AdminSDHolder

In so gut wie jedem Unternehmen gibt es einen First- oder gerne auch Second Level Support oder eine Abteilung namens Managed Services, die unteranderem die Aufgabe haben, die Benutzer im Active Directory zu administrieren.

Dieser Personenkreis sollte unter guten Bedingungen mit abgespeckten Rechten (least privileges) arbeiten. In der Regel sollten diese Personen auf etwaige OUs delegiert werden und nur die Rechte bekommen die sie zur Ausführung ihrer Tätigkeit benötigen und nicht mehr.

Hin und wieder kommt es aber vor, dass nach der Bearbeitung/Pflege eines Accounts die zuvor entzogenen oder hinzugefügten Rechte, wie von Geisterhand wieder verschwinden oder vorhanden sind. – Was ist hier los?

Im Active Directory gibt es spezielle High Privileged Groups, die unter der Schirmherrschaft des AdminSDHolder stehen. Zu diesen Gruppen gehören die:

- Administrators
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Domain Admins
- Schema Admins
- Enterprise Admins
- Cert Publishers sowie die Benutzer
    - Administrator
    - Krbtgt

Jedes Mitglied dieser Gruppen ob direkt oder indirekt wird als sehr schützenswert angesehen. Wenn jetzt z.B. eine Person aus den oben genannten Kreisen auf einer dieser schützenswerten Gruppen/Member Veränderungen an den Rechten vornehmen sollte, wird der AdminSDHolder dieses zu verhindern wissen.

Leider erkennt der AdminSDHolder die stattgefundenen Veränderungen an diesen Gruppen/Member nicht sofort.

Im Hintergrund läuft nämlich ein zeitgesteuerter Prüfmechanismus*****, der über die Registry angepasst werden kann.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
DWORD: AdminSDProtectFrequency
Wert: von 60-7200
Default: 3600

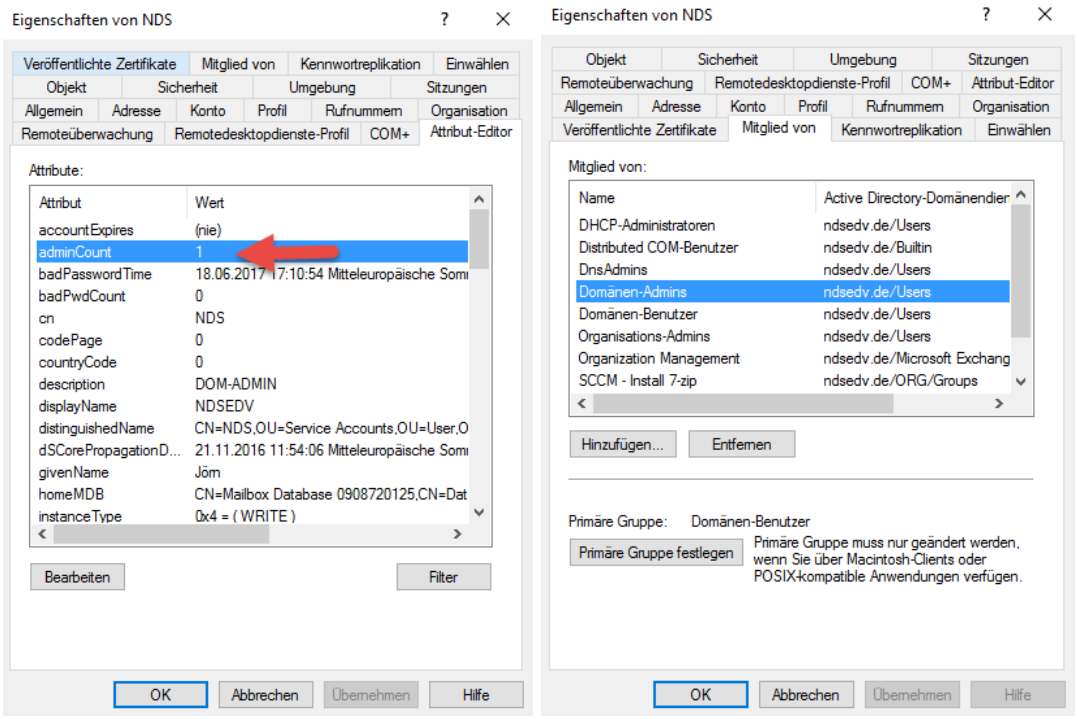
*****SDProp (Security Descriptor Propagation) heißt der Prozess, der jede Stunde auf dem DC (PDC) ausgeführt wird. Der AdminSDHolder vergleicht seine Berechtigungen** (Template) mit den Berechtigungen der schützenswerten Gruppen/Member. Weicht nur eine Berechtigung (ACE) dieser Gruppen ab, wird diese automatisch korrigiert (zurückgesetzt). Auch eine Veränderung an der Vererbung wird korrigiert (vererbte Berechtigungen übernehmen wird wieder deaktiviert, falls diese aktiviert wurde).

AdminSDHolder

Woran erkennen wir denn nun ein schützenwertes Objekt?

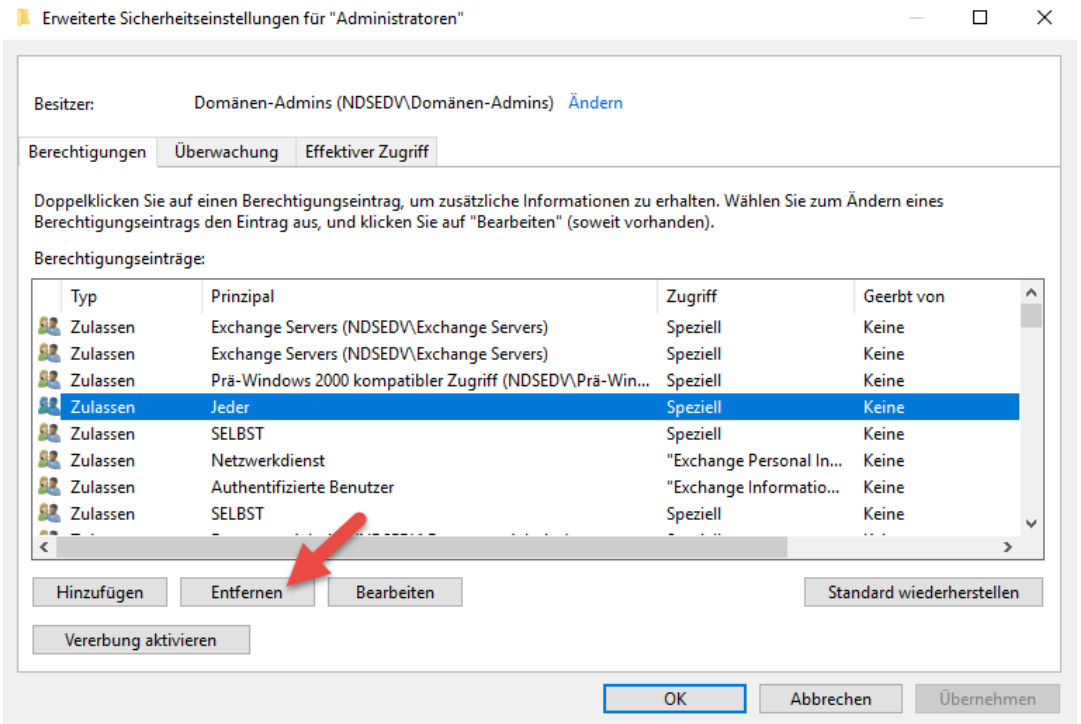
Dazu öffnen wir den Attribut-Editor und schauen uns das Attribut Admincount = 1 an. AdminCount = 1 sagt aus, das der User NDS in einer der schützenswerten Gruppen enthalten seien könnte.

In der Tat, der User NDS ist z.B. Mitglied der Gruppe Domänen-Admins und somit schützenswert. Der Wert = 0 ist nicht schützenswert.

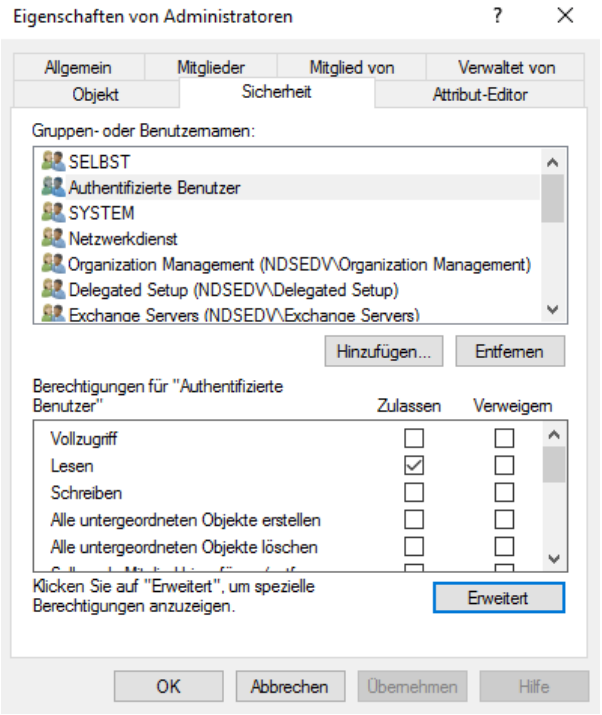


Ein Beispiel:

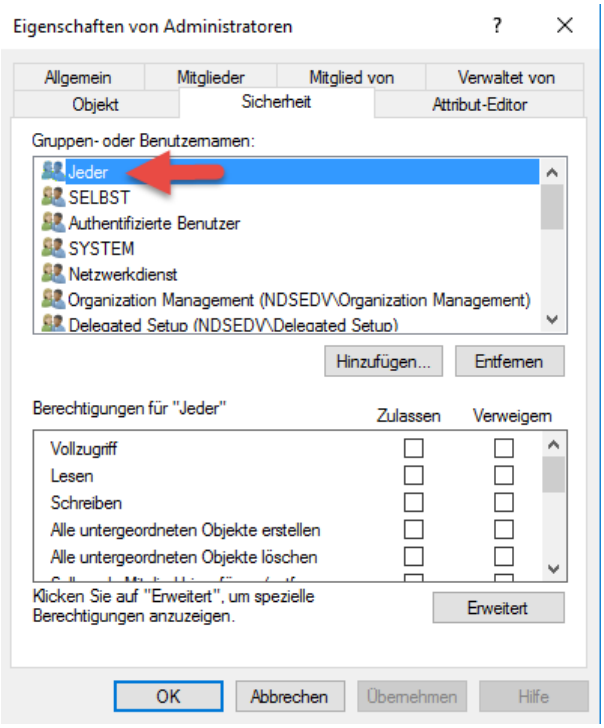
Ich entferne jetzt mal die Gruppe „Jeder" aus der Sicherheit der Domänen-Admins.



Ok ist entfernt.



Zum nächsten Prüfintervall* wurde die Gruppe „Jeder“ wieder hinzugefügt.

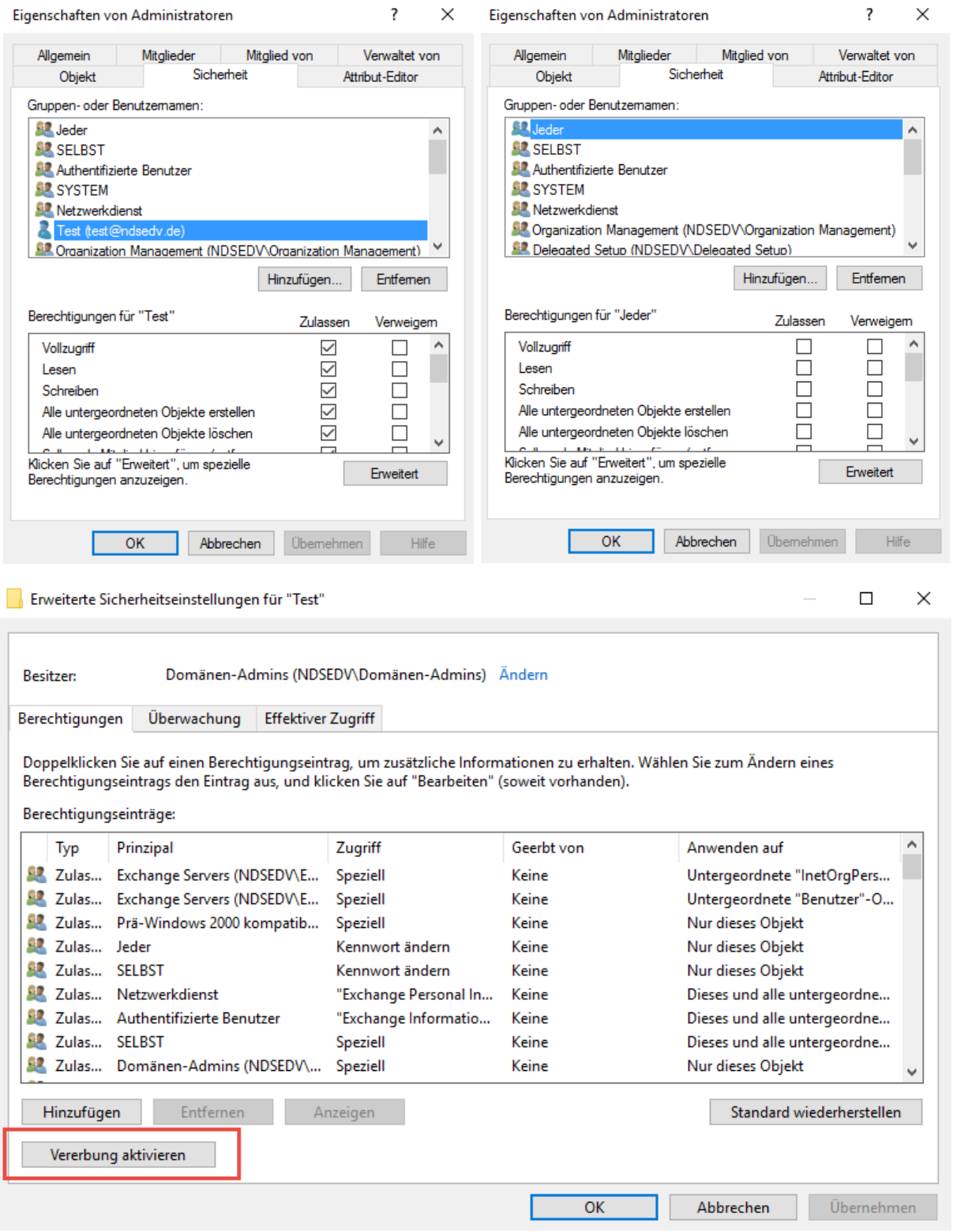


Info:

Wird der User NDS aus allen previligierten Gruppen entfernt, behält er das Flag admincount = 1, ist aber nicht mehr schützenswert. Ändert man den Wert auf = 0 obwohl der User NDS weiterhin Mitglied einer der schützenswerten Gruppen ist, wird der Wert automatisch wieder auf = 1 gesetzt.

AdminSDHolder

Kommen wir zum zweiten Test. Ich füge nun den User Test den Sicherheitseigenschaften der Gruppe Administratoren hinzu. Auch der wird zum nächsten Prüfintervall automatisch entfernt werden. Zusätzlich wird zum Schutz der Gruppe/Users die Vererbung deaktiviert, um zu verhindern, das die Berechtigungen einer OU auf die Gruppe/Users vererbt werden können, falls diese/dieser verschoben werden sollte.



AdminSDHolder

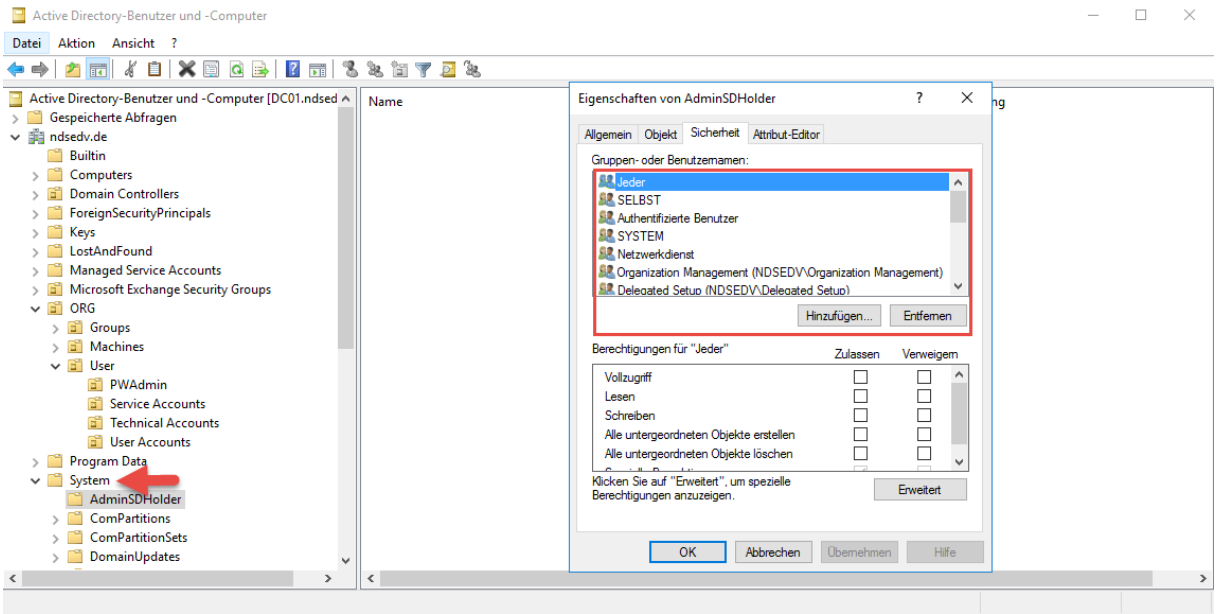
Ein nicht privilegierter Account kann einen privilegierten Account nicht dauerhaft administrieren, er würde durch den Prüfmechanismus bestenfalls jede Stunde, automatisch aus der Sicherheitsgruppe entfernt werden, in die er bedingt durch fehlende Privilegien, nicht hinein gehört.

Achtung: In der Zwischenzeit (Delta zum nächsten Intervall) kann er schalten und walten wir er will!

Ein First-Level-Mitarbeiter der auf eine OU berechtigt ist Passwörter zurücksetzen, in der OU auch zufällig ein ehemaliger Domänen Administrator enthalten ist, so wird er diesen ehemaligen Domänen Administrator das Passwort nicht zurücksetzen können. Das liegt ganz einfach daran, dass er den Wert = 1 im Attribut AdminCount stehen hat. Der Wert = 1 bleibt für ewig stehen und muss händisch auf = 0 gesetzt oder gelöscht werden. Zusätzlich schützt der Wert = 1 weiterhin vor ungewollten Vererbungen.

****Berechtigungen:**

Hier ist zu erkennen, das der AdminSDHolder die gleichen Berechtigungen innehat, wie die schützenswerten Gruppen. Der AdminSDHolder dient quasi als Template.



dsacls „CN=Test,OU=User Accounts,OU=User,OU=ORG,DC=ndsedv,DC=de"

ldifde -d "dc=ndsedv,dc=de" -r "(admincount=*)" -f admincount.txt -l "dn,admincount"

dsquery * -filter "(admincount=1)"

Powershell: Korrektur des Attributs AdminCount = 1; wird auf Null gesetzt

([adsisearcher]"(AdminCount=1)").findall()

Get-ADuser -LDAPFilter "(admincount=1)" | Select-Object name

Get-ADgroup -LDAPFilter "(admincount=1)" | Select-Object name

Get-AdUser [user name] | Set-AdObject -clear adminCount

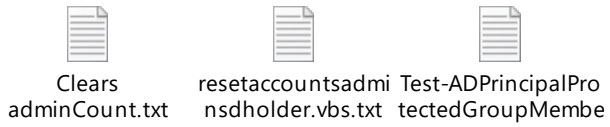
https://technet.microsoft.com/en-us/library/2009.09.sdadminholder.aspx

AdminSDHolder

Ich fasse das Ganze mal zusammen.

Das Active Directory Attribut adminCount wird verwendet, um den Schutzstatus eines Objektes auszudrücken. Der Wert dieses Attributs wird vom System festgelegt, wenn ein Objekt einer administrativen Gruppe / geschützten Gruppe angehört bzw. hinzugefügt wird.

Das Objekt AdminSDHolder befindet sich im Systemcontainer **CN=Container,CN=Schema,CN=Configuration,DC=ndsedv,DC=de** und verfügt über eine eindeutige Zugriffsteuerungsliste (ACL), die verwendet wird, um die Berechtigungen von Sicherheitsprinzipalen zu steuern/korrigieren, die Mitglieder von den oben aufgeführten Verwaltungskonten sind.

Wird ein Sicherheitsprinzipal aus allen Verwaltungskonten entfernt, behält er zwar das Flag AdminCount = 1 ist aber nicht mehr schützenswert. Das einzige was der Wert =1 weiterhin verhindert, ist eine mögliche Vererbung von Rechten. Denn der Wert = 1 deaktiviert das Vererbungs-Bit der Gruppe/User.

Dieses Schutzprinzip funktioniert nur domänenlokal also nicht über eine Domänen-Vertrauensstellung hinweg.