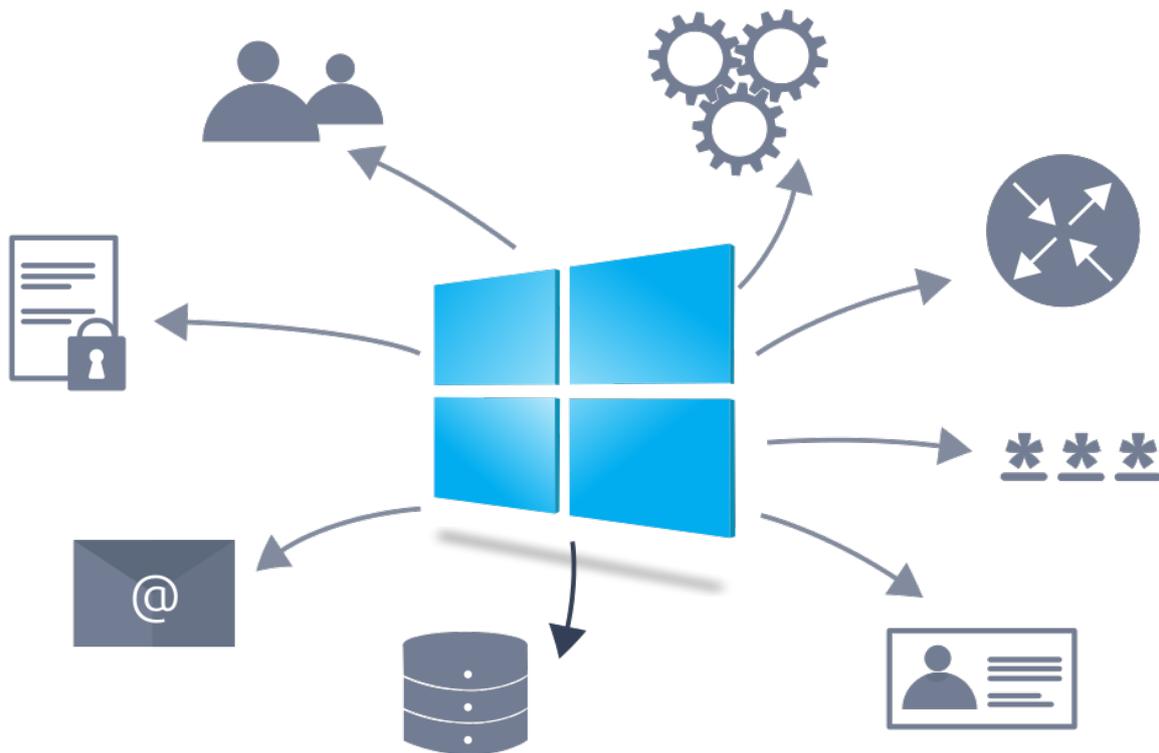


# [Énumération] Windows

## Introduction

Cette page décrit les procédés pour énumérer un système Windows lorsque vous y avez accès.



## Manuel

### Afficher les informations systèmes

```
systeminfo
```

### Afficher les mises à jour installées

```
wmic qfe get Caption,Description
```

## Afficher les services installés et démarrés

```
net start
```

## Afficher les applications installées

```
wmic product get name,version,vendor
```

## Afficher les privilèges de l'utilisateur actif

```
whoami /priv
```

## Afficher les groupes de l'utilisateur actif

```
whoami /groups
```

## Afficher les utilisateurs du système

```
net user
```

## Afficher le SID des utilisateurs du système

```
wmic useraccount get name,sid
```

À noter que le dernier octet du SID représente le **RID** de l'utilisateur.

## Afficher les groupes du système

```
net localgroup
```

## Afficher les membre d'un groupe

```
net localgroup <GROUP>
```

## Afficher les configurations locales

```
net accounts
```

## Lister les tâches planifiées

```
schtasks
```

Et pour afficher le détail d'une tâche planifiée :

```
schtasks /query /tn <TASK_NAME> /fo list /v
```

---

Revision #4

Created 12 February 2024 14:04:27 by Elieroc

Updated 3 May 2024 14:28:42 by Elieroc