TP 4.2 - Maîtrise du CMD Windows : Administration système et réseau

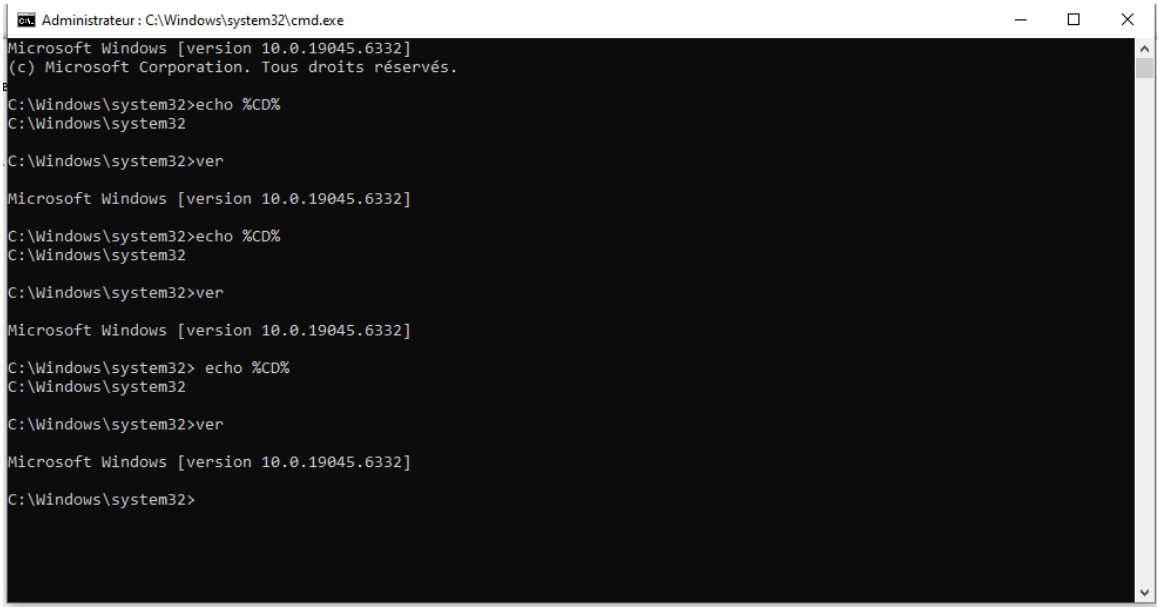
Objectifs pédagogiques

Maîtriser les commandes essentielles de l'invite de commandes Windows
Comprendre la gestion des fichiers, processus et réseaux
Développer des compétences en troubleshooting système
Exercice 1 : Prise en main de l'environnement CMD

1.1 Lancement et configuration

Ouvrez CMD en tant qu'administrateur :
Win + X → Invite de commandes (admin) **OU**
Win + R → cmd → Ctrl + Shift + Entrée
Tâches :

1. Vérifiez votre dossier courant avec ***echo %CD%***
2. Affichez la version de Windows avec ver
3. Capture d'écran montrant ces informations



1.2 Personnalisation de l'environnement

Tapez ***color 0A***
Tapez ***prompt $T [$P]$G***
Tapez ***title Session_Admin_CMD***
Questions :

Que fait la commande color ?
La commande color permet de changer la couleur des caractères present sur le cmd
Comment le prompt a-t-il changé ?
Non cela n'a rien changer
À quoi sert la commande title ?
La commande title sert à) modifier le nom de la session.

Exercice 2 : Exploration avancée du système de fichiers

2.1 Navigation et arborescence

Tâches :

1. Créez la structure suivante :

TP_CMD

Documents/

Textes/

Images/

Archives/

Temp/

2.2 Attributs de fichiers avancés

echo CONTENU_SECRET > Documents\fichier_cache.txt

dir

attrib +H Documents\fichier_cache.txt

dir Documents

dir Documents /A

Questions :

Que signifient les attributs +H ?
Cela rend le fichier caché, il ne s'affiche pas dans un `dir` normal.
Comment afficher les fichiers cachés avec dir ?

En utilisant l'option `/A`, qui affiche tous les fichiers, y compris cachés et système.

Exercice 3 : Gestion des processus et services

3.1 Analyse des processus système

tasklist /FO TABLE /V

Tâches :

1. Lancez le Bloc-notes et Paint
2. Identifiez leurs PID avec :

tasklist | findstr "notepad mspaint"

3.2 Gestion fine des processus

:: Tuer un processus par PID

taskkill /PID [PID_NUMBER] /F

:: Tuer par nom d'image

taskkill /IM notepad.exe /T

Questions :

Quelle est la différence entre /F et /T ?

La différence entre `/F` et `/T` ?

- *`/F` force la fermeture du processus.*
- *`/T` termine aussi tous les processus enfants (les processus lancés par ce processus).*

Pourquoi faut-il être prudent avec taskkill ?
Parce que tuer un processus important ou système peut provoquer une instabilité ou une perte de données.

Exercice 4 : Diagnostic réseau avancé

4.1 Analyse complète de la configuration

ipconfig /all

ou

netsh interface ip show config

Questions :

Quelle est votre adresse MAC ?
00-15-5D-6F-D2-7D
Le DHCP est-il activé ?
Non
C'est quoi un DHCP ? *Le **DHCP** (Dynamic Host Configuration Protocol) est un **protocole réseau** qui permet à un appareil (ordinateur, smartphone, etc.) d'obtenir **automatiquement une adresse IP** et d'autres paramètres réseau essentiels (comme la passerelle, le masque de sous-réseau, les serveurs DNS) dès qu'il se connecte à un réseau.*

Quel serveur DNS utilisez-vous ?
f*ec0:0:0:ffff::1%1*
fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

4.2 Tests de connectivité

ping 8.8.8.8 -n 4

ping google.com

tracert google.com

pathping google.com

Tâches :

1. Explique le résultat du premier ping

La réponse signifie que ton ordinateur a réussi à contacter le serveur Google DNS (8.8.8.8). Le temps (14 ms) est le délai aller-retour, indiquant la rapidité de la connexion. TTL montre le nombre de routeurs traversés (souvent 115 ici). Réponse de 8.8.8.8 : octets=32 temps=14 ms TTL=114

2. Comparez les résultats de tracert et pathping

- `tracert` *Affiche chaque saut entre ta machine et google.com, c'est une route avec les temps à chaque étape..*
- `pathping` *Combine ping et tracert, donne aussi des statistiques de perte de paquets par saut.*
- ***`ping google.com`***
  Envoie des paquets ICMP à google.com, teste la résolution DNS (nom → IP) et la connectivité.
- `tracert` *montre uniquement les chemins et temps par saut.*
- `pathping` *ajoute en plus la perte de paquets et la qualité de la connexion par saut, plus détaillé pour diagnostiquer les problèmes réseau.*

3. Testez la résolution DNS avec nslookup google.com

4.3 Statistiques réseau

netstat -ano

netstat -an | find ":80"

netstat -e 5

Questions :

Que montre netstat -ano ?

Montre toutes les connexions réseau actives avec :

- *Protocole (TCP/UDP)*
- *Adresse locale et distante*
- *État de la connexion (ÉTABLI, LISTENING, etc.)*
- *PID du processus associé*

La liste complète des connexions réseau actives et leurs PID (utile pour identifier quel programme utilise une connexion).

Comment identifier les connexions établies sur le port 80 ?
En filtrant avec `netstat -an | find ":80"` on voit toutes les connexions TCP ou UDP où le port local ou distant est 80.

Exercice 5 : Scripting basique et automatisation

5.1 Création d'un script de sauvegarde

Créez un fichier sauvegarde.bat :

```
@echo off

echo === SAUVEGARDE DOSSIERS IMPORTANTS ===

set BACKUP_DIR=%USERPROFILE%\Backup_%DATE%

mkdir "%BACKUP_DIR%"

xcopy "%USERPROFILE%\Documents\*.txt" "%BACKUP_DIR%\Textes\" /S /I /Y

xcopy "%USERPROFILE%\Desktop\*.pdf" "%BACKUP_DIR%\PDF\" /S /I /Y

echo Sauvegarde terminee: %BACKUP_DIR%

dir "%BACKUP_DIR%" /S

pause
```

1. Que fait la commande @echo off et pourquoi est-elle utile ici ?

Désactive l'affichage des commandes dans la console pour rendre la sortie plus propre.

2. Que fait la commande set BACKUP_DIR=%USERPROFILE%\Backup_%DATE% ?

Définit une variable d'environnement `BACKUP_DIR` qui pointe vers un dossier Backup dans ton profil utilisateur, suffixé par la date du jour.

Que contient la variable %USERPROFILE% ?
Le chemin vers le dossier utilisateur actuel, ex : `C:\Users\TonNom`.

Que contient la variable %BACKUP_DIR% après son exécution ?
Le chemin complet vers le dossier de sauvegarde, par ex :
`C:\Users\TonNom\Backup_06-10-2025`

3. Que fait mkdir "%BACKUP_DIR%" ?

Crée ce dossier s'il n'existe pas.

Que se passerait si le dossier existait déjà ?
`mkdir` *ne génère pas d'erreur, il laisse le dossier intact.*

4. Que fait xcopy "%USERPROFILE%\Documents*.txt" "%BACKUP_DIR%\Textes\" /S /I /Y ?
   Que signifient les options /S /I /Y ?

Copie tous les fichiers `.txt` *du dossier Documents dans le sous-dossier Textes du dossier de sauvegarde, avec :*

- `/S` *: inclut sous-dossiers*
- `/I` *: considère la cible comme un dossier*
- `/Y` *: écrase sans demander confirmation*

5. Pourquoi crée-t-on deux dossiers différents (Textes et PDF) ?

Pour organiser la sauvegarde par type de fichiers.

6. Que fait la commande dir "%BACKUP_DIR%" /S ?

Liste tous les fichiers dans le dossier de sauvegarde et ses sous-dossiers.

7. Quel est le rôle de pause ? Que se passerait si on le supprimait ?

Pause l'exécution et attend une touche avant de fermer la fenêtre pour que tu puisses voir les résultats.

Améliorations

1.Comment pourriez-vous **sauvegarder d'autres types de fichiers** (images, vidéos) ?

Ajouter des lignes xcopy avec extensions `.jpg`, `.png`, `.mp4`, *etc.*

2. Comment rendre le script **plus robuste** si un fichier est en cours d'utilisation ou s'il y a un problème de droits ?

- *Ajouter des vérifications d'erreurs*
- *Utiliser* `robocopy` *pour gérer mieux les fichiers verrouillés*
- *Exécuter avec des privilèges admin si besoin*

3. Comment automatiser ce script pour qu'il **s'exécute tous les jours** sans intervention manuelle ?

- *Utiliser le **Planificateur de tâches Windows** pour lancer le script à une heure donnée.*

5.2 Surveillance système

Créez monitor.bat :

@echo off

:loop

cls

echo === MONITORING SYSTEME ===

echo Date: %DATE% - Heure: %TIME%

echo.

echo === PROCESSUS ===

tasklist /FO TABLE | findstr /I "chrome firefox"

echo.

echo === CONNEXIONS RESEAU ===

netstat -an | find ":80"

timeout /t 10 /nobreak

goto loop

1. Que fait la commande @echo off ? Pourquoi est-elle utile dans ce script ?
   Cache l'affichage des commandes, sortie plus propre.
2. Quelle est la fonction de l'étiquette :loop et du goto loop ?

`:Loop` est une étiquette marquant le début de la boucle.
`goto Loop` renvoie à cette étiquette pour répéter le bloc.

3. Que se passe-t-il quand on exécute cls ? Pourquoi est-ce important dans ce script ?

Efface l'écran pour un affichage clair à chaque cycle.

4. Que vont afficher %DATE% et %TIME% ? Que se passerait si on supprimait cette ligne ?
   La date et l'heure actuelles.

Pas d'affichage de la date/heure, moins d'informations temporelles.

5. À quoi sert tasklist /FO TABLE | findstr /I "chrome firefox" ?

- *`tasklist /FO TABLE` affiche la liste des processus en cours dans un format tableau.*
- *`|` redirige la sortie vers la commande suivante.*
- *`findstr /I "chrome firefox"` filtre les lignes contenant "chrome" ou "firefox" (la recherche est insensible à la casse grâce à `/I`).*

***Donc**, cette commande affiche uniquement les processus liés à Chrome ou Firefox, ce qui est utile pour surveiller ces navigateurs.*

Que se passerait si on remplaçait "chrome firefox" par "notepad" ?

Le script afficherait uniquement les processus contenant "notepad" dans leur nom. Cela permet de surveiller un programme spécifique, ici le Bloc-notes.

6. Que fait la commande netstat -an | find ":80" ? Que signifie le :80 ?

`netstat -an` affiche toutes les connexions et ports d'écoute avec adresses numériques (IP + port).

*`| find ":80"` filtre pour ne montrer que les connexions où le port (local ou distant) est le **80**, qui est le port standard HTTP.*

***Donc**, cette commande montre toutes les connexions réseau liées au port 80, typiquement les serveurs ou clients web*

7. Quel est le rôle de timeout /t 10 /nobreak ? Que se passerait si on mettait /t 0 ?

- *`timeout /t 10 /nobreak` met le script en pause pendant 10 secondes, et empêche l'utilisateur d'interrompre cette pause par une touche.*
- *Si on mettait `/t 0`, la pause serait de 0 secondes, donc aucune pause, le script tournerait en boucle très rapidement, ce qui peut surcharger le CPU.*

8. Pourquoi le script utilise-t-il une boucle infinie ? Quels sont les avantages et inconvénients d'un tel fonctionnement ?

Pourquoi ?
Pour surveiller en continu les processus et connexions, en mettant à jour toutes les 10 secondes.

Avantages :

a. *Monitoring en temps réel.*
b. *Permet de détecter rapidement tout changement.*

Inconvénients :

c. *Utilise des ressources système (CPU).*
d. *La fenêtre console reste ouverte en permanence.*
e. *Nécessite une intervention manuelle pour arrêter.*

Améliorations

1. Comment pourriez-vous modifier le script pour surveiller **plusieurs ports réseau** en même temps, par exemple 80 et 443 ?

Pour surveiller plusieurs ports réseau en même temps, comme les ports 80 et 443, il suffit d'intégrer une boucle dans le script utilisant netstat

2. Comment pourriez-vous faire en sorte que le script **enregistre l'historique** des processus et connexions dans un fichier texte pour consultation ultérieure ?

Pour enregistrer l'historique des processus et des connexions dans un fichier texte pour consultation ultérieure, il suffit de rediriger les sorties des commandes comme `tasklist` *et* `netstat` *vers un fichier à l'aide de l'opérateur*

3. Comment pourriez-vous modifier le script pour qu'il **s'arrête automatiquement** après un certain nombre de cycles ou après un certain temps ?

Pour que le script s'arrête automatiquement après un certain nombre de cycles ou après un certain temps, vous pouvez ajouter un compteur de boucles ou utiliser la commande `timeout` *combinée à* `set /a` *et* `if` *pour contrôler la durée ou le nombre d'itérations.*

4. Que pourriez-vous faire pour rendre l'affichage **plus lisible ou esthétique**, par exemple avec des couleurs différentes pour les sections ?

Pour que le script s'arrête automatiquement, on peut ajouter un compteur de cycles ou mesurer le temps écoulé, puis utiliser une condition `if` *pour interrompre la boucle une fois le seuil atteint.*