

Commandes CMD Essentielles du Support Informatique

Ce TD a pour but de familiariser les étudiants avec les commandes essentielles de l'invite de commandes Windows (CMD) utilisées quotidiennement en support informatique : diagnostic système, dépannage réseau, gestion des utilisateurs, réparation et gestion de session. Chaque section présente des commandes clés suivies d'exercices d'application.

1. Information et Diagnostic du Système

Ces commandes permettent de collecter des informations sur la configuration matérielle, logicielle et l'état général du poste.

Commande	Fonction
SYSTEMINFO	<p>Affiche des informations détaillées sur l'OS, les mises à jour et la configuration matérielle.</p> <pre>C:\Users\etudinfo>systeminfo Nom de l'hôte: DESKTOP-RN4VDBF Nom du système d'exploitation: Microsoft Windows 10 Professionnel Version du système: 18.0.19045 M/A build 19045 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: Utilisateur Windows Organisation enregistrée: Identificateur de produit: 00330-51044-09659-AADEM Date d'installation originale: 05/12/2025, 10:00:41 Heure de démarrage du système: 06/12/2025, 17:39:05 Fabricant du système: HP Modèle du système: HP ProDesk 400 G4 SFF Type du système: x64-based PC Processeur(s): 1 processeur(s) installé(s). [01] : Intel64 Family 6 Model 158 Stepping 9 GenuineIntel ~3408 MHz Version du BIOS: HP P08 Ver. 02.49, 08/12/2023 Répertoire Windows: C:\Windows Répertoire système: C:\Windows\System32 Périphérique d'amorçage: \Device\HarddiskVolume1 Option régionale du système: fr;Français (France) Paramètres régionaux d'entrée: fr;Français (France) Fuseau horaire: (UTC+01:00) Bruxelles, Copenhague, Madrid, Paris Mémoire physique totale: 16 275 Mo Mémoire physique disponible: 10 309 Mo Mémoire virtuelle : taille maximale: 19 219 Mo Mémoire virtuelle : disponible: 13 439 Mo Mémoire virtuelle : en cours d'utilisation: 5 708 Mo Emplacements des fichiers d'échange: C:\pagefile.sys Domaine: WORKGROUP Serveur d'ouverture de session: \\DESKTOP-RN4VDBF Correctif(s): 11 Corrections installées.</pre>
HOSTNAME	<p>Affiche le nom du poste local.</p> <pre>C:\Users\etudinfo>hostname DESKTOP-RN4VDBF</pre>
TASKLIST	Liste l'ensemble des processus en cours d'exécution.

```
C:\Users\etudinfo>tasklist

Nom de l'image                                PID Nom de la sessio Numéro de s Utilisation
=====
System Idle Process                          0 Services 0 8 Ko
System                                        4 Services 0 328 Ko
Registry                                     108 Services 0 42 624 Ko
smss.exe                                     392 Services 0 516 Ko
csrss.exe                                    540 Services 0 3 036 Ko
wininit.exe                                 624 Services 0 2 384 Ko
csrss.exe                                    632 Console 1 4 664 Ko
services.exe                                700 Services 0 8 672 Ko
winlogon.exe                                728 Console 1 8 144 Ko
lsass.exe                                   772 Services 0 19 016 Ko
svchost.exe                                908 Services 0 26 768 Ko
fontdrvhost.exe                             944 Console 1 17 472 Ko
fontdrvhost.exe                             936 Services 0 2 716 Ko
svchost.exe                                 356 Services 0 15 288 Ko
svchost.exe                                 488 Services 0 5 080 Ko
dwm.exe                                     1120 Console 1 103 020 Ko
svchost.exe                                 1132 Services 0 14 612 Ko
svchost.exe                                 1148 Services 0 7 648 Ko
svchost.exe                                 1272 Services 0 3 416 Ko
svchost.exe                                 1284 Services 0 4 976 Ko
svchost.exe                                 1312 Services 0 6 052 Ko
svchost.exe                                 1400 Services 0 4 468 Ko
svchost.exe                                 1424 Services 0 6 920 Ko
igfxCUIService.exe                          1536 Services 0 6 044 Ko
svchost.exe                                 1612 Services 0 8 404 Ko
svchost.exe                                 1628 Services 0 12 700 Ko
svchost.exe                                 1648 Services 0 10 932 Ko
svchost.exe                                 1660 Services 0 2 728 Ko
svchost.exe                                 1668 Services 0 11 032 Ko
svchost.exe                                 1744 Services 0 2 760 Ko
svchost.exe                                 1816 Services 0 3 984 Ko
svchost.exe                                 1824 Services 0 3 592 Ko
Memory Compression                          1860 Services 0 45 108 Ko
svchost.exe                                 1984 Services 0 7 364 Ko
svchost.exe                                 2056 Services 0 2 476 Ko
svchost.exe                                 2168 Services 0 10 680 Ko
svchost.exe                                 2244 Services 0 4 476 Ko
svchost.exe                                 2308 Services 0 8 328 Ko
svchost.exe                                 2364 Services 0 6 360 Ko
svchost.exe                                 2408 Services 0 11 796 Ko
svchost.exe                                 2500 Services 0 5 892 Ko
```

Testez les commandes suivantes

2. Dépannage Réseau

Commandes recourues pour analyser la connectivité et les flux réseau.

Commande	Fonction
PING	Teste la connectivité réseau vers une machine. Envoi d'une requête 'ping' sur riot.de [151.101.67.7] avec 32 octets de données : Réponse de 151.101.67.7 : octets=32 temps=29 ms TTL=52 Réponse de 151.101.67.7 : octets=32 temps=35 ms TTL=52 Réponse de 151.101.67.7 : octets=32 temps=67 ms TTL=52 Réponse de 151.101.67.7 : octets=32 temps=33 ms TTL=52 Réponse de 151.101.67.7 : octets=32 temps=33 ms TTL=52

TRACERT

Montre les routeurs traversés jusqu'à une destination.

```
Détermination de l'itinéraire vers riot.de [151.101.131.7]
avec un maximum de 30 sauts :

 1  <1 ms  <1 ms  <1 ms  192.168.28.253
 2  <1 ms  <1 ms  <1 ms  10.96.9.245
 3  10 ms  10 ms  10 ms  172.18.128.93
 4  10 ms  10 ms  10 ms  10.251.0.3
 5  22 ms  26 ms  31 ms  routeur-upjv.ac-amiens.fr [195.221.156.15]
 6  12 ms  14 ms  16 ms  194.167.1.185
 7  17 ms  21 ms  25 ms  vl221-be2-ren-nr-compiegne-rtr-091.noc.renater.fr [193.51.181.190]
 8  21 ms  25 ms  20 ms  xe-0-0-8-ren-nr-paris2-rtr-131.noc.renater.fr [193.51.177.206]
 9  18 ms  19 ms  15 ms  et-5-0-1-ren-nr-paris1-rtr-131.noc.renater.fr [193.55.204.194]
10  22 ms  22 ms  23 ms  renater-ias-geant-gw.par.fr.geant.net [83.97.89.9]
11  *      *      *      Délai d'attente de la demande dépassé.
12  *      *      *      Délai d'attente de la demande dépassé.
13  29 ms  29 ms  28 ms  151.101.131.7

Itinéraire déterminé.
```

IPCONFIG /ALL

Affiche la configuration réseau complète (DNS, IP, MAC...).

```
C:\Users\etudinfo>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : DESKTOP-RN4VDBF
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: sio.loc

Carte Ethernet Ethernet :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
    Description. . . . . : Intel(R) Ethernet I210-T1 GbE NIC
    Adresse physique . . . . . : 68-05-CA-80-2D-1E
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . : sio.loc
    Description. . . . . : Realtek PCIe GbE Family Controller
    Adresse physique . . . . . : 18-60-24-F4-CF-28
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
```

NETSTAT -ANO

Affiche les connexions actives, les ports d'écoute et les PIDs associés.

```
C:\Users\etudinfo>netstat -ano

Connexions actives

    Proto  Adresse locale          Adresse distante        État           PID
    ---
    TCP    0.0.0.0:135              0.0.0.0:0               LISTENING      356
    TCP    0.0.0.0:445              0.0.0.0:0               LISTENING      4
    TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING      4860
    TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING      4
    TCP    0.0.0.0:49664            0.0.0.0:0               LISTENING      772
    TCP    0.0.0.0:49665            0.0.0.0:0               LISTENING      624
    TCP    0.0.0.0:49666            0.0.0.0:0               LISTENING      1132
    TCP    0.0.0.0:49667            0.0.0.0:0               LISTENING      1668
    TCP    0.0.0.0:49668            0.0.0.0:0               LISTENING      2724
    TCP    0.0.0.0:49669            0.0.0.0:0               LISTENING      700
    TCP    192.168.28.54:139        0.0.0.0:0               LISTENING      4
    TCP    192.168.28.54:49925      98.66.133.185:443       ESTABLISHED    3140
    TCP    192.168.28.54:50147      96.17.207.157:443       CLOSE_WAIT     2876
    TCP    192.168.28.54:50149      23.51.98.7:80           CLOSE_WAIT     2876
    TCP    192.168.28.54:50153      23.200.87.15:443        CLOSE_WAIT     2876
    TCP    192.168.28.54:50154      23.46.189.219:80        CLOSE_WAIT     2876
    TCP    192.168.28.54:50155      96.17.207.145:443       CLOSE_WAIT     2876
    TCP    192.168.28.54:50156      96.17.207.145:443       CLOSE_WAIT     2876
    TCP    192.168.28.54:50157      96.17.207.145:443       CLOSE_WAIT     2876
    TCP    192.168.28.54:50158      96.17.207.145:443       CLOSE_WAIT     2876
    TCP    192.168.28.54:50159      96.17.207.145:443       CLOSE_WAIT     2876
    TCP    192.168.28.54:50160      23.200.87.23:443        CLOSE_WAIT     2876
```

ARP -A

Affiche le cache ARP (association IP ↔ MAC).

	Interface : 192.168.28.54 --- 0xa		
	Adresse Internet	Adresse physique	Type
	192.168.28.38	18-60-24-f4-ce-ec	dynamique
	192.168.28.42	18-60-24-f4-d0-20	dynamique
	192.168.28.43	18-60-24-f4-ce-6f	dynamique
	192.168.28.44	18-60-24-f4-cf-35	dynamique
	192.168.28.51	18-60-24-f4-cf-9e	dynamique
	192.168.28.53	18-60-24-f4-ce-bf	dynamique
	192.168.28.63	18-60-24-f4-ce-f3	dynamique
	192.168.28.64	18-60-24-f4-ce-9c	dynamique
	192.168.28.71	68-05-ca-80-27-ef	dynamique
	192.168.28.73	18-60-24-f4-cc-a4	dynamique
	192.168.28.74	18-60-24-f4-cf-59	dynamique
	192.168.28.92	68-05-ca-80-2d-dc	dynamique
	192.168.28.114	68-05-ca-80-2d-be	dynamique
	192.168.28.250	70-5a-0f-0e-f6-a9	dynamique
	192.168.28.251	a0-21-b7-c2-0d-5a	dynamique
	192.168.28.253	00-0c-29-a6-ae-f4	dynamique
	192.168.28.255	ff-ff-ff-ff-ff-ff	statique
	224.0.0.2	01-00-5e-00-00-02	statique
	224.0.0.22	01-00-5e-00-00-16	statique
	224.0.0.251	01-00-5e-00-00-fb	statique
	224.0.0.252	01-00-5e-00-00-fc	statique
	239.255.255.250	01-00-5e-7f-ff-fa	statique
	255.255.255.255	ff-ff-ff-ff-ff-ff	statique

Testez les commandes suivantes

3. Gestion des Utilisateurs et de la Sécurité

Commandes utilisées pour l’administration locale des comptes.

Commande	Fonction
NET USER	<p>Affiche les utilisateurs locaux ou permet d’en ajouter/supprimer.</p> <pre> C:\Users\etudinfo>net user comptes d'utilisateurs de \\DESKTOP-RN4VDBF ----- Administrateur DefaultAccount etudinfo Invité WDAGUtilityAccount La commande s'est terminée correctement. </pre>
NET LOCALGROUP ADMINISTRATORS	<p>Ajoute un utilisateur au groupe Administrateurs</p> <pre> C:\Users\etudinfo>net localgroup administrateurs Nom alias administrateurs Commentaire Les membres du groupe Administrateurs disposent d'un accès complet et Membres ----- Administrateur etudinfo La commande s'est terminée correctement. C:\Users\etudinfo> </pre>
WHOAMI	Affiche l'utilisateur actuellement connecté ainsi que son domaine.

```
C:\Users\etudinfo>whoami
desktop-rn4vdbf\etudinfo
```

Testez les commandes suivantes

4. Réparation Système et Gestion des Processus

Commandes destinées à vérifier l'intégrité du système ou à gérer des processus problématiques.

Commande	Fonction	Testez les
CHKDSK /F	Analyse et répare les erreurs sur un disque.	
SFC /SCANNOW	Vérifie et répare les fichiers système corrompus.	
TASKKILL /PID	Termine un processus en fonction de son identifiant (PID).	
TREE	Affiche la structure des répertoires en arborescence. <pre>C:\Users\etudinfo>tree Structure du dossier pour le volume SI01 Le numéro de série du volume est 041B-F488 C:. ├── 3D Objects ├── Contacts ├── Desktop ├── Documents ├── Downloads ├── Favorites │ └── Links ├── Links ├── Music ├── OneDrive ├── Pictures │ ├── Camera Roll │ └── Saved Pictures ├── Saved Games ├── Searches ├── Videos │ └── Captures</pre>	

commandes suivantes

5. Gestion de Session et Accès à Distance

Commandes utiles pour les tâches d'administration à distance ou la gestion de session.

Commande	Fonction
MSTSC	Ouvre l'interface de Connexion Bureau à Distance.
SHUTDOWN /f	Lance une boîte de dialogue de redémarrage/arrêt à distance.
LOGOFF	Déconnecte l'utilisateur actuel.

NET USE	Mappe ou démonte un lecteur réseau.
----------------	-------------------------------------

Exemple

Mapper le partage \\SERVEUR\PARTAGE sur la lettre Z:

~~NET USE Z: \\SERVEUR\PARTAGE~~

Exercices

1. Diagnostic et Information

Situation :

Un professeur signale que son ordinateur est « extrêmement lent » et démarre anormalement. Avant d'envisager un remplacement ou une opération lourde, vous souhaitez vérifier **les processus en cours**, afin d'identifier une éventuelle surcharge CPU ou un programme bloqué.

Question :

Quelle commande utilisez-vous pour **répertorier l'ensemble des processus actuellement actifs** sur le poste afin d'effectuer un premier diagnostic ?

J'utilise la commande `tasklist`

2. Dépannage Réseau & Authentification

Situation :

Un utilisateur n'arrive plus à accéder à son dossier personnel sur le serveur et pense « ne pas être reconnu par le domaine ».

Avant de vérifier côté Active Directory, vous devez d'abord confirmer **le compte réellement utilisé** par la session, ainsi que le domaine auquel il appartient.

Question :

Quelle commande permet d'afficher **l'utilisateur connecté** ainsi que **le domaine de connexion** ?

J'utilise la commande `whoami` afin de voir l'utilisateur connecté et le domaine de connexion

3. Analyse Réseau et Sécurité

Situation :

Vous suspectez qu'un programme inconnu utilise un **port réseau critique** sur un poste d'un utilisateur.

Pour identifier précisément ce processus, vous devez examiner les **connexions actives**, les **ports ouverts**, et les **PIDs associés** afin de déterminer quel logiciel occupe ce port.

Question :

Quelle commande permet d'obtenir, en une seule fois, la **liste des connexions actives**, les **ports d'écoute**, et les **processus correspondants** ?

`netstat -ano`

5. Administration des Comptes Utilisateurs

Situation :

Un ancien employé du lycée ou de l'entreprise quitte définitivement l'établissement. Conformément aux procédures internes, son compte local doit être **supprimé** des postes Windows concernés.

Question :

Quelle commande supprime le compte local nommé **ancienemploye** ?

`net user ancienemploye /delete`

6. Identification du Poste dans un Parc Informatique

Situation :

Tu dois inventorier rapidement les postes d'une salle informatique pour préparer une mise à jour Windows.

Avant de lancer le script automatisé, tu dois relever **le nom de la machine** afin de t'assurer que tu opères sur le bon poste.

Question :

Quelle commande permet d'afficher le nom du poste sur lequel vous êtes connecté ?

`hostname`

7. Vérification Complète de la Configuration Réseau

Situation :

Un élève n'arrive plus à imprimer depuis son poste. Tu suspectes une mauvaise configuration réseau (DNS ou passerelle).

Pour confirmer tes soupçons, tu dois examiner **l'intégralité** de la configuration réseau du PC.

Question :

Quelle commande permet d'afficher l'ensemble des paramètres réseau (adresse IP, DNS, passerelle, MAC, etc.) ?

`ipconfig /all`

8. Analyse du Chemin Réseau vers un Serveur

Situation :

Le serveur pédagogique srv-pedago semble répondre très lentement à certains utilisateurs.

Tu dois déterminer si un routeur intermédiaire provoque une latence anormale.

Question :

Quelle commande affiche **toutes les étapes** (sauts) traversées par les paquets pour atteindre une machine distante ?

tracert

9. Vérification de l'intégrité du système

Situation :

Une machine présente des erreurs étranges et certains services refusent de démarrer. Tu suspectes un fichier système corrompu.

Question :

Quelle commande analyse l'intégrité des fichiers système et tente de les réparer automatiquement ?

sfc /scannow

10. Détection d'erreurs sur un disque

Situation :

Un professeur se plaint d'erreurs répétées lors de l'enregistrement de documents. Avant de remplacer le disque, tu veux réaliser une **analyse et réparation automatique** du volume.

Question :

Quelle commande permet d'analyser le disque C: et de réparer les erreurs détectées ?

chkdsk /f

Script 1 : Audit rapide d'un poste utilisateur

Réaliser un diagnostic express d'un poste Windows afin d'identifier les principales causes de lenteur ou d'anomalies réseau.

Aucune interaction utilisateur (script autonome).

Le script doit afficher

- Affichage de l'utilisateur connecté.
- Liste des processus lourds.
- Liste des partages réseau montés.
- Connexions réseau établies (pour suspicion malware).

```
@echo off
echo utilisateur connecté
whoami
```

```
echo liste des processus lourds
tasklist /fo table
```

```
echo Liste des partages réseau montés
net use
```

```
echo Connexion réseaux établis
netstat -ano
```

```
echo Fin du diagnostic
```

```
pause
```

Script 2 : Onboarding utilisateur

Automatiser la création d'un nouvel utilisateur local et la configuration initiale de son environnement réseau.

Déploiement de nouveaux employés ou stagiaires dans une PME ou un établissement scolaire nécessitant un onboarding rapide.

Le script saisie les données suivantes :

- Nom du nouvel utilisateur.
- Mot de passe temporaire.

Le script doit effectuer :

- La création du compte.
- L'Ajout à un groupe spécifique.
- Le montage automatique du lecteur réseau personnel.

```
@echo off
```

```
set /p username=Nom utilisateur :
```

```
set /p password=Mot de passe :
```

```
net user %username% %password% /add
```

```
net localgroup Utilisateurs %username% /add
```

```
net use Z: \\SERVEUR\Dossiers\%username% /persistent:yes
```

