



Lokaler Admin auf Zeit

Anlehnend 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"

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Windows\system32> Enable-ADOptionalFeature -Identity "Privileged Access Management Feature" -Scope ForestOrConfigurationSet -Target "dwp.local"
WARNUNG: Das Aktivieren von "Privileged Access Management Feature" auf "CN=Partitions,CN=Configuration,DC=dwp,DC=local" kann nicht rückgängig gemacht werden. Wenn Sie den Vorgang fortsetzen, können Sie "Privileged Access Management Feature" auf "CN=Partitions,CN=Configuration,DC=dwp,DC=local" nicht deaktivieren.

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Enable" für das Ziel "Privileged Access Management Feature".
[Y] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "Y"): A
PS C:\Windows\system32>
```

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

The screenshot shows the Active Directory console with the 'dwp.local' domain selected. The left pane shows the tree structure, and the right pane shows a list of objects. The objects are organized into a table:

Name	Typ	Beschreibung
SRVDB	Computer	
SRVEX	Computer	
SRVFILE	Computer	
SRVKMS	Computer	
SRVSUBCA	Computer	
SRVTOOLS	Computer	
SRVWSUS	Computer	

Name	Typ	Beschreibung
SRVDB_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien
SRVEX_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien
SRVFILE_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien
SRVKMS_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien
SRVSUBCA_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien
SRVTOOLS_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien
SRVWSUS_LA	Sicherheitsgruppe - Lokal (in Domäne)	Benutzer mit Privilegien



Lokaler Admin auf Zeit

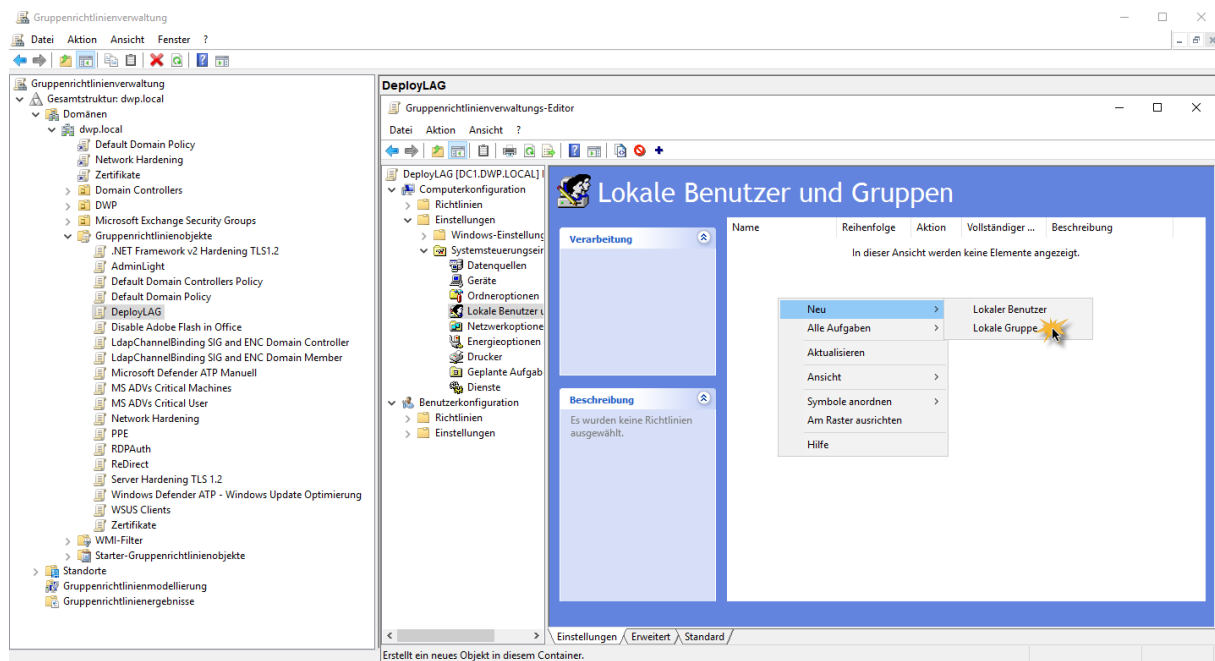
Gerne auch mit der Powershell:

```
$Clients = ($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:

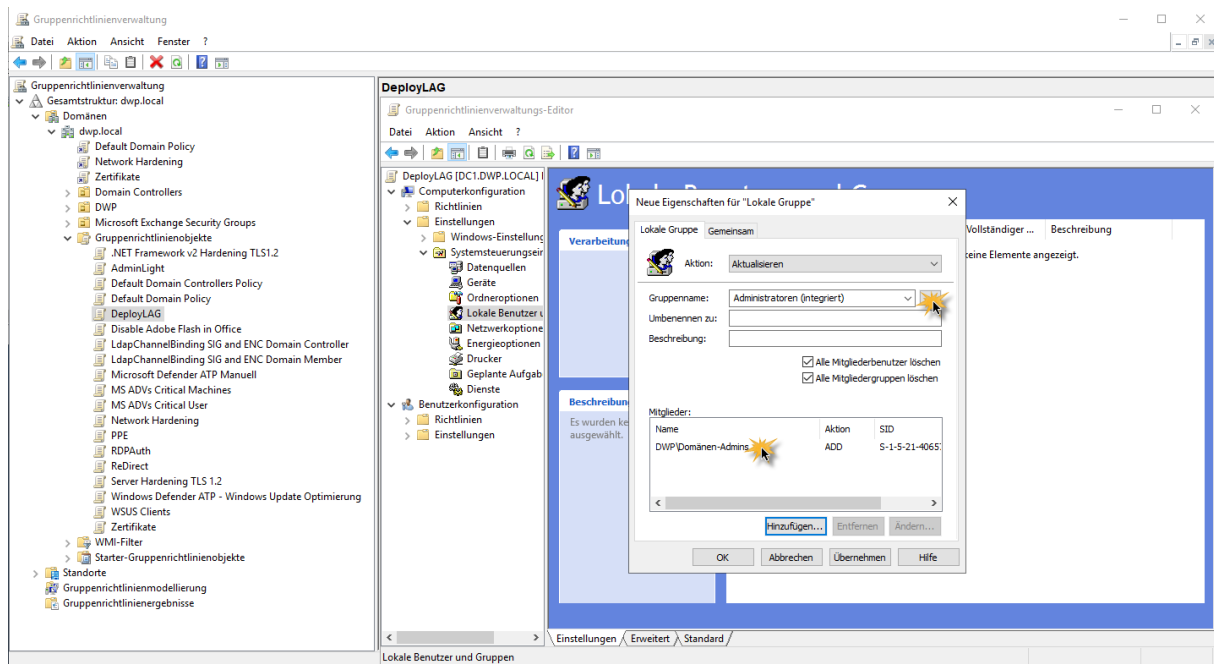
Nun erstellen wir das erste Gruppenrichtlinienobjekt namens DeployLAG. LAG steht für lokale Admin Gruppe.

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

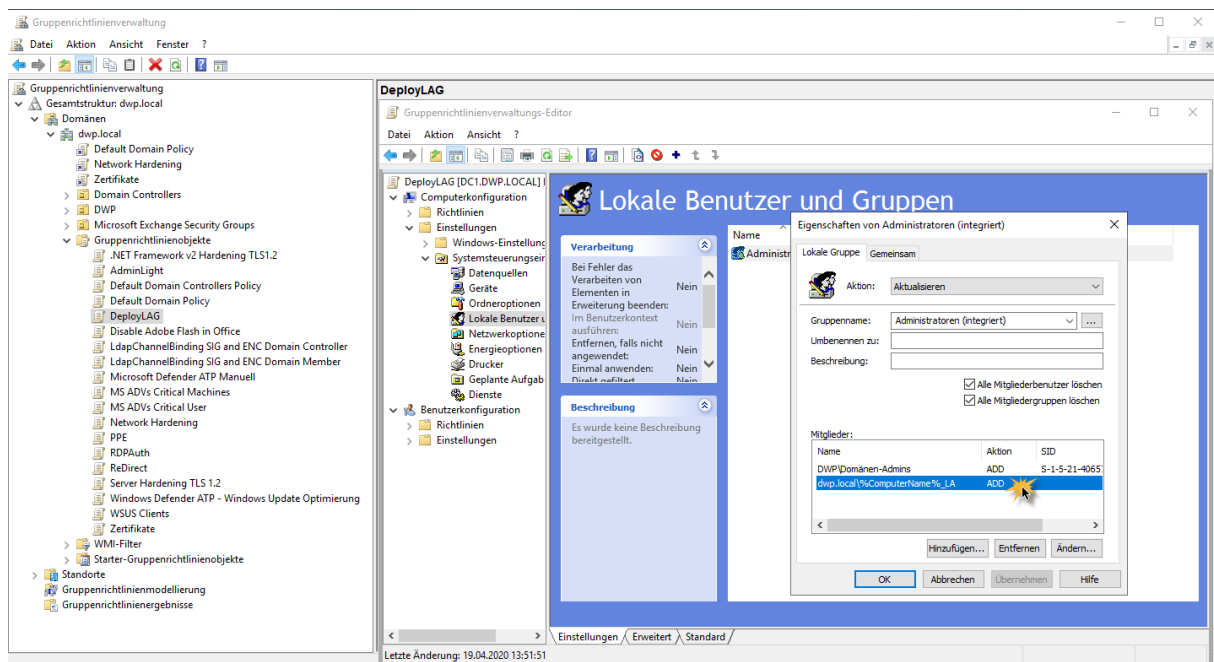




Lokaler Admin auf Zeit



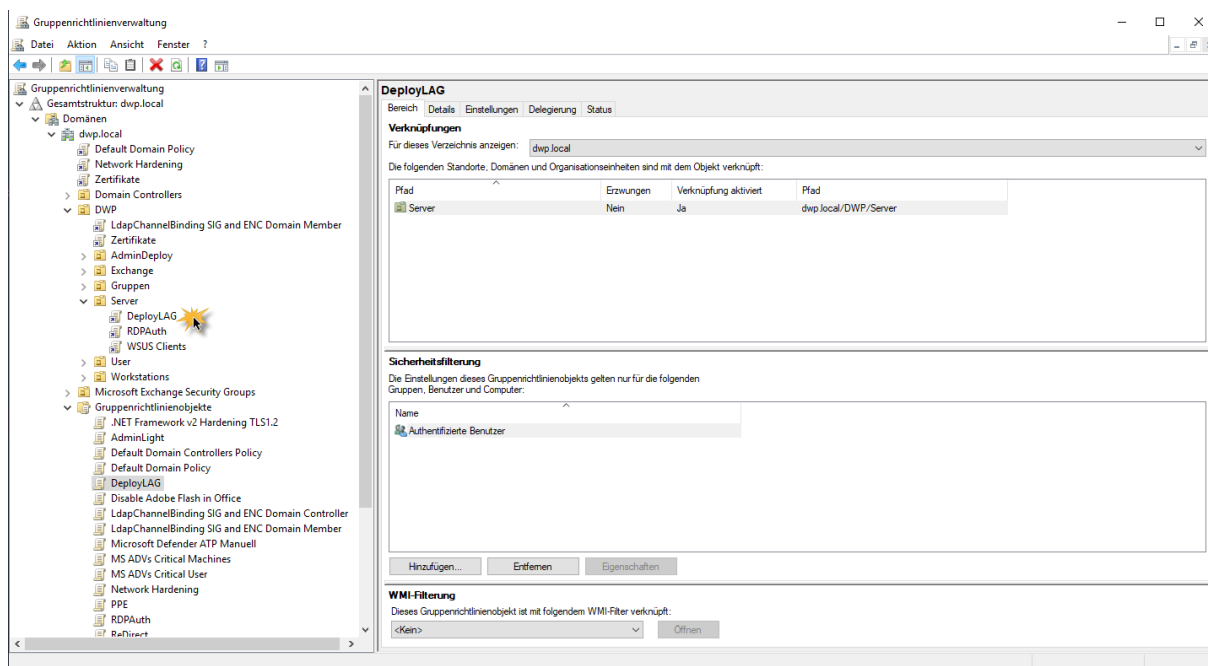
Fügen jedem Server die zuvor erstellte eigene Sicherheitsgruppe hinzu.





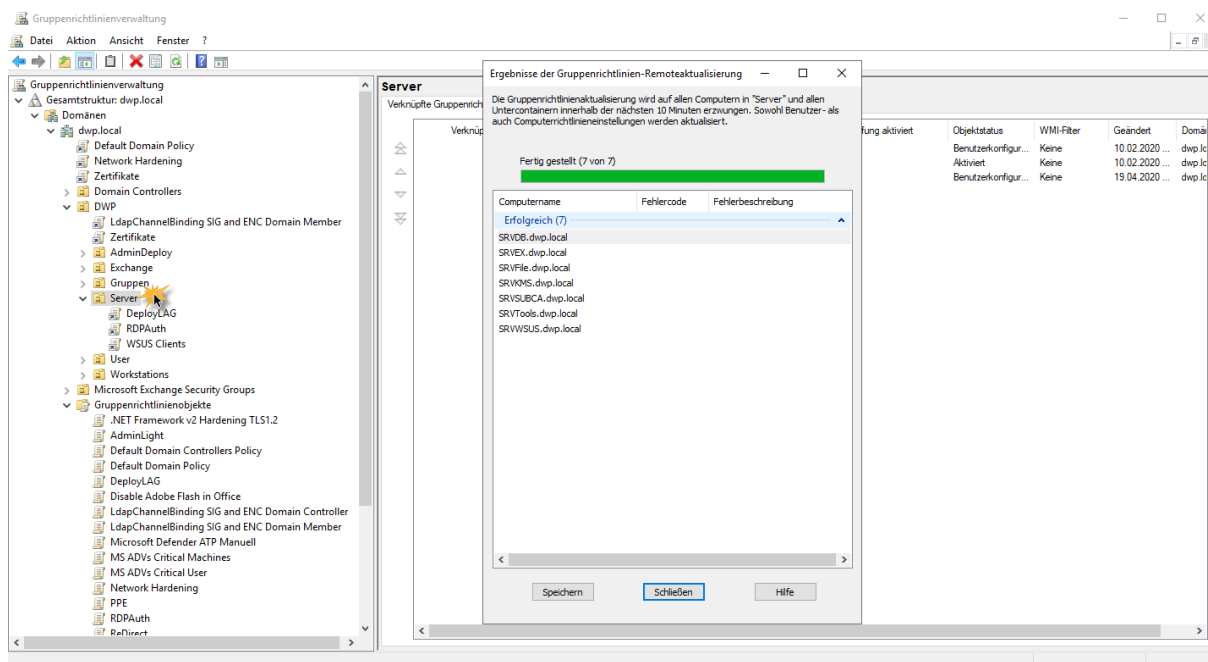
Lokaler Admin auf Zeit

Verknüpfen das neue Gruppenrichtlinienobjekt mit der OU = Server.



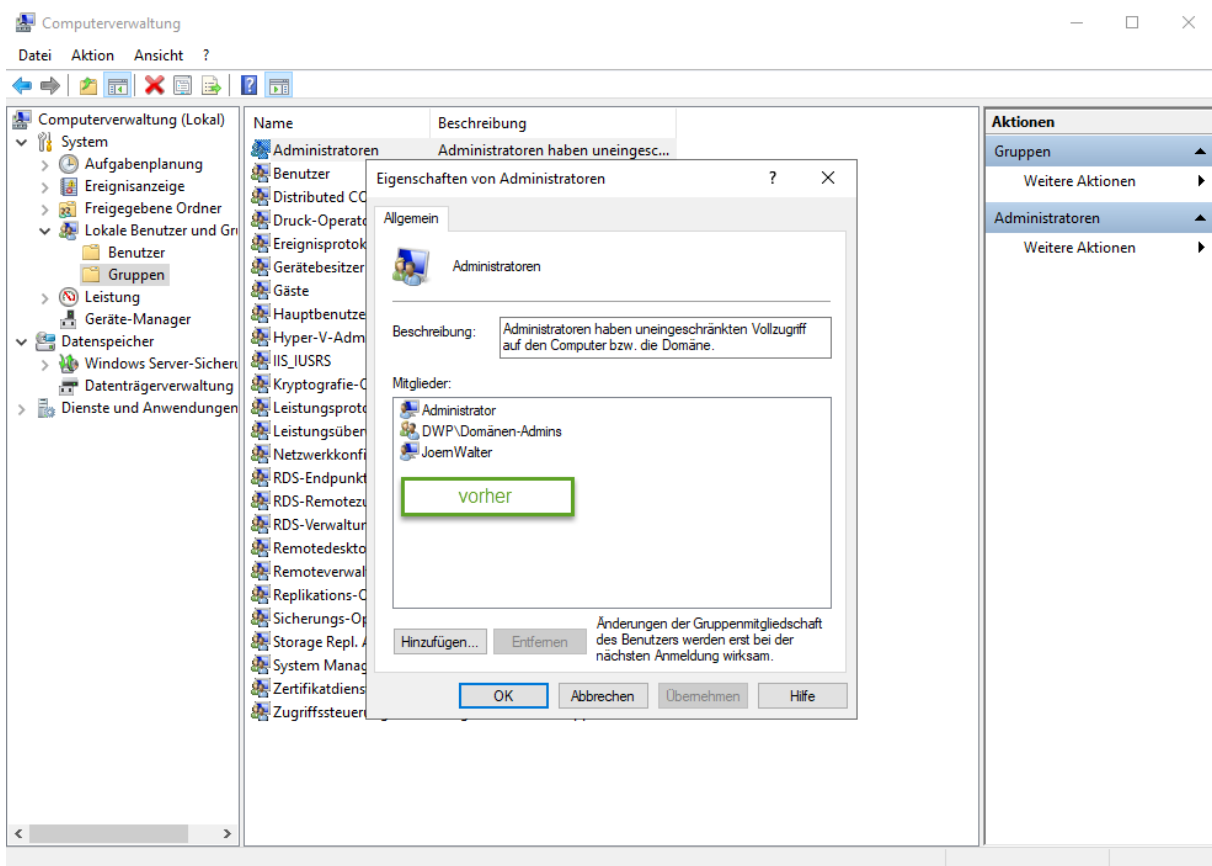
Führen ein Gruppenrichtlinienupdate aus:

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

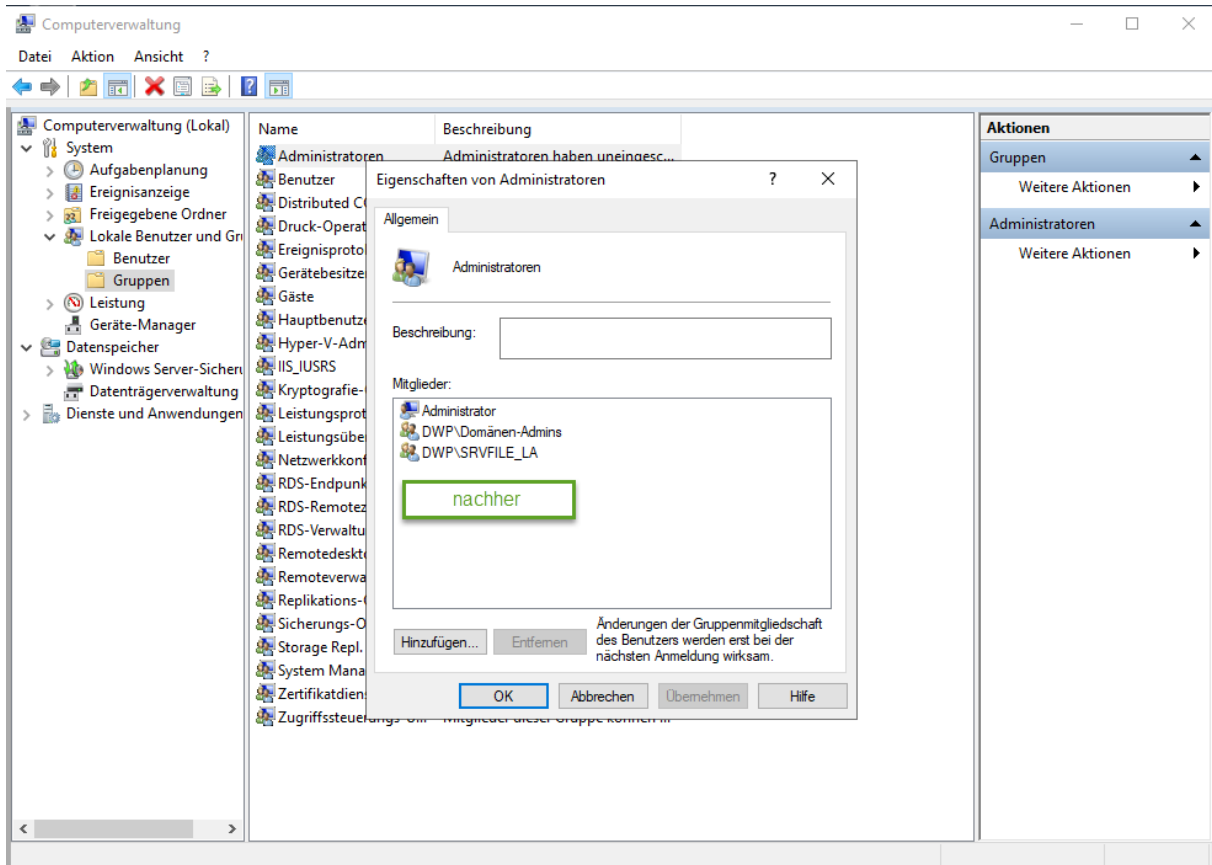




Lokaler Admin auf Zeit



Nachdem die Gruppenrichtlinie angewendet wurde.





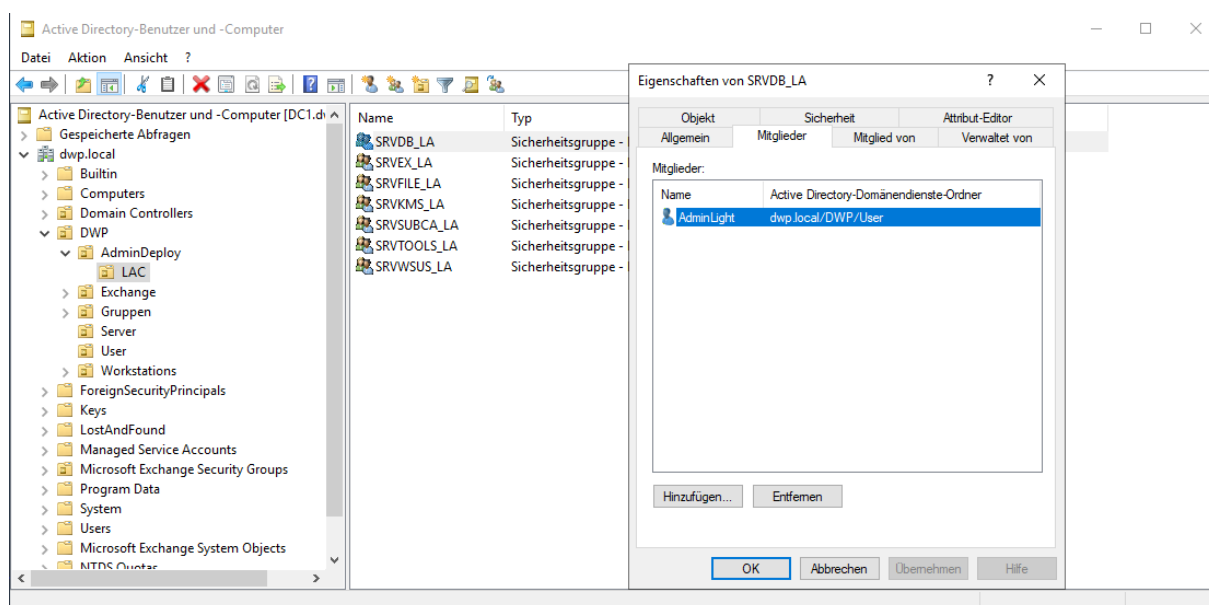
Lokaler Admin auf Zeit

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
```

```
Administrator: Windows PowerShell
PS C:\Windows\system32> $TTL = New-TimeSpan -Minutes 120
PS C:\Windows\system32> Add-ADGroupMember -Identity "SRVDB_LA" -Members "AdminLight" -MemberTimeToLive $TTL
PS C:\Windows\system32>
```



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

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

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-ADGroup SRVDB_LA -Property member -ShowMemberTimeToLive

DistinguishedName : CN=SRVDB_LA,OU=LAC,OU=AdminDeploy,OU=DWP,DC=dwp,DC=local
GroupCategory      : Security
GroupScope         : DomainLocal
member             : {{TTL=6796},CN=AdminLight,OU=User,OU=DWP,DC=dwp,DC=local}
Name               : SRVDB_LA
ObjectClass        : group
ObjectGUID         : 59f4e1de-21dd-4a09-8d8a-026d5860526b
SamAccountName     : SRVDB_LA
SID                : S-1-5-21-4065798888-1699211482-840237158-1204

PS C:\Windows\system32>
```

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