

Übungsprotokoll

SYTB – Betriebssysteme

 htlkrems Bautechnik & IT	Übungsdatum: KW 12/2021 – KW 20/2021	Klasse: 3AHIT	Name: Felix Schneider
	Abgabedatum: 19.05.2021	Gruppe: SYTB_2	Note:
Leitung: DI (FH) Alexander MESTL	Mitübende: Clemens Schlipfinger		
Übungsbezeichnung: Windows Server			

Inhaltsverzeichnis:

1	Aufgabenstellung.....	3
2	Abstract (English).....	3
3	Begriffserklärung	3
4	Theoretische Grundlagen	4
4.1	Virtuelle Maschine.....	4
4.2	Domain Controller	4
4.3	Active Directory.....	5
5	Übungsdurchführung	8
5.1	Windows Server	8
5.2	Windows Client	15
5.3	Netzwerkshare	19
5.4	Gruppen.....	23
5.5	Gruppenrichtlinienobjekte	25
5.6	XigmaNAS	37
6	Ergebnisse.....	44
7	Code.....	44
8	Kommentar.....	44

1 Aufgabenstellung

Wie besprochen setzen wir einen Server mit Windows Server 2019 auf (Standard mit Desktopdarstellung) und werden ihn als Domain Controller (DC) mit Active Directory, DNS und DHCP konfigurieren.

Siehe Skriptum in den "Dateien", Kapitel 7, 8 und 9.

2 Abstract (English)

As discussed, we will set up a server with Windows Server 2019 (standard with desktop representation) and will configure it as a Domain Controller (DC) with Active Directory, DNS and DHCP.

See the script in the "Files", chapters 7, 8 and 9.

3 Begriffserklärung

Begriff	Erklärung / Beschreibung
Domain Controller	Server zur zentralen Authentifizierung von Computern und Benutzern in einem Rechnernetz
Domain	Bereich innerhalb des Forest, der Authentifikationen der Benutzer und Computer enthält
Active Directory	Rolle, die Methoden zum Speichern und Abrufen von Daten zur Verfügung stellt
Schema	Hierarchie, Ordnung, Plan
Workstation	der Client in einem Rechnernetzwerk
Partitionen	zusammenhängenden, aufeinanderfolgenden Datenblöcke eines Teils eines Volumes
Organisationseinheit	Unterteilung z.B.: in Abteilungen
Replikation	Vervielfältigung der Erbinformation (jede Domäne bekommt neuestes Schema)
Gesamtstruktur / Forest	Netzwerk an Domänen
Policy	Richtlinie einer Gruppe (z.B.: Hintergrund, Passwort, Installation, ...)

4 Theoretische Grundlagen

Overall picture: <https://serverfault.com/questions/886655/difference-between-domain-domain-controller-and-active-directory>

4.1 Virtuelle Maschine

Die Virtuelle Maschine benötigt diese Spacks/Einstellungen:

- mind. 50GB Festplattenspeicher
- mind. 2GB RAM (4GB ist besser)
- 2 Netzwerkkarten (NAT und internes Netz (Name: intnet_windows))

4.2 Domain Controller

Der Domain Controller ist der Controller aller Domänen. Aus diesem Grund muss er besonders gut gesichert / geschützt sein, weil er die anderen Domänen verwaltet. Als Anmeldeoption steht hier eigentlich nur das Administratorkonto zur Verfügung. Für mehr Sicherheit kann man den Domain Controller auf mehrere Standorte aufteilen, sprich man hat bessere Redundanz. Meistens installiert man dort auch einen DNS-Server und einen DHCP-Server.

4.2.1 RODC

RODC steht für Read-Only-Domain-Controller. Der Unterschied zu einem normalen Domain Controller ist, dass dieser Replikationen nur lesen / bekommen kann, allerdings nichts verändern kann.

4.2.2 Partitionen

4.2.2.1 Schema Partition

Die Schemapartition enthält das Klassen- und Attributenschema. Das bedeutet, dass hier die Hierarchie gespeichert ist, also welche Objekte im Forest existieren können. Jeder Domain Controller in diesem Forest hat ein Replikat des gleichen Schemas.

4.2.2.2 Configuration Partition

Die Konfigurationspartition enthält die Einstellungen bzgl. des Domain Controllers. Hierunter fallen dann solche Einstellungen wie Policies, DNS-Server oder DHCP-Server. Jeder Domain Controller im Forest verfügt wieder über ein Replikat derselben Konfigurationspartition.

4.2.2.3 Domain Partition

Die Domainpartition enthält die mit der lokalen Domäne verknüpften Verzeichnisobjekte, wie Benutzer und Computer. Eine Domäne kann mehrere Domänencontroller haben und eine Gesamtstruktur kann mehrere Domänen haben. Jeder Domänencontroller speichert ein vollständiges Replikat der Domänenpartition für seine lokale Domäne, speichert aber keine Replikate der Domänenpartitionen für andere Domänen.

4.3 Active Directory

4.3.1 Grundlagen

Active Directory Domain Services (AD DS) stellen Methoden zur Verfügung, die das Speichern von Daten innerhalb des Netzwerkes und das Zur-Verfügung-Stellen der Daten für Benutzer und Administratoren ermöglicht.

<https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/deploy/ad-ds-deployment>

4.3.2 Services von AD DS

AD DS enthält mehrere Services (eigentlich nicht notwendig zu wissen...):

- **Domänendienste:** Speichern Daten und verwalten die Kommunikation zwischen den Benutzern und dem Domänen-Controller (DC). Dies ist die primäre Funktionalität der AD DS.
- **Zertifizierungsdienste:** Ermöglichen Ihrem DC die Bereitstellung digitaler Zertifikate, Signaturen und Public-Key-Kryptographie.
- **Lightweight Directory Services:** Unterstützen das LDAP für plattformübergreifende Domänendienste, wie alle Linux-Computer in Ihrem Netzwerk.
- **Directory Federation Services:** Ermöglichen die SSO-Authentifizierung für mehrere Anwendungen in derselben Sitzung, so dass Benutzer nicht mehrfach dieselben Anmeldeinformationen angeben müssen.
- **Berechtigungsverwaltung:** Steuert Zugriffsberechtigungen und Datenzugriffsrichtlinien. So bestimmt beispielsweise die Berechtigungsverwaltung, ob Sie auf einen Ordner zugreifen oder eine E-Mail senden dürfen.

4.3.3 Begriffserklärung

Hier sind einige wichtige Begriffe im Zusammenhang mit Active Directory Domain Services:

- **Schema:** Der Satz benutzerdefinierter Regeln für Objekte und Attribute in den AD DS.
- **Globaler Katalog:** Der Container aller Objekte in den AD DS. Wenn Sie den Namen eines Benutzers finden müssen, finden Sie ihn im Globalen Katalog.
- **Such- und Indexmechanismus:** Dieses System ermöglicht es den Benutzern, sich gegenseitig im AD zu finden. Ein gutes Beispiel ist, wenn Ihnen während des Eingabens eines Namens in Ihrem E-Mail-Programm vom E-Mail-Programm mögliche Übereinstimmungen angezeigt werden.
- **Replikationsdienst:** Der Replikationsdienst stellt sicher, dass jeder DC im Netzwerk über denselben Globalen Katalog und dasselbe Schema verfügt.
- **Sites:** Sites sind Darstellungen der Netzwerktopologie, die den AD DS zeigen, welche Objekte zusammengehören, um die Replikation und Indexierung zu optimieren.
- **Lightweight Directory Access Protocol:** LDAP ist ein Protokoll, über die das AD mit anderen LDAP-fähigen Verzeichnisdiensten plattformübergreifend kommunizieren kann.

<https://www.varonis.com/de/blog/active-directory-domain-services-ad-ds#:~:text=Als%20Active%20Directory%20Domain%20Services,in%20logischen%20Hierarchien%20organisieren%20k%C3%B6nnen.>

4.3.4 Vorteile

- Sie können die Organisation Ihrer Daten an die Bedürfnisse Ihres Unternehmens anpassen.
- Sie können im Bedarfsfall die AD DS von jedem Computer im Netzwerk aus verwalten.
- Die AD DS bietet eingebaute Replikation und Redundanz: Wenn ein Domänen-Controller (DC) ausfällt, übernimmt ein anderer DC dessen Aufgaben.
- Der gesamte Zugriff auf Netzwerkressourcen erfolgt über die AD DS, in denen die Netzwerkzugriffsberechtigungen zentral verwaltet werden.

4.3.5 Replikationen

Dank Replikationen bleiben Änderungen im Forest immer zwischen allen Domänen und dem Domain Controller synchronisiert.

4.3.6 OU = Organizational Unit

Active Directory Organisationseinheiten sind spezielle Container um Benutzer, Gruppen, Computer und andere OUs aufnehmen zu können. OUs werden von Administratoren erstellt, um Active Directory Objekte logisch zu ordnen (z.B. nach Abteilung) und um Gruppenrichtlinienobjekte anzuwenden. Container dagegen sind vordefinierte, unveränderliche Active Directory Objekte.

Jeder OU kann man verschiedene Berechtigungen (policies) geben. OUs können auch verschachtelt sein, sodass OUs in OUs in OUs in einer OU sind...

4.3.7 Gruppenrichtlinienobjekte = Policy

Mithilfe von Policies kann man bestimmten OUs Richtlinien geben, an die sie sich halten müssen. Zum Beispiel kann man festlegen, dass das Hintergrundbild auf jeder **Workstation** (so nennt man die Clients auch) das Firmenlogo ist oder das Passwörter gewisse Zeichen enthalten müssen, damit sie sicher genug sind. Außerdem kann man Software automatisch installieren, mithilfe von Policies.

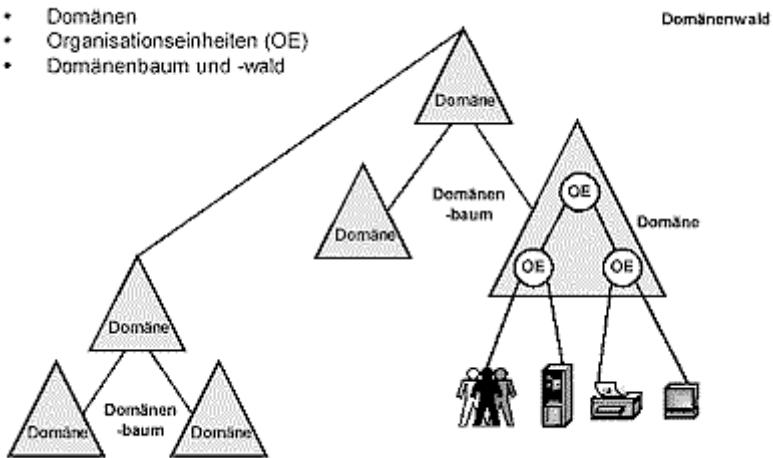
Einige Anwendungsbeispiele, welche wir mithilfe von Gruppenrichtlinienobjekten umgesetzt haben sind:

- Laufwerke verbinden, sodass Benutzer Zugriff auf Ordner im Active Directory haben.
- die Firewall jeder Workstation deaktivieren

4.3.8 Forest

Ein Active Directory Forest (AD Forest) ist ein Container auf der höchsten Organisationsebene einer Active Directory-Konfiguration, in der Domänen, Benutzer, Computer und Gruppen-Richtlinien enthalten sind.

- Domänen
- Organisationseinheiten (OE)
- Domänenbaum und -wald



- Domänenwald = Domänengesamtstruktur = Gesamtstruktur = Forest
- Domänenbaum = Domain Tree
- Domäne = Domain
- Organisationseinheiten = OE = Organisation Units = OU

<https://www.it-zeugs.de/was-ist-active-directory.html>

5 Übungsdurchführung

5.1 Windows Server

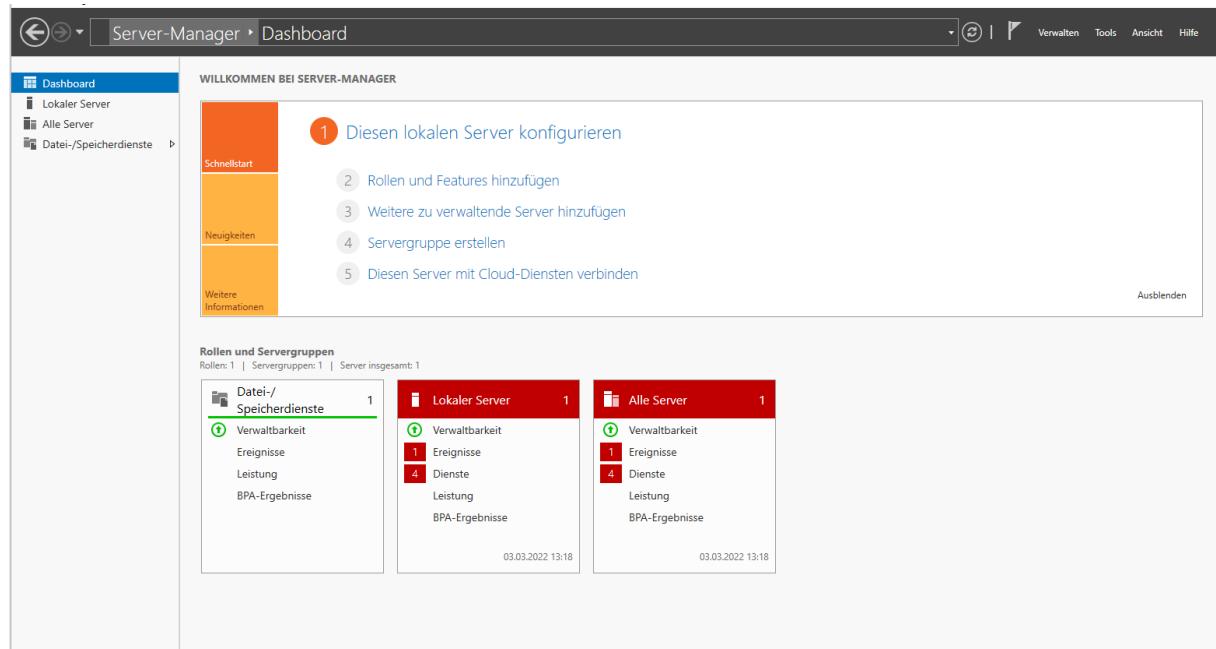
5.1.1 Installation Windows Server

Als erstes neue VM erstellen (RAM und Speicher beachten). Anschließend 2 Netzwerkkarten hinzufügen. Starten → ISO auswählen → Installationsschritte befolgen.

Folgende Möglichkeiten stehen Ihnen zur Auswahl:

- Windows Betriebssystem: Windows Server 2019 Standard (Desktopdarstellung)
- Benutzerdefiniert: nur Windows installieren
- sicheres Passwort vergeben (aufschreiben!): Admin123

Zuletzt sollten Sie dieses Dashboard sehen:



5.1.1.1 Gasterweiterungen Windows Server

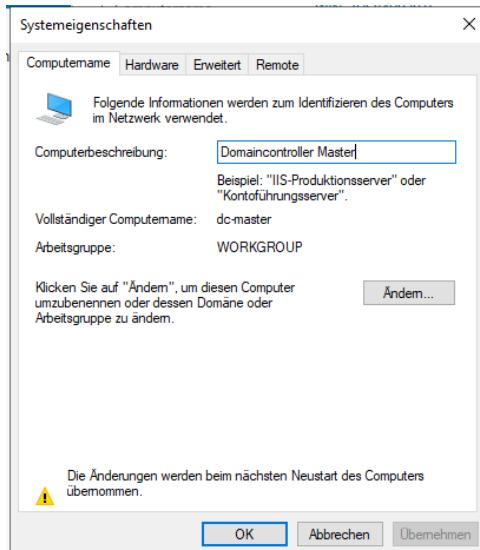
Gehen Sie in der Menuleiste des Windows Servers auf Geräte. Dort finden Sie als letzten Punkt Gasterweiterungen hinzufügen. Nachdem Sie das geklickt haben, gehen Sie in den Explorer und führen Sie die exe-Datei aus. Folgen Sie den Anweisungen und starten Sie anschließend die VM neu.

5.1.2 Windows Server konfigurieren

5.1.2.1 Server umbennen

Benennen Sie Ihre Virtuelle Windows Server Maschine als erstes um (zum Beispiel: dc-master).

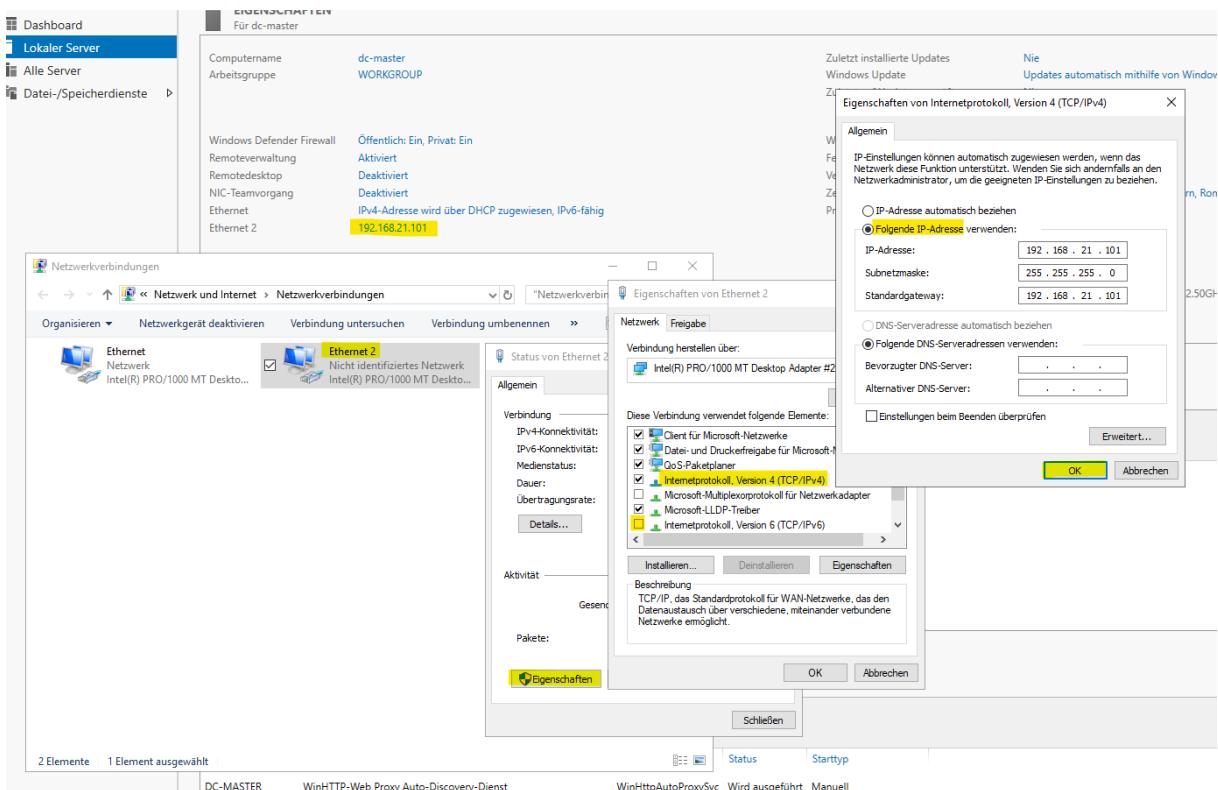
Durch einen Klick auf den „Computernamen“ unter „Lokaler Server“ kommen Sie direkt zu den Einstellungen:



Starten Sie den Server neu.

5.1.2.2 Netzwerkkarten konfigurieren

Der zweiten Netzwerkkarte (intnet_windows) müssen Sie noch eine IP-Adresse zuordnen. Befolgen Sie dafür folgend Schritte (gelb markiert):

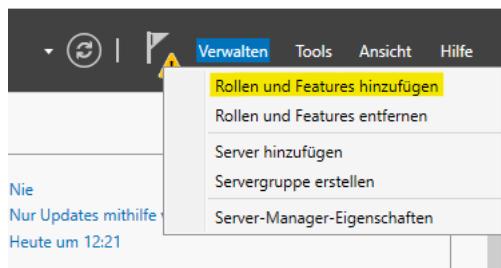


Wie Sie sehen haben wir eine IPv4-Adresse vergeben (192.168.21.101/24) und IPv6 deaktiviert.

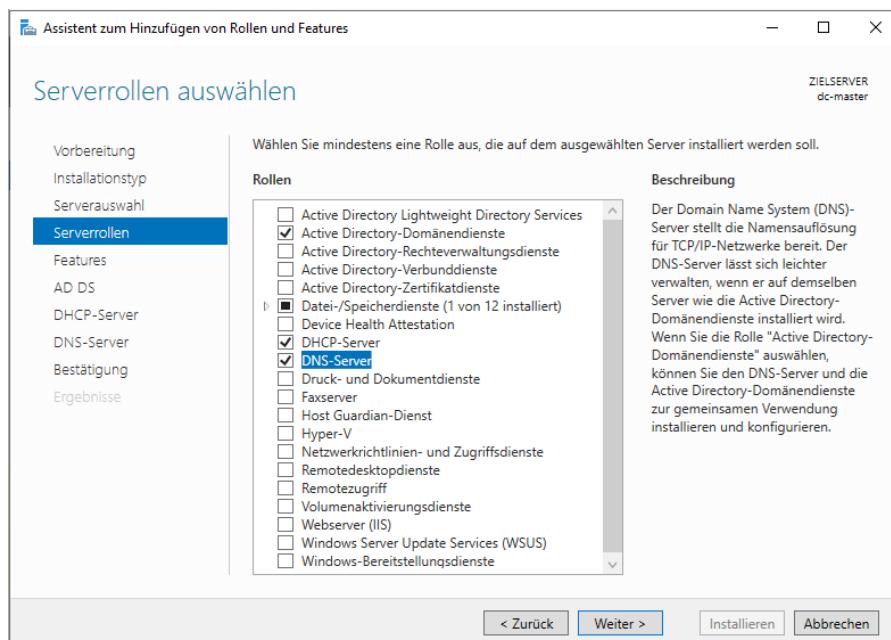
5.1.2.3 Serverrollen & Features installieren

Features können beim Windows Server folgendermaßen hinzugefügt werden:

1. gehen Sie beim Server-Manager auf Verwalten → Rollen und Features hinzufügen



2. Bis zu diesem Fenster können Sie immer auf *Weiter klicken*. Bei diesem Fenster fügen Sie dann die Rollen hinzu, die Sie verwenden möchten (wir fügen Active Directory, DHCP und DNS hinzu):



3. Anschließend können Sie auch wieder immer *Weiter klicken* (wenn Sie wollen können Sie die ganzen Erklärungen auch durchlesen...), bis Sie dann auch *Installieren* klicken.

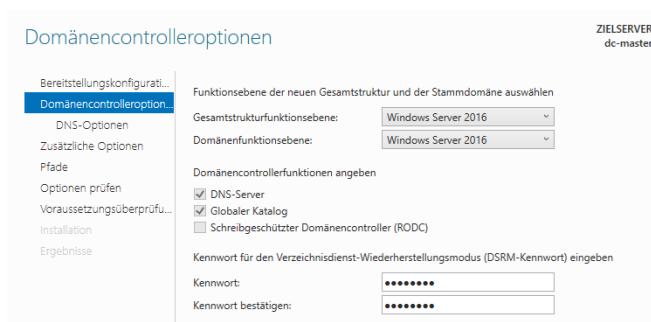
5.1.2.4 Active Directory konfigurieren

Der Server-Manager schlägt uns gleich nach dieser Installation vor, den Server zu einem Domaincontroller heraufzustufen. Das ist genau das, was wir machen wollen.

Geben Sie einen Namen für die Stammdomäne ein und klicken Sie auf Weiter.



Wählen Sie bei einer neuen Installation die neueste Serverversion aus. Weil die Struktur von DNS im Domaincontroller weitergeführt wird, bestätigen wir dieses Häckchen bei DNS-Server. Geben Sie auch ein sicheres Passwort mit Sonderzeichen, Zahlen, Klein- und Großbuchstaben ein: &thF4h3d.

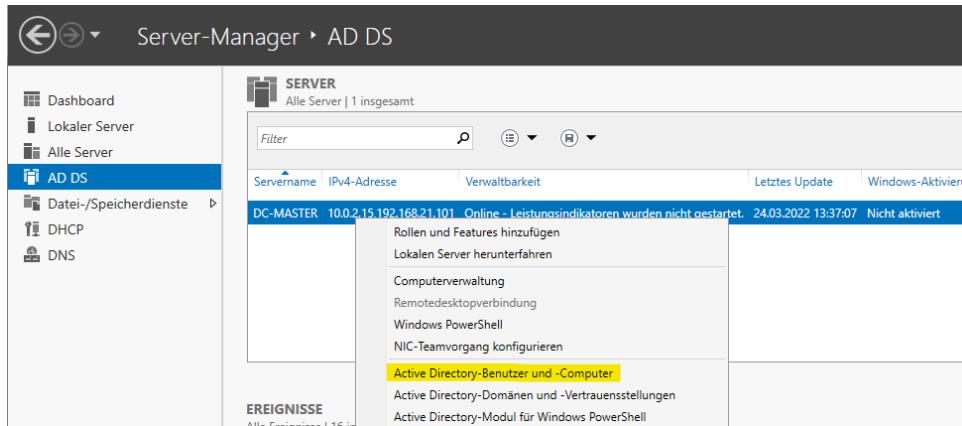


Klicken Sie immer auf Weiter, außer bei dieser Seite, wo Sie zuerst noch das Skript anzeigen und speichern sollten:



Schließen Sie schlussendlich die Installation ab und warten Sie, bis der Server neu gestartet hat (sollte automatisch passieren).

Um anschließend in die Einstellungen des Active Directories zu kommen, klicken Sie auf AD DS, Rechtsklick auf das Element in der auftauchenden Liste und Active Directory-Benutzer und -Computer.



Es sollte sich ein weiteres Fenster öffnen, in dem Sie nun die OUs sehen können, und das Active Directory verwalten können. Standardmäßig sind bereits folgende OUs vorhanden:

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- Users

Damit die Unordnung nicht so groß, wie in folgendem Bild, ist, können Sie nun weiter OUs erstellen, die Ihr Unternehmen in Abteilungen, Länder oder was auch immer aufteilen.

Name	Typ	Beschreibung
Abgelehnte RODC-Kennwortreplikationsgruppe	Sicherheitsgruppe	Mitglieder dieser Gruppe
Administrator	Benutzer	Vordefiniertes Konto für
DHCP-Administratoren	Sicherheitsgruppe	Mitglieder, die Administ...
DHCP-Benutzer	Sicherheitsgruppe	Mitglieder, die nur über ...
DnsAdmins	Sicherheitsgruppe	Gruppe "DNS-Administrat...
DnsUpdateProxy	Sicherheitsgruppe	DNS-Clients, die dynami...
Domänen-Admins	Sicherheitsgruppe	Administratoren der Do...
Domänen-Benutzer	Sicherheitsgruppe	Alle Domänenbenutzer
Domänen-Gäste	Sicherheitsgruppe	Alle Domänengäste
Domänencomputer	Sicherheitsgruppe	Alle Arbeitsstationen un...
Domänencontroller	Sicherheitsgruppe	Alle Domänencontroller ...
Gast	Benutzer	Vordefiniertes Konto für
Klonbare Domänencontroller	Sicherheitsgruppe	Mitglieder dieser Grupp...
Organisations-Admins	Sicherheitsgruppe	Angegebene Administrat...
Protected Users	Sicherheitsgruppe	Mitglieder dieser Grupp...
RAS- und IAS-Server	Sicherheitsgruppe	Server in dieser Gruppe ...
Richtlinien-Erststeller-Besitzer	Sicherheitsgruppe	Mitglieder dieser Grupp...
Schema-Admins	Sicherheitsgruppe	Designierte Administrat...
Schlüsseladministratoren	Sicherheitsgruppe	Mitglieder dieser Grupp...
Schreibgeschützte Domänencontroller	Sicherheitsgruppe	Mitglieder dieser Grupp...
Schreibgeschützte Domänencontroller der Organisation	Sicherheitsgruppe	Mitglieder dieser Grupp...
Unternehmensschlüsseladministratoren	Sicherheitsgruppe	Mitglieder dieser Grupp...
Zertifikatherausgeber	Sicherheitsgruppe	Mitglieder dieser Grupp...
Zulässige RODC-Kennwortreplikationsgruppe	Sicherheitsgruppe	Mitglieder dieser Grupp...

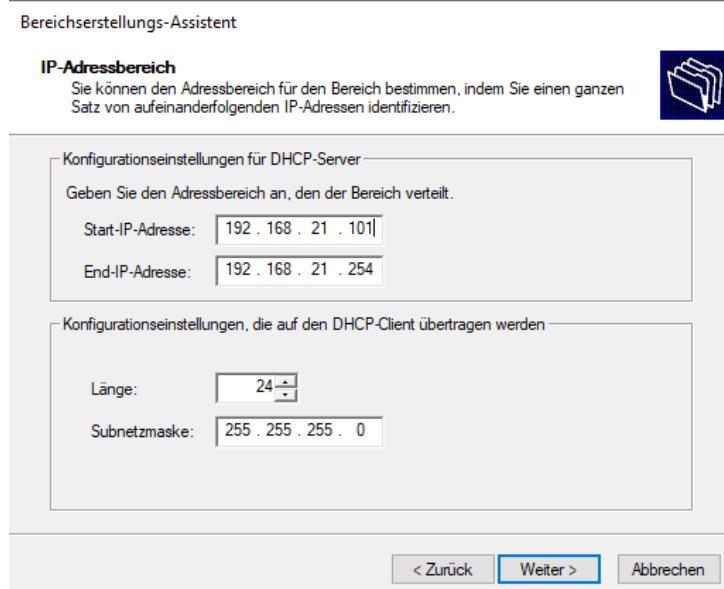
5.1.2.5 DHCP-Server konfigurieren

Um den DHCP-Server zu konfigurieren, gehen Sie im Server-Manager auf DHCP, machen Sie einen Rechtsklick auf das erste Element und klicken Sie auf *DHCP-Manager*.

Erstellen Sie einen neuen Adressbereich, indem Sie bei IPv4 auf *neuer Bereich* klicken.

Geben Sie dem DHCP-Bereich einen Namen und beschreiben Sie diesen in kurzen Worten.

Stellen Sie den IP-Adressbereich so ein, dass er sich nicht mit anderen Servern (beispielsweise unser Debian-Server; folgende Protokolle in der Datenbank verfügbar 😊: [SYTB Protokoll 1 DebianServer](#), [SYTB Protokoll 2 DebianServer](#), [SYTB Protokoll 3 DHCP und DNS](#), [SYTB Protokoll 4 DDNS](#), [SYTB Protokoll 5 Zonentransfer](#), [SYTB Protokoll 6 ApacheWebserver](#), [SYTB Protokoll 7 PXE-Boot](#)) überschneidet. Wenn der Server-Manager es nicht automatisch richtig machen sollte, müssen Sie die Subnetzmaske auch noch richtig konfigurieren.



Alle IP-Adressen, die später oder jetzt noch Server werden sollen, sollten nicht mit DHCP vergeben werden. Aus diesem Grund müssen Sie diese als Ausschüsse markieren. Normalerweise nimmt man ca. 10 freie IP-Adressen, damit auch in Zukunft noch Platz für mehrere Server da ist.

Wichtig ist hierbei anzumerken, dass es nicht möglich ist, die IP-Adressen, die Server representieren, einfach aus dem Adressbereich auszuschließen!

Stellen Sie die Leasedauer auf eine sinnvolle Zeit ein (bei McDonald's eher nur 5min, weil die Leute gleich wieder gehen; bei einem großen Unternehmen eher 12h, weil viele Stand-PCs verwendet werden, die eher nicht in ein anderes Netzwerk wechseln wollen und auch immer kommunizieren können wollen)! Wir haben 10min eingestellt.

Bestätigen Sie die Konfigurationsabfrage mit Weiter und geben Sie als Default-Gateway / Router den Server selbst an. Alle weiteren Schritte können Sie immer mit Weiter bestätigen.

Schließen Sie die Konfiguration ab und starten Sie den Server neu. Anschließend sollte es funktionieren. Falls es immer noch nicht funktioniert, können Sie noch probieren den DHCP-Server zu Autorisieren.

5.1.2.6 DNS-Server konfigurieren

Die Forward-Lookup-Zone des DNS-Servers wird durch das Aufsetzen vom Active Directory-Server bereits automatisch konfiguriert. Um auch die Reverse-Lookup-Zone zu erstellen, starten Sie zuerst den DNS-Manager.

Erstellen Sie eine neue Reverse-Lookup-Zone, indem Sie auf *neue Zone* klicken.

Der Zonentyp der ersten Zone ist logischerweise primär.

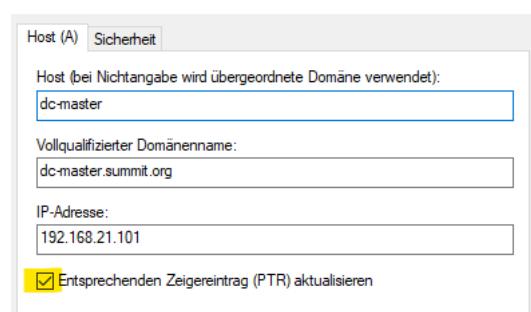
Die Zonenreplikation soll auf allen Domänencontrollern in dieser Domäne ausgeführt werden.

Wählen Sie IPv4 oder IPv6 (IPv5 steht leider nicht zur Auswahl, weil es das nicht gibt... 😊).

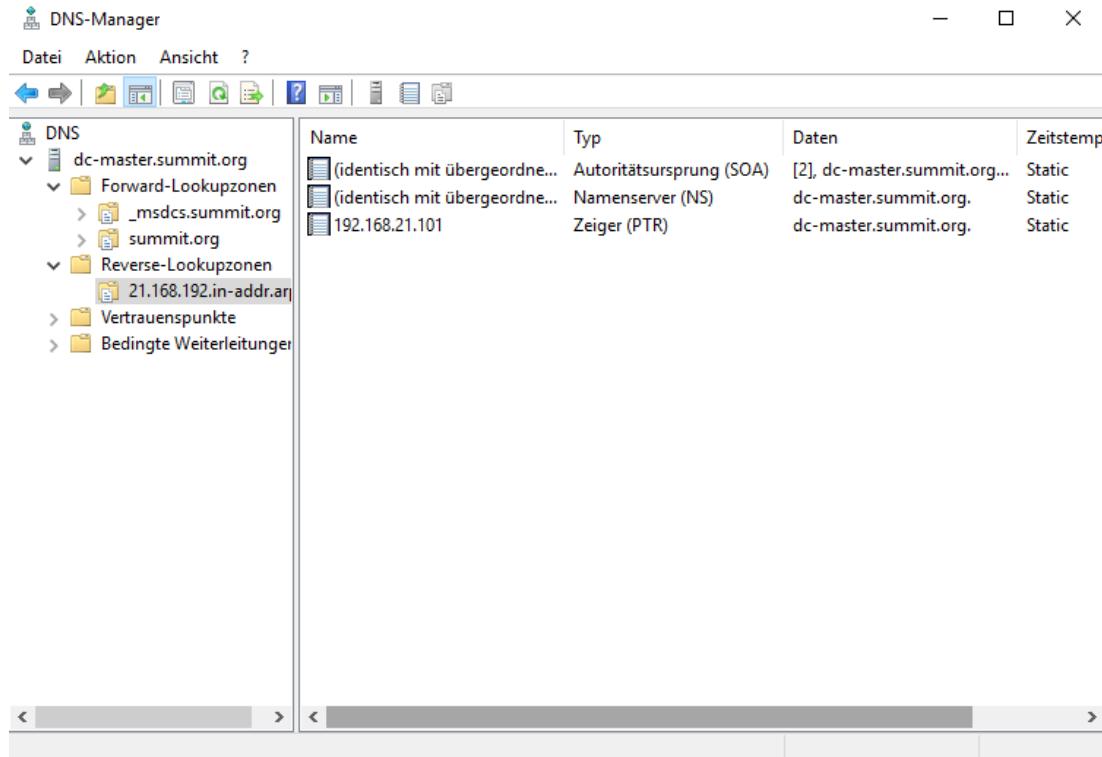
Geben Sie die Reverse-Lookup-Namen ein (21.168.192.in-addr-arpa).

Am geschicktesten ist das Zulassen aller sicheren dynamischen Updates.

Wenn Sie die Erstellung der Zone fertig haben, müssen Sie bei den Forward-Lookupzonen die Eigenschaften des Servers mit der richtigen Adresse (192.168.21.101) verstetllen:



Anschließend sollten Sie bei den Reverse-Lookupzonen den PTR-Eintrag sehen:



The screenshot shows the Windows Server DNS Manager window. On the left, a tree view displays the DNS structure under 'dc-master.summit.org'. Under 'Forward-Lookupzonen', there are entries for '_msdcs.summit.org' and 'summit.org'. Under 'Reverse-Lookupzonen', there is an entry for '21.168.192.in-addr.arpa'. On the right, a table lists DNS records:

Name	Typ	Daten	Zeitstemp
(identisch mit übergeordneter)	Autoritätsursprung (SOA)	[2], dc-master.summit.org...	Static
(identisch mit übergeordneter)	Namenserver (NS)	dc-master.summit.org.	Static
192.168.21.101	Zeiger (PTR)	dc-master.summit.org.	Static

5.2 Windows Client

5.2.1 Installation Windows Client

Als erstes neue VM erstellen (RAM und Speicher beachten). Anschließend eine Netzwerkkarte hinzufügen. Starten → ISO auswählen → Installationsschritte befolgen.

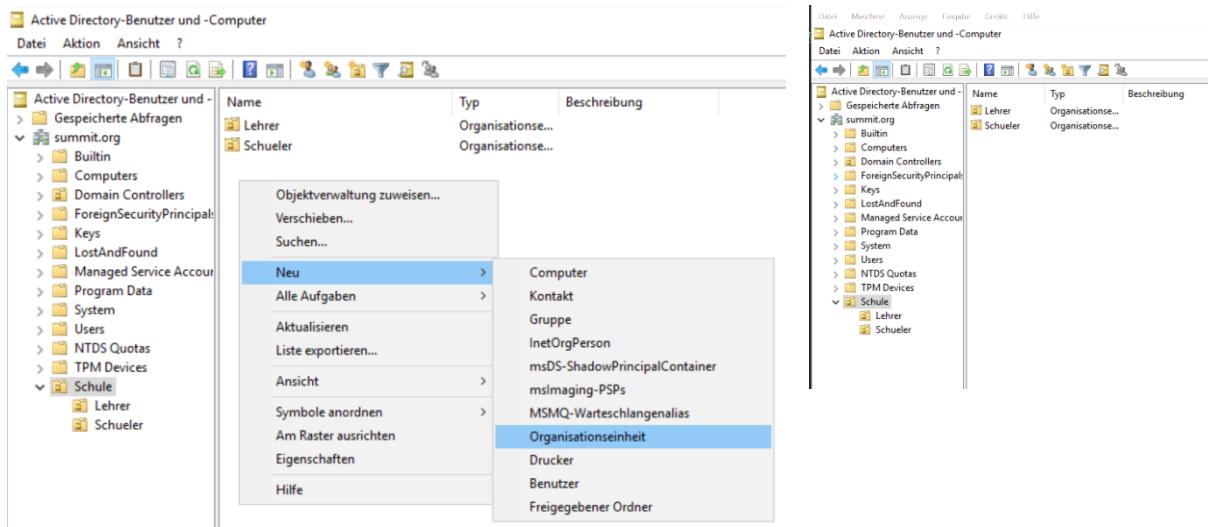
Folgende Möglichkeiten stehen Ihnen zur Auswahl:

- Windows Betriebssystem: Windows 10 Pro
- Tastaturlayout: Deutsch
- Benutzer: Felix; Passwort: xilef

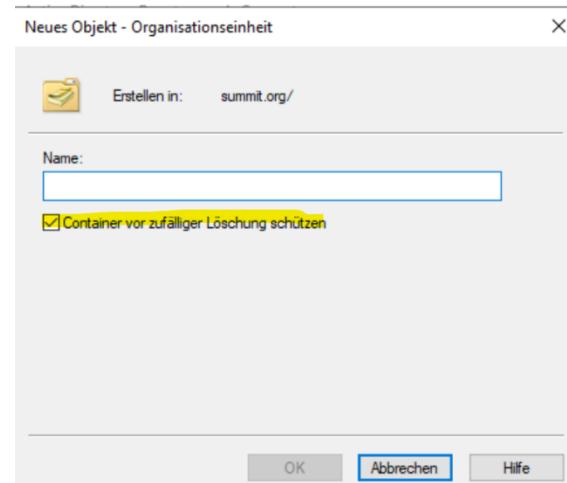
5.2.2 Benutzergruppen hinzufügen

5.2.2.1 OUs hinzufügen

Fügen Sie eine OU hinzu (z.B.: Schule) und wenn Sie wollen können Sie noch weitere OUs in dieser OU erstellen (z.B.: Schueler, Lehrer).



Wenn Sie dieses Häckchen anmachen, können Sie wegen Berechtigungen die OU nicht mehr löschen. Falls Sie die OU trotzdem löschen möchten, müssen Sie die erweiterten Features aktivieren und mittels Rechtsklick auf die OU, Eigenschaften, Objekt. Dort können Sie dieses Häckchen wieder deaktivieren.



5.2.2.2 Benutzer anlegen

Legen Sie ein paar Benutzer im Lehrer-OU und im Schueler-OU an.

Name	Typ	Beschreibung
Felix Schneider	Benutzer	
Clemens Schlipfinger	Benutzer	
Alexander Schindl	Benutzer	
Lukas Flickentanz	Benutzer	
Matthias Swatek	Benutzer	
Lorenz Toifl	Benutzer	

Neues Objekt - Benutzer

Erstellen in: summit.org/Schule/Schueler

Vorname: Felix Initialen:
Nachname: Schneider
Vollständiger Name: Felix Schneider

Benutzeranmeldename:
Benutzeranmeldename (Prä-Windows 2000):
SUMMIT\felix

< Zurück Weiter > Abbrechen

Name	Typ	Beschreibung
Paul Mag. Nagl	Benutzer	
Alexander Ing. Mestl	Benutzer	
Herwig Ing. Macho	Benutzer	

Active Directory-Benutzer und -Computer

Neues Objekt - Benutzer

Erstellen in: summit.org/Schule/Lehrer

Vorname: Paul Mag. Nagl Initialen:
Nachname: Nagl
Vollständiger Name: Paul Mag. Nagl

Benutzeranmeldename:
Benutzeranmeldename (Prä-Windows 2000):
SUMMIT\paulmag.nagl

< Zurück Weiter > Abbrechen

5.2.3 Windows Client Netzwerkkarte

Stellen Sie die Netzwerkkarte des Windows Clients auf interes Netzwerk um, sodass sich der Windows Server im gleichen Netzwerk wie der Windows Client befindet.

Erneuern Sie die IP-Adresse des Clients mit # ipconfig /renew und prüfen Sie, ob der DNS-Server die Adresse des Windows Servers ist.

```

C:\> ipconfig /renew
C:\> nslookup
Standardserver: dc-master.summit.org
Address: 192.168.21.101

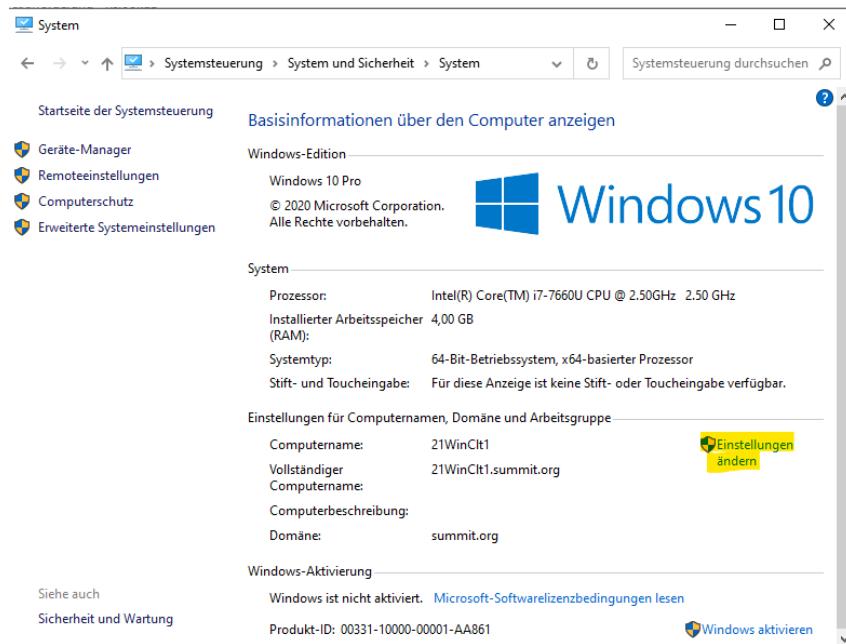
> dc-master.summit.org
Server: dc-master.summit.org
Address: 192.168.21.101

Name: dc-master.summit.org
Addresses: 192.168.21.101
          10.0.2.15

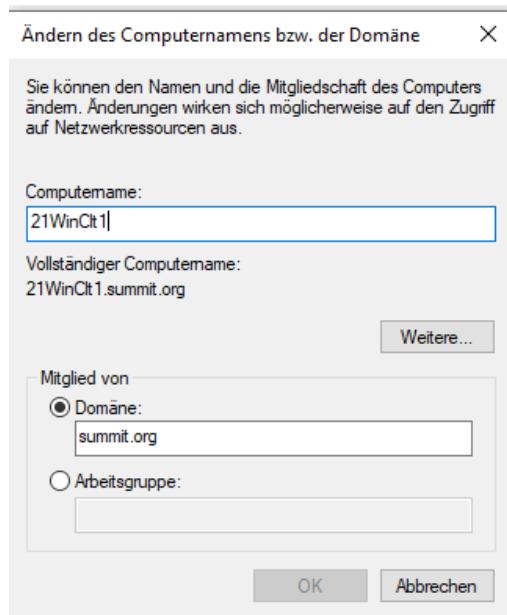
```

5.2.4 Client zu Domain hinzufügen

Um den Client in die Domain hinzuzufügen, gehen Sie in die Systemsteuerungen des Windows Clients, System und Sicherheit, System und klicken Sie auf das gelb markierte Feld:



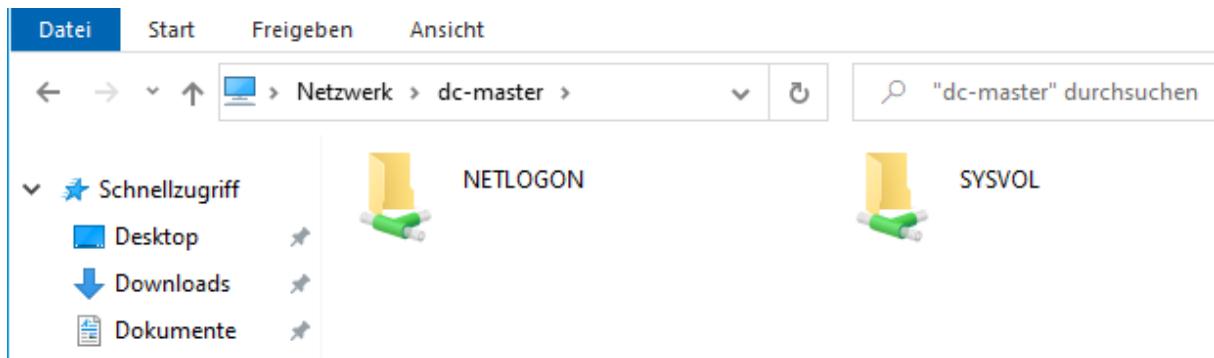
Melden Sie sich anschließend mit dem Administrator-Konto an (diese benötigen Sie, damit Sie Änderungen durchführen können) und klicken Sie auf Ändern...



Nachdem bestätigen dieses Fenster kann es einige Minuten dauern bis Windows das erfolgreiche Ändern mitteilt. Starten Sie den Client anschließend neu.

5.2.5 Netzwerk Datenträger finden

Wie Sie sehen können, lassen sich jetzt Netzwerkdatenträger in der Domain finden.



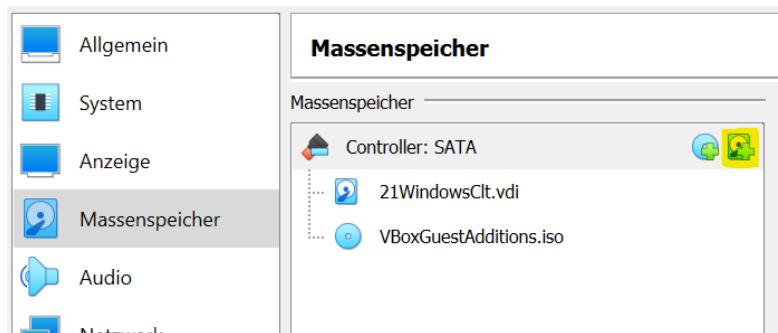
5.3 Netzwerkshare

Normalerweise verwendet man einen eigenen Server, der sich nur um die Netzwerkfreigabe kümmert. Sprich: Auf diesem extra Server werden die Daten der gesamten Benutzer, sowie Administratoren, gespeichert. Wir haben allerdings für diese Übung einfach den Domain Controller, sprich unser Standard-Server, für diese Aufgabe verwendet.

5.3.1 neue Disk hinzufügen

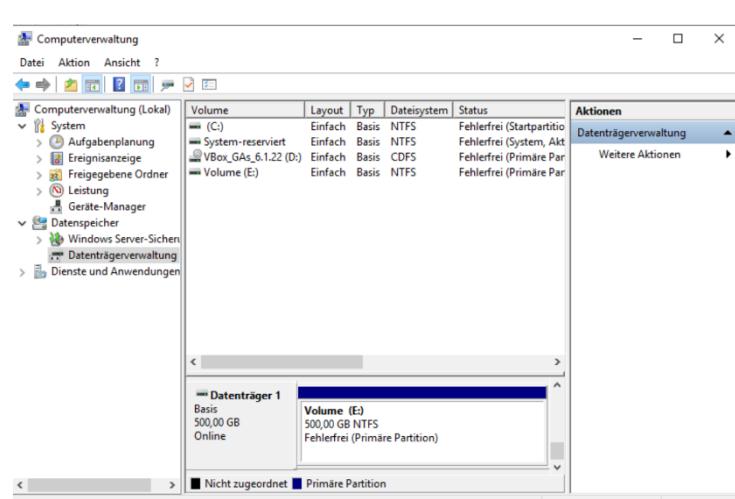
Als erstes müssen Sie eine neue virtuelle Festplatte zu dem Server hinzufügen. Dafür müssen Sie alle Clients und anschließend auch den Server herunterfahren.

Gehen Sie in die Einstellung zu Massenspeicher und klicken Sie auf den im Screenshot gelb markierten Button.

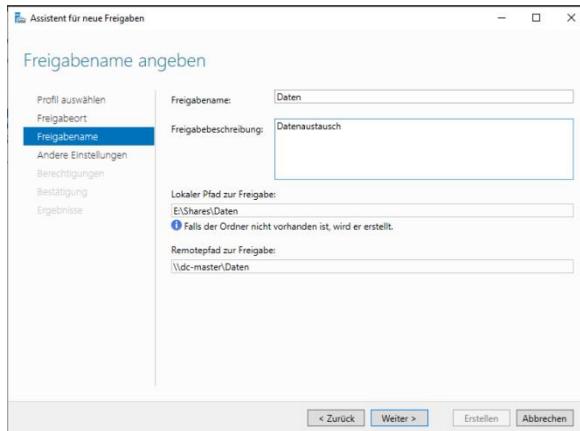


Erstellen Sie anschließend ein neues Medium, wo Sie am besten eine sinnvolle große Menge an Speicherplatz für Ihre Festplatte einstellen. Wir haben 500GB verwendet.

Starten Sie den Windows Server, gehen Sie in die Computerverwaltung → Datenträgerverwaltung und formatieren Sie die neue Platte, indem Sie einen Rechtsklick auf diese machen und "neues Volume" klicken.

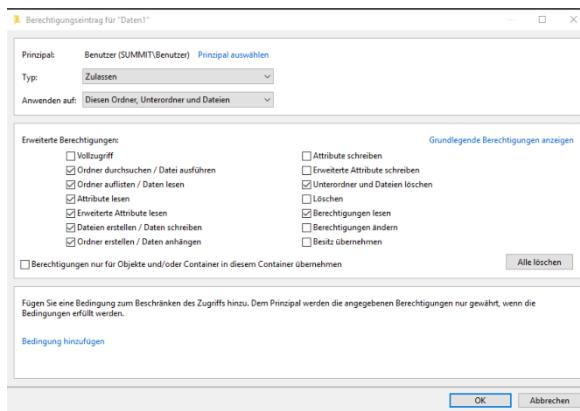


5.3.2 Freigabe konfigurieren (Assistant)



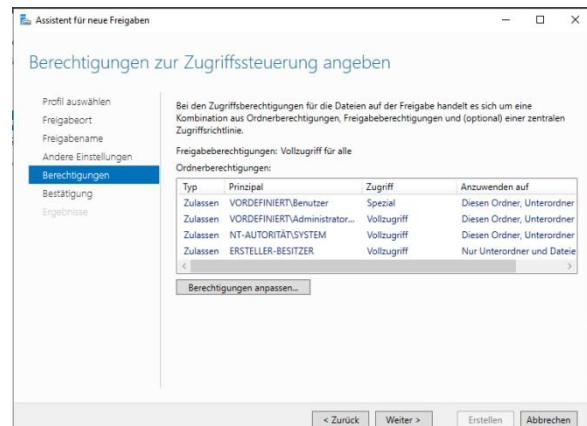
Wie Sie sehen können, haben alle in der Hierarchie höhergestellten Konten als das Benutzerkonto einen Vollzugriff auf diese Freigabe. Der Benutzer selbst hat einen speziell eingestellten Zugriff.

Dieses Ergebnis haben wir erreicht, indem wir zuerst die Vererbung deaktiviert, einen der beiden vorhanden Benutzereinstellungen (Lesen und Ausführen) gelöscht haben und anschließend die speziellen Benutzereinstellungen so bearbeitet haben, dass dieser:



Erstellen Sie anschließend am Server unter „Freigabe“ eine neue Freigabe und folgen Sie dem Assistenten. Beachten Sie dabei folgende Aspekte:

- Vergeben Sie einen sinnvollen Namen für den Datenträger (links im Bild zu sehen)!
- Stellen Sie die Berechtigungen zur Zugriffssteuerung folgendermaßen ein:



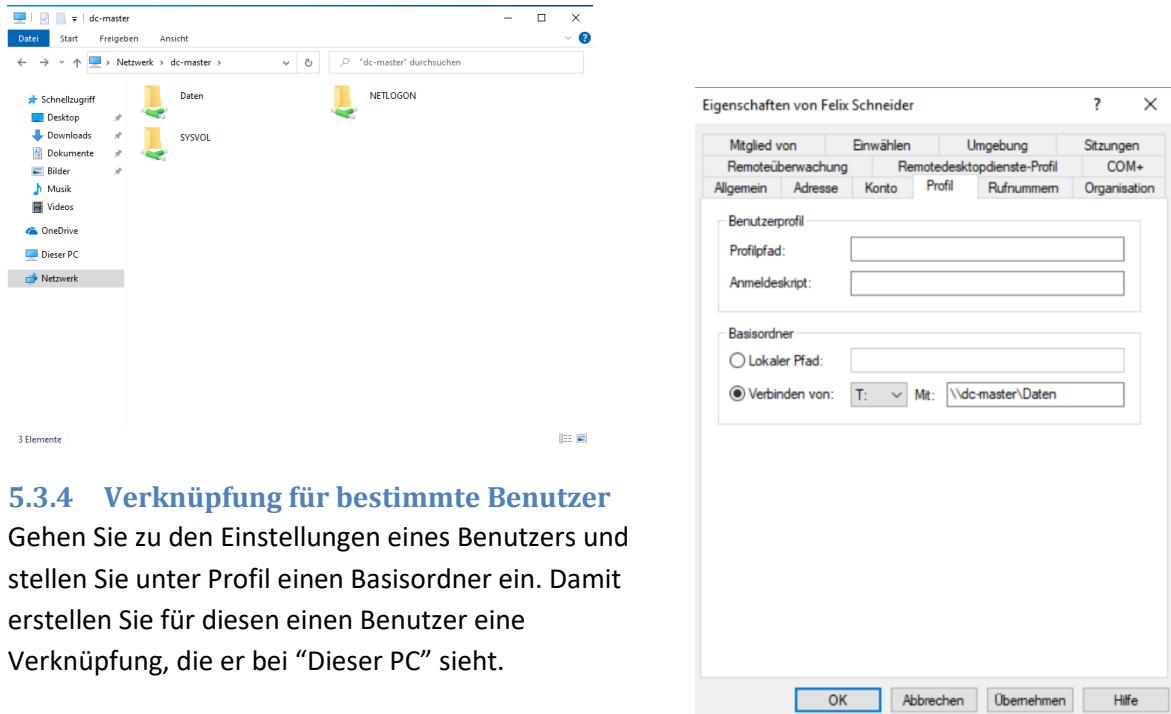
- Ordner durchsuchen, auflisten und erstellen,
- Attribute lesen,
- Dateien erstellen und löschen,
- Unterordner löschen und
- allgemein lesen kann.

Beenden Sie die Erstellung, indem Sie Fertigstellen.

5.3.3 Ergebnisse prüfen

Melden Sie sich am Client einmal mit einem Schüler an, erstellen Sie eine random Datei in einem random Ordner und sehen Sie nach, ob diese Datei bei einem Lehrer auch noch existiert.

Damit das funktioniert müssten Sie natürlich vorher den Datenträger sehen:

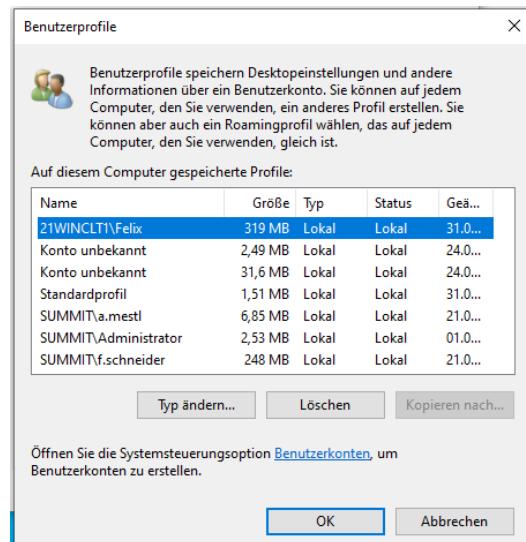
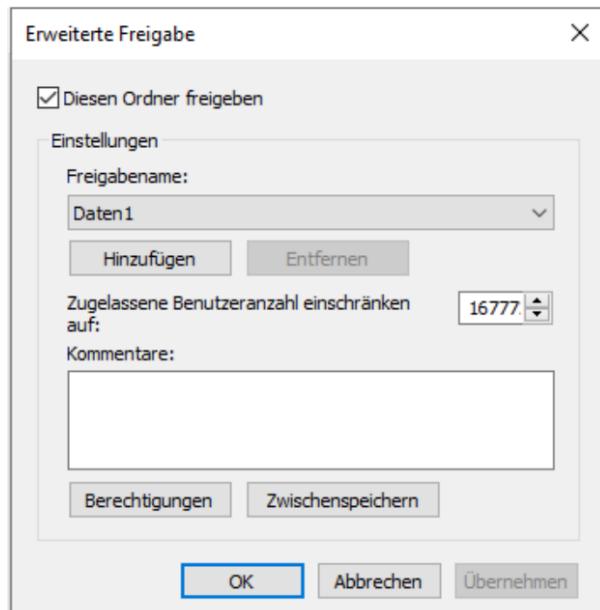


5.3.4 Verknüpfung für bestimmte Benutzer

Gehen Sie zu den Einstellungen eines Benutzers und stellen Sie unter Profil einen Basisordner ein. Damit erstellen Sie für diesen einen Benutzer eine Verknüpfung, die er bei "Dieser PC" sieht.

5.3.5 Benutzerprofile werden gespeichert

Die Benutzer, die sich bei einem Client lokal angemeldet haben, werden in den Systemsteuerung → System und Sicherheit → System → Erweiterte Systemeinstellungen → Benutzerprofile → Einstellungen gespeichert.



5.3.6 Freigabe manuell konfigurieren

Erstellen Sie einen neuen Ordner auf dem Windows Server, im Ordner E:\Shares, klicken Sie unter Eigenschaften auf Freigabe → Erweiterte Freigabe und aktivieren Sie diese wie im Bild links. Wenn beim Namen hinten ein \$-Zeichen steht, ist diese Freigabe versteckt.

5.3.7 net use

Mithilfe des net use – Befehls kann man sich sowohl die aktiven Netzwerklaufwerke anzeigen lassen als auch neue Netzwerklaufwerke hinzufügen.

```
PS T:\> net use
Neue Verbindungen werden gespeichert.
E:

Status      Lokal      Remote          Netzwerk
-----
OK          T:      \\dc-master\Daten      Microsoft Windows Network
Der Befehl wurde erfolgreich ausgeführt.

PS T:\> -
```

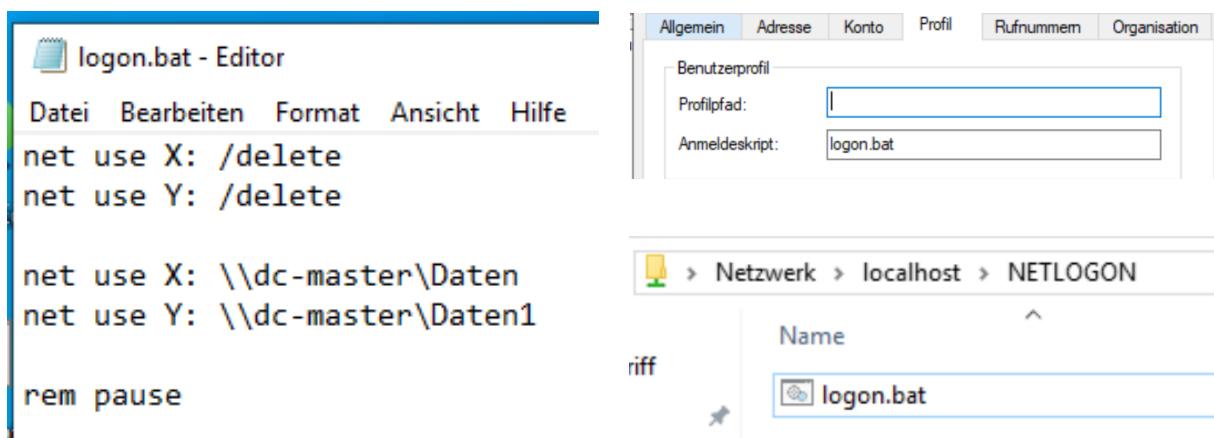
```
PS T:\> net use Q: \\dc-master\Daten2
Der Befehl wurde erfolgreich ausgeführt.

PS T:\> net use
Neue Verbindungen werden gespeichert.

Status      Lokal      Remote          Netzwerk
-----
OK          Q:      \\dc-master\Daten2    Microsoft Windows Network
OK          T:      \\dc-master\Daten      Microsoft Windows Network
Der Befehl wurde erfolgreich ausgeführt.
```

5.3.8 Script

Damit der Benutzer diese Befehle nicht jedes mal nach seiner Anmeldung eintippen braucht, kann man als Administrator ein Script schreiben, welches bei der Anmeldung eines Benutzers jedes mal ausgeführt wird. Damit dies funktioniert muss das folgende Script am Server im Ordner <\\localhost\NETLOGON> liegen. Außerdem muss der Name des Scripts auch beim Benutzer in das Feld, wie im Screenshot rechts unten gezeigt wird, stehen.



5.4 Gruppen

5.4.1 Gruppen zuordnen

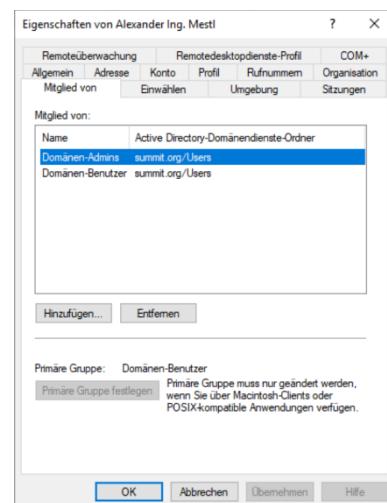
Man kann auf mehrere Arten Benutzern Richtlinien zuzuordnen:

- Benutzer zu einer Gruppe hinzufügen
- einer Gruppe einen Benutzer hinzufügen
- einer Gruppe eine Gruppe hinzufügen

5.4.1.1 Benutzer zu Gruppe hinzufügen

Man kann über die Einstellungen eines Benutzers, diesen zu bestimmten Gruppen hinzufügen. Diese Einstellung ist im rechten Bild zu erkennen.

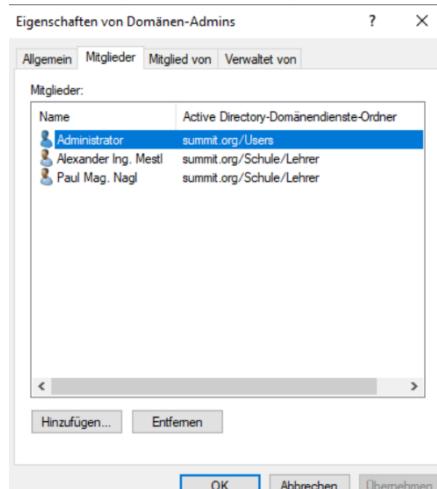
Diese Variante, einen Benutzer einer Gruppe hinzuzufügen, hat den Vorteil, dass man schnell einen Benutzer in mehrere Gruppen hinzufügen kann, was im Normalfall nicht so oft verwendet wird, wie die andere Variante, weil man wahrscheinlich im Normalfall eine Gruppe für viele Benutzer macht, die wiederum einer Gruppe hinzugefügt wird.



5.4.1.2 einer Gruppe einen Benutzer hinzufügen

Man kann einen Benutzer auch auf anderem Wege zu einer Gruppe hinzufügen, indem man nicht über die Einstellungen des Benutzers, sondern über die der Gruppe geht.

Im Prinzip ist das Endergebnis beider Varianten dasselbe. Allerdings ist es deutlich einfacher über diese Variante Benutzer zu einer Gruppe hinzuzufügen, wenn es sich um mehrere Benutzer handelt, die zu dieser Gruppe hinzugefügt werden sollen.



5.4.1.3 eine Gruppe einer Gruppe hinzufügen

Um Dinge zu vereinfachen, kann man Gruppen verschachteln. Das bedeutet, dass man zum Beispiel eine Gruppe für alle Lehrer machen kann und diese „Lehrergruppe“ wird allen Gruppen hinzugefügt, dessen Regeln Lehrer benötigen bzw. haben dürfen. Jeder neue Lehrer muss anschließend nur diese einen Lehrergruppe hinzugefügt werden, anstatt zu allen Gruppen hinzugefügt werden zu müssen, über die Lehrer verfügen.

The screenshot shows two windows for managing group properties. The top window is titled 'Eigenschaften von Alle_Lehrer' and has tabs for Allgemein, Mitglieder, Mitglied von, and Verwaltet von. The 'Mitglieder' tab is selected, showing a table with columns 'Name' and 'Active Directory-Domänen Dienste-Ordner'. It lists three users: Alexander Ing..., Herwig Ing. M..., and Paul Mag. Nagl, all under the 'summit.org/Schule/Lehrer' path. The bottom window is also titled 'Eigenschaften von Alle_Lehrer' and has the same four tabs. The 'Verwaltet von' tab is selected, showing a table with columns 'Name' and 'Active Directory-Domänen Dienste-Ordner'. It lists one group: 'Domänen-Admins' under the 'summit.org/Users' path.

Name	Active Directory-Domänen Dienste-Ordner
Alexander Ing...	summit.org/Schule/Lehrer
Herwig Ing. M...	summit.org/Schule/Lehrer
Paul Mag. Nagl	summit.org/Schule/Lehrer

Name	Active Directory-Domänen Dienste-Ordner
Domänen-Admins	summit.org/Users

5.5 Gruppenrichtlinienobjekte

The screenshot shows the 'Gruppenrichtlinienverwaltung' (Group Policy Management) console. On the left, the navigation pane shows the structure: 'Gesamtstruktur: summit.org' > 'Domänen' > 'summit.org' > 'Domain Controllers' > 'Default Domain Controller'. On the right, the main window displays the 'Default Domain Controllers Policy' configuration. It includes tabs for 'Bereich' (Scope), 'Details', 'Einstellungen', and 'Delegierung'. Under 'Verknüpfungen' (Linking), it shows that the object is linked to 'summit.org'. A table lists the link to 'Domain Controllers' with 'Erzwungen' (Enforced) set to 'Nein' (No) and 'Verknüpfung aktiviert' (Link active) set to 'Ja' (Yes). Under 'Sicherheitsfilterung' (Security Filtering), it specifies that the policy applies to 'Authentifizierte Benutzer' (Authenticated Users). The 'WMI-Filterung' (WMI Filtering) section indicates that the policy is linked via a WMI filter.

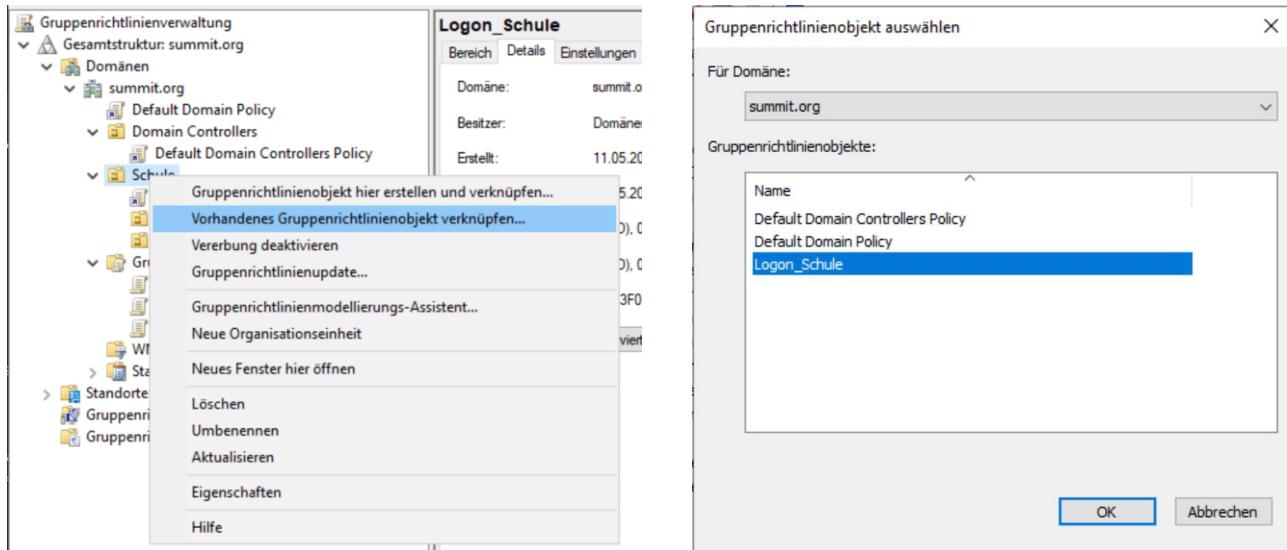
5.5.1 Gruppenrichtlinienobjekte Basiswissen

Alle Gruppenrichtlinienobjekte sind immer im Ordner `\SYSVOL\<Domain-Name>\Policies`. Jedes Gruppenrichtlinienobjekt kann mehreren OUs zugewiesen werden und jede OU kann mehrere Gruppenrichtlinienobjekte haben (n:m-Beziehung).

Wenn Sie sich im Ordner "Gruppenrichtlinienobjekte" befinden können Sie mittels Rechtsklick ein neues Gruppenrichtlinienobjekt hinzufügen. Geben Sie diesem einen sinnvollen Namen.

The screenshot shows the 'Gruppenrichtlinienverwaltung' console. The left pane shows the same navigation structure as the previous screenshot. The right pane shows a list of existing group policies under 'Gruppenrichtlinienobjekte in summit.org'. The table has columns for Name, Objektstatus (Object status), WMI-Filter (WMI Filter), Geändert (Changed), and Besitzer (Owner). Three entries are listed: 'Default Domain Controller' (Aktiviert, Keine, 29.03.2022 07:5..., Domänen-Admi...), 'Default Domain Policy' (Aktiviert, Keine, 29.03.2022 08:0..., Domänen-Admi...), and 'Logon_Schule' (Aktiviert, Keine, 11.05.2022 14:2..., Domänen-Admi...). A context menu is open at the bottom left of the right pane, with the 'Neu' (New) option highlighted. Other options in the menu are 'Alle sichern' (Secure all) and 'Sicherungen verwalten' (Manage protections).

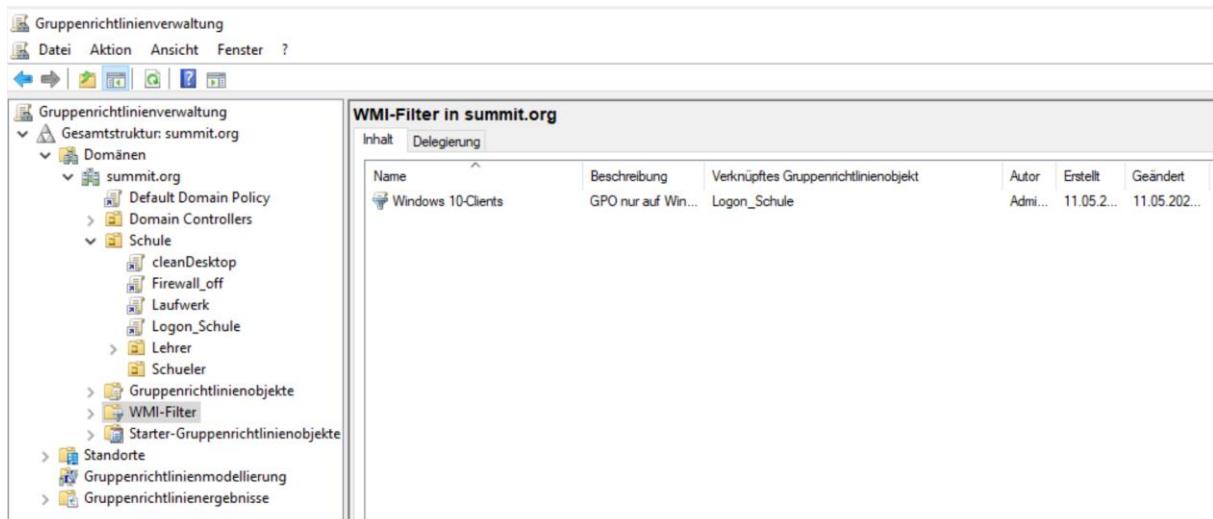
Mittels Rechtsklick auf eine OU kann man unter dem Punkt "Vorhandenes Gruppenrichtlinienobjekt verknüpfen..." dieses Gruppenrichtlinienobjekt dann der OU hinzufügen, sodass diese Regeln für alle Konten in der OU (außer bei Einschränkungen → [WMI-Filter](#)) gelten.



5.5.2 WMI-Filter

Zur detaillierteren Einschränkung, für welche Konten das Gruppenrichtlinienobjekt gilt, kann man WMI-Filter verwenden. Diese ermöglichen dann das Einschränken bzgl. Windows-Version oder Architektur (32-bit / 64-bit). Wegen der schlechten und unübersichtlichen Dokumentierung der WMI-Filter auf Seiten Microsofts ist es ein risikohaftes, aber gleichzeitig auch nützliches Tool.

Dokumentation: <https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>



In unserem Fall haben wir einen WMI-Filter mithilfe eines Rechtsklicks im Reiter "Inhalt" (Screenshot oberhalb) → Neu hinzugefügt, einen sinnvollen Namen vergeben und eine Abfrage hinzugefügt, wie Sie im nächsten Screenshot sehen können. Dabei haben wir den Namespace laut Microsofts (ausführlicher 😊 Dokumentation) unberührt gelassen und nur die Abfrage selbst verändert, wobei der Code vom Herrn Professor Mestl kommt, welcher ihn wiederrum vom Browser des Vertrauens gegooglt hat...

Windows 10-Clients

Allgemein Delegierung

WMI-Filter

Beschreibung: GPO nur auf Windows 10-Clients ausführen

Abfragen:

Namespace	Abfrage
root\CIMv2	select * from Win32_OperatingSystem where Version like "10.%"

Gruppenrichtlinienobjekte, die diesen WMI-Filter verwenden

Folgende Gruppenrichtlinienobjekte sind mit diesem WMI-Filter verknüpft:

Gruppenrichtlinienobjekt

Logon_Schule

Windows 10-Clients

Name: **Windows 10-Clients**

Beschreibung: GPO nur auf Windows 10-Clients ausführen

Abfragen:

Namespace	Abfrage
root\CIMv2	select * from Win32_OperatingSystem where Version like "10.%"

Hinzufügen Entfernen Bearbeiten

Speichern Abbrechen

WMI-Abfrage

Namespace: root\CIMv2 Durchsuchen...

Abfrage:

```
select * from Win32_OperatingSystem where Version like "10.%"
```

OK Abbrechen

5.5.3 Einstellungen eines Gruppenrichtlinienobjekts

5.5.3.1 Bereich

Im Reiter Bereich kann man sehen, welche OUs mit dem Gruppenrichtlinienobjekt verknüpft sind. Außerdem sieht man hier die Benutzer- / Computerfilter, sprich, auf welchen Konten dieses Gruppenrichtlinienobjekt gilt und angewendet werden muss. Hier sind auch die vorher beschriebenen WMI-Filter finden und einstellen.

Logon_Schule

Bereich Details Einstellungen Delegierung Status

Verknüpfungen

Für dieses Verzeichnis anzeigen: summit.org

Die folgenden Standorte, Domänen und Organisationseinheiten sind mit dem Objekt verknüpft:

Pfad	Erzwungen	Verknüpfung aktiviert	Pfad
Schule	Nein	Ja	summit.org/Schule

Sicherheitsfilterung

Die Einstellungen dieses Gruppenrichtlinienobjekts gelten nur für die folgenden Gruppen, Benutzer und Computer:

Name
Authentifizierte Benutzer

Hinzufügen... Entfernen Eigenschaften

WMI-Filterung

Dieses Gruppenrichtlinienobjekt ist mit folgendem WMI-Filter verknüpft:

<Kein> Öffnen

5.5.3.2 Details

Im Reiter Details findet man nähere Beschreibungen und Daten bzgl. des Gruppenrichtlinienobjekts. Im rechten Screenshot finden Sie die einzelnen Felder:

Wie Sie sehen können, kann man einen Objektstatus festlegen. Schlau Administratoren deaktivieren entweder die Benutzerkonfigurationseinstellungen oder die Computerkonfigurationseinstellungen, je nach dem, welches sie nicht benötigen. Wenn in einer Gruppenrichtlinie beide Einstellungen gesetzt werden, lassen Sie diesen auf Aktiviert.

Logon_Schule

Bereich Details Einstellungen Delegierung Status

Domäne: summit.org

Besitzer: Domänen-Admins (SUMMIT\Domänen-Admins)

Erstellt: 11.05.2022 14:22:18

Geändert: 11.05.2022 14:22:18

Benutzerversion: 0 (AD), 0 (SYSVOL)

Computerversion: 0 (AD), 0 (SYSVOL)

Eindeutige ID: {4633F01C-B75B-456E-A9CE-3883A32C8AF2}

Objektstatus: Aktiviert

Kommentar: Alle Einstellungen deaktiviert

5.5.3.3 Einstellungen

Im Reiter Einstellungen kann man dann die Richtlinien (policies) ansehen. Sprich: Hier sieht man, welche Scripts ausgeführt wurden bzw. welche WMI-Filter gesetzt sein, ob diese funktionieren oder nicht.

Logon_Schule

Bereich Details Einstellungen Delegierung Status

Logon_Schule
Daten ermittelt am: 11.05.2022 14:33:02

Allgemein

Details	Ausblenden
Verknüpfungen	Einblenden
Sicherheitsfilterung	Einblenden
Delegierung	Einblenden

Computerkonfiguration (Aktiviert)

Keine Einstellungen definiert	Ausblenden
-------------------------------	------------

Benutzerkonfiguration (Aktiviert)

Keine Einstellungen definiert	Ausblenden
-------------------------------	------------

5.5.3.4 Delegierung

Im Reiter Delegierung kann man die Richtlinie einem anderen Nutzer oder einer Gruppe delegieren.

Logon_Schule

Bereich Details Einstellungen Delegierung Status

Folgende Gruppen und Benutzer haben die angegebene Berechtigung für dieses Gruppenrichtlinienobjekt:

Gruppen und Benutzer:

Name	Zulässige Berechtigungen	Vererbt
Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
Domänen-Admins (SUMMIT\...)	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
DOMANENCONTROLLER D...	Lesen	Nein
Organisations-Admins (SUMMI...)	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

5.5.3.5 Status

Also Herr Professor Mestl glaubt, dass der Reiter Status anzeigen, ob das Gruppenrichtlinienobjekt bereits auf allen Domain Controllern repliziert wurde. Nach kürzerer Recherche hat sich herausgestellt, dass er damit Recht behalten soll: <https://administrator.de/forum/gpmc-reiter-status-nur-in-windows-server-2012-267426.html>

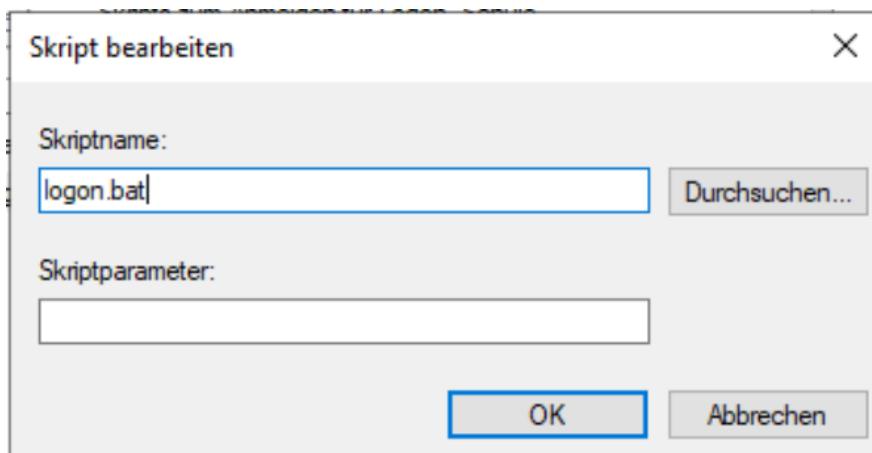
The screenshot shows a web-based status page for the 'Logon_Schule' domain. At the top, there's a navigation bar with tabs: Bereich, Details, Einstellungen, Delegierung, and Status. The Status tab is selected. Below the tabs, a message states: 'Auf dieser Seite wird der Status der Active Directory- und SYSVOL-Replikation für diese Domäne in Beziehung zu Gruppenrichtlinien angezeigt.' Under the heading 'Statusdetails', it says: '"dc-master.summit.org" ist der Basisdomänencontroller für diese Domäne.' A note below states: 'Für diese Domäne sind keine Infrastrukturstatusinformationen vorhanden.' A final note at the bottom says: 'Klicken Sie unten auf die Schaltfläche 'Jetzt ermitteln', um den Infrastrukturstatus von allen Domänencontrollern in dieser Domäne zu erfassen.'

5.5.4 Editor

Computerkonfigurationen werden ausgeführt, wenn der Computer gestartet / heruntergefahren wird, und Benutzerkonfigurationen werden ausgeführt, wenn der Benutzer sich anmeldet / abmeldet. Unter Benutzerkonfiguration → Richtlinien → Windows-Einstellungen → Scripts → Anmelden kann man ein Script hinzufügen, welches beim Anmelden eines Kontos ausgeführt werden soll.

The screenshot shows the 'Gruppenrichtlinienverwaltungs-Editor' (Group Policy Management Editor) window. The left pane shows a tree structure of Group Policy objects: Computerkonfiguration and Benutzerkonfiguration. Under Benutzerkonfiguration, there are Richtenlinien, Softwareeinstellungen, and Windows-Einstellungen. The Windows-Einstellungen node is expanded, showing Skripts (Anmelde). The right pane shows the properties for the 'Anmelden' script. It lists 'Name' (Anmelden) and 'Abmelden'. The 'Beschreibung' field says: 'Enthält Benutzeranmeldeskripts.' A detailed dialog box titled 'Eigenschaften von Anmelden' is open, showing a table with one item: 'Name' (logon.bat) and 'Parameter' (empty). Buttons for 'Nach oben', 'Nach unten', 'Hinzufügen...', 'Bearbeiten...', and 'Entfernen' are visible. A note at the bottom says: 'Klicken Sie auf die Schaltfläche, um die Skriptdateien in diesem Gruppenrichtlinienobjekt anzuzeigen.' At the bottom of the dialog are 'OK', 'Abbrechen', and 'Übernehmen' buttons.

Geben Sie hierfür am besten nicht den absoluten, sondern den relativen Dateipfad an, damit dieser auch von Clients auch erreichbar ist (localhost am Client enthält nämlich kein SYSVOL). Bestätigen Sie das Fenster mit OK.



5.5.5 logon.bat

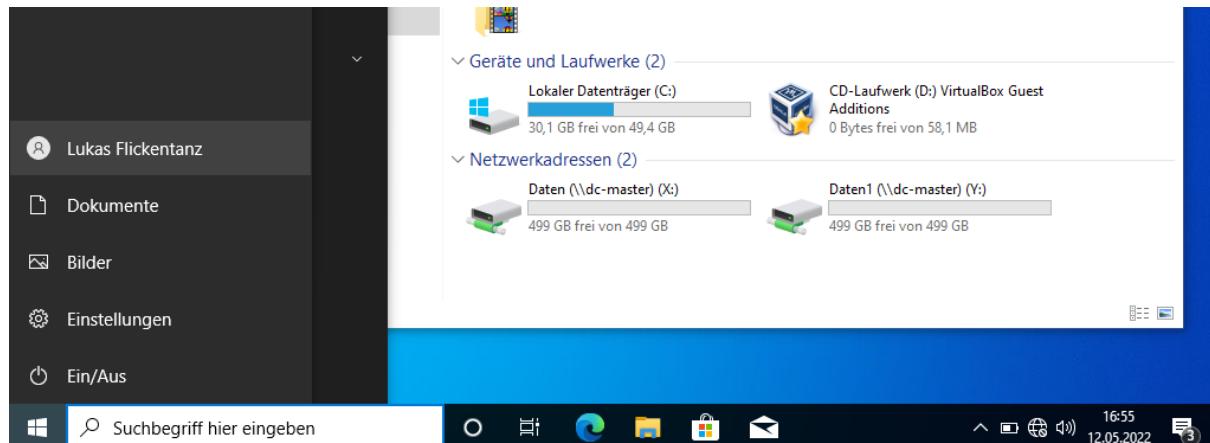
Wie sie im unten abgebildeten Screenshot sehen können, wurde das logon.bat – Script erfolgreich zu dem Gruppenrichtlinienobjekt hinzugefügt. (Das heißt nicht, dass es bei Administratoren funktioniert)

Name	Parameter
logon.bat	

5.5.6 Überprüfen

Um nun zu Überprüfen, ob das Gruppenrichtlinienobjekt auch funktioniert, melden Sie sich bei einem beliebigen Benutzerkonto (außer Admins) auf einem beliebigen Computerkonto (natürlich muss das Gruppenrichtlinienobjekt für dieses Benutzer und diesen Computer auch gelten) an, und

sehen nach, ob das Script erfolgreich ausgeführt wurde. In unserem Fall können Sie nachsehen, ob ein X: und ein Y: Laufwerk vorhanden sind.



Bei mir hat dies erst funktioniert, als ich das Script nach dem Hinzufügen noch einmal geändert habe.

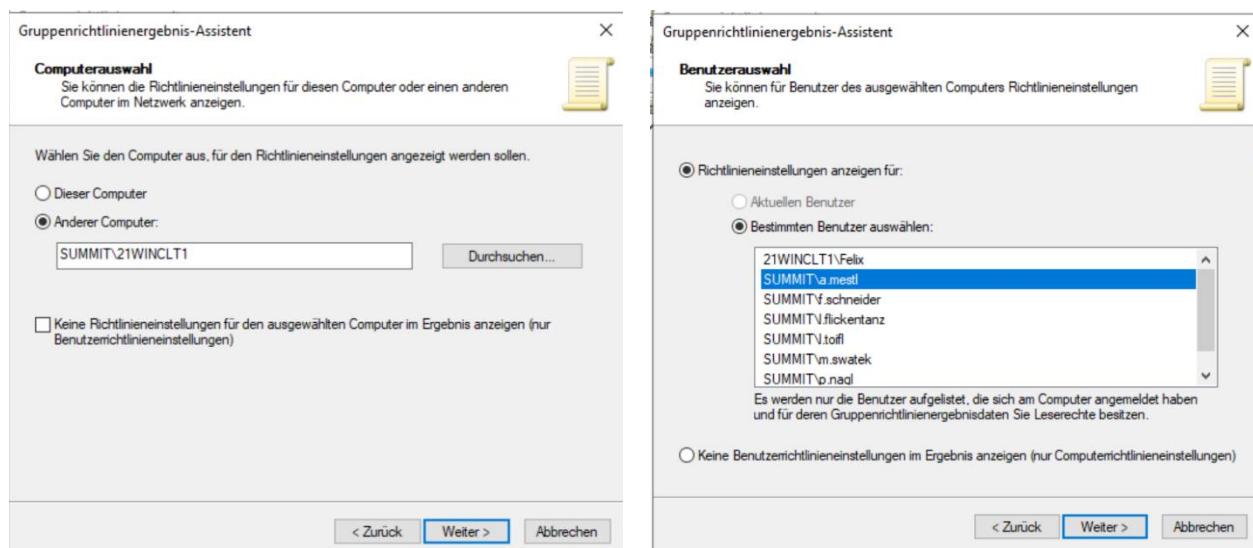
5.5.7 Ergebnisse

5.5.7.1 von Server aus

Unter dem Ordner Gruppenrichtlinienergebnisse kann man sich Berichte von bestimmten Benutzern auf Computern erstellen lassen.

Machen Sie in diesem Ordner einen Rechtsklick und wählen Sie "Gruppenrichtlinienergebnis-Assistant..." aus.

Wählen Sie das Computerobjekt aus, welches Sie überprüfen möchten und anschließend eines der lokalen Benutzerobjekte auf diesem Computerobjekt.



Nach der Fertigstellung erhalten Sie einen Bericht. Hier können Sie zum Beispiel sehen, dass das logon.bat – Script beim Benutzer a.mestl auf 21WINCLT1 ausgeführt wird. **Dies bedeutet aber nicht zwingend, dass es auch funktioniert**, weil Logon-Scripts auf Administratorkonten nicht ausgeführt werden. Wir bezeichnen so ein komplexes, verwirrendes Verhalten in der IT als **BUG!**

Name	Parameter	Zuletzt ausgeführt	Skriptreihenfolge im Gruppenrichtlinienobjekt	Ausschlaggebendes Gruppenrichtlinienobjekt
logon.bat	Logon_Schule	11.05.2022 15:53:31	Nicht konfiguriert	

5.5.7.2 von Client aus

Ob die Gruppenrichtlinienobjekte auch richtig greifen, können Sie auch vom Client aus überprüfen.
Aktualisieren Sie jedoch vorher sicherheitshalber die Gruppenrichtlinieobjekte:

```
PS C:\Users\l.flickentanz> gpupdate
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.
```

```
PS C:\Users\l.flickentanz> gpupdate /force
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.
```

Überprüfen Sie anschließend die Gruppenrichtlinienobjekte: (Wenn Logon_Schule dasteht, bedeutet das wieder nicht, dass es funktionieren muss...)

```
PS C:\Users\l.flickentanz> gpresult /r

Betriebssystem Microsoft (R) Windows (R) Gruppenrichtlinienergebnis-Tool v2.0
© 2020 Microsoft Corporation. Alle Rechte vorbehalten.

Am 18.05.2022 um 14:19:37 erstellt

RSOP-Daten für SUMMIT\l.flickentanz auf 21WINCLT1: Protokollmodus
-----
Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion: 10.0.19041
Standortname: Nicht zutreffend
Roamingprofil:Nicht zutreffend
Lokales Profil: C:\Users\l.flickentanz
Langsame Verbindung? Nein

BENUTZEREINSTELLUNGEN
-----
CN=Lukas Flickentanz,OU=Schueler,OU=Schule,DC=summit,DC=org
Letzte Gruppenrichtlinienanwendung: 18.05.2022, um 14:19:11
Gruppenrichtlinienanwendung von: dc-master.summit.org
Schwellenwert für langsame Verbindung:500 kbps
Domänenname: SUMMIT
Domänenotyp: Windows 2008 oder höher

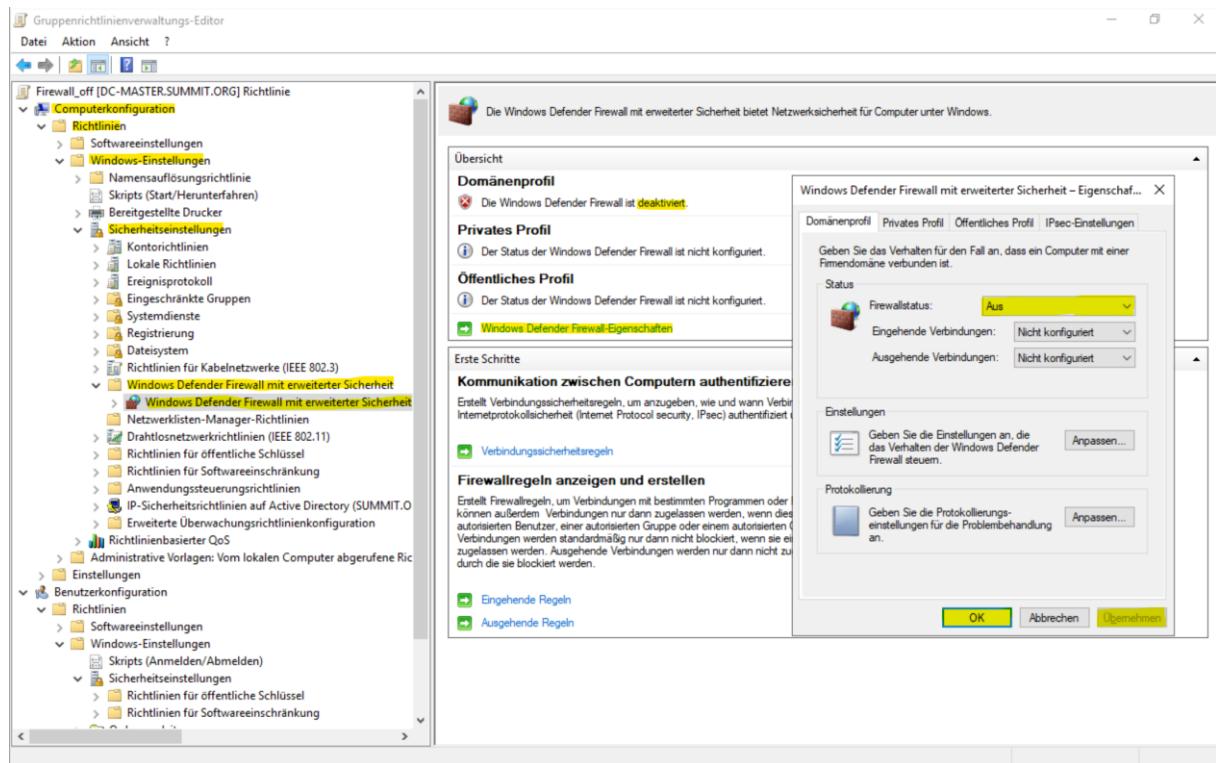
Angewendete Gruppenrichtlinienobjekte
-----
Logon_Schule

Folgende herausgefilterte Gruppenrichtlinien werden nicht angewendet.
-----
Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet (Leer)

Der Benutzer ist Mitglied der folgenden Sicherheitsgruppen
-----
Domänen-Benutzer
Jeder
Benutzer
INTERAKTIV
KONSELENANMELDUNG
Authentifizierte Benutzer
Diese Organisation
LOKAL
Von der Authentifizierungsstelle bestätigte ID
Mittlere Verbindlichkeitsstufe
```

5.5.8 Firewall off

Nun erstellen wir ein neues Gruppenrichtlinienobjekt, bei welchem wir die Firewall für Domainprofile deaktivieren. Folgen Sie den gelb markierten Ordner / Links, um dies zu erreichen.



Auf einem Computer, dem dieses Gruppenrichtlinienobjekt dann zugeordnet wurde, kann man die Statusmeldung lesen, dass einige Firewall-Einstellungen vom Systemadministrator verwaltet.
(Vergessen Sie nicht, das GPO mit der OU zu verknüpfen)

Den PC mithilfe der Windows Defender Firewall schützen

Mithilfe der Windows Defender Firewall kann verhindert werden, dass Hacker oder Schadsoftware über das Internet bzw. über ein Netzwerk Zugriff auf den PC erhalten.

Zu Ihrer Sicherheit werden einige Einstellungen vom Systemadministrator verwaltet.

Firealleinstellungen aktualisieren

Die zum Schutz des Computers empfohlenen Einstellungen werden nicht von der Windows Defender Firewall verwendet.

Was sind die empfohlenen Einstellungen?

Domänen Netzwerke

Verbunden

Netzwerke am Arbeitsplatz, die zu einer Domäne gehören

Windows Defender Firewall-Zustand:	Aus
Eingehende Verbindungen:	Alle Verbindungen mit Apps blockieren, die nicht in der Liste zugelassener Apps vorhanden sind
Aktive Domänen Netzwerke:	summit.org
Benachrichtigungsstatus:	Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird

Private Netzwerke

Nicht verbunden

Gast oder öffentliche Netzwerke

Nicht verbunden

5.5.9 Laufwerkzuordnung

Unter Benutzerkonfiguration → Einstellungen → Windows-Einstellungen → Laufwerkzuordnung können Sie Benutzern Laufwerke zuordnen.

The screenshot displays two windows related to drive mapping:

- Gruppenrichtlinienverwaltungs-Editor:** Shows a tree structure under "Computerkonfiguration" and "Benutzerkonfiguration". Under "Windows-Einstellungen", "Laufwerkzuordnung" is selected. A table lists a single entry for drive Z:

Name	Reihenfolge	Aktion	Pfad	Verbindung wiederherstellen
Z:	1	Aktualisieren	\dc-master\Datenv2	Nein

- Eigenschaften von Z:** This dialog box shows settings for drive Z:
 - Allgemein:** Speicherort: \dc-master\Datenv2, Aktion: Aktualisieren.
 - Laufwerkbuchstabe:** Ersten verfügbaren verwenden, beginnend mit: z.
 - Verbinden als (optional):** Benutzername: [empty], Kennwort: [empty], Kennwort bestätigen: [empty].
 - Laufwerk aus-/einblenden:** Keine Änderung (selected).
 - Alle Laufwerke aus-/einblenden:** Keine Änderung (selected).

Bottom Panel:

- Geräte und Laufwerke (2):**
 - Lokaler Datenträger (C): 30,1 GB frei von 49,4 GB
 - CD-Laufwerk (D): VirtualBox Guest Additions 0 Bytes frei von 58,1 MB
- Netzwerkadressen (3):**
 - Daten (\dc-master) (X): 499 GB frei von 499 GB
 - Daten1 (\dc-master) (Y): 499 GB frei von 499 GB
 - Daten2 (\dc-master) (Z): 499 GB frei von 499 GB

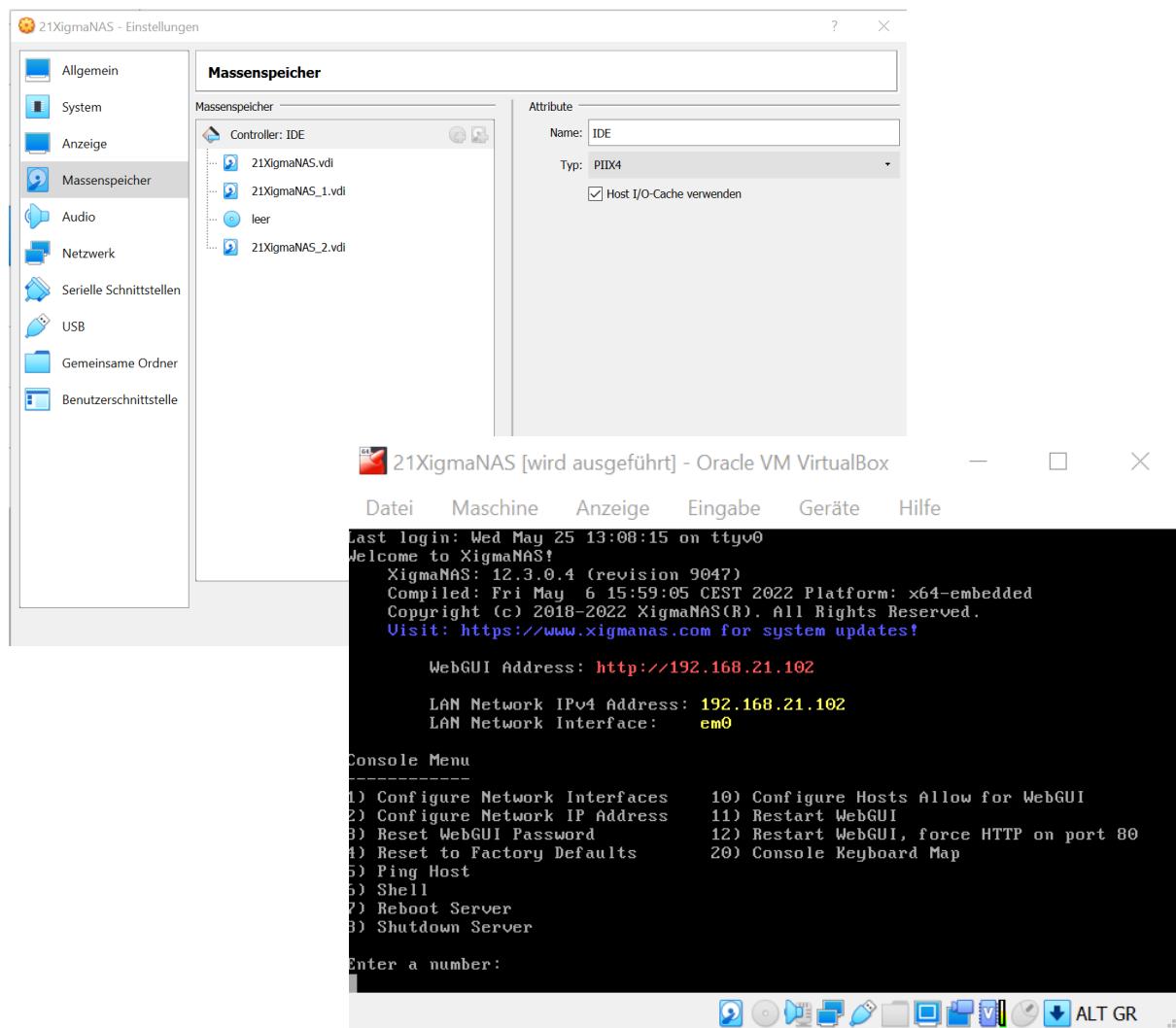
5.6 XigmaNAS

5.6.1 XigmaNAS konfigurieren

5.6.1.1 Server aufsetzen

Als erstes setzen wir eine neue Virtuelle Maschine mit folgenden Einstellungen auf:

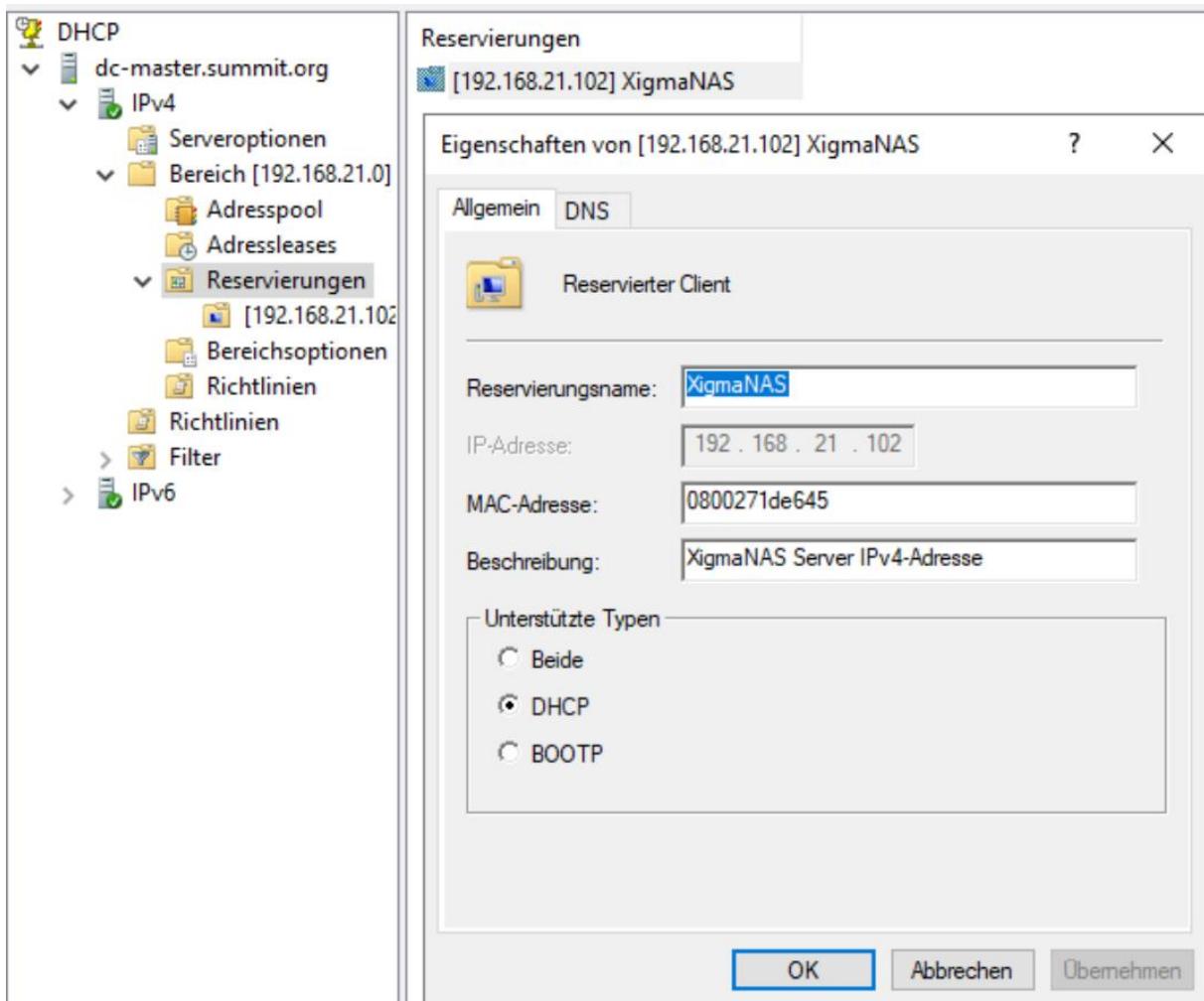
- 2GB Ram (sollte reichen)
- Festplatte mit XigmaNAS Installation: 8GB
- 1. Festplatte mit Daten: 16GB
- 2. Festplatte mit Daten: 16GB
- zuerst NAT Netzwerk, damit Installation funktioniert, nach der Installation wechseln zum internen Netz
- ISO-File von XigmaNAS-Homepage einfügen als optisches Laufwerk (<https://sourceforge.net/projects/xigmanas/files/>)
- Installation von XigmaNAS mit Swap (GPT)
- IPv4-Adresse: 192.168.21.102



5.6.1.2 IPv4 Adresse konfigurieren

Man könnte (das wäre ein einfacherer Weg) eine statische IPv4-Adresse vergeben). Allerdings finden wir es schöner, wenn wir eine Reservierung beim DHCP-Server (Windows Server) erstellen, damit im Falle von DDNS, dieser Server automatisch auch einen Namen bekommt.

Also gehen wir zu den Server-DHCP-Konfigurationen und erstellen diese neue IPv4-Reservierung:



Dies kann man entweder mit einem Rechtsklick → Neue Reservierung im Ordner "dc-master.summit.org" → IPv4 → Bereich → Reservierungen" erzielen oder man klickt oben auf folgendes Symbol:



5.6.1.3 Festplatten konfigurieren

Unter “Disks→Management” kann man die Festplatten zuerst hinzufügen, dann formatieren und schlussendlich raiden.

Device	Device Model	Size	Serial Number	Contr...	Controller Model	Standby	Filesystem	Status	Toolbox
ada1	VBOX HARDDISK	17.17GB	VB301c8280-24b0ea4c	ata0	Intel PIIX4 UDMA33 controller	Always On	SoftRaid	ONLINE	
ada2	VBOX HARDDISK	17.17GB	VBF7fc2978-2e16dec0	ata1	Intel PIIX4 UDMA33 controller	Always On	SoftRaid	ONLINE	

Delete Selected Disks Rescan Busses

5.6.1.4 Raid konfigurieren

Unter “Disks→Software RAID” kann man dann das RAID-System konfigurieren und aufsetzen. Wir haben ein RAID1 namens RaidShadowLegends aufgesetzt.

Volume Name	Type	Size	Description	Status	Toolbox
RaidShadowLegen	RAID-1	17.17GB	GEOM Software RAID	COMPLETE	

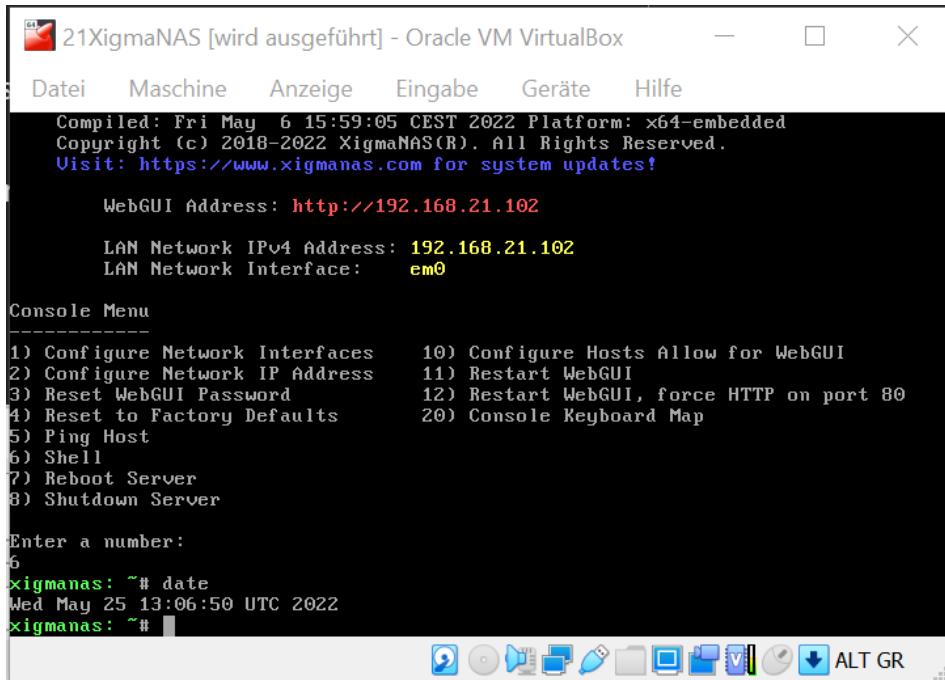
5.6.1.5 SMB konfigurieren

Um SMB (Server Message Block(s)) zu aktivieren, gehen Sie im Overview zu “Service → SMB”

5.6.1.6 NTP konfigurieren

Damit der XigmaNAS Server die Zeit des Windows Servers verwendet, kann man in dem Feld NTP Time Server unter “System→General” den Server mit Domainname eintragen. Außerdem muss man beim Hostnamen die Domain angeben.

Time	
Time Zone	Europe/Vienna Select the location closest to you.
Date Format	Wednesday June 01 14:20:08 CEST 2022 Select a date format.
System Time	<input type="text"/> Enter desired system time directly (format mm/dd/yyyy hh:mm) or use icons.
Enable NTP	<input checked="" type="checkbox"/> Use the specified NTP server.
NTP Time Server	dcmaster.summit.org Use a space to separate multiple hosts (only one required). Remember to add the port number if needed.
Time Synchronization	60 Minutes between the next network time synchronization.
Hostname	
Hostname	21nas Name of the NAS host, without domain part e.g. xigmanas.
Domain	summit.org e.g. com, local



zusätzliche Informationen zu NTP: NTP ist das Network Time Protocol, ein Protokoll, welches nach daytime und time entwickelt wurde, allerdings hat es einen großen Vorteil / Verbesserung: NTP berücksichtigt die Packetlaufzeit, weshalb es nicht nur sekundengenau, sondern auch auf 10 Millisekunden.

Bzw. Wikipedia: Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Echtzeituhren in Computersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Transportprotokoll UDP oder das verbindungsbezogene TCP. Es wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen.

5.6.2 XigmaNAS zur Domain hinzufügen

5.6.2.1 Neuen XigmaNAS Benutzer erstellen

Als erstes erstellen wir einen neuen Benutzer, weil wir diesen benötigen, um uns in der Domain anmelden zu können.

5.6.2.2 Domainenintegration

Gehen Sie in der Overview von XigmaNAS zu "Access→Active Directory" und aktivieren Sie dieses Active Directory. Konfigurieren Sie die Felder richtig (Passoword: User123):

Active Directory	
Domain Controller Name	dc-master Enter AD or PDC name.
Domain Name (DNS/Realm-Name)	summit.org Enter the domain name.
Domain Name (NetBIOS-Name)	SUMMIT Enter NetBIOS name.
Administrator Name	xigmanas Enter user name of a domain administrator account.
Administrator Password	Password Enter the password of the domain administrator account.

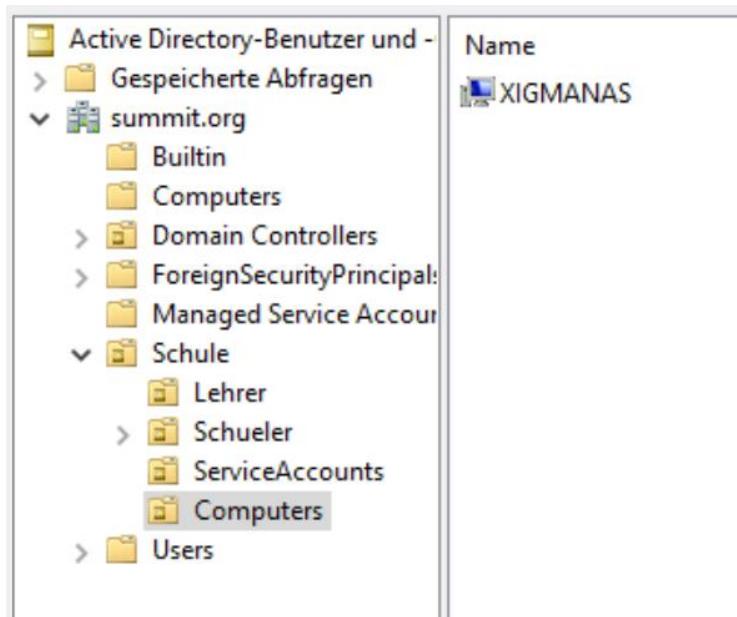
5.6.2.3 SMB auf AD umstellen

Gehen Sie in die SMB-Einstellungen ("Services→SMB") und editieren Sie die Einstellungen auf Active Directory um. Konfigurieren Sie die WINS-Server-IP-Adresse und die Workgroup:

SMB Settings	
Service Active	Yes
Authentication	Authentication <input type="radio"/> Local User <input checked="" type="radio"/> Active Directory <input type="checkbox"/> Allow trusted domains. If allowed, a user of the trust Password server name or IP address dc-master.summit.org WINS server IP address (e.g. This option affects how clients respond to requests
NetBIOS Name	xigmanas The NetBIOS name of this Samba server
Workgroup	SUMMIT The workgroup in which the server belongs

5.6.2.4 Neuen Computer in OU verschieben

Zur besseren Strukturierung verschieben wir den neuen Computer nach "Schule→Computers".

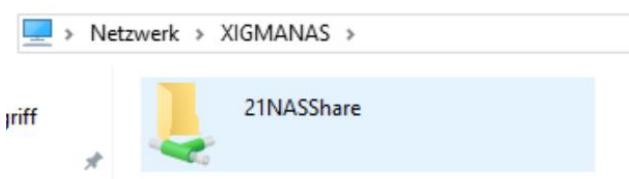


5.6.2.5 SMB Share hinzufügen

Damit nun alle Clients und Server auf die Daten vom Xigma NAS Server zugreifen können, gehen Sie zu den "SMB-Settings → Shares". Fügen Sie über dieses – Symbol einen neuen Share hinzu und konfigurieren Sie diesen nach Ihren Bedürfnissen.

Share Settings	
Name	21NASShare
Comment	Xigma NAS Share of RaidShadowLegends
Path	/mnt/RaidShadowLegends Path to be shared.

Überprüfen Sie die Einstellungen, indem Sie beim Server oder Client "\\\XIGMANAS" in die Adressleiste beim Explorer eingeben und hoffentlich den Share sehen:



5.6.2.6 Logon-Script oder Gruppenrichtlinienobjekte updaten

Damit alle Clients eine Verlinkung auf den Share haben, können Sie nun entweder das Logon-Script updaten oder einfach das Gruppenrichtlinienobjekt updaten (wir haben es mit Gruppenrichtlinienobjekten verknüpft).

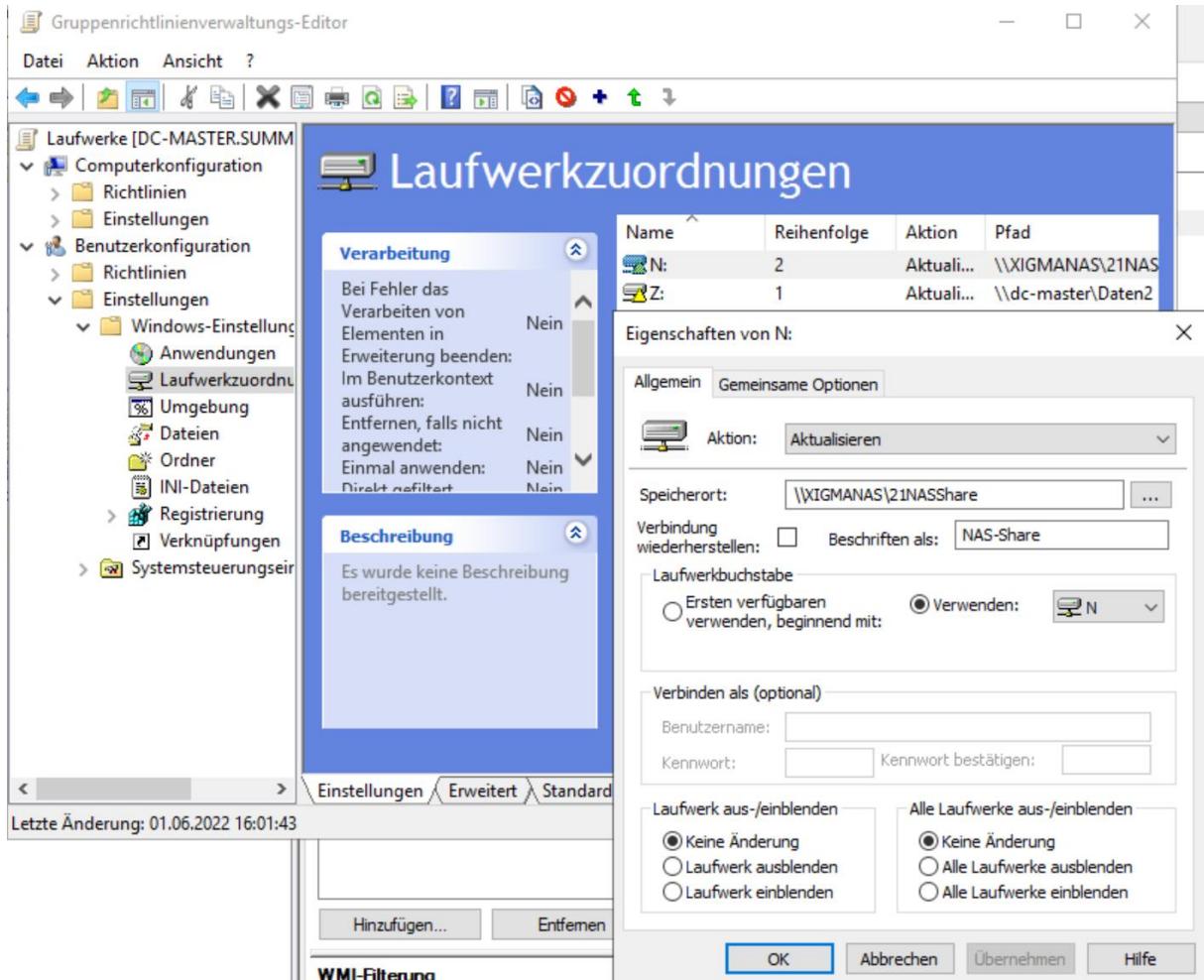
logon.bat - Editor

```

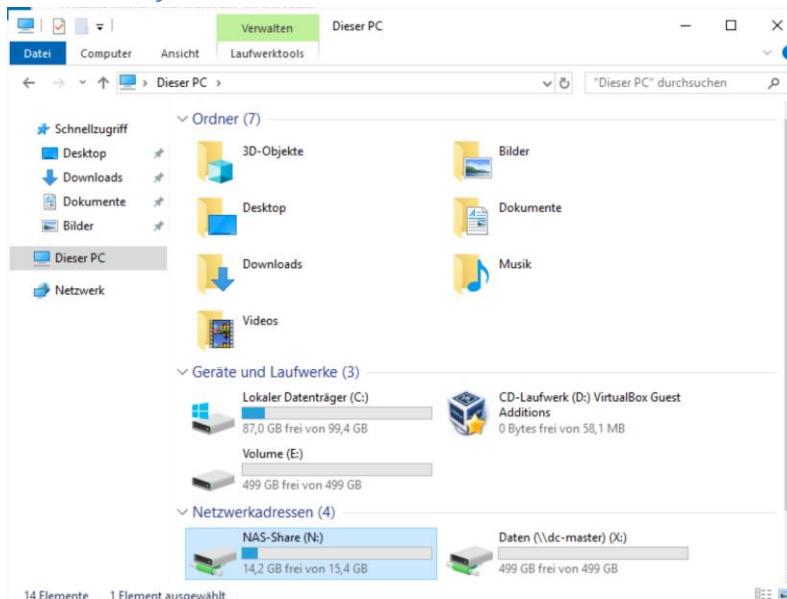
Datei  Bearbeiten  Format  Ansicht  Hilfe
het use X: /delete
net use Y: /delete
net use N: /delete

net use X: \\dc-master\Daten
net use Y: \\dc-master\Daten1
net use N: \\XIGMANAS/21NASShare

```



5.6.2.7 Es funktioniert!



6 Ergebnisse

Ewerythink ist vorking! LOL

7 Code

8 Kommentar

Clemens mag kein Windows.