

159 -

Directoryservices konfigurieren und in Betrieb nehmen

- [OpenLDAP Samba Share](#)
- [Samba OpenLDAP AD Integration](#)

OpenLDAP Samba Share

Diese Anleitung geht davon aus, dass die folgenden Schritte bereits durchgeführt wurden und alles funktioniert:

<https://www.howtoforge.de/anleitung/so-installierst-du-openldap-unter-ubuntu-22-04/>

Installation der notwendigen Pakete:

Installiere Samba und die LDAP-Unterstützungspakete:

```
sudo apt update
sudo apt install samba smbldap-tools libnss-ldap libpam-ldap
```

Konfiguration von NSS und PAM für LDAP:

Während der Installation wirst du aufgefordert, die LDAP-Konfiguration bereitzustellen. Gib dabei die Details deines OpenLDAP-Servers an, wie z.B. die Basis-DN und den LDAP-Server-URI.

Bearbeite die Datei `/etc/nsswitch.conf`, um LDAP in die Namensauflösung einzubeziehen:

```
sudo nano /etc/nsswitch.conf
```

Ändere die Zeilen `passwd`, `group` und `shadow` wie folgt:

```
# /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:    compat ldap
group:     compat ldap
shadow:    compat ldap
gshadow:   files

hosts:     files dns
networks:  files
```

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

netgroup:    nis
```

Konfiguration von Samba für LDAP:

Erstelle eine Sicherungskopie der aktuellen Samba-Konfigurationsdatei:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Bearbeite die Samba-Konfigurationsdatei:

```
sudo nano /etc/samba/smb.conf
```

Füge oder passe folgende Parameter im `[global]`-Abschnitt an:

```
[global]
workgroup = test.local
security = user
passdb backend = ldapsam:ldap://ldap.test.local
ldap admin dn = cn=admin,dc=test,dc=local
ldap suffix = dc=test,dc=local
ldap user suffix = ou=Sales
ldap group suffix = ou=group
ldap machine suffix = ou=Computers
ldap passwd sync = yes
ldap ssl = no
```

Einrichten des Samba-Administrators:

Füge den LDAP-Administrator als Samba-Benutzer hinzu:

```
sudo smbpasswd -W
```

```
ldapadd -Q -LLL -Y EXTERNAL -H ldapi:/// -f /usr/share/doc/samba/examples/LDAP/samba.ldif
```

Gib das Passwort des LDAP-Administrators ein.

Erstellen eines Samba-Shares:

Füge am Ende der Datei `/etc/samba/smb.conf` folgenden Abschnitt hinzu:

```
[shared]
    path = /srv/samba/shared
    browseable = yes
    writable = yes
    guest ok = no
    valid users = john.doe
```

Erstelle das Verzeichnis und setze die Berechtigungen:

```
sudo mkdir -p /srv/samba/shared
sudo chown -R nobody:nogroup /srv/samba/shared
sudo chmod -R 777 /srv/samba/shared
```

User Konfigurieren:

Der User sollte schlussendlich eine ähnliche konfiguration wie die folgende haben.

```
root@ldap:~# ldapsearch -x -H ldap://ldap.test.local -b "uid=john.doe,ou=Sales,dc=test,dc=local"
dn: uid=john.doe,ou=Sales,dc=test,dc=local
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
cn: John Doe
sn: Doe
mail: john.doe@test.local
uid: john.doe
sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
00000000
sambaAcctFlags: [U      ]
loginShell: /bin/bash
homeDirectory: /home/john.doe
uidNumber: 15258
gidNumber: 4549
sambaPwdLastSet: 1731871539
sambaSID: S-1-5-21-1055546307-1221338049-756278767-1001
```

```
sambaNTPassword: A9FDFA038C4B75EBC76DC855DD74F0DA
```

sambaSID: Kann über den folgenden befehl generiert werden. (muss hintendran noch eine 4 Stellige nummer konfiguriert werden)

```
root@ldap:~# net getlocalsid
```

```
SID for domain LDAP is: S-1-5-21-1055546307-1221338049-756278767
```

sambaNTPassword: To make the NT Password you can use the following Site:

<https://www.browserling.com/tools/ntlm-hash>

Machen würde man es mit dem folgenden Idif file:

```
dn: uid=john.doe,ou=Sales,dc=test,dc=local
changetype: modify
add: objectClass
objectClass: sambaSamAccount
objectClass: posixAccount
-
add: loginShell
loginShell: /bin/bash
-
add: homeDirectory
homeDirectory: /home/john.doe
-
add: uidNumber
uidNumber: 15258
-
add: gidNumber
gidNumber: 4549
-
add: sambaSID
sambaSID: S-1-5-21-1055546307-1221338049-756278767-1001
-
add: sambaNTPassword
sambaNTPassword: A9FDFA038C4B75EBC76DC855DD74F0DA
```

Um das File dann auszuführen benutzen sie dann denn folgenden befehl:

```
ldapmodify -x -D "cn=admin,dc=test,dc=local" -W -H ldap://ldap.test.local -f modify_john_doe.ldif
```

```
smbpasswd -a john.doe
```

Neustart der Dienste

Starte die Samba-Dienste neu, um die Änderungen zu übernehmen:

```
sudo systemctl restart smbd nmbd
```

Testen

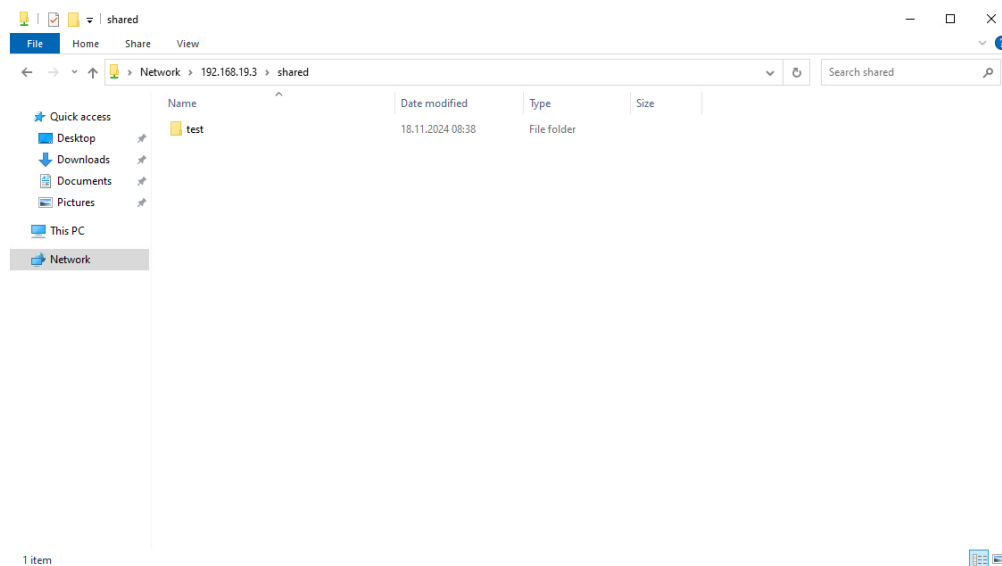
Linux

```
smbclient //192.168.19.3/shared -U john.doe
```

```
root@ldap:~# smbclient //192.168.19.3/shared -U john.doe
Password for [TEST.LOCAL\john.doe]:
Try "help" to get a list of possible commands.
smb: \> mkdir test
smb: \> ls
.                D            0   Mon Nov 18 07:38:32 2024
..               D            0   Mon Nov 18 07:38:32 2024
test             D            0   Mon Nov 18 07:38:32 2024

                24050032 blocks of size 1024. 14773196 blocks available
smb: \> |
```

Windows



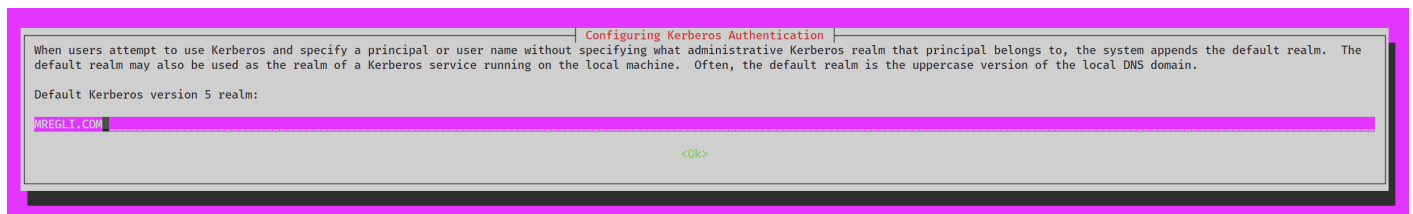
Samba OpenLDAP AD Integration

Installation der benötigten Pakete

```
sudo apt update  
sudo apt install samba smbclient krb5-user winbind libpam-winbind libnss-winbind -y
```

Während der Installation kommen die folgenden Fenster die man befüllen müsste:

Domain in Grossbuchstaben:



Configuring Kerberos Authentication

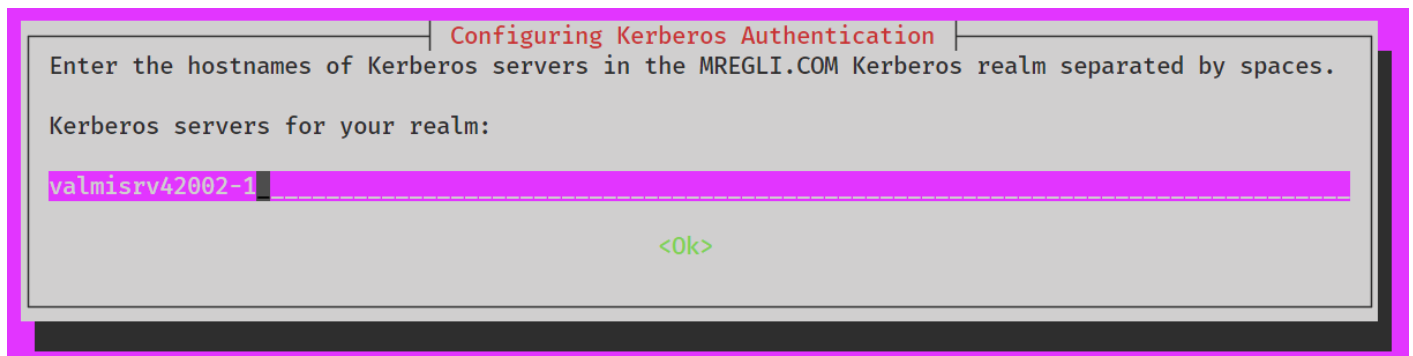
When users attempt to use Kerberos and specify a principal or user name without specifying what administrative Kerberos realm that principal belongs to, the system appends the default realm. The default realm may also be used as the realm of a Kerberos service running on the local machine. Often, the default realm is the uppercase version of the local DNS domain.

Default Kerberos version 5 realm:

MREGLI.COM

<Ok>

Für eine Standalone-Umgebung zu erstellen, gib den Hostnamen des Servers ein.



Configuring Kerberos Authentication

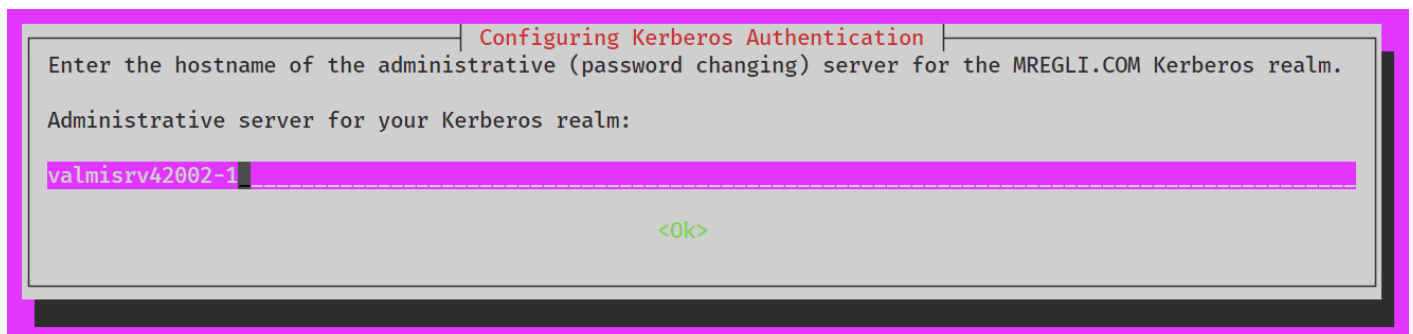
Enter the hostnames of Kerberos servers in the MREGLI.COM Kerberos realm separated by spaces.

Kerberos servers for your realm:

valmisrv42002-1

<Ok>

Für eine Standalone-Umgebung zu erstellen, gib den Hostnamen des Servers ein.



Configuring Kerberos Authentication

Enter the hostname of the administrative (password changing) server for the MREGLI.COM Kerberos realm.

Administrative server for your Kerberos realm:

valmisrv42002-1

<Ok>

Initialisierung der Domain

Entfernen der Standardkonfigurationsdatei:

```
sudo rm /etc/samba/smb.conf
```

Provisionieren der Domain:

```
sudo samba-tool domain provision --use-rfc2307 --interactive
```

```
root@valmisrv42002-1:~# sudo rm /etc/samba/smb.conf
sudo samba-tool domain provision --use-rfc2307 --interactive
Realm [MREGLI.COM]:
Domain [MREGLI]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.53]:
Administrator password:
Retype password:
INFO 2024-11-19 11:45:22,956 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2128: Looking up IPv4 addresses
INFO 2024-11-19 11:45:22,957 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2145: Looking up IPv6 addresses
WARNING 2024-11-19 11:45:22,958 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2152: No IPv6 address will be assigned
INFO 2024-11-19 11:45:23,404 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2318: Setting up share.ldb
INFO 2024-11-19 11:45:23,428 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2322: Setting up secrets.ldb
INFO 2024-11-19 11:45:23,446 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2327: Setting up the registry
INFO 2024-11-19 11:45:23,504 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2330: Setting up the privileges database
INFO 2024-11-19 11:45:23,536 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2333: Setting up idmap db
INFO 2024-11-19 11:45:23,558 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2340: Setting up SAM db
INFO 2024-11-19 11:45:23,567 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #886: Setting up sam.ldb partitions and settings
INFO 2024-11-19 11:45:23,568 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #898: Setting up sam.ldb rootDSE
INFO 2024-11-19 11:45:23,575 pid:2731 /usr/lib/python3/dist-packages/samba/provision/__init__.py #1320: Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce uniqueness constraint on local domainSIDs
```

DNS Konfiguration

Deaktivieren des systemd-resolved Dienstes:

```
sudo systemctl disable --now systemd-resolved
```

```
root@valmisrv42002-1:~# sudo systemctl disable --now systemd-resolved
Removed "/etc/systemd/system/sysinit.target.wants/systemd-resolved.service"
Removed "/etc/systemd/system/dbus-org.freedesktop.resolve1.service".
```

Anpassen der `/etc/resolv.conf`:

```
sudo rm /etc/resolv.conf
sudo nano /etc/resolv.conf
```

Inhalt:

```
nameserver 127.0.0.1
search <deine-domain.local>
```

Konfiguration von `/etc/samba/smb.conf`

Füge die Konfiguration hinzu:


```
[global]
```

```
dns forwarder = <externer-DNS-IP>
```

Starten und Aktivieren der Dienste

```
sudo systemctl start smbd nmbd winbind
```

```
sudo systemctl stop smbd nmbd winbind
```

```
sudo systemctl start samba-ad-dc
```

```
sudo systemctl enable samba-ad-dc
```

Testen der Internetverbindung

```
host -t SRV _ldap._tcp.mregli.com
```

```
root@valmisrv42002-1:~# host -t SRV _ldap._tcp.mregli.com
_ldap._tcp.mregli.com has SRV record 0 100 389 valmisrv42002-1.mregli.com.
```

```
ping google.com
```

```
root@valmisrv42002-1:~# ping google.com
PING google.com (172.217.168.14) 56(84) bytes of data.
64 bytes from zrh11s03-in-f14.1e100.net (172.217.168.14): icmp_seq=1 ttl=117 time=20.8 ms
64 bytes from zrh11s03-in-f14.1e100.net (172.217.168.14): icmp_seq=2 ttl=117 time=10.8 ms
64 bytes from zrh11s03-in-f14.1e100.net (172.217.168.14): icmp_seq=3 ttl=117 time=12.1 ms
64 bytes from zrh11s03-in-f14.1e100.net (172.217.168.14): icmp_seq=4 ttl=117 time=14.0 ms
64 bytes from zrh11s03-in-f14.1e100.net (172.217.168.14): icmp_seq=5 ttl=117 time=13.2 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 10.832/14.190/20.842/3.495 ms
```

Benutzerverwaltung

Benutzer erstellen

Erstellen eines neuen Benutzers:

```
sudo samba-tool user create <username> <password>
```

```
root@valmisrv42002-1:~# sudo samba-tool user create manuel.regli Bbw.2024
User 'manuel.regli' added successfully
```

Benutzer einer Gruppe hinzufügen

Gruppe erstellen:

```
sudo samba-tool group add "GroupName"
```

Benutzer zur Gruppe hinzufügen:

```
sudo samba-tool group addmembers "GroupName" "username"
```

```
root@valmisrv42002-1:~# sudo samba-tool group add samba-share
Added group samba-share
root@valmisrv42002-1:~# sudo samba-tool group addmembers samba-share manuel.regli
Added members to group samba-share
```

Benutzer anzeigen

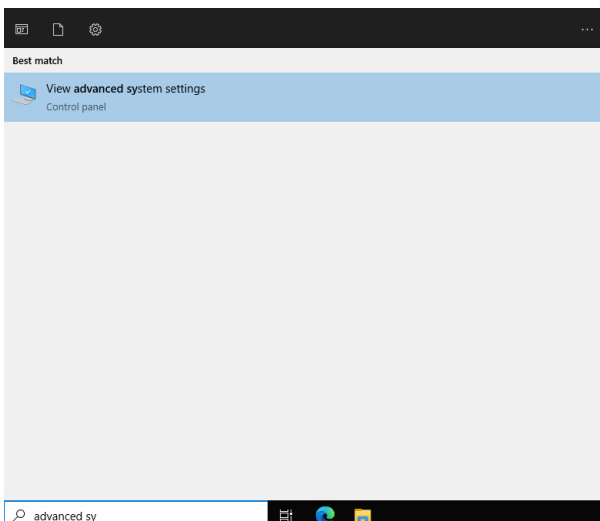
Liste aller Benutzer im Active Directory:

```
sudo samba-tool user list
```

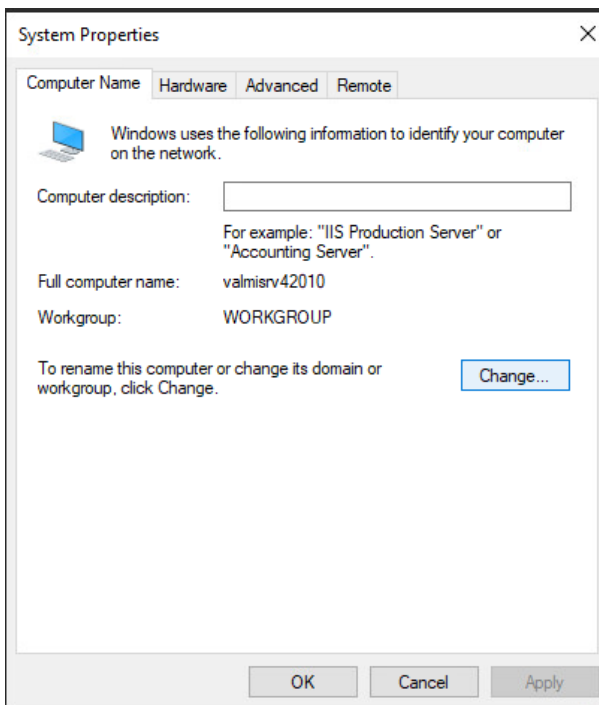
```
root@valmisrv42002-1:~# sudo samba-tool user list
krbtgt
manuel.regli
Administrator
Guest
```

Active Directory Join

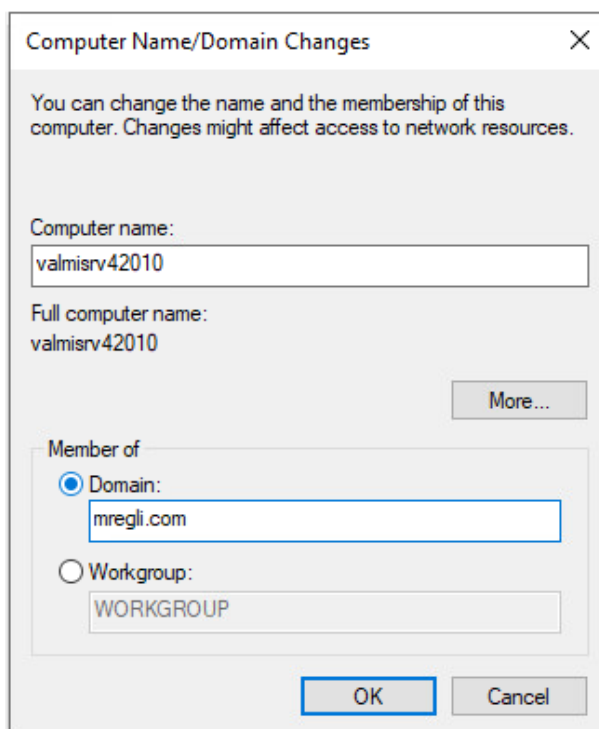
Öffnen der "Advanced System Settings"



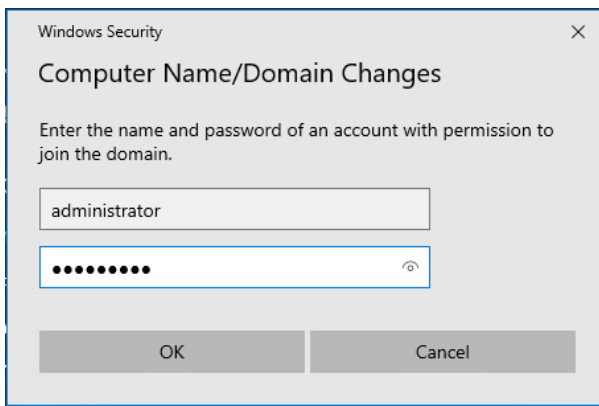
Gehe zum Reiter "Computer Name" und wähle unten "change".



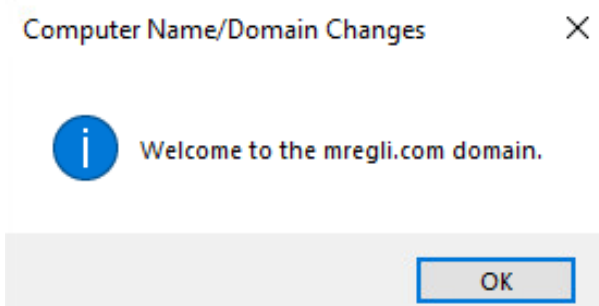
Danach einfach den Domain-Button auswählen und die konfigurierte Domain eingeben. Ebenfalls kontrollieren, ob der Computername richtig ist.



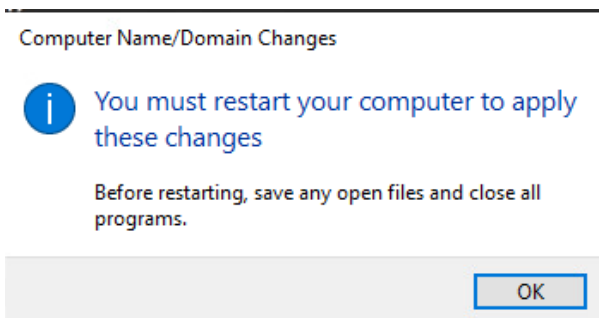
Um sich zur Domain zu verbinden, kannst du entweder den Administrator nutzen oder einen User mit den richtigen Berechtigungen.



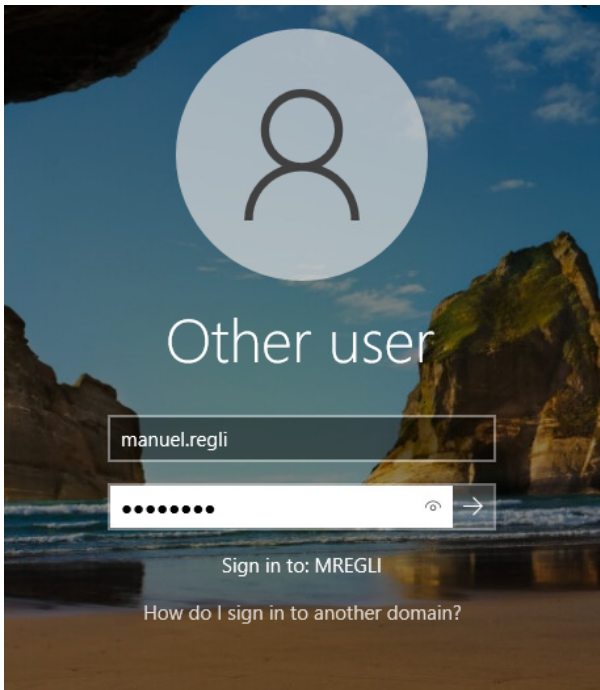
Wenn alles richtig eingestellt ist, müsste dieses Fenster erscheinen.



Danach muss man den Computer neu starten, damit er vollständig verbunden werden kann.



Jetzt kann man sich mit dem erstellten Active Directory-Benutzer anmelden.



Share erstellen

Ordner erstellen und Berechtigungen für die Freigabe setzen

```
sudo mkdir -p /srv/samba/share  
sudo chmod 770 /srv/samba/share
```

Füge die Freigabe in die smb.conf ein.

```
sudo nano /etc/samba/smb.conf
```

Ganz unten hinzufügen.

```
[share]  
path = /srv/samba/share  
read only = no  
create mask = 0666  
directory mask = 0777  
valid users = @samba-share
```

Samba testen

