GESTIONAR PERMISOS NTFS CON POWERSHELL

Los administradores del sistema configuran las listas de control de acceso NTFS `ACL` agregando entradas de control de acceso `ACE` en los servidores de archivos NTFS para implementar un modelo de privilegios mínimos.

TIPOS DE PERMISOS NTFS EN POWERSHELL

Hay permisos NTFS tanto avanzados como básicos. Por ejemplo, puede establecer cada permiso en `Denegar` o `Permitir`.

- `Control Total`: Los usuarios con este permiso pueden modificar, agregar, mover y eliminar archivos y directorios, así como sus propiedades asociadas. Además, los usuarios con este permiso pueden cambiar la configuración de permisos para todos los subdirectorios y archivos.
- `Modificar`: los usuarios con este permiso pueden ver y modificar archivos y propiedades de archivos, incluso agregar y eliminar archivos en un directorio o propiedades de archivo en un archivo.
- `Leer y ejecutar`: los usuarios con este permiso pueden ejecutar archivos ejecutables, incluidos los scripts.
- `Leer`: los usuarios pueden ver archivos, propiedades de archivos y directorios con este permiso.
- `Escribir`: los usuarios con este permiso pueden escribir en un archivo y agregar archivos a los directorios.

Aquí está la lista de permisos avanzados:

- `Atravesar Carpeta` o `Ejecutar Archivo`: Los usuarios con este permiso avanzado pueden navegar a través de carpetas para llegar a otras carpetas o archivos, incluso si no tienen permisos para estos archivos o carpetas. Los usuarios con este permiso avanzado también pueden ejecutar archivos ejecutables. El permiso “Carpeta transversal” surte efecto cuando el usuario o grupo no tiene el derecho “Omitir comprobación transversal” en el complemento de directiva de grupo.
- `Lista de carpetas` o `Leer datos`: los usuarios con este permiso avanzado pueden ver una lista de archivos y subcarpetas dentro de la carpeta y el contenido de los archivos.
- `Leer atributos`: los usuarios con este permiso avanzado pueden ver los atributos de una carpeta o archivo, como si está oculto o es de solo lectura.
- `Escribir atributos`: los usuarios con este permiso avanzado pueden cambiar los atributos de un archivo o carpeta.
- `Leer atributos extendidos`: los usuarios con este permiso avanzado pueden ver los atributos extendidos de una carpeta o archivo, como permisos y tiempos de creación y modificación.
- `Escribir atributos extendidos`: los usuarios con este permiso avanzado pueden cambiar los atributos extendidos de una carpeta o archivo.
- `Crear archivos` o `Escribir datos`: el permiso `Crear archivos` permitirá a los usuarios crear archivos dentro de la carpeta con este permiso avanzado. `Este permiso se aplica solo a las carpetas.` El permiso `Escribir datos` permitirá a los usuarios con este permiso avanzado cambiar el archivo y sobrescribir el contenido existente. Este permiso solo se aplica a los archivos.
- `Crear carpetas` o `Anexar datos`: el permiso `Crear carpetas` permite a los usuarios crear carpetas dentro de una carpeta con este permiso avanzado. `Este permiso se aplica solo a las carpetas.` El permiso `Agregar datos` permitirá a los usuarios con este permiso avanzado realizar cambios al final del archivo, pero no pueden cambiar, sobrescribir ni eliminar datos existentes. Este permiso solo se aplica a los archivos.
- `Eliminar`: los usuarios con este permiso avanzado pueden eliminar la carpeta o el archivo. Si los usuarios no tienen el permiso `Eliminar` en una carpeta o archivo, aún pueden eliminar un objeto si tienen el permiso `Eliminar subcarpetas y archivos` en la carpeta principal.
- `Permisos de lectura`: los usuarios con este permiso avanzado pueden leer los permisos de una carpeta o archivo, como `Control total`, `Leer` y `Escritura`.
- `Cambiar permisos`: los usuarios con este permiso avanzado pueden cambiar los permisos de un archivo o carpeta.

- `Tomar posesión`: los usuarios con este permiso avanzado pueden tomar posesión del archivo o carpeta. El propietario del archivo o la carpeta siempre puede cambiar sus permisos, independientemente de los permisos existentes que protegen el archivo o la carpeta.
- `Sincronizar`: los usuarios con este permiso avanzado pueden utilizar el objeto para la sincronización. Este permiso permitirá que un subproceso espere hasta que el objeto esté en el estado señalado. Este permiso no se presenta en ACL Editor.

Podemos encontrar toda la información sobre estos permisos de usuario ejecutando el siguiente script de PowerShell a continuación:

```
[System.Enum]::GetNames([System.Security.AccessControl.FileSystemRights])
```

Los permisos NTFS pueden ser explícitos o heredados. Los permisos explícitos se configuran individualmente, mientras que los permisos heredados se heredan de la carpeta principal.

La jerarquía de permisos es la siguiente:

- Denegación explícita
- Permitir explícitamente
- Denegación heredada
- Permitir heredado

GET-ACL PARA OBTENER ACL DE CARPETAS Y ARCHIVOS

El primer comando de PowerShell utilizado para administrar los permisos de archivos y carpetas es `Get-Acl`; enumera todos los permisos de objeto.

```
Get-Acl \\fs1\shared\hr | fl
```

Un usuario debe ser propietario de las carpetas de origen y de destino para poder copiar los permisos.

```
Get-Acl \\fs1\shared\hr | Set-Acl \\fs1\shared\hr
```

SET-ACL PARA CONFIGURAR ACL PARA ARCHIVOS Y CARPETAS

El comando PowerShell `Set-Acl` se usa para cambiar el descriptor de seguridad de un elemento específico, como un archivo, una carpeta o una clave de registro; es decir, se utiliza para modificar permisos de archivos o carpetas.

```
$acl = Get-Acl \\fs1\shared\hr
$AccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule("ENTERPRISE\User01","FullControl","Allow")
$acl.SetAccessRule($AccessRule)
$acl | Set-Acl \\fs1\shared\hr
```

PARÁMETRO -REMOVEACCESSRULE PARA ELIMINAR PERMISOS DE USUARIO

```
$acl = Get-Acl \\fs1\shared\hr
$AccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule("ENTERPRISE\User01","FullControl","Allow")
$acl.RemoveAccessRule($AccessRule)
$acl | Set-Acl \\fs1\shared\hr
```

DESHABILITAR O HABILITAR LA HERENCIA DE PERMISOS

Para gestionar una herencia podemos utilizar el método `SetAccessRuleProtection`. El método tiene dos parámetros:

- El primer parámetro es responsable de bloquear la herencia de la carpeta principal. Devuelve estados booleanos: `$true` y `$false`.
- El segundo parámetro se usa si los permisos heredados actuales se eliminan o conservan. También devuelve estados booleanos: `$true` y `$false`.

```
$acl = Get-Acl \\fs1\shared\hr
$acl.SetAccessRuleProtection($true,$false)
$acl | Set-Acl \\fs1\shared\hr
```

Reviertamos este cambio y habilitemos la herencia para la carpeta nuevamente:

```
$acl = Get-Acl \\fs1\shared\hr
$acl.SetAccessRuleProtection($false,$true)
$acl | Set-Acl \\fs1\shared\hr
```

MÉTODO SETOWNER PARA CAMBIAR LA PROPIEDAD DE ARCHIVOS Y CARPETAS EN POWERSHELL

Si queremos establecer un propietario para una carpeta, debe ejecutar el método `SetOwner`.

```
$acl = Get-Acl \\fs1\shared\hr
$object = New-Object System.Security.Principal.Ntaccount("ENTERPRISE\User01")
$acl.SetOwner($object)
$acl | Set-Acl \\fs1\shared\hr
```