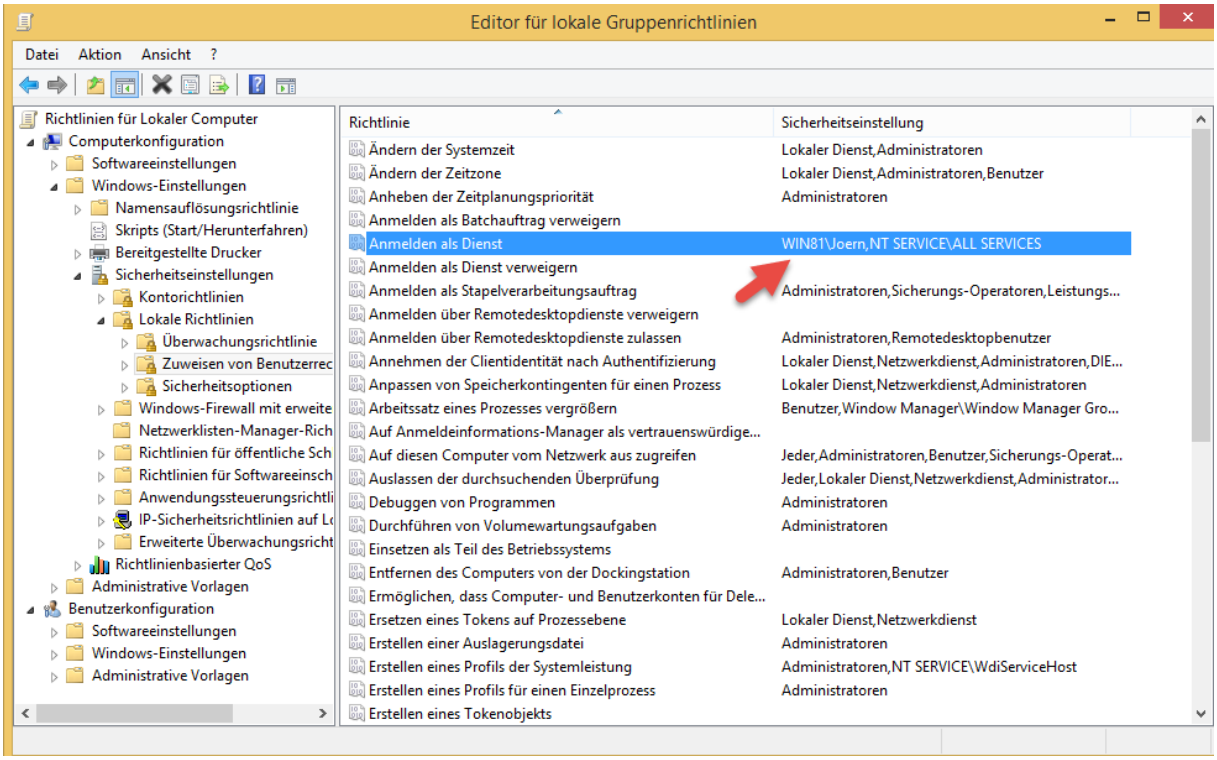
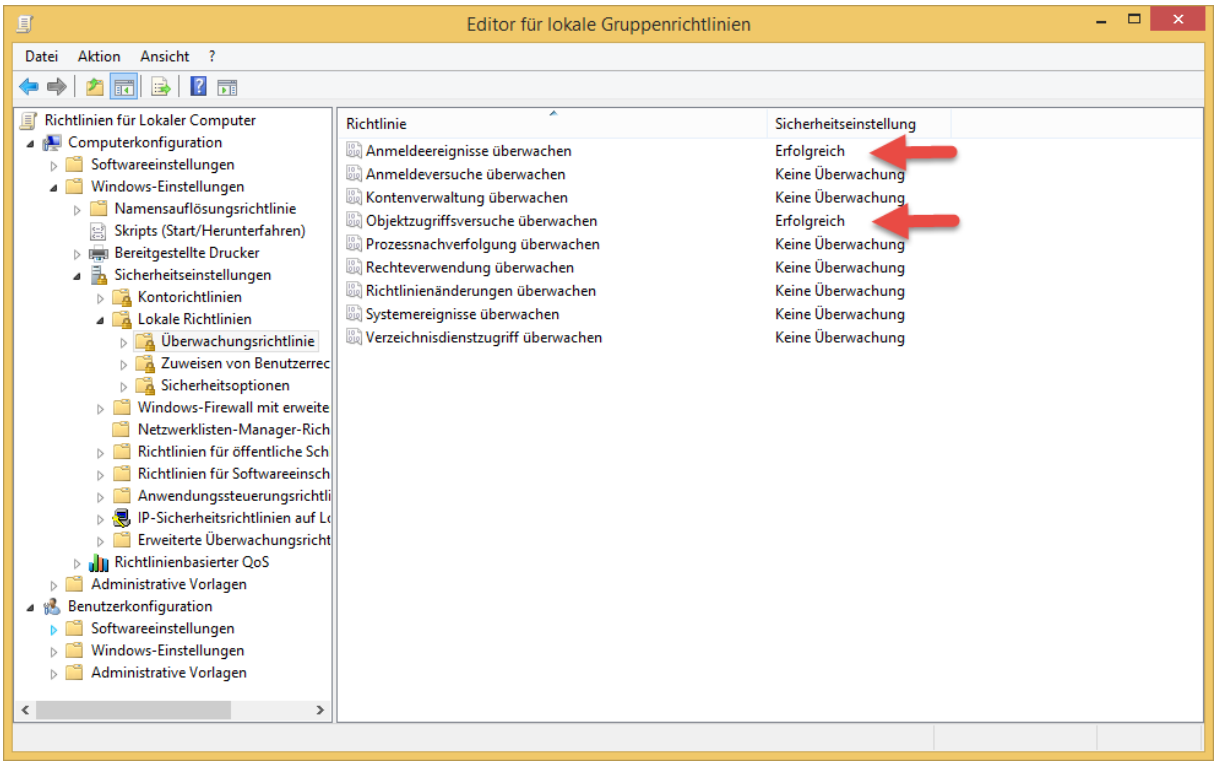
Standard Sicherheitsrichtlinien zurücksetzen

In diesem Dokument möchte ich beschreiben, wie angewandte Sicherheitsrichtlinien auf einem Client System zurückgesetzt werden können. Der Grund dafür kann unterschiedlich sein; Domänenbeitritt nicht möglich, Dateisystem oder Registry falsch berechtigt

Konfigurierte Sicherheitsrichtlinie als Beispiel:



Konfigurierte Überwachungsrichtlinie als Beispiel:

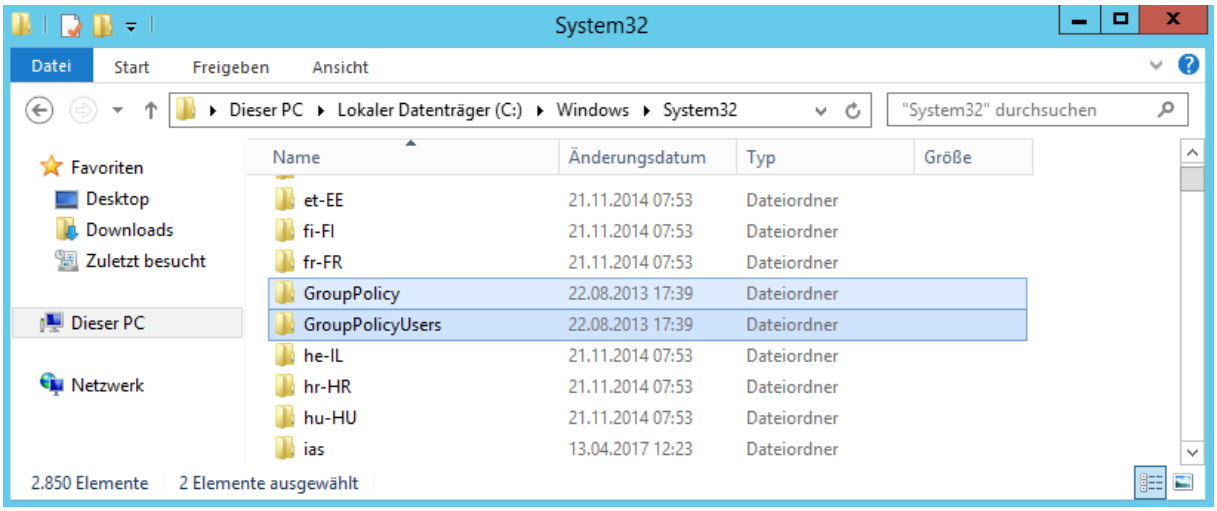


Erstellt von Jörn Walter **18.05.2014/16.06.2017**

Standard Sicherheitsrichtlinien zurücksetzen

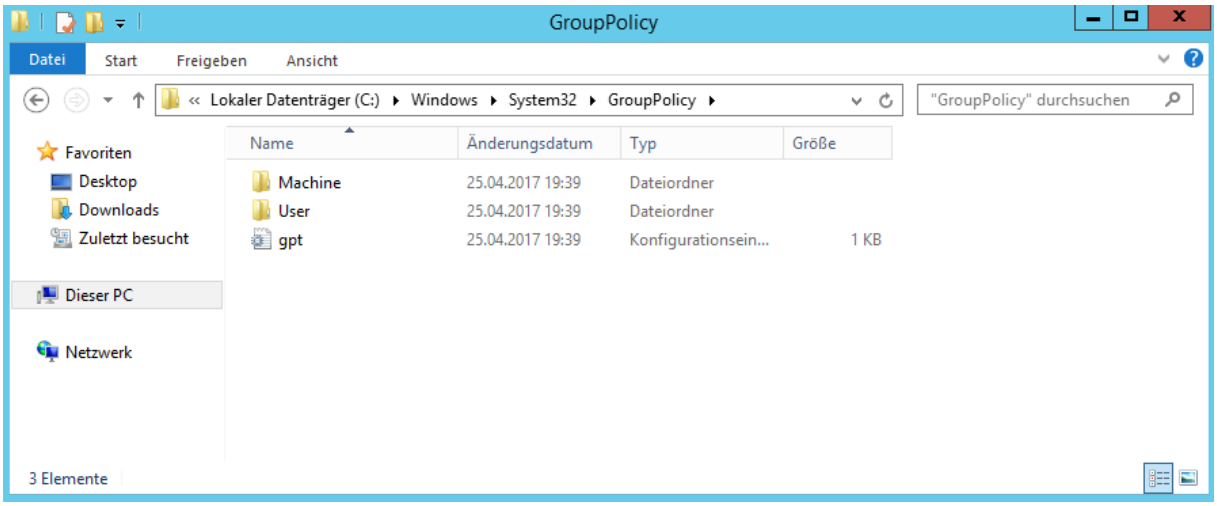
Der Speicherort der Einstellungen im Dateisystem ist:

C:\Windows\System32\GroupPolicy



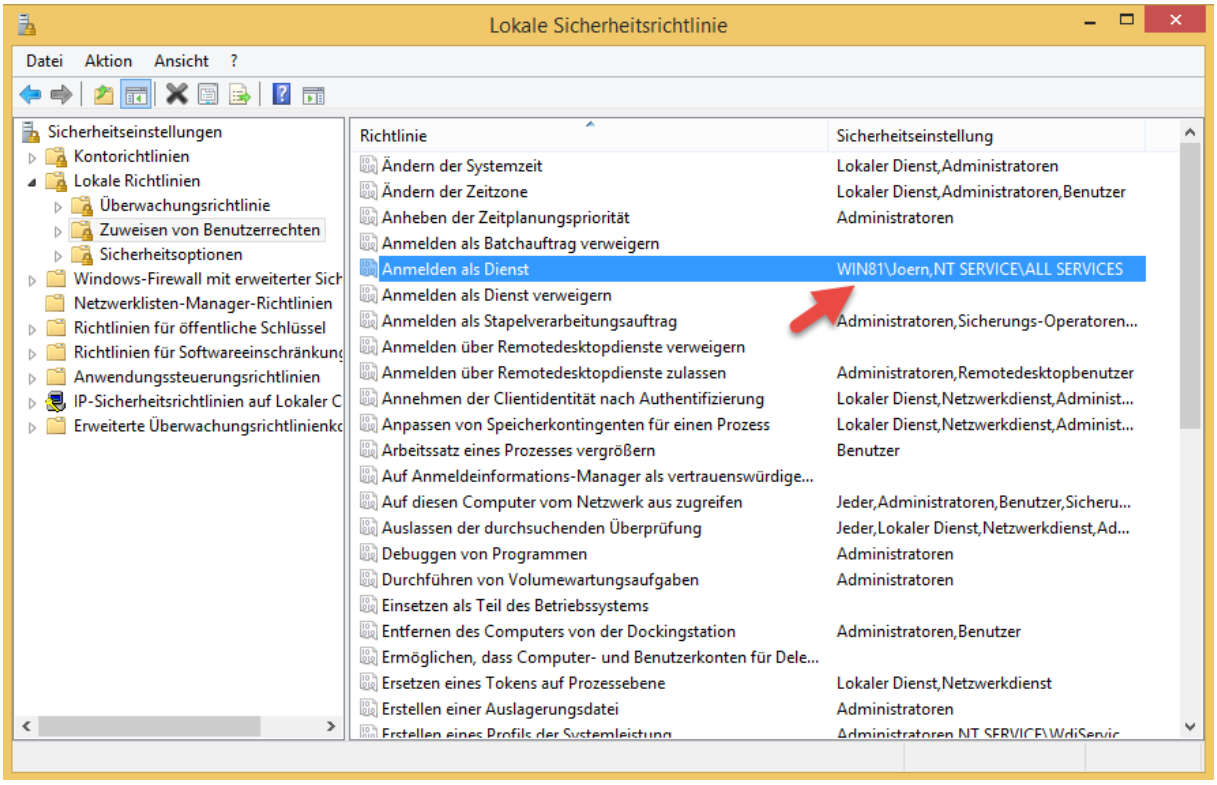
Speicherort in der Registry:

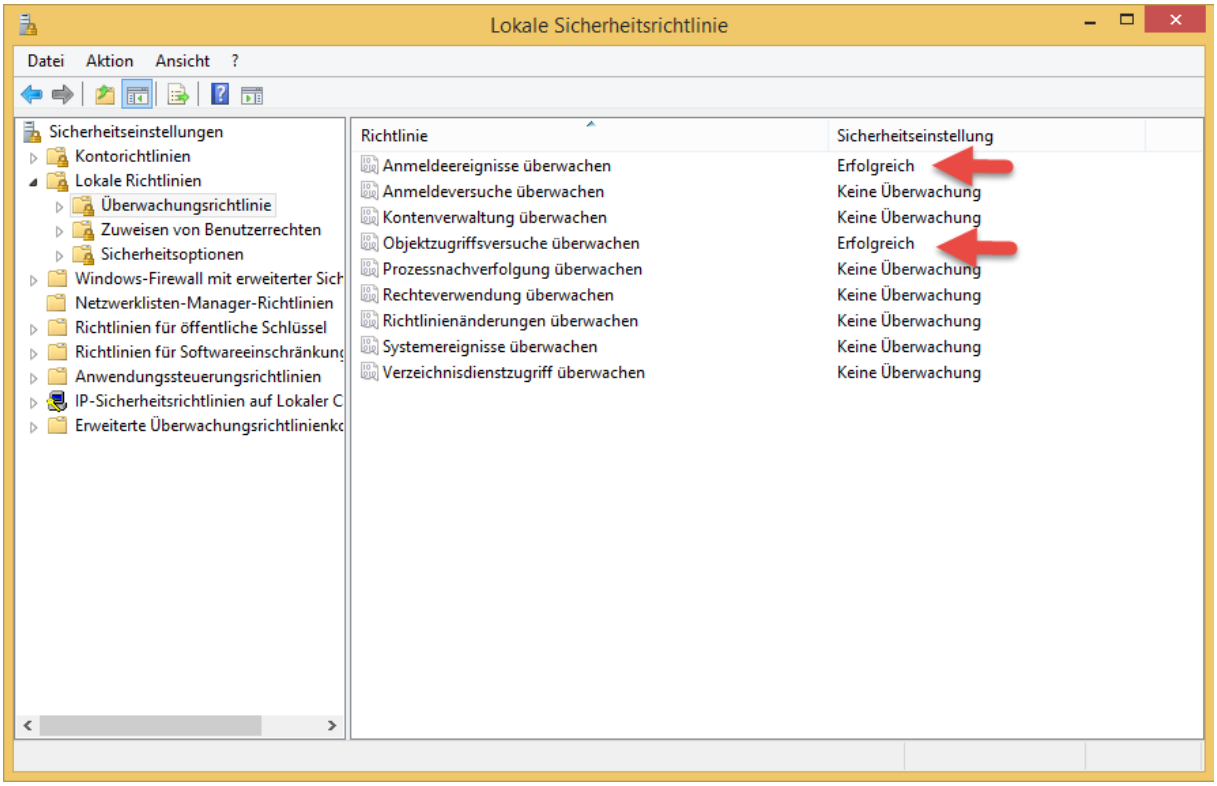
Machine = HKEY_LOCAL_MACHINE; User = HKEY_CURRENT_USER



Standard Sicherheitsrichtlinien zurücksetzen

Die lokalen Sicherheitsrichtlinien (Local Security Policies) sind aufzurufen über das Tool secpol.msc:

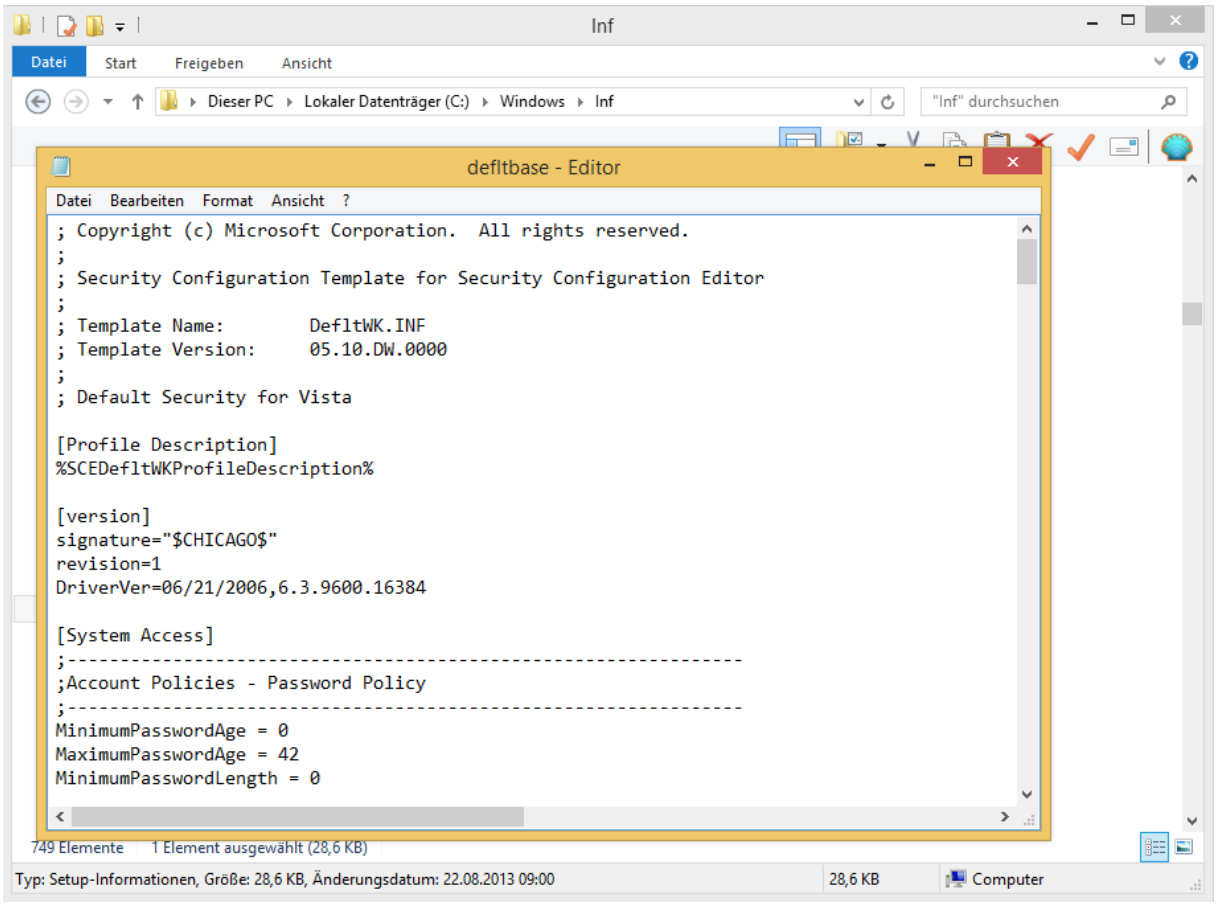




Standard Sicherheitsrichtlinien zurücksetzen

Reset-Befehl:

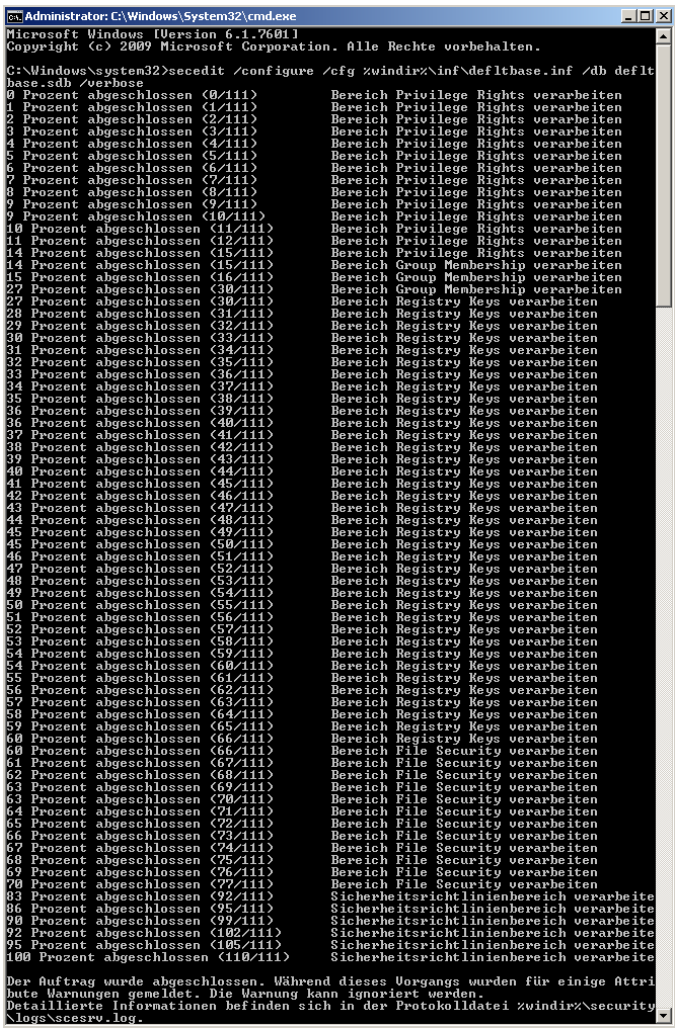
C:\Windows\Inf\defltbase.inf = Template aus dem die Wiederherstellung initiert wird.



Standard Sicherheitsrichtlinien zurücksetzen

Dieser Befehl setzt die Richtlinien auf Basis des oben gezeigten Templates zurück.

secedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose

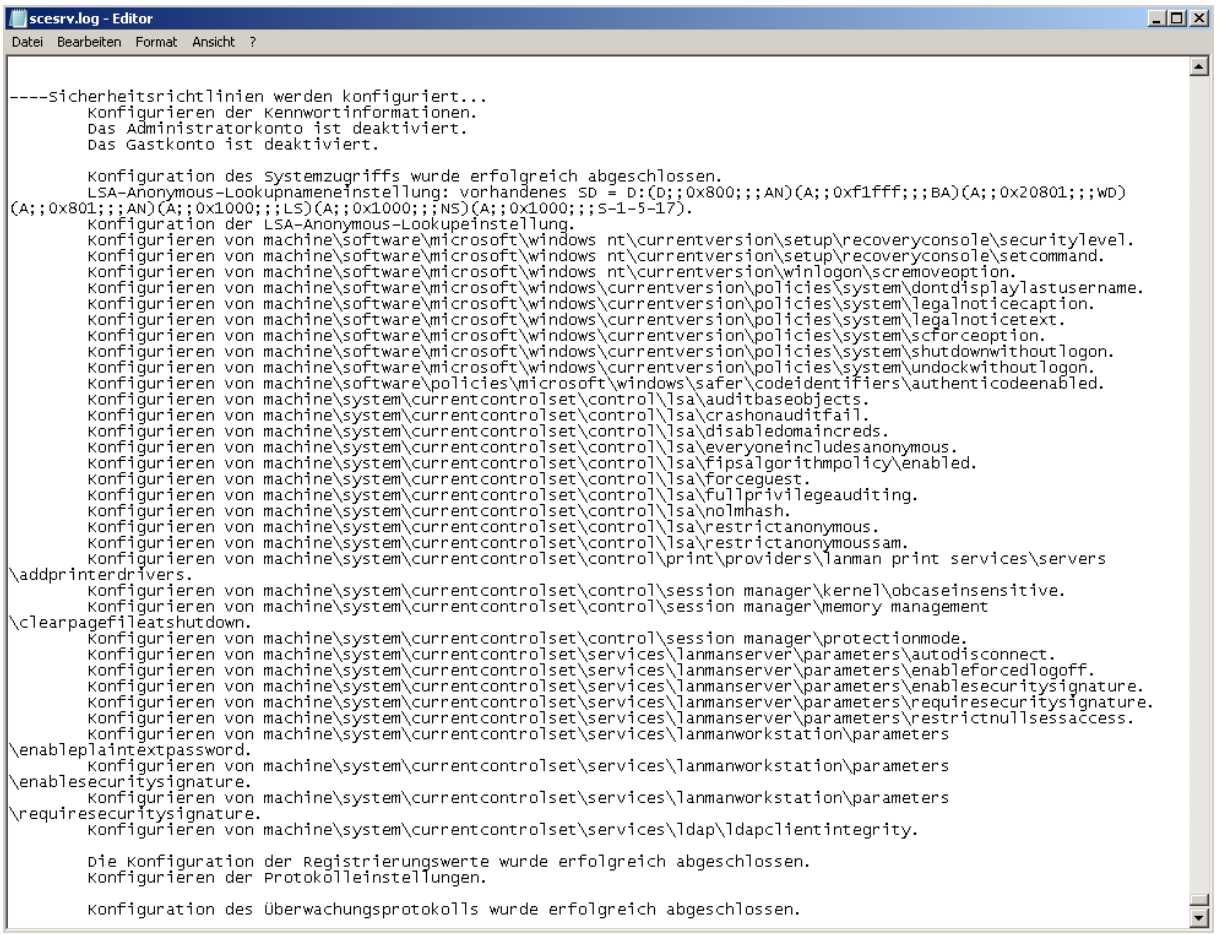


Diese Methode kann angewendet werden, wenn z.B. eine Fehlermeldung/Laufzeitfehler etc. auftrat in Zusammenhang mit der defltbase.sdb. Natürlich auch bei einer Fehlkonfiguration des Dateisystems, der Registry usw.

Standard Sicherheitsrichtlinien zurücksetzen

Alle Änderungen werden in diese Log-Datei geschrieben:

C:\Windows\security\logs



scesrv.log - Editor

Datei Bearbeiten Format Ansicht ?

```
----Sicherheitsrichtlinien werden konfiguriert...
        Konfigurieren der Kennwortinformationen.
        Das Administratorkonto ist deaktiviert.
        Das Gastkonto ist deaktiviert.

        Konfiguration des Systemzugriffs wurde erfolgreich abgeschlossen.
        LSA-Anonymous-Lookupnameneinstellung: vorhandenes SD = D:(D;;0x800;;;AN)(A;;0xf1fff;;;BA)(A;;0x20801;;;WD)
(A;;0x801;;;AN)(A;;0x1000;;;LS)(A;;0x1000;;;NS)(A;;0x1000;;;S-1-5-17).
        Konfiguration der LSA-Anonymous-Lookupeinstellung.
        Konfigurieren von machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel.
        Konfigurieren von machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand.
        Konfigurieren von machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption.
        Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername.
        Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption.
        Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
        Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\scforceoption.
        Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon.
        Konfigurieren von machine\software\microsoft\windows\currentversion\policies\system\undockwithoutlogon.
        Konfigurieren von machine\software\policies\microsoft\windows\safer\codeidentifiers\authenticodeenabled.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\auditbaseobjects.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\crashonauditfail.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\disabledomaincreds.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\everyoneincludesanonymous.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\fipsalgorithmpolicy\enabled.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\forceguest.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\nolmhash.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\restrictanonymous.
        Konfigurieren von machine\system\currentcontrolset\control\lsa\restrictanonymoussam.
        Konfigurieren von machine\system\currentcontrolset\control\print\providers\lanman print services\servers
\addprinterdrivers.
        Konfigurieren von machine\system\currentcontrolset\control\session manager\kernel\obcaseinsensitive.
        Konfigurieren von machine\system\currentcontrolset\control\session manager\memory management
\clearpagefileatshutdown.
        Konfigurieren von machine\system\currentcontrolset\control\session manager\protectionmode.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanserver\parameters\restrictnullsessaccess.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanworkstation\parameters
\enableplaintextpassword.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanworkstation\parameters
\enablesecuritysignature.
        Konfigurieren von machine\system\currentcontrolset\services\lanmanworkstation\parameters
\requiresecuritysignature.
        Konfigurieren von machine\system\currentcontrolset\services\ldap\ldapclientintegrity.

        Die Konfiguration der Registrierungswerte wurde erfolgreich abgeschlossen.
        Konfigurieren der Protokolleinstellungen.

        Konfiguration des Überwachungsprotokolls wurde erfolgreich abgeschlossen.
```

Optional:

GPOs per Powershell sichern:

```
Get-GPO -All | where CreationTime -gt 01.01.2015 | Backup-GPO -Path C:\backup\GPO
```

GPOs per Powershell wiederherstellen:

```
Restore-GPO -All -Path C:\backup\GPO
```

Leere GPOs ermitteln:

```
$AllGPOs = Get-GPO –all
foreach($GP in $AllGPOs){if($GP.User.DSVersion -eq 0 -and $GP.Computer.DSVersion -
eq 0)
{Write-Host "Leere GPOs:" $GP.DisplayName}}
```

GPO report XML:

```
Get-GPOReport -All -ReportType XML
```

Nicht zugewiesene GPOs ermitteln:

```
Get-GPO -All | %{[XML]$GPOs = Get-GPOReport -Name $_.DisplayName -ReportType
XML; $GPOs.GPO.Name + ";" + $GPOs.GPO.LinksTo.SOMName}
```

Erstellt von Jörn Walter **18.05.2014/16.06.2017**