

## Leçon 2 : PowerShell

### 2.1 Introduction

Powershell est le langage de script mis à disposition par Microsoft sur les systèmes d'exploitation de nouvelle génération (Windows Server 2016, Windows 10, Windows Server 2012, Windows 8.1/7). Ce langage avancé est fortement utilisé par les administrateurs systèmes pour automatiser leurs tâches. C'est pourquoi nous allons nous concentrer, dans cette leçon, à l'étude de ce langage de script.

**Attention :** Il s'agit d'une simple introduction à Powershell. Bien sûr, nous aborderons celui-ci souvent lorsque nous étudierons certains aspects du système. Nous allons donc d'abord commencer par les éléments simples du langage avant d'approfondir celui-ci tout au long de notre étude.

PowerShell est complet et complexe. Dans un souci pédagogique, la présentation faite ici est simplifiée. Les lecteurs souhaitant une description plus précise peuvent se référer à la référence bibliographique.

### Ressource bibliographique

Cette leçon s'inspire du livre suivant : « William R. Stanek, Windows PowerShell™ 6 – IT Pro Solutions, Stanek & Associates, 2017 »

### 2.2 Démarrer le shell PowerShell

Pour démarrer le *shell* spécifique *PowerShell*, il faut simplement effectuer une recherche et celui-ci est trouvé assez facilement :

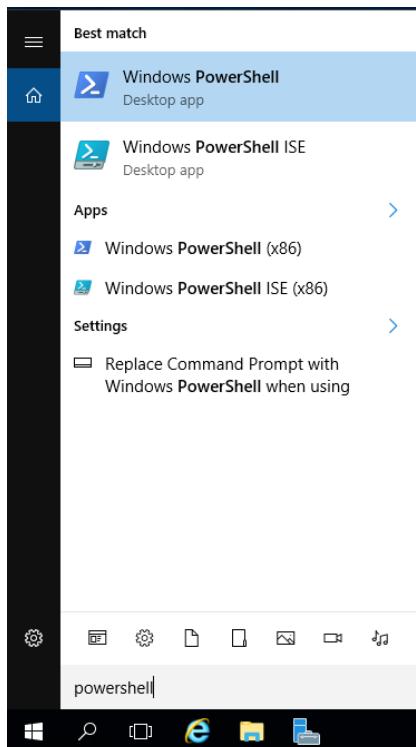


Figure 2.1 : Lancement de l'environnement Powershell

Les **scripts powershell** sont des fichiers textes portant l'extension **.ps1**. **Windows Powershell** est le terminal permettant d'exécuter des scripts Powershell. **Windows Powershell ISE** est l'outil de « développement » Powershell.

## 2.3 Premier script et première exécution

En utilisant un éditeur quelconque ou **Windows Powershell ISE**, il est possible de créer un premier script *PowerShell* assez simple :

```
$a = "Hello"  
$b = "world !"  
write-output "$a $b"  
write-output $a $b
```

Script 2.1 : « Hello Word » en PowerShell

Une fois ce script entré, on va l'enregistrer sous le nom **helloworld.ps1**. Pour exécuter ce script, il suffit :

1. De démarrer le shell Powershell
2. D'aller dans le dossier contenant le script
3. Démarrer le script en entrant :

```
PS C:\Users\Administrateur\Documents> .\helloworld.ps1
```

Le résultat à l'écran devrait être :

```
Hello world !  
Hello  
world !
```

Cependant, il se peut que l'erreur suivante survienne :

**Impossible de charger le fichier (...) car l'exécution de scripts est désactivée sur ce système.**

Pour des raisons de sécurité, les systèmes Windows Serveur peuvent ne pas exécuter directement des scripts non-signés numériquement. Si cela se produit, il est possible de changer ce comportement en exécutant la commande suivante dans le PowerShell :

```
PS C:\Users\Administrateur\Documents> Set-ExecutionPolicy unrestricted
```

Une fois la commande entrée, il faut répondre *Oui* à la question posée et les scripts pourront être exécutés.

Dans ce premier exemple simple, nous avons vu comment assigner une valeur à une variable mais également comment afficher quelque chose à l'écran (`Write-Output` ou encore `Write-Host`).

Pour lire un élément au clavier, il faut utiliser `Read-Host`. Ainsi, on peut écrire dans un script la ligne suivante pour capturer une chaîne de caractères :

```
$val = Read-Host "Entrez une chaine "
```

La commande `Read-Host` ajoute automatiquement un symbole « : » après le texte mentionné. On verra ainsi apparaître à l'écran ceci :

Entrez une chaine :

Si l'élément à lire est une valeur entière, il convient de forcer le type de la variable :

```
[int] $val = Read-Host "Entrez une valeur entiere "
```

## 2.4 Les Commandlet

PowerShell<sup>5</sup> est un invite de commande acceptant du scripting. Ainsi, il comprend les commandes standards héritées de MS-DOS comme *cls*, *cd*, *md*, *dir*, ...

En plus des commandes standards, PowerShell ajoute des *commandlet* (appelée aussi *cmdlet*). Il s'agit de commandes internes à l'invite et qui peuvent être appelées directement. Ces *cmdlet* sont composées d'un verbe et d'un nom.

Dans le tableau 1, nous trouverons une liste des principaux verbes utilisés dans le langage PowerShell.

Verbe Cmdlet	Signification
Add	Ajoute une occurrence ou un élément
Clear	Efface le contenu d'un objet
ConvertFrom	Convertit un élément à partir d'un format vers autre
ConvertTo	Convertit un élément dans un format particulier
Disable	Désactive un élément actif
Enable	Active un élément désactivé (ou inactif)
Export	Exporte les propriétés d'un élément dans un format donné
Get	Questionne (envoie une requête à) un objet donné ou (à) un sous-ensemble d'un type d'objet
Import	Importe les propriétés d'un élément à partir d'un format donné
Invoke	Exécute une occurrence d'un objet
New	Crée une nouvelle occurrence d'un élément
Remove	Supprime l'instance d'un objet
Set	Modifie des paramètres spécifiques d'un objet
Start	Démarrer une occurrence d'un élément
Stop	Arrête l'occurrence d'un élément
Test	Vérifie l'occurrence d'un élément pour un état ou une valeur donnée
Write	Réalise une opération d'écriture sur l'instance d'un objet

Tableau 2.1 : Aperçu des verbes<sup>6</sup>

Dans le tableau 2, nous trouvons quelques *cmdlet* utiles pour l'administrateur système.

Commande cmdlet	Description
Add-Computer, Remove-Computer	Ajoute ou supprime un ordinateur membre d'un domaine ou d'un workgroup
Checkpoint-Computer, Restore-Computer	Crée un point de restauration, restaure d'un point de restauration
Compare-Object, Group-Object, Sort-Object, Select-Object, New-Object	<i>Cmdlet</i> pour comparer, grouper, trier, sélectionner et créer des objets
ConvertFrom-SecureString, ConvertTo-SecureString	<i>Cmdlet</i> pour créer ou exporter une chaîne sécurisée
Debug-Process	Débogue un processus actif sur un ordinateur
Get-Alias, New-Alias, Set-Alias, Export-Alias, Import-Alias	<i>Cmdlet</i> pour obtenir, créer, modifier, exporter ou importer des raccourcis
Get-AuthenticodeSignature, Set-AuthenticodeSignature	Obtenir ou placer une signature à un fichier
Get-Command, Invoke-Command, Measure-Command, Trace-Command	<i>Cmdlet</i> pour obtenir des informations sur des <i>Cmdlet</i> , invoquer des commandes, mesurer le

<sup>5</sup> Donc si vous démarrez Windows Powershell

<sup>6</sup> Ce tableau est extrait du livre de référence

	Temps d'exécution de commandes ou tracer des commandes
<b>Get-Counter</b>	Obtenir les données du compteur de performance
<b>Get-Credential</b>	Obtenir un objet <i>Credential</i> basé sur le mot de passe
<b>Get-Date, Set-Date</b>	Obtenir ou fixer la date et l'heure courante
<b>Get-EventLog, Write-EventLog, Clear-EventLog</b>	Obtenir des événements, écrire des événements ou effacer des événements d'un journal
<b>Get-ExecutionPolicy, Set-ExecutionPolicy</b>	Obtient ou définit la politique d'exécution pour le shell courant
<b>Get-Host</b>	Obtient les informations à propos du système exécutant PowerShell
<b>Get-HotFix</b>	Obtient les patches et autres mises à jour appliquées à l'ordinateur
<b>Get-Location, Set-Location</b>	Affiche ou définit des informations concernant l'espace de travail actuel
<b>Get-Process, Start-Process, Stop-Process</b>	Obtient, démarre ou arrête un processus
<b>Get-PSDrive, New-PSDrive, Remove-PSDrive</b>	Obtient, crée ou supprime un lecteur PowerShell spécifié
<b>Get-Service, New-Service, Set-Service</b>	Obtient, crée ou définit un service système
<b>Get-Variable, New-Variable, Set-Variable, Remove-Variable, Clear-Variable</b>	<i>Cmdlet</i> pour obtenir, créer, définir et supprimer une variable ou sa valeur
<b>Import-Counter, Export-Counter</b>	Importe ou exporte le compteur de performance des fichiers journaux
<b>Limit-EventLog</b>	Fixe la taille et la durée d'un événement dans le journal
<b>New-EventLog, Remove-EventLog</b>	Crée ou supprime un événement personnalisé et sa source
<b>Ping-Computer</b>	Envoie des requêtes ICMP vers la destination
<b>Pop-Location</b>	Obtient une localisation en tête de pile
<b>Push-Location</b>	Sauvegarde une localisation en tête de pile
<b>Read-Host, Write-Host, Clear-Host</b>	Lit une entrée à partir -, écrit une sortie vers -, efface – la fenêtre
<b>Rename-Computer, Stop-Computer, Restart-Computer</b>	Renomme, arrête ou redémarre un ordinateur
<b>Reset-ComputerMachinePassword</b>	Modifie et annule le mot de passe utilisé par la machine pour s'identifier dans le domaine
<b>Show-EventLog</b>	Affiche un événement de l'ordinateur dans l'observateur d'événements
<b>Show-Service</b>	Affiche les services de l'ordinateur dans l'outil de gestion des services
<b>Start-Sleep</b>	Suspend l'exécution du shell ou du script pendant une période de temps définie
<b>Stop-Service, Start-Service, Suspend-Service, Resume-Service, Restart-Service</b>	<i>Cmdlet</i> pour arrêter, démarrer, suspendre, reprendre ou redémarrer un service
<b>Wait-Process</b>	Attend la fin du processus avant de continuer
<b>Write-Output</b>	Écrit un objet dans le <i>pipeline</i>
<b>Write-Warning</b>	Affiche un message d'avertissement

Tableau 2.2: Aperçu des commandes courantes<sup>3</sup>

Les *cmdlets* permettent d'enrichir les options de scripts. Ainsi, comme nous l'avons vu dans le code 2.1, `Write-Output` est un cmdlet permettant d'afficher une information à l'écran.

## 2.5 Obtenir de l'aide

PowerShell inclut beaucoup d'aide et même des exemples d'utilisation. Grâce à la *cmdlet* `Get-Help`, il est possible d'obtenir des informations précises.

Ainsi, si vous entrez ceci :

```
PS C:\Users\Administrateur\Documents> Get-Help Get-Date
```

Vous obtenez le manuel de la *cmdlet* `Get-Date`. Sans surprise, cette commande permet d'obtenir la date et l'heure courante. Comme plusieurs formats sont possibles, la page de manuel permet facilement de comprendre le format attendu.

Enfin, **des exemples** sont également fournis. Ainsi, si vous entrez :

```
PS C:\Users\Administrateur\Documents> Get-Help Get-Date -examples
```

Vous obtenez des exemples d'utilisation de `Get-Date`. Pour être sûr de pouvoir lire tous ces exemples, il est conseillé d'ajouter la commande `more` afin de voir l'affiche de manière paginée. Ainsi la commande devient :

```
PS C:\Users\Administrateur\Documents> Get-Help Get-Date -examples | more
```

L'affichage est ainsi rendu page après page.

## 2.6 Types de variable en Powershell

### Les variables élémentaires

Les variables élémentaires sont des variables qui peuvent contenir des chaînes de caractères, des nombres ou encore des valeurs booléennes. Pour déclarer ce type de variable, il faut simplement préfixer le nom de celle-ci par le symbole \$. On peut **forcer le type** d'une variable en précisant son type au moment de son utilisation. Il y a beaucoup de types différents, les principaux sont :

Type	Description
[int]	Entier 32 bits signé
[long]	Entier 64 bits signé
[bool]	Booléen (True / False)
[string]	Chaîne de caractères de taille fixe Unicode
[char]	Un caractère unicode (codage sur 16 bits)
[byte]	Un caractère non-signé (codage sur 8 bits)
[decimal]	Une valeur décimale codée sur 128 bits
[single]	Un nombre en virgule flottante codé sur 32 bits
[double]	Un nombre en virgule flottante codé sur 64 bits

Les opérations sur **les chaînes de caractères** :

Concaténation	La concaténation entre des chaînes de caractères s'obtient également avec l'opérateur « + » Ex: <code>Write-Output (\$a + \$b)</code>
---------------	---

<b>Comparaison</b>	Pour effectuer des comparaisons :
-eq	vérifie si 2 chaînes sont identiques
-ne	vérifie si 2 chaînes sont différentes
-ge	vérifie si la première est plus grande ou égale à la seconde
-gt	vérifie si la première est plus grande que la seconde
-lt	vérifie si la première est plus petite que la seconde
-le	vérifie si la première est plus petite ou égale à la seconde
-match	effectue une vérification sur base d'une expression régulière
-replace	permet d'effectuer un remplacement
<b>Modification<sup>7</sup></b>	\$a = "The Scriptign Guys"
	 \$a = \$a.Replace("Scriptign", "Scripting") <i>Remplace une chaîne par une autre</i>
	 \$b1 = \$a.Substring(4) <i>Extrait une sous-chaine d'une chaîne à partir de la 5<sup>ème</sup> position. \$b1 contient donc la chaîne « Scripting Guys ».</i>
	 \$b2 = \$a.Substring(4,9) <i>Extrait une sous-chaine de 9 caractères d'une chaîne à partir de la 5<sup>ème</sup> position. \$b2 contient donc la sous-chaine « Scripting ».</i>
	 \$c1 = \$a.ToLower() <i>Convertit toutes les lettres en minuscule. La chaîne \$c1 contiendra la valeur « the scripting guys »</i>
	 \$c2 = \$a.ToUpper() <i>Convertit toutes les lettres en majuscule. La chaîne \$c2 contiendra la valeur « THE SCRIPTING GUYS »</i>
	 \$d = \$b2.ToCharArray() <i>Convertit une chaîne de caractères en tableau de caractères. Le tableau \$d contiendra les éléments @("S","c","r","l","p","t","l","n","g")</i>
	 \$tab = \$a -split " " <i>Découpe la chaîne de caractères en utilisant le séparateur mentionné (espace dans cet exemple). Le résultat est un tableau comprenant les différents éléments. Dans notre exemple, \$tab contiendra @("The", "Scripting", "Guys")</i>
	 \$e = \$tab -join "*" <i>Applatit tous les éléments du tableau dans une chaîne de caractères. Les éléments seront séparés par le caractère mentionné (« * » dans cet exemple). La chaîne \$e contiendra la valeur « The*Scripting*Guys »</i>

Les opérations sur **les données numériques** :

---

<sup>7</sup> Ces exemples sont extraits du site *Technet* de Microsoft : <http://technet.microsoft.com/en-us/library/ee692804.aspx>

<b>Arithmétique</b>	Les opérations arithmétiques sont conformes à celles que l'on trouve dans le langage C. Ainsi :
	\$a = \$a + 1 ; \$a +=1 ; \$a++
	\$a = \$a - 1 ; \$a -=1 ; \$a--
	\$a = \$a * 3 ; \$a *= 3
	\$a = \$a / 5 ; \$a /= 5
	Le reste de la division entière s'obtient avec le symbole %
	\$reste = 5 % 2 # Le reste vaut 1
<b>Comparaison</b>	Pour effectuer des comparaisons :
	-eq vérifie si 2 nombres sont identiques
	-ne vérifie si 2 nombres sont différentes
	-ge vérifie si le premier est plus grand ou égale au second
	-gt vérifie si le premier est plus grand que le second
	-lt vérifie si le premier est plus petit que le second
	-le vérifie si le premier est plus petit ou égale au seconde
<b>Affichage d'une expression</b>	S'il faut afficher le résultat d'une expression directement à l'intérieur d'un cmdlet, il convient d'entourer l'expression de parenthèses afin que Powershell identifie clairement celle-ci :
	Write-Output ("Le reste de la division entière de 5 par 2 vaut " + (5 % 2) )

## Les tableaux

Powershell permet à l'utilisateur d'utiliser des tableaux. Les tableaux sont des variables *simples* qui contiennent des éléments indicés. Ainsi, ils sont également créés en utilisant le symbole \$. Pour initialiser les éléments d'un tableau, il suffit de lister ses éléments :

```
$montableau = @ (3, 5, 9, 10)
$montableau2 = @("Bonjour", "Salut", "Hello")
$montableau3 = @()
```

Il est possible d'accéder à un élément du tableau via son indice. Le premier élément se trouve à la position 0. Par exemple :

```
Write-output ("Le second élément se trouve à la position 1 et vaut " +
$montableau[1])
```

Dans ces exemples, on déclare et initialise un tableau avec un nombre fixe d'élément. Ainsi, il n'est pas possible d'accéder à l'indice 3 du tableau \$montableau2 puisque celui-ci contient 3 éléments (stockés aux indices 0, 1 et 2). Si l'on souhaite « étendre » un tableau (ajouter dynamiquement un élément supplémentaire), il faut utiliser l'opérateur +=.

**Quelques opérateurs sur les tableaux :**

```
$montableau.count
Retourne le nombre d'éléments dans le tableau (4)
```

```
$montableau2 = $montableau2 | Sort-Object
Permet de trier les éléments du tableau (Bonjour,Hello,Salut).
```

```
$montableau3 += 5
```

Etend le tableau \$montableau3 (actuellement vide) en lui ajoutant l'élément « 5 » à la position 1 (donc à l'indice 0).

### Les tables hachées

Powershell permet une utilisation simple des tables hachées (ou tableaux associatifs). Pour rappel, il s'agit de faire correspondre à une clé (unique donc) une valeur déterminée. Les tables hachées sont utilisées dans beaucoup de cas, mais notamment, pour garantir l'unicité d'un ensemble.

```
$capitales = @{"Belgique" = "Bruxelles"; "France" = "Paris"; "Allemagne" =  
"Berlin"; "Suisse" = "Berne" }  
  
$hash = @{ }
```

Nous pouvons effectuer les opérations suivantes :

```
$capitales.Add("Pays-Bas", "Amsterdam")
```

Dans cet exemple nous ajoutons un élément à la table.

```
$capitales.Remove("Allemagne")
```

Dans cet exemple nous supprimons de la table la valeur associée à la clé Allemagne.

```
$capitales.Set_Item("Pays-Bas", "Amsterdam")
```

Dans cet exemple nous modifions la valeur associée à la clé « Pays-Bas ».

```
$capitales.Get_Item("Belgique")
```

```
$capitales["Belgique"]
```

Dans cet exemple nous récupérons la valeur associée à la clé « Belgique ». La valeur récupérée est donc « Bruxelles ».

```
if($capitales.ContainsKey("Belgique")) {
```

Dans cet exemple nous vérifions si la clé « Belgique » est définie dans la table.

```
if($capitales.ContainsValue("Berlin")) {
```

Dans cet exemple nous vérifions si la valeur « Berlin » est stockée dans la table.

```
$capitales.keys
```

Cette propriété de la table hachée donne la liste des clés définies.

```
$capitales.values
```

Cette propriété de la table hachée donne la liste des valeurs stockées dans la table.

## 2.7 Quelques opérateurs

Powershell propose, comme dans tous les langages, des connecteurs logiques pour lier des expressions. Il y a également d'autres opérateurs comme les opérations bits à bits. Voici une liste de ces opérateurs :

Opérateurs	Description
-and	Effectue un ET logique entre les deux expressions. Vrai si chaque expression est vraie.

<b>-or</b>	Effectue un OU logique entre les deux expressions. Vrai si au moins une des expressions est vraie.
<b>-xor</b>	Effectue un OU EXCLUSIF entre les deux expressions. Vrai si une seule expression est vraie.
<b>-not</b>	Effectue une NEGATION de l'expression. Vrai si le résultat de l'expression est fausse.
<b>-band</b>	Effectue un ET bit à bit entre deux valeurs
<b>-bor</b>	Effectue un OU bit à bit entre deux valeurs
<b>-bnot</b>	Effectue un NOT bit à bit (inverse tous les bits) de la valeur donnée
<b>-bxor</b>	Effectue un OU EXCLUSIF bit à bit entre deux valeurs

## 2.8 Les sélections

Powershell permet la sélection au moyen des structures `if` et `switch`. Il faut **être vigilant à bien utiliser les opérateurs vus** précédemment.

```
[int] $val = Read-Host "Entrez une valeur "

if($val -gt 0) {
    Write-Output "La valeur est positive !"
} elseif($val -lt 0) {
    Write-Output "La valeur est négative !"
} else {
    Write-Output "La valeur est nulle !"

}
```

La structure du `if` est conforme à celle du langage C. La partie `elseif` est bien sûr facultative.

```
[string]$val = Read-Host "Entrez un chiffre en lettre "
switch($val) {
    "zero" { $val_num = 0 }
    "un" { $val_num = 1 }
    "deux" { $val_num = 2 }
    "trois" { $val_num = 3 }
    "quatre" { $val_num = 4 }
    "cinq" { $val_num = 5 }
    "six" { $val_num = 6 }
    "sept" { $val_num = 7 }
    "huit" { $val_num = 8 }
    "neuf" { $val_num = 9 }
    default { $val_num = -1 }
}

if($val_num -ge 0) {
    Write-Output ("Le chiffre entré est " + $val_num + " et son carre vaut: "
        + ($val_num * $val_num))
}
```

La structure `switch` est assez simple à écrire. Elle admet l'utilisation de chaîne de caractères ou des données numériques.

## 2.9 Les répétitions

Powershell admet plusieurs formes de répétitions. On dénombre ainsi les boucles de type *while* et *for* mais également des boucles de type *foreach*.

### Les boucles while

```
$i = 0
while($i -le 5) {
    Write-Output ("Tour dans la boucle = " + $i)
    $i++
}
```

Dans cet exemple, il y aura 6 tours dans la boucle (puisque *i* va évoluer de 0 à 5).

### Les boucles for

```
for($i=0 ; $i -le 5 ; $i++) {
    Write-Output ("Tour dans la boucle = $i")
}
```

Dans cet exemple, il y aura également 6 tours dans la boucle. La structure de la boucle *for* est très proche de celle utilisée en C. **Attention aux opérateurs de comparaison !**

### Les boucles foreach

```
$tableau = @(1,4,9,0,3,1)
foreach($element in $tableau) {
    Write-Output ("Elément courant = " + $element)
}
```

Dans cet exemple, on parcourt tous les éléments d'un tableau un à un.

La boucle *foreach* est particulièrement adaptée au parcours d'une table hachée :

```
$capitales = @{"Belgique" = "Bruxelles"; "France" = "Paris"; "Allemagne" =
"Berlin"; "Suisse" = "Berne" }
foreach ($pays in $capitales.keys) {
    Write-Output ("La capitale de $pays est $($capitales[$pays])")
}
```

Nous utilisons ici l'interpolation de chaînes en Powershell. Il faut noter l'écriture particulière lorsqu'il s'agit d'aller retrouver la valeur associée à un tableau associatif avec un *\$()* encadrant l'ensemble.

## 2.10 Parcourir un fichier texte

Powershell permet de parcourir un fichier texte et d'en traiter chaque ligne. C'est particulièrement utile s'il faut créer des utilisateurs à partir d'une liste, créer des dossiers, ... Le fonctionnement est assez simple, il faut utiliser la cmdlet `Get-Content` et ensuite, utiliser des expressions régulières pour traiter le résultat.

Si le fichier est conforme au schéma suivant (`C:\monfichier.txt`) :

```
Element1;Element2;Element3
Element1;Element2;Element3
Element1;Element2;Element3
Element1;Element2;Element3
```

Voici comment il est possible d'en traiter les différentes lignes :

```
$contenu = Get-Content "C:\monfichier.txt"
foreach($ligne in $contenu) {
    if($ligne -match '^(.*) ; (.*) ; (.*)$') {
        write-output ("Element 2 = $($matches[2])")
    }
}
```

Dans cet exemple, nous commençons par lire le contenu du fichier grâce au cmd-let `Get-Content`. Le tableau contenant les différentes lignes du fichier s'appelle `$contenu`. Grâce à une boucle `foreach`, il est possible de parcourir chaque ligne et d'analyser celle-ci grâce à une expression régulière. Enfin, grâce à la variable `$matches`, il est possible de récupérer les éléments capturés dans l'expression.

Quelques éléments d'une **expression régulière** :

<code>[...]</code>	1 caractère compris dans la séquence mentionnée. Ex : <code>[a-z]</code> <i>N'importe quelle lettre</i>
<code>[^...]</code>	1 caractère <u>non</u> compris dans la séquence mentionnée. Ex : <code>[^;]</code> <i>N'importe quel caractère qui n'est pas le signe de ponctuation « ; »</i>
<code>.</code>	N'importe quel caractère
<code>\w</code>	Une lettre
<code>\W</code>	N'importe quel caractère qui n'est pas une lettre
<code>\d</code>	Un chiffre
<code>\D</code>	N'importe quel caractère qui n'est pas un chiffre
<code>\s</code>	Un espace, une tabulation
<code>\S</code>	N'importe quel caractère qui n'est pas un espace ou une tabulation
<code>*</code>	Répétition 0-N Ex : <code>.*</code> <i>Séquence éventuelle de n'importe quel caractères</i>
<code>+</code>	Répétition 1-N Ex : <code>.+</code> <i>Séquence d'au moins un caractère quelconque</i>
<code>^</code>	Correspond au début de la chaîne
<code>\$</code>	Correspond à la fin de la chaîne
<code>()</code>	Permet de capturer un élément accessible par après au moyen de la variable <code>\$matches[]</code> . <b>Attention !</b> <code>\$matches[0]</code> reprend l'ensemble de la ligne. Les éléments capturés commencent donc à l'indice 1.

## 2.11 Commentaires en Powershell

Les commentaires peuvent, comme en C, être limité à une seule ligne. Dans ce cas, il suffit de préfixer la ligne par le symbole #

```
# Ceci est un commentaire sur une ligne
```

Si le commentaire s'étale sur plusieurs lignes, il faut utiliser les éléments <# et #> comme délimiteur.

```
<# Voici un commentaire
qui se trouve
sur plusieurs lignes #>
```

## 2.12 Quelques commandes utiles

### Créer un dossier

```
PS C:\...> New-Item C:\Scripts -type directory
```

### Se placer dans un dossier

```
PS C:\...> Set-Location C:\Scripts
```

### Exécuter un programme ou une commande (résultat affiché)

```
PS C:\...> Invoke-expression "C:\Windows\system32\tasklist.exe"
```

### Exécuter un programme ou une commande (résultat caché)

```
PS C:\...> Invoke-expression "C:\Windows\system32\tasklist.exe" | out-null
```

### Exécution directe et récupération du résultat dans une variable

```
PS C:\...> $resultat = &"C:\Windows\system32\tasklist.exe"
```

## 2.13 Pour finir ...

Il est bien clair que cette leçon constitue **une introduction** à PowerShell. Des éléments importants utilisables à l'intérieur de scripts seront vus par la suite. N'oubliez pas de combiner tous ces éléments afin de constituer vos scripts !

La plupart des cmdlet accepte bon nombre d'options. Ainsi, par exemple, le cmdlet de lecture d'une information au clavier `Read-Host` admet une option `-AsSecureString` qui permet de lire les données sensibles (comme un mot de passe). Les options sont détaillées dans l'aide associée à chaque cmdlet (`Get-Help Read-Host` par exemple).

Internet et, en particulier, le site de Microsoft regorge d'information et d'exemples sur l'utilisation de PowerShell (par exemple : <http://technet.microsoft.com/en-us/scriptcenter/powershell.aspx>). N'oubliez donc pas d'aller y jeter un coup d'œil pour trouver des solutions à des problèmes rencontrés.

## 2.14 Exercices

1. Sur base du fichier « liste-users.csv », on vous demande, pour chaque ligne présente dans le fichier, **d'afficher à l'écran** le contenu de celle-ci en ajoutant deux nouveaux champs : le *login* et le *mot de passe* de l'utilisateur.
  - a. Le login sera formé comme suit : la 1<sup>ère</sup> et la dernière lettre de la catégorie (**administratif → af**). Ces lettres seront suivies d'un numéro de séquence par catégorie. Ainsi, s10073 identifie le 73<sup>ème</sup> utilisateur de la catégorie *social* alors que p10040 identifie le 40<sup>ème</sup> utilisateur de la catégorie *personnel*.
  - b. Le mot de passe comptera exactement 8 caractères et comprendra 2 chiffres, deux lettres majuscules et 4 lettres minuscules. Pour composer ce mot de passe, vous pouvez faire appel à la cmdlet Get-Random qui fournit un nombre aléatoire. On vous demande de coder vous-même la génération du mot de passe. Pensez que la position des lettres et chiffres dans le mot de passe est aléatoire (il serait incorrect de supposer que le mot de passe commence par une minuscule puis un chiffre, ...). **Attention ! Tous les utilisateurs numérotés 50 (af0050, pl0050, ie0050, ...) doivent avoir « P@ssw0rd » comme mot de passe.**

Les lignes commençant par un '#' doivent être ignorées, ce sont des commentaires.

(Solution : le script fait moins de 25 lignes)

## Leçon 3 : Administration locale

### 3.1 Introduction

Dans cette leçon nous allons aborder les éléments d'administration locale. Ainsi, nous allons étudier comment nous pouvons administrer un serveur *autonome* ne servant pas à authentifier des machines et des utilisateurs sur le réseau. Bon nombre des éléments vus ici sont également applicables aux versions desktop *professionnelles* des systèmes d'exploitation Microsoft comme par exemple *Windows 10/8.1/7 Professionnel*.

Les éléments abordés dans cette leçon sont :

- Les utilisateurs, les groupes locaux et les profils
- Le système de fichiers, les quotas et la sécurité NTFS
- La stratégie locale
- Divers : la console MMC, l'observateur d'événements, les tâches planifiées

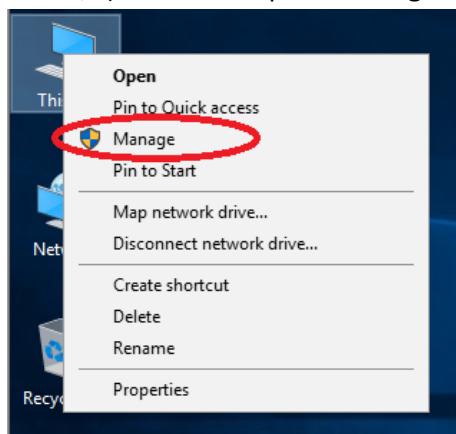
### Référence bibliographique

Ce chapitre se base sur la référence bibliographique suivante :

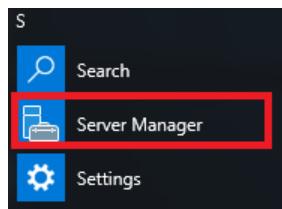
[1] C. Zacker, *Exam Ref 70-740 Installation, Storage and Compute with Windows Server 2016*, Microsoft Press, 19 January 2017.

Nous utiliserons beaucoup l'outil **Server Manager**. On peut procéder de 2 manières :

- Cliquer sur **Démarrer** puis faire un **clic-droit** sur **Ordinateur** (cette méthode est compatible avec Windows 10 et Windows 8.1/7) et choisir l'option **Manage** :



- Cliquer sur l'icône qui se trouve dans le menu démarrer.



L'interface de gestion du serveur démarre. Cette interface permet de configurer le serveur et ses ressources locales.

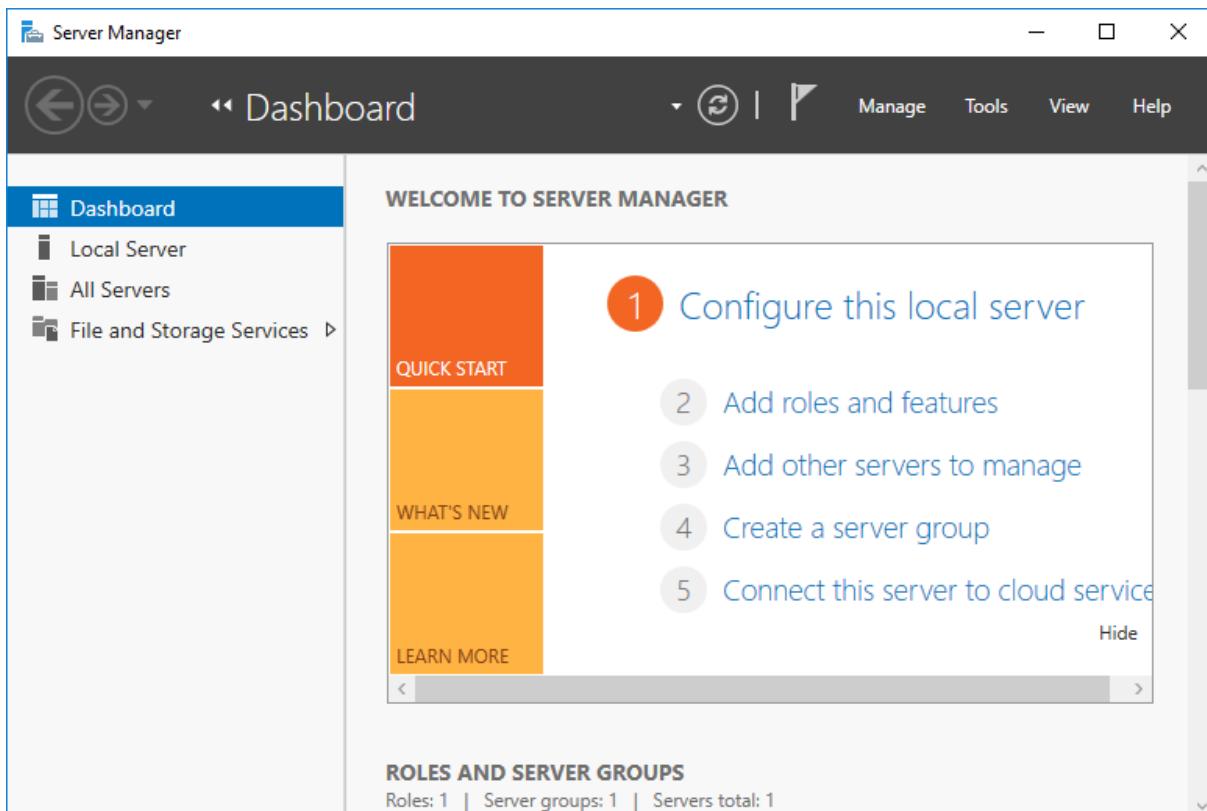


Figure 3.1 : Interface de gestion du serveur

Sur la figure 3.1, nous pouvons voir l'interface de gestion du serveur qui se compose d'un menu à gauche avec les options **Dashboard**, **Local Serveur**, **All Servers**, ... et un menu en haut à droite composé des options **Manage**, **Tools**, **View** et **Help**.

Le menu **Manage** permet, notamment, d'**Ajouter des rôles** (*Add Roles and Features*) :

- **Roles** : permet d'ajouter des *rôles* au serveur courant. Les rôles principaux sont :
  - Des services Active Directory (notamment, AD Certificate Service, AD Domain Service, AD Federation Services, AD Lightweight Directory Services, AD Right Management Services)
  - DHCP Server (qui permet au serveur de distribuer des adresses IP sur le réseau),
  - DNS Server (qui permet d'installer un serveur de nom et de gérer des noms DNS),
  - Fax server (qui autorise le serveur à envoyer et recevoir des fax),
  - *Hyper-V* (gestion de machines virtuelles),
  - *Web Server (IIS)* (qui permet d'héberger des sites web et déployer des applications .NET),
  - ...
- **Features** : permet d'ajouter une fonctionnalité au serveur autonome. La distinction entre les fonctionnalités et les rôles est relativement difficile à faire étant donné qu'on y retrouve par exemple le *SMTP Serveur* (envoi de courriers).

Parmis les outils importants dans l'administration locale d'un serveur, il y a l'outil de *Gestion de l'ordinateur*, accessible depuis le **Server Manager > menu Tools > Computer Management**. On y trouve :

- **System Tools.** On y trouve les outils suivants :
  - Le *Task Scheduler* qui permet de démarrer automatiquement des jobs sur le serveur
  - L'*Event Viewer* qui reprend les fichiers journaux du système. Ainsi, les erreurs consignées par le serveur ou les applications peuvent se trouver ici.
  - Les *Shared Folders* qui reprennent les partages actifs (ie. les dossiers partagés) sur le serveur. Intéressant pour visualiser tous les partages en cours.
  - Les *Local Users and Groups* qui permet d'ajouter et de gérer les utilisateurs et les groupes locaux au serveur
  - L'outil *Performance* qui consigne les éléments des rapports et journaux concernant les performances du système.
  - Le *Device Manager* reprenant la configuration matérielle du serveur.
- **Storage.** On y trouve les éléments suivants :
  - *Windows Server Backup* qui permet de réaliser des backups du système
  - *Disk Management* qui permet de gérer les disques, partitions et systèmes de fichiers et les lettres attribuées à chaque lecteur.
- **Services and Applications.** On y trouve les éléments suivants :
  - L'option *Routing and Remote Access* permet d'ajouter des options NAT ou encore configurer un serveur VPN sur Windows Serveur.
  - L'option *Services* qui permettent de démarrer des programmes serveurs et de les arrêter.

## 3.2 Les utilisateurs et groupes locaux

Le serveur **dispose d'une base de données locale des utilisateurs**. Il est possible d'installer une base de données **globale** si l'on installe Active Directory *Directory Service*. Une base de données globale sert à identifier les utilisateurs au travers d'un réseau tandis que la base de données des utilisateurs locale est uniquement utilisée par le serveur courant.

Gérer des utilisateurs et la sécurité qui leur est attachée est une des occupations de l'administrateur système. En effet, gérer efficacement les ressources partagées entre tous n'est pas une tâche toujours facile.

Pour **visualiser les utilisateurs locaux** configurés sur le système, il suffit de démarrer le *Server Manager* et aller dans **Tools > Computer Management > Local Users and Groups > Users**<sup>8</sup>. On peut ainsi voir que seul 3 utilisateurs sont présents : *Administrator*, *DefaultAccount* et *Guest*. La flèche vers le bas, probablement présente sur les comptes *DefaultAccount* et *Guest* mentionne que ce compte **est désactivé**. Nous reparlerons du compte *Guest* plus tard, qui dispose de droits limités.

Pour **visualiser les groupes de sécurité locaux** configurés sur le système, il faut aller dans **Computer Management > Local Users and Groups > Groups**. Il y a déjà bon nombre de groupes de sécurité présents. Parmi ceux-ci, pointons :

- **Administrators** : Tous les utilisateurs membres de ce groupe sont administrateurs du serveur.
- **Guests** : Tous les utilisateurs membres de ce groupe sont *Invités*.

<sup>8</sup> Windows donne l'impression d'identifier les utilisateurs sur base de leur nom d'utilisateur. Ce n'est pas la réalité, les utilisateurs sont identifiés sur base de leur SID. Le SID d'un utilisateur est composé du SID de la machine, complété par l'utilisateur. Ainsi, ce dernier est unique.

- Users : Tous les utilisateurs membres de ce groupe sont des *utilisateurs standards* du serveur
- Power Users : Tous les utilisateurs membre de ce groupe sont des *utilisateurs avancés* (ils ont plus de droit que les utilisateurs standard). **Ne devrait plus être utilisé !**

Pour **créer un utilisateur**, il suffit de faire un clic-droit et choisir l'option **New User** (également présente par le menu *More Actions* à droite). Il faut mentionner les données suivantes :

- User name : c'est son login, la façon dont celui-ci pourra se connecter au système
- Full name : c'est le nom qui apparaîtra dans l'interface
- Description : un texte facultatif (p.ex. moment de la création, ...)
- Password : le mot de passe attribué à cet utilisateur
- Confirm password : afin de vérifier si le mot de passe est correct
- Certaines options :
  - *User must change password at next login* : impose que l'utilisateur modifie le mot de passe attribué par l'administrateur
  - *User cannot change password* : interdit les modifications de mot de passe par l'utilisateur
  - *Password never expires* : certaines politiques de sécurité imposent des changements réguliers du mot de passe.
  - *Account is disabled* : empêche toute connexion via ce mot de passe

Par défaut, quand un utilisateur est créé, il est placé dans le groupe Users. Il est donc considéré comme *un utilisateur standard* du système. Si cet utilisateur doit administrer le serveur, il est nécessaire qu'il soit *membre* du groupe de sécurité *Administrators*.

Si l'on **examine les propriétés d'un utilisateur** (clic-droit sur l'utilisateur concerné puis **propriétés**), on peut voir toutes les informations mémorisées pour un utilisateur.

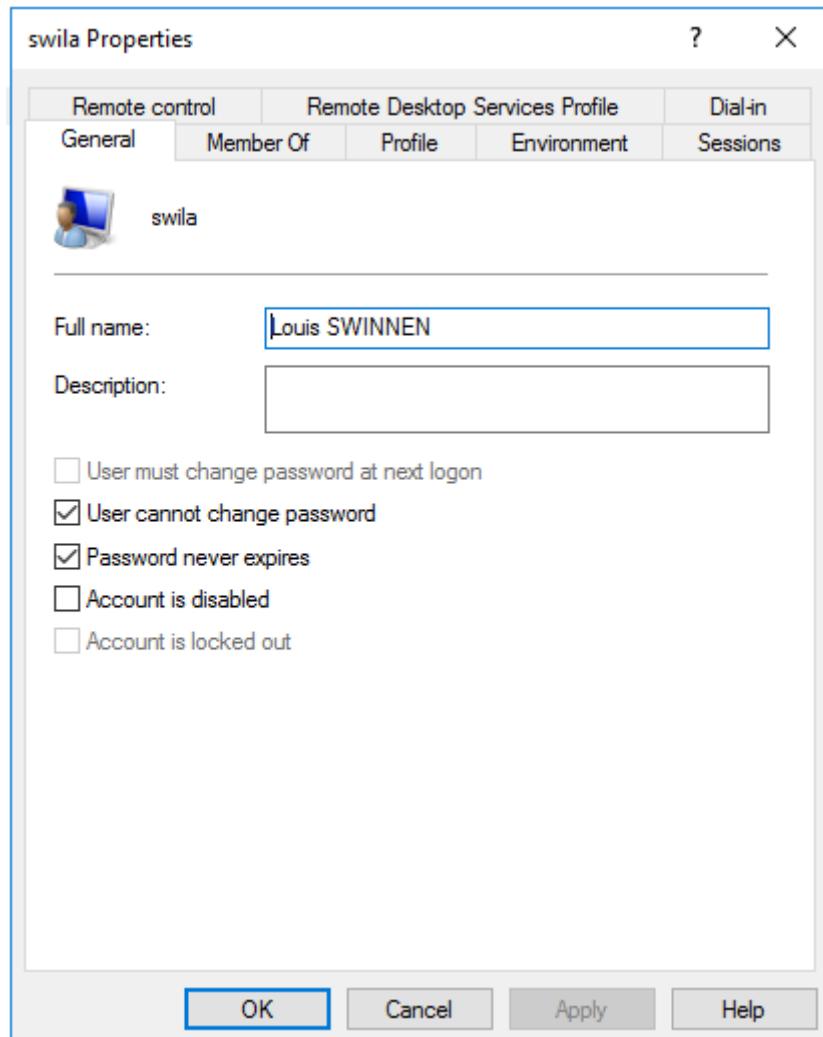


Figure 3.2 : Propriétés de l'utilisateur « swila »

Comme nous pouvons le voir sur la figure 3.2, il y a plusieurs onglets et donc beaucoup d'informations mémorisées par utilisateur. L'onglet *General* reprend les informations remplies lors de la création de l'utilisateur. L'onglet *Member Of* reprend les groupes auxquels cet utilisateur appartient. Il est possible d'ajouter des groupes directement par cet onglet. L'onglet *Profile* reprend les informations concernant *le profil* de cet utilisateur. Il est courant de spécifier le chemin dans lequel ce profil sera enregistré. Ainsi, dans notre exemple, on aurait pu mentionner le chemin suivant :

- Local path : C:\profile\swila  
Ce chemin mentionne l'endroit où les fichiers de l'utilisateur seront sauvegardés. La plupart des applications proposent par défaut cet endroit pour enregistrer ou charger un document.
- Profile path : C:\profile\swila\ntprof  
Ce chemin mentionne l'endroit où le *profil* de l'utilisateur est enregistré. Le profil comprend sa configuration (fond d'écran, icônes du bureau, contenu des « Documents »).

On mentionne dès lors que le **dossier de base** se trouve dans un chemin d'accès local (stocké sur le disque local dans le dossier *profile*) et que le **profil** de l'utilisateur se trouve dans un dossier *ntprof* à l'intérieur du chemin d'accès local. Ces options seront d'une très grande importance lors de l'étude d'Active Directory.

L'onglet *Environnement* permet de déterminer les programmes à lancer lorsque l'utilisateur ouvre sa session. Les autres onglets seront soit vus plus tard ou pas du tout. En effet, bon nombre des paramètres ici sont **gérés globalement via Active Directory**.

### 3.2.1 Création des groupes et utilisateurs en Powershell

Avant Windows Server 2016, il était nécessaire d'utiliser les objets ADSI pour réaliser les tâches d'administration locales. Cependant, toutes les possibilités ne sont pas encore implémentées. Ainsi, pour l'administration locale des utilisateurs, il faut faire un mélange des options, nous verrons cela dans la suite. Pour créer un groupe, **sous Windows Server 2016** :

```
$group = New-LocalGroup -Name "MonGroupe" -Description "Groupe de test"
```

Dans le script ci-dessus, nous créons un groupe de sécurité très simplement. Il suffit de passer les paramètres souhaités et ce groupe apparaîtra alors dans les *groupes locaux*.

Une méthode analogue peut être utilisée pour créer des utilisateurs et fixer certains paramètres<sup>9</sup> :

```
$user = New-LocalUser -AccountNeverExpires -PasswordNeverExpires  
    -FullName "Super SWILA" -name "Powerswila"  
    -Password (ConvertTo-SecureString -AsPlainText "P@ssw0rd" -Force)  
    -UserMayNotChangePassword  
  
Add-LocalGroupMember -Group "Users" -Member $user  
Add-LocalGroupMember -Group "MonGroupe" -Member $user  
  
<# Section ADSI #>  
$userADSI = [ADSI] "WinNT://$env:computername/Powerswila"  
$userADSI.Profile = "C:\profiles\Powerswila\ntprof"  
$userADSI.HomeDirectory = "C:\profiles\Powerswila"  
$userADSI.SetInfo()
```

Le script ci-dessus permet la création d'un utilisateur. L'utilisateur créé a, comme login, Powerswila et comme mot de passe P@ssw0rd, il ne peut modifier son mot de passe et celui-ci n'expire jamais. Ensuite, cet utilisateur est ajouté aux groupes *Users* et *MonGroupe* (par défaut il n'appartient à aucun groupe). Enfin, on modifie le chemin vers son profil et son chemin de base. Cette dernière partie est réalisée avec des objets ADSI puisque cette possibilité ne semble pas (encore) possible avec la nouvelle cmdlet *New-LocalUser*. Il ne faut surtout pas oublier d'appeler la méthode *SetInfo* qui va fixer la nouvelle valeur des paramètres.

### 3.2.2 Le profil

Le profil de l'utilisateur est un espace disque où toutes les informations le concernant (fichiers personnels, fichiers de configuration, fichiers systèmes, ...) y sont stockées. Il s'agit donc d'un élément important puisque ces données constituent le paramétrage de cet utilisateur. On y trouve également le dossier spécifique contenant son bureau, ses documents, ses images, son fond d'écran, etc.

Nous verrons que, dès qu'on utilise une authentification centralisée, l'emplacement du profil est un élément important.

---

<sup>9</sup> basé sur : <http://powershell.com/cs/forums/t/6215.aspx?PageIndex=1>

### Création du profil

Lors de la première connexion d'un utilisateur, le système va lui créer un nouveau profil en prenant le profil par défaut comme exemple. Une fois le profil créé, il devient celui de cet utilisateur et seul ce dernier peut en modifier les paramètres.

Par défaut, les profils sont conservés dans le dossier C:\Users. On y trouve les profils suivants :

Dossiers	Signification
Administrateur	Profil de l'administrateur système dont le login est <i>Administrateur</i> .
Public	Contient les données pour tous les utilisateurs (icônes sur le bureau de tous les utilisateurs, menu démarrer partagé pour tous les utilisateurs, ...)
Default User	Contient le profil « type » utilisé pour la duplication et la création d'un nouveau profil utilisateur (lors de sa première connexion).
All Users	Est maintenu pour une compatibilité avec les systèmes pré-Vista.

### Types de profil

Le profil de l'utilisateur peut être :

Type	Description
Local	Les informations de l'utilisateur sont stockées dans le dossier associé à cet utilisateur. Toutes les modifications réalisées par l'utilisateur sont enregistrées dans son profil.
Obligatoire	Le profil est <i>pré-configuré</i> et <b>ne peut pas être modifié par l'utilisateur</b> . Ainsi, toute modification du profil est perdue. Ce type de profil est utile lorsqu'un compte est partagé entre plusieurs personnes (par exemple : compte <i>guest</i> ).
Temporaire	Un profil <i>temporaire</i> est créé par le système lorsqu'il y a un problème d'accès au profil de l'utilisateur. Le profil temporaire est détruit après la fermeture de la session. A l'inverse d'un profil obligatoire, il ne s'agit pas ici d'un profil pré-configuré mais bien d'un profil créé de manière temporaire.

Par défaut, le profil est *local*. Si l'on veut obtenir un profil *obligatoire*, il faut **renommer**, une fois la configuration terminée, le fichier NTUSER.DAT en NTUSER.MAN. Ce profil devient alors *obligatoire* et tout changement réalisé par l'utilisateur dans son profil (bureau, paramètres, ...) est perdu.

Le dossier contenant le profil dépend des paramètres ajoutés au compte utilisateur. Si l'utilisateur est *local* et qu'aucun dossier n'a été mentionné dans son compte, son profil est sauvegardé dans le dossier local C:\Users. Si un dossier est précisé dans le compte utilisateur, le profil sera stocké dans le dossier mentionné **suffixé soit** par « .v2 » (Windows < 10 version 1607), **soit** par « .v6 » (Windows 10 >= 1607, Windows Server 2016)<sup>10</sup>. En effet, le dossier mentionné peut contenir un profil « ancienne génération » (pré-Vista sans le suffixe, ...) tandis que le dossier suffixé par « .v6 » contient les informations pour les versions les plus récentes de Windows 10.

<sup>10</sup> Une modification du registre peut causer la création de multiples versions du dossier profil en fonction du système d'exploitation client : extension « .v2 » (Windows Vista, Windows 7), « .v3 » (Windows 8), « .v4 » (Windows 8.1), « .v5 » (Windows 10 version < 1607) ou « .v6 » (Windows 10, version >= 1607).

### 3.3 Le système de fichiers

Les serveurs Windows peuvent utiliser plusieurs disques (ou volumes). Les volumes pris en charge peuvent être des disques *simples*, des disques *en RAID*, ... Le matériel supporté est relativement vaste.

Chaque volume peut être découpé en partition précise. La gestion des disques et des partitions est accessible depuis l'élément **Storage > Disk Management** de l'outil **Computer Management** disponible dans le **Server Management**. Grâce à cette interface, on peut :

- Voir tous les disques connectés au système
- Agrandir / Réduire un volume
- Formater un volume

Il faut être prudent car il y a des risques de perte d'information en cas de mauvaises manipulations.

Lors du formatage d'un volume (disque local, clé USB, ...) il faut mentionner **le système de fichiers** à utiliser. Microsoft utilise, depuis de nombreuses années, le système de fichiers NTFS. Ce système de fichiers, à l'inverse des systèmes FAT, **permet d'ajouter des permissions à chaque objet** présent sur le système. Ainsi, il est possible de limiter l'accès à des fichiers et/ou des dossiers en fonction de l'utilisateur connecté.

Pour ce faire, Windows utilise des ACL (liste de contrôle d'accès) pour limiter et contrôler les droits qui sont positionnés. En plus, chaque objet **hérite** des droits d'accès de son conteneur parent. Ainsi, si je crée un fichier dans un dossier qui n'est pas accessible à l'utilisateur *Powerswila*, le fichier hérite de cette propriété automatiquement.

En plus des permissions de type ACL, le système de fichiers permet d'ajouter **des attributs**. Ainsi, chaque objet sur le système de fichier peut posséder l'attribut *Lecture seule* (qui s'applique uniquement aux fichiers) qui empêche toute modification du fichier, *caché* qui cache le dossier sauf si l'utilisateur a mentionné qu'il souhaitait les voir, *système* qui mentionne que le fichier/dossier est de type système (utilisé par le système d'exploitation seulement), *archive* (qui était utilisé pour déterminer les fichiers qui avaient été modifiés depuis la dernière sauvegarde).

Avant de continuer, il est bon d'activer la visualisation des fichiers cachés et systèmes comme suit : dans l'explorateur, choisir le menu **View** puis **Options (à droite)** puis **Change folder and search options**. Choisir ensuite l'onglet **View** et ajuster les options *Show hidden files, folders and drives*, **désactiver** *Hide extensions for known file types* mais aussi *Hide protected operating system files*. Ainsi tous les fichiers/dossiers apparaîtront dans l'explorateur de fichier.

#### 3.3.1 Visualiser les attributs et permissions

Pour visualiser les permissions actives sur un objet, il faut simplement sélectionner celui-ci puis faire un **clic-droit** et choisir **Properties**.

L'onglet **General** reprend les informations courantes du fichier / dossier mais également ses attributs. L'onglet **Security** reprend les permissions ACL de ce fichier / dossier.

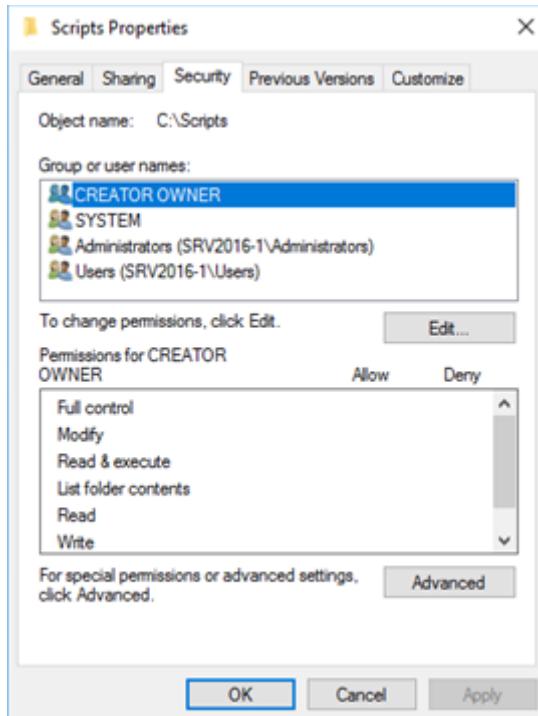


Figure 3.3 : Exemple de permissions sur le dossier C:\Scripts

Comme nous pouvons le voir sur la figure 3.3, la fenêtre reprenant les permissions est présentée en deux panneaux : le panneau supérieur reprend les utilisateurs disposant de permissions ou autorisations particulières. Le volet inférieur mentionne les autorisations accordées pour cet utilisateur.

Comme nous pouvons le voir, il y a des utilisateurs et des groupes courants :

Désignation	Explication
CREATOR OWNER	Cet intitulé reprend le créateur de l'objet en question (scripts dans notre exemple). Le propriétaire a, par défaut, des droits complets sur les objets qu'il possède.
SYSTEM	Cet utilisateur est utilisé par le système d'exploitation pour des tâches spécifiques. Il convient de ne pas toucher à ces permissions
Administrators	Reprend les autorisations associées au <b>groupe</b> des administrateurs (remarquez le « s », >< de l'utilisateur administrator). Il est possible de limiter les droits pour ce groupe. Cependant, un administrateur peut toujours reprendre la propriété d'un objet et, dès ce moment, en modifier les permissions.
Users	Reprend les autorisations associées au groupe des utilisateurs.

Si l'on clique sur le bouton **Advanced** en bas de la fenêtre, on arrive sur une autre fenêtre qui décrit plus complètement les permissions et d'où elles viennent.

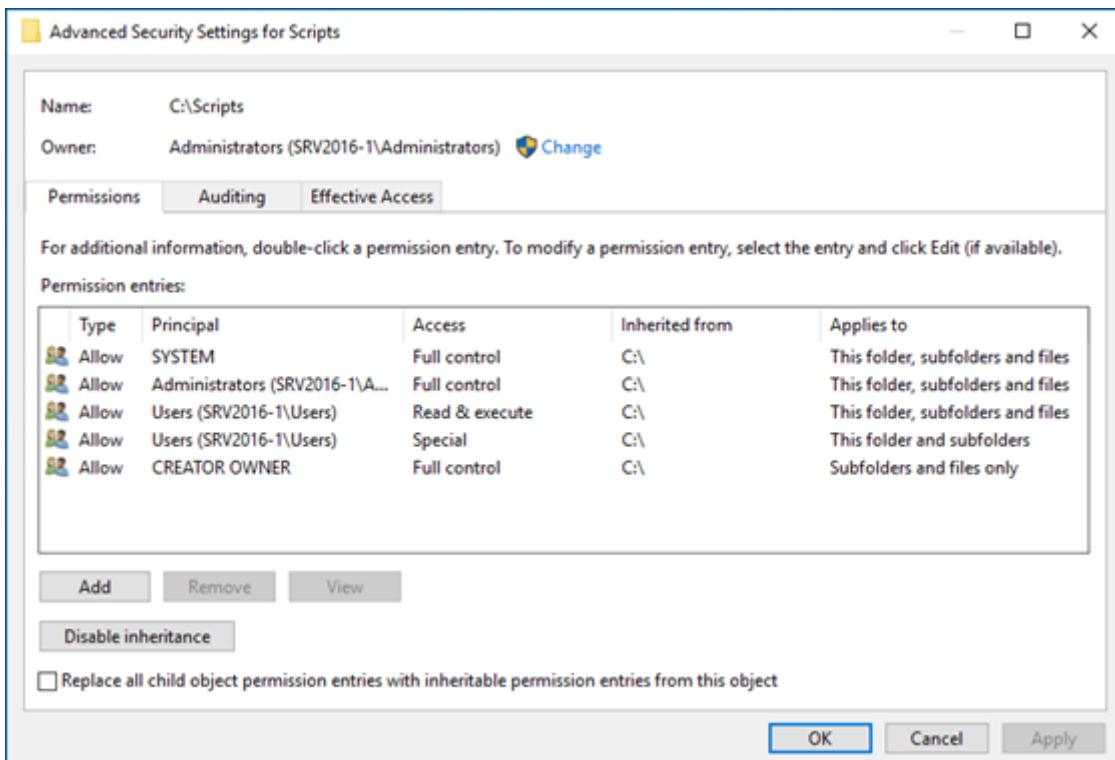


Figure 3.4 : Permissions avancées pour le dossier C:\scripts

La figure 3.4 nous montre comment les *permissions avancées* sont présentées. On peut y voir que, par exemple, *CREATOR OWNER*, *SYSTEM* et *Administrators* (2<sup>ème</sup> colonne) ont une autorisation de type *Full control* (3<sup>ème</sup> colonne) sur ce dossier, les sous-dossiers et fichiers (5<sup>ème</sup> colonne : *This folder, subfolders and files*).

Les membres de *Users* (2<sup>ème</sup> colonne) ont une autorisation *lecture et exécution* (3<sup>ème</sup> colonne : *Read & execute*) sur ce dossier, les sous-dossiers et fichiers (5<sup>ème</sup> colonne). On remarque également que les membres de *Users* ont des autorisations *spéciales* (notée *Special*). De plus, ces autorisations *spéciales* portent sur ce dossier, les sous-dossiers (5<sup>ème</sup> colonne : *This folder and subfolders*).

Enfin, on peut lire que toutes ces autorisations sont **héritées** de C:\ (colonne *Inherited from*).

### Comment comprendre ces autorisations ?

Tout d'abord, faisons un rapide état des lieux des autorisations courantes (extrait de [1]<sup>11</sup>) :

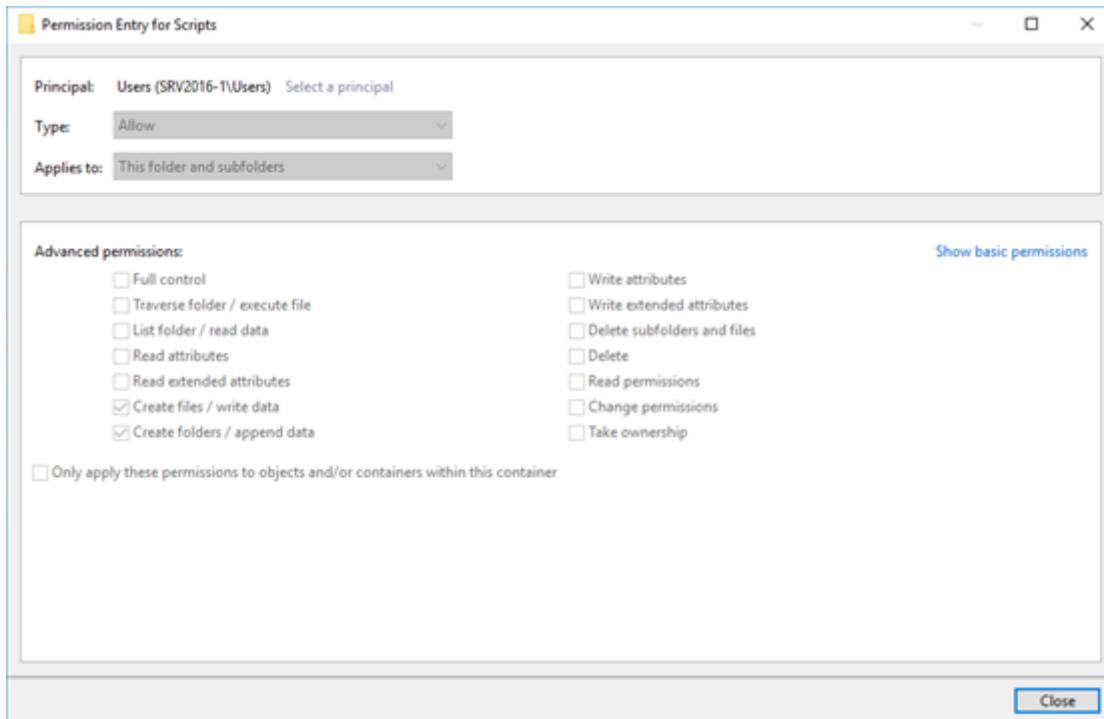
Autorisation	Description
Read	Peut voir le contenu d'un dossier et ouvrir des fichiers. Il ne peut pas exécuter les programmes présents.
Read & Execute	Peut voir le contenu d'un dossier et ouvrir des fichiers. En outre, il peut exécuter les programmes présents.
Write	Peut créer des fichiers dans un dossier mais pas nécessairement les lire. Cette permission est intéressante pour la création d'un dossier dans lequel plusieurs utilisateurs peuvent déposer des fichiers sans avoir accès aux fichiers déposés par les autres (ex. : depot-labo)
Modify	Peut lire, modifier et supprimer des fichiers et dossiers (ex. C:\AdmSys)
Full Control	Peut réaliser toutes les opérations, y compris changer les permissions.

<sup>11</sup> Voir « Référence bibliographique » au début de la leçon.

## Special

## Autorisation personnalisée

Les autorisations spéciales sont donc une personnalisation. Voici quelques éléments :



Ainsi, l'autorisation *Read & execute* reprend les éléments suivants : *PTraverse folder / execute file, list folder / read data, Read attributes, Read extended attributes et Read permissions.*

Une autorisation peut s'appliquer à :

Désignation	Explication
<b>This folder, subfolders and files</b>	L'autorisation s'applique à ce dossier et sera héritée par tous les objets (dossiers et fichiers) créés dans ce dossier.
<b>This folder only</b>	L'autorisation s'applique à ce dossier seulement. Elle ne sera pas héritée par les objets présents dans le dossier.
<b>This folder and subfolders</b>	L'autorisation s'applique à ce dossier et sera héritée par tous les dossiers qui seront créés dans ce dossier.
<b>This folder and files</b>	L'autorisation s'applique à ce dossier et sera héritée par tous les fichiers présents dans ce dossier.
<b>Subfolders and files only</b>	L'autorisation sera héritée par tous les objets (dossiers et fichiers) créés dans ce dossier. Cependant, elle ne s'applique pas au dossier lui-même.
<b>Subfolders only</b>	L'autorisation sera héritée par tous les dossiers créés dans ce dossier. Cependant, elle ne s'applique pas au dossier lui-même.
<b>Files only</b>	L'autorisation sera héritée par tous les fichiers présents dans ce dossier. Cependant, elle ne s'applique pas au dossier lui-même.

Comme nous pouvons le voir, la compréhension des permissions n'est pas aisée car il y a beaucoup (trop) de possibilités.

### 3.3.2 Modification des permissions

La modification des permissions peut prendre deux formes très différentes :

1. Ajouter/Retirer des autorisations pour des utilisateurs donnés. Donc *aucune modification aux permissions héritées*.
2. Modifier les permissions héritées

#### Ajouter / modifier des autorisations

S'il s'agit d'ajouter/retirer des autorisations, cela peut se faire très facilement en suivant les étapes suivantes :

1. **Clic-droit** sur l'objet pour lequel des permissions doivent être ajoutées, puis **Properties**
2. Onglet **Security** et choisir le bouton **Edit**.
3. Choisir **Add** puis entrer le nom du groupe ou de l'utilisateur dont il faut adapter les permissions puis choisir **Check names** afin de s'assurer que celui-ci existe, puis choisir **OK**<sup>12</sup>
4. Les autorisations pour l'élément ajouté peuvent ensuite être précisées dans le panneau du bas.

#### Modifier les autorisations héritées

Modifier des autorisations héritées impose une étape supplémentaire. En effet, il faut **bloquer l'héritage** des permissions avant de pouvoir réaliser une quelconque modification. Pour ce faire, il faut suivre les étapes suivantes :

1. **Clic-droit** sur l'objet pour lequel des permissions doivent être ajoutées, puis **Properties**
2. Onglet **Security** et choisir le bouton **Advanced**.
3. Cliquer sur le bouton **Disable inheritance**.
  - a. Le système vous informe que dans ce cas, les autorisations ne seront pas héritées et vous demande ce qu'il doit faire des autorisations actuelles.
  - b. Le plus souvent, il suffit de choisir l'option **Convert inherited permissions into explicit permissions on this object** qui va ainsi copier les permissions héritées et permettre de les modifier. Le bouton **Remove all inherited permissions from this object** retire toutes les autorisations héritées et l'administrateur doit alors les définir à nouveau.
4. Appuyer sur le bouton **Apply** puis **OK** pour fermer la fenêtre *Advanced Security Settings*.
5. Cliquer sur le bouton **Edit** dans le panneau du haut
6. Il est désormais possible de modifier les permissions des utilisateurs

---

<sup>12</sup> Vous pouvez également choisir **Avancé** et préciser les paramètres de votre recherche et choisir **Rechercher**. Vous pouvez alors effectuer votre choix parmi la liste proposée.

### Gérer le propriétaire d'un objet

Le propriétaire (ou CREATOR OWNER) est visible et peut être modifié comme suit :

1. **Clic-droit** sur l'objet pour lequel des permissions doivent être ajoutées, puis **Properties**
2. Onglet **Security** et choisir le bouton **Advanced**.
3. Dans le panneau du haut, l'option **Owner** montre le propriétaire actuel de l'objet et le bouton **Change** permet de changer celui-ci.

Ainsi, il est possible de s'approprier un objet. Cette option est indispensable dans certains cas quand l'administrateur doit reprendre la main sur un objet pour lequel tous les droits d'accès lui ont été supprimés.

### 3.3.3 Commandes et scripting

La gestion des ACL (et donc la modification des permissions ou autorisations) peut se faire au moyen du programme **icacls.exe**. Ce programme permet de réaliser bon nombre d'opérations, l'aide est disponible en tapant **icacls.exe /?**.

Ainsi, si nous créons le dossier C:\testACL, il hérite par défaut des ACL placées sur le disque C:. On peut donc bloquer l'héritage et configurer des ACL particulières pour l'utilisateur powerswila :

```
C:\> icacls testACL /inheritance:d
```

Cette commande bloque l'héritage et copie les ACL

```
C:\> icacls testACL /grant powerswila:(M)
```

Cette commande ajoute l'autorisation en modification sur le dossier seulement. Voir l'aide de **icacls** pour plus d'information.

```
C:\> icacls testACL /grant powerswila:(OI)(CI)(F)
```

Cette commande ajoute l'autorisation contrôle total sur le dossier, les sous-dossiers et les fichiers.

En PowerShell, deux possibilités s'offrent à nous : **l'exécution directe** d'une commande externe ou l'utilisation de cmdlets particulier. Pour l'*exécution directe* (i.e. appel à la commande **icacls** depuis un script PowerShell), il suffit de faire comme suit :

```
$resultat= &"icacls" "testACL" "/grant" "powerswila:(OI)(CI)(F)"
```

Bien sûr, il est possible d'utiliser directement des objets particuliers, disponibles en PowerShell pour modifier les ACL.

Voici un premier script introductif<sup>13</sup> de modification des ACL pour le dossier C:\testACL :

```
$autorisation= [System.Security.AccessControl.FileSystemRights]"Modify"  
$heritage= [System.Security.AccessControl.InheritanceFlags]::None  
$propagation= [System.Security.AccessControl.PropagationFlags]::None  
$decision= [System.Security.AccessControl.AccessControlType]::Allow  
  
$utilisateur = New-Object System.Security.Principal.NTAccount("powerswila")  
  
$acl= Get-Acl "C:\testACL"  
$ace= New-Object Security.AccessControl.FileSystemAccessRule($utilisateur,`  
$autorisation, $heritage, $propagation, $decision)
```

<sup>13</sup> Extrait de <http://technet.microsoft.com/en-us/library/ff730951.aspx>

```
$acl.AddAccessRule($ace)
Set-Acl "C:\testACL" $acl
```

Dans ce script, nous **ajoutons** une entrée ACL (appelée dans le script \$ace) au dossier C:\testACL. Cette entrée concerne :

- Un utilisateur System.Security.Principal.NTAccount("powerswila")
- Une autorisation [System.Security.AccessControl.FileSystemRights]"Modify"
- Aucune option d'héritage, ni de propagation :  
[System.Security.AccessControl.InheritanceFlags]::None  
[System.Security.AccessControl.PropagationFlags]::None
- Une décision [System.Security.AccessControl.AccessControlType]::Allow

Après exécution de ce script, l'utilisateur PowerSwila se voit *ajouter* une autorisation de *modification* sur *le dossier uniquement* C:\testACL.

Voici les valeurs possibles pour les **autorisations** (FileSystemRights): AppendData, ChangePermissions, CreateDirectories, CreateFiles, Delete, DeleteSubdirectoriesAndFiles, ExecuteFile, FullControl, ListDirectory, **Modify**, Read, ReadAndExecute, ReadAttributes, ReadData, ReadExtendedAttributes, ReadPermissions, Synchronize, TakeOwnership, Traverse, **Write**, WriteAttributes, WriteData, WriteExtendedAttributes

Les valeurs pour la **propagation** sont : InheritOnly, NoPropagateInherit et None. Pour **l'héritage**, les valeurs possibles sont : ContainerInherit, ObjectInherit et None. En fonction de la portée souhaitée, il faut combiner<sup>14</sup> ces deux valeurs *propagation* et *héritage* comme suit :

	Héritage	Propagation
This folder only	None	None
This folder, Subfolders and files	Container Object	None
This folder and subfolders	Container	None
This folder and files	Object	None
Subfolders and files only	Container Object	InheritOnly
Subfolders only	Container	InheritOnly
Files only	Object	InheritOnly

Dans le tableau précédent, il faut comprendre Container|Object comme étant une opération OU bit à bit. En PowerShell, cela se traduirait par une ligne du type :

```
$heritage= `'
[System.Security.AccessControl.InheritanceFlags]::ContainerInherit -bor `'
[System.Security.AccessControl.InheritanceFlags]::ObjectInherit
```

### 3.3.4 La gestion des quotas

Windows Server 2016 supporte deux types de quota :

- **Les quotas disques** : il s'applique sur un volume complet prennent en compte l'occupation de l'espace par les utilisateurs. Des entrées de quota, par utilisateur, peuvent être configurées.

<sup>14</sup> Repris de <http://stackoverflow.com/questions/3282656/settings-inheritance-and-propagation-flags-with-set-acl-and-powershell>

- **Les quotas sur un chemin donné** : il s'applique à un dossier ou des sous-dossiers. La portée de ces quotas est plus fine. Il est possible de définir un *modèle de quota* qui s'appliquera sur le dossier en question.

Pour configurer les quotas sur base d'un chemin donné, il faut **installer un rôle supplémentaire**, pour ce faire, aller dans **le Server Manager**, choisir **Manage > Add Roles and Features**. Dans la liste des **rôles** disponibles, il faut déployer **File and Storage Services** et, ensuite, déployer **Files and iSCSI Services**, il convient d'installer le **File Server Ressource Manager** (et accepter toutes les dépendances). Une fois ce rôle ajouté, une nouvelle option apparaît dans le menu **Tools** s'appelant **File Server Resource Manager**.

### Les quotas disques

Il est possible de définir des quotas sur le disque dur. Les quotas sont des limites imposées par utilisateur quant à l'espace disque. Ils sont particulièrement intéressants pour s'assurer que l'utilisateur ne dépasse pas une limite donnée. Ils sont indispensables pour les ressources partagées entre plusieurs utilisateurs.

Pour **activer** les quotas, il faut aller dans **Démarrer > This PC**. Il faut, ensuite, faire un **clic-droit** sur le volume concerné (C: par exemple) et choisir **Properties**.

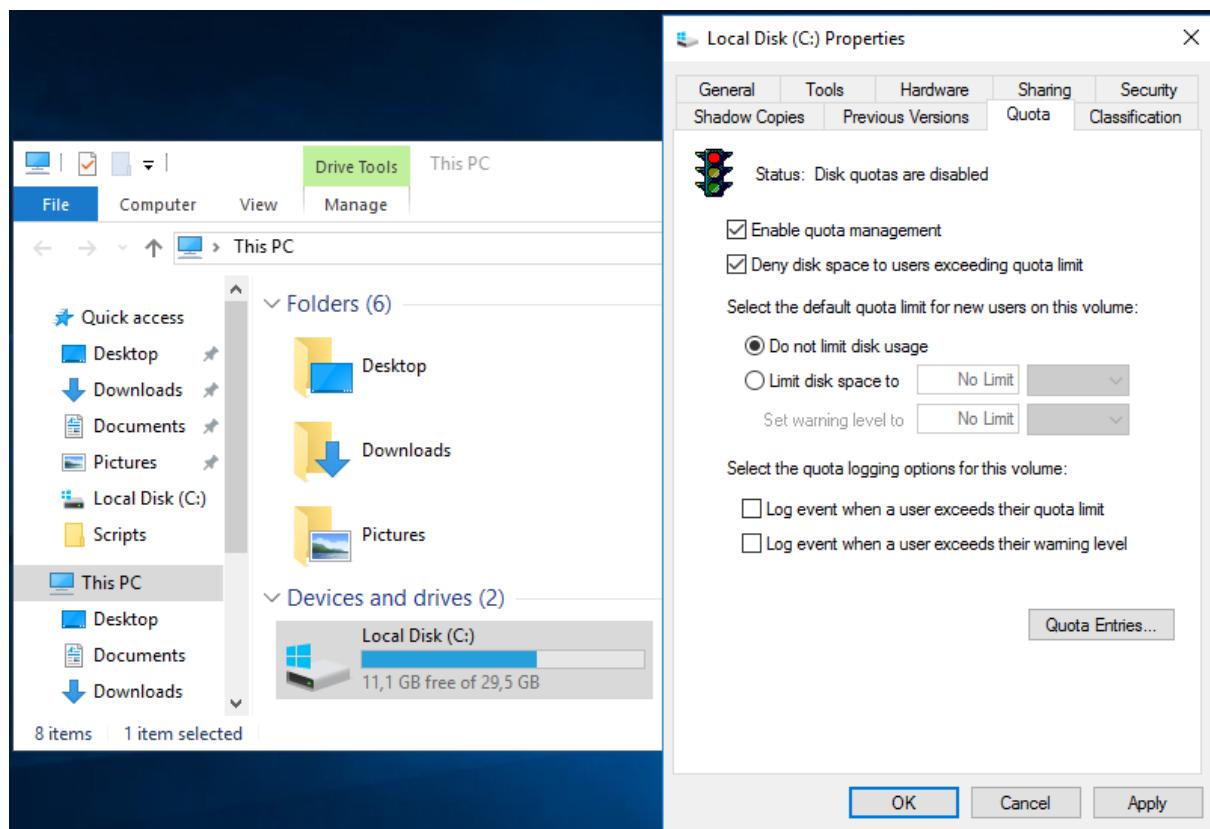


Figure 3.5 : Gestion des quotas

Il faut alors choisir **l'onglet Quota** (voir figure 3.5) et cocher **Enable quota management** ainsi que **Deny disk space to users exceeding quota limit**. Une fois que l'on confirme la gestion des quotas, ceux-ci sont actifs sur le disque concerné.

Il faut remarquer que si l'on ne définit pas d'**entrées de quota** (figure 3.5, bouton en bas à droite, *Quota Entries...*), aucune limite n'est observée sur le système.

Il est possible de définir une *limite par défaut* (figure 3.5, *limit disk space to*) pour les nouveaux utilisateurs. Cette limite s'applique alors à tous les nouveaux utilisateurs déposant un fichier sur le disque concerné. Ensuite, il est possible de spécifier des entrées particulières, par utilisateur, grâce au bouton **Quota Entries**.

Une fois dans la fenêtre montrant les **entrées de quotas**, il faut choisir l'option **New quota entry** et fixer les limites voulues. Le quota est alors actif pour cet utilisateur **sur tout le volume**.

**En ligne de commande**, il est possible de fixer les quotas disques en utilisant la commande **fsutil quota**.

Cette commande permet de :

- Activer/Désactiver les quotas sur un volume
- Activer l'application des quotas
- Ajouter ou modifier des entrées de quota

Cette dernière option est particulièrement intéressante lorsqu'on crée des scripts d'ajout des utilisateurs, on peut ainsi créer les entrées de quotas correspondantes. Surtout si la politique de quota est différente en fonction des utilisateurs (un utilisateur d'une orientation donnée pourrait ne pas avoir les mêmes quotas qu'un autre).

```
C:\> fsutil quota modify /?
```

Cette commande explique comment utiliser cette option pour ajouter ou modifier une entrée de quota. Par exemple, si nous voulons ajouter une entrée de quota pour l'utilisateur *powerswila* sur le disque C:, il faut entrer la commande suivante :

```
C:\> fsutil quota modify C: 900000000 1000000000 powerswila
```

Cette commande permet d'ajouter une entrée de quota pour l'utilisateur *powerswila* sur le volume C: avec un seuil d'avertissement autour<sup>15</sup> de 900 Mo et une limite autour de 1000 Mo.

**Powershell !** Il est facile d'intégrer cette commande dans un script *Powershell en exécution directe*. Pour ce faire, il faut simplement précéder la commande du symbole « & ». A l'intérieur d'un script Powershell, nous obtiendrons :

```
$resultat = &"fsutil" "quota" "modify" "C:" "900000000" "1000000000"  
"powerswila"
```

Tous les arguments sont séparés par des espaces et des guillemets. Le résultat de la commande se trouve dans la variable \$resultat.

### **Les quotas sur un chemin donné**

L'interface permettant de définir *les quotas sur un chemin donné* se trouve dans **Server Manager > Tools > File Server Resource Manager**. Avant de pouvoir fixer un quota sur un chemin déterminé, il convient de déterminer la **politique spécifique** à appliquer (au moyen d'un *template*). La présence des

---

<sup>15</sup> Par facilité, j'ai compté ici le Mo à 1000 000 o ce qui n'est pas correct. Pour rappel, 1 Mo = 1024\*1024 octets

modèles de quota (**Quota Templates**) sont une réelle avancée en termes de granularité (**Quota Management > Quota Templates**).

Un modèle de quota peut reprendre :

- Une limite **soft** (qui est principalement utilisée pour les notifications et les rapports) ou une **limite hard** (qui ne peut être dépassée)
- Des *seuils de notification* (**Notifications thresholds**) exprimés en pourcentage de la limite. A chaque seuil, on peut définir :
  - Un mail qui est envoyé automatiquement à l'utilisateur pour lui notifier que le seuil a été atteint (colonne E-mail)
  - Un événement qui sera consigné dans le journal pour permettre aux administrateurs de suivre l'évolution (colonne Event)
  - Une commande à exécuter qui permet à l'administrateur de faire tout ce qu'il veut (colonne Command). Ainsi, certains modèles de quota proposent une extension unique de 50 Mo par l'exécution de la commande dirquota (voir plus loin).

Comme nous pouvons le voir, il est facile de définir un modèle de quota. Une fois les modèles nécessaires définis, il faut les faire appliquer à des chemins particuliers.

Pour ce faire, il faut aller dans **Quota** pour **Create Quota**. Lors de l'ajout, il faut mentionner :

- *Quota path* – le dossier qui est visé par le quota que nous allons créer.
- S'il s'agit d'un *Quota on a path* (s'applique donc au dossier mentionné, dans sa globalité) ou s'il s'agit d'un quota automatique *Auto apply template and create quotas on existing and new subfolders* (auquel cas, tous les dossiers existants et nouveaux se verront définir le quota en fonction du modèle choisi).
- Lier le modèle de quota définissant la politique choisie (via *Derive properties from this quota template*)

Dès qu'on appuie sur **Create**, l'entrée est ajoutée et active.

Par exemple, si je crée le dossier C:\testQuota, je peux lui attribuer le quota comme suit :

- *Quota path* : C:\testQuota
- *Create quota on path*
- *Derives properties from this quota template* : 200 Mb Limit with 50 MB Extension

Dans ce mode, le dossier C:\testQuota peut occuper une taille maximale de 250 Mo.

Si on supprime l'entrée précédente et que nous la remplaçons par la suivante :

- *Quota path* : C:\testQuota
- *Auto apply template and create quotas on existing and new subfolders*
- *Derives properties from this quota template* : 200 Mb Limit with 50 MB Extension

Dans ce mode, tous les dossiers présents ou créés dans C:\testQuota se verront attribuer un quota automatiquement et chacun pourra occuper une taille maximale de 250 Mo. Intéressant pour fixer un quota sur le dossier contenant l'ensemble des répertoires personnels des utilisateurs.

En ligne de commande, il est possible de définir des quotas sur un chemin déterminé au moyen de la commande `dirquota`.

Pour les quotas qui s'appliquent sur le dossier directement :

```
C:\> dirquota quota /?
```

Cette commande affiche l'aide en ligne pour ce type de quota.

Pour les quotas automatiques (quotas créés automatiquement sur les sous-dossiers) :

```
C:\> dirquota autoquota /?
```

Cette commande affiche l'aide en ligne pour ce type de quota.

Dans la suite, vous trouverez quelques exemples d'utilisation, pour plus d'information, veuillez-vous reporter à la documentation.

```
C:\> dirquota quota add /path:C:\testQuota /SourceTemplate:"200 Mb Limit with 50 MB Extension"
```

Cette commande ajoute une entrée de quota pour le dossier `C:\testQuota` en lui appliquant le modèle mentionné.

```
C:\> dirquota autoquota add /path:C:\testQuota /SourceTemplate:"200 Mb Limit with 50 MB Extension"
```

Cette commande ajoute un quota automatique pour le dossier `C:\testQuota` en lui appliquant le modèle mentionné.

En **Powershell**, il est possible de scripter facilement ce type de quotas. Pour les quotas définis sur un chemin précis, il suffit<sup>16</sup> de faire comme suit :

```
$fqtm = New-Object -com Fsrm.FsrmQuotaManager  
$quota = $fqtm.CreateQuota("C:\testQuota")  
$quota.ApplyTemplate("200 Mb Limit with 50 MB Extension")  
$quota.Commit()
```

Pour les quotas automatiques, c'est tout aussi simple<sup>17</sup> :

```
$fqtm = New-Object -com Fsrm.FsrmQuotaManager  
$quota = $fqtm.CreateAutoApplyQuota("200 Mb Limit with 50 MB Extension",  
"C:\testQuota")  
$quota.Commit()
```

Bien sûr, il est aussi possible de faire appel à la commande `dirquota` depuis **Powershell en exécution directe** comme suit :

```
$resultat = &"dirquota" "autoquota" "add" "/path:C:\testQuota"  
"/SourceTemplate: 200 Mb Limit with 50 MB Extension"
```

### 3.4 La stratégie locale

Comme nous l'avons vu dans la leçon 1 concernant l'installation initiale, il existe une **stratégie locale** définissant beaucoup de paramètres concernant la *politique locale* du serveur. On y trouve,

<sup>16</sup> Extrait de : <http://blog.dboden.be/2009/03/managing-fsrm-by-using-powershell/>

<sup>17</sup> Extrait de : <http://www.simple-talk.com/sysadmin/exchange/implementing-windows-server-2008-file-system-quotas/>

notamment, la *stratégie concernant les mots de passe*. Nous allons maintenant explorer d'autres éléments de cette stratégie locale.

**Attention !** Les éléments de stratégies sont importants dans l'administration des serveurs Windows Server. Ainsi, lorsqu'un serveur intègre un réseau (précisément avec Active Directory), des stratégies globales peuvent s'appliquer sur la machine. Nous retrouverons donc les stratégies lors de notre étude d'Active Directory.

Pour modifier la stratégie locale, il faut aller dans le **Server Manager > Tools > Local Security Policy**.

Par exemple, il est possible de *ne pas afficher le dernier utilisateur qui s'est connecté* en modifiant la stratégie locale comme suit : **Security Settings > Local Policies > Security Options > Interactive login : Do not display last user name > Enabled**.

Il est également possible d'activer *un écran d'accueil* juste avant la procédure de connexion en modifiant les paramètres suivants : **Security Settings > Local Policies > Security Options > Interactive login : Message title for users attempting to log on** et **Interactive login : Message text for users attempting to log on**.

Enfin, on trouve également dans la stratégie de sécurité locale un dernier élément important : *la stratégie d'audit (Audit Policy)*. La stratégie d'audit permet de superviser des éléments importants du système. Les événements audités sont consignés dans les journaux systèmes. On peut ainsi auditer l'ouverture de la connexion (aussi bien la réussite que l'échec), les événements systèmes (modification de l'heure, les tentatives de démarrage/d'arrêt de certains éléments critiques, ...), les tentatives de modification des stratégies ...

Pour modifier ces paramètres, il faut suivre le chemin **Security Settings > Local Policies > Audit Policy**. Il est alors aisément d'activer les stratégies voulues dans le panneau de droite.

## 3.5 Divers

### 3.5.1 La console MMC

L'outil de **Computer Manager** est un exemple de ce que peut être la console MMC. Il s'agit d'un composant à l'intérieur duquel l'administrateur peut ajouter des *Snap-in* (ie. Des composants). Ces composants sont prévus pour fonctionner dans la console. L'intérêt d'utiliser la console est double :

- L'administrateur peut personnaliser sa console avec les outils de gestion qu'il utilise
- La console peut lorsqu'elle ajoutée, se rapporter à l'ordinateur local, à un ordinateur distant ou parfois à un compte de service. Elle permet donc des modifications plus fines.

Pour démarrer la console MMC, il suffit de *rechercher et exécuter mmc.exe*. Une fois lancée, il faut choisir l'option *Add/Remove Snap-in* et choisir le composant souhaité, par exemple **Computer Management**. Lors de l'ajout, la console vous demande si l'on doit réaliser cet ajout pour l'ordinateur local ou un ordinateur distant. Le choix par défaut nous convient. On se retrouve donc avec une console de gestion reprenant l'outil de gestion des serveurs. Il est possible d'ajouter plusieurs éléments à l'intérieur de la console afin de regrouper les éléments souvent utilisés par l'administrateur.

Lorsque vous quittez cette console, un message vous demandant si vous souhaitez sauvegarder cette dernière s'affiche (il ne s'agit pas des modifications qui ont pu être effectuées mais simplement de la configuration de la console avec les composants enfichables ajoutés).

### 3.5.2 L'observateur d'événements

**Event Viewer** est l'outil permettant de consulter les journaux systèmes. Les journaux sont une mine d'information en cas de problèmes sur un serveur car ils renseignent (de manière pas toujours claire) la nature de l'erreur rencontrée. Ce doit être le premier réflexe de l'administrateur système lorsqu'un événement étrange survient : il faut consulter ces journaux pour déterminer s'est passé.

En plus, en précisant la *stratégie d'audit (Audit Policy)* souhaitée, les journaux vont également se souvenir des événements importants pour l'administrateur comme les tentatives (réussies ou ratées) d'ouverture de sessions, ...

Pour ouvrir l'observateur d'événements, il faut démarrer le **Server Manager> Tools > Event Viewer > Windows Logs**.

### 3.5.3 Planification de tâches

A l'instar des systèmes Linux, il existe également dans les systèmes Windows une possibilité pour planifier une tâche ponctuelle ou répétitive. Pour atteindre cet outil : **Server Manager > Tools > Task Scheduler**.

Il faut ensuite, dans la section **Task Scheduler Library**, créer une tâche et lui donner tous ses paramètres pour travailler.

## Exercices

### Création des comptes

1. En reprenant le fichier obtenu à l'exercice 1 de la leçon 2, écrivez un script Powershell permettant de créer les comptes des utilisateurs.
    - Le script fixera le mot de passe, le chemin d'accès local à C:\UserData\<login> ainsi que le chemin vers le profil à C:\UserData\<login>\myprofile.
    - Un groupe particulier sera créé par catégorie<sup>18</sup>. Tous les utilisateurs seront membres du groupe *Users* et du groupe spécifique correspondant à sa catégorie (*administratif-communication-comptabilité ...*)
    - Les dossiers suivants seront créés :
      - C:\UserData\<login>
      - C:\UserData\<login>\myprofile.V6
- Vous ajouterez une autorisation de type *contrôle total* à l'utilisateur sur ces dossiers.
- Vérifiez si tout s'est bien passé ! Tentez de vous connecter avec l'un des comptes créés.

(Conseil : testez votre script sur un nombre très réduit d'utilisateurs : les deux premiers par exemple)

<sup>18</sup> Pour déterminer si un groupe existe déjà, vous pourriez utiliser la cmdlet Get-LocalGroup avec un bloc try/catch.

2. Localisez le profil de l'utilisateur avec lequel vous vous êtes connectés. Jetez un œil aux données présentes à l'intérieur
3. Ecrivez le script qui permet de supprimer les comptes des utilisateurs créés précédemment.  
Pour ce faire, utilisez la cmdlet `Remove-LocalUser`
4. (Via l'interface graphique) Créez un compte *helmo*
  - o Sans mot de passe.
  - o Fixer le chemin le chemin d'accès local à `C:\UserData\helmo` et le profil dans `C:\UserData\helmo\preconfig`
  - o Créer les dossiers `C:\UserData\helmo` et `C:\UserData\helmo\preconfig.v6`. Fixer les droits pour que *helmo* dispose d'un *contrôle total* sur ces dossiers
  - o Connectez-vous avec ce login.
  - o Créer un lien vers le serveur DATA (`\\\192.168.128.3`) et placez ce raccourci sur le bureau.
  - o Transformer ce profil standard en profil obligatoire.
  - o Testez-le !

## Les quotas

5. Modifier le script d'ajout des utilisateurs pour que des quotas soient ajoutés en même temps.  
**Prévoyez deux versions** : l'utilisation des quotas disques et l'utilisation des quotas basés sur le chemin. Les quotas à respecter par catégories sont les suivants :
  - a. Administratif, social, comptabilité et direction : quota=400 Mo ; Alerte=390 Mo
  - b. E-Learning, étudiant, juridique et travaux: quota = 300 Mo ; Alerte à 290 Mo
  - c. Informatique, communication et personnel : quota = 800 Mo ; Alerte à 750 Mo

Il sera peut être nécessaire de modifier le script suivant le type de quota à adapter.

6. Vérifiez que les quotas sont effectivement appliqués.

## La stratégie locale

7. Activez la stratégie visant à *ne pas afficher le dernier utilisateur qui s'est connecté*. Redémarrez votre serveur. Quel changement observez-vous ?
8. Activez un écran et un message d'accueil comme suit :
  - a. Titre : Welcome on Windows Server 2016
  - b. Message : System Administrator : <VotreNom>



Fermez votre session et connectez-vous à nouveau. Qu'observez-vous ?

## Leçon 4 : Les partages

### 4. 1 Introduction

Dans cette leçon, nous allons étudier les **partages** disponibles sous Windows. Les deux principales ressources qui peuvent être partagées sont les *partages disques* et les *partages imprimantes*.

Nous aborderons les thèmes suivants :

- Rappels concernant les partages
- Configuration d'un partage disque
- Configuration d'un partage d'imprimante

### 4.2 Rappels concernant les partages

Sous les systèmes *Windows 2016* mais également *Windows 10 Professionnel*, il est possible de donner l'accès à une partie d'un disque dur à des utilisateurs au travers du réseau. Cette possibilité de configuration est très intéressante car elle permet l'échange de fichiers entre deux machines Windows très facilement.

Il faut bien se rendre compte que les partages sont liés à d'autres éléments du système :

- La configuration du firewall : si le firewall Windows (ou un autre) est actif, il est tout à fait possible que celui-ci bloque l'accès aux partages disques
- La sécurité NTFS : si les permissions définies sur le dossier partagé n'autorisent pas l'accès, il ne sera pas possible d'accéder à la ressource à distance.

Windows propose des *partages administratifs* qui sont **déjà configurés** et uniquement accessibles à l'administrateur et au système. Ainsi, il y a :

Nom du partage	Explication
C\$, D\$, E\$, ...	Partage disque, actif par défaut. Il est accessible à l'administrateur et permet d'avoir accès à distance au contenu du disque dur. Très utile pour rechercher / copier un fichier.
ADMIN\$	Partage utilisé par le système pour réaliser des tâches d'administration (installation à distance, ...)
IPC\$	Partage utilisé pour la connexion à une ressource

Bien sûr, l'administrateur peut configurer des partages supplémentaires accessibles aux utilisateurs. **Attention !** Pour vous connecter à un partage, il est nécessaire d'utiliser *un compte pourvu d'un mot de passe*. En effet, par défaut, Windows désactive toute utilisation de compte sans mot de passe à distance, ce qui est une sage précaution !

Lorsque vous tentez de vous connecter à un partage, **Windows tente une authentification automatique** en utilisant vos identifiants actuels sur la machine distante. Cela explique que parfois aucune authentification n'est demandée.

## 4.3 Configuration d'un partage disque

Pour configurer un partage disque, il faut naviguer sur le dossier que l'on souhaite partager et puis faire un **clic-droit** sur celui-ci et choisir **Properties**. Dans l'onglet **Sharing**, choisir l'option **Advanced Sharing**.

Il faut alors choisir **Share this folder** et entrer un nom dans **Share Name**. Ce nom apparaîtra dans l'explorateur réseau comme nom de la ressource. Enfin, il faut *modifier les autorisations* en cliquant sur **Permissions**. En effet, par défaut le partage est accessible à *tout le monde (Everyone)* en *lecture (Read)*. Ce mode de partage est très souvent inadapté et il convient de le modifier en fonction des besoins.

Ainsi, supprimer l'autorisation **Everyone** pour la remplacer par **Authenticated Users** est la première étape (il est nécessaire d'être identifié par le serveur pour pouvoir accéder au partage). Ensuite, il convient de déterminer le niveau d'autorisation pour le partage.

**Avertissement !** Il est possible de définir des autorisations sur le partage, comme sur le système de fichier. Il faut être conscient que **le système vérifie les deux autorisations** successivement :

1. La première vérification est réalisée au niveau des autorisations de partage : l'utilisateur remplit-il les conditions pour avoir accès à ce partage ?
2. La seconde vérification est réalisée par les sécurités NTFS : l'utilisateur peut-il obtenir l'accès souhaité à la ressource demandée ? Dispose-t-il des droits suffisants ?

Un conseil dans la gestion de ces droits et autorisations est de **rester simple**. Ainsi, il est conseillé de placer toutes les permissions voulues au niveau du système de fichiers (puisque celles-ci s'appliquent quelque soit le moyen d'accès) et de limiter les autorisations au niveau du partage lorsque c'est vraiment nécessaire.

Il est ainsi courant d'avoir **une permission large au niveau des autorisations du partage** (comme l'autorisation de modifier la ressource pour les utilisateurs authentifiés) **et avoir des permissions NTFS précises sur le dossier partagé**.

### 4.3.1 Mise en cache des dossiers partagés

Pour les utilisateurs nomades (portables, ...), l'accès aux fichiers partagés n'est, à priori possible que si l'ordinateur est connecté au réseau de l'entreprise. Cependant, Microsoft offre la possibilité de *mise en cache* des partages réseaux afin de permettre aux utilisateurs d'accéder à leurs documents même quand ils ne sont pas connectés au réseau de l'entreprise.

Le système s'occupe alors de **synchroniser** les fichiers modifiés lorsque l'utilisateur se connecte à nouveau au réseau. Cette possibilité consomme de l'espace disque sur le poste client et peut parfois poser des problèmes de synchronisation lorsqu'un même fichier a été modifié par plusieurs utilisateurs durant la même période de temps. Cependant, cette technique est assez aboutie pour qu'elle soit largement utilisée dans les entreprises.

Les options de mise en cache sont affichées lorsque l'administrateur clique sur le bouton **Caching** dans la fenêtre décrivant les autorisations sur un partage.

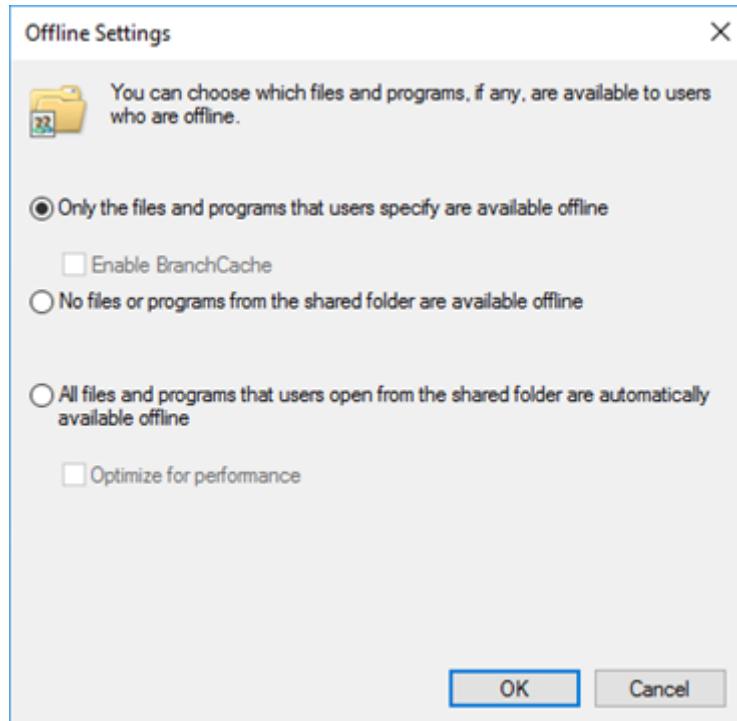


Figure 4.1 : Configuration de la mise en cache

Comme nous pouvons le voir sur la figure 4.1, les options suivantes se présentent à l'administrateur qui configure le partage :

- *Only the files and programs that users specify are available offline* : on laisse le soin à l'ordinateur client d'activer la synchronisation sur des fichiers et programmes précis. Cette option nécessite une compréhension du mécanisme de la part de l'utilisateur.
- *No files or programs from the shared folder are available offline* : on désactive cette option et aucune synchronisation n'est possible sur ce partage
- *All files and programs that users open from the shared folder are automatically available offline* : La mise en cache est alors automatique et se fait vers le poste de travail de l'utilisateur sans que ce dernier ne doive s'en préoccuper.

### 4.3.2 Accès à un dossier partagé

Pour accéder à un dossier partagé sur le réseau, il existe plusieurs techniques. La première, qui fonctionne bien pour les utilisateurs avertis, est, dans le champ de recherche du menu démarrer d'entrer la chaîne suivante : \\<nom\_du\_serveur>\nom\_du\_partage. Ainsi, pour avoir accès au partage `Public` sur le serveur `DATA`, il faut entrer : \\DATA\Public. Il est également possible, si le nom de la machine n'est pas connu ou résolu, d'utiliser l'adresse IP comme suit : \\<ip\_du\_serveur>\nom\_du\_partage. Ainsi, pour le serveur DATA dont l'adresse IP est 192.168.128.3, l'accès se fait comme suit : \\192.168.128.3\Public.

La seconde méthode consiste à naviguer en utilisant l'option `Réseau` de l'explorateur de fichiers. Les différentes machines accessibles s'affichent alors et il est possible de sélectionner la machine et le partage sur lequel on souhaite se connecter.

Enfin, pour les utilisateurs finaux, ces manières de procéder sont très souvent un peu ésoptériques. Ainsi, il est courant que les administrateurs configurent **des lecteurs réseaux** sur les postes des

machines. Ainsi, un nouveau lecteur apparaît dans le poste de travail pointant sur le chemin réseau souhaité. Pour l'utilisateur final, cette manière de procéder est bien plus simple car analogue à l'utilisation d'une clé USB, ...

Pour ce faire, il faut aller dans **File Explorer > This PC** et choisir le **menu Computer** puis l'option **Map network drive**.

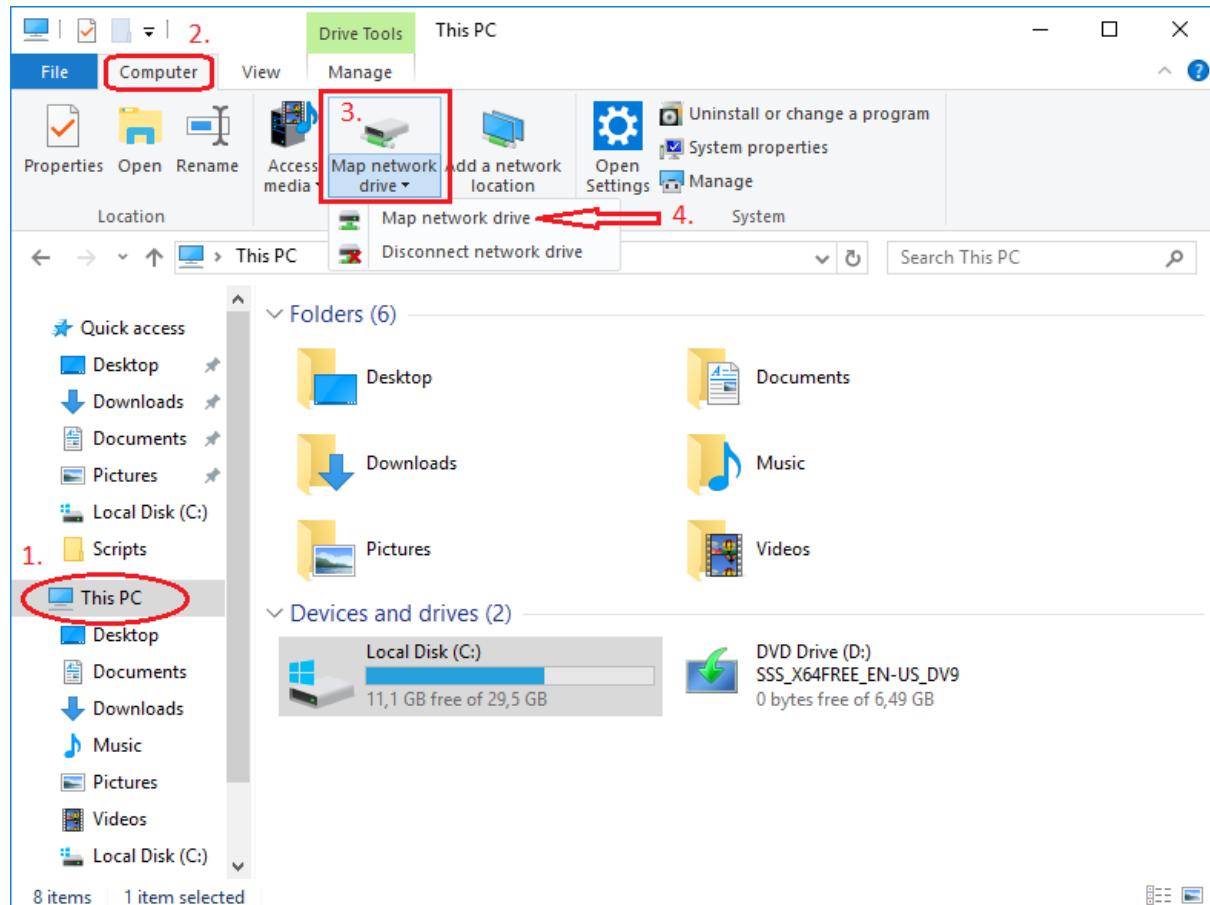


Figure 4.2 : Option pour connecter un lecteur réseau

Une fois cette option choisie, le système vous demande *le lecteur Drive* (i.e. la lettre choisie), *le dossier Folder* visé par la connexion et puis si *la reconnexion doit être faite automatiquement* (**Reconnect at sign-in**) ou encore s'il *faut utiliser d'autres identifiants que ceux courants* (**Connect using different credentials**) pour se connecter.

**Attention !** La connexion des lecteurs réseaux est une configuration **propre à l'utilisateur courant**. Ainsi, une connexion réalisée pour un utilisateur n'est pas visible pour un autre. Nous verrons plus tard comment cette connexion peut se faire automatiquement pour tous les utilisateurs qui ouvriront une session sur un ordinateur intégrant un domaine.

### 4.3.3 Visualiser les partages configurés

A première vue, il n'est pas facile de connaître les différents dossiers partagés configurés<sup>19</sup> sur un serveur. Il y a deux méthodes permettant de voir ces dossiers. La première est de passer par le **Server**

<sup>19</sup> On peut facilement connaître les différents partages (i.e. ce que le serveur propose via le réseau) mais pas les dossiers qui sont partagés.

**manager > menu Tools > Computer Management > Shared folders.** La seconde méthode est de recourir à un composant MMC (voir leçon 3). Pour ce faire, il faut démarrer la console MMC et puis **ajouter le snap-in** qui se nomme *Shared Folders*.

Dans les deux cas, nous avons chaque fois les noms des partages configurés, les chemins partagés et bien d'autres informations utiles.

#### 4.3.4 Scripting

La **ligne de commande** permet facilement la configuration et la connexion à des dossiers partagés. Ces commandes existent depuis de nombreuses années et font parties des choses que les administrateurs doivent connaître.

Les commandes importantes sont **net share /?**, **net view /?** et **net use /?**. Nous allons maintenant détailler certaines d'entre elles. Reportez vous à l'aide en ligne pour toute autre information.

```
C:\> net share monPartage=C:\partage /GRANT:"Authenticated Users",CHANGE  
/Cache:None
```

Cette commande permet de créer le partage *monPartage* pointant vers le dossier *C:\partage*. Les autorisations pour ce partage permettent à tous les utilisateurs authentifiés (ie. *authenticated users*) de modifier les informations (en fonction des permissions NTFS). Enfin, la mise en cache est désactivée.

```
C:\> net share monPartage /DELETE
```

Cette commande permet de supprimer un partage créé (nommé ici *monPartage*).

```
C:\> net view \\DATA
```

```
C:\> net view \\192.168.128.3
```

Cette commande permet de visualiser les partages disponibles sur un serveur donné (*DATA* dans notre exemple). Il est également possible de préciser l'adresse IP plutôt que le nom (surtout si le nom n'est pas connu dans le réseau concerné). Il se peut qu'une erreur « Access is denied » soit retournée. Dans ce cas, il faut d'abord faire une commande « *net use* » pour s'authentifier.

```
C:\> net use G: \\DATA\Public C:\> net use G: \\192.168.128.3\Public
```

Cette commande permet de **connecter un lecteur réseau**. Le lecteur *G:* est connecté au chemin réseau *\\DATA\\Public*. Il est aussi possible d'utiliser l'adresse IP plutôt que le nom de la machine.

```
C:\> net use
```

Cette commande permet de **lister tous les lecteurs réseaux connectés**.

```
C:\> net use G: /D
```

Cette commande permet de **supprimer un lecteur réseau connecté**.

En **Powershell**, il est aisément d'utiliser l'**exécution directe de commandes** pour établir, configurer ou supprimer un partage.

#### 4.4 Configuration d'un partage d'imprimante

L'autre partage particulièrement important est le partage d'imprimante. Ce partage permet d'installer une imprimante connectée à un serveur sur une machine cliente. Ainsi, les travaux d'impression sont transmis au serveur distant et gérés par celui-ci.

Pour **partager** une imprimante, il faut que celle-ci soit configurée sur le serveur et puis que l'administrateur décide de partager l'imprimante pour les utilisateurs. Pour partager une imprimante,

Il y a plusieurs méthodes : la première est de configurer ce partage durant l'installation du pilote d'impression. Cette option est très souvent présente. L'autre solution est de faire un **clic-droit** sur l'imprimante configurée et choisir **Printing preferences (Control Panel > Hardware > Devices and Printers)** et puis de réaliser la configuration. Celle-ci est semblable à un partage disque.

Pour **connecter une imprimante**, il faut se connecter au serveur partageant cette imprimante et faire un **clic-droit** puis **Connect** (il est également possible d'établir la connexion par un chemin réseau du type `\nom_du_serveur\nom_du_partage`). Si les pilotes sont disponibles sur le serveur, ceux-ci seront automatiquement installés sur le poste client. Une fois l'imprimante ajoutée, elle est visible dans le panneau de configuration.

## 4.5 Partages et comptes

Lorsqu'un utilisateur accède à un partage, le serveur distant lui demande de s'authentifier en fournissant un login et un mot de passe. Si le serveur distant est membre d'un domaine, il est nécessaire de mentionner qui réalise l'authentification : soit la machine, soit le domaine. Si l'on se connecte avec un compte du domaine (i.e. compte global), il faut mentionner `<nomDuDomaine>\<nomUtilisateur>` comme login. A l'inverse, si l'on se connecte avec un compte local, la connexion peut se faire par `<NomDeLaMachine>\<nomUtilisateur>` (si la machine fait partie du domaine ou simplement `<nomUtilisateur>` s'il s'agit d'un serveur autonome).

Cependant, dans certains cas, ces connexions sont automatiques :

- Si l'utilisateur a sauvegardé ses informations de connexion lors d'un accès précédent ;
- Si le login et le mot de passe de l'utilisateur courant existe sur le serveur distant, aucune demande de connexion n'est réalisée. En effet, Windows tente une connexion sur base des informations de l'utilisateur courant. Cette particularité est très intéressante pour faciliter les connexions des utilisateurs aux différentes ressources.

## 4.6 Exercices

1. Configurer un partage disque nommé « HR » qui pointe vers le dossier `C:\SharedHR` que vous aurez créé
  - a. Ce partage doit être accessible en modification aux membres du groupe `personnel` et en lecture aux membres de `direction` (voir leçon 3)
  - b. Testez votre configuration en utilisant l'hôte Windows pour y accéder
2. En **utilisant la ligne de commande**, accéder à votre dossier personnel sur `DATA`. Déconnectez-vous complètement du serveur en utilisant également la ligne de commande.
3. Configurer un compte à votre nom (matricule et mot de passe `HELMo`) sur votre serveur, connectez-vous et tentez une connexion sur les imprimantes partagées sur `DC`. Qu'observez-vous (par rapport à la connexion sur `DATA` à l'exercice précédent) ?
4. Pour le compte Administrateur de votre serveur, ajouter un lecteur réseau `H:` connectant votre dossier personnel sur `DATA` et activez la reconnexion automatique.

## Leçon 5 : services réseaux de base

### 5.1 Introduction

Dans cette leçon, nous allons étudier les services réseaux de base que sont le service DNS, le service DHCP et leur gestion. Avant d'entrer dans les détails de configuration de ces services, nous commencerons par un rappel succinct des éléments importants sous-jacent à chaque service étudié.

Nous aborderons dès lors les thèmes suivants :

- Rappel réseau IPv4 et IPv6
- Rappel concernant le service DNS
- Rappel concernant le service DHCP
- Installation et configuration du service DNS
- Installation et configuration du service DHCP

### 5.2 Rappels IP

Le protocole réseau utilisé est le protocole IP (Internet Protocol). Les deux versions principales de ce protocole sont IPv4 et IPv6. Il y a de grandes similitudes dans le fonctionnement de ces deux protocoles mais également de grandes différences.

En **IPv4**, les adresses sont codées sur 32 bits et représentées sous la forme *décimale pointée*. Ainsi, on groupe l'adresse par blocs de 8 bits qu'on transforme en décimal afin de pouvoir lire cette adresse facilement. IPv4 réserve des adresses spécifiques à des usages donnés. Ainsi :

Adresses	Usage
127.0.0.1	Adresse qui désigne toujours la machine courante. Cette adresse porte le nom de <i>localhost</i> . Elle permet de contacter un service qui s'exécute sur la même machine que le programme client
10.0.0.0/8	Ces adresses IP sont <i>locales</i> et réservées pour des réseaux internes. Elles sont utilisées par les utilisateurs pour connecter ensemble toutes les machines d'un réseau privé.
172.16.0.0/12	
192.168/16	
224.0.0.0 à 239.255.255.255	Adresses réservées au multicast. Ces adresses sont utilisées pour atteindre <i>un groupe de machines</i> . La même information arrive à l'ensemble des machines du groupe.

En **IPv6**, les adresses sont codées sur 128 bits et représentées sous une forme *hexadécimale* dans laquelle on sépare chaque groupe de 16 bits par le symbole « : ». Elles sont nettement moins lisibles que des adresses IPv4. Certaines adresses ont une signification particulière :

Adresses	Usage
::1	Adresse qui désigne la machine courante en IPv6. Elle porte également le nom de <i>localhost</i>
fe80::/10	Adresses locale-lien. Ces adresses sont attachées à une interface donnée. Elles ont une portée limitée au LAN (ne traverse pas les routeurs). Elles sont souvent configurées automatiquement.
fc00::/7	Adresses locale-unique. Ces adresses sont des adresses privées qui ne peuvent pas être routées sur l'internet.

2000 : : /3	Adresses globale-unique. Ce sont les adresses publiques que l'on retrouve sur l'internet. Elles sont uniques et attribuées par un ISP.
ff00 : : /8	Adresses multicast. Ces adresses sont utilisées dans bien des cas (déterminer l'adresse physique correspondant à une adresse IP déterminée, ...) quand il faut adresser une information à un groupe de machines.

En **IPv4**, le protocole **ARP** (Address Resolution Protocol) est utilisé pour trouver l'adresse physique correspondant à une adresse IP donnée (envoi d'une trame en broadcast sur le réseau en demandant : « Qui est le propriétaire de 192.168.190.2 »).

En **IPv6**, le protocole **NDP** (Neighbour Discovery Protocol) est utilisé pour découvrir ses voisins, construire une adresse IPv6 unique et connaître l'adresse physique d'une machine en fonction de son adresse IPv6 (envoi d'un message en multicast sur une adresse déterminée et reprenant les 24 derniers bits de l'adresse IPv6).

### 5.3 Rappels concernant le service DNS

Le service DNS est un des services critiques sur l'Internet. Il s'agit du service permettant de convertir un nom réseau en adresse IP et inversement. Sans ce service, nous serions obligés de mémoriser des adresses IP directement, ce qui ne serait guère pratique. Le service DNS est donc une base de données *décentralisée* capable de répondre *localement* à une demande du style « Qui est www.swila.be ». Pour rappel, le système hiérarchique assure qu'un nom sur l'Internet est unique car les propriétaires d'un domaine (swila.be par exemple) sont responsables de la gestion des noms et adresses de son domaine uniquement. Quand une requête ne concerne pas son domaine, le service DNS renvoie la requête à un serveur racine pour que celle-ci soit résolue.

Le système de noms fait donc correspondre des informations précises (adresses, ...) à des noms configurés. Ainsi, pour l'enregistrement de www.swila.be, nous avons une entrée de type A qui mentionne son adresse IPv4 (195.154.39.227) et une entrée de type AAAA qui mentionne son adresse IPv6 (2001:bc8:38eb:fe10::11). Plusieurs types d'entrées sont possibles en fonction de l'information que l'on souhaite annoncer.

Il faut être prudent avec le système DNS car si les entrées qu'il contient ne sont pas valides, on peut tromper l'utilisateur sur les sites qu'il croit visiter. Enfin, les systèmes Microsoft utilisent le service DNS pour localiser l'annuaire Active Directory. Dès lors, dès qu'on installe Active Directory, des entrées particulières sont ajoutées dans le serveur DNS.

Enfin, mentionnons que pour des raisons de sécurité, il est possible de configurer un serveur DNS *secondaire* capable de répondre à toutes les requêtes (en fonction de sa configuration) lorsque le serveur principal est indisponible. La synchronisation entre les deux serveurs est automatique.

### 5.4 Rappels concernant le service DHCP

Le service DHCP est un autre service intéressant pour les administrateurs systèmes et réseaux. En effet, ce service est responsable de la distribution des adresses IP dans un réseau. L'intérêt est que le service envoie au client tous les éléments de configuration réseau afin que ce dernier soit configuré directement et sans intervention de l'utilisateur. Grâce à ce système, un ordinateur peut être connecté

sur le réseau et recevoir sa configuration depuis celui-ci. Ce mécanisme est particulièrement adapté aux périphériques nomades. Peu importe où ils se trouvent, le réseau leur donne la configuration à appliquer.

Cependant, si cela facilite la vie de l'administrateur, qui ne doit plus passer sur chaque ordinateur pour le configurer manuellement, cela ne facilite pas le contrôle. En effet, une adresse IP est attribuée à un périphérique durant un temps déterminé (= durée du bail). Une fois ce délai écoulé, le client doit faire une nouvelle demande au serveur. Dès lors, contrôler les utilisateurs devient plus difficile car une même adresse peut être attribuée à plusieurs personnes successivement.

Cependant, l'administrateur peut *réserv*er des adresses à des utilisateurs. Cela revient à attribuer une adresse donnée à un client déterminé. On procède alors à une *réservation*. L'administrateur peut, de cette manière *réserv*er les adresses pour l'ensemble des postes à connecter. Ainsi, les clients ne doivent rien configurer localement et l'administrateur garde la main mise sur toute la configuration réseau.

Il n'y a pas que les éléments réseaux qui peuvent être envoyés au client mais bon nombre d'options. Le service DHCP permet ainsi une configuration PXE (démarrage d'un ordinateur par le réseau), donner l'imprimante à utiliser, ...

Le service DHCP existe à la fois pour les adresses IPv4 et IPv6. Cependant, en IPv6 la règle est plutôt de construire son adresse IP en utilisant le protocole NDP en fonction des informations reçues par le réseau (comme le préfixe à utiliser, ...).

## 5.5 Installation et configuration du service DNS

Pour **installer** le service DNS, il faut d'abord vérifier que votre serveur dispose bien d'une adresse IP statique (fixe, non attribuée par le DHCP). Ensuite, il faut démarrer le **Server Manager > Manage > Add Roles and Features**. Dans la liste des rôles, il faut sélectionner *DNS Server*.

Une fois le rôle ajouté, il apparaît dans la liste des rôles disponibles sur le serveur. Pour la configuration, il faut donc se rendre dans **Server Manager > Tools > DNS** puis déployer **DNS > WIN16-1** (ou quelque soit le nom de votre serveur). On voit apparaître la fenêtre suivante :

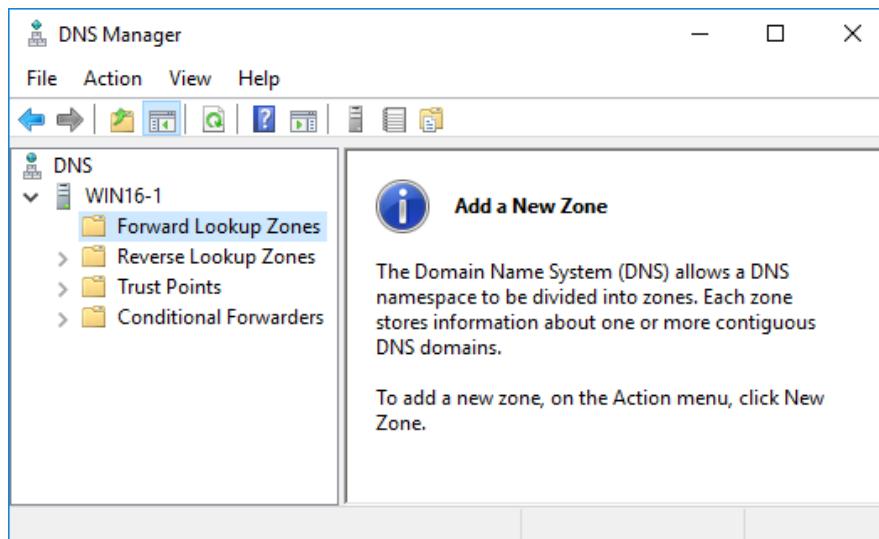


Figure 5.1 : tableau de configuration du service DNS

Dans la figure 5.1, nous remarquons les éléments suivants :

- *Forward Lookup Zones* : Ce sont les zones configurées pour faire les résolutions d'un nom vers l'adresse IP
- *Reverse Lookup Zones* : Ce sont les zones configurées pour faire les résolutions inverses d'une adresse IP vers le nom.
- *Trust Points* : Permet de configurer les éléments cryptographiques compatible avec DNSSEC qui permet de signer toutes les entrées d'une zone.
- *Conditional Forwarders* : ce sont les autres serveurs DNS à interroger suivant certaines conditions rencontrées. Un redirecteur est un serveur DNS vers lequel il est possible de rediriger une requête pour obtenir la résolution du nom.

Le **redirecteur** conditionnel ou non est un élément facultatif de la configuration du serveur DNS. En effet, tous les serveurs DNS disposent de la liste des serveurs racines qui servent à démarrer la recherche d'un nom donné. Cependant, dans certains cas, il est possible de rediriger une requête vers un autre serveur DNS configuré dans le redirecteur : par exemple si le nom à atteindre est local mais est servi par un autre serveur. De plus, à l'intérieur de certains réseaux, les requêtes DNS émises par d'autres serveurs que ceux autorisés peuvent être bloquées.

### 5.5.1 Propriétés du serveur DNS

Pour atteindre la **configuration générale** du service DNS, il faut faire un **clic-droit** sur le nom du serveur (WIN16-1 sur la figure 5.1) et choisir l'option **Properties**. La fenêtre qui apparaît contient plusieurs onglets et plusieurs options :

- *Interfaces* : cet onglet permet de configurer les interfaces (et donc les adresses IP) sur lesquelles le service DNS écoute.
- *Forwarders* : cet onglet permet d'ajouter des redirecteurs *globaux* (non conditionnel). Ces redirecteurs reçoivent alors les requêtes DNS que le serveur ne sait pas résoudre et sont chargés de fournir la réponse au serveur. Sur le campus, on pourrait configurer un redirecteur vers l'adresse IP 192.168.128.2 afin de relayer toutes les requêtes vers lui.
- *Advanced* : précise des options avancées comme *désactiver la récursivité* (le serveur ne tente plus de résoudre des requêtes pour lesquelles il n'a pas de réponse), ...
- *Root Hints* : cet onglet mentionne tous les serveurs racines connus par le serveur DNS. On trouve donc les 13 serveurs racines et leurs adresses IP.
- *Debug Logging, Event Logging et Monitoring* : ces onglets présentent les options d'analyse afin de trouver les dysfonctionnements du serveur DNS.

### 5.5.2 Ajout d'une nouvelle zone directe (Forward Lookup Zones)

Pour **ajouter une nouvelle zone** de recherche (nom DNS géré par ce serveur), il y a 2 possibilités. La première est de passer par l'*assistant d'ajout d'une zone* en faisant un **clic-droit** sur le nom du serveur (WIN16-1 sur la figure 5.1) et en choisissant l'option *Configure a DNS Server Wizard*. La seconde méthode est d'aller sur l'élément **DNS > WIN16-1 > Forward Lookup Zones** et de choisir l'option *new zone* (soit par un *clic-droit*, soit en passant par le menu *autres actions*).

Lors de l'ajout d'une nouvelle zone, le serveur propose 3 types de zone :

- *Primary Zone* : ce serveur connaît et maintient les informations de conversion des noms vers les adresses IP
- *Secondary Zone* : le serveur est un backup d'un autre serveur DNS. Il synchronise automatiquement les informations avec l'autre serveur DNS (celui qui a cette zone en zone principale).
- *Stub Zone* : le serveur DNS stocke les informations concernant les serveurs pouvant résoudre cette zone particulière. Ce mécanisme plutôt étrange, ne sera pas abordé ici.

Si l'utilisateur ajoute **une zone principale (Primary Zone)**, il doit mentionner le nom de la zone pour laquelle il fait *autorité* (il a acheté cette zone et en est donc responsable). Si le suffixe de la zone est *.local* (au lieu de *.be* ou *.com*), cette zone est considérée comme privée et ne se retrouve pas sur l'internet. Les zones locales peuvent donc être ajoutées sans risque. Ensuite, le système vous demande s'il faut utiliser un nouveau fichier ou un fichier existant (la plupart du temps, un nouveau fichier est l'option qu'il faut choisir). Ensuite, le système vous demande s'il faut *autoriser les mises à jour dynamiques* des zones. Pour des raisons de sécurité, nous choisirons l'option *Do not allow dynamic updates*. Enfin, un écran récapitulatif nous permet de contrôler si toutes les informations sont bien correctes. Si c'est le cas, il faut cliquer sur **Finish**.

La zone configurée apparaît alors dans la liste des *Forward Lookup Zones* (zone de recherche directe). Une fois la zone créée, il est possible d'ajouter des entrées :

Type d'entrée	Explication
A ou AAAA	Permet de faire correspondre un nom à une adresse. Le nom donné sera complété du suffixe DNS choisi. Ensuite, il faut mentionner l'adresse IPv4 ou IPv6 correspondant à cette entrée. On peut faire correspondre plusieurs adresses IP à une entrée.  Normalement, une adresse IP est référencée dans une seule entrée de type A ou AAAA. Si plusieurs noms arrivent sur la même adresse, il faut créer des alias (CNAME)
CNAME	Permet d'ajouter un alias. L'alias est un élément inscrit dans le DNS servant à faire pointer un nom vers une entrée de type A ou AAAA (il est donc interdit de faire pointer un CNAME vers un autre CNAME).
MX	Permet de mentionner le serveur mail qui est chargé de traiter les mails pour ce domaine.
NS	Permet de mentionner le serveur DNS responsable d'un nom de domaine. Cette entrée <b>permet également de renseigner une délégation de zone</b> . Ainsi, un sous-domaine pourrait être géré par un autre serveur DNS.

Il est également possible de créer un **sous-domaine** qui est géré par le serveur actuel en utilisant l'option *new domain*. Une fois tous les hôtes configurés, la zone DNS est prête à être utilisée.

Si l'utilisateur ajoute **une zone secondaire**, il doit mentionner le nom de domaine concerné et puis le ou les serveurs principaux auprès desquels il faut se synchroniser. Une fois la synchronisation démarrée, le serveur secondaire est à même de répondre aux requêtes concernant cette zone.

### 5.5.3 Ajout d'une zone de recherche inversée (Reverse Lookup Zones)

La *Reverse Lookup Zones* permet de réaliser la conversion dans l'autre sens : d'une adresse IP vers un nom. Il est nécessaire d'ajouter une zone de recherche inversée par sous-réseau /24. Ainsi, si l'on dispose du sous-réseau suivant : 192.168.128.0/20 et qu'on souhaite avoir une zone inverse pour

l'ensemble, il faut créer 16 zones différentes : 192.168.128, 192.168.129, 192.168.130, ..., 192.168.143.

Le nom de la zone inverse est un peu étrange car il reprend, par convention, chaque nombre décimal de l'adresse IP mais inversé. Ceux-ci sont ensuite suffixés par .in-addr.arpa. Ainsi, un nom valide de zone inverse pourrait être 128.168.192.in-addr.arpa.

Une fois la zone créée, elle est prête pour accueillir des entrées. Les entrées possibles sont :

Type d'entrée	Explication
PTR	Permet de faire pointer une adresse vers un nom. Normalement, seul le dernier octet de l'adresse doit être complété.
CNAME	Permet de créer un alias

#### 5.5.4 Configuration du client DNS

Le serveur Windows doit être configuré pour disposer d'un nom dans le domaine DNS configuré et, de plus, il doit être configuré pour utiliser le service DNS installé. Pour ce faire, il faut :

- Créer une entrée correspondant au serveur DNS courant et faire correspondre l'adresse IP
- Modifier le nom de l'ordinateur comme suit : **clic-droit sur This PC, Properties**. Choisir **Advanced system settings**, onglet **Computer Name** ensuite bouton **Change** puis le bouton **More** pour ajouter, comme suffixe DNS principal, le nom de la zone DNS configuré. Comme le nom est modifié, il sera nécessaire de redémarrer le serveur.
- Configurer le réseau pour utiliser le serveur DNS. Pour ce faire, il faut **modifier les paramètres de la carte réseau**. En effet, il faut modifier **le serveur DNS préféré** pour le remplacer par 127.0.0.1 (localhost) puisque le service DNS s'exécute sur notre serveur.

#### 5.5.5 Scripting

Il est possible de configurer les entrées DNS au moyen **de la ligne de commande** en utilisant l'outil `dnscmd`. Cette commande permet d'ajouter des zones mais également d'ajouter les enregistrements de tous types à l'intérieur de celles-ci. L'aide en ligne est disponible par la commande `dnscmd /?`.

Par exemple, les commandes suivantes sont valides (si notre serveur s'appelle DC) :

```
C:\> dnscmd DC /RecordAdd 128.168.192.in-addr.arpa 3 PTR  
                                data.cg.local
```

Cette commande ajoute, sur le serveur DC, dans la zone inverse (Reverse Lookup) l'enregistrement 192.168.128.3<sup>20</sup> qui pointe vers le nom `data.cg.local`.

```
C:\> dnscmd DC /RecordAdd cg.local data.cg.local_ A 192.168.128.3
```

Cette commande ajoute, sur le serveur DC, dans la zone directe (Forward Lookup) `cg.local` l'enregistrement `data.cg.local` qui a, comme adresse IP, l'adresse 192.168.128.3. Il faut **absolument mentionner le point à la fin de l'enregistrement** afin de mentionner que le nom est complètement qualifié.

<sup>20</sup> Pour rappel, une zone inverse (Reverse Lookup Zones) nécessite d'inverser tous les octets de l'adresse

On pourrait également écrire cette dernière commande comme suit :

```
C:\> dnscmd DC /RecordAdd cg.local data A 192.168.128.3
```

Dans cette dernière commande, nous avons uniquement mentionné le nom *data*, qui, puisque ce dernier ne se termine pas par un « . », est interprété comme *data.cg.local*. (et donc le nom mentionné est complété par celui de la zone).

En **Powershell**, en utilisant l'**exécution directe de commandes**, il est simple d'ajouter des enregistrements DNS :

```
$resultat = &"dnscmd" "DC" "/RecordAdd" "cg.local" "data"  
"A" "192.168.128.3"
```

## 5.6 Installation et configuration du service DHCP

Pour installer ce service, il faut démarrer le **Server Manager > Manage** puis choisir **Add Roles and Features**. Dans la liste proposée, il faut sélectionner **DHCP Server**. Une fois installé, une notification est ajoutée *Complete DHCP Configuration*. Il faut cliquer sur le lien et appuyer sur **Commit**.

Pour démarrer la configuration du service DHCP, il faut démarrer le **Server Manager > Tools > DHCP**.

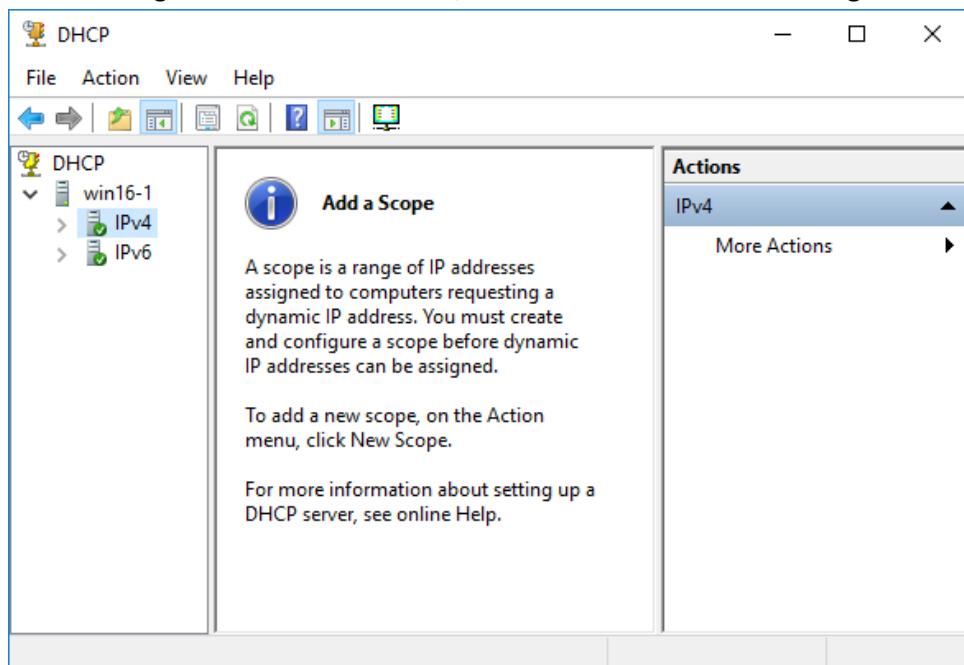


Figure 5.2 : Configuration du service DHCP

Il faut commencer par *ajouter une étendue* en faisant un **clic-droit** sur **IPv4** et en choisissant l'option **New Scope**. On doit donner un nom à l'étendue (dans *Name*) qui doit être unique. Ensuite, il faut mentionner les adresses IP de départ et de fin qui pourront être distribuées aux clients. Le masque est ensuite renseigné, veillez à ce que celui-ci soit conforme au sous-réseau concerné.

Le *wizard* propose ensuite d'exclure une plage IP, cette configuration est facultative, elle permet d'empêcher l'attribution de certaines adresses IP.

Ensuite, il faut mentionner la durée du bail (*Lease duration*) qui indique le nombre de jours, d'heures et de minutes de validité de l'adresse IP. Si les utilisateurs sont nombreux et nomades (comme dans une école), une durée de bail courte (4 heures) est plus appropriée.

Enfin, le *wizard* vous propose de configurer certaines options :

- *Router (Default Gateway)* : mentionne l'adresse IP du routeur qui sera utilisé par les machines clientes pour sortir du réseau et atteindre Internet.
- *Domain Name and DNS Server* : mentionne les informations DNS qui seront distribuées aux machines clientes comme le *parent domain* (ou le domaine DNS utilisé) et les adresses IP (IP Address) des serveurs DNS à fournir. Veillez à donner l'adresse IP réelle de votre serveur et pas l'adresse *localhost* 127.0.0.1.
- *WINS Servers* : cette fonctionnalité n'est pas nécessaire dans notre installation
- *Activate Scope* : une fois l'étendue active, le serveur DHCP sera actif.

**Attention !** Il est toujours imprudent d'avoir plus d'un serveur DHCP actif sur le même sous-réseau. Ainsi lorsque vous activez un serveur DHCP, veillez bien à vous assurer qu'aucun autre serveur n'est actif sur ce même réseau<sup>21</sup>.

Une fois le *wizard* fermé, en déployant les éléments à gauche, on voit apparaître les options configurées (comme l'étendue visible dans l'option *Address Pool*).

### 5.6.1 Les réservations DHCP (Reservations)

Une option intéressante du service DHCP est *la réservation*. Celle-ci consiste à associer une adresse physique à une adresse IP donnée. Ainsi, la machine concernée reçoit toujours la même adresse IP. En plus, si l'administrateur souhaite modifier la configuration réseau, il doit juste mettre à jour les données du serveur et redémarrer les machines.

Lors de l'encodage d'une réservation, il faut mentionner :

- *Reservation name* : Le nom de la réservation
- *IP address* : L'adresse IP réservée
- *MAC address* : L'adresse MAC sans aucun séparateur. Par exemple : 000C29DFBF93
- *Description* : Une description
- *Supported types* : Type pris en charge, dans notre cas, DHCP

Pour assurer que le service DHCP n'entre jamais en conflit avec une réservation réalisée, il est possible d'exclure l'adresse (ou la plage d'adresses) reprenant les réservations encodées. Les plages d'exclusion peuvent être configurées dans l'élément *Address Pool* via l'option *New Exclusion Range*.

### 5.6.2 Scripting

Il est possible d'ajouter des réservations DHCP directement **via la ligne de commande** en utilisant le programme *netsh*. Il s'agit d'un outil générique agissant sur la configuration réseau. Ainsi, pour obtenir l'aide concernant les entrées dans le DHCP, il faut entrer :

```
C:\> netsh dhcp server 127.0.0.1 list
```

Cette commande affiche l'aide et l'ensemble des commandes possibles. Pour chacune, il est possible d'obtenir l'aide en suffixant celle-ci par un « /? » .

<sup>21</sup> Si plus d'un serveur DHCP est actif, les clients pourraient recevoir des adresses de l'un ou l'autre serveur. Cela perturberait fortement le fonctionnement du réseau. **Vérifiez la configuration de pfSense !**

C:\> **netsh dhcp server 127.0.0.1 scope 192.168.128.0 /?**

*Cette commande les commandes applicables à une étendue donnée (une plage configurée dans le DHCP). L'étendue est précisée par l'option scope.*

C:\> **netsh dhcp server 127.0.0.1 scope 192.168.128.0 add reservedip  
192.168.128.3 000C3A5BCDB9 data DHCP**

*Cette commande ajoute une réservation (add reservedip) au serveur DHCP courant (server 127.0.0.1) pour l'étendue 192.168.128.0 (scope 192.168.128.0). L'entrée ajoutée a pour nom data, pour adresse IP réservée 192.168.128.3 associée à l'adresse MAC 00-0C-3A-5B-CD-B9 avec comme type pris en charge : DHCP.*

**En Powershell, par l'exécution directe de commandes,** il est facile d'ajouter des entrées dans le DHCP.

Ainsi, la commande précédente prendrait la forme suivante :

```
$resultat = &"netsh" "dhcp" "server" "127.0.0.1" "scope" "192.168.128.0"  
"add" "reservedip" "192.168.128.3" "000C3A5BCDB9" "data" "DHCP"
```

## 5.7 Exercices

1. Installer le **service DNS** comme suit :
  - a. Le nom de domaine correspondra à *votre nom de famille* suffixé par « *.local* ». Par exemple `swinnen.local`
  - b. Ajouter les entrées suivantes :
    - i. `fw` qui pointera vers l'adresse IP du firewall
    - ii. `win16-01` qui pointera vers l'adresse IP de votre serveur
    - iii. `host` qui pointera vers l'adresse IP de la machine hôte `192.168.190.1`
    - iv. créer la zone inverse pour le sous-réseau `192.168.190.0` et ajoutez les entrées PTR pour `fw`, `host` et `win16-01`
  - c. Configurer le redirecteur pour qu'il pointe vers le serveur DNS `192.168.128.2`
2. Configurer votre serveur Windows pour qu'il **soit client du serveur DNS configuré**.
3. Installer le **service DHCP** comme suit :
  - a. Désactiver le serveur DHCP présent dans pfSense (**Services > DHCP Server**)
  - b. Configurer une nouvelle étendue DHCP entre les adresses `192.168.190.150-200`
  - c. Précisez toutes les options nécessaires (DNS, ...)
4. Créer un **script Powershell** qui va créer des entrées dans le serveur DNS pour chaque adresse comprise dans la plage DHCP (entre `192.168.190.150` et `192.168.190.200`). Chaque entrée comprendra un enregistrement dans la zone directe et dans la zone de recherche inversée. Par exemple, voici un nom configuré : `ip-192-168-190-200.<votre-nom>.local` qui pointera vers l'adresse `192.168.190.200`, et ainsi de suite pour toutes les autres adresses.
5. Installer une nouvelle machine **Windows 10**<sup>22</sup> (mot de passe : `rootroot`)
  - a. Configurée en mode DHCP
  - b. Vérifiez la configuration réseau reçue et assurez-vous qu'elle a bien accès à Internet
6. A l'aide de la **ligne de commande** :
  - a. Ajouter une réservation DHCP pour cette machine avec l'adresse `192.168.190.155` (assurez-vous que le serveur ne distribue plus cette adresse)
  - b. Ajouter un alias DNS (**CNAME**) pour faire pointer le nom suivant : `vm10.<votre-nom>.local` vers le nom `ip-192-168-190-155.<votre-nom>.local`.

---

<sup>22</sup> Une machine virtuelle proposant la version d'évaluation de 90 jours de windows 10 est fournie dans le dossier `c:\admsys`

## Leçon 6 : Installation d'Active Directory

### 6.1 Introduction

Active Directory est un élément central des systèmes *Windows Server*. En effet, il s'agit d'installer une base de données d'utilisateur « globale » sur le réseau. Cette base de données globale permet aux utilisateurs de se connecter sur n'importe quelle machine membre du *domaine* configuré.

En plus d'authentifier les utilisateurs depuis le serveur, Active Directory permet de définir et distribuer des politiques de configuration à l'ensemble des machines. Cet aspect particulier rend Active Directory particulièrement puissant et intéressant. Pour les administrateurs cependant, ces configurations peuvent devenir complexes.

Dans la suite de cette leçon, nous allons aborder :

- Une description succincte d'Active Directory
- Les éléments d'installation d'Active Directory
- Les objets à l'intérieur d'Active Directory (Ordinateurs, Utilisateurs, Unité Organisationnelle, Groupe de sécurité, ...)
- Active Directory et les profils des utilisateurs

### Référence bibliographique

[1] A. Warren, Exam Ref 70-742 : Identity with Windows® Server® 2016, 1<sup>st</sup> edition, Microsoft Press, March 2017

## 6.2 Description d'Active Directory

### 6.2.1 Infrastructure d'Active Directory

L'infrastructure d'Active Directory comprend un certain nombre d'éléments (extrait de [1]) :

- **Active Directory Data Store.** C'est l'endroit où sont sauvegardées les informations d'identité dans l'annuaire. Le *data store* est hébergé sur un contrôleur de domaine. L'annuaire se concrétise par un fichier particulier (NTDS.DIT) stocké sur le contrôleur de domaine. On y trouve le schéma LDAP<sup>23</sup>, la configuration, les objets du domaine (utilisateurs, groupes, ordinateurs, ...) et dans certains cas, le catalogue global
- **Domain controllers.** Il s'agit de serveurs qui exécutent le rôle AD Domain Service. Ce rôle est responsable du maintien de toutes les informations nécessaires utiles pour le domaine (i.e. une copie du *data store*).
- **Domain.** Un ou plusieurs contrôleurs de domaine sont nécessaires pour créer un *domaine Active Directory*. Le domaine comprend toutes les informations d'identité et les objets créés. On trouve cette information répliquée dans tous les contrôleurs de ce domaine. Ainsi, les utilisateurs, groupes et ordinateurs sont créés dans le domaine et cette information est

---

<sup>23</sup> Le schéma LDAP est une définition des objets et données qui peuvent être intégrées dans les objets LDAP. Ainsi, en ajoutant des éléments au schéma LDAP (définissant de nouvelles données), les objets créés peuvent mémoriser de nouvelles valeurs.

répliquée sur tous les contrôleurs de domaine installés. Ainsi, si un contrôleur tombe en panne, un autre prend le relai (puisque il dispose de l'information).

- **Forest.** Une forêt est une collection d'un ou plusieurs domaines Active Directory. Le premier domaine installé dans une forêt est le *forest root domain*. La forêt contient une seule définition de la configuration réseau, et une seule occurrence du schéma. Il faut bien noter qu'il n'y a jamais de réPLICATION au-delà la forêt.
- **Tree.** Les espaces de nom DNS des domaines d'une forêt forment des arbres. Ainsi, si un domaine est enfant d'un autre (`swila.local` et `louis.swila.local`), ceux-ci forment une seule branche alors que 2 domaines différents (`swila.local` et `swinnen.local`) forment deux arbres dans la forêt. Il est possible d'établir des relations particulières (d'approbation par exemple) entre deux domaines d'une forêt.
- **Functional level.** Le niveau fonctionnel d'une forêt ou d'un domaine limite ses fonctionnalités. Les niveaux fonctionnels vont de *Windows Server 2000* (première version d'Active Directory) à *Windows Server 2016*. Ce niveau est limité par le plus vieux **contrôleur de domaine** présent dans la forêt. Il est recommandé, pour disposer de toutes les fonctionnalités, d'avoir le niveau fonctionnel le plus élevé. Bien sûr, il est impossible de travailler en niveau fonctionnel *Windows Server 2016* si tous les contrôleurs de domaine ne supportent pas celui-ci (si d'anciens serveurs sont présents).
- **Organizational units.** Ces éléments permettent de structurer Active Directory. Pour rappel, la structure LDAP est hiérarchique et l'unité organisationnelle, comme sous Linux, est un moyen de structurer et grouper des objets (utilisateurs, groupes, ordinateurs) créés. Active Directory ajoute, en plus, la possibilité de lier une politique (appelée *Group Policy Object* ou GPO) aux objets d'une unité.

Il faut bien remarquer qu'Active Directory nécessite le service DNS installé. En effet, l'infrastructure AD va inscrire des éléments à l'intérieur de la zone DNS. De plus, le domaine *Active Directory* se confond avec un domaine DNS (il en prend la forme car il nécessite un nom de domaine pour pouvoir fonctionner). Par conséquent, il est impossible d'utiliser *Active Directory* sans disposer d'un service DNS.

### Le service DNS interne et externe

Etant donné que Active Directory nécessite un service DNS, il serait tentant d'utiliser un seul service DNS (pour répondre aux requêtes internes et externes) sur le système. Or, il me semble une bonne idée de ne pas publier à l'extérieur les enregistrements d'*Active Directory*. Ainsi, un bon conseil serait de définir deux zones distinctes : la zone *locale* reprenant les entrées *Active Directory* et les informations locales (machines locales, ...) et une zone *publique* reprenant les informations à publier à l'extérieur (adresse IP publique et nom du serveur web, information pour le service mail, ...).

Ainsi, il n'est pas possible d'obtenir des informations *internes* à l'entreprise en interrogeant le service DNS depuis l'extérieur. Il est également possible d'installer un service DNS sur un autre serveur qui contiendrait uniquement les informations publiées vers l'internet.

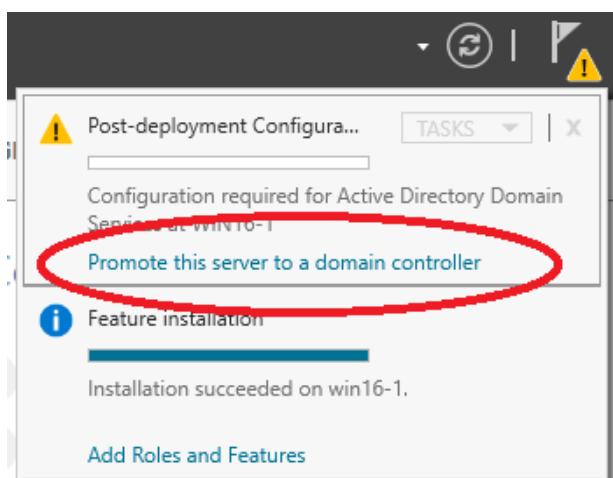
### 6.2.2 Les différents rôles Active Directory

Windows Server 2016 propose plusieurs rôles différents pour Active Directory en fonction des besoins de l'administrateur et des utilisateurs. Ainsi, on distingue :

- **Active Directory Domain Services** (*Services de domaine Active Directory*). Il s'agit de l'annuaire qui fournira l'authentification, l'autorisation et le monitoring. Il s'agit du service complet d'Active Directory.
- **Active Directory Lightweight Directory Services** (*LDS*). Il s'agit d'une version réduite du service AD DS. Cette version, autonome, sert à héberger les éléments des applications compatibles. Il s'agit réellement d'un sous-ensemble de AD DS (on installe donc pas les deux versions en même temps).
- **Active Directory Certificate Services** (*Services de certificats Active Directory*). Ce rôle, qui peut être ajouté à un rôle AD DS permet de créer une autorité de certification et d'obtenir des certificats pour l'entreprise. Les certificats générés ne sont pas reconnus par des applications externes (et sont donc limités aux ordinateurs du domaine).
- **Active Directory Rights Management Services** (*AD RMS*). Ce rôle particulier permet d'ajouter, à un rôle AD existant, une sécurité renforcée quant aux documents (pour autant que les applications soient compatibles avec le service). Ainsi, il est possible de définir des ACL propres aux documents créés (DACL). L'intérêt étant clairement de contrôler ce que l'on peut faire avec un document produit par l'entreprise (copie, impression, ...) dans le but de protéger l'information vitale de l'entreprise.
- **Active Directory Federation Services** (*ADFS*). Ce rôle, qui peut être ajouté à un AD DS existant, permet d'intégrer Active Directory dans une *fédération*. Ainsi, tous les membres d'une fédération peuvent être identifiés et accéder aux ressources misent à leur disposition. Par exemple, si une fédération était créée entre toutes les hautes écoles, n'importe quel étudiant pourrait se connecter, avec ses propres identifiants, dans n'importe quelle école membre de la fédération. La requête de connexion serait acheminée vers l'annuaire qui contient l'utilisateur (ex. : un étudiant de HELMo qui s'identifierait à l'extérieur serait accepté par l'AD de HELMo qui garderait le rôle d'authentification).

### 6.3 Installation d'Active Directory

Pour l'installer, il faut choisir **Active Directory Domain Services**, il faut passer par le **Server Manager > Manage > Add Roles and Features** et choisir **Active Directory Domain Services** dans la liste. Lors de la sélection, l'assistant propose l'ajout de fonctionnalités particulières qu'il faut accepter. Une fois l'installation terminée, il faut choisir **Promote this server to a domain controller** en cliquant sur le menu pour terminer l'installation d'Active Directory.



Lors de la première installation, il faut *Ajouter une nouvelle forêt (add a new forest)* et *Spécifier un nom de domaine racine (Root domain name)* sous la forme d'un nom DNS pour la forêt. Même si une zone DNS de recherche directe est déjà configurée pour les machines *locales*, il est préférable d'en créer une nouvelle pour le domaine à gérer (pour éviter des problèmes lors de l'installation de ce dernier). Ainsi, nous pourrions choisir *swila.local* comme nom DNS pour la forêt.

Ensuite, il convient de choisir *le niveau fonctionnel de la forêt (Functional Level)*. En fait, le niveau fonctionnel est limité par le plus vieux contrôleur de domaine actif<sup>24</sup> dans la forêt. Si nous créons une nouvelle structure, nous pouvons choisir le niveau fonctionnel le plus élevé : Windows Server 2016. Il faut également entrer le mot de passe pour le mode de restauration. Je propose de garder le mot de passe *P@ssw0rd* déjà adopté pour le compte Administrateur (il est bien clair que dans un environnement de production, un mot de passe fort est requis).

Le système nous avertit alors : *A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found* (puisque nous utilisons un domaine local). Ce n'est pas un problème et nous pouvons continuer l'installation. Le nom NetBios est ensuite déterminé (partie gauche du domaine). Ensuite, les dossiers hébergeant *le datastore* et les journaux et *SYSVOL* doivent être configurés (les options par défaut sont acceptables). Enfin, après un résumé, l'installation peut se terminer.

Une fois l'installation terminée et le redémarrage réalisé, on remarque que la fenêtre de connexion a changé : en effet, le système nous informe désormais qu'on ouvre une session **sur un domaine** (*swila* dans l'exemple ci-dessous) :



**Attention !** Lors de la reconnexion avec le compte *Administrator*, il est possible que le système mentionne que le mot de passe a expiré et doit être changé. Au besoin, vous pouvez changer celui-ci en *Pa\$\$w0rd*.

### 6.3.1 Changements suites à l'installation d'Active Directory

Depuis l'installation d'Active Directory, on remarque qu'il n'y a *plus d'utilisateurs et groupes locaux* (Local Users and Groups a disparu). En effet, puisque le serveur est désormais *contrôleur de domaine*,

<sup>24</sup> Ainsi si un contrôleur de domaine Windows Server 2003 est toujours actif dans la forêt, le niveau fonctionnel doit être limité à cette version.

tous les utilisateurs définis sont *des utilisateurs du domaine*. A l'inverse d'un utilisateur local, un utilisateur du domaine peut s'identifier sur toutes les machines membres du domaine (base de données globale). Si nous avions un second serveur membre du domaine mais pas contrôleur de domaine, il pourrait continuer à définir des utilisateurs (propres au serveur en question alors).

Pour trouver les utilisateurs et groupes du domaine, il est possible d'utiliser une console MMC avec *un composant snap-in* ou, dans le gestionnaire de serveurs, de suivre le chemin suivant : **Server Manager > Tools > Active Directory Users and Computers >** puis choisir votre domaine > **Users**.

Un autre changement important est **que les utilisateurs ne peuvent plus se connecter sur le serveur**. En effet, pour des raisons de sécurité, seul les administrateurs peuvent ouvrir une session sur le contrôleur de domaine.



Nous verrons qu'une politique particulière doit être activée pour autoriser les utilisateurs du domaine à ouvrir une session interactive. Ceci dit, cette précaution est assez logique afin de protéger le serveur des tentatives d'accès.

Un autre changement est **que le service DHCP ne fonctionne plus** depuis le passage en domaine. En effet, afin d'éviter d'avoir plusieurs services DHCP sur le même réseau et dans le même domaine, il est nécessaire d'**autoriser le serveur DHCP**. Pour ce faire, il faut aller dans **Server Manager > Tools > DHCP** choisir votre serveur puis faire un **clic-droit** et choisir **Authorize**.

Depuis l'installation d'Active Directory, la stratégie des mots de passe est active dans le domaine. Pour supprimer cette stratégie, il faut aller dans **Server Manager > Tools > Group Management Policy**. Il faut ensuite déployer les éléments *Forest*, *Domains* puis le *domaine courant* et faire un **clic-droit** sur l'élément *Default Domain Policy* puis choisir **Edit**.

L'éditeur de gestion des stratégies de groupe s'ouvre alors. Il faut aller dans **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**. Il faut ensuite modifier les paramètres comme suit :

- Enforce password history : **0 passwords remembered**
- Maximum password age : **0 days**
- Minimum password age : **0 days**
- Minimum password length : **0 characters**

- Password must meet complexity requirements : **Disabled**
- Store passwords using reversible encryption : **Disabled**

Une fois cette modification effectuée, il faut redémarrer le serveur pour qu'elle soit prise en compte.

### 6.3.2 Structure d'Active Directory

La structure d'Active Directory est visible lorsqu'on déploie **Utilisateur et ordinateur** à partir des **Services de domaine Active Directory**. On y voit l'annuaire LDAP contenant des éléments comme des *utilisateurs, des ordinateurs, des unités organisationnelles* ou encore *des groupes de sécurités*.

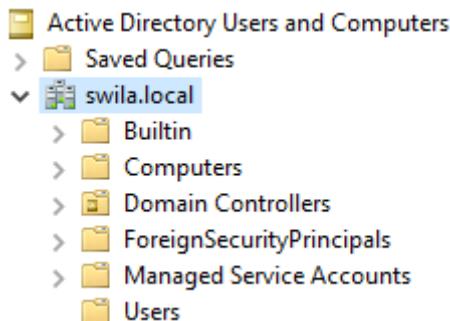


Figure 6.1 : structure LDAP du contrôleur de domaine swila.local

Comme nous pouvons le voir sur la figure 6.1, l'annuaire LDAP contient déjà un certain nombre d'éléments : *builtin* qui reprend tous les éléments par défaut présents sur les contrôleurs de domaine. Il n'est pas conseillé de modifier les éléments présents à moins de savoir exactement ce qu'on fait.

Ensuite, il y a l'élément *Computers* qui peut accueillir les ordinateurs qui seront membres du domaine. L'élément *Domain Controllers* reprend tous les contrôleurs de domaine configurés pour le domaine en question. L'élément *Users* reprend les utilisateurs et groupes configurés. Ainsi, on y trouve tous les utilisateurs locaux qui ont été promus dans le domaine, mais également des groupes particuliers. Les deux principaux à ce stade sont :

- *Domain Users* : Reprend tous les utilisateurs membres du domaine qui pourront se connecter sur les machines configurées dans ce domaine.
- *Domain Admins* : Reprend tous les administrateurs du domaine (permet de modifier toute la configuration). Sur un serveur qui n'est pas contrôleur de domaine, il est possible d'avoir un utilisateur membre du groupe *Administrators* de ce serveur (pouvant modifier toute la configuration de ce serveur, ajout d'imprimantes, ...) mais non membre de *Domain Admins* (ne pouvant donc pas modifier des paramètres de politique du domaine ou des comptes utilisateurs du domaine).

Il est particulièrement courant d'adapter la structure d'Active Directory pour refléter l'organisation interne de l'entreprise. Ainsi, il est courant d'utiliser les conteneurs *Organizational Units* afin de reprendre les différents services de l'entreprise. A l'intérieur de ces unités, il est possible de placer tous les objets mémorisables d'Active Directory comme *les utilisateurs (Users)*, *les groupes (Groups)* ou encore *les ordinateurs (Computers)*. La hiérarchie créée est ainsi plus facile à gérer, on peut regrouper logiquement les éléments qui sont en relation.

Dans une école, on pourrait ainsi créer les *unités organisationnelles* : Enseignants, Etudiants, Administratifs et Ordinateurs. Dans Etudiants, nous pourrions différencier les étudiants des différentes

sections (*info, compta, commex, marketing, ...*) et puis placer les étudiants concernés par année (1B, PE et AD). Ainsi, la gestion est beaucoup plus aisée.

### 6.3.3 Création d'une unité d'organisation

Pour créer une nouvelle unité d'organisation, il faut démarrer **Active Directory Users and Computers** et faire **un clic-droit** sur le nom de domaine (ex : `swila.local`). Il faut alors choisir l'option *New > Organizational Unit*. Il faut ensuite lui donner un nom. L'unité est alors prête à accueillir des éléments à l'intérieur : d'autres unités d'organisation, des ordinateurs, des utilisateurs ou des groupes de sécurité.

En **ligne de commande**, il faut utiliser la commande `dsadd.exe`. Pour l'aide, il suffit d'exécuter la commande `dsadd.exe ou /?`.

```
C:\> dsadd.exe ou "OU=Service Informatique,DC=swila,DC=local"
```

Cette commande permet de créer la nouvelle unité d'organisation *Service Informatique* à l'intérieur du domaine `swila.local`<sup>25</sup>.

En **Powershell**, la création d'une nouvelle unité d'organisation peut se faire de trois façons : soit en utilisant les modules spécifiques de PowerShell pour Active Directory, soit en utilisant les objets ADSI ou encore en utilisant une exécution directe de commande. Les objets ADSI **ne sont pas recommandés pour cette opération**, nous n'en parlerons pas.

L'environnement Powershell contient de nouvelles commandes pour gérer et créer des objets dans Active Directory. Ainsi, il est possible de créer une nouvelle unité d'organisation simplement en entrant la cmdlet suivante :

```
PS C:\> New-ADOrganizationalUnit -Name "Service Informatique" -Path  
"DC=swila,DC=local"
```

### 6.3.4 Création d'un utilisateur de domaine

La création d'un nouvel utilisateur de domaine se fait aisément depuis l'interface **Active Directory Users and Computers**. Il suffit de faire **un clic-droit** et de choisir l'option *New > User*. L'interface de création d'un utilisateur du domaine est un peu différente de celle d'un utilisateur local. Outre le *prénom*, le *nom* et le *nom complet*, il faut mentionner le *nom d'ouverture de session de l'utilisateur (User logon name)* et le nom utilisé pour les systèmes antérieur à Windows 2000 (**User logon name pre-Windows 2000**). Ces deux dernières informations reprennent le *login* de l'utilisateur. Un nom conforme à des postes antérieurs à Windows 2000 implique de ne pas utiliser de caractères spéciaux et d'en limiter la taille.

D'une façon générale, il est intéressant de limiter la taille du nom d'utilisateur de façon à permettre à l'utilisateur de ne pas devoir entrer une information trop longue.

---

<sup>25</sup> L'élément **OU** fait référence à une *unité d'organisation* tandis que l'élément **DC** fait référence au *contrôleur de domaine*. Ainsi `DC=swila, DC=local` fait bien référence au domaine `swila.local`

Une fois le premier écran rempli, le système demande d'entrer un mot de passe et propose les options habituelles. **Attention !** Si la stratégie des mots de passe est toujours active, la complexité du mot de passe sera vérifiée.

L'utilisateur est, par défaut, membre du groupe *Domain Users* et pourra ainsi ouvrir une session sur tous les ordinateurs membres de ce domaine (excepté les contrôleur de domaine).

En **ligne de commande**, la commande `dsadd.exe` permet de créer des utilisateurs. Pour obtenir l'aide sur cette partie, il faut entrer `dsadd.exe user /?`.

```
C:\> dsadd user "cn=Louis SWINNEN,ou=Service Informatique,dc=swila,dc=local" -samid lsw -upn lsw@swila.local -fn Louis -ln SWINNEN -display "Louis SWINNEN" -pwd "P@ssw0rd" -canchpwd no -pwdneverexpires yes
```

Cette commande permet d'ajouter un utilisateur (*Louis SWINNEN*) dans l'unité d'organisation *Service Informatique*, le nom d'ouverture est *lsw@swila.local* et celui pour les systèmes antérieurs à Windows 2000 est *lsw*. Le prénom est fixé à *Louis* et le nom de famille à *SWINNEN*. Le nom affiché sera et le mot de passe *Louis SWINNEN*. Enfin, le mot de passe est fixé *P@ssw0rd* avec les options suivantes : l'utilisateur ne peut changer son mot de passe (`-canchpwd no`) et celui-ci n'expire jamais (`-pwdneverexpires yes`).

Il y a bien d'autres options possibles à la commande `dsadd.exe` notamment celles qui permettent de fixer les chemins vers les dossiers de bases et le profil. Nous en parlerons plus loin dans cette leçon.

En **Powershell**, il est possible d'ajouter un utilisateur en utilisant les commandes spécifiques pour Active Directory comme suit :

```
PS C:\> new-ADUser -Name "Louis SWINNEN" -AccountPassword (ConvertTo-SecureString -AsPlainText "P@ssw0rd" -Force) -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true -SamAccountName lsw -UserPrincipalName lsw@swila.local -Path "OU=Service Informatique,DC=swila,DC=local" -GivenName "Louis" -Surname "SWINNEN" -DisplayName "Louis SWINNEN"
```

Cette commande `New-ADUser` permet de créer un nouvel utilisateur dans Active Directory. Dans cet exemple, l'utilisateur est créé dans l'unité d'organisation *Service Informatique*. Il est nécessaire de consulter la documentation<sup>26</sup> pour connaître toutes les options.

Comme toujours, l'exécution directe permet également d'appeler la commande `dsadd.exe user` directement depuis Powershell.

### 6.3.5 Création d'un groupe de sécurité

Les groupes de sécurité ont, comme dans le cas des groupes locaux, les mêmes fonctionnalités. La différence principale est que leur portée s'étant à tout le domaine. Ainsi, un groupe de sécurité défini sur le contrôleur de domaine est *visible* sur toutes les machines du domaine. C'est une particularité intéressante qui permet ainsi de définir un groupe depuis le contrôleur de domaine et celui-ci peut alors être utilisé (pour fixer des permissions sur des fichiers et/ou dossiers sur les machines membres du domaine) n'importe où.

<sup>26</sup> <http://technet.microsoft.com/en-us/library/ee617253.aspx>

Pour créer un groupe de sécurité, il faut faire un **clic-droit** et choisir l'option *New > Group*. La fenêtre de création du groupe apparaît alors. Il faut mentionner son nom (et son nom compatible pour les systèmes pré-Windows 2000), mentionner son étendue et son type.

L'étendue peut être *domain local* et dans ce cas, le groupe est connu du contrôleur de domaine seulement, *global* et dans ce cas, le groupe est connu à travers le domaine pour lequel le contrôleur est configuré (c'est l'option par défaut) ou *universal* et, dans ce cas, l'étendue est définie à la forêt complète.

Le type de groupe peut être *Security* et dans ce cas, ils sont utilisés pour définir des droits et autorisations sur des ressources données ou *Distribution* et sont, dans ce cas, utilisable uniquement par le logiciel de courrier électronique pour faire la distribution du courrier à plusieurs utilisateurs directement.

En **ligne de commande**, la commande `dsadd.exe` permet d'ajouter des groupes de sécurité. Pour obtenir l'aide, veuillez-vous référer à la commande `dsadd.exe group /?`.

```
C:\> dsadd group "CN=Informatique,OU=Service Informatique,DC=swila,  
DC=local" -secgrp yes -scope g
```

Cette commande permet de créer un groupe de sécurité nommé *Informatique* localisé dans l'unité d'organisation *Service Informatique*. L'étendue de ce groupe est globale.

```
C:\> dsmod group "CN=Informatique,OU=Service Informatique,DC=swila,  
DC=local" -addmbr "CN=Louis SWINNEN,OU=Service Informatique,  
DC=swila,DC=local"
```

Cette commande permet d'ajouter l'utilisateur *Louis SWINNEN* au groupe de sécurité *Informatique* présent dans l'unité d'organisation *Service Informatique*.

En **Powershell**, il est possible d'ajouter un groupe comme suit :

```
PS C:\> New-ADGroup -Name "Informatique" -samAccountName Informatique  
-GroupCategory Security -GroupScope Global  
-Path "OU=Service Informatique,DC=swila,DC=local"
```

Cette commande permet de créer un groupe de sécurité d'étendue globale nommé *Informatique* et placé dans l'unité d'organisation *Service Informatique*.

```
PS C:\> Add-ADGroupMember "CN=Informatique,OU=Service Informatique,  
DC=swila,DC=local" -Members "CN=Louis SWINNEN,OU=Service  
Informatique,DC=swila,DC=local"
```

Cette commande permet d'ajouter l'utilisateur *Louis SWINNEN* au groupe *Informatique* tous deux situés dans l'unité *Service Informatique*.

### 6.3.6 Création d'un compte Ordinateur

Dans Active Directory, les ordinateurs membres du domaine sont stockés sous la forme d'objet particulier, les comptes « Ordinateurs ». Tous les ordinateurs membres du domaine doivent apparaître dans l'annuaire.

Lorsqu'on ajoute un ordinateur au domaine, le compte ordinateur peut être créé à ce moment. Il est pourtant bien plus commode de créer ce compte au préalable. Ainsi, il est déjà placé dans la bonne unité d'organisation et la structure d'Active Directory reste cohérente.

Pour créer un compte ordinateur, il suffit de connaître le nom de cette machine. Ensuite, il faut faire un **clic-droit** à l'endroit où l'on souhaite ajouter ce compte et choisir l'option *New > Computer*. Il faut ensuite mentionner son nom ainsi que le nom compatible pré-Windows 2000.

En **ligne de commande**, l'ordinateur peut être créé par la commande `dsadd.exe`. Pour obtenir l'aide concernant cette commande, référez-vous à la documentation en ligne `dsadd.exe computer /?`.

```
C:\> dsadd computer "CN=Win7,OU=Service Informatique,DC=swila,DC=local"  
-samid Win7
```

*Cette commande permet de créer un compte ordinateur pour la machine nommée Win7.*

En **Powershell**, il est possible d'ajouter un ordinateur comme suit :

```
PS C:\> New-ADComputer -Name "Win7" -SamAccountName "Win7"  
-Path "OU=Service Informatique,DC=swila,DC=local"
```

*Cette commande permet de créer un compte d'ordinateur pour la machine Win7. Le compte d'ordinateur est créé dans l'unité d'organisation Service Informatique.*

## 6.4 Les profils itinérants

Nous avons vu dans une leçon précédente que les profils utilisateurs renseignent les paramètres et la configuration de celui-ci. Or, la mise en domaine pose un certain nombre de questions : souhaite-t-on que l'utilisateur dispose d'un profil différent sur chaque machine sur lesquelles il se connecte ? Souhaite-t-on, au contraire, qu'il récupère son profil et retrouve ses documents quelque soit la machine sur laquelle il se connecte ?

Dans la plupart des cas, la seconde proposition est la plus souhaitable : l'utilisateur se connecte sur une machine membre du domaine et il récupère son profil. Pour réaliser cette opération, il est nécessaire que le profil de l'utilisateur soit stocké dans un endroit accessible pour toutes les machines membres du domaine. Il est nécessaire que les autorisations soient fixées correctement pour permettre une modification de ces données.

Ainsi, il convient de sauvegarder le profil de l'utilisateur sur **un partage réseau**. Ce partage doit être renseigné dans les informations de profil de l'utilisateur afin que les machines puissent y accéder dès qu'il se connecte.

Pour ce faire, il va falloir :

- Créer un dossier qui contiendra les données de profil des utilisateurs
- Partager ce dossier de sorte à ce qu'il puisse être accessible sur le réseau (**autorisations de partage & droits**)
- Placer les profils des utilisateurs, ainsi que son répertoire de base dans le dossier créé et renseigner ce dossier dans l'onglet profil de l'utilisateur. **Attention ! Il faut** mentionner **un chemin réseau valide pour toutes les machines membres du domaine**. Par exemple :  
`\SWINNEN\Users\%USERNAME%` pour le dossier de base et  
`\SWINNEN\Users\%USERNAME%\ntprof` pour le chemin vers son profil.

Ainsi, le chemin devra commencer par les caractères `\` mentionnant que le chemin est de type réseau (appelé parfois UNC). On mentionne ensuite le nom du serveur (ou son adresse IP) et puis le nom du

partage contenant les données utilisateurs<sup>27</sup>. Il est intéressant de savoir que la variable %USERNAME% désigne le login de cet utilisateur. Ainsi, nous aurons un dossier particulier par utilisateur.

Il convient également de fixer les permissions précisément car l'**utilisateur** doit disposer d'**une permission de type contrôle totale** sur son dossier de base et sur le chemin vers son profil. Pour rappel, le profil est mémorisé dans le chemin mentionné dans le compte de l'utilisateur. Sans modification particulière du registre, le dossier contenant le profil est suffixé suivant le système d'exploitation utilisé (en supposant que ntprof soit renseigné comme chemin du profil) comme suit : « .v2 » pour les systèmes Vista, 7, Server 2008, Server 2008 R2, 8, Server 2012, 8.1, Server 2012R2 et Windows 10 < 1607 et « .v6 » pour les systèmes Windows 10 >= 1607 et Server 2016.

Nous remarquons également qu'il est possible de *connecter automatiquement* un lecteur réseau vers le répertoire de base de l'utilisateur. Cela lui permet d'avoir un accès simple à son dossier personnel.

Enfin, il est également possible de créer un profil **itinérant obligatoire**. Il s'agit d'un profil configuré sur le contrôleur de domaine que l'administrateur personnalise selon ses besoins. Une fois terminé, l'administrateur le rend obligatoire et toutes les machines du domaine acceptent une connexion sur base de ce profil mais aucune modification ne peut y être apportée.

## 6.5 Intégrer une machine à un domaine

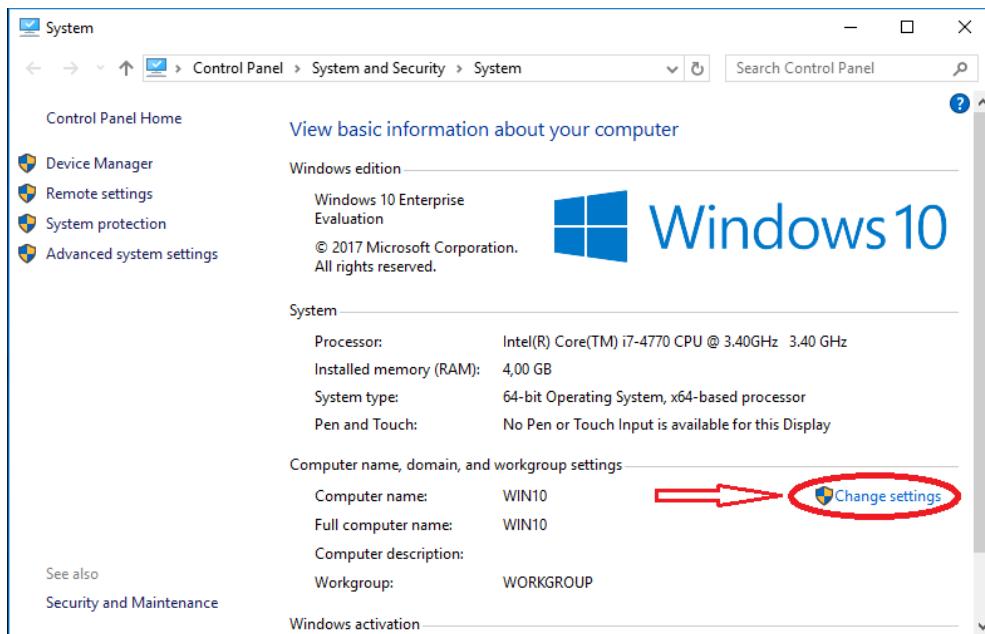
Le grand intérêt du passage en domaine est d'intégrer des postes clients dans le domaine afin de permettre une authentification centralisée et distribuer une politique de configuration à l'ensemble des machines.

Cette entrée des machines dans le domaine peut s'opérer de plusieurs manières. La façon la plus courante est la suivante : faire un **clic-droit** sur **This PC** et choisir l'option **Properties**<sup>28</sup>. Il faut alors sélectionner **Change settings** dans la section *Computer name, domain, and workgroup settings*. Dans l'onglet *Computer Name*, choisir le bouton *Change*.

---

<sup>27</sup> Dans notre exemple, le dossier de base se trouve sur le serveur dont le nom est SWINNEN et le nom du partage est Users. Un dossier reprend le login de l'utilisateur concerné (%USERNAME%) est présent.

<sup>28</sup> Sous Windows XP, Vista et Windows 7, il est également possible d'utiliser l'option **Gérer** en faisant un **clic-droit** sur **Ordinateur** et en choisissant **Gérer** dans le menu.



Ensuite, il convient d'entrer un nom de domaine dans l'option domaine (par exemple `swila.local`).

Afin de pouvoir contacter le contrôleur de domaine, il faut impérativement **que la machine utilise le contrôleur de domaine comme serveur DNS principal**. Pensez-donc à vérifier cela avant de tenter d'introduire une machine dans le domaine.

Une fois le nom de domaine configuré et **pour autant que le serveur puisse contacter le contrôleur** de domaine gérant celui-ci (voir la remarque concernant le DNS dans le paragraphe précédent), il devrait demander d'entrer un compte d'administrateur pour entrer cette machine dans le domaine.

Le compte mentionné doit faire partie du groupe *Domain Admins* afin de permettre l'entrée de la machine dans le domaine. Si tout se passe correctement, la machine est intégrée au domaine et le système vous demande de redémarrer celle-ci (en effet, le nom de la machine a changé).

Si aucun compte machine n'avait été créé au préalable sur le contrôleur de domaine, un compte a été ajouté dans le groupe *Computer* du contrôleur de domaine. Au contraire, si la machine avait déjà un compte à son nom, ce compte est utilisé pour l'affiliation au domaine.

Au redémarrage de la machine, nous observons quelques modifications :

- L'écran de sélection de l'utilisateur a disparu. Il faut entrer l'identité de l'utilisateur avec laquelle on souhaite se connecter
- Par défaut, la machine ouvre une session sur le domaine configuré, sauf pour le compte Administrateur/Administrator où elle choisit une connexion sur la machine locale
- Le firewall est à nouveau actif. En effet, comme un *nouvel emplacement* a été ajouté à la liste (nommé *réseau avec domaine*), le firewall est actif sur cet emplacement. Il convient de désactiver le firewall.

La machine est désormais membre du domaine et accepte l'authentification de n'importe quel compte utilisateur du domaine.

## 6.6 Exercices

1. Supprimer tous les comptes utilisateurs créés par script (leçon 3, exercice 3)
2. Installer le rôle AD Domain Services et configurez votre contrôleur de domaine AD :
  - a. Le nom de domaine est `cgXXdom.local` (où XX est votre numéro de machine)
  - b. Utiliser le mot de passe `P@ssw0rd` pour le mode restauration
  - c. Fixer le niveau fonctionnel de la forêt à Windows 2016
  - d. (*optionnel*) Si votre système propose de changer votre mot de passe Administrateur, utilisez `Pa$$w0rd`
  - e. Supprimez la stratégie de mot de passe par défaut du domaine
3. Créer un dossier partagé `c:\CGData` muni des autorisations adéquates pour stocker les profils des utilisateurs.
4. Créer une unité d'organisation `CGComputers` et créer un compte d'ordinateur `VM-WIN10` pour la machine virtuelle Windows 10.
5. Réécrire votre script de création des utilisateurs pour :
  - a. Créer des utilisateurs membres du domaine AD
  - b. Les utilisateurs seront créés dans une OU `CGUsers` et vous créerez une OU par catégorie. Ainsi les utilisateurs de *direction* seront placés dans la branche `CGUsers\direction`.
  - c. Créer un groupe de sécurité globale par catégorie. Ainsi, dans le groupe de sécurité informatique, on trouvera tous les utilisateurs de la catégorie *informatique*.
  - d. Fixer le chemin vers le profil de l'utilisateur vers le chemin `CGData\<login>\netprofile`. Fixer également le chemin vers le dossier de base `CGData\<login>` et connectez un lecteur P: (cf. exercice 3).
  - e. Fixer les ACL vers les dossiers correctement
6. Ajouter la VM Win10 à votre domaine et tentez une connexion avec un compte utilisateur
  - a. Changez son nom en `VM-WIN10` et ajoutez-la dans le domaine
  - b. Vérifiez bien que le profil de l'utilisateur est trouvé
7. Créer un compte `helmodom` avec comme mot de passe `cgdom2016` comme étant un compte de domaine obligatoire. Fixer le chemin vers son profil et son répertoire de base (comme pour les utilisateurs créés à l'étape 5).
8. Connectez-vous avec le compte `Administrator` du domaine sur la VM Win10.
  - a. Comment procéder ? 
  - b. Où est stocké le profil ? 
  - c. Créez un dossier `AdmSys` sur le disque C: uniquement accessible aux utilisateurs de la catégorie *informatique*

## Leçon 7 : Introduction aux GPO

Cette introduction aux GPO se base sur livre de référence (chapitre 3) :

[70-742] A. Warren, Exam Ref 70-742 : Identity with Windows® Server® 2016, 1<sup>st</sup> edition, Microsoft Press, March 2017

### 7.1 Introduction

La **stratégie de groupe (Group policy)** est un moyen important mis en place par les serveurs Windows Server afin de gérer de manière globale les politiques de configuration. Ainsi, il est possible de transmettre une politique de configuration déterminée à un ordinateur, un utilisateur ou un groupe de façon simple.

La stratégie de groupe est directement liée à la structure d'Active Directory. Ainsi, les paramètres que nous pouvons configurer sont *déployés* sur l'ensemble du domaine, sur les contrôleurs de domaine ou sur une unité d'organisation précise.

Les paramètres d'une stratégie de groupe, appelé **stratégie (Policy)** sont à sélectionner parmi les milliers d'option possibles. Les paramètres d'une stratégie peuvent porter sur des éléments très différents : ainsi, il est par exemple possible de désactiver l'utilisation de *regedit.exe*, le programme d'édition du registre ou encore, empêcher l'utilisateur d'atteindre le panneau de configuration.

Certains paramètres **sont applicables aux utilisateurs** (par exemple pour empêcher un utilisateur déterminé à modifier la configuration du système) alors que **d'autres sont applicables aux ordinateurs**. Nous en verrons quelques uns plus tard.

### 7.2 Les GPO

Une GPO<sup>29</sup> est une configuration reprenant une ou plusieurs stratégies et faisant partie d'une *stratégie de groupe*. La GPO s'applique à un ou plusieurs utilisateurs ou ordinateurs. Elle est déployée au niveau des postes et utilisateurs membres du domaine. Pour **créer ou modifier** une GPO, il faut utiliser l'outil de *Group Policy Management*

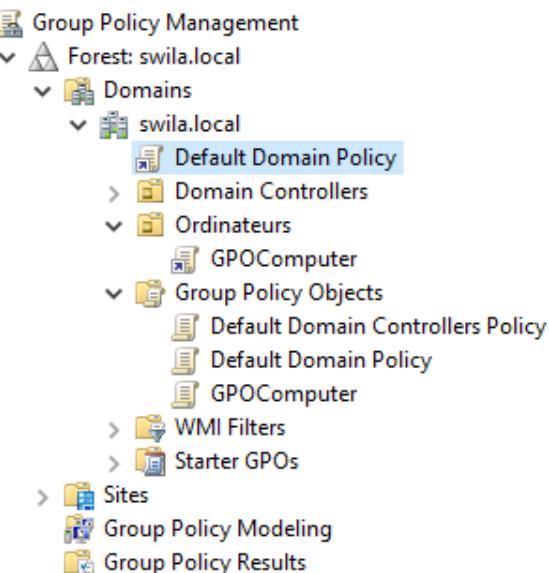


Figure 7.1 : Outil de gestion de stratégie de groupe

<sup>29</sup> Group Policy Object

Comme nous pouvons le voir sur la figure 7.1, dans le conteneur *Group Policy Object*, il y a 3 éléments : *Default Domain Policy*, *Default Domain Policy* et *GPOComputer* (qui est une stratégie créée).

Pour créer une nouvelle stratégie, il faut simplement faire un **clic-droit** sur ce conteneur et choisir **New**. Une fois le nom entré (par exemple *GPOComputer*), la stratégie est créée. Si nous souhaitons modifier la stratégie créée, il faut faire un **clic-droit** sur cette stratégie et choisir **Edit**.

Dès ce moment, on arrive dans l'outil d'édition de la stratégie de groupe. Sur la figure 7.2, on peut voir l'édition de la stratégie *Default Domain Policy*.

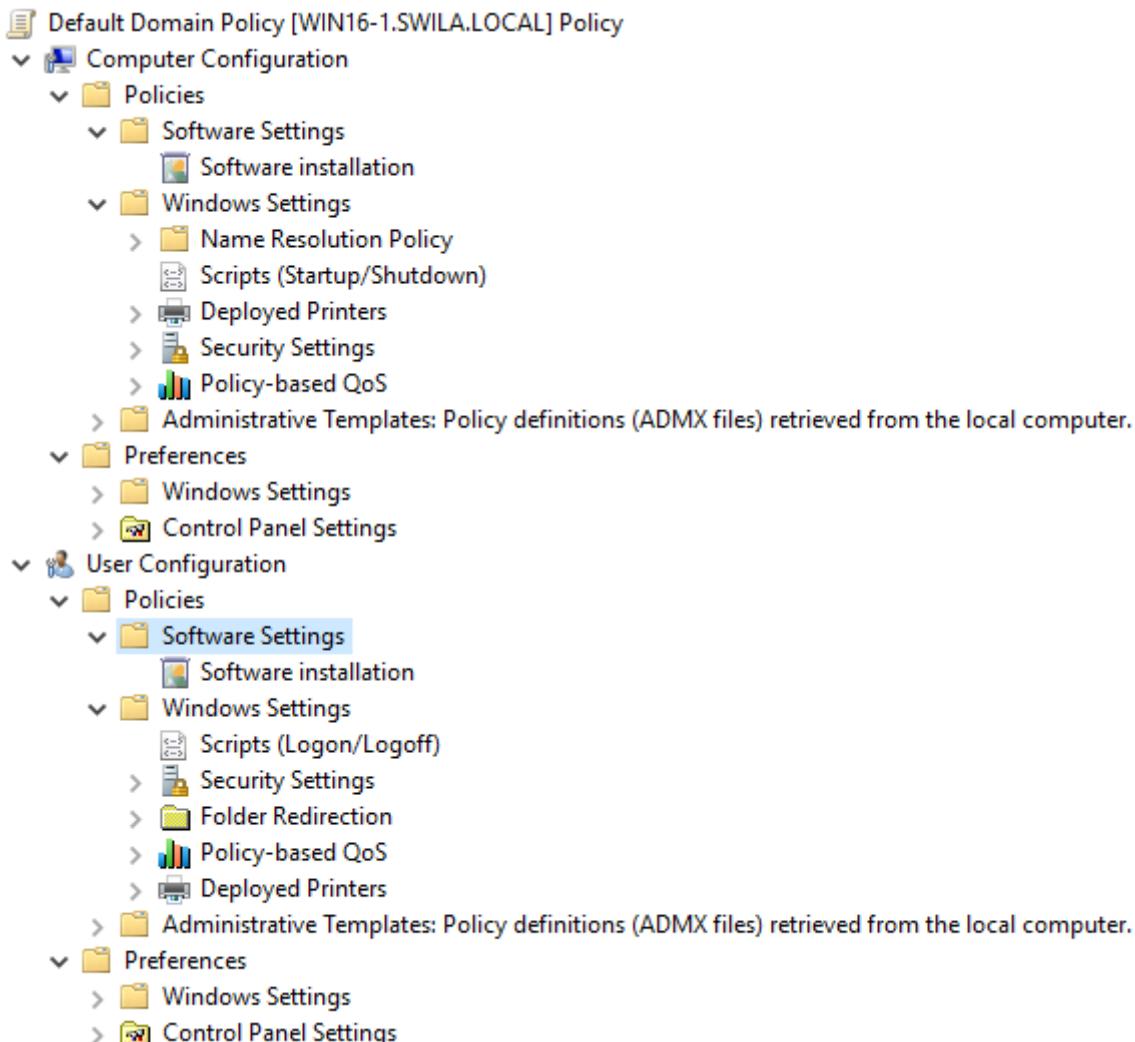


Figure 7.2 : Edition de stratégie *Default Domain Policy*

Dans le panneau de droite, on trouve toutes les stratégies configurables. Il y a des milliers de stratégies possibles et il faut dès lors faire son choix parmi celles qui sont proposées.

Sur la figure 7.3, on trouve les stratégies configurables de *User Configuration\Administrative Templates\System*. On remarque que les stratégies sont regroupées par thème (*Système, Accès au stockage amovible, Démarrage à chaud de Windows, Gestion de l'alimentation, ...*). A l'intérieur de chaque groupe, on retrouve les stratégies configurables. Chaque stratégie peut être *Not configured* (et

donc non modifiée par cette stratégie de groupe), *disabled* (désactivée) ou *enabled* (activée et donc prise en charge par la stratégie). Certaines stratégies, quand elles sont activées, nécessitent des éléments de configuration précis (comme par exemple le *délai d'expiration de mot de passe*).

Setting	State	Comment
Ctrl+Alt+Del Options		
Driver Installation		
Folder Redirection		
Group Policy		
Internet Communication Management		
Locale Services		
Logon		
Mitigation Options		
Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
<b>Do not display the Getting Started welcome screen at logon</b>	<b>Not configured</b>	<b>No</b>
Custom User Interface	Not configured	No
Prevent access to the command prompt	Not configured	No
Prevent access to registry editing tools	Not configured	No
Don't run specified Windows applications	Not configured	No
Run only specified Windows applications	Not configured	No
Windows Automatic Updates	Not configured	No

Figure 7.3 : configuration de la stratégie de groupe

Ainsi, par exemple, nous pourrions configurer dans cette stratégie la **désactivation de l'invite de commande**. Il faut alors *activer* la stratégie *Prevent access to the command prompt*. Dans l'écran de configuration de cette stratégie, nous pouvons également désactiver le traitement des scripts (*disable the command prompt script processing*). Une fois cette stratégie active, l'utilisateur concerné par cette stratégie ne pourra plus accéder à l'invite de commande (l'invite de commande est la commande MS-DOS ou encore cmd.exe).

### 7.2.1 Etendue

Une fois la stratégie de groupe définie, il faut déterminer à quels utilisateurs et/ou ordinateurs elle va s'appliquer. L'étendue peut être **le site, le domaine ou une unité d'organisation** définie dans Active Directory. L'étendue définit la *frontière d'application* de la stratégie. Ainsi, une stratégie s'appliquant sur une unité d'organisation déterminée se limitera aux éléments contenus (i.e. les descendants) dans cette unité. On remarque dès lors l'apparition d'une notion d'*héritage* : la stratégie s'applique à tous les éléments enfants. En conséquence, plusieurs stratégies peuvent s'appliquer. Par exemple, si nous définissons une stratégie au niveau du domaine et une stratégie au niveau d'une unité d'organisation, les deux stratégies s'appliquent aux objets enfants (effectivement, les objets contenus dans l'unité d'organisation héritent des deux stratégies). Il est possible de déterminer la stratégie appliquée sur un objet donné en utilisant le *jeu de stratégie résultant* (RSoP) qui évalue toutes les stratégies applicables.

Il est également possible de *limiter* la partie d'une stratégie en spécifiant, par exemple, les **Security Filtering**. Ce paramètre permet de limiter l'application de la stratégie à des groupes de sécurité définis (i.e. aux utilisateurs, ordinateurs, ... faisant partie ou non de ces groupes). La stratégie peut également s'appliquer sur base des *filtres WMI* qui mentionnent des caractéristiques du système d'exploitation (version, service pack, ...).

Par défaut, **Security Filtering** contient l'élément *Authenticated Users* (les utilisateurs authentifiés). Si vous modifiez cette option (en remplaçant par un groupe d'utilisateur précis par exemple), il faut impérativement donner au groupe *Domain Computers* un accès en lecture (READ) sur cette GPO, via l'onglet **Delegation > Advanced**. Sans cette action, la stratégie pourrait ne pas s'appliquer<sup>30</sup>.

### 7.2.2 Prise en compte

Une fois la stratégie définie, liée et appliquée, il faut que celle-ci se déploie sur l'ensemble des ordinateurs membres du domaine. En fait, les stratégies sont mises en place *coté client*. Ainsi, les ordinateurs membres du domaine téléchargent les stratégies et les appliquent à leur propre configuration (modification du registre).

Les stratégies sont automatiquement téléchargées lorsque l'ordinateur démarre (stratégie *Computer Configuration*), lorsque l'utilisateur se connecte (stratégie *User Configuration*) et toutes les 90 à 120 minutes. Il est possible de demander à l'ordinateur client de mettre à jour sa stratégie en utilisant l'outil `GPUTupdate.exe`. L'outil peut être exécuté sur le contrôleur de domaine ou sur le poste client.

### 7.2.3 Types de GPO

Il existe, depuis l'apparition de Windows Server 2000, la possibilité de définir une stratégie s'appliquant localement au serveur lui-même. Cette stratégie est particulièrement intéressante lorsque le serveur travaille en mode autonome (i.e. ne fait pas partie d'un domaine). Depuis Windows Server 2008, il est possible de définir *plusieurs* stratégies locales s'appliquant par exemple à des groupes d'utilisateur différents (i.e. les administrateurs, les non-administrateurs, ...). Ces stratégies locales sont accessibles au moyen de la console MMC si l'on ajoute le *composant snap-in* nommé *Group Policy Object*. Lors de l'ajout de ce composant, en cliquant sur **Browse**, il y a 2 onglets (Computers et Users), il est possible de spécifier le groupe auquel elle s'applique. Uniquement si l'ordinateur ne fait pas partie du domaine.

Dans un **domaine Active Directory**, deux GPO par défaut sont ajoutées :

- **Default Domain Policy** – Politique par défaut s'appliquant à tout le domaine installé (car elle est *liée* au domaine). Cette politique définit les contraintes de mot de passe et de sécurité qui sont appliquées pour tous les utilisateurs et ordinateurs. Il n'est pas recommandé de modifier cette politique (sauf pour modifier les éléments qu'elle configure comme la stratégie des mots de passe), il faut plutôt ajouter une nouvelle politique et lier celle-ci au domaine.
- **Default Domain Controllers Policy** – Cette politique est liée à la GPO *Domain Controllers* installée par Active Directory. Elle s'applique à tous les contrôleurs de domaine du domaine (car elle est *liée* à l'OU *Domain Controllers*). Cette politique définit donc les restrictions qui sont appliquées aux contrôleurs. Si d'autres restrictions ou configurations particulières doivent être prévues, il convient de modifier cette GPO.

<sup>30</sup> <https://blogs.technet.microsoft.com/askds/2016/06/22/deploying-group-policy-security-update-ms16-072-kb3163622/>

#### 7.2.4 Lier des GPO

Nous avons déjà vu comment il était possible de créer une nouvelle stratégie. Cependant, une fois la stratégie créée, il convient de la *lier* (i.e. l'appliquer) à un élément particulier d'Active Directory. Ainsi, pour réaliser cette opération de liaison, il faut, dans l'outil *Group Policy Management* (voir figure 7.1), faire un **clic-droit** sur l'élément auquel on souhaite appliquer la stratégie (le site, le domaine ou l'unité d'organisation) et choisir l'option **Link an Existing GPO**. Ensuite, il faut choisir la stratégie à appliquer.

Une fois liée, il est possible de spécifier les paramètres de filtre (*filtrage Security Filtering et WMI Filtering*) pour limiter la portée de la stratégie. Il est également possible de spécifier des paramètres de *délégation* (onglet *Delegation*). Ces paramètres mentionnent les utilisateurs (ou groupes) et autorisations applicables à la modification de cette stratégie. Ainsi, il est possible de définir une stratégie qui est gérée (i.e. déléguée) par quelqu'un d'autre. Il est ainsi possible de définir des administrateurs particuliers ayant des pouvoirs limités dans l'adaptation de la stratégie.

Les GPO sont mémorisées sur tous les contrôleurs de domaine dans le dossier %SystemRoot%\SYSVOL\Domain\Policies\GUID GPO. La GPO se matérialise en deux composants : un conteneur de stratégie de groupe et un modèle de stratégie de groupe. Ces fichiers sont répliqués entre les contrôleurs de domaine en cas de modification.

### 7.3 Paramètres d'une GPO

Les paramètres d'une GPO regroupent les stratégies que l'on peut activer. Comme dit précédemment, il y a des milliers de stratégies possibles.

Comme l'on peut le voir sur la figure 7.2, on distingue 2 sections principales : la *Computer configuration* et la *User Configuration*. A l'intérieur de chaque configuration, on trouve **les policies** (i.e. politiques applicables) et **les Preferences** (nouvelles à partir de Windows Server 2008).

Les **Policies** comprennent chacune les *Software Settings*, les *Windows Settings* et les *Administrative Templates*. Les *Software Settings* permettent une installation et un déploiement de programmes. Les *Windows Settings* permettent de définir des scripts, des paramètres de sécurité, rediriger des dossiers (dans le cas des utilisateurs), ... Il faut **bien distinguer les stratégies applicables à l'ordinateur et celles applicables à l'utilisateur**. Ainsi, la section *script* (présente des deux côtés) se comporte comme suit :

- Un script définit au niveau de la *Computer Configuration* s'exécute au démarrage ou à l'arrêt de la machine alors qu'aucun utilisateur n'est connecté
- Un script définit au niveau de la *User Configuration* s'exécute au démarrage ou à l'arrêt de la session de l'utilisateur (par conséquent, on sait qui se connecte et le script s'exécute avec les droits de ce dernier).

Dans l'élément *Administrative Templates*, on trouve des stratégies de configuration de l'environnement utilisateur ou ordinateur. Il est ainsi possible de limiter l'accès à certaines fonctionnalités : verrouillage de l'ordinateur, accès au panneau de configuration, ...

Etant donné le nombre de stratégies différentes (plusieurs milliers), elles sont présentées de manière hiérarchique dans des dossiers les regroupant logiquement.

Les **Preferences** sont des nouveaux éléments introduits à partir de Windows Server 2008 et Windows Vista. Elles permettent une gestion centralisée des variables d'environnement, de certaines applications, des disques réseaux, ... Ces préférences sont également intéressantes pour gérer les connexions aux imprimantes, ...

## 7.4 Etude de l'étendue d'une stratégie de groupe

Comme nous l'avons vu, plusieurs stratégies de groupe peuvent être applicables à un ordinateur ou un utilisateur. En effet, il est possible de *lier* une stratégie à un site, un domaine ou une unité d'organisation en sachant que celle-ci se propage à tous les éléments enfants (effet d'héritage).

Il est même possible de lier une stratégie de groupe à **plusieurs** unités d'organisation. Cette particularité peut s'avérer utile pour des unités d'organisation qui ne sont pas parentes (par exemple pour appliquer une même stratégie aux membres de l'unité Professeur et Etudiant).

Cependant, cette liaison et cet héritage complexifient un peu la stratégie applicable à un élément. En effet, quels sont les éléments prioritaires ? Que se passe-t-il si des éléments contradictoires, de deux stratégies différentes sont définis ? Lesquels s'appliquent ?

### 7.4.1 Priorité

Pour connaître la priorité d'une GPO, il faut aller dans l'outil *Group Management Policy* et cliquer sur le conteneur souhaité (une unité d'organisation, le domaine, ...) et regarder l'onglet *Group Policy Inheritance*.

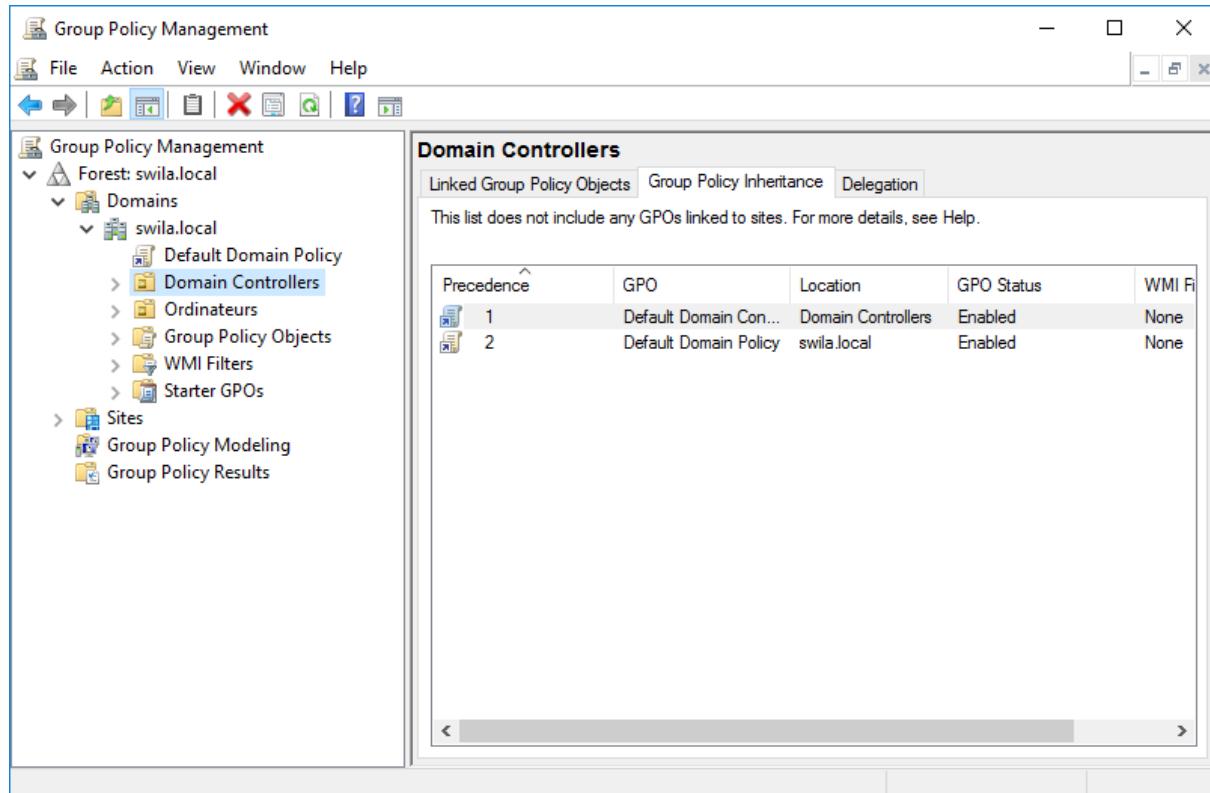


Figure 7.4 : Héritage des stratégies sur l'unité *Domain Controllers*

Comme nous pouvons le voir sur la figure 7.4, cet onglet renseigne les GPO applicables mais également leurs priorités. Il s'agit d'un élément important pour comprendre comment les stratégies définies vont effectivement s'appliquer sur les utilisateurs et ordinateurs membres du domaine. Dans notre exemple, nous remarquons que la GPO *Default Domain Controllers Policy* s'applique en premier (directement liée à l'unité d'organisation *Domain Controllers*) et ensuite, la GPO *Default Domain Policy* s'applique.

La priorité<sup>31</sup> avec laquelle les GPOs s'appliquent est la suivante (plus le numéro est élevé, plus la priorité est importante) : «

1. *L'objet de stratégie de groupe local (LPGO) est appliqué.*
2. *Les objets de stratégie de groupe (GPO) sont liés aux sites.*
3. *Les objets de stratégie de groupe (GPO) sont liés aux domaines.*
4. *Les objets de stratégie de groupe (GPO) sont liés aux unités d'organisation. Dans le cas d'unités d'organisation imbriquées, les GPO associés aux unités d'organisation parentes sont traitées avant les GPO associés aux unités d'organisation enfants.*

Ainsi, on pourrait résumer comme suit : le traitement des objets de stratégie de groupe (GPO) repose sur le principe selon lequel **le dernier qui écrit gagne**, et les GPO qui sont traitées ensuite ont priorité sur ceux qui ont été traités précédemment. »

Bien sûr, lorsque plusieurs GPO sont liées au même conteneur (à la même unité d'organisation par exemple), la priorité est définie par l'ordre des liens (montré dans l'onglet *Objets de stratégie de groupe liés*, premier onglet de la fenêtre figure 7.4).

Il est possible de modifier cet ordre de plusieurs manières. La première est la possibilité est l'option **Block Inheritance** sur un conteneur donné (une unité d'organisation par exemple). Ce faisant, cette unité n'hérite plus d'aucune autre GPO et seules les GPO directement liées à cette unité dans l'ordre mentionné s'appliquent. **Dans la plupart des cas, ce n'est pas une bonne manière de fonctionner**<sup>32</sup>. Il convient de limiter l'utilisation de cette possibilité lorsque celle-ci s'avère vraiment indispensable. Si nous reprenons l'exemple de la figure 7.4, bloquer l'héritage reviendrait à n'avoir que la seule GPO *Default Domain Controllers Poicy* active sur l'unité.

Une autre méthode pour modifier l'ordre de priorité est d'utiliser l'**option Enforced** d'une GPO. Dans ce cas, cette GPO *Enforced* se voit gratifiée de la priorité la plus grande. A nouveau, si dans notre exemple nous activons cette option sur la GPO *Default Domain Policy*, les priorités d'application des GPO sont, à nouveau, chamboulées : la GPO *Default Domain Policy* s'applique d'abord. **Attention !** L'option *Enforced* est prioritaire sur la possibilité de bloquer l'héritage. De plus, activer cette option sur une GPO définie à un niveau supérieur est toujours prioritaire sur l'activation de l'option sur une GPO définie dans l'objet courant (ainsi, activer *Enforced* sur la GPO *Default Domain Policy* et *Default Domain Controllers Policy* implique un ordre de priorité suivant : *Default Domain* puis *Default Controllers*). Ce choix est finalement assez logique, cela permet à une entreprise de définir une politique de sécurité globale appliquée à toute l'entreprise et non modifiable par un administrateur local (en charge de la gestion des stratégies d'une GPO, d'une branche de l'entreprise, ...).

<sup>31</sup> Extrait de [http://technet.microsoft.com/fr-fr/library/cc757050\(v=ws.10\).aspx](http://technet.microsoft.com/fr-fr/library/cc757050(v=ws.10).aspx)

<sup>32</sup> Ainsi, appliquer cette option doit être une exception, plutôt qu'une règle.

### 7.4.2 Application

Nous avons vu précédemment qu'il était possible de restreindre l'application d'une GPO en utilisant les options de filtres. Cette possibilité permet, par exemple, d'appliquer une GPO à un groupe de sécurité donné ou un type d'ordinateur défini. Par contre, il est souvent intéressant d'**exclure un groupe** d'une GPO afin que celle-ci ne s'applique jamais aux membres de ce groupe. Pour y arriver, il faut passer par l'onglet *Delegation* sur une GPO (qui permet normalement de déléguer la gestion d'une unité à un groupe donné). Il est possible de modifier le droit associé (via l'option *Advanced*) sur l'unité et cocher *Deny* pour la permission *Apply group policy* (qui refusera l'application de la stratégie).

Il est également possible de définir des filtres dans la section *WMI Filtering* pour restreindre l'application d'une GPO à une configuration donnée. Des exemples de tels filtres sont donnés sur le site suivant : <https://docs.microsoft.com/en-us/windows/access-protection/windows-firewall/create-wmi-filters-for-the-gpo>.

Ainsi, pour cibler les ordinateurs dont la configuration est Windows 10 ou Windows Server 2016, il est possible d'utiliser la requête WMI suivante (tirée du livre de référence [70-742]) :

```
Select * FROM Win32_OperatingSystem WHERE Version LIKE "10.%"
```

Ainsi la GPO ne s'applique alors qu'à ces seules configurations.

Enfin, il est également possible (via l'option *GPO Status* dans l'onglet *Details*) d'activer ou désactiver des paramètres définis dans la *Computer Configuration* ou de la *User Configuration* d'une GPO. Ainsi, une GPO peut être en état *Enabled* et donc tous les paramètres sont traités durant le déploiement, *All settings disabled* ainsi cette GPO n'est pas utilisée ou encore *computer configuration disabled* ou *user configuration disabled*. L'utilisation de ces options est à réserver à des cas très spécifiques !

### 7.4.3 La boucle de rappel

Parfois, on souhaite modifier la stratégie qui s'applique à l'utilisateur en fonction de l'ordinateur sur lequel il se connecte. Par exemple, un ordinateur particulier, sur lequel un logiciel précis tourne pourrait disposer de protection différente au niveau de la configuration utilisateur.

Or, la stratégie utilisateur s'applique quelque soit l'ordinateur sur lequel il se connecte. Afin de pouvoir personnaliser la stratégie utilisateur en fonction de l'ordinateur, Active Directory supporte le concept de *boucle de rappel*.

C'est une stratégie *Computer Configuration* visible dans Policies\Administrative Templates\System\Group Policy\Configure user Group Policy loopback processing mode. Ce paramètre peut être *not configured*, *enabled* ou *disabled*. Une fois activé (*enabled*), cette stratégie propose deux modes de fonctionnement : **replace** qui permet de ne pas tenir compte de la stratégie actuelle de l'utilisateur mais de traiter tous les utilisateurs sur base de la configuration utilisateur de cette stratégie ; **merge** qui permet d'ajouter des nouvelles stratégies à la stratégie utilisateur (uniquement applicable à la connexion sur cet ordinateur). La boucle de rappel sera étudiée plus précisément dans une leçon ultérieure.

## 7.5 Déterminer la stratégie appliquée

Comme nous l'avons décrit, les stratégies applicables à l'utilisateur et à l'ordinateur peuvent être multiples, héritées, liées, et parfois, des configurations viennent compliquer les choses comme les options *Enforced* ou *block inheritance* sans oublier l'activation de *la boucle de rappel* ou encore *les filtres*. Tous ces mécanismes rendent difficile l'analyse en cas de défaillance d'une configuration.

En effet, il est dès lors peu aisé d'identifier clairement les stratégies qui sont appliquées à un utilisateur donné. Pour ce faire, il est possible de déterminer le *jeu de stratégie résultant* (*RSoP* pour *Result Set of Policies*) qui analyse et déduit la stratégie appliquée. RSoP peut envoyer une requête à un ordinateur concernant la stratégie appliquée à celui-ci ou à un utilisateur qui se connecterait sur ce dernier. Le rapport est intéressant pour analyser et comprendre ce qui se passe.

Cet outil existe en deux versions : dans la console *Group Policy Management* (figure 7.4), on peut voir, comme dernière option sur la gauche, l'élément **Group Policy Results**. Grâce à cette option, il est possible en faisant un **clic-droit** sur le panneau de droite de choisir l'option **Group Policy Results Wizard**. Une fois les options spécifiées, le système affiche un rapport précisant la stratégie appliquée.

La seconde version de l'outil est un *programme exécutable nommé gpreresult.exe*. Ce programme rédige un rapport HTML mentionnant la stratégie applicable en fonction des options activées. L'aide de cet outil est disponible ici : **gpreresult.exe /?**.

## 7.6 Quelques stratégies courantes

### 7.6.1 Connexion à des dossiers partagés

Un des grands avantages de l'utilisation des GPO est la possibilité de **connecter automatiquement** les lecteurs réseaux des utilisateurs sans devoir faire les modifications manuellement à l'intérieur de chaque session.

Pour ce faire, il y a 2 méthodes : l'utilisation d'un **script d'ouverture de session** et l'utilisation de la commande `net use` vue précédemment. Cette méthode était utilisée pour connecter les lecteurs réseaux sur des systèmes antérieur à Windows Vista / Windows Server 2008. L'autre méthode est de passer par les **préférences** dans la stratégie. Nous allons présenter les deux.

En ce qui concerne **le script**, il faut aller dans `User Configuration\Policies\Windows Settings\Scripts\Logon` et puis ajouter un nouveau script à l'emplacement proposé (ou bien dans un chemin réseau accessible). Les scripts supportés sont les scripts batch (fichier `.bat`) ou Powershell pour des ordinateurs clients Windows 7 et suivants (fichier `.ps1`).

En ce qui concerne **les préférences**, il faut aller dans `User Configuration\Preferences\Windows Settings\Drive Maps`. Il convient alors d'ajouter un nouveau mappage en mentionnant, comme emplacement, un chemin réseau `\SERVEUR\Partage`.

### 7.6.2 Ouvrir une session sur le contrôleur de domaine

Il est parfois utile de permettre à certains utilisateurs d'ouvrir une session locale sur le contrôleur de domaine. Pour activer cette option, **il faut modifier** une GPO existante : **Default Domain Controllers Policy**. L'élément à modifier se trouve dans : `Computer Configuration\Policies\Windows Settings\Scripted GPOs\Default Domain Controllers Policy`.

Settings\Security settings\Local Policies\User Rights Assignment\Allow log on locally. **Attention, il convient d'ajouter les utilisateurs / groupes souhaités sans modifier les valeurs déjà définies !**

### 7.6.3 Ne pas afficher le dernier utilisateur connecté

On remarque que, par défaut, le système mentionne le dernier utilisateur connecté sur la machine. Ce comportement peut être dérangeant sur des ordinateurs partagés. Dès lors, il faut modifier la stratégie suivante : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name.

**Attention !** Il s'agit d'une stratégie sur l'ordinateur, elle s'applique donc aux objets ordinateurs d'Active Directory. Elle doit donc être placée dans une branche contenant de tels objets.

### 7.6.4 Redirection des dossiers

Comme nous l'avons vu, le profil de l'utilisateur reprend toutes ses informations. Depuis le passage en domaine, il convient de mentionner un chemin réseau pour le profil de l'utilisateur. Nous avons également vu que lors de la connexion en utilisant un profil itinérant, celui-ci était copié sur la machine locale, géré localement, puis recopié sur le serveur lors de la déconnexion. Enfin, nous avons également vu que **plusieurs versions** du profil (suffixées par « .V2 » ou « .V6 ») peuvent être créées suivant la version du système.

Le problème est que, plus le profil grossit (nouveaux documents, fichiers importants sur le bureau, ...), plus le temps de connexion grandit également. Une solution à ce problème est de *rediriger* les dossiers importants (Bureau, Mes documents, ...) dans un espace réseau. De cette manière, ces informations ne sont plus recopierées sur chaque machine, elles restent sur le serveur et la modification est réalisée directement depuis cet endroit. De plus, elles sont communes à toutes les versions du profil.

Ainsi, il est tout à fait possible de préciser une stratégie pour rediriger ces dossiers. Il faut modifier le paramètre suivant : User Configuration\Policies\Windows Settings\Folder Redirection et choisir les modifications souhaitées. Il convient, bien sûr, de préciser un chemin réseau vers l'emplacement souhaité.

Pour que la modification soit effective dans tous les cas, il faut également ajouter une stratégie sur les ordinateurs concernés : Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure folder redirection policy processing.

### 7.6.5 Et le reste ...

Il existe des milliers de stratégies possibles et il n'est pas possible de les détailler toutes ici. Il est parfois difficile de trouver une stratégie voulue. C'est pourquoi Microsoft a introduit une option de filtre sur la branche *Administrative Templates*. Cette option est particulièrement intéressante pour trouver une stratégie dans l'ensemble. Pour l'activer, il suffit de faire un **clic-droit** sur *Administrative Templates* puis **Filter Options**.

## 7.7 Exercices

1. Empêcher les membres des catégories *étudiants* et *e-learning* d'avoir accès à l'outil d'édition du registre. **Créez une seule GPO liée aux OUs concernées.**
2. Empêcher tous les utilisateurs, excepté les membres de la catégorie *informatique*, de lancer l'invite de commande. **Limitez aux utilisateurs concernés en utilisant les filtrages de sécurité (Security Filtering) uniquement.**
3. Créer un partage réseau SharedSocial et connecter les membres de la catégorie *social* à ce partage **en utilisant un script batch** (lecteur X:, accès en modification pour *social*, inaccessible pour les autres). Ajoutez une GPO Ordinateur « *Configure Logon Script Delay* » à 0 minute, sur les postes clients (VM Windows 10).
4. Pour protéger la stratégie des mots de passe du domaine, arrangez-vous pour que celle-ci soit toujours prioritaire (en 1<sup>ère</sup> position dans l'onglet *Group Policy Inheritance*).
5. Permettre aux membres de la catégorie *informatique* d'ouvrir une session locale sur le contrôleur de domaine
6. Pour des questions de sécurité, on ne souhaite pas voir apparaître le nom de la dernière personne connectée sur les postes clients (VM Windows 10).
7. Réaliser une redirection de dossier (tous) pour les membres de la catégorie *travaux* de sorte que les dossiers soient placés dans leur profil. Ainsi, leur bureau devra se trouver dans CGData\<login>\Desktop (et ainsi de suite pour tous les dossiers).
8. Créer un partage réseau SharedPublic et connecter tous les utilisateurs à ce partage au moyen d'une préférence (lecteur Q:, tout le monde en lecture, *direction* en modification).
9. Pour s'amuser : restrictions pour les membres de la catégorie *juridique* :
  - a. Supprimer : l'accès au menu contextuel de la barre des tâches, Supprimer l'horloge,
  - b. Le bureau : supprimer tous les éléments du bureau
  - c. Système : Désactiver le verrouillage de l'ordinateur ; supprimer le gestionnaire des tâches

## Leçon 8 : gestion des GPO

Dans cette leçon, nous allons aborder la **délégation de la gestion** des ordinateurs à d'autres utilisateurs prenant le rôle d'administrateur. Nous aborderons également le déploiement d'un logiciel sur l'ensemble du domaine et, finalement, les options d'audit.

Cette leçon suit le livre de référence suivant :

[70-742] A. Warren, Exam Ref 70-742 : Identity with Windows® Server® 2016, 1<sup>st</sup> edition, Microsoft Press, March 2017

### 8.1 Déléguer la gestion

Il y a plusieurs manières de déléguer des tâches sur des réseaux Microsoft. Ainsi, on peut *déléguer l'administration de certaines machines* à des utilisateurs particuliers (qui sont alors administrateurs de ces machines). On peut également déléguer *la gestion de tâches d'administration* comme la gestion des utilisateurs, par exemple, à un ou plusieurs utilisateurs.

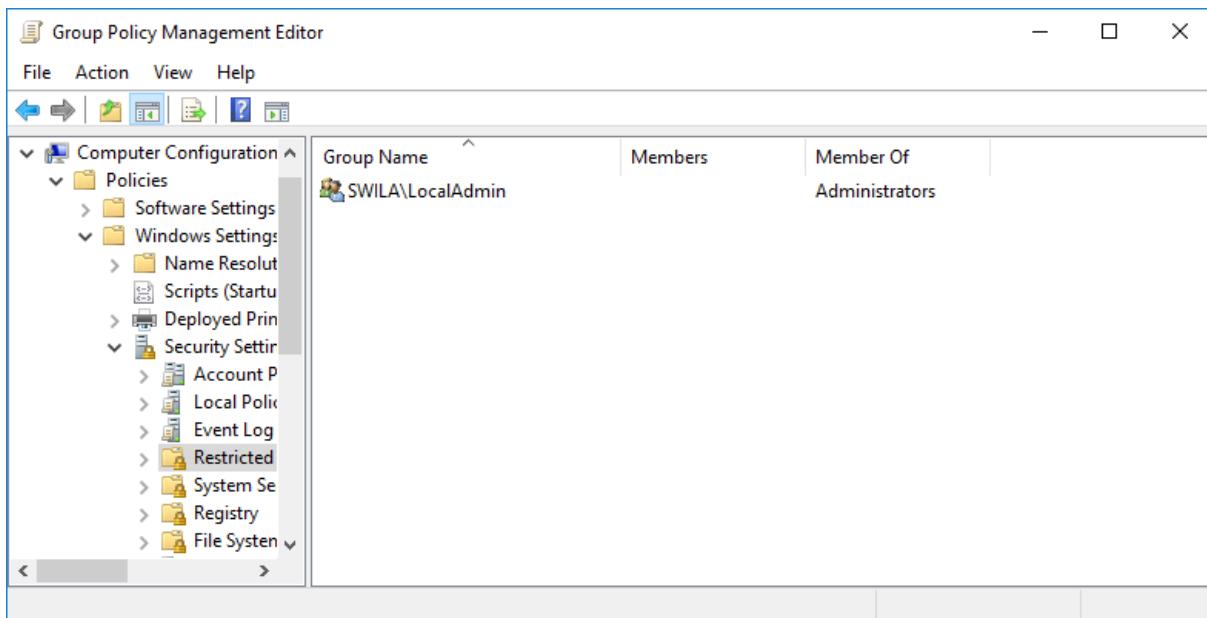
#### 8.1.1 Déléguer l'administration de machines

Il est parfois nécessaire de pouvoir *déléguer l'administration d'un groupe de machines* à des utilisateurs différents de l'administrateur. Pour rappel, sur les machines, il y a un groupe *local Administrators*. Les membres de ce groupe sont des administrateurs *locaux* et peuvent réaliser des tâches d'administration telles que : installation de pilotes, ajout et configuration d'imprimantes, configuration réseau .... Ainsi *déléguer l'administration des machines* revient à donner des droits d'administrateur sur ces machines.

Si nous définissons un groupe de sécurité *LocalAdmin* sur le domaine, il est possible d'ajouter ce groupe au groupe local *Administrators* sur *chaque machine*. Cette opération peut vite se révéler très contraignante, dans ce cas, nous pouvons ajouter cette appartenance sur toutes les machines concernées directement au moyen d'une GPO.

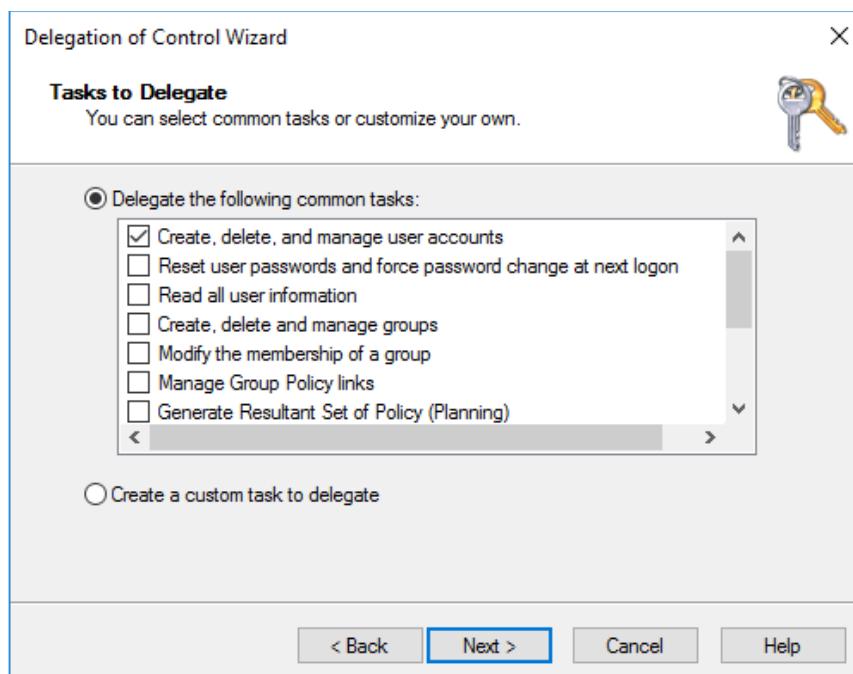
Cet élément de configuration est **une GPO Ordinateur** (ie. *Computer Configuration*). Il faut modifier l'option *Restricted Groups* qui se trouve dans *Computer Configuration\Policies\Windows Settings\Security Settings*. Ensuite, il faut, par un *clic-droit*, choisir **Add Group** et mentionner, par exemple *SWILA\LocalAdmin* et mentionner que **ce groupe est membre de** (option *This group is member of*, en bas) *Administrators*. Une fois cette manipulation terminée, tous les ordinateurs sur lesquels cette GPO s'applique verront leur groupe local *Administrators* modifié avec *SWILA\LocalAdmin* comme membre.

Tous les membres du groupe de sécurité *LocalAdmin* sont désormais *Administrateurs locaux des ordinateurs appliquant cette GPO*.

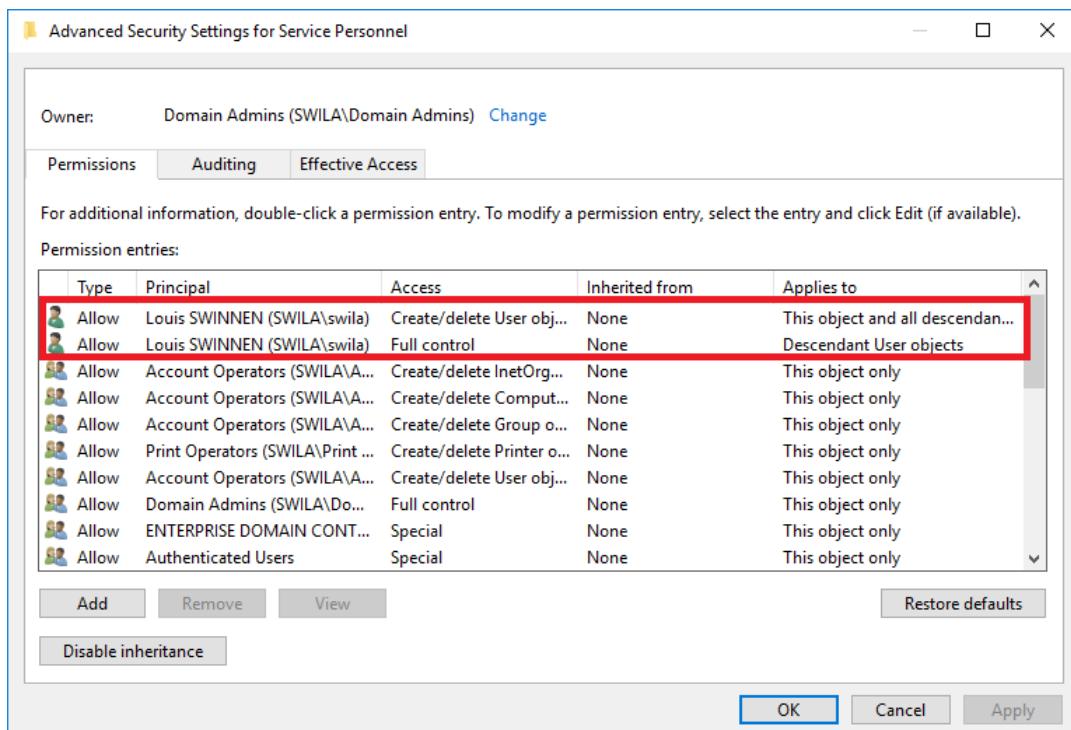


### 8.1.2 Déléguer des tâches d'administration AD

Il est possible de déléguer la gestion de certaines parties d'Active Directory à des utilisateurs qui ne sont pas des administrateurs. Nous avons déjà vu qu'il est possible de déléguer, à des utilisateurs, la gestion d'une GPO liée à une unité d'organisation.



Nous pouvons également déléguer la possibilité de créer des objets dans une branche d'Active Directory au moyen de la **Délégation de contrôle** (clic-droit sur l'élément, **Delegate Control**). Il est ainsi possible de préciser les actions qui sont déléguées à l'utilisateur ou au groupe d'utilisateurs renseigné. Une fois la délégation de contrôle effectuée, il est possible de visualiser / modifier / supprimer les autorisations via les *Advanced Security Settings* (clic-droit **Properties** puis **Security** puis **Advanced**).



Une fois la délégation terminée, l'utilisateur peut accéder aux éléments d'Active Directory par les outils d'administration ou via une console MMC spécifique pour gérer sa branche.

## 8.2 Installation et déploiement de logiciels

Il est possible de procéder à l'installation et au déploiement de logiciels via une GPO. Cette possibilité peut être intéressante si de nombreuses machines sont mises à disposition des utilisateurs et que ces derniers doivent pouvoir utiliser un *pack* de logiciels identiques quel que soit la machine sur laquelle ils se connectent.

Cette possibilité d'installation se base sur le service *Windows Installer*. Il est donc important de savoir que **seuls les logiciels utilisant ce service d'installation peuvent être déployés via une GPO**. Pour être plus précis, il est nécessaire de disposer du logiciel à installer sous la forme d'un fichier *.msi*. Si le logiciel n'est pas disponible sous le format MSI, le déploiement au travers d'une GPO ne sera pas possible.

Il existe bon nombre de systèmes de déploiement de logiciels à travers des réseaux, mais ceux-ci sont des applications supplémentaires et payantes à ajouter aux serveurs et postes clients. Il est important de remarquer que si le nombre de postes de travail de l'entreprise est élevé, ces outils de gestion et maintien de la configuration sont indispensables. Dans des environnements plus réduits, l'outil de déploiement à travers une GPO peut suffire.

### 8.2.1 Configuration Ordinateur ou Configuration Utilisateur

Le déploiement de logiciel est présent à la fois dans la partie **Computer Configuration** et **User Configuration**. A l'instar de l'option d'exécution des scripts, il y a une différence entre configurer un déploiement au niveau utilisateur et au niveau ordinateur.

En effet, en mode *Computer Configuration*, le déploiement est d'office en mode *Assigned* alors qu'en mode *User Configuration*, les modes de déploiement possibles sont *Assigned* ou *Published*. Nous allons expliquer ces deux modes dans la suite :

- **Pour une configuration utilisateur (*user configuration*),**
  - Le déploiement en mode « *published* » permet d'installer l'application via le *Control Panel > Programs and Features* et puis en choisissant *Install a program from the network*. Il faut donc que l'utilisateur **choisisse** d'installer l'application pour que celle-ci soit présente. Cette option d'installation est disponible sur *toutes les machines* sur lesquelles l'utilisateur se connecte.
  - Le déploiement en mode « *assigned* » montre l'application *comme si* elle était déjà installée (icône sur le bureau, groupe dans le menu démarrer). Lorsque l'utilisateur clique sur le programme, il est installé (si ce n'était pas déjà fait) puis est utilisé. L'application est donc ici installée en fonction des besoins.
- **Pour une configuration ordinateur (*computer configuration*),**
  - Le déploiement en mode « *assigned* » permet d'installer le package durant le démarrage de la machine. Cette application est donc installée de manière silencieuse avant de permettre la connexion d'un utilisateur sur le système. Cette option peut être très intéressante pour déployer un nouveau programme rapidement sur l'ensemble d'un parc de machines.

Lorsqu'on supprime la GPO de déploiement du logiciel, le système vous demande de décider s'il faut laisser l'application installée (pour les utilisateurs et/ou machines sur lesquelles elle est déjà déployée) ou supprimer l'application.

Le mode **Advanced** permet de spécifier des options particulières. Ainsi, il est possible d'ajouter, via l'onglet **Modifications**, des fichiers MST qui sont *des modifications à l'installation de base* ou encore des fichiers MSP qui sont *des correctifs (Patch)*.

### 8.2.2 Distribution par le réseau

Il est important que les applications mises à disposition soient disponibles depuis le réseau. Il est donc important de **configurer un partage** pour distribuer et gérer le déploiement des applications. L'autorisation de *Lecture* est nécessaire sur le partage alors que l'autorisation NTFS de *lecture et exécution* est nécessaire sur le fichier à déployer.

Ainsi le chemin vers le package d'installation doit toujours être un chemin réseau de la forme \\SERVER\Partage\Package.msi.

### 8.2.3 Configurer la GPO de déploiement

1. Décider le mode de déploiement (User ou Computer – Assigned ou Published).
2. Placer le fichier d'installation MSI dans un dossier partagé accessible.
3. Créer une nouvelle GPO de déploiement. Il faut procéder comme suit,
  - a. dans le cas d'une GPO computer :

- i. Computer Configuration \Policies\Software Settings\Software Installation puis choisir **New** puis **Package**.
  - ii. Choisir le MSI d'installation
  - iii. Sélectionner le type de déploiement (*assigned* ou *advanced*). Le mode *advanced* permet de préciser de nombreuses options.
  - iv. Appuyer sur **OK**
  - v. Lier cette stratégie à **une unité d'organisation** contenant des objets **ordinateurs**
- b. Dans le cas d'une GPO user :
    - i. User Configuration \Policies\Software Settings\Software installation puis choisir **New** puis **package**
    - ii. Choisir le MSI d'installation
    - iii. Sélectionner le type de déploiement (*published*, *assigned* ou *advanced*). Le mode *advanced* permet de préciser de nombreuses options.
    - iv. Appuyer sur **OK**
    - v. Lier cette stratégie à **une unité d'organisation** contenant des objets **utilisateurs**.

Le déploiement par poste de travail (par ordinateur) semble plus naturel. Cependant, en fonction des contrats de licence négociés, l'installation par utilisateur peut être une option intéressante.

#### 8.2.4 Maintenance

Une fois l'installation déployée sur un ordinateur, ce dernier n'essaiera plus d'installer le logiciel, et ce même si le package logiciel change. Ainsi, si une mise à jour est nécessaire, il est nécessaire de modifier la GPO pour que celle-ci provoque une modification de l'installation effectuée.

De plus, lorsqu'un problème survient, il est parfois nécessaire d'effectuer un redéploiement, par l'option « *redeploy application* ». Les options de maintenance sont disponibles dans la GPO.

Pour **mettre à jour** un package logiciel, il faut soit créer une nouvelle GPO et ajouter la nouvelle version du package, soit modifier la GPO déjà créée en ajoutant le nouveau package. Il convient de choisir le mode de déploiement **Advanced** (ou alors de reprendre l'option au moyen d'un clic-droit **Properties**) et, dans l'onglet **Upgrades**, choisir le package logiciel qui est mis à niveau. Lors de la configuration, il est possible de spécifier si l'ancienne version doit être désinstallée au préalable ou non.

Pour provoquer un **redéploiement d'une application**, il faut se rendre dans la GPO contenant le package à déployer et, via un **clic-droit** sur ce package, choisir l'option **All Tasks** puis **Redeploy application**.

Pour **supprimer une application déployée**, il suffit de supprimer le package dans la GPO déployant ce logiciel (**clic-droit** puis **All tasks** puis **Remove**). A ce moment, le système vous demande s'il faut supprimer les packages qui ont été installés sur les machines ou si l'on peut permettre aux utilisateurs de continuer à utiliser le logiciel, tout en empêchant de nouvelles installations.

### 8.3 Stratégies d'audit

Les audits permettent de consigner dans les journaux systèmes des événements déterminés. Cela permet de *tracer* les actions des utilisateurs sur le réseau. La capacité d'audit est assez importante

puisque il est possible de consigner aussi bien les tentatives *réussies* que les tentatives *ratées* (connexion par exemple).

Il est également possible de consigner l'accès aux différentes ressources (accès à un partage par exemple) dans les journaux d'audit.

Il faut être vigilant : il est possible d'activer les audits sur beaucoup d'éléments du système. **Vouloir tout auditer ne mène à rien** étant donné la masse considérable d'information que cela représente. Ainsi vouloir auditer trop d'élément conduit à remplir les journaux d'audit et les rendre illisible car l'information vraiment intéressante est perdue parmi l'ensemble.

De plus, organiser la surveillance des différents éléments par le système et écrire dans les fichiers journaux est une **opération qui a un coût** (négligeable si cette opération n'est faite qu'aux moments intéressant mais élevé si cette opération survient fréquemment).

Il convient donc de garder une bonne gestion en auditant les éléments qui semblent important, en **limitant un audit élevé dans le temps** (pour trouver une anomalie par exemple), ...

Il faut tenir compte que les contrôleurs de domaine sont configurés pour auditer un certain nombre d'éléments : *la création réussie d'un utilisateur*, *la réinitialisation réussie d'un mot de passe*, *la connexion réussie au domaine*, *la récupération réussie du script d'ouverture de session*. Il est souvent intéressant d'ajouter des audits d'échec permettant de consigner les événements (i.e. tentatives) qui n'ont pas aboutis.

### 8.3.1 Modifier la stratégie d'audit

Il est possible de créer une stratégie d'audit en ajoutant une GPO et en activant un paramètre dans Computer Configuration \Policies\Windows Settings\Security Settings\Local Policy\Audit Policy. Depuis Windows Server 2008 R2, il y a également la possibilité d'utiliser une stratégie d'audit avancée dont les paramètres sont disponibles ici : Computer Configuration \Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration.

### 8.3.2 Accès aux objets et audit

Il est également possible d'auditer l'accès aux objets (dans Active Directory ou sur le système de fichiers comme un dossier ou à un fichier). Cette option d'audit se trouve dans les paramètres de sécurité associés à l'objet (*advanced security settings* de l'unité d'organisation, d'un fichier ou d'un dossier). Pour y accéder, il faut faire un **clic-droit** sur l'objet concerné **Properties**, choisir l'onglet **Security** puis **Advanced** et enfin aller dans l'onglet **Auditing**. Il est possible d'auditer *la réussite (Success)* ou *l'échec (fail)* à un certain nombre d'accès. L'audit peut être restreint à un utilisateur ou groupe donné.

Dès qu'un audit sur un objet est réalisé, il faut également **activer des stratégies** particulières nommées : *Audit object access* (fichiers ou dossiers) et *Audit directory service access* (éléments dans Active Directory) dans la GPO. Sans cette activation, les modifications réalisées au niveau de l'audit de l'objet seront sans effet.

### 8.3.3 Visualiser les audits

Une fois la stratégie d'audit installée, il est possible d'en observer les résultats en consultant les journaux systèmes. En effet, dans l'outil **event viewer**, on trouve, dans les journaux *Windows Logs*, le journal *Security* reprenant tous les audits configurés.

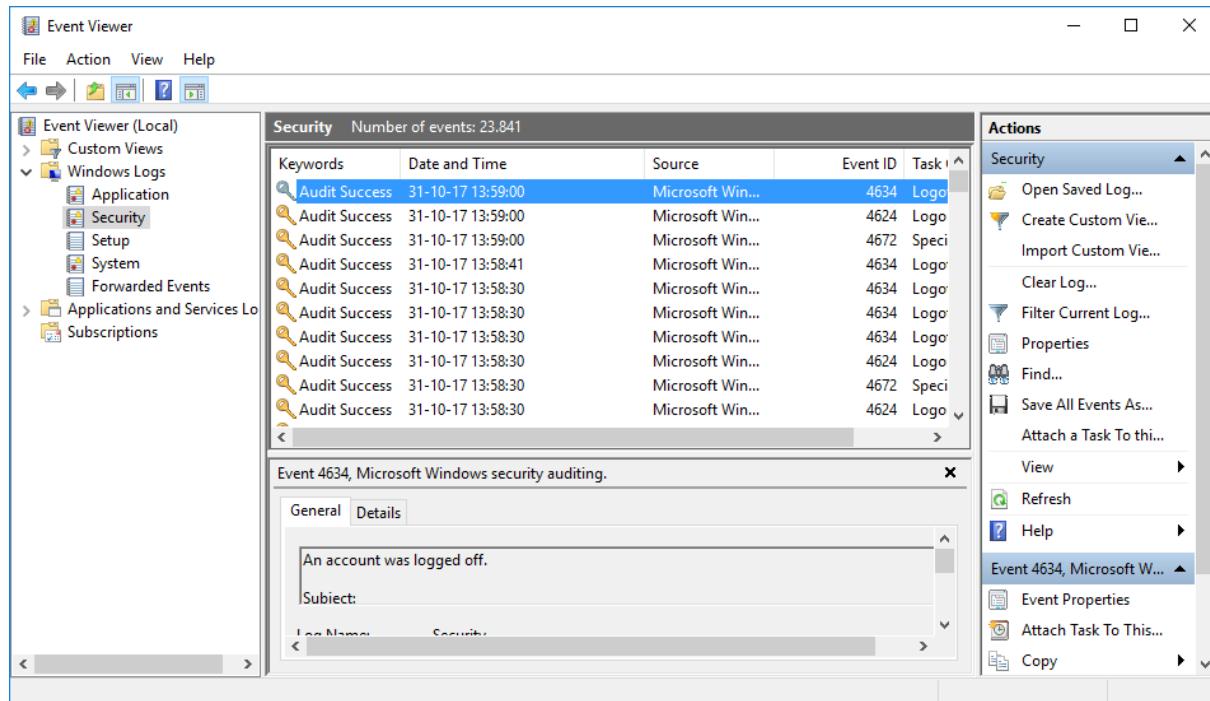


Figure 8.1 : Visualiser les audits

### 8.4 La boucle de rappel

Lors de la leçon précédente, nous avons abordé le concept de boucle de rappel. Cependant, il me semble important de revenir sur ce point étant donné la spécificité de celle-ci et l'importance de son utilisation dans le monde professionnel.

Pour rappel, une GPO contenant une *user configuration* doit être liée à des objets utilisateurs dans Active Directory alors qu'une GPO contenant une *computer configuration* doit être liée à des objets ordinateurs (une unité d'organisation par exemple). C'est assez logique puisque les stratégies s'appliquent à des objets différents et il est souvent bon de séparer, dans la structure d'Active Directory, les objets ordinateurs et utilisateurs.

#### 8.4.1 L'exception boucle de rappel

L'activation de la boucle de rappel se fait sur des objets *ordinateurs*. Lorsque celle-ci est active et qu'un utilisateur se connecte, la GPO qui devrait être appliquée n'est plus celle dont il a hérité.

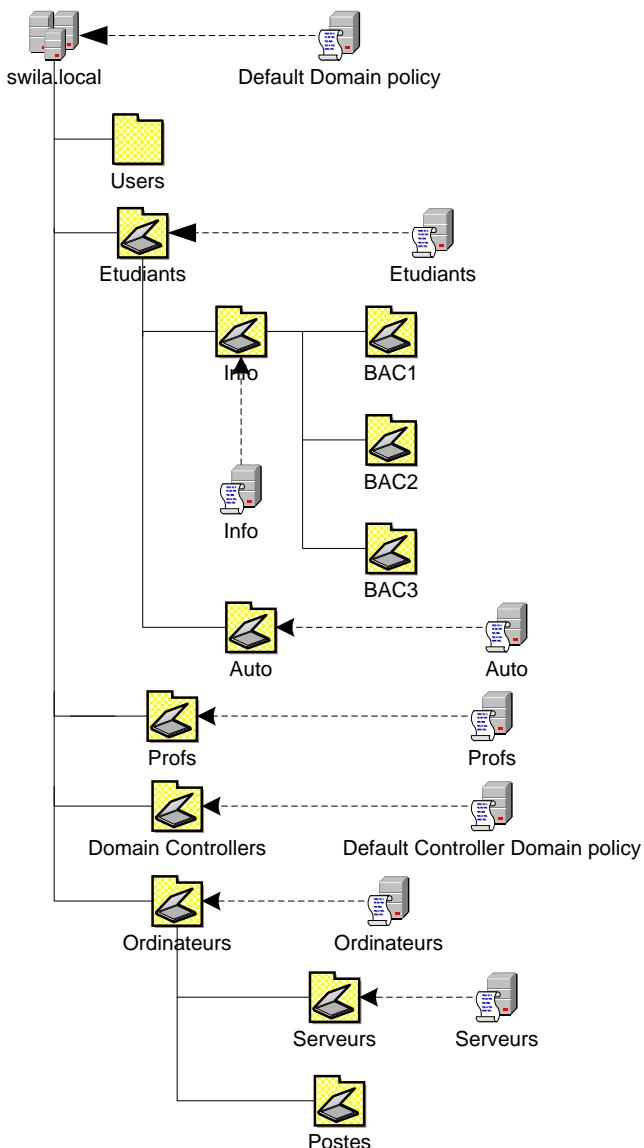


Figure 8.2 : Structure possible d'Active Directory

Sur la figure 8.2, si nous activons la boucle de rappel au niveau de stratégie *Serveurs* liée à l'unité d'organisation *Serveurs*, et qu'un utilisateur membre du groupe *Profs* par exemple se connecte sur une machine de cette unité, la stratégie qui lui sera appliquée sera modifiée.

En effet, la boucle de rappel supporte 2 modes de fonctionnement :

- Mode **merge** : la stratégie utilisateur va être modifiée en ajoutant les éléments contenus dans la configuration utilisateur de la boucle de rappel
- Mode **remplace** : la stratégie utilisateur va être supprimée et remplacée par les éléments contenus dans la configuration utilisateur de la boucle de rappel.

Ainsi, dans notre exemple, si nous activons, dans la GPO *Serveurs* la boucle de rappel et qu'un membre de l'unité d'organisation *Profs* se connecte, la stratégie utilisateur qui lui sera appliquée sera : GPO *Profs* + GPO *Serveurs* (mode *merge*) ou GPO *Serveurs* (mode *replace*).

Nous voyons donc ici apparaître une contradiction par rapport à ce que nous avions dit précédemment. En effet, la GPO définissant la boucle de rappel contient à la fois des éléments de configuration ordinateur et utilisateur bien que, *seuls des objets ordinateurs* soient présents dans l'unité d'organisation.

Ce mode de fonctionnement est particulièrement intéressant lorsqu'on dispose de *serveurs partagés* entre plusieurs utilisateurs : la stratégie appliquée sur celui-ci peut donc être complètement différente de celle appliquée à l'utilisateur lorsqu'il se connecte ailleurs, sur une autre machine.

#### **8.4.2 Mise en place**

Il faut commencer par activer la stratégie *Configure user Group Policy loopback processing mode* qui se trouve dans Computer Configuration\Policies\Administrative Templates\System\Group Policy. Il faut ensuite décider s'il faut *ajouter des nouvelles stratégies à l'utilisateur* (mode **merge**) ou s'il faut *supprimer toutes les stratégies utilisateurs existantes pour n'avoir que celles définies dans la boucle de rappel* (mode **remplace**).

Ensuite, il faut définir les stratégies utilisateurs à ajouter ou remplacer. Nous allons donc, dans cette stratégie, ajouter des éléments *User Configuration* bien que celle-ci s'applique sur des ordinateurs.

Une fois ces paramètres définis, notre GPO est terminée.

## 8.5 Exercices

1. Modifier la structure de votre Active Directory en créant les OU suivantes dans CGComputers : Clients et Servers. Déplacer l'objet ordinateur correspondant à la VM Windows 10 dans l'OU Clients.
2. Installer un nouveau serveur Windows Server 2016 (en suivant la procédure de la leçon 1). Spécifier les informations suivantes :
  - a. Nom : Srv2016-2
  - b. IP : 192.168.190.40
  - c. Ajouter cette machine à votre domaine, dans l'OU Servers (cf. étape 1).
3. Créer un groupe de sécurité AdminMachines et ajoutez-y le groupe administratif
4. Déléguer le contrôle de l'OU personnel aux membres du groupe informatique.
5. Créer les GPO suivantes nommées comme indiqué :
  - a. auditObjet - GPO d'audit sur la création / suppression d'utilisateurs dans l'OU personnel (voir exercice 4)
  - b. outilsInstall - GPO d'installation sur les ordinateurs contenus dans l'OU clients. On vous demande de déployer les programmes *firefox 32.0* et *putty 0.69*. Vérifiez que l'installation s'est déroulée correctement sur votre VM Windows 10.
  - c. auditEchecConnexion - GPO d'audit sur tous les ordinateurs (clients et servers) du domaine consignant les échecs de connexion.
  - d. boucleRappel - GPO appliquée sur l'OU Servers, activation du mode boucle de rappel (en mode *merge*), **mais ne pas appliquer aux administrateurs**. Imposer les restrictions suivantes :
    - i. Start Menu : Supprimer l'entrée « Tous les programme », Supprimer l'horloge et supprimer l'option « Se Déconnecter »
    - ii. Desktop : supprimer l'icône de la corbeille, ne pas enregistrer les modifications. Supprimer l'icône Ordinateur du bureau.
    - iii. System : Désactiver le verrouillage de l'ordinateur, la modification du mot de passe et supprimer le gestionnaire des tâches
  - e. outilsInstall - Modifier la GPO, pour faire la mise à jour du programme *firefox* vers la version 52.4.1. Vérifiez que la mise à jour s'est propagée correctement sur la VM Windows 10.
  - f. clientAdmin - GPO pour déléguer l'administration des machines dans l'OU clients aux membres du groupe AdminMachines (créé à l'exercice 3)
6. Etablir un audit sur le partage SharedSocial créé précédemment (cf. leçon 7, exercice 3) pour consigner les ajouts et suppressions de fichiers ou dossiers par un membre du groupe social. Au besoin, vous modifierez la GPO auditObject créée à l'exercice 5.

## Leçon 9 : Backup et restauration

*"L'erreur est humaine, mais pour provoquer une vraie catastrophe, il faut un ordinateur"<sup>33</sup>*

### 9.1 Introduction

Une tâche importante des administrateurs concerne la gestion des sauvegardes. En effet, depuis le début de l'informatique, la sauvegarde des fichiers, des programmes et des données était et reste un problème difficile à gérer.

En fait, la masse d'information à sauvegarder n'a fait que croître, obligeant les administrateurs à toujours gérer cette tâche. Il faut être conscient qu'un backup qui ne se fait pas automatiquement est un backup qui risque de ne pas servir (manque de temps, oubli de l'utilisateur, ...). De même, compter sur les utilisateurs pour faire leur backup peut sembler idéal mais ne fonctionne pas.

Dès lors, des solutions de backup en tout genre ont vu le jour. Cela va d'une simple copie, régulière et automatique, de certains dossiers à un système de bande automatisé avec un robot chargé de placer la bande de lecteur à la demande de l'utilisateur en passant par des solutions *cloud* qui sauvegardent et synchronisent les données utilisateurs sur des serveurs éparpillés dans le monde entier. Tout dépend des moyens mis en place et de l'importance des données à sauvegarder.

### 9.2 Un peu de culture

Idéalement, un backup ne doit pas prendre trop de temps à l'administrateur car c'est du temps *relativement* improductif. De plus, il est bon d'avoir plusieurs backup des données à des endroits différents sur des médias différents, sous des formats différents.

Enfin, suivant les technologies utilisées, les programmes de backup peuvent être très différents. Ainsi, parmi les grands noms des programmes de backup, citons **Symantec Backup-Exec** qui est probablement un des outils les plus répandu dans la gestion des sauvegardes (fonctionnement notamment avec des lecteurs de bandes, ...), ou encore **Veeam backup** gérant des backup complets de machines virtuelles avec des options particulières pour pouvoir redémarrer un serveur depuis le backup.

A coté de ces grands noms, Microsoft propose, à l'intérieur de ces installations Windows Server, un outil de sauvegarde nommé **Windows Server Backup**. Cet outil, limité, est suffisant pour gérer les sauvegardes d'une petite entreprise.

En plus de cet outil, Microsoft propose également le système **des shadow copies (ou clichés instantanés)**. L'objectif est, à l'instar d'un système de gestion de version, de pouvoir revenir à une version précédente d'un fichier. La combinaison de ces deux outils permet d'obtenir un certain niveau de sécurité.

---

<sup>33</sup> [http://fr.wikipedia.org/wiki/Loi\\_de\\_Murphy](http://fr.wikipedia.org/wiki/Loi_de_Murphy)

## 9.3 Les clichés instantanés

Les clichés instantanés sont prévus pour mémoriser les versions précédentes des fichiers. Ils sont disponibles sur les partages réseaux. Cependant, comme tous les disques sont partagés par défaut (partage *administratif* c\$, d\$, ...), le disque entier fait, par défaut, l'objet d'un cliché instantané.

### 9.3.1 Activation des clichés

Comme expliqué ci-avant, les clichés instantanés permettent de *mémoriser* plusieurs versions des mêmes fichiers ou dossiers permettant ainsi de *revenir* à une version précédente d'un fichier (en cas de modification malencontreuse) ou de récupérer un fichier supprimé.

Bien sûr, l'utilisation des clichés instantanés consomme des ressources systèmes (de l'espace disque et du temps processeur) pour réaliser les sauvegardes. Cependant, le gain en termes de sécurité est réel. Ainsi, même les dossiers partagés sont également protégés par ce mécanisme (et donc si un utilisateur écrase un fichier par erreur, ce dernier peut être retrouvé facilement). De plus, il faut mentionner que l'utilisation des clichés instantanés permet à l'administrateur d'éviter de rechercher dans des sauvegardes diverses puisque la version souhaitée du fichier est directement disponible.

Pour **activer** les clichés instantanés, il faut aller démarrer **Server Manager > Tools > Computer Management**. Il faut ensuite choisir **Storage > Disk Management** et sélectionner le *volume* sur lequel on souhaite appliquer les clichés instantanés.

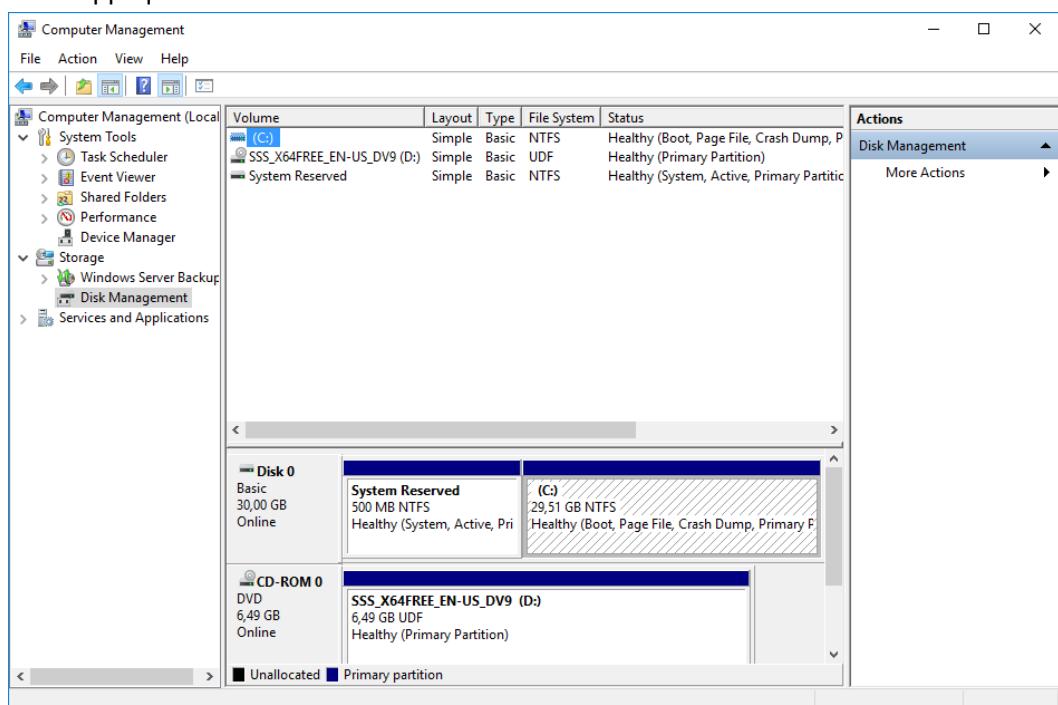


Figure 8.1 : Gestion des disques

© Louis SWINNEN 2020, tous droits réservés

Il suffit de faire un **clic-droit** sur le volume choisi et choisir **Properties**. Ensuite, il faut choisir l'onglet **shadow copies**. Par défaut, les clichés instantanés sont désactivés. Pour les activer, il faut d'abord cliquer sur le bouton *Settings*.

Dans les Paramètres, il est possible de choisir le volume *de stockage* (dans *storage area*) des clichés. Une bonne règle est de systématiquement placer ces clichés instantanés sur un autre volume (quand c'est possible). Ensuite, il est possible de définir l'espace disque alloué aux clichés instantanés. Cette information est importante puisque l'espace disque alloué à ces clichés va conditionner le *nombre de*

*versions* qui seront disponibles. Plus l'espace disque est grand, plus important sera le nombre de « *versions précédentes* » qui pourra être mémorisée (avec un maximum de 64 versions par fichier).

Le bouton *Schedule* permet de déterminer quand les clichés seront construits. Par défaut, la planification réalise deux clichés par jour : le premier à 7h et le second à 12h.

Bien sûr, les clichés reprennent les *versions différentes* des fichiers. Ainsi, si un fichier n'a pas été modifié, il n'y aura pas de *version précédente* liée à ce fichier.

Une fois la planification terminée, il faut encore **activer** les clichés sur le volume en cliquant sur le bouton **Enable**.

### 9.3.2 Retrouver une version précédente

Une fois les clichés instantanés activés, il est possible de revenir à *des versions précédentes* d'un fichier de plusieurs manières. La première, pour l'administrateur, est de faire un **clic-droit** puis **Properties** sur le volume dans **Server Manager > Tools > Computer Management** (figure 8.1). L'onglet **Previous Versions** affiche les versions disponibles.

Une fois la version choisie, il est possible de cliquer sur **Open** et on peut ainsi naviguer sur le disque local en voyant uniquement les fichiers présents à cette date là. Ainsi l'administrateur peut facilement retrouver le dossier ou le fichier que l'utilisateur souhaite récupérer.

De plus, l'utilisateur a, lui-même, la possibilité de retourner à une version précédente d'un fichier ou dossier. En effet, les partages disques sont couverts par le système des clichés. Dès lors, un utilisateur peut, sur un dossier contenu dans un partage donné, faire un **clic-droit** puis **properties** et choisir l'onglet **previous versions**. Ainsi, il lui est possible de retrouver une version précédente du fichier souhaité sans le demander à l'administrateur. Bien sûr, il ne peut agir que sur les dossiers, partages, pour lesquels il dispose des droits nécessaires.

### 9.3.3 Supprimer les clichés instantanés

Si vous choisissez de *désactiver* les clichés instantanés d'un volume (via le bouton **Disable**), le système supprimera tous les clichés mémorisés sur le serveur. Cela conduira à un gain de place mais à la perte des sauvegardes réalisées. Cependant, si vous souhaitez modifier certains paramètres concernant les clichés instantanés (volume sur lesquels ils sont sauvegardés par exemple), leur désactivation préalable est nécessaire.

### 9.3.4 Clichés instantanés d'Active Directory

Il est également possible de réaliser des clichés instantanés d'Active Directory afin de retrouver un état donné de l'annuaire. L'outil à utiliser est disponible *en ligne de commande* uniquement.

Pour **créer** un cliché, il faut entrer la commande suivante :

```
C:\> ntdsutil
ntdsutil : snapshot
snapshot : activate instance ntds
Active instance set to « ntds ».
snapshot : create
Creating snapshot...
snapshot : quit
ntdsutil : quit
```

Cette méthode interactive permet de créer un cliché instantané pour Active Directory. Il est possible de créer ce cliché en une seule commande (intéressante pour les scripts) en entrant toutes les réponses sur la ligne de commande. Ainsi, il est possible de créer le cliché en entrant la commande suivante :

```
C:\> ntdsutil snapshot "activate instance ntds" create quit quit
```

Il est possible ensuite de **lister** tous les clichés créés en entrant directement :

```
C:\> ntdsutil snapshot "list all" quit quit
```

Ensuite, il est possible de **monter** le cliché souhaité (en fonction du numéro donné par la commande **list all**) et visualiser les données comme suit :

```
C:\> ntdsutil snapshot "list all"
1: 2017/10/31:21:03 {6e7b1bfb-4691-459e-9a2f-8c1e739d41bd}
2:   C: {a2e3b24c-3868-4841-ac47-aa67e33ef18c}
snapshot: mount 1
Snapshot {a2e3b24c-3868-4841-ac47-aa67e33ef18c} mounted as
C:\$SNAP_201710312103_VOLUMEC$\\
snapshot: quit
ntdsutil: quit
```

Cette première commande permet de lister les clichés créés puis monter le cliché numéro 1 qui a été réalisé, dans notre exemple, le 31/10/2017 à 21h03. Ce cliché est disponible sur C:\\$SNAP\_201710312103\_VOLUMEC\$\|

```
C:\> dsamain -dbpath "C:\$SNAP_201710312103_VOLUMEC$\Windows\NTDS\ntds.dit"
-ldapport 10289
```

Cette commande permet de lancer un serveur LDAP qui va lire le contenu de la base Active Directory. Grâce à ce serveur LDAP, il est maintenant possible de s'y connecter et vérifier les objets présents à cette date. Il faut, bien sûr, laisser le programme s'exécuter durant la consultation.

Pour **consulter** les objets contenant dans la version d'Active Directory à cette date, il suffit de lancer l'outil **Active Directory Users and Computers** et, faire un **clic-droit** sur le premier élément et choisir **change domain controller** puis, dans la fenêtre qui apparaît, choisir *this Domain Controller or AD LDS instance* et entrer dans la liste en dessous le nom **localhost:10289**.

A proprement parler, il n'est pas possible de restaurer des objets (utilisateurs et ordinateurs) depuis le cliché *monté* vers la version en cours d'exécution d'Active Directory. Il est cependant possible d'*exporter* une liste d'objets (utilisateurs ou ordinateurs) et d'*importer* celle-ci dans la version actuelle d'Active Directory. C'est parfois plus rapide que de repasser par l'outil de sauvegarde Windows.

Une fois **les opérations terminées**, il faut **quitter l'outil dsamin** en faisant un CTRL+C dans la console. Il faut également *démonter* le cliché monté par une commande *unmount*.

```
C:\> ntdsutil snapshot "unmount *" quit quit
```

## 9.4 Outil de sauvegarde Windows

L'outil de sauvegarde de Windows Server permet de réaliser un backup vers un autre média, des dossiers et fichiers voulus. Il s'agit d'un outil relativement simple à utiliser mais permettant déjà d'effectuer une sauvegarde intéressante.

Pour accéder à l'outil de sauvegarde, il faut aller dans **Server Manager > Tools > Windows Server Backup**. Au préalable, il peut être nécessaire d'installer l'outil via l'option **add roles and features** sur le serveur. Pour ce faire, il faut aller dans **Server Manager > Manage > Add Roles and Features** et ajouter la fonctionnalité **Windows Server Backup**.

#### 9.4.1 Fonctionnalités

L'outil de sauvegarde permet de :

- Planifier des sauvegardes régulières
- Réaliser une sauvegarde ponctuelle
- Restaurer des fichiers

Il est ainsi possible de sauvegarder (source) :

- Le serveur entier
- Un volume donné
- Un dossier déterminé
- L'état du système (registre, Active Directory, ...)

La sauvegarde peut se faire vers (destination) :

- Un disque dur réservé à la sauvegarde (**système de fichier particulier**)
- Un volume (disque dur formaté en NTFS connecté au serveur)
- Un partage réseau (et donc un autre serveur, un NAS, ...) – Copie unique, pas de version précédente possible

#### 9.4.2 Création d'une sauvegarde

Il est possible de créer une sauvegarde par l'option *Backup schedule* ou par l'option *backup once*. La première option permet de créer une sauvegarde récurrente alors que la seconde permet de réaliser une sauvegarde ponctuelle.

Les paramètres sont ensuite presque les mêmes : *quel type de sauvegarde* faut-il réaliser (le serveur entier [**Full Server**] ou une sauvegarde personnalisée [**Custom**]). Si une sauvegarde personnalisée est demandée, il faut *entrer les éléments à sauvegarder* [**Select Items for Backup**] (un fichier ou dossier donné, un volume, l'état du système, ...). Ensuite, il faut spécifier *l'endroit où la sauvegarde sera réalisée* avec la possibilité de choisir *un disque dur dédié à la sauvegarde* [**dedicated for backups**], *un volume ou disque local* [**to a volume**] ou *un partage réseau* [**to a shared network folder**]. Si une sauvegarde planifiée est choisie, il convient de déterminer quand celle-ci doit être effectuée.

#### 9.4.3 Restauration

Il est possible de restaurer en fonction d'une date donnée, des fichiers et dossiers, des volumes, des applications compatibles avec Windows Server Backup ou encore l'état du système. La récupération de fichiers ou dossiers est simple à réaliser : il faut simplement aller sélectionner le fichier ou dossier à récupérer dans la sauvegarde.

La restauration d'un volume est également une tâche possible. Cependant, si le volume à récupérer est le volume système (disque système qui contient l'installation de Windows Server), il est nécessaire

d'utiliser l'environnement de restauration. Il faut donc **redémarrer le serveur** dans un mode particulier comme suit : *au démarrage, il faut taper la touche F8 pour voir l'option Repair Computer. C'est ici que le mot de passe de restauration (placé durant l'installation d'Active Directory) peut être nécessaire. Il faut choisir le menu Troubleshoot puis l'option System Image Recovery.*

Ensuite, il faut choisir la sauvegarde et démarrer la récupération.

## 9.5 Exercices

1. Planifier un cliché instantané d'Active Directory, tous les mardi et mercredi à 12h. Vérifier celui-ci avec les outils dsamain et Active Directory Users and Computers.
2. Arrêter votre serveur SRV2016-1. Dans VMWare, modifier les paramètres de la VM pour ajouter un nouveau disque dur de 5 Go. Démarrer votre serveur et formatez celui-ci. Il doit être accessible par la lettre S :
3. Sauvegarder le contenu du dossier CGData, en utilisant *Windows Server Backup*. La sauvegarde doit être planifiée tous les mercredi à 11h, vers votre disque S :
4. Activer les clichés instantanés sur le volume C :, le mercredi à 15h. Les clichés doivent être sauvegardés sur le disque S :

Vérifiez toutes les sauvegardes et tester les clichés instantanés.

## Leçon 10 : Service de bureau à distance<sup>34</sup>

### 10.1 Introduction

Le service de bureau à distance est un moyen simple de permettre à des utilisateurs de se connecter *en mode graphique* sur le serveur. En effet, ce service permet aux utilisateurs désignés d'ouvrir une session distante sur le serveur : les programmes sont lancés à distance mais l'affichage est local.

Microsoft propose, depuis Windows XP, l'accès bureau à distance sur toutes les versions professionnelles de son système d'exploitation. Sur ces versions *non-serveurs*, seul un utilisateur peut être connecté à la machine (soit localement, soit à distance).

Sur un serveur Windows Server *sans le service de bureau à distance*, Microsoft autorise 2 connexions au total : soit 2 sessions distantes, soit une session locale et une session distante. Si le service de bureau à distance est activé, le nombre de connexion est limité en fonction des licences acquises.

### 10.2 Activation du bureau à distance

Sans installation du service bureau à distance (service RD), il est possible d'activer le bureau à distance sur des postes clients (Windows XP, Windows Vista, ...) ou sur des serveurs. Pour ce faire, il faut aller dans **Control Panel > System and security > System** et choisir l'option **Remote Settings**.

Dans le panneau du bas, on trouve l'espace *remote desktop*. Il suffit de choisir l'option *autorisant la connexion* [Allow remote connection] pour que le bureau à distance limité soit activé. Par défaut, seuls les administrateurs peuvent ouvrir une session à distance. Si vous souhaitez autoriser des utilisateurs, il faut cliquer sur **select Users** et ajouter les utilisateurs souhaités.

Une fois le bureau à distance activé, il est possible de se connecter à l'ordinateur en question en démarrant, depuis une autre machine, le programme de **Remote Desktop connection**<sup>35</sup> et en entrant **le nom ou l'adresse IP de la machine** sur laquelle vous souhaitez vous connecter.

Pour information, le port réseau utilisé pour la connexion bureau à distance est le port TCP 3389. **Attention !** La connexion bureau à distance n'est pas jugée comme *suffisamment* sûre que pour pouvoir l'autoriser à travers l'internet. Il est possible de sécuriser cette installation en déployant une passerelle TS utilisant SSL. Il est également possible d'activer des options de verrouillage dans le cas de plusieurs tentatives de connexion ratées.

### 10.3 Le service bureau à distance

Le service bureau à distance est moins limité que le bureau à distance. En effet, utiliser le service permet :

- D'avoir plusieurs utilisateurs connectés en même temps (en fonction du modèle de licences choisi).
- De lancer des applications distantes, s'exécutant sur le serveur mais visible sur le poste client (sans avoir besoin d'ouvrir une session au préalable)
- D'avoir une interface web d'accès au service de bureau à distance

<sup>34</sup> Ce service se nommait *Terminal Server* dans les versions Windows Server 2008 et antérieures

<sup>35</sup> Vous pouvez également chercher après le programme mstsc.exe (MicroSoft Terminal Server Client)

- D'installer une passerelle bureau à distance permettant l'accès à d'autres serveurs même s'ils sont localisés derrière un routeur (qui cache leur adresse IP en faisant du NAT). De plus, la communication est sécurisée au moyen de SSL.

### 10.3.1 Modèle de licences

Le service bureau à distance admet 2 modèles de licences : les licences *par utilisateur* et *par périphérique*<sup>36</sup>. Un modèle de licence *par utilisateur* permet une connexion simultanée d'un nombre défini d'utilisateurs (les licences n'étant pas attribuées mais consommées et libérées au fur et à mesure). Ainsi, si une entreprise achète 10 licences utilisateurs pour ses 30 employés, 10 utilisateurs maximum peuvent se connecter au serveur à un instant donné.

A l'inverse, les licences *par périphérique* sont attachées au périphérique. Elles sont donc permanentes et réservées. Ce modèle de licence est rarement utilisé pour la gestion des connexions au service bureau à distance.

Pour gérer ces licences, il faut installer le service des licences bureau utilisateur sur un serveur. Cependant, nous n'étudierons pas cet aspect. De plus, Microsoft propose une période *de grâce* (sans limitation) de 120 jours.

### 10.3.2 Installation

L'installation du service bureau à distance passe par l'ajout d'un rôle sur les serveurs concernés. Pour ce faire, **il faut être connecté avec un compte du domaine** (comme l'administrateur du domaine DOMAINE\Administrator) et aller dans **Server Manager > Manage > Add Roles and Features**. Dans le *type d'installation*, choisir **Remote Desktop Services installation**.

*Attention !* Le service ne doit être installé que sur les machines qui doivent accueillir des connexions d'utilisateurs en mode graphique. S'il s'agit simplement de permettre à l'administrateur d'accéder à distance à ses serveurs le mécanisme *bureau à distance* intégré à toutes les versions de Windows est suffisant.

L'installation se passe en plusieurs étapes :

1. L'écran suivant propose le *type de déploiement*, il convient de choisir l'option **Standard deployment**.
2. Ensuite, le *Scénario de déploiement* propose deux choix, il convient de choisir l'option **Session-based desktop deployment**. Ainsi les services de rôle suivants seront installés : Service Broker pour les connexions Bureau à distance, Accès Bureau à distance par le web et Hôte de session Bureau à distance.
3. Dans l'étape suivante (*Specify RD Connection Broker Server*) il faut ajouter le serveur courant dans les ordinateurs sélectionnés.
4. Sur l'écran *Specify RD Web Access server*, il faut cocher l'option *Install the RD Web Access role service on the RD connection Broker server* qui se trouve en haut de la fenêtre, puis choisir **Next**.
5. Sur l'écran *Specify RD Session Host Servers*, il faut ajouter le serveur courant aux serveurs sélectionnés, puis choisir **Next**.

---

<sup>36</sup> On parle de *licence CAL par utilisateur* ou de *licence CAL par périphérique*

6. Dans l'écran de confirmation, il faut simplement cocher la case *Restart the destination server automatically if required* et choisir l'option **Deploy**.

Pour des raisons de sécurité, il n'est pas recommandé d'installer les services bureau à distance sur le contrôleur de domaine.

### 10.3.3 Configuration

La configuration du service de bureau à distance passe par le **server manager** via l'option *Remote Desktop Services* dans le menu de gauche (cf. figure 10.1).

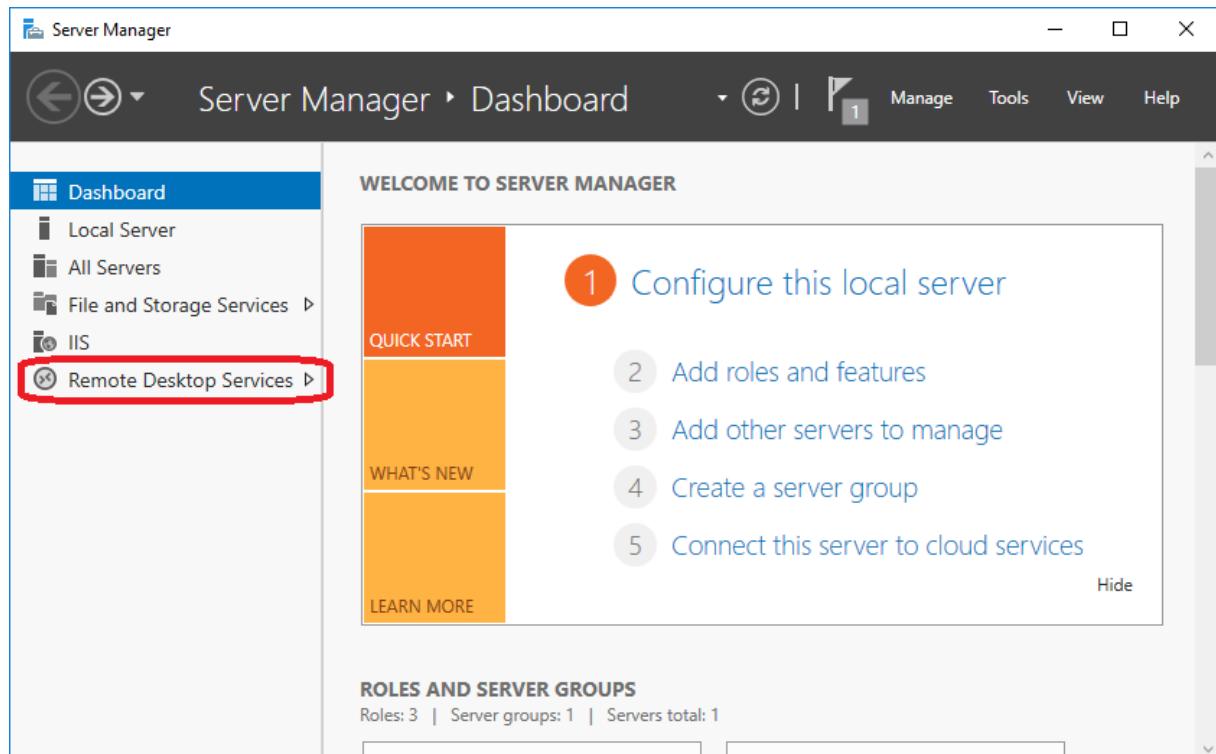


Figure 10.1 : Gestionnaire de serveur et l'option de configuration du service bureau à distance

Dans la configuration, on trouve :

- *Overview* : qui reprend le mode de déploiement des différents services liés au bureau à distance.
- *Servers* : qui reprennent la liste des serveurs sur lesquels les services bureau à distance sont déployés
- *Collections* : elles permettent de gérer les connexions actives et de définir une collection de sessions. La collection de sessions permet d'autoriser la connexion sur un ou plusieurs serveurs.

Il faut donc créer une **nouvelle collection** (en cliquant sur **Tasks > Create Session Collection**) pour débuter. Sur l'écran *Name the collection*, il faut choisir un nom. Sur l'écran *Specify RD Session Host servers*, il faut ensuite sélectionner le ou les serveurs inclus dans cette collection. Le système propose alors de sélectionner les utilisateurs (*Specify user groups*) qui seront autorisés à se connecter au service de bureau à distance. Il est possible d'inclure un groupe d'utilisateurs ici. L'option *User Profile Disks* est une option que nous n'utiliserons pas ici, il convient donc de **désactiver** ce paramètre. Apparaît alors l'écran de *Confirmation*. En cliquant sur **Create** la collection de sessions est créée.

Une fois la session créée, elle apparaît dans le **Server Manager**. Les paramètres de la collection de sessions peuvent être modifiés via l'option **Tasks > Edit Properties** (voir figure 10.2).

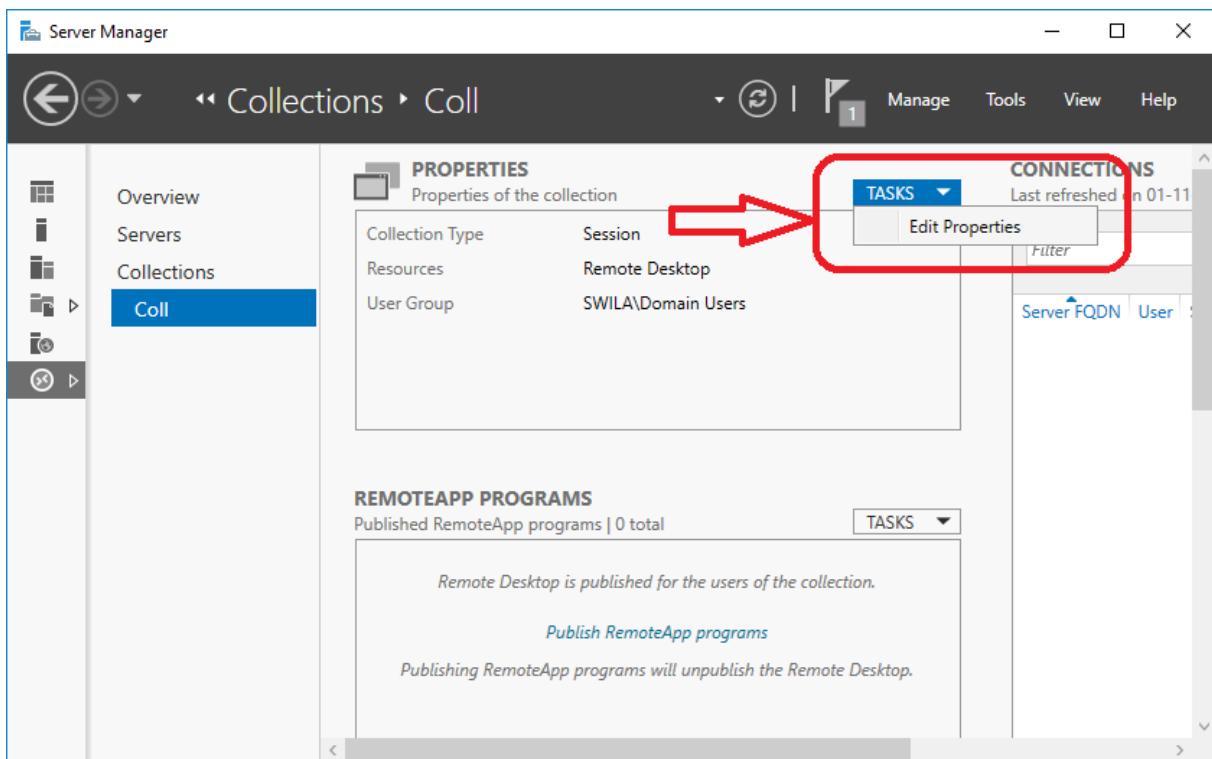


Figure 10.2 : Propriétés d'une collection de sessions (ici nommée Coll)

Par cette option, il est possible de modifier/préciser les propriétés suivantes :

- *General* : qui précise le nom de la collection
- *User Groups* : précise les groupes d'utilisateurs qui sont autorisés à accéder au service de bureau à distance et aux éventuelles RemoteApp configurées.
- *Session* : qui permet de définir les paramètres propres à la session de l'utilisateur qui se connecte. On y trouve ainsi tous les paramètres permettant de *limiter* dans le temps la session bureau à distance. En effet, tant que l'utilisateur ne clique pas expressément sur *Sign out*, celle-ci reste présente au niveau du serveur. Il est donc impératif de configurer les paramètres de fin de session sinon celles-ci peuvent durer plusieurs jours et consommer une licence. Cependant, on gère rarement ces paramètres depuis le serveur lui-même. En effet, on préfère habituellement définir une *policy* particulière qui s'appliquera au(x) serveur(s) concerné(s). Le comportement lorsque la limite de la session est atteinte peut également être précisé ici.
- *Security* : permet de mentionner les paramètres de sécurité applicables à la collection de sessions. Précisément, cette option détermine comment les informations sont chiffrées, avec quel niveau de chiffrement. Il faut noter que l'option **allow connections only from computers running Remote Desktop with Network Level Authentication** exige que les postes clients exécutent au moins Windows XP SP2 ou supérieur.
- *Load Balancing* : détermine quels serveurs doivent être préférés en fonction des ressources disponibles. Nous utiliserons un seul serveur, ce paramètre n'est pas important pour nous.

- *Client Settings* : permet d'autoriser ou non les redirections des ressources (disques, presse-papier, imprimantes) du client.
- *User Profile Disks* : permet d'activer ou non le stockage des paramètres utilisateurs (dans des profils particuliers) vers un emplacement réseau. Cette option est intéressante si les utilisateurs qui se connectent sur le serveur n'ont pas de profil itinérant stocké sur un serveur particulier ou si l'administrateur souhaite que l'utilisateur dispose d'un profil particulier lorsqu'il ouvre une session bureau à distance.

Les différents états d'une session sont : **active** lorsque l'utilisateur est connecté à la session et est en occupé à travailler, **inactive** lorsque l'utilisateur est connecté à la session mais n'y travaille plus depuis un certain temps et **disconnected** lorsque l'utilisateur a fermé la connexion au serveur sans fermer la session (*sans passer par l'option Sign Out*). Ainsi il est recommandé de limiter le temps des différents états d'une session et, dans certains cas, de fermer automatiquement les sessions déconnectées après un temps donné.

En ce qui concerne **les utilisateurs autorisés** : une bonne pratique serait de créer un groupe dans le domaine reprenant tous les utilisateurs autorisés à se connecter en bureau à distance. Il est également possible de spécifier les utilisateurs autorisés à se connecter au moyen d'une GPO applicable à cet ordinateur : **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services**. On peut, là aussi, y mentionner les groupes qui peuvent se connecter. La **GPO est prioritaire** (écrase les paramètres) dans le choix des groupes qui peuvent se connecter au serveur.

#### 10.3.4 Déploiement de logiciels sur le serveur RD

Très souvent, on utilise le service de bureau à distance pour mettre à disposition des utilisateurs une application commune. Cette application peut, dès lors, être utilisée en même temps par plusieurs utilisateurs connectés à des sessions bureau à distance.

Afin de pouvoir réaliser l'installation de l'application pour l'ensemble des utilisateurs, Microsoft propose de réaliser l'installation en *basculant* le serveur en mode d'installation bureau à distance. Pour ce faire, il faut aller dans le **Control Panel** du serveur exécutant le service RD et choisir **Install Application on Remote Desktop Server**. Une autre possibilité existe en utilisant la *ligne de commande*. En effet, il suffit d'entrer :

```
C:\> change user /install
```

Cette commande permet de basculer le serveur en mode installation.

```
C:\> change user /query
```

Cette commande permet de connaître le mode dans lequel le serveur se trouve.

```
C:\> change user /execute
```

Cette commande permet de basculer le serveur en mode exécution (mode par défaut).

Cette étape, nécessaire sous Windows Server 2008 R2 et précédent ne *semble plus nécessaire dans tous les cas*<sup>37</sup> avec la version Windows Server 2016.

---

<sup>37</sup> Notamment lors de l'installation de packages .msi. Cependant, en cas de problème, cette option reste toujours disponible.

## 10.4 Les sessions Bureau à distance

### 10.4.1 Démarrer une session depuis un poste client

Le poste client peut démarrer une connexion bureau à distance en démarrant l'outil *remote desktop connection* ou en exécutant le programme `mstsc.exe`. L'intérêt de l'outil est de pouvoir configurer quelques éléments en cliquant sur le bouton **Show Options**.

Comme nous pouvons le voir sur la figure 10.3, que de nombreuses options sont présentes :

- *L'onglet General* : présente les options principales comme l'ordinateur distant vers lesquels il faut établir la connexion dans le champ *Computer* (son nom ou son adresse IP), le nom d'utilisateur à utiliser dans le champ *User name* (il est toujours préférable de mentionner **DOMAINE\Login** dans le cas d'une connexion avec un compte d'utilisateur définit dans le domaine ou **MACHINE\Login** dans le cas d'une connexion avec un compte d'utilisateur local au serveur. Mentionnons également la possibilité de **créer un fichier RDP de connexion**. Ce fichier contient alors tous les paramètres et peut être facilement distribué aux utilisateurs.
- *L'onglet Display* : qui mentionne les paramètres d'affichage comme la résolution ou le nombre de couleurs.
- *L'onglet Local Ressources* : qui mentionne les ressources locales qui seront automatiquement connectées à la session de l'utilisateur lors de la connexion.

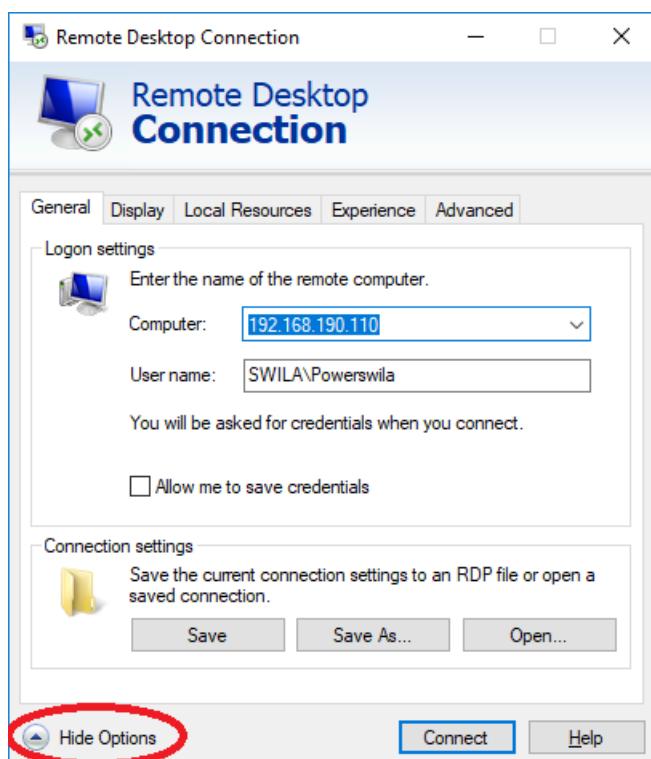


Figure 10.3 : Options pour la connexion Bureau à distance

- *L'onglet Experience* : gère les options d'optimisation et de reconnexion en cas de perte de celle-ci.
- *L'onglet Advanced* : permet de déterminer comment la connexion doit être réalisée vers le serveur. Il est ainsi possible de mentionner les options d'authentification mais également les options de passerelles. La passerelle est un mécanisme utilisant le serveur Web IIS pour

réaliser une connexion sécurisée vers un serveur RD au travers d'internet. Pour configurer cette particularité, il faut sélection l'option *RD Gateway* dans le tableau *Overview* (cf. Figure 10.1).

Une fois l'ensemble des paramètres définit, il est possible d'enregistrer ceux-ci dans un fichier RDP (onglet *General* option *Save* en bas de la fenêtre). La connexion se fait en cliquant sur le bouton **Connect** (ou en cliquant deux fois sur le fichier RDP sauvegardé).

#### 10.4.2 Gestion des sessions utilisateurs

Lorsque des utilisateurs sont connectés via le service RD, il est possible de gérer les différentes sessions depuis le serveur lui-même. En effet, via la *collection des sessions* dans *le service Bureau à distance*, il est possible de visualiser les sessions en cours.

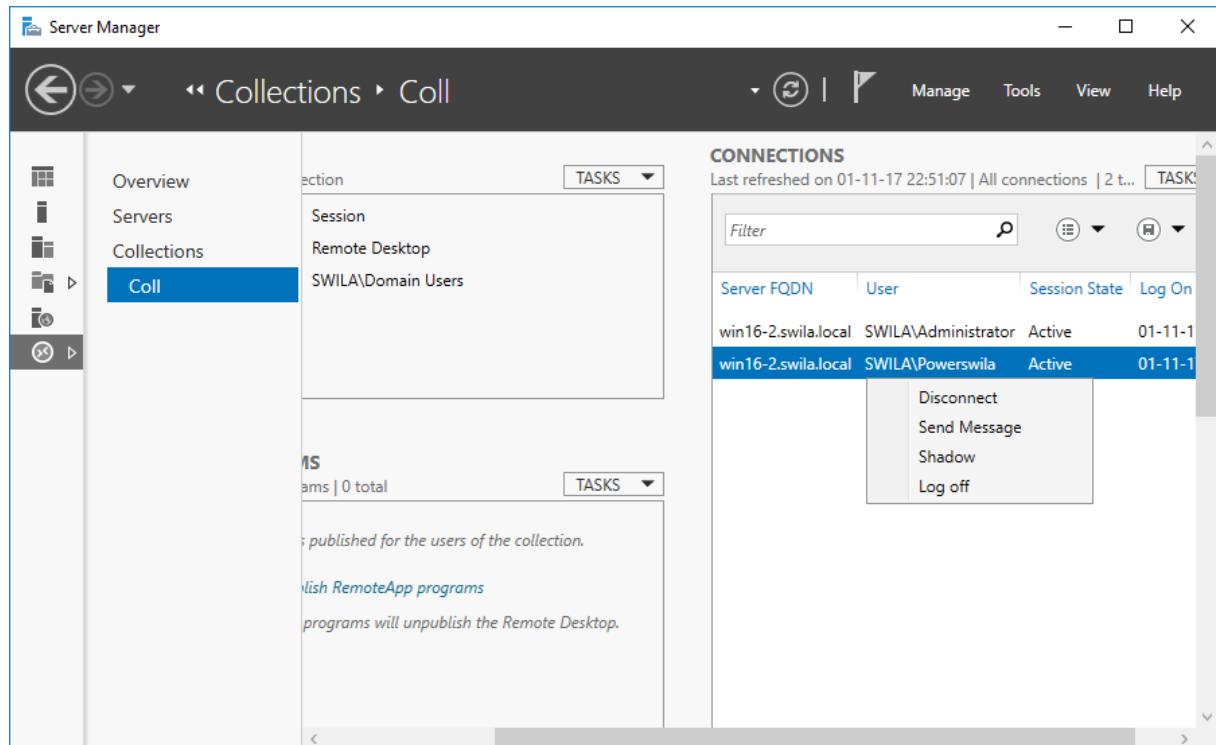


Figure 10.4 : Les sessions en cours sur le serveur RD

La figure 10.4 montre les sessions en cours sur le serveur : l'*administrator* est connecté en console et l'utilisateur *powerswila* est connecté par une connexion bureau à distance. Il faut remarquer l'état *active* mentionné.

En effectuant un **clic-droit** sur une session, on voit les quatre actions possibles :

1. Disconnect – qui permet de déconnecter l'utilisateur (la session devient Disconnected, les programmes démarrés restent actifs)
2. Send message – qui permet de faire apparaître un message (pop-up) dans la session de l'utilisateur
3. Shadow – qui permet de voir la session utilisateur. Le consentement de l'utilisateur peut être nécessaire.
4. Log off – qui permet de clôturer la session (déconnexion et fermeture de tous les programmes démarrés).

Il faut remarquer que des options complémentaires sont possibles **par le Task Manager (ou gestionnaire des tâches)**. En effet, il est possible (par l'onglet *Users*), en choisissant l'option *Connect* (après un clic-droit) de récupérer la session de l'utilisateur (en fournissant son mot de passe). Il est possible aussi de **tuer un processus (par l'option end task)** lancé par l'utilisateur.

## 10.5 Configurer une RemoteApp

### 10.5.1 Les RemoteApp

Une *RemoteApp* ou application distante est une fonctionnalité du service bureau à distance permettant de lancer une application sur le serveur mais d'afficher l'application lancée sur le poste client. En fait, une session sera ouverte sur le serveur afin de lancer l'application mais cette session ne sera pas visible par l'utilisateur qui verrait uniquement l'application s'exécuter.

C'est une fonctionnalité intéressante pour lancer des applications s'exécutant à distance. Il faut cependant ne pas perdre de vue que l'application, s'exécutant sur un ordinateur distant, n'a pas nécessairement accès aux ressources locales (il convient de configurer ces ressources locales convenablement pour que l'utilisateur ne soit pas perdu).

En effet, un des grands dangers de l'utilisation des *RemoteApp* est que l'utilisateur ne perçoive pas nécessairement qu'il travaille depuis un serveur distant et que, par conséquent, l'accès à son environnement (dossiers, fichiers, imprimantes, mail, ...) ne soit pas possible.

### 10.5.2 Configuration de l'application RemoteApp

La première étape est de procéder à l'installation de l'application sur le serveur exécutant le service RD. Pour installer l'application, comme nous l'avons vu précédemment (cf. 10.3.4), il faut basculer le serveur en mode *installation* afin de réaliser une installation propre.

Une fois l'installation de l'application achevée, il faut procéder à la configuration *RemoteApp* en allant dans **Server Manager > Remote Desktop Services > Collection > collection créée et puis RemoteApp Programs** (voir figure 10.5).

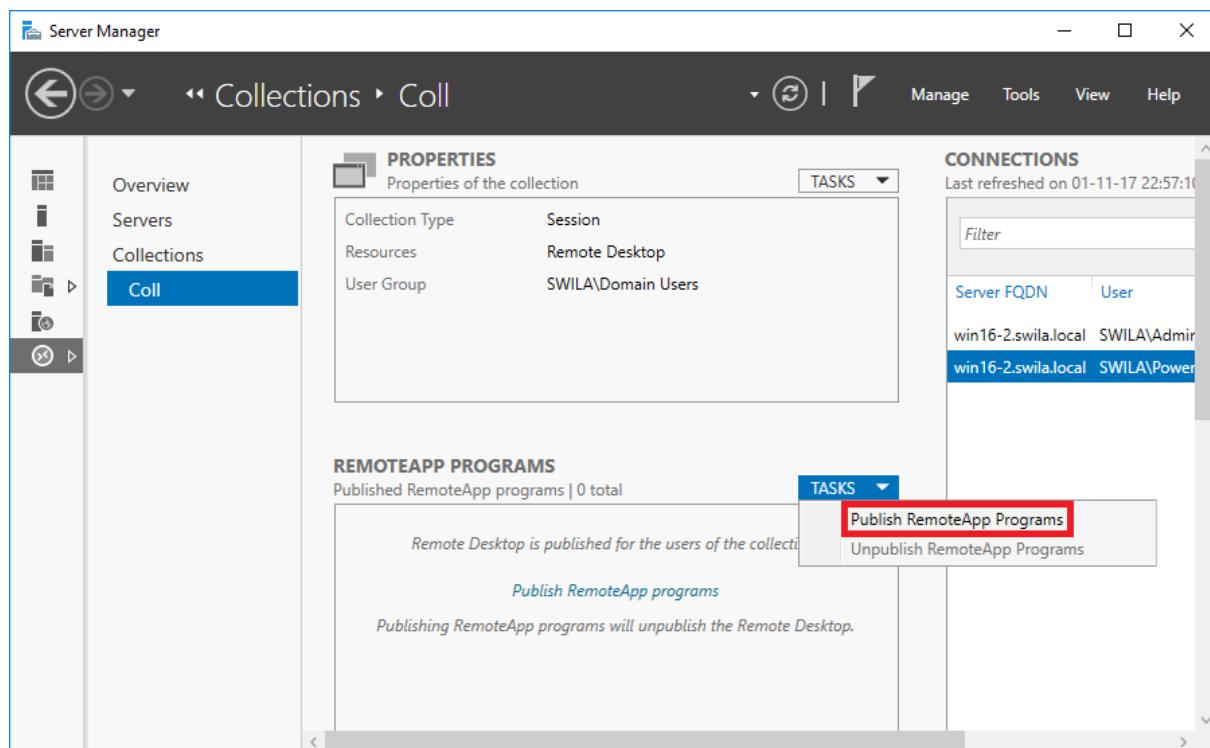


Figure 10.5 : Publication d'une RemoteApp

Pour ce faire, il faut choisir l'option *Publish RemoteApp programs* et sélectionner le programme souhaité dans la liste ou, s'il n'apparaît pas, via l'option *Add*. Une fois le programme ajouté, il est possible, en faisant un **clic-droit** sur celui-ci puis **Edit Properties**, d'interdire ou autoriser les paramètres en ligne de commande (option *Do not allow/Allow any command-line parameters*), de modifier les utilisateurs qui peuvent exécuter l'application distante (*specify users and groups who should see this Remote App program*) ou encore d'associer des types de fichier avec l'application RemoteApp (*Select the file types to associate with this Remote App*). Par défaut, tout utilisateur ayant le droit d'ouvrir une session sur le serveur peut exécuter l'application en mode *RemoteApp*.

Nous verrons dans la suite comment il est possible **d'obtenir le fichier .rdp permettant le lancement de l'application**.

### 10.5.3 Apparition des RemoteApp du côté client

Les *RemoteApp* apparaissent dans le *Menu Démarrer* dès que le client s'y est abonné. Cela peut se faire au moyen d'une GPO (uniquement pour les clients Windows 8 et supérieur) ou bien en configurant le flux dans l'outil adéquat.

Voici les étapes à suivre, **à partir du poste client** :

1. En *Administrator*, accepter le certificat créé pour la distribution des *RemoteApp*. Pour ce faire, il faut démarrer *Internet Explorer*<sup>38</sup> et entrer l'adresse suivante : <https://nomDNS.domaine> (exemple : <https://win16-2.swila.local>). Internet Explorer vous informe qu'il y a un problème de certificat. Il faut choisir l'option **Go to the webpage (not recommended)**.

<sup>38</sup> Pour démarrer Internet Explorer sous Windows 10, il faut rechercher `iexplore`

- a. La barre d'adresse apparaît en rouge, avec la mention **Certificate Error**. Il faut cliquer sur cette erreur et **view certificates**<sup>39</sup>.
  - b. Une fois que la fenêtre donnant les informations sur le certificat apparaît, il faut choisir l'option **Install Certificate**.
  - c. L'assistant d'importation apparaît, il faut alors choisir **Local Machine** et puis **Place all certificates in the following store : Trusted Root Certification Authorities** et confirmer l'importation.
  - d. Quitter Internet Explorer et retourner sur la page, l'erreur de certificat doit avoir disparu.
2. Avec l'utilisateur souhaité, démarrer l'outil **RemoteApp and Desktop Connections**, qui est accessible dans **le control panel** (voir figure 10.6) :

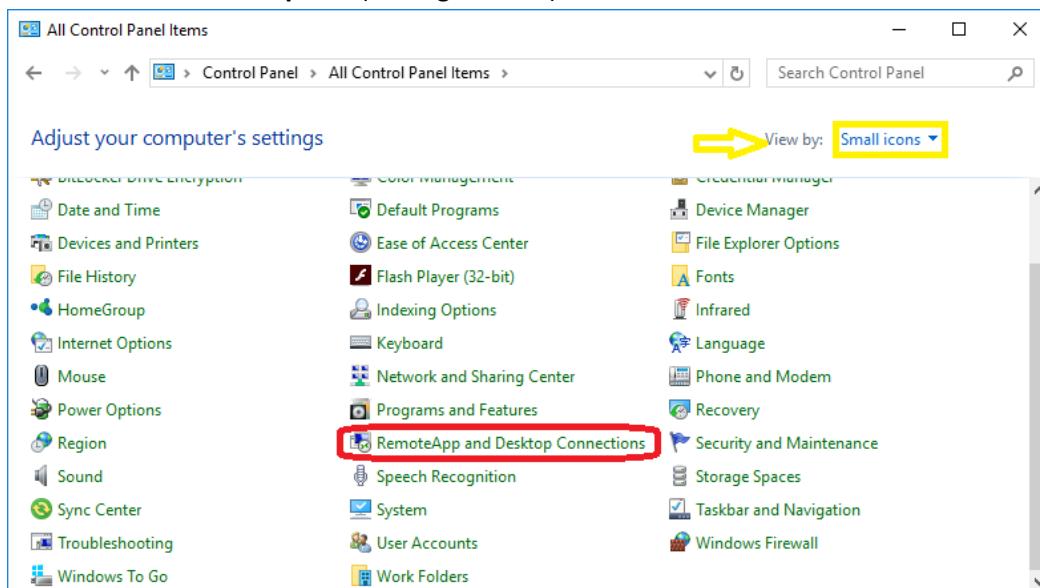


Figure 10.6 : RemoteApp and Desktop Connections

- a. Dans le menu de droite, choisir **Access RemoteApp and Desktops**
- b. Le système attend une URL de connexion. L'URL à fournir est de la forme : `https://nomDNS.domaine/RDWeb/Feed/webfeed.aspx` (le nom de votre serveur exécutant le service Bureau à Distance).
- c. Si le système vous informe d'un problème de certificat, il convient de se reporter à l'étape 1 ci-dessus.
- d. Une fois l'ajout terminé, un nouveau groupe *Work Ressources* apparaît dans le *Start Menu* du poste en question renseignant les applications RemoteApp publiées.
- e. Pour **obtenir le RDP de l'application**, il faut retourner dans la fenêtre *RemoteApp and Desktop Connections* depuis le panneau de configuration et choisir **View resources**. Faire ensuite un **clic-droit** sur l'application souhaitée (celle dont on veut obtenir le fichier `.rdp`) et choisir **Properties**. Le champ *Target* mentionne le chemin vers le fichier `.rdp` qui peut être ainsi récupéré pour être copié sur une autre machine.

## 10.6 Les GPO intéressantes pour les sessions RD

La première GPO intéressante est celle permettant de *Mentionner les utilisateurs qui peuvent se connecter en bureau à distance* : comme nous l'avons déjà mentionné, il est possible, par une stratégie,

<sup>39</sup> Cette possibilité n'est pas offerte dans Edge

de mentionner les groupes d'utilisateurs qui peuvent se connecter en mode bureau à distance. Il faut bien se rappeler que si une GPO définit cette propriété, cela écrase toute autre configuration. La GPO à configurer se trouve ici : **Computer Configuration\Policies\Windows Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services**.

Il y a un certain nombre de d'autres GPO utiles lorsqu'on active le service RD aussi bien en *Computer Configuration* (et donc applicable à la machine) qu'en *User Configuration* (applicable aux utilisateurs se connectant par le service RD).

On trouve parfois les mêmes éléments dans la *Computer Configuration* et dans la *User Configuration*. L'objectif est alors différent : faut-il autoriser la configuration pour l'utilisateur, quelque soit le serveur RD sur lequel il se connecte (=> user configuration) ou faut-il autoriser la configuration sur le ou les serveurs donnés, peu importe les utilisateurs qui se connecte (=> computer configuration).

Les stratégies applicables à la configuration ordinateur se trouvent dans **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services**.

Les stratégies applicables à la configuration utilisateur se trouvent dans **User Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services**.

Quelques stratégies intéressantes :

- *Restrict Remote Desktop Services users to a single Remote Desktop Services Session* : Cette stratégie permet d'éviter qu'un utilisateur (avec son login) ne puisse ouvrir plus d'une session sur le serveur (et donc économie des licences) à la fois (*computer configuration*).
- *Session Time Limits* : il y a quelques stratégies importantes permettant de définir les délais d'expiration des sessions. Ces paramètres permettent d'éviter que des sessions ne restent ouvertes indéfiniment. Ces paramètres sont présents dans la computer configuration et user configuration. S'ils sont définis des deux côtés, la *computer configuration* est prioritaire.
- *Printer Redirection* : Ces stratégies mentionnent le comportement à adopter face aux imprimantes. En effet, les imprimantes de l'utilisateur qui se connecte sont par défaut émulées dans la session RD. Or, si de nombreux utilisateurs se connectent avec, pour chacun, toutes leurs imprimantes, le système peut vite saturer. Il est dès lors conseillé d'activer *Redirect only the default client printer* (uniquement l'imprimante par défaut de l'utilisateur). Ces paramètres sont présents dans la computer configuration et user configuration. S'ils sont définis des deux cotés, la computer configuration est prioritaire.
- *Device and Resource Redirection* : ces stratégies permettent de limiter les ressources et redirections réalisées entre le client et le serveur RD. Ces paramètres sont présents dans la computer configuration et user configuration. S'ils sont définis des deux cotés, la computer configuration est prioritaire.

## 10.7 Exercices

1. Installer le service Remote Desktop sur la machine *SRV2016-2* (cf. leçon 8, exercice 2).
  - a. Autoriser les membres `elearning` et `travaux` à se connecter au serveur (via la collection de session)
  - b. Tester la connexion depuis la machine VM Windows 10 (par exemple `eg005040`)
2. Modifier la stratégie `boucleRappel` (exercice 5d, leçon 8) :
  - a. Empêcher toute redirection du presse-papier et n'autoriser que la redirection de l'imprimante par défaut
  - b. N'autoriser qu'une session par utilisateur
  - c. Définir les délais pour une session inoccupée à 5 minutes. Mentionner qu'une session déconnectée depuis 10 minutes doit être fermée.
  - d. Autoriser le groupe `travaux` à ouvrir une session via le service Desktop Services
  - e. Tester la connexion depuis la machine VM Windows 10 (pour `tx005040` et `eg0050`).
3. Configurer une *RemoteApp*
  - a. Installer, au préalable, le programme WinSCP sur le serveur *SRV2016-2* (cf. leçon 8, exercice 2)
  - b. Configurer une *RemoteApp* pour permettre l'exécution de ce programme
  - c. Tester la *RemoteApp* depuis votre machine VM Windows 10 avec un membre du groupe `travaux` (par exemple `tx0050`). Connectez-vous à *Dartagnan<sup>41</sup>* et copier le contenu de votre dossier `public_html` depuis votre espace vers le disque C:. Quitter la *RemoteApp*. Trouver les fichiers transférés.
  - d. Obtenir le fichier `.rdp` permettant de démarrer la *RemoteApp*. Copier ce dernier sur le bureau de l'utilisateur.

<sup>40</sup> Pour rappel, tous les utilisateurs portant le numéro 50 ont comme mot de passe `P@ssw0rd`

<sup>41</sup> L'adresse IP de Dartagnan est 192.168.128.13

## Leçon 11 : Serveur IIS et FTP

### 11.1 Introduction

Le service IIS est le service Web proposé par Microsoft. IIS est nécessaire pour l'installation de site web sur le serveur. Il est également fortement utilisé par des services propres de Microsoft comme le service des certificats Active Directory ou encore le service de passerelle pour le bureau à distance (permettant ainsi de sécuriser la connexion en utilisant SSL).

Le service FTP est le service d'échange de fichiers courant. Il va souvent de pair avec service Web car il permet aux utilisateurs de déposer leurs fichiers sur le serveur. Il existe bon nombre de services FTP concurrents comme, par exemple, FileZilla FTP Server. Le grand avantage du service FTP de Microsoft est qu'il est directement lié à Active Directory. Ainsi les utilisateurs du domaine peuvent se connecter sur le service FTP directement.

### 11.2 IIS

Le service IIS comprend les protocoles HTTP (port 80) et HTTPS<sup>42</sup> (port 443). Il peut être utilisé pour développer et mettre en ligne :

- Un site web public accessible à tous les visiteurs
- Un site web intranet accessible uniquement à l'intérieur du réseau
- Une application internet utilisant la technologie .NET. En effet, une des grandes utilisations des services IIS est la mise en ligne d'applications internet écrites avec la plateforme .NET (services web, ...)
- Il est possible d'intégrer à IIS d'autres langages comme, par exemple, PHP. Pour ce faire, il faut utiliser une extension ISAPI<sup>43</sup>

#### 11.2.1 Installation du service IIS

Pour installer IIS, il faut ajouter le rôle Serveur Web. Pour ce faire, il faut démarrer l'outil **server manager > Manage > Add Roles and Features**. Dans la liste, il faut ajouter le rôle **Web Server (IIS)**. Une fois l'ajout des dépendances réalisées, il faut déterminer *les services de rôles* à installer. Les services de rôle sont des prises en charge particulières pour le service web, on y trouve notamment :

- Common HTTP Features (mise à disposition de pages Web HTML via HTTP)
  - **Default Document** : Permet de configurer le nom par défaut qui sera recherché par le service IIS (index.htm par exemple).
  - **Directory Browsing** : Permet l'exploration des dossiers directement dans le navigateur du client
  - **HTTP Errors** : pages d'erreur à retourner dès qu'un problème est détecté (401, 403, 404, 500, ...)
  - **Static Content** : page HTML simple, sans scripting. Contenu statique.
  - **HTTP Redirection** : permet de réaliser des redirections (code d'état 3XX) vers d'autres pages.

<sup>42</sup> L'utilisation de la version sécurisée nécessite de disposer d'un certificat numérique obtenu auprès d'une autorité de certification reconnue

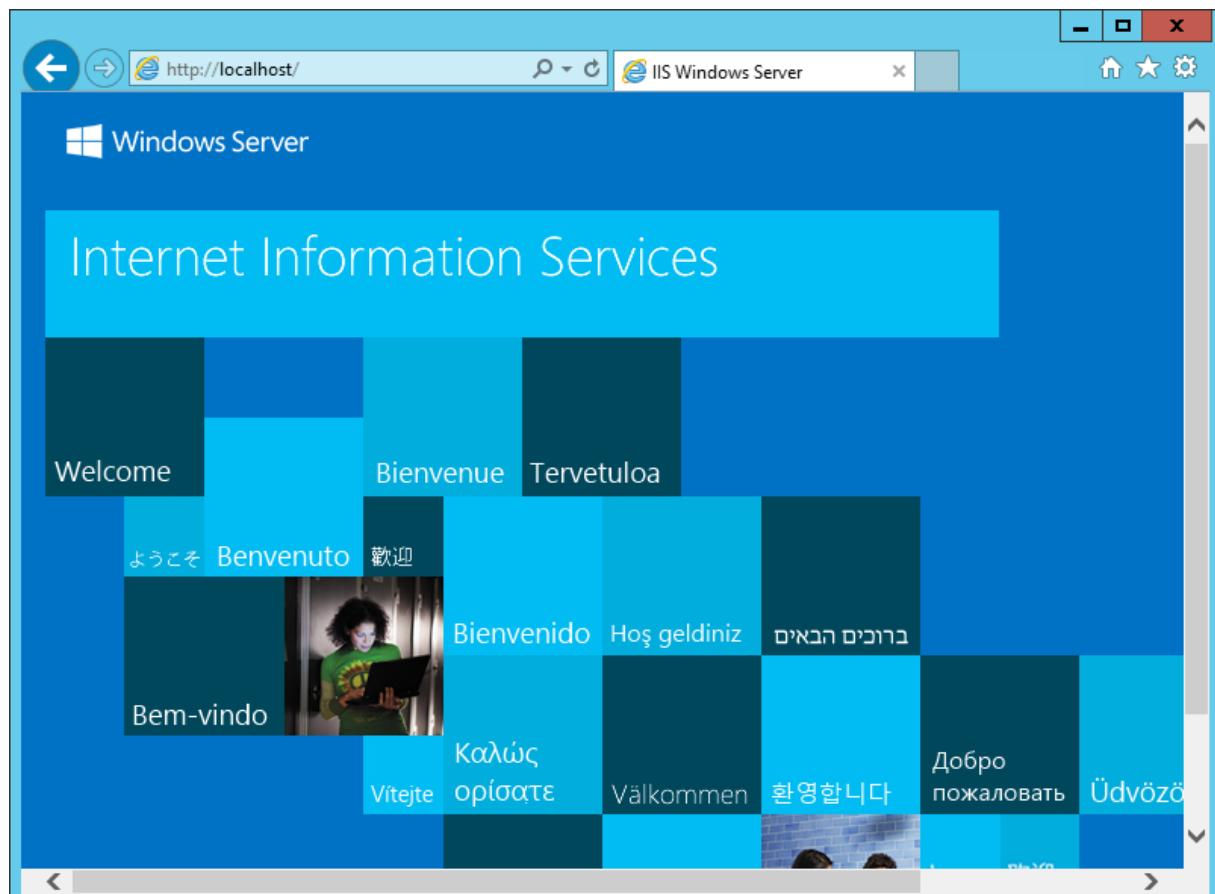
<sup>43</sup> Si l'objectif est d'exécuter des applications écrites en PHP, il est préférable d'utiliser le serveur Web Apache pour déployer l'application. Ce service existe aussi sous Windows par un package spécifique comme WAMP (Windows Apache Mysql Php) ou XAMP.

- **WebDAV Publication** : permet de publier des documents vers le serveur Web directement.
- Health and Diagnostics (reprennent les éléments importants pour la journalisation des événements et leurs traitements). Par défaut, l'option **HTTP Logging** est activée, il peut être intéressant d'activer l'option **Request Monitor** (qui collecte les informations sur les requêtes http). Cependant, lors de la phase de développement, il est parfois utile de disposer d'outils plus précis pour analyser les requêtes et leurs traitements.
- Performance (permet d'activer la compression de contenu afin que les paquets soient transmis plus rapidement à la destination)
- Sécurité (reprend les éléments importants pour la gestion de la sécurité au niveau du serveur Web)
  - **Request Filtering** : sur base de règles définies par l'administrateur, permet de protéger le serveur web. En effet, un certain nombre d'attaque partage des particularités communes et, grâce aux règles de filtrage, il est possible de minimiser certaines attaques connues.
  - **Basic Authentication** : C'est un mécanisme d'authentification courant présent dans tous les serveurs Web. Celui-ci permet de faire afficher, sur le navigateur du poste client, une fenêtre simple d'authentification. Les données sont par défaut transmises en clair sur le réseau.
  - **Centralized SSL Certificate Support** : Permet de localiser les certificats SSL sur un partage réseau (ainsi les certificats sont localisés à un seul endroit).
  - **Client Certificate Mapping Authentication** : permet d'identifier l'utilisateur sur base d'un certificat numérique qu'il possède et qui est installé dans son navigateur
  - **Digest Authentication** : amélioration de l'authentification de base puisque le mot de passe est transmis sous forme hachée.
  - **IIS Client Certificate Mapping Authentication** : Cette fonctionnalité est équivalente à celle de *client certificate mapping authentication* mais adaptée au application .NET/IIS.
  - **IP and Domain Restrictions** : en fonction de l'adresse IP ou du domaine du client, il est possible de refuser la connexion.
  - **URL Authorization** : permet de protéger certaines parties du site web
  - **Windows Authentication**: Cette méthode d'authentification permet de réaliser un lien vers Active Directory. Ainsi les utilisateurs sont identifiés sur base de leur connexion au domaine.
- Application Development (permet le déploiement d'application Web)
  - **.NET Extensibility (3.5 / 4.6)** : permet d'étendre des fonctionnalités du serveur Web IIS.
  - **Application Initialization** : permet l'initialisation d'opérations coûteuses avant de fournir les pages au client.
  - **ASP** : C'est le précurseur d'ASP.NET. Il est présent pour des raisons de rétrocompatibilité
  - **ASP.NET 3.5 / 4.6**: c'est le principal standard des serveurs Web IIS. Permet le support d'applications développées dans ce langage.
  - **CGI** : c'est une norme présente dans la majorité des serveurs web permettant de faire appel à un programme extérieur pour répondre à la requête.

- **ISAPI Extensions and Filters** : ces éléments permettent de prendre en charge des autres langages de développement de contenu Web dynamique comme PHP par exemple. Il est cependant nécessaire de disposer de l'extension compilée pour les systèmes Microsoft.
- **Server Side Includes** : Active un langage de script utilisé pour générer des pages web dynamique. Permet de générer des pages HTML.
- **WebSocket Protocol** : Permet d'activer le protocole WebSocket sur le serveur.
- **FTP Server** (permet d'activer le service FTP sur le serveur IIS)
- **Management Tools** (permet d'installer la console de gestion IIS ainsi que la rétrocompatibilité vers IIS 6).

Une fois le service IIS installé, nous voyons apparaître, dans la console **Server Manager**, l'outil **Internet Information Services (IIS) Manager**. C'est par cette console qu'il sera possible de configurer le service web IIS.

Dès que le service Web IIS est installé et démarré, il doit être possible de se connecter sur le site web par défaut installé. Pour ce faire, il faut démarrer un navigateur et entrer comme URL : <http://localhost>. Normalement, la page web par défaut doit alors s'afficher :



### 11.2.2 Configuration d'IIS

La configuration d'IIS peut se faire par l'outil **Internet Information Services (IIS) Manager** qui se trouve dans le menu Start > Windows Administrative Tools ou via le **Server Manager > Tools > Internet Information Services (IIS) Manager**.

La première chose à bien distinguer est *le niveau de configuration*. En effet, il est possible de définir des paramètres au niveau du *serveur* ou du *site* souhaité. La configuration au niveau du serveur est *générale* tandis que la configuration au niveau du site est *particulière au site donné*. Ainsi, même si on trouve les mêmes éléments, leurs portées est bien différentes.

Par exemple, on trouve, dans ces deux niveaux, l'élément *default document*. Ce paramètre désigne le fichier par défaut que le serveur web tentera de trouver si l'URL n'en mentionne pas. Ainsi, une requête vers `http://localhost` doit trouver une page à afficher. Les éléments recherchés par le serveur web sont : `Default.html`, `Default.asp`, `index.htm`, `index.html`, `iisstart.htm` ou parfois `default.aspx`. Si je modifie l'option *default document* au niveau du serveur, cette configuration sera héritée pour tous les sites web. Si je modifie cet élément au niveau du site web, cette modification sera locale à ce site.

Nous allons maintenant pointer quelques éléments de configuration importants :

- **Authentication** : mentionne comment il faut authentifier l'utilisateur. Nous aborderons ce point plus loin.
- **Authorization Rules** : mentionne qui (i.e. quels utilisateurs) peut accéder au site web. Ces règles vont de pair avec les méthodes d'authentification.
- **Default Document** : qui détermine la page par défaut à ouvrir si l'URL n'en renseigne pas.
- **Directory Browsing** : cette fonctionnalité permet, lorsqu'aucun document par défaut n'est trouvé, d'afficher la liste des fichiers et dossiers présents plutôt que de retourner une erreur 404.
- **Error Pages** : reprend les chemins vers les pages d'erreur standards. Ces pages peuvent être personnalisées par l'administrateur.
- **HTTP Redirect**: permet de réaliser une redirection HTTP vers une autre URL
- **IP and Domain Restrictions** : permet de limiter l'accès du site à une plage IP ou un nom de domaine donné.
- **Logging** : mentionne l'emplacement et le traitement (roulement) des fichiers journaux.
- **Modules** : reprend tous les modules actifs au niveau du serveur IIS
- **Request Filtering** : permet de limiter l'accès à certains *types* de fichier (sur base de leur extension), de critères spécifiques définis par l'administrateur (onglet *rules*), l'accès à un fichier donné (onglet *hidden segments*), des URL contenant un masque donné (onglet *URL*), des commandes HTTP comme GET, HEAD, POST, ... (onglet *HTTP verbs*) ou encore des éléments de l'entête (onglet *Headers*).
- **SSL Settings** : permet de configurer le mode HTTPS sur le serveur. Attention : un certificat numérique est requis pour pouvoir activer ce mode.

Bien sûr, en fonction de l'installation effectuée, bien d'autres éléments peuvent (ou pas) apparaître comme les liens vers une base de données SQL Server ou encore vers le serveur SMTP d'envoi de mail (si ASP.NET est installé), ... Les éléments présentés ici sont les éléments courants d'un serveur IIS.

Les **sites** mentionnent les différents sites web gérés par le serveur IIS. Le site web *par défaut* est nommé *Default Web Site*. Il correspond au site web sur lequel l'utilisateur arrive quand le nom qu'il a indiqué n'est repris nulle part ailleurs pour les autres sites. En effet, quand on crée un nouveau site, il faut mentionner :

- **Site name** : c'est sous ce nom que le site apparaîtra dans IIS
- **Physical path** : c'est le dossier qui contiendra tous les fichiers de ce site.
- **Binding** (i.e. comment on peut atteindre le site) : avec le protocole, l'adresse IP accessible, le numéro de port et le nom DNS du site. En effet, nous avons vu dans la configuration DNS que plusieurs noms peuvent pointer vers la même adresse IP (CNAME ou raccourci au niveau de la zone DNS). On peut créer un site par nom DNS en mentionnant le nom en question dans ce champ. Ainsi, si je mentionne *talkto.swila.local* et que l'entrée *talkto* est un CNAME vers le serveur exécutant le service IIS, alors, quand j'entrerai <http://talkto.swila.local>, j'arriverai sur ce site.

### 11.2.3 Authentification d'un utilisateur

Par défaut, les sites créés sont accessibles à l'ensemble des utilisateurs. Il n'y a donc pas d'authentification. Cependant, parfois on souhaite créer des sites qui sont uniquement accessibles à certains utilisateurs authentifiés. Cette configuration est possible dans IIS grâce au paramètre *Authentication* et au paramètre *Authorization Rules*.

Dans *Authentication*, les différents types d'authentification disponibles sont (si installées):

- **Anonymous Authentication**: cette authentification permet à des utilisateurs *non identifié* d'accéder au site
- **Basic Authentication** : méthode d'authentification de base reposant sur un nom d'utilisateur et un mot de passe (envoyé tout deux en clair sur le réseau). L'utilisateur est soit un *utilisateur local* du serveur ou *un utilisateur du domaine*. Il est d'ailleurs possible, dans les options liées à l'authentification de mentionner un *default domain* pour l'utilisateur. Depuis l'internet, il faut toujours combiner une *authentification basique* avec l'utilisation d'un site web sécurisé (SSL avec un certificat).
- **Digest Authentication** : méthode d'authentification ne transmettant pas le mot de passe en clair sur le réseau (à l'inverse de l'authentification de base). La prise en charge de cette méthode d'authentification suppose que le navigateur client supporte l'envoi du mot de passe haché (en utilisant la bonne fonction).
- **Windows Authentication** : méthode d'authentification reposant sur Active Directory pour les ordinateurs dans le même domaine que le serveur. Cette méthode d'authentification *sûre* (car le mot de passe ne circule pas en clair sur le réseau) est particulièrement adaptée au déploiement d'applications dans un intranet (la machine cliente doit faire partie du domaine).

**Remarque importante :** activer l'authentification windows sur un serveur et effectuer les tests depuis ce serveur pourrait ne pas fonctionner pour des raisons obscures. Dans ce cas, le système retourne systématiquement une erreur 401 alors que l'accès depuis une autre machine fonctionne parfaitement. Pour résoudre ce problème<sup>44</sup>, démarrez **regedit.exe** et déployez **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**. Faites un **clic-droit** sur **Lsa** et

---

<sup>44</sup> <http://support.microsoft.com/kb/896861>

choisissez **Nouveau** puis **DWORD**, entrez le nom **DisableLoopbackCheck** et affecter la valeur **1** puis **redémarrer le serveur** ou effectuer vos tests depuis une autre machine.

Une fois la méthode d'authentification sélectionnée, il faut mentionner le site, le dossier, ... qui sera soumis à cette authentification. Pour ce faire, il faut modifier les règles dans *Authorization Rules*. Il y a 2 types de règles d'autorisation : les règles d'autorisation et les règles de refus. Les règles de refus sont toujours prioritaires par rapport aux règles d'autorisation. Il faut savoir que lorsqu'on insère une règle d'autorisation, seuls les utilisateurs visés par cette règle sont autorisés à accéder à la ressource en question. Il est bien sûr possible d'insérer plusieurs règles d'autorisation. Il est possible d'autoriser (ou refuser) un utilisateur, un groupe, tous les utilisateurs ou tous les utilisateurs anonymes.

Ainsi, si l'on veut autoriser l'utilisateur *swila* à accéder au site, il suffit d'ajouter **la seule règle** autorisant cet utilisateur précis, et la configuration est terminée.

## 11.3 Le service FTP

Le service FTP peut être ajouté lors de l'installation d'IIS. Ainsi, si le rôle *Web Server* est déjà installé, il suffit de déployer « *Web Server(IIS)* » pour ajouter les services associés à FTP. Si le rôle *Web Server* n'est pas installé, il faut commencer par l'installer et choisir les options concernant le service FTP.

La configuration du service FTP se fait à deux endroits : en premier lieu, il y a la configuration du serveur en lui-même, avec les différentes options de connexion, les règles de filtrages, .... Ensuite, il convient souvent<sup>45</sup> d'ajouter des **sites FTP** afin de permettre aux utilisateurs de se connecter.

### 11.3.1 Configuration d'un site FTP

La création d'un site FTP est assez simple, il faut faire un **clic-droit** sur l'élément *Sites* et choisir l'option **Add FTP site**. Lors de l'ajout du site FTP, il faut lui donner son *FTP site name* (nom sous lequel il apparaîtra dans l'arborescence des sites) et ensuite mentionner le chemin *physical path*. Enfin, l'écran suivant demande les informations de connexion (adresse IP et port), le nom DNS du site et les options de chiffrement (qu'il convient de désactiver en l'absence de certificats valides).

Enfin, le dernier écran mentionne les utilisateurs autorisés à se connecter : l'utilisateur anonyme et/ou l'authentification de base (utilisateur ayant un compte sur le serveur ou dans Active Directory). Enfin, il faut fixer les permissions d'accès : lecture ou écriture.

### 11.3.2 Les répertoires virtuels

A l'instar des liens symboliques sous Unix, les répertoires virtuels permettent de faire apparaître dans l'arborescence du site FTP des dossiers situés ailleurs sur le système. Il s'agit d'un élément de configuration important : on souhaite rendre accessible un dossier donné mais pas le dossier parent et pour cela, on fait pointer un répertoire virtuel vers le dossier à rendre visible.

Pour créer un répertoire virtuel, il faut faire un **clic-droit** dans l'arborescence FTP (dans le gestionnaire de serveur) et choisir l'option **add virtual directory**. Il faut ensuite mentionner le nom et le chemin d'accès. Attention ! L'accès au dossier pointé dépend des droits d'accès actuels de l'utilisateur identifié. Ainsi, si je m'identifie comme l'utilisateur *swila*, je dois disposer des droits suffisants pour naviguer dans le dossier pointé.

<sup>45</sup> En fait un dossier *racine* FTP est déjà prévu dans la configuration et peut être utilisé. Si l'on souhaite avoir une ou plusieurs configurations plus précises, il est nécessaire de créer des sites FTP.

### 11.3.3 Quelques options avancées

Via *Advanced Settings*, il est par exemple possible de *modifier les délais d'expiration (Data channel Timeout)* ou encore de *limiter le nombre de connexions simultanées (Max Connections)*. Il est indispensable de configurer cette option si l'on autorise l'utilisateur anonyme à se connecter au serveur. Cette option permet de limiter les possibilités d'attaques en déni de service.

Comme pour les sites web, il est possible, via l'option *edit bindings* sur le site FTP de préciser et modifier les paramètres de connexion ainsi que le nom DNS associé.

### 11.3.4 Configuration de l'authentification et de la connexion FTP

L'authentification sur le site FTP (configurable également au niveau du serveur) est disponible via l'icône *FTP Authentication*. Il y a deux authentifications possibles :

- *Anonymous authentication*: qui permet à un utilisateur de se connecter au moyen du compte *anonymous* ou *ftp*.
- *Basic Authentication* : qui permet à un utilisateur de se connecter via son compte Windows (configuré sur le serveur ou sur le domaine AD).

Une fois la phase d'authentification terminée, l'utilisateur voit apparaître l'arborescence FTP dans son client (i.e. filezilla par exemple). S'il s'est connecté au moyen d'un compte déterminé, il a les droits de cet utilisateur (et peut donc lire les différents dossiers et fichiers en fonction des droits NTFS). Si, par contre, il est connecté en mode anonyme, il se connecte comme l'utilisateur IUSR et peut donc naviguer, télécharger, lire, ... en fonction des permissions NTFS données à cet utilisateur. Il faut néanmoins mentionner qu'il est possible de remplacer l'utilisateur par défaut IUSR par un autre utilisateur dont on fournit le mot de passe (**FTP Authentication > Anonymous Authentication > Edit**).

Pour information, il est possible, en choisissant *Custom Providers* dans la fenêtre de configuration de l'authentification FTP de choisir une authentification *IISManagerAuth* qui autorise une connexion en utilisant un login et un mot de passe n'ayant pas de compte créé sur le serveur ou encore, *AspNetAuth* qui utilise la gestion d'utilisateurs .NET pour réaliser l'authentification.

Une fois l'authentification configurée, il convient de spécifier les règles via **FTP Authorization Rules** afin de déterminer qui peut effectuer quelle action sur le site en question. Cette option est intéressante pour limiter l'accès à certains utilisateurs (ainsi, pour l'authentification de base, tous les utilisateurs ayant un compte peuvent se connecter au service FTP) et limiter également certaines actions.

Enfin, la dernière option qui doit être configurée est **FTP User Isolation**. Cette option permet de déterminer si tous les utilisateurs qui se connectent accèdent au même dossier FTP ou bien, s'il accède à un dossier précis en fonction de leur nom d'utilisateur. Par défaut, les utilisateurs authentifiés ont accès à la racine du site FTP. Si l'on souhaite amener l'utilisateur dans un dossier qui lui est propre, il faut faire pointer la racine du site FTP au répertoire parent contenant l'ensemble des dossiers des utilisateurs et puis configurer l'isolation d'utilisateur FTP. Cette option est particulièrement intéressante si l'on souhaite permettre aux utilisateurs d'accéder à leur dossier personnel (contenant leur profile par exemple) via FTP. Il faut donc configurer le répertoire FTP racine vers le dossier partagé contenant tous les répertoires personnels des utilisateurs et, ensuite, choisir l'option *isolate users : restrict users to following directory : User name directory*.

Enfin on pourrait également créer, par script Powershell, des dossiers précis dédiés à chaque utilisateur ou accessibles par groupes d'utilisateurs, ...

### 11.3.5 La sécurité de FTP

FTP est un protocole dont la sécurité est assez pauvre puisque les logins et mots de passe circulent, par défaut, en clair sur le réseau. Pour améliorer la sécurité de FTP, il est possible d'utiliser un certificat SSL (lorsqu'on dispose d'un tel certificat émis par une autorité de certification reconnue).

L'autre point important concernant la sécurité concerne *les firewalls* et l'option **FTP Firewall Support**. Pour rappel, FTP propose deux modes de fonctionnement très distincts : le mode *actif* dans lequel le client demande l'envoi d'un fichier par le serveur (requête du client vers le serveur) et le serveur démarre le transfert du fichier vers le client (requête du serveur vers le client). Cette connexion pose souvent des problèmes si le client se trouve derrière un routeur qui fait du NAT ou derrière un firewall.

L'autre mode de fonctionnement proposé par FTP est le mode *passif* dans lequel le client demande l'envoi d'un fichier par le serveur (requête du client vers le serveur) et le client démarre le transfert vers le serveur (connexion du client vers le serveur). Dans ce cas, le problème est reporté du côté serveur qui, s'il se trouve derrière un firewall, doit permettre l'échange du fichier.

Pour ce faire, il faut configurer les options de *FTP Firewall* coté serveur. Il faut dès lors mentionner : *port range* (i.e. redirigés au niveau du firewall vers le serveur FTP) ainsi que l'adresse IP externe *External IP address* (celle qui sera utilisée par le client pour se connecter). Ces éléments sont analogues à ceux fournis pour configurer le service FTP sous Linux.

### 11.3.6 Les autres options

Il y a encore d'autres options dont nous n'avons pas parlé comme :

- **FTP Directory Browsing** : Cet élément permet de modifier le comportement par défaut du service FTP : doit-il se comporter comme sous MS-DOS ou doit-il imiter le fonctionnement d'un serveur UNIX. Quelques options d'affichage sont également renseignées.
- **FTP Request Filtering** : Comme pour le serveur Web, il est possible de filtrer certaines demandes via *file name extensions* (interdire / autoriser certaines extensions), *hidden segments* (cacher certains fichiers), *denied URL sequence* (pour empêcher l'accès à un dossier donné contenant des programmes par exemple) ou finalement interdire certaines commandes FTP via *Commands* (comme PUT pour empêcher le dépôt de fichiers ou encore GET pour empêcher le téléchargement d'un fichier, ...).
- **FTP Logging** : journaux systèmes utilisés pour consigner les événements relatifs au service FTP.
- **FTP Messages**: Permet d'afficher une bannière lors de la connexion au service
- **FTP SSL Settings**: permet de mentionner tous les paramètres pour la configuration SSL (certificats, ...)
- **FTP IP Address and Domain Restrictions** : permet de restreindre l'accès au service FTP à certaines IP ou certains domaines.
- **FTP Current Sessions**: outil de surveillance qui permet de visualiser les sessions en cours de traitement par le serveur FTP.

## 11.4 Exercices

1. Créer l'utilisateur du domaine *webeditor*, avec le mot de passe P@ssw0rd
2. Installer Web Server (IIS)
  - a. Sur le serveur SRV2016-2 (cf. Leçon 8, exercice 2)
  - b. Compléter l'installation par les éléments suivants :
    - i. HTTP Common : tout
    - ii. Security : Basic Authentication, Digest Authentication, Windows Authentication, IP and Domains Restrictions, URL Authorization
    - iii. FTP Server : FTP Service
  - c. Créer un nouveau site Web, pour le nom www.<votre-nom>.local<sup>46</sup>. Créer une page web par défaut affichant clairement le nom du site. Il doit être accessible à tous. Le site sera enregistré dans C:\inetpub\wwwlocal
  - d. Créer un nouveau site FTP, nommé MainFTP :
    - i. Il pointera vers le dossier C:\inetpub\ftproot
    - ii. Autoriser les connexions pour les utilisateurs anonymes et identifiés.
    - iii. Créer un sous-dossier pub dans le dossier ftproot. Tous les utilisateurs (y compris anonymous) doivent pouvoir déposer des dossiers et fichiers.
    - iv. Ajouter un dossier virtuel www qui pointe vers le dossier wwwlocal. Seul l'utilisateur webeditor doit pouvoir modifier ces fichiers et dossiers.
  - e. Tester votre site web dans votre navigateur et votre site FTP au moyen de FileZilla
3. Créer un nouveau site winauth.<votre-nom>.local.
  - a. Enregistrer le site dans C:\inetpub\winauth
  - b. Créer une page web par défaut identifiant celui-ci
  - c. Configurer l'authentification Windows. Seuls les membres des groupes *etudiant* et *juridique* doivent pouvoir s'y connecter.
  - d. Tester votre configuration avec les utilisateurs et0050 et je0050
4. Créer un nouveau site basicauth.<votre-nom>.local.
  - a. Enregistrer le site dans C:\inetpub\basicauth
  - b. Créer une page web par défaut identifiant celui-ci
  - c. Configurer l'authentification basique. Seuls les membres des groupes *communication* et *comptabilite* doivent pouvoir s'y connecter.
  - d. Tester votre configuration avec les utilisateurs cn0050 et ce0050
5. Installer Web Server (IIS)
  - a. Sur le serveur SRV2016-1 (cf. leçon 1)
  - b. Uniquement : IIS Management Console et FTP Service
  - c. Ajouter le site FTP FTPData
    - i. Qui pointe vers le dossier C:\CGData
    - ii. Permettant à tous les utilisateurs identifiés d'accéder en lecture et modification pour télécharger leurs fichiers personnels
    - iii. Tester votre configuration au moyen de FileZilla

<sup>46</sup> Il faut que ce nom soit référencé dans votre DNS et pointe vers l'adresse IP correcte.

## Annexe A : Installation d'un certificat SSL

Dans cette première annexe, nous allons étudier l'installation d'un certificat SSL dans IIS afin de sécuriser la connexion HTTP → HTTPS et FTP. Pour ce faire, nous avons besoin d'un certificat numérique. Vous trouverez sur l'espace e-learning un certificat numérique disponible.

### A.1 Rappel sur TLS (ex-SSL)

TLS est le protocole de sécurisation des échanges utilisés aujourd'hui. La version 1.2<sup>47</sup> est la dernière révision disponible et est implémentée dans la version IIS disponible avec Windows Server 2016. Pour rappel, un certificat numérique est un fichier, associé à un nom DNS donné et signé par une autorité de certification<sup>48</sup>.

Ainsi, par exemple, si je souhaite protéger le nom DNS `www.louis-swinnen.be`, il faut un certificat contenant ce nom et délivré par une autorité reconnue. On distingue de nombreux types de certificats (protégeant un site web, signature de documents ou de codes, ...). Parmis ceux protégeant des sites web, on distingue :

- Les certificats protégeant **2 noms** : ils contiennent et peuvent vérifier un nom DNS (avec et sans www). Par exemple : `www.amazon.fr` (qui protège `www.amazon.fr` et `amazon.fr`)
- Les certificats UCC protégeant plusieurs noms DNS (pouvant appartenir à des domaines différents). Par exemple : `swi.la`, `www.swi.la`, `www.louis-swinnen.be`, `www.swila.be`
- Les certificats *wildcard* protégeant tous les noms DNS d'un domaine donné. Par exemple : `*.helmo.be` protège tous les noms se terminant directement par `helmo.be`. Attention, pour protéger `dartagnan.cg.helmo.be`, un autre certificat est nécessaire (par exemple : `*.cg.helmo.be`).

L'autorité de certification doit procéder à une validation. Celle-ci peut être de 3 types :

- Les certificats *Domain Validated* (ou **DV**) dont seule la propriété du domaine DNS (`louis-swinnen.be` dans l'exemple précédent) a été vérifiée
- Les certificats *Organization Validated* (ou **OV**) dont l'identité de l'organisation a été vérifiée par l'autorité et incluse dans les propriétés du certificat.
- Les certificats *Extended Validation* (ou **EV**) dont l'identité et la qualité de l'organisation ont été vérifiées auprès des autorités. Ces certificats activent **la barre verte** dans le navigateur.

### A.2 Vérification du certificat

Lorsqu'un site est protégé par TLS et qu'on accède à ce site de manière sécurisée (via HTTPS), le navigateur :

1. Télécharge le certificat associé au serveur. Jusqu'il y a peu, un seul certificat pouvait être associé à un serveur Web, comme IIS. Ainsi, si plusieurs sites sont hébergés sur un même serveur, il faut que le certificat utilisé puisse protéger l'ensemble des sites (d'où l'intérêt des

<sup>47</sup> La version 1.3 est en cours d'élaboration. Elle fait l'objet d'un *draft* à l'IETF.

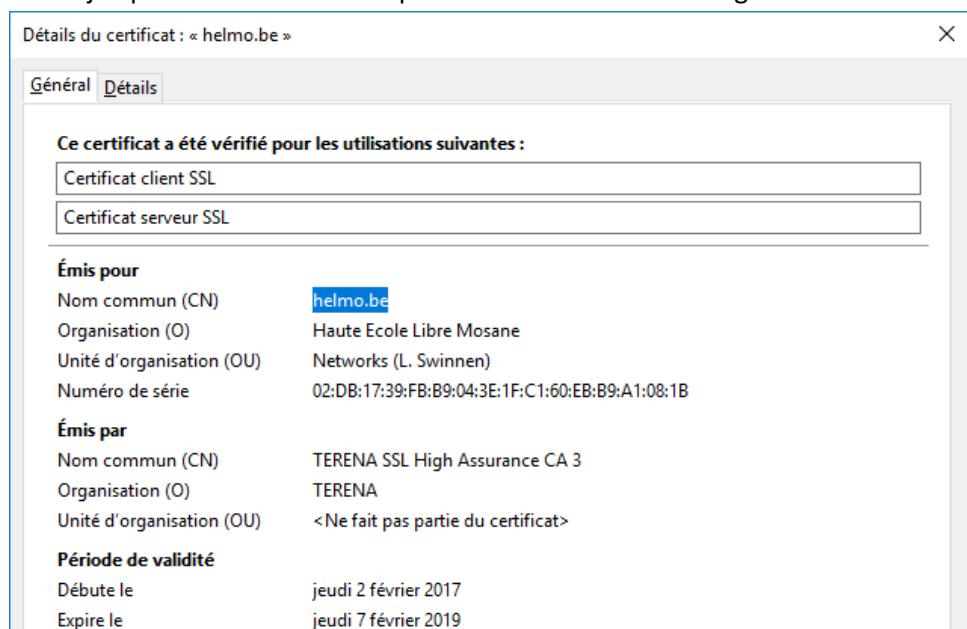
<sup>48</sup> Parmi les autorités de certification: citons Comodo, GlobalSign (marques AlphaSSL et GlobalSign), DigiCert (marques DigiCert, VeriSign, Geotrust, Thawte et RapidSSL), GoDaddy (marques GoDaddy et Starfield), Amazon, Trustwave, Entrust Datacard, SwissSign, IdenTrust, QuoVadis ou encore Certum. Tous les certificats racines de ces autorités sont reconnus.

certificats UCC ou wildcard). Aujourd'hui, avec l'option SNI<sup>49</sup>, un même serveur Web peut utiliser plusieurs certificats.

2. Vérifie si le certificat est valide et n'est pas expiré (en vérifiant les dates contenues dans le certificat).
3. Vérifie s'il est capable de trouver *une chaîne de certification* vers l'autorité racine qui a émis ce certificat. Ainsi, il arrive très souvent que des certificats intermédiaires doivent être installés afin que le serveur puisse les proposer au navigateur client.

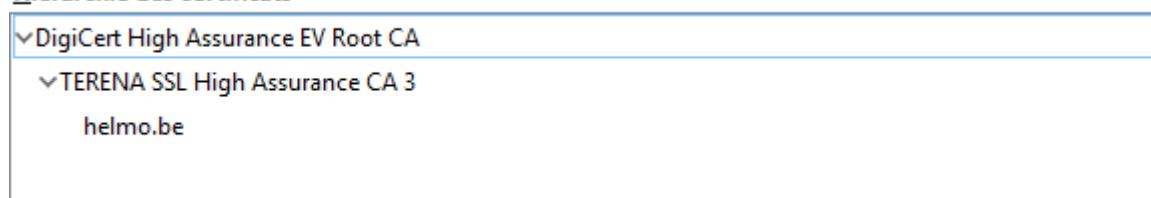
### Exemple :

Le site <https://helmo.be>, utilise un certificat EV avec les données de la haute école. Ce certificat est valide jusqu'en 2019 et est émis par l'autorité TERENA SSL High Assurance CA 3



La *chaîne de certification* est établie comme suit :

#### Hiérarchie des certificats



Ainsi, l'autorité *TERENA SSL High Assurance CA 3* est une *autorité intermédiaire* émise par *DigiCert High Assurance EV Root CA*, l'une des autorités racines de DigiCert, reconnue par tous les navigateurs. Afin de permettre au poste client de réaliser cette vérification, il faut installer tous les certificats intermédiaires sur le serveur Web également. Si ces certificats ne sont pas installés, le navigateur client affichera une erreur car il ne sera pas capable d'établir le chemin partant du certificat vers une autorité qu'il connaît.

<sup>49</sup> **Server Name Indication** : extension du protocole TLS qui permet au client d'indiquer le site à consulter avant de télécharger le certificat et chiffrer la connexion.

Le certificat est de type UCC (car plusieurs noms sont inclus à l'intérieur) et EV (activant la « barre verte » dans le navigateur) :

The screenshot shows a list of certificate subject names. At the top, there are two sections: 'Clé d'identification du sujet du certificat' (Subject Key Identifier) and 'Nom alternatif du sujet du certificat' (Subject Alternative Name). Below these, a section titled 'Valeur du champ' (Field value) lists various DNS names associated with the certificate.

Valeur du champ
Non critique
Nom DNS: helmo.be
Nom DNS: www.helmo.be
Nom DNS: connect.helmo.be
Nom DNS: inscription.helmo.be
Nom DNS: hv.helmo.be
Nom DNS: hopitalvirtuel.helmo.be
Nom DNS: project.helmo.be
Nom DNS: perso.helmo.be

### A.3 Installation d'un certificat sur IIS

Il faut disposer d'un tel certificat sur la forme d'un fichier *pfx* ou *p12* reconnu par Windows. Ce fichier contient le certificat, une clé privée associé à celui-ci et le ou les certificats intermédiaires.

Pour installer le certificat sous Windows Server 2016, il faut simplement faire un double-clic sur le fichier *p12* ou *pfx*. Windows Server vous demande alors l'emplacement de stockage du certificat. Dans notre cas, l'emplacement à choisir est *Local Machine*. L'importation se poursuit ensuite en mentionnant le mot de passe associé au fichier *p12* ou *pfx*. Dans les options d'importation, il peut être intéressant de cocher l'option **mark this key as exportable**.

Une fois le certificat importé, celui-ci est visible en utilisant la console MMC et en utilisant l'option *add/remove snap-in certificates* et en précisant ensuite **computer account** puis **Local computer**.

Dans IIS, lors de la création d'un site web, il est possible de modifier les liaisons (option **edit bindings**) pour ajouter une liaison sur le protocole HTTPS et le port 443<sup>50</sup>, ainsi que le certificat qui doit être utilisé. Une fois la liaison configurée, il suffit de redémarrer le service IIS et le site doit être accessible en utilisant le certificat installé.

<sup>50</sup> Il est possible, lors de l'activation de SSL/TLS sur IIS que ce dernier vous informe qu'un autre certificat est utilisé pour un autre serveur et vous demande si le changement peut être réalisé (un seul certificat SSL par serveur). Si vous souhaitez utiliser des certificats différents pour des sites différents, il faut cocher l'option "Require Server Name Indication"

## A.4 Exercice

On vous demande de :

1. Créer un site web `wwwswilabus` sur `WIN2016-2`
  - a. Au préalable, d'ajouter la zone DNS `secured.swilabus.xyz` et l'entrée `www.secured.swilabus.xyz` qui doit pointeur vers le serveur `WIN2016-2`
  - b. D'installer le certificat fournis sur le serveur `WIN2016-2`
  - c. Créer le site web en utilisant le protocole `https` et le nom de site `www.secured.swilabus.xyz`. On vous demande également d'activer la sécurisation SSL. Le site se trouvera dans le dossier `C:\inetpub\wwwswilabus`. Ajouter une page web par défaut reconnaissable.
  - d. De vérifier, depuis votre machine VM Windows 10, la connexion à `https://www.secured.swilabus.xyz`. Le site est-il sécurisé ? Quelles sont les propriétés du certificat ?
2. Tenter d'accéder au site web `https://www.secured.swilabus.xyz` depuis votre machine Windows hôte (exécutant VMware), qu'observez-vous ? Pourquoi ?
3. Sécuriser le site FTP installé sur `WIN2016-1`
  - a. Au préalable, ajouter l'entrée `secured.swilabus.xyz` qui doit pointer vers le serveur `WIN2016-1`
  - b. Installer le certificat la machine `WIN2016-1`
  - c. Sécuriser le site FTP en exigeant la connexion SSL
  - d. Tester votre configuration en utilisant FileZilla

---

Laboratoire d'administration système

# Partie « Windows »

---

## Références bibliographiques principales

Ce document se base sur les principales références suivantes :

- [70-740] C. Zacker, Exam Ref 70-740 : Installation, Storage and Compute with Windows® Server® 2016, 1<sup>st</sup> edition, Microsoft Press, January 2017
- [70-741] A. Warren, Exam Ref 70-741 : Networking with Windows® Server® 2016, 1<sup>st</sup> edition, Microsoft Press, December 2016
- [70-742] A. Warren, Exam Ref 70-742 : Identity with Windows® Server® 2016, 1<sup>st</sup> edition, Microsoft Press, March 2017



SWILABUS