# Windows

# Windows - Commande diagnostic Active directory

Diagnostics arborescence

- tree

---

Diagnostic général

- dcdiag

---

Diagnostic rôles

- netdom query

---

Diagnostic replication

- repadmin

---

Sites & services

- nltest

# Windows - Commandes windows core de base

Obtenir les informations systèmes :

```
systeminfo
```

Lancer powershell :

```
powershell
```

Lancer l’éditeur de registre :

```
regedit
```

Lancer le configurateur de serveur :

```
sconfig
```

Activer / désactiver un ou tous les firewall(s):

```
netsh advfirewall set <local|domain|public|allprofiles> state <on|off>
```

Vérifier si le proxy est présent :

```
netsh winhttp show proxy
```

Redémarrer le système immédiatement :

```
shutdown /r /t 00
```

Arrêter le système immédiatement :

```
shutdown /s /t 00
```

Monter / démonter un lecteur réseau (les options /persistent et /user sont facultatives) :

```
net use <lettreLecteur> <chemin UNC> /persistent /user:<username>
net use /delete <lettreLecteur>
```

Afficher le gestionnaire de tâches :

```
taskmgr
```

Afficher le magasin de certificats :

```
dir cert:/localmachine/<magasin>
```

Configurer un service :

```
sc config [<ServiceName>] [type= {own | share | kernel | filesys | rec | adapt | interact
type= {own | share}}] [start= {boot | system | auto | demand | disabled | delayed-auto}]
[error= {normal | severe | critical | ignore}] [binpath= <BinaryPathName>] [group=
<LoadOrderGroup>] [tag= {yes | no}] [depend= <dependencies>] [obj= {<AccountName> |
<ObjectName>}] [displayname= <DisplayName>] [password= <Password>]
```

Voir les mises à jours Windows installées :

```
Get-Hotfix
```

Voir avec quel compte l’on est logué :

```
whoami
```

Activation Windows :

```
slmgr /ipk <ProductKey>
slmgr /ato
```

Paramétrage source NTP :

```
net stop w32time
w32tm /config /syncfromflags:manual /manualpeerlist:"<AdresseServerNTP>"
w32tm /config /reliable:yes
net start w32time
w32tm /config /update
w32tm /resync /rediscover
w32tm /query /status
```

# Windows - Liste des url windows update

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://download.microsoft.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com

# Windows - Matrice des permissions NTFS

## I. Introduction

Lors de la création des acl avec powershell, il faut utiliser un formatage spécifique.

```
$acl.AddAccessRule([System.Security.AccessControl.FileSystemAccessRule]::new(
  "<groupeAD>", "ReadAndExecute","ContainerInherit,ObjectInherit","none","Allow"
  ))
```

Le document ci-dessous décrit les éléments attendus pour chaque attribut.

---

## II. Valeurs attendues

### 2.1 Attribut 1 : Nom de groupe

Le premier attribut est le nom du groupe / utilisateur sur lequel les permissions vont s'appliquer. Celui-ci est au format '***Scope\Groupe***'

| Groupe / Utilisateur |
| --- |
| Domaine\groupe |
| Builtin\groupe |

| |
|---|
| groupe local |
| everyone |
| "NT AUTHORITY\SYSTEM" |

## 2.2 Attribut 2 : Droits à appliquer

Le Second attribut contiennent le(s) droit(s) à appliquer. Il est possible d'en mettre plusieurs, en les séparant par une virgule.

*exemple : "Read,Write,ReadAndExecute"*

Ils sont de trois types :

- **Normaux**
  - `Read`
  - `Write`
  - `ReadAndExecute`
  - `Modify`
  - `FullControl`
  - `ListDirectory`
  - `ReadAttributes`
  - `ReadExtendedAttributes`
  - `WriteAttributes`
  - `WriteExtendedAttributes`
  - `Delete`
  - `DeleteSubdirectoriesAndFiles`
  - `ReadPermissions`
  - `ChangePermissions`
  - `TakeOwnership`
  - `Synchronize`
- **Combinés**
  - `ReadData`
  - `WriteData`
  - `AppendData`
  - `ExecuteFile`
- **Spéciaux**

- `Traverse`
- `CreateFiles`
- `CreateDirectories`

## 2.3 Attribut 3 : Héritage

Le troisième attribut concerne la portée des droits.

| Valeur | Signification |
|---|---|
| None | S'applique uniquement à ce dossier |
| ContainerInherit | S'applique aux sous-dossiers |
| ObjectInherit | S'applique aux fichiers |
| ContainerInherit,ObjectInherit | S'applique aux sous-dossiers et aux fichiers |

## 2.4 Attribut 4 : Propagation

Le quatrième attribut désigne la propagations des permissions.

| Valeur | Signification |
|---|---|
| None | Héritage normal récursif. |
| NoPropagateInherit | S'applique aux enfants direct mais pas en dessous. |
| InheritOnly | S'applique uniquement aux enfants mais pas aux parents. |

## 2.5 Attribut 5 : Type

Le dernier paramètre définit le type d'ACL. Deux types :

- Allow
- Deny

> 

**Info** : Pour rappel, les ACL de type 'Deny' sont prioritaire par rapport à un 'Allow'.

# Windows - Système de fichier

**C:** Racine du système

- **Perflog** (Contient des fichiers journaux)
  - sur les performances du système
  - diagnostics du système
- **Program Files** (Contient les programmes installés (64 bits))
- **Program Files (x86)** (Contient les programmes installés (32 bits))
- (caché) **Program data** (Contient les fichiers liés aux programmes installés)
  - fichiers de configurations
  - fichiers temporaires
  - mises à jours applicatives
- (caché) **Recovery** (Contient l'environnement de récupération)
- (caché) **System Volume Informations** (contient des informations sur le volume)
  - points de restauration systèmes
  - données systèmes (shadow copy service, windows backup,...)
- **Users** (contient les données utilisateurs)
  - <nom utilisateur>
    - 3D objects
    - (caché) Appdata --> données et configurations des applications propres à l'utilisateur
    - (caché) Application data --> même que ci dessus (Legacy)
    - Contacts
    - (caché) Cookies
    - Desktop
    - Documents
    - Downloads
    - Favorites
    - Links
    - (caché) Local settings --> Réglages applicatifs propres à l'utilisateur
    - Music
    - (caché) My documents --> (Legacy)
    - (caché) NetHood --> raccourcis du voisinage réseau (suite à une découverte réseau avec UPnP ou autre)
    - Pictures
    - (caché) Recent --> raccourcis vers les fichiers récemment utilisés
    - Saved Games
    - Searches --> historique des recherches récentes
    - (caché) SendTo --> Contient les raccourcis du menu contextuel "envoyer vers"

    - (caché) Start Menu --> Contient les raccourcis du menu démarrer
    - Videos
    - (caché) NTUSER.DAT (et associés) --> le profil "système" de l'utilisateur
        - son identité pour le système et ses clé de registre
- **Windows** (Contient les fichiers et exécutables du système d'exploitation)
- (caché) **pagefile.sys** (swap) --> fichier d'échange entre la mémoire et le disque