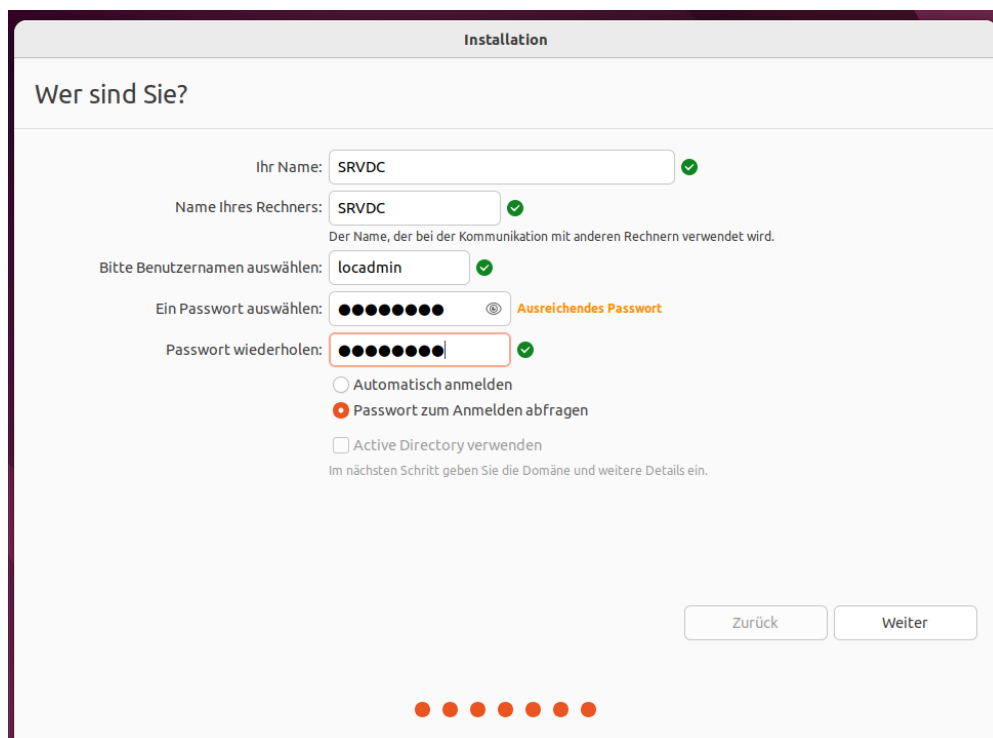


Linux Betriebssystem (Ubuntu) als Domain Controller

Mit samba (Linux-Implementierung von SMB) kann man aus einem Linux-Rechner einen Domänencontroller machen.

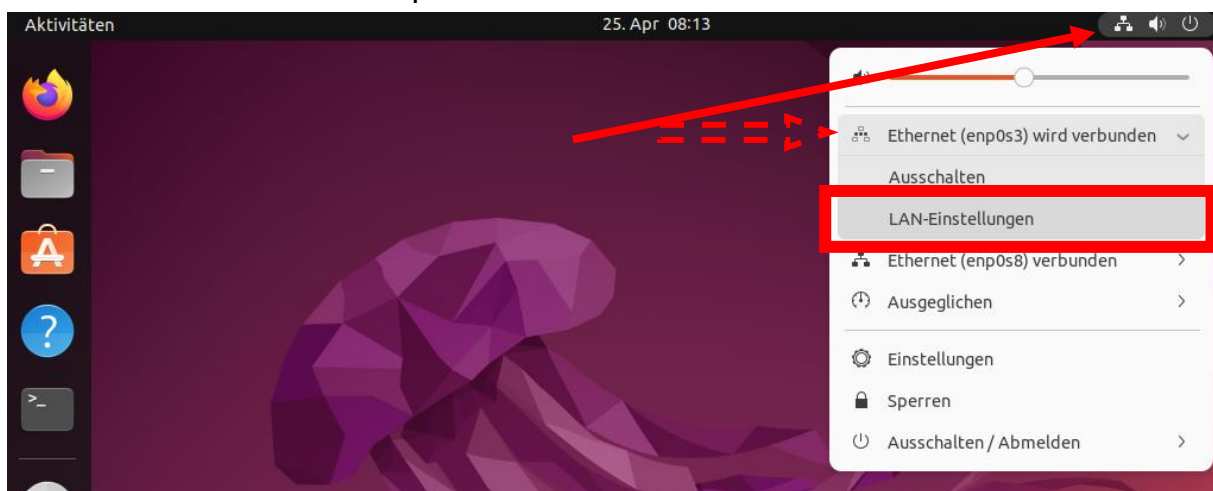
Für die Installation ist eine Internetverbindung nötig, um die benötigten Softwarepakete zu installieren.

Ubuntu installieren. Für die Installation wird keine Internetverbindung benötigt und kann später für die Paketinstallationen aktiviert werden.

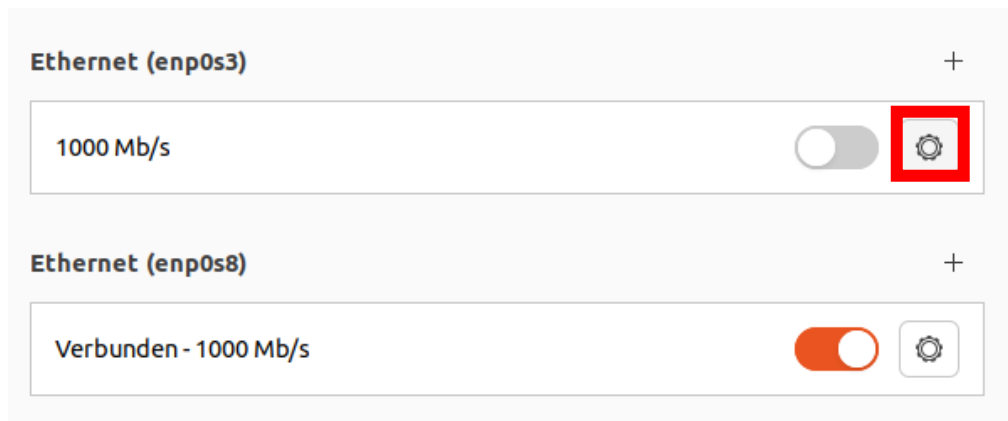


IP-Adresse konfigurieren. Falls man zwei Schnittstellen aktiviert hat, die Schnittstelle aktivieren, die nicht mit dem Internet verbunden ist.

In diesem Screenshot ist enp0s3 die interne Schnittstelle.



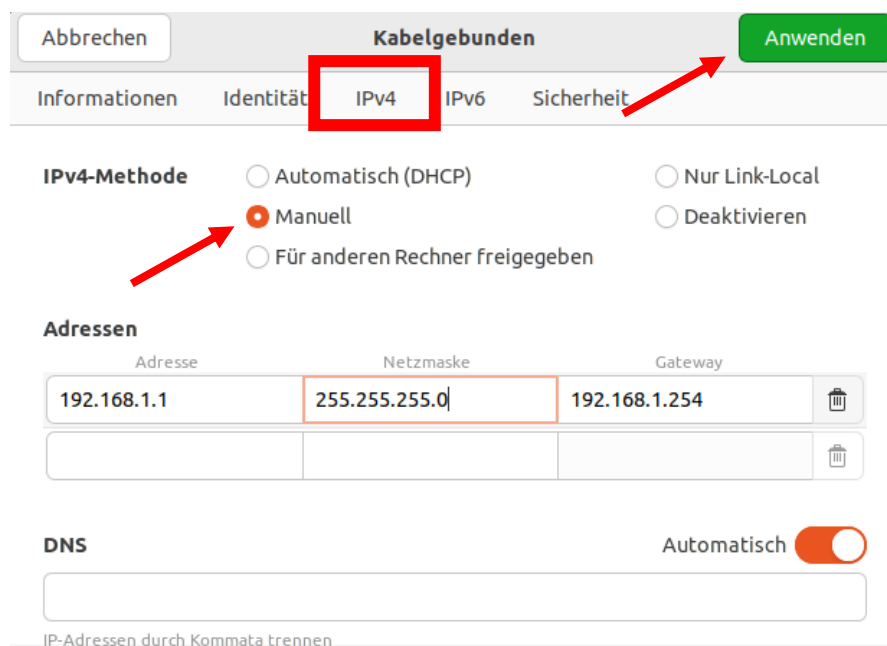
Den Zahnradzeichen anklicken



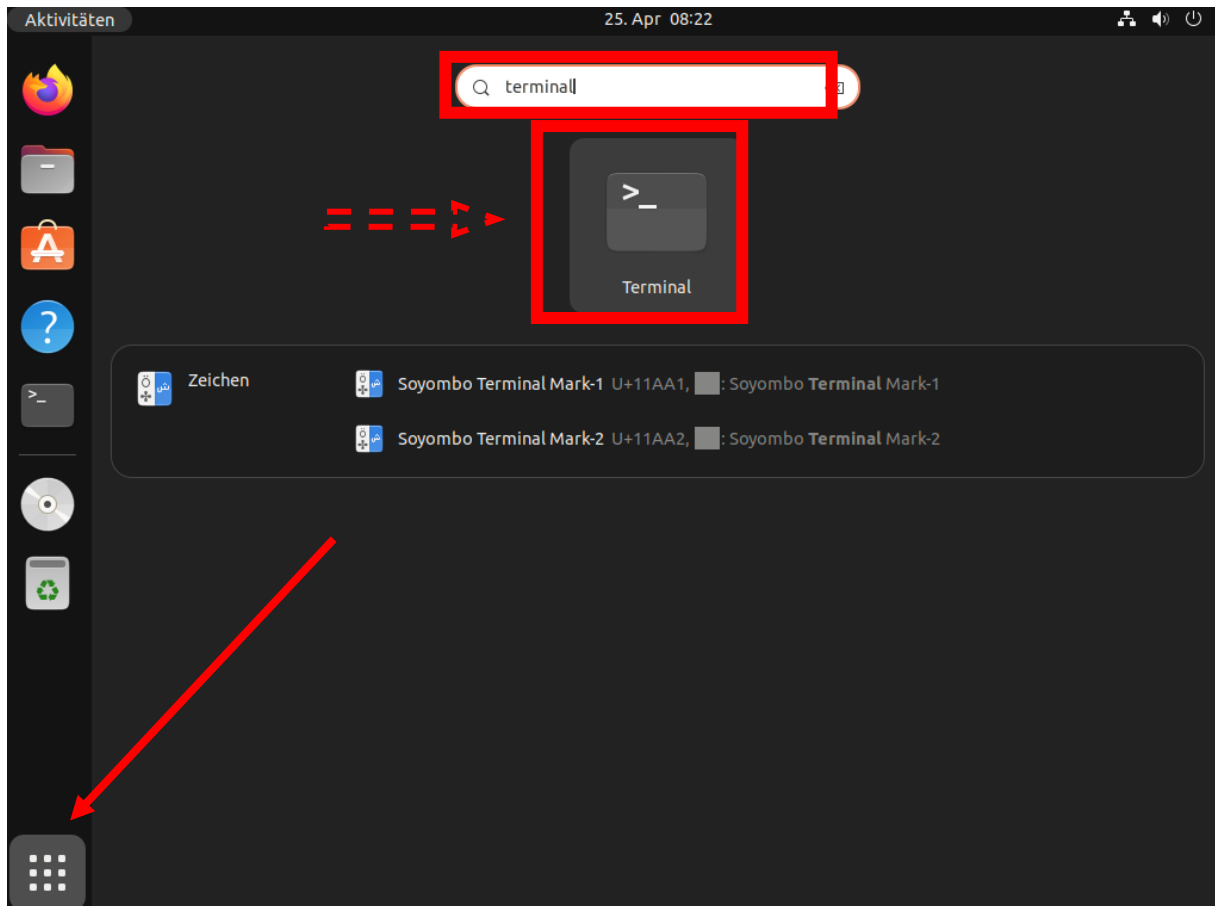
IPv4 anklicken und die Einstellungen festlegen.

Falls nötig, IPv6 klicken und „Deaktivieren“ ticken.

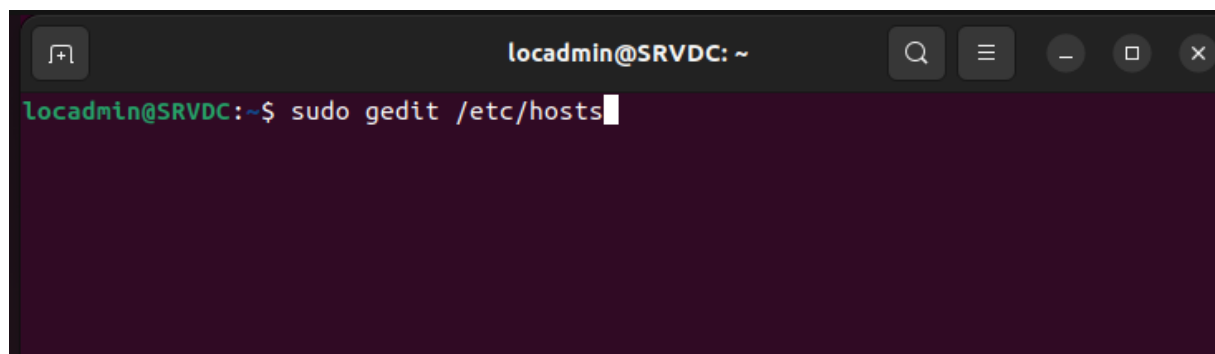
Nachdem man die Einstellungen festgelegt hat, muss man auf „Anwenden“ klicken.



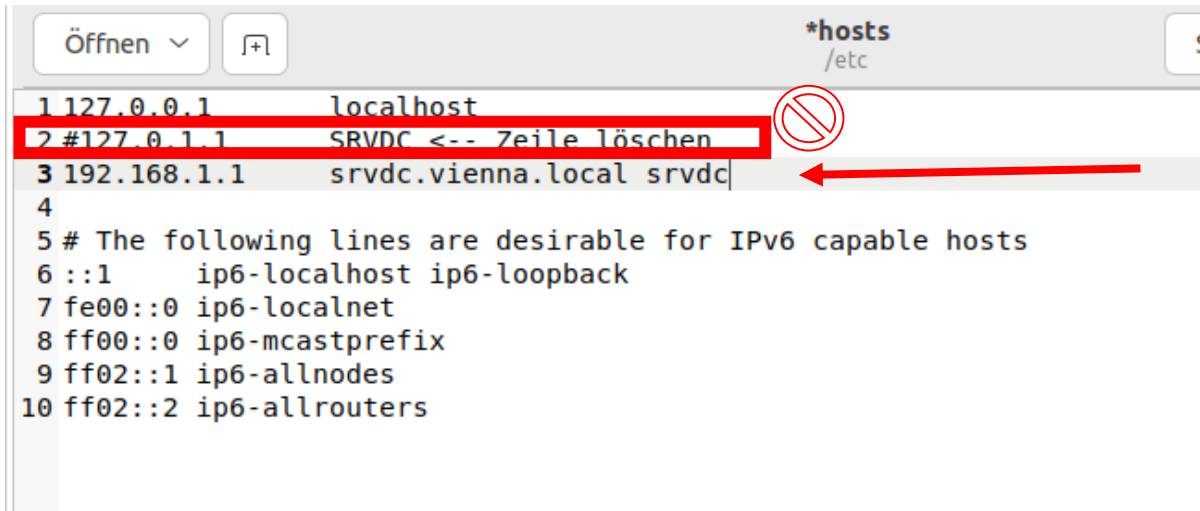
Den Knopf mit 9 Quadrate anklicken und „terminal“ in die Suchleiste eingeben.
Man kriegt das Programm „Terminal“ angezeigt.
Auf das Programm „Terminal“ anklicken, um den Terminalemulator zu öffnen.



Folgenden Befehl eingeben: „**sudo gedit /etc/hosts**“



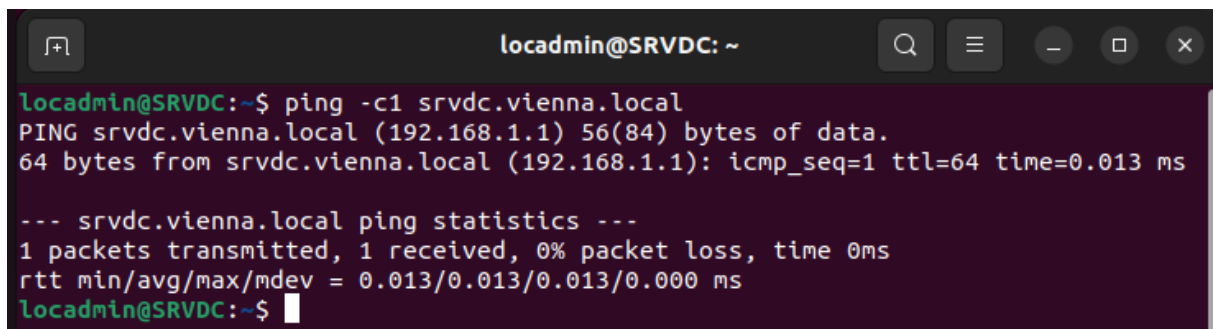
Die Zeile mit 127.0.1.1 löschen und eine neue Zeile hinschreiben:
„192.168.1.1 srvdc.vienna.local srvdc“ (IP DOMÄNENNAME NAME)
Dann auf „Speichern“ drücken.



```
*hosts
/etc

1 127.0.0.1    localhost
2 #127.0.1.1  SRVDC <-- Zeile löschen
3 192.168.1.1  srvdc.vienna.local srvdc
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1         ip6-localhost ip6-loopback
7 fe00::0     ip6-localnet
8 ff00::0     ip6-mcastprefix
9 ff02::1     ip6-allnodes
10 ff02::2    ip6-allrouters
```

Mit „ping -c1 srvdc.vienna.local“ kontrolliert man den neuen FQDN.

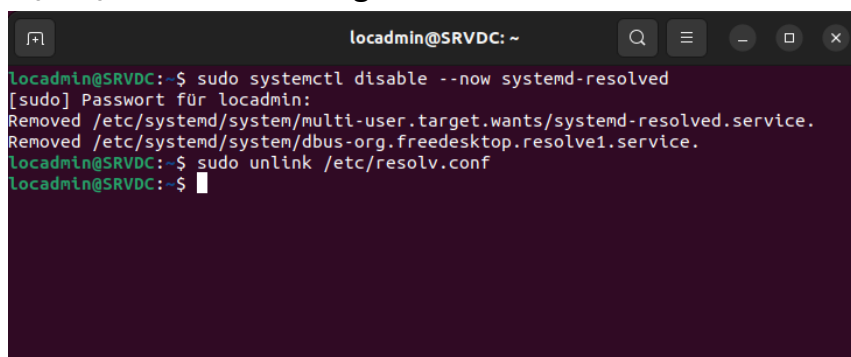


```
locadmin@SRVDC: ~
locadmin@SRVDC:~$ ping -c1 srvdc.vienna.local
PING srvdc.vienna.local (192.168.1.1) 56(84) bytes of data:
64 bytes from srvdc.vienna.local (192.168.1.1): icmp_seq=1 ttl=64 time=0.013 ms

--- srvdc.vienna.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.013/0.013/0.013/0.000 ms
locadmin@SRVDC:~$
```

Den DNS-Resolver von systemd ausschalten und manuell die DNS-Einstellungen konfigurieren.

„sudo systemctl disable --now systemd-resolved“ und
„sudo unlink /etc/resolv.conf“ eingeben.



```
locadmin@SRVDC: ~
locadmin@SRVDC:~$ sudo systemctl disable --now systemd-resolved
[sudo] Passwort für locadmin:
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
locadmin@SRVDC:~$ sudo unlink /etc/resolv.conf
locadmin@SRVDC:~$
```

resolv.conf mit „sudo gedit /etc/resolv.conf“ bearbeiten.



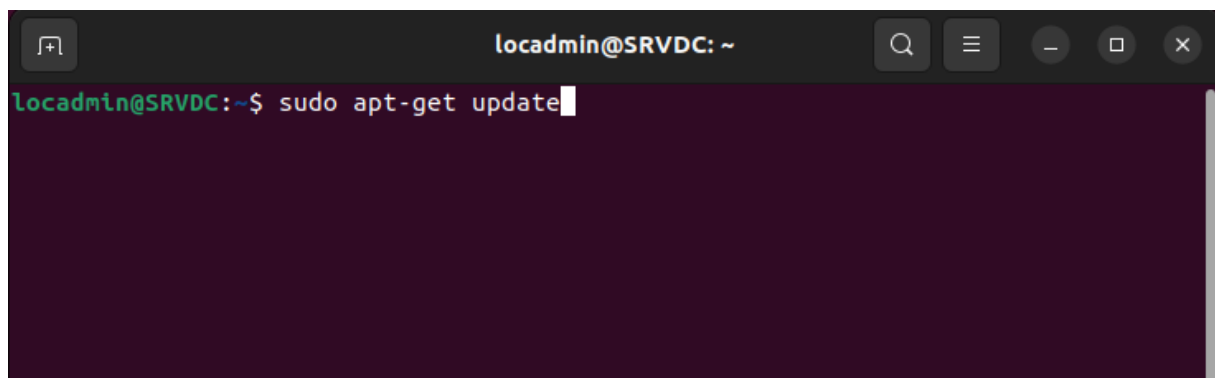
```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo gedit /etc/resolv.conf
```

Einstellungen wie im Beispiel eingeben. Die # Zeilen sind nur Kommentare.
Die Textdatei muss man unbedingt speichern.



```
*resolv.conf  
1 ##Domaenencontroller IP-Adresse  
2 nameserver 192.168.1.1  
3  
4 ##Fallback DNS-Adresse  
5 nameserver 8.8.8.8  
6  
7 ##Domaenenname  
8 search vienna local
```

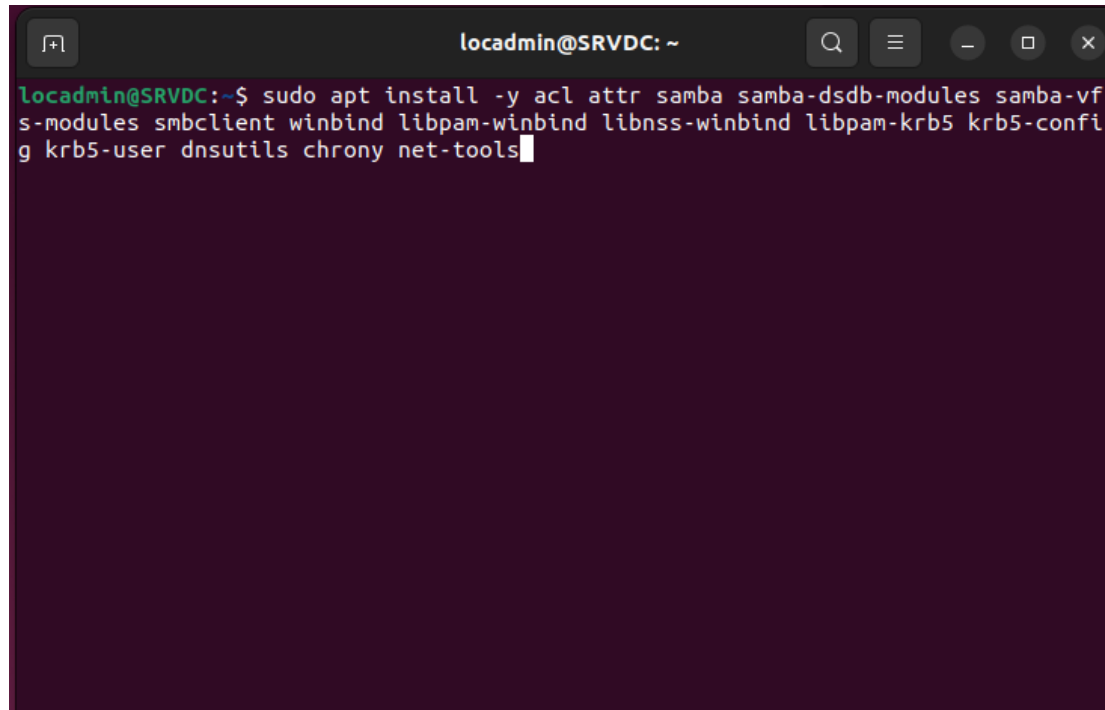
Debian und Ubuntu Repositoren aktualisieren mit „**sudo apt-get update**“



```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo apt-get update
```

Alle Pakete mit:

„**sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony net-tools**“

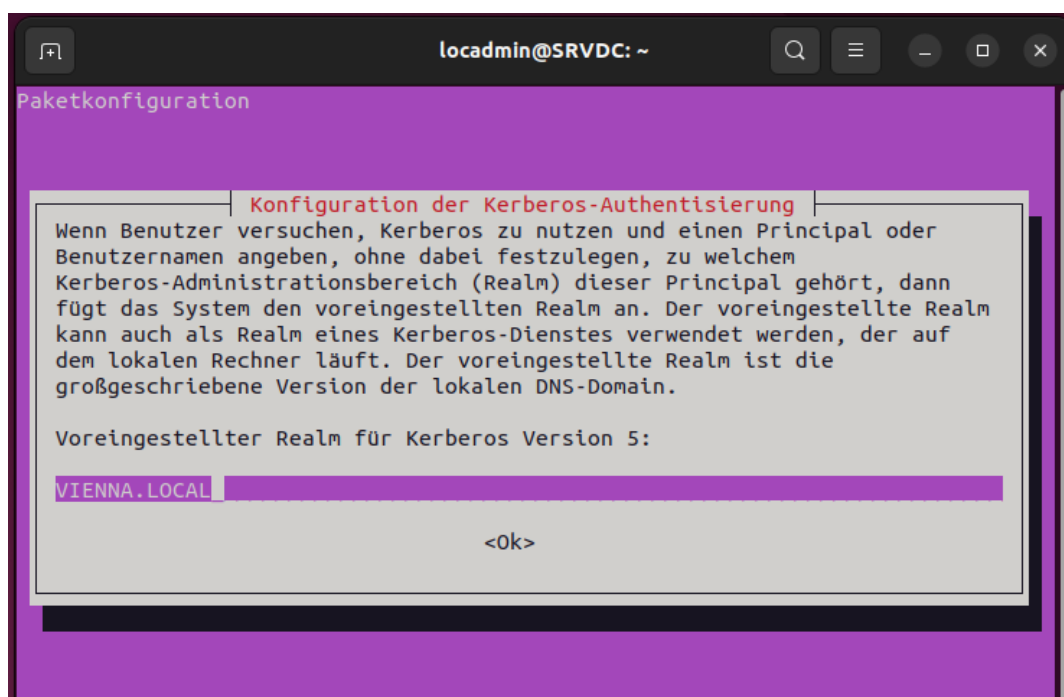
A terminal window titled 'locadmin@SRVDC: ~' with search, menu, and window control icons. The command 'sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony net-tools' is entered and executed, with a cursor at the end of the line.

```
locadmin@SRVDC:~$ sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony net-tools
```

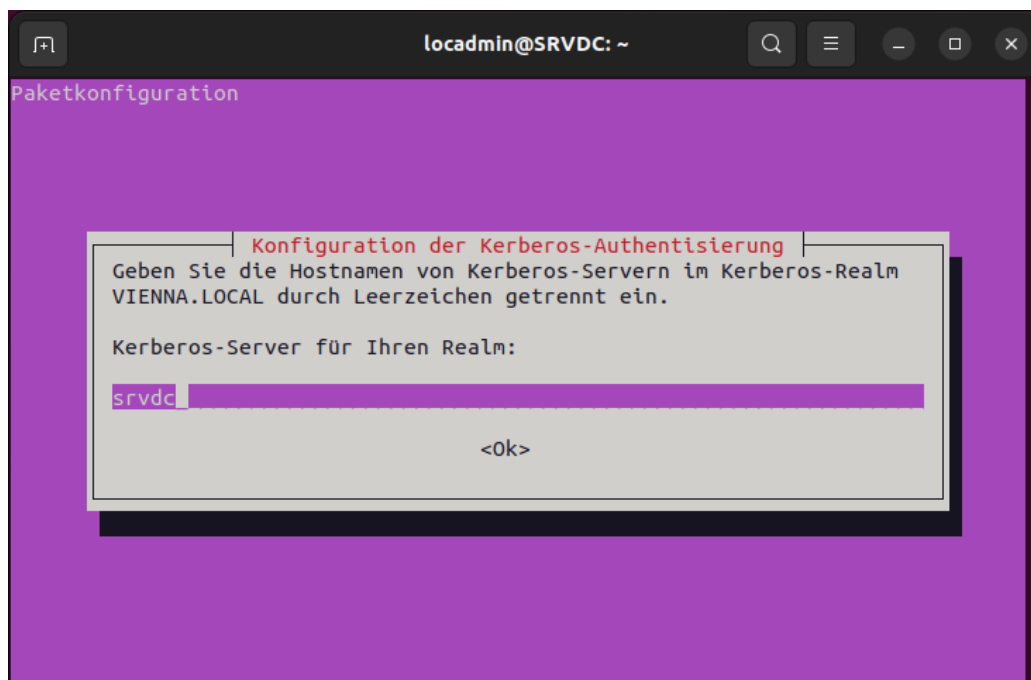
Während der Installation öffnet sich im Terminal der Kerberos-Setup.

Man kriegt automatisch den Domänennamen hinzugefügt.

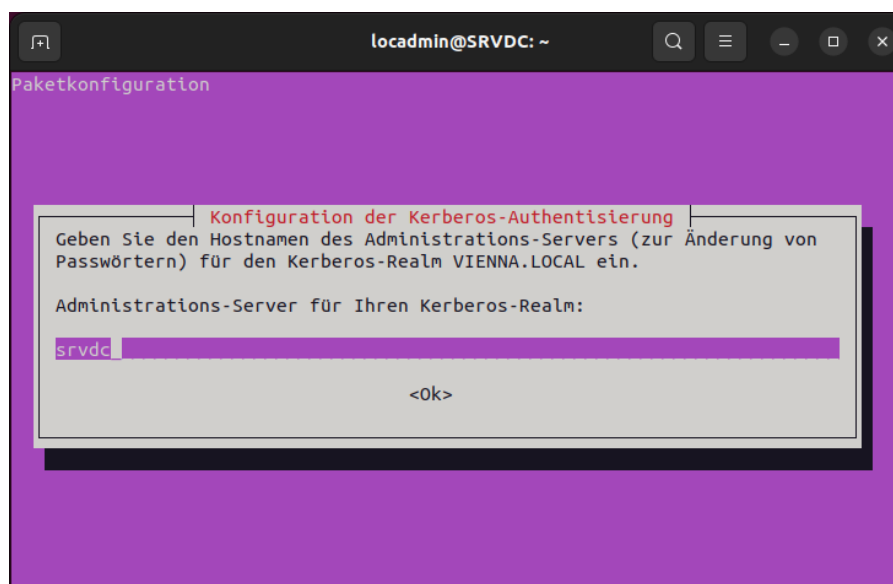
Den Tab-Knopf drücken und Enter drücken.



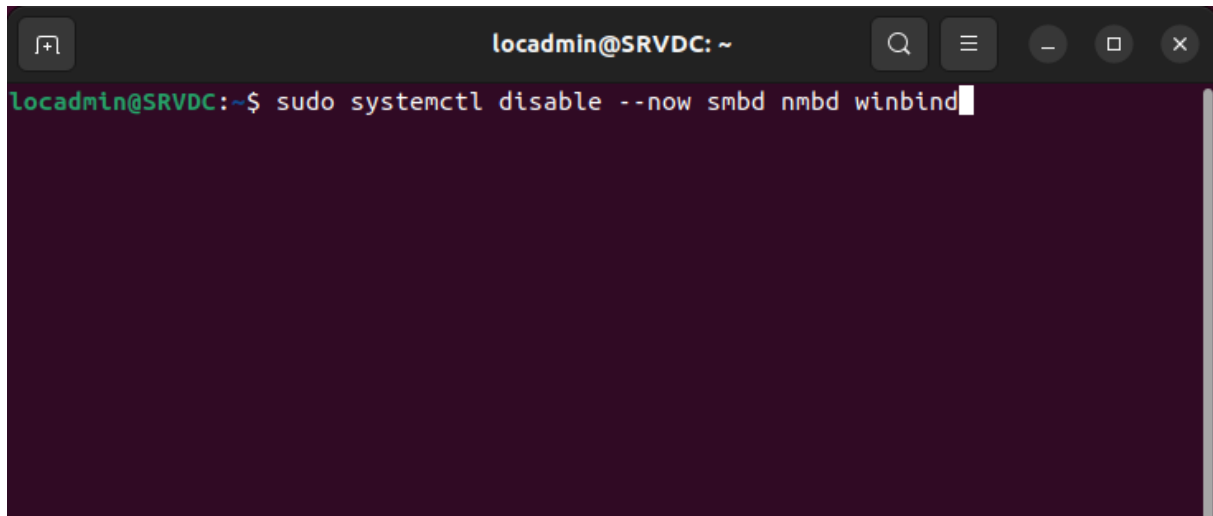
Den Domänencontrollernamen eingeben (in meinem Fall wäre es srvdc)
Tab und Enter.



→DC-Name eingeben. Tab und Enter.

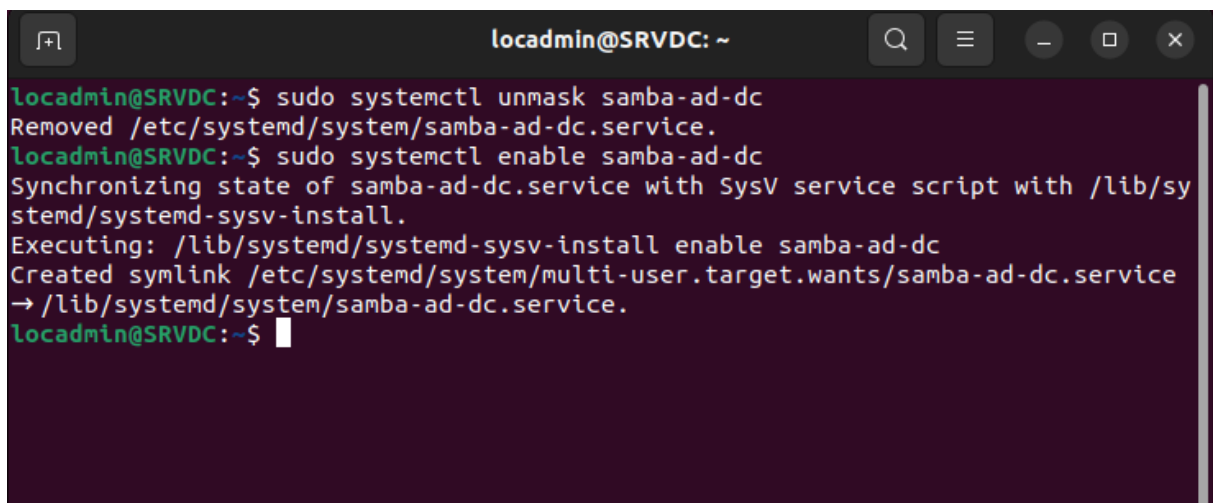


Die unbenötigte Dienste ausschalten mit
„**sudo systemctl disable --now smb** **smbd** **nmbd** **winbind**“

A terminal window titled 'locadmin@SRVDC: ~' with search, menu, and window control icons in the title bar. The command 'sudo systemctl disable --now smb smbd nmbd winbind' is entered at the prompt. The terminal background is dark purple.

```
locadmin@SRVDC:~$ sudo systemctl disable --now smb smbd nmbd winbind
```

Die Domänencontroller-Dienste mit
„**sudo systemctl unmask samba-ad-dc**“ und
„**sudo systemctl enable samba-ad-dc**“ aktivieren.

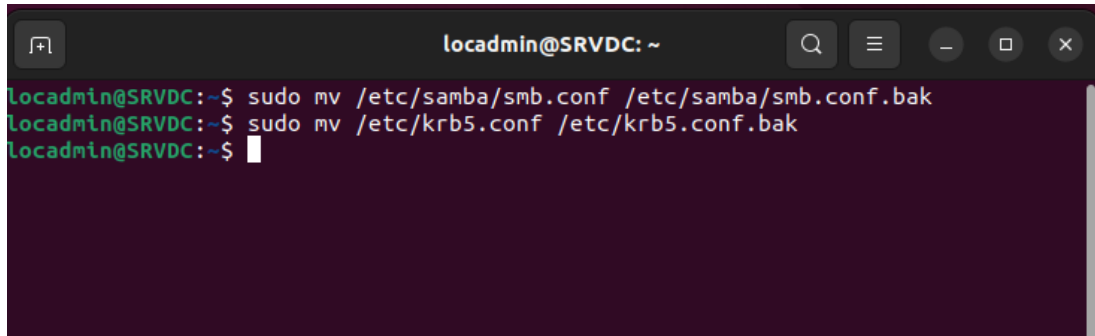
A terminal window titled 'locadmin@SRVDC: ~' with search, menu, and window control icons in the title bar. The commands 'sudo systemctl unmask samba-ad-dc' and 'sudo systemctl enable samba-ad-dc' are entered. The output shows the removal of the service file and the synchronization of the service state with SysV. The terminal background is dark purple.

```
locadmin@SRVDC:~$ sudo systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.
locadmin@SRVDC:~$ sudo systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
Created symlink /etc/systemd/system/multi-user.target.wants/samba-ad-dc.service
→ /lib/systemd/system/samba-ad-dc.service.
locadmin@SRVDC:~$
```


Weil man neue SMB und Kerberosconfigfiles erstellen muss, ist es empfohlen, die conf-Dateien aufzubewahren, falls die conf-Datei beschädigt worden sind und die Samba-Software nicht mehr funktioniert.

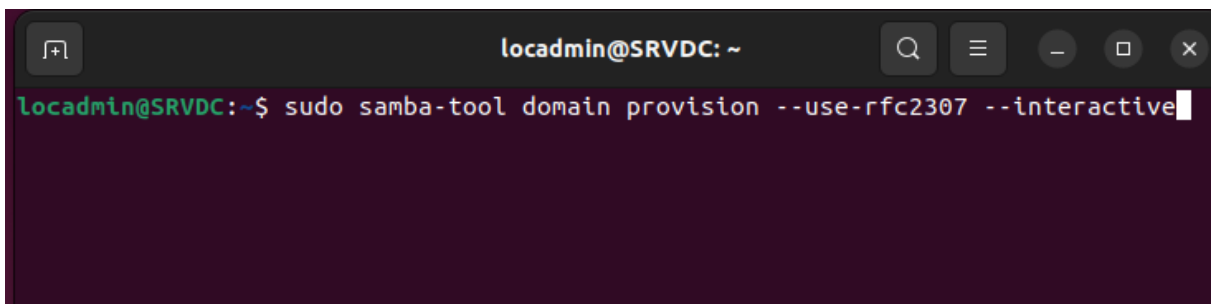
„**sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak**“

„**sudo mv /etc/krb5.conf /etc/krb5.conf.bak**“



```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak  
locadmin@SRVDC:~$ sudo mv /etc/krb5.conf /etc/krb5.conf.bak  
locadmin@SRVDC:~$
```

Mit „**sudo samba-tool domain provision --use-rfc2307 --interactive**“ erstellt man spezielle Samba und Kerberos conf-Datei für den Domänencontroller.

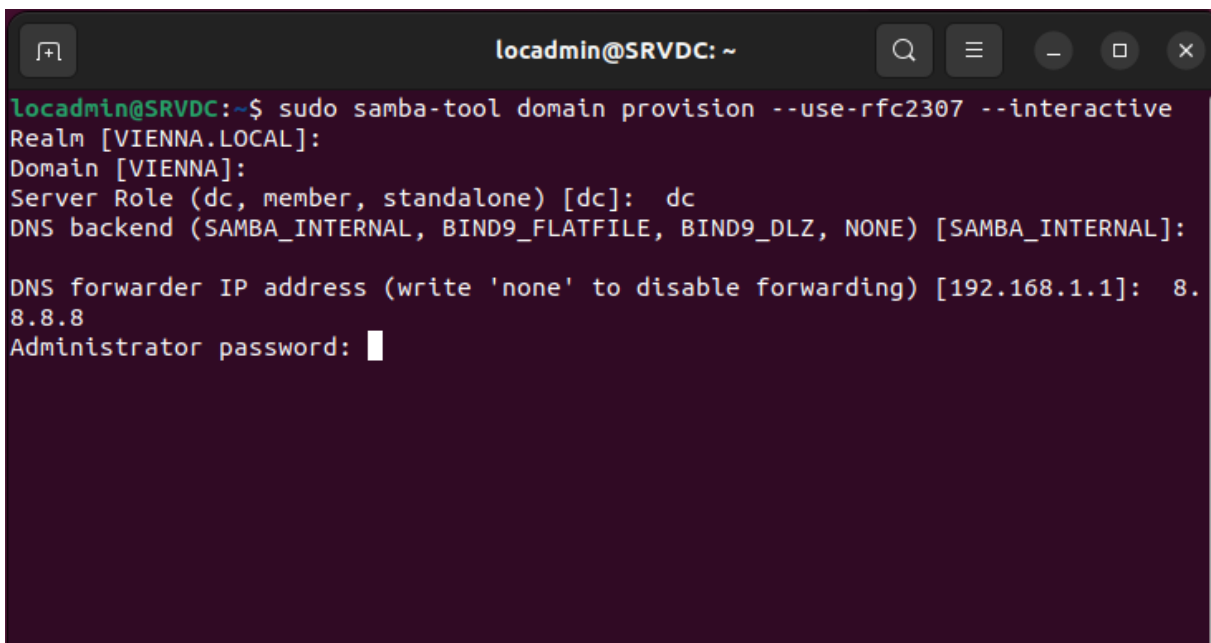


```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo samba-tool domain provision --use-rfc2307 --interactive
```

Die ersten vier Setupfragen die Entertaste drücken. Bei der fünften Frage (DNS forwarder) kann man eine DNS-Resolver Adresse eingeben.

Ich habe die Google Resolver DNS Adresse eingegeben.

Als letztes den Administratorpasswort eingeben.



```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo samba-tool domain provision --use-rfc2307 --interactive  
Realm [VIENNA.LOCAL]:  
Domain [VIENNA]:  
Server Role (dc, member, standalone) [dc]: dc  
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:  
  
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.1.1]: 8.  
8.8.8  
Administrator password:
```

„sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf“

```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

„sudo systemctl start samba-ad-dc“

```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo systemctl start samba-ad-dc  
locadmin@SRVDC:~$
```

In diesen Screenshot sieht man, dass Kerberos und Samba erfolgreich als Domänencontroller konfiguriert wurde.

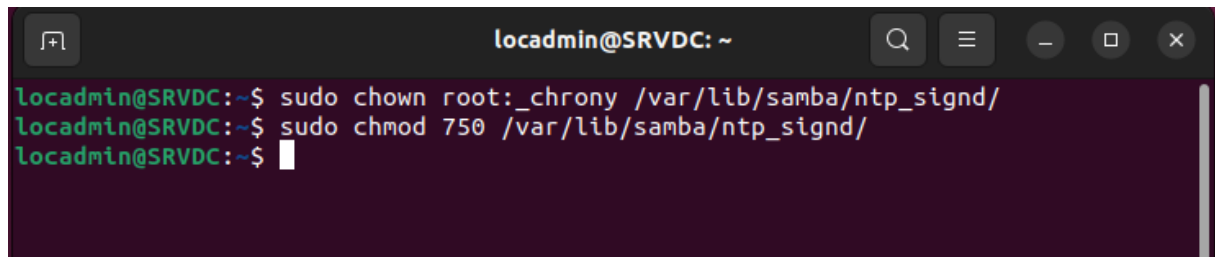
```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ smbclient //localhost/netlogon -U Administrator -c 'ls'  
Password for [VIENNA\Administrator]:  
.  
..  
25108740 blocks of size 1024. 14672316 blocks available  
locadmin@SRVDC:~$ kinit administrator  
Passwort für administrator@VIENNA.LOCAL:  
Warnung: Ihr Passwort wird in 41 Tagen am Di 06 Jun 2023 09:09:38 ablaufen.  
locadmin@SRVDC:~$ klist  
Ticketzwischenspeicher: FILE:/tmp/krb5cc_1000  
Standard-Principal: administrator@VIENNA.LOCAL  
  
Valid starting Expires Service principal  
2023-04-25 09:17:52 2023-04-25 19:17:52 krbtgt/VIENNA.LOCAL@VIENNA.LOCAL  
erneuern bis 2023-04-26 09:17:50  
locadmin@SRVDC:~$
```

Aus Bug- und Sicherheitsgründen muss man auch NTP (Network Time Protocol; Zeitserver)

Die Berechtigungen der ntp_signd soll an chrony zugewiesen werden.

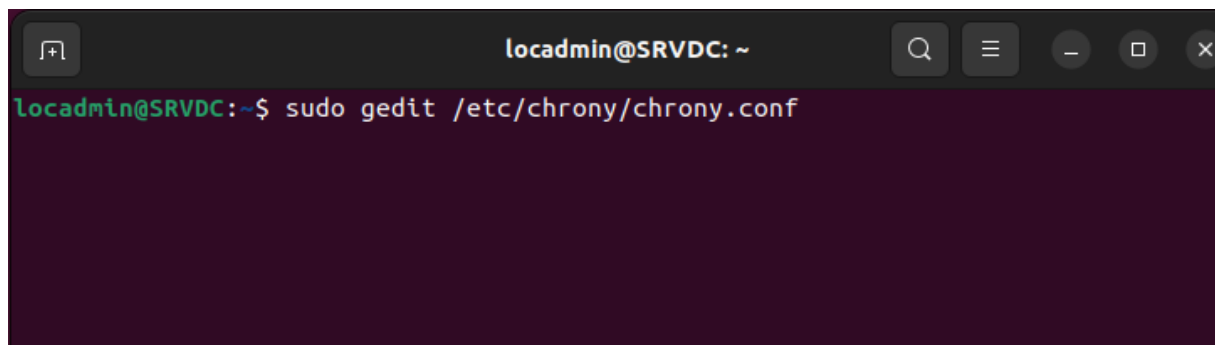
„**sudo chown root:_chrony /var/lib/samba/ntp_signd/**“

„**sudo chmod 750 /var/lib/samba/ntp_signd/**“



```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo chown root:_chrony /var/lib/samba/ntp_signd/  
locadmin@SRVDC:~$ sudo chmod 750 /var/lib/samba/ntp_signd/  
locadmin@SRVDC:~$
```

Die chrony conf-Datei mit „**sudo gedit /etc/chrony/chrony.conf**“ öffnen.



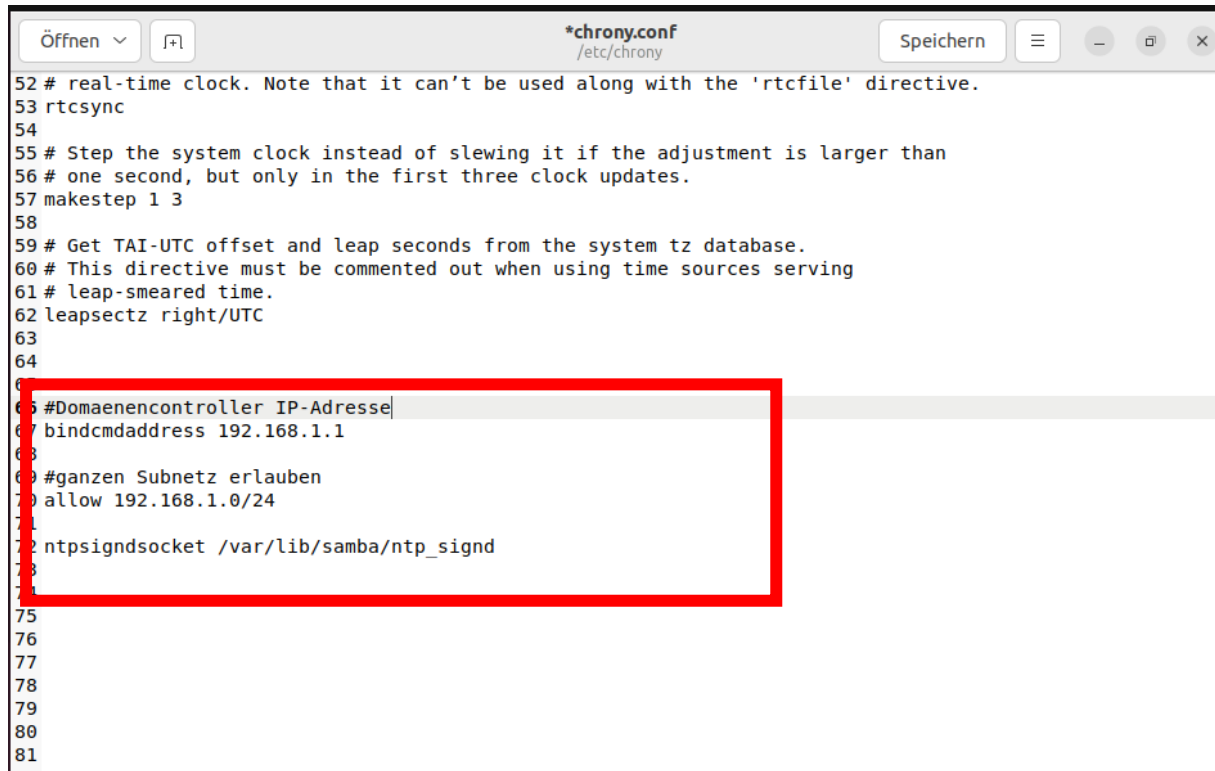
```
locadmin@SRVDC: ~  
locadmin@SRVDC:~$ sudo gedit /etc/chrony/chrony.conf
```

Ganz unten scrollen und die folgende Einträge hinzufügen.

„bindcmdaddress 192.168.1.1“

„allow 192.168.1.0/24“

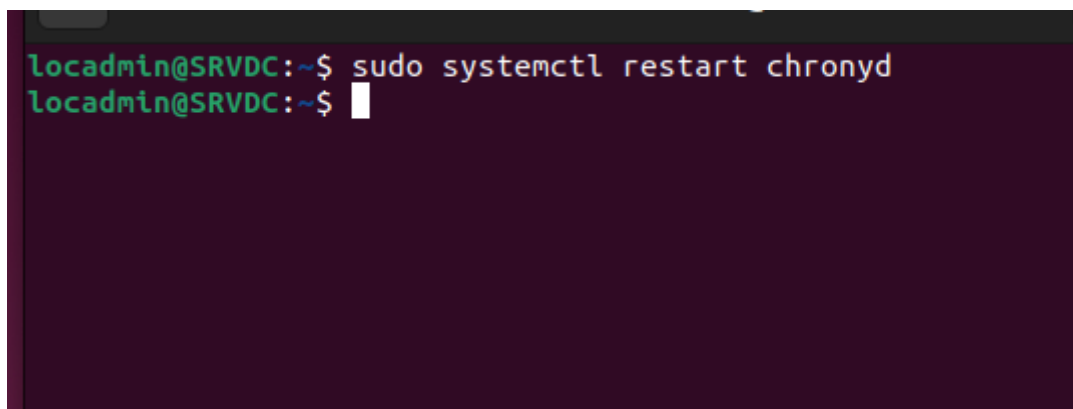
„ntpsigndsocket /var/lib/samba/ntp_signd“



```
*chrony.conf
/etc/chrony

52 # real-time clock. Note that it can't be used along with the 'rtcfile' directive.
53 rtsync
54
55 # Step the system clock instead of slewing it if the adjustment is larger than
56 # one second, but only in the first three clock updates.
57 makestep 1 3
58
59 # Get TAI-UTC offset and leap seconds from the system tz database.
60 # This directive must be commented out when using time sources serving
61 # leap-smearred time.
62 leapsectz right/UTC
63
64
65 #Domainencontroller IP-Adresse
66 bindcmdaddress 192.168.1.1
67
68 #ganzen Subnetz erlauben
69 allow 192.168.1.0/24
70
71 ntpsigndsocket /var/lib/samba/ntp_signd
72
73
74
75
76
77
78
79
80
81
82
```

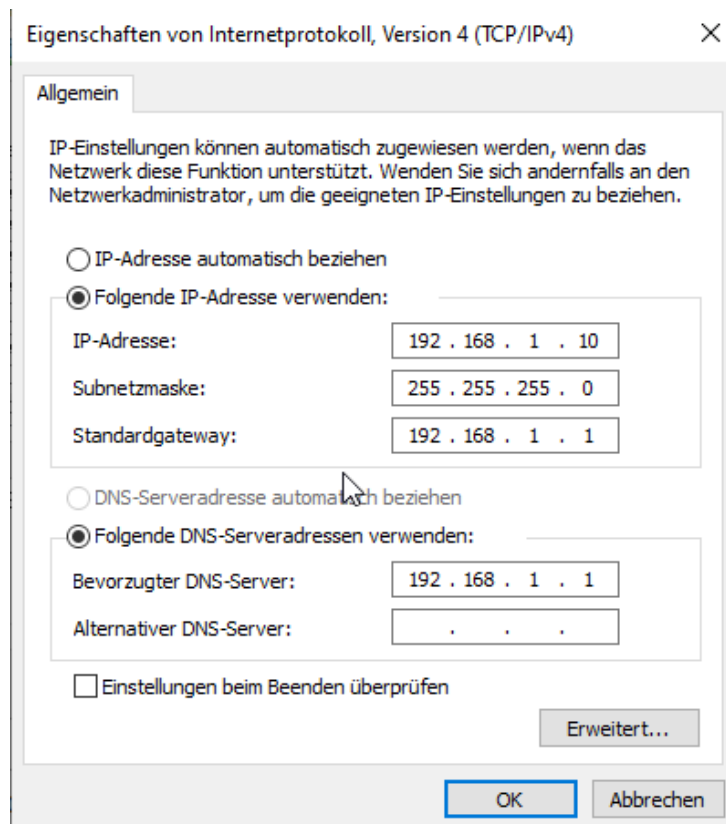
chronyd mit „**sudo systemctl restart chronyd**“ neustarten.



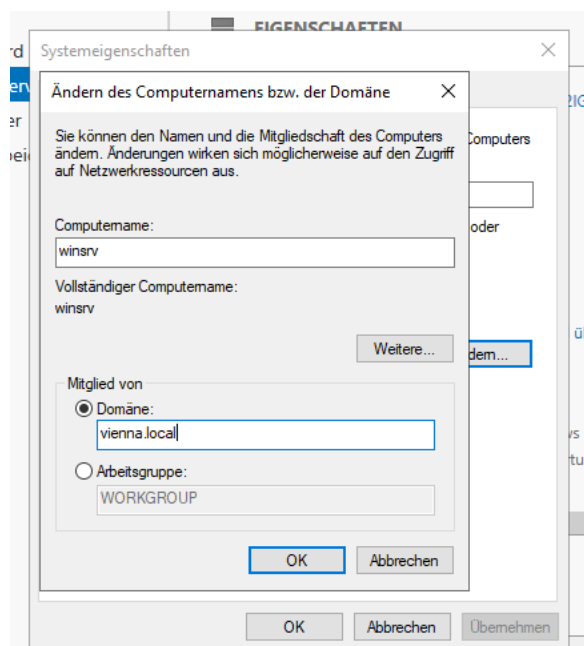
```
locadmin@SRVDC:~$ sudo systemctl restart chronyd
locadmin@SRVDC:~$
```

→ Windows Server

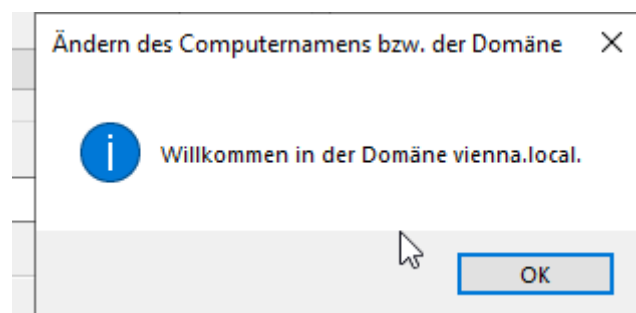
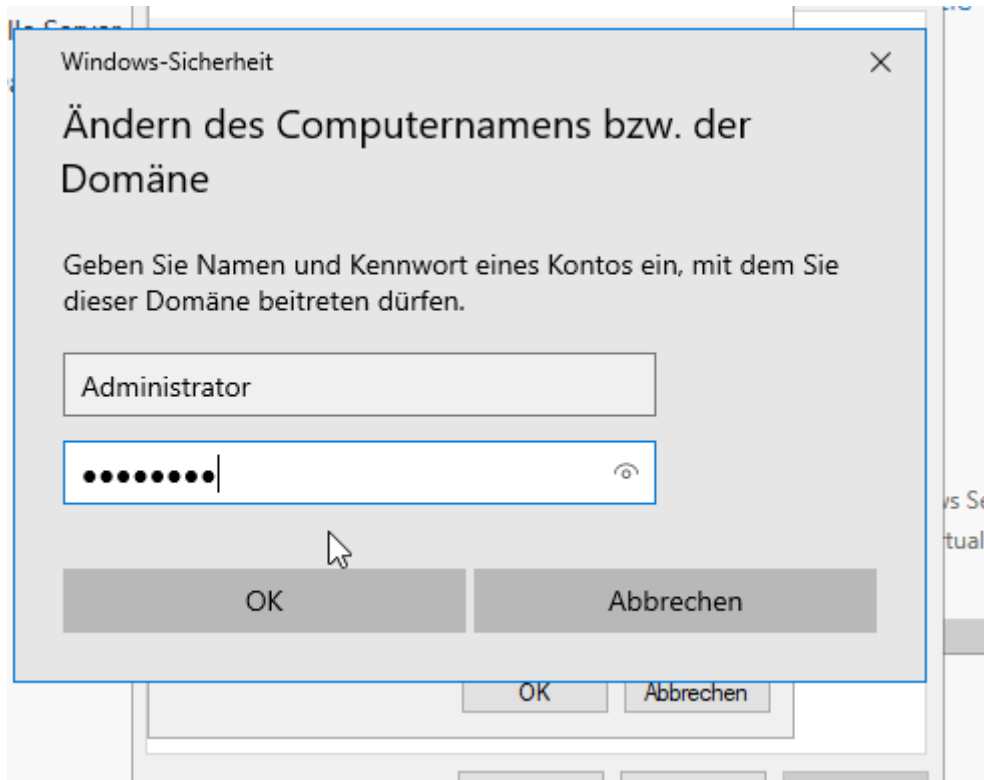
Netzwerkeinstellungen konfigurieren. Linux-Rechner soll als DNS-Server eingetragen sein.



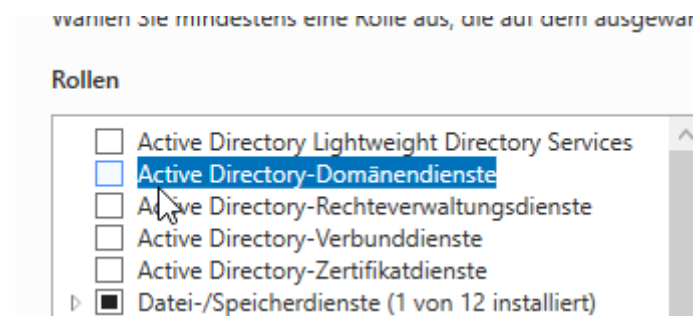
Server in die Domäne hinzufügen.



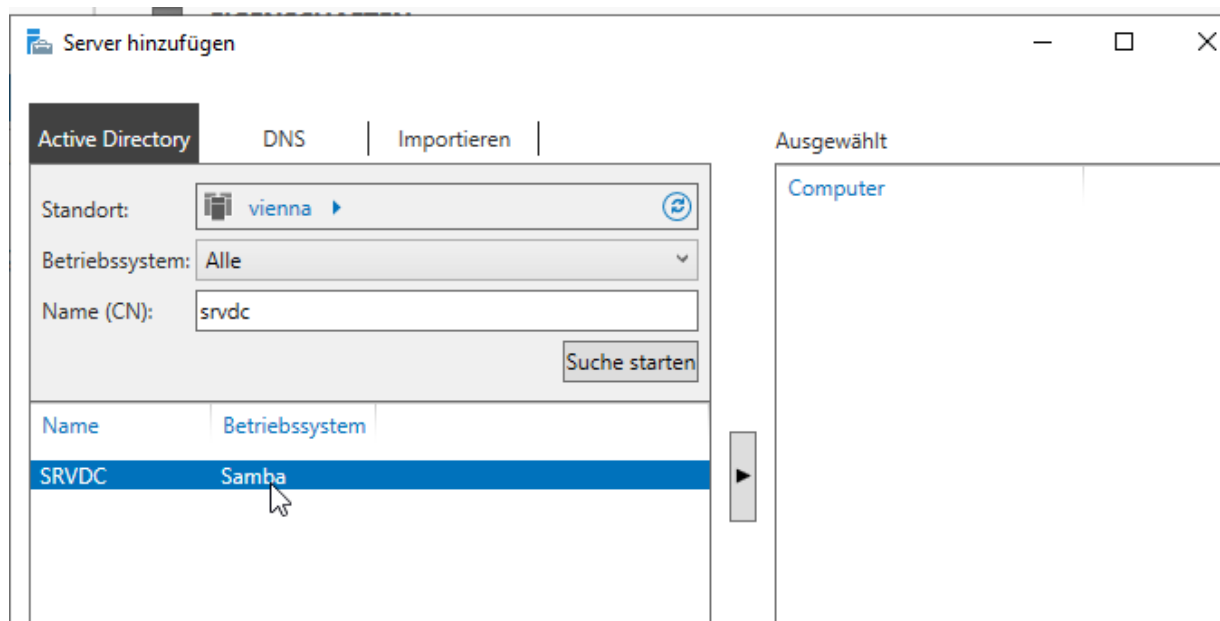
Administrator als Benutzername eingeben und das Kennwort, den man bei dem Konfigurieren von Samba und Kerberos eingegeben hat eingeben.



Active-Directory-Domänendienste installieren.



Linux-DC suchen und hinzufügen.



Jetzt kann man die AD-Benutzer und Computer hinzufügen.

