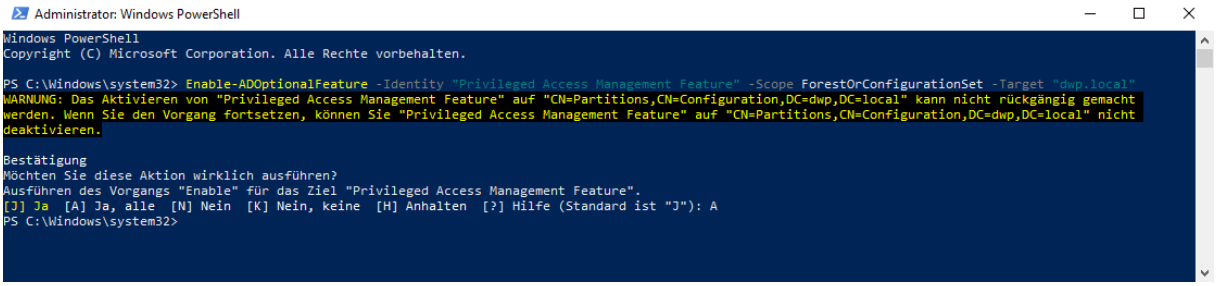
Lokaler Admin auf Zeit

Anlehned an diese Dokumentation zeige ich den flächendeckenden roll-out einer Möglichkeit, Admins auf Zeit zu managen.

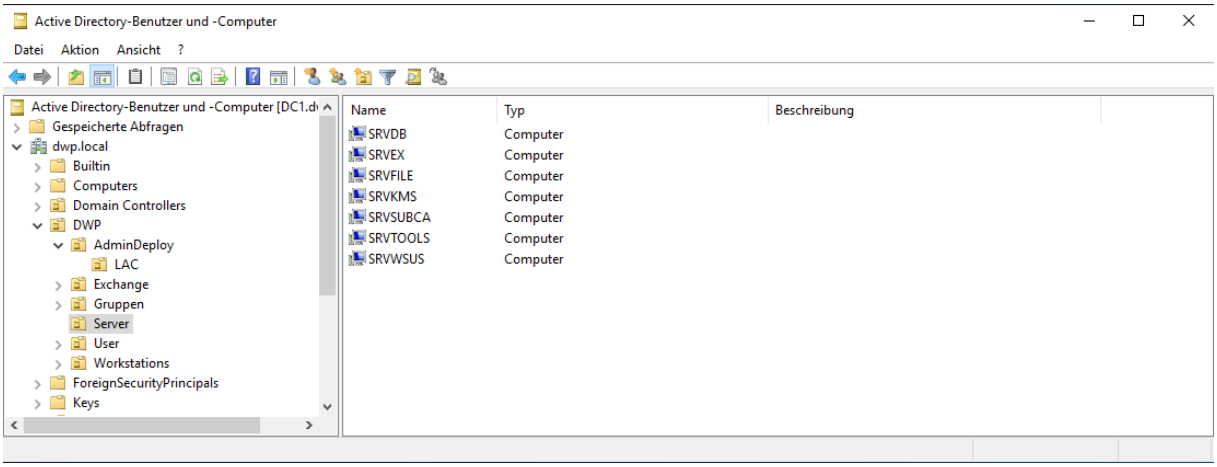
https://www.der-windows-papst.de/2017/04/17/server-2016-privileged-access-management-berechtigung-auf-zeit/

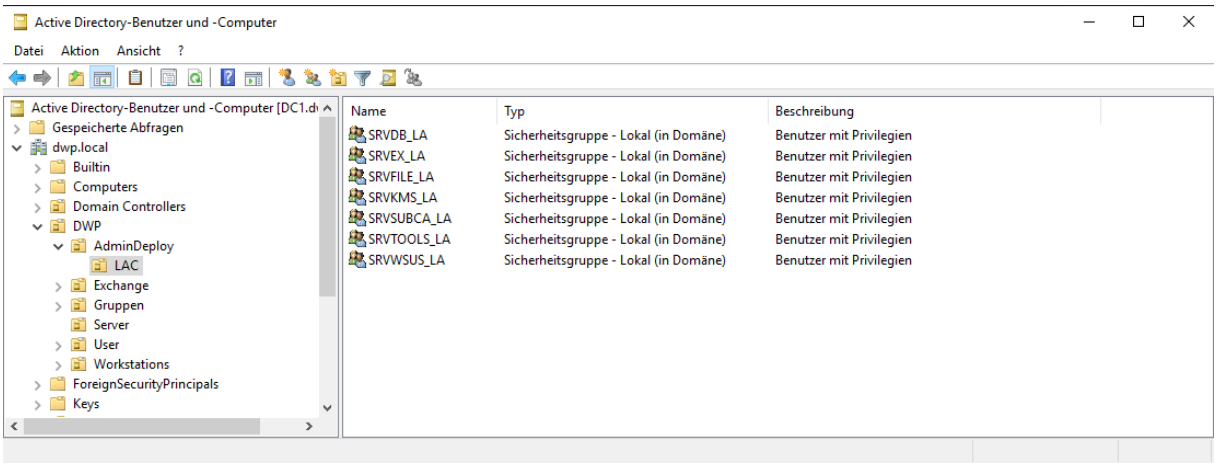
Zuerst installieren wir auf einem DC das Feature PAM.

```
Enable-ADOptionalFeature -Identity "Privileged Access Management Feature" -Scope ForestOrConfigurationSet -Target "dwp.local"
```



Dann erstellen wir für jeden Server eine domänen-lokale Sicherheitsgruppe zur Steuerung der lokalen Admins.





Lokaler Admin auf Zeit

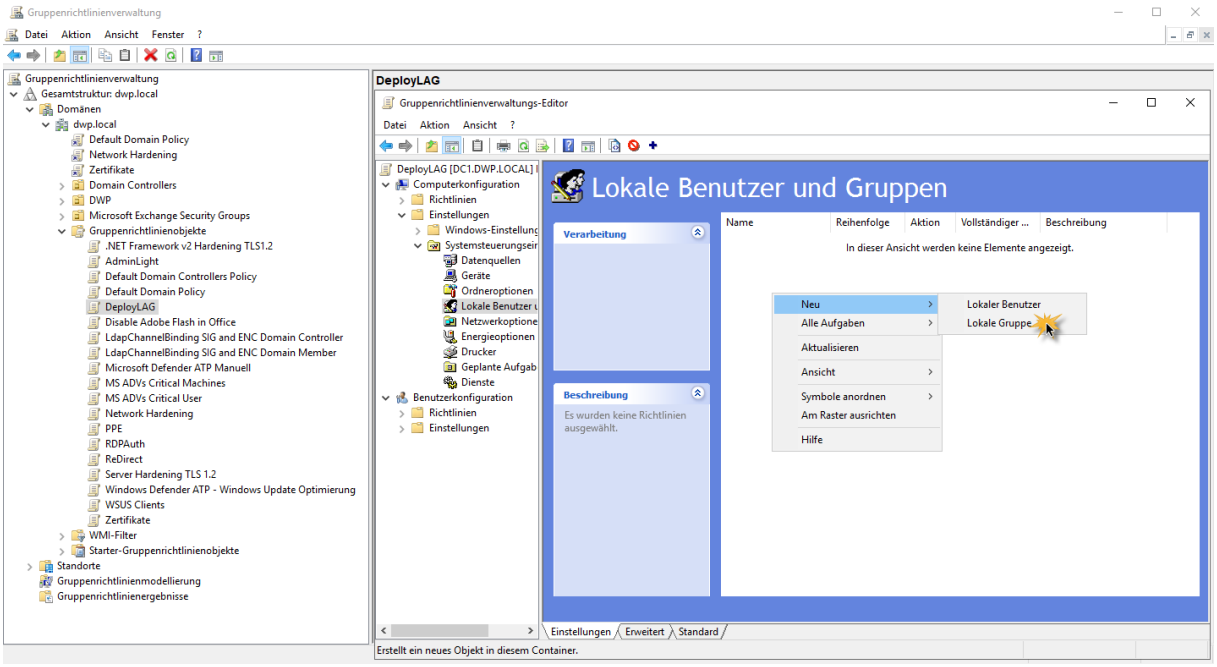
Gerne auch mit der Powershell:

```
$Clients = ($Clients = Get-ADComputer -Filter * -SearchBase
"OU=Server,OU=DWP,DC=dwp,DC=local").Name
$Groups = $NULL
foreach ($Client in $Clients) {
[Array]$Groups += $Client + "_LA"}
foreach ($Group in $Groups) {
$NewGroup = New-ADGroup -Name $Group -Path
"OU=LAC,OU=AdminDeploy,OU=DWP,DC=dwp,DC=local" -GroupCategory Security -
GroupScope DomainLocal -Description "Benutzer mit Privilegien"}
```

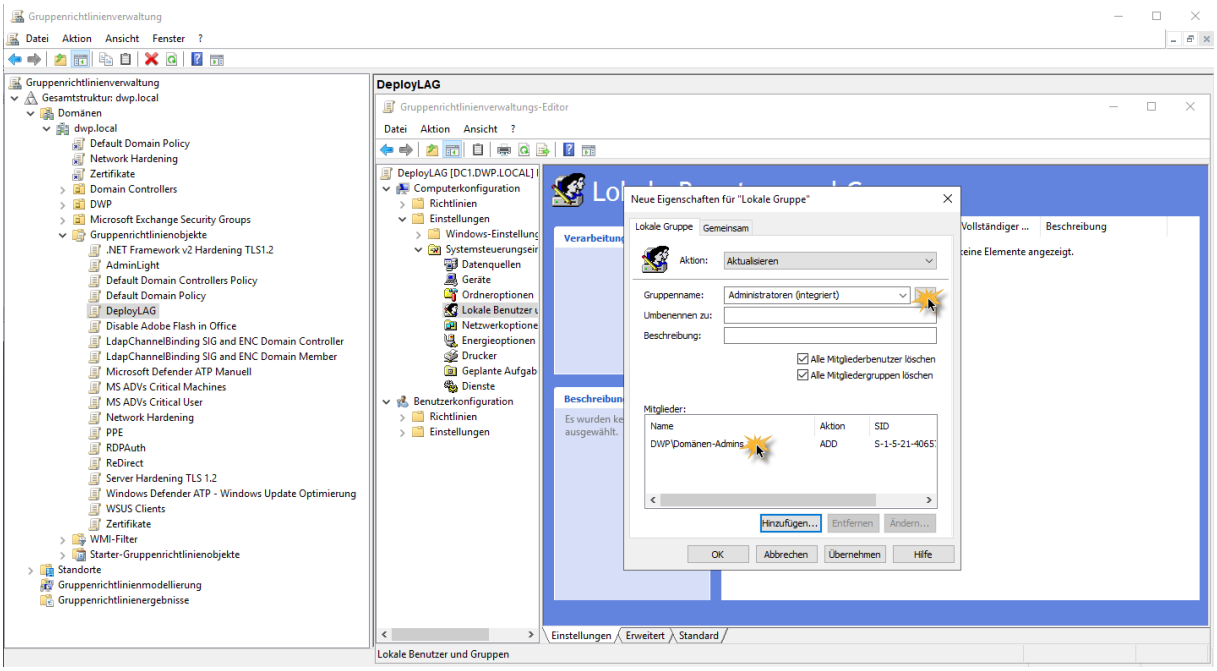
Gruppenrichtlinie erstellen:

Nun erstellen wir das erste Gruppenrichtlinienobjekt namens DeployLAG. LAG steht für lokale Admin Gruppe.

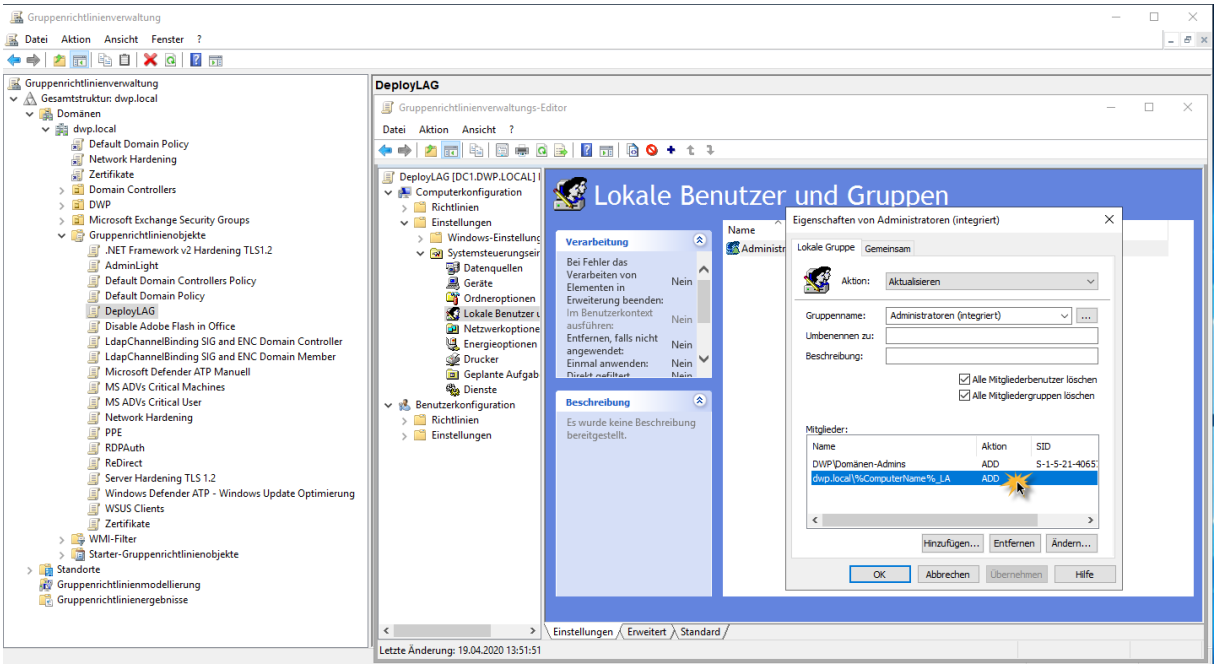
Domänen-Admins bekommen administrativen Zugriff auf alle Server, indem sie Mitglied der Gruppe Administratoren bleiben. Alle anderen werden entfernt.



Lokaler Admin auf Zeit

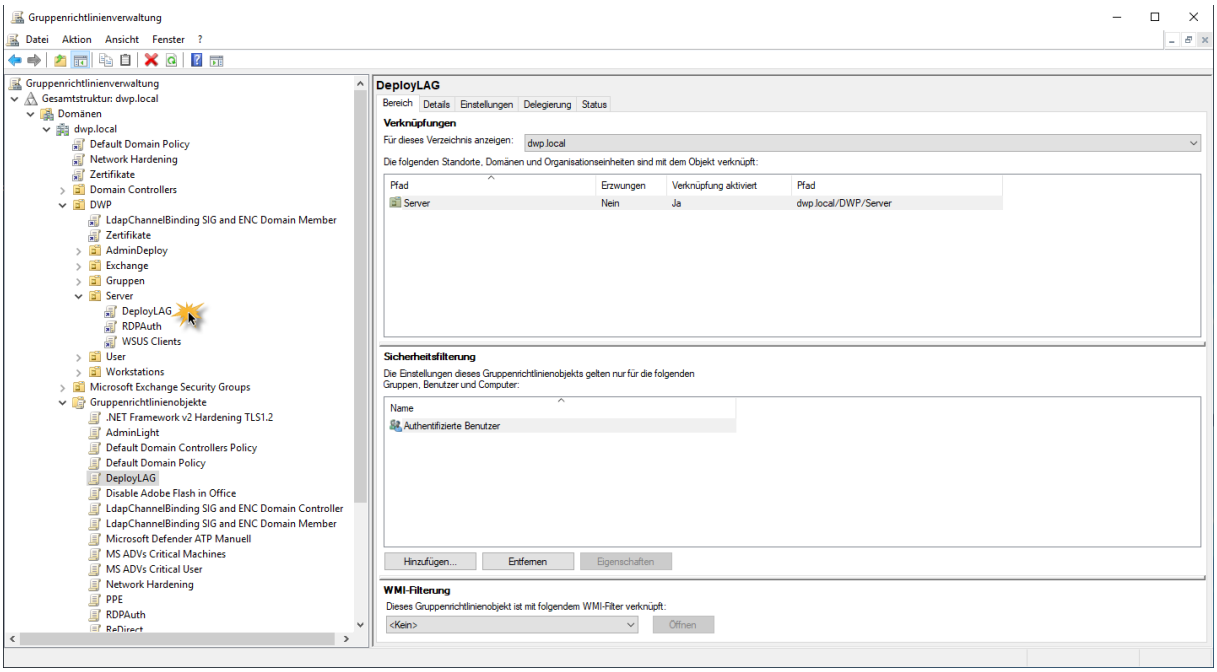


Fügen jedem Server die zuvor erstellte eigene Sicherheitsgruppe hinzu.



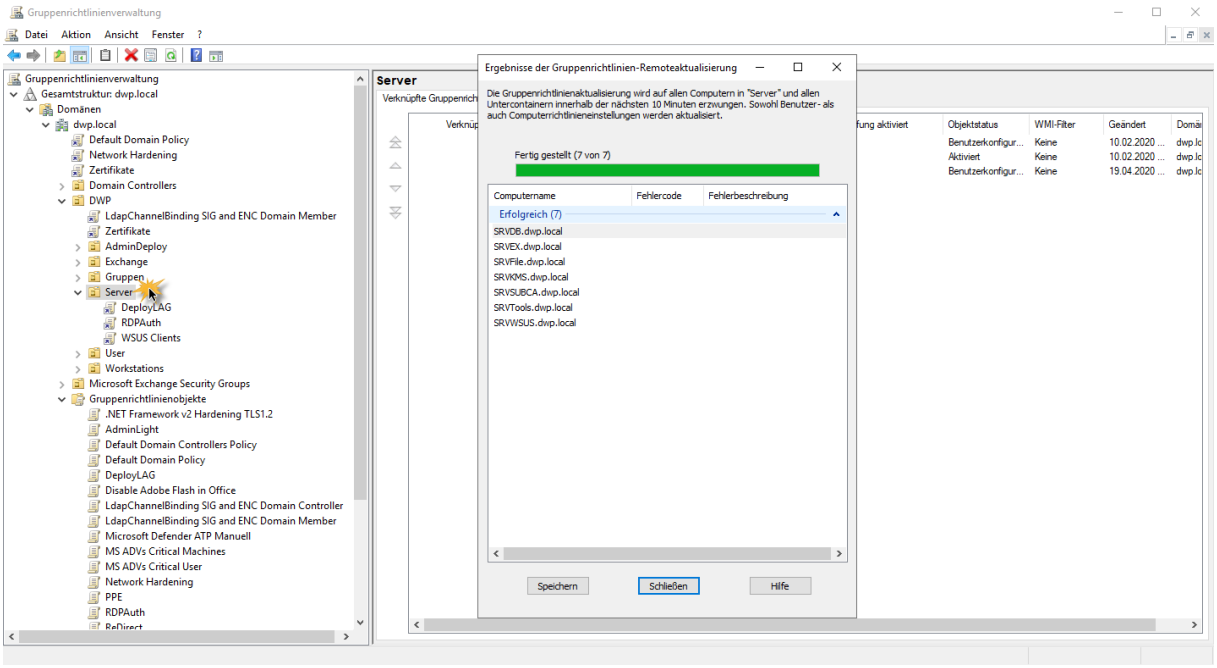
Lokaler Admin auf Zeit

Verknüpfen das neue Gruppenrichtlinienobjekt mit der OU = Server.

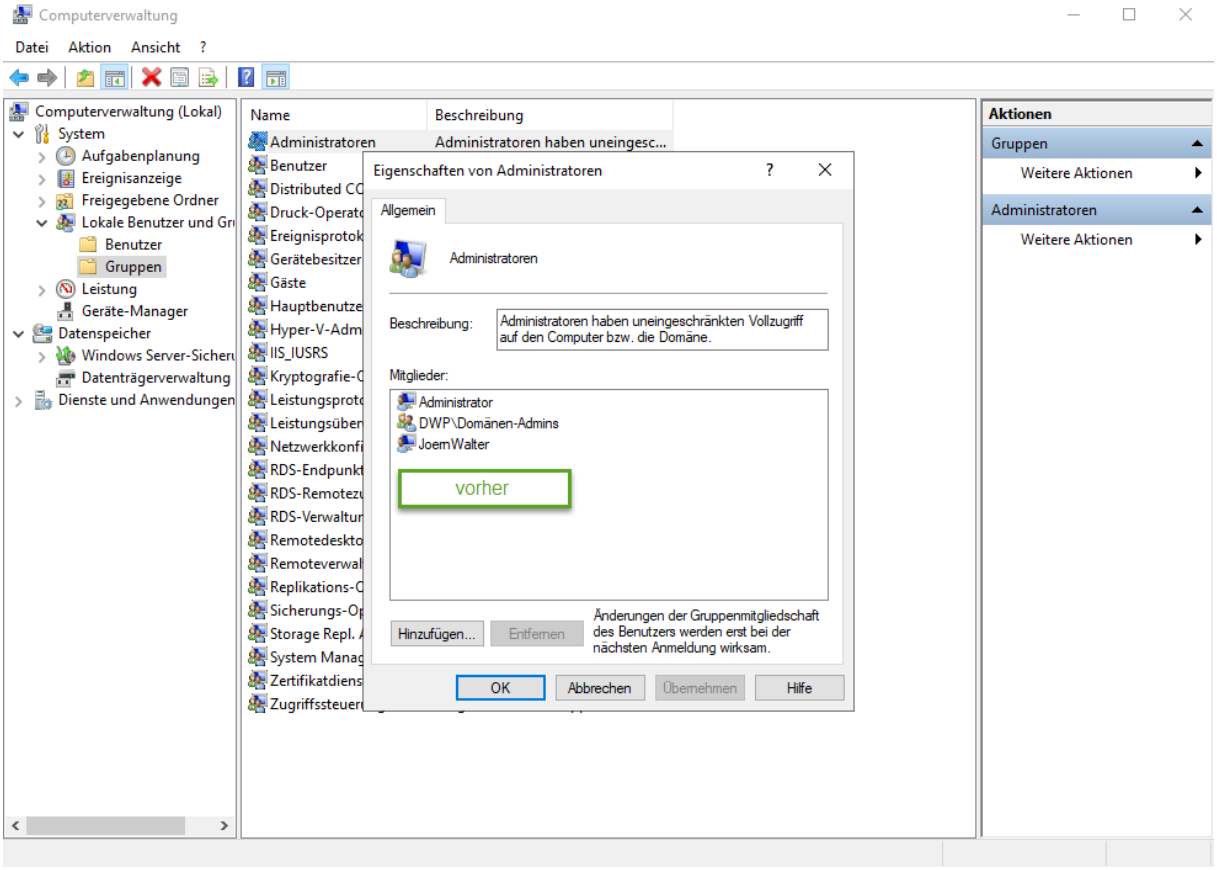


Führen ein Gruppenrichtlinienupdate aus:

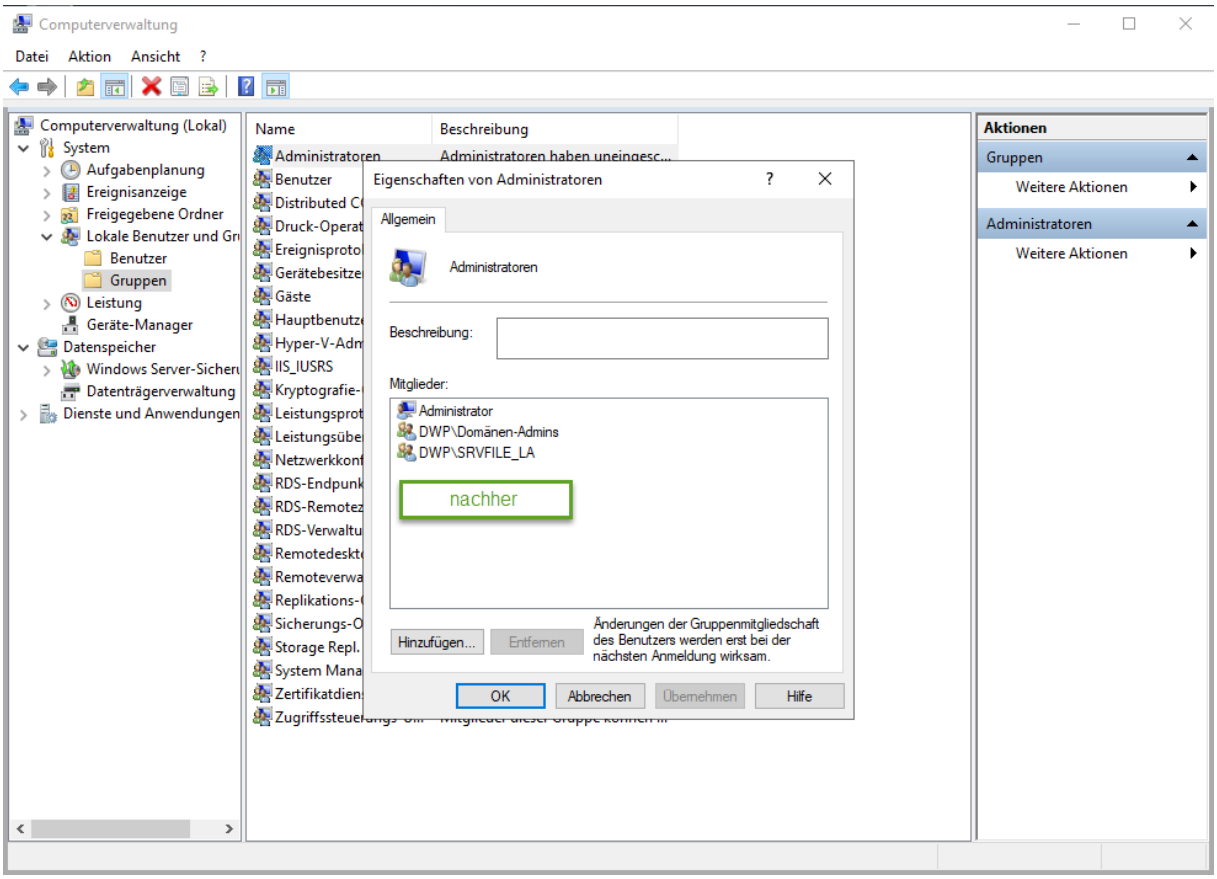
Innerhalb der nächsten 10 Minuten wird die individuelle Sicherheitsgruppe (Servername_LA) Mitglied der Gruppe der lokalen Administratoren sein.



Lokaler Admin auf Zeit



Nachdem die Gruppenrichtlinie angewendet wurde.

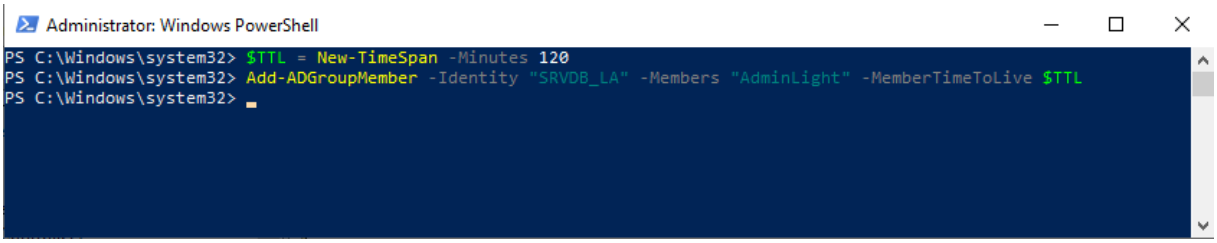


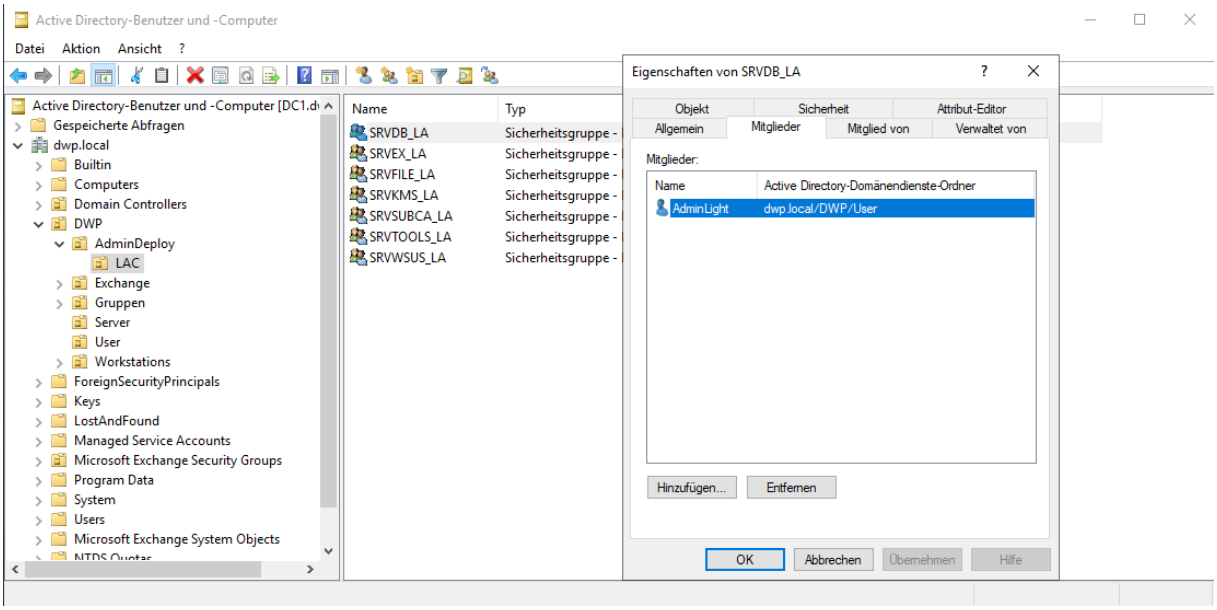
Erstellt von Jörn Walter **19.04.2020**

Lokaler Admin auf Zeit

Jetzt bekommt der User AdminLight exemplarisch 2 Stunden lokale Admin-Rechte auf Server SRVDB.

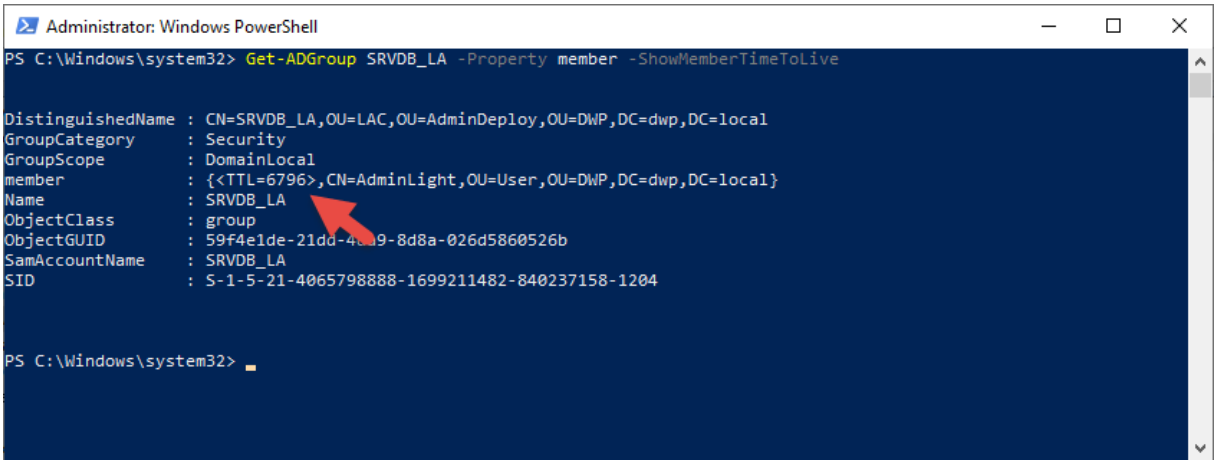
```
$TTL = New-TimeSpan -Minutes 120
Add-ADGroupMember -Identity "SRVDB_LA" -Members "AdminLight" -MemberTimeToLive $TTL
```





Wie lange hat der Benutzer AdminLight noch lokale Admin-Rechte?
Zeit in Sekunden, noch 113 Minuten verbleiben.

```
Get-ADGroup SRVDB_LA -Property member -ShowMemberTimeToLive
```



Bitte beachtet bei der Umseztung, das alle bisherigen lokalen Admins entfernt werden!

Erstellt von Jörn Walter **19.04.2020**