

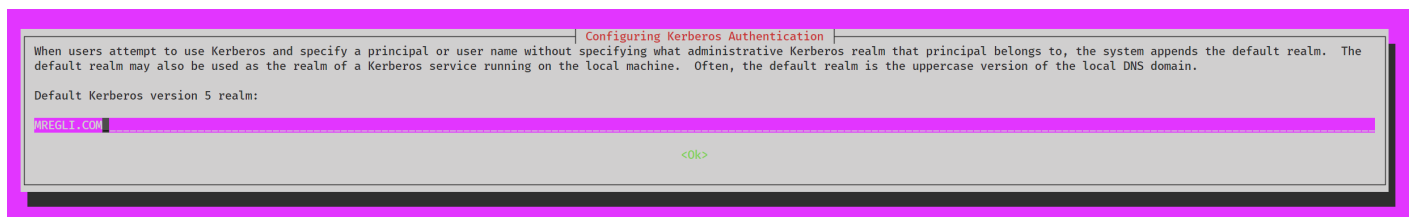
Samba OpenLDAP AD Integration

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:



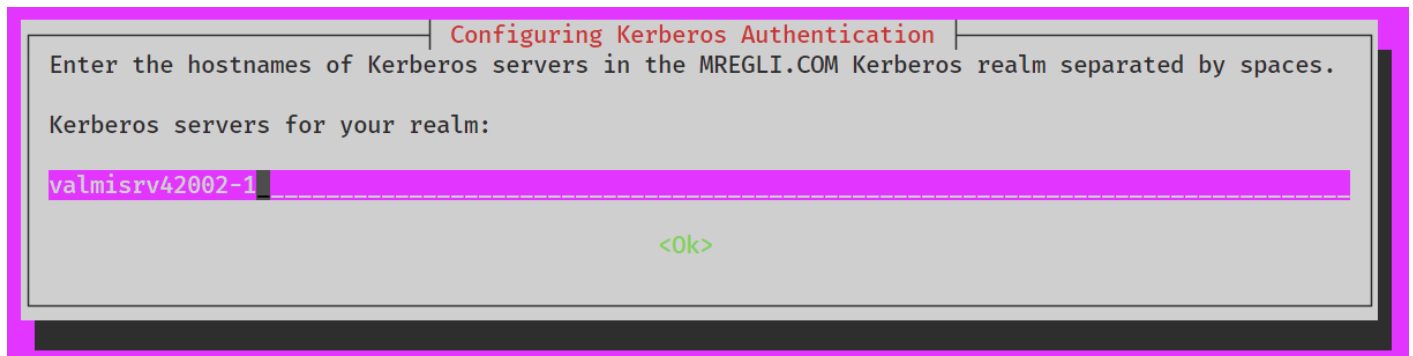
When users attempt to use Kerberos and specify a principal or user name without specifying what administrative Kerberos realm that principal belongs to, the system appends the default realm. The default realm may also be used as the realm of a Kerberos service running on the local machine. Often, the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

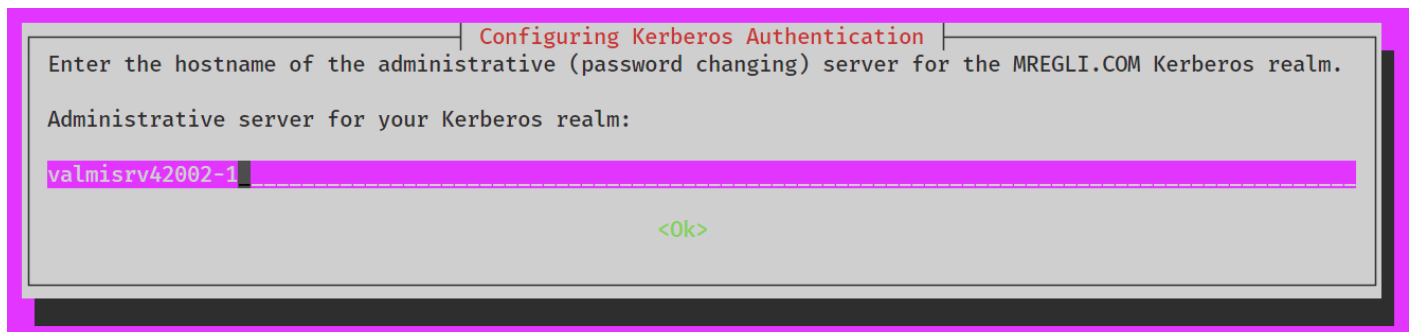
Enter the hostnames of Kerberos servers in the MREGLI.COM Kerberos realm separated by spaces.

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

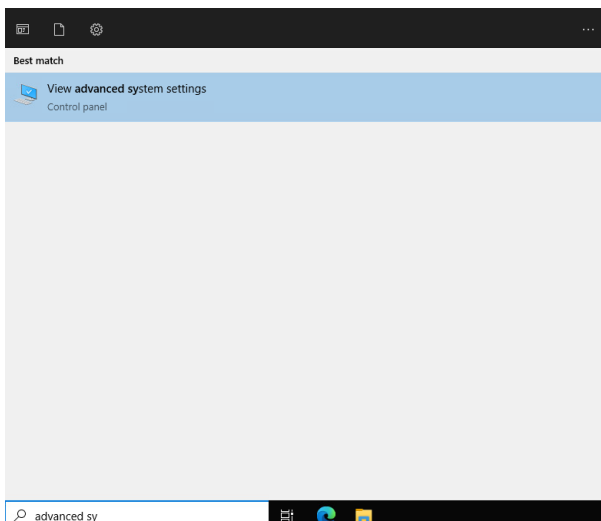
Liste aller Benutzer im Active Directory:

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

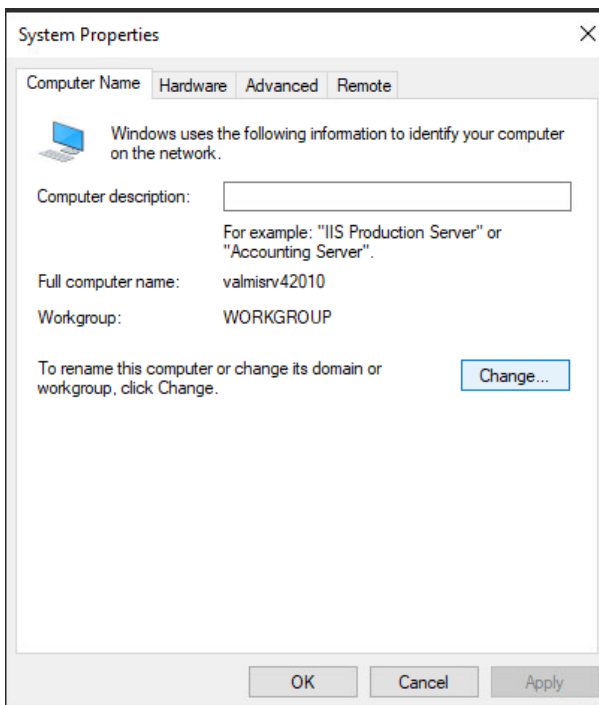
```
root@valmisrv42002-1:~# sudo samba-tool user list
krbtgt
manuel.regli
Administrator
Guest
```

Active Directory Join

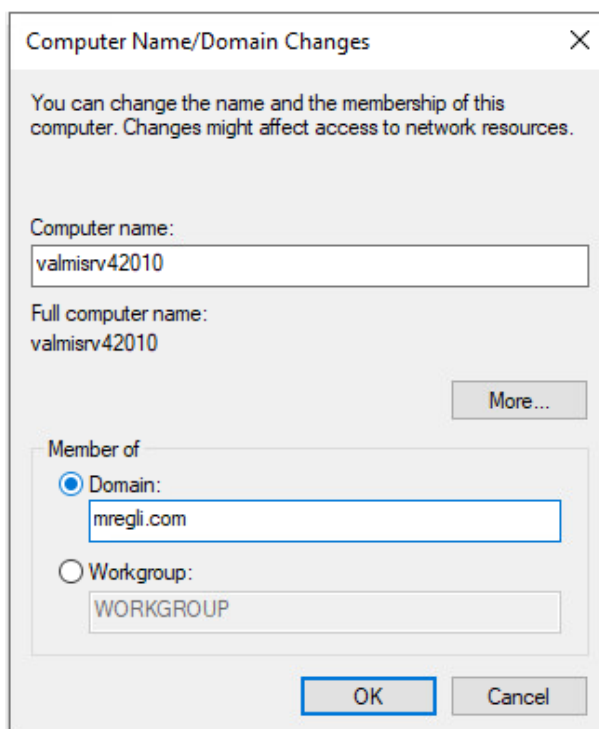
Öffnen der "Advanced System Settings"



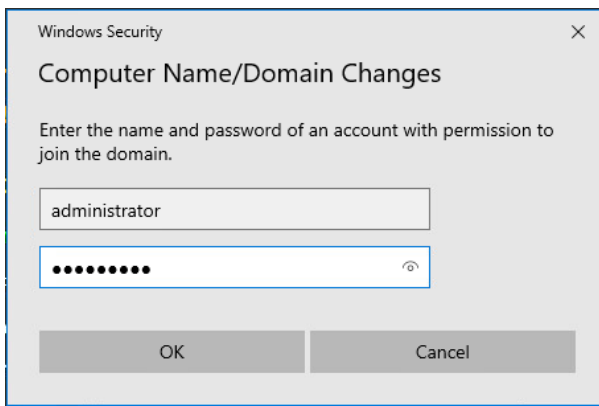
Gehe zum Reiter "Computer Name" und wähle unten "change".



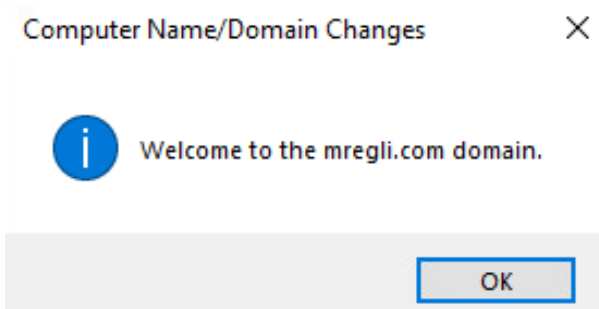
Danach einfach den Domain-Button auswählen und die konfigurierte Domain eingeben. Ebenfalls kontrollieren, ob der Computername richtig ist.



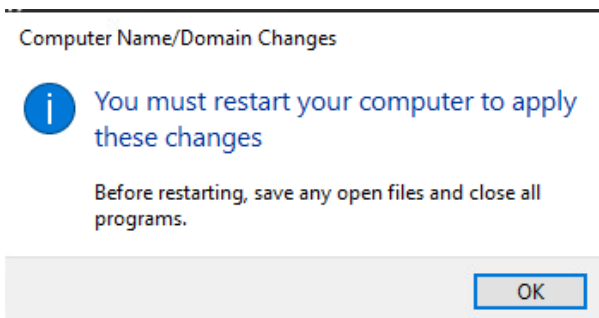
Um sich zur Domain zu verbinden, kannst du entweder den Administrator nutzen oder einen User mit den richtigen Berechtigungen.



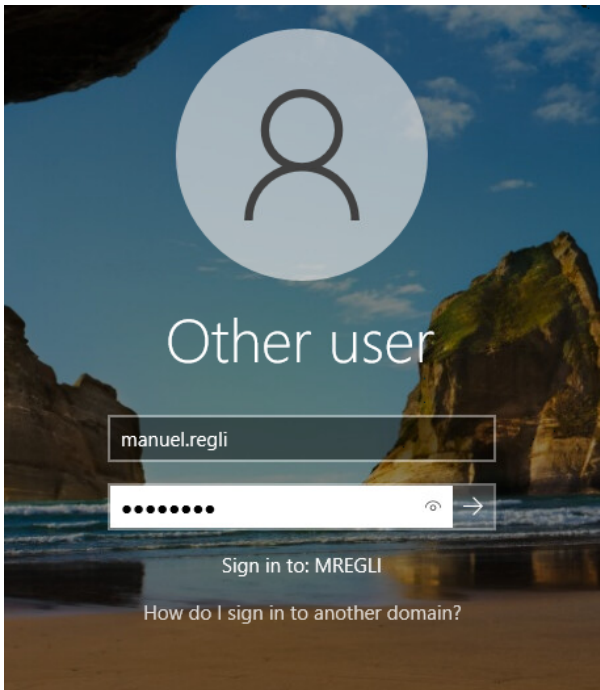
Wenn alles richtig eingestellt ist, müsste dieses Fenster erscheinen.



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
```

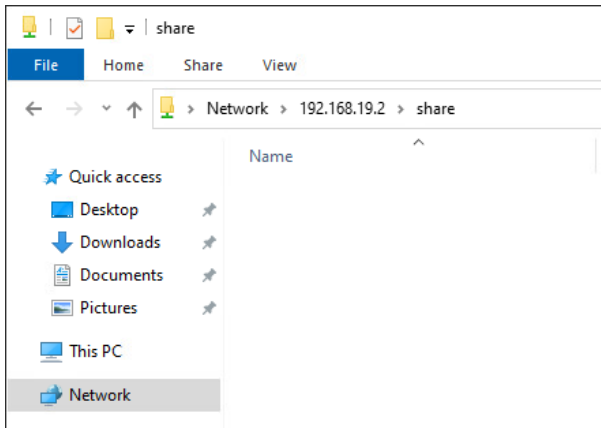
Füge die Freigabe in die smb.conf ein.

```
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



Revision #8

Created 19 November 2024 10:17:37 by Manuel Regli

Updated 9 December 2024 12:47:35 by Manuel Regli