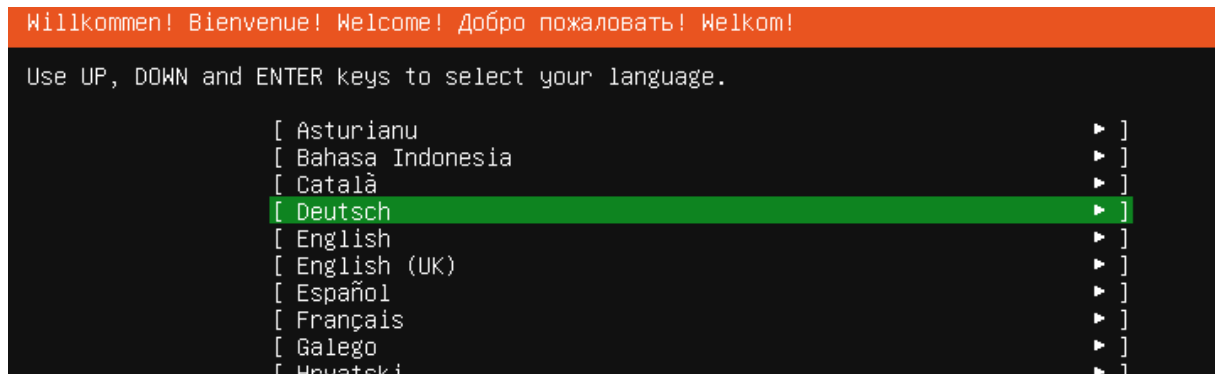
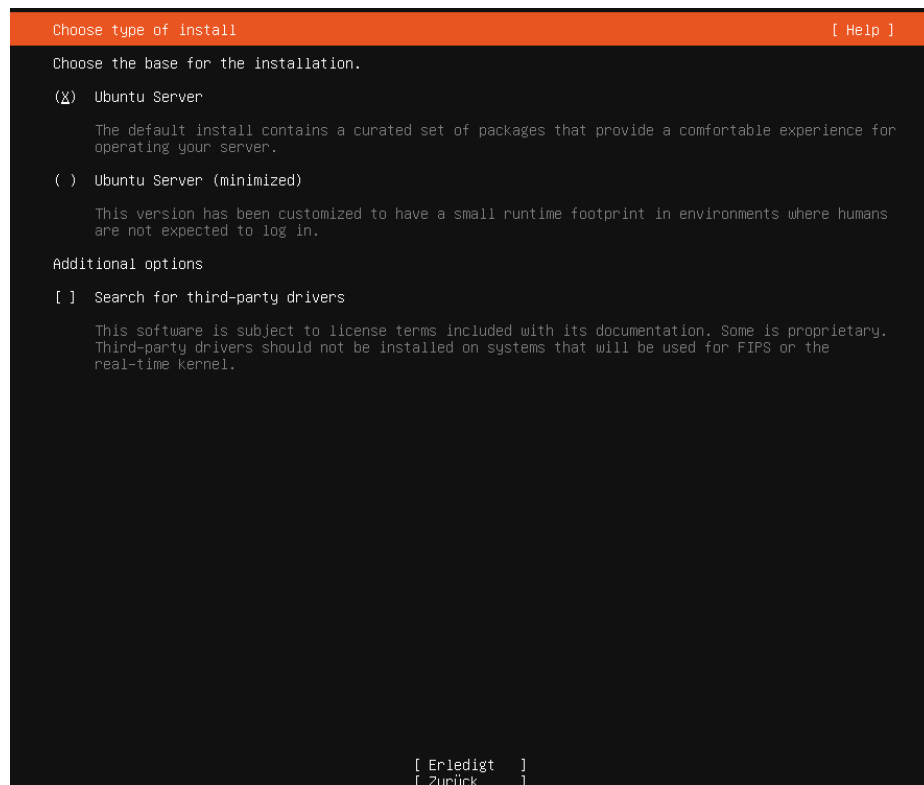


Ubuntu Server als Domänen-Controller

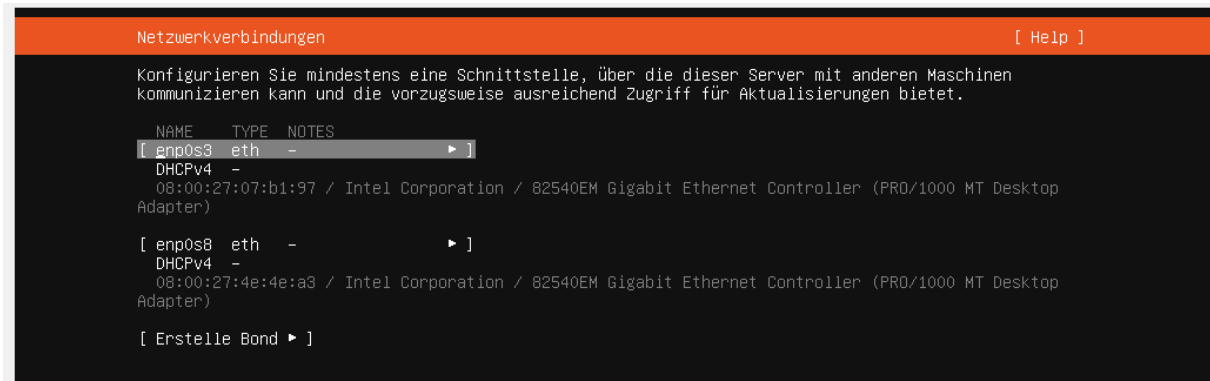
Deutsch als Installationssprache auswählen.



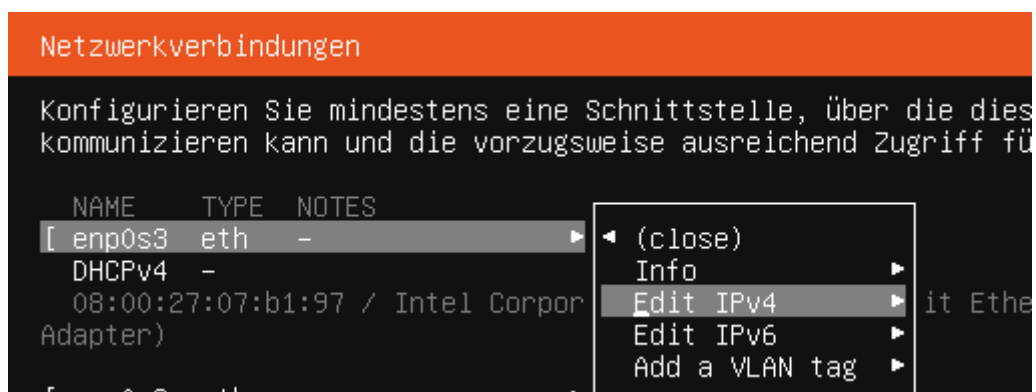
Drei Mal den Tab-Knopf drücken und mit Enter bestätigen.



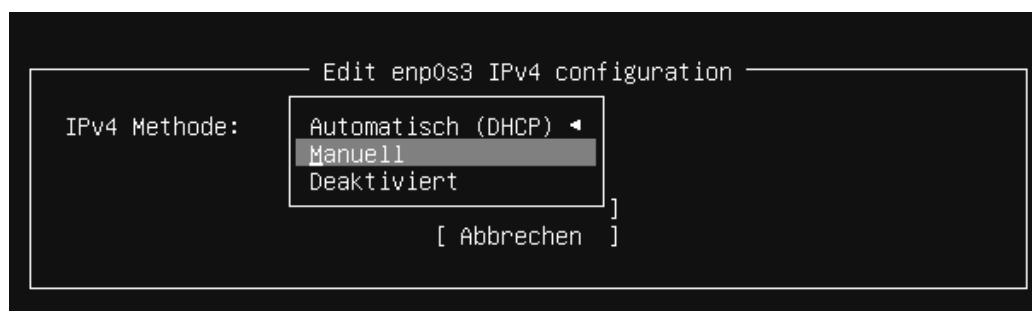
Diesen Setup navigiert man mit den Pfeiltasten. Den ersten Netzwerkadapter auswählen. Enter drücken.



„Edit IPv4“ auswählen und Enter drücken.



→Manuell



Einstellungen eingeben. → Speichern

— Edit enp0s3 IPv4 configuration —

IPv4 Methode: [Manuell ▼]

Subnetz: 192.168.1.0/24

Adresse: 192.168.1.1

Gateway: 192.168.1.254

Namensserver: 192.168.1.1_
IP addresses, comma separated

Suchdomänen:
Domains, comma separated

[Speichern]
[Abbrechen]

Falls nötig, Proxy-Adresse eingeben

Proxy konfigurieren [Help]

Wenn dieses System einen Proxy erfordert, um mit dem Internet verbunden zu werden, geben Sie seine Details hier an.

Proxy-Adresse: http://172.16.0.252:800
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[user][:pass}@host[:port]/".

[Erledigt]
[Zurück]

Festplatte/Partition auswählen.

Begleitete Speicherplatzkonfiguration [Help]

Konfiguriere ein geführtes Speicherlayout oder erstelle ein eigenes:

(X) Eine ganze Festplatte verwenden
[VBOX_HARDDISK_VB2d47b911-10c41333 local disk 25.000G ▼]

[X] Diese Festplatte als LVM-Gruppe konfigurieren
[] Die LVM-Gruppe mit LUKS verschlüsseln
Passphrase:
Passphrase bestätigen:

() Benutzerdefinierte Partitionierung

[Erledigt]
[Zurück]

LOGIN

Profileinrichtung [Help]

Geben Sie den Benutzernamen und das Passwort ein, mit dem Sie sich am System anmelden möchten. Sie können den SSH-Zugang auf dem nächsten Bildschirm konfigurieren, aber für sudo wird weiterhin ein Passwort benötigt.

Ihr Name:

Name Ihres Servers:
The name it uses when it talks to other computers.

Bitte Benutzernamen auswählen:

Bitte Passwort auswählen:

Passwort bestätigen:

Jetzt neustarten

```
Installation komplett! [ Help ]

    configuring mount: mount-0
    executing curtin install extract step
    curtin command install
    writing install sources to disk
    running 'curtin extract'
    curtin command extract
    acquiring and extracting image from cp:///tmp/tmpzbd4q2g/mount
    executing curtin install curthooks step
    curtin command install
    configuring installed system
    running 'mount --bind /cdrom /target/cdrom'
    running 'curtin in-target -- setupcon --save-only'
    curtin command in-target
    running 'curtin curthooks'
    curtin command curthooks
    configuring apt configuring apt
    installing missing packages
    installing packages on target system: ['efibootmgr', 'grub-efi-amd64',
'grub-efi-amd64-signed', 'shim-signed']
    configuring iscsi service
    configuring raid (mdadm) service
    installing kernel
    setting up swap
    apply networking config
    writing etc/fstab
    configuring multipath
    updating packages on target system
    configuring pollinate user-agent on target
    updating initramfs configuration
    configuring target system bootloader
    installing grub to target devices
final system configuration
    configuring cloud-init
    calculating extra packages to install
    downloading and installing security updates
    curtin command in-target
    restoring apt configuration
    curtin command in-target
subiquity/Late/run

[ View full log ]
[ Jetzt neustarten ]
```

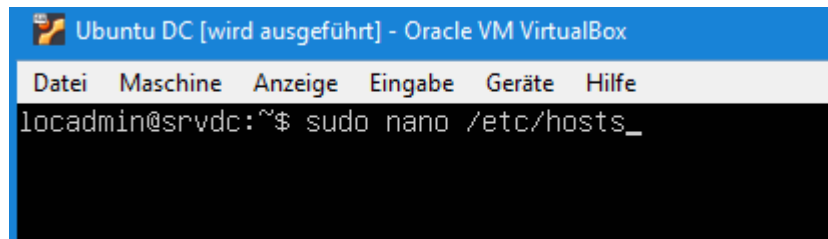
Nachdem man den Server neustartet, muss man sich anmelden.

Enter drücken. Man muss den lokalen Administratorbenutzer eingeben.

```
4qXobTlKSfntR52MOB2SNxpARElcyUfP5KDWL+QNNBN9vpt1f1w2CU1LWAPU15uok62JOPDH/awcd/m6FvCRBo2fx0f j62FA1sm0910CpKUGU1VS/101fMDKXA1WU0
n2c9IcHmvuEbiaQgtOKxLMzbmVMknkdhc02KKVsTEvp/1hgD4fTngNmTukaCq/ILGNoCno0Xq+1H1fc5XHEyK2BkGXyYdX01KGyfkf jvz8kgpq8P8fiMYbmz4qtgvQk
QWNIv3UfuDIyhetYDQM0Qg7hIe0UqsNudMS0LSGJOUGL2u5C/YN1G1U/8U3xMtYh4LV1UkxgDk119sJatg4/S1FC7J+qUv0TOA8a3BK/hkvIOFA/UwR1hE1TffVMUG5
D3wXcuNzdxjI4Rpm3YSA25nAYKEWLwDr2XR22mM= root@srvdc
-----END SSH HOST KEY KEYS-----
[ 42.591902] cloud-init[1290]: Cloud-init v. 22.4.2-0ubuntu0~22.04.1 finished at Tue, 25 Apr 2023 08:38:51 +0000. Datasource [
ataSourceNone. Up 42.58 seconds
[ 42.592701] cloud-init[1290]: 2023-04-25 08:38:51,213 - cc_final_message.py[WARNING]: Used fallback datasource
[ OK ] Finished Execute cloud user/final scripts.
[ OK ] Reached target Cloud-init target.

srvdc login:
srvdc login: locadmin
Password:
```

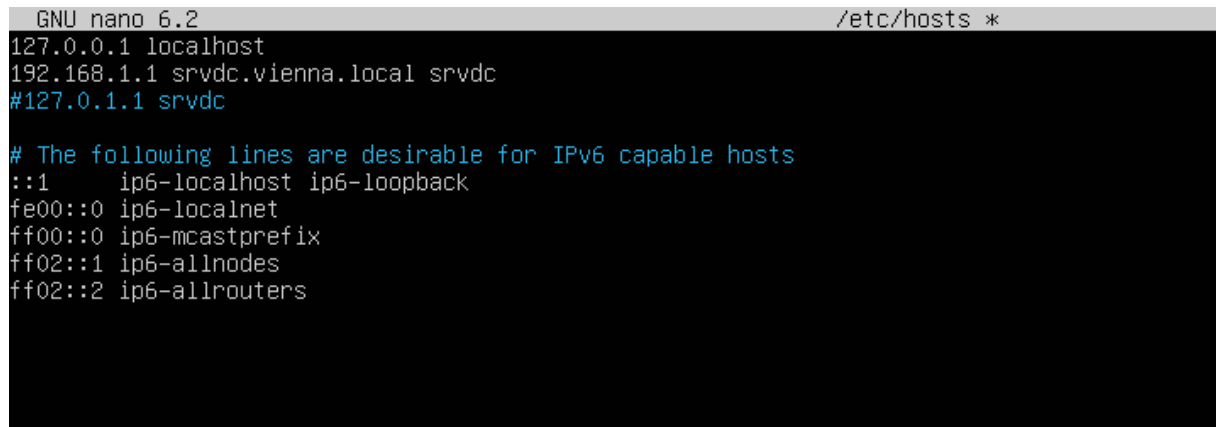
„sudo nano /etc/hosts“ eingeben.



```
Ubuntu DC [wird ausgeführt] - Oracle VM VirtualBox
Datei  Maschine  Anzeige  Eingabe  Geräte  Hilfe
locadmin@srvdc:~$ sudo nano /etc/hosts_
```

Gesteuert wird mit den Pfeiltasten. Die Zeile beginnend mit 127.0.1.1 mit der Rautezeichen kommentieren lassen und in einer neuen Zeile „192.168.1.1 srvdc.vienna.local srvdc“ (IP DOMÄNENNAME NAME) schreiben. Mit STRG + Linke/Rechte Pfeiltasten kann man schneller navigieren.

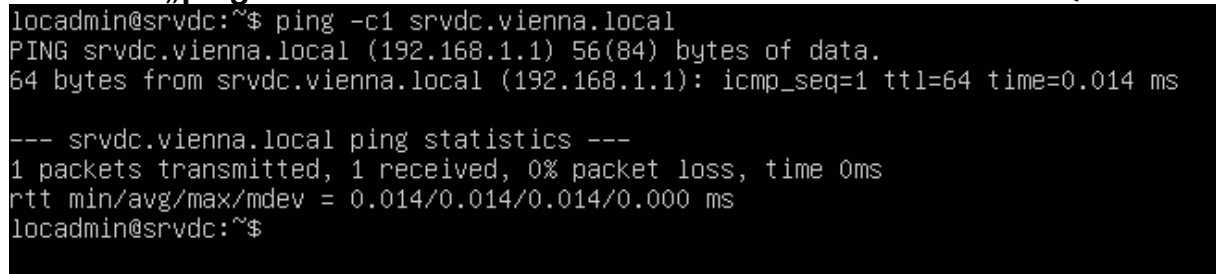
STRG+S und dann STRG+X drücken, um die Änderungen abzuspeichern.



```
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
192.168.1.1 srvdc.vienna.local srvdc
#127.0.1.1 srvdc

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

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



```
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=0.014 ms

--- srvdc.vienna.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.014/0.014/0.014/0.000 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:~$ sudo systemctl disable --now systemd-resolved
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
locadmin@srvdc:~$ sudo unlink /etc/resolv.conf
locadmin@srvdc:~$ _
```

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

```
locadmin@srvdc:~$ sudo nano /etc/resolv.conf
```

Einstellungen wie im Beispiel eingeben.

Die Textdatei muss man unbedingt speichern. (STRG+S → STRG+X)

```
GNU nano 6.2 /etc/resolv.conf *
##DOMAINCONTROLLER_IP
nameserver 192.168.1.1

##Fallback DNS
nameserver 8.8.8.8

##Domainname
search vienna.local
```

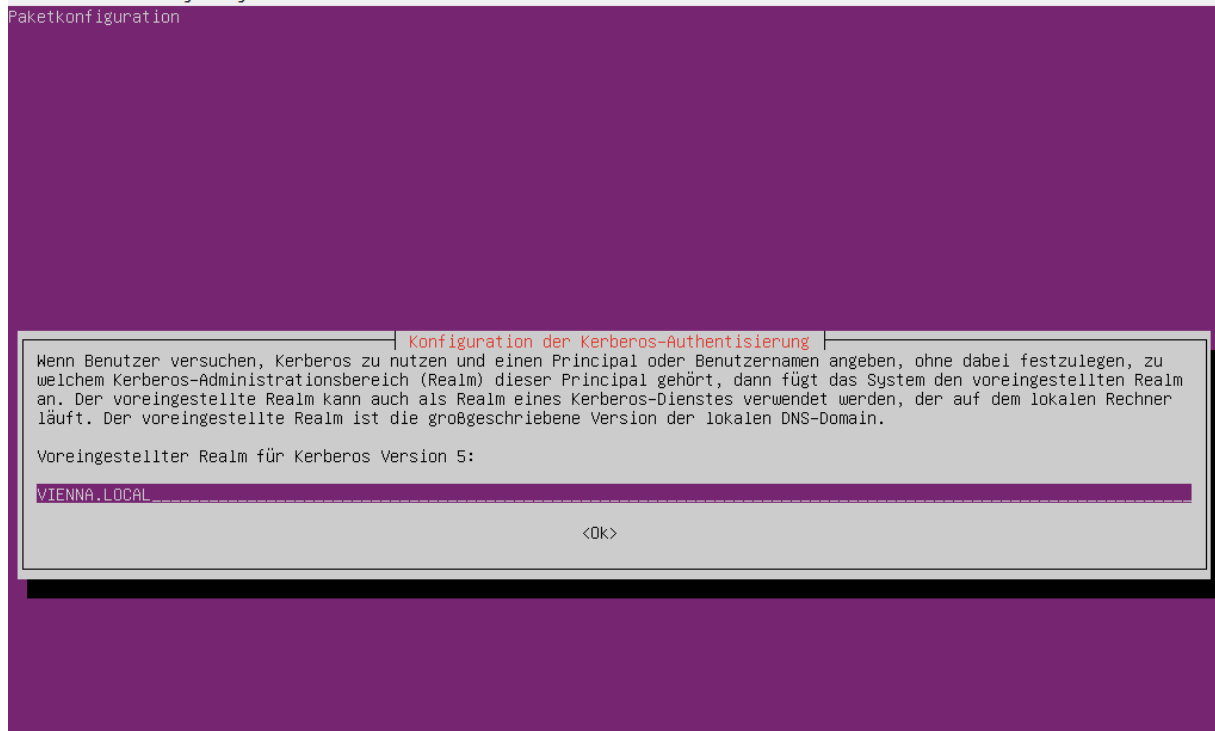
Debian und Ubuntu Repositoren aktualisieren mit „**sudo apt-get update**“ (Kann auch mit gekürzter Form „**sudo apt update**“ ausgeführt werden)

```
locadmin@srvdc:~$ sudo apt update_
```

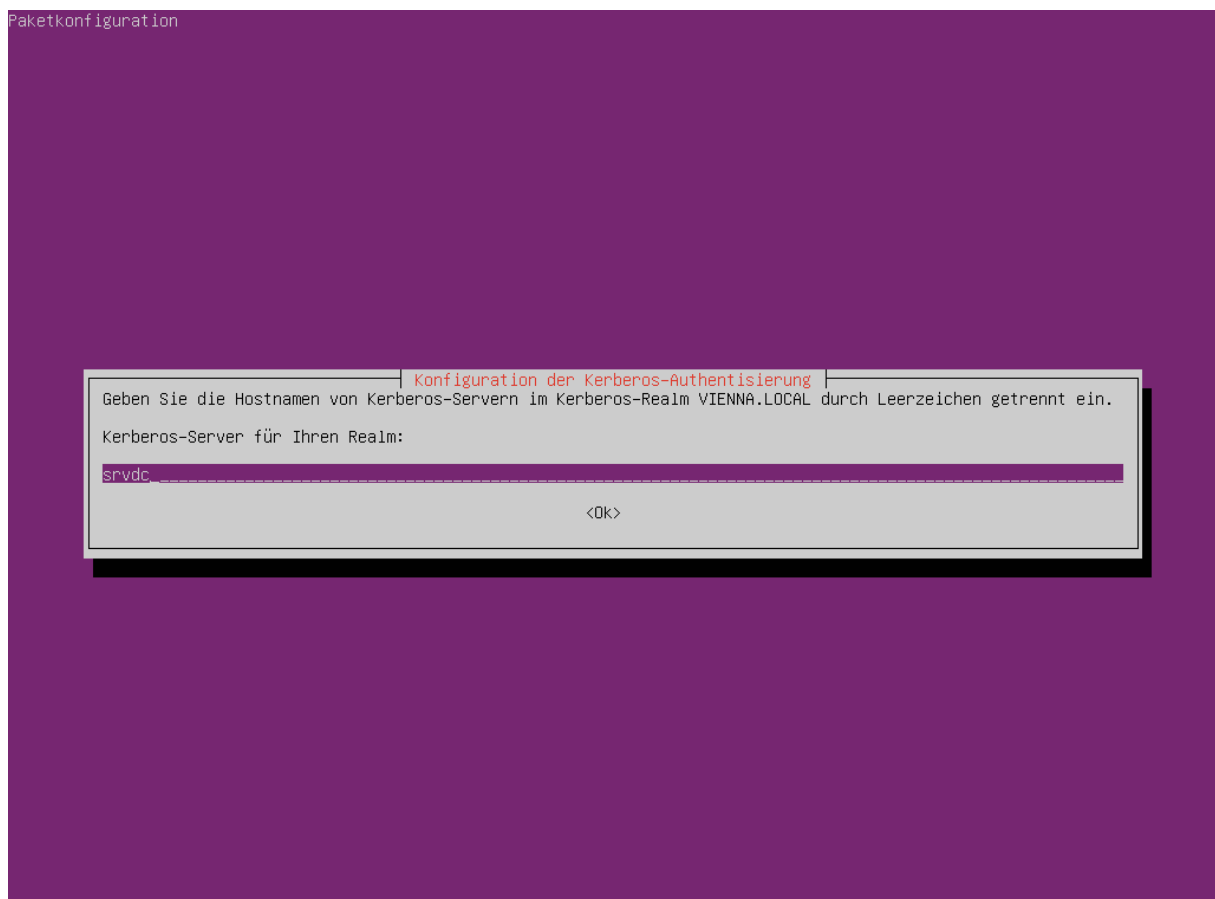
Alle Pakete mit: „**sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony net-tools**“ installieren.

```
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_
```

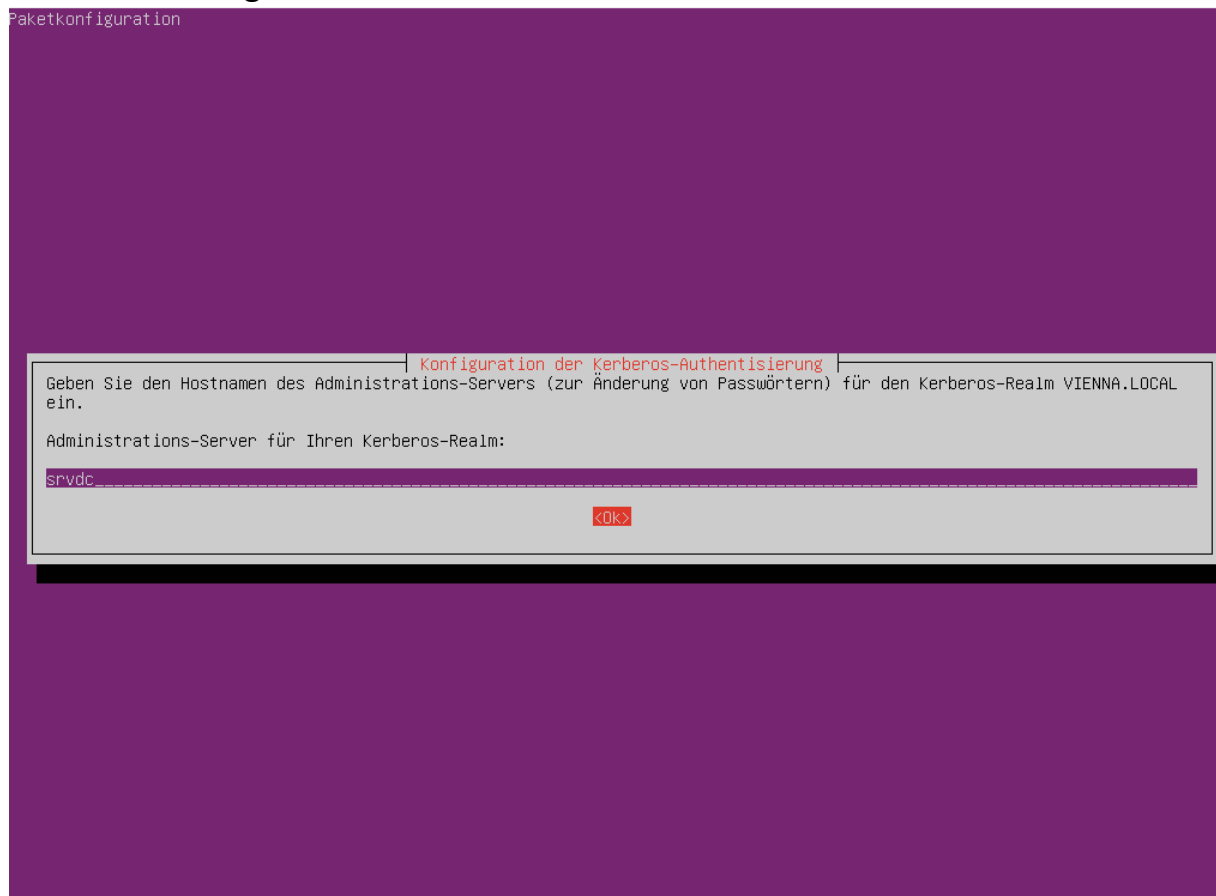
Während der Installation öffnet sich im Terminal der Kerberos-Setup. Man kriegt automatisch den Domänennamen hinzugefügt. Den Tab-Knopf drücken und Enter drücken.



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 smbd nmbd winbind**“

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

```
locadmin@srvdc:/etc/netplan$ sudo systemctl disable --now smbd nmbd winbind
Synchronizing state of smbd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable smbd
Synchronizing state of nmbd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable winbind
Removed /etc/systemd/system/multi-user.target.wants/winbind.service.
Removed /etc/systemd/system/multi-user.target.wants/nmbd.service.
Removed /etc/systemd/system/multi-user.target.wants/smbd.service.
locadmin@srvdc:/etc/netplan$ sudo systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.
locadmin@srvdc:/etc/netplan$ 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:/etc/netplan$ _
```

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:/etc/netplan$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
locadmin@srvdc:/etc/netplan$ sudo mv /etc/krb5.conf /etc/krb5.conf.bak
locadmin@srvdc:/etc/netplan$
```

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

```
locadmin@srvdc:/etc/netplan$ sudo samba-tool domain provision --use-rfc2307 --interactive
Realm [VIENNA.LOCAL]:
Domain [VIENNA]:
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) [192.168.1.1]: 8.8.8.8
Administrator password: _
```

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

„sudo systemctl start samba-ad-dc“

```
locadmin@srvdc:/etc/netplan$ sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
locadmin@srvdc:/etc/netplan$ sudo systemctl start samba-ad-dc
locadmin@srvdc:/etc/netplan$ _
```

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:/etc/netplan$ sudo chown root:_chrony /var/lib/samba/ntp_signd/
locadmin@srvdc:/etc/netplan$ sudo chmod 750 /var/lib/samba/ntp_signd/
locadmin@srvdc:/etc/netplan$ _
```

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

```
locadmin@srvdc:/etc/netplan$ sudo nano /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“

STRG+S und STRG+X, um zu speichern.

```
GNU nano 6.2 /etc/chrony/chrony.conf
#log_tracking measurements statistics

# Log files location.
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0

# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtctest' directive.
rtctest

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 1 3

# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smear time.
leapsectz right/UTC

#####

#Domaenencontroller IP-Adresse
bindcmdaddress 192.168.1.1

#Ganzen Subnetz erlauben
allow 192.168.1.0/24

ntpsigndsocket /var/lib/samba/ntp_signd
```

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

```
locadmin@srvdc:/etc/netplan$ sudo systemctl restart chronyd
locadmin@srvdc:/etc/netplan$ sudo systemctl status chronyd
• chrony.service - chrony, an NTP client/server
   Loaded: loaded (/lib/systemd/system/chrony.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-04-25 09:39:26 UTC; 16s ago
     Docs: man:chronyd(8)
           man:chronyc(1)
           man:chrony.conf(5)
  Process: 5352 ExecStart=/usr/lib/systemd/scripts/chronyd-starter.sh $DAEMON_OPTS (code=exited, status=0/SUCCESS)
 Main PID: 5363 (chronyd)
    Tasks: 3 (limit: 4560)
   Memory: 1.3M
      CPU: 46ms
   CGroup: /system.slice/chrony.service
           └─5363 /usr/sbin/chronyd -F 1
             5364 /usr/sbin/chronyd -F 1

Apr 25 09:39:26 srvdc systemd[1]: Starting chrony, an NTP client/server...
Apr 25 09:39:26 srvdc chronyd[5363]: chronyd version 4.2 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYN
Apr 25 09:39:26 srvdc chronyd[5363]: Frequency -15.290 +/- 1000000.000 ppm read from /var/lib/chrony/chrony.drift
Apr 25 09:39:26 srvdc chronyd[5363]: Using right/UTC timezone to obtain leap second data
Apr 25 09:39:26 srvdc chronyd[5363]: MS-SNTP authentication enabled
Apr 25 09:39:26 srvdc chronyd[5363]: Loaded seccomp filter (level 1)
Apr 25 09:39:26 srvdc systemd[1]: Started chrony, an NTP client/server.
lines 1-22/22 (END)
```

Ein Benutzer kann man z.B. mit „**sudo samba-tool user create maxmustermann**“ erstellen.

```
locadmin@srvdc:/etc/netplan$ sudo samba-tool user create maxmustermann_
```

Alle Befehle kann man mit „**sudo samba-tool --help**“ nachschauen.

```
locadmin@srvdc:/etc/netplan$ sudo samba-tool --help
Usage: samba-tool <subcommand>

Main samba administration tool.

Options:
  -h, --help            show this help message and exit

Version Options:
  -V, --version          Display version number

Available subcommands:
  computer              - Computer management.
  contact               - Contact management.
  dbcheck               - Check local AD database for errors.
  delegation            - Delegation management.
  dns                   - Domain Name Service (DNS) management.
  domain               - Domain management.
  drs                   - Directory Replication Services (DRS) management.
  dsacl                - DS ACLs manipulation.
  forest               - Forest management.
  fsmo                 - Flexible Single Master Operations (FSMO) roles management.
  gpo                  - Group Policy Object (GPO) management.
  group                - Group management.
  ldapcmp              - Compare two ldap databases.
  ntacl                - NT ACLs manipulation.
  ou                   - Organizational Units (OU) management.
  processes            - List processes (to aid debugging on systems without setproctitle).
  rodc                 - Read-Only Domain Controller (RODC) management.
  schema               - Schema querying and management.
  sites                - Sites management.
  spn                  - Service Principal Name (SPN) management.
  testparm             - Syntax check the configuration file.
  time                 - Retrieve the time on a server.
  user                 - User management.
  visualize            - Produces graphical representations of Samba network state.
For more help on a specific subcommand, please type: samba-tool <subcommand> (-h|--help)

locadmin@srvdc:/etc/netplan$
```

Informationen über ein Befehl schaut man z.B. mit

„**sudo samba-tool user --help**“ an.

```
locadmin@srvdc:/etc/netplan$ sudo samba-tool user --help
Usage: samba-tool user <subcommand>

User management.

Options:
  -h, --help  show this help message and exit

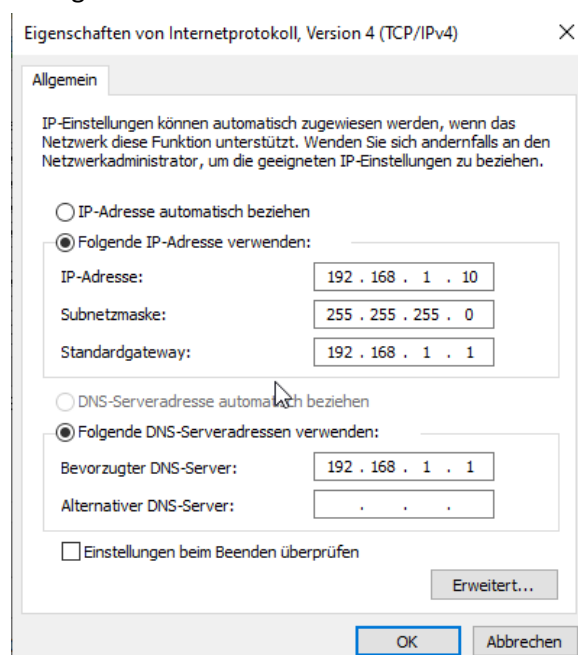
Available subcommands:
  add                - Add a new user.
  addunixattrs       - Add RFC2307 attributes to a user.
  create             - Add a new user.
  delete             - Delete a user.
  disable            - Disable a user.
  edit               - Modify User AD object.
  enable             - Enable a user.
  getgroups           - Get the direct group memberships of a user account.
  getpassword         - Get the password fields of a user/computer account.
  list               - List all users.
  move               - Move a user to an organizational unit/container.
  password           - Change password for a user account (the one provided in authentication).
  rename             - Rename a user and related attributes.
  sensitive           - Set/unset or show UF_NOT_DELEGATED for an account.
  setexpiry          - Set the expiration of a user account.
  setpassword         - Set or reset the password of a user account.
  setprimarygroup     - Set the primary group a user account.
  show               - Display a user AD object.
  syncpasswords       - Sync the password of user accounts.
  unlock             - Unlock a user account.

For more help on a specific subcommand, please type: samba-tool user <subcommand> (-h|--help)

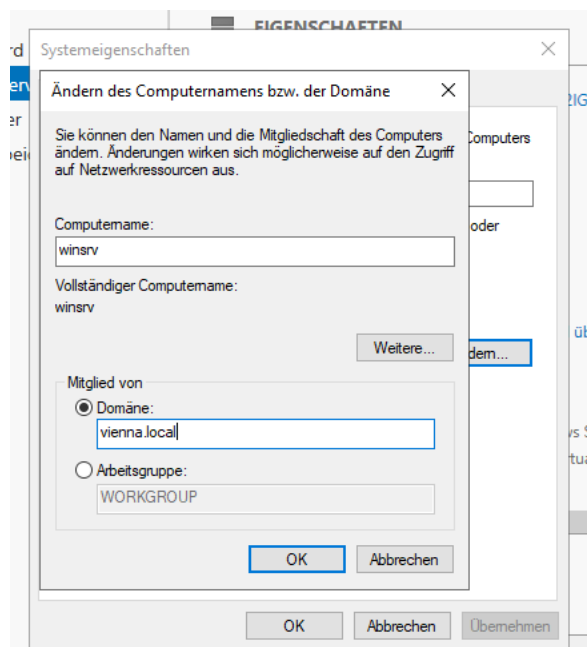
locadmin@srvdc:/etc/netplan$ _
```

→ Windows Server

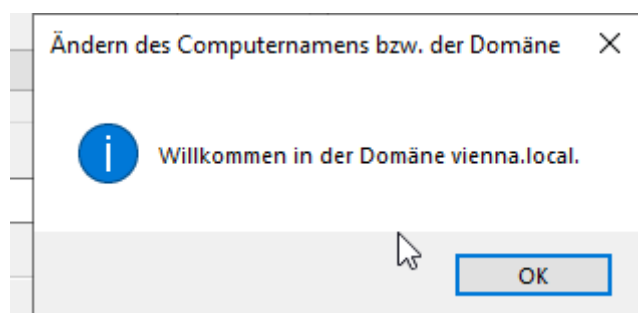
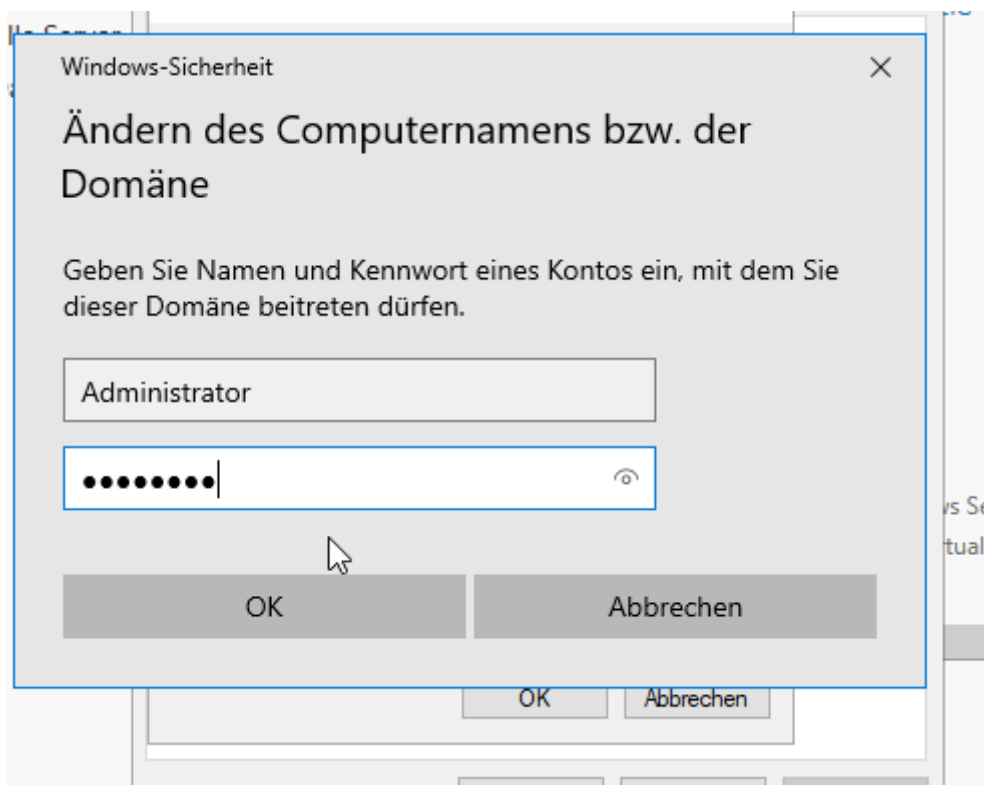
Netzwerkeinstellungen konfigurieren. Linux-Rechner soll als DNS-Server eingetragen sein.



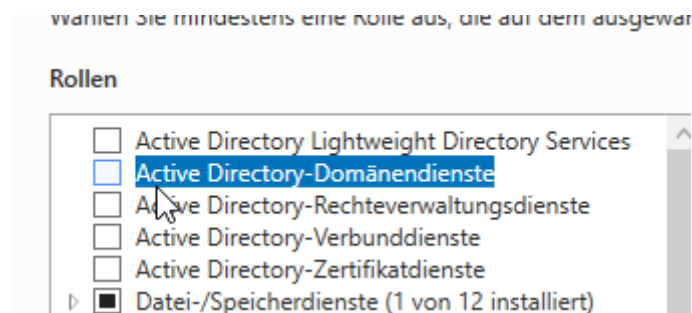
Server in die Domäne hinzufügen.



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.

