Security Identifier (SID)

Einleitung:

Windows verwendet zur Identifizierung von Objekten sogenannte SID (Security Identifier). SIDs bestehen aus einer folge alphanumerischer Werte. Jedes Objekt wie z.B. Benutzer, Computerkonten, Gruppen und Betriebssysteme erhalten eine eindeutige Windows-Sicherheitskennung (SID).

Eine SID besteht aus 4 Komponenten.

S-**1**-**5**-**32**-**544**

S = SID
1 = Revisionstand
5 = Bezeichner-Berechtigungswert
32 = Domänenkennung oder lokales System
544 = Benutzernummer (RID) - relative Kennung (Administrator)

SIDs für integrierte Konten und Gruppen haben immer die gleiche Kennung „32", da sie auf jedem System vorhanden sind. Der Geltungsbereich für Konten und Gruppen beschränkt sich immer auf das lokale System, daher gibt es keine Unterschiede zu anderen Systemen.

Vordefinierte Konten und Gruppen müssen im Rahmen der vordefinierten Domäne voneinander unterschieden werden. Daher weist die SID für jedes Konto und jede Gruppe eine eindeutige relative Kennung auf. Ein relativer Bezeichnerwert von 544 ist unique und steht für die integrierte Administratorgruppe. Kein anderes Benutzerkonto oder Gruppe in der vordefinierten Domäne hat eine SID mit dem Wert 544.

Ein Beispiel:

Das ist eine SID der lokalen Gruppe Domänenadministratoren. Jede Domäne hat eine Gruppe Domänen-Admins mit unterschiedlicher SID wobei die relative Kennung 512 immer gleich ist.

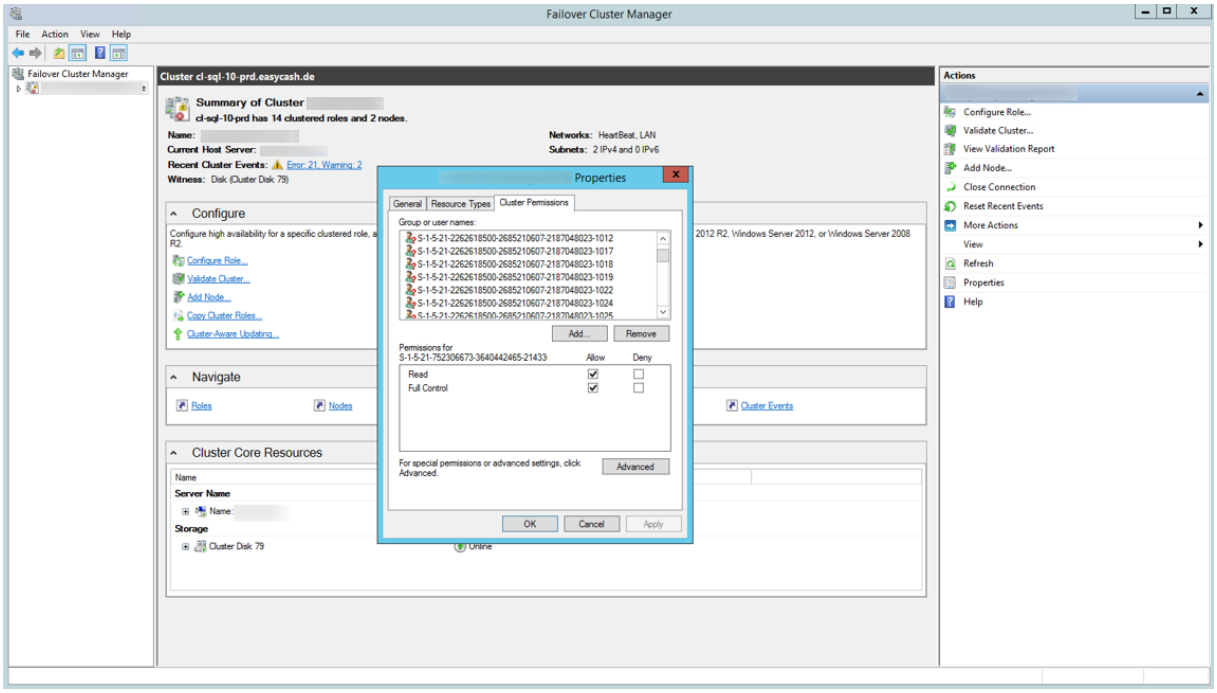
S-1-5-21-1004336348-1177238915-682003330-512

Security Identifier (SID)

Zustandsbeschreibung:

Die Berechtigungen zur Verwaltung eingebundener Nodes über den Failover Cluster Manager, sind aktuell nicht transparent und somit zweifelhaft was die Zugriffsteuerung angeht.

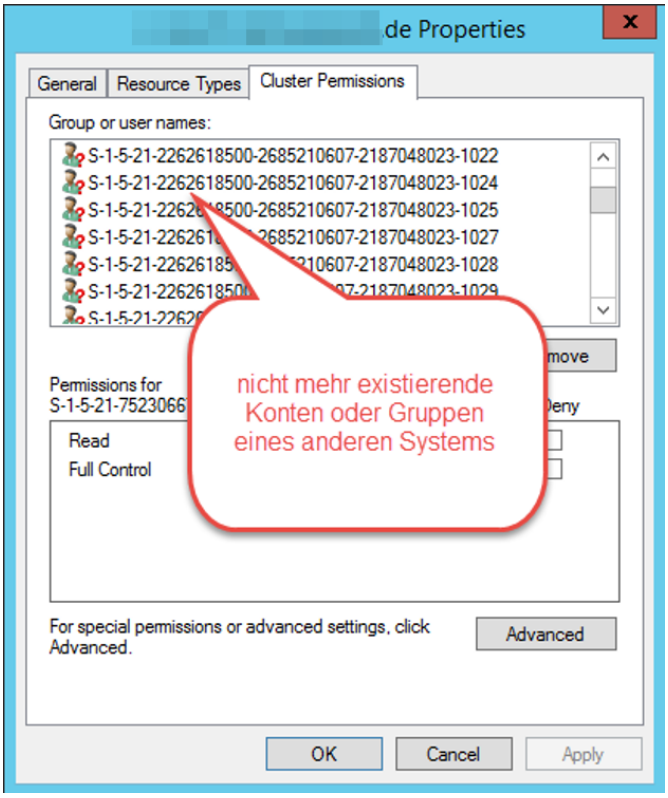
Unter dem Tab „Cluster Permissions“ finden wir eine Menge an nicht auflösbaren SIDs. Hinter den SIDs stehen sonst Benutzer-, System- oder entsprechende Gruppenberechtigungen.

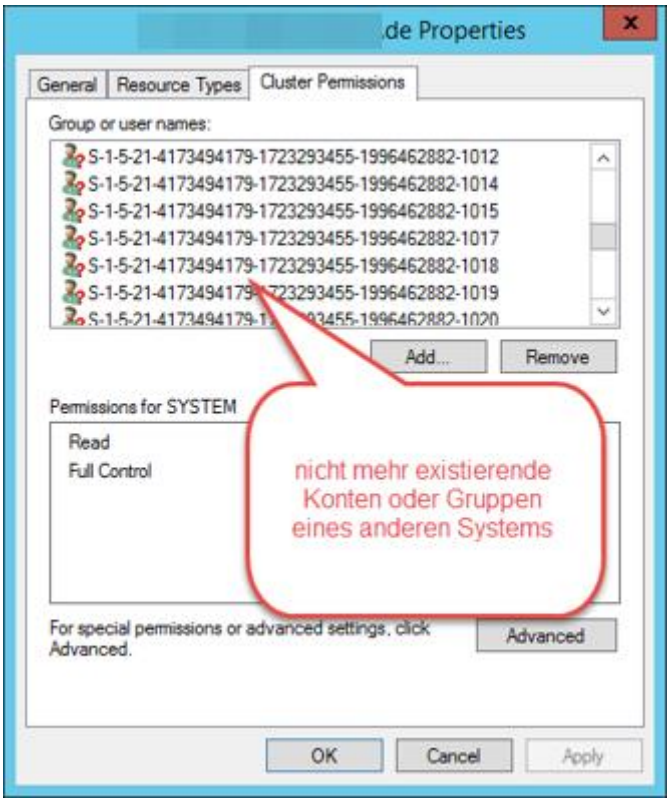


Security Identifier (SID) sind unique und somit unverwechselbar. Jede Domäne hat ihre eigene Kennung. In der Domäne ndsedv.de lautet die Kennung eines Accounts **„1070480190-636505833-1543857936**“. Da sich diese Kennung von den nicht auflösbaren SID in den Cluster Permissions bis auf *4 Ausnahmen unterscheidet, können wir davon ausgehen, dass es sich hierbei um fremd eingebundene lokale Benutzer-, System- oder entsprechende Gruppenberechtigungen anderer Systeme handelt.

Security Identifier (SID)

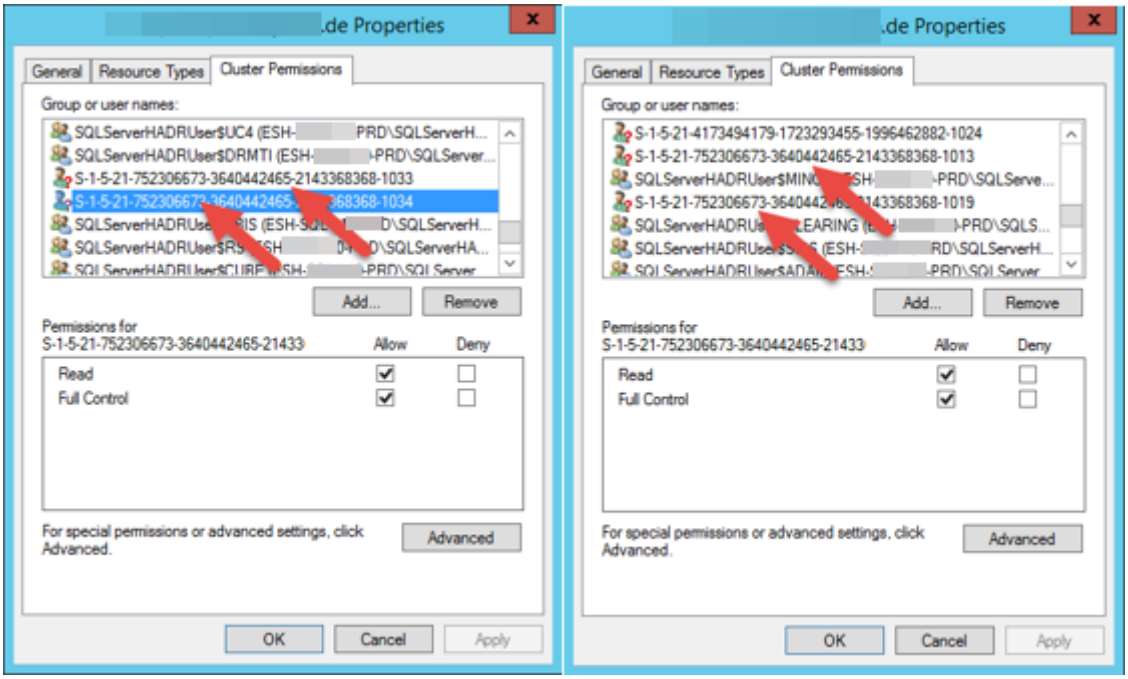
Leider lassen sich die Systeme nicht mehr ermitteln, da sie bereits aus der Domäne entfernt worden sind.
Achtung: Es könnten auch Systeme sein die über eine Domänen-Vertrauensstellung sichtbar sind/waren!



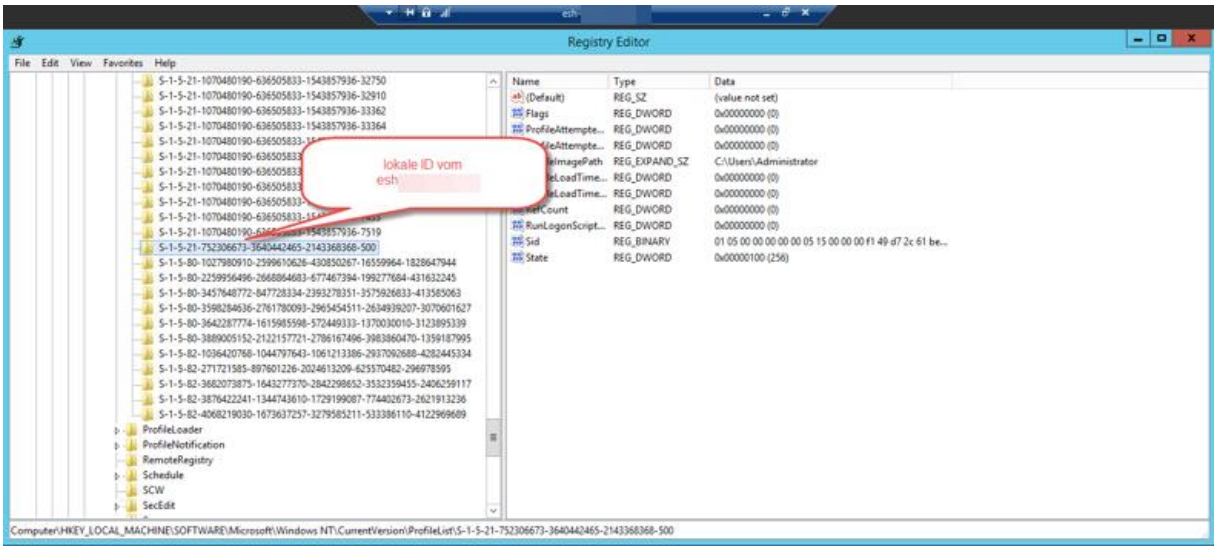


Security Identifier (SID)

*Bei den 4 Ausnahmen handelt es sich um SIDs die auf den esh-prd verweisen. Siehe (Remote Bild)



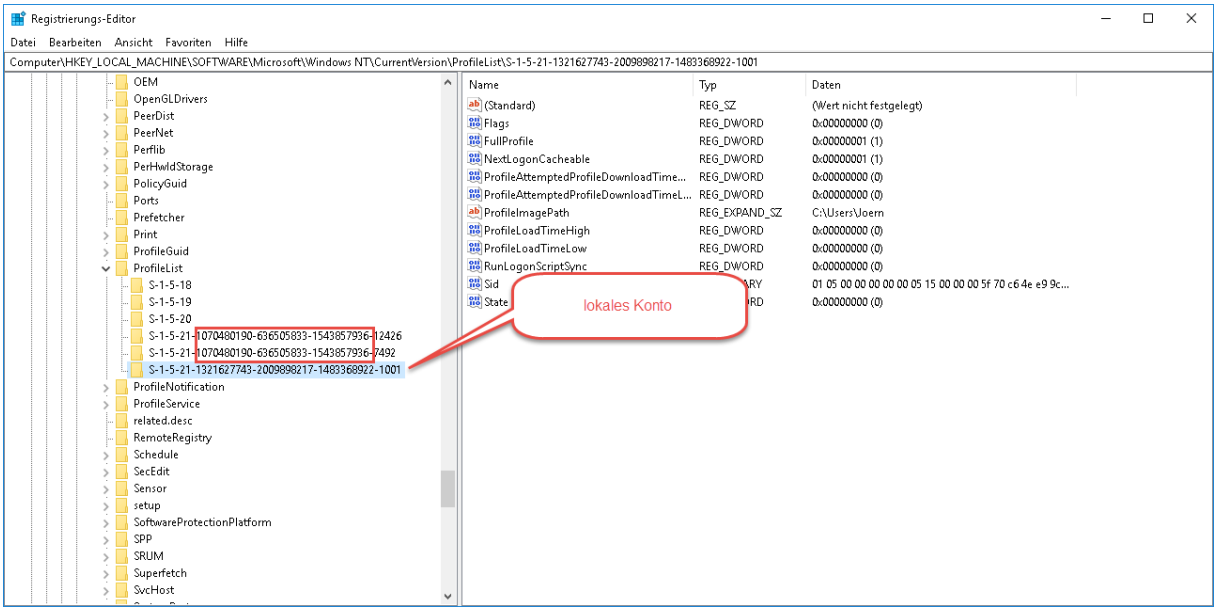
Wie zu erkennen ist, gibt es diese 4 Identifier mit den relativen Kennungen „1013,1019,1033,1034" nicht auf dem esh-prd.



Security Identifier (SID)

Erklärung zur Annahme:

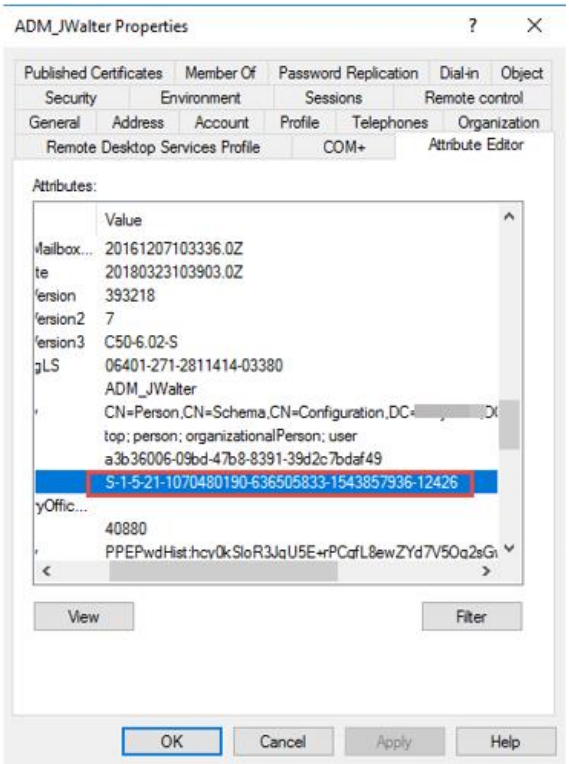
Hier ist klar zu erkennen, das auf diesem System (DE17080) 2 Domänenkonten und ein lokales Konto existieren. Die Kennungen unterscheiden sich eindeutig. Das ist auch der Grund, warum ich zu dem Entschluss gekommen bin, dass es sich bei den nicht auflösbaren SIDs um Benutzer-, System- oder entsprechende Gruppenberechtigungen anderer Systeme handelt.



Untermauerung der Annahme:

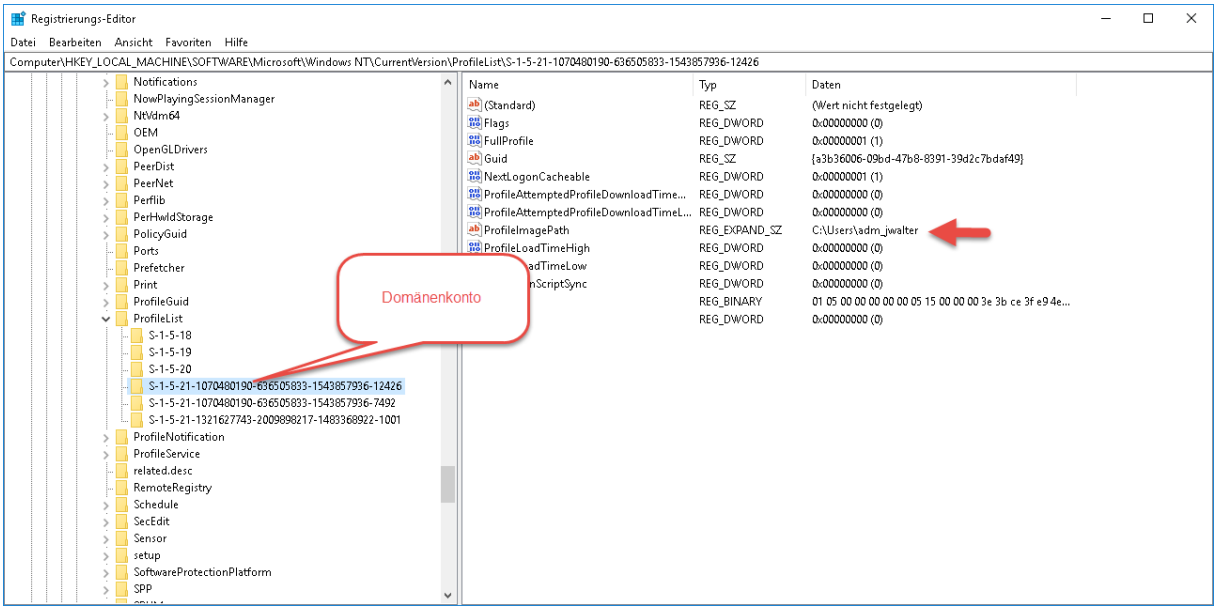
Dieser Screenshot soll zeigen, dass die Benutzer-SID des Users **adm_jwalter** unique ist und auf anderen Systemen wiederzufinden ist.

Relative Kennung: 12426



Security Identifier (SID)

System: DE17080
Relative Kennung: 12426



Meine Empfehlung:

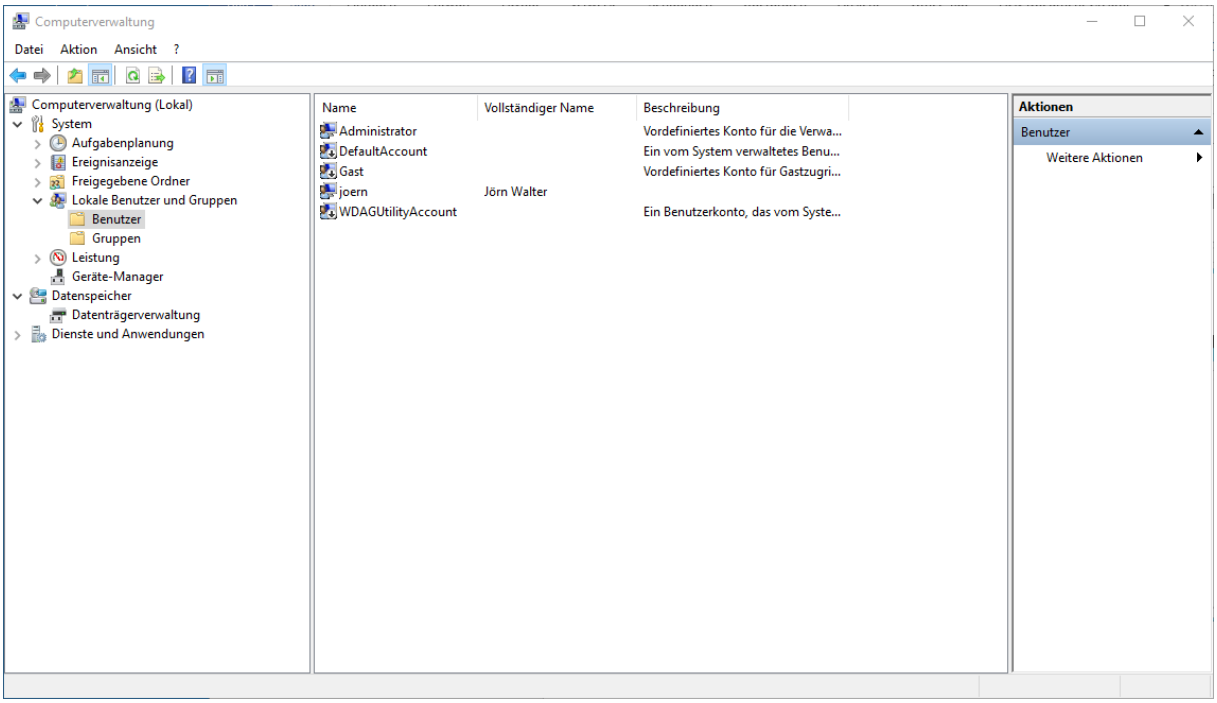
Die nicht auflösbaren SIDs bis auf die 4 Ausnahmen entfernen

- um die Übersichtlichkeit der tatsächlichen Berechtigungen wiederherzustellen
- zur Steigerung der Performance, da die SIDs immer wieder versucht werden aufzulösen

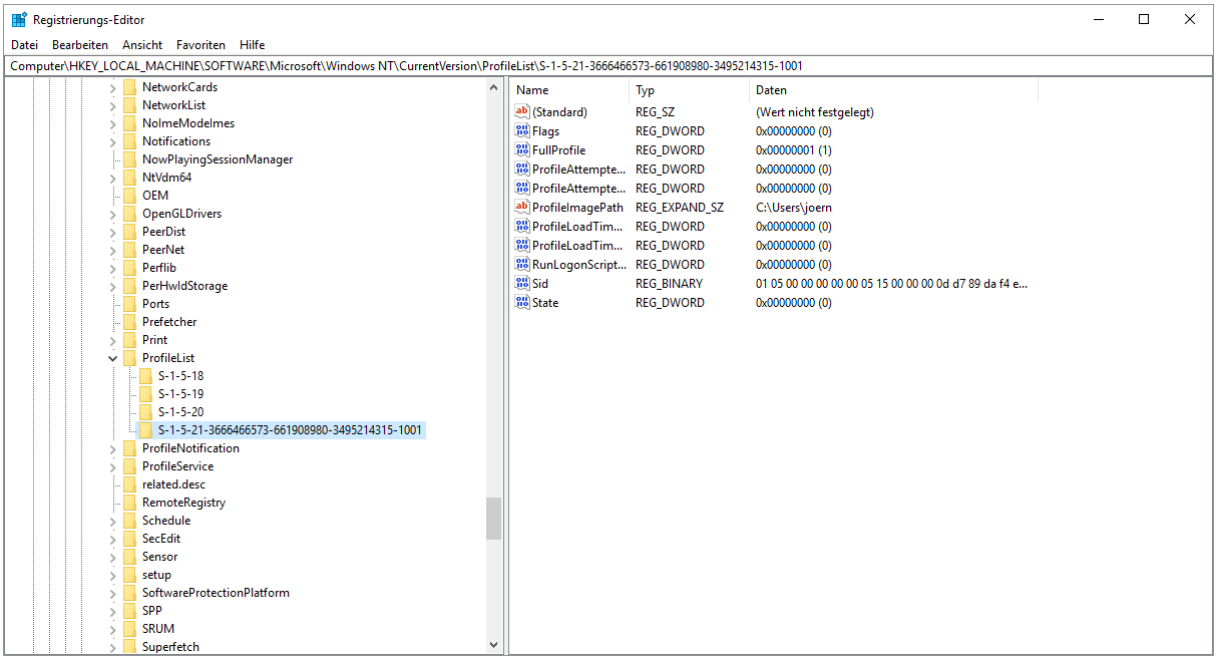
Security Identifier (SID)

Optional:

Auf meinem System gibt es folgende lokale Konten:

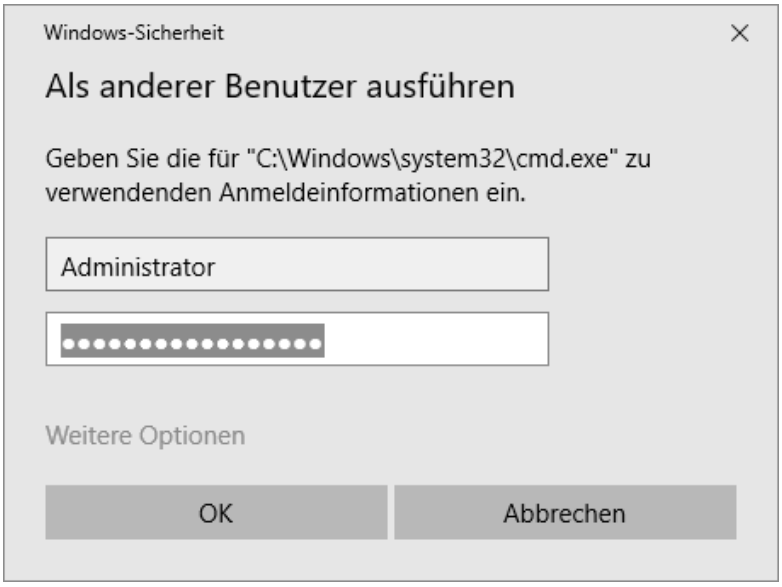


Angemeldet bzw. authentifiziert hat sich bisher nur der Benutzer „Joern“, mit der relativen Kennung 1001. Der lokale Administrator hat sich bisher nicht authentifiziert, sonst würde es eine SID mit der relativen Kennung 500 geben.

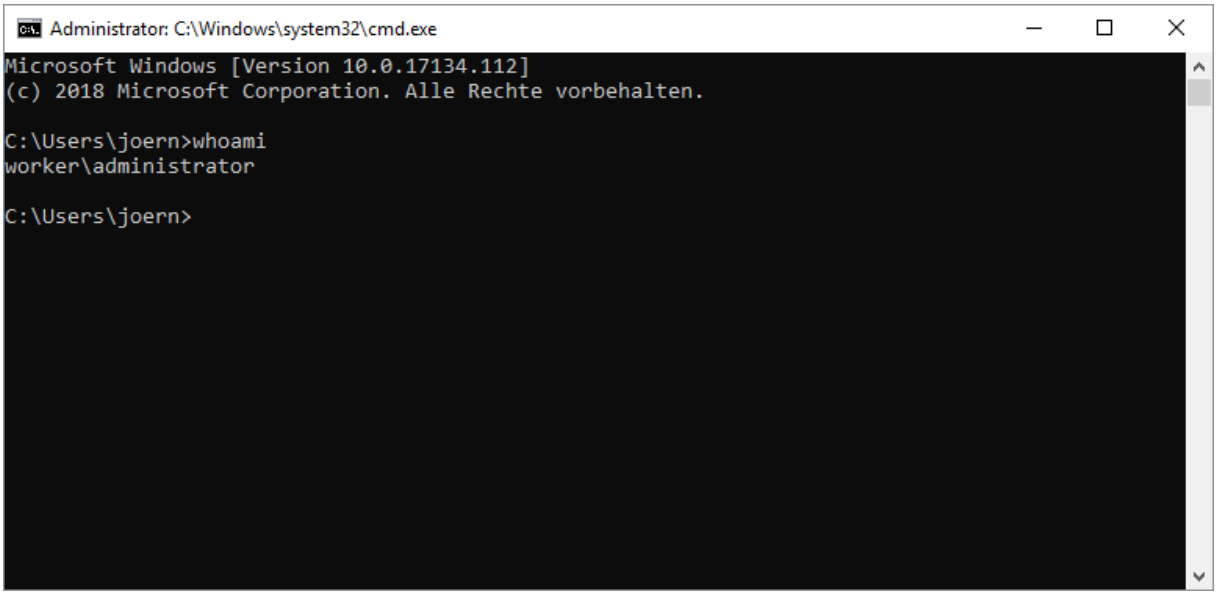


Security Identifier (SID)

Das hole ich jetzt nach, in dem ich die CMD mit den Rechten des Administrators ausführe.

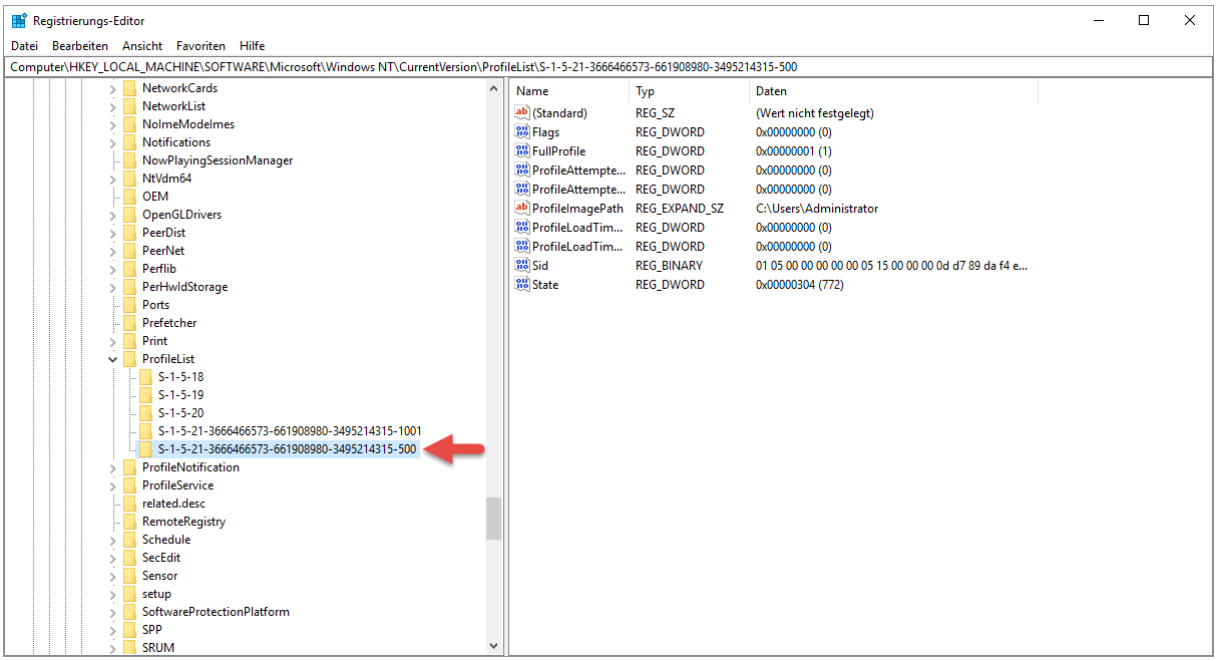


„Whoami" zur Ermittlung des Benutzers.

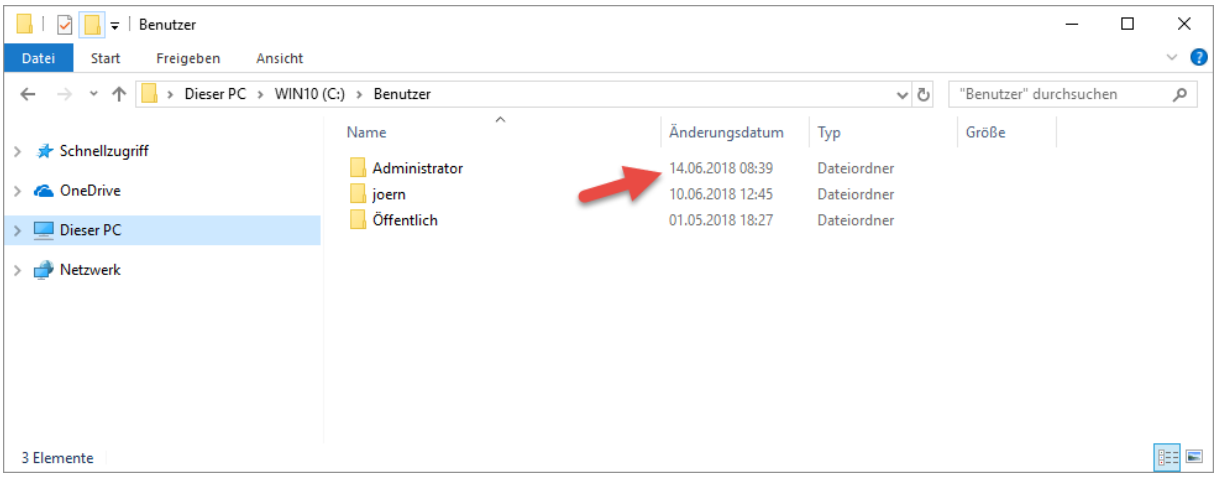


Security Identifier (SID)

In der Registry wird die neue SID angelegt und im Profilpfad der Ordner des Benutzers.



Profilpfad:



Security Identifier (SID)

Neu angelegte Benutzer und Gruppen werden ab der relativen Kennung 1001 durchnummeriert:

Get-WmiObject -Class Win32_Group | select Name, Description, SID, LocalAccount | format-list