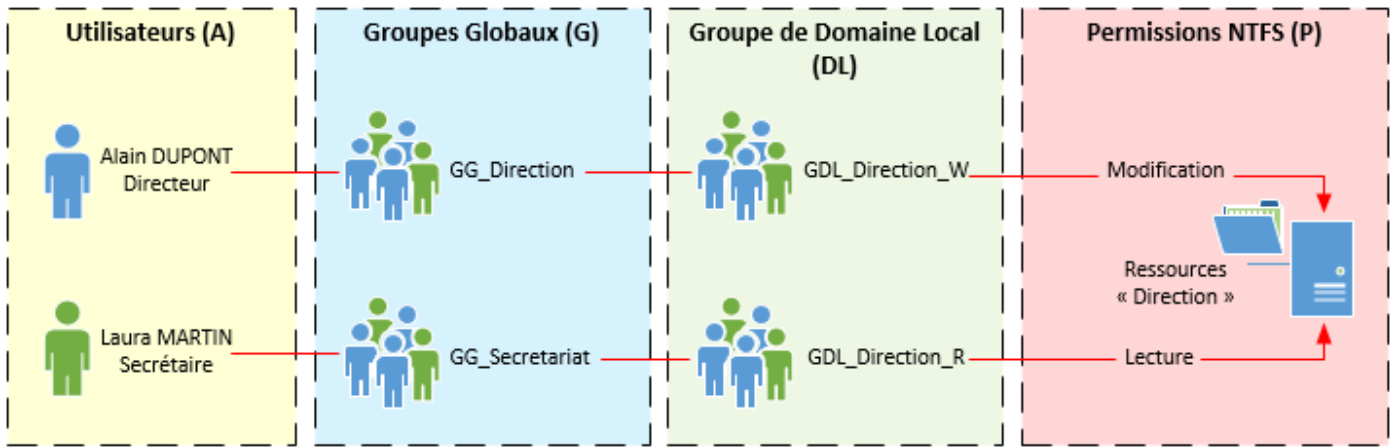


Appliquer les ACL



Introduction

Nous reprenons une nouvelle fois notre fichier CSV :

NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4	NIVEAU 5	NIVEAU 6	NIVEAU 7	NIVEAU 8	FolderPath	CREER_GROUPS	GG_ECRITURE	GG_LECTURE	GDL_ECRITURE	GDL_LECTURE	GDL_VUE	Parent_GDL
01-DIRECTION								01-DIRECTION		ORG_GG_DIRECTION		GDL_01_ECRITURE	GDL_01_LECTURE	GDL_01_VUE	
02-FINANCE								02-FINANCE		ORG_GG_FINANCE	ORG_GG_DIRECTION	GDL_02_ECRITURE	GDL_02_LECTURE	GDL_02_VUE	
02-FINANCE	01-BUDGET							02-FINANCE\01-BUDGET		ORG_GG_FINANCE	ORG_GG_DIRECTION	GDL_02-01_ECRITURE	GDL_02-01_LECTURE	GDL_02-01_VUE	GDL_02_VUE
02-FINANCE	02-FACTURES							02-FINANCE\02-FACTURES		ORG_GG_FINANCE	ORG_GG_DIRECTION	GDL_02-02_ECRITURE	GDL_02-02_LECTURE	GDL_02-02_VUE	GDL_02_VUE
03-RH								03-RH		ORG_GG_RH	ORG_GG_DIRECTION	GDL_03_ECRITURE	GDL_03_LECTURE	GDL_03_VUE	
03-RH	01-CONTRATS							03-RH\01-CONTRATS		ORG_GG_RH	ORG_GG_DIRECTION	GDL_03-01_ECRITURE	GDL_03-01_LECTURE	GDL_03-01_VUE	GDL_03_VUE
03-RH	02-PAIE							03-RH	NON						
04-IT								04-IT		ORG_GG_IT	ORG_GG_DIRECTION	GDL_04_ECRITURE	GDL_04_LECTURE	GDL_04_VUE	
04-IT	01-INFRA							04-IT\01-INFRA		ORG_GG_IT	ORG_GG_DIRECTION	GDL_04-01_ECRITURE	GDL_04-01_LECTURE	GDL_04-01_VUE	GDL_04_VUE
04-IT	02-PROJETS							04-IT\02-PROJETS		ORG_GG_IT	ORG_GG_DIRECTION	GDL_04-02_ECRITURE	GDL_04-02_LECTURE	GDL_04-02_VUE	GDL_04_VUE

```

NIVEAU 1;NIVEAU 2;NIVEAU 3;NIVEAU 4;NIVEAU 5;NIVEAU 6;NIVEAU 7;NIVEAU
8;FolderPath;CREER_GROUPS;GG_ECRITURE;GG_LECTURE;GDL_ECRITURE;GDL_LECTURE;GDL_VUE;Parent_GDL
01-DIRECTION;;;;;;;01-DIRECTION;;ORG_GG_DIRECTION;;GDL_01_ECRITURE;GDL_01_LECTURE;GDL_01_VUE;
02-FINANCE;;;;;;;02-
FINANCE;;ORG_GG_FINANCE;ORG_GG_DIRECTION;GDL_02_ECRITURE;GDL_02_LECTURE;GDL_02_VUE;
02-FINANCE;01-BUDGET;;;;;;02-FINANCE\01-BUDGET;;ORG_GG_FINANCE;ORG_GG_DIRECTION;GDL_02-
01_ECRITURE;GDL_02-01_LECTURE;GDL_02-01_VUE;GDL_02_VUE
02-FINANCE;02-FACTURES;;;;;;02-FINANCE\02-FACTURES;;ORG_GG_FINANCE;ORG_GG_DIRECTION;GDL_02-
02_ECRITURE;GDL_02-02_LECTURE;GDL_02-02_VUE;GDL_02_VUE
03-RH;;;;;;;03-RH;;ORG_GG_RH;ORG_GG_DIRECTION;GDL_03_ECRITURE;GDL_03_LECTURE;GDL_03_VUE;
03-RH;01-CONTRATS;;;;;;03-RH\01-CONTRATS;;ORG_GG_RH;ORG_GG_DIRECTION;GDL_03-
01_ECRITURE;GDL_03-01_LECTURE;GDL_03-01_VUE;GDL_03_VUE
03-RH;02-PAIE;;;;;;;03-RH;NON;;;;;;
04-IT;;;;;;;04-IT;;ORG_GG_IT;ORG_GG_DIRECTION;GDL_04_ECRITURE;GDL_04_LECTURE;GDL_04_VUE;
    
```

```
04-IT;01-INFRA;;;;;;04-IT\01-INFRA;;ORG_GG_IT;ORG_GG_DIRECTION;GDL_04-01_ECRITURE;GDL_04-01_LECTURE;GDL_04-01_VUE;GDL_04_VUE
04-IT;02-PROJETS;;;;;;04-IT\02-PROJETS;;ORG_GG_IT;ORG_GG_DIRECTION;GDL_04-02_ECRITURE;GDL_04-02_LECTURE;GDL_04-02_VUE;GDL_04_VUE
04-IT;02-PROJETS;2026;;;;;;04-IT\02-PROJETS\2026;NON;;;;;;
```

Application des droits

Voici le script qui permet d'appliquer les droits à chaque GDL homonymique de son répertoire, ainsi que l'héritage des groupes RW à l'ensemble des enfants.

Encore une fois, le script ne se sert que des colonnes utiles dans le cas présent : FolderPath, GDL_RW et GDL_RO :

```
<#
=====
SCRIPT : 4.1 - Appliquer_ACL.ps1
OBJET  : Appliquer les ACL NTFS tri-niveaux (ECRITURE / LECTURE / VUE)
=====

DESCRIPTION :
  Pour chaque dossier present dans le CSV :
    * Desactiver l'heritage NTFS
    * Supprimer toutes les ACL existantes
    * Appliquer les droits :
      - GDL_ECRITURE : Modify (herite)
      - GDL_LECTURE  : ReadAndExecute (herite)
      - GDL_VUE      : ReadAndExecute (non herite)
      - Administrateurs : Modify (herite)
      - Admins du domaine : Modify (herite)
      - SYSTEM : Modify (herite)

REMARQUE :
  - Le script suppose que 2.1 et 3.1 ont deja genere les GDL
    et les chainages Parent_GDL.
=====
#>
```

```

Param(
    [string]$RootPath = "\\SRV-DATAS\datas\",
    [string]$CsvPath  = "C:\AGDLP\ORG_ARBO_GDL.csv"
)

$errorActionPreference = "Stop"

# -----
# 1. Verification des droits administrateur (indispensable pour Set-Acl)
# -----
$principal = New-Object
Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())
if (-not $principal.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {
    Write-Warning "Ce script doit etre lance en tant qu administrateur."
    exit 1
}

# -----
# 2. Lecture du CSV
# -----
if (-not (Test-Path $CsvPath)) {
    Write-Error "CSV introuvable : $CsvPath"
    exit 1
}

$rows = Import-Csv -Path $CsvPath -Delimiter ";" -Encoding UTF8
$total = $rows.Count
$index = 0

Write-Host "Application des ACL NTFS a partir du fichier : $CsvPath"
Write-Host "Racine de donnees : $RootPath"
Write-Host ""

# -----
# 3. Comptes administratifs ayant toujours Modify (herite)
# -----
$RWAdmins = @(
    "Administrateurs",
    "Admins du domaine",
    "Administrateur-lcc",

```

```

"SYSTEM"
)

# -----
# 4. Traitement principal
# -----

foreach ($entry in $rows) {
    $index++

    # Mise a jour de la barre de progression
    Write-Progress -Activity "Application ACL" `
        -Status "$index / $total" `
        -PercentComplete (($index / $total) * 100)

    # Verifier la presence de FolderPath
    if ([string]::IsNullOrEmpty($entry.FolderPath)) { continue }

    # Construit le chemin complet
    $folderFullPath = Join-Path -Path $RootPath -ChildPath $entry.FolderPath

    if (-not (Test-Path -LiteralPath $folderFullPath)) {
        Write-Warning "Dossier introuvable : $folderFullPath"
        continue
    }

    try {
        # -----
        # 4.1 Recuperation des ACL actuelles et desactivation de l heritage
        # -----
        $acl = Get-Acl -LiteralPath $folderFullPath
        $acl.SetAccessRuleProtection($true, $false) # Disable inheritance, remove inherited
rules

        # Suppression de toutes les ACL existantes
        foreach ($rule in @($acl.Access)) {
            [void]$acl.RemoveAccessRule($rule)
        }

        # Types et drapeaux utiles
        $Allow = [System.Security.AccessControl.AccessControlType]::Allow

```

```

$CI_OI = [System.Security.AccessControl.InheritanceFlags] "ContainerInherit,
ObjectInherit"
$NonePF = [System.Security.AccessControl.PropagationFlags]::None

# -----
# 4.2 GDL_ECRITURE : Modify (herite)
# -----
if ($entry.GDL_ECRITURE -and $entry.GDL_ECRITURE.Trim() -ne "") {
    $ruleE = New-Object System.Security.AccessControl.FileSystemAccessRule(
        $entry.GDL_ECRITURE,
        [System.Security.AccessControl.FileSystemRights]::Modify,
        $CI_OI, $NonePF, $Allow
    )
    [void]$acl.AddAccessRule($ruleE)
}

# -----
# 4.3 GDL_LLECTURE : ReadAndExecute (herite)
# -----
if ($entry.GDL_LLECTURE -and $entry.GDL_LLECTURE.Trim() -ne "") {
    $ruleL = New-Object System.Security.AccessControl.FileSystemAccessRule(
        $entry.GDL_LLECTURE,
        [System.Security.AccessControl.FileSystemRights]::ReadAndExecute,
        $CI_OI, $NonePF, $Allow
    )
    [void]$acl.AddAccessRule($ruleL)
}

# -----
# 4.4 GDL_VUE : ReadAndExecute (non herite)
# -----
if ($entry.GDL_VUE -and $entry.GDL_VUE.Trim() -ne "") {
    $ruleV = New-Object System.Security.AccessControl.FileSystemAccessRule(
        $entry.GDL_VUE,
        [System.Security.AccessControl.FileSystemRights]::ReadAndExecute,
        [System.Security.AccessControl.InheritanceFlags]::None,
        $NonePF,
        $Allow
    )
    [void]$acl.AddAccessRule($ruleV)
}

```

```

}

# -----
# 4.5 Comptes administratifs : Modify (herite)
# -----
foreach ($admin in $RWAdmins) {
    $ruleA = New-Object System.Security.AccessControl.FileSystemAccessRule(
        $admin,
        [System.Security.AccessControl.FileSystemRights]::Modify,
        $CI_OI, $NonePF, $Allow
    )
    [void]$acl.AddAccessRule($ruleA)
}

# -----
# 4.6 Application finale des ACL
# -----
Set-Acl -LiteralPath $folderFullPath -AclObject $acl
Write-Host "ACL appliquees : $folderFullPath"

} catch {
    Write-Warning "Erreur ACL sur $folderFullPath -> $_"
}

# Effacer la barre de progression
Write-Progress -Activity "Application ACL" -Completed

Write-Host ""
Write-Host "Application des ACL terminee." -ForegroundColor Green

```

Parfait ! Nous avons à présent mis en place l'AGDLP pour une gestion des droits beaucoup plus fine, facile, et modulable dans le temps.

De plus, ce script s'appuie sur un répertoire racine qui peut être modifié, si jamais une nouvelle branche devait être créée dans le partage.

Revision #5

Created 2025-10-29 12:37:01 UTC

Updated 2026-02-25 15:48:32 UTC by clement-derouet