

SYSTEMINFO affiche des informations détaillées sur le système d'exploitation : version de Windows, constructeur, RAM, BIOS, etc.

```
D:\>systeminfo

Nom de l'hôte:                                DESKTOP-AJBUS26
Nom du système d'exploitation:               Microsoft Windows 10 Entreprise LTSC
Version du système:                          10.0.17763 N/A build 17763
Fabricant du système d'exploitation:         Microsoft Corporation
Configuration du système d'exploitation:     Station de travail autonome
Type de build du système d'exploitation:     Multiprocessor Free
Propriétaire enregistré:                     ldv
Organisation enregistrée:
Identificateur de produit:                   00425-00000-00002-AA247
Date d'installation originale:               29/08/2025, 11:52:37
Heure de démarrage du système:               16/09/2025, 16:05:12
Fabricant du système:                        LENOVO
Modèle du système:                           11JAS1J200
Type du système:                             x64-based PC
Processeur(s):                               1 processeur(s) installé(s).
                                              [01] : AMD64 Family 23 Model 24 Stepping
1 AuthenticAMD ~3400 MHz
Version du BIOS:                             LENOVO M3AKT3FA, 19/11/2021
Répertoire Windows:                          C:\Windows
Répertoire système:                          C:\Windows\system32
Périphérique d'amorçage:                     \Device\HarddiskVolume2
Option régionale du système:                 fr;Français (France)
Paramètres régionaux d'entrée:               fr;Français (France)
Fuseau horaire:                              (UTC+01:00) Bruxelles, Copenhagen, Madrid
, Paris
```

VER

Aide en ligne

```
D:\>VER /?
Affiche la version de Windows.

VER
```

VER affiche simplement la version actuelle de Windows.

```
D:\>ver

Microsoft Windows [version 10.0.17763.7792]
```

SHUTDOWN

Aide en ligne

```

D:\>shutdown /?
Syntax : shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o] [/hybrid]
[/soft] [/fw] [/f]
[/m \\ordinateur][t xxx][d [p|u:]xx:yy [/c "commentaire"]]

Sans argument    Afficher l'aide. Cela revient à entrer /?.
/?              Afficher l'aide. Cela revient à n'entrer aucune option.
/i              Afficher l'interface utilisateur graphique (GUI).
                Ce doit être la première option.
/l              Fermer la session. Ne peut pas être utilisé avec l'option /m
                ou /d.
/s              Arrêter l'ordinateur.
/sg             Arrêtez l'ordinateur. Au prochain démarrage,
                redémarrez toutes les applications enregistrées.
/r             Arrêtez complètement l'ordinateur et redémarrez-le.
/g             Redémarrer complètement l'ordinateur. Redémarrer
                redémarré, redémarrez toutes les applications enregistrées.
/a             Annuler un arrêt du système.
                Utilisable uniquement pendant le délai imparti.
                Regrouper avec /fw pour effacer tout démarrage en attente vers le microprogramme.
/p             Arrêter l'ordinateur local sans délai d'expiration ou
                avertissement.
                Peut être utilisé avec les options /d et /f.
/h             Mettre l'ordinateur local en veille prolongée.
                Utilisable avec l'option /f.
/hybrid        Arrête l'ordinateur et le prépare pour un démarrage rapide.
                Doit être utilisé avec l'option /s.
/fw            S'associe à l'option d'arrêt pour transférer le prochain démarrage vers un autre ordinateur.
                Accédez aux paramètres pour activer Windows.
/e             l'interface utilisateur du microprogramme.
                Documenter la raison de l'arrêt inattendu d'un ordinateur.

```

SHUTDOWN permet d'arrêter, redémarrer ou déconnecter un ordinateur local ou distant. On peut aussi planifier un arrêt dans quelques secondes, forcer la fermeture des applications, ou annuler un arrêt déjà programmé.

```
D:\>SHUTDOWN /S
```

```
D:\>SHUTDOWN /A
```

TASKLIST

Aide en ligne

```
D:\>tasklist /?
```

TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]
 [/M [module] | /SVC | /V] [/FI filtre] [/FO format] [/NH]

Description :
 Cet outil affiche une liste des processus actuellement en cours sur un ordinateur local ou un ordinateur distant.

Liste de paramètres :

/S	système	Spécifie le système distant auquel se connecter.
/U	[domaine\]utili.	Spécifie le contexte utilisateur sous lequel la commande doit exécuter.
/P	[mot_passe]	Spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
/M	[module]	Liste toutes les tâches utilisant le nom de fichier exe ou dll donné. Si le nom de module n'est pas spécifié, tous les modules chargés sont affichés.
/SVC		Affiche les services hébergés dans chaque processus.
/APPS		Afficher les applications du Store et leurs processus associés.
/V		Affiche les informations de tâches détaillées.
/FI	filtre	Affiche un ensemble de tâches qui correspond au critère spécifié par le filtre.

Accédez aux paramètres pour activer Windows.

TASKLIST affiche tous les processus actuellement en cours sur la machine, avec leur nom, leur PID (identifiant), l'utilisation mémoire, etc. Cela permet d'identifier ce qui tourne en arrière-plan.

Options utiles :

- **/V** : informations détaillées


```
D:\>tasklist
```

Nom de l'image	PID	Nom de la session	Numéro de s	Utilisation
System Idle Process	0	Services	0	8 Ko
System	4	Services	0	3 868 Ko
Registry	96	Services	0	14 948 Ko
smss.exe	368	Services	0	400 Ko
csrss.exe	496	Services	0	2 776 Ko
wininit.exe	612	Services	0	2 964 Ko
services.exe	756	Services	0	7 412 Ko
lsass.exe	796	Services	0	11 604 Ko
svchost.exe	912	Services	0	1 176 Ko
fontdrvhost.exe	948	Services	0	1 312 Ko
svchost.exe	964	Services	0	15 084 Ko
svchost.exe	428	Services	0	10 576 Ko
svchost.exe	624	Services	0	3 884 Ko
svchost.exe	1052	Services	0	4 656 Ko
svchost.exe	1084	Services	0	4 748 Ko
svchost.exe	1160	Services	0	14 580 Ko
atiesrxx.exe	1356	Services	0	2 108 Ko
svchost.exe	1392	Services	0	5 776 Ko
svchost.exe	1444	Services	0	9 300 Ko
svchost.exe	1460	Services	0	3 752 Ko
svchost.exe	1508	Services	0	6 012 Ko
svchost.exe	1520	Services	0	2 572 Ko
svchost.exe	1640	Services	0	8 612 Ko
svchost.exe	1672	Services	0	4 404 Ko
svchost.exe	1688	Services	0	5 436 Ko
svchost.exe	1696	Services	0	5 076 Ko
svchost.exe	1724	Services	0	1 704 Ko
Memory Compression	1836	Services	0	1 148 Ko
svchost.exe	1880	Services	0	5 016 Ko
svchost.exe	1936	Services	0	5 668 Ko

TASKKILL

Aide en ligne

```
D:\>taskkill /?
```

TASKKILL [/S système] [/U utilisateur [/P [mot_passe]]]
 { [/FI filtre] [/PID ID_processus | /IM image] } [/T] [/F]

Description :
 Cet outil est utilisé pour arrêter des tâches par id de processus (PID) ou nom d'image.

Liste de paramètres :

- /S système** Spécifie le système distant auquel se connecter.
- /U [domaine\]utili.** Spécifie le contexte utilisateur sous lequel la commande doit s'exécuter.
- /P [mot_de_passe]** Spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
- /FI filtre** Applique un filtre pour sélectionner un ensemble de tâches. Permet à "*" d'être utilisé. Par exemple, imagename eq test*
- /PID ID_processus** Spécifie le PID du processus à arrêter. Utilisez Tasklist afin d'obtenir le PID.
- /IM nom_image** Spécifie le nom d'image du processus à terminer. Le caractère générique '*' peut être utilisé pour spécifier toutes les tâches ou les noms d'images.
- /T** Met fin au processus spécifié et tous les processus enfants qu'il a démarrés.
- /F** Force les processus à se terminer.

taskkill permet d'arrêter une opération

```
D:\> TASKKILL /IM firefox.exe /F
Opération réussie : le processus "firefox.exe" de PID 10556 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 7404 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 6456 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 9264 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 9340 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 4172 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 7156 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 4196 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 12200 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 7920 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 10692 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 11424 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 8888 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 3040 a été arrêté.
Opération réussie : le processus "firefox.exe" de PID 7120 a été arrêté.
```

IPCONFIG

- **Fonction** : Affiche les informations des interfaces réseau (adresse IP, masque de sous-réseau, passerelle, etc.)
- **Utilité** : Vérifier la configuration réseau de l'ordinateur.

```
D:\>ipconfig /?
```

UTILISATION :

```
ipconfig [/allcompartments] [/? | /all |
    /renew [carte] | /release [carte] |
    /renew6 [carte] | /release6 [carte] |
    /flushdns | /displaydns | /registerdns |
    /showclassid carte |
    /setclassid carte [ID_classe] |
    /showclassid6 carte |
    /setclassid6 carte [ID_classe] ]
```

où

carte Nom de connexion
(caractères génériques * et ? autorisés, voir les
exemples)

Options :

/?	Affiche ce message d'aide
/all	Affiche toutes les informations de configuration.
/release	Libère l'adresse IPv4 pour la carte spécifiée.
/release6	Libère l'adresse IPv6 pour la carte spécifiée.
/renew	Renouvelle l'adresse IPv4 pour la carte spécifiée.
/renew6	Renouvelle l'adresse IPv6 pour la carte spécifiée.
/flushdns	Purge le cache de résolution DNS.
/registerdns	Actualise tous les baux DHCP et réenregistre les noms DNS
/displaydns	Affiche le contenu du cache de résolution DNS.
/showclassid	Affiche tous les ID de classe DHCP autorisés pour la carte.
/setclassid	Modifie l'ID de classe DHCP.
/showclassid6	Affiche tous les ID de classe DHCP IPv6 autorisés pour

```
D:\>ipconfig
```

Configuration IP de Windows

Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . . : fe80::d7fb:d736:be8a:3be8%8
Adresse IPv4. . . . . : 172.30.15.1
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 172.30.255.254
```

PING [adresse]

- **Fonction** : Envoie des requêtes ICMP pour tester la connectivité avec un autre hôte.
- **Utilité** : Vérifier si un hôte est accessible (test de connexion réseau). -t option ne s'arrête pas ip du serveur google 8.8.8.8

```
D:\>ping /?

Utilisation : ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
               [-r count] [-s count] [[-j host-list] | [-k host-list]]
               [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
               [-4] [-6] nom_cible

Options :
  -t           Effectue un test ping sur l'hôte spécifié jusqu'à son arrêt.
                Pour afficher les statistiques et continuer,
                appuyez sur Ctrl+Attn.
                Pour arrêter, appuyez sur Ctrl+C.
  -a           Résout les adresses en noms d'hôtes.
  -n count     Nombre de demandes d'écho à envoyer.
  -l size      Taille du tampon d'envoi.
  -f           Active l'indicateur Ne pas fragmenter dans le paquet (IPv4
                uniquement).
  -i TTL       Durée de vie.
  -v TOS       Type de service (IPv4 uniquement. La
                configuration de ce paramètre n'a aucun effet sur le type
                de service dans l'en-tête IP).
  -r count     Itinéraire d'enregistrement du nombre de sauts (IPv4
                uniquement).
  -s count     Horodatage du nombre de sauts (IPv4 uniquement).
  -j host-list Itinéraire source libre parmi la liste d'hôtes (IPv4
                uniquement).
  -k host-list Itinéraire source strict parmi la liste d'hôtes (IPv4
                uniquement).
  -w timeout   Délai d'attente pour chaque réponse, en millisecondes.
  -R           Utilise l'en-tête de routage pour tester également
                l'itinéraire inverse (IPv6 uniquement).
                D'après la RFC 5095, l'utilisation de cet en-tête de routage
                est déconseillée. Certains systèmes peuvent supprimer des
                demandes d'écho si cet en-tête est utilisé.
  -S srcaddr   Adresse source à utiliser.
  -c compartment Identificateur de compartiment de routage.
  -p           Effectue un test ping sur l'adresse de fournisseur
```

```
D:\>ping -t
Une adresse IP doit être spécifiée.

D:\>ping 8.8.8.8 -t

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=299 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=622 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=573 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=609 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=309 ms TTL=115
```

GETMAC

- **Fonction** : Affiche l'adresse MAC (physique) de la carte réseau.
- **Utilité** : Identifier un appareil sur un réseau local.

```
D:\>GETMAC /?
```

```
GETMAC [/S système [/U nom_utilisateur [/P [mot_de_passe]]]] [/FO format]
      [/NH] [/V]
```

Description :

Cet outil permet à un administrateur d'afficher l'adresse MAC des cartes réseaux d'un ordinateur.

Liste de paramètres :

/S	système	Spécifie le système distant auquel se connecter.
/U	[domaine\]utili.	Spécifie le contexte utilisateur sous lequel la commande doit s'exécuter.
/P	[mot_de_passe]	Spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
/FO	format	Spécifie le format dans lequel la sortie doit être affichée. Valeurs autorisées : "TABLE", "LIST", "CSV".
/NH		Spécifie que les en-têtes de colonnes ne doivent pas apparaître dans la sortie. N'est valide que pour les formats TABLE et CSV.
/V		Détaille l'affichage des résultats.
/?		Affiche cet écran d'aide.

Exemples :

```
GETMAC /?
GETMAC /FO csv
GETMAC /S système /NH /V
GETMAC /S système /U utilisateur
GETMAC /S système /U domaine\utilisateur /P mot_de_passe /FO list /V
GETMAC /S système /U domaine\utilisateur /P mot_de_passe /FO table /NH
```

```
D:\>getmac
```

Adresse physique	Nom du transport
88-AE-DD-1C-1E-5C	N/A

Accédez aux paramètres pour activer Windows.

NETSTAT

- **Fonction** : Affiche les connexions réseau actives, les ports à l'écoute, les statistiques réseau.
- **Utilité** : Diagnostiquer les connexions réseau ou repérer des connexions suspectes.

```
D:\>netstat /?
```

Affiche les statistiques de protocole et les connexions réseau TCP/IP actuelles

```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
```

-a Affiche toutes les connexions et tous les ports d'écoute.
-b Affiche l'exécutable impliqué dans la création de chaque connexion ou port d'écoute. Dans certains cas, des exécutables reconnus hébergent plusieurs composants indépendants, et la séquence des composants impliqués dans la création de la connexion ou du port d'écoute s'affiche alors. Dans ce cas, le nom de l'exécutable se trouve dans [] en bas, au-dessus du composant qu'il a appelé, et ainsi de suite jusqu'à ce que TCP/IP soit atteint. Notez que cette option peut être très longue et qu'elle est susceptible d'échouer si vous n'avez pas d'auto
-e Affiche des statistiques Ethernet. Cette option peut être combinée avec l'option -s.
-f Affiche les noms de domaine complets (FQDN) pour des adresses étrangères.
-n Affiche des adresses et numéros de ports en format numérique.
-o Affiche l'identificateur du processus propriétaire associé à chaque connexion.
-p proto Affiche les connexions pour le protocole spécifié par proto ; proto peut être l'une des valeurs suivantes : TCP, UDP, TCPv6 ou UDPv6. S'il est utilisé avec l'option -s pour afficher les statistiques par protocole, le protocole peut être l'une des valeurs suivantes : IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6.

```
D:\>netstat -an
```

Connexions actives

Proto	Adresse locale	Adresse distante	État
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	127.0.0.1:58859	127.0.0.1:58860	ESTABLISHED
TCP	127.0.0.1:58860	127.0.0.1:58859	ESTABLISHED
TCP	127.0.0.1:58861	127.0.0.1:58862	ESTABLISHED
TCP	127.0.0.1:58862	127.0.0.1:58861	ESTABLISHED
TCP	172.30.15.1:139	0.0.0.0:0	LISTENING
TCP	172.30.15.1:58879	172.16.63.130:3128	ESTABLISHED
TCP	172.30.15.1:58930	172.16.63.130:3128	ESTABLISHED
TCP	172.30.15.1:58935	172.16.63.130:3128	ESTABLISHED
TCP	172.30.15.1:58954	172.16.63.130:3128	ESTABLISHED
TCP	172.30.15.1:58955	172.16.63.130:3128	ESTABLISHED
TCP	172.30.15.1:58956	172.16.63.130:3128	ESTABLISHED
TCP	172.30.15.1:58957	172.16.63.130:3128	ESTABLISHED
TCP	:::135	:::0	LISTENING
TCP	:::445	:::0	LISTENING
TCP	:::49664	:::0	LISTENING
TCP	:::49665	:::0	LISTENING
TCP	:::49666	:::0	LISTENING
TCP	:::49667	:::0	LISTENING

Ici

-a : affiche toutes les connexions

`-n` : affiche les adresses et ports sous forme numérique

II. Tutoriel pour DOSKEY

DOSKEY est un utilitaire intégré à Windows qui permet :

Rappel de commandes précédentes (historique),

Édition rapide de la ligne de commande,

Création de macros (raccourcis personnalisés pour des commandes longues),

Automatisation de tâches répétitives.

II. Commandes de base

`doskey /history` — Affiche l'historique des commandes tapées dans la session actuelle.

`doskey macross` — Affiche toutes les macros définies.

`doskey /reinstall` — Recharge DOSKEY

`doskey /listsize=N` — Définit le nombre maximal de commandes en historique.

III. Rappel d'historique

Flèche ↑ : Rappelle la commande précédente.

Flèche ↓ : Rappelle la commande suivante.

Définition d'une macro simple

`doskey nom_macro=commande`

doskey a=cls

a chaque fois que vous tapez A cela permet de faire un cls un clear

Conclusion

Le tp est long mais simple juste il faut bien comprendre mais pratique pour réviser les commandes.

Carte mental
Voir plus