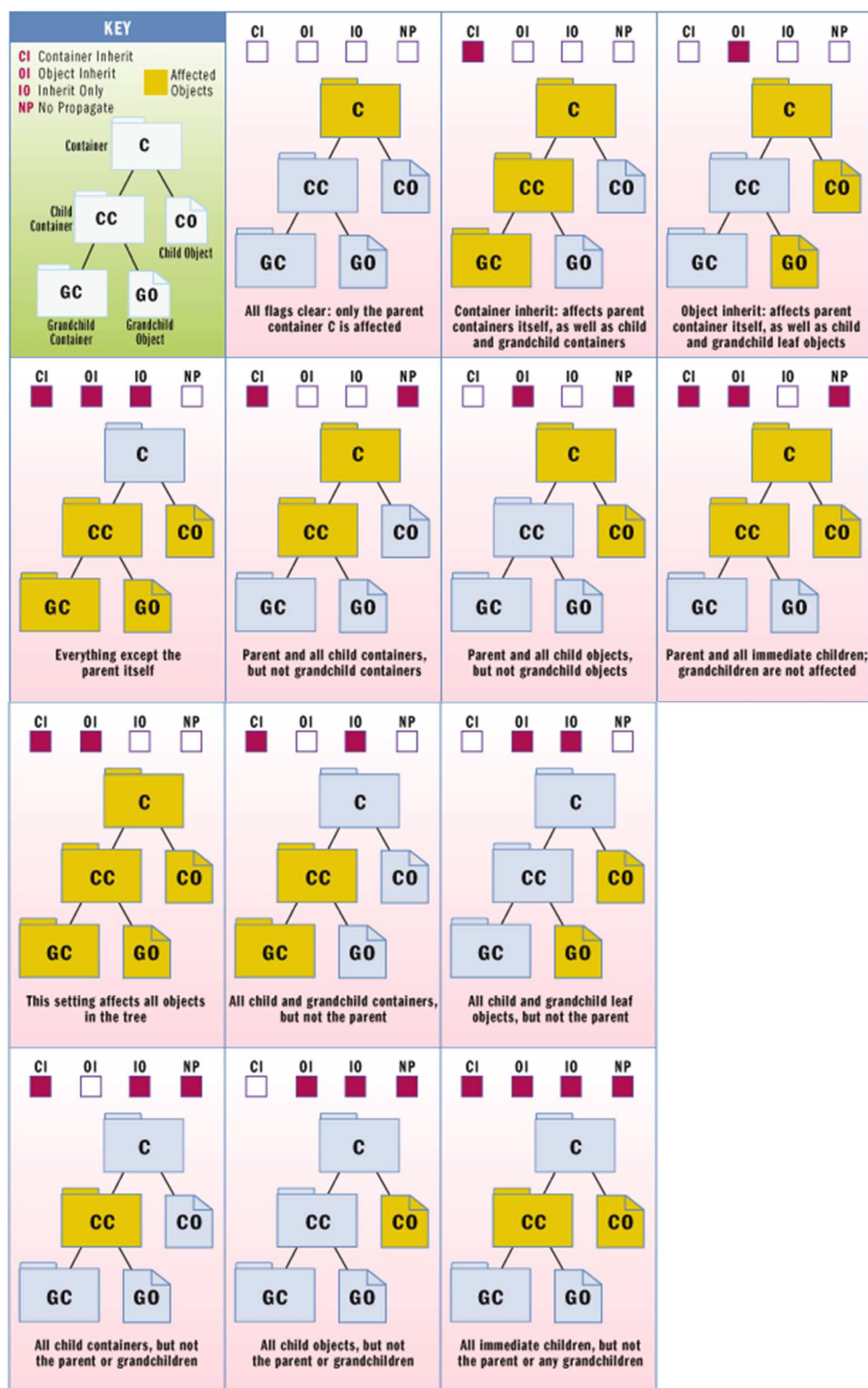


## Propagation des autorisations NTFS



Le tableau suivant vous permet d'interpréter les codes pour les 13 modes de propagation.

| Code             | Propagation des autorisations NTFS   |
|------------------|--|
| Aucun code       | Ce dossier seulement   |
| (CI)             | Ce dossier et les sous-dossiers  |
| (OI)             | Ce dossier et les fichiers   |
| (CI)(OI)(IO)     | Les sous-dossiers et les fichiers seulement  |
| (CI)(NP)         | Ce dossier et les sous-dossiers mais SEULEMENT sur les sous-dossiers de premier niveau   |
| (OI)(NP)         | Ce dossier et les fichiers mais SEULEMENT sur les fichiers de premier niveau   |
| (CI)(OI)(NP)     | Ce dossier, les sous-dossiers et les fichiers mais SEULEMENT sur les sous-dossiers de premier niveau ET les fichiers de premier niveau |
| <b>(CI)(OI)</b>  | <b>Ce dossier, les sous-dossiers et les fichiers</b>   |
| (CI)(IO)         | Les sous-dossiers seulement  |
| (OI)(IO)         | Fichiers seulement   |
| (CI)(IO)(NP)     | Les sous-dossiers seulement mais SEULEMENT sur les sous-dossiers de premier niveau   |
| (OI)(IO)(NP)     | Fichiers seulement mais SEULEMENT sur les fichiers de premier niveau   |
| (CI)(OI)(IO)(NP) | Les sous-dossiers et les fichiers seulement mais SEULEMENT sur les sous-dossiers de premier niveau ET les fichiers de premier niveau   |

### Les autorisations NTFS et la commande ICACLS.EXE

**c:\windows\system32\icaccls.exe**

Pour avoir de l'aide sur la commande icaccls.exe  
**icaccls.exe /?**

#### **Les codes qui correspondent aux autorisations NTFS de base**

|           |                               |
|-----------|-------------------------------|
| <b>F</b>  | Accès complet                 |
| <b>M</b>  | Accès en modification         |
| <b>RX</b> | Accès en lecture et exécution |
| <b>R</b>  | Accès en lecture seule        |
| <b>W</b>  | Accès en écriture seule       |

Exemples:

- pour rétablir les autorisations NTFS par défaut sur un répertoire  
`icaccls.exe c:\_toto /reset`
- pour supprimer toutes les autorisations NTFS héritées sur un répertoire  
`icaccls.exe c:\_toto /inheritance:r`
- pour attribuer plusieurs autorisations NTFS sur un répertoire  
`icaccls.exe c:\_toto /grant Administrateurs:(OI)(CI)(F)`  
`icaccls.exe c:\_toto /grant SYSTEM:(OI)(CI)(F)`  
`icaccls.exe c:\_toto /grant u1:(OI)(CI)(M)`
- pour attribuer plusieurs autorisations NTFS sur un répertoire  
`icaccls.exe c:\_toto /grant Administrateurs:(OI)(CI)(F) SYSTEM:(OI)(CI)(F) u1:(OI)(CI)(M)`
- pour attribuer des autorisations NTFS en utilisant le SID de "Utilisateurs authentifiés"  
`icaccls.exe c:\_toto /grant *S-1-5-11:(OI)(CI)(M)`
- pour afficher les autorisations NTFS sur un répertoire  
`icaccls.exe c:\_toto`
- pour modifier le propriétaire d'un répertoire  
`icaccls.exe c:\_toto /setowner Administrateurs`

### Récupérer l'accès sur un dossier ou un fichier avec TAKEOWN.EXE

**takeown.exe**

- Cet outil permet à un administrateur de récupérer l'accès à un fichier qui avait été refusé en réassignant l'appartenance de fichier.

La commande "**takeown.exe**" est utile, si vous avez un dossier sur lequel vous n'êtes pas le propriétaire et que les autorisations sont restreintes à un point tel que la commande "**icaccls.exe**" refuse de modifier les autorisations.

- /F spécifie le nom de fichier ou le modèle de nom du répertoire.  
Un caractère générique "\*" peut être utilisé pour spécifier le modèle. Autorise nopathage\nomfichier.
- Si /A n'est pas spécifié, l'appartenance de fichier sera attribuée à l'utilisateur actuellement connecté.
- /R est utilisé pour forcer l'outil à traiter tous les fichiers du répertoire spécifié et tous ses sous-répertoires.
- /D est utilisé pour supprimer la demande de confirmation, "O" pour prendre possession ou "N" pour ignorer.

**takeown.exe /F "M:\TEST" /A /R /D O**

**icaccls.exe "M:\TEST" /reset**

### **Utiliser PowerShell pour exécuter la commande ICACLS**

Si une commande fonctionne dans une fenêtre CMD on peut l'exécuter dans une fenêtre PowerShell.  
Mais dans certaine situation, il faut modifier la syntaxe de la commande pour réussir à l'exécuter correctement.

#### **La syntaxe pour la commande "icaccls.exe" si on l'exécute dans une fenêtre CMD**

**Les parenthèses sont obligatoires si le nom du groupe contient des espaces.**

```
icaccls.exe c:\_toto /grant Administrateurs:(OI)(CI)(F)
```

```
icaccls.exe c:\_toto /grant "tout le monde):(OI)(CI)(F)
```

**Pour exécuter la commande "icaccls.exe" dans PowerShell, il faut changer la position des guillemets.**

**PowerShell interprète mal les parenthèses de la commande icaccls.**

```
icaccls.exe c:\_toto /grant "Administrateurs:(OI)(CI)(F)"
```

```
icaccls.exe c:\_toto /grant "tout le monde):(OI)(CI)(F)"
```

---

Utilisation d'une variable PowerShell dans la section des autorisations de la commande "icaccls.exe".

**\$nom = "tout le monde"**

```
icaccls.exe c:\_toto /grant $nom):(OI)(CI)(F)"
```

**ou**

```
icaccls.exe c:\_toto /grant "${nom}):(OI)(CI)(F)"
```

---

#### **Utilisation du paramètre --% avec la commande "icaccls.exe"**

Le paramètre --% indique à PowerShell de ne pas interpréter le reste de la ligne.

```
icaccls.exe --% c:\_toto /grant "tout le monde):(OI)(CI)(F)
```

L'utilisation du paramètre --% ne permet pas d'utiliser une variable dans la section des autorisations.

L'utilisation du paramètre --% permet d'utiliser une variable pour le nom du dossier.

**\$chemin="c:\\_toto"**

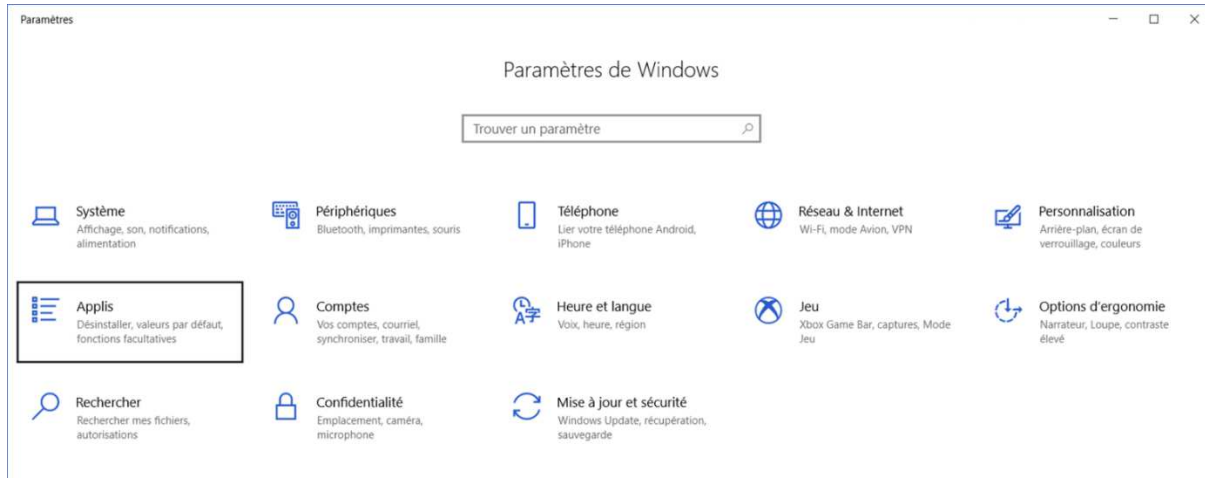
```
icaccls.exe $chemin --% /grant "tout le monde):(OI)(CI)(F)
```

Si un ordinateur est membre d'un domaine "Active Directory" et utilise "**Windows 10**" ou "**Windows 11**", il est possible d'installer les différentes consoles de gestion d'un serveur Windows.

À partir de "Windows 10 version 1809" RSAT (Remote Server Administration Tools) est inclus dans les "Fonctionnalités facultatives".

### Installation de RSAT en utilisant l'environnement graphique

Dans la console "**Paramètres de Windows**"



On doit ouvrir "**Applis**"

- cliquer sur "**Fonctionnalités facultatives**"
  - cliquer sur "**Ajouter une fonctionnalité**"



**Attention aux dépendances pour l'installation et la désinstallation d'une fonctionnalité facultative.**

### Installation de RSAT en utilisant la commande DISM.EXE

**Voici la commande pour lister tous les composants facultatifs**

```
dism.exe /Online /Get-Capabilities /FORMAT:Table
```

---

**Voici la commande pour lister les composants facultatifs dont le nom contient "RSAT."**

```
dism.exe /Online /Get-Capabilities /Format:Table | find.exe /I "RSAT."
```

---

**Voici la commande pour lister les composants facultatifs dont le nom débute par "RSAT."**

```
dism.exe /Online /Get-Capabilities /Format:Table | findstr.exe /B /I "RSAT."
```

---

**Voici la liste des fonctionnalités facultatives dont le nom débute par "RSAT."**

|  |             |
|--|-------------|
| Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0             | Not Present |
| Rsat.AzureStack.HCI.Management.Tools~~~~0.0.1.0          | Not Present |
| Rsat.BitLocker.Recovery.Tools~~~~0.0.1.0                 | Not Present |
| Rsat.CertificateServices.Tools~~~~0.0.1.0                | Not Present |
| Rsat.DHCP.Tools~~~~0.0.1.0                               | Not Present |
| Rsat.Dns.Tools~~~~0.0.1.0                                | Not Present |
| Rsat.FailoverCluster.Management.Tools~~~~0.0.1.0         | Not Present |
| Rsat.FileServices.Tools~~~~0.0.1.0                       | Not Present |
| Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0             | Not Present |
| Rsat.IPAM.Client.Tools~~~~0.0.1.0                        | Not Present |
| Rsat.LLDP.Tools~~~~0.0.1.0                               | Not Present |
| Rsat.NetworkController.Tools~~~~0.0.1.0                  | Not Present |
| Rsat.NetworkLoadBalancing.Tools~~~~0.0.1.0               | Not Present |
| Rsat.RemoteAccess.Management.Tools~~~~0.0.1.0            | Not Present |
| Rsat.RemoteDesktop.Services.Tools~~~~0.0.1.0             | Not Present |
| Rsat.ServerManager.Tools~~~~0.0.1.0                      | Not Present |
| Rsat.StorageMigrationService.Management.Tools~~~~0.0.1.0 | Not Present |
| Rsat.StorageReplica.Tools~~~~0.0.1.0                     | Not Present |
| Rsat.SystemInsights.Management.Tools~~~~0.0.1.0          | Not Present |
| Rsat.VolumeActivation.Tools~~~~0.0.1.0                   | Not Present |
| Rsat.WSUS.Tools~~~~0.0.1.0                               | Not Present |

---

**Cette commande installe la console "Gestionnaire de serveur".**

```
dism.exe /Online /Add-Capability  
/CapabilityName:Rsat.ServerManager.Tools~~~~0.0.1.0
```

**Cette commande installe la console "Active Directory".**

**La console "Active Directory" est dépendante de la console "Gestionnaire de serveur".**

```
dism.exe /Online /Add-Capability  
/CapabilityName:Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
```

---

**Il faut désinstaller la console "Active Directory" en premier.**

```
dism.exe /Online /Remove-Capability  
/CapabilityName:Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
```

**Cette commande désinstalle la console "Gestionnaire de serveur".**

```
dism.exe /Online /Remove-Capability  
/CapabilityName:Rsat.ServerManager.Tools~~~~0.0.1.0
```

---

### Installation de RSAT en utilisant PowerShell

**Cette commande liste les composants facultatifs dont le nom débute par "RSAT."**

```
Get-WindowsCapability -Name RSAT.* -Online
```

```
Get-WindowsCapability -Name RSAT.* -Online | Select-Object -Property DisplayName, State  
Get-WindowsCapability -Name RSAT.* -Online | Select-Object -Property Name, State
```

---

**Cette commande installe la console "Gestionnaire de serveur"**

```
Add-WindowsCapability -Online -Name Rsat.ServerManager.Tools~~~~0.0.1.0
```

**Cette commande installe la console "Active Directory".**

**La console "Active Directory" est dépendante de la console "Gestionnaire de serveur".**

```
Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
```

---

**Il faut désinstaller la console "Active Directory" en premier.**

```
Remove-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
```

**Cette commande désinstalle la console "Gestionnaire de serveur"**

```
Remove-WindowsCapability -Online -Name Rsat.ServerManager.Tools~~~~0.0.1.0
```

---

**Cette commande affiche les consoles RSAT qui sont installées**

```
Get-WindowsCapability -Online | Where-Object {$PSItem.Name -like "RSAT.*" -and `  
$PSItem.State -eq "Installed"}
```

**Cette commande affiche les consoles RSAT qui ne sont pas installées**

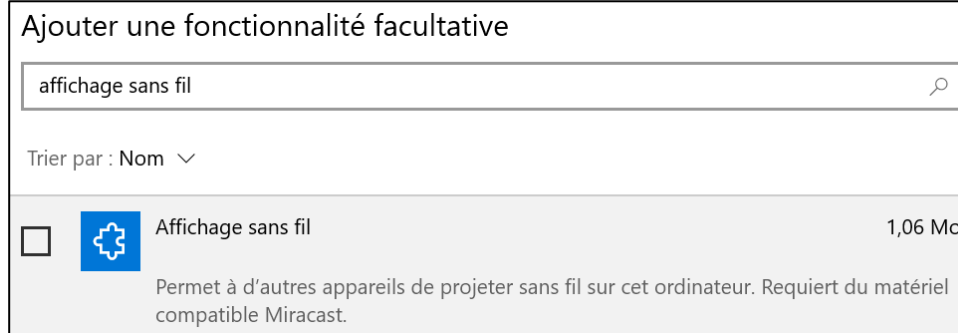
```
Get-WindowsCapability -Online | Where-Object {$PSItem.Name -like "RSAT.*" -and `  
$PSItem.State -eq "NotPresent"}
```

## ANNEXE

### Fonctionnalité facultative "Affichage sans fil"

La fonctionnalité facultative "**Affichage sans fil**" permet d'afficher l'écran d'un cellulaire sur votre ordinateur à condition d'utiliser "**Windows 10**" ou "**Windows 11**".

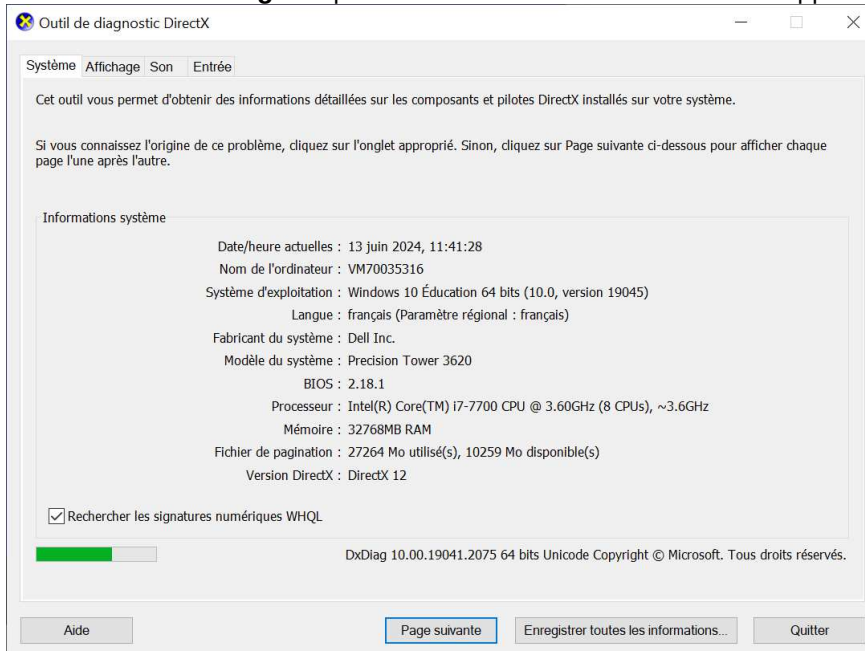
Installation de la fonctionnalité facultative "**Affichage sans fil**" par l'environnement graphique.



Installation de la fonctionnalité facultative "**Affichage sans fil**" avec la commande **DISM.EXE**.

```
dism.exe /Online /Add-Capability  
/CapabilityName:App.WirelessDisplay.Connect~~~~0.0.1.0
```

La commande **DxDiag.exe** permet de vérifier si votre ordinateur supporte Miracast.



Vous devez cliquer sur le bouton "**Enregistrer toutes les informations...**".

Dans le fichier, vous devez chercher la ligne qui contient Miracast.

**Miracast: Not Available**

ou

**Miracast: Available, no HDCP**

ou

**Miracast: Available, with HDCP**



## Une liste de SID

Le SID (Security identifier) est une valeur unique qui est utilisée pour identifier un utilisateur ou un groupe du système d'exploitation Windows.

| SID   | Utilisateur   |
|---|---|
| <b>S-1-5-21</b> -<nombre>-<nombre>-<nombre>- <b>500</b> | <b>Administrateur</b><br>ou<br><b>Administrator</b> |

| SID   | Groupe   |
|---|--|
| <b>S-1-5-32-544</b>                                     | <b>Administrateurs</b><br>ou<br><b>Administrators</b>            |
| <b>S-1-5-32-545</b>                                     | <b>Utilisateurs</b><br>ou<br><b>Users</b>                        |
| <b>S-1-5-21</b> -<nombre>-<nombre>-<nombre>- <b>512</b> | <b>Admins du domaine</b><br>ou<br><b>Domain Admins</b>           |
| <b>S-1-5-21</b> -<nombre>-<nombre>-<nombre>- <b>513</b> | <b>Utilisateurs du domaine</b><br>ou<br><b>Domain Users</b>      |
| <b>S-1-5-21</b> -<nombre>-<nombre>-<nombre>- <b>515</b> | <b>Ordinateurs du domaine</b><br>ou<br><b>Domain Computers</b>   |
| <b>S-1-5-21</b> -<nombre>-<nombre>-<nombre>- <b>516</b> | <b>Contrôleurs de domaine</b><br>ou<br><b>Domain Controllers</b> |

| SID             | Principaux de sécurité intégrés                                      |
|-----------------|--|
| <b>S-1-1-0</b>  | <b>Tout le monde</b><br>ou<br><b>Everyone</b>                        |
| <b>S-1-3-4</b>  | <b>DROITS DU PROPRIÉTAIRE</b><br>ou<br><b>OWNER RIGHTS</b>           |
| <b>S-1-5-11</b> | <b>Utilisateurs authentifiés</b><br>ou<br><b>Authenticated Users</b> |
| <b>S-1-5-18</b> | <b>Système</b><br>ou<br><b>SYSTEM</b>                                |

# Commande pour afficher la valeur **S-1-5-21-<nombre>-<nombre>-<nombre>** d'un domaine  
(Get-ADDomain).DomainSID.Value

On peut savoir si un utilisateur a ouvert l'invite de commandes avec une élévation des autorisations.  
En exécutant la commande suivante "**whoami.exe /all**" et en vérifiant la valeur du SID.

| SID          | Interprétation du SID       |
|--------------|-----------------------------|
| S-1-16-8192  | Autorisations standard      |
| S-1-16-12288 | Élévation des autorisations |

## Les propriétés des ordinateurs dans l'Active Directory

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectifs

- Utiliser l'onglet "Éditeur d'attribut"
- Comprendre la différence entre le nom des attributs et les paramètres des cmdlets

### Les principaux attributs d'un ordinateur

Le SERVEUR1 est dans l'unité d'organisation "Domain Controllers".

The image shows two side-by-side screenshots of the 'Propriétés de : SERVEUR1' window in Active Directory. The left screenshot shows the 'Général' tab with the following fields: 'Nom d'ordinateur (antérieur à Windows 2000)' with value 'SERVEUR1', 'Nom DNS' with value 'SERVEUR1.FORMATION.LOCAL', 'Type de contrôleur de domaine' with value 'Catalogue global', 'Site' with value 'Default-First-Site-Name', and 'Description' which is empty. The right screenshot shows the 'Éditeur d'attributs' tab with the following fields: 'Nom' with value 'Windows Server 2019 Datacenter', 'Version' with value '10.0 (17763)', and 'Service Pack' which is empty. Both windows have tabs for 'Général', 'Système d'exploitation', 'Sécurité', 'Appel entrant', 'Membre de', 'Délégation', and 'Emplacement'.

# Cette commande affiche plusieurs propriétés du SERVEUR1

```
Get-ADComputer -Identity SERVEUR1
```

```
DistinguishedName : CN=SERVEUR1,OU=Domain Controllers,DC=FORMATION,DC=LOCAL
DNSHostName       : SERVEUR1.FORMATION.LOCAL
Enabled           : True
Name              : SERVEUR1
ObjectClass       : computer
ObjectGUID        : a0f468b1-9066-4ea4-9f2b-aa1f2ae20a27
SamAccountName    : SERVEUR1$
SID               : S-1-5-21-2424922765-3573753519-521296372-1000
UserPrincipalName :
```

DNSHostName est présent si l'ordinateur est membre d'un domaine.

Le SamAccountName d'un ordinateur de l'Active Directory se termine toujours par un \$.

**# Cette commande affiche des propriétés supplémentaires pour le SERVEUR1**

```
$serveur = "SERVEUR1"
```

```
Get-ADComputer -Identity $serveur `
    -Properties CanonicalName,Description,
    IPv4Address,OperatingSystem,OperatingSystemVersion | `
Format-List Name,CanonicalName,DistinguishedName,
    DNSHostName,SamAccountName,
    Description,IPv4Address,
    OperatingSystem,OperatingSystemVersion,
    Enabled
```

```
Name : SERVEUR1
CanonicalName : FORMATION.LOCAL/Domain Controllers/SERVEUR1
DistinguishedName : CN=SERVEUR1,OU=Domain Controllers,DC=FORMATION,DC=LOCAL
DNSHostName : SERVEUR1.FORMATION.LOCAL
SamAccountName : SERVEUR1$
Description :
IPv4Address : 192.168.1.10
OperatingSystem : Windows Server 2019 Datacenter
OperatingSystemVersion : 10.0 (17763)
Enabled : True
```

La propriété **IPv4Address** retournée par la commande est une propriété calculée par PowerShell.  
PowerShell calcule la valeur de **IPv4Address** en résolvant l'adresse IPv4 associée au nom de l'ordinateur en utilisant le serveur DNS.

Le SERVEUR2 est dans le conteneur "Computers".

Propriétés de : SERVEUR2

Emplacement   Géré par   Objet   Sécurité   Appel entrant   Éditeur d'attributs  
Général   Système d'exploitation   Membre de   Délégation   Réplication de mot de passe

SERVEUR2

Nom d'ordinateur (antérieur à Windows 2000) :

Nom DNS :

Type de contrôleur de domaine :

Site :

Description :

OK   Annuler   Appliquer   Aide

Propriétés de : SERVEUR2

Emplacement   Géré par   Objet   Sécurité   Appel entrant   Éditeur d'attributs  
Général   Système d'exploitation   Membre de   Délégation   Réplication de mot de passe

Nom :

Version :

Service Pack :

OK   Annuler   Appliquer   Aide

# Cette commande affiche plusieurs propriétés du SERVEUR2

`Get-ADComputer -Identity SERVEUR2`

```
DistinguishedName : CN=SERVEUR2,CN=Computers,DC=FORMATION,DC=LOCAL
DNSHostName       : SERVEUR2.FORMATION.LOCAL
Enabled           : True
Name              : SERVEUR2
ObjectClass       : computer
ObjectGUID        : 05ceb1e5-f68d-4efd-82a1-e210a3cb8db4
SamAccountName    : SERVEUR2$
SID               : S-1-5-21-2424922765-3573753519-521296372-1103
UserPrincipalName :
```

DNSHostName est présent si l'ordinateur est membre d'un domaine.

Le SamAccountName d'un ordinateur de l'Active Directory se termine toujours par un \$.

### # Cette commande affiche des propriétés supplémentaires pour le SERVEUR2

```
$serveur = "SERVEUR2"
```

```
Get-ADComputer -Identity $serveur `
    -Properties CanonicalName,Description,
    IPv4Address,OperatingSystem,OperatingSystemVersion | `
Format-List Name,CanonicalName,DistinguishedName,
    DNSHostName,SamAccountName,
    Description,IPv4Address,
    OperatingSystem,OperatingSystemVersion,
    Enabled
```

```
Name : SERVEUR2
CanonicalName : FORMATION.LOCAL/Computers/SERVEUR2
DistinguishedName : CN=SERVEUR2,CN=Computers,DC=FORMATION,DC=LOCAL
DNSHostName : SERVEUR2.FORMATION.LOCAL
SamAccountName : SERVEUR2$
Description :
IPv4Address : 192.168.1.20
OperatingSystem : Windows Server 2019 Datacenter
OperatingSystemVersion : 10.0 (17763)
Enabled : True
```

La propriété **IPv4Address** retournée par la commande est une propriété calculée par PowerShell. PowerShell calcule la valeur de **IPv4Address** en résolvant l'adresse IPv4 associée au nom de l'ordinateur en utilisant le serveur DNS.

## Programmation d'un ordinateur avec PowerShell ISE

Le module **ActiveDirectory** de PowerShell contient quatre cmdlets pour gérer les ordinateurs.

```
Get-ADComputer
New-ADComputer
Remove-ADComputer
Set-ADComputer
```

Exemple de création d'un ordinateur avec PowerShell.

L'avantage de créer un ordinateur avant de le joindre au domaine, c'est que l'ordinateur sera préinstallé dans la bonne unité d'organisation.

On veut créer l'ordinateur **SRVWEB1** dans l'unité organisation "**WEB**".

Le paramètre **-Path** utilise la valeur de l'attribut **DistinguishedName**

### # Code PowerShell pour ajouter un ordinateur

```
New-ADComputer -Name SRVWEB1 `
    -Path "OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL" `
    -Description "Serveur WEB principal"
```

## **Introduction à Active Directory**

Active Directory a été introduit pour la première fois en 1999 avec la sortie de "Windows 2000 Server".

Active Directory partage plusieurs caractéristiques avec une base de données.

### **Les avantages de l'Active Directory**

- 1) Active Directory permet aux administrateurs de centraliser la gestion des comptes utilisateurs, des groupes, des ordinateurs, des unités d'organisations et des autres objets.
- 2) Active Directory simplifie l'administration et la maintenance des systèmes.
- 3) Active Directory assure une authentification sécurisée des utilisateurs et des ordinateurs dans le réseau.

Le schéma de l'Active Directory est similaire à un dictionnaire, il contient les définitions de chaque classe d'objet et de chaque attribut.

Les versions des schémas de l'Active Directory.

|                        |                    |
|------------------------|--------------------|
| Windows Server 2025    | Schema version: 90 |
| Windows Server 2022    | Schema version: 88 |
| Windows Server 2019    | Schema version: 88 |
| Windows Server 2016    | Schema version: 87 |
| Windows Server 2012 R2 | Schema version: 69 |
| Windows Server 2012    | Schema version: 56 |
| Windows Server 2008 R2 | Schema version: 47 |
| Windows Server 2008    | Schema version: 44 |
| Windows Server 2003 R2 | Schema version: 31 |
| Windows Server 2003    | Schema version: 30 |
| Windows Server 2000    | Schema version: 13 |

Voici la commande PowerShell qui permet d'afficher la version du schéma de l'Active Directory.

**Get-ADObject (Get-ADRootDSE).schemaNamingContext -Properties objectVersion**

```
PS C:\Users\Administrateur> Get-ComputerInfo | Select-Object WindowsProductName,WindowsVersion

WindowsProductName      WindowsVersion
-----
Windows Server 2019 Datacenter 1809

PS C:\Users\Administrateur> Get-ADObject (Get-ADRootDSE).schemaNamingContext -Properties objectVersion

DistinguishedName : CN=Schema,CN=Configuration,DC=FORMATION,DC=LOCAL
Name               : Schema
ObjectClass        : dMD
ObjectGUID         : af7dd477-62e8-4443-8469-cbc5b4475bf8
objectVersion      : 88

PS C:\Users\Administrateur>
```

---

L'Active Directory a un nombre maximum d'objets qu'il peut gérer.

Le nombre d'objet maximum est  $2^{31} - 255 = 2\,147\,483\,648 - 255 = 2\,147\,483\,393$

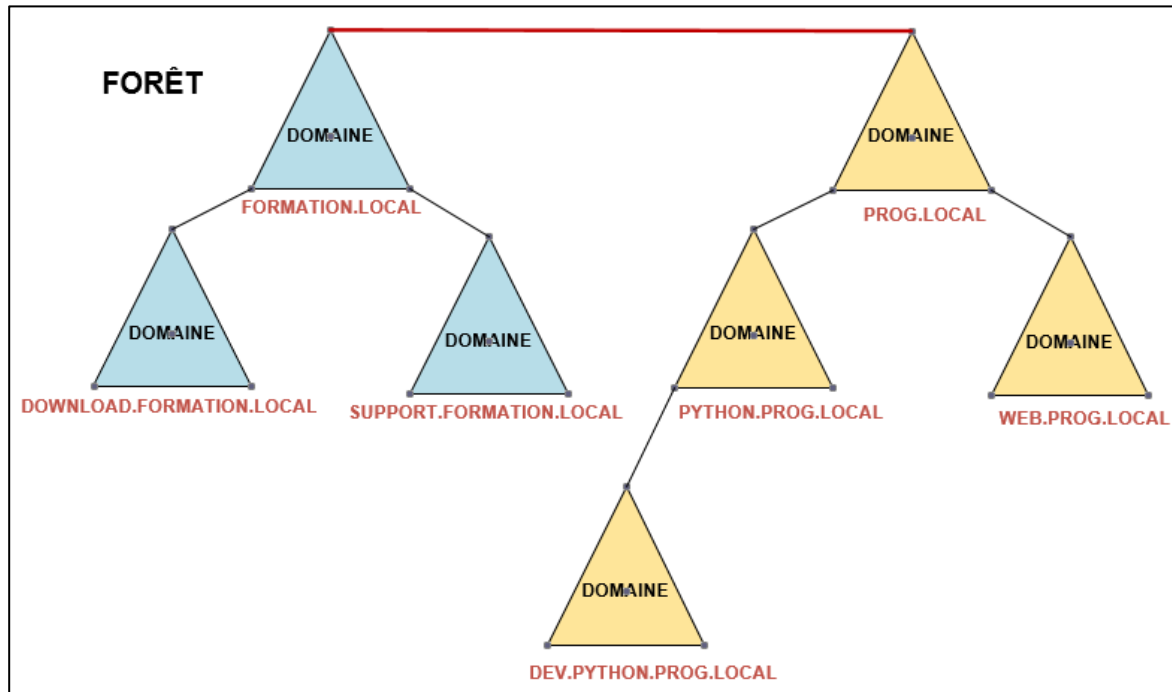
---

### Aperçu d'une structure "Active Directory"

Active Directory (AD) est une organisation hiérarchisée d'objets.

Les objets sont classés en trois grandes catégories:

- Les ressources (exemple: ordinateurs, imprimantes)
- Les services (exemple: courrier électronique)
- Les utilisateurs et les groupes
- L'AD fournit des informations sur les objets, il organise et contrôle les accès.



Cette forêt est constituée de deux arbres et chaque arbre est constitué de plusieurs domaines.

### Catalogue global

Le catalogue global est l'ensemble de tous les objets d'une forêt AD DS (Active Directory Domain Services). Un serveur de catalogue global est un contrôleur de domaine qui enregistre une copie complète de tous les objets de l'annuaire pour son domaine hôte et une copie partielle en lecture seule de tous les objets pour tous les autres domaines de la forêt.

Un domaine Active Directory contient au moins un contrôleur de domaine.

### Installation de l'Active Directory en mode graphique

Dans la console "**Gestionnaire de serveur**" installer le rôle "**Services AD DS**"

- L'installation de l'Active Directory nécessite l'installation du rôle DNS
- L'installation de l'Active Directory exige un redémarrage.
- Après le redémarrage, nous devons compléter la post-installation afin de "promouvoir ce serveur en contrôleur de domaine".
- On doit choisir "Ajouter une nouvelle forêt" si c'est un nouveau domaine

---

Le répertoire **C:\Windows\NTDS** contient les journaux de transaction, les logs et les fichiers temporaires utiles au fonctionnement de l'Active Directory.

Le fichier **ntds.dit** constitue la base de données de l'Active Directory.

- Ce fichier est présent sur chaque contrôleur de domaine.
- DIT signifie (Directory Information Tree)

---

### Les partages administratifs (NETLOGON, SYSVOL)

Après l'installation de l'Active Directory nous avons accès à deux partages

- \\FORMATION.LOCAL\NETLOGON      C:\Windows\SYSVOL\sysvol\FORMATION.LOCAL\scripts
- \\FORMATION.LOCAL\SYSVOL        C:\Windows\SYSVOL\sysvol

On remarque que le partage NETLOGON est un sous-dossier du partage SYSVOL.

- Le partage NETLOGON est accessible en lecture pour "Tout le monde".
- Le partage NETLOGON est accessible en écriture pour le groupe "FORMATION\Administrateurs".  
**L'accès en écriture n'est pas permis si l'accès se fait directement sur le contrôleur de domaine.**

Le partage SYSVOL est répliqué entre les contrôleurs de domaine.

Le partage SYSVOL contient deux dossiers

- \\FORMATION.LOCAL\SYSVOL\FORMATION.LOCAL\**Politiques**  
**Ce dossier contient les GPO.**
- \\FORMATION.LOCAL\SYSVOL\FORMATION.LOCAL\**scripts**  
**Ce dossier contient les scripts de démarrage ou d'ouverture de session.**

---

### Gestion des utilisateurs, des groupes, des ordinateurs et des unités d'organisation

- La console "**Utilisateurs et ordinateurs Active Directory**" permet la gestion des utilisateurs, des groupes, des ordinateurs et des unités d'organisation.
- La console "**Centre d'administration Active Directory**" permet la gestion des utilisateurs, des groupes, des ordinateurs et des unités d'organisation.  
Cette console est plus récente que la console "Utilisateurs et ordinateurs Active Directory".

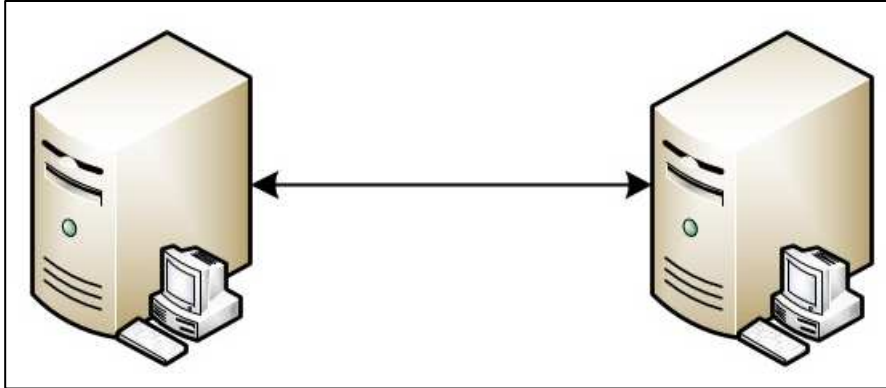


## ANNEXE 1

### "Active Directory" avec deux contrôleurs de domaine

**Dans le cours, nous n'utiliserons pas deux contrôleurs de domaine.**

Il est préférable d'avoir au minimum deux contrôleurs de domaine pour assurer la disponibilité et la continuité des services de l'Active Directory.



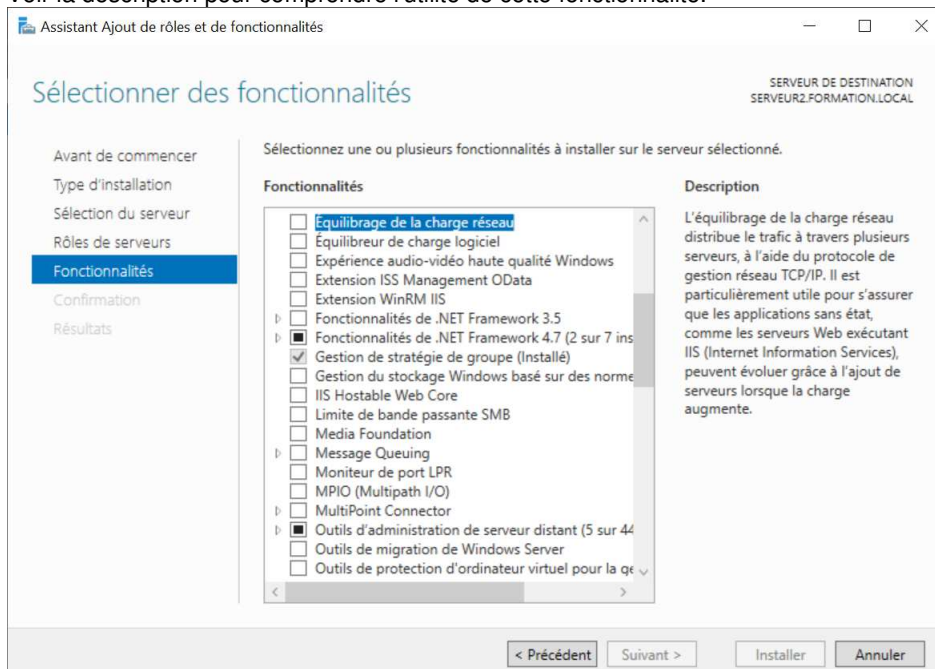
Les contrôleurs de domaine répliquent les informations entre eux à intervalle régulier, afin de disposer d'un annuaire Active Directory identique. En plus, les contrôleurs de domaine répliquent le contenu du dossier "SYSVOL" qui est utilisé pour distribuer les stratégies de groupe et les scripts de connexion.

## ANNEXE 2

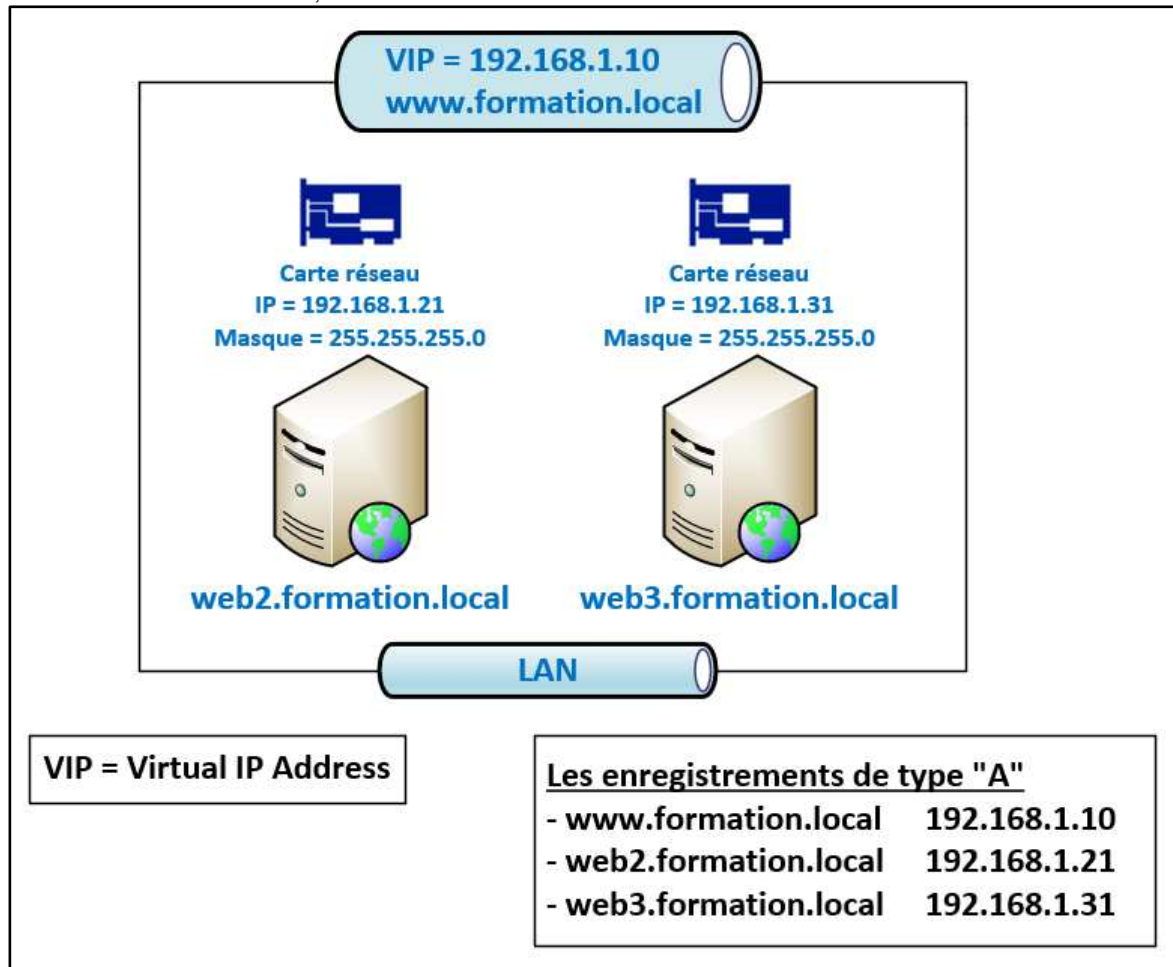
### La fonctionnalité "Équilibrage de la charge réseau"

**Dans le cours, nous n'utiliserons pas la fonctionnalité "Équilibrage de la charge réseau".**

Voir la description pour comprendre l'utilité de cette fonctionnalité.



Voici un schéma qui montre deux serveurs qui utilisent la fonctionnalité "**Équilibrage de la charge réseau**".  
Chaque serveur héberge un site web dont le contenu est identique.  
Sur le premier serveur, l'adresse IP virtuelle 192.168.1.10 est associée à l'adresse IP 192.168.1.20.  
Sur le deuxième serveur, l'adresse IP virtuelle 192.168.1.10 est associée à l'adresse IP 192.168.1.21.  
Pour avoir accès au site web, on doit utiliser l'adresse IP virtuelle 192.168.1.10.

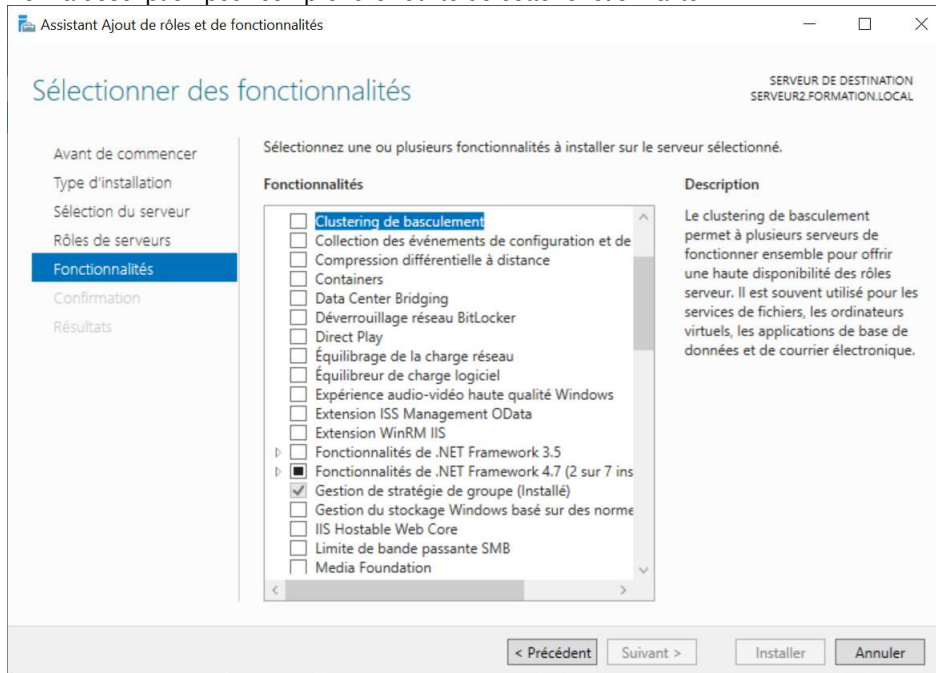


### ANNEXE 3

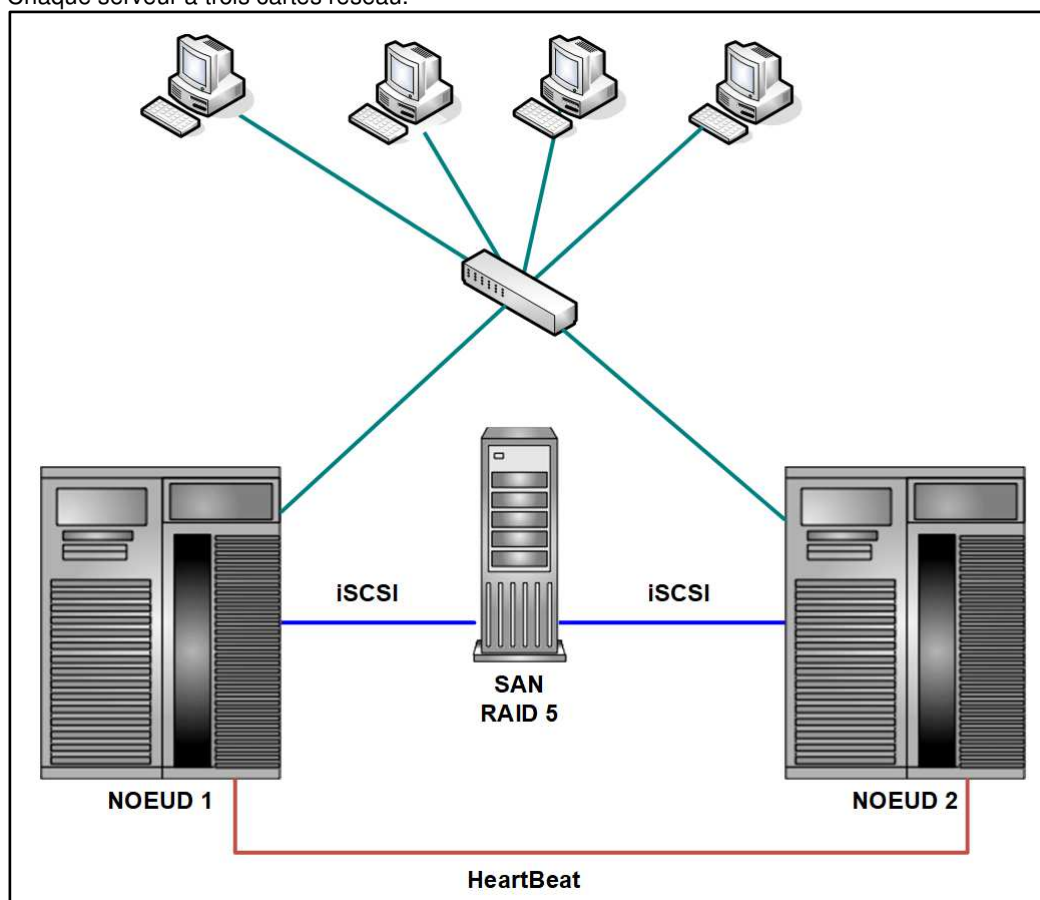
#### La fonctionnalité "Clustering de basculement"

**Dans le cours, nous n'utiliserons pas la fonctionnalité "Clustering de basculement".**

Voir la description pour comprendre l'utilité de cette fonctionnalité.



Voici un schéma d'un cluster de basculement.  
Chaque serveur a trois cartes réseau.



## ANNEXE 4 "Active Directory" et Linux

**Dans le cours, nous ne joindrons pas de distribution Linux à l'Active Directory.**

"Ubuntu 21.04" apporte l'intégration native de Microsoft Active Directory.

Ce n'est pas nouveau que de pouvoir joindre un ordinateur Linux à l'Active Directory, ce qui est nouveau avec "Ubuntu 21.04" c'est qu'il est possible de le faire pendant l'installation.

The screenshot shows the 'Qui êtes-vous ?' (Who are you?) screen during the Ubuntu 21.04 installation. The window has a title bar with the date 'Apr 23 11:48' and system icons. The main content area is titled 'Installation' and 'Qui êtes-vous ?'. It contains several input fields and checkboxes:

- Votre nom :** A text box containing 'tech' with a green checkmark to its right.
- Le nom de votre ordinateur :** A text box containing 'tech-VM-Ubuntu' with a green checkmark to its right. Below it, a smaller text box contains 'Le nom qu'il utilise pour communiquer avec d'autres ordinateurs.'
- Choisir un nom d'utilisateur :** A text box containing 'tech' with a green checkmark to its right.
- Choisir un mot de passe :** A text box with masked characters (dots) and a green checkmark to its right. To the right of the text box, it says 'Mot de passe sûr'.
- Confirmez votre mot de passe :** A text box with masked characters and a green checkmark to its right.
- Session options:** Two radio buttons: 'Ouvrir la session automatiquement' (unselected) and 'Demander mon mot de passe pour ouvrir une session' (selected).
- Active Directory:** A checkbox labeled 'Utiliser Active Directory' which is checked. Below it, a smaller text box contains 'Vous saisissez le domaine et d'autres détails à l'étape suivante.'

At the bottom right, there are two buttons: 'Précédent' and 'Continuer'. At the bottom center, there are seven purple dots, with the first one being larger, indicating the current step in the installation process.

Apr 23 11:50

Installation

### Configurer Active Directory

Domaine :   ✓


Administrateur du domaine :  ✓

Mot de passe :

● ● ● ● ● ● ● ●

Propriétés de : tech-VM-Ubuntu

| Emplacement | Géré par               | Appel entrant |
|-------------|------------------------|---------------|
| Général     | Système d'exploitation | Membre de     |

 **tech-VM-Ubuntu**

Nom d'ordinateur (antérieur à Windows 2000) :

Nom DNS :

Type de contrôleur de domaine :

Site :

Description :

Propriétés de : tech-VM-Ubuntu

| Emplacement | Géré par               | Appel entrant |
|-------------|------------------------|---------------|
| Général     | Système d'exploitation | Membre de     |

Nom :

Version :

Service Pack :

## Installation de l'Active Directory

---

### Objectifs

- Installer le rôle AD DS (Active Directory Domain Services) sur le SERVEUR1
- Joindre le SERVEUR2 au domaine

### Matériels

- L'ordinateur réel avec deux ordinateurs virtuels avec "Windows Server 2019"

### Étape 1 - Vérification du contrôleur de domaine

Démarrer l'ordinateur virtuel "SERVEUR1" et connectez-vous avec l'utilisateur Administrateur.

Vérifier la configuration du serveur virtuel "SERVEUR1"

- Le nom du serveur est **SERVEUR1**
- Modifier la configuration DNS de la carte réseau  
DNS: **127.0.0.1**

### Étape 2 - Création d'un domaine

Démarrer la console "Gestionnaire de serveur", dans le menu "Gérer"

Installer le rôle "Services AD DS"

- Lire les informations qui vous sont données
- Cocher "Redémarrer automatiquement le serveur de destination, si nécessaire"
- Quand les fonctionnalités seront installées, fermer la fenêtre et cliquez sur le triangle jaune qui est en haut et à droite, à côté du drapeau
  - Il faut effectuer la configuration post-déploiement (choisir "Promouvoir ce serveur en contrôleur de domaine")

---

Répondre aux questions de la post-configuration du domaine

- Écran "Configuration de déploiement"
  - Choisir "Ajouter une nouvelle forêt"
  - Le nom de domaine racine est **FORMATION.LOCAL**
- Écran "Options du contrôleur de domaine"
  - Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)  
Mot de passe: AAAaaa111  
Confirmer le mot de passe: AAAaaa111
  - Vous aurez un avertissement "Il est impossible de créer une délégation pour ce serveur DNS ..."  
**Ne vous en occupez pas et cliquer sur le bouton "Suivant".**
- Écran "Options supplémentaires"
  - Le nom de domaine NetBIOS: **FORMATION**  
**Vous aurez besoin de cette information pour joindre le SERVEUR2 au domaine.**
- Écran "Chemins d'accès"
  - Ne pas changer l'emplacement des dossiers proposés par défaut

- Écran "Examiner les options"

Assistant Configuration des services de domaine Active Directory

Examiner les options

SERVEUR CIBLE  
SERVEUR1

Configuration de déploie...  
Options du contrôleur de...  
Options DNS  
Options supplémentaires  
Chemins d'accès  
**Examiner les options**  
Vérification de la configur...  
Installation  
Résultats

Vérifiez vos sélections :

Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.

Le nouveau nom de domaine est « **FORMATION.LOCAL** ». C'est aussi le nom de la nouvelle forêt.

Nom NetBIOS du domaine : FORMATION

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Options supplémentaires :

Catalogue global : Oui

Serveur DNS : Oui

Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires

[Afficher le script](#)

[En savoir plus sur les options d'installation](#)

< Précédent Suivant > Installer Annuler

Il est important de vérifier que le nom du domaine est **FORMATION.LOCAL**

Assistant Configuration des services de domaine Active Directory

Examiner les options

SERVEUR CIBLE  
SERVEUR1

Configuration de déploie...  
Options du contrôleur de...  
Options DNS  
Options supplémentaires  
Chemins d'accès  
**Examiner les options**  
Vérification de la configur...  
Installation  
Résultats

Vérifiez vos sélections :

Serveur DNS : Oui

Créer une délégation DNS : Non

Dossier de la base de données : C:\Windows\NTDS

Dossier des fichiers journaux : C:\Windows\NTDS

Dossier SYSVOL : C:\Windows\SYSVOL

Le service Serveur DNS sera configuré sur cet ordinateur.

Cet ordinateur sera configuré pour utiliser ce serveur DNS en tant que serveur DNS préféré.

Le mot de passe du nouvel administrateur de domaine sera le même que celui de l'administrateur local de cet ordinateur.

Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires

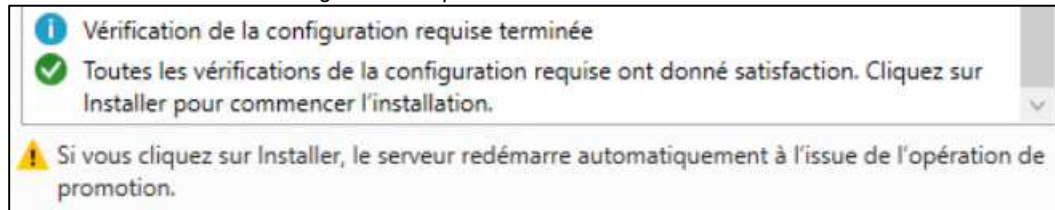
[Afficher le script](#)

[En savoir plus sur les options d'installation](#)

< Précédent Suivant > Installer Annuler



- Écran "Vérification de la configuration requise"



- Il est important de vérifier que la dernière ligne confirme que la configuration minimale requise est satisfaite.
- Démarrer l'installation
- Le serveur va redémarrer à la fin de l'installation.

### Étape 3 - Validation du domaine

Connectez-vous sur le contrôleur de domaine.

Dans la console DNS (Gestionnaire de serveur / Outils / DNS)

- Sélectionner "SERVEUR1 / Zones de recherche directes" / FORMATION.LOCAL" pour vérifier la présence d'un enregistrement de type "A" au nom de votre serveur SERVEUR1

Dans une invite de commandes exécuter la commande suivante

**ping SERVEUR1.FORMATION.LOCAL -4**

Vérifier la présence des partages: NETLOGON et SYSVOL

- exécuter "net share" dans une "Invite de commandes"
- tester l'accès aux partages SYSVOL et NETLOGON  
\\FORMATION.LOCAL\NETLOGON  
\\FORMATION.LOCAL\SYSVOL


### Étape 4 - Joindre le SERVEUR2 au domaine

Connectez-vous sur le "SERVEUR2" en utilisant le compte Administrateur.

Vérifier la configuration du serveur virtuel "SERVEUR2"

- Le nom du serveur 2 est **SERVEUR2**
- Modifier la configuration DNS de la carte réseau  
DNS: 192.168.1.10 (adresse IP du "Contrôleur de Domaine")

#### Joindre l'ordinateur à votre domaine

( + Pause) permet d'afficher la fenêtre "Propriétés système"

Cliquer sur "Modifier les paramètres"

- Choisir l'option "Membre d'un Domaine:"
- Taper le nom de domaine NetBIOS qui est **FORMATION**

Authentifiez-vous avec le compte Administrateur du domaine avec FORMATION\administrateur

- Après le message de bienvenue, vous devez redémarrer l'ordinateur client.

#### Canal sécurisé entre un ordinateur et le contrôleur de domaine

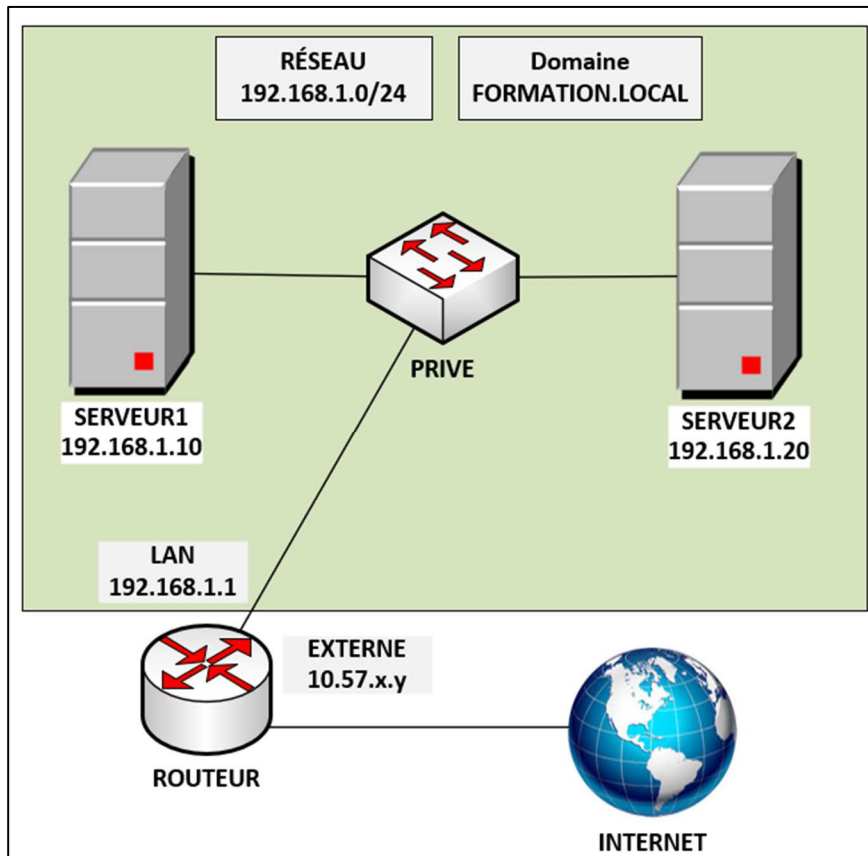
Lorsqu'un ordinateur est joint au domaine, un compte ordinateur est créé.

Le compte ordinateur possède un nom (samAccountName ) et un mot de passe.

Le samAccountName d'un ordinateur de l'Active Directory se termine toujours par un \$.

Le mot de passe est enregistré sous forme de secret LSA (Local Security Account) et est changé à chaque 30 jours.

**Le schéma de nos serveurs.**



## Toujours sur le "SERVEUR2", connectez-vous au domaine.

Utilisation d'un compte de l'Active Directory

- FORMATION\Administrateur
- Administrateur@formation.local

utilise le compte Administrateur du domaine  
utilise le compte Administrateur du domaine



"Connectez-vous à FORMATION" indique vous utilisez un compte de l'Active Directory.

---

## Pour le cours, il ne sera pas nécessaire de se connecter avec un compte local sur le SERVEUR2.

Utilisation d'un compte local du SERVEUR2

- Administrateur
- .\Administrateur
- SERVEUR2\Administrateur

utilise le compte Administrateur local  
utilise le compte Administrateur local  
.\ fait référence à l'ordinateur local  
utilise le compte Administrateur local  
SERVEUR2\ force l'utilisation du compte Administrateur local



"Connectez-vous à SERVEUR2" indique que vous utilisez un compte local du SERVEUR2.

## Étape 5 – Renommer le compte "Administrateur" local sur le SERVEUR2

Pour éviter de se connecter par erreur avec le compte "Administrateur" local sur le SERVEUR2, je vous conseille de renommer le compte "Administrateur" local.

**Le nom de l'utilisateur dont le SID se termine par 500 varie selon la langue.**

- En français, le nom de l'utilisateur est "Administrateur".
- En anglais, le nom de l'utilisateur est "Administrator".
- En espagnol, le nom de l'utilisateur est "Administrador".
- ...

# Le code doit s'exécuter sur le SERVEUR2  
\$NewAdminName = "AdminLocal"

```
$Objet = Get-LocalUser | Where-Object { $PSItem.SID -like "S-1-5-21-*500" }  
Rename-LocalUser -InputObject $Objet -NewName $NewAdminName
```

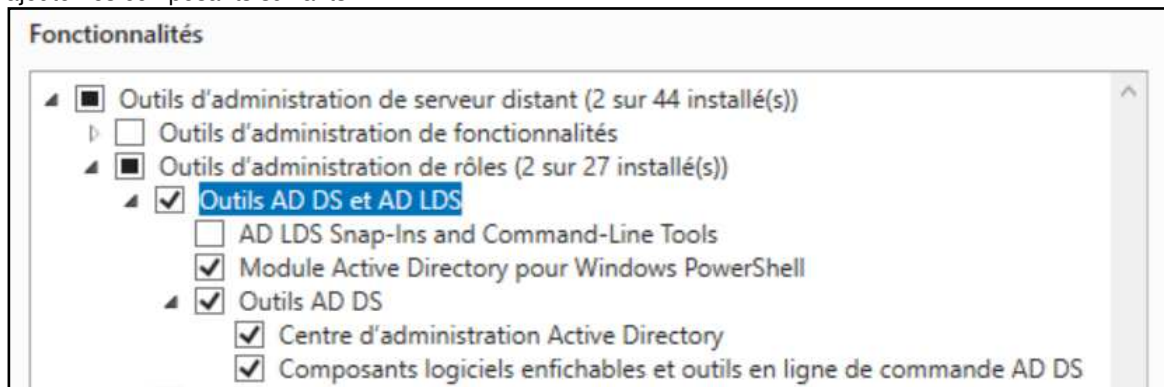
## Étape 6 – Installer la console UOAD sur le SERVEUR2

Par défaut, la console UOAD n'est pas installée sur un serveur qui est joint à un domaine Active Directory.

### Installer les outils d'administration

Dans la fonctionnalité "Outils d'administration de serveur distant", développer "Outils d'administration de rôles".

- ajouter les composants suivants



Si tout s'est bien passé, la console UOAD (Utilisateurs et Ordinateurs Active Directory) sera installée sur le SERVEUR2.

## ANNEXE

### Comment sortir un ordinateur du domaine

**Vous devez utiliser ces commandes en cas de besoin seulement.**

Cette commande permet de sortir un ordinateur du domaine si le contrôleur de domaine existe.  
Cette commande demande le mot de passe du compte " **NomDuDomaine\Administrateur**".

```
Remove-Computer -ComputerName NomDeLordinateur `
                 -UnjoinDomainCredential NomDuDomaine\Administrateur `
                 -WorkgroupName NomDuGroupeDeTravail `
                 -Force `
                 -Restart
```

---

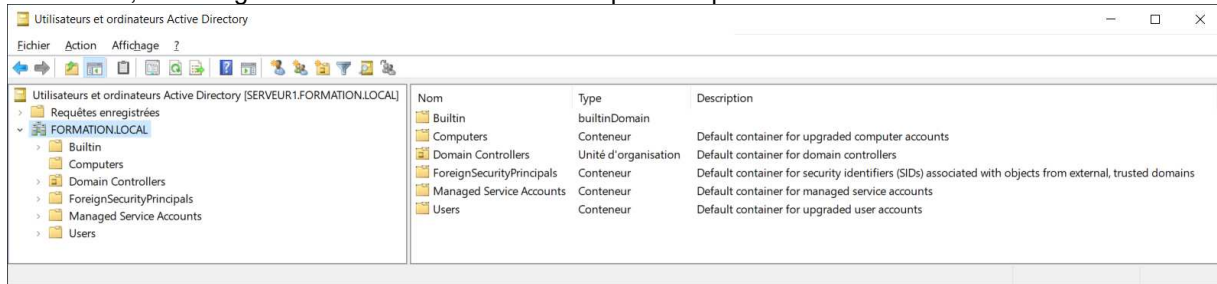
Cette commande permet de sortir un ordinateur du domaine même si le contrôleur de domaine n'existe plus.  
Après l'exécution de la commande, le groupe de travail portera le nom du domaine.

```
netdom.exe remove NomDeLordinateur /Domain:NomDuDomaine /Force /Reboot
```

## La console "Utilisateurs et ordinateurs Active Directory" (UOAD)

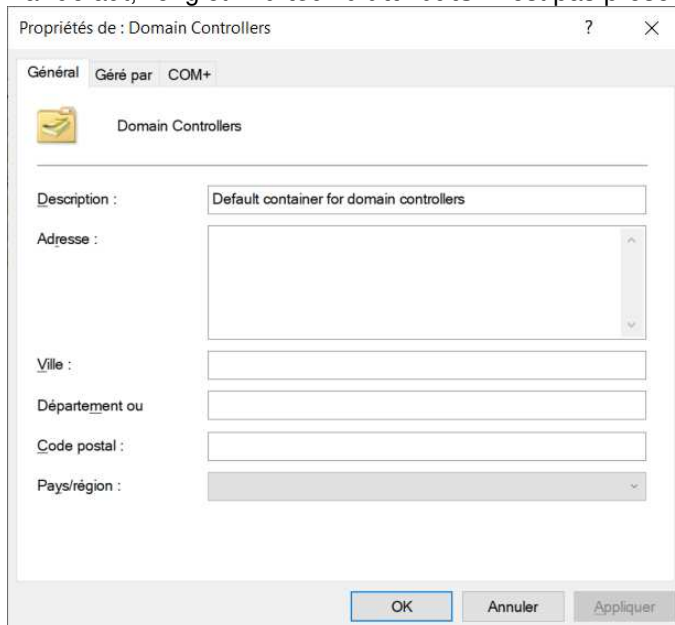
Le nom anglais de la console est "Active Directory Users and Computers" et l'abréviation est (ADUC).

Par défaut, l'affichage dans la console UOAD n'est pas complet.

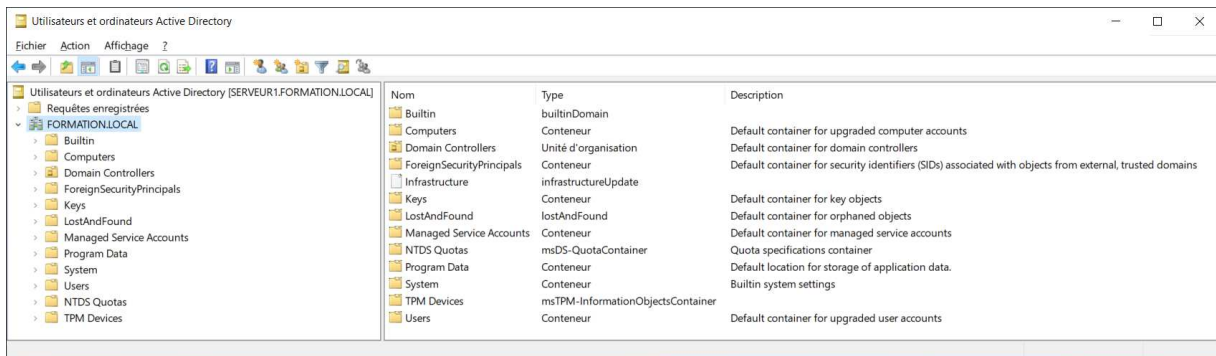
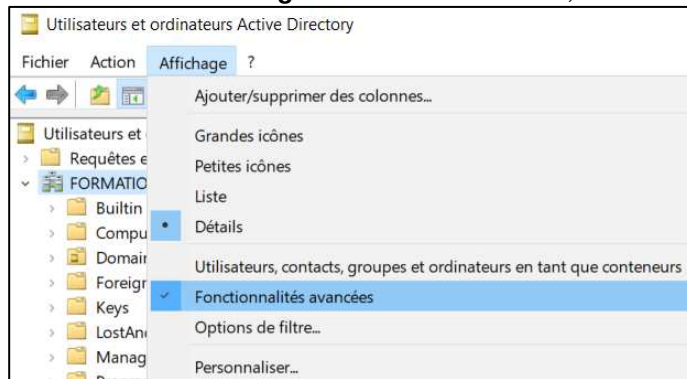


Chaque objet de l'Active Directory a des attributs.

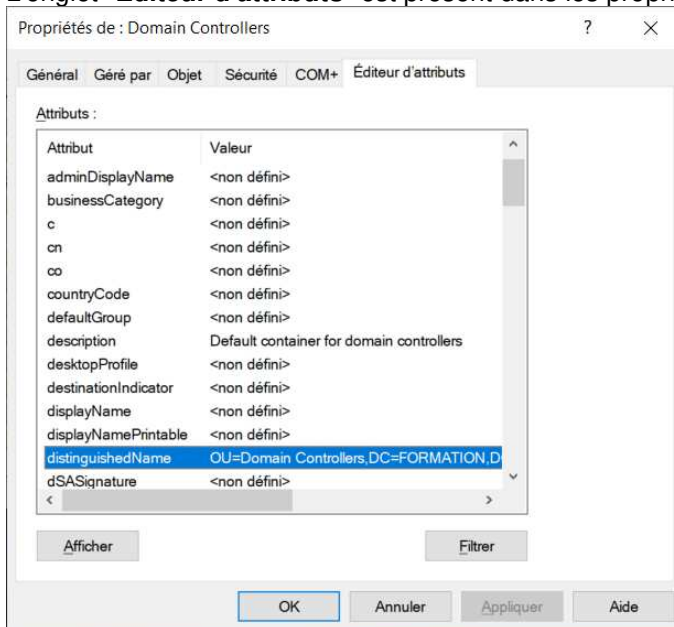
Par défaut, l'onglet "**Éditeur d'attributs**" n'est pas présent dans les propriétés d'un objet.



Dans le menu "**Affichage**" de la console UOAD, il faut activer "**Fonctionnalités avancées**"



L'onglet "**Éditeur d'attributs**" est présent dans les propriétés d'un objet.



La propriété DistinguishedName est très importante.  
La propriété DistinguishedName est unique pour chaque objet dans l'Active Directory.

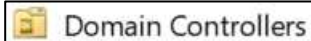
## L'attribut DistinguishedName

La valeur de l'attribut **DistinguishedName** est utilisée dans plusieurs commandes PowerShell.

| Attribut | Description         |
|----------|---------------------|
| DC       | Domain Component    |
| CN       | Common Name         |
| OU       | Organizational Unit |

### Exemple de valeur pour l'attribut "distinguishedName" pour une "Unité d'organisation"

L'unité d'organisation "Domain Controllers" existe par défaut.



OU=Domain Controllers,DC=FORMATION,DC=LOCAL

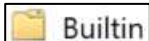
**NOTE:** Un Administrateur peut créer des unités d'organisation.



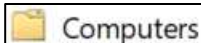
OU=Utilisateurs,DC=FORMATION,DC=LOCAL

### Exemple de valeur pour l'attribut "distinguishedName" pour un "Conteneur"

Voici les "Conteneurs" les plus utilisés dans le cours.



CN=Builtin,DC=FORMATION,DC=LOCAL



CN=Computers,DC=FORMATION,DC=LOCAL

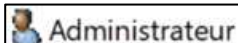


CN=Users,DC=FORMATION,DC=LOCAL

**NOTE:** Un Administrateur ne peut pas créer des objets "Conteneur".

### Exemple de valeur pour l'attribut "distinguishedName" pour un "Utilisateur"

L'utilisateur "Administrateur" est dans le conteneur "Users".



CN=Administrateur,CN=Users,DC=FORMATION,DC=LOCAL

### Exemple de valeur pour l'attribut "distinguishedName" pour un "Groupe"

Le groupe "Administrateurs" est dans le conteneur "Builtin".



CN=Administrateurs,CN=Builtin,DC=FORMATION,DC=LOCAL

### Exemple de valeur pour l'attribut "distinguishedName" pour un "Ordinateur"

L'ordinateur "SERVEUR2" est dans le conteneur "Computers".



CN=SERVEUR2,CN=Computers,DC=FORMATION,DC=LOCAL

L'ordinateur "SERVEUR1" est dans l'unité d'organisation "Domain Controllers".



CN=SERVEUR1,OU=Domain Controllers,DC=FORMATION,DC=LOCAL



## Création d'un utilisateur dans l'Active Directory

### Objectifs

- Introduction à la console "Utilisateurs et Ordinateurs Active Directory" (UOAD)
- Création d'un utilisateur avec les mêmes privilèges que l'utilisateur "Administrateur" du domaine

Voici deux recommandations de sécurité concernant l'utilisation du compte Administrateur du domaine.

- 1) Il est recommandé de désactiver le compte Administrateur du domaine.  
Avant de désactiver le compte Administrateur du domaine, vous devez créer un ou plusieurs comptes administratifs avec les mêmes privilèges pour gérer le domaine.
- 2) Vous devez utiliser des mots de passe forts et complexes pour tous les comptes administratifs.

## Création de l'utilisateur TECH dans l'Active Directory

**De préférence, chaque étudiant doit travailler sur un serveur membre.  
Je vous suggère de ne pas travailler directement sur le contrôleur de domaine.**

Connectez-vous sur le "SERVEUR2" avec l'utilisateur "FORMATION\Administrateur".

Démarrer la console "Utilisateurs et Ordinateurs Active Directory"

Le but est de créer un nouvel utilisateur FORMATION\TECH qui aura les mêmes caractéristiques que le compte "Administrateur" du domaine.

- À l'intérieur du conteneur "**Users**" sélectionner l'utilisateur "**Administrateur**"  
Dans le menu contextuel, il faut sélectionner "**Copier...**"

Copier l'objet - Utilisateur

Créer dans : FORMATION.LOCAL/Users

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  
 @FORMATION.LOCAL

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent **Suivant >** Annuler

Copier l'objet - Utilisateur

Créer dans : FORMATION.LOCAL/Users

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

< Précédent Suivant > Annuler

Mot de passe

- Le mot de passe doit avoir au moins 6 caractères et être complexe.
- Cocher "Le mot de passe n'expire jamais"

● Vérification des deux utilisateurs

Propriétés de : TECH

Environnement Sessions Contrôle à distance

Profil des services Bureau à distance COM+ Éditeur d'attributs

Général Adresse Compte Profil Téléphones Organisation Certificats publiés

Membre de Réplication de mot de passe Appel entrant Objet Sécurité

Membre de :

| Nom   | Dossier Services de domaine Active Direct |
|---|---|
| Administrateurs                                   | FORMATION.LOCAL/Builtin                   |
| Administrateurs de l'entreprise                   | FORMATION.LOCAL/Users                     |
| Administrateurs du schéma                         | FORMATION.LOCAL/Users                     |
| Admins du domaine                                 | FORMATION.LOCAL/Users                     |
| Propriétaires créateurs de la stratégie de groupe | FORMATION.LOCAL/Users                     |
| Utilisateurs du domaine                           | FORMATION.LOCAL/Users                     |

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Définir le groupe principal

Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK Annuler Appliquer Aide

Propriétés de : Administrateur

Environnement Sessions Contrôle à distance

Profil des services Bureau à distance COM+ Éditeur d'attributs

Général Adresse Compte Profil Téléphones Organisation Certificats publiés

Membre de Réplication de mot de passe Appel entrant Objet Sécurité

Membre de :

| Nom   | Dossier Services de domaine Active Direct |
|---|---|
| Administrateurs                                   | FORMATION.LOCAL/Builtin                   |
| Administrateurs de l'entreprise                   | FORMATION.LOCAL/Users                     |
| Administrateurs du schéma                         | FORMATION.LOCAL/Users                     |
| Admins du domaine                                 | FORMATION.LOCAL/Users                     |
| Propriétaires créateurs de la stratégie de groupe | FORMATION.LOCAL/Users                     |
| Utilisateurs du domaine                           | FORMATION.LOCAL/Users                     |

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Définir le groupe principal

Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK Annuler Appliquer Aide

Les deux utilisateurs sont membres des mêmes groupes.

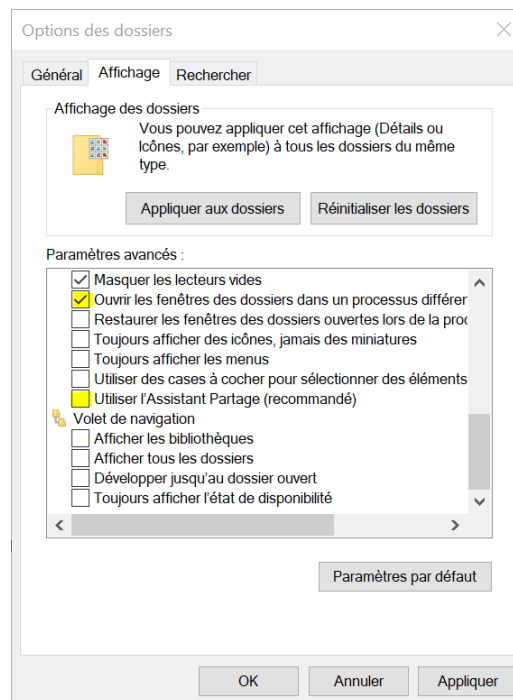
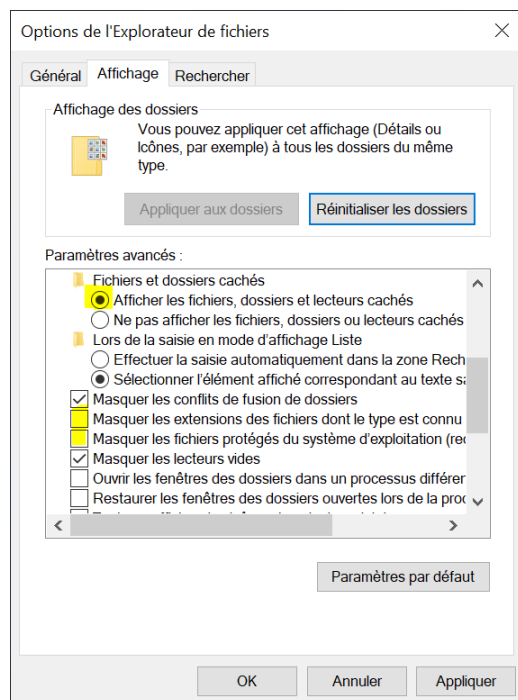
**À PARTIR DE MAINTENANT, VOUS NE DEVEZ PLUS UTILISER LE COMPTE "ADMINISTRATEUR" DU DOMAINE.**

## Configurations pour l'utilisateur TECH sur le SERVEUR2

### Explorateur de fichiers - Affichage - Options des dossiers

#### Onglet Affichage

- Sélectionner **Afficher les fichiers, dossiers et lecteurs cachés**
- Décocher **Masquer les extensions des fichiers dont le type est connu**
- Décocher **Masquer les fichiers protégés du système d'exploitation (recommandé)**
  - Il faut confirmer votre choix
- Cocher **Ouvrir les fenêtres des dossiers dans un processus différent**
- Décocher **Utiliser l'Assistant Partage (recommandé)**



### Gestionnaire de serveur - Serveur local

Dans les **Propriétés** de votre serveur

- Désactiver la **Configuration de sécurité renforcée d'Internet Explorer** pour les administrateurs
- Désactiver la **Configuration de sécurité renforcée d'Internet Explorer** pour les utilisateurs

### Vous devez installer au moins un des navigateurs web

Voici les liens pour télécharger les versions complètes de trois navigateurs

#### Chrome

<https://chromeenterprise.google/browser/download/#windows-tab>

#### Edge Chromium

<https://www.microsoft.com/en-us/edge/business/download>

#### Firefox

<https://www.mozilla.org/fr/firefox/all>

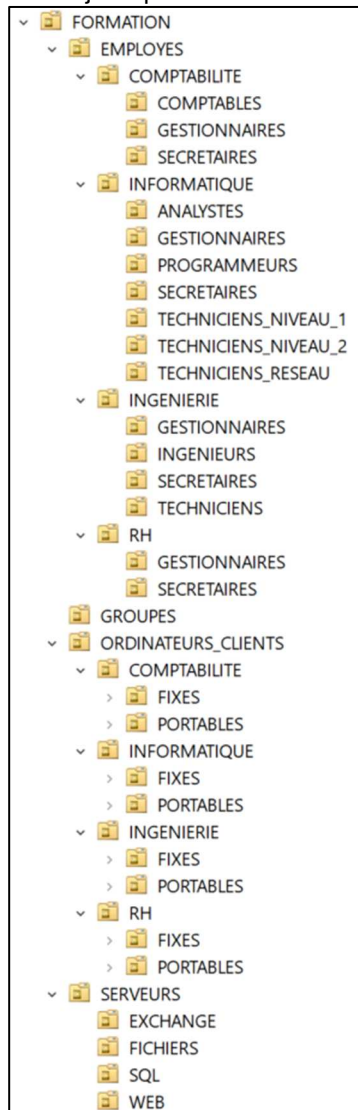
## Les propriétés des unités d'organisation dans l'Active Directory

### Objectifs

- Utiliser l'onglet "Éditeur d'attribut"
- Utiliser plusieurs attributs de l'objet "Unité d'organisation"

### Le but d'une unité d'organisation

Les objets qui seront administrés de la même manière devront être placés dans la même unité d'organisation.



- La conception d'UO aura une incidence sur le déploiement des stratégies de groupe.
- Il est important de ne pas mélanger les comptes utilisateurs et ordinateurs dans une même UO.
- Ne gardez pas les utilisateurs et les ordinateurs dans les conteneurs par défaut.
- Il est important d'activer le paramètre "Protéger le conteneur contre une suppression accidentelle".

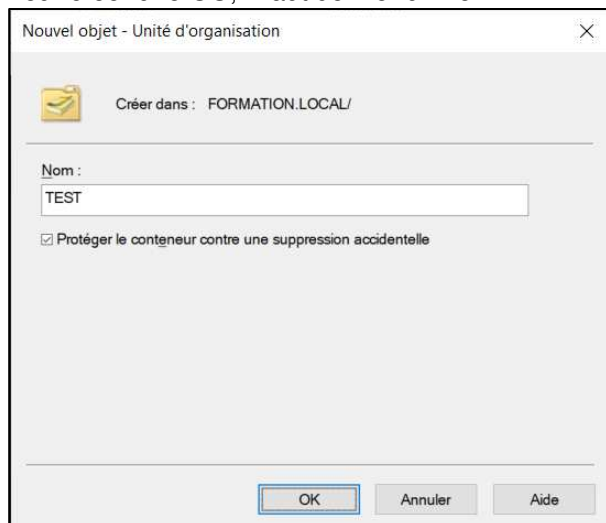
## Les attributs d'une unité d'organisation

Ouvrir la console "Utilisateurs et ordinateurs Active Directory" (UOAD)

- Vérifier que votre affichage est en "Fonctionnalités Avancées"

Sélectionner le domaine "FORMATION\LOCAL" et créer l'unité d'organisation "TEST".

Pour créer une OU, il faut donner un nom.



Nouvel objet - Unité d'organisation

Créer dans : FORMATION.LOCAL/

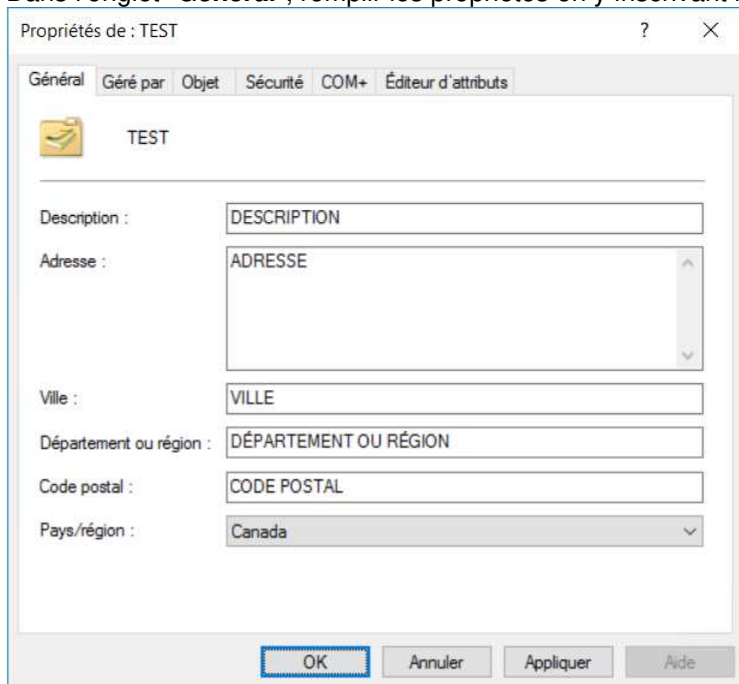
Nom :  
TEST

☒ Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

Par défaut, le paramètre "Protéger le conteneur contre une suppression accidentelle" est activé. Cliquer sur le bouton "OK"

Après la création de l'unité d'organisation "TEST", nous allons modifier les propriétés. Dans l'onglet "**Général**", remplir les propriétés en y inscrivant les valeurs suivantes.



Propriétés de : TEST

Général Géré par Objet Sécurité COM+ Éditeur d'attributs

TEST

Description : DESCRIPTION

Adresse : ADRESSE

Ville : VILLE

Département ou région : DÉPARTEMENT OU RÉGION

Code postal : CODE POSTAL

Pays/région : Canada

OK Annuler Appliquer Aide

Cliquer sur le bouton "**Filtrer**" et cocher "**Afficher uniquement les attributs ayant des valeurs**"  
En utilisant l'onglet "**Éditeur d'attributs**", trouvez le nom des attributs qui contiennent vos valeurs.

Propriétés de : TEST ? X

Général Géré par Objet Sécurité COM+ Éditeur d'attributs

Attributs :

| Attribut              | Valeur  |
|-----------------------|---|
| c                     | CA  |
| co                    | Canada  |
| countryCode           | 124   |
| description           | DESCRIPTION                                       |
| distinguishedName     | OU=TEST,DC=FORMATION,DC=LOCAL                     |
| dSCorePropagationData | 2021-05-29 11:59:25 Est; 2021-05-29 11:59:25 Est  |
| instanceType          | 0x4 = ( WRITE )                                   |
| l                     | VILLE   |
| name                  | TEST  |
| objectCategory        | CN=Organizational-Unit,CN=Schema,CN=Configuration |
| objectClass           | top; organizationalUnit                           |
| objectGUID            | be2fbf7f-cad2-45ce-b405-12260e58307b              |
| ou                    | TEST  |
| postalCode            | CODE POSTAL                                       |

Afficher Filtrer

OK Annuler Appliquer Aide

Propriétés de : TEST ? X

Général Géré par Objet Sécurité COM+ Éditeur d'attributs

Attributs :

| Attribut             | Valeur  |
|----------------------|---|
| name                 | TEST  |
| objectCategory       | CN=Organizational-Unit,CN=Schema,CN=Configuration |
| objectClass          | top; organizationalUnit                           |
| objectGUID           | be2fbf7f-cad2-45ce-b405-12260e58307b              |
| ou                   | TEST  |
| postalCode           | CODE POSTAL                                       |
| replPropertyMetaData | AttID Ver Loc.USN Org.DSA                         |
| st                   | DÉPARTEMENT OU RÉGION                             |
| street               | ADRESSE   |
| uSNChanged           | 24604   |
| uSNCreated           | 24600   |
| whenChanged          | 2021-05-29 12:12:30 Est                           |
| whenCreated          | 2021-05-29 11:59:25 Est                           |

Afficher Filtrer

OK Annuler Appliquer Aide

| Nom du champ dans l'onglet "Général" | Nom de l'attribut  |
|--------------------------------------|--|
| Description                          | <a href="#">description</a>  |
| Adresse                              | <a href="#">street</a>   |
| Ville                                | <a href="#"> </a>  |
| Département ou région                | <a href="#">st</a>   |
| Code postal                          | <a href="#">postalCode</a>   |
| Pays/région                          | <b>note: il y a trois attributs par pays</b><br><a href="#">c=CA</a><br><a href="#">co=Canada</a><br><a href="#">countryCode=124</a> |

Trouvez la valeur pour les attributs suivants:

| Nom de l'attribut | Valeur de l'attribut                          |
|-------------------|---|
| DistinguishedName | <a href="#">OU=TEST,DC=FORMATION,DC=LOCAL</a> |
| name              | <a href="#">test</a>                          |
| ou                | <a href="#">test</a>                          |
| WhenChanged       | <a href="#">2019-05-29 12:12:30 Est</a>       |
| WhenCreated       | <a href="#">2019-05-29 11:59:25 Est</a>       |

## Étape 2 - Programmation d'une unité d'organisation avec PowerShell ISE

Il existe 4 cmdlet spécifiques pour la gestion des unités d'organisation.

- Get-ADOrganizationalUnit
- New-ADOrganizationalUnit
- Remove-ADOrganizationalUnit
- Set-ADOrganizationalUnit

Avant de créer une unité d'organisation par programmation PowerShell, il faut faire le lien entre le nom des attributs dans l'Active Directory et le nom des propriétés dans PowerShell.

| Nom du champ dans l'onglet "Général" | Nom de la propriété dans PowerShell pour le cmdlet New-ADOrganizationalUnit  |
|--------------------------------------|--|
| Description                          | <a href="#">-Description</a>   |
| Adresse                              | <a href="#">-Street</a>  |
| Ville                                | <a href="#">-City</a>  |
| Département ou région                | <a href="#">-State</a>   |
| Code postal                          | <a href="#">-PostalCode</a>  |
| Pays/région                          | <a href="#">-Country</a><br><b>Il est préférable d'utiliser le paramètre -OtherAttributes avec les trois attributs c, co et countryCode.</b> |

Exemple de création d'une unité d'organisation avec PowerShell.

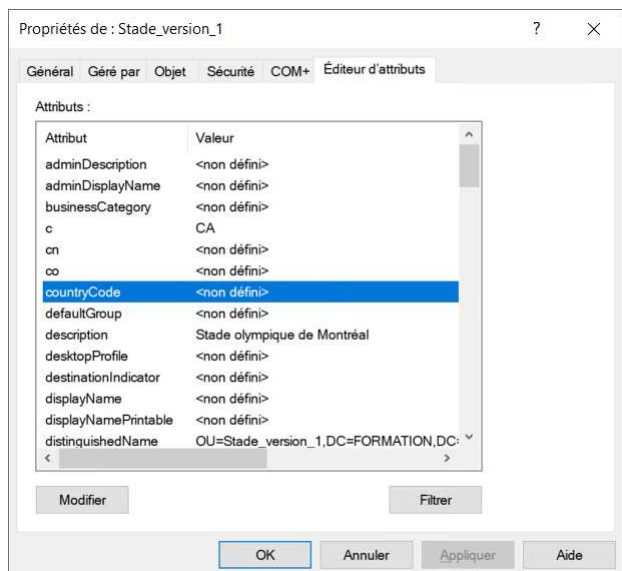
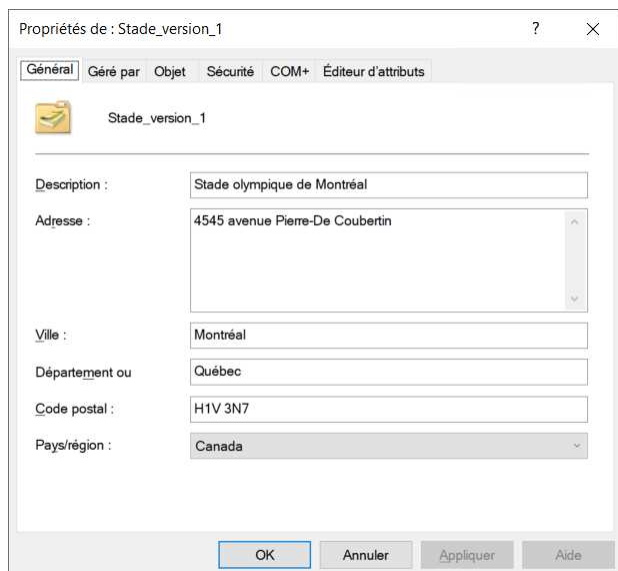
### Méthode avec le paramètre -Country

On veut créer l'unité organisationnelle "Stade\_version\_1" qui sera directement sous le domaine.

Le paramètre **-Path** utilise la valeur de l'attribut **DistinguishedName**

Pour le pays, nous utiliserons le paramètre **-Country**

```
New-ADOrganizationalUnit -Name "Stade_version_1" `
    -Path "DC=formation,DC=local" `
    -Description "Stade olympique de Montréal" `
    -street "4545 avenue Pierre-De Coubertin" `
    -City "Montréal" `
    -PostalCode "H1V 3N7" `
    -State "Québec" `
    -Country "CA" `
    -ProtectedFromAccidentalDeletion $false
```



Sur l'onglet "Général" le pays est Canada.

Sur l'onglet "Éditeur d'attributs", les attributs **co** et **countryCode** sont vides.

Le résultat final est différent de celui de l'environnement graphique.

**Malheureusement, le paramètre -Country configure seulement l'attribut c.**

Les attributs **co** et **countryCode** ne sont pas indispensables pour la fonctionnalité de base d'une unité d'organisation dans Active Directory.

Les attributs **co** et **countryCode** sont utiles pour les organisations multinationales qui veulent gérer les ressources par région.



### Méthode avec le paramètre -OtherAttributes

On veut créer l'unité organisationnelle "Stade\_version\_2" qui sera directement sous le domaine.

Le paramètre **-Path** utilise la valeur de l'attribut **DistinguishedName**

Pour le pays, nous utiliserons le paramètre **-OtherAttributes** avec les trois attributs **c**, **co** et **countryCode**

```
New-ADOrganizationalUnit -Name "Stade_version_2" `
    -Path "DC=formation,DC=local" `
    -Description "Stade olympique de Montréal" `
    -street "4545 avenue Pierre-De Coubertin" `
    -City "Montréal" `
    -PostalCode "H1V 3N7" `
    -State "Québec" `
    -OtherAttributes @{ 'c'="CA";
                        'co'="Canada";
                        'countryCode'="124" } `
    -ProtectedFromAccidentalDeletion $false
```

Propriétés de : Stade\_version\_2

Général | Géré par | Objet | Sécurité | COM+ | Éditeur d'attributs

Stade\_version\_2

Description : Stade olympique de Montréal

Adresse : 4545 avenue Pierre-De Coubertin

Ville : Montréal

Département ou : Québec

Code postal : H1V 3N7

Pays/région : Canada

OK Annuler Appliquer Aide

Propriétés de : Stade\_version\_2

Général | Géré par | Objet | Sécurité | COM+ | Éditeur d'attributs

Attributs :

| Attribut             | Valeur                              |
|----------------------|-------------------------------------|
| adminDescription     | <non défini>                        |
| adminDisplayName     | <non défini>                        |
| businessCategory     | <non défini>                        |
| c                    | CA                                  |
| cn                   | <non défini>                        |
| co                   | Canada                              |
| countryCode          | 124                                 |
| defaultGroup         | <non défini>                        |
| description          | Stade olympique de Montréal         |
| desktopProfile       | <non défini>                        |
| destinationIndicator | <non défini>                        |
| displayName          | <non défini>                        |
| displayNamePrintable | <non défini>                        |
| distinguishedName    | OU=Stade_version_2,DC=FORMATION,DC= |

Modifier Filtre

OK Annuler Appliquer Aide

Sur l'onglet "Général" le pays est Canada.

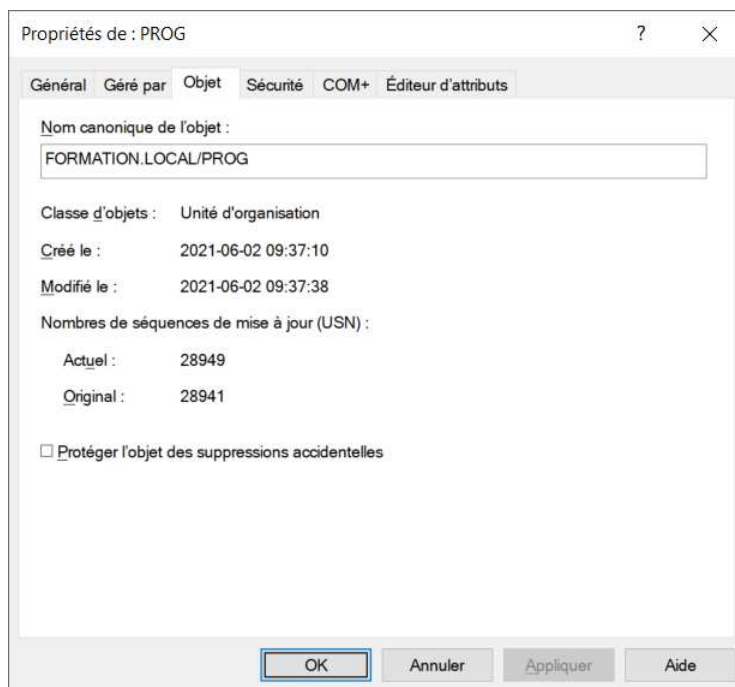
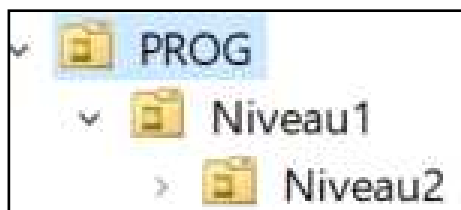
Sur l'onglet "Éditeur d'attributs" les attributs co et countryCode ont des valeurs.

Nous avons le même comportement que celui de l'environnement graphique.

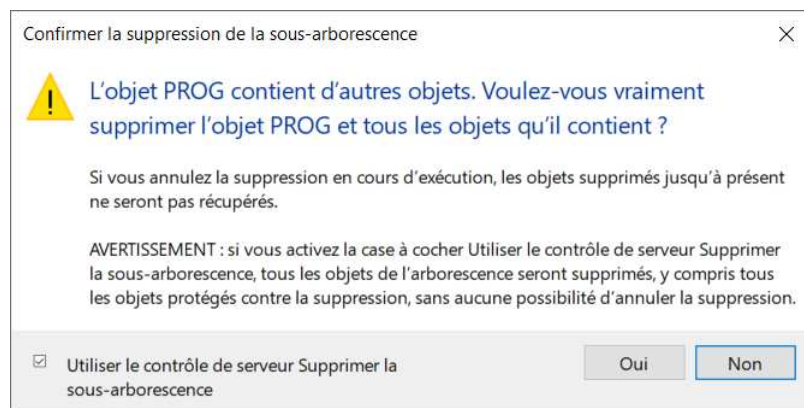
Conclusion: il est préférable d'utiliser le paramètre -OtherAttributes avec les trois attributs c, co et countryCode.

## Supprimer une unité d'organisation par l'environnement graphique

Pour supprimer une OU qui a une arborescence, il faut enlever le crochet "**Protéger l'objet des suppressions accidentelles**" sur la OU à supprimer.



Le nom canonique de l'objet correspond à l'attribut CanonicalName. L'attribut CanonicalName affiche le nom de l'objet du haut vers le bas, comme pour un dossier dans l'Explorateur de fichiers.



Pour supprimer l'arborescence de la OU, il faut cocher "**Utiliser le contrôle de serveur Supprimer la sous-arborescence**".

## Supprimer une unité d'organisation par programmation PowerShell

Pour supprimer une OU qui a une arborescence par programmation PowerShell.

Le paramètre **-Identity** utilise la valeur de l'attribut **DistinguishedName**

### # Enlève la protection contre la suppression accidentelle

```
Set-ADOrganizationalUnit -Identity "OU=prog,DC=formation,DC=local" `
    -ProtectedFromAccidentalDeletion $false
```

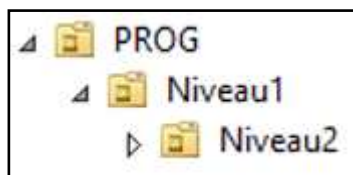
### # Pour supprimer l'unité d'organisation "PROG"

```
Remove-ADOrganizationalUnit -Identity "OU=prog,DC=formation,DC=local" `
    -Confirm:$false `
    -Recursive
```

Le paramètre **-Recursive** est obligatoire si l'unité d'organisation n'est pas vide.

## Exercice

En utilisant la console "PowerShell ISE", écrire un script pour créer la structure suivante directement sous le domaine. Inclure le code qui permet de détruire la structure si elle existe déjà.



Votre code doit utiliser **Remove-ADOrganizationalUnit** et **New-ADOrganizationalUnit** qui sont dans le module ActiveDirectory.

## Programmation d'une structure d'unité d'organisation

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectifs

- Utiliser un fichier CSV pour créer des unités d'organisation en utilisant PowerShell

### Description du travail

Écrire un programme en PowerShell qui créera une structure complexe de UO.  
La structure sera créée directement sous le domaine.

### Notes techniques

Pour créer les unités d'organisation, vous devez lire les données du fichier "UO\_FORMATION.CSV".

Vous devez ajouter des commentaires pertinents dans votre code.

Vous devez utiliser des variables.

Au début de votre programme, vous devez ajouter du code pour supprimer les unités d'organisation déjà existantes avant de les recréer.

Votre code doit utiliser un "Try and Catch" pour ne pas afficher les messages d'erreurs de PowerShell.  
Dans la section "Catch", vous devez utiliser le nom complet de l'erreur lorsqu'un objet de l'Active Directory n'existe pas.

La page 9 du fichier "**C53 - Introduction PowerShell - 3 de 5.docx**" montre comment trouver le nom des messages d'erreur.

À la fin du traitement, vous devez afficher le nombre d'unités d'organisation créées.

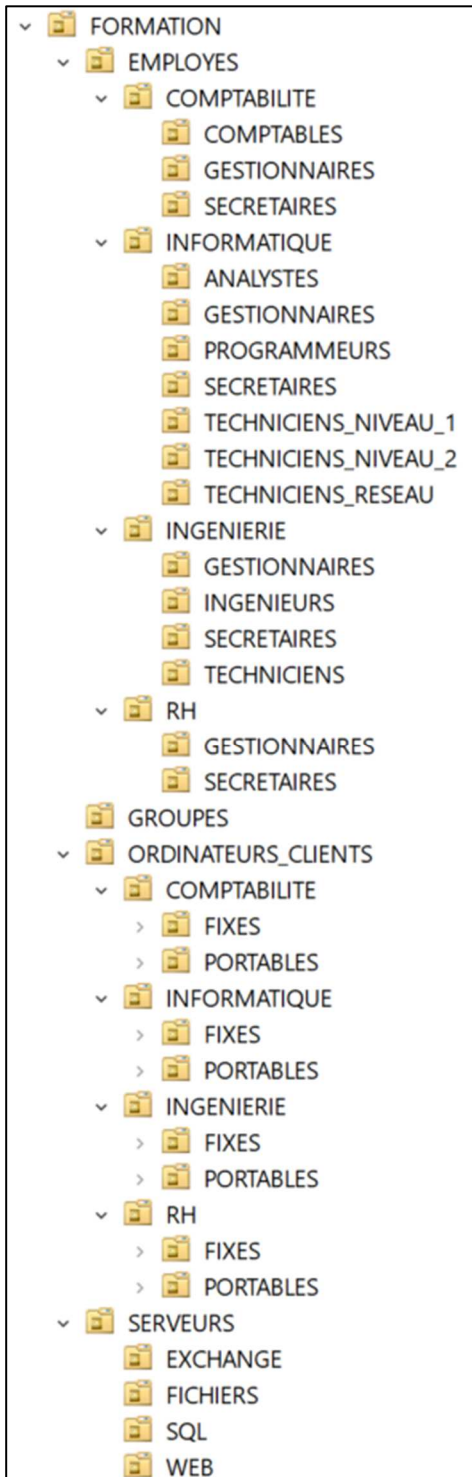
```
OU=FORMATION,DC=formation,DC=local n'existe pas.  
Création de 41 unités d'organisation.
```

```
OU=FORMATION,DC=formation,DC=local existe, donc on l'efface.  
Création de 41 unités d'organisation.
```

**Le module ActiveDirectory de PowerShell contient quatre cmdlets pour gérer les unités d'organisation.**

Get-ADOrganizationalUnit  
New-ADOrganizationalUnit  
Remove-ADOrganizationalUnit  
Set-ADOrganizationalUnit

**Voici la structure des 41 unités d'organisation**



## Informations sur les unités d'organisation de l'unité d'organisation FORMATION

### CanonicalName

-----  
FORMATION.LOCAL/FORMATION  
FORMATION.LOCAL/FORMATION/EMPLOYES  
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE  
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE/COMPTABLES  
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE/GESTIONNAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE/SECRETAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/ANALYSTES  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/GESTIONNAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/PROGRAMMEURS  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/SECRETAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/TECHNICIENS\_NIVEAU\_1  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/TECHNICIENS\_NIVEAU\_2  
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/TECHNICIENS\_RESEAU  
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE  
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/GESTIONNAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/INGENIEURS  
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/SECRETAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/TECHNICIENS  
FORMATION.LOCAL/FORMATION/EMPLOYES/RH  
FORMATION.LOCAL/FORMATION/EMPLOYES/RH/GESTIONNAIRES  
FORMATION.LOCAL/FORMATION/EMPLOYES/RH/SECRETAIRES  
FORMATION.LOCAL/FORMATION/GROUPES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/COMPTABILITE  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/COMPTABILITE/FIXES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/COMPTABILITE/PORTABLES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/INFORMATIQUE  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/INFORMATIQUE/FIXES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/INFORMATIQUE/PORTABLES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/INGENIERIE  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/INGENIERIE/FIXES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/INGENIERIE/PORTABLES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/RH  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/RH/FIXES  
FORMATION.LOCAL/FORMATION/ORDINATEURS\_CLIENTS/RH/PORTABLES  
FORMATION.LOCAL/FORMATION/SERVEURS  
FORMATION.LOCAL/FORMATION/SERVEURS/EXCHANGE  
FORMATION.LOCAL/FORMATION/SERVEURS/FICHIERS  
FORMATION.LOCAL/FORMATION/SERVEURS/SQL  
FORMATION.LOCAL/FORMATION/SERVEURS/WEB  
-----

## Informations sur les unités d'organisation de l'unité d'organisation FORMATION

### DistinguishedName

-----  
OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=COMPTABILITE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=COMPTABLES,OU=COMPTABILITE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=GESTIONNAIRES,OU=COMPTABILITE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=SECRETAIRES,OU=COMPTABILITE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=ANALYSTES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=GESTIONNAIRES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=PROGRAMMEURS,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=SECRETAIRES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=TECHNICIENS\_NIVEAU\_1,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=TECHNICIENS\_NIVEAU\_2,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=TECHNICIENS\_RESEAU,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=INGENIERIE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=GESTIONNAIRES,OU=INGENIERIE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=INGENIEURS,OU=INGENIERIE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=SECRETAIRES,OU=INGENIERIE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=TECHNICIENS,OU=INGENIERIE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=RH,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=GESTIONNAIRES,OU=RH,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=SECRETAIRES,OU=RH,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=COMPTABILITE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=FIXES,OU=COMPTABILITE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=PORTABLES,OU=COMPTABILITE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=INFORMATIQUE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=FIXES,OU=INFORMATIQUE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=PORTABLES,OU=INFORMATIQUE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=INGENIERIE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=FIXES,OU=INGENIERIE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=PORTABLES,OU=INGENIERIE,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=RH,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=FIXES,OU=RH,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=PORTABLES,OU=RH,OU=ORDINATEURS\_CLIENTS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=EXCHANGE,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=FICHIERS,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=SQL,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL  
-----

## Les propriétés des utilisateurs dans l'Active Directory

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectifs

- Utiliser l'onglet "Éditeur d'attribut"
- Comprendre la différence entre le nom des attributs et les paramètres des cmdlets

Site qui affiche la liste complète des attributs de l'Active Directory avec des explications pour chaque attribut.

#### Active Directory Schema

<https://docs.microsoft.com/en-us/windows/win32/adschema/attributes-all>

<https://docs.microsoft.com/fr-fr/windows/win32/adschema/attributes-all>

### Étape 1.1 - Les propriétés de bases d'un utilisateur

Ouvrir la console UOAD et vérifier que votre affichage est en "Fonctionnalités Avancées"

Dans l'unité d'organisation **TEST** qui est directement sous le domaine **FORMATION.LOCAL**

- Créer l'utilisateur en utilisant les paramètres
  - Prénom: **PRÉNOM**
  - Nom: **NOM**
  - Nom complet: **PRÉNOM NOM**
  - Nom d'ouverture de session de l'utilisateur: **test1@FORMATION.LOCAL**
  - Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000): **FORMATION\test1**
  - Mot de passe: **AAAAaa111**
  - Le mot de passe n'expire jamais

Nouvel objet - Utilisateur

Créer dans : FORMATION.LOCAL/TEST

Prénom : PRÉNOM Initiales :

Nom : NOM

Nom complet : PRÉNOM NOM

Nom d'ouverture de session de l'utilisateur :  
test1 @FORMATION.LOCAL

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :  
FORMATION\ test1

< Précédent Suivant > Annuler

Le nom de connexion de l'utilisateur (nom d'ouverture de session) doit être unique dans tout le domaine.



Nouvel objet - Utilisateur

Créer dans : FORMATION.LOCAL/TEST

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

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : FORMATION.LOCAL/TEST

Quand vous cliquerez sur Terminer, l'objet suivant sera créé :


Nom complet : PRÉNOM NOM

Nom de connexion de l'utilisateur : test1@FORMATION.LOCAL

Le mot de passe n'expire jamais.

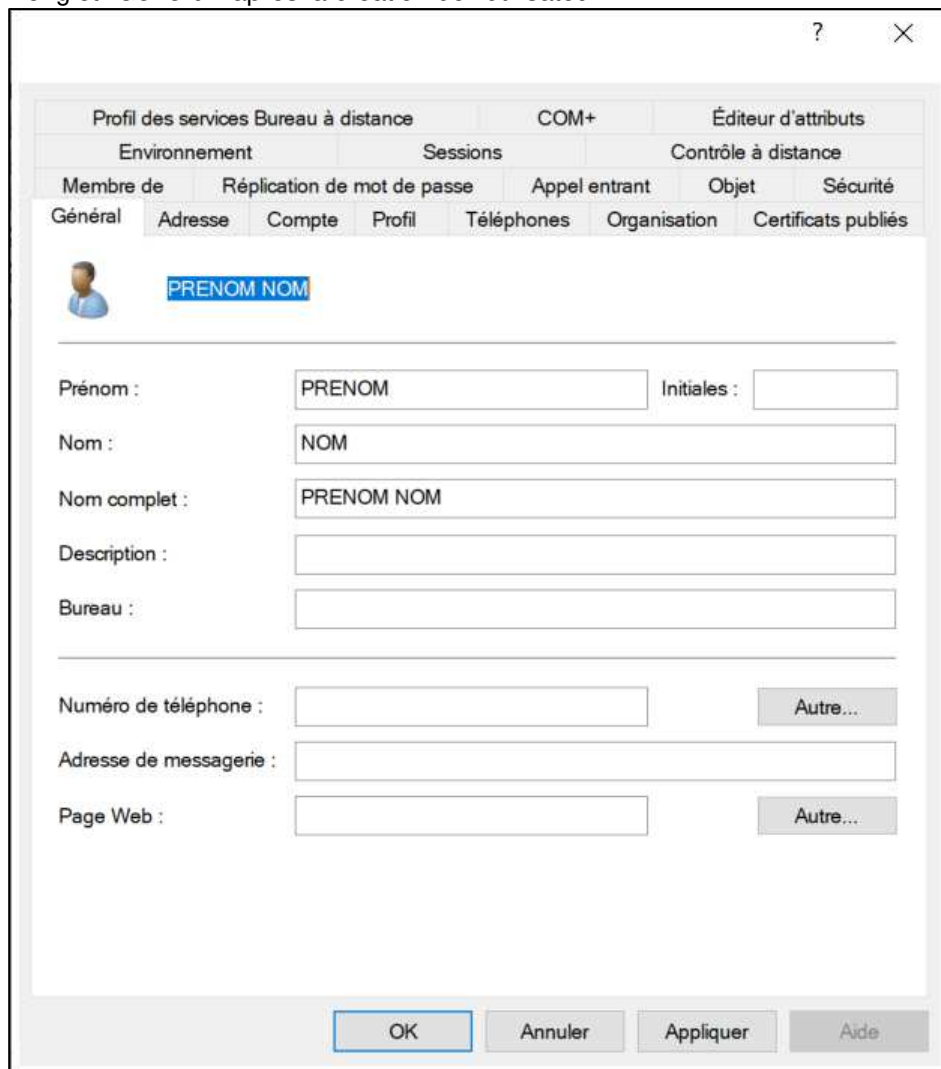
< Précédent Terminer Annuler

L'utilisateur est créé dans l'unité d'organisation "TEST"

| Nom  | Type        | Description |
|--|-------------|-------------|
|  PRÉNOM NOM | Utilisateur |             |

## Vérification de la configuration de l'utilisateur après sa création

L'onglet "Général" après la création de l'utilisateur



The screenshot shows a window titled "Général" with a tabbed interface. The tabs include: Profil des services Bureau à distance, COM+, Éditeur d'attributs, Environnement, Sessions, Contrôle à distance, Membre de, Réplication de mot de passe, Appel entrant, Objet, Sécurité, and Général (selected). The "Général" tab contains a user profile section with a placeholder image and the text "PRENOM NOM". Below this are several input fields: "Prénom :" (containing "PRENOM"), "Initiales :" (empty), "Nom :" (containing "NOM"), "Nom complet :" (containing "PRENOM NOM"), "Description :" (empty), and "Bureau :" (empty). Further down are "Numéro de téléphone :" (empty), "Adresse de messagerie :" (empty), and "Page Web :" (empty). Each of these three fields has an "Autre..." button next to it. At the bottom of the window are four buttons: "OK", "Annuler", "Appliquer", and "Aide".

L'onglet "**Compte**" après la création de l'utilisateur

Propriétés de : PRÉNOM NOM

Membre de   Réplication de mot de passe   Appel entrant   Objet   Sécurité

Environnement   Sessions   Contrôle à distance

Profil des services Bureau à distance   COM+   Éditeur d'attributs

Général   Adresse   **Compte**   Profil   Téléphones   Organisation   Certificats publiés

Nom d'ouverture de session de l'utilisateur :

test1   @FORMATION.LOCAL

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

FORMATION\   test1

Horaires d'accès...   Se connecter à...

☐ Déverrouiller le compte

Options de compte :

- ☐ L'utilisateur ne peut pas changer de mot de passe
- ☒ Le mot de passe n'expire jamais
- ☐ Enregistrer le mot de passe en utilisant un chiffrement réversible
- ☐ Le compte est désactivé

Date d'expiration du compte

☒ Jamais

☐ Fin de : 7 mars 2023

OK   Annuler   Appliquer   Aide

**"Date d'expiration du compte"** Par défaut, le compte d'un utilisateur n'expire jamais.

**"Horaire d'accès..."**

Par défaut, un utilisateur n'a pas de restriction pour les heures d'accès.

Horaire d'accès pour PRÉNOM NOM

0 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 0

Tous

dimanche

lundi

mardi

mercredi

jeudi

vendredi

samedi

OK

Annuler

☒ Ouverture de session autorisée

☐ Ouverture de session refusée

Du dimanche au samedi, de 00:00 à 00:00

**"Se connecter à..."**

Par défaut, un utilisateur peut ouvrir une session sur tous les ordinateurs.

Stations de travail accessibles ? X

Dans le champ Nom de l'ordinateur, mettez le nom du NetBIOS de l'ordinateur ou de son DNS.

Cet utilisateur peut ouvrir une session sur :

☒ Tous les ordinateurs

☐ Les ordinateurs suivants

Nom de l'ordinateur :

Ajouter

Modifier

Supprimer

OK

Annuler

**Vérification des attributs lorsqu'un utilisateur est créé avec la console UOAD.**

En utilisant l'onglet "Éditeur d'attributs", trouvez le nom des attributs qui contiennent vos valeurs.  
note: cliquer sur le bouton "Filtrer" et cocher "Afficher uniquement les attributs ayant des valeurs"

| Attribut              | Valeur                         |
|-----------------------|--------------------------------|
| accountExpires        | (jamais)                       |
| badPasswordTime       | (jamais)                       |
| badPwdCount           | 0                              |
| cn                    | PRÉNOM NOM                     |
| codePage              | 0                              |
| countryCode           | 0                              |
| displayName           | PRÉNOM NOM                     |
| distinguishedName     | CN=PRÉNOM NOM,OU=TEST,DC=FORMA |
| dSCorePropagationD... | 0x0 = ( )                      |
| givenName             | PRÉNOM                         |
| instanceType          | 0x4 = ( WRITE )                |
| lastLogoff            | (jamais)                       |
| lastLogon             | (jamais)                       |
| logonCount            | 0                              |

cn PRÉNOM NOM  
displayName PRÉNOM NOM  
distinguishedName CN=PRÉNOM NOM,OU=TEST,DC=FORMATION,DC=LOCAL  
givenName PRÉNOM

Lors de la création d'un utilisateur en utilisant l'environnement graphique.

**L'attribut "CN" contient le nom complet de l'utilisateur.**

**L'attribut "CN" est unique dans une unité d'organisation.**

**L'attribut "distinguishedName" est unique dans le domaine.**

**L'attribut "distinguishedName" débute par l'attribut "CN".**

Pour être capable de créer un utilisateur qui a le même prénom et le même nom qu'un autre utilisateur qui est dans la même unité d'organisation, il faut simplement modifier le nom complet.

Propriétés de : PRÉNOM NOM

Membre de    Réplication de mot de passe    Appel entrant    Objet    Sécurité

Environnement    Sessions    Contrôle à distance

Général    Adresse    Compte    Profil    Téléphones    Organisation    Certificats publiés

Profil des services Bureau à distance    COM+    Éditeur d'attributs

Attributs :

| Attribut             | Valeur                                  |
|----------------------|---|
| logonCount           | 0                                       |
| name                 | PRÉNOM NOM                              |
| objectCategory       | CN=Person,CN=Schema,CN=Configuration,   |
| objectClass          | top; person; organizationalPerson; user |
| objectGUID           | 1a6f1750-4231-43e3-bb40-de20c9505889    |
| objectSid            | S-1-5-21-3523712887-290544647-17807520  |
| primaryGroupID       | 513 = ( GROUP_RID_USERS )               |
| pwdLastSet           | 2021-06-03 11:27:06 Est                 |
| replPropertyMetaData | AttID Ver Loc.USN Org.DSA               |
| sAMAccountName       | test1                                   |
| sAMAccountType       | 805306368 = ( NORMAL_USER_ACCOUNT       |
| sn                   | NOM                                     |
| userAccountControl   | 0x10200 = ( NORMAL_ACCOUNT   DONT_      |
| userPrincipalName    | test1@FORMATION.LOCAL                   |

< >

Modifier    Filtrer

OK    Annuler    Appliquer    Aide

name                      PRÉNOM NOM  
sAMAccountName        test1  
sn                        NOM  
userPrincipalName      test1@FORMATION.LOCAL

L'attribut "name" correspond au nom du compte de l'utilisateur.

Lors de la création d'un utilisateur en utilisant l'environnement graphique l'attribut "sAMAccountName" contient le nom d'ouverture de session (antérieur à Windows 2000) de l'utilisateur.

| Nom du champ<br>lors de la création de l'utilisateur                      | Nom de l'attribut |
|---|-------------------|
| Prénom  | givenName         |
| Nom   | sn                |
| Nom Complet   | displayName       |
| Nom d'ouverture de session de l'utilisateur                               | userPrincipalName |
| Nom d'ouverture de session de l'utilisateur<br>(antérieur à Windows 2000) | sAMAccountName    |

### Vérification des attributs par programmation PowerShell

Voici la commande PowerShell qui affiche la liste des attributs qui correspondent aux propriétés de bases lorsqu'un utilisateur est créé avec la console UOAD.

```
Get-ADuser -Identity test1 `
    -Properties * | `
    Select-Object CN,DisplayName,DistinguishedName,GivenName,
        Name,SamAccountName,sn,UserPrincipalName
```

```
CN                : PRÉNOM NOM
DisplayName        : PRÉNOM NOM
DistinguishedName  : CN=PRÉNOM NOM,OU=TEST,DC=FORMATION,DC=LOCAL
GivenName         : PRÉNOM
Name              : PRÉNOM NOM
SamAccountName     : test1
sn                : NOM
UserPrincipalName  : test1@FORMATION.LOCAL
```

## Étape 1.2 - Programmation d'un utilisateur avec PowerShell ISE

Il existe 4 cmdlet spécifiques pour la gestion des utilisateurs de l'Active Directory.

- Get-ADUser
- New-ADUser
- Remove-ADUser
- Set-ADUser

| Nom du champ<br>lors de la création de l'utilisateur                      | Nom de la propriété dans PowerShell<br>pour le cmdlet New-ADUser |
|---|--|
| Prénom  | -GivenName   |
| Nom   | -Surname   |
| Nom Complet   | -DisplayName   |
| Nom d'ouverture de session de l'utilisateur                               | -UserPrincipalName   |
| Nom d'ouverture de session de l'utilisateur<br>(antérieur à Windows 2000) | -SamAccountName  |

Exemple de création d'un utilisateur avec PowerShell.

```
# Supprime l'utilisateur test1 sans aucune confirmation
Remove-ADUser -Identity test1 `
    -Confirm:$false
```

```
$mdp = ConvertTo-SecureString -AsPlainText "AAAAaa111" -Force
```


```
PS E:\> $mdp = ConvertTo-SecureString -AsPlainText "AAAAaa111" -Force
PS E:\> $mdp
System.Security.SecureString

PS E:\> $mdp | ConvertFrom-SecureString
01000000d08c9ddf0115d1118c7a00c04fc297eb0100000020b34493f2a76e478acce7dacc07087a00000000200000000010660000000100002
000000079186dd1da767d78b0007356096ebb3f94d14c65e093db376dfcb8f215fbbc7f000000000e8000000002000020000000ba0a42e3eb04c0
4fe739f2df04d2722174cfd65d63950b07c56f3060c8264c612000000067d1e3b37876151a18967ed8de9015d894d4fae8b4e8d76da3d126a1a38
106884000000081dcedcf7b/a217cc26dca1e51a47382ce4ee2529a416ceb025ad0646c352e4dcd202621731e2ce8681f96462082f6b5d45ec752
a9a03f11dbffd9db0b64abb1

PS E:\>
```

```
# Ce code permet de recréer l'utilisateur test1 avec les mêmes propriétés qu'à l'étape 1.1.
New-ADUser -Name "PRÉNOM NOM" `
    -SamAccountName test1 `
    -UserPrincipalName "test1@formation.local" `
    -Path "OU=TEST,DC=FORMATION,DC=LOCAL" `
    -GivenName "PRÉNOM" `
    -Surname "NOM" `
    -DisplayName "PRÉNOM NOM" `
    -AccountPassword $mdp `
    -PasswordNeverExpires $true `
    -Enabled $true
```

L'utilisateur est créé dans l'unité d'organisation "TEST"

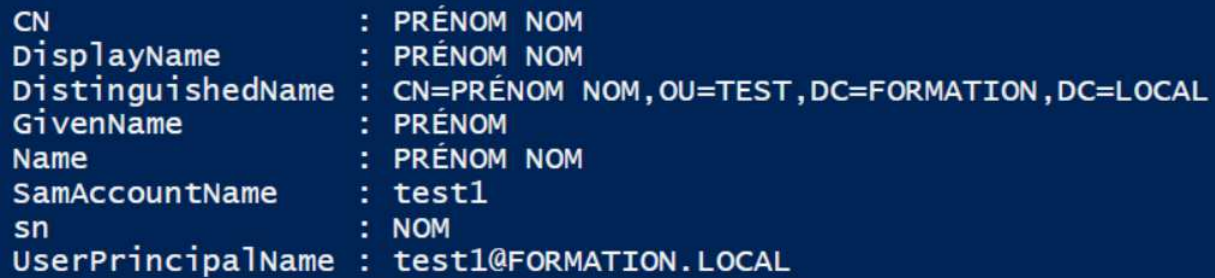
| Nom  | Type        | Description |
|--|-------------|-------------|
|  PRÉNOM NOM | Utilisateur |             |

Le résultat final semble identique.



### Vérification des attribututs par programmation PowerShell

```
Get-ADuser -Identity test1 `
    -Properties * | `
    Select-Object CN, DisplayName, DistinguishedName, GivenName,
        Name, SamAccountName, sn, UserPrincipalName
```



```
CN                : PRÉNOM NOM
DisplayName        : PRÉNOM NOM
DistinguishedName : CN=PRÉNOM NOM, OU=TEST, DC=FORMATION, DC=LOCAL
GivenName         : PRÉNOM
Name              : PRÉNOM NOM
SamAccountName     : test1
sn                : NOM
UserPrincipalName  : test1@FORMATION.LOCAL
```

Les attributs sont identiques à ceux dont l'utilisateur a été créé avec la console UOAD.

Lors de la création d'un utilisateur dans l'Active Directory avec la commande New-ADUser, vous devez vous assurer de configurer correctement les paramètres **-Name**, **-SamAccountName** et **-UserPrincipalName**.


Le paramètre **-Name** est obligatoire.

## Étape 2.1 - Les attributs d'un utilisateur dans l'onglet "Général"

Dans l'onglet "Général", remplir les propriétés en y inscrivant les valeurs suivantes:

Propriétés de : PRÉNOM NOM ? X

|                                       |                             |                     |                     |            |
|---------------------------------------|-----------------------------|---------------------|---------------------|------------|
| Membre de                             | Réplication de mot de passe | Appel entrant       | Objet               | Sécurité   |
| Environnement                         | Sessions                    | Contrôle à distance |                     |            |
| Profil des services Bureau à distance |                             | COM+                | Éditeur d'attributs |            |
| Général                               | Adresse                     | Compte              | Profil              | Téléphones |
| Organisation                          | Certificats publiés         |                     |                     |            |

 PRÉNOM NOM

---

Prénom : PRÉNOM      Initiales :

Nom : NOM

Nom complet : PRÉNOM NOM

Description : DESCRIPTION

Bureau : BUREAU

---

Numéro de téléphone : 514-111-1111     

Adresse de messagerie : test1@courriel.local

Page Web : www.pageweb.local

Numéro de téléphone (Autres) ? X

Nouvelle valeur :

Ajouter

Valeurs actuelles :

514-111-2222

514-333-4444

Modifier

Supprimer

OK Annuler

Ajouter des numéros de téléphones

Adresse de page Web (Autres) ? X

Nouvelle valeur :

Ajouter

Valeurs actuelles :

www.info.local

www.support.local

Modifier

Supprimer

OK Annuler

Ajouter des pages web

En utilisant l'onglet "Éditeur d'attributs", trouvez le nom des attributs qui contiennent vos valeurs.  
note: cliquer sur le bouton "Filtrer" et cocher "Afficher uniquement les attributs ayant des valeurs"

| Nom du champ<br>dans l'onglet "Général" | Nom de l'attribut   |
|---|---|
| Prénom                                  | <a href="#">givenName</a>   |
| Nom                                     | <a href="#">sn</a>  |
| Nom complet                             | <a href="#">displayName</a>                                       |
| Description                             | <a href="#">description</a>                                       |
| Bureau                                  | <a href="#">physicalDeliveryOfficeName</a>                        |
| Numéro de telephone<br>Autre...         | <a href="#">telephoneNumber</a><br><a href="#">otherTelephone</a> |
| Adresse de messagerie                   | <a href="#">mail</a>  |
| Page Web<br>Autre...                    | <a href="#">wWWHomePage</a><br><a href="#">url</a>                |

## Étape 2.2 - Programmation d'un utilisateur avec PowerShell ISE

Il existe 4 cmdlet spécifiques pour la gestion des utilisateurs de l'Active Directory.

- Get-ADUser
- New-ADUser
- Remove-ADUser
- Set-ADUser

| Nom du champ dans l'onglet "Général" | Nom de la propriété dans PowerShell pour le cmdlet New-ADUser                  |
|--------------------------------------|--|
| Prénom                               | -GivenName   |
| Nom                                  | -Surname   |
| Nom complet                          | -DisplayName   |
| Description                          | -Description   |
| Bureau                               | -Office  |
| Numéro de telephone                  | -OfficePhone   |
| Autre...                             | Il faut utiliser le paramètre -OtherAttributes avec l'attribut otherTelephone. |
| Adresse de messagerie                | -EmailAddress  |
| Page Web                             | -HomePage  |
| Autre...                             | Il faut utiliser le paramètre -OtherAttributes avec l'attribut url.            |

Exemple de création d'un utilisateur avec PowerShell.

```
# Permet de recréer l'utilisateur test1
# avec les mêmes propriétés qu'à l'étape 1.1 (rouge sur fond jaune)
# et avec les propriétés de l'étape 2.1 (rouge sur fond noir)
Remove-ADUser -Identity test1 `
    -Confirm:$false

$mdp = ConvertTo-SecureString -AsPlainText "AAAAaa111" -Force

New-ADUser -Name "PRÉNOM NOM" `
    -SamAccountName test1 `
    -UserPrincipalName "test1@formation.local" `
    -Path "OU=TEST,DC=FORMATION,DC=LOCAL" `
    -GivenName "PRÉNOM" `
    -Surname "NOM" `
    -DisplayName "PRÉNOM NOM" `
    -Description "DESCRIPTION" `
    -Office "BUREAU" `
    -OfficePhone "514-111-1111" `
    -EmailAddress "test1@courriel.local" `
    -HomePage "www.pageweb.local" `
    -OtherAttributes @{ 'otherTelephone'="514-111-2222","514-333-4444";
        'url'="www.info.local","www.support.local"} `
    -AccountPassword $mdp `
    -PasswordNeverExpires $true `
    -Enabled $true
```

### Étape 3.1 - Les attributs d'un utilisateur dans l'onglet "Adresse"

Dans l'onglet "Adresse", remplir les propriétés en y inscrivant les valeurs suivantes:

Propriétés de : PRÉNOM NOM ? X

|                                       |                             |                     |                     |            |
|---------------------------------------|-----------------------------|---------------------|---------------------|------------|
| Membre de                             | Réplication de mot de passe | Appel entrant       | Objet               | Sécurité   |
| Environnement                         | Sessions                    | Contrôle à distance |                     |            |
| Profil des services Bureau à distance |                             | COM+                | Éditeur d'attributs |            |
| Général                               | Adresse                     | Compte              | Profil              | Téléphones |
|                                       |                             | Organisation        | Certificats publiés |            |

Adresse : ADRESSE

Boîte postale : BOITE POSTALE

Ville : VILLE

Département ou DÉPARTEMENT OU RÉGION

Code postal : CODE POSTAL

Pays/région : Canada

OK Annuler Appliquer Aide

En utilisant l'onglet "Éditeur d'attributs", trouvez le nom des attributs qui contiennent vos valeurs.  
note: cliquer sur le bouton "Filtrer" et cocher "Afficher uniquement les attributs ayant des valeurs"

| Nom du champ dans l'onglet "Adresse" | Nom de l'attribut  |
|--------------------------------------|--|
| Adresse                              | streetAddress  |
| Boîte postale                        | postOfficeBox  |
| Ville                                |  |
| Département ou région                | st   |
| Code postal                          | postalCode   |
| Pays/région                          | <b>note: il y a trois attributs par pays</b><br>c=CA<br>co=Canada<br>countryCode=124 |

### Étape 3.2 - Programmation d'un utilisateur avec PowerShell ISE

Il existe 4 cmdlet spécifiques pour la gestion des utilisateurs de l'Active Directory.

- Get-ADUser
- New-ADUser
- Remove-ADUser
- Set-ADUser

| Nom du champ dans l'onglet "Adresse" | Nom de la propriété dans PowerShell pour le cmdlet New-ADUser  |
|--------------------------------------|--|
| Adresse                              | -StreetAddress   |
| Boîte postale                        | -POBox   |
| Ville                                | -City  |
| Département ou région                | -State   |
| Code postal                          | -PostalCode  |
| Pays/région                          | -Country<br><br><b>Il est préférable d'utiliser le paramètre -OtherAttributes avec les trois attributs c, co et countryCode.</b> |

**Exemple pour configurer le pays avec le paramètre -OtherAttributes**

**-OtherAttributes @{'c'="CA"; 'co'="Canada"; 'countryCode'="124"}**

## Étape 4.1 - Les attributs d'un utilisateur dans l'onglet "Téléphones"

Dans l'onglet "Téléphones", remplir les propriétés en y inscrivant les valeurs suivantes:

Propriétés de : PRÉNOM NOM ? X

|                                       |                             |                     |                     |            |
|---------------------------------------|-----------------------------|---------------------|---------------------|------------|
| Membre de                             | Réplication de mot de passe | Appel entrant       | Objet               | Sécurité   |
| Environnement                         | Sessions                    | Contrôle à distance |                     |            |
| Profil des services Bureau à distance |                             | COM+                | Éditeur d'attributs |            |
| Général                               | Adresse                     | Compte              | Profil              | Téléphones |
| Organisation                          |                             | Certificats publiés |                     |            |

Numéros de téléphone

|                   |              |           |
|-------------------|--------------|-----------|
| Domicile :        | 514-222-2222 | Autres... |
| Radiomessagerie : | 514-333-3333 | Autres... |
| Tél. mobile :     | 514-444-4444 | Autres... |
| Télécopie :       | 514-555-5555 | Autres... |
| Téléphone IP :    | 514-666-6666 | Autres... |

Remarques :

REMARQUES

OK Annuler Appliquer Aide

En utilisant l'onglet "Éditeur d'attributs", trouvez le nom des attributs qui contiennent vos valeurs.  
note: cliquer sur le bouton "Filtrer" et cocher "Afficher uniquement les attributs ayant des valeurs"

| Nom du champ<br>dans l'onglet "Téléphones" | Nom de l'attribut   |
|--|---|
| Domicile<br>Autres...                      | homePhone<br>otherHomePhone                               |
| Radiomessagerie<br>Autres...               | pager<br>otherPager                                       |
| Tél. mobile<br>Autres...                   | mobile<br>otherMobile                                     |
| Télécopie<br>Autres...                     | facsimileTelephoneNumber<br>otherFacsimileTelephoneNumber |
| Téléphone IP<br>Autres...                  | ipPhone<br>otherIpPhone                                   |
| Remarques                                  | info  |

## Étape 4.2 - Programmation d'un utilisateur avec PowerShell ISE

Il existe 4 cmdlet spécifiques pour la gestion des utilisateurs de l'Active Directory.

- Get-ADUser
- New-ADUser
- Remove-ADUser
- Set-ADUser

| Nom du champ<br>dans l'onglet "Téléphones" | Nom de la propriété dans PowerShell<br>pour le cmdlet New-ADUser  |
|--|---|
| Domicile<br>Autres...                      | -HomePhone<br><br>Il faut utiliser le paramètre -OtherAttributes avec l'attribut otherHomePhone.  |
| Radiomessagerie<br>Autres...               | Il faut utiliser le paramètre -OtherAttributes avec l'attribut Pager.<br><br>Il faut utiliser le paramètre -OtherAttributes avec l'attribut otherPager. |
| Tél. mobile<br>Autres...                   | -MobilePhone<br><br>Il faut utiliser le paramètre -OtherAttributes avec l'attribut otherMobile.   |
| Télécopie<br>Autres...                     | -Fax<br><br>Il faut utiliser le paramètre -OtherAttributes avec l'attribut otherFacsimileTelephoneNumber.   |
| Téléphone IP<br>Autres...                  | ipPhone<br><br>Il faut utiliser le paramètre -OtherAttributes avec l'attribut otherIpPhone.   |
| Remarques                                  | Il faut utiliser le paramètre -OtherAttributes avec l'attribut info.  |



## Étape 5 - Autres attributs d'un utilisateur

Trouvez les valeurs des attributs suivants pour l'utilisateur TECH

| Nom de l'attribut  | Valeur de l'attribut                           |
|--------------------|--|
| accountExpires     | (jamais)                                       |
| badPasswordTime    | (jamais)                                       |
| badPwdCount        | 0  |
| DistinguishedName  | CN=Richard Jean,CN=users,DC=formation,DC=local |
| lastLogoff         | (jamais)                                       |
| lastLogon          | 2021-06-03 21:36:22 Est                        |
| lastLogonTimestamp | 2021-06-01 09:44:58 Est                        |
| logonCount         | 7  |
| pwdLastSet         | 2020-06-01 09:37:46 Est                        |
| UserAccountControl | 0x10200 (NORMAL_ACCOUNT DONT_EXPIRE_PASSWORD)  |
| WhenChanged        | 2020-06-01 09:53:13 Est                        |
| WhenCreated        | 2020-06-01 09:37:45 Est                        |

**accountExpires** La date d'expiration du compte  
**lastLogoff** C'est un attribut que Microsoft n'a jamais utilisé.  
**logonCount** Le nombre de fois que l'utilisateur s'est connecté avec succès.

### accountExpires

accountExpires est un entier qui représente le nombre de 100 nano secondes depuis le 1601/01/01 (UTC).

Si la valeur de **accountExpires** correspond à **0** ou **9223372036854775807** alors le compte n'expire jamais.  
**9223372036854775807** correspond à la valeur hexadécimale **0x7FFFFFFFFFFFFFFF**

```
[int64]::MaxValue = 9223372036854775807
```

### lastLogon

Cet attribut n'est jamais répliqué, ce qui veut dire que sa valeur est spécifique à chaque contrôleur de domaine.  
LastLogon est un entier qui représente le nombre de 100 nanosecondes depuis le 1601/01/01 (UTC).

### lastLogonTimeStamp

Cet attribut est répliqué sur chaque contrôleur de domaine mais seulement dans un intervalle de 9 à 14 jours.  
LastLogonTimeStamp est un entier qui représente le nombre de 100 nano secondes depuis le 1601/01/01 (UTC).

### Exemple avec LastLogon

```
Get-ADUser -Identity TECH `
    -Properties accountExpires,LastLogon,LastLogonDate,LastLogonTimeStamp
```

```
accountExpires      : 9223372036854775807
DistinguishedName   : CN=Richard Jean,CN=Users,DC=FORMATION,DC=LOCAL
Enabled             : True
GivenName           : Richard
LastLogon           : 132672441821805799
LastLogonDate       : 1 juin 2021 09:44:58
LastLogonTimeStamp  : 132670286986966976
Name                : Richard Jean
ObjectClass         : user
ObjectGUID          : 58aae375-36dd-432e-b2c6-20395ad28cb1
SamAccountName      : TECH
SID                 : S-1-5-21-3523712887-290544647-1780752054-1104
Surname             : Jean
UserPrincipalName   : TECH@FORMATION.LOCAL
```

```
# Avec PowerShell, permet de convertir la valeur qui correspond au LastLogon
[DateTime]::FromFileTime(132672441821805799)
```

3 juin 2021 21:36:22

```
# Avec PowerShell, permet de convertir la valeur qui correspond au
LastLogonTimeStamp
[DateTime]::FromFileTime(132670286986966976)
```

1 juin 2021 09:44:58

LastLogonDate correspond à la date de LastLogonTimeStamp.

---

```
Get-ADUser -Identity TECH `
    -Properties * | `
    Select-Object Name,accountExpires,LastLogonTimeStamp,LastLogon,
        @{label='accountExpires - DATE';
            expression={if ( ($PSItem.accountExpires -eq 0) -or
                            ($PSItem.accountExpires -eq 9223372036854775807) )
                {
                    Write-Output "JAMAIS"
                }
                else
                {
                    [DateTime]::FromFileTime($PSItem.accountExpires)
                }
            },
        @{label='LastLogonTimeStamp - DATE';
            expression={ [DateTime]::FromFileTime($PSItem.LastLogonTimeStamp) }
        },
        @{label='LastLogon - DATE';
            expression={ [DateTime]::FromFileTime($PSItem.LastLogon) }
        }
```

## ANNEXE

### L'attribut UserAccountControl

Ce tableau présente les différentes valeurs de l'attribut **UserAccountControl**.  
Les valeurs sont cumulatives.

| Nom de la constante pour la valeur | Valeur hexadécimale | Explication de la valeur   |
|------------------------------------|---------------------|--|
| SCRIPT                             | 0x1                 | Exécution du script d'ouverture de session   |
| ACCOUNTDISABLE                     | 0x2                 | Désactivation du compte utilisateur  |
| HOMEDIR_REQUIRED                   | 0x8                 | Dossier de base requis   |
| LOCKOUT                            | 0x10                | Aucun mot de passe n'est requis.   |
| PASSWD_NOTREQD                     | 0x20                | Vous pouvez lire cette valeur, mais vous ne pouvez pas la définir directement.   |
| PASSWD_CANT_CHANGE                 | 0x40                | Impossible de modifier le mot de passe.  |
| ENCRYPTED_TEXT_PWD_ALLOWED         | 0x80                | L'utilisateur peut envoyer un message crypté.  |
| TEMP_DUPLICATE_ACCOUNT             | 0x100               | Compte pour les utilisateurs dont le compte principal se trouve dans un autre domaine. Ce compte fournit l'accès à ce domaine, mais pas à tous les domaines qui ont des relations d'approbation avec ce domaine. Il est parfois appelé compte utilisateur local. |
| NORMAL_ACCOUNT                     | 0x200               | Type de compte par défaut représentant un utilisateur  |
| INTERDOMAIN_TRUST_ACCOUNT          | 0x800               | Autorisation d'approuver un compte pour un domaine du système qui a des relations d'approbation avec d'autres domaines.  |
| WORKSTATION_TRUST_ACCOUNT          | 0x1000              | Compte d'ordinateur  |
| SERVER_TRUST_ACCOUNT               | 0x2000              | Compte d'ordinateur d'un contrôleur de domaine membre de ce domaine.   |
| DONT_EXPIRE_PASSWORD               | 0x10000             | Représente le mot de passe, qui ne doit jamais expirer pour le compte.   |
| MNS_LOGON_ACCOUNT                  | 0x20000             | Compte d'ouverture de session de jeu de nœuds majoritaire.   |
| SMARTCARD_REQUIRED                 | 0x40000             | Cette valeur force l'utilisateur à ouvrir une session avec une carte à puce.   |
| TRUSTED_FOR_DELEGATION             | 0x80000             | Le compte de service (compte d'utilisateur ou d'ordinateur) est approuvé pour la délégation Kerberos. N'importe lequel de ces services peut prendre l'identité d'un client demandant le service.   |
| NOT_DELEGATED                      | 0x100000            | Le contexte de sécurité de l'utilisateur n'est pas délégué à un service même si le compte de service est approuvé pour la délégation Kerberos.   |
| PASSWORD_EXPIRED                   | 0x800000            | Le mot de passe de l'utilisateur a expiré.   |

**# Exemple pour trouver les utilisateurs avec "NORMAL\_ACCOUNT" et "DONT\_EXPIRE\_PASSWORD"**  
**# -band est un "ET binaire"**

Clear-Host

\$n = 0x10200

```
Get-ADUser -Filter {userAccountControl -band $n} `
    -Properties * `
    | Sort-Object canonicalname `
    | Format-Table CanonicalName,Name,userAccountControl `
    -AutoSize
```

---

**# AMÉLIORATION de la commande précédente pour afficher la valeur**  
**# du paramètre userAccountControl en hexadécimale sur 8 caractères (32 bits)**  
**# et de l'aligner à droite.**

Clear-Host

\$n = 0x10200

```
Get-ADUser -Filter {userAccountControl -band $n} `
    -Properties * `
    | Sort-Object canonicalname `
    | Format-Table CanonicalName, `
        Name, `
        @{Label="AccountControl (hex)"; `
            Expression='{0:x8}' -f ($PSItem.userAccountControl)}; `
            Align="Right"} `
    -AutoSize
```

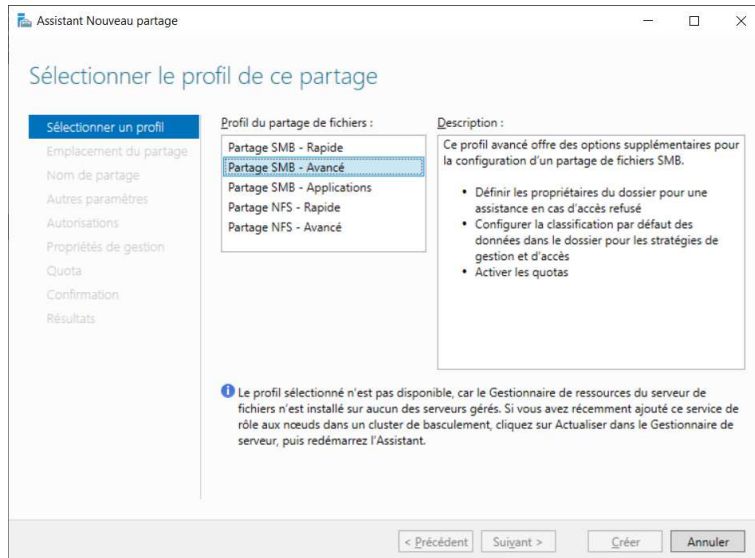
## Gestion des partages sur les serveurs de fichiers

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectif

Dans le prochain laboratoire, nous avons besoin de créer des partages sur le SERVEUR1 mais à partir du SERVEUR2.

Pour utiliser l'option "**Partage SMB – Avancé**", il faut ajouter la console "**Gestionnaire de ressources du serveur de fichiers**".



**Vous devez ajouter le rôle "Gestionnaire de ressources du serveur de fichiers" sur les deux serveurs.**

**Il est possible d'installer des rôles sur le SERVEUR1 à partir du SERVEUR2 à condition d'ajouter le SERVEUR1 à l'aide de l'option "Gestionnaire de serveur / Gérer / Ajouter des serveurs".**

Sur le SERVEUR2, nous pouvons ajouter des rôles et des fonctionnalités sur le SERVEUR2.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION  
SERVEUR2.FORMATION.LOCAL

Avant de commencer  
Type d'installation  
**Sélection du serveur**  
Rôles de serveurs  
Fonctionnalités  
Confirmation  
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs  
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

| Nom                      | Adresse IP   | Système d'exploitation                   |
|--------------------------|--------------|--|
| SERVEUR2.FORMATION.LOCAL | 192.168.1.20 | Microsoft Windows Server 2019 Datacenter |

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Sur le SERVEUR2, nous pouvons ajouter des rôles et des fonctionnalités sur le SERVEUR2 et le SERVEUR1.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION  
SERVEUR1.FORMATION.LOCAL

Avant de commencer  
Type d'installation  
**Sélection du serveur**  
Rôles de serveurs  
Fonctionnalités  
Confirmation  
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs  
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

| Nom                      | Adresse IP   | Système d'exploitation                   |
|--------------------------|--------------|--|
| SERVEUR2.FORMATION.LOCAL | 192.168.1.20 | Microsoft Windows Server 2019 Datacenter |
| SERVEUR1.FORMATION.LOCAL | 192.168.1.10 | Microsoft Windows Server 2019 Datacenter |

2 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

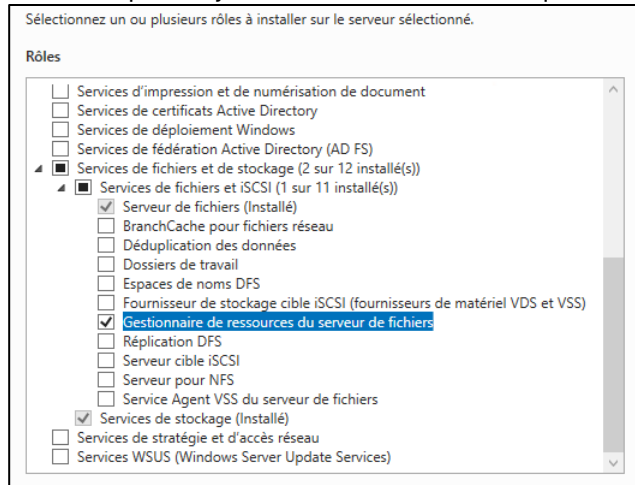
< Précédent Suivant > Installer Annuler

**Vous devez effectuer les prochaines étapes sur le SERVEUR2 et sur le SERVEUR1.**

Dans la console "**Gestionnaire de serveur**"

- Sélectionner le serveur
- Ajouter le rôle "**Gestionnaire de ressources du serveur de fichiers**"

note: accepter d'ajouter les fonctionnalités requises



## Dossiers personnels

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectifs

- Révision des autorisations NTFS, du champ d'application et de la propagation  
Vous devez consulter les fichiers "**Annexe - ICACLS.docx**" et "**Annexe - SID.docx**".
- Révision des dossiers partagés et des autorisations sur les partages  
Vous devez consulter le fichier "**Annexe - Partage avec PowerShell.docx**".
- Utilisation de la console "Gestionnaire de serveur\Services de fichiers et de stockage\Partages"
- Création d'une structure de dossiers personnels par l'interface graphique et par programmation PowerShell

### Directives générales

La configuration de dossiers personnels au sein d'une corporation demande une certaine planification. Afin de faciliter la gestion de ces dossiers les administrateurs de réseau vont préférer centraliser ces dossiers sur un serveur de fichiers et sous un même partage.

Selon les corporations et le besoin de sécurité, différents emplacements peuvent être utilisés. Par exemple au CVM, les professeurs et les étudiants ont des dossiers personnels sur des serveurs de fichiers différents.

Il est certain que la sécurité est un critère très important. Un utilisateur peut s'attendre à ce que ses informations personnelles soient à l'abri du regard des autres utilisateurs.

Dans le cadre de ce laboratoire, et afin de bien maîtriser les dossiers personnels, vous allez créer plusieurs structures de dossier

- Sur le SERVEUR1 en utilisant l'interface graphique du SERVEUR2
- Sur le SERVEUR1 par programmation PowerShell à partir du SERVEUR2

### Utilisateurs pour le laboratoire

Pour ce laboratoire, vous devez créer deux utilisateurs:

- Nom de l'utilisateur: U1  
Emplacement: CN=users,DC=formation,DC=local
- Nom de l'utilisateur: U2  
Emplacement: CN=users,DC=formation,DC=local



## **Résumé des étapes que vous ferez dans ce laboratoire pour la configuration des dossiers personnels**

Assigner un dossier personnel à un utilisateur lui permet de centraliser ses documents sur un serveur de fichiers.

Voici les trois grandes étapes à effectuer pour réussir la configuration des dossiers personnels.

Création du dossier racine et du partage

- Création d'un dossier racine qui va contenir les dossiers personnels des utilisateurs
- Attribution des autorisations NTFS adéquates sur le dossier racine
- Création d'un partage sur le dossier racine
- Attribution des autorisations de partage sur le dossier racine

Création des dossiers personnels pour les utilisateurs

- Création d'un sous-dossier pour l'utilisateur
- Attribution des autorisations NTFS adéquates sur le sous-dossier de l'utilisateur

Modification des propriétés des utilisateurs dans la console UOAD

- nom du dossier personnel
- lettre du dossier personnel

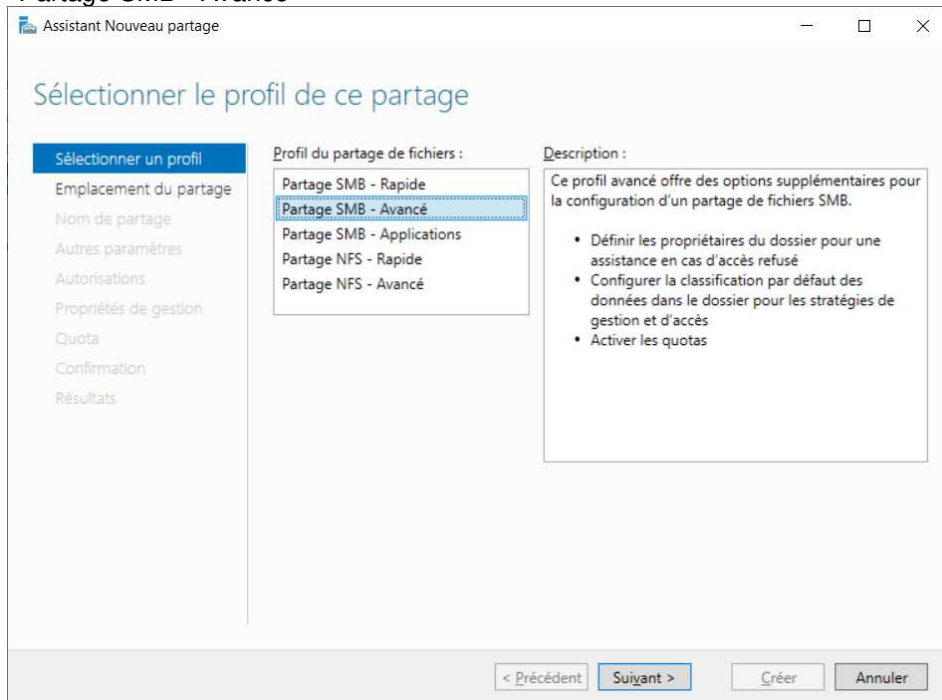
## Étape 1 – Création d'un dossier personnel en utilisant les consoles

Les dossiers seront sur le SERVEUR1 mais le travail se fait à partir du SERVEUR2

Création du dossier racine et du partage

Dans la console "Gestionnaire de serveur \ Services de fichiers et de stockage \ Partages"

- Bouton "Tâche"
- Nouveau partage...
  - "Partage SMB - Avancé"



Sélectionner le serveur et le chemin d'accès au partage

- Serveur: **SERVEUR1**
- Tapez un chemin personnalisé: **E:\\_Perso**

Indiquer le nom de partage

- Nom de partage: **PERSO\$**
- Description du partage: **Test pour les dossiers personnels**

Configurer les paramètres de partage

- Cocher "**Activer l'énumération basée sur l'accès**"
- Décocher "**Autoriser la mise en cache du partage**"
- Cocher "**Chiffrer l'accès aux données**"

Spécifier les autorisations pour contrôler l'accès

- Personnaliser les autorisations...

#### ONGLET "Autorisations"

- Désactiver l'héritage sur E:\\_Perso
  - ✓ "Convertir les autorisations héritées en autorisations explicites sur cet objet"

#### VOICI LES AUTORISATIONS FINALES QUE DOIT AVOIR LE DOSSIER

|                           |                      |   |
|---------------------------|----------------------|---|
| FORMATION\TECH            | Contrôle total       | Ce dossier, les sous-dossiers et les fichiers |
| FORMATION\Administrateurs | Contrôle total       | Ce dossier, les sous-dossiers et les fichiers |
| Système                   | Contrôle total       | Ce dossier, les sous-dossiers et les fichiers |
| DROITS DU PROPRIÉTAIRE    | Modification         | Ce dossier, les sous-dossiers et les fichiers |
| Utilisateurs du domaine   | Lecture et exécution | Ce dossier seulement                          |

#### ONGLET "Partage"

- Modifier
  - Autoriser "Tout le monde" "Contrôle total"

Spécifier les propriétés de gestion des dossiers

- Ne rien sélectionner

Appliquer le quota à un dossier ou un volume

- Ne pas appliquer de quota

Confirmer les sélections

- Cliquer sur le bouton "Créer"

---

#### Création du dossier personnel pour l'utilisateur U1

Créer le dossier \\SERVEUR1\E\$\\_PERSO\U1

Sur ce dossier, ajouter les autorisations NTFS suivantes:

- U1 Modification Ce dossier, les sous-dossiers et les fichiers

---

#### Modification des propriétés de l'utilisateur U1

##### Dans la console UOAD

Sélectionner l'utilisateur U1

Dans les propriétés de l'utilisateur U1, sélectionner l'onglet "Profil"

- Inscrire les propriétés pour le "Dossier de base"
  - Connecter: X:
  - À: \\SERVEUR1\PERSO\$U1

**IMPORTANT: Il ne faut pas utiliser le chemin suivant: \\SERVEUR1\E\$\\_PERSO\U1**

Tester si l'utilisateur U1 a accès à son X: lorsqu'il se connecte sur le serveur SERVEUR2

## Étape 2 – Création d'un dossier personnel par programmation PowerShell

Les dossiers seront créés sur le SERVEUR1 mais le code s'exécute sur le SERVEUR2

Écrire un script PowerShell pour créer des dossiers sur le SERVEUR1

### Création du dossier racine

- Nom du dossier: **\\SERVEUR1\E\$\\_PERSO2**
- Autorisations NTFS: **voir l'étape 1**

```
$chemin = "\\SERVEUR1\E$\_PERSO2"
```

```
# Avec New-Item, le chemin doit être un nom UNC si le dossier est distant
New-Item -Path $chemin `
    -ItemType directory
```

### La commande ICACLS.EXE est plus performante que les cmdlets Get-Acl et Set-Acl.

```
# Pour désactiver l'héritage et supprimer les autorisations NTFS existantes
icaccls.exe $chemin /inheritance:r
```

```
# Avec icaccls.exe, le chemin doit être un nom UNC si le dossier est distant
# S-1-5-18 est le SID pour "Système"
# S-1-3-4 est le SID pour "DROITS DU PROPRIÉTAIRE"
icaccls.exe $chemin /grant "Administrateurs: (OI) (CI) (F) "
icaccls.exe $chemin /grant "TECH: (OI) (CI) (F) "
icaccls.exe $chemin /grant "*S-1-5-18: (OI) (CI) (F) "
icaccls.exe $chemin /grant "*S-1-3-4: (OI) (CI) (M) "
icaccls.exe $chemin /grant "Utilisateurs du domaine: (RX) "
```

### Création du partage sur le dossier racine

- Nom du dossier racine: **E:\\_Perso2**
- Nom du partage: **PERSO2\$**
- Autorisations de partage: **"Contrôle total" pour "Tout le monde"**
- Autres paramètres
  - Activer l'énumération basée sur l'accès
  - Activer "Chiffrer l'accès aux données"
  - Désactiver "Autoriser la mise en cache du partage"

```
# Avec New-SMBShare, le chemin est toujours un chemin local
# si le dossier est distant, il faut utiliser le paramètre -CIMSsession
New-SMBShare -Name "PERSO2$" `
    -Path "E:\_Perso2" `
    -FullAccess "Tout le monde" `
    -FolderEnumerationMode AccessBased `
    -EncryptData $True `
    -CachingMode none `
    -CIMSsession "SERVEUR1"
```

### Pour modifier les propriétés de l'utilisateur U2 afin de lui attribuer un dossier personnel

- création du dossier personnel pour l'utilisateur U2
- modification des autorisations NTFS sur le dossier personnel de l'utilisateur U2
- la lettre pour accéder au dossier personnel de l'utilisateur U2 sera "X:"

```
New-Item -Path "\\SERVEUR1\PERSO2$\U2" `
-ItemType directory
```

```
icacls.exe \\SERVEUR1\PERSO2$\U2 /grant "U2:(OI)(CI)(M)"
```

```
# IMPORTANT: Il ne faut pas utiliser le chemin suivant: \\SERVEUR1\E$\_PERSO2\U2
Set-ADUser -Identity "U2" `
-HomeDrive "X:" `
-HomeDirectory "\\SERVEUR1\PERSO2$\U2"
```

### Étape 3 - Création des dossiers PERSO pour les utilisateurs EMP01 à EMP32

Les utilisateurs EMP01 à EMP32 doivent avoir un dossier personnel.

Vous devez rechercher les utilisateurs de l'unité d'organisation FORMATION par programmation.

Les dossiers personnels seront sur le SERVEUR1

- Nom partage: **\\SERVEUR1\PERSO\$**  
note: le partage PERSO\$ existe déjà, vous l'avez créé à l'étape 1
- Nom du dossier pour les utilisateurs: **\\SERVEUR1\PERSO\$\EMP\***  
note: chaque utilisateur aura le droit "Modification" sur son dossier personnel
- Le dossier personnel de chaque utilisateur sera associé à la lettre X:

## Programmation d'un utilisateur dans l'Active Directory

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectifs

- Utiliser PowerShell dans le cadre de la création d'objets d'un domaine
- Créer un objet utilisateur dans votre domaine
- Supprimer et récupérer un utilisateur

### Étape 1 - Mise en place

L'arborescence des unités d'organisation du domaine Formation.Local doit être déjà créée.

### Étape 2 - Introduction au cmdlet New-ADUser

Le paramètre -Name est le seul paramètre obligatoire de New-ADUser.

Voici la commande la plus simple pour créer un utilisateur: **New-ADUser -Name TOTO**

- Le compte est créé mais il est désactivé.
- L'utilisateur doit changer le mot de passe à l'ouverture de session
- L'utilisateur TOTO est créé dans le conteneur "Users".
- La valeur de l'attribut SamAccountName est le même que celui du paramètre -Name

**Si on ne déclare pas le paramètre -SamAccountName le contenu de l'attribut SamAccountName sera le même que celui du paramètre -Name.**

### Étape 3 - Création d'un utilisateur avec le cmdlet New-ADuser

Écrire un programme en PowerShell pour créer un utilisateur dans l'unité d'organisation TEST.  
Votre code doit utiliser les cmdlets du module ActiveDirectory et des variables autant que possible.

Le mot de passe de l'utilisateur sera AAAaaa111

```
$mdp = ConvertTo-SecureString -AsPlainText "AAAaaa111" -Force
```

Voici les propriétés de l'onglet "**Général**" du nouvel utilisateur

- Prénom: JOHN
- Nom: DOE
- Nom complet: JOHN DOE
- Description: Mon premier utilisateur
- Bureau: Informatique
- Numéros de téléphone du bureau: 514-999-6000
  - 514-999-7000, 514-999-8000
- Adresse de messagerie: JOHN.DOE@FORMATION.LOCAL
- Page WEB: www.formation.local

Voici les propriétés de l'onglet "**Adresse**" du nouvel utilisateur

- Pays: Canada
- note: un pays est constitué de trois attributs**

Voici les propriétés de l'onglet "**Compte**" du nouvel utilisateur

- Nom d'ouverture de session de l'utilisateur: JOHN.DOE@FORMATION.LOCAL
- Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000): FORMATION\JOHN.DOE
- Le mot de passe n'expire jamais: OUI
- Le compte est désactivé: NON

Voici les propriétés de l'onglet "**Téléphones**" du nouvel utilisateur

- Téléphone à domicile: 450-222-2222
- Téléphone mobile: 450-333-3333
- Télécopie: 450-444-4444

Le nom du compte de l'utilisateur sera identique au nom complet.

Au début de votre script de création de l'utilisateur ajouter une ligne de code qui va détruire votre utilisateur.

Votre code doit utiliser un "Try and Catch" pour ne pas afficher les messages d'erreurs de PowerShell. Dans la section "Catch" vous devez utiliser le nom complet de l'erreur lorsqu'un objet de l'Active Directory n'existe pas.

---


Vous pouvez consulter les trois exemples de la section "**Utilisation d'une table de hachage pour initialiser les paramètres d'un cmdlet**" à la page 17 du fichier "**C53 - Introduction PowerShell - 1 de 5.docx**".

---

## Étape 4 - Validation

Après la création de l'utilisateur, vous devez vérifier les valeurs de chacune des propriétés dans l'onglet "Éditeur d'attribut" de ce nouvel utilisateur.

Le nom du compte de l'utilisateur est "John Doe" mais le nom d'ouverture de session est "John.Doe".

| Nom  | Type        | Description             |
|--|-------------|-------------------------|
|  John Doe | Utilisateur | Mon premier utilisateur |

Voici la commande PowerShell qui affiche la liste des attributs qui correspondent aux propriétés de bases lorsqu'un utilisateur est créé avec la console UOAD.

```
Get-ADuser -Identity "John.Doe" `
    -Properties * | `
    Select-Object CN,DisplayName,DistinguishedName,GivenName,
        Name,SamAccountName,sn,UserPrincipalName
```

```
CN                : John Doe
DisplayName        : John Doe
DistinguishedName  : CN=John Doe,OU=TEST,DC=FORMATION,DC=LOCAL
GivenName         : John
Name              : John Doe
SamAccountName     : John.Doe
sn                : Doe
UserPrincipalName  : John.Doe@FORMATION.LOCAL
```

Une fois toutes les propriétés exactes, vérifier la fonctionnalité de votre utilisateur en vous connectant.

**Pour "changer d'utilisateur" vous pouvez exécuter TSDISCON.EXE**

**Il est important de fermer la session d'un utilisateur si votre intention est de modifier ses propriétés.**

Par défaut, les utilisateurs qui ne sont pas membre du groupe "Administrateurs" ne peuvent pas se connecter au serveur membre si on utilise le mode de session étendu.

Pour la solution à ce problème, voir la dernière page de ce document.



## ANNEXE

### Une liste de plusieurs cmdlets pour gérer un utilisateur

- Get-ADuser
- New-ADuser
- Remove-ADuser
- Set-ADuser
  
- Set-ADAccountPassword  
permet de modifier le mot de passe d'un utilisateur
  
- Get-ADUserResultantPasswordPolicy  
Nous utiliserons ce cmdlet lorsque nous parlerons des GPO.
  
- Disable-ADAccount
- Enable-ADAccount
  
- Unlock-ADAccount  
permet de déverrouiller un compte utilisateur
  
- Search-ADAccount  
permet de chercher des comptes (utilisateurs, ordinateurs et des comptes de service) selon plusieurs critères
  
- Set-ADAccountControl  
permet de modifier plusieurs propriétés des comptes (utilisateurs, ordinateurs et des comptes de service)
  
- Clear-ADAccountExpiration
- Set-ADAccountExpiration

#### Exemples

# Trouver les comptes qui sont verrouillés

**Search-ADAccount -LockedOut**

# Trouver les comptes dont le mot de passe n'expire jamais

**Search-ADAccount -PasswordNeverExpires**

# Trouver les comptes utilisateurs qui sont inactifs depuis 90 jours 0 heure 0 minute et 0 seconde

**Search-ADAccount -UserOnly -AccountInactive -TimeSpan 90.00:00:00**

# Trouver les comptes utilisateurs qui sont inactifs depuis 90 jours

**Search-ADAccount -UserOnly -AccountInactive -TimeSpan "90"**

# Trouver les comptes utilisateurs qui sont inactifs depuis 12 heures

**Search-ADAccount -UserOnly -AccountInactive -TimeSpan "12:00"**

# Trouver les comptes utilisateurs qui sont désactivés et affiche plusieurs propriétés

**Search-ADAccount -UsersOnly -AccountDisabled | `**  
**Format-List -Property Name,LastLogonDate,UserPrincipalName**

# Remplacer le mot de passe d'un utilisateur et

# forcer l'utilisateur à modifier son mot de passe à la prochaine ouverture de session

**\$mdp = ConvertTo-SecureString -String "AAAAaa111" -AsPlainText -Force**  
**Set-ADAccountPassword -Identity ETU -NewPassword \$mdp -Reset**

**Set-ADUser -Identity ETU -ChangePasswordAtLogon \$true**

## PROBLÈME AVEC LE MODE DE SESSION ÉTENDU

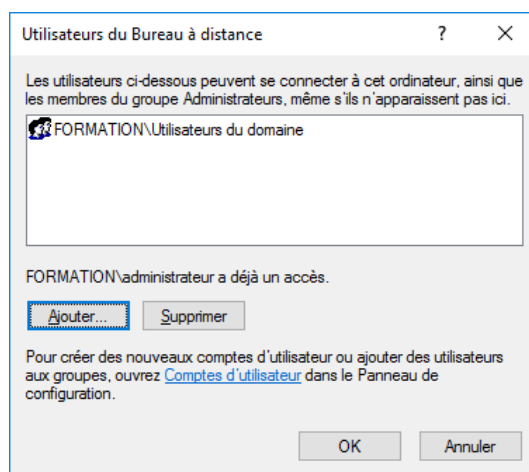
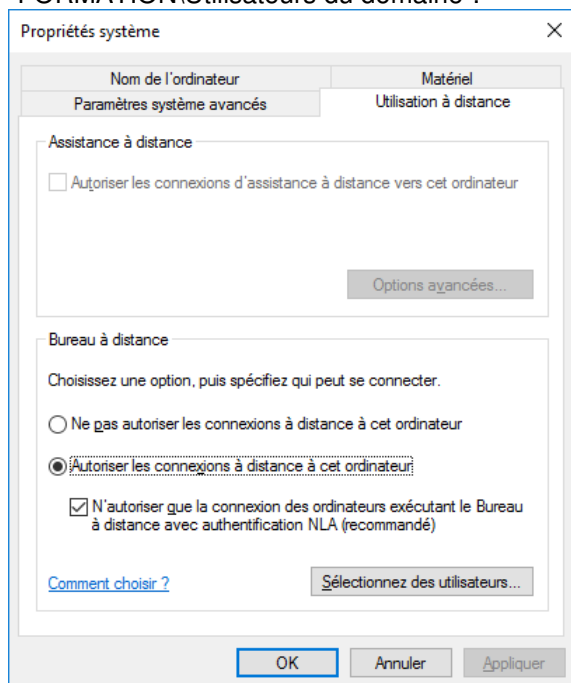
Par défaut, les utilisateurs qui ne sont pas membre du groupe "Administrateurs" ne peuvent pas se connecter au serveur membre si on utilise le mode de session étendu.



## SOLUTION SIMPLE À CE PROBLÈME

### Modification à effectuer sur le serveur membre

Dans "Propriétés système" cliquer sur le bouton "Sélectionnez des utilisateurs..." et ajouter le groupe "FORMATION\Utilisateurs du domaine".



## Propriétés des objets "Groupe"

Ce laboratoire doit être fait individuellement sur l'ordinateur virtuel 2

### Objectifs

- Maîtriser l'onglet "Éditeur d'attribut"
- Distinguer les propriétés de l'objet "Groupe"
- Maîtriser la différence entre les noms de propriétés et les options des cmdlets

### Étape 1 - Créer un groupe à l'aide de la console UOAD

Ouvrir la console UOAD

- Vérifier que votre affichage est en "Fonctionnalités Avancées"

Dans l'unité d'organisation "TEST"

- Créer le groupe "**grVotrePrénom**"

Nouvel objet - Groupe

Créer dans : FORMATION.LOCAL/TEST

Nom du groupe :  
grVotrePrénom

Nom de groupe (antérieur à Windows 2000) :  
grVotrePrénom

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

OK Annuler

### L'équivalent en PowerShell

```
New-ADGroup -Name "grVotrePrénom" `
             -GroupScope Global `
             -GroupCategory Security `
             -Path "OU=TEST,DC=FORMATION,DC=LOCAL"
```

## Étape 2 - Modifier les propriétés de l'onglet "Général" du groupe

Après la création d'un groupe, il est possible de modifier plusieurs propriétés.

Voici le contenu de l'onglet "**Général**" après la création du groupe

The screenshot shows the 'Propriétés de : grVotPrénom' dialog box with the 'Général' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are tabs: 'Général', 'Membres', 'Membre de', and 'Géré par'. The 'Général' tab contains a group icon and name 'grVotPrénom'. Below this are several fields: 'Nom de groupe (antérieur à Windows 2000) : grVotPrénom', 'Description :', 'Adresse de messagerie :', 'Étendue du groupe' (with radio buttons for 'Domaine local', 'Globale' (selected), and 'Universelle'), 'Type de groupe' (with radio buttons for 'Sécurité' (selected) and 'Distribution'), and 'Remarques :'. At the bottom are 'OK', 'Annuler', and 'Appliquer' buttons.

Dans l'onglet "**Général**", modifier les propriétés: Description, Adresse de messagerie, Remarques

This screenshot shows the same 'Propriétés de : grVotPrénom' dialog box, but with the following modifications: the 'Description' field now contains 'grVotPrénom est un groupe Globale', the 'Adresse de messagerie' field contains 'votrePrénom@formation.local', and the 'Remarques' field contains 'La création de mon premier groupe dans l'Active Directory.' The 'OK', 'Annuler', and 'Appliquer' buttons remain at the bottom.

**La modification des trois propriétés avec PowerShell**

```
$desc = "grVotrePrénom est un groupe Globale"
```

```
$courriel = "votrePrénom@formation.local"
```

```
$remarques = "La création de mon premier groupe dans l'Active Directory."
```

```
Set-ADGroup -Identity grVotrePrénom `
    -Description $desc `
    -Replace @{ mail = $courriel; info= $remarques }
```

## Création de groupes

Ce laboratoire doit être fait individuellement sur l'ordinateur virtuel 2

### Objectifs

- Maîtriser PowerShell dans le cadre de la création d'objets d'un domaine
- Créer des objets "Groupes" dans votre domaine

### Description du travail

Écrire un programme en PowerShell qui créera trois groupes en utilisant les cmdlets du module ActiveDirectory.

#### Généralités

- Le nom du domaine ne doit pas être explicitement présent
- Les groupes doivent être créés dans l'unité d'organisation TEST
- À la fin de votre script faites afficher la liste de vos groupes en utilisant le cmdlet Get-ADGroup
  - Vous devez afficher seulement le nom des groupes dont le nom débute par **gr**.

**NOTE: Dans votre code, il n'est pas nécessaire de configurer le paramètre -SamAccountName.**

### Documentation sur les groupes

#### Étendue du groupe

- Les membres d'un groupe d'étendue "**Globale**" peuvent provenir uniquement du domaine local mais les membres peuvent accéder aux ressources de n'importe quel domaine de la forêt.
- Les membres d'un groupe d'étendue "**Domaine local**" peuvent provenir de n'importe quel domaine de la forêt mais les membres peuvent accéder qu'aux ressources du domaine local.
- Les membres d'un groupe d'étendue "**Universelle**" peuvent provenir de n'importe quel domaine de la forêt et les membres peuvent accéder aux ressources de n'importe quel domaine de la forêt.

#### Synthèse

| Groupe        | Membres                | Autorisations              |
|---------------|------------------------|----------------------------|
| Globale       | Du domaine de création | Sur la forêt               |
| Domaine local | De la forêt            | Sur le domaine de création |
| Universel     | De la forêt            | Sur la forêt               |

#### Type de groupe

- Le type de groupe "**Sécurité**" permet d'affecter des autorisations sur les objets.  
Il est possible d'utiliser ces groupes comme listes de distribution par courriel.
- Le type de groupe "**Distribution**" ne permet pas d'affecter des autorisations sur les objets.  
Ces groupes sont destinés à être utilisés uniquement comme listes de distribution par courriel.  
Ces groupes sont utilisés avec des applications de messagerie comme "Microsoft Exchange".

## Création de trois groupes dans l'unité d'organisation TEST

```
# Création d'un groupe d'étendue "Globale"
New-ADGroup -Name "grGlobale" `
  -GroupScope Global `
  -GroupCategory Security `
  -Path "OU=TEST,DC=FORMATION,DC=LOCAL" `
  -Description "Groupe: Globale de TEST"
```

---

```
# Création d'un groupe d'étendue "Domaine local"
New-ADGroup -Name "grDomaineLocal" `
  -GroupScope DomainLocal `
  -GroupCategory Security `
  -Path "OU=TEST,DC=FORMATION,DC=LOCAL" `
  -Description "Groupe: 'Domaine local' de TEST"
```

---

```
# Création d'un groupe d'étendue "Universelle"
New-ADGroup -Name "grUniverselle" `
  -GroupScope Universal `
  -GroupCategory Security `
  -Path "OU=TEST,DC=FORMATION,DC=LOCAL" `
  -Description "Groupe: Universelle de TEST"
```

---

Voici la commande pour afficher les groupes dont le nom débute par **gr**

```
$groupes = Get-ADGroup -Filter 'name -like "gr*"' `
  -SearchBase "OU=TEST,DC=FORMATION,DC=LOCAL"

$groupes.Name
```

## Pour ajouter des utilisateurs à des groupes

**Add-ADGroupMember** Ajoute un ou plusieurs utilisateurs à un groupe de l'Active Directory

**Add-ADPrincipalGroupMembership** Ajoute un utilisateur à un ou plusieurs groupes de l'Active Directory

### Exemple 1

```
$groupe = "gr3"
```

```
Add-ADGroupMember -Identity $groupe `
                  -Members U1
```

```
Add-ADGroupMember -Identity $groupe `
                  -Members U2,U3,U4
```

### Exemple 2

```
Add-ADPrincipalGroupMembership -Identity U1 `
                              -MemberOf gr1,gr2,gr3
```

## Pour afficher les membres d'un groupe

**Get-ADGroupMember** Affiche les membres d'un groupe de l'Active Directory

### Exemple

```
Get-ADGroupMember -Identity gr1
```

## Pour afficher les groupes dont est membre un utilisateur

### Première méthode

**Get-ADPrincipalGroupMembership** Affiche les groupes dont est membre un utilisateur

### Exemple

```
# Commande pour afficher le distinguishedName des groupes de l'utilisateur U1
(Get-ADPrincipalGroupMembership -Identity U1).distinguishedName
```

```
CN=Utilisateurs du domaine,CN=Users,DC=FORMATION,DC=LOCAL
```

```
CN=gr1,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
```

```
CN=gr2,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
```

```
CN=gr3,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
```

NOTE: Le groupe "Utilisateurs du domaine" est affiché dans la liste.

```
# Commande pour afficher le nom des groupes de l'utilisateur U1
(Get-ADPrincipalGroupMembership -Identity U1).Name
```

```
Utilisateurs du domaine
```

```
gr1
```

```
gr2
```

```
gr3
```

NOTE: Le groupe "Utilisateurs du domaine" est affiché dans la liste.



## Pour afficher les groupes dont est membre un utilisateur

### Deuxième méthode

La propriété **MemberOf** de **Get-ADUser** ne retourne que les groupes de sécurité et les groupes de distribution auxquels l'utilisateur appartient, à l'exception de son groupe principal.

```
# Commande pour afficher les groupes de l'utilisateur U1
# excluant le groupe principal
(Get-ADUser -Identity U1 -Properties MemberOf).MemberOf
CN=gr3,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=gr2,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=gr1,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
```

**NOTE:** Le groupe "Utilisateurs du domaine" n'est pas affiché parce que c'est le groupe principal.

Le groupe principal est défini dans l'attribut **primaryGroupID** de chaque utilisateur.

```
(Get-ADUser -Identity U1 -Properties primaryGroupID).primaryGroupID
513
```

Le fichier "**Annexe - SID.docx**" contient le SID du groupe "Utilisateurs du domaine".

Le SID du groupe "Utilisateurs du domaine" est **S-1-5-21-<nombre>-<nombre>-<nombre>-513**.

La valeur **513** de l'attribut **primaryGroupID** correspond aux trois derniers chiffres du SID du groupe "Utilisateurs du domaine".

---

La propriété **MemberOf** de **Get-ADUser** affiche le **distinguishedName** de chaque groupe.

```
# Commande pour afficher seulement le nom de chaque groupe
$gr = (Get-ADUser -Identity U1 -Properties MemberOf).MemberOf
$gr | ForEach-Object {
    $groupe = Get-ADGroup -Identity $_
    Write-Host $groupe.Name -ForegroundColor Cyan
}

gr1
gr2
gr3
```

## Pour enlever des utilisateurs à des groupes

**Remove-ADGroupMember** Enlève un ou plusieurs utilisateurs d'un groupe de l'Active Directory

### **Remove-Add-ADPrincipalGroupMembership**

Enlève un utilisateur à un ou plusieurs groupes de l'Active Directory

#### Exemple 1

`$groupe = "gr3"`

```
Remove-ADGroupMember -Identity $groupe `
    -Members U2,U3,U4 `
    -Confirm:$false
```

#### Exemple 2

```
Remove-ADPrincipalGroupMembership -Identity U1 `
    -MemberOf gr1,gr2,gr3 `
    -Confirm:$false
```

## Pour supprimer des groupes

**Remove-ADGroup** Supprime un groupe de l'Active Directory

# Voici comment supprimer plusieurs groupes avec Remove-ADGroup

`$chemin = "OU=TEST,DC=FORMATION,DC=LOCAL"`

```
Get-ADGroup -SearchBase $chemin `
    -filter 'Name -like "gr*"' | Remove-ADGroup -Confirm:$false
```

## Les groupes imbriqués

### Pour afficher les utilisateurs d'un groupe si le groupe contient des groupes

Avec l'Active Directory, il est possible d'ajouter un groupe à un groupe.

```
# Commande qui ajoute les groupes gr2 et gr3 au groupe gr1
Add-ADGroupMember -Identity gr1 `
    -Members gr2,gr3
```

Pour afficher tous les utilisateurs d'un groupe Active Directory, y compris ceux qui appartiennent à des sous-groupes (groupes imbriqués), vous devez utiliser le paramètre **-Recursive** de **Get-ADGroupMember**.

Par exemple, le groupe Administrateurs est un groupe qui contient des groupes.

```
(Get-ADGroupMember -Identity "Administrateurs" -Recursive).Name
```

Le paramètre **"-Recursive"** demande beaucoup de ressource.

## Les groupes imbriqués

### Pour vérifier si un utilisateur est membre d'un groupe si le groupe contient des groupes

- 1) Vous devez créer le groupe grTEST.  
`New-ADGroup -Name grTEST -GroupScope Global`
- 2) Vous devez ajouter l'utilisateur John.Doe au groupe grTEST.  
`Add-ADGroupMember -Identity grTEST -Members John.Doe`
- 3) Vous devez ajouter le groupe grTEST au groupe "Admins du domaine".  
`Add-ADGroupMember -Identity "Admins du domaine" -Members grTEST`

### Est-ce que l'utilisateur John.Doe est membre du groupe "Admins du domaine" ?

Nous avons besoin du DistinguishedName de l'utilisateur John.Doe et du groupe "Admins du domaine".

```
$user_info = (Get-ADUser -Identity John.Doe).DistinguishedName
$group_info = (Get-ADGroup -Identity "Admins du domaine").DistinguishedName

(Get-ADUser -SearchBase $user_info -Filter {memberOf -RecursiveMatch $group_info}).Name
John.Doe
```

### Le résultat confirme que l'utilisateur John.Doe est membre du groupe "Admins du domaine".

Si l'utilisateur est membre du groupe "Admins du domaine", la requête retourne le nom de l'utilisateur.

Si l'utilisateur n'est pas membre du groupe "Admins du domaine", la requête ne retourne pas de valeur.

Le paramètre **"-RecursiveMatch"** demande beaucoup de ressource.

**Avant de continuer, vous devez détruire le groupe grTEST pour que l'utilisateur John.Doe ne soit plus membre du groupe "Admins du domaine".**

```
Remove-ADGroup -Identity grTEST -Confirm:$false
```

## Information sur le nom du groupe "Administrateurs de l'entreprise"

Le nom du groupe "Administrateurs de l'entreprise" contient une apostrophe courbée.

L'apostrophe courbe correspond au caractère UNICODE 2019.  
note: 2019 est une valeur hexadécimale

```
PS C:\_SCRIPTS\GROUPES> (Get-ADGroupMember -Identity "Administrateurs de l'entreprise").Name
TECH
Administrateur

PS C:\_SCRIPTS\GROUPES>
```

Selon votre clavier, il est possible que la commande ne trouve pas l'objet.

L'apostrophe droite correspond au code ASCII 39.  
note: 39 est une valeur décimale

L'apostrophe droite correspond au caractère UNICODE 0027.  
note: 0027 est une valeur hexadécimale

```
PS C:\_SCRIPTS\GROUPES> Get-ADGroupMember -Identity "Administrateurs de l'entreprise"
Get-ADGroupMember : Impossible de trouver un objet avec l'identité «Administrateurs de
l'entreprise» sous: «DC=FORMATION,DC=LOCAL».
Au caractère Ligne:1 : 1
+ Get-ADGroupMember -Identity "Administrateurs de l'entreprise"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Administrateurs de l'entreprise:ADGroup)
[Get-ADGroupMember], ADIdentityNotFoundException
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management
.ADIdentityNotFoundException,Microsoft.ActiveDirectory.Management.Commands.GetADGrou
pMember

PS C:\_SCRIPTS\GROUPES>
```

## Annexe

### Voici comment insérer un caractère UNICODE

- 1) Appuyer sur la touche **Alt** (celle à la gauche du clavier) sans relâcher la touche
- 2) Appuyer sur la touche **+** sur le clavier numérique
- 3) Taper la valeur hexadécimale sur le clavier numérique
- 4) Relâcher la touche **Alt**

Vous avez besoin de modifier le registre

```
reg.exe add "HKCU\Control Panel\Input Method" /v EnableHexNumpad /t REG_SZ /d 1 /f
```

**Cette modification dans le registre n'est pas effective immédiatement, l'utilisateur doit se déconnecter et ouvrir une nouvelle session pour que la modification du registre soit fonctionnelle.**

## Modification sur les utilisateurs

Ce laboratoire doit être fait individuellement sur le SERVEUR2

### Objectifs

- Maîtriser PowerShell dans le cadre de la recherche d'objets d'un domaine
- Maîtriser la nomenclature des objets
- Maîtriser les fichiers CSV

### Description du travail

Écrire un programme en PowerShell en utilisant les cmdlets du module "ActiveDirectory" qui créera plusieurs groupes à partir de fichiers CSV et ajoutera des utilisateurs à des groupes.

### Généralités

Le nom du domaine doit être dans une variable.

Tous les groupes seront dans l'unité d'organisation "**FORMATION.LOCAL/FORMATION/GROUPES**".

Informations sur les fichiers CSV

- C53 L07D ListeGroupes.csv
  - Ce fichier CSV est constitué de 3 champs séparés par des ":"
- C53 L07D ListeMembres.csv
  - Ce fichier CSV est constitué de 2 champs séparés par des ";"
  - La dernière colonne du fichier correspond à des noms de groupe
  - Le champ "Groupe" contient un ou plusieurs groupes qui sont séparés par des ","

**Les utilisateurs qui sont dans le fichier "C53 L07D ListeMembres.csv" existent déjà.**

### Travail

Créer les groupes

- Vous devez créer les groupes dans l'unité d'organisation "**FORMATION.LOCAL/FORMATION/GROUPES**"
- Vous devez utiliser le fichier "**C53 L07D ListeGroupes.CSV**"

Ajouter chaque utilisateur dans les groupes spécifiés en utilisant le fichier "**C53 L07D ListeMembres.csv**"

Pour récupérer chaque groupe dans le champ "Groupe", vous aurez besoin de l'opérateur **-split**.

Pour obtenir de l'aide sur **-split** → **Get-Help about\_split**

# Voici un exemple

```
"grTEST1", "grTEST2", "grTEST3", "grTEST4" -split " , "  
grTEST1  
grTEST2  
grTEST3  
grTEST4
```

## Création du script PowerShell pour créer les groupes et ajouter les utilisateurs aux groupes

Votre script ne doit pas afficher les messages d'erreurs générés par PowerShell.

- supprime tous les groupes qui sont dans la OU "GROUPES"
- création des groupes
- ajout des utilisateurs aux groupes

## ANNEXE

Comment créer un compte qui a sensiblement les mêmes propriétés que le compte Administrateur du domaine.

```
# Le SID du compte Administrateur du domaine se termine toujours par 500
# peut importe son nom Administrateur, Administrator, Administrador, ...
$userInstance = Get-ADUser -Filter * `
                    -Properties MemberOf | `
                    Where-Object { $PSItem.SID -like "S-1-5-21-*500" }

$newAdmin = "AdminAD"
$mdp = Read-Host "Mot de passe pour l'utilisateur $NewAdmin" -AsSecureString
$desc = "Compte d'utilisateur d'administration"

$nomDNS = (Get-ADDomain).DnsRoot

New-ADUser -Name $newAdmin `
            -Instance $userInstance `
            -Description $desc `
            -DisplayName $newAdmin `
            -SAMAccountName $newAdmin `
            -UserPrincipalName "$newAdmin@$nomDNS " `
            -AccountPassword $mdp `
            -PasswordNeverExpires $true `
            -Enabled $true

# Par défaut, un nouvel utilisateur est membre du groupe "Utilisateurs du domaine".
foreach($group in $userInstance.MemberOf)
{
    Add-ADGroupMember -Identity $group `
                     -Members $newAdmin

    Write-Host $group -ForegroundColor Yellow
}
```

Le compte TECH et le compte AdminAD sont similaires au compte Administrateur du domaine.

**Informations sur les groupes de l'unité d'organisation GROUPES**

| Nom   | Type                        |
|---|-----------------------------|
|  grCOMP_Comptables     | Groupe de sécurité - Global |
|  grCOMP_Gestionnaires  | Groupe de sécurité - Global |
|  grCOMP_Secretaires    | Groupe de sécurité - Global |
|  grCOMPTABILITE        | Groupe de sécurité - Global |
|  grFormation           | Groupe de sécurité - Global |
|  grINF_Analystes       | Groupe de sécurité - Global |
|  grINF_Gestionnaires   | Groupe de sécurité - Global |
|  grINF_Programmeurs    | Groupe de sécurité - Global |
|  grINF_Secretaires     | Groupe de sécurité - Global |
|  grINF_Tech_Niveau_1   | Groupe de sécurité - Global |
|  grINF_Tech_Niveau_2  | Groupe de sécurité - Global |
|  grINF_Tech_Reseau   | Groupe de sécurité - Global |
|  grINFORMATIQUE      | Groupe de sécurité - Global |
|  grING_Gestionnaires | Groupe de sécurité - Global |
|  grING_Ingenieurs    | Groupe de sécurité - Global |
|  grING_Secretaires   | Groupe de sécurité - Global |
|  grING_Techniciens   | Groupe de sécurité - Global |
|  grINGENIERIE        | Groupe de sécurité - Global |
|  grRH                | Groupe de sécurité - Global |
|  grRH_Gestionnaires  | Groupe de sécurité - Global |
|  grRH_Secretaires    | Groupe de sécurité - Global |

## Informations sur les groupes de l'unité d'organisation GROUPES

### CanonicalName

FORMATION.LOCAL/FORMATION/GROUPES/grCOMP\_Comptables  
FORMATION.LOCAL/FORMATION/GROUPES/grCOMP\_Gestionnaires  
FORMATION.LOCAL/FORMATION/GROUPES/grCOMP\_Secretaires  
FORMATION.LOCAL/FORMATION/GROUPES/grCOMPTABILITE  
FORMATION.LOCAL/FORMATION/GROUPES/grFormation  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Analystes  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Gestionnaires  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Programmeurs  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Secretaires  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Tech\_Niveau\_1  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Tech\_Niveau\_2  
FORMATION.LOCAL/FORMATION/GROUPES/grINF\_Tech\_Reseau  
FORMATION.LOCAL/FORMATION/GROUPES/grINFORMATIQUE  
FORMATION.LOCAL/FORMATION/GROUPES/grING\_Gestionnaires  
FORMATION.LOCAL/FORMATION/GROUPES/grING\_Ingenieurs  
FORMATION.LOCAL/FORMATION/GROUPES/grING\_Secretaires  
FORMATION.LOCAL/FORMATION/GROUPES/grING\_Techniciens  
FORMATION.LOCAL/FORMATION/GROUPES/grINGENIERIE  
FORMATION.LOCAL/FORMATION/GROUPES/grRH  
FORMATION.LOCAL/FORMATION/GROUPES/grRH\_Gestionnaires  
FORMATION.LOCAL/FORMATION/GROUPES/grRH\_Secretaires

## Informations sur les groupes de l'unité d'organisation GROUPES

### DistinguishedName

CN=grCOMP\_Comptables,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grCOMP\_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grCOMP\_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grCOMPTABILITE,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grFormation,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Analystes,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Programmeurs,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Tech\_Niveau\_1,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Tech\_Niveau\_2,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINF\_Tech\_Reseau,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINFORMATIQUE,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grING\_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grING\_Ingenieurs,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grING\_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grING\_Techniciens,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grINGENIERIE,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grRH,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grRH\_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=grRH\_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL