Windows Server-Client-Active Directory - 12.11.2024

Diese Dokumentation zeigt eine Mitschrift als Dokumentation eines im Anhang befindlichen Laborauftrages im Unterrichtsfach **Betriebssysteme & Labor**.

Inhalt

1. Geräteübersicht

	Geräte	VM	Betriebssystem	IP-Adresse (LAN)
1	LENOVO E15	nein	WIN11_pro	192.168.1.124
2	---„---	ja	VM_Windows Server 2025	192.168.1.125
3	---„---	ja	VM_WIN11_pro	192.168.100.2

1.1 Benutzereinstellungen (Software)

	Anwendung	Benutzername	Passwort	Gerätename	domain (AD)
User-PC	WIN11_pro	admin_lugstein	Aa_123456	*srvlumex*	*local*
	WIN11_pro	Markus	Aa_123456		*domain*
	WIN11_pro	Franz	Aa_123456		*domain*

	Anwendung	Benutzername	Passwort	Gerätename
Server	WIN-Server2025	Administrator	Aa_123456	srvlumex
	Verzeichnisdienst-Wiederherstellungsmodus	Administrator	Aa_123456	

1.2 Geräteeinstellungen (Hardware)

	Netzwerkadapter #1 (Intranet)
User-PC	internes Netzwerk
IP	per DHCP von Server
SUB	255.255.255.0
DNS	127.0.0.1

Achtung!

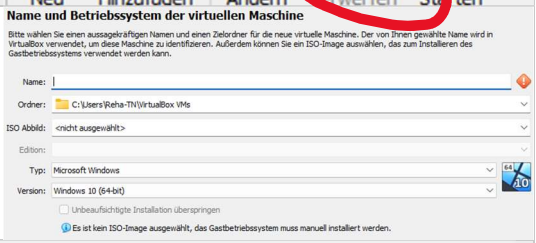
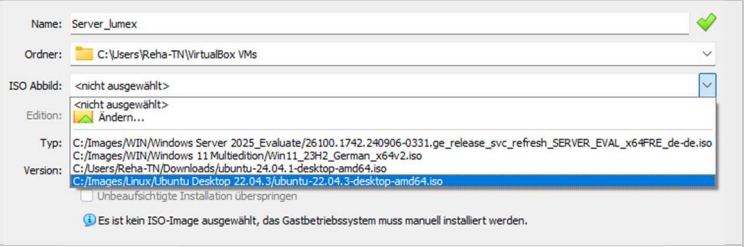
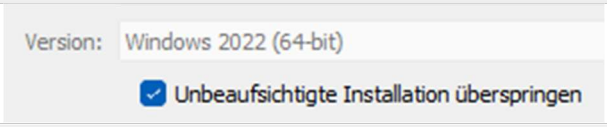
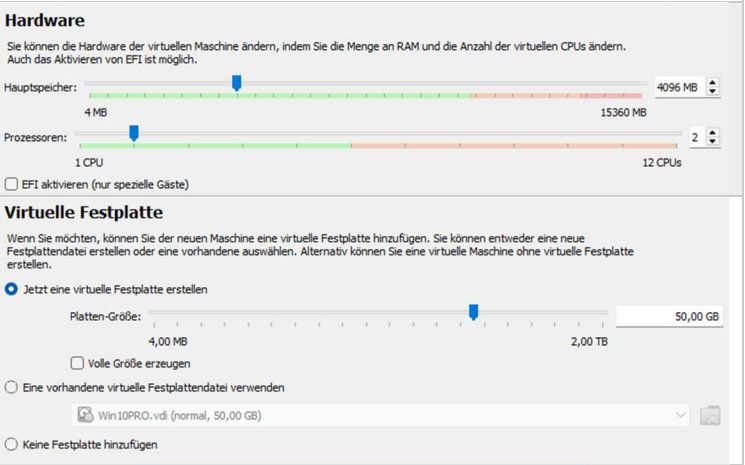
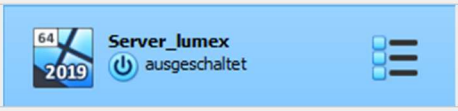
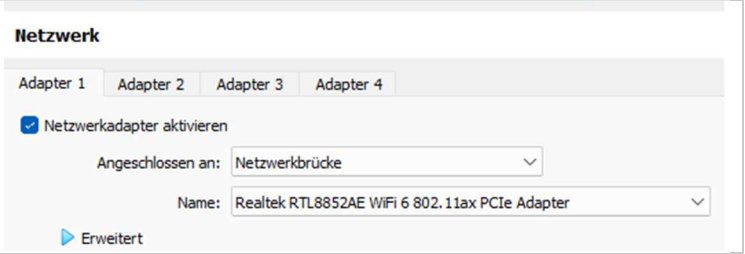
Server muss über 2. Netzwerkadapter verfügen!!!

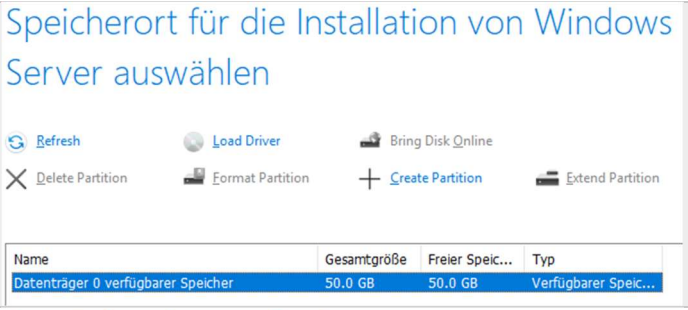
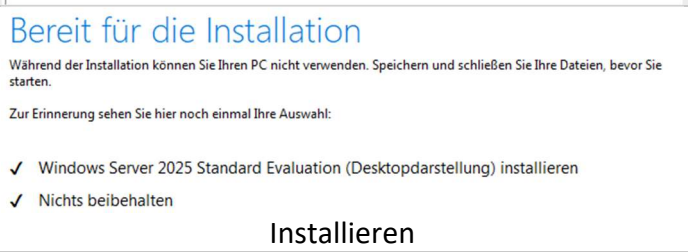
	Netzwerkadapter #1 (Internet)	Netzwerkadapter #2 (Intranet)
Server	Verbindungsart	Netzwerkbrücke	internes Netzwerk
	IP	192.168.1.125 (DHCP)	192.168.100.1 (fixe IP)
	SUB	255.255.255.0	255.255.255.0
	Gateway	192.168.1.1	
	DNS	192.168.1.1	
	DNS	8.8.8.8 bevorzugt	127.0.0.1

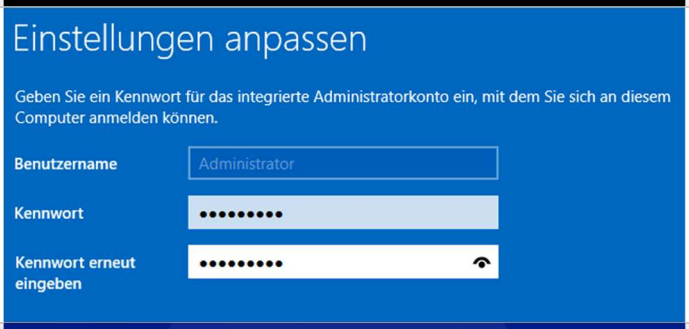
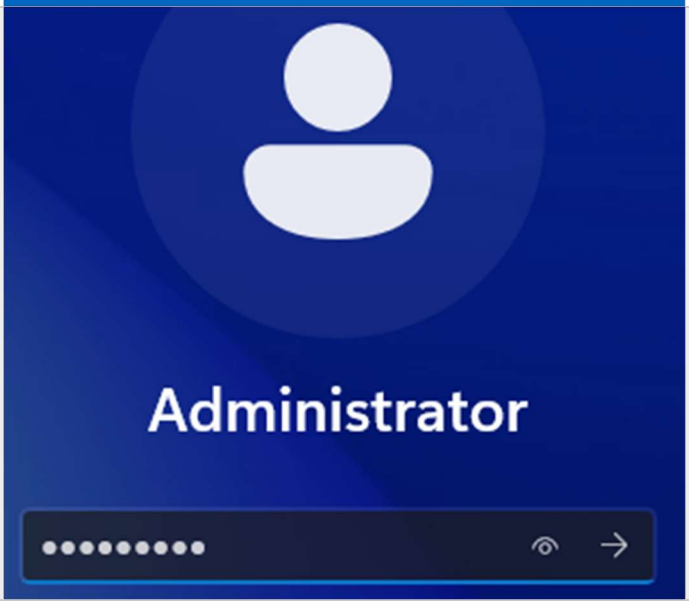
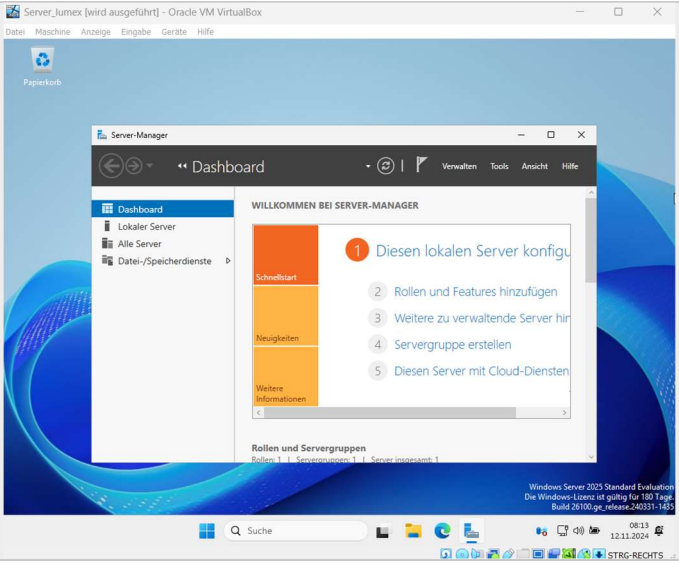
2. Arbeitsziel

Ziel:
Erstellung und Nutzung einer Active Directory-Infrastruktur

3. Installation VM-Windows-Server 2025

Neu-Erstellung der virtuellen-Maschine „Windows-Server 2025“	
Namens-Vergabe: **Server_lumex**	
Auswahl der .iso-Datei	
Haken bei „unbeaufsichtigte Installation“ setzen	
Vergabe von Resourcen	
Die VM wurde erstellt und kann gestartet werden!	
WICHTIG! **Aktivierung und Einstellung von zwei Netzwerkadaptern** **➔ Siehe Tabelle unter Pkt. 1.2**	
Nun kann die VM gestartet werden	

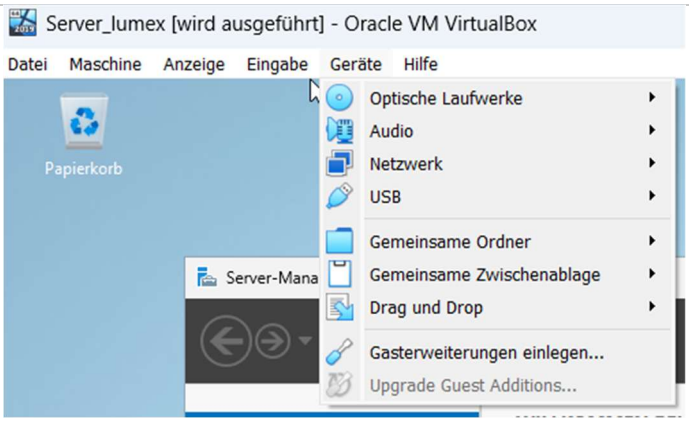
Spracheinstellungen auswählen	2x Deutsch
Tastatureinstellungen auswählen	Deutsch
Setupoptionen auswählen	 Windows Server installieren, Haken setzen
Auswahl des zu installierenden OS	
Lizenzbedienungen	Akzeptieren
Speicherort für die Installation auswählen	
Installation bestätigen	 Installieren
Installation läuft ….	
WICHTIG! Um die Installation fortzusetzen unbedingt die LEERTASTE drücken!!	Drücken Sie eine Taste um von der CD zu starten

Die Installation wird fortgesetzt!	
Benutzer: Administrator **Kennwort** **Aa_123456**	
Erstanmeldung	
Diagnosedaten an Microsoft senden	Nur erforderlich
Erststart des „Server-Managers“	

Gasterweiterung einlegen!!

VBoxWindowsAdditions-amd64

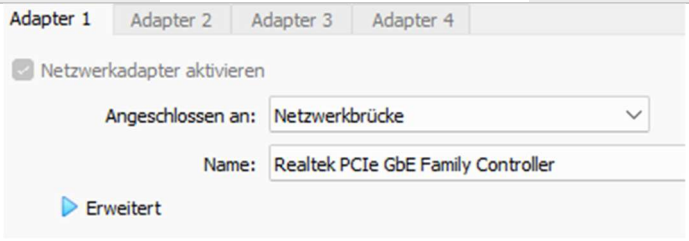
→ als Admin ausführen, installieren und System neu starten!



Nach updates suchen und installieren!

Windows Update

1 Netzwerkadapter



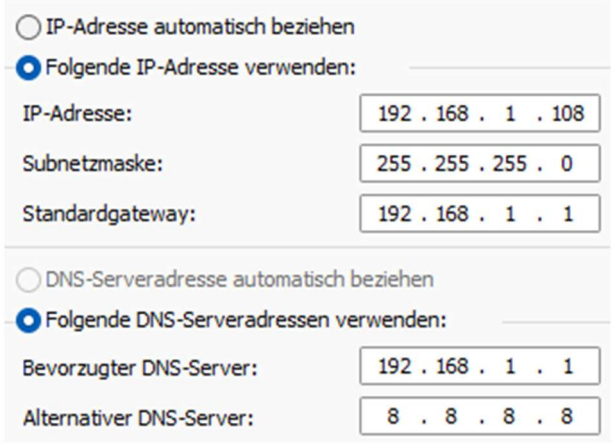
WICHTIG: Auswahl des richtigen Netzwerkadapters

cmd auf VM:

```
Ethernet-Adapter Internet:

   Verbindungsspezifisches DNS-Suffix:
   Verbindungslokale IPv6-Adresse  . : fe80::f98f:1f33:7976:d649%15
   IPv4-Adresse  . . . . . . . . . . : 192.168.1.108
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.1.1

C:\Users\Administrator>
```

Einstellungen an der VM

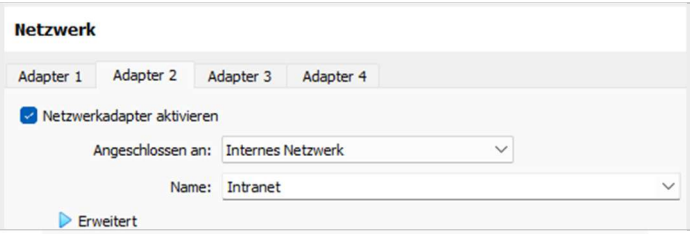
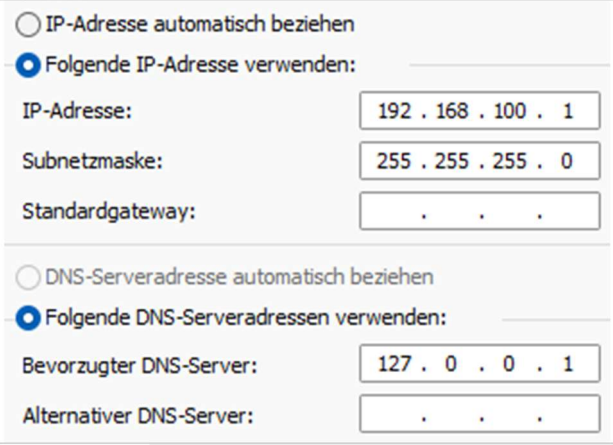
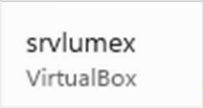
Vergabe einer festen IP



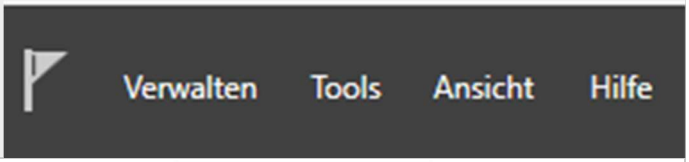
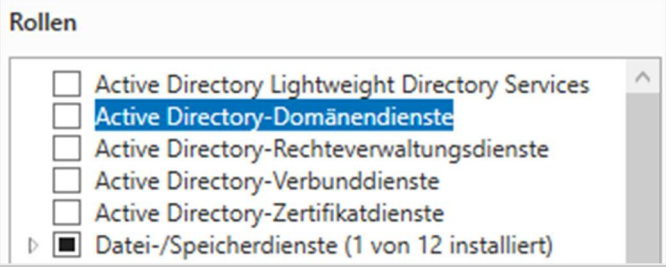
cmd Host-PC

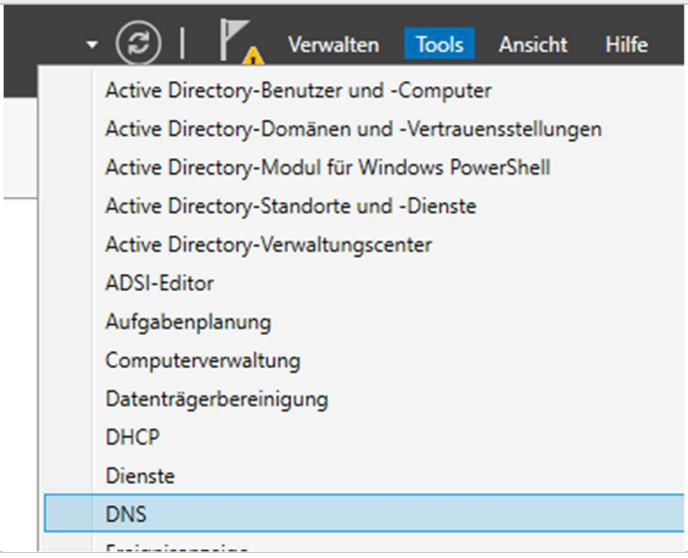
```
Ethernet-Adapter Ethernet 3:

   Verbindungsspezifisches DNS-Suffix:
   Verbindungslokale IPv6-Adresse  . : fe80::14d9:d2ff:8617:8b3f%21
   IPv4-Adresse  . . . . . . . . . . : 192.168.1.24
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.1.1
```

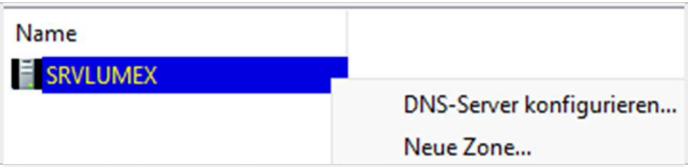
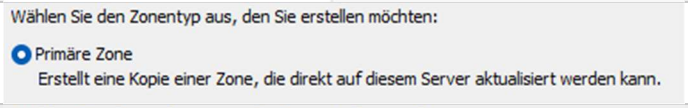
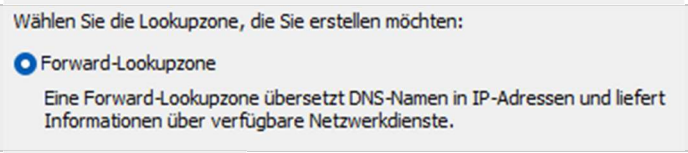
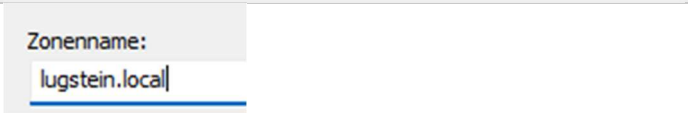
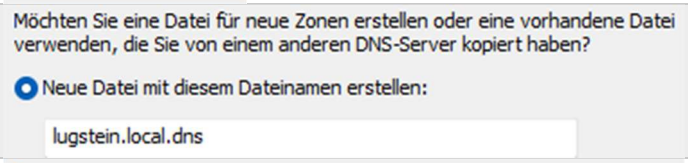
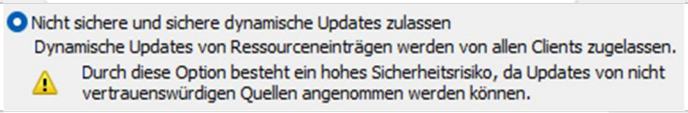
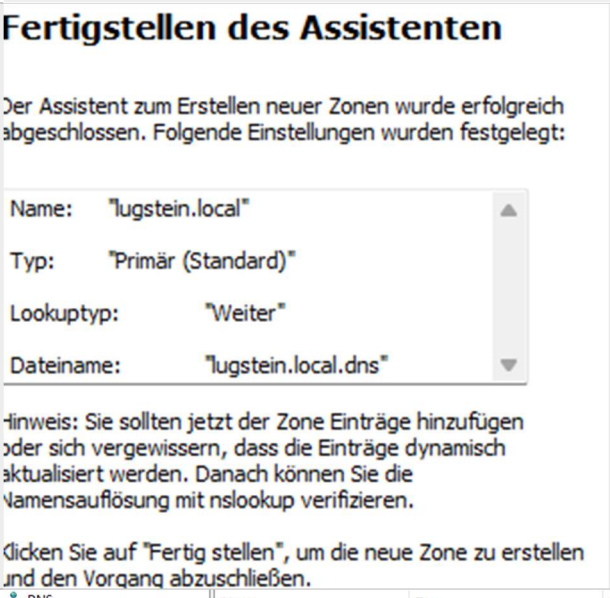
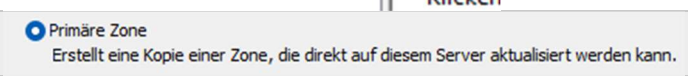
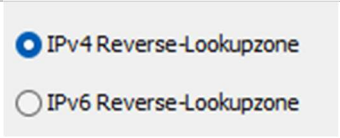
Netzwerkfreigaben aktivieren!!!

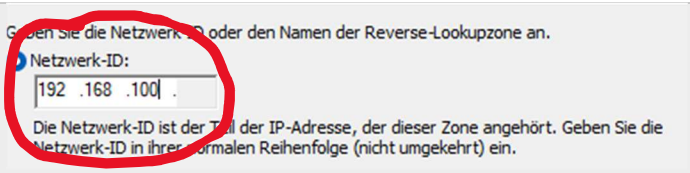
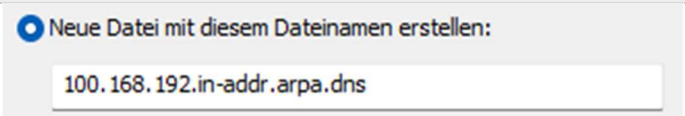
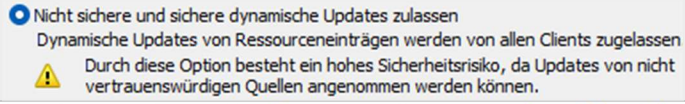
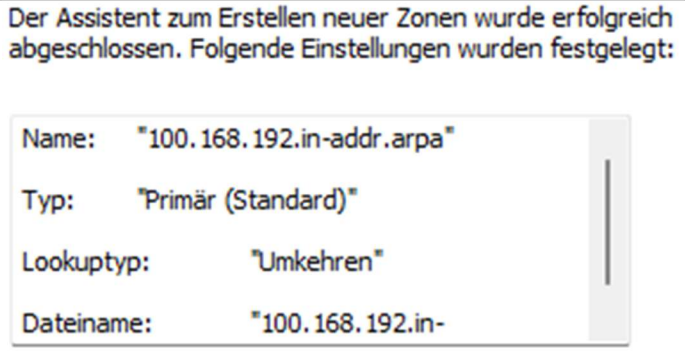
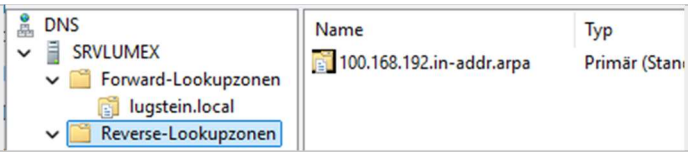
2 Netzwerkadapter	
Einstellungen Netzwerkadapter 2	
PC umbenennen System→ Info	 Diesen PC umbenennen und NEUSTART durchführen
Sicherungspunkt von VM erstellen	
ping zwischen Host und VM durchführen	

3.1 Serverdienste installieren auf VM-Server WIN2025

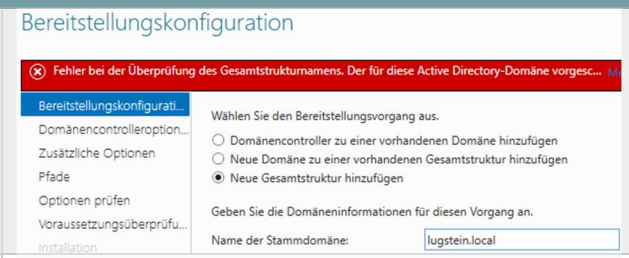
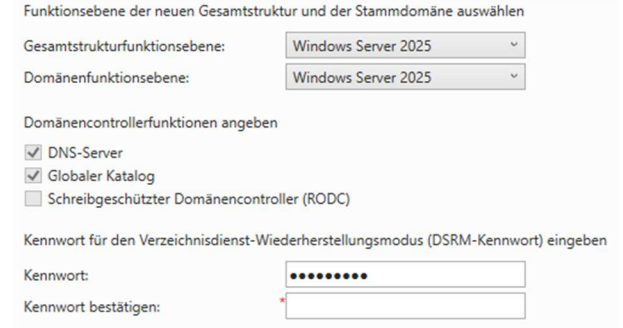
Verwalten **Rollen und Features hinzufügen**	
Serverauswahl **srvlumex auswählen und weiter**	
unter Rollen → Active Directory-Domänendienst auswählen und Features hinzufügen	

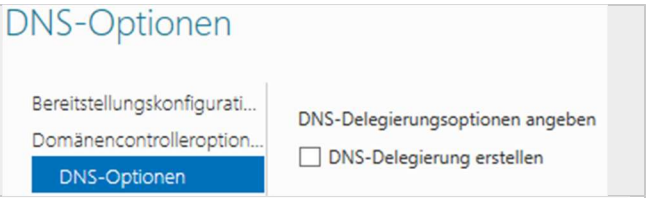
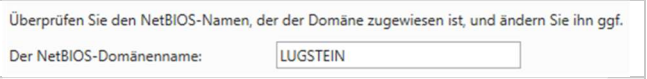
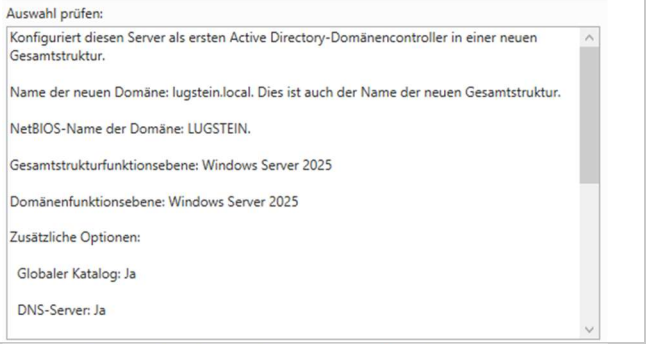
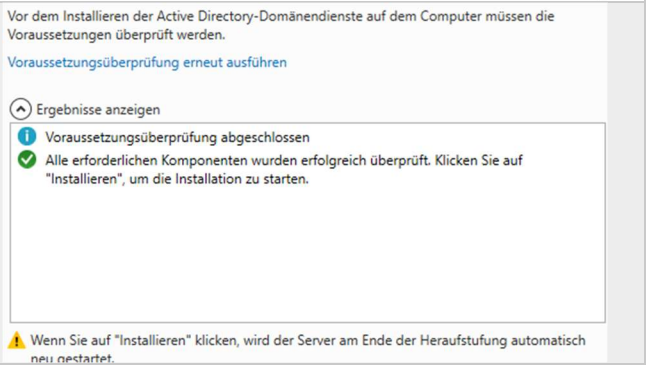
Auswahl „Features hinzufügen“	
DHCP-Server auswählen und Feature hinzufügen	
DNS-Server auswählen und Feature hinzufügen	
mehrmals auf weiter drücken	
DNS-Server einrichten	

neue Zone auswählen	
Auswahl primäre Zone	
Auswahl Forward-Lookupzone	
Eingabe Domänenname	
Auswahl neue Datei…	
Nicht sichere dynamische….	
Assistenten fertigstellen	
	
Reverse-Lookupzone einrichten **rechte MT** → neue Zone **Assistent wird gestartet**	
Auswahl primäre Zone	
Auswahl IPv Bereich	

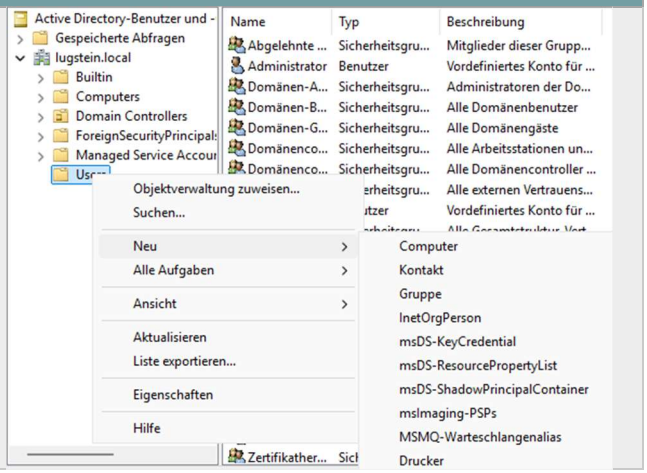
Eingabe der Reverse-Lookupzone	
	
Auswahl treffen	
Assistent wird fertiggestellt	
	

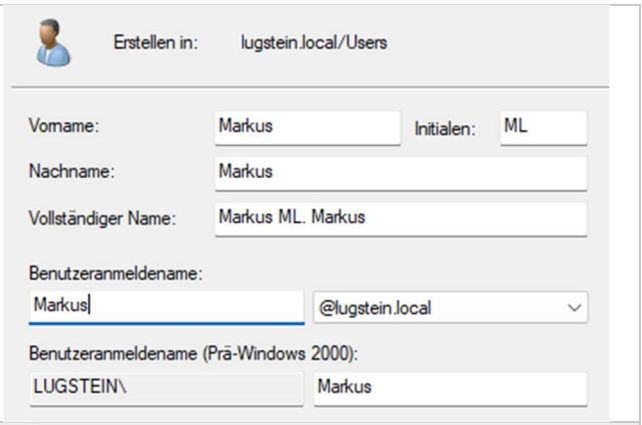
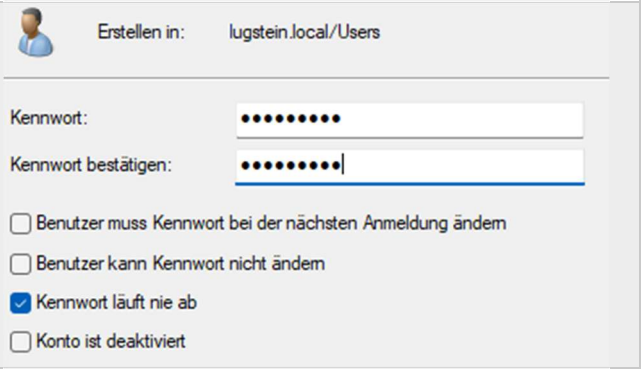
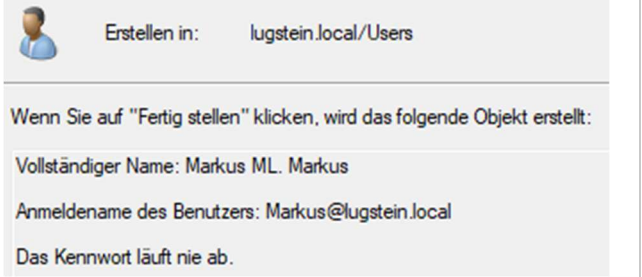
3.2 Active Directory

Neue Gesamtstruktur hinzufügen **Namen der neuen Stammdomäne eingeben.** **lugstein**	
Kennwortvergabe für den Verzeichnisdienst-Wiederherstellungsmodus DSMR-KW **Aa_123456**	

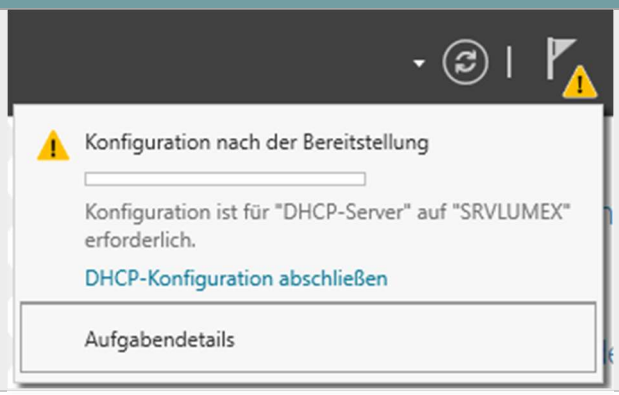
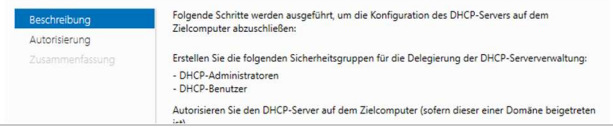
Haken entfernen	
wird vorgeschlagen	
Pfade für Speicherorte	
Auswahl überprüfen und weiter	
Voraussetzungsprüfung und Neustart	

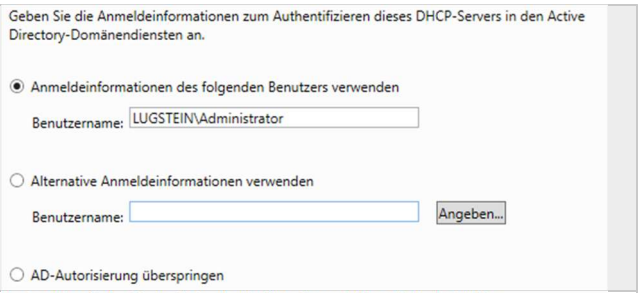
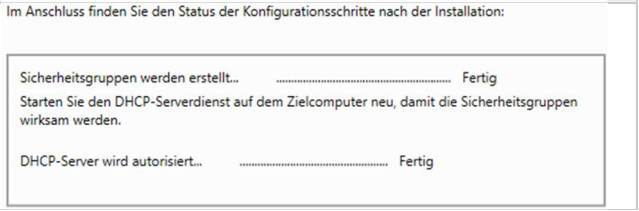
3.3 Benutzer anlegen

neuen Benutzer anlegen	

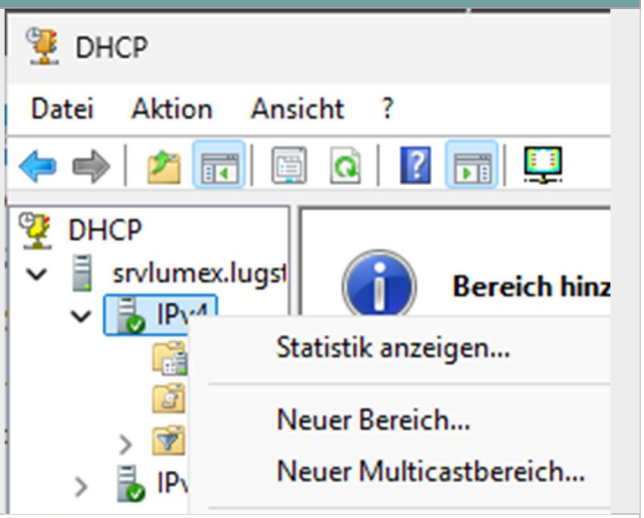
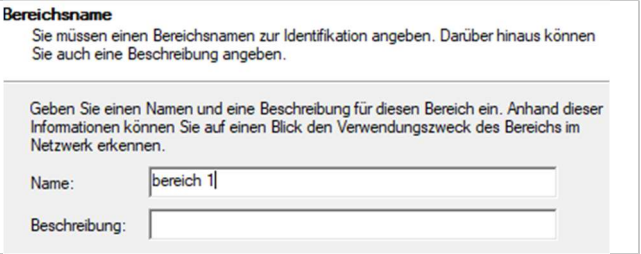
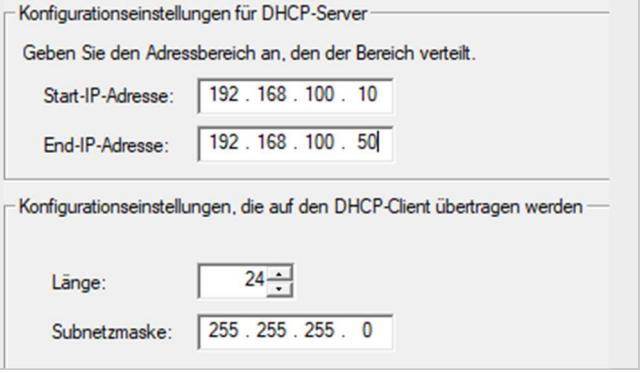
Eintrag der Daten vom neuen Benutzer	
Kennwort Kriterien Eingabe	
	

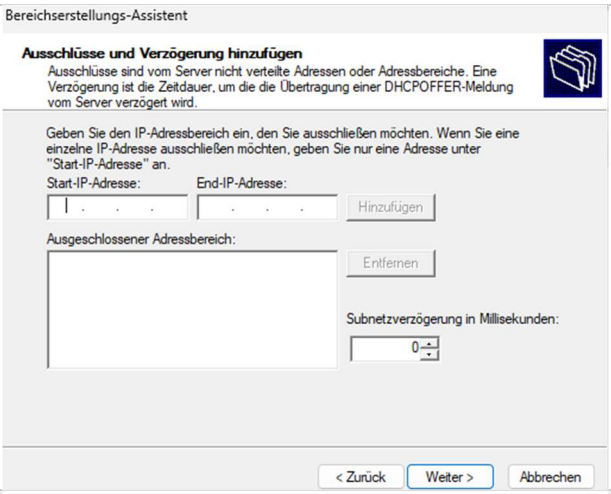
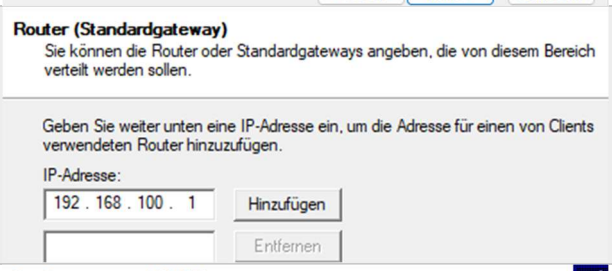
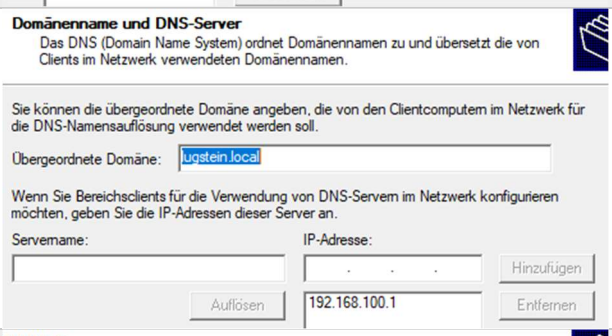
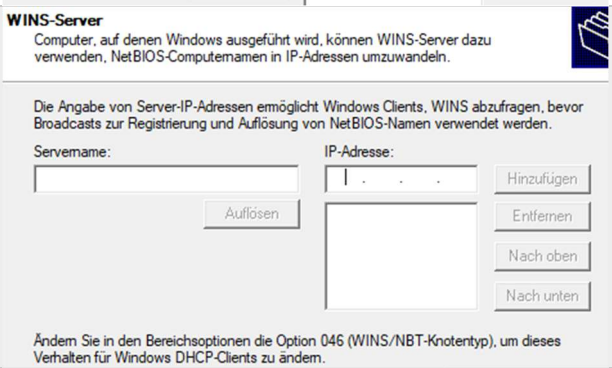
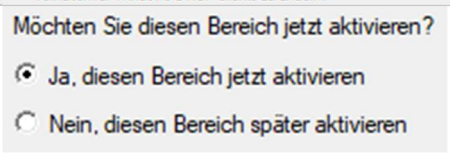
3.4 DHCP-Konfiguration abschließen

	
Beschreibung der folgenden Schritte	

Commit ausführen	
Schließen und Beenden	

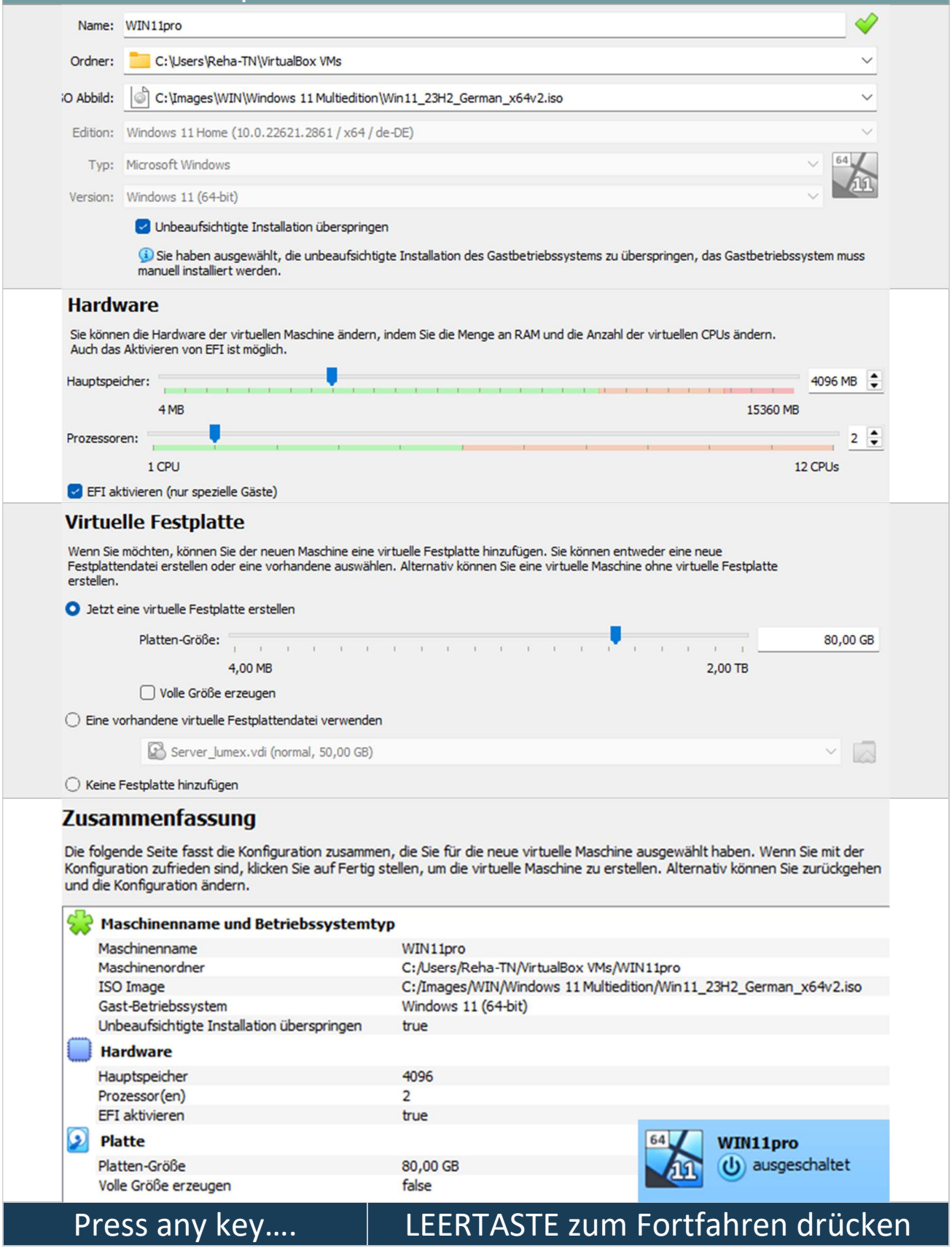
3.5 Einstellungen DHCP

Auswahl neuer Bereich ➔ **Assistent startet**	
Bereichsnamen festlegen	
Vergabe des DHCP-IP Bereiches der genutzt werden soll	

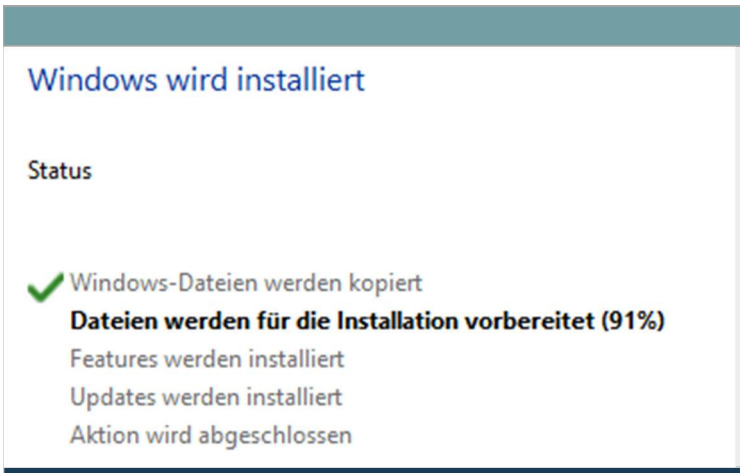
immer weiter, weiter, weiter…. **Leasedauer** **DHC-Optionen konfigurieren**	
Router → 192.168.100.1 → **hinzufügen**	
Domänenname und DNS-Server	
Kein Eintrag	
Mit Weiter…. Bis Fertigstellen	

4. Installation WIN 11 Pro

Installation von WIN11 pro als Virtual-Machine



4.1 Installation eines lokalen Benutzers



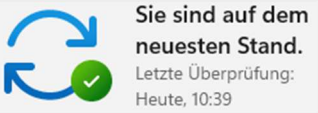
Installation eines lokalen Konto´s ohne besondere Eingaben/Anforderungen von WIN 11_pro

Einrichtung Schul- oder Geschäftskonto
→ lokales Konto

Benutzer: admin_lugstein
KW: Aa_123456

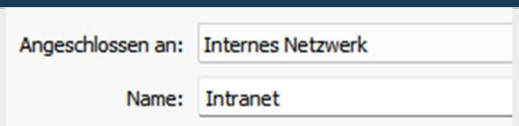
Gasterweiterung eingelegt

Durchführen und System auf neusten Stand bringen



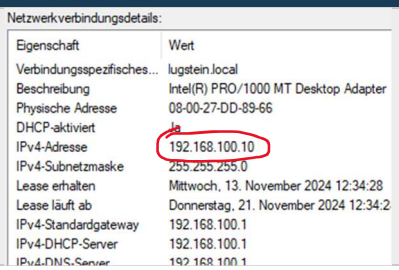
Sicherungspunkt der VM WIN11_pro erstellen

Einstellungen am Netzwerkadapter 1 des Clint PC auf „internes Netzwerk“ ändern



Die Vergabe der IP-Adresse am Client-PC wurde per DHCP gemacht!!

Verbindungsdetails am Client-PC der Verbindung „Intranet“




```
Ethernet-Adapter Intranet:

   Verbindungsspezifisches DNS-Suffix: lugstein.local
   Verbindungslokale IPv6-Adresse  . : fe80::2cb8:3cfb:35af:f66f%4
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.10
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.100.1

C:\Users\lumex>
```

Durch die Eingabe „ipconfig“ im CMD wird die aktuelle Konfiguration des Ethernet-Adapters (Intranet) angezeigt.

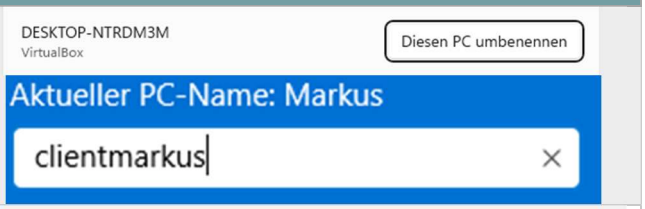
aktuelle Konfiguration der Ethernet-Adapter am Server.
Internet: per DHCP vom lokalen Zugriffspunkt

Intranet: per DHCP vom Server erhalten!

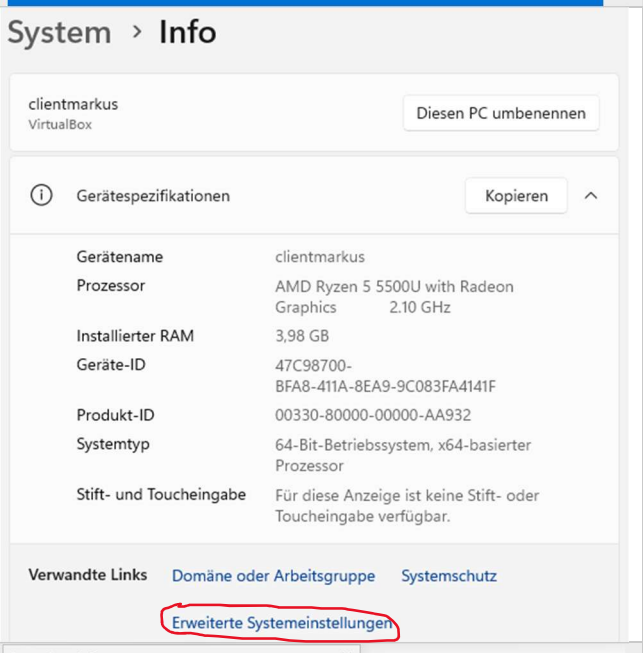
```
Ethernet-Adapter Internet:

   Verbindungsspezifisches DNS-Suffix: company.local
   Verbindungslokale IPv6-Adresse  . : fe80::f98f:1f33:7976:d649%15
   IPv4-Adresse  . . . . . . . . . . : 10.2.30.43
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 10.2.30.1

Ethernet-Adapter Intranet:

   Verbindungsspezifisches DNS-Suffix:
   Verbindungslokale IPv6-Adresse  . : fe80::55eb:23c3:a0bc:62d6%6
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.1
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . :
```

5. PC zur Domain hinzufügen

Client-PC umbenennen
Systemsteuerung\System und Sicherheit\System
→ PC umbenennen



Erweiterte Systemeinstellungen
Nach der Umbenennung des PC´s und einem NEUSTART kann man die Erweiterten Systemeinstellungen aufrufen.

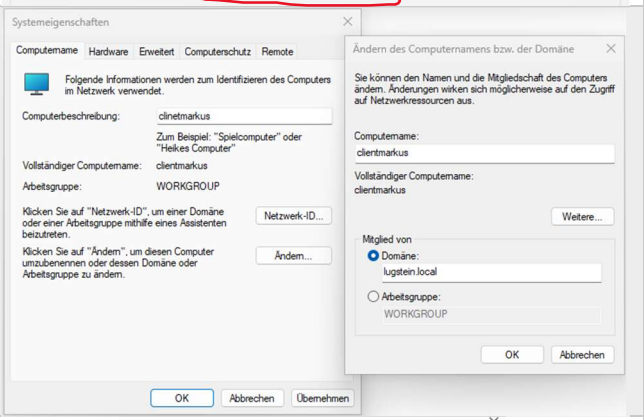


Computername ändern

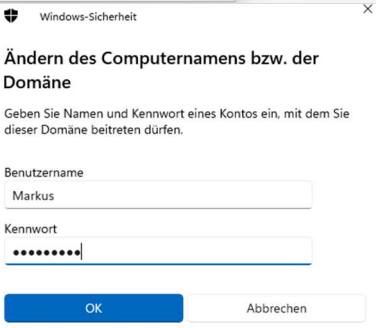
Unter dem Reiter „Computername“ kann eine Eintragung erfolgen, muss aber nicht.

Ändern... →**Computername und Domäne ändern!**

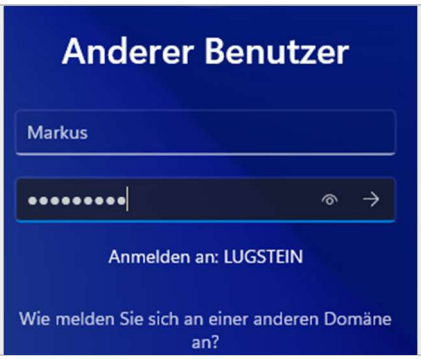
Eintragung: lugstein.local

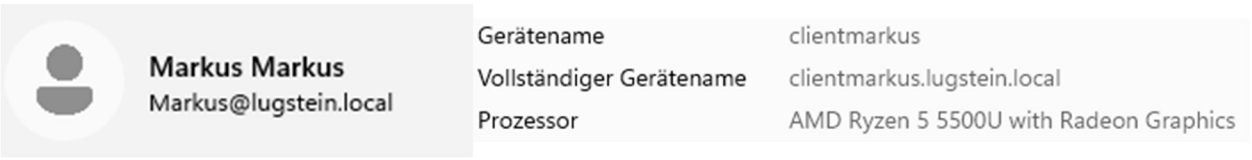


Domain ändern
Hier nun den unter AD erstellten Benutzer (Client, Konto) samt Zugangsdaten angeben.



Nach einem Reboot kann man sich dann nach der Auswahl „Anderer Benutzer“ an der neuen Domäne anmelden.

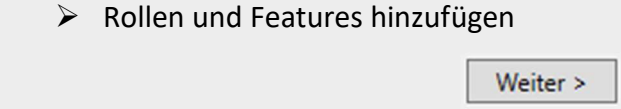


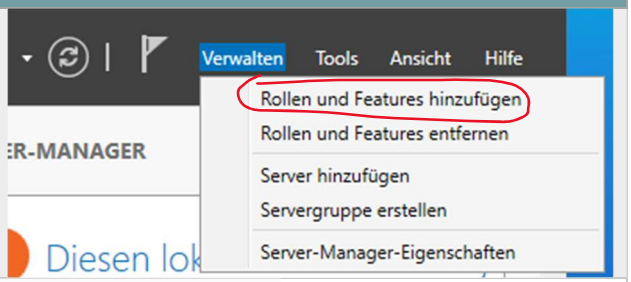


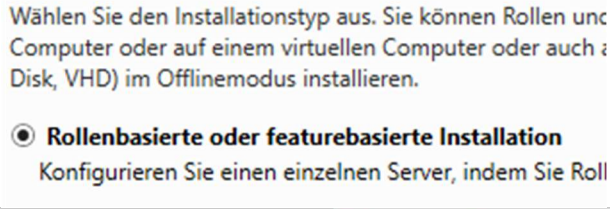
5.1 Einrichtung Routing & RAS am WIN-Server

Unter „Verwalten“

- Rollen und Features hinzufügen

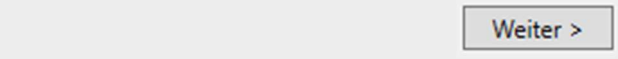


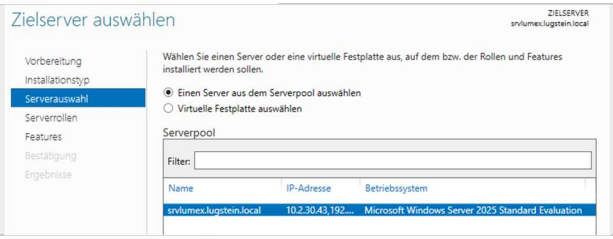




Serverauswahl

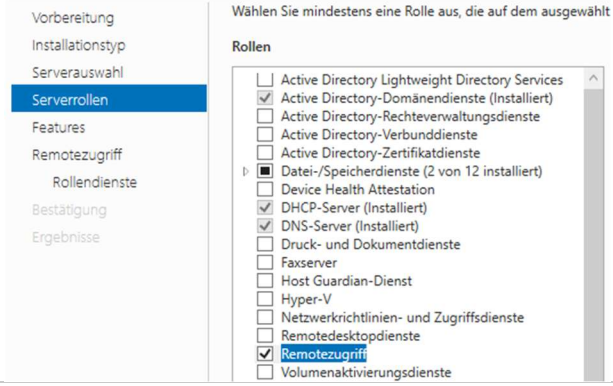
- Zielserver auswählen





Serverrollen

- Remotezugriff aktivieren (Haken)

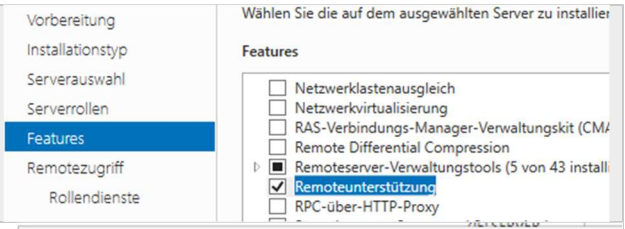


Features

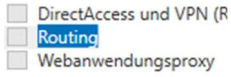
- Remoteunterstützung

Weiter >

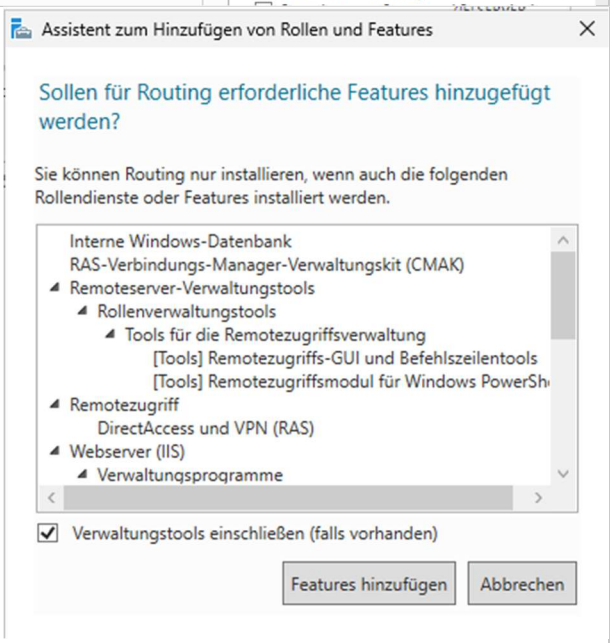
Auch nächsten Schritt mit Weiter >



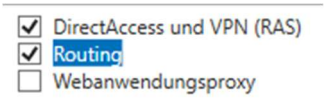
Bei der Auswahl „Routing“ öffnet sich ein neues Fenster mit einem Assistenten.



Klick auf → Features hinzufügen



Nachdem die Features hinzugefügt wurden, werden die Haken bei Routing und RAS automatisch gesetzt!

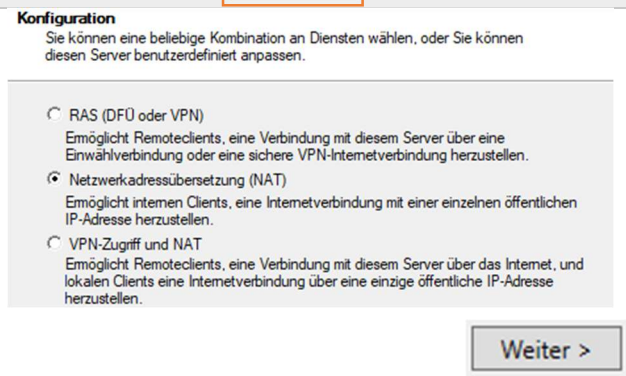


Weiter >

Überprüfung der aller Auswahlpunkte und anschließender finaler Bestätigung vor der Installation!!!!

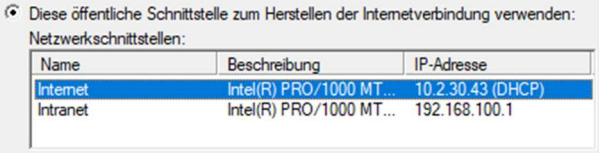
Tools/Routing and RAS konfigurieren und aktivieren Assistent starten

Auswahl „NAT“



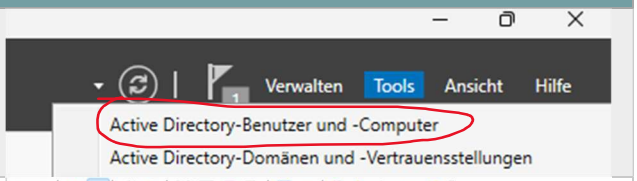
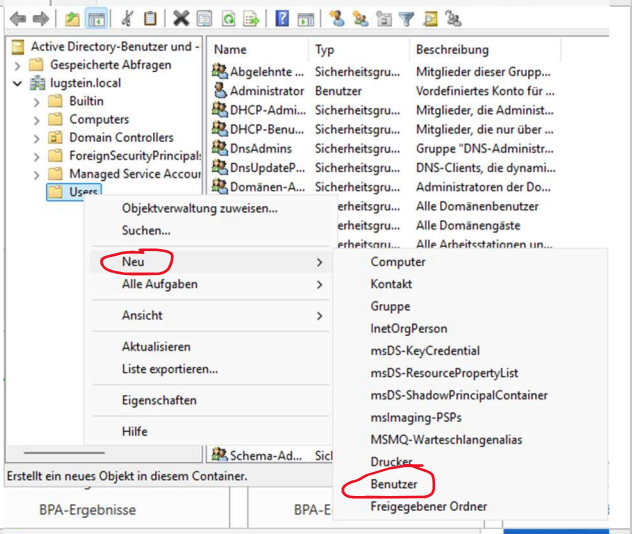
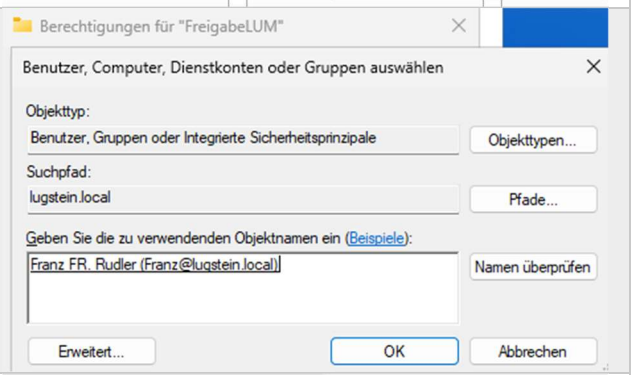
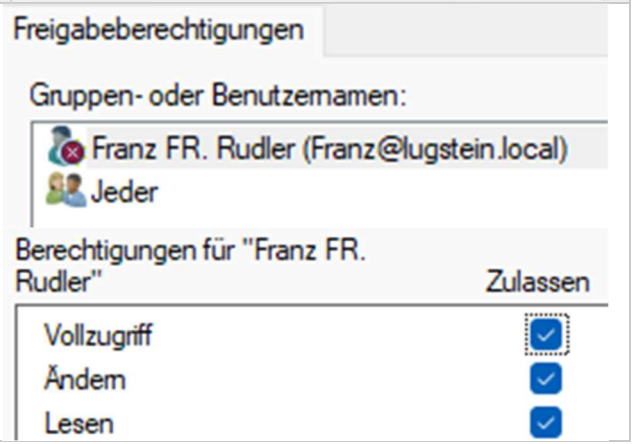
Auswahl der Netzwerkverbindung

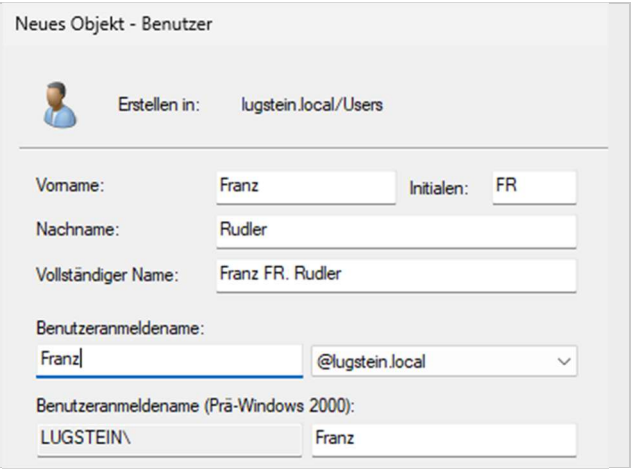
Weiter



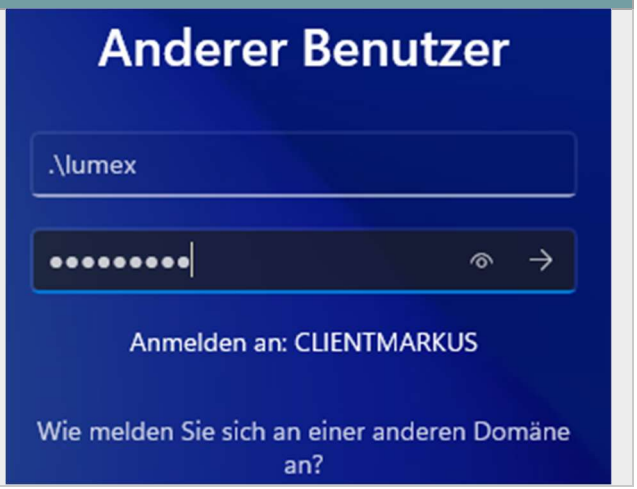
Nun den Client starten und die Verbindung zum Internet ausprobieren!!!
Sollte funktionieren wenn alles richtig installiert wurde!

5.2 Verzeichnis-Freigabe

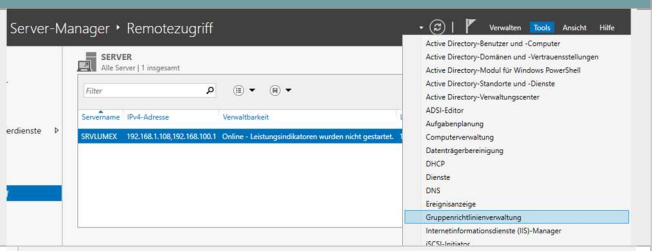
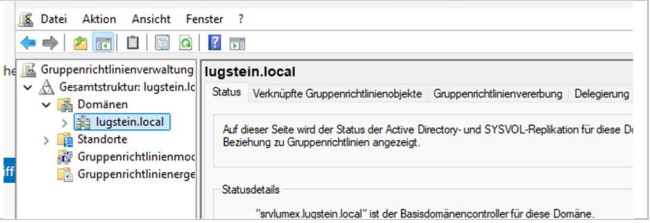
öffnen „Active Directory-Benutzer und -Computer“ am WIN_server2025	
Anlegen eines neuen Benutzers für Testzwecke	
• Freigabeverzeichnis „FreigabeLUM“ am Rechner“Server“ erstellen • Berechtigungen wählen 1. Hinzufügen einer Gruppe oder Benutzernamens **Eingabe „Franz“ und Namen überprüfen** →OK	
Nun erscheint der User „Franz“ **Berechtigungen auf „Vollzugriff“ setzen** →	

Benutzer: Franz Rudler Kennwort: Aa_123456 Benutzeranmeldename: Franz@lugstein.local	

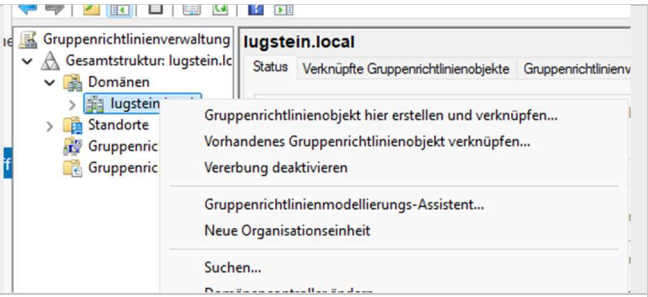
6. Anmeldung als lokaler Benutzer an einem Client-PC

Eingabe: .\lumex (für lokalen Benutzer) **Passwort: Aa_123456**	

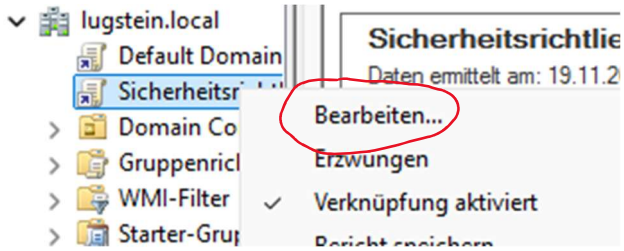
7. Gruppenrichtlinien

Server-Manager-Tools **„Gruppenrichtlinienverwaltung“**	
⮟Gesamtstruktur **⮟Domänen** **⮟lugstein.local**	

neue GPO erstellen
Rechtsklick auf die Domäne oder OU und wähle "Gruppenrichtlinie hier erstellen und verknüpfen".
Benenne die GPO, z. B. "Sicherheitsrichtlinien".



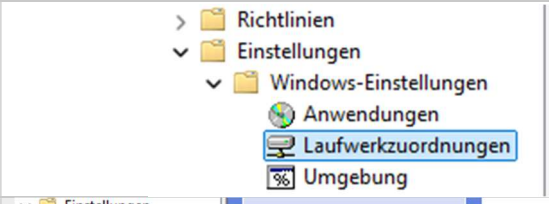
GPO bearbeiten
Rechtsklick auf die neu erstellte GPO und wähle "Bearbeiten".
Navigiere durch den Gruppenrichtlinien-Editor, um Richtlinien unter "Computerkonfiguration" oder "Benutzerkonfiguration" festzulegen.



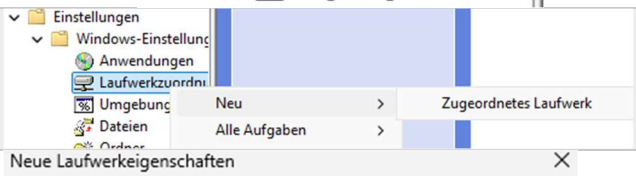
GPO durchsetzen
Kontrolliere die Verknüpfung mit der OU und setze die Richtlinie ggf. auf "Erzwungen", um sie priorisiert durchzusetzen.

⮟Benutzerkonfiguration
⮟Einstellungen
⮟Windows-Einstellungen

„Laufwerkzuordnungen“



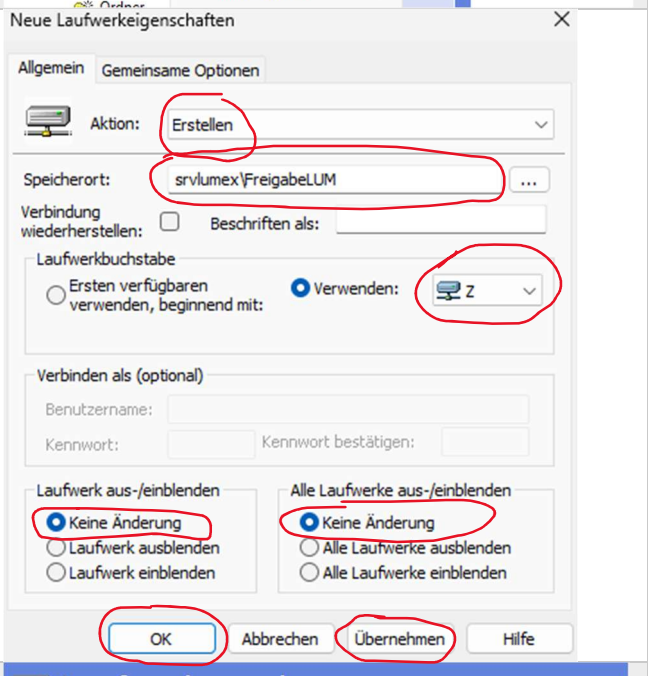
rechte Maustaste → „Neu“
→ Zugeordnetes Laufwerk



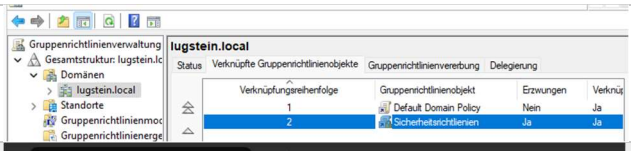
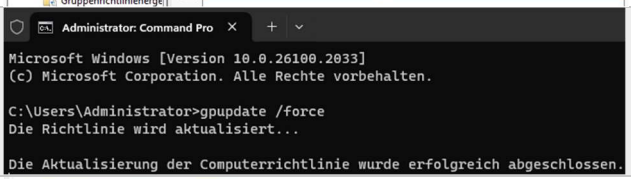
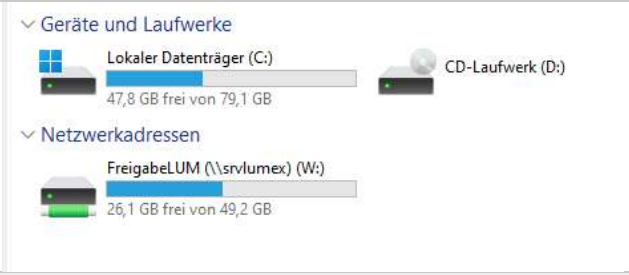
Aktion: erstellen

Eingabe des Speicherortes:
\\srvlumex\FreigabeLUM

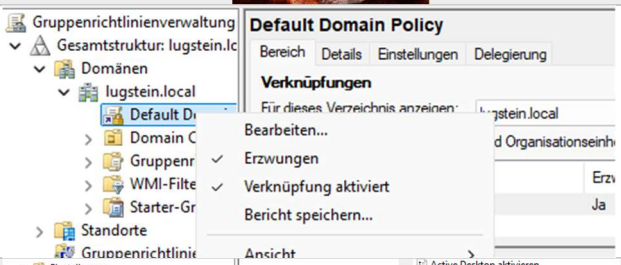
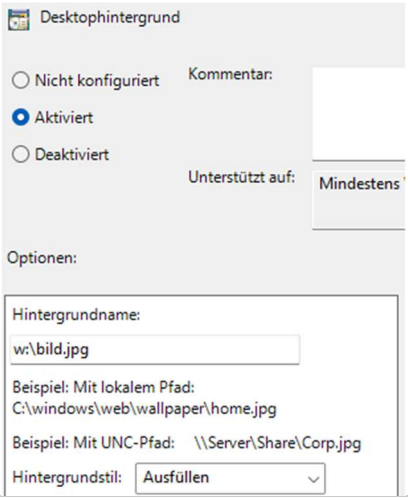
Laufwerksbuchstaben zuweisen

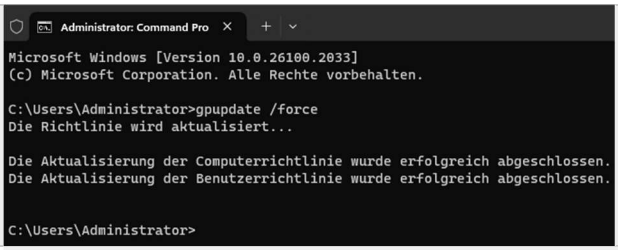


WICHTIG!
Wenn aktiv, sollte kleines grünes Dreieck erscheinen

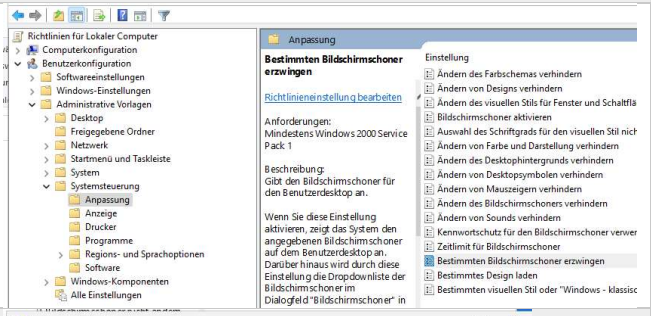
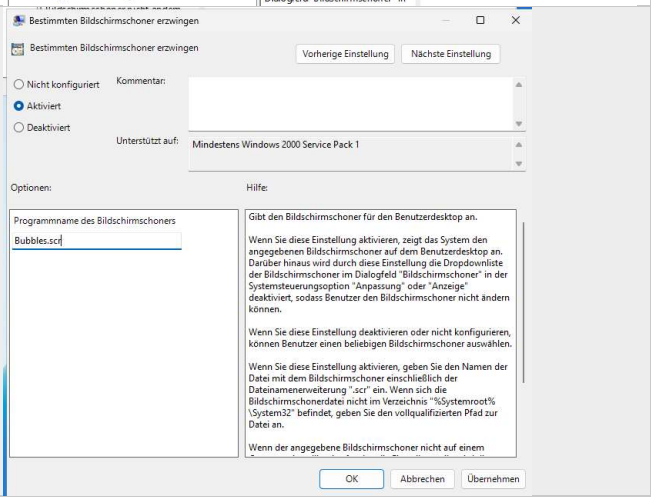
Gruppenrichtlinien „erzwingen“	
Richtlinien aktualisieren am server & client PC gpupdate /force	
Nach dem Anmelden bzw. Neustart ist die Netzwerkadresse nun sichtbar!	

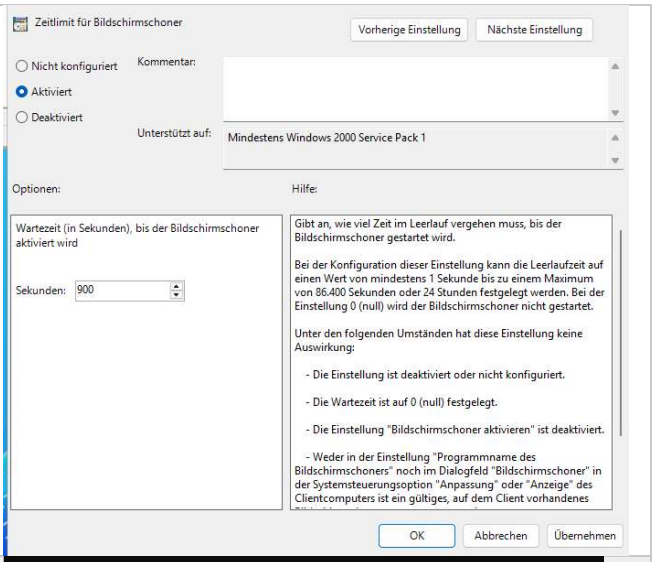
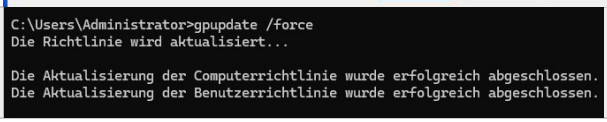
7.1 Desktop-Hintergrund für alle Nutzer ändern

download eines beliebigen Hintergrund-Bildes und dieses in den Freigabeordner \\srvlumex\FreigabeLUM ablegen.	
Öffnen der Gruppenrichtlinienverwaltung ➔ **Default Domain policy (**rechte Maustaste „Bearbeiten) **Gruppenrichtlinienverwaltungs-Editor öffnet sich**	
Im Editor unter Benutzerkonfiguration → Richtlinien → **Administrative Vorlage →** Desktophintergrund bearbeiten	
Hier zuerst auf „Aktiviert“ setzen **Unter Hintergrundname:** **Ablageort und Dateiname der Bilddatei mit Kürzel angeben.** **Außerdem kann hier noch eine Auswahl zum Hintergrundstil getroffen werden.**	

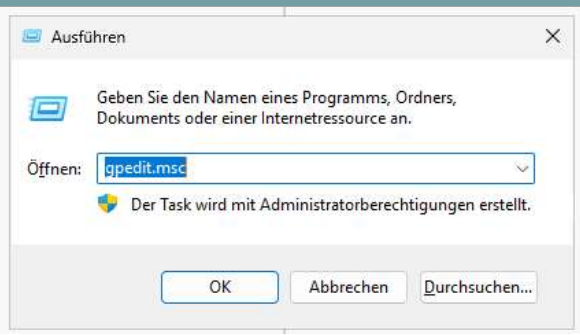
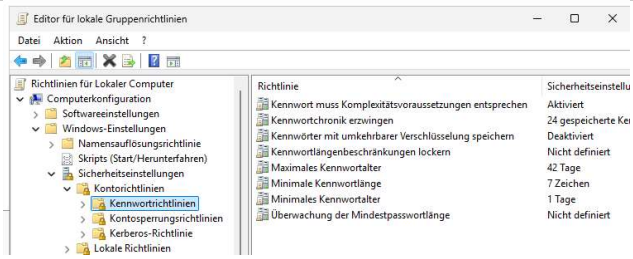
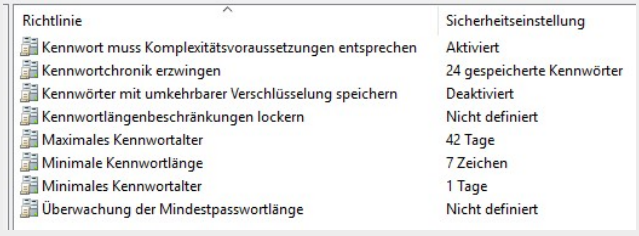
Richtlinien aktualisieren am server & client PC gpupdate /force	
Nach dem Anmelden bzw. Neustart wurde der Desktophintergrund geändert!	

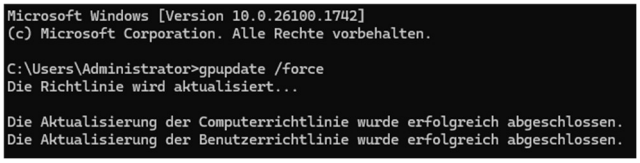
7.2 Bildschirmschoner über die Gruppenrichtlinien verwalten

Gruppenrichtlinien-Editor öffnen	
Gruppenrichtlinien-Editor öffnen Melde dich als Administrator auf Server an. Drücke Windows-Taste + R, gib *gpedit.msc* ein und drücke Enter, um den Gruppenrichtlinien-Editor zu öffnen.	
Navigiere zu den Richtlinieneinstellungen Im Gruppenrichtlinien-Editor navigiere zu: Benutzer*konfiguration > Administrative Vorlagen > Systemsteuerung > Anpassen >bestimmten Bildschirmschoner erzwingen.*	
Richtlinie „Bildschirmschoner aktivieren“ konfigurieren Doppelklicke auf die Einstellung "Bildschirmschoner aktivieren". Wähle "Aktiviert" aus und klicke auf "OK". Diese Einstellung sorgt dafür, dass der Bildschirmschoner aktiviert wird.	

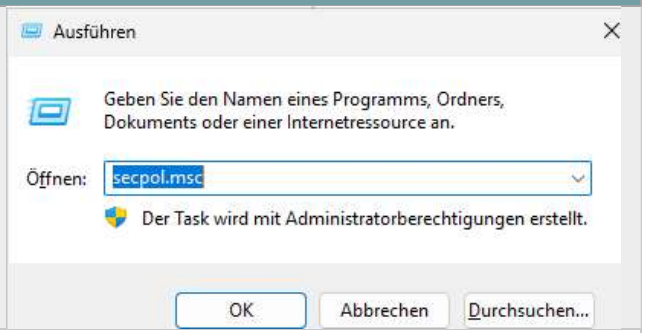
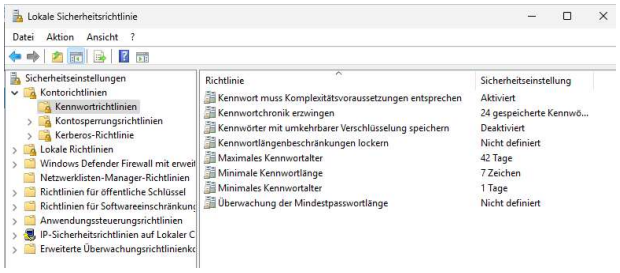
Richtlinie „Zeitlimit für Bildschirmschoner“ festlegen Doppelklicke auf die Einstellung "Zeitlimit für Bildschirmschoner“. Klicke auf „aktiviert“. Gib die Zeit in Sekunden ein, nach der der Bildschirmschoner automatisch gestartet werden soll (z.B. 900 für 15 Minuten). Klicke auf "OK".	
Gruppenrichtlinien aktualisieren am ServerA Eingabe CMD: *gpupdate /force*	

7.3 Methode 1: Passwortrichtlinien über die Gruppenrichtlinien (GPO) ändern

Schritt 1: Gruppenrichtlinien-Editor öffnen • Melden Sie sich als Administrator am Server an. • Drücken Sie Win + R, geben Sie *gpmc.msc* ein und drücken Sie Enter, um die Gruppenrichtlinien-Verwaltungskonsole zu öffnen.	
Schritt 2: Gruppenrichtlinien für PW bearbeiten • Navigieren Sie zu Computerkonfiguration → **Windows-Einstellungen** → Sicherheitseinstellungen → **Kontorichtlinien** → Kennwortrichtlinien	
Schritt 3: Kennwortrichtlinien ändern • **Maximales Passwortalter** • **Minimales Passwortalter** • **Mindestlänge des Passwortes** • **Komplexität des Passwortes** • **…..**	

Schritt 4: Gruppenrichtlinien anwenden Nachdem die gewünschten Änderungen vorgenommen haben, müssen die Richtlinien angewendet werden. Durch die Eingabe *gpupdate /force* in der Kommandozeile (CMD) oder einen Neustart wird es ausgeführt.	

7.4 Methode 2: Über die lokalen Sicherheitsrichtlinien (secpol.msc)

Lokale Sicherheitsrichtlinien öffnen Drücken Sie Windows-Taste + R, geben Sie *secpol.msc* ein und bestätigen Sie. Dies öffnet die lokalen Sicherheitsrichtlinien.	
Passwortrichtlinien konfigurieren Gehen Sie zu Sicherheitsoptionen → Kontorichtlinien → Passwortrichtlinien und ändern Sie die Einstellungen nach Bedarf.	
Änderungen speichern und anwenden Speichern Sie die Änderungen und schließen Sie das Fenster. Diese Richtlinien gelten dann für das lokale System.	

8. Google-Chrome per Gruppenrichtlinien installieren und Startseite festlegen

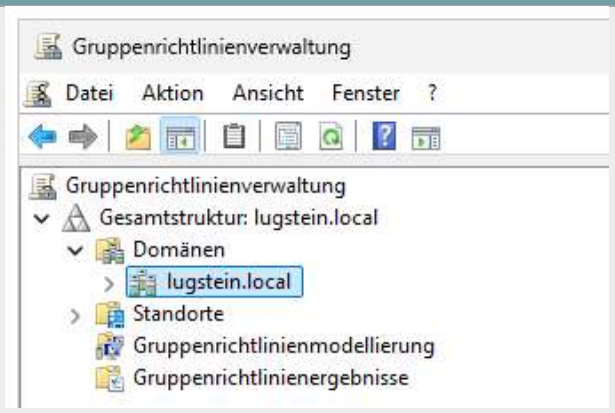
8.1 Google Chrome Installation über Gruppenrichtlinien vorbereiten

Google Chrome MSI herunterladen Gehe auf die Google Chrome Enterprise Download-Seite. Lade das MSI-Installationspaket für Chrome herunter.	
MSI-Datei in einer Netzwerkfreigabe ablegen	

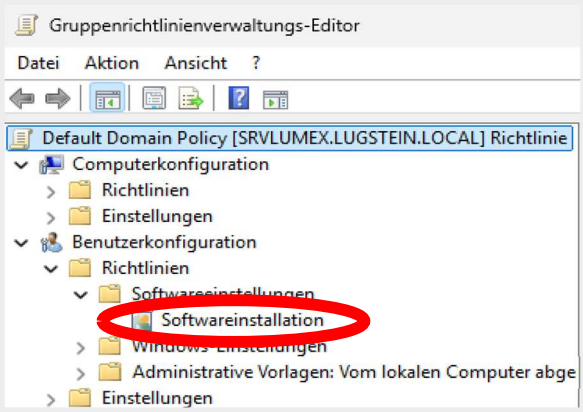
Lege die Datei auf einer freigegebenen Netzwerkressource ab, die von den Client-Computern erreicht werden kann. Beispiel: \\ServerName\Freigabe\chrome_installer.msi. Stelle sicher, dass die Berechtigungen für die Freigabe korrekt gesetzt sind (Lesezugriff für alle relevanten Computer).	

8.2 Chrome über Gruppenrichtlinien installieren

Gruppenrichtlinien erstellen oder bearbeiten
Öffne die *„Gruppenrichtlinienverwaltung“* (unter Tools) auf deinem Windows Server. Erstelle eine neue Gruppenrichtlinie oder bearbeite eine vorhandene, die auf die Ziel-Computer angewendet wird**.**
Gehe dazu zur **Domäne** *„lugstein.local“* und mache einen Rechtsklick auf *„Default Domain Policy“*→ **Bearbeiten**



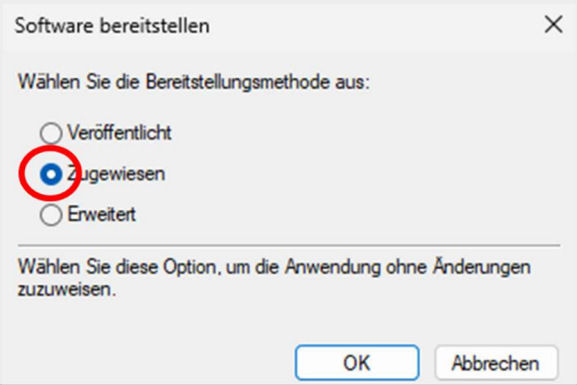
Der Gruppenrichtlinienverwaltungs-Editor öffnet sich und wir navigieren unter „Benutzerkonfiguration“ zu „Softwareinstallation“**.**
Rechte Mausklick auf Softwareinstallation → „Neu“ → **„Paket“**



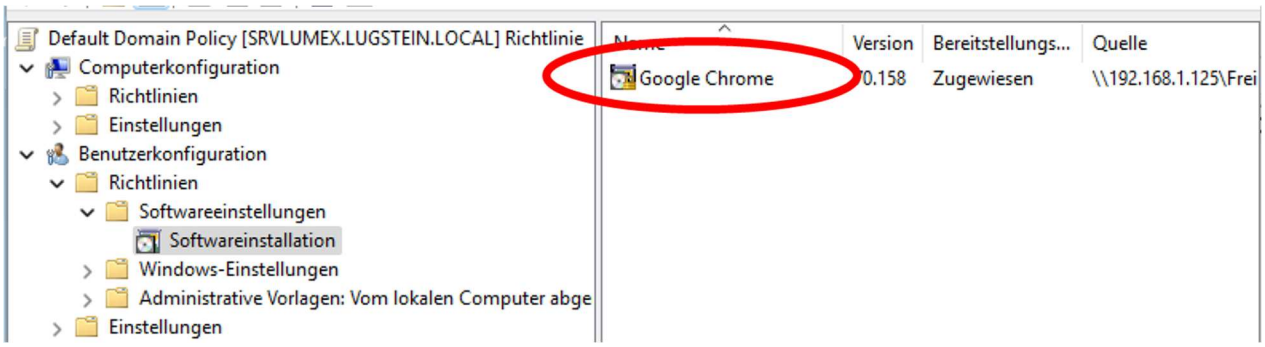
Hier öffnet sich ein Fenster in dem wir den Ablageort der zu installierenden Software auswählen können.

Wähle die Option Zugewiesen aus.

<u>Hinweis: Das MSI-Paket wird installiert, wenn sich die Computer das nächste Mal starten und die Gruppenrichtlinie angewendet wird.</u>

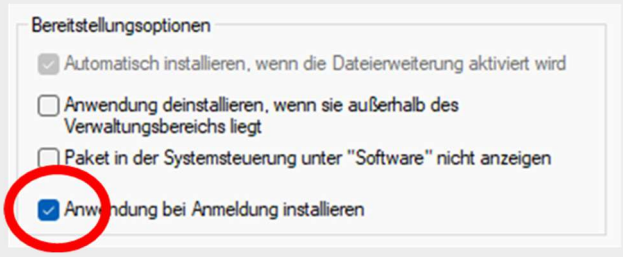


Nach dem Bestätigen mit „OK“ sollte die Bereitstellung ersichtlich sein:



Durch Doppelklick auf die Richtlinie „Google Chrome“ können Einstellungen verändert werden.

Unter „Bereitstellung von Software“ unbedingt unter Bereitstellungsoptionen den Haken bei „**Anwendung bei Anmeldung installieren**“ setzen!



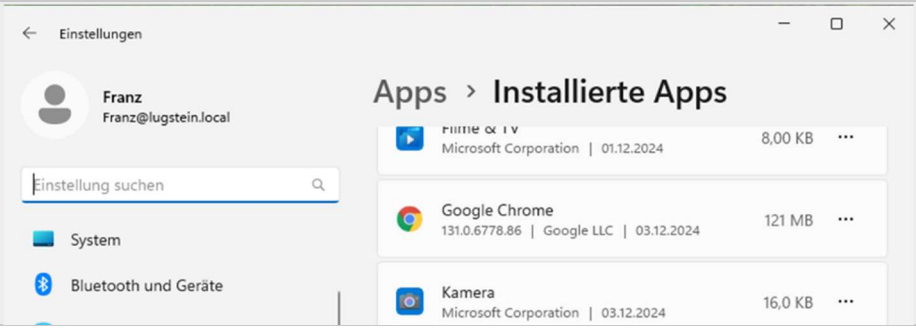
Gruppenrichtlinie anwenden

Stelle sicher, dass die Gruppenrichtlinie auf die Organisationseinheit (OU) angewendet wird, in der die Ziel-Computer enthalten sind.

Aktualisiere die Gruppenrichtlinien auf den Server und Client → `gpupdate /force`

Nun den Computer neu starten, um zu testen, ob die Installation ausgeführt wird.

Installation von google-chrom wurde nach dem Neustart ausgeführt!

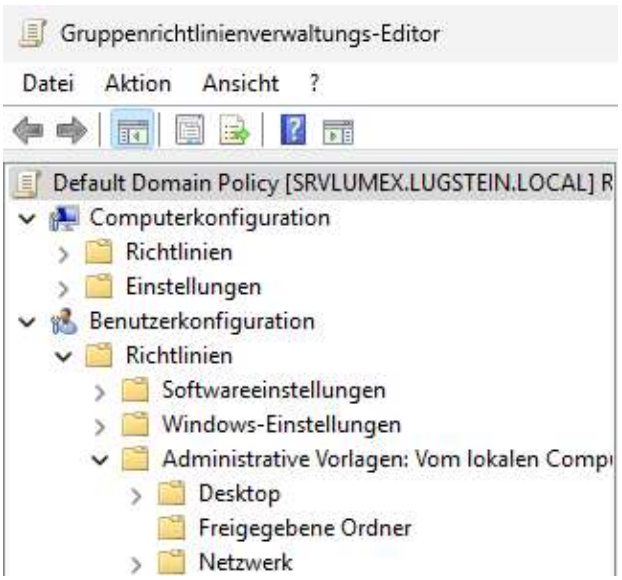


8.3 Startseite für Chrome über Gruppenrichtlinien festlegen

Administrative Vorlagen für Google Chrome hinzufügen
Lade die Administrative Vorlagen (ADMX) für Google Chrome von der Google-Enterprise-Seite herunter.
Kopiere die heruntergeladenen .admx-Dateien in den Freigabe-Ordner

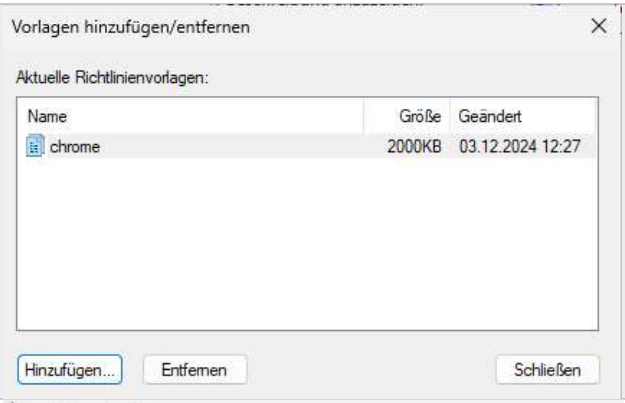
Gehe dazu zur **Domäne** *„lugstein.local“* und mache einen Rechtsklick auf *„Default Domain Policy“* → **Bearbeiten**

Navigiere: → Benutzerkonfiguration → **Richtlinien** → Administrative Vorlagen: Vom lokalen Computer
Rechter Mausklick → **Vorlagen hinzufügen/entfernen** → hinzufügen!



In den vorhin heruntergeladenen Policy Templates unter G:\windows\adm\de-DE finden wir eine Datei mit dem Namen „chrome.adm“ die wir öffnen.

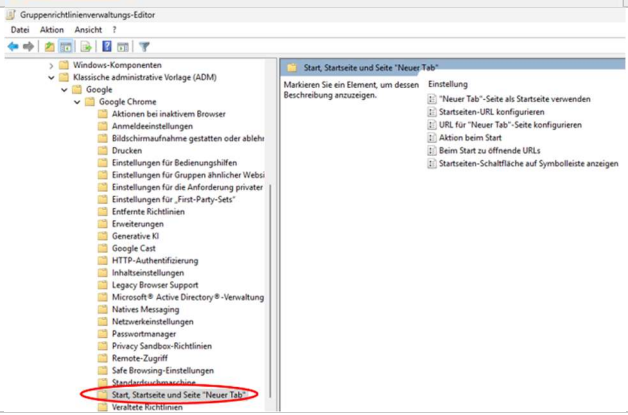
Klick auf schließen

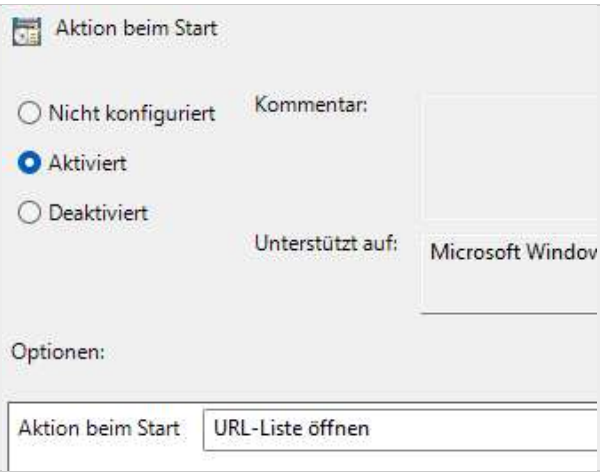


Anschließend navigieren wir zu:
→ Klassische administrative Vorlage
→ **Google**
→ Google chrome
→ **Start, Startseite und Seite „Neuer Tab“**

Im rechten Bereich sehen wir nun die Richtlinien für **„Aktion beim Start“**

Rechter Mausklick darauf → bearbeiten



Auswahl auf „Aktiviert“ setzen **Auswahl bei „Aktion beim Start“** → „URL-Liste öffnen“. **„Übernehmen“ und mit „OK“ bestätigen** **Status = Aktiviert**	
Als nächstes öffnen wir durch einen Klick auf die rechte Maustaste und durch Auswahl von „bearbeiten“ die Richtlinie „Beim Start zu öffnende URLs“, setzen den Haken bei „Aktiviert“ und tragen nach Klick auf „Anzeigen“ die Adresse ein die beim Start von Chrome geöffnet werden soll. **Hier: https://orf.at/ Übernehmen und OK**	
Erzwinge die Aktualisierung der Gruppenrichtlinien auf den Clients mit dem Befehl: *gpupdate /force*