Installer et configurer un Serveur Windows Server 2022 Core avec réplication AD et DNS

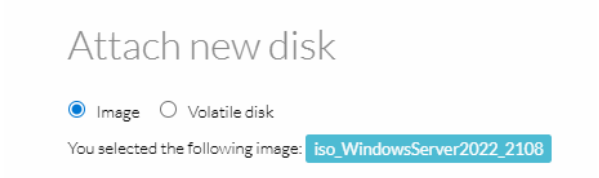
Nécessités :

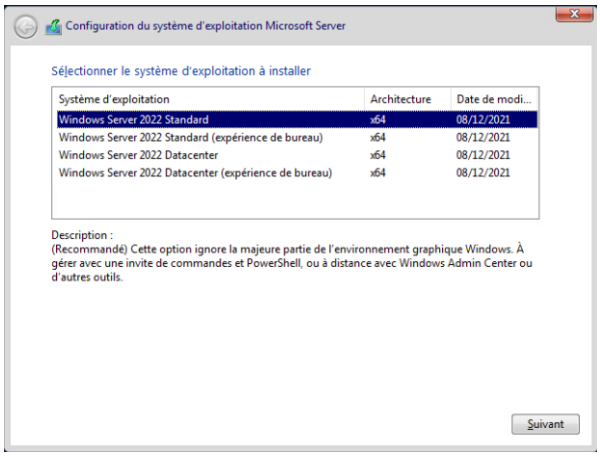
- Avoir une machine (virtuelle ou non) vide
- Avoir un ISO de Windows Server 2022 Core
- Avoir un serveur AD et DNS fonctionnels

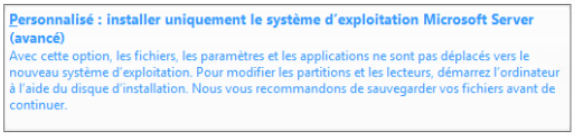
Sommaire

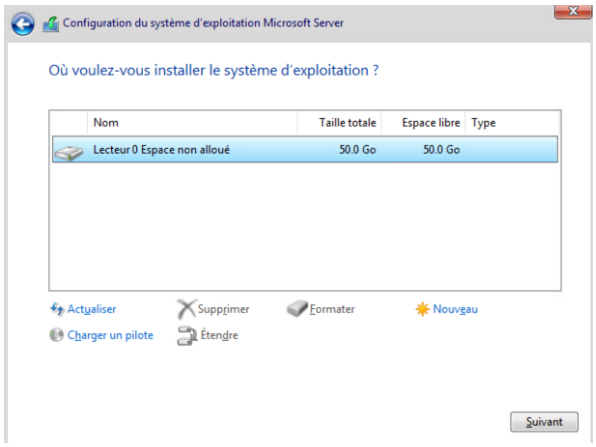
Etape 1 - Installation de Windows Server 2022 Core :

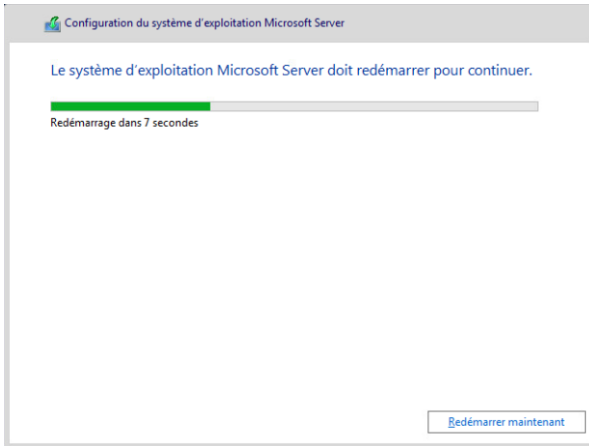
Attacher à votre VM ou brancher à votre machine un ISO de Windows Server 2022 Core et démarrer dessus.
Installer Windows sur un disque vide.





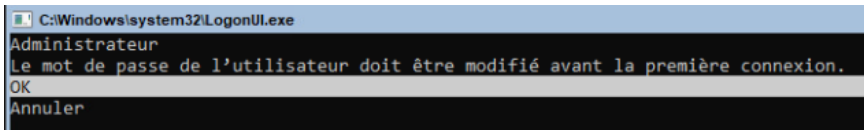


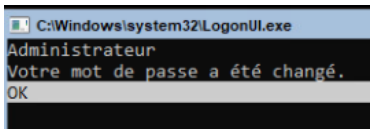




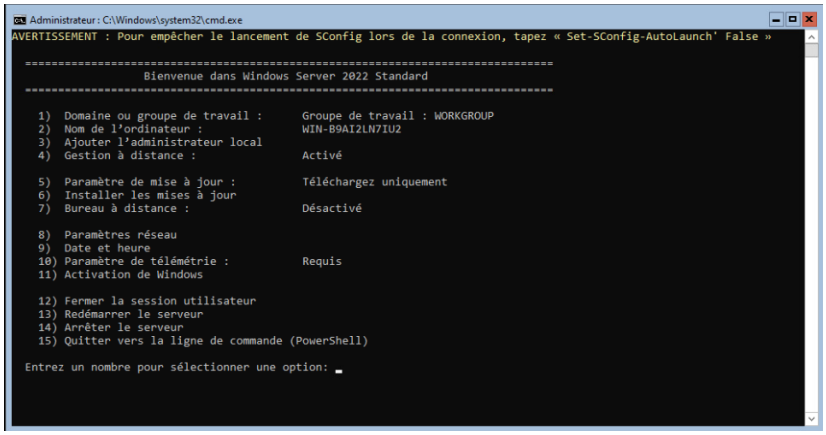
Etape 2 – Configuration du serveur :

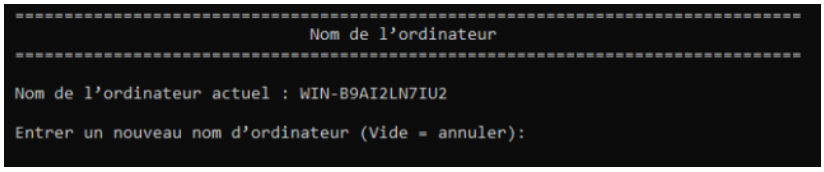
Modifier le mot de passe de l'utilisateur.



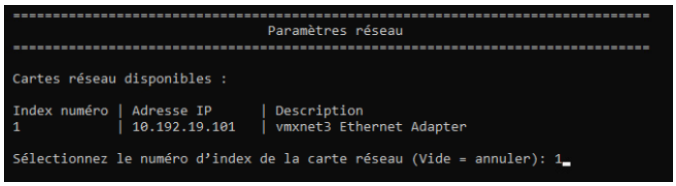


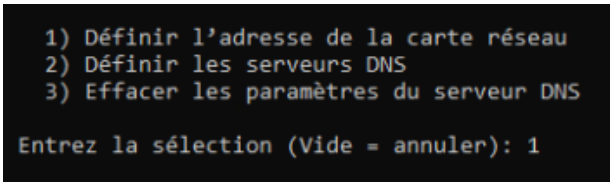
Une fois sur l'interface de configuration, taper 2 pour modifier le nom du serveur (par AD02 par exemple).

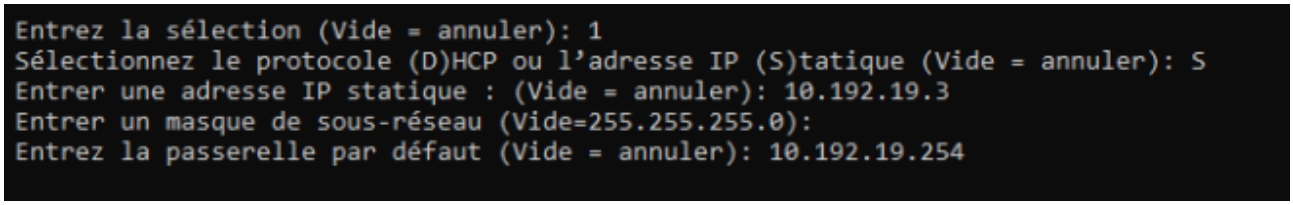




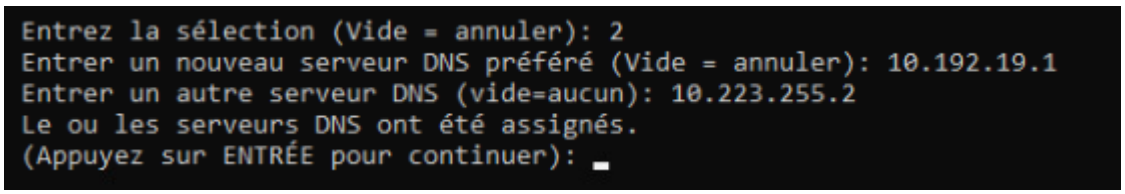
Ensuite, taper 8 pour modifier les paramètres réseau de votre carte réseau (choisir laquelle si vous en avez plusieurs).
Une fois la carte réseau choisie, taper 1 pour modifier l'adresse de votre carte réseau.
Taper S pour le protocole d'adresse IP statique, puis rentrez votre adresse IP statique, le masque et la passerelle par défaut.



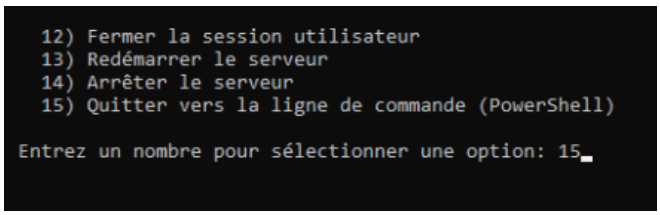




Puis, taper 2 pour définir les serveurs DNS, mettre comme DNS préféré votre serveur DNS préalablement créé et comme secondaire le DNS de votre organisation par exemple (ou rien du tout).



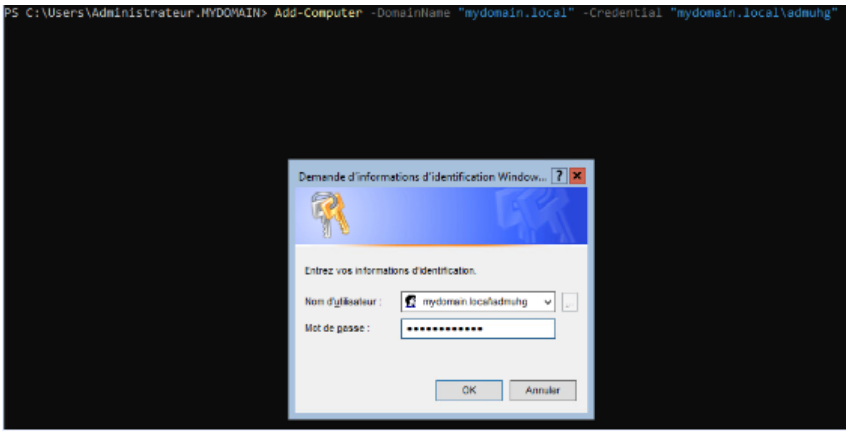
Enfin, du menu du SConfig, rentrer l'option 15 pour passer en ligne de commande PowerShell.



Rentrer la commande suivante :

```
Add-Computer -DomainName "mydomain.local" -Credential "mydomain.local\admuhg"
```

Cette commande ajoute ce serveur au domaine « mydomain.local » avec les droits du compte « mydomain.local\admuhg ». Vous devrez ensuite redémarrer le serveur pour prendre en compte les modifications.

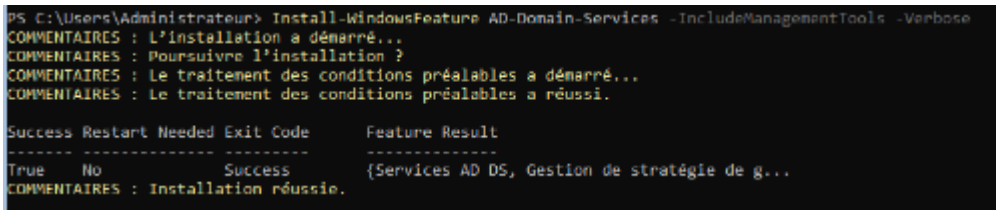


Etape 3 – Mise en place de la réplication AD et DNS :

Retourner en ligne de commande PowerShell, puis taper cette commande :

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools -Verbose
```

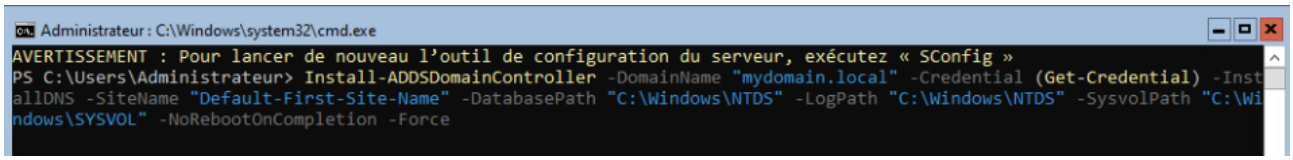
Cela permet d'installer le rôle Active Directory Domain Service sur le serveur, avec toutes les fonctionnalités nécessaires à son fonctionnement. Le « -Verbose » permet d'avoir plus d'information sur le déroulement de la commande.

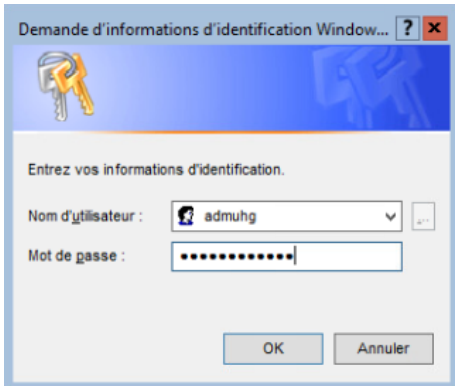


Maintenant, écrire cette commande afin de promouvoir le serveur en contrôleur de domaine supplémentaire (**Attention : bien vérifier que sur votre DNS principal le partage de zone soit bien activé, sinon la réplication sur votre deuxième DNS ne pourra pas se faire)** :

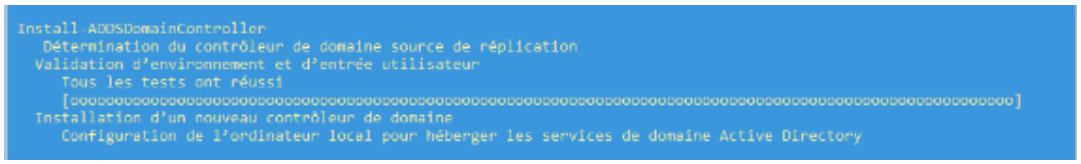
```
Install-ADDSDomainController -DomainName "mydomain.local" -Credential (Get-
Credential) -InstallDNS -SiteName "Default-First-Site-Name" -DatabasePath "C:
\Windows\NTDS" -LogPath "C:\Windows\NTDS" -SysvolPath "C: \Windows\SYSVOL"
-NoRebootOnCompletion -Force
```

A l'option « -DomainName » on va indiquer le domaine de notre premier contrôleur de domaine, le « -Credential » demande de s'authentifier pour obtenir les droits (avec un compte administrateur du domaine par exemple). Ensuite, « -InstallDNS » va venir répliquer le serveur DNS avec comme SiteName celui par défaut qui est nommé « Default-First-Site-Name ». « DatabasePath » indique le répertoire où vont être stockées les données concernant les utilisateurs, groupes etc, « -LogPath » indique le répertoire pour tous les logs de l'AD, et « -SysvolPath » indique le répertoire où seront tous les scripts ou les stratégies de groupe. Enfin « -NoRebootOnCompletion » empêche le serveur de redémarrer après avoir terminé d'exécuter la commande malgré que cela soit nécessaire, et « -Force » force l'exécution du programme, ce qui permet notamment de voir les erreurs s'il y en a.

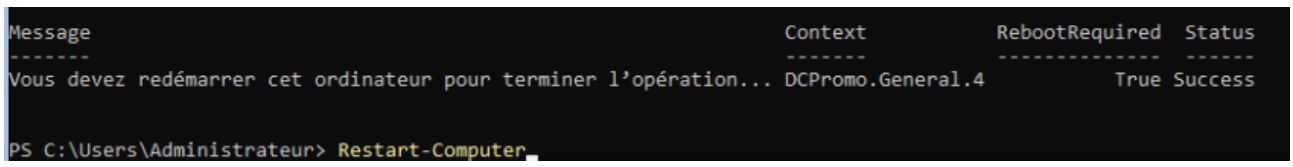




Il va également être demandé de définir un mot de passe « de secours » pour l'AD, en plus de l'authentification ci dessus.



Une fois terminé, redémarrer le serveur.



Etape 4 – Vérification de la réplication de l’AD + DNS :

```
repadmin / replsummary
```

« repadmin » permet de diagnostiquer des problèmes de réplication, puis « replsummary » récapitule l’état de la réplication.

```
repadmin / showrepl
```

« showrepl » donne un rapport détaillé pour la réplication sur le serveur local (si non précisé).

```
Get-DnsServerZone
```

Cette commande donne toutes les zones présentes sur le serveur DNS sur lequel elle est exécutée.

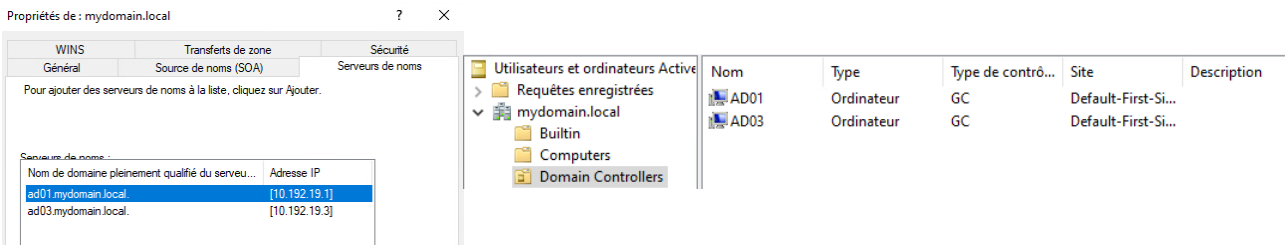
```
PS C:\Users\Administrateur.MYDOMAIN> Get-DnsServerZone

ZoneName                          ZoneType        IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                          --------        -------------   --------------  -------------------  --------
_msdcs.mydomain.local             Primary         False           True            False                False
0.in-addr.arpa                    Primary         True            False           True                 False
127.in-addr.arpa                  Primary         True            False           True                 False
19.192.10.in-addr.arpa            Primary         False           True            True                 False
255.in-addr.arpa                  Primary         True            False           True                 False
mydomain.local                    Primary         False           True            False                False
TrustAnchors                      Primary         False           True            False                False
```

```
Get-DnsServerResourceRecord -ZoneName "mydomain.local"
```

Enfin, celle ci liste tous les enregistrements de la zone spécifiée, ici « mydomain.local ».

```
ad01                    A       1       0                   01:00:00        10.192.19.1
AD02                    A       1       0                   00:20:00        10.192.19.2
ad03                    A       1       0                   01:00:00        10.192.19.3
DESKTOP-TJRA1LJ         A       1       02/09/2025 12:00:00 00:20:00        10.192.19.100
DomainDnsZones          A       1       03/09/2025 13:00:00 00:10:00        10.192.19.3
DomainDnsZones          A       1       02/09/2025 10:00:00 00:10:00        10.192.19.1
_ldap._tcp.Default-Fir... SRV   33      02/09/2025 10:00:00 00:10:00        [0][100][389][ad01.mydomain.loc...
_ldap._tcp.Default-Fir... SRV   33      03/09/2025 13:00:00 00:10:00        [0][100][389][ad03.mydomain.loc...
_ldap._tcp.DomainDnsZones SRV   33      03/09/2025 13:00:00 00:10:00        [0][100][389][ad03.mydomain.loc...
_ldap._tcp.DomainDnsZones SRV   33      02/09/2025 10:00:00 00:10:00        [0][100][389][ad01.mydomain.loc...
ForestDnsZones          A       1       03/09/2025 13:00:00 00:10:00        10.192.19.3
ForestDnsZones          A       1       02/09/2025 10:00:00 00:10:00        10.192.19.1
_ldap._tcp.Default-Fir... SRV   33      02/09/2025 10:00:00 00:10:00        [0][100][389][ad01.mydomain.loc...
_ldap._tcp.Default-Fir... SRV   33      03/09/2025 13:00:00 00:10:00        [0][100][389][ad03.mydomain.loc...
_ldap._tcp.ForestDnsZones SRV   33      02/09/2025 10:00:00 00:10:00        [0][100][389][ad01.mydomain.loc...
_ldap._tcp.ForestDnsZones SRV   33      03/09/2025 13:00:00 00:10:00        [0][100][389][ad03.mydomain.loc...
FS01                    A       1       0                   01:00:00        10.192.19.11
FS02                    A       1       0                   01:00:00        10.192.19.12
```

Il est également possible de vérifier sur le serveur principal la bonne remontée du serveur Core, à la fois sur le DNS ainsi que sur l’AD :



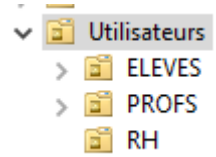
Il est donc bien apparu en tant que Serveur de noms sur le DNS, et comme Contrôleur de Domaine sur l'AD (AD03).

Etape 5 - Tests d'ajouts dans l'AD via PowerShell :

Pour tester si l'AD que l'on vient de créer est bien fonctionnel et répliqué, nous allons utiliser 4 commandes essentielles pour gérer un AD en PowerShell :

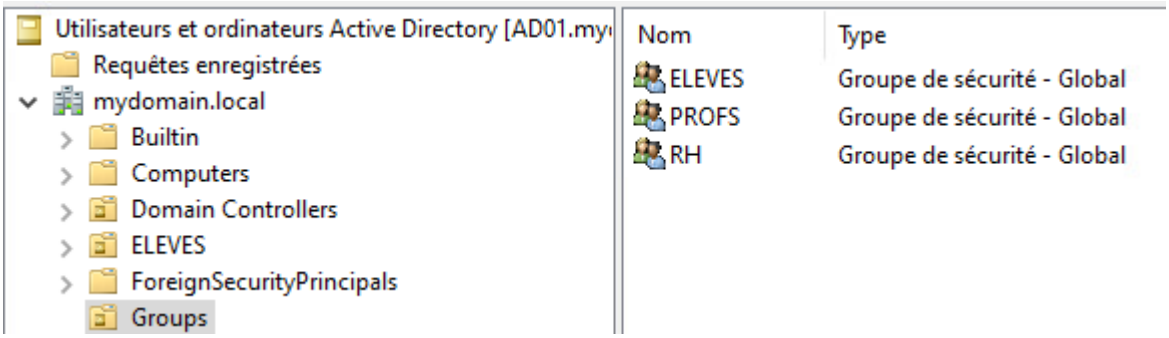
```
New-ADOrganizationalUnit -Name "RH" -Path "OU=Utilisateurs,DC=mydomain,DC=local"
```

Cette commande crée une OU (Unité Organisationnelle) nommée « RH », qui va se trouver dans une OU « Utilisateurs » qui elle même est à la racine de « mydomain.local ».



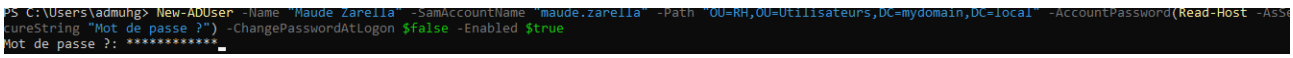

```
New-ADGroup -Name "RH" -Path "OU=Groups,DC=mydomain,DC=local" -GroupScope Globam
```

Cette commande crée un groupe nommé « RH » de type « Global », qui va se trouver dans une OU « Groups » à la racine de « mydomain.local ».




```
New-ADUser -Name "Maude Zarella" -SamAccountName "maude.zarella" -Path
"OU=RH,OU=Utilisateurs,DC=mydomain,DC=local" -AccountPassword(Read-Host
-AsSecureString "Mot de passe ?") -ChangePasswordAtLogon $false -Enabled $true
```

Cette commande permet de créer un utilisateur, ici nommé « Maude Zarella », donc l'identifiant de connexion sera « maude.zarella », qui sera situé dans l'OU « RH » lui-même situé dans l'OU « Utilisateurs », il faudra lui rentrer un mot de passe, qui ne sera pas à changer lors de la prochaine connexion, et le compte est activé.



Il est également possible de renseigner d'autres informations lors de la création d'un utilisateur tel que :

Le prénom `-GivenName`
Le nom `-Surname`
Une adresse mail `-EmailAddress`

On peut désormais rentrer notre utilisateur dans un groupe :

```
Add-AdGroupMember -Identity RH -Members "maude.zarella"
```

Le paramètre « Identity » désigne le groupe auquel appartiendra notre utilisateur et « Members » donne l'utilisateur à ajouter au groupe « RH ».