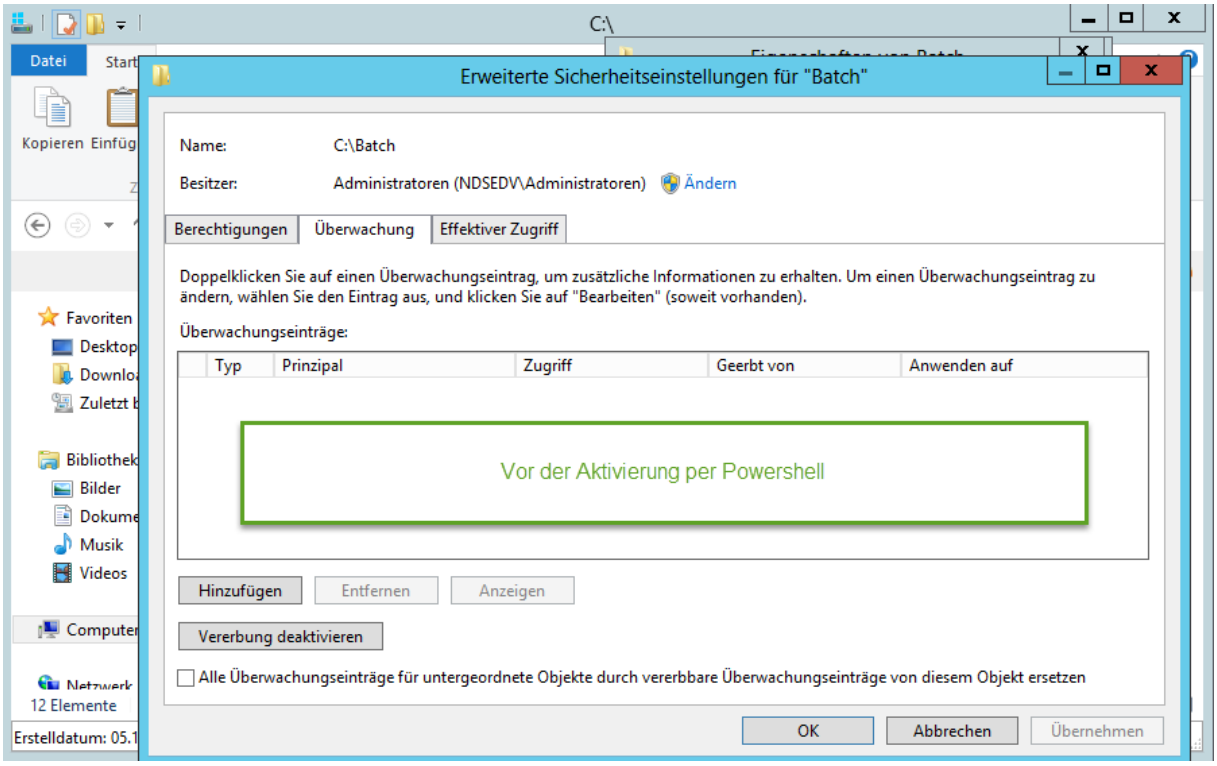
Server 2012 R2 - Auditing per Powershell aktivieren

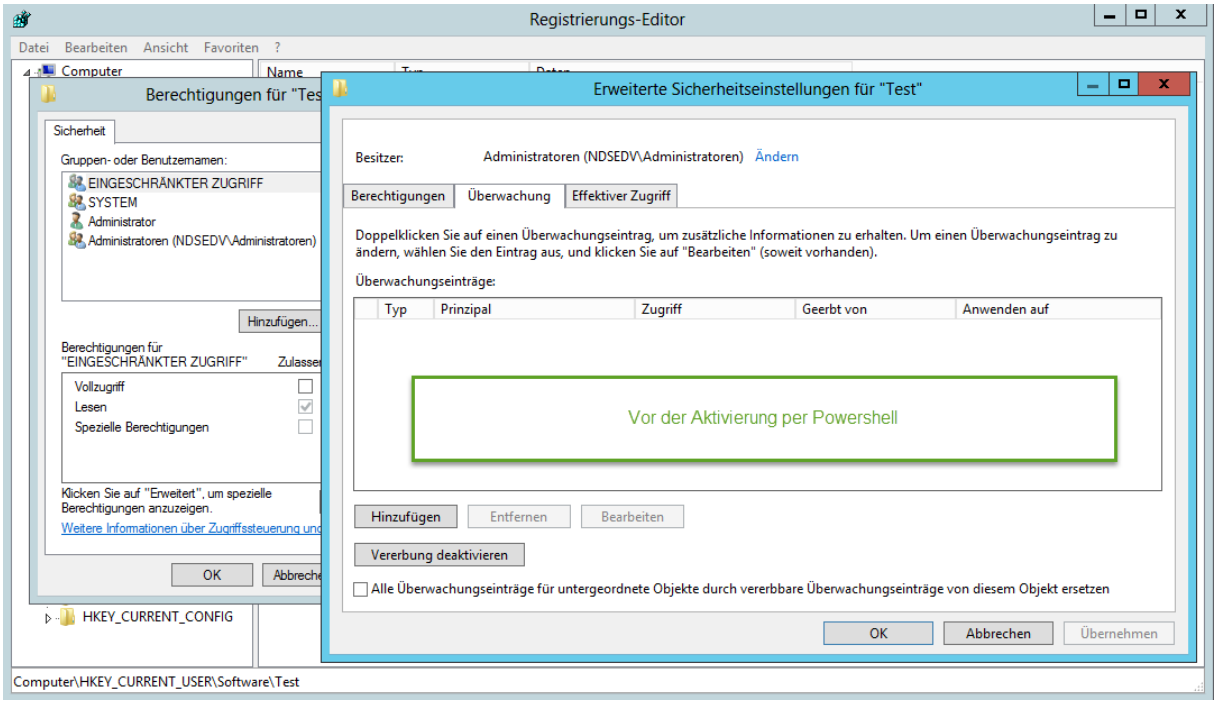
In dieser Anleitung möchte ich euch zeigen wie ich das Auditing auf über 300 Servern aktiviert habe. PCI-DSS fordert die Überwachung diverser Verzeichnisse und Registry Einträge.

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

Verzeichnisse vorher:

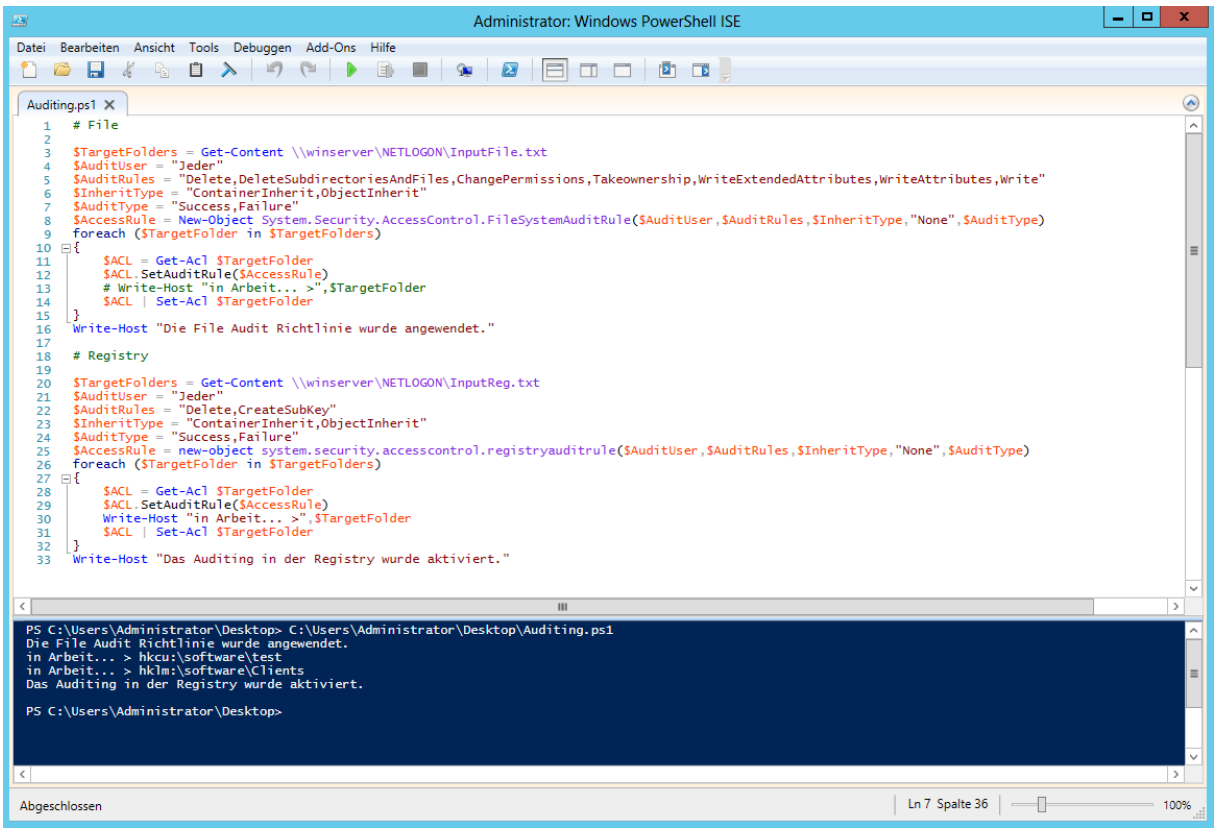


Registry vorher:

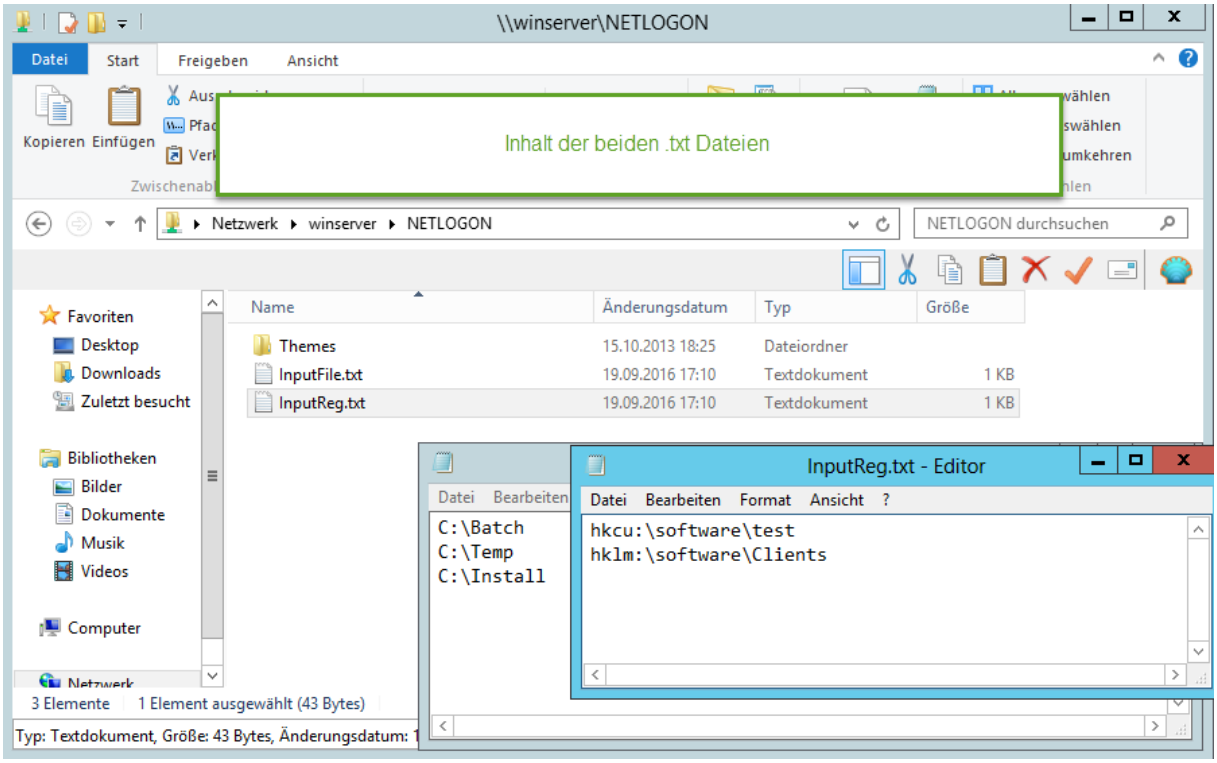


Server 2012 R2 - Auditing per Powershell aktivieren

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.



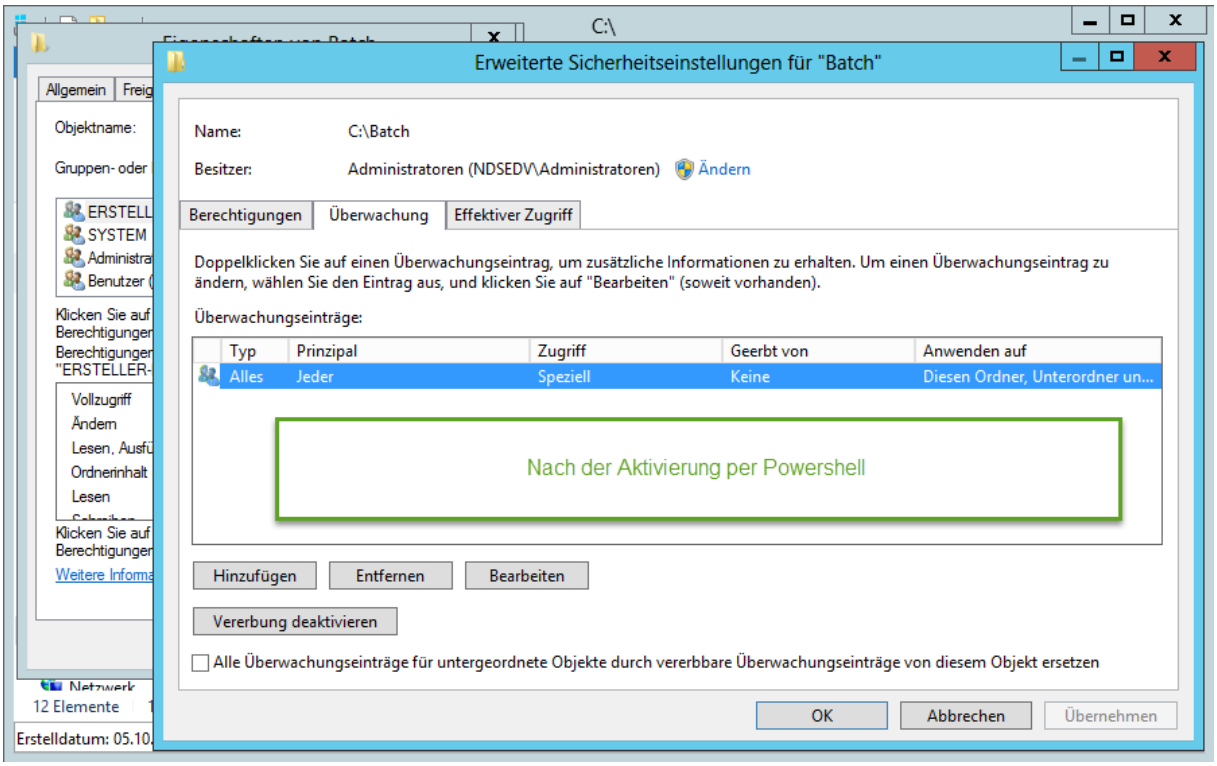
Aufbau und Inhalt der .txt Dateien



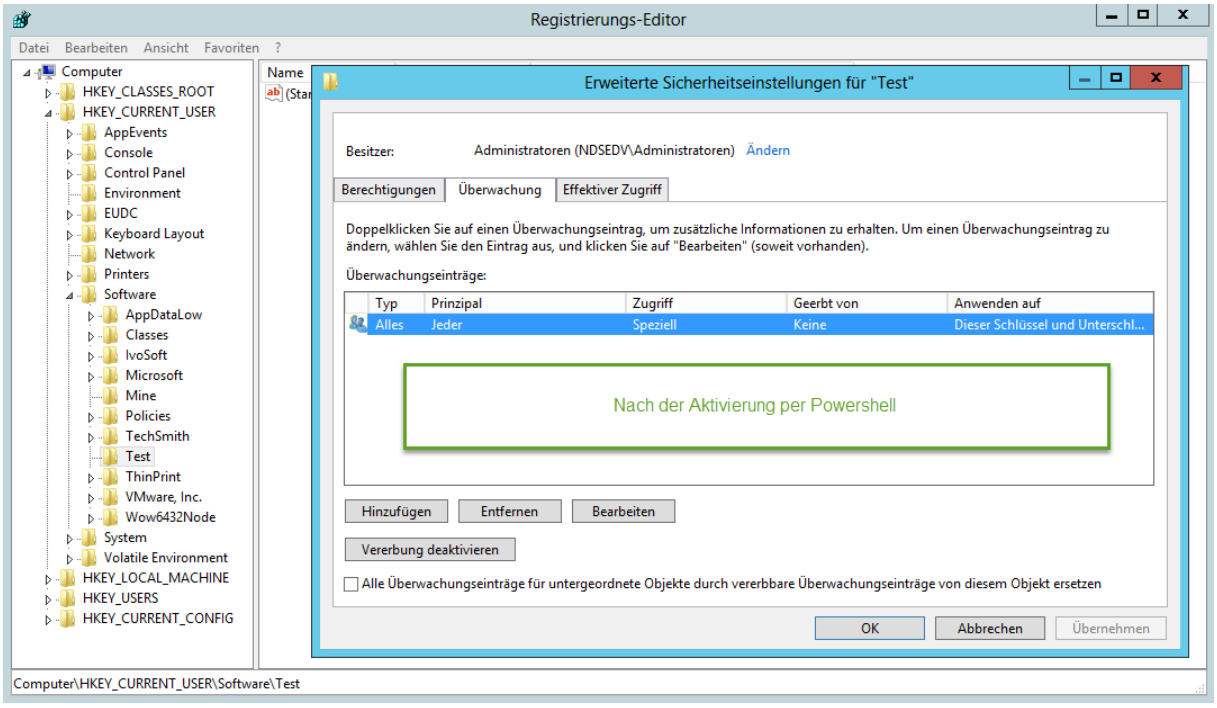
Erstellt von Jörn Walter www.der-windows-papst.de – 05.10.2016

Server 2012 R2 - Auditing per Powershell aktivieren

Das Ergebnis auf Verzeichnis-Ebene:



Das Ergebnis des Registry-Schlüssels TEST:



Erstellt von Jörn Walter www.der-windows-papst.de – 05.10.2016

Server 2012 R2 - Auditing per Powershell aktivieren

```
# File

$TargetFolders = Get-Content \\winserver\NETLOGON\InputFile.txt
$AuditUser = "Jeder"
$AuditRules =
"Delete,DeleteSubdirectoriesAndFiles,ChangePermissions,Takeownership,WriteExtendedA
ttributes,WriteAttributes,Write"
$InheritType = "ContainerInherit,ObjectInherit"
$AuditType = "Success,Failure"
$AccessRule = New-Object
System.Security.AccessControl.FileSystemAuditRule($AuditUser,$AuditRules,$InheritTy
pe,"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."
```