KB - Windows - Autoriser un utilisateur à redémarrer le service

> Applicable à : windows 10 et supérieur, windows 2012 et supérieur

Besoin

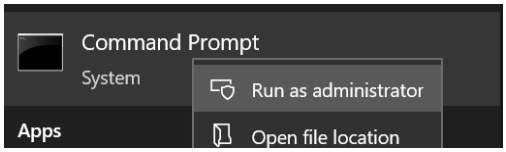
Un utilisateur est gestionnaire du service applicatif et doit pouvoir relancer le service au besoin.

Cependant, il ne faut pas lui donner de droits d'administration.

Solution

Solution CMD

lancer un CMD en tant qu'administrateur.



> ***Info*** : la commande va réécrire les permission en remplaçant l'existant. il faut donc d'abord récupérer les droits existants afin de ne pas les perdre.

Voir les droits existants avec la commande :

```
sc sdshow <nomDeService>.exe
```

```
C:\Windows\system32>sc sdshow winservicesample.exe

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU
(A;;CCLCSWRPWPDTLOCRRC;;;NS)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Copier le résultat, récupérer également le SID de l'utilisateur pour lequel rajouter les droits.

Puis créer la chaîne SDDL en se basant sur les informations fournies au format : (<action>;;<droits>;;;<SID>)

exemple : on veux ajouter à l'utilisateur x les droits de voir le status du service et de le stopper / démarrer.

- *(A;;LCRPWPCR;;;<sid de x>)*

ce qui donne la chaine complète suivante :

```
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;LCRPW
CR;;;S-1-5-21-1697030563-960874936-1853802646-53053)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Appliquer les nouvelles autorisation avec la commande :

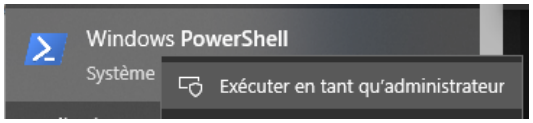
```
sc sdset <NomDeService> "<chaine d'autorisations"
```

```
[SC] SetServiceObjectSecurity SUCCESS
```

Solution Powershell

> Prérequis : Powershell 6 ou plus.

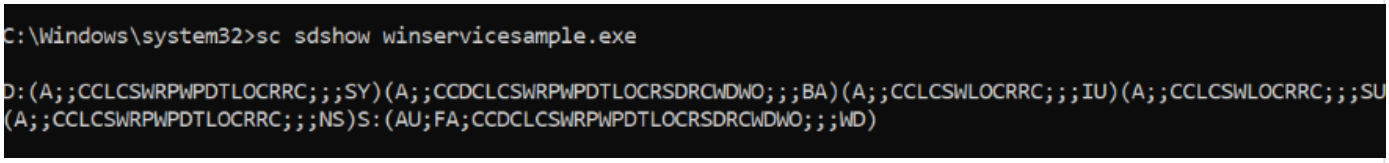
Lancer Powershell en tant qu'administrateur.



> ***Info*** : la commande va réécrire les permission en remplaçant l'existant. il faut donc d'abord récupérer les droits existants afin de ne pas les perdre.

Voir les droits existants avec la commande :

```
sc sdshow <nomDeService>.exe
```



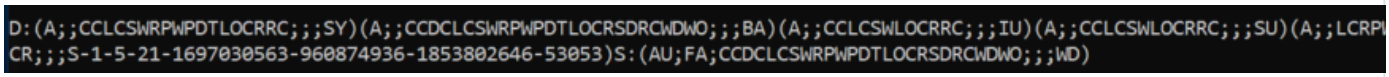
Copier le résultat, récupérer également le SID de l'utilisateur pour lequel rajouter les droits.

Puis créer la chaîne SDDL en se basant sur les informations fournies au format : (<action>;;<droits>;;;<SID>)

exemple : on veux ajouter à l'utilisateur x les droits de voir le status du service et de le stopper / démarrer.

- *(A;;LCRPWPCR;;;<sid de x>)*

ce qui donne la chaine complète suivante :



Appliquer les nouvelles autorisation avec la commande :

```
Set-Service -Name Spooler -SecurityDescriptorSddl "<chaîne sddl>"
```

Signification de l'encodage

Les lettres avant les parenthèses **D:** and **S:**

- **D:** pour ***discretionary access control list*** (***DACL***)
- **S:** pour ***system access control list*** (***SACL***)

Voir **"Access Control Lists"** pour plus d'informations (article en anglais).

La première lettre a deux valeurs possibles selon que l'on va autoriser ou interdire les actions: ***allow (A)*** or ***deny (D)***.

La chaîne de caractère qui suivra représente les autorisations sur le services :

- **CC** — SERVICE_QUERY_CONFIG (request service settings)
- **LC** — SERVICE_QUERY_STATUS (service status polling)
- **SW** — SERVICE_ENUMERATE_DEPENDENTS
- **LO** — SERVICE_INTERROGATE
- **CR** — SERVICE_USER_DEFINED_CONTROL
- **RC** — READ_CONTROL
- **RP** — SERVICE_START
- **WP** — SERVICE_STOP
- **DT** — SERVICE_PAUSE_CONTINUE

Les deux derniers caractères représentent les comptes et groupes built-in de windows et peuvent être remplacé par le SID de l'utilisateur ou du groupe auquel s'appliquera la politique.

- AU --> Authenticated Users
- AO --> Account operators
- AN --> Anonymous logon
- AU --> Authenticated users
- BA --> Built-in administrators

- BG --> Built-in guests
- BO --> Backup operators
- BU --> Built-in users
- CA --> Certificate server administrators
- CG --> Creator group
- CO --> Creator owner
- DA --> Domain administrators
- DC --> Domain computers
- DD --> Domain controllers
- DG --> Domain guests
- DU --> Domain users
- EA --> Enterprise administrators
- ED --> Enterprise domain controllers
- WD --> Everyone
- PA --> Group Policy administrators
- IU --> Interactively logged-on user
- LA --> Local administrator
- LG --> Local guest
- LS --> Local service account
- SY --> Local system
- NU --> Network logon user
- NO --> Network configuration operators
- *NS --> Network service account*
- PO --> Printer operators

- PS --> Personal self
- PU --> Power users
- RS --> RAS servers group
- RD --> Terminal server users
- SA --> Schema administrators
- SU --> Service logon user

Sources

How to set a Windows Service's permissions using ServiceControl and SDDL - Advanced Installer Community

How to Allow Non-Admin User to Start/Stop Service in Windows | Windows OS Hub

---

Revision #3
Created 2026-07-29 13:07:25 UTC by Olivier
Updated 2026-07-29 13:17:01 UTC by Olivier