

29. März 2021

Noël Graf;Nils Yannik Stooss

Gibb

Lernjournal

Modul 123

Lernjournal

# Inhalt

[Inhalt 1](#_Toc74531046)

[Betriebssystem Installation 2](#_Toc74531047)

[Betriebssystem Installation 3](#_Toc74531048)

[Server einrichten 5](#_Toc74531049)

[Systemanforderungen 5](#_Toc74531050)

[Benutzer erstellen 5](#_Toc74531051)

[Netzwerkadapter konfigurieren 6](#_Toc74531052)

[Härten 7](#_Toc74531053)

[Hostname anpassen 8](#_Toc74531054)

[Datenträger einrichten 9](#_Toc74531055)

[AD DS 9](#_Toc74531056)

[DHCP 19](#_Toc74531057)

[DHCP Funktionen 19](#_Toc74531058)

[Ablauf 19](#_Toc74531059)

[Vorteile 20](#_Toc74531060)

[Nachteile 20](#_Toc74531061)

[Die Installationsanleitung für einen DHCP Servers 20](#_Toc74531062)

[DNS 23](#_Toc74531063)

[Subdomains und Zonen 23](#_Toc74531064)

[Die Installationsanleitung für einen DNS Servers 23](#_Toc74531065)

[Netzwerkadapter vorbereiten 23](#_Toc74531066)

[DNS-Rolle installieren 24](#_Toc74531067)

[DNS konfigurieren 24](#_Toc74531068)

[Forward-Lookupzone erstellen 25](#_Toc74531069)

[Zonenname: 25](#_Toc74531070)

[Reverse-Lookupzone konfigurieren 25](#_Toc74531071)

[Name der Reverse-Lookupzone: 25](#_Toc74531072)

[Weiterleitungen 25](#_Toc74531073)

[Eintrag in den Adaptereinstellungen anpassen 25](#_Toc74531074)

[Den Server im DNS eintragen 26](#_Toc74531075)

[Test DNS-Server-Konfiguration durch Server 26](#_Toc74531076)

[Anpassungen im DHCP-Server 27](#_Toc74531077)

[Dynamische DNS-Updates durch den DHCP-Server 27](#_Toc74531078)

[Die Host-Datei 27](#_Toc74531079)

[Die Hostdatei liegt unter: 27](#_Toc74531080)

[Nachteile: 27](#_Toc74531081)

[Gefahren: 27](#_Toc74531082)

[Berechtigungen und Freigaben 28](#_Toc74531083)

[Domänenlokalen, globalen und universellen Gruppen 28](#_Toc74531084)

[Wo ist eine überall Gruppe sichtbar? 28](#_Toc74531085)

[Wer kann in einer Gruppe Mitglied sein? 28](#_Toc74531086)

[Zugriffs- und Berechtigungskonzept erstellen 28](#_Toc74531087)

[Berechtigungskonzept auf Server implementieren 30](#_Toc74531088)

[Freigabeberechtigungen vs. NTFS-Berechtigungen 34](#_Toc74531089)

[Welches sind die Unterschiede zwischen den beiden Systemen? 34](#_Toc74531090)

[Welche Freigabeberechtigungen gibt es und was bedeuten diese? 34](#_Toc74531091)

[Welche Berechtigungen gelten schliesslich, wenn ein Benutzer über das Netzwerk auf einen freigegebenen Ordner zugreift? 35](#_Toc74531092)

[Best-Practices für Freigaben 35](#_Toc74531093)

[Wichtige Eingabebefehle 35](#_Toc74531094)

[CMD 35](#_Toc74531095)

[PowerShell 35](#_Toc74531096)

# Betriebssystem Installation

# Betriebssystem Installation

|  |  |
| --- | --- |
|  | Einstellungen auswählen und “Next”.  Die Sprache belassen wir auf English.  Time and currency format: German (Switzerland)  Das Tastaturlayout wird automatisch auf das korrekte umgestellt. |
|  | Auf “Install now” klicken. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Die gewünschte Serverinstallation wählen.  Bei dieser Installation darauf achten, dass du die Installation mit Desktop Experience auswählst. | | |
|  | Lizenzvereinbarungen akzeptieren und weiter mit „Next“. | | |
|  | Wähle die **Custom**-Installation (Custom: Install Windows only advanced) aus. | | |
|  | | Hier kann der gewünschte Datenspeicher gewählt werden. Wir werden die Installation auf die einzig im Moment vorhandene Disk vornehmen.  “Next” drücken.  (Die Festplattengrösse kann variieren.) |
|  | Warten bis die Installation fertig ist. | | |
|  | Setze das Administratorpasswort auf: Welcome$21 und klicke auf „Finish“. Melde dich anschliessend mit dem Administrator an.  CTRL + ALT + End | | |

# Server einrichten

## Systemanforderungen

Die Anforderungen sind:

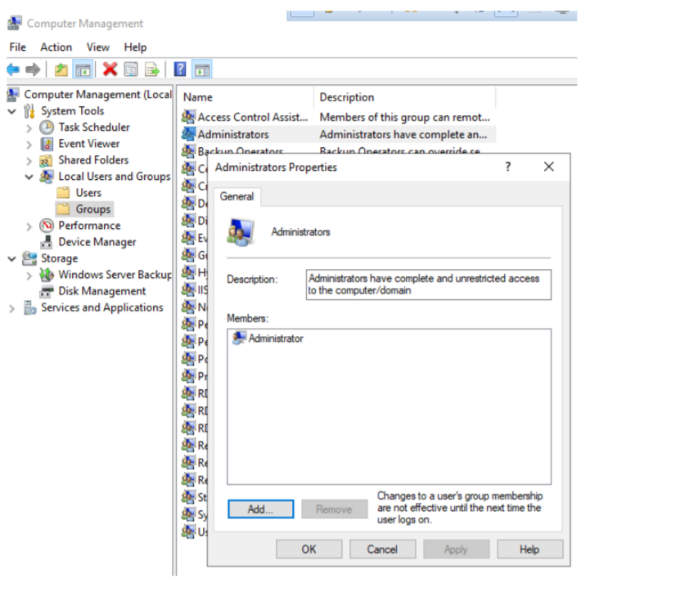
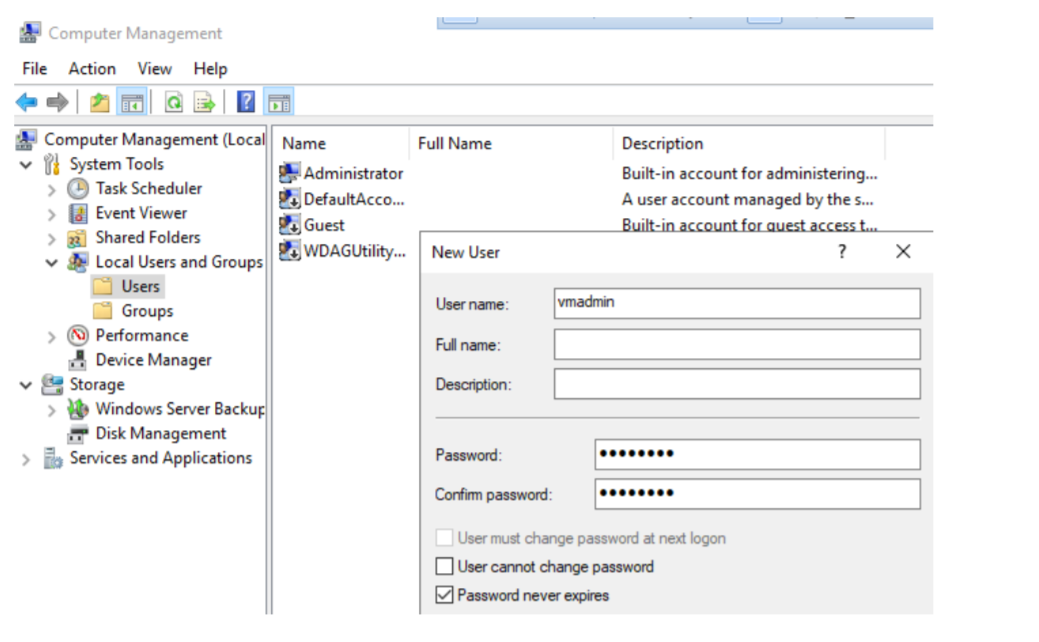
**Mindestanforderungen** **Virtueller Server**

16- 32 GB Speicher 60 GB Speicher

2Gb (0.5 GB für Core) 4 GB RAM

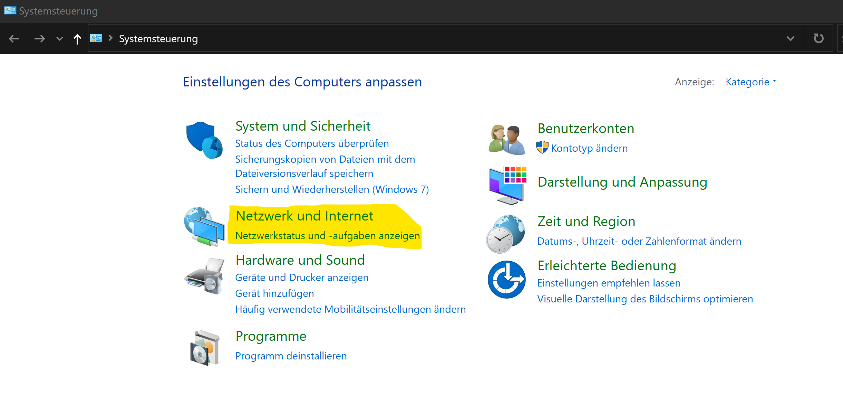
## Benutzer erstellen

Im Computer Management kann man Benutzer erstellen und sie auch direkt den Gruppen hinzufügen



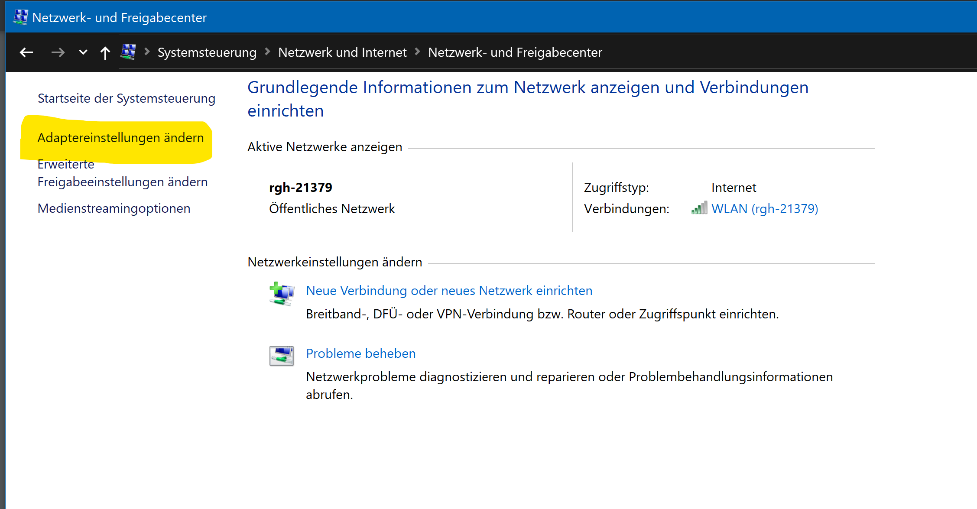
## Netzwerkadapter konfigurieren

Um den Netzwerkadapter zu konfigurieren, muss man in die Systemsteuerung

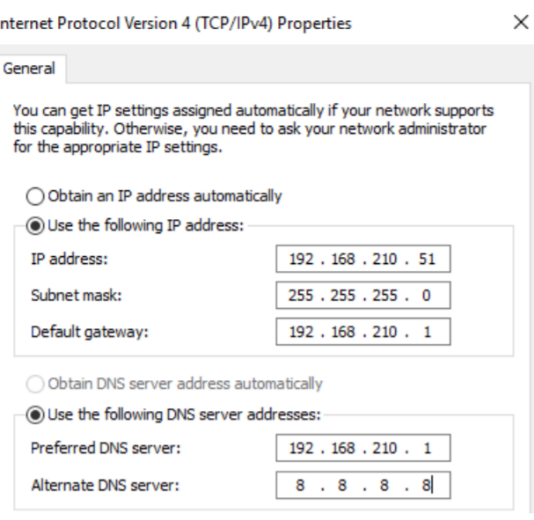
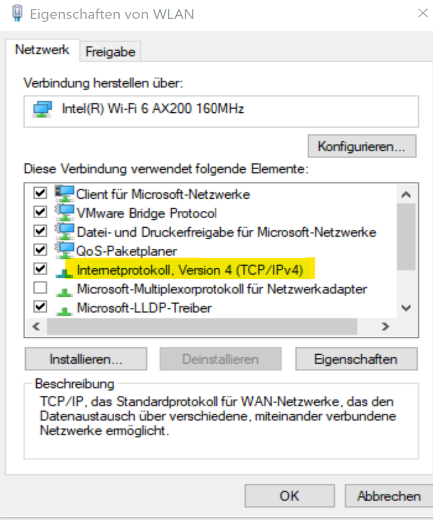


Dort Netzwerk und Internet auswählen, und weiter zu Netzwerk- und Freigabecenter gehen.

Dort kann man die Option “Adaptereinstellungen ändern” auswählen



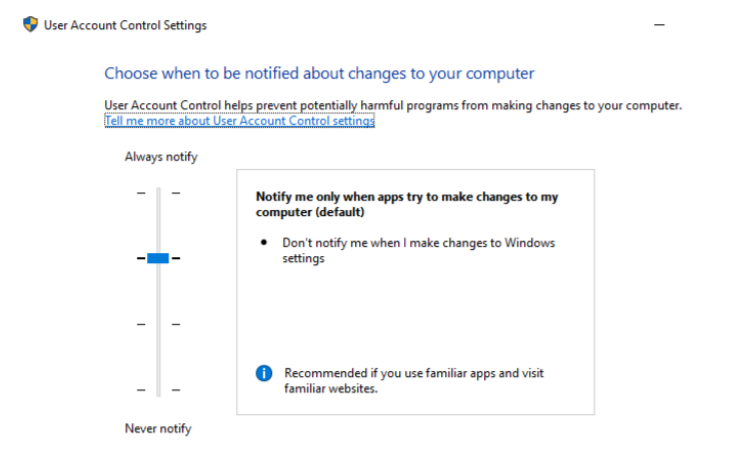
In dem neu geöffneten Fenster kann man sich einen Adapter per Doppelklick auswählen. Über das Feld Eigenschaften und danach über PCP/IPv4 kann man die Adapteroptionen ändern.



Härten

Um den Server zu härten sollte man am Anfang zuerst alle Updates ausführen.

Wenn der Server auf dem neusten Stand der Updates ist, muss man einen Benutzer auswählen der als Administrator fungiert, bei uns ist es der vmadmin. Für den ausgewählten Benutzer sollte man danach die UAC konfigurieren:



Ausserdem sollte man unbedingt einen Virenschutz aktivieren. Bei uns reicht der normale Windows Virenschutz.

Damit wir ohne Probleme im Browser surfen können müssen wir die Internet Explorer Enhanced Security Configuration (IE ESC) deaktivieren. Aber nur für Administratoren!

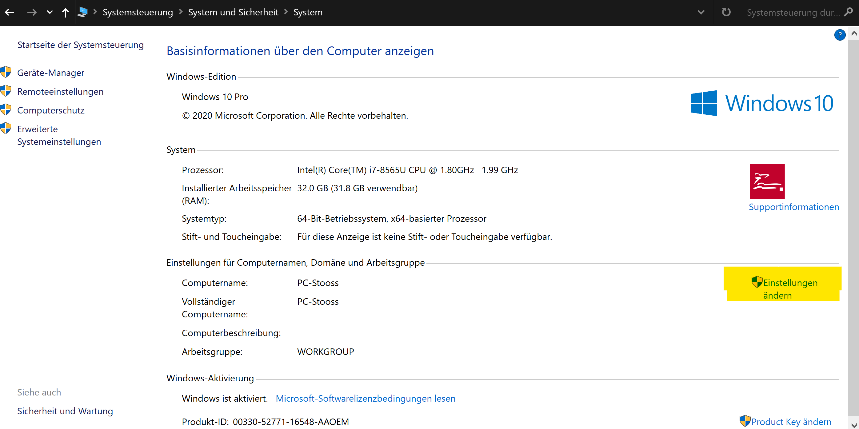


## Hostname anpassen

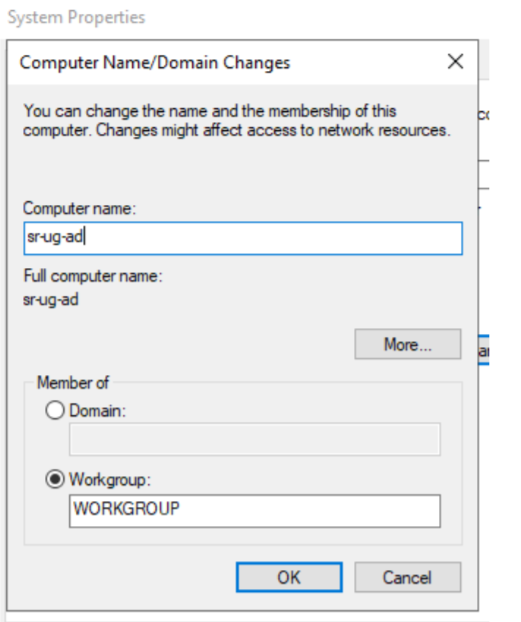
Den Hostname ändern wir wieder in den Systemsteuerung aber unter dem Pfad:

System und Sicherheit --> System

Dort kann man unter “Einstellungen ändern” den Hostname ändern.



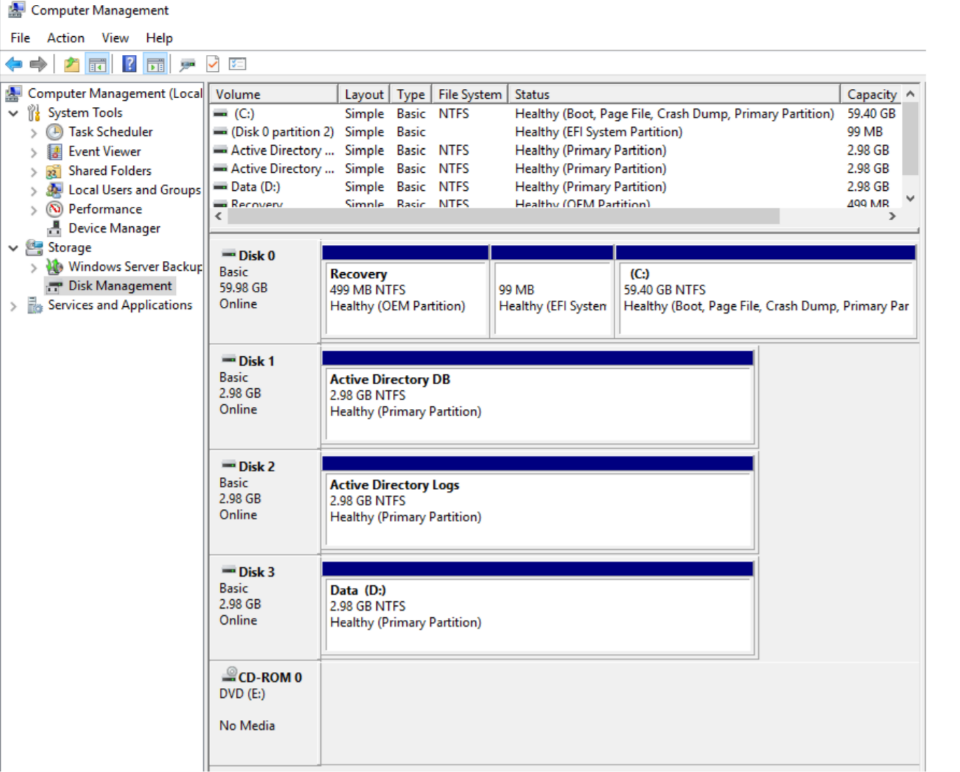
**Und dann ganz wichtig das Feld “Ändern...” auswählen!**



Hier kann man auch die Domaine angeben (Siehe DNS)

## Datenträger einrichten

Um die Datenträger einzurichten muss man als erstes das Windows Logo Rechtsklicken und dann Datenträgerverwaltung auswählen. In diesem Fenster kann man die Datenträger einrichten, RAID’s erstellen und viel mehr.

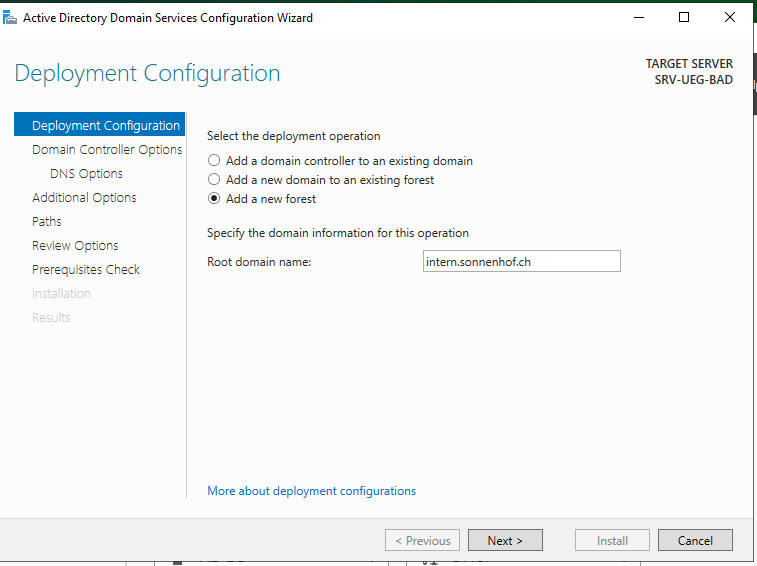


# AD DS

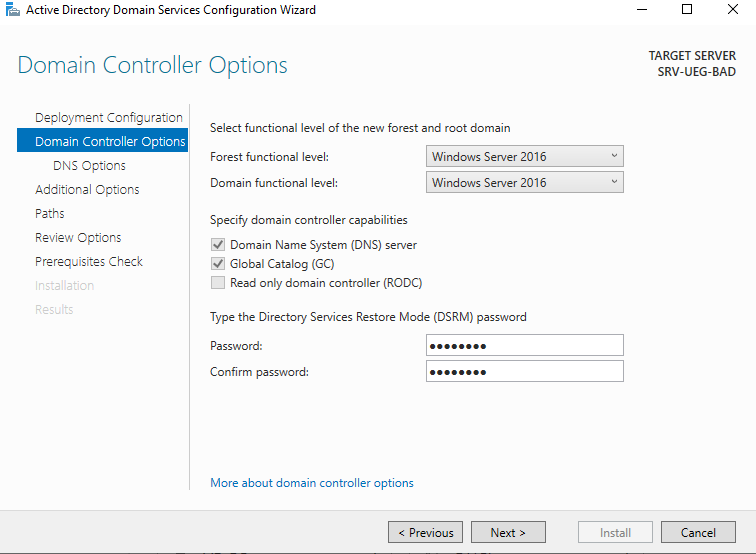
Unser Vorschlag ist es die OU Altersheim und die OU Praxis zu machen, um die zwei Beriech voneinander zu trennen.

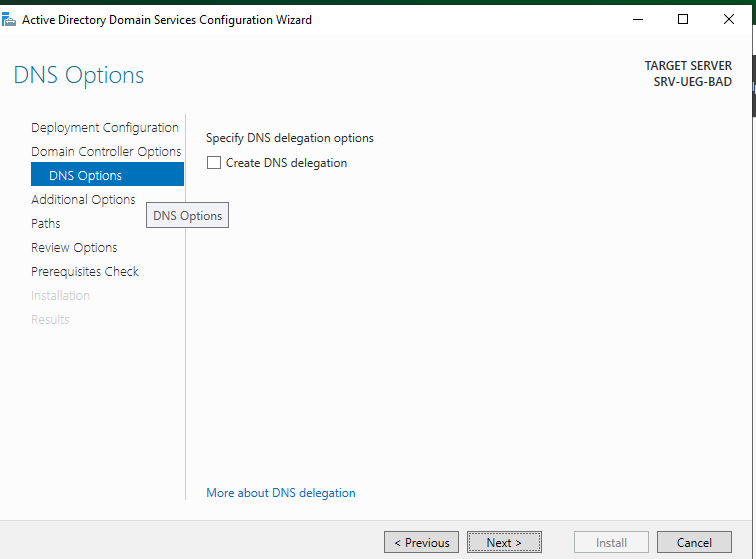
Der Nachteil dieser Art der Trennung ist es, falls es grössere Bearbeitungen geben sollte (z.B. Die Praxis wurde selbständig und trennt sich von dem Altersheim) wird ein grösserer Aufwand erstehen.

Zu Beginn muss man die AD Rolle installieren.

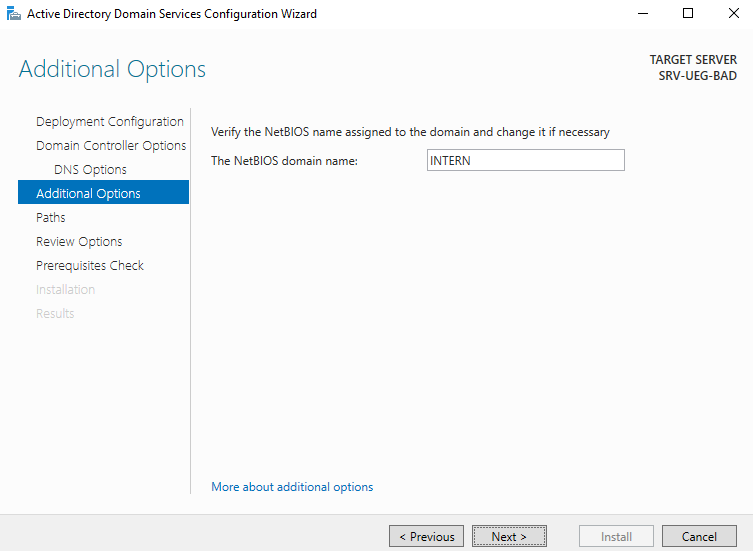


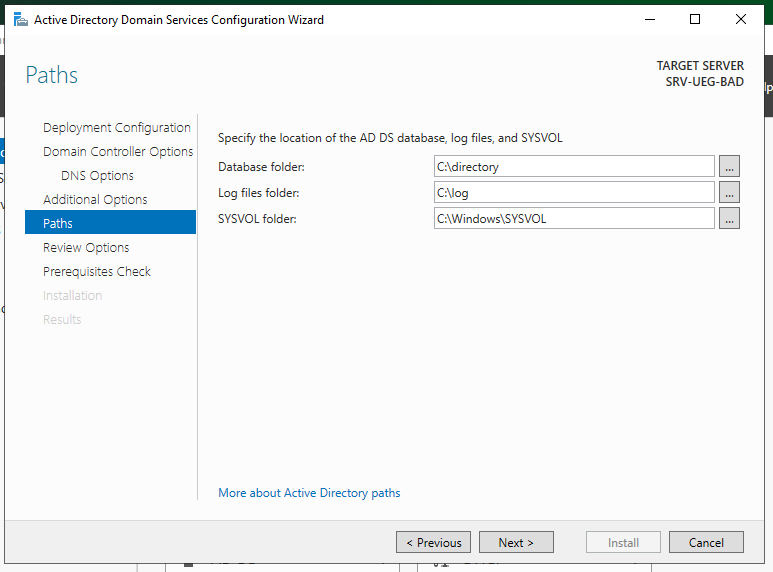
Hier “Add a new forest” wählen.



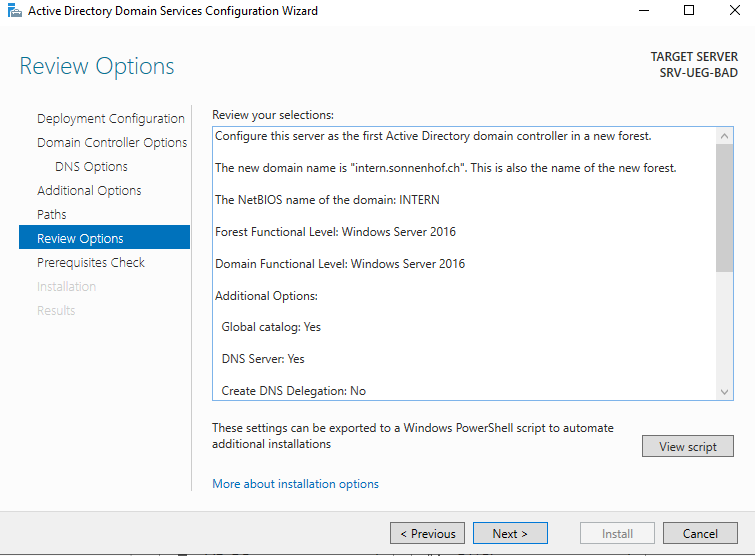
Jetzt ein Passwort festlegen. Wir haben “sml12345” genommen, damit wir es uns merken können. 

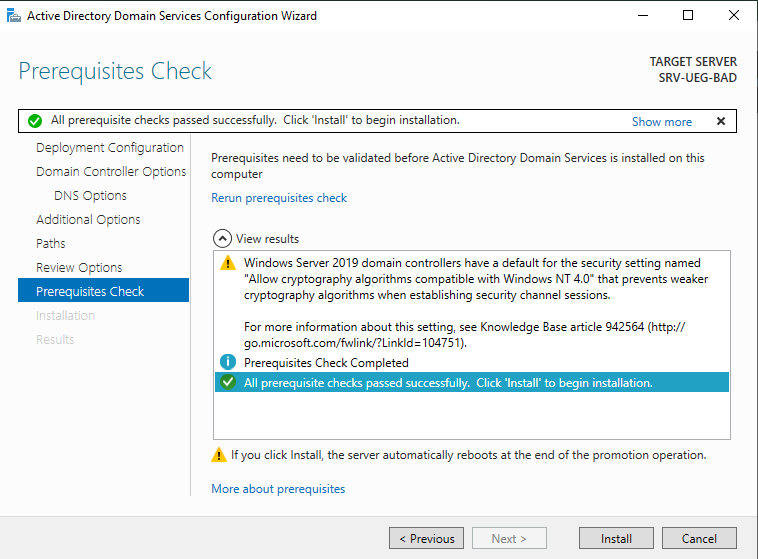
Hier können wir alles belassen.

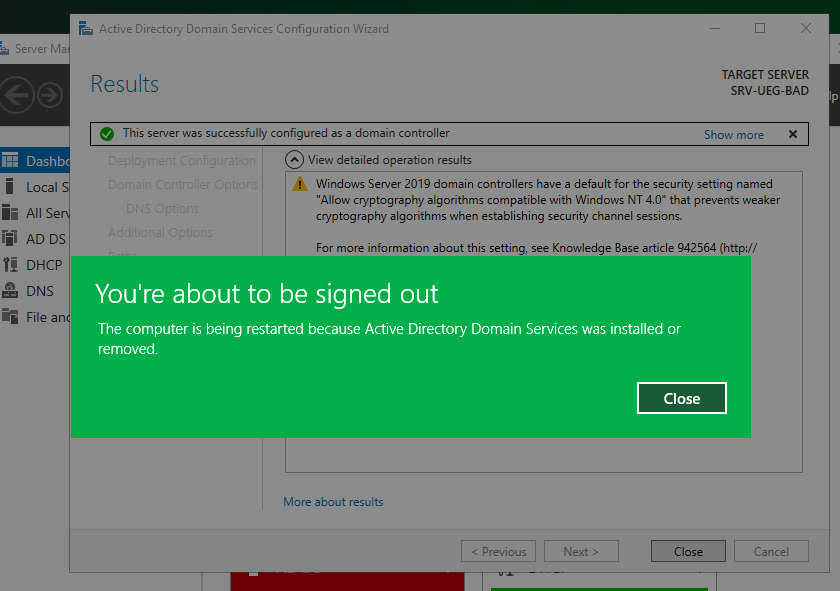


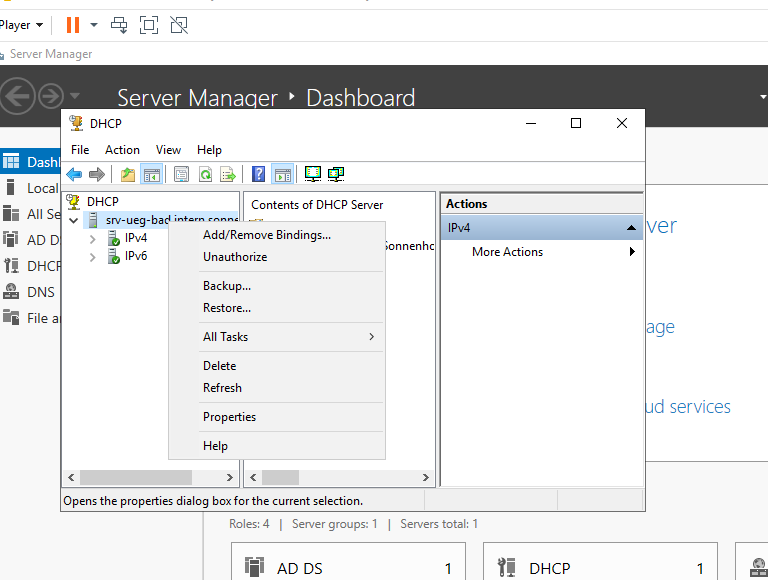
Als NetBIOS Name unserer Domain, haben wir “INTERN” gewählt.

Hier ändern wir den Database und Log Files speicherort. Database = C:\directory | log files = C:\log

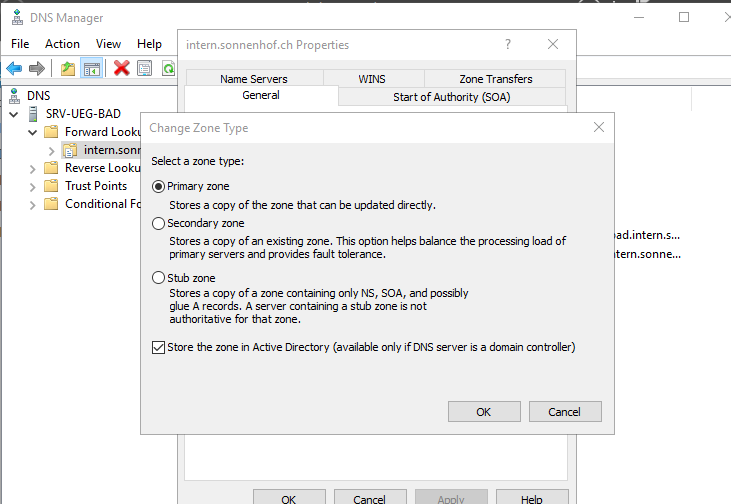
Üperprüfen

Die Warnung darf ignoriert werden.

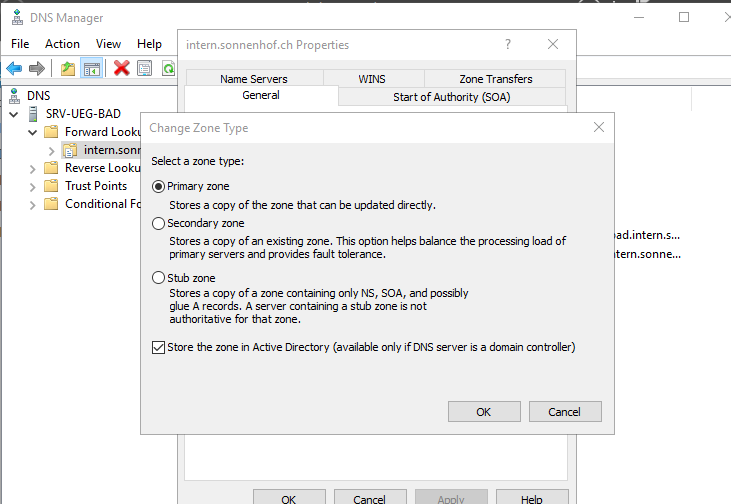
Nach der Installation muss der PC neugestartet werden.

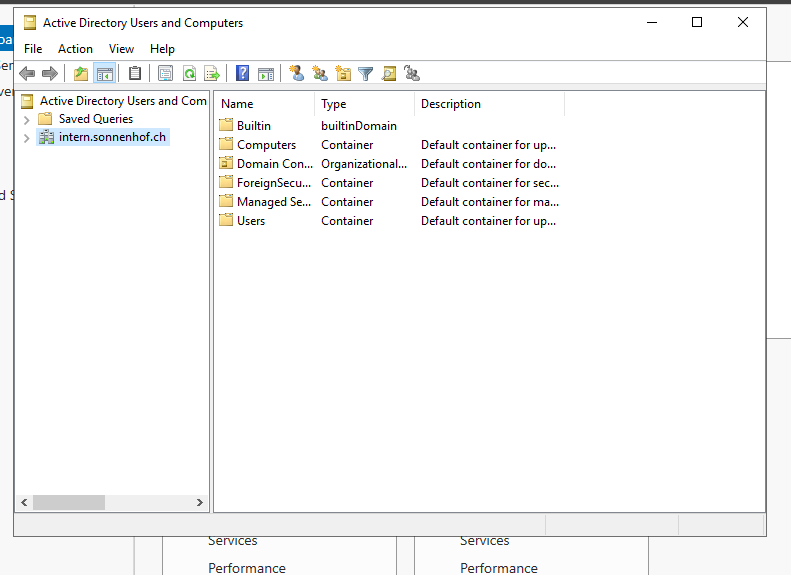


Dass der DHCP weiter funktioniert muss man diesen autorisieren, wenn dies nicht schon geschehen ist.

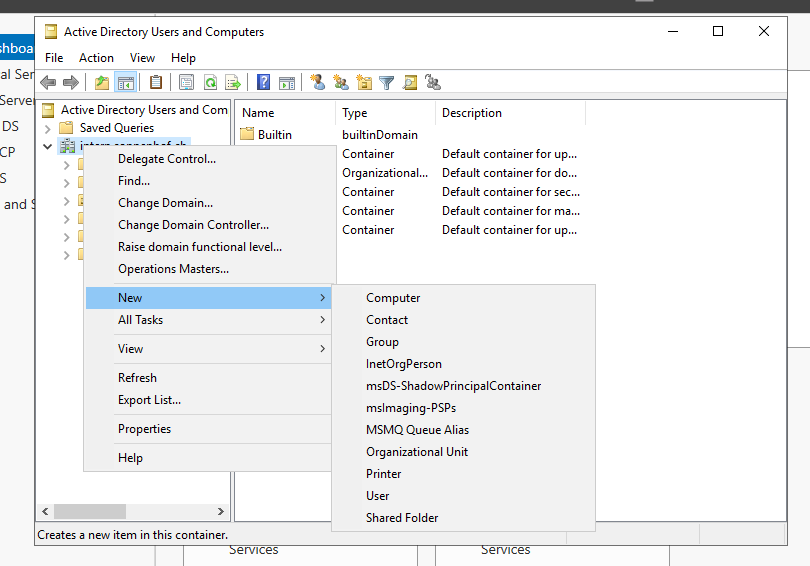


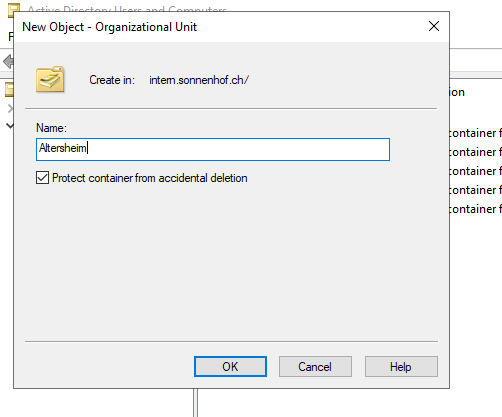
Auch den DNS muss man autorisieren.

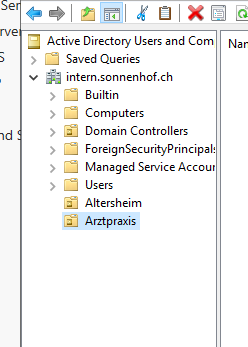
Nicht vergessen auch die reverse lookup zone einzubinden.



So sieht das AD aus.

 Jetzt erstellen wir eine neue OU (Organizational Unit) und nennen sie Altersheim.





Und eine namens Praxis.

# DHCP

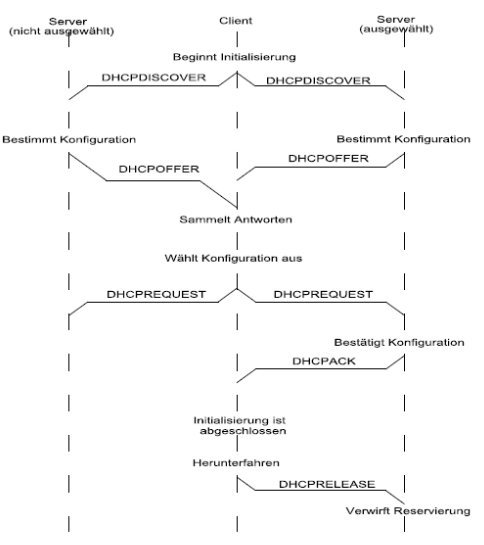
## DHCP Funktionen

Der DHCP ist ein Kommunikationsprotokoll in der Computertechnik. Er ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.

Ablauf

Der Ablauf zwischen einem Client-Computer und dem Server, damit

der Client-Computer seine IP-Adresse bekommt.



Vorteile

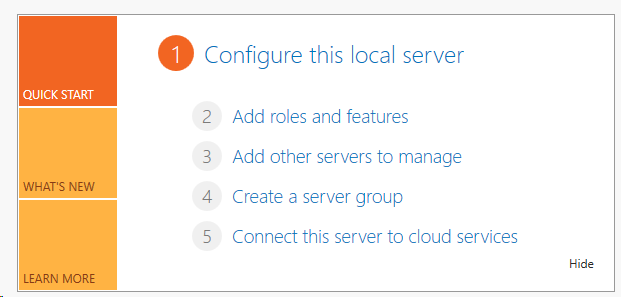
Erhöht Skalierbarkeit des Netzes, Zeitersparnis bei Inbetriebnahme/Änderung von PC Hardware, Konfigurationsmöglichkeiten

Nachteile

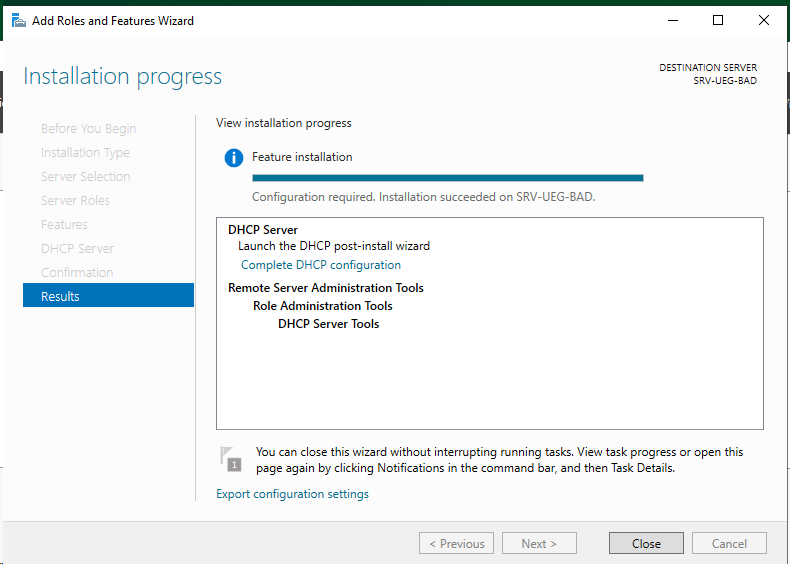
Sicherheit, Serverabsturz

## Die Installationsanleitung für einen DHCP Servers

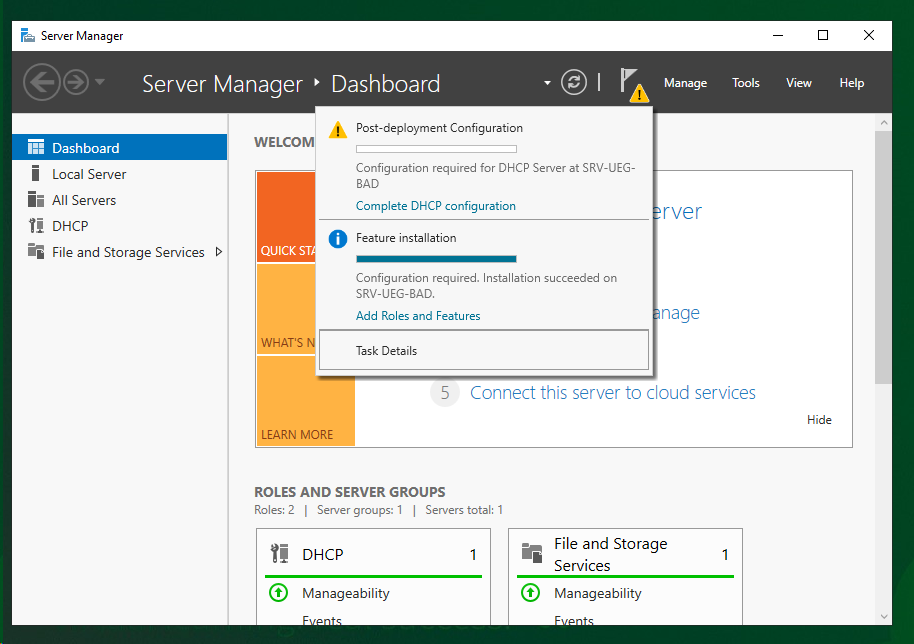
Um die Installation zu beginnen sollte man im Dashboard auf “Add roles and features”



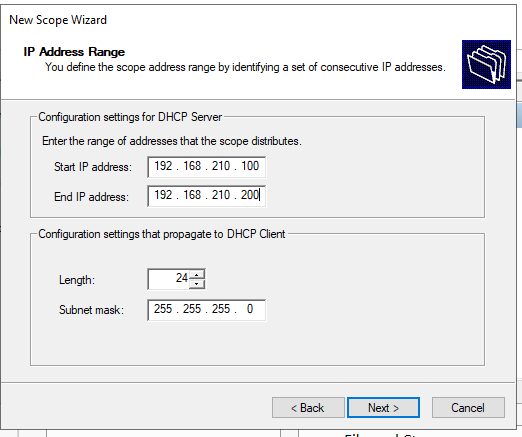
Weiter klicken bis man in “Server Roles” ist. Dort DHCP anwenden, die zusätzlichen Features auch aktivieren und wieder weiter klicken und am Schluss auf Install klicken.



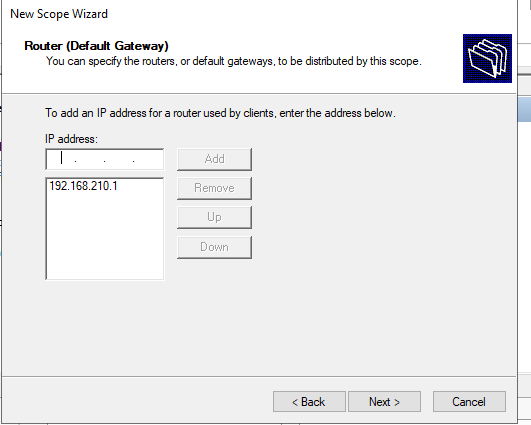
Sobald die Installation fertig ist auf Close klicken. Auf die Flagge klicken und die DHCP fertigstellen



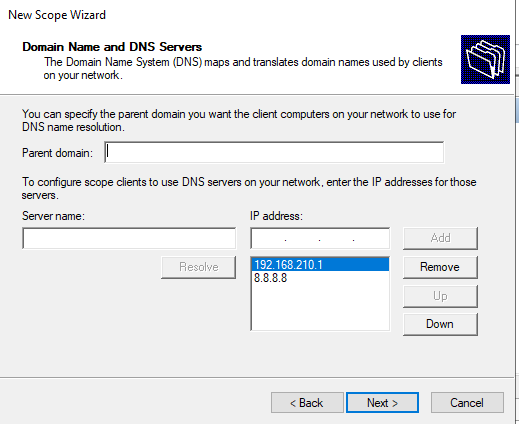
Nach der Installation und Neustart ein neues Scope erstellen mit dem folgenden Parameter, wir haben uns für eine Range von 192.168.210.100 – 192.168.210.200 entschieden:



“Die DHCP Einstellungen jetzt fertigstellen” auswählen und unter Router die IP des Domain Controllers angeben:



Und unter DNS auch die IP des Domain Controllers angeben, da wir später einen DNS konfigurieren werden:

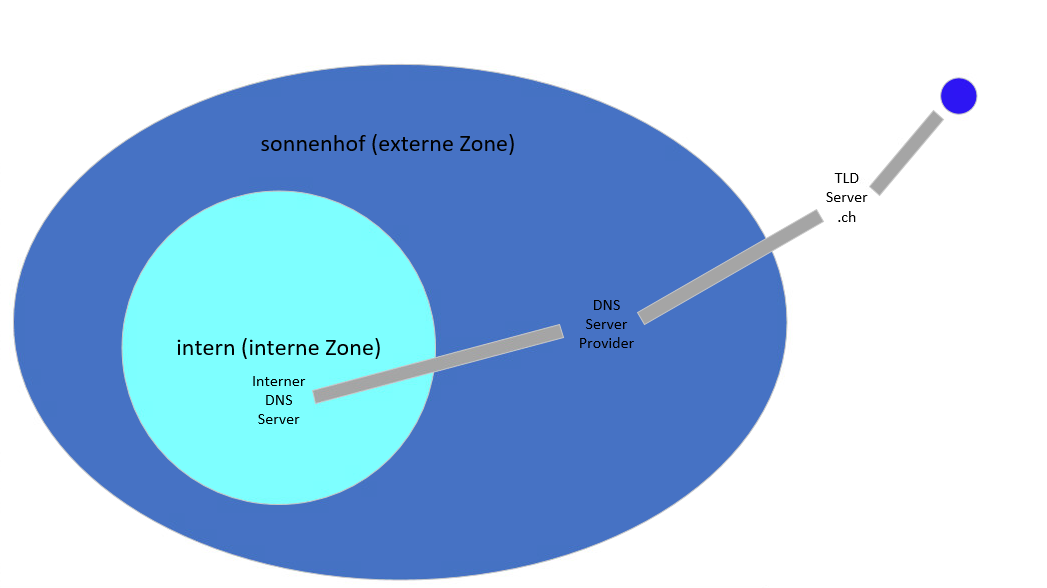


# DNS

## Subdomains und Zonen

Vorgeschlagenes Label: intern

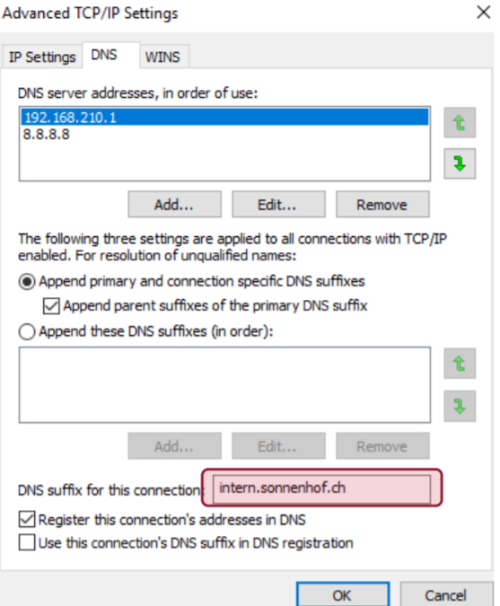
Domänenname: intern.sonnenhof.ch



## Die Installationsanleitung für einen DNS Servers

### Netzwerkadapter vorbereiten

Sofern Ihr DNS Server später in einem Active Directory zum Einsatz kommen soll, sollten Sie das zukünftige Domänen-DNS-Suffix (z.B. «intern.sonnenhof.ch») vorher in den DNS-Einstellungen des Netzwerkadapters hinterlegen.



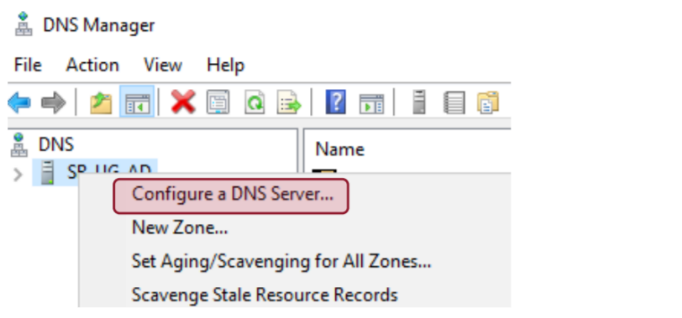
## DNS-Rolle installieren

Sie mit Hilfe des Server-Managers die Rolle DNS, samt Konfigurationstools.

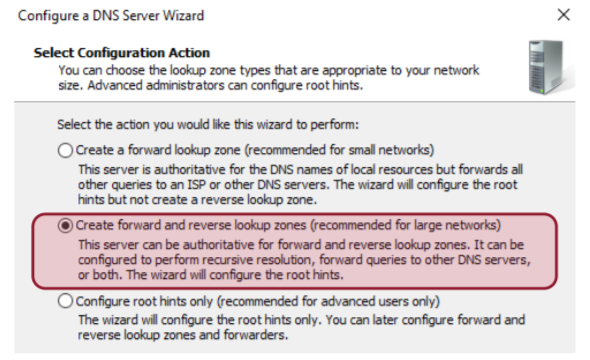
**DIE FOLGENDEN IP-ADRESSEN IMMER MIT DEN EIGENEN ADRESSEN ERSTETZEN!**

## DNS konfigurieren

Die Konfiguration der Serverrolle können Sie direkt nach der Installation vornehmen. Ein Neustart ist nicht erforderlich. Hierfür öffnen Sie im Server-Manager unter Tools den Eintrag „DNS“. Angezeigt wird daraufhin die Management-Konsole des DNS Servers. Um den DNS Server einrichten zu können müssen Sie mit der rechten Maustaste auf den Servernamen klicken und anschließend „DNS-Server konfigurieren“ auswählen. Damit startet der Assistent, welcher durch alle wichtigen Abschnitte führt.



Es empfiehlt sich im ersten Schritt sowohl eine Foward- als auch eine Reverse-Lookupzone einzurichten. Die Forward-Lookupzone löst die Hostnamen nach IP-Adressen auf. Die Reverse-Lookupzone tut das gleiche in die andere Richtung, also IP-Adressen in Hostnamen auflösen.

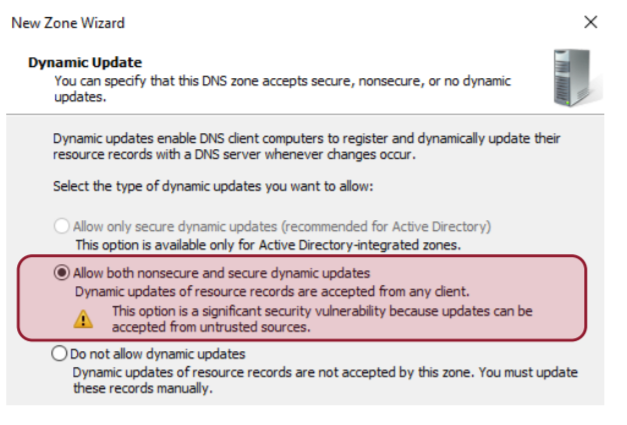


### Forward-Lookupzone erstellen

Da Sie noch keinen anderen DNS-Server im Netzwerk haben, erstellen Sie die Forward-Lookupzone als primäre Zone. Der Name der Zone muss zwingend dem zuvor eingetragenen DNS-Suffix des Servers, sowie dem zukünftigen DNS-Domänennamen entsprechen:

Zonenname: intern.sonnenhof.ch

Im nächsten Schritt wählen Sie die Option „Nicht sichere und sichere dynamische Updates zulassen“. Diese Auswahl ist wichtig, da der Assistent für die Installation des Active Directory in den Lookupzonen mehrere Einträge anlegen muss. Nach der Installation der Domänendienste wird diese Auswahl auf „Nur sichere dynamische Updates zulassen“ geändert werden.



### Reverse-Lookupzone konfigurieren

Die Reverse-Lookupzone erstellen Sie ebenso wie die Forward-Lookupzone als Primäre Zone. In das Feld „Netzwerk-ID“ geben Sie die ersten drei Abschnitte der Netzadresse (192.168.210) ein. Der Name der Reverse-Lookupzone wird dann automatisch erstellt.

Name der Reverse-Lookupzone: 210.168.192.in-addr.arpa

Auch in der Reverse-Lookupzone gilt, zunächst die „nicht sicheren und sicheren dynamischen Updates“ zuzulassen und später wieder zu ändern. Die Änderung auf „Nur sichere dynamische Updates zulassen“ ist deshalb wichtig, damit sich später nur noch Computer des Active Directory in den Lookupzonen des DNS Servers eintragen können.

Weiterleitungen

In dem Punkt Weiterleitungen werden diejenigen DNS-Server angegeben, an die DNS-Anfragen weitergeleitet werden, wenn unser DNS-Server diese nicht bearbeiten kann (externe Namen und IP-Adressen).

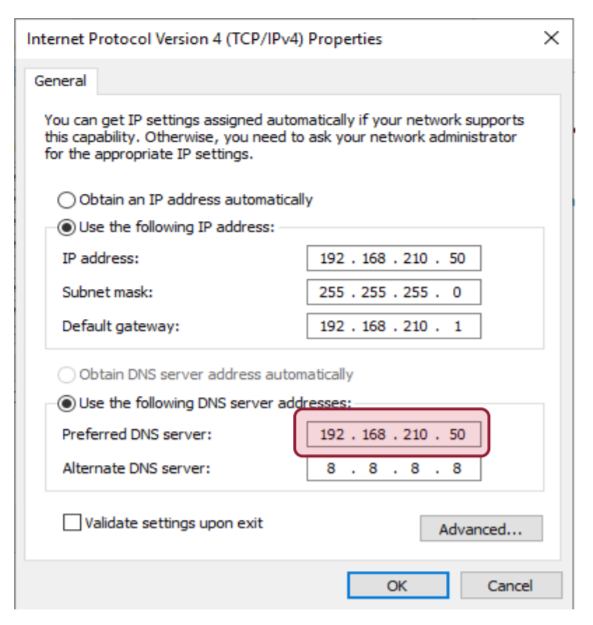
Für unser Fallbeispiel sind dies:

192.168.210.1 (vmLF1)

8.8.8.8 (DNS-Server von Google)

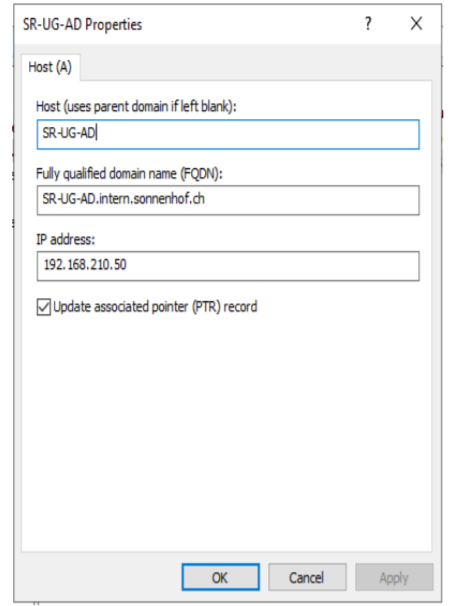
## Eintrag in den Adaptereinstellungen anpassen

Weil unser Server sich jetzt selbst als DNS-Server anfragen kann, müssen Sie nun in den Einstellungen des Netzwerkadapters seine IP (192.168.210 51) als primären DNS-Server eintragen:



## Den Server im DNS eintragen

Erstellen Sie nun in der Forward-Lookupzone einen neuen Host-Eintrag. Ihr Server wird mit Namen und IP-Adresse registriert. Durch die Option unten wird auch gleich der entsprechende Eintrag in die Reverse-Lookupzone erstellt.



## Test DNS-Server-Konfiguration durch Server

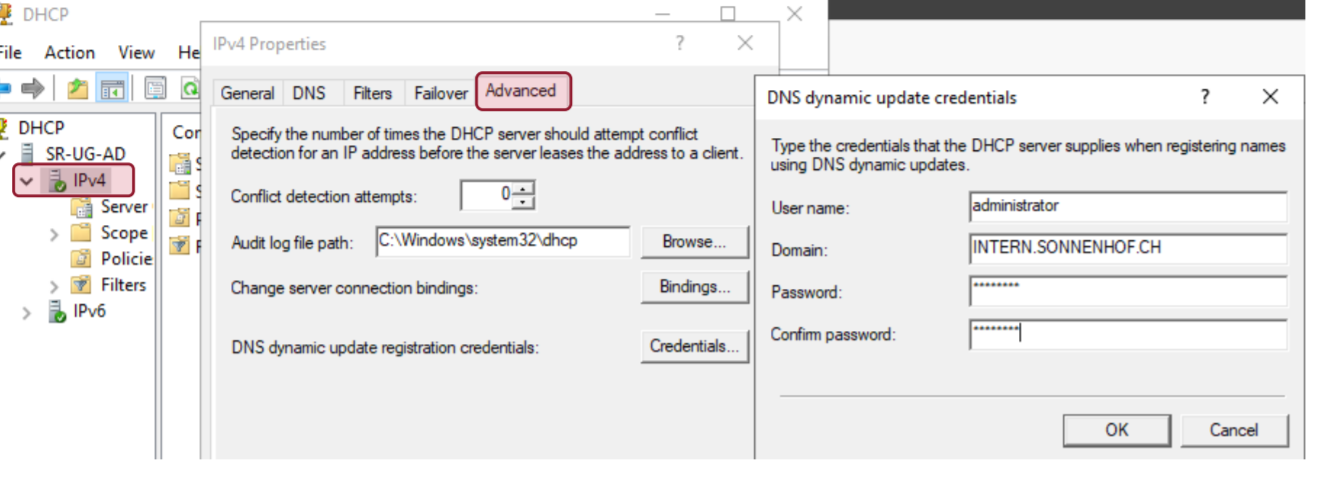
Nun fehlt noch der Funktionstest des DNS Servers. Hierfür öffnen Sie die Eingabeaufforderung (oder PowerShell) und geben den Befehl nslookup ein. Als Standardserver (DNS-Server) sollte der Hostname des soeben eingerichteten Servers, sowie dessen IP-Adresse angezeigt werden.

Die Überprüfung mit nslookup liefert nun den korrekten Hostnamen nach Eingabe der IP-Adresse.

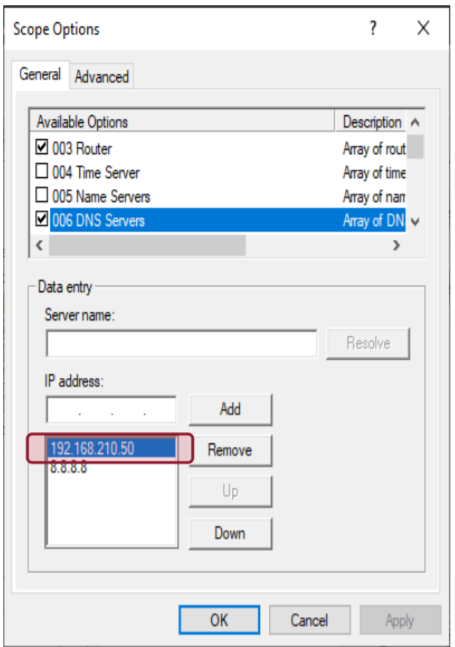
Anpassungen im DHCP-Server

Dynamische DNS-Updates durch den DHCP-Server

Damit beim Verteilen von IP-Adressen im Netzwerk automatisch die notwendigen DNS-Einträge aktualisiert werden, müssen Sie noch ein berechtigtes Konto in den IPv4-Einstellungen des DHCP-Servers eintragen:

DHCP-Option anpassen

Bisher haben unsere Clients durch den DHCP die Adressen 192.168.210.1 und 8.8.8.8 als DNS-Server erhalten. Da nun unser Server diesen Dienst übernimmt, müssen Sie in den Optionen des DHCP den mitzuliefernden DNS-Server auf 192.168.210.50 abändern.



## Die Host-Datei

Die Hostdatei liegt unter: C:\windows\system32\drivers\etc

Nachteile: Die Hosts-Datei ist lokal und statisch gespeichert

Die Vorteile des DNS-Systems können nicht ausgenutzt werden.

Gefahren: Durch eine Anpassung der Datei können Benutzer auf falsche

Webseiten umgeleitet werden.

# Berechtigungen und Freigaben

## Domänenlokalen, globalen und universellen Gruppen

Die Eigenschaften von domänenlokalen, globalen und universellen Gruppen erscheinen auf

den ersten Blick verwirrend. Wichtig ist folgende Unterscheidung:

### Wo ist eine überall Gruppe sichtbar?

Nur in der eigenen Domäne

In allen Domänen der Gesamtstruktur

### Wer kann in einer Gruppe Mitglied sein?

Benutzer

domänenlokale Gruppen

globale Gruppen

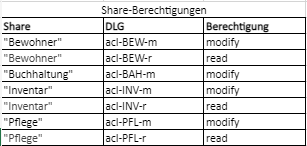
universelle Gruppen

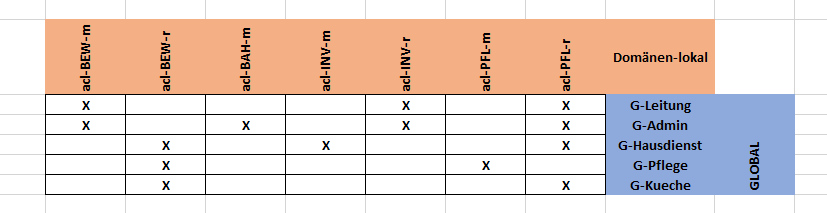
Bei der Mitgliedschaft muss zusätzlich berücksichtigt werden, ob die Mitglieder aus der

eigenen Domäne oder auch aus anderen Domänen stammen können.

|  |  |  |
| --- | --- | --- |
| Gruppenart | Verwendbar in | Mögliche Mitglieder |
| Domänenlokale Gruppe | In der eigenen Domäne | Benutzer und Gruppen aus der eigenen Domäne und aus allen anderen Domänen der Gesamtstruktur. |
| Globale Gruppe | In allen Domänen der Gesamtstruktur | Nur Benutzer und Gruppen aus der eigenen Domäne |
| Universelle Gruppe | In allen Domänen der Gesamtstruktur | Benutzer und Gruppen aus der eigenen Domäne und aus allen anderen Domänen der Gesamtstruktur. |

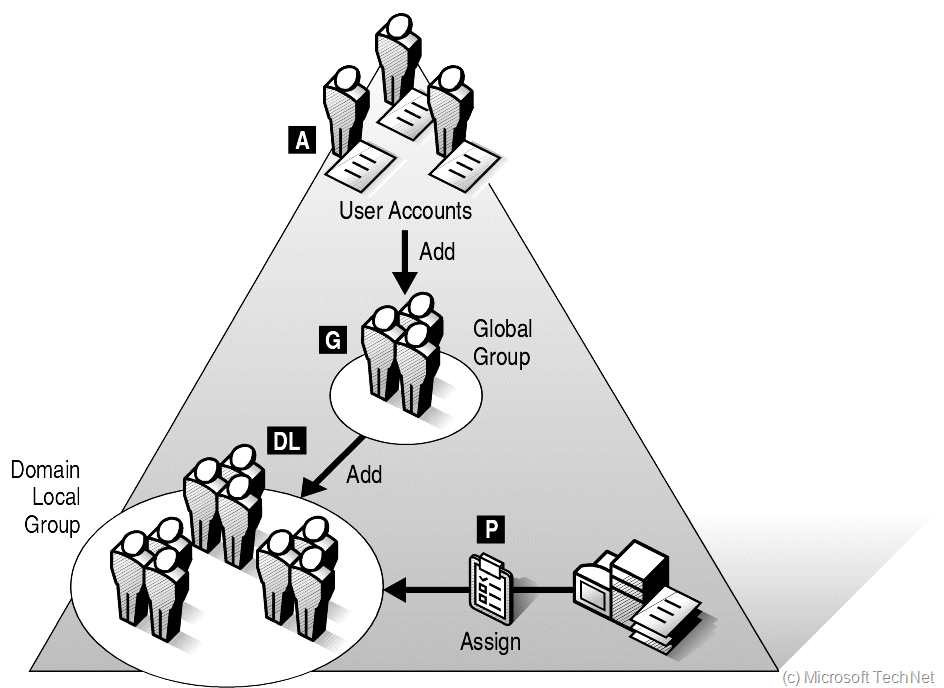
## Zugriffs- und Berechtigungskonzept erstellen





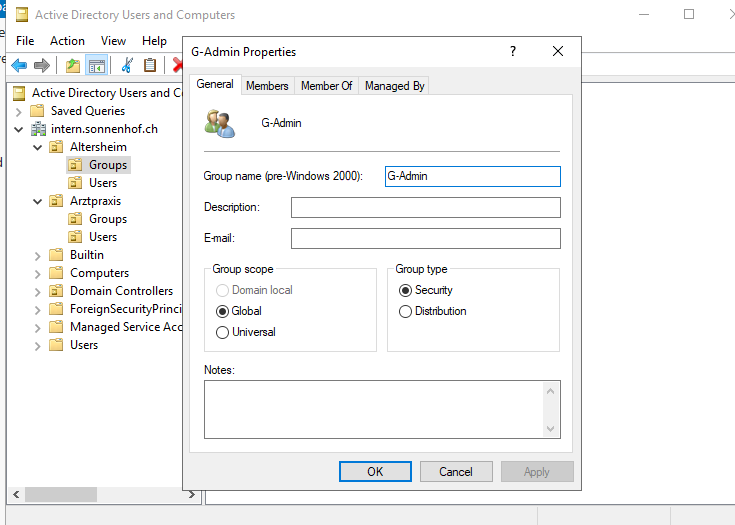


## AGDLP Aufbau:

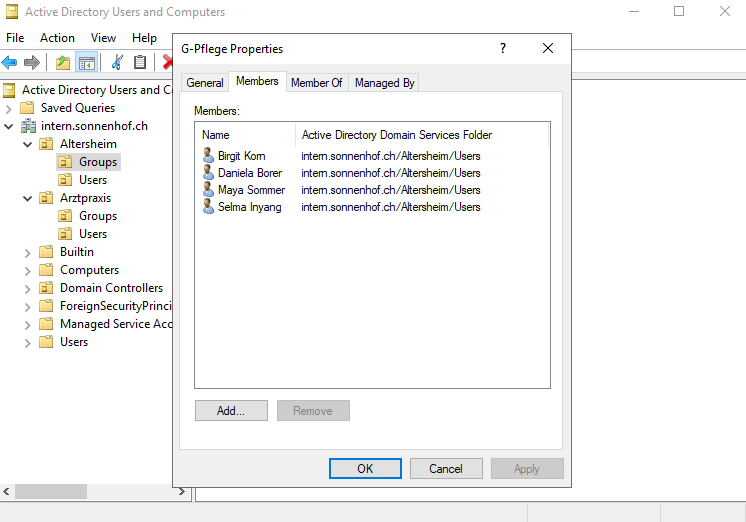


## Berechtigungskonzept auf Server implementieren

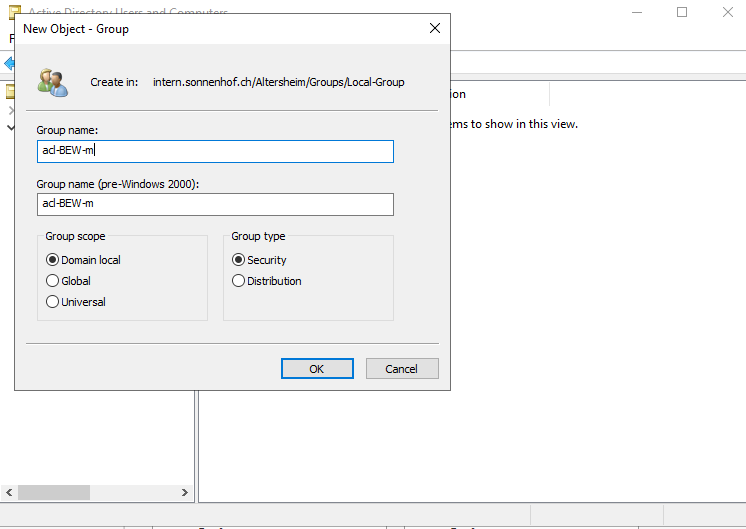
Hier haben wir die lokalen Gruppen erstellt:

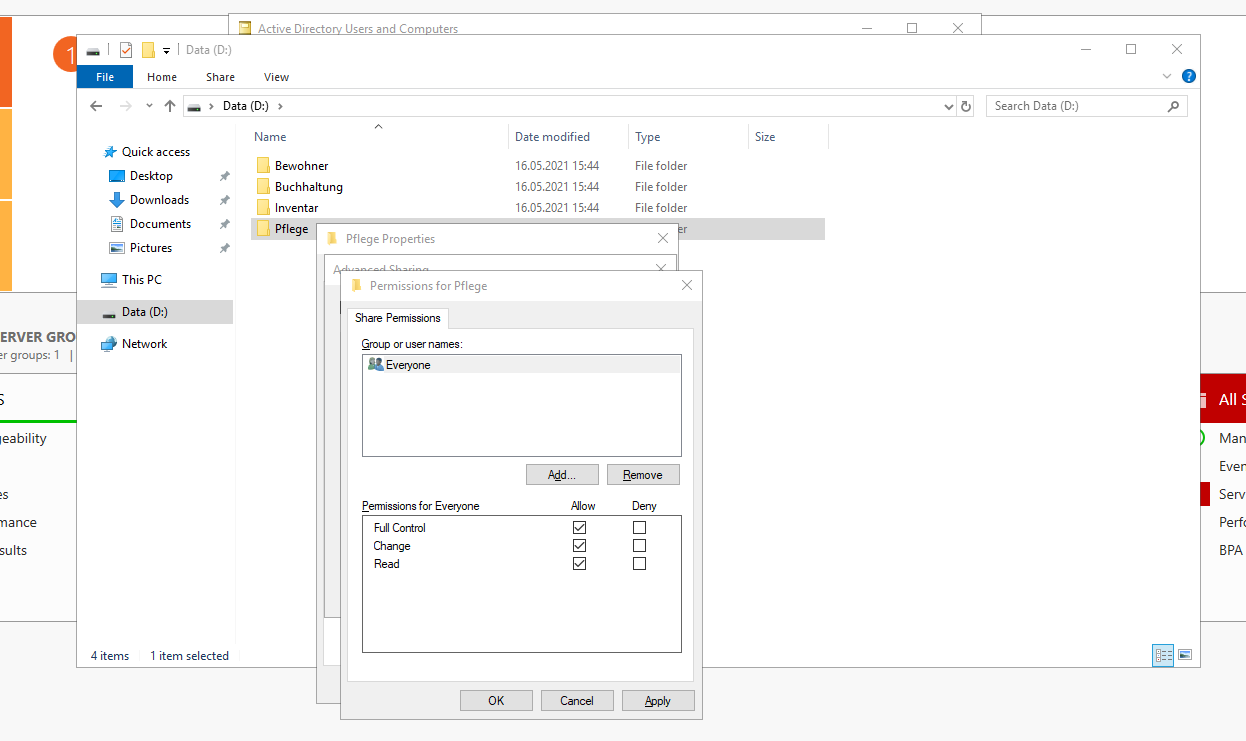


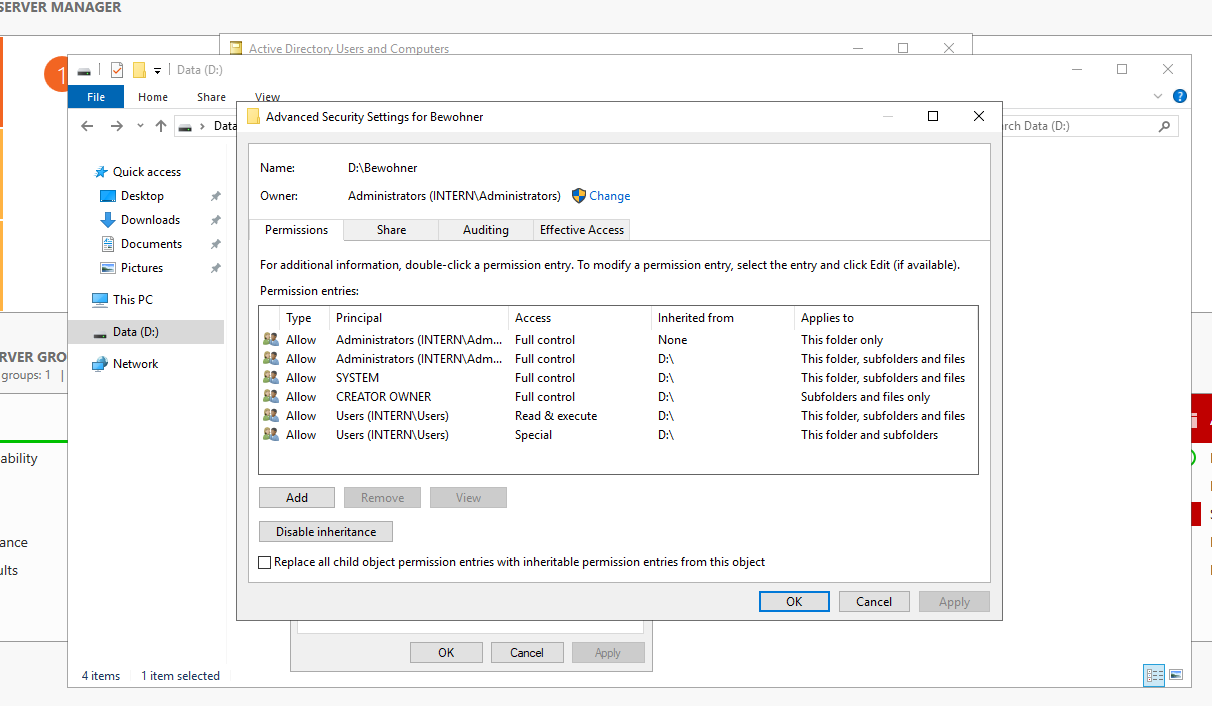
Danach haben wir die Benutzer den Gruppen zugewiesen:

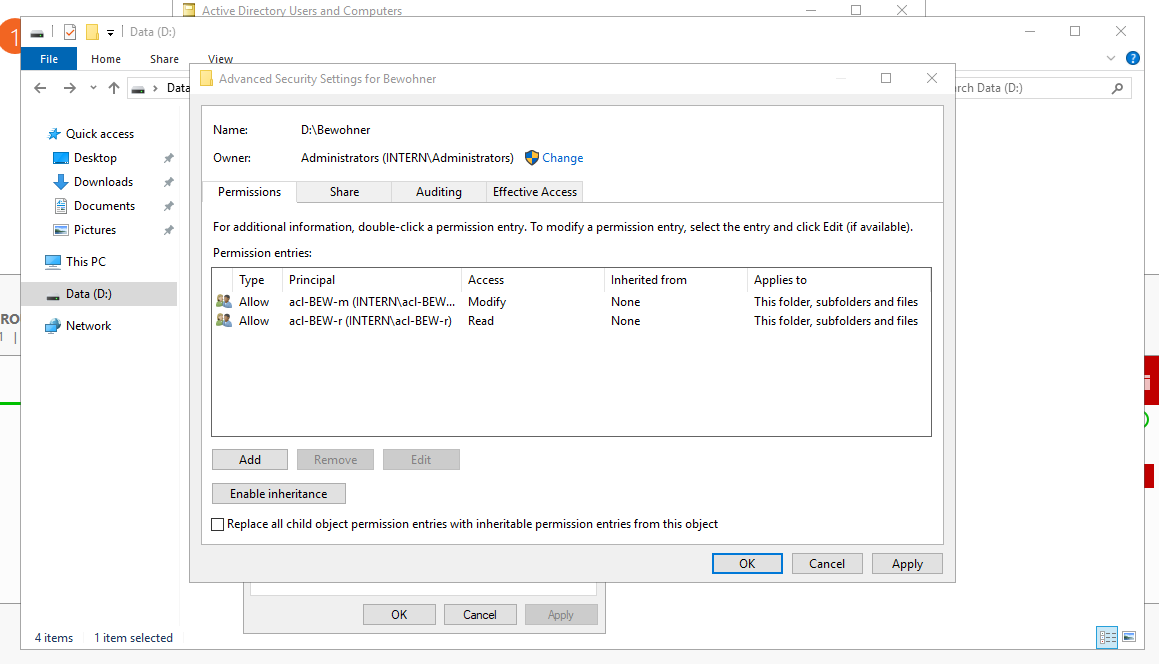


Hier haben wir die lokalen Gruppen erstellt:

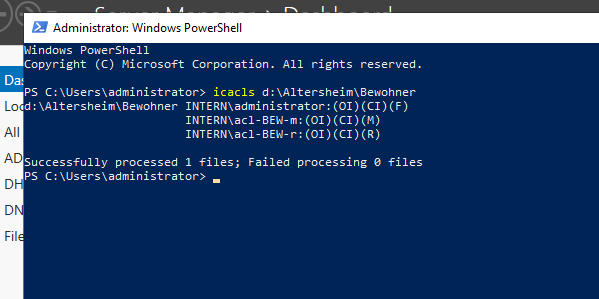


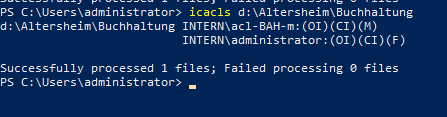
Hier haben wir die Freigabeberechtigung für everyone auf full konfiguriert:

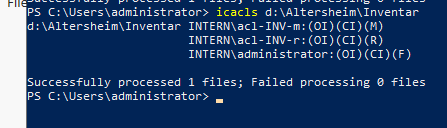
Danach haben wir die alten Security Settings gelöscht:

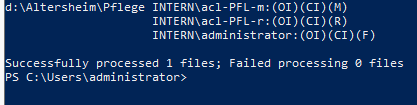
Und unsere Lokalen Gruppen darauf richtig berechtigt:

Nun überprüfen wir in Powershell die Berechtigungen:









## Freigabeberechtigungen vs. NTFS-Berechtigungen

### Welches sind die Unterschiede zwischen den beiden Systemen?

Freigabeberechtigungen lediglich die drei Möglichkeiten Vollzugriff, Ändern und Lesen zulassen, können Sie die Zugriffe bei NTFS-Berechtigungen sowohl für Einzelpersonen als auch für Gruppen deutlich detaillierter einstellen. Theoretisch ist es also möglich, mithilfe von NTFS Berechtigungen sehr spezielle Rechte zu vergeben. So können die gesetzten Zugriffsrechte über die Eigenschaft der Vererbung von NTFS Berechtigungen z.B. auf untergeordnete Dateien oder Ordner weitergegeben werden.

### Welche Freigabeberechtigungen gibt es und was bedeuten diese?

Lesen: Benutzer dürfen die Inhalte des Ordners sehen.

Ändern: Der Benutzer darf Ordner und Dateien innerhalb der Freigabe lesen, ausführen, schreiben und löschen.

Vollzugriff: Der Benutzer darf Ordner und Dateien innerhalb der Freigabe ändern, außerdem aber auch Berechtigungen bearbeiten sowie die Kontrolle über Dateien übernehmen.

### Welche Berechtigungen gelten schliesslich, wenn ein Benutzer über das Netzwerk auf einen freigegebenen Ordner zugreift?

Freigabeberechtigungen, gelten bei per Netzwerkfreigegeben Ordnern mehr.

## Best-Practices für Freigaben

Beim Zugriff über Netzwerk haben Freigabeberechtigungen immer den Vorrang vor den eingestellten NTFS-Berechtigungen. Erfolgt der Zugriff auf einen Ordner jedoch lokal am Fileserver, gelten die NTFS-Berechtigungen. Das Entscheidende: Selbst beim Zugriff über Netzwerk kann die Freigabeberechtigung die NTFS Berechtigung NICHT erweitern. Sie kann sie lediglich weiter einschränken, wenn sie dem User z.B. geringere Berechtigungen einräumt als die NTFS-Berechtigung.

# GPO (Gruppenrichtlinien)

## Was ist eine Gruppenrichtlinie?

Sammlung von vielen möglichen Richtlinien und Einstellungen für einen Windows-Computer

Was ist ein Gruppenrichtlinien-Objekt?

Objekt, welches bestimmte konkrete Werte für Richtlinien und Einstellungen enthält. Meistens auf dem AD-Server gespeichert.

## Zwischen welchen zwei Arten von Gruppenrichtlinien wird auf der obersten Ebene

## Unterschieden?

Computer-Richtlinien (werden auf die Computer angewandt) Benutzer-Richtlinien (werden auf die Benutzer angewandt)

Mit welchen Objekten des ADDS können GPOs verlinkt werden? Was wird durch die Verlinkung bewirkt?

GPOs werden entweder mit einer Domäne oder mit einer OU verlinkt. Die GPO wird dann innerhalb und unterhalb der Domäne oder der OU angewandt.

## Viele Richtlinien kennen drei mögliche Einstellungen. Welche sind das? Was bedeuten sie?

Not configured Die Richtlinie wird nicht angewandt. Es gelten die Defaultwerte oder Werte aus anderen GPOs.

Enabled Die Richtlinie ist eingeschaltet und wird angewandt.

Disabled Richtlinie ist ausgeschaltet und wird nicht angewandt.

# Wichtige Eingabebefehle

## CMD

Ping hostname

Ping Ip-Adresse

Ipconfig /all

ipconfig /release

ipconfig /renew

Ipconfig/flushdns

Gpupdate /force

Gpresult /r

arp –a

Nslookup

PowerShell

Icacls dateipfad (d:\Altersheim\Verwaltung\Buchhaltung\Inventar)