

# Utilisateurs, Groupes & Permissions Windows

420-1S6 Systèmes d'exploitation

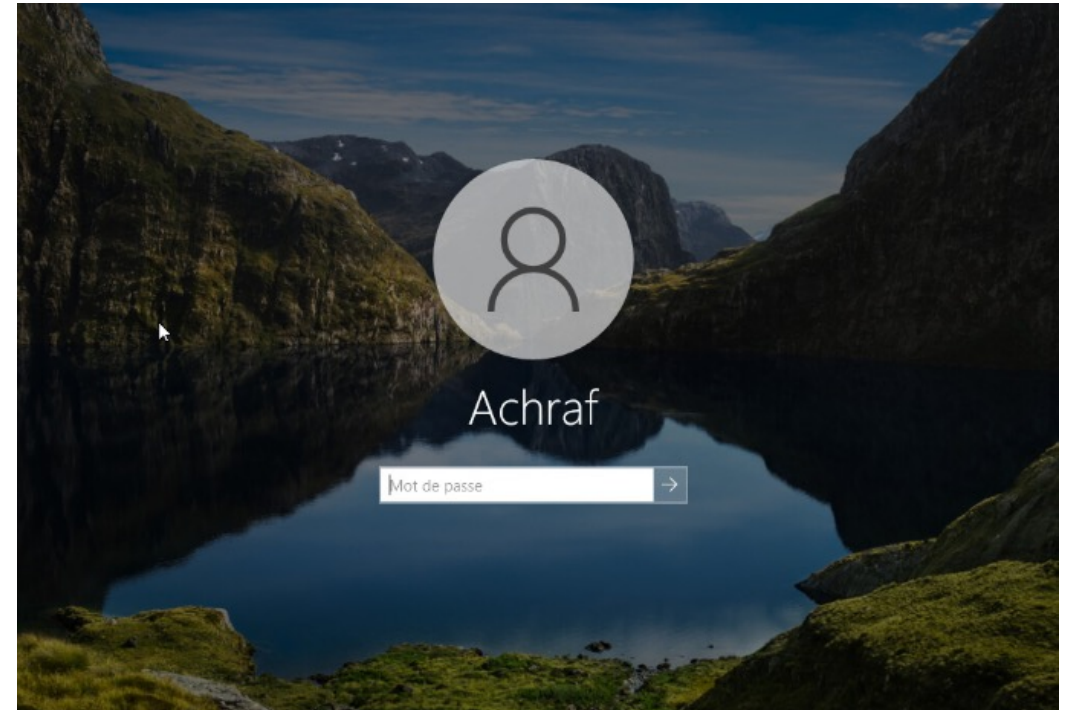
Automne 2022

Séance 11

# Système d'exploitation multi-utilisateurs



- Windows permet à plusieurs utilisateurs d'utiliser un système.
- Chaque utilisateur possède un compte doté d'un nom d'utilisateur et d'un mot de passe.



# Création du premier utilisateur



Lorsque vous installez Windows, vous devez définir le compte du premier utilisateur du système.

Ce compte possède des privilèges d'**administrateur**. Il peut (presque) tout faire sur Windows.

Il peut par la suite créer d'autres utilisateurs.

# Compte local, domaine et « cloud »



- ✓ Un **compte local** est défini localement sur l'ordinateur.
- ✓ On peut lui associer un compte Microsoft afin de pouvoir intégrer plusieurs services (OneDrive, Hotmail/Outlook.com, etc.)
- ✓ On peut aussi configurer des comptes professionnels ou scolaires, comme un accès à Microsoft Office 365.
- ✓ Dans les entreprises, on utilise souvent des comptes de domaine pour une authentification centralisée.

# Identification du compte



La commande WHOAMI permet de savoir quel est mon nom d'utilisateur.

```
C:\Users\Achraf>whoami
desktop-29c3bj3\achraf
```

**Nom d'utilisateur**

**Domaine ou nom d'hôte**



Lorsqu'un utilisateur est un administrateur, il peut :

- Installer et désinstaller des applications
- Changer des paramètres réseau
- Changer la configuration du système
- Créer et supprimer des utilisateurs et des groupes
- Lire et modifier (presque) tous les fichiers
- Gérer des partitions et des disques
- Gérer le matériel
- Modifier la base de registre du système
- etc.

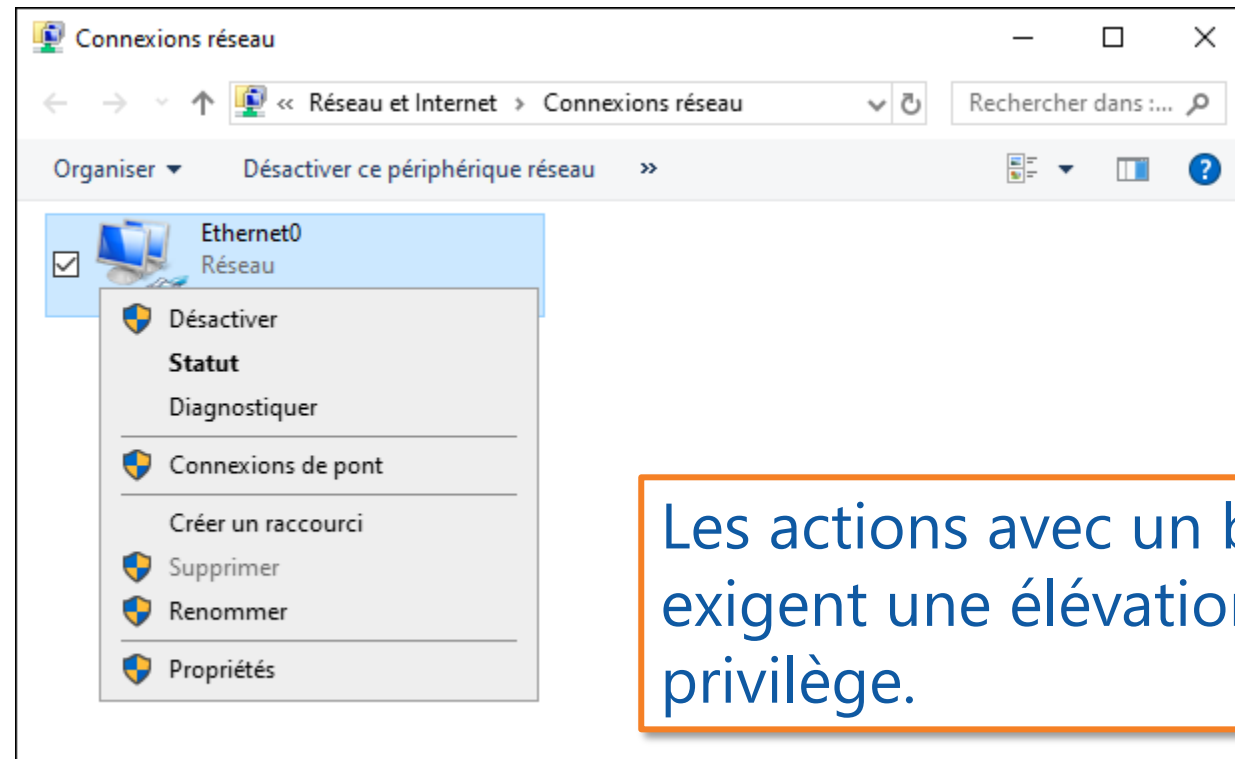
# User Account Control (UAC)




- Fonctionnalité introduite dans Windows Vista
- Même si un utilisateur possède des droits d'administration, **ces droits ne sont pas actifs**
- Il doit **élever** ses privilèges chaque fois qu'il exécute une application, pour que l'application bénéficie de ces droits (un peu comme **sudo** sous Linux)
- Les actions ou programmes qui demandent ce privilège portent généralement cette icône:
- On peut élever ses privilèges manuellement en choisissant « exécuter en tant qu'administrateur »



# Actions exigeant une élévation



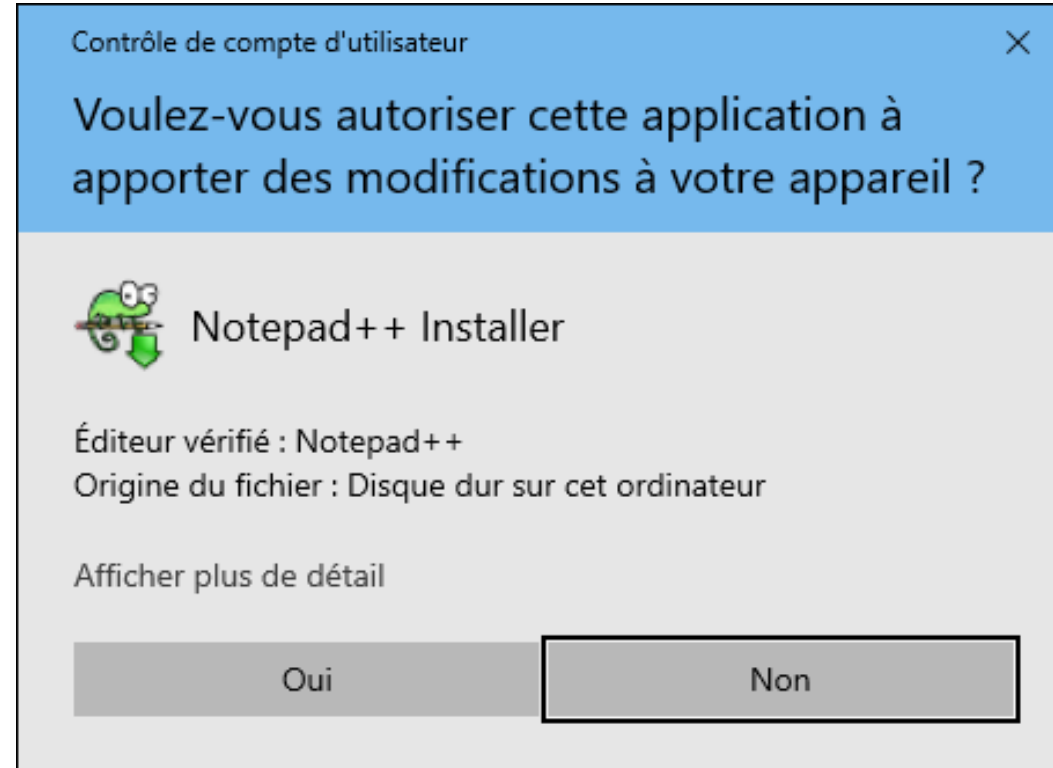
Les actions avec un bouclier  exigent une élévation de privilège.



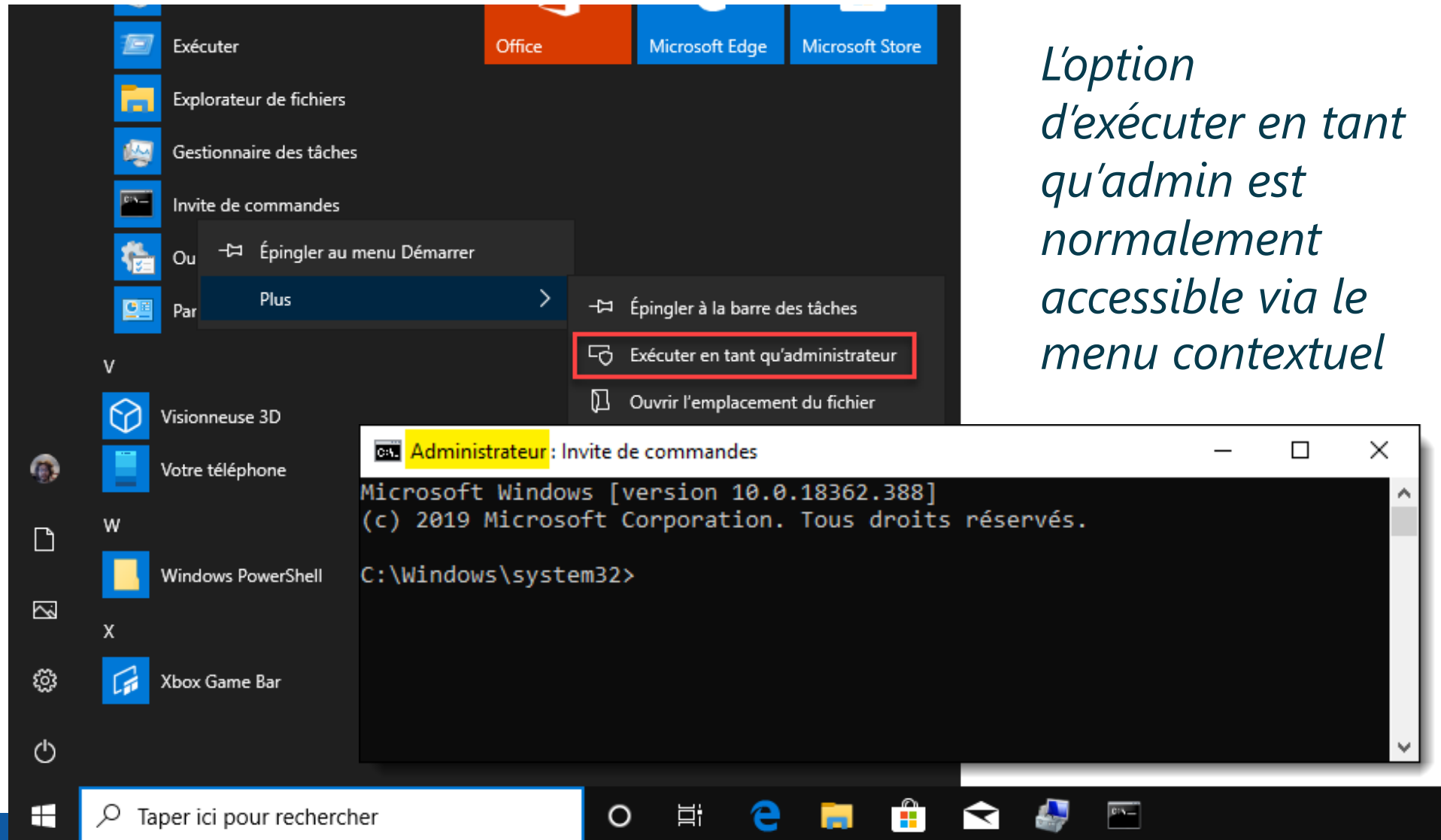
# Avertissement UAC



Un avertissement est affiché lorsque vous exécutez un programme qui demande des privilèges d'admin

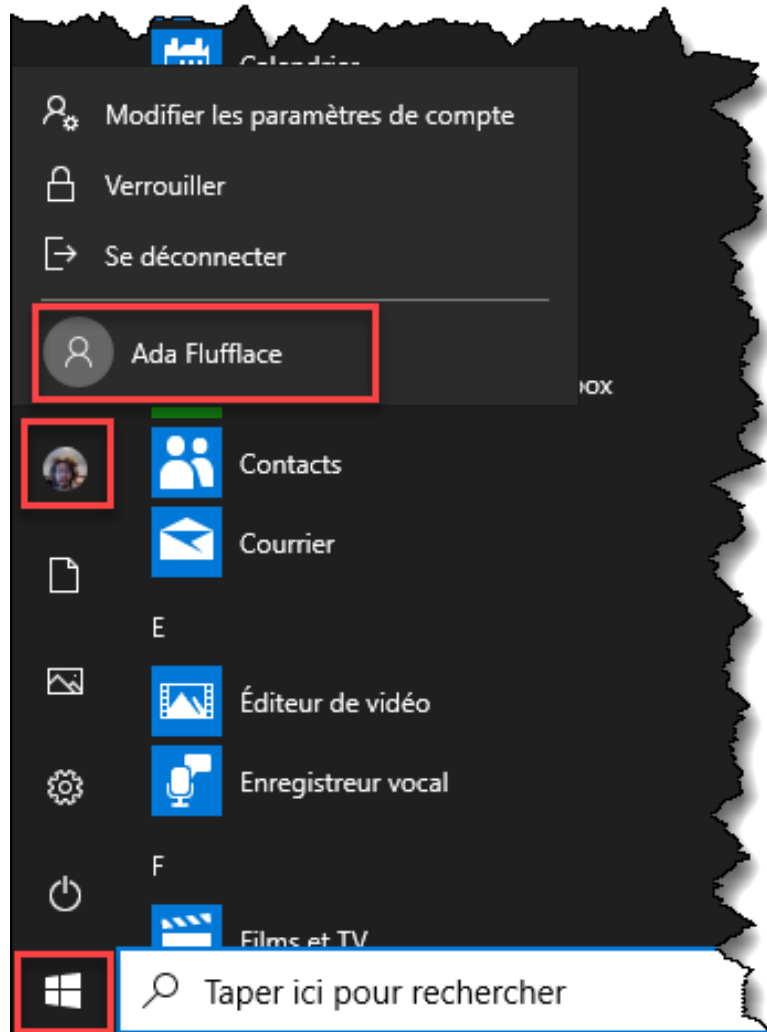


# Exécuter en tant qu'administrateur



*L'option  
d'exécuter en tant  
qu'admin est  
normalement  
accessible via le  
menu contextuel*

# Basculer entre utilisateurs



On peut démarrer une session avec un deuxième utilisateur sans mettre fin à la session du premier.

Cette fonctionnalité se nomme « Fast User Switching ».



# Utilisateurs et groupes locaux

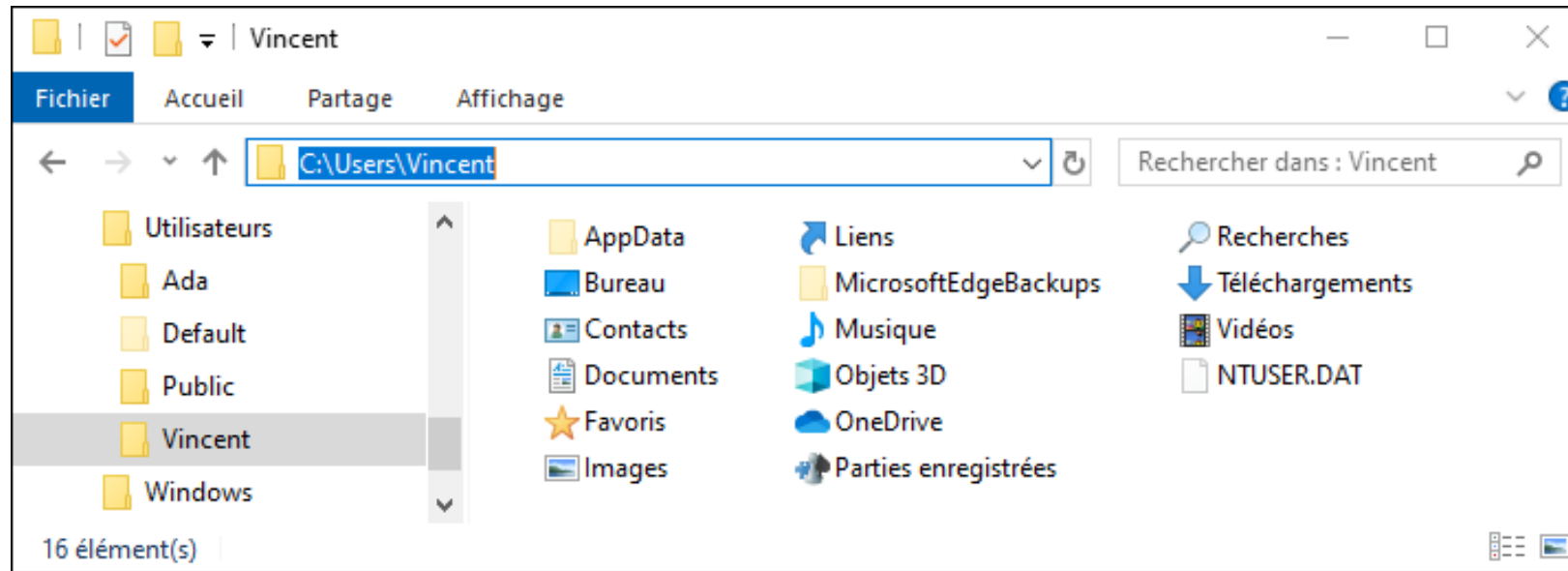


Chaque utilisateur possède :

Un nom d'utilisateur et un mot de passe

Un profil (répertoire personnel sous C:\Users)






On peut lui attribuer des permissions



# Comptes utilisateurs prédéfinis



- Compte utilisateur principal, que vous avez créé lors de l'installation de Windows
- Administrateur local
- Invité (Peu utilisé, il sert à des kiosques / démos)
- Comptes spéciaux utilisés par le système

Nom	
 Administrateur	Administrateur
 DefaultAccount	DefaultAccount
 Invité	Invité
 Vincent	Vincent
 WDAGUtilityAccount	WDAGUtilityAccount

# L'administrateur local



Toujours le même pour chaque système, mais traduit dans certaines langues

Français : Administrateur

Anglais : Administrator

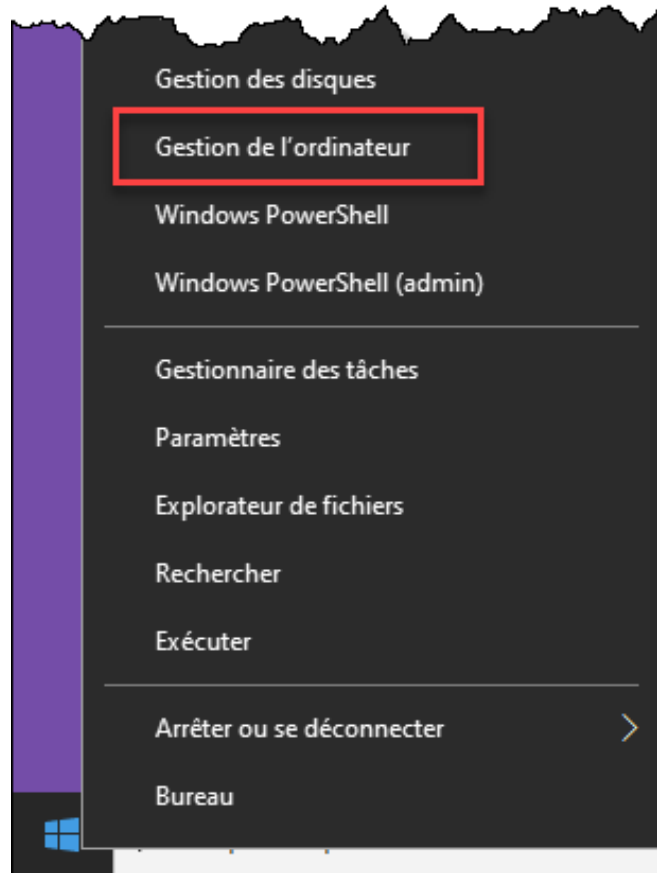
Espagnol : Administrador

Finnois : Järjestelmänvalvoja 🤔

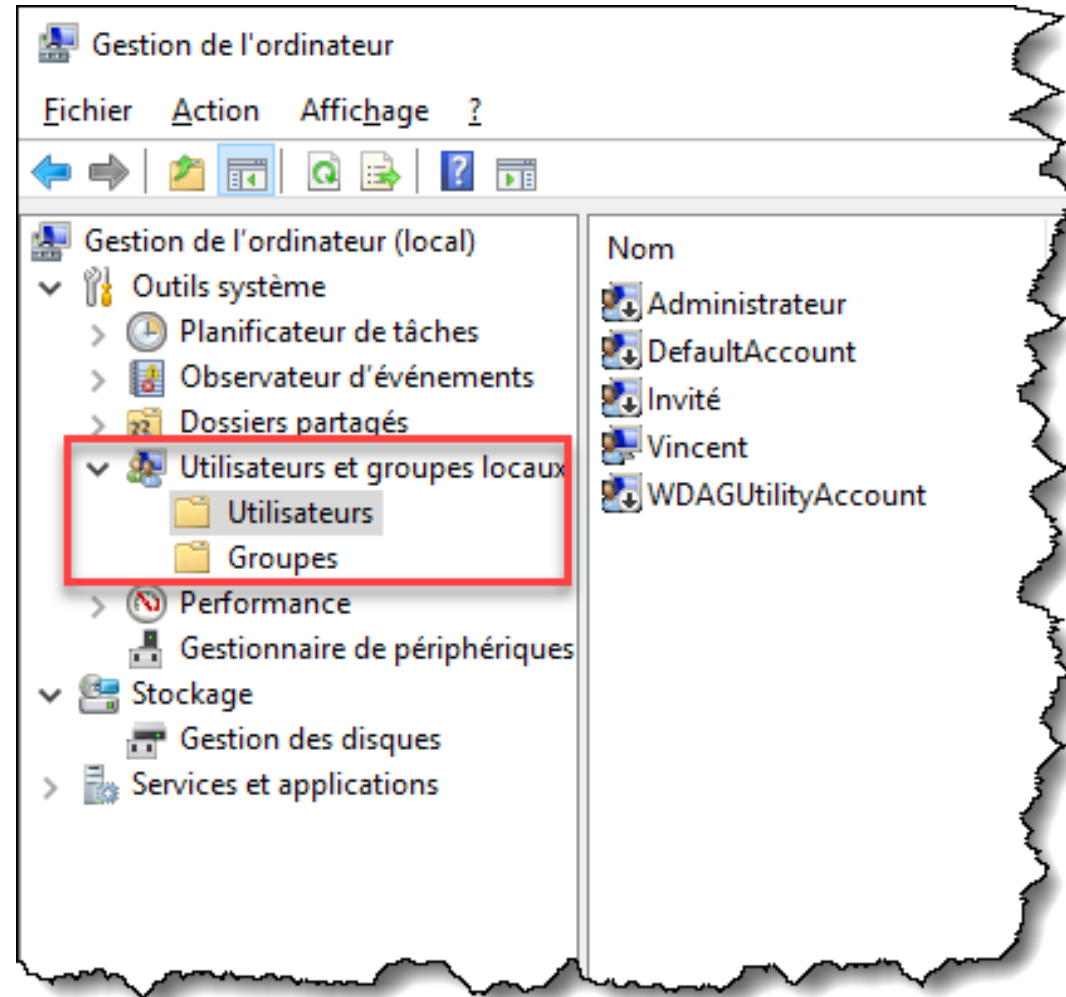
Possède des droits d'administration (membre du groupe des administrateurs)

Désactivé par défaut, pour des raisons de sécurité

# Console de gestion des utilisateurs

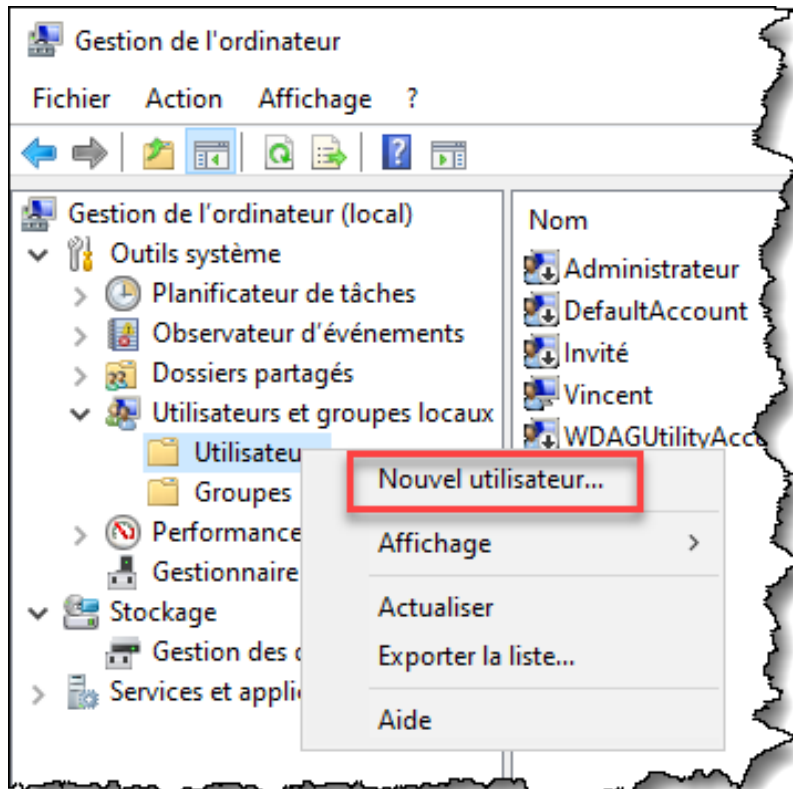


Clic droit sur le menu démarrer,  
Gestion de l'ordinateur





# Créer un compte utilisateur



Nouvel utilisateur

Nom d'utilisateur : Ada

Nom complet : Ada Flufflace

Description : Chatte de Vincent

Mot de passe : .....

Confirmer le mot de passe : .....

☒ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé


Aide Créer Fermer

# Propriétés d'un compte utilisateur



Propriétés de : Ada ? X

Général Membre de Profil

 Ada

---

Nom complet :

Description :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

☐ Le compte est verrouillé



Un groupe est un ensemble d'utilisateurs qui possèdent des droits ou des autorisations communes

Principaux groupes prédéfinis:

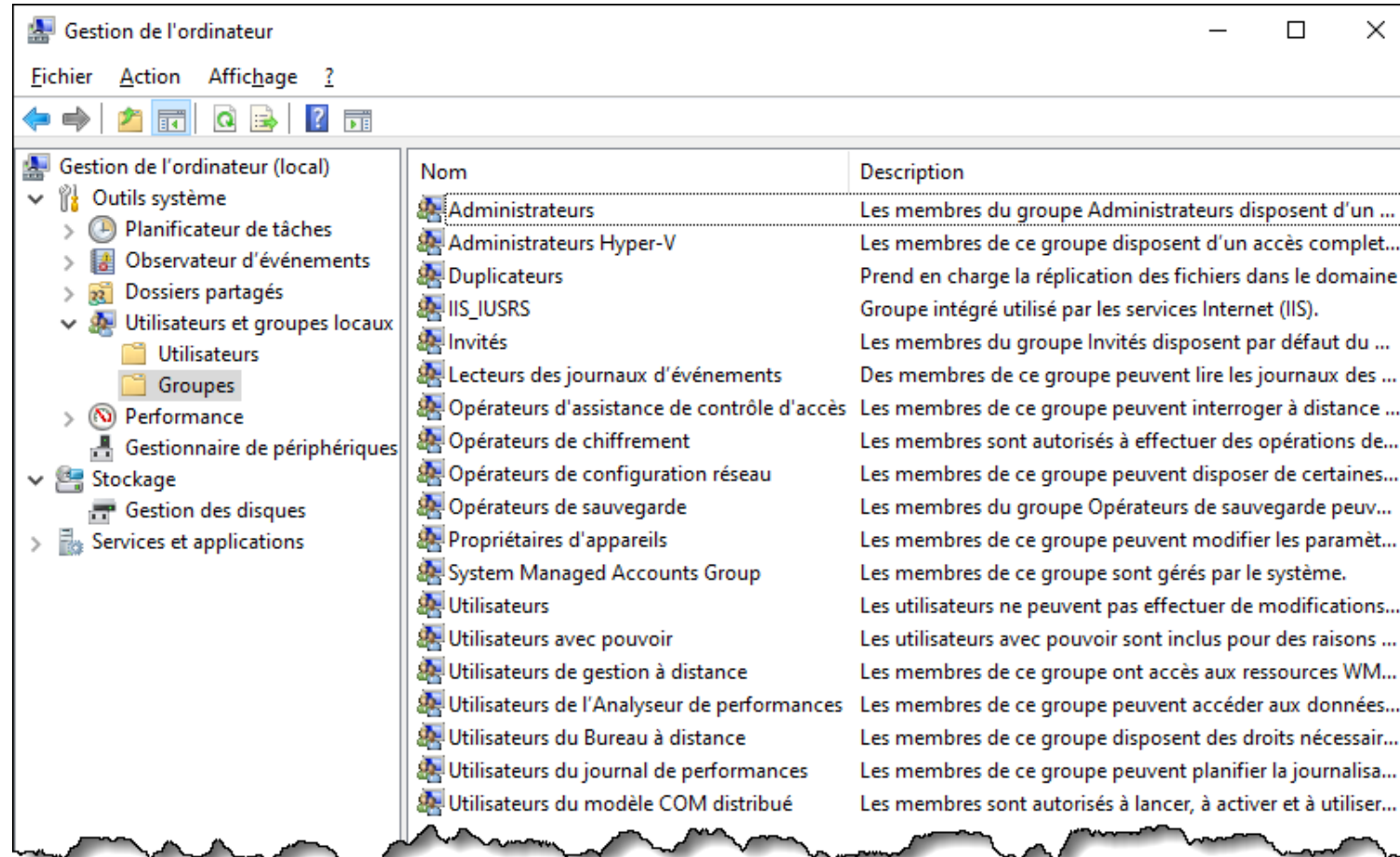
**Administrateurs:** dispose de droits d'administration

**Utilisateurs:** dispose d'un accès régulier au système

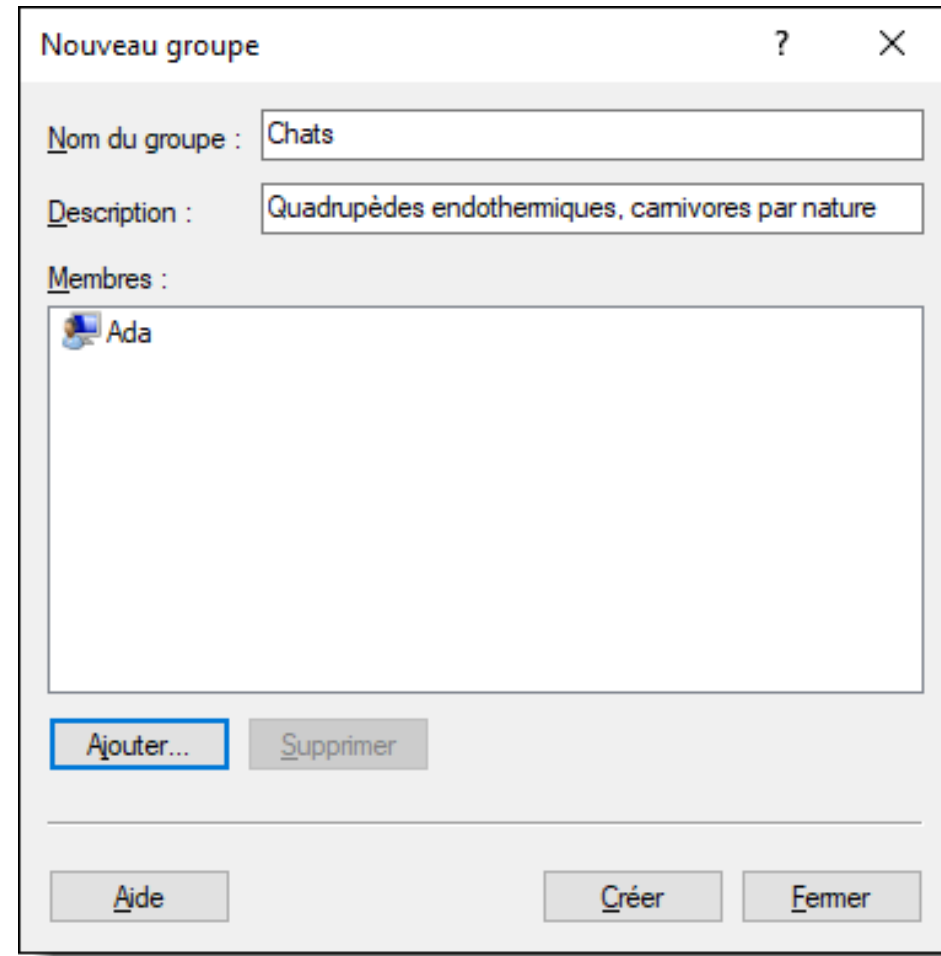
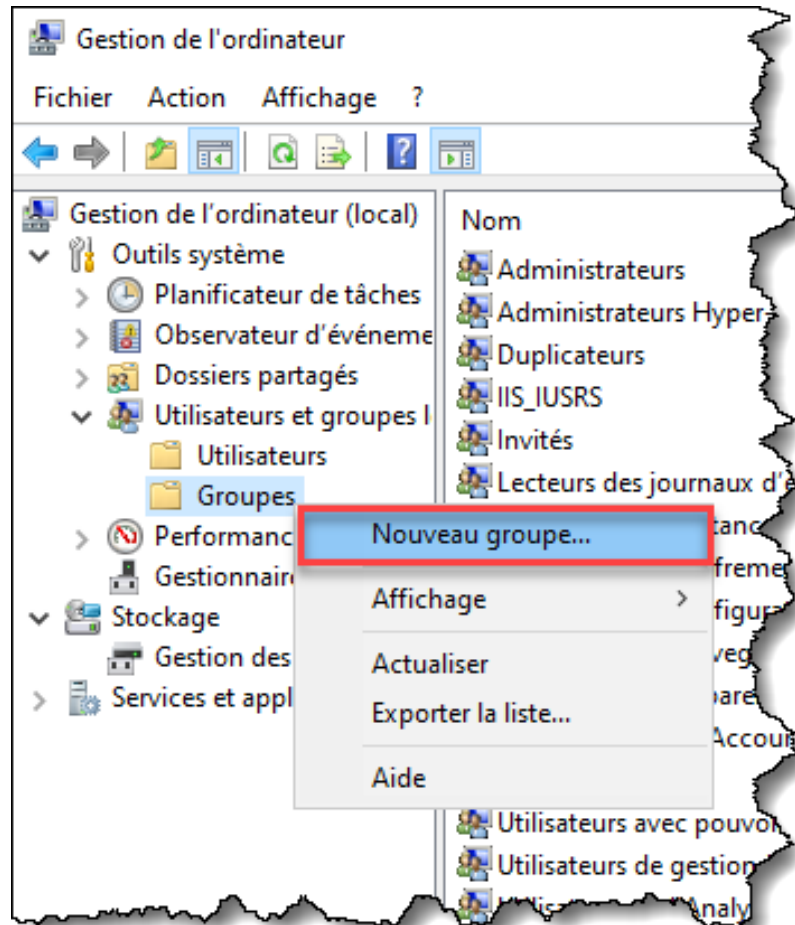
**Autres groupes** donnant des droits spécialisés

Par défaut, le premier utilisateur du système est placé dans le groupe Administrateurs, les utilisateurs subséquents dans Utilisateurs.

# Console de gestion des groupes



# Créer un groupe



# Ajouter des membres à un groupe



Sélectionnez des utilisateurs

Sélectionnez le type de cet objet :  
des utilisateurs ou Principaux de sécurité intégrés

À partir de cet emplacement :  
MEOWBOX

Entrez les noms des objets à sélectionner (exemples) :

Avancé...

Sélectionnez des utilisateurs

Sélectionnez le type de cet objet :  
des utilisateurs ou Principaux de sécurité intégrés

À partir de cet emplacement :  
MEOWBOX

Requêtes communes

Nom : Commence par

Description : Commence par

☐ Comptes désactivés

☐ Mot de passe sans date d'expiration

Nombre de jours depuis la dernière session :

Colonnes...

Rechercher

Arrêter

OK

Annuler

Résultats de la recherche :

Nom	Dossier
Ada	MEOWBOX
Administrateur	MEOWBOX
ANONYMOU...	
Ce certifica...	

# Utilisateurs et groupes locaux



On parle d'utilisateurs et de groupes locaux car il est possible de mettre des ordinateurs en réseau à l'aide d'un système appelé Active Directory. Il y a alors des utilisateurs et des groupes gérés centralement (comme ceux que vous utilisez sur les machines du CÉGEP).

On les appelle les utilisateurs et les groupes du domaine.

Les étudiant(e)s qui choisissent la voie de sortie en réseautique verront ce système dans le cours de Serveurs 1, en deuxième session.



# Permissions

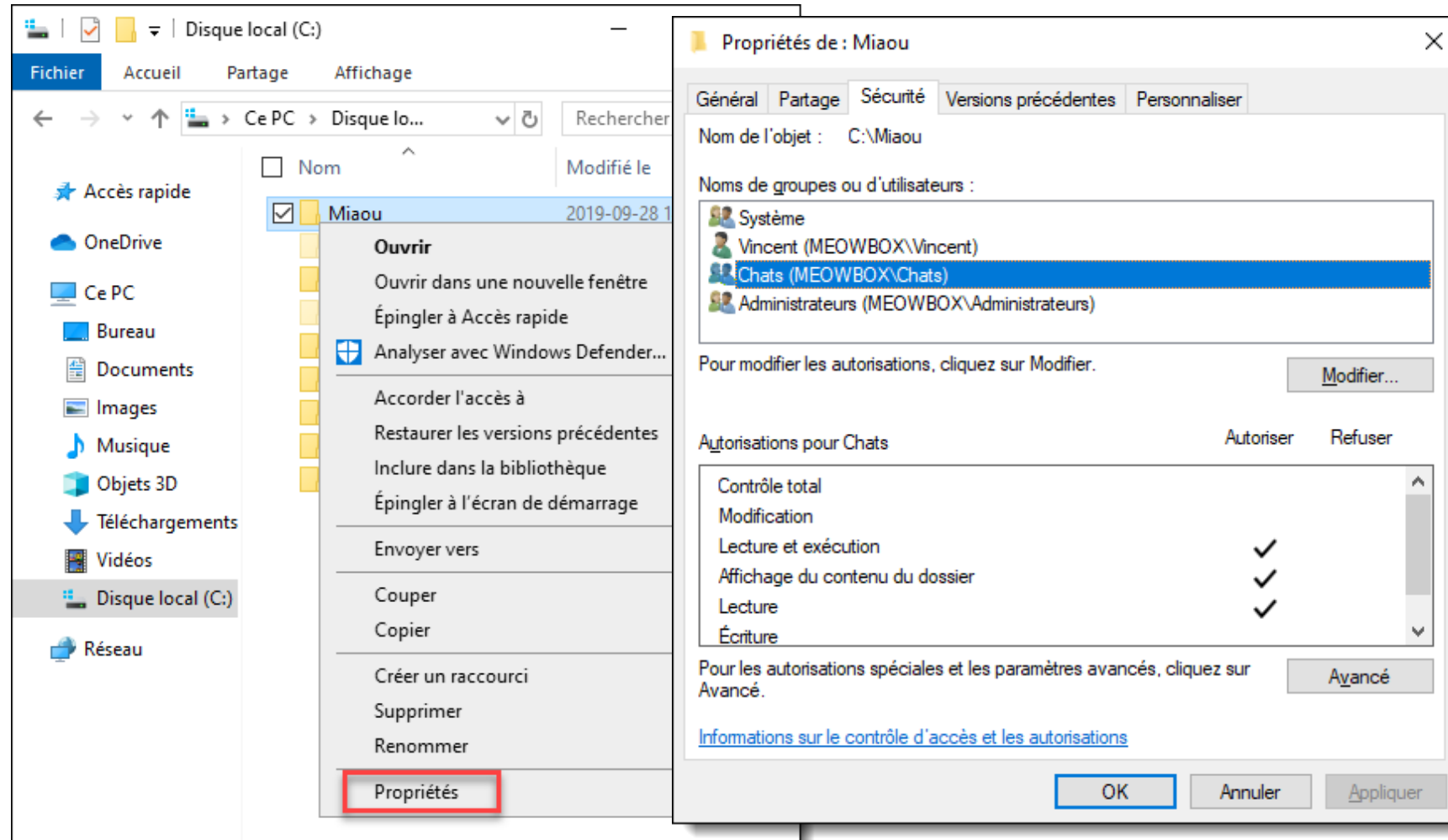




# Permissions sur les fichiers

- ❖ Sous Windows, les fichiers et les dossiers possèdent une **liste de contrôle d'accès** discrétionnaire (DACL)
- ❖ On peut **accorder** ou **refuser** des droits d'accès à des **utilisateurs** et des **groupes**.
- ❖ Les droits d'accès qu'on attribue à un groupe s'appliquent à **tous ses membres**.
- ❖ Par défaut, tous les fichiers et dossiers **héritent** des accès de leur parent dans l'arborescence
- ❖ Seuls les systèmes de fichiers **NTFS** et **exFAT** offrent un tel contrôle d'accès. Pas FAT32.

# Accéder à la liste de contrôle d'accès



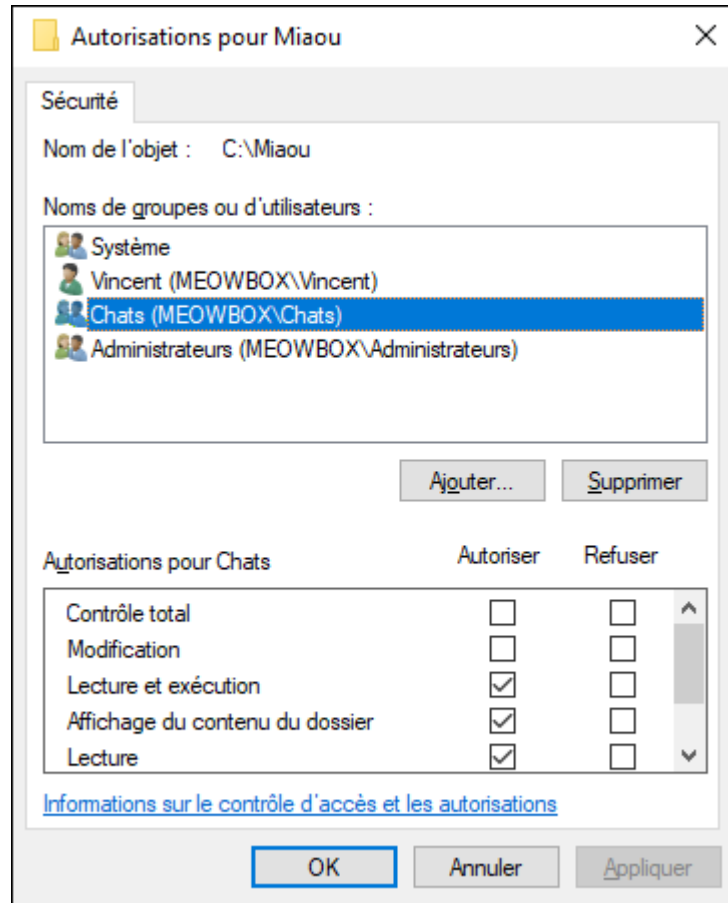
# Permissions



Autorisation	Effet
<b>Lecture</b>	Lire les fichiers
<b>Écriture</b>	Créer des nouveaux fichiers et dossiers
<b>Lecture et exécution</b>	Lire les fichiers et exécuter des fichiers de programme (.exe)
<b>Affichage du contenu du dossier</b>	Lister le contenu du dossier. Ne permet pas de lire le contenu des fichiers.
<b>Modification</b>	Modifier et effacer les fichiers ou dossiers
<b>Contrôle total</b>	Même chose que Modification, y compris la modification des permissions et la modification du propriétaire

*Lorsque ces permissions s'appliquent à un dossier, tout son contenu (fichiers et sous-dossiers) en héritent, à moins que l'héritage ne soit explicitement bloqué.*

# Modifier les permissions



Vous pouvez autoriser la modification, la lecture seulement, etc.

Vous pouvez aussi refuser ces privilèges.

Attention! Un refus de privilège a préséance sur toutes les autorisations.  
*C'est **peu recommandé** d'en faire usage.*

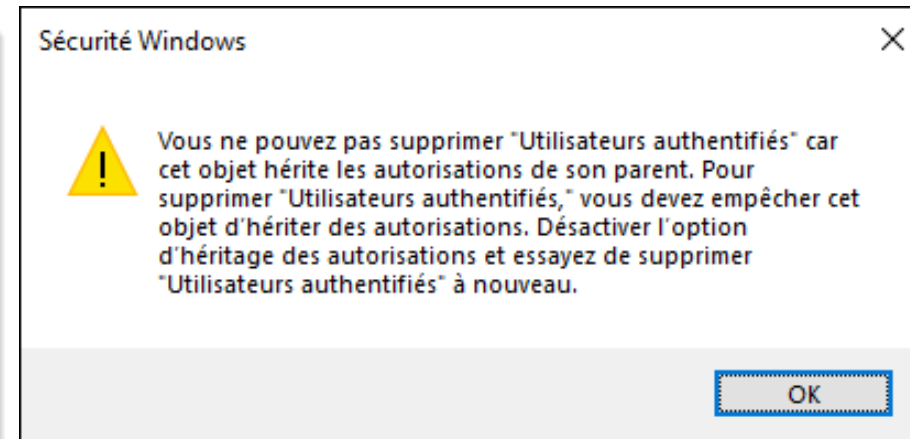
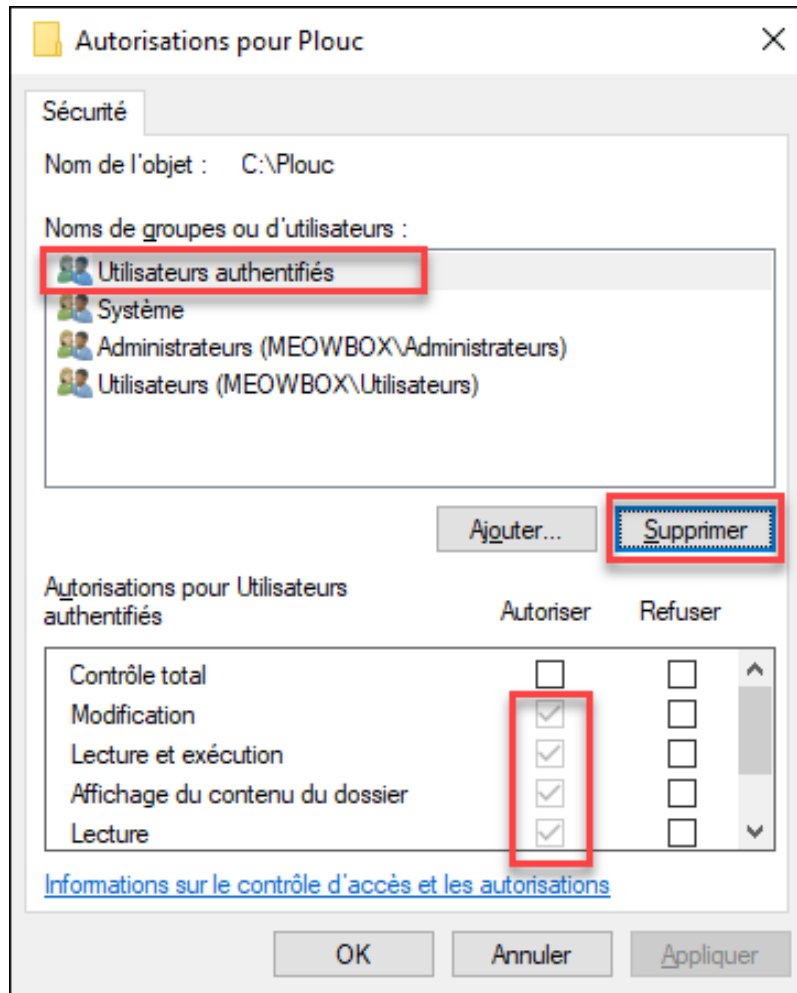


Par défaut, tous les utilisateurs du système ont les droits de modification à la racine du C:\ via le groupe spécial « Utilisateurs authentifiés ».

Donc, tout dossier qu'on y crée hérite de ces permissions. Tous les utilisateurs du système y ont un accès en modification.

Que faire si on veut que seuls les membres d'un groupe particulier aient accès à ce dossier?

# Suppression d'une permission héritée



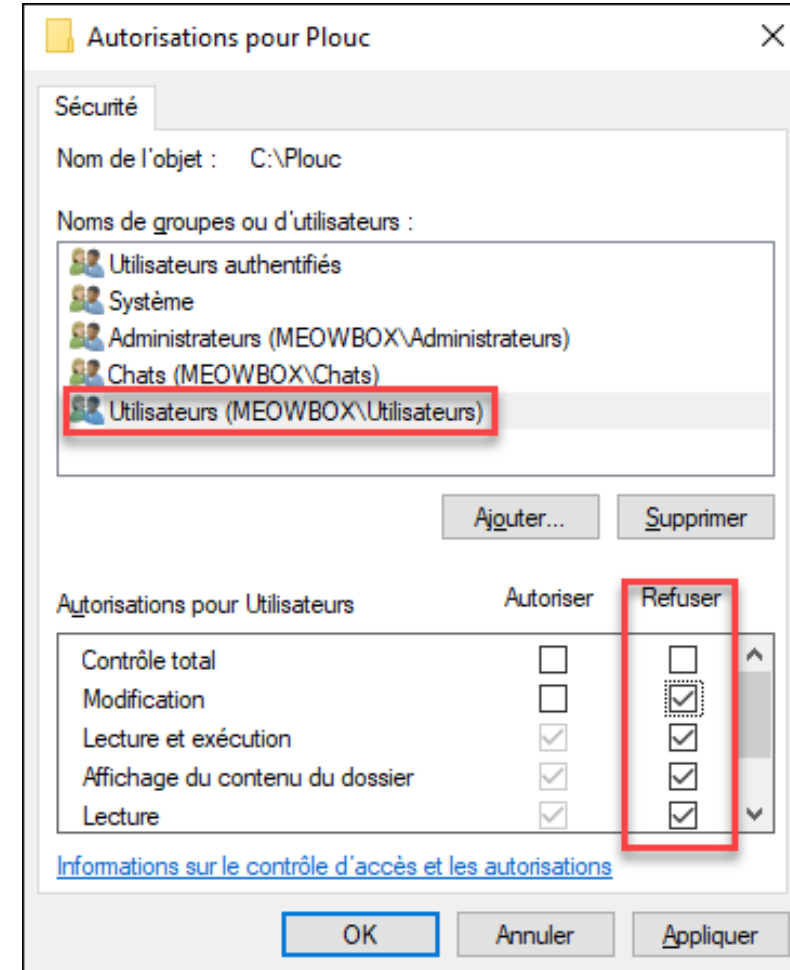
On ne peut pas supprimer un accès hérité du parent!

# Mauvaise solution : refuser l'accès



Si on refuse l'accès à Utilisateurs et qu'on accorde l'accès au groupe Chats, les membres du groupe Chats **n'auront pas accès**, car ils sont aussi membres du groupe Utilisateurs.

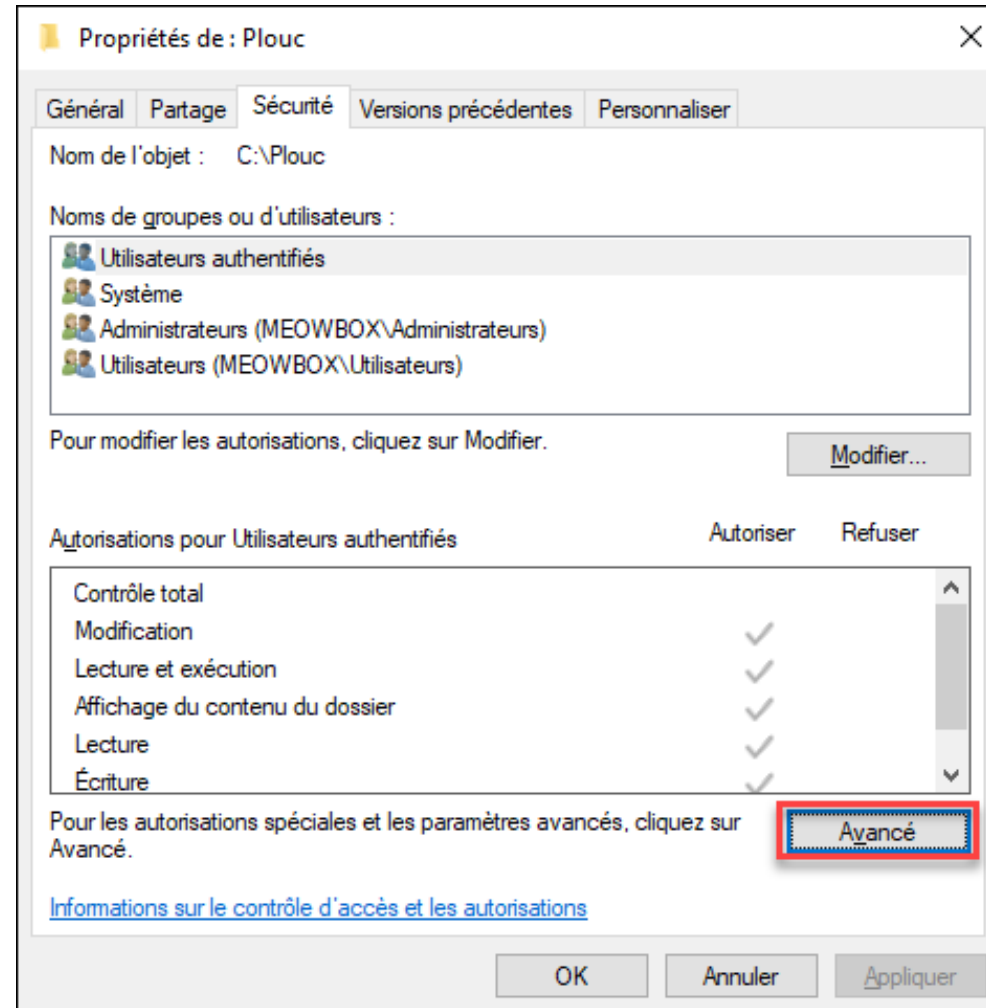
**IL NE FAUT PAS FAIRE ÇA!!!**



# Bonne solution : désactiver l'héritage

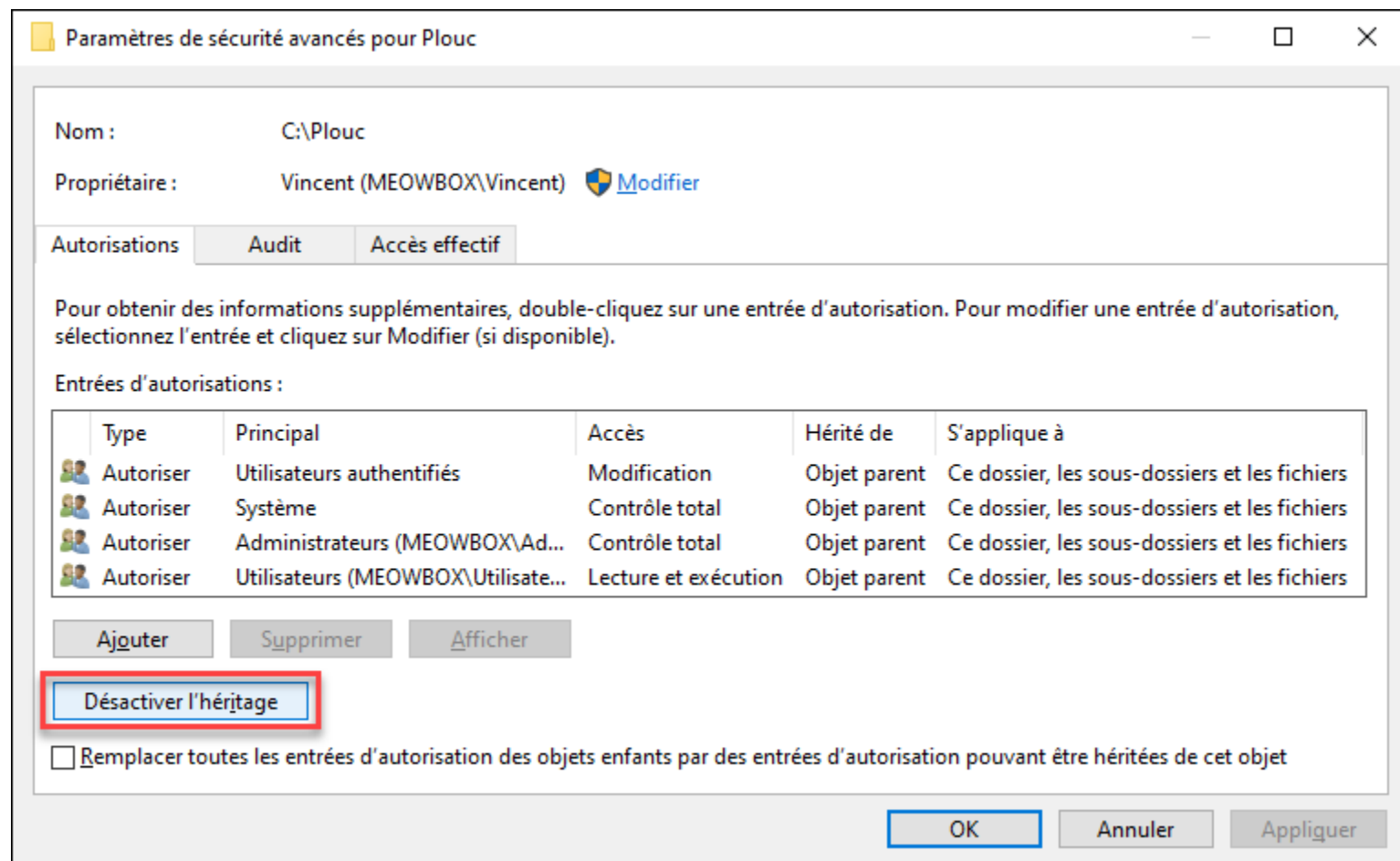


Il faut désactiver l'héritage pour se débarrasser des permissions héritées du parent. Pour cela, il faut accéder aux options avancées.





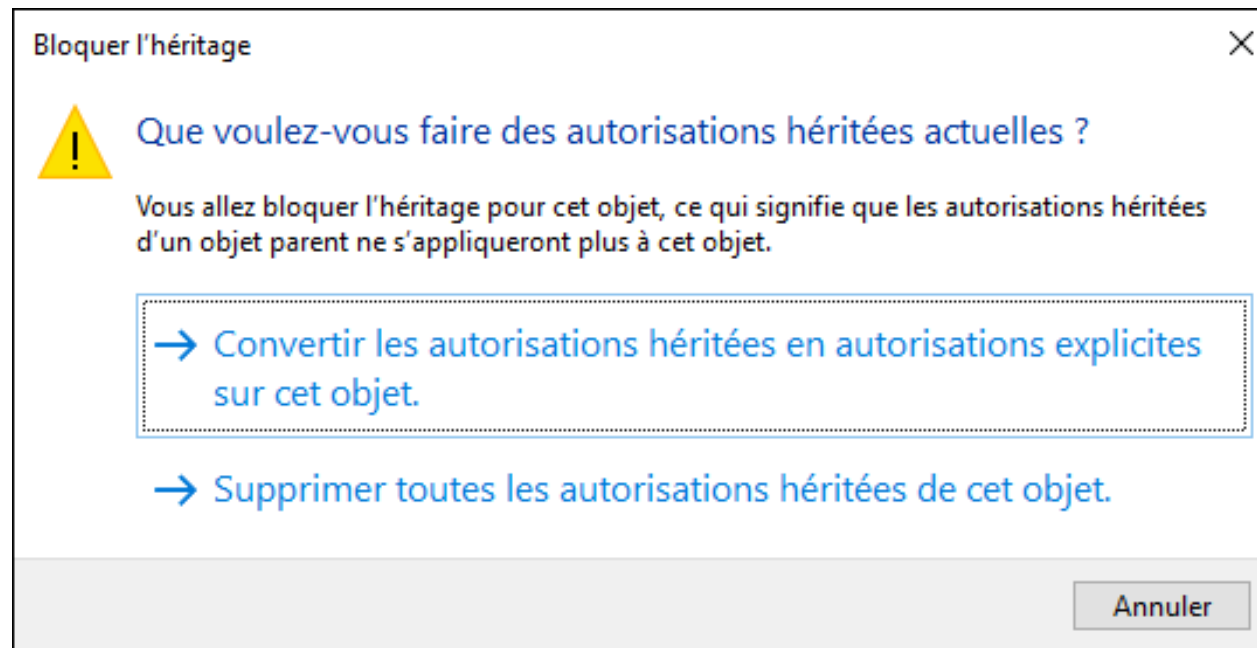
# Désactiver l'héritage



# Supprimer ou garder les autorisations?



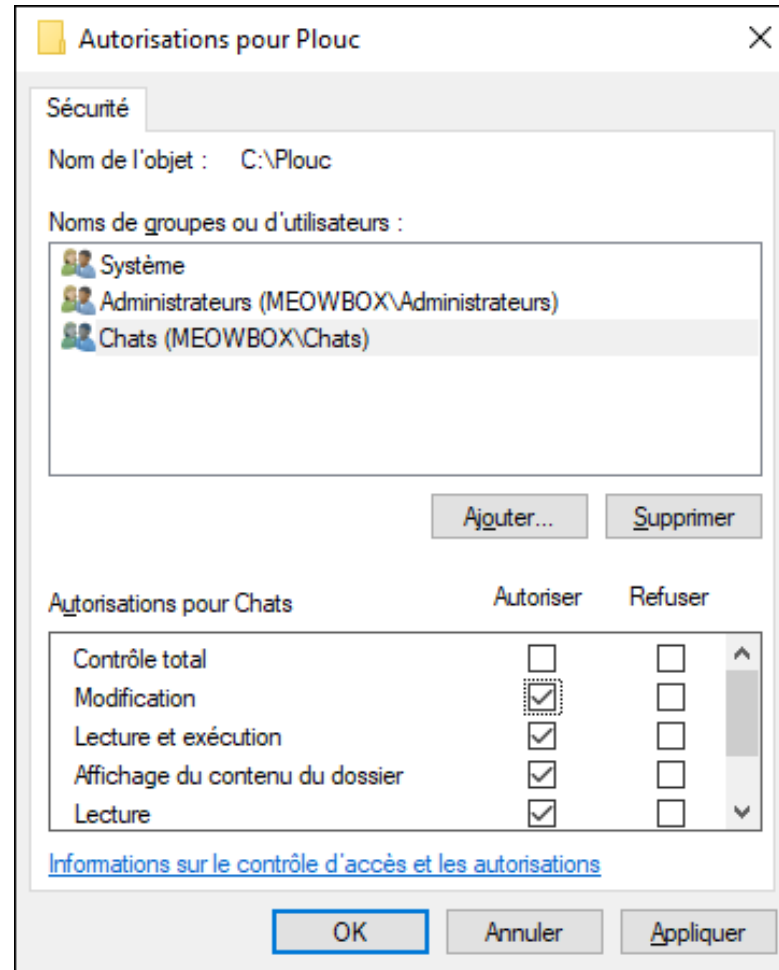
On peut soit copier les autorisations héritées (on pourra enfin les effacer et les changer) ou soit tout effacer et partir d'une liste vide.





# Héritage bloqué = problème réglé!

On peut maintenant modifier les privilèges existants.



Ici, seuls les chats, les administrateurs et les services du système auront accès à ce dossier. Les autres utilisateurs auront un accès refusé.

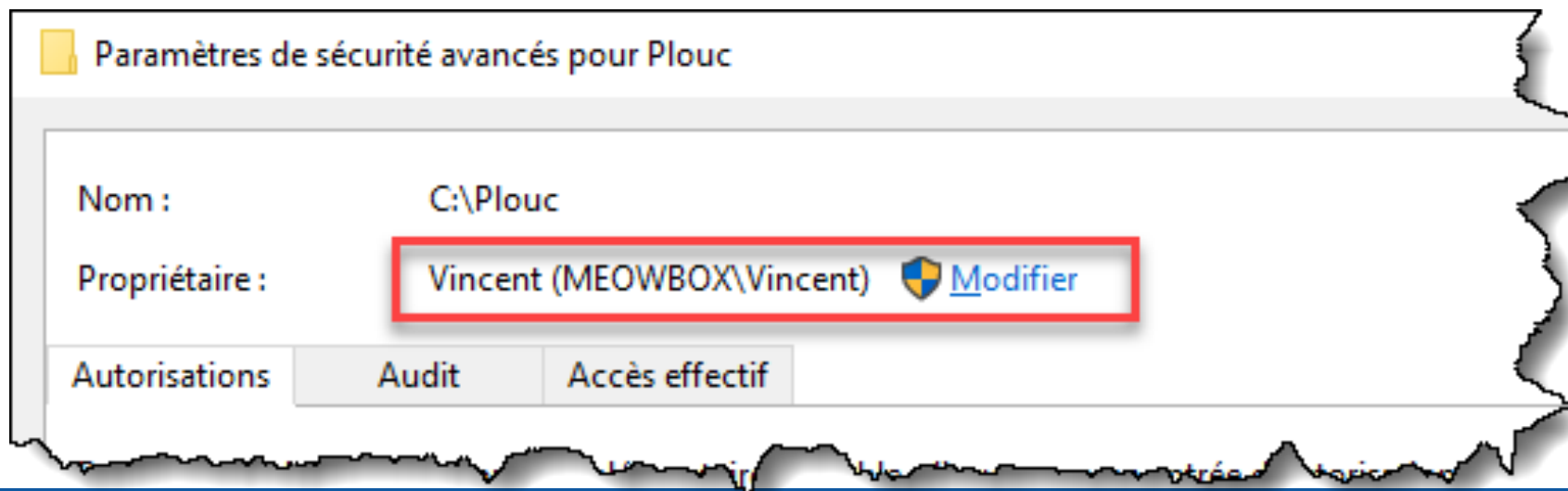
# Propriétaire



Le propriétaire d'un fichier ou dossier peut toujours modifier la liste de contrôle d'accès.

Généralement, c'est l'utilisateur qui a créé l'item qui en est propriétaire

Un administrateur peut en prendre possession.





# Ligne de commande

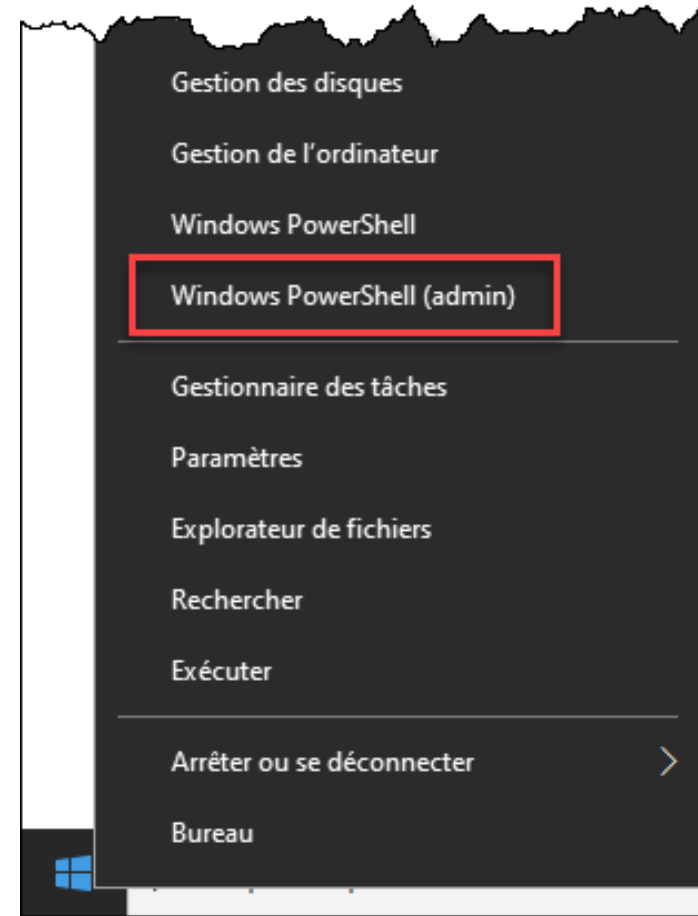
Exemples de commandes pour manipuler des utilisateurs, groupes et permissions avec l'invite de commande Windows PowerShell

# Utilisation de PowerShell



PowerShell permet une manipulation des utilisateurs, groupes et permissions plus simple et intuitive que l'invite de commande classique (CMD)

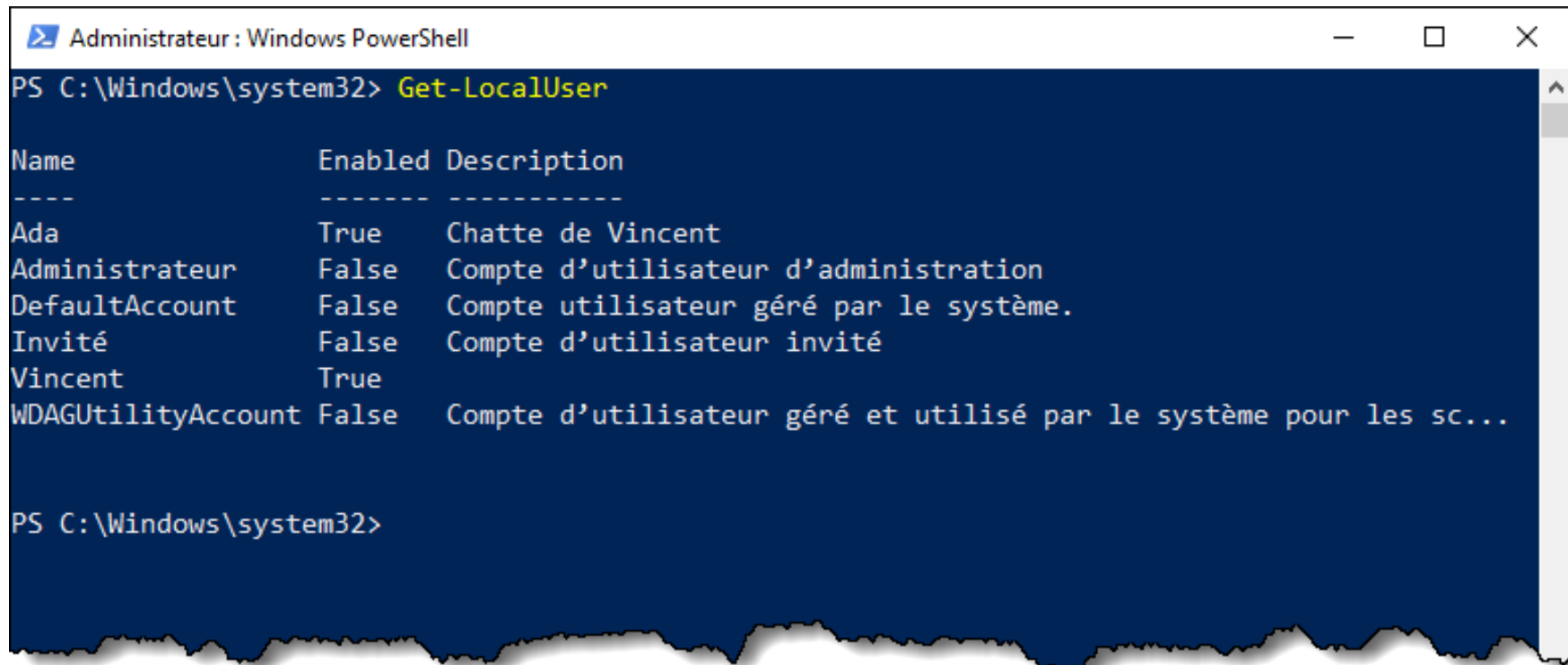
Ouvrir une invite PowerShell en tant qu'admin par un clic-droit sur le bouton Démarrer.





# Obtenir la liste des utilisateurs locaux

## Get-LocalUser



```
PS C:\Windows\system32> Get-LocalUser
```

Name	Enabled	Description
Ada	True	Chatte de Vincent
Administrateur	False	Compte d'utilisateur d'administration
DefaultAccount	False	Compte utilisateur géré par le système.
Invité	False	Compte d'utilisateur invité
Vincent	True	
WDAGUtilityAccount	False	Compte d'utilisateur géré et utilisé par le système pour les sc...

```
PS C:\Windows\system32>
```

# Information sur un utilisateur local



`Get-LocalUser -Name "username" | Format-List`

```
Administrateur : Windows PowerShell
PS C:\Windows\system32> Get-LocalUser -Name Ada | Format-List

AccountExpires      :
Description         : Chatte de Vincent
Enabled             : True
FullName            : Ada Flufflace
PasswordChangeableDate : 2019-10-05 19:28:53
PasswordExpires     : 2019-11-16 18:28:53
UserMayChangePassword : True
PasswordRequired    : True
PasswordLastSet     : 2019-10-05 19:28:53
LastLogon           : 2019-10-05 19:29:13
Name                : Ada
SID                 : S-1-5-21-1507397334-1719320053-894517008-1002
PrincipalSource      : local
```



# Obtenir la liste des groupes locaux



## Get-LocalGroup

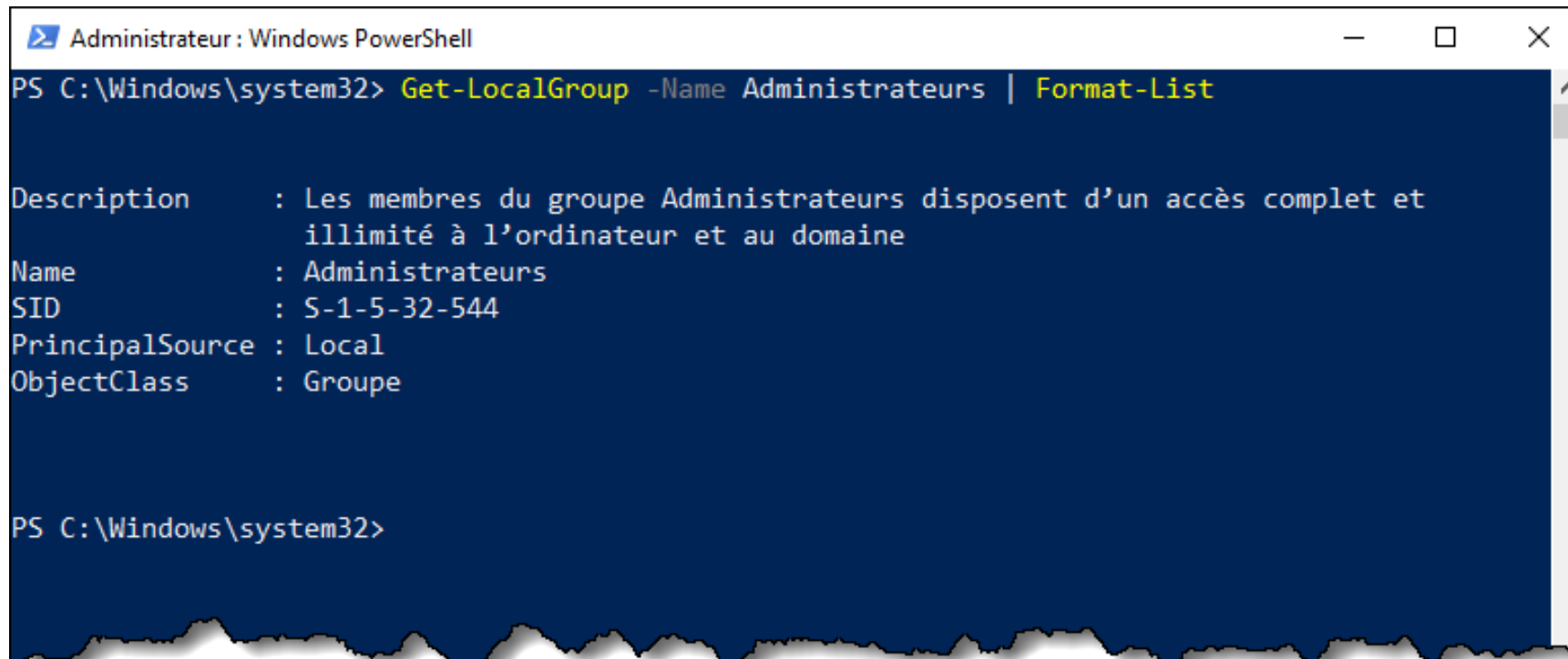
```
Administrateur : Windows PowerShell
PS C:\Windows\system32> Get-LocalGroup

Name                Description
----                -
Chats                Quadrupède endothermique, carnivore par nature
Administrateurs      Les membres du groupe Administrateurs disposen...
Administrateurs Hyper-V Les membres de ce groupe disposent d'un accès ...
Duplicateurs         Prend en charge la répllication des fichiers da...
IIS_IUSRS            Groupe intégré utilisé par les services Intern...
Invités              Les membres du groupe Invités disposent par dé...
Lecteurs des journaux d'événements Des membres de ce groupe peuvent lire les jour...
Opérateurs d'assistance de contrôle d'accès Les membres de ce groupe peuvent interroger à ...
Opérateurs de chiffrement Les membres sont autorisés à effectuer des opé...
Opérateurs de configuration réseau Les membres de ce groupe peuvent disposer de c...
Opérateurs de sauvegarde Les membres du groupe Opérateurs de sauvegarde...
Propriétaires d'appareils Les membres de ce groupe peuvent modifier les
```

# Information sur un groupe local



`Get-LocalGroup -Name "groupname" | Format-List`



```
Administrateur : Windows PowerShell
PS C:\Windows\system32> Get-LocalGroup -Name Administrateurs | Format-List

Description      : Les membres du groupe Administrateurs disposent d'un accès complet et
                   illimité à l'ordinateur et au domaine
Name             : Administrateurs
SID              : S-1-5-32-544
PrincipalSource  : Local
ObjectClass      : Groupe

PS C:\Windows\system32>
```

# Créer un nouveau groupe local



`New-LocalGroup -Name "groupname"`

```
Administrateur : Windows PowerShell
PS C:\Windows\system32> New-LocalGroup -Name "Astronautes"

Name      Description
----      -
Astronautes

PS C:\Windows\system32>
```

# Lister les membres d'un groupe local



`Get-LocalGroupMember -Name "username"`

```
PS C:\Windows\system32> Get-LocalGroupMember -Name Administrateurs
```

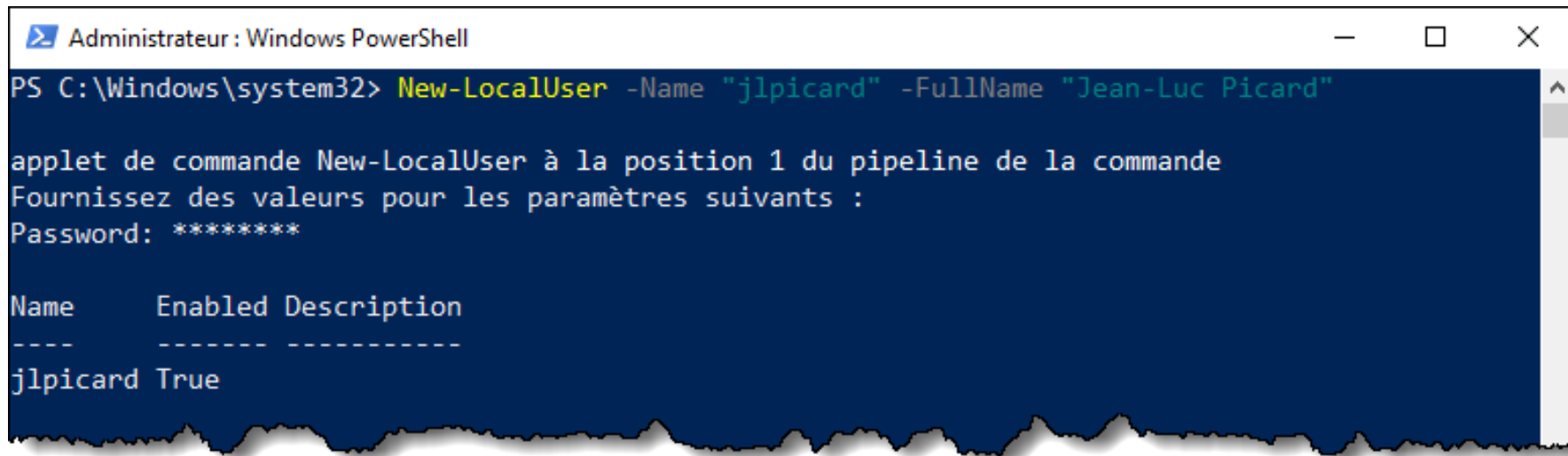
ObjectClass	Name	PrincipalSource
Utilisateur	MEOWBOX\Administrateur	Local
Utilisateur	MEOWBOX\Vincent	Local

```
PS C:\Windows\system32>
```

# Créer un nouvel utilisateur local



```
New-LocalUser -Name "username" -FullName  
"Prenom Nom"
```



```
PS C:\Windows\system32> New-LocalUser -Name "jlpicard" -FullName "Jean-Luc Picard"
```

applet de commande New-LocalUser à la position 1 du pipeline de la commande  
Fournissez des valeurs pour les paramètres suivants :  
Password: \*\*\*\*\*

Name	Enabled	Description
jlpicard	True	

**Attention!** Le compte est créé, mais il n'est membre d'aucun groupe. Il ne pourra pas se connecter au système s'il n'est pas au moins membre du groupe Utilisateurs. Il faudra l'ajouter à ce groupe avec une seconde commande.

# Ajouter un membre à un groupe local



```
Add-LocalGroupMember -Group "groupname" -Member "username"
```

```
Administrateur : Windows PowerShell
PS C:\Windows\system32> Add-LocalGroupMember -Group "Astronautes" -Member "jlpicard"
PS C:\Windows\system32> Get-LocalGroupMember -Group "Astronautes"

ObjectClass Name                PrincipalSource
-----
Utilisateur MEOWBOX\jlpicard Local

PS C:\Windows\system32> 
```

# Afficher la liste de contrôle d'accès (ACL)



Get-Acl -Path "*chemin*" | Format-List

```
Administrateur : Windows PowerShell
PS C:\Windows\system32> Get-Acl -Path "C:\Plouc" | Format-List

Path      : Microsoft.PowerShell.Core\FileSystem::C:\Plouc
Owner     : MEOWBOX\Vincent
Group     : MEOWBOX\Aucun
Access    : AUTORITE NT\Utilisateurs authentifiés Allow Modify, Synchronize
           AUTORITE NT\Système Allow FullControl
           BUILTIN\Administrateurs Allow FullControl
           BUILTIN\Utilisateurs Allow ReadAndExecute, Synchronize
Audit     :
Sddl      : O:S-1-5-21-1507397334-1719320053-894517008-1001G:S-1-5-21-1507397334-1719320053-8945
           17008-513D:PAI(A;OICI;0x1301bf;;;AU)(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;OICI;0x1200a9
           ;;;BU)
```