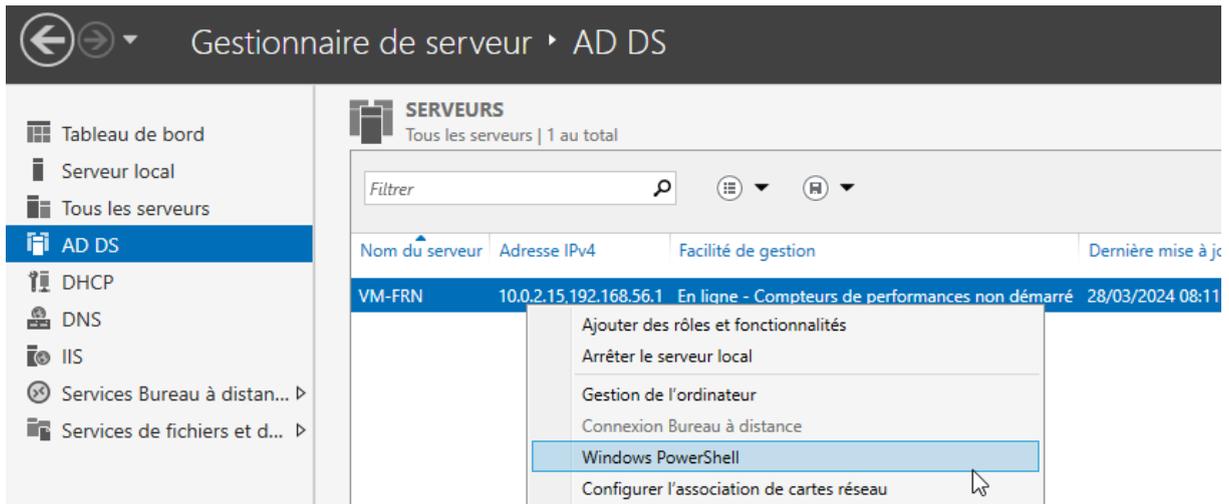


Administration AD avec Powershell

1. Préalable

Pour pouvoir utiliser les commandes powershell spécifique à l'active directory, il faut lancer Windows powershell depuis le contrôleur de domaine. Pour cela, il faut, depuis le tableau de bord, il faut sélectionner le rôle AD DS puis le serveur et ensuite lancer le powershell.



Vous pouvez lister les commandes spécifiques pour gérer AD en tapant :

`Get-Command | Where-Object Source -match 'ActiveDirectory'`

`Get-Command | findstr.exe /c:"ActiveDirectory"` (Car Where-Object-Source ne marche pas)

```
PS C:\Users\Administrateur> Get-Command | findstr.exe /c:"ActiveDirectory"
Cmdlet          Add-ADCentralAccessPolicyMember          1.0.1.0    ActiveDirectory
Cmdlet          Add-ADComputerServiceAccount             1.0.1.0    ActiveDirectory
Cmdlet          Add-ADDomainControllerPasswordReplicatio 1.0.1.0    ActiveDirectory
Cmdlet          Add-ADFineGrainedPasswordPolicySubject   1.0.1.0    ActiveDirectory
Cmdlet          Add-ADGroupMember                        1.0.1.0    ActiveDirectory
Cmdlet          Add-ADPrincipalGroupMembership           1.0.1.0    ActiveDirectory
Cmdlet          Add-ADResourcePropertyListMember         1.0.1.0    ActiveDirectory
Cmdlet          Clear-ADAccountExpiration                 1.0.1.0    ActiveDirectory
Cmdlet          Clear-ADClaimTransformLink                1.0.1.0    ActiveDirectory
Cmdlet          Disable-ADAccount                        1.0.1.0    ActiveDirectory
Cmdlet          Disable-ADOptionalFeature                 1.0.1.0    ActiveDirectory
Cmdlet          Enable-ADAccount                          1.0.1.0    ActiveDirectory
Cmdlet          Enable-ADOptionalFeature                  1.0.1.0    ActiveDirectory
Cmdlet          Get-ADAccountAuthorizationGroup           1.0.1.0    ActiveDirectory
Cmdlet          Get-ADAccountResultantPasswordReplicatio 1.0.1.0    ActiveDirectory
Cmdlet          Get-ADAuthenticationPolicy               1.0.1.0    ActiveDirectory
```

(Il y'en a bien plus que ça)

2. Création d'un utilisateur

L'objectif est de créer un nouveau compte utilisateur pour le service compta.

Ce nouveau compte aura les attributs suivants :

Nom –Altman

Prénom – Robert

Nom du compte – RobertA

Pour cela, on utilise la commande New-ADUser avec les **bons paramètres**

```
New-ADUser -Name "Robert Altman" -GivenName "Robert" -Surname "Altman"  
-SamAccountName "RobertA" -UserPrincipalName "Roberta@votre_domaine.limayrac.inet"  
-Path "OU=service compta,OU=Site,DC=votre_domaine,DC=limayrac,DC=inet"  
-AccountPassword(Read-Host -AsSecureString "Entrer le mot de passe") -Enabled $true
```

Vous pouvez vérifier la bonne création du compte avec la commande :

Get-ADUser roberta

```
PS C:\Users\Administrateur> New-ADUser -Name "Robert Altman" -GivenName "Robert" -Surname "Altman" -SamAccountName "RobertA" -UserPrincipalName "Roberta@votre_domaine.limayrac.inet" -Path "OU=service compta,OU=Site,DC=votre_domaine,DC=limayrac,DC=inet" -AccountPassword(Read-Host -AsSecureString "Entrer le mot de passe") -Enabled $true  
Entrer le mot de passe: *****  
PS C:\Users\Administrateur> get-ADUser roberta  
  
DistinguishedName : OU=Robert Altman,OU=Service Compta,OU=Site,DC=votre_domaine,DC=limayrac,DC=inet  
Enabled           : True  
DisplayName       : Robert  
Name              : Robert Altman  
ObjectClass       : user  
ObjectGUID        : e17c51e7-78a7-46b4-9197-cb1e45c056e2  
SamAccountName    : RobertA  
SID               : S-1-5-21-2436572114-224129429-3453362795-2111  
Surname           : Altman  
UserPrincipalName : Roberta@votre_domaine.limayrac.inet  
  
PS C:\Users\Administrateur>
```

3. Création d'un groupe utilisateurs

L'objectif est de créer un groupe pour les utilisateurs du service compta.

Pour créer le groupe « compta » dans l'unité d'organisation « OU=service compta,OU=Site,DC=votre_domaine,DC=limayrac,DC=inet », avec l'étendue « local » et la description « Service Comptabilité », on utilise la commande New-ADGroupe avec les **bons paramètres** :

```
New-ADGroup -Name "compta" -Path " OU=service  
compta,OU=Site,DC=votre_domaine,DC=limayrac,DC=inet " -GroupScope Global  
-Description "Service Comptabilité"
```

Vous pouvez vérifier la bonne création du compte avec la commande :

Get-ADGroup compta

```

PS C:\Users\Administrateur> New-ADGroup -Name "compta" -Path "OU=service compta,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -GroupScope Global -Description "Service comptabilité"
PS C:\Users\Administrateur> Get-ADGroup compta

DistinguishedName : CN=compta,OU=Service Compta,OU=Site,DC=nikolap,DC=limayrac,DC=inet
GroupCategory     : Security
GroupScope        : Global
Name              : compta
ObjectClass       : group
ObjectGUID        : fb543be3-78a1-4468-4432-783b666971f2
SamAccountName    : compta
SID               : S-1-5-21-2436572114-224129429-3453362755-2114

PS C:\Users\Administrateur>

```

4. Affecter des utilisateurs à un groupe

L'objectif est les utilisateurs du service compta dans le groupe compta.

Pour ajouter un utilisateur à un groupe Active Directory, on utilise la commande « Add-ADGroupMember ».

Exemple :

```
Add-ADGroupMember -Identity nom_du_groupe -Members "login_name_user1",
"login_name_user2"
```

Ajouter les utilisateurs du service compta dans le groupe compta et lister ensuite les membres du groupe compta avec la commande : *Get-ADGroupMember -Identity compta*

```

PS C:\Users\Administrateur> Add-ADGroupMember -Identity compta -Members "Jeanprout", "Roberta"
PS C:\Users\Administrateur> Get-ADGroupMember -Identity compta

DistinguishedName : OU=Jean Prout,OU=Service Compta,OU=Site,DC=nikolap,DC=limayrac,DC=inet
name              : Jean Prout
objectClass       : user
objectGUID        : e642e671-bb72-43d8-b69a-2650fd2fab90
SamAccountName    : Jeanprout
SID               : S-1-5-21-2436572114-224129429-3453362755-2109

DistinguishedName : CN=Robert Altman,OU=Service Compta,OU=Site,DC=nikolap,DC=limayrac,DC=inet
name              : Robert Altman
objectClass       : user
objectGUID        : e17c51e7-78a7-49b4-9197-cb1ea5cd96e2
SamAccountName    : Roberta
SID               : S-1-5-21-2436572114-224129429-3453362755-2111

```

5. Création d'unité organisationnelle

L'objectif est de créer une nouvelle OU : service informatique.

Vous pouvez créer une nouvelle UO dans Active Directory en utilisant le cmdlet New-ADOrganizationalUnit et en spécifiant le nom d'un nouvel objet OU. Par défaut, PowerShell créera l'OU dans la racine du domaine. Si vous avez besoin d'un chemin d'accès OU différent, spécifiez son nom distinctif en utilisant le paramètre -Path cmdlet :

```
New-ADOrganizationalUnit "Regions" -Path "OU=xxx,DC=xxxx,DC=xxx"
```

Dans notre cas, la commande sera donc :

```
New-ADOrganizationalUnit "service informatique" -Path
"OU=Site,DC=votre_domaine,DC=limayrac,DC=inet "
```

Vous pouvez vérifier la bonne création du compte avec la commande :

```
Get-ADOrganizationalUnit -filter {name -like "service informatique" }
```

```
PS C:\Users\Administrateur> New-ADOrganizationalUnit "service informatique" -Path "OU=Site,DC=nikolap,DC=limayrac,DC=inet "
PS C:\Users\Administrateur> Get-ADOrganizationalUnit -filter {name -like "service informatique"}

City                :
Country             :
DistinguishedName   : OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
LinkedGroupPolicyObjects : {}
ManagedBy          :
Name                : service informatique
ObjectClass         : organizationalUnit
ObjectGUID          : 47ca4698-7844-4a51-80c3-aa739870ae38
PostalCode          :
State               :
StreetAddress       :

PS C:\Users\Administrateur> _
```

6. UO Service informatique

L'objectif est de créer une OU support dans l'OU service informatique, de créer des groupes utilisateurs pour ces 2 UOs ainsi que des utilisateurs pour ces 2 UOs qui seront affecter au groupe correspondant à leur OU sachant que les membres du groupe support sont aussi membre du groupe service informatique.

a - Création des OU

```
New-ADOrganizationalUnit "service informatique" -Path "OU=Site,DC=nikolap,DC=limayrac,DC=inet "
```

```
New-ADOrganizationalUnit "support" -Path "OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet "
```

```
PS C:\Users\Administrateur> New-ADOrganizationalUnit "support" -Path "OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet "
PS C:\Users\Administrateur> Get-ADOrganizationalUnit -filter {name -like "support"}

City                :
Country             :
DistinguishedName   : OU=support,OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
LinkedGroupPolicyObjects : {}
ManagedBy          :
Name                : support
ObjectClass         : organizationalUnit
ObjectGUID          : 63ab4d37-05a5-4112-8a13-b572a3a088bd
PostalCode          :
State               :
StreetAddress       :

PS C:\Users\Administrateur> _
```

b - Création groupes et utilisateurs

Les groupes :

```
New-ADGroup -Name "support" -Path "OU=support,OU=service
informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -GroupScope Global -Description
"Support"
```

```
New-ADGroup -Name "informatique" -Path "OU=service
informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -GroupScope Global -Description
"Informatique"
```

```
PS C:\Users\Administrateur> New-ADGroup -Name "support" -Path "OU=support,OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -GroupScope Global -Description "Support"
PS C:\Users\Administrateur> New-ADGroup -Name "Informatique" -Path "OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -GroupScope Global -Description "Informatique"
PS C:\Users\Administrateur> Get-ADGroup support

DistinguishedName : CN=support,OU=support,OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
GroupCategory     : Security
GroupScope        : Global
Name              : support
ObjectClass       : group
ObjectGUID        : c427d818-14af-43d1-a071-74f0217c3c5f
SamAccountName    : support
SID               : S-1-5-21-2436572114-224129429-3453362755-2115

PS C:\Users\Administrateur> Get-ADGroup Informatique

DistinguishedName : CN=Informatique,OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
GroupCategory     : Security
GroupScope        : Global
Name              : Informatique
ObjectClass       : group
ObjectGUID        : ff896bcc-acd9-4f7b-9449-6d2a914aed7f
SamAccountName    : Informatique
SID               : S-1-5-21-2436572114-224129429-3453362755-2116

PS C:\Users\Administrateur> _
```

Les users :

Création

```
New-ADUser -Name "John Doe" -GivenName "John" -Surname "Doe" -SamAccountName
"johndoe" -UserPrincipalName "johndoe@nikolap.limayrac.inet" -Path "OU=service
informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -AccountPassword(Read-Host
-AsSecureString "Entrer le mot de passe") -Enabled $true
```

```
New-ADUser -Name "Jane Doe" -GivenName "Jane" -Surname "Doe" -SamAccountName
"janedoe" -UserPrincipalName "janedoe@nikolap.limayrac.inet" -Path
"OU=support,OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet"
-AccountPassword(Read-Host -AsSecureString "Entrer le mot de passe") -Enabled $true
```

```
PS C:\Users\Administrateur> New-ADUser -Name "John Doe" -GivenName "John" -Surname "Doe" -SamAccountName "johndoe" -UserPrincipalName "johndoe@nikolap.limayrac.inet" -Path "OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -AccountPassword(Read-Host -AsSecureString "Entrer le mot de passe") -Enabled $true
Entrer le mot de passe: *****
PS C:\Users\Administrateur> New-ADUser -Name "Jane Doe" -GivenName "Jane" -Surname "Doe" -SamAccountName "janedoe" -UserPrincipalName "janedoe@nikolap.limayrac.inet" -Path "OU=support,OU=service Informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet" -AccountPassword(Read-Host -AsSecureString "Entrer le mot de passe") -Enabled $true
Entrer le mot de passe: *****
```

Ajout au groupes

Add-AdGroupMember -Identity informatique -Members "johndoe", "janedoe"

Add-AdGroupMember -Identity support -Members "janedoe"

```
PS C:\Users\Administrateur> Add-AdGroupMember -Identity informatique -Members "johndoe", "janedoe"
PS C:\Users\Administrateur> Add-AdGroupMember -Identity support -Members "janedoe"
PS C:\Users\Administrateur> Get-ADGroupMember -Identity informatique

distinguishedName : CN=John Doe,OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
name              : John Doe
objectClass       : user
objectGUID        : 7d150457-81ed-42ca-9226-3712ac41e8b6
SamAccountName    : johndoe
SID               : S-1-5-21-2436572114-224129429-3453362755-2117

distinguishedName : CN=Jane Doe,OU=support,OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
name              : Jane Doe
objectClass       : user
objectGUID        : 2f03cf02-3bff-46b8-aad0-73b453d4f600
SamAccountName    : janedoe
SID               : S-1-5-21-2436572114-224129429-3453362755-2118

PS C:\Users\Administrateur> Get-ADGroupMember -Identity support

distinguishedName : CN=Jane Doe,OU=support,OU=service informatique,OU=Site,DC=nikolap,DC=limayrac,DC=inet
name              : Jane Doe
objectClass       : user
objectGUID        : 2f03cf02-3bff-46b8-aad0-73b453d4f600
SamAccountName    : janedoe
SID               : S-1-5-21-2436572114-224129429-3453362755-2118

PS C:\Users\Administrateur> _
```