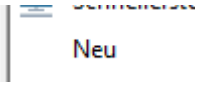
Inhalt

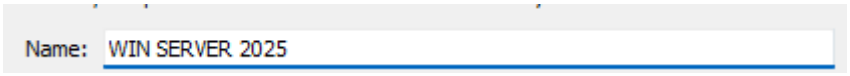
1.Server vorbereiten LABOR: Windows Server 2025 2
2. NAT + IP-Routing einrichten 5
RRAS – Routing und RAS-Dienst einrichten 6
Firewall für Routing konfigurieren 7
Aufgabe 3: Active Directory Domain Services 7
Aufgabe 4: DNS – intern und mit Internet-Weiterleitung 10
Forward-Lookupzone firma.local 10
Reverse-Lookupzone 11
DNS-Auflösung testen 11
Aufgabe 5 – DHCP-Server für das INTRANET 12
Aufgabe 7: Benutzer, Gruppen und Organisationseinheiten 16
Aufgabe 8: Freigaben und Berechtigungen (über Intranet) 18
Aufgabe 9: Gruppenrichtlinien 20
Aufgabe 10: IIS-Webserver (erreichbar über INTRANET) 24

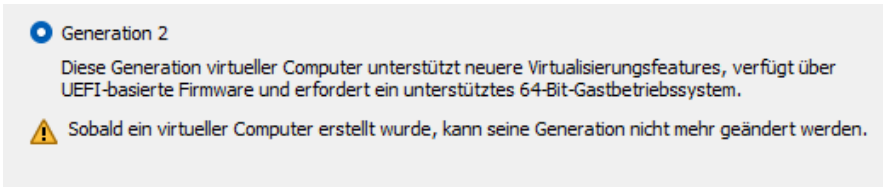
1.Server vorbereiten LABOR: Windows Server 2025

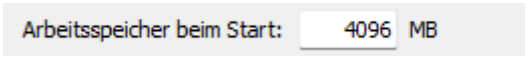
Windows Server 2025 Erstellen -> ISO-Download

Virtuelle Maschine unter Hyper V erstellen







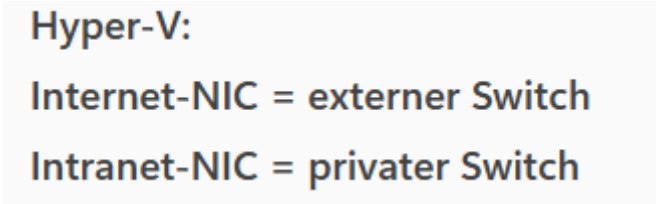


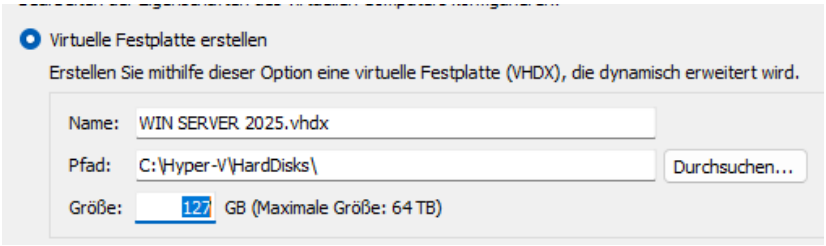
NIC	Zweck	Hyper-V Auswahl
NIC 1	Internet	LAN (Internet)
NIC 2	Intranet	Intranet

NIC 1 ->

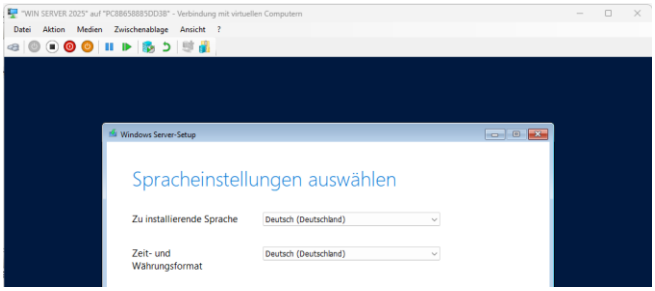


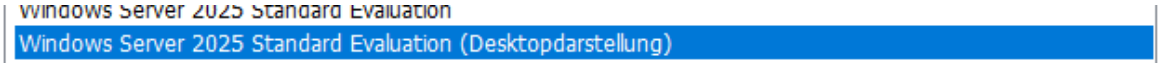
beim Erstellen ausgewählt

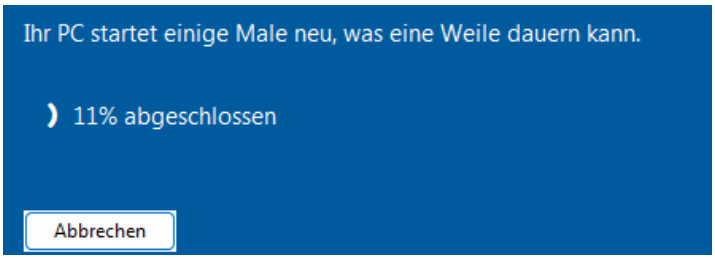


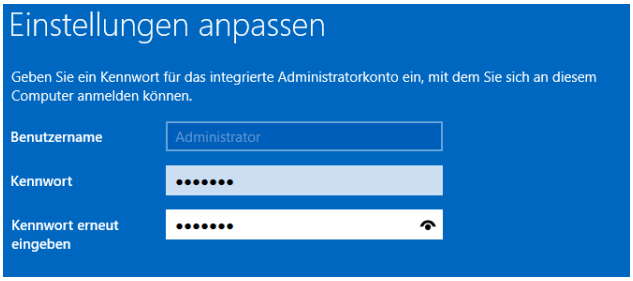


Name:	WIN SERVER 2025
Generation:	Generation 2
Arbeitsspeicher:	4096 MB
Netzwerk:	LAN (Internet)
Festplatte:	C:\Hyper-V\HardDisks\WIN SERVER 2025.vhdx (VHDX, dynamisch erweiterbar)
Betriebssystem:	Installation von "D:\ISO WIN11 2025\26100.1742.240906-0331.ge_release_svc_re





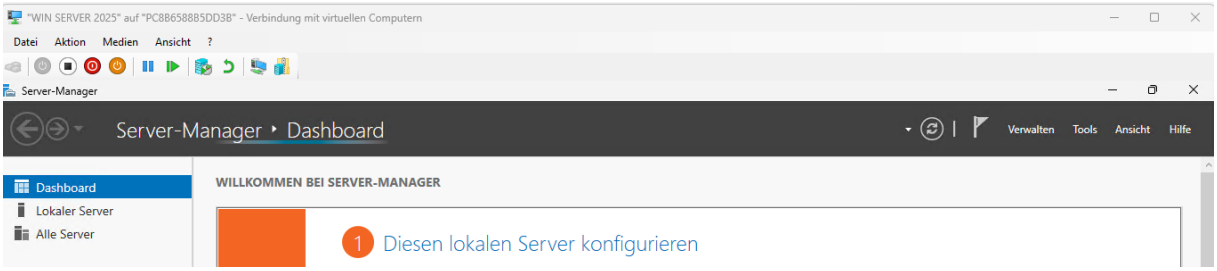




PW: Admin1!



Erst Einstieg im Server



Server IP +Subnetzmaske +Standardgateway

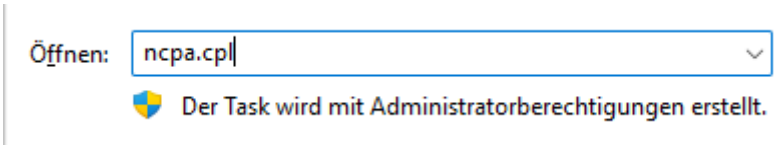
```
Ethernet-Adapter Ethernet:

   Verbindungsspezifisches DNS-Suffix: fritz.box
   IPv6-Adresse. . . . . . . . . . . . : fd2a:e6b1:5a9:0:ee95:1d70:aac6:5e82
   Verbindungslokale IPv6-Adresse  . . : fe80::3a97:ec37:ff4c:889d%6
   IPv4-Adresse  . . . . . . . . . . . : 10.0.0.44
   Subnetzmaske  . . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . . : 10.0.0.1
```

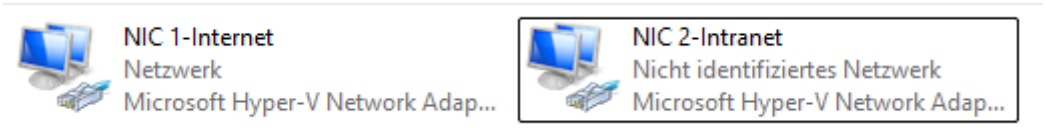
Name Server ändern auf SRV-DC01

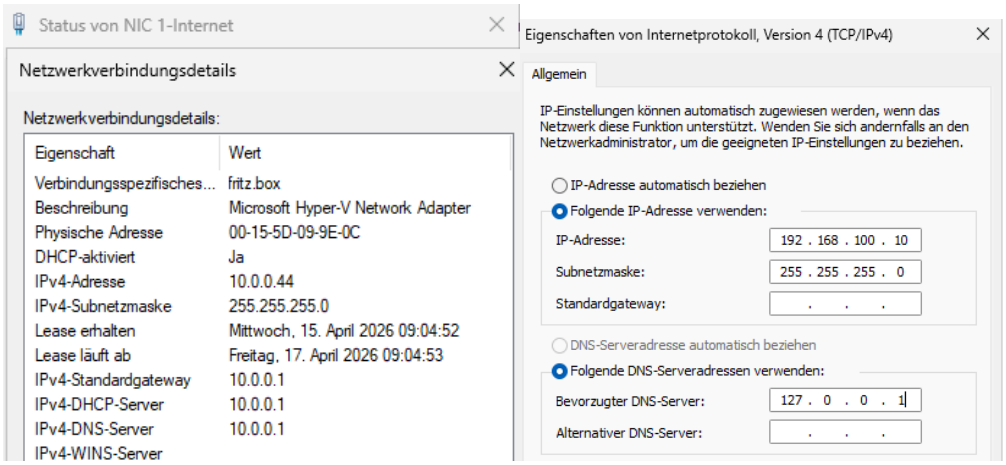


Weiter mit

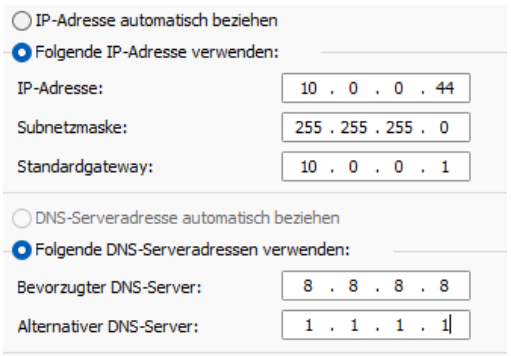


Zwei Karten sind ersichtlich – mit doppelklicken und Details sehe ich, welche ein IP mit 10.0.0.x gezogen hat, dann weiß ich, welche ich mit NIC-Internet bezeichnen muss.





NIC 1 laut meinem Labor angepasst NIC2 laut Plan (Aufgabenstellung)



Beide NICs und ihre IPs anzeigen:

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

```
InterfaceAlias IPv4Address      IPv4DefaultGateway
-------------- -----------      ------------------
NIC 1-Internet {10.0.0.44}      {MSFT_NetRoute (InstanceID = ":8:8:8:9:55;?55;:8:8:8;55;")}
NIC 2-Intranet {192.168.100.10}


PS C:\Users\Administrator> route print -4
===========================================================================
Schnittstellenliste
  6...00 15 5d 09 9e 0d ......Microsoft Hyper-V Network Adapter #2
 14...00 15 5d 09 9e 0c ......Microsoft Hyper-V Network Adapter
  1...........................Software Loopback Interface 1
===========================================================================
```

Routing-Tabelle prüfen - nur eine Default-Route (via NIC-INTERNET):

route print -4

```
IPv4-Routentabelle
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle Metrik
          0.0.0.0          0.0.0.0         10.0.0.1        10.0.0.44    291
         10.0.0.0    255.255.255.0   Auf Verbindung         10.0.0.44    291
        10.0.0.44  255.255.255.255   Auf Verbindung         10.0.0.44    291
       10.0.0.255  255.255.255.255   Auf Verbindung         10.0.0.44    291
        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
    192.168.100.0    255.255.255.0   Auf Verbindung    192.168.100.10    271
   192.168.100.10  255.255.255.255   Auf Verbindung    192.168.100.10    271
  192.168.100.255  255.255.255.255   Auf Verbindung    192.168.100.10    271
        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    192.168.100.10    271
        224.0.0.0        240.0.0.0   Auf Verbindung         10.0.0.44    291
  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    192.168.100.10    271
  255.255.255.255  255.255.255.255   Auf Verbindung         10.0.0.44    291
```

Internetverbindung vom Server testen:

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; Test-NetConnection -ComputerName google.com -Port 80

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

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 13ms, Maximum = 14ms, Mittelwert = 13ms


ComputerName     : google.com
RemoteAddress    : 142.251.14.102
RemotePort       : 80
InterfaceAlias   : NIC 1-Internet
SourceAddress    : 10.0.0.44
TcpTestSucceeded : True
```

2. NAT + IP-Routing einrichten

Windows-Kernel aktivieren

IP-Weiterleitung (IP Forwarding) dauerhaft aktivieren:

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

Sofort wirksam machen (ohne Neustart):
Set-NetIPInterface -Forwarding Enabled

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

```
PS C:\Users\Administrator> Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters' -Name 'IPEnableRouter' -Value 1 -Type DWord

PS C:\Users\Administrator> Set-NetIPInterface -Forwarding Enabled

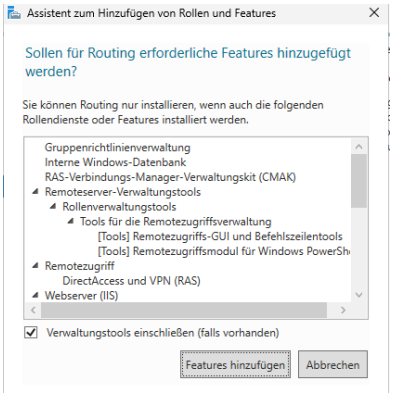
PS C:\Users\Administrator> Get-NetIPInterface | Select-Object InterfaceAlias, Forwarding | Format-Table -AutoSize

InterfaceAlias              Forwarding
--------------              ----------
NIC 2-Intranet                 Enabled
NIC 1-Internet                 Enabled
Loopback Pseudo-Interface 1    Enabled
NIC 2-Intranet                 Enabled
NIC 1-Internet                 Enabled
Loopback Pseudo-Interface 1    Enabled
```

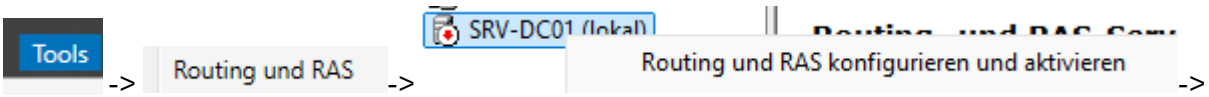
RRAS – Routing und RAS-Dienst einrichten



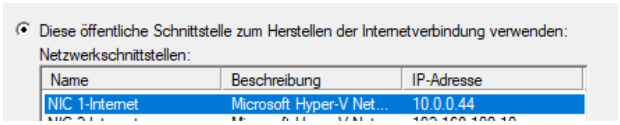
auswählen

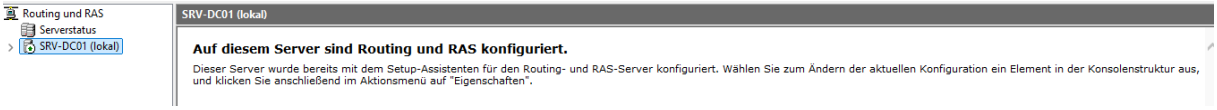






->





Firewall für Routing konfigurieren

ICMP (Ping) auf beiden NICs erlauben:

New-NetFirewallRule -DisplayName 'ICMP IPv4 eingehend' -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow

```
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName 'ICMP IPv4 eingehend' -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow


Name                          : {13633338-1c8e-49ce-a1f2-bed46a6a0429}
DisplayName                   : ICMP IPv4 eingehend
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

IP-Weiterleitung in der Firewall explizit erlauben:

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

```
PS C:\Users\Administrator> Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled True
```

RRAS-Dienst Autostart sicherstellen:

Set-Service -Name RemoteAccess -StartupType Automatic

Start-Service RemoteAccess

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


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

Ping wird ausgefhrt fr 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=14ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=14ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=14ms TTL=114
Antwort von 8.8.8.8: Bytes=32 Zeit=14ms TTL=114

Ping-Statistik fr 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 14ms, Maximum = 14ms, Mittelwert = 14ms
```

```
PS C:\Users\Administrator> Get-NetIPInterface | Select-Object InterfaceAlias, AddressFamily, Forwarding | Format-Table -AutoSize

InterfaceAlias              AddressFamily Forwarding
--------------              ------------- ----------
NIC 2-Intranet                       IPv6    Enabled
NIC 1-Internet                       IPv6    Enabled
Loopback Pseudo-Interface 1          IPv6    Enabled
NIC 2-Intranet                       IPv4    Enabled
NIC 1-Internet                       IPv4    Enabled
Loopback Pseudo-Interface 1          IPv4    Enabled
```

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

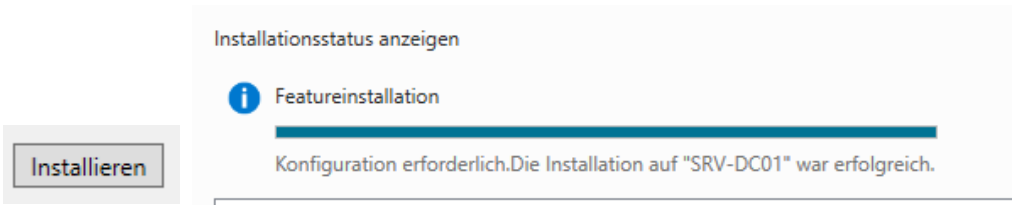
IP-EnableRouter = 1?

```
IPEnableRouter : 1
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
PSParentPath   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip
PSChildName    : Parameters
PSDrive        : HKLM
PSProvider     : Microsoft.PowerShell.Core\Registry
```

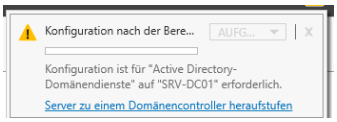
Aufgabe 3: Active Directory Domain Services

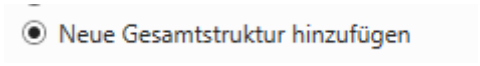
- AD-Rolle installieren

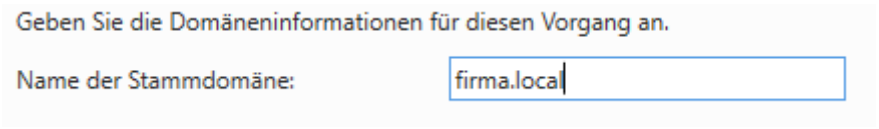


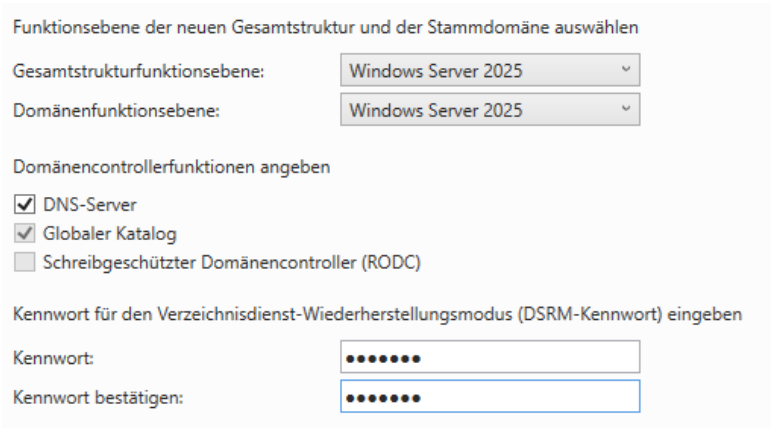


- Server zu einem Domänencontroller heraufstufen



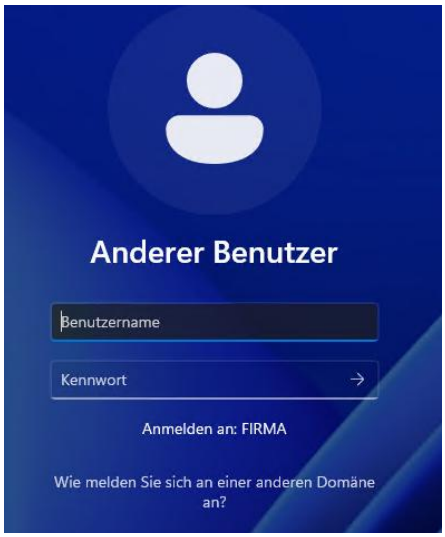






Admin1!

Anmelden in der Domäne

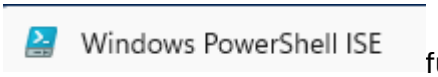


Administrator
Admin1!

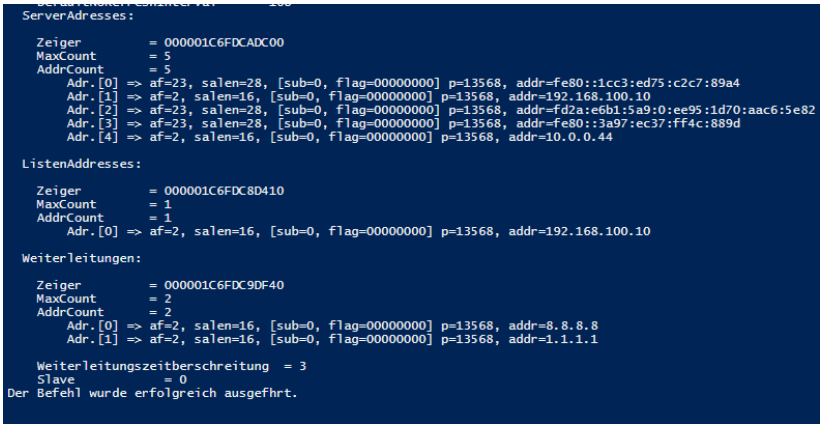
- DNS-Dienst auf eine bestimmte IP-Adresse festlegen:
  Cmd-Befehl

dnscmd /ResetListenAddresses 192.168.100.10

- Die Konfiguration prüfen:
  dnscmd /info | findstr Listen

im  funktioniert nur dieser Befehl

dnscmd /info



AD -Status prüfen

1.Zeigt Basisinfos zu deiner Domain (Name und Funktionslevel).

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

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

DNSRoot      NetBIOSName        DomainMode
-------      -----------        ----------
firma.local FIRMA       Windows2025Domain
```

Listet alle Domain Controller mit ihren IP-Adressen und Standorten (Sites) auf.

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

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

Name     IPv4Address    Site
----     -----------    ----
SRV-DC01 192.168.100.10 Default-First-Site-Name
```

Prüft die grundlegende Netzwerk-Konnektivität der Domain Controller.

dcdiag /test:connectivity

```
Erforderliche Anfangstests werden ausgefhrt.

   Server wird getestet: Default-First-Site-Name\SRV-DC01

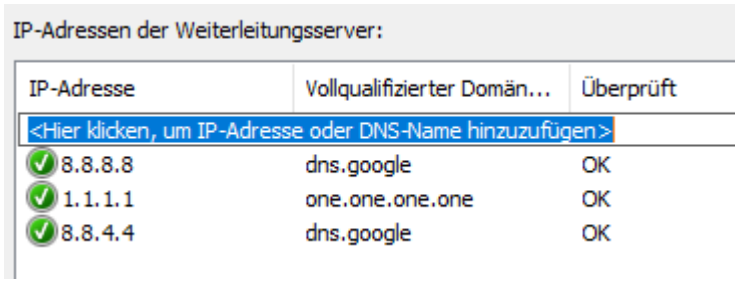
      Starting test: Connectivity

         ..... SRV-DC01 hat den Test Connectivity

         bestanden.
```

Aufgabe 4: DNS – intern und mit Internet-Weiterleitung

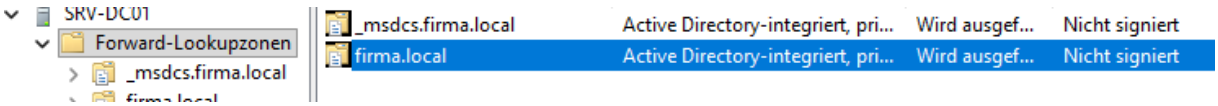
1. Öffne den **Server-Manager**
2. Gehe zu **Tools** → **DNS**
3. Rechtsklick auf **SRV-DC01 DNS Manager**
4. Wähle **Eigenschaften**
5. Wechsel zum Tab **Weiterleitungen**
6. Klicke auf **Bearbeiten**
7. Füge folgende DNS-Server hinzu:
   - **8.8.8.8** (Google – primärer Forwarder)
   - **8.8.4.4** (Google – sekundärer Forwarder)
   - **1.1.1.1** (Cloudflare – alternativer Forwarder)
8. Bestätige mit **OK** → **Übernehmen** → **OK**



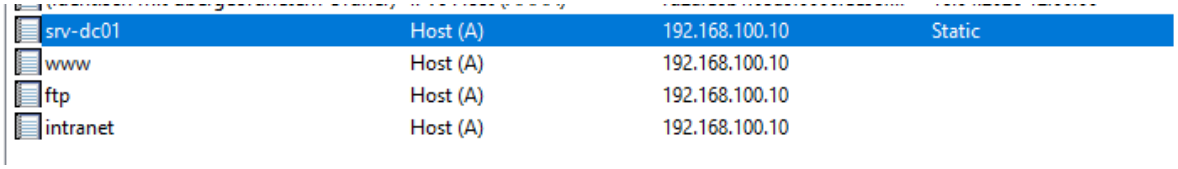
Forward-Lookupzone firma.local

Im DNS-Manager:

Forward-Lookupzonen



Auswählen -> Doppel klicken

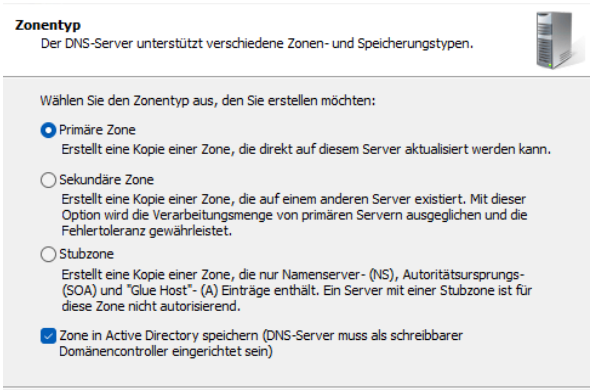


Rechtsklick in die Zone → **Neuer Host (A oder AAAA)**

Name	IP-Adresse	PTR	Zweck
www	192.168.100.10	Ja	Webserver (INTRANET)
ftp	192.168.100.10	Ja	FTP-Server (INTRANET)
intranet	192.168.100.10	Ja	Intranet-Alias
srv-dc01	192.168.100.10	Ja	Servername (prüfen)

Reverse-Lookupzone

im DNS-Manager:
Reverse-Lookupzonen → Rechtsklick → Neue Zone

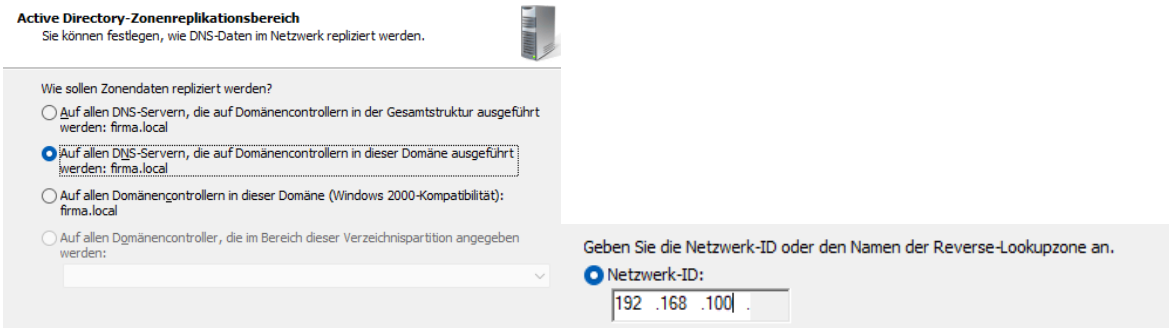


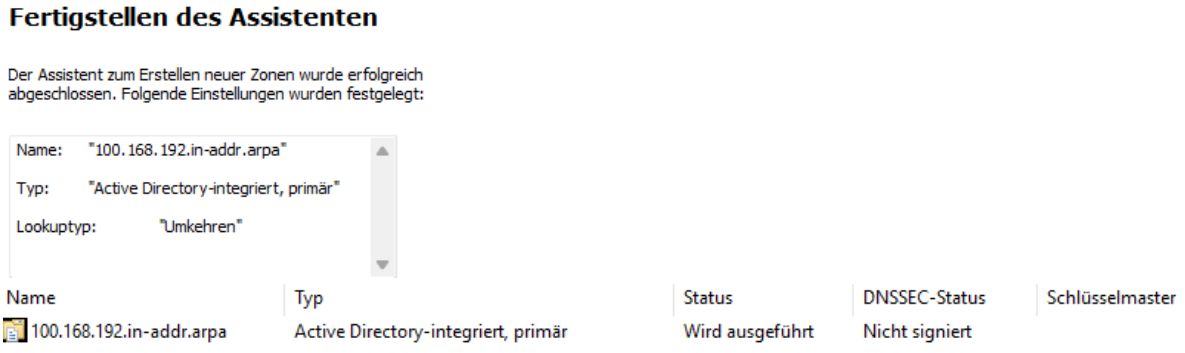
Einstellungen:

- **Primäre Zone**
- **AD-integriert**

Netzwerk-ID eingeben:
192.168.100

Assistent abschließen





DNS-Auflösung testen

Intern testen – muss die INTRANET-IP zurückgeben:

Resolve-DnsName www.firma.local -Server 192.168.100.10

```
PS C:\Users\Administrator> Resolve-DnsName www.firma.local -Server 192.168.100.10

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.firma.local                                A      3600  Answer     192.168.100.10
```

Resolve-DnsName srv-dc01.firma.local

Extern testen – Forwarder muss funktionieren:

Resolve-DnsName google.com -Server 192.168.100.10

```
PS C:\Users\Administrator> Resolve-DnsName google.com -Server 192.168.100.10

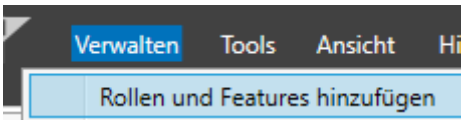
Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::71
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::64
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::66
google.com                                     AAAA   299   Answer     2a00:1450:4001:c15::65
google.com                                     A      299   Answer     142.251.14.102
google.com                                     A      299   Answer     142.251.14.100
google.com                                     A      299   Answer     142.251.14.101
google.com                                     A      299   Answer     142.251.14.138
google.com                                     A      299   Answer     142.251.14.139
google.com                                     A      299   Answer     142.251.14.113
```

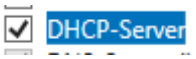
Resolve-DnsName microsoft.com

```
PS C:\Users\Administrator> Resolve-DnsName microsoft.com

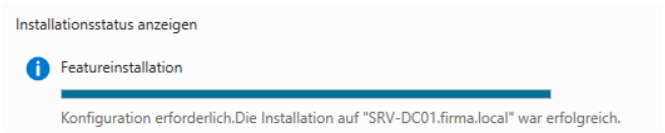
Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
microsoft.com                                  AAAA   2989  Answer     2620:1ec:48:1::45
microsoft.com                                  AAAA   2989  Answer     2620:1ec:29:1::45
microsoft.com                                  A      880   Answer     13.107.226.45
microsoft.com                                  A      880   Answer     13.107.253.45
```

Aufgabe 5 – DHCP-Server für das INTRANET





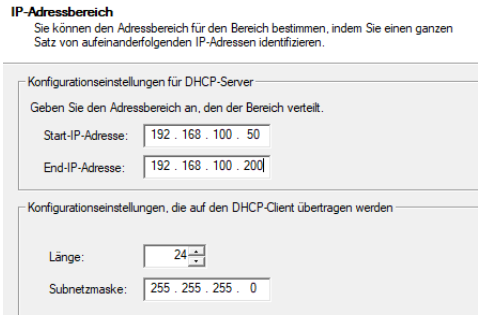
auswählen

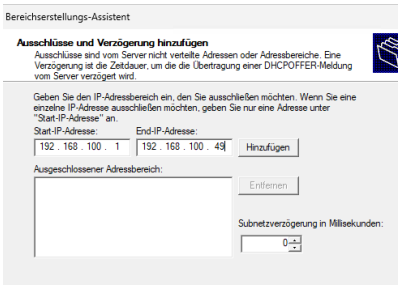


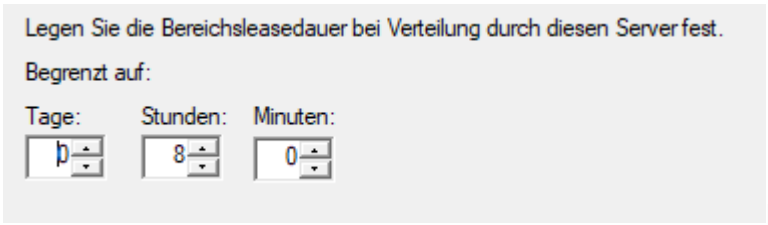
Servermanager -> Tools -> IPV4 -> Rechtsklick -> Neuer Bereich



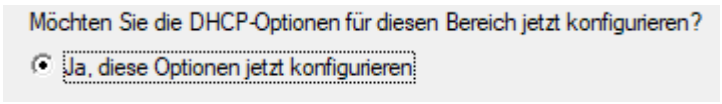
Ausschlüsse:





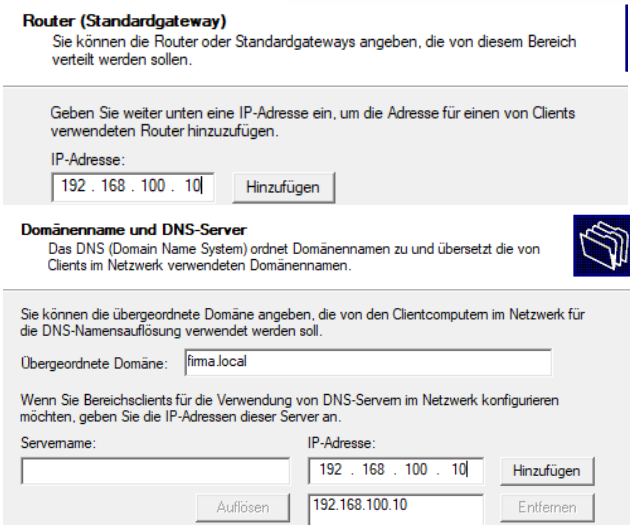


Leasedauer 8h

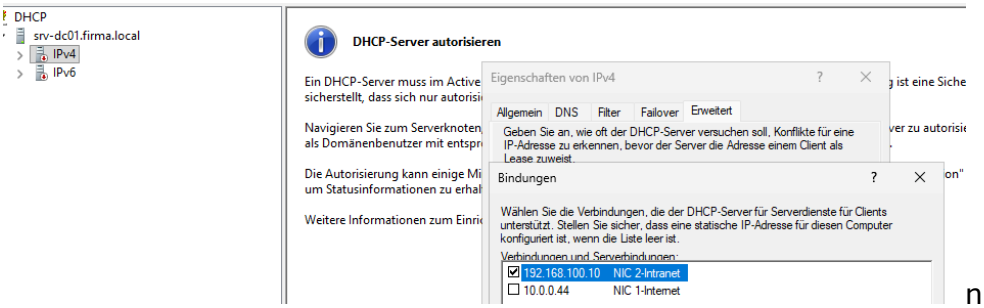


Option003

Option006



DHCP nur an NIC-INTRANET binden



nur NIC2 Intranet

Kontrolle per PowerShell

```
PS C:\Users\Administrator> Get-DhcpServerv4Binding

InterfaceAlias                          IPAddress              BindingState
--------------                          ---------              ------------
NIC 2-Intranet                          192.168.100.10         True
NIC 1-Internet                          10.0.0.44              False
```

Server Kontrolle Ipconfig

```
Windows-IP-Konfiguration

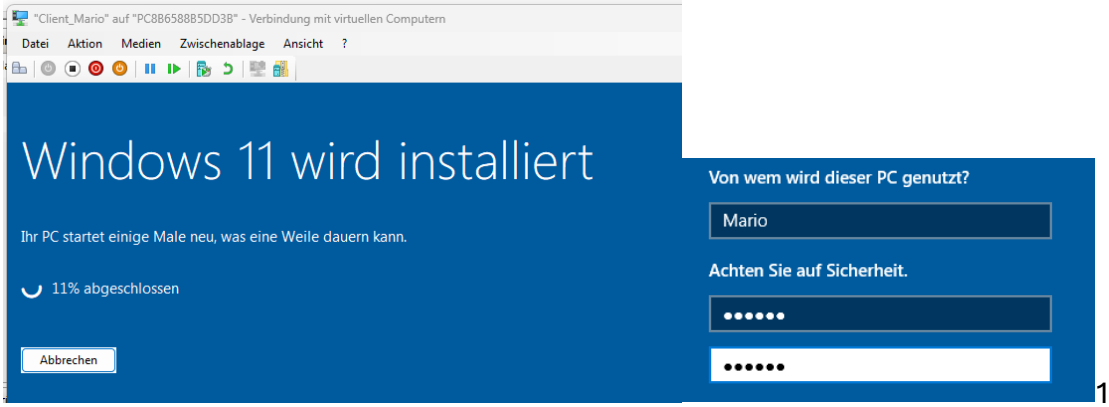

Ethernet-Adapter NIC 2-Intranet:

   Verbindungsspezifisches DNS-Suffix:
   Verbindungslokale IPv6-Adresse  . : fe80::1cc3:ed75:c2c7:89a4%6
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.10
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . :

Ethernet-Adapter NIC 1-Internet:

   Verbindungsspezifisches DNS-Suffix:
   IPv6-Adresse. . . . . . . . . . . : fd2a:e6b1:5a9:0:ee95:1d70:aac6:5e82
   Verbindungslokale IPv6-Adresse  . : fe80::3a97:ec37:ff4c:889d%14
   IPv4-Adresse  . . . . . . . . . . : 10.0.0.44
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 10.0.0.1
```

Windows 11 Client auf Hyper V erstellt



123456

Domänenbeitritt und IP-Prüfen

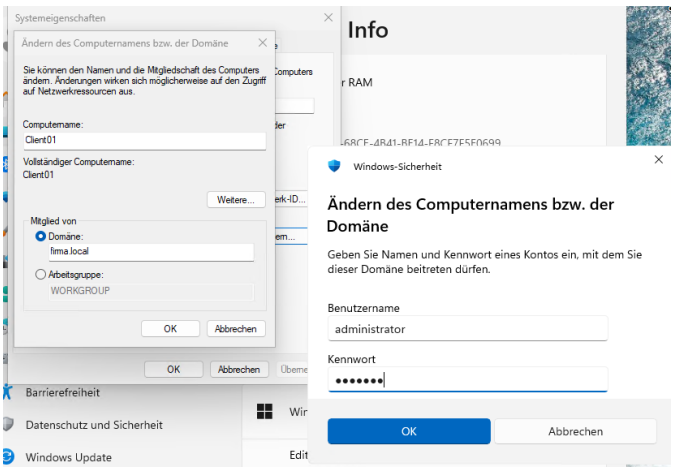
```
Ethernet-Adapter Ethernet:

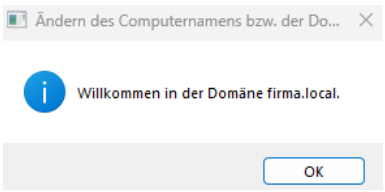
   Verbindungsspezifisches DNS-Suffix: firma.local
   Verbindungslokale IPv6-Adresse  . : fe80::9968:bc25:9809:e282%11
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.51
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . :
```

```
C:\Users\Mario>ipconfig /all | findstr Physisch
   Physische Adresse . . . . . . . . : 00-15-5D-09-9E-0E
```

```
Ethernet-Adapter Ethernet:

   Verbindungsspezifisches DNS-Suffix: firma.local
   Beschreibung. . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physische Adresse . . . . . . . . : 00-15-5D-09-9E-0E
   DHCP aktiviert. . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . : Ja
   Verbindungslokale IPv6-Adresse  . : fe80::9968:bc25:9809:e282%11(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.51(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Lease erhalten. . . . . . . . . . : Mittwoch, 22. April 2026 09:24:52
   Lease läuft ab. . . . . . . . . . : Mittwoch, 22. April 2026 17:24:52
   Standardgateway . . . . . . . . . :
   DHCP-Server . . . . . . . . . . . : 192.168.100.10
   DHCPv6-IAID . . . . . . . . . . . : 83891549
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-31-7A-2E-A3-00-15-5D-09-9E-0E
   DNS-Server  . . . . . . . . . . . : 192.168.100.10
                                       192.168.100.10
   NetBIOS über TCP/IP . . . . . . . : Aktiviert
```






```
Ethernet-Adapter Ethernet:

   Verbindungsspezifisches DNS-Suffix:
   Verbindungslokale IPv6-Adresse  . : fe80::9968:bc25:9809:e282%11
   Standardgateway . . . . . . . . . :

C:\Windows\System32>ipconfig /renew

Windows-IP-Konfiguration


Ethernet-Adapter Ethernet:

   Verbindungsspezifisches DNS-Suffix: firma.local
   Verbindungslokale IPv6-Adresse  . : fe80::9968:bc25:9809:e282%11
   IPv4-Adresse  . . . . . . . . . . : 192.168.100.51
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 192.168.100.10
```

6.2 Routing-Test: Internet über den Server funktioniert

Trace-Tabelle

```
 1    <1 ms     *       <1 ms  SRV-DC01.firma.local [192.168.100.10]
 2     *        *        *     Zeitüberschreitung der Anforderung.
 3     1 ms     1 ms     1 ms  10.0.0.1
 4     2 ms     1 ms     1 ms  10.170.17.254
 5     4 ms     3 ms     3 ms  10.170.0.6
 6    40 ms    42 ms    32 ms  10.170.0.1
 7    20 ms    19 ms    29 ms  85.31.21.253
 8    31 ms    22 ms    35 ms  we.corou0008.as21013.net [80.243.161.85]
 9    29 ms    29 ms    33 ms  fra.corou0010.as21013.net [80.243.161.101]
10     *        *        *     Zeitüberschreitung der Anforderung.
11    26 ms    21 ms    22 ms  209.85.244.249
12    20 ms    19 ms    33 ms  142.250.209.243
13    34 ms    22 ms    22 ms  dns.google [8.8.8.8]
```

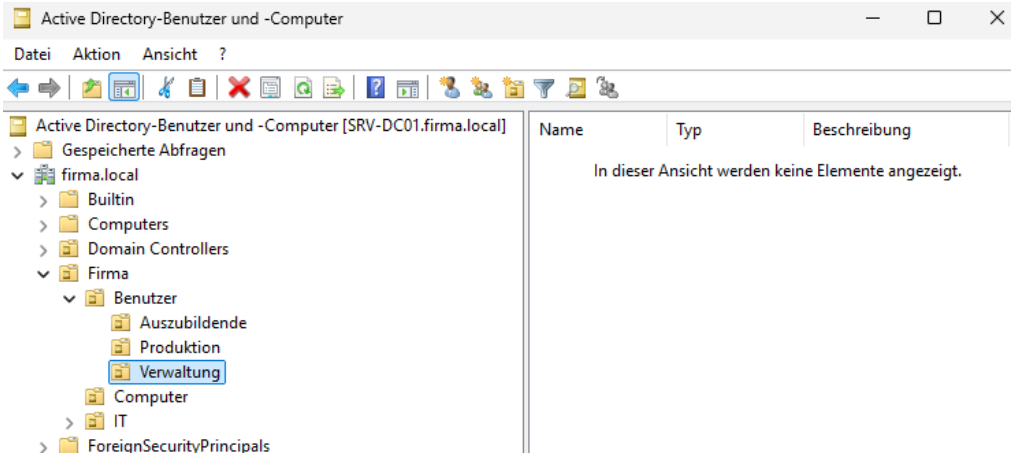
Reservierung für Client 5.4 von vorhin einen Punkt zurück!!!

```
C:\Windows\System32>ipconfig /all | findstr Physisch
   Physische Adresse . . . . . : 00-15-5D-09-9E-0E
```

Aufgabe 7: Benutzer, Gruppen und Organisationseinheiten

OU-Struktur per PowerShell anlegen

New-ADOrganizationalUnit -Name "Firma" -Path "DC=firma,DC=local"
New-ADOrganizationalUnit -Name "Benutzer" -Path "OU=Firma,DC=firma,DC=local"
New-ADOrganizationalUnit -Name "IT" -Path "OU=Firma,DC=firma,DC=local"
New-ADOrganizationalUnit -Name "Verwaltung" -Path
"OU=Benutzer,OU=Firma,DC=firma,DC=local"
New-ADOrganizationalUnit -Name "Produktion" -Path
"OU=Benutzer,OU=Firma,DC=firma,DC=local"
New-ADOrganizationalUnit -Name "Auszubildende" -Path
"OU=Benutzer,OU=Firma,DC=firma,DC=local"
New-ADOrganizationalUnit -Name "Computer" -Path "OU=Firma,DC=firma,DC=local"



Benutzer anlegen

```
# Passwort definieren
$pw = ConvertTo-SecureString "123456" -AsPlainText -Force

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

# Benutzer erstellen
foreach ($u in $users) {
  New-ADUser `
    -Name $u.Name `
    -SamAccountName $u.Sam `
    -UserPrincipalName "$($u.Sam)@firma.local" `
    -Path "OU=$($u.OU),OU=Benutzer,OU=Firma,DC=firma,DC=local" `
    -AccountPassword $pw `
    -Enabled $true
}
```

Gruppen anlegen

```
$path = "OU=Gruppen,OU=Firma,DC=firma,DC=local"

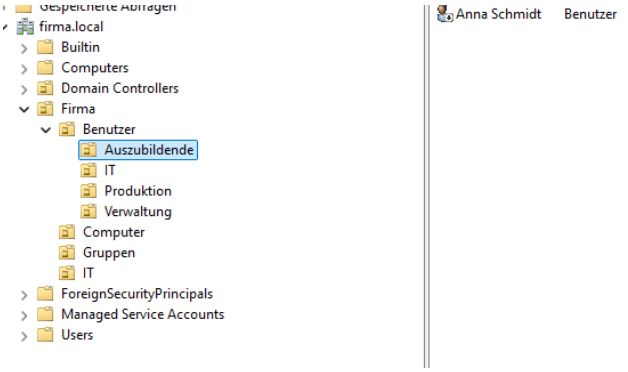
# OU für Gruppen (falls noch nicht vorhanden)
New-ADOrganizationalUnit -Name "Gruppen" -Path "OU=Firma,DC=firma,DC=local"

# Gruppen erstellen
New-ADGroup -Name "GRP-IT" -GroupScope Global -Path $path
New-ADGroup -Name "GRP-Verwaltung" -GroupScope Global -Path $path
New-ADGroup -Name "GRP-Azubis" -GroupScope Global -Path $path

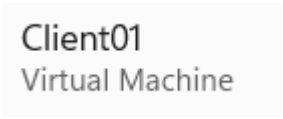
# Neue Gruppe erstellen
New-ADGroup -Name 'GRP-Alle' -GroupScope Global -Path $oPath

# Mitglieder zu bestehenden 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'
```



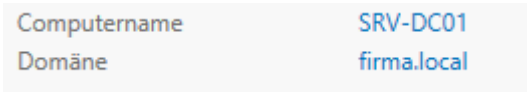
7.4 PC -Client01 in die OU verschieben



Computer aus 'Computers' in die richtige OU verschieben:

```
Get-ADComputer 'CLIENT01' | Move-ADObject -TargetPath 'OU=Computer,OU=Firma,DC=firma,DC=local'
```

Aufgabe 8: Freigaben und Berechtigungen (über Intranet)




```
PS C:\Users\Administrator> Get-AdGroup -Identity "Domänen-Admins"


DistinguishedName : CN=Domänen-Admins,CN=Users,DC=firma,DC=local
GroupCategory     : Security
GroupScope        : Global
Name              : Domänen-Admins
ObjectClass       : group
ObjectGUID        : 05bb84b8-0196-4534-9afd-d8c5edb3c329
SamAccountName    : Domänen-Admins
SID               : S-1-5-21-3100771535-1295469216-3197283694-512
```

Schritt 8.1: Ordnerstruktur auf dem Server erstellen

Erstellt das Hauptverzeichnis und die Unterordner

```
New-Item -ItemType Directory -Path 'C:\Freigaben\Allgemein' -Force
New-Item -ItemType Directory -Path 'C:\Freigaben\IT' -Force
New-Item -ItemType Directory -Path 'C:\Freigaben\Verwaltung' -Force
New-Item -ItemType Directory -Path 'C:\Freigaben\Azubis' -Force
```

Schritt 8.2: SMB-Freigaben anlegen

Jetzt geben wir diese Ordner im Netzwerk frei und legen fest, wer darauf zugreifen darf.

 # Freigabe Allgemein: Jeder in der Gruppe GRP-Alle darf lesen/schreiben

```
Name      ScopeName Path                  Description
----      --------- ----                  -----------
Allgemein *         C:\Freigaben\Allgemein
```

```
New-SmbShare -Name 'Allgemein' -Path 'C:\Freigaben\Allgemein' `
-FullAccess 'FIRMA\Domänen Admins' `
-ChangeAccess 'FIRMA\GRP-Alle'
```

 # Freigabe IT: Nur die IT-Gruppe darf zugreifen

```
Name ScopeName Path           Description
---- --------- ----           -----------
IT   *         C:\Freigaben\IT
```

```
New-SmbShare -Name 'IT' -Path 'C:\Freigaben\IT' `
-FullAccess 'FIRMA\Domänen-Admins' `
-ChangeAccess 'FIRMA\GRP-IT' `
-NoAccess 'Jeder'
```

 # Freigabe Verwaltung: Nur Admins und Verwaltung

```
Name       ScopeName Path                  Description
----       --------- ----                  -----------
Verwaltung *         C:\Freigaben\Verwaltung
```

```
New-SmbShare -Name 'Verwaltung' -Path 'C:\Freigaben\Verwaltung' `
-FullAccess 'FIRMA\Domänen-Admins', 'FIRMA\GRP-Verwaltung' `
-NoAccess 'Jeder'
```

 # Freigabe Azubis: Admins voll, Azubis dürfen lesen/schreiben

```
Name   ScopeName Path                Description
----   --------- ----                -----------
Azubis *         C:\Freigaben\Azubis
```

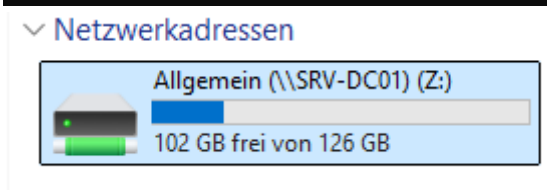
```
New-SmbShare -Name 'Azubis' -Path 'C:\Freigaben\Azubis' `
-FullAccess 'FIRMA\Domänen-Admins' `
-ChangeAccess 'FIRMA\GRP-Azubis'
```

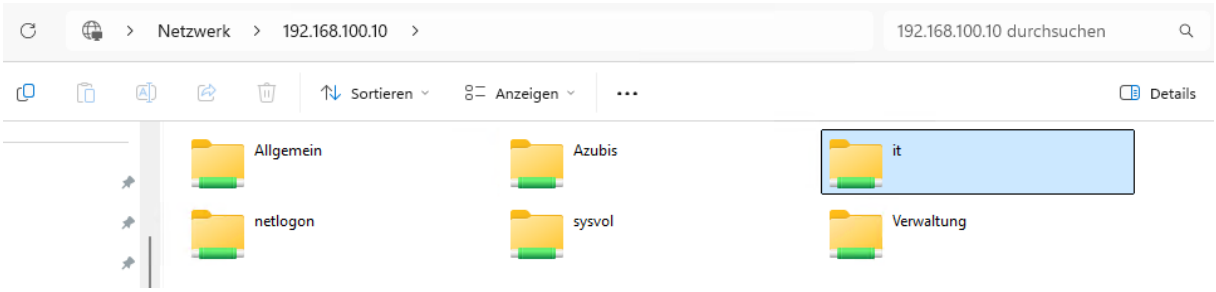
Schritt 8.3: Freigaben vom Client testen

```
C:\Users\m.mustermann>net view \\SRV-DC01
Freigegebene Ressourcen auf \\SRV-DC01


Freigabename  Typ     Verwendet als  Kommentar

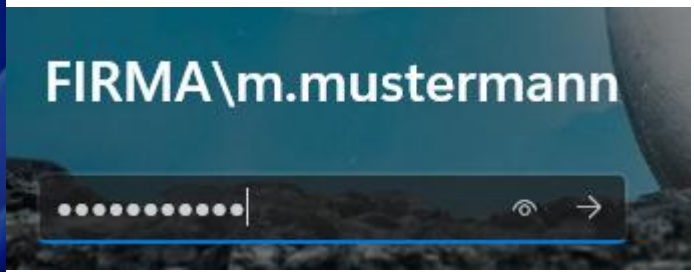
-------------------------------------------------------------------------------
Allgemein     Platte  Z:
Azubis        Platte
IT            Platte
NETLOGON      Platte                 Ressource für Anmeldeserver
SYSVOL        Platte                 Ressource für Anmeldeserver
Verwaltung    Platte
Der Befehl wurde erfolgreich ausgeführt.
```





Neues Passwort max.mustermann = Mittwoch01#

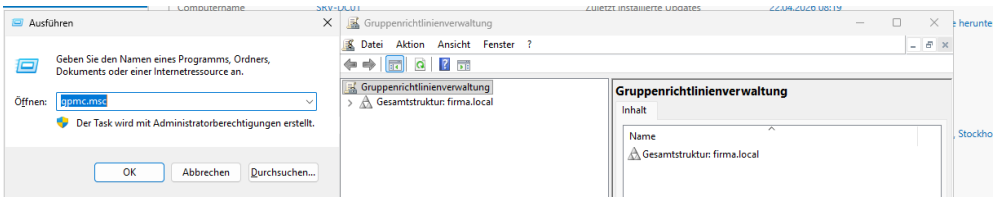




In der einfachen Sitzung anmelden sonst Remote Meldung Fehler

Aufgabe 9: Gruppenrichtlinien

WIN+R = gpmc.msc



Neue GPO erstellen ->

1. Rechtsklick auf **firma. local**
2. **Neues GPO erstellen**
3. Name: Kennwortrichtlinie-Firma

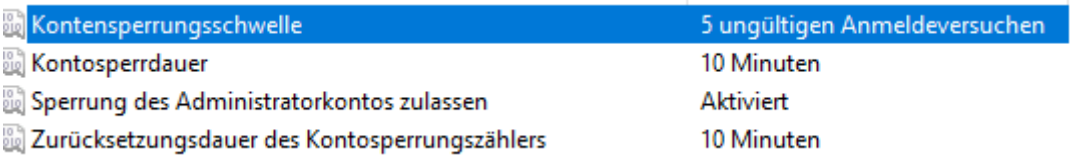
GPO bearbeiten

Ablauf: genau

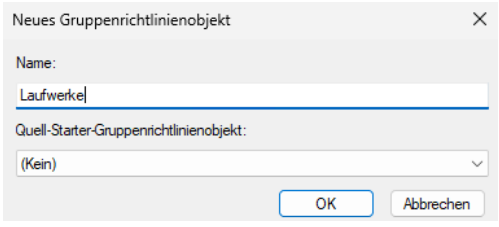
Computerkonfiguration
└ Richtlinien
  └ Windows-Einstellungen
    └ Sicherheitseinstellungen
      └ Kontorichtlinien
        └ Kennwortrichtlinien

Richtlinie	Wert
Minimale Kennwortlänge	12 Zeichen
Maximales Kennwortalter	90 Tage
Kennwort muss Komplexitätsvoraussetzungen erfüllen	Aktiviert
Kontosperrschwelle	5 Versuche
Kontosperrdauer	30 Minuten

Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen	Nicht definiert
Kennwörter mit umkehrbarer Verschlüsselung speichern	Nicht definiert
Kennwortlängenbeschränkungen lockern	Nicht definiert
Maximales Kennwortalter	90 Tage
Minimale Kennwortlänge	12 Zeichen
Minimales Kennwortalter	30 Tage
Überwachung der Mindestpasswortlänge	Nicht definiert



9.2 Laufwerk **Z:** per GPO verbinden

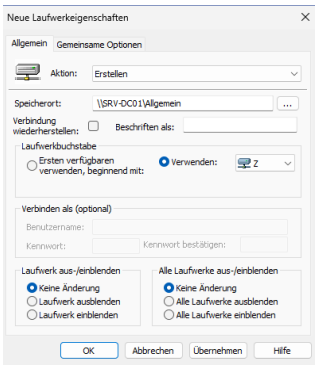


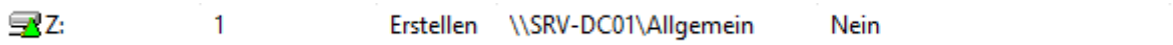


Klicken -> rechte Maustaste -> bearbeiten

GPO bearbeiten

Benutzerkonfiguration
└ Einstellungen
  └ Windows-Einstellungen
    └ Laufwerkzuordnungen -> Rechtsklick NEU

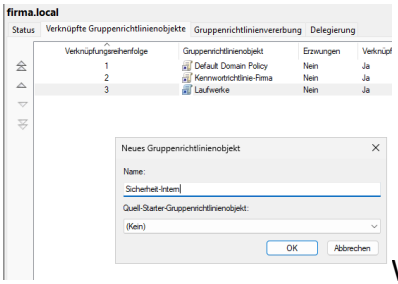




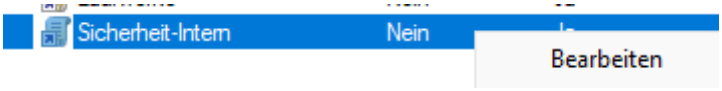
9.3 Sicherheits-GPO

wieder unter Gruppenrichtlinienverwaltung

Rechtsklick auf **OU Firma\Benutzer** → **Neues GPO**

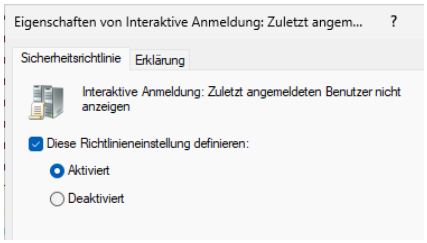


Wieder Rechtsklick bearbeiten



Letzten Benutzernamen nicht anzeigen

```
1  Computerkonfiguration
2   └ Richtlinien
3     └ Windows-Einstellungen
4       └ Sicherheitseinstellungen
5         └ Lokale Richtlinien
6           └ Sicherheitsoptionen
```



Dann ->

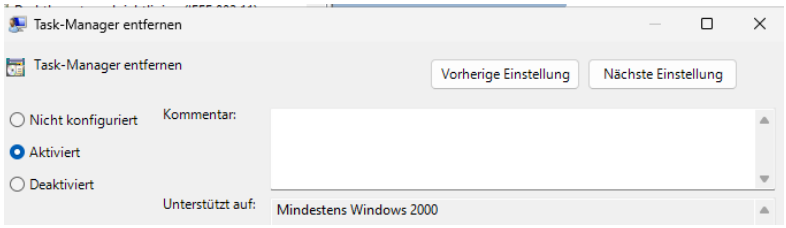


Dann



❌ Task-Manager deaktivieren

Benutzerkonfiguration
└ Richtlinien
  └ Administrative Vorlagen
    └ System
      └ Strg+Alt+Entf-Optionen



🌐 Netzwerkverbindungen deaktivieren

Benutzerkonfiguration
└ Richtlinien
  └ Administrative Vorlagen
    └ Netzwerk
      └ Netzwerkverbindungen





GPO anwenden und testen

```
C:\Users\m.mustermann>gpupdate /force
```

```
C:\Users\m.mustermann>gpresult /r

Betriebssystem Microsoft (R) Windows (R) Gruppenrichtlinienergebnis-Tool v2
© Microsoft Corporation. Alle Rechte vorbehalten.

Am 29.04.2026 um 10:18:58 erstellt


RSOP-Daten für FIRMA\m.mustermann auf CLIENT01: Protokollmodus
-------------------------------------------------------------

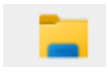
Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion:       10.0.26200
Standortname:                Nicht zutreffend
Roamingprofil:Nicht zutreffend
Lokales Profil:              C:\Users\m.mustermann
Langsame Verbindung?         Nein


BENUTZEREINSTELLUNGEN
---------------------
    CN=Max Mustermann,OU=IT,OU=Benutzer,OU=Firma,DC=firma,DC=local
    Letzte Gruppenrichtlinienanwendung:   29.04.2026, um 10:18:56
    Gruppenrichtlinieanwendung von:       SRV-DC01.firma.local
    Schwellenwert für langsame Verbindung:500 kbps
    Domänenname:                          FIRMA
    Domänentyp:                           Windows 2008 oder höher
```

```
Angewendete Gruppenrichtlinienobjekte
-------------------------------------
    Laufwerke
    Sicherheit-Intern

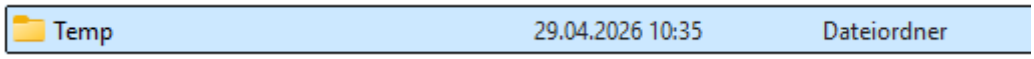
Folgende herausgefilterte Gruppenrichtlinien werden nicht angewendet.
----------------------------------------------------------------------
    Richtlinien der lokalen Gruppe
        Filterung:  Nicht angewendet (Leer)

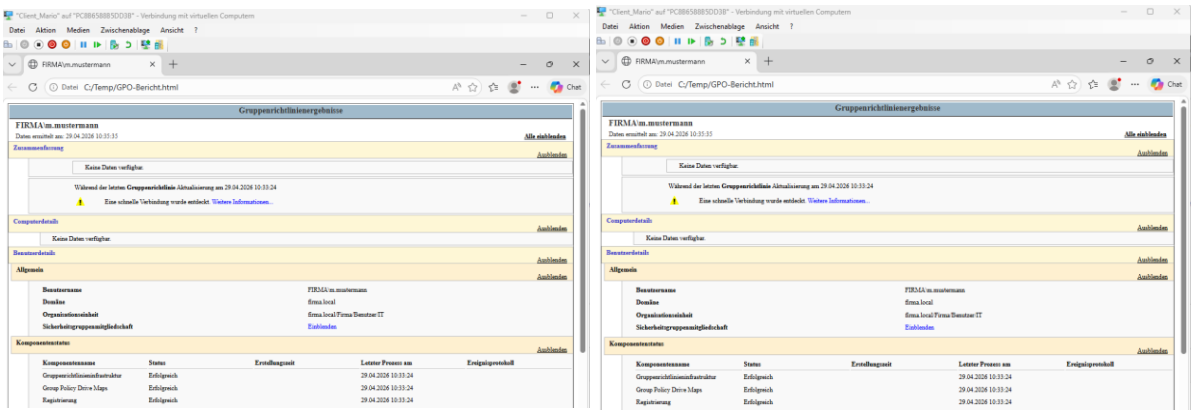
Der Benutzer ist Mitglied der folgenden Sicherheitsgruppen
----------------------------------------------------------
    Domänen-Benutzer
    Jeder
    Benutzer
    INTERAKTIV
    KONSOLENANMELDUNG
    Authentifizierte Benutzer
    Diese Organisation
    LOKAL
    GRP-IT
    GRP-Alle
    Von der Authentifizierungsstelle bestätigte ID
    Mittlere Verbindlichkeitsstufe
```

C: Temp Ordner erstellt 

gpresult /h C:\Temp\GPO-Bericht.html

```
C:\Users\m.mustermann>gpresult /h C:\Temp\GPO-Bericht.html
```







Aufgabe 10: IIS-Webserver (erreichbar über INTRANET)

Der **IIS-Webserver** steht für **Internet Information Services**

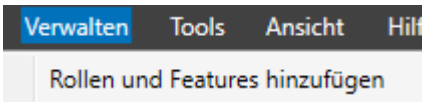
Ausgangssituation (wichtig)

- Server hat **2 Netzwerkkarten**:
  - **INTRANET-NIC:** `192.168.100.10`
  - **INTERNET-NIC:** öffentliche oder andere externe IP
- Ziel:
  - IIS-Website **nur intern erreichbar**
  - Kein Zugriff über Internet-NIC
  - Zugriff **ausschließlich über INTRANET-IP**

10.1 IIS installieren

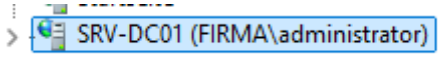
Schritt 1: Server-Manager öffnen

Start → **Server-Manager**

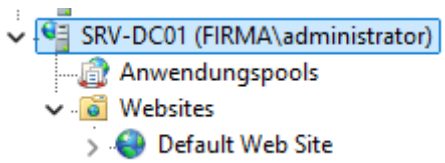


IIS-Manager öffnen

Hier klicken



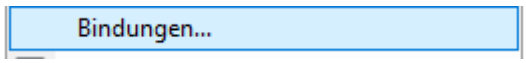
Pfeil links klicken um Websites zu sehen

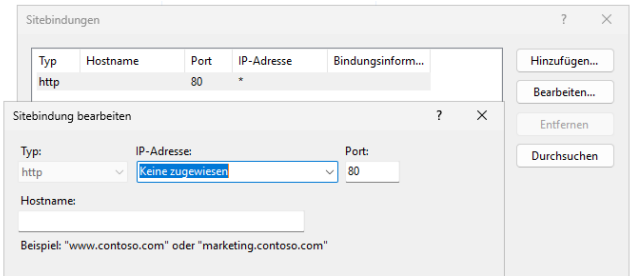


Default Web Site auswählen

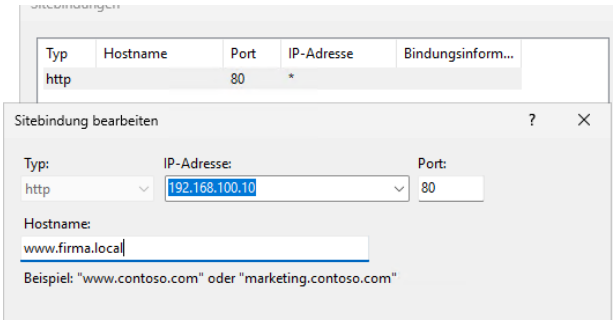
- Links: Sites
- Klick auf Default Web Site







192.168.100.10



10.3 Intranet Startseite erstellen

Ordner sicherstellen

```
New-Item -ItemType Directory -Path "C:\inetpub\wwwroot" -Force
```

HTML-Datei erstellen:

```
notepad C:\inetpub\wwwroot\index.html
```

```
<!DOCTYPE html>
<html lang="de">
<head>
<meta charset="UTF-8">
<title>Firma Intranet</title>
<style>
body { font-family: Arial; background:#f0f4f8; margin:0; }
header { background:#1565c0; color:white; padding:20px; text-align:center; }
main { max-width:900px; margin:20px auto; padding:20px; }
.box {
  background:white;
  padding:20px;
  margin-bottom:15px;
  border-radius:8px;
  box-shadow:0 2px 5px rgba(0,0,0,0.1);
}
footer {
  text-align:center;
  color:#888;
  padding:20px;
}
</style>
</head>
<body>

<header>
  <h1>Firma Intranet</h1>
  <p>Interne Seite</p>
</header>

<main>
  <div class="box">
    <h2>Schnellzugriff</h2>
    <p>Server-IP: 192.168.100.10</p>
  </div>

  <div class="box">
    <h3>Support</h3>
    <p>IT-Abteilung erreichbar intern</p>
```

```
 </div>

 <div class="box">
  <h3>Dateien</h3>
  <p>\\fileserver\share</p>
 </div>
</main>

<footer>
 Firma GmbH © 2026
</footer>

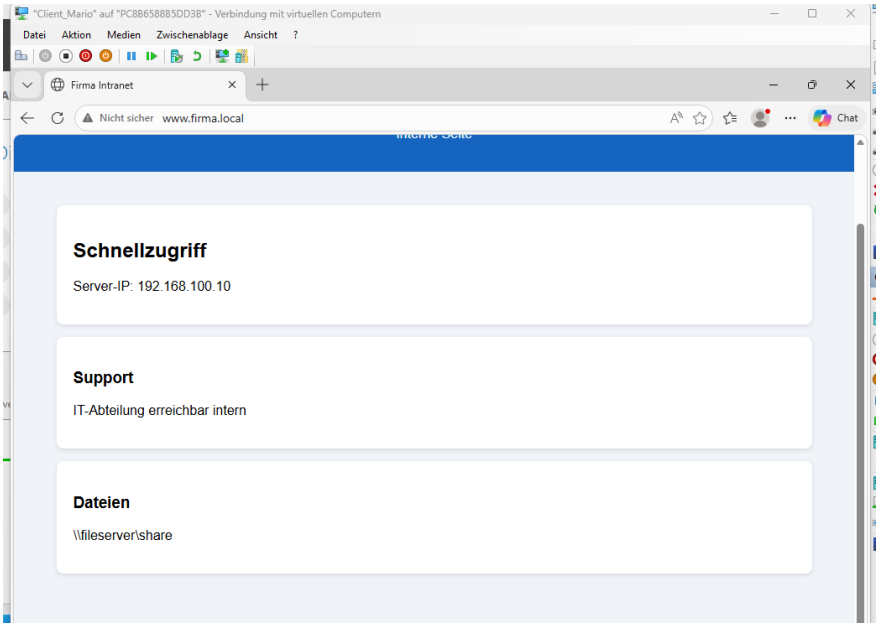
</body>
</html>
```

IIS neu starten: (Powershell) iisreset

10.4 http-Zugriff auf INTRANET per Firewall sichern

```
# Nur INTRANET darf auf Port 80 zugreifen:
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

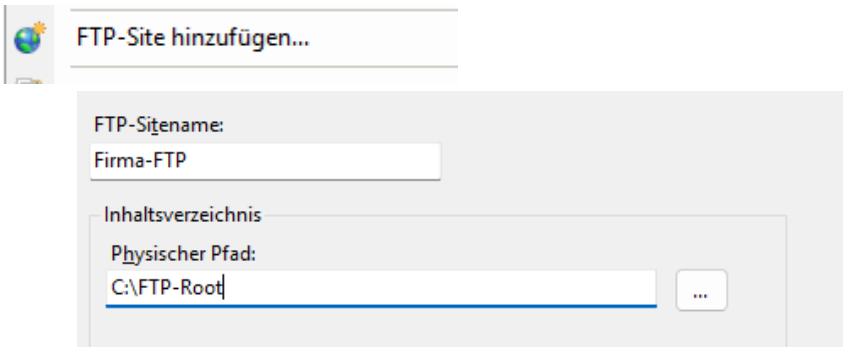
# Zugriff von INTERNET-Seite auf Port 80 blockieren:
New-NetFirewallRule -DisplayName 'HTTP INTERNET blockieren' -Direction Inbound `
  -Protocol TCP -LocalPort 80 `
  -LocalAddress 10.0.0.10 `
  -Action Block
```



Aufgabe11: FTP -SERVER (Intranet-only)

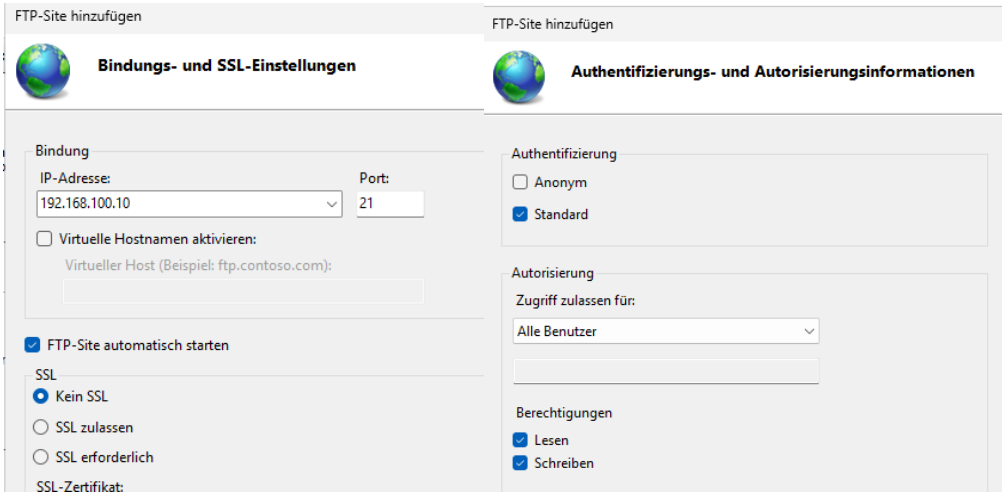
FTP-Dienste sind schon installiert sonst unter Rollendienste nachinstallieren.

ISS Manager öffnen



Ordner korrekt erstellen:
New-Item -ItemType Directory -Path "C:\FTP-Root" -Force

Prüfen, ob der Ordner wirklich existiert:
Test-Path "C:\FTP-Root"



📁 2. Ordnerstruktur erstellen

New-Item -ItemType Directory -Path "C:\FTP-Root" -Force
New-Item -ItemType Directory -Path "C:\FTP-Root\Allgemein" -Force
New-Item -ItemType Directory -Path "C:\FTP-Root\LocalUser\mu.mustermann" -Force
New-Item -ItemType Directory -Path "C:\FTP-Root\LocalUser\m.mueller" -Force
New-Item -ItemType Directory -Path "C:\FTP-Root\LocalUser\Public" -Force

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

```
# FTP Port 21 nur von 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 von INTERNET blockieren:
New-NetFirewallRule -DisplayName 'FTP INTERNET blockieren' -Direction Inbound `
  -Protocol TCP -LocalPort 21 `
  -LocalAddress 10.0.0.44 `
  -Action Block

# Passiv-Modus Portbereich (Vorbereitung):
New-NetFirewallRule -DisplayName 'FTP Passiv INTRANET' -Direction Inbound `
  -Protocol TCP -LocalPort 49152-65535 `
  -LocalAddress 192.168.100.10 `
  -RemoteAddress 192.168.100.0/24 `
  -Action Allow
```

11.4 FTP-Test vom Client

1. Erreichbarkeit des Ports prüfen (PowerShell):

```
# Test der Erreichbarkeit:
Test-NetConnection -ComputerName 192.168.100.10 -Port 21
```

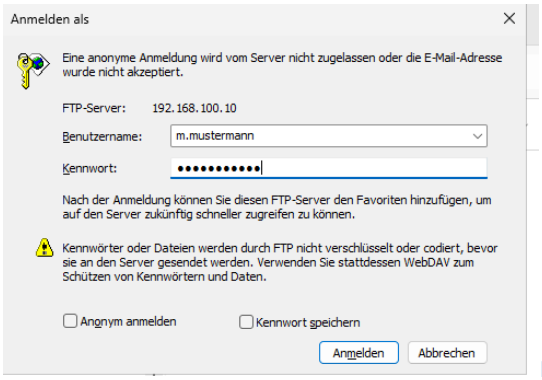
```
ComputerName     : 192.168.100.10
RemoteAddress    : 192.168.100.10
RemotePort       : 21
InterfaceAlias   : NIC 2-Intranet
SourceAddress    : 192.168.100.10
TcpTestSucceeded : True
```

Verbindung über die Kommandozeile (CMD):

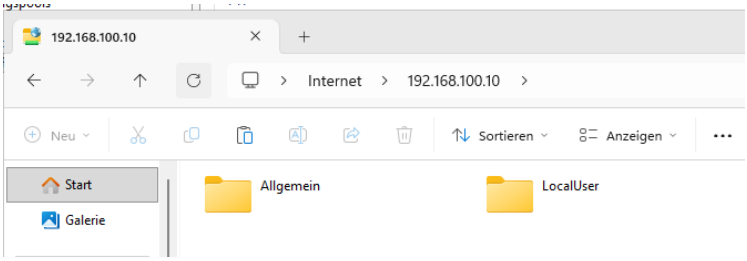
```
Verbindung mit 192.168.100.10 wurde hergestellt.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Benutzer (192.168.100.10:(none)):
```

Verbindung im Windows Explorer:

ftp://192.168.100.10



Passwort: Mittwoch01#



ENDE