Server 2016 - Privileged Access Management

Wie bereits unter Server 2012 R2 mit DynamicObjetcs temporäre Berechtigungen vergeben werden konnten, mittels einer Mitgliedschaft in einer AD Gruppe auf Zeit, kann man auch unter Server 2016 und dem neuen Privileged Access Management Feature, zeitlich begrenzte Berechtigungen vergeben.

Die einzige Voraussetzung ist, dass die Gesamtstrukturfunktionsebene auf Windows Server 2016 laufen muss!

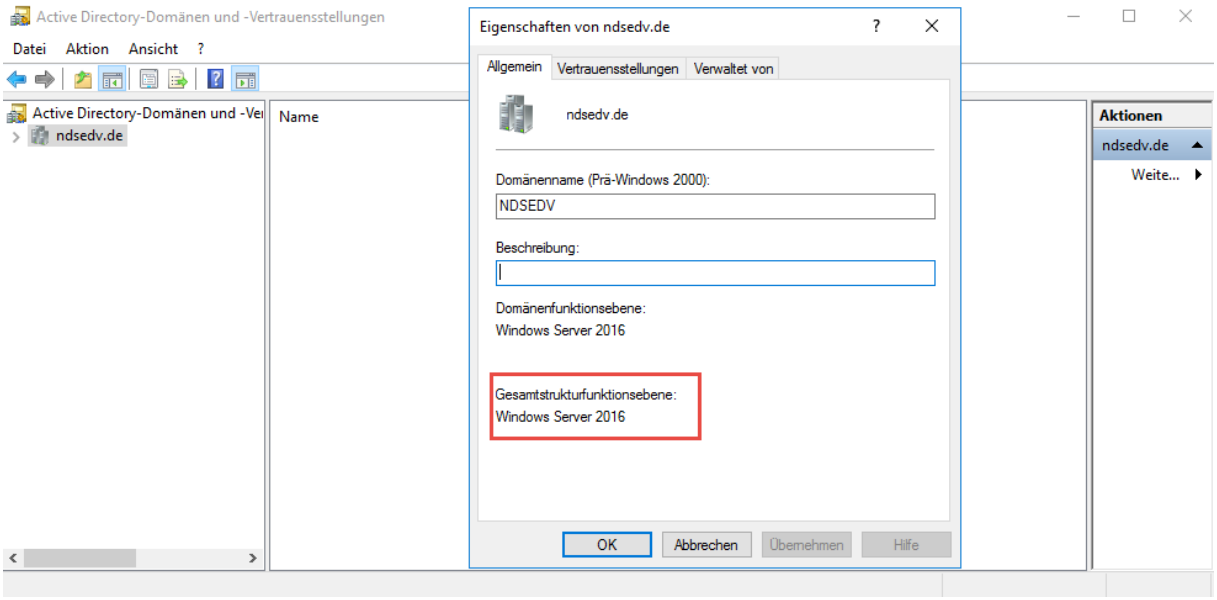
Wie funktioniert das Ganze?

Benutzer verbleiben für eine definierte Zeit Member einer AD Gruppe bis sie automatisch entfernt werden. Dabei spielt es keine Rolle ob es sich um eine Sicherheitsgruppe oder Verteilergruppe handelt.

Das Thema Privileged Access Management darf nicht mit dem Thema Identity Management verwechselt werden, auch wenn es hier thematische Überschneidungen gibt.

Los geht's…

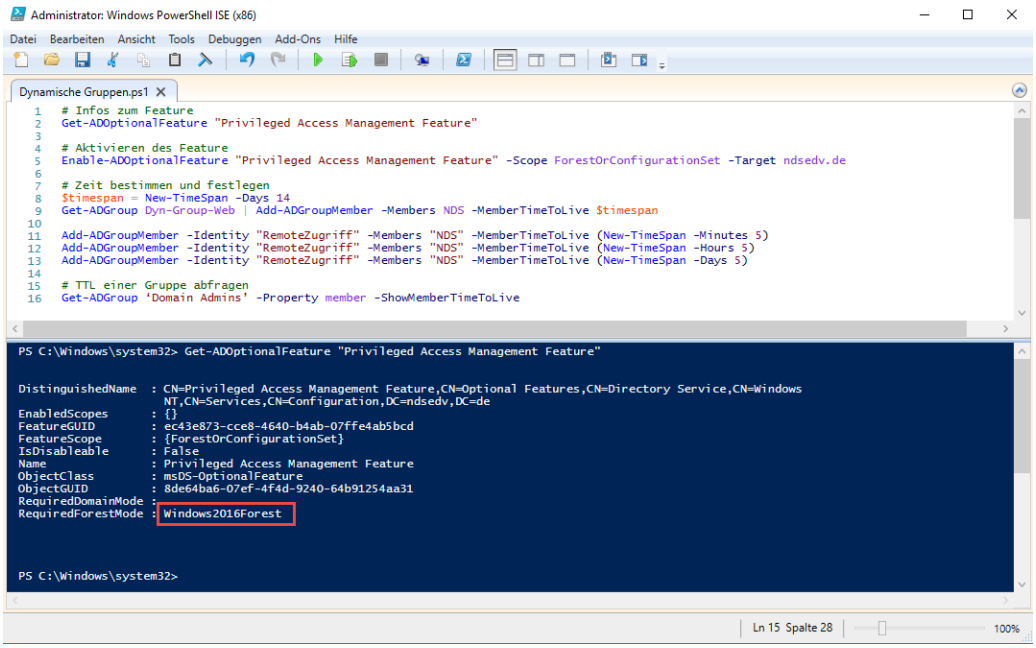
Als erstes prüfen wir die Gesamtstrukturfunktionsebene.



Server 2016 - Privileged Access Management

Ziehen uns mal ein paar Infos zum Feature:

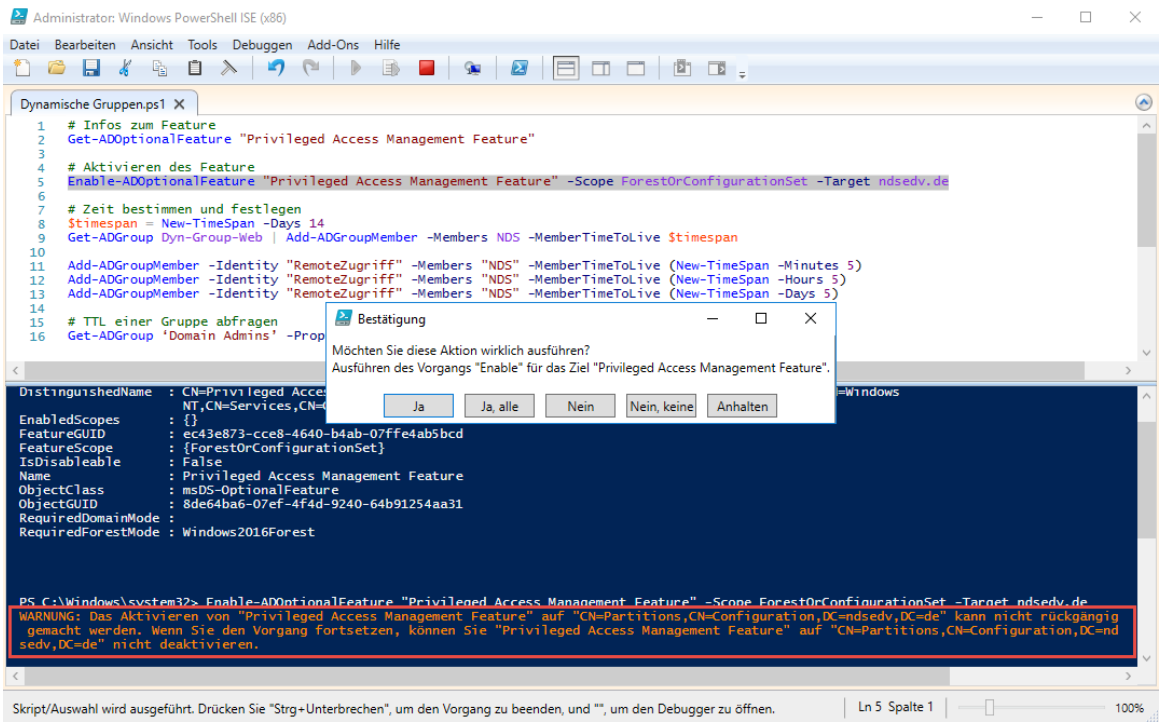
Get-ADOptionalFeature "Privileged Access Management Feature"



Aktivieren als nächstes das Feature mithilfe der Powershell:

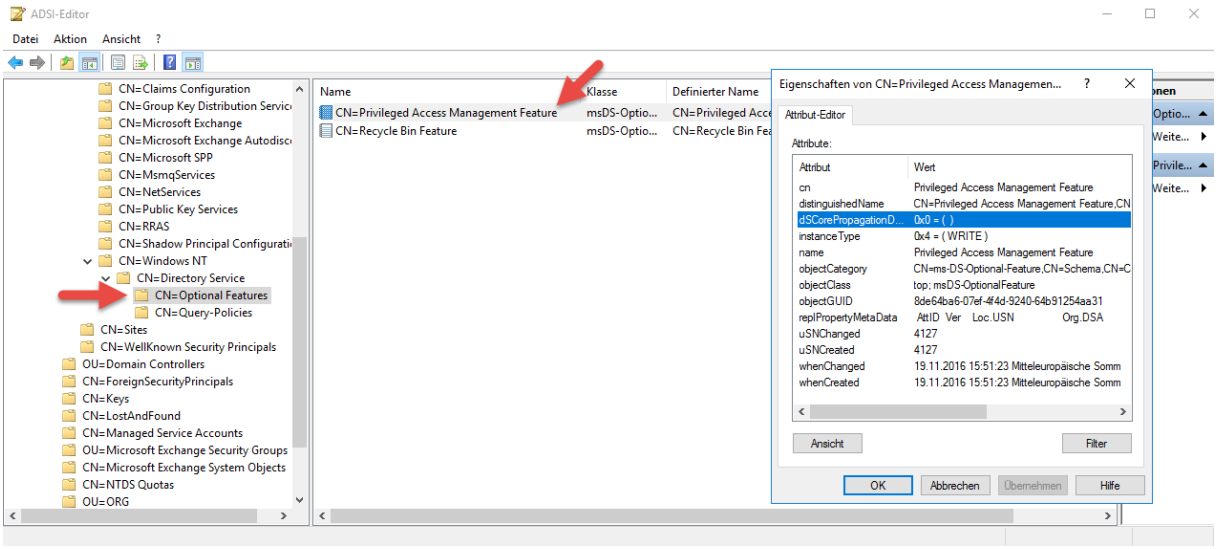
Enable-ADOptionalFeature "Privileged Access Management Feature" -Scope ForestOrConfigurationSet -Target ndsedv.de

Bitte beachtet den Hinweis!



Server 2016 - Privileged Access Management

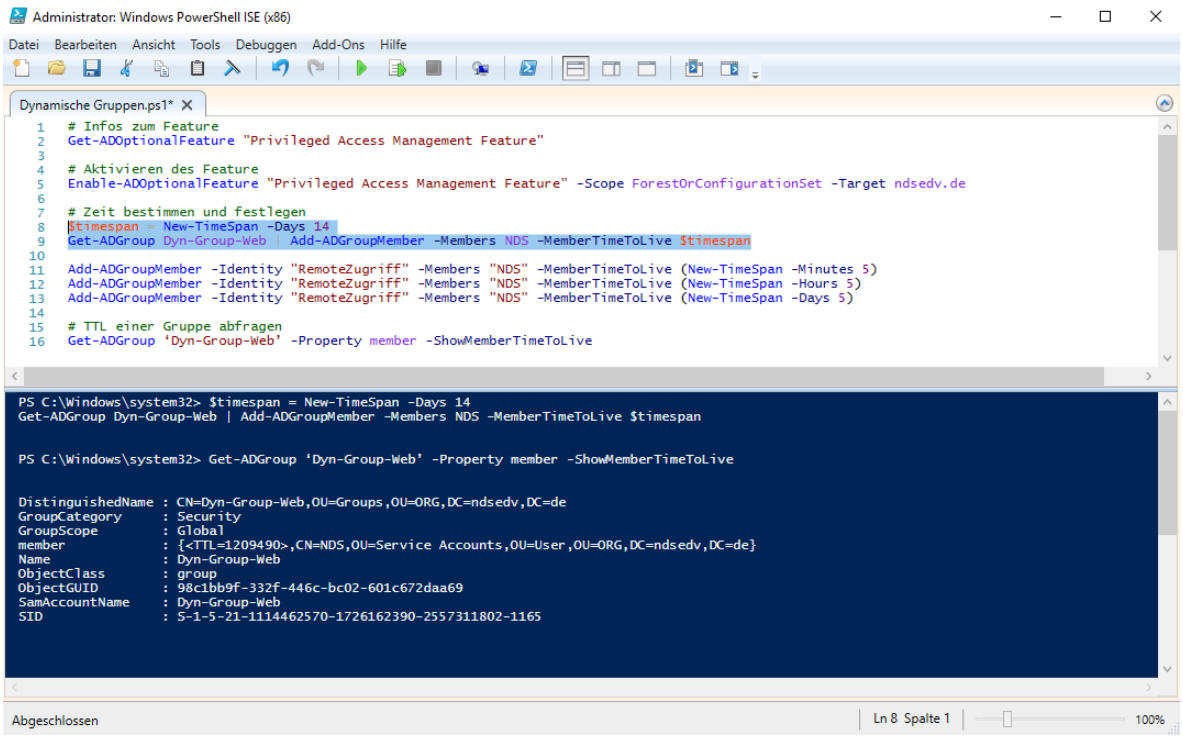
Starten den ADSI-Editor und gucken mal in die Services:



Fügen den User NDS nun der Gruppe Dyn-Group-Web für 14 Tage hinzu:

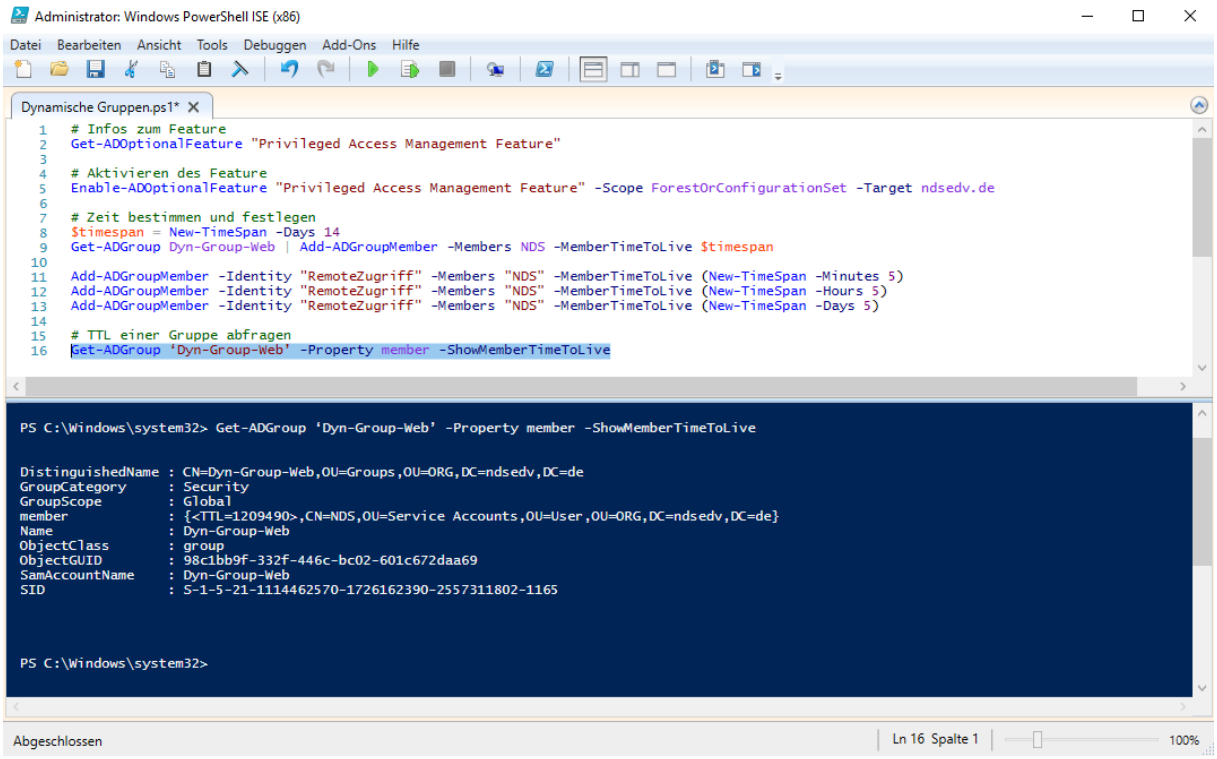
```
$timespan = New-TimeSpan -Days 14
```

```
Get-ADGroup Dyn-Group-Web | Add-ADGroupMember -Members NDS -MemberTimeToLive $timespan
```



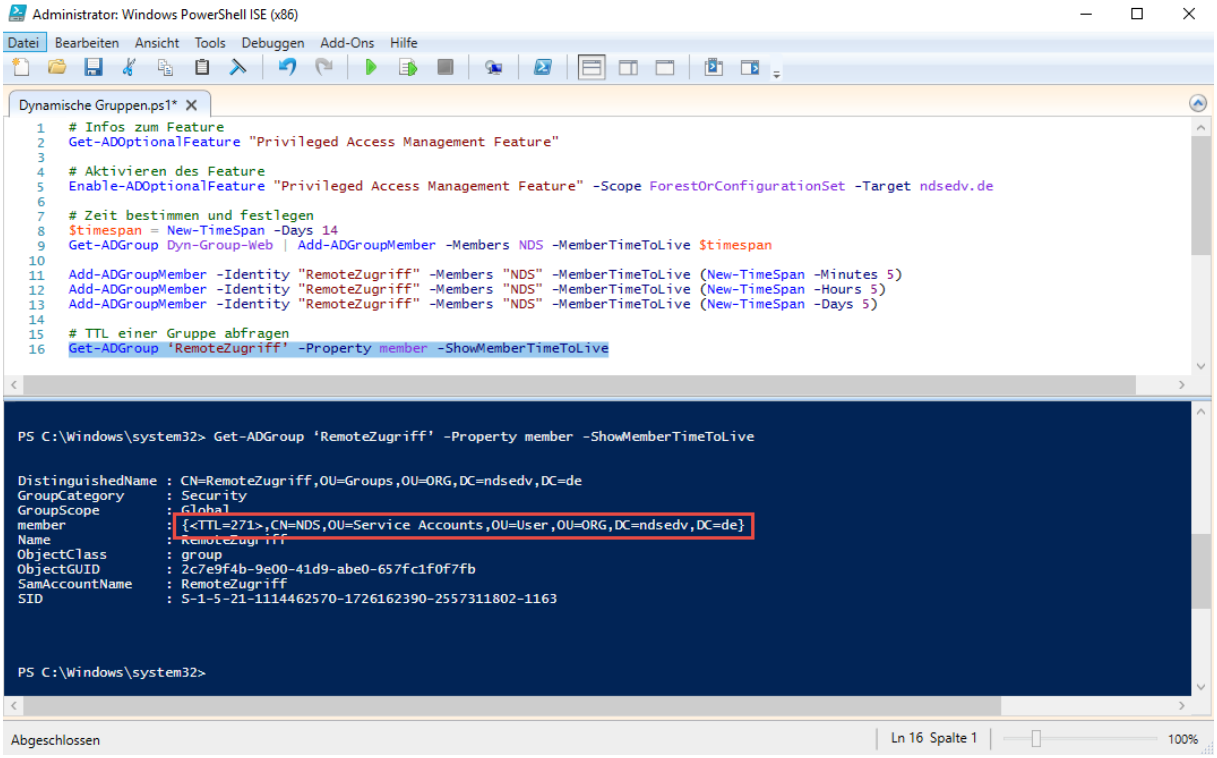
Fragen die verbleibende Mitgliedschaft ab:

Get-ADGroup 'Dyn-Group-Web' -Property member -ShowMemberTimeToLive



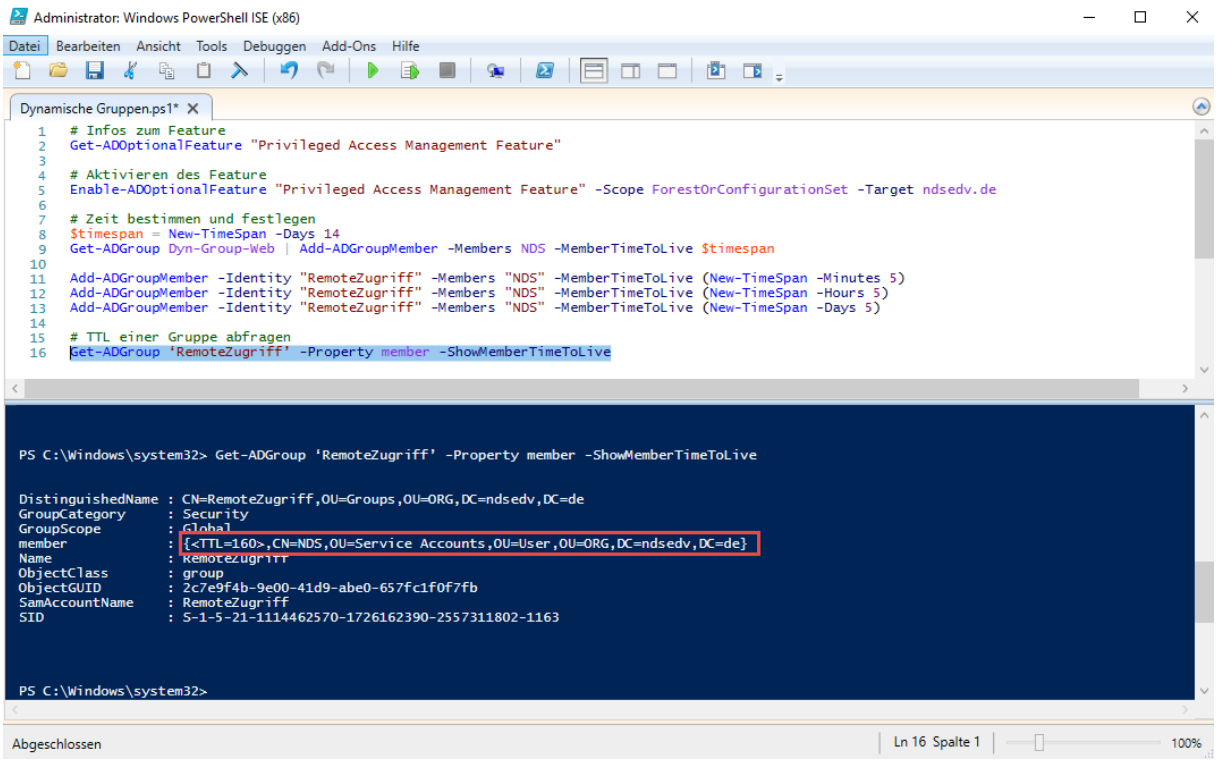
Nun wird der User NDS noch Mitglied der Gruppe RemoteZugriff und zwar für 5 Minuten:

Add-ADGroupMember -Identity "RemoteZugriff" -Members "NDS" -MemberTimeToLive (New-TimeSpan -Minutes 5)

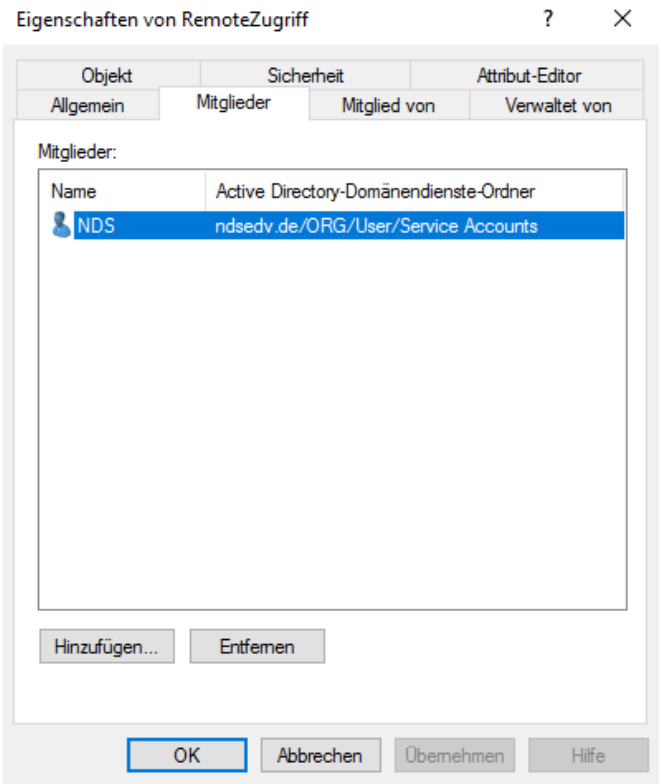


Wir sehen das die TTL abläuft:

Get-ADGroup 'RemoteZugriff' -Property member -ShowMemberTimeToLive



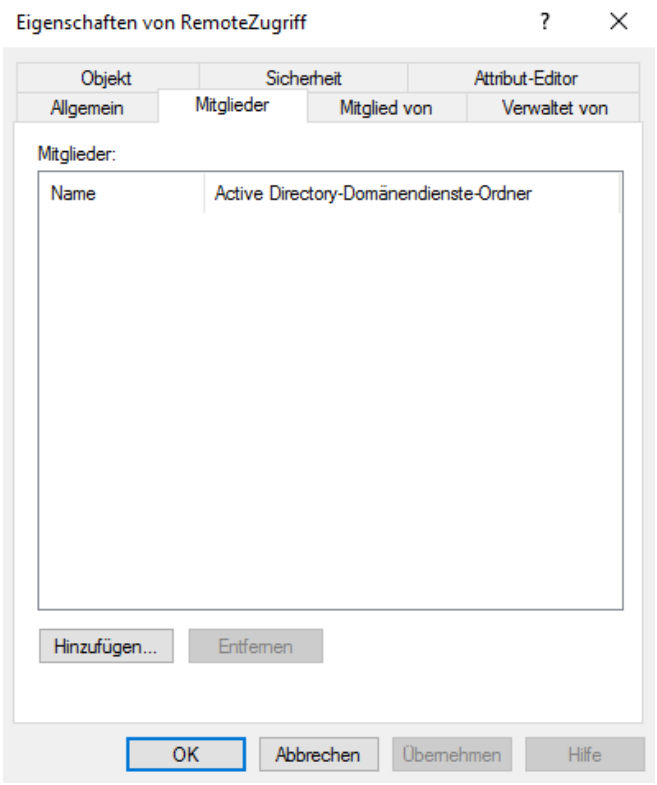
Der User NDS ist noch Mitglied der Gruppe RemoteZugriff:



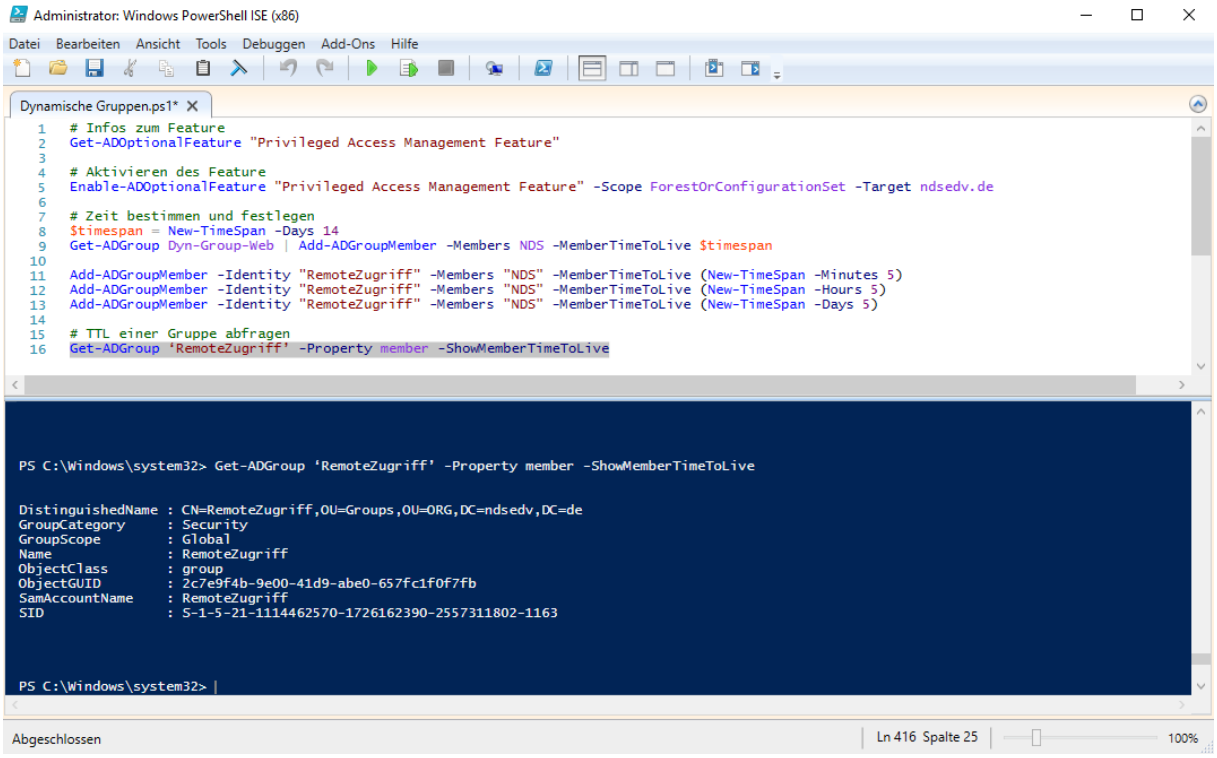
Nach verbleibenden Sekunden wir der User NDS automatisch der Gruppe entzogen:

```
PS C:\Windows\system32> Get-ADGroup 'RemoteZugriff' -Property member -ShowMemberTimeToLive


DistinguishedName : CN=RemoteZugriff,OU=Groups,OU=ORG,DC=ndsedv,DC=de
GroupCategory     : Security
GroupScope        : Global
member            : {<TTL=1>,CN=NDS,OU=Service Accounts,OU=User,OU=ORG,DC=ndsedv,DC=de}
Name              : RemoteZugriff
ObjectClass       : group
ObjectGUID        : 2c7e9f4b-9e00-41d9-abe0-657fc1f0f7fb
SamAccountName    : RemoteZugriff
SID               : S-1-5-21-1114462570-1726162390-2557311802-1163
```



Eine weitere Abfrage zeigt nun keine Mitglieder mehr an. Das Attribut Member ist außerdem nicht mehr vorhanden.



Hinweis:

Zur Erhöhung der Sicherheit hat Microsoft das Kerberos Ticket an die TTL angepasst. Das bedeutet, wenn ein AD Benutzer auf Zeit, Mitglied einer Gruppe ist, läuft nach der TTL das gesamte Kerberos Ticket ab.

Powershell:

```
# Infos zum Feature
Get-ADOptionalFeature "Privileged Access Management Feature"

# Aktivieren des Feature
Enable-ADOptionalFeature "Privileged Access Management Feature" -Scope
ForestOrConfigurationSet -Target ndsedv.de

# Zeit bestimmen und festlegen
$timespan = New-TimeSpan -Days 14
Get-ADGroup Dyn-Group-Web | Add-ADGroupMember -Members Test -MemberTimeToLive
$timespan

Add-ADGroupMember -Identity "RemoteZugriff" -Members "NDS" -MemberTimeToLive (New-
TimeSpan -Minutes 5)
Add-ADGroupMember -Identity "RemoteZugriff" -Members "NDS" -MemberTimeToLive (New-
TimeSpan -Hours 5)
Add-ADGroupMember -Identity "RemoteZugriff" -Members "NDS" -MemberTimeToLive (New-
TimeSpan -Days 5)

# TTL einer Gruppe abfragen
Get-ADGroup 'Dyn-Group-Web' -Property member -ShowMemberTimeToLive
```

Jetzt könnte man das Thema temporäre Mitgliedschaften weiter ausbauen und mit der Funktion Shadow Principals und MIM-PAM verschmelzen.

Shadow Principals

Shadow Principals ist ein weiterer Teil der PAM Funktion wie die eben beschriebenen temporären Mitgliedschaften.

Shadow Principals repräsentieren AD Objekte aus einer vertrauten Domäne. Es kann für eine Gruppe, einen Benutzer oder für ein Computerkonto einstehen.

Angenommen wir haben 2 AD Forests die sich vertrauen. Ein Forest in dem wir alle Admins pflegen (Admin-Forest) und ein Forest in dem die Produktionssysteme stehen (Prod-Forest).

Als nächstes legen wir im Admin-Forest Shadow-Principals an, die die SID der Domain-Admin Gruppe aus dem Prod-Forest tragen. Nun wird Benutzer1 im Admin-Forest dem „memberof" Attribut des Shadow Principals hinzugefügt. Meldet sich nun der Benutzer1 an einer Ressource im Prod-Forest an, führt er die SID der lokalen Domain-Admins im Kerberos Ticket mit und kann etwaige privilegierte Tätigkeiten ausführen.

Das Prinzip ist klar, oder?

Benutzer1 hat keinen Account in dem Prod-Forest, kann aber mittels der Shadow Principals administrative Rechte zugesprochen bekommen.

MIM-PAM

Um das Ganze noch weiter rund zu machen und überwachen zu können, wer wann und wie lange erhöhte Rechte bekommen soll, kommt MIM-PAM ins Spiel. MIM steht für Microsoft Identity Manager und PAM ist eine Funktion von MIM.

Mit diesen zusammenzuführenden Technologien erzeugen wir die Just-In-Time Administration. Es werden Rollen definiert, die wiederum geregelt werden, wer sich wann welche Privilegien anfordern darf.

Das Ganze sieht dann in etwa so aus.

Als Beispiel könnte es eine Rolle „Domain Admins" geben, welche die Benutzer zum Shadow Principal „Domain Administratoren" hinzufügt. Die Rolle darf von den Benutzern Markus und Philipp zwischen 6 und 18 Uhr angefordert werden. Der Benutzer Joern muss die Anfrage genehmigen. Die Rolle hat eine Laufzeit von 45 Minuten.

Wenn ich Zeit habe, werde ich das Ganze noch zu Papier bringen.