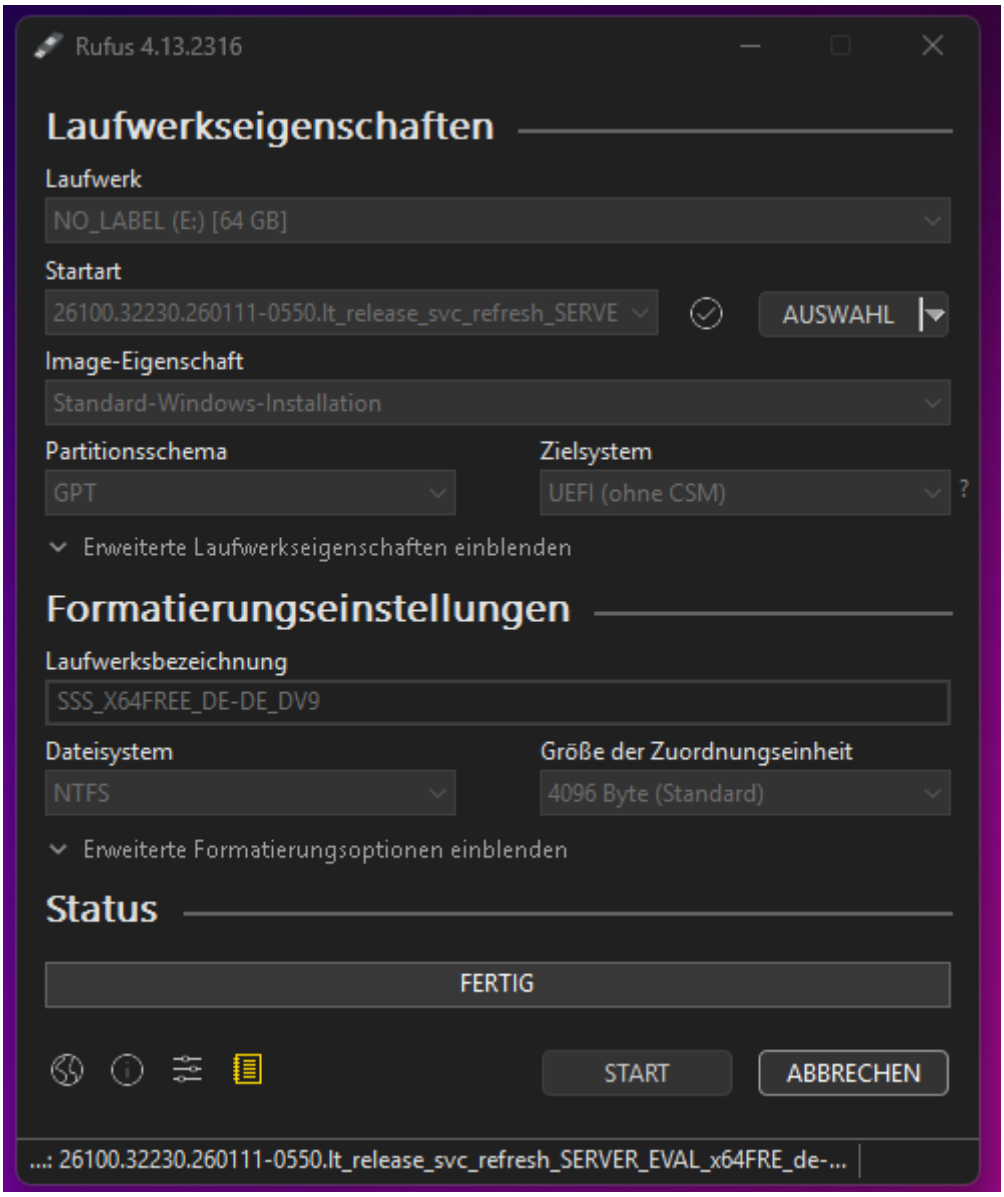
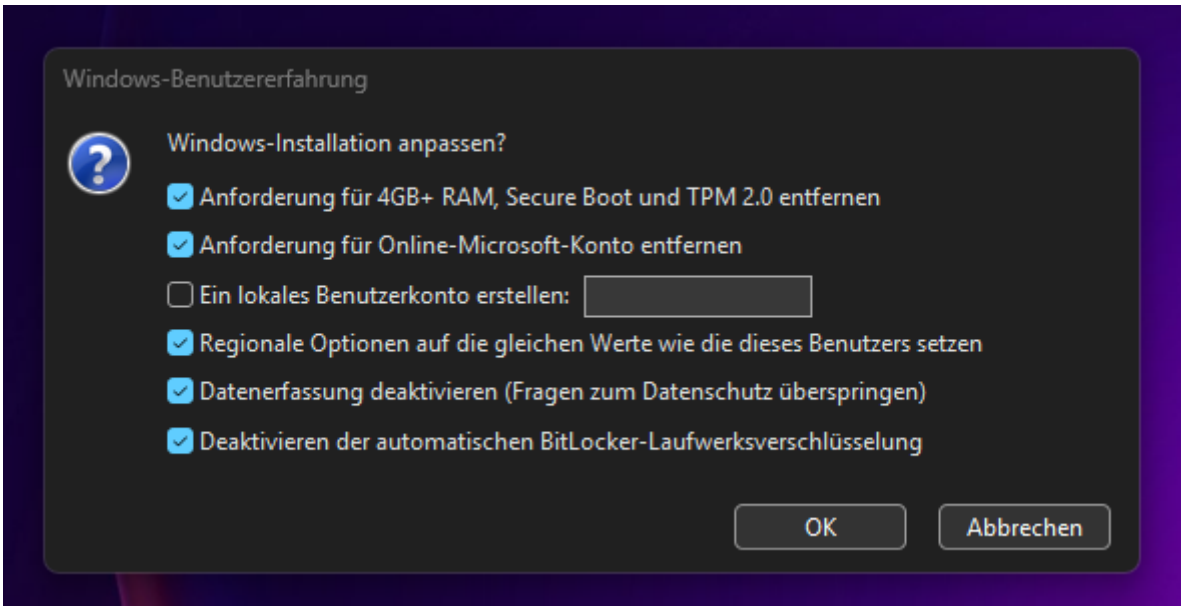
Windows installieren 5
Login: 5
Netzwerk Adapter Konfigurieren 6
Adapter umbenennen 6
Adapter 1 – INTERNET 7
Adapter 2 – intranet 7
Konfig prüfen 7
NAT und IP-Routing 9
Routing und RAS einrichtem 9
NAT per PowerShell (Alternative zu RRAS) 11
Firewall für Routing konfigurieren 12
RRAS-Dienst Autostart 12
NAT-Funktion testen 12
NAT / Routing Prüfliste 13
Active Directory Domain Services (AD DS) 15
AD DS-Rolle installieren 15
Domäne erstellen 15
AD nur auf INTRANET-NIC binden (Sicherheit) 16
AD-Status prüfen 17
DNS – intern & Internet-Weiterleitung 18
DNS-Forwarder konfigurieren 18
Forward-Lookupzone (andrea-srv-25.local) 18
Reverse-Lookupzone erstellen 19
DNS-Auflösung testen 19
DHCP-Server für das INTRANET 21
DHCP-Rolle installieren & autorisieren 21
DHCP-Bereich erstellen 21
DHCP nur auf INTRANET-NIC binden 23
DHCP-Reservierung für den Client 24
DHCP-Prüfpunkte 25

Aufgabe 6: Windows 11 zur Domäne hinzufügen & Routing testen ___ 26
Client-Netzwerk prüfen ___ 26
Verbindung zum Server testen ___ 26
Routing-Test – Internet über den Server ___ 26
Aufgabe 7: Benutzer, Gruppen und Organisationseinheiten (OU) ___ 28
OU-Struktur erstellen ___ 28
OU-Struktur per PowerShell erstellen ___ 28
Benutzer anlegen ___ 29
Benutzerliste erstellen ___ 29
Benutzer automatisch anlegen ___ 30
Gruppen anlegen ___ 30
Gruppen erstellen ___ 30
Benutzer zu Gruppen hinzufügen ___ 31
PC-CLIENT01 in richtige OU verschieben ___ 31
Aufgabe 8: Freigaben und Berechtigungen (INTRANET) ___ 32
SMB-Freigabe über UI (Windows Server) ___ 34
Freigaben testen (Client) ___ 35
Aufgabe 9: Gruppenrichtlinien (GPO) ___ 36
Kennwortrichtlinie konfigurieren ___ 36
Netzlaufwerk Z: automatisch verbinden ___ 37
Sicherheits-GPO ___ 39
Gruppenrichtlinien anwenden und testen ___ 40
IIS-Webserver (nur im INTRANET erreichbar) ___ 41
IIS installieren ___ 41
Website nur an die INTRANET-IP binden ___ 41
Intranet-Startseite erstellen ___ 42
Website testen ___ 43
HTTP-Zugriff per Firewall absichern ___ 44
Webserver testen ___ 45
FTP-Server (nur im INTRANET) ___ 46

FTP-Dienst installieren _____ 46
FTP-Site erstellen _____ 46
Firewall für FTP konfigurieren _____ 48
FTP testen _____ 49


Rufus 4.13.2316
Laufwerkseigenschaften
Laufwerk
NO_LABEL (E:) [64 GB]
Startart
26100.32230.260111-0550.lt_release_svc_refresh_SERVE
AUSWAHL
Image-Eigenschaft
Standard-Windows-Installation
Partitionsschema
GPT
Zielsystem
UEFI (ohne CSM)
Erweiterte Laufwerkseigenschaften einblenden
Formatierungseinstellungen
Laufwerksbezeichnung
SSS_X64FREE_DE-DE_DV9
Dateisystem
NTFS
Größe der Zuordnungseinheit
4096 Byte (Standard)
Erweiterte Formatierungsoptionen einblenden
Status
FERTIG
START
ABBRECHEN
...: 26100.32230.260111-0550.lt_release_svc_refresh_SERVER_EVAL_x64FRE_de-...


Windows-Benutzererfahrung
Windows-Installation anpassen?
Anforderung für 4GB+ RAM, Secure Boot und TPM 2.0 entfernen
Anforderung für Online-Microsoft-Konto entfernen
Ein lokales Benutzerkonto erstellen:
Regionale Optionen auf die gleichen Werte wie die dieses Benutzers setzen
Datenerfassung deaktivieren (Fragen zum Datenschutz überspringen)
Deaktivieren der automatischen BitLocker-Laufwerksverschlüsselung
OK
Abbrechen

Windows installieren

Login:
Administrator

Abc123

Server Name:

WIN-25-SRV

Clientname:	Client
User:	User
Passwort:	123456

Anmeldung Client in Domäne:

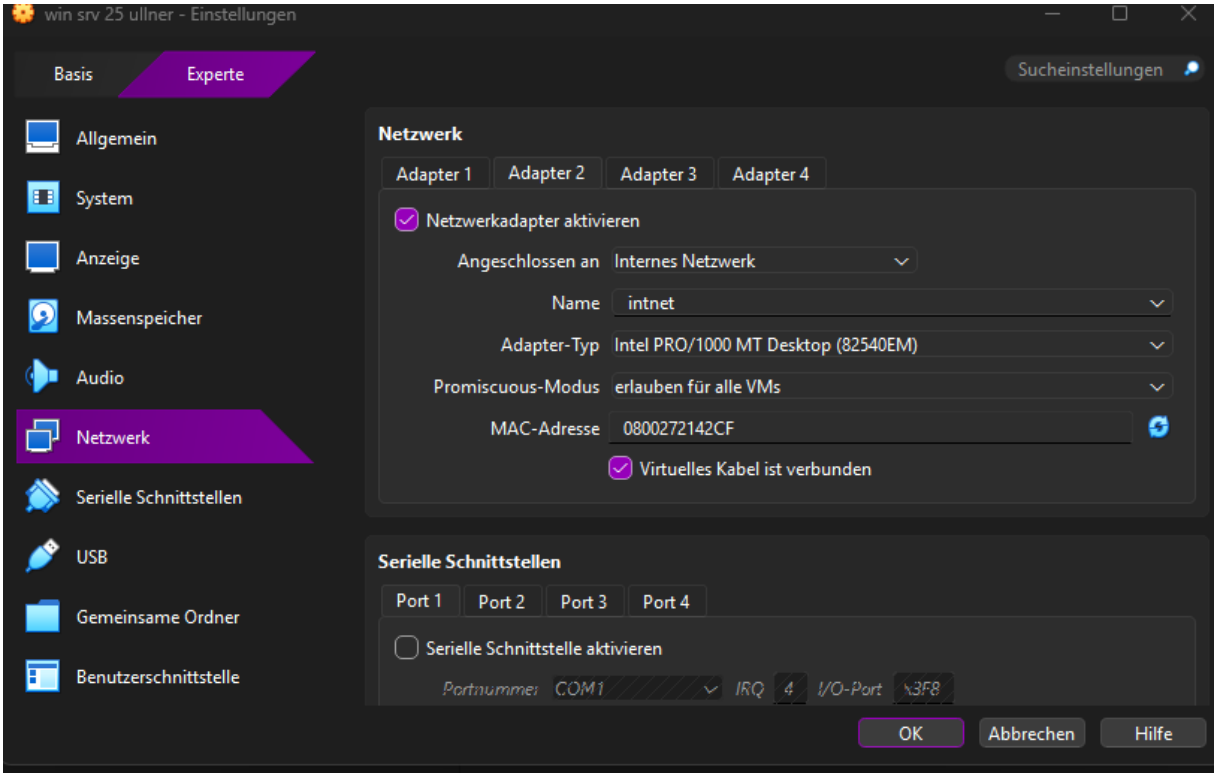
andrea-srv-25\administrator

Abc123

User Passwort: Passwort123!

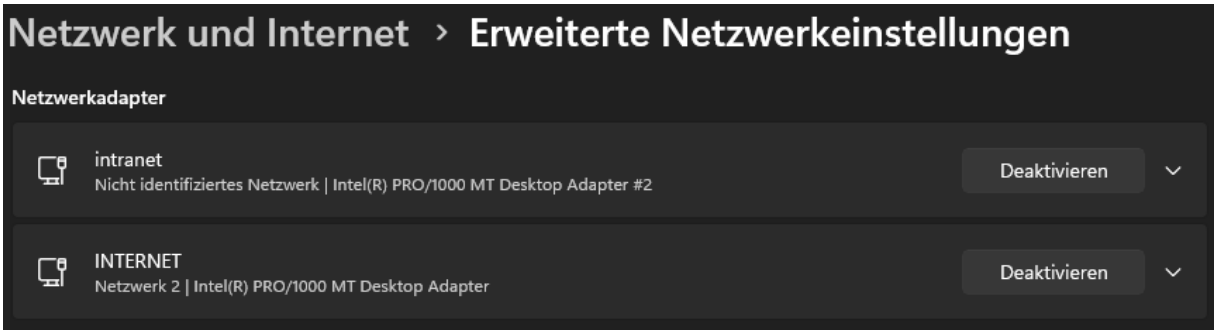
Netzwerk Adapter Konfigurieren

2. Netzwerk Adapter einbinden für internes Netz



Adapter umbenennen

Einstellungen → Netzwerk und internet → erweiterte Netzwerkeinstellungen → adapter → umbenennen



Systemsteuerung → Netzwerk und Internet → Adaptereinstellungen ändern

oder

Win + R → ncpa.cpl

Rechtsklick → Eigenschaften → …IPv4

Adapter 1 – INTERNET

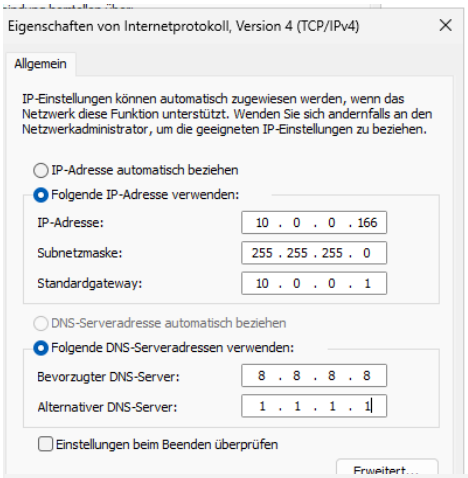
IP-Adresse: 10.0.0.166

Subnetzmaske: 255.255.255.0

Gateway: 10.0.0.1

DNS: 8.8.8.8

DNS alternativ: 1.1.1.1



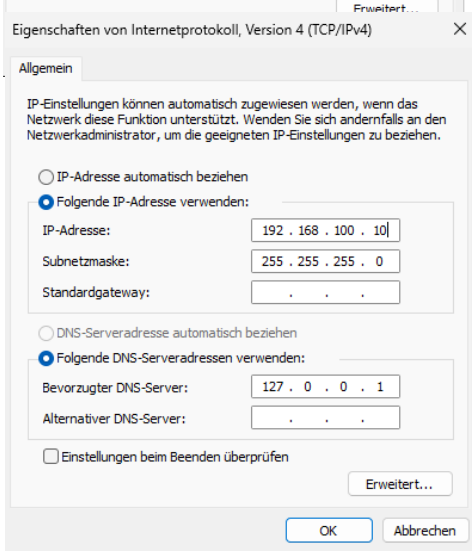
Adapter 2 – intranet

IP-Adresse: 192.168.100.10

Subnetzmaske: 255.255.255.0

Gateway: (leer lassen)

DNS: 127.0.0.1



Konfig prüfen

Get-NetIPConfiguration | Select-Object InterfaceAlias, IPv4Address, IPv4DefaultGateway

```
PS C:\Users\Administrator> Get-NetIPConfiguration | Select-Object InterfaceAlias, IPv4Address, IPv4DefaultGateway

InterfaceAlias IPv4Address                 IPv4DefaultGateway
-------------- -----------                 ------------------
intranet       {192.168.100.10}
INTERNET       {169.254.120.193, 10.0.0.166} {MSFT_NetRoute (InstanceID = ":8:8:8:9:55?55;:8:8:8;55;")}
```

route print -4

```
PS C:\Users\Administrator> route print -4
===========================================================================
Schnittstellenliste
  4...08 00 27 ad 27 d2 ......Intel(R) PRO/1000 MT Desktop Adapter
 10...08 00 27 21 42 cf ......Intel(R) PRO/1000 MT Desktop Adapter #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4-Routentabelle
===========================================================================
Aktive Routen:
    Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle Metrik
          0.0.0.0          0.0.0.0         10.0.0.1                4    281
        127.0.0.0        255.0.0.0   Auf Verbindung         127.0.0.1    331
        127.0.0.1  255.255.255.255   Auf Verbindung         127.0.0.1    331
  127.255.255.255  255.255.255.255   Auf Verbindung         127.0.0.1    331
      169.254.0.0      255.255.0.0   Auf Verbindung                 4    281
  169.254.120.193  255.255.255.255   Auf Verbindung                 4    281
  169.254.255.255  255.255.255.255   Auf Verbindung                 4    281
    192.168.100.0    255.255.255.0   Auf Verbindung    192.168.100.10    281
   192.168.100.10  255.255.255.255   Auf Verbindung    192.168.100.10    281
  192.168.100.255  255.255.255.255   Auf Verbindung    192.168.100.10    281
        224.0.0.0        240.0.0.0   Auf Verbindung         127.0.0.1    331
        224.0.0.0        240.0.0.0   Auf Verbindung                 4    281
        224.0.0.0        240.0.0.0   Auf Verbindung    192.168.100.10    281
  255.255.255.255  255.255.255.255   Auf Verbindung         127.0.0.1    331
  255.255.255.255  255.255.255.255   Auf Verbindung                 4    281
  255.255.255.255  255.255.255.255   Auf Verbindung    192.168.100.10    281
===========================================================================
Ständige Routen:
  Netzwerkadresse          Netzmaske  Gatewayadresse  Metrik
          0.0.0.0          0.0.0.0         10.0.0.1  Standard
===========================================================================
```

ping 8.8.8.8 -n 4

Test-NetConnection -ComputerName google.com -Port 80

```
PS C:\Users\Administrator> ping 8.8.8.8 -n 4

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=19ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=15ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=14ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=17ms TTL=114

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 14ms, Maximum = 19ms, Mittelwert = 16ms
PS C:\Users\Administrator> Test-NetConnection -ComputerName google.com -Port 80


ComputerName     : google.com
RemoteAddress    : 192.178.183.113
RemotePort       : 80
InterfaceAlias   : INTERNET
SourceAddress    : 169.254.120.193
TcpTestSucceeded : True
```

NAT und IP-Routing

Powershell als Admin starten

IP-Weiterleitung dauerhaft aktivieren

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "IPEnableRouter" -Value 1 -Type DWord

Sofort wirksam (ohne Neustart)

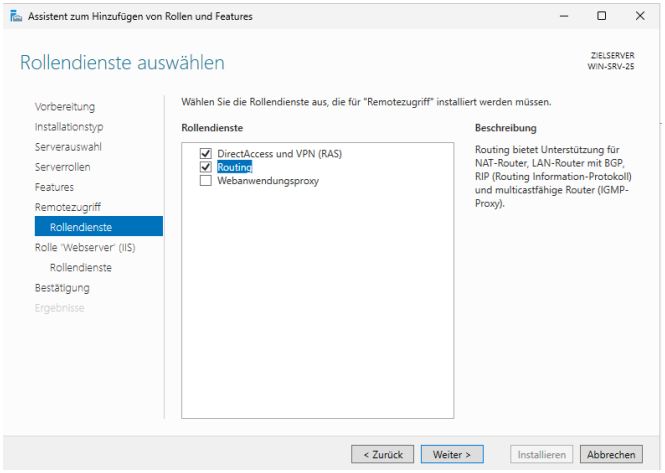
Set-NetIPInterface -Forwarding Enabled

Prüfen

Get-NetIPInterface | Select-Object InterfaceAlias, Forwarding | Format-Table -AutoSize

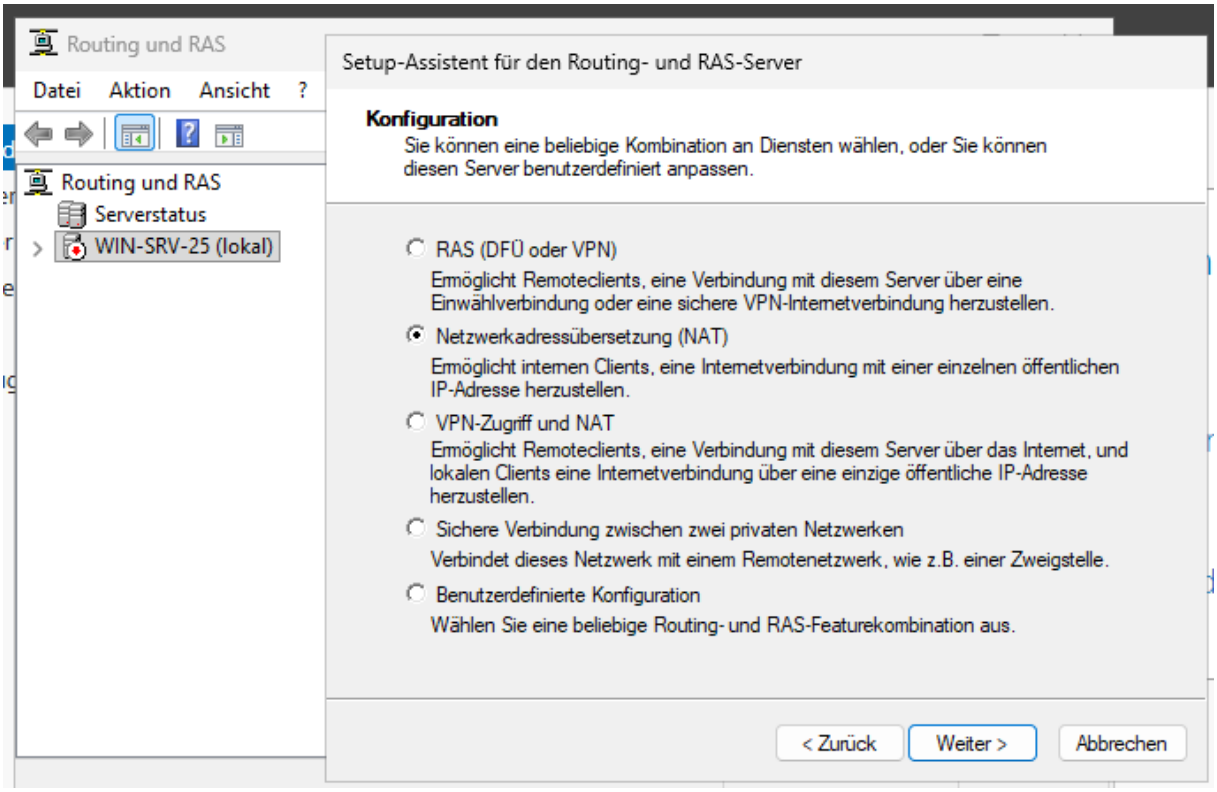
Routing und RAS einrichtem

1. Server-Manager → *Verwalten* → Rollen und Features hinzufügen
2. Rolle auswählen:
   - Remotezugriff
3. Rollendienste:
   - Routing auswählen → Installieren



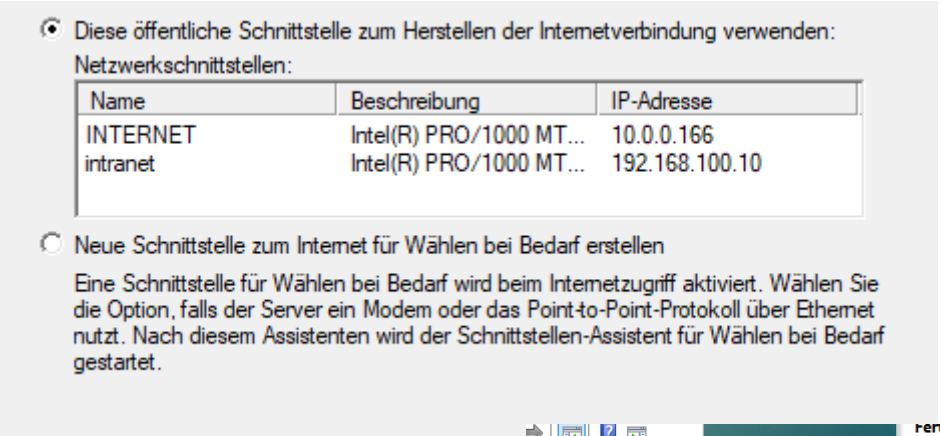
4. Nach Installation:
   - Server-Manager → Tools → Routing und RAS
5. Rechtsklick auf WIN-SRV-25 → Routing und RAS konfigurieren und aktivieren

6. Assistant:
   - Netzwerkadressübersetzung (NAT) auswählen

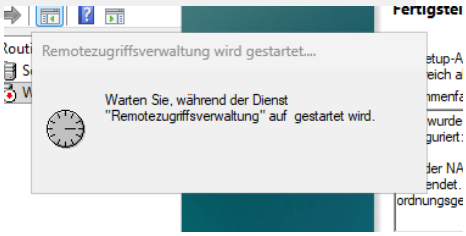


7. Öffentliche Schnittstelle wählen:
   - Adapter mit INTERNET → Haken bei:

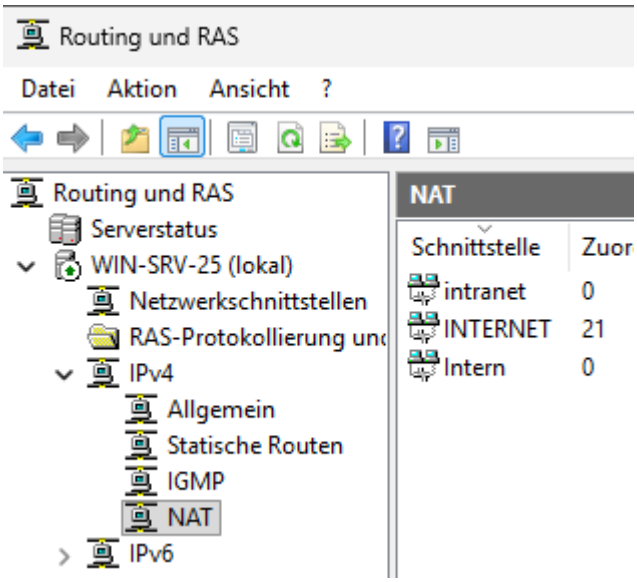
     „Öffentliche Schnittstelle mit Internetverbindung“



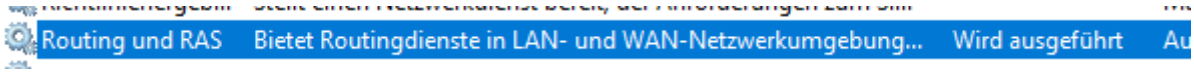
→ *Weiter* → *Fertigstellen*



8. Ergebnis prüfen:
    - IPv4 → NAT
    - Dort sollte die Schnittstelle sichtbar sein



← ig das?



WIN + R → services.msc

NAT per PowerShell (Alternative zu RRAS)
nicht beides machen → ansonsten funktioniert vielleicht garnichts

NAT erstellen (internes Netz definieren)

New-NetNat -Name "INTRANET-NAT" -InternalIPInterfaceAddressPrefix "192.168.100.0/24"

Status prüfen

Get-NetNat

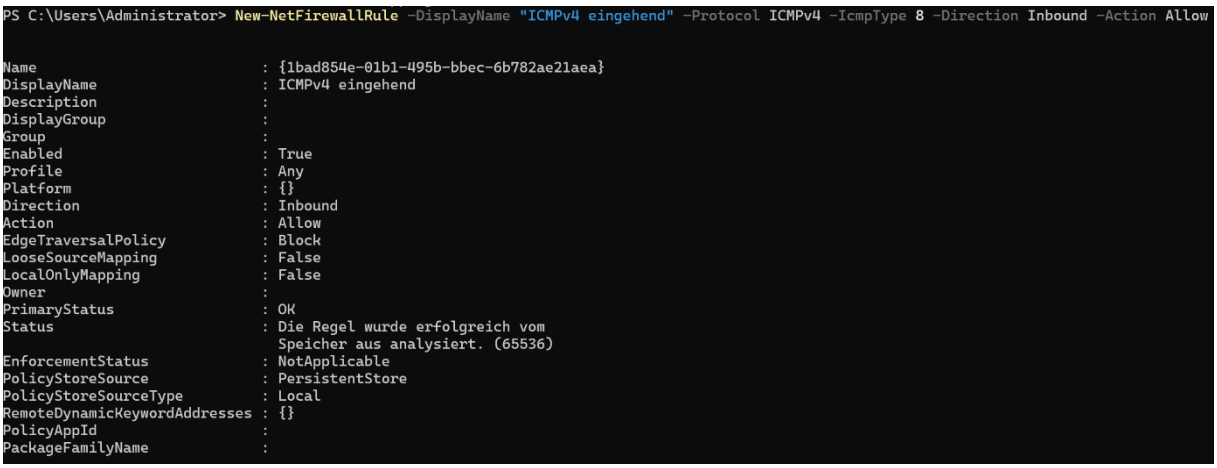
Statische Mappings anzeigen

Get-NetNatStaticMapping

Firewall für Routing konfigurieren

ICMP (Ping) eingehend erlauben

New-NetFirewallRule -DisplayName "ICMPv4 eingehend" -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow



Firewall-Profile aktivieren

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

RRAS-Dienst Autostart

Set-Service -Name RemoteAccess -StartupType Automatic

Start-Service -Name RemoteAccess

NAT-Funktion testen

(Test wird später mit Client wiederholt, hier vorab am Server)

Ping ins Internet

ping 8.8.8.8 -n 4

Routingtabelle prüfen (Default-Route)

route print -4 | findstr "0.0.0.0"

```
PS C:\Users\Administrator> route print -4 | findstr "0.0.0.0"
          0.0.0.0          0.0.0.0         10.0.0.1        10.0.0.38    281
         10.0.0.0    255.255.255.0   Auf Verbindung         10.0.0.38    281
        224.0.0.0        240.0.0.0   Auf Verbindung         127.0.0.1    331
        224.0.0.0        240.0.0.0   Auf Verbindung         10.0.0.38    281
        224.0.0.0        240.0.0.0   Auf Verbindung    192.168.100.10    281
          0.0.0.0          0.0.0.0         10.0.0.1  Standard
```

NAT-Verbindungen anzeigen (NetNat nicht eingerichtet weil RRAS)

Get-NetNatSession

NAT / Routing Prüfliste

IPEnableRouter = 1 in Registry

Aktivieren:

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name IPEnableRouter -Value 1

Prüfen:

Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name IPEnableRouter

Ohne IPEnableRouter=1:

- Server empfängt Pakete
- leitet sie aber NICHT weiter

Mit =1:

- Server arbeitet als Router
- NAT/RRAS kann korrekt routen

IP-Forwarding auf allen NICs aktiv

Prüfen:

Get-NetIPInterface | Select-Object InterfaceAlias, Forwarding

```
PS C:\WINDOWS\system32> Get-NetIPInterface | Select-Object InterfaceAlias, Forwarding

InterfaceAlias               Forwarding
--------------               ----------
intranet                        Enabled
INTERNET                        Enabled
Loopback Pseudo-Interface 1     Enabled
intranet                        Enabled
INTERNET                        Enabled
Loopback Pseudo-Interface 1     Enabled
```

RRAS-Dienst läuft

Get-Service RemoteAccess

```
PS C:\WINDOWS\system32> Get-Service RemoteAccess

Status   Name               DisplayName
------   ----               -----------
Running  RemoteAccess       Routing und RAS
```

Ping 8.8.8.8 erfolgreich

```
PS C:\WINDOWS\system32> ping 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=17ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=13ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=14ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=13ms TTL=114
```

Default-Route → NIC-INTERNET

route print -4 | findstr "0.0.0.0"

```
PS C:\WINDOWS\system32> route print -4 | findstr "0.0.0.0"
          0.0.0.0          0.0.0.0         10.0.0.1         10.0.0.38     281
          0.0.0.0          0.0.0.0         10.0.0.1  Standard
```

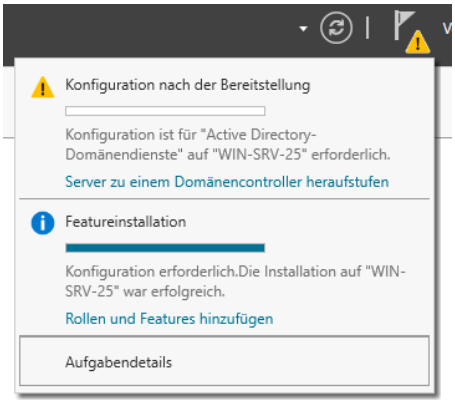
Active Directory Domain Services (AD DS)

AD DS-Rolle installieren

1. Server-Manager öffnen
2. Verwalten → Rollen und Features hinzufügen
3. Installationstyp:
    - Rollenbasierte oder featurebasierte Installation
4. Serverrolle auswählen:
    - Active Directory-Domänendienste
5. Installieren

Domäne erstellen

1. Im Server-Manager:
    - Server zu einem Domänencontroller heraufstufen



2. Option wählen:
    - Neue Gesamtstruktur hinzufügen
3. Stammdomäne eingeben: andrea-srv-25.local
4. Einstellungen:
    - DNS-Server aktiviert lassen
    - Globaler Katalog aktiviert lassen
    - DSRM-Passwort festlegen: Abc123
    - keine DNS-Delegierung
5. NetBIOS Domänenname: ANDREA-SRV-25
6. Installieren
7. Server startet neu

Anmeldung nach Neustart

Anmelden als:

ANDREA-SRV-25\Administrator

AD nur auf INTRANET-NIC binden (Sicherheit)

Standardmäßig lauschen AD und DNS auf allen Netzwerkkarten.
Aus Sicherheitsgründen sollte dies nur über die interne NIC erfolgen.

DNS nur auf INTRANET-IP lauschen lassen

dnscmd /ResetListenAddresses 192.168.100.10

Prüfen

dnscmd /info

```
ListenAddresses:

      Zeiger         = 0000020E18ADEF90
      MaxCount       = 1
      AddrCount      = 1
             Adr.[0] => af=2, salen=16, [sub=0, flag=00000000] p=13568, addr=192.168.100.10
```

AD-Status prüfen

Domäneninformationen

Get-ADDomain | Select-Object DNSRoot, NetBIOSName, DomainMode

```
PS C:\WINDOWS\system32> Get-ADDomain | Select-Object DNSRoot, NetBIOSName, DomainMode

DNSRoot             NetBIOSName          DomainMode
-------             -----------          ----------
andrea-srv-25.local ANDREA-SRV-25 Windows2025Domain
```

Domain Controller prüfen

Get-ADDomainController | Select-Object Name, IPv4Address, Site

```
PS C:\WINDOWS\system32> Get-ADDomainController | Select-Object Name, IPv4Address, Site

Name       IPv4Address    Site
----       -----------    ----
WIN-SRV-25 192.168.100.10 Default-First-Site-Name
```

Verbindungstest

dcdiag /test:connectivity

AD-Parameter

Parameter	Wert
DNS-Root (FQDN)	andrea-server-25.local
NetBIOS-Name	ANDREA-SRV-25
DC-IP	192.168.100.10
AD Status dcdiag	

Set-DnsClientServerAddress -InterfaceAlias "INTERNET" -ServerAddresses 192.168.100.10

Set-DnsClientServerAddress -InterfaceAlias "intranet" -ServerAddresses 192.168.100.10

DNS – intern & Internet-Weiterleitung

Der DNS-Server auf dem Domain Controller löst interne Namen der Zone andrea-srv-25.local selbst auf.
Externe Anfragen (z. B. google.com) werden über DNS-Forwarder an öffentliche DNS-Server weitergeleitet.

Clients verwenden ausschließlich diesen DNS-Server.

DNS-Forwarder konfigurieren

1. Server-Manager öffnen
2. Tools → DNS
3. Rechtsklick auf WIN-SRV-25 → Eigenschaften
4. Tab Weiterleitungen (Forwarders) öffnen
5. Bearbeiten → folgende DNS-Server hinzufügen:

   8.8.8.8 (Google)

   8.8.4.4 (Google Backup)

   1.1.1.1 (Cloudflare)
6. OK → Übernehmen → OK

Forward-Lookupzone (andrea-srv-25.local)

1. DNS → Forward-Lookupzonen → andrea-srv-25.local
2. Rechtsklick → Neuer Host (A- oder AAAA-Record)
3. Einträge erstellen:

Name	IP-Adresse	PTR
WWW	192.168.100.10	Ja
ftp	192.168.100.10	Ja
intranet	192.168.100.10	Ja
srv-dc01	192.168.100.10	Ja

Reverse-Lookupzone erstellen

1. DNS-Manager → Reverse-Lookupzonen
2. Neue Zone
3. Typ:
    - Primärzone
    - AD-integriert
4. Netzwerk-ID eingeben: 192.168.100.
5. nicht sichere und sichere Updates….
6. Fertigstellen

DNS-Auflösung testen

Intern (andrea-srv-25.local)

Resolve-DnsName www.andrea-srv-25.local -Server 192.168.100.10

```
PS C:\WINDOWS\system32> Resolve-DnsName www.andrea-srv-25.local -Server 192.168.100.10

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.andrea-srv-25.local                        A      3600  Answer     192.168.100.10
```

Resolve-DnsName srv-dc01.andrea-srv-25.local -Server 192.168.100.10

```
PS C:\WINDOWS\system32> Resolve-DnsName srv-dc01.andrea-srv-25.local -Server 192.168.100.10

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
srv-dc01.andrea-srv-25.local                   A      3600  Answer     192.168.100.10
```

Extern (Internet via Forwarder)

Resolve-DnsName google.com -Server 192.168.100.10

```
PS C:\WINDOWS\system32> Resolve-DnsName google.com -Server 192.168.100.10

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::64
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::71
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::8b
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::66
google.com                                     A      232   Answer     192.178.183.139
google.com                                     A      232   Answer     192.178.183.101
google.com                                     A      232   Answer     192.178.183.113
google.com                                     A      232   Answer     192.178.183.138
google.com                                     A      232   Answer     192.178.183.102
google.com                                     A      232   Answer     192.178.183.100
```

Resolve-DnsName microsoft.com -Server 192.168.100.10

```
PS C:\WINDOWS\system32> Resolve-DnsName microsoft.com -Server 192.168.100.10

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
microsoft.com                                  AAAA   907   Answer     2603:1061:14:63::1
microsoft.com                                  A      2870  Answer     150.171.109.100
```

Ziel der Aufgabe

- Interne Namen → DNS auf DC
- Externe Namen → Forwarder (Google / Cloudflare)
- Clients nutzen nur 192.168.100.10 als DNS

DHCP-Server für das INTRANET

Der DHCP-Server vergibt IP-Adressen ausschließlich im INTRANET-Netz (192.168.100.0/24).
Er ist an die interne Netzwerkkarte (NIC-INTRANET) gebunden.

Clients erhalten dadurch:

- IP-Adresse aus dem INTRANET-Netz
- Standard-Gateway = Server (192.168.100.10)
- DNS = Domain Controller

DHCP-Rolle installieren & autorisieren

1. Server-Manager → Verwalten → Rollen und Features hinzufügen
2. Rolle auswählen:
    - DHCP-Server → Installieren
3. Nach der Installation:
    - „DHCP-Server konfigurieren“ öffnen
    - Assistent ausführen → Commit
    - Schließen

DHCP-Bereich erstellen

1. Server-Manager → Tools → DHCP
2. IPv4 → Rechtsklick → Neuer Bereich

DHCP-Parameter

Einstellung	Wert
Bereichsname	INTRANET-LAN
Start-IP	192.168.100.50
End-IP	192.168.100.200
Subnetzmaske	255.255.255.0
Ausschlussbereich	192.168.100.1 - 192.168.100.49
Lease-Dauer	8 Stunden

DHCP-Optionen

Option	Wert
003 Router (Gateway)	192.168.100.10
006 DNS-Server	192.168.100.10
015 DNS-Domäne	andrea-srv-25.local

Wichtiger Hinweis

Das Gateway für Clients ist immer:

192.168.100.10

Nicht die Internet-IP (10.0.0.x), da der Server das Routing übernimmt.

DHCP nur auf INTRANET-NIC binden

GUI-Methode

1. DHCP-Manager → Rechtsklick auf IPv4 → Eigenschaften
2. Tab Erweitert → Bindungen
3. Aktivieren:
    - ✓ NIC-INTRANET (192.168.100.10)
4. Deaktivieren:
    - ❌ NIC-INTERNET

PowerShell

Set-DhcpServerv4Binding -InterfaceAlias "NIC-INTRANET" -BindingState $true

Set-DhcpServerv4Binding -InterfaceAlias "NIC-INTERNET" -BindingState $false

Bindungen prüfen

Get-DhcpServerv4Binding

```
PS C:\WINDOWS\system32> Get-DhcpServerv4Binding

InterfaceAlias                          IPAddress           BindingState
--------------                          ---------           ------------
intranet                                192.168.100.10      True
INTERNET                                10.0.0.38           False
```

DHCP-Reservierung für den Client

MAC-Adresse des Clients ermitteln

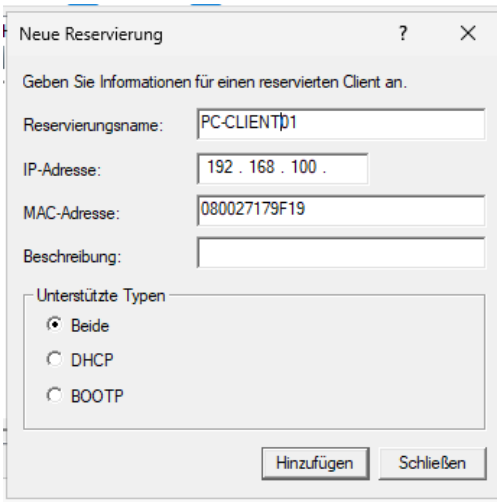
Am Client:

ipconfig /all

MAC: 08-00-27-17-9F-19

Reservierung erstellen

1. DHCP-Manager öffnen
2. IPv4 → Bereich → Reservierungen
3. Rechtsklick → Neue Reservierung



Werte

Reservierungsname: PC-CLIENT01

IP: 192.168.100.101

MAC-Adresse: 080027179F19

MAC des Clients (ohne Bindestriche)

Client der Domäne hinzufügen:

- VM Netzwerk Adapter auf Internes Netzwerk ändern
- DNS im Client auf 192.168.100.10 ändern

Dann der Domäne hinzufügen: andrea-srv-25.local

Über Powershell:

Add-Computer -DomainName "andrea-srv-25.local" -Credential "FIRMA\Administrator" -Restart -Force

DHCP-Prüfpunkte

Bereich INTRANET-LAN aktiv	[x] Ja / [ ] Nein
Gateway = 192.168.100.10	[x] Ja / [ ] Nein
DNS = 192.168.100.10	[x] Ja / [ ] Nein
DHCP bindet nur auf NIC-INTRANET	[x] Ja / [ ] Nein
Client erhält IP via DHCP	[x] Ja / [ ] Nein
Client erhält Gateway 192.168.100.10	[x] Ja / [ ] Nein

Aufgabe 6: Windows 11 zur Domäne hinzufügen & Routing testen

Nach dem Domänenbeitritt muss der Windows-11-Client:

- interne Ressourcen (andrea-srv-25.local) erreichen
- sowie Internetzugriff über den Server erhalten

Dies ist der wichtigste Test der Dual-NIC-Konfiguration.

Client-Netzwerk prüfen

Netzwerkkonfiguration anzeigen

Am Windows-11-Client:

ipconfig /all

Erwartete Werte

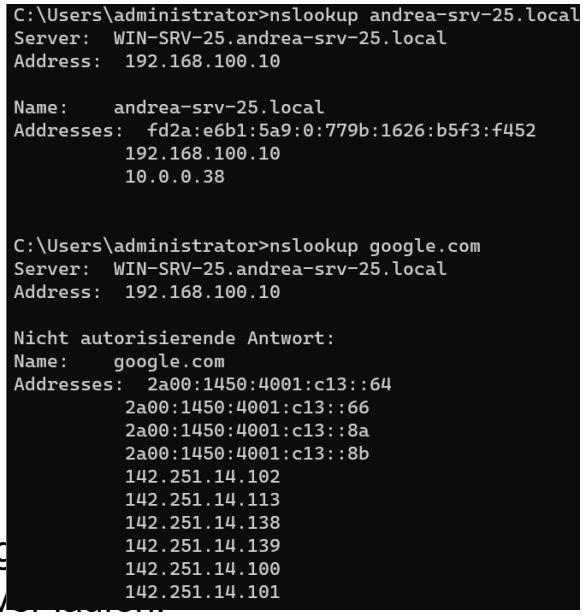
Einstellung	Erwarteter Wert
IP-Adresse	192.168.100.101 *(oder andere DHCP-Adresse)*
Gateway	192.168.100.10
DNS-Server	192.168.100.10

Verbindung zum Server testen

ping 192.168.100.10

nslookup andrea-srv-25.local

nslookup google.com



Routing-Test – Internet über den Server

Der Client darf keinen direkten Internetzug
Der gesamte Verkehr muss über den Serv

Internetverbindung testen

ping 8.8.8.8

Routing prüfen

tracert 8.8.8.8

```
Routenverfolgung zu dns.google [8.8.8.8]
über maximal 30 Hops:

  1     1 ms     *        1 ms  WIN-SRV-25.andrea-srv-25.local [192.168.100.10]
  2     *        *        *     Zeitüberschreitung der Anforderung.
  3     3 ms     3 ms     3 ms  10.0.0.1
  4     4 ms     3 ms     7 ms  10.170.17.254
  5     4 ms     3 ms     4 ms  10.170.0.6
  6     5 ms     4 ms     4 ms  10.170.0.1
  7     7 ms     6 ms     7 ms  85.31.21.253
  8     7 ms     5 ms     6 ms  we.corou0008.as21013.net [80.243.161.85]
  9    19 ms    15 ms    14 ms  fra.corou0010.as21013.net [80.243.161.101]
 10     *        *        *     Zeitüberschreitung der Anforderung.
 11    19 ms    17 ms    17 ms  209.85.244.249
 12    16 ms    16 ms    14 ms  142.250.209.243
 13    17 ms    14 ms    14 ms  dns.google [8.8.8.8]
```

Der erste Hop muss sein:

192.168.100.10

(INTRANET-NIC des Servers)

Webseite abrufen

curl https://www.google.at -UseBasicParsing

oder:

(Invoke-WebRequest https://www.google.at -UseBasicParsing).StatusCode

Erwartung

200 oder →

```
C:\Users\administrator>curl https://www.google.at -UseBasicParsing
Enter proxy password for user 'seBasicParsing':
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.google.com/">here</A>.
</BODY></HTML>
```

Aufgabe 7: Benutzer, Gruppen und Organisationseinheiten (OU)

Die Benutzerverwaltung erfolgt im internen Active Directory der Domäne:

andrea-srv-25.local

Die Haupt-OU lautet:

Firma

OU-Struktur erstellen

Firma

```
├── Benutzer
│   ├── IT
│   ├── Verwaltung
│   └── Auszubildende
├── Gruppen
└── Computer
```

OU-Struktur per PowerShell erstellen

```
New-ADOrganizationalUnit -Name "firma" `
-Path "DC=andrea-srv-25,DC=local"

New-ADOrganizationalUnit -Name "Benutzer" `
-Path "OU=firma,DC=andrea-srv-25,DC=local"

New-ADOrganizationalUnit -Name "IT" `
-Path "OU=Benutzer,OU=firma,DC=andrea-srv-25,DC=local"
```

```
New-ADOrganizationalUnit -Name "Verwaltung" `
-Path "OU=Benutzer,OU=firma,DC=andrea-srv-25,DC=local"

New-ADOrganizationalUnit -Name "Auszubildende" `
-Path "OU=Benutzer,OU=firma,DC=andrea-srv-25,DC=local"

New-ADOrganizationalUnit -Name "Gruppen" `
-Path "OU=firma,DC=andrea-srv-25,DC=local"

New-ADOrganizationalUnit -Name "Computer" `
-Path "OU=firma,DC=andrea-srv-25,DC=local"
```

Benutzer anlegen

Passwort definieren

```
$pw = ConvertTo-SecureString "Pas$wOrd!23“ -AsPlainText -Force
```

Pas$wOrd!23

Neues Passwort: Passwort123!

Benutzerliste erstellen

```
$users = @(
    @{Name="Max Mustermann"; Sam="m.mustermann"; OU="IT"},
    @{Name="Erika Muster"; Sam="e.muster"; OU="Verwaltung"},
    @{Name="Anna Schmidt"; Sam="a.schmidt"; OU="Auszubildende"},
    @{Name="Tom Berger"; Sam="t.berger"; OU="Auszubildende"},
    @{Name="IT Admin"; Sam="admin.it"; OU="IT"}
)
```

Benutzer automatisch anlegen

```
foreach ($u in $users) {

    New-ADUser `
    -Name $u.Name `
    -SamAccountName $u.Sam `
    -UserPrincipalName "$($u.Sam)@andrea-srv-25.local" `
    -Path "OU=$($u.OU),OU=Benutzer,OU=firma,DC=andrea-srv-25,DC=local" `
    -AccountPassword $pw `
    -Enabled $true

    Write-Host "Angelegt: $($u.Sam)"
}
```

Gruppen anlegen

Gruppen-OU Pfad

```
$gPath = "OU=Gruppen,OU=firma,DC=andrea-srv-25,DC=local"
```

Gruppen erstellen

```
New-ADGroup -Name "GRP-IT" `
-GroupScope Global `
-Path $gPath

New-ADGroup -Name "GRP-Verwaltung" `
-GroupScope Global `
```

```
-Path $gPath

New-ADGroup -Name "GRP-Azubis" `
-GroupScope Global `
-Path $gPath

New-ADGroup -Name "GRP-Alle" `
-GroupScope Global `
-Path $gPath
```

Benutzer zu Gruppen hinzufügen

```
Add-ADGroupMember -Identity "GRP-IT" `
-Members "m.mustermann","a.schmidt","admin.it"

Add-ADGroupMember -Identity "GRP-Verwaltung" `
-Members "e.muster","t.berger"

Add-ADGroupMember -Identity "GRP-Azubis" `
-Members "a.schmidt","t.berger"

Add-ADGroupMember -Identity "GRP-Alle" `
-Members "m.mustermann","e.muster","a.schmidt","t.berger","admin.it"
```

PC-CLIENT01 in richtige OU verschieben

Computer prüfen

```
Get-ADComputer "CLIENT"
```

Verschieben

Move-ADObject -Identity "CN=CLIENT,CN=Computers,DC=andrea-srv-25,DC=local" `

-TargetPath "OU=Computer,OU=Firma,DC=andrea-srv-25,DC=local"

Aufgabe 8: Freigaben und Berechtigungen (INTRANET)

Alle Freigaben sind nur über das **INTRANET-Netz (192.168.100.10)** erreichbar.
Die INTERNET-NIC wird nicht für Freigaben verwendet.

Clients greifen über den Servernamen oder die interne IP zu.

Ordnerstruktur erstellen

New-Item -ItemType Directory -Path "C:\Freigaben\Allgemein"

New-Item -ItemType Directory -Path "C:\Freigaben\IT"

New-Item -ItemType Directory -Path "C:\Freigaben\Verwaltung"

New-Item -ItemType Directory -Path "C:\Freigaben\Azubis"

SMB-Freigaben erstellen

Allgemein

New-SmbShare -Name "Allgemein" `

-Path "C:\Freigaben\Allgemein" `

-FullAccess "ANDREA-SRV-25\Domänen-Admins" `

-ChangeAccess "ANDREA-SRV-25\GRP-Alle"

IT

New-SmbShare -Name "IT" `

-Path "C:\Freigaben\IT" `

-FullAccess "ANDREA-SRV-25\Domänen-Admins" `

-ChangeAccess "ANDREA-SRV-25\GRP-IT" `

-NoAccess "Jeder"

Verwaltung

New-SmbShare -Name "Verwaltung" `

-Path "C:\Freigaben\Verwaltung" `

-FullAccess "ANDREA-SRV-25\Domänen-Admins", "ANDREA-SRV-25\GRP-Verwaltung" `

-NoAccess "Jeder"

Azubis

New-SmbShare -Name "Azubis" `

-Path "C:\Freigaben\Azubis" `

-FullAccess "ANDREA-SRV-25\Domänen-Admins" `

-ChangeAccess "ANDREA-SRV-25\GRP-Azubis"

Wichtig:
Auf die Windows Server Sprache achten, Powershell ist empfindlich und kann selbst nicht übersetzen.

Domain Admins ≠ Domänen-Admins

Everyone ≠ Jeder

SMB-Freigabe über UI (Windows Server)

1. Explorer öffnen

   C:\Freigaben\IT → Rechtsklick → Eigenschaften

2. Tab „Freigabe“

   „Erweiterte Freigabe“ klicken

   Haken bei „Diesen Ordner freigeben“

3. Freigabename

   z. B. IT

4. Berechtigungen

   Klick auf „Berechtigungen“

5. Benutzer/Gruppen hinzufügen

   „Hinzufügen“

   - Domänen-Admins
   - GRP-IT
   - oder ANDREA-SRV-25\GRP-IT

   Rechte setzen

   Typisch:

   - Domänen-Admins → Vollzugriff
   - GRP-IT → Ändern oder Lesen
   - Jeder / Everyone → entfernen

Freigaben testen (Client)

Im AD muss das PW der Benutzer geändert werden damit diese aktiviert werden können.

Neues PW für jeden user: Passwort123!

Explorer

\\andrea-srv-25\Allgemein

\\192.168.100.10\IT

CMD testen

net use Z: \\andrea-srv-25\Freigabe\Allgemein /persistent:yes

net view \\andrea-srv-25

Typische Fehler (wichtig)

- falsche Domain-Gruppe (FIRMA\GRP-... muss exakt existieren)
- Tippfehler in Pfaden (FreigabenIIT, verwaltung etc.)
- Leerzeichen in Pfaden vermeiden
- falscher Servername (immer DC / Hostname prüfen)

Aufgabe 9: Gruppenrichtlinien (GPO)

Gruppenrichtlinien werden vom Domain Controller an die Clients verteilt. Die Clients müssen den DC über die INTRANET-IP erreichen können:

192.168.100.10

Die bisherige Netzwerk-, DNS- und AD-Konfiguration stellt dies sicher.

Kennwortrichtlinie konfigurieren

Neues GPO erstellen:

1. CMD:

gpmc.msc

2. Rechtsklick auf:

andrea-srv-25.local

3. *Gruppenrichtlinie erstellen und verknüpfen*

Name:

Kennwortrichtlinie-Firma

4. GPO bearbeiten

Pfad

Computerkonfiguration

→ Richtlinien

→ Windows-Einstellungen

→ Sicherheitseinstellungen

→ Kontorichtlinien

→ Kennwortrichtlinie

Einstellungen

Richtlinie	**Wert**
Minimale Kennwortlänge	12 Zeichen
Maximales Kennwortalter	90 Tage
Kennwort muss Komplexitätsanforderungen erfüllen	Aktiviert
Kontosperrungsrichtlinien:	
Kontosperrschwelle	5 Fehlversuche
Kontosperrdauer	30 Minuten

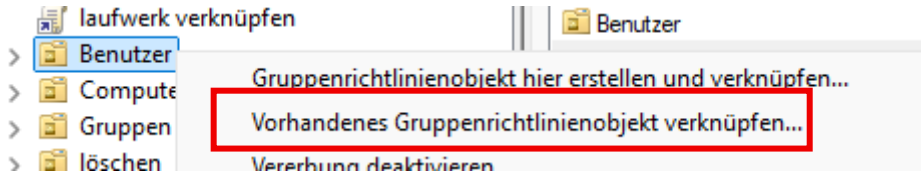
Netzlaufwerk Z: automatisch verbinden

Neues GPO erstellen

Name: Laufwerke

Verknüpfen mit:

OU=Benutzer,OU=Firma



GPO bearbeiten

Pfad:

Benutzerkonfiguration

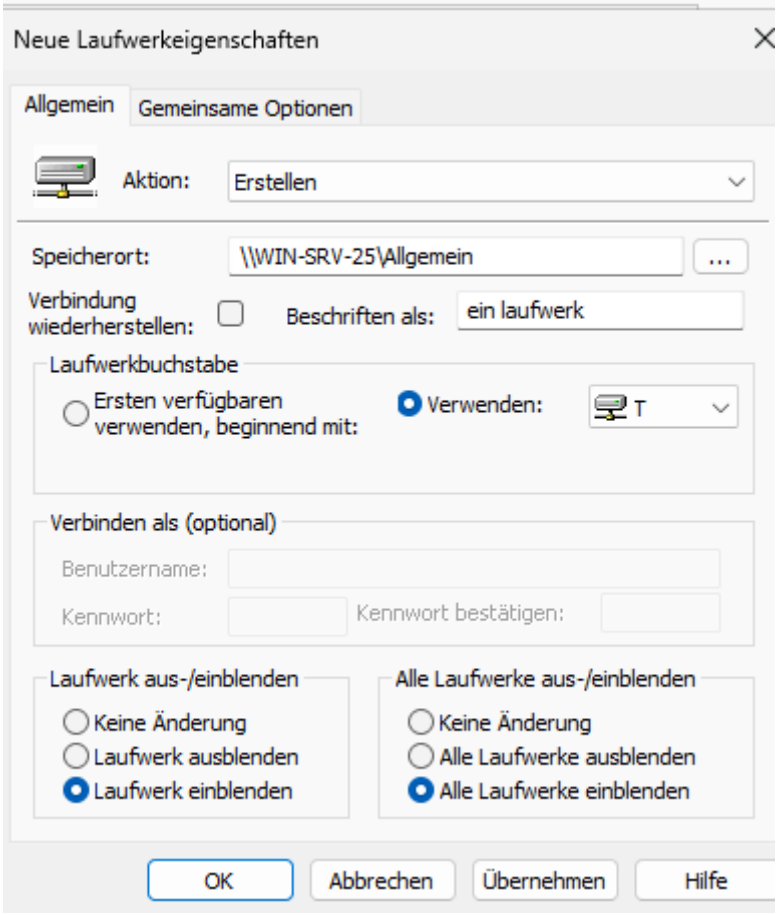
→ Einstellungen

→ Windows-Einstellungen

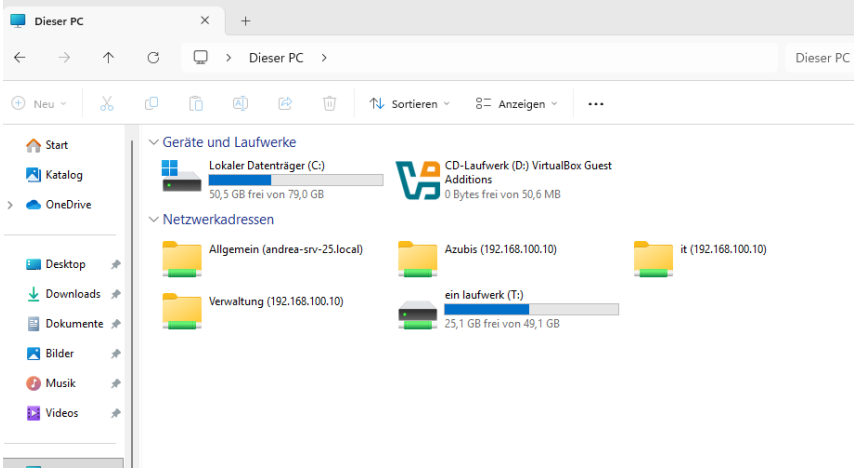
→ Laufwerkzuordnungen

Neues Laufwerk erstellen

Einstellung	Wert
Aktion	Erstellen
Speicherort	\SRV-DC01\Allgemein
Laufwerksbuchstabe	Z
Wiederverbinden	Aktiviert



Beim anmelden am Client PC in die Domäne sollte das Laufwerk sichtbar sein



Sicherheits-GPO

Neues GPO erstellen

Name: Sicherheit-Intern

Verknüpfen mit:

OU=Benutzer,OU=Firma

Letzten Benutzernamen ausblenden

Pfad:

Computerkonfiguration

→ Richtlinien

→ Windows-Einstellungen

→ Sicherheitseinstellungen

→ Lokale Richtlinien

→ Sicherheitsoptionen

Einstellung:

Interaktive Anmeldung: zuletzt angemeldeten Benutzer nicht anzeigen

Status: Aktiviert

Task-Manager deaktivieren

Pfad:

Benutzerkonfiguration

→ Richtlinien

→ Administrative Vorlagen

→ System

→ Strg+Alt+Entf-Optionen

Einstellung:

Task-Manager entfernen

Status: Aktiviert

Nach dem Test ggf. wieder deaktivieren.

Netzwerkadapter deaktivieren verhindern

Pfad:

Computerkonfiguration

→ Richtlinien

→ Administrative Vorlagen

→ Netzwerk

→ Netzwerkverbindungen

Einstellung:

Zugriff auf Eigenschaften einer LAN-Verbindung verbieten

Status: Aktiviert

Einstellung nicht vorhanden

Gruppenrichtlinien anwenden und testen

Am Windows-11-Client:

gpupdate /force

Angewendete Richtlinien anzeigen

gpresult /r

IIS-Webserver (nur im INTRANET erreichbar)

Der IIS-Webserver wird auf dem Domain Controller installiert.

In deinem Setup soll die Website ausschließlich über die interne Adresse erreichbar sein:

192.168.100.10

Die Website darf nicht über die INTERNET-NIC erreichbar sein.

IIS installieren

1. Server-Manager → Rollen und Features hinzufügen
2. Rolle auswählen:

Webserver (IIS)

3. Folgende Rollendienste aktivieren:

   Statischer Inhalt

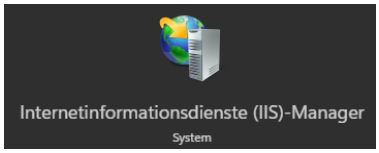
   Standarddokument

   Windows-Authentifizierung

   IIS-Verwaltungskonsole

4. Installation abschließen

Website nur an die INTRANET-IP binden



1. IIS-Manager öffnen:

   inetmgr

2. Websites → Default Website
3. Rechtsklick → Bindungen
4. Vorhandene HTTP-Bindung bearbeiten

Einstellungen:

Typ: http

IP-Adresse: 192.168.100.10

Port: 80

Hostname: www.andrea-srv-25.local

Hinweis

Da die Website nur an

192.168.100.10

gebunden ist, kann sie nicht direkt über die INTERNET-NIC aufgerufen werden.

Das ist für ein internes Intranet gewünscht.

Intranet-Startseite erstellen

PowerShell:

```
$html = @"
<!DOCTYPE html>
<html lang="de">
<head>
<meta charset="UTF-8">
<title>ANDREA-SRV-25 Intranet</title>

<style>
body{
    font-family:Arial;
    background:#f0f4f8;
    margin:0;
}

header{
    background:#1A5C36;
    color:white;
    padding:20px 40px;
}

main{
    max-width:900px;
    margin:40px auto;
    padding:0 20px;
}

.box{
    display:inline-block;
    background:white;
    border-radius:8px;
    padding:20px;
    margin:10px;
    width:200px;
    text-align:center;
    box-shadow:0 2px 8px rgba(0,0,0,.1);
}

footer{
    text-align:center;
    color:#888;
    padding:20px;
}
</style>
</head>

<body>

<header>
<h1>ANDREA-SRV-25 Intranet</h1>
<p>Server-IP: 192.168.100.10</p>
</header>

<main>

<h2>Schnellzugriff</h2>

<div class="box">
<h3>IT-Support</h3>
</div>

<div class="box">
<h3>Dateifreigaben</h3>
</div>

<div class="box">
<h3>FTP</h3>
</div>

</main>

<footer>
ANDREA-SRV-25.local © 2026
</footer>

</body>
</html>
"@

$html | Out-File "C:\inetpub\wwwroot\index.html" -Encoding UTF8
```

Website testen

Server:

Invoke-WebRequest http://localhost

Client:

Invoke-WebRequest http://192.168.100.10

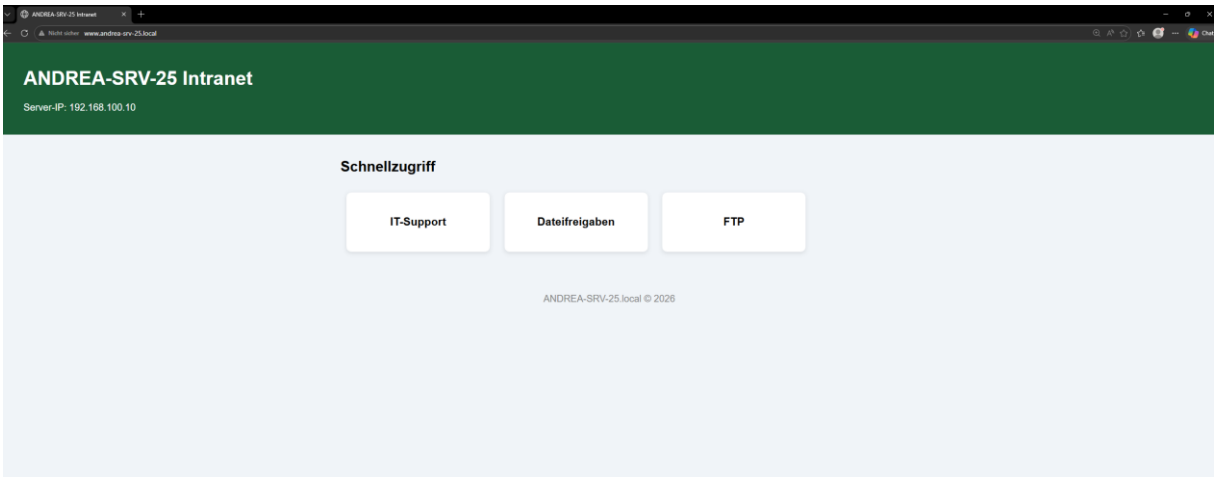
oder im Browser:

http://192.168.100.10

bzw.

http://www.andrea-srv-25.local

Wenn die Startseite erscheint, funktioniert IIS korrekt.



HTTP-Zugriff per Firewall absichern

Der Webserver soll nur aus dem INTRANET erreichbar sein.

Powershell:

HTTP-Zugriff aus dem INTRANET erlauben

```
New-NetFirewallRule `
-DisplayName "HTTP nur INTRANET" `
-Direction Inbound `
-Protocol TCP `
-LocalPort 80 `
-LocalAddress 192.168.100.10 `
-RemoteAddress 192.168.100.0/24 `
-Action Allow
```

HTTP-Zugriff über die INTERNET-NIC blockieren

```
New-NetFirewallRule `
-DisplayName "HTTP INTERNET blockieren" `
-Direction Inbound `
-Protocol TCP `
-LocalPort 80 `
-LocalAddress 10.0.0.10 `
-Action Block
```

Firewallregeln prüfen

```
Get-NetFirewallRule | Where-Object DisplayName -like "*HTTP*"
```

Webserver testen

Vom Windows-11-Client

Im Browser:

http://www.andrea-srv-25.local

oder

http://192.168.100.10

Vom Server

Im Browser:

http://localhost

oder per PowerShell:

Invoke-WebRequest http://localhost

Test von der INTERNET-Seite

Aufruf:

http://10.0.0.10

Erwartung:

Keine Verbindung

bzw. Zugriff durch Firewall blockiert.

Prüfpunkte

- http://www.andrea-srv-25.local vom Client erreichbar ja
- http://192.168.100.10 vom Client erreichbar nein
- http://localhost am Server erreichbar nein
- http://10.0.0.10 von außen blockiert

FTP-Server (nur im INTRANET)

Der FTP-Server wird ausschließlich über die INTRANET-NIC bereitgestellt.

192.168.100.10

Zugriffe über die INTERNET-NIC werden durch die Windows-Firewall blockiert.

FTP-Dienst installieren

Server-Manager → Rollen und Features hinzufügen

Unter:

Webserver (IIS)

- FTP-Server

aktivieren:

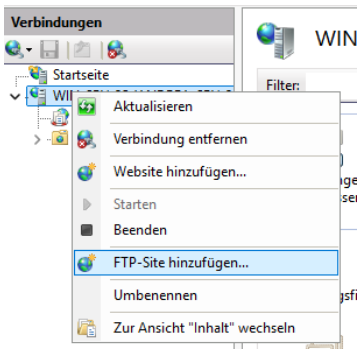
- FTP-Dienst
- FTP-Erweiterbarkeit

Installation abschließen.

FTP-Site erstellen

IIS-Manager öffnen

inetmgr



Rechtsklick auf:

Domain

- FTP-Site hinzufügen

Name:

- FTP-Andrea

Folgende Einstellungen verwenden:

- FTP-Sitename:
- FIRMA-FTP

Physischer Pfad:

C:\FTP-Root

IP-Adresse:

192.168.100.10

Port:

21

SSL:

Kein SSL

Authentifizierung:

Standard

Autorisierung:

Alle Benutzer

Berechtigungen:

Lesen und Schreiben

FTP-Ordnerstruktur erstellen

New-Item -ItemType Directory -Path "C:\FTP-Root\Allgemein"

New-Item -ItemType Directory -Path "C:\FTP-Root\LocalUser\m.mustermann"

New-Item -ItemType Directory -Path "C:\FTP-Root\LocalUser\e.muster"

New-Item -ItemType Directory -Path "C:\FTP-Root\LocalUser\Public"

Testdatei erstellen

"FTP OK" | Out-File "C:\FTP-Root\Allgemein\readme.txt"

Firewall für FTP konfigurieren

Powershell:

FTP-Port 21 nur im INTRANET erlauben

New-NetFirewallRule `

-DisplayName "FTP INTRANET" `

-Direction Inbound `

-Protocol TCP `

-LocalPort 21 `

-LocalAddress 192.168.100.10 `

-RemoteAddress 192.168.100.0/24 `

-Action Allow

FTP über INTERNET-NIC blockieren

New-NetFirewallRule `

-DisplayName "FTP INTERNET blockieren" `

-Direction Inbound `

-Protocol TCP `

-LocalPort 21 `

-LocalAddress 10.0.0.10 `

-Action Block

Passiv-Modus freigeben

New-NetFirewallRule `

-DisplayName "FTP Passiv INTRANET" `

-Direction Inbound `

-Protocol TCP `

-LocalPort 50000-50100 `

-LocalAddress 192.168.100.10 `

-RemoteAddress 192.168.100.0/24 `

-Action Allow

FTP testen

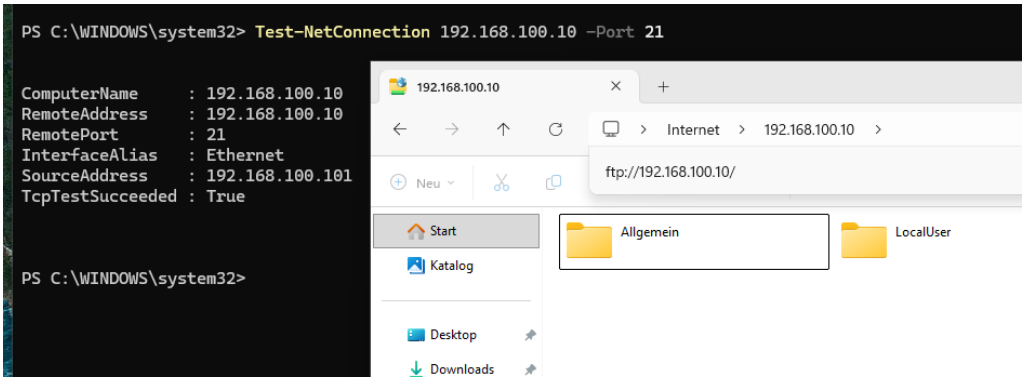
Port 21 prüfen

Vom Client:

Test-NetConnection 192.168.100.10 -Port 21

Erwartung:

TcpTestSucceeded: True



FTP im Explorer

ftp://192.168.100.10

FTP per CMD

ftp 192.168.100.10

Anmelden mit:

Benutzer:

m.mustermann

Passwort:

(dein AD-Passwort)