

PowerShell offre la possibilité de personnaliser l'affichage des colonnes.

```
Get-Help about_Calculated_Properties
```

Format-List

- **name/label** – optionnel
- **expression**
- **formatstring** – optionnel

Format-Table

- **name/label** – optionnel
- **expression**
- **formatstring** – optionnel
- **width** – optionnel
- **alignment** – optionnel

Select-Object

- **name/label** – optionnel
- **expression**

Sort-Object

- **expression**
 - **ascending/descending** – optionnel
-

name/label

- Spécifie le nom de la propriété en cours de création.
- Vous pouvez utiliser **name** ou son alias **label**.

expression

- Un bloc de script utilisé pour calculer la valeur de la nouvelle propriété.

alignment

- Utilisé par les cmdlets qui produisent une sortie tabulaire pour définir comment les valeurs sont affichées dans une colonne.
- La valeur doit être **left**, **center**, ou **right**.

formatstring

- Spécifie une chaîne de format qui définit comment la valeur est formatée pour la sortie.
- Pour plus d'informations sur les chaînes de format, voir Types de format dans .NET.

width

- Spécifie la largeur maximale de la colonne d'un tableau lorsque la valeur est affichée.
- La valeur doit être supérieure à 0.

ascending / descending

- Les deux paramètres permettent de spécifier l'ordre de tri pour une ou plusieurs propriétés.
- Ce sont des valeurs booléennes.

Exemple 1a - Exemple avec des colonnes personnalisées avec Format-List

```
Get-ADUser -Filter * -Properties DisplayName |  
Format-List Name,DisplayName,UserPrincipalName,DistinguishedName
```

On affiche le DistinguishedName de l'unité d'organisation parent des utilisateurs.

```
Get-ADUser -Filter * -Properties DisplayName |  
Format-List Name,DisplayName,UserPrincipalName,DistinguishedName,  
@{label="OU parent"  
expression={$PSItem.DistinguishedName -split ',',2)[1]}
```

Exemple 1b - Exemple avec des colonnes personnalisées avec Format-List

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

```
Get-ADOrganizationalUnit -Filter *  
-SearchBase $OU |  
Format-List Name,DistinguishedName
```

On affiche le DistinguishedName de l'unité d'organisation parent des unités d'organisation.

```
$OU = "OU=FORMATION,DC=FORMATION,DC=LOCAL"  
  
Get-ADOrganizationalUnit -Filter *  
-SearchBase $OU |  
Format-List Name,DistinguishedName,  
@{label="OU parent"  
expression={$PSItem.DistinguishedName -split ',',2)[1]}}
```

Exemple 2 - Exemple avec des colonnes personnalisées avec Format-List

```
$NOM_VM = "routeur"  
Get-VMNetworkAdapter -VMName $NOM_VM  
| Format-List Name,SwitchName,MacAddress,IPAddresses
```

Utilisation du paramètre -ExpandProperty avec plusieurs propriétés.

```
$NOM_VM = "routeur"  
Get-VMNetworkAdapter -VMName $NOM_VM  
| Format-List Name,SwitchName,MacAddress,  
@{label="IP"  
expression={$PSItem | Select-Object -ExpandProperty IPAddresses} -Join ','}
```

Exemple 3 - Exemple avec des colonnes personnalisées avec Format-List

Par défaut la capacité des barrettes de mémoire est affichée en octets.

```
Get-CIMInstance -Class Win32_PhysicalMemory `  
| Format-List Caption,Capacity,  
    Speed,DeviceLocator,Manufacturer,SerialNumber
```

note: pas besoin d'utiliser le paramètre **FormatString** pour afficher la taille des barrettes de mémoire

```
Get-CIMInstance -Class Win32_PhysicalMemory `  
| Format-List Caption,  
    @{label='Size(GO)'  
        expression={$PSitem.Capacity / 1GB}}  
    },  
    Speed,DeviceLocator,Manufacturer,SerialNumber
```

Exemple 4 - Exemple avec des colonnes personnalisées avec Format-Table

Par défaut la taille des disques est affichée en octets.

```
$partition = 'C:'  
  
Get-CIMinstance -Class Win32_LogicalDisk `  
    -Filter "DeviceId='\$partition'" `  
    | Format-Table SystemName,DeviceID,VolumeName,Size,FreeSpace -AutoSize
```

note 1: on modifie le titre de plusieurs colonnes du tableau avec le paramètre Label

note 2: on utilise le paramètre FormatString='N2' pour afficher le résultat des calculs

```
$partition = 'C:'  
  
Get-CIMinstance -Class Win32_LogicalDisk `  
    -Filter "DeviceId='\$partition'" `  
    | Format-Table SystemName,  
        @{label='Partition'  
            expression={$PSItem.DeviceId}  
        },  
        @{label='Description'  
            expression={$PSItem.VolumeName}  
        },  
        @{label='Size(GO)'  
            expression={$PSItem.Size / 1GB}  
            formatstring='N2'  
            alignment='center'  
        },  
        @{label='FreeSpace(GO)'  
            expression={$PSItem.FreeSpace / 1GB}  
            formatstring='N2'  
            alignment='center'  
        } -AutoSize
```

Exemple 5 - Exemple avec des colonnes personnalisées avec Format-Table

Utilisation des paramètres width et alignment avec Format-Table.

```
$chemin = "F:\_VIRTUEL\DISQUE"  
  
$nom = @{label = 'Nom'  
    expression= {$PSItem.Name}  
    width=100  
    alignment='left'  
}  
  
$taille = @{label='KB'  
    expression={ ($PSItem.Length / 1KB) }  
    width=20  
    alignment='right'  
}  
  
Get-ChildItem -Path $chemin | Format-Table $nom,$taille
```

Exemple 6 - Exemple avec des colonnes personnalisées avec Sort-Object

Pour utiliser **Sort-Object** avec plusieurs paramètres, il faut utiliser des "hash table" pour trier par ordre croissant, décroissant, ou une combinaison d'ordres de tri.

```
Get-Service | Sort-Object -Property @{expression = "Status"  
                               descending = $true  
                           },  
                         @{expression = "DisplayName"  
                           ascending = $true  
                         }
```

Exemple 7 - Exemple avec des colonnes personnalisées avec Select-Object

```
Get-NetAdapter | Select-Object Name,MacAddress
```

On modifie l'affichage de l'adresse MAC.

```
Get-NetAdapter | Select-Object Name,  
                  @{label='MacAddress'  
                    expression={ $PSitem.MacAddress -replace ':+,-' }}
```

Exemple 8 - Exemple avec des colonnes personnalisées avec Select-Object

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

```
Get-ADOrganizationalUnit -Filter * `  
-SearchBase $OU -Properties CanonicalName | Sort-Object CanonicalName | `  
Select-Object Name,DistinguishedName
```

On affiche le DistinguishedName de l'unité d'organisation parent des unités d'organisation.
Les unités d'organisation sont triées en ordre alphabétique sur la propriété CanonicalName.
On enregistre le résultat de la commande dans un fichier CSV.

```
$OU = "OU=FORMATION,DC=FORMATION,DC=LOCAL"  
  
Get-ADOrganizationalUnit -Filter * `  
-SearchBase $OU -Properties CanonicalName | Sort-Object CanonicalName | `  
Select-Object @{label="NOM"  
              expression={$PSitem.Name}  
            },  
             @{label="OU_PARENT"  
               expression= {($PSitem.DistinguishedName -split ',',2)[1]}  
             } | `  
Export-Csv -Delimiter ";" `  
          -NoTypeInformation `  
          -Path "E:\_TEMP\OU_FORMATION.csv"
```

Pour le cours, il n'est pas nécessaire de comprendre le contenu des annexes 1 et 2.

Le contenu de ce document est un complément pour les prochains cours.

Informations sur le module ActiveDirectory

Active Directory

<https://learn.microsoft.com/en-us/powershell/module/activedirectory>

Le module ActiveDirectory contient 147 cmdlets.

`(Get-Command -Module ActiveDirectory).Count`

Utilisation de plusieurs GET-AD* et SET-AD*

Utiliser plusieurs cmdlets de PowerShell afin de se familiariser avec les objets d'un domaine Active Directory

- Utiliser plusieurs cmdlets GET du module ActiveDirectory
`Get-ADForest, Get-ADDomain,
Get-ADOrganizationalUnit, Get-ADComputer, Get-ADUser, Get-ADGroup, Get-ADObject`
- Utiliser plusieurs cmdlets SET du module ActiveDirectory
`Set-ADDomain, Set-ADObject`
- Utiliser le cmdlet **Move-ADObject** pour déplacer un objet de l'Active Directory

Les opérateurs du paramètre **-Filter** avec des objets de l'Active Directory

Commande pour afficher des informations sur le paramètre "-Filter" avec des objets de l'Active Directory.
`Get-Help about_ActiveDirectory_Filter`

Mahleureusement, depuis plusieurs années la commande ne fonctionne pas.

Le contenu de la commande est disponible sur le site

[https://docs.microsoft.com/en-us/previous-versions/windows/server/hh531527\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/server/hh531527(v=ws.10))

Voici la liste des opérateurs du paramètre **-Filter** pour les objets de l'Active Directory.

Les opérateurs du paramètre -Filter pour les objets de l'Active Directory	Description
<code>-eq</code>	Égal à
<code>-ne</code>	Pas égal à
<code>-le</code>	Plus petit que ou égal à
<code>-lt</code>	Plus petit que
<code>-ge</code>	Plus grand que ou égal à
<code>-gt</code>	Plus grand que
<code>-like</code>	Similaire à <ul style="list-style-type: none">• supporte le caractère *
<code>-notlike</code>	Pas similaire à <ul style="list-style-type: none">• supporte le caractère *
<code>-approx</code>	Approximativement égal à
<code>-bor</code>	OU binaire
<code>-band</code>	ET binaire
<code>-recursivematch</code>	Le filtre est appliqué récursivement
<code>-and</code>	ET logique
<code>-or</code>	OU logique
<code>-not</code>	NON logique

Les opérateurs du paramètre `-Filter` pour les objets de l'Active Directory.

-Filter

Specifies a query string that retrieves Active Directory objects. This string uses the PowerShell Expression Language syntax. The PowerShell Expression Language syntax provides rich type-conversion support for value types received by the *Filter* parameter. The syntax uses an in-order representation, which means that the operator is placed between the operand and the value. For more information about the *Filter* parameter, type `Get-Help about_ActiveDirectory_Filter`.

Syntax:

The following syntax uses Backus-Naur form to show how to use the PowerShell Expression Language for this parameter.

```
<filter> ::= "{" <FilterComponentList> "}"  
  
<FilterComponentList> ::= <FilterComponent> | <FilterComponent> <JoinOperator> <FilterComponent> |  
<NotOperator> <FilterComponent>  
  
<FilterComponent> ::= <attr> <FilterOperator> <value> | "(" <FilterComponent> ")"  
  
<FilterOperator> ::= "-eq" | "-le" | "-ge" | "-ne" | "-lt" | "-gt" | "-approx" | "-bor" | "-band" | "-recursivematch" | "-like" |  
"-notlike"  
  
<JoinOperator> ::= "-and" | "-or"  
  
<NotOperator> ::= "-not"  
  
<attr> ::= <PropertyName> | <LDAPDisplayName of the attribute>  
  
<value> ::= <compare this value with an <attr> by using the specified <FilterOperator>>
```

For a list of supported types for <value>, type `Get-Help about_ActiveDirectory_ObjectModel`.

Note: For String parameter type, PowerShell will cast the filter query to a string while processing the command. When using a string variable as a value in the filter component, make sure that it complies with the [PowerShell Quoting Rules](#). For example, if the filter expression is double-quoted, the variable should be enclosed using single quotation marks: `Get-ADUser -Filter "Name -like '$UserName'"`. On the contrary, if curly braces are used to enclose the filter, the variable should not be quoted at all: `Get-ADUser -Filter {Name -like $UserName}`.

Note: PowerShell wildcards other than *, such as ?, are not supported by the *Filter* syntax.

Obtenir des informations sur la forêt avec Get-ADForest

Get-ADForest

Trouvez la valeur des propriétés suivantes:

Nom de la propriété	Valeur de la propriété
ForestMode	Windows2016Forest
DomainNamingMaster	SERVEUR1.FORMATION.LOCAL
GlobalCatalogs	{SERVEUR1.FORMATION.LOCAL}
SchemaMaster	SERVEUR1.FORMATION.LOCAL

Obtenir des informations sur le domaine avec Get-ADDomain

Get-ADDomain

Trouvez la valeur des propriétés suivantes:

Nom de la propriété	Valeur de la propriété
DistinguishedName	DC=FORMATION,DC=LOCAL
DNSRoot	FORMATION.LOCAL
DomainMode	Windows2016Domain
Name	FORMATION
Forest	FORMATION.LOCAL

La commande qui retourne SEULEMENT la valeur de la propriété DistinguishedName de votre domaine:
[`\(Get-ADDomain\).DistinguishedName`](#)

La commande qui retourne SEULEMENT la valeur de la propriété DNSRoot de votre domaine:
[`\(Get-ADDomain\).DNSRoot`](#)

La commande qui retourne SEULEMENT la valeur du SID (Security Identifier) d'un domaine Active Directory.
[`\(Get-ADDomain\).DomainSID.Value`](#)

Get-ADDefaultDomainPasswordPolicy

La commande affiche les propriétés sur la configuration des mots de passe au niveau du domaine.

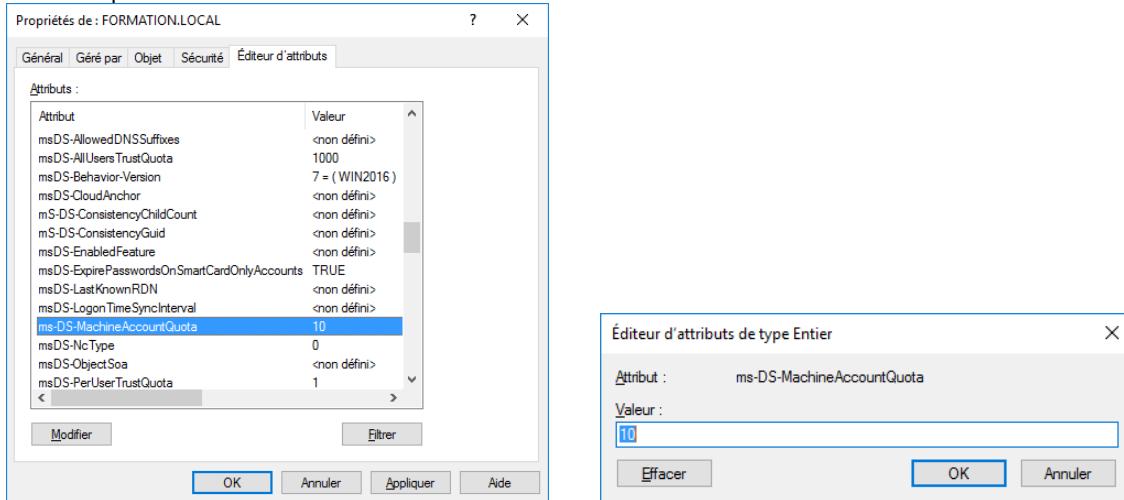
[`Get-ADDefaultDomainPasswordPolicy`](#)

Empêcher un utilisateur de joindre un ordinateur au domaine avec Set-ADDomain

Par défaut, un utilisateur authentifié qui n'est pas membre du groupe Administrateurs peut joindre 10 ordinateurs au domaine.

Dans la console UOAD

- Afficher les attributs du domaine **FORMATION.LOCAL** et sélectionner l'onglet "Éditeur d'attributs"
- Sélectionner l'attribut **ms-DS-MachineAccountQuota**
- La valeur par défaut de l'attribut **ms-DS-MachineAccountQuota** est **10**



Pour empêcher un utilisateur authentifié de joindre des ordinateurs au domaine on doit modifier la valeur de l'attribut **ms-DS-MachineAccountQuota** pour **0**.

Par programmation PowerShell

```
Set-ADDomain -Identity ((Get-ADDomain).DistinguishedName) `  
-Replace @{'ms-DS-MachineAccountQuota'=0}
```

Obtenir des informations sur les unités d'organisation d'un domaine avec Get-ADOrganizationalUnit

La commande qui affiche les principales propriétés de l'unité d'organisation FORMATION
`Get-ADOrganizationalUnit -Identity "OU=formation,DC=formation,DC=local"`

La commande qui affiche toutes les propriétés de l'unité d'organisation FORMATION
`Get-ADOrganizationalUnit -Identity "OU=formation,DC=formation,DC=local" -Properties *`

La commande qui affiche les principales propriétés de toutes les unités d'organisation de votre domaine
`Get-ADOrganizationalUnit -Filter *`

La commande qui affiche toutes les propriétés de toutes les unités d'organisation de votre domaine
`Get-ADOrganizationalUnit -Filter * -Properties *`

La commande qui affiche les principales propriétés des unités d'organisation dont le nom contient "gestion"
`Get-ADOrganizationalUnit -Filter {Name -like "*gestion*"}`

La commande qui affiche les principales propriétés des unités d'organisation dont le nom commence par "inf"
`Get-ADOrganizationalUnit -Filter {Name -like "inf*"}`

La commande qui affiche les principales propriétés des unités d'organisation dont le nom est similaire à "gestionnaire?"

Le paramètre -Filter ne fonctionne pas avec le caractère ? qui remplace un seul caractère.
`et-ADOrganizationalUnit -Filter {Name -like "gestionnaire?")}`

SOLUTION À CE PROBLÈME

On doit obligatoirement utiliser **Where-Object** qui s'exécute sur le résultat de la commande.

`Get-ADOrganizationalUnit -Filter * | Where-Object { $PSItem.Name -like "gestionnaire?" }`

La commande qui affiche les propriétés "Name" et "DistinguishedName" de toutes les unités d'organisation de votre domaine

`Get-ADOrganizationalUnit -Filter * | Format-Table Name,DistinguishedName -AutoSize`

La commande qui affiche les propriétés "Name" et "Created" de toutes les unités d'organisation de votre domaine
`Get-ADOrganizationalUnit -Filter * -Properties created | Format-Table Name,Created -AutoSize`

La commande qui affiche en ordre alphabétique la propriété CanonicalName de toutes les unités d'organisation de votre domaine

`Get-ADOrganizationalUnit -Filter * -Properties CanonicalName | Select-Object -Property CanonicalName | Sort-Object CanonicalName`

Le paramètre -Filter et l'attribut DistinguishedName

Exemple 1

Trouver l'unité d'organisation dont le DistinguishedName est ou=formation,dc=formation,dc=local

```
# Commande PowerShell avec le paramètre -Identity
$OU = "ou=formation,dc=formation,dc=local"
Get-ADOrganizationalUnit -Identity $OU
```

Trouver l'unité d'organisation dont le DistinguishedName est ou=formation,dc=formation,dc=local

```
# Commande PowerShell avec le paramètre -Filter
$OU = "ou=formation,dc=formation,dc=local"
Get-ADOrganizationalUnit -Filter {DistinguishedName -eq $OU}
```

La commande avec le paramètre -Filter fonctionne parce qu'on vérifie avec -eq et que \$OU ne contient pas le caractère générique *****

Exemple 2

Trouver la liste des unités d'organisation dont le DistinguishedName se termine par ou=formation,dc=formation,dc=local

```
$OU = "*ou=formation,dc=formation,dc=local"
Get-ADOrganizationalUnit -Filter {DistinguishedName -like $OU}
```

La commande avec le paramètre -Filter ne fonctionne pas parce qu'on vérifie avec -like et que \$OU contient le caractère générique *****

Vous ne pouvez pas utiliser de caractères génériques lors du filtrage basé sur le DistinguishedName.

SOLUTION À CE PROBLÈME

On doit obligatoirement utiliser **Where-Object** qui s'exécute sur le résultat de la commande.

```
$OU = "*ou=formation,dc=formation,dc=local"
Get-ADOrganizationalUnit -Filter * | ` 
    Where-Object {$PSItem.DistinguishedName -like $OU}
```

Obtenir des informations sur les ordinateurs d'un domaine avec Get-ADComputer

La commande qui affiche les principales propriétés de l'ordinateur SERVEUR2.
`Get-ADComputer -Identity "SERVEUR2"`

La commande qui affiche toutes les propriétés de l'ordinateur SERVEUR2.

```
Get-ADComputer -Identity "SERVEUR2" `  
    -Properties *
```

Chaque ordinateur a un mot de passe qui est géré par le contrôleur de domaine.
Le mot de passe est automatiquement modifié tous les 30 jours.

PasswordLastSet affiche la date à laquelle le mot de passe de l'ordinateur a été modifié.

```
Get-ADComputer -Identity SERVEUR2 `  
    -Properties PasswordLastSet
```

La commande qui affiche les principales propriétés des ordinateurs dont le nom commence par "SERVEUR"
`Get-ADComputer -Filter {Name -like "SERVEUR*"}`

La commande qui affiche SEULEMENT le nom de tous les ordinateurs de votre domaine

```
(Get-ADComputer -Filter *).Name
```

La commande qui affiche les principales propriétés des ordinateurs dont le nom est similaire à "SERVEUR?"
Le paramètre -Filter ne fonctionne pas avec le caractère ? qui remplace un seul caractère.

```
Get-ADComputer -Filter {Name -like "SERVEUR?"}
```

SOLUTION À CE PROBLÈME

On doit obligatoirement utiliser **Where-Object** qui s'exécute sur le résultat de la commande.

```
(Get-ADComputer -Filter * | Where-Object { $PSItem.Name -like "SERVEUR?" }).Name
```

La commande qui affiche seulement six propriétés de l'ordinateur SERVEUR2

```
Get-ADComputer -Identity SERVEUR2 `  
    -Properties IPv4Address,OperatingSystem,OperatingSystemVersion | `  
    Format-List Name,DNSHostName,SamAccountName,  
        IPv4Address,OperatingSystem,OperatingSystemVersion
```

Name	:	SERVEUR2
DNSHostName	:	SERVEUR2.FORMATION.LOCAL
SamAccountName	:	SERVEUR2\$
IPv4Address	:	192.168.1.20
OperatingSystem	:	Windows Server 2019 Datacenter
OperatingSystemVersion	:	10.0 (17763)

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

Voici une commande qui affiche plusieurs propriétés de tous les ordinateurs de votre domaine en triant deux paramètres en ordre croissant et en triant un paramètre en ordre décroissant.

```
Get-ADComputer -Filter * ` 
    -Properties * | ` 
    Sort-Object -Property @{{Expression = "Description"; Ascending = $true}, 
        @{{Expression = "OperatingSystem"; Ascending = $true}, 
            @{{Expression = "OperatingSystemVersion"; Descending = $true}} | ` 
    Format-Table Description,Name,OperatingSystem,OperatingSystemVersion,WhenChanged -AutoSize
```

Voici le code qui permet d'afficher le nom de l'utilisateur qui a joint un ordinateur à l'Active Directory.

Si l'utilisateur a une délégation pour créer des objets dans l'Active Directory ou est un membre du groupe "Admins du domaine" alors mS-DS-CreatorSID est vide.

```
$nom = Get-ADComputer -Identity SERVEUR2 ` 
    -Properties mS-DS-CreatorSID | ` 
    Select-Object -Expandproperty mS-DS-CreatorSID | ` 
    Select-Object -ExpandProperty Value | ` 
    Foreach-Object {Get-ADUser -Filter {SID -eq $PSItem}} 

if ([string]::IsNullOrEmpty($nom)) 
{
    Write-Host "mS-DS-CreatorSID est vide" -ForegroundColor Yellow
}
else
{
    Write-Host "mS-DS-CreatorSID correspond à $nom" -ForegroundColor Cyan
}
```

Obtenir des informations sur les utilisateurs d'un domaine avec Get-ADUser

La commande qui affiche les principales propriétés de l'utilisateur dont le nom d'ouverture de session est EMP01

```
Get-ADUser -Identity "EMP01"
```

La commande qui affiche toutes les propriétés de l'utilisateur dont le nom d'ouverture de session est EMP01

```
Get-ADUser -Identity "EMP01"  
-Properties *
```

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

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

```
$rep = Get-ADUser -Filter * | Where-Object { $PSItem.SID -like "S-1-5-21-*-500" }  
$rep.Name
```

La commande qui affiche les principales propriétés des utilisateurs dont le nom de famille est Coutu.

```
Get-ADUser -Filter 'Surname -eq "Coutu"'
```

La commande qui affiche les principales propriétés des utilisateurs dont le nom d'ouverture de session débute par "EMP".

```
Get-ADUser -Filter {SamAccountName -like "EMP*"}

---


```

La commande qui affiche les principales propriétés des utilisateurs dont le nom d'ouverture de session est similaire à "EMP3?"

Le paramètre -Filter ne fonctionne pas avec le caractère ? qui remplace un seul caractère.

```
Get-ADUser -Filter {SamAccountName -like "EMP3?"}
```

SOLUTION À CE PROBLÈME

On doit obligatoirement utiliser **Where-Object** qui s'exécute sur le résultat de la commande.

```
Get-ADUser -Filter * | Where-Object { $PSItem.SamAccountName -like "EMP3?" }
```

La commande qui affiche les principales propriétés des utilisateurs qui sont dans l'unité d'organisation "FORMATION" qui est directement sous le domaine "FORMATION.LOCAL".

```
$sb= "OU=formation,DC=formation,DC=local"
```

```
Get-ADUser -Filter * -SearchBase $sb -SearchScope Subtree  
ou  
Get-ADUser -Filter * -SearchBase $sb  
# Subtree est la valeur par défaut de SearchScope
```

Voici le code qui permet d'afficher les utilisateurs dont le nom débute par 0,1,2,3,4,5,6,7,8,9.

```
for ($i = 0; $i -le 9; $i++)
{
    $nom = -join ($i,"*")
    Get-ADUser -Filter {Name -like $nom}
}
```

Trouver les utilisateurs dans l'Active Directory qui ont une "adresse de messagerie" en utilisant -Filter.

```
$sb = (Get-ADDomain).DistinguishedName

Get-ADUser -SearchBase $sb -Filter {mail -like "*"} -Properties *
ou
Get-ADUser -SearchBase $sb -Filter * -Properties * | `

Where-Object {$PSitem.mail -like "*"}  


---


```

Trouver les utilisateurs dans l'Active Directory qui ont un "gestionnaire" en utilisant -Filter.

L'attribut "manager" contient le "DistinguishedName" du gestionnaire.

Vous ne pouvez pas utiliser de caractères génériques lors du filtrage basé sur le DistinguishedName.

SOLUTION À CE PROBLÈME

On doit obligatoirement utiliser **Where-Object** qui s'exécute sur le résultat de la commande.

```
$sb = (Get-ADDomain).DistinguishedName

Get-ADUser -SearchBase $sb -Filter * -Properties * | `

Where-Object {$PSitem.manager -ne $null}  


---


```

Obtenir des informations sur les groupes d'un domaine avec Get-ADGroup

La commande qui affiche les principales propriétés du groupe Administrateurs
`Get-ADGroup -Identity "Administrateurs"`

La commande qui affiche toutes les propriétés du groupe Administrateurs
`Get-ADGroup -Identity "Administrateurs" -Properties *`

Le nom du groupe dont le SID se termine par 513 varie selon la langue

- En français le nom du groupe est "Utilisateurs du domaine"
- En anglais le nom du groupe est "Domain Users"
- ...

```
$rep = Get-ADGroup -Filter * | Where-Object { $PSItem.SID -like "S-1-5-21-*-513" }  
$rep.Name
```

La commande qui affiche les principales propriétés des groupes dont le nom commence par "Adm"

```
Get-ADGroup -Filter {Name -like "Adm*"}  
$rep.Name
```

La commande qui affiche SEULEMENT le nom des groupes dont le nom commence par "Adm".

```
(Get-ADGroup -Filter {Name -like "Adm*"}).Name
```

La commande qui affiche les principales propriétés des groupes dont le nom est similaire à "gr???"

Le paramètre -Filter ne fonctionne pas avec le caractère ? qui remplace un seul caractère.

```
Get-ADGroup -Filter {Name -like "gr???"}
```

SOLUTION À CE PROBLÈME

On doit obligatoirement utiliser **Where-Object** qui s'exécute sur le résultat de la commande.

```
Get-ADGroup -Filter * | Where-Object { $PSItem.Name -like "gr???" }
```

Obtenir des informations sur des objets de l'Active Directory avec Get-ADObject

Il est souvent plus avantageux d'utiliser Get-ADForest, Get-ADDomain, Get-ADOrganizationalUnit, Get-ADComputer, Get-ADUser et Get-ADGroup.

Dans certaines situations, nous devons utiliser Get-ADObject.

Il n'est pas possible d'afficher le contenu de l'attribut ms-DS-MachineAccountQuota du domaine en utilisant Get-ADDomain parce que les paramètres -Filter et -Properties n'existent pas.

Requête qui permet d'afficher le contenu de l'attribut ms-DS-MachineAccountQuota du domaine

```
Get-ADObject -Identity ((Get-ADDomain).DistinguishedName) `  
-Properties ms-DS-MachineAccountQuota
```

Modifier des informations sur des objets de l'Active Directory avec Set-ADObject

Il est souvent plus avantageux d'utiliser Set-ADForest, Set-ADDomain, Set-ADOrganizationalUnit, Set-ADComputer, Set-ADUser et Set-ADGroup.

Dans certaines situations, nous devons utiliser Set-ADObject.

Il n'est pas possible de protéger les utilisateurs, les groupes et les ordinateurs contre une suppression accidentelle en utilisant Get-ADComputer, Get-ADUser, Get-ADGroup.

Requête qui permet de protéger l'ordinateur SERVEUR2 d'une suppression accidentelle.

```
Get-ADComputer -Identity SERVEUR2 | Set-ADObject -ProtectedFromAccidentalDeletion:$true
```

Requête qui permet de protéger l'utilisateur TECH d'une suppression accidentelle.

```
Get-ADUser -Identity TECH | Set-ADObject -ProtectedFromAccidentalDeletion:$true
```

Requête qui permet de protéger le groupe grFormation d'une suppression accidentelle.

```
Get-ADGroup -Identity grFormation | Set-ADObject -ProtectedFromAccidentalDeletion:$true
```

Requête qui permet de trouver tous les objets du domaine dont le nom débute par "Adm"

```
$sb = "DC=formation,DC=local"  
  
(Get-ADObject -SearchBase $sb -Filter {Name -like "Adm*"}) | `  
Sort-Object ObjectClass | `  
Format-Table ObjectClass,DistinguishedName -AutoSize
```

Déplacer des objets de l'Active Directory avec Move-ADObject

Pour déplacer un objet de l'Active Directory, il faut utiliser Move-ADObject.

```
# Nous avons besoin du DistinguishedName de l'objet et
# du DistinguishedName du nouvel emplacement.
$ordi = "CN=S9,OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"
$emplacement = "OU=SQL,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"

Move-ADObject -Identity $ordi -TargetPath $emplacement
```

Le nom d'un utilisateur est unique dans l'Active Directory.

Le nom d'un groupe est unique dans l'Active Directory.

Le nom d'un ordinateur est unique dans l'Active Directory.

```
# Nous avons besoin du DistinguishedName du nouvel emplacement.
$emplacement = "OU=SQL,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"

Get-ADComputer -Identity S9 | Move-ADObject -TargetPath $emplacement
```

Pour le déplacement d'une unité d'organisation, nous devons utiliser le DistinguishedName.

Le nom d'une unité d'organisation n'est pas unique dans l'Active Directory.

Le déplacement d'une unité d'organisation implique le déplacement de tous les objets qui sont dans l'unité d'organisation qui sera déplacée.

```
# Nous avons besoin du DistinguishedName de l'unité d'organisation et
# du DistinguishedName du nouvel emplacement.
$OU = "OU=SRVTEST,DC=FORMATION,DC=LOCAL"
$emplacement = "OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"

Move-ADObject -Identity $OU -TargetPath $emplacement
```

ANNEXE 1

Utilisation du paramètre -LDAPFilter avec Get-ADUser

Il est possible d'effectuer des requêtes en utilisant la syntaxe LDAP (Lightweight Directory Access Protocol).

- LDAP est un protocole ouvert et multiplateforme utilisé pour l'authentification des services d'annuaire.
- LDAP est un moyen de communiquer avec Active Directory.

Get-ADUser permet d'utiliser le paramètre **-LDAPFilter**.

Les opérateurs sont différents selon l'utilisation du paramètre **-Filter** ou l'utilisation du paramètre **-LDAPFilter**.

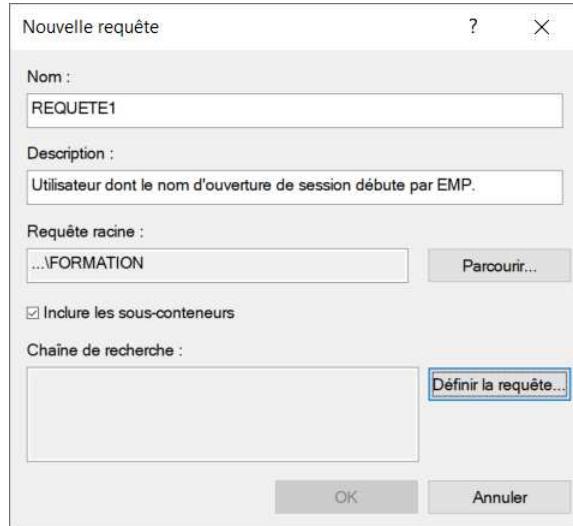
Les opérateurs du paramètre -Filter	Les opérateurs du paramètre -LDAPFilter
-eq	=
-ne	! x=y
-le	<=
-lt	! x >= y
-ge	>=
-gt	! x <= y
-like	=
-notlike	! x = y
-and	&
-or	
-not	!

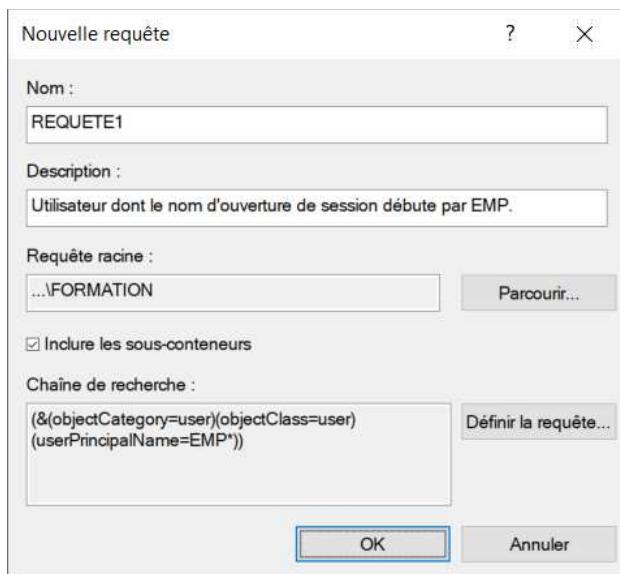
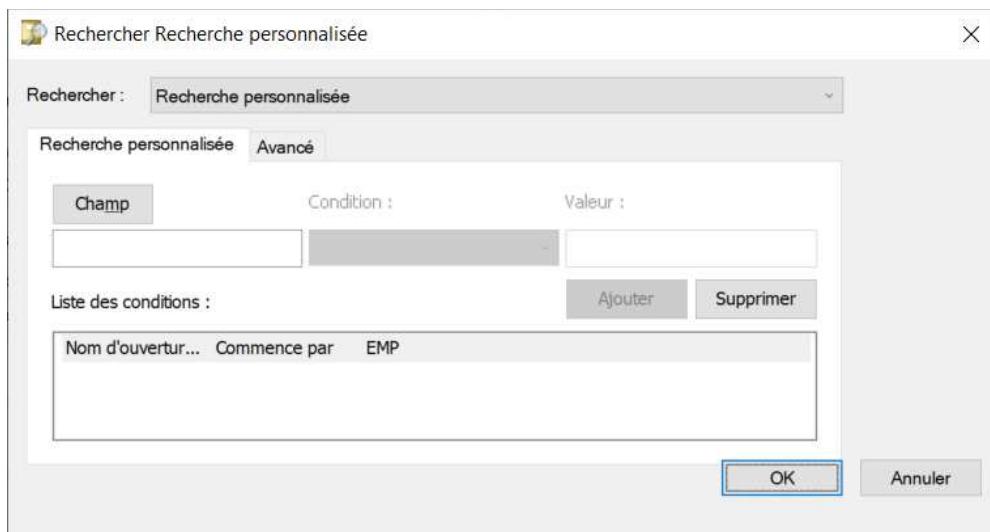
Utilisation de "Requêtes enregistrées" pour générer le code LDAP



Dans la console UOAD, "**Requêtes enregistrées**" permet de générer le code LDAP d'une requête.

Utilisateur dont le nom d'ouverture de session débute par EMP.





`(& (objectCategory=user) (objectClass=user) (userPrincipalName=EMP*))`

Voici plusieurs exemples qui utilisent le paramètre -LDAPFilter avec Get-ADUser

```
$sb = (Get-ADDomain).DistinguishedName
$user_LDAP = "&(objectCategory=user) (objectClass=user)"
```

le nom d'ouverture de session débute par EMP

```
$q1 = "(" + $user_LDAP +
      "(userPrincipalName=EMP*)" +
      ")"
Get-ADUser -SearchBase $sb -LDAPFilter $q1 -Properties *
```

le nom d'ouverture de session débute par EMP **ET** l'adresse de messagerie se termine par @formation.local

```
$q2 = "(" + $user_LDAP +
      "(userPrincipalName=EMP*) (mail=*@formation.local)" +
      ")"
Get-ADUser -SearchBase $sb -LDAPFilter $q2 -Properties *
```

le nom = Richard **OU** le nom = Michelle **OU** le nom = Patrick

```
$q3 = "(" + $user_LDAP +
      "(|(cn=Richard)(cn=Michelle)(cn=Patrick))" +
      ")"
Get-ADUser -SearchBase $sb -LDAPFilter $q3 -Properties *
```

le prénom = Richard **ET** (la ville = Laval **OU** la ville = Verdun)

```
$q4 = "(" + $user_LDAP +
      "(&(givenName=EMP01) (|(l=Laval) (l=Verdun)))" +
      ")"
Get-ADUser -SearchBase $sb -LDAPFilter $q4 -Properties *
```

La liste des utilisateurs qui n'ont pas de gestionnaire en utilisant **-LDAPFilter**

```
$q5 = "(" + $user_LDAP +
      "(!manager=*)" +
      ")"
Get-ADUser -SearchBase $sb -LDAPFilter $q5 -Properties *
```

ANNEXE 2

Utilisation de LDAP pour rechercher un ou plusieurs utilisateurs de l'Active Directory

Les deux exemples n'utilisent pas le module ActiveDirectory.

Les deux exemples utilisent la classe "System.DirectoryServices.DirectorySearcher" du ".NET Framework".

```
# Code pour rechercher l'utilisateur EMP01 qui est dans la OU "FORMATION"
# $nom correspond au nom d'ouverture de session
$nom = " EMP01"

# ADSI signifie (Active Directory Service Interfaces)
$root = [ADSI]"LDAP://OU=formation,DC=formation,DC=local"

$searcher = New-Object -TypeName System.DirectoryServices.DirectorySearcher -ArgumentList ($root)
$searcher.filter = "(&(objectCategory=person) (objectClass=User) (name=$nom))"

$resultat = ($searcher.findOne()).GetDirectoryEntry()

$login      = $user.sAMAccountName
$prenom     = $user.givenName
$nom        = $user.sn
$nomComplet = $user.displayName

$info = "$login`t$prenom`t$nom`t$nomComplet"
Write-Host $info -ForegroundColor Yellow

$info = "-" * 80
Write-Host $info -ForegroundColor Cyan
```

```
# Code pour rechercher les utilisateurs dont le nom débute par EMP
# et qui sont dans la OU "FORMATION"
# $nom correspond au nom d'ouverture de session
$nom = "EMP*"

# ADSI signifie (Active Directory Service Interfaces)
$root = [ADSI]"LDAP://OU=formation,DC=formation,DC=local"

$searcher = New-Object -TypeName System.DirectoryServices.DirectorySearcher # -ArgumentList ($root)
$searcher.filter = "(&(objectCategory=person) (objectClass=User) (name=$nom))"

$searcher.findall() | ForEach-Object {
    $user = $PSItem.GetDirectoryEntry()

    $login      = $user.sAMAccountName
    $prenom     = $user.givenName
    $nom        = $user.sn
    $nomComplet = $user.displayName

    $info = "$login`t$prenom`t$nom`t$nomComplet"
    Write-Host $info -ForegroundColor Yellow

    $info = "-" * 80
    Write-Host $info -ForegroundColor Cyan
}
```

Pour le cours, il n'est pas nécessaire de comprendre le contenu des annexes 1 et 2.

PowerShell - WMI - CIM

Vous devez exécuter les commandes sur le serveur réel

Objectifs

- Utilisation de **Get-CimInstance** et de **Set-CimInstance** pour utiliser les classes du namespace **ROOT\CIMV2**
- Utiliser les cmdlets Format-Table et Format-List
note: -AutoSize et -Wrap sont deux paramètres du cmdlet Format-Table

Documentation

Computer System Hardware Classes

<https://learn.microsoft.com/en-us/windows/win32/cimwin32prov/computer-system-hardware-classes>

Operating System Classes

<https://learn.microsoft.com/en-us/windows/win32/cimwin32prov/operating-system-classes>

Outils pour explorer les classes WMI

WMI Explorer 2.0.0.2

<https://github.com/vinaypamnani/wmie2>

Les avantages de CIM

- CIM** est basé sur des standards ouverts définis par la DMTF (Distributed Management Task Force).
- Les cmdlets **CIM** utilisent le protocole **WS-Man** (Web Services for Management) pour la communication, qui est plus moderne et sécurisé.

Les désavantages de WMI

- WMI** est spécifique à Windows.
- WMI** utilise **DCOM** (Distributed Component Object Model), qui est plus ancien et peut être plus compliqué à configurer et à sécuriser à travers des pare-feux.

Les classes Win32*

Pour afficher le nom des classes Win32_* en ordre alphabétique.

```
(Get-CimClass -Namespace "root\cimv2" -ClassName "Win32_*") .CimClassName | Sort-Object
```

Pour afficher le nombre de classes Win32_*.

```
(Get-CimClass -Namespace "root\cimv2" -ClassName "Win32_*") .Count
```

Il existe près de huit cents classes Win32 sous "root\cimv2".

Avantage de CimInstance versus WmiObject

```
Utilisation de Win32_OperatingSystem pour afficher la date d'installation du système d'exploitation
# Retourne la date d'installation du système d'exploitation
$rep1 = (Get-WmiObject -Class Win32_OperatingSystem).InstallDate

$rep1 contient "20160910092428.000000-240"
```

```
# Utilisation de Win32_OperatingSystem pour afficher la date d'installation du système d'exploitation
# Retourne la date d'installation du système d'exploitation
$rep2 = (Get-CimInstance -ClassName Win32_OperatingSystem).InstallDate

$rep2 contient "10 septembre 2016 09:24:28"
```

Conclusion: La date est plus facile à lire avec Get-CimInstance.

Exemples avec Win32_OperatingSystem

```
# Voici la commande pour afficher toutes les propriétés de Win32_OperatingSystem
Get-CimInstance -ClassName Win32_OperatingSystem | Select-Object *
```

Voici trois requêtes PowerShell qui permettent de vérifier si le système d'exploitation est 'Microsoft Windows Server 2019 Datacenter' et si la version est '10.0.17763'.

```
Get-CimInstance -ClassName Win32_OperatingSystem | `
    Where-Object { $PSItem.Caption -eq 'Microsoft Windows Server 2019 Datacenter' -and
                  $PSItem.Version -eq '10.0.17763' }

Get-CimInstance -ClassName Win32_OperatingSystem |
    -Filter "(Caption = 'Microsoft Windows Server 2019 Datacenter' and
              Version = '10.0.17763')"

Get-CimInstance -Query "select * from Win32_OperatingSystem ``
    where (Caption = 'Microsoft Windows Server 2019 Datacenter' and
           Version = '10.0.17763')"
```

Exemples avec Win32_OperatingSystem

```
# Voici la commande pour afficher la propriété "Description" de Win32_OperatingSystem
Get-CimInstance -ClassName Win32_OperatingSystem | Select-Object Description
```

Voici trois requêtes PowerShell qui permettent de vérifier la description d'un ordinateur

```
Get-CimInstance -ClassName Win32_OperatingSystem | Where-Object Description -eq "ORDI1"

Get-CimInstance -ClassName Win32_OperatingSystem -Filter "Description ='ORDI1'"

Get-CimInstance -Query "Select * from Win32_OperatingSystem where Description ='ORDI1'"
```

Exemples avec Win32_OperatingSystem

Exemple de l'utilisation de Set-CimInstance avec la classe Win32_OperatingSystem pour modifier la description d'un ordinateur.

```
# Voici quatre requêtes PowerShell qui permettent de modifier la description d'un ordinateur

# EXEMPLE 1
$nom = Get-CimInstance -ClassName Win32_OperatingSystem
$nom.Description = "ORDI1"
Set-CimInstance -CimInstance $nom

# EXEMPLE 2
$nom = Get-CimInstance -ClassName Win32_OperatingSystem
Set-CimInstance -CimInstance $nom -Property @{Description="ORDI2"}

# EXEMPLE 3
Set-CimInstance -Query 'Select * from Win32_OperatingSystem' `

# EXEMPLE 4
Get-CimInstance -ClassName Win32_OperatingSystem | `
    Set-CimInstance -Property @{Description = "ORDI4"}
```

Exemples avec Win32_ComputerSystem

```
# Voici la commande pour afficher toutes les propriétés de Win32_ComputerSystem
Get-CimInstance -ClassName Win32_ComputerSystem | Select-Object *
```

Voici la commande qui affiche

- Le nom de votre ordinateur
- Le nom du domaine ou du groupe de travail
- Le nom de l'utilisateur qui est connecté pour exécuter le test
- L'affichage utilise Format-Table avec le paramètre -AutoSize

```
Get-CimInstance -ClassName Win32_ComputerSystem | `
    Format-Table -AutoSize Caption,Domain,UserName
```

Exemples avec Win32_Group

```
# Voici la commande pour afficher toutes les propriétés de Win32_Group
Get-CimInstance -ClassName Win32_Group | Select-Object *
```

```
# Voici la commande pour afficher le nom et le SID de tous les groupes du serveur réel
```

- L'affichage utilise Format-Table avec le paramètre -AutoSize
- ```
Get-CimInstance -ClassName Win32_Group | `
 Format-Table -AutoSize Name,SID
```

### Exemples avec Win32\_UserAccount

```
Voici la commande pour afficher toutes les propriétés de Win32_UserAccount
Get-CimInstance -ClassName Win32_UserAccount | Select-Object *
```

```
Voici la commande pour afficher le nom et le SID de tous les usagers du serveur réel
```

- L'affichage utilise Format-Table avec le paramètre -AutoSize
- ```
Get-CimInstance -ClassName Win32_UserAccount | `
    Format-Table -AutoSize Name,SID
```

Exemples avec Win32_UserAccount

VERSION 1

NOTE: il n'y a pas de cmdlet pour déverrouiller le compte d'un utilisateur local

Voici le code pour déverrouiller le compte d'un utilisateur local

```
$liste = "ETU", "TEST", "TECH"

$users = Get-CimInstance -ClassName Win32_UserAccount ` 
    -Filter "LocalAccount=True and Lockout=True" | ` 
    Where-Object Name -in $liste

foreach ($user in $users)
{
    # Affiche le nom de l'utilisateur
    $nom = $User.name
    Write-Warning "Nom de l'utilisateur: $nom"

    # Affiche le contenu de la propriété Lockout avant la modification
    $user.Lockout

    # Modification de la propriété Lockout
    $user.Lockout = "False"

    # Affiche le contenu de la propriété Lockout après la modification
    $user.Lockout

    # Mise à jour de l'utilisateur
    Set-CimInstance -CimInstance $user
}
```

VERSION 2

NOTE: il n'y a pas de cmdlet pour déverrouiller le compte d'un utilisateur local

Voici le code pour déverrouiller le compte d'un utilisateur local

```
$liste = "ETU", "TEST", "TECH"

$users = Get-CimInstance -ClassName Win32_UserAccount ` 
    -Filter "LocalAccount=True and Lockout=True" | ` 
    Where-Object Name -in $liste

foreach ($user in $users)
{
    # Mise à jour de l'utilisateur pour déverrouiller son compte
    Set-CimInstance -CimInstance $user ` 
        -Property @{LockOut=$false}

    $nom = $user.name
    Write-Warning "Le compte de l'utilisateur est déverrouillé: $nom"
}
```

Exemples avec Win32_VideoController

Voici la commande pour afficher des informations sur la carte vidéo de votre ordinateur

- Le nom de votre ordinateur
- Le nom du modèle de la carte vidéo
- Le nom du processeur vidéo
- La résolution de l'écran utilisée et le nombre de couleurs
- La quantité de mémoire sur la carte vidéo
- La version du pilote de la carte vidéo

```
Get-CimInstance -ClassName Win32_VideoController | `  
    Select-Object -Property SystemName,  
                  Name,  
                  VideoProcessor,  
                  AdapterRAM,  
                  VideoModeDescription,  
                  CurrentRefreshRate,  
                  MaxRefreshRate,  
                  DriverDate,  
                  DriverVersion | Format-List
```

```
SystemName      : VM70035316  
Name           : NVIDIA Quadro M2000  
VideoProcessor  : Quadro M2000  
AdapterRAM     : 4293918720  
VideoModeDescription : 1680 x 1050 x 4294967296 couleurs  
CurrentRefreshRate : 59  
MaxRefreshRate   : 75  
DriverDate       : 2021-02-22 19:00:00  
DriverVersion     : 27.21.14.6172
```

Exemples avec Win32_Processor

```
# Voici la commande pour afficher toutes les propriétés de Win32_Processor  
Get-CimInstance -ClassName Win32_Processor | Select-Object *
```

Exemples avec Win32_LogicalDisk

Comment afficher la liste des disques locaux présents avec les informations suivantes:

- Leur nom (lettre)
- Leur type
- Leur système de fichier
 - Les lecteurs de disque qui ne contiennent pas de média n'ont pas de système de fichier.
 - Consulter le site <https://learn.microsoft.com/en-us/windows/win32/cimwin32prov/win32-logicaldisk> pour connaître les valeurs de l'attribut DriveType.
- La taille
- L'espace libre
- L'affichage utilise Format-Table avec les paramètres -AutoSize et -Wrap

Voici trois réponses en utilisant trois façons différentes de faire cette requête (where-object, -filter, -query)

```
Get-CimInstance -ClassName Win32_LogicalDisk | Where-Object drivetype -eq 3 | `  
Format-Table -AutoSize -Wrap DeviceID,Description,FileSystem,Size,FreeSpace  
  
Get-CimInstance -ClassName Win32_LogicalDisk -Filter "DriveType = 3" | `  
Format-Table -AutoSize -Wrap DeviceID,Description,FileSystem,Size,FreeSpace  
  
Get-CimInstance -Query "select * from Win32_LogicalDisk where DriveType = 3" | `  
Format-Table -AutoSize -Wrap DeviceID,Description,FileSystem,Size,FreeSpace
```

Exemples avec Win32_Service

Comment afficher la liste des services dont l'état est à "démarrer" avec les informations suivantes:

- Le nom du service
- Le nom complet du service
- Le chemin
- Le mode de démarrage
- L'affichage utilise Format-List

Voici trois réponses en utilisant trois façons différentes de faire cette requête (where-object, -filter, -query)

```
Get-CimInstance -ClassName Win32_Service | Where-Object state -eq "Running" | `  
Format-List name,displayname,pathname,startmode  
  
Get-CimInstance -ClassName Win32_Service -Filter 'state = "running"' | `  
Format-List name,displayname,pathname,startmode  
  
Get-CimInstance -Query 'select * from Win32_Service where state = "running"' | `  
Format-List name,displayname,pathname,startmode
```

Exemples avec Win32_NetworkConnection

Comment afficher le nom et le chemin des disques réseaux présentement connectés

- L'affichage utilise Format-Table avec le paramètre -AutoSize
- ```
Get-CimInstance -ClassName win32_NetworkConnection |
 Format-Table -AutoSize LocalName,RemoteName
```

Comment afficher le nom et le chemin des disques réseaux présentement connectés

- L'affichage utilise Out-GridView
- ```
Get-CimInstance -ClassName win32_NetworkConnection |  
    Select-Object LocalName,RemoteName | Out-GridView
```

Exemples avec Win32_NetworkAdapter

Comment afficher l'index, l'adresse MAC et le nom des cartes réseaux (NetConnectionID).

- Le paramètre MACAddress ne doit pas être nul
- Le paramètre NetConnectionID ne doit pas être nul
- L'affichage utilise Format-Table avec les paramètres -AutoSize et -Wrap

Voici trois réponses en utilisant trois façons différentes de faire cette requête (where-object, -filter, -query)

```
Get-CimInstance -ClassName Win32_NetworkAdapter |  
    Where-Object { $PSItem.MACAddress -ne $null -and  
        $PSItem.NetConnectionID -ne $null } |  
    Format-Table -AutoSize -Wrap Index,MACAddress,NetConnectionID  
  
Get-CimInstance -ClassName Win32_NetworkAdapter |  
    -Filter "MACAddress is not null and NetConnectionID is not null" |  
    Format-Table -AutoSize -Wrap Index,MACAddress,NetConnectionID  
  
Get-CimInstance -Query "select * from Win32_NetworkAdapter |  
    where MACAddress is not null and NetConnectionID is not null" |  
    Format-Table -AutoSize -Wrap Index,MACAddress,NetConnectionID
```

Exemples avec Win32_NetworkAdapterConfiguration

Comment afficher l'index, la description des cartes réseaux, l'adresse MAC, l'adresse IP, le masque de sous-réseau, la passerelle, les adresses des serveurs DNS

- Le paramètre MACAddress ne doit pas être nul
- Le paramètre Description net doit pas être nul
- L'affichage utilise Format-List

Voici trois réponses en utilisant trois façons différentes de faire cette requête (where-object, -filter, -query)

```
Get-CimInstance -ClassName Win32_NetworkAdapterConfiguration |  
    Where-Object { $PSItem.MACAddress -ne $null -and  
        $PSItem.Description -ne $null } |  
    Format-List Index,Description,MACAddress,IPAddress,IPSubnet,  
        DefaultIPGateway,DNSServerSearchOrder  
  
Get-CimInstance -ClassName Win32_NetworkAdapterConfiguration |  
    -Filter "MACAddress is not null and Description is not null" |  
    Format-List Index,Description,MACAddress,IPAddress,IPSubnet,  
        DefaultIPGateway,DNSServerSearchOrder  
  
Get-CimInstance -Query "select * from Win32_NetworkAdapterConfiguration |  
    where MACAddress is not null and Description is not null" |  
    Format-List Index,Description,MACAddress,IPAddress,IPSubnet,  
        DefaultIPGateway,DNSServerSearchOrder
```

Exemples avec Win32_BIOS

Les propriétés de **Win32_BIOS** sont en lecture seulement.

```
Clear-Host
$computer = $env:COMPUTERNAME
$namespace = "ROOT\CIMV2"
$classname = "Win32_BIOS"

Write-Output "===="
Write-Output "Computer : $computer"
Write-Output "NameSpace : $namespace"
Write-Output "ClassName : $classname"
Write-Output "===="

Get-CimInstance -Namespace $namespace -ClassName $classname
```

ANNEXE 1
Modules PowerShell pour modifier les propriétés du BIOS

La compagnie "Hewlett Packard Enterprise" offre le module PowerShell "HPEBIOSCmdlets 4.0.0.0" pour administrer le BIOS/UEFI des serveurs.

<https://www.powershellgallery.com/packages/HPEBIOSCmdlets>

HPEBIOSCmdlets 4.0.0.0

Scripting Tools for Windows PowerShell : BIOS Cmdlets creates an interface to HPE BIOS ROM-Based Setup Utility (RBSU) or UEFI System Utilities. These cmdlets can be used to configure the BIOS settings on HPE ProLiant servers.

Le module "**HPEBIOSCmdlets**" est offert avec des scripts pour faciliter la gestion du BIOS/UEFI.

- ConfigureAdminInfo.ps1
- ConfigureAMDCorePerformanceBoosting.ps1
- ConfigureBIOSAdminPassword.ps1
- ConfigureBootMode.ps1
- ConfigureBootOrder.ps1
- ConfigureEMSConsoleAndSerialPort.ps1
- ConfigureIntelCoreBoosting.ps1
- ConfigureIntelTurboBoost.ps1
- ConfigureNetworkBootsettings.ps1
- ConfigureNVDIMMConfiguration.ps1
- ConfigurePCIDeviceWithPCIeLinkSpeedForGen10.ps1
- ConfigurePowerOnPassword.ps1
- ConfigureProcessorJitterControl.ps1
- ConfigureProcessorPower.ps1
- ConfigureServerAvailability.ps1
- ConfigureServerSecurity.ps1
- ConfigureThermalAndFanOption.ps1
- ConfigureTPM.ps1
- ConfigureUEFIOptimizedBoot.ps1
- ConfigureVirtualInstallDisk.ps1
- ConfigureWorkloadProfileForGen10servers.ps1
- ResetBIOSAdminPassword.ps1
- ResetBIOSDefaultManufacturingSettings.ps1
- ResetPowerOnPassword.ps1

La compagnie DELL offre le module PowerShell "DellBIOSProvider 2.8.0" pour administrer le BIOS des ordinateurs Dell Optiplex, Latitude, Precision, XPS Notebook et Venue 11.

<https://www.powershellgallery.com/packages/DellBIOSProvider>

DellBIOSProvider 2.8.0

The 'Dell Command | PowerShell Provider' provides native configuration capability of Dell Optiplex, Latitude, Precision, XPS Notebook and Venue 11 systems within PowerShell.

ANNEXE 2
Exemples pour trouver la valeur UUID du BIOS

Voici le code pour afficher la valeur UUID du BIOS de chaque ordinateur virtuel.

Le code doit s'exécuter sur le serveur réel.

Le code affiche le BiosGUID même si l'ordinateur virtuel n'est pas démarré.

Clear-Host

```
$VMNames = (Get-VM).Name

ForEach ($VMName in $VMNames)
{
    Get-CimInstance -Namespace Root\Virtualization\V2 ` 
        -ClassName Msvm_VirtualSystemSettingData ` 
        -Filter "ElementName = '$VMName'" ` 
        | Select-Object ElementName,BiosGUID
}
```

Le code doit s'exécuter dans un ordinateur virtuel.

La valeur de UUID est identique à la valeur BiosGUID.

Clear-Host

```
$computerSystemProduct = Get-CimInstance -Namespace root\cimv2 ` 
    -ClassName Win32_ComputerSystemProduct | Select-Object *

$computersrSystemProduct.UUID
```

Introduction à PowerShell

Objectifs

- Explorer les environnements de programmation de PowerShell
- Maîtriser les cmdlets de bases

PowerShell Documentation
PowerShell Gallery

<https://learn.microsoft.com/en-us/powershell>
<https://www.powershellgallery.com>

Mise en place

Je vous conseille de créer un raccourci sur la barre des tâches, en exécution "administrateur" pour la console

- PowerShell ISE (Attention: choisir la version 64 bits)

Informations sur PowerShell

"Windows 10", "Windows 11", "Windows Server 2016", "Windows Server 2019" et "Windows Server 2022" utilise "Windows PowerShell version 5.1".

"PowerShell 7.4.4" ne remplace pas "Windows PowerShell version 5.1".

"PowerShell 7.4.4" s'installe en parallèle à "Windows PowerShell version 5.1".

"PowerShell 7.4.4" peut s'installer sur Windows, Linux et OSX

- Windows (x64), Windows (x86)
- Debian, Red Hat
- OSX

"PowerShell 7.4.4" est la plus récente version de PowerShell.

"PowerShell 7.4.4" est disponible depuis le 2024-07-18.

"PowerShell 7.4.4" est basé sur ".NET 8 version 8.0.303".

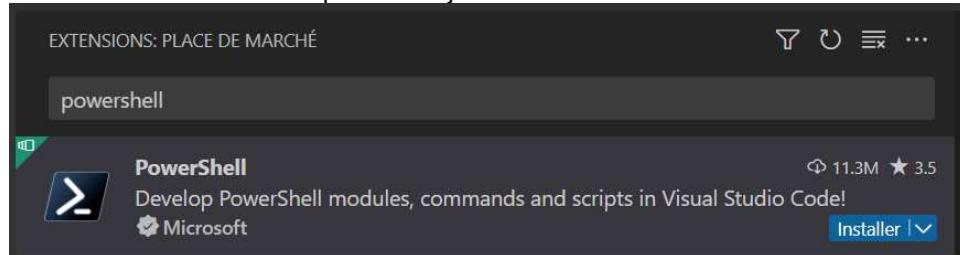
Le code source de "PowerShell 7.4.4" est disponible.

"PowerShell" est programmé en C#.

<https://github.com/PowerShell/PowerShell/tags>

Pour utiliser PowerShell avec "Visual Studio Code", vous devez ajouter l'extension "PowerShell".

Le raccourci **Ctrl+Shift+X** permet d'ajouter des extensions.



Modules supplémentaires

Il existe des modules supplémentaires pour gérer les ressources qui sont sur "**Microsoft Azure**".

Microsoft Azure PowerShell

<https://www.powershellgallery.com/packages/Az>

Pour gérer les ressources qui sont sur "**Microsoft Azure**" vous devez avoir un compte Azure.

Le module Az.Accounts contient deux cmdlets pour se connecter ou se déconnecter.

```
(Get-Command -Name *connect* -Module Az.Accounts) .Name  
Connect-AzAccount  
Disconnect-AzAccount
```

Voici la liste des cmdlets que vous pouvez utiliser pour gérer les machines virtuelles sur Azure.

```
(Get-Command -Module Az.Compute -Name *AzVm) .Name  
Get-AzVm  
New-AzVm  
Remove-AzVm  
Restart-AzVm  
Set-AzVm  
Start-AzVm  
Stop-AzVm  
Update-AzVm
```

Il existe des modules supplémentaires pour gérer les ressources qui sont sur "**Amazon Web Services**".

Outils AWS pour PowerShell

<https://aws.amazon.com/fr/powershell>

<https://www.powershellgallery.com/packages/AWSPowerShell>

Il existe des modules supplémentaires pour gérer les ressources des serveurs **ESXi** et **vCenter**.

VMware PowerCLI

<https://www.powershellgallery.com/packages/VMware.PowerCLI>

Il existe des modules supplémentaires pour gérer les autorisations NTFS.

NTFSSecurity

<https://www.powershellgallery.com/packages/NTFSSecurity>

Le site "PowerShell Gallery" contient plusieurs milliers de modules.

Introduction à PowerShell

La programmation avec PowerShell permet de manipuler des objets du système d'exploitation.

cmdlet (commandlet)

Un cmdlet est une commande fournie par PowerShell.

Les cmdlets sont écrits en C# ou en VB.NET et sont inclus dans les modules PowerShell.

function

Une fonction PowerShell est une commande personnalisée créée par un utilisateur.

Les fonctions sont écrites en PowerShell.

alias

Un alias est un raccourci vers un cmdlet ou une fonction.

Pour afficher la liste des cmdlet.

`Get-Command - CommandType cmdlet`

Pour afficher le nombre de cmdlet.

`(Get-Command - CommandType cmdlet).Count`

Pour afficher la liste des cmdlet qui sont dans un module particulier

`Get-Command - Module Hyper-V - CommandType cmdlet`

Pour afficher le nom du module qui contient le cmdlet **Get-VM**

`(Get-Command - Name Get-VM).ModuleName`

Pour afficher la liste des cmdlets qui contiennent **vm**

`Get-Command - Name *vm* - CommandType Cmdlet`

Pour afficher la liste des fonctions qui contiennent **vm**

`Get-Command - Name *vm* - CommandType Function`

Pour afficher la liste des alias qui contiennent **vm**

`Get-Command - Name *vm* - CommandType Alias`

Un cmdlet est constitué d'un verbe (VERB) suivi d'un nom (NOUN).

Pour afficher la liste des verbes utilisés par Windows PowerShell
Get-Verb

Pour afficher la liste des cmdlets, fonctions et alias si le verbe est **convert**
Get-Command -Verb convert

Pour afficher la liste des cmdlets, fonctions et alias si le verbe débute par **convert**
Get-Command -Verb convert*

Pour afficher la liste des cmdlets, fonctions et alias qui contiennent le nom **vm**
Get-Command -Noun *vm*

Pour trouver la relation entre l'alias **ls** et son raccourci
Get-Command -Name ls | Select-Object Name,ResolvedCommandName

Effectuer des calculs avec PowerShell

```
3 + 2          # le résultat est 5
3 - 2          # le résultat est 1
3 * 2          # le résultat est 6
3 / 2          # le résultat est 1.5
2 / 3          # le résultat est 0,6666666666666667
5%4           # le résultat est 1
              # % est l'opérateur MODULO qui calcule le reste de la division

"-" * 80        # affiche 80 tirets

1kb            # affiche 1024
1mb            # affiche 1048576
1gb            # affiche 1073741824
1tb            # affiche 1099511627776
1pb            # affiche 1125899906842624

1gb / 1mb      # le résultat est 1024
1tb / 1gb      # le résultat est 1024
1pb / 1gb      # le résultat est 1048576
2gb * 5        # le résultat est 10737418240

0xffff         # affiche 65535
16 + 0x10      # le résultat est 32
```

Utilisation du cmdlet Get-Help

Dans PowerShell, on peut afficher de l'aide sur plus d'une centaine de sujets.

La commande suivante permet d'afficher la liste complète des sujets:

```
Get-Help -Name about
```

```
# Commande pour afficher en ordre alphabétique la liste complète des sujets
$info = (Get-Help -Name about).Name | Sort-Object -Unique
$info
"-" * 80
$total = $info.Count
Write-Host "Nombre de sujet = $total" -ForegroundColor Yellow
"-" * 80
```

Voici une liste de plusieurs sujets intéressants:

```
about_Arithmetic_Operators
about_Assignment_Operators
about_Comparison_Operators
about_Logical_Operators
about_Operator_Precedence
about_Operators
about_Type_Operators

about_Do
about_For
about_Foreach
about_If
about_Switch
about_While

about_Arrays
about_Functions
about_Functions_Advanced
about_Functions_Advanced_Methods
about_Functions_Advanced_Parameters
about_Functions_CmdletBindingAttribute
about_Functions_OutputTypeAttribute
about_Hash_Tables
about_Ref
about-Regular_Expressions
about_Scopes
about_Script_Blocks
about_Scripts
about_Try_Catch_Finally
about_Variables
```

Utilisation de plusieurs paramètres de Get-Help

Ces exemples affichent des informations d'aide plus détaillées du cmdlet **Format-Table**.

```
Get-Help -Name Format-Table -Detailed  
Get-Help -Name Format-Table -Full
```

Ces exemples affichent les parties sélectionnées du cmdlet **Format-Table**.

```
Get-Help -Name Format-Table -Examples  
Get-Help -Name Format-Table -Parameter *  
Get-Help -Name Format-Table -Parameter AutoSize
```

Cet exemple montre comment afficher la version en ligne de l'article d'aide du cmdlet **Format-Table** dans votre navigateur web par défaut.

```
Get-Help -Name Format-Table -Online
```

Mise à jour de l'aide dans PowerShell

L'aide de PowerShell est disponible ou sera téléchargée au besoin.

Le cmdlet "**update-help**" permet d'effectuer la mise à jour de l'aide à condition d'avoir une connexion internet. La mise à jour de l'aide peut prendre un certain temps.

Cette commande force la mise à jour de l'aide pour PowerShell.

```
Update-help -Force
```

Utilisation des ALIAS

Un alias remplace le nom d'un cmdlet par un nom très court.

Le cmdlet "**Get-Alias**" permet d'afficher les alias.

Il n'est pas recommandé d'utiliser les alias dans des scripts parce qu'ils peuvent porter à confusion.

Les alias peuvent être difficiles à comprendre en particulier pour les programmeurs débutants.

Le code est plus difficile à maintenir en particulier pour un autre programmeur que l'auteur du script.

Exemple d'alias facile à comprendre

```
clear      Clear-Host  
cp        Copy-Item
```

Plusieurs alias pour le même cmdlet

```
cd        Set-Location  
chdir    Set-Location  
copy     Copy-Item  
cp       Copy-Item  
cpi      Copy-Item
```

Exemple d'alias difficile à comprendre

```
%       ForEach-Object  
?       Where-Object
```

Introduction à la programmation PowerShell

Les opérateurs arithmétiques

Get-Help -Name about_Arithmetic_Operators

PowerShell supports the following arithmetic operators:

Operator	Description	Example
+	Adds integers; concatenates strings, arrays, and hash tables.	6 + 2 "file" + "name" @(1, "one") + @(2.0, "two") @{"one" = 1} + @{"two" = 2}
-	Subtracts one value from another value	6 - 2
-	Makes a number a negative number	-6
*	Multiply numbers or copy strings and arrays the specified number of times.	(Get-Date).AddDays(-1) 6 * 2 @("!") * 4 "!" * 3
/	Divides two values.	6 / 2
%	Modulus - returns the remainder of a division operation.	7 % 2
-band	Bitwise AND	5 -band 3
-bnot	Bitwise NOT	-bnot 5
-bor	Bitwise OR	5 -bor 0x03
-bxor	Bitwise XOR	5 -bxor 3
-shl	Shifts bits to the left the specified number of times	102 -shl 2
-shr	Shifts bits to the right	102 -shr 2

The bitwise operators only work on integer types.

OPERATOR PRECEDENCE

PowerShell processes arithmetic operators in the following order:

Precedence	Operator	Description
1	()	Parentheses
2	-	For a negative number or unary operator
3	*, /, %	For multiplication and division
4	+, -	For addition and subtraction

PowerShell processes the expressions from left to right according to the precedence rules. The following examples show the effect of the precedence rules:

Expression	Result
3+6/3*4	11
3+6/(3*4)	3.5
(3+6)/3*4	12

Les opérateurs de comparaison

Get-Help -Name about_Comparison_Operators

Powershell includes the following comparison operators:

Type	Operators	Description
Equality	-eq -ne -gt -ge -lt -le	equals not equals greater than greater than or equal less than less than or equal
Matching	-like -notlike -match -notmatch	Returns true when string matches wildcard pattern Returns true when string does not match wildcard pattern Returns true when string matches regex pattern; \$matches contains matching strings Returns true when string does not match regex pattern; \$matches contains matching strings
Containment	-contains -notcontains -in -notin	Returns true when reference value contained in a collection Returns true when reference value not contained in a collection Returns true when test value contained in a collection Returns true when test value not contained in a collection
Replacement	-replace	Replaces a string pattern
Type	-is -isnot	Returns true if both object are the same type Returns true if the objects are not the same type

Les opérateurs logiques

Get-Help -Name about_Logical_Operators

PowerShell supports the following logical operators.

Operator	Description	Example
-and	Logical AND. TRUE when both statements are TRUE.	(1 -eq 1) -and (1 -eq 2) False
-or	Logical OR. TRUE when either statement is TRUE.	(1 -eq 1) -or (1 -eq 2) True
-xor	Logical EXCLUSIVE OR. TRUE when only one statement is TRUE	(1 -eq 1) -xor (2 -eq 2) False
-not	Logical not. Negates the statement that follows.	-not (1 -eq 1) False
!	Same as -not	!(1 -eq 1) False

Voici les commandes pour obtenir de l'aide sur les instructions:

- IF Get-Help -Name about_if
- FOR Get-Help -Name about_for
- FOREACH Get-Help -Name about_foreach
- SWITCH Get-Help -Name about_switch
- WHILE Get-Help -Name about_while

L'opérateur IF est utilisé pour tester des conditions

```
if ($a -gt 2)
{
    Write-Host "La valeur $a est plus grande que 2."
}

if ($a -gt 2)
{
    Write-Host "La valeur $a est plus grande que 2."
}
else
{
    Write-Host ("La valeur $a est plus petite ou égale à 2," +
               " ou n'existe pas ou n'est pas initialisée.")
}

if ($a -gt 2)
{
    Write-Host "La valeur $a est plus grande que 2."
}
elseif ($a -eq 2)
{
    Write-Host "La valeur $a est égale à 2."
}
else
{
    Write-Host ("La valeur $a est plus petite que 2," +
               " ou n'existe pas ou n'est pas initialisée.")
}
```

L'opérateur FOR est utilisé pour effectuer une boucle

Une boucle FOR s'exécute en utilisant une valeur de départ, un test et un incrément.

```
# La boucle s'exécute 10 fois et affiche les valeurs 1,2,3,4,5,6,7,8,9,10
```

```
for($i=1; $i -le 10; $i++)  
{  
    Write-Host $i  
}
```

```
# La boucle s'exécute 10 fois et affiche les valeurs 10,9,8,7,6,5,4,3,2,1
```

```
for($i=10; $i -ge 1; $i--)  
{  
    Write-Host $i  
}
```

L'opérateur FOREACH est utilisé pour parcourir tous les éléments d'une collection

Une boucle FOREACH exécute une itération à partir des valeurs d'une collection.

```
$lettres = "a", "b", "c", "d"  
  
foreach ($lettre in $lettres)  
{  
    Write-Host $lettre  
}
```

L'opérateur SWITCH est utilisé pour évaluer une expression

```
$i = 3  
switch ($i)  
{  
    1 {"La valeur est un."}  
    2 {"La valeur est deux."}  
    3 {"La valeur est trois."}  
    4 {"La valeur est quatre."}  
}  
La valeur est trois.
```

```
$i = 3  
switch ($i)  
{  
    1 {"La valeur est un."}  
    2 {"La valeur est deux."}  
    3 {"La valeur est trois."}  
    4 {"La valeur est quatre."}  
    3 {"Encore trois."}  
}  
La valeur est trois.  
Encore trois.
```

```
# Break permet d'arrêter immédiatement
$i = 3
switch ($i)
{
    1 {"La valeur est un."}
    2 {"La valeur est deux."}
    3 {"La valeur est trois."; Break}
    4 {"La valeur est quatre."}
    5 {"Encore trois."}
}
La valeur est trois.
```

```
# La commande SWITCH teste deux valeurs
switch (4,2)
{
    1 {"La valeur est un."}
    2 {"La valeur est deux."}
    3 {"La valeur est trois."; Break}
    4 {"La valeur est quatre."}
    5 {"Encore trois."}
}
La valeur est quatre.
La valeur est deux.
```

```
# Default est utilisé si aucun teste fonctionne
$i = 5
switch ($i)
{
    1 {"La valeur est un."; Break }
    2 {"La valeur est deux."; Break }
    3 {"La valeur est trois."; Break}
    4 {"La valeur est quatre."; Break }
    Default {"Aucune valeur."}
}
Aucune valeur.
```

```
# La commande switch permet d'utiliser des tests pour valider une valeur
$heure = $(Get-Date).hour
switch ($heure)
{
    { $heure -ge 0 -and $heure -lt 8 } { Write-Host "Nous sommes la nuit." }
    { $heure -ge 8 -and $heure -lt 18 } { Write-Host "Nous sommes le jour." }
    { $heure -ge 18 -and $heure -lt 24 } { Write-Host "Nous sommes le soir." }
}
```

L'opérateur WHILE est utilisé pour effectuer une boucle

Il ne faut pas oublier d'incrémenter la valeur de la variable dans la boucle WHILE.

```
$val =1
while($val -le 3)
{
    Write-Host $val
    $val++
}
```

Les variables

Une variable débute avec \$

- 1) Une variable peut contenir le résultat d'une commande Windows

```
$resultat = ping 10.57.22.100  
$resultat
```

- 2) Une variable peut contenir les propriétés d'un objet.

```
$col = Get-CimInstance -ClassName win32_processor  
$col  
$col.NumberOfCores  
$col.NumberOfLogicalProcessors
```

- 3) Normalement, une variable est en mémoire mais PowerShell permet qu'une variable soit un fichier.

```
 ${C:\Temp\Test.txt} = "Test pour écrire dans un fichier."  
 ${C:\Temp\Test.txt} += "`n" + "Ligne 2 !!!"
```

Pour afficher la liste des variables d'environnement

- Get-ChildItem env:

Pour afficher le contenu d'une variable d'environnement

On doit ajouter \$env: devant le nom de la variable d'environnement de Windows

- \$env:computername

Pour afficher la liste des variables

- Get-Variable

Pour créer une nouvelle variable, variable en lecture seule ou constante

- New-Variable -Name pi -Value ([system.math]::Pi) -Option Constant

Pour effacer le contenu d'une variable

- Clear-Variable -Name resultat

Pour supprimer une variable et son contenu

- Remove-Variable -Name resultat

La variable \$?

Le contenu de la variable \$? indique si l'exécution de la dernière commande a réussie ou échouée.

Les variables booléennes

- \$true
- \$false

Concaténation des chaînes de caractères

Guillemet simple

La substitution de la variable \$nombre ne fonctionne pas

```
$nombre = 5
```

```
'Nombre = $nombre'  
résultat: Nombre = $nombre
```

Guillemet double

La substitution de la variable \$nombre fonctionne

```
$nombre = 5
```

```
"Nombre = $nombre"  
résultat: Nombre = 5
```

L'opérateur + permet de concaténer des chaînes de caractères

```
$c = 'abc' + 'xyz'  
$c  
résultat: abcxyz
```

L'opérateur + permet de concaténer des variables

```
$c1 = 'abc'  
$c2 = 'xyz'  
  
$c3 = $c1 + $c2  
$c3  
résultat: abcxyz
```

Les tableaux

Un tableau contient plusieurs valeurs.
Chaque valeur est séparée par une virgule.

```
$data = @()                                # déclaration d'un tableau vide
$stab1 = @(1,2,3,4,5,6,7,8,9,10)          # un tableau qui contient 10 valeurs
$stab1 = 1,2,3,4,5,6,7,8,9,10              # autre syntaxe pour un tableau

$stab2 = @("python", "rust", "C++")        # un tableau qui contient 10 valeurs
$stab2 = "python", "rust", "C++"            # autre syntaxe pour un tableau

$stab3 = @(1..10)                          # l'opérateur .. permet de générer plusieurs valeurs
$stab3 = 1..10                             # autre syntaxe pour un tableau
```

Manipuler un tableau

Le premier élément d'un tableau commence à la position d'index [0].

```
$stab1[0]                                  # affiche le premier élément du tableau $stab1
$stab1[4]                                  # affiche le cinquième élément du tableau $stab1
$stab1[-1]                                 # affiche le dernier élément du tableau $stab1
$stab1[-4..-1]                            # affiche les quatre derniers éléments du tableau $stab1

Get-Member -InputObject $stab1             # affiche les méthodes disponibles pour le tableau $stab1

$stab1.SetValue(500,5)                    # change la valeur de l'index 5
                                           # le nouveau contenu de $stab1 est 1,2,3,4,5,500,7,8,9,10

$stab1[5]=6                               # le nouveau contenu de $stab1 est 1,2,3,4,5,6,7,8,9,10

$stab1.Contains(5)                        # vérifie si la valeur 5 est présente dans le tableau
$stab1

$stab1.Length                             # affiche le nombre de valeurs dans le tableau $stab1

$stab2 += "Android"                      # ajout d'un élément dans le tableau $stab2
                                           # $stab2 contient "python", "rust", "C++", "Android"
```

Table de hachage (hash table)

Une table de hachage est une structure de données qui consiste à associer des paires [clé = valeur]. Il est important de savoir que l'ordre d'affichage des éléments ne correspond pas à celui de la définition de la table de hachage.

Déclaration d'une table de hachage sur une ligne

```
$var = @{ "cd"="ordi1";"routeur"="ordi6" }  
$var.cd  
$var.routeur
```

Déclaration d'une table de hachage sur plusieurs lignes

```
$var2 = @{ "cd"="ordi1"  
          "routeur"="ordi6" }  
$var2.cd  
$var2.routeur
```

Trier une table de hachage

```
$hash = @{a = 1; b = 2; c = 3; d = 4; e = 5; f = 6}  
  
foreach ($h in $hash.GetEnumerator() | Sort-Object Key)  
{  
    Write-Host "Nom= $($h.Key) Valeur= $($h.Value)" -ForegroundColor Green  
}
```

Créer une table de hachage en forçant le respect de l'ordre

```
$hash = [ordered]@{a = 1; b = 2; c = 3; d = 4; e = 5; f = 6}  
  
foreach ($h in $hash.GetEnumerator())  
{  
    Write-Host "Nom= $($h.Key) Valeur= $($h.Value)" -ForegroundColor Green  
}
```

GetEnumerator()	# permet de récupérer chaque combinaison clé/valeur
\$hash.keys	# liste les clés de la table de hachage \$hash
\$hash.values	# liste les valeurs de la table de hachage \$hash
\$hash.a	# récupère la valeur de la clé "a"
\$hash["a"]	# récupère la valeur de la clé "a"
\$hash["a","d"]	# récupère la valeur de la clé "a" et de la clé "d"
Get-Member -InputObject \$hash	# affiche les méthodes disponibles pour la table de hachage \$hash
\$hash.Add("g",7)	# ajoute une paire à la table de hachage \$hash
\$hash.Remove("a")	# supprime une paire à la table de hachage \$hash
\$hash.Clear()	# efface le contenu
\$ageList = @{}	# création d'une "Hast Table" vide ou efface le contenu

Exemples

Voici une table de hachage qui contient plusieurs variables.

```
$messages = @{
    # Les erreurs pour la variable "PATHS".
    MSG_CHECKING_PATHS = "Checking paths..."
    MSG_COMPUTING_PATHS = "Computing paths..."
    MSG_CREATING_PATHS = "Creating paths..."

    # Les erreurs pour la variable "IMAGE".
    MSG COPYING IMAGE = "Copying image..."
    MSG_MOUNTING_IMAGE = "Mounting image..."
    MSG_CONVERTING_IMAGE = "Converting image..."
    MSG_SKIPPING_IMAGE_CONVERSION = "Skipping image conversion..."
}
```

Voici deux exemples qui affichent des messages qui sont dans la table de hachage

```
Write-Host $messages.MSG_CHECKING_PATHS
Write-Host $messages.MSG_MOUNTING_IMAGE
```

Utilisation d'une table de hachage pour initialiser les paramètres d'un cmdlet

Exemple 1 – les paramètres sont sur une ligne

```
$params = @{
    Name = "TEMP"; Path = "E:\_TEMP"; Description = "test ..."; FullAccess = "Tout le monde" }
New-SmbShare @params
```

Exemple 2 – les paramètres sont sur plusieurs lignes

```
$params = @{
    Name      = "TEMP"
    Path      = "E:\_TEMP"
    Description = "test ..."
    FullAccess = "Tout le monde"
}
New-SmbShare @params
```

Exemple 3 – permet de mettre un paramètre en commentaire

```
$params = @{
    Name      = "TEMP"
    Path      = "E:\_TEMP"
    # Description = "test ..."
    FullAccess = "Tout le monde"
}
New-SmbShare @params
```

Pour utiliser **Sort-Object** avec plusieurs paramètres, il faut utiliser une table de hachage par paramètre pour trier par ordre croissant, décroissant, ou une combinaison d'ordres de tri.

```
Get-Service | Sort-Object -Property @{
    Expression = "Status"; Descending = $true},
    @{
        Expression = "DisplayName"; Ascending = $true}
```

L'utilisation de la variable \$PSItem lorsqu'on utilise un "PIPE"

note: "PowerShell 3.0" remplace \$_ par \$PSItem

PSItem contient la valeur courante d'une commande "PIPE".

Syntaxe avant "PowerShell 3.0"

```
Get-Service | Where-Object { $_.Status -eq "Stopped" }
```

Syntaxe standard avec "PowerShell 3.0"

```
Get-Service | Where-Object { $PSItem.Status -eq "Stopped" }
```

Si on utilise un seul paramètre, on peut utiliser la syntaxe simplifiée

```
Get-Service | Where-Object Status -eq "Stopped"
```

Si on utilise deux paramètres, on ne peut pas utiliser la syntaxe simplifiée

```
Get-Service | Where-Object `n{ $PSItem.Status -eq "Stopped" -and $PSItem.DisplayName -like "*Windows*" }
```

Exemple intéressant

La variable \$serveurs va contenir: HV01,HV02,HV03,HV04,HV05,HV06,HV07,HV08,HV09,HV10

```
$serveurs = 1..10 | ForEach-Object { "HV{0:D2}" -f $PSItem }
```

Write-Output permet à d'autres cmdlets de capturer et de traiter cette sortie

Avec Write-Output, le contenu du fichier output.txt ne sera pas vide.

```
$messages = "Cours", "C53"
```

```
$messages | ForEach-Object { Write-Output $PSItem } | Out-File -FilePath output.txt
```

Write-Host ne permet pas à d'autres cmdlets de capturer et de traiter cette sortie

Avec Write-Host, le contenu du fichier output.txt sera vide.

```
$messages = "Cours", "C53"
```

```
$messages | ForEach-Object { Write-Host $PSItem } | Out-File -FilePath output.txt
```

Out-Host force l'affichage du résultat à l'écran

Lors de l'exécution de plusieurs commandes, il arrive que le résultat des deux commandes soit fusionné.
Les deux commandes affichent deux colonnes avec exactement les mêmes noms.

```
Get-LocalUser -Name Administrateur | Select-Object Name, SID  
Get-LocalGroup -Name Administrateurs | Select-Object Name, SID
```

Name	SID
---	---
Administrateur	S-1-5-21-2975316056-3426304165-532087291-500
Administrateurs	S-1-5-32-544

Le résultat des deux commandes est simplement les deux colonnes Name et SID.

```
Get-LocalUser -Name Administrateur | Select-Object Name, SID | Out-Host  
Get-LocalGroup -Name Administrateurs | Select-Object Name, SID
```

Name	SID
---	---
Administrateur	S-1-5-21-2975316056-3426304165-532087291-500
Name	SID
---	---
Administrateurs	S-1-5-32-544

Out-Host force l'affichage du résultat de la première commande.

Le résultat de la deuxième commande s'affiche à la suite du résultat de la première commande.

Exemple de code

Voici le code qui affiche le nom de la carte réseau et sa vitesse de transmission.
note: le nom de la carte réseau doit être le même sur chaque serveur

```
Clear-Host

$carte = "Ethernet"

# La variable $serveurs va contenir: HV01,HV02,HV03,HV04,HV05,HV06,HV07,HV08,HV09,HV10
$serveurs = 1..10 | ForEach-Object { "HV{0:D2}" -f $PSItem }

foreach ($serveur in $serveurs)
{
    Write-Host $serveur -ForegroundColor Yellow

    Get-NetAdapter -Name $carte -CimSession $serveur | Format-Table Name,LinkSpeed
    "-"*100
}
```

Détails sur les boucles

```
1..10 | ForEach-Object { "HV{0:D2}" -f $PSItem }

# Dans cet exemple ForEach est l'alias de ForEach-Object
1..10 | ForEach { "HV{0:D2}" -f $PSItem }

# Dans cet exemple, foreach est une méthode de la collection
(1..10).foreach({"HV{0:D2}" -f $PSItem})
```

Exemple de code

Voici le code qui affiche la liste complète des fonctions, cmdlet, alias de tous les modules disponibles.

```
Clear-Host

$modules = (Get-Module -ListAvailable).Name

foreach ($module in $modules)
{
    Write-Host "Nom du module: $module" -ForegroundColor Green

    Get-Command -All -Module $module

    "*" * 80
}
```

Utilisation d'un workflow et d'une boucle FOREACH et du paramètre -Parallel

Ce script envoie la commande Restart-Computer en parallèle aux ordinateurs.

Ce script n'est pas ralenti par le fait qu'il peut y avoir des ordinateurs qui sont fermés.

```
# La variable $computers va contenir les noms 407P01 à 407P32
$computers = 1..32 | ForEach-Object { "407P{0:D2}" -f $PSItem }

Workflow Restart-AllComputers
{
    param([string[]]$Computers)

    ForEach-Object -Parallel ($computer in $computers)
    {
        Restart-Computer -PSCoMPuterName $computer -Force -Verbose
    }
}

Restart-AllComputers -Computers $computers
```

IMPORTANT: On ne peut pas prédire l'ordre des résultats lorsqu'on exécute des tâches en parallèles.

Comment afficher le nom de l'ordinateur

Il existe plusieurs manières d'afficher le nom de l'ordinateur.

Méthode 1: utilisation de hostname.exe

```
hostname.exe
```

Méthode 2: utilisation de la variable d'environnement

```
$env:COMPUTERNAME
```

Méthode 3: utilisation d'un objet WMI

```
(Get-WMIObject Win32_ComputerSystem).Name
```

Méthode 4: utilisation d'une instance CIM

```
(Get-CIMInstance CIM_ComputerSystem).Name
```

Méthode 5: utilisation d'une méthode ".Net Framework"

```
[system.environment]::MachineName
```

Méthode 6: utilisation d'une méthode ".Net Framework"

```
[system.net.dns]::GetHostName()
```

Méthode 7: utilisation du cmdlet Get-ComputerInfo

```
(Get-ComputerInfo).CsName
```

Comment trouver la méthode la plus rapide

Le cmdlet Measure-Command permet de mesurer la vitesse d'exécution d'une commande.

exemple: Measure-Command { hostname.exe }

La propriété TotalMilliseconds permet de comparer facilement la vitesse d'exécution d'une méthode par rapport à une autre.

Le cmdlet Measure-Object permet d'effectuer des calculs comme la moyenne

exemple:

```
1..100 | Foreach-Object { Measure-Command { hostname.exe } } | Measure-Object -Average TotalMilliseconds
```

On exécute 100 fois le cmdlet Measure-Command et le cmdlet Measure-Object calcule la moyenne de la propriété "TotalMilliseconds".

Effectuons des tests pour déterminer la différence dans le temps d'exécution.

```
Clear-Host
```

```
# IMPORTANT: on ne doit pas utiliser des variables qui contiennent les commandes
# Foreach-Object possède deux alias: foreach et %
# Les tests vont du plus rapide au plus lent.

1..100 | % {Measure-Command {[system.environment]::MachineName}} | ` 
    Measure-Object -Average TotalMilliseconds
0,008832 ms

1..100 | % {Measure-Command {$env:computername}} | ` 
    Measure-Object -Average TotalMilliseconds
0,024194 ms

1..100 | % {Measure-Command {[system.net.dns]::GetHostName()}} | ` 
    Measure-Object -Average TotalMilliseconds
0,047328 ms

1..100 | % {Measure-Command {(Get-WMIOBJECT Win32_ComputerSystem).Name}} | ` 
    Measure-Object -Average TotalMilliseconds
8,362251 ms

1..100 | % {Measure-Command {hostname.exe}} | ` 
    Measure-Object -Average TotalMilliseconds
9,12406 ms

1..100 | % {Measure-Command {(Get-CIMInstance CIM_ComputerSystem).Name}} | ` 
    Measure-Object -Average TotalMilliseconds
9,330143 ms

1..100 | % {Measure-Command {(Get-ComputerInfo).CsName}} | ` 
    Measure-Object -Average TotalMilliseconds
1659,054235 ms
```

Comparaison de la vitesse d'exécution des commandes

La commande 1 est toujours la plus rapide avec un temps d'exécution d'environ **0.008 ms**

Les commandes 2 et 3 sont environ 5 fois plus lentes que la commande 1

Les commandes 4, 5 et 6 sont environ 1000 fois plus lentes que la commande 1

La commande 7 est environ 200 000 fois plus lente que la commande 1

La commande la plus rapide

"[system.environment]::MachineName" est toujours extrêmement rapide.

La commande la plus lente

"(Get-ComputerInfo).CsName" est toujours extrêmement lente.

Stratégie d'exécution des scripts avec PowerShell

Les fichiers de script PowerShell doivent avoir l'extension PS1.

La commande **Get-ExecutionPolicy** est utilisée pour obtenir la valeur de la stratégie d'exécution.

La commande **Set-ExecutionPolicy** est utilisée pour modifier la stratégie d'exécution des scripts.

Les valeurs possibles pour le paramètre **-ExecutionPolicy** sont

- **AllSigned**
Nécessite que tous les scripts et tous les fichiers de configuration soient signés par un éditeur approuvé, y compris les scripts écrits sur l'ordinateur local.
- **Bypass**
Permet l'exécution de tous les scripts sans restriction ni avertissement.
- **Default**
Définit la stratégie d'exécution par défaut.
Restricted pour les clients Windows ou RemoteSigned pour les serveurs Windows.
- **RemoteSigned**
Permet l'exécution de scripts créés localement.
Les scripts téléchargés doivent être signés par un éditeur de confiance.
C'est le paramètre par défaut pour les serveurs Windows.
- **Restricted**
Ne permet pas l'exécution de scripts.
C'est le paramètre par défaut pour les clients Windows.
- **Undefined**
Supprime la stratégie d'exécution actuelle et la stratégie d'exécution effective est Restricted.
- **Unrestricted**
Permet l'exécution de tous les scripts, mais avertit avant d'exécuter des scripts téléchargés.

Exemple

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Force
```

IMPORTANT: on ne peut pas exécuter un script PowerShell en double cliquant sur le fichier.

Pour exécuter un script PowerShell, il faut spécifier le chemin absolu ou le chemin relatif lors de l'appel.

Il est possible d'exécuter un script PowerShell sans modifier la stratégie d'exécution.

La ligne de code s'exécute dans une invite de commandes CMD.

```
powershell.exe -ExecutionPolicy Bypass X:\PS\votre_script.ps1
```

Les commentaires

Cette ligne est en commentaire à cause du symbole #.

```
<#  
 Ceci est un commentaire  
 sur plusieurs lignes.  
#>
```

Caractère de continuité

Il est possible d'écrire une ligne d'instruction sur plusieurs lignes en utilisant un caractère de continuité.

Le caractère de continuité correspond à l'accent de grave (**code ASCII 96**).

Les fichiers de configuration pour PowerShell

Un profil applicable à tous les utilisateurs et aux consoles powershell.exe et powershell_ise.exe.

- **\$PSHOME\profile.ps1**
-

Un profil applicable à tous les utilisateurs et à la console powershell.exe.

- **\$PSHOME\Microsoft.PowerShell_profile.ps1**

Un profil applicable à tous les utilisateurs et à la console powershell_ise.exe.

- **\$PSHOME\Microsoft.PowerShellISE_profile.ps1**
-

Un profil applicable à l'utilisateur courant et aux consoles powershell.exe et powershell_ise.exe.

- **\$HOME\Documents\WindowsPowerShell\profile.ps1**
-

Un profil applicable à l'utilisateur courant et à la console powershell.exe.

- **\$HOME\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1**

Un profil applicable à l'utilisateur courant et à la console powershell_ise.exe

- **\$HOME\Documents\WindowsPowerShell\Microsoft.PowerShellISE_profile.ps1**
-

L'ordre d'exécution des fichiers de configuration pour "powershell.exe"

```
$PROFILE | Select-Object *
```

```
AllUsersAllHosts      : $PSHOME\profile.ps1
AllUsersCurrentHost   : $PSHOME\Microsoft.PowerShell_profile.ps1
CurrentUserAllHosts   : $HOME\Documents\WindowsPowerShell\profile.ps1
CurrentUserCurrentHost : $HOME\WindowsPowerShell\Microsoft.PowerShell_profile.ps1
```

L'ordre d'exécution des fichiers de configuration pour "powershell_ise.exe"

```
$PROFILE | Select-Object *
```

```
AllUsersAllHosts      : $PSHOME\profile.ps1
AllUsersCurrentHost   : $PSHOME\Microsoft.PowerShellISE_profile.ps1
CurrentUserAllHosts   : $HOME\Documents\WindowsPowerShell\profile.ps1
CurrentUserCurrentHost : $HOME\Documents\WindowsPowerShell\Microsoft.PowerShellISE_profile.ps1
```

```
# commande pour créer un fichier "profile" pour "CurrentUserAllHosts"
if (!(Test-Path -Path $PROFILE.CurrentUserAllHosts))
{ New-Item -Type File -Path $PROFILE.CurrentUserAllHosts -Force }
```

```
# psedit permet d'éditer facilement les différents fichiers "profile" si les fichiers existent
psedit $profile.AllUsersAllHosts
psedit $profile.AllUsersCurrentHost
psedit $profile.CurrentUserAllHosts
psedit $profile.CurrentUserCurrentHost
```

```
# Commande pour afficher les variables dont le nom débute par ps donc des variables de PowerShell  
Get-Variable ps*
```

La variable **\$psISE** permet de configurer l'environnement ISE de PowerShell.

Exemple d'un fichier \$PSHOME\profile.ps1

```
# Modification de la variable BufferSize  
$InfoHost = Get-Host  
$InfoWindow = $InfoHost.UI.RawUI  
$NewSize = $InfoWindow.BufferSize  
$NewSize.Height = 8192  
$NewSize.Width = 512  
$InfoWindow.BufferSize = $NewSize  
  
# Force l'affichage du volet de script dans "PowerShell ISE"  
if ($psISE.CurrentPowerShellTab.ExpandedScript -eq $false)  
{  
    $psISE.CurrentPowerShellTab.ExpandedScript = $true  
}  
  
# Modification du texte dans la barre de titre  
$InfoWindow.WindowTitle = "Console de " + [system.environment]::UserName
```

Exemple d'un fichier \$HOME\Documents\WindowsPowerShell\profile.ps1

```
# Change le dossier actif  
Set-Location E:\scriptPS1
```

Pour démarrer "**PowerShell ISE**" sans utiliser les fichiers de configuration pour PowerShell.
powershell_ISE.exe -NoProfile

Pour le cours, il n'est pas nécessaire de comprendre le contenu des annexes 1, 2 et 3.

Notions avancées de PowerShell

L'opérateur -f est utilisé pour le formatage de l'affichage

{I,A:FS}... -f nombre

- I Indexe des items à afficher
A Alignement
Si A est un nombre positif alors l'alignement sera de n caractères vers la droite
Si A est un nombre négatif alors l'alignement sera de n caractères vers la gauche
FS Un paramètre optionnel de formatage qui agit sur l'item en fonction de son type

Voici la liste des paramètres FS valides

:c	Représentation monétaire
:d	Padded. (:dP precision=number of digits); if needed, leading zeros are added to the beginning of the (whole) number.
:e	Scientific (exp) notation
:f	Fixed point :f5 = fix to 5 places
:g	Most compact format, fixed or sci :g5 = 5 significant digits
:n	Number (:nP precision=number of decimal places), includes culture separator for thousands 1,000.00
:p	Pourcentage
:r	Précision réversible
:x	Représentation en format hexadécimal
:hh :mm :ss	Affiche l'heure, les minutes et les secondes d'une date "{0:hh}:{0:mm}:{0:ss}"
:HH	Affiche l'heure sous le format 24H
MM	Affiche le mois
MMMM	Affiche le nom au complet du mois
:dd	Affiche le jour du mois
:ddd	Affiche le nom du jour de la semaine
:dddd	Affiche le nom au complet du jour de la semaine
:yyyy	Affiche l'année au complet
#	Caractère spécial

Voici plusieurs exemples

```
"{0:c}" -f 5.25
5,25 $

"{0:d5}" -f 123
00123

"{0,10:d5}" -f 123
00123

# Pour créer une liste de nom avec un suffixe (ORDI01 à ORDI10)
1..10 | ForEach-Object {"ORDI{0:d2}" -f $PSItem}
ORDI01
ORDI02
ORDI03
ORDI04
ORDI05
ORDI06
ORDI07
ORDI08
ORDI09
ORDI10

"{0,15:n4}" -f 2123.24597
2 123,2460

"{0:x}" -f 255
ff

# Convertir le caractère 'A' en valeur hexadécimale
'0x' + "{0:x}" -f [int][char]'A'
0x41

"{0:###-###-###}" -f 123456789
123-456-789
```

```
# Alignement de texte à gauche et à droite
"{0,-10}|{1,10}" -f "Power", "Shell"
Power      |      Shell

# Affichage de texte et de nombre
"{1,10:d5}{0,10}{2,10:x}" -f "Salut", 64, 255
00064      Salut      ff
```

```
# Affiche l'heure, les minutes et les secondes de la date
# note: n'indique pas AM ou PM
"{0:hh}:{0:mm}:{0:ss}" -f (Get-Date)
02:44:49

# Affiche l'heure (format 24H), les minutes et les secondes de la date
"{0:HH}:{0:mm}:{0:ss}" -f (Get-Date)
14:45:57

# Affiche le jour du mois de la date
"{0:dd}" -f (Get-Date)
11

# Affiche le nom du jour de la semaine de la date
"{0:ddd}" -f (Get-Date)
jeu.

# Affiche le nom au complet du jour de la semaine de la date
"{0:dddd}" -f (Get-Date)
Jeudi

# Affiche l'année de la date
"{0:yyyy}" -f (Get-Date)
2021

# Affiche le mois de la date
"{0:MM}" -f (Get-Date)
02

# Affiche le nom au complet du mois de la date
PS D:\_OUTILS> "{0:MMMM}" -f (Get-Date)
février
```

Utilisation de la classe "System.Math" du ".NET Framework"

Voici plusieurs méthodes de la classe **system.math** du ".NET Framework".

```
[system.math]::Abs(n)
[system.math]::Equals(m,n)
[system.math]::Exp(n)          # retourne la valeur de la constante "e" à la puissance "n"
[system.math]::Ceiling(n)
[system.math]::Floor(n)
[system.math]::Max(m,n)
[system.math]::Min(m,n)
[system.math]::Pow(m,n)        # retourne la valeur du nombre "m" à la puissance "n"
[system.math]::Round(n)
[system.math]::Sqrt(n)
[system.math]::Truncate(n)
```

Voici deux propriétés de la classe **system.math** du ".NET Framework".

```
[system.math]::E               # constante E = 2.71828182845905
[system.math]::PI              # constante PI = 3.14159265358979
```

Utilisation de la classe "System.Environment" du ".NET Framework"

NOTE: c'est la commande la plus rapide pour récupérer le nom d'un ordinateur

```
[system.environment]::MachineName
```

```
[system.environment]::UserDomainName
```

```
[system.environment]::UserName
```

```
[system.environment]::OSVersion
```

Utilisation de la classe "System.Windows.MessageBox" du ".NET Framework"

Voici comment afficher un message dans un **MessageBox** en utilisant la méthode **Show**.

NOTE: La méthode Show est surchargée.

Voici la syntaxe d'une surcharge de la méthode Show

```
Show (string messageBoxText,  
       string caption)
```

Exemple

```
[System.Windows.MessageBox]::Show('Le message.', 'Le titre')
```

Voici la syntaxe d'une surcharge de la méthode Show

```
Show (string messageBoxText,  
       string caption,  
       System.Windows.MessageBoxButton button,  
       System.Windows.MessageBoxImage icon)
```

Exemple

```
$rep = [System.Windows.MessageBox]::Show('Le message', 'Le titre', 'YesNoCancel', 'Error')  
  
switch ($rep)  
{  
    'Yes'     { Write-Host 'Oui' }  
    'No'      { Write-Host 'Non' }  
    'Cancel'  { Write-Host 'Annuler' }  
}
```

Voici la liste des valeurs possibles pour l'objet "System.Windows.MessageBoxButton"

```
[System.Enum]::GetNames([System.Windows.MessageBoxButton])  
OK  
OKCancel  
YesNoCancel  
YesNo
```

Voici la liste des valeurs possibles pour l'objet "System.Windows.MessageBoxImage"

```
[System.Enum]::GetNames([System.Windows.MessageBoxImage])  
None  
Hand  
Error  
Stop  
Question  
Exclamation  
Warning  
Asterisk  
Information
```

Utilisation de la classe "Microsoft.VisualBasic.Interaction" du ".NET Framework"

Voici comment afficher un message dans un **MsgBox** qui est toujours au premier plan.

```
Add-Type -AssemblyName Microsoft.VisualBasic
$rep =
[Microsoft.VisualBasic.Interaction]::MsgBox('Message', 'YesNoCancel, SystemModal, Information', 'Titre')
$rep

switch ($rep)
{
    'Yes'      { Write-Host 'Oui' }
    'No'       { Write-Host 'Non' }
    'Cancel'   { Write-Host 'Annuler' }
}
```

"Microsoft.VisualBasic.MsgBoxStyle" a plusieurs valeurs qu'il est possible de combiner par une virgule

```
[System.Enum]::GetNames([Microsoft.VisualBasic.MsgBoxStyle])
ApplicationModal
DefaultButton1
OkOnly
OkCancel
AbortRetryIgnore
YesNoCancel
YesNo
RetryCancel
Critical
Question
Exclamation
Information
DefaultButton2
DefaultButton3
SystemModal
MsgBoxHelp
MsgBoxSetForeground
MsgBoxRight
MsgBoxRtlReading
```

Utilisation de la classe "System.Convert" du ".NET Framework"

Convertit la représentation d'une chaîne de caractères d'un nombre dans une base spécifiée en un entier 32 bits signé.
ToInt32(String, Int32)

```
# Conversion d'un nombre binaire en entier  
[system.convert]::ToInt32('10000000',2)
```

```
# Conversion d'un nombre octal en entier  
[system.convert]::ToInt32('10',8)
```

```
# Conversion d'un nombre hexadécimal en entier  
[system.convert]::ToInt32('FF',16)
```

Convertit la représentation d'une chaîne de caractères d'un nombre dans une base spécifiée en un entier 64 bits signé.
ToInt64(String, Int32)

```
# Conversion d'un grand nombre hexadécimal en entier  
[system.convert]::ToInt64('FFFFFFFF',16)
```

```
# Conversion d'un grand nombre binaire en entier  
[system.convert]::ToInt64('10000000000000000000000000000000',2)
```

```
# Définir le nombre décimal  
$nombreDecimal = 1024
```

```
# Conversion d'un nombre entier en binaire (chaîne de caractères)  
$nombreBinaire = [system.convert]::ToString($nombreDecimal,2)
```

```
# Affichage du nombre binaire sur 32 colonnes (32 bits)  
$nombreBinaire.PadLeft(32,'0')
```

```
# Définir le nombre décimal  
$nombreDecimal = 255
```

```
# Conversion d'un nombre entier en hexadécimal (chaîne de caractères)  
$nombreHexa = [system.convert]::ToString(255,16)
```

```
# Conversion en majuscule du nombre hexadécimal  
$nombreHexa = $nombreHexa.ToUpper()
```

```
# Affichage du nombre hexadécimal sur 8 colonnes (32 bits)  
$nombreHexa.PadLeft(8,'0')
```

Chargement d'une classe avant l'appel d'une méthode

```
Add-Type -AssemblyName System.Web  
[System.Web.Security.Membership]::GeneratePassword(8,1)
```

- le premier paramètre de GeneratePassword spécifie la longueur du mot de passe
 - le deuxième paramètre de GeneratePassword spécifie le nombre minimum de caractères spéciaux
-

Get-Member permet d'obtenir la liste des propriétés et des méthodes des objets.

```
# $S contient la liste des services sur un ordinateur local  
$S = Get-Service
```

```
# Get-Member obtient le type System.ServiceProcess.ServiceController et la liste des membres  
# contient des méthodes comme Pause, Start, Stop et des propriétés comme StartType, Status.  
$S | Get-Member
```

```
# Get-Member obtient le type System.Object[] et la liste des membres contient des méthodes  
# comme Add, Remove et des propriétés comme Length.  
Get-Member -InputObject $S
```

Utilisation d'objet COM

Voici un exemple de code qui utilise l'objet COM **Wscript.Shell** pour créer un raccourci sur le Bureau.

```
$cible = "C:\_TEMP\info.txt"
$lien = "C:\Users\richard\Desktop\Mon_Lien.lnk"

$WshShell = New-Object -ComObject Wscript.Shell
$raccourci = $WshShell.CreateShortcut($lien)
$raccourci.TargetPath = $cible
$raccourci.Save()
```

Le fichier **COM_Object_Excel.ps1** qui est sur LÉA montre comment utiliser l'objet COM **Excel.Application** pour insérer des valeurs et effectuer des calculs dans Excel.

Le fichier **GUI_map_drive.ps1** qui est sur LÉA montre comment utiliser la classe **System.Windows.Forms** pour créer des objets: Form, Button, Label, TextBox, MaskedTextBox.

PSDrive

Un PSDrive a un comportement similaire à l'Explorateur de fichiers.
Un PSDrive est relié à un fournisseur.

Pour s'assurer que le module ActiveDirectory est accessible par un fournisseur PSDrive

```
Import-Module ActiveDirectory
```

Affiche la liste des fournisseurs

```
Get-PSProvider | Format-Table -AutoSize
```

Name	Capabilities	Drives
Registry	ShouldProcess, Transactions	{HKLM, HKCU}
Alias	ShouldProcess	{Alias}
Environment	ShouldProcess	{Env}
FileSystem	Filter, ShouldProcess, Credentials	{C, R}
Function	ShouldProcess	{Function}
Variable	ShouldProcess	{Variable}
Certificate	ShouldProcess	{Cert}
WSMan	Credentials	{WSMan}
ActiveDirectory	Include, Exclude, Filter, ShouldProcess, Credentials	{AD}

Affiche les lecteurs disponibles pour PSDrive

```
Get-PSDrive | Format-Table -AutoSize
```

Name	Used (GB)	Free (GB)	Provider	Root	CurrentLocation
AD			ActiveDirectory	//RootDSE/	
Alias				Alias	
C	15,69	110,76	FileSystem	C:\	Users\Administrateur.HV1
Cert			Certificate	\	
Env			Environment		
Function			Function		
HKCU			Registry	HKEY_CURRENT_USER	
HKLM			Registry	HKEY_LOCAL_MACHINE	
Variable			Variable		
WSMan			WSMan		

"AD" est le nom du lecteur qui permet d'accéder au fournisseur "ActiveDirectory".

Déplacement au niveau du lecteur "AD"

```
cd AD:
```

Pour afficher les objets qui sont directement sous le lecteur "AD".

```
Get-ChildItem
```

Name	ObjectClass	DistinguishedName
formation	domainDNS	DC=formation,DC=local
Configuration	configuration	CN=Configuration,DC=formation,DC=local
Schema	dMD	CN=Schema,CN=Configuration,DC=formation,DC=local
DomainDnsZones	domainDNS	DC=DomainDnsZones,DC=formation,DC=local
ForestDnsZones	domainDNS	DC=ForestDnsZones,DC=formation,DC=local

Naviguer dans le lecteur "AD"

```
# Déplacement au niveau du domaine FORMATION.LOCAL  
cd "DC=formation,DC=local"
```

```
# Pour afficher les objets qui sont directement sous le lecteur "AD:\DC=formation,DC=local".  
Get-ChildItem
```

Name	ObjectClass	DistinguishedName
-----	-----	-----
_DATA	organizationalUnit	OU=_DATA,DC=formation,DC=local
Builtin	builtinDomain	CN=Builtin,DC=formation,DC=local
Computers	container	CN=Computers,DC=formation,DC=local
Domain Controllers	organizationalUnit	OU=Domain Controllers,DC=formation,DC=local
ForeignSecurityPr...	container	CN=ForeignSecurityPrincipals,DC=formation,DC=local
Infrastructure	infrastructureUpdate	CN=Infrastructure,DC=formation,DC=local
Keys	container	CN=Keys,DC=formation,DC=local
LostAndFound	lostAndFound	CN=LostAndFound,DC=formation,DC=local
Managed Service A...	container	CN=Managed Service Accounts,DC=formation,DC=local
NTDS Quotas	msDS-QuotaContainer	CN=NTDS Quotas,DC=formation,DC=local
ORDINATEURS	organizationalUnit	OU=ORDINATEURS,DC=formation,DC=local
Program Data	container	CN=Program Data,DC=formation,DC=local
System	container	CN=System,DC=formation,DC=local
TPM Devices	msTPM-Information...	CN=TPM Devices,DC=formation,DC=local
Users	container	CN=Users,DC=formation,DC=local
UTILISATEURS	organizationalUnit	OU=UTILISATEURS,DC=formation,DC=local

```
# Déplacement au niveau du conteneur "Users"  
cd "CN=Users"
```

```
# Pour sortir du lecteur PSDrive, il suffit de se déplacer dans le lecteur "C"  
c:
```

ANNEXE 1

WINNT:// et LDAP://

Les deux fournisseurs les plus utilisés pour l'administration système et réseau sont

WINNT:// # c'est le fournisseur Windows et Windows Server
LDAP:// # c'est le fournisseur qui permet d'accéder à LDAP
LDAP (Lightweight Directory Access Protocol)

Syntaxe générique pour WINNT://

```
WINNT://<nom_domaine>,<nom_objet>,<nom_classe>
```

```
# L'utilisateur "Richard" est un utilisateur local  
$a = [ADSI]"WinNT://127.0.0.1/RICHARD,user"
```

```
# L'utilisateur "Administrateur" est un utilisateur du domaine "FORMATION"  
$b = [ADSI]"WinNT://formation/Administrateur,user"
```

```
# Liste les propriétés de l'objet $b  
$b | Get-Member
```

Syntaxe générique pour LDAP://

```
LDAP://<nom_unique>
```

Le nom_unique correspond au DistinguishedName.
L'objet recherché doit être parfaitement connu.

```
LDAP://CN=Administrateur,CN=Users,DC=formation,DC=local
```

```
$c = [ADSI]"LDAP://CN=Administrateur,CN=Users,DC=formation,DC=local"
```

```
# Liste les propriétés de l'objet $c  
$c | Get-Member
```

La liste des propriétés de "**\$b | Get-Member**" est différente de "**\$c | Get-Member**".

ANNEXE 2

Module Microsoft.Windows.Bcd.Cmdlets dans "Windows 11"

Pour configurer le fichier BCD (Boot Configuration Database) les administrateurs peuvent utiliser BCDEDIT.EXE. Avec la commande BCDEDIT.EXE, c'est difficile d'automatiser la modification du fichier BCD.

La configuration du "Windows Boot Manager" dans le UEFI de votre ordinateur modifie indirectement le contenu du fichier BCD.

Le module Microsoft.Windows.Bcd.Cmdlets permet d'automatiser la configuration du fichier BCD.

```
# Commande qui affiche la liste complète des cmdlets
(Get-Command -Module Microsoft.Windows.Bcd.Cmdlets).Name

Copy-BcdEntry
Disable-BcdElementBootDebug
Disable-BcdElementBootEms
Disable-BcdElementDebug
Disable-BcdElementEms
Disable-BcdElementEventLogging
Disable-BcdElementHypervisorDebug
Enable-BcdElementBootDebug
Enable-BcdElementBootEms
Enable-BcdElementDebug
Enable-BcdElementEms
Enable-BcdElementEventLogging
Enable-BcdElementHypervisorDebug
Export-BcdStore
Get-BcdEntry
Get-BcdEntryDebugSettings
Get-BcdEntryHypervisorSettings
Get-BcdStore
Import-BcdStore
New-BcdEntry
New-BcdStore
Remove-BcdElement
Remove-BcdEntry
Set-BcdBootDefault
Set-BcdBootDisplayOrder
Set-BcdBootSequence
Set-BcdBootTimeout
Set-BcdBootToolsDisplayOrder
Set-BcdDebugSettings
Set-BcdElement
Set-BcdHypervisorSettings
```

ANNEXE 3

Conflits entre le module Hyper-V et le module VMware.VimAutomation.Core

La compagnie VMware utilise PowerShell pour gérer les machines virtuelles et son hyperviseur ESXi.

Malheureusement, le module VMware.VimAutomation.Core inclus dans PowerCLI contient plusieurs cmdlet qui portent le même nom que les cmdlet du module Hyper-V.

Pour utiliser le bon cmdlet, il faut utiliser la syntaxe suivante: **[ModuleName]\[Cmdlet_or_Function_Name]**

Par exemple, **Get-VM** existe dans le module Hyper-V et le module VMware.VimAutomation.Core

```
# Pour vérifier si une commande existe dans plusieurs modules,  
# ajouter le caractère * devant le nom de la commande.  
(Get-Command *Get-VM) .Source  
VMware.VimAutomation.Core  
Hyper-V  
  
# Si le caractère * n'est pas devant le nom de la commande,  
# le résultat affiche seulement un module.  
(Get-Command Get-VM) .Source  
VMware.VimAutomation.Core
```

Il est important de spécifier le nom du module pour utiliser le bon cmdlet.

```
Get-Help VMware.VimAutomation.Core\Get-VM  
  
Get-Help Hyper-V\Get-VM
```

PowerShell Direct

Pour créer une session "PowerShell Direct" sur une machine virtuelle

- L'ordinateur virtuel doit s'exécuter localement sur l'ordinateur réel.
- Vous devez utiliser un compte qui est membre du groupe "Administrateurs".
- Vous devez fournir les informations pour s'authentifier à l'ordinateur virtuel.
- L'ordinateur réel doit exécuter le système d'exploitation Windows 10 ou Windows Server 2016.
- L'ordinateur virtuel doit exécuter le système d'exploitation Windows 10 ou Windows Server 2016.

Exemple 1:

```
Enter-PSSession -VMName "VMName"
```

- **Les commandes s'exécutent sur la machine virtuelle.**

```
Exit-PSSession
```

Exemple 2:

```
# on enregistre les informations pour l'authentification dans une variable
$Cred = Get-Credential
```

```
Invoke-Command -VMName "C53-SERVEUR1" ` 
    -Credential $Cred ` 
    -ScriptBlock { get-process }
```

Exemple 3:

```
# on enregistre les informations pour l'authentification dans une variable
$Cred = Get-Credential
```

```
$NOM_VM = "C53-SERVEUR1"
$nom_fichier = "D:\script\mon_script.ps1"
```

```
# Le fichier de script doit utiliser le cmdlet Write-Output
# si on veut récupérer les messages affichés
$rep = Invoke-Command -VMName $NOM_VM ` 
    -Credential $Cred ` 
    -FilePath $nom_fichier
```

Utilisation d'une variable globale dans un ScriptBlock

Il est possible d'utiliser une variable globale dans un ScriptBlock à condition d'utiliser **\$using:** devant le nom de la variable.

```
$Cred = Get-Credential -Credential "FORMATION\Administrateur"

$prog = "win*"
$NOM_VM = "C53-SERVEUR1"

Invoke-Command -VMName $NOM_VM ` 
    -Credential $Cred ` 
    -ScriptBlock { Get-Process -Name $using:prog }
```

Utilisation du paramètre -ArgumentList avec "Invoke-Command"

Utilisation de la variable \$args[0] dans "Invoke-Command"

\$args[0] accepte seulement une valeur

```
$p = "power*"  
Invoke-Command -VMName "C53-SERVEUR1" `  
    -Credential "FORMATION\Administrateur" `  
    -ScriptBlock { Get-Process -Name $args[0] } `  
    -ArgumentList $p
```

Utilisation de la variable \$args dans "Invoke-Command"

\$args peut accepter plus d'une valeur mais dans cet exemple \$p contient une seule valeur

```
$p = "power*"  
Invoke-Command -VMName "C53-SERVEUR1" `  
    -Credential "FORMATION\Administrateur" `  
    -ScriptBlock { Get-Process -Name $args } `  
    -ArgumentList $p
```

Utilisation de la variable \$args dans "Invoke-Command"

\$args permet de passer un tableau en paramètre comme dans l'exemple

```
$p = "power*","win*"  
Invoke-Command -VMName "C53-SERVEUR1" `  
    -Credential "FORMATION\Administrateur" `  
    -ScriptBlock { Get-Process -Name $args } `  
    -ArgumentList $p
```

Utilisation d'une variable nommée dans "Invoke-Command"

Avec cette méthode, on doit utiliser **param** pour utiliser une variable nommée.

La variable nommée peut accepter plus d'une valeur mais dans cet exemple \$p contient une seule valeur
\$p = "power*"

```
Invoke-Command -VMName "C53-SERVEUR1" `  
    -Credential "FORMATION\Administrateur" `  
    -ScriptBlock {  
        param ($proc)  
        Get-Process -Name $proc  
    } `  
    -ArgumentList $p
```

Utilisation d'une variable nommée dans "Invoke-Command"

La variable nommée permet de passer un tableau en paramètre comme dans l'exemple

Par contre, on doit obligatoirement respecter la syntaxe dans le paramètre -ArgumentList.

```
$p = "power*","win*"  
Invoke-Command -VMName "C53-SERVEUR1" `  
    -Credential "FORMATION\Administrateur" `  
    -ScriptBlock {  
        param ($proc)  
        Get-Process -Name $proc  
    } `  
    -ArgumentList (,$p)
```

Exemple 1 – Exécution d'un ScriptBlock qui utilise des commandes Write-Output

```
# on enregistre les informations pour l'authentification dans une variable
$Cred = Get-Credential

$NOM_VM = "C53-SERVEUR2"
$siteFTP= "FTP_ADR1"

# on doit utiliser le cmdlet Write-Output si on veut récupérer les messages affichés
$code = { Write-Output "=====
        Write-Output "Nom, état et dossier du site FTP"
        Write-Output "=====
        Get-Website -name $args[0] `n
                    | Select-Object Name,State,PhysicalPath `n
                    | Format-Table -AutoSize `n
                    | Out-String
    }

$siteInfo = Invoke-Command -VMName $NOM_VM `n
                        -Credential $Cred `n
                        -ScriptBlock $code `n
                        -ArgumentList $siteFTP

$siteInfo
```

Résultat de l'exécution du ScriptBlock

```
# Le contenu de la variable $siteInfo
=====
Nom, état et dossier du site FTP
=====

name      state    physicalPath
----      ----     -----
FTP_ADR1  Started  C:\_FTP\FTP_ADR1
```

Exemple 2 – Exécution d'un ScriptBlock sur plusieurs ordinateurs virtuels

```
# on enregistre les informations pour l'authentification dans une variable
$Cred = Get-Credential -Credential "Administrateur"

# Les VM "WIN10-1" et "WIN10-2" ne sont pas dans l'Active Directory.
Invoke-Command -VMName "WIN10-1","WIN10-2" `n
                -Credential $Cred `n
                -ScriptBlock { Get-LocalUser -Name t* | Out-Host }
```

Résultat de l'exécution du ScriptBlock

```
Name Enabled Description
--- ----- -----
TECH True

Name Enabled Description
--- ----- -----
TEST True
```

L'ordinateur virtuel "Server_Core_2019" est sur le SERVEUR2.
EXÉCUTION DU CODE À PARTIR DU SERVEUR1

Le SERVEUR1 et le SERVEUR2 sont dans un domaine "Active Directory".
L'ordinateur virtuel "Server_Core_2019" est sur le SERVEUR2.

Voici comment exécuter du code dans l'ordinateur virtuel qui est sur le SERVEUR2 mais en exécutant le code PowerShell sur le SERVEUR1,

```
# Voici le contenu du fichier "E:\core_info.ps1" qui est sur le SERVEUR1
Write-Output "=====
Write-Output "Configuration de la VM"
Write-Output "=====
(Get-ComputerInfo).CsName
(Get-NetIPAddress -AddressFamily IPv4).IPAddress

#-----
# Ce code doit s'exécuter sur le SERVEUR1
#-----
# Lire le contenu du fichier PS1 qui est sur le SERVEUR1
# '\n\r' correspond à un saut de ligne dans Windows
$fichier = Get-Content -Path "E:\core_info.ps1"
    -Delimiter '\n\r'

$cred_VM = Get-Credential -UserName "Administrateur"
    -Message "Server_Core_2019"

# $using:cred_VM permet de passer la variable $cred_VM dans la requête imbriquée.
# $using:fichier permet de passer la variable $fichier dans la requête imbriquée.

Invoke-Command -ComputerName "SERVEUR2"
    -ScriptBlock { hostname.exe
        Invoke-Command -VMName "Server_Core_2019"
            -Credential $using:cred_VM
            -scriptblock { param($code)
                Invoke-Expression $code
            }
            -ArgumentList ($using:fichier)
    }
```

Résultat de l'exécution du code

```
SERVEUR2
=====
Configuration du serveur 'CORE'
=====
CORE
192.168.53.140
127.0.0.1
```

Sauvegarder l'authentification d'un utilisateur dans une variable

Ce code permet de conserver dans une variable le nom de l'utilisateur et le mot de passe qui est enregistré sous forme "System.Security.SecureString" dans une variable.

```
# Script qui utilise trois paramètres obligatoires
[CmdletBinding()]
Param
(
    [Parameter(Mandatory=$True)] $NOM_VM,
    [Parameter(Mandatory=$True)] $UserName,
    [Parameter(Mandatory=$True)] $MDP
)
Clear-Host

$pass = ConvertTo-SecureString -AsPlainText $MDP -Force
$Cred = New-Object -TypeName System.Management.Automation.PSCredential ` 
        -ArgumentList $Username,$pass

$code = { Start-VM -Name $args[0] }

Invoke-Command -ComputerName SERVEUR1 ` 
    -ScriptBlock $code ` 
    -ArgumentList $NOM_VM ` 
    -Credential $Cred
```

Plusieurs commandes de PowerShell utilisent le paramètre -Password qui est de type <System.Security.SecureString>.

```
Le paramètre -Password de New-LocalUser est de type <System.Security.SecureString>
# si le paramètre est de type <System.Security.SecureString>
# Read-Host permet facilement de sécuriser le mot de passe
$mdp = Read-Host -Prompt "Entrer le mot de passe" -AsSecureString

New-LocalUser -Name "admin" ` 
    -Password $mdp ` 
    -FullName "Prénom Nom" ` 
    -Description "admin est membre du groupe Administrateurs"
```

Plusieurs commandes de PowerShell utilisent le paramètre -Password qui est de type <string>.

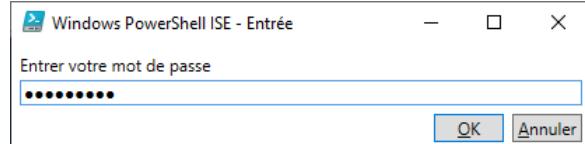
Le paramètre -Password de New-SmbMapping est de type <String>.

Convertir une chaîne sécurisée en texte clair

Ce code est utile pour des cmdlets qui ont besoin du mot de passe en texte clair.

Par exemple, pour se connecter à un partage réseau avec New-SmbMapping
Le paramètre `-Password` de `New-SmbMapping` est de type `<String>`

```
$SecurePassword = Read-Host -Prompt "Entrer votre mot de passe" -AsSecureString
```



```
# Ces deux lignes de code permettent de récupérer le mot de passe en texte clair.  
$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecurePassword)  
$UnsecurePassword = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR)
```

```
# Voici le contenu de la variable $SecurePassword pour le mot de passe AAAaaa111  
System.Security.SecureString
```

```
# Le contenu de la variable $BSTR n'est jamais le même  
1548010025976
```

```
# Voici le contenu de la variable $UnsecurePassword  
AAAaaa111
```

Exemple sécuritaire pour se connecter à un partage réseau avec New-SmbMapping

```
$utilisateur = Read-Host -Prompt "Entrer le nom de l'utilisateur"  
$mdp = Read-Host -Prompt "Entrer le mot de passe" -AsSecureString
```

```
# Ces deux lignes de code permettent de récupérer le mot de passe en texte clair.  
$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($mdp)  
$UnsecurePassword = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR)
```

```
New-SmbMapping -LocalPath R:  
    -RemotePath '\\127.0.0.1\C$`  
    -UserName $utilisateur`  
    -Password $UnsecurePassword
```

```
Clear-Variable -Name UnsecurePassword
```

Exemple moins sécuritaire pour se connecter à un partage réseau avec New-SmbMapping

```
$utilisateur = Read-Host -Prompt "Entrer le nom de l'utilisateur"  
$mdp = Read-Host -Prompt "Entrer le mot de passe"
```

```
New-SmbMapping -LocalPath R:  
    -RemotePath '\\127.0.0.1\C$`  
    -UserName $utilisateur`  
    -Password $mdp
```

```
Clear-Variable -Name mdp
```

Exécution du code PowerShell sur un ordinateur distant

Exécution de commandes PowerShell sur un ordinateur distant

Si on a des ordinateurs qui ne sont pas membres d'un domaine mais d'un "Groupe de travail", c'est plus difficile d'avoir accès à un autre ordinateur par programmation PowerShell.

Sur chaque ordinateur il faut exécuter la commande suivante:

- o **Enable-PSRemoting -Force**

Cette commande démarre le service WinRM et active la fonctionnalité "Gestion à distance de Windows" dans le "Pare-feu Windows".

- "Get-Service WinRM" permet de vérifier l'état du service WinRM

note: si vous avez une carte réseau de type "Réseau public" vous devez utiliser la commande suivante: **Enable-PSRemoting -SkipNetworkProfileCheck -Force**

Sur chaque ordinateur il faut exécuter la commande suivante:

- o **Set-Item wsman:\localhost\client\trustedhosts -Value * -Force**

Cette commande ajoute des ordinateurs auxquels on a confiance.

On peut remplacer le paramètre * par une liste de noms ou d'adresses IP qui sont séparés par des virgules.

Sur chaque ordinateur il faut exécuter la commande suivante:

- o **Restart-Service WinRM**

On redémarre le service WinRM pour s'assurer que les nouveaux paramètres sont utilisés.

Pour vérifier si WinRM est fonctionnel sur un ordinateur distant il faut exécuter la commande suivante:

- o **Test-WsMan NomOrdinateurDistant**

NomOrdinateurDistant est le nom de l'ordinateur distant sur lequel on veut avoir accès à l'aide de PowerShell.

Configurations dans le "Pare-feu Windows" de l'ordinateur distant

- Activé le paramètre "Partage de fichiers et d'imprimantes"

Modification dans le registre Windows de l'ordinateur distant

- Configurer le paramètre "**LocalAccountTokenFilterPolicy**"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001

Modifier la liste des "TrustedHosts" pour autoriser tous les ordinateurs

```
set-item wsman:\localhost\Client\TrustedHosts -value *
```

Modifier la liste des "TrustedHosts" pour autoriser des ordinateurs

```
set-item wsman:\localhost\Client\TrustedHosts -value ordi1,ordi2
```

Modifier la liste des "TrustedHosts" pour autoriser tous les ordinateurs d'un domaine

```
set-item wsman:\localhost\Client\TrustedHosts *.decinfo.cvm
```

Pour ajouter un ordinateur à une liste existante des "TrustedHosts"

```
$curValue = (get-item wsman:\localhost\Client\TrustedHosts).value  
set-item wsman:\localhost\Client\TrustedHosts -value "$curValue,ordi99"
```

Modifier la liste des "TrustedHosts" pour autoriser des adresses IP

note: une adresse IPv6 doit être entre crochet

```
set-item wsman:\localhost\Client\TrustedHosts -value 192.168.0.100,[0:0:0:0:0:0:0]
```

Modifier la liste des "TrustedHosts" sur un ordinateur distant pour autoriser des adresses IP

```
connect-wsman -computername ordi99
```

```
set-item wsman:\ordi99\Client\TrustedHosts -value 192.168.0.100,[0:0:0:0:0:0:0]
```

```
disconnect-wsman -computername ordi99
```

Pour afficher la liste des "TrustedHosts"

```
get-item wsman:\localhost\Client\TrustedHosts
```

- Par défaut, l'item TrustedHosts existe mais sa valeur est vide.

Pour afficher la liste des "TrustedHosts" sur un ordinateur distant

```
connect-wsman -computername ordi99
```

```
get-item WSMAN:\ordi99\Client\TrustedHosts
```

```
disconnect-wsman -computername ordi99
```

Utilisation du cmdlet invoke-command

invoke-command exécute des commandes ou des scripts sur un ordinateur distant

- invoke-command -computername ordi1,ordi2 {get-process}
- invoke-command -computername ordi1,ordi2 -filepath c:\scripts\MonScript.ps1

Utilisation du cmdlet Enter-PSSession

Enter-PSSession démarre une session interactive avec un ordinateur distant

- Enter-PSSession -computername NomOrdinateur
- Enter-PSSession -computername NomOrdinateur -Credential Domaine\utilisateur

Pour terminer la session interactive on exécute la commande EXIT.

Comment trouver le nom de l'exception pour "Try / Catch"

```
PS D:\_OUTILS> Get-ChildItem -Path "C:\TOTO"
Get-ChildItem : Impossible de trouver le chemin d'accès « C:\TOTO », car il n'existe pas.
Au caractère Ligne:1 : 1
+ Get-ChildItem -Path "C:\TOTO"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\TOTO:String) [Get-ChildItem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand
```

PS D:_OUTILS>

Le message d'erreur affiche l'exception "ItemNotFoundException" mais ce n'est pas le nom complet de cette exception.

\$Error[0] contient toujours l'erreur la plus récente

```
PS D:\_OUTILS> $Error[0].Exception.GetType().FullName
System.Management.Automation.ItemNotFoundException
PS D:\_OUTILS>
```

\$Error[0].Exception.GetType().FullName

- Cette commande affiche le nom complet de l'exception

\$Error.Count

- Pour compter le nombre d'erreurs dans la variable \$Error

\$Error.Clear()

- Pour vider la liste des erreurs dans la variable \$Error

Le paramètre "-ErrorAction Stop" est souvent utilisé pour que "Try / Catch" fonctionne correctement.

Exemple sans "Try and Catch"

```
Remove-Item -Path "C:\TOTO"
```

```
$Error[0].Exception.GetType().FullName
```

```
PS E:\ps> $Error[0].Exception.GetType().FullName
System.Management.Automation.ItemNotFoundException
```

```
$Error.Clear()
```

Exemple avec "Try and Catch"

```
$chemin = "C:\TOTO"
```

```
try
{
    Remove-Item -Path $chemin -ErrorAction Stop
    Write-Host "'$chemin' existe !!" -ForegroundColor Cyan
}
catch [System.Management.Automation.ItemNotFoundException]
{
    Write-Host "'$chemin' n'existe pas !!" -ForegroundColor Yellow
}
```

Code pour afficher la liste complète des exceptions

```
$nbExceptions = 0
$nbErreurs = 0

$rep = [appdomain]::CurrentDomain.GetAssemblies() | ForEach-Object {
    Try
    {
        $PSItem.GetExportedTypes() | Where-Object {
            $PSItem.FullName -Match 'Exception'
        }
    }
    Catch
    {
        $nbErreurs++
    }
}

$exceptions = $rep | Select-Object FullName | Sort-Object FullName
$nbExceptions = $rep.Count
$exceptions

Write-Host "$nbExceptions exceptions" -ForegroundColor Green
Write-Host "$nbErreurs erreurs" -ForegroundColor Yellow
```

Exemple avec les cmdlet Compress-Archive et Expand-Archive

Compress-Archive est un cmdlet du module Microsoft.PowerShell.Archive
Expand-Archive est un cmdlet du module Microsoft.PowerShell.Archive

```
Get-Command -Module Microsoft.PowerShell.Archive

Compress-Archive -Path c:\temp -DestinationPath c:\backup\temp.zip

Expand-Archive -Path c:\backup\temp.zip -DestinationPath c:\temp -Force
```

Exemple avec le cmdlet Copy-Item

Copy-Item est un cmdlet du module Microsoft.PowerShell.Management

Création d'une session vers l'ordinateur 407P33
`$cs = New-PSSession -ComputerName 407P33`

Le paramètre -ToSession est utilisé pour copier un fichier sur un ordinateur distant
`Copy-Item -Path C:\Source\test.csv -Destination C:\Source\test.csv -ToSession $cs`

Le paramètre -FromSession est utilisé pour copier un fichier à partir d'un ordinateur distant
`Copy-Item -Path C:\Source\srv.csv -Destination C:\Source\srv.csv -FromSession $cs`

Exemple avec le cmdlet Get-FileHash

Get-FileHash est un cmdlet du module Microsoft.PowerShell.Utility

Le cmdlet Get-FileHash permet d'utiliser plusieurs algorithmes de hachage sur un fichier
`$info_shal = (Get-FileHash -Path win10.iso -Algorithm SHA1).HASH`

Exemple avec le cmdlet Invoke-WebRequest

Invoke-WebRequest est un cmdlet du module Microsoft.PowerShell.Utility

Exemple pour afficher le contenu du fichier par défaut d'un site WEB

```
# Le site "http://ifconfig.me" retourne l'adresse IP qui donne accès à internet.
$ip = (Invoke-WebRequest -Uri https://ifconfig.me/ip).Content

# Voici le contenu de la variable $ip
206.167.112.182
```

Exemple pour sauvegarder dans un fichier, le contenu du fichier par défaut d'un site WEB
`Invoke-WebRequest -Uri https://ifconfig.me -OutFile C:_TEMP\ADR1.HTML`

Le fichier IP.TXT contient SEULEMENT l'adresse IP externe qui donne accès à internet
`(Invoke-WebRequest -Uri https://ifconfig.me/ip).Content | Out-File C:_TEMP\IP.TXT`

Exemple avec le cmdlet Format-Hex

Format-Hex est un cmdlet du module Microsoft.PowerShell.Utility

Le cmdlet Format-Hex permet de convertir un caractère en une valeur hexadécimale
`'PowerShell' | Format-Hex`

Exemple avec le cmdlet New-TemporaryFile

New-TemporaryFile est un cmdlet du module Microsoft.PowerShell.Utility

Le cmdlet New-TemporaryFile permet de créer un fichier temporaire.

```
$fichier1 = New-TemporaryFile  
$fichier1
```

Le fichier temporaire est créé automatiquement dans le dossier de la variable d'environnement TEMP.
`$ENV:TEMP`

Exemple avec le cmdlet Send-MailMessage

Send-MailMessage est un cmdlet du module Microsoft.PowerShell.Utility

```
Send-MailMessage -From "Nom@Compagnie.ca" `  
-To "AutreNom@AutreCompagnie.ca" `  
-Subject "WDS: $ENV:COMPUTERNAME" `  
-Body "Fin de l'installation sur l'ordinateur: $ENV:COMPUTERNAME" `  
-SmtpServer smtp.compagnie.ca
```

Continuer l'exécution d'un script après un redémarrage

Dans le registre de Windows, il y a quatre clés qui permettent d'exécuter du code selon quatre situations.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- permet d'exécuter du code à chaque ouverture de session d'un utilisateur spécifique

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

- permet d'exécuter du code une seule fois lors de l'ouverture de session d'un utilisateur spécifique

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- permet d'exécuter du code à chaque démarrage de l'ordinateur et à l'ouverture de session d'un utilisateur de l'ordinateur

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

- permet d'exécuter du code une seule fois lors du démarrage de l'ordinateur et à l'ouverture de session d'un utilisateur de l'ordinateur
-

Exemple d'un script qui va exécuter du code après un redémarrage de l'ordinateur.

```
$RunOnceKey = "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"

$code = "c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe"
$code += " -ExecutionPolicy Unrestricted"
$code += " -File C:\script\JoindreDomaine.ps1"

Set-ItemProperty -Path $RunOnceKey ` 
    -Name 'JoindreDomaine' ` 
    -Value $code ` 
    -Force

Rename-Computer -NewName HV1 ` 
    -Restart
```

Fonction avancée dans PowerShell

Utilisation de l'attribut **CmdletBinding** et de l'attribut **Parameter**

Voici la fonction avancée la plus simple

```
Function F1 {  
    [CmdletBinding()]Param()  
}
```

Si on enregistre la fonction F1 dans un fichier TEST_F1.PS1

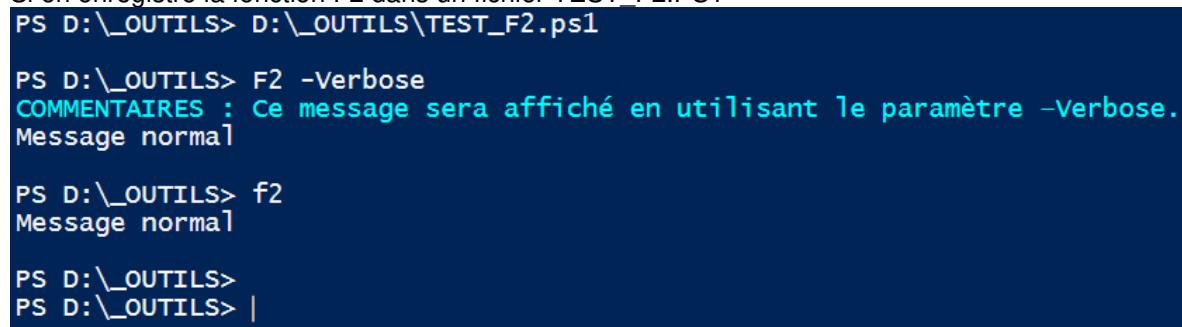
L'attribut **CmdletBinding** permet d'avoir accès à plusieurs paramètres



L'attribut **CmdletBinding** permet d'utiliser **Write-Verbose** dans une fonction

```
Function F2 {  
    [CmdletBinding()]Param()  
    Write-Verbose "Ce message sera affiché en utilisant le paramètre -Verbose."  
    Write-Host "Message normal"  
}
```

Si on enregistre la fonction F2 dans un fichier TEST_F2.PS1



La fonction F3 utilise un paramètre obligatoire

```
Function F3 {  
    [CmdletBinding()]  
    Param([Parameter(Mandatory=$True)]  
        [String]$Source  
    )  
    Write-Host $Source -ForegroundColor Yellow  
}
```

Si on enregistre la fonction F3 dans un fichier TEST_F3.PS1

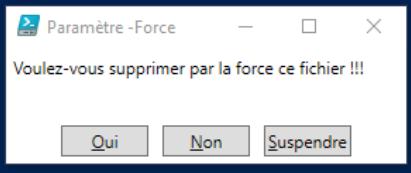
PowerShell nous demande de fournir une valeur pour le paramètre de notre fonction

```
PS D:\_OUTILS> D:\_OUTILS\TEST_F3.ps1  
  
PS D:\_OUTILS> F3  
applet de commande F3 à la position 1 du pipeline de la commande  
Fournissez des valeurs pour les paramètres suivants :  
Source :
```

La fonction F4 utilise un paramètre pour afficher une fenêtre de confirmation.

```
Function F4 {  
    [CmdletBinding(SupportsShouldProcess)]  
    Param([String]$Fichier)  
  
    $ConfirmPreference = "Low"  
  
    $info = "Voulez-vous supprimer par la force ce fichier !!!"  
    If ($PSCmdlet.ShouldContinue($info, "Paramètre -Force"))  
    {  
        Remove-Item $Fichier -Force  
    } Else  
    {  
        Write-Host "Annulation de la suppression du fichier !!!" -ForegroundColor Cyan  
    }  
}
```

Si on enregistre la fonction F4 dans un fichier FORCE_F4.PS1

```
PS D:\_OUTILS> D:\_OUTILS\FORCE_F4.ps1  
  
PS D:\_OUTILS> f4 -Fichier "C:\temp\toto.txt"  
  

```

Fonctions avec des variables de type "reference"

Exemple 1

```
function carre([ref]$x)
{
    $x.value = $x.value * $x.value
}

$nombre = 2
Write-Host "Valeur initiale = $nombre" -ForegroundColor Yellow

carre([ref]$nombre)
Write-Host "Valeur modifiée = $nombre" -ForegroundColor Yellow
```

Exemple 2

```
function double
{
    Param ([ref]$x)
    $x.value = $x.value * 2
}

$nombre = 8
Write-Host "Valeur initiale = $nombre" -ForegroundColor Yellow

double([ref]$nombre)
Write-Host "Valeur modifiée = $nombre" -ForegroundColor Yellow
```

Installation d'un module PowerShell

Cette section explique où installer un module PowerShell.

L'emplacement du module varie selon l'utilisation

- Pour un utilisateur spécifique
- Pour tous les utilisateurs

Un module est constitué d'une ou plusieurs fonctions.

Si votre script contient plusieurs fonctions (f1, f2, f3, f4, f5) mais que vous voulez rendre disponibles seulement les fonctions f4 et f5, à la fin du module vous devez ajouter les lignes de code suivantes:

```
Export-ModuleMember -Function f4
Export-ModuleMember -Function f5
```

Les différents dossiers pour les modules

```
$env:PSModulePath -split ';'
```



```
# La commande affiche les trois dossiers
C:\Users\TECH.FORMATION\Documents\WindowsPowerShell\Modules
C:\Program Files\WindowsPowerShell\Modules
C:\Windows\system32\WindowsPowerShell\v1.0\Modules
```

```
C:\Users\TECH.FORMATION\Documents\WindowsPowerShell\Modules
$HOME\Documents\WindowsPowerShell\Modules
```

Ce dossier est utilisé pour ajouter des modules à un utilisateur spécifique.

```
C:\Program Files\WindowsPowerShell\Modules
$env:ProgramFiles\WindowsPowerShell\Modules
```

Ce dossier est utilisé pour ajouter des modules à tous les utilisateurs.

```
C:\Windows\system32\WindowsPowerShell\v1.0\Modules
$PSSHome\Modules
```

Ce dossier est réservé aux modules de Windows.

Il ne faut pas installer des modules dans ce dossier.

Ajout d'un module pour un "utilisateur spécifique"

Pour qu'un utilisateur puisse avoir accès à un module qu'il a créé ou téléchargé à partir d'un site web comme <https://www.powershellgallery.com>, il faut installer le module dans un dossier qui est spécifique à l'utilisateur.

\$HOME\Documents\WindowsPowerShell\Modules\MonModule\MonModule.psm1

IMPORTANT: le nom du dossier **MonModule** et le préfixe du nom du fichier **MonModule.psm1** doivent être exactement le même, sinon PowerShell ne trouvera pas le module.

Ajout d'un module pour "tous les utilisateurs"

Pour que tous les utilisateurs puissent avoir accès à un module qu'un administrateur a créé ou téléchargé à partir d'un site web comme <https://www.powershellgallery.com>, il faut installer le module dans le dossier "**C:\Program Files\WindowsPowerShell\Modules**".

\$env:ProgramFiles\WindowsPowerShell\Modules\MonModule\MonModule.psm1

IMPORTANT: le nom du dossier **MonModule** et le préfixe du nom du fichier **MonModule.psm1** doivent être exactement le même, sinon PowerShell ne trouvera pas le module.

Exemple d'un module PowerShell

```
# Voici le code du fichier EmptyFile.psm1
# Permet de créer rapidement un fichier vide en spécifiant sa taille
function New-EmptyFile
{
    param( [string]$FilePath, [double]$Size )

    # Utilisation d'une classe .NET
    $file = [System.IO.File]::Create($FilePath)
    $file.SetLength($Size)
    $file.Close()

    Get-Item $file.Name
}

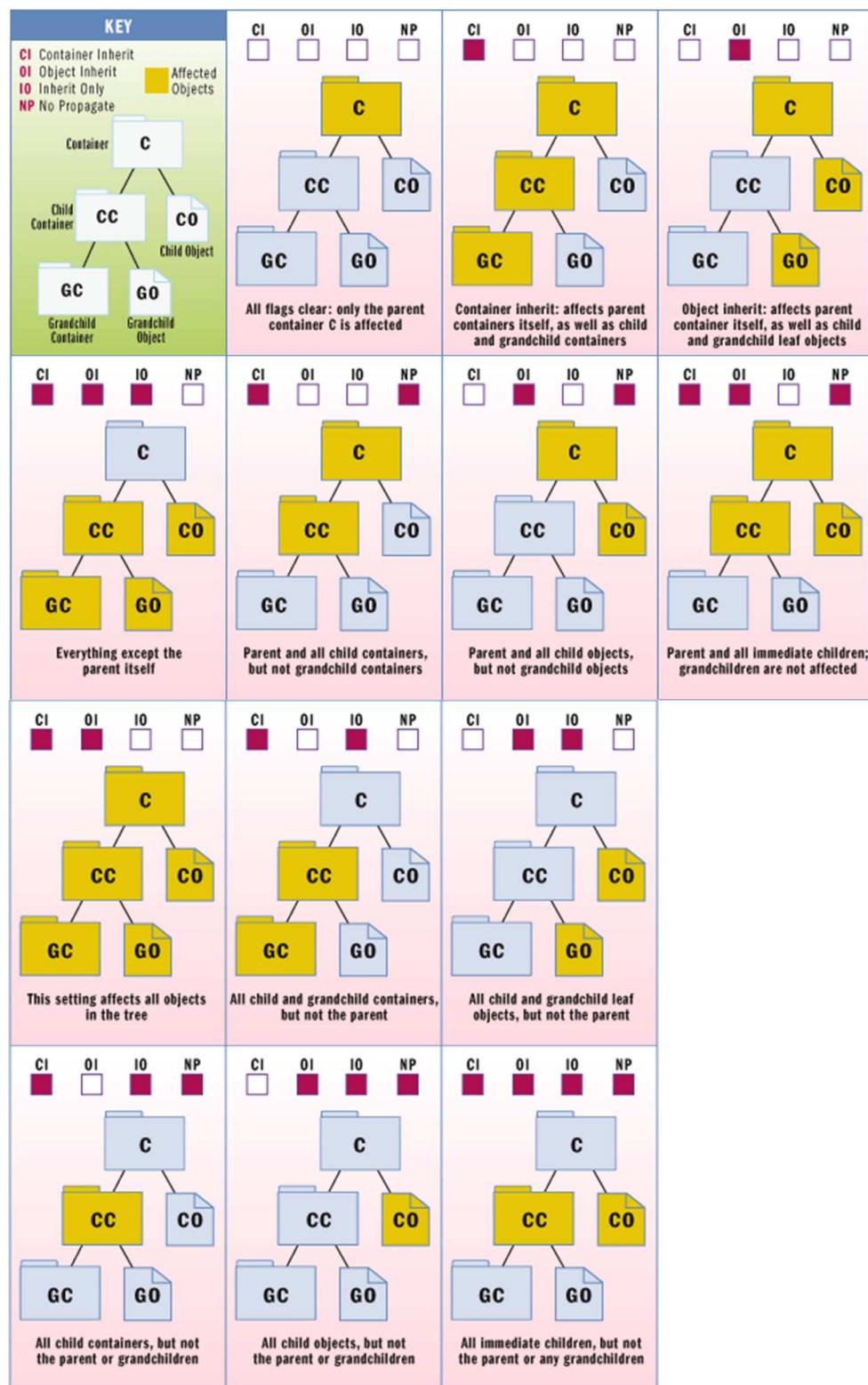
# Voici l'emplacement du fichier EmptyFile.psm1
$HOME\Documents\WindowsPowerShell\Modules\EmptyFile\EmptyFile.psm1

# Exemple d'utilisation de la fonction New-EmptyFile
New-EmptyFile -FilePath c:\_temp\big_file.txt -Size 100gb
```

Répertoire : c:_temp

Mode	LastWriteTime	Length	Name
----	-----	-----	-----
-a---	2023-04-30 08:06	107374182400	big_file.txt

Propagation des autorisations NTFS



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

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

Les autorisations NTFS et la commande ICACLS.EXE

c:\windows\system32\icacls.exe

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

Les codes qui correspondent aux autorisations NTFS de base

F	Accès complet
M	Accès en modification
RX	Accès en lecture et exécution
R	Accès en lecture seule
W	Accès en écriture seule

Exemples:

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

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

takeown.exe

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

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

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

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

icacls.exe "M:\TEST" /reset

Utiliser PowerShell pour exécuter la commande ICACLS

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

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

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

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

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

PowerShell interprète mal les parenthèses de la commande icacls.

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

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

```
$nom = "tout le monde"  
icacls.exe c:\_toto /grant $nom":(OI)(CI)(F)"  
ou  
icacls.exe c:\_toto /grant "${nom}":(OI)(CI)(F)"
```

Utilisation du paramètre --% avec la commande "icacls.exe"

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

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

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

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

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

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

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

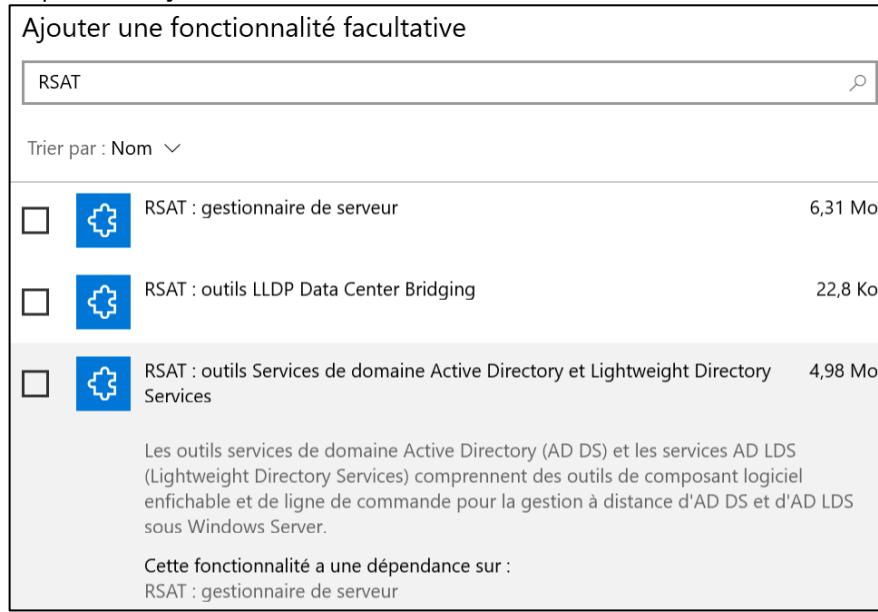
Installation de RSAT en utilisant l'environnement graphique

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



On doit ouvrir "**Applis**"

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



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

Installation de RSAT en utilisant la commande DISM.EXE

Voici la commande pour lister tous les composants facultatifs

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

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

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

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

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

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

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

Cette commande installe la console "Gestionnaire de serveur".

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

Cette commande installe la console "Active Directory".

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

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

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

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

Cette commande désinstalle la console "Gestionnaire de serveur".

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

Installation de RSAT en utilisant PowerShell

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

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

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

Cette commande installe la console "Gestionnaire de serveur"

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

Cette commande installe la console "Active Directory".

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

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

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

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

Cette commande désinstalle la console "Gestionnaire de serveur"

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

Cette commande affiche les consoles RSAT qui sont installées

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

Cette commande affiche les consoles RSAT qui ne sont pas installées

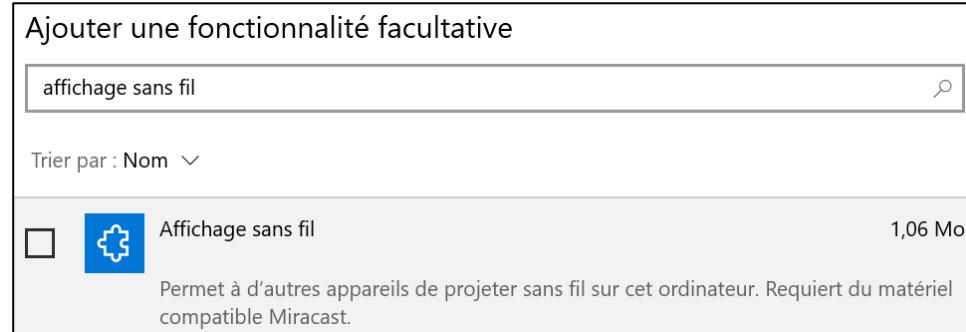
```
Get-WindowsCapability -Online | Where-Object {$PSItem.Name -like "RSAT.*" -and `  
$PSItem.State -eq "NotPresent"}
```

ANNEXE

Fonctionnalité facultative "Affichage sans fil"

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

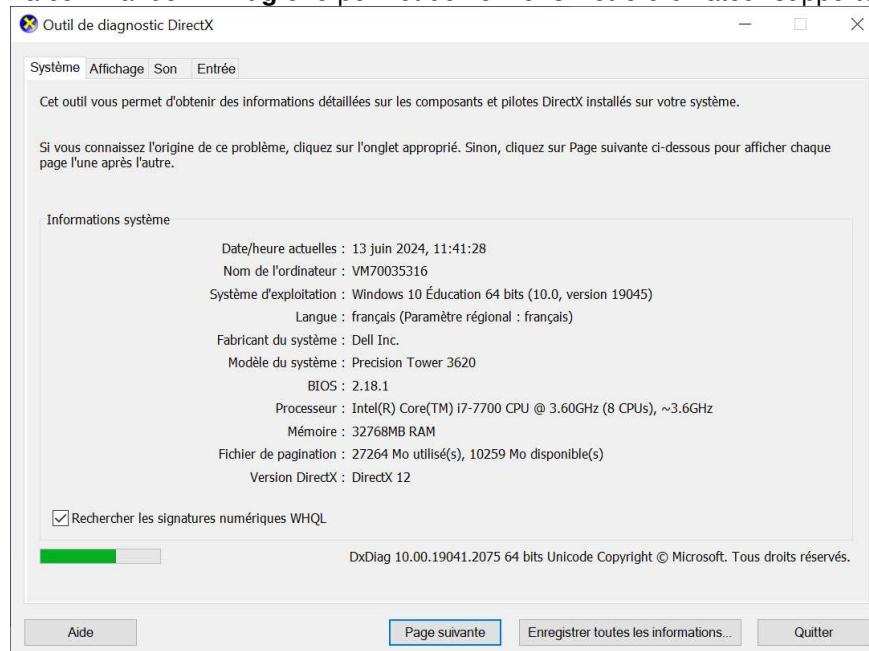
Installation de la fonctionnalité facultative "**Affichage sans fil**" par l'environnement graphique.



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

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

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



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

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

Miracast: Not Available

OU

Miracast: Available, no HDCP

OU

Miracast: Available, with HDCP

Une liste de SID

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

SID	Utilisateur
S-1-5-21-<nombre>-<nombre>-<nombre>-500	Administrateur ou Administrator

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

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

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

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

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

Les propriétés des ordinateurs dans l'Active Directory

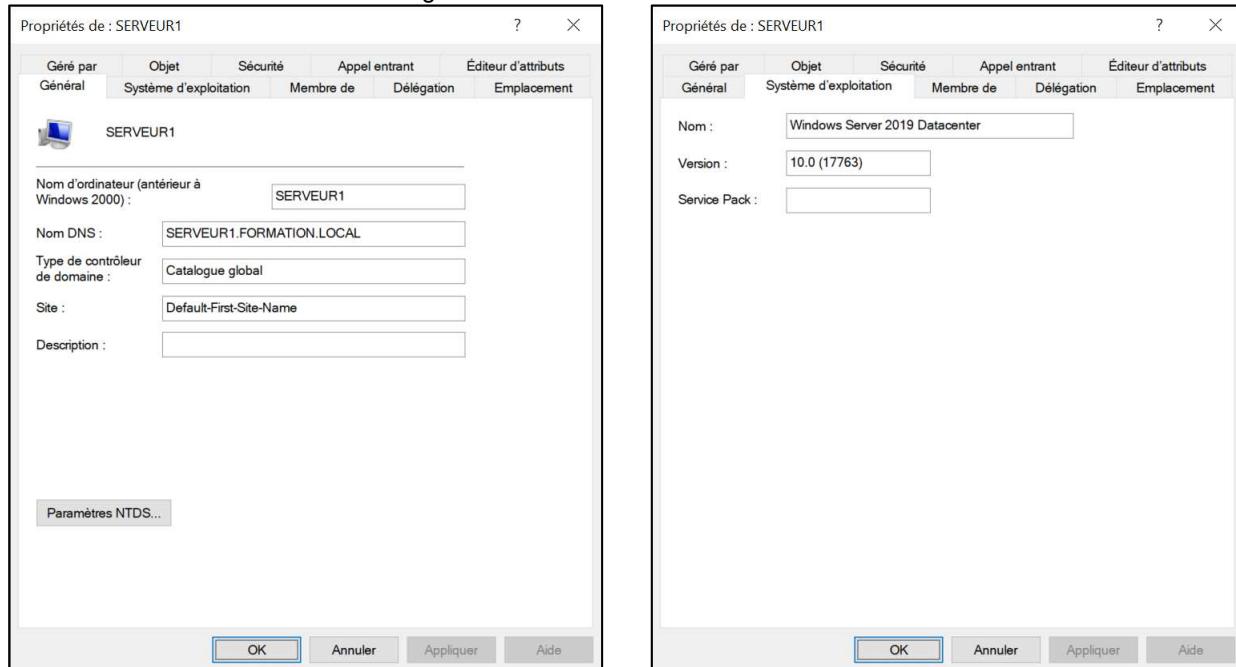
Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

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

Les principaux attributs d'un ordinateur

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



Cette commande affiche plusieurs propriétés du SERVEUR1

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

```
DistinguishedName : CN=SERVEUR1,OU=Domain Controllers,DC=FORMATION,DC=LOCAL
DNSHostName      : SERVEUR1.FORMATION.LOCAL
Enabled          : True
Name              : SERVEUR1
ObjectClass       : computer
ObjectGUID        : a0f468b1-9066-4ea4-9f2b-aa1f2ae20a27
SamAccountName   : SERVEUR1$  

SID              : S-1-5-21-2424922765-3573753519-521296372-1000
UserPrincipalName :
```

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

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

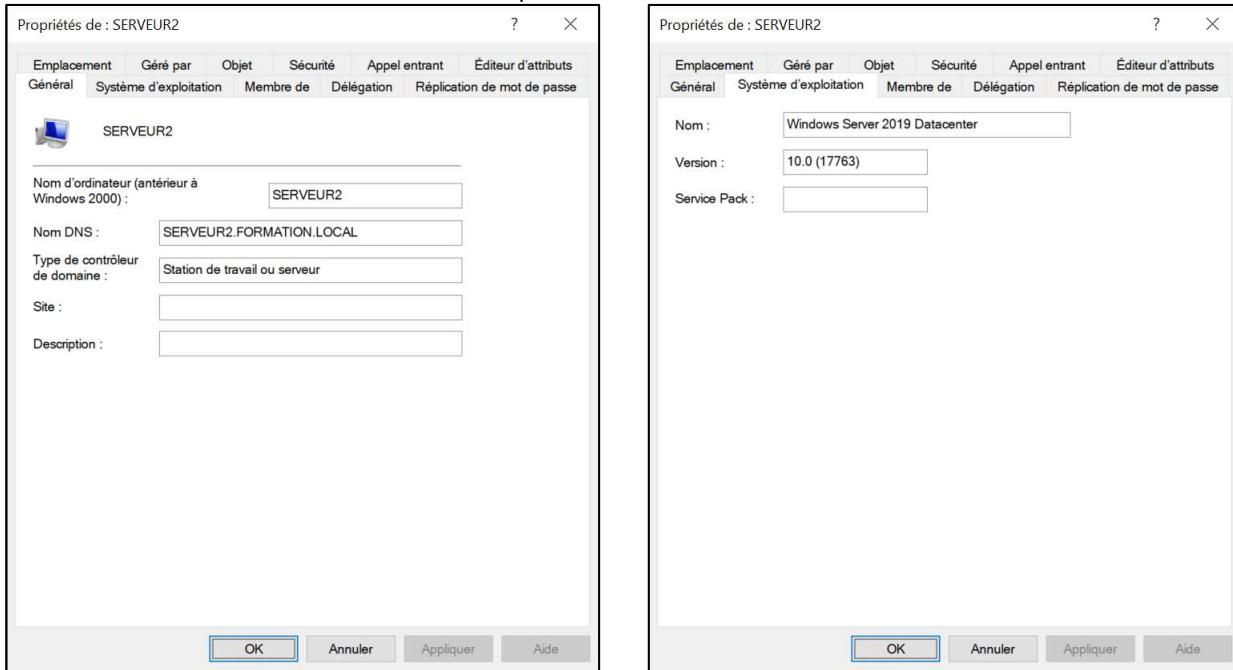
Cette commande affiche des propriétés supplémentaires pour le SERVEUR1
\$serveur = "SERVEUR1"

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

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

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

Le SERVEUR2 est dans le conteneur "Computers".



Cette commande affiche plusieurs propriétés du SERVEUR2

Get-ADComputer -Identity SERVEUR2

```
DistinguishedName : CN=SERVEUR2,CN=Computers,DC=FORMATION,DC=LOCAL
DNSHostName      : SERVEUR2.FORMATION.LOCAL
Enabled          : True
Name              : SERVEUR2
ObjectClass       : computer
ObjectGUID        : 05ce81e5-f68d-4efd-82a1-e210a3cb8db4
SamAccountName   : SERVEUR2$  

SID              : S-1-5-21-2424922765-3573753519-521296372-1103
UserPrincipalName :
```

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

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

Cette commande affiche des propriétés supplémentaires pour le SERVEUR2
\$serveur = "SERVEUR2"

```
Get-ADComputer -Identity $serveur `  
    -Properties CanonicalName,Description,  
        IPv4Address,OperatingSystem,OperatingSystemVersion | `  
Format-List Name,CanonicalName,DistinguishedName,  
    DNSHostName,SamAccountName,  
    Description,IPv4Address,  
    OperatingSystem,OperatingSystemVersion,  
    Enabled  
  
Name : SERVEUR2  
CanonicalName : FORMATION.LOCAL/Computers/SERVEUR2  
DistinguishedName : CN=SERVEUR2,CN=Computers,DC=FORMATION,DC=LOCAL  
DNSHostName : SERVEUR2.FORMATION.LOCAL  
SamAccountName : SERVEUR2$  
Description :  
IPv4Address : 192.168.1.20  
OperatingSystem : Windows Server 2019 Datacenter  
OperatingSystemVersion : 10.0 (17763)  
Enabled : True
```

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

Programmation d'un ordinateur avec PowerShell ISE

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

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

Exemple de création d'un ordinateur avec PowerShell.

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

On veut créer l'ordinateur **SRVWEB1** dans l'unité organisation "WEB".
Le paramètre **-Path** utilise la valeur de l'attribut **DistinguishedName**

```
# Code PowerShell pour ajouter un ordinateur  
New-ADComputer -Name SRVWEB1 `  
    -Path "OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL" `  
    -Description "Serveur WEB principal"
```

Introduction à Active Directory

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

Active Directory partage plusieurs caractéristiques avec une base de données.

Les avantages de l'Active Directory

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

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

Les versions des schémas de l'Active Directory.

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

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

```
Get-ADObject (Get-ADRootDSE).schemaNamingContext -Properties objectVersion
PS C:\Users\Administrateur> Get-ComputerInfo | Select-Object WindowsProductName,WindowsVersion
WindowsProductName          WindowsVersion
-----                    -----
Windows Server 2019 Datacenter 1809

PS C:\Users\Administrateur> Get-ADObject (Get-ADRootDSE).schemaNamingContext -Properties objectVersion
DistinguishedName : CN=Schema,CN=Configuration,DC=FORMATION,DC=LOCAL
Name              : Schema
ObjectClass       : dMD
ObjectGUID        : af7dd477-62e8-4443-8469-cbc5b4475bf8
objectVersion     : 88

PS C:\Users\Administrateur>
```

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

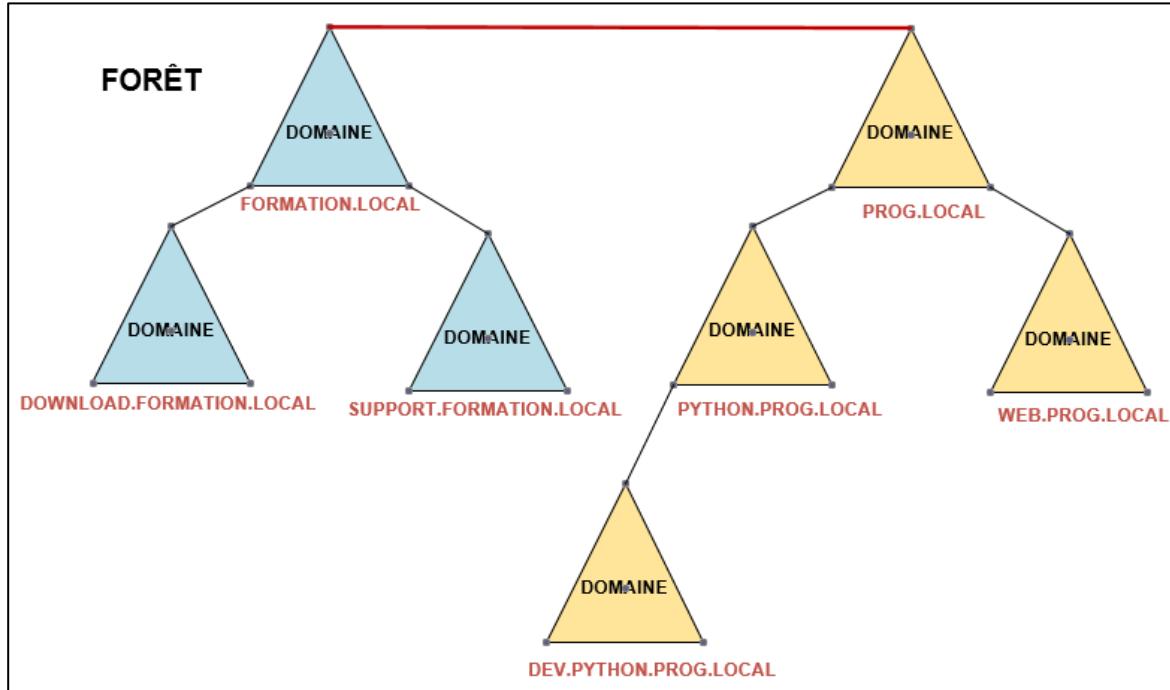
Le nombre d'objet maximum est $2^{31} - 255 = 2\ 147\ 483\ 648 - 255 = 2\ 147\ 483\ 393$

Aperçu d'une structure "Active Directory"

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

Les objets sont classés en trois grandes catégories:

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



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

Catalogue global

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

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

Installation de l'Active Directory en mode graphique

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

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

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

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

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

Les partages administratifs (NETLOGON, SYSVOL)

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

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

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

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

Le partage SYSVOL est répliqué entre les contrôleurs de domaine.

Le partage SYSVOL contient deux dossiers

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

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

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

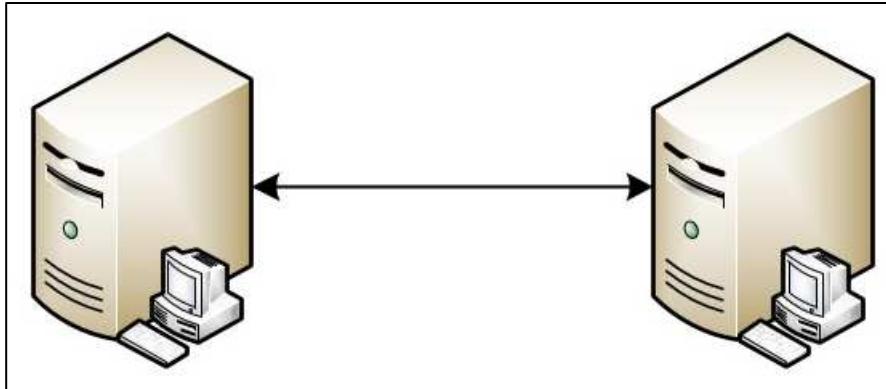
Cette console est plus récente que la console "Utilisateurs et ordinateurs Active Directory".

ANNEXE 1

"Active Directory" avec deux contrôleurs de domaine

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

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



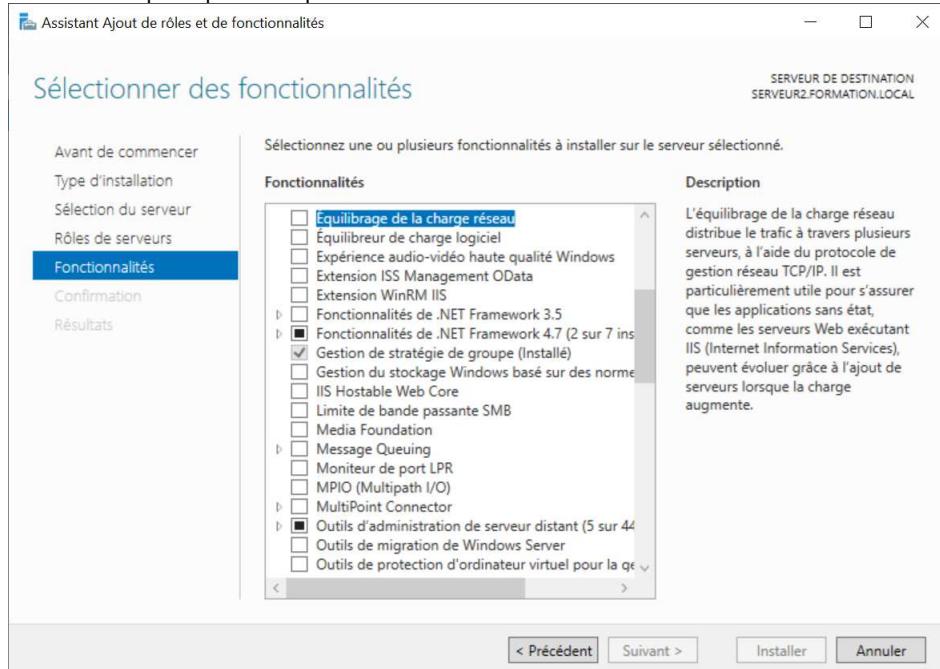
Les contrôleurs de domaine répliquent les informations entre eux à intervalle régulier, afin de disposer d'un annuaire Active Directory identique. En plus, les contrôleurs de domaine répliquent le contenu du dossier "SYSVOL" qui est utilisé pour distribuer les stratégies de groupe et les scripts de connexion.

ANNEXE 2

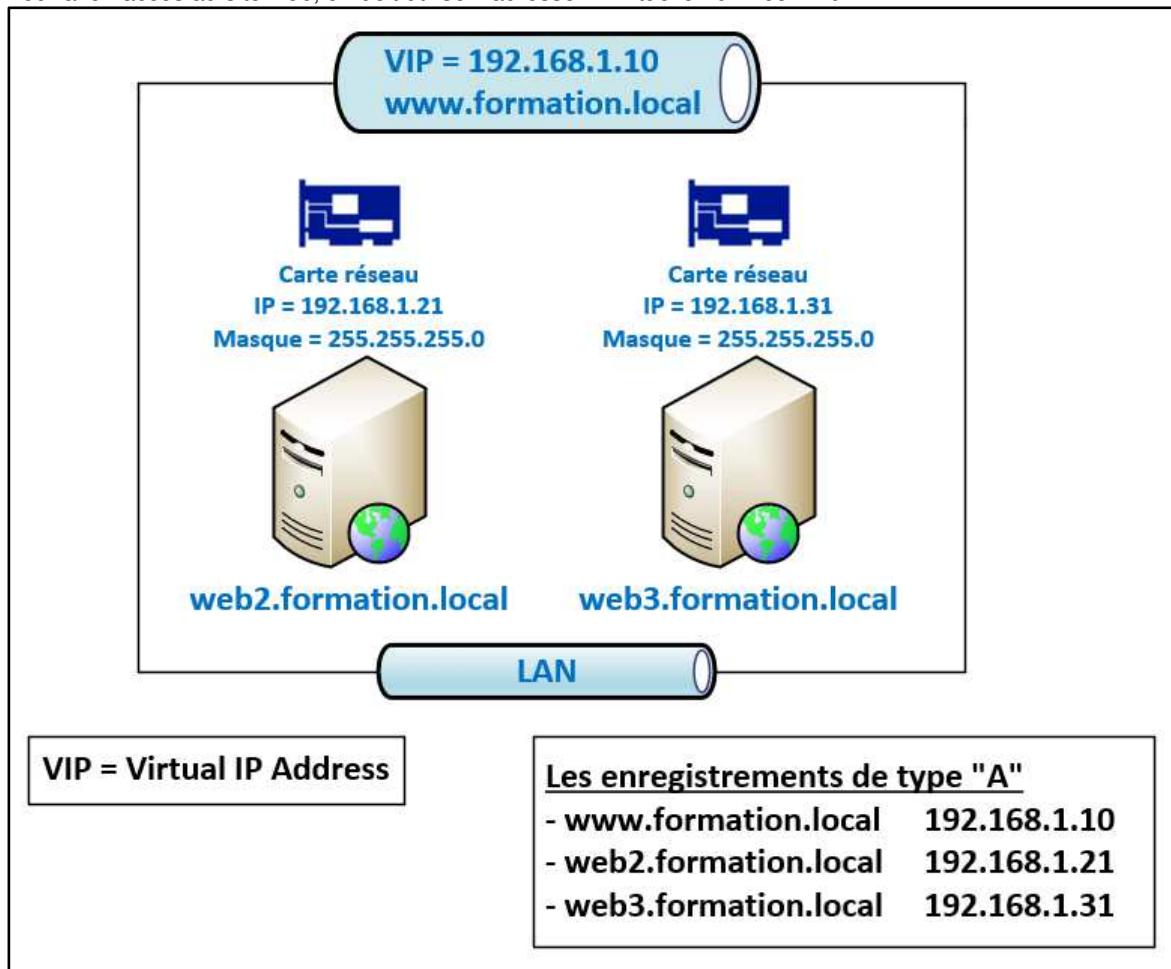
La fonctionnalité "Équilibrage de la charge réseau"

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

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



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

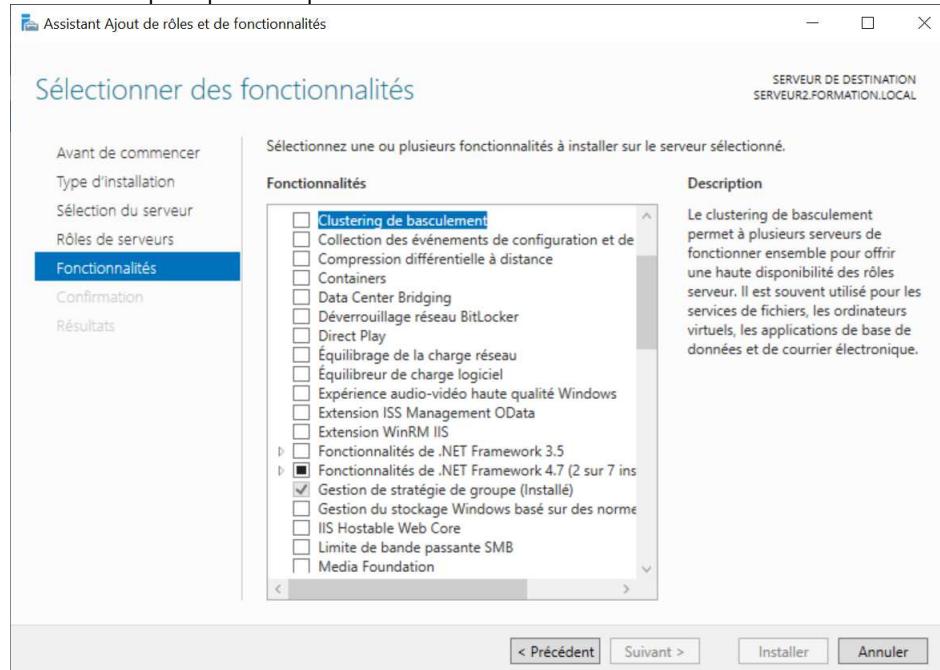


ANNEXE 3

La fonctionnalité "Clustering de basculement"

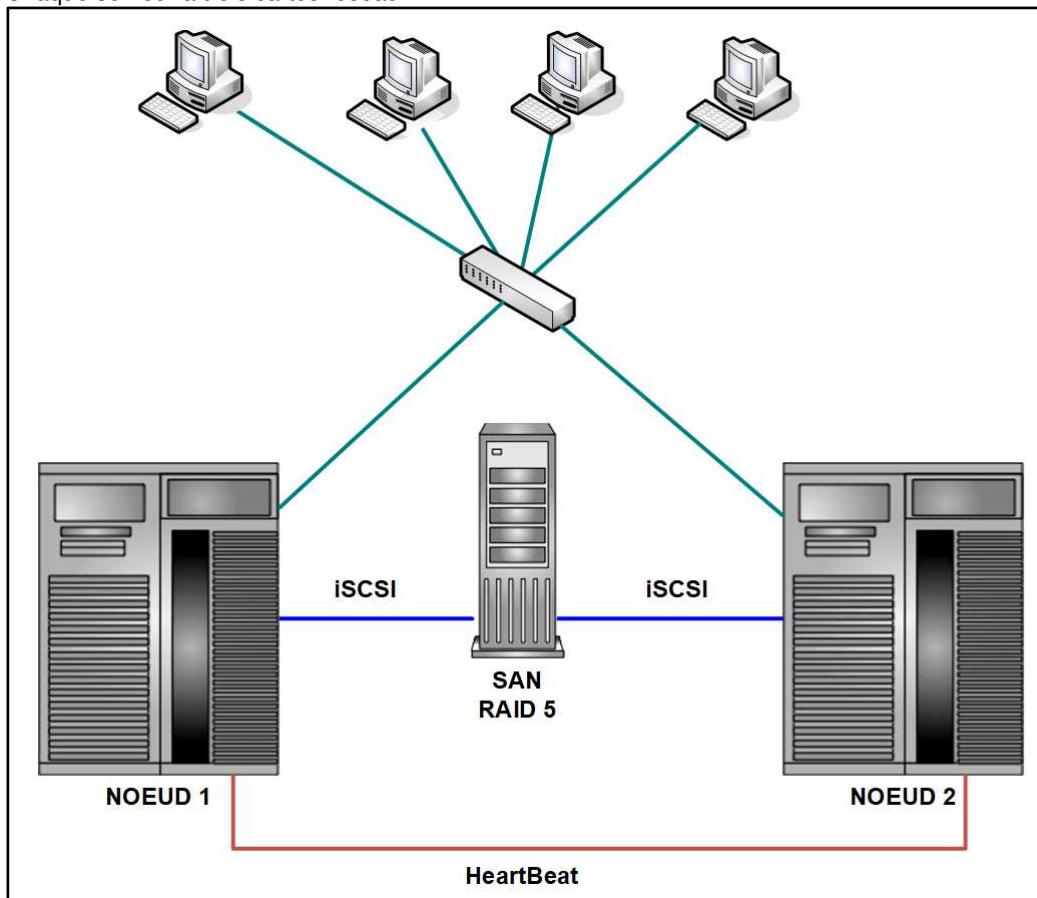
Dans le cours, nous n'utiliserons pas la fonctionnalité "Clustering de basculement".

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



Voici un schéma d'un cluster de basculement.

Chaque serveur a trois cartes réseau.

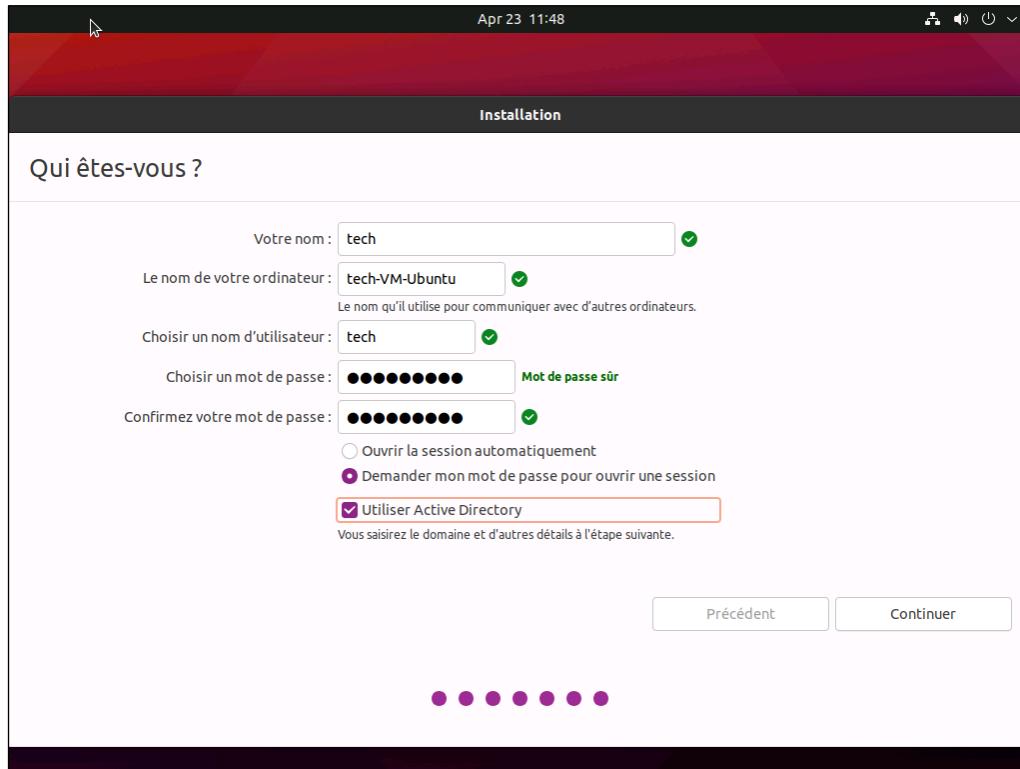


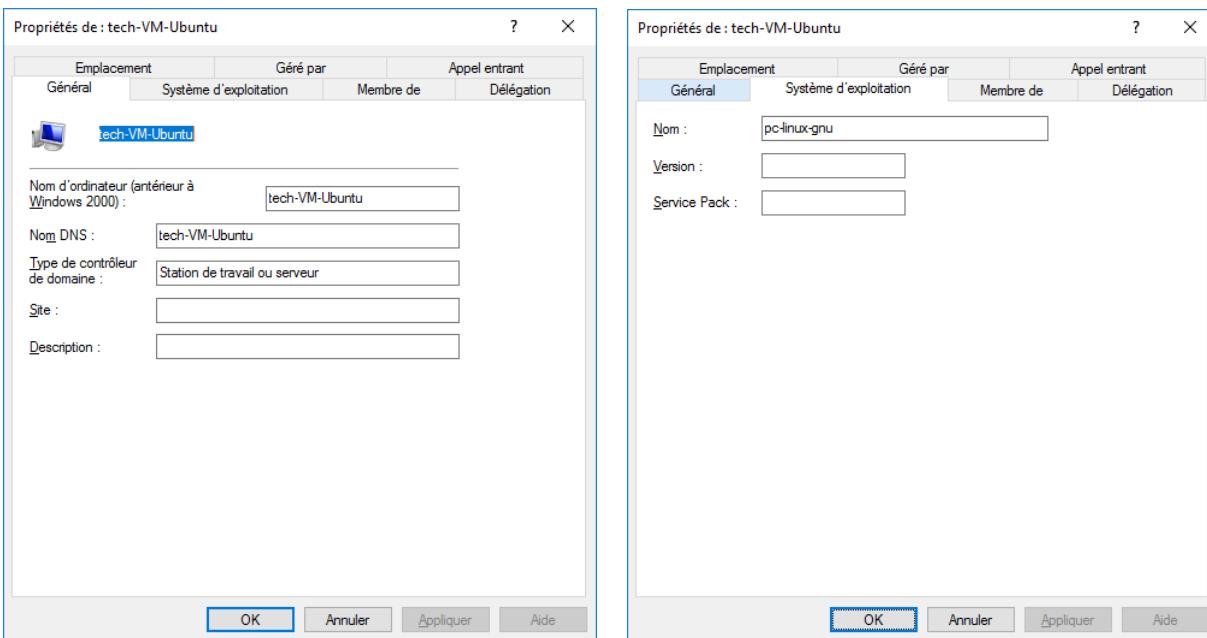
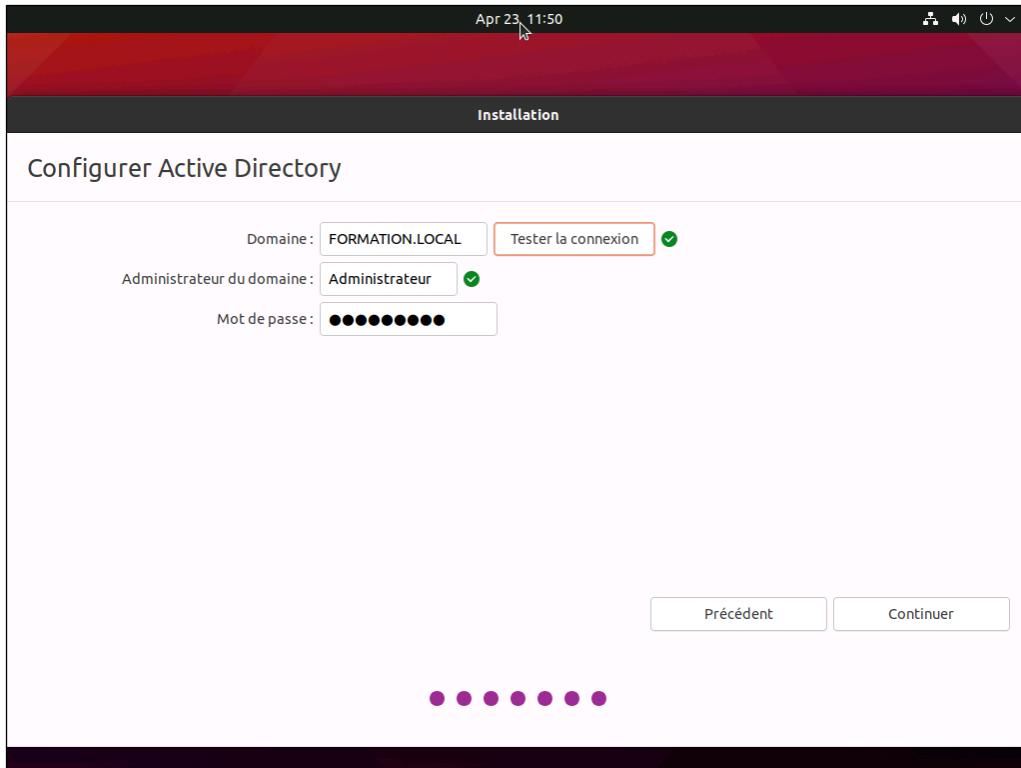
ANNEXE 4
"Active Directory" et Linux

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

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

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





Installation de l'Active Directory

Objectifs

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

Matériaux

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

Étape 1 - Vérification du contrôleur de domaine

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

Vérifier la configuration du serveur virtuel "SERVEUR1"

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

Étape 2 - Création d'un domaine

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

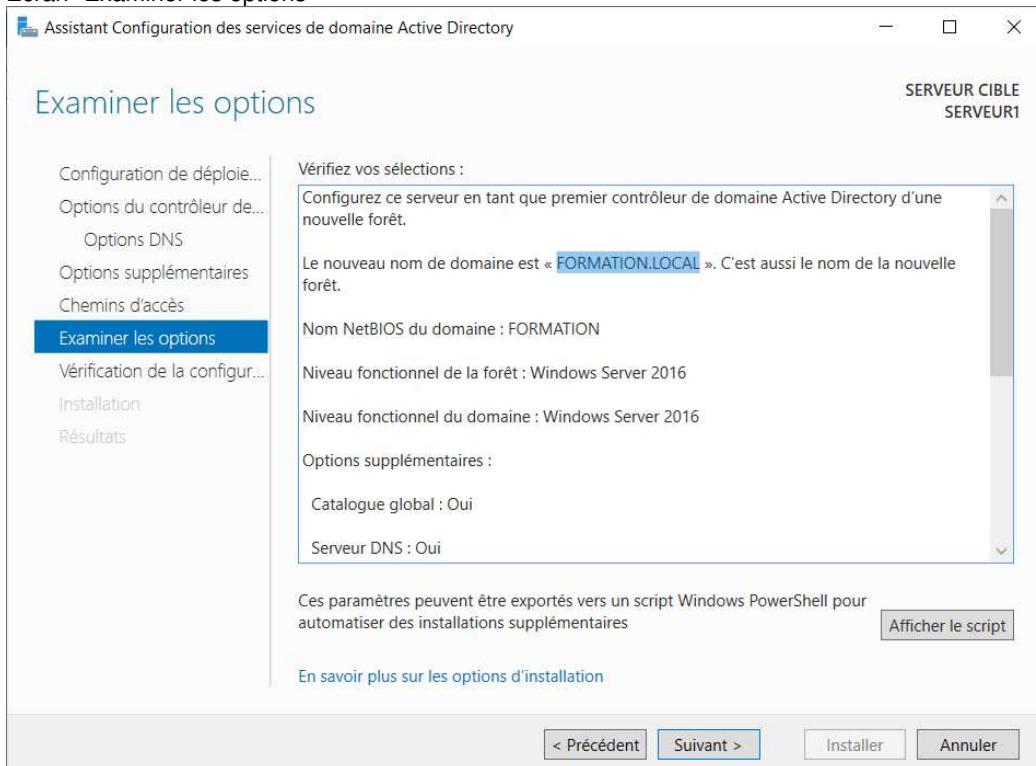
Installer le rôle "Services AD DS"

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

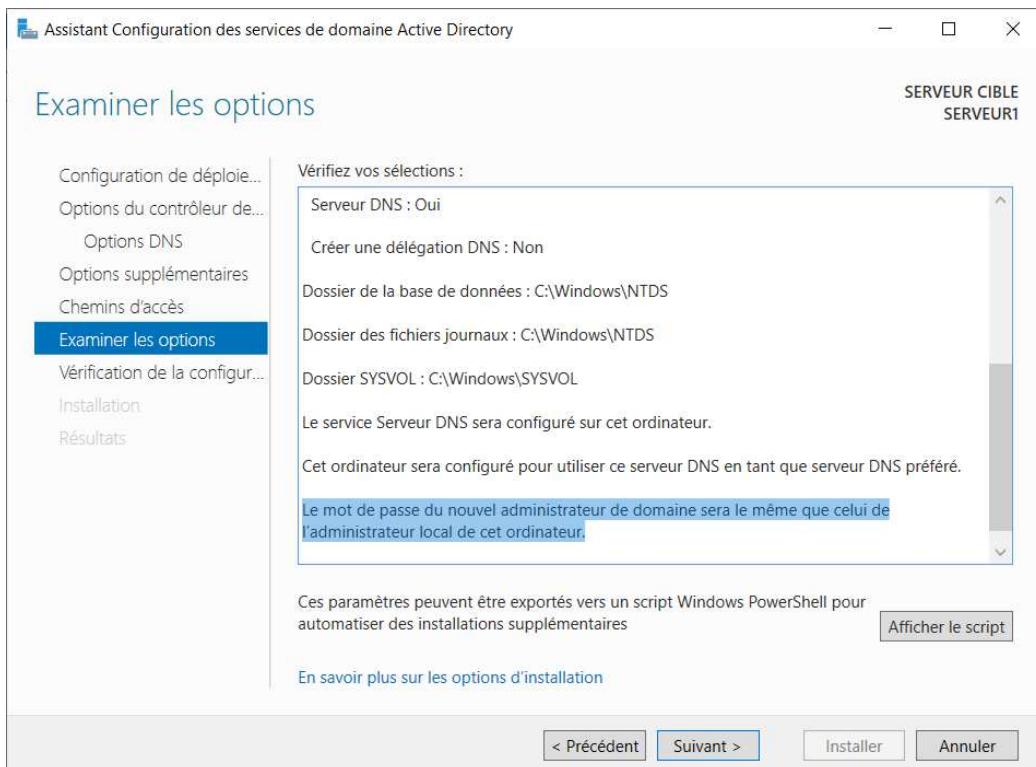
Répondre aux questions de la post-configuration du domaine

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

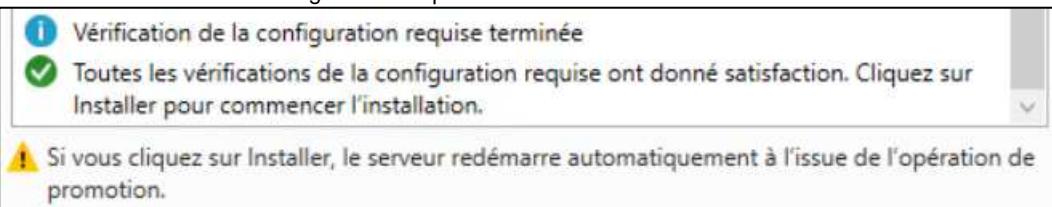
● Écran "Examiner les options"



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



- Écran "Vérification de la configuration requise"



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

Étape 3 - Validation du domaine

Connectez-vous sur le contrôleur de domaine.

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

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

Dans une invite de commandes exécuter la commande suivante

ping SERVEUR1.FORMATION.LOCAL -4

Vérifier la présence des partages: NETLOGON et SYSVOL

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

Étape 4 - Joindre le SERVEUR2 au domaine

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

Vérifier la configuration du serveur virtuel "SERVEUR2"

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

Joindre l'ordinateur à votre domaine

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

Cliquer sur "Modifier les paramètres"

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

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

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

Canal sécurisé entre un ordinateur et le contrôleur de domaine

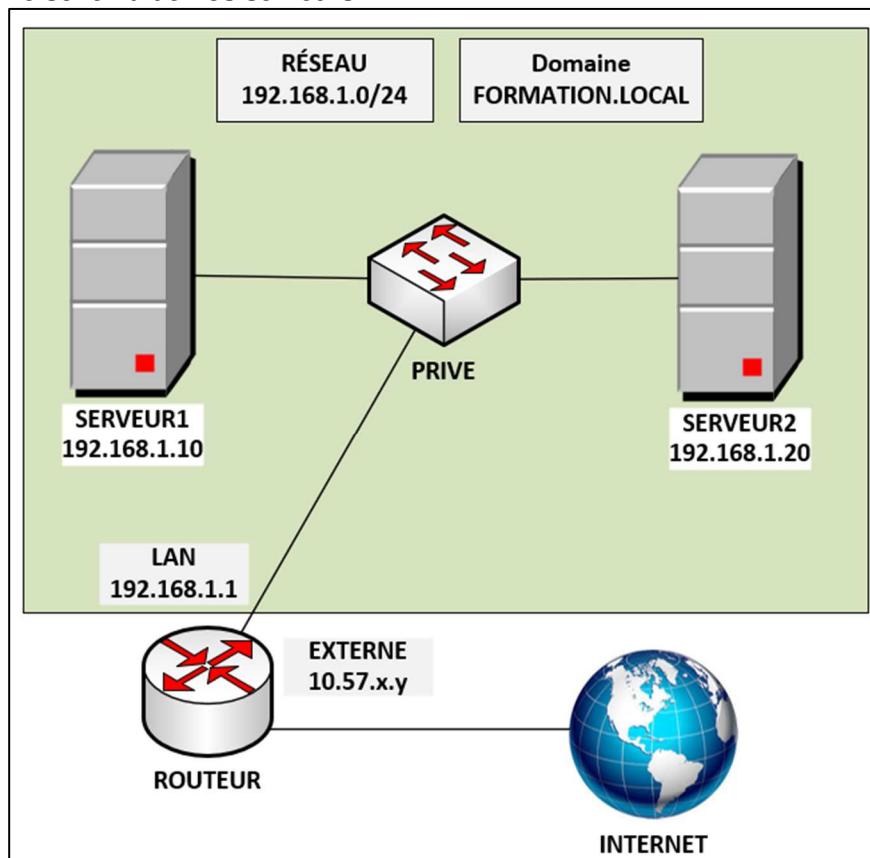
Lorsqu'un ordinateur est joint au domaine, un compte ordinateur est créé.

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

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

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

Le schéma de nos serveurs.



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

Utilisation d'un compte de l'Active Directory

- FORMATION\Administrateur
- Administrateur@formation.local

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



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

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

Utilisation d'un compte local du SERVEUR2

- Administrateur
- .\Administrateur
- SERVEUR2\Administrateur

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



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

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

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

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

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

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

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

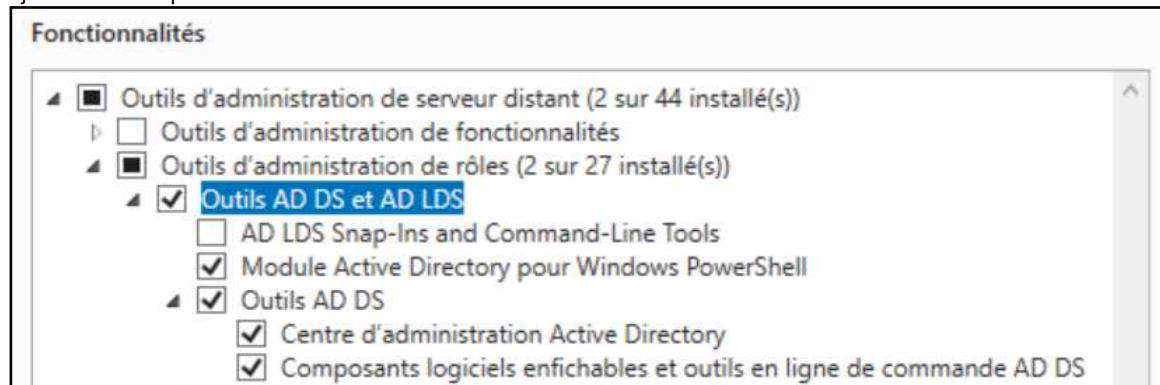
Étape 6 – Installer la console UOAD sur le SERVEUR2

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

Installer les outils d'administration

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

- ajouter les composants suivants



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

ANNEXE

Comment sortir un ordinateur du domaine

Vous devez utiliser ces commandes en cas de besoin seulement.

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

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

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

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

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

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

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

The screenshot shows the ADUC interface. On the left, there's a navigation pane with a tree view of the Active Directory structure under 'Utilisateurs et ordinateurs Active Directory [SERVEUR1.FORMATION.LOCAL]'. The 'Domain Controllers' node is selected. On the right, a table displays the properties of the 'Domain Controllers' container:

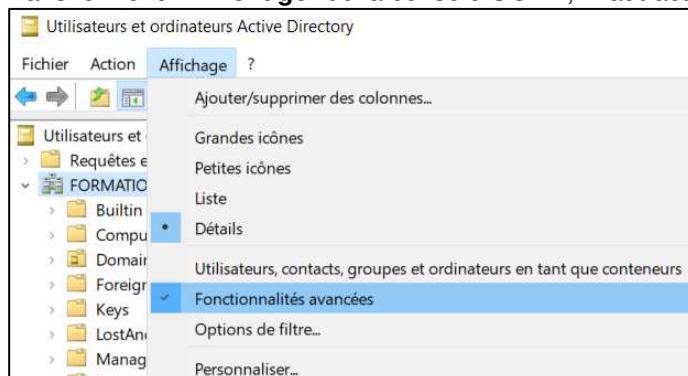
Nom	Type	Description
Builtin	builtInDomain	Default container for upgraded computer accounts
Computers	Conteneur	Default container for domain controllers
Domain Controllers	Unité d'organisation	Default container for security identifiers (SIDs) associated with objects from external, trusted domains
ForeignSecurityPrincipals	Conteneur	Default container for managed service accounts
Managed Service Accounts	Conteneur	Default container for upgraded user accounts
Users	Conteneur	

Chaque objet de l'Active Directory a des attributs.

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

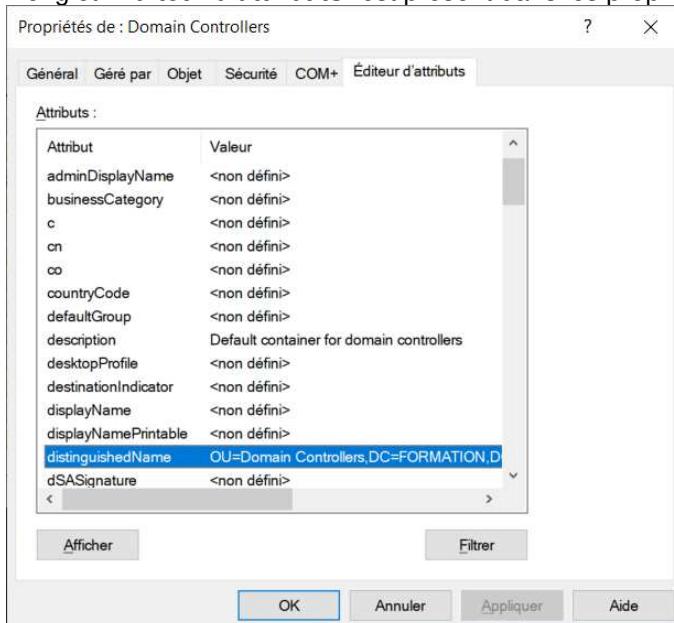
The screenshot shows the 'Propriétés de : Domain Controllers' dialog box. The 'Général' tab is selected. The 'Domain Controllers' object is identified by a small icon. The 'Description' field contains the value 'Default container for domain controllers'. Below it, there are fields for 'Adresse', 'Ville', 'Département ou', 'Code postal', and 'Pays/région', all of which are currently empty. At the bottom, there are 'OK', 'Annuler' (Cancel), and 'Appliquer' (Apply) buttons.

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



Nom	Type	Description
Builtin	builtInDomain	Default container for upgraded computer accounts
Computers	Conteneur	Default container for domain controllers
Domain Controllers	Unité d'organisation	Default container for security identifiers (SIDs) associated with objects from external, trusted domains
ForeignSecurityPrincipals	Conteneur	
Infrastructure	infrastructureUpdate	
Keys	Conteneur	Default container for key objects
LostAndFound	lostAndFound	Default container for orphaned objects
Managed Service Accounts	Conteneur	Default container for managed service accounts
NTDS Quotas	msDS-QuotaContainer	Quota specifications container
Program Data	Conteneur	Default location for storage of application data.
System	Conteneur	Builtin system settings
Users	Conteneur	Default container for upgraded user accounts
TPM Devices	msTPM-InformationObjectsContainer	

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



La propriété DistinguishedName est très importante.

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

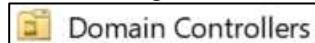
L'attribut DistinguishedName

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

Attribut	Description
DC	Domain Component
CN	Common Name
OU	Organizational Unit

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

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



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

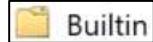
NOTE: Un Administrateur peut créer des unités d'organisation.



OU=Utilisateurs,DC=FORMATION,DC=LOCAL

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

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



CN=Builtin,DC=FORMATION,DC=LOCAL



CN=Computers,DC=FORMATION,DC=LOCAL



CN=Users,DC=FORMATION,DC=LOCAL

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

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

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



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

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

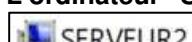
Le groupe "Administrateurs" est dans le conteneur "BuiltIn".



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

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

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



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

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



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

Création d'un utilisateur dans l'Active Directory

Objectifs

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

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

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

Création de l'utilisateur TECH dans l'Active Directory

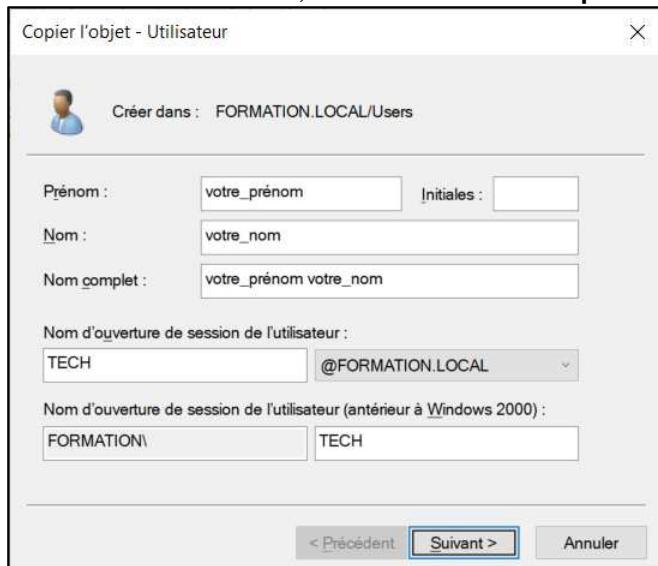
**De préférence, chaque étudiant doit travailler sur un serveur membre.
Je vous suggère de ne pas travailler directement sur le contrôleur de domaine.**

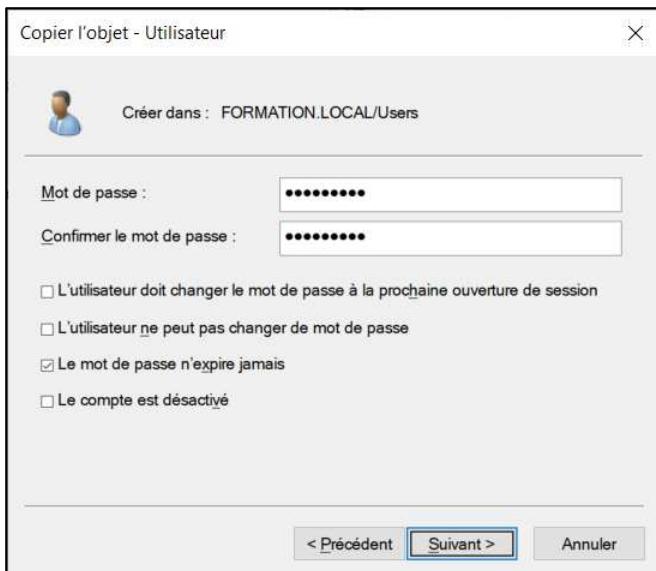
Connectez-vous sur le "SERVEUR2" avec l'utilisateur "FORMATION\Administrateur".

Démarrer la console "Utilisateurs et Ordinateurs Active Directory"

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

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





Mot de passe

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

● Vérification des deux utilisateurs

Propriétés de : TECH

Général	Adresse	Compte	Profil	Téléphones	Organisation	Certificats publiés

Membre de :

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

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Definir le groupe principal

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

OK Annuler Appliquer Aide

Propriétés de : Administrateur

Général	Adresse	Compte	Profil	Téléphones	Organisation	Certificats publiés

Membre de :

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

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Definir le groupe principal

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

OK Annuler Appliquer Aide

Les deux utilisateurs sont membres des mêmes groupes.

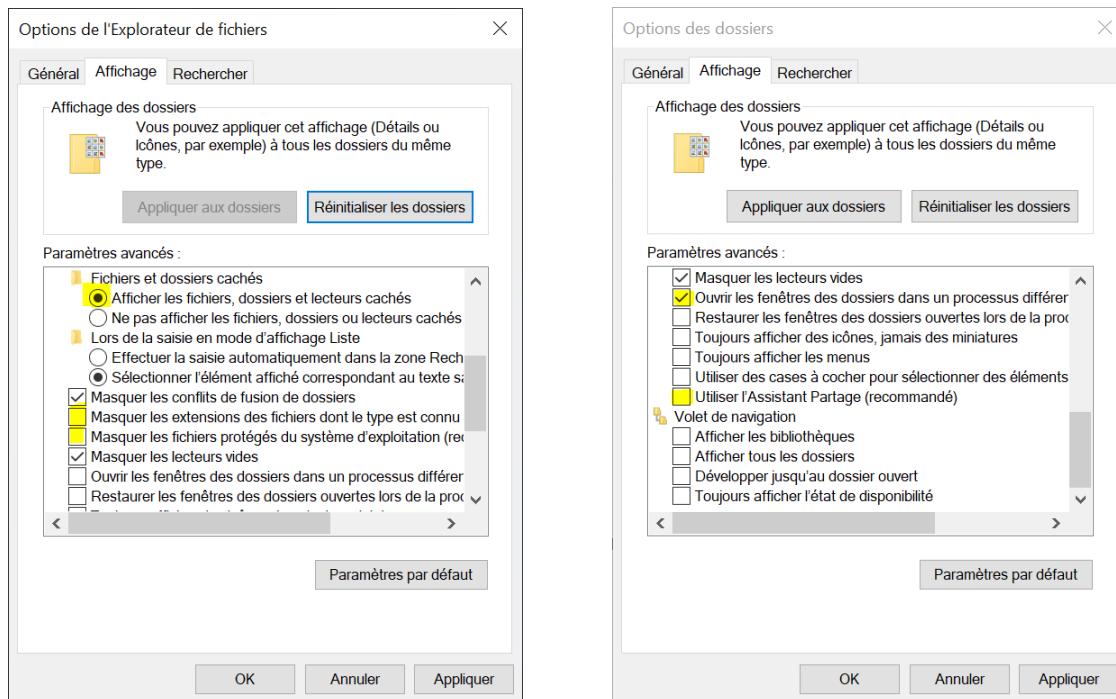
À PARTIR DE MAINTENANT, VOUS NE DEVEZ PLUS UTILISER LE COMPTE "ADMINISTRATEUR" DU DOMAINE.

Configurations pour l'utilisateur TECH sur le SERVEUR2

Explorateur de fichiers - Affichage - Options des dossiers

Onglet Affichage

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



Gestionnaire de serveur - Serveur local

Dans les **Propriétés** de votre serveur

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

Vous devez installer au moins un des navigateurs web

Voici les liens pour télécharger les versions complètes de trois navigateurs

Chrome

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

Edge Chromium

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

Firefox

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

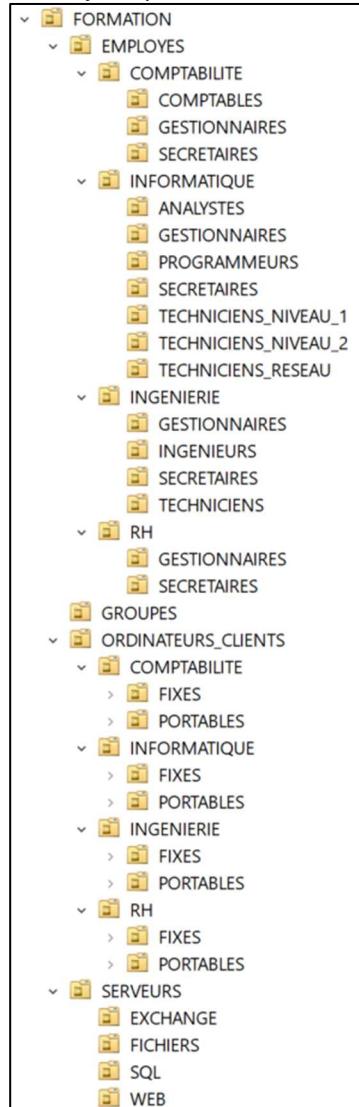
Les propriétés des unités d'organisation dans l'Active Directory

Objectifs

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

Le but d'une unité d'organisation

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



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

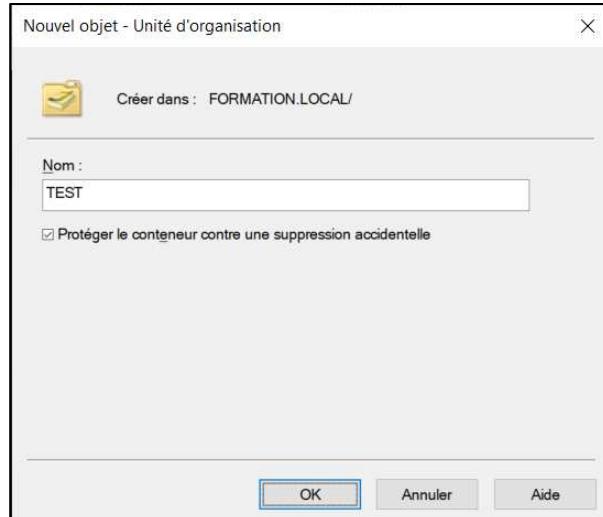
Les attributs d'une unité d'organisation

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

- Vérifier que votre affichage est en "Fonctionnalités Avancées"

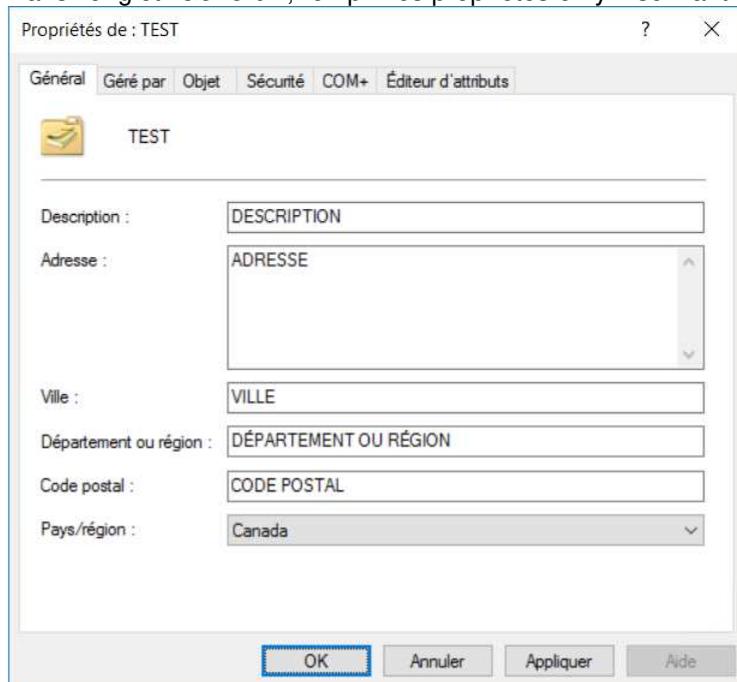
Selectionner le domaine "FORMATION\LOCAL" et créer l'unité d'organisation "TEST".

Pour créer une OU, il faut donner un nom.

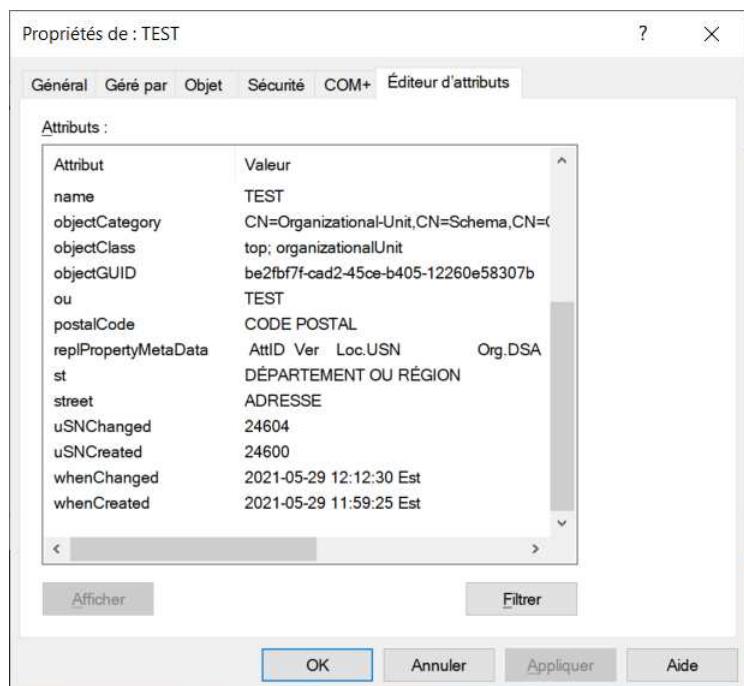
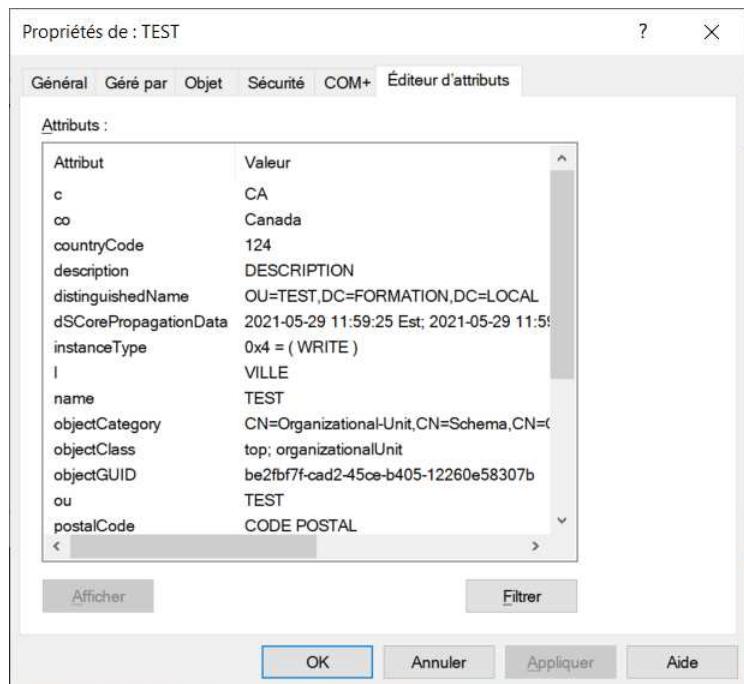


Par défaut, le paramètre "Protéger le conteneur contre une suppression accidentelle" est activé.
Cliquer sur le bouton "OK"

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



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



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

Trouvez la valeur pour les attributs suivants:

Nom de l'attribut	Valeur de l'attribut
DistinguishedName	OU=TEST,DC=FORMATION,DC=LOCAL
name	test
ou	test
WhenChanged	2019-05-29 12:12:30 Est
WhenCreated	2019-05-29 11:59:25 Est

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

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

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

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

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

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

Méthode avec le paramètre -Country

On veut créer l'unité organisationnelle "Stade_version_1" qui sera directement sous le domaine.

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

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

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

Attribut	Valeur
adminDescription	<non défini>
adminDisplayName	<non défini>
businessCategory	<non défini>
c	CA
cn	<non défini>
co	<non défini>
countryCode	<non défini>
defaultGroup	<non défini>
description	Stade olympique de Montréal
desktopProfile	<non défini>
destinationIndicator	<non défini>
displayName	<non défini>
displayNamePrintable	<non défini>
distinguishedName	OU=Stade_version_1,DC=FORMATION,DC=local

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

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

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

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

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

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

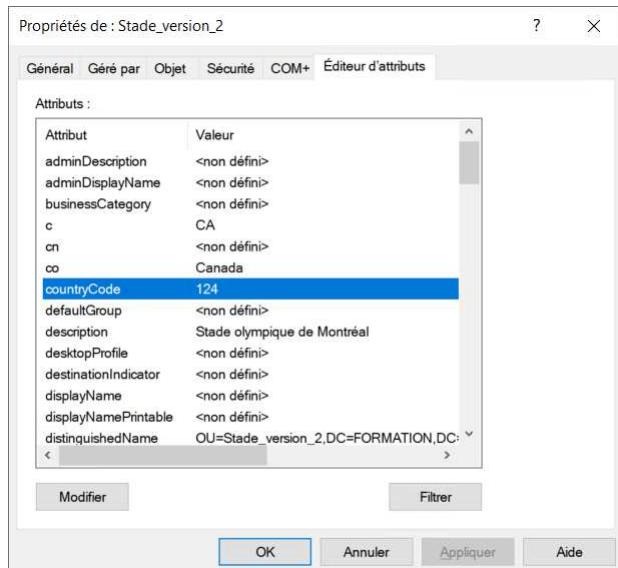
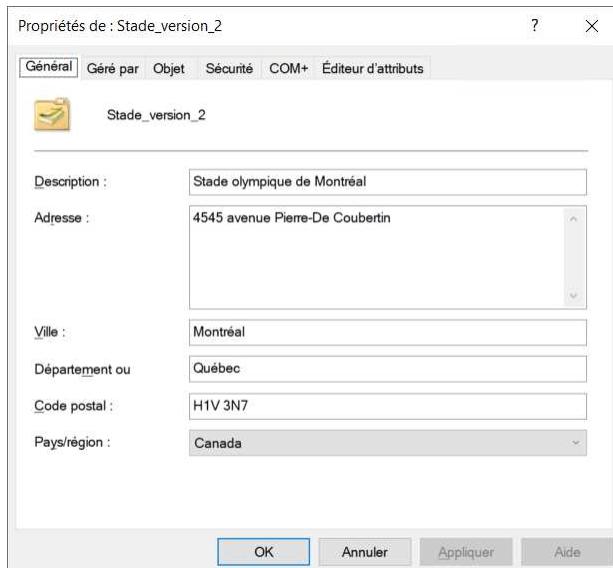
Méthode avec le paramètre -OtherAttributes

On veut créer l'unité organisationnelle "Stade_version_2" qui sera directement sous le domaine.

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

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

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



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

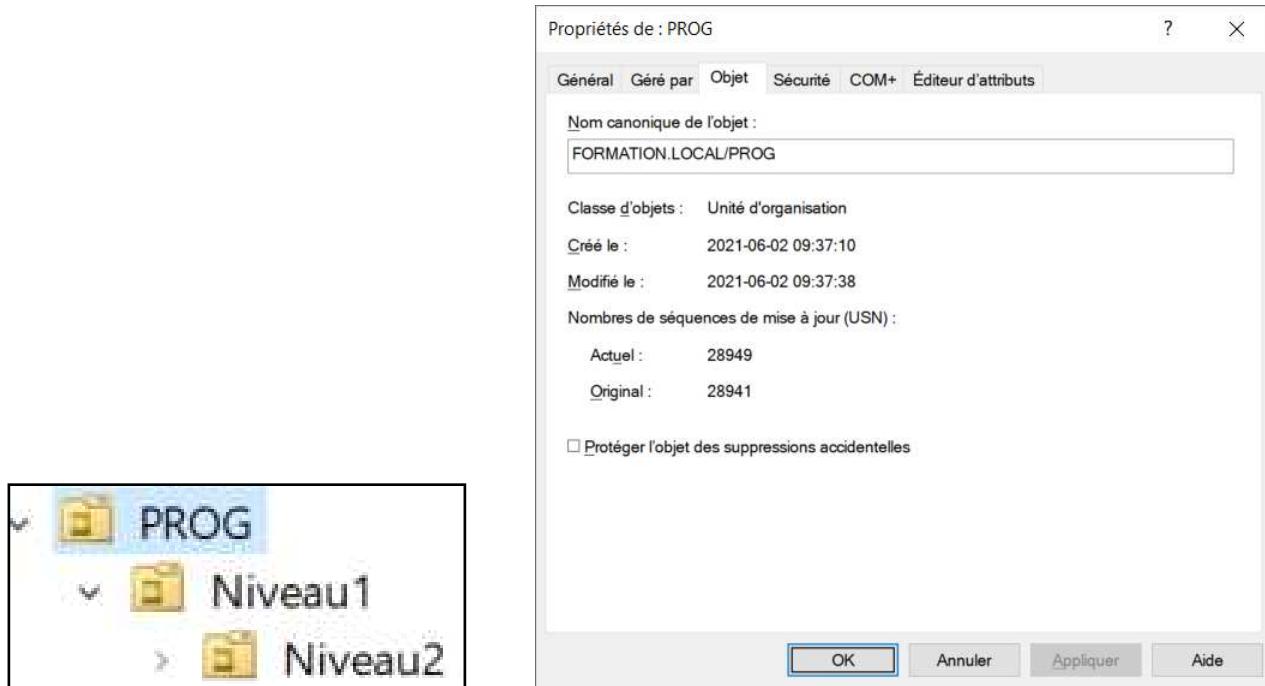
Sur l'onglet "Éditeur d'attributs" les attributs co et countryCode ont des valeurs.

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

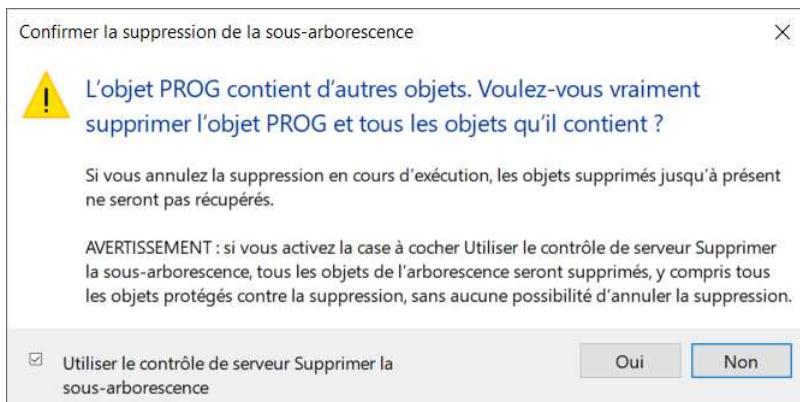
Conclusion: il est préférable d'utiliser le paramètre **-OtherAttributes** avec les trois attributs **c**, **co** et **countryCode**.

Supprimer une unité d'organisation par l'environnement graphique

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



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



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

Supprimer une unité d'organisation par programmation PowerShell

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

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

Enlève la protection contre la suppression accidentelle

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

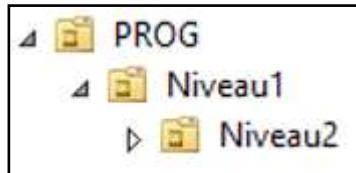
Pour supprimer l'unité d'organisation "PROG"

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

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

Exercice

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



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

Programmation d'une structure d'unité d'organisation

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

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

Description du travail

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

Notes techniques

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

Vous devez ajouter des commentaires pertinents dans votre code.

Vous devez utiliser des variables.

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

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

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

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

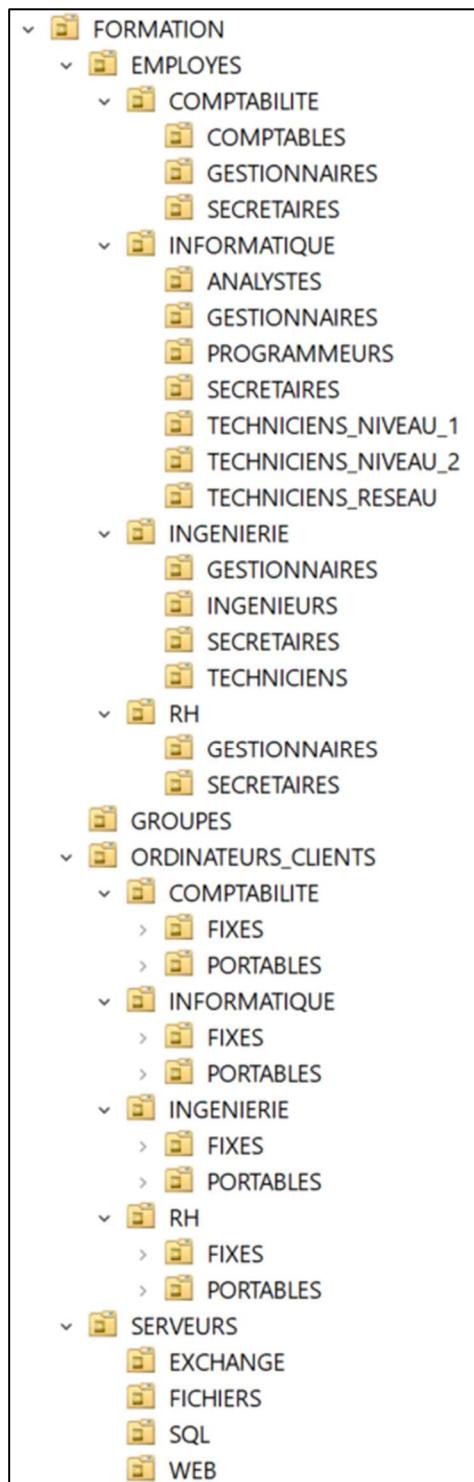
**OU=FORMATION,DC=formation,DC=local n'existe pas.
Création de 41 unités d'organisation.**

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

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

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

Voici la structure des 41 unités d'organisation



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

CanonicalName

FORMATION.LOCAL/FORMATION
FORMATION.LOCAL/FORMATION/EMPLOYES
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE/COMPTABLES
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE/GESTIONNAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/COMPTABILITE/SECRETAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/ANALYSTES
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/GESTIONNAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/PROGRAMMEURS
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/SECRETAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/TECHNICIENS_NIVEAU_1
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/TECHNICIENS_NIVEAU_2
FORMATION.LOCAL/FORMATION/EMPLOYES/INFORMATIQUE/TECHNICIENS_RESEAU
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/GESTIONNAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/INGENIEURS
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/SECRETAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/INGENIERIE/TECHNICIENS
FORMATION.LOCAL/FORMATION/EMPLOYES/RH
FORMATION.LOCAL/FORMATION/EMPLOYES/RH/GESTIONNAIRES
FORMATION.LOCAL/FORMATION/EMPLOYES/RH/SECRETAIRES
FORMATION.LOCAL/FORMATION/GROUPES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/COMPTABILITE
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/COMPTABILITE/FIXES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/COMPTABILITE/PORTABLES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/INFORMATIQUE
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/INFORMATIQUE/FIXES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/INFORMATIQUE/PORTABLES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/INGENIERIE
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/INGENIERIE/FIXES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/INGENIERIE/PORTABLES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/RH
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/RH/FIXES
FORMATION.LOCAL/FORMATION/ORDINATEURS_CLIENTS/RH/PORTABLES
FORMATION.LOCAL/FORMATION/SERVEURS
FORMATION.LOCAL/FORMATION/SERVEURS/EXCHANGE
FORMATION.LOCAL/FORMATION/SERVEURS/FICHIER
FORMATION.LOCAL/FORMATION/SERVEURS/SQL
FORMATION.LOCAL/FORMATION/SERVEURS/WEB

Informations sur les unités d'organisation de l'unité d'organisation FORMATION**DistinguishedName**

OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=COMPTABILITE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=COMPTABLES, OU=COMPTABILITE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=GESTIONNAIRES, OU=COMPTABILITE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=SECRETAIRES, OU=COMPTABILITE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=ANALYSTES, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=GESTIONNAIRES, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=PROGRAMMEURS, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=SECRETAIRES, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=TECHNICIENS_NIVEAU_1, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=TECHNICIENS_NIVEAU_2, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=TECHNICIENS_RESEAU, OU=INFORMATIQUE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=INGENIERIE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=GESTIONNAIRES, OU=INGENIERIE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=INGENIERS, OU=INGENIERIE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=SECRETAIRES, OU=INGENIERIE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=TECHNICIENS, OU=INGENIERIE, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=RH, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=GESTIONNAIRES, OU=RH, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=SECRETAIRES, OU=RH, OU=EMPLOYES, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=GROUPEs, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=COMPTABILITE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=FIXES, OU=COMPTABILITE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=PORTABLES, OU=COMPTABILITE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=INFORMATIQUE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=FIXES, OU=INFORMATIQUE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=PORTABLES, OU=INFORMATIQUE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=INGENIERIE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=FIXES, OU=INGENIERIE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=PORTABLES, OU=INGENIERIE, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=RH, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=FIXES, OU=RH, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=PORTABLES, OU=RH, OU=ORDINATEURS_CLIENTS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=SERVEURS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=EXCHANGE, OU=SERVEURS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=FICHIERs, OU=SERVEURS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=SQL, OU=SERVEURS, OU=FORMATION, DC=FORMATION, DC=LOCAL
OU=WEB, OU=SERVEURS, OU=FORMATION, DC=FORMATION, DC=LOCAL

Les propriétés des utilisateurs dans l'Active Directory

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

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

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

Active Directory Schema

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

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

Étape 1.1 - Les propriétés de bases d'un utilisateur

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

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

- Créer l'utilisateur en utilisant les paramètres
 - Prénom: **PRÉNOM**
 - Nom: **NOM**
 - Nom complet: **PRÉNOM NOM**
 - Nom d'ouverture de session de l'utilisateur: **test1@FORMATION.LOCAL**
 - Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000): **FORMATION\test1**
 - Mot de passe: **AAaaaa111**
 - Le mot de passe n'expire jamais

Nouvel objet - Utilisateur X

Créer dans : FORMATION.LOCAL/TEST

Prénom :	PRÉNOM	Initiales :	<input type="text"/>
Nom :	NOM		
Nom complet :	PRÉNOM NOM		
Nom d'ouverture de session de l'utilisateur :			
<input type="text"/> test1		@FORMATION.LOCAL	
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
<input type="text"/> FORMATION\		<input type="text"/> test1	

[< Précédent](#) [Suivant >](#) [Annuler](#)

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

Nouvel objet - Utilisateur

Créer dans : FORMATION.LOCAL/TEST

Mot de passe : ······

Confirmer le mot de passe : ······

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

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : FORMATION.LOCAL/TEST

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

Nom complet : PRÉNOM NOM
Nom de connexion de l'utilisateur : test1@FORMATION.LOCAL
Le mot de passe n'expire jamais.

< Précédent Terminer Annuler

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

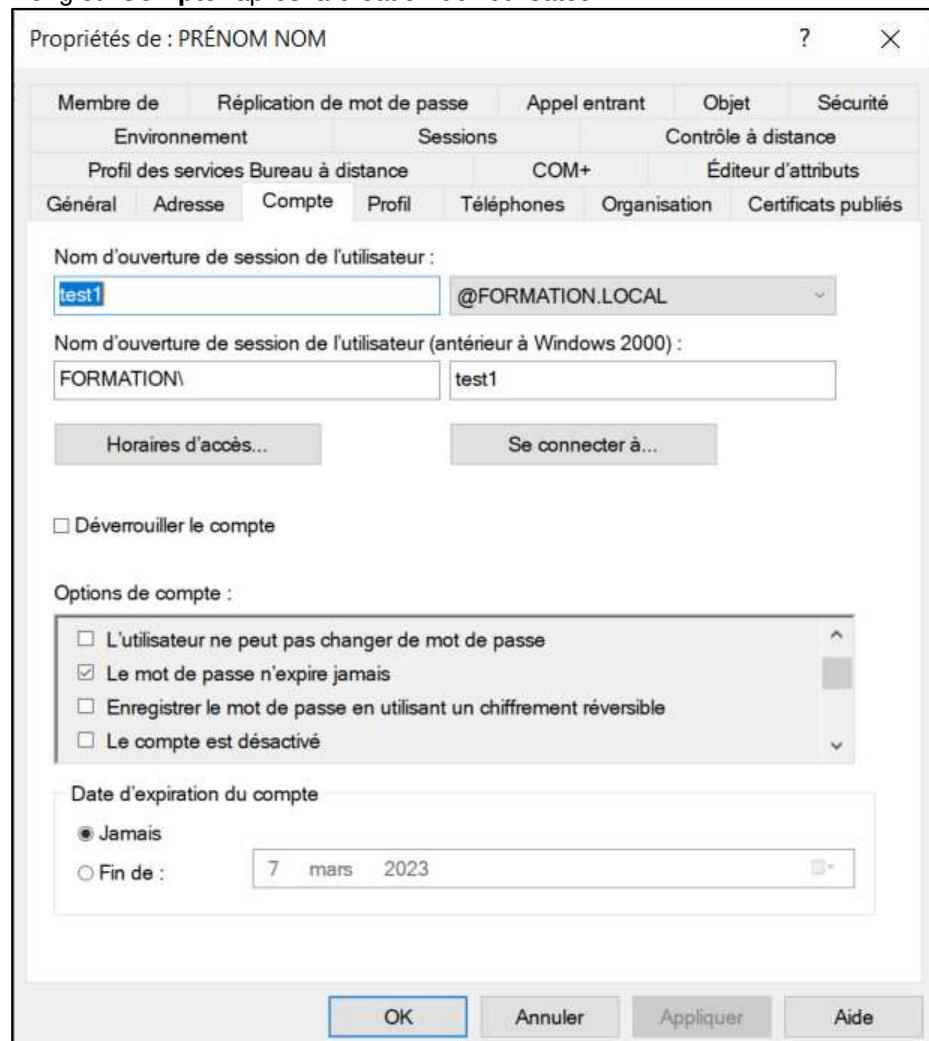
Nom	Type	Description
 PRÉNOM NOM	Utilisateur	

Vérification de la configuration de l'utilisateur après sa création

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

The screenshot shows the 'General' tab of the User Properties dialog box. The title bar includes tabs for 'Profil des services Bureau à distance', 'COM+', and 'Éditeur d'attributs'. Below these are tabs for 'Environnement', 'Sessions', and 'Contrôle à distance'. A secondary navigation bar at the top has tabs for 'Membre de', 'RéPLICATION de mot de passe', 'Appel entrant', 'Objet', and 'Sécurité'. The main area contains fields for 'Prénom' (PRENOM), 'Nom' (NOM), 'Nom complet' (PRENOM NOM), 'Description' (empty), 'Bureau' (empty), 'Numéro de téléphone' (empty), 'Adresse de messagerie' (empty), and 'Page Web' (empty). At the bottom are buttons for 'OK' (highlighted in blue), 'Annuler', 'Appliquer', and 'Aide'.

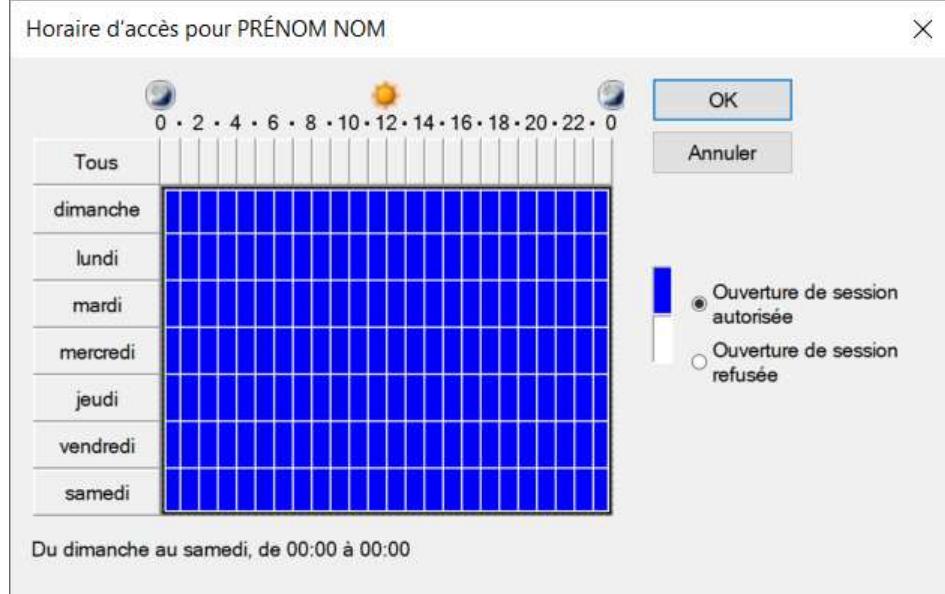
L'onglet "**Compte**" après la création de l'utilisateur



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

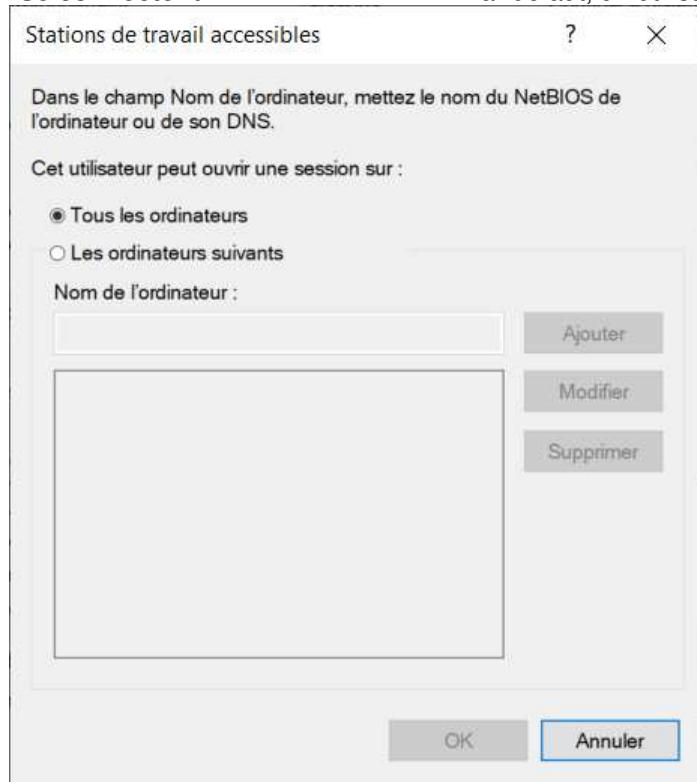
"Horaire d'accès..."

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



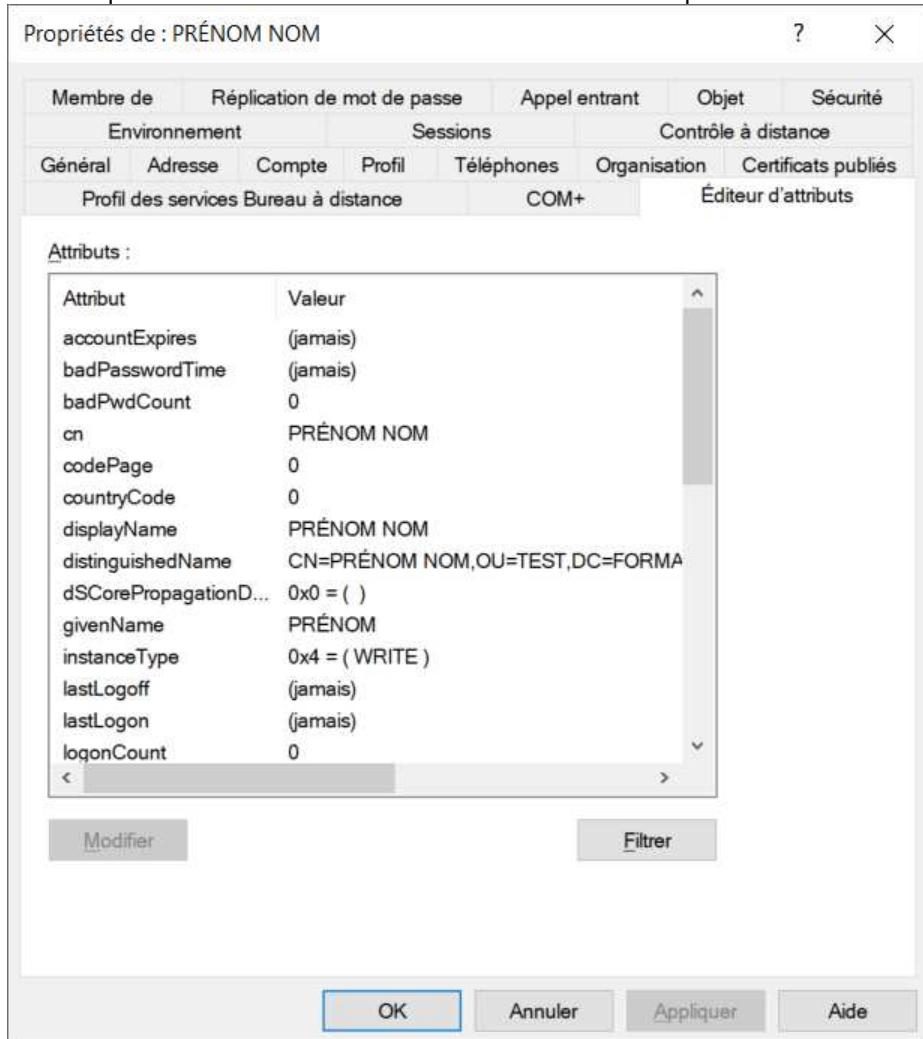
"Se connecter à..."

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



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

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



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

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

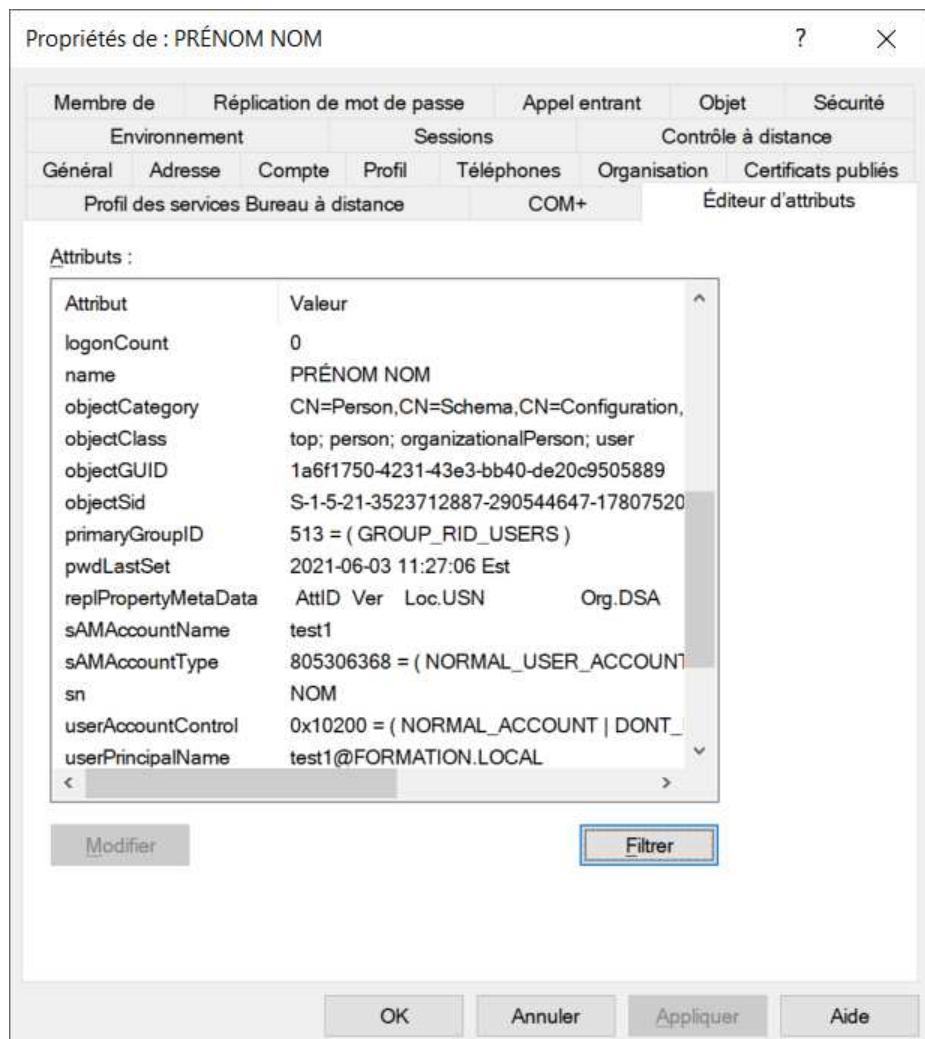
L'attribut "CN" contient le nom complet de l'utilisateur.

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

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

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

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



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

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

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

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

Vérification des attributs par programmation PowerShell

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

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

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

Étape 1.2 - Programmation d'un utilisateur avec PowerShell ISE

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

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

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

Exemple de création d'un utilisateur avec PowerShell.

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

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

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

PS E:\> $mdp | ConvertFrom-SecureString
01000000d08c9ddf0115d1118c7a00c04fc297eb0100000020b34493f2a76e478acce7dacc07087a000000000020000000000010660000000100002
000000079186dd1da767d78b0007356096ebb3f94d14c65e093db376dfcb8f215fbfc7f000000000e8000000002000020000000ba0a42e3eb04c0
4fe739f2df04d2722174cf065d63950b07c56f3060c8264c612000000067d1e3b37876151a18967ed8de9015d894d4fae8b4e8d76da3d126a1a38
106884000000081dcedcf7b7a217cc26dca1e51a47382ce4ee2529a416ceb025ad0646c352e4dc0202621731e2ce8681f96462082f6b5d45ec752
a9a03f11dbffd9db0b64abb1

PS E:\>

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

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

Nom	Type	Description
PRÉNOM NOM	Utilisateur	

Le résultat final semble identique.

Vérification des attributs par programmation PowerShell

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

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

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

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

Le paramètre **-Name** est obligatoire.

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

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

Propriétés de : PRÉNOM NOM

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

PRÉNOM NOM

Prénom : PRÉNOM Initiales :

Nom : NOM

Nom complet : PRÉNOM NOM

Description : DESCRIPTION

Bureau : BUREAU

Numéro de téléphone : 514-111-1111 Autre...

Adresse de messagerie : test1@courriel.local

Page Web : www.pageweb.local Autre...

OK Annuler Appliquer Aide

Numéro de téléphone (Autres) ? X

Nouvelle valeur :

Valeurs actuelles :
514-111-2222
514-333-4444

Ajouter Modifier Supprimer

OK Annuler

Ajouter des numéros de téléphones

Adresse de page Web (Autres) ? X

Nouvelle valeur :

Valeurs actuelles :
www.info.local
www.support.local

Ajouter Modifier Supprimer

OK Annuler

Ajouter des pages web

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

Nom du champ dans l'onglet "Général"	Nom de l'attribut
Prénom	givenName
Nom	sn
Nom complet	displayName
Description	description
Bureau	physicalDeliveryOfficeName
Numéro de téléphone	telephoneNumber
Autre...	otherTelephone
Adresse de messagerie	mail
Page Web	wWWHomePage
Autre...	url

Étape 2.2 - Programmation d'un utilisateur avec PowerShell ISE

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

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

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

Exemple de création d'un utilisateur avec PowerShell.

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

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

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

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

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

Propriétés de : PRÉNOM NOM

?

X

Membre de	RéPLICATION de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	Contrôle à distance		
Profil des services	Bureau à distance	COM+	Éditeur d'attributs	

Général Adresse Compte Profil Téléphones Organisation Certificats publiés

Adresse :

Boîte postale :

Ville :

Département ou :

Code postal :

Pays/région :

OK Annuler **Appliquer** Aide

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

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

Étape 3.2 - Programmation d'un utilisateur avec PowerShell ISE

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

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

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

Exemple pour configurer le pays avec le paramètre -OtherAttributes

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

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

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

Propriétés de : PRÉNOM NOM

Membre de	RéPLICATION de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	Contrôle à distance		
Profil des services	Bureau à distance	COM+	Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones

Numéros de téléphone

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

Remarques :

REMARQUES

OK Annuler Appliquer Aide

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

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

Étape 4.2 - Programmation d'un utilisateur avec PowerShell ISE

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

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

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

Étape 5 - Autres attributs d'un utilisateur

Trouvez les valeurs des attributs suivants pour l'utilisateur TECH

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

accountExpires La date d'expiration du compte

lastLogoff C'est un attribut que Microsoft n'a jamais utilisé.

logonCount Le nombre de fois que l'utilisateur s'est connecté avec succès.

accountExpires

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

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

9223372036854775807 correspond à la valeur hexadécimale **0x7FFFFFFFFFFFFFFF**

`[int64] ::.MaxValue = 9223372036854775807`

lastLogon

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

lastLogonTimeStamp

Cet attribut est répliqué sur chaque contrôleur de domaine mais seulement dans un intervalle de 9 à 14 jours.

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

Exemple avec LastLogon

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

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

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

3 juin 2021 21:36:22

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

1 juin 2021 09:44:58

LastLogonDate correspond à la date de LastLogonTimeStamp.

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

ANNEXE

L'attribut UserAccountControl

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

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

```
# Exemple pour trouver les utilisateurs avec "NORMAL_ACCOUNT" et "DONT_EXPIRE_PASSWORD"  
# -band est un "ET binaire"
```

```
Clear-Host
```

```
$n = 0x10200
```

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

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

```
Clear-Host
```

```
$n = 0x10200
```

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

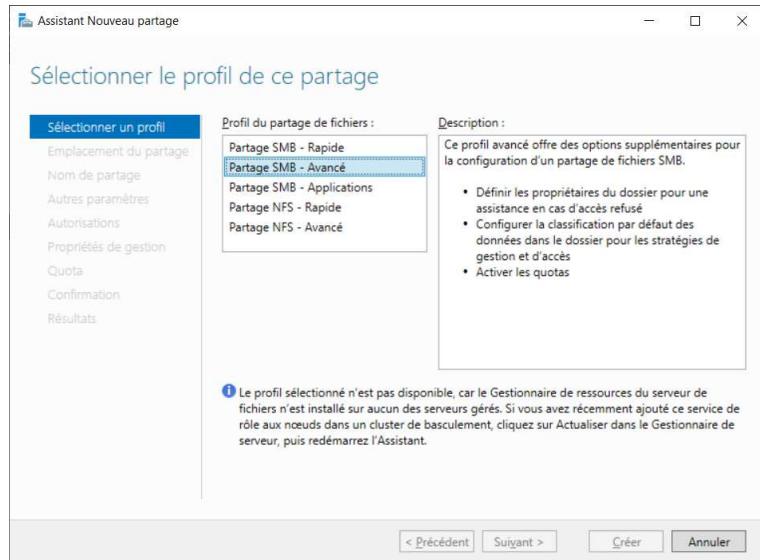
Gestion des partages sur les serveurs de fichiers

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

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

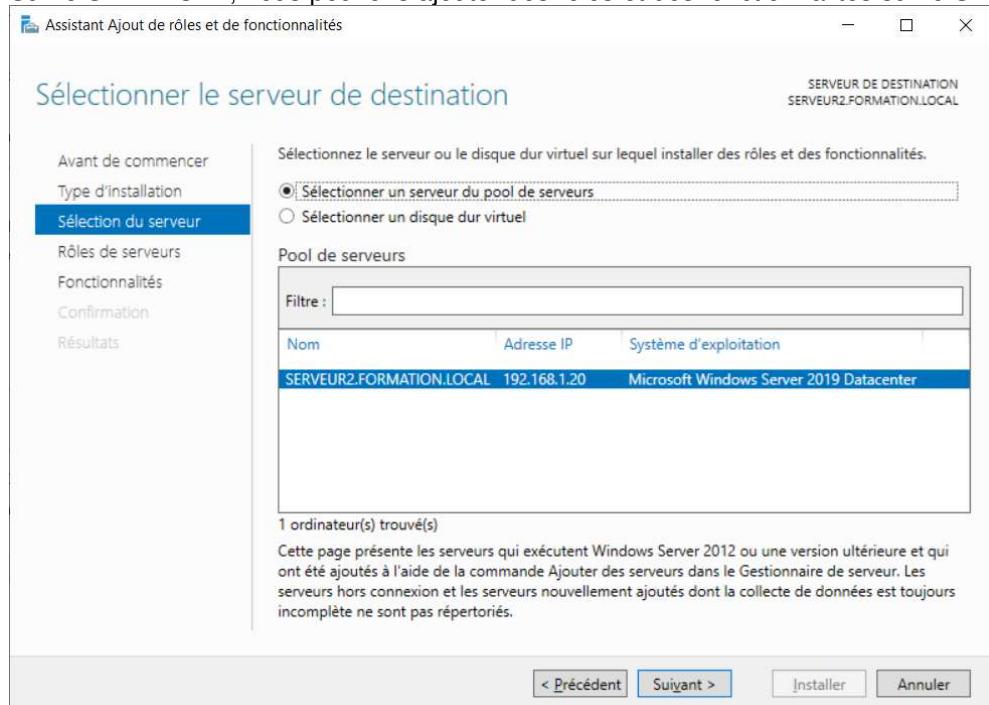
Pour utiliser l'option "**Partage SMB – Avancé**", il faut ajouter la console "**Gestionnaire de ressources du serveur de fichiers**".



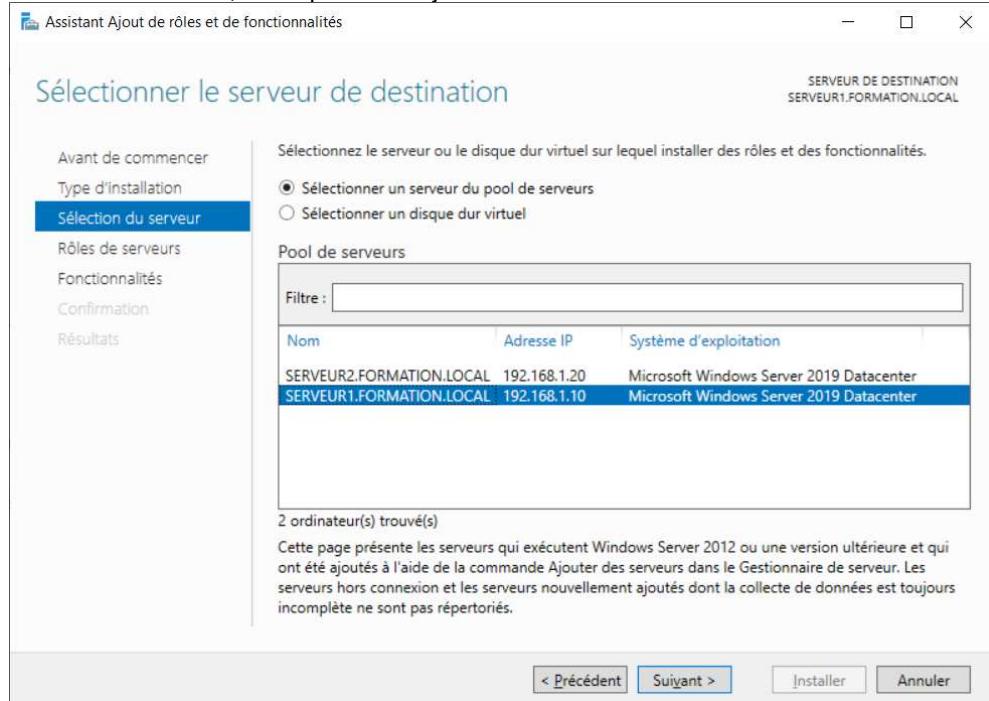
Vous devez ajouter le rôle "Gestionnaire de ressources du serveur de fichiers" sur les deux serveurs.

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

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



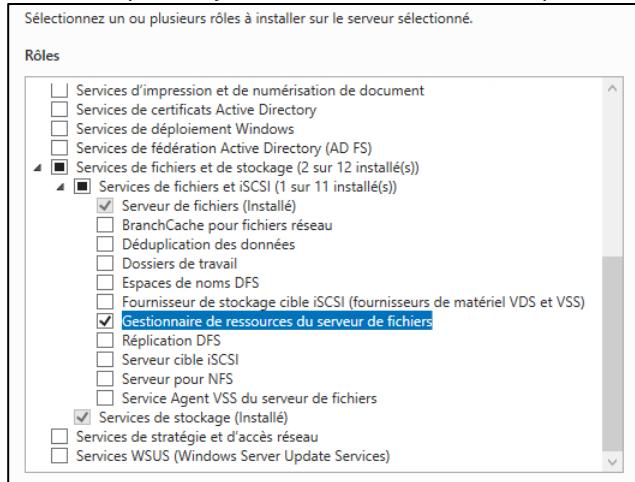
Sur le SERVEUR2, nous pouvons ajouter des rôles et des fonctionnalités sur le SERVEUR2 et le SERVEUR1.



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

Dans la console "Gestionnaire de serveur"

- Sélectionner le serveur
- Ajouter le rôle "**Gestionnaire de ressources du serveur de fichiers**"
note: accepter d'ajouter les fonctionnalités requises



Dossiers personnels

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

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

Directives générales

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

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

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

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

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

Utilisateurs pour le laboratoire

Pour ce laboratoire, vous devez créer deux utilisateurs:

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

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

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

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

Création du dossier racine et du partage

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

Création des dossiers personnels pour les utilisateurs

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

Modification des propriétés des utilisateurs dans la console UOAD

- nom du dossier personnel
- lettre du dossier personnel

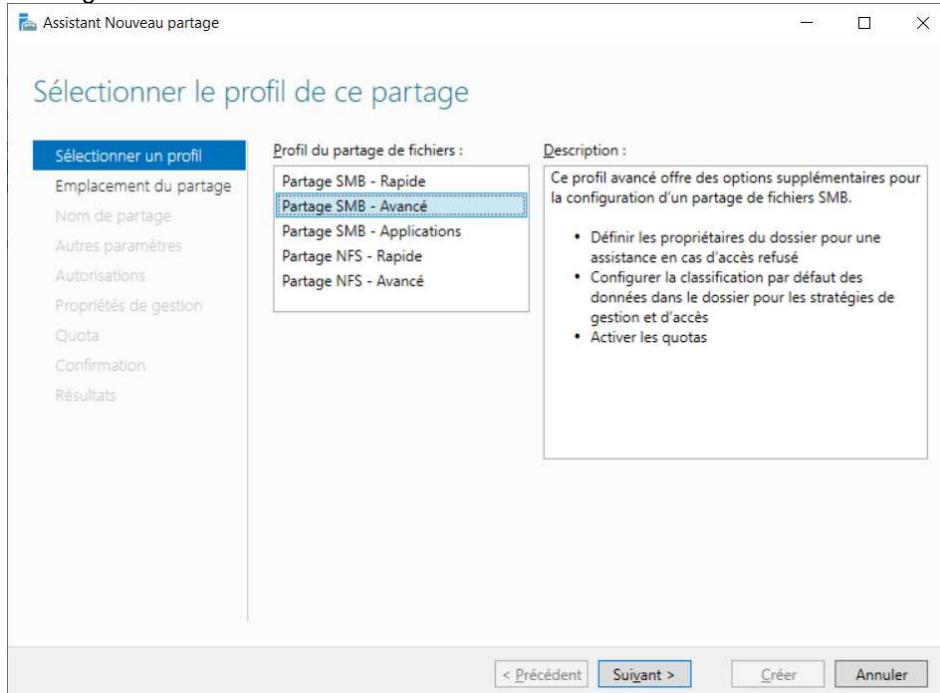
Étape 1 – Création d'un dossier personnel en utilisant les consoles

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

Création du dossier racine et du partage

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

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



Sélectionner le serveur et le chemin d'accès au partage

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

Indiquer le nom de partage

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

Configurer les paramètres de partage

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

Spécifier les autorisations pour contrôler l'accès

- Personnaliser les autorisations...

ONGLET "Autorisations"

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

VOICI LES AUTORISATIONS FINALES QUE DOIT AVOIR LE DOSSIER

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

ONGLET "Partage"

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

Spécifier les propriétés de gestion des dossiers

- Ne rien sélectionner

Appliquer le quota à un dossier ou un volume

- Ne pas appliquer de quota

Confirmer les sélections

- Cliquer sur le bouton "Créer"

Création du dossier personnel pour l'utilisateur U1

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

Sur ce dossier, ajouter les autorisations NTFS suivantes:

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

Modification des propriétés de l'utilisateur U1

Dans la console UOAD

Sélectionner l'utilisateur U1

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

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

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

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

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

Les dossiers seront créés sur le SERVEUR1 mais le code s'exécute sur le SERVEUR2
Écrire un script PowerShell pour créer des dossiers sur le SERVEUR1

Création du dossier racine

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

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

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

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

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

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

Création du partage sur le dossier racine

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

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

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

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

```
New-Item -Path "\\SERVEUR1\PERSO2$\U2" `  
        -ItemType directory  
  
icacls.exe \\SERVEUR1\PERSO2$\U2 /grant "U2:(OI)(CI)(M)"  
  
# IMPORTANT: Il ne faut pas utiliser le chemin suivant: \\SERVEUR1\E$\_PERSO2\U2  
Set-ADUser -Identity "U2" `  
        -HomeDrive "X:" `  
        -HomeDirectory "\\SERVEUR1\PERSO2$\U2"
```

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

Les utilisateurs EMP01 à EMP32 doivent avoir un dossier personnel.

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

Les dossiers personnels seront sur le SERVEUR1

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

Programmation d'un utilisateur dans l'Active Directory

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

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

Étape 1 - Mise en place

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

Étape 2 - Introduction au cmdlet New-ADUser

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

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

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

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

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

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

Le mot de passe de l'utilisateur sera AAAaaa111

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

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

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

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

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

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

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

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

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

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

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

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

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

Étape 4 - Validation

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

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

Nom	Type	Description
John Doe	Utilisateur	Mon premier utilisateur

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

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

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

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

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

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

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

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

ANNEXE

Une liste de plusieurs cmdlets pour gérer un utilisateur

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

- Set-ADAccountPassword
permet de modifier le mot de passe d'un utilisateur

- Get-ADUserResultantPasswordPolicy
Nous utiliserons ce cmdlet lorsque nous parlerons des GPO.

- Disable-ADAccount
- Enable-ADAccount

- Unlock-ADAccount
permet de déverrouiller un compte utilisateur

- Search-ADAccount
permet de chercher des comptes (utilisateurs, ordinateurs et des comptes de service) selon plusieurs critères

- Set-ADAccountControl
permet de modifier plusieurs propriétés des comptes (utilisateurs, ordinateurs et des comptes de service)

- Clear-ADAccountExpiration
- Set-ADAccountExpiration

Exemples

Trouver les comptes qui sont verrouillés

```
Search-ADAccount -LockedOut
```

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

```
Search-ADAccount -PasswordNeverExpires
```

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

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

Trouver les comptes utilisateurs qui sont inactifs depuis 90 jours

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

Trouver les comptes utilisateurs qui sont inactifs depuis 12 heures

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

Trouver les comptes utilisateurs qui sont désactivés et affiche plusieurs propriétés

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

Remplacer le mot de passe d'un utilisateur et

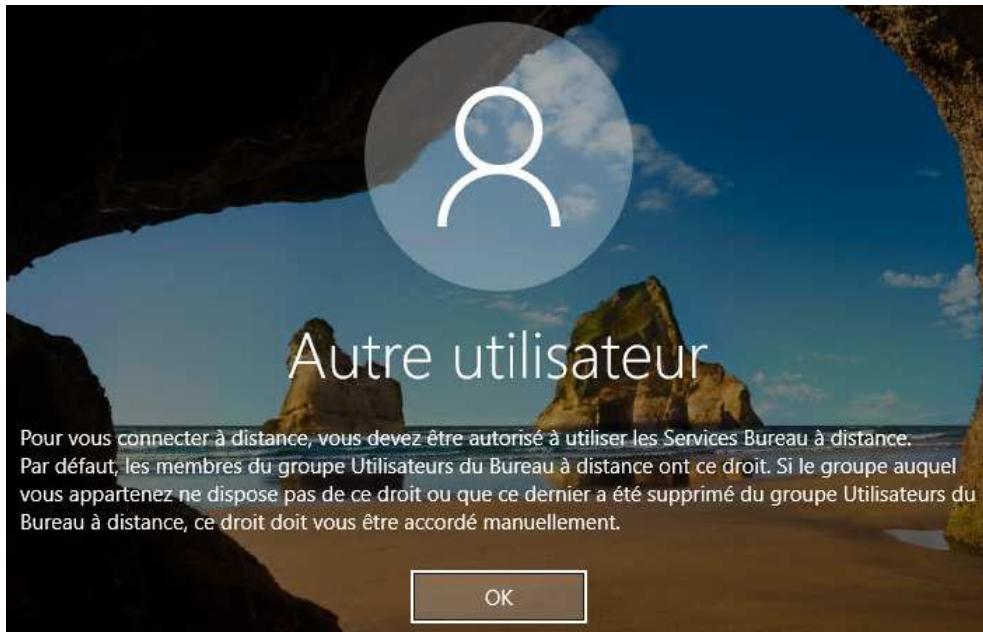
forcer l'utilisateur à modifier son mot de passe à la prochaine ouverture de session

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

```
Set-ADUser -Identity ETU -ChangePasswordAtLogon $true
```

PROBLÈME AVEC LE MODE DE SESSION ÉTENDU

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



SOLUTION SIMPLE À CE PROBLÈME

Modification à effectuer sur le serveur membre

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

The left screenshot shows the "Propriétés système" (System Properties) window. Under "Bureau à distance", the "Autoriser les connexions à distance à cet ordinateur" checkbox is checked. The right screenshot shows the "Utilisateurs du Bureau à distance" (Remote Desktop Users) dialog box, which lists the "FORMATION\Utilisateurs du domaine" group. Both windows have "OK" and "Annuler" buttons at the bottom.

Propriétés des objets "Groupe"

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

Objectifs

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

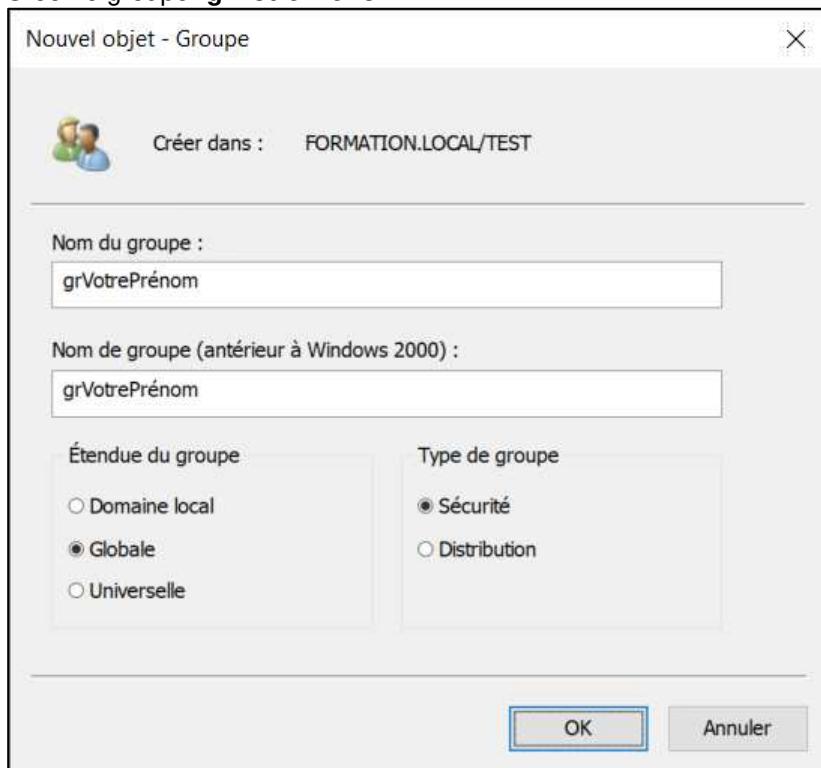
Étape 1 - Créer un groupe à l'aide de la console UOAD

Ouvrir la console UOAD

- Vérifier que votre affichage est en "Fonctionnalités Avancées"

Dans l'unité d'organisation "TEST"

- Créer le groupe "grVotrePrénom"



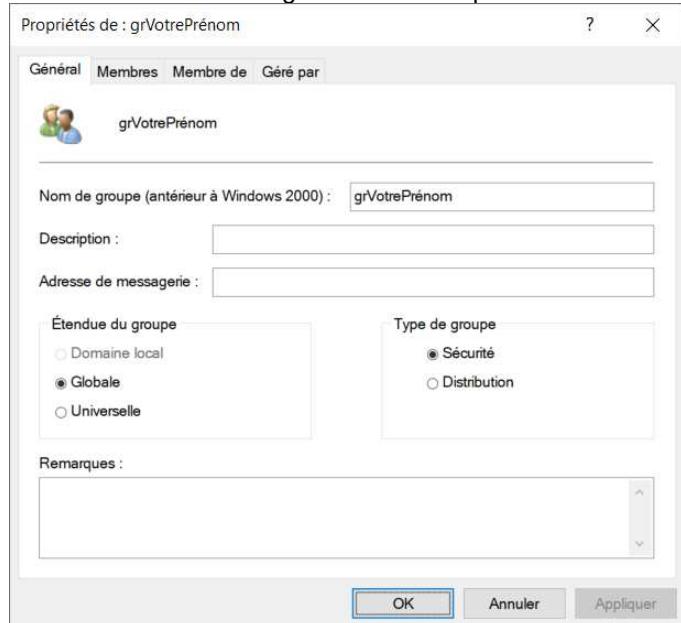
L'équivalent en PowerShell

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

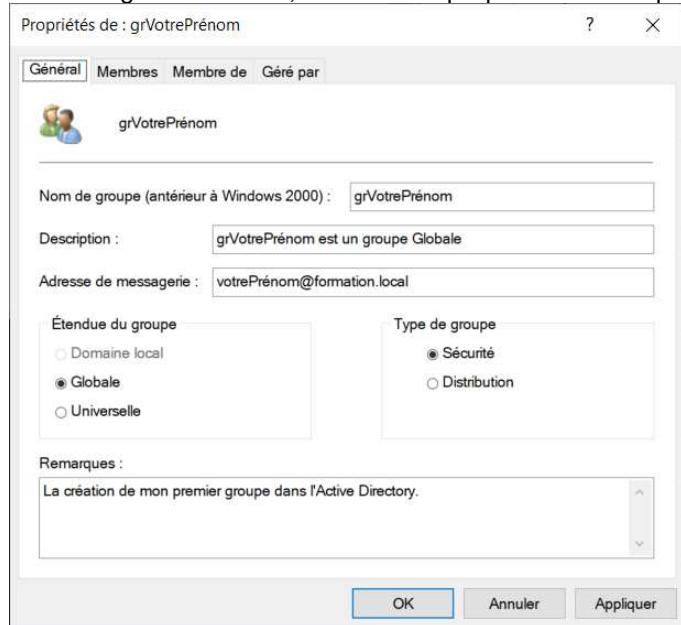
Étape 2 - Modifier les propriétés de l'onglet "Général" du groupe

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

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



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



La modification des trois propriétés avec PowerShell

```
$desc = "grVotrePrénom est un groupe Globale"  
$courriel = "votrePrénom@formation.local"  
$remarques = "La création de mon premier groupe dans l'Active Directory."  
  
Set-ADGroup -Identity grVotrePrénom `  
    -Description $desc `  
    -Replace @{ mail = $courriel; info= $remarques }
```

Création de groupes

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

Objectifs

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

Description du travail

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

Généralités

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

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

Documentation sur les groupes

Étendue du groupe

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

Synthèse

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

Type de groupe

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

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

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

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

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

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

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

Pour ajouter des utilisateurs à des groupes

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

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

Exemple 1

```
$groupe = "gr3"  
Add-ADGroupMember -Identity $groupe  
    -Members U1  
  
Add-ADGroupMember -Identity $groupe  
    -Members U2,U3,U4
```

Exemple 2

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

Pour afficher les membres d'un groupe

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

Exemple

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

Pour afficher les groupes dont est membre un utilisateur

Première méthode

Get-ADPrincipalGroupMembership Affiche les groupes dont est membre un utilisateur

Exemple

```
# Commande pour afficher le distinguishedName des groupes de l'utilisateur U1  
(Get-ADPrincipalGroupMembership -Identity U1).distinguishedName  
CN=Utilisateurs du domaine,CN=Users,DC=FORMATION,DC=LOCAL  
CN=gr1,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=gr2,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
CN=gr3,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL  
NOTE: Le groupe "Utilisateurs du domaine" est affiché dans la liste.
```

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

```
Utilisateurs du domaine  
gr1  
gr2  
gr3
```

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

Pour afficher les groupes dont est membre un utilisateur Deuxième méthode

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

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

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

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

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

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

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

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

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

```
# Commande pour afficher seulement le nom de chaque groupe
$gr = (Get-ADUser -Identity U1 -Properties MemberOf) .MemberOf
$gr | ForEach-Object {
    $groupe = Get-ADGroup -Identity $PSItem
    Write-Host $groupe.Name -ForegroundColor Cyan
}
gr1
gr2
gr3
```

Pour enlever des utilisateurs à des groupes

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

Remove-Add-ADPrincipalGroupMembership
Enlève un utilisateur à un ou plusieurs groupes de l'Active Directory

Exemple 1

```
$groupe = "gr3"  
Remove-ADGroupMember -Identity $groupe `  
                      -Members U2,U3,U4 `  
                      -Confirm:$false
```

Exemple 2

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

Pour supprimer des groupes

Remove-ADGroup Supprime un groupe de l'Active Directory

```
# Voici comment supprimer plusieurs groupes avec Remove-ADGroup  
$chemin = "OU=TEST,DC=FORMATION,DC=LOCAL"  
Get-ADGroup -SearchBase $chemin `  
            -filter 'Name -like "gr*"' | Remove-ADGroup -Confirm:$false
```

Les groupes imbriqués

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

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

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

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

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

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

Le paramètre "-Recursive" demande beaucoup de ressource.

Les groupes imbriqués

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

- 1) Vous devez créer le groupe grTEST.

```
New-ADGroup -Name grTEST -GroupScope Global
```

- 2) Vous devez ajouter l'utilisateur John.Doe au groupe grTEST.

```
Add-ADGroupMember -Identity grTEST -Members John.Doe
```

- 3) Vous devez ajouter le groupe grTEST au groupe "Admins du domaine".

```
Add-ADGroupMember -Identity "Admins du domaine" -Members grTEST
```

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

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

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

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

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

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

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

Le paramètre "-RecursiveMatch" demande beaucoup de ressource.

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

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

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

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

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

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

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

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

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

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

Annexe

Voici comment insérer un caractère UNICODE

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

Vous avez besoin de modifier le registre

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

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

Modification sur les utilisateurs

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

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

Description du travail

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

Généralités

Le nom du domaine doit être dans une variable.

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

Informations sur les fichiers CSV

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

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

Travail

Créer les groupes

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

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

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

Pour obtenir de l'aide sur **-split** → **Get-Help about_split**

```
# Voici un exemple
"grTEST1", "grTEST2", "grTEST3", "grTEST4" -split ", "
grTEST1
grTEST2
grTEST3
grTEST4
```

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

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

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

ANNEXE

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

```
# Le SID du compte Administrateur du domaine se termine toujours par 500
# peut importe son nom Administrateur, Administrator, Administrador, ...
$userInstance = Get-ADUser -Filter *`  
                    -Properties MemberOf | `  
                    Where-Object { $PSItem.SID -like "S-1-5-21-*-500" }`  
  
$newAdmin = "AdminAD"  
$mdp = Read-Host "Mot de passe pour l'utilisateur $NewAdmin" -AsSecureString  
$desc = "Compte d'utilisateur d'administration"  
  
$nomDNS = (Get-ADDomain).DnsRoot  
  
New-ADUser -Name $newAdmin `  
           -Instance $userInstance `  
           -Description $desc `  
           -DisplayName $newAdmin `  
           -SAMAccountName $newAdmin `  
           -UserPrincipalName "$newAdmin@$nomDNS" `  
           -AccountPassword $mdp `  
           -PasswordNeverExpires $true `  
           -Enabled $true  
  
# Par défaut, un nouvel utilisateur est membre du groupe "Utilisateurs du domaine".  
foreach($group in $userInstance.MemberOf)  
{  
    Add-ADGroupMember -Identity $group `  
                      -Members $newAdmin  
  
    Write-Host $group -ForegroundColor Yellow  
}
```

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

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

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

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

CanonicalName

FORMATION.LOCAL/FORMATION/GROUPES/grCOMP_Comptables
FORMATION.LOCAL/FORMATION/GROUPES/grCOMP_Gestionnaires
FORMATION.LOCAL/FORMATION/GROUPES/grCOMP_Secretaires
FORMATION.LOCAL/FORMATION/GROUPES/grCOMPTABILITE
FORMATION.LOCAL/FORMATION/GROUPES/grFormation
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Analystes
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Gestionnaires
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Programmeurs
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Secretaires
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Tech_Niveau_1
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Tech_Niveau_2
FORMATION.LOCAL/FORMATION/GROUPES/grINF_Tech_Reseau
FORMATION.LOCAL/FORMATION/GROUPES/grINFORMATIQUE
FORMATION.LOCAL/FORMATION/GROUPES/grING_Gestionnaires
FORMATION.LOCAL/FORMATION/GROUPES/grING_Ingenieurs
FORMATION.LOCAL/FORMATION/GROUPES/grING_Secretaires
FORMATION.LOCAL/FORMATION/GROUPES/grING_Techniciens
FORMATION.LOCAL/FORMATION/GROUPES/grINGENIERIE
FORMATION.LOCAL/FORMATION/GROUPES/grRH
FORMATION.LOCAL/FORMATION/GROUPES/grRH_Gestionnaires
FORMATION.LOCAL/FORMATION/GROUPES/grRH_Secretaires

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

DistinguishedName

CN=grCOMP_Comptables,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grCOMP_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grCOMP_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grCOMPTABILITE,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grFormation,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Analystes,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Programmeurs,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Tech_Niveau_1,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Tech_Niveau_2,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINF_Tech_Reseau,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINFORMATIQUE,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grING_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grING_Ingenieurs,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grING_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grING_Techniciens,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grINGENIERIE,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grRH,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grRH_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL
CN=grRH_Secretaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL

La console "Centre d'administration Active Directory"

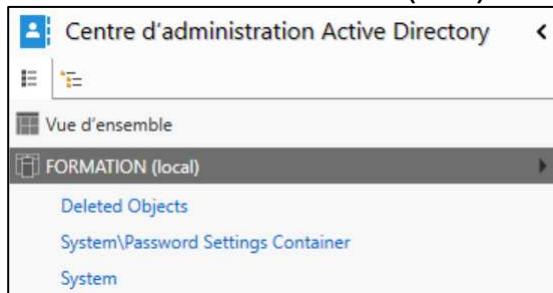
Le nom français de la console est "Centre d'administration Active Directory" mais dans le cours je vais utiliser l'abréviation anglaise (ADAC).

Le nom anglais de la console est "Active Directory Administrative Center" et l'abréviation est (ADAC).

La console ADAC offre des options qui ne sont pas disponibles dans la console "Utilisateurs et ordinateurs Active Directory".

DSAC.EXE est l'exécutable pour ouvrir la console ADAC.

En sélectionnant "FORMATION (local)"



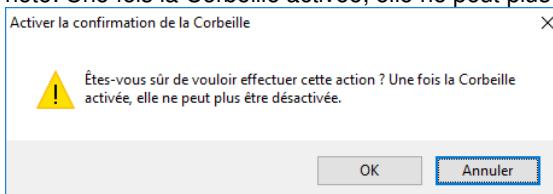
Activation de la corbeille "Active Directory"

"Activer la Corbeille..."

important: Pour activer la Corbeille, le niveau fonctionnel doit être au minimum "Serveur 2012".

note: La Corbeille va contenir des objets de l'Active Directory.

note: Une fois la Corbeille activée, elle ne peut plus être désactivée.



Il est possible d'activer la corbeille par programmation PowerShell.

```
# Cette commande doit s'exécuter sur le contrôleur de domaine
Enable-ADOptionalFeature -Identity "Recycle Bin Feature" `  
    -Scope Domain `  
    -Target "FORMATION.LOCAL" `  
    -Server SEVEUR1
```

Avertissement : L'activation de « Recycle Bin Feature » sur « DC=FORMATION,DC=LOCAL » est une action irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur « DC=FORMATION,DC=LOCAL » si vous continuez.



Supprimer et récupérer un utilisateur supprimé

Vous devez supprimer l'utilisateur "John.Doe".

```
Remove-ADUser -Identity "John.Doe" `  
-Confirm:$false
```

Avant de récupérer des utilisateurs qui sont supprimés, vous devez vérifier avec une commande s'il y a plus d'un utilisateur qui répond aux critères.

Cette commande liste les utilisateurs qui sont supprimés dont le SamAccountName est "John.Doe".

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `  
-IncludeDeletedObjects
```

Cette commande récupère l'utilisateur à son emplacement d'origine

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `  
-IncludeDeletedObjects | Restore-ADObject
```

Cette commande récupère l'utilisateur dans un emplacement différent

```
$path = "CN=Users,DC=FORMATION,DC=LOCAL"
```

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `  
-IncludeDeletedObjects | Restore-ADObject -TargetPath $path
```

Si vous avez plusieurs utilisateurs supprimés qui ont le même SamAccountName, vous devez vérifier la date de suppression du compte en affichant la propriété "**Modified**".

Cette commande affiche les utilisateurs qui sont supprimés dont le SamAccountName est "John.Doe"

en affichant la date de suppression

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `  
-Properties Modified `  
-IncludeDeletedObjects
```

Cette commande affiche les utilisateurs qui sont supprimés dont le SamAccountName est "John.Doe"

en affichant la date de suppression et la date de suppression la plus récente est en première position

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `  
-Properties Modified `  
-IncludeDeletedObjects | Sort-Object Modified -Descending
```

Cette commande affiche seulement l'utilisateur qui est supprimé dont le SamAccountName est "John.Doe"

dont la date de suppression est la plus récente

```
Get-ADObject -Filter 'SamAccountName -eq "EMP100" -AND Deleted -eq $true' `  
-Properties Modified `  
-IncludeDeletedObjects | `  
Sort-Object Modified -Descending | `  
Select-Object -First 1
```

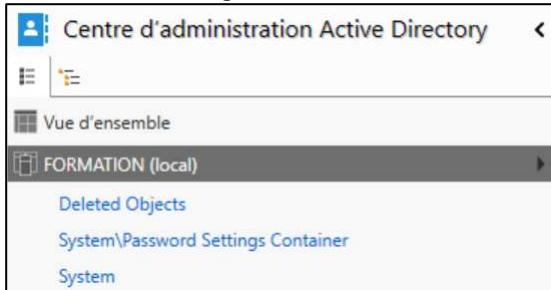
Cette commande récupère l'utilisateur à son emplacement d'origine en vérifiant la date de suppression

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND  
Deleted -eq $true -AND  
Modified -eq "2023-04-19 13:28:21"' `  
-Properties Modified `  
-IncludeDeletedObjects | Restore-ADObject
```

Stratégie de mot de passe affinée (Fine-Grained Password Policies)

Les propriétés de "**Password Settings Container**" permettent de configurer des stratégies différentes de mot de passe selon les utilisateurs ou les groupes de sécurité globaux.

"**Password Settings Container**" est sous "**FORMATION (local) / System**"



Historique de Windows PowerShell

En sélectionnant le bouton "Afficher tout", le code PowerShell sera disponible lorsque vous aurez effectué une modification à l'Active Directory à condition d'avoir utilisé la console ADAC.

Informations supplémentaires sur les GPO

Objectifs

- Comprendre l'implication du blocage de l'héritage
- Comprendre la différence entre "Appliqué" et "Lien activé"

Étape 1 - Création et test d'un objet de stratégie de groupe

Si l'unité d'organisation "EMPLOYES" est directement sous le domaine "FORMATION.LOCAL".

Si l'utilisateur EMP100 est dans l'unité d'organisation "EMPLOYES".

Si l'utilisateur PROG100 est dans l'unité d'organisation "PROGRAMMEURS".



Si la stratégie "Execute" est liée à l'unité d'organisation "EMPLOYES" et la section "Ordinateur" est désactivée.

En supposant que les paramètres de la stratégie "Execute" sont les suivants:

Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration

"Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC"

- Activé

Configuration utilisateur / Stratégies / Modèles d'administration / Système

"Ne pas exécuter les applications Windows spécifiées"

- calc.exe
- win32calc.exe

Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
 - **EMP100 n'a pas d'accès à la calculatrice**
-

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 n'a pas d'accès au panneau de configuration**
 - **PROG100 n'a pas d'accès à la calculatrice**
-

C'est le comportement normal de l'application des GPO.

Étape 2 - L'option "Bloquer l'héritage"

L'option "Bloquer l'héritage" est dans le menu contextuel d'une unité d'organisation.



Un point d'exclamation blanc dans un rond bleu nous indique que l'option "Bloquer l'héritage" est activée.

Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
 - **EMP100 n'a pas d'accès à la calculatrice**
-

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 n'a pas d'accès au panneau de configuration**
 - **PROG100 n'a pas d'accès à la calculatrice**
-

Le blocage de l'héritage n'a aucun effet sur la GPO qui est liée directement à "EMPLOYES".

L'héritage est bloqué à deux niveaux.



Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
 - **EMP100 n'a pas d'accès à la calculatrice**
-

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 a accès au panneau de configuration**
- **PROG100 a accès à la calculatrice**

La GPO "Execute" ne s'applique pas sur les utilisateurs de l'unité d'organisation "PROGRAMMEURS".

Le blocage empêche l'application des GPO qui sont au-dessus d'une UO mais pas à celles qui sont liées directement à une UO.

En pratique, il faut éviter d'utiliser le blocage des GPO.

Si vous avez besoin d'utiliser l'option "Bloquer l'héritage", vous devez revoir la conception de vos GPO et de vos unités d'organisation.

Avant de continuer

Laisser le blocage d'héritage sur la UO "EMPLOYES"

Laisser le blocage d'héritage sur la UO "PROGRAMMEURS"

Étape 3 - L'option "Appliqué"

L'option "Appliqué" est dans le menu contextuel du lien d'une GPO.



Un cadenas nous indique que l'option "Appliqué" est activée.

L'option "Bloquer l'héritage" doit être active pour voir l'effet de l'option "Appliqué".

Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
 - **EMP100 n'a pas d'accès à la calculatrice**
-

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 n'a pas d'accès au panneau de configuration**
- **PROG100 n'a pas d'accès à la calculatrice**

L'option "Appliqué" a priorité sur l'option "Bloquer l'héritage".

IMPORTANT: Il ne faut pas confondre l'option "Appliqué" et "Lien activé".



En français	En anglais
Appliqué	Enforced
Lien activé	Link Enabled

En pratique, il faut éviter d'utiliser l'option "Appliqué".

Si vous avez besoin d'utiliser l'option "Appliqué", vous devez revoir la conception de vos GPO et de vos unités d'organisation.

Stratégies pour le navigateur "Google Chrome"

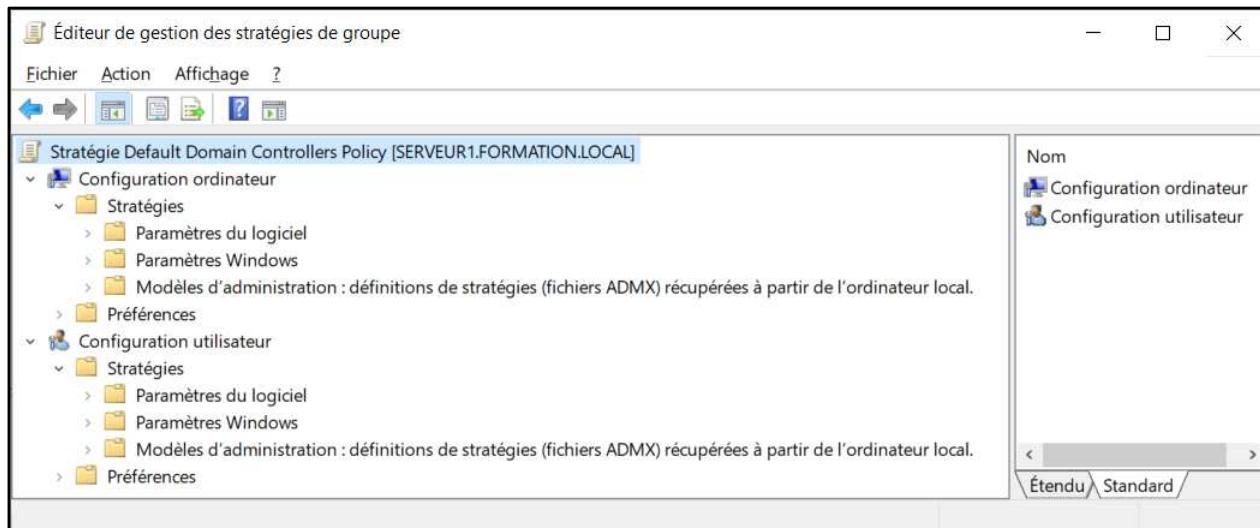
Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

- Création du "Magasin central"
- Ajout des fichiers ADMX et ADML pour le navigateur "Google Chrome"

L'utilisation d'un magasin central permet d'utiliser les mêmes fichiers ADMX et ADML sur l'ensemble des contrôleurs de domaine quelle que soit la version de Windows Server. Le magasin central permet de centraliser les modèles d'administration dans le répertoire SYSVOL.

Avant la création du "Magasin central", les stratégies dans "Modèles d'administration" sont récupérées à partir de l'ordinateur local.



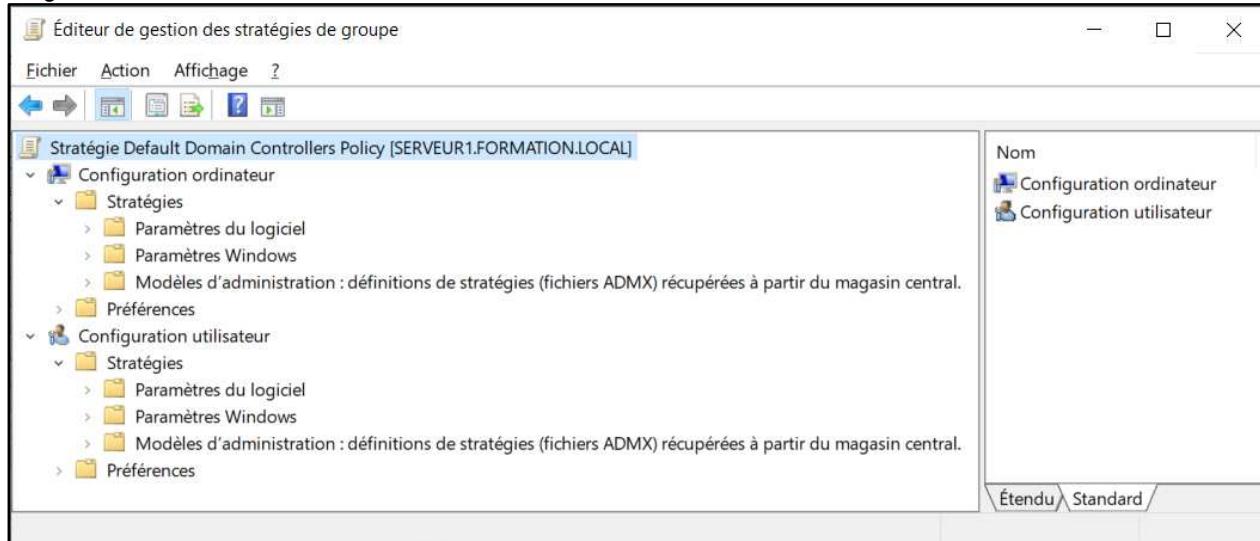
Étape 1 - Création du "Magasin central"

Copier le dossier "\SERVEUR1\C\$\Windows\PolicyDefinitions" dans le dossier "\\formation.local\SYSVOL\formation.local\Policies"

Pour éviter les erreurs, vous pouvez utiliser la commande suivante:

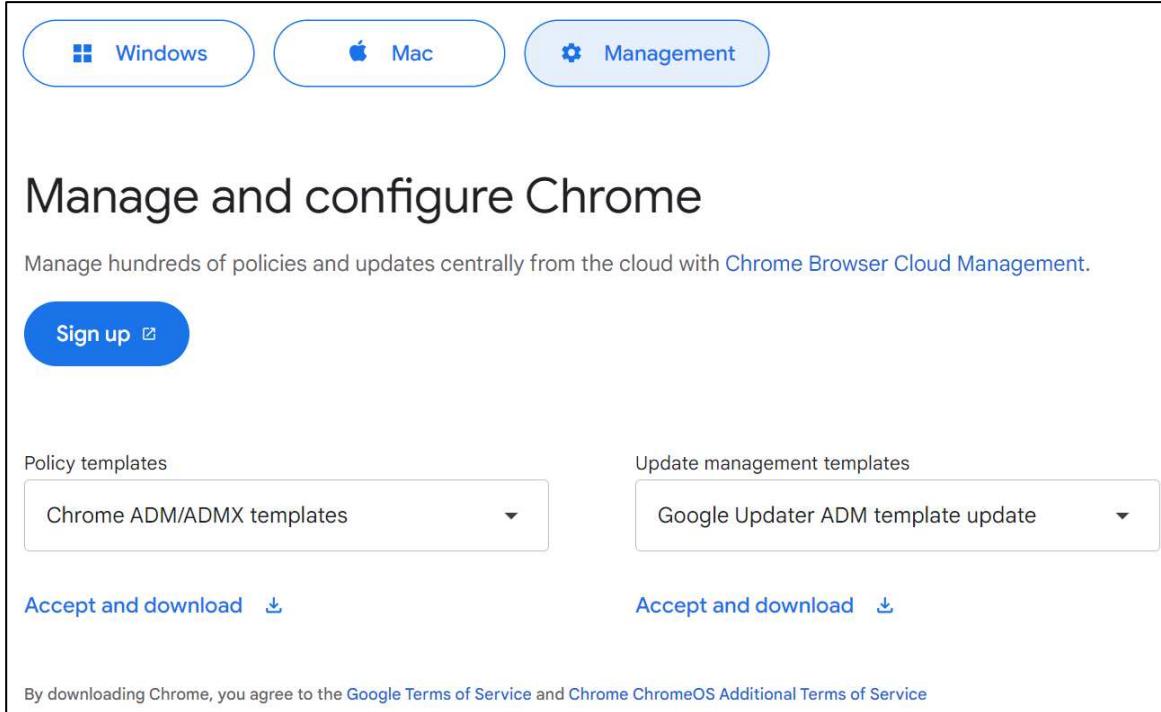
```
xcopy \\SERVEUR1\C$\Windows\PolicyDefinitions  
\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\ /s
```

Après la création du "Magasin central", les stratégies dans "Modèles d'administration" sont récupérées à partir du magasin central.



Étape 2 - Copier les fichiers ADMX et ADML de "Chrome" dans le magasin central

Le fichier **policy_templates.zip** est disponible sur le site "**Chrome enterprise**"
<https://chromeenterprise.google/download>



The screenshot shows the 'Manage and configure Chrome' page. At the top, there are three navigation buttons: 'Windows', 'Mac', and 'Management'. Below them, the title 'Manage and configure Chrome' is displayed. A sub-instruction reads: 'Manage hundreds of policies and updates centrally from the cloud with [Chrome Browser Cloud Management](#)'. A blue 'Sign up' button is visible. Two dropdown menus are shown: 'Policy templates' set to 'Chrome ADM/ADMX templates' and 'Update management templates' set to 'Google Updater ADM template update'. Each dropdown has an 'Accept and download' link below it. A note at the bottom states: 'By downloading Chrome, you agree to the [Google Terms of Service](#) and [Chrome ChromeOS Additional Terms of Service](#)'.

Extraire le contenu du fichier **policy_templates.zip** dans un dossier.

Vous devez récupérer les fichiers suivants

..\\windows\\admx\\chrome.admx
..\\windows\\admx\\google.admx
..\\windows\\admx\\fr-FR\\chrome.adml
..\\windows\\admx\\fr-FR\\google.adml

Copier les fichiers "..\\windows\\admx\\chrome.admx" et "..\\windows\\admx\\google.admx"
dans le dossier
\\formation.local\\SYSVOL\\formation.local\\Policies\\PolicyDefinitions\\

Copier les fichiers "..\\windows\\admx\\fr-FR\\chrome.adml" et "..\\windows\\admx\\fr-FR\\google.adml"
dans le dossier
\\formation.local\\SYSVOL\\formation.local\\Policies\\PolicyDefinitions\\fr-FR\\

Étape 3 - Création d'une GPO pour "Google Chrome"

Créer la stratégie "**U_EMPLOYES_Google_Chrome**" et la lier à votre unité d'organisation "**EMPLOYES**"

Désactiver la section "Ordinateur" de votre stratégie

Les paramètres de la GPO serviront à configurer les pages d'accueil du navigateur "Google Chrome".

On doit activer le paramètre de stratégie "**Action au démarrage**" qui est sous:

Configuration utilisateur / Modèles d'administration / Google / Google Chrome / Démarrage, page d'accueil et page Nouvel onglet

On doit sélectionner l'action au démarrage "**Ouvrir une liste d'URL**".

On doit activer le paramètre de stratégie "**URL à ouvrir au démarrage**" qui est sous:

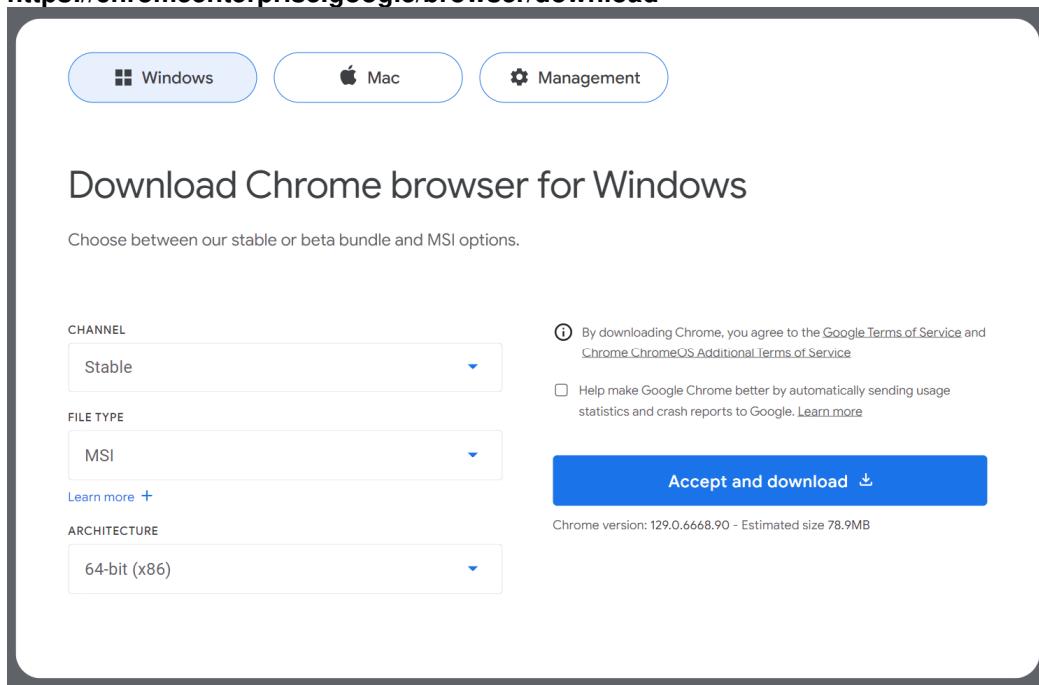
Configuration utilisateur / Modèles d'administration / Google / Google Chrome / Démarrage, page d'accueil et page Nouvel onglet

On doit inscrire une liste de site web que l'on désire ouvrir au démarrage de Chrome.

Étape 4 - Vérifier l'application de la GPO pour le navigateur "Google Chrome"

Vous devez installer le navigateur "Google Chrome" sur le SERVEUR2.

Le fichier googlechromestandaloneenterprise64.msi est disponible sur le site suivant dans la section "Windows"
<https://chromeenterprise.google/browser/download>



- 1) Fermer la session de l'utilisateur "FORMATION\TECH"
- 2) Ouvrir une session avec un des utilisateurs EMP01 à EMP32
- 3) Vérifier l'application des GPO pour le navigateur "Google Chrome".

ANNEXE

Voici des programmes que vous pouvez contrôler avec des fichiers ADMX et ADML.

Voici le lien pour récupérer les fichiers ADMX et ADML pour "**Edge Chromium**".

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

The screenshot shows a download page for Microsoft Edge Chromium. It features a large blue header with the text "Windows 64-bit". Below it is a smaller text "129.0.2792.65". A prominent black button labeled "Download ↓" is centered. At the bottom, there is a link "Download Windows 64-bit Policy".

Voici le lien pour récupérer les fichiers ADMX et ADML pour

"**Microsoft 365 Apps for enterprise - Office LTSC 2024 - Office LTSC 2021 - Office 2019 - Office 216**".

<https://www.microsoft.com/en-us/download/office.aspx>

note: vous devez rechercher "Administrative Template files"

The screenshot shows a download page for Microsoft Office administrative template files. The main title is "Administrative Template files (ADMX/ADML) for Microsoft Office". Below the title, a note states: "This download includes the Group Policy Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise, Office LTSC 2024, Office LTSC 2021, Office 2019, and Office 2016 and also includes the OPAX/OPAL files for the Office Customization Tool (OCT) for Office 2016." A message at the bottom says: "Important! Selecting a language below will dynamically change the complete page content to that language." There are buttons for "Select language" (set to English) and "Download".

Filtres WMI

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

- Utiliser des stratégies avec filtres WMI (Windows Management Instrumentation)
- Les filtres WMI font partie des outils de ciblage de la console GPMC.

Les filtres WMI permettent de cibler les postes clients ou les utilisateurs d'une stratégie de groupe avec précision. Avec un filtre WMI, il est possible d'appliquer des "GPO Utilisateurs" sur des ordinateurs en spécifiant une requête WMI afin de sélectionner un ou plusieurs ordinateurs.

Il est possible de filtrer l'application d'une stratégie en supprimant "**Utilisateurs authentifiés**" dans la section "**Filtrage de sécurité**" et d'ajouter seulement les utilisateurs, les ordinateurs ou les groupes visés par la stratégie.

C'est une solution trop compliquée, voir l'annexe à la fin du fichier.

Le plus simple est de configurer le filtrage WMI.

The screenshot shows the 'Filtre SERVEUR2' dialog box from the GPMC. It has tabs for 'Étendue', 'Détails', 'Paramètres', 'Délégation', and 'État'. The 'État' tab is selected. Under 'Liaisons', it shows 'FORMATION.LOCAL'. Below that, it lists 'Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :'. A large list box is empty. At the bottom of this section are buttons for 'Emplacement', 'Appliqué', 'Lien activé', and 'Chemin d'accès'. Below this is the 'Filtrage de sécurité' section, which contains a list box with 'Utilisateurs authentifiés' selected. At the bottom of this section are buttons for 'Ajouter...', 'Supprimer', and 'Propriétés'. The final section is 'Filtrage WMI', which contains a list box with '<aucun>' selected. At the bottom of this section are buttons for 'Ouvrir' and '<aucun>'. At the very bottom of the dialog box, there is a navigation bar with icons for 'Objets de stratégie de groupe' and 'Filtres WMI'.

Le fichier "**C53 - PowerShell - WMI - CIM.docx**" contient des exemples de code WMI.

Les filtres WMI sont basés sur le langage WQL (WMI Query Language) qui est très proche du langage de programmation SQL (Structured Query Language).

Étape 1 - Mise en place

Les unités d'organisations et les utilisateurs de l'unité d'organisation FORMATION doivent exister.

Vous devez supprimer le lien de la GPO "Bouclage_Fichiers" qui est sur l'unité d'organisation "FICHIERS".

Code PowerShell pour ajouter un ordinateur

```
New-ADComputer -Name SERVEUR3  
-Path "OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"
```

Étape 2 - Création des filtres WMI

- 1) Créer une requête WMI pour sélectionner le serveur SERVEUR2

Nom de la requête WMI: **SERVEUR2**

```
select * from Win32_ComputerSystem where Name = "SERVEUR2"
```

- 2) Créer une requête WMI pour sélectionner le serveur SERVEUR3

Nom de la requête WMI: **SERVEUR3**

note: cette requête vérifie exactement le nom du serveur

```
select * from Win32_ComputerSystem where Name = "SERVEUR3"
```

- 3) Créer une requête WMI pour sélectionner les deux serveurs: SERVEUR2 et SERVEUR3

Nom de la requête WMI: **SERVEUR2 et SERVEUR3**

note: cette requête vérifie exactement le nom des deux serveurs

```
select * from Win32_ComputerSystem where ((Name = "SERVEUR2") OR (Name = "SERVEUR3"))
```

- 4) Créer une requête WMI pour sélectionner les ordinateurs dont le nom débute par SERVEUR

Nom de la requête WMI: **SERVEUR***

note: cette requête vérifie si le nom débute par SERVEUR

```
select * from Win32_ComputerSystem where Name LIKE "SERVEUR%"
```

Voici comment vérifier une requête WMI dans PowerShell

```
Get-CimInstance -Query 'une requête WMI'
```

Exemple

```
$req = 'select * from Win32_ComputerSystem where Name = "SERVEUR2"'
```

```
Get-CimInstance -Query $req | Format-Table -AutoSize
```

Étape 3 - Création d'un objet de stratégie de groupe

Vous devez trouver un fichier JPG qui servira de fond d'écran et qui sera déposé dans le partage \\formation.local\netlogon.

Le nom du fichier sera "Fond_UO_Programmeurs.jpg".

Créer la stratégie "U_Programmeurs_filtre" qui sera liée à l'unité d'organisation
OU=PROGRAMMEURS,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

Désactiver la section "Ordinateur" de la stratégie

Modifier la stratégie "U_Programmeurs_filtre" en paramétrant ce qui suit:

Paramètres pour l'utilisateur

Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau

"Papier peint du Bureau"

- Activé
Nom du papier peint = \\formation.local\netlogon\Fond_UO_Programmeurs.jpg
Style du papier peint = Remplir

Filtrage WMI

Vous devez lier la requête WMI "**SERVEUR2**" à la GPO "**U_Programmeurs_Filtre**"

Étape 4 – Test sur le SERVEUR2

Ouvrir une session avec l'utilisateur **EMP11** ou **EMP12**

- Vérifier que le fond d'écran qui est spécifié dans le paramètre de la stratégie "**U_Programmeurs_filtre**" s'applique
- Fermer la session

Étape 5 - Modification du filtrage WMI sur la GPO "U_Programmeurs_filtre"

Vous devez lier la requête WMI "**SERVEUR3**" à la GPO "**U_Programmeurs_Filtre**"

Étape 6 – Test sur le SERVEUR2

Ouvrir une session avec l'utilisateur **EMP11** ou **EMP12**

- Vérifier que le fond d'écran qui est spécifié dans le paramètre de la stratégie "**U_Programmeurs_filtre**" ne s'applique pas
- Fermer la session

Étape 7 - Modélisation

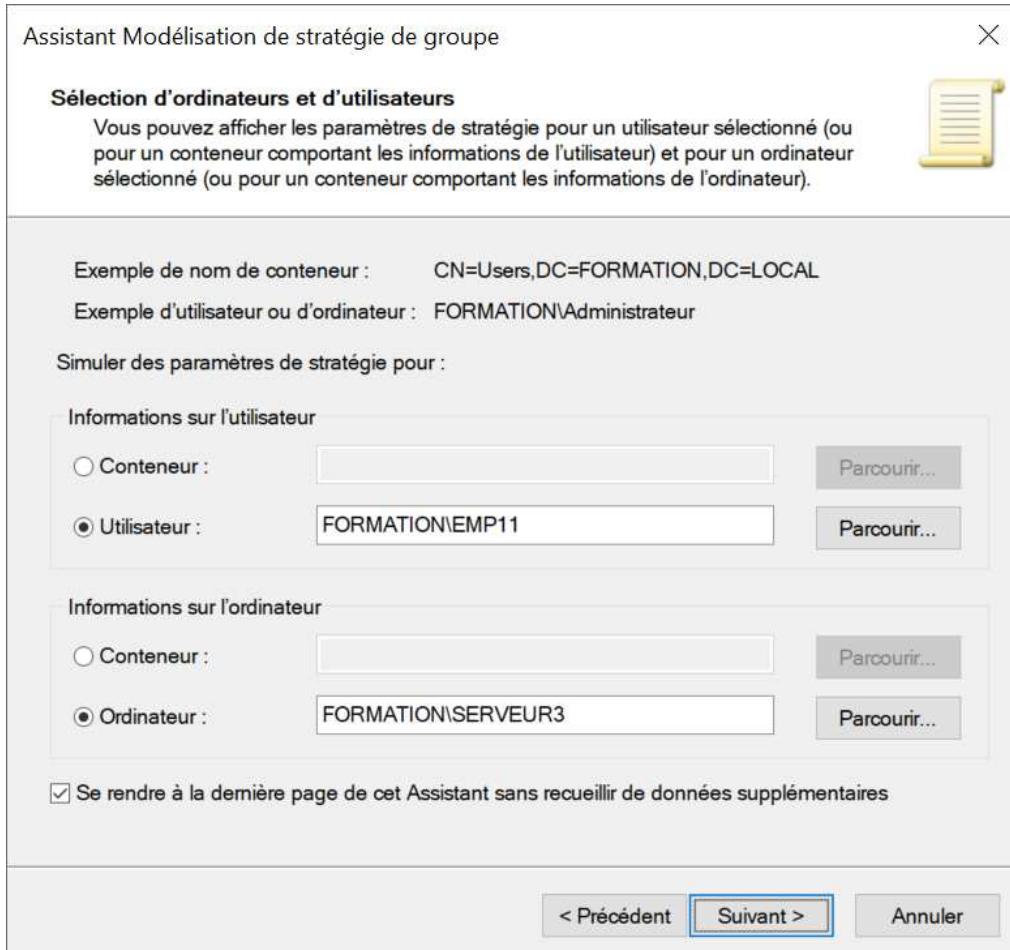
Il est possible de générer un rapport de modélisation même si le SERVEUR3 n'existe pas physiquement.

Dans la console "Gestion de stratégie de groupe"

- Section "Modélisation de stratégie de groupe"
Dans le menu contextuel, vous devez sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations à effectuer dans l'Assistant de modélisation de stratégie de groupe

- Sélection du contrôleur de domaine
Vous devez sélectionner l'option "Tout contrôleur de domaine exécutant ..."
- Sélection d'ordinateurs et d'utilisateurs



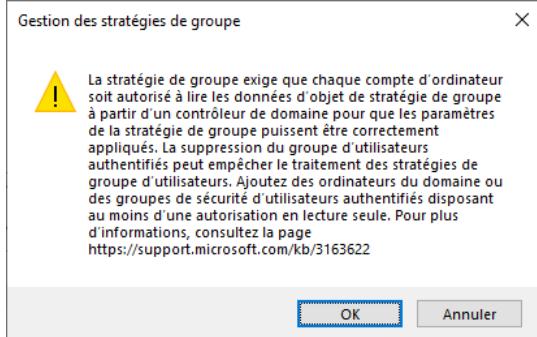
Cocher l'option "**Se rendre à la dernière page de cet Assistant ...**"

Le rapport de la modélisation montre que le fond d'écran qui est spécifié dans le paramètre de la stratégie "**U_Programmeurs_filtre**" s'applique.

ANNEXE

C'est possible de supprimer "Utilisateurs authentifiés" dans la section "Filtrage de sécurité" et d'ajouter seulement les utilisateurs, les ordinateurs ou les groupes visés par la stratégie. **C'est une solution trop compliquée.**

En supprimant "Utilisateurs authentifiés" dans la section "Filtrage de sécurité", il y a un message qui s'affiche.



L'onglet "Délégation" affiche les autorisations.

Nom	Autorisations acceptées
Administrateurs de l'entreprise (FORMATION\Administrateurs de l'entreprise)	Modifier les paramètres, supprimer, modifier la sécurité
Admins du domaine (FORMATION\Admins du domaine)	Modifier les paramètres, supprimer, modifier la sécurité
ENTERPRISE DOMAIN CONTROLLERS	Lecture
Système	Modifier les paramètres, supprimer, modifier la sécurité
Utilisateurs authentifiés	Lecture (à partir du filtrage de sécurité)

Dans l'onglet "Délégation", cliquer sur le bouton "Avancé..." et sélectionner "Utilisateurs authentifiés".

Par exemple, si vous voulez que la stratégie s'applique seulement à l'utilisateur EMP11.

Il faut ajouter l'utilisateur "**EMP11**".

Les autorisations pour "**EMP11**" seront:

- **Lire**
- **Appliquer la stratégie de groupe**

Il faut **obligatoirement** ajouter le groupe "**Ordinateurs du domaine**".

Les autorisations minimales pour "**Ordinateurs du domaine**" seront

- **Lire**
-

Pour revenir au comportement normal de la stratégie, vous devez défaire vos modifications

- Ajouter "**Utilisateurs authentifiés**"
note: vérifier que les autorisations "**Lire**" et "**Appliquer la stratégie de groupe**" sont cochées
- Supprimer l'utilisateur **EMP11**
- Supprimer le groupe "**Ordinateurs du domaine**"

Cette méthode de filtrage est à éviter.

Stratégies ORDINATEUR

Ce laboratoire doit être fait individuellement sur le SERVEUR2

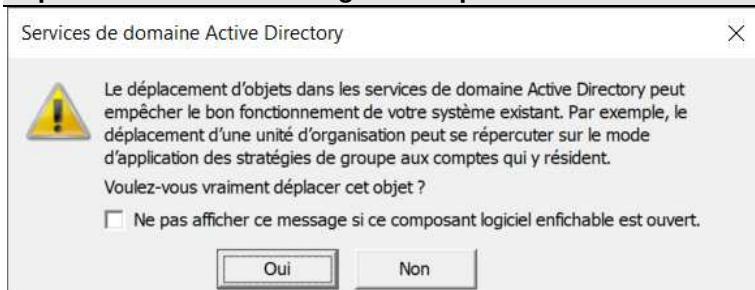
Objectif

- Introduction aux stratégies "Ordinateur"

Étape 1 - Mise en place

Déplacer l'ordinateur SERVEUR2 dans l'unité d'organisation
OU=FICHIERS,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL

Lors du déplacement de l'ordinateur SERVEUR2 un message va s'afficher à l'écran si vous effectuer le déplacement avec un "drag and drop".



Étape 2 - Création d'une stratégie ordinateur

Créer la stratégie "C_Serveurs_Fichiers" liée à votre unité d'organisation "FICHIERS".

Désactiver la section "Utilisateur" de votre stratégie

Modifier votre stratégie "C_Serveurs_Fichiers" en paramétrant ce qui suit:

Paramètres pour l'ordinateur

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

"Accès réseau: ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification du réseau"

- Activé

"Ouverture de session interactive: titre du message pour les utilisateurs essayant de se connecter"

- Le titre sera: "Message important"

"Ouverture de session interactive: contenu du message pour les utilisateurs essayant de se connecter"

- Le contenu du message sera: "Le serveur ne sera pas accessible à partir de 23:00."

Configuration ordinateur / Stratégies /

Modèles d'administration / Système / Ouverture de session

"Afficher l'animation à la première connexion"

- Désactivé

Étape 3 - Création d'une stratégie ordinateur

Créer la stratégie "C_Serveurs_Fichiers_Administrateurs" liée à votre unité d'organisation "FICHIERS".

Désactiver la section "Utilisateur" de votre stratégie

Modifier votre stratégie "C_Serveurs_Fichiers_Administrateurs" en paramétrant ce qui suit:

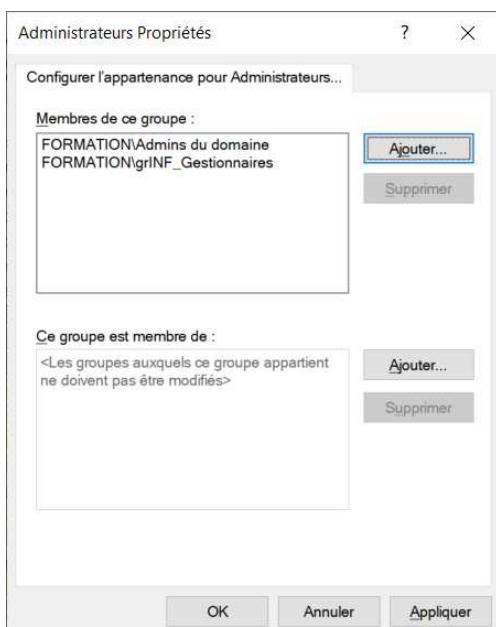
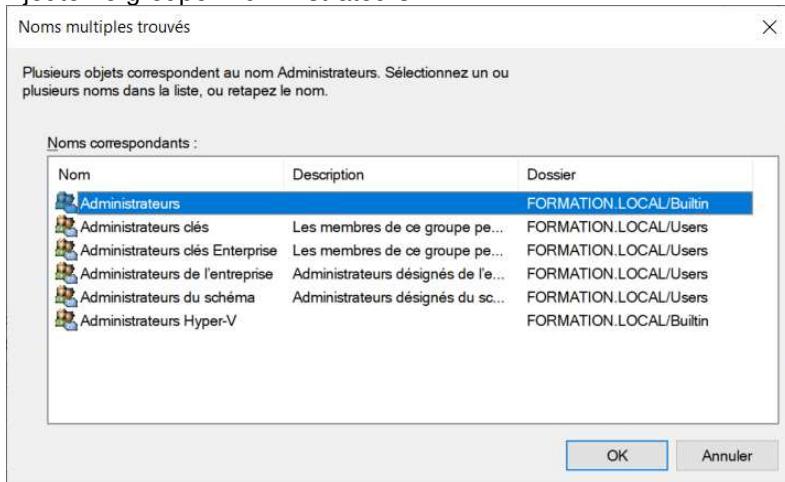
Paramètres pour l'ordinateur

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Groupes restreints

Dans le menu contextuel de "Groupes restreints" choisir l'option "Ajouter un groupe..."

- Ajouter le groupe "Administrateurs"



Ajouter le groupe "**FORMATION\Admins du domaine**" dans la section "**Membres de ce groupe**".
Ajouter le groupe "**FORMATION\griNF_Gestionnaires**" dans la section "**Membres de ce groupe**"

Étape 4 - Test

Ouvrir une "Invite de commandes" en tant qu'administrateur et exécuter la commande "**gpupdate.exe /force**".

Fermer la session de FORMATION\TECH sur le SERVEUR2.

Vous devez ouvrir une session avec **EMP09** ou **EMP10**.

- Vérifier l'application de la stratégie "**C_Serveurs_Fichiers**"
Un message s'affiche avant de s'authentifier au serveur.
- Vérifier l'application de la stratégie "**C_Serveurs_Fichiers Administrateurs**"
Ouvrir une fenêtre cmd.exe et exécuter la commande suivante "**whoami /groups**"
Dans la liste des groupes, vous allez voir que **EMP09** ou **EMP10** est membre du groupe **BUILTIN\Administrateurs**

Vous devez vous déconnecter de la session **EMP09** ou **EMP10**.

IMPORTANT: il n'y a que les membres des groupes **grINF_Gestionnaires** et "**FORMATION\Admins du domaine**" qui auront des autorisations **Administrateurs** sur le serveur SERVEUR2.

Étape 5 - TRAITEMENT PAR BOUCLAGE

Le traitement par bouclage permet d'appliquer des paramètres utilisateurs dans une unité d'organisation qui contient des ordinateurs.

Il existe deux modes pour le traitement par bouclage.

- "Remplacer" indique que les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" remplacent les paramètres utilisateur normalement appliqués à l'utilisateur.
- "Fusionner" indique que les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" et les paramètres utilisateur normalement appliqués à l'utilisateur se combinent.
Si les paramètres entrent en conflit, les paramètres utilisateur dans la stratégie de groupe de "traitement par bouclage" prévalent sur les paramètres normalement appliqués à l'utilisateur.

Cette solution est souvent appliquée pour des lecteurs réseaux et des imprimantes.

Créer la GPO "**Bouclage_Fichiers**" liée à votre unité d'organisation "FICHIERS".

Paramètres pour l'ordinateur

Configuration ordinateur / Stratégies /

Modèles d'administration / Système / Stratégie de groupe

"Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur"

- Activé le paramètre et choisir le mode **Remplacer**.

Paramètres pour l'utilisateur

Configuration utilisateur / Stratégies /

Modèles d'administration / Bureau / Bureau

Vous devez trouver un fichier JPG qui servira de fond d'écran et qui sera déposé dans le partage NETLOGON.

Vous devez donner un nom significatif au fichier, par exemple "serveur2.jpg".

"Papier peint du Bureau"

- Activé

Nom du papier peint = \\formation.local\\netlogon\\serveur2.jpg

Style du papier peint = Remplir

Je vous recommande de vérifier que le chemin pour le papier peint est valide.

Si le fond d'écran est complètement noir lorsque la GPO s'applique c'est parce que le chemin pour le papier peint n'est pas valide.

La section "Configuration ordinateur" et la section "Configuration utilisateur" sont activées.

Bouclage_Fichiers

Étendue Détails Paramètres Délégation

Configuration ordinateur (activée)

Stratégies

Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/ Stratégie de groupe

Stratégie	Paramètre	Commentaire
Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur	Activé	
Mode :	Remplacer	

Configuration utilisateur (activée)

Stratégies

Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Bureau/ Bureau

Stratégie	Paramètre	Commentaire
Papier peint du Bureau	Activé	\\\formation.local\\netlogon\\serveur2.jpg
Nom du papier peint :		
Exemple : avec un chemin local : C:\\windows\\web\\wallpaper\\home.jpg		
Exemple : avec un chemin UNC : \\\\Server\\Share\\Corp.jpg		
Style du papier peint :	Ajuster	

Tester l'application de la GPO "**Bouclage_Fichiers**" avec le mode "**Remplacer**".

Les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" remplacent les paramètres utilisateur normalement appliqués à l'utilisateur.

Après l'ouverture d'une session:

Le papier peint du Bureau s'affiche avec l'image serveur2.jpg.

"Bouclage_Fichiers"

Dans la GPO "**Bouclage_Fichiers**" changé le mode pour "**Fusionner**".

La section "Configuration ordinateur" et la section "Configuration utilisateur" sont activées.

Bouclage_Fichiers

Étendue Détails Paramètres Délégation

Configuration ordinateur (activée)

Stratégies

Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/ Stratégie de groupe

Stratégie	Paramètre	Commentaire
Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur	Activé	
Mode :	Fusionner	

Configuration utilisateur (activée)

Stratégies

Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Bureau/ Bureau

Stratégie	Paramètre	Commentaire
Papier peint du Bureau	Activé	
Nom du papier peint :	\\formation.local\netlogon\serveur2.jpg	
Exemple : avec un chemin local : C:\windows\web\wallpaper\home.jpg		
Exemple : avec un chemin UNC : \\Server\Share\Corp.jpg		
Style du papier peint :	Ajuster	

Tester l'application de la GPO "**Bouclage_Fichiers**" avec le mode "**Fusionner**".

Les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" et les paramètres utilisateur normalement appliqués à l'utilisateur se combinent.

Si les paramètres entrent en conflit, les paramètres utilisateur dans la stratégie de groupe de "traitement par bouclage" prévalent sur les paramètres normalement appliqués à l'utilisateur.

Après l'ouverture d'une session:

Le papier peint du Bureau s'affiche avec l'image serveur2.jpg.
L'écran de veille spécifique est "bubbles.scr".

"Bouclage_Fichiers"
"U_EMPLOYES"

...
Les bulles de l'écran de veille sont métalliques

"PU_EMPLOYES"

...

ANNEXE 1

Pour votre information, les fichiers pour l'image de l'écran de verrouillage et d'ouverture de session pour les ordinateurs du CVM sont dans le dossier **\reseau.cvm\NETLOGON\CapsuleInfo**

Le dossier contient plusieurs fichiers JPG, mais celui qui est utilisé par défaut a un nom particulier.
\reseau.cvm\NETLOGON\CapsuleInfo\CVMFondEcranActif.jpg

Configuration ordinateur / Stratégies /

Modèles d'administration / Panneau de configuration / Personnalisation

"Forcer une image de l'écran de verrouillage et d'ouverture de session par défaut spécifique"

- Activé

Chemin d'accès de l'image de l'écran de verrouillage = **\formation.local\netlogon\Logo_Corpo.jpg**

Cocher l'option "Désactiver les faits fantaisistes, conseils, astuces et plus encore sur l'écran de verrouillage"

ANNEXE 2

Cette GPO pourrait être liée à l'unité d'organisation "**SERVEURS**".

Exemple d'une GPO "C_powershell"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies /

Modèles d'administration / Composants Windows / Windows PowerShell

- Activer l'exécution des scripts
note: configurer la valeur de ce paramètre à "Autoriser tous les scripts"

ANNEXE 3

Cette GPO pourrait être liée à l'unité d'organisation "**ORDINATEURS_CLIENTS**".

Exemple d'une GPO "C_arret_système"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

- Arrêt: permet au système d'être arrêté sans avoir à se connecter
note: configurer la valeur de ce paramètre à Activé

ANNEXE 4

Cette GPO pourrait être liée à l'unité d'organisation "**SERVEURS**".

Exemple d'une GPO "C_securite"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

- Ouverture de session interactive: ne pas afficher le nom du dernier utilisateur connecté
note: configurer la valeur de ce paramètre à Activé
- Ouvertures de sessions interactives: nombre d'ouverture de sessions précédentes réalisées en utilisant la cache (lorsqu'aucun contrôleur de domaine n'est disponible)
note: configurer la valeur de ce paramètre à 0

ANNEXE 5

Cette GPO pourrait être liée à l'unité d'organisation "**SERVEURS**".

Exemple d'une GPO "C_divers"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies /

Modèles d'administration / Composants Windows / Options d'ouverture de session Windows

- Afficher les informations sur les ouvertures de session précédentes au cours d'une ouverture de session utilisateur
note: configurer la valeur de ce paramètre à Activé

Configuration ordinateur / Stratégies / Modèles d'administration / Système

- Afficher le moniteur d'événements de mise hors tension
note: configurer la valeur de ce paramètre à Désactivé

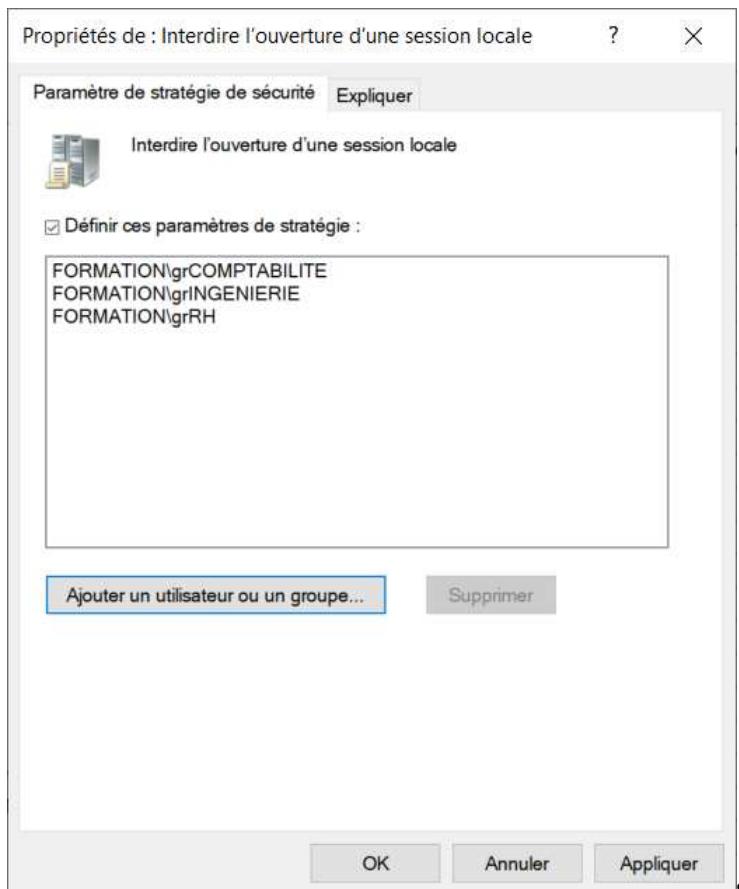
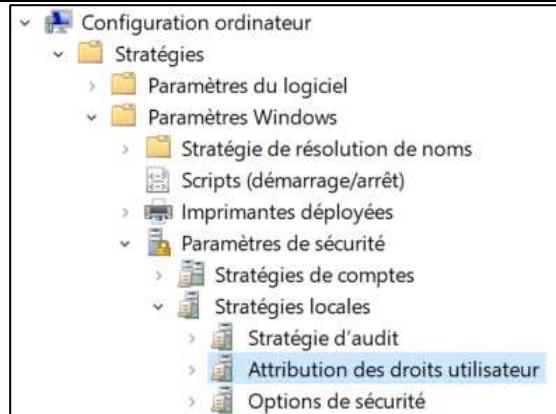
Configuration ordinateur / Stratégies / Modèles d'administration / Système / Ouverture de session

- Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session
note: configurer la valeur de ce paramètre à Activé

ANNEXE 6

Voici comment refuser l'accès à des utilisateurs d'ouvrir une session locale sur des ordinateurs qui sont dans une unité d'organisation.

Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur



Si la GPO est liée à l'unité d'organisation SERVEURS, il sera impossible aux utilisateurs des trois groupes d'ouvrir une session locale sur les ordinateurs qui sont dans l'unité d'organisation SERVEURS.
"OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"

Préférences UTILISATEUR

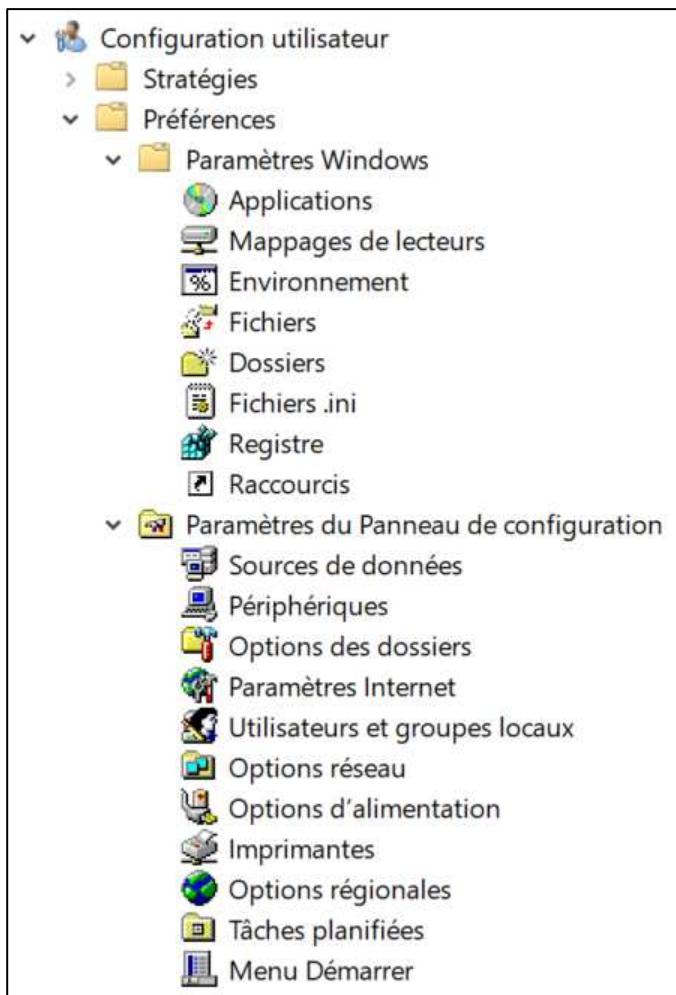
Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

- Introduction aux préférences "Utilisateur"

IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy



Les utilisateurs peuvent modifier les configurations qui sont configurées par des préférences.
Les préférences ne sont pas supprimées quand la GPO n'est plus appliquée.

Lors de la création d'une préférence, nous devons choisir entre Créer, Remplacer, Mettre à jour, Supprimer

Créer

Permet de créer un nouveau paramètre de préférence pour l'utilisateur ou l'ordinateur.

Remplacer

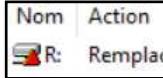
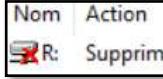
Permet de remplacer et de recréer un paramètre de préférence pour l'utilisateur ou l'ordinateur.

Mettre à jour

Permet de modifier un paramètre de préférence existant pour l'utilisateur ou l'ordinateur.

Supprimer

Permet de supprimer un paramètre de préférence existant pour un utilisateur ou un ordinateur.

Créer	Un triangle vert est présent.	
Remplacer	Un triangle rouge est présent.	
Mettre à jour	Un triangle jaune est présent.	
Supprimer	Un X rouge est présent.	

Création d'une GPO avec des préférences au niveau de la UO EMPLOYES

Créer la GPO "PU_EMPLOYES" et la lier à votre unité d'organisation "EMPLOYES"

Désactiver la section "Configuration ordinateur".

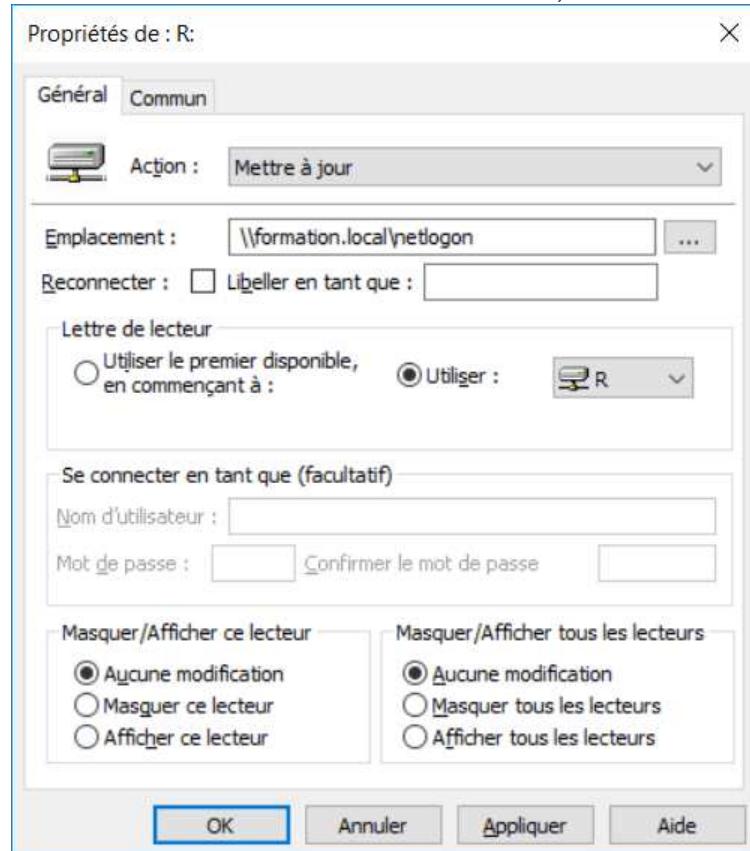
Toutes les options se trouvent dans la section "Configuration utilisateur / Préférences"

Configuration utilisateur / Préférences / Paramètres Windows / Mappages de lecteurs

Lier la lettre "R:" au partage "\\\formation.local\\netlogon".

● Mappages de lecteurs

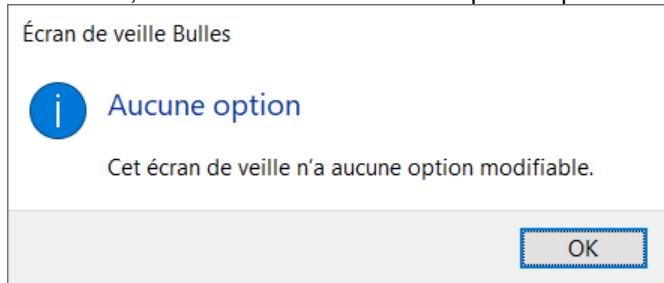
dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Lecteur mappé"



- Action: Mette à jour
- Emplacement: \\\formation.local\\netlogon
- Utiliser: R
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Configuration utilisateur / Préférences / Paramètres Windows / Registre

Par défaut, l'écran de veille "Bulles" ne permet pas de modifier le comportement des bulles.



En modifiant le registre Windows, il est possible de modifier l'aspect des bulles pour l'écran de veille "Bulles".

● **Registre**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Élément Registre"

- Action: Mettre à jour
- Ruche: HKEY_CURRENT_USER
- Chemin d'accès de la clé: Software\Microsoft\Windows\CurrentVersion\Screensavers\Bubbles
- Nom de valeur: MaterialGlass
- Type de valeur: REG_DWORD
- Données de valeur: 0
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

MaterialGlass

- 0 pour afficher des bulles métalliques
- 1 pour afficher des bulles transparentes

Configuration utilisateur / Préférences / Paramètres Windows / Raccourcis

Créer un raccourci sur le Bureau vers NCPA.CPL

● **Raccourcis**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Raccourci"

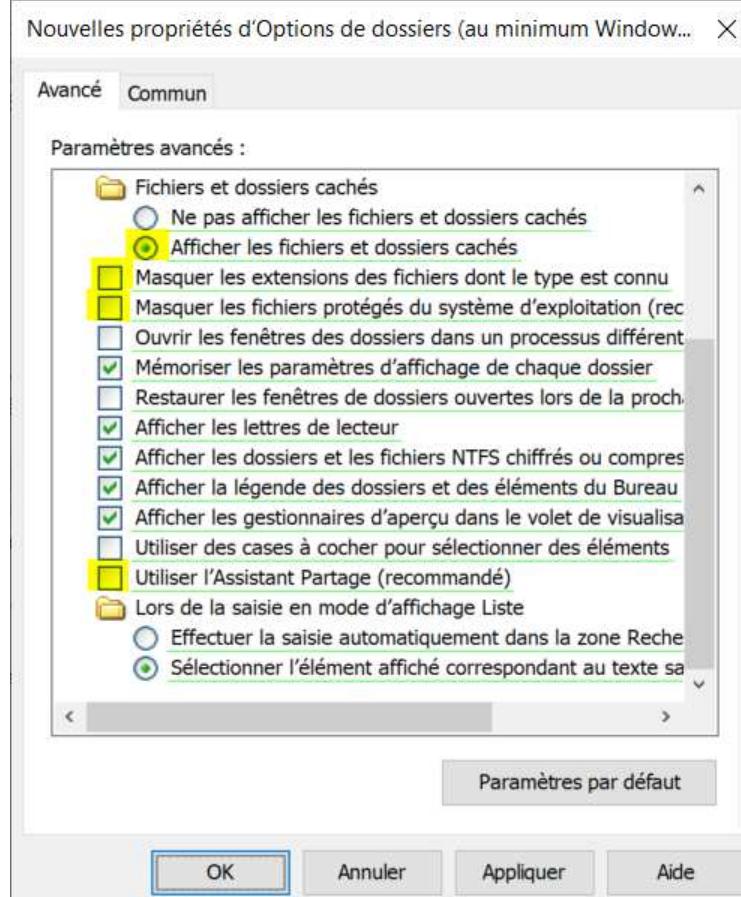
- Action: Mettre à jour
- Nom: Connexions réseau
- Type de cible: Objet du système de fichiers
- Emplacement: Bureau
- Chemin d'accès cible: c:\windows\system32\ncpa.cpl
- Chemin d'accès du fichier d'icône: c:\windows\system32\netshell.dll
- Index de l'icône: 0
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Configuration utilisateur / Préférences / Paramètres du Panneau de configuration / Options des dossiers

Configurer les options de dossiers qui permettront

● Options des dossiers

dans le menu contextuel de la fenêtre blanche,
sélectionner "Nouveau / Options des dossiers (au minimum Windows Vista)"



- ACTIVÉ Afficher les fichiers et dossiers cachés
- DÉSACTIVÉ Masquer les extensions des fichiers dont le type est connu
- DÉSACTIVÉ Masques les fichiers protégés du système d'exploitation (recommandé)
- DÉSACTIVÉ Utiliser l'assistant de Partage (recommandé)
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Création d'une GPO de préférences au niveau de la UO INFORMATIQUE

Créer une GPO "PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20" et la lier à votre unité d'organisation "INFORMATIQUE"

Désactiver la section "Configuration ordinateur".

Toutes les options se trouvent dans la section "Configuration utilisateur / Préférences"

Configuration utilisateur / Préférences / Paramètres Windows / Environnement

Créer une variable d'environnement pour l'utilisateur EMP09.

Créer une variable d'environnement pour l'utilisateur EMP20.

Créer une variable d'environnement pour les utilisateurs.

Nom	Action	Valeur	Utilisateur	Ordre
V09	Remplacer	EMP09	Oui	1
V20	Remplacer	EMP20	Oui	2
DIRCMD	Remplacer	/a/o	Oui	3

● Environnement

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

- Action: Remplacer
- Onglet Général
 - ❖ Variable utilisateur
 - ❖ Nom: V09
 - ❖ Valeur: EMP09
- Onglet Commun
 - ❖ Cocher "Supprimer l'élément lorsqu'il n'est plus appliqué"
 - ❖ Ciblage au niveau de l'élément: **EMP09**
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

- Action: Remplacer
- Onglet Général
 - ❖ Variable utilisateur
 - ❖ Nom: V20
 - ❖ Valeur: EMP20
- Onglet Commun
 - ❖ Cocher "Supprimer l'élément lorsqu'il n'est plus appliqué"
 - ❖ Ciblage au niveau de l'élément: **EMP20**
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

- Action: Remplacer
- Onglet Général
 - ❖ Variable utilisateur
 - ❖ Nom: DIRCMD
 - ❖ Valeur: /a/o
- Onglet Commun
 - ❖ Cocher "Supprimer l'élément lorsqu'il n'est plus appliqué"
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Validation

Sur le SERVEUR2

Ouvrir une session avec l'utilisateur **EMP07**

- Vérifier l'application des paramètres des préférences qui sont dans les deux GPO
"PU_EMPLOYES"
"PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"
- Fermer la session

Ouvrir une session avec l'utilisateur **EMP09**

- Vérifier l'application des paramètres des préférences qui sont dans les deux GPO
"PU_EMPLOYES"
"PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"
- Fermer la session

Ouvrir une session avec l'utilisateur **EMP20**

- Vérifier l'application des paramètres des préférences qui sont dans les deux GPO
"PU_EMPLOYES"
"PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"
- Fermer la session

Tableau résumé

Paramètres des préférences de la GPO "PU_EMPLOYES"	EMP07	EMP09	EMP20
Le lecteur R: est mappé vers \\formation.local\\netlogon	OUI	OUI	OUI
Écran de veille "Bulles" et les bulles sont opaques	OUI	OUI	OUI
Présence du raccourci vers NCPA.CPL sur le Bureau	OUI	OUI	OUI
Les quatre options des dossiers sont présentes	OUI	OUI	OUI

Paramètres des préférences de la GPO "PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"	EMP07	EMP09	EMP20
Présence des variables d'environnement: V09 V20 DIRCMD	NON NON OUI	OUI NON OUI	NON OUI OUI

L'utilisateur EMP07 est dans l'unité d'organisation suivante:

OU=ANALYSTES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

L'utilisateur EMP09 est dans l'unité d'organisation suivante:

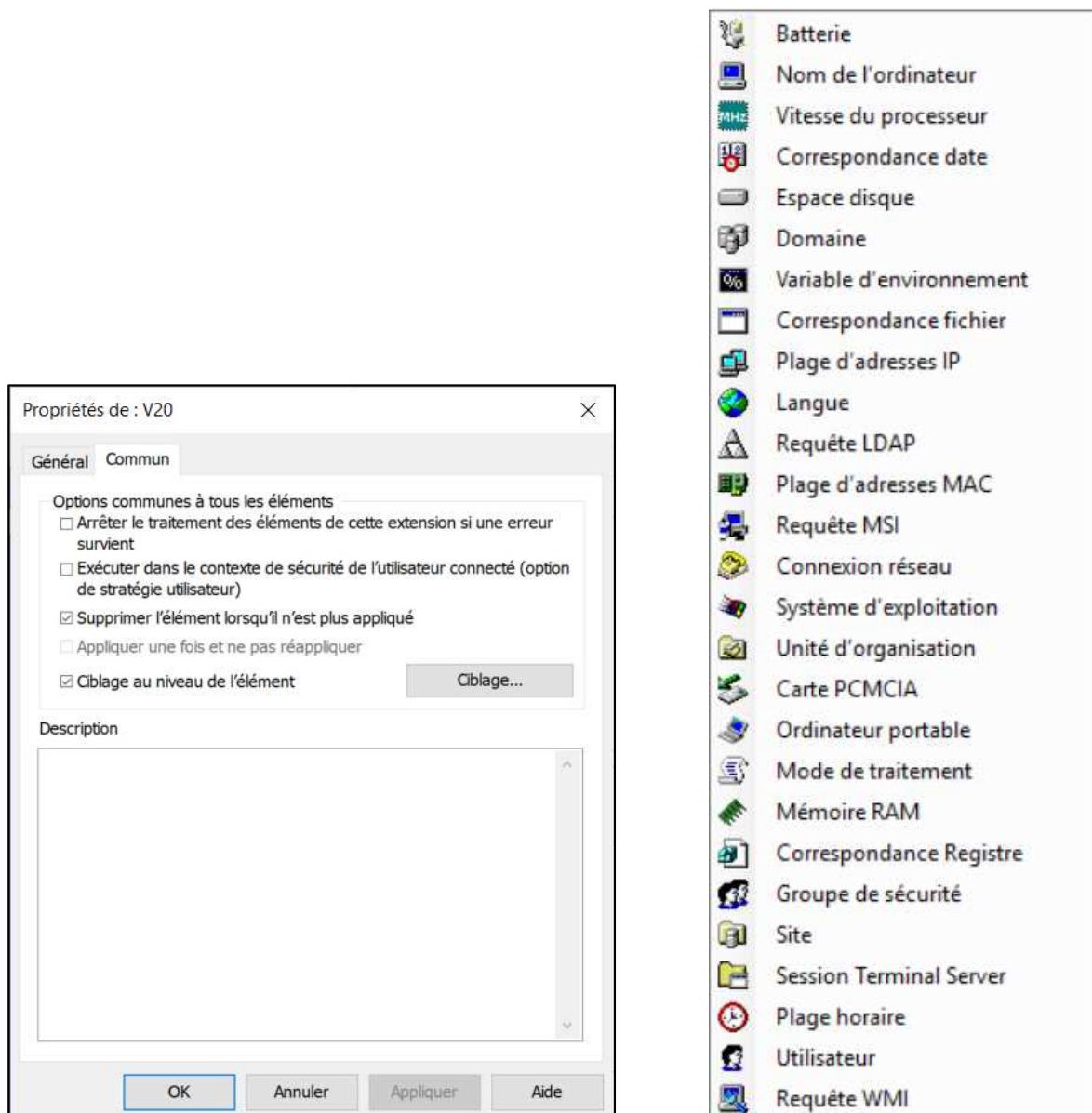
OU=GESTIONNAIRES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

L'utilisateur EMP20 est dans l'unité d'organisation suivante:

OU=TECHNICIENS_RESEAU,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

ANNEXE

Voici les différents critères qui sont disponibles pour le ciblage.



ANNEXE

Commande qui permet de démarrer l'écran de veille "Bulles" avec une commande.
`C:\Windows\System32\Bubbles.scr /s`

Stratégies "Utilisateur"

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Introduction aux stratégies "Utilisateur"
- Utiliser la modélisation et les rapports résultants

Étape 1 - Mise en place

Les unités d'organisations et les utilisateurs de l'unité d'organisation FORMATION doivent exister.

Voici la structure des 41 unités d'organisation



IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

Étape 2 - Création d'un objet de stratégie de groupe

Créer la stratégie "U_EMPLOYES" et la lier à votre unité d'organisation "EMPLOYES".

Désactiver la section "Ordinateur" de votre stratégie

Modifier votre stratégie "U_EMPLOYES" en paramétrant ce qui suit:

Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau

"Papier peint du Bureau"

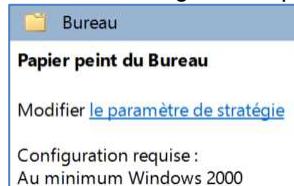
- Activé
Nom du papier peint = \\formation.local\netlogon\Logo_Corpo.jpg
Style du papier peint = Remplir

Vous devez trouver un fichier JPG qui servira de fond d'écran et qui sera déposé dans le partage NETLOGON.
Vous devez donner un nom significatif au fichier, par exemple "Logo_Corpo.jpg".

Je vous recommande de vérifier que le chemin pour le papier peint est valide.

Si le fond d'écran est complètement noir lorsque la GPO s'applique c'est parce que le chemin pour le papier peint n'est pas valide.

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.

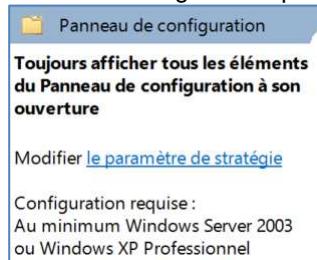


Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration

"Toujours afficher tous les éléments du Panneau de configuration à son ouverture"

- Activé

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.



Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration / Personnalisation

"Forcer un écran de veille spécifique"

- Activé

Nom du fichier exécutable de l'écran de veille: bubbles.scr

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.

Personnalisation

Forcer un écran de veille spécifique

Modifier [le paramètre de stratégie](#)

Configuration requise :
Au minimum Windows 2000 Service Pack 1

Configuration utilisateur / Stratégies / Modèles d'administration / Composants Windows / Explorateur de fichiers

"Démarrer l'Explorateur de fichiers avec le ruban réduit"

- Activé

Sélectionner: "Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit"

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.

Explorateur de fichiers

Démarrer l'Explorateur de fichiers avec le ruban réduit

Modifier [le paramètre de stratégie](#)

Configuration requise :
Au minimum Windows Server 2012, Windows 8 ou Windows RT

Étape 3 - Validation

Sur le SERVEUR2

Ouvrir une session avec un des utilisateurs de l'unité d'organisation FORMATION
note: le nom des utilisateurs varie de **EMP01** à **EMP32**

- Vérifier l'application de chaque paramètre de votre stratégie "U_EMPLOYES"
- Fermer la session

Tableau résumé

Paramètres	EMP01 à EMP32 Répondre par Oui ou NON
Papier peint utilise le fichier Logo_Corpo.jpg	OUI
Affichage du panneau de configuration (pas en catégorie)	OUI
Écran de veille est "Bulles"	OUI
Explorateur de fichiers ouvre sans le ruban réduit	OUI

Étape 4 - Modélisation

Dans la console "Gestion de stratégie de groupe"

- Section "Modélisation de stratégie de groupe"
- Menu contextuel
Vous devez sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations générales à effectuer dans l'Assistant de modélisation de stratégie de groupe

- Sélection du contrôleur de domaine
Vous devez sélectionner l'option "Tout contrôleur de domaine exécutant ..."
- Sélection d'ordinateurs et d'utilisateurs
 - Sélectionner "Utilisateur"
Parcourir pour sélectionner l'utilisateur visé par la modélisation
 - Sélectionner "Ordinateur"
Parcourir pour sélectionner le serveur virtuel 2
 - Cocher l'option "Se rendre à la dernière page de cet Assistant ..."

Lorsque le rapport s'affiche, il est possible de l'enregistrer dans un fichier HTML.

Étape 5 - Jeu de stratégies résultant

Sur votre serveur virtuel 2

Ouvrir une session avec un des utilisateurs de l'unité d'organisation FORMATION

note: le nom des utilisateurs varie de **EMP01** à **EMP32**

Exécuter la commande suivante: RSOP.MSC

Le refus sur la section Ordinateur est normal étant donné que les utilisateurs de l'unité d'organisation FORMATION ne sont pas membres du groupe "Administrateurs".

RSOP.MSC affiche le jeu de stratégies résultant dans une fenêtre.

RSOP.MSC ne permet pas de sauvegarder le résultat dans un fichier.

Exécuter la commande suivante dans une invite de commandes (ne pas exécuter en tant qu'administrateur)

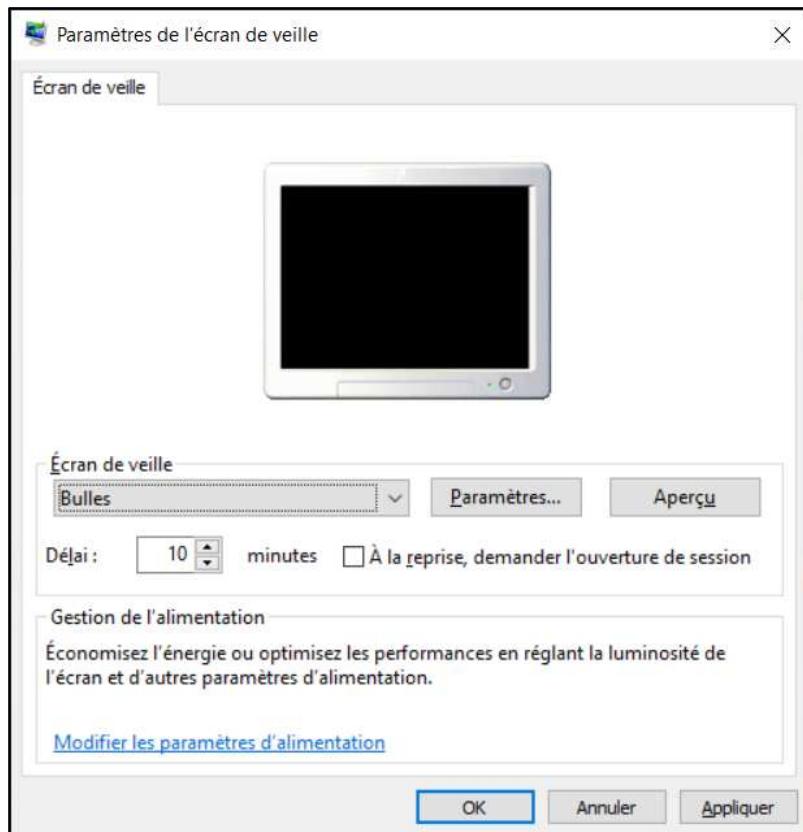
- **gpresult.exe /SCOPE USER /H C:_outils\rapport_EMPxx.html /F**
Consulter le fichier C:_outils\rapport_EMPxx.html

Fermer cette session

La commande gpresult.exe permet de sauvegarder le résultat dans un fichier HTML.

ANNEXE

Comment ouvrir la console "Paramètres de l'écran de veille" avec une commande.
control.exe desk.cpl,screensaver,@screensaver



GPO au niveau du domaine

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Créer une GPO au niveau du domaine

IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

Lorsqu'on configure des paramètres de sécurité au niveau du domaine c'est pour améliorer la sécurité.

Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos doivent être configurées au niveau du domaine.

Création d'une GPO au niveau du domaine

Exemple d'une GPO "C_Domaine_Mot de passe"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de mot de passe

- Longueur minimale du mot de passe
note: configurer la valeur de ce paramètre à 9 caractères

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de verrouillage du compte

- Seuil de verrouillage du compte
note: configurer la valeur de ce paramètre à 5

Les deux autres paramètres sont configurés automatiquement à 30 minutes.

Stratégie	Paramètres de stratégie
Durée de verrouillage des comptes	30 minutes
Réinitialiser le compteur de verrouillages du compte après	30 minutes
Seuil de verrouillage du compte	5 tentatives d'ouvertures de session non valides

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

- Ouverture de session interactive: prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire
note: configurer la valeur de ce paramètre à 7 jours

Dans la console de gestion des GPO

- Lier la GPO "C_Domaine_Mot de passe" au niveau du domaine
- Dans **"Ordre des liens"**

Vous devez associer le plus petit chiffre (le chiffre 1) à la GPO "**C_Domaine_Mot de passe**".
Plus le chiffre est petit, plus grande est la priorité d'exécution de la GPO.

FORMATION.LOCAL					
État	Objets de stratégie de groupe liés	Héritage de stratégie de groupe	Délégation		
Ordre des liens	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO	
1	C_Domaine_Mot de passe	Non	Oui	Paramètres de configuration utilisateurs désactivés	
2	Default Domain Policy	Non	Oui	Activé	

La commande "**net accounts**" permet d'afficher des informations pour les stratégies de mot de passe et les stratégies de verrouillage du compte.

```
C:\Windows\system32\cmd.exe
E:\>whoami
formation\emp09

E:\>net accounts
Fermeture forcée de la session après expiration ? : Jamais
Durée de vie minimale du mot de passe (jours) : 1
Durée de vie maximale du mot de passe (jours) : 42
Longueur minimale du mot de passe : 9
Nombre de mots de passe antérieurs à conserver : 24
Seuil de verrouillage : 5
Durée du verrouillage (min) : 30
Fenêtre d'observation du verrouillage (min) : 30
Rôle de l'ordinateur : SERVEUR
La commande s'est terminée correctement.

E:\>
```

Voici les informations pour les stratégies de mot de passe et les stratégies de verrouillage du compte pour le domaine **RESEAUCVM**.

```
Invité de commandes
X:\>echo %USERDOMAIN%
RESEAUCVM

X:\>net accounts
Fermeture forcée de la session après expiration ? : Jamais
Durée de vie minimale du mot de passe (jours) : 0
Durée de vie maximale du mot de passe (jours) : 42
Longueur minimale du mot de passe : 6
Nombre de mots de passe antérieurs à conserver : 1
Seuil de verrouillage : 5
Durée du verrouillage (min) : 5
Fenêtre d'observation du verrouillage (min) : 5
Rôle de l'ordinateur : STATION
La commande s'est terminée correctement.

X:\>
```

Modélisation

Dans la console "Gestion de stratégie de groupe"

- Section "Modélisation de stratégie de groupe"

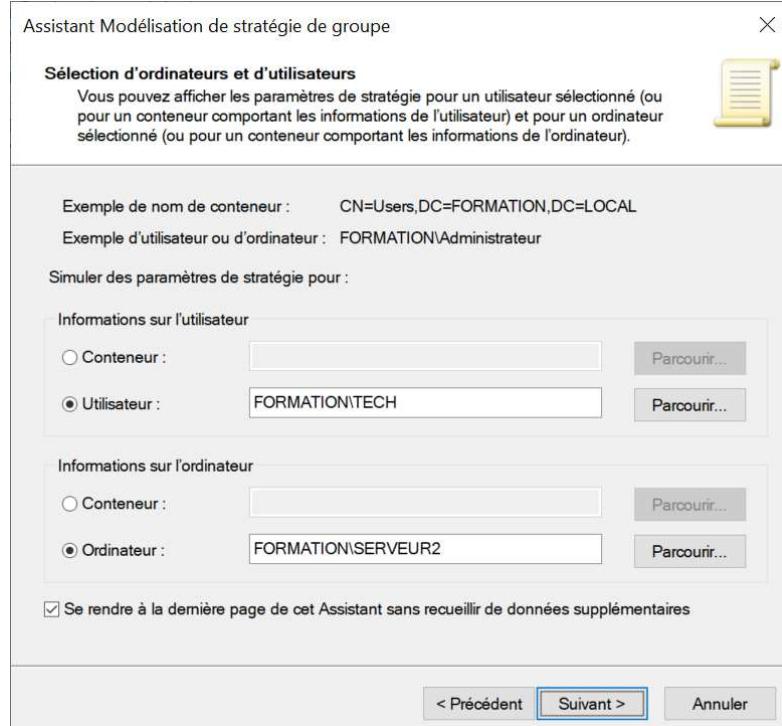
Dans le menu contextuel, vous devez sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations à effectuer dans l'Assistant de modélisation de stratégie de groupe

- Sélection du contrôleur de domaine

Vous devez sélectionner l'option "Tout contrôleur de domaine exécutant ..."

- Sélection d'ordinateurs et d'utilisateurs



Cocher l'option "**Se rendre à la dernière page de cet Assistant ...**"

Lorsque le rapport s'affiche, il est possible de l'enregistrer dans un fichier HTML.

"Default Domain Policy" et "Default Domain Controllers Policy"

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Insaller la console "Gestion des stratégies de groupe" sur le SERVEUR2
- Utiliser la console "Gestion des stratégies de groupe"
- Se familiariser avec les objets de stratégie "Default Domain Policy" et "Default Domain Controllers Policy"

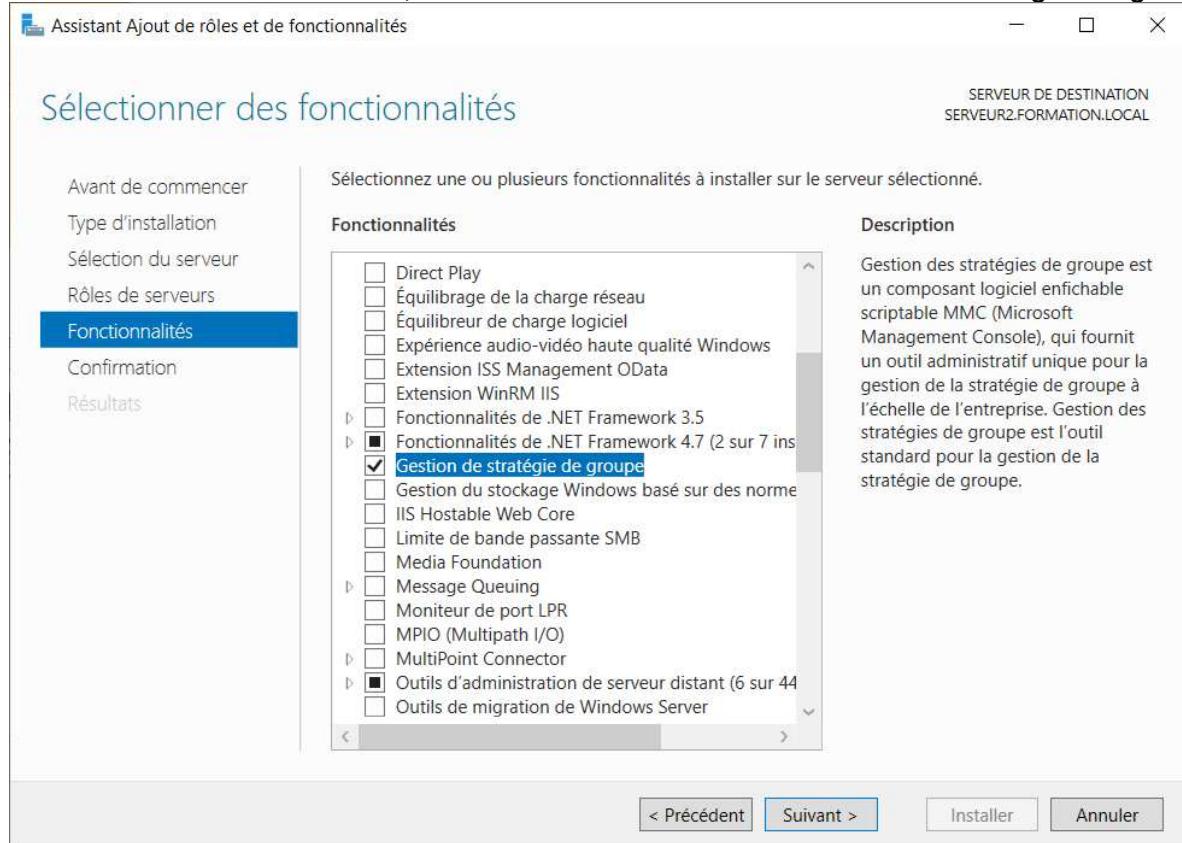
IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

La console "Gestion des stratégies de groupe"

La console "Gestion des stratégies de groupe" est présente par défaut sur le SERVEUR1 parce que c'est le contrôleur de domaine.

Sur le serveur virtuel SERVEUR2, vous devez installer la console "Gestion des stratégies de groupe".



Informations sur la GPO "Default Domain Policy"

Aucun paramètre n'est défini dans la section "Configuration utilisateur" de la GPO "Default Domain Policy".

Default Domain Policy

Étendue Détails Paramètres Délegation État

Default Domain Policy
Données recueillies le : 2024-06-04 15:13:09

Général

Détails afficher tout
Liaisons masquer
Filtrage de sécurité afficher
Délegation afficher

Configuration ordinateur (activée)

Stratégies masquer
Paramètres Windows masquer
Paramètres de sécurité afficher

Configuration utilisateur (activée)

Aucun paramètre n'est défini.

Les paramètres de la GPO "Default Domain Policy" s'appliquent sur toutes les OU du domaine.

Ce n'est pas une bonne idée de modifier les paramètres des la GPO "Default Domain Policy".

Ce n'est pas une bonne idée de configurer des GPO au niveau du domaine parce que les paramètres s'appliquent sur toutes les OU du domaine incluant l'unité d'organisation "Domain Controllers".

Informations sur la GPO "Default Domain Controllers Policy"

Aucun paramètre n'est défini dans la section "Configuration utilisateur" de la GPO "Default Domain Controllers Policy".

Default Domain Controllers Policy

Étendue Détails Paramètres Délegation État

Default Domain Controllers Policy
Données recueillies le : 2024-06-04 15:06:42

Général

Détails masquer
Liaisons afficher
Filtrage de sécurité afficher
Délegation afficher

Configuration ordinateur (activée)

Stratégies masquer
Paramètres Windows masquer
Paramètres de sécurité afficher

Configuration utilisateur (activée)

Aucun paramètre n'est défini.

Ce n'est pas une bonne idée de modifier les paramètres des la GPO "Default Domain Controllers Policy".

Étape 1a - La GPO "Default Domain Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "**Paramètres**".



Vous pouvez créer un rapport HTM de la GPO "Default Domain Policy" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "Default Domain Policy" et dans le menu contextuel sélectionner "**Enregistrer le rapport...**".

L'avantage d'un fichier HTM par rapport à l'onglet "**Paramètres**", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 1b – Les paramètres de la GPO "Default Domain Policy"

Voici les paramètres de la GPO "Default Domain Policy".

Configuration ordinateur (activée)															
Stratégies	masquer														
Paramètres Windows	masquer														
Paramètres de sécurité	masquer														
Stratégies de comptes/ Stratégie de mot de passe	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Antériorité maximale du mot de passe</td><td>42 jours</td></tr><tr><td>Antériorité minimale du mot de passe</td><td>1 jours</td></tr><tr><td>Appliquer l'historique des mots de passe</td><td>24 mots de passe mémorisés</td></tr><tr><td>Enregistrer les mots de passe en utilisant un chiffrement réversible</td><td>Désactivé</td></tr><tr><td>Le mot de passe doit respecter des exigences de complexité</td><td>Activé</td></tr><tr><td>Longueur minimale du mot de passe</td><td>7 caractères</td></tr></tbody></table>	Stratégie	Paramètre	Antériorité maximale du mot de passe	42 jours	Antériorité minimale du mot de passe	1 jours	Appliquer l'historique des mots de passe	24 mots de passe mémorisés	Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé	Le mot de passe doit respecter des exigences de complexité	Activé	Longueur minimale du mot de passe	7 caractères	
Stratégie	Paramètre														
Antériorité maximale du mot de passe	42 jours														
Antériorité minimale du mot de passe	1 jours														
Appliquer l'historique des mots de passe	24 mots de passe mémorisés														
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé														
Le mot de passe doit respecter des exigences de complexité	Activé														
Longueur minimale du mot de passe	7 caractères														
Stratégies de comptes/ Stratégie de verrouillage du compte	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Seuil de verrouillage de comptes</td><td>0 tentative d'ouverture de session non valides</td></tr></tbody></table>	Stratégie	Paramètre	Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides											
Stratégie	Paramètre														
Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides														
Stratégies de comptes/ Stratégie Kerberos	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Appliquer les restrictions pour l'ouverture de session</td><td>Activé</td></tr><tr><td>Durée de vie maximale du ticket d'utilisateur</td><td>10 heures</td></tr><tr><td>Durée de vie maximale du ticket de service</td><td>600 minutes</td></tr><tr><td>Durée de vie maximale pour le renouvellement du ticket utilisateur</td><td>7 jours</td></tr><tr><td>Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur</td><td>5 minutes</td></tr></tbody></table>	Stratégie	Paramètre	Appliquer les restrictions pour l'ouverture de session	Activé	Durée de vie maximale du ticket d'utilisateur	10 heures	Durée de vie maximale du ticket de service	600 minutes	Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours	Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes			
Stratégie	Paramètre														
Appliquer les restrictions pour l'ouverture de session	Activé														
Durée de vie maximale du ticket d'utilisateur	10 heures														
Durée de vie maximale du ticket de service	600 minutes														
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours														
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes														
Stratégies locales/ Options de sécurité	masquer														
Accès réseau	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Accès réseau : permet la traduction de noms/ SID anonymes</td><td>Désactivé</td></tr></tbody></table>	Stratégie	Paramètre	Accès réseau : permet la traduction de noms/ SID anonymes	Désactivé											
Stratégie	Paramètre														
Accès réseau : permet la traduction de noms/ SID anonymes	Désactivé														
Sécurité réseau	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe</td><td>Activé</td></tr><tr><td>Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent</td><td>Désactivé</td></tr></tbody></table>	Stratégie	Paramètre	Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé	Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé									
Stratégie	Paramètre														
Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé														
Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé														
Stratégies de clé publique/ Système de fichiers de chiffrement	masquer														
Certificats	masquer														
<table><thead><tr><th>Émise à</th><th>Délivré par</th><th>Date d'expiration</th><th>Rôles prévus</th></tr></thead><tbody><tr><td>Administrateur</td><td>Administrateur</td><td>2123-08-10 19:49:04</td><td>Récupération de fichiers</td></tr></tbody></table>	Émise à	Délivré par	Date d'expiration	Rôles prévus	Administrateur	Administrateur	2123-08-10 19:49:04	Récupération de fichiers							
Émise à	Délivré par	Date d'expiration	Rôles prévus												
Administrateur	Administrateur	2123-08-10 19:49:04	Récupération de fichiers												

Pour obtenir plus d'informations sur les paramètres, exécutez l'Éditeur d'objet de stratégie de groupe locale.

Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos sont définies pour l'ensemble du domaine dans Active Directory.

En utilisant la console "Gestion des stratégies de groupe" sélectionner la GPO "Default Domain Policy"

- Vous devez choisir "**Modifier...**" dans le menu contextuel.
- Vous devez sélectionner le paramètre.
note: vous devez vous déplacer jusqu'à l'emplacement du paramètre recherché
- Vous devez afficher les propriétés du paramètre et cliquer sur l'onglet "**Expliquer**".

Voici la section que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de mot de passe**

Stratégie	Paramètres de stratégie
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	42 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	7 caractère(s)

"Antériorité maximale du mot de passe" **42 jours**

Quelle est la valeur recommandée pour le paramètre "Durée de vie maximale du mot de passe" ?
un délai entre 30 et 90 jours

réponse: _____

Quelle est la valeur maximale pour le paramètre "Durée de vie maximale du mot de passe" ?

999 jours

réponse: _____

"Antériorité minimale du mot de passe" **1 jours**

Que signifie le paramètre "Durée de vie minimale du mot de passe" ?

Le nombre de jours avant qu'un utilisateur puisse changer son mot de passe.

réponse: _____

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

1 jours

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

0 jours

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Appliquer l'historique des mots de passe

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

24

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

0

réponse: _____

Remarque : par défaut, les ordinateurs membres suivent la configuration de leur contrôleur de domaine.

Le mot de passe doit respecter des exigences de complexité Activé

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

Activé

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

Désactivé

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Voici les recommandations de Microsoft sur les exigences de complexité.

Le mot de passe doit respecter des exigences de complexité

Ce paramètre de sécurité détermine si les mots de passe doivent respecter des exigences de complexité.

Si cette stratégie est activée, les mots de passe doivent respecter les exigences minimales suivantes :

Ne pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur comptant plus de deux caractères successifs

Comporter au moins six caractères

Contenir des caractères provenant de trois des quatre catégories suivantes :

- Caractères majuscules anglais (A à Z)
- Caractères minuscules anglais (a à z)
- Chiffres en base 10 (0 à 9)
- Caractères non alphabétiques (par exemple, !, \$, #, %)

Les exigences de complexité sont appliquées lors du changement ou de la création de mots de passe.

Longueur minimale du mot de passe

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

7

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

0

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Quelle est la plus grande longueur minimale pour les mots de passe ?

14 caractères

réponse: _____

Voici la section que vous devez consulter pour répondre à la prochaine question.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de verrouillage du compte**

Stratégie	Paramètres de stratégie
Durée de verrouillage des comptes	Non défini
Réinitialiser le compteur de verrouillages du compte après	Non défini
Seuil de verrouillage du compte	0 tentatives d'ouvertures de session non valides

Seuil de verrouillage de comptes

0 tentative d'ouverture de session non valides

Que signifie la valeur 0 pour ce paramètre ?

La valeur 0 signifie que le compte ne se sera jamais verrouillé.

réponse: _____

Quelle est la plus grande valeur pour le seuil de verrouillage de comptes ?

999

réponse: _____

Le paramètre "Seuil de verrouillage de comptes" dans une GPO fonctionne seulement si la GPO est liée au domaine en raison de la manière dont les stratégies de verrouillage de compte sont appliquées dans Active Directory.

Si vous définissez ces paramètres dans une GPO liée à une OU, les contrôleurs de domaine ne prendront pas en compte ces paramètres pour la gestion des tentatives de connexion et du verrouillage des comptes.

Voici l'explication d'un paramètre important de cette GPO.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie Kerberos**

Stratégie	Paramètres de stratégie
Appliquer les restrictions pour l'ouverture de session	Activé
Durée de vie maximale du ticket de service	600 minutes
Durée de vie maximale du ticket utilisateur	10 minutes
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 minutes
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

"Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur" 5 minutes

Pour permettre le bon fonctionnement des horodatages, les horloges du client et du contrôleur de domaine doivent être aussi synchronisées que possible. En d'autres termes, les deux ordinateurs doivent être réglés aux mêmes date et heure. Ce paramètre accepte une marge d'erreur de 5 minutes.

C'est un paramètre important de l'Active Directory.

Étape 2a - La GPO "Default Domain Controllers Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "Paramètres".

Default Domain Controllers Policy

Étendue Détails Paramètres Délégation État

Vous pouvez créer un rapport HTM de la GPO "Default Domain Controllers Policy" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "Default Domain Controllers Policy" et dans le menu contextuel sélectionner "Enregistrer le rapport..." .

L'avantage d'un fichier HTM par rapport à l'onglet "Paramètres", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 2b – Les paramètres de la GPO "Default Domain Controllers Policy"

Voici les paramètres de la GPO "Default Domain Controllers Policy".

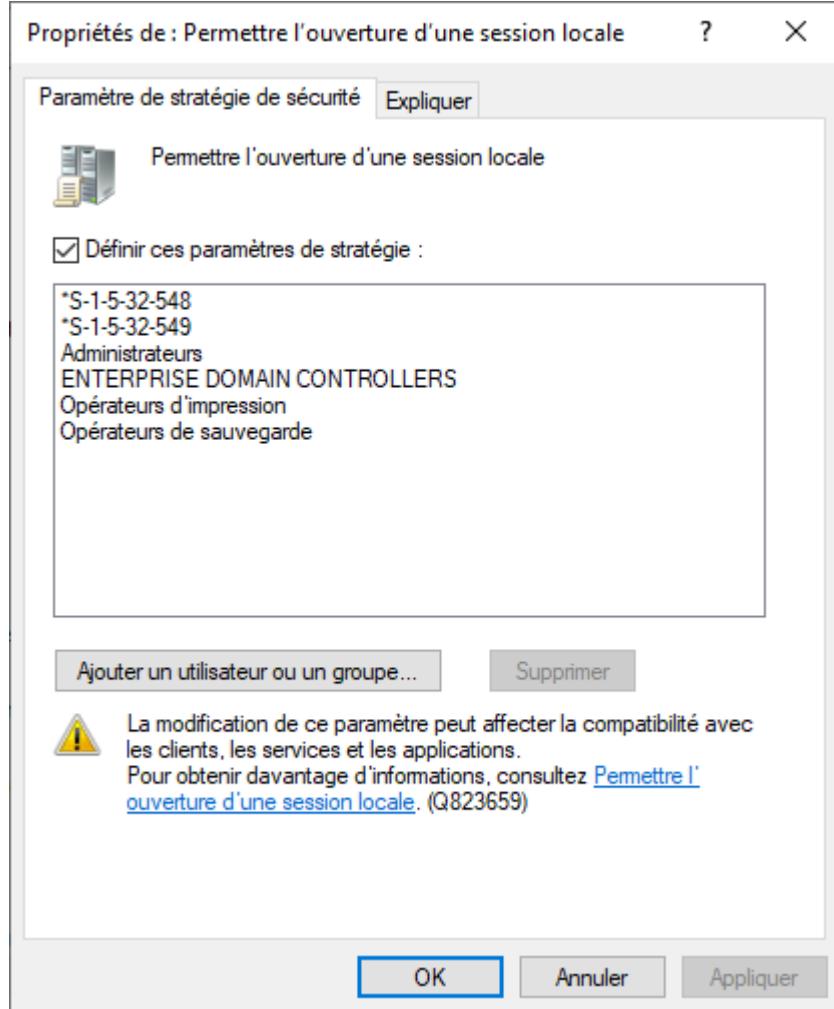
Configuration ordinateur (activée)	
Stratégies	masquer
Paramètres Windows	masquer
Paramètres de sécurité	masquer
Stratégies locales/ Attribution des droits utilisateur	masquer
Stratégie	Paramètre
Accéder à cet ordinateur à partir du réseau	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, Tout le monde
Ajouter des stations de travail au domaine	AUTORITE NT\Utilisateurs authentifiés
Ajuster les quotas de mémoire pour un processus	BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL
Arrêter le système	BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Augmenter la priorité de planification	Window Manager\Window Manager Group, BUILTIN\Administrateurs
Charger et décharger les pilotes de périphériques	BUILTIN\Opérateurs d'impression, BUILTIN\Administrateurs
Contourner la vérification de parcours	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL, Tout le monde
Créer un fichier d'échange	BUILTIN\Administrateurs
Déboguer les programmes	BUILTIN\Administrateurs
Forcer l'amét à partir d'un système distant	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs
Générer des audits de sécurité	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL
Gérer le journal d'audit et de sécurité	BUILTIN\Administrateurs
Modifier l'heure système	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs, AUTORITE NT\SERVICE LOCAL
Modifier les valeurs de l'environnement du microprogramme	BUILTIN\Administrateurs
Ouvrir une session en tant que tâche	BUILTIN\Utilisateurs du journal de performances, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Performance système du profil	NT SERVICE\WdiServiceHost, BUILTIN\Administrateurs
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	BUILTIN\Administrateurs
Permettre l'ouverture d'une session locale	AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de compte, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Prendre possession de fichiers ou d'autres objets	BUILTIN\Administrateurs
Processus unique du profil	BUILTIN\Administrateurs
Remplacer un jeton de niveau processus	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL
Restaurer les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Retirer l'ordinateur de la station d'accueil	BUILTIN\Administrateurs
Sauvegarder les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs

Les paramètres de la section "Attribution des droits utilisateur" servent à déterminer **qui peut faire quoi**.

Voici l'explication d'un paramètre important de cette GPO.

Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur

Permettre l'ouverture d'une session locale



Les utilisateurs du domaine ne peuvent pas se connecter sur le "Contrôleur de domaine".

C'est un paramètre important de l'Active Directory.

"Default Domain Policy" et "Default Domain Controllers Policy"

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Installer la console "Gestion des stratégies de groupe" sur le SERVEUR2
- Utiliser la console "Gestion des stratégies de groupe"
- Se familiariser avec les objets de stratégie "Default Domain Policy" et "Default Domain Controllers Policy"

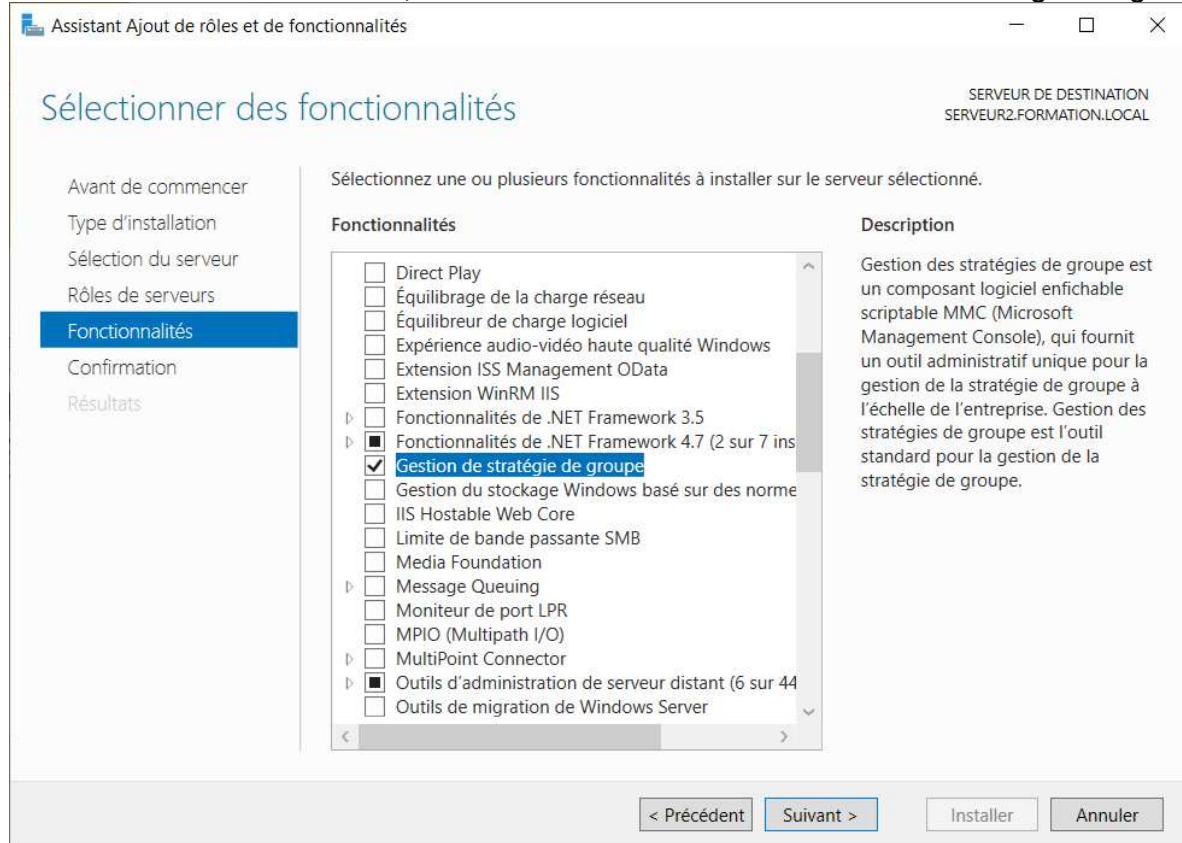
IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

La console "Gestion des stratégies de groupe"

La console "Gestion des stratégies de groupe" est présente par défaut sur le SERVEUR1 parce que c'est le contrôleur de domaine.

Sur le serveur virtuel SERVEUR2, vous devez installer la console "Gestion des stratégies de groupe".



Informations sur la GPO "Default Domain Policy"

Aucun paramètre n'est défini dans la section "**Configuration utilisateur**" de la GPO "**Default Domain Policy**".

Default Domain Policy

Étendue Détails Paramètres Délegation État

Default Domain Policy
Données recueillies le : 2024-06-04 15:13:09

Général

Détails afficher tout
Liaisons masquer
Filtrage de sécurité afficher
Délegation afficher

Configuration ordinateur (activée)

Stratégies masquer
Paramètres Windows masquer
Paramètres de sécurité afficher

Configuration utilisateur (activée)

Aucun paramètre n'est défini.

Les paramètres de la GPO "**Default Domain Policy**" s'appliquent sur toutes les OU du domaine.

Ce n'est pas une bonne idée de modifier les paramètres des la GPO "**Default Domain Policy**".

Ce n'est pas une bonne idée de configurer des GPO au niveau du domaine parce que les paramètres s'appliquent sur toutes les OU du domaine incluant l'unité d'organisation "**Domain Controllers**".

Informations sur la GPO "Default Domain Controllers Policy"

Aucun paramètre n'est défini dans la section "**Configuration utilisateur**" de la GPO "**Default Domain Controllers Policy**".

Default Domain Controllers Policy

Étendue Détails Paramètres Délegation État

Default Domain Controllers Policy
Données recueillies le : 2024-06-04 15:06:42

Général

Détails afficher tout
Liaisons masquer
Filtrage de sécurité afficher
Délegation afficher

Configuration ordinateur (activée)

Stratégies masquer
Paramètres Windows masquer
Paramètres de sécurité afficher

Configuration utilisateur (activée)

Aucun paramètre n'est défini.

Ce n'est pas une bonne idée de modifier les paramètres de la GPO "**Default Domain Controllers Policy**".

Étape 1a - La GPO "Default Domain Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "**Paramètres**".



Vous pouvez créer un rapport HTM de la GPO "Default Domain Policy" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "Default Domain Policy" et dans le menu contextuel sélectionner "**Enregistrer le rapport...**".

L'avantage d'un fichier HTM par rapport à l'onglet "**Paramètres**", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 1b – Les paramètres de la GPO "Default Domain Policy"

Voici les paramètres de la GPO "Default Domain Policy".

Configuration ordinateur (activée)															
Stratégies	masquer														
Paramètres Windows	masquer														
Paramètres de sécurité	masquer														
Stratégies de comptes/ Stratégie de mot de passe	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Antériorité maximale du mot de passe</td><td>42 jours</td></tr><tr><td>Antériorité minimale du mot de passe</td><td>1 jours</td></tr><tr><td>Appliquer l'historique des mots de passe</td><td>24 mots de passe mémorisés</td></tr><tr><td>Enregistrer les mots de passe en utilisant un chiffrement réversible</td><td>Désactivé</td></tr><tr><td>Le mot de passe doit respecter des exigences de complexité</td><td>Activé</td></tr><tr><td>Longueur minimale du mot de passe</td><td>7 caractères</td></tr></tbody></table>	Stratégie	Paramètre	Antériorité maximale du mot de passe	42 jours	Antériorité minimale du mot de passe	1 jours	Appliquer l'historique des mots de passe	24 mots de passe mémorisés	Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé	Le mot de passe doit respecter des exigences de complexité	Activé	Longueur minimale du mot de passe	7 caractères	
Stratégie	Paramètre														
Antériorité maximale du mot de passe	42 jours														
Antériorité minimale du mot de passe	1 jours														
Appliquer l'historique des mots de passe	24 mots de passe mémorisés														
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé														
Le mot de passe doit respecter des exigences de complexité	Activé														
Longueur minimale du mot de passe	7 caractères														
Stratégies de comptes/ Stratégie de verrouillage du compte	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Seuil de verrouillage de comptes</td><td>0 tentative d'ouverture de session non valides</td></tr></tbody></table>	Stratégie	Paramètre	Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides											
Stratégie	Paramètre														
Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides														
Stratégies de comptes/ Stratégie Kerberos	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Appliquer les restrictions pour l'ouverture de session</td><td>Activé</td></tr><tr><td>Durée de vie maximale du ticket d'utilisateur</td><td>10 heures</td></tr><tr><td>Durée de vie maximale du ticket de service</td><td>600 minutes</td></tr><tr><td>Durée de vie maximale pour le renouvellement du ticket utilisateur</td><td>7 jours</td></tr><tr><td>Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur</td><td>5 minutes</td></tr></tbody></table>	Stratégie	Paramètre	Appliquer les restrictions pour l'ouverture de session	Activé	Durée de vie maximale du ticket d'utilisateur	10 heures	Durée de vie maximale du ticket de service	600 minutes	Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours	Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes			
Stratégie	Paramètre														
Appliquer les restrictions pour l'ouverture de session	Activé														
Durée de vie maximale du ticket d'utilisateur	10 heures														
Durée de vie maximale du ticket de service	600 minutes														
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours														
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes														
Stratégies locales/ Options de sécurité	masquer														
Accès réseau	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Accès réseau : permet la traduction de noms/ SID anonymes</td><td>Désactivé</td></tr></tbody></table>	Stratégie	Paramètre	Accès réseau : permet la traduction de noms/ SID anonymes	Désactivé											
Stratégie	Paramètre														
Accès réseau : permet la traduction de noms/ SID anonymes	Désactivé														
Sécurité réseau	masquer														
<table><thead><tr><th>Stratégie</th><th>Paramètre</th></tr></thead><tbody><tr><td>Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe</td><td>Activé</td></tr><tr><td>Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent</td><td>Désactivé</td></tr></tbody></table>	Stratégie	Paramètre	Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé	Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé									
Stratégie	Paramètre														
Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé														
Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé														
Stratégies de clé publique/ Système de fichiers de chiffrement	masquer														
Certificats	masquer														
<table><thead><tr><th>Émise à</th><th>Délivré par</th><th>Date d'expiration</th><th>Rôles prévus</th></tr></thead><tbody><tr><td>Administrateur</td><td>Administrateur</td><td>2123-08-10 19:49:04</td><td>Récupération de fichiers</td></tr></tbody></table>	Émise à	Délivré par	Date d'expiration	Rôles prévus	Administrateur	Administrateur	2123-08-10 19:49:04	Récupération de fichiers							
Émise à	Délivré par	Date d'expiration	Rôles prévus												
Administrateur	Administrateur	2123-08-10 19:49:04	Récupération de fichiers												

Pour obtenir plus d'informations sur les paramètres, exécutez l'Éditeur d'objet de stratégie de groupe locale.

Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos sont définies pour l'ensemble du domaine dans Active Directory.

En utilisant la console "**Gestion des stratégies de groupe**" sélectionner la GPO "**Default Domain Policy**"

- Vous devez choisir "**Modifier...**" dans le menu contextuel.
- Vous devez sélectionner le paramètre.
note: vous devez vous déplacer jusqu'à l'emplacement du paramètre recherché
- Vous devez afficher les propriétés du paramètre et cliquer sur l'onglet "**Expliquer**".

Voici la section que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de mot de passe**

Stratégie	Paramètres de stratégie
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	42 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	7 caractère(s)

"Antériorité maximale du mot de passe" **42 jours**

Quelle est la valeur recommandée pour le paramètre "**Durée de vie maximale du mot de passe**" ?

réponse: _____

Quelle est la valeur maximale pour le paramètre "**Durée de vie maximale du mot de passe**" ?

réponse: _____

"Antériorité minimale du mot de passe" **1 jours**

Que signifie le paramètre "**Durée de vie minimale du mot de passe**" ?

réponse: _____

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Appliquer l'historique des mots de passe

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

Réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

Réponse: _____

Remarque : par défaut, les ordinateurs membres suivent la configuration de leur contrôleur de domaine.

Le mot de passe doit respecter des exigences de complexité Activé

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

Réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

Réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Voici les recommandations de Microsoft sur les exigences de complexité.

Le mot de passe doit respecter des exigences de complexité

Ce paramètre de sécurité détermine si les mots de passe doivent respecter des exigences de complexité.

Si cette stratégie est activée, les mots de passe doivent respecter les exigences minimales suivantes :

Ne pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur comptant plus de deux caractères successifs

Comporter au moins six caractères

Contenir des caractères provenant de trois des quatre catégories suivantes :

- Caractères majuscules anglais (A à Z)
- Caractères minuscules anglais (a à z)
- Chiffres en base 10 (0 à 9)
- Caractères non alphabétiques (par exemple, !, \$, #, %)

Les exigences de complexité sont appliquées lors du changement ou de la création de mots de passe.

Longueur minimale du mot de passe

7 caractères

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

Réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

Réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Quelle est la plus grande longueur minimale pour les mots de passe ?

Réponse: _____

Voici la section que vous devez consulter pour répondre à la prochaine question.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de verrouillage du compte**

Stratégie	Paramètres de stratégie
Durée de verrouillage des comptes	Non défini
Réinitialiser le compteur de verrouillages du compte après	Non défini
Seuil de verrouillage du compte	0 tentatives d'ouvertures de session non valides

Seuil de verrouillage de comptes

0 tentative d'ouverture de session non valides

Que signifie la valeur 0 pour ce paramètre ?

Réponse: _____

Quelle est la plus grande valeur pour le seuil de verrouillage de comptes ?

Réponse: _____

Le paramètre "Seuil de verrouillage de comptes" dans une GPO fonctionne seulement si la GPO est liée au domaine en raison de la manière dont les stratégies de verrouillage de compte sont appliquées dans Active Directory.

Si vous définissez ces paramètres dans une GPO liée à une OU, les contrôleurs de domaine ne prendront pas en compte ces paramètres pour la gestion des tentatives de connexion et du verrouillage des comptes.

Voici l'explication d'un paramètre important de cette GPO.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie Kerberos**

Stratégie	Paramètres de stratégie
Appliquer les restrictions pour l'ouverture de session	Activé
Durée de vie maximale du ticket de service	600 minutes
Durée de vie maximale du ticket utilisateur	10 minutes
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 minutes
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

"Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur" 5 minutes

Pour permettre le bon fonctionnement des horodatages, les horloges du client et du contrôleur de domaine doivent être aussi synchronisées que possible. En d'autres termes, les deux ordinateurs doivent être réglés aux mêmes date et heure. Ce paramètre accepte une marge d'erreur de 5 minutes.

C'est un paramètre important de l'Active Directory.

Étape 2a - La GPO "Default Domain Controllers Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "Paramètres".

Default Domain Controllers Policy

Étendue Détails Paramètres Délégation État

Vous pouvez créer un rapport HTM de la GPO "Default Domain Controllers Policy" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "Default Domain Controllers Policy" et dans le menu contextuel sélectionner "Enregistrer le rapport..." .

L'avantage d'un fichier HTM par rapport à l'onglet "Paramètres", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 2b – Les paramètres de la GPO "Default Domain Controllers Policy"

Voici les paramètres de la GPO "Default Domain Controllers Policy".

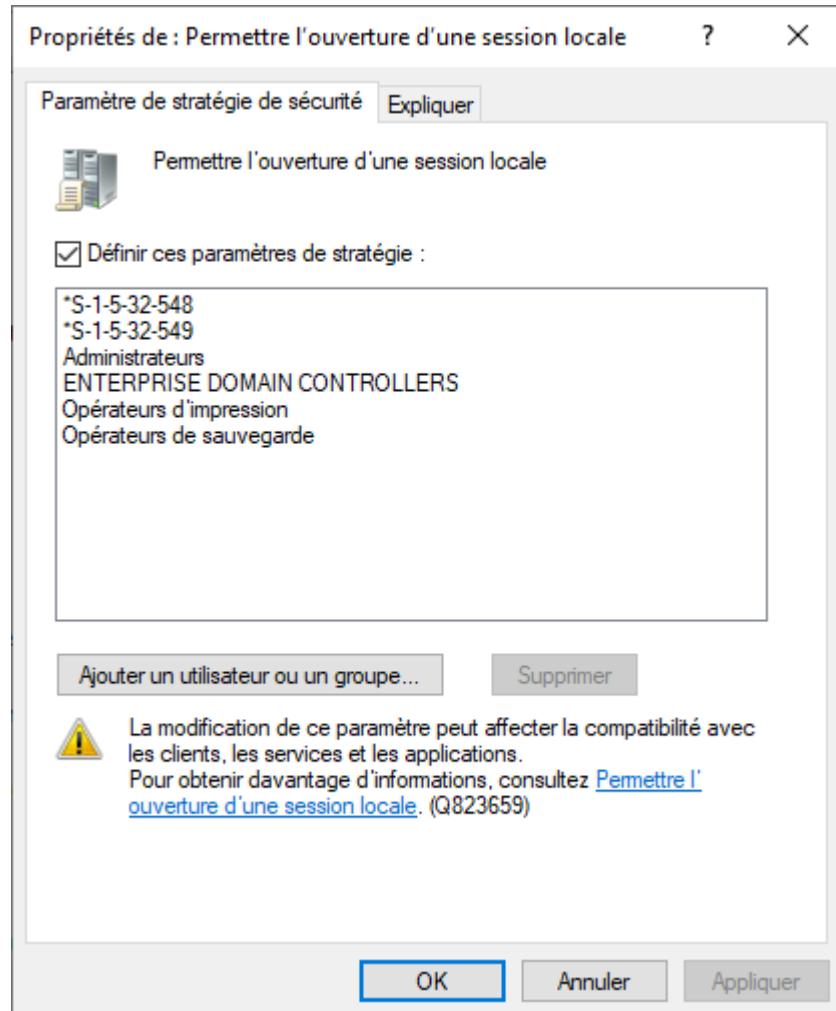
Configuration ordinateur (activée)	
Stratégies	masquer
Paramètres Windows	masquer
Paramètres de sécurité	masquer
Stratégies locales/ Attribution des droits utilisateur	masquer
Stratégie	Paramètre
Accéder à cet ordinateur à partir du réseau	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, Tout le monde
Ajouter des stations de travail au domaine	AUTORITE NT\Utilisateurs authentifiés
Ajuster les quotas de mémoire pour un processus	BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL
Arrêter le système	BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Augmenter la priorité de planification	Window Manager\Window Manager Group, BUILTIN\Administrateurs
Charger et décharger les pilotes de périphériques	BUILTIN\Opérateurs d'impression, BUILTIN\Administrateurs
Contourner la vérification de parcours	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL, Tout le monde
Créer un fichier d'échange	BUILTIN\Administrateurs
Déboguer les programmes	BUILTIN\Administrateurs
Forcer l'amét à partir d'un système distant	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs
Générer des audits de sécurité	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL
Gérer le journal d'audit et de sécurité	BUILTIN\Administrateurs
Modifier l'heure système	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs, AUTORITE NT\SERVICE LOCAL
Modifier les valeurs de l'environnement du microprogramme	BUILTIN\Administrateurs
Ouvrir une session en tant que tâche	BUILTIN\Utilisateurs du journal de performances, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Performance système du profil	NT SERVICE\WdiServiceHost, BUILTIN\Administrateurs
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	BUILTIN\Administrateurs
Permettre l'ouverture d'une session locale	AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de compte, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Prendre possession de fichiers ou d'autres objets	BUILTIN\Administrateurs
Processus unique du profil	BUILTIN\Administrateurs
Remplacer un jeton de niveau processus	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL
Restaurer les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs
Retirer l'ordinateur de la station d'accueil	BUILTIN\Administrateurs
Sauvegarder les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs

Les paramètres de la section "Attribution des droits utilisateur" servent à déterminer **qui peut faire quoi**.

Voici l'explication d'un paramètre important de cette GPO.

Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur

Permettre l'ouverture d'une session locale



Les utilisateurs du domaine ne peuvent pas se connecter sur le "Contrôleur de domaine".

C'est un paramètre important de l'Active Directory.

Stratégie de groupe locale avec Windows

Le service "Client de stratégie de groupe" (gpsvc) est responsable de l'application des paramètres configurés par les administrateurs pour les ordinateurs et pour les utilisateurs.

Les fichiers ADMX et ADML

- les fichiers ADMX sont dans le dossier c:\windows\PolicyDefinitions
les fichiers ADMX sont basés sur un format XML
- les fichiers ADML sont dans le dossier c:\windows\PolicyDefinitions\fr-FR
les fichiers ADML sont des fichiers spécifiques à la langue

On peut ajouter des fichiers ADMX et ADML supplémentaires.

Microsoft distribue des fichiers ADMX et ADML "**Microsoft Office**"

"Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise/Office LTSC 2021/Office 2019/Office 2016 and the Office Customization Tool for Office 2016"

- admintemplates_x64_5452-1000_en-us.exe
- office2016groupolicyandoctsettings.xlsx

Microsoft distribue des fichiers ADMX et ADML pour "**Edge Chromium**".

- MicrosoftEdgePolicyTemplates.zip

Microsoft distribue des fichiers ADMX et ADML pour "**PowerToys**".

- GroupPolicyObjectsFiles-0.82.1.zip

Google distribue des fichiers ADMX et ADML pour "**Chrome**".

- policy_templates.zip

Lien entre stratégie de groupe locale et le registre

La "Stratégie de groupe locale" permet de configurer des restrictions pour l'utilisation de Windows en spécifiant des paramètres à appliquer à l'ordinateur ou à l'utilisateur.

Lorsqu'on configure un paramètre de la stratégie de groupe locale on modifie une clé de registre.

Les clés du registre pour la "Configuration utilisateur":

- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

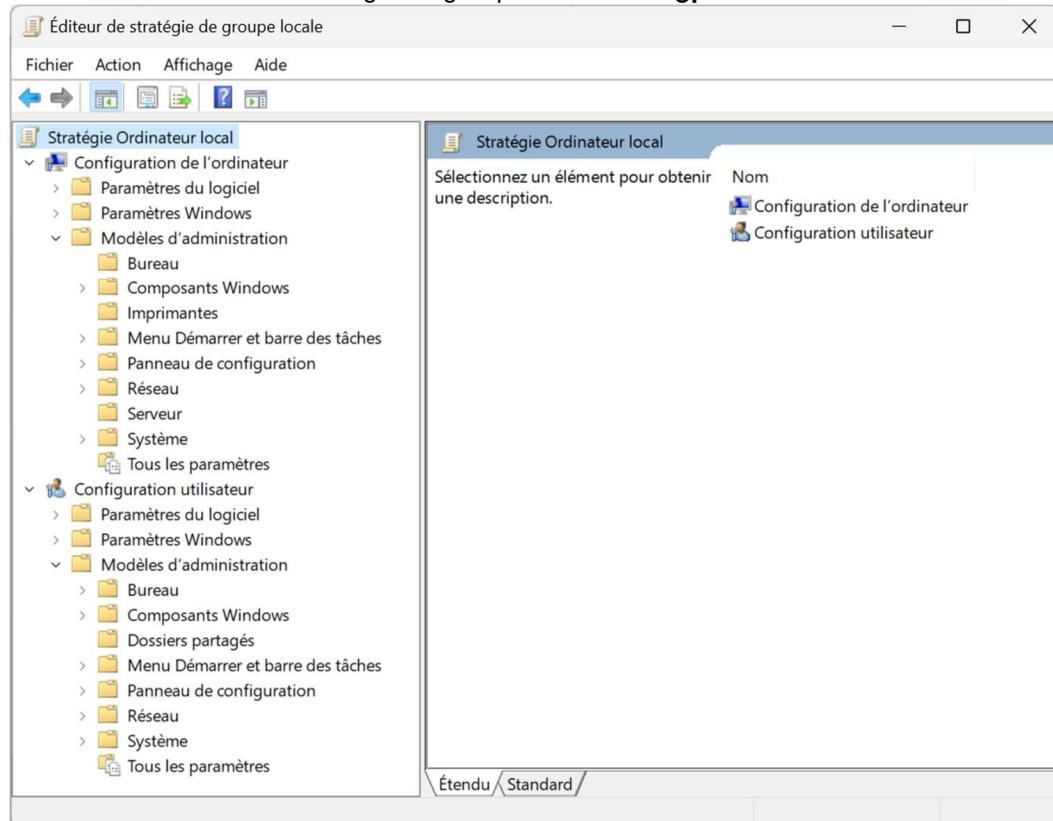
Les clés du registre pour la "Configuration ordinateur":

- HKEY_LOCAL_MACHINE\Software\Policies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

"Windows Serveur 2019" et "Windows 10" permettent de configurer environ 4500 stratégies.

Les paramètres qui sont dans les Stratégies ne peuvent pas être modifiés par l'utilisateur.

On démarre l'éditeur de stratégie de groupe locale avec **gpedit.msc**.



Configuration ordinateur / Stratégies / Modèles d'administration / **Tous les paramètres**
 Configuration utilisateur / Stratégies / Modèles d'administration / **Tous les paramètres**

GPEDIT.MSC et la "Configuration ordinateur"

- Lorsque l'on configure la partie "**Configuration ordinateur**", elle s'applique que si la GPO est liée à une OU contenant des ordinateurs.
- **Les paramètres de la stratégie de l'ordinateur sont appliqués lors du démarrage du poste et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

Les fichiers POL pour la configuration ordinateur

- %ALLUSERSPROFILE%\ntuser.pol
- %windir%\system32\GroupPolicy\Machine\Registry.pol

GPEDIT.MSC et la "Configuration utilisateur"

- Lorsque l'on configure la partie "**Configuration utilisateur**", elle s'applique que si la GPO est liée à une OU contenant des utilisateurs.
- **Les paramètres de la stratégie utilisateur sont appliqués à l'ouverture d'une session et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

Les fichiers POL de la configuration utilisateur

- %USERPROFILE%\ntuser.pol
 - %windir%\system32\GroupPolicy\User\Registry.pol
-

Les outils avec une interface graphique

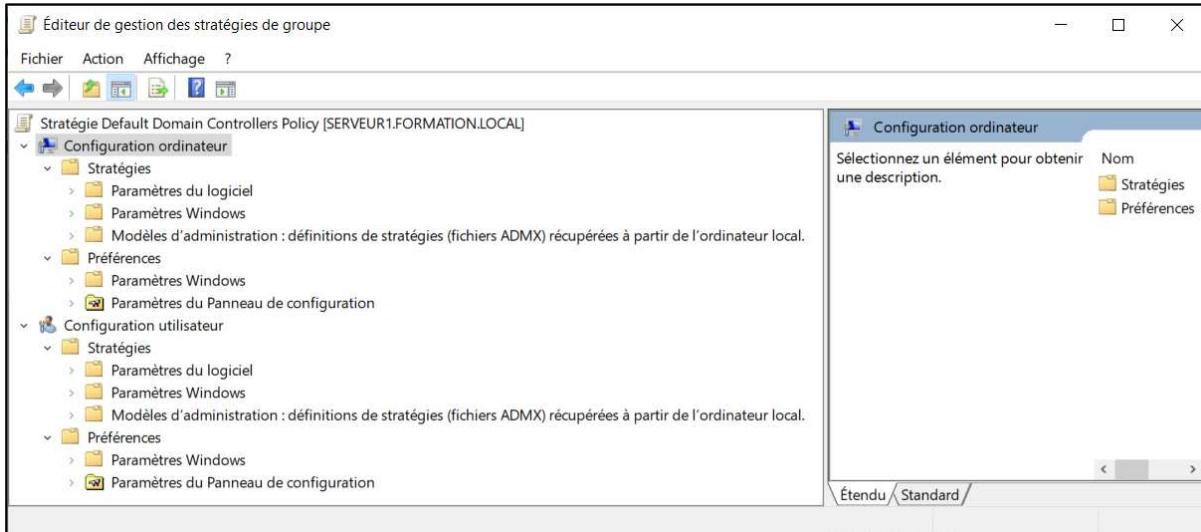
- **gpedit.msc** est l'éditeur de stratégie de groupe locale
- **rsop.msc**
 - Cet outil affiche le jeu de stratégies résultant (RSoP).
 - Cet outil ne permet pas de sauvegarder le résultat.
 - RSOP (Resultant Set of Policy)

Les programmes sans interface graphique

- **gpresult.exe**
 - Cet outil de ligne de commande affiche le jeu de stratégies résultant (RSoP).
 - Cet outil permet de sauvegarder le résultat de la commande dans un fichier HTML.
 - **gpupdate.exe**
 - Cet outil met à jour les paramètres de stratégie de groupe.
-

Les GPO dans un domaine

Les stratégies de groupe permettent une gestion centralisée des ordinateurs et des utilisateurs dans un environnement Active Directory.



Dans un domaine, un administrateur peut configurer des Stratégies et des Préférences.

Les paramètres qui sont dans les Préférence peuvent être modifiés par l'utilisateur.

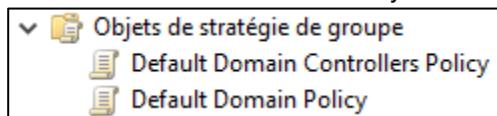
Une GPO peut être liée

- à une OU → on la voit sous la OU
- à plusieurs OU → on la voit sous chaque OU
- à aucune OU → on la voit seulement dans la section OSG (Objets de stratégie de groupe)

Les GPO sont emmagasinées dans SYSVOL.

Dans un domaine, il existe deux GPO par défaut:

- Default Domain Policy
- Default Domain Controllers Policy



Pour une question de performance, Microsoft limite à 999 le nombre de GPO qui peuvent être appliquées à un ordinateur ou à un utilisateur.

Documentation sur l'ordre d'exécution des GPO

L'ordre d'exécution des GPO respecte la formule LSDOU.

- | | |
|----|----------------------------|
| L | pour "Local" |
| S | pour "Site" |
| D | pour "Domain" |
| OU | pour "Organizational Unit" |

exemples

- Il est possible de gérer l'accès aux périphériques amovibles (USB, CD-RW, DVD-RW, ...) si on modifie un des nombreux paramètres dans

Configuration ordinateur / Stratégies /
Modèles d'administration / Système / Accès au stockage amovible

Exemples de paramètres intéressants

Disques amovibles: refuser l'accès en écriture

Disques amovibles: refuser l'accès en exécution

Disques amovibles: refuser l'accès en lecture

- Il est possible de modifier plusieurs paramètres pour gérer les stratégies de groupe.

Configuration ordinateur / Stratégies /
Modèles d'administration / Système / Stratégie de groupe

Exemples de paramètres intéressants

Définir l'intervalle d'actualisation de la stratégie de groupe pour les contrôleurs de domaine

Définir l'intervalle d'actualisation de la stratégie de groupe pour les ordinateurs

Désactiver le jeu de stratégie résultant

Désactiver le traitement des objets de stratégie de groupe locaux

Configuration utilisateur / Stratégies /
Modèles d'administration / Système / Stratégie de groupe

Exemples de paramètres intéressants

Définir l'intervalle d'actualisation de la stratégie de groupe pour les utilisateurs

Déterminer si les utilisateurs interactifs peuvent générer des données de jeu de stratégie résultant

Les bonnes pratiques pour la gestion des GPO

1) Ne modifiez pas les stratégies "Default Domain Policy" et "Default Domain Controller Policy".

2) Votre structure Active Directory doit faciliter l'application des stratégies.

La conception d'UO a une incidence sur le déploiement des stratégies de groupe.

Il est important de ne pas mélanger les utilisateurs et les ordinateurs dans une même UO.

Ne gardez pas les utilisateurs et les ordinateurs dans les conteneurs "**Users**" et "**Computers**".

3) Vous devez donner des noms significatifs à vos stratégies.

Les stratégies qui s'appliquent à des utilisateurs

U_nom_de_la_GPO

Les stratégies qui s'appliquent à des ordinateurs

C_nom_de_la_GPO

Les préférences qui s'appliquent à des utilisateurs

PU_nom_de_la_GPO

Les préférences qui s'appliquent à des ordinateurs

PC_nom_de_la_GPO

4) Il est recommandé d'ajouter des commentaires à vos stratégies.

5) Vous devez éviter de créer des stratégies au niveau du domaine.

Parce que les stratégies s'appliquent à tous les utilisateurs et à tous les ordinateurs du domaine.

6) Il est préférable de créer plusieurs petites stratégies qui ont des paramètres communs.

- mot de passe
- sécurité
- ...

7) Vous devez éviter de configurer le même paramètre dans des GPO différentes.

8) Pour augmenter la vitesse d'application des stratégies

Il faut désactiver les paramètres de configuration ordinateurs si la stratégie n'a aucun paramètre dans la section "**Configuration ordinateur**".

État GPO :	Paramètres de configuration ordinateurs désac
Commentaire :	Activé Paramètres de configuration ordinateurs désacti Paramètres de configuration utilisateurs désacti Tous les paramètres désactivés

Il faut désactiver les paramètres de configuration utilisateurs si la stratégie n'a aucun paramètre dans la section "**Configuration utilisateur**".

État GPO :	Paramètres de configuration utilisateurs désa
Commentaire :	Activé Paramètres de configuration ordinateurs désacti Paramètres de configuration utilisateurs désacti Tous les paramètres désactivés

La sauvegarde et la restauration des GPO

Ce laboratoire doit être fait individuellement sur le SEVEUR2

Objectif

- Apprendre à lire le contenu du fichier manifest.xml
- Sauvegarder et restaurer des GPO dans un domaine

Mise en place

Vous devez créer les dossiers E:_GPO_BACKUP et E:_GPO_BACKUP_PS.

Créer une sauvegarde des GPO en utilisant PowerShell

La commande pour sauvegarder la GPO "C_DisableRDP"

- Emplacement: le dossier E:_GPO_BACKUP_PS
note: le dossier utilisé pour les backups doit obligatoirement exister
- Description: "La GPO désactive le Bureau à distance"

```
Backup-GPO -Name "C_DisableRDP" `  
-Path E:\_GPO_BACKUP_PS `  
-Comment "La GPO désactive le Bureau à distance"
```

Créer une sauvegarde des GPO en utilisant la console

Vous devez créer une copie de sécurité de la GPO "C_Serveurs_Fichiers" dans le dossier E:_GPO_BACKUP.

- Dans le menu contextuel de la GPO "C_Serveurs_Fichiers"
 - Vous devez sélectionner l'option "Sauvegarder..."

Supprimer une GPO et la récupérer dans la sauvegarde en utilisant la console

Vous devez supprimer la GPO "C_Serveurs_Fichiers".

- Dans le menu contextuel de "Objets de stratégie de groupe"
 - Vous devez sélectionner l'option "Gérer les sauvegardes..."

Vous devez restaurer la GPO "C_Serveurs_Fichiers".

Vous devez lier la GPO "C_Serveurs_Fichiers" à l'unité d'organisation
"OU=FICHIERS,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL".

Informations sur la structure du fichier manifest.xml

Quand on effectue une sauvegarde de nos stratégies de groupe, à la racine de notre dossier un fichier "manifest.xml" est créé.

Ce fichier a la structure suivante:

- Backups
 - BackupInst
 - ❖ GPOGuid
 - ❖ GPODomain
 - ❖ GPODomainGuid
 - ❖ GPODomainController
 - ❖ BackupTime
 - ❖ ID
 - ❖ Comment
 - ❖ GPODisplayName

Pour exécuter le cmdlet Import-GPO, nous avons besoin du contenu de la balise "**GPODisplayName**" ou de la balise "**ID**".

Avant de commencer, vous devez sauvegarder les GPO suivantes dans le dossier "**E:_GPO_BACKUP\UTILISATEURS**".

- PU_EMPLOYES
- PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20
- U_EMPLOYES

Informations

La sauvegarde des GPO génère un fichier manifest.xml et des dossiers dont le nom ne correspond pas au nom des stratégies.

Par exemple, voici le contenu du dossier "E:_GPO_BACKUP\UTILISATEURS".



Le nom de chaque dossier correspond à la balise "**ID**" du fichier manifest.xml.

Attribut	Valeur
Domaine	FORMATION.LOCAL
Propriétaire	FORMATION\Admins du domaine
Créé le	2022-10-01 22:57:20
Modifié le	2022-10-07 08:26:18
Révisions utilisateur	5 (AD), 5 (SYSVOL)
Révisions ordinateur	0 (AD), 0 (SYSVOL)
ID unique	{798A7B12-C4C2-48CA-A7B4-D64BAD89FA08}
État GPO	Paramètres ordinateur désactivés

La valeur de "**ID unique**" correspond à la balise "**GPOGuid**" du fichier manifest.xml.

Attribut	Valeur
objectGUID	f40e856f-bd7d-457c-9ba5-7888d499dc72

La valeur de l'attribut "**objectGUID**" du domaine correspond à la balise "**GPODomainGuid**" du fichier manifest.xml.

Voici un script PowerShell qui va lire le contenu d'un fichier "manifest.xml" et afficher toutes les informations des stratégies qui sont dans le dossier de la sauvegarde.

```
# Le chemin complet du fichier MANIFEST.XML
$xmlPath = 'E:\_GPO_BACKUP\UTILISATEURS\manifest.xml'

$xml = [xml](Get-Content -Path $xmlPath -Encoding UTF8)
$xmlExpanded = $xml.DocumentElement.BackupInst

Write-Host $("-" * 80) -ForegroundColor Cyan

foreach ($item in $xmlExpanded)
{
    "GPOGuid" = $item.GPOGuid.InnerText
    "GPODomain" = $item.GPODomain.InnerText
    "GPODomainGuid" = $item.GPODomainGuid.InnerText
    "GPODomainController" = $item.GPODomainController.InnerText
    "BackupTime" = $item.BackupTime.InnerText
    "ID" = $item.ID.InnerText
    "Comment" = $item.Comment.InnerText
    "GPODisplayName" = $item.GPODisplayName.InnerText

    Write-Host $("-" * 80) -ForegroundColor Cyan
}
```

```
GPOGuid = {AD1087E6-426F-49B2-8045-1063C4F5069F}
GPODomain = FORMATION.LOCAL
GPODomainGuid = {F40e856f-bd7d-457c-9ba5-7888d499dc72}
GPODomainController = SERVEUR1.FORMATION.LOCAL
BackupTime = 2022-10-17T16:30:27
ID = {6E836373-3A7B-474C-9A86-9B3478968C8E}
Comment = Version 2
GPODisplayName = U_EMPLOYES

GPOGuid = {652AB980-1E74-4E67-A173-92BE27EA206B}
GPODomain = FORMATION.LOCAL
GPODomainGuid = {F40e856f-bd7d-457c-9ba5-7888d499dc72}
GPODomainController = SERVEUR1.FORMATION.LOCAL
BackupTime = 2022-10-02T03:48:51
ID = {1FB4D329-37A8-4BFB-8E89-79A747F74E2A}
Comment = PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20
GPODisplayName = PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20

GPOGuid = {D826A6C3-19A9-4645-9121-17EC495A09FE}
GPODomain = FORMATION.LOCAL
GPODomainGuid = {F40e856f-bd7d-457c-9ba5-7888d499dc72}
GPODomainController = SERVEUR1.FORMATION.LOCAL
BackupTime = 2022-10-02T03:48:36
ID = {547F8A49-670E-45D0-AE0B-AF7CB20F3690}
Comment = PU_EMPLOYES
GPODisplayName = PU_EMPLOYES
```

Restauration d'une GPO par programmation PowerShell

Il existe deux cmdlets pour importer des GPO: Import-GPO ou Restore-GPO.

Import-GPO

- Import-GPO permet de restaurer une GPO en utilisant un nom différent de l'original.
- La restauration d'une GPO peut se faire dans un domaine ou une forêt différente de la sauvegarde qui a été faite et n'a pas besoin d'exister.

Restore-GPO

- Restore-GPO permet de restaurer une ou plusieurs GPO dans un domaine à condition que les GPO proviennent du même domaine.
- Si le domaine original n'est pas disponible ou si la GPO n'existe plus dans le domaine alors le cmdlet génère une erreur.

Il est préférable d'utiliser Import-GPO.

Exemples en utilisant le nom de la GPO qui est dans la balise "**GPODisplayName**".

```
# Importation de la GPO si elle n'existe plus.  
# Dans ce cas, le paramètre -CreateIfNeeded est obligatoire.  
Import-GPO -BackupGpoName "U_EMPLOYES" `  
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `  
    -TargetName "U_EMPLOYES" `  
    -CreateIfNeeded  
  
# Importation de la GPO si elle existe.  
# Dans ce cas, le paramètre -CreateIfNeeded n'est pas obligatoire.  
Import-GPO -BackupGpoName "U_EMPLOYES" `  
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `  
    -TargetName "U_EMPLOYES"
```

Exemples en utilisant la valeur qui est dans la balise "**ID**".

```
# Importation de la GPO si elle n'existe plus.  
# Dans ce cas, le paramètre -CreateIfNeeded est obligatoire.  
Import-GPO -BackupId 6E836373-3A7B-474C-9A86-9B3478968C8E `  
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `  
    -TargetName "U_EMPLOYES" `  
    -CreateIfNeeded  
  
# Importation de la GPO si elle existe.  
# Dans ce cas, le paramètre -CreateIfNeeded n'est pas obligatoire.  
Import-GPO -BackupId 6E836373-3A7B-474C-9A86-9B3478968C8E `  
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `  
    -TargetName "U_EMPLOYES"
```

GPO avec PowerShell

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Utiliser plusieurs cmdlets relatifs aux stratégies de groupe.

Le lien entre une stratégie et la base de registre

La configuration d'un paramètre de stratégie de groupe modifie une clé de registre.

Les clés de registre pour la section "**Configuration utilisateur**"

- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Les clés de registre pour la section "**Configuration ordinateur**"

- HKEY_LOCAL_MACHINE\Software\Policies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

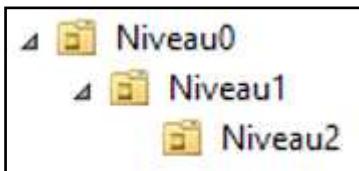
Le fichier "**Windows11andWindowsServer2019PolicySettings--23H2.xlsx**" contient les clés de registre qui sont sous "**Configuration ordinateur \ Stratégies \ Modèles d'administration**" et "**Configuration utilisateur \ Stratégies \ Modèles d'administration**".

Étape 1 - Mise en place

Connectez-vous sur votre serveur virtuel "SERVEURV2" avec l'utilisateur "FORMATION\TECH"

Créer des unités d'organisation

- Sous votre domaine créer la structure d'unités d'organisation suivante.



Pour la création des unités d'organisation, vous pouvez utiliser la console "Utilisateurs et ordinateurs Active Directory" ou la programmation PowerShell.

Vous devez créer le dossier E:_RAPPORTS.

L'annexe à la fin du document contient la liste complète des cmdlets du module GroupPolicy.

Étape 2 - Gestion des objets de stratégie de groupe (GPO)

Vous allez utiliser PowerShell pour gérer les objets de stratégie de groupe:

Création par la console "Gestion de stratégie de groupe"

Ouvrir la console "Gestion de stratégie de groupe"

Créer un objet

- Dans la section "Objets de stratégie de groupe" créer l'objet GPO "gpoA"

Créer un objet et le lier

- Dans la section "Objets de stratégie de groupe" créer l'objet GPO "gpoB"
- Dans l'unité Niveau2 lier l'objet GPO "gpoB"

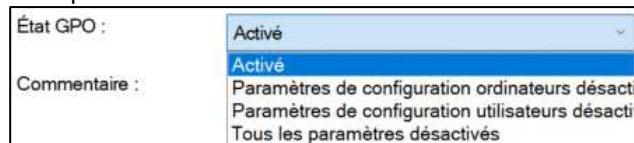
Créer deux objets et lier directement dans les unités

- Directement dans l'unité "Niveau0" créer l'objet GPO "gpoC"
 - Directement dans l'unité Niveau1 créer l'objet GPO "gpoD"
-

La commande pour créer un objet GPO dont le nom est "gpo1"

New-GPO -Name "gpo1"

Il est possible de modifier l'état d'une GPO en modifiant la propriété "GpoStatus".



```
(Get-GPO -Name "gpo1") .GpoStatus = "AllSettingsEnabled"  
(Get-GPO -Name "gpo1") .GpoStatus = "ComputerSettingsDisabled"  
(Get-GPO -Name "gpo1") .GpoStatus = "UserSettingsDisabled"  
(Get-GPO -Name "gpo1") .GpoStatus = "AllSettingsDisabled"
```

La commande pour afficher la valeur de "GpoStatus" de l'objet GPO "gpo1"

(Get-GPO -Name gpo1) .GpoStatus

La commande pour modifier le commentaire de l'objet GPO "gpo1"

(Get-GPO -Name "gpo1") .Description = "La GPO gpo1 n'est pas liée à une OU."

La commande pour afficher le commentaire de l'objet GPO "gpo1"

(Get-GPO -Name gpo1) .Description

La commande pour créer un objet GPO et configurer un commentaire.

New-GPO -Name "gpo2" `
-Comment "gpo2 est liée à la OU Niveau0"

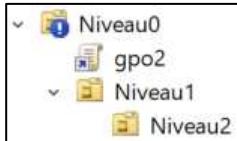
La commande pour lier l'objet GPO "gpo2" à l'unité d'organisation "Niveau0"

New-GPLink -Name "gpo2" `
-Target "ou=Niveau0,dc=formation,dc=local"

Étape 3 - Bloquer l'héritage sur une unité d'organisation

La commande pour bloquer l'héritage sur une OU

```
Set-GPInheritance -Target "ou=niveau0,dc=formation,dc=local" `  
-IsBlocked Yes
```



La commande pour ne pas bloquer l'héritage sur une OU

```
Set-GPInheritance -Target "ou=niveau0,dc=formation,dc=local" `  
-IsBlocked No
```

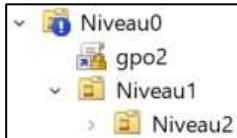
Étape 4 - "Appliqué" une GPO

IMPORTANT: Il ne faut pas confondre l'option "Appliqué" et "Lien activé".



En français	En anglais
Appliqué	Enforced
Lien activé	Link Enabled

```
Set-GPLink -Name gpo2 `  
-Target "ou=niveau0,dc=formation,dc=local" `  
-Enforced Yes
```



Le paramètre **-Enforced** existe également dans **New-GPLink**.

Étape 5 - Changer l'ordre d'application d'une GPO

La commande qui place une GPO en position 1 donc la plus haute priorité.

```
Set-GPLink -Name "gpo2" `  
-Target "OU=niveau0,DC=formation,DC=local" `  
-Order 1
```

Le paramètre **-Order** existe également dans **New-GPLink**.

Étape 6 - Suppression d'objets de stratégie de groupe (GPO) et de liaison

Supprimer le lien d'une GPO sur une unité d'organisation

La commande pour supprimer le lien "gpoB" qui est sur l'unité d'organisation "Niveau2" sans confirmation

```
Remove-GPLink -Name "gpoB"  
    -Target "ou=Niveau2,ou=Niveau1,ou=Niveau0,dc=formation,dc=local"  
    -Confirm:$false
```

Supprimer une GPO

La commande pour supprimer l'objet GPO "gpoB" sans confirmation

```
Remove-GPO -Name gpoB  
    -Confirm:$false
```

Étape 7a - Créer une GPO et configurer les paramètres avec les clés de registre

```
(Get-Command -Module GroupPolicy -Name *GPRegistryValue).Name
```

```
Get-GPRegistryValue  
Remove-GPRegistryValue  
Set-GPRegistryValue
```

Il est possible de désactiver le "Bureau à distance" à l'aide d'une clé de registre qui est une GPO.

La clé de registre est dans le fichier "Windows11andWindowsServer2019PolicySettings--23H2.xlsx".

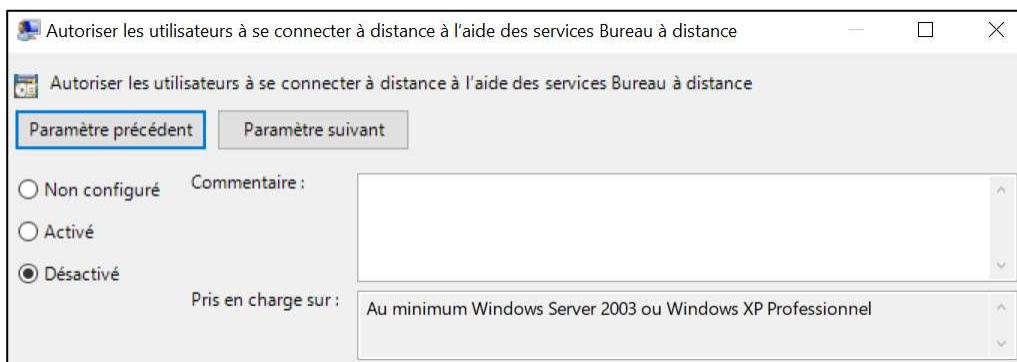
```
$pol = New-GPO -Name "C_DisableRDP" -Comment "Désactive RDP"  
$pol.GpoStatus = "UserSettingsDisabled"  
  
# Si la valeur est 0 alors l'accès au Bureau à distance est "Activé".  
# Si la valeur est 1 alors l'accès au Bureau à distance est "Désactivé".
```

Première syntaxe

```
Set-GPRegistryValue `  
    -Name "C_DisableRDP" `  
    -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" `  
    -ValueName "fDenyTSConnections" `  
    -Type DWord `  
    -Value 1
```

Deuxième syntaxe

```
# Utilisation d'une "hash table" pour passer les paramètres  
$HT1= @{  
    Name      = "C_DisableRDP"  
    Key       = "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"  
    ValueName = "fDenyTSConnections"  
    Type      = "DWord"  
    Value     = 1  
}  
  
Set-GPRegistryValue @HT1
```



Configuration ordinateur (activée)	
Stratégies	
Modèles d'administration	
Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.	
Composants Windows/ Services Bureau à distance/ Hôte de la session Bureau à distance/ Connexions	
Stratégie	Paramètre
Autoriser les utilisateurs à se connecter à distance à l'aide des services Bureau à distance	Désactivé
Configuration utilisateur (désactivée)	
Aucun paramètre n'est défini.	

Nous voulons que le paramètre de la GPO soit "Non configuré".

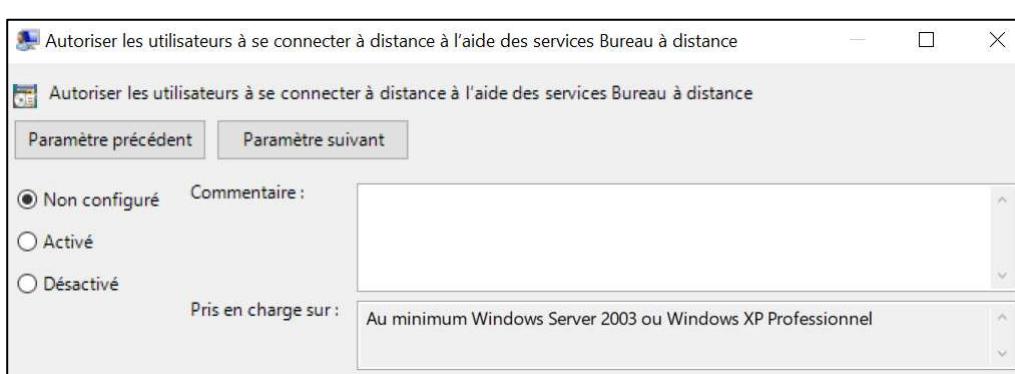
Première syntaxe

```
Set-GPRegistryValue ` 
    -Name "C_DisableRDP" ` 
    -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" ` 
    -Disable
```

Deuxième syntaxe

```
# Utilisation d'une "hash table" pour passer les paramètres
$HT2= @{
    Name      = "C_DisableRDP"
    Key       = "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"
    Disable   = $true
}

Set-GPRegistryValue @HT2
```



Configuration ordinateur (activée)	
Aucun paramètre n'est défini.	
Configuration utilisateur (désactivée)	
Aucun paramètre n'est défini.	

Étape 7b - Créer une préférence et configurer les paramètres avec les clés du registre

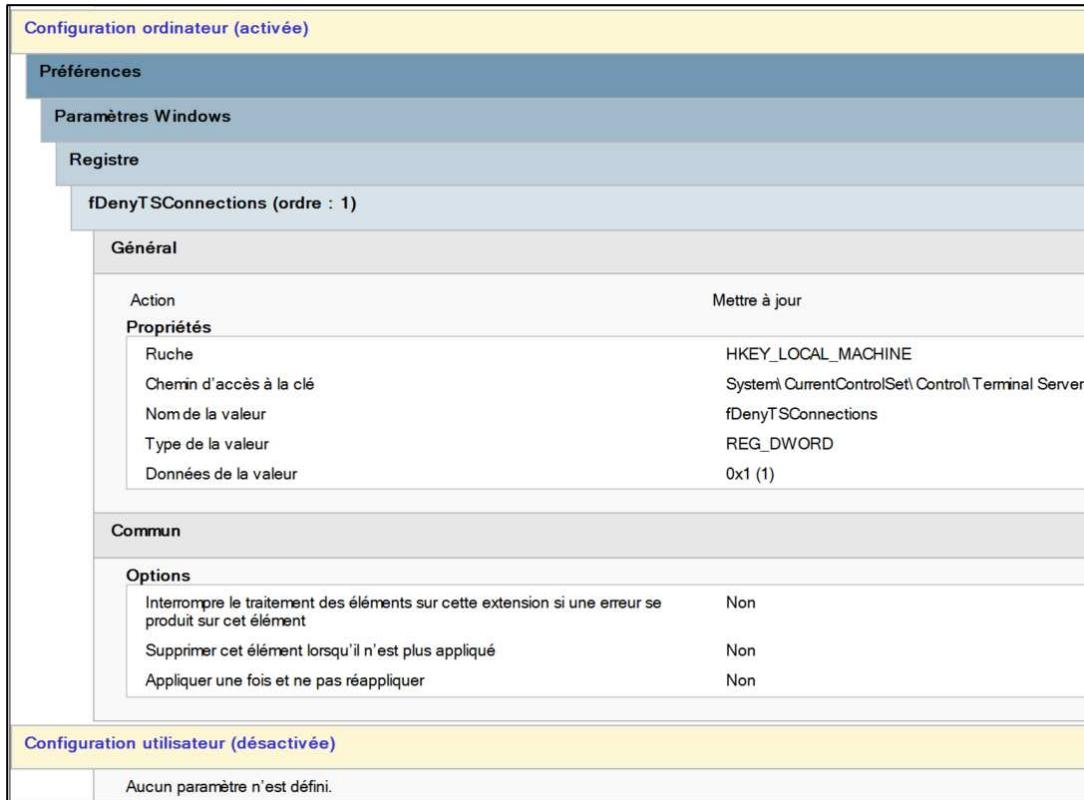
```
(Get-Command -Module GroupPolicy -Name *GPPrefRegistryValue).Name
```

```
Get-GPPrefRegistryValue  
Remove-GPPrefRegistryValue  
Set-GPPrefRegistryValue
```

Il est possible de désactiver le "Bureau à distance" à l'aide d'une clé de registre qui n'est pas une GPO.

Pour cet exemple, nous utiliserons une préférence pour modifier une clé de registre.

```
$pol = New-GPO -Name "PC_DisableRDP" -Comment "Désactive RDP"  
$Pol.GpoStatus = "UserSettingsDisabled"  
  
# Configuration d'une préférence "Ordinateur"  
Set-GPPrefRegistryValue `  
    -Name "PC_DisableRDP" `  
    -Key "HKLM\System\CurrentControlSet\Control\Terminal Server" `  
    -ValueName fDenyTSConnections `  
    -Type Dword `  
    -Value 1 `  
    -Context Computer `  
    -Action Update
```



Nous voulons supprimer la préférence "PC_DisableRDP".

```
Remove-GPPrefRegistryValue  
  -Name "PC_DisableRDP"  
  -Key "HKLM\System\CurrentControlSet\Control\Terminal Server"  
  -Context Computer
```

Configuration ordinateur (activée)	
	Aucun paramètre n'est défini.
Configuration utilisateur (désactivée)	
	Aucun paramètre n'est défini.

Étape 8 - Mise à jour des GPO

Invoke-GPUpdate est l'équivalent de "gpupdate.exe".

```
# Mise à jour des GPO pour les utilisateurs et les ordinateurs
# sur l'ordinateur local
Invoke-GPUpdate -Force

# Mise à jour des GPO pour les utilisateurs et les ordinateurs
# sur un ordinateur distant
Invoke-GPUpdate -Computer "SERVEUR2"
    -Force

# Mise à jour des GPO pour les utilisateurs
# sur un ordinateur distant
Invoke-GPUpdate -Computer "SERVEUR2"
    -Target "User"
    -Force
```

Étape 9 - Sauvegarder la résultante des stratégies

Get-GPResultantSetOfPolicy est l'équivalent de "gpresult.exe".

```
# Jeu de stratégie résultant sur l'ordinateur local
Get-GPResultantSetOfPolicy -ReportType Xml
    -Path "e:\_rapports\UserAndComputer.xml"

# Jeu de stratégie résultant sur un ordinateur distant
Get-GPResultantSetOfPolicy -ReportType Xml
    -Path "e:\_rapports\SERVEUR2_UserAndComputer.xml"
    -Computer "SERVEUR2"
```

Étape 10 - Création d'un rapport HTML par programmation PowerShell

La commande pour créer un rapport HTML pour l'objet "C_DisableRDP"

```
Get-GPOReport -Name "C_DisableRDP"
    -ReportType HTML
    -Path e:\_rapports\C_DisableRDP.html
```

ANNEXE

Voici la liste des CMDLETS du module GroupPolicy.

```
PS E:\_OUTILS> (Get-Command -Module GroupPolicy) .Name
Get-GPPermissions
Set-GPPermissions
Backup-GPO
Copy-GPO
Get-GPIinheritance
Get-GPO
Get-GPReport
Get-GPPermission
Get-GPPrefRegistryValue
Get-GPRegistryValue
Get-GPResultantSetOfPolicy
Get-GPStarterGPO
Import-GPO
Invoke-GPUpdate
New-GPLink
New-GPO
New-GPStarterGPO
Remove-GPLink
Remove-GPO
Remove-GPPrefRegistryValue
Remove-GPRegistryValue
Rename-GPO
Restore-GPO
Set-GPIinheritance
Set-GPLink
Set-GPPermission
Set-GPPrefRegistryValue
Set-GPRegistryValue
```

Voici deux cmdlets du ActiveDirectory.

```
Get-ADDefaultDomainPasswordPolicy
Set-ADDefaultDomainPasswordPolicy
```

Stratégie de mot de passe affinée

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- La configuration de "Stratégie de mot de passe affinée" avec la console "Centre d'administration Active Directory".

IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

Lorsqu'on configure des paramètres de sécurité au niveau du domaine c'est pour améliorer la sécurité.

Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos doivent être configurées au niveau du domaine.

Il est possible d'améliorer la sécurité en créant une stratégie de mot de passe affinée.

Stratégie de mot de passe affinée (Fine-Grained Password Policies)

Les stratégies de mot de passe affinées permettent de spécifier plusieurs stratégies de mot de passe au sein d'un même domaine et appliquer des restrictions différentes pour les stratégies de mot de passe et de verrouillage de compte à des ensembles d'utilisateurs différents dans un domaine.

La configuration des stratégies de mot de passe affinée est disponible seulement dans la console "Centre d'administration Active Directory".

Les stratégies de mot de passe affinées s'appliquent uniquement à des objets utilisateur et à des groupes de sécurité globaux. Par défaut, seuls les membres du groupe "**Admins du domaine**" peuvent définir des stratégies de mot de passe affinées.

Créer Paramètres de mot de passe : MOT_DE_PASSE_14

Paramètres de mot de passe

S'applique directement à

Nom	Courrier
grINF.Gestionnaires	

Options d'âge du mot de passe :

- Appliquer l'âge minimal de mot de passe
L'utilisateur ne peut pas changer le mot de passe d'ici à (jours) :
- Appliquer l'âge maximal de mot de passe
L'utilisateur doit changer le mot de passe après (jours) :
- Appliquer la stratégie de verrouillage des comptes :
 - Nombre de tentatives de connexion échouées autorisé :
 - Réinitialiser le nombre de tentatives de connexion échouées a...
 - Le compte va être verrouillé
 - Pendant une durée de (mins) :
 - Jusqu'à ce qu'un administrateur déverrouille manuellement le compte

Description :

Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE

Informations supplémentaires...

OK Annuler

FORMATION (local) > System > Password Settings Container

Centre d'administ... <

Vue d'ensemble

FORMATION (local)

..\\Password Settings Container

System

Contrôle d'accès dynamique

Authentification

Recherche globale

Filterer

Nom Priorité Description Type

MOT_DE_PASSE_14 1 Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE Paramètres de mot de passe

Dans la console UOAD.

Nom	Type	Description
MOT_DE_PASSE_14	msDS-PasswordSettings	Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE

La console "**Gestion des stratégies de groupe**" ne montre pas "**MOT_DE_PASSE_14**" parce que cette "**Stratégie de mot de passe affinée**" est dans le conteneur "**Password Settings Container**".

CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL

L'historique de Windows PowerShell affiche le code.

HISTORIQUE DE WINDOWS POWERSHELL

	Rechercher	Copier	Démarrer la tâche	Arrêter la tâche	Effacer tout
Applet de commande					
□	New-ADFineGrainedPasswordPolicy	<pre>-ComplexityEnabled:\$true -description:"Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE" -LockoutDuration:"00:30:00" -LockoutObservationWindow:"00:30:00" -LockoutThreshold:"3" -MaxPasswordAge:"42.00:00:00" -MinPasswordAge:"1.00:00:00" -MinPasswordLength:"7" -Name:"MOT_DE_PASSE_14" -PasswordHistoryCount:"24" -Precedence:"1" -ReversibleEncryptionEnabled:\$false -Server:"SERVEUR1.FORMATION.LOCAL"</pre>			
□	Set-ADObject	<pre>-Identity:"CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL" -ProtectedFromAccidentalDeletion:\$true -Server:"SERVEUR1.FORMATION.LOCAL"</pre>			
□	Add-ADFineGrainedPasswordPolicySubject	<pre>-Identity:"CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL" -Server:"SERVEUR1.FORMATION.LOCAL" -Subjects:"CN=grlNF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL"</pre>			

Trois commandes PowerShell sont utilisées pour la création d'une stratégie de mot de passe affinée.

Le conteneur "**Password Settings Container**" est visible dans la console UOAD.

```
# Définir le DistinguishedName pour le conteneur "Password Settings Container"
$nom = "CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL"

# Utiliser Get-ADObject pour afficher le contenu du conteneur
Get-ADObject -Filter *
    -SearchBase $nom | Format-List Name,DistinguishedName,ObjectClass
```

Name	:	MOT_DE_PASSE_14
DistinguishedName	:	DN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
ObjectClass	:	msDS-PasswordSettings

Le contenu de l'attribut **ObjectClass** est **msDS-PasswordSettings**

```
# Définir le DistinguishedName pour le conteneur "Password Settings Container"  
$nom = "CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL"  
  
# Utiliser Get-ADObject pour afficher le contenu du conteneur  
Get-ADObject -Filter *  
    -SearchBase $nom  
    -Properties * | Format-List Name,  
        DistinguishedName,  
        ObjectClass,  
        msDS-LockoutDuration,  
        msDS-LockoutObservationWindow,  
        msDS-LockoutThreshold,  
        msDS-MaximumPasswordAge,  
        msDS-MinimumPasswordAge,  
        msDS-MinimumPasswordLength,  
        msDS-PasswordComplexityEnabled,  
        msDS-PasswordHistoryLength,  
        msDS-PasswordReversibleEncryptionEnabled,  
        msDS-PasswordSettingsPrecedence,  
        msDS-PSOAppliesTo
```

Name	:	MOT_DE_PASSE_14
DistinguishedName	:	CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
ObjectClass	:	msDS-PasswordSettings
msDS-LockoutDuration	:	-18000000000
msDS-LockoutObservationWindow	:	-18000000000
msDS-LockoutThreshold	:	3
msDS-MaximumPasswordAge	:	-362880000000000
msDS-MinimumPasswordAge	:	-864000000000
msDS-MinimumPasswordLength	:	7
msDS-PasswordComplexityEnabled	:	True
msDS-PasswordHistoryLength	:	24
msDS-PasswordReversibleEncryptionEnabled	:	False
msDS-PasswordSettingsPrecedence	:	1
msDS-PSOAppliesTo	:	{CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL}

msDS-LockoutDuration, msDS-LockoutObservationWindow, msDS-MaximumPasswordAge et msDS-MinimumPasswordAge ont des valeurs négatives.

Par exemple, la valeur **-18000000000** pour la propriété **msDS-LockoutDuration** est déroutante.
Cette valeur est exprimée en unités de 100 nanosecondes (ou 0.0000001 secondes).
Active Directory utilise ce format pour représenter les durées de temps.

La fonction **Convert-ADTime** convertit les valeurs de 100 nanosecondes en minutes.
La formule de conversion est basée sur le fait qu'une minute contient 600,000,000 unités de 100 nanosecondes.

```
function Convert-ADTime  
{  
    param ([long]$time)  
  
    return ($time / -600000000)  
}
```

```
# Définir le DN pour le conteneur "Password Settings Container"
$nom = "CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL"

# Utiliser Get-ADObject pour afficher le contenu du conteneur
Get-ADObject -Filter * `
    -SearchBase $nom `
    -Properties * | Format-List Name,
                    DistinguishedName,
                    ObjectClass,
                    @{Name="LockoutDuration (minutes)" ;
                     Expression={Convert-ADTime $PSItem."msDS-LockoutDuration"}},
                    @{Name="LockoutObservationWindow (minutes)" ;
                     Expression={Convert-ADTime $PSItem."msDS-LockoutObservationWindow"}},
                    msDS-LockoutThreshold,
                    @{Name="MaxPasswordAge (minutes)" ;
                     Expression={Convert-ADTime $PSItem."msDS-MaximumPasswordAge"}},
                    @{Name="MinPasswordAge (minutes)" ;
                     Expression={Convert-ADTime $PSItem."msDS-MinimumPasswordAge"}},
                    msDS-MinimumPasswordLength,
                    msDS-PasswordComplexityEnabled,
                    msDS-PasswordHistoryLength,
                    msDS-PasswordReversibleEncryptionEnabled,
                    msDS-PasswordSettingsPrecedence,
                    msDS-PSOAppliesTo
```

Name	:	MOT_DE_PASSE_14
DistinguishedName	:	: CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
ObjectClass	:	: msDS-PasswordSettings
LockoutDuration (minutes)	:	: 30
LockoutObservationWindow (minutes)	:	: 30
msDS-LockoutThreshold	:	: 3
MaxPasswordAge (minutes)	:	: 60480
MinPasswordAge (minutes)	:	: 1440
msDS-MinimumPasswordLength	:	: 7
msDS-PasswordComplexityEnabled	:	: True
msDS-PasswordHistoryLength	:	: 24
msDS-PasswordReversibleEncryptionEnabled	:	: False
msDS-PasswordSettingsPrecedence	:	: 1
msDS-PSOAppliesTo	:	: {CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL}

Les commandes PowerShell pour les stratégies de mot de passe affinée

```
(Get-Command -Name *FineGrainedPasswordPolicy*).Name
```

```
Add-ADFineGrainedPasswordPolicySubject  
Get-ADFineGrainedPasswordPolicy  
Get-ADFineGrainedPasswordPolicySubject  
New-ADFineGrainedPasswordPolicy  
Remove-ADFineGrainedPasswordPolicy  
Remove-ADFineGrainedPasswordPolicySubject  
Set-ADFineGrainedPasswordPolicy
```

Voici la commande pour afficher un jeu de stratégies résultant pour un utilisateur qui utilise une stratégie de mot de passe affinée.

```
Get-ADUserResultantPasswordPolicy -Identity EMP09
```

```
PS E:\PowerShell> Get-ADUserResultantPasswordPolicy -Identity EMP09

AppliesTo : {CN=grrRH_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL,
CN=grING_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL,
CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL,
CN=grCOMP_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL}

ComplexityEnabled : True
DistinguishedName : CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
LockoutDuration : 00:30:00
LockoutObservationWindow : 00:30:00
LockoutThreshold : 3
MaxPasswordAge : 30.00:00:00
MinPasswordAge : 1.00:00:00
MinPasswordLength : 14
Name : MOT_DE_PASSE_14
ObjectClass : msDS>PasswordSettings
ObjectGUID : e3e5c5a1-9c17-4a8f-8004-d93aa5a348bc
PasswordHistoryCount : 24
Precedence : 1
ReversibleEncryptionEnabled : False
```

Si **Get-ADUserResultantPasswordPolicy** retourne rien, c'est parce que l'utilisateur n'utilise pas de stratégie de mot de passe affinée.

```
PS E:\PowerShell> Get-ADUserResultantPasswordPolicy -Identity EMP08
```

```
PS E:\PowerShell>
```

Une stratégie de mot de passe affinée permet de configurer l'historique des mots de passe entre 1 et 1024

```
Set-ADFineGrainedPasswordPolicy -Identity MOT_DE_PASSE_14  
-PasswordHistoryCount:"60"
```

Les commandes pour supprimer une stratégie de mot de passe affinée

```
Set-ADFineGrainedPasswordPolicy -Identity MOT_DE_PASSE_14  
-ProtectedFromAccidentalDeletion $False
```

```
Remove-ADFineGrainedPasswordPolicy -Identity MOT_DE_PASSE_14  
-Confirm
```

DFS Mise en place

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

Objectifs

- Révision de PowerShell pour
 - la création des dossiers et l'attribution des autorisations NTFS
 - la création des partages et l'attribution des autorisations de partage
- Création d'une structure de dossiers sur plusieurs serveurs
- Installation des services de rôle pour les DFS

Documentation sur les DFS

Les espaces de noms DFS et la réPLICATION DFS dans "Windows Server" sont des services de rôle au sein du rôle "Services de fichiers et de stockage".

Espaces de noms DFS

Ils permettent de grouper des dossiers partagés qui se trouvent sur des serveurs différents en un ou plusieurs espaces de noms logiquement structurés. Pour les utilisateurs, chaque espace de noms apparaît sous la forme d'un dossier partagé unique avec une série de sous-dossiers.

RéPLICATION DFS

Elle permet de répliquer des dossiers de manière efficace (y compris les dossiers désignés par un chemin d'accès à un espace de noms DFS) sur une multitude de serveurs et de sites. La réPLICATION DFS utilise un algorithme de compression appelé "compression différentielle à distance" (RDC). L'algorithme RDC détecte les changements de données dans un fichier et permet à la réPLICATION DFS de répliquer uniquement les blocs de fichiers modifiés à la place du fichier entier.

L'accès à un dossier partagé se fait avec \\NomDuServeur\NomPartage

L'accès à une DFS se fait avec \\NomDuDomaine\NomDFS

Étape 1 - Identification des serveurs

Pour ce laboratoire nous utiliserons vos deux ordinateurs pour simuler un "datacenter" comportant plusieurs serveurs de fichiers.

Nom du serveur	Informations supplémentaires
SERVEUR1	Le contrôleur de domaine
SERVEUR2	Le serveur membre du domaine

Étape 2 - Les utilisateurs

Nous utiliserons les 2 utilisateurs EMP09 et EMP10 qui sont membres du groupe grINF_Gestionnaires.

Étape 3a - Les dossiers et les autorisations NTFS

La création de tous les dossiers et les attributions des autorisations NTFS se fera dans un seul script à partir du serveur SERVEUR2.

Pour attribuer les autorisations NTFS, vous devez utiliser la commande "icacls.exe".

Liste des autorisations communes

Sauf avis contraire, les autorisations sur les dossiers utilisent l'héritage standard (OI)(CI).

Pour chaque dossier qui débute par E:_C53

- Désactiver l'héritage et choisir l'option "Supprimer toutes les autorisations héritées de cet objet".
- Ajouter les autorisations
 - "Administrateurs" "Contrôle total" "Ce dossier, les sous-dossiers et les fichiers"
 - "Système" "Contrôle total" "Ce dossier, les sous-dossiers et les fichiers"
 - TECH "Contrôle total" "Ce dossier, les sous-dossiers et les fichiers"

Liste des autres autorisations particulières:

Nom du serveur	Dossiers	Ajouter les autorisations suivantes
SERVEUR1	E:_C53_Clients	grINF_Gestionnaires "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR1	E:_C53_Inventaire	grINF_Gestionnaires "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR1	E:_C53_Publicite	grINF_Gestionnaires "Lecture et exécution" "Ce dossier seulement"
SERVEUR1	E:_C53_Publicite\EMP09	Le dossier EMP09 hérite des autorisations de son parent. EMP09 "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR1	E:_C53_Publicite\EMP10	Le dossier EMP10 hérite des autorisations de son parent. EMP10 "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR2	E:_C53_Commande	grINF_Gestionnaires "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR2	E:_C53_Inventaire	grINF_Gestionnaires "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR2	E:_C53_Production	grINF_Gestionnaires "Lecture et exécution" "Ce dossier, les sous-dossiers et les fichiers" EMP10 "Modification" "Ce dossier, les sous-dossiers et les fichiers"
SERVEUR2	E:_C53_Web	grINF_Gestionnaires "Modification" "Ce dossier, les sous-dossiers et les fichiers"

Étape 3b - Les partages sur les dossiers et les autorisations de partage

La création de tous les partages se fera dans un seul script à partir du serveur SERVEUR2.

Pour chaque partage, les autorisations de partage seront "Tout le monde", "Contrôle total".

Pour chaque partage, vous devez désactiver la mise en cache du partage.

Pour chaque partage, vous devez activer l'énumération basée sur l'accès

Nom du serveur	Dossiers	Partages
SERVEUR1	E:_C53_Clients	C53_Cli
	E:_C53_Inventaire	C53_InvB
	E:_C53_Publicite	C53_Pub
	E:_C53_Publicite\EMP09	aucun partage sur ce dossier
	E:_C53_Publicite\EMP10	aucun partage sur ce dossier
SERVEUR2	E:_C53_Commande	C53_Cmd
	E:_C53_Inventaire	C53_InvA
	E:_C53_Production	C53_Prod
	E:_C53_Web	C53_Web

Vérification des partages

Pour vérifier la liste de vos partages, vous pouvez utiliser les commandes

- `Get-SmbShare -CimSession SERVEUR1`
- `Get-SmbShare -CimSession SERVEUR2`

Pour vérifier la liste de vos partages, vous pouvez utiliser

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

Étape 4 - Exemples pour la programmation des dossiers et des partages

L'objectif est d'écrire un script PowerShell qui permet de créer des dossiers et des partages sur votre serveur et sur des serveurs à distance. Le script PowerShell doit s'exécuter à partir du SERVEUR2.

Je vous conseille d'inclure des instructions de "suppression" des partages et des dossiers, avant les énoncés de création afin d'éviter les problèmes si vous devez exécuter votre script à plusieurs reprises.

IMPORTANT: vous devez supprimer les partages avant de supprimer les dossiers

```
#-----
# Le serveur SERVEUR1 est le contrôleur de domaine
#-----
# Supprime les anciens partages sur le SERVEUR1
Get-SmbShare -Name C53_* -CimSession $ordi | ` 
    Remove-SmbShare -Force -ErrorAction SilentlyContinue

# Supprime les anciens dossiers sur le SERVEUR1
$chemin = "\SERVEUR1\C$\_C53_"
Remove-Item -Path $chemin*" -Recurse -Force -ErrorAction SilentlyContinue
```

New-Item permet de créer des fichiers et des dossiers.

Pour créer un dossier sur un ordinateur distant, vous devez utiliser l'accès au partage administratif C\$ de l'ordinateur distant.

Commandes pour créer le dossier E:_C53_TEST sur le SERVEUR1 à partir de l'ordinateur SERVEUR2
\$dossierTEST = "\SERVEUR1\c\$_C53_TEST"

New-Item -ItemType Directory -Path \$dossierTEST

Commande pour "Désactiver l'héritage" et "Supprimer toutes les autorisations héritées de cet objet"
icacls.exe \$dossierTEST /inheritance:r

Commandes pour ajouter des autorisations NTFS

```
icacls.exe $dossierTEST /grant "administrateurs:(CI)(OI)(F)"
icacls.exe $dossierTEST /grant "system:(CI)(OI)(F)"
icacls.exe $dossierTEST /grant "FORMATION\TECH:(CI)(OI)(F)"
icacls.exe $dossierTEST /grant "grINF_Gestionnaires:(CI)(OI)(M)"
```

New-SMBShare permet de créer un partage sur un dossier.

Pour créer un partage sur un dossier qui est sur un ordinateur distant, vous devez utiliser le chemin local et utiliser le paramètre -CimSession pour spécifier le nom de l'ordinateur distant.

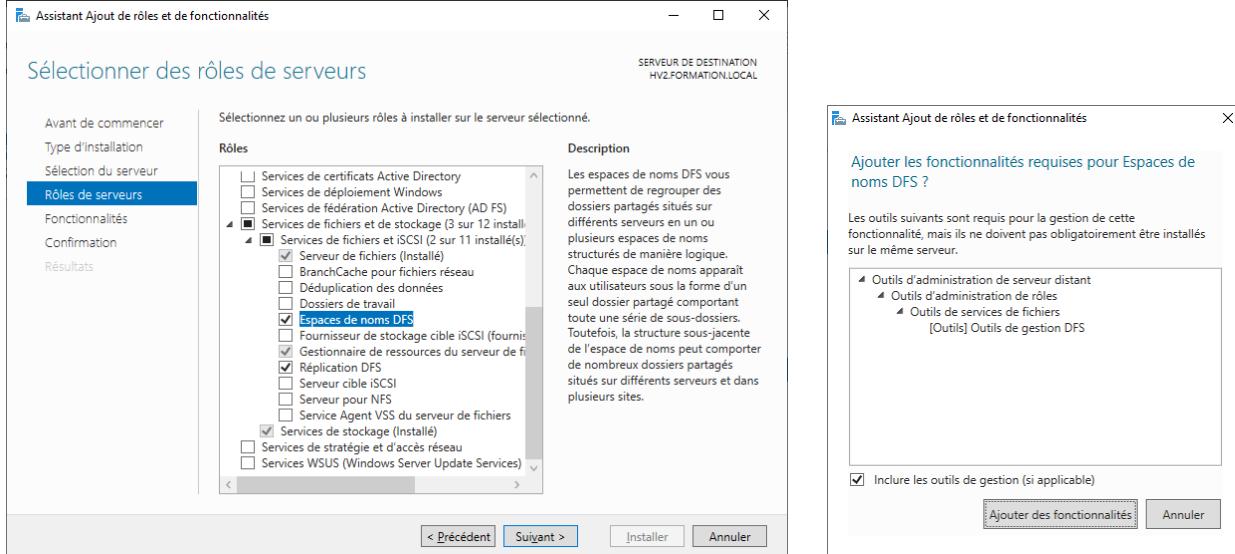
Pour créer le partage C53_TEST sur le dossier E:_C53_TEST qui est sur l'ordinateur SERVEUR1 à partir de l'ordinateur SERVEUR2

```
New-SMBShare -Name C53_TEST ` 
    -Path E:\_C53_TEST ` 
    -FullAccess "Tout le monde" ` 
    -CachingMode none ` 
    -FolderEnumerationMode AccessBased ` 
    -CimSession SERVEUR1
```

Étape 5 - Installation du rôle DFS

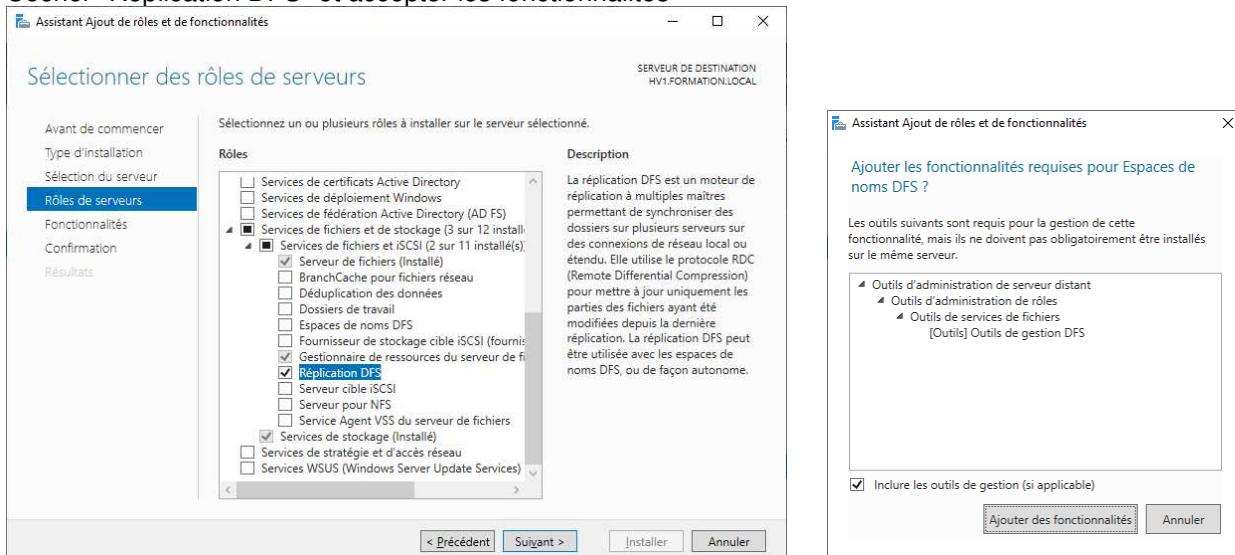
Dans le gestionnaire du serveur SERVEUR2

- Sélectionner le rôle "Services de fichiers et de stockage"
- Sélectionner "Services de fichiers et iSCSI"
- Cocher "Espaces de noms DFS" et accepter les fonctionnalités
- Cocher "RéPLICATION DFS"



Dans le gestionnaire du serveur SERVEUR1

- Sélectionner le rôle "Services de fichiers et de stockage"
- Sélectionner "Services de fichiers et iSCSI"
- Cocher "RéPLICATION DFS" et accepter les fonctionnalités



Le rôle de réPLICATION DFS est obligatoire sur un serveur qui héberge une copie des espaces de noms DFS.

ANNEXE

Installation du rôle DFS par programmation PowerShell

Get-WindowsFeature permet d'afficher l'état des rôles et des fonctionnalités.

Display Name	Name	Install State
[X] Services de fichiers et de stockage	FileAndStorage-Services	Installed
[X] Services de fichiers et iSCSI	File-Services	Installed
[X] Serveur de fichiers	FS-FileServer	Installed
[] BranchCache pour fichiers réseau	FS-BranchCache	Available
[] Déduplication des données	FS-Data-Deduplication	Available
[] Dossiers de travail	FS-SyncShareService	Available
[] Espaces de noms DFS	FS-DFS-Namespace	Available
[] Fournisseur de stockage cible iSCSI (fou...	iSCSITarget-VSS-VDS	Available
[X] Gestionnaire de ressources du serveur de...	FS-Resource-Manager	Installed
[] Réplication DFS	FS-DFS-Replication	Available
[] Serveur cible iSCSI	FS-iSCSITarget-Server	Available
[] Serveur pour NFS	FS-NFS-Service	Available
[] Service Agent VSS du serveur de fichiers	FS-VSS-Agent	Available
[X] Services de stockage	Storage-Services	Installed
[X] outils de services de fichiers	RSAT-File-Services	Installed
[] Outils de gestion DFS	RSAT-DFS-Mgmt-Con	Available
[X] Outils du Gestionnaire de ressources...	RSAT-FSRM-Mgmt	Installed
[] Services des outils de gestion du sy...	RSAT-NFS-Admin	Available

Pour afficher les rôles et fonctionnalités qui sont installés

```
Get-WindowsFeature | Where-Object InstallState -eq "Installed"
```

FS-DFS-Namespace	correspond à "Espaces de noms DFS"
FS-DFS-Replication	correspond à "Réplication DFS"
RSAT-DFS-Mgmt-Con	correspond à "Outils de gestion DFS"

```
Get-WindowsFeature -Name FS-DFS-Namespace,FS-DFS-Replication,RSAT-DFS-Mgmt-Con
```

Display Name	Name	Install State
[] Espaces de noms DFS	FS-DFS-Namespace	Available
[] Réplication DFS	FS-DFS-Replication	Available
[] outils de gestion DFS	RSAT-DFS-Mgmt-Con	Available

Install-WindowsFeature permet d'installer des rôles et des fonctionnalités.

Sur le serveur SERVEUR2

```
Install-WindowsFeature -Name FS-DFS-Namespace -Verbose
Install-WindowsFeature -Name FS-DFS-Replication -Verbose
Install-WindowsFeature -Name RSAT-DFS-Mgmt-Con -Verbose
```

Sur le serveur SERVEUR1

```
Install-WindowsFeature -Name FS-DFS-Replication -Verbose
Install-WindowsFeature -Name RSAT-DFS-Mgmt-Con -Verbose
```

L'ÉVALUATION EST SUR 70
25% de la note finale

Partie 1 (10 points)

Le fichier **P1_matricule.docx** est sur LÉA.

2 points pour la remise du fichier et le respect du nom du fichier.

2 points pour la création d'une unité d'organisation sous
"ETUmatricule.LOCAL/INFORMATIQUE"

6 points pour la création des 3 unités d'organisation sous
"ETUmatricule.LOCAL/INFORMATIQUE/UTILISATEURS"

Partie 2 (6 points)

Le fichier **P2_matricule.docx** est sur LÉA.

2 points pour la remise du fichier et le respect du nom du fichier.

4 points pour la création des 2 groupes dans l'unité d'organisation
"ETUmatricule.LOCAL/INFORMATIQUE/GROUPES "

Partie 3 (22 points)

Le fichier **P3_matricule.ps1** est sur LÉA.

2 points pour la remise du fichier et le respect du nom du fichier.

2 points pour lire le fichier CSV

10 points pour créer les utilisateurs avec les bons paramètres

4 points pour placer les utilisateurs dans les bons groupes

4 points pour placer les utilisateurs dans les bonnes unités d'organisation

Partie 4 (10 points)

Le fichier **P4_matricule.ps1** est sur LÉA.

2 points pour la remise du fichier et le respect du nom du fichier.

2 points pour créer le dossier personnel des utilisateurs

2 points pour les autorisations NTFS sur le dossier personnel des utilisateurs

4 points pour modifier les deux propriétés des utilisateurs

Partie 5 (22 points)

Le fichier **P5_UTILISATEURS_matricule.htm** est sur LÉA.
2 points pour la remise du fichier et le respect du nom du fichier.

1 point si la GPO est liée à l'unité d'organisation "**ETUmatricule.LOCAL/INFORMATIQUE/Utilisateurs**"

1 point si la section ORDINATEUR est désactivé.

7 points - 1 point par paramètre **correctement** configuré

Le fichier **P5_ORDINATEURS_matricule.htm** est sur LÉA.
2 points pour la remise du fichier et le respect du nom du fichier.

1 point si la GPO est liée à l'unité d'organisation "**ETUmatricule.LOCAL/INFORMATIQUE/SERVEURS**"

1 point si la section UTILISATEUR est désactivé.

7 points - 1 point par paramètre **correctement** configuré

PROJET FINAL C53

Département INFORMATIQUE



Automne 2024

Cahier de charge

420-C53 Implantation d'un réseau corporatif sous Active Directory

Table des matières

INTRODUCTION.....	3
Objectif général du projet	3
Objectifs particuliers du projet.....	3
FONCTIONNEMENT GÉNÉRAL	4
Étape préliminaire	4
Rédaction du code PowerShell.....	5
LA CORPORATION.....	6
INFRASTRUCTURE DU DOMAINE.....	6
Le domaine.....	6
INFRASTRUCTURE DU RESEAU	7
Le plan d'adressage	7
Description des serveurs	8
Les serveurs de fichiers	8
LE SERVEUR RÉEL	9
Création des ordinateurs virtuels	9
Configuration des ordinateurs virtuels.....	9
LE SERVEUR DNS.....	9
STRATÉGIES DE GROUPE - DOMAINE.....	10
LE DÉPARTEMENT "INFORMATIQUE".....	11
LES UNITÉS D'ORGANISATION.....	12
LES UTILISATEURS	13
Généralités sur les utilisateurs	13
LES GROUPES	14
Généralités sur les groupes.....	14
Ajouter les utilisateurs aux groupes.....	14

LES SERVEURS DE FICHIERS	15
Les dossiers personnels.....	15
Les dossiers du département	16
Autorisations sur les dossiers du département.....	17
Un espace de noms.....	18
LES QUOTAS DE DOSSIERS.....	18
Description des quotas	18
Les rapports de quotas	18
STRATÉGIES DE GROUPE	19
Stratégie pour les postes clients du département.....	19
Stratégie pour les utilisateurs du département	20
ANNEXE - ÉVALUATIONS.....	21
<i>Évaluation de la deuxième étape.....</i>	21

INTRODUCTION

Objectif général du projet

Ce projet constitue la partie pratique de l'épreuve certificative du cours 420-C53.

Ce projet vérifie les compétences en lien avec l'Active Directory. Il vérifie aussi la capacité de réaliser des tâches par la programmation de scripts PowerShell.

L'objectif général poursuivi est de mettre en production une structure physique et logique d'un réseau corporatif.

Le projet est le résultat d'un travail individuel.

Les dernières semaines de cours sont réservées à la préparation de ce projet.

Objectifs particuliers du projet

Il s'agit d'installer une gestion des ressources d'un réseau corporatif sous Active Directory. Vous serez responsable d'un département.

Voici les principaux objectifs techniques du projet.

Vous devez configurer un serveur en tant que contrôleur de domaine.

Vous devez créer une structure d'unités d'organisation qui contiendra tous les objets de votre département.

Vous devez créer plusieurs utilisateurs dans votre département, ayant chacun des propriétés particulières.

Mettre en place plusieurs rôles et fonctionnalités de l'Active Directory.

- Créer tous les objets de l'Active Directory par programmation PowerShell
- Planifier et créer des stratégies de groupes
- Planifier et implanter les autorisations NTFS et de partage afin d'offrir un environnement sécurisé
- Implanter une structure de dossiers pour les dossiers personnels
- Implanter des DFS
- Implanter des quotas

FONCTIONNEMENT GÉNÉRAL

Le projet s'étale sur environ plusieurs semaines à partir de la semaine du **11 novembre**.

L'examen pratique final est divisé en deux grandes étapes.

La première étape **du 11 novembre au 12 décembre** consiste à mettre en place la configuration décrite dans ce document.

La deuxième étape sera le **13 décembre**, il s'agira pour vous d'apporter des modifications que le professeur vous demandera d'effectuer.

Étape préliminaire

Les semaines précédant la deuxième étape du projet sont dédiées à sa préparation.

Il est possible que j'apporte des modifications ou des correctifs à ce cahier de charge. Vous êtes responsable de vérifier vos MIO.

Vous devez mettre en place un nouveau domaine "Active Directory" en respectant les configurations demandées dans ce document.

Rédaction du code PowerShell

Dans les fichiers de script à remettre, les premières lignes devront être des commentaires dans lesquelles vous devrez clairement identifier les informations suivantes:

- Votre nom et votre prénom
- Votre matricule
- La date de création du script
- L'objectif du code
- Le serveur à partir duquel le code doit être exécuté
- Les serveurs qui seront modifiés par l'exécution du code

Votre code devra contenir des commentaires pertinents. La présentation du code devra être structurée.

Si une valeur est utilisée à plusieurs reprises vous devez mettre cette valeur dans une variable.

L'évaluation du code passe par sa validité d'exécution mais aussi par sa qualité.

Votre code doit être compatible avec "PowerShell 5.1".

LA CORPORATION

Votre firme de consultants doit implanter un nouveau domaine "Active Directory" convenant à tous les types d'employés de l'entreprise.

Vous devez satisfaire les besoins corporatifs pour des accès à toutes les ressources à l'interne de la compagnie, mais aussi certains accès de l'externe.

Votre premier contrat au sein de l'entreprise, sera d'installer une gestion des ressources du département "Informatique".

Dans le département "Informatique" vous retrouverez les employés qui s'occupent entre-autres de la programmation Android, de la programmation Python, des techniciens du réseau, des concepteurs web, des testeurs de logiciels Android et des testeurs de logiciels Python.

INFRASTRUCTURE DU DOMAINE

Le domaine

Vous devez installer un nouveau domaine "Active Directory". Le nom du domaine sera "**ETUmatricule.LOCAL**" et **matricule** correspond à votre matricule étudiant.

Le niveau fonctionnel du domaine sera le plus élevé possible. Un serveur DNS sera présent sur ce serveur et contiendra tous les enregistrements relatifs à l'Active Directory.

En plus du contrôleur de domaine vous aurez un serveur membre.

Le nom des deux ordinateurs du domaine sera "**S1**" pour le contrôleur de domaine et "**S2**" pour le serveur membre.

INFRASTRUCTURE DU RESEAU

L'infrastructure est similaire à celle avec laquelle vous avez travaillé pendant le cours. Vous avez besoin d'un routeur pfSense et de deux machines virtuelles "Windows Serveur 2019" dans Hyper-V. Une des deux machines "Windows Serveur 2019" virtuelles sera le contrôleur de domaine.

Le plan d'adressage

Voici la configuration IPv4 des deux serveurs.

Contrôleur de domaine IP = 192.168.1.100/24
 Passerelle = 192.168.1.1
 DNS = 127.0.0.1

Serveur membre IP = 192.168.1.200/24
 Passerelle = 192.168.1.1
 DNS = 192.168.1.100

Vous pouvez utiliser le même routeur pfSense.

Description des serveurs

Les ordinateurs avec lesquels vous travaillerez tiendront des rôles très précis.

Le premier ordinateur virtuel sera le contrôleur de domaine. Ce serveur sera responsable des services "Active Directory", DNS et GPO.

Le deuxième serveur virtuel (serveur membre) sera responsable de gérer les services qui sont sur le contrôleur de domaine.

Sur ces deux serveurs, vous devez installer que les rôles et fonctionnalités qui sont nécessaires.

Les serveurs de fichiers

Le serveur S1 aura deux dossiers "E:_S1_INFO" et "E:_S1_PERSO".

Vous trouverez plus de détails sur les dossiers à créer dans la section se rapportant aux utilisateurs de votre département.

LE SERVEUR RÉEL

Hyper-V est déjà installé sur votre serveur réel. Vous avez besoin d'un commutateur virtuel de type "Privé" dont le nom sera PRIVE.

Création des ordinateurs virtuels

- Pour le projet, le nom des ordinateurs virtuels dans la console Hyper-V sera **PROJET_SERVEUR1** et **PROJET_SERVEUR2**.
- L'ordinateur virtuel **PROJET_SERVEUR1** aura une carte réseau. La carte réseau de l'ordinateur virtuel **PROJET_SERVEUR1** utilisera le commutateur virtuel **PRIVE**.
- L'ordinateur virtuel **PROJET_SERVEUR2** aura une carte réseau. La carte réseau de l'ordinateur virtuel **PROJET_SERVEUR2** utilisera le commutateur virtuel **PRIVE**.
- L'ordinateur virtuel **PROJET_SERVEUR1** aura un deuxième disque dur virtuel.

Configuration des ordinateurs virtuels

- Pour le projet, le nom des ordinateurs virtuels dans Windows sera **\$1** et **\$2**.
-

LE SERVEUR DNS

Un serveur DNS devra être implanté pour le projet.

Ce serveur DNS sera localisé sur le contrôleur de domaine.

La zone directe principale pour le domaine, sera automatiquement créée lors de la création du domaine "**ETUmatricule.LOCAL**".

STRATÉGIES DE GROUPE - DOMAINE

Vous devez planter deux stratégies au niveau du domaine.

- Les noms des stratégies devront être respectés.
- Les sections non utilisées des stratégies devront être désactivées.

Il est interdit de modifier les stratégies

- Default Domain Policy
- Default Domain Controllers Policy

LA GPO DOMAINE_Securite

■ ACTIVER LE PARAMÈTRE

Arrêt: permet au système d'être arrêté sans avoir à se connecter

■ ACTIVER ET CONFIGURER LA VALEUR DU PARAMÈTRE

Ouvertures de sessions interactives : nombre d'ouverture de sessions précédentes réalisées en utilisant la cache (lorsqu'aucun contrôleur de domaine n'est disponible)

- ❖ VALEUR = 0 ouvertures de session

LA GPO DOMAINE_Mot-de-passe

■ ACTIVER ET CONFIGURER LA VALEUR DU PARAMÈTRE

Durée de vie maximale du mot de passe

- ❖ VALEUR = 30 jours

■ ACTIVER ET CONFIGURER LA VALEUR DU PARAMÈTRE

Durée de vie minimale du mot de passe

- ❖ VALEUR = 0 jours

■ ACTIVER ET CONFIGURER LA VALEUR DU PARAMÈTRE

Longueur minimale du mot de passe

- ❖ VALEUR = 9 caractères

LE DÉPARTEMENT "INFORMATIQUE"

Comme nous l'avons mentionné dans la section de présentation de la corporation, le département "Informatique" regroupe les employés et les gestionnaires suivants:

■ **Les concepteurs WEB**

- ❖ Employés
- ❖ Gestionnaires

■ **Les programmeurs Android**

- ❖ Employés
- ❖ Gestionnaires

■ **Les programmeurs Python**

- ❖ Employés
- ❖ Gestionnaires

■ **Les techniciens du réseau**

- ❖ Employés
- ❖ Gestionnaires

■ **Les testeurs de logiciels Android**

- ❖ Employés
- ❖ Gestionnaires

■ **Les testeurs de logiciels Python**

- ❖ Employés
- ❖ Gestionnaires

Un gestionnaire n'est pas un employé.

LES UNITÉS D'ORGANISATION

Toutes vos unités d'organisation seront sous une unité d'organisation représentant votre département et se nommant "**INFORMATIQUE**".

NOTE: L'unité d'organisation "**INFORMATIQUE**" sera directement sous le domaine.

Vous devrez avoir une unité d'organisation qui portera le nom "Utilisateurs" qui se trouvera directement sous l'unité d'organisation "**INFORMATIQUE**".

Sous l'unité d'organisation "Utilisateurs" vous devez avoir un total de dix-huit unités d'organisation pour les employés et les gestionnaires, voir la page précédente.

Vous devrez avoir une unité d'organisation qui contient les groupes de votre domaine. L'unité d'organisation dédiée à contenir les groupes de votre domaine se trouvera directement sous l'unité d'organisation "**INFORMATIQUE**" et portera le nom "Groupes".

Vous devrez avoir une unité d'organisation qui contient les ordinateurs membres de votre domaine. L'unité d'organisation dédiée à contenir les ordinateurs membres de votre domaine se trouvera directement sous l'unité d'organisation "**INFORMATIQUE**" et portera le nom "Ordinateurs". Dans le cadre du projet cette unité d'organisation ne contiendra qu'un seul objet ordinateur.

Aucun nom d'unité d'organisation doit contenir d'espace ou de caractère accentué.

LES UTILISATEURS

Généralités sur les utilisateurs

Tous vos utilisateurs auront le même mot de passe.

Tous vos utilisateurs devront obligatoirement avoir les propriétés suivantes:

- le nom d'ouverture de session sera le matricule de l'employé

- un prénom, un nom et un nom complet

Le nom complet sera constitué du prénom du nom et d'un code.

Exemple: PRÉNOM NOM – CODE

- une description significative

- le compte est actif

- le mot de passe n'expire jamais

- un dossier personnel lié à la lettre P:

PROGRAMMATION DES UTILISATEURS

Le fichier PRATIQUE_ETU_A2024.CSV contient les informations nécessaires pour créer les utilisateurs.

LES GROUPES

Généralités sur les groupes

Pour chaque groupe créé, il devra y avoir

- Nom de groupe (antérieur à Windows 2000)
- Une description significative

Tous les groupes devront être de type "Sécurité" et d'étendue "Globale".

- Vous devez créer un groupe par corps de métier pour les employés.
- Vous devez créer un groupe par corps de métier pour les gestionnaires.
- Vous devez créer un groupe qui va contenir tous les employés.
- Vous devez créer un groupe qui va contenir tous les gestionnaires.
- Vous devez créer un groupe qui va contenir tous les employés et tous les gestionnaires.
- Vos noms de groupe doivent être significatifs.

Pour l'emplacement des groupes dans l'Active Directory, je vous demande de les placer dans l'unité d'organisation "Groupes".

Ajouter les utilisateurs aux groupes

Chaque utilisateur sera membre du groupe qui contient tous les utilisateurs de la corporation.

De plus, vous devrez placer vos utilisateurs dans leur groupe respectif et dans leur unité d'organisation respective.

Le matricule de l'employé indique le groupe de l'utilisateur et le nom de l'unité d'organisation dans lequel il doit être présent.

- Matricule entre 10000 et 19999 = Programmeurs Python
- Matricule entre 20000 et 29999 = Programmeurs Android
- Matricule entre 30000 et 39999 = Techniciens du réseau
- Matricule entre 40000 et 49999 = Concepteurs WEB
- Matricule entre 50000 et 59999 = Testeurs de logiciels Python
- Matricule entre 60000 et 69999 = Testeurs de logiciels Android

De plus, les utilisateurs dont le matricule est 10000, 20000, 30000, 40000, 50000 et 60000 sont des gestionnaires.

LES SERVEURS DE FICHIERS

Les dossiers personnels

Les dossiers personnels seront sous le dossier E:_S1_PERSO du contrôleur de domaine.

Tous vos utilisateurs devront avoir un dossier personnel, auquel aucun autre utilisateur du département "INFORMATIQUE" n'aura accès.

Les autorisations NTFS sur le dossier E:_S1_PERSO seront:

- Le groupe Administrateurs aura l'autorisation "Contrôle total".
- Le groupe Système aura l'autorisation "Contrôle total".
- "DROITS DU PROPRIÉTAIRE" aura l'autorisation "Modification".
- Le groupe qui contient tous les employés aura l'autorisation "Lecture et exécution" sur ce dossier seulement.
- Le groupe qui contient tous les gestionnaires aura l'autorisation "Lecture et exécution" sur ce dossier seulement.

Chaque utilisateur aura l'autorisation "**Modification**" sur son dossier personnel.

Le dossier racine de vos dossiers personnels sera partagé.

Le nom du partage devra avoir un nom significatif.

L'énumération basée sur l'accès devra être activée.

La mise en cache sera désactivée.

Les dossiers du département

Des dossiers sont mis à la disposition des utilisateurs du département.

Le nom des dossiers qui seront sous "E:_S1_INFO"

- CONCEPTEURS_WEB
- PROGRAMMATION_ANDROID
- PROGRAMMATION_PYTHON
- TECHNICIENS
- TESTEURS_ANDROID
- TESTEURS_PYTHON

Le dossier racine qui contient les dossiers du département sera partagé.

Le nom du partage devra avoir un nom significatif.

L'énumération basée sur l'accès devra être activée.

La mise en cache doit être désactivée.

Autorisations sur les dossiers du département

Les autorisations NTFS sur le dossier "**E:_S1_INFO**" seront:

- Le groupe Administrateurs aura l'autorisation "Contrôle total".
- Le groupe Système aura l'autorisation "Contrôle total".
- "DROITS DU PROPRIÉTAIRE" aura l'autorisation "Modification".
- Le groupe qui contient tous les employés aura l'autorisation "Lecture et exécution" sur ce dossier seulement.
- Le groupe qui contient tous les gestionnaires aura l'autorisation "Lecture et exécution" sur ce dossier seulement.

Pour le dossier **CONCEPTEURS_WEB** ajouter les autorisations NTFS

- Le groupe des **concepteurs WEB** aura l'autorisation "**Modification**"
- Le groupe des gestionnaires des **concepteurs WEB** aura l'autorisation "Contrôle total".

Pour le dossier **PROGRAMMATION_ANDROID** ajouter les autorisations NTFS

- Le groupe des **programmeurs Android** aura l'autorisation "**Modification**"
- Le groupe des gestionnaires des **programmeurs Android** aura l'autorisation "Contrôle total".

Pour le dossier **PROGRAMMATION_PYTHON** ajouter les autorisations NTFS

- Le groupe des **programmeurs Python** aura l'autorisation "**Modification**"
- Le groupe des gestionnaires des **programmeurs Python** aura l'autorisation "Contrôle total".

Pour le dossier **TECHNICIENS** ajouter les autorisations NTFS

- Le groupe des **techniciens du réseau** aura l'autorisation "**Modification**"
- Le groupe des gestionnaires des **techniciens du réseau** aura l'autorisation "Contrôle total".

Pour le dossier **TESTEURS_ANDROID** ajouter les autorisations NTFS

- Le groupe des **testeurs de logiciels Android** aura l'autorisation "**Modification**"
- Le groupe des gestionnaires des **testeurs de logiciels Android** aura l'autorisation "Contrôle total".

Pour le dossier **TESTEURS_PYTHON** ajouter les autorisations NTFS

- Le groupe des **testeurs de logiciels Python** aura l'autorisation "**Modification**"
- Le groupe des gestionnaires des **testeurs de logiciels Python** aura l'autorisation "Contrôle total".

Un espace de noms

Vous devez créer un espace de noms pour tous les employés du département.

L'espace de noms sera de type "Domaine" et sera géré par le serveur 1.

Le nom de l'espace de noms sera DFSinformatique.

L'espace de nom DFSinformatique contiendra un dossier qui donnera accès au partage du dossier "E:_S1_INFO".

LES QUOTAS DE DOSSIERS

Description des quotas

Le dossier qui contient les dossiers personnels de vos utilisateurs sera soumis à un quota automatique inconditionnel de 250 Mo.

Le dossier "E:_S1_INFO" sera soumis à un quota conditionnel de 500 Mo.

Les rapports de quotas

Un rapport sur l'utilisation de vos quotas de dossiers devra être généré.

Les rapports de quotas devront être en format HTML.

STRATÉGIES DE GROUPE

Vous devez implanter une stratégie de groupe au niveau des ordinateurs clients du département INFORMATIQUE et une stratégie de groupe au niveau des utilisateurs du département INFORMATIQUE.

- Les noms des stratégies devront être respectés.
- Les sections non utilisées des stratégies devront être désactivées.

Stratégie pour les postes clients du département

Tous les ordinateurs clients de votre département devront être soumis aux paramètres de la stratégie de groupe. Votre serveur membre est considéré comme un poste client de votre département.

LA GPO ORDINATEURS_INFORMATIQUE

■ ACTIVER LE PARAMÈTRE

Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session

■ DÉSACTIVER LE PARAMÈTRE

Afficher l'animation à la première connexion

■ DÉSACTIVER LE PARAMÈTRE

Afficher le moniteur d'évènements de mise hors tension

■ ACTIVER ET CONFIGURER LA VALEUR DU PARAMÈTRE

Désactiver l'affichage (sur secteur)

❖ **Désactiver l'affichage (secondes) = 0**

■ ACTIVER ET CONFIGURER LA VALEUR DU PARAMÈTRE

Activer l'exécution des scripts

❖ **VALEUR = Autoriser tous les scripts**

■ ACTIVER ET CONFIGURER LES DEUX VALEURS DU PARAMÈTRE

Définir l'intervalle d'actualisation de la stratégie de groupe pour les ordinateurs

❖ **la fréquence d'application de la stratégie de groupe aux ordinateurs = 5 minutes**

❖ **l'ajout d'une durée aléatoire = 1 minute**

Stratégie pour les utilisateurs du département

Tous les utilisateurs de votre département seront soumis aux paramètres de la stratégie de groupe.

LA GPO UTILISATEURS_INFORMATIQUE

■ ACTIVER LE PARAMÈTRE

Toujours afficher tous les éléments du Panneau de configuration à son ouverture

■ ACTIVER ET CONFIGURER LE PARAMÈTRE

Démarrer l'Explorateur de fichiers avec le ruban réduit

- ❖ Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit

■ ACTIVER ET CONFIGURER LES DEUX VALEURS DU PARAMÈTRE

Définir l'intervalle d'actualisation de la stratégie de groupe pour les utilisateurs

- ❖ la fréquence d'application de la stratégie de groupe aux utilisateurs = 5 minutes
- ❖ l'ajout d'une durée aléatoire = 1 minute

■ AJOUTER ET METTRE À JOUR LA VARIABLE D'ENVIRONNEMENT SUIVANTE

- ❖ DIRCMD=/a/o

■ AJOUTER ET METTRE À JOUR LA CLÉ DE REGISTRE SUIVANTE

- ❖ Chemin d'accès à la clé = HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
- ❖ Nom de la valeur = ShowSecondsInSystemClock
- ❖ Type de la valeur = REG_DWORD
- ❖ Données de la valeur = 0x1

■ AJOUTER ET METTRE À JOUR LE MAPPAGE DE LECTEURS

- ❖ Emplacement: \\ETUmatricule.LOCAL\DFSi informatique
- ❖ Utiliser la lettre R:

■ MODIFIER LES OPTIONS DES DOSSIERS

- ❖ Sélectionner "Afficher les fichiers et dossiers cachés" dans la section "Fichiers et dossiers cachés"
- ❖ Décocher "Masquer les extensions des fichiers dont le type est connu"
- ❖ Décocher "Masquer les fichiers protégés du système d'exploitation (recommandé)"
- ❖ Décocher "Utiliser l'Assistant Partage (recommandé)"

ANNEXE - ÉVALUATIONS

Évaluation de la deuxième étape

Les modifications que le professeur vous demandera d'effectuer seront disponibles seulement le **13 décembre**.

Cette étape représente **25%** de la note finale du cours.

Quotas sur les dossiers

Objectifs

- Créer, modifier ou détruire des quotas sur les répertoires.
- Utiliser la console de gestion des quotas.
- Obtenir des rapports sur l'utilisation des espaces disque.
- Utiliser smtp4dev.exe sur le SERVEUR1 afin de recevoir les courriels du SERVEUR2
smtp4dev - the fake SMTP email server for development and testing
smtp4dev-2.0.10-binaries.zip est disponible sur LEA

Étape 1 - Installation du rôle "Gestionnaire de ressources du serveur de fichiers"

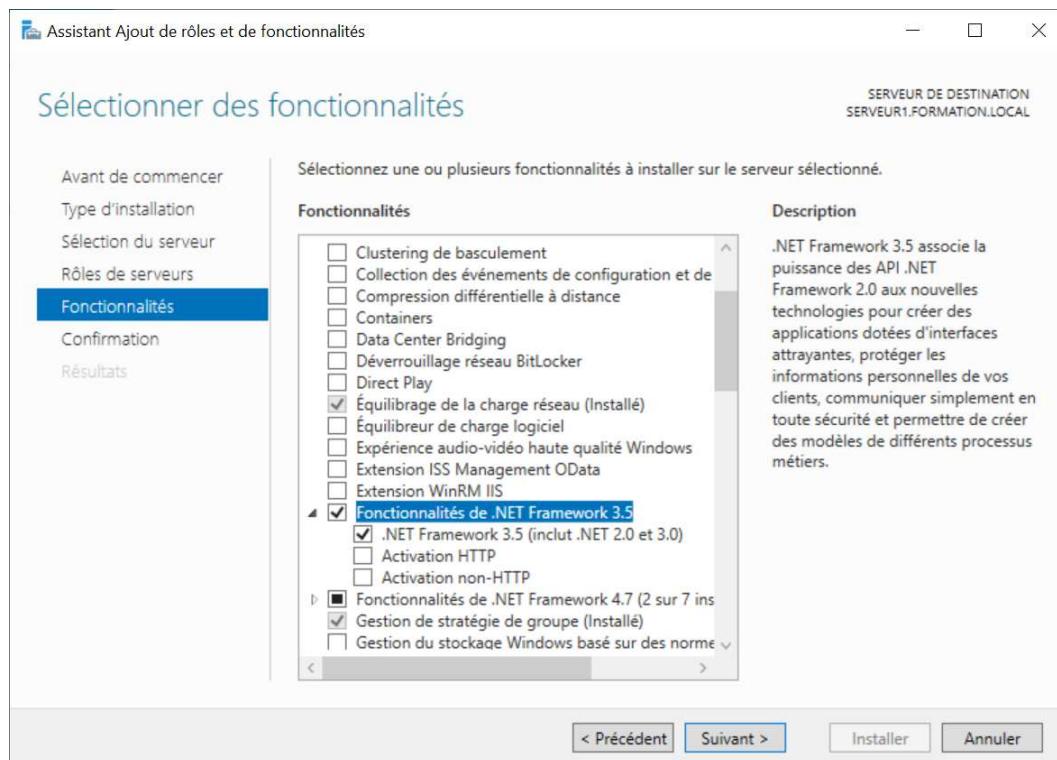
La gestion des quotas de disque se fait via la console "Gestionnaire de ressources du serveur de fichiers".
Cette console est présente seulement si le rôle "Gestionnaire de ressources du serveur de fichiers" est installé.

Nous avons déjà installé ce rôle sur les deux serveurs dans un laboratoire précédent.

Étape 2 - Utiliser et configurer smtp4dev.exe sur le SERVEUR1

SMTP4DEV.EXE oblige l'installation de la fonctionnalité ".NET Framework 3.5".

Méthode 1 - Utilisation de "Gestionnaire de serveur"

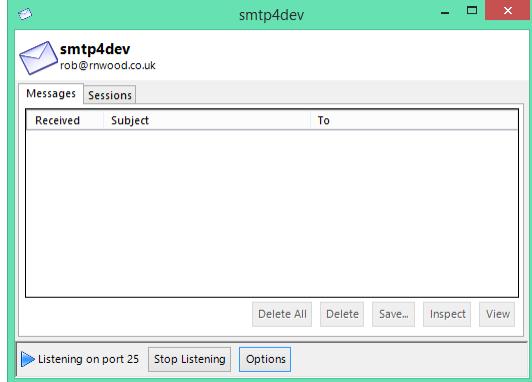


Méthode 2 – Utilisation du dossier "sources" qui est dans le ISO d'installation

Si l'installation de la fonctionnalité ".NET Framework 3.5" ne fonctionne pas en utilisant le "Gestionnaire de serveur", vous devez récupérer le dossier **sources** et son contenu et le copier dans un dossier du SERVEUR1.
"\\\uranusprof.reseau.cvm\intranet\rjean\SERVEUR_2019\sources\sxs"

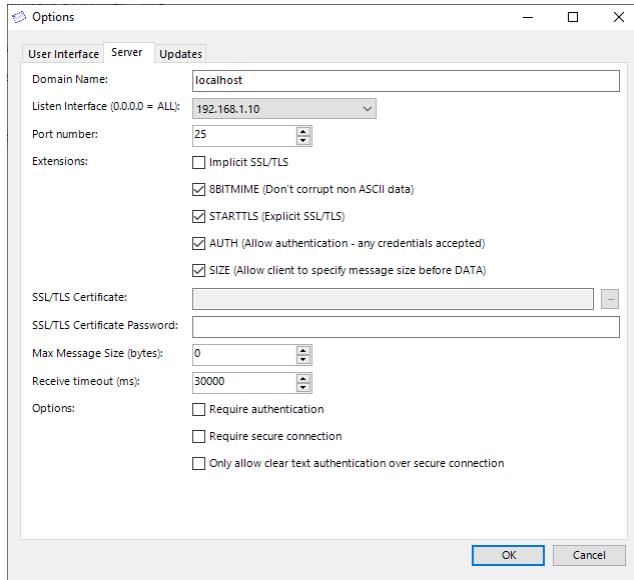
```
# Le dossier peut varier
$chemin = "e:\_temp\sources\sxs"
Install-WindowsFeature NET-Framework-Core -Source $chemin
```

Exécuter **smtp4dev.exe**



note: pour afficher le contenu d'un courriel, on doit utiliser le bouton "**Inspect**".

Le bouton "**Options**" permet de configurer le paramètre "**Listen interface**" avec la valeur **192.168.1.10**
note: indiquer l'adresse IP du SERVEUR1



Étape 3 - Configurer le "Pare-feu Windows" sur le SERVEUR1

Dans la console "Pare-feu Windows Defender" autoriser une application et sélectionner l'emplacement du fichier SMTP4DEV.EXE et cocher DOMAINE, PRIVÉ et PUBLIC.

Les prochaines étapes se font sur le SERVEUR2.

Étape 4 - Configuration du serveur SMTP dans la console des quotas

Dans la console "Gestionnaire de ressources du serveur de fichiers"

- Dans le menu "Action / Configurer les options..."

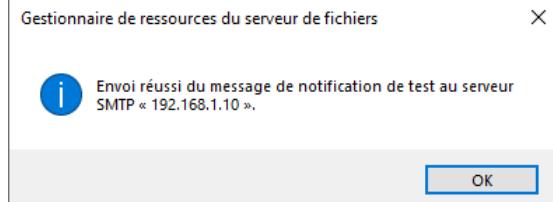
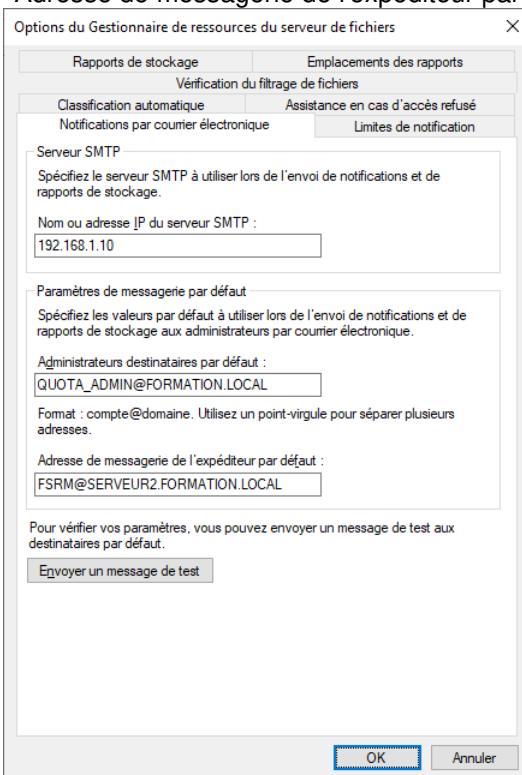
Selectionner l'onglet "Notifications par courrier électronique"

❖ "Nom ou adresse IP du serveur SMTP" = **192.168.1.10**

note: indiquer l'adresse IP du SERVEUR1

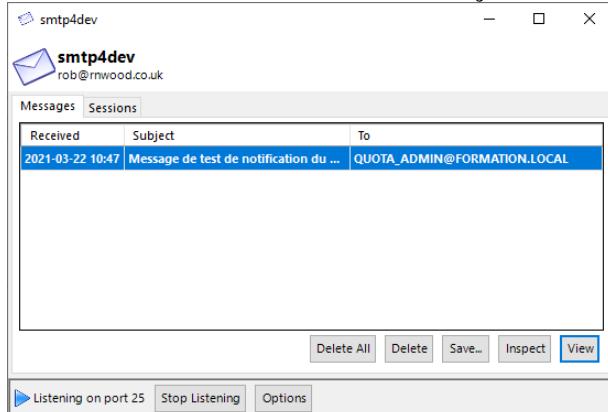
❖ "Administrateurs destinataires par défaut" = **QUOTA_ADMIN@FORMATION.LOCAL**

❖ "Adresse de messagerie de l'expéditeur par défaut" = **FSRM@SERVEUR2.FORMATION.LOCAL**



- ❖ Cliquer sur le bouton "Envoyer un message de test" pour vérifier la fonctionnalité

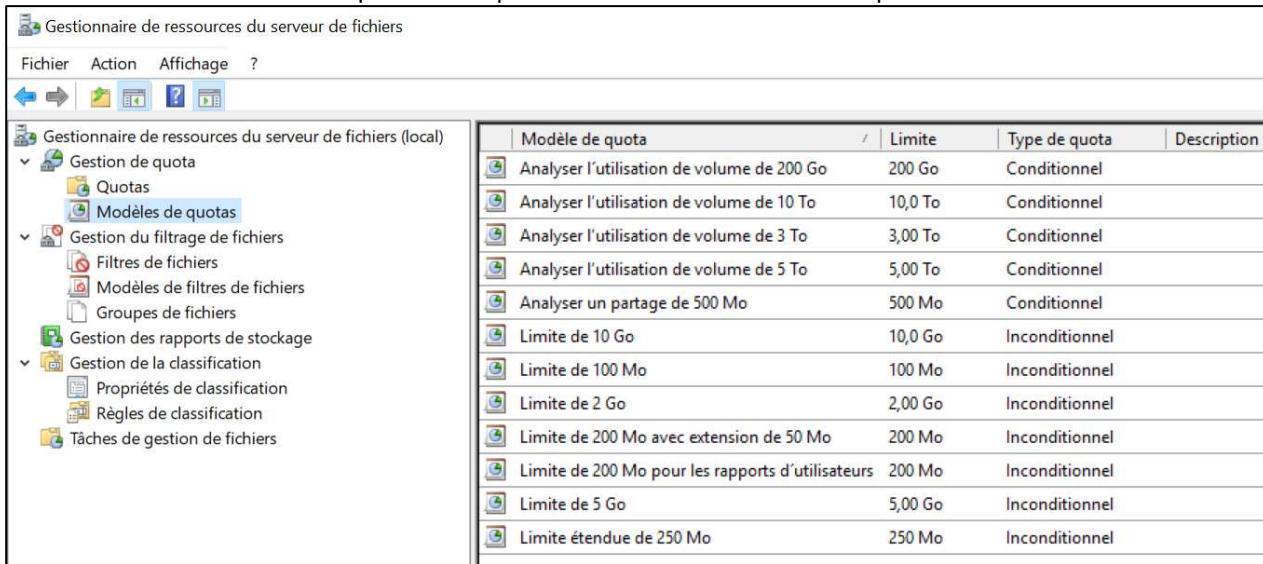
Sur le SERVEUR1, vous devez avoir reçu un courriel qui confirme que le serveur SMTP est fonctionnel.



Étape 5 - Exploration de la sous-console "Gestion de quota"

Dans la console "Gestionnaire de ressources du serveur de fichiers"

- Ouvrir la section "Gestion de quota" et cliquer sur la section "Modèles de quotas".



The screenshot shows the Windows Server Resource Management console. The left pane displays a tree view of resources under 'Gestion de ressources du serveur de fichiers (local)'. The 'Modèles de quotas' node is selected. The right pane lists 13 quota models in a table:

Modèle de quota	Limite	Type de quota	Description
Analyser l'utilisation de volume de 200 Go	200 Go	Conditionnel	
Analyser l'utilisation de volume de 10 To	10,0 To	Conditionnel	
Analyser l'utilisation de volume de 3 To	3,00 To	Conditionnel	
Analyser l'utilisation de volume de 5 To	5,00 To	Conditionnel	
Analyser un partage de 500 Mo	500 Mo	Conditionnel	
Limite de 10 Go	10,0 Go	Inconditionnel	
Limite de 100 Mo	100 Mo	Inconditionnel	
Limite de 2 Go	2,00 Go	Inconditionnel	
Limite de 200 Mo avec extension de 50 Mo	200 Mo	Inconditionnel	
Limite de 200 Mo pour les rapports d'utilisateurs	200 Mo	Inconditionnel	
Limite de 5 Go	5,00 Go	Inconditionnel	
Limite étendue de 250 Mo	250 Mo	Inconditionnel	

- Mettre votre curseur sur un des modèles de quota dans la section à droite de la console.

En vous servant du menu contextuel "**Modifier les propriétés du modèle...**" trouvez la différence entre le type de quota "Conditionnel" et "Inconditionnel"

- Quota inconditionnel**

réponse: **Empêcher les utilisateurs de dépasser la limite**

- Quota conditionnel**

réponse: **Autoriser les utilisateurs à dépasser la limite (utilisé pour l'analyse)**

Sélectionner le modèle "**Limite de 200 Mo avec extension de 50 Mo**"

Trouver la commande qui est exécutée lorsque la limite de 200 Mo est atteinte.

- Commande**

réponse: **%windir%\system32\dirquota.exe**

- Arguments de la commande**

réponse: **quota modify /path:[Quota Path] /sourcetemplate:"Limite étendue de 250 Mo"**

À quoi servent les seuils de notification ?

- réponse: **Génère automatiquement des actions quand une limite est franchie**

Identifier les quatre actions qui peuvent être entreprises quand on définit un seuil de notification.

- Envoyer un courriel
- Envoyer un avertissement au journal des événements
- Exécuter une commande
- Générer un rapport

Étape 6 - Création de quota sur chemin d'accès

La création de quota sur "chemin d'accès" permet de fixer une limite d'espace disque pour le contenu total d'un dossier. Vous devez créer le dossier "E:_CHEMIN".

La création

- Dans la section "Quotas", dans le menu contextuel choisir l'option "Créer un quota..."
- Dans la boîte de dialogue
 - À l'aide du bouton "Parcourir" sélectionner le dossier "E:_CHEMIN"
 - Choisir l'option "Créer un quota sur le chemin d'accès"
 - Choisir l'option "Dériver les propriétés de ce modèle de quota (recommandé):"
Choisir le modèle "Limite de 200 Mo avec extension de 50 Mo"

La vérification

- Déposer des fichiers dans ce dossier
 - Créer un fichier de 20 Mo dans le dossier

```
fsutil.exe file createnew E:\_CHEMIN\F1_20MO.txt 20971520
```
- Observer le résultat dans la console "Gestionnaire de ressources du serveur de fichiers"
note: la touche F5 permet d'actualiser l'affichage

Étape 7 - Création d'un modèle de quota

Un modèle de quota est un gabarit qui est utilisé comme base pour les quotas. La modification d'un modèle de quotas est utile, car toute modification à cet objet entraîne automatiquement une mise à jour des quotas qui l'utilise.

La création du modèle

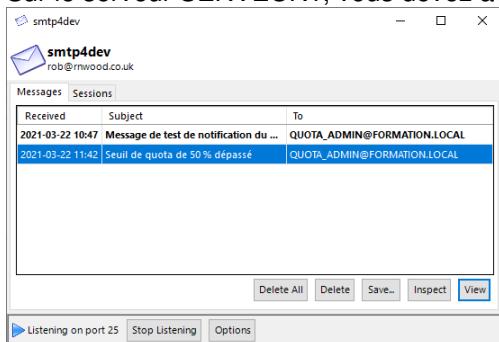
- Dans la section "Modèles de quotas", dans le menu contextuel choisir l'option "Créer un modèle de quota..."
- Dans la boite de dialogue
 - Dans l'item "Copier les propriétés du modèle de quota (facultatif)":
 - Choisir le modèle "Limite de 100 Mo"
 - Cliquer sur le bouton "Copier"
 - Dans la section "Paramètres"
 - Nom du modèle: **votre_prénom** - Limite de 50 Mo
 - Description: Premier modèle de **votre_prénom**
 - Limite: 50 Mo
 - Choisir l'option "Quota inconditionnel"
 - Ajouter un seuil de notification à 50%Dans l'onglet "Journal des événements" cocher "Envoyer un avertissement au journal des événements"
Dans l'onglet "Message électronique" cocher "Envoyer un courriel électronique aux administrateurs suivants" **[Admin Email]**

La création du quota

- Dans la section "Quotas", dans le menu contextuel choisir l'option "Créer un quota..."
- Dans la boite de dialogue
 - À l'aide du bouton "Parcourir" sélectionner le dossier "E:_WEB"
 - Choisir l'option "Créer un quota sur le chemin d'accès"
 - Choisir l'option "Dériver les propriétés de ce modèle de quota (recommandé)":
 - Choisir le modèle "**votre_prénom** - Limite de 50 Mo"

La vérification

- Créer un fichier de 30 Mo dans le dossier
`fsutil.exe file createnew E:_WEB\F1_30MO.txt 31457280`
- Observer le résultat dans la console "Gestionnaire de ressources du serveur de fichiers"
 - La console ne s'actualise pas en temps réel
 - Vous pouvez utiliser l'option "Actualiser" sur la section "Quotas" ou dans le panneau d'actions (à droite)
- Observer le résultat dans la console "Observateur d'événements"
 - Section "Affichages personnalisés"
 - Sous-section "Événements d'administration"
note: un avertissement de la source SRMSVC est présent
- Sur le serveur SERVEUR1, vous devez avoir reçu un courriel pour le seuil de quota de 50% dépassé



Étape 8 - Création d'un rapport de quota

La création

- Dans la console "Gestion de ressources du serveur de fichiers", section "Gestion des rapports de stockage" menu contextuel, choisir l'option "Planifier une nouvelle tâche de rapport..."
- Dans la boîte de dialogue
 - Dans l'onglet "Paramètres"
 - Le nom du rapport: Mon premier rapport
 - Dans la section "Données de rapport"
 - Sélectionner seulement la rubrique "Utilisation du quota"
 - Dans la section "Formats des rapports"
 - Sélectionner seulement le format HTML
 - Dans l'onglet "Étendue"
 - Dans l'étendue "Ajouter" le disque E:\
 - Dans l'onglet "Planification"
 - Elle doit être tous les jours à 09:00

Que permet de faire le bouton "Modifier les paramètres..." dans l'onglet "Paramètres" ?

- réponse: **Définir le nombre de jours qui doivent être considéré, ainsi que les utilisateurs**

La vérification

- Sur la nouvelle tâche de rapport (écran de droite) dans le menu contextuel choisir "Exécuter la tâche de rapport maintenant..."
- Procéder en choisissant l'option "Attendre que les rapports soient générés avant de les afficher"
- Vérifier les résultats qui seront affichés dans votre navigateur Web

Le dossier **C:\StorageReports\Interactives** contient les rapports qui ne sont pas planifiés

Le dossier **C:\StorageReports\Scheduled** contient les rapports qui sont planifiés

Étape 9 - Création d'un quota automatique

Le quota automatique s'applique sur un dossier, comme les quotas vus précédemment, mais il n'a pas d'impact sur ce dossier directement.

Ce dossier représente plutôt la racine qui héberge des sous-dossiers.

Ce quota sera hérité "automatiquement" par tous les dossiers situés directement sous cette racine.

Chaque sous-dossier individuellement sera donc limité en espace selon le quota automatique imposé.

La création du modèle

- Créer un modèle
 - Nom: **Mini quota**
 - Inconditionnel de 5 Mo

La création du quota

- Créer un quota
 - Chemin d'accès: À l'aide du bouton "Parcourir" sélectionner le dossier "E:_MINI"
 - Choisir l'option "Appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux"
 - Choisir l'option "Dériver les propriétés de ce modèle de quota (recommandé):
 - Choisir le modèle "**Mini quota**"

La vérification

- Avec votre utilisateur déposer un petit fichier dans le dossier "E:_MINI\EMP02"
- À partir du SERVEUR2, avec l'utilisateur "EMP02"
 - Déposer un petit fichier de 1 Ko dans le dossier "E:_MINI\EMP02"
`fsutil.exe file createnew E:_MINI\EMP02\F1_1KO.txt 1024`
 - Déposer trois fichiers de 2 Mo dans le dossier "E:_MINI\EMP02"
`fsutil.exe file createnew E:_MINI\EMP02\F1_2MO.txt 2097152`
`fsutil.exe file createnew E:_MINI\EMP02\F2_2MO.txt 2097152`
`fsutil.exe file createnew E:_MINI\EMP02\F3_2MO.txt 2097152`
- Dans votre console des quotas vérifier le détail des affichages
- Générer un rapport de quota

Quand on crée un quota automatique, peut-on choisir de définir des propriétés personnalisées ?

- réponse: **Non on doit obligatoirement dériver d'un modèle**

Dans l'interface GUI, comment peut-on distinguer les quotas de chemin d'accès des quotas automatiques ?

- réponse: **Leur icône est différente, on peut aussi utiliser le filtrage.**

Quotas sur les dossiers

Objectifs

- Créer, modifier ou détruire des quotas sur les répertoires.
- Utiliser la console de gestion des quotas.
- Obtenir des rapports sur l'utilisation des espaces disque.
- Utiliser smtp4dev.exe sur le SERVEUR1 afin de recevoir les courriels du SERVEUR2
smtp4dev - the fake SMTP email server for development and testing
smtp4dev-2.0.10-binaries.zip est disponible sur LÉA

Étape 1 - Installation du rôle "Gestionnaire de ressources du serveur de fichiers"

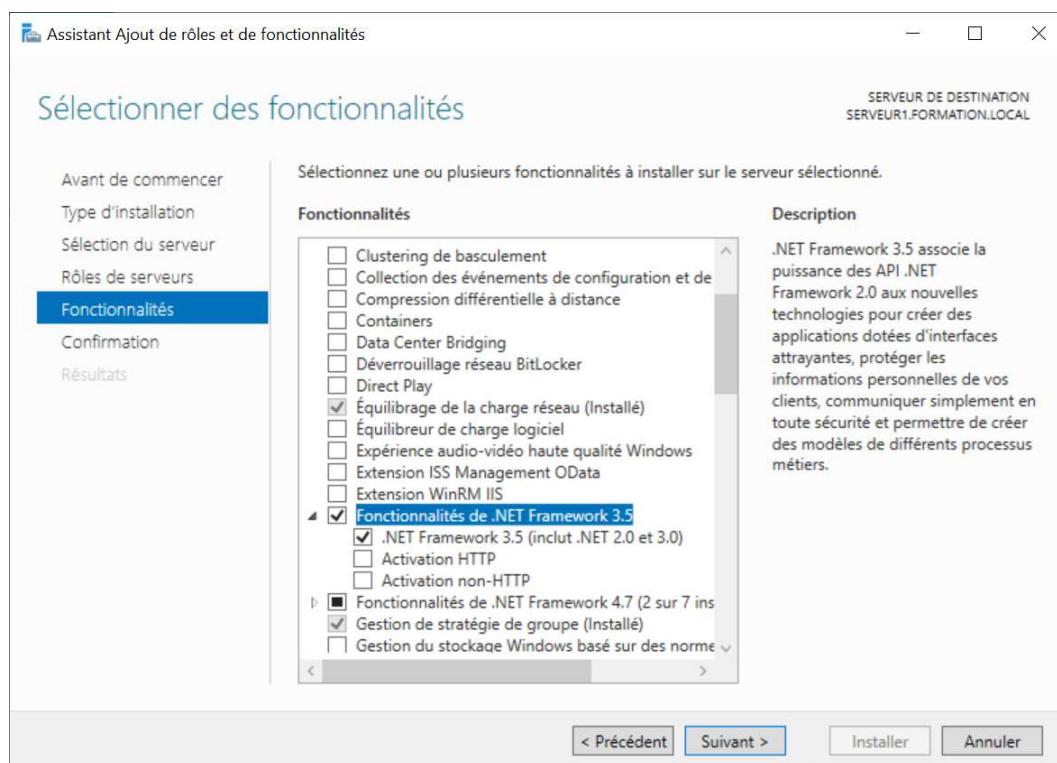
La gestion des quotas de disque se fait via la console "Gestionnaire de ressources du serveur de fichiers".
Cette console est présente seulement si le rôle "Gestionnaire de ressources du serveur de fichiers" est installé.

Nous avons déjà installé ce rôle sur les deux serveurs dans un laboratoire précédent.

Étape 2 - Utiliser et configurer smtp4dev.exe sur le SERVEUR1

SMTP4DEV.EXE oblige l'installation de la fonctionnalité ".NET Framework 3.5".

Méthode 1 - Utilisation de "Gestionnaire de serveur"

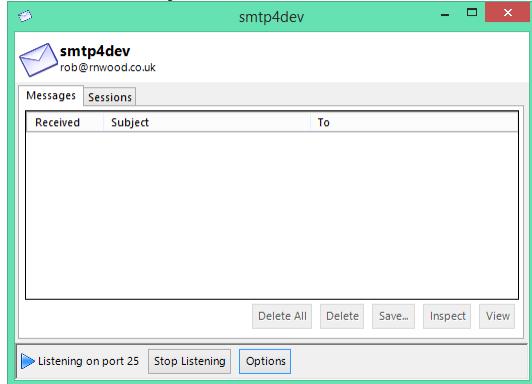


Méthode 2 – Utilisation du dossier "sources" qui est dans le ISO d'installation

Si l'installation de la fonctionnalité ".NET Framework 3.5" ne fonctionne pas en utilisant le "Gestionnaire de serveur", vous devez récupérer le dossier **sources** et son contenu et le copier dans un dossier du SERVEUR1.
"\\"uranusprof.reseau.cvm\intranet\rjean\SERVEUR_2019\sources\sxs"

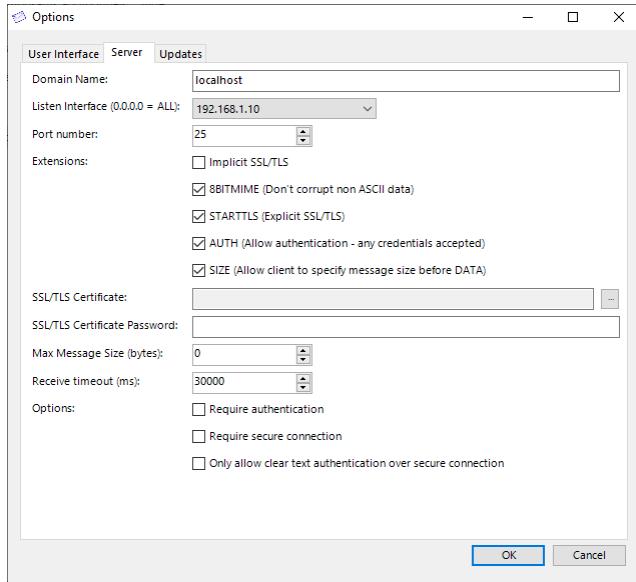
```
# Le dossier peut varier
$chemin = "e:\_temp\sources\sxs"
Install-WindowsFeature NET-Framework-Core -Source $chemin
```

Exécuter **smtp4dev.exe**



note: pour afficher le contenu d'un courriel, on doit utiliser le bouton "**Inspect**".

Le bouton "**Options**" permet de configurer le paramètre "**Listen interface**" avec la valeur **192.168.1.10**
note: indiquer l'adresse IP du SERVEUR1



Étape 3 - Configurer le "Pare-feu Windows" sur le SERVEUR1

Dans la console "Pare-feu Windows Defender" autoriser une application et sélectionner l'emplacement du fichier SMTP4DEV.EXE et cocher DOMAINE, PRIVÉ et PUBLIC.

Les prochaines étapes se font sur le SERVEUR2.

Étape 4 - Configuration du serveur SMTP dans la console des quotas

Dans la console "Gestionnaire de ressources du serveur de fichiers"

- Dans le menu "Action / Configurer les options..."

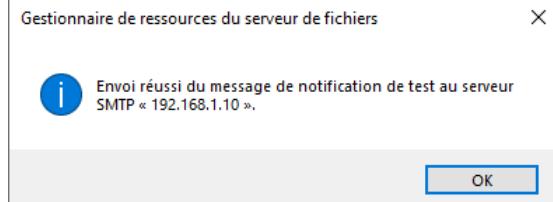
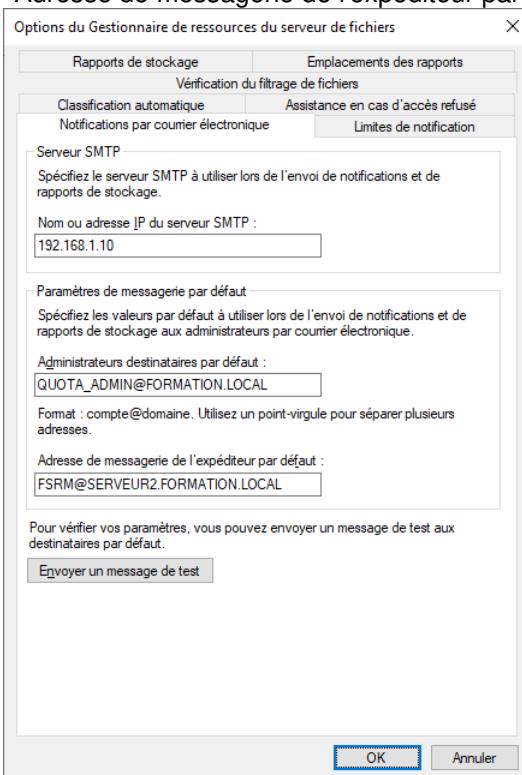
Selectionner l'onglet "Notifications par courrier électronique"

❖ "Nom ou adresse IP du serveur SMTP" = **192.168.1.10**

note: indiquer l'adresse IP du SERVEUR1

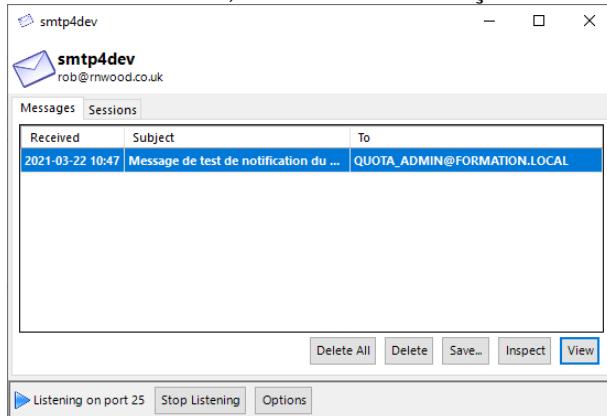
❖ "Administrateurs destinataires par défaut" = **QUOTA_ADMIN@FORMATION.LOCAL**

❖ "Adresse de messagerie de l'expéditeur par défaut" = **FSRM@SERVEUR2.FORMATION.LOCAL**



- ❖ Cliquer sur le bouton "Envoyer un message de test" pour vérifier la fonctionnalité

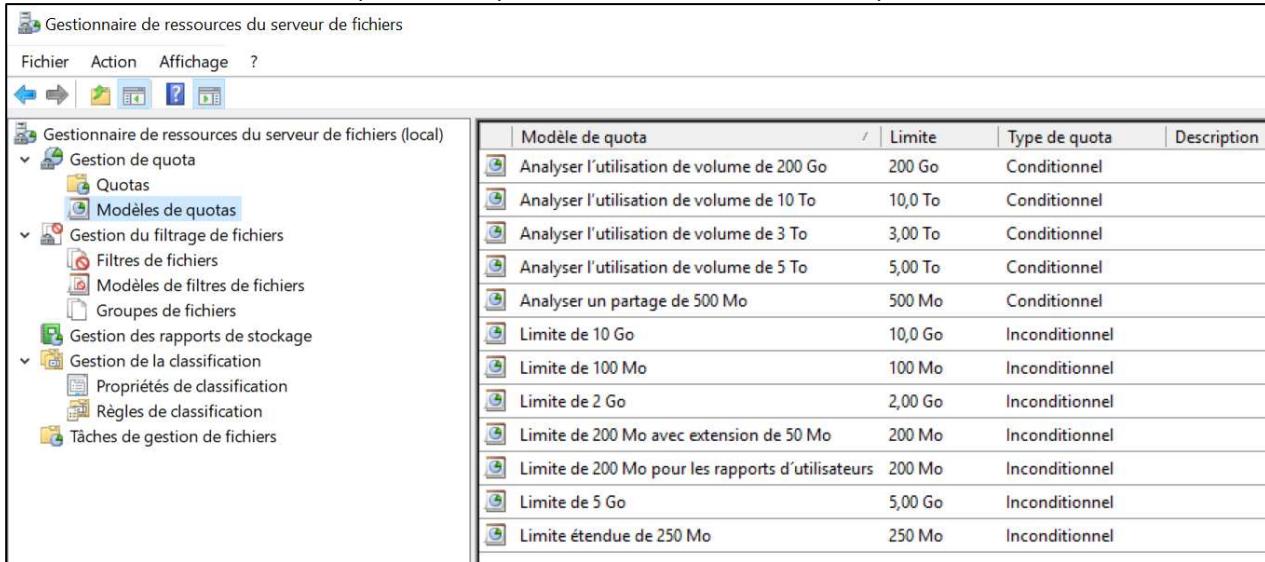
Sur le SERVEUR1, vous devez avoir reçu un courriel qui confirme que le serveur SMTP est fonctionnel.



Étape 5 - Exploration de la sous-console "Gestion de quota"

Dans la console "Gestionnaire de ressources du serveur de fichiers"

- Ouvrir la section "Gestion de quota" et cliquer sur la section "Modèles de quotas".



The screenshot shows the Windows Server File Resource Manager console. The left pane displays a tree view of resources under 'Gestionnaire de ressources du serveur de fichiers (local)'. The 'Modèles de quotas' node is selected. The right pane shows a table titled 'Modèle de quota' listing various quota models with their limits and types.

Modèle de quota	Limite	Type de quota	Description
Analyser l'utilisation de volume de 200 Go	200 Go	Conditionnel	
Analyser l'utilisation de volume de 10 To	10,0 To	Conditionnel	
Analyser l'utilisation de volume de 3 To	3,00 To	Conditionnel	
Analyser l'utilisation de volume de 5 To	5,00 To	Conditionnel	
Analyser un partage de 500 Mo	500 Mo	Conditionnel	
Limite de 10 Go	10,0 Go	Inconditionnel	
Limite de 100 Mo	100 Mo	Inconditionnel	
Limite de 2 Go	2,00 Go	Inconditionnel	
Limite de 200 Mo avec extension de 50 Mo	200 Mo	Inconditionnel	
Limite de 200 Mo pour les rapports d'utilisateurs	200 Mo	Inconditionnel	
Limite de 5 Go	5,00 Go	Inconditionnel	
Limite étendue de 250 Mo	250 Mo	Inconditionnel	

- Mettre votre curseur sur un des modèles de quota dans la section à droite de la console.

En vous servant du menu contextuel "**Modifier les propriétés du modèle...**"

trouvez la différence entre le type de quota "Conditionnel" et "Inconditionnel"

- Quota inconditionnel**

réponse:

- Quota conditionnel**

réponse:

Sélectionner le modèle "**Limite de 200 Mo avec extension de 50 Mo**"

Trouver la commande qui est exécutée lorsque la limite de 200 Mo est atteinte.

- Commande**

réponse:

- Arguments de la commande**

réponse:

À quoi servent les seuils de notification ?

- réponse:

Identifier les quatre actions qui peuvent être entreprises quand on définit un seuil de notification.

- Envoyer un courriel
- Envoyer un avertissement au journal des événements
- Exécuter une commande
- Générer un rapport

Étape 6 - Création de quota sur chemin d'accès

La création de quota sur "chemin d'accès" permet de fixer une limite d'espace disque pour le contenu total d'un dossier. Vous devez créer le dossier "E:_CHEMIN".

La création

- Dans la section "Quotas", dans le menu contextuel choisir l'option "Créer un quota..."
- Dans la boîte de dialogue
 - À l'aide du bouton "Parcourir" sélectionner le dossier "E:_CHEMIN"
 - Choisir l'option "Créer un quota sur le chemin d'accès"
 - Choisir l'option "Dériver les propriétés de ce modèle de quota (recommandé):"
Choisir le modèle "Limite de 200 Mo avec extension de 50 Mo"

La vérification

- Déposer des fichiers dans ce dossier
 - Créer un fichier de 20 Mo dans le dossier

```
fsutil.exe file createnew E:\_CHEMIN\F1_20MO.txt 20971520
```
- Observer le résultat dans la console "Gestionnaire de ressources du serveur de fichiers"
note: la touche F5 permet d'actualiser l'affichage

Étape 7 - Création d'un modèle de quota

Un modèle de quota est un gabarit qui est utilisé comme base pour les quotas. La modification d'un modèle de quotas est utile, car toute modification à cet objet entraîne automatiquement une mise à jour des quotas qui l'utilise.

La création du modèle

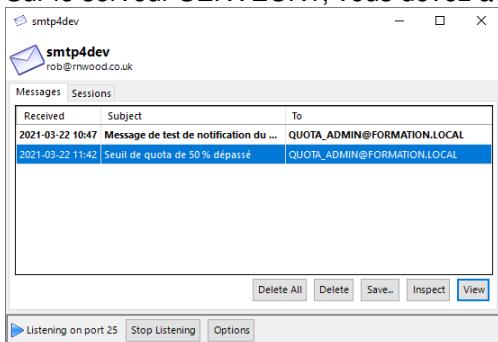
- Dans la section "Modèles de quotas", dans le menu contextuel choisir l'option "Créer un modèle de quota..."
- Dans la boîte de dialogue
 - Dans l'item "Copier les propriétés du modèle de quota (facultatif)":
 - Choisir le modèle "Limite de 100 Mo"
 - Cliquer sur le bouton "Copier"
 - Dans la section "Paramètres"
 - Nom du modèle: **votre_prénom** - Limite de 50 Mo
 - Description: Premier modèle de **votre_prénom**
 - Limite: 50 Mo
 - Choisir l'option "Quota inconditionnel"
 - Ajouter un seuil de notification à 50%Dans l'onglet "Journal des événements" cocher "Envoyer un avertissement au journal des événements"
Dans l'onglet "Message électronique" cocher "Envoyer un courriel électronique aux administrateurs suivants" **[Admin Email]**

La création du quota

- Dans la section "Quotas", dans le menu contextuel choisir l'option "Créer un quota..."
- Dans la boîte de dialogue
 - À l'aide du bouton "Parcourir" sélectionner le dossier "E:_WEB"
 - Choisir l'option "Créer un quota sur le chemin d'accès"
 - Choisir l'option "Dériver les propriétés de ce modèle de quota (recommandé)":
 - Choisir le modèle "**votre_prénom** - Limite de 50 Mo"

La vérification

- Créer un fichier de 30 Mo dans le dossier
`fsutil.exe file createnew E:_WEB\F1_30MO.txt 31457280`
- Observer le résultat dans la console "Gestionnaire de ressources du serveur de fichiers"
 - La console ne s'actualise pas en temps réel
 - Vous pouvez utiliser l'option "Actualiser" sur la section "Quotas" ou dans le panneau d'actions (à droite)
- Observer le résultat dans la console "Observateur d'événements"
 - Section "Affichages personnalisés"
 - Sous-section "Événements d'administration"
note: un avertissement de la source SRMSVC est présent
- Sur le serveur SERVEUR1, vous devez avoir reçu un courriel pour le seuil de quota de 50% dépassé



Étape 8 - Création d'un rapport de quota

La création

- Dans la console "Gestion de ressources du serveur de fichiers", section "Gestion des rapports de stockage" menu contextuel, choisir l'option "Planifier une nouvelle tâche de rapport..."
- Dans la boîte de dialogue
 - Dans l'onglet "Paramètres"
 - Le nom du rapport: Mon premier rapport
 - Dans la section "Données de rapport"
 - Sélectionner seulement la rubrique "Utilisation du quota"
 - Dans la section "Formats des rapports"
 - Sélectionner seulement le format HTML
 - Dans l'onglet "Étendue"
 - Dans l'étendue "Ajouter" le disque E:\
 - Dans l'onglet "Planification"
 - Elle doit être tous les jours à 09:00

Que permet de faire le bouton "Modifier les paramètres..." dans l'onglet "Paramètres" ?

- réponse:

La vérification

- Sur la nouvelle tâche de rapport (écran de droite) dans le menu contextuel choisir "Exécuter la tâche de rapport maintenant..."
- Procéder en choisissant l'option "Attendre que les rapports soient générés avant de les afficher"
- Vérifier les résultats qui seront affichés dans votre navigateur Web

Le dossier **C:\StorageReports\Interactives** contient les rapports qui ne sont pas planifiés

Le dossier **C:\StorageReports\Scheduled** contient les rapports qui sont planifiés

Étape 9 - Création d'un quota automatique

Le quota automatique s'applique sur un dossier, comme les quotas vus précédemment, mais il n'a pas d'impact sur ce dossier directement.

Ce dossier représente plutôt la racine qui héberge des sous-dossiers.

Ce quota sera hérité "automatiquement" par tous les dossiers situés directement sous cette racine.

Chaque sous-dossier individuellement sera donc limité en espace selon le quota automatique imposé.

La création du modèle

- Créer un modèle
 - Nom: **Mini quota**
 - Inconditionnel de 5 Mo

La création du quota

- Créer un quota
 - Chemin d'accès: À l'aide du bouton "Parcourir" sélectionner le dossier "E:_MINI"
 - Choisir l'option "Appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux"
 - Choisir l'option "Dériver les propriétés de ce modèle de quota (recommandé):
 - Choisir le modèle "**Mini quota**"

La vérification

- Avec votre utilisateur déposer un petit fichier dans le dossier "E:_MINI\EMP02"
- À partir du SERVEUR2, avec l'utilisateur "EMP02"
 - Déposer un petit fichier de 1 Ko dans le dossier "E:_MINI\EMP02"
`fsutil.exe file createnew E:_MINI\EMP02\F1_1KO.txt 1024`
 - Déposer trois fichiers de 2 Mo dans le dossier "E:_MINI\EMP02"
`fsutil.exe file createnew E:_MINI\EMP02\F1_2MO.txt 2097152`
`fsutil.exe file createnew E:_MINI\EMP02\F2_2MO.txt 2097152`
`fsutil.exe file createnew E:_MINI\EMP02\F3_2MO.txt 2097152`
- Dans votre console des quotas vérifier le détail des affichages
- Générer un rapport de quota

Quand on crée un quota automatique, peut-on choisir de définir des propriétés personnalisées ?

- réponse:

Dans l'interface GUI, comment peut-on distinguer les quotas de chemin d'accès des quotas automatiques ?

- réponse:

Introduction aux "Espaces de noms"

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

Objectifs

- Maîtriser les concepts reliés aux DFS (espace de nom, racine, cible et dossier, réPLICATION)
- Maîtriser la gestion des DFS (création, modification, réPLICATION)
- Maîtriser l'utilisation des DFS

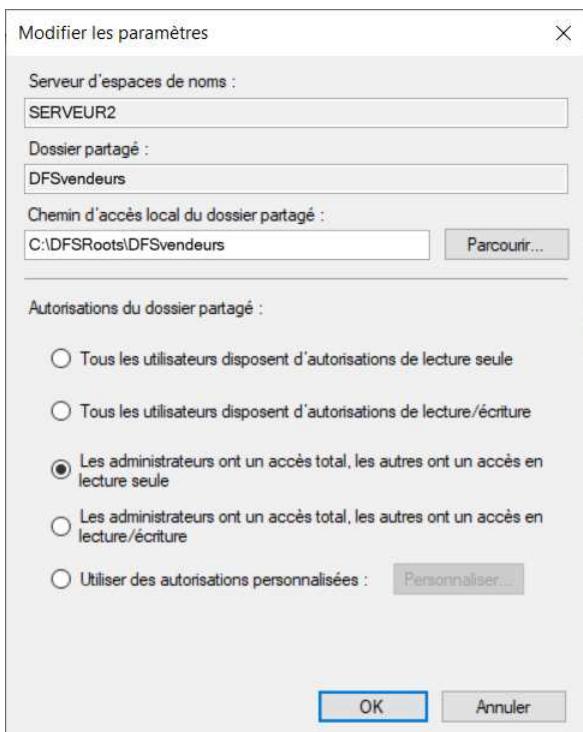
Étape 1 - Création de la racine d'un espace de noms

Sur le SERVEUR2, dans la console "Gestion du système de fichiers distribués DFS"

- Sur l'item "Espace de noms", dans le menu contextuel, choisir l'option "Nouvel espace de noms..."

Répondre aux questions de l'assistant "Nouvel Espace de noms"

- Écran "Serveur d'espaces de noms"
 - inscrire le nom de votre serveur virtuel 2 = **SERVEUR2**
- Écran "Nom et paramètres de l'espace de noms"
Vous devez inscrire le nom de l'espace de noms pour que le bouton "Modifier les paramètres..." soit actif.
 - Nom: **DFSVendeurs**
 - Bouton "Modifier les paramètres..."
 - Serveur d'espaces de noms = SERVEUR2
 - Dossier partagé = DFSvendeurs
 - Chemin d'accès local du dossier partagé = C:\DFSRoots\DFSVendeurs
Le dossier "**C:\DFSRoots**" est créé lors de la création du premier espace de noms.
 - Autorisations du dossier partagé
 - "Les administrateurs ont un accès total, les autres ont un accès en lecture seule"



- Écran "**Type d'espace de noms**"
 - Sélectionner "Espace de noms de domaine"
 - Cocher "Activer le mode Windows Server 2008"
 - Aperçu de l'espace de noms de domaine
Le nom de référence de votre espace de nom est **\FORMATION.LOCAL\DFSVendeurs**
 - Écran "**Revoir les paramètres et créer l'espace de noms**"
 - Cliquer sur le bouton "Créer" pour déclencher la création de votre espace de noms
-

Lors de la création de votre Espace de Noms via la console, voici les étapes qui sont faites automatiquement:

- Création du dossier C:\DFSRoots\DFSVendeurs
- Création du partage DFSvendeurs sur le dossier C:\DFSRoots\DFSVendeurs
- Création de l'espace de noms \FORMATION.LOCAL\DFSVendeurs

Il est important de connaître ces étapes, car elles ne sont pas faites automatiquement lors de la création d'un espace de nom en PowerShell. Il faut utiliser des cmdlets pour faire les différentes étapes.

Étape 2 - Insertion de dossiers et de cibles

Dans votre console, dans l'écran de gauche, sélectionner votre nouvel espace de noms \\FORMATION.LOCAL\DFSVendeurs et ajouter des dossiers.

Vous pouvez utiliser les fonctionnalités Ajouter, Parcourir, Rechercher et Afficher les partages pour trouver les "cibles du dossier"

Premier dossier

- Sur votre espace de nom, dans le menu contextuel, choisir l'option "**Nouveau dossier...**"
 - Nom: Commandes
 - Cible du dossier (chemin d'accès): **SERVEUR2\C53_Cmd**

La console va créer le dossier "C:\DFSRoots\DFSVendeurs\Commandes" qui sera utilisé pour la gestion de cet espace de noms.

Deuxième dossier

- Sur votre espace de nom, dans le menu contextuel, choisir l'option "**Nouveau dossier...**"
 - Nom: Clients
 - Cible du dossier (chemin d'accès): **SERVEUR1\C53_Cli**

La console va créer le dossier "C:\DFSRoots\DFSVendeurs\Clients" qui sera utilisé pour la gestion de cet espace de noms.

Étape 3 - Utilisation de votre espace de noms

Tester votre espace de noms en l'associant à une lettre dans votre explorateur de fichiers.

Ouvrir l'Explorateur de fichiers

- Effectuer l'opération "Connecter un lecteur réseau"
- Lier cet espace de noms à la lettre V:
- Le nom de référence de l'espace de noms: **FORMATION.LOCAL\DFSVendeurs**
- Ne pas cocher "Se reconnecter lors de la connexion"

Test 1

Ouvrir l'explorateur de fichiers et accéder à votre espace de noms en utilisant la lettre V.
Vous devez vérifier si les deux dossiers "Commandes" et "Clients" sont présents sous la DFS.

Test 2

Vous devez vérifier que vous pouvez écrire dans les dossiers "Commandes" et "Clients".

Test 3

Vous devez vérifier que le contenu des partages **SERVEUR2\C53_Cmd** et **SERVEUR1\C53_Cli** correspond au contenu des dossiers "**Commandes**" et "**Clients**" qui sont sous la DFS.

Étape 4 - Création d'un espace de noms avec réPLICATION

Sur le SERVEUR2, dans la console "Gestion du système de fichiers distribués DFS" créer un nouvel espace de noms ayant les caractéristiques suivantes

- Écran "**Serveur d'espaces de noms**"
 - inscrire le nom du contrôleur de domaine (SERVEUR1)
- Écran "**Nom et paramètres de l'espace de noms**"
Vous devez inscrire le nom de l'espace de noms, mais faites attention un bouton "Modifier les paramètres..." sera disponible dès que votre nom sera inscrit et vous devrez l'utiliser.
 - Nom: **DFSproduction**
 - Bouton "Modifier les paramètres..."
 - Chemin d'accès local du dossier partagé: C:\DFSRoots\DFSproduction
 - Autorisations du dossier partagé
 - "Les administrateurs ont un accès total, les autres ont un accès en lecture seule"
- Écran "**Type d'espace de noms**"
 - Sélectionner "Espace de noms de domaine"
 - Cocher "Activer le mode Windows Server 2008"
 - Aperçu de l'espace de noms de domaine
Le nom de référence de votre espace de nom est **\FORMATION.LOCAL\DFSproduction**
- Écran "**Revoir les paramètres et créer l'espace de noms**"
 - Cliquer sur le bouton "Créer" pour déclencher la création de votre espace de noms

Dans votre console, dans l'écran de gauche, sélectionner votre nouvel espace de noms "**\FORMATION.LOCAL\DFSproduction**"

Premier dossier

- Nom: Commandes
- Cible du dossier (chemin d'accès): **\SERVEUR2\C53_Cmd**

Deuxième dossier

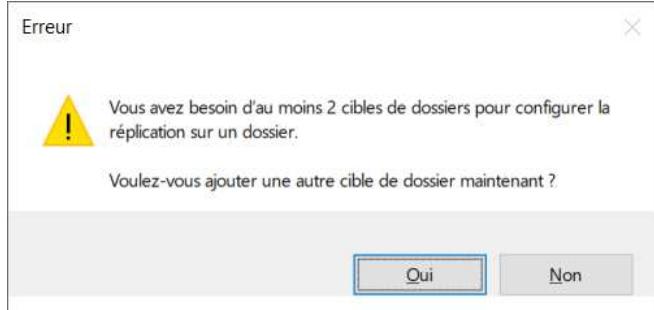
- Nom: Inventaire
- Cible du dossier (chemin d'accès): **\SERVEUR1\C53_InvB**

Troisième dossier

- Nom: Production
- Cible du dossier (chemin d'accès): **\SERVEUR2\C53_Prod**

Comme l'inventaire est un dossier d'une importance primordiale pour la compagnie, il est emmagasiné à deux endroits. En créant une "réplique" dans un espace de noms pour un dossier, on crée un processus de synchronisation automatique. Nous aurons donc par la même occasion un mécanisme de tolérance de panne.

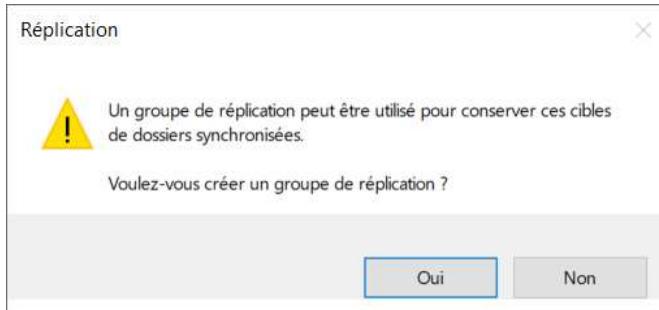
Le curseur sur "Inventaire", dans le menu contextuel vous devez sélectionner "**Répliquer un dossier...**".



Cliquer sur le bouton "**Oui**"

Choisir l'option "**Ajouter une cible de dossier...**"

- Chemin d'accès à la cible du dossier: \\SERVEUR2\C53_InvA



Vous devez répondre OUI pour créer un groupe de réplication.

- Écran "**Nom du groupe de réplication et du dossier répliqué**"
 - Ne rien changer dans le premier écran
- Écran "**Éligibilité de réplication**"
 - Les deux partages d'inventaire devraient être listés
- Écran "**Membre principal**"
 - Choisir le contrôleur de domaine (SERVEUR1)
- Écran "**Sélection de topologie**"
 - Sélectionner "Maille pleine"
- Écran "**Planification du groupe de réplication et bande passante**"
 - Choisir l'option "Répliquer aux jours et heures spécifiés"
 - Horaire de réplication: **Tous les jours de 08:00 à 18:00, avec une utilisation complète de la bande passante**
- Écran "**Vérifier les paramètres et créer le groupe de réplication**"
 - Cliquer sur le bouton "Créer" pour déclencher la création du groupe de réplication



Lier cet espace de noms à la lettre T:

Tester les dossiers de votre espace de nom.

La modification du contenu de \\FORMATION.LOCAL\DFSproduction\Inventaire met à jour automatiquement les partages \\SERVEUR1\C53_InvB et \\SERVEUR2\C53_InvA

Étape 5 - Création d'un espace de noms avec une DFS

Créer un "nouvel espace de nom"

- Écran "Serveur d'espaces de noms"
 - inscrire le nom de votre serveur virtuel 2
- Écran "**Nom et paramètres de l'espace de noms**"
 - Nom: **DFSmkteting**
 - Bouton "Modifier les paramètres..."
 - Chemin d'accès local du dossier partagé: C:\DFSRoots\DFSmkteting
 - Autorisations du dossier partagé
 - "Les administrateurs ont un accès total, les autres ont un accès en lecture seule"
- Écran "**Type d'espace de noms**"
 - Sélectionner "Espace de noms de domaine"
 - Cocher "Activer le mode Windows Server 2008"
 - Aperçu de l'espace de noms de domaine
 - Le nom de référence de votre espace de nom est **\FORMATION.LOCAL\DFSmkteting**
- Écran "**Revoir les paramètres et créer l'espace de noms**"
 - Cliquer sur le bouton "Créer" pour déclencher la création de votre espace de noms

Dans votre nouvel espace de noms créer trois dossiers

Premier dossier

- Nom : Publicité
- Cible du dossier (chemin d'accès): **\SERVEUR1\C53_Pub**

L'espace de noms "Publicité" pointe vers le partage \SERVEUR1\C53_Pub, ce partage contient des dossiers avec des autorisations spécifiques à chaque utilisateur. L'énumération basée sur l'accès est activée sur le partage \SERVEUR1\C53_Pub.

Deuxième dossier

- Nom : WEB
- Cible du dossier (chemin d'accès): **\SERVEUR2\C53_Web**

Troisième dossier (attention: ce sera une DFS et non un partage simple)

- Nom : Vendeurs
- Cible du dossier (chemin d'accès): **\SERVEUR2\DFSVendeurs**

Tester votre DFS avec les utilisateurs du groupe grINF_Gestionnaires à partir du SERVEUR2.

Vérifier vos droits de lecture et d'écriture dans les dossiers qui sont dans cette DFS.

Vérifier ce qui est visible dans le cas du dossier "Publicité" de la DFS \FORMATION.LOCAL\DFSmkteting.

- EMP09 voit seulement son dossier.
- EMP10 voit seulement son dossier.