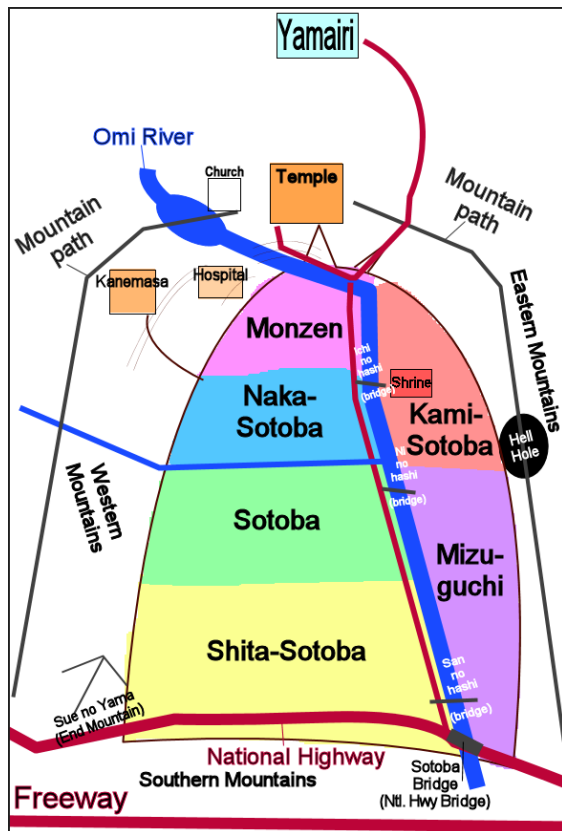


## Die Active Directory Domäne Sotoba

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



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.

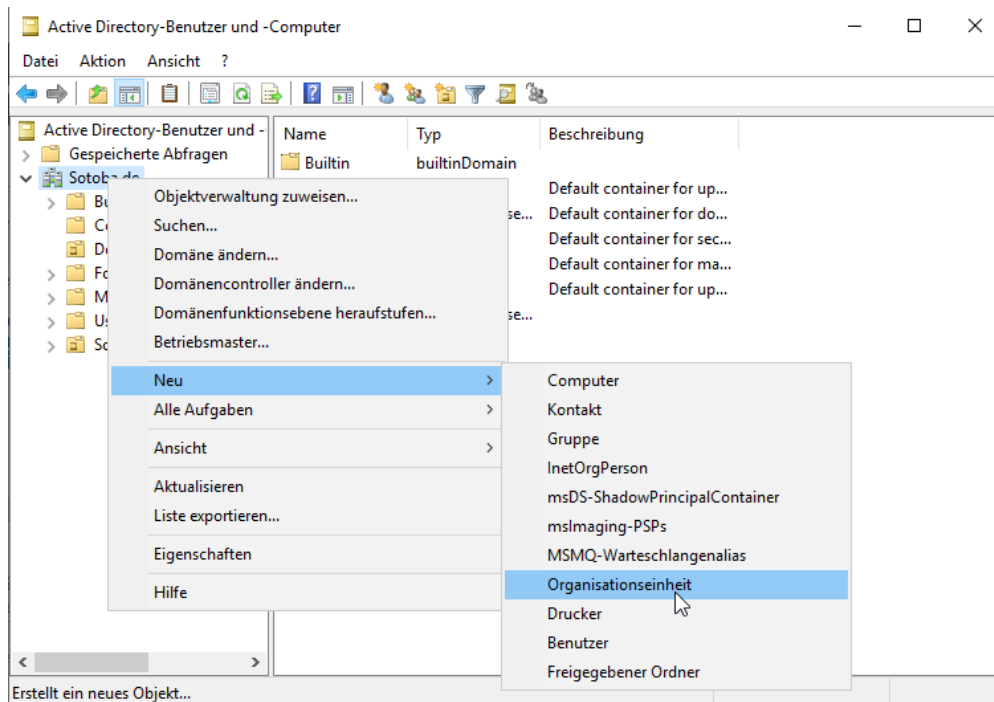
Umgebung	Software
Server-Software	Windows Server 2019 Proxmox, TrueNAS
Client-Software	Windows 10 Enterprise, Windows 11 Enterprise Ubuntu

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

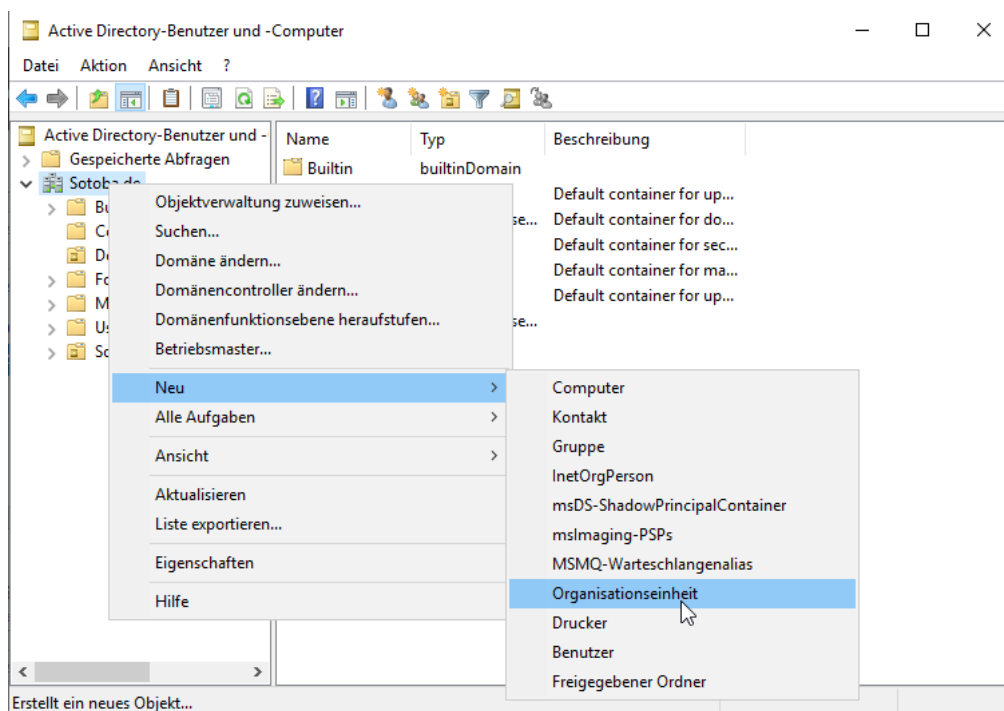
Rechner mit	Namen
Hypervisor	Hiryu, Soryu, Kaga, AkagiA
Domain Controller	Musashi, Yamato, Nagato, Mutsu
Andere Serverdienste	Fuso, Yamashiro, Hiei, Haruna, Kirishima
Windows Client	Mogami, Takao, Ashigara, Haguno.
Linux Client	Kuma, Natori, Sendai, Nagara
Container	Fubuki, Kagero, Shimakaze, Akizuki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

Aufbau der Domäne.

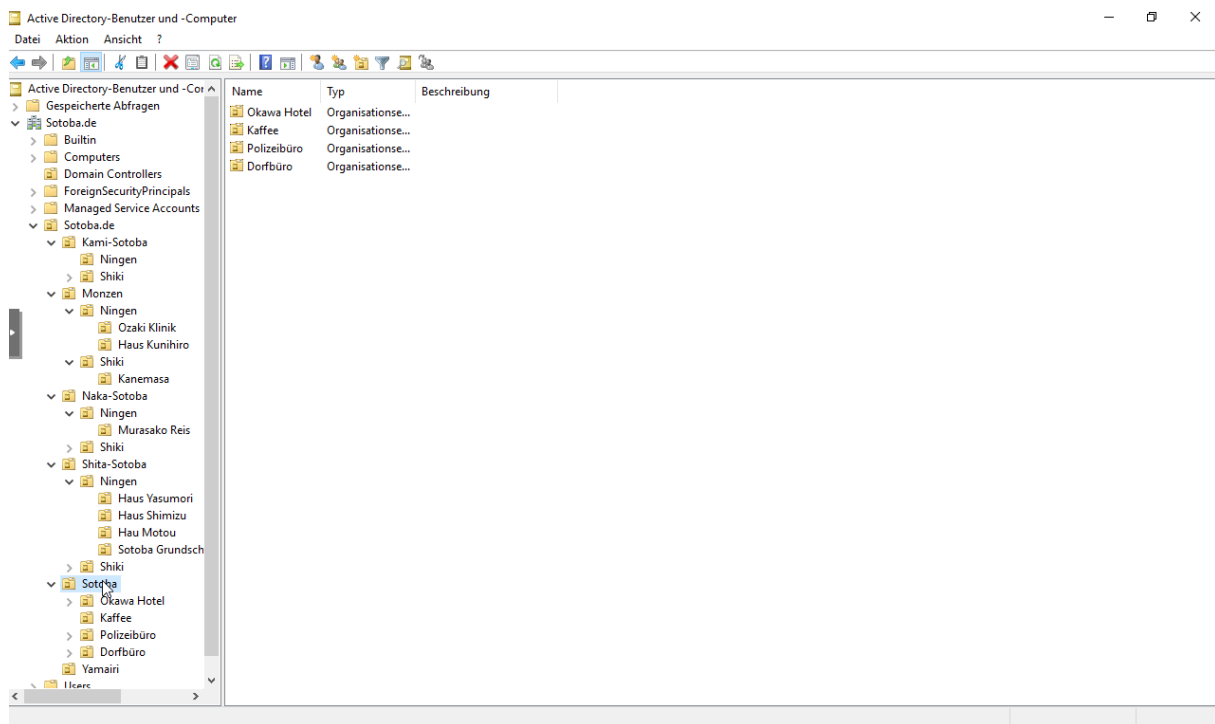
Als erstes habe ich Im Active Directory eine neue Organisationseinheit (OU) als Haupt OU angelegt und entsprechend benannt



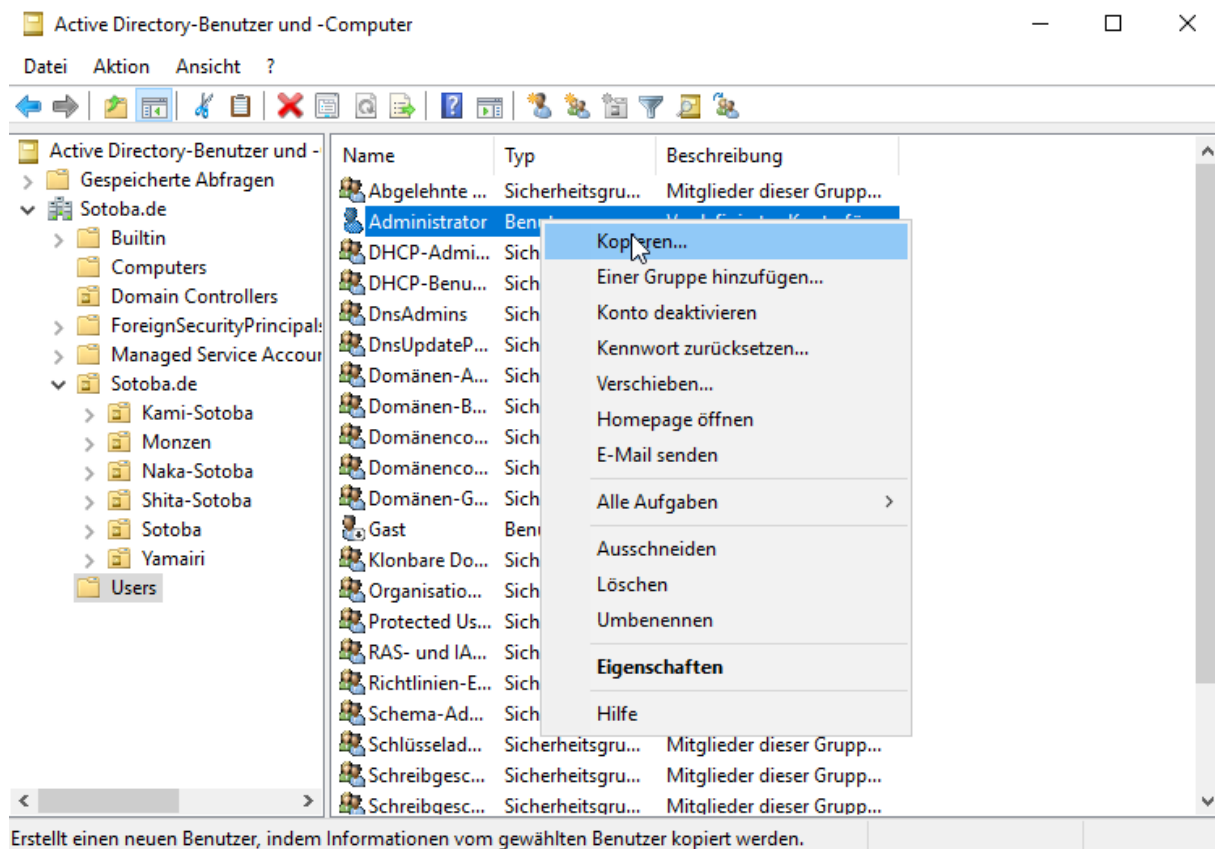
Und in dieser OU habe ich dann diverse Unter-OUs erstellt und benannt



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:

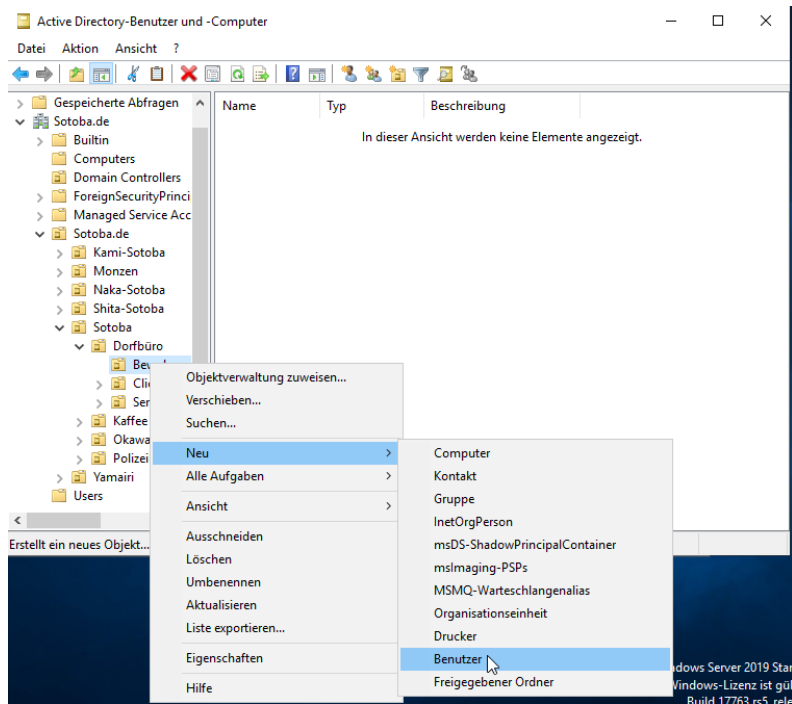
Benutzeranmeldename:  @Sotoba.de ▾

Benutzeranmeldename (Prä-Windows 2000): SOTOBA\

---

< 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

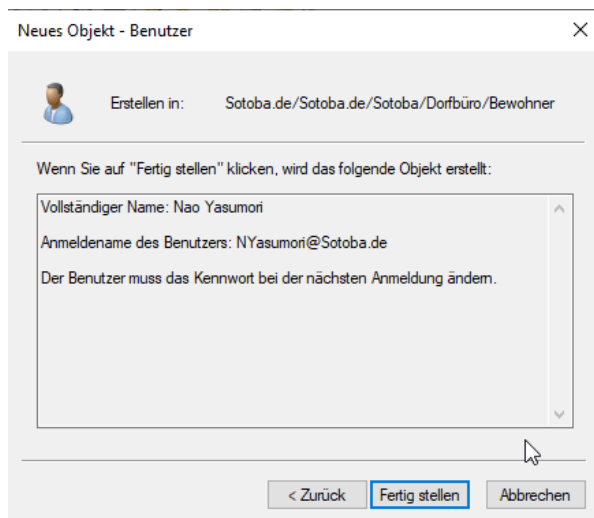


The 'Neues Objekt - Benutzer' dialog box is shown. The 'Erstellen in:' (Create in:) field is set to 'Sotoba.de/Sotoba.de/Sotoba/Dorfbüro/Bewohner'. The 'Vorname:' (First name) field contains 'Nao' and the 'Nachname:' (Last name) field contains 'Yasumori'. The 'Vollständiger Name:' (Full name) field shows 'Nao Yasumori'. The 'Benutzeranmeldename:' (User logon name) field contains 'NYasumori' and the domain dropdown is set to '@Sotoba.de'. Below this, the 'Benutzeranmeldename (Prä-Windows 2000):' (User logon name (Pre-Windows 2000)) section shows 'SOTOBA\' and 'NYasumori'. At the bottom, there are three buttons: '< Zurück' (Back), 'Weiter >' (Next), and 'Abbrechen' (Cancel). The 'Weiter >' button is highlighted by the mouse.

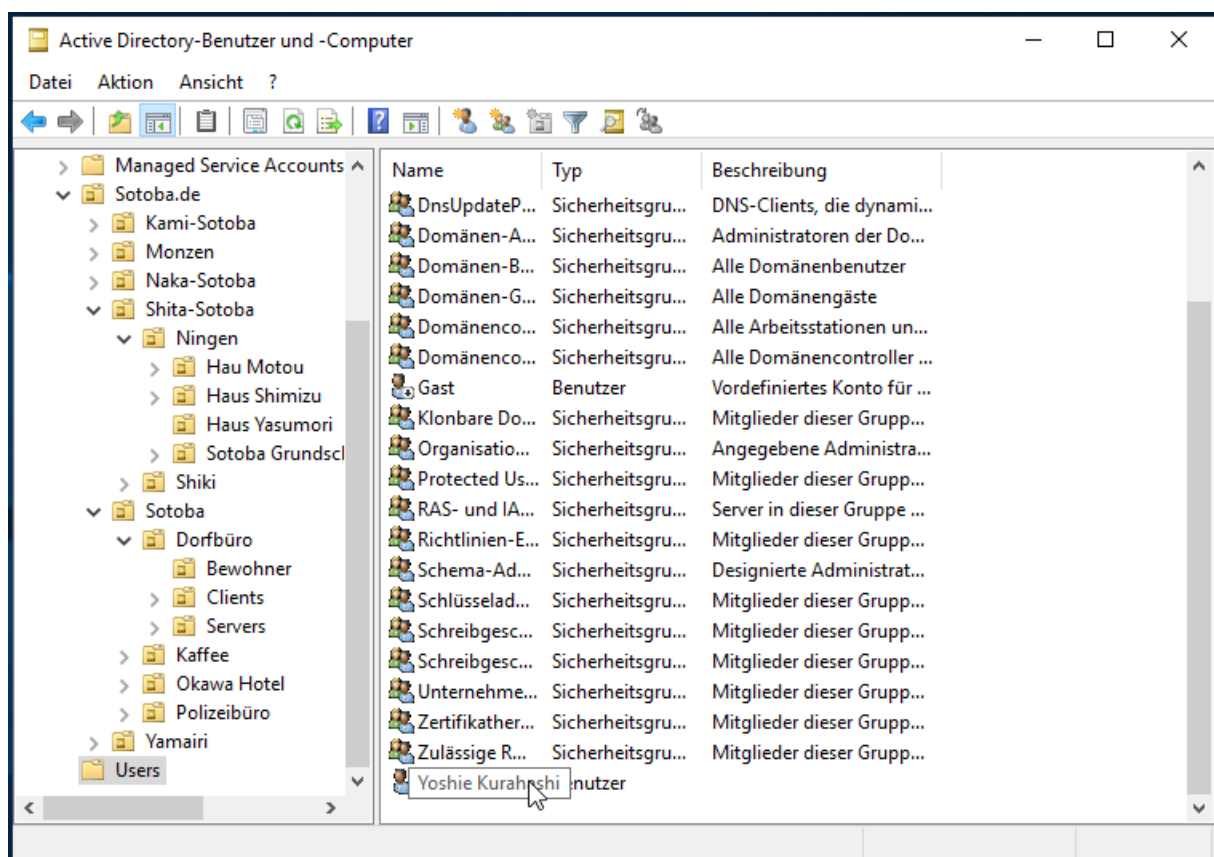
Und gebe dann das Passwort an.

The 'Neues Objekt - Benutzer' dialog box is shown, now at the password setup step. The 'Kennwort:' (Password) field is filled with dots, and the 'Kennwort bestätigen:' (Confirm password) field is also filled with dots. Below these fields are four checkboxes:   
☒ Benutzer muss Kennwort bei der nächsten Anmeldung ändern (User must change password at next login)   
☐ Benutzer kann Kennwort nicht ändern (User cannot change password)   
☐ Kennwort läuft nie ab (Password never expires)   
☐ Konto ist deaktiviert (Account is disabled)   
At the bottom, there are three buttons: '< Zurück' (Back), 'Weiter >' (Next), and 'Abbrechen' (Cancel). The 'Weiter >' button is highlighted by the mouse.

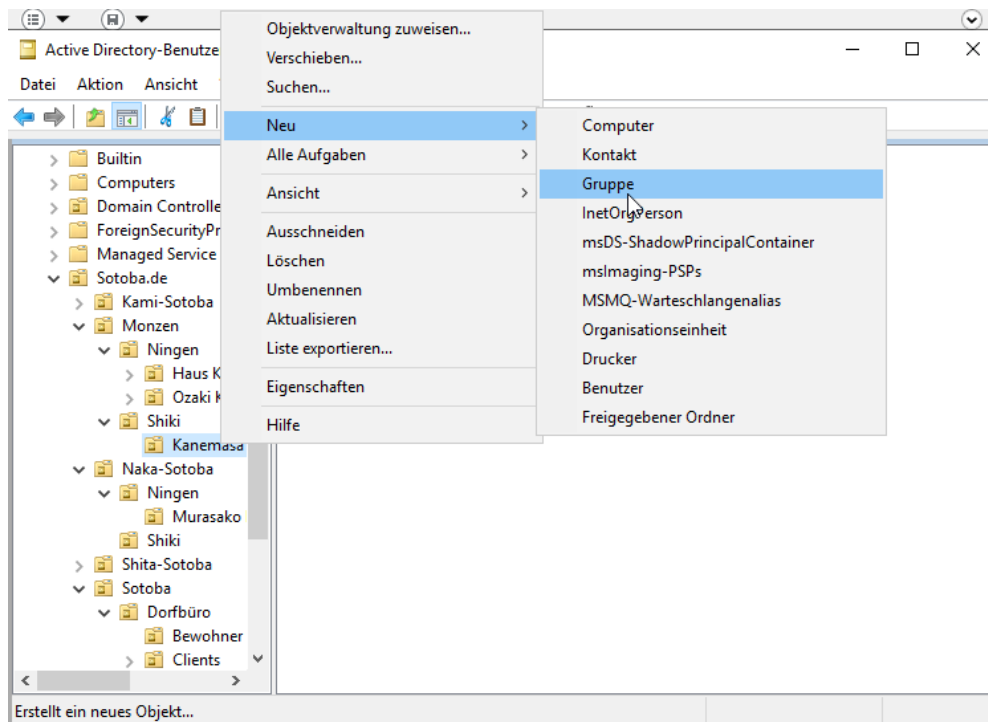
Und der Benutzer wird dem Klick auf fertig stellen erzeugt



Jetzt habe ich aber ein Problem, ich aus Versehen einen Benutzer in der OU-Users erstellt. Da Users ein Legacy-Container ist, der sich nicht mit GPOs versteht. Möchte ich den Account in die Benutzer-OU des Dorfbüros verschieben. Dazu gehe ich in die Gruppe Users und suche den Benutzer.



Als nächstes erstelle ich die entsprechenden Gruppen.



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

### **Benutzer (Accounts)**

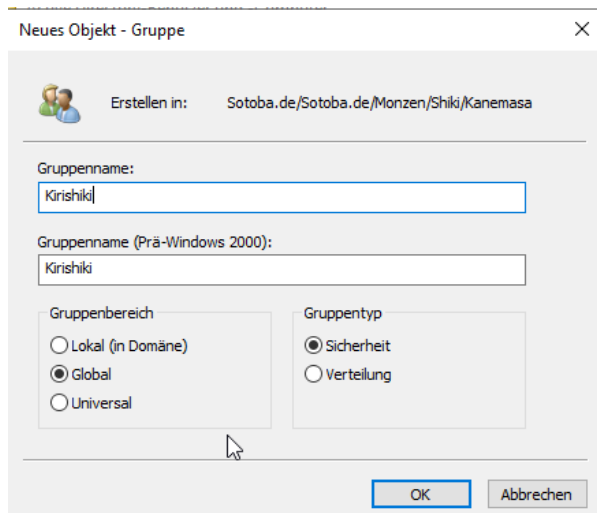
sind Mitglied in →

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

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

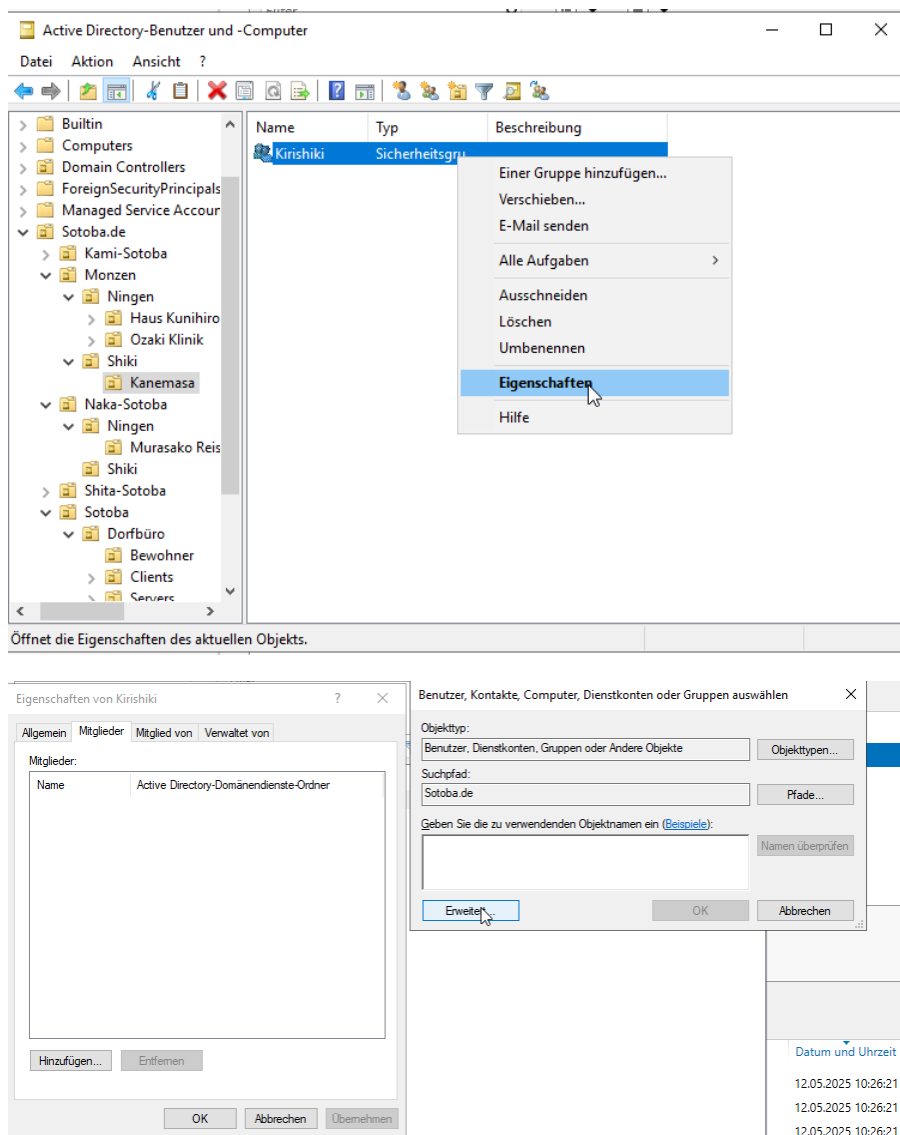
**Rechte (Permissions)** auf z. B. Ordner, Freigaben, Drucker etc.

Also wähle ich eine Globale Gruppe.





Und füge dieser Gruppe nun die Benutzer zu



Leider ist dieses Tool nur Schrott. Denn eine Detaillierte suche Nach beispielsweise Nachnamen geht nicht, also muss ich mit die drei Benutzer selbst herausuchen

Benutzer, Kontakte, Computer, Dienstkonten oder Gruppen auswählen

Objekttyp:  
Benutzer, Dienstkonten, Gruppen oder Andere Objekte

Suchpfad:  
Bewohner

Allgemeine Abfragen

Name:

Beschreibung:

☐ Deaktivierte Konten

☐ Nicht-ablaufende Kennwörter

Tage seit der letzten Anmeldung:

Suchergebnisse:

Name	Name	Ordner
Chizuru Kirishiki	Chizuru Kirishiki	Sotoba.de/Soto...
Megumi Shimizu	Megumi Shimizu	Sotoba.de/Soto...
Mikiyasu Yas...	Mikiyasu Yasumori	Sotoba.de/Soto...
Nao Yasumori	Nao Yasumori	Sotoba.de/Soto...
Seishirou Kiri...	Seishirou Kirishiki	Sotoba.de/Soto...
Shizuka Matsuo	Shizuka Matsuo	Sotoba.de/Soto...
Sunako Kirishiki	Sunako Kirishiki	Sotoba.de/Soto...
Tatsumi Jinrou	Tatsumi Jinrou	Sotoba.de/Soto...
Yoshie Kurah...	Yoshie Kurahashi	Sotoba.de/Soto...

Benutzer, Kontakte, Computer, Dienstkonten oder Gruppen auswählen

Objekttyp:  
Benutzer, Dienstkonten, Gruppen oder Andere Objekte

Suchpfad:  
Bewohner

Geben Sie die zu verwendenden Objektnamen ein (Beispiele):

Chizuru Kirishiki (CKirishiki@Sotoba.de);  
Seishirou Kirishiki (SeKirishiki@Sotoba.de);  
Sunako Kirishiki (SKirishiki@Sotoba.de)

Und die drei sind zuhause

Eigenschaften von Kirishiki

Allgemein Mitglieder Mitglied von Verwaltet von

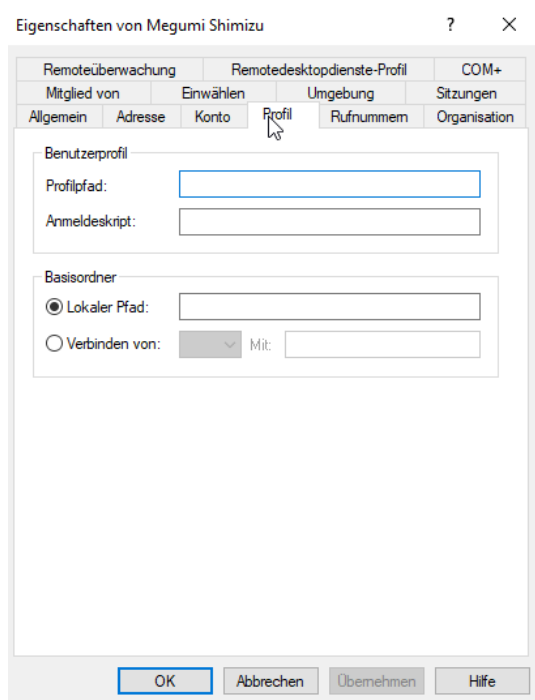
Mitglieder:

Name	Active Directory-Domänenendste-Ordner
Chizuru Kirishiki	Sotoba.de/Sotoba.de/Sotoba/Dorfbüro/Bewohner
Seishirou Kiri...	Sotoba.de/Sotoba.de/Sotoba/Dorfbüro/Bewohner
Sunako Kirishiki	Sotoba.de/Sotoba.de/Sotoba/Dorfbüro/Bewohner



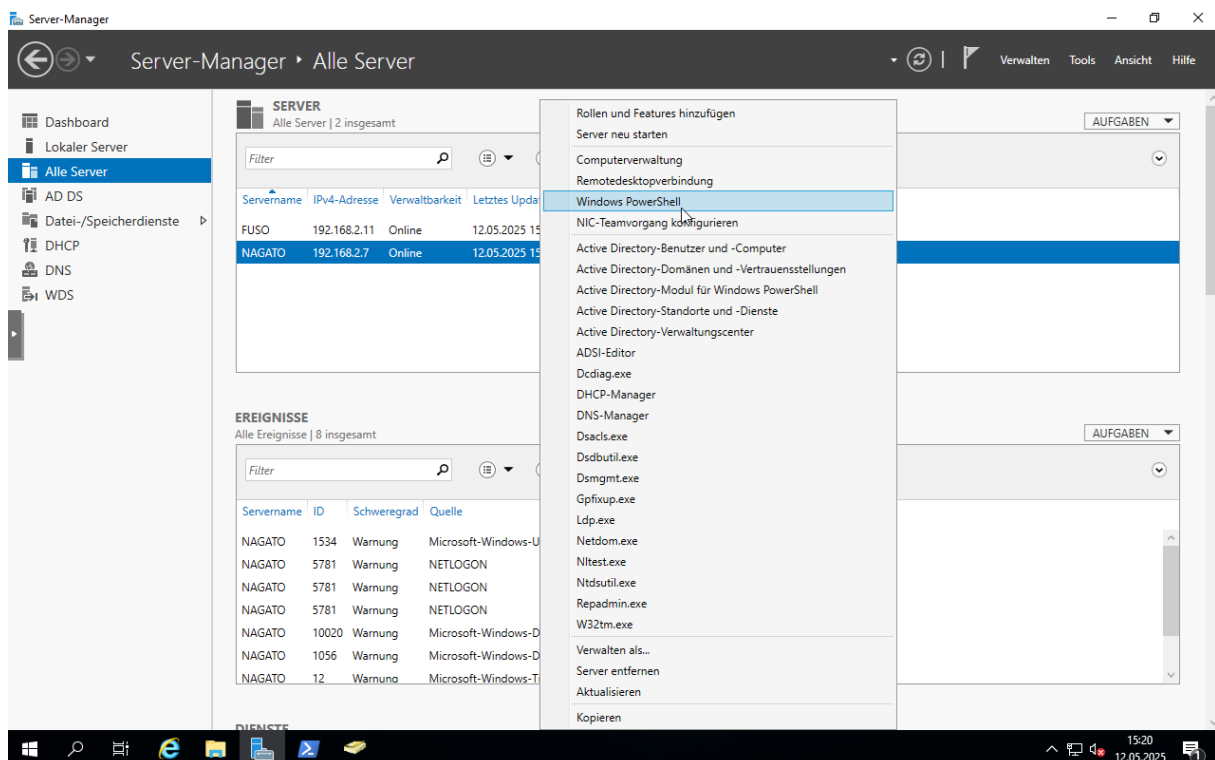


Wenn ich in die Eigenschaften eines Benutzers gehe, finden sich dort viele Informationen, wie zum Beispiel das Profil.



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\SYSVOL\sysvol\Sotoba.de\SCRIPTS Ressource für Anmeldeserver
profile *      h:\profile
SYSVOL *      C:\H\Ad\SYSVOL\sysvol Ressource für Anmeldeserver

[Nagato.Sotoba.de]: PS H:\> █
```

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

Eigenschaften von Megumi Shimizu

Remoteüberwachung RemoteDesktopdienste-Profil COM+

Mitglied von Einwählen Umgebung Sitzungen

Allgemein Adresse Konto Profil Rufnummern Organisation

Benutzerprofil

Profilpfad:

Anmeldeskript:

Basisordner

☐ Lokaler Pfad:

☒ Verbinden von:  Mit:

OK Abbrechen Überehmen Hilfe

Und schaue noch ob der Ordner richtig gesetzt wurde

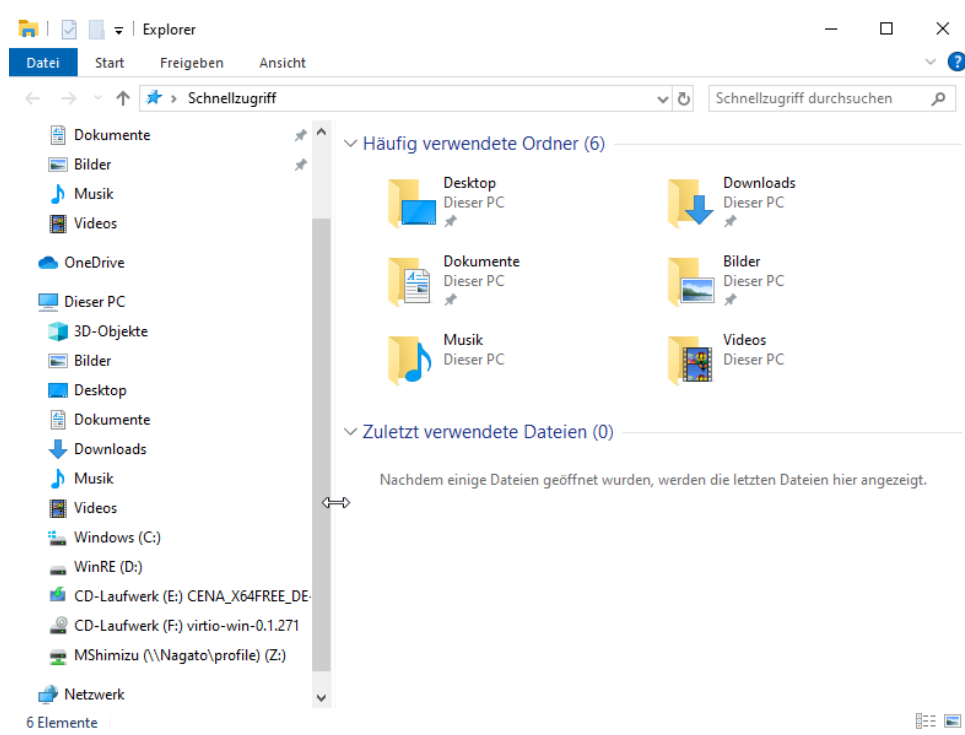
```
[Nagato.Sotoba.de]: PS H:\> cd profile
[Nagato.Sotoba.de]: PS H:\profile> dir

Verzeichnis: H:\profile

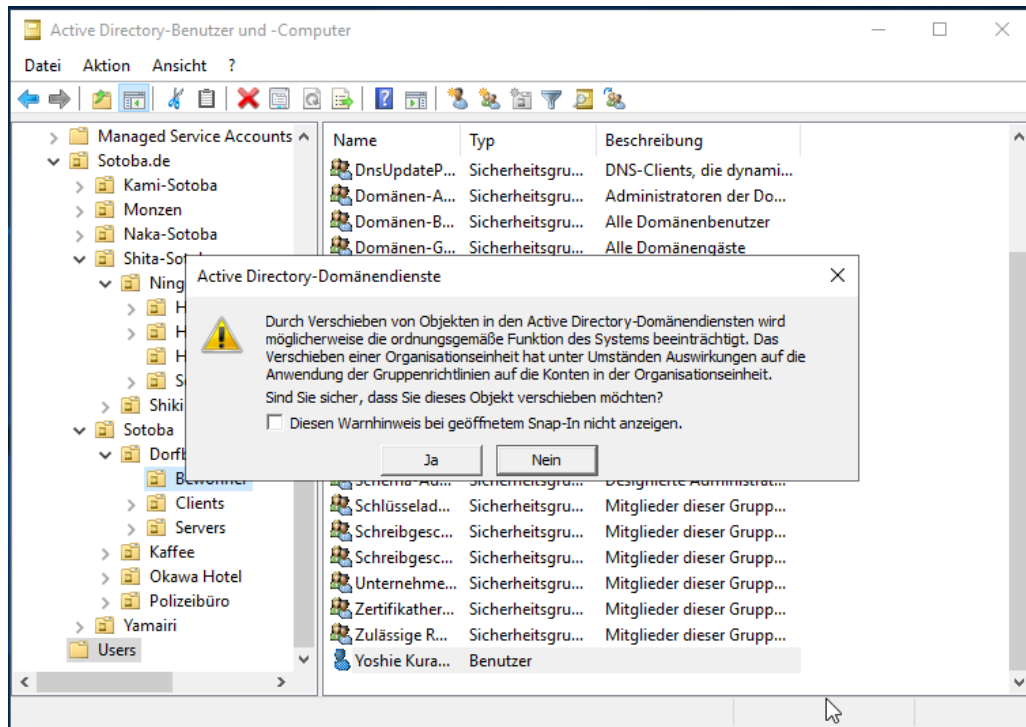

Mode                LastWriteTime         Length Name
----                -
d-----          12.05.2025   15:59             MShimizu

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

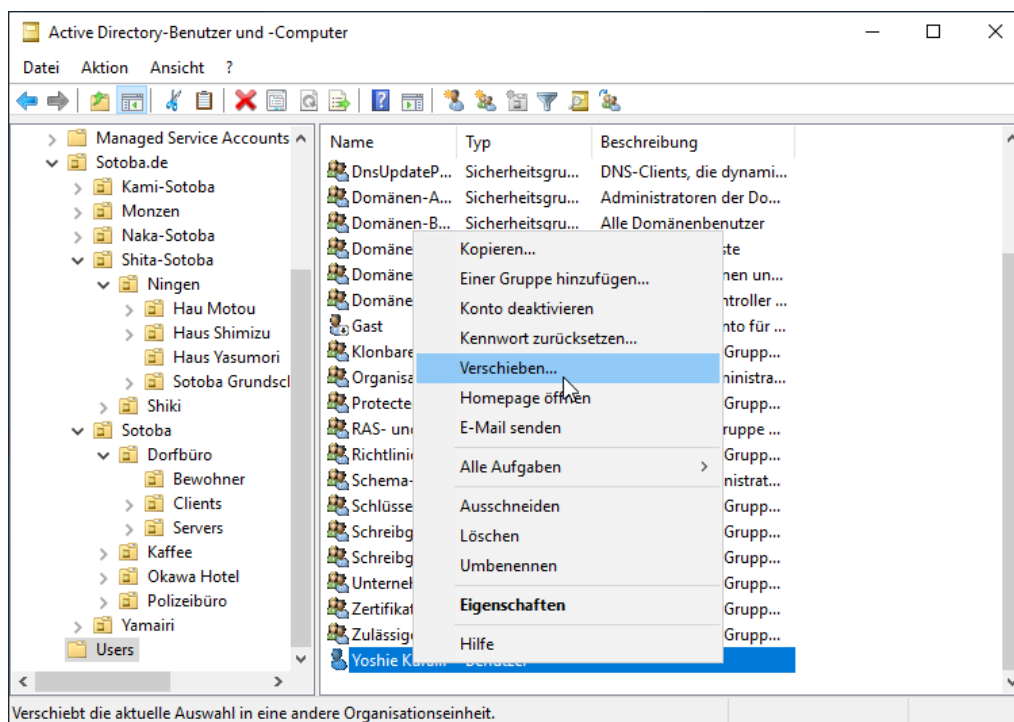
Und der Benutzer hat sein Basisordner als Netzwerklaufrwerk



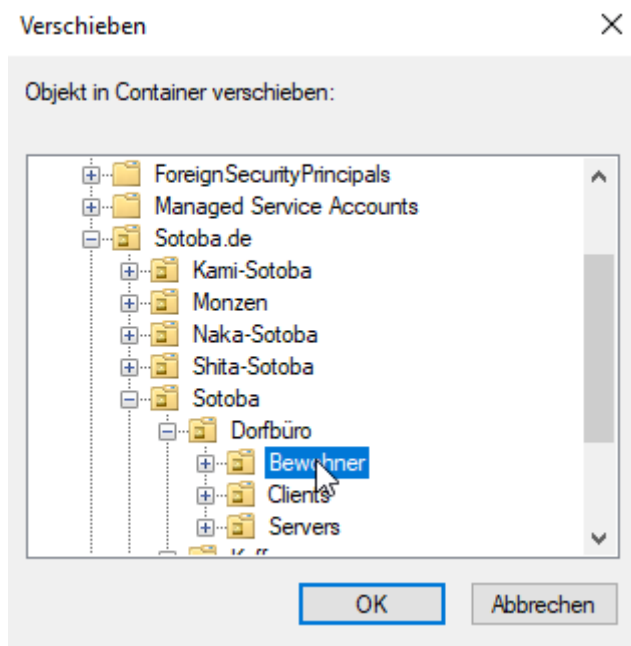
Ich könnte nun mit Drag and Drop den Benutzer verschieben, aber gibt eine Warnung.



Stattdessen verschiebe ich den Benutzer.





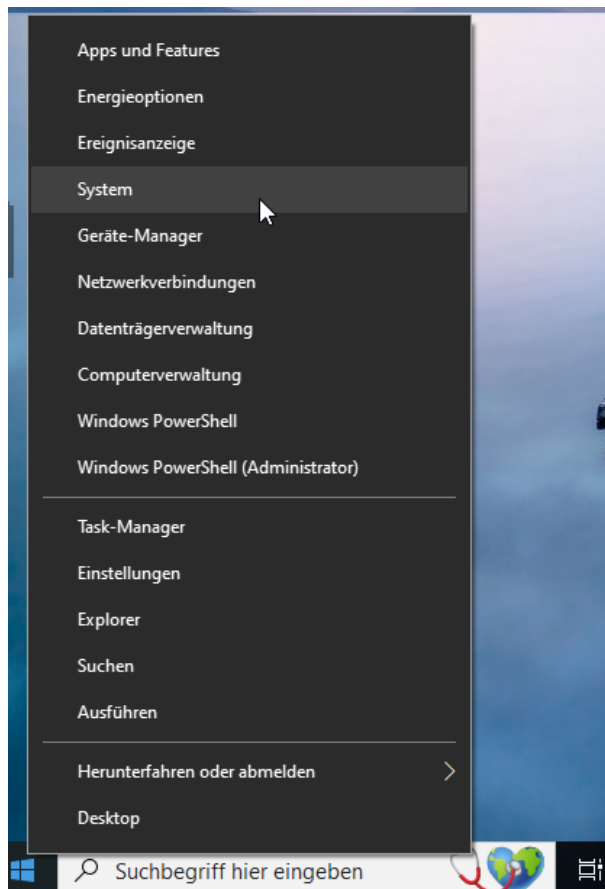


Da ist der Benutzer am richtigen Ort. Das genauso mit Computer

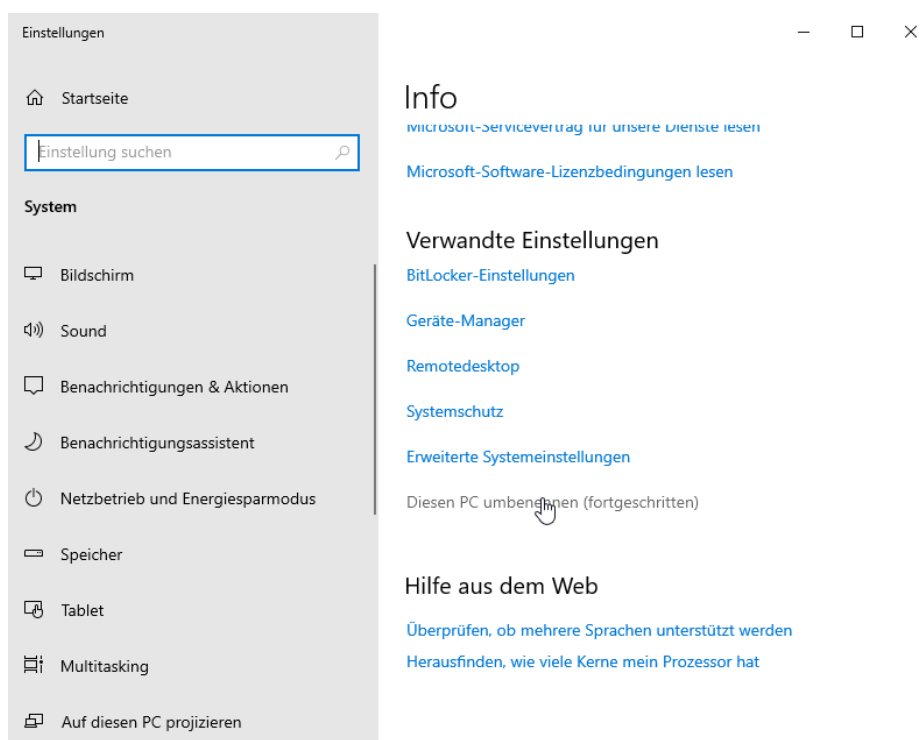


Wie füge ich einen Rechner der Domäne hinzu

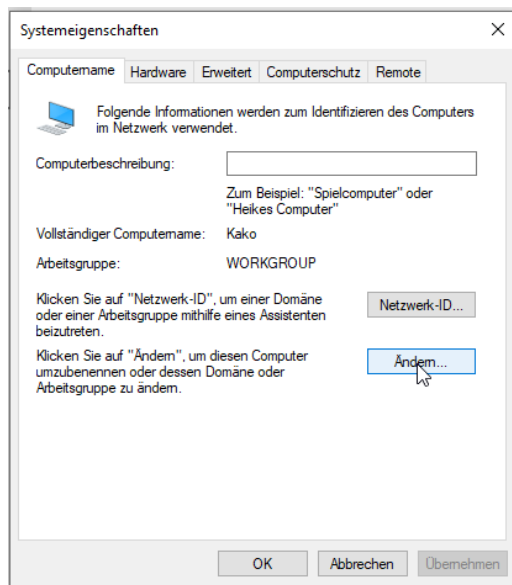
Dazu gehe ich über die startleiste, rechte Maustaste klickend auf System



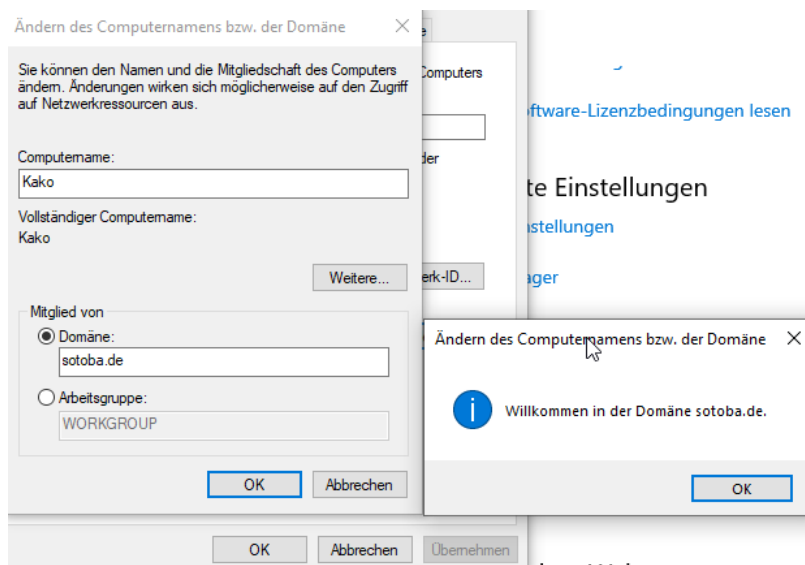
und suche mir dort den Punkt



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



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



OU\_Polizeistation

└─ OU\_Sicherheitslabor

| └─ VM\_Kali

| └─ VM\_Parrot

| └─ VM\_Caine

└─ OU\_Honeypots

| └─ Win\_Honeypot01

| └─ Lin\_SSH\_Honeypot

└─ OU\_Logserver

| └─ Wazuh\_Server

└─ OU\_DigitalSheriffs

└─ Azubi\_Polizei01

└─ svc\_monitoring

└─ GG\_Sicherheitsdienst