

Travaux pratiques : Commandes de l'interface de ligne de commande des tâches et du système

Introduction

Au cours de ces travaux pratiques, vous allez utiliser les commandes de l'interface de ligne de commande des tâches et du système.

Ressources requises

- Un ordinateur équipé de Windows

Instructions

Partie 1 : Commandes de l'interface de ligne de commandes des tâches

La commande `tasklist` affiche les processus exécutés sur un ordinateur, alors que la commande `taskkill` met fin à ces processus. Ces deux commandes peuvent être utilisées sur un ordinateur distant. Il est possible de les filtrer et de les cibler à l'aide des options disponibles correspondantes. Dans ces travaux pratiques, le nom d'utilisateur pris comme exemple est `ITEUser`.

Étape 1 : La commande `tasklist`

- Ouvrez le Bloc-notes. Ouvrez Internet Explorer. Si Internet Explorer n'est pas disponible, utilisez Microsoft Edge.

- Ouvrez une invite de commande. À l'invite, saisissez la commande **`tasklist`**.

```
C:\Users\ITEUser> tasklist
```

Question :

Quelle commande utiliseriez-vous pour afficher les résultats page par page ?

Saisissez vos réponses ici

- Saisissez la commande `tasklist help` pour vérifier la syntaxe et les options de la commande `tasklist`.

```
C:\Users\ITEUser> tasklist /?
```

Ou

```
C:\Users\ITEUser> help tasklist
```

Questions :

Quelle option permet de répertorier les modules associés à une tâche ?

Saisissez vos réponses ici

Quelle commande utiliseriez-vous pour rechercher toutes les tâches qui utilisent le module `oleaut32.dll` ? Citez des tâches qui utilisent `oleaut32.dll`.

Saisissez vos réponses ici

Les options disponibles avec la commande `tasklist` vous permettent de filtrer les résultats pour un nom d'image spécifique, tel que `notepad.exe` pour le Bloc-notes. Notez le PID pour l'étape suivante.

```
C:\Users\ITEUser> tasklist /FI "imagename eq notepad.exe"
```

Nom de l'image	PID	Nom de la session	N° session	Mém	Utilisation
notepad.exe	3128	Console	1	14	016 K

Questions :

Quelle commande utiliseriez-vous pour rechercher toutes les tâches associées à votre nom d'utilisateur ?

Saisissez vos réponses ici

Quelle commande utiliseriez-vous pour détecter tous les processus ayant été exécutés depuis plus de 1 heure et 40 minutes ?

Saisissez vos réponses ici

Étape 2 : La commande taskkill

Vous pouvez utiliser le Gestionnaire des tâches pour mettre fin à un processus. Néanmoins, il est parfois nécessaire de mettre fin à un processus non autorisé manuellement à l'aide de la commande de l'interface de ligne de commande. La commande taskkill peut vous éviter de forcer un redémarrage non programmé du système. F

- a. Utilisez la commande taskkill help pour vérifier la syntaxe de la commande et les options disponibles.

```
C:\Users\ITEUser> taskkill /?
```

Question :

Quelle commande utiliseriez-vous pour mettre fin à tous les processus appartenant à un utilisateur particulier ?

Saisissez vos réponses ici

Remarque : si vous avez exécuté la commande à l'étape précédente, rouvrez le Bloc-notes et Internet Explorer. Utilisez la commande tasklist pour afficher la liste des PID pour notepad.exe.

- b. Utilisez le PID de notepad.exe que vous avez enregistré à l'étape précédente. Le PID 3128 est utilisé dans cet exemple.

```
C:\Users\ITEUser> taskkill /PID 3128
```

Opération réussie : un signal de fin a été envoyé au processus de PID 3128.

- c. L'application Bloc-notes doit être fermée. Utilisez également la commande tasklist pour vérifier que le processus a été arrêté.
- d. Utilisez l'option /IM pour utiliser le nom du processus avec la commande taskkill afin de mettre fin au processus. Internet Explorer (iexplore.exe)

```
C:\Users\ITEUser> taskkill /IM iexplore.exe
```

Opération réussie : un signal de fin a été envoyé au processus "iexplore. exe" de PID 3916.

Opération réussie : un signal de fin a été envoyé au processus "iexplore. exe" de PID 6740.

- e. Selon la version de Windows, il est possible que l'application Internet Explorer ne soit pas fermée. Vous devrez peut-être ajouter /T pour mettre fin au processus enfant associé.

```
C:\Users\ITEUser> taskkill /IM iexplore.exe /T
```

Opération réussie : un signal de fin a été envoyé au processus de PID 6740, processus enfant de PID 3916.

Opération réussie : un signal de fin a été envoyé au processus de PID 3916, processus enfant de PID 2828.

- f. Il est parfois possible que vous deviez forcer l'arrêt d'un processus. Pour cela, ajoutez l'option /F à la commande taskkill.

```
C:\Users\ITEUser> taskkill /IM iexplore.exe /T /F
```

Opération réussie : le processus avec PID 6740 (processus enfant de PID 3916) a été terminé.

Opération réussie : le processus avec PID 3916 (processus enfant de PID 2828) a été terminé.

- g. Vérifiez que l'application Internet Explorer est fermée.

Partie 2 : Commandes de l'interface de ligne de commande du système

Étape 1 : La commande sfc

Lorsque vous rencontrez des erreurs aléatoires ou des problèmes au cours du démarrage, ou si certains composants Windows ne fonctionnent pas correctement, le vérificateur des fichiers système (sfc) peut analyser l'intégrité du système et remplacer les fichiers système endommagés ou manquants par une version correcte connue.

- a. Ouvrez une invite de commandes avec des privilèges d'administrateur.
- b. Examinez la syntaxe et les options de la commande sfc.

```
C:\Windows\system32> sfc /?
```

Question :

Quelle option utiliseriez-vous pour analyser uniquement l'intégrité de l'ensemble des fichiers système protégés ?

Saisissez vos réponses ici

- c. Utilisez l'option **/scannow** pour analyser et réparer tous les fichiers système protégés.

```
C:\Windows\system32> sfc /scannow
```

```
Début de l'analyse système. Cette opération peut nécessiter un certain temps.
```

```
Démarrage de la phase de vérification de l'analyse du système.
```

```
Vérification achevée à 2 %.
```

```
<output omitted>
```

Étape 2 : La commande dism

L'Outil de gestion et de maintenance des images de déploiement (DISM) est un utilitaire de ligne de commande Windows qui permet de traiter et de préparer des images Windows. Vous pouvez par exemple utiliser DISM pour gérer les informations incluses dans l'image Windows ou pour traiter l'image elle-même, notamment l'ajout ou la suppression de pilotes ou la mise à niveau vers une version plus récente de Windows.

Dans cette étape, vous examinerez les options disponibles avec cette commande et dresserez la liste de tous les pilotes disponibles sans apporter de modifications au système d'exploitation.

- a. Pour afficher les options disponibles avec la commande dism, saisissez **dism** dans une invite de commandes avec des privilèges d'administrateur. Les options disponibles varient selon votre version de Windows.

```
C:\Windows\system32> dism
```

```
Outil de gestion et de maintenance des images de déploiement
```

```
Version : 10.0.17763.1
```

```
DISM.exe [dism_options] {Imaging_command} [<Imaging_arguments>]
```

```
DISM.exe [/Image:<path_to_offline_image> | /Online] [dism_options]
```

```
{servicing_command} [<servicing_arguments>]
```

```
<output omitted>
```

- b. Pour en savoir plus sur le système d'exploitation exécuté, saisissez **dism /online /?** afin d'afficher les options disponibles.

```
C:\Windows\system32> dism /online /?
```

- c. Lorsque vous utilisez dism, vous pouvez obtenir des informations supplémentaires sur les pilotes tiers du système d'exploitation exécuté ; pour cela, saisissez **dism /online /get-drivers** à l'invite.

```
C:\Windows\system32> dism /online /get-drivers
```

- d. Pour afficher tous les pilotes, ajoutez les options **/all** à la commande.

```
C:\Windows\system32> dism /online /get-drivers /all
```

- e. Pour faciliter la lecture, vous pouvez mettre en forme le résultat dans un tableau en ajoutant l'option **/format:table**.

```
C:\Windows\system32> dism /online /get-drivers /all /format:table
```

Question :

Quelles options pouvez-vous ajouter à la commande pour afficher le résultat page par page ?

Saisissez vos réponses ici

- f. Vous pouvez enregistrer les résultats du pilote dans un fichier texte si nécessaire. **>** permet de créer un nouveau fichier C:\Users\ITEUser\Drivers_Results.txt et d'écrire les résultats dans ce nouveau fichier. Si vous souhaitez ajouter d'autres résultats à ce fichier, remplacez **>** par **>>** de sorte que le fichier ne soit pas remplacé par de nouvelles informations.

```
C:\Windows\system32> dism /online /get-drivers /all /format:table >
C:\Users\ITEUser\Drivers_Results.txt
```

- g. Utilisez la commande **more** ou **type** pour vérifier la création du fichier texte.

```
C:\Windows\system32> more C:\Users\ITEUser\Drivers_Results.txt
```

Outil de gestion et de maintenance des images de déploiement

Version : 10.0.17763.1

Version de l'image : 10.0.17763.475

<some output omitted>

Étape 3 : La commande shutdown

Si votre ordinateur ne parvient pas à se fermer via le menu Démarrer, la commande **shutdown** de la ligne de commande peut s'avérer utile.

- a. Dans une invite de commandes, saisissez **shutdown**. Examinez la syntaxe et les options disponibles pour arrêter l'ordinateur via la ligne de commande.

```
C:\Windows\system32> shutdown
```

Utilisation : shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o]
[/hybrid] [/soft] [/fw] [/f]

[/m \\computer] [/t xxx] [/d [p|u:]xx:yy [/c "comment"]]

<output omitted>

Notez les options d'arrêt ou de redémarrage d'un ordinateur distant, d'ajout de commentaires concernant la raison du redémarrage ou de l'arrêt, ainsi que la possibilité de définir un délai avant l'arrêt.

Question :

Saisissez la commande permettant de vous déconnecter de votre ordinateur. Notez la commande ci-dessous.

Saisissez vos réponses ici

- b. Connectez-vous de nouveau à l'ordinateur et arrêtez-le dans un délai de 120 secondes via la ligne de commande.

Questions :

Notez la commande ci-dessous. Quel message d'avertissement s'est-il affiché ?

Saisissez vos réponses ici

Quelle commande utiliseriez-vous pour abandonner l'arrêt ?

Saisissez vos réponses ici