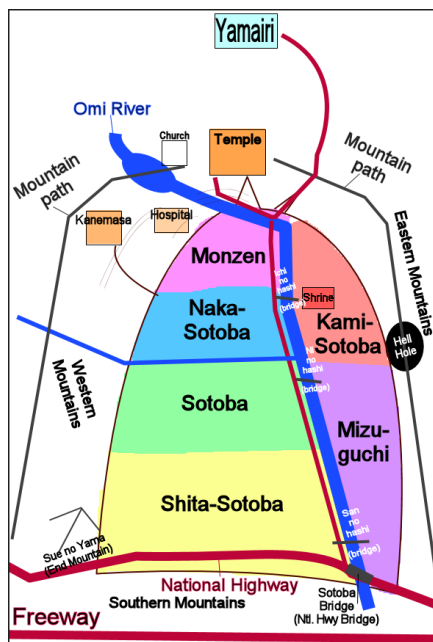


Konfiguration von Active Directory

Der Plan

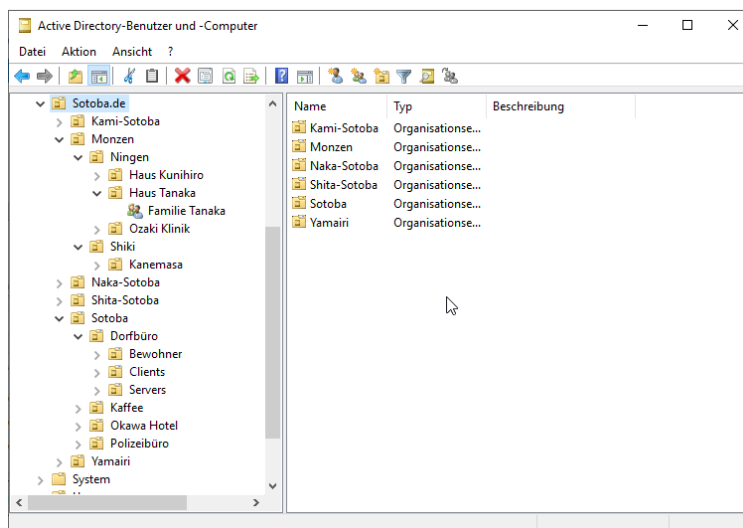
In diesem Kapitel möchte ich Active Directory anhand der Domäne Sotoba.de beschreiben.

Die Struktur dieser Domäne basiert auf den Aufbau des fiktiven Dorf Sotoba aus dem Anime bzw Manga Shiki.



Das AD wird dementsprechend in fünf Organisationseinheiten aufgeteilt wobei die OU Sotoba mit der Unter OU Dorfzentrum und Polizeistation das Dorfzentrum bildet.

Dann wird nochmal unterschieden, ob es Vampire oder Menschen sind. Die Bewohner des Dorfes werden in Gruppen dann in Gruppen organisiert.



Die Technik

Die Technische Grundlage des Systems sieht wie folgt aus. Das Netzwerk besteht derzeit aus 3 Rechner

Umgebung	Hardware
Server	3 PCs mit Proxmox 1x Ryzen5 5500, 32 GB Ram, 3 TB HDD/SDD 1x I3-7020U, 8 GB 500 GB SSD 1x I3-3220 8 GB 1 TB HDD
Client	Clients laufen in unterschiedlichen VMs
Zusätzlich benötigt	2 Monitore 1x 5 Port Switch 1x Easybox Router USB to LAN Adapter

Als Betriebssysteme wird folgende Software eingesetzt.

Umgebung	Software
Server-Software	Windows Server 2019 Proxmox, TrueNAS
Client-Software	Windows 10 Enterprise, Windows 11 Enterprise Ubuntu

In diesem Netzwerk werden folgende IP-Adressen genutzt

Bereich	Beschreibung
192.168.2.2 – 192.168.2.6	Hypervisoren
192.168.2.7 – 192.168.2.10	Domänen Controller
192.168.2.11 – 192.168.2.20	Andere Server
192.168.2.1	Router
192.168.2.50	Switch
192.168.2.21 – 192.168.2.45	werden über den DHCP-Dienst an die Clients verteilt
192.168.2.46 – 192.168.2.49	Können statisch vergeben werden

Folgende Namen werden für die jeweiligen Rechner je nach Rolle vergeben

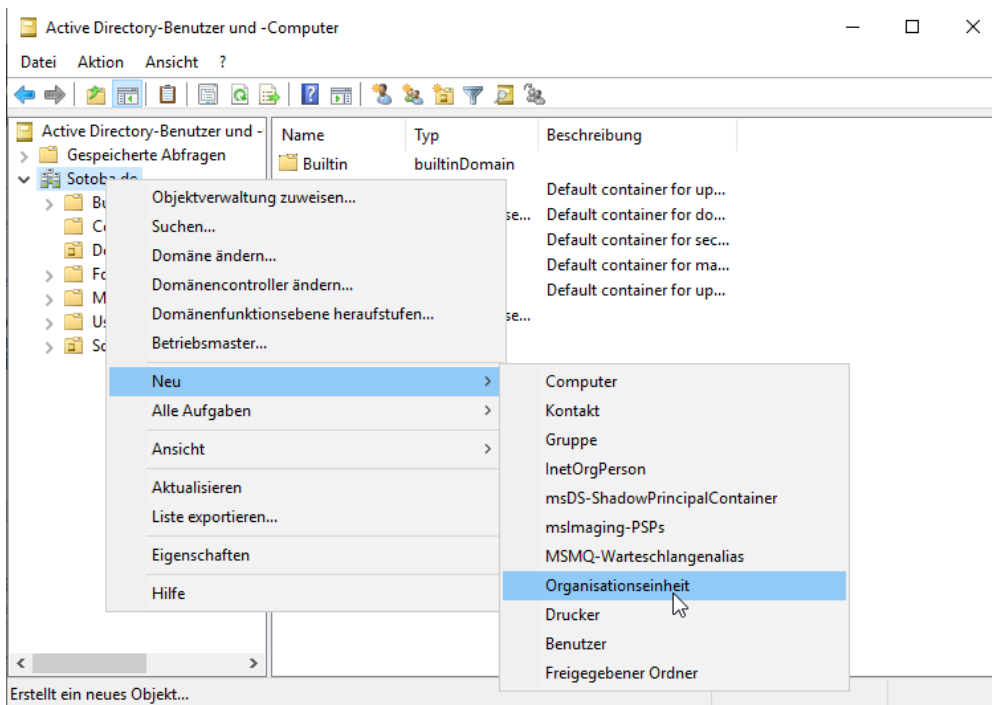
Rechner mit	Namen
Hypervisor	Hiryu, Soryu, Kaga, AkagiA
Domain Controller	Musashi, Yamato, Nagato, Mutsu
Andere Serverdienste	Fuso, Yamashiro, Hiei, Haruna, Kirishima
Windows Client	Mogami, Takao, Ashigara, Haguno.
Linux Client	Kuma, Natori, Sendai, Nagara
Container	Fubuki, Kagero, Shimakaze, Akizuki
NAS	I-400, I401
Domäne	Sotoba.de

Folgende Rechner haben Feste IP'S und führen folgende Dienste aus

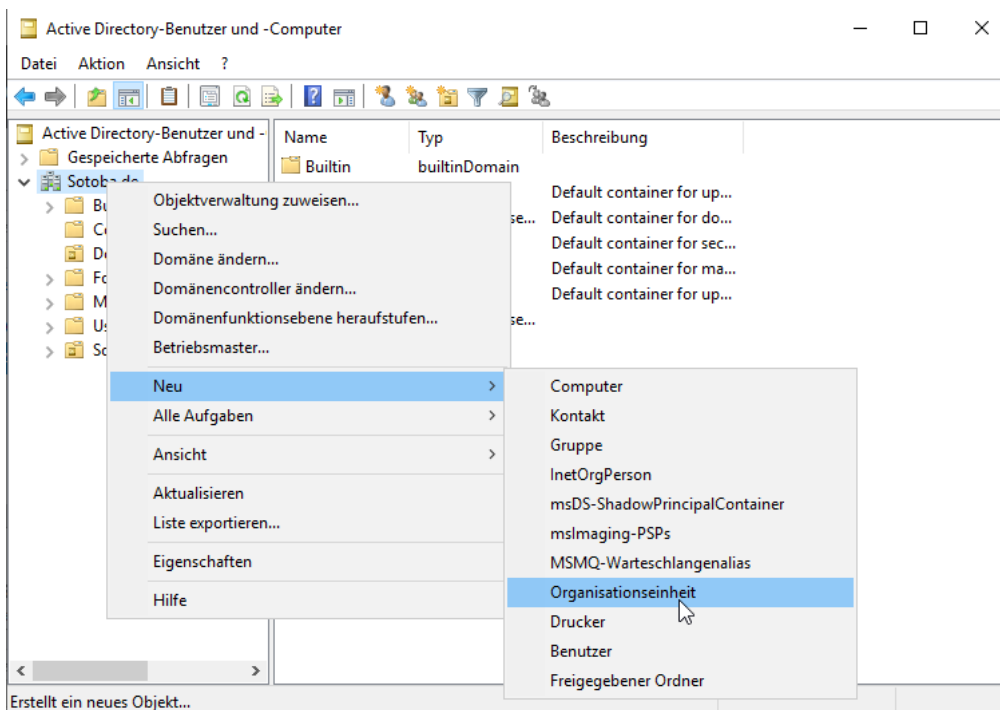
Feste IP	von	Rollen
192.168.2.2	Soryu	Hypervisor Proxmox
192.168.2.3	Hiryu	Hypervisor Proxmox
192.168.2.4	Kaga	Hypervisor Proxmox
192.168.2.7	Nagato	ADDS,DHCP,DNS
192.168.2.11	Fuso	WDS
192.168.2.12	I-400	TrueNAS
192.168.2.13	Hyuga	WUSUS
192.168.2.14	Hiei	Exchange2019
192.168.2.19	Yukikaze	Opsi

Der Aufbau

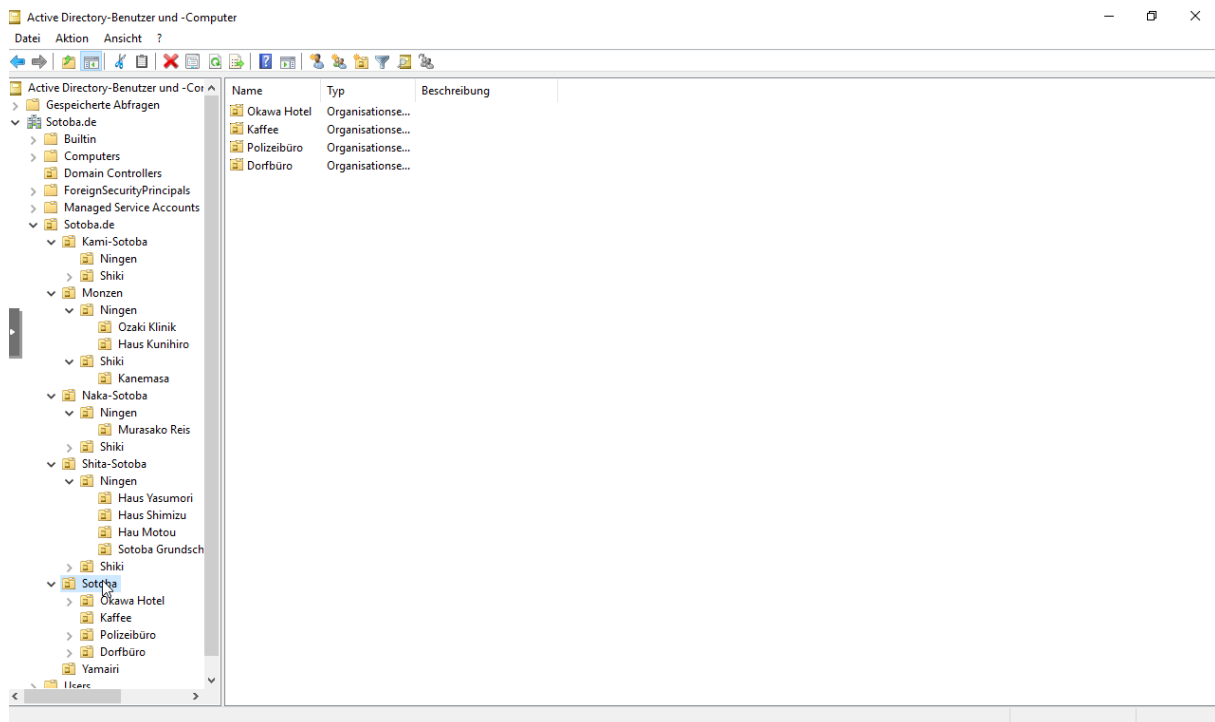
Als erstes habe ich Im Active Directory eine neue Organisationseinheit (OU) als Haupt OU angelegt und entsprechend benannt



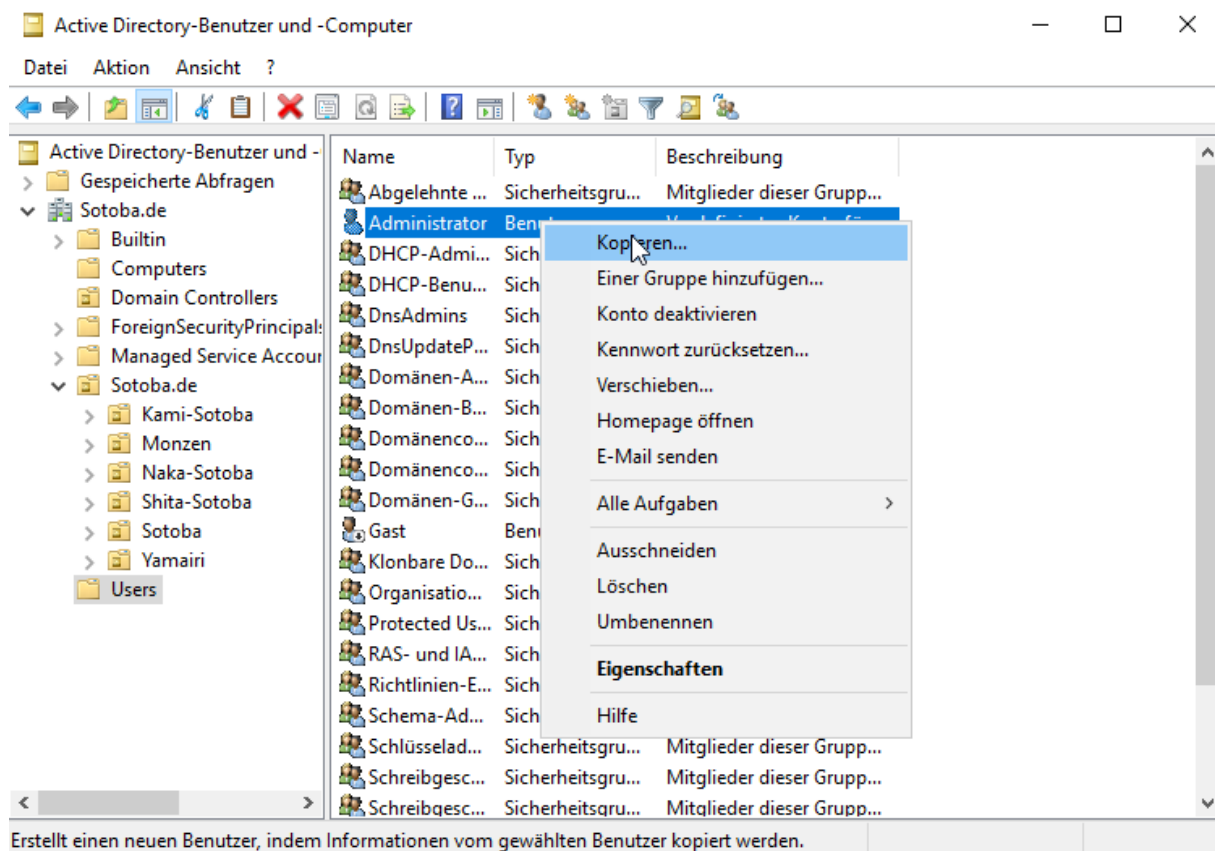
Und in dieser OU habe ich dann diverse Unter-OUs erstellt und benannt



Das Ergebnis ist dann folge AD-Struktur



Jetzt wird das Dorf mit Leben gefüllt, dazu erstelle ich ein paar Benutzer. Unter anderem einen anderen Admin. Da kopiere ich das Original Administratorkonto



Und fülle dann die Informationen aus

Objekt kopieren - Benutzer

Erstellen in: Sotoba.de/Users

Vorname: Initialen:

Nachname:

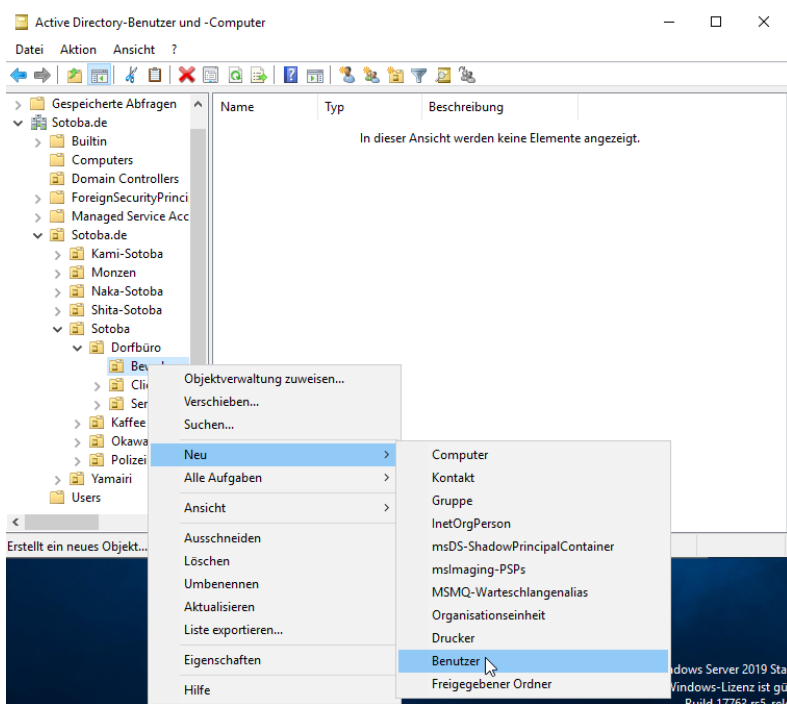
Vollständiger Name:

Benutzeranmeldename: @Sotoba.de

Benutzeranmeldename (Prä-Windows 2000): SOTOBAN\'

< Zurück Weiter > Abbrechen

Als nächstes erstelle ich einen normalen Benutzer direkt Einwohner OU des Dorfbüros, der auch später als Vorlage gilt. Nutze für die Anmeldenamen erster Buchstabe des Vornamens mit Nachnamen



Neues Objekt - Benutzer

Erstellen in: Sotoba.de/Sotoba.de/Sotoba/Dorfbüro/Bewohner

Vorname: Nao Initialen:

Nachname: Yasumori

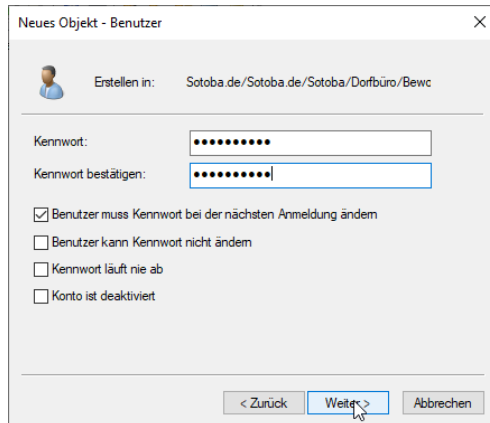
Vollständiger Name: Nao Yasumori

Benutzeranmeldename: NYasumori @Sotoba.de

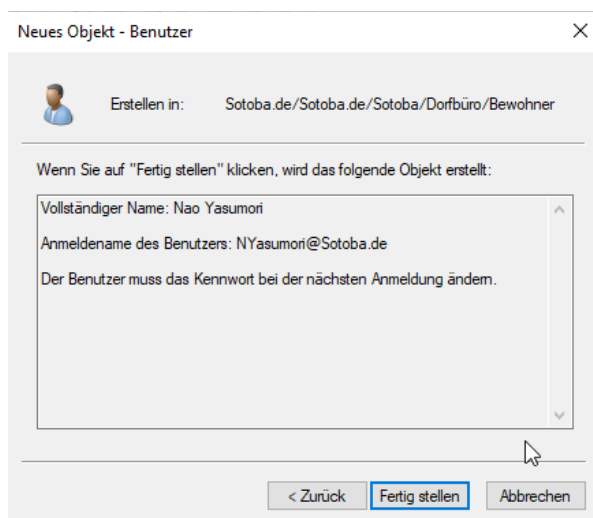
Benutzeranmeldename (Prä-Windows 2000): SOTOBAN\' NYasumori

< Zurück Weiter > Abbrechen

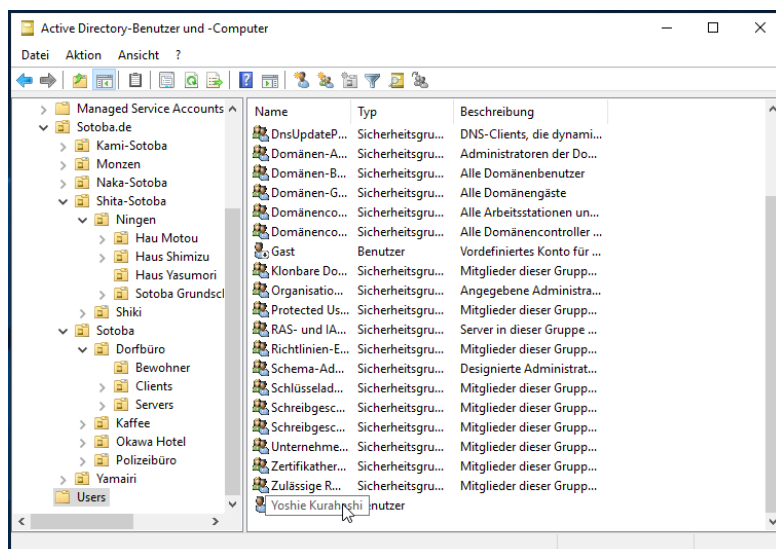
Und gebe dann das Passwort an.



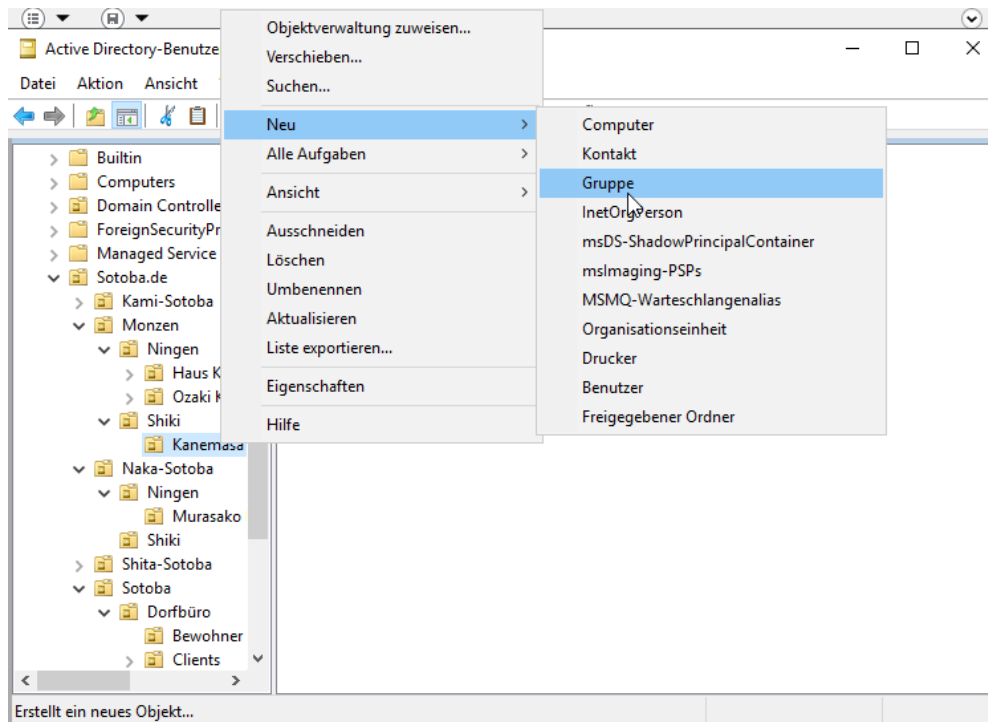
Und der Benutzer wird beim Klick auf fertig stellen erzeugt



Jetzt habe ich aber ein Problem, ich aus Versehen einen Benutzer in der OU User erstellt. Da Users ein Legacy-Container ist, der sich nicht mit GPOs versteht. Möchte ich den Account in die Benutzer-OU des Dorfbüros verschieben. Das beschreibe ich weiter unten.



Als nächstes erstelle ich die entsprechenden Gruppen.



Bei Gruppen sollte man nach dem AGDLP Prinzip vorgehen, das heißt

Benutzer (Accounts)

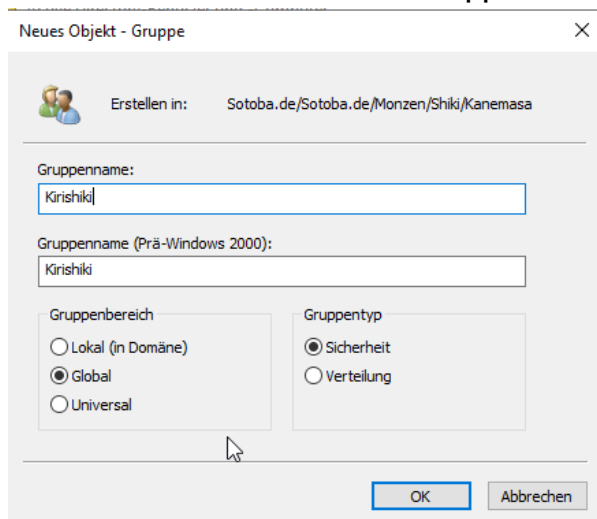
sind Mitglied in →

Globalen Gruppen (G) → bündeln Benutzer einer Funktion/Rolle je Domäne
werden Mitglied in →

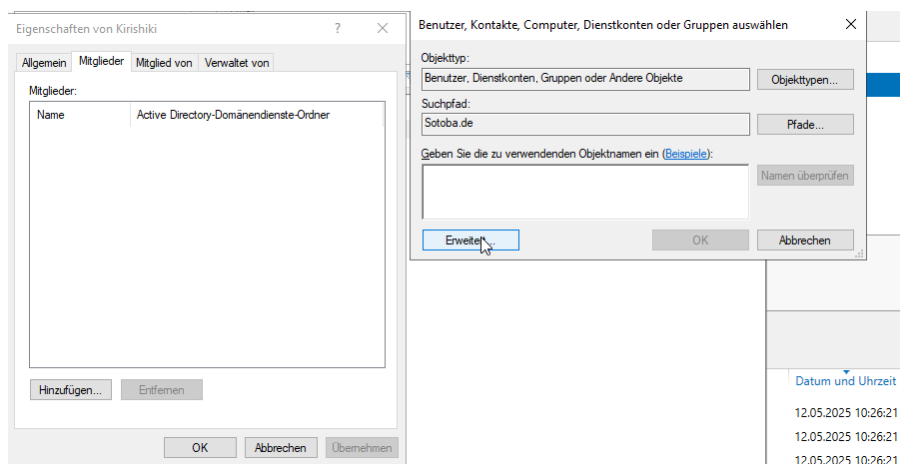
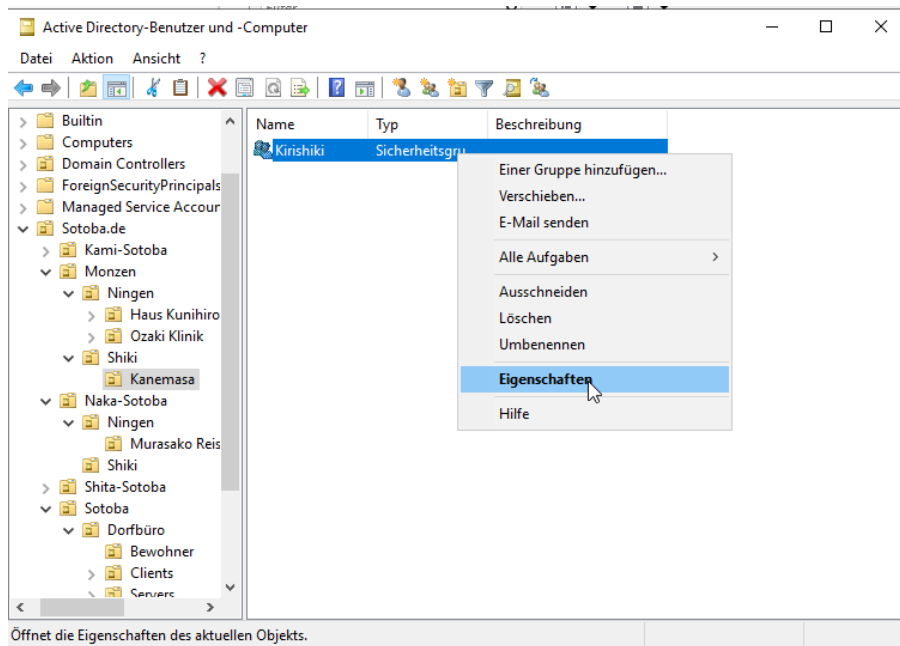
Domain-Lokale Gruppen (DL) → haben Zugriff auf bestimmte Ressourcen
haben →

Rechte (Permissions) auf z. B. Ordner, Freigaben, Drucker etc.

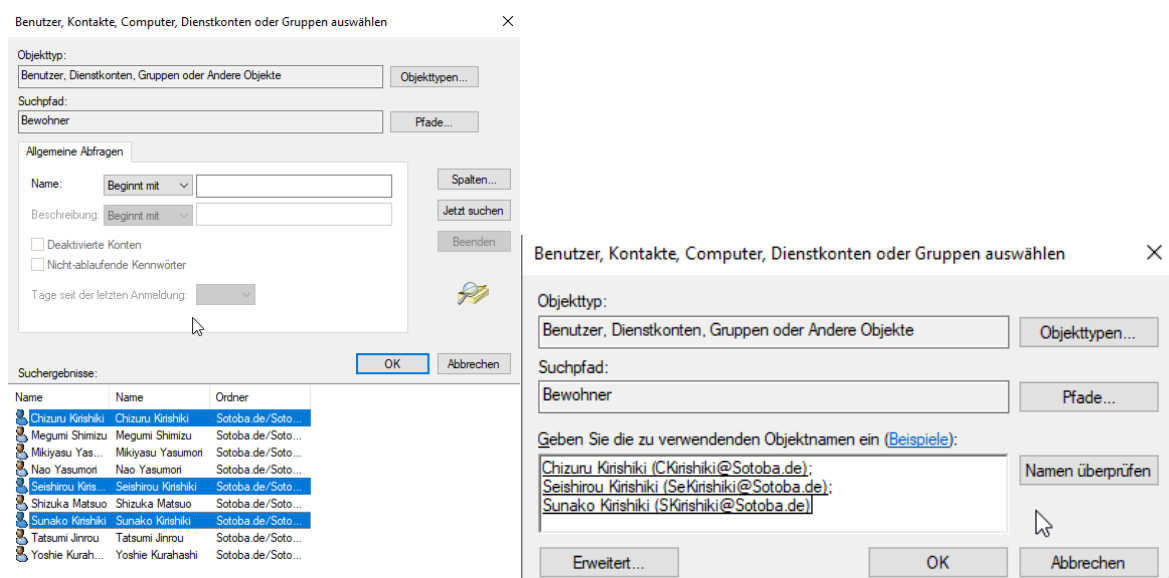
Also wähle ich eine Globale Gruppe.



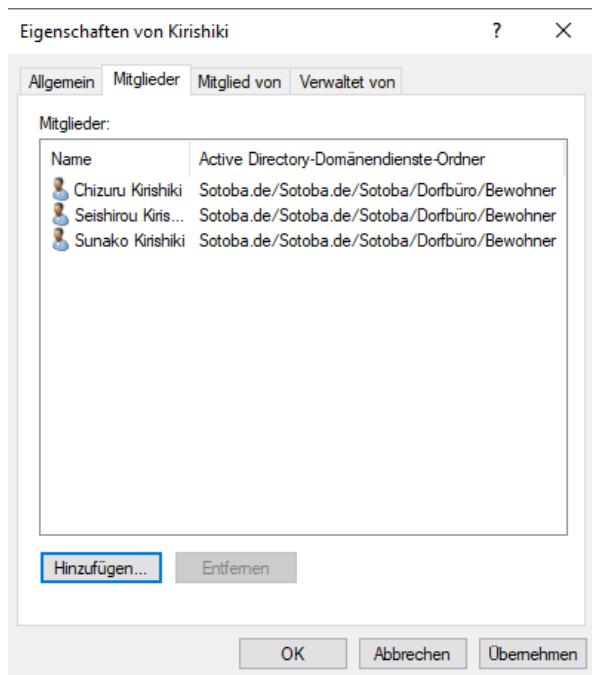
Und füge dieser Gruppe nun die Benutzer zu



Leider ist dieses Tool komisch. Denn eine detaillierte Suche, nach beispielsweise Nachnamen geht nicht, also muss ich mit die drei Benutzer selbst herausuchen.



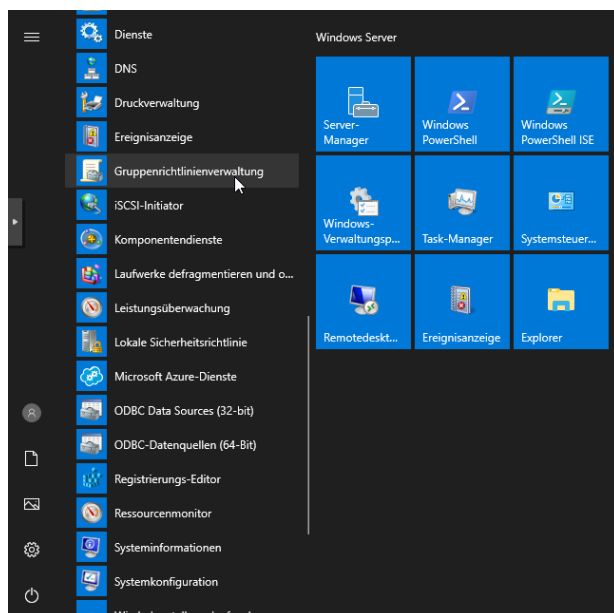
Und die drei sind zuhause



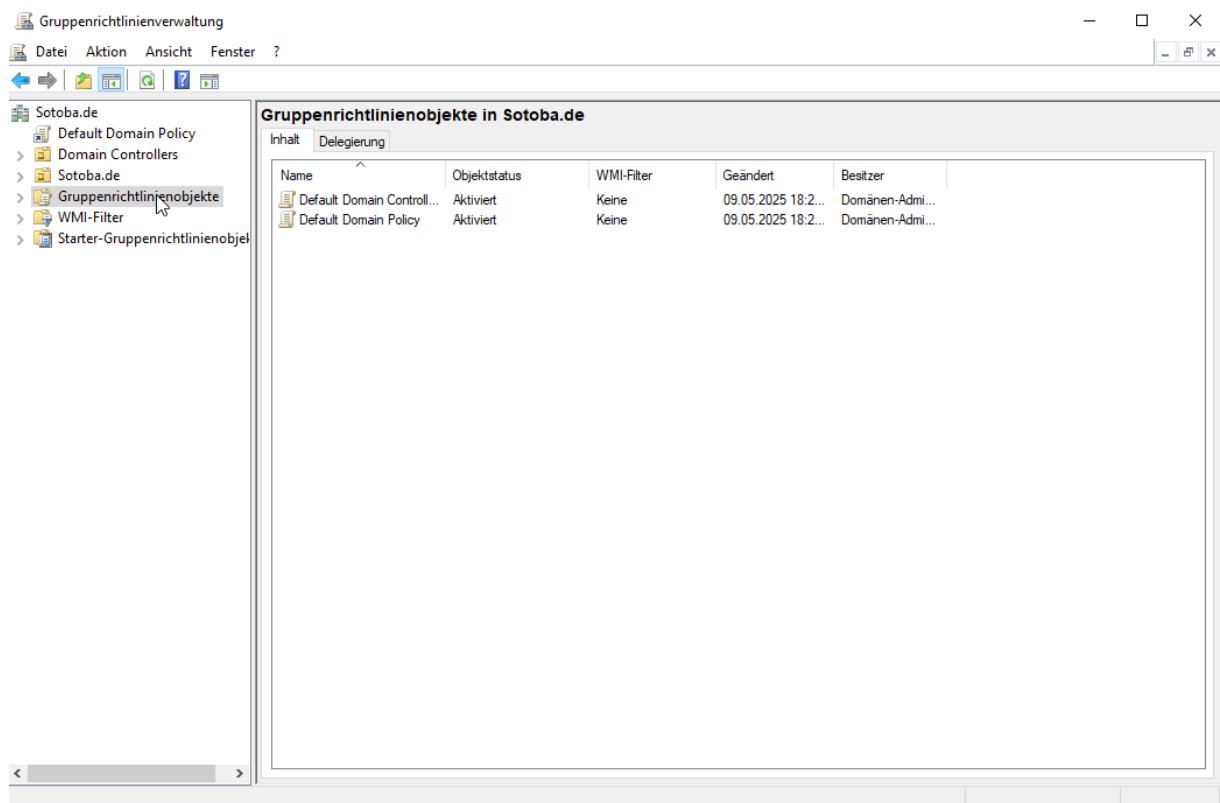
Die Regeln

Jede Gemeinschaft braucht Regeln. Von daher sind Gruppenrichtlinien ein spannendes Thema. Damit kann ich Registereinträge ändern.

Das mache ich mit der Gruppenrichtlinienverwaltung

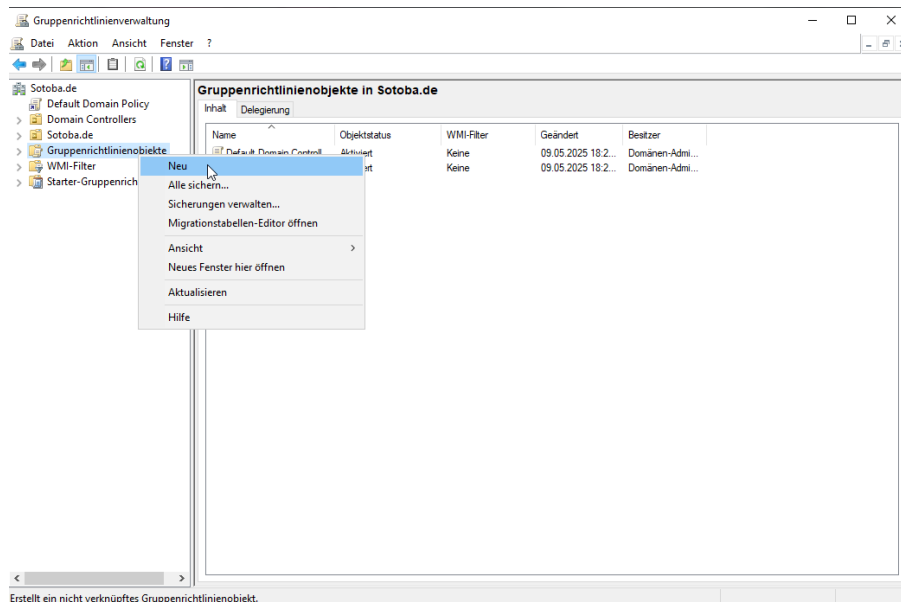


Die dann wie folgt aussieht

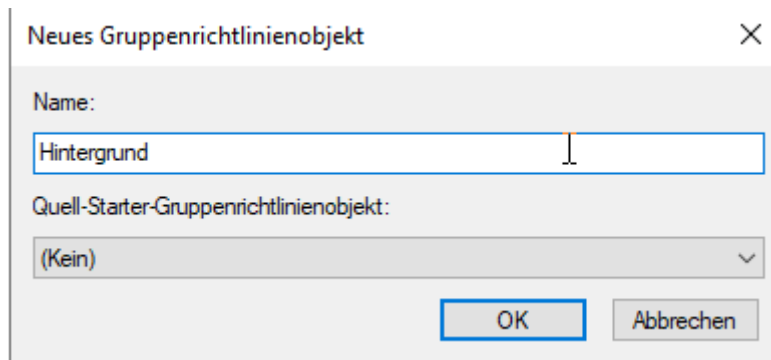


Als Beispiel möchte ich ein Hintergrundbild für alle Bewohner des Dorfes hinterlegen

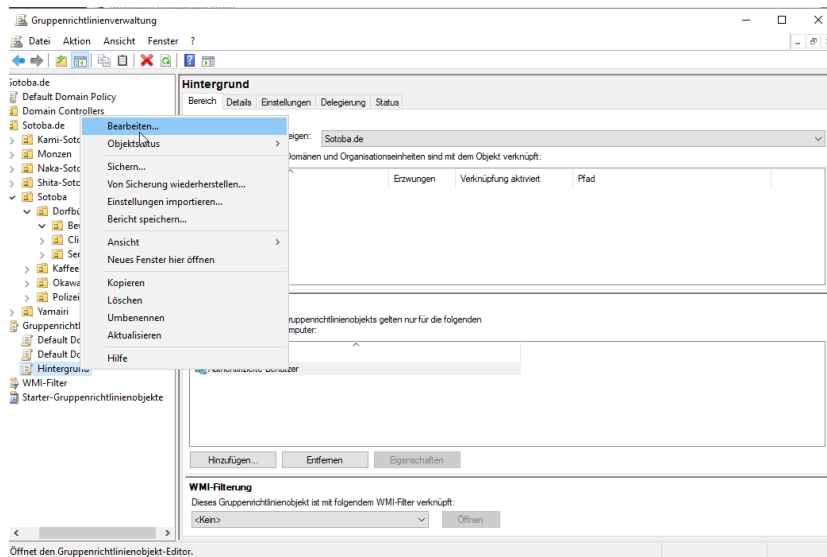
Dazu erstelle ich zuerst eine neue Gruppenrichtlinie



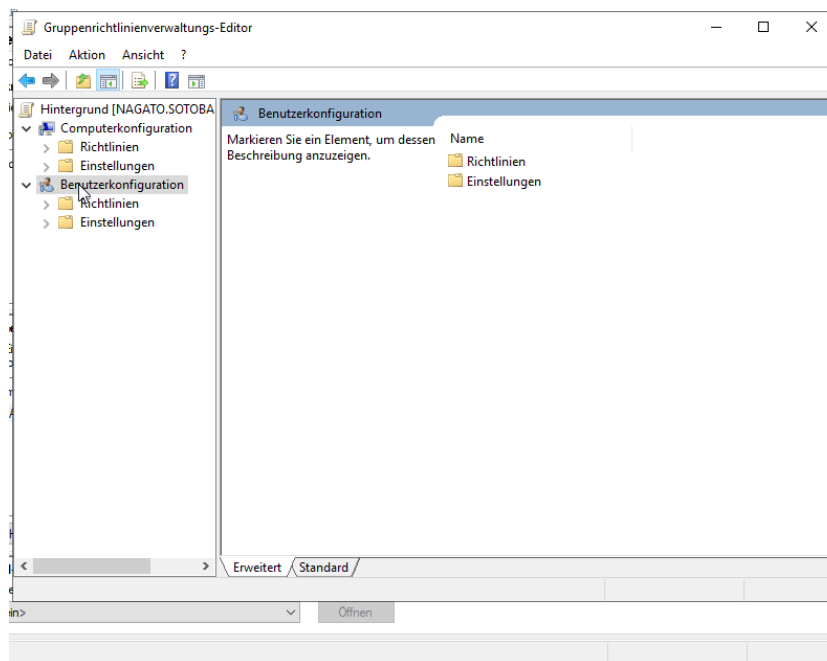
die ich dann entsprechend benenne,



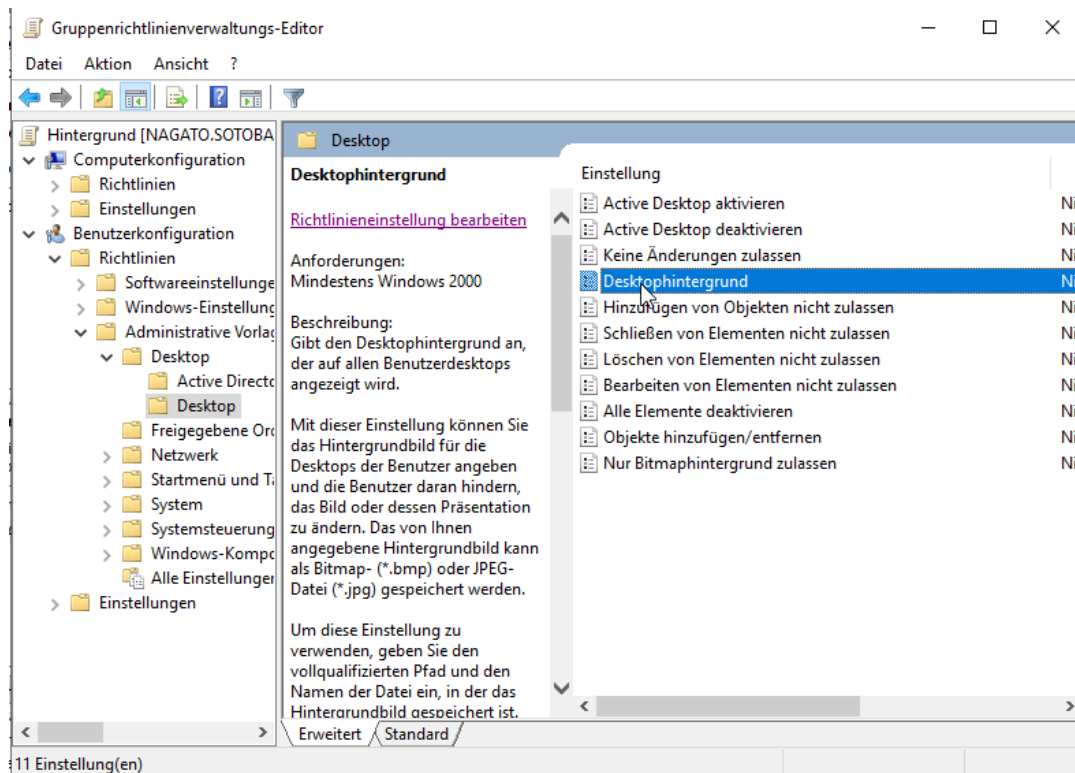
und bearbeite.



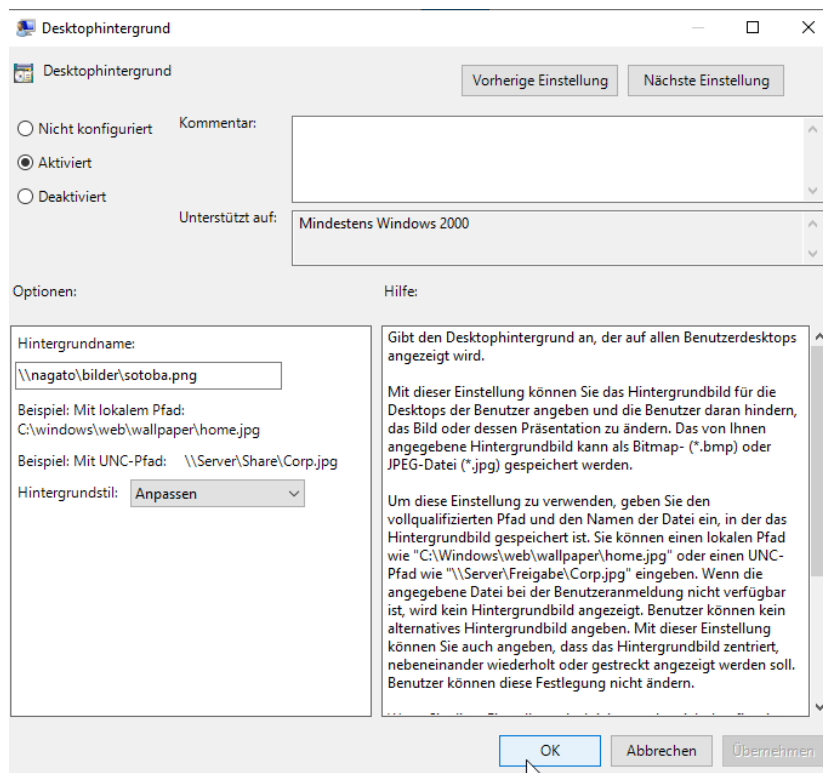
Das Hintergrundbild wird über die Benutzerkonfiguration gesetzt



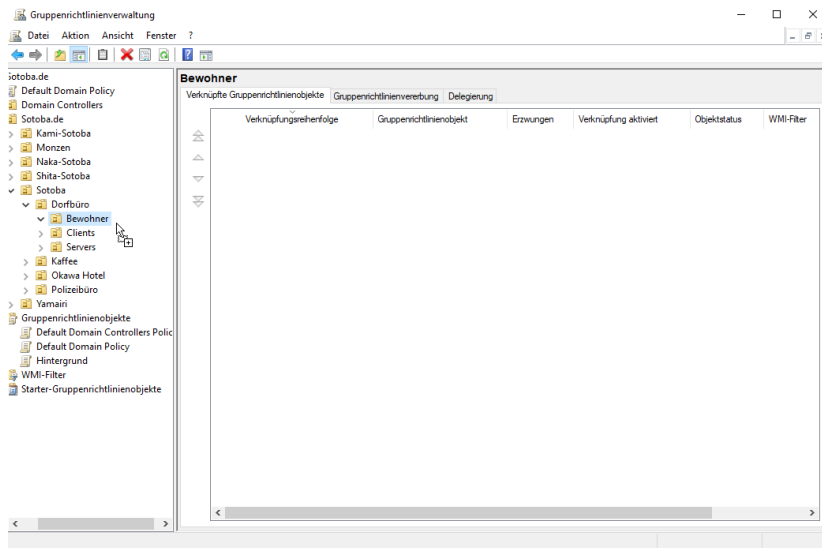
Dazu folge ich folgenden Pfad in den administrativen Vorlagen



Zuerst aktiviere ich diese Regel und gebe den Pfad für das Hintergrund ein. Das Bild liegt auf dem Server



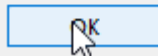
Danach verlinke ich die Gruppenrichtlinie mit der OU wo die Benutzer drin sind, via Drag und Drop.



Gruppenrichtlinienverwaltung

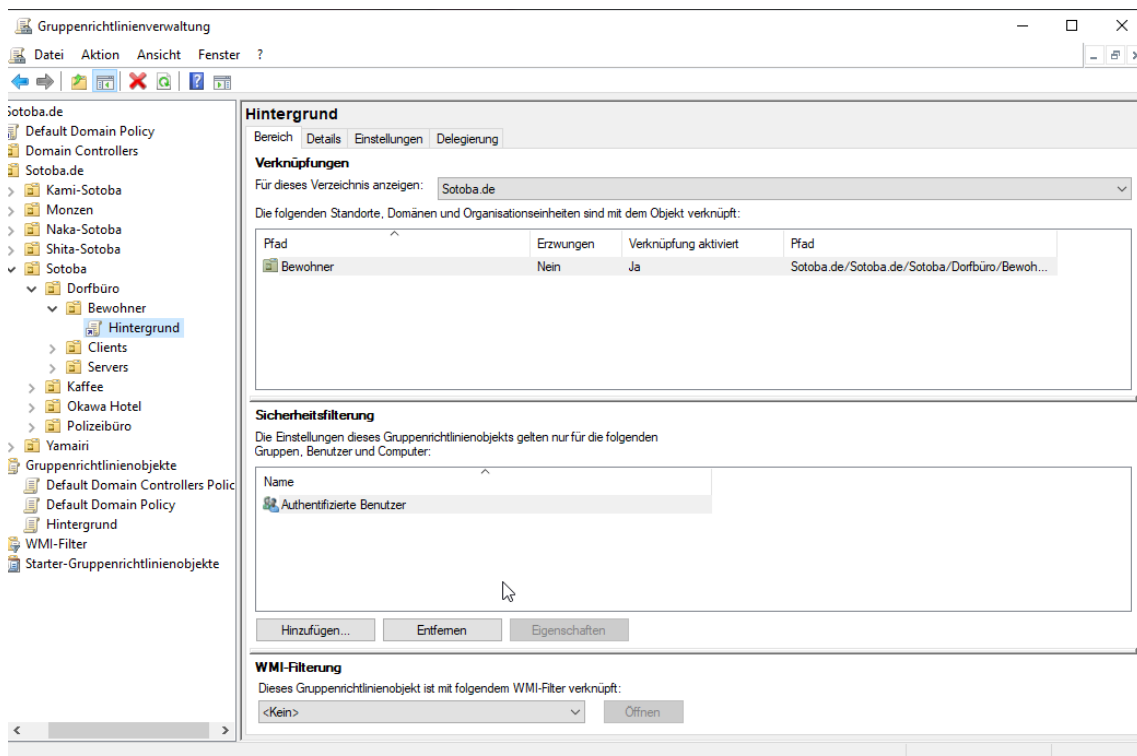


Möchten Sie die ausgewählten Gruppenrichtlinienobjekte mit dieser Organisationseinheit verknüpfen?

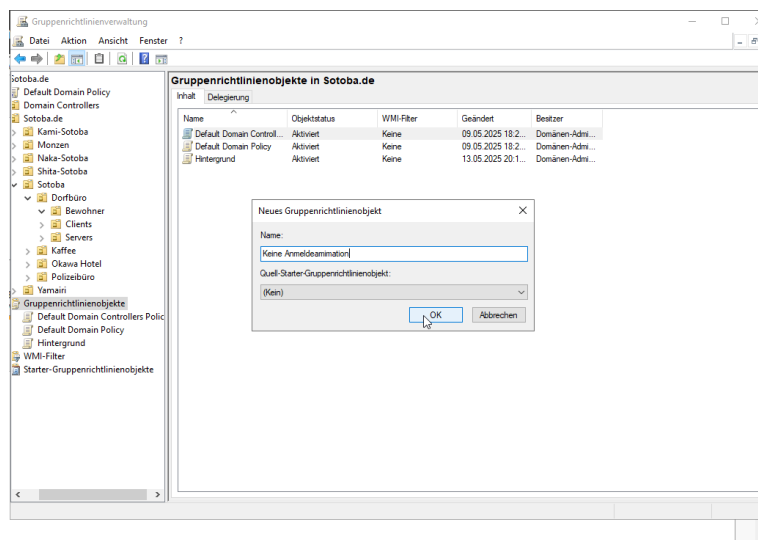


Abbrechen

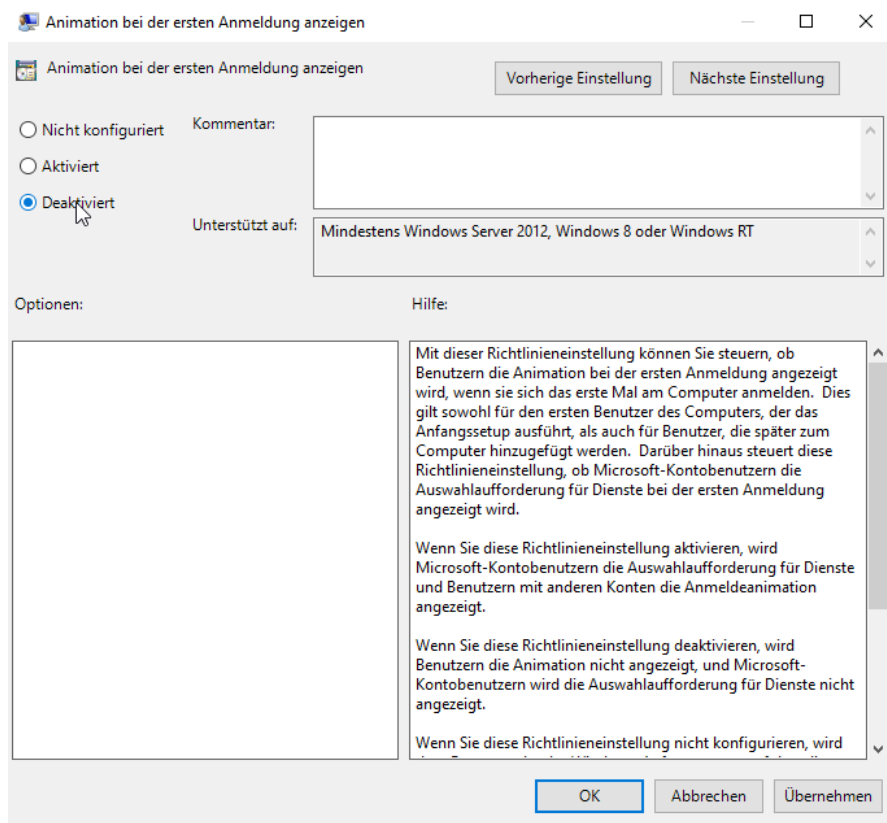
Das Ganze sieht dann später so aus. Eine Gruppenrichtlinie die mit der OU Benutzer verlinkt ist.



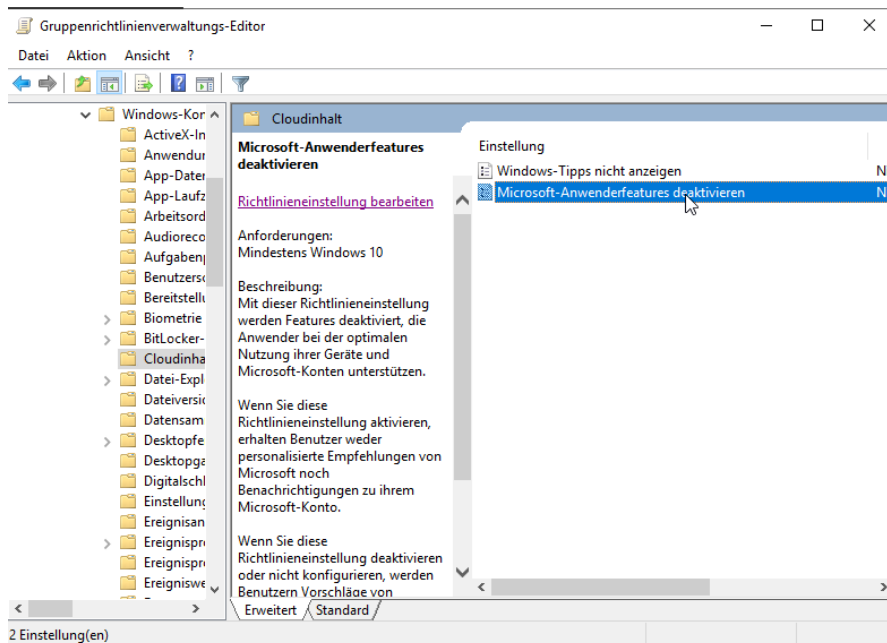
Dazu erstelle ich folgende Gruppenrichtlinie

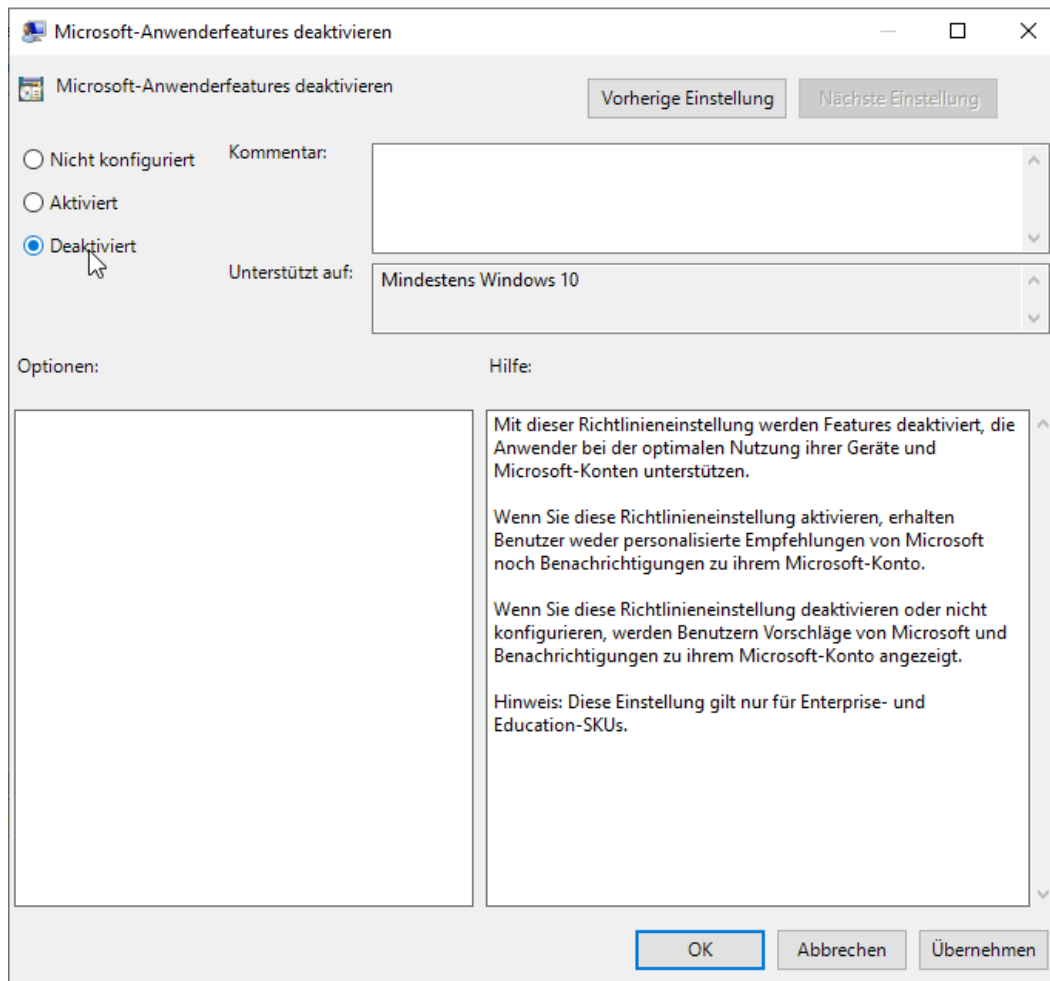


Und suche die Funktion „Animation bei der ersten Anmeldung“.

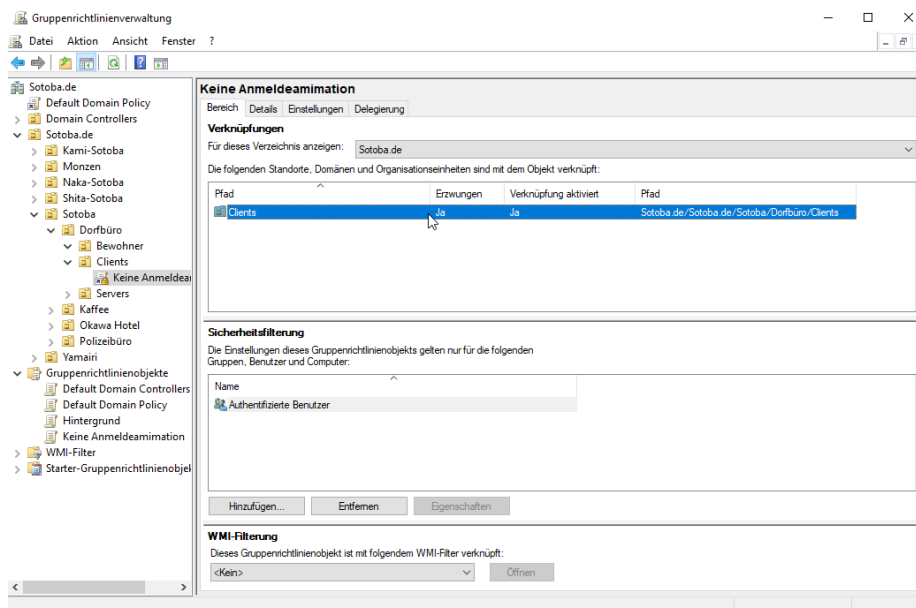


Und zusätzlich die Cloud Inhalte deaktivieren

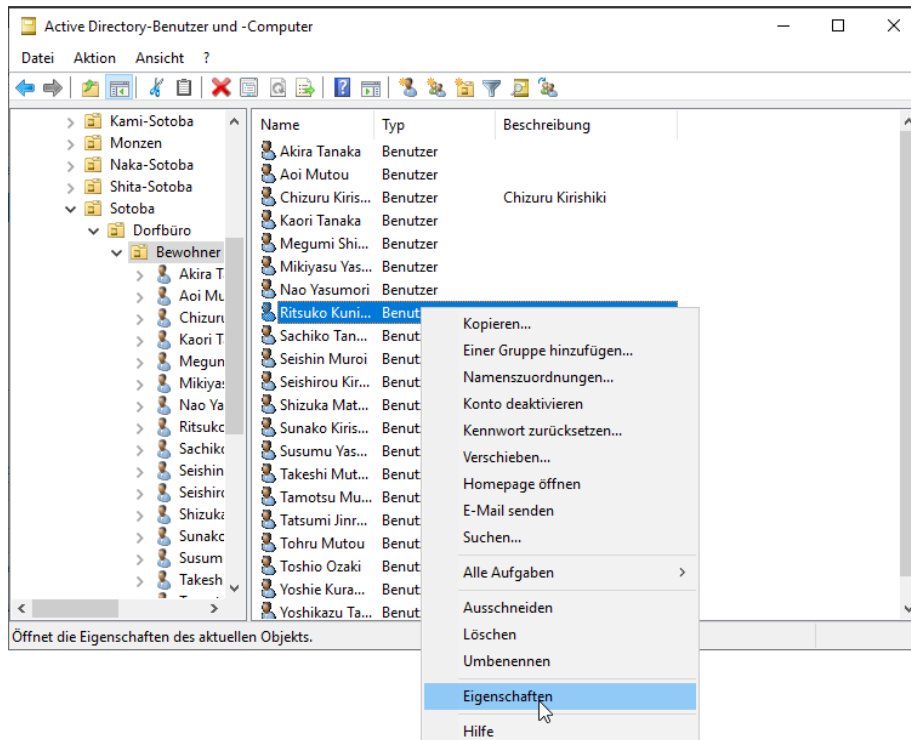




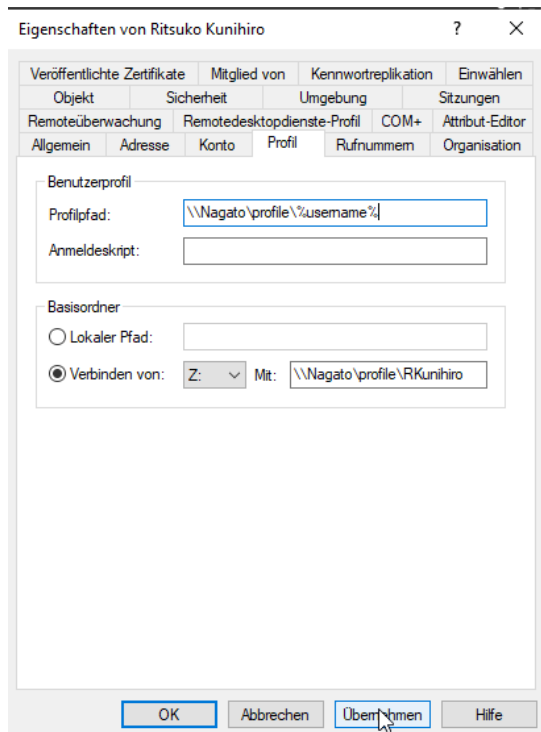
Als letztes verlinke ist diese GPO mit der entsprechenden OU wo die Computer sind. Und aktiviere das Erzwingen.



Also, weiter geht's mit dem servergespeicherten Profil. Um diese Profile zu aktivieren, gehe ich wieder in AD und suche mir einen Benutzer aus.

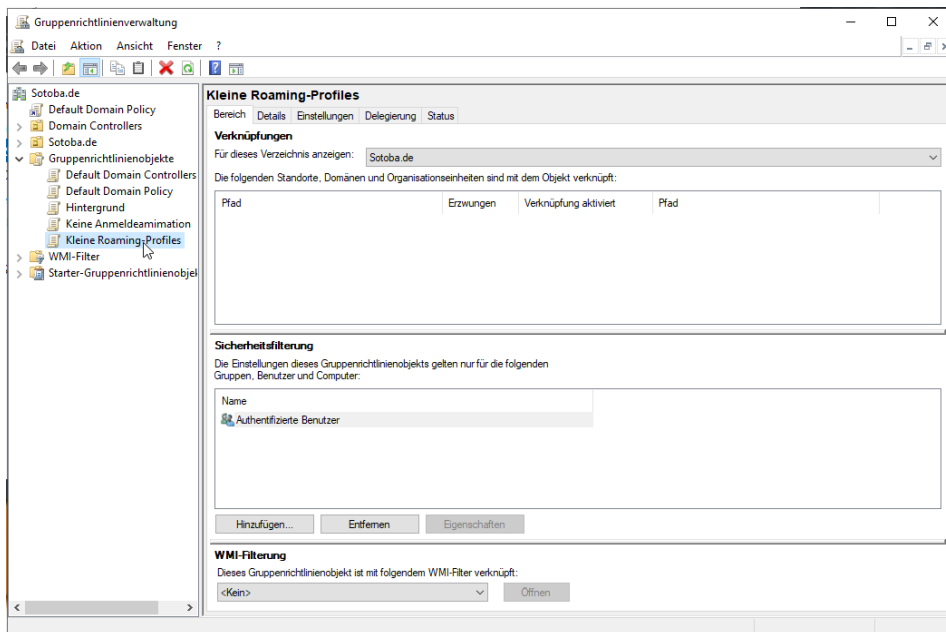


Und füge bei dem Konto dann den Pfad zum servergespeicherten Profil hinzu:

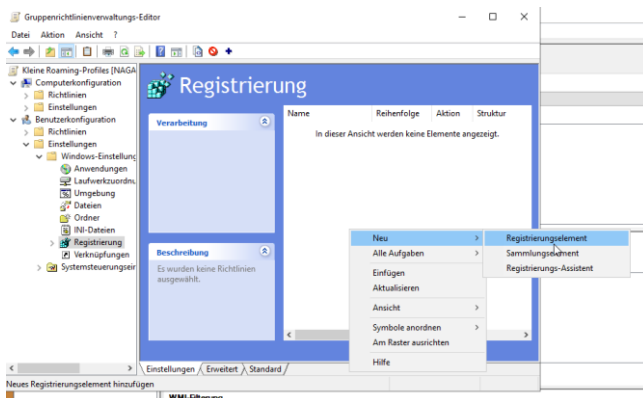


Der Benutzer kann sein Hintergrund Bild selbst setzen und es wird auf dem Server gespeichert.

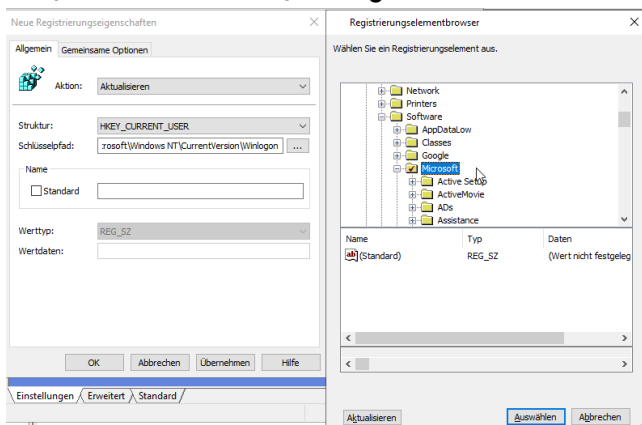
Da diese Profile alles speichern das beispielsweise auf den Desktop ist. Sind diese Profile nicht empfehlenswert, da sie zu groß werden können. Deswegen begrenze ich die Größe der Profile. Dazu erstelle ich eine Richtlinie.



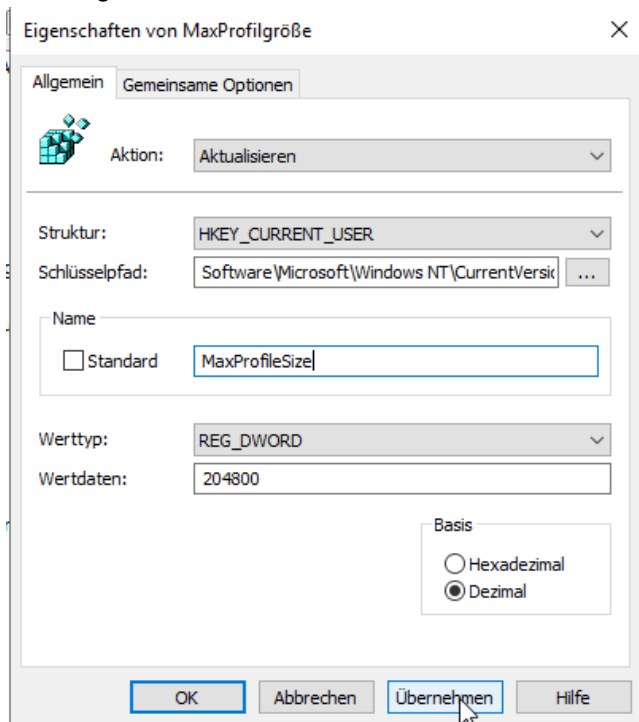
Die ich dann wie folgt bearbeite



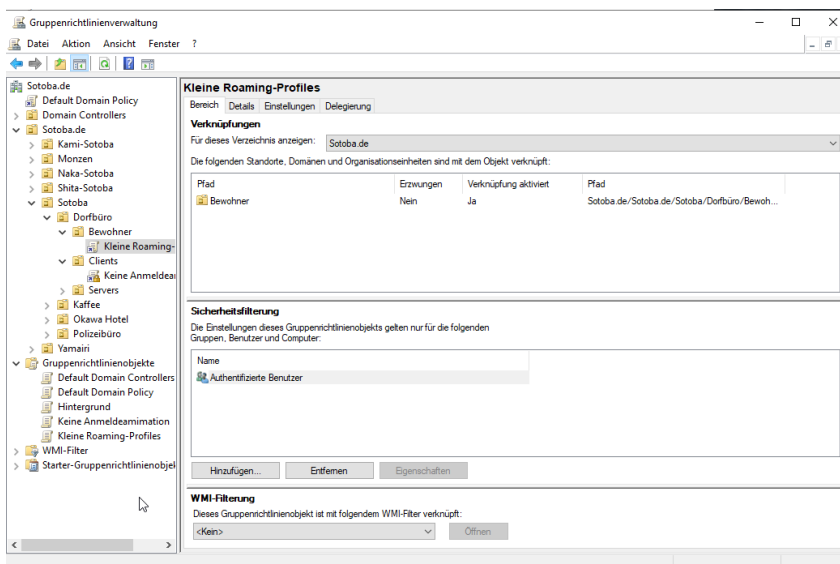
Und erstelle eine neue Eigenschaft im Schlüsselfad „Software\Microsoft\Windows NT\CurrentVersion\Winlogon“



Mit folgenden Werten

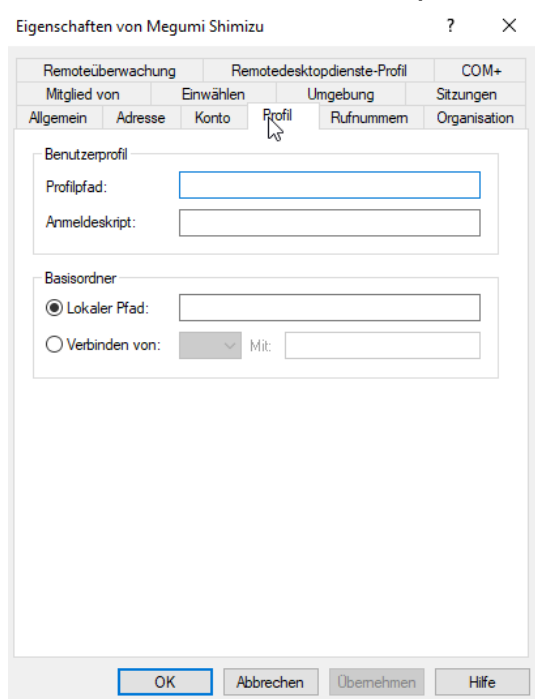


Danach verlinke ich die neue Regel mit der Benutzergruppe



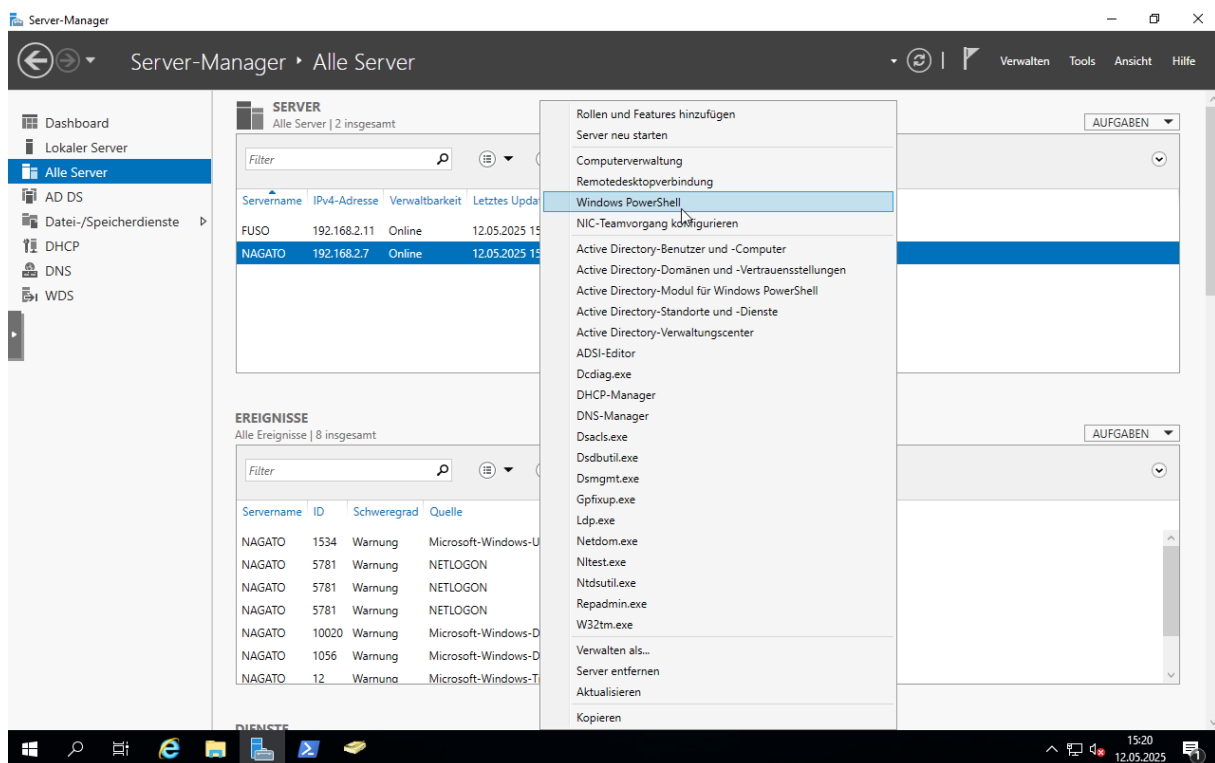
(kleine Info, hat noch nicht so funktioniert wie gewünscht)

Wenn ich in die Eigenschaften eines Benutzers gehe, finden sich dort viele Informationen, wie zum Beispiel das Profil.



Benutzerprofile sind heute nicht mehr gern gesehen, da sie als veraltet gelten und störanfällig sind.

Die servergespeicherten Basisordner hingegen sind interessant. Um ein solches zu erstellen, gehe ich via Remote Powershell auf den DC



In Powershell erstelle ich mir dann einen Ordner für die Profile und gebe diesen frei. Zum Schluss schaue ich, ob der Ordner erfolgreich freigegeben wurde

```
[Nagato.Sotoba.de]: PS H:\> mkdir Profile

Verzeichnis: H:\

Mode                LastWriteTime         Length Name
----                -
d-----         12.05.2025        17:16         Profile

[Nagato.Sotoba.de]: PS H:\> new-smbshare "h:\profile" -name "profile" -fullaccess "administratoren","system","Domänen-Benutzer"

Name      ScopeName Path      Description
-----
profile *      h:\profile

[Nagato.Sotoba.de]: PS H:\> get-smbshare

Name      ScopeName Path      Description
-----
ADMIN$ *      C:\Windows Remoteverwaltung
C$ *      C:\ Standardfreigabe
H$ *      H:\ Standardfreigabe
IPC$ *      Remote-IPC
NETLOGON *      C:\H\Ad\SYVOL\sysvol\Sotoba.de\SCRIPTS Ressource für Anmeldeserver
profile *      h:\profile
SYVOL *      C:\H\Ad\SYVOL\sysvol Ressource für Anmeldeserver

[Nagato.Sotoba.de]: PS H:\> 
```

Nun gebe ich bei dem Basisordner folgendes ein. Das %username% wird d angewendet, um der Freigabe den Anmeldename zu geben

The screenshot shows the 'Eigenschaften von Megumi Shimizu' (Properties of Megumi Shimizu) dialog box. The 'Basisordner' (Basic Folder) tab is active. Under the 'Benutzerprofil' (User Profile) section, the 'Profilpfad' (Profile path) and 'Anmeldeskript' (Logon script) fields are empty. In the 'Basisordner' section, the 'Verbinden von' (Connect from) radio button is selected. The 'Z:' drive is chosen from the dropdown, and the path '\\Nagato\profile\MShimizu' is entered in the 'Mit:' (With) field. The 'OK' button is highlighted.

Und schaue noch ob der Ordner richtig gesetzt wurde,

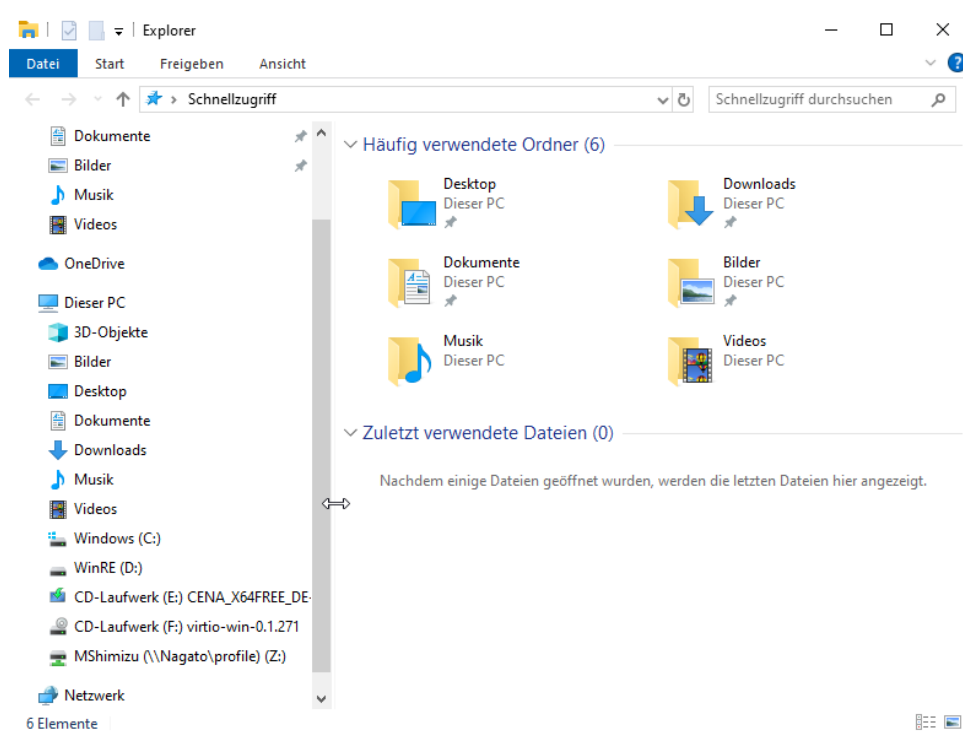
```
[Nagato.Sotoba.de]: PS H:\> cd profile
[Nagato.Sotoba.de]: PS H:\profile> dir

Verzeichnis: H:\profile

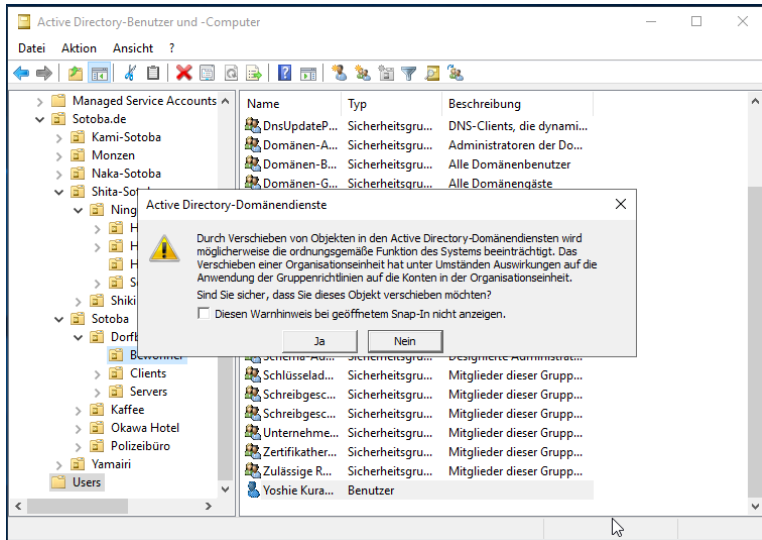

Mode                LastWriteTime         Length Name
----                -
d-----         12.05.2025   15:59                MShimizu

[Nagato.Sotoba.de]: PS H:\profile>
```

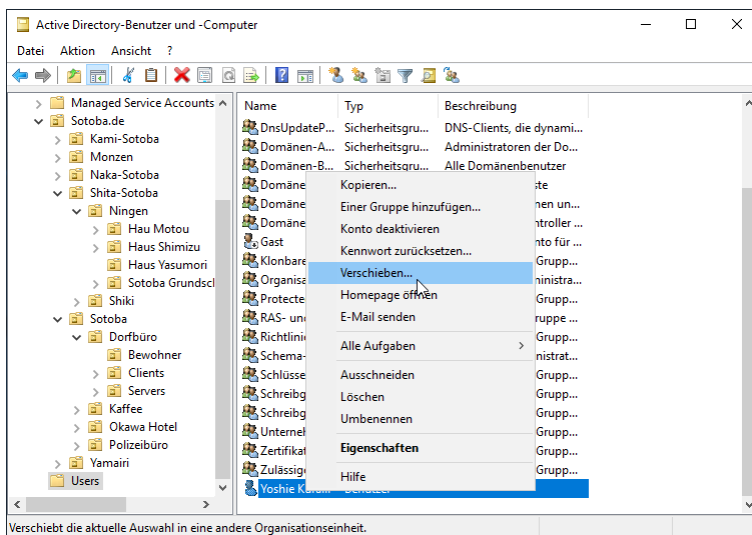
und der Benutzer hat sein Basisordner als Netzwerklaufwerk



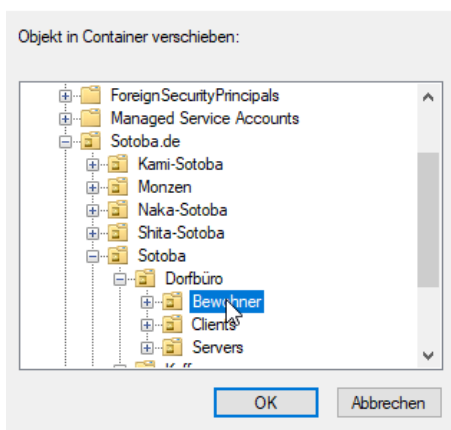
Wie ich anfangs erwähnte, habe ich da noch ein Problem mit einem Benutzer in der falschen OU. Ich könnte nun mit Drag and Drop den Benutzer verschieben, aber gibt eine Warnung.



Stattdessen verschiebe ich den Benutzer.

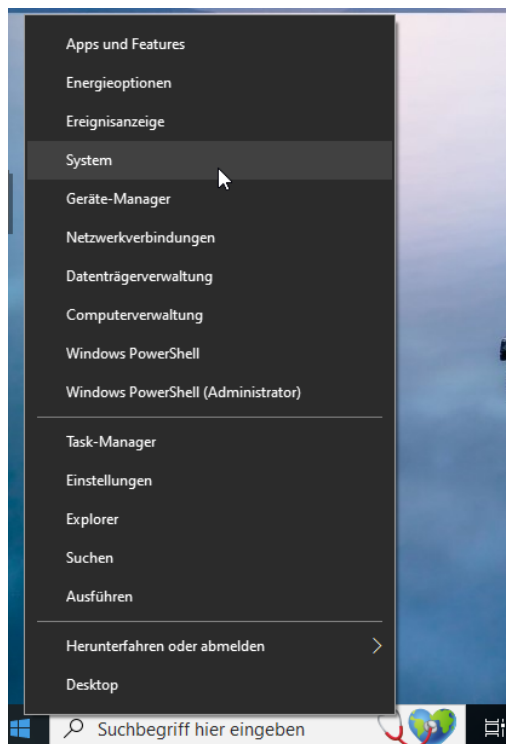


Verschieben

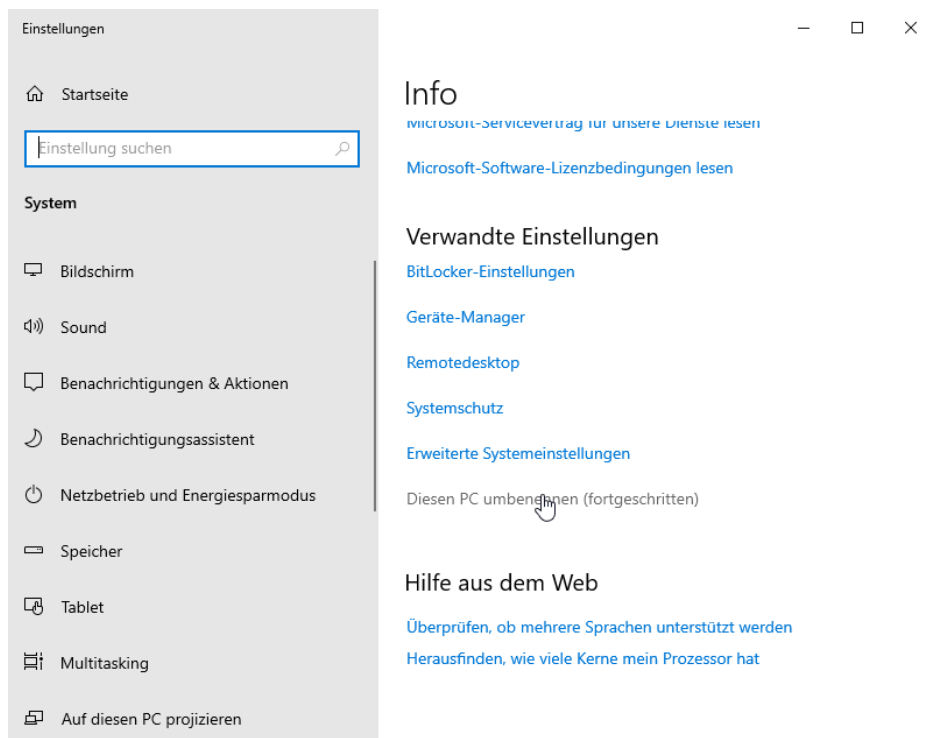


Da ist der Benutzer am richtigen Ort. Das geht genauso mit Computer.

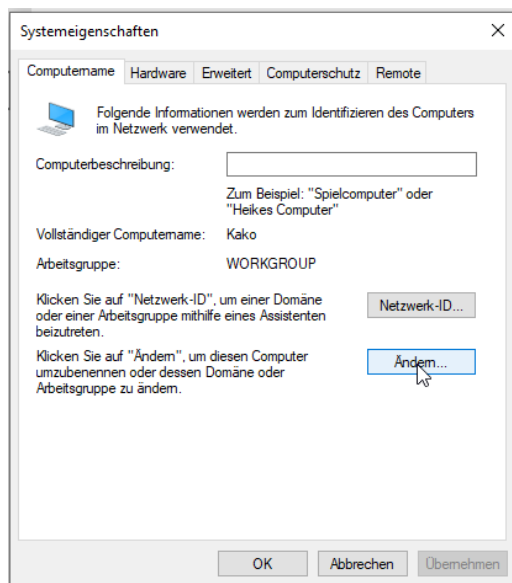
Wie füge ich einen Rechner der Domäne hinzu. Dazu gehe ich über die Startleiste, rechte Maustaste klickend auf System



und suche mir dort den Punkt



Wenn ich dort auf Ändern klicke, kann ich den Rechner nicht nur umbenennen, sondern auch der Domäne hinzufügen.



Dort gebe ich den Domännennamen ein, klicke auf weiter und gebe dann die Das Admin Konto an. Danach ist eine erfolgreiche Einladung zu sehen

