

## 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
<b>SYSTEMINFO</b>	Affiche des informations détaillées sur l'OS, les mises à jour et la configuration matérielle.
<b>HOSTNAME</b>	Affiche le nom du poste local.
<b>TASKLIST</b>	Liste l'ensemble des processus en cours d'exécution.

Testez les commandes suivantes : `systeminfo` :

Nom de l'hôte: PCV4  
Nom du système d'exploitation: Microsoft Windows 10 Professionnel  
Version du système: 10.0.19045 N/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: 00330-51044-69447-AAOEM  
Date d'installation originale: 13/06/2024, 11:08:15  
Heure de démarrage du système: 04/12/2025, 14:09:55  
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  
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, Copenhagen, Madrid, P  
Mémoire physique totale: 16 275 Mo  
Mémoire physique disponible: 10 438 Mo  
Mémoire virtuelle : taille maximale: 18 707 Mo  
Mémoire virtuelle : disponible: 12 448 Mo  
Mémoire virtuelle : en cours d'utilisation: 6 259 Mo  
Emplacements des fichiers d'échange: C:\pagefile.sys  
Domaine: WORKGROUP  
Serveur d'ouverture de session: \\PCV4  
Correctif(s): 31 Corrections installées.  
[01]: KB5066130  
[02]: KB5037592  
[03]: KB5003791  
[04]: KB5011048  
[05]: KB5011058  
[06]: KB5015684  
[07]: KB5020683  
[08]: KB5026037  
[09]: KB5033052  
[10]: KB5072653  
[11]: KB5071959  
[12]: KB5037995  
[13]: KB5041579  
[14]: KB5041581  
[15]: KB5043935  
[16]: KB5043130  
[17]: KB5046823  
[18]: KB5050388  
[19]: KB5050111  
[20]: KB5052916  
[21]: KB5054682  
[22]: KB5055663  
[23]: KB5058526  
[24]: KB5059504

Hostname :

```
C:\Users\etudinfo>hostname  
PCV4
```

Tasklist :

```
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	2 216 Ko
Secure System	56	Services	0	39 152 Ko
Registry	116	Services	0	64 132 Ko
smss.exe	424	Services	0	1 248 Ko
csrss.exe	616	Services	0	6 432 Ko
wininit.exe	700	Services	0	7 136 Ko
services.exe	772	Services	0	14 492 Ko
LsaIso.exe	836	Services	0	3 884 Ko
lsass.exe	860	Services	0	26 392 Ko
svchost.exe	992	Services	0	32 380 Ko
fontdrvhost.exe	1020	Services	0	4 992 Ko
svchost.exe	940	Services	0	19 164 Ko
svchost.exe	1028	Services	0	10 848 Ko
svchost.exe	1108	Services	0	5 572 Ko
svchost.exe	1208	Services	0	10 748 Ko
svchost.exe	1216	Services	0	12 340 Ko
IntelCpHDCPSvc.exe	1328	Services	0	7 384 Ko
svchost.exe	1356	Services	0	6 760 Ko
svchost.exe	1372	Services	0	7 976 Ko
svchost.exe	1440	Services	0	17 340 Ko
svchost.exe	1468	Services	0	21 232 Ko
IntelCpHeciSvc.exe	1532	Services	0	7 208 Ko
svchost.exe	1548	Services	0	8 660 Ko
svchost.exe	1620	Services	0	14 396 Ko
igfxCUIService.exe	1700	Services	0	9 216 Ko
svchost.exe	1716	Services	0	11 396 Ko
svchost.exe	1792	Services	0	14 220 Ko
svchost.exe	1804	Services	0	6 132 Ko
svchost.exe	1828	Services	0	6 492 Ko
svchost.exe	1892	Services	0	8 704 Ko
svchost.exe	1956	Services	0	10 980 Ko
svchost.exe	1972	Services	0	8 164 Ko
svchost.exe	1980	Services	0	10 236 Ko
AppHelperCap.exe	1996	Services	0	16 500 Ko
DiagsCap.exe	2016	Services	0	23 984 Ko
Memory Compression	920	Services	0	240 864 Ko
NetworkCap.exe	1180	Services	0	14 656 Ko
SysInfoCap.exe	912	Services	0	21 072 Ko
TouchpointAnalyticsClient	1928	Services	0	78 720 Ko
svchost.exe	2348	Services	0	14 012 Ko
svchost.exe	2456	Services	0	18 888 Ko
svchost.exe	2492	Services	0	7 300 Ko
svchost.exe	2552	Services	0	11 124 Ko
svchost.exe	2612	Services	0	8 548 Ko

## 2. Dépannage Réseau

Commandes recourues pour analyser la connectivité et les flux réseau.

Comman de	Fonction
<b>PING</b>	Teste la connectivité réseau vers une machine.

```
C:\Users\etudinfo>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 de la virtualisation réseau Hyper-V.
  -4          Force l'utilisation d'IPv4.
  -6          Force l'utilisation d'IPv6.
```

<b>TRACERT</b>	Montre les routeurs traversés jusqu'à une destination.
<b>IPCONFIG /ALL</b>	Affiche la configuration réseau complète (DNS, IP, MAC...).
<b>NETSTAT -ANO</b>	Affiche les connexions actives, les ports d'écoute et les PIDs associés.
<b>ARP -A</b>	Affiche le cache ARP (association IP ↔ MAC).

Testez les commandes suivantes

### 3. Gestion des Utilisateurs et de la Sécurité

Commandes utilisées pour l'administration locale des comptes.

Commande	Fonction
<b>NET USER</b>	Affiche les utilisateurs locaux ou permet d'en ajouter/supprimer.

<b>NET LOCALGROUP ADMINISTRATORS</b>	Ajoute un utilisateur au groupe Administrateurs.
<b>WHOAMI</b>	Affiche l'utilisateur actuellement connecté ainsi que son domaine.

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
<b>CHKDSK /F</b>	Analyse et répare les erreurs sur un disque.
<b>SFC /SCANNOW</b>	Vérifie et répare les fichiers système corrompus.
<b>TASKKILL /PID</b>	Termine un processus en fonction de son identifiant (PID).
<b>TREE</b>	Affiche la structure des répertoires en arborescence.

Testez les 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
<b>MSTSC</b>	Ouvre l'interface de Connexion Bureau à Distance.
<b>SHUTDOWN /I</b>	Lance une boîte de dialogue de redémarrage/arrêt à distance.
<b>LOGOFF</b>	Déconnecte l'utilisateur actuel.
<b>NET USE</b>	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 ?

## 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** ?

## 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** ?

## 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** ?

## 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 ?

## 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.) ?

## 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 ?

## 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 ?

## 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 ?

### 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).

### 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.