

Contents

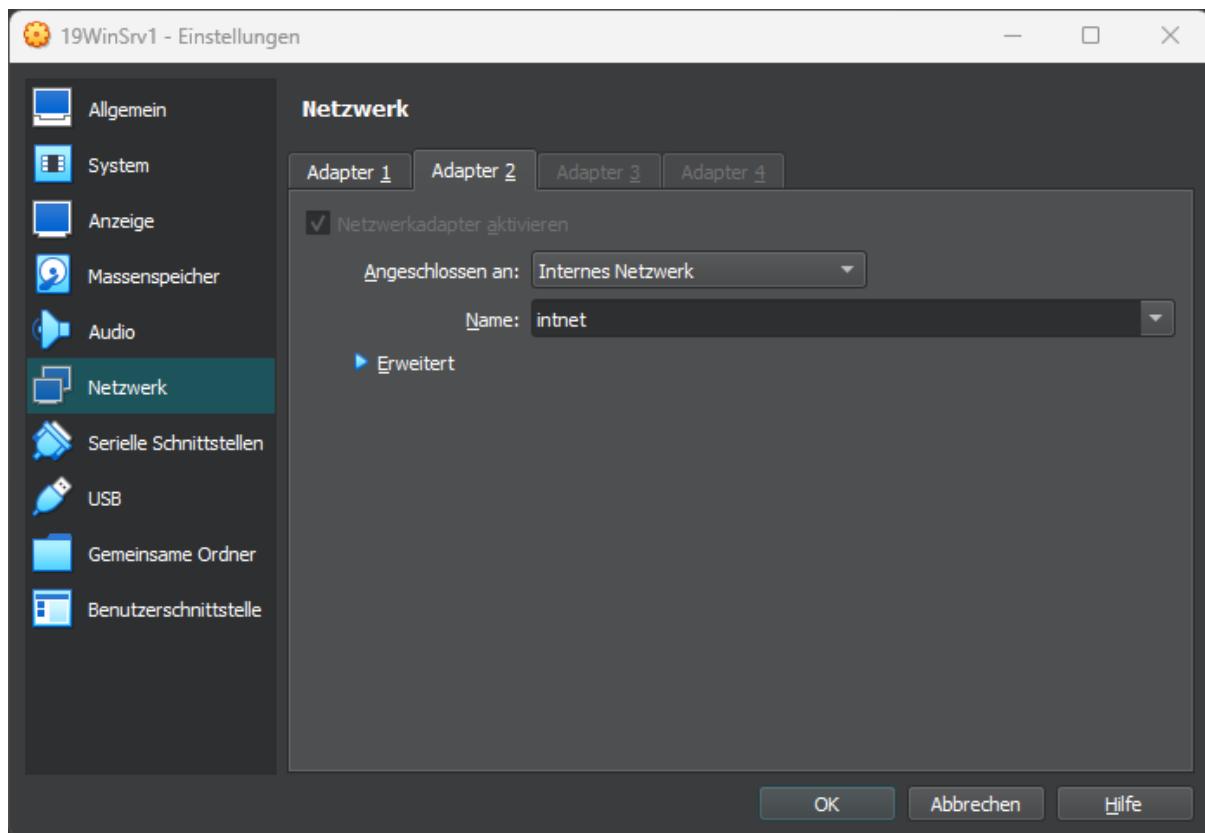
SYTS Fachtheorie	2
Internes Netz einstellen (zusätzliche Karte hinzufügen)	3
Installationsmedium auswerfen und Gasterweiterungen einlegen	4
IP config checken	6
IP Adresse vergeben	7
Partition	8
Rollen und Features hinzufügen	13
ADDS einrichten	15
DHCP einrichten	19
DNS einrichten	25
Client aufsetzen	28
Netzwerk, Namen ändern und Domain beitreten	30
Benutzer erstellen und Gruppen.....	33
Dienste	36
WSUS.....	36
WDS.....	45
Ubuntu Client.....	49
Was wahrscheinlich kommen wird.....	55

SYTS Fachtheorie

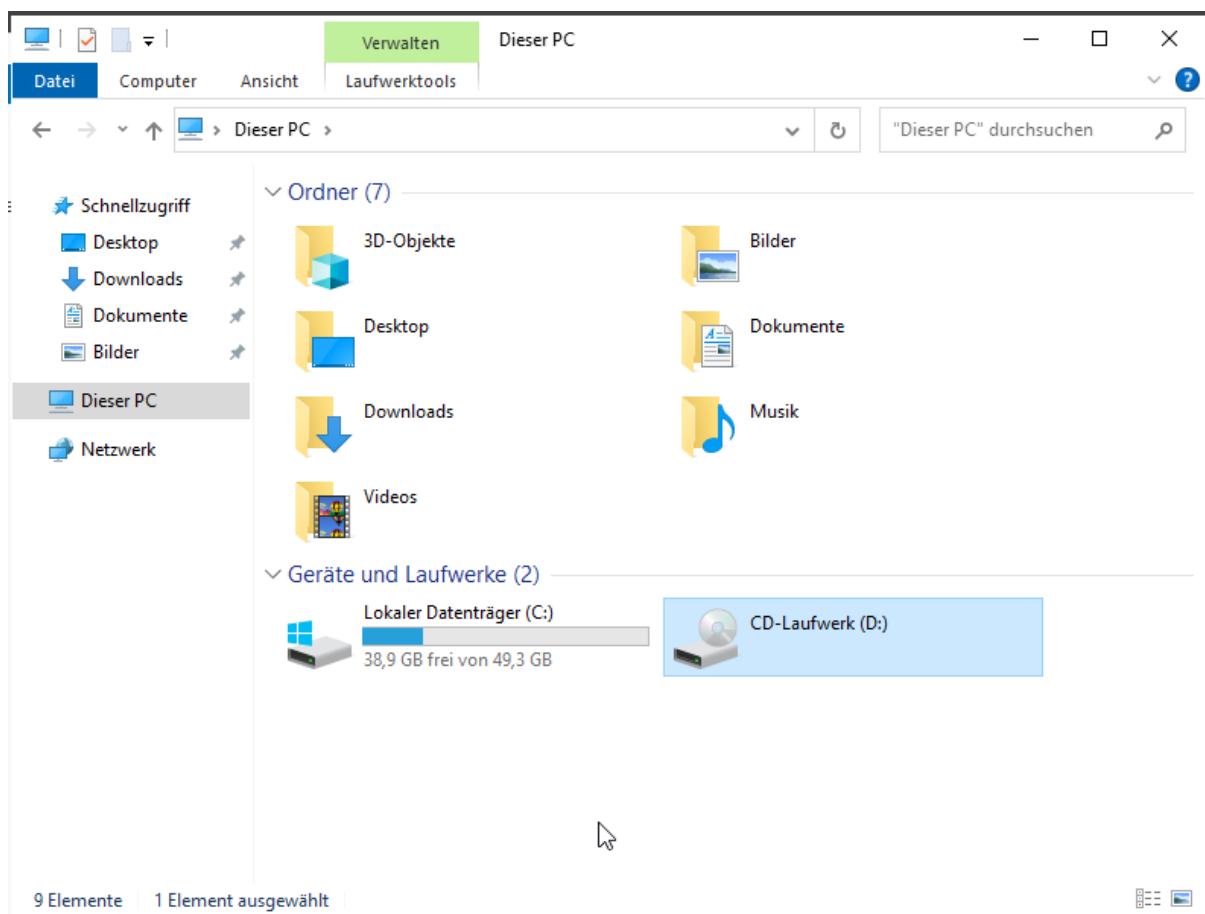
Auf jeden fall kommt eine Windows Server Maschine vor.

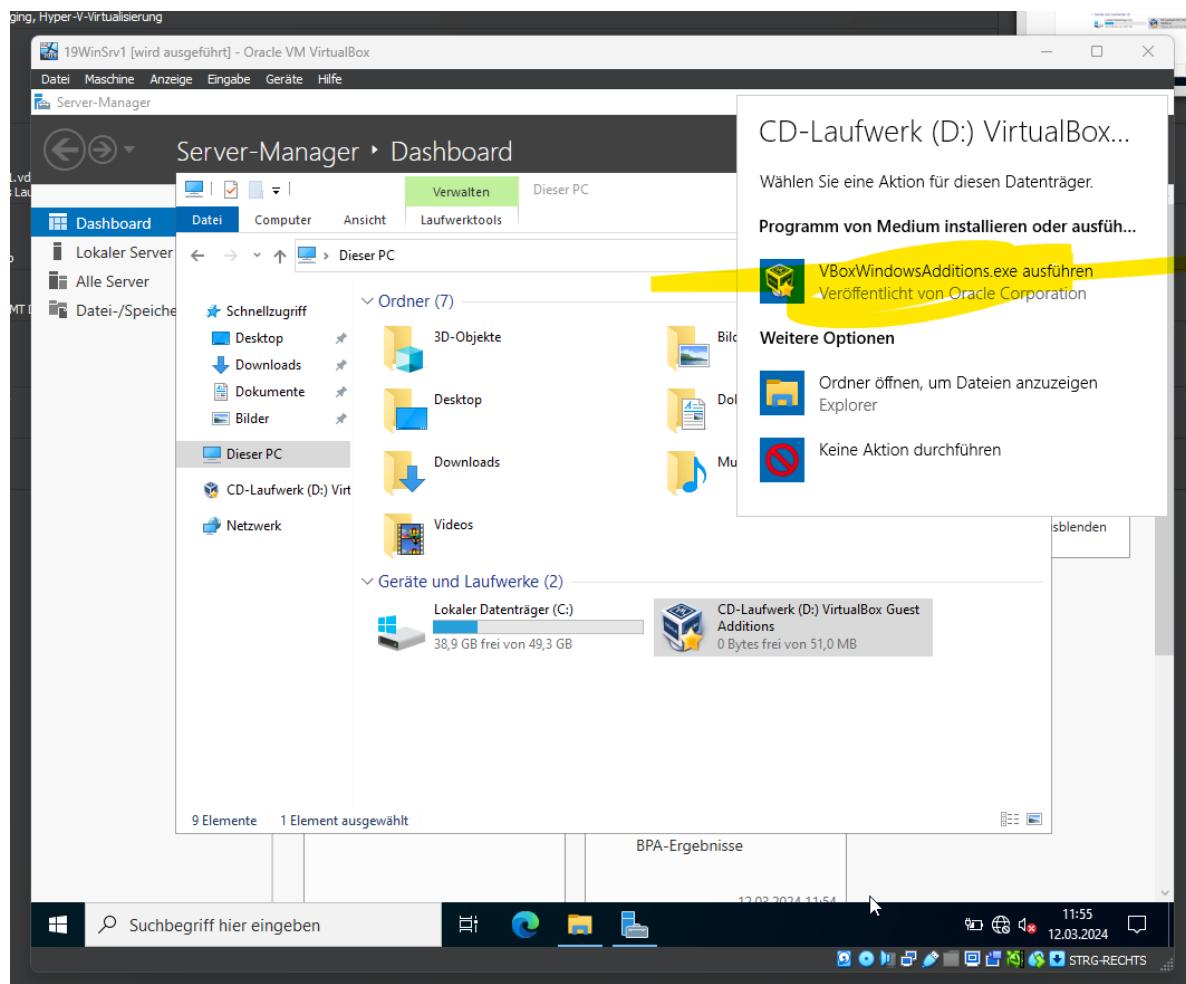
Bei neuer Maschine: in Angabe welcher Name (ist meistens auch als Hostname zu wählen)
Name und Hostname ist nicht das Gleiche!

Internes Netz einstellen (zusätzliche Karte hinzufügen)



Installationsmedium auswerfen und Gasterweiterungen einlegen





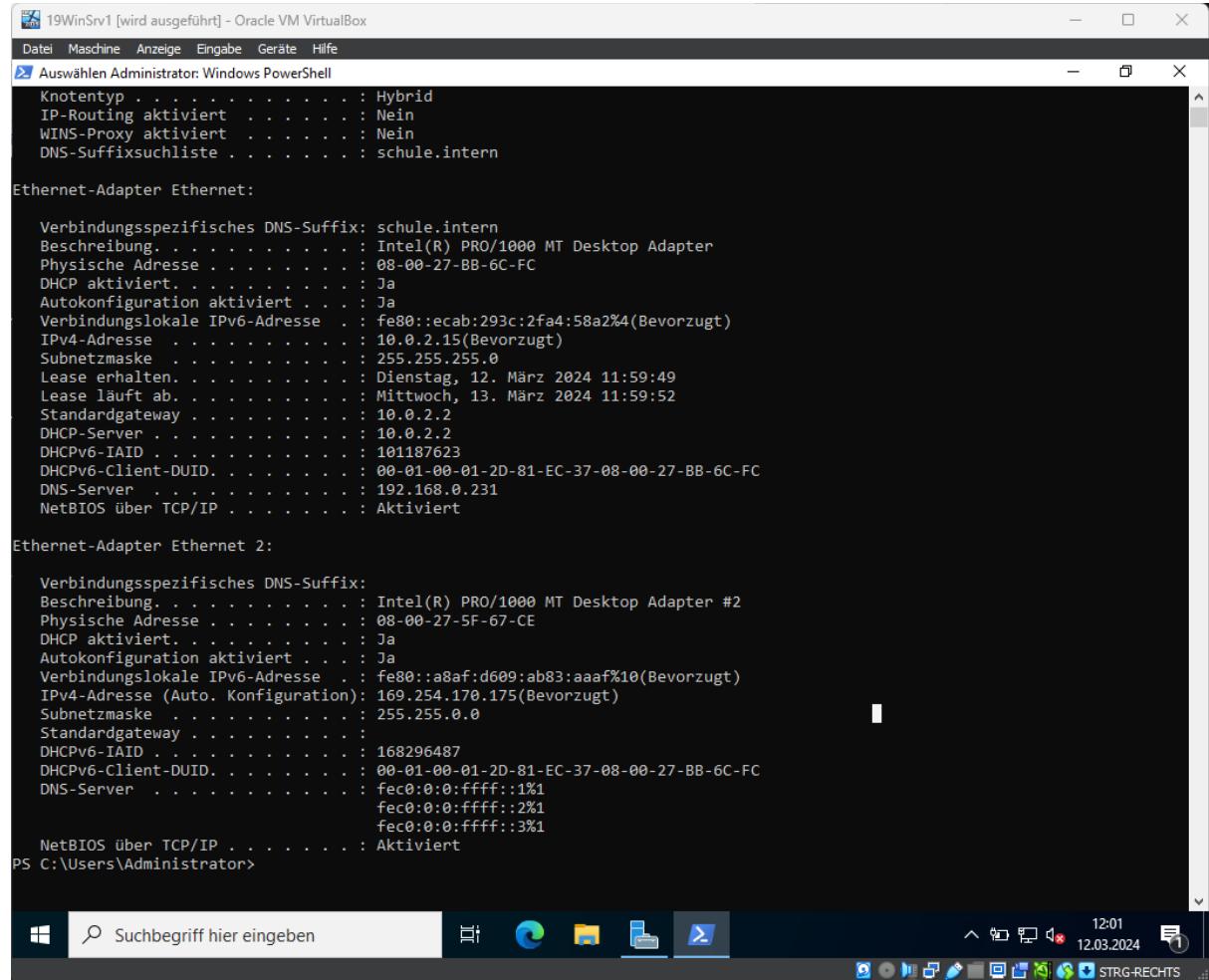
IP config checken

Ethernet Adapter Ethernet (genattet):

10.0.2.15

Ethernet Adapter Ethernet 2 (zero config addressen):

169.254



19WinSrv1 [wird ausgeführt] - Oracle VM VirtualBox

Datei Maschine Anzeige Eingabe Geräte Hilfe

Auswählen Administrator: Windows PowerShell

```
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert . . . . . : Nein
WINS-Proxy aktiviert . . . . . : Nein
DNS-Suffixsuchliste . . . . . : schule.intern

Ethernet-Adapter Ethernet:

Verbindungsspezifisches DNS-Suffix: schule.intern
Beschreibung. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physische Adresse . . . . . : 08-00-27-BB-6C-FC
DHCP aktiviert. . . . . : Ja
Aukonfiguration aktiviert . . . . . : Ja
Verbindungslokale IPv6-Adresse . . . . : fe80::ecab:293c:2fa4:58a2%4(Bevorzugt)
IPv4-Adresse . . . . . : 10.0.2.15(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Dienstag, 12. März 2024 11:59:49
Lease läuft ab. . . . . : Mittwoch, 13. März 2024 11:59:52
Standardgateway . . . . . : 10.0.2.2
DHCP-Server . . . . . : 10.0.2.2
DHCPv6-IAID . . . . . : 101187623
DHCPv6-Client-DUID. . . . . : 00-01-00-01-2D-81-EC-37-08-00-27-BB-6C-FC
DNS-Server . . . . . : 192.168.0.231
NetBIOS über TCP/IP . . . . . : Aktiviert

Ethernet-Adapter Ethernet 2:

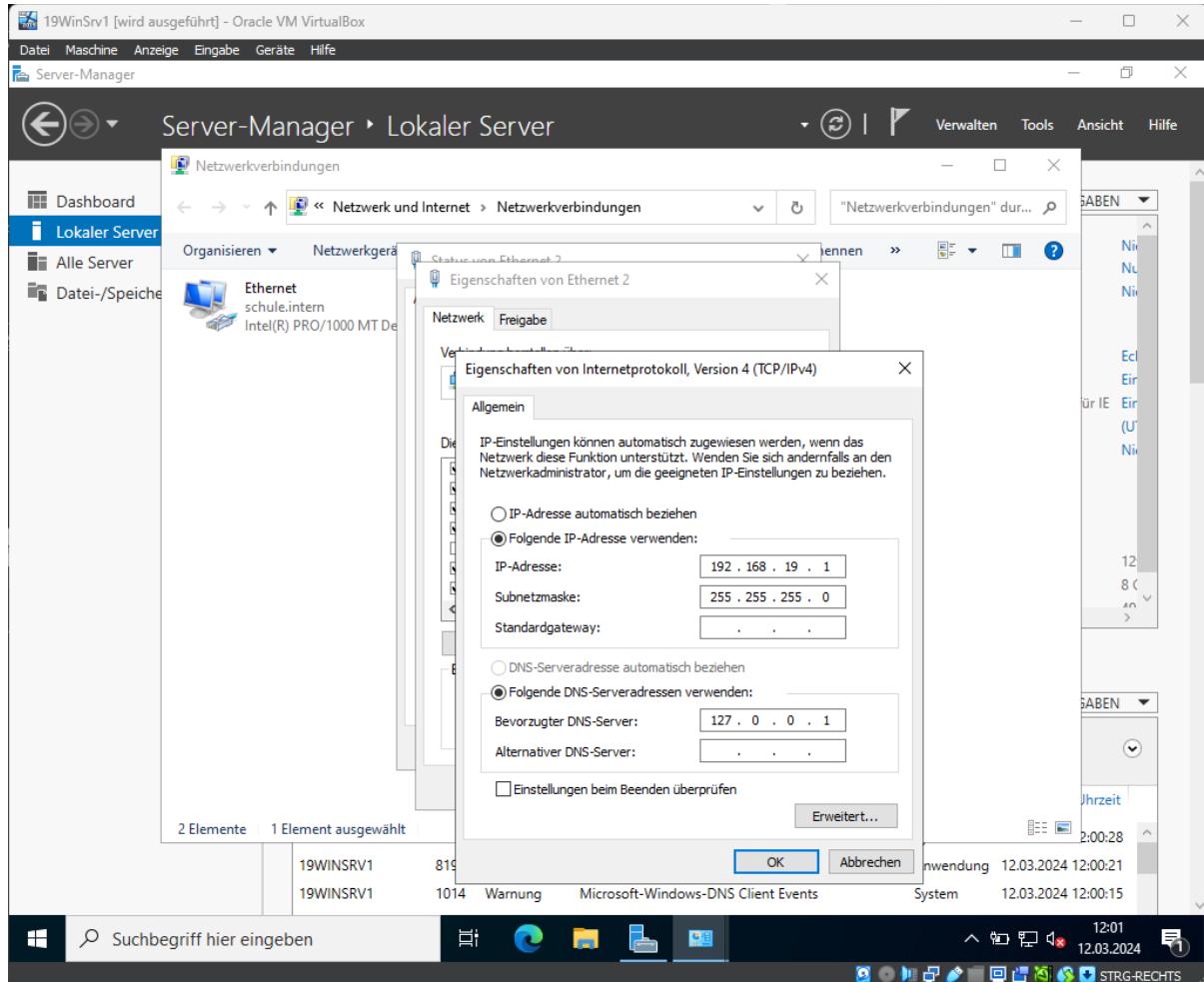
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
Physische Adresse . . . . . : 08-00-27-5F-67-CF
DHCP aktiviert. . . . . : Ja
Aukonfiguration aktiviert . . . . . : Ja
Verbindungslokale IPv6-Adresse . . . . : fe80::a8af:d609:ab83:aaaf%10(Bevorzugt)
IPv4-Adresse (Auto. Konfiguration): 169.254.170.175(Bevorzugt)
Subnetzmaske . . . . . : 255.255.0.0
Standardgateway . . . . . :
DHCPv6-IAID . . . . . : 168296487
DHCPv6-Client-DUID. . . . . : 00-01-00-01-2D-81-EC-37-08-00-27-BB-6C-FC
DNS-Server . . . . . : fec0::0:ffff::1%1
                           fec0::0:0:ffff::2%1
                           fec0::0:0:ffff::3%1
NetBIOS über TCP/IP . . . . . : Aktiviert
PS C:\Users\Administrator>
```

Suchbegriff hier eingeben 12:01 12.03.2024 STRG-RECHTS

IP Adresse vergeben

DNS gleich auf eigenen Server stellen (127.0.0.1)

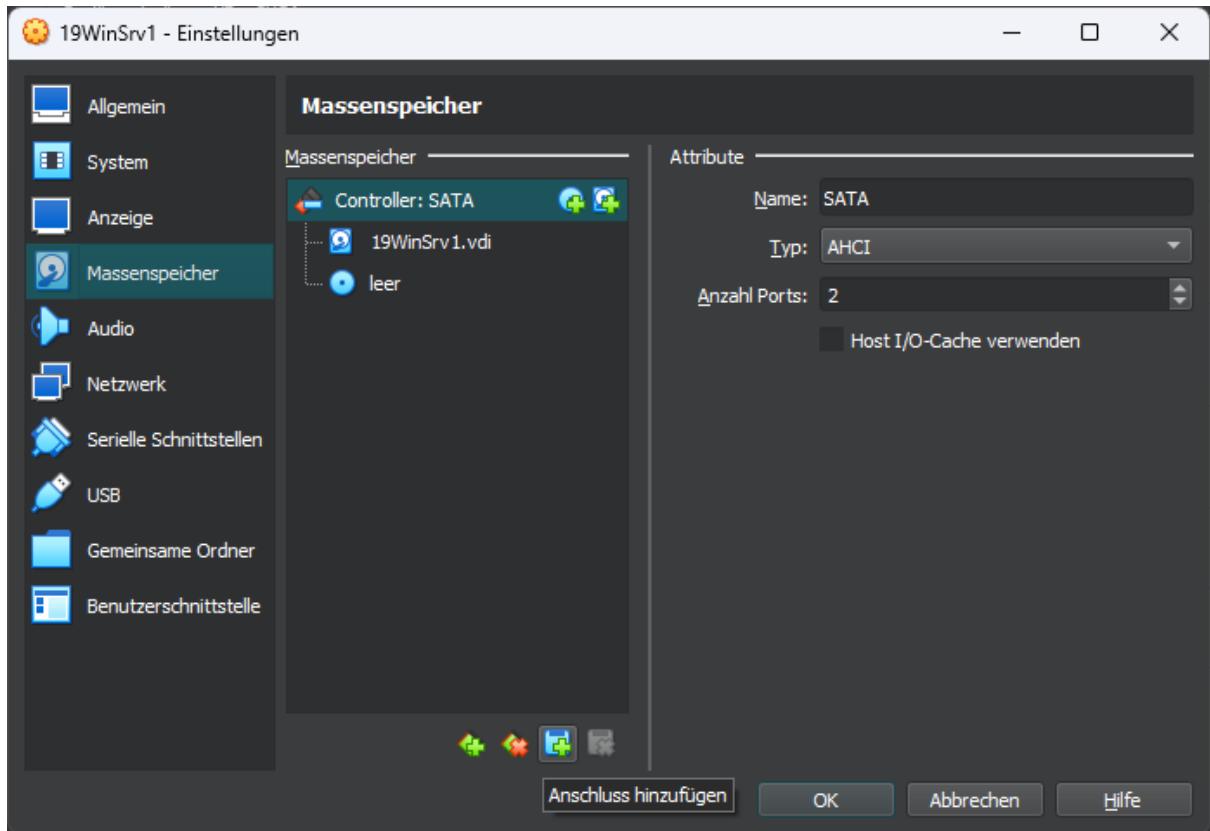
Kein IPv6 machen

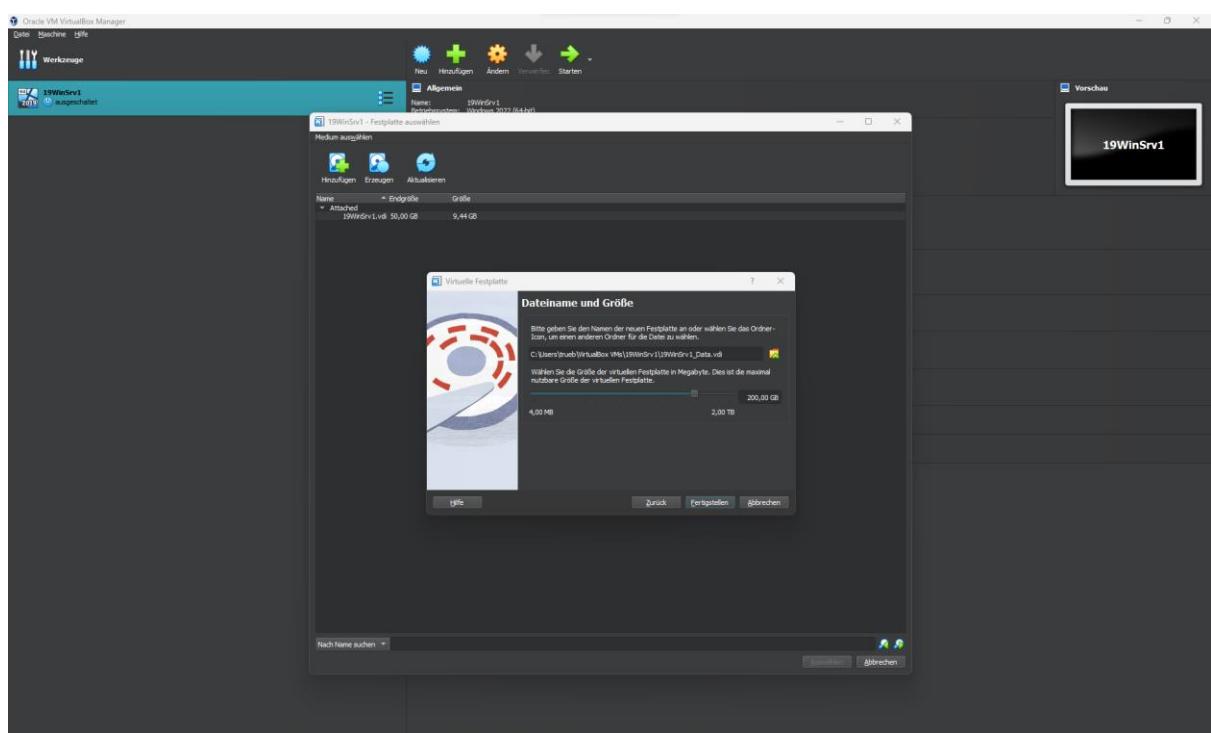
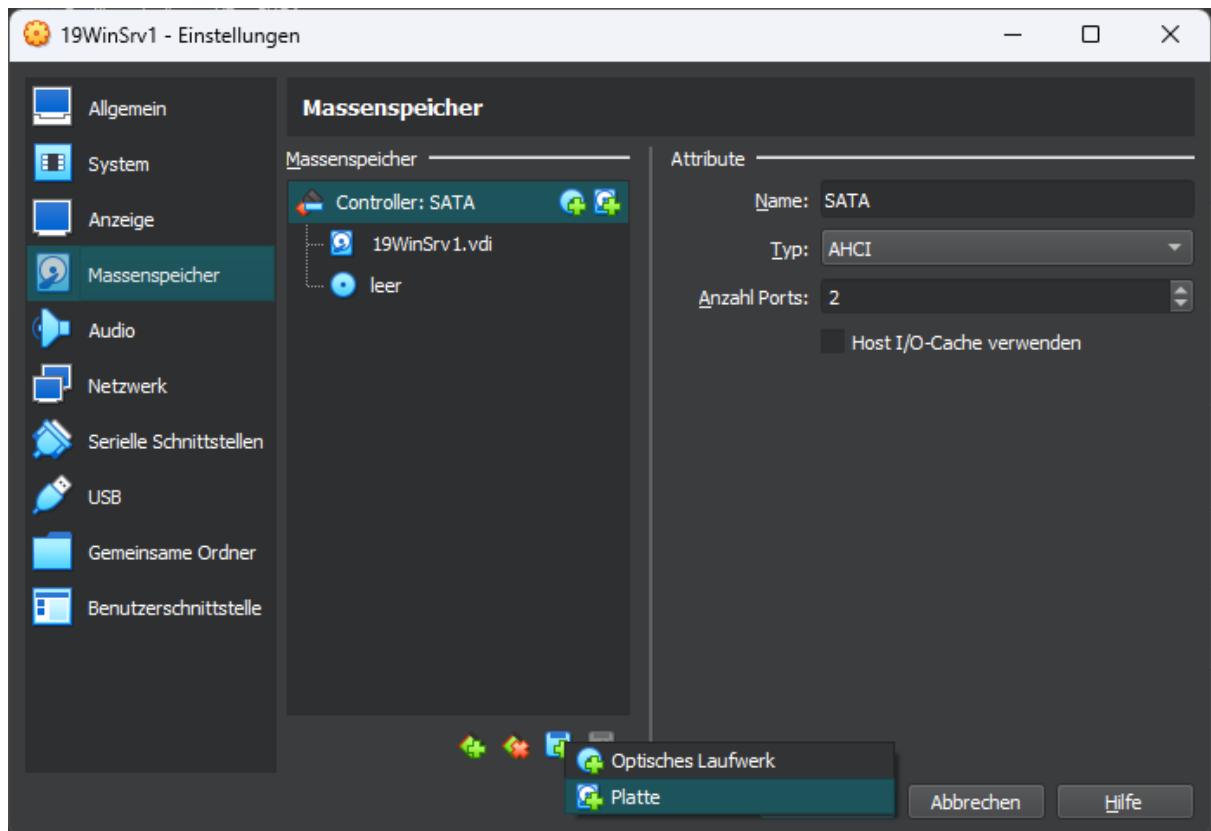


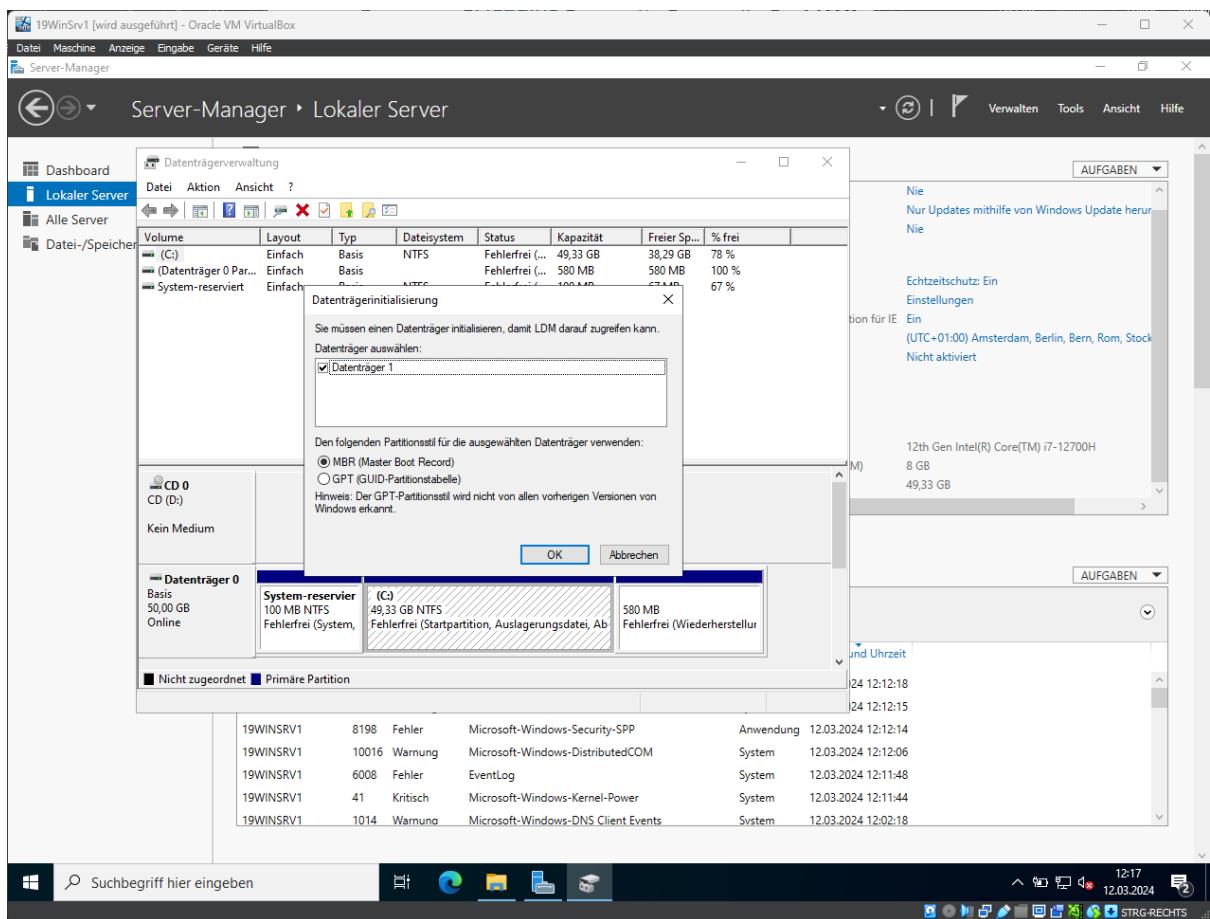
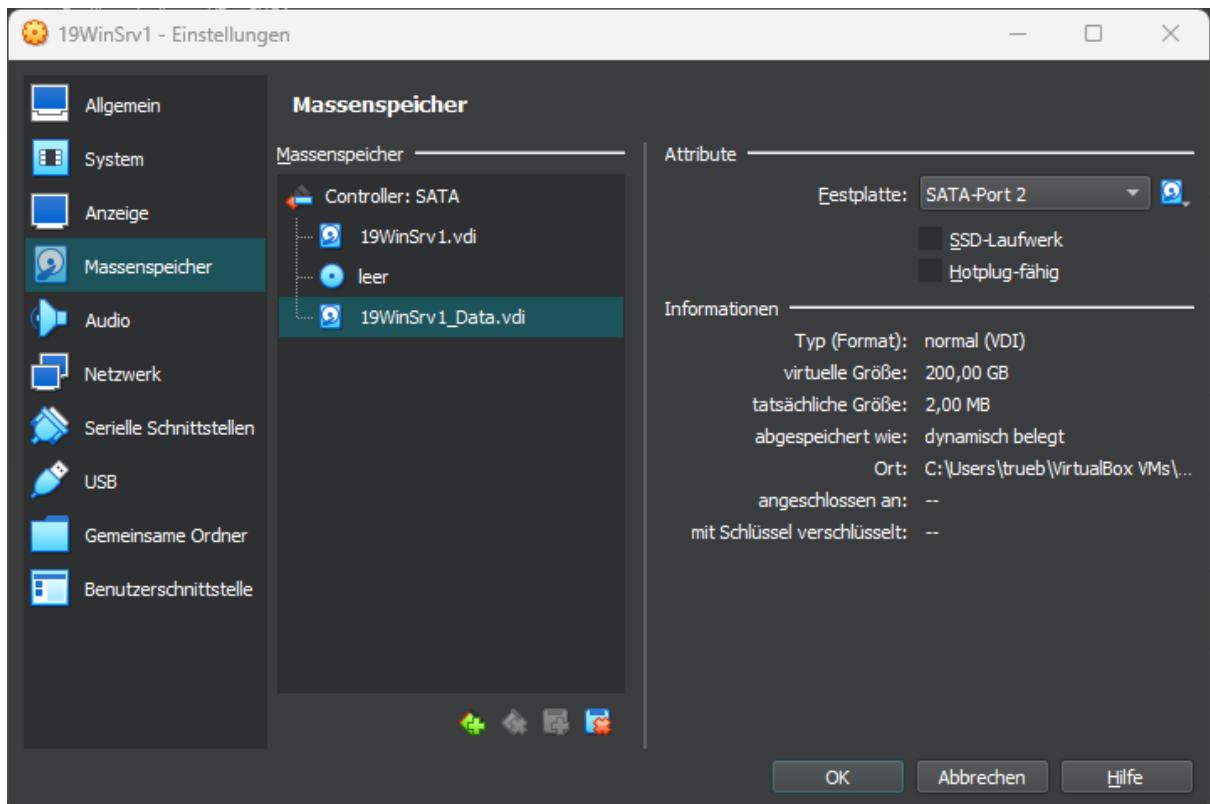
Partition

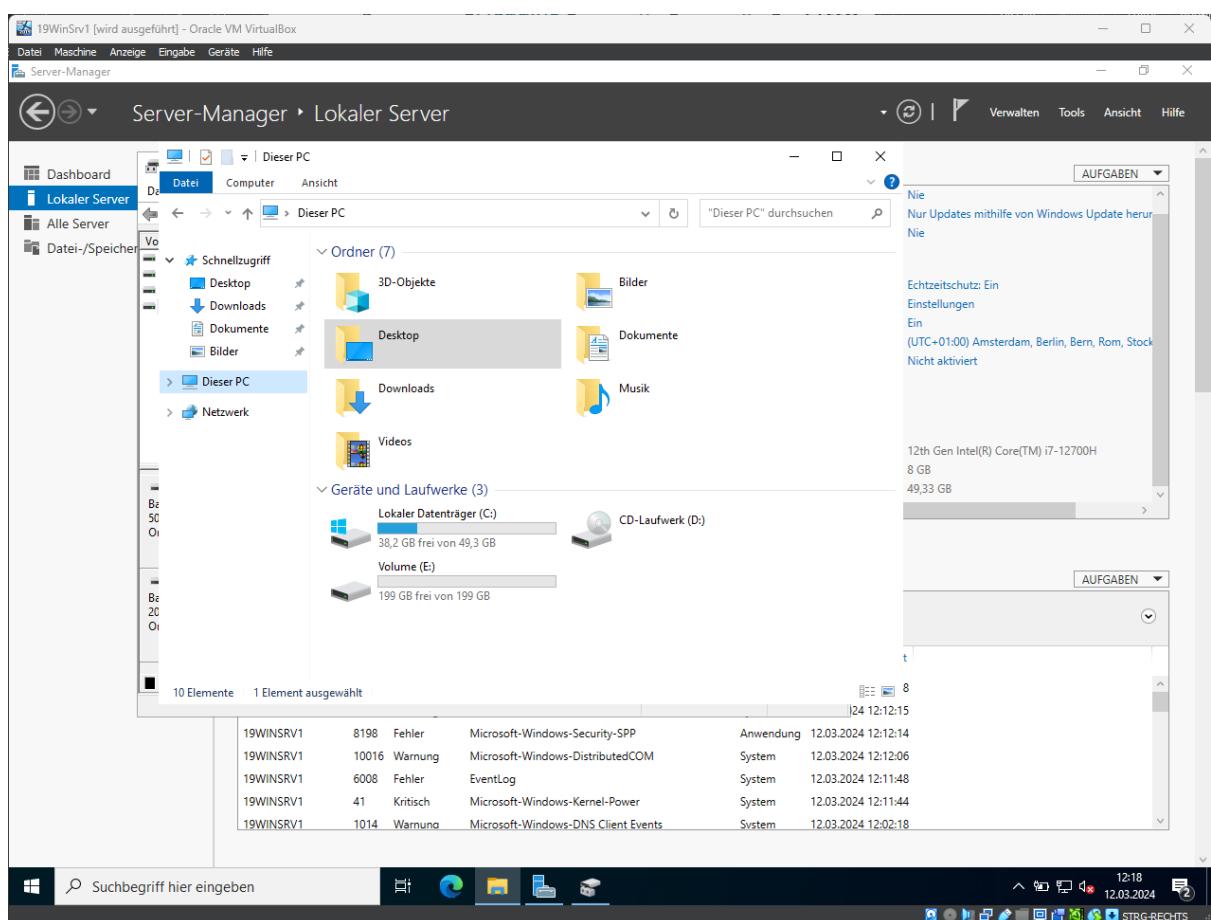
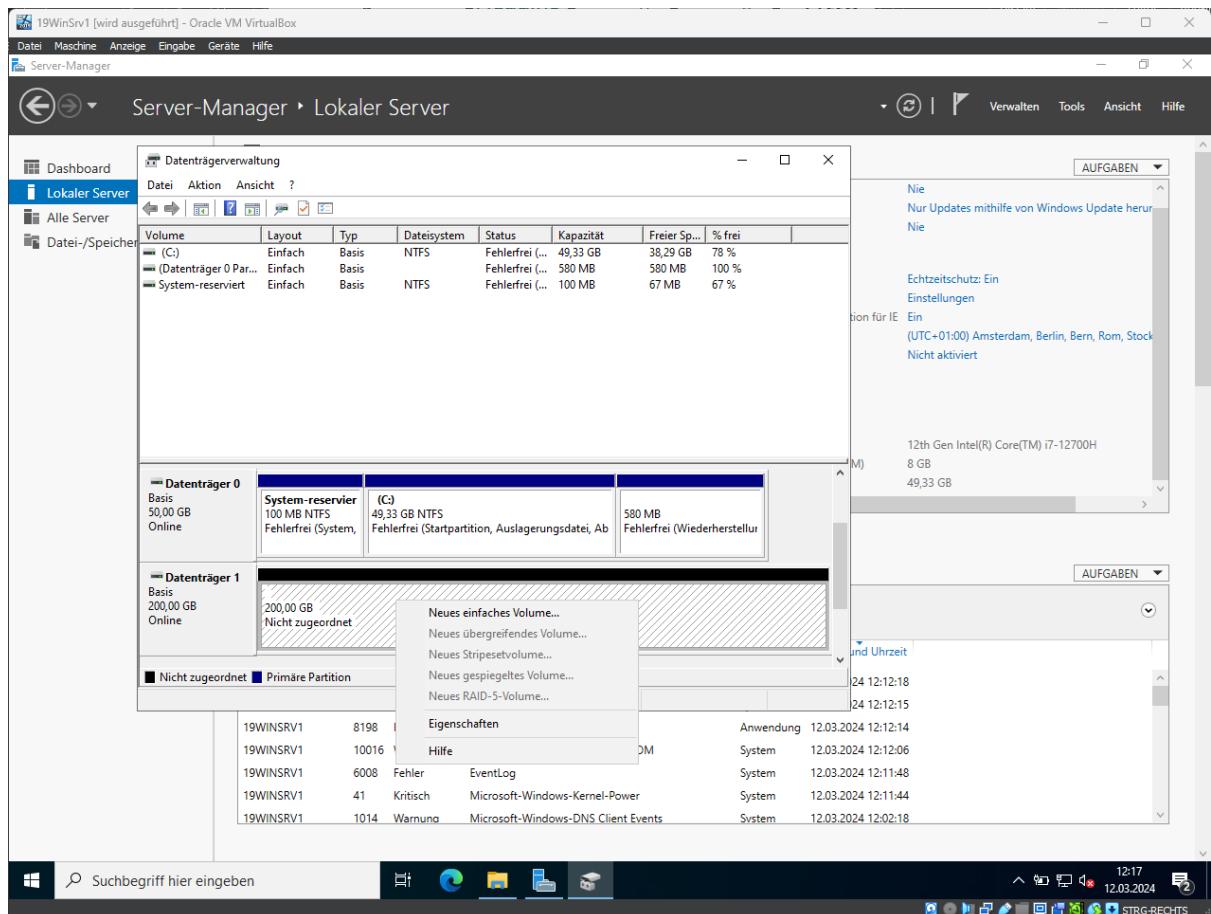
Neue Platte zum Controller hinzufügen und eigene Partition zum Server hinzufügen.

Normalerweise kann ein Server ja zB einen Dienst zur Verfügung stellen aber keine DC sein, wie zum Beispiel einen FTP-Server (Datenspeicherplatz).









[9WinSrv1 [wird ausgeführt] - Oracle VM VirtualBox]

Datei Maschine Anzeige Eingabe Geräte Hilfe

Server-Manager

Server-Manager • Lokaler Server

EIGENSCHAFTEN
Für 9WinSrv1

AUFGABEN

Dashboard

Lokaler Server

Alle Server

Datei-/Speicherdienste

Computername: 9WinSrv1
Arbeitsgruppe: WORKGROUP
Zuletzt installierte Updates: Nie
Windows Update: Nur Updates mithilfe von Windows Update heruntergeladen
Zuletzt auf Updates geprüft: Nie

Microsoft Defender Firewall: Öffentlich: Ein, Privat: Ein
Remoteverwaltung: Aktiviert
Remotedesktop: Deaktiviert
NIC-Teamvorgang: Deaktiviert
Ethernet: IPv4-Adresse wird über DHCP zugewiesen, IPv6-fähig
Ethernet 2: 192.168.1.1, IPv6-fähig

Microsoft Defender Antivirus: Echtzeitshutz: Ein
Feedback und Diagnose: Einstellungen
Verstärkte Sicherheitskonfiguration für IE: Ein
Zeitzone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholms
Produkt-ID: Nicht aktiviert

Betriebssystemversion: Microsoft Windows Server 2022 Standard
Hardwareinformationen: innoteck GmbH VirtualBox
Prozessoren: 12th Gen Intel(R) Core(TM) i7-12700H
Installierter Arbeitsspeicher (RAM): 8 GB
Speicherplatz insgesamt: 249,33 GB

EREIGNISSE
Alle Ereignisse | 36 insgesamt

AUFGABEN

Filter

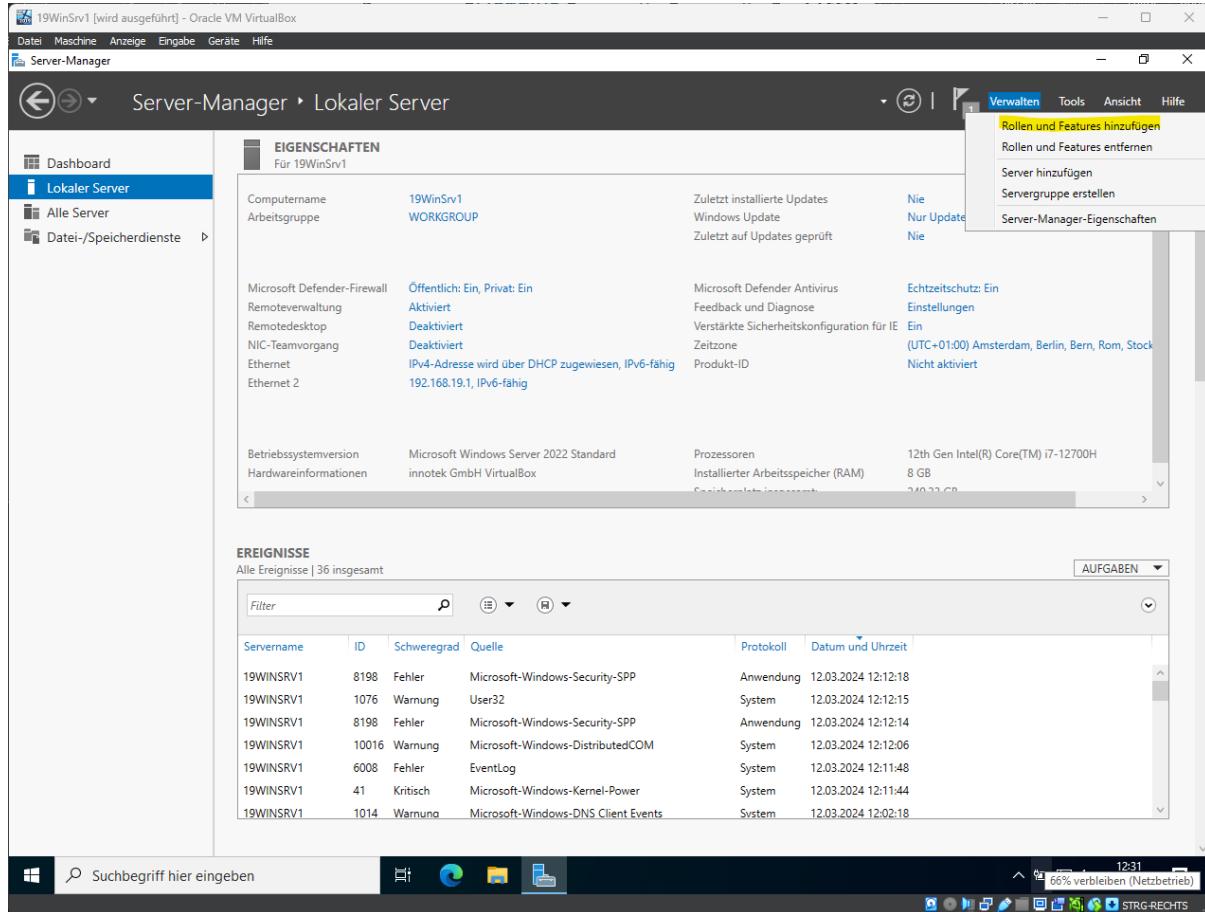
Servername	ID	Schweregrad	Quelle	Protokoll	Datum und Uhrzeit
19WINSRV1	8198	Fehler	Microsoft-Windows-Security-SPP	Anwendung	12.03.2024 12:12:18
19WINSRV1	1076	Warnung	User32	System	12.03.2024 12:12:15
19WINSRV1	8198	Fehler	Microsoft-Windows-Security-SPP	Anwendung	12.03.2024 12:12:14
19WINSRV1	10016	Warnung	Microsoft-Windows-DistributedCOM	System	12.03.2024 12:12:06
19WINSRV1	6008	Fehler	EventLog	System	12.03.2024 12:11:48
19WINSRV1	41	Kritisch	Microsoft-Windows-Kernel-Power	System	12.03.2024 12:11:44
19WINSRV1	1014	Warnung	Microsoft-Windows-DNS Client Events	System	12.03.2024 12:02:18

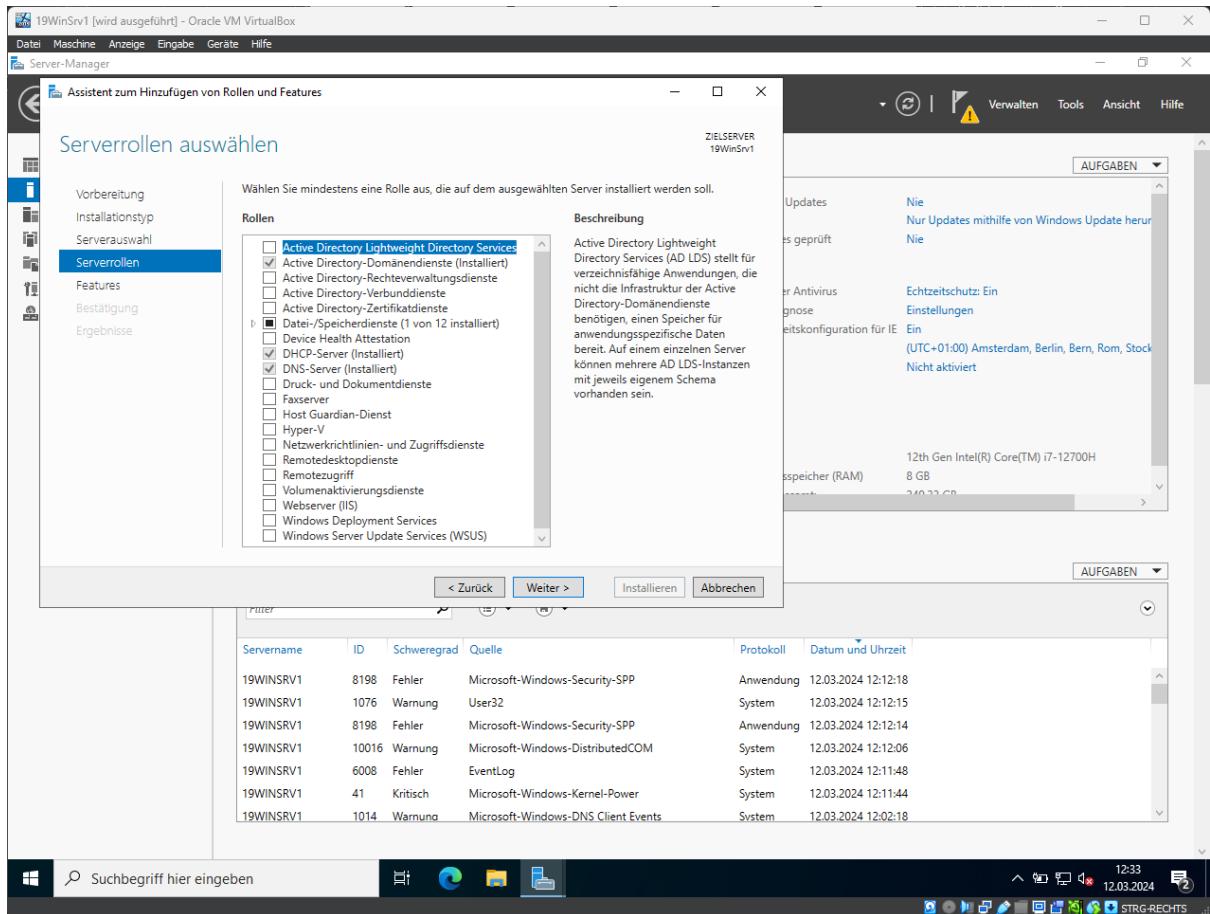
Suchbegriff hier eingeben

12:19 12.03.2024 STRG-RECHTS

Rollen und Features hinzufügen

Nun transformiert der Windows Server zum DC. Dazu installieren wir gleichzeitig alle drei Features: DHCP, DNS und AD-Domainendienst.

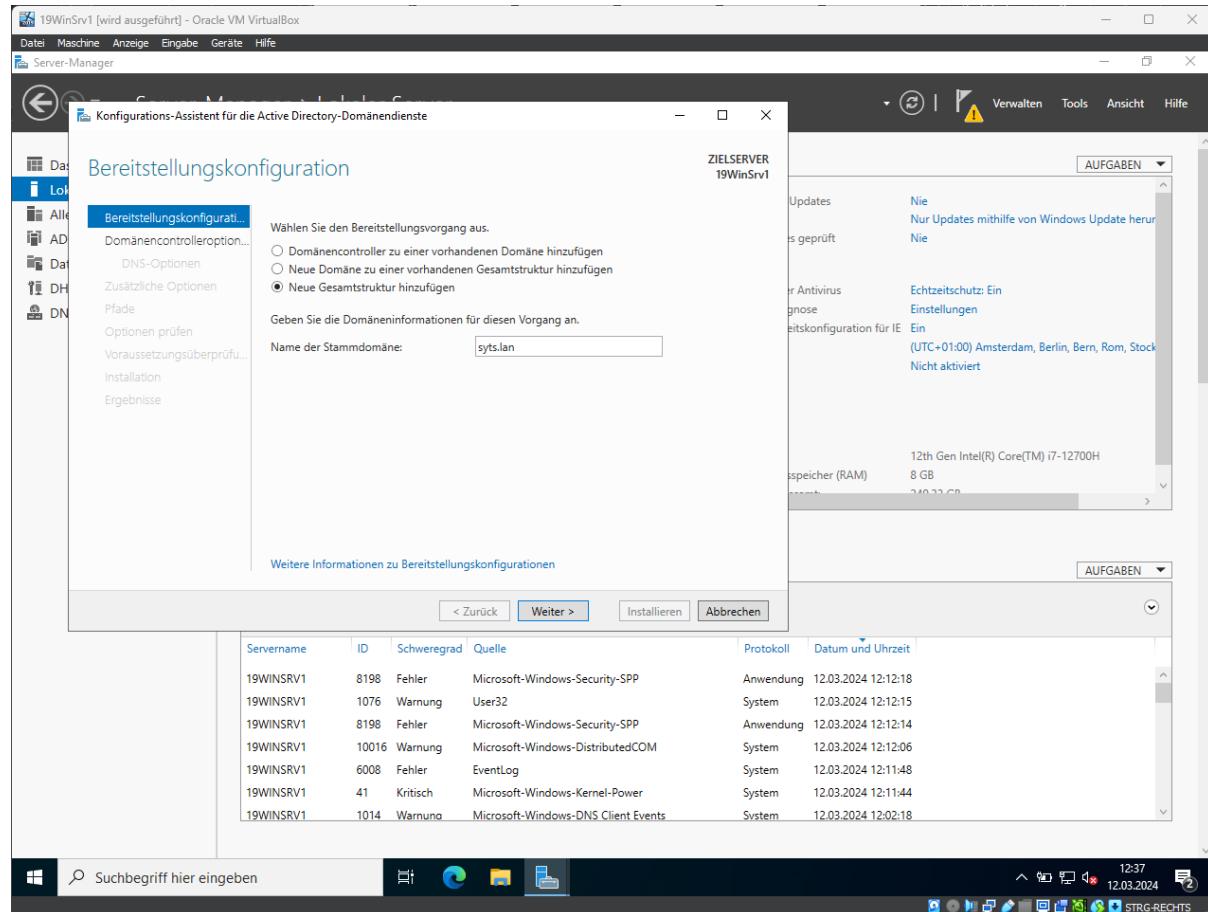


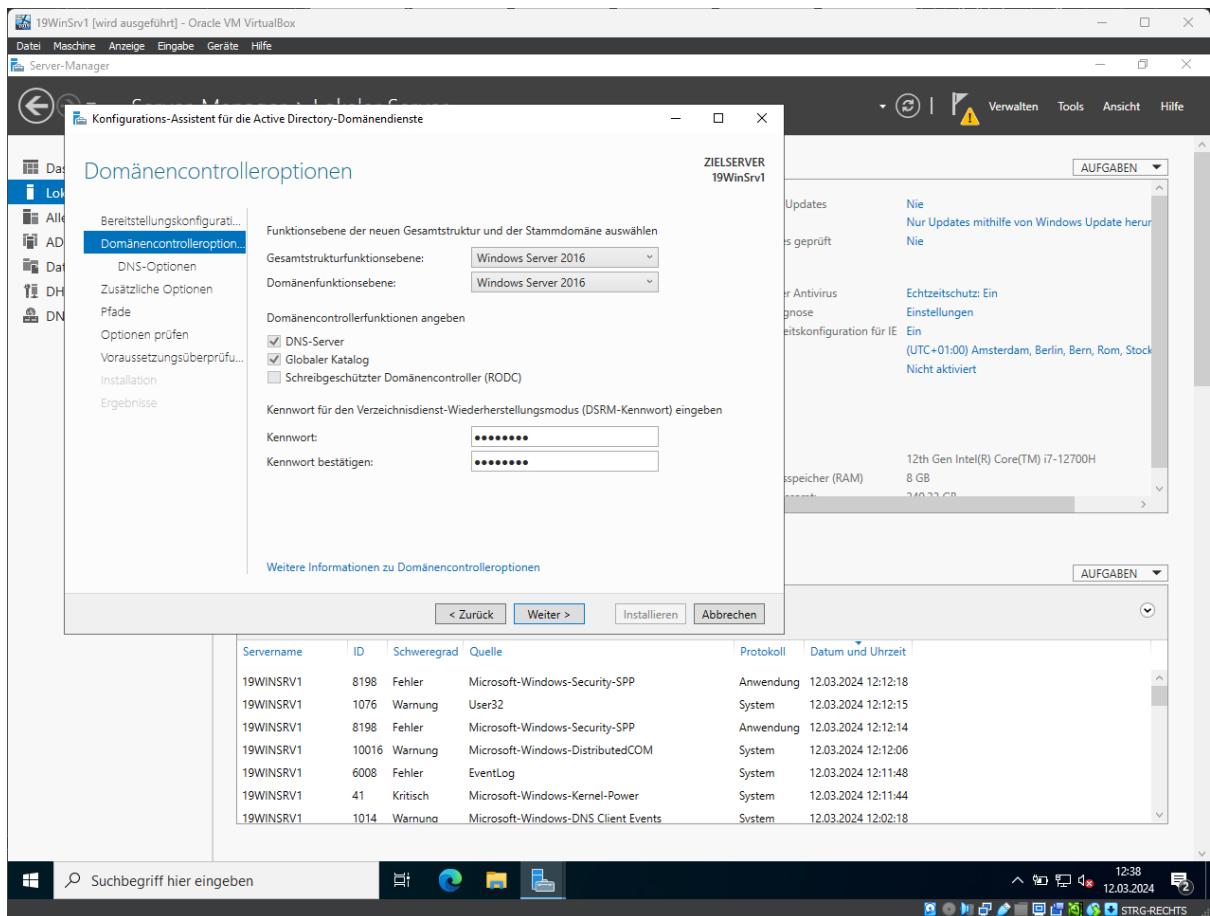


ADDS einrichten

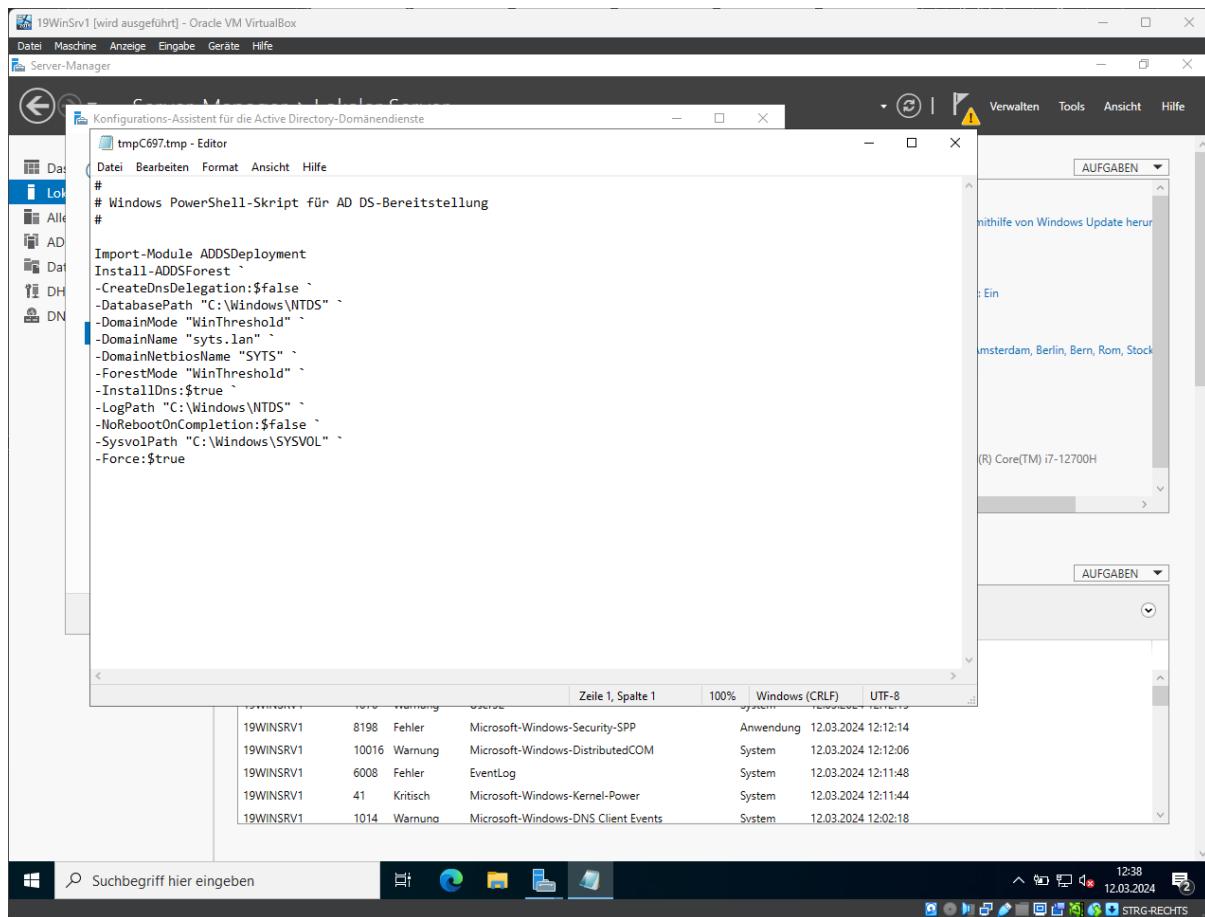
Zuerst richten wir das Active Directory ein, damit die DHCP Benutzer (welche später automatisch angelegt werden) gleich im AD sind und der DHCP und DNS Server autorisierte Server im AD sind.

Beim ersten neue Gesamtstruktur, kein ReadOnly (weil erster).

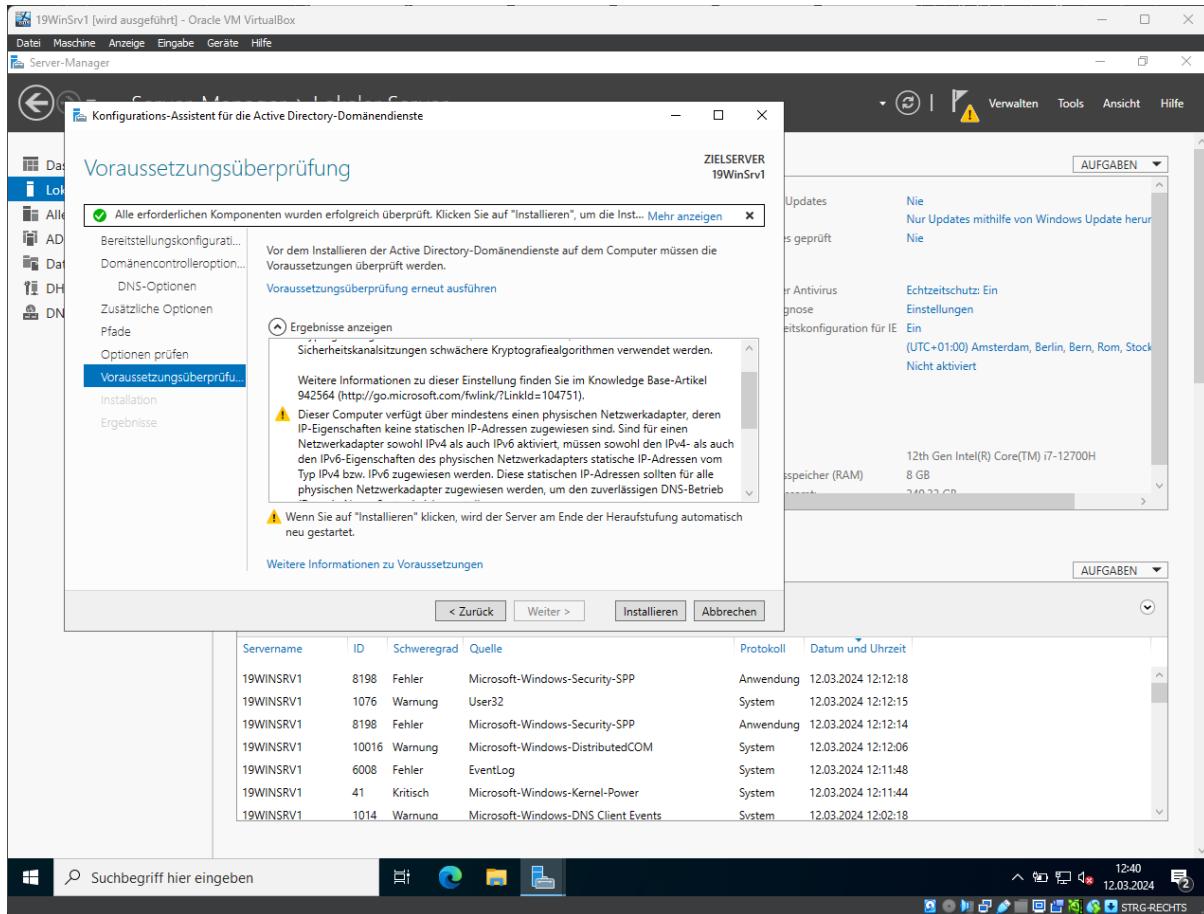




Man könnte alles auch mit zwei PS Befehlen machen:

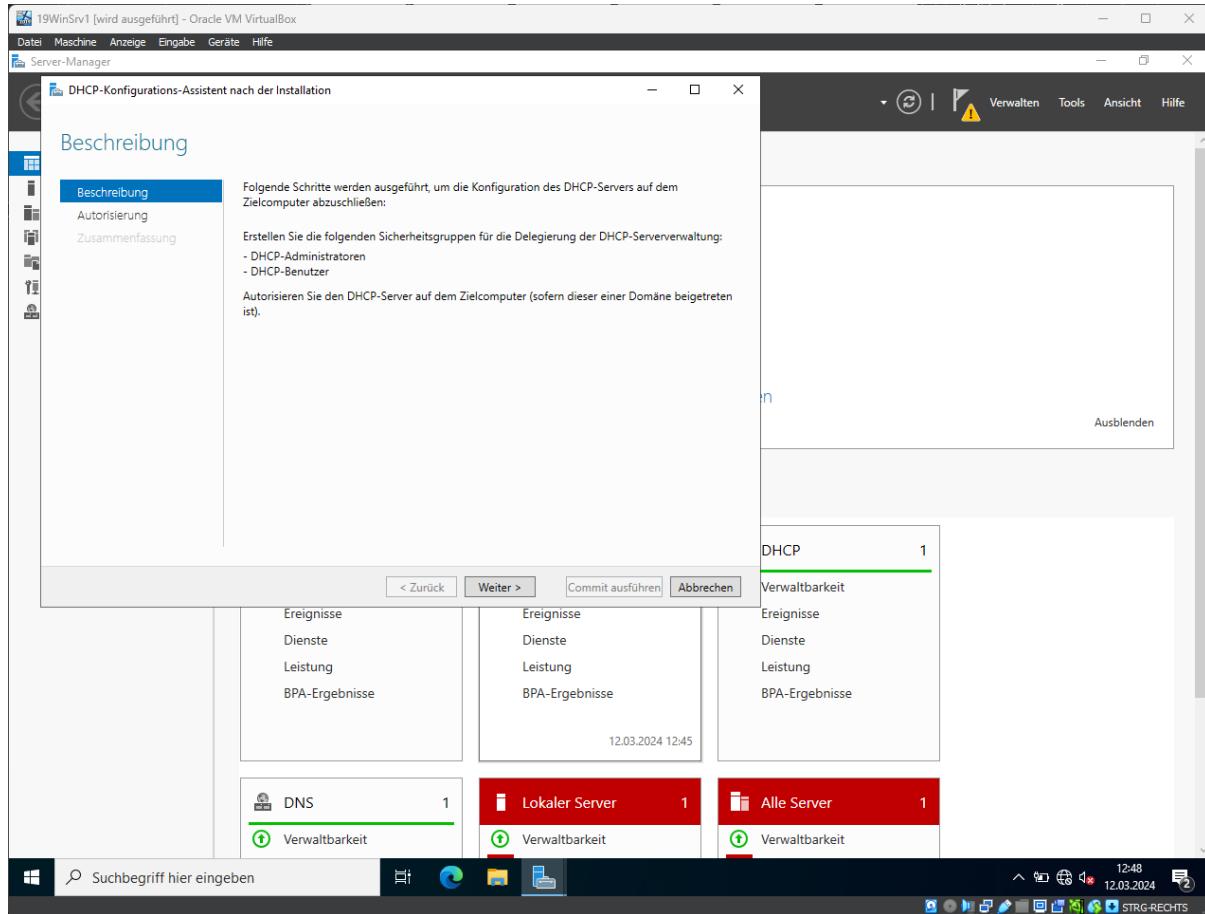


Wenn der Installieren Button klickbar ist, dann klicken, dann geht alles. Falls nicht, muss irgendetwas schief gegangen sein, und man muss die Fehlermeldungen anschauen.



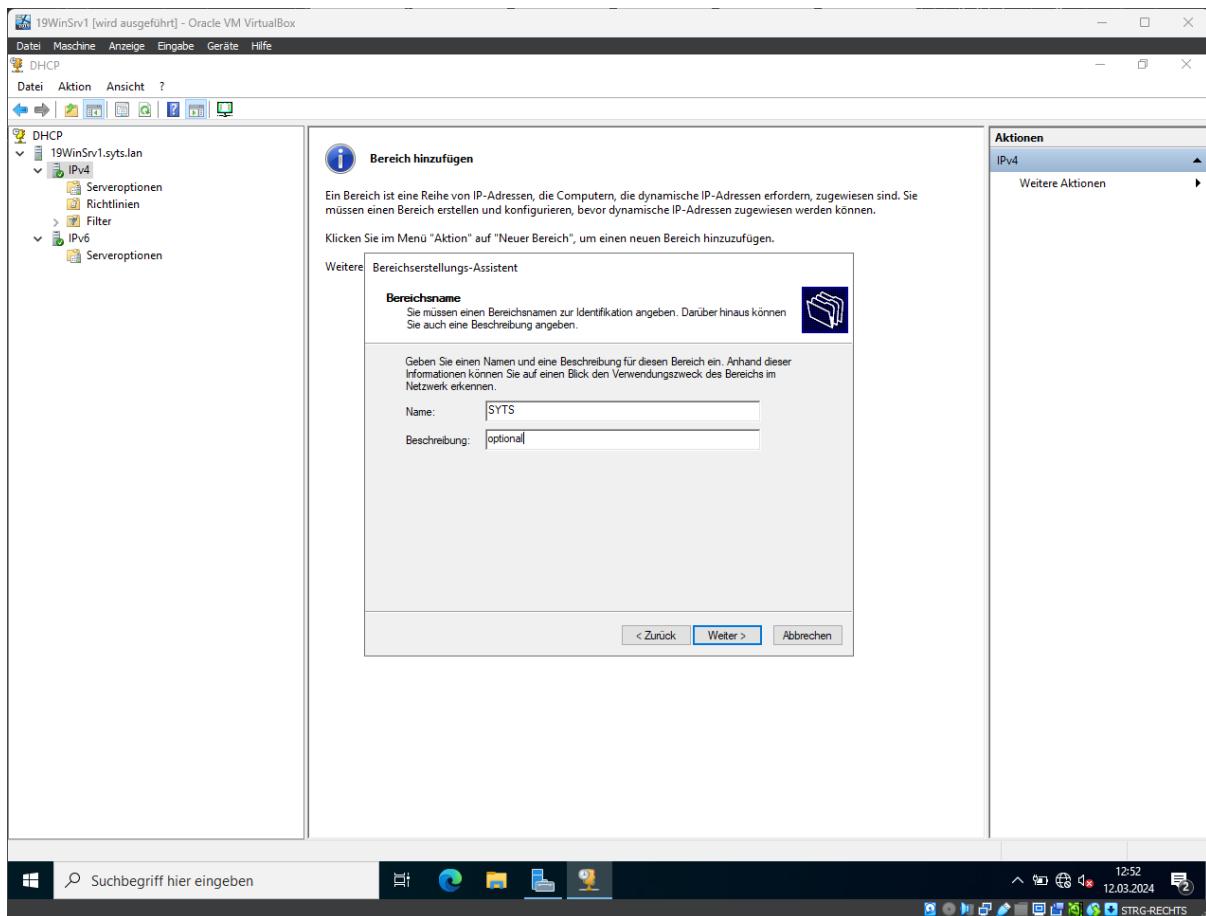
DHCP einrichten

Dabei werden auch 2 Benutzer angelegt, die DHCP verwaltet.

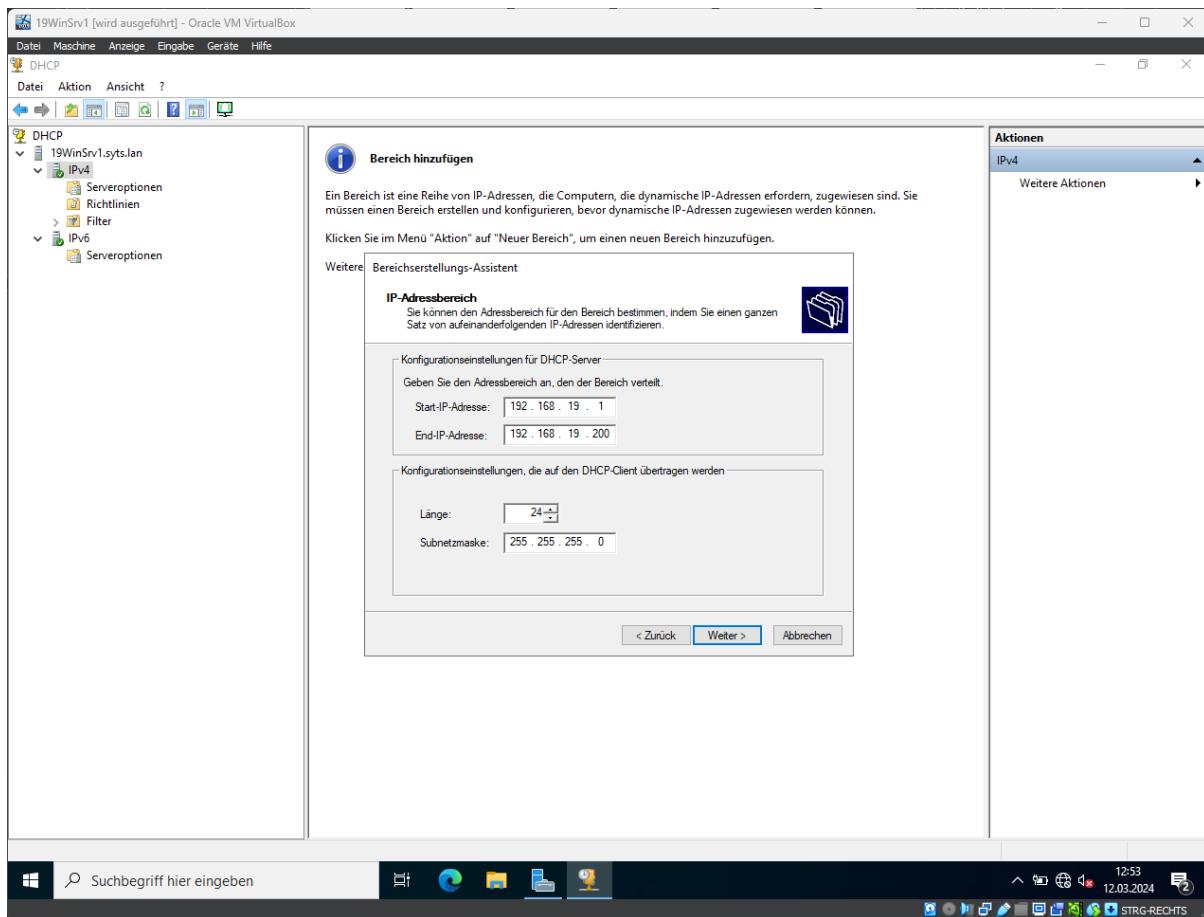


Commit = Bestätigen (wird dauerhaft in Datenbank gespeichert), AD im Hintergrund ja Datenbank

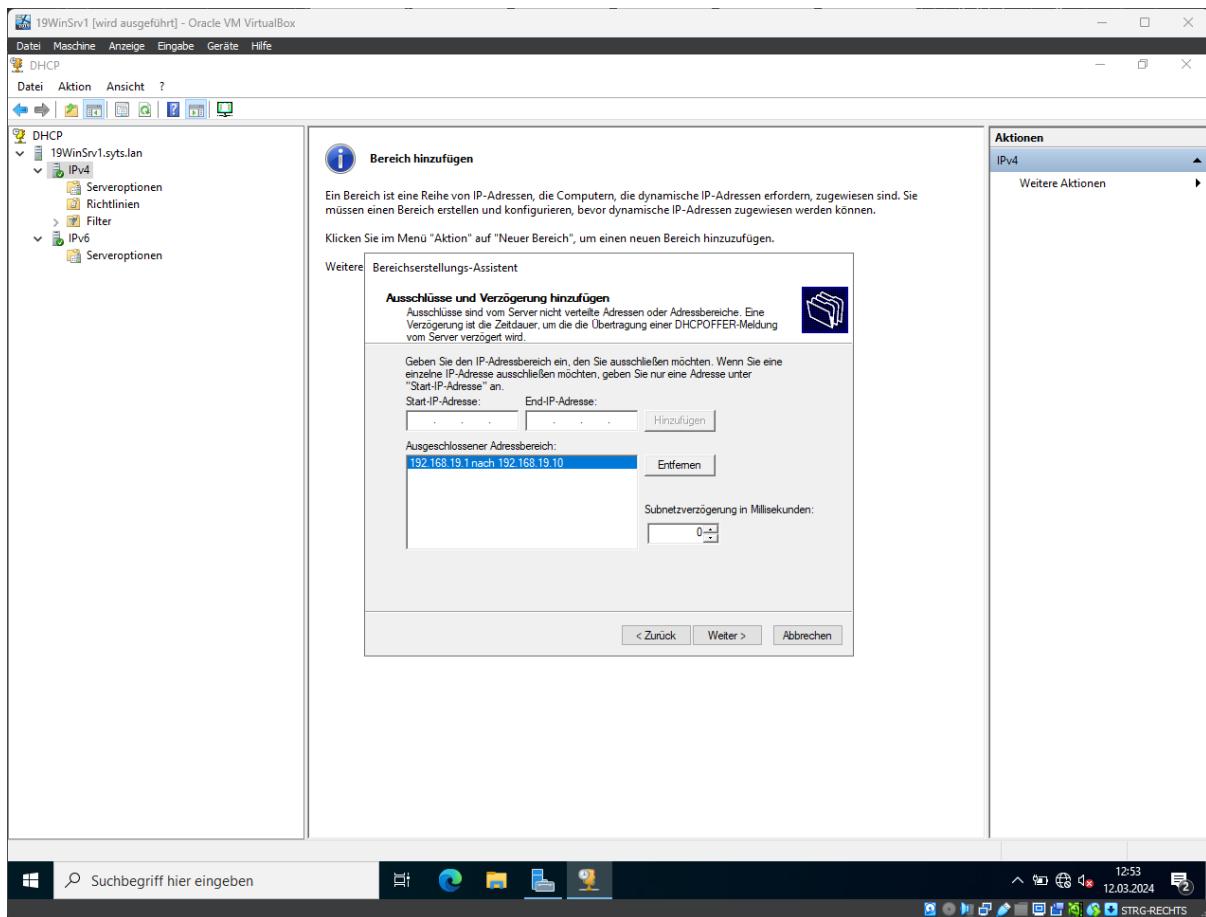
Rollback = Zurücksetzen auf einen alten Stand der Datenbank.

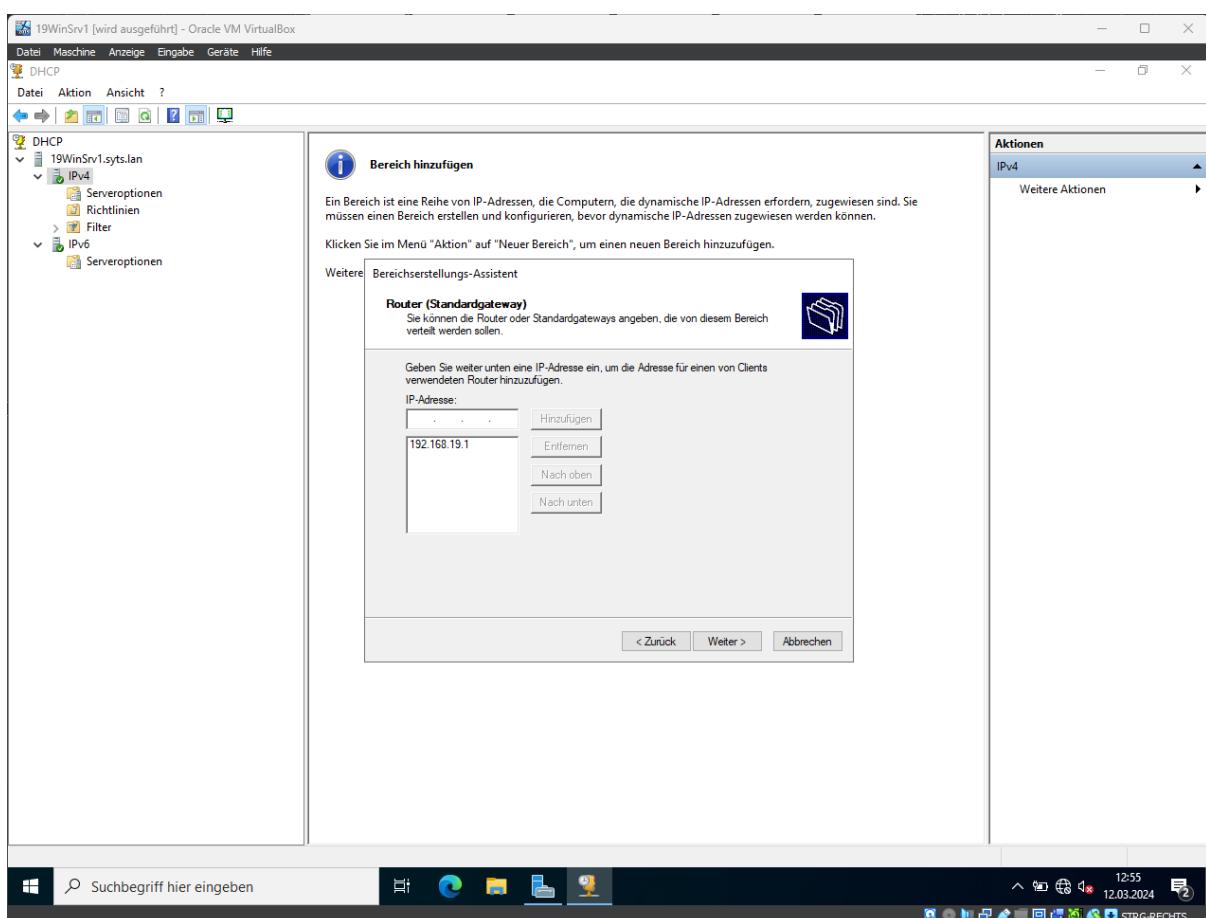
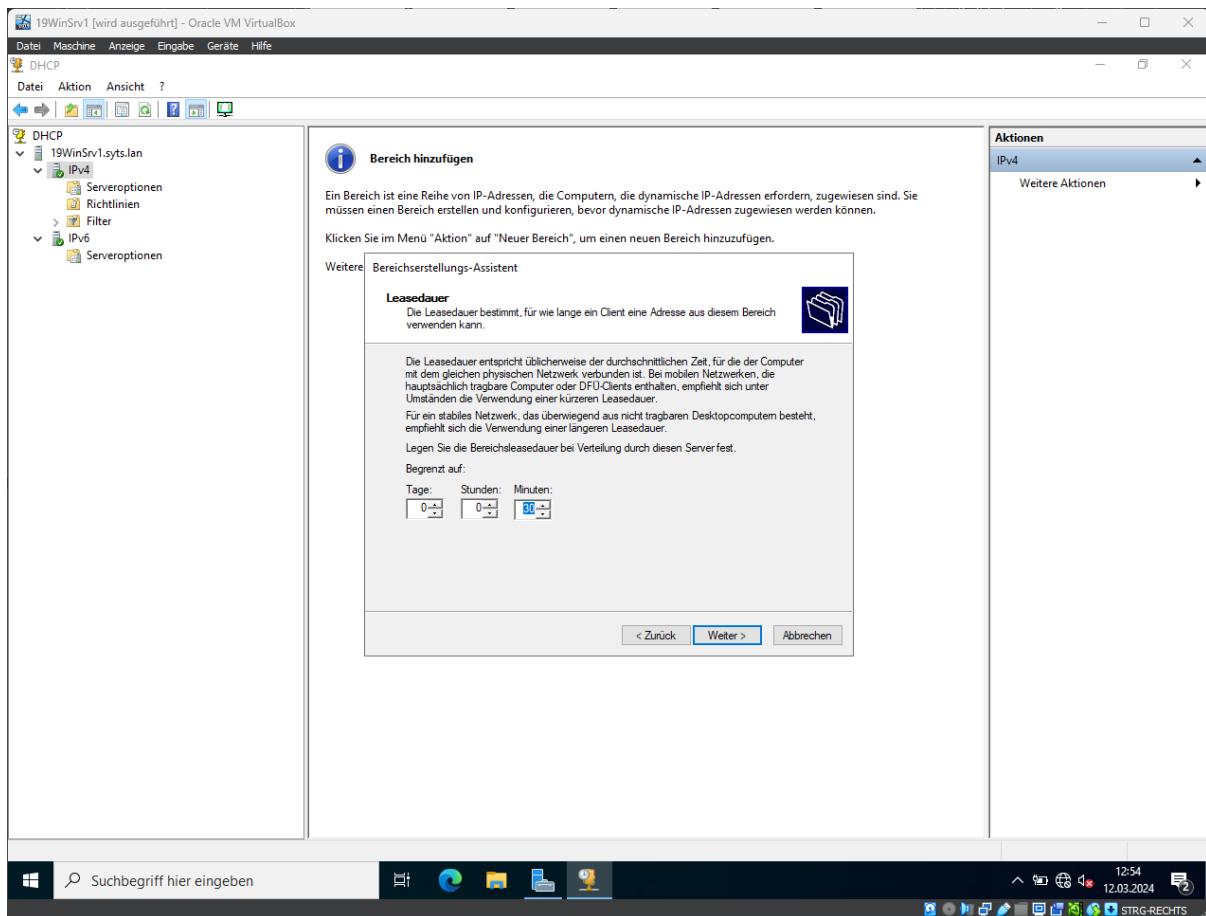


Selbst im Bereich drinnen sein:



Dafür den Bereich ausschließen, wo Server liegen:





Gerade eben konfigurierte Konfiguration:

The screenshot shows the Windows Server 2019 DHCP Management console. The left pane displays a tree view of the DHCP configuration for the scope 'Bereich [192.168.19.0] SYTS'. The right pane shows a table of options with their values. The 'Bereichsoptionen' action is selected in the Actions pane.

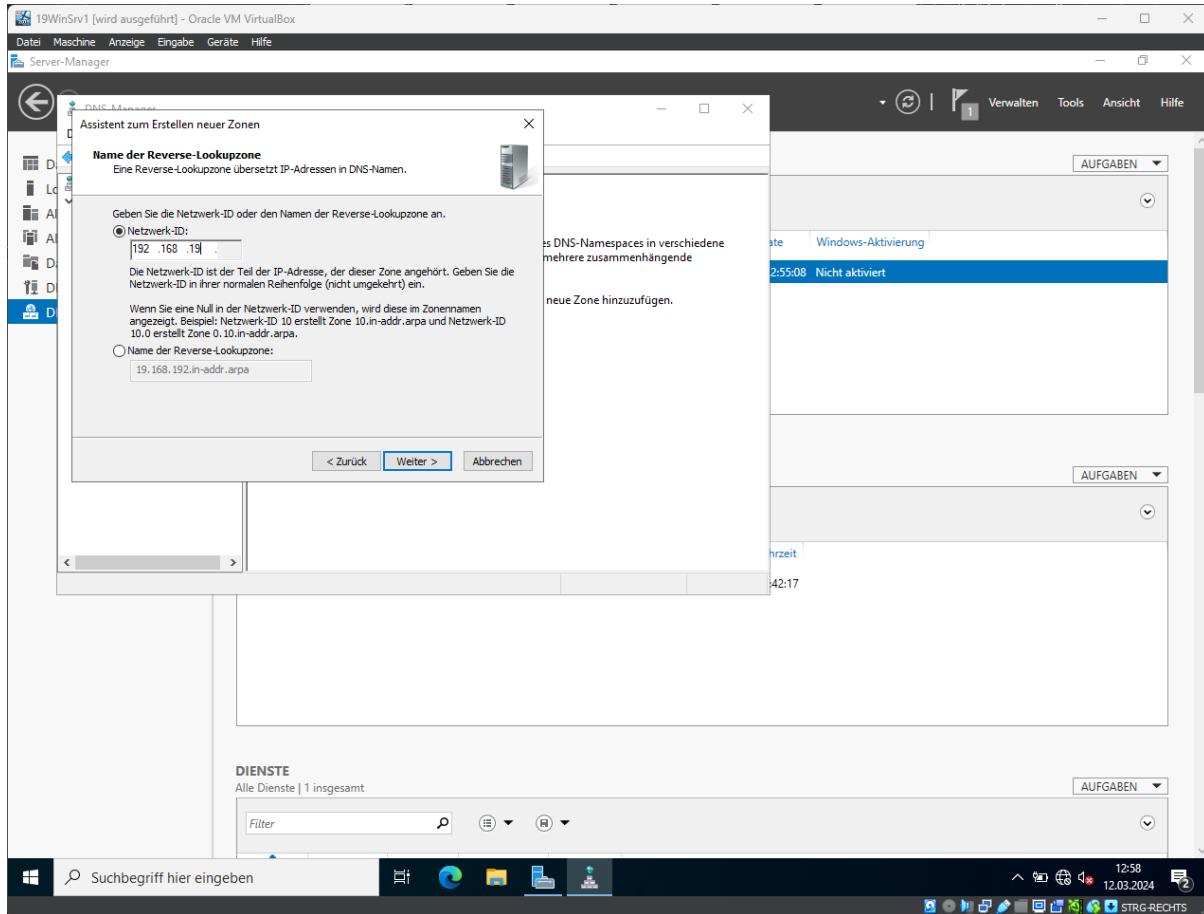
Optionsname	Hersteller	Wert	Richtliniename
003 Router	Standard	192.168.19.1	Keine
006 DNS-Server	Standard	192.168.19.1	Keine
015 DNS-Domänenname	Standard	syts.lan	Keine

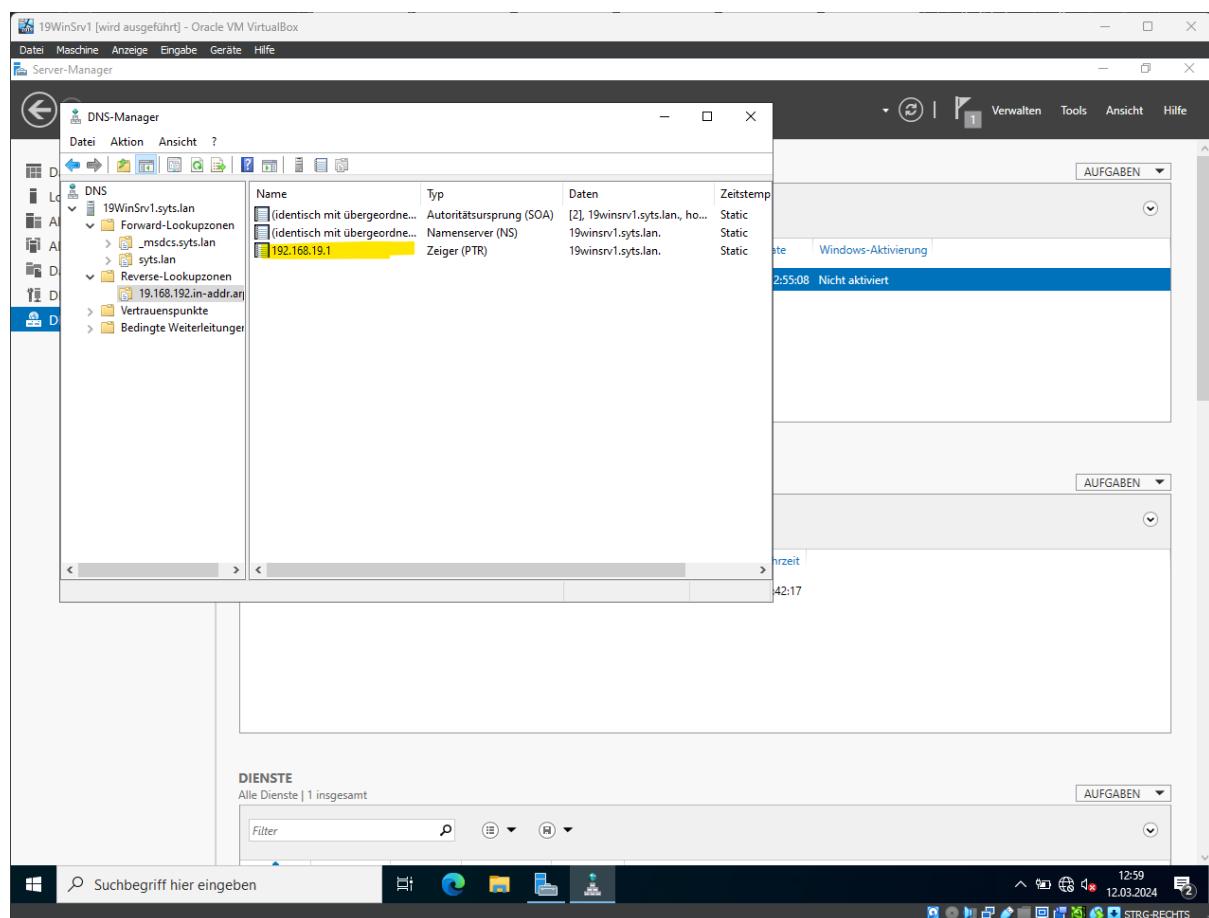
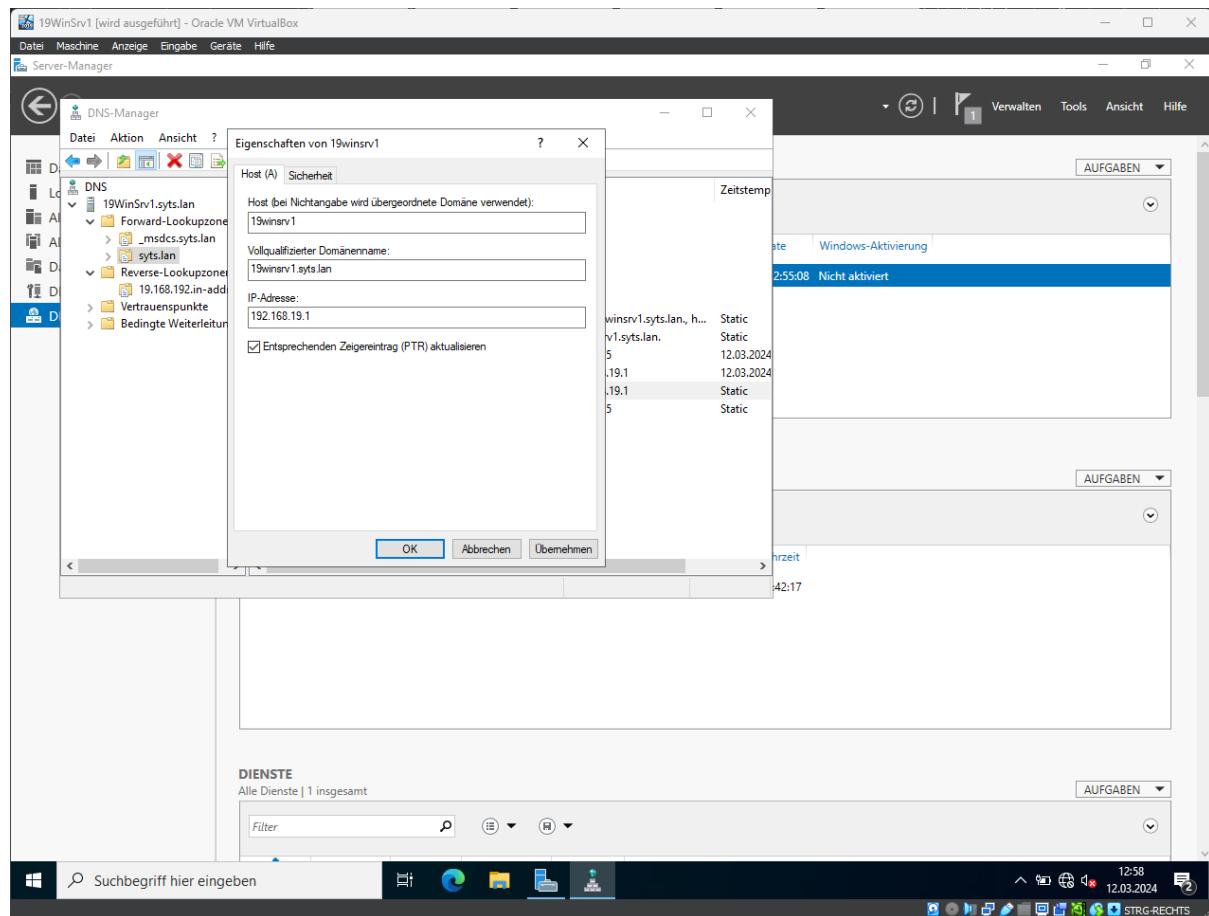
Aktionen

- Bereichsoptionen
- Weitere Aktionen

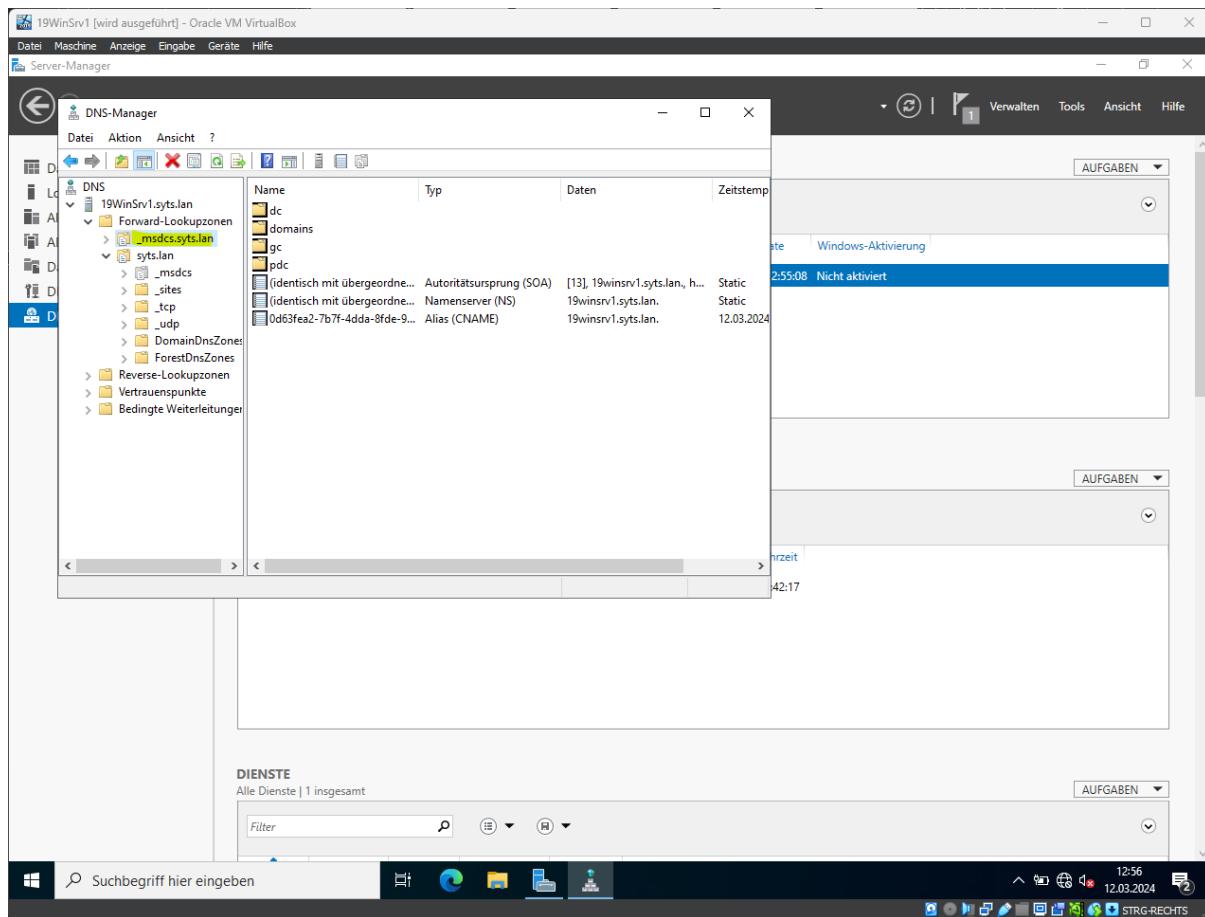
DNS einrichten

Ist automatisch eingerichtet worden. Nur die Reverse Zone muss noch erstellt werden:

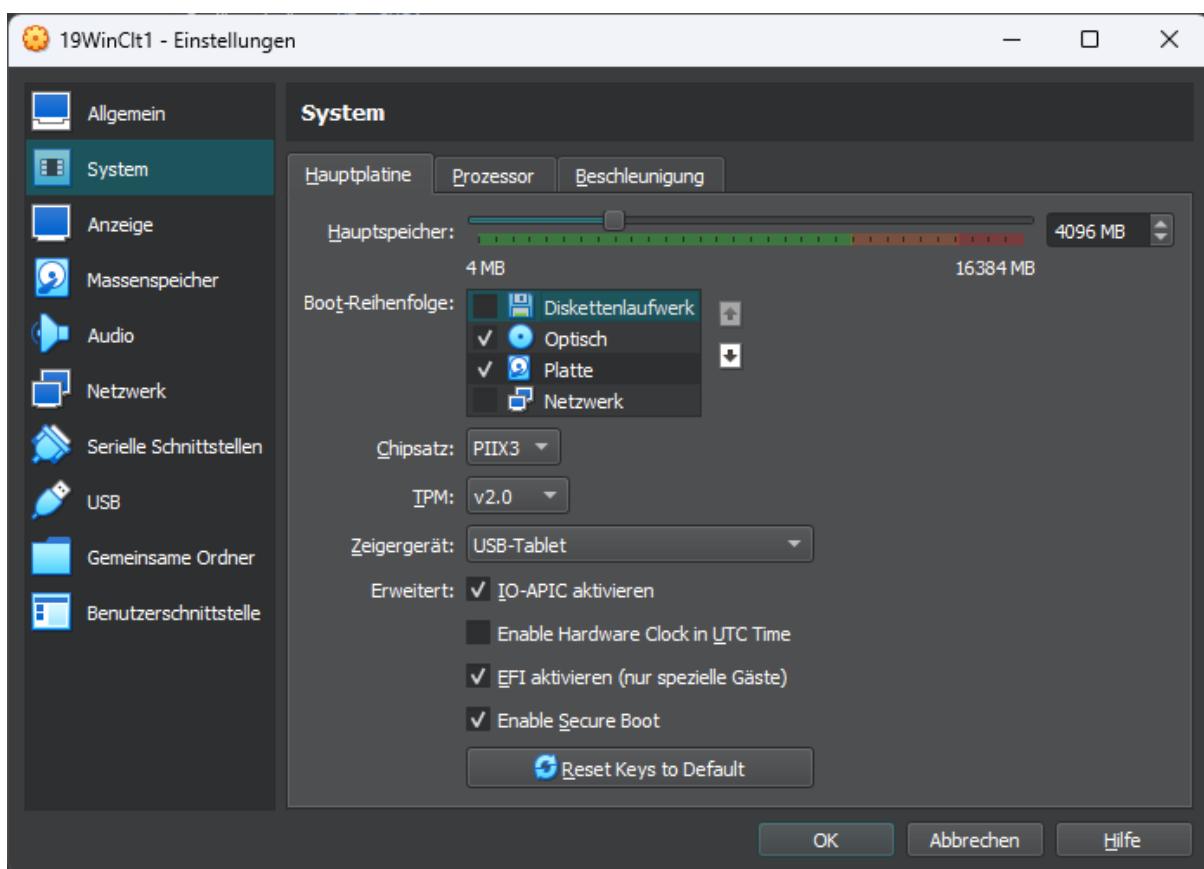
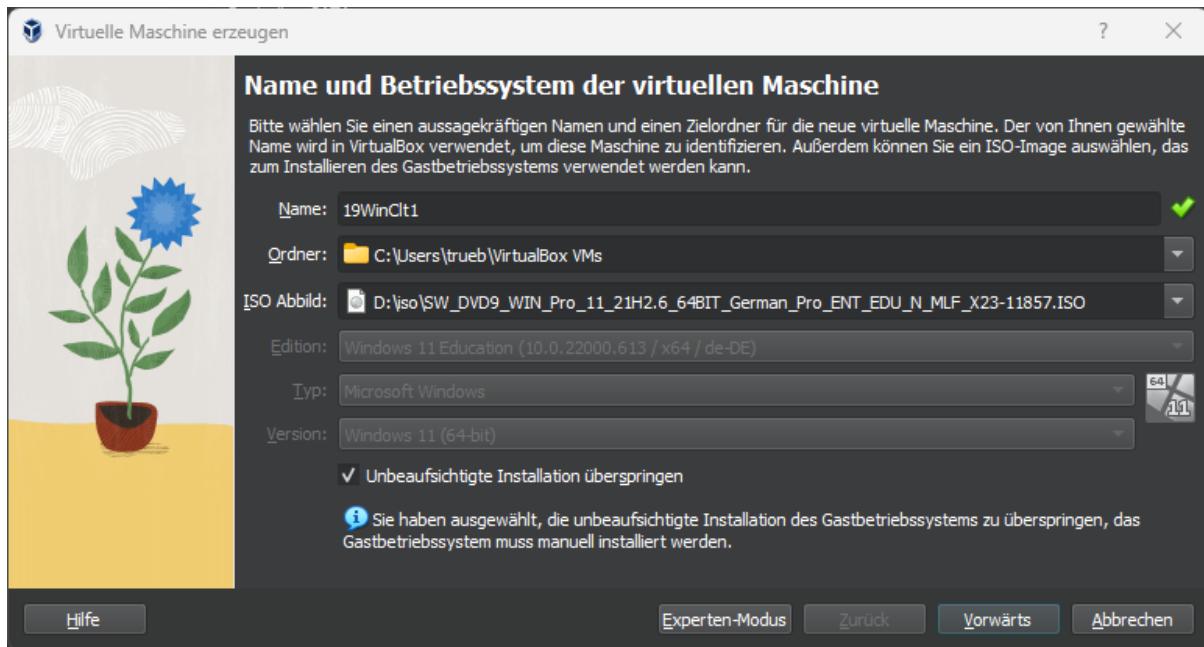


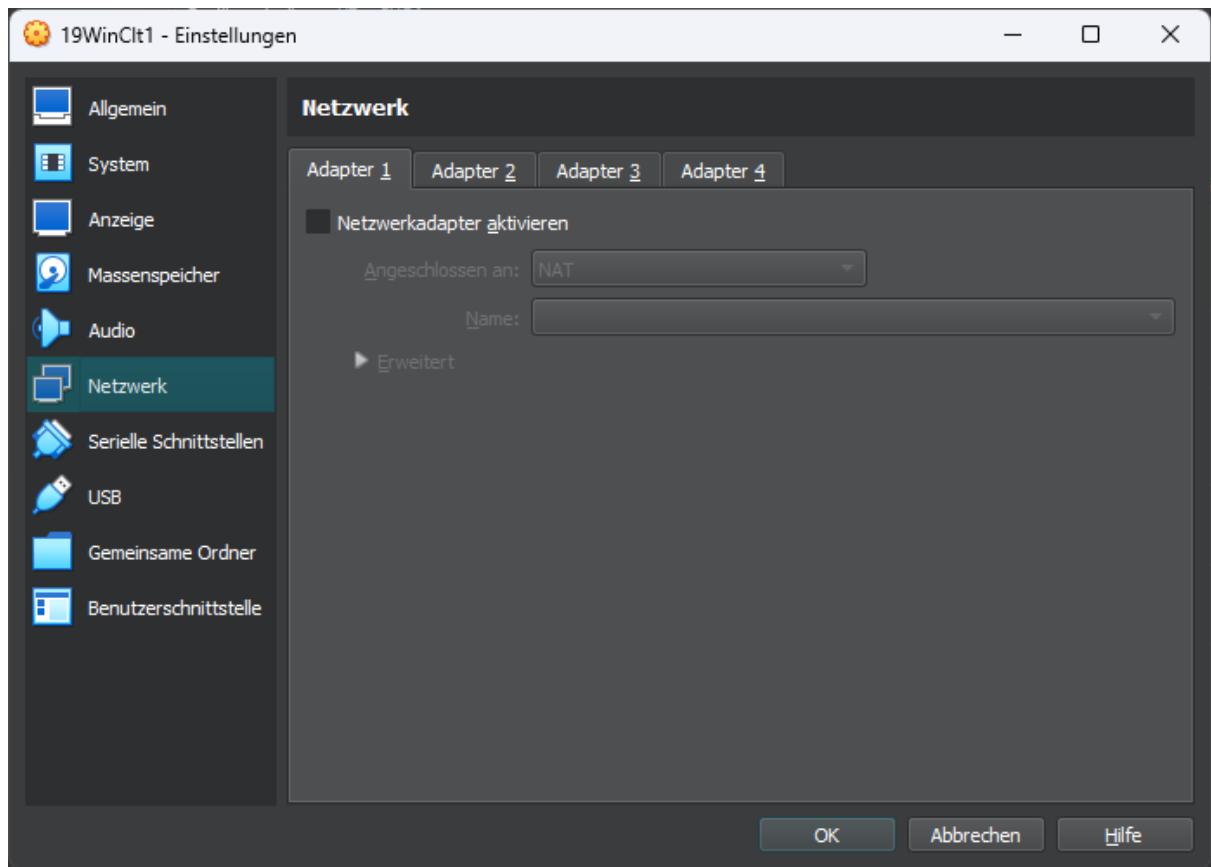


Domainenspezifische Sache in der komischen Zone:



Client aufsetzen





Starten: Die boot.wim Datei in der iso Datei gibt die Liste mit verschiedenen Versionen von Windows an, welche man beim Installieren von Windows auswählen kann. Sicherheitsfragen könnten beim WDS (PXE Boot) auch mittels Antwortdatei umgangen werden.

Netzwerk, Namen ändern und Domain beitreten

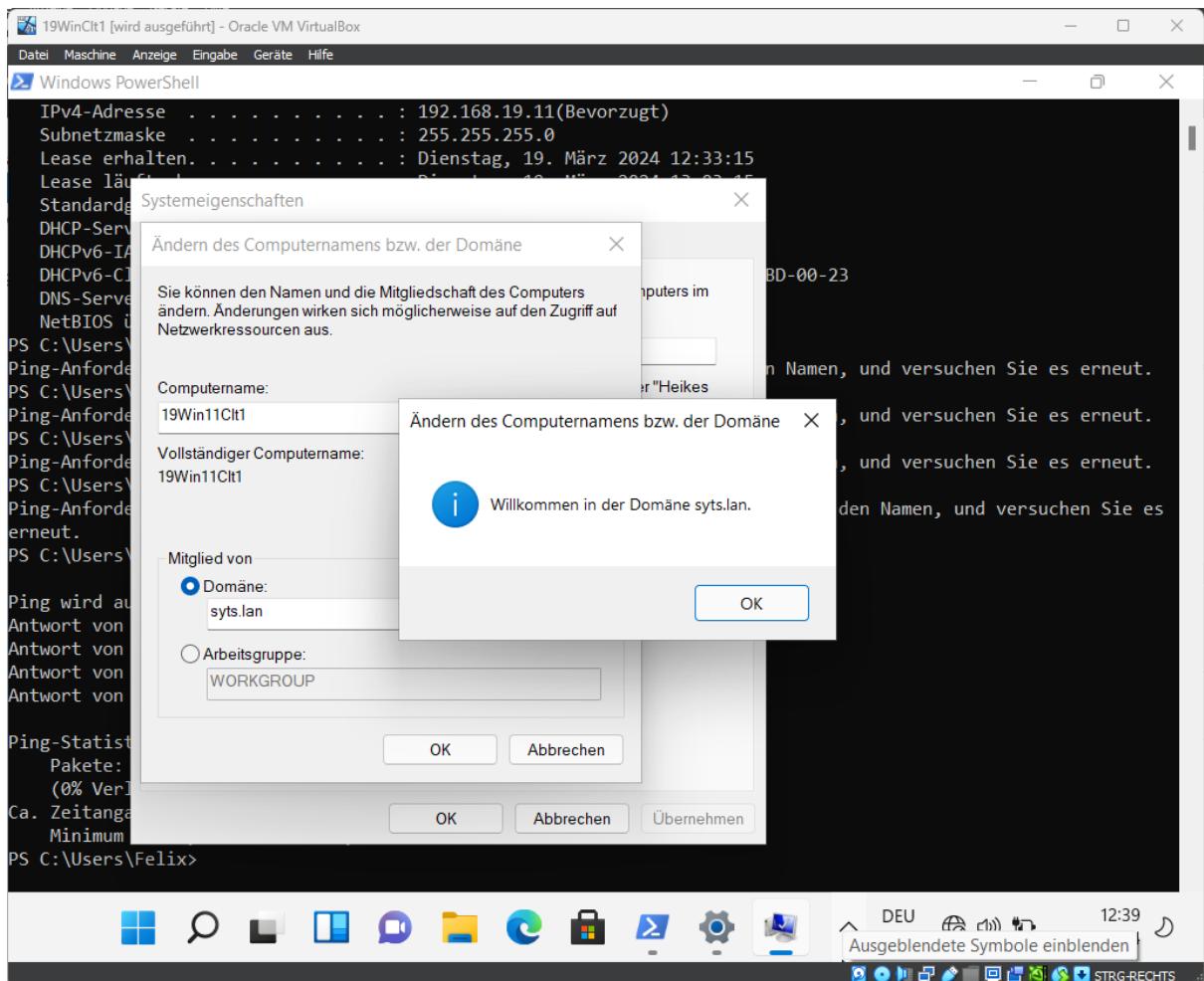
```
19WinClt1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Windows PowerShell
PS C:\Users\Felix> ipconfig /all

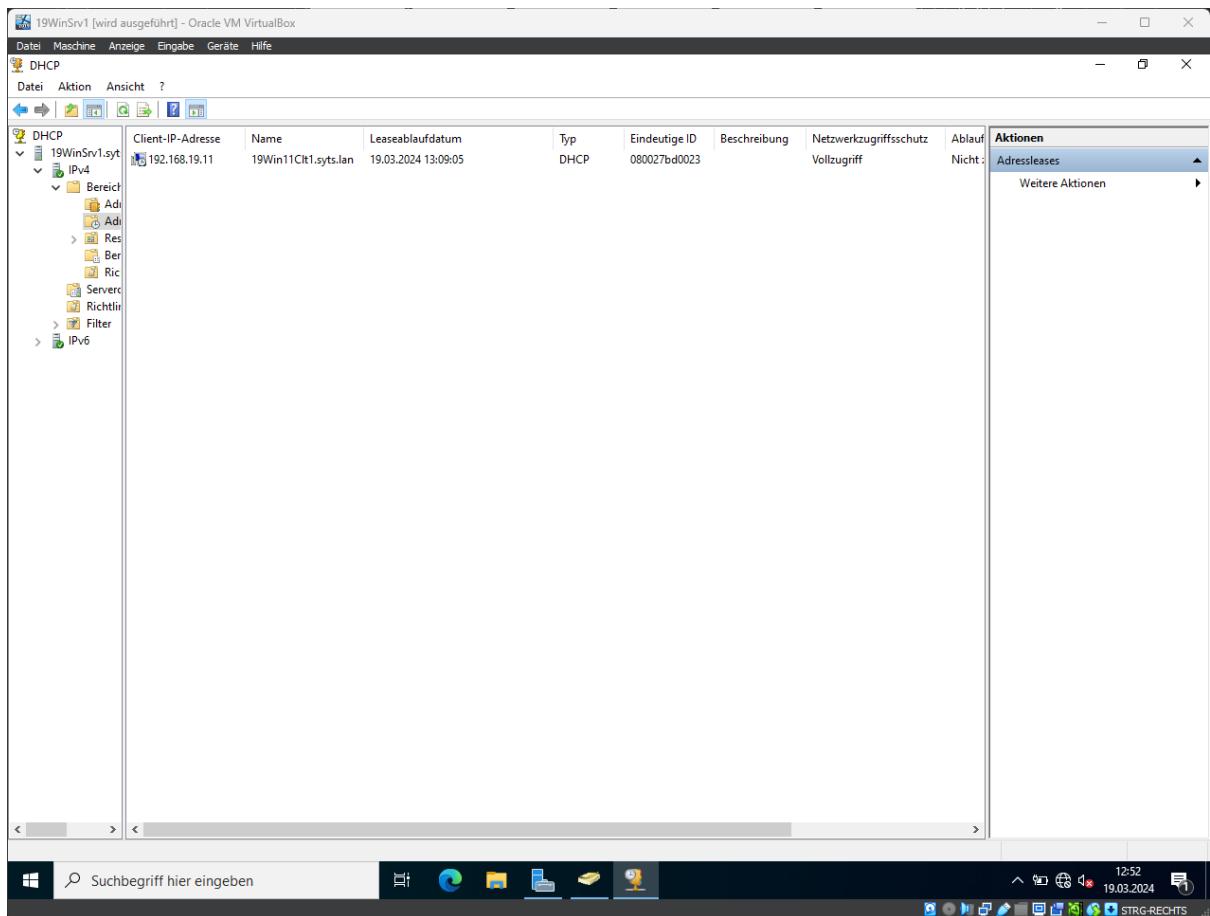
Windows-IP-Konfiguration

Hostname . . . . . : DESKTOP-QSRA8DG
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert . . . . . : Nein
WINS-Proxy aktiviert . . . . . : Nein
DNS-Suffixsuchliste . . . . . : syts.lan

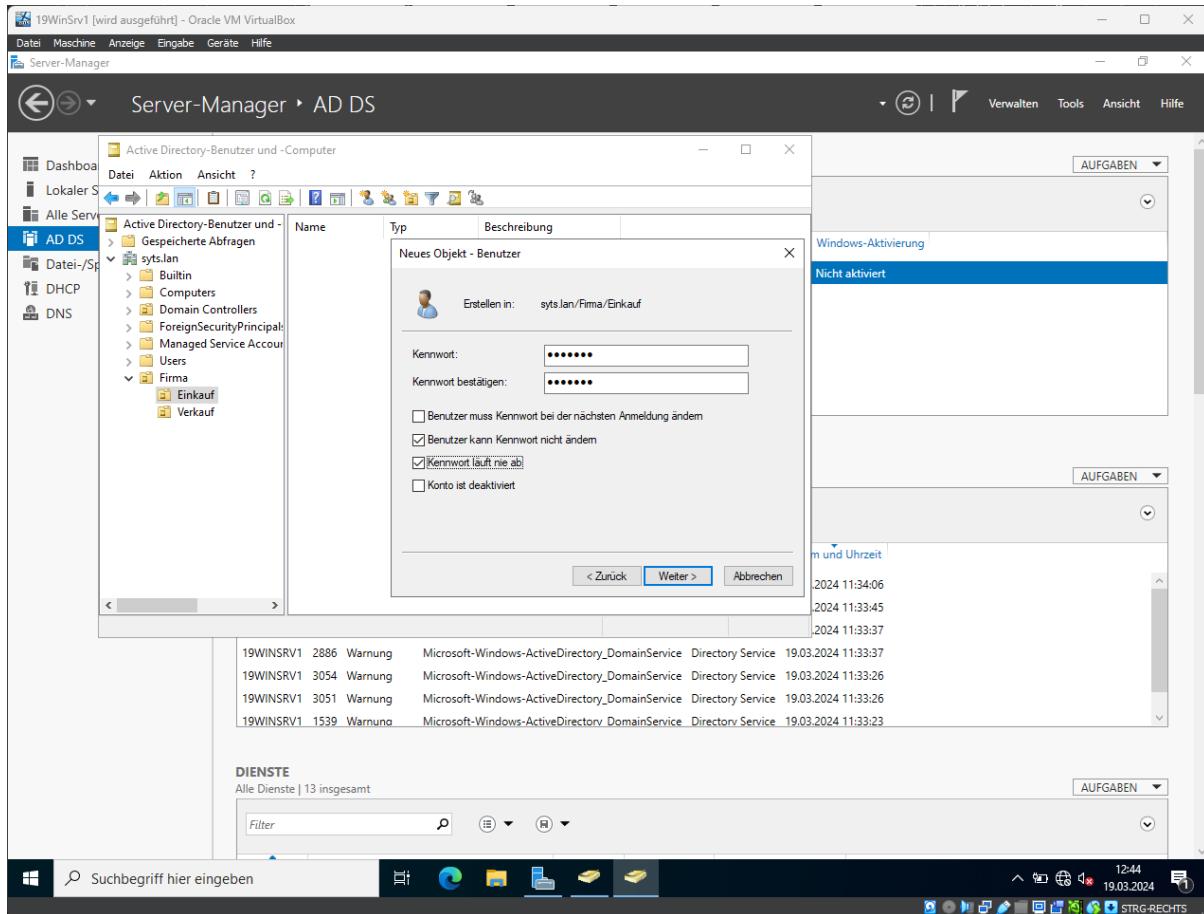
Ethernet-Adapter Ethernet:

Verbindungsspezifisches DNS-Suffix: syts.lan
Beschreibung. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physische Adresse . . . . . : 08-00-27-BD-00-23
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . . . : Ja
Verbindungslokale IPv6-Adresse . . . . . : fe80::e5ea:7a45:1440:287b%14(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.19.11(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Dienstag, 19. März 2024 12:33:15
Lease läuft ab. . . . . : Dienstag, 19. März 2024 13:03:15
Standardgateway . . . . . : 192.168.19.1
DHCP-Server . . . . . : 192.168.19.1
DHCPv6-IAID . . . . . : 235405351
DHCPv6-Client-DUID. . . . . : 00-01-00-01-2D-8B-30-53-08-00-27-BD-00-23
DNS-Server . . . . . : 192.168.19.1
NetBIOS über TCP/IP . . . . . : Aktiviert
PS C:\Users\Felix>
```





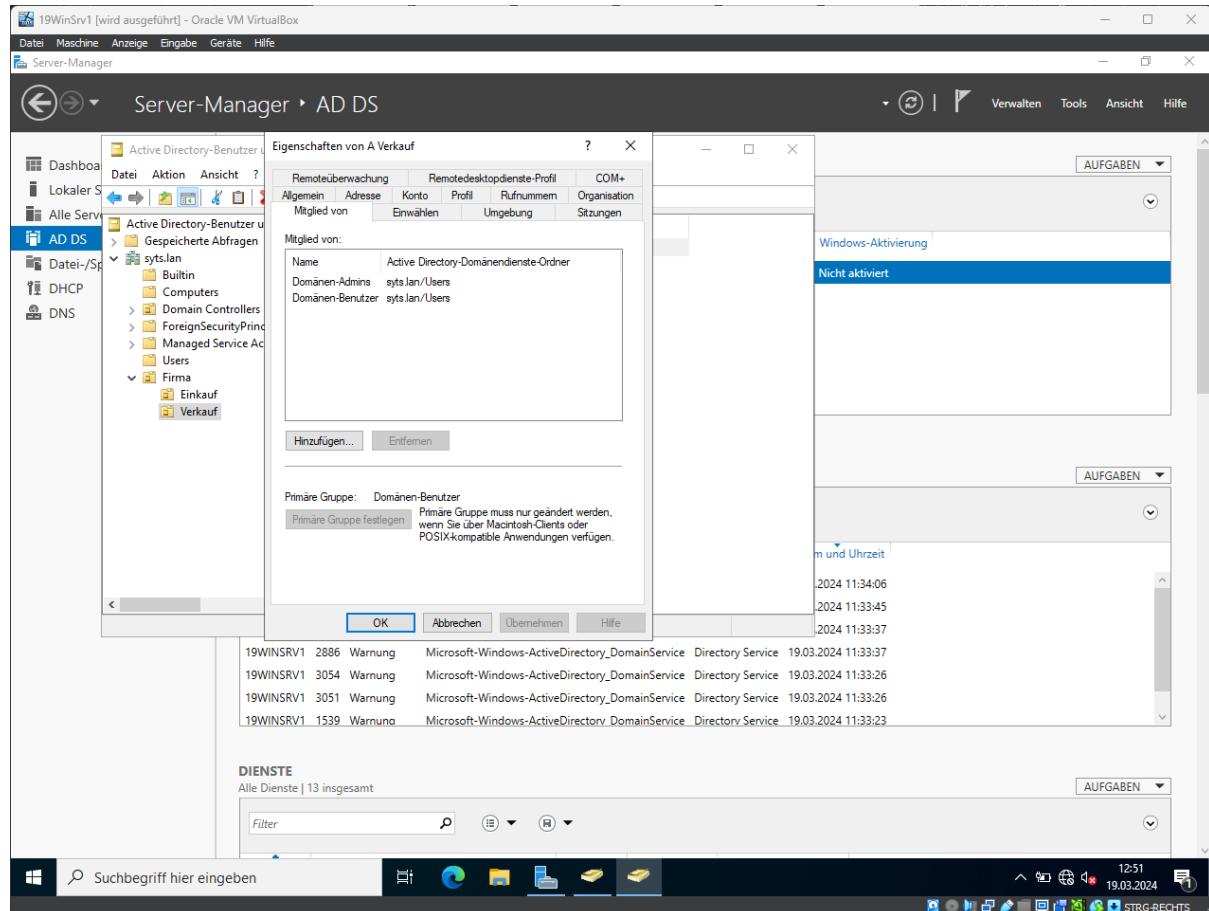
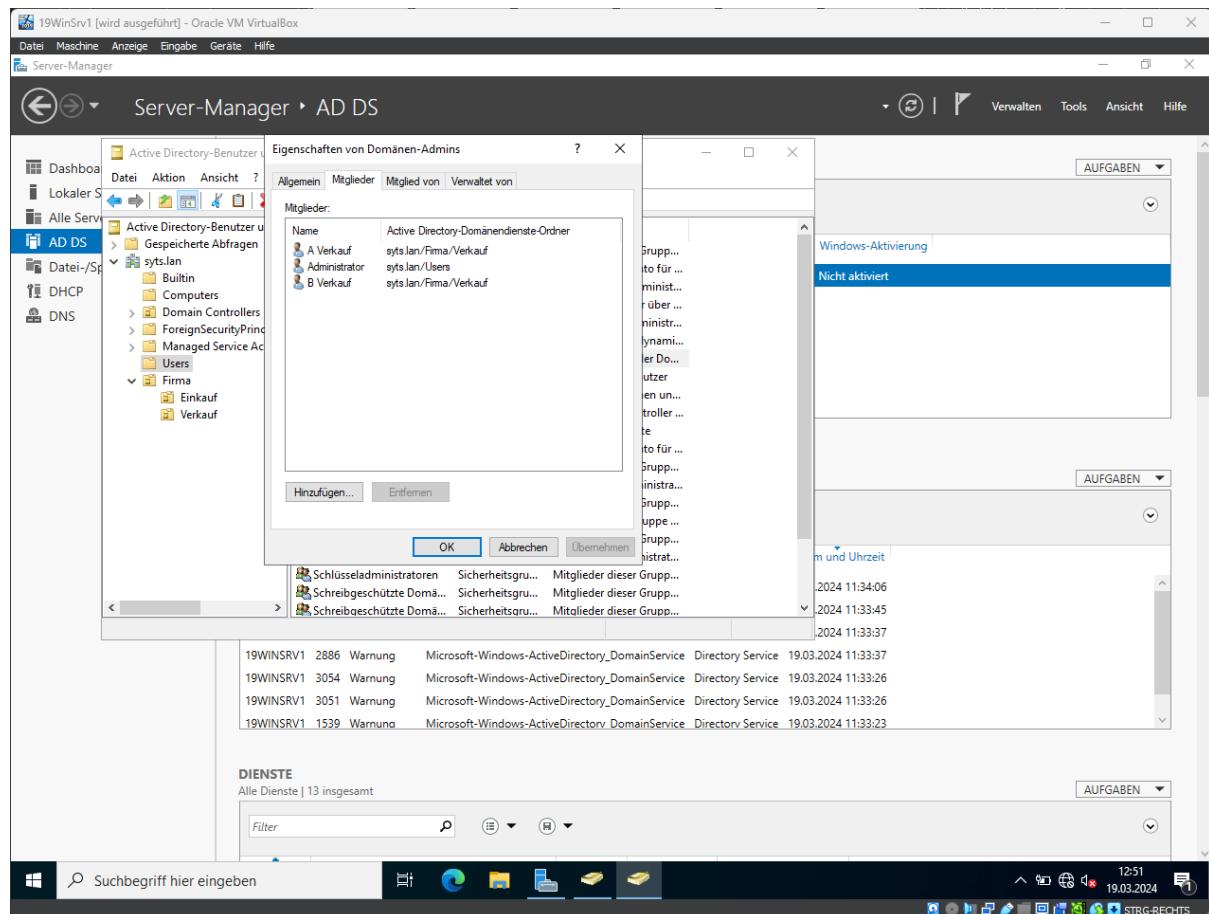
Benutzer erstellen und Gruppen

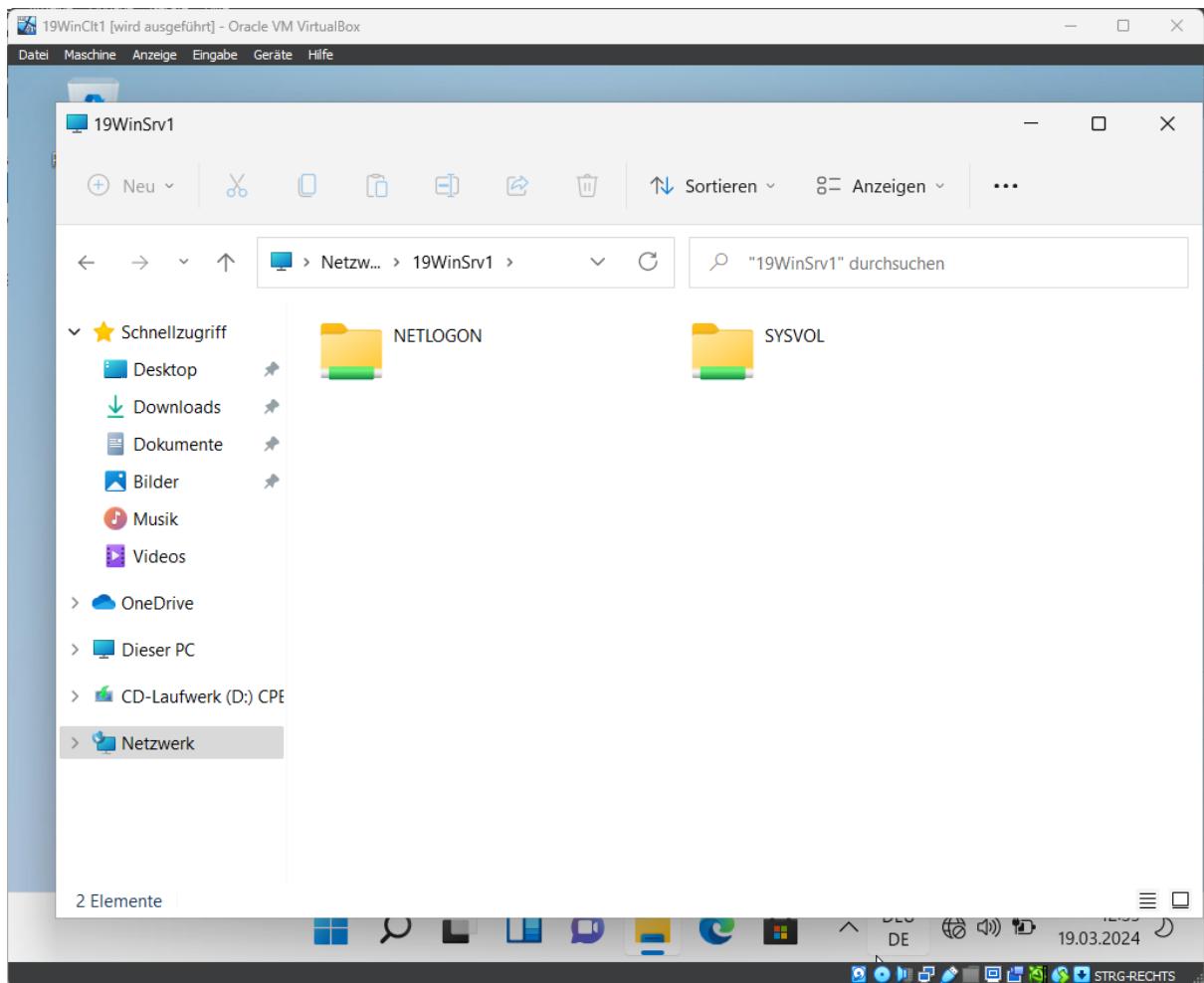


Kennwort läuft standardmäßig nach 2 Monaten ab, wegen einer Domain Policy, die standardmäßig bei Kennwörtern zuschlägt.

Beim Kopieren von Benutzern werden die Einstellungen, Rollen, ... kopiert.

Benutzer können über den Benutzer und über die Gruppe der Gruppe hinzugefügt werden.





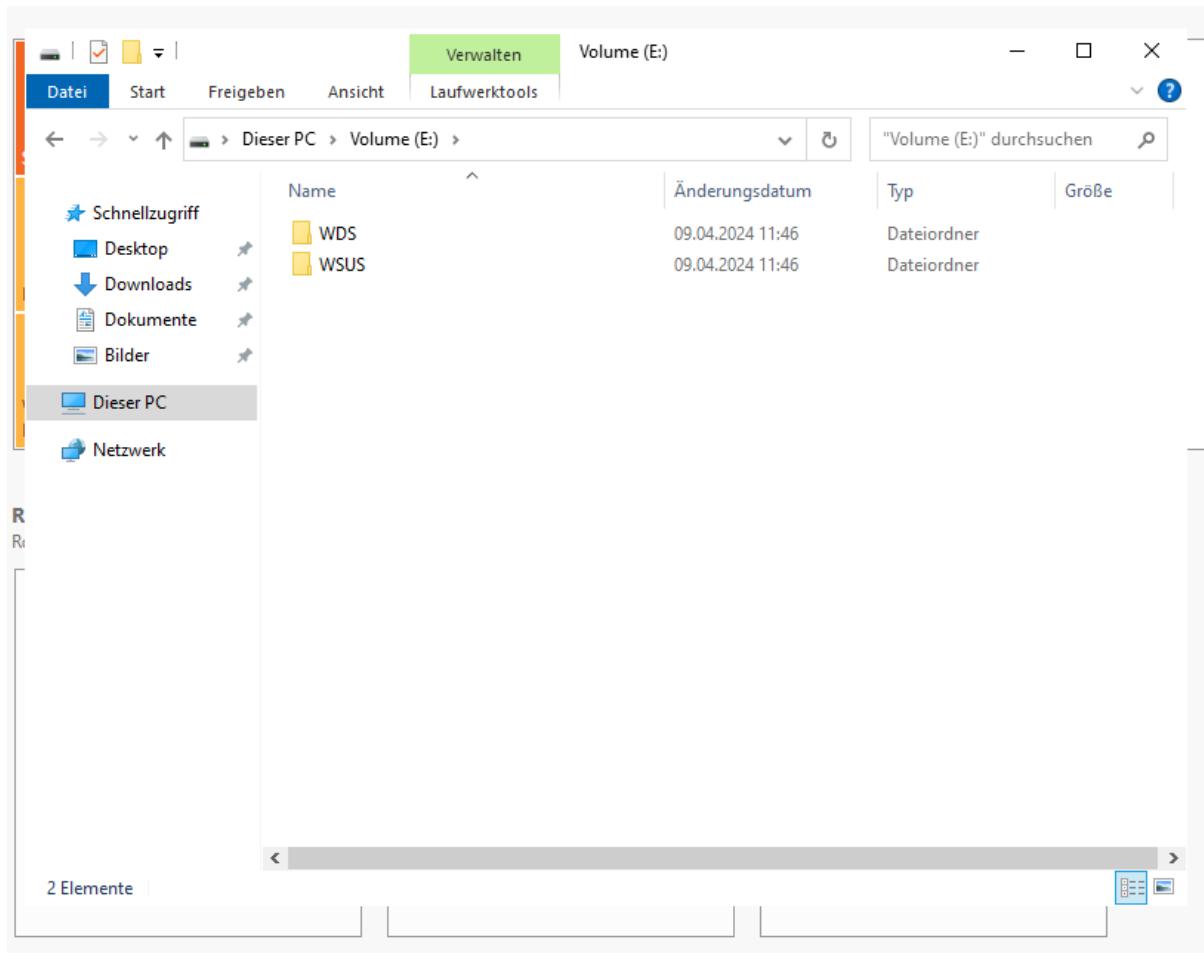
Dienste

WSUS

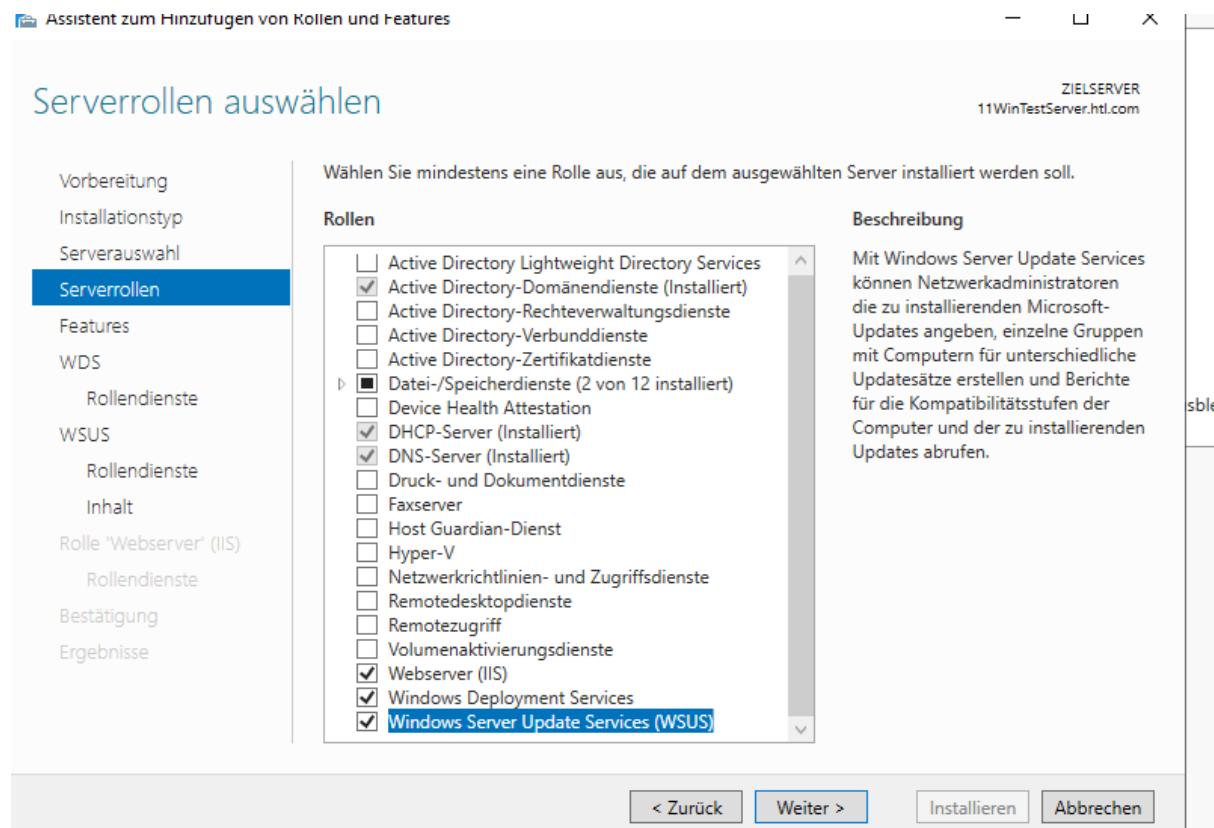
- Weniger Traffik (nicht jeder Client holt selbst updates)
- Man bestimmt, welche Updates Clients bekommen (zentrale Verwaltung)
- Möglichkeit: gar keine Updates

Kann sich Updates auch von anderen Servern holen (Redundanz).

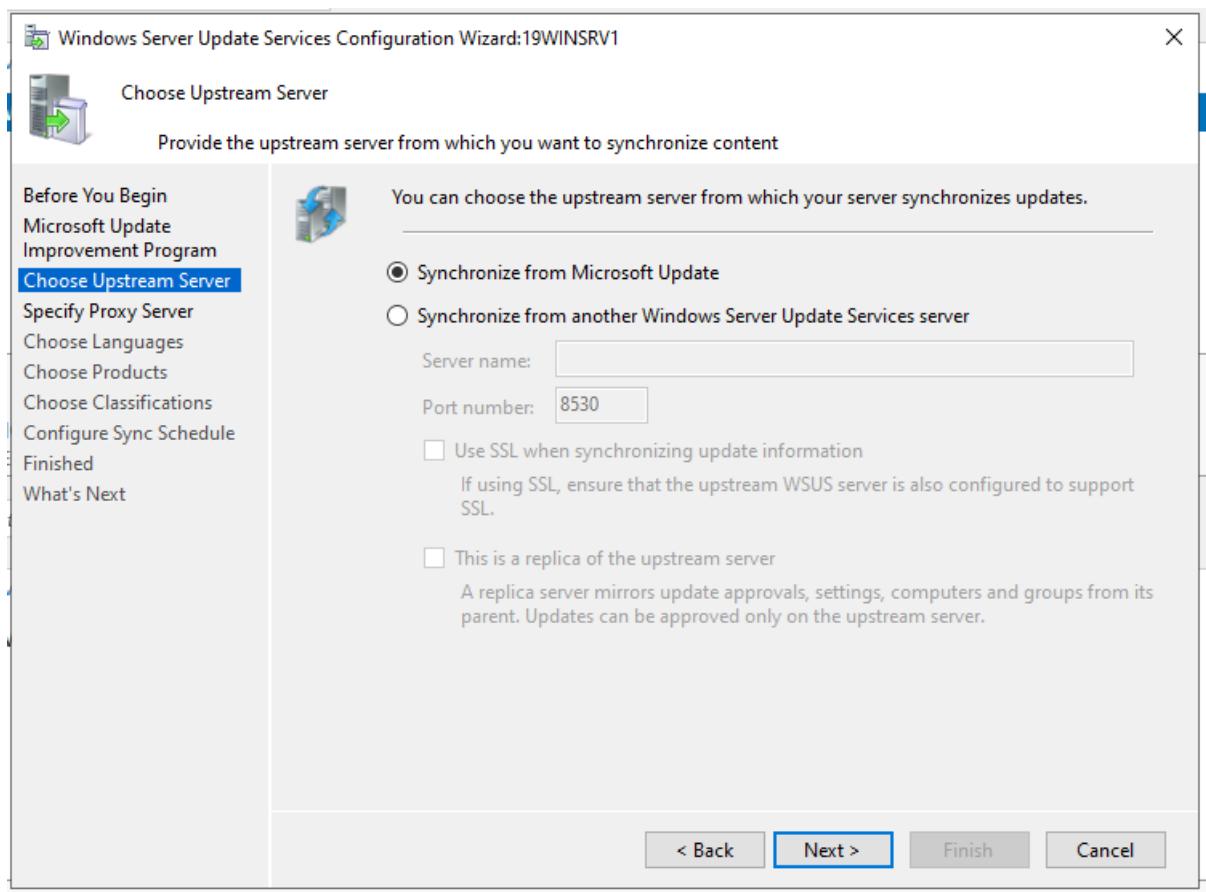
Folder am Volume E erstellen (WSUS) (eigene Platte, damit die Updates nicht die Systemplatte voll machen).



Rolle WSUS installieren (default Features lassen)

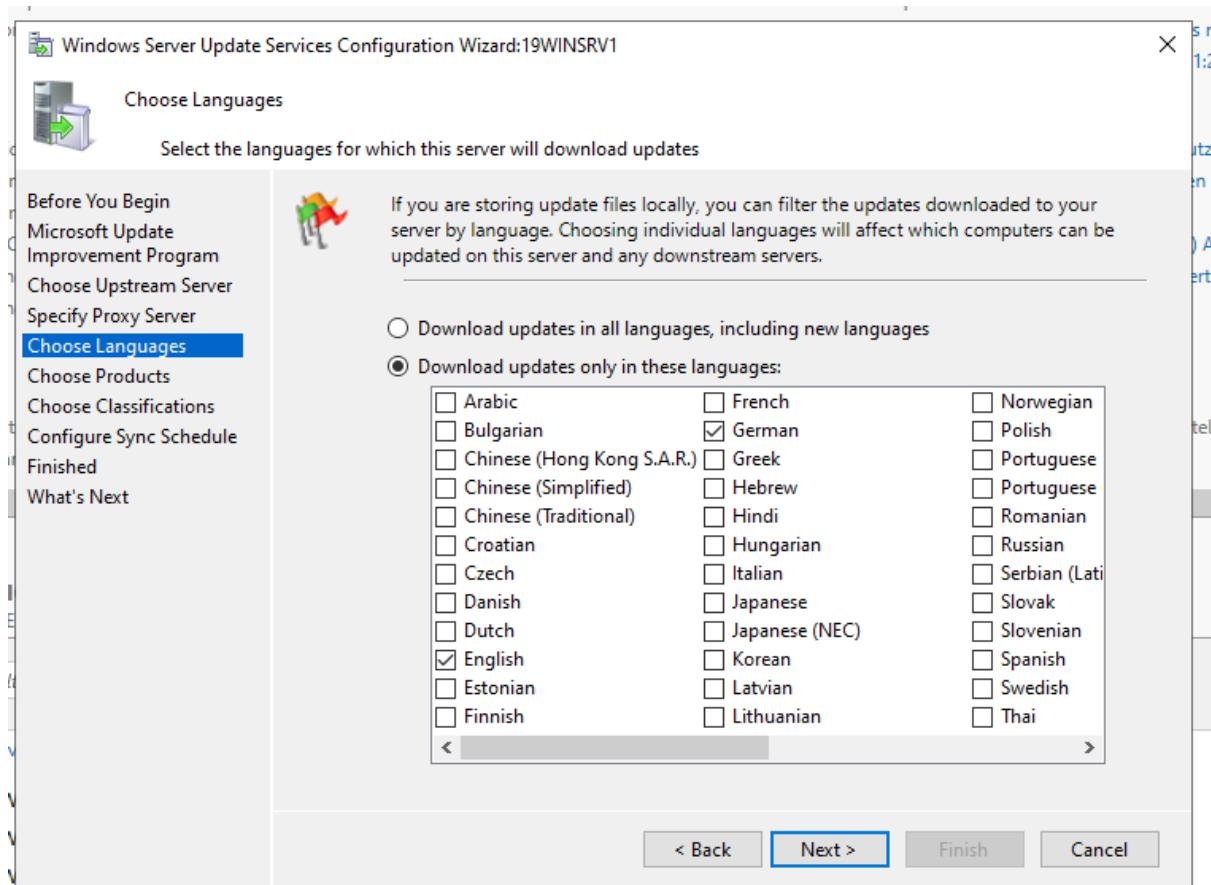


Nachinstallation starten:

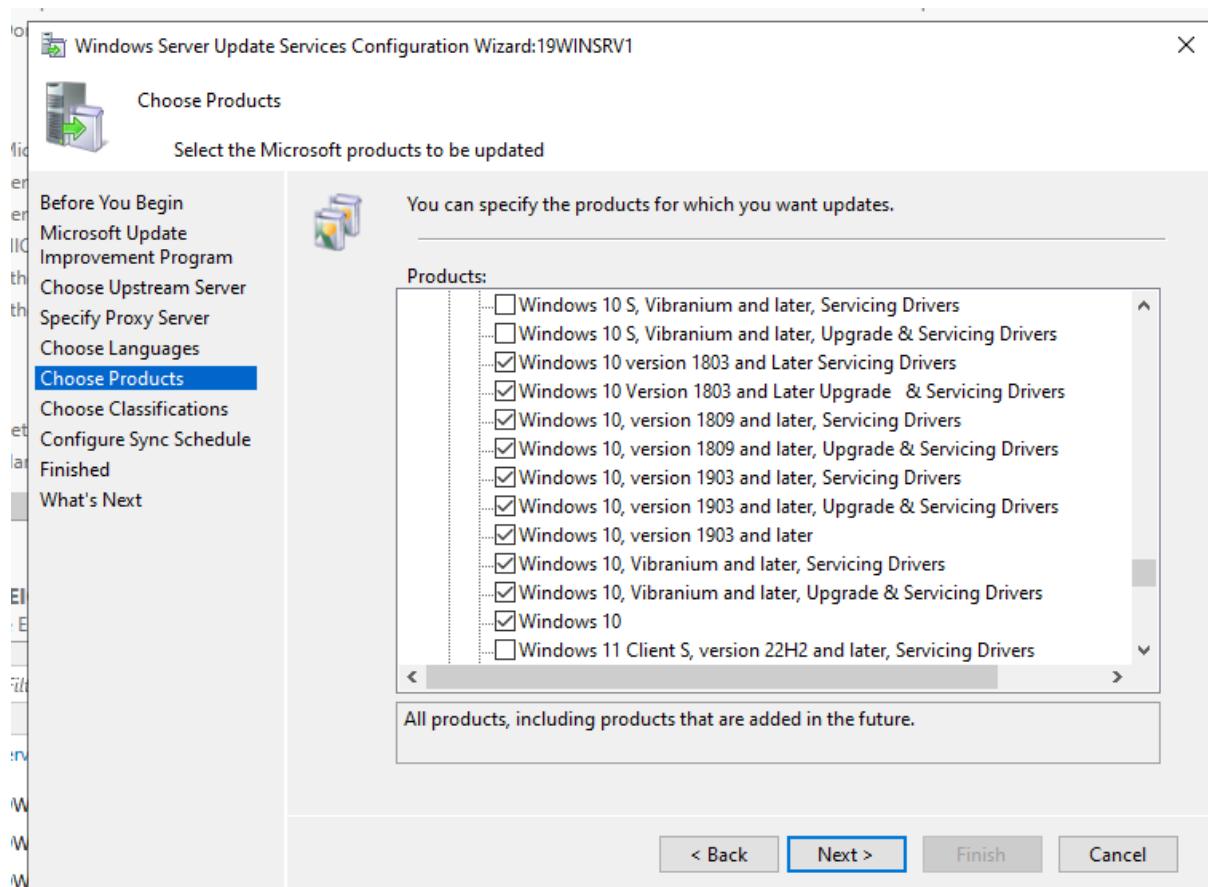


Hier kann man eben bei Matura einen anderen „lokalen“ Server nehmen, der die Updates bereits hat, weil wir kein Internet haben.

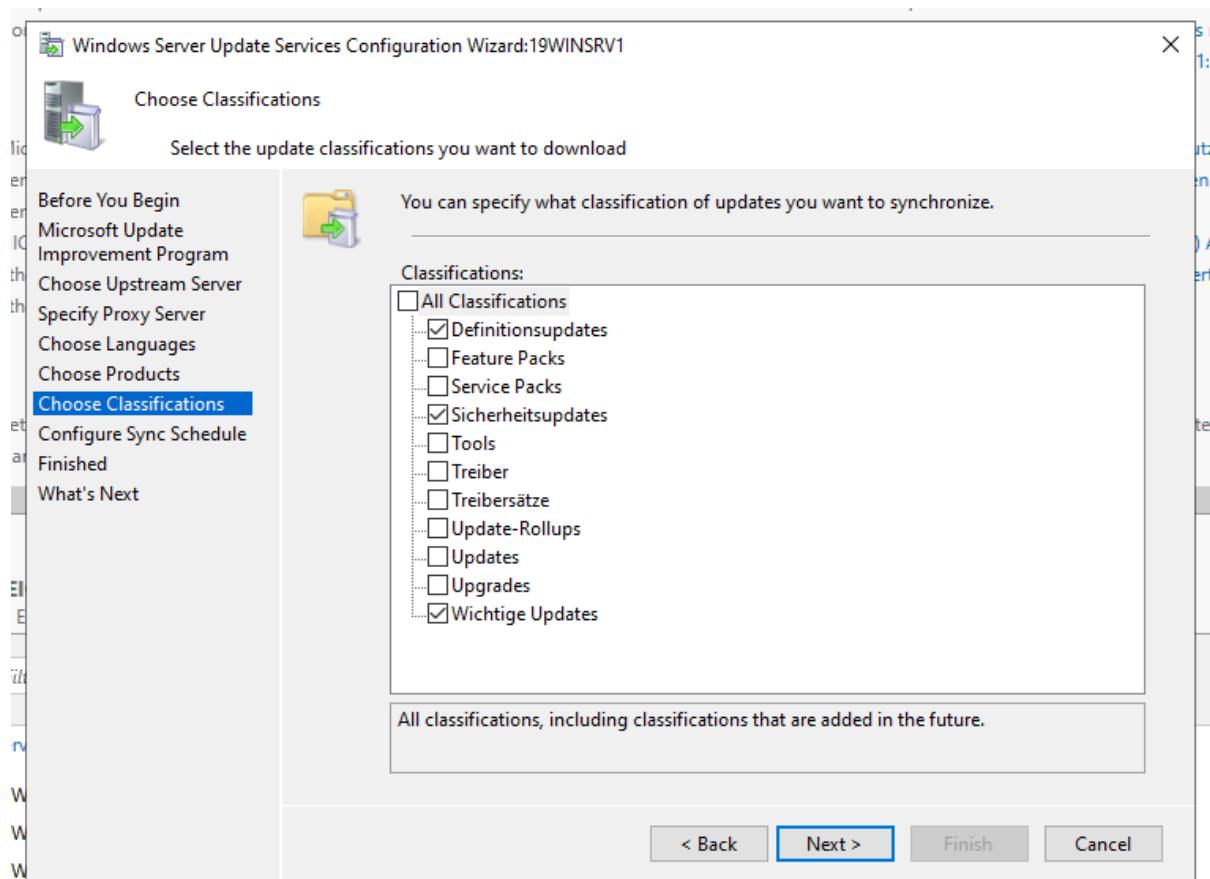
Beim Katalog nur Deutsch und Englisch auswählen und nur die Produkte, die wir brauchen.
Wenn nur Win11 Client, brauchen wir keine Updates für Win10 Client.



Paar auswählen:

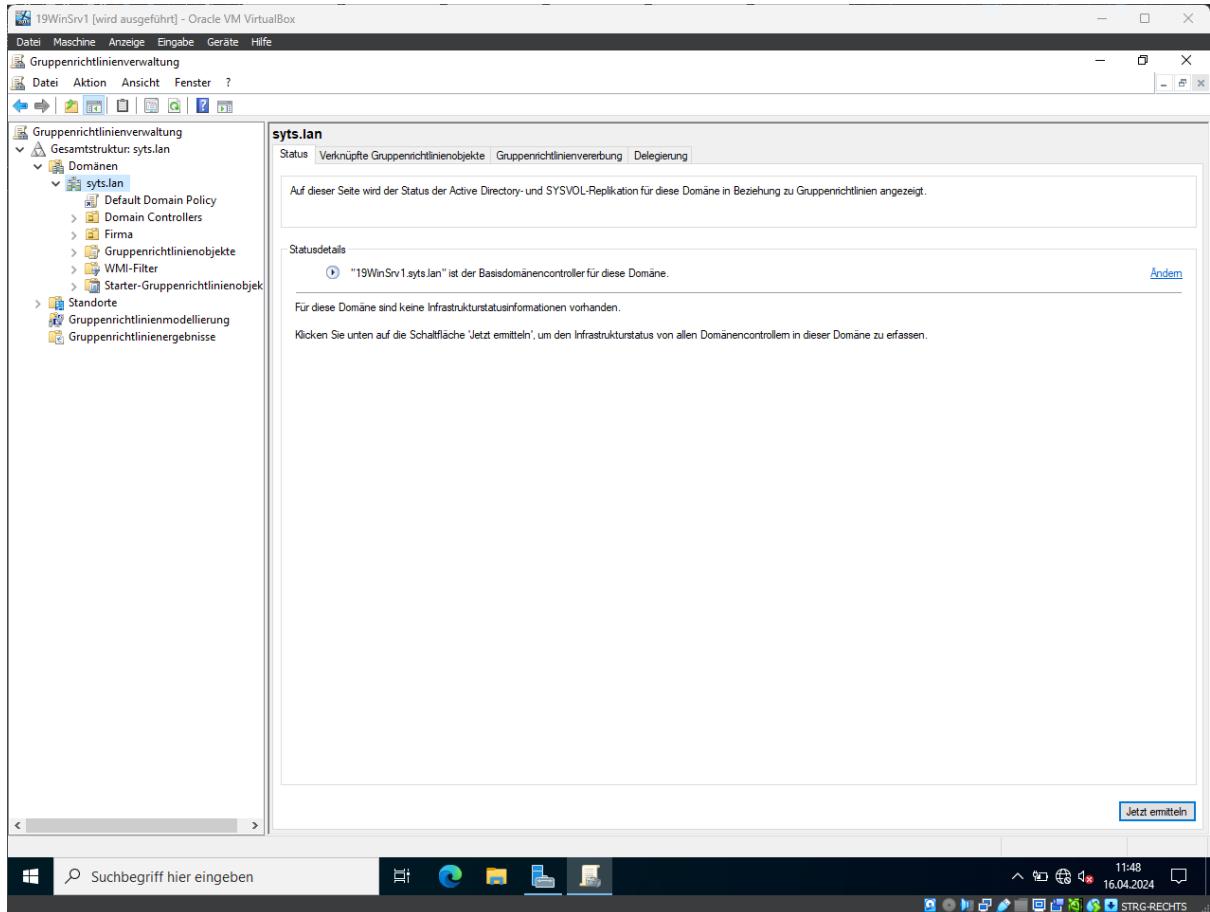


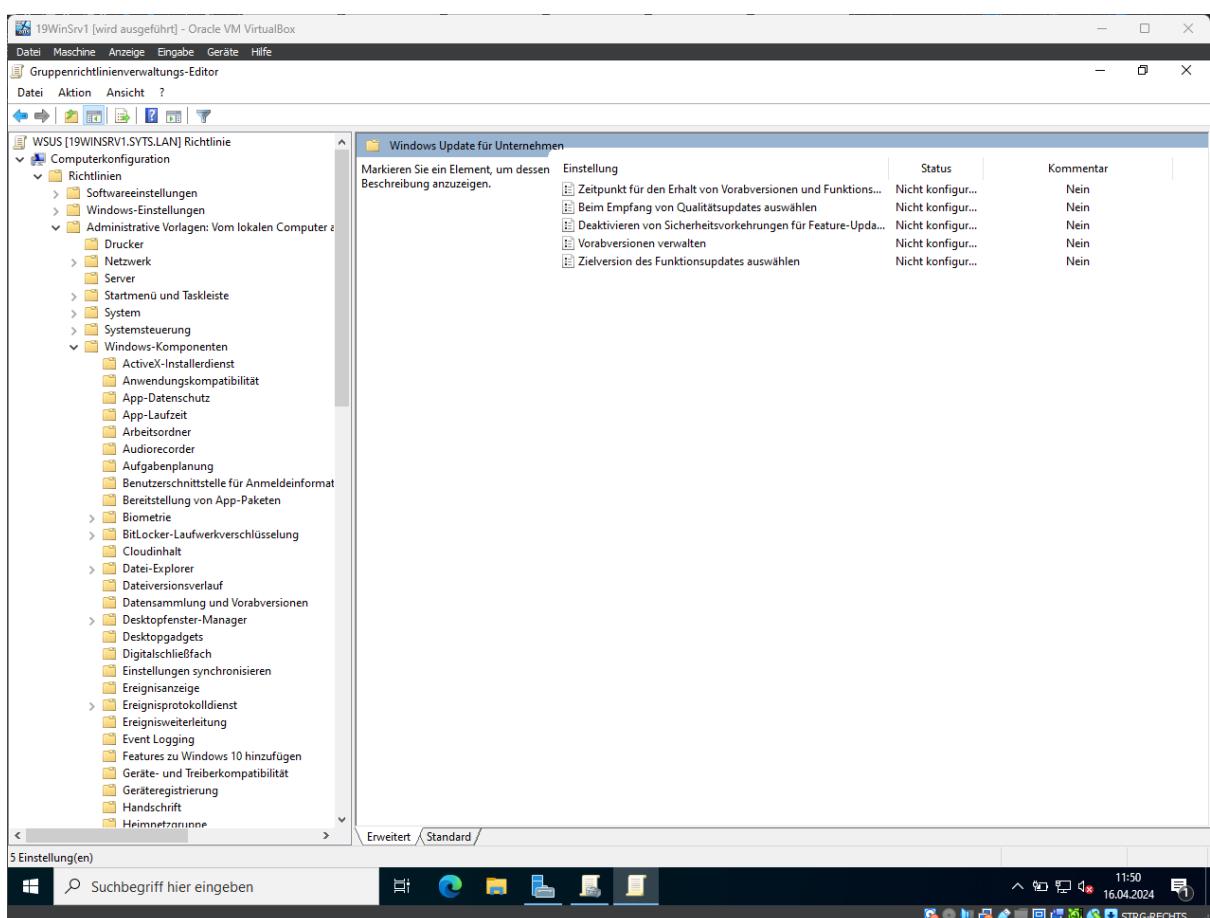
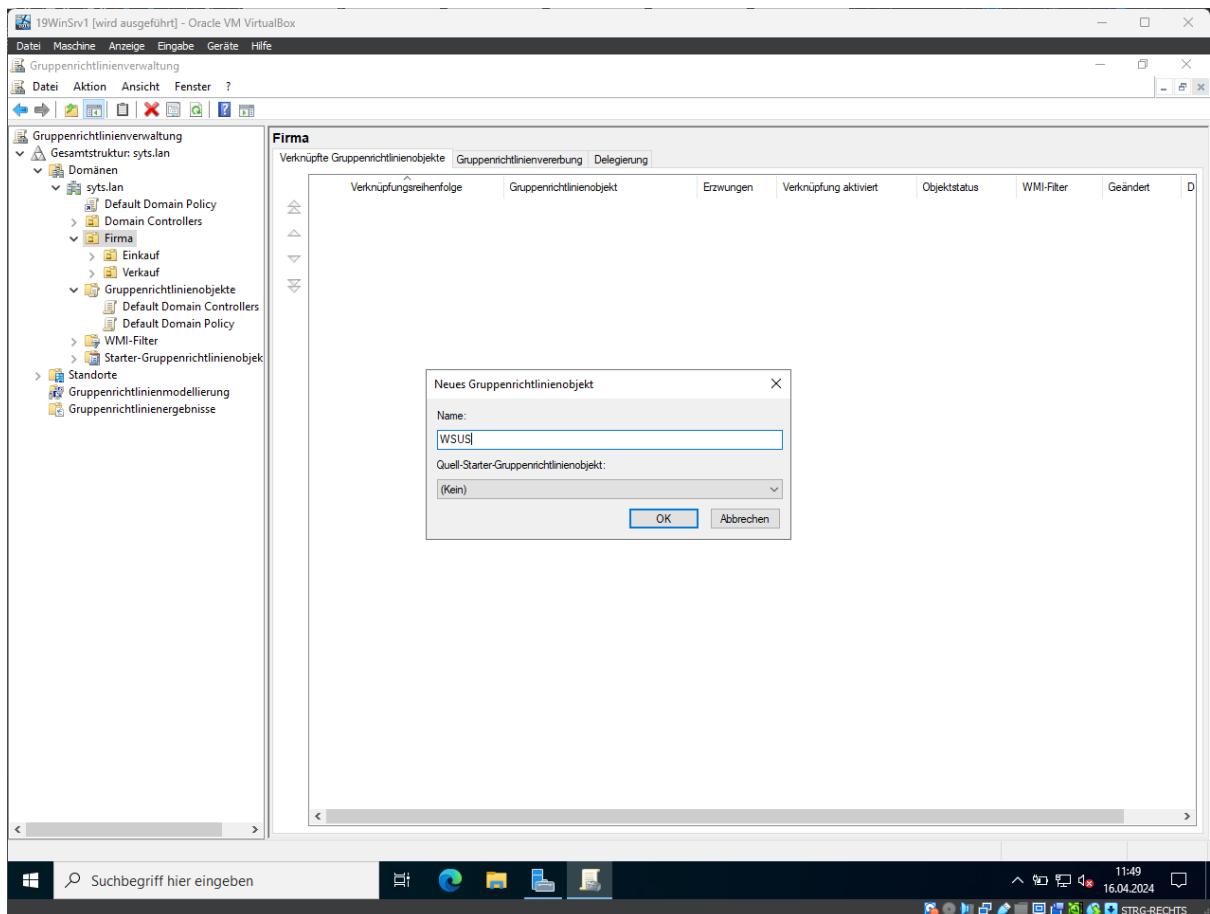
Nur wichtige Updates und so Sachen:



Für die Clients müssen wir nun Gruppenrichtlinien machen, damit sie wissen, dass es WSUS gibt.

Nach Gruppenrichtlinienverwaltung suchen in WIN.





Windows Update

Internen Pfad für den Microsoft Updatedienst angeben

Richtlinieneinstellung bearbeiten

Anforderungen:
Mindestens Windows XP Professional Service Pack 1 oder Windows 2000 Service Pack 3, Windows RT ausgenommen

Beschreibung:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. An optional server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet

Einstellung	Status	Kommentar
Windows Update für Unternehmen	Nicht konfigur...	Nein
Option "Updates installieren und herunterfahren" im Dialog...	Nicht konfigur...	Nein
Die Standardoption "Updates installieren und herunterfahre...	Nicht konfigur...	Nein
Windows Update-Energieverwaltung aktivieren, um das Syst...	Nicht konfigur...	Nein
Automatischen Neustart nach Updates während der Nutzen...	Nicht konfigur...	Nein
Nutzungzeitbereich für automatische Neustarts angeben	Nicht konfigur...	Nein
Automatisches Herunterladen von Updates über getaktete V...	Nicht konfigur...	Nein
Neustart immer automatisch zur geplanten Zeit durchführen	Nicht konfigur...	Nein
Frist angeben, nach der ein automatischer Neustart zur Upd...	Nicht konfigur...	Nein
Erinnerungsbenachrichtigungen über den automatischen N...	Nicht konfigur...	Nein
Benachrichtigungen für den automatischen Neustart zur Upd...	Nicht konfigur...	Nein
Erforderliche Benachrichtigung für automatischen Neustart ...	Nicht konfigur...	Nein
Automatischen Updates konfigurieren	Nicht konfigur...	Nein
Stichtage für automatische Updates und Neustarts angeben	Nicht konfigur...	Nein
Internen Pfad für den Microsoft Updatedienst angeben	Nicht konfigur...	Nein
Suchhäufigkeit für automatische Updates	Nicht konfigur...	Nein
Keine Richtlinien für Updaterückstellungen zulassen, durc...	Nicht konfigur...	Nein
Zugriff auf Feature "Updates aussetzen" entfernen	Nicht konfigur...	Nein
Zugriff auf alle Windows Update-Funktionen entfernen	Nicht konfigur...	Nein
Keine Verbindungen mit Windows Update-Internetadressen ...	Nicht konfigur...	Nein
Nichtadministratoren gestatten, Updatebenachrichtigungen...	Nicht konfigur...	Nein
Wechsel zum erzwungenen Neustart und Benachrichtigung...	Nicht konfigur...	Nein
Keine Treiber in Windows-Updates einschließen	Nicht konfigur...	Nein
Softwarebenachrichtigungen aktivieren	Nicht konfigur...	Nein
Automatische Updates sofort installieren	Nicht konfigur...	Nein
Empfohlene Updates über automatische Updates aktivieren	Nicht konfigur...	Nein
Keinen automatischen Neustart für geplante Installationen ...	Nicht konfigur...	Nein
Erneut zu einem Neustart für geplante Installationen aufford...	Nicht konfigur...	Nein
Neustart für geplante Installationen verzögern	Nicht konfigur...	Nein
Zeitplan für geplante Installationen neu erstellen	Nicht konfigur...	Nein
Warnbenachrichtigungszeitplan für den automatischen Neu...	Nicht konfigur...	Nein
Energieregelung für den Neustart nach einem Update, die fü...	Nicht konfigur...	Nein
Clientseitige Zielzuordnung aktivieren	Nicht konfigur...	Nein
Signierte Updates aus einem Intranetspeicherort für Microso...	Nicht konfigur...	Nein
Anzeigeeoptionen für Updatebenachrichtigungen	Nicht konfigur...	Nein

34 Einstellung(en)

Suchbegriff hier eingeben

11:50 16.04.2024 STRG-RECHTS

Windows Update

Internen Pfad für den Microsoft Updatedienst angeben

Richtlinieneinstellung bearbeiten

Aktiviert

Unterstützt auf: Mindestens Windows XP Professional Service Pack 1 oder Windows 2000 Service Pack 3, Windows RT ausgenommen

Optionen:

Interner Updatedienst zum Ermitteln von Updates:

Intranetserver für die Statistik: <http://19WinSrv1:8530>

Alternativen Downloadserver festlegen:

(Beispiel: https://IntranetUpd01)

Dateien ohne URL in den Metadaten herunterladen

Do not enforce TLS certificate pinning for Windows

Select the proxy behavior for Windows Update client to use a system proxy for the detection of updates.

Nur System-Proxy für die Erkennung von Aktualisierun...

Hilfe:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. An optional server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.

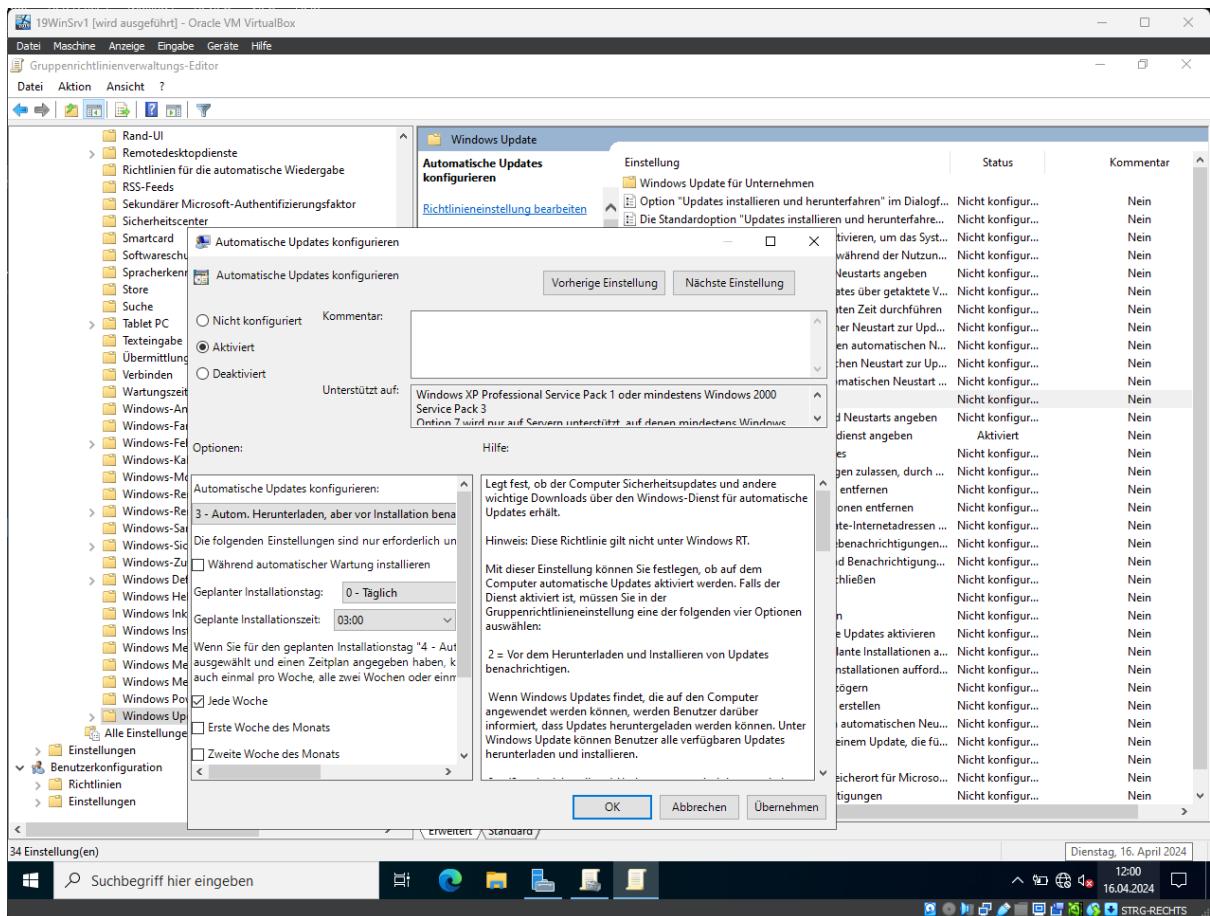
If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service (or alternate download server), instead of Windows Update, to

Einstellung	Status	Kommentar
Windows Update für Unternehmen	Nicht konfigur...	Nein
Option "Updates installieren und herunterfahren" im Dialog...	Nicht konfigur...	Nein
Die Standardoption "Updates installieren und herunterfahre...	Nicht konfigur...	Nein
Windows Update-Energieverwaltung aktivieren, um das Syst...	Nicht konfigur...	Nein
Automatischen Neustart nach Updates während der Nutzen...	Nicht konfigur...	Nein
Nutzungzeitbereich für automatische Neustarts angeben	Nicht konfigur...	Nein
Automatisches Herunterladen von Updates über getaktete V...	Nicht konfigur...	Nein
Neustart immer automatisch zur geplanten Zeit durchführen	Nicht konfigur...	Nein
Frist angeben, nach der ein automatischer Neustart zur Upd...	Nicht konfigur...	Nein
Erinnerungsbenachrichtigungen über den automatischen N...	Nicht konfigur...	Nein
Benachrichtigungen für den automatischen Neustart zur Upd...	Nicht konfigur...	Nein
Erforderliche Benachrichtigung für automatischen Neustart ...	Nicht konfigur...	Nein
Automatischen Updates konfigurieren	Nicht konfigur...	Nein
Stichtage für automatische Updates und Neustarts angeben	Nicht konfigur...	Nein
Internen Pfad für den Microsoft Updatedienst angeben	Nicht konfigur...	Nein
Suchhäufigkeit für automatische Updates	Nicht konfigur...	Nein
Keine Richtlinien für Updaterückstellungen zulassen, durc...	Nicht konfigur...	Nein
Zugriff auf Feature "Updates aussetzen" entfernen	Nicht konfigur...	Nein
Zugriff auf alle Windows Update-Funktionen entfernen	Nicht konfigur...	Nein
Keine Verbindungen mit Windows Update-Internetadressen ...	Nicht konfigur...	Nein
Nichtadministratoren gestatten, Updatebenachrichtigungen...	Nicht konfigur...	Nein
Wechsel zum erzwungenen Neustart und Benachrichtigung...	Nicht konfigur...	Nein
Keine Treiber in Windows-Updates einschließen	Nicht konfigur...	Nein
Softwarebenachrichtigungen aktivieren	Nicht konfigur...	Nein
Automatische Updates sofort installieren	Nicht konfigur...	Nein
Empfohlene Updates über automatische Updates aktivieren	Nicht konfigur...	Nein
Keinen automatischen Neustart für geplante Installationen ...	Nicht konfigur...	Nein
Erneut zu einem Neustart für geplante Installationen aufford...	Nicht konfigur...	Nein
Neustart für geplante Installationen verzögern	Nicht konfigur...	Nein
Zeitplan für geplante Installationen neu erstellen	Nicht konfigur...	Nein
Warnbenachrichtigungszeitplan für den automatischen Neu...	Nicht konfigur...	Nein
Energieregelung für den Neustart nach einem Update, die fü...	Nicht konfigur...	Nein
Clientseitige Zielzuordnung aktivieren	Nicht konfigur...	Nein
Signierte Updates aus einem Intranetspeicherort für Microso...	Nicht konfigur...	Nein
Anzeigeeoptionen für Updatebenachrichtigungen	Nicht konfigur...	Nein

34 Einstellung(en)

Suchbegriff hier eingeben

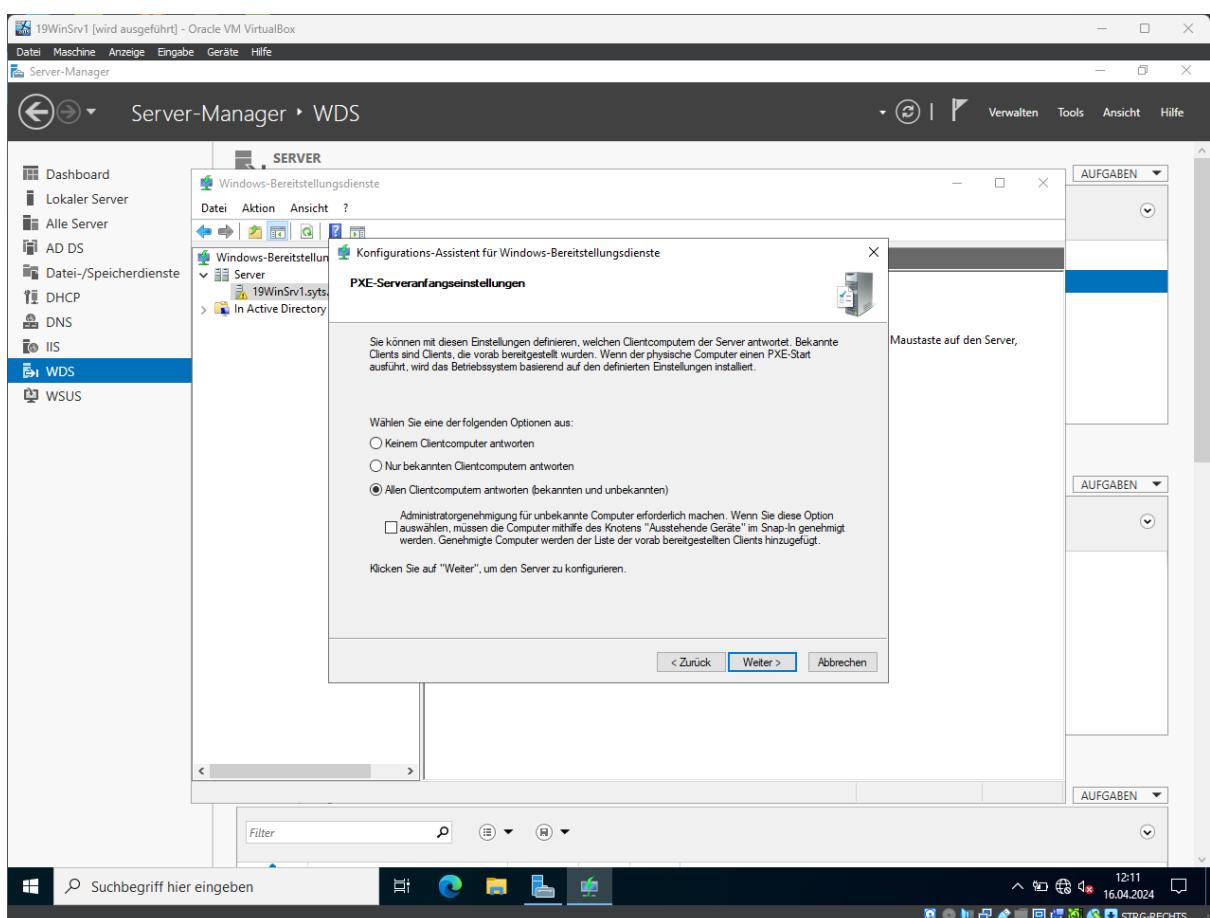
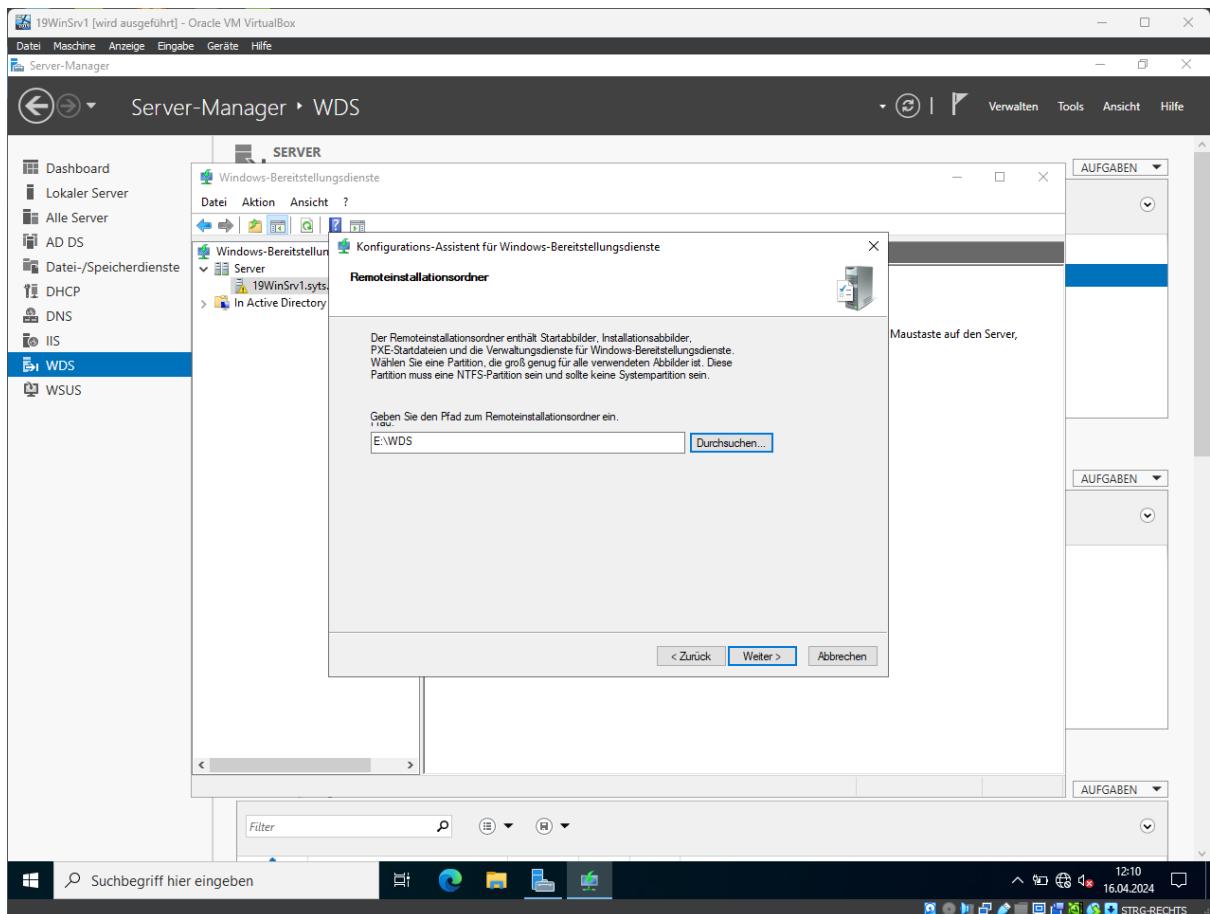
11:53 16.04.2024 STRG-RECHTS

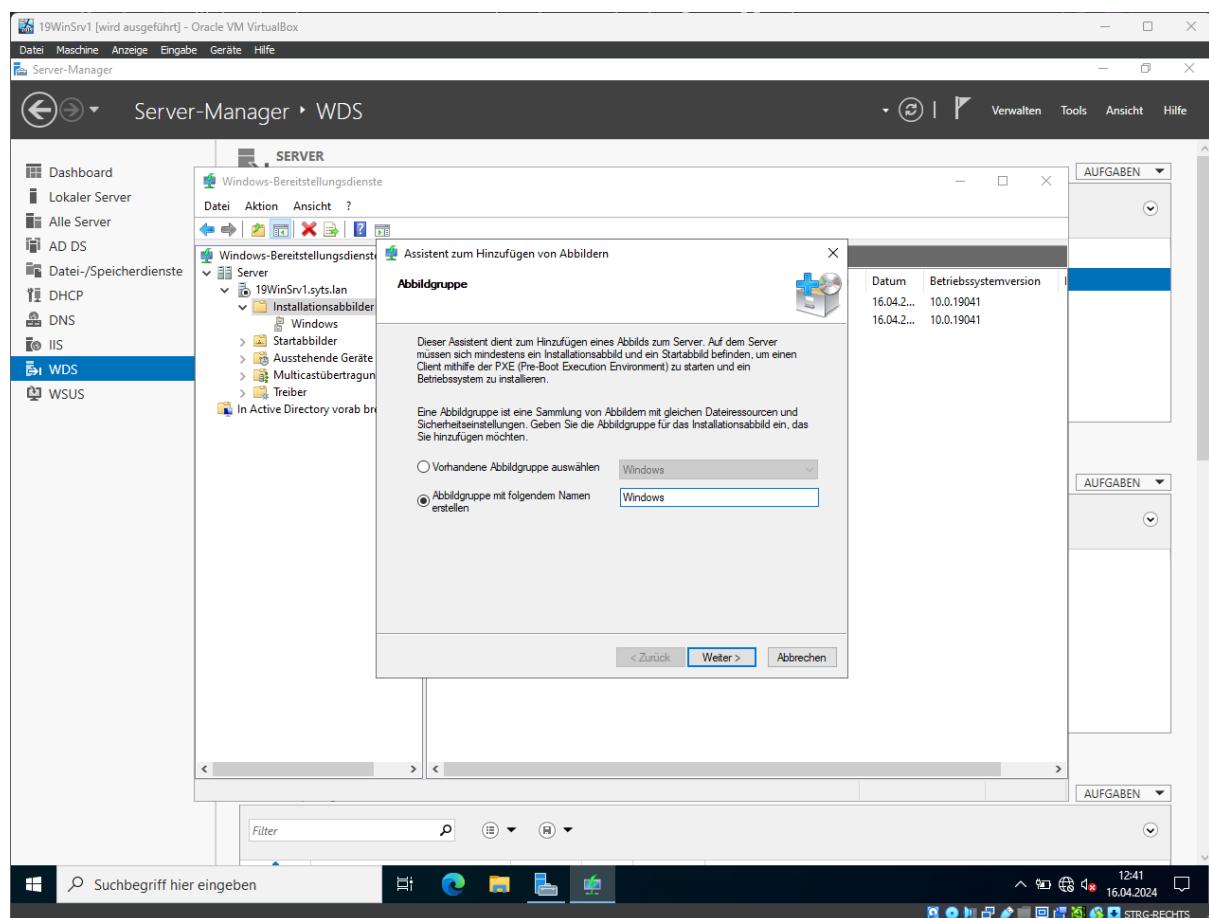
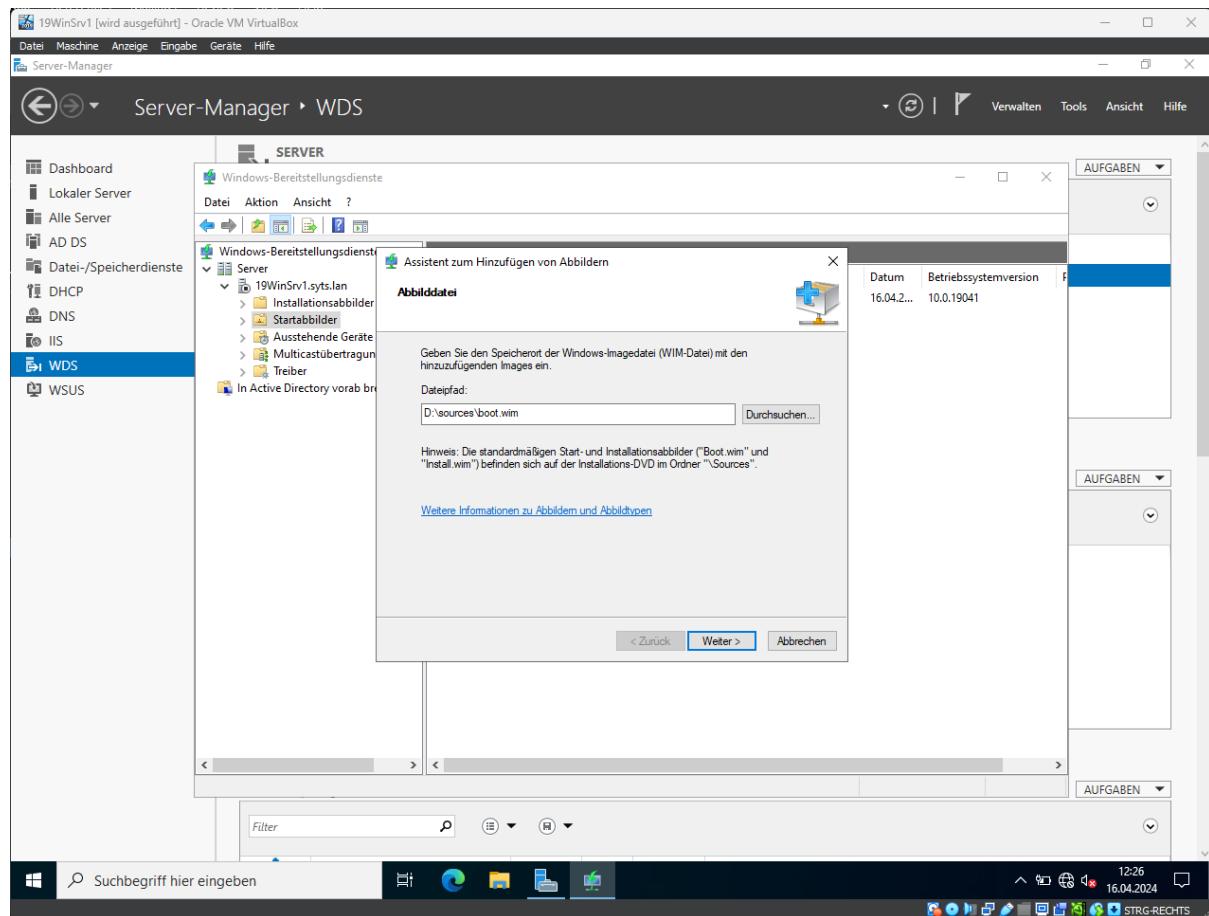


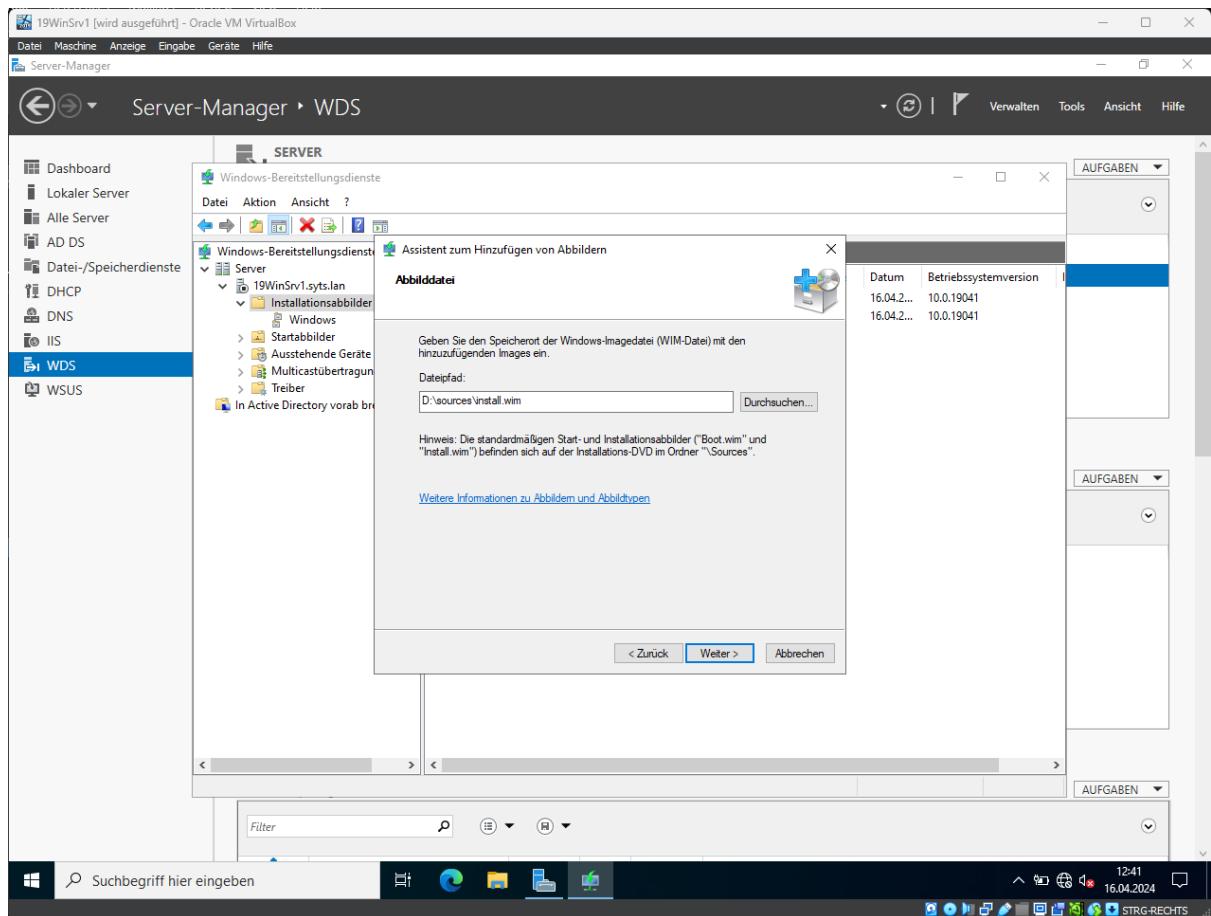
WDS

Folder am Volume E erstellen (WDS)

Rolle WDS installieren (default Features lassen)







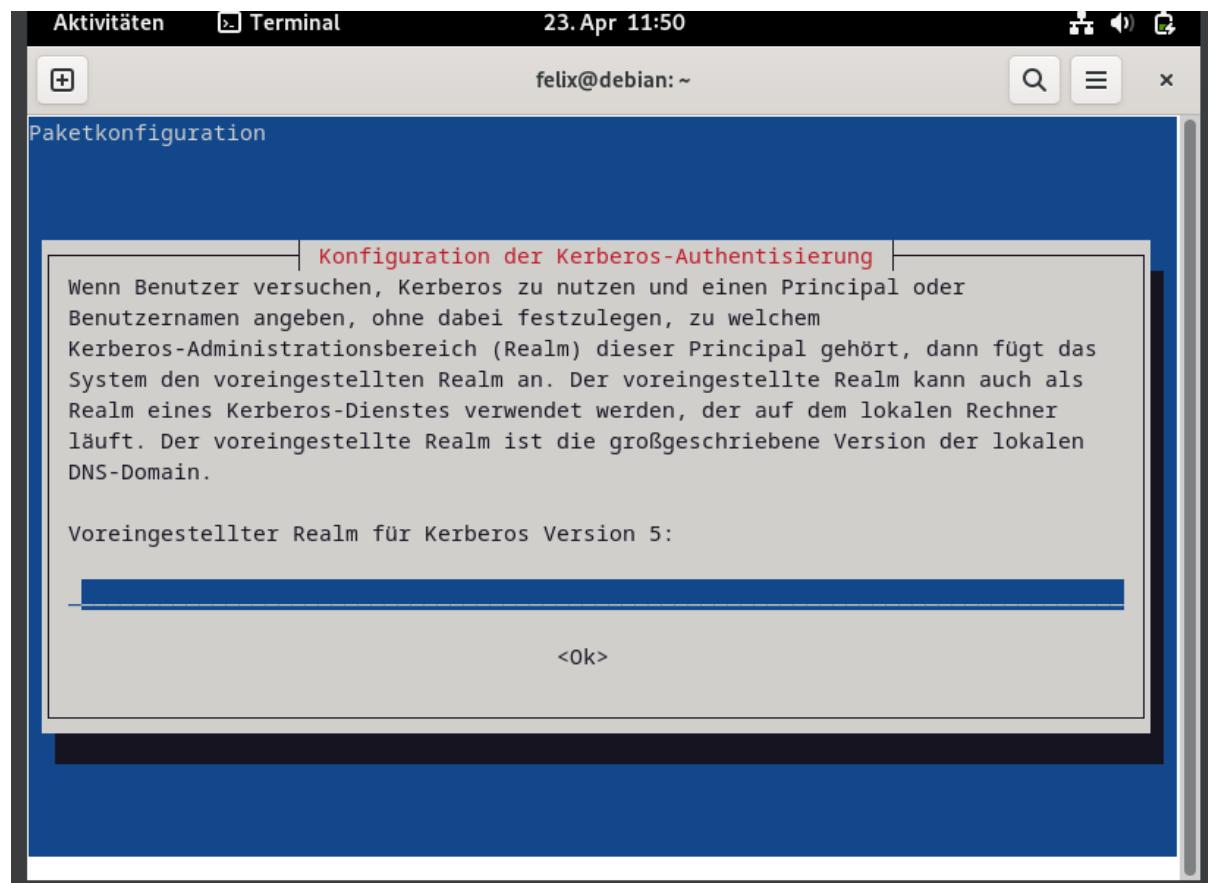
Ubuntu Client

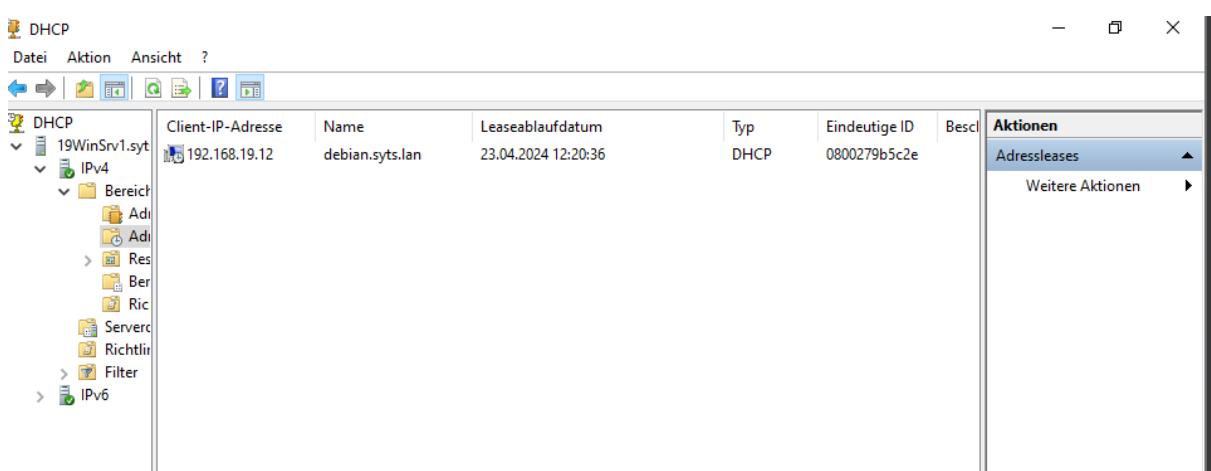
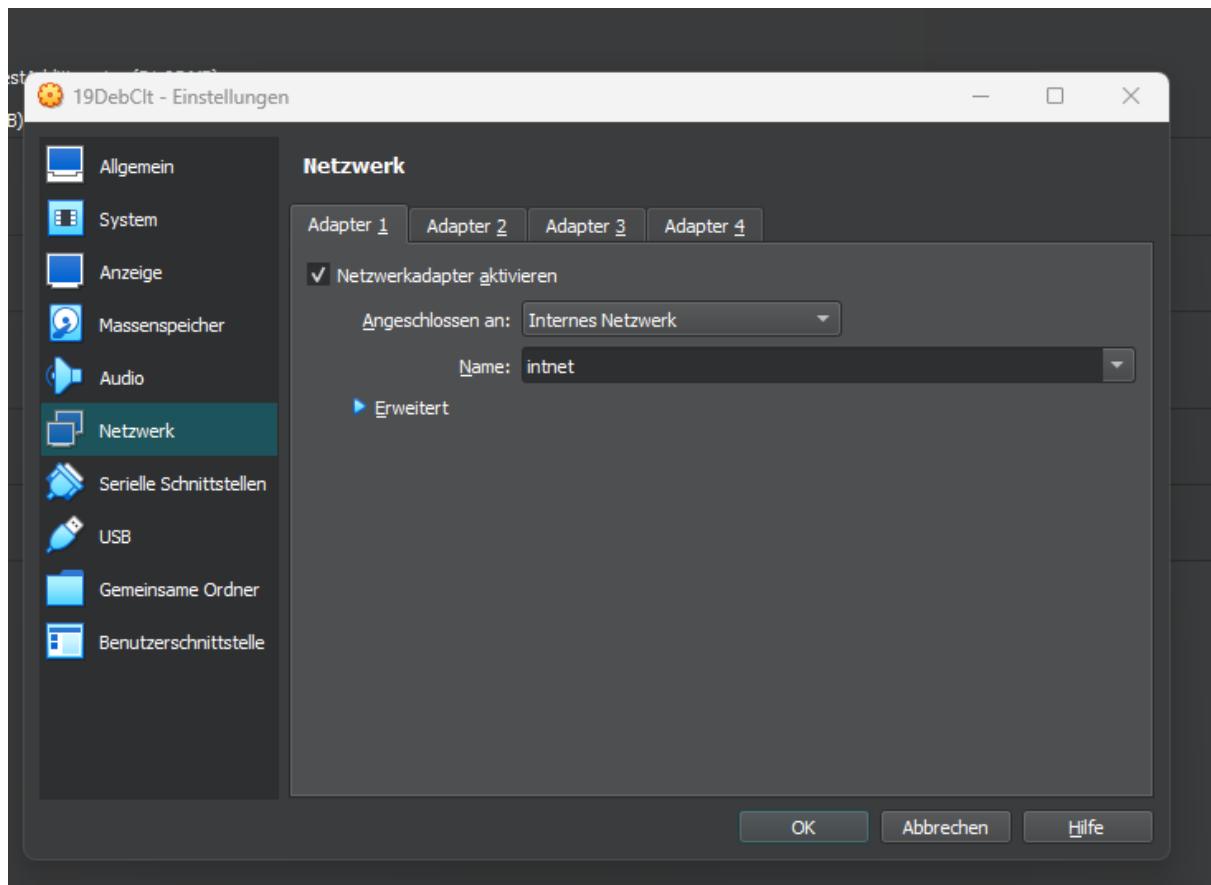
In Windows Domain hinzufügen

Client und KRB5 + alle Pakete bereits installiert. Nur krb5.conf anpassen, dann sollte gehen:

```
media/ mnt/
felix@debian:~$ sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss krb5-user
adcli samba-common-bin
[sudo] Passwort für felix:
```

Da die Pakete bereits installiert wurde, ist die Kerberos Konfig bereit gelassen worden:

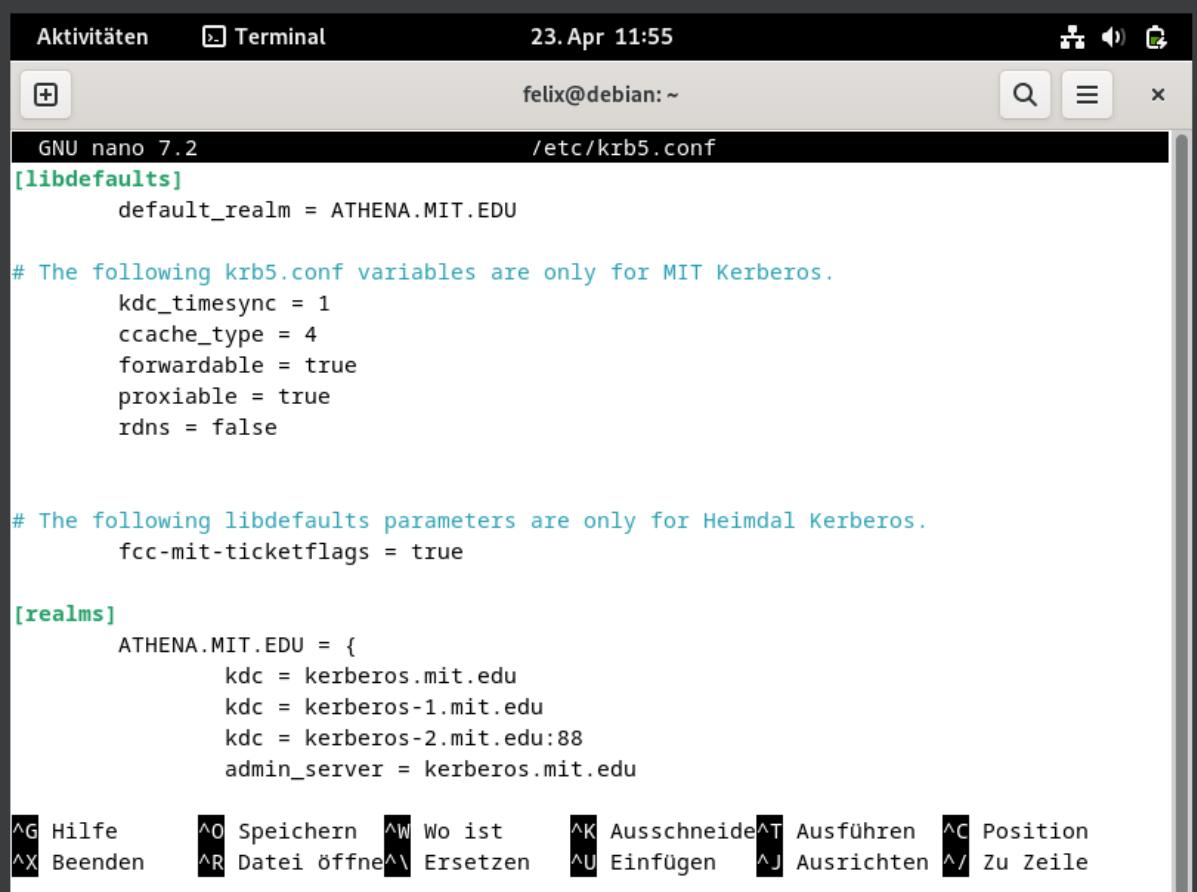




```

rtt min/avg/max/mdev = 0.887/1.167/1.447/0.280 ms
felix@debian:~$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9b:5c:2e brd ff:ff:ff:ff:ff:ff
    inet 192.168.19.12/24 brd 192.168.19.255 scope global dynamic noprefixroute enp0s3
        valid_lft 1689sec preferred_lft 1689sec
    inet6 fe80::a00:27ff:fe9b:5c2e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
felix@debian:~$ █
```

Default konfig:



The screenshot shows a terminal window titled "Terminal" with the command "felix@debian: ~". The window displays the contents of the file "/etc/krb5.conf" using the "GNU nano 7.2" editor. The configuration file includes sections for [libdefaults] and [realms].

```

Aktivitäten Terminal 23. Apr 11:55
felix@debian: ~
GNU nano 7.2 /etc/krb5.conf

[libdefaults]
default_realm = ATHENA/MIT.EDU

# The following krb5.conf variables are only for MIT Kerberos.
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
rdns = false

# The following libdefaults parameters are only for Heimdal Kerberos.
fcc-mit-ticketflags = true

[realms]
ATHENA/MIT.EDU = {
    kdc = kerberos.mit.edu
    kdc = kerberos-1.mit.edu
    kdc = kerberos-2.mit.edu:88
    admin_server = kerberos.mit.edu

^G Hilfe ^O Speichern ^W Wo ist ^K Ausschneide^T Ausführen ^C Position
^X Beenden ^R Datei öffne^V Ersetzen ^U Einfügen ^J Ausrichten ^/ Zu Zeile
```

Aktivitäten Terminal 23. Apr 11:59

```
GNU nano 7.2 /etc/krb5.conf

[libdefaults]
    default_realm = SYTS.LAN

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    rdns = false

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    SYTS.LAN = {
        kdc = 99WinSrv1.syts.lan
        admin_server = 99WinSrv1.syts.lan
        default_domain = syts.lan
    }

[ 82 Zeilen gelesen ]
^G Hilfe ^O Speichern ^W Wo ist ^K Ausschneide^T Ausführen ^C Position
^X Beenden ^R Datei öffne^V Ersetzen ^U Einfügen ^J Ausrichten ^/ Zu Zeile
```

Aktivitäten Terminal 23. Apr 12:00

```
GNU nano 7.2 /etc/krb5.conf

    kdc = kerberos3.utoronto.ca
    admin_server = kerberos1.utoronto.ca
    default_domain = utoronto.ca
}

[domain_realm]
    .syts.lan = SYTS.LAN
    syts.lan = SYTS.LAN
    .media.mit.edu = MEDIA-LAB.MIT.EDU
    media.mit.edu = MEDIA-LAB.MIT.EDU
    .csail.mit.edu = CSAIL.MIT.EDU
    csail.mit.edu = CSAIL.MIT.EDU
    .whoi.edu = ATHENA.MIT.EDU
    whoi.edu = ATHENA.MIT.EDU
    .stanford.edu = stanford.edu
    .slac.stanford.edu = SLAC.STANFORD.EDU
    .toronto.edu = UTORONTO.CA
    .utoronto.ca = UTORONTO.CA

[ 82 Zeilen gelesen ]
^G Hilfe ^O Speichern ^W Wo ist ^K Ausschneide^T Ausführen ^C Position
^X Beenden ^R Datei öffne^V Ersetzen ^U Einfügen ^J Ausrichten ^/ Zu Zeile
```

Reboot

```
root@debian:~# kinit Administrator@SYTS.LAN
Passwort für Administrator@SYTS.LAN:
root@debian:~#
```

```
root@debian:~# klist
Ticketzwischenspeicher: FILE:/tmp/krb5cc_0
Standard-Principal: Administrator@SYTS.LAN

Valid starting      Expires              Service principal
2024-04-23 12:07:04  2024-04-23 22:07:04  krbtgt/SYTS.LAN@SYTS.LAN
    erneuern bis 2024-04-24 12:07:00
root@debian:~#
```

```
root@debian:~# realm discover -v SYTS.LAN
* Resolving: _ldap._tcp.syts.lan
* Performing LDAP DSE lookup on: 10.0.2.15
* Performing LDAP DSE lookup on: 192.168.19.1
* Successfully discovered: syts.lan
syts.lan
  type: kerberos
  realm-name: SYTS.LAN
  domain-name: syts.lan
  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@debian:~#
```

```
root@debian:~# realm join -v SYTS.LAN -U Administrator@SYTS.LAN
* Resolving: _ldap._tcp.syts.lan
* Performing LDAP DSE lookup on: 10.0.2.15
* Performing LDAP DSE lookup on: 192.168.19.1
* Successfully discovered: syts.lan
Passwort für Administrator@SYTS.LAN:
* Unconditionally checking packages
* Resolving required packages

* LANG=C /usr/sbin/adcli join --verbose --domain syts.lan --domain-realm SYTS.LAN --do
main-controller 192.168.19.1 --login-type user --login-user Administrator@SYTS.LAN --st
din-password
* Using domain name: syts.lan
* Calculated computer account name from fqdn: DEBIAN
* Using domain realm: syts.lan
* Sending NetLogon ping to domain controller: 192.168.19.1
* Received NetLogon info from: 19Win$rv1.syts.lan
```

Client ist in Domain:

Name	Type	Description
19WIN10CLT2	Computer	
19WIN11CLT1	Computer	
DEBIAN	Computer	

EZ

Was wahrscheinlich kommen wird...

- 2 Windows Server aufsetzen mit AD, DHCP & DNS; alles repliziert (Beweise, dass Replikation)
- WDS oder WSUS
- 1 Windows Client in die Domain
- 1 Linux Client in die Domain