

Übungsprotokoll

SYTS – Systemtechnik Systemintegration und Infrastruktur

 htlkrems Bautechnik & IT	Übungsdatum: KW 42/2022 – KW 47/2022	Klasse: 5AHIT	Name: Felix Schneider
	Abgabedatum: 21.11.2023	Gruppe: SYTS_2	Note:
Leitung: DI (FH) Alexander MESTL	Mitübende: -		
Übungsbezeichnung:		NAS Userprofils	

Inhaltsverzeichnis:

1	Aufgabenstellung.....	4
2	Abstract (English).....	4
3	Theoretische Grundlagen.....	5
3.1	Winbind	5
3.2	SSSD	5
3.3	Kerberos	6
3.3.1	Tickets.....	6
4	Übungsdurchführung	7
4.1	Openmediavault aufsetzen	7
4.2	Weboberfläche.....	9
4.2.1	IP-Adresse konfigurieren	11
4.2.2	NTP konfigurieren.....	12
4.3	OVM Domainbeitritt.....	13
4.3.1	mit SSSD.....	13
4.3.1.1	DNS Einstellungen zeigen auf AD	13
4.3.1.2	AD erkunden.....	14
4.3.1.3	Informationen eines AD Nutzers abfragen.....	16
4.3.1.4	Automatisch einen Ordner erstellen (optional)	16
4.3.1.5	Automatischer Domain Name	17
4.3.1.6	Anmeldung	18
4.3.1.7	RAID	19
4.3.1.8	Benutzerübersicht	19
4.3.2	mit Winbind	21
4.3.2.1	Open Tutorial.....	21
4.3.2.2	Install packages	21
4.3.2.3	Kerberos konfigurieren.....	21
4.3.2.4	Kerberos Ticket holen.....	21
4.3.2.5	Samba konfigurieren	22
4.3.2.6	Name Service Switch auf Winbind umstellen	22
4.3.2.7	Automatisch Home Verzeichnis erstellen	23
4.3.2.8	ADS joinen	24
4.3.2.9	User Infos.....	24
4.3.2.10	User Web.....	25

4.3.2.11	Samba	26
4.3.2.12	RAID	27
4.3.2.13	Dateisystem erstellen	27
4.3.2.14	Freigegebener Ordner erstellen	28
4.3.2.15	SMB Share	28
4.3.2.16	Zugriffskontrolllisten einstellen.....	29
4.3.2.17	Ordnerzugriff	29
4.3.2.18	File erstellen	30
4.3.2.19	Zugriffsrechte ansehen.....	30
4.3.2.20	Client zu OU hinzufügen	30
4.3.2.21	Gruppenrichtlinienobjekt erstellen (servergespeichertes Profil).....	31
4.3.2.22	Gruppenrichtlinienobjekt erstellen (Ordnerumleitung).....	33
5	Ergebnis	34

1 Aufgabenstellung

Als nächste Ausbaustufe unseres Domänennetzwerkes werden wir die Benutzerprofile zentral speichern. Dazu ist ein NAS vom Typ openmediavault in die Domäne zu integrieren.

- **Erste Schritte:**
OMV auf neuer virtueller Maschine aufsetzen und entweder als RAID1 oder RAID5 konfigurieren. Hostnamen passend wählen, Domänennamen angeben (auch wenn das noch nicht der Beitritt zur Domäne ist) und den Windows-DC als NTP-Zeitquelle definieren.
- **Domänenbeitritt:**
Recherche über benötigte Dienste, Einstellungen, Pakete (nicht vergessen: OMV basiert auf Debian) und entsprechende Installationen/Konfigurationen vornehmen.

2 Abstract (English)

As the next expansion stage of our domain network, we will store the user profiles centrally. A NAS of the type openmediavault is to be integrated into the domain for this purpose.

- **First steps:**
Set up OMV on a new virtual machine and configure it as either RAID1 or RAID5. Select a suitable host name, enter the domain name (even if this is not yet the domain join) and define the Windows DC as the NTP time source.
- **Join the domain:**
Research required services, settings, packages (don't forget: OMV is based on Debian) and carry out appropriate installations/configurations.

3 Theoretische Grundlagen

Im Internet findet man zwei Hauptmöglichkeiten, wie man einen UNIX Computer in eine Windows Domain integrieren kann: **Winbind** oder **SSSD**. Beide basieren auf dem SMB (Server Message Block) Protokoll.

Story Time kann übersprungen werden

In einigen Foren meinen Menschen, sie hätten total viele Probleme mit der einen Variante, jedoch ihr gesamtes Leben einen reibungslosen Verlauf mit der anderen gehabt. Im nächsten Forum behauptet ein User das genaue Gegenteil. Diese Argumente sind meist unbegründet, weil die User wahrscheinlich nicht endlos Fehler suchen wollten und zur anderen Variante gewechselt sind, verständlicherweise. Doch grundlos will ich nicht eine Variante verwenden, deswegen liste ich gleich jeweils die besonderen Merkmale von Winbind und SSSD auf.

Hier sind die wichtigsten Vorteile von Winbind und SSSD aufgelistet:

3.1 Winbind

Winbind ist ein Bestandteil von Samba, welches wiederum auf dem SMB-Protokoll basiert.

- Einfache Konfiguration: Im Gegensatz zu SSSD empfinden Administratoren das Integrieren eines UNIX-Servers in eine Windows Domain mithilfe von Winbind einfacher.
- PAM-Integration: Winbind unterstützt die Integration von verschiedenen Authentifizierungsmethoden mittels Pluggable Authentication Modules (PAM).
- Benutzer- und Gruppeninformationen: Wenn man Winbind verwendet, kann man Benutzer- und Gruppeninformationen direkt via Windows-Domain-System ansehen.

3.2 SSSD

SSSD ist eine eigenständige Software basierend auf dem SMB-Protokoll. Es ist ein Daemon, der verschiedene Identitäts- und Authentifizierungsdienste für Linux bereitstellt.

- Flexibilität und Skalierbarkeit: SSSD hat Vorteile gegenüber Winbind, wenn es um die Integration verschiedener Identitätsquellen geht. Zum Beispiel kann es auch mit Diensten wie LDAP (Lightweight Directory Access Protocol) arbeiten, um Benutzer- und Gruppeninformationen zentral zu speichern.
- Offline-Unterstützung: Dies ist wohl ein herausragendes Merkmal. SSSD kann einen Benutzer im AD anmelden, auch wenn keine Verbindung zu einem Domain Controller zur Verfügung steht.
- Leider unterstützt Samba kein SSSD mehr, was bedeutet, dass zum Beispiel servergespeicherte Benutzerprofile Winbind benötigen.

Für welche Art der Integration und Verwendung des SMB Protokolls Sie sich entscheiden, steht Ihnen offen. Egal, welche Identitätsintegration Sie bei der virtuellen NAS Maschine verwenden, Sie benötigen auch noch die Möglichkeit, diese Maschine in der Windows Domain zu authentifizieren. Diese Aufgabe übernimmt **Kerberos**.

3.3 Kerberos

Kerberos ist ein Netzwerkauthentifizierungsprotokoll, das für die sichere Überprüfung der Identität von Benutzern in verteilten Computernetzwerken entwickelt wurde. Das grundlegende Ziel von Kerberos besteht darin, einen vertrauenswürdigen Mechanismus bereitzustellen, mit dem sich Benutzer gegenüber verschiedenen Netzwerkdiensten authentifizieren können, ohne ihre Anmeldeinformationen ständig offenlegen zu müssen.

3.3.1 Tickets

Die Kernidee von Kerberos beruht auf der Verwendung von verschlüsselten Tickets für die Authentifizierung. Der Schlüsselverteilungsdienst (KDC) spielt dabei eine zentrale Rolle. Wenn ein Benutzer sich erfolgreich gegenüber dem KDC authentifiziert, erhält er ein sogenanntes Ticket-Granting Ticket (TGT). Dieses TGT dient als "Eintrittskarte" für den Benutzer, um zusätzliche Service Tickets vom Ticket-Granting Server (TGS) zu erhalten.

Die Tickets sind verschlüsselt und enthalten Informationen wie die Benutzeridentität, die Gültigkeitsdauer des Tickets und einen geheimen Sitzungsschlüssel. Der geheime Sitzungsschlüssel ermöglicht es dem Benutzer, sicher mit verschiedenen Diensten im Netzwerk zu kommunizieren, ohne sensible Informationen wie Passwörter offenlegen zu müssen.

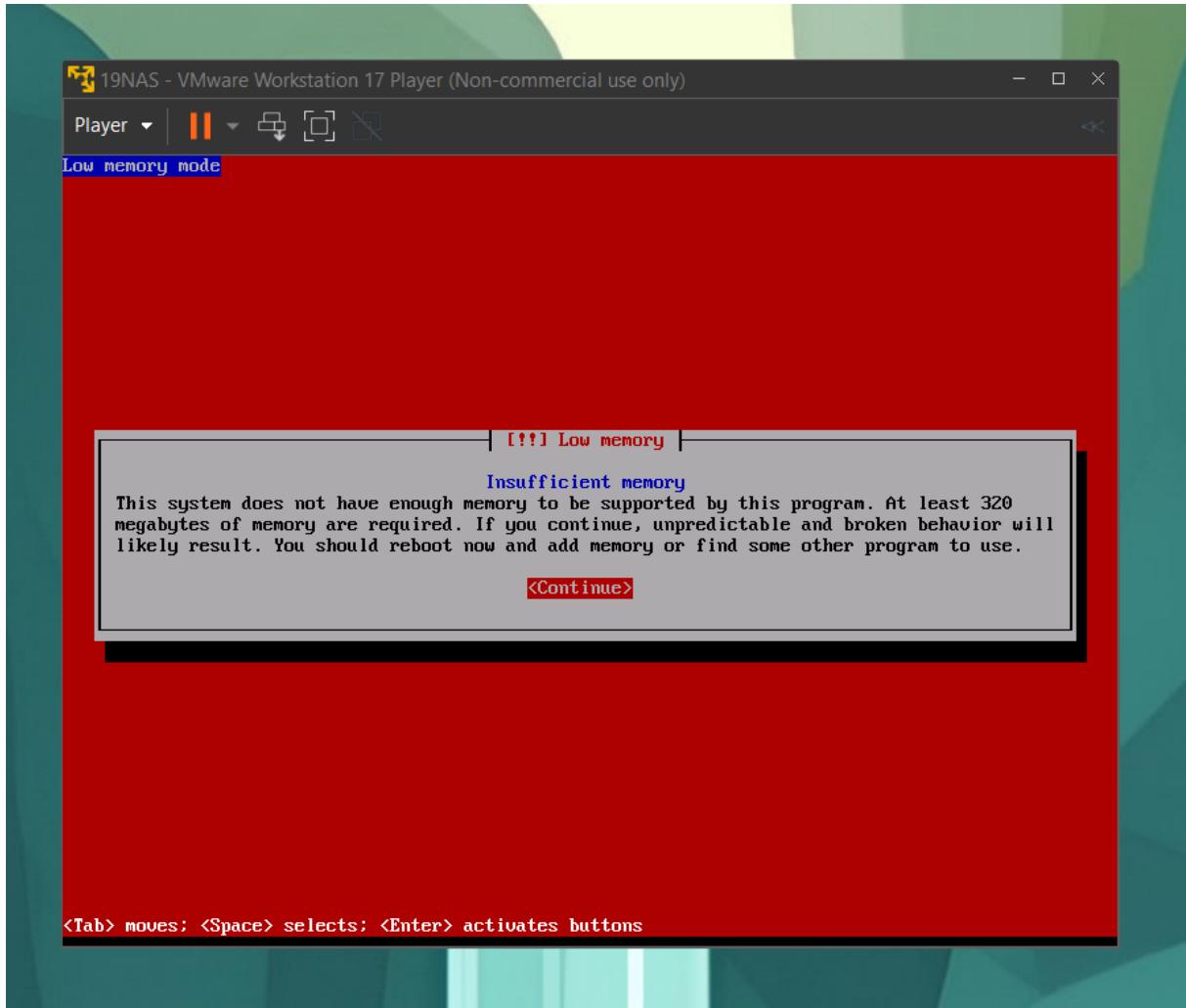
Die Gültigkeitsdauer der Tickets begrenzt das Risiko von Sicherheitsbedrohungen, da selbst im Falle einer Kompromittierung eines Tickets, die Zeit für einen Angreifer begrenzt ist. Kerberos setzt auf Zeitstempel, um sicherzustellen, dass Tickets nicht für unbegrenzte Zeit gültig sind.

Aus diesem Grund ist es auch wichtig, dass der Windows Server die gleiche Uhrzeit wie der NAS-Server hat. Solange dieses Zeitfenster innerhalb von fünf Minuten liegt, ist die Gültigkeit der Kerberos-Tickets gewährleistet.

4 Übungsdurchführung

4.1 Openmediavault aufsetzen

Laden Sie sich die neustes ISO von openmediavault.org herunter und erstellen Sie eine virtuelle Maschine, welche die Mindestanforderungen erfüllt (RAM, Storage, ...). Wenn Sie diese Error Message erhalten, wissen Sie, dass Sie zu wenig RAM vergeben haben und sollten dies in den Einstellungen nochmals ändern.

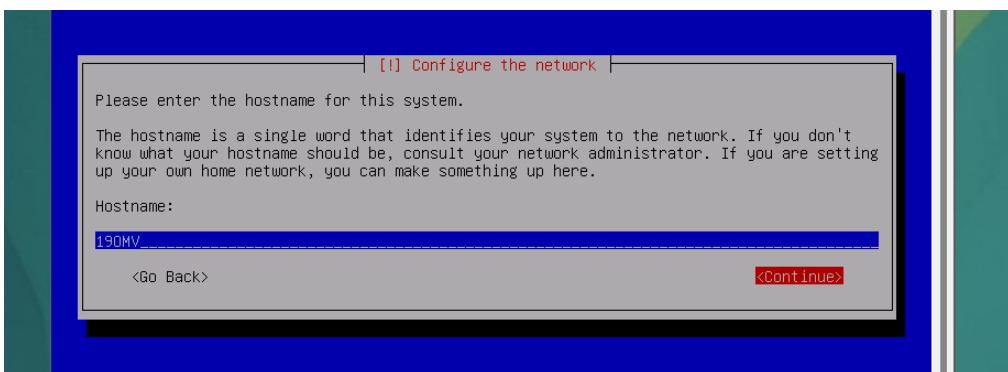


(Okay, zugegebenermaßen ist es nicht die beste Idee ein Protokoll direkt mit einer Fehlermeldung zu starten, jedoch finde ich das Dokumentieren der Fehler sehr nützlich.)

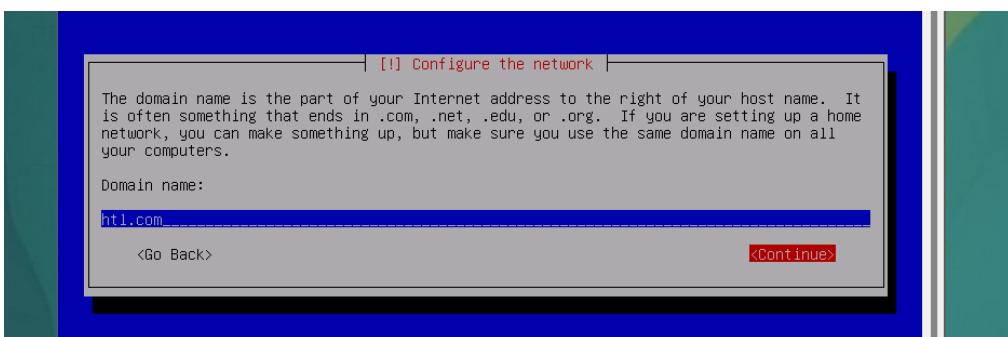
Konfigurieren Sie beim Installationsvorgang die virtuelle Maschine folgendermaßen:

- Vergeben Sie einen sinnvollen Hostnamen. Ich habe mich für `190MV` entschieden.

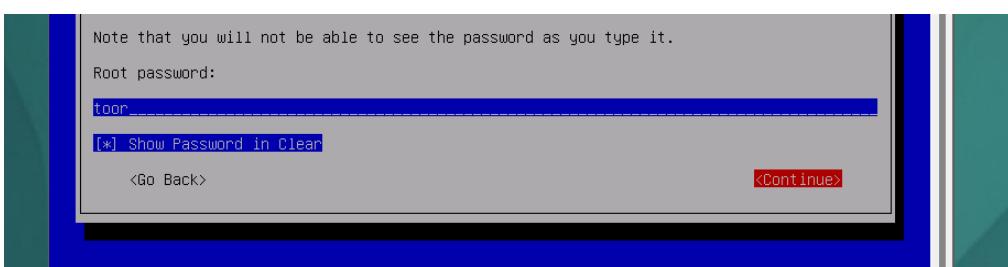
Diesen können Sie später auch noch auf einfache Art ändern. Verwenden Sie dazu den Befehl `hostnamectl set-hostname <neuer-hostname>` und ändern Sie den Hostnamen auch in der Datei `/etc/hosts`.



- Damit später die Domainenintegration einfach ist, können Sie außerdem auch schon den Domainnamen angeben. Damit wird jedoch leider nicht automatisch die virtuelle Maschine der Domain hinzugefügt. In meinem Fall lautet der Name der Domain `ht1.com`.



- Konfigurieren Sie das root-Password, wie Sie es hier sehen können. Ich habe mich für `toor` entschieden.



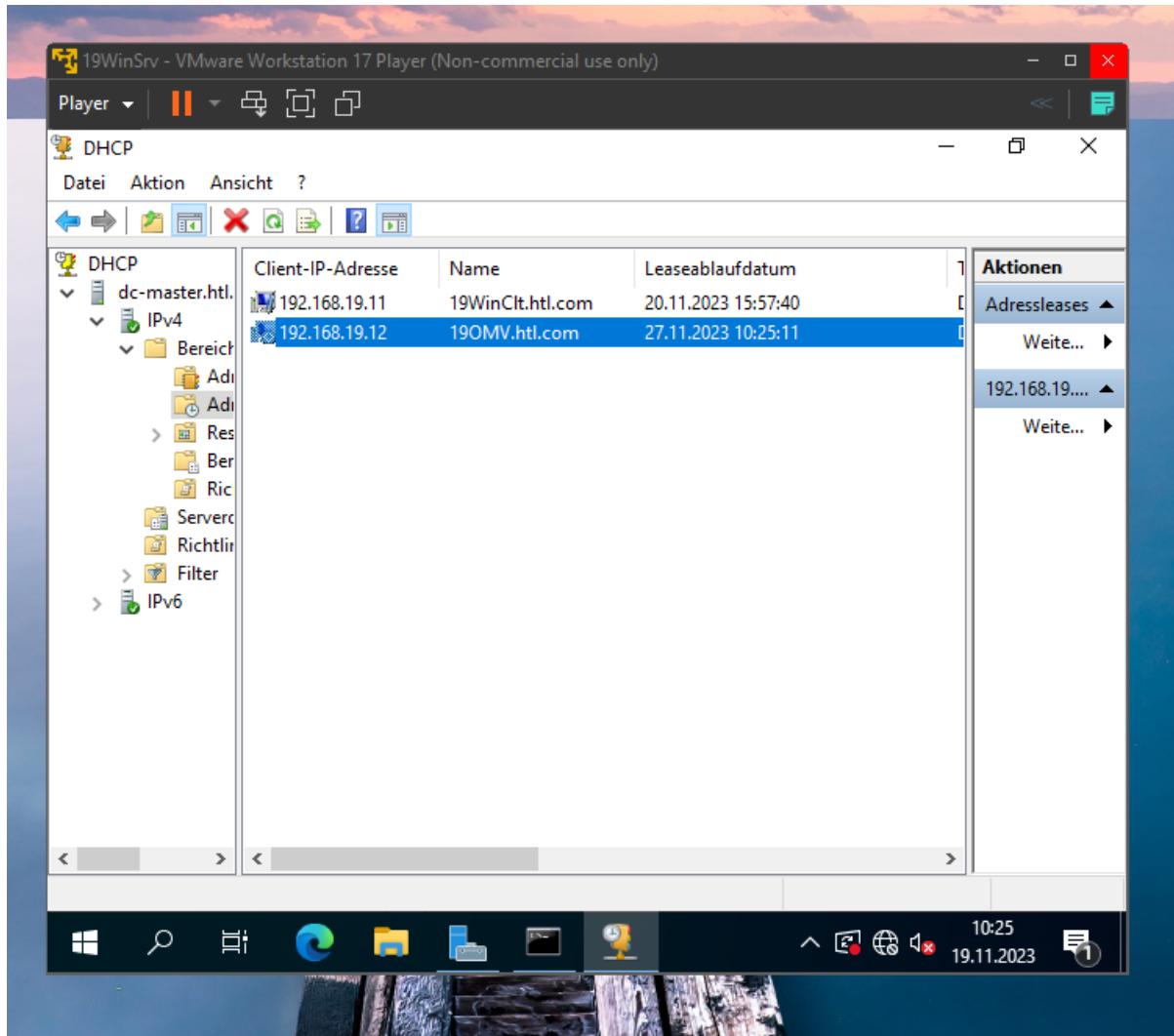
- Sobald die Installation fertig ist und der virtuelle Computer neu startet, werfen Sie die virtuelle CD mittels Mausklicks virtuell aus und führen die virtuelle Maschine erneuert aus.

Voila, Sie haben OMV fertig konfiguriert!

4.2 Weboberfläche

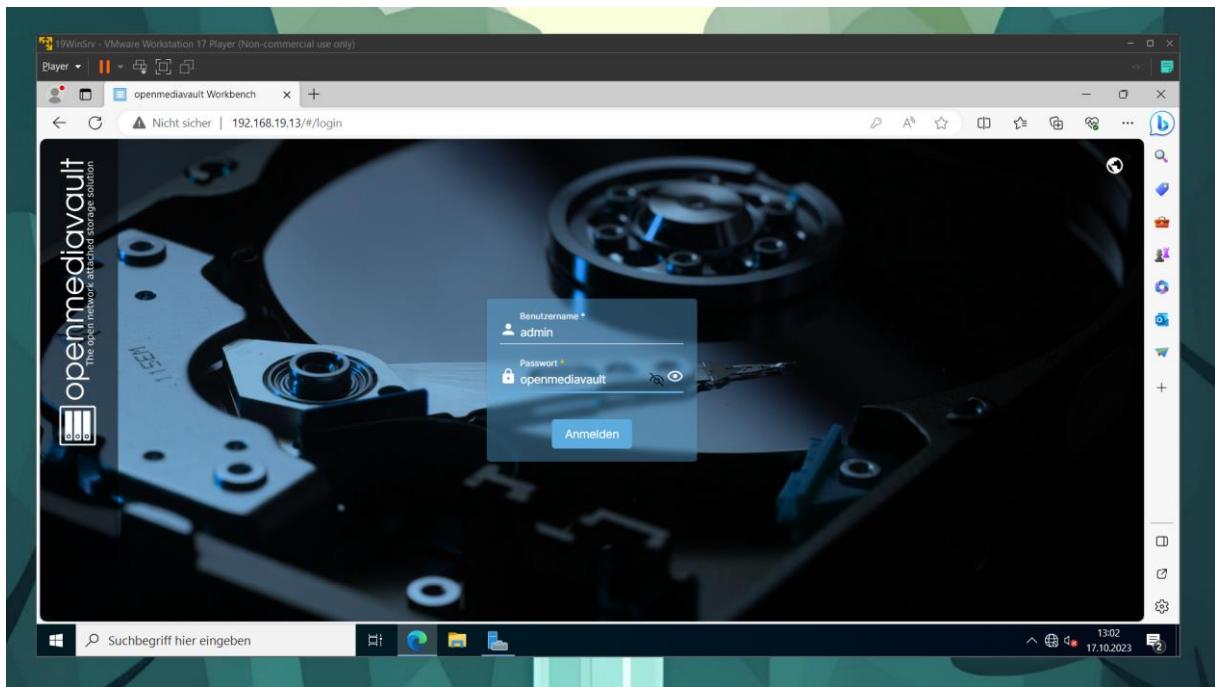
Damit OMV vom Windows DHCP Server eine IP-Adresse zugewiesen bekommt, führen Sie nach dem Hinzufügen der Netzwerkkarte (LAN) diese Befehle aus:

- `dhclient`: Holt sich vom DHCP Server eine IP-Adresse.
- `ip -c a`: Zeigt diese IP-Adresse an, damit Sie das **Webportal** aufrufen können.



Nach diesen beiden Schritten können Sie erstmals das Webportal aufrufen

- Benutzername: `admin`
- Password: `openmediavault`

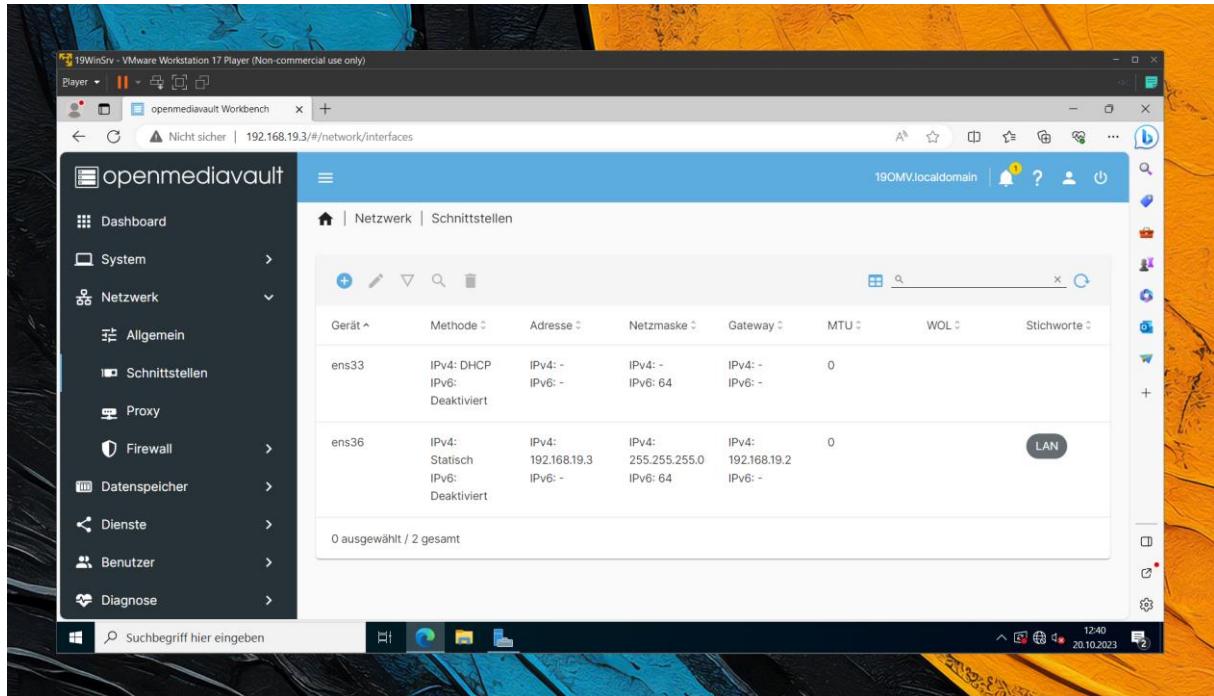


In den folgenden Schritten werden wir alle Einstellungen im Webportal vornehmen und anschließend zur Shell bei der virtuellen Maschine mit OMV zurückkehren, da das Beitreten zur Domain leider nicht über das Webportal möglich ist (obwohl genau dieses Feature in der Praxis wahrscheinlich am häufigsten zum Einsatz kommt...).

4.2.1 IP-Adresse konfigurieren

Als erstes müssen Sie die IPv4-Adresse entweder in der Shell direkt bei OMV oder in der GUI konfigurieren. Führen Sie bei Variante zwei alle Schritte von [dhclient](#) nach einem Neustart durch, gehen Sie beim Windows Server im Browser auf die IPv4-Adresse, welche Sie sich vorhin ausgeben haben lassen, und geben Sie die Anmeldedaten ein. (Anmeldedaten finde Sie unter [Weboberfläche](#))

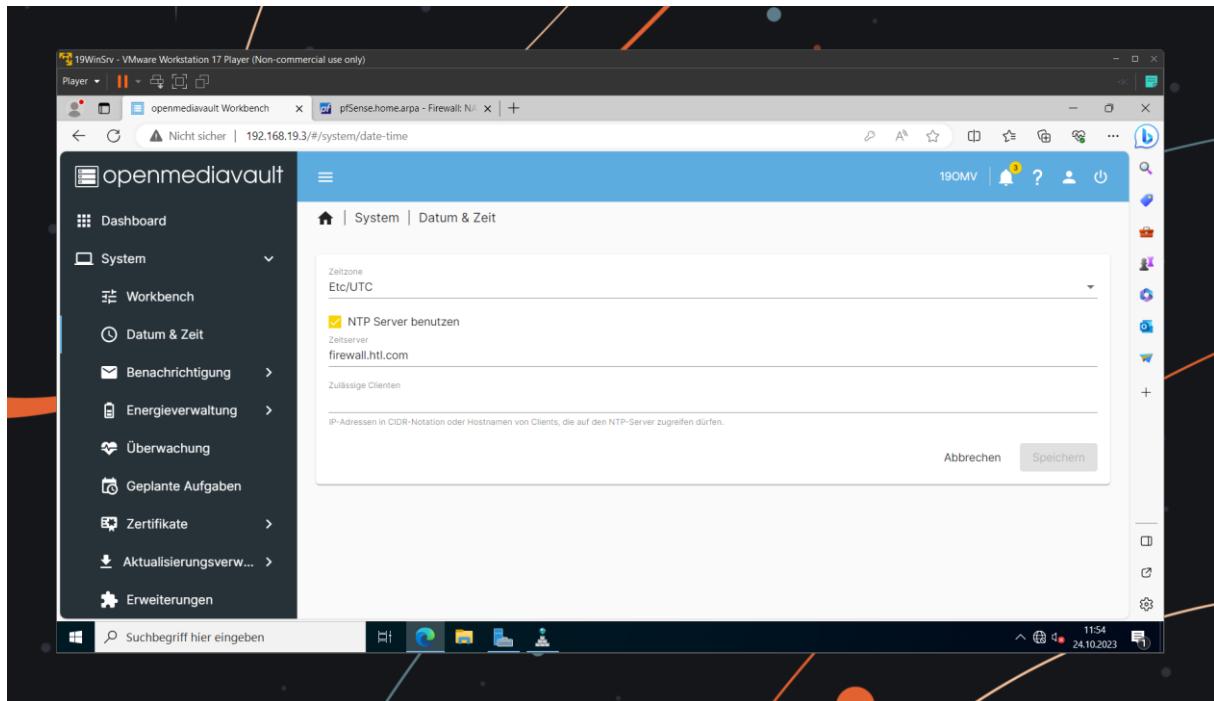
Unter „Netzwerk → Schnittstellen“ können Sie nun eine neue „Ethernet“-Schnittstelle einfügen und statisch fürs LAN konfigurieren, wie man es hier sieht:



```
Creating directory '/home/f.schneider@htl.com'.
f.schneider@190MV:~$ date
So 19 Nov 2023 16:48:34 CET
f.schneider@190MV:~$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:28:75:f2 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.11.135/24 brd 192.168.11.255 scope global dynamic ens33
        valid_lft 1733sec preferred_lft 1733sec
    inet 192.168.11.136/24 brd 192.168.11.255 scope global secondary dynamic ens33
        valid_lft 999sec preferred_lft 999sec
    inet6 fe80::20c:29ff:fe28:75f2/64 scope link
        valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:28:75:fc brd ff:ff:ff:ff:ff:ff
    altname enp2s4
    inet 192.168.19.3/24 brd 192.168.19.255 scope global ens36
        valid_lft forever preferred_lft forever
f.schneider@190MV:~$ _
```

4.2.2 NTP konfigurieren

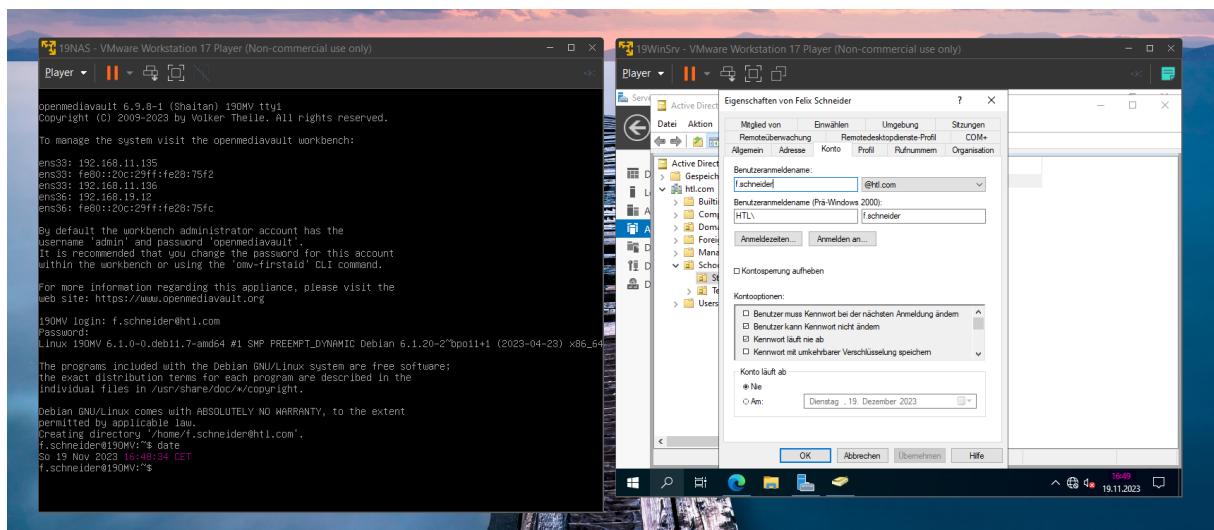
Damit das NAS die richtige Zeit bekommt, stellen wir bei Openmediavault den DC als Zeitserver ein. Weil unser DC der Erste in der Gesamtstruktur ist, und aus diesem Grund über alle 5 FSMO Rollen verfügt – PDC-Emulator inkludiert –, fungiert er automatisch als NTP Server.



Tragen Sie als Zeitserver entweder die Firewall firewall.htl.com oder den Windows Server dc-master.htl.com ein.

Wie man sehen kann, haben die beiden Maschinen somit eine (fast perfekt) synchronisierte Zeit (im unteren Screenshot rosa markiert).

```
C:\Users\Administrator>w32tm /tz
Zeitzone: Aktuell:TIME_ZONE_ID_STANDARD Bias: -60 Min. (UTC=Ortszeit+Bias)
[Standardname:"Mitteleuropäische Zeit" Bias:0 Min. Datum:(M:10 T:5 DoW:0)]
[Sommerzeitname:"Mitteleuropäische Sommerzeit" Bias:-60 Min. Datum:(M:3 T:5 DoW:0)]
```



4.3 OVM Domainbeitritt

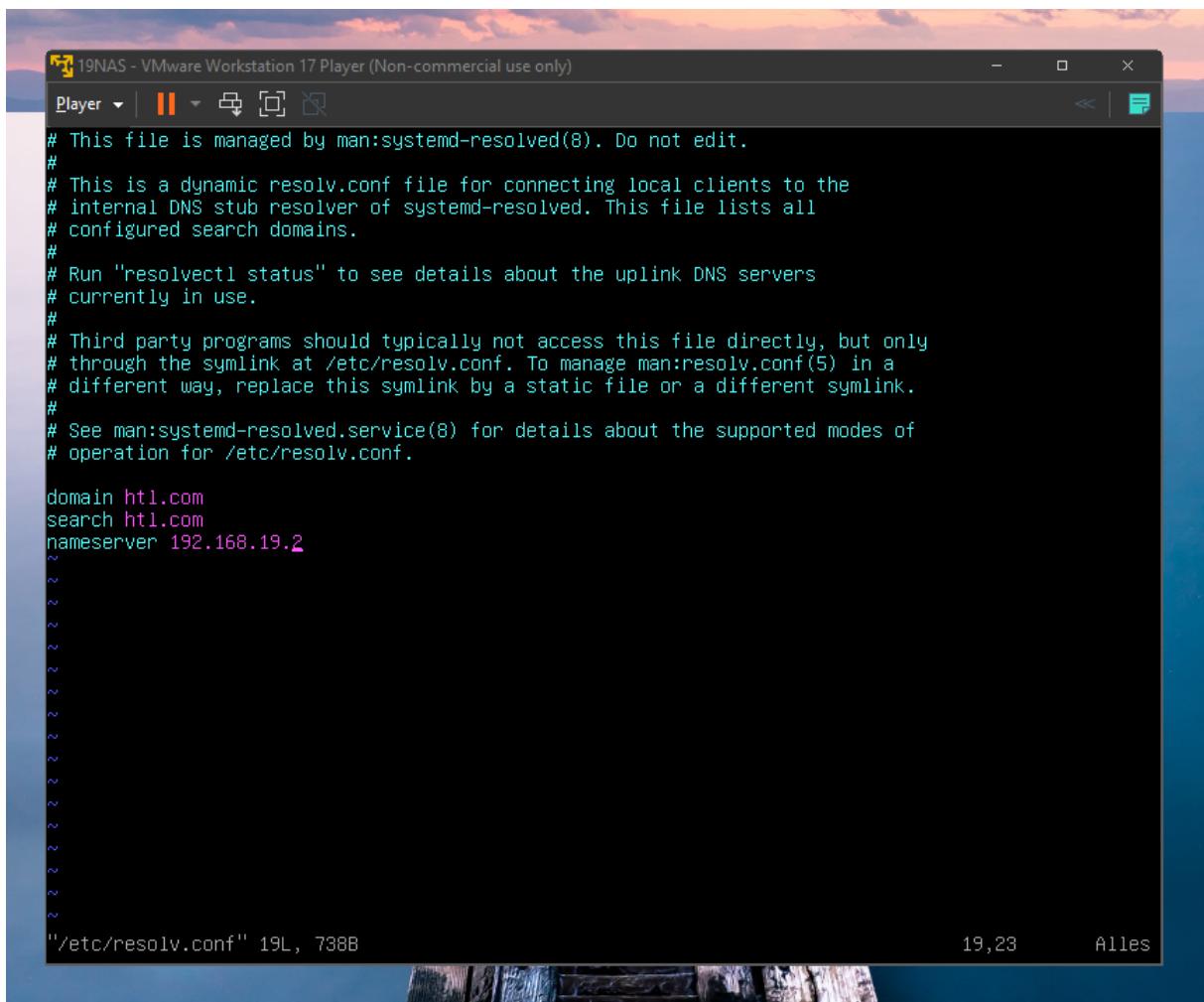
4.3.1 mit SSSD

Wir verwenden in diesem Protokoll SSSD, um der Domain beizutreten. Dazu halten wir uns an dieses Tutorial: https://www.server-world.info/en/note?os=Debian_11&p=realmd. Leider wird seit Samba 4.8.0 kein SSSD mehr Unterstützt, wie man [hier](#) nachlesen kann.

```
Domain member setups require winbindd
-----
Setups with "security = domain" or "security = ads" require a
running 'winbindd' now. The fallback that smbd directly contacts
domain controllers is gone.
```

4.3.1.1 DNS Einstellungen zeigen auf AD

Stellen Sie in der Datei `/etc/resolv.conf` die Domain und den Nameserver richtig ein. Damit die Datei nicht bei jedem Reboot überschrieben wird, können Sie das Service `systemd-resolved` komplett deaktivieren, mittels: `systemctl disable --now systemd-resolved`.



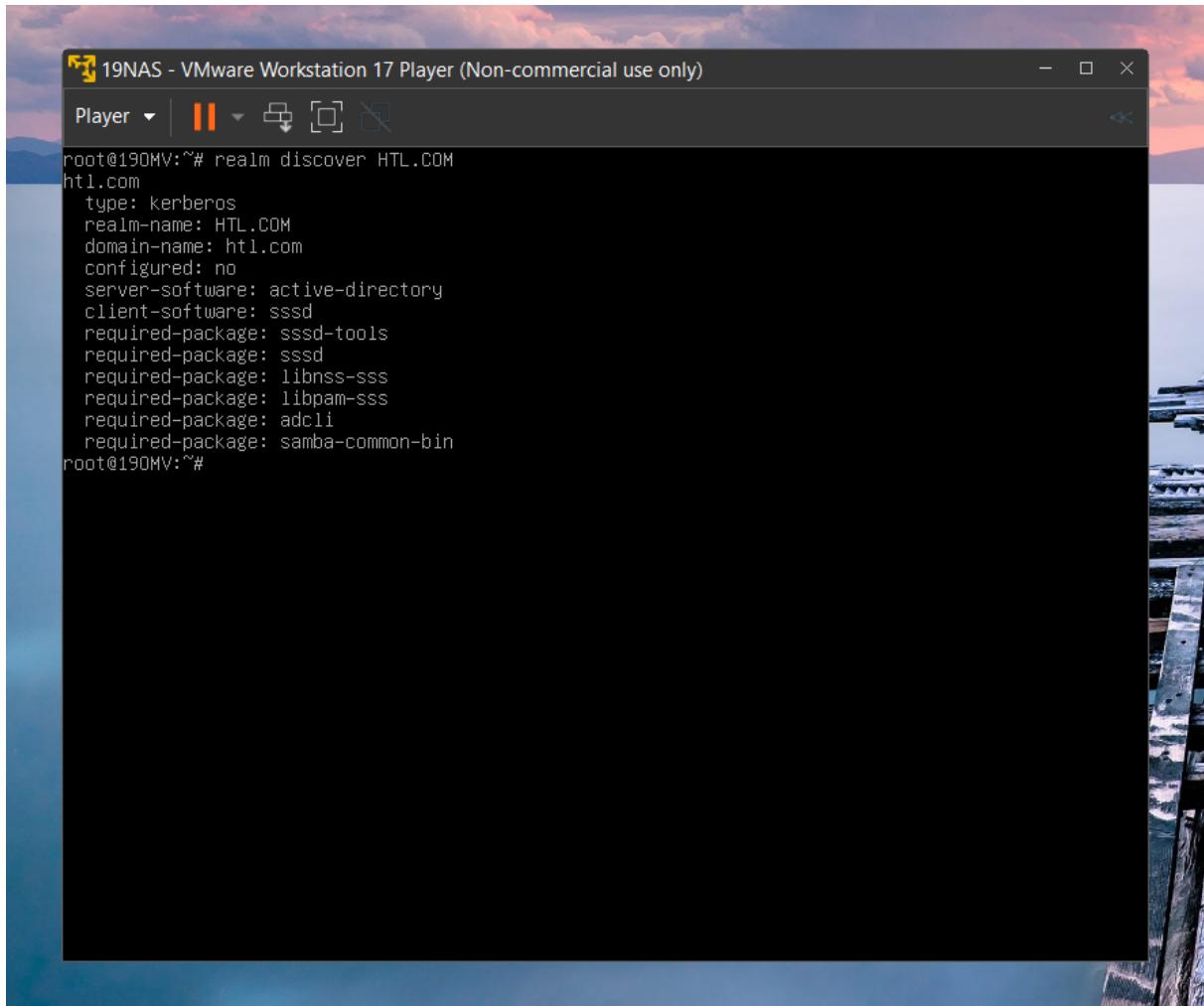
The screenshot shows a terminal window titled "19NAS - VMware Workstation 17 Player (Non-commercial use only)". The window contains the contents of the /etc/resolv.conf file. The file starts with a header indicating it is managed by systemd-resolved, followed by a list of search domains and a nameserver entry. The terminal window has a dark background with light-colored text. The bottom status bar shows the file path "/etc/resolv.conf", the line count "19L", the byte count "738B", the cursor position "19,23", and the word "Alles".

```
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

domain ht1.com
search ht1.com
nameserver 192.168.19.2
~
```

4.3.1.2 AD erkunden

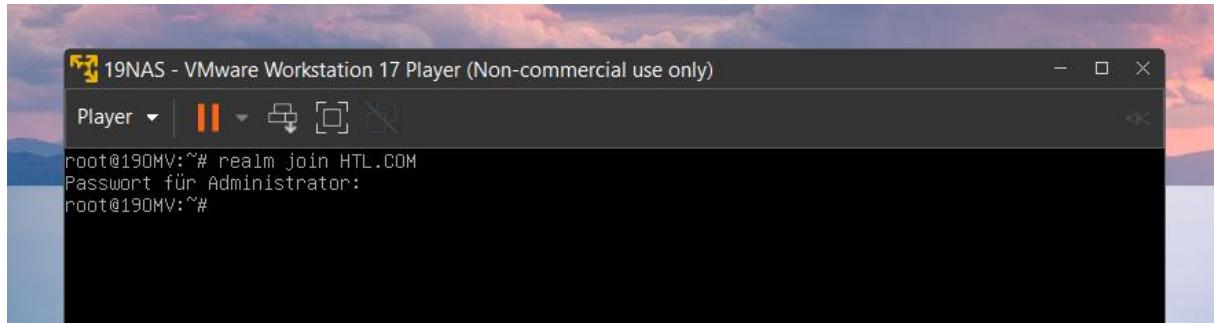
Damit das Kerberos Ticket im Hintergrund vom REALM automatisch konfiguriert wird, führen Sie den Befehl `realm discover HTL.COM` aus. Wenn alles richtig funktioniert hat bis jetzt, sollten Sie folgenden Output erhalten:



```
root@190MV:~# realm discover HTL.COM
htl.com
type: kerberos
realm-name: HTL.COM
domain-name: htl.com
configured: no
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin
root@190MV:~#
```

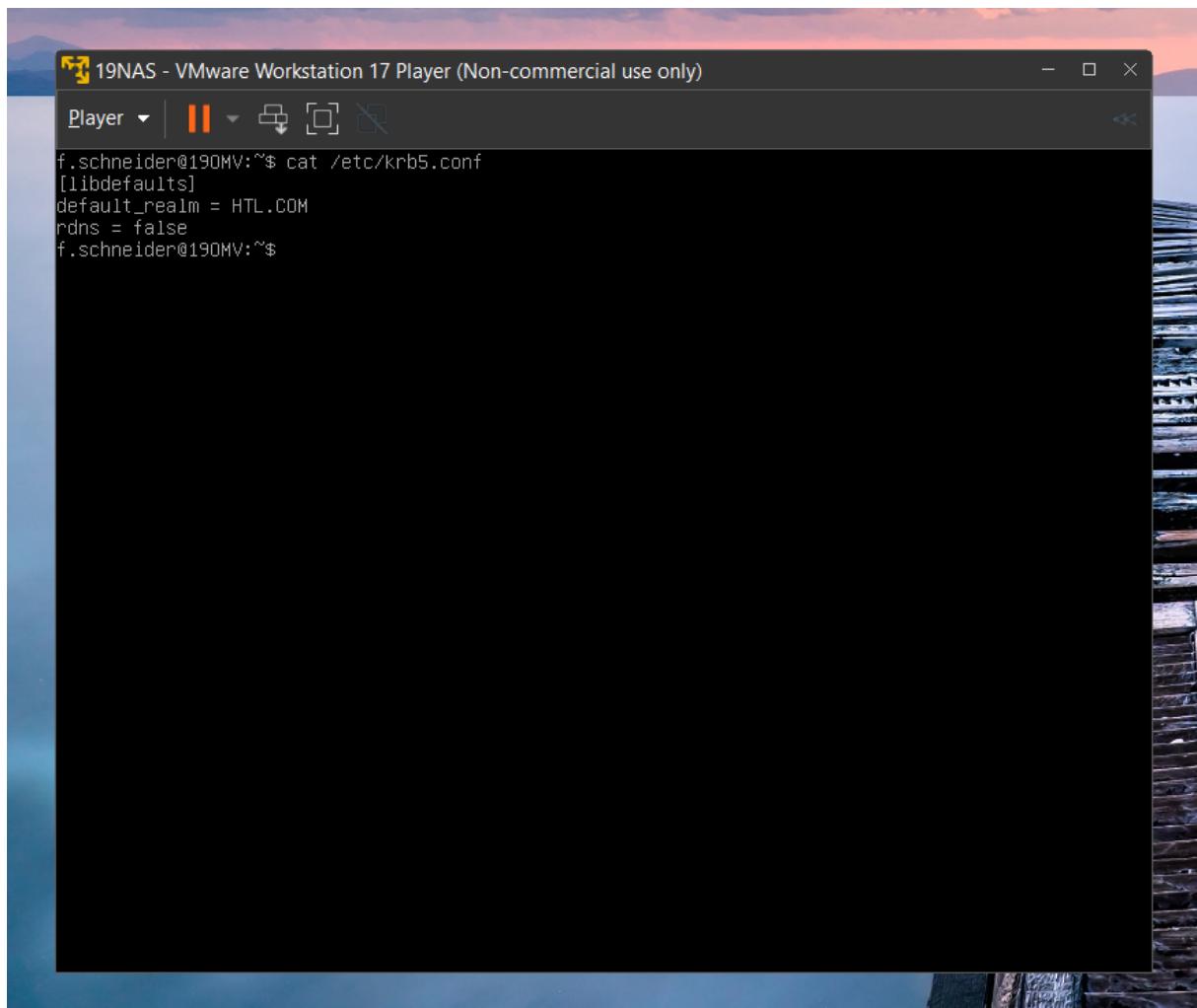
4.3.1.2.1 AD beitreten

Nun kommt endlich der Moment, wo die NAS-Maschine dem AD beitreten kann. Überprüfen Sie zuerst, ob Kerberos richtig konfiguriert wurde von REALM (bei mir wurde nichts konfiguriert, deswegen habe ich es manuell konfiguriert) und führen Sie anschließend diesen Befehl aus: `realm join HTL.COM`.



```
Player ▾ | II ▾ [ ] [ ] [ ] [ ]  
root@190MV:~# realm join HTL.COM  
Passwort für Administrator:  
root@190MV:~#
```

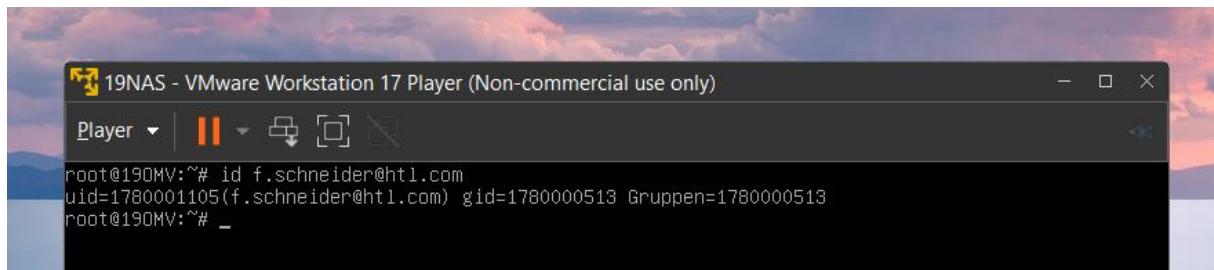
Falls Sie auch auf das Problem stoßen, dass die Maschine zu wenige Berechtigungen (`insufficient permissions`) haben sollte, fügen Sie zumindest diese Konfiguration in `/etc/krb5.conf` ein:



```
Player ▾ | II ▾ [ ] [ ] [ ] [ ]  
f.schneider@190MV:~$ cat /etc/krb5.conf  
[libdefaults]  
default_realm = HTL.COM  
rdns = false  
f.schneider@190MV:~$
```

4.3.1.3 Informationen eines AD Nutzers abfragen

Um auszuprobieren, ob Sie Informationen eines AD Nutzers bekommen können, führen Sie folgenden Befehl aus: `id f.schneider@htl.com`.



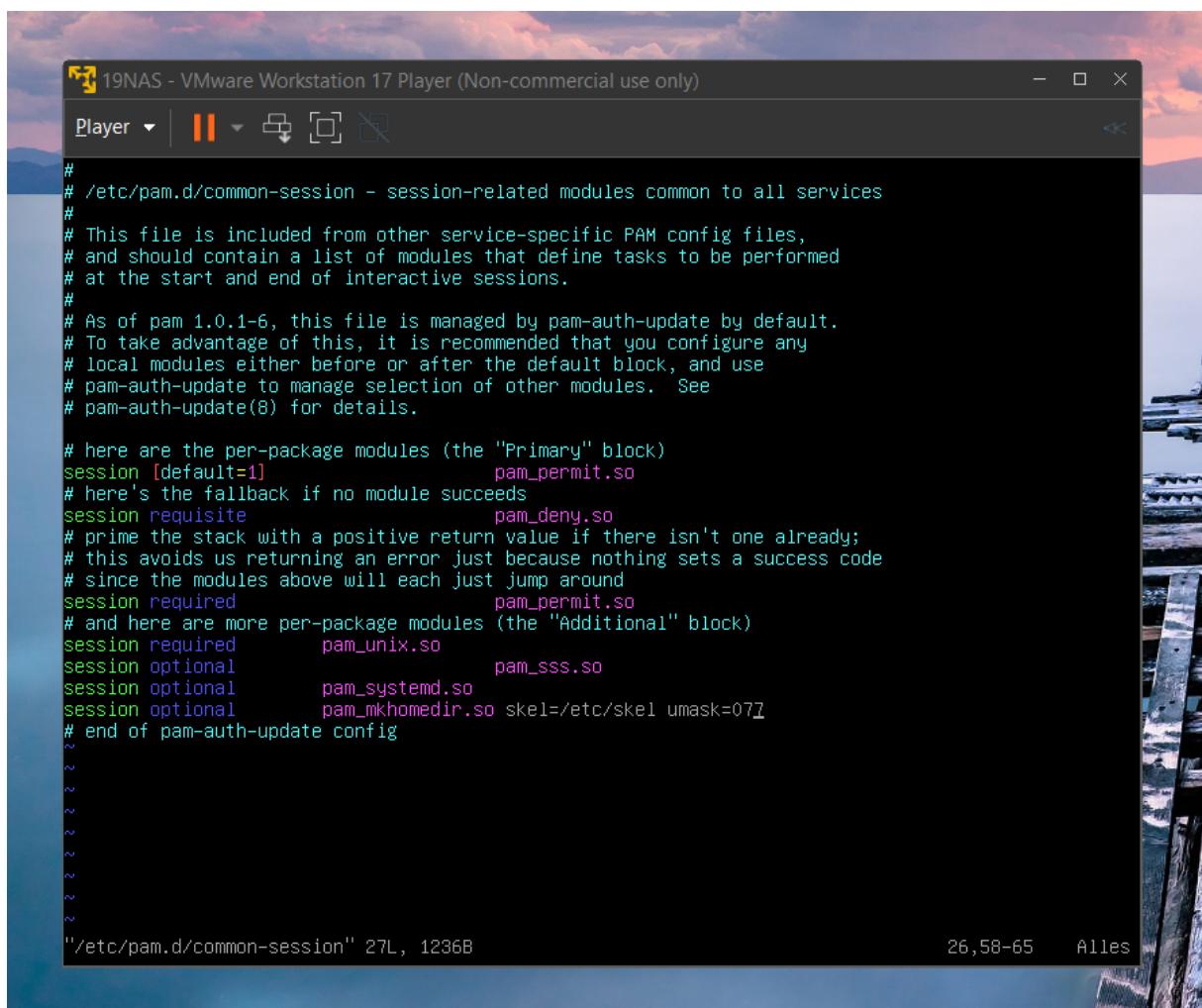
```
root@190MV:~# id f.schneider@htl.com
uid=1780001105(f.schneider@htl.com) gid=1780000513 Gruppen=1780000513
root@190MV:~# _
```

4.3.1.4 Automatisch einen Ordner erstellen (optional)

Sie können auch konfigurieren, dass bei einer Anmeldung mit einem AD Nutzer automatisch ein Ordner erstellt werden soll. Dies können Sie bewerkstelligen, indem folgende Zeile in `/etc/pam.d/common-session` hinzufügen.

```
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

(Schade, dass die Berechtigungen nicht 007 sind... 😊)



```
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

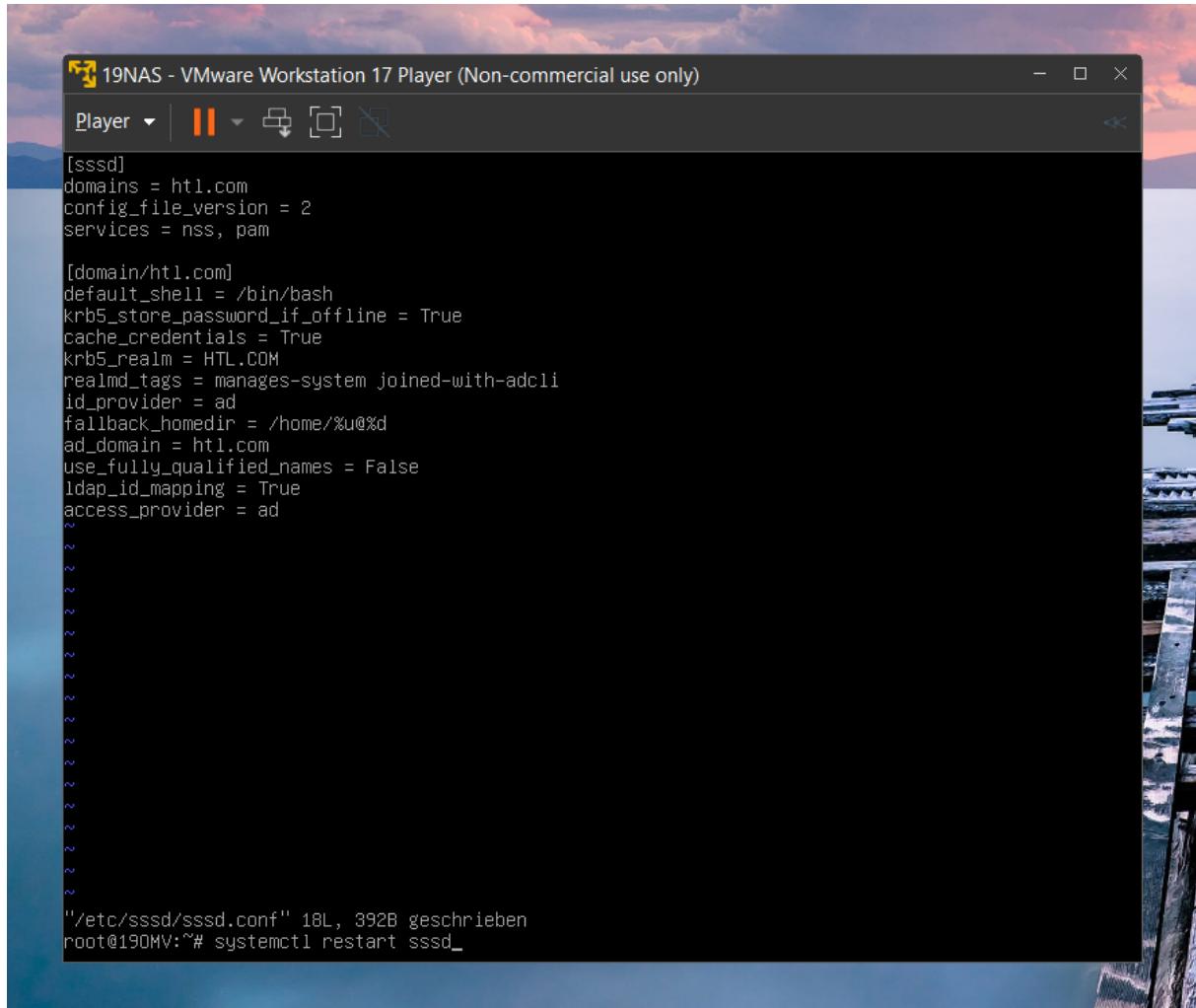
# here are the per-package modules (the "Primary" block)
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
session requisite           pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required             pam_permit.so
# and here are more per-package modules (the "Additional" block)
session required             pam_unix.so
session optional              pam_sss.so
session optional              pam_systemd.so
session optional              pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
~

"/etc/pam.d/common-session" 27L, 1236B
```

26,58-65 Alles

4.3.1.5 Automatischer Domain Name

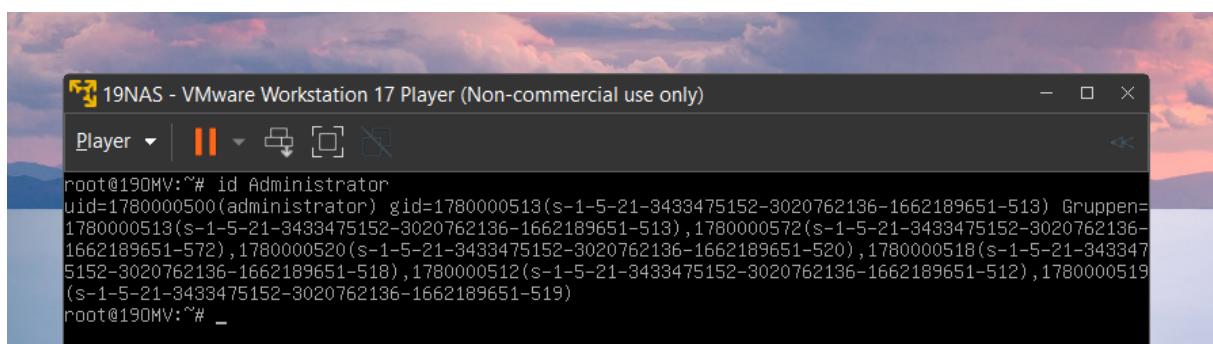
Meistens wollen Sie nicht immer @htl.com schreiben müssen, wenn Sie sich anmelden oder Informationen von Nutzern erhalten wollen. Damit Sie dies nicht machen müssen, gibt es die Option `use_fully_qualified_names = False` in `/etc/sssd/sssd.conf`. Stellen Sie dies ein, wenn Sie möchten:



```
[sssd]
domains = htl.com
config_file_version = 2
services = nss, pam

[domain/htl.com]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = HTL.COM
realm_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = htl.com
use_fully_qualified_names = False
ldap_id_mapping = True
access_provider = ad
~

"/etc/sssd/sssd.conf" 18L, 392B geschrieben
root@190MV:~# systemctl restart sssd
```



```
root@190MV:~# id Administrator
uid=1780000500(administrator) gid=1780000513(s-1-5-21-3433475152-3020762136-1662189651-518) Gruppen=
1780000513(s-1-5-21-3433475152-3020762136-1662189651-518),1780000572(s-1-5-21-3433475152-3020762136-
1662189651-572),1780000520(s-1-5-21-3433475152-3020762136-1662189651-520),1780000518(s-1-5-21-343347
5152-3020762136-1662189651-518),1780000512(s-1-5-21-3433475152-3020762136-1662189651-512),1780000519
(s-1-5-21-3433475152-3020762136-1662189651-519)
root@190MV:~# _
```

4.3.1.6 Anmeldung

Nun können Sie noch viele weitere Einstellungen konfigurieren. Je nachdem, was Sie alles möchten.

Außerdem können Sie sich nun mittels AD Nutzer am NAS anmelden, wie Sie hier sehen können:

```
19NAS - VMware Workstation 17 Player (Non-commercial use only)
Player | || □ □ X

openmediavault 6.9.8-1 (Shaitan) 190MV tty1
Copyright (C) 2009-2023 by Volker Theile. All rights reserved.

To manage the system visit the openmediavault workbench:

ens33: 192.168.11.135
ens33: fe80::20c:29ff:fe28:75f2
ens33: 192.168.11.136
ens36: 192.168.19.12
ens36: fe80::20c:29ff:fe28:75fc

By default the workbench administrator account has the
username 'admin' and password 'openmediavault'.
It is recommended that you change the password for this account
within the workbench or using the 'omv-firstaid' CLI command.

For more information regarding this appliance, please visit the
web site: https://www.openmediavault.org

190MV login: f.schneider@htl.com
Password:
Linux 190MV 6.1.0-0.deb11.7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-2~bpo11+1 (2023-04-23) x86_64

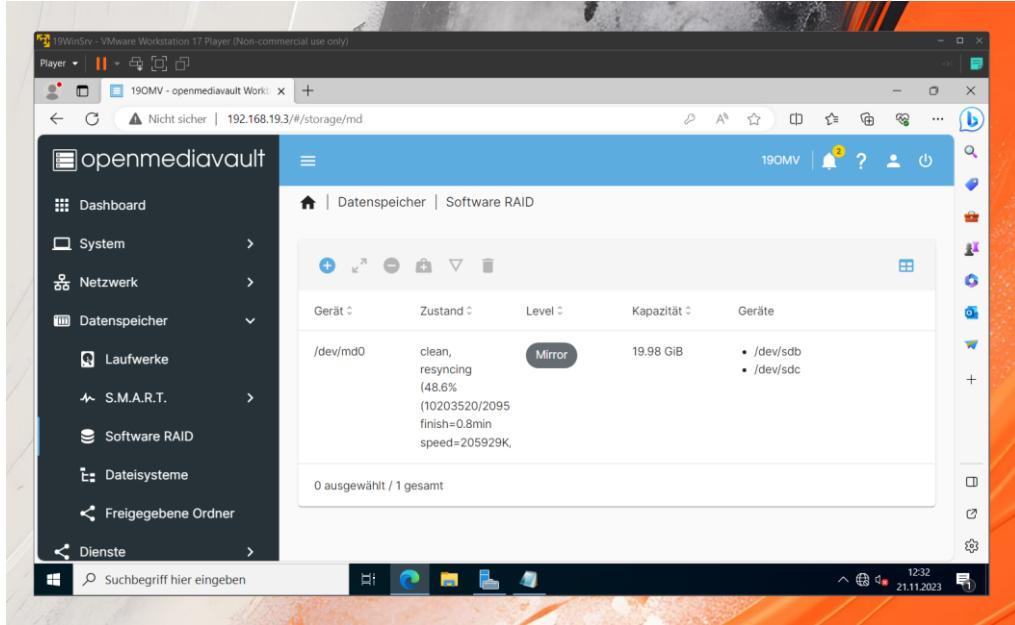
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/f.schneider@htl.com'.
f.schneider@190MV:~$ _
```

Wenn Sie genau hinsehen, kann man sogar die Zeile `Creating directory `/home/f.schneider@htl.com`` entdecken, wie wir es vorher konfiguriert haben.

4.3.1.7 RAID

Sie können zusätzlich auch noch ein RAID 1 oder RAID 5 oder RAID 10 oder sonst was konfigurieren:



4.3.1.8 Benutzerübersicht

Damit man die Benutzer in der Weboberfläche aufgelistet werden, muss die Datei `/etc/sssd/sssd.conf` richtig konfiguriert werden.

```
[sssd]
domains = htl.com
config_file_version = 2
services = nss, pam

[domain/htl.com]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = HTL.COM
realm_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = htl.com
use_fully_qualified_names = True
ldap_id_mapping = True
access_provider = ad
ad_gpo_access_control = permissive
enumerate = True

/etc/sssd/sssd.conf" 20L, 443B
```


4.3.2 mit Winbind

4.3.2.1 Open Tutorial

Wir folgen diesem Tutorial https://www.server-world.info/en/note?os=Debian_11&p=samba&f=4 für die ersten Schritte.

4.3.2.2 Install packages

```
apt install krb5-user libpam-krb5 winbind samba smbclient libnss-winbind libpam-winbind samba-dsdb-modules samba-vfs-modules
```

4.3.2.3 Kerberos konfigurieren

Editieren Sie die Datei `/etc/krb5.conf` für Ihre Domain. Da meine Domain HTL.COM lautet, sieht meine Datei so aus:

```
[logging]
    default = FILE:/var/log/krb5.log

[libdefaults]
    ticket_lifetime = 24000
    clock_skew = 300
    default_realm = HTL.COM

[realms]
    EXAMPLE.COM = {
        kdc = htl.com
        admin_server = htl.com
        default_domain = HTL.COM
    }

[domain_realm]
    .htl.com = HTL.COM
    htl.com = HTL.COM
```

4.3.2.4 Kerberos Ticket holen

Holen Sie sich mittels `kinit` ein Kerberos-Ticket.

```
root@190MV:~# vim /etc/krb5.conf
root@190MV:~# kinit Administrator@HTL.COM
Password for Administrator@HTL.COM:
root@190MV:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@HTL.COM

Valid starting     Expires            Service principal
2023-12-13 10:18:28  2023-12-13 16:58:25  krbtgt/HTL.COM@HTL.COM
```

4.3.2.5 Samba konfigurieren

Konfigurieren Sie Samba in der Datei `/etc/samba/smb.conf`:

```
[global]
kerberos method = secrets and keytab
realm = HTL.COM
workgroup = HTL
security = ads
template shell = /bin/bash
winbind enum groups = Yes
winbind enum users = Yes
winbind separator =
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
~
```

4.3.2.6 Name Service Switch auf Winbind umstellen

Damit GNU Name Service Switch Winbind verwendet, müssen Sie in der Datei `/etc/nsswitch.conf` in zwei Zeilen `winbind` hinzufügen.

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference` and `info` packages installed, try:
# `info libc "Name Service Switch"` for information about this file.

passwd:      files systemd winbind
group:       files systemd winbind
shadow:      files
gshadow:     files

hosts:        files mdns4_minimal [NOTFOUND=return] resolve [!UNAVAIL=return] dns myhostname
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
~
```

4.3.2.7 Automatisch Home Verzeichnis erstellen

Sie können auch konfigurieren, dass bei einer Anmeldung mit einem AD Nutzer automatisch ein Ordner erstellt werden soll. Dies können Sie bewerkstelligen, indem folgende Zeile in `/etc/pam.d/common-session` hinzufügen.

```
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

```
#  
# /etc/pam.d/common-session - session-related modules common to all services  
#  
# This file is included from other service-specific PAM config files,  
# and should contain a list of modules that define tasks to be performed  
# at the start and end of interactive sessions.  
#  
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.  
# To take advantage of this, it is recommended that you configure any  
# local modules either before or after the default block, and use  
# pam-auth-update to manage selection of other modules. See  
# pam-auth-update(8) for details.  
  
# here are the per-package modules (the "Primary" block)  
session [default=1]          pam_permit.so  
# here's the fallback if no module succeeds  
session requisite           pam_deny.so  
# prime the stack with a positive return value if there isn't one already;  
# this avoids us returning an error just because nothing sets a success code  
# since the modules above will each just jump around  
session required             pam_permit.so  
# and here are more per-package modules (the "Additional" block)  
session optional              pam_krb5.so minimum_uid=1000  
session required              pam_unix.so  
session optional              pam_winbind.so  
session optional              pam_systemd.so  
session optional              pam_mkhomedir.so skel=/etc/skel umask=077  
# end of pam-auth-update config
```

4.3.2.8 ADS joinen

Joinen Sie so der Domain:

```
root@190MV:~# net ads join -U Administrator
Enter Administrator's password:
Using short domain name -- HTL
Joined '190MV' to dns domain 'htl.com'
DNS Update for 190mv.htl.com failed: ERROR_DNS_UPDATE_FAILED
DNS update failed: NT_STATUS_UNSUCCESSFUL
root@190MV:~# systemctl restart winbind
root@190MV:~# net ads info
LDAP server: 192.168.11.134
LDAP server name: dc-master.htl.com
Realm: HTL.COM
Bind Path: dc=HTL,dc=COM
LDAP port: 389
Server time: Mi, 13 Dez 2023 10:53:07 CET
KDC server: 192.168.11.134
Server time offset: -1
Last machine account password change: Mi, 13 Dez 2023 10:50:58 CET
root@190MV:~# |
```

Wie man sehen kann, kann 190mv nicht automatisch seinen eigenen DNS-Record hinzufügen. Das ist jedoch nicht schlimm.

4.3.2.9 User Infos

Mit Befehlen, wie `wbinfo -u` oder `getent passwd` können Sie sich Informationen bezüglich der Benutzer der AD holen.

```
root@190MV:~# wbinfo -u
administrator
gast
trueberryless
krbtgt
a.mestl
f.schneider
root@190MV:~# |
```

```
root@190MV:~# getent passwd | grep HTL
HTL-administrator:*:2000500:2000513::/home/HTL/administrator:/bin/bash
HTL-gast:*:2000501:2000513::/home/HTL/gast:/bin/bash
HTL-trueberryless:*:2001000:2000513::/home/HTL/trueberryless:/bin/bash
HTL-krbtgt:*:2000502:2000513::/home/HTL/krbtgt:/bin/bash
HTL-a.mestl:*:2001104:2000513::/home/HTL/a.mestl:/bin/bash
HTL-f.schneider:*:2001105:2000513::/home/HTL/f.schneider:/bin/bash
root@190MV:~# |
```

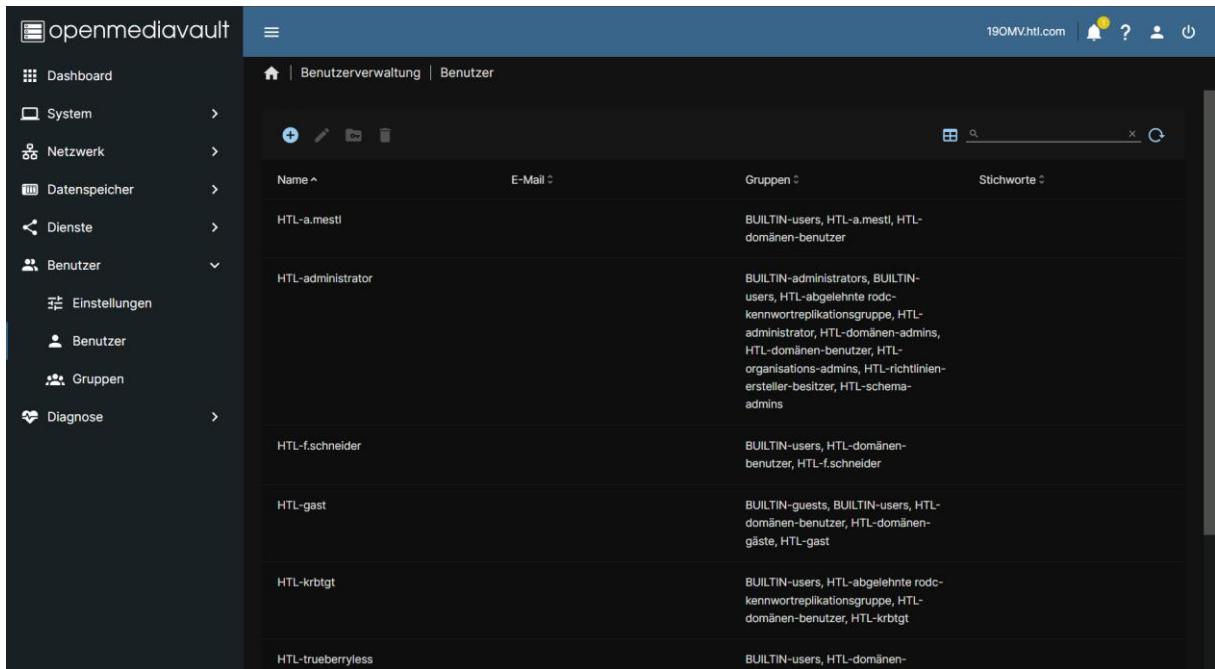
4.3.2.10 User Web

Damit die User in der Web Applikation von OMV angezeigt werden, muss zuerst noch in `/etc/login.defs` der MAX Wert der UID und GID höhergestellt werden:

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN          1000
UID_MAX         99999999999999
# System accounts
#SYS_UID_MIN      100
#SYS_UID_MAX      999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN          1000
GID_MAX         99999999999999
# System accounts
#SYS_GID_MIN      100
#SYS_GID_MAX      999
```

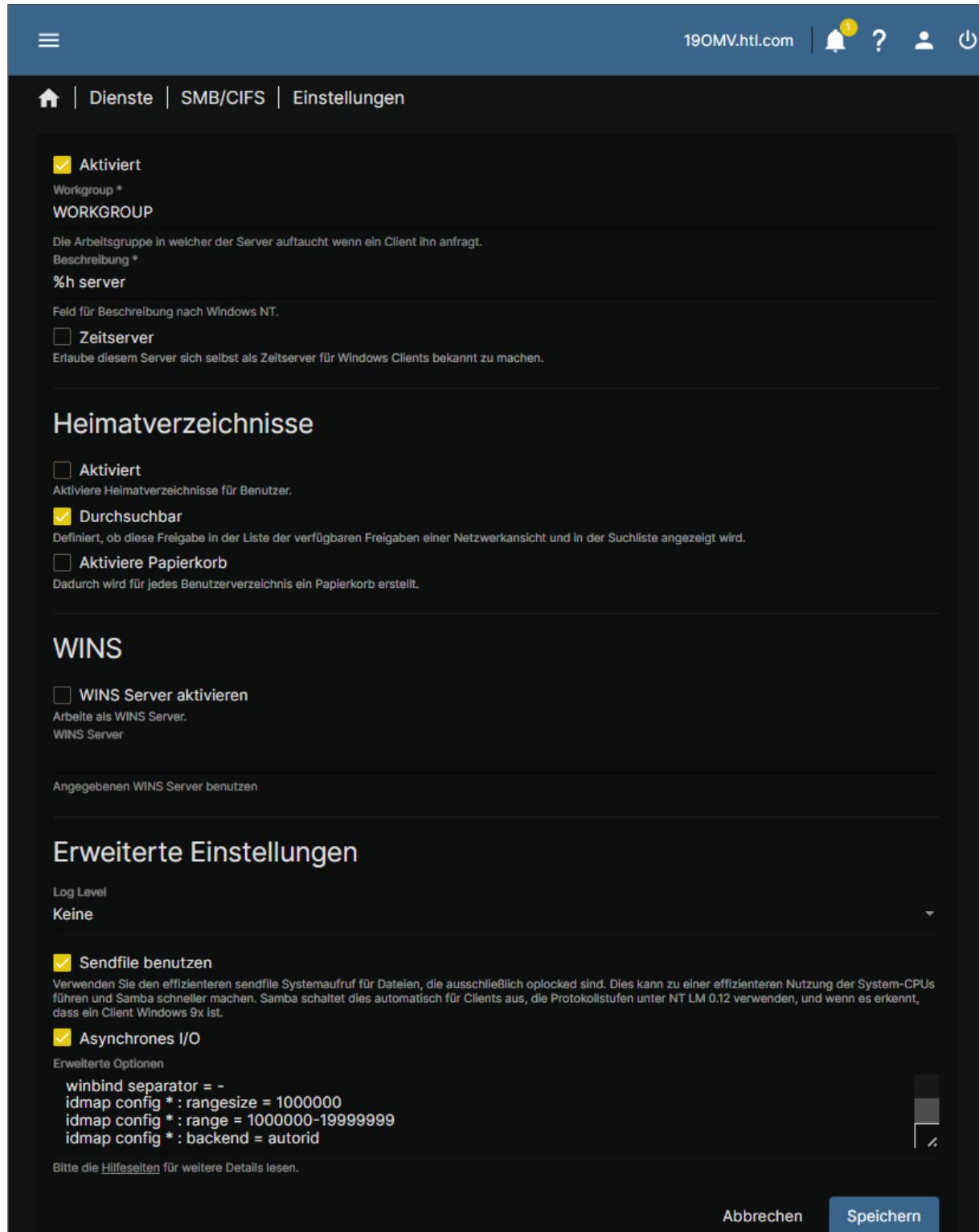
Speichern in VIM mittels `:wq` und schon sieht man die Domainenbenutzer:



Name	E-Mail	Gruppen	Stichworte
HTL-a.mesti		BUILTIN-users, HTL-a.mesti, HTL-domänen-benutzer	
HTL-administrator		BUILTIN-administrators, BUILTIN-users, HTL-abgelehnte rodc-kennwortreplicationsgruppe, HTL-administrator, HTL-domänen-admins, HTL-domänen-benutzer, HTL-organisation-admins, HTL-richtlinien-ersteller-besitzer, HTL-schema-admins	
HTL-f.schneider		BUILTIN-users, HTL-domänen-benutzer, HTL-f.schneider	
HTL-gäst		BUILTIN-gäste, BUILTIN-users, HTL-domänen-benutzer, HTL-domänen-gäste, HTL-gäst	
HTL-krbtgt		BUILTIN-users, HTL-abgelehnte rodc-kennwortreplicationsgruppe, HTL-domänen-benutzer, HTL-krbtgt	
HTL-trueberryless		BUILTIN-users, HTL-domänen-benutzer	

4.3.2.11 Samba

Nun müssen Sie Samba aktivieren. Hierbei ist es besonders wichtig, dass Sie darauf achten, die aktuelle Konfiguration nicht zu überschreiben. Blöderweise werden diese aktuellen Einstellungen nämlich nicht in der GUI angezeigt. Deswegen müssen Sie nochmals die Konfigurationen aus `/etc/samba/smb.conf` in die Erweiterten Optionen kopieren und das Häkchen bei Aktivieren nicht vergessen.



The screenshot shows the 'Dienste | SMB/CIFS | Einstellungen' section of the configuration interface. It includes sections for 'WORKGROUP' (activated), 'Zeitserver' (disabled), 'Heimatverzeichnisse' (activated, checked 'Durchsuchbar'), 'WINS' (disabled), and 'Erweiterte Einstellungen' (activated, showing 'Sendfile benutzen' and 'Asynchrones I/O' options). Navigation icons like 'Home', 'Dienste', 'SMB/CIFS', and 'Einstellungen' are visible at the top.

Aktiviert

Workgroup *

WORKGROUP

Die Arbeitsgruppe in welcher der Server auftaucht wenn ein Client ihn anfragt.

Beschreibung *

%h server

Feld für Beschreibung nach Windows NT.

Zeitserver

Erlaube diesem Server sich selbst als Zeitserver für Windows Clients bekannt zu machen.

Heimatverzeichnisse

Aktiviert

Aktiviere Heimatverzeichnisse für Benutzer.

Durchsuchbar

Definiert, ob diese Freigabe in der Liste der verfügbaren Freigaben einer Netzwerkansicht und in der Suchliste angezeigt wird.

Aktiviere Papierkorb

Dadurch wird für jedes Benutzerverzeichnis ein Papierkorb erstellt.

WINS

WINS Server aktivieren

Arbeite als WINS Server.

WINS Server

Angegebenen WINS Server benutzen

Erweiterte Einstellungen

Log Level

Keine

Sendfile benutzen

Verwenden Sie den effizienteren sendfile Systemaufruf für Dateien, die ausschließlich oplocked sind. Dies kann zu einer effizienteren Nutzung der System-CPUs führen und Samba schneller machen. Samba schaltet dies automatisch für Clients aus, die Protokollstufen unter NT LM 0.12 verwenden, und wenn es erkennt, dass ein Client Windows 9x ist.

Asynchrones I/O

Erweiterte Optionen

winbind separator = -
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autroid

Bitte die [Hilfeseiten](#) für weitere Details lesen.

Abbrechen Speichern

4.3.2.12 RAID

Nun können Sie unter [Datenspeicher → Software RAID](#) ein neues RAID hinzufügen. Ich habe mich für RAID 5 entschieden, doch Sie können auch einfach Mirror oder alle anderen Optionen verwenden.

Gerät	Zustand	Level	Kapazität	Geräte
/dev/md0	clean, resyncing (57.0% (11959772/20954112) finish=0.7min speed=198567K/sec)	RAID 5	39.97 GiB	• /dev/sdb • /dev/sdc • /dev/sdd

0 ausgewählt / 1 gesamt

4.3.2.13 Dateisystem erstellen

Wenn Sie das RAID haben, erstellen Sie gleich auch das Dateisystem unter [Datenspeicher → Dateisystem](#). Dabei müssen Sie zuerst das zuvor erstellte RAID auswählen, um das Dateisystem zu erstellen. Und anschließend müssen Sie dieses gerade eben erstellte Dateisystem hinzufügen, da dies nicht von alleine passiert.

Schlussendlich sollten Sie ungefähr so etwas sehen:

Gerät	Typ	Verfügbar	Verwendet	Eingehängt	Referenziert	Status
/dev/md0	EXT4	39.03 GiB	40.00 KiB	✓		Online

0 ausgewählt / 1 gesamt

4.3.2.14 Freigegebener Ordner erstellen

Der nächste Schritt ist das Erstellen eines freigegebenen Ordners. Dies können Sie unter Dateispeicher → Freigegebene Ordner tun.

The screenshot shows a list of shared folders. There is one entry named 'data' which is mounted on the device '/dev/md0' at the relative path 'data/'. The absolute path is '/srv/dev-disk-by-uuid-70dda524-d53a-4326-b07a-91f644cedea3/data'. The status bar at the bottom indicates '0 ausgewählt / 1 gesamt' (0 selected / 1 total).

Name	Gerät	Relativer Pfad	Absoluter Pfad	Referenziert	Stichworte
data	/dev/md0	data/	/srv/dev-disk-by-uuid-70dda524-d53a-4326-b07a-91f644cedea3/data		

4.3.2.15 SMB Share

Unter Dienste → SMB/CIFS → Freigaben können Sie anschließend einen SMB Share konfigurieren und erstellen.

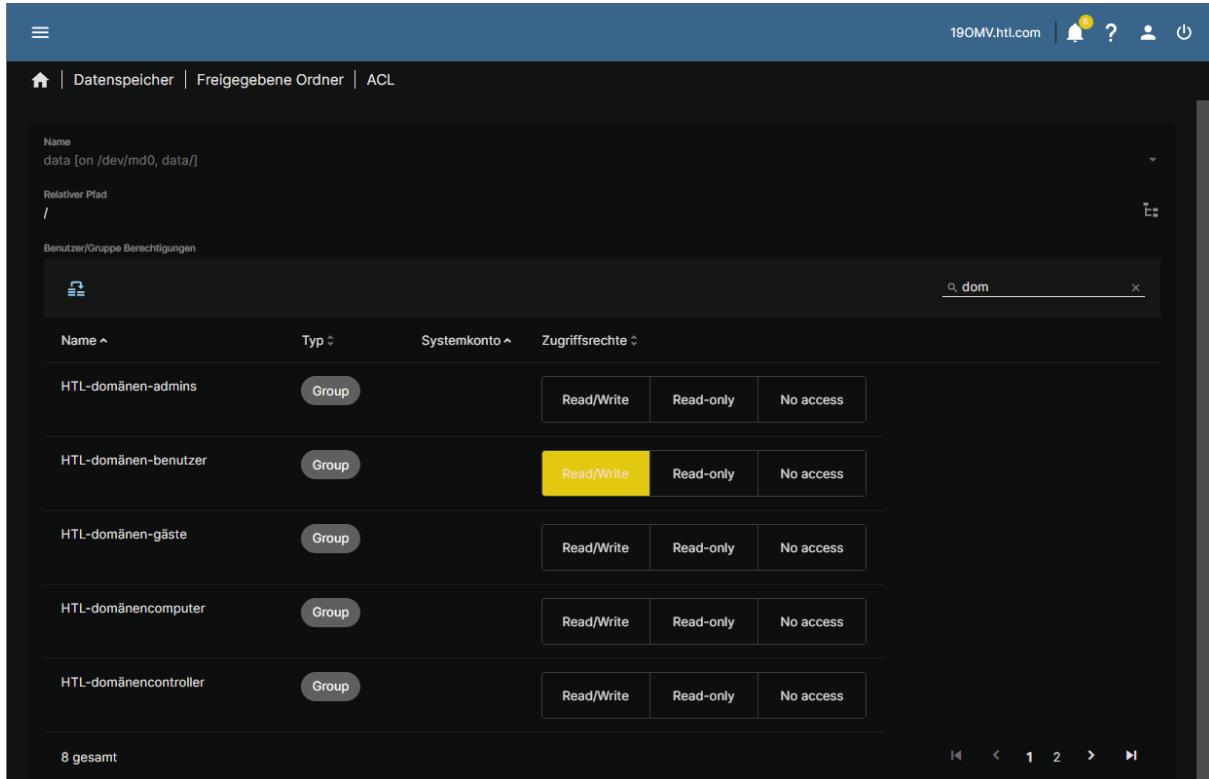
The screenshot shows a configuration page for a share. The share is named 'data' and is marked as active ('Aktiviert'). It has the comment 'No' and is set to be publicly accessible ('Öffentlich') and readable ('Nur lesen'). The status bar at the bottom indicates '0 ausgewählt / 1 gesamt' (0 selected / 1 total).

Aktiviert	Freigegebener Ordner	Kommentar	Öffentlich	Nur lesen	Durchsuchbar
✓	data	No		✓	

4.3.2.16 Zugriffskontrolllisten einstellen

Geben Sie nun allen HTL-domänen-benutzer eine Lese- und Schreibberechtigung für diesen Share.

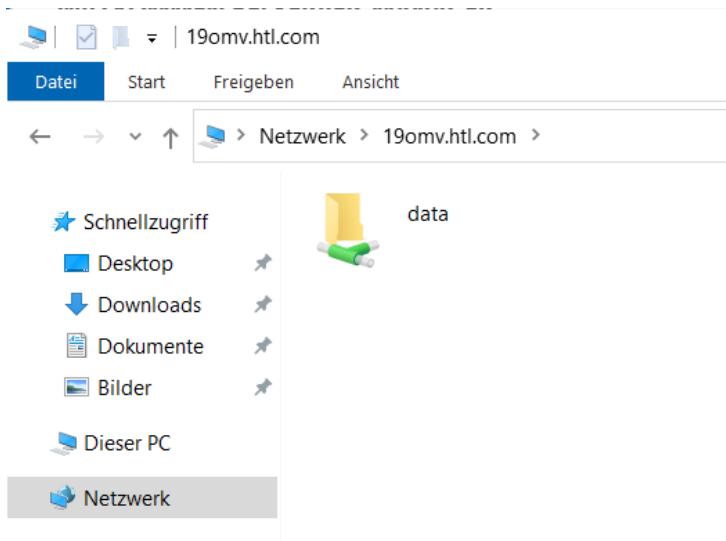
Diese Einstellung kann mittels klicken auf dieses:  Symbol unter Dateispeicher → Freigegebene Ordner erzielt werden, nachdem Sie den richtigen (wir haben nur einen) Share ausgewählt haben.



Name	Typ	Systemkonto	Zugriffsrechte
HTL-domänen-admins	Group		Read/Write Read-only No access
HTL-domänen-benutzer	Group		Read/Write Read-only No access
HTL-domänen-gäste	Group		Read/Write Read-only No access
HTL-domänencomputer	Group		Read/Write Read-only No access
HTL-domänencontroller	Group		Read/Write Read-only No access

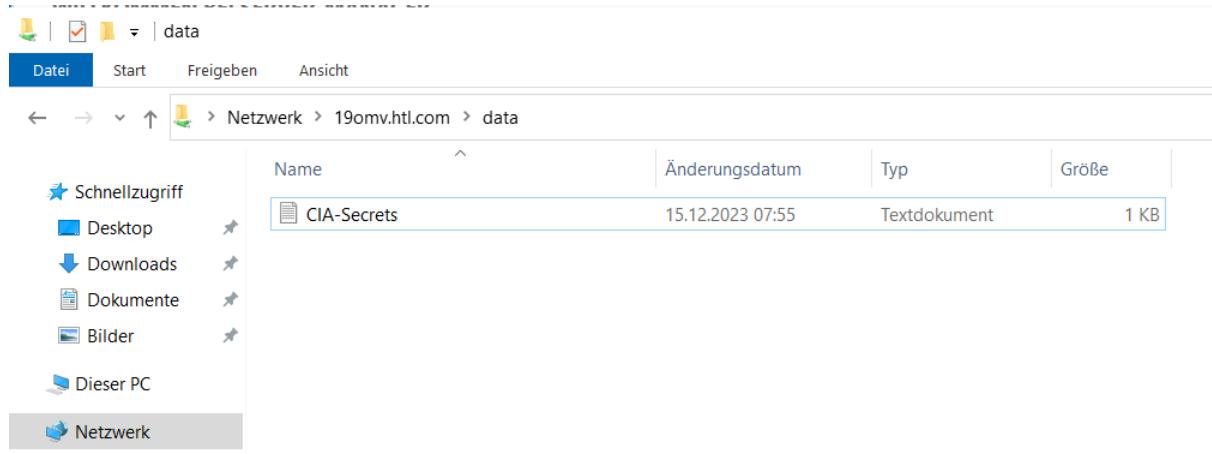
4.3.2.17 Ordnerzugriff

Nun sehen Sie einen Ordner **data**, wenn Sie auf einem Client 19omv.htl.com eingeben.



4.3.2.18 File erstellen

Erstellen Sie eine Datei, welche Sie anschließend am NAS sehen können.



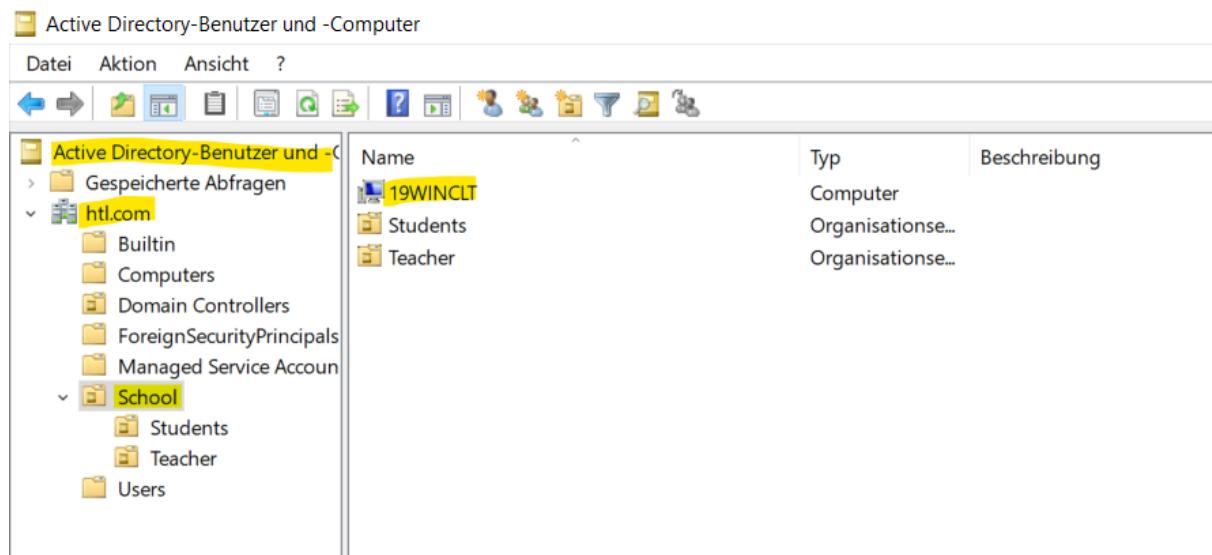
4.3.2.19 Zugriffsrechte ansehen

Wie Sie sehen, wurde die Datei von einem Administrator erstellt (weil ich die Datei am Server hinzugefügt habe) und die Berechtigungen sind 674 (nein, ich habe keinen [CHMOD-Rechner](#) verwendet), sprich: der Besitzer kann lesen und schreiben, während die Gruppe auch ausführen kann. Leserberechtigungen hat jeder.

```
root@190MV:/srv/dev-disk-by-uuid-70dda524-d53a-4326-b07a-91f644cedea3/data# ls -al
insgesamt 12
drwxrwsr-x+ 2 root          users 4096 15. Dez 07:55 .
drwxr-xr-x  4 root          root   4096 15. Dez 07:45 ..
-rw-rwrxr--+ 1 HTL-administrator users  23 15. Dez 07:55 CIA-Secrets.txt
root@190MV:/srv/dev-disk-by-uuid-70dda524-d53a-4326-b07a-91f644cedea3/data# |
```

4.3.2.20 Client zu OU hinzufügen

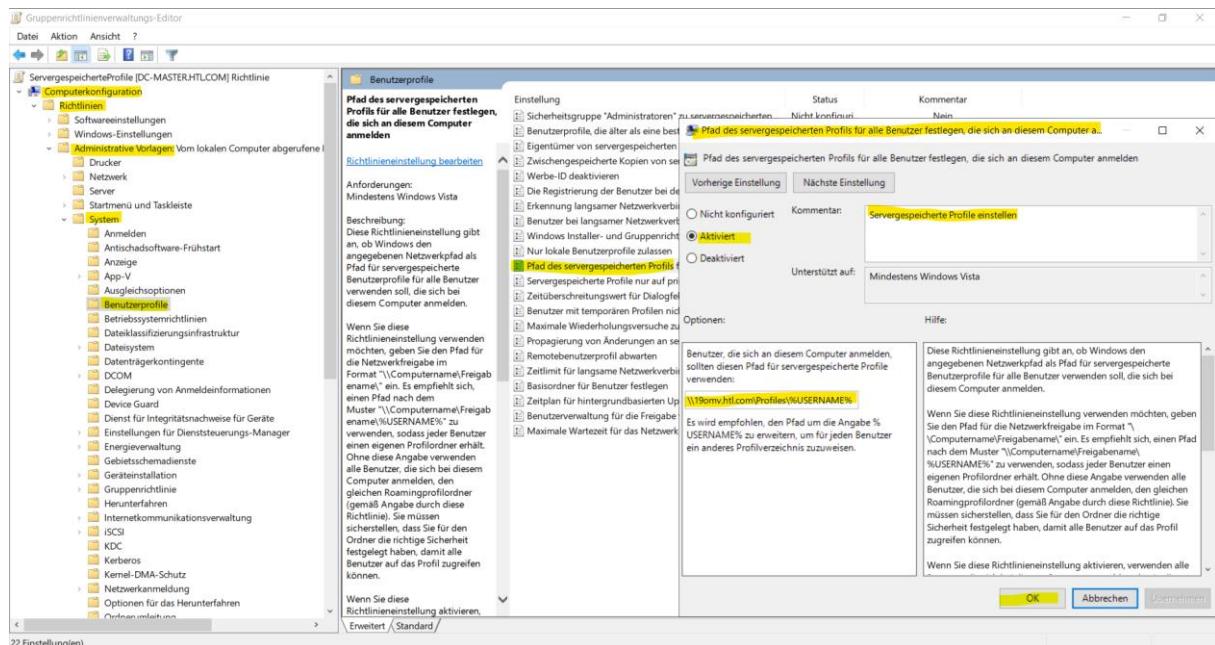
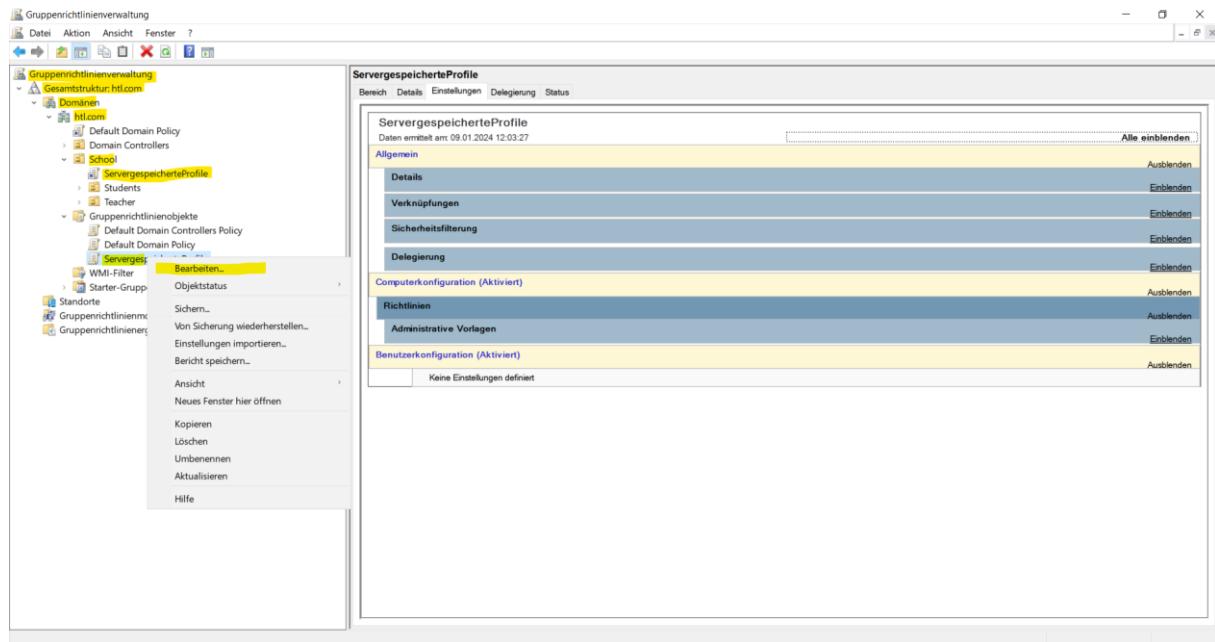
Damit wir später das Gruppenrichtlinienobjekt einfach zu unserem Client hinzufügen können (damit die Computereinstellungen funktionieren) und alle Benutzer ebenfalls in diesem Gruppenrichtlinienobjekt sind (Benutzereinstellungen funktionieren), ziehen wir den Client einfach in die OU School (Client unbedingt neu starten nach dieser Verschiebung):



Name	Typ	Beschreibung
19WINCLT	Computer	
Students	Organisationseinheit	
Teacher	Organisationseinheit	

4.3.2.21 Gruppenrichtlinienobjekt erstellen (servergespeichertes Profil)

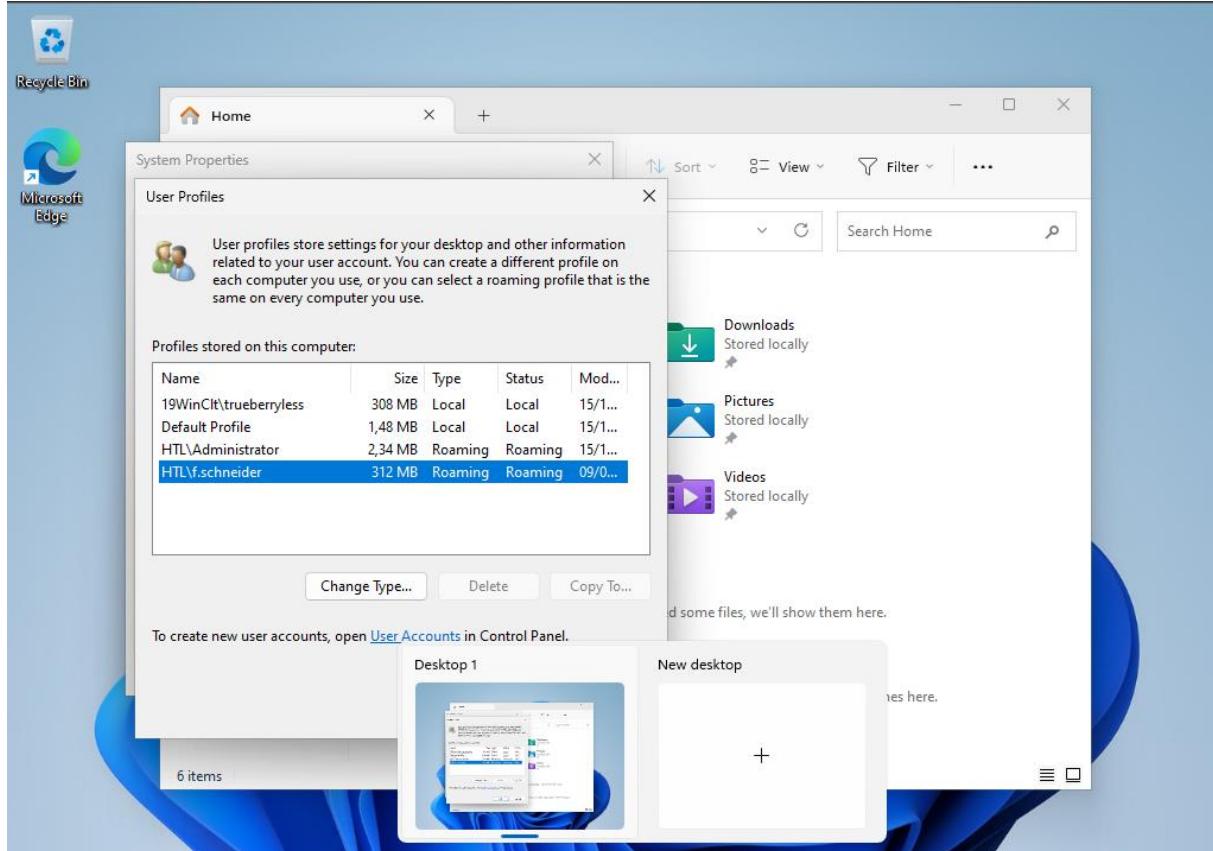
Damit beim Anmelden eines Benutzerkontos automatisch im richtigen Ordner am NAS ein Ordner für den Benutzer angelegt wird, müssen wir tief in den Gruppeneinstellungen diese Option einstellen und sicherstellen, dass es für die virtuelle Maschine Client gilt:



Tipp: Vorab müssen Sie einen weiteren Share erstellen (Profiles in meinem Fall) und die SMB Freigabe zugehörig konfigurieren.

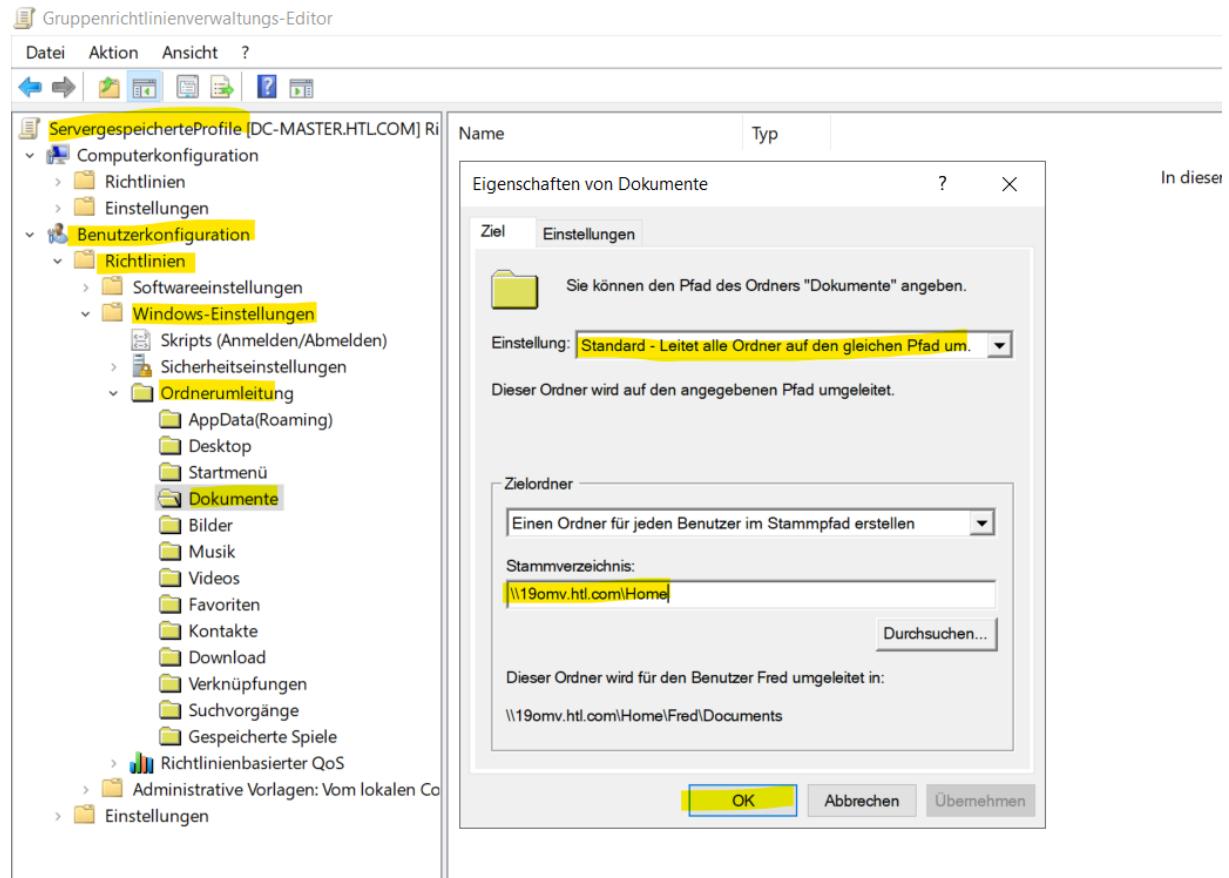
Nun wird beim Anmelden ein Ordner für den Benutzer erstellt (welcher noch leer ist) und beim Abmelden alle Daten des Benutzers auf den Server geladen.

Deswegen sieht man bei den User Profiles, dass diese vom Typ her auf Roaming gesetzt sind:



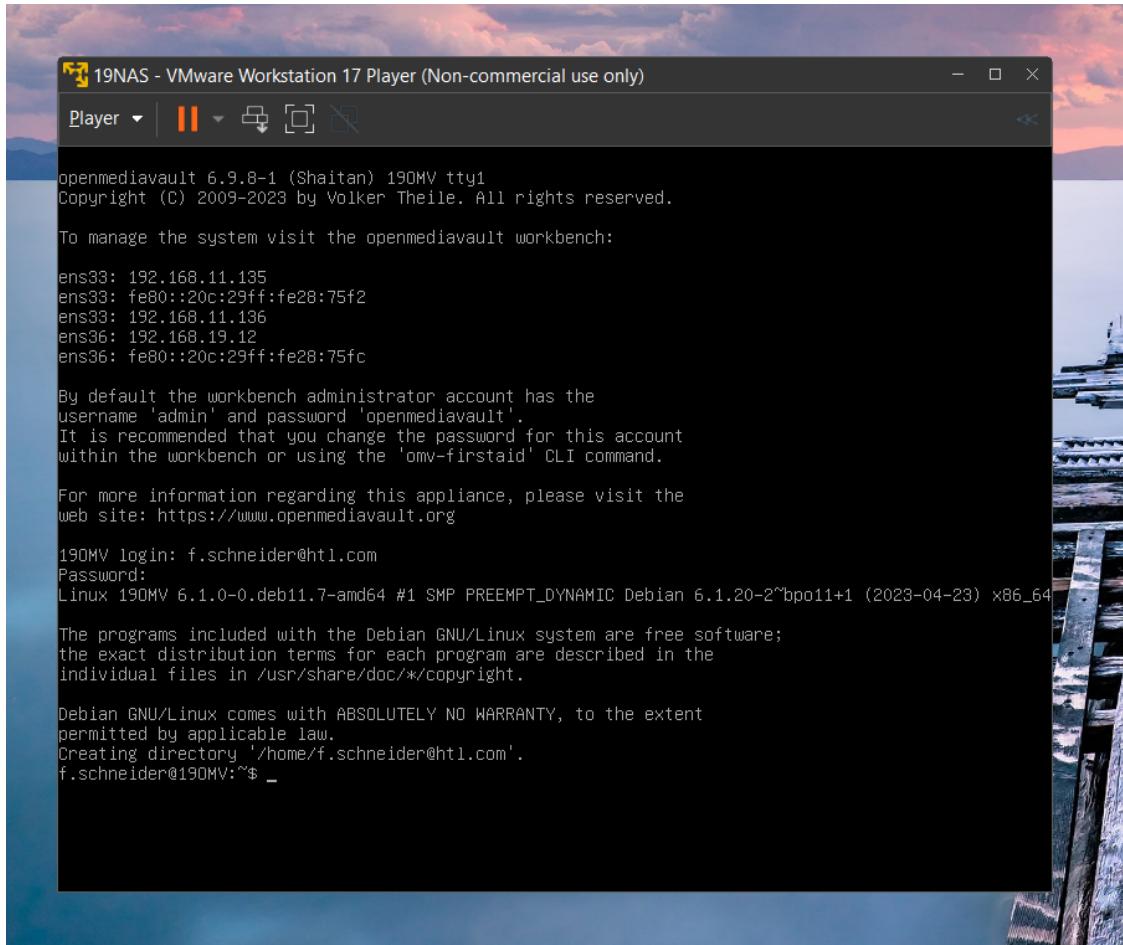
4.3.2.22 Gruppenrichtlinienobjekt erstellen (Ordnerumleitung)

Unter Benutzerkonfiguration → Richtlinien → Windows-Einstellungen → Ordnerumleitung können Sie für jegliche Ordner deren Umleitung auf einen Share einrichten, sodass auch die Daten der Benutzer serverseitig gespeichert werden.



5 Ergebnis

Anschließend können Sie sich beim NAS mit Domainbenutzern anmelden, die Benutzer in der Weboberfläche sehen, auf den Share zugreifen und sich mit einem Benutzer überall anmelden (falls der Computer in der OU School ist), wobei ihre Daten auf dem Server liegen und von überall aus verfügbar sind.



The screenshot shows the OpenMediaVault web interface. The left sidebar menu includes "Dashboard", "System", "Netzwerk", "Datenspeicher", "Dienste", "Benutzer", "Einstellungen", "Diagnose", and "Logout". The main content area is titled "Benutzerverwaltung | Benutzer". It displays a list of users with their details:

Name	E-Mail	Gruppen	Stichworte
HTL-a.mesti		BUILTIN-users, HTL-a.mesti, HTL-domänen-benutzer	
HTL-administrator		BUILTIN-administrators, BUILTIN-users, HTL-abgelehnte rdc-kennwortreplikationsgruppe, HTL-administrator, HTL-domänen-admins, HTL-domänen-benutzer, HTL-organisation-admins, HTL-richtlinien-hersteller-bezirker, HTL-schema-admins	
HTL-f.schneider		BUILTIN-users, HTL-domänen-benutzer, HTL-f.schneider	
HTL-gast		BUILTIN-guests, BUILTIN-users, HTL-domänen-benutzer, HTL-domänen-gäste, HTL-gast	
HTL-krbtgt		BUILTIN-users, HTL-abgelehnte rdc-kennwortreplikationsgruppe, HTL-domänen-benutzer, HTL-krbtgt	
HTL-trueberryless		BUILTIN-users, HTL-domänen-	

