Server2025-Dokumentation

Einrichtung einer Windows Server Domänenumgebung mit AD, GPOs und Windows 11 Client**

Autor: Markus Lugstein

Datum:

Modul: Betriebssysteme & Labor

Thema: Aufbau einer virtuellen Testumgebung mit Netzwerk

Inhalt

1. Zielsetzung

Ziel dieses Arbeitsauftrages ist der Aufbau einer vollständigen virtuellen Schulnetzwerk-Infrastruktur.
Dabei wird ein Windows Server als Domänencontroller eingerichtet, zentrale Netzwerkdienste bereitgestellt und ein Windows-11-Client in die Domäne aufgenommen.

Am Ende soll eine funktionsfähige Mini-Domänenumgebung existieren, die folgende Anforderungen erfüllt:

- **Einrichtung der Domäne schule.local**
- **Zentrale Benutzer- und Gruppenverwaltung über Active Directory**
- **Unterschiedliche Benutzerrechte für Schüler und Lehrer**
- **Automatisches Laufwerksmapping über Gruppenrichtlinien (GPO)**
- **Zentrale Netzwerkdienste: DNS, DHCP, NAT (RRAS)**
- **Bereitstellung von Dateifreigaben**
- **Betrieb einer IIS-Webseite und eines FTP-Servers**
- **Einrichtung einer Serversicherung**
- **Funktionierender Windows-11-Client mit erfolgreicher Domänenanmeldung**

2. Ausgangsumgebung

2.1 Virtuelle Maschinen

Rolle	Betriebssystem	Besonderheiten
Server	Windows-Server 2025	zwei Netzwerkkarten (LAN und WAN)
Client	Windows 11 Pro	wird Mitglied der Domäne

2.2 Netzwerk-Grundkonfiguration

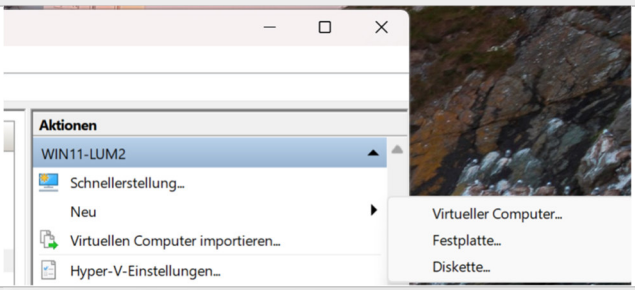
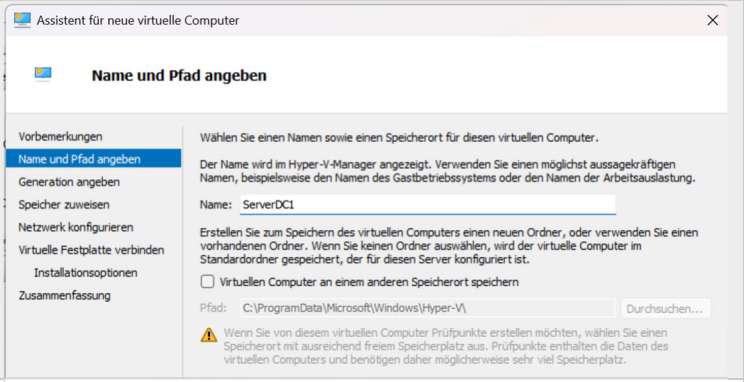
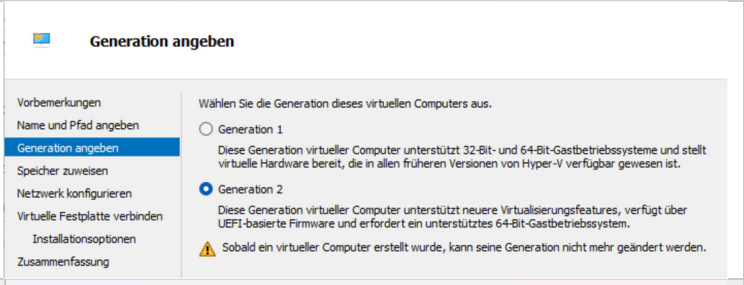
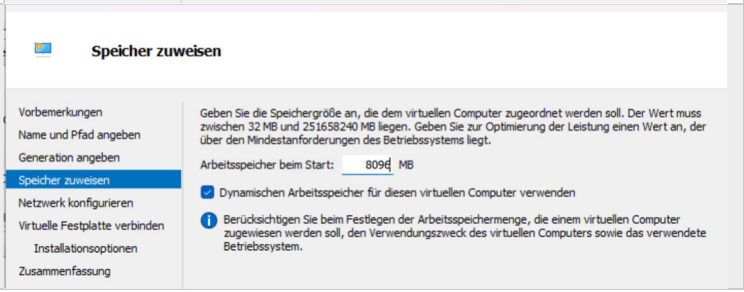
Der Server besitzt zwei Netzwerkadapter, der Client einen.

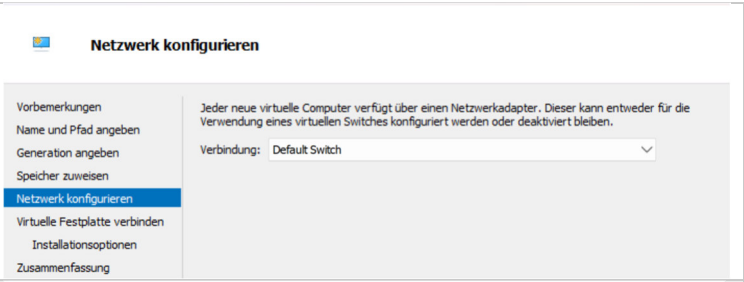
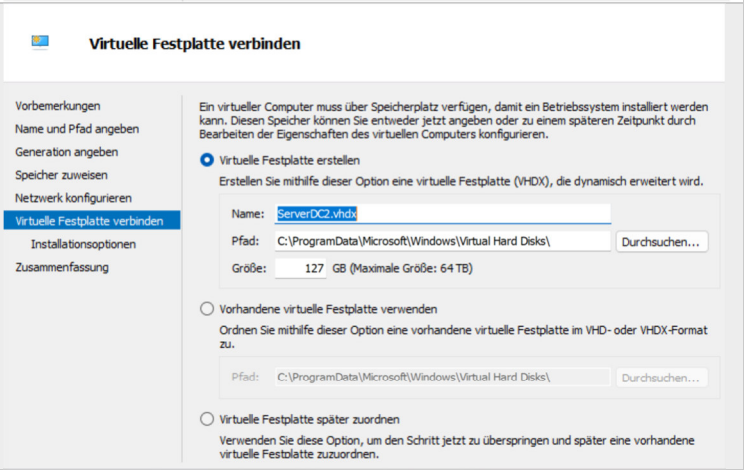
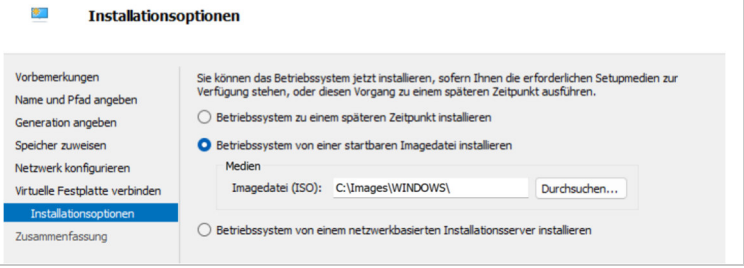
	SERVER			CLIENT
	EXTERN (Internet)	INTERN (Intranet)		ADAPTER (Intranet)
IP-Adresse	192.168.0.173	192.168.10.1		192.168.10.50
Subnet-Mask	255.255.255.0	255.255.255.0		255.255.255.0
Gateway	192.168.0.254	kein Eintrag		192.168.10.1
DNS	192.168.0.254	192.168.10.1		192.168.10.1
Modus	DHCP/statisch	statisch		statisch

2.3 Windows Server 2025 als VM installieren

- Edition: Standard (Desktop Experience)
- Updates vollständig installieren

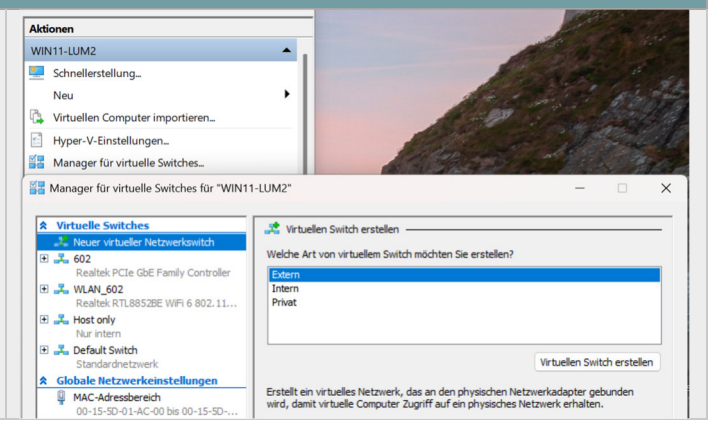
Server DC1 als VM unter Hyper-V erstellt

Download der .iso-Datei unter Microsoft	
Hyper-V starten und unter Aktion „Neu“ → Virtueller Computer auswählen. **erstes Fenster „Vorbemerkung“ mit „weiter“ überspringen…**	
Name des Servers eingeben: ServerDC1	
Bei Windows ist Generation 2 auszuwählen.	
wenn möglich 8GB RAM oder mehr zuweisen für einen Server!	

vorerst „default Switch“ auswählen → Konfiguration und Zuweisung eines passensen Switches folgt im Anhang	
Hier „virtuelle Festplatte erstellen“ auswählen da wir ein neues Gerät aus einer .iso Datei erstellen wollen.	
Hier suchen wir nun den Speicherort der .iso Datei und geben diesen an **passende .iso:** 26100.1742.240906-0331.ge_release_svc_refresh_SERVER_EVAL_x64FRE_de-de.iso **Dann mit „Weiter“ und Fertig stellen!**	

2.4 Virtuellen Switch erstellen

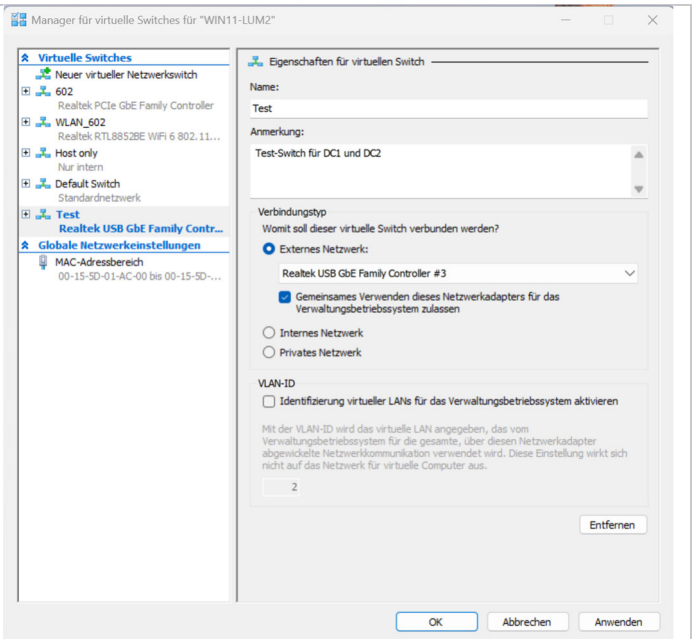
Um die VM´s an das Netzwerk anzubinden muss ein „virtueller Switch“ erstellt werden.

Dafür unter „Aktionen“ den **Manager für virtuelle Switches** öffnen und „extern“ auswählen und mit „virtuellen Switch erstellen“ bestätigen. Darauf hin öffnet sich ein neues Fenster für die Eigenschaften	

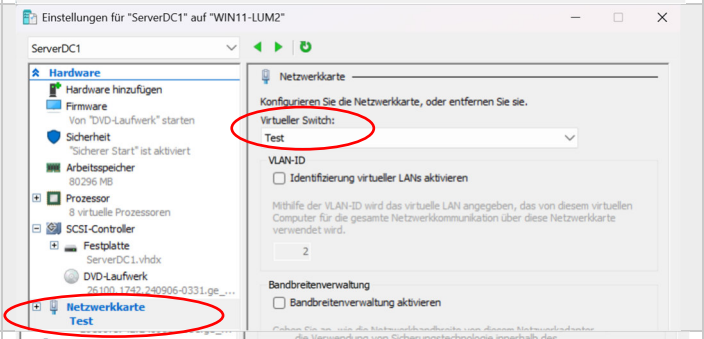
Namen vergeben: Test

externes Netzwerk:

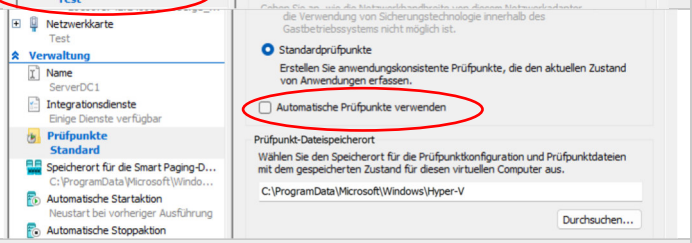
Auswahl der zu verwendenden Ethernet-Schnittstelle (in meinem Fall: #3, externer USB-Adapter)



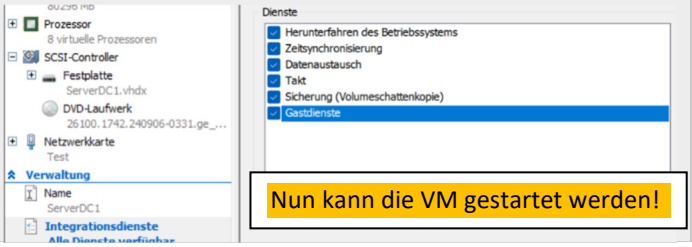
WICHTIG: nun kann der neu erstellte virtuelle Switch den neuen VM´s zugeordnet werden → re. Maustaste auf die VM → **Einstellungen**→ Auswahl „Test“→ **Anwenden**



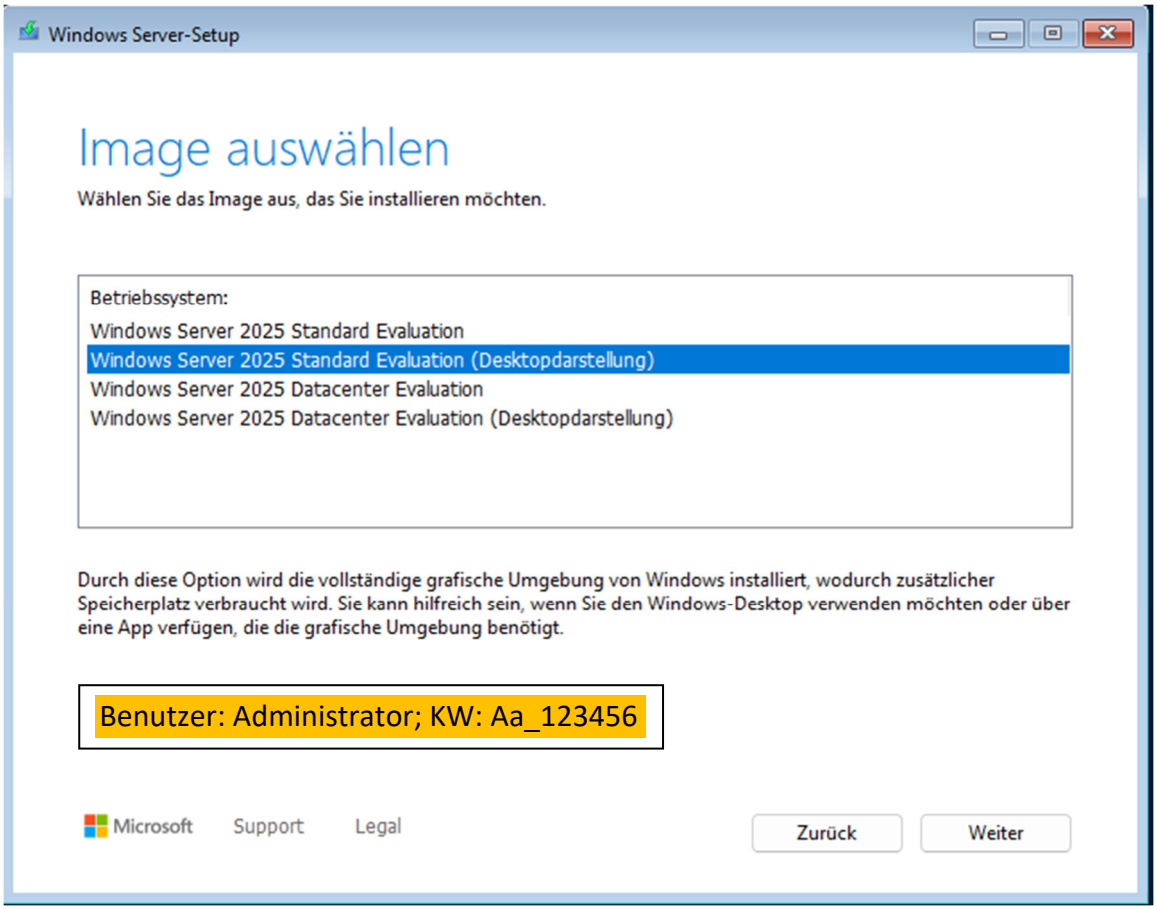
Deaktivieren der automatischen Prüfpunkte!



Aktivierung der Integritätsdienste (Gastdienste)



2.5 Server-Installation



2.6 Updates & zusätzlich Software-Installation

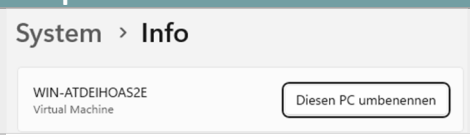
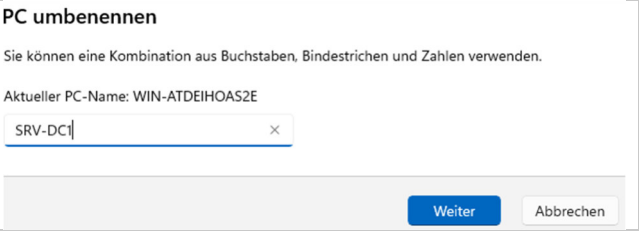
- ➔ Windows-Updates durchführen (Dauer mehr als 30 Min!)
- ➔ Browser installieren (Firefox & Google-Chrome)
- ➔ Notepad++ installieren
- ➔ Putty installieren
- ➔ WinSCP installieren
- ➔ Advanced IP-Scanner installieren
- ➔ Prüfpunkt „Basisinstallation“ erstellt.

2.7 Server Konfiguration

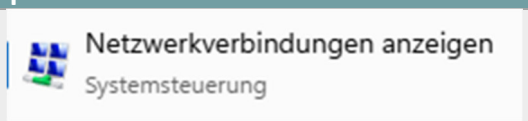
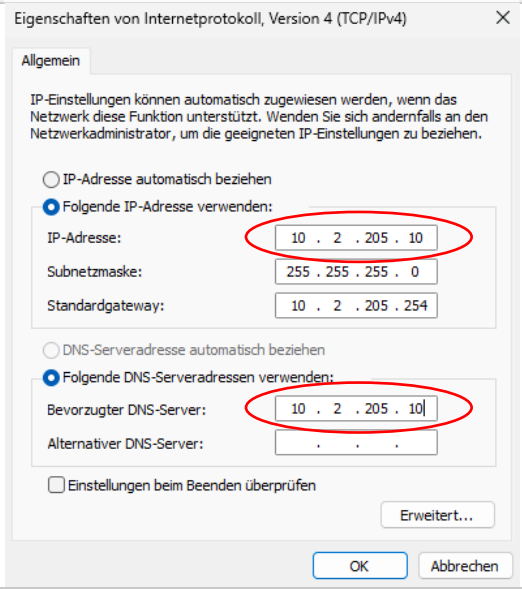
SRV-DC1

- Computername: SRV-DC1
- Statische IP: 10.2.205.10
- Subnetz: 255.255.255.0
- Gateway: 10.2.205.254
- DNS: 10.2.205.10
- **IPv6 Loopback (::1) entfernen!**

2.7.1 Computername vergeben/umbenennen

Erklärung	Beispiel
re. Maustaste → Start → **System**→ Diesen PC umbenennen	
neuer Name: SRV-DC1 **NEUSTART durchführen!**	

2.7.2 Statische IP des Servers einstellen

Erklärung	Beispiel
öffnen der Netzwerkverbindungen	
re. Maustaste → Eigenschaften→**IPv4** **Eintragung der gewünschten Adressierung und Subnetzmaske** **sowie als bevorzugten DNS-Server** → auf sich selber zeigen lassen!	

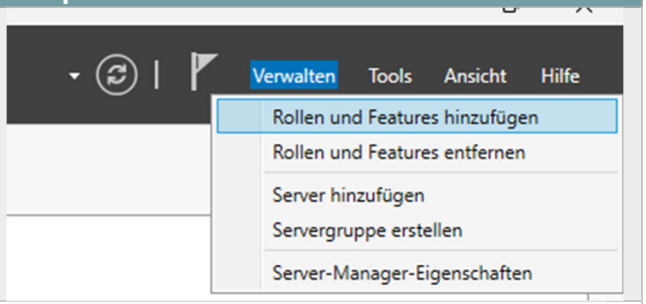
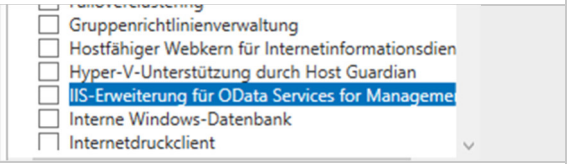
3. Ausgangszustand

- Beide virtuellen Maschinen sind installiert.
- Der Server ist noch kein Domänencontroller
- Hostname am Server geändert.
- Der Client ist noch kein Domänenmitglied.
- Netzwerkadapter sind eingerichtet, IP-Adressen statisch gesetzt.

Dieser Zustand bildet die Ausgangsbasis für die folgenden Konfigurationsschritte.

4. Installation der Rollen

4.1 DNS-Server installieren

Erklärung	Beispiel
Im Server-Manager unter „Verwalten“ → Rollen und Features hinzufügen auswählen. **Darauf hin öffnet sich ein Assistent zum Hinzufügen von Rollen und Features.**	
Die erste Auswahl muss bei den Serverrollen gemacht werden→ Haken bei DNS-Server →Features hinzufügen **Weiter**	
im Zuge dessen kann auch gleich die IIS-Erweiterung mit installiert werden. **Weiter bis zur Bestätigung →** Installieren	
Wenn fertig installiert, so erscheint unter Tools das entsprechende Feature und kann so verwaltet werden.	NEUSTART durchgeführt!

Oder per Powershell

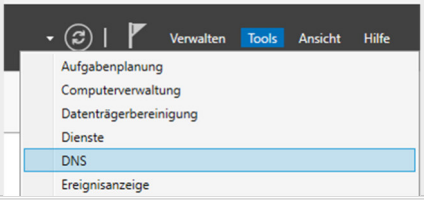
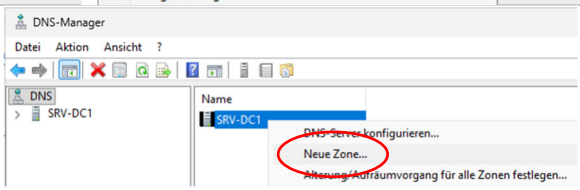
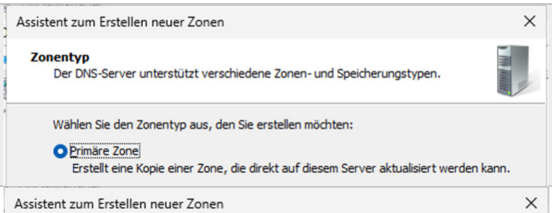
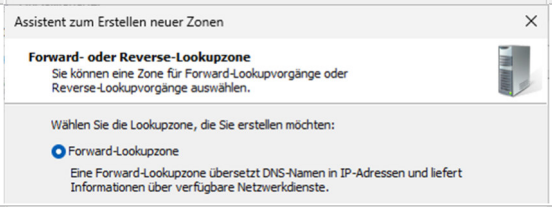
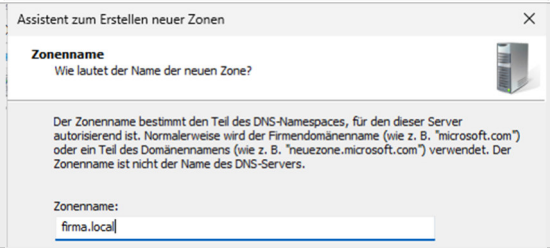
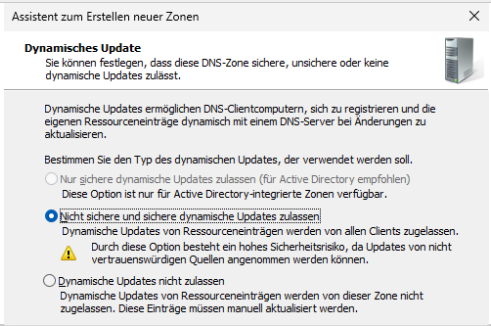
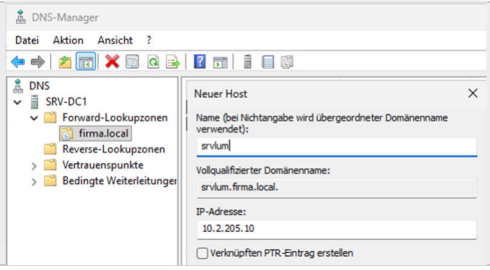
Beschreibung	PowerShell-Befehl
DNS mit Admin-Tools installieren	`Install-WindowsFeature DNS -IncludeManagementTools`

4.2 AD-Domain Controller erstellen

- Neue Gesamtstruktur
- Domänenname: schule.local
- DSRM-Kennwort: Sicher!2025
- Nach Neustart per CMD prüfen
- Standardserver: srv.schule.local

4.2.1 Einrichten einer Forward-Lookupzone im DNS

Erklärung	Beispiel

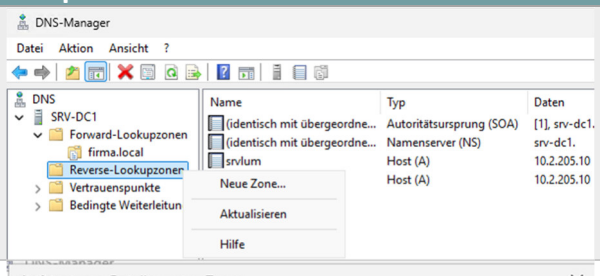
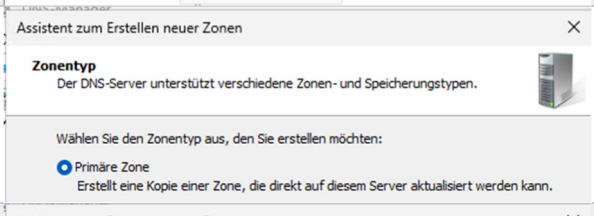
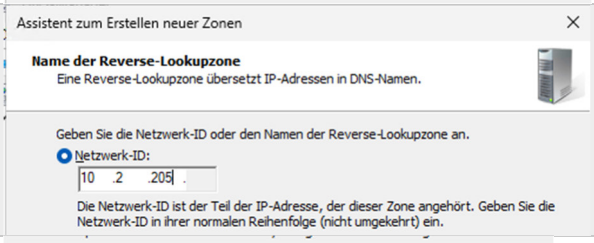
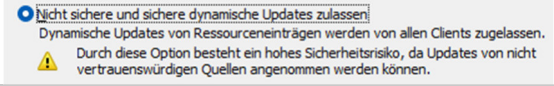
Im Server-Manager unter „Tools“ **➔ „DNS“ auswählen** **Daraufhin öffnet sich der DNS-Manager**	
re. Maustaste auf den Server-Namen und „Neue Zone“ erstellen **Daraufhin startet der Assistent zum Erstellen neuer Zonen…**	
Auswahl: primäre Zone **Weiter**	
Auswahl: Forward-Lookupzone **Weiter**	
Eingabe: z.B.: schule.local **Weiter** →neue Datei mit diesem Dateinamen erstellen? **→Weiter**	
Auswahl: Nicht sichere und sichere dynamische Updates zulassen. **es folgt eine Zusammenfassung…. Fertig stellen!**	
nun noch einen A-Record im DNS erstellen. **Dazu re. Maustaste auf die Domäne und „neuer Host (A oder AAAA)… auswählen.** **Namen eingeben und die IP des Servers:**	
Wozu dient dieser A-Record? Wenn jemand im Netzwerk srvlum.firma.local fragt, antworte mit IP 10.2.205.10	
zum Erzwingen des Eintrages im CMD eingeben	ipconfig /registerdns

Erklärung	PowerShell-Befehl

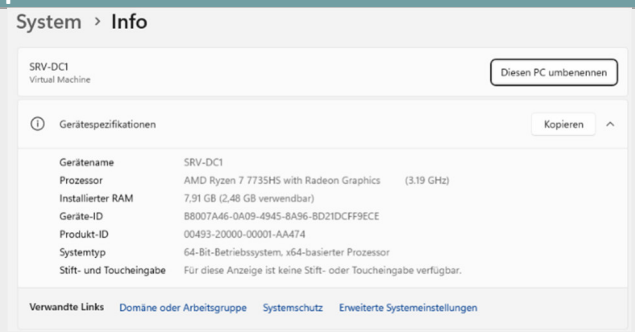
Primäre DNS-Zone schule.local erstellen	`Add-DnsServerPrimaryZone -Name "schule.local" -ZoneFile "schule.local.dns" -DynamicUpdate None -PassThru`
Nicht sichere + sichere Updates	`Set-DnsServerPrimaryZone -Name "schule.local" -DynamicUpdate NonsecureAndSecure`

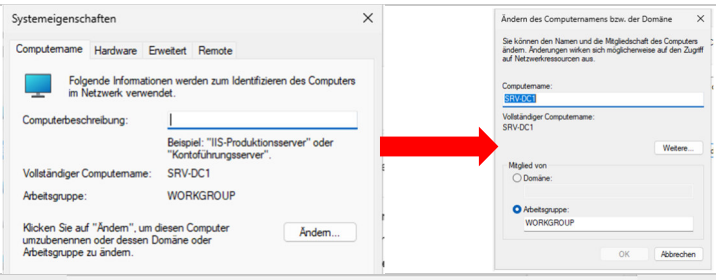
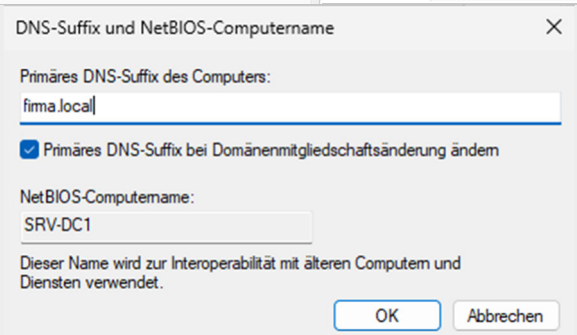
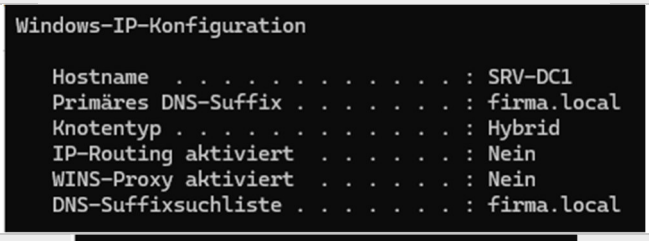
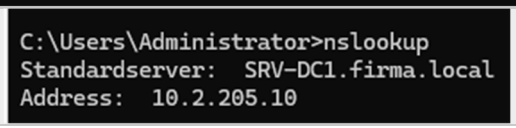
4.2.2 Einrichten einer Reverse-Lookupzone im DNS

- Reverse Lookup Zone erstellen für 10.2.205.x
- Dynamische Updates zulassen

Erklärung	Beispiel
wir befinden uns bereits im DNS-Manager und öffnen mit einem Rechtsklick auf „Reverse-Lookupzonen“ → Neue Zone **Daraufhin öffnet sich wieder der Assistent zum Erstellen neuer Zonen…**	
Auswahl: primäre Zone **dann IPv4 Reverse-Lookupzone**	
dann die ersten 3 Oktete des IP-Bereiches eingeben in dem Server sich befindet! **WEITER** **WEITER**	
Bei den update → **Weiter und Fertig stellen**	

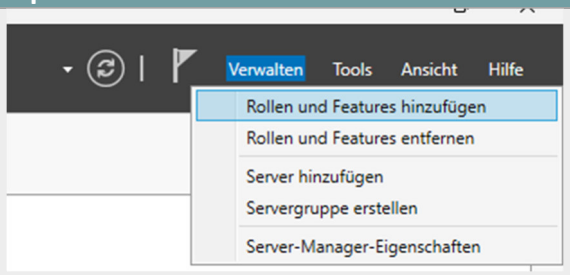
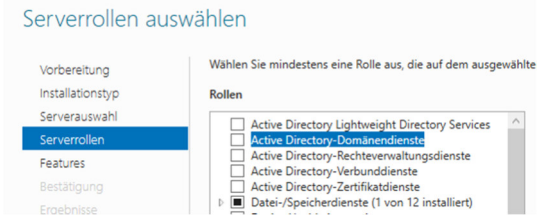
4.2.3 Server einer Domäne hinzufügen

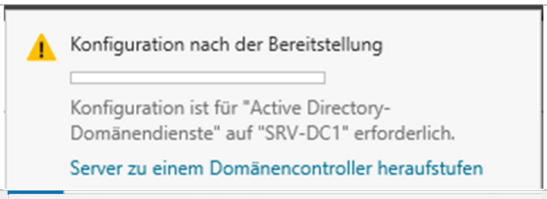
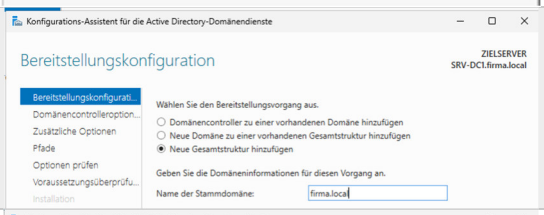
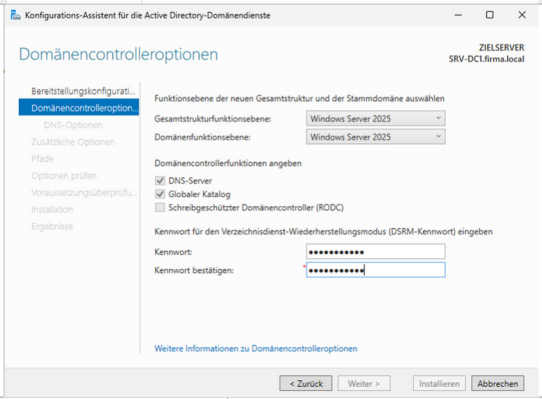
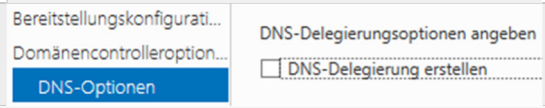
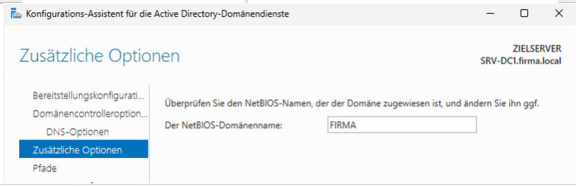
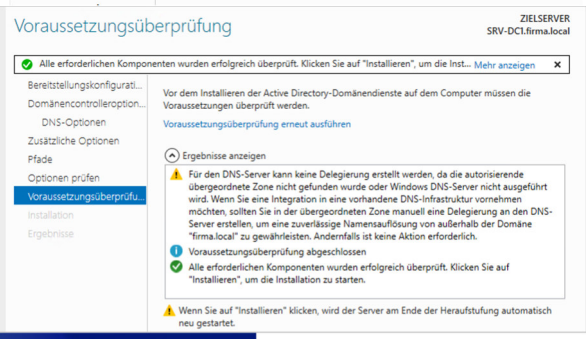
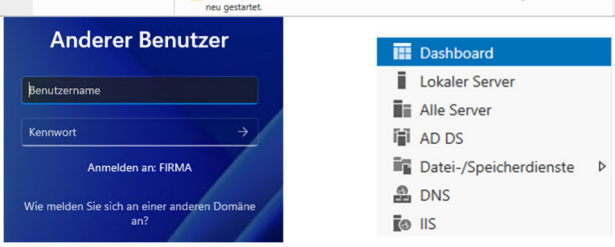
Erklärung	Beispiel
re. Maustaste→ Start ➔ **System** ➔ **Domäne oder Arbeitsgruppe**	

Systemeigenschaften ➔ **Ändern** ➔ **weitere**	
Eintrag „schule.local“ als primäres DNS-Suffix **OK** → Computer muss neu gestartet werden!	
nach dem Neustart → schule.local ➔ **ipconfig /all**	
`nslookup`	

5. Active-Directory

5.1 Active Directory-Domänendienst installieren

Erklärung	Beispiel
Im Server-Manager unter „Verwalten“ → Rollen und Features hinzufügen auswählen. **Darauf hin öffnet sich ein Assistent zum Hinzufügen von Rollen und Features.**	
Die erste Auswahl muss bei den Serverrollen gemacht werden → Haken bei „Active-Directory-Domänendienst“ **es öffnet sich der Assistent zum Hinzufügen…**	
keine zusätzlichen Eingaben bis zum Start der Installation notwendig.	

Als nächsten Schritt muss der Server zum Domänencontroller hochgestuft werden…	
Der Server soll der bestehenden Domäne „schule.local“ hinzugefügt werden.	
DSRM-Kennwort: Sicher!2025	
DNS-Delegierung NICHT anhaken	
auch hier braucht nichts geändert werden.	
Alle erforderlichen Komponenten wurden erfolgreich überprüft…. **Installieren** →Rechner startet von selbst neu	
neue, geänderte Anmeldemaske…. **Administrator** **Aa_123456** **Installation erfolgreich!**	

6. Dateidienste- AD-Benutzer-Gruppen, Dateifreigaben und Berechtigungen

6.1 Active Directory – Organisationsstruktur erstellen

Erklärung	PowerShell-Befehl
OU „Schueler“ anlegen	`New-ADOrganizationalUnit -Name "Schueler" -Path "DC=schule,DC=local"`
OU „Lehrer“ anlegen	`New-ADOrganizationalUnit -Name "Lehrer" -Path "DC=schule,DC=local"`
Gruppe „Schueler“ erstellen	`New-ADGroup -Name "Schueler" -GroupScope Global -GroupCategory Security -Path "OU=Schueler,DC=schule,DC=local"`
Gruppe „Lehrer“ erstellen	`New-ADGroup -Name "Lehrer" -GroupScope Global -GroupCategory Security -Path "OU=Lehrer,DC=schule,DC=local"`

6.2 Active Directory – Benutzer anlegen

Erklärung	PowerShell-Befehl
Benutzer schueler1 erstellen	`New-ADUser -Name "schueler1" -SamAccountName "schueler1" -Path "OU=Schueler,DC=schule,DC=local" -AccountPassword (ConvertTo-SecureString "Passwort!" -AsPlainText -Force) -Enabled $true`
Benutzer schueler2 erstellen	`New-ADUser -Name "schueler2" -SamAccountName "schueler2" -Path "OU=Schueler,DC=schule,DC=local" -AccountPassword (ConvertTo-SecureString "Passwort!" -AsPlainText -Force) -Enabled $true`
Benutzer lehrer1 erstellen	`New-ADUser -Name "lehrer1" -SamAccountName "lehrer1" -Path "OU=Lehrer,DC=schule,DC=local" -AccountPassword (ConvertTo-SecureString "Passwort!" -AsPlainText -Force) -Enabled $true`

6.3 Gruppenmitgliedschaften setzen

Erklärung	PowerShell-Befehl
Schüler den Schüler-Benutzern zuweisen	`Add-ADGroupMember -Identity "Schueler" -Members "schueler1","schueler2"`
Lehrer der Lehrer-Gruppe zuweisen	`Add-ADGroupMember -Identity "Lehrer" -Members "lehrer1"`

6.4 Fileserver-Rolle installieren

Erklärung	PowerShell-Befehl
Fileserver-Rolle installieren	`Fileserver-Rolle installieren`

6.5 Ordnerstruktur erstellen

Erklärung	PowerShell-Befehl
Ordner C:\Schueler erstellen	`New-Item -ItemType Directory -Path "C:\Schueler" -Force`

Ordner C:\Lehrer erstellen	`New-Item -ItemType Directory -Path "C:\Lehrer" -Force`
Ordner C:\Public erstellen	`New-Item -ItemType Directory -Path "C:\Public" -Force`

6.6 NTFS-Berechtigungen setzen

Erklärung	PowerShell-Befehl
Vererbung bei C:\Schueler deaktivieren	`icacls "C:\Schueler" /inheritance:r`
Schüler Vollzugriff ändern (Modify)	`icacls "C:\Schueler" /grant "SCHULE\Schueler:(OI)(CI)(M)"`
Domänen-Admins Vollzugriff	`icacls "C:\Schueler" /grant "SCHULE\Domänen-Admins:(OI)(CI)(F)"`
SYSTEM Vollzugriff	`icacls "C:\Schueler" /grant "SYSTEM:(OI)(CI)(F)"`
Vererbung bei C:\Lehrer deaktivieren	`icacls "C:\Lehrer" /inheritance:r`
Lehrer Vollzugriff	`icacls "C:\Lehrer" /grant "SCHULE\Lehrer:(OI)(CI)(F)"`
Domänen-Admins Vollzugriff	`icacls "C:\Lehrer" /grant "SCHULE\Domänen-Admins:(OI)(CI)(F)"`
SYSTEM Vollzugriff	`icacls "C:\Lehrer" /grant "SYSTEM:(OI)(CI)(F)"`
Vererbung bei C:\Public deaktivieren	`icacls "C:\Public" /inheritance:r`
Jeder Leserechte	`icacls "C:\Public" /grant "Jeder:(OI)(CI)(RX)"`
Domänen-Admins Vollzugriff	`icacls "C:\Public" /grant "SCHULE\Domänen-Admins:(OI)(CI)(F)"`
SYSTEM Vollzugriff	`icacls "C:\Public" /grant "SYSTEM:(OI)(CI)(F)"`

6.7 SMB-Freigaben erstellen

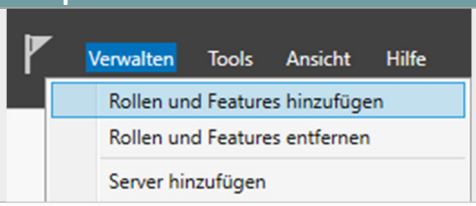
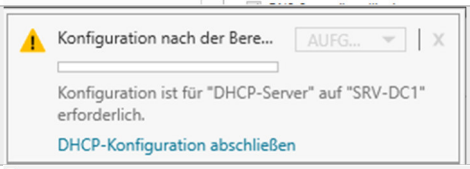
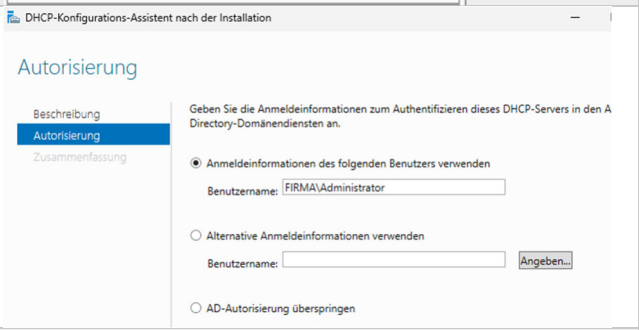
Erklärung	PowerShell-Befehl
Share „Schueler“ erstellen	`New-SmbShare -Name "Schueler" -Path "C:\Schueler"`
Share „Lehrer“ erstellen	`New-SmbShare -Name "Lehrer" -Path "C:\Lehrer"`
Share „Public“ erstellen	`New-SmbShare -Name "Public" -Path "C:\Public"`

6.8 Share-Berechtigungen setzen

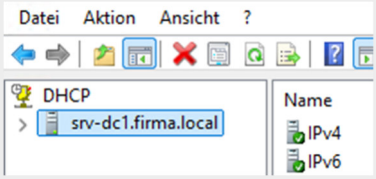
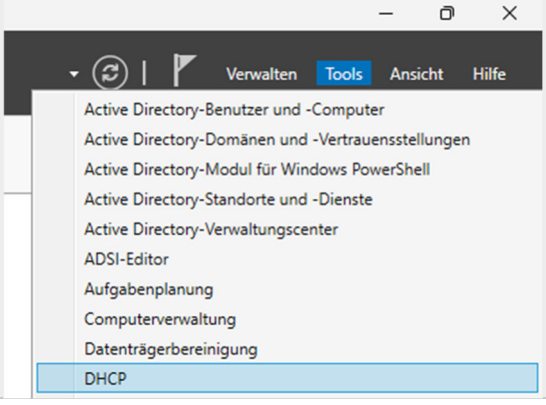
Erklärung	PowerShell-Befehl
Standardzugriff „Jeder“ bei Schueler entfernen	`Revoke-SmbShareAccess -Name "Schueler" -AccountName "Jeder" -Force`
Standardzugriff „Jeder“ bei Lehrer entfernen	`Revoke-SmbShareAccess -Name "Lehrer" -AccountName "Jeder" -Force`
Schülergruppe Änderungsrechte	`Grant-SmbShareAccess -Name "Schueler" -AccountName "SCHULE\Schueler" -AccessRight Change -Force`
Lehrergruppe Vollzugriff	`Grant-SmbShareAccess -Name "Lehrer" -AccountName "SCHULE\Lehrer" -AccessRight Full -Force`
Öffentlicher Share Leserechte für alle	`Grant-SmbShareAccess -Name "Public" -AccountName "Jeder" -AccessRight Read -Force`

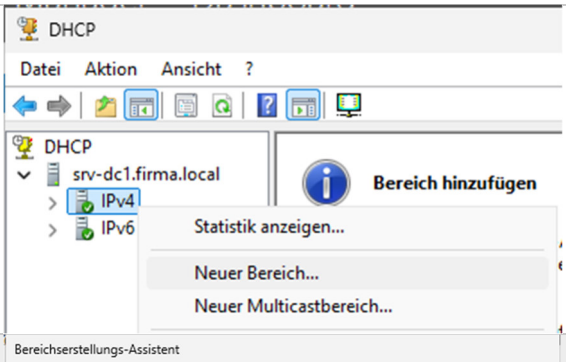
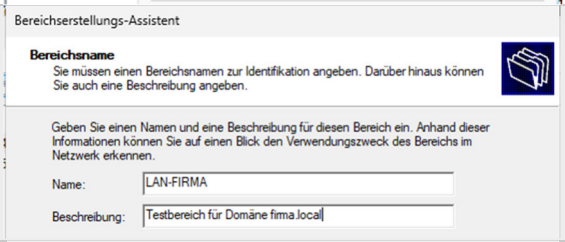
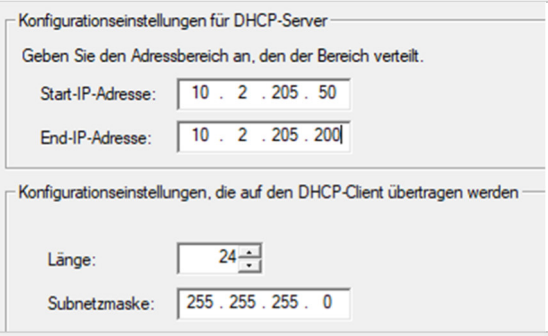
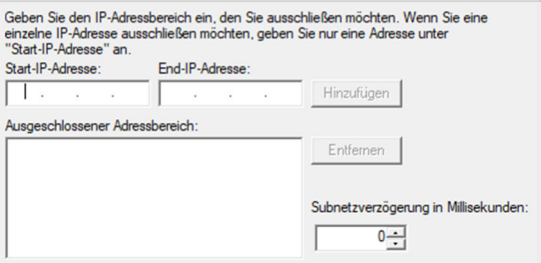
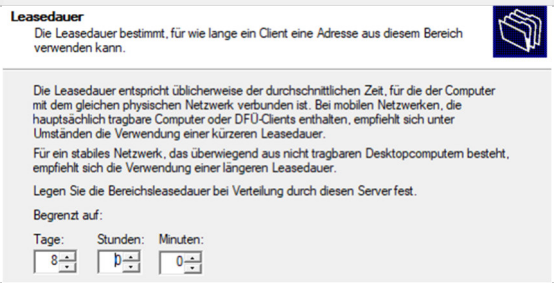
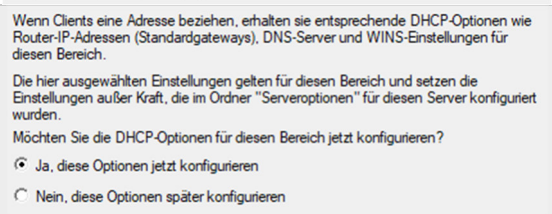
7. DHCP

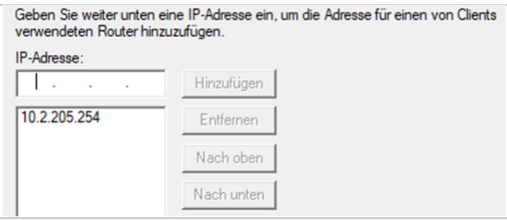
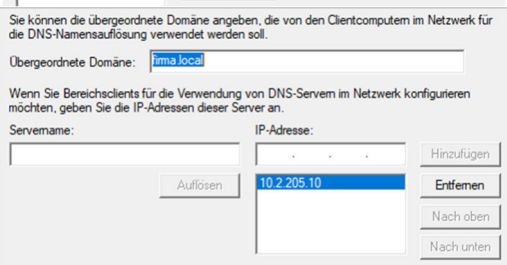
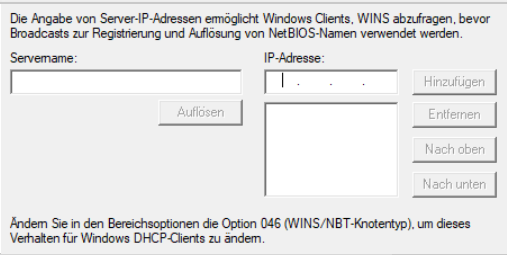
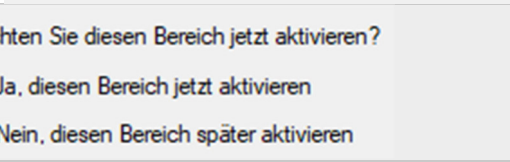
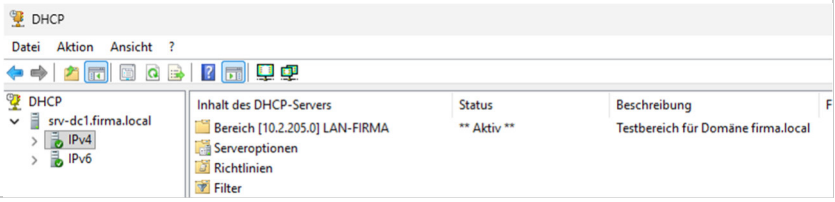
7.1 DHCP-Rolle installieren

Erklärung	Beispiel
Unter „Verwalten“→Rollen und Features hinzufügen…	
Auswahl der Rolle „DHCP-Server“ **weiter, weiter, weiter** →Installieren	
wurde die Rolle/Dienst installiert so erscheint rechts oben ein gelbes Rufzeichen!	
es erscheint erneut ein Assistent zur DHCP-Konfiguration →keine Änderungen →Commit… →Schließen/fertig	
NEUSTART durchführen!!	

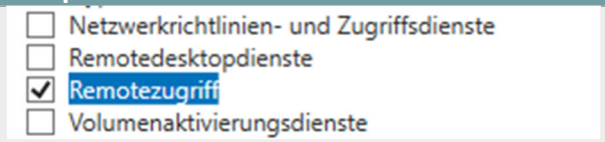
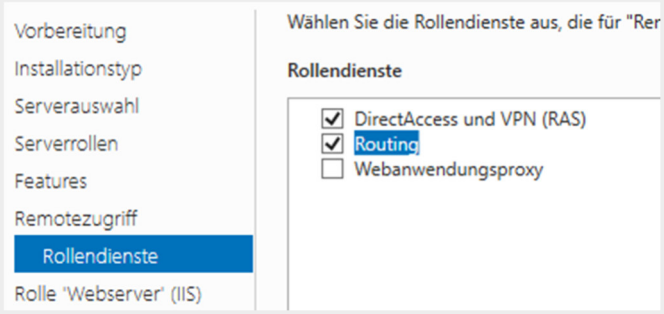
7.2 Neuen DHCP-Bereich erstellen

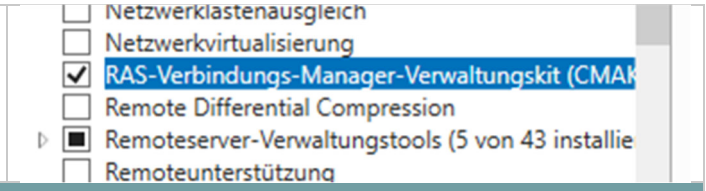
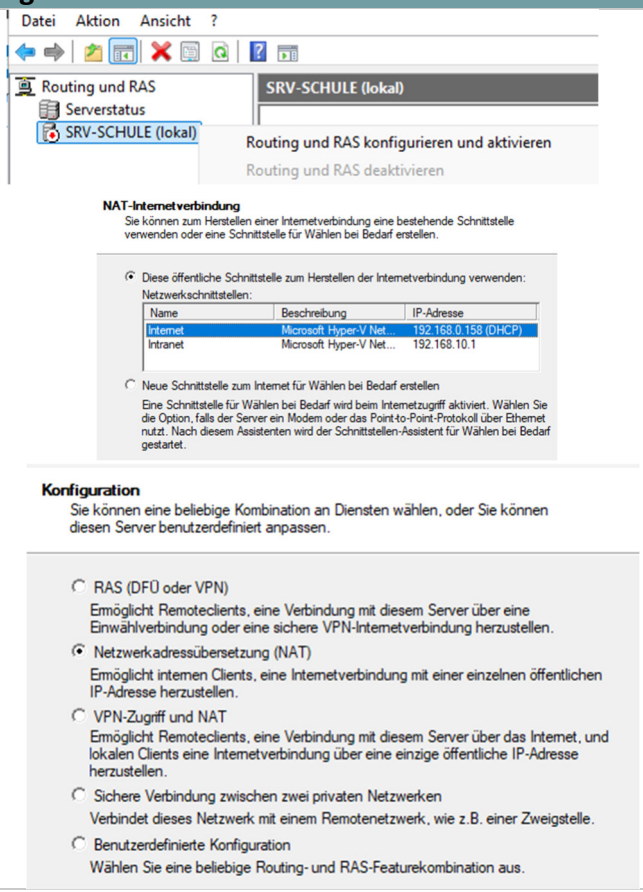
Erklärung	Beispiel
Im Server-Manager unter „tools“ wird DHCP geöffnet. **Daraufhin öffnet sich eine Oberfläche in der unser Server erscheint.** **rechts davon ist IPv4**→re. MT→ 	

→Neuer Bereich→**Bereichserstellungsassistent öffnet sich→**	
Im Feld Name tragen wir den gewünschten Bereichsnamen ein: z.B.: LAN-FIRMA **Bei Beschreibung: Um was es sich handelt** **Weiter**	
im nächsten Fenster tragen wir den gewünschten Adressbereich ein in dem der Server IP-Adressen vergeben soll. **und die Subnetzmaske nicht vergessen!** **Weiter**	
möchte Man innerhalb des DHCP-Pools nochmals Adressen ausschließen so kann man es hier tun… wir machen es nicht! **Weiter**	
im nächsten Fenster kann man noch die Lease-Dauer der Clients verändert wenn man möchte… wir bleiben bei 8 Tage! **Weiter**	
dann kommen wir zu den DHCP-Optionen, wo wir einstellen können was alles für Informationen an die Clients ausgeliefert werden soll…. **→Ja, diese Optionen jetzt konfigurieren!**	

als nächstes geben wir die IP-Adresse unseres Gateways ein: 10.2.205.254 in unserem Fall! →hinzufügen →Weiter	
Da wir bereits im Vorfeld den DNS aktiviert haben können wir dieses Fenster ohne Änderungen übernehmen… **Weiter**	
Auch beim nächsten Fenster (WINS-Server) brauchen keine Änderungen gemacht werden… **Weiter**	
zum Abschluss werden wir gefragt ob wir den Bereich aktivieren möchten →JA **Weiter & Fertigstellen**	
aktiver DHCP-Bereich	

8. Routing und RAS (RRAS)

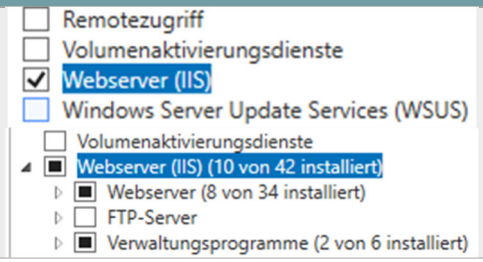
Erklärung	Beispiel
Server-Manager öffnen **Rollen und Features hinzufügen** **Rolle auswählen: Remotezugriff** **Unter Rollendienste anhaken:** **Routing** **RAS (Remote Access Service)** **Optional: DirectAccess und VPN (RAS) falls VPN benötigt wird**	 

Installation abschließen **Nach der Installation erscheint im Server-Manager das Tool Routing und RAS.**	
Konfiguration	
Routing und RAS Konsole öffnen **Rechtsklick auf den Servernamen** **Routing und RAS konfigurieren und aktivieren** **Der Assistent startet**→BUG! Assistent schließen und erneut starten dann erscheinen auch die Netzwerkschnittstellen **wir möchten hier „NAT“ um unseren Clients ins Internet zu bringen** 👉 **Installieren**	

9. IIS (Webserver)

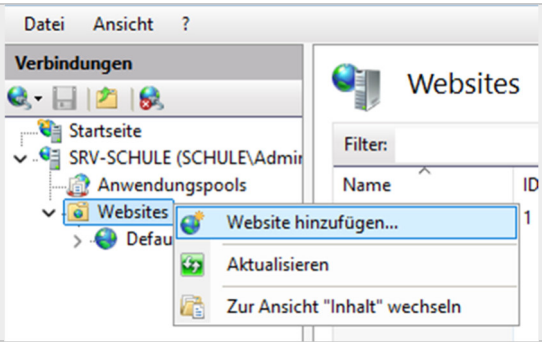
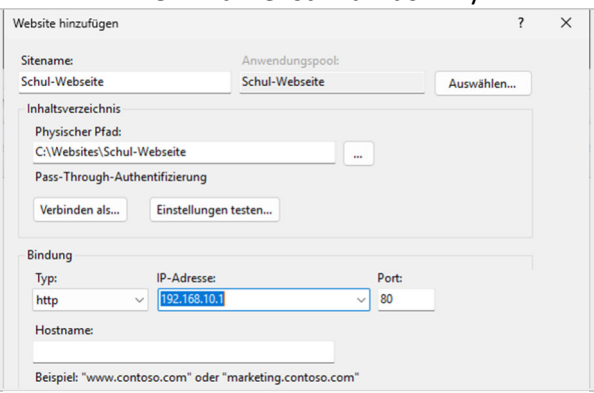
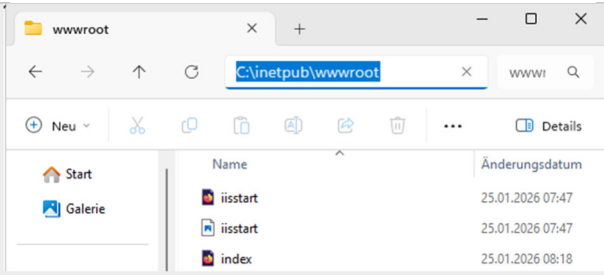
Zur Aktivierung/Installation des Dienstes

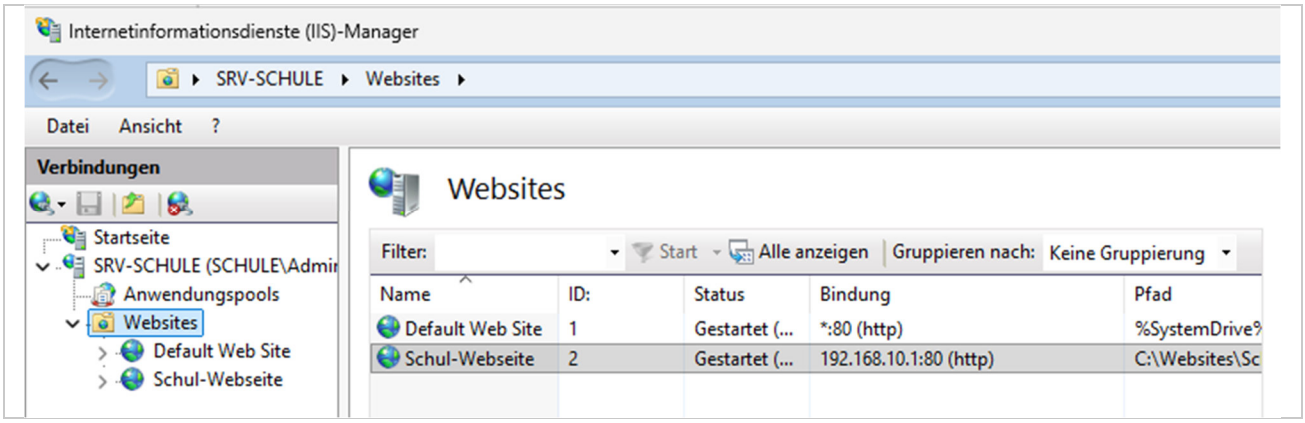
Verwalten→Rollen und Features hinzufügen!

Erklärung	Beispiel
Unter **„Serverrollen“**→ Webserver (IIS) auswählen INFO: Hier kann, wenn notwendig auch gleich ein **FTP-Server** mit installiert werden!	
Bei Rollendienste keine zusätzliche Auswahl notwendig, bzw. auch hier nochmals die Möglichkeit den FTP oder zusätzliche Dienste zu aktivieren. →Bestätigung und Installieren	

Per Powershell: `Install-WindowsFeature -name Web-Server -IncludeManagementTools`	

9.1 Basis-Konfiguration IIS (Webserver)

Erklärung	Beispiel
Unter Tools→**Internetinformationsdienst (IIS)-Manager** öffnen	
Standard-Website: Überprüfen Sie, ob die Standard-Website funktioniert, indem Sie in einem Browser zu **http://localhost** navigieren.	
Website hinzufügen Klicken Sie mit der rechten Maustaste auf Websites > Website hinzufügen, geben Sie einen Namen, einen physischen Pfad und einen Hostnamen an.	
Inhalt der index.html	Willkommen an der Schule 🎉 Mein Name ist Markus L.
Speichern der index.html in einem eigenen Verzeichnis: **C:\Websites\Schul-Webseite** **Auswahl der Server-IP** ➔ **Fertig!**	
http://schule.local/ **oder** http://localhost/	
ALTERNATIVE: **die index.html in den 📂Ordner** **C:\inetpub\wwwroot** **speichern**	



10. FTP-Server (über IIS)

ein FTP-Verzeichnis für eine Gruppe wie z.B.: GG_Lehrer

Erklärung	Powershell-Befehl
IIS-Verwaltungsmodul laden (macht IIS-Befehle verfügbar)	`Import-Module WebAdministration`
FTP-Site erstellen	`New-WebFtpSite -Name "Lehrer-FTP" -IPAddress "*" -Port 21`
FTP-Ordner anlegen	`New-Item -ItemType Directory -Path "C:\Lehrer" -Force`
Ordner der FTP-Site zuweisen	`Set-ItemProperty "IIS:\Sites\Lehrer-FTP" -Name physicalPath -Value "C:\Lehrer"`
Unverschlüsseltes FTP auf Steuerkanal erlauben	`Set-ItemProperty "IIS:\Sites\Lehrer-FTP" -Name ftpServer.security.ssl.controlChannelPolicy -Value "SslAllow"`
Unverschlüsseltes FTP auf Datenkanal erlauben	`Set-ItemProperty "IIS:\Sites\Lehrer-FTP" -Name ftpServer.security.ssl.dataChannelPolicy -Value "SslAllow"`
Basic-Authentifizierung aktivieren	`Set-ItemProperty "IIS:\Sites\Lehrer-FTP" -Name ftpServer.security.authentication.basicAuthentication.enabled -Value $true`
Alte FTP-Zugriffsregeln löschen	`Clear-WebConfiguration -PSPath "IIS:\" -Location "Lehrer-FTP" -Filter "/system.ftpServer/security/authorization"`
Neue Zugriffsregel setzen (Lehrer Read+Write)	`Add-WebConfiguration -PSPath "IIS:\" -Location "Lehrer-FTP" -Filter "/system.ftpServer/security/authorization" -Value @{accessType="Allow";roles="SCHULE\Lehrer";permissions="Read,Write"}`
Interne/externe FTP-IP setzen	`Set-ItemProperty "IIS:\Sites\Lehrer-FTP" -Name ftpServer.firewallSupport.externalIp4Address -Value "192.168.10.1"`
NTFS-Rechte auf Ordner vergeben	`icacls "C:\Lehrer" /grant "SCHULE\Lehrer:(OI)(CI)(M)"`
FTP-Site neu starten	`Restart-WebItem -PSPath "IIS:\Sites\Lehrer-FTP"`
Prüfen ob Site läuft	`Get-WebSite -Name "Lehrer-FTP"`
PS-Skript (ISE)	
# --- Variablen ---	

```
$DomainNetBIOS = "SCHULE"
$GroupName     = "Lehrer"
$GroupRole     = "$DomainNetBIOS\$GroupName"   # SCHULE\Lehrer

$SiteName      = "Lehrer-FTP"
$PhysicalDir   = "C:\Lehrer"
$ExternalIP    = "192.168.10.1"
$Port          = 21

# --- 0) IIS WebAdministration laden (falls nicht automatisch geladen) ---
Import-Module WebAdministration -ErrorAction Stop

# --- 1) FTP-Site anlegen (nur wenn sie noch nicht existiert) ---
if (-not (Test-Path "IIS:\Sites\$SiteName")) {
    New-WebFtpSite -Name $SiteName -IPAddress "*" -Port $Port
} else {
    Write-Host "FTP-Site '$SiteName' existiert bereits -> überspringe New-WebFtpSite"
}

# --- 2) FTP-Verzeichnis erstellen und zuweisen ---
New-Item -ItemType Directory -Path $PhysicalDir -Force | Out-Null
Set-ItemProperty "IIS:\Sites\$SiteName" -Name physicalPath -Value $PhysicalDir

# --- 3) Unverschlüsseltes FTP erlauben (SSL/TLS optional, nicht erzwungen) ---
Set-ItemProperty "IIS:\Sites\$SiteName" -Name ftpServer.security.ssl.controlChannelPolicy -Value "SslAllow"
Set-ItemProperty "IIS:\Sites\$SiteName" -Name ftpServer.security.ssl.dataChannelPolicy   -Value "SslAllow"

# --- 4) Basic Authentication aktivieren ---
Set-ItemProperty "IIS:\Sites\$SiteName" -Name ftpServer.security.authentication.basicAuthentication.enabled -Value
$true

# --- 5) FTP Authorization: vorhandene Regeln löschen, dann genau eine saubere Regel setzen ---
Clear-WebConfiguration -PSPath "IIS:\" -Location $SiteName -Filter "/system.ftpServer/security/authorization"
Add-WebConfiguration   -PSPath "IIS:\" -Location $SiteName -Filter "/system.ftpServer/security/authorization" `
    -Value @{accessType="Allow";roles=$GroupRole;permissions="Read,Write"}

# --- 6) External IP (hier interne IP wie gewünscht) ---
Set-ItemProperty "IIS:\Sites\$SiteName" -Name ftpServer.firewallSupport.externalIp4Address -Value $ExternalIP

# --- 7) NTFS-Rechte: Domänengruppe auf C:\Lehrer (Modify) ---
# Wichtig: ${GroupRole} wegen Doppelpunkt in icacls-String
icacls $PhysicalDir /grant "${GroupRole}:(OI)(CI)(M)" | Out-Null

# --- 8) FTP-Site neu starten ---
Restart-WebItem -PSPath "IIS:\Sites\$SiteName"

Write-Host "Fertig. FTP-Site '$SiteName' zeigt auf '$PhysicalDir' für Gruppe '$GroupRole'."
```

11. Serversicherung

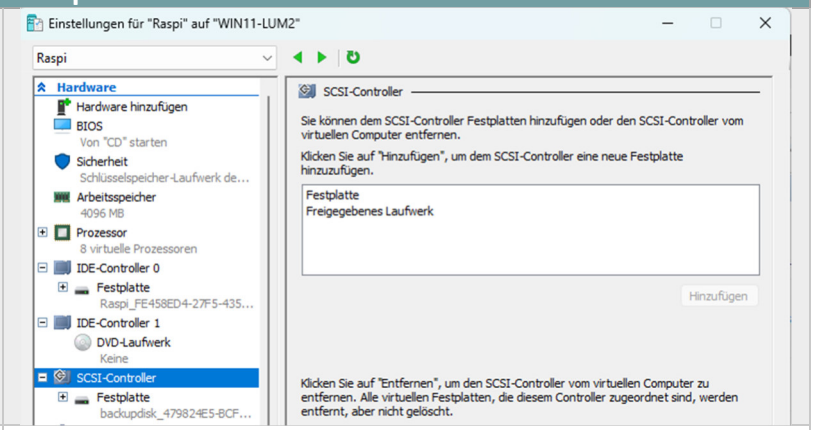
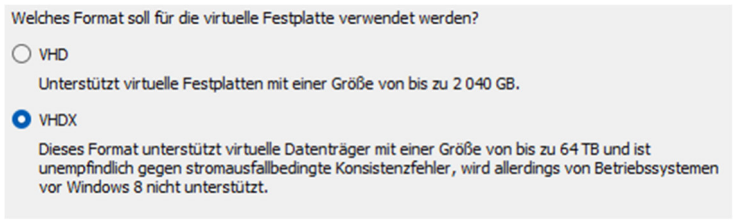
Windows Server Backup auf Raspberry Pi VM über iSCSI

Ein Windows Server (Domain Controller) sichert sich selbst automatisch auf eine virtuelle Festplatte, die von einer Raspberry-Pi-VM per iSCSI bereitgestellt wird.

Das Backup-Ziel erscheint für Windows als lokale Festplatte, wodurch keine SMB- oder Richtlinienprobleme auftreten.

11.1 Hyper-V: Zusätzliche Festplatte für Raspberry-Pi-VM erstellen

Am Hypervisor läuft eine Raspberry-PI-VM → 2022-07-01-raspios-bullseye-i386 die als Ziel für die Servsersicherung verwendet werden soll. Dazu muss ein zusätzliches Laufwerk erstellt werden um die Sicherungsdateien darauf abzulegen.

Beschreibung	Beispiel
Hyper-V-Manager → Einstellungen der **Raspberry-Pi-VM** SCSI-Controller → Festplatte → Hinzufügen	
Neue virtuelle Festplatte (VHDX) Dynamisch erweiterbar Namen und Größe festlegen (z. B. backupdisk, 500 GB) 👉 VM starten	

11.2 Grundinstallation Raspberry

Läuft ein Raspberry-Device (egal ob physisches Device oder als VM) so wird eine Grundinstallation benötigt um diverse Funktionen und Dienste zur Verfügung zu stellen.

11.2.1 System-update, SSH-Aktivierung, statische IP-Konfiguration

Beschreibung	Terminal-Befehl
System aktualisieren	`sudo apt update &&sud sudo apt upgrade -y`
Standard-Passwort ändern	`passwd`
SSH aktivieren	`sudo systemctl enable ssh`
Statische IP konfigurieren öffnen	`sudo nano /etc/dhcpcd.conf`

Nützen von nmcli um die Netzwerkeinstellungen zu konfigurieren…	`sudo nmcli connection modify "Wired connection 1" \`
	`ipv4.addresses 192.168.10.50/24 \`
	`ipv4.gateway 192.168.10.1 \`
	`ipv4.dns 192.168.10.1 \`
	`ipv4.method manual`

Neustart der Verbindung	`sudo nmcli connection down "Wired connection 1"` `sudo nmcli connection up "Wired connection 1"`

Testen der IPv4 Einstellungen	`nmcli device show | grep -A4 IP4`
Raspberry Pi neu starten	`sudo reboot`
IP-Adresse anzeigen	`hostname -I`

11.3 Raspberry Pi & Windows Server: Installationen der Funktionen & Dienste

11.3.1 Raspberry Pi: Neues Laufwerk finden, formatieren und einbinden

Beschreibung	Erklärung

Platte erkennen	lsblk → Ausgabe z.B.: sdb1 500G
	`administrator@raspberry:~ $ lsblk`
	`NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT`
	`fd0 2:0 1 4K 0 disk`
	`sda 8:0 0 127G 0 disk`
	`├─sda1 8:1 0 126G 0 part /`
	`├─sda2 8:2 0 1K 0 part`
	`└─sda5 8:5 0 975M 0 part [SWAP]`
	`sdb 8:16 0 500G 0 disk`
	`└─sdb1 8:17 0 500G 0 part /backupdisk`
	`sr0 11:0 1 1024M 0 rom`

Prüfen ob Dateisystem existiert	sudo blkid /dev/sdb1
Ausgabe	`administrator@raspberry:~ $ sudo blkid /dev/sdb1` `/dev/sdb1: UUID="09a36d23-8c2c-45ba-bc43-eae7ea469727" BLOCK_SIZE="4096" TYPE="ext4" PARTUUID="2788fc81-01"`
	Wenn TYPE angezeigt wird → Dateisystem vorhanden→OK
Wenn Ausgabe <u>nicht</u> so aussieht dann Dateisystem erstellen:	
Dateisystem erstellen	sudo mkfs.ext4 /dev/sda1
Partition anlegen mit fdisk	sudo fdisk /dev/sda1 → n → p → Enter → Enter → w
Mountpunkt erstellen	sudo mkdir /backupdisk sudo mount /dev/sda1 /backupdisk
Falsches Mount wieder lösen	sudo umount /backupdisk
Prüfen	df -h | grep backupdisk

so sollte die Ausgabe sein:	`administrator@raspberry:~ $ sudo mount /dev/sda1 /backupdisk`
	`administrator@raspberry:~ $ df -h | grep backupdisk`
	`/dev/sda1 492G 28K 467G 1% /backupdisk`

Wenn Dateisystem mit „Type“ angezeigt wird→in der fstab eintragen	(Optional: später in `/etc/fstab` eintragen)
öffnen der fstab mit nano→	sudo nano /etc/fstab

hier wie in der letzten Zeile die UUID….. genau so eintragen!	`# <file system> <mount point> <type> <options> <dump> <pass>`
	`# / was on /dev/sda1 during installation`
	`UUID=180321ab-42d1-407b-a863-9fb4b7a9fc17 / ext4 errors=remount-ro 0 1`
	`# swap was on /dev/sda5 during installation`
	`UUID=d0d262dc-ed75-4abf-a7ab-62af22c4f605 none swap sw 0 0`
	`/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0`
	`# a swapfile is not a swap partition, no line here`
	`# use dphys-swapfile swap[on|off] for that`
	`UUID=09a36d23-8c2c-45ba-bc43-eae7ea469727 /backupdisk ext4 defaults,noatime 0 2`

UUID=09a36d23-8c2c-45ba-bc43-eae7ea469727 /backupdisk ext4 defaults,noatime 0 2	

11.3.2 Raspberry Pi: Samba installieren & Backup-Freigabe erstellen

Erklärung	Terminal-Befehle
Samba installieren	`sudo apt install samba -y`
Samba-Benutzer anlegen	`sudo smbpasswd -a administrator`
Backup-Ordner erstellen	`sudo mkdir -p /backupdisk/backup`
Besitzer setzen	`sudo chown nobody:nogroup /backupdisk/backup`
Ordnerrechte setzen	`sudo chmod 777 /backupdisk/backup`
Samba-Konfiguration öffnen	`sudo nano /etc/samba/smb.conf`

Am Ende der Datei eintragen:	`[Backup]`
	`path = /backupdisk/backup`
	`browseable = yes`
	`writeable = yes`
	`create mask = 0777`
	`directory mask = 0777`
	`valid users = administrator`

Samba neu starten	`sudo systemctl restart smbd`
Vom Windows-Server (Explorer) Freigabe öffnen	\\192.168.10.50\Backup

11.3.3 Raspberry Pi: iSCSI-Target installieren

Ist der Mountpunkt am Raspi erstellt, kann der Dienst tgt installiert werden.

Beschreibung	Terminal-Befehle
Paket installieren	`sudo apt update` `sudo apt install tgt -y`
Target konfigurieren	`sudo nano /etc/tgt/conf.d/backupdisk.conf`

Einfügen in leere Datei:	`<target iqn.2024-01.local.schule:backupdisk>`
	`  backing-store /dev/sda1`
	`  initiator-address 192.168.10.1`
	`</target>`

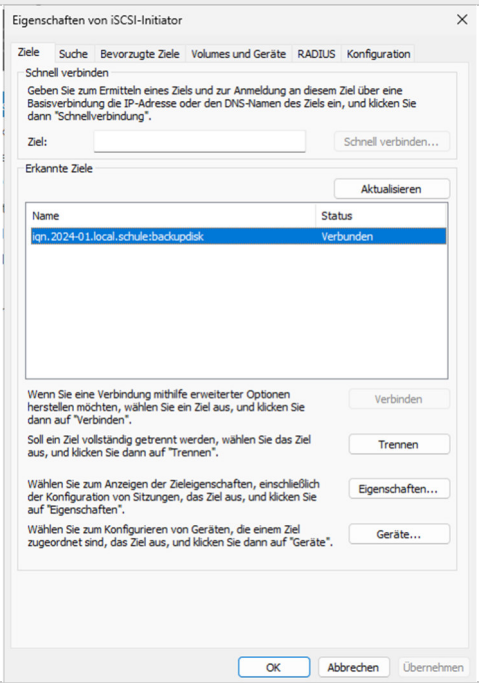
Dienst starten	`sudo systemctl restart tgt` `sudo systemctl enable tgt`
Status prüfen	`sudo tgtadm --mode target --op show`

Erwartet	`Target 1: iqn.2024-01.local.schule:backupdisk`
	`Backing store: /dev/sdb1`
	`ACL: 192.168.10.1`
	`State: ready`

11.3.4 Windows Server: iSCSI-Initiator verbinden

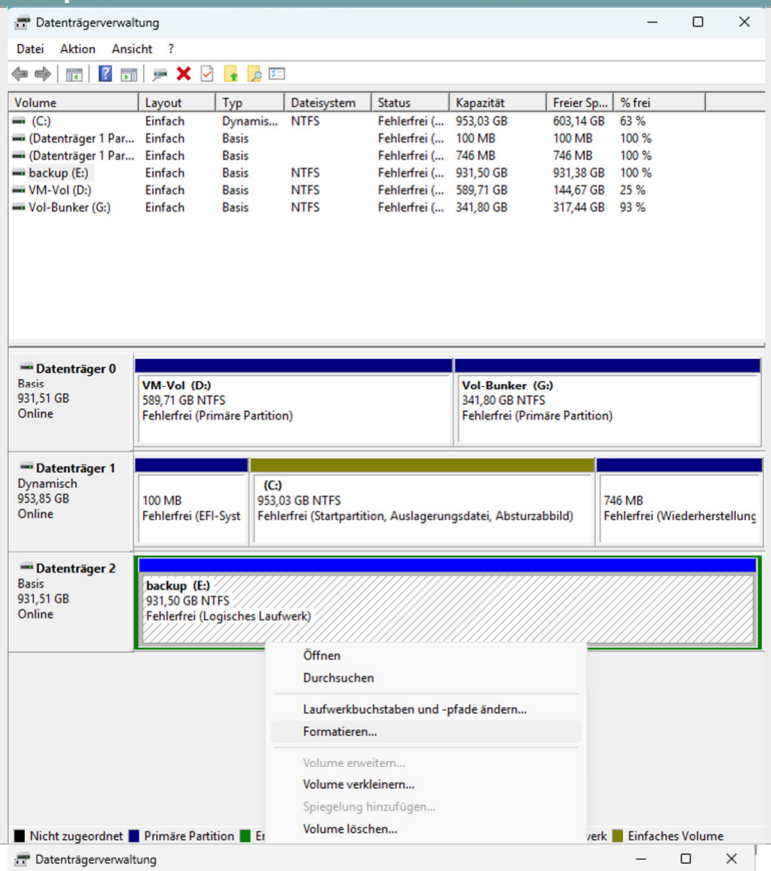
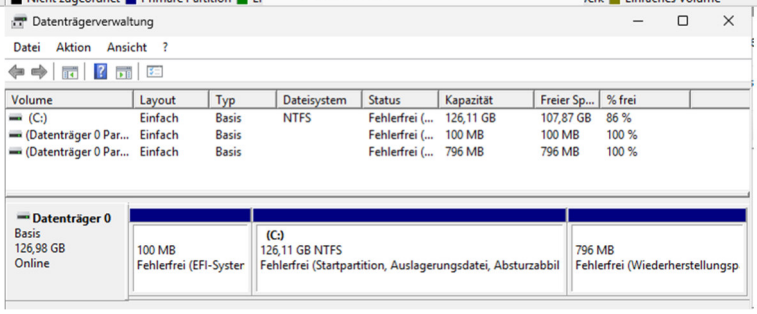
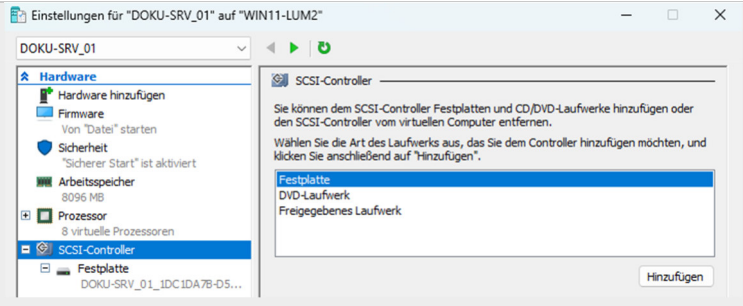
Der iSCSI-Initiator in Windows Server 2025 ist ein in das Betriebssystem integrierter Dienst, der es ermöglicht, über TCP/IP-Netzwerke auf entfernte, blockbasierte Speicherressourcen (iSCSI-Targets) zuzugreifen.

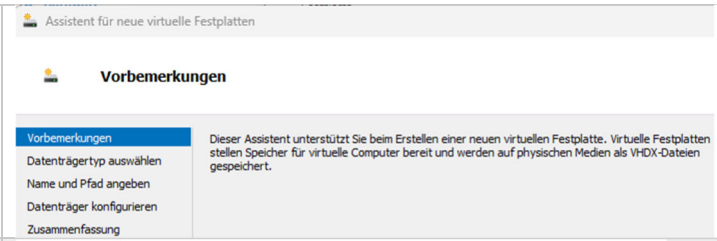
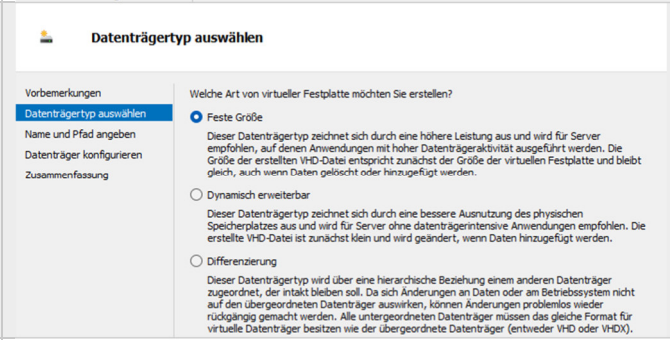
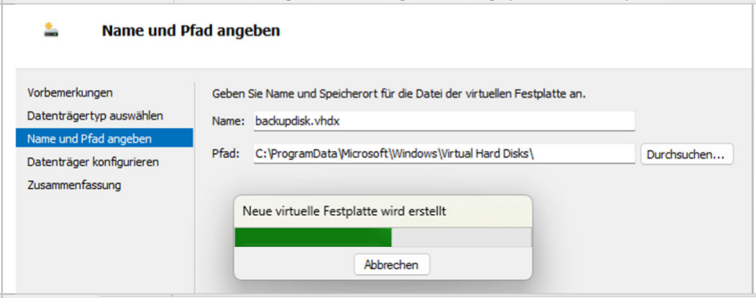
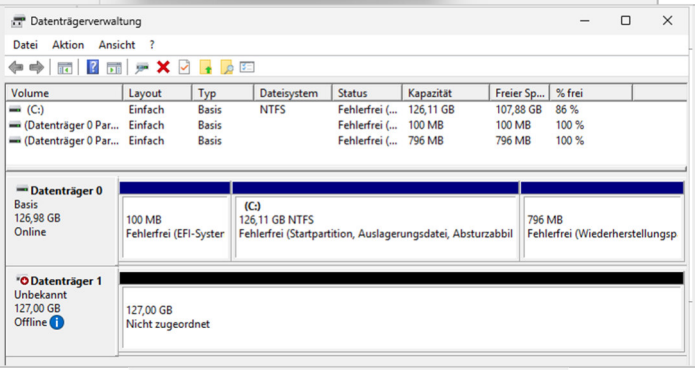
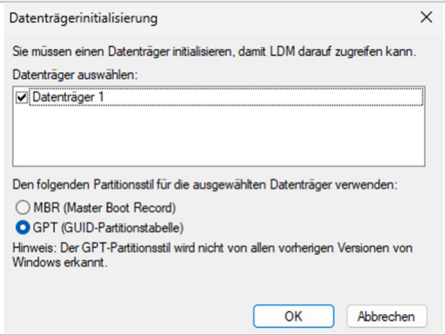
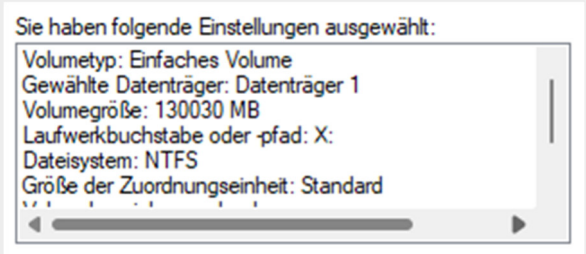
In unserem Fall möchten wir auf die Speicherressource am RASPBERRY-PI zugreifen um dort unser Backup zu speichern.

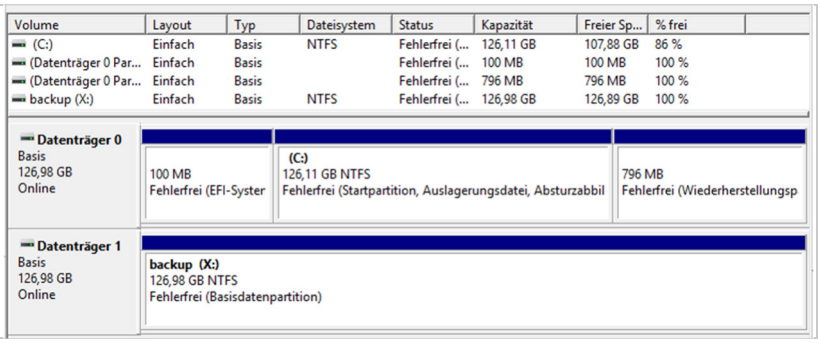
Beschreibung	PowerShell-Befehl
Dienst prüfen	`New-IscsiTargetPortal -TargetPortalAddress 192.168.10.103 -TargetPortalPortNumber 3260`
Target abfragen	`Get-IscsiTarget`
Erwartet:	`iqn.2024-01.local.schule:backupdisk`
Target verbinden (persistent)	`Connect-IscsiTarget -NodeAddress "iqn.2024-01.local.schule:backupdisk" -IsPersistent $true`
Verbindung prüfen	`Get-IscsiSession`
auch über eine grafische Oberfläche hat man die Möglichkeit zu konfigurieren.	

11.3.5 Windows Server: Neue Festplatte in Windows initialisieren

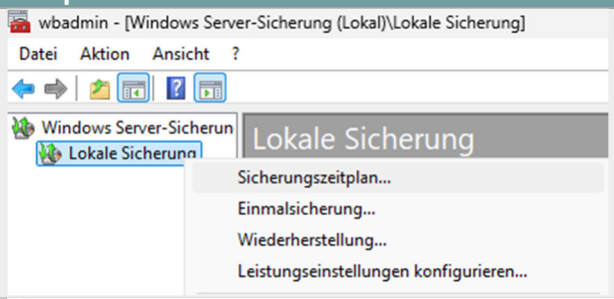
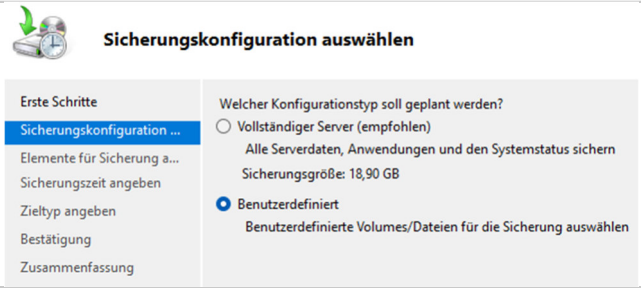
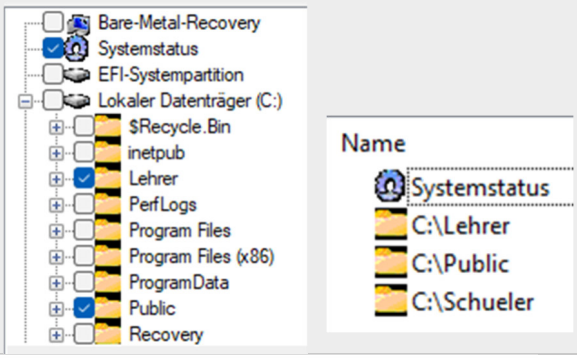
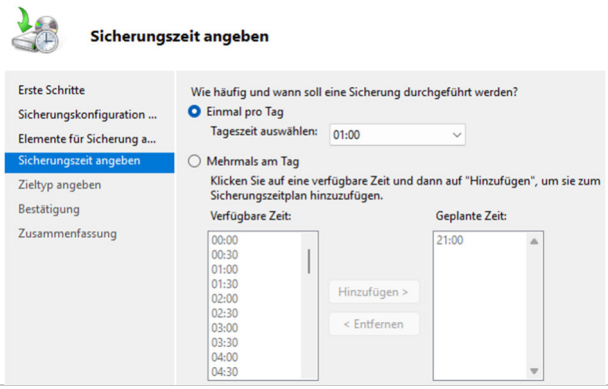
Damit Windows Server die Speicherressource nutzen kann muss diese ins System eingebunden und initialisiert werden → somit wird dieses Medium als „systemintern“ erkannt und kann ohne Probleme genutzt werden.

Erklärung	Beispiel
USB-Laufwerk wird mit dem physischen Rechner per USB-Port verbinden. **öffnen der Datenträgerverwaltung** →bei Bedarf das Laufwerk Partitionieren / Formatieren	
Wechsel in die VM „Server2025“ unter Datenträgerverwaltung ist kein externer Datenträger sichtbar **nur das interne LW**	
zurück zum Host→Einstellungen der Server-VM öffnen **unter SCSI-Controller können wir eine neue virtuelle Festplatte hinzufügen.**	

ein neuer Assistent öffnet sich	
feste Größe da empfohlen	
hier wird der Name und der Pfad für den Speicherort der virtuellen Festplatte festgelegt, noch nicht die externe Festplatte selbst!	
nun wechseln wir wieder in die VM Server2025 und gehen zu **→Datenträgerverwaltung** **Dort erscheint nun die neue Festplatte!**	
um den Datenräger „online“ zu bringen**→re.MT.-->Online** **und gleich im Anschluss erneut re.MT.** →Datenträgerinitialisierung GPT auswählen	
erneut re.MT.-->neues einfaches Volume… Assistent startet und können die neue Festplatte konfigurieren **→Fertigstellen**	

neue Festplatte wurde erstellt und kann verwendet werden in der VM!	

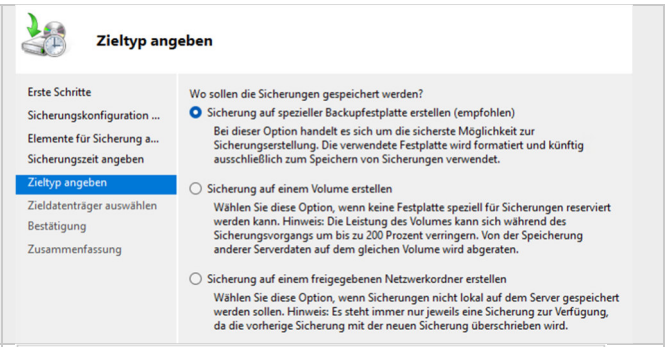
11.3.6 Windows Server Backup konfigurieren

Erklärung	Beispiel
Unter „Tools“ →Windows-Server-Sicherung →re. MT. **→Sicherungszeitplan** **Der Assistent für Sicherungszeitplan öffnet sich…**	
hier kann man zwischen einer vollständigen Sicherung oder Benutzerdefinierten Sicherung auswählen→ **wir entscheiden uns für Benutzdefiniert da wir nur den Systemstatus und Freigaben sichern möchten**	
im nächsten Fenster können wir die Auswahl der zu sichernden Komponenten treffen indem wir auf „Elemente hinzufügen“ klicken →Systemstatus →Freigaben • **Lehrer** • **Schueler** • **Public** →WEITER	
hier treffen wir die Einstellungen für den Sicherungszeitpunkt. →einmal täglich um 1:00	

Sicherungsziel auswählen

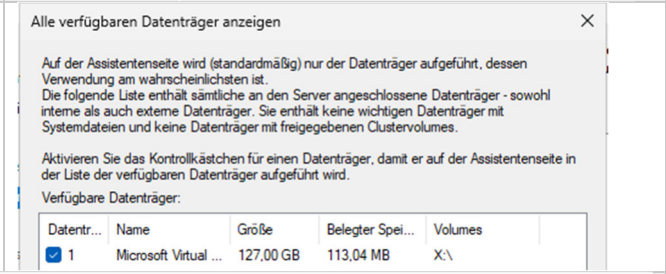
➔ **Spezielle Festplatte**

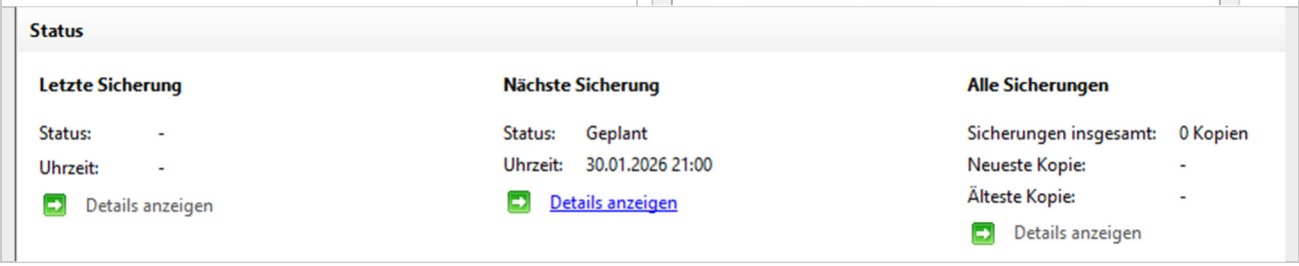
→WEITER

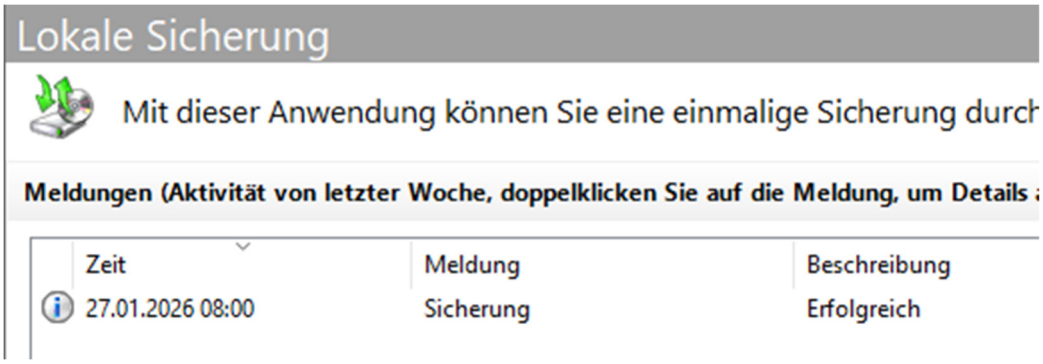


den Datenträger für die Speicherung der backup-Datei auswählen

→**Bestätigung & Fertigstellen**







11.3.6.1 Einmalige Sicherung

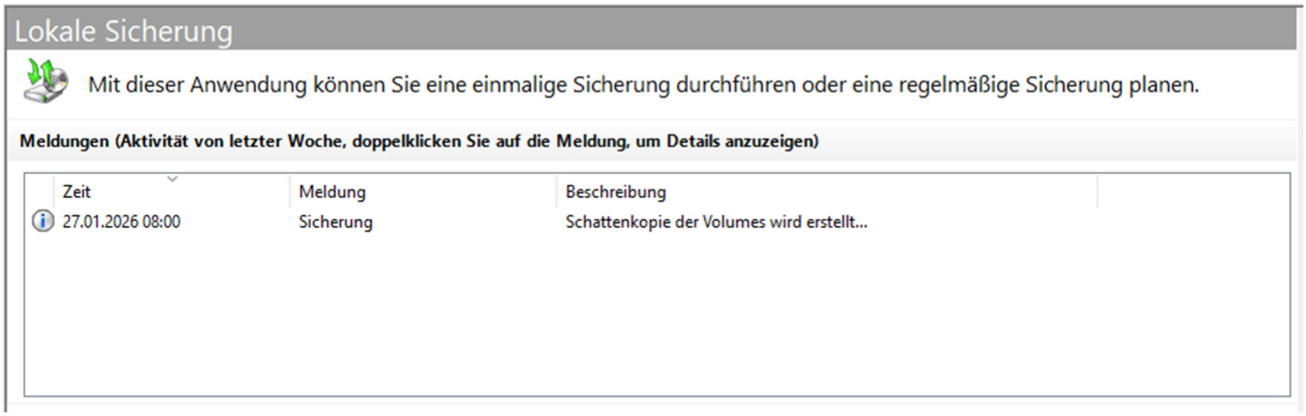
(Systemstatus + alle Freigabeordner)

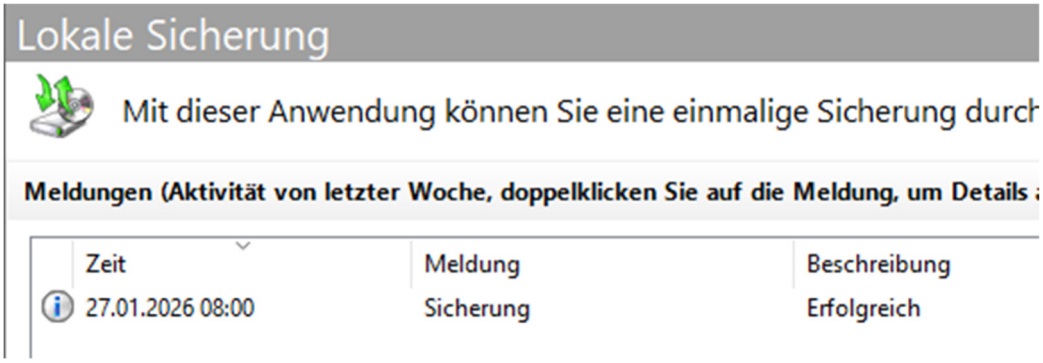
Beschreibung	PowerShell-Befehl
Einmalige Sicherung starten	`wbadmin start backup -backupTarget:Z: -systemState -include:C:\Schueler,C:\Lehrer,C:\Public,C:\Websites,C:\Bilder -quiet`

11.3.6.2 Wöchentliche automatische Sicherung

(Sonntag – 01:00 Uhr)

Beschreibung	PowerShell-Befehl
Windows-Backup-Zeitplan deaktivieren (falls vorher gesetzt)	
Bestehende Backup-Planung entfernen	`wbadmin disable backup`
Geplante Aufgabe für Sonntag 01:00 erstellen	
Wöchentliche Sicherung anlegen	`schtasks /Create /SC WEEKLY /D SUN /TN "WBADMIN_Weekly_Backup" /TR "wbadmin start backup -backupTarget:Z: -systemState -include:C:\Schueler,C:\Lehrer,C:\Public,C:\Websites,C:\Bilder -quiet" /ST 01:00 /RU SYSTEM`
Kontrollbefehle	
Vorhandene Backups anzeigen	`wbadmin get versions`
Prüfen ob Backupziel erreichbar ist	`dir Z:\`





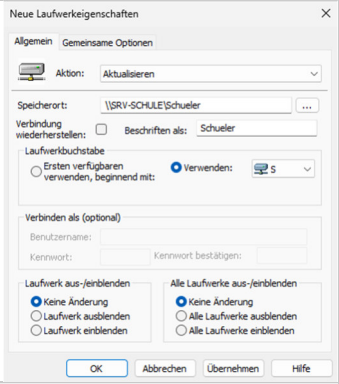
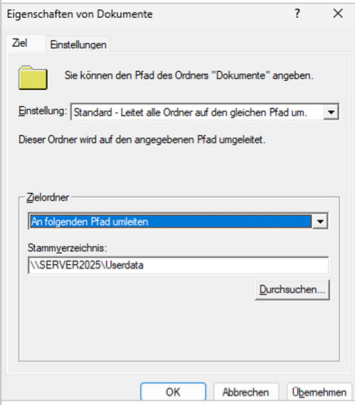
12. Gruppenrichtlinien (GPOs)

Die Gruppenrichtlinien sorgen für automatische Konfiguration der Benutzerumgebung.

12.1 GPO-Beispiele für Benutzer oder Gruppen

Jedem Punkt geht eine Erstellung oder Bearbeitung (re.MT.) einer GPO mit entsprechend eindeutiger Bezeichnung voran!

Einstellung	Pfad in der GPO-Verwaltung

Desktop-Hintergrund = Schullogo	Benutzerkonfiguration Administrative Vorlagen Desktop Desktop Hintergrundbild
Systemsteuerung blockieren	Benutzerkonfiguration Administrative Vorlagen Systemsteuerung Zugriff verhindern
Nur bestimmte Programme zulassen	OFFEN
Netzlaufwerk S: = \\Server\Schueler **Netzlaufwerk P: = \\Server\Public** **Netzlaufwerk L: = \\Server\Lehrer**	Benutzerkonfiguration Einstellungen Windows-Einstellungen Laufwerkszuordnung 
Ordnerumleitung „Dokumente“	 Benutzerkonfiguration Richtlinien Windows-Einstellungen Ordnerumleitung re.MT Eigenschaften
MMC Snap-Ins erlauben **Ereignisanzeige**	Benutzerkonfiguration Administrative Vorlagen Windows-Komponenten MMC Snap-Ins
MMC Snap-Ins erlauben **Computerverwaltung**	Benutzerkonfiguration Administrative Vorlagen Windows-Komponenten MMC Snap-Ins
Alle MMC Snap-Ins außer Ereignisanzeige & Computerverwaltung blockieren	
Gruppenrichtlinienverwaltung → Group Policy Objects →Neu erstellen **„GPO_Lehrer_MMC_Beschraenkung“**	**Benutzerkonfiguration** **→ Richtlinien** **→ Administrative Vorlagen** **→ Windows-Komponenten** **→ Microsoft Management Console**

	Benutzer auf die Verwendung von zugelassenen Snap-Ins beschränken→AKTIVIEREN
anschließend noch die Ausnahmen definieren: Eingeschränkte/Zugelassene Snap-Ins →dazu die gewünschten Snap-Ins aktivieren. Computerverwaltung & Ereignisanzeige	
Anders Snap-Ins blockieren	Benutzerkonfiguration Administrative Vorlagen Windows-Komponenten MMC Snap-Ins

12.2 Schüler-GPOs (OU: Schueler)

Einstellung	PoerShell	Hinweis
GPO erstellen + an OU linken	`New-GPO -Name "GPO-Schueler" | New-GPLink -Target "OU=Schueler,DC=schule,DC=local"`	Module: GroupPolicy
Desktop-Hintergrund (Schullogo)	`Set-GPRegistryValue -Name "GPO-Schueler" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "Wallpaper" -Type String -Value "\\SRV-SCHULE\Public\logo.jpg"`	Logo-Datei vorher in Public ablegen.
	`Set-GPRegistryValue -Name "GPO-Schueler" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "WallpaperStyle" -Type String -Value "2"`	2 = Stretch (je nach Wunsch).
Systemsteuerung/Einstellungen blockieren	`Set-GPRegistryValue -Name "GPO-Schueler" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -ValueName "NoControlPanel" -Type DWord -Value 1`	Deckt „Systemsteuerung und Einstellungen“ ab.
Nur bestimmte Programme ausführen (Basis)	`Set-GPRegistryValue -Name "GPO-Schueler" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -ValueName "RestrictRun" -Type DWord -Value 1`	Dazu Liste pflegen (s.u.).
Erlaubte Programme definieren (Beispiel)	`Set-GPRegistryValue -Name "GPO-Schueler" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun" -ValueName "1" -Type String -Value "WINWORD.EXE"`	Browser z. B. msedge.exe als "2".
Netzlaufwerk S: -> Schueler	`Logon-Script erstellen (s.u.) + per GPO setzen`	GPP wäre GUI-lastig, Script ist

		schnell & prüfbar.
Netzlaufwerk P: -> Public	Logon-Script	
Ordnerumleitung „Dokumente“ -> \\Server\Schueler\%username%	Logon-Script (Known Folder Move per Registry)	In Prüfungs-Labs meist akzeptiert.

Logon-Script (Schüler) auf dem Server anlegen (z. B. in \\SRV-SCHULE\NETLOGON\schueler-logon.ps1)

```
# schueler-logon.ps1
New-Item -ItemType Directory -Path "\\SRV-SCHULE\Schueler\$env:USERNAME" -Force | Out-Null

# Drive mappings
net use S: "\\SRV-SCHULE\Schueler" /persistent:yes
net use P: "\\SRV-SCHULE\Public"  /persistent:yes

# "Dokumente" umbiegen (User Shell Folders)
$docs = "\\SRV-SCHULE\Schueler\$env:USERNAME"
New-Item -ItemType Directory -Path $docs -Force | Out-Null
Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" `
  -Name "Personal" -Value $docs
```

Script per GPO zuweisen

```
Set-GPRegistryValue -Name "GPO-Schueler" `
  -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon\0\0" `
  -ValueName "Script" -Type String -Value "powershell.exe"
Set-GPRegistryValue -Name "GPO-Schueler" `
  -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon\0\0" `
  -ValueName "Parameters" -Type String -Value "-ExecutionPolicy Bypass -File \\SRV-SCHULE\NETLOGON\schueler-logon.ps1"
```

12.3 Lehrer-GPOs (OU: Lehrer)

Einstellung	PowerShell	Hinweis
GPO erstellen + linken	New-GPO -Name "GPO-Lehrer" | New-GPLink -Target "OU=Lehrer,DC=schule,DC=local"	
MMC Snap-Ins: Ereignisanzeige/Computerverwaltung erlauben, andere blockieren (praktisch)	Ansatz: AppLocker-Regeln oder „nur erlaubte Programme“ (RestrictRun) auf mmc.exe + nur bestimmte .msc freigeben	Reines „MMC Snap-In Whitelisting“ ist in PS deutlich komplexer. In Labs wird meist „RestrictRun/AppLocker“ akzeptiert.
Netzlaufwerk L: -> Lehrer	Logon-Script wie bei Schülern	
Netzlaufwerk P: -> Public	Logon-Script	
Ordnerumleitung „Dokumente“ -> \\Server\Lehrer\%username%	Logon-Script	

Logon-Script (Lehrer) \\SRV-SCHULE\NETLOGON\lehrer-logon.ps1

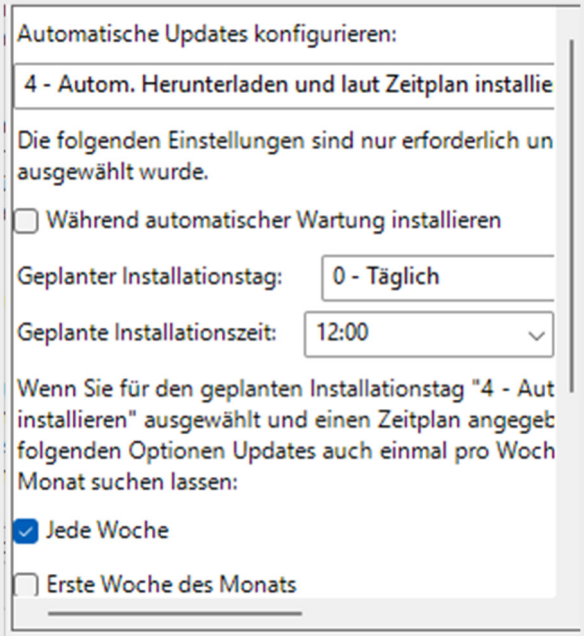
```
New-Item -ItemType Directory -Path "\\SRV-SCHULE\Lehrer\$env:USERNAME" -Force | Out-Null
net use L: "\\SRV-SCHULE\Lehrer" /persistent:yes
net use P: "\\SRV-SCHULE\Public" /persistent:yes

$docs = "\\SRV-SCHULE\Lehrer\$env:USERNAME"
New-Item -ItemType Directory -Path $docs -Force | Out-Null
Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" `
  -Name "Personal" -Value $docs
```

12.4 Domänenweite GPOs

12.4.1 GPO-Beispiele für gesamte Domäne (Domänenweit)

Soll die GPO auf die gesamte Domäne angewendet werde → **Default Domain Policy**

Einstellung	Pfad in der GPO-Verwaltung
Mindestkennwortlänge = 8 Zeichen	Computerkonfiguration→Windows-Einstellungen→ Sicherheitseinstellungen→Kontorichtlinien→ Kennwortrichtlinien
Kennwortkomplexität aktivieren	Computerkonfiguration→Windows-Einstellungen→ Sicherheitseinstellungen→Kontorichtlinien→ Kennwortrichtlinien
Kennwortgültigkeit = 90 Tage	Computerkonfiguration→Windows-Einstellungen→ Sicherheitseinstellungen→Kontorichtlinien→ Kennwortrichtlinien
Automatische Updates täglich 12:00	
Gruppenrichtlinienverwaltung → Group Policy Objects → **Default Domain Policy**→bearbeiten **Computerkonfiguration** Administrative Vorlage Windows-Komponenten Windows Update Endbenutzeroberfläche verwalten Automatische Updates konfigurieren	
Aktivieren Sie "Automatische Updates konfigurieren". • Wählen Sie Option 4 - Automatische Downloads und laut Plan installieren. • Stellen Sie den Tag auf 0 - Jeder Tag (oder spezifisch). • Stellen Sie die Uhrzeit auf 12:00. GPO aktualisieren: **gpupdate /force** ausführen.	

Einstellung	PowerShell	Hinweis
Kennwortrichtlinie: min 8, Komplexität aktiv, max 90 Tage	`Set-ADDefaultDomainPasswordPolicy -Identity "schule.local" -MinPasswordLength 8 -ComplexityEnabled $true -MaxPasswordAge (New-TimeSpan -Days 90)`	Gilt für ganze Domäne.
Windows Updates: automatische	`New-GPO -Name "GPO-Domain-Updates" | New-GPLink -Target "DC=schule,DC=local"`	Domain-root linken.

Installation täglich 12:00	`Set-GPRegistryValue -Name "GPO-Domain-Updates" -Key "HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU" -ValueName "AUOptions" -Type DWord -Value 4`	
	`Set-GPRegistryValue -Name "GPO-Domain-Updates" -Key "HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU" -ValueName "AUOptions" -Type DWord -Value 4`	4 = Auto download + schedule install
	`Set-GPRegistryValue -Name "GPO-Domain-Updates" -Key "HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU" -ValueName "ScheduledInstallDay" -Type DWord -Value 0`	0 = täglich
	`Set-GPRegistryValue -Name "GPO-Domain-Updates" -Key "HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU" -ValueName "ScheduledInstallTime" -Type DWord -Value 12`	12:00 Uhr

12.4.2 Ordnerumleitung „Dokumente“ per GPO (PowerShell)

Erklärung	PS-Befehl
GroupPolicy-Modul laden	`Import-Module GroupPolicy`
Neue GPO erstellen	`New-GPO -Name "GPO_Lehrer_Dokumente_Umleitung"`
GPO mit Lehrer-OU verknüpfen	`New-GPLink -Name "GPO_Lehrer_Dokumente_Umleitung" -Target "OU=Lehrer,DC=schule,DC=local"`
Sicherheitsfilter setzen (nur GG_Lehrer darf GPO anwenden)	`Set-GPPermission -Name "GPO_Lehrer_Dokumente_Umleitung" -TargetName "SCHULE\GG_Lehrer" -TargetType Group -PermissionLevel GpoApply`
Ordnerumleitung für „Dokumente“ setzen	`Set-GPRegistryValue -Name "GPO_Lehrer_Dokumente_Umleitung" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" -ValueName "Personal" -Type ExpandString -Value "\\SRV-Schule\Lehrer\%USERNAME%\Dokumente"`
Freigabe- und NTFS-Befehle für den Server (falls Share noch fehlt)	
Ordner für Share „Lehrer“ erstellen	`New-Item -ItemType Directory -Path "C:\Lehrer" -Force`
SMB-Freigabe erstellen	`New-SmbShare -Name "Lehrer" -Path "C:\Lehrer" -FullAccess "SCHULE\Administratoren"`
Freigaberechte für Lehrergruppe setzen	`Grant-SmbShareAccess -Name "Lehrer" -AccountName "SCHULE\GG_Lehrer" -AccessRight Change -Force`
NTFS-Rechte für Lehrergruppe setzen	`icacls "C:\Lehrer" /grant "SCHULE\GG_Lehrer:(OI)(CI)(M)"`
Kontrollbefehle	
Prüfen ob GPO existiert	`Get-GPO -Name "GPO_Lehrer_Dokumente_Umleitung"`
Prüfen ob GPO verlinkt ist	`Get-GPLink -Name "GPO_Lehrer_Dokumente_Umleitung" -Target "OU=Lehrer,DC=schule,DC=local"`
Am Client neue Richtlinien ziehen	`gpupdate /force`

13. Windows 11 Client

14. Dokumentation der Ergebnisse