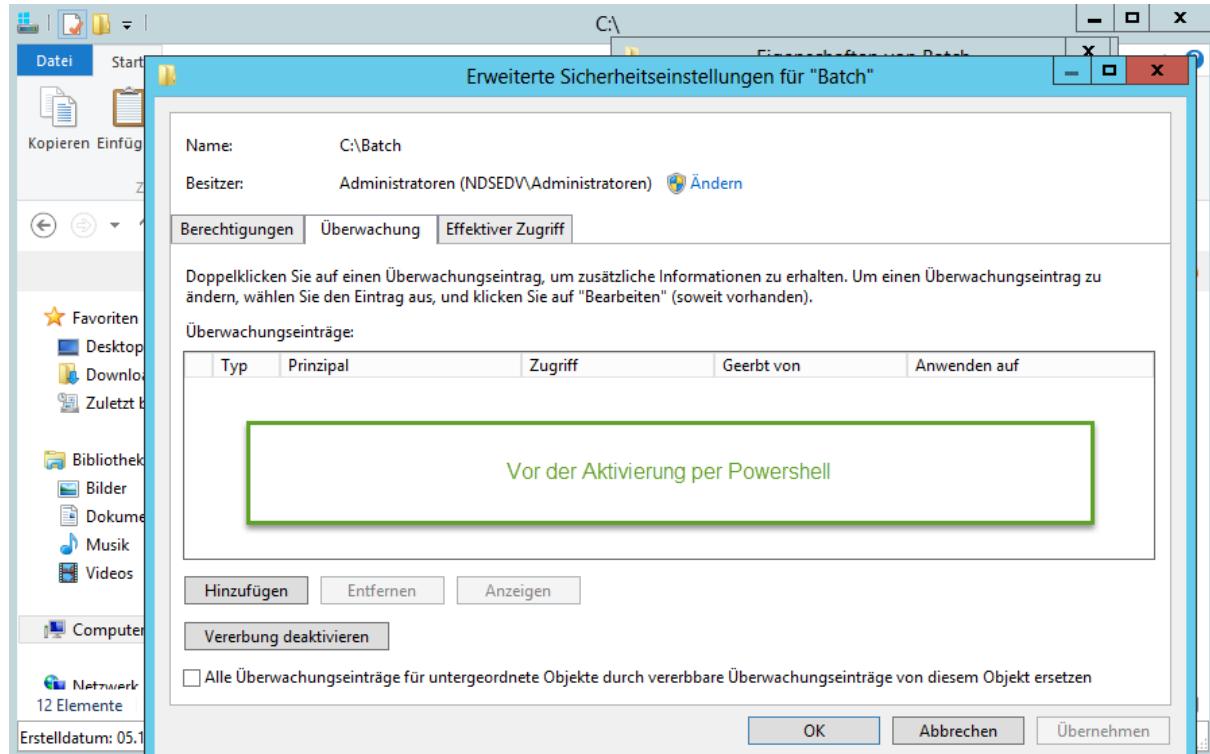


Server 2012 R2 - Auditing per Powershell aktivieren

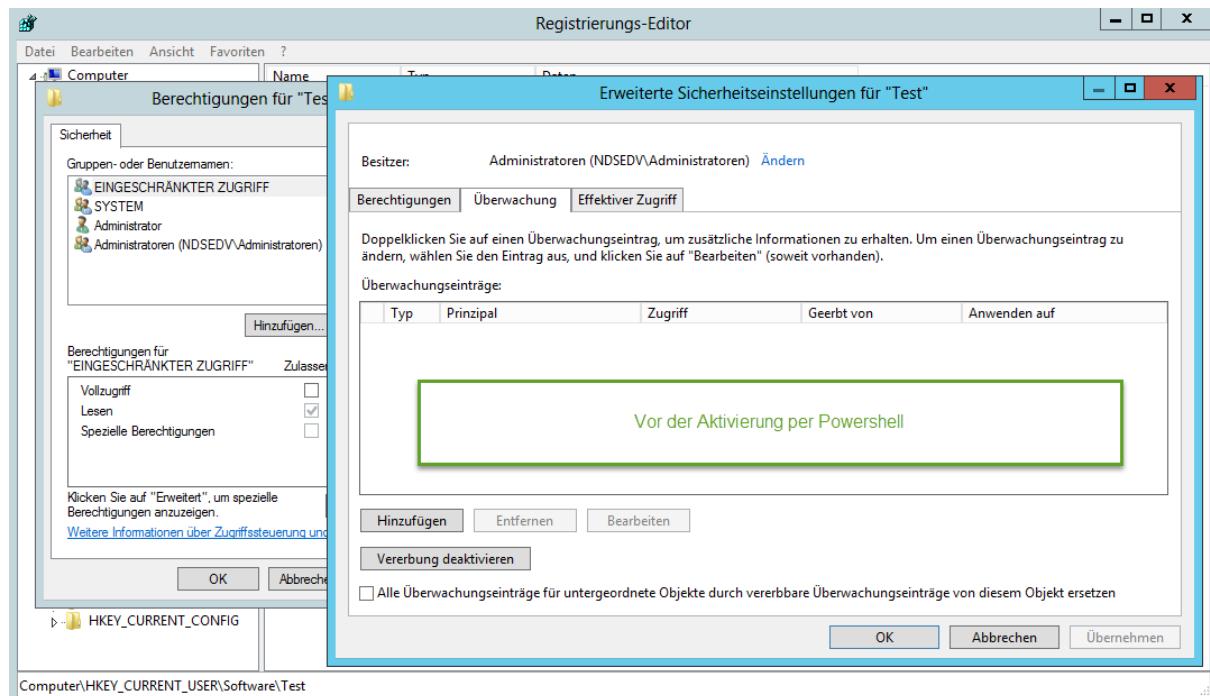
In dieser Anleitung möchte ich euch zeigen wie ich das Auditing auf über 300 Servern aktiviert habe. PCI-DSS fordert die Überwachung diverser Verzeichnisse und Registry Einträge.

Die beiden Screenshots zeigen die Einstellungen vor der Ausführung des Powershell Skripts.

Verzeichnisse vorher:

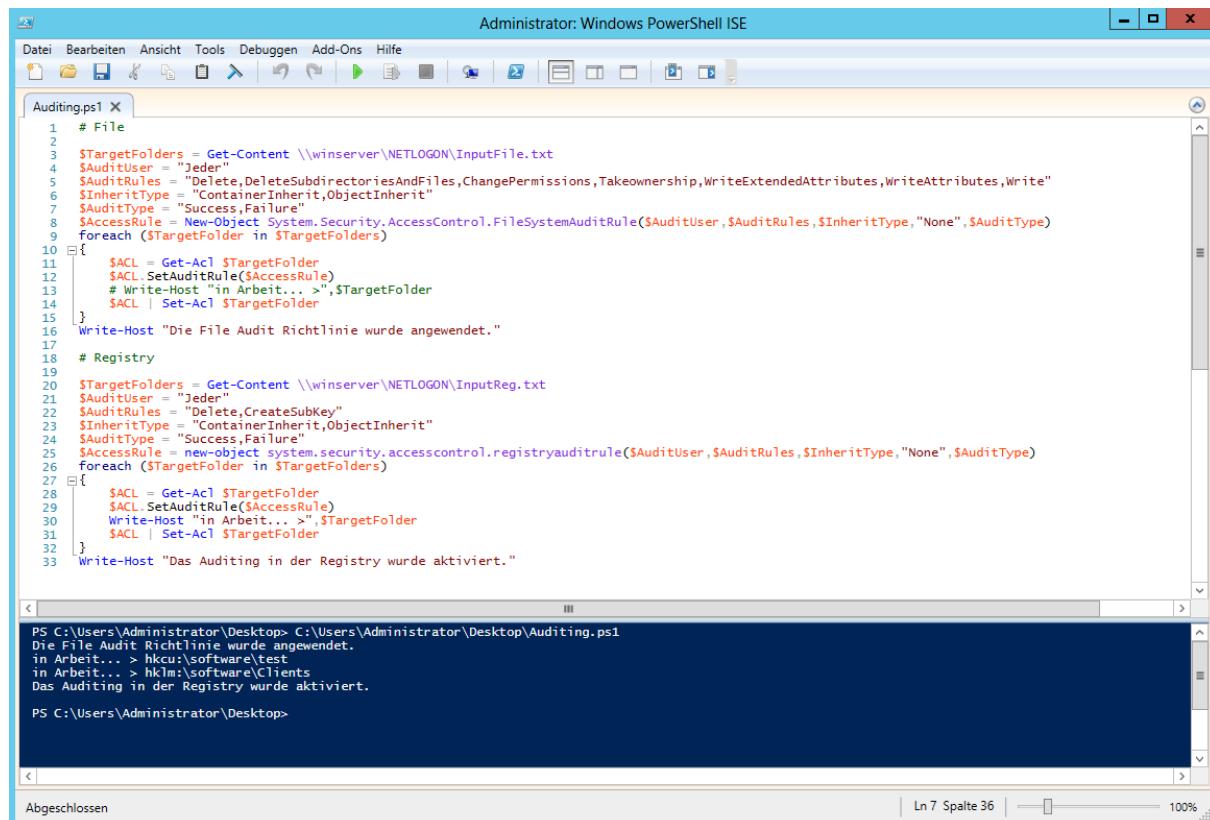


Registry vorher:



Server 2012 R2 - Auditing per Powershell aktivieren

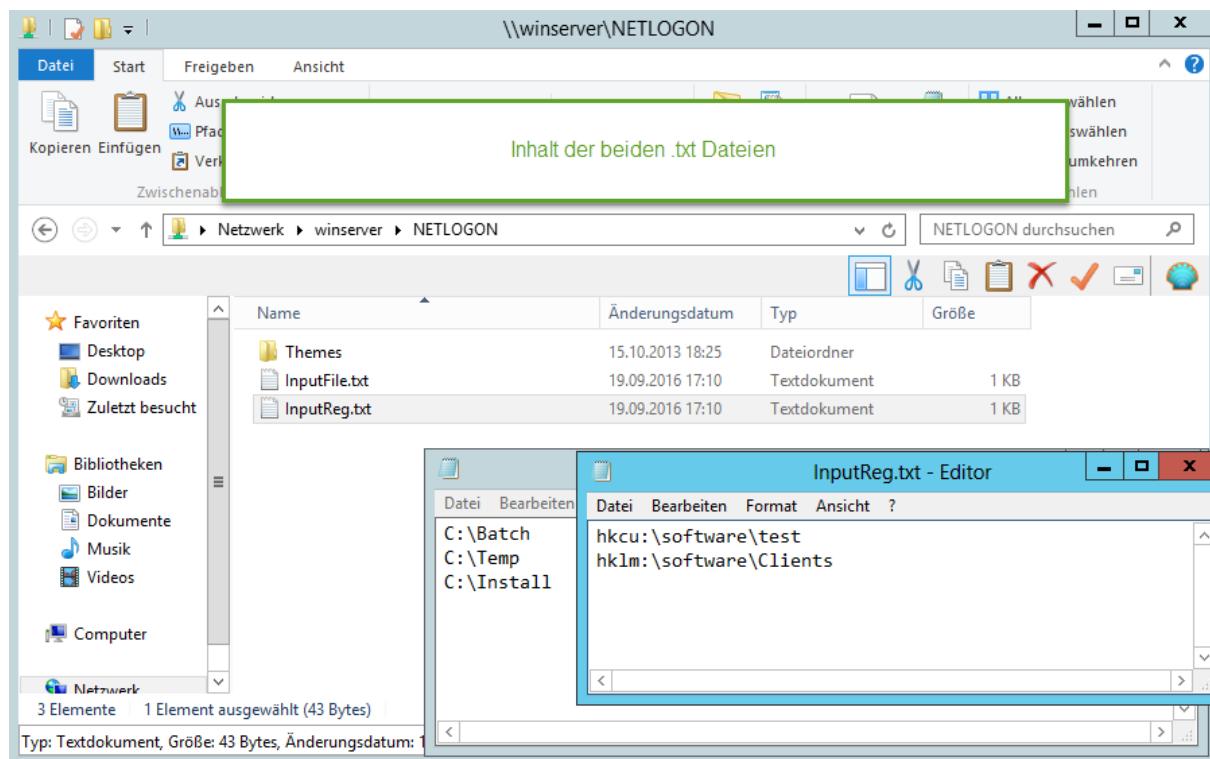
Dieses Powershell Skript aktiviert das Auditing mithilfe von editierbaren .txt Dateien und bietet somit die nötige Flexibilität. Die Audit Rules sind entsprechend der persönlichen Bedürfnisse anzupassen.



The screenshot shows the Windows PowerShell ISE interface. The code editor window contains the PowerShell script `Auditing.ps1`. The script performs two main tasks: auditing files and auditing registry keys. It uses `Get-Content` to read configuration from `\winserver\NETLOGON\InputFile.txt` and `\winserver\NETLOGON\InputReg.txt`. It then creates `FileSystemAuditRule` objects and applies them to target folders and registry keys using `Set-Acl`. The PowerShell window below shows the output of the script's execution, confirming the application of audit rules to specific registry keys like `hkcu:\software\test` and `hklm:\software\Clients`.

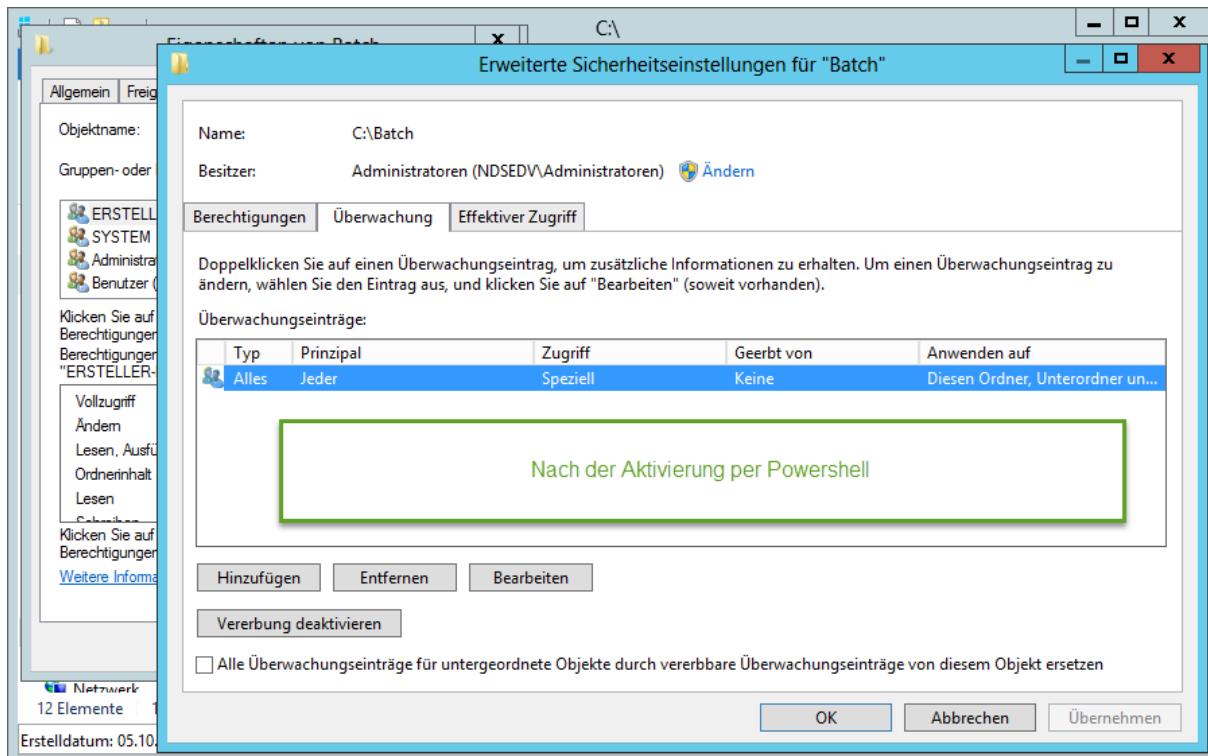
```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Auditing.ps1 X
1 # File
2
3 $TargetFolders = Get-Content \\winserver\NETLOGON\InputFile.txt
4 $AuditUser = "Jeder"
5 $AuditRules = "Delete,DeleteSubdirectoriesAndFiles,ChangePermissions,TakeOwnership,WriteExtendedAttributes,WriteAttributes,Write"
6 $InheritType = "ContainerInherit,ObjectInherit"
7 $AuditType = "Success,Failure"
8 $AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,$AuditRules,$InheritType,"None",$AuditType)
9 foreach ($TargetFolder in $TargetFolders)
10 {
11     $SACL = Get-Acl $TargetFolder
12     $SACL.SetAuditRule($AccessRule)
13     # Write-Host "in Arbeit... >",$TargetFolder
14     $SACL | Set-Acl $TargetFolder
15 }
16 Write-Host "Die File Audit Richtlinie wurde angewendet."
17
18 # Registry
19
20 $TargetFolders = Get-Content \\winserver\NETLOGON\InputReg.txt
21 $AuditUser = "Jeder"
22 $AuditRules = "Delete,CreateSubKey"
23 $InheritType = "ContainerInherit,ObjectInherit"
24 $AuditType = "Success,Failure"
25 $AccessRule = new-object system.security.accesscontrol.registryauditrule($AuditUser,$AuditRules,$InheritType,"None",$AuditType)
26 foreach ($TargetFolder in $TargetFolders)
27 {
28     $SACL = Get-Acl $TargetFolder
29     $SACL.SetAuditRule($AccessRule)
30     Write-Host "in Arbeit... >",$TargetFolder
31     $SACL | Set-Acl $TargetFolder
32 }
33 Write-Host "Das Auditing in der Registry wurde aktiviert."
PS C:\Users\Administrator\Desktop> C:\Users\Administrator\Desktop\Auditing.ps1
Die File Audit Richtlinie wurde angewendet.
in Arbeit... > hkcu:\software\test
in Arbeit... > hklm:\software\Clients
Das Auditing in der Registry wurde aktiviert.
PS C:\Users\Administrator\Desktop>
```

Aufbau und Inhalt der .txt Dateien

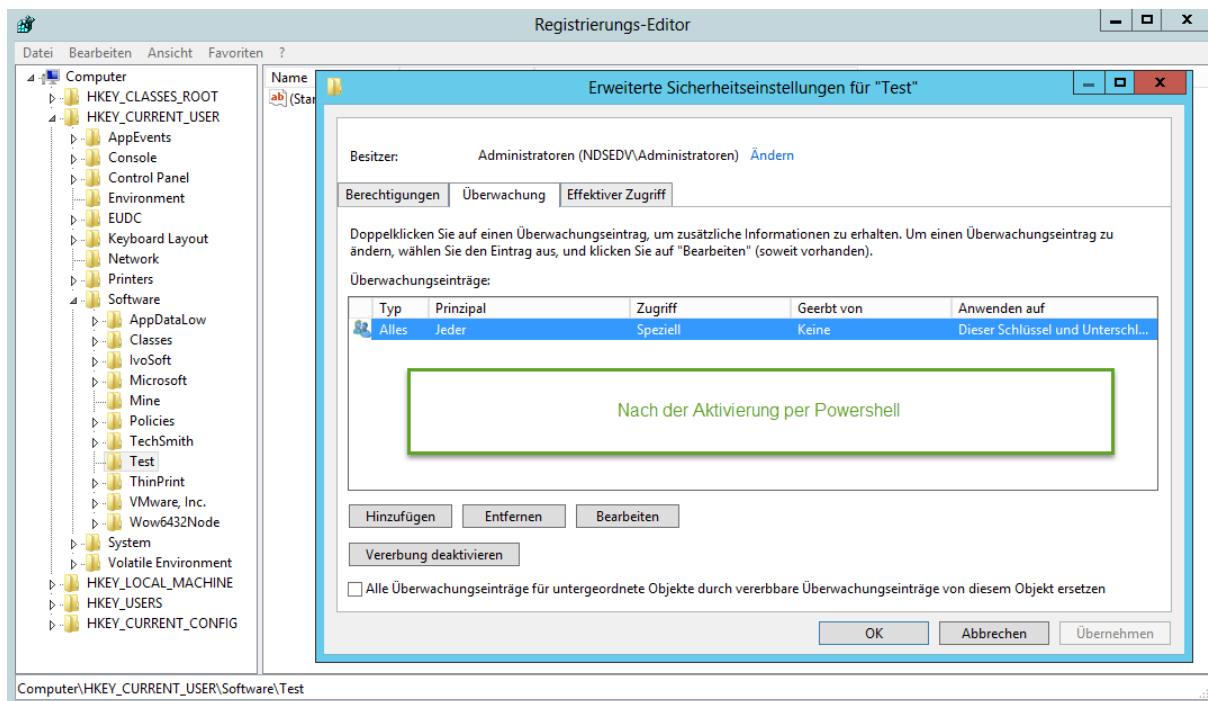


Server 2012 R2 - Auditing per Powershell aktivieren

Das Ergebnis auf Verzeichnis-Ebene:



Das Ergebnis des Registry-Schlüssels TEST:



Server 2012 R2 - Auditing per Powershell aktivieren

```
# File

$TargetFolders = Get-Content \\winserver\NETLOGON\InputFile.txt
$AuditUser = "Jeder"
$AuditRules =
"Delete,DeleteSubdirectoriesAndFiles,ChangePermissions,Takeownership,WriteExtendedAttributes,WriteAttributes,Write"
$InheritType = "ContainerInherit,ObjectInherit"
$AuditType = "Success,Failure"
$AccessRule = New-Object
System.Security.AccessControl.FileSystemAuditRule($AuditUser,$AuditRules,$InheritType,"None",$AuditType)
foreach ($TargetFolder in $TargetFolders)
{
    $ACL = Get-Acl $TargetFolder
    $ACL.SetAuditRule($AccessRule)
    # Write-Host "in Arbeit... >",$TargetFolder
    $ACL | Set-Acl $TargetFolder
}
# Write-Host "Die File Audit Richtlinie wurde angewendet."

# Registry

$TargetFolders = Get-Content \\winserver\NETLOGON\InputReg.txt
$AuditUser = "Jeder"
$AuditRules = "Delete>CreateSubKey"
$InheritType = "ContainerInherit,ObjectInherit"
$AuditType = "Success,Failure"
$AccessRule = new-object
System.Security.accesscontrol.registryauditrule($AuditUser,$AuditRules,$InheritType,"None",$AuditType)
foreach ($TargetFolder in $TargetFolders)
{
    $ACL = Get-Acl $TargetFolder
    $ACL.SetAuditRule($AccessRule)
    write-Host "in Arbeit... >",$TargetFolder
    $ACL | Set-Acl $TargetFolder
}
# Write-Host "Das Auditing in der Registry wurde aktiviert."
```