ی حذف گروپ پالیسی (GPO) های منسوخ شده از SYSVOL با
ل (نسخه PDF)

ش بسیار بسیار کاربردی و عملی قصد داریم نحوه پیدا کردن Orphaned GPO ها را که درون پوشه SYSVOL قرار دارند را به شما عزیزان آموزش سازمان های بزرگ بسـیار قطعا به کمک شما می آید. GPO های اکتیودایرکتوری اگر به درستی نگهـداری نشوند میتوانند از محدوده کنترل ما مخصوصا در سازمان های بزرگ که تعدادی زیادی از افراد میتوانند روی GPO ها دسترسی داشته باشند و تغییرات خود را روی آنها انجام دهند.

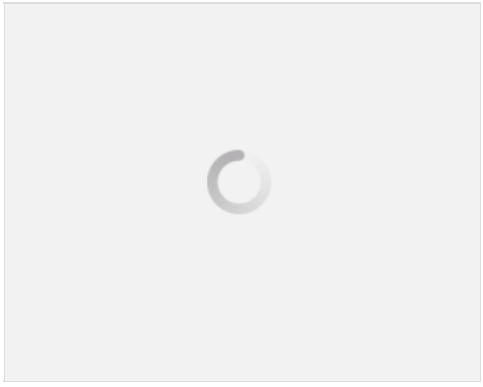
کلاتی که در این گونه مواقع در شـبکه رخ میدهد وجود Orphaned GPO هـا می باشـد. همانطور که در مقالات قبلی نیز اشاره کردیم یک GPO جزء GPT و GPC تشکیل می شود که GPC ها در دیتابیس اکتیودایرکتوری و GPT ها در پوشه SYSVOL Share قرار میگیرند. گاهی اوقات یک ابیس اکتیودایرکتوری پاک می شود و ممکن است در کنسول مـدیریتی GPMC نشان داده نشونـد اما با این وجود در پوشه SYSVOL Share ود دارند در این حالت ما میگوییم که GPO های ما بصورت Orphaned در آمده است.

که کجا و چگونه دیتابیس AD و پوشه SYSVOL را بـا هم مقایسه کنیم به ما کمک شایانی در پیـدا کردن و پاک کردن Orphaned GPO ها می ی بهتر از استفاده از PowerShell ! در ابتـدا ما نیاز داریم که یک لیست از تمام GPO هـای موجود در دیتابیس اکتیودایرکتوری را تهیه کنیم. به ر ما از دسـتور Get-GPO در PowerShell استفاده می کنیم. دستور Get-GPO اطلاعـات مختلفی را به ما میدهـد اما ما فقط به دنبال GUID ها به GUID هـا به این خاطر نیاز داریم که با GUID های درون پوشه SYSVOL مقایسه کنیم. ما GUID ها را بوسیله دستور Get-GPO میتوانیم از یس اکتیودایرکتوری با ریختن Id property در یک String بیرون بکشیم. به دستور زیر توجه کنید :

```
$gpoGuids = Get-GPO -All | Select-Object @{ n='GUID'; e = {$_.Id.ToString()}} | Select-Object -ExpandProperty GUID
```

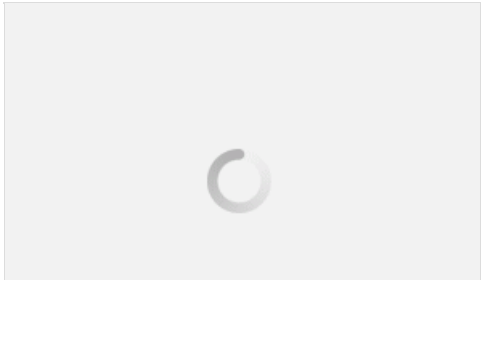
ی Script تمامی GUID های موجود در AD در خروجی نمایش داده می شوند. حالا ما نیاز است تا مسیری را پیدا کنیم که به این GUID ها اشاره GPO بایستی یک پوشه در هر دامین کنترلر داشته باشد که در مسیر زیر قرار دارد :

```
\\<DomainName>\SYSVOL\<DomainName>\Policies
```



شه ، پوشه هایی قرار دارند که با نام GUID ها نامگذاری شده اند و نشان دهنده همه GPO ها در دامین هستند. از آنجا که ما تنها به GUID ها ی پوشه ای به نام PolicyDefinitions را Exclude می کنیم که خود درون پوشه Policies قرار دارد. به دستور زیر توجه کنید :

```
$polFolders = Get-ChildItem \\<DomainName>\SYSVOL\<DomainName>\Policies …Exclude 'PolicyDefinitions' | Select-Object -ExpandProp
```



تور شبیه به تصویر فوق است. حالا بایـد یکی یکی GUID هـا را بـا هم مقایسه کنیم. اسم پوشه ها در انتهای خروجی دسـتور داخل آکولاد قرار
دستور زیر با ایجاد یک متغیر به نام $sysvolGuids آنها را حذف می کنیم. به دستور زیر توجه کنید :

```
$sysvolGuids = @()
foreach ($folder in $polFolders) {
    $sysvolGuids += $folder -replace '{|}', ''
}
```

لیست از GUID هـا داریم که یکی از آنهـا در دیتـابیس اکتیودایرکتوری و دیگری در پوشه SYSVOL قرار دارد. مـا بایـد این دو لیست را با هم
و ببینیم که آیا پوشه SYSVOL ای وجود دارد که در دیتابیس AD وجود نداشته باشد ؟ یکی از این راه ها استفاده از دستور Compare-Object
مانطور که از اسم این دسـتور نیز مشـخص است ما بوسیله این دستور میتوانیم دو لیست را با هم مقایسه کنیم و تفاوت های آنها را دربیاوریم.
وجـود داشت خروجی Script زیر GUID هـا را نشـان خواهـد داد و در اینجاست که میتوانیـد مطمئن شویـد که Orphaned GPO ها در پوشـه
SY دامین کنترلر ها وجود دارد!

```
Compare-Object -ReferenceObject $sysvolGuids -DifferenceObject $gpoGuids | Select-Object -ExpandProperty InputObject
```

ساده تر از این دستورات بتوانید استفاده کنید یک Script آماده کرده ایم که تمامی دستوراتی که تا کنون اجرا کرده ایم را شامل می شود و شما
ی Multi-Domain میتوانید از آن براحتی استفاده کنید :

```
function Get-OrphanedGPO {

    [CmdletBinding()]
    param (
        [Parameter(Mandatory)]
        [string]$ForestName
    )
    try {
        ## Find all domains in the forest
        $domains = Get-AdForest -Identity $ForestName | Select-Object -ExpandProperty Domains

        $gpoGuids = @()
        $sysvolGuids = @()
        foreach ($domain in $Domains) {
            $gpoGuids += Get-GPO -All -Domain $domain | Select-Object @{ n='GUID'; e = {$_.Id.ToString()}} | Select-Object -ExpandProper
            foreach ($guid in $gpoGuids) {
                $polPath = "\\$domain\SYSVOL\$domain\Policies"
                $polFolders = Get-ChildItem $polPath -Exclude 'PolicyDefinitions' | Select-Object -ExpandProperty name
                foreach ($folder in $polFolders) {
                    $sysvolGuids += $folder -replace '{|}'
                }
            }
```

```
        }

        Compare-Object -ReferenceObject $sysvolGuids -DifferenceObject $gpoGuids | Select-Object -ExpandProperty InputObject
    } catch {
        $PSCmdlet.ThrowTerminatingError($_)
    }
}
```

دن Orphaned GPO ها در Forest کافیست که دستور Get-OrphanedGPO -ForestName <ForestName> را اجرا کنید. امیدوارم مورد توجه شما
شد.

یرحسین کریم پور

سرویس های شبکه مایکروسافت وب سایت توسینسو

مطلب اصلی