

# Thorsten Butz

## Mythos file server

09. November 2018,

Pathé Dietlikon



geekmania  
2018

Gold-Sponsor:



Silver-Sponsor:



Thank You  
geekmania  
2018

about\_me

```
$name = 'Thorsten Butz'
```

```
$uiCulture = 'de-DE'
```

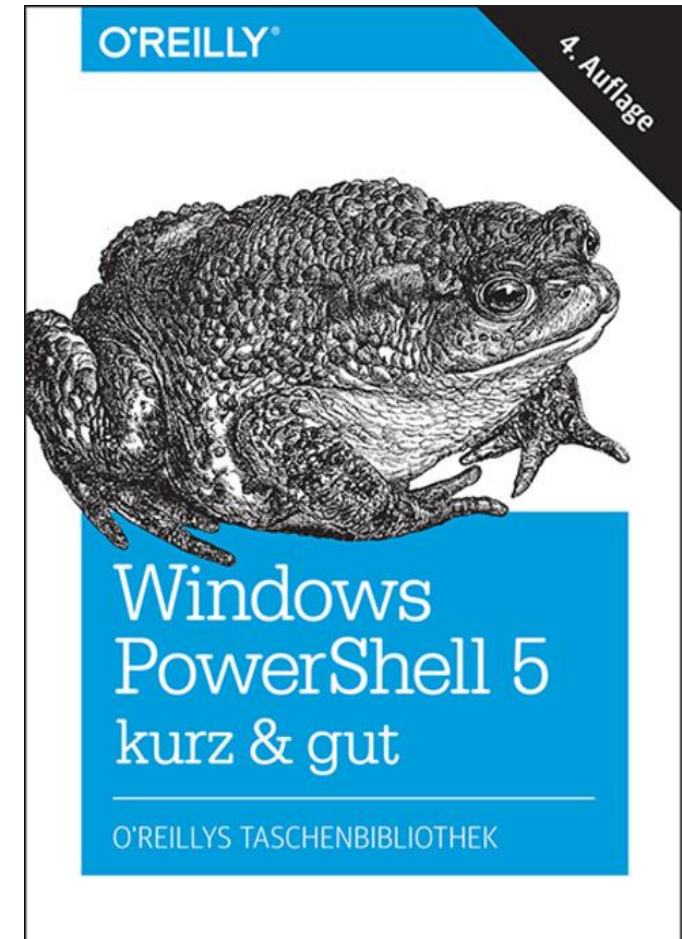
```
$mct -ge 2000
```

```
$focus = 'Scripting', 'OS', 'InterOp'
```

```
$liking = '0.0.0.0/0', '::/0'
```

 = @thorstenbutz

 = [slidingwindows.de/?feed=slw-mp3](https://slidingwindows.de/?feed=slw-mp3)



## List of content

- Episode 1: The untouchables
- Episode 2: Hidden beauties
- Episode 3: Adults only

# #region Episode 1

The untouchables

# The basic stuff: remote administration

The screenshot displays the Windows Server Manager interface. The left-hand navigation pane shows the 'Shares' console selected. The main area shows a list of shares, with 'marketing' selected. A 'New Share Wizard' dialog box is open in the foreground, prompting the user to 'Select the profile for this share'. The wizard shows a list of file share profiles, with 'SMB Share - Quick' selected. A description of this profile is provided on the right side of the wizard.

**Server Manager**

Server Manager ▸ File and Storage Services ▸ Shares

**SHARES**  
All shares | 1 total

Filter

Share	Local Path	Protocol	Availability Type
sea-sv2 (1)			
marketing	C:\marketing	SMB	Not Clustered

**New Share Wizard**

Select the profile for this share

Select Profile

- Share Location
- Share Name
- Other Settings
- Permissions
- Confirmation
- Results

**File share profile:**

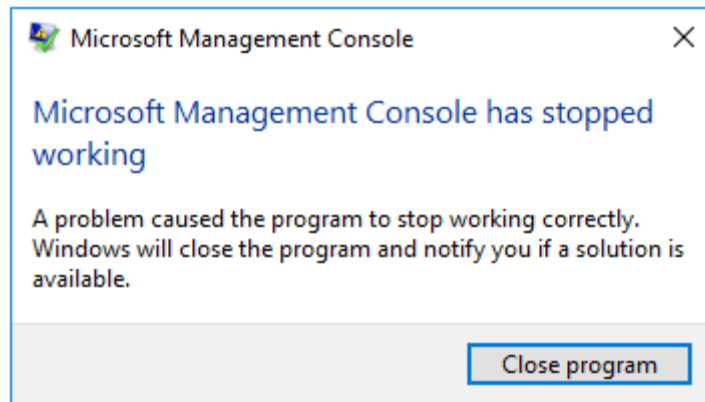
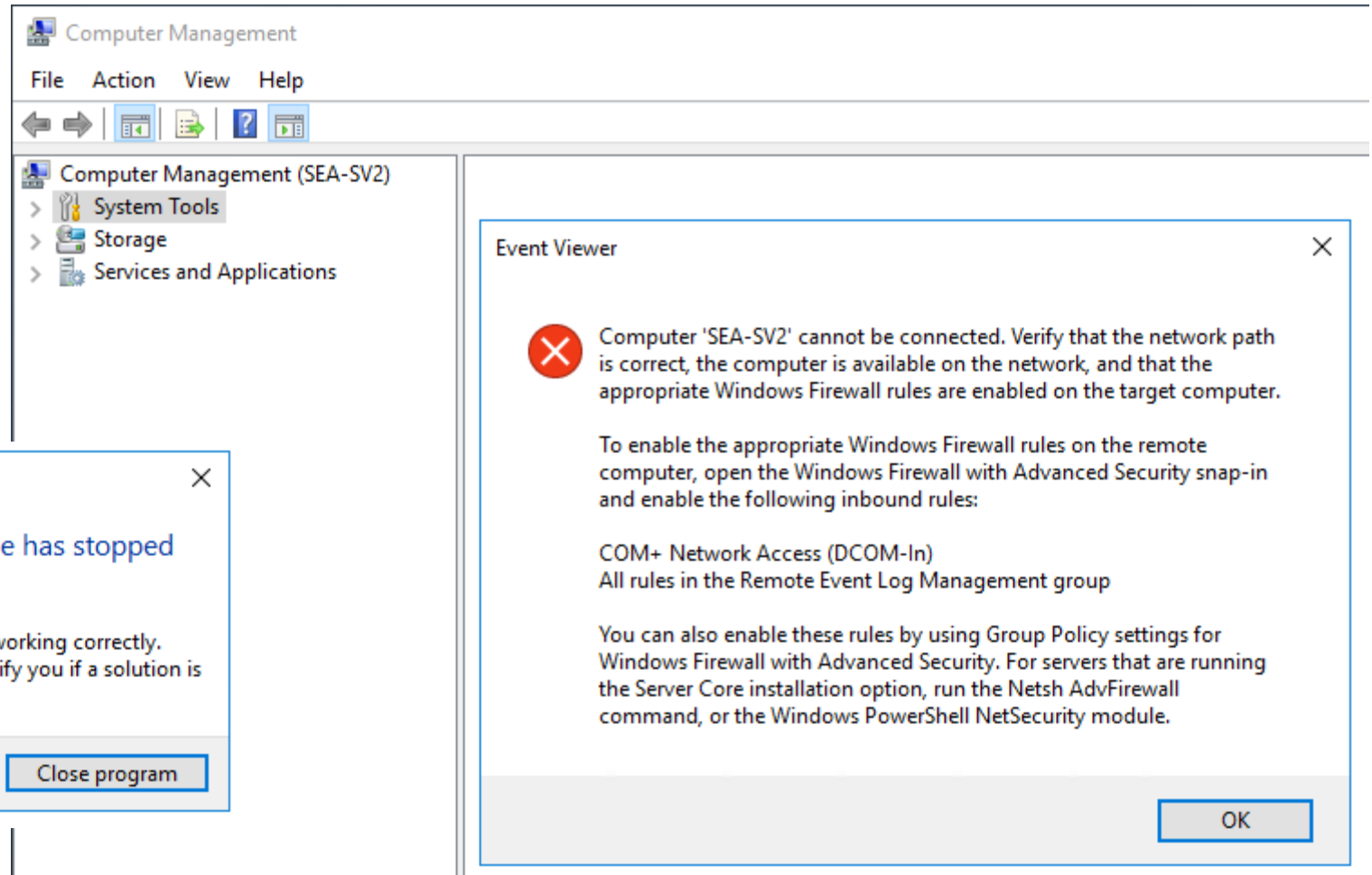
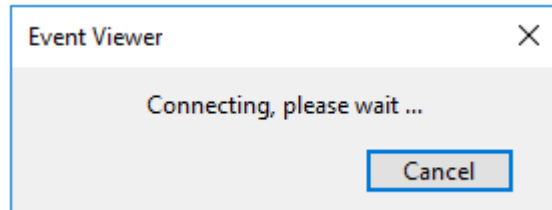
- SMB Share - Quick
- SMB Share - Advanced
- SMB Share - Applications
- NFS Share - Quick
- NFS Share - Advanced

**Description:**

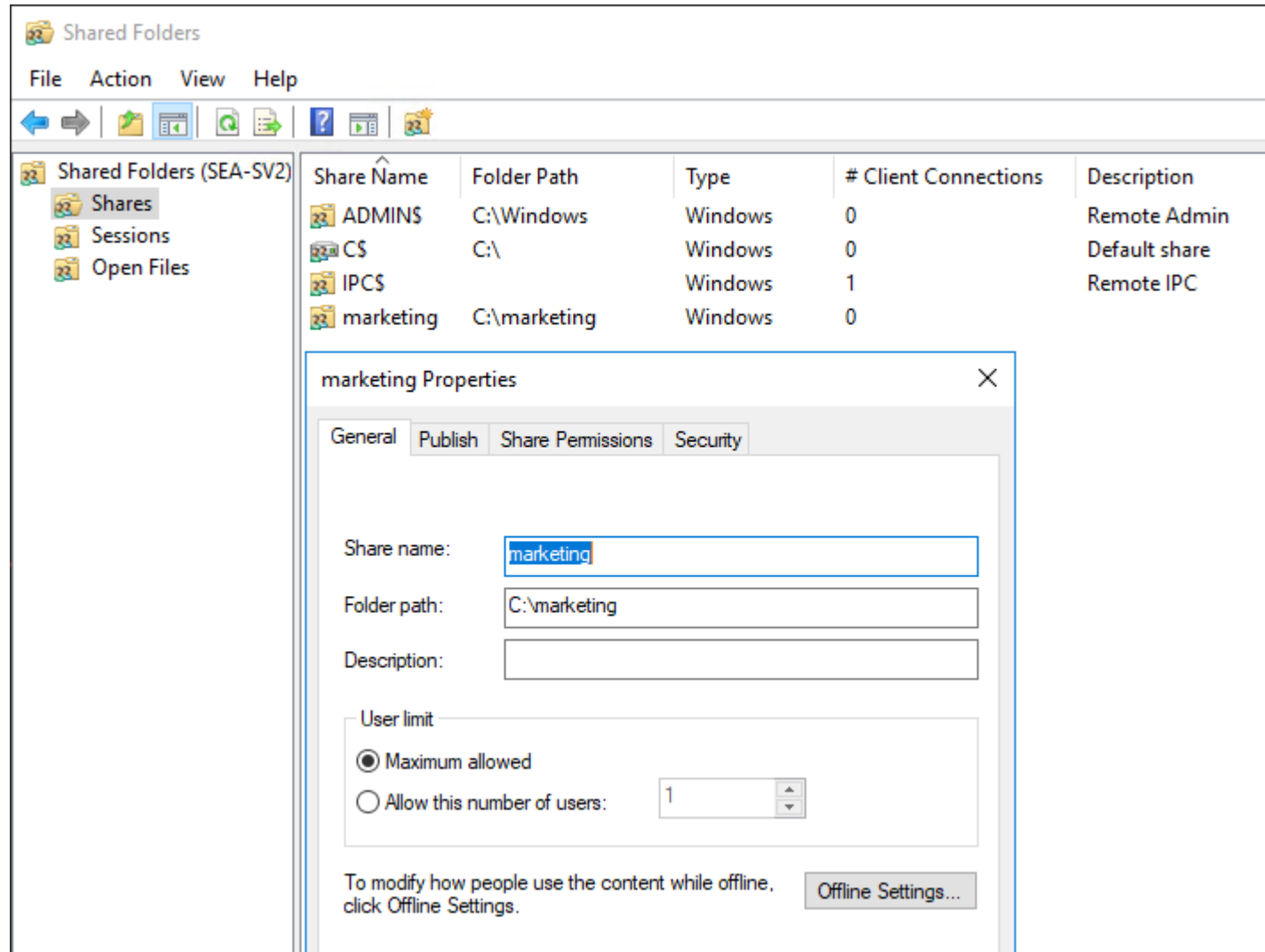
This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog

# Shadows of the past

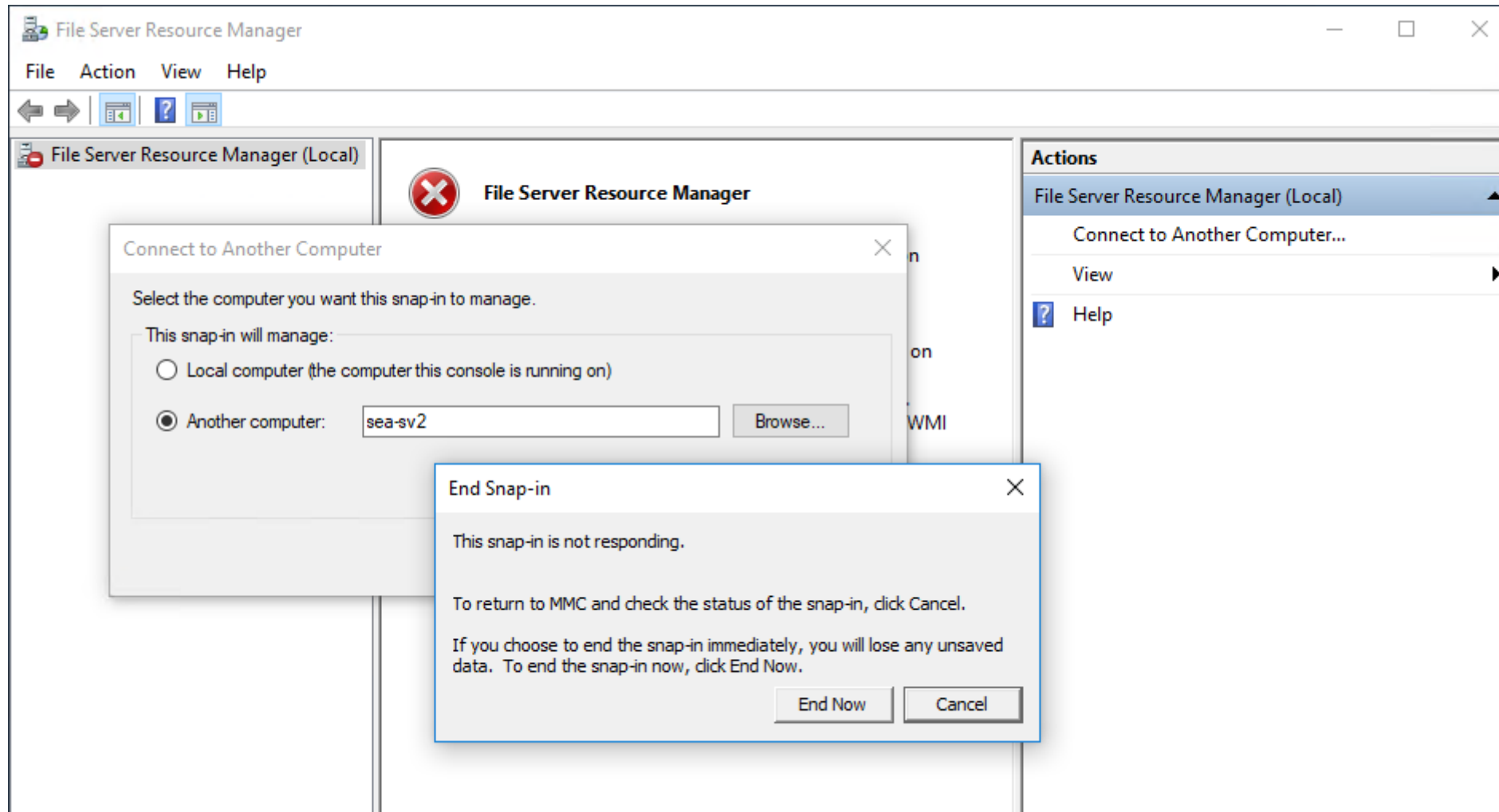


# fsmgmt.msc

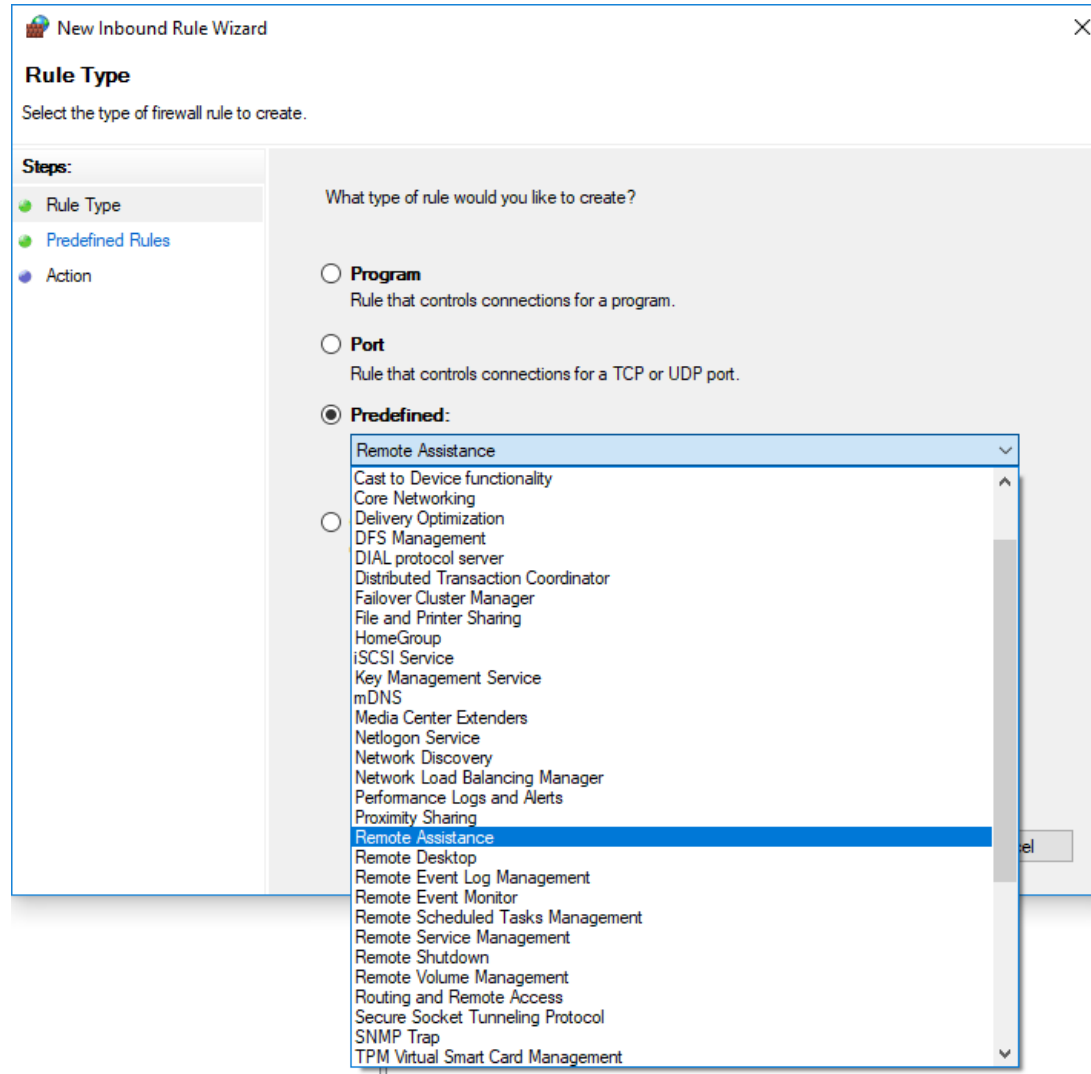




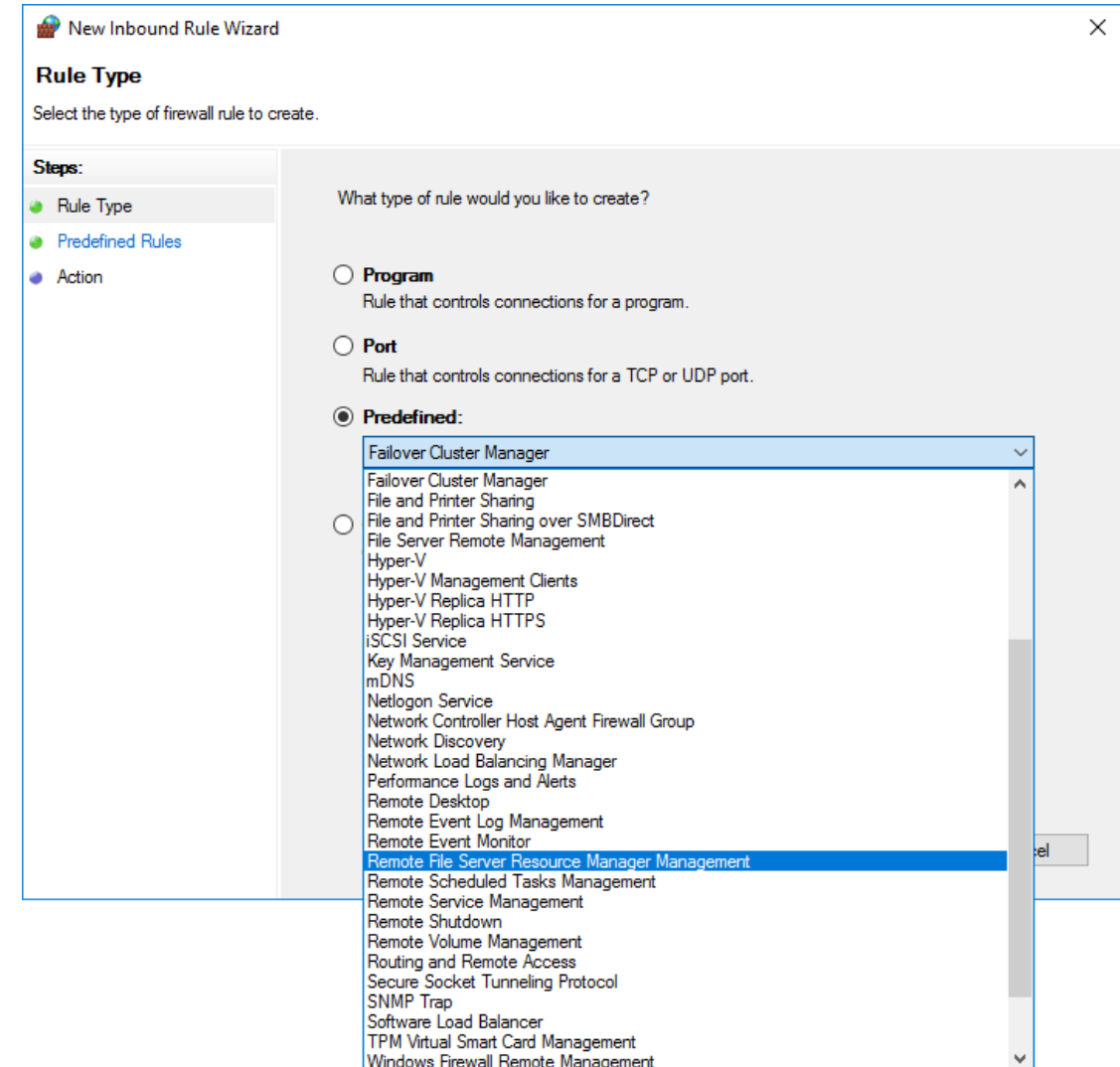
# fsrm.msc



# FSRM feature installed



# FSRM feature not installed





KEEP  
CALM  
IT'S  
DEMO  
TIME

# Firewall rules for FSRM

## Inbound Rules Filtered by: Remote File Server Resource Manager Management

Name	Group	Profile	Enabled	Action	Override
Remote File Server Resource Manager Management - FSRM Reports Service (RPC-In)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management - FSRM Service (RPC-In)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management - Remote Registry (RPC-In)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management - RpcSs (RPC-EPMAP)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management - Task Scheduler (RPC-In)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management - Windows Management Instrumentation (Async-In)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management - Windows Management Instrumentation (WMI-In)	Remote File Server Resource Manager Management	All	No	Allow	No
Remote File Server Resource Manager Management (SMB-In)	Remote File Server Resource Manager Management	All	No	Allow	No

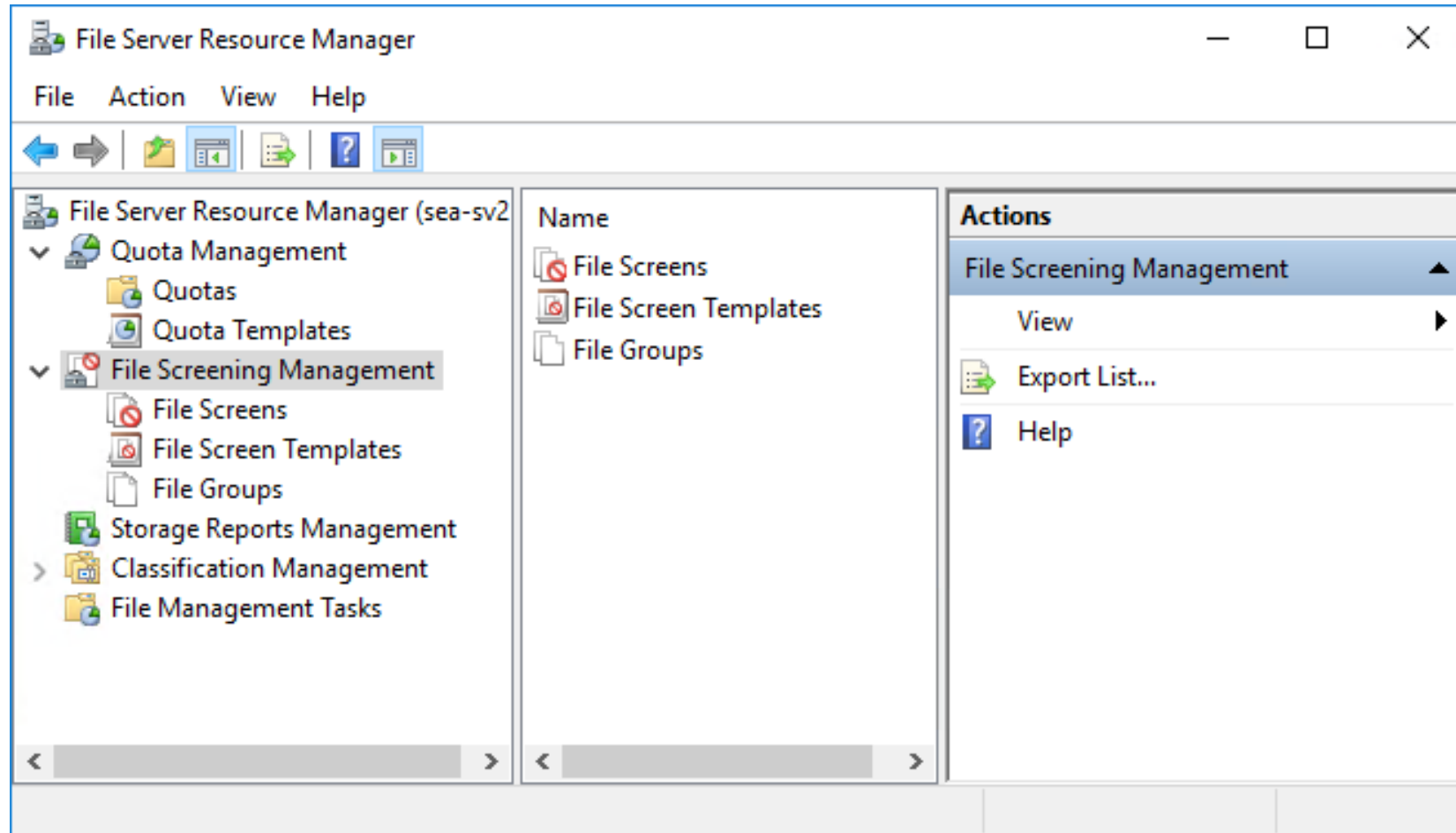
### # Check config

```
$CimSession = New-CimSession -ComputerName $fileserver
$DisplayGroup = 'Remote File Server Resource Manager Management'
Get-NetFirewallRule -DisplayGroup $DisplayGroup -CimSession $CimSession |
    Format-Table Enabled,Display*, *store* -AutoSize
```

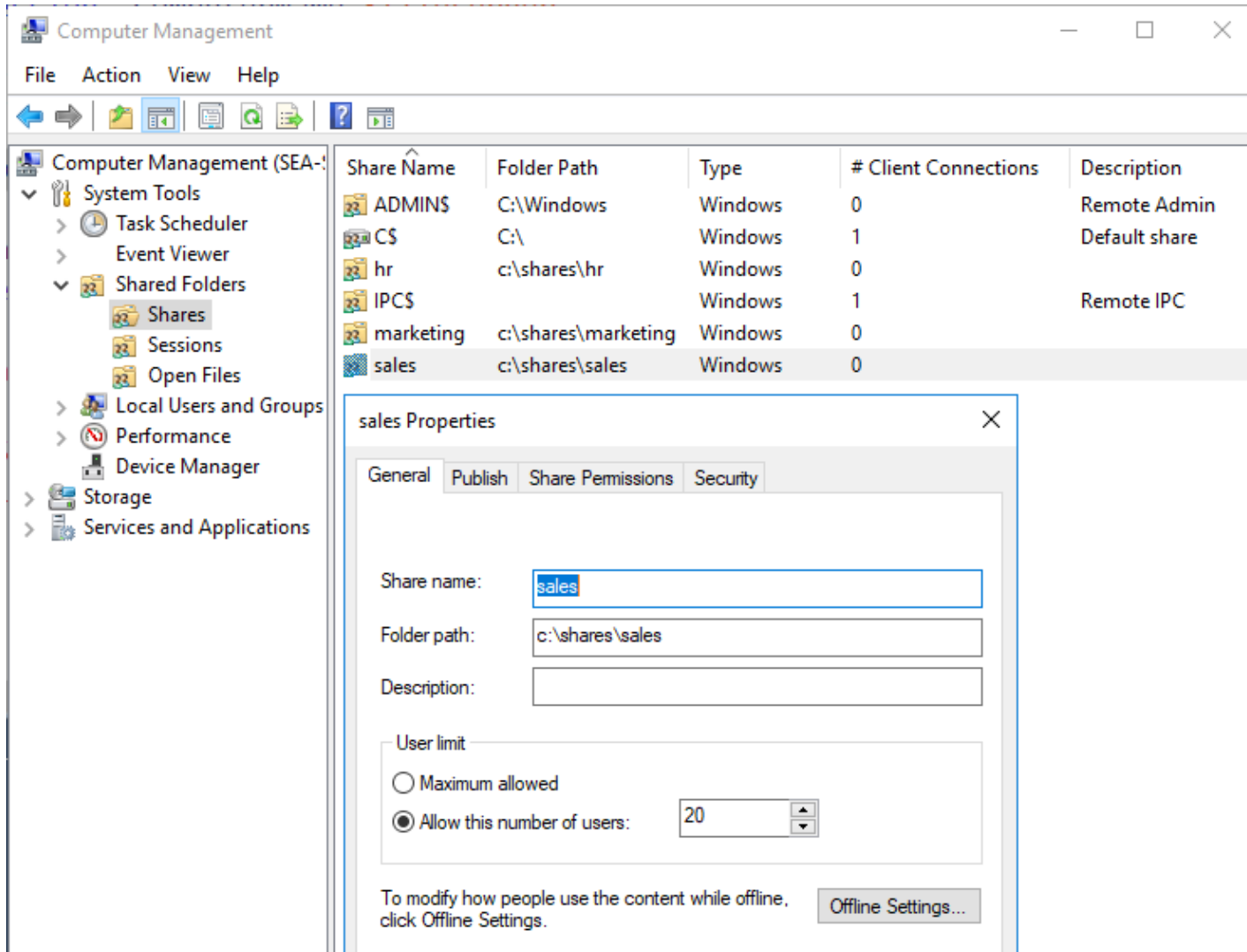
### # Enable rules

```
Get-NetFirewallRule -DisplayGroup $DisplayGroup -CimSession $CimSession |
    Set-NetFirewallRule -Enabled True
```

# Ready for take off



# Sharing and mapping



# A

net.exe use s: <\\sea-fs1\Sales>

# B

New-SmbMapping

-LocalPath 's:'

-RemotePath '\\sea-fs1\sales'

# C

New-PSDrive

-Name 's'

-PSProvider FileSystem

-Root '\\sea-fs1\sales'

# #region Episode 2

Hidden beauties

# Less known NTFS object types



WIKIPEDIA  
The Free Encyclopedia

## NTFS reparse point

---

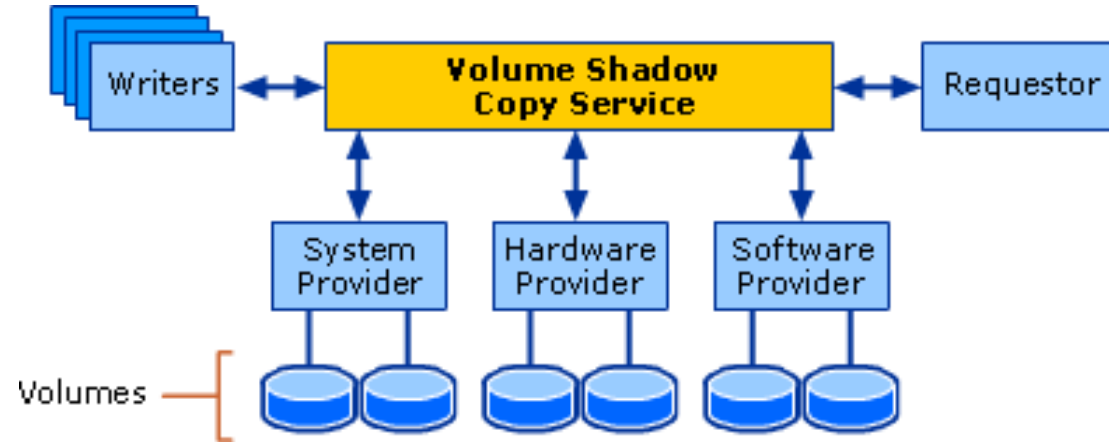
From Wikipedia, the free encyclopedia

An **NTFS reparse point** is a type of **NTFS file system** object. It is available with the NTFS v3.0 found in **Windows 2000** or later versions. Reparse points provide a way to extend the NTFS filesystem. A reparse point contains a reparse tag and data that are interpreted by a filesystem filter identified by the tag. Microsoft includes several default tags including **NTFS symbolic links**, **directory junction points** and **volume mount points**. Also, reparse points are used as placeholders for files moved by Windows 2000's **Hierarchical Storage System**. They also can act as **hard links**, but aren't limited to point to files on the same volume: they can point to directories on any local volume.<sup>[1]</sup>

[https://en.wikipedia.org/wiki/NTFS\\_reparse\\_point](https://en.wikipedia.org/wiki/NTFS_reparse_point)



# Volume Shadow Copy Service



```
vssadmin.exe list shadows
```

```
vssadmin create shadow /for=c:
```

```
mklink /D C:\vss \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\
```

```
vssadmin delete shadows /all
```

MSDN:

"The Volume Shadow Copy Service (VSS) is a set of COM interfaces that implements a framework to allow volume backups to be performed while applications on a system continue to write to the volumes.

VSS is supported on Microsoft Windows XP and later."

# HardLinks, Symlinks/Softlinks

- Hardlinks (files)  
Can be used in file shares, cannot cross volume borders
- Junctions (directories)  
Can be used in file shares, can cross volume borders
- Softlinks  
Cannot be used in file shares, can cross volume borders

# HardLinks, Symlinks/Softlinks

	Hardlinks (file)	Junctions (directory)	Symlinks (file)	Symlinks (directory)
Can be used in shared folders	YES	YES	NO	NO
Can point from one volume to another	NO	YES	YES	YES

## Problem statement:

- Weird differences throughout different OS version
- Strange collection of (built-in) tools, lacking functionality
- Generally not "popular" in Windows

# Why do Hardlinks/Symlinks exist?

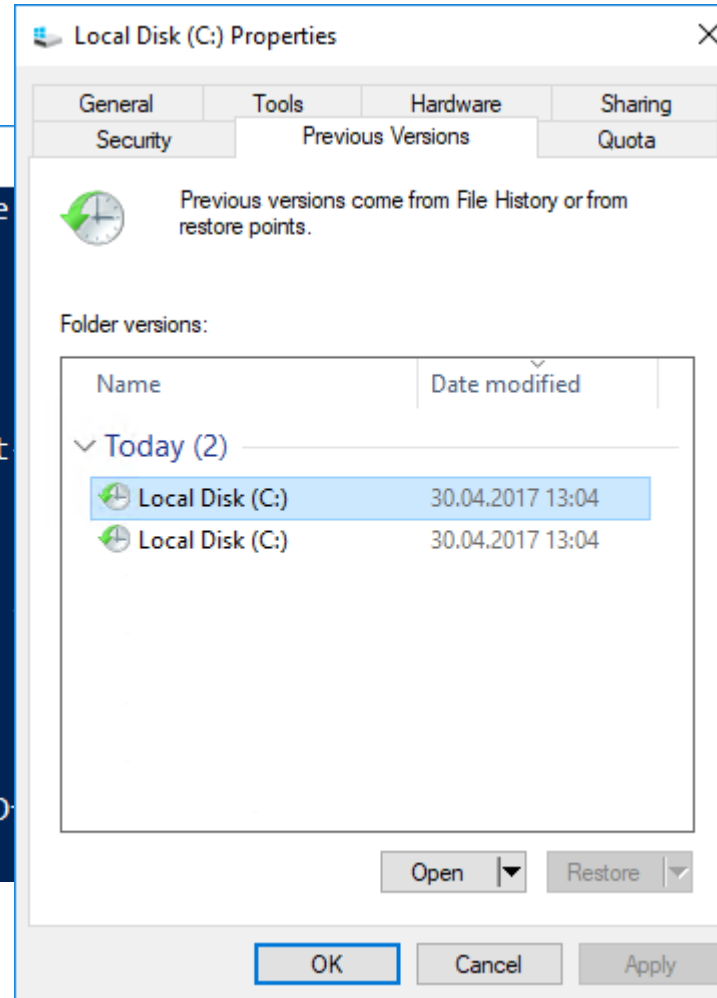
```
powershell.exe

PS C:\> Get-ChildItem C:\Windows\explorer.exe

FullName : C:\Windows\explorer.exe
LinkType  : HardLink
Mode      : -a----
Target    : {C:\Windows\WinSxS\amd64_microsoft

PS C:\> Get-ChildItem -Path C:\Windows -File
Linktype

Count Name          Group
-----
57882 HardLink      {bfsvc.exe, D
```



```
Target

5063.0_none_62c8804bb28b2827\explorer.exe}

Where-Object { $_.LinkType } | Group-Object
..}
```

# #region Episode 3

Adults only

# UAC trouble

- Protected Administrator

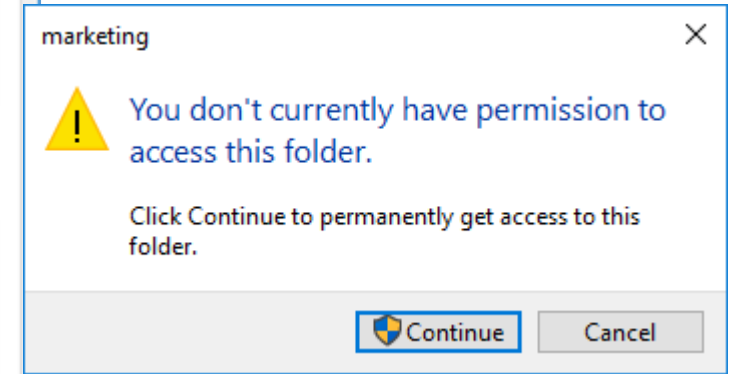
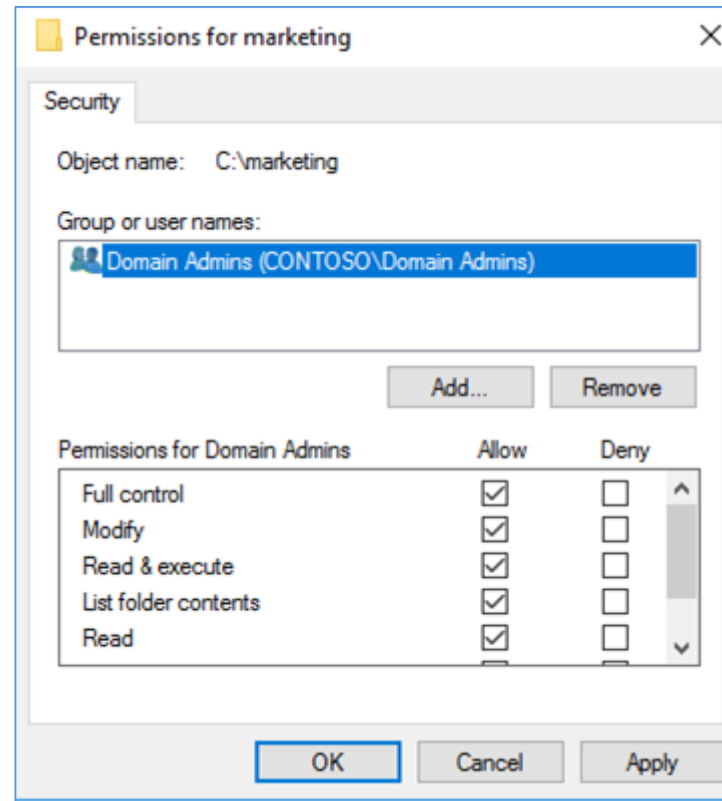


- Standard mode

- Elevated mode

(Run as Administrator)

- Standard User Account

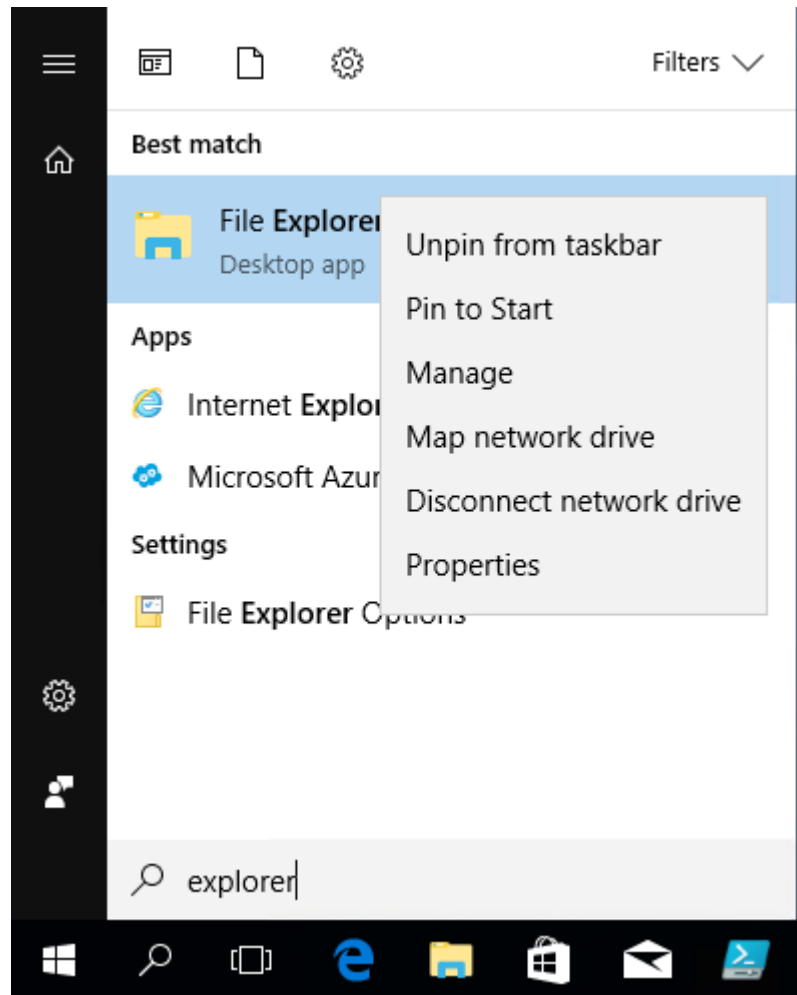


```
powershell.exe
PS C:\> whoami /groups /fo csv | ConvertFrom-Csv | Where-Object { $_.Attributes -like '*deny*' }

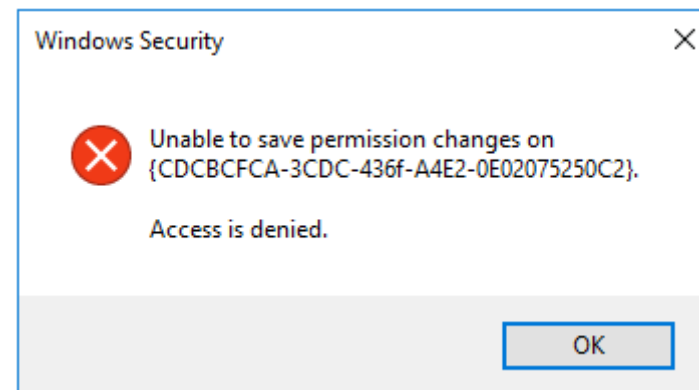
Group Name          Type  SID                               Attributes
-----
BUILTIN\Administrators Alias S-1-5-32-544                     Group used for deny only
CONTOSO\Domain Admins Group S-1-5-21-807576472-1908576611-259626709-512 Group used for deny only
```



# Trouble again with UAC



- Very sophisticated:  
Running Windows Explorer elevated
- Requires Registry-Change  
HKEY\_CLASSES\_ROOT\AppID\{CDCBCFCA-3CDC-436f-A4E2-0E02075250C2}\RunAs
- Owner of the RegKey: "TrustedInstaller"



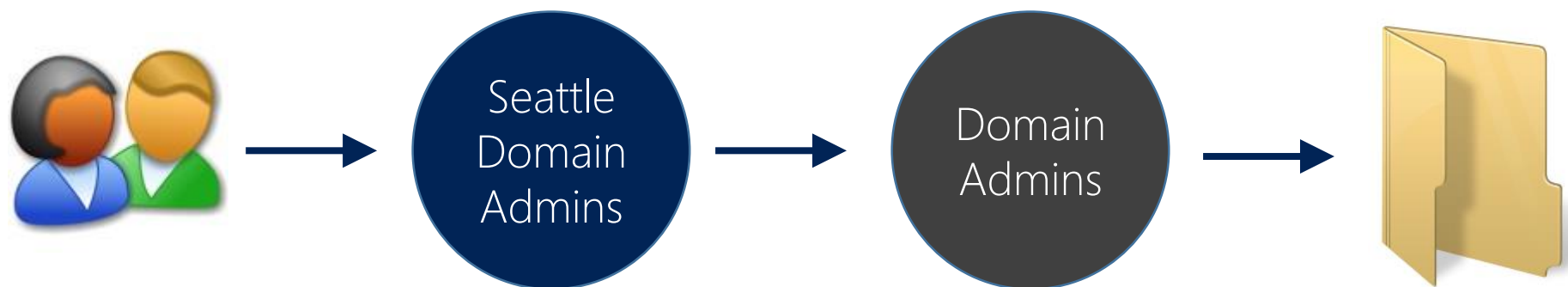


KEEP  
CALM  
IT'S  
DEMO  
TIME



## Avoiding the glitches

- **Always** (!) use your own groups to grant distinct permissions
- Simplify your life:



Permission Entry for Marketing

Principal: Seattle Domain Admins (CONTOSO\Seattle Domain Admins) [Select a principal](#)

Type: Allow

Applies to: This folder, subfolders and files

Basic permissions:

- ☒ Full control
- ☒ Modify
- ☒ Read & execute
- ☒ List folder contents
- ☒ Read
- ☒ Write
- ☐ Special permissions

☐ Only apply these permissions to objects and/or containers within this container

```
icaccls.exe $fileshareroot /grant "$SeattleAdmins`:(OI)(CI)(F)"
```

```
# (OI) Object inherit
```

```
# (CI) Container inherit
```

Permission Entry for Marketing

Principal: London Domain Admins (CONTOSO\London Domain Admins) [Select a principal](#)

Type: Allow

Applies to: This folder and subfolders

Basic permissions:

- ☒ Full control
- ☒ Modify
- ☒ Read & execute
- ☒ List folder contents
- ☒ Read
- ☒ Write
- ☐ Special permissions

☐ Only apply these permissions to objects and/or containers within this container

Permission Entry for Marketing

Principal: Vancouver Domain Admins (CONTOSO\Vancouver Domain Admins)

Type: Allow

Applies to: This folder only

Basic permissions:

- ☒ Full control
- ☒ Modify
- ☒ Read & execute
- ☒ List folder contents
- ☒ Read
- ☒ Write
- ☐ Special permissions

☐ Only apply these permissions to objects and/or containers within this container

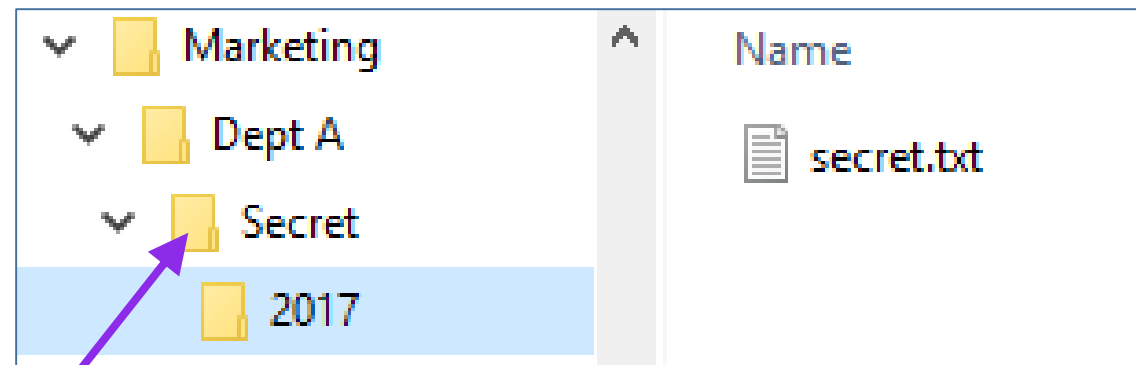
```
icaccls.exe $fileshareroot /grant "$LondonAdmins`:(CI)(F)"
```

```
icaccls.exe $fileshareroot /grant "$VancouverAdmins`:(F)"
```

# Implicit deny vs. implicit grant

ICACLS preserves the canonical ordering of ACE entries:

1. Explicit denials
2. Explicit grants
3. Inherited denials
4. Inherited grants



```
icaccls.exe ".\Secret\" /deny "$user`:(OI)(CI)(F)"
```

```
icaccls.exe ".\Secret\2017\secret.txt" /grant "$user`:(F)"
```

# SeBackupPrivilege

```
Administrator: powershell.exe
PS C:\> Get-ChildItem 'C:\System Volume Information'
Get-ChildItem : Access to the path 'C:\System Volume Information' is denied.
At line:1 char:1
+ Get-ChildItem 'C:\System Volume Information'
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\System Volume Information:String) [Get-ChildItem], UnauthorizedAccessExcept
ion
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

PS C:\> Set-TokenPrivilege -Privilege SeBackupPrivilege
True
PS C:\> Get-ChildItem 'C:\System Volume Information'

Directory: C:\System Volume Information

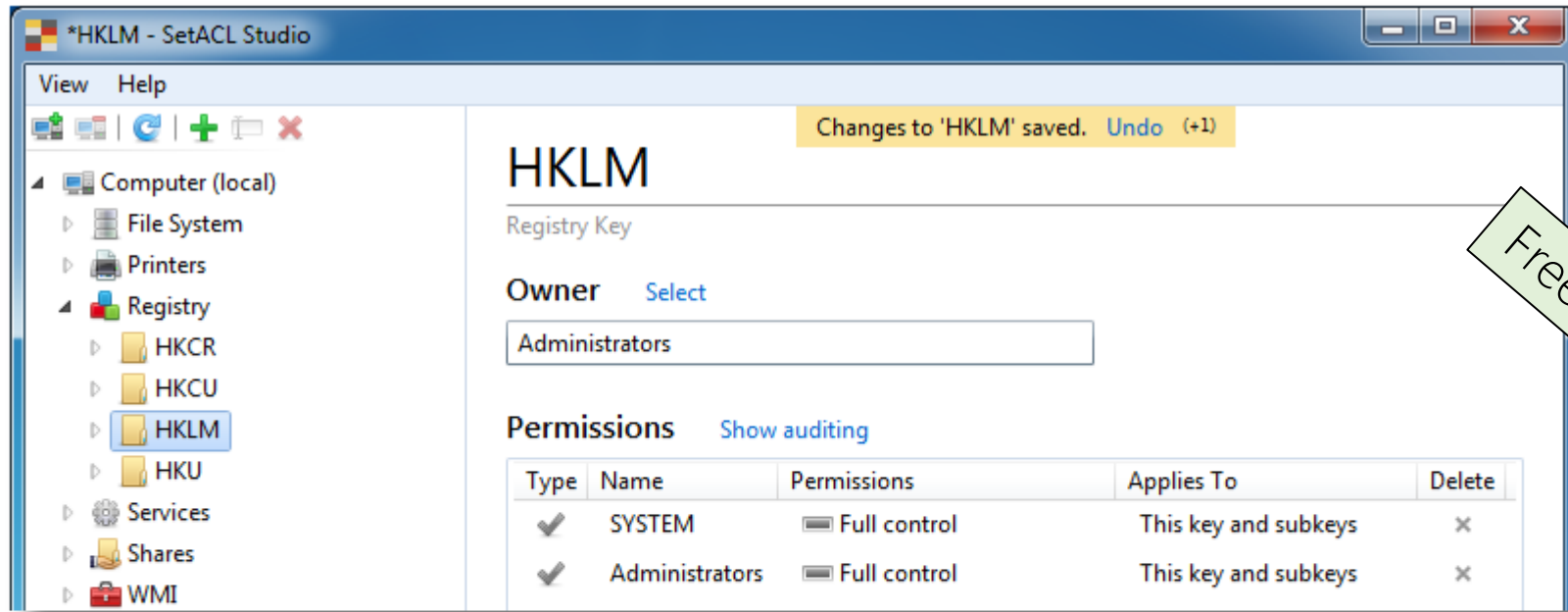
Mode                LastWriteTime         Length Name
----                -
d-----         29.04.2017        18:44           Windows Backup
-a-----         19.04.2017        10:18           76 IndexerVolumeGuid
-a-----         19.04.2017        10:18           12 WPSettings.dat
```

<http://www.leeholmes.com/blog/2010/09/24/adjusting-token-privileges-in-powershell/>

# Wrap up!

- Remote administration is possible .. but awkward
- Not a single solution is feature complete  
(icacls.exe, takeown.exe, Get-ACL/Set-ACL ..)
- No reason to disable UAC, use your own groups!

## Tip: SetACL Studio by Helge Klein



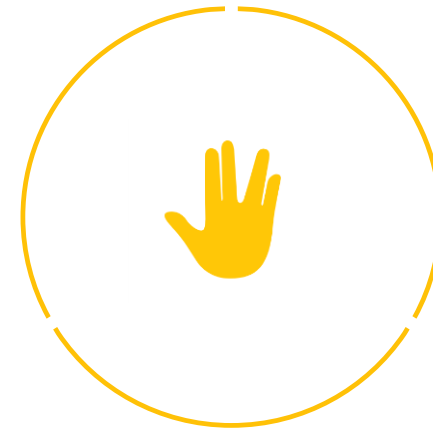
### Permissions minus Complexity

Intuitive permission management with the power of SetACL.  
Less clicks, no more UAC prompts, increased productivity.

Gold-Sponsor:



Silver-Sponsor:



Thank you  
geekmania  
2018