



Durée 2 heures

420-1S6 Système d'exploitation

Département d'informatique

Automne 2022

## Lab18 – Utilisateurs, groupes &amp; permissions Windows

Formatif

## Solutionnaire






### Configuration d'utilisateurs, groupes et permissions dans Windows

## 1 Utilisateurs

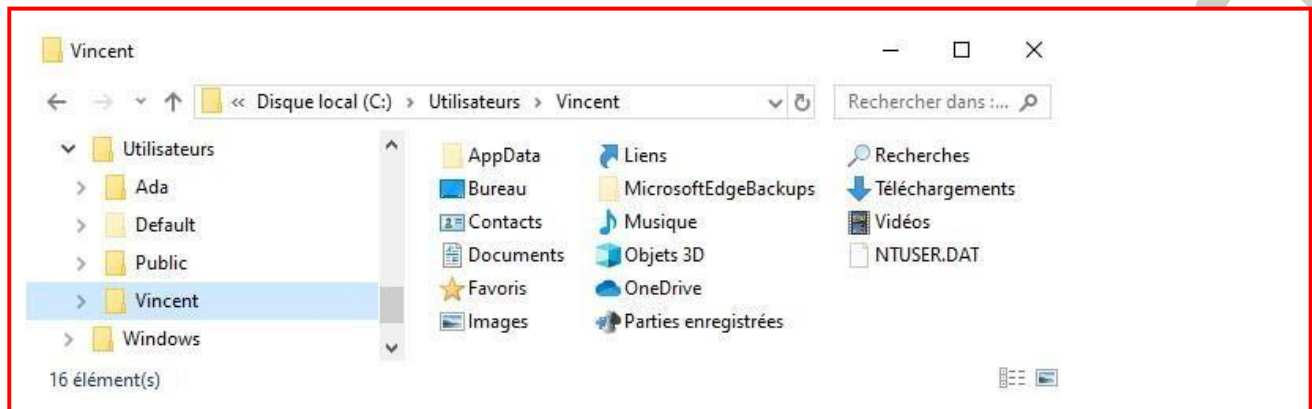
Les utilisateurs sont des identités définies sur le système afin de donner accès aux ressources du système. Chaque utilisateur possède un nom d'utilisateur et un mot de passe, ainsi que d'autres attributs (le nom complet, une description, etc.)

Pour voir les utilisateurs du système, vous devez d'abord démarrer la console de gestion de l'ordinateur. Vous trouverez cet outil dans le menu contextuel qui apparaît en cliquant sur le bouton Démarrer avec le bouton de droite de la souris, mais il existe d'autres manières d'y accéder (comme taper `compmgmt.msc` dans une invite de commandes).

Q1 Quels sont les comptes utilisateurs prédéfinis sous Windows? Faites une capture d'écran.

 Administrateur	Compte d'utilisateur d'administration
 DefaultAccount	Compte utilisateur géré par le système.
 Invité	Compte d'utilisateur invité
 Vincent	
 WDAGUtilityAccount	Compte d'utilisateur géré et utilisé par le...

Q2 Quel est l'équivalent du répertoire personnel dans Windows? Faites une capture d'écran de sa racine dans l'explorateur de fichiers.



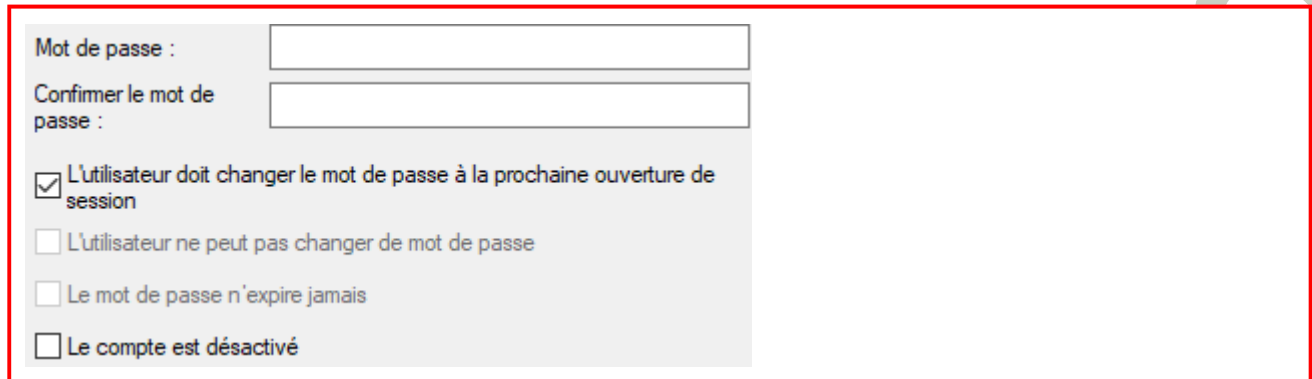
Q3 Certains comptes prédéfinis sont marqués d'une petite flèche pointant vers le bas. Que cela signifie-t-il?

Le compte est désactivé.

Q4 Créez les quatre comptes suivants à l'aide de la console de gestion des utilisateurs : Luke, Han, Yoda, Vader. Mettez-leur le mot de passe `Passw0rd` et décochez « *L'utilisateur doit changer le mot de passe...* ». Montrez une capture d'écran de la console graphique montrant les nouveaux comptes.

Nom	Nom complet	Description
Administrateur		Compte d'utilisateur d'administrateur
DefaultAccount		Compte utilisateur géré par le système
Han	Han	
Invité		Compte d'utilisateur invité
Luke	Luke	
Vader	Vader	
Vincent		
WDAGUtilityAccount		Compte d'utilisateur géré par le système
Yoda	Yoda	

Q5 Pendant la création d'un utilisateur, quelles sont les options qui s'offrent à vous relativement à son mot de passe?



Mot de passe :

Confirmer le mot de passe :

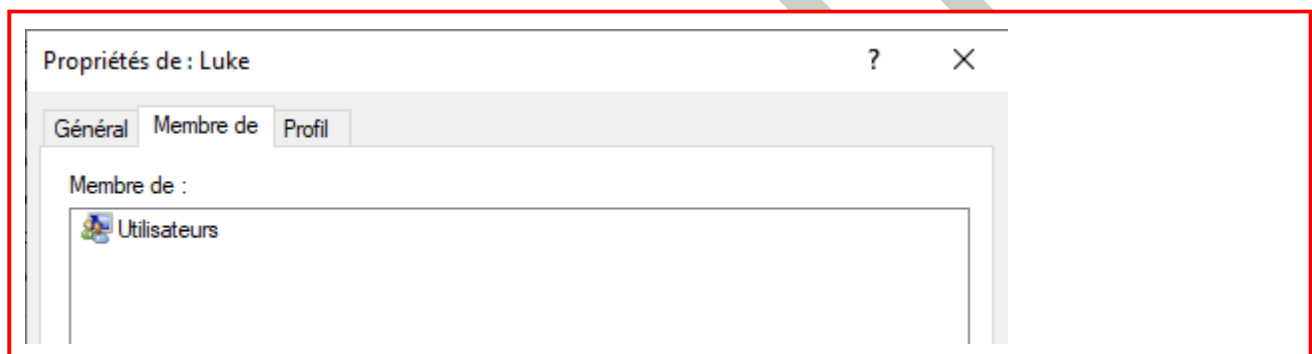
☒ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

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

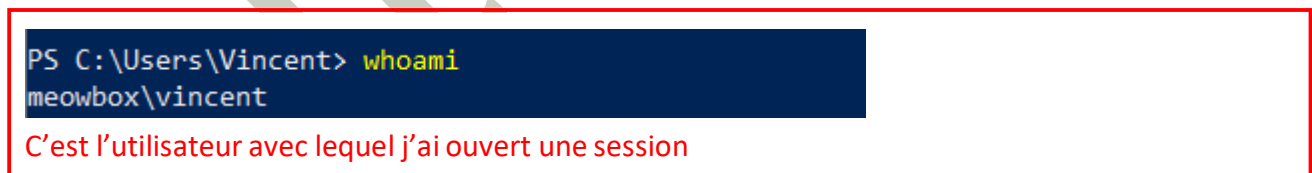
☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

Q6 De quel(s) groupe(s) font partie ces utilisateurs? Insérez une capture d'écran avec Luke.



Q7 Ouvrez un terminal CMD ou PowerShell et tapez la commande `whoami`. Que représente le résultat?



```
PS C:\Users\Vincent> whoami
meowbox\vincent
```




















C'est l'utilisateur avec lequel j'ai ouvert une session

## 2 Groupes

Les groupes sont des regroupements d'utilisateurs auxquels on peut conférer des permissions ou des privilèges sur le système.

Ouvrez la console de gestion des groupes. Vous constaterez que plusieurs groupes ont été créés automatiquement lors de l'installation de Windows.

Q8 Quels sont les groupes prédéfinis sous Windows? Faites une capture d'écran.

 Administrateurs	Les membres du groupe Administ...
 Administrateurs Hyper-V	Les membres de ce groupe dispos...
 Duplicateurs	Prend en charge la réplication des...
 IIS_IUSRS	Groupe intégré utilisé par les servi...
 Invités	Les membres du groupe Invités di...
 Lecteurs des journaux d'événements	Des membres de ce groupe peuve...
 Opérateurs d'assistance de contrôle d'accès	Les membres de ce groupe peuve...
 Opérateurs de chiffrement	Les membres sont autorisés à effe...
 Opérateurs de configuration réseau	Les membres de ce groupe peuve...
 Opérateurs de sauvegarde	Les membres du groupe Opérate...
 Propriétaires d'appareils	Les membres de ce groupe peuve...
 System Managed Accounts Group	Les membres de ce groupe sont g...
 Utilisateurs	Les utilisateurs ne peuvent pas eff...
 Utilisateurs avec pouvoir	Les utilisateurs avec pouvoir sont ...
 Utilisateurs de gestion à distance	Les membres de ce groupe ont ac...
 Utilisateurs de l'Analyseur de performances	Les membres de ce groupe peuve...
 Utilisateurs du Bureau à distance	Les membres de ce groupe dispos...
 Utilisateurs du journal de performances	Les membres de ce groupe peuve...
 Utilisateurs du modèle COM distribué	Les membres sont autorisés à lan...

Q9 Quel groupe confère à l'utilisateur un pouvoir quasi-absolu sur le système, comme installer des applications, changer les paramètres du système et gérer les utilisateurs et les groupes?

Administrateurs

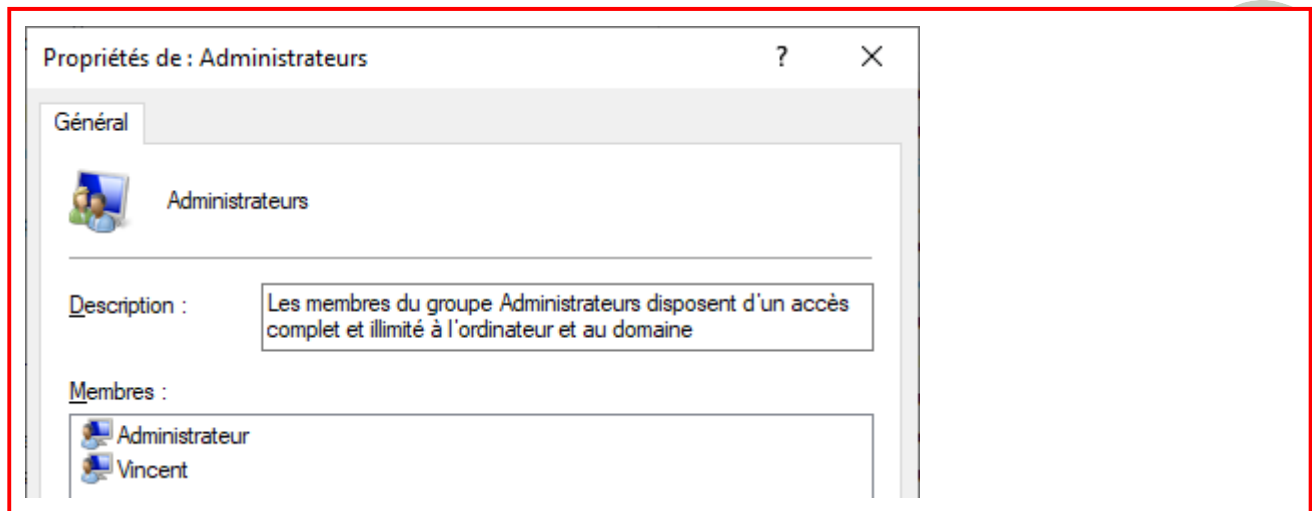
Q10 Quel groupe donne le droit d'utiliser le système et y démarrer une session?

Utilisateurs

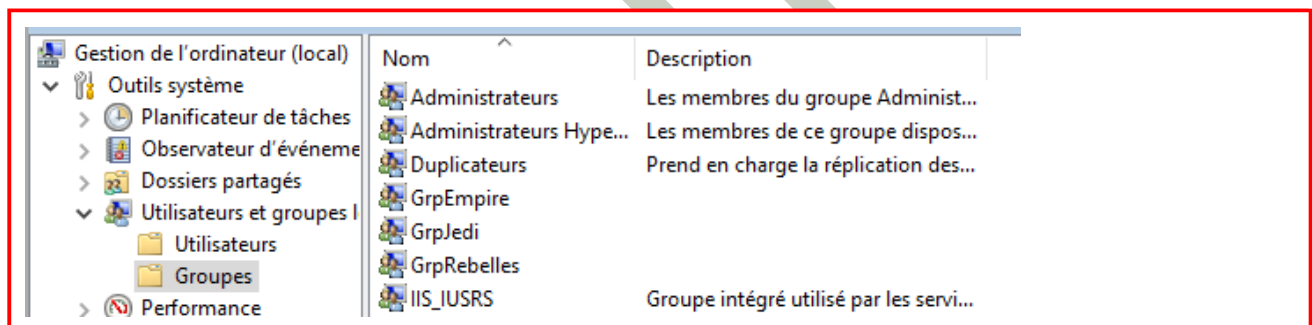
Q11 Selon vous, pourquoi y a-t-il autant de groupes prédéfinis? À quoi servent-ils?

A attribuer des privilèges spécifiques pour réaliser des tâches, sans donner tous les droits.

Q12 Quel(s) utilisateur(s) sont administrateurs du système? Insérez une capture d'écran le montrant.

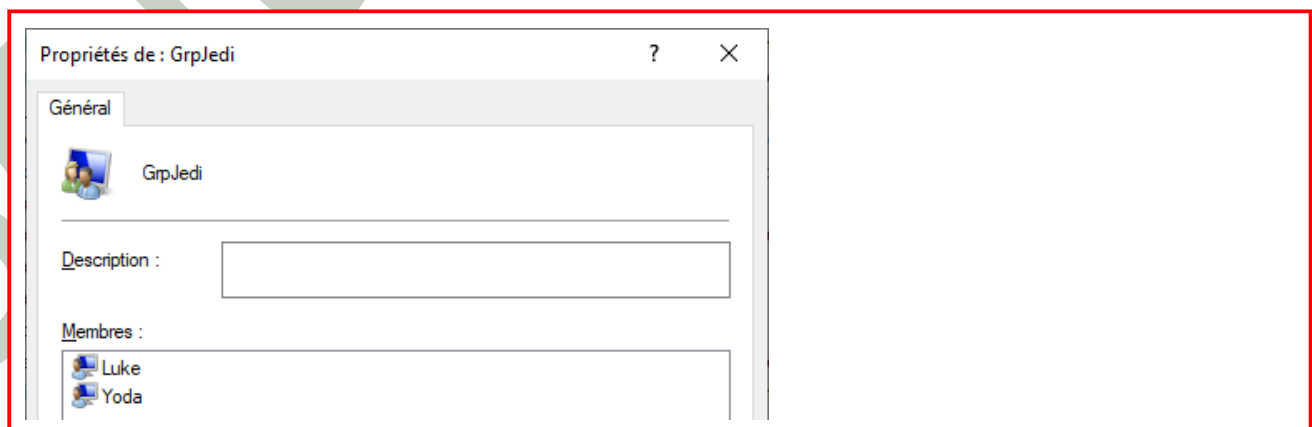


Q13 Dans la console de gestion des groupes, créez trois groupes : GrpJedi, GrpRebelles, GrpEmpire. Insérez une capture d'écran de la console graphique après la création de ces groupes.

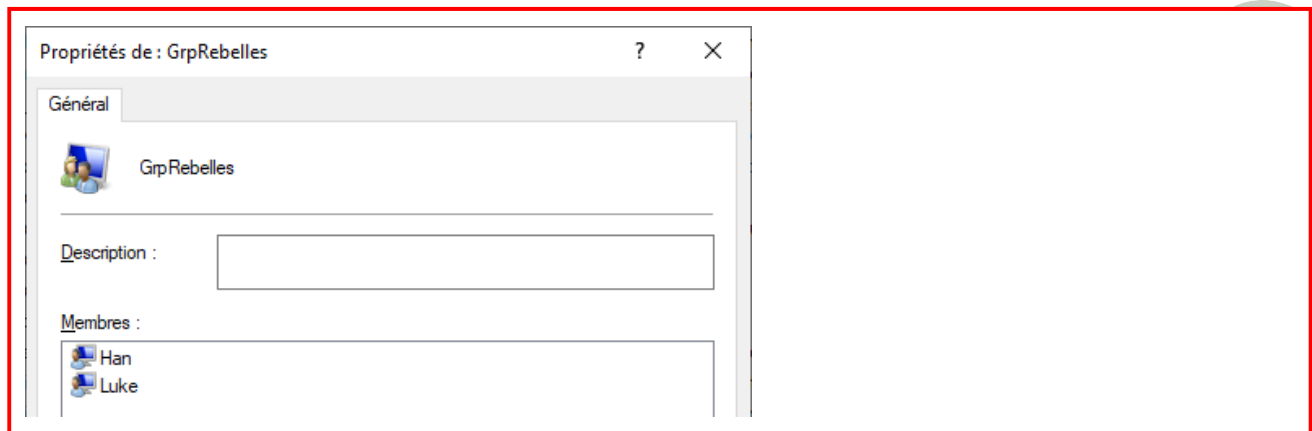


Q14 Ajoutez les utilisateurs suivants dans le groupe spécifié, et montrez une capture d'écran du groupe.

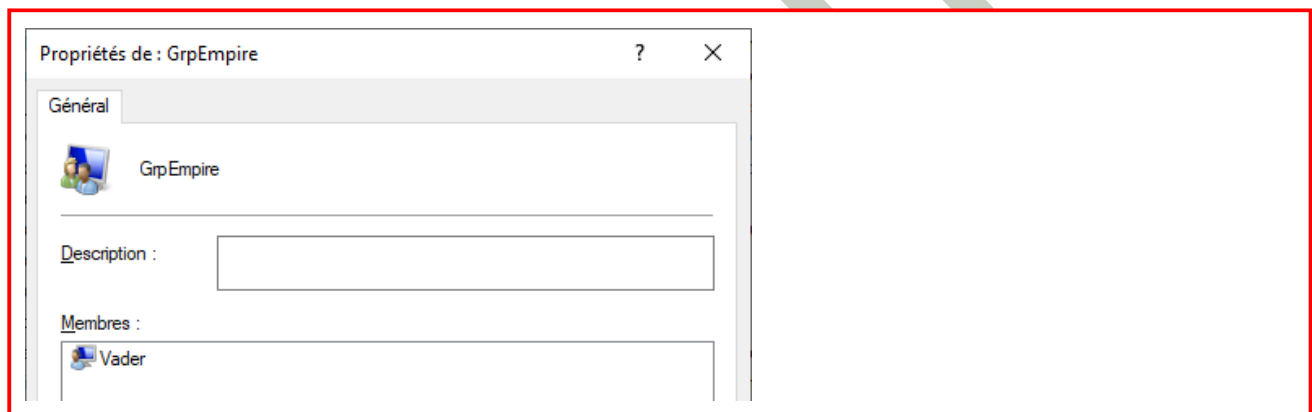
a) Luke et Yoda dans le groupe GrpJedi



b) Luke et Han dans le groupe GrpRebelles

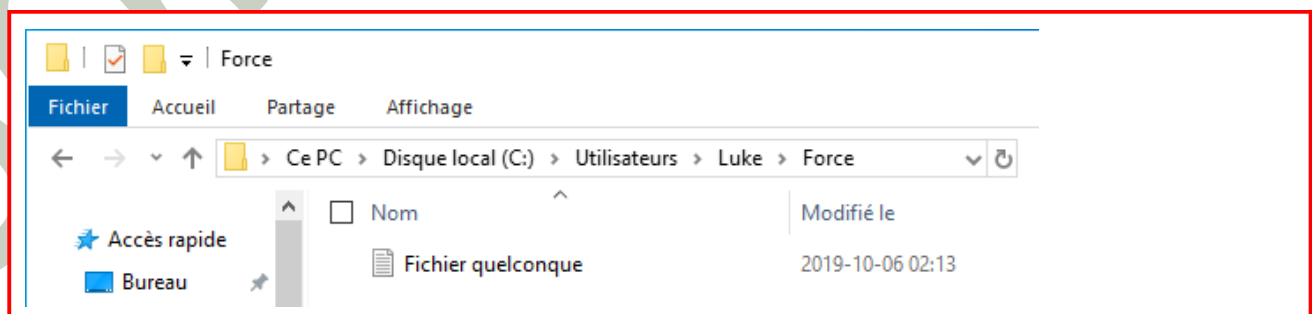


c) Vader dans le groupe GrpEmpire



### 3 Profils utilisateurs

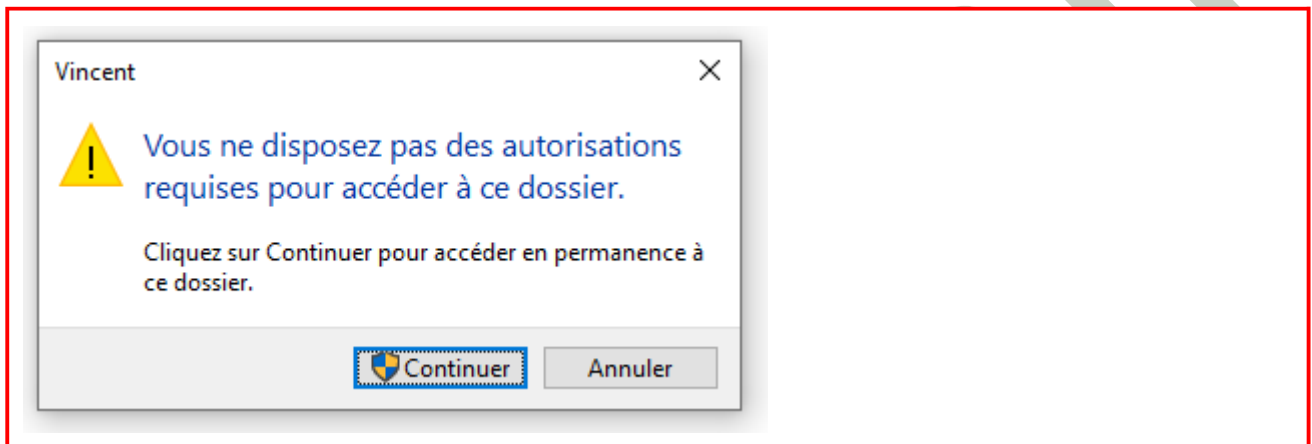
Q15 Connectez-vous avec le compte Luke (vous pouvez utiliser Fast User Switching). À l'aide de l'explorateur de fichiers, naviguez vers le profil de Luke et créez-y un répertoire nommé « Force » et placez-y un fichier quelconque. Faites une capture d'écran du résultat.



Q16 Dans le répertoire qui contient tous les profils des utilisateurs, pourquoi ne voyez-vous pas les profils de Han, Yoda et Vader?

Ils ne se sont pas encore connectés

Q17 Toujours à l'aide de l'explorateur de fichiers, naviguez vers le profil de votre utilisateur principal pour faire la même chose. Qu'est-ce que ça fait?



Q18 Que manque-t-il à Luke pour être capable de regarder le profil de votre utilisateur initial?

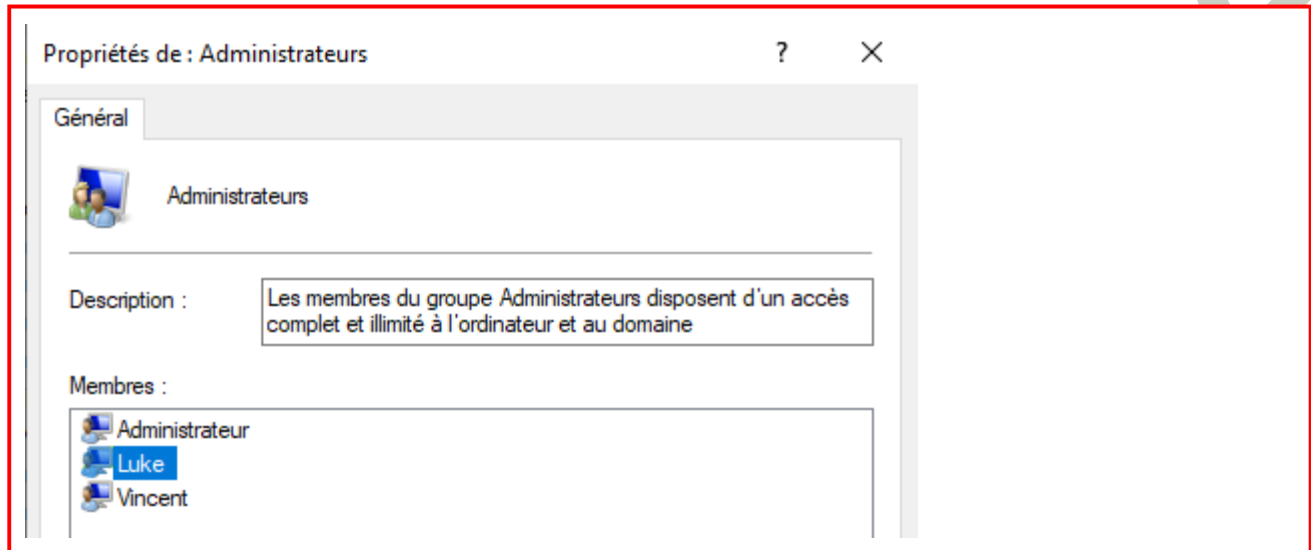
Des droits d'administrateur

Q19 Balancez vers la session de votre utilisateur initial. À l'aide de l'explorateur de fichiers, tentez d'accéder au fichier du répertoire Force dans le profil de Luke. Que se passe-t-il?

Il se fait demander d'élever ses privilèges, puis est capable d'entrer dans le dossier.

Attribuez à **Luke** le privlège qui lui permettra d'accéder à tout le contenu du disque dur, afin qu'il puisse accéder au contenu du répertoire de profil des autres utilisateurs.

Q20 Montrez ce que vous avez fait avec une capture d'écran.



#### 4 Ligne de commande

Les questions de cette section doivent être réalisées à l'aide de l'invite de commandes PowerShell avec privilèges administrateur. Assurez-vous que votre console soit élevée (c'est écrit Administrateur dans la barre de titre). Dans vos captures d'écran, montrez la commande et son résultat.

Q21 Listez tous les utilisateurs du système.

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

Name	Enabled	Description
Administrateur	False	Compte d'utilisateur d'administration
DefaultAccount	False	Compte utilisateur géré par le système.
Han	True	
Invité	False	Compte d'utilisateur invité
Luke	True	
Vader	True	
Vincent	True	
WDAGUtilityAccount	False	Compte d'utilisateur géré et utilisé par le système pour les sc...
Yoda	True	



Q22 Créez les utilisateurs suivants : Sidious, ObiWan.

```
PS C:\Windows\system32> New-LocalUser Sidious

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
----      -
Sidious   True

PS C:\Windows\system32> Add-LocalGroupMember -Group Utilisateurs -Member Sidious
PS C:\Windows\system32> New-LocalUser ObiWan

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
----      -
ObiWan    True

PS C:\Windows\system32> Add-LocalGroupMember -Group Utilisateurs -Member ObiWan
```

Q23 Listez tous les groupes du système.

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

Name	Description
GrpEmpire	
GrpJedi	
GrpRebelles	
Administrateurs	Les membres du groupe Administrateurs disposen...
Administrateurs Hyper-V	Les membres de ce groupe disposent d'un accès ...
Duplicateurs	Prend en charge la réplication 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 ...
System Managed Accounts Group	Les membres de ce groupe sont gérés par le sys...
Utilisateurs	Les utilisateurs ne peuvent pas effectuer de m...
Utilisateurs avec pouvoir	Les utilisateurs avec pouvoir sont inclus pour...
Utilisateurs de gestion à distance	Les membres de ce groupe ont accès aux ressour...
Utilisateurs de l'Analyseur de performances	Les membres de ce groupe peuvent accéder aux d...
Utilisateurs du Bureau à distance	Les membres de ce groupe disposent des droits ...
Utilisateurs du journal de performances	Les membres de ce groupe peuvent planifier la ...
Utilisateurs du modèle COM distribué	Les membres sont autorisés à lancer, à activer...

Q24 Créez le groupe GrpSith.

```
PS C:\Windows\system32> New-LocalGroup GrpSith
```

Name	Description
GrpSith	

Q25 Ajoutez les utilisateurs Vader et Sidious au groupe GrpSith.

```
PS C:\Windows\system32> Add-LocalGroupMember -Group GrpSith -Member Vader, Sidious
```

Q26 Ajoutez l'utilisateur ObiWan au groupe GrpJedi.

```
PS C:\Windows\system32> Add-LocalGroupMember -Group GrpJedi -Member ObiWan
```

Q27 Montrez les membres des groupes GrpJedi et GrpSith.

```
PS C:\Windows\system32> Get-LocalGroupMember GrpJedi

ObjectClass Name      PrincipalSource
-----
Utilisateur MEOBOX\Luke Local
Utilisateur MEOBOX\ObiWan Local
Utilisateur MEOBOX\Yoda Local

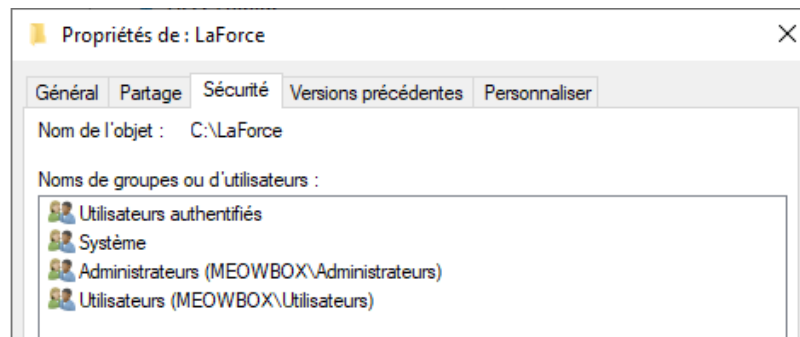
PS C:\Windows\system32> Get-LocalGroupMember GrpSith

ObjectClass Name      PrincipalSource
-----
Utilisateur MEOBOX\Sidious Local
Utilisateur MEOBOX\Vader Local
```

## 5 Permissions

Cette section porte sur les permissions NTFS.

Q28 Dans la racine du lecteur C:\, dans la session de votre utilisateur principal, créez un dossier appelé **LaForce**. Quelles sont les permissions sur ce dossier? Listez-les à l'aide de PowerShell.



```
PS C:\> Get-Acl .\LaForce\ | Format-List

Path      : Microsoft.PowerShell.Core\FileSystem::C:\LaForce\
Owner     : MEOWBOX\Vincent
Group     : MEOWBOX\Aucun
Access    : BUILTIN\Administrateurs Allow FullControl
            AUTORITE NT\Système Allow FullControl
            BUILTIN\Utilisateurs Allow ReadAndExecute, Synchronize
            AUTORITE NT\Utilisateurs authentifiés Allow Modify, Synchronize
            AUTORITE NT\Utilisateurs authentifiés Allow -536805376
Audit     :
Sddl      : O:S-1-5-21-1507397334-1719320053-894517008-1001G:S-1-5-21-1507397334-1719320053-8945
            17008-513D:AI(A;OICIID;FA;;;BA)(A;OICIID;FA;;;SY)(A;OICIID;0x1200a9;;;BU)(A;ID;0x130
            1bf;;;AU)(A;OICIID;SDGXGWGR;;;AU)
```

Q29 D'où viennent ces permissions? Pourquoi n'avez-vous pas eu besoin de les définir?

Elles sont héritées de la racine du C:\

Q30 Donnez aux groupes GrpJedi et GrpSith un accès en modification. Ensuite, connectez-vous avec le compte de **Yoda**. Pouvez-vous entrer dans le dossier?

Oui

Q31 Connectez-vous ensuite avec le compte de **Han**. Il n'est pas un Jedi ni un Sith, donc il ne devrait pas y avoir accès. Est-ce le cas? Pourquoi?

Il a accès, parce que tous les utilisateurs du système ont au lecteur C:\ et que le dossier LaForce hérite ses permissions du lecteur C:\.

Q32 Reconnectez-vous avec votre compte principal. Essayez de retirer les permissions des groupes *Utilisateurs authentifiés* et *Utilisateurs*. En êtes-vous capables?

Non. On obtient une erreur.

Q33 Reconnectez-vous avec votre compte principal. Désactivez l'héritage des permissions sur ce dossier et choisissez de convertir les autorisations héritées en autorisations explicites. Maintenant, pouvez-vous retirer les droits des utilisateurs authentifiés et des utilisateurs?

Oui.

Q34 Testez les accès avec les comptes de Han et de Yoda. Yoda devrait avoir accès et Han non. Est-ce le cas?

Oui. Yoda a accès, Han n'a pas accès.

