



Microsoft System Administration

# Einleitung

Name, Vorname: Wyer Kevin

Kontaktdaten: +41 79 824 60 28  
[kevin.wyer@gibb.ch](mailto:kevin.wyer@gibb.ch)

Beruflich: Productmanager Cloud at Swiss Post  
Teamleiter Microsoft Platforms Operation bei Post CH AG  
Leiter IT-Infrastruktur / Fachreferent bei ICT Berufsbildungscenter AG  
Experte bei ICT Berufsbildung Schweiz  
System Engineer bei MTF Thörishaus AG

Ausbildung: Master of Advanced Studies in Information Technology  
Dipl. Techniker HF Informatik

- Nach dem Kurs Microsoft System Administration sind sie befähigt
  - Installation einer Windows Server Umgebung mit folgenden Komponenten:
    - Active Directory Domain System
    - Domain Name System
    - Dynamic Host Configuration Protocol
    - Anbindung eines Azure Active Directory
      - Diverse Konfigurationen
    - Group policy objects
    - *File Server mit Berechtigungskonzept*

- Name, Vorname
- Firma
- Tätigkeitsbereich
- Welches Know-how habt ihr bereits im Windows Server Umfeld?
- Erwartungen an den Kurs Microsoft System Administration

■ Notengebung für Systemmanagement Windows

Erfahrungsnote

?? %

Theoretische Prüfung

TBD

?? %

Praktische Prüfung

?? %

- Prüfungsvorbereitung ist Sache des Teilnehmers
- Umsetzen des praktischen Teils kann im Unterricht erfolgen
- Abwesenheiten
  - Bitte per Mail mitteilen
  - Selber organisieren was verpasst wurde (Holschuld)

- <https://learn.microsoft.com/>
- Windows Server 2019 Autor
  - Jörg Schieb
- Microsoft Windows Server 2012 R2 - Das Handbuch
  - Autor: Thomas Joos

- Smartlearn Environment als Basis
  - Beta Klasse ;)!

## ■ Software und Lizenz für Windows Server und Client

- [www.smartlearn.ch](http://www.smartlearn.ch) → einloggen mit Gibb Account
- Software → Microsoft Azure DEV Tools for teaching
- Registrieren mit [@iet-gibb.ch](mailto:@iet-gibb.ch) Adresse
- Einloggen auf <https://portal.azure.com/>
- Access student benefits
- Windows 11 & Windows Server 2022 ISO herunterladen & Key speichern

The screenshot shows a software catalog interface. At the top, there's a search bar with 'Windows 11' and a dropdown menu showing 'Product category: Operating System'. Below the search bar, it says '2 Items'. There are two entries listed:

| Name ↑↓   | Product category ↑↓ |
|---|---------------------|
| Windows 11 Education (updated Nov 2021) - DVD   | Operating System    |
| Windows 11 Education N (updated Nov 2021) - DVD | Operating System    |

On the left sidebar, there are links for Overview, Get started, Learning resources (which is currently selected), Roles, Software, and Learning.

The screenshot shows the Microsoft Azure homepage. It features a large 'Welcome to Azure!' message and a callout for 'Start with an Azure free trial'. Below this, there are three main sections: 'Manage Azure Active Directory', 'Access student benefits', and another 'Start with an Azure free trial' section.

**Welcome to Azure!**  
Don't have a subscription? Check out the following options.

**Start with an Azure free trial**  
Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.  
[Start](#) [Learn more](#)

**Manage Azure Active Directory**  
Manage access, set smart policies, and enhance security with Azure Active Directory.  
[View](#) [Learn more](#)

**Access student benefits**  
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.  
[Explore](#) [Learn more](#)

The screenshot shows the Microsoft Azure Dev Tools for Teaching landing page. It has a purple header with the word 'Software'. On the left is a sidebar with links for HOME, DISKS, SOFTWARE, and ABMELDEN. The main area features a large image of a person's hands working on a laptop, with two callout boxes: 'ONTHEHUB STORE (VMWARE)' and 'MICROSOFT AZURE DEV TOOLS FOR TEACHING'.



Microsoft System Administration

# Windows Server 2022

- Ihr kennt verschiedene Windows Server 2022 Rollen und Features
- Ihr kennt die neuen Rollen und Features von Windows Server 2022
- Ihr kennt die verschiedenen Windows Server 2022 Versionen
- Ihr kennt das Lizenzierungsmodell von Windows Server 2022
- Ihr könnt einen Windows Server GUI/CORE installieren und grundkonfigurieren

- Server Konfigurieren (vmWS1, VMCS1)
- Basiskonfiguration der Server (vmWS1, VMCS1)
- Remote Management konfiguriert (WinRM)

- [Windows Server documentation | Microsoft Learn](#)
- [Get started with Windows Server | Microsoft Learn](#)

- Active Directory Certificate Services
- **Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- **DHCP Server**
- **DNS Server**
- Fax Server
- Host Guardian Service
- **Hyper-V**
- Network Controller
- **Network Policy and Access Services**
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- **Windows Server Update Services**

## ► Server Rollen File and Storage Services

- File and iSCSI Services
  - **File Server**
  - BrancheCache for Network Files
  - **Data Deduplication**
  - **DFS Namespace**
  - **DFS Replication**
  - **File Server Resource Manager**
  - File Server VSS Agent Service
  - iSCSI Target Server
  - iSCSI Target Storage Provider
  - Server for NFS
  - Work Folders
- Storage Services (immer vorinstalliert)

- Features sind kleine «Addons»
- Oftmals durch Rollen mitinstalliert
- Verwaltungstools
  - Remote Server Administration Tools
  - Gibt es auch für Clients
- Beispiele
  - BitLocker
  - Failover Clustering
  - Group Policy Management
  - Multipath I/O
  - SMTP Server
  - Telnet Client
  - Windows Server Backup

- Windows Admin Center
- HCI - hyper-converged Infrastructure
- Windows Defender ATP – Advanced Threat Protection
- Windows Core Server wurde weiter verschlankt
- Windows-Subsystem für Linux

- Sicherheit
- Azure-Hybridfunktionen
  - Azure Arc
  - Windows Admin Center
  - Hotpatching (kein Neustart nötig)
- Weiteres
  - Edge Browser
  - Netzwerk & Storage optimierungen
- [Neues in Windows Server 2022 | Microsoft Docs](#)

- Windows Server 2022 Standard
- Windows Server 2022 Datacenter
- Windows Server 2022 Datacenter
  - Azure Edition
- Windows Server 2022 Essentials

| Feature                                  | Standard Edition | Datacenter Edition |
|--|------------------|--------------------|
| Wichtigste Funktionen von Windows Server | ●                | ●                  |
| Hybrid-Integration                       | ●                | ●                  |
| OSE*/Hyper-V isolierte Container         | 2 <sup>[1]</sup> | Unbegrenzt         |
| Windows Server-Container                 | Unbegrenzt       | Unbegrenzt         |
| Speicherreplikat <sup>[2]</sup>          | ●                | ●                  |
| Software-definierte Netzwerke            | ○                | ●                  |
| Software-definierter Speicher            | ○                | ●                  |

- [Windows Server 2022-Lizenzierung und -Preise | Microsoft](#)
- [Vergleich der Windows Server 2022-Editionen Standard, Datacenter und Datacenter Azure Edition | Microsoft Docs](#)

- Pro Prozessor-Kern (Core)
  - Minimum 16 Cores müssen lizenziert werden.  
Beim Kauf des Servers unbedingt beachten.
- Datacenter pro Core ca. 300 CHF
- Standard pro Core ca. 55 CHF
- Speziallizenzierung für
  - NGOs
  - Education
- Lizenzrechner von HP:  
<https://techlibrary.hpe.com/us/en/enterprise/servers/licensing/index.aspx>

## ■ Verwaltung des Servers

- Computername
- Domäne
- IP Konfiguration
- Remoteadministration
- Windows Updates

Learning by doing

# PRACTICE

## ■ **Installieren dieser Systeme:**

### **Server**

Server Basisinstallation GUI

Server Installation mit GUI

Server Installation ohne GUI

Client Installation

### **Funktion**

Sysprep Image

Domain Controller (SRVDC)

SRVCore

Smartlearn Client oder eigene  
Installation (CLI01)

## ■ Server OS Windows Server 2022 Standard/Datacenter

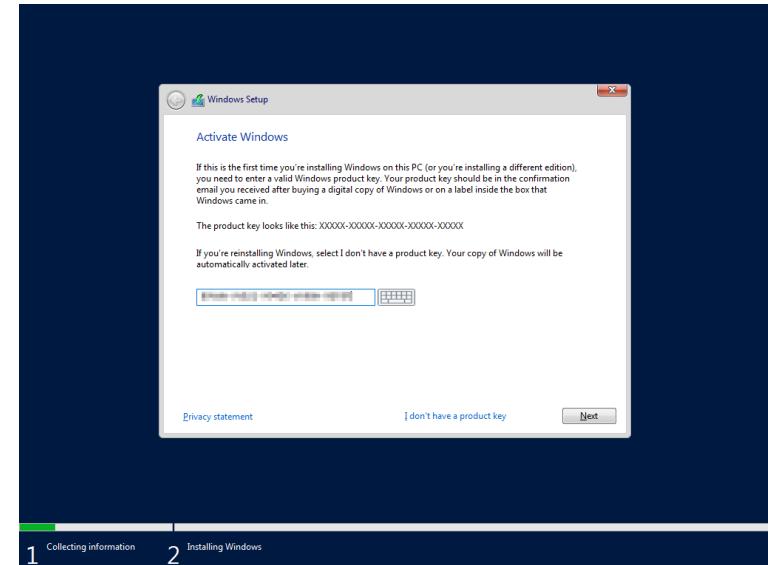
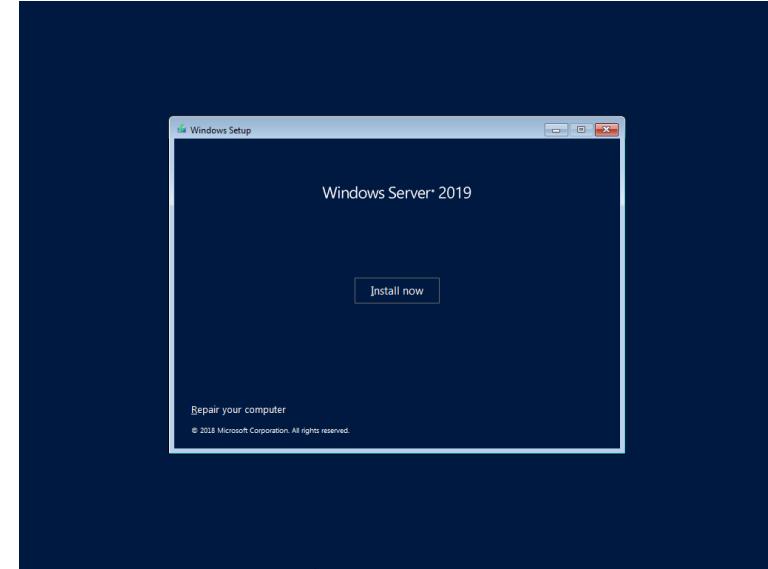
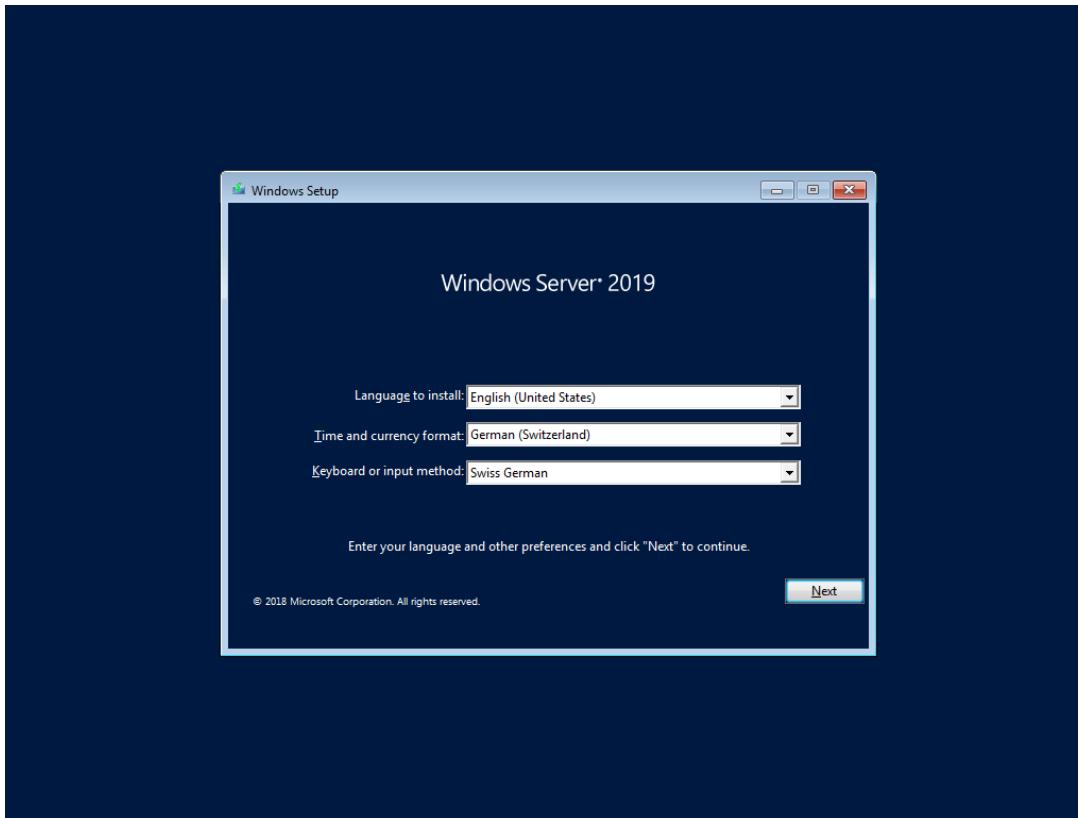
## ■ Grundkonfiguration der Server

- Name, Remote Management Windows Server, IP Adressierung

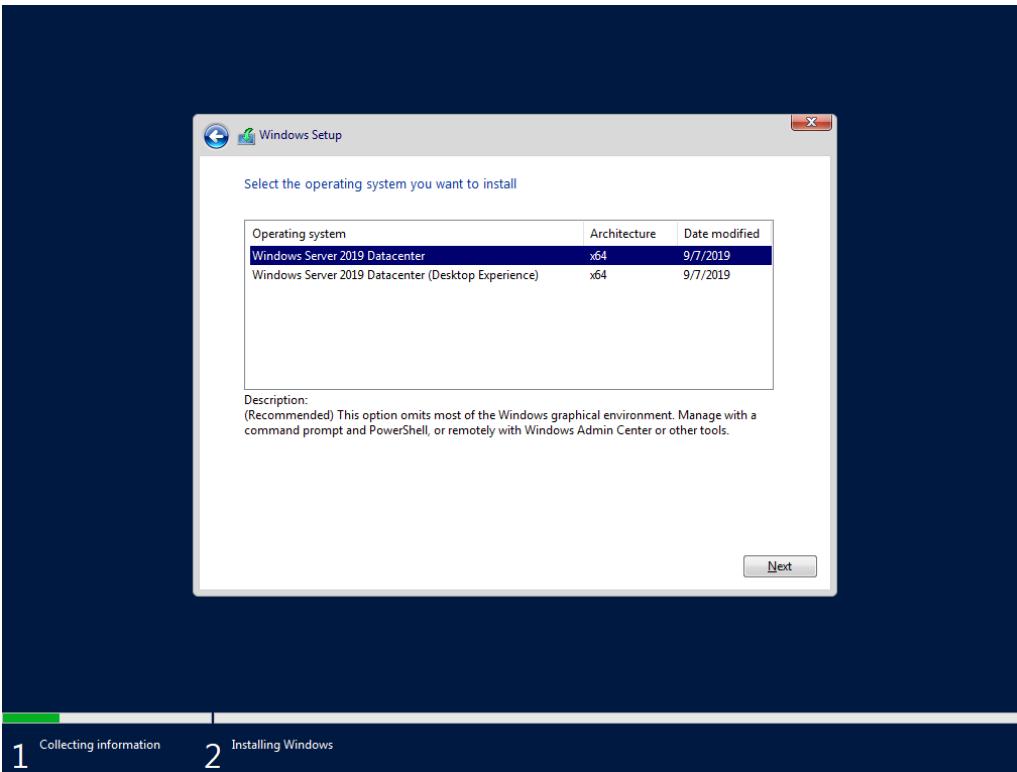
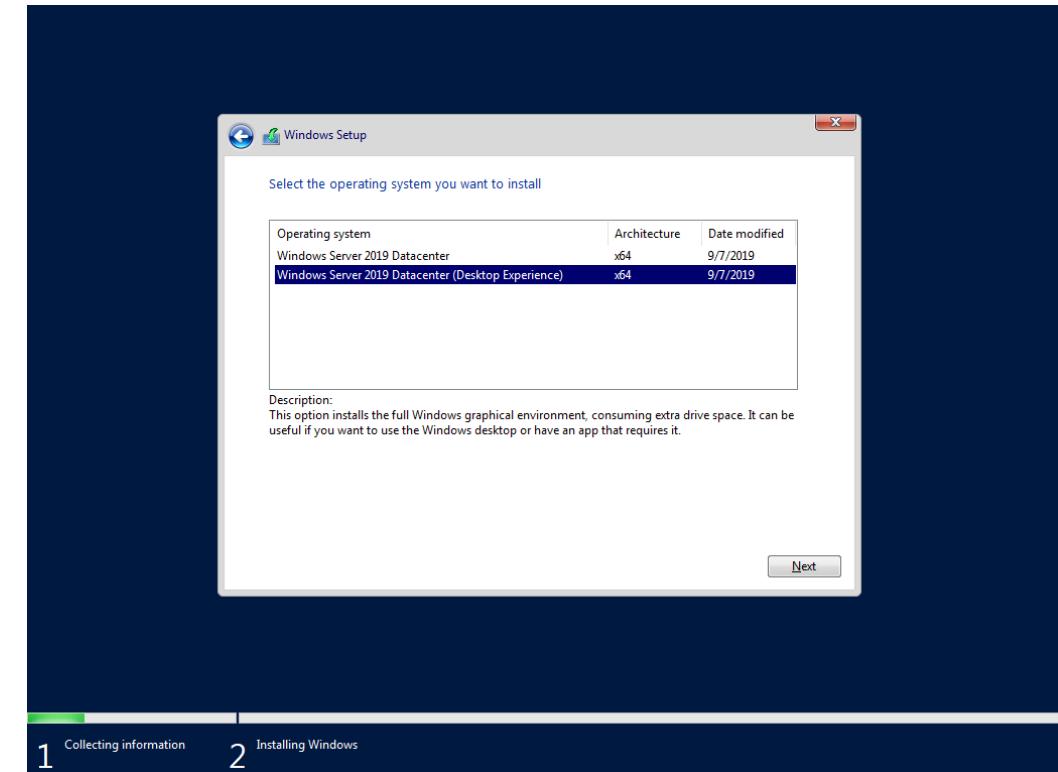
# INSTALLATION SERVER 2022

- Bootbares Medium
  - USB Stick
  - CD
- ISO Datei
  - Download bei Microsoft
  - Einbinden in VM
- Bootarchitektur beachten
  - BIOS
  - UEFI

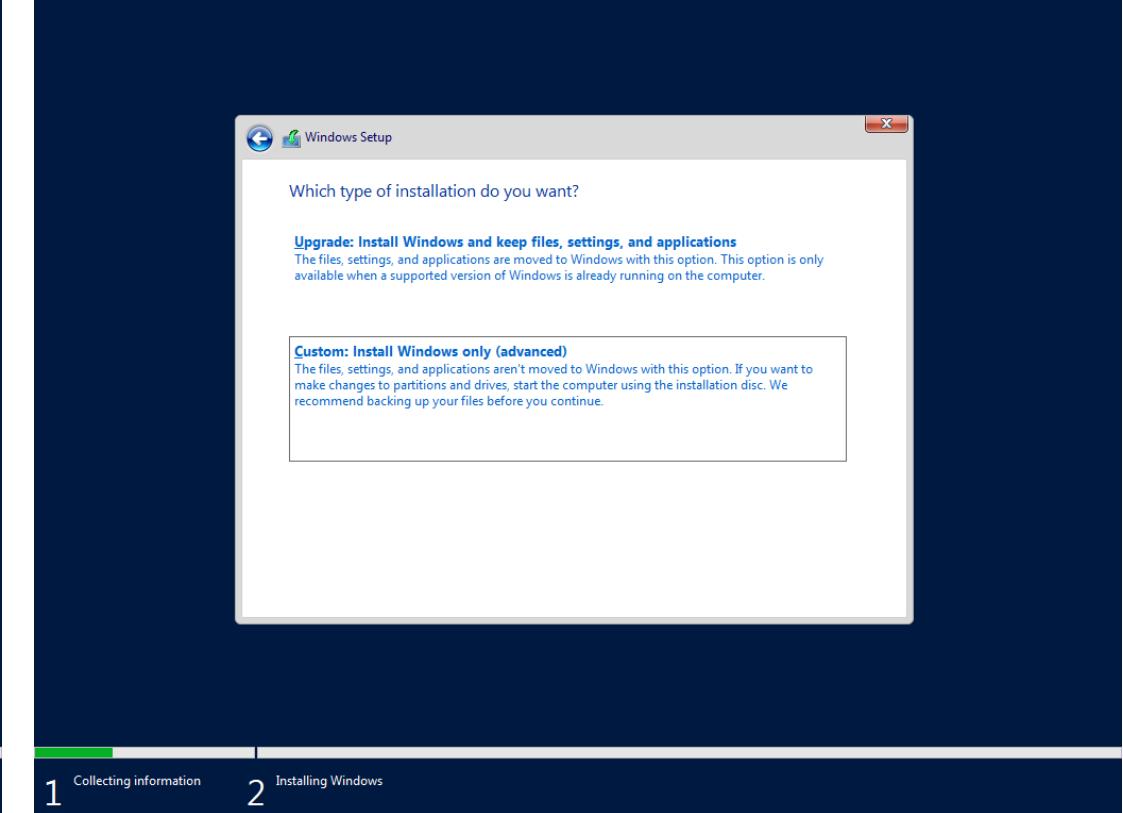
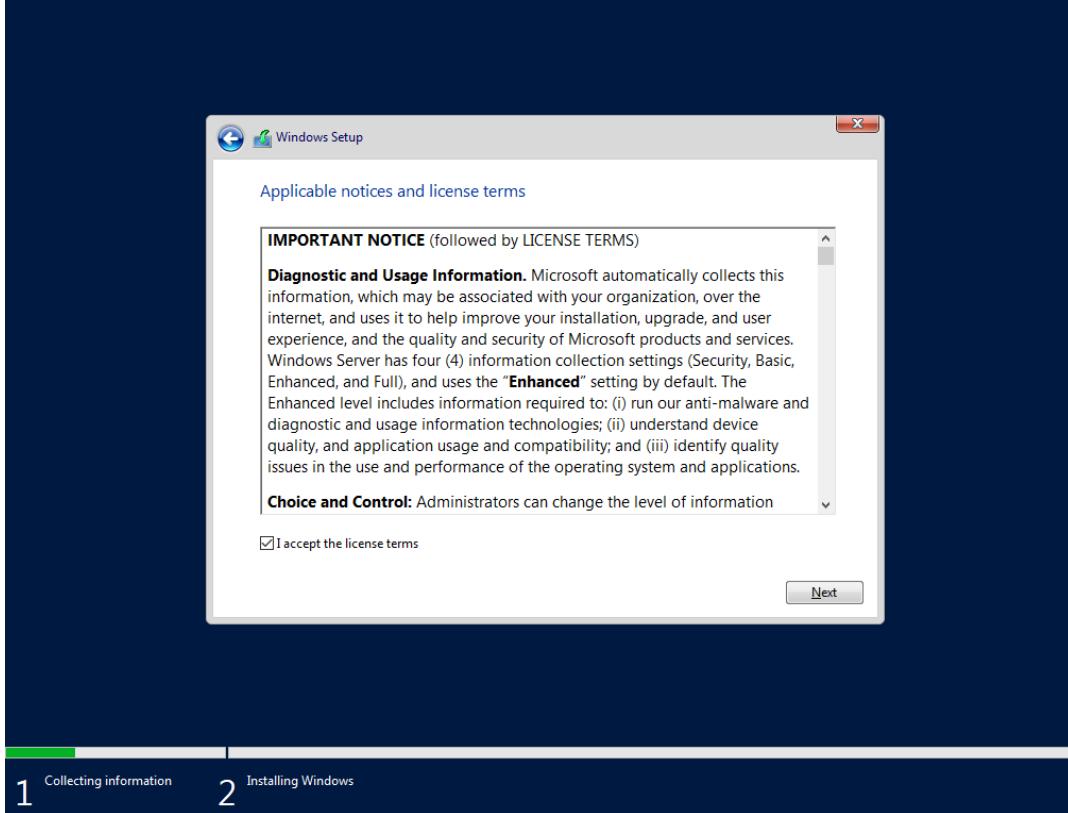
## ▶ Installation



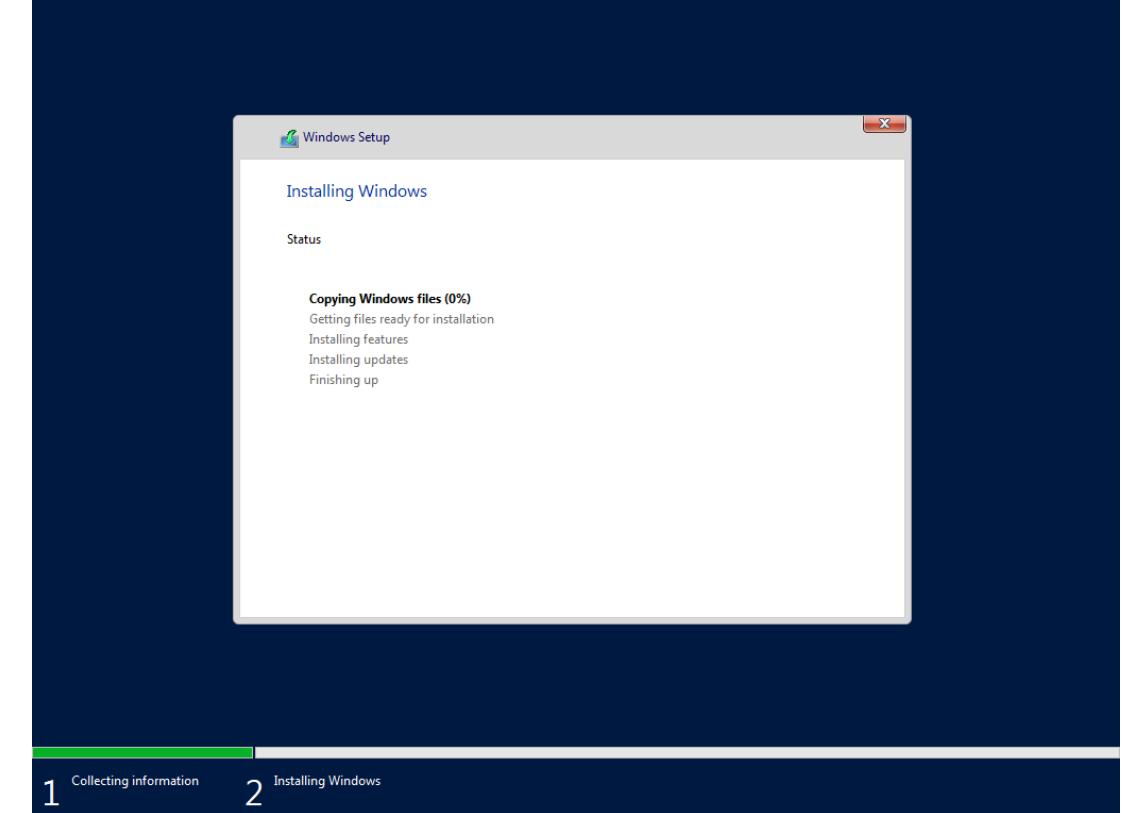
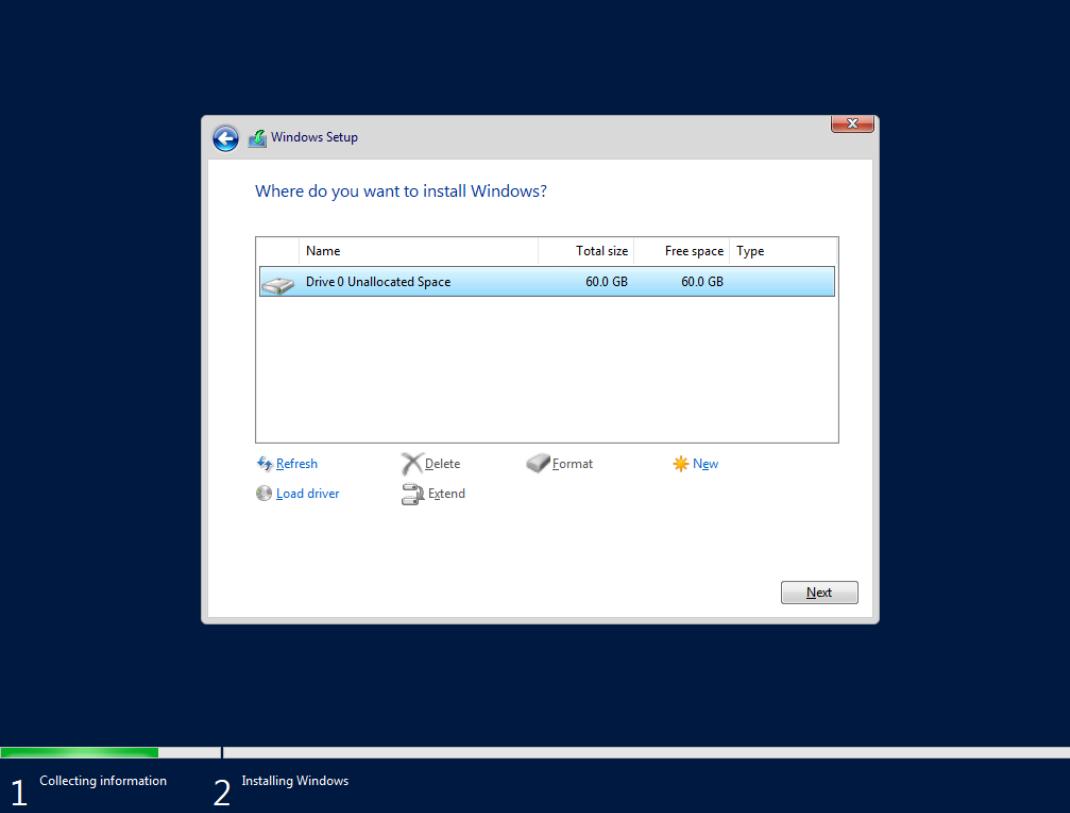
## ▶ Installation

**Ohne GUI****Mit GUI**

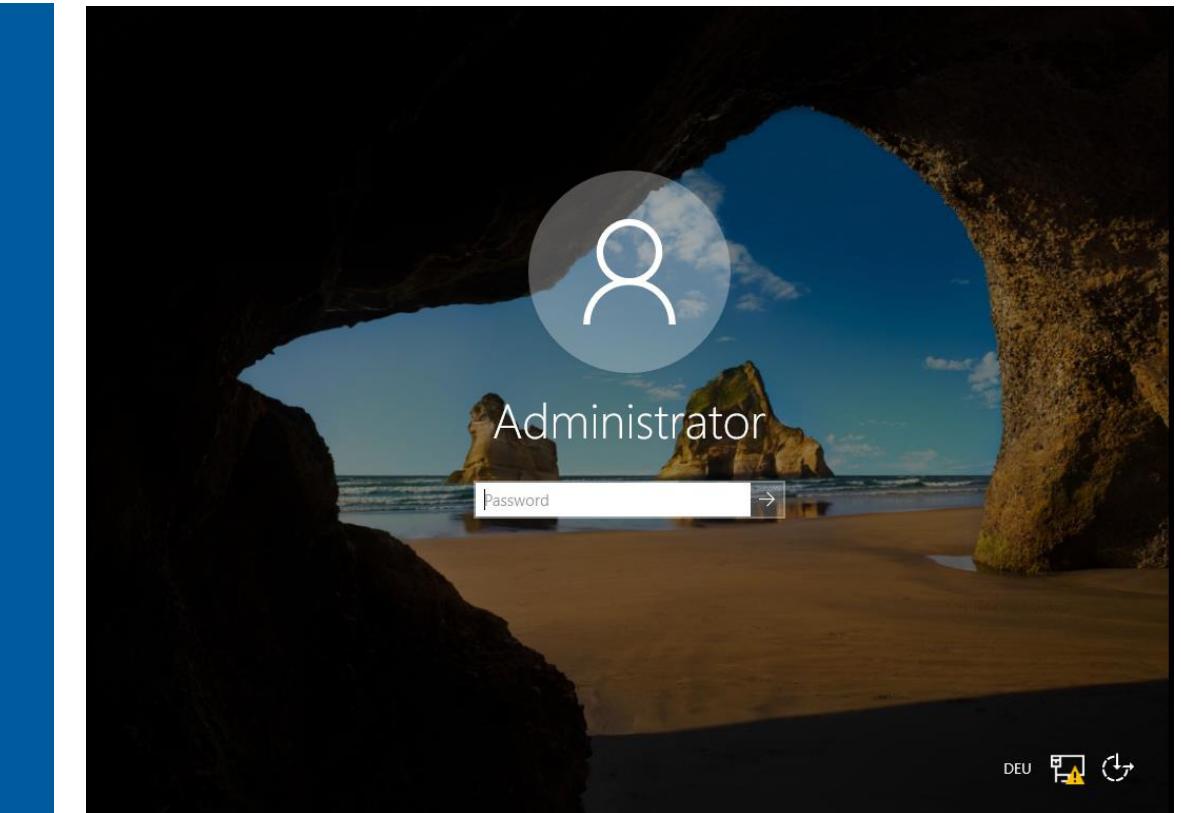
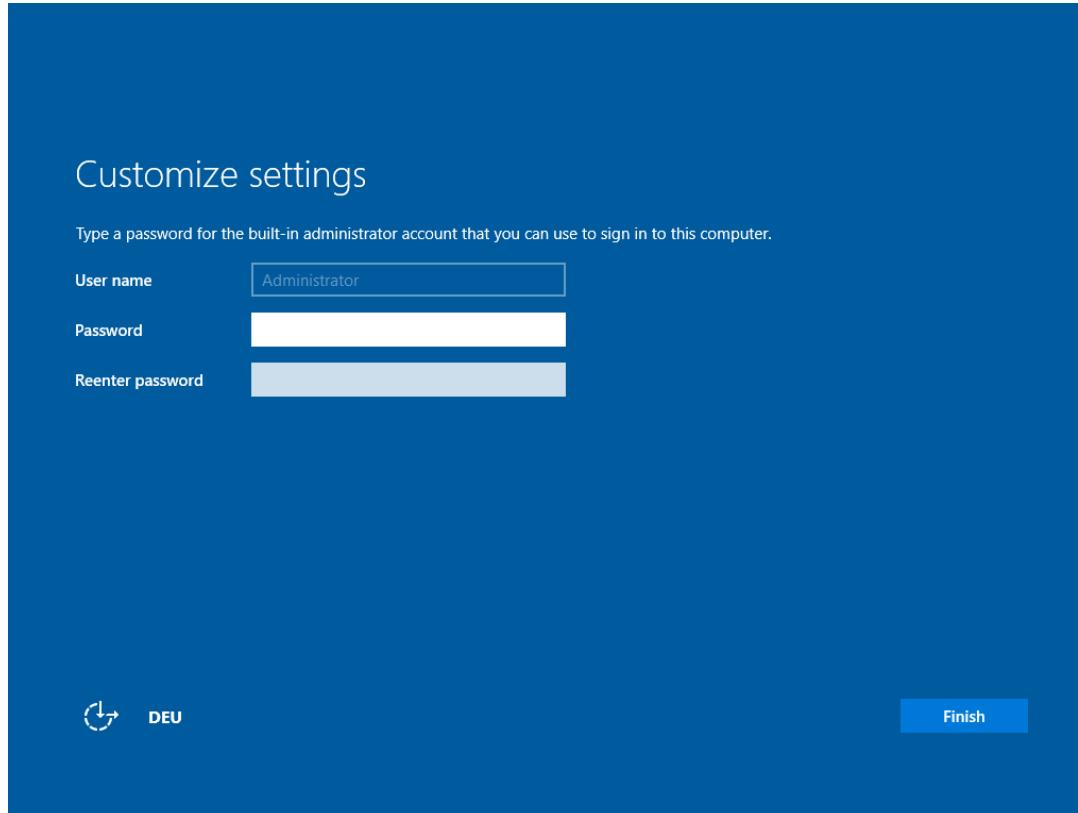
## ▶ Installation



## ▶ Installation



## ► Abschluss Installation

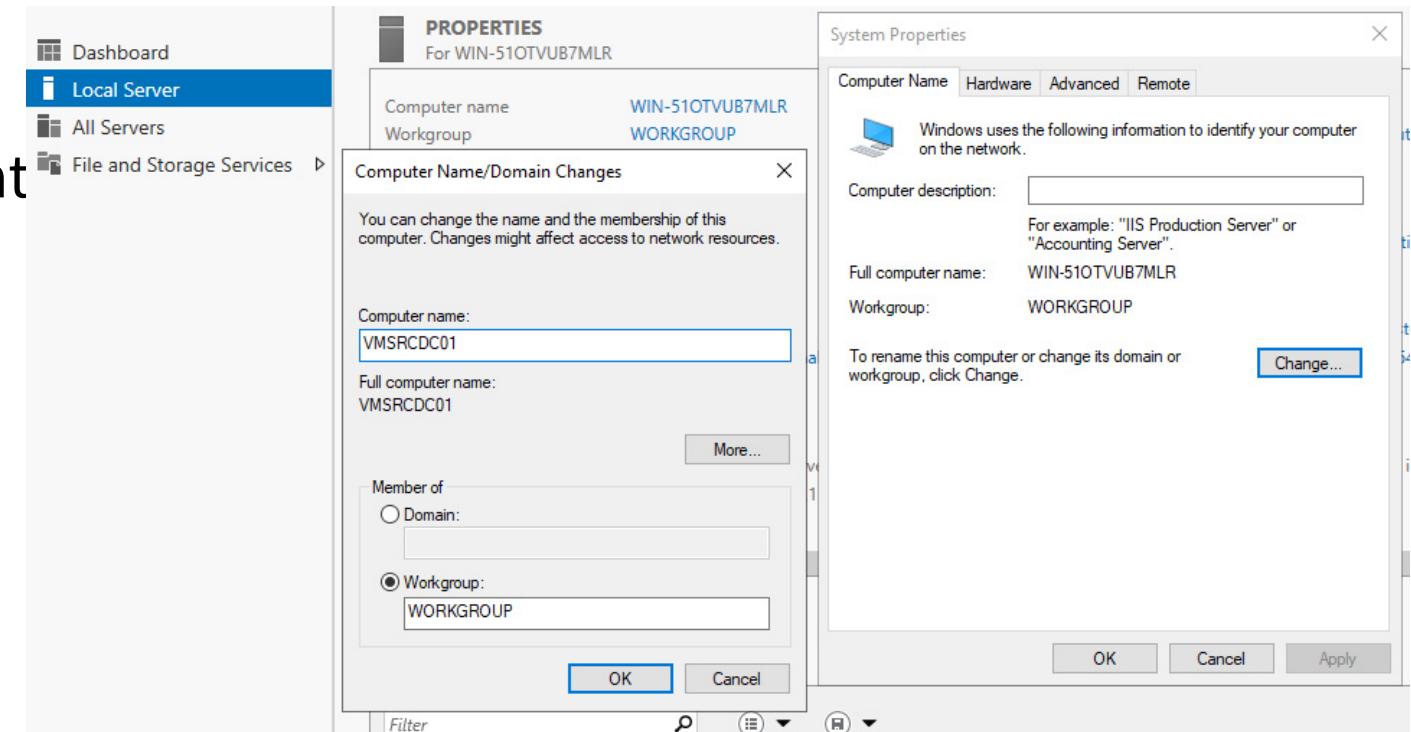


Patching, Remote Desktop, IE Vor Sysprep

# BASISKONFIGURATION VORNEHMEN

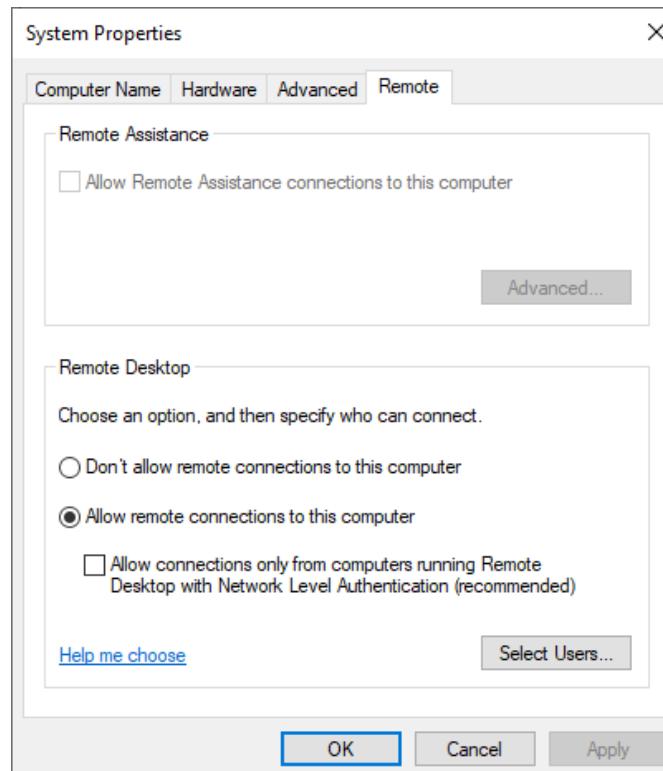
## ► Grundkonfiguration Local Server

- Basiskonfiguration unter Local Server
- Remotedesktop aktivieren
- ~~Updates installieren~~
- IE Enhanced Security Configuration  
OFF -> Administrators

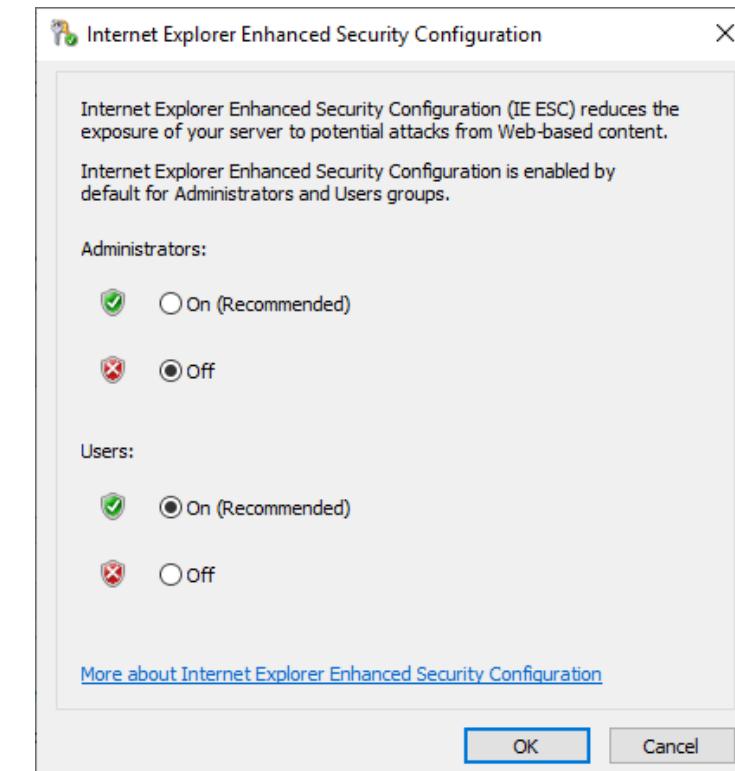


## ► Grundkonfiguration

## Remotedesktop



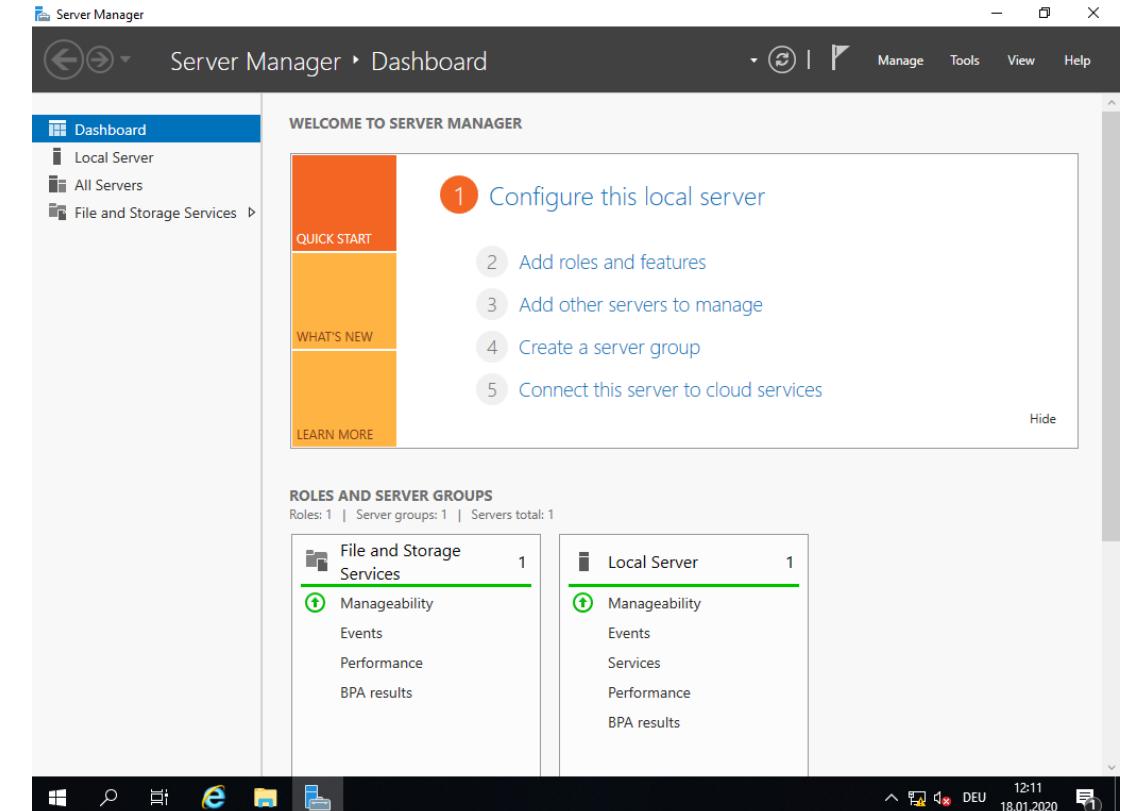
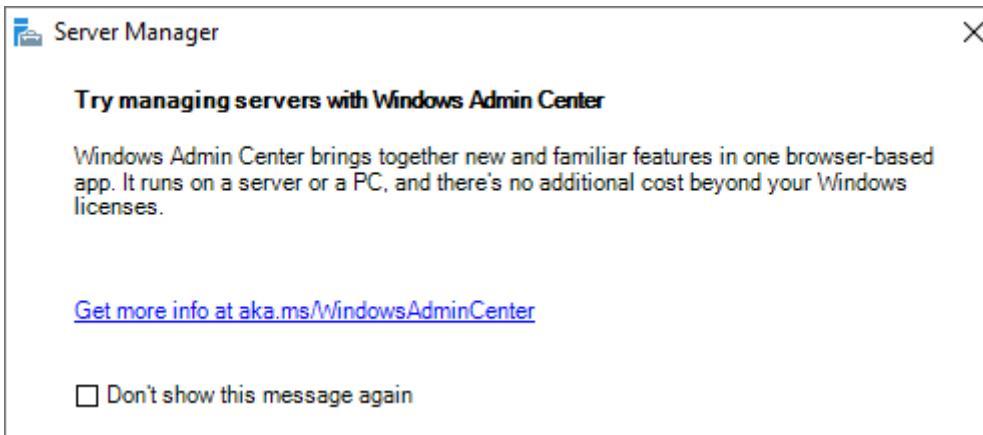
## IE Enhanced Security Configuration



# BASISKONFIGURATION SRVDC

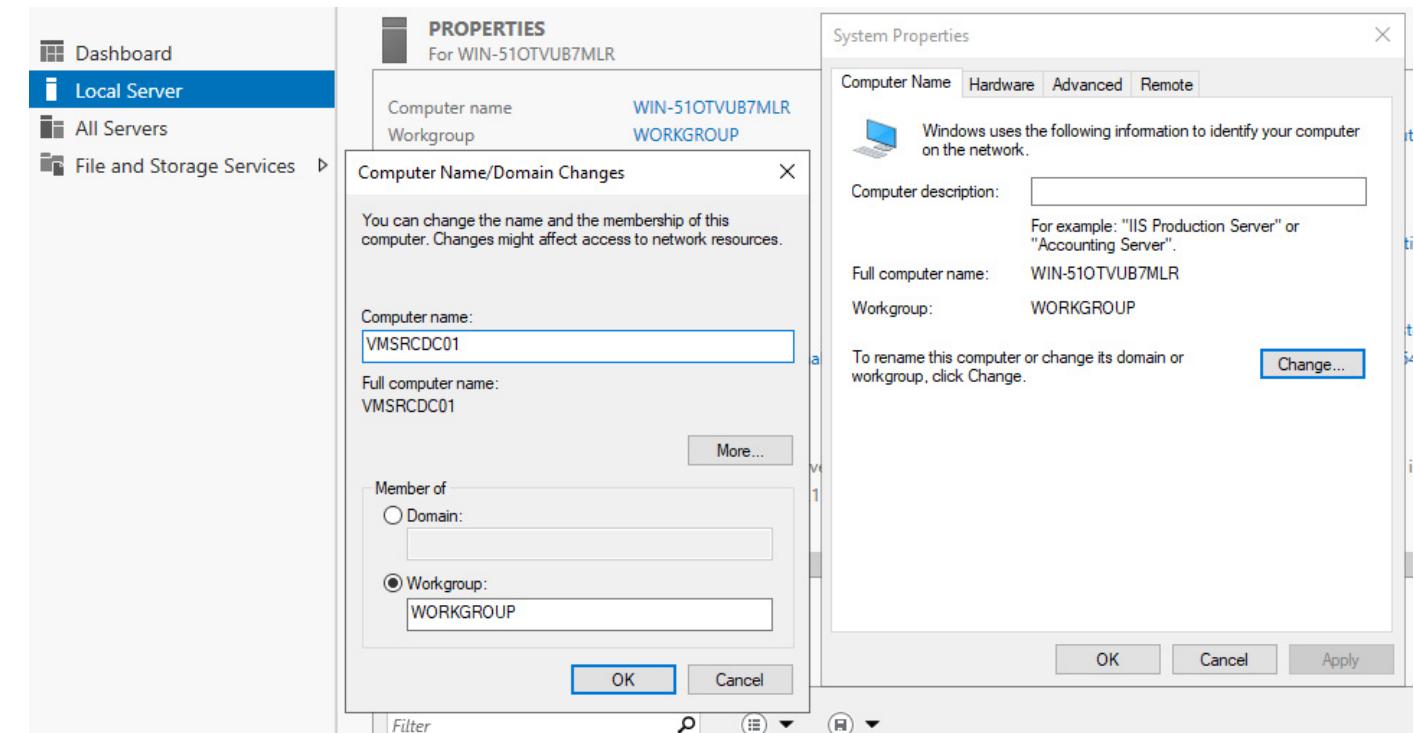
## ► Konfiguration SRVDC

- Server Manager
- Windows Admin Center
  - Werden wir noch anschauen



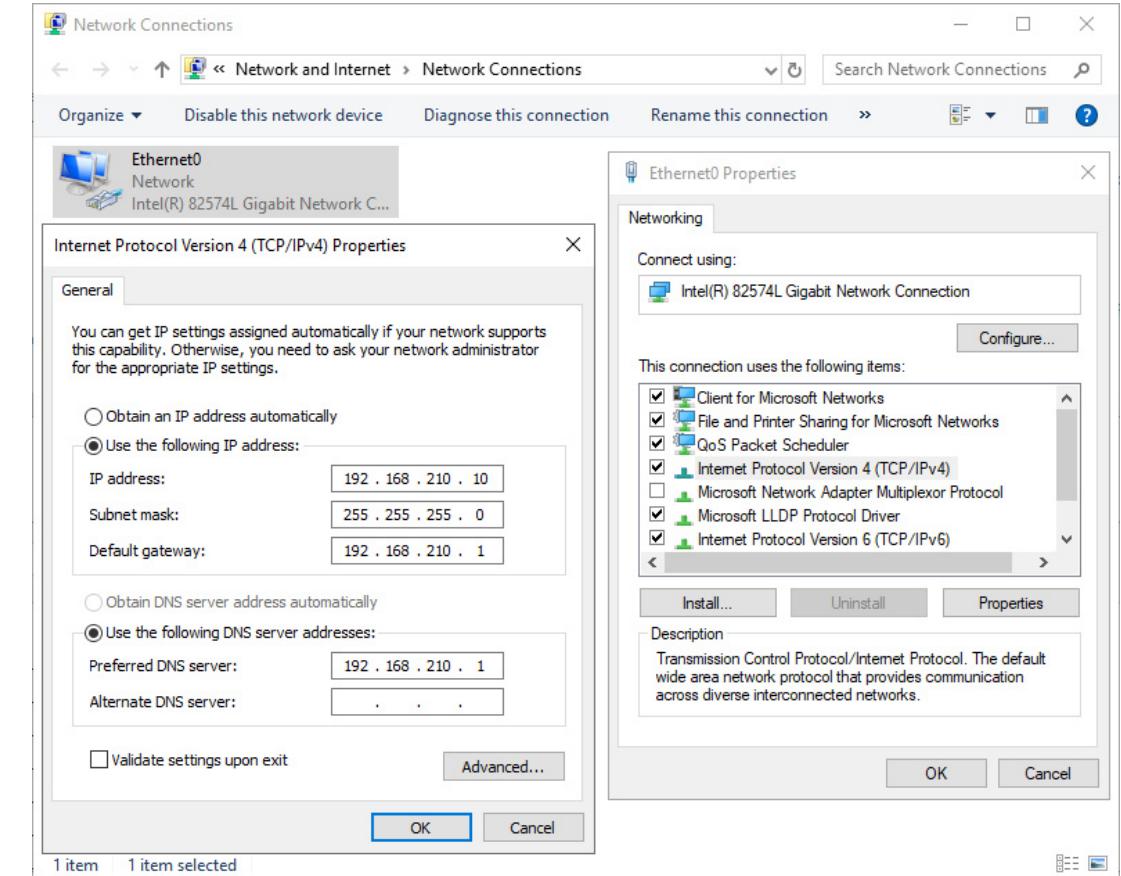
## ► Grundkonfiguration Local Server

- Servername anpassen
- Ethernet Konfiguration
- Updates installieren
- Updates konfigurieren



## ► Grundkonfiguration «Ethernet»

- Konfiguration des Ethernet Adapter 0
- Windows +R «ncpa.cpl»
- IP Konfiguration
  - IP/Subnetz: 192.168.110.XX/24
  - Gateway: 192.168.110.1
  - DNS: 192.168.110.1
- Eigenes Adresskonzept verwenden



## ► Abschluss Grundkonfiguration

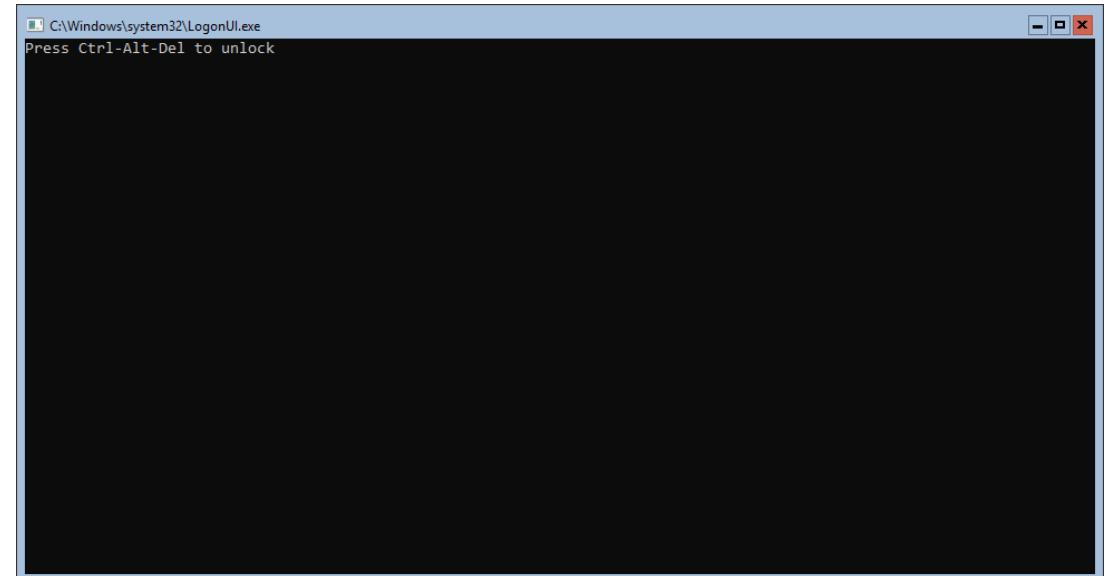
| PROPERTIES                |  |                                    |   |
|---------------------------|--|------------------------------------|---|
| For VMSRCDC01             |  |                                    |   |
|                           |  | Last installed updates             | Today at 12:30  |
| Computer name             | VMSRCDC01                                | Windows Update                     | <a href="#">Download updates only, using Windows Update</a>         |
| Workgroup                 | WORKGROUP                                | Last checked for updates           | Today at 12:20  |
| Windows Defender Firewall | Public: On                               | Windows Defender Antivirus         | Real-Time Protection: On  |
| Remote management         | Enabled                                  | Feedback & Diagnostics             | <a href="#">Settings</a>  |
| Remote Desktop            | Enabled                                  | IE Enhanced Security Configuration | Off   |
| NIC Teaming               | Disabled                                 | Time zone                          | (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna        |
| Ethernet0                 | 192.168.210.10, IPv6 enabled             | Product ID                         | 00430-70306-70541-AA347 (activated)                                 |
| Operating system version  | Microsoft Windows Server 2019 Datacenter | Processors                         | Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz, Intel(R) Core(TM) i7-8665 |
| Hardware information      | VMware, Inc. VMware7,1                   | Installed memory (RAM)             | 4 GB  |
|                           |  | Total disk space                   | 59.4 GB   |

- Standard Desktop Icons einblenden
  - Windows +R «desk.cpl ,5»

# BASISKONFIGURATION SRVCORE

## ► Grundkonfiguration

- CTRL+ALT+INSERT (VMPlayer)
- Passwort ändern



## ► Grundkonfiguration mit Terminal

- Alle Basiskonfigurationen mit einem Befehl:
  - sconfig
- ~~Servername anpassen~~
- Remotedesktop aktivieren
- Ethernet konfigurieren
- ~~Updates installieren~~

```
Administrator: C:\Windows\system32\cmd.exe - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

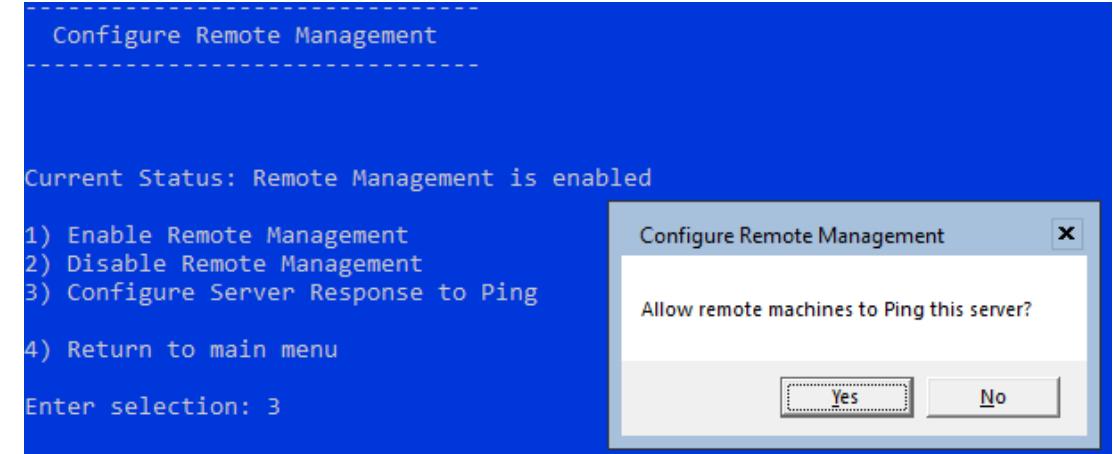
=====
          Server Configuration
=====

1) Domain/Workgroup:           Workgroup: WORKGROUP
2) Computer Name:             WIN-7CFFSATKL2T
3) Add Local Administrator
4) Configure Remote Management   Enabled
5) Windows Update Settings:    DownloadOnly
6) Download and Install Updates
7) Remote Desktop:             Disabled
8) Network Settings
9) Date and Time
10) Telemetry settings
11) Windows Activation          Unknown
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

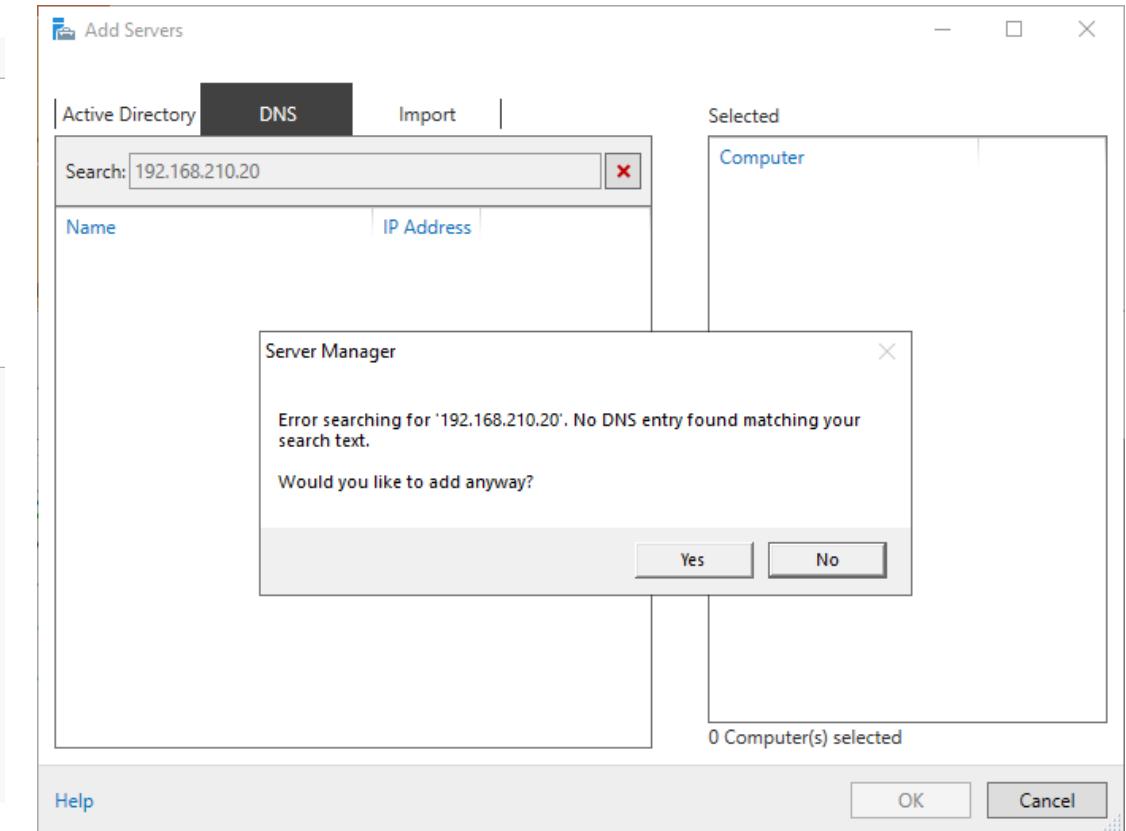
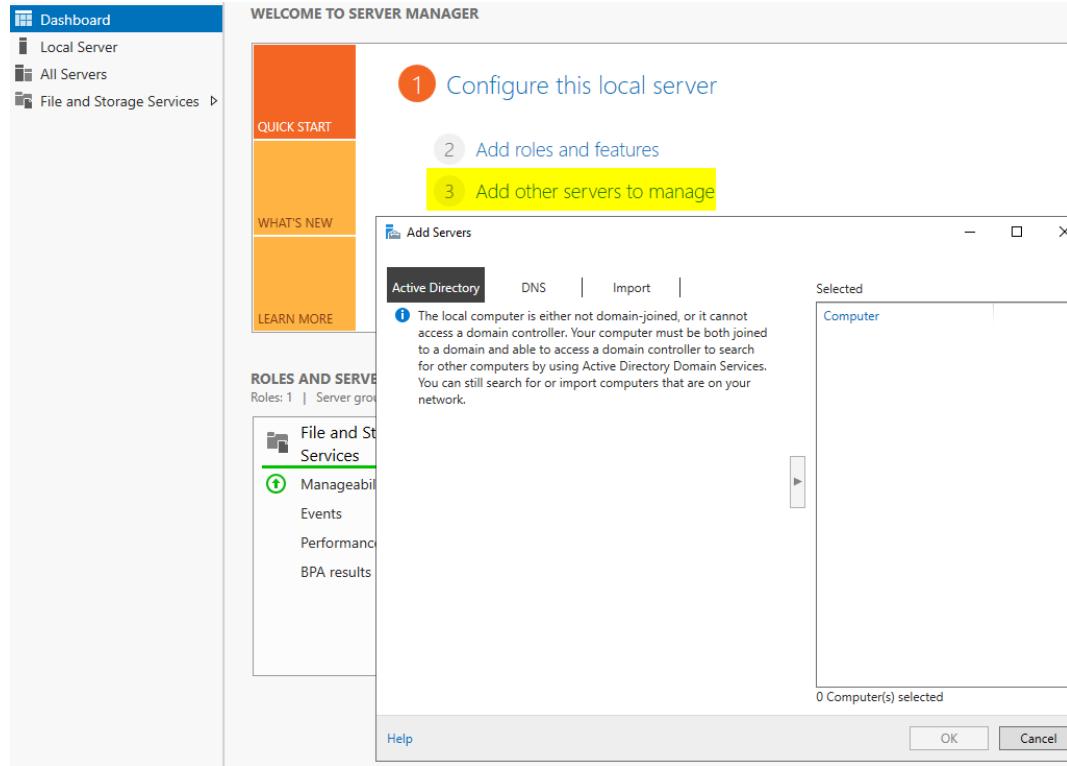
Enter number to select an option:
```

## ► Remote Konfiguration CORE

- Configure Remote Management
  - Enable Ping
- Verbindung zwischen GUI und CORE Server mit Ping prüfen
- winrm konfigurieren CMD:
  - WinRM quickconfig
- SRVDC CMD
  - WinRM set winrm/config/client @{TrustedHosts="192.168.XXX.XX"}
  - IP des SRVCore Servers
- SRVCORE CMD
  - WinRM set winrm/config/client @{TrustedHosts="192.168.XXX.XX"}
  - IP des SRVDC Servers



## ► Remote Konfiguration von SRVCore



► Remote Konfiguration ist nun möglich

The screenshot displays a server management interface with the following details:

**Servers Overview:**

| Server Name | IPv4 Address   | Manageability                             | Last Update         | Windows Activation                  |
|-------------|----------------|---|---------------------|-------------------------------------|
| VMSRCDC01   | 192.168.210.10 | Online - Performance counters not started | 18.01.2020 13:39:56 | 00430-70306-70541-AA347 (Activated) |
| VMSRVCORE   | 192.168.210.20 | Online - Performance counters not started | 18.01.2020 13:43:27 | 00430-70306-70541-AA775 (Activated) |

**PowerShell Session:**

```
[> Administrator: Windows PowerShell]
[192.168.210.20]: PS C:\Users\Administrator\Documents> hostname
VMSRVCORE
[192.168.210.20]: PS C:\Users\Administrator\Documents>
```

Selbständig durchführen oder VM von Smartlearn verwenden.

# CLIENT INSTALLATION



Microsoft System Administration

# Active Directory Domain Services Part 1

■ Die studierenden

- können erklären was ein Verzeichnisdienst ist
- wissen was die Rolle Active Directory Domain Services (ADDS) ist
- wissen welche Komponenten ADDS beinhaltet
- wissen welche Strukturen es in ADDS gibt
- können die 5 Betriebsmaster Rollen benennen
- Können die Rolle ADDS installieren und konfigurieren

- Installierte Domäne (Initialen-tsbe.local)
- Administrator umbenannt
- Recycle bin aktiviert
- NTP konfiguriert
- OU Struktur mit Benutzer erstellt

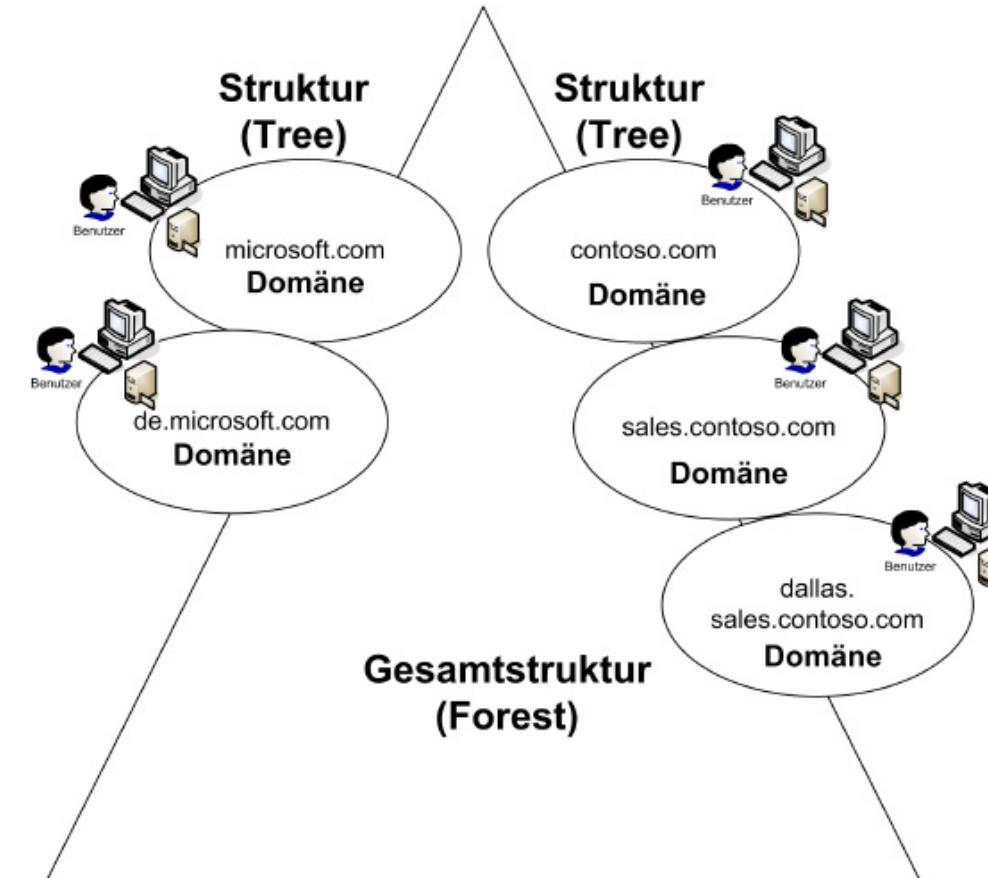
- [Active Directory Domain Services | Microsoft Learn](#)
- [Planen der Platzierung der Rolle „Betriebsmaster“ | Microsoft Learn](#)
- [Planen der Platzierung des globalen Katalogservers | Microsoft Learn](#)
- Microsoft Windows Server 2012 R2 - Das Handbuch
  - S. 424 – 432
  - S. 437 – 448

- Verschiedene Produkte
  - Active Directory Domain Services (ADDS) (Microsoft)
- Hierarchische Datenbank
- Client-Server-Prinzip

- Abbilden des Unternehmens im Active Directory muss gut geplant sein.
- Heutzutage wird meist nur noch eine Domäne für das gesamte Unternehmen erstellt.
- Server 2019 – Keine neuen AD Features: [Microsoft](#)
- JET-Datenbank (Joint-Engine-Technologie)
- Komponenten
  - Schema
    - Vorlagen für Objekte die erstellt werden können
  - Konfiguration
    - Beschreibt die Gesamtstruktur
  - Domain
    - Alle Informationen zusammen

- Gesamtstruktur (Forest)
  - Dieser Container kann Strukturen (Trees) beinhalten
- Struktur (Tree)
  - Dieser Container beinhaltet die einzelnen Domänen von Active Directories
  - Childdomains - Subdomänen
  - Treedomain - Domäne in eine neuen Tree
- Domänen
  - Dieser Containertyp beinhaltet Organisationseinheiten
- Organisationseinheiten (Organizational Units, OUs)
  - Dieser Container beinhaltet Benutzer und Computerkonten, kann aber auch weitere OUs beinhalten.
  - Mithilfe OUs können Objekte im Active Directory organisiert werden

► Beispiel



- Organizational Unit – OU
  - Verwaltungscontainer für Benutzer, Computer, Gruppen und Drucker
- Replikation
  - Daten werden innerhalb der Domäne von einem DC zum anderen repliziert
- Site
  - Physikalisch getrennter Standort meist über VPN verbunden
- Objekte
  - Element die in Active Directory erstellt werden können:
    - Benutzer, Computer, Gruppen und Drucker

- Verwaltung einer Domäne innerhalb eines Forest
- Innerhalb einer Domäne kann es mehrere DCs geben
- Organisation und Verwaltung von
  - Benutzer-, Computer-, Freigaben-, und Druckerinformationen
- Authentifizierung von Benutzer läuft über einen DC (Kerberos)

- Erster DC einer Gesamtstruktur ist immer GC
- An jeder Site/Standort sollte ein DC mit GC konfiguriert werden
- Jeder DC kann theoretisch auch GC sein
- Der GC enthält Informationen der Gesamtstruktur und somit von jeder Domäne.

- 5 Rollen
  - Pro Forest einmalige Rollen
    - Schema Master
    - Domain Naming Master
  - Pro Domain vorhanden
    - RID Master
    - PDC Emulator
    - Infrastructure Master
- Support Microsoft
- Auf Deutsch auch «Betriebsmaster Rollen» genannt

## Schema Master

- Schema Master wird benötigt um das Schema zu erweitern
  - Exchange macht dies
- Um das Schema anzuschauen muss auf dem DC der Befehl: «regsvr32 schmmgmt.dll» ausgeführt werden. Danach kann ein mmc geöffnet werden und das Snap-In Active Directory-Schema geöffnet werden.

## Domain Naming Master

- Wird benötigt
  - Wenn die Domäne erweitert wird
  - Zum Hochstufen eines neuen DCs
- Er hat im normalen produktiv Betrieb keine Aufgabe

## RID Master

- Verteilt RID (Relative identifier)
- Wird für die SIDs benötigt (Security ID)
- Jedes Objekt erstellt wird erhält eine SID
- Ist der RID Pool eines DCs aufgebraucht erhält er vom RID-Master neue RIDs zugewiesen
- Eine SID ist einzigartig

## PDC Emulator

- Anwendung und Verwaltung von Gruppenrichtlinien
- Kennwortänderungen laufen über den PDC
- Zeitserver der Domäne

## Infrastructure Master

- Berechtigungsverwaltung wenn mehrere Domänen im Einsatz sind
- Beschleunigt Abfragen von Berechtigungen und fungiert als ein Cache
- Sollte nicht auf einem GC sein
  - Ausser wenn nur 1 DC existiert
  - Bei 2 DCs beide zu GC machen

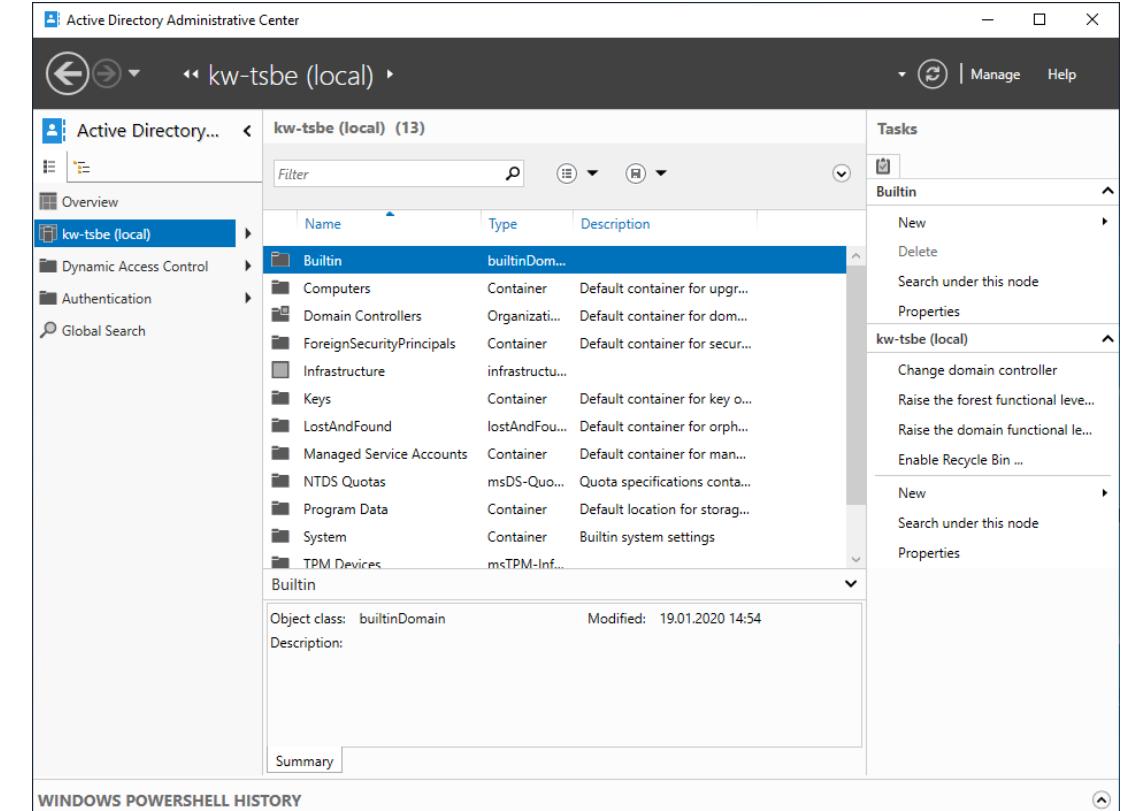
- Zur optimalen Verteilung der FSMO-Rollen gibt es folgende Empfehlungen:
  - Der Infrastrukturmaster sollte nicht auf einem globalen Katalog liegen, da ansonsten Probleme bei der Auflösung von Gruppen, die Mitglieder aus verschiedenen Domänen haben, auftreten können
  - Domänennamenmaster und Schemamaster sollten auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist
  - PDC-Emulator und RID-Master kommunizieren viel miteinander und sollten daher auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist
- Die Verteilung der Rollen ist eine kleine Wissenschaft, bei einem Forest mit mehreren Domänen muss dies gut geplant werden.

- Schutz für Domäne an einem zweiten Standort
- Replizieren nur Informationen
- Nehmen selber keine Änderungen an
- Kennwörter werden nur von gewünschten Accounts repliziert dies wird mittels Gruppen gesteuert:
  - Allowed RODC Password Replication Group
  - Denied RODC Password Replication Group

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers
- ADSI Edit
- DNS
- Group Policy Management

## ► Active Directory Administrative Center

- Neue Administrative Center
  - Eingeführt mit Server 2012
- Neue Features
  - Recycle Bin
  - Fine-Grained Password Policy
  - Windows PowerShell History Viewer



Learning by doing

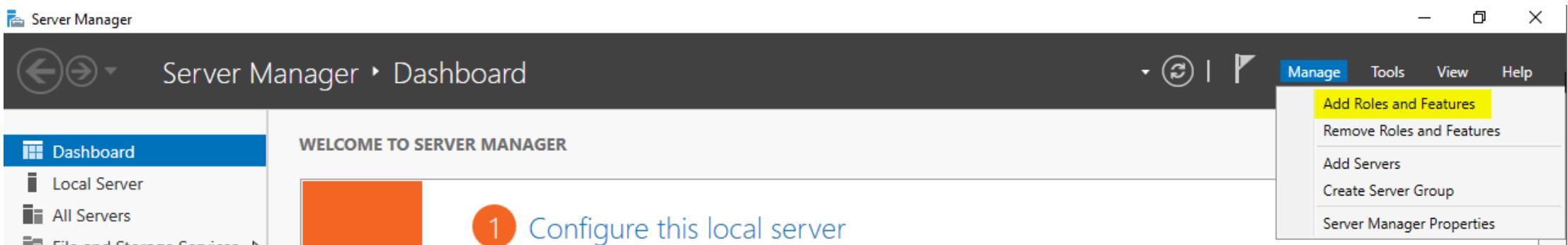
# PRACTICE

- Installation und Konfiguration der ADDS Rolle
  - Nach Vorgaben siehe Foliensatz

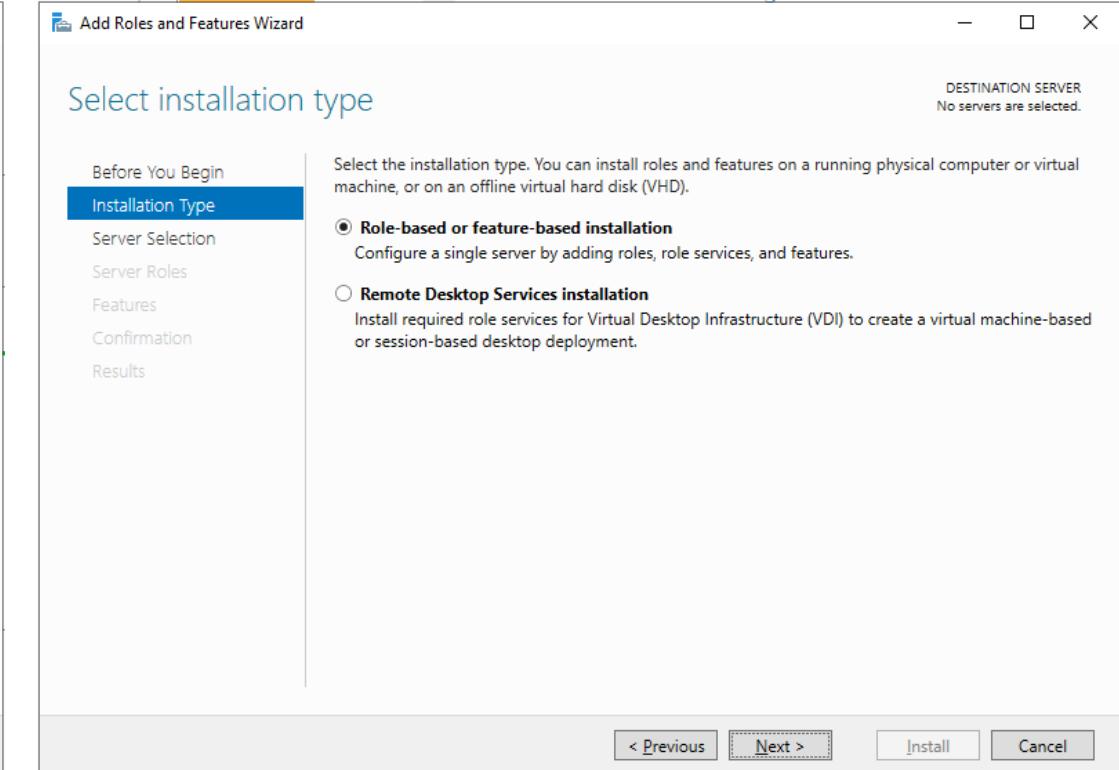
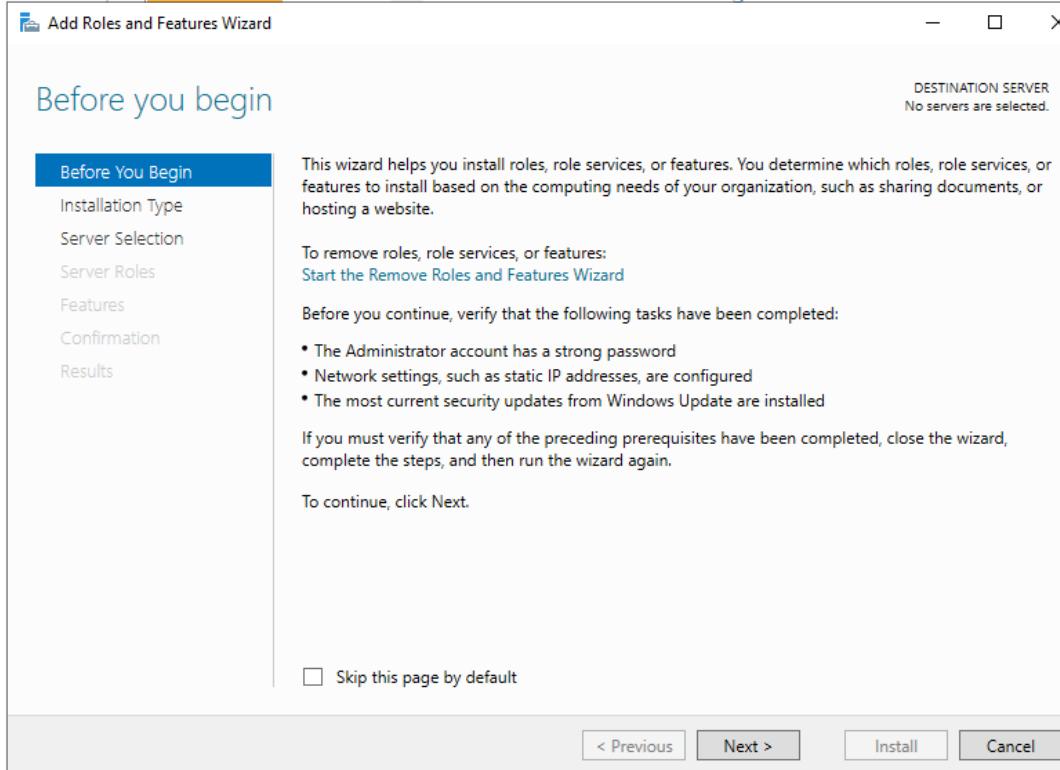
- Servername angepasst
- IP Konfiguration
  - Fixe IP
  - **DNS 127.0.0.1**
- ~~Windows Updates installiert~~

- Lokaler Admin Account vor der Installation umbenennen
- Windows + R -> Lusrmgr.msc
- Windows + X -> C
- Local User and Groups -> Users
- Rechtsklick auf Administrator -> Rename
- Neuer Name domainadmin

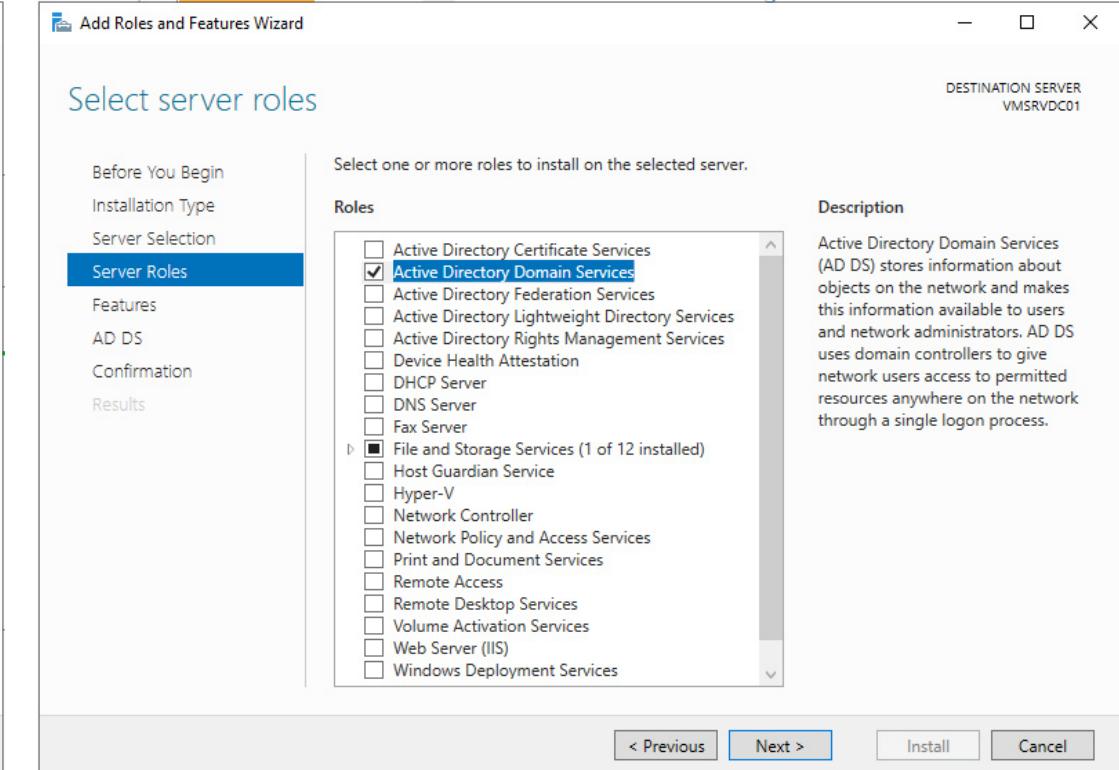
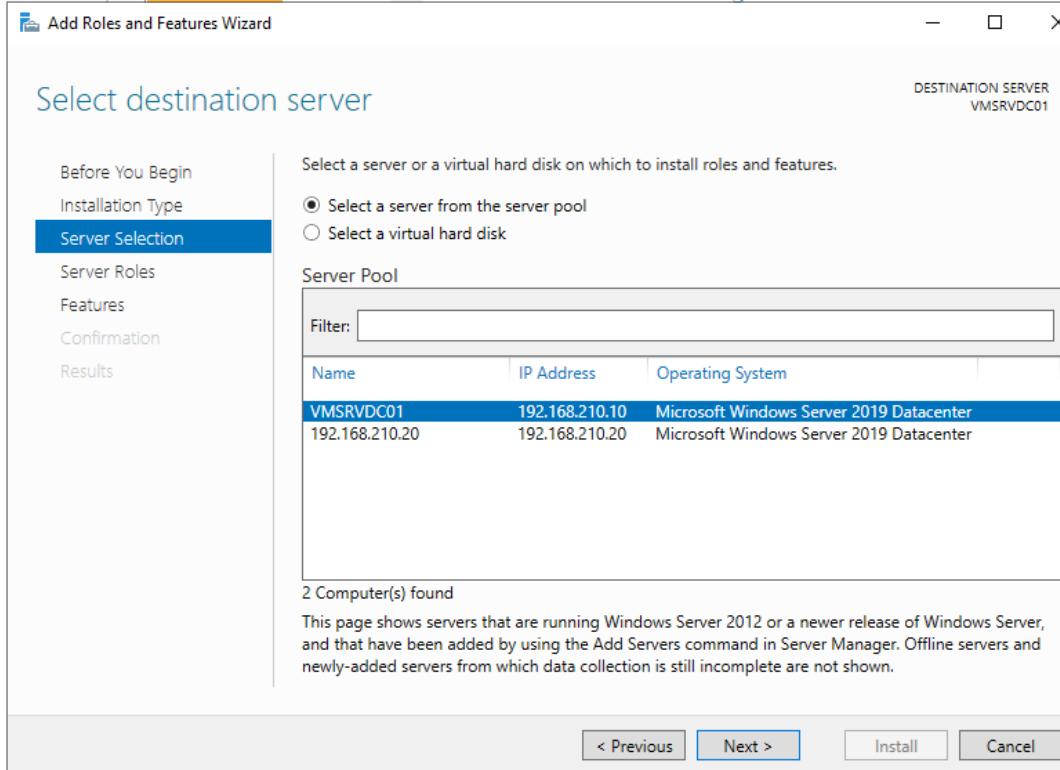
## ► ADDS Rollen Installation



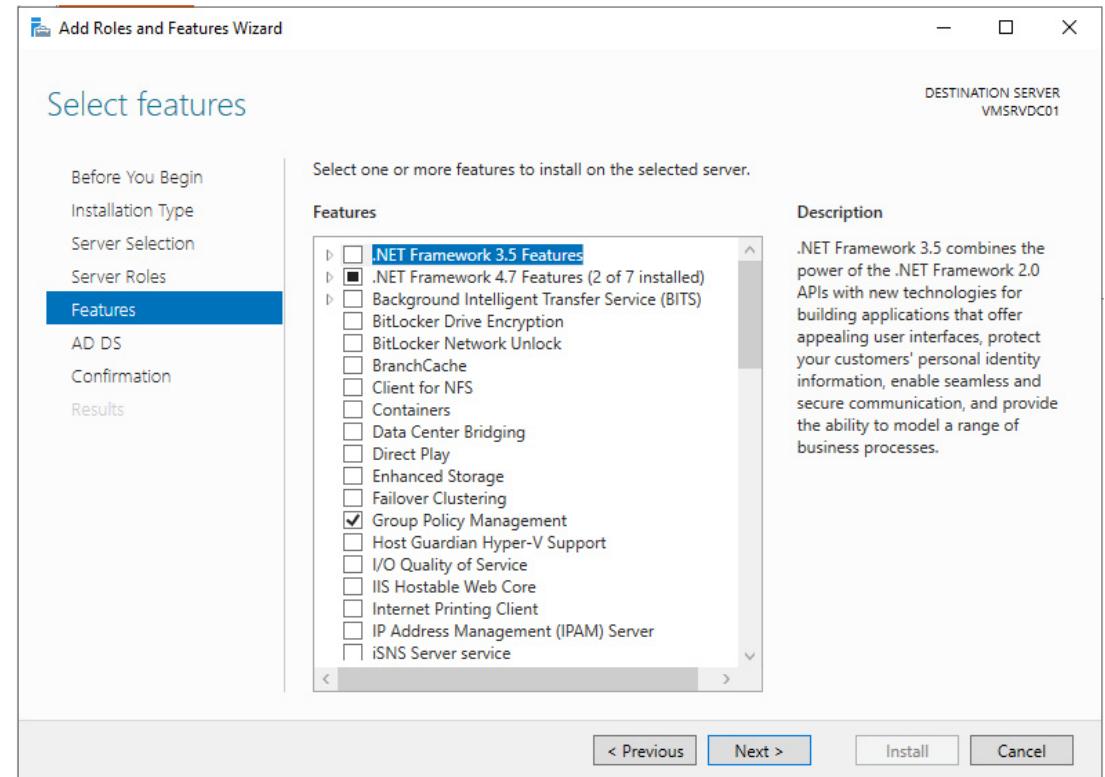
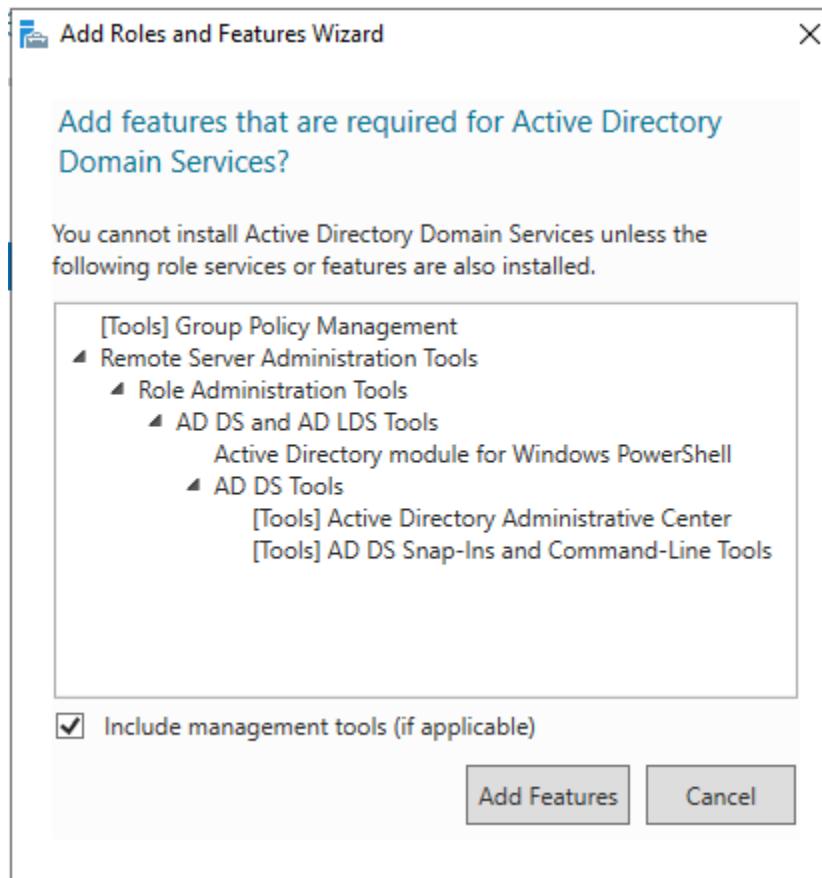
## ► ADDS Rollen Installation



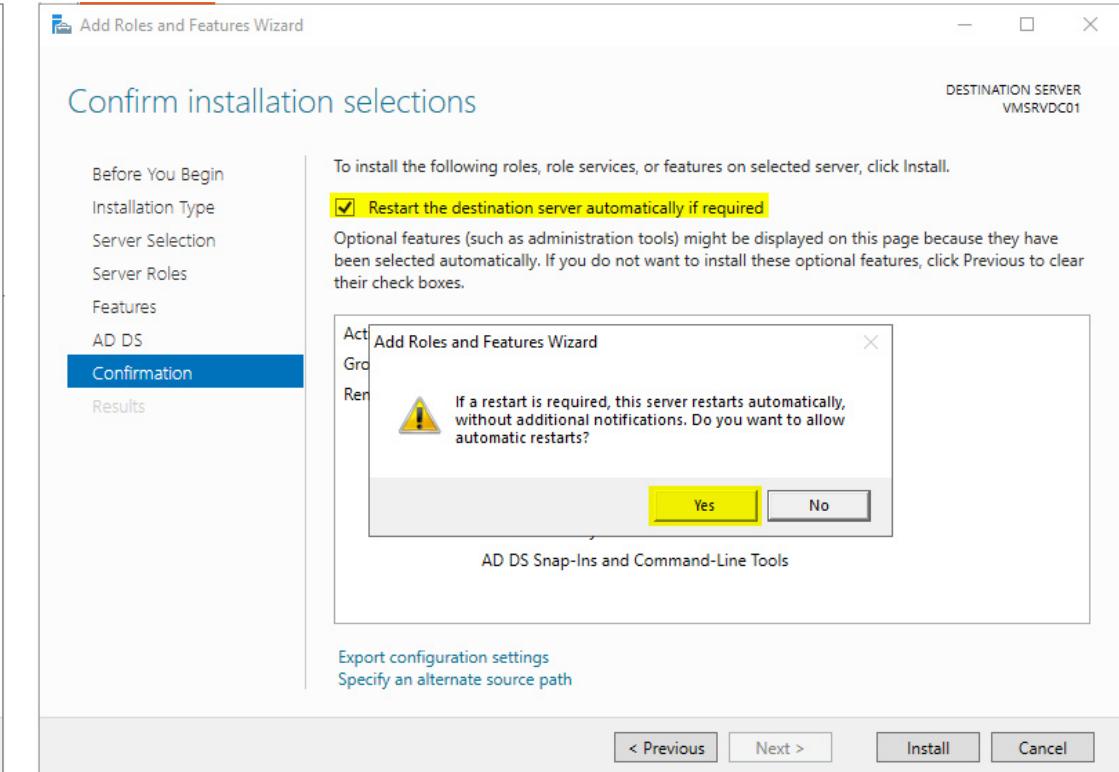
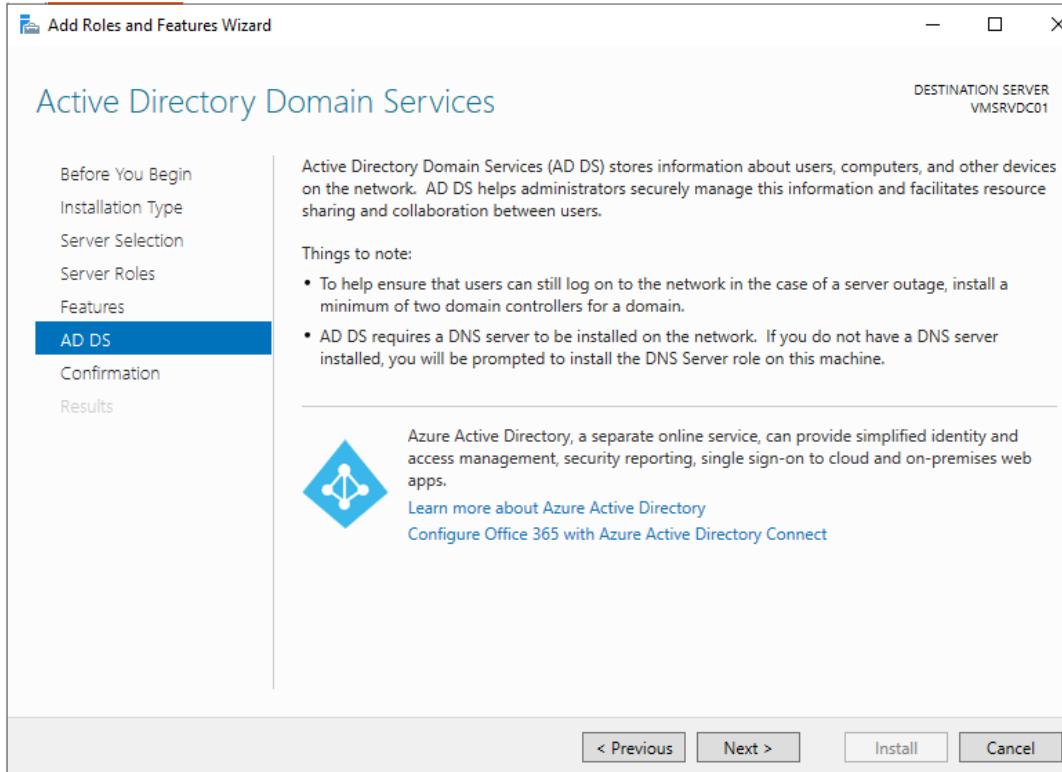
## ► ADDS Rollen Installation



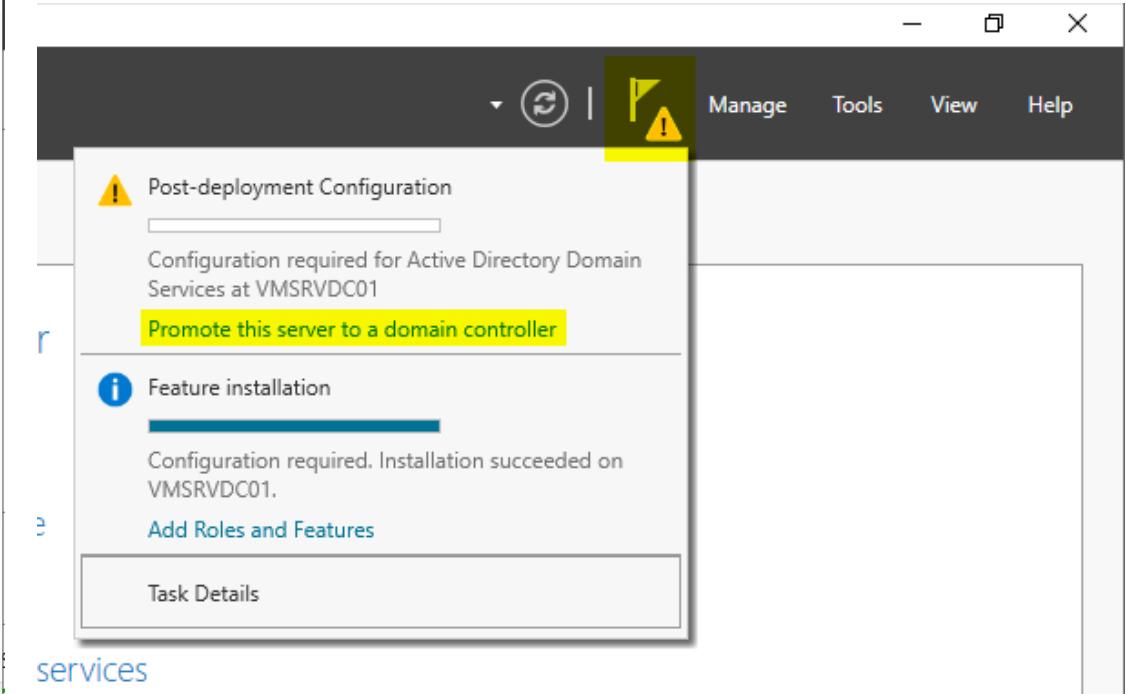
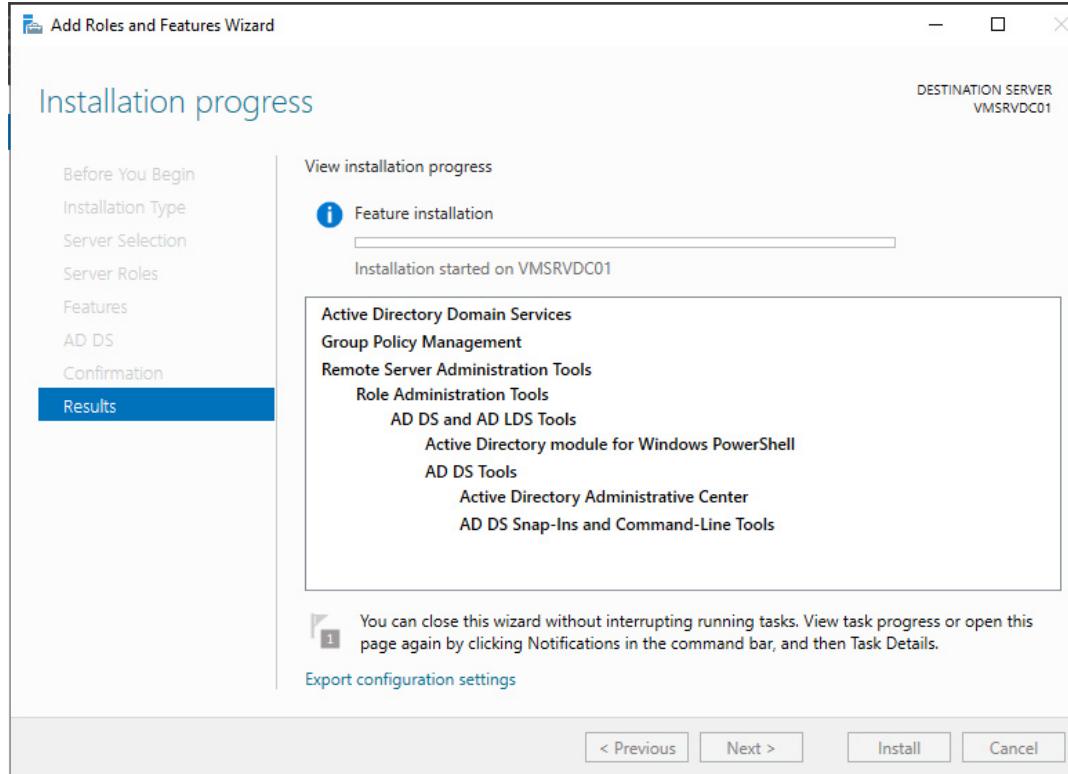
## ► ADDS Rollen Installation



## ► ADDS Rollen Installation

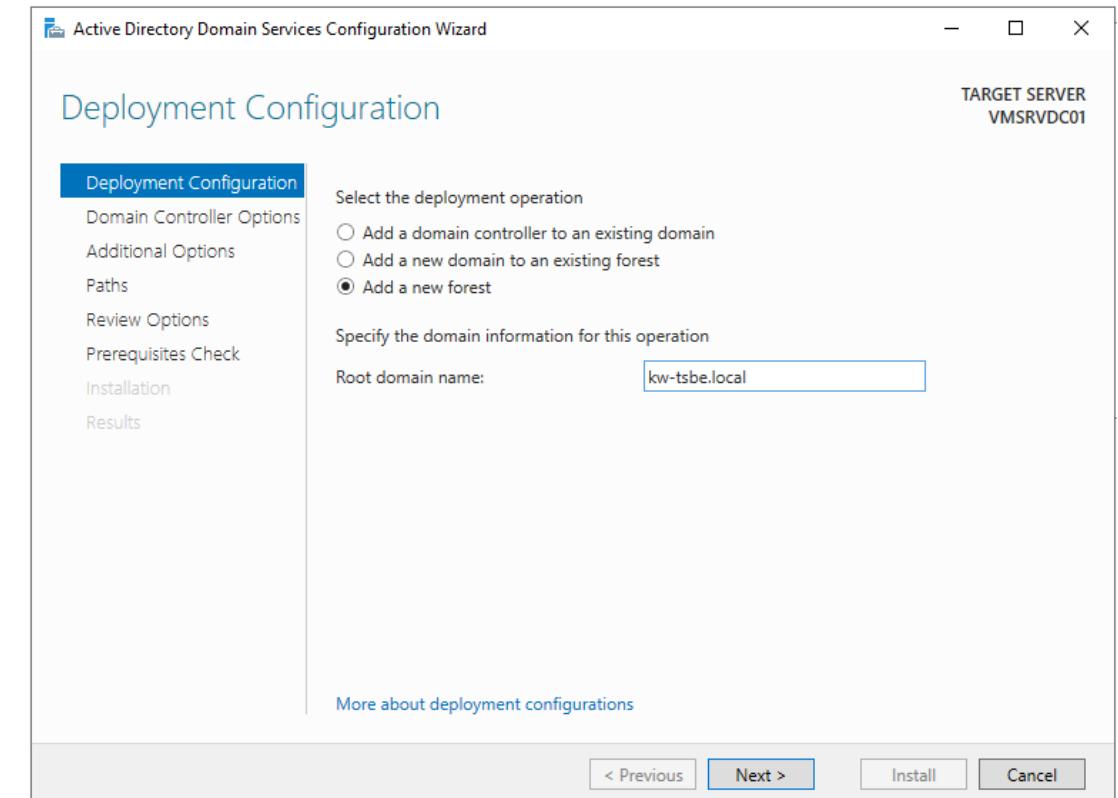


## ► ADDS Rollen Installation

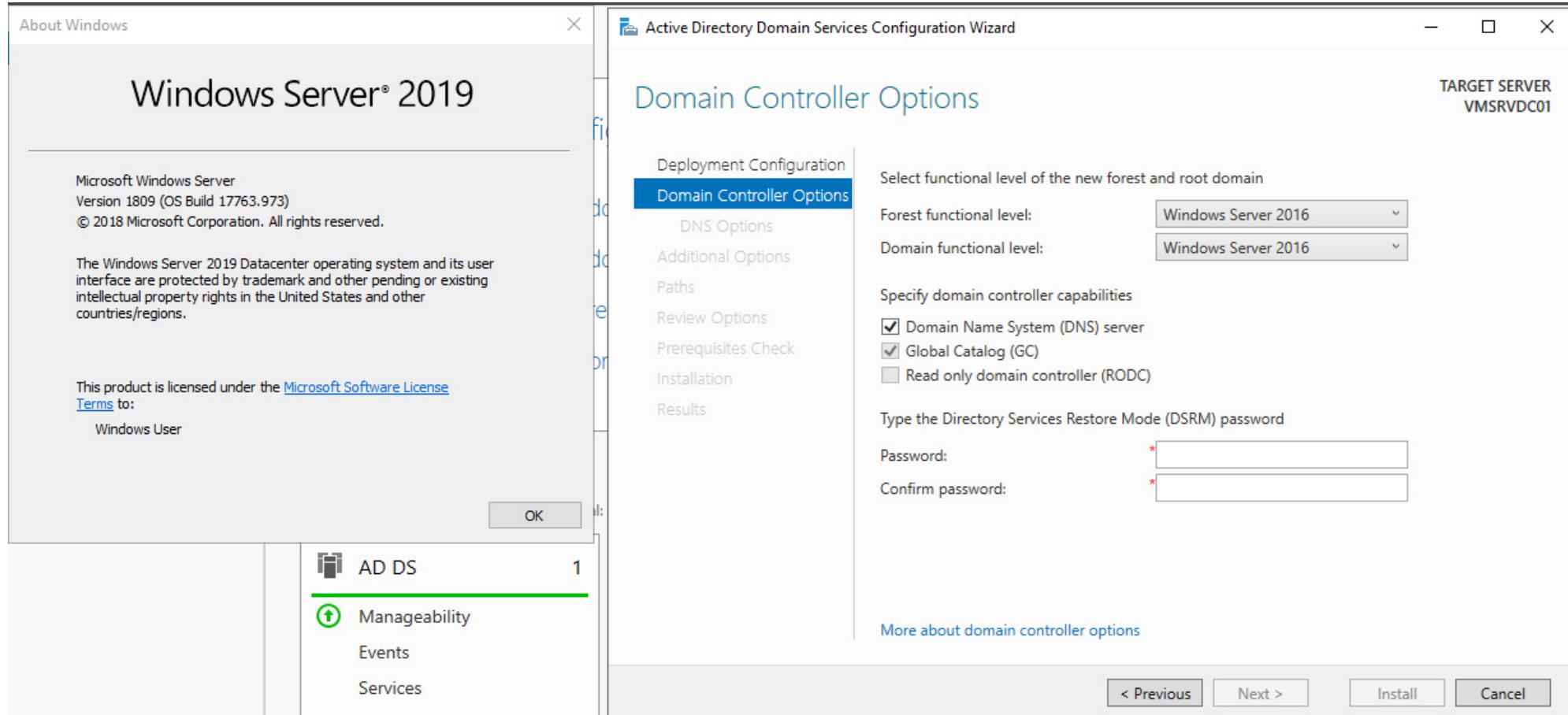


## ► ADDS Rollen Installation

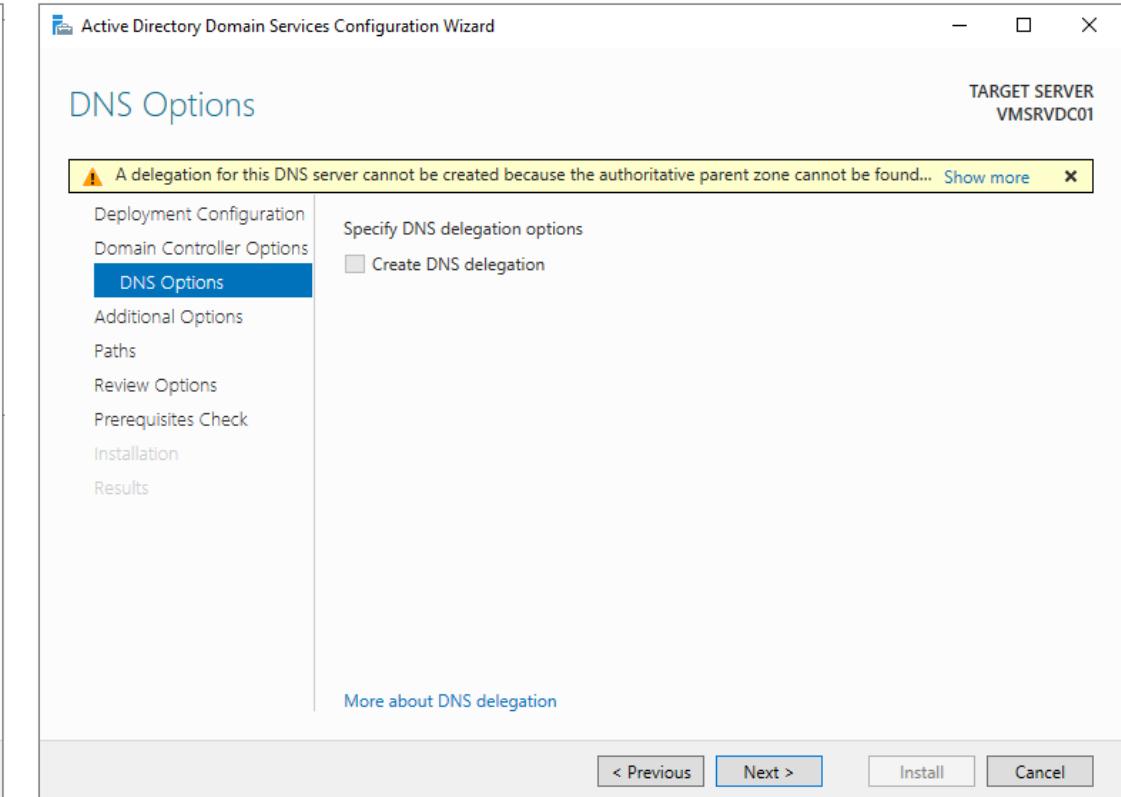
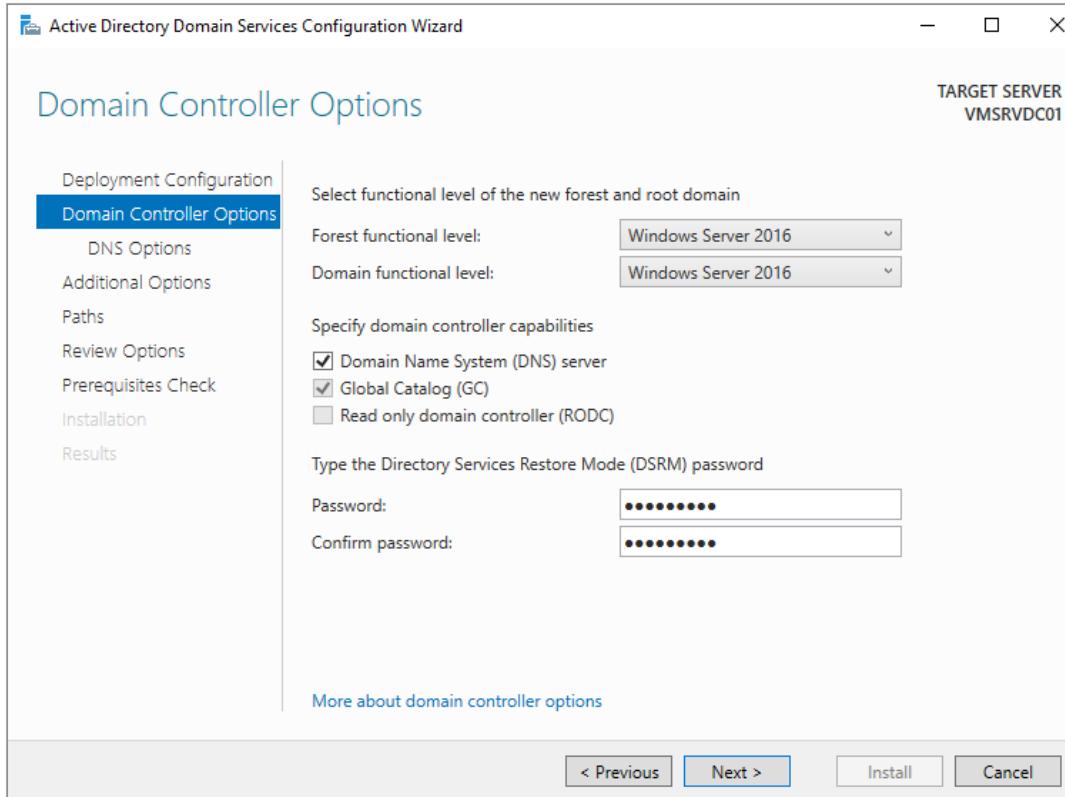
- Domain Name festlegen
- Initialen-tsbe.local
  - kw-tsbe.local
- Mit dem gleichen Wizard kann ein weiterer Domain Controller hinzugefügt werden oder eine neue Childdomain erstellt werden.



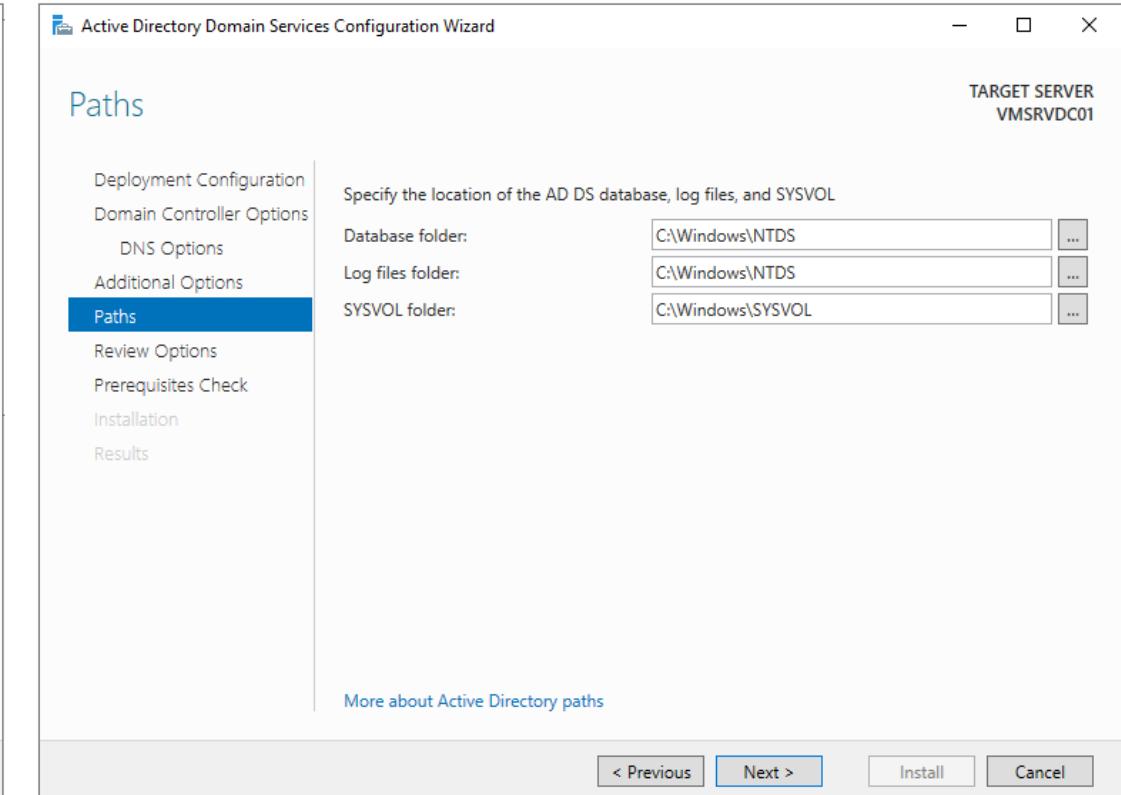
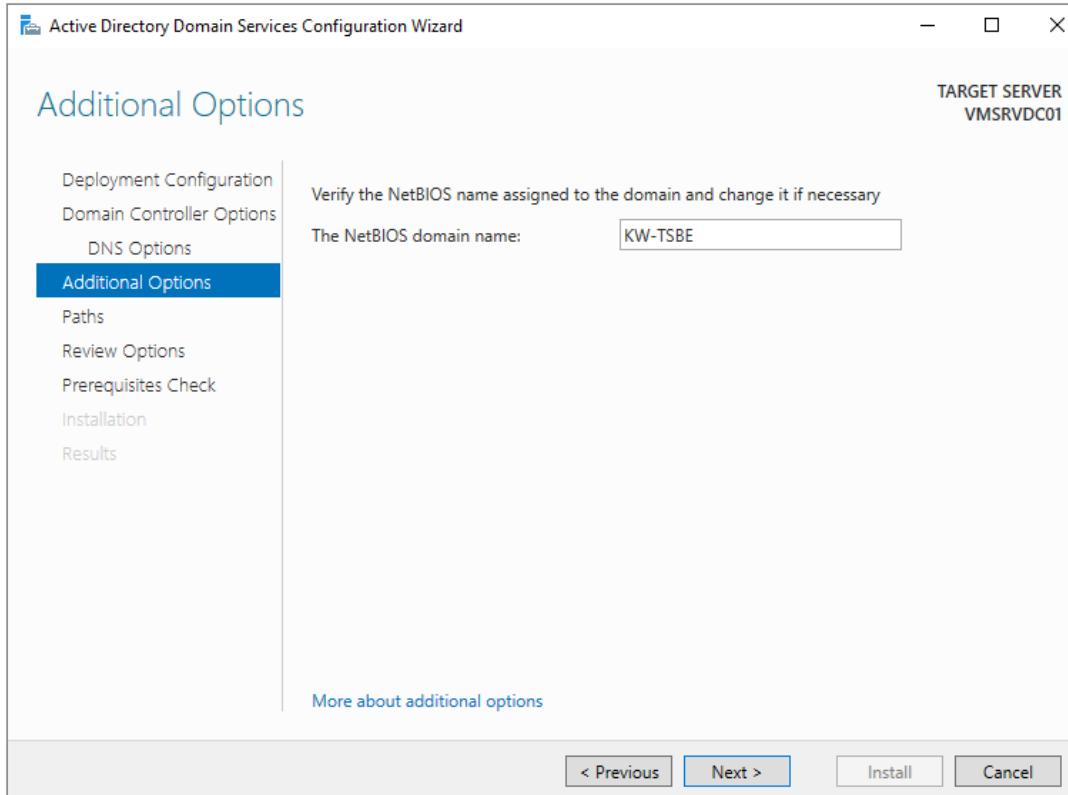
## ► Microsoft warum?



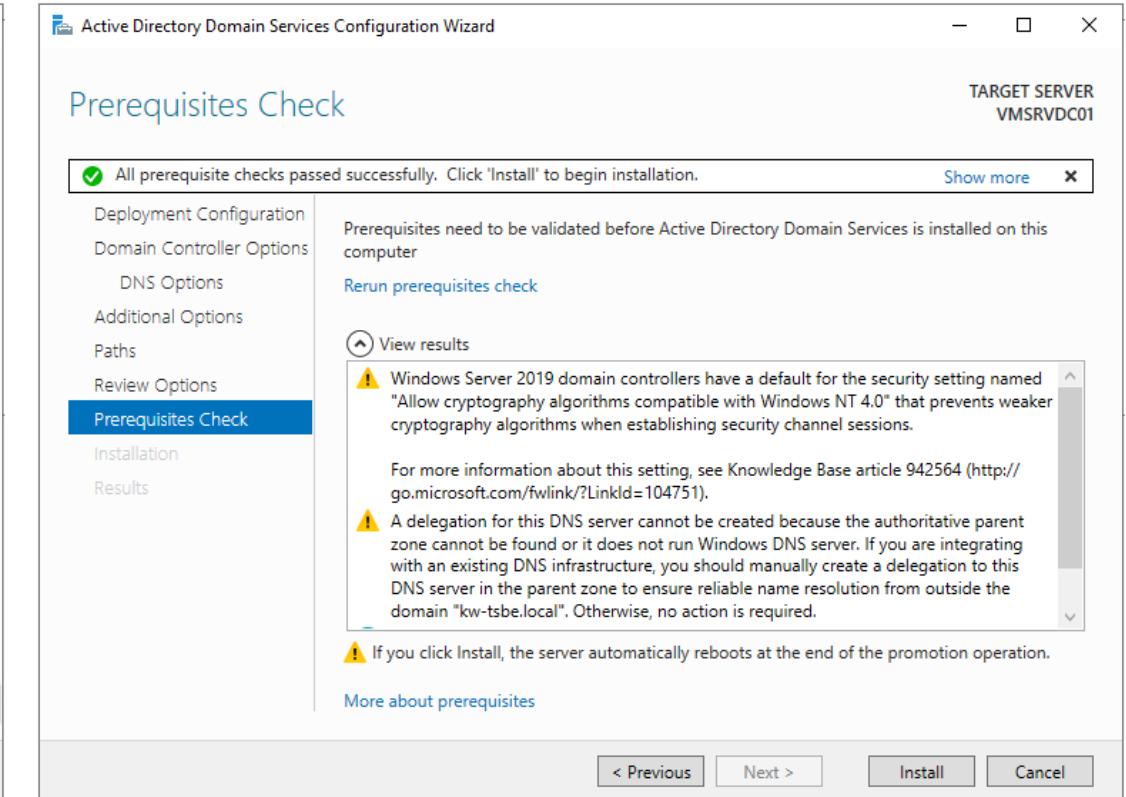
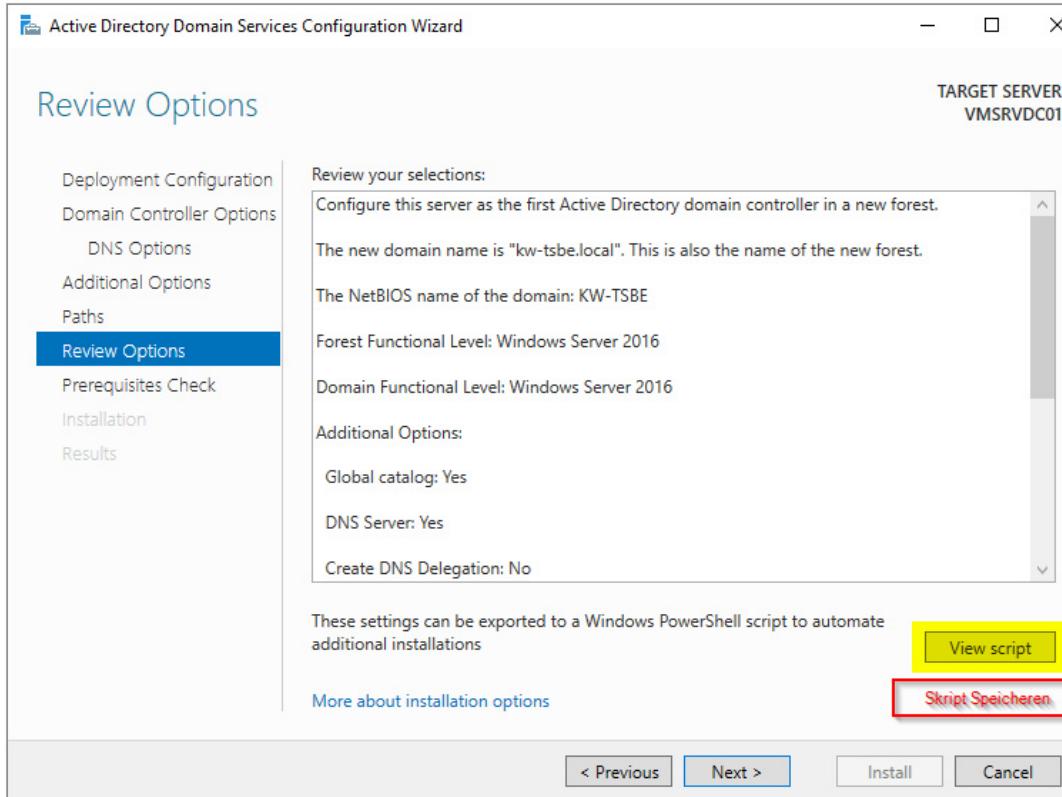
## ► ADDS Rollen Installation



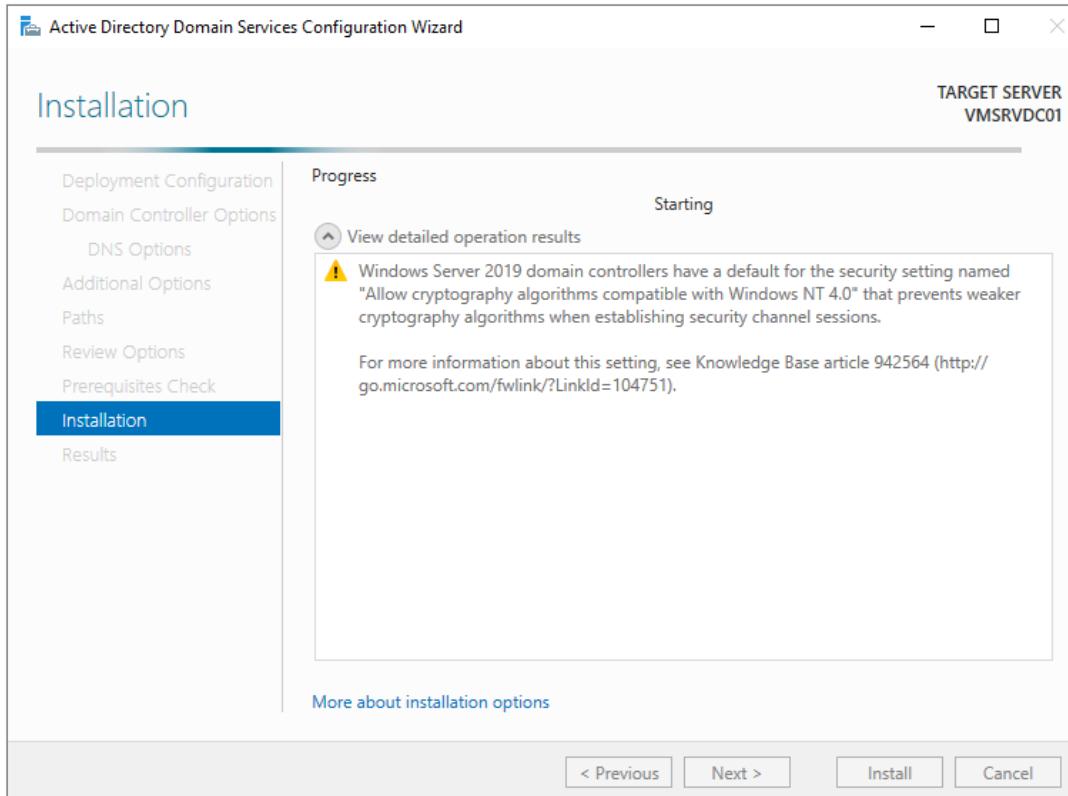
## ► ADDS Rollen Installation



## ► ADDS Rollen Installation

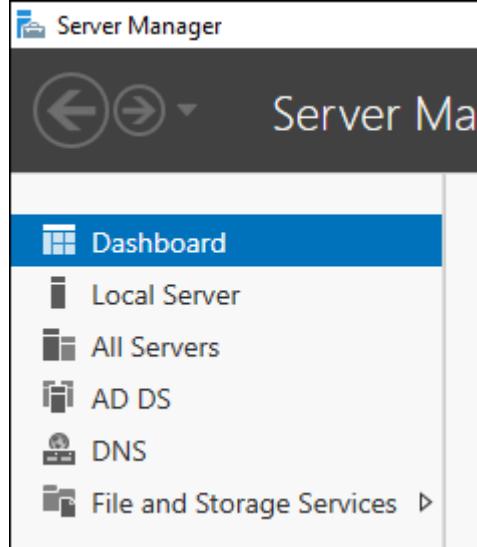


## ► ADDS Rollen Installation



- Neustart erfolgt nach der Installation
- Erstes Login erfolgt wieder mit domainadmin
- Domain ist installiert

## ► Neue Verwaltungstools

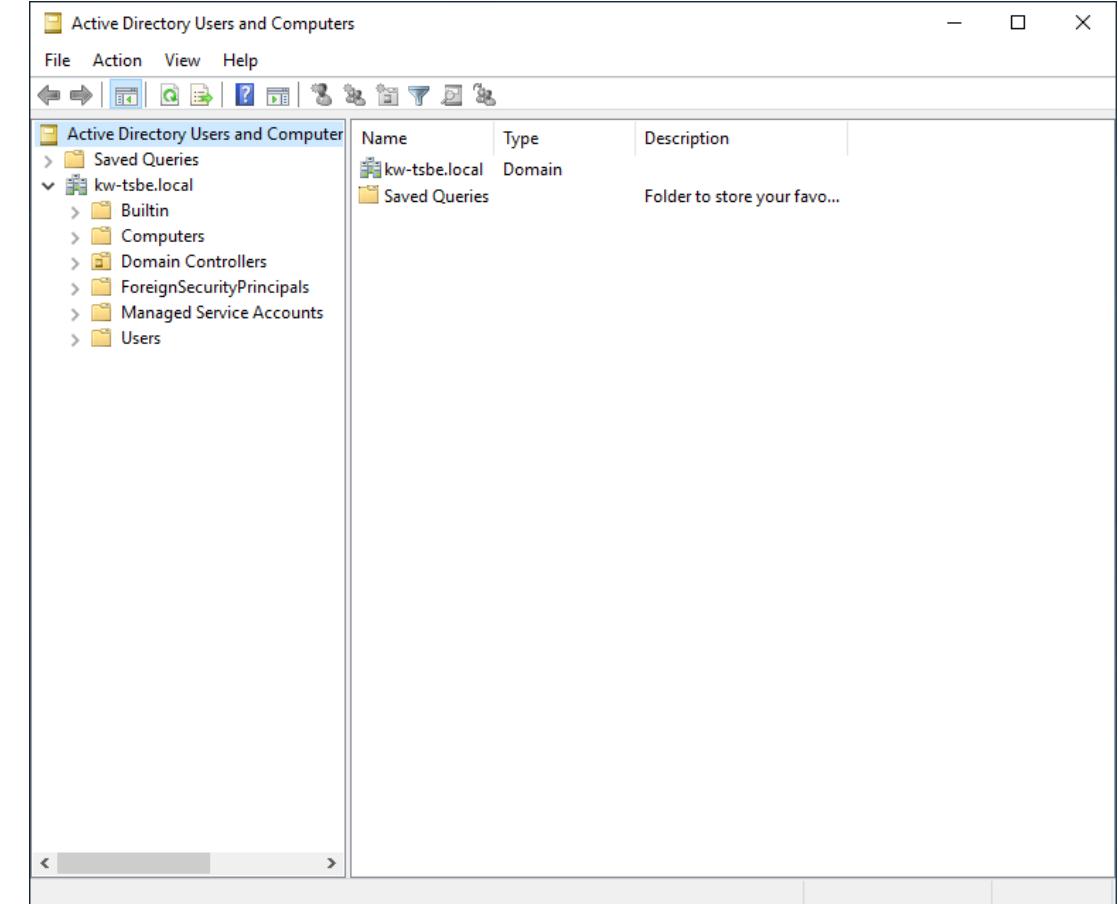


| Name                                      | Date modified    | Type        | Size |
|---|------------------|-------------|------|
| Terminal Services                         | 15.09.2018 09:19 | File folder |      |
| Active Directory Administrative Center    | 15.09.2018 09:13 | Shortcut    | 2 KB |
| Active Directory Domains and Trusts       | 15.09.2018 09:14 | Shortcut    | 2 KB |
| Active Directory Module for Windows Po... | 15.09.2018 09:13 | Shortcut    | 2 KB |
| Active Directory Sites and Services       | 15.09.2018 09:13 | Shortcut    | 2 KB |
| Active Directory Users and Computers      | 15.09.2018 09:14 | Shortcut    | 2 KB |
| ADSI Edit                                 | 15.09.2018 09:13 | Shortcut    | 2 KB |
| Component Services                        | 15.09.2018 09:12 | Shortcut    | 2 KB |
| Computer Management                       | 15.09.2018 09:12 | Shortcut    | 2 KB |
| Defragment and Optimize Drives            | 15.09.2018 09:12 | Shortcut    | 2 KB |
| Disk Cleanup                              | 15.09.2018 09:12 | Shortcut    | 2 KB |
| DNS                                       | 15.09.2018 09:13 | Shortcut    | 2 KB |
| Event Viewer                              | 15.09.2018 09:12 | Shortcut    | 2 KB |
| Group Policy Management                   | 15.09.2018 09:13 | Shortcut    | 2 KB |
| iSCSI Initiator                           | 15.09.2018 09:12 | Shortcut    | 2 KB |
| Local Security Policy                     | 15.09.2018 09:13 | Shortcut    | 2 KB |

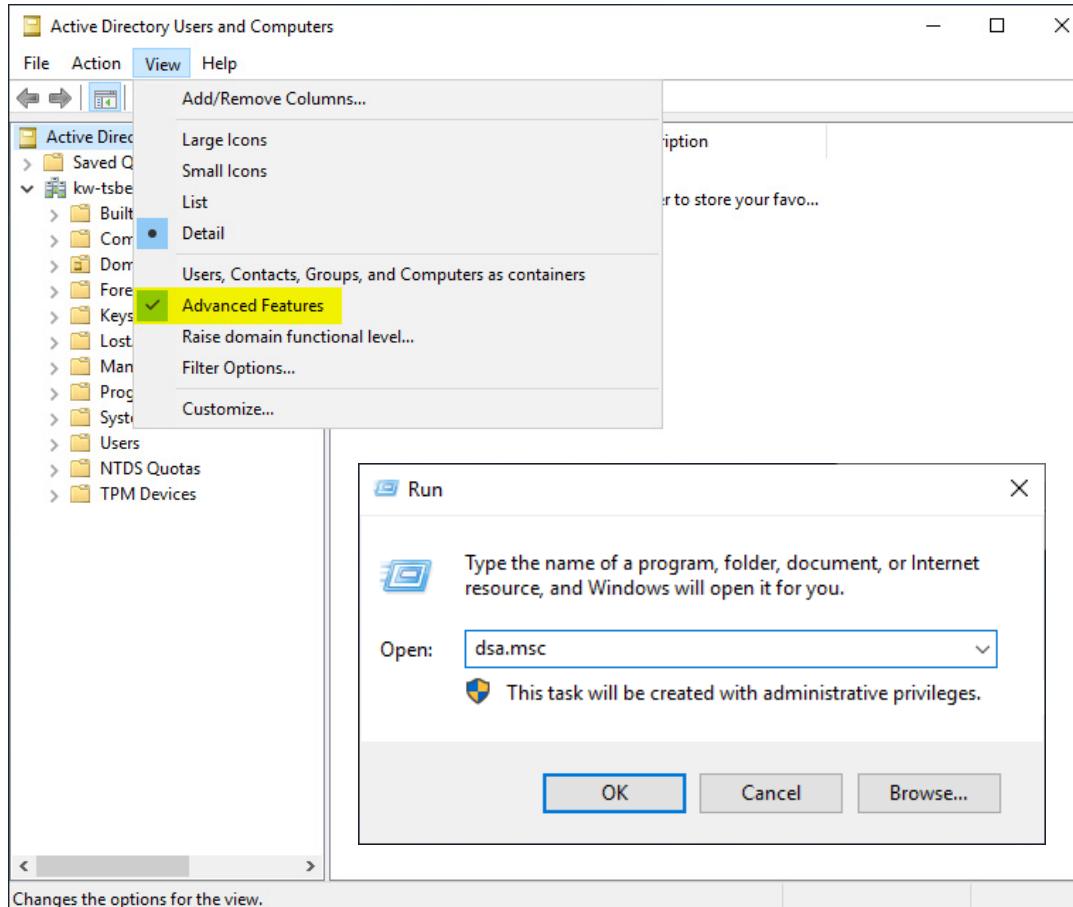
|  |
|--|
| Add Roles and Features                         |
| Shut Down Local Server                         |
| Computer Management                            |
| Remote Desktop Connection                      |
| Windows PowerShell                             |
| Configure NIC Teaming                          |
| Active Directory Administrative Center         |
| Active Directory Domains and Trusts            |
| Active Directory Module for Windows PowerShell |
| Active Directory Sites and Services            |
| Active Directory Users and Computers           |
| ADSI Edit                                      |
| Dcdiag.exe                                     |
| Dsacls.exe                                     |
| Dsdbutil.exe                                   |
| Dsmgmt.exe                                     |
| Gpfixup.exe                                    |
| Ldp.exe  |
| Netdom.exe                                     |
| Nltest.exe                                     |
| Ntdsutil.exe                                   |
| Repadmin.exe                                   |
| W32tm.exe                                      |
| Manage As ...                                  |
| Start Performance Counters                     |
| Refresh  |
| Copy   |

## ► Active Directory Users and Computers

- Verwaltung von Active Directory Objekten:
  - User
  - Computer
  - Gruppen



## ► Active Directory Users and Computers



| Name                       | Type              | Description                  |
|----------------------------|-------------------|------------------------------|
| Allowed RODC Password ...  | Security Group... | Members in this group c...   |
| Cert Publishers            | Security Group... | Members of this group ...    |
| Cloneable Domain Contr...  | Security Group... | Members of this group t...   |
| Denied RODC Password R...  | Security Group... | Members in this group c...   |
| DnsAdmins                  | Security Group... | DNS Administrators Gro...    |
| DnsUpdateProxy             | Security Group... | DNS clients who are per...   |
| Domain Admins              | Security Group... | Designated administrato...   |
| Domain Computers           | Security Group... | All workstations and ser...  |
| Domain Controllers         | Security Group... | All domain controllers i...  |
| Domain Guests              | Security Group... | All domain guests            |
| Domain Users               | Security Group... | All domain users             |
| domainadmin                | User              | Built-in account for ad...   |
| Enterprise Admins          | Security Group... | Designated administrato...   |
| Enterprise Key Admins      | Security Group... | Members of this group ...    |
| Enterprise Read-only Do... | Security Group... | Members of this group ...    |
| Group Policy Creator Ow... | Security Group... | Members in this group c...   |
| Guest                      | User              | Built-in account for gue...  |
| Key Admins                 | Security Group... | Members of this group ...    |
| krbtgt                     | User              | Key Distribution Center ...  |
| Protected Users            | Security Group... | Members of this group ...    |
| RAS and IAS Servers        | Security Group... | Servers in this group can... |
| Read-only Domain Contr...  | Security Group... | Members of this group ...    |
| Schema Admins              | Security Group... | Designated administrato...   |

## ▶ Enable Recycle Bin

Active Directory Administrative Center

kw-tsbe (local)

Active Directory... Overview kw-tsbe (local) (13)

Builtin

| Name                      | Type          | Description                    |
|---------------------------|---------------|--------------------------------|
| Builtin                   | Container     | builtinDom...                  |
| Computers                 | Container     | Default container for upgr...  |
| Domain Controllers        | Organizati... | Default container for dom...   |
| ForeignSecurityPrincipals | Container     | Default container for secur... |
| Infrastructure            |               | infrastructu...                |
| Keys                      | Container     | Default container for key o... |
| LostAndFound              | lostAndFou... | Default container for orph...  |
| Managed Service Accounts  | Container     | Default container for man...   |
| NTDS Quotas               | msDS-Quo...   | Quota specifications conta...  |
| Program Data              | Container     | Default location for storag... |
| System                    | Container     | Builtin system settings        |
| TPM Devices               | msTPM-Inf...  |                                |

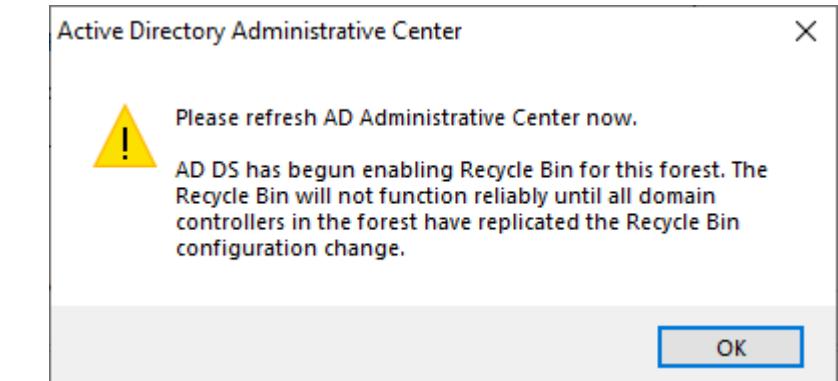
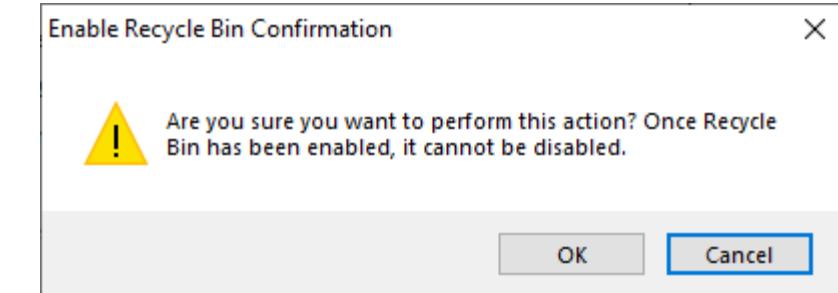
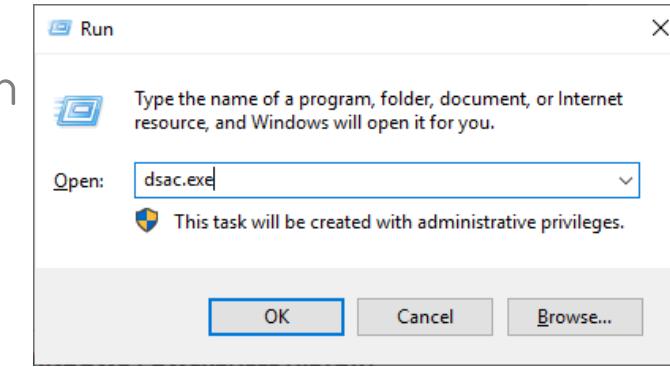
Builtin

Object class: builtinDomain Modified: 19.01.2020 14:54

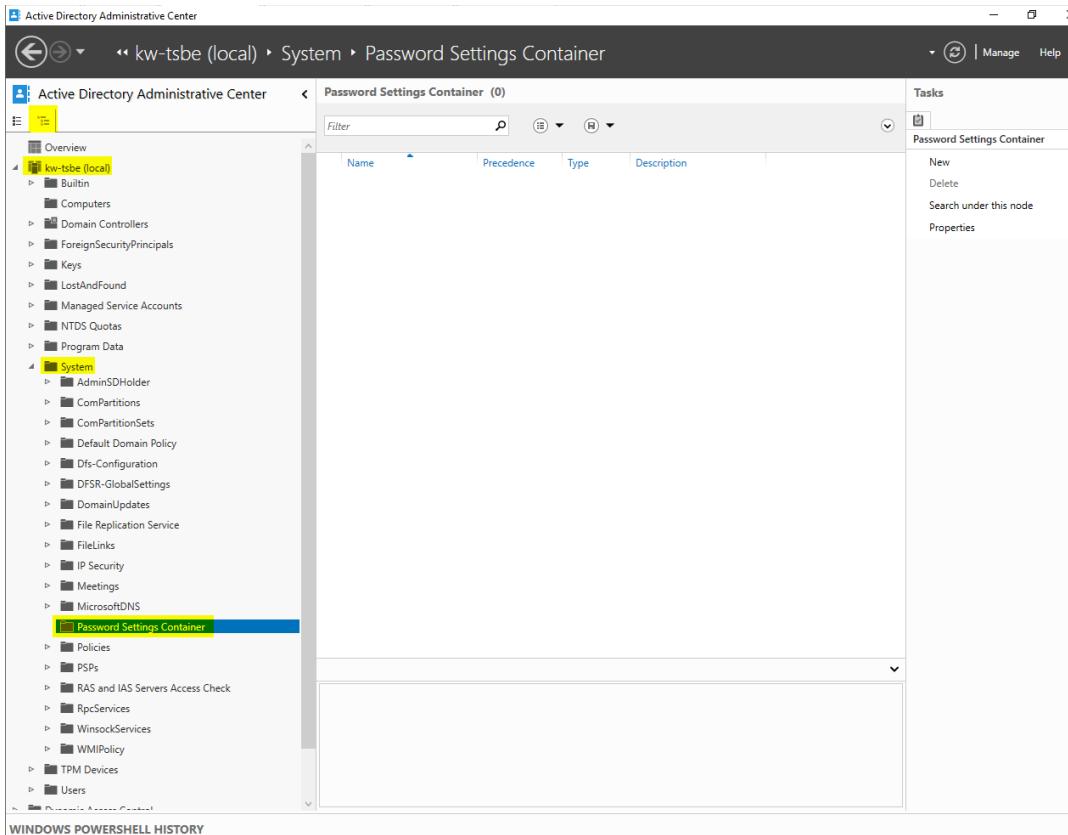
Description:

Summary

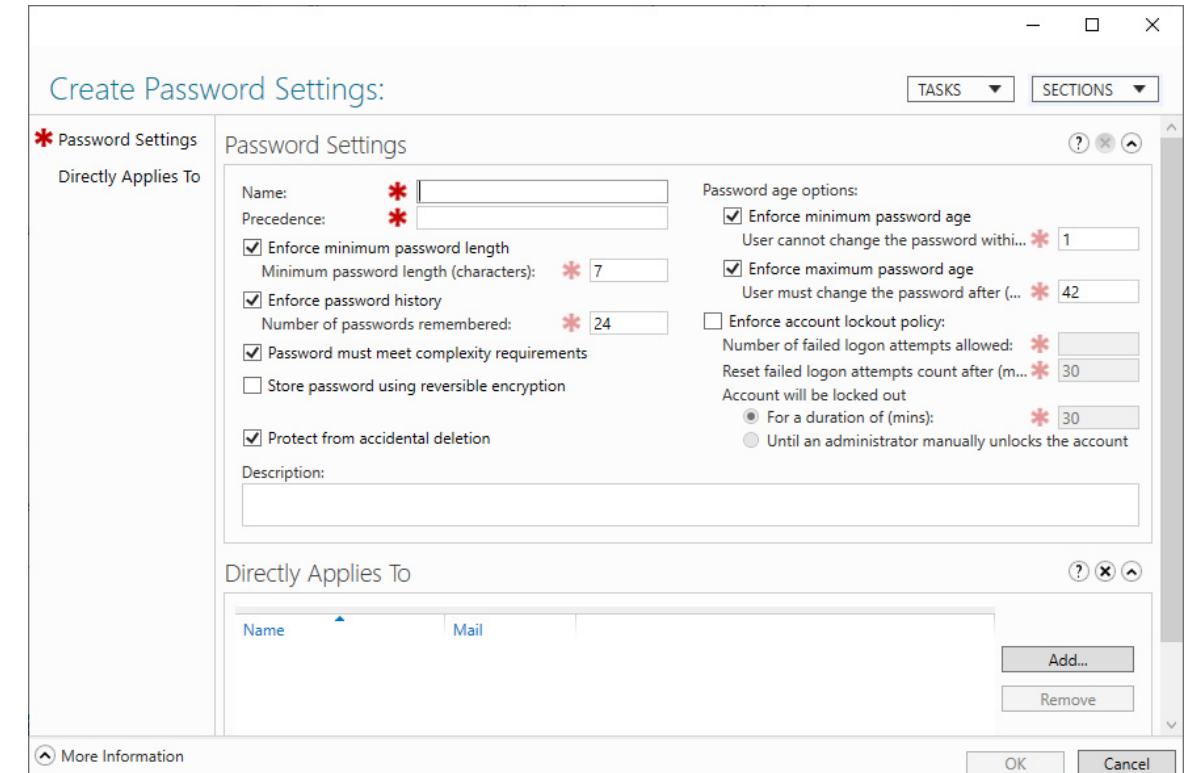
WINDOWS POWERSHELL HISTORY



## ► Fine-Grained Password Policy



- Rechtsklick -> New -> Passwords Settings



- Konfiguration erfolgt mit CMD
  - w32tm /config /manualpeerlist:[ntp.metas.ch](http://ntp.metas.ch) /syncfromflags:manual /reliable:yes /update
  - w32tm /config /update
  - net stop w32time
  - net start w32time
  - w32tm /query /peers
  - w32tm /query /status
  - w32tm /query /configuration

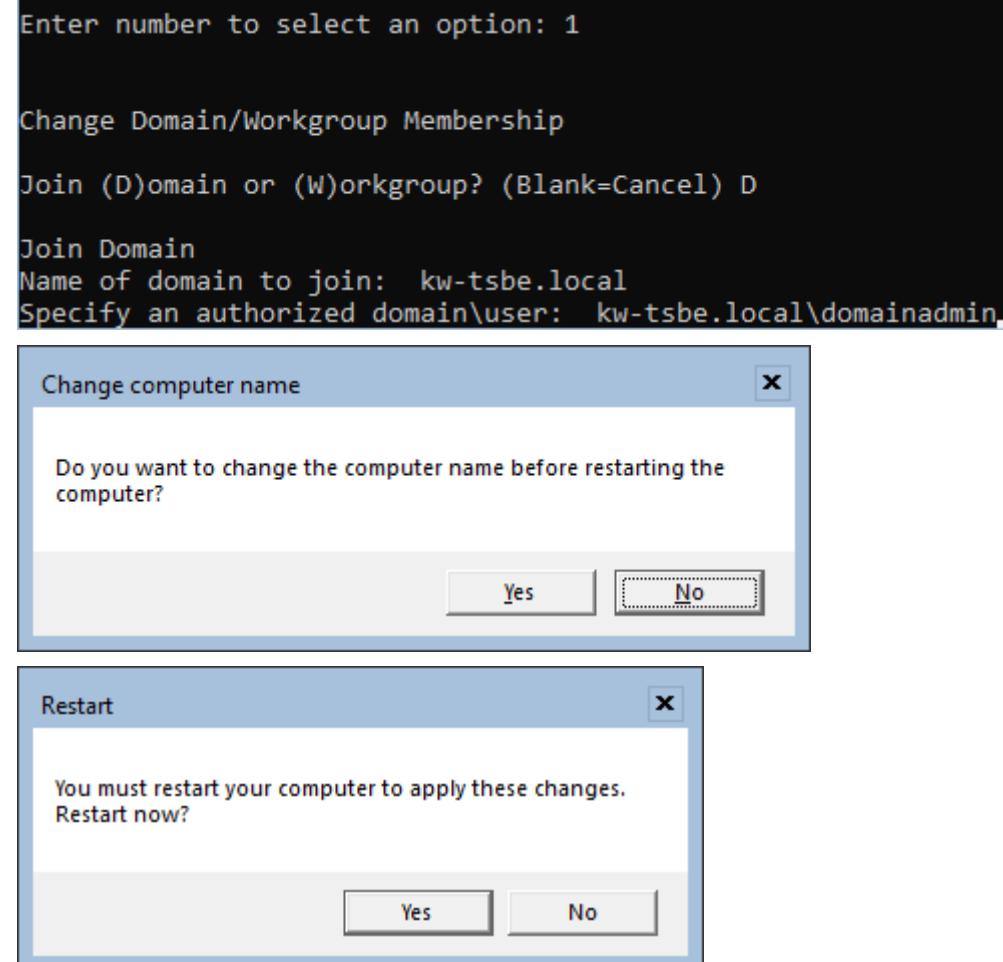
## ► Core Server Domain Join

## ■ DNS Anpassen

- Sconfig
- 8 -> 1 -> 2
- 192.168.210.10 -> Enter
- Enter

## ■ Domain Join

- Sconfig
- 1 -> D ->



► User Switch an Core Server

- Entsperren mit CTRL + ALT + DLE (INSERT)
  - ESC
  - Other User
  - Benutzername und Passwort eingeben

```
Enter credentials for Administrator or hit ESC to switch users/sign-in methods
Password : 
Select a user
Administrator
Other user

Enter credentials for Other user or hit ESC to switch users/sign-in methods
User name : domainadmin
Password : *****
Sign in to: KW-TSBE
How do I sign in to another domain?
```

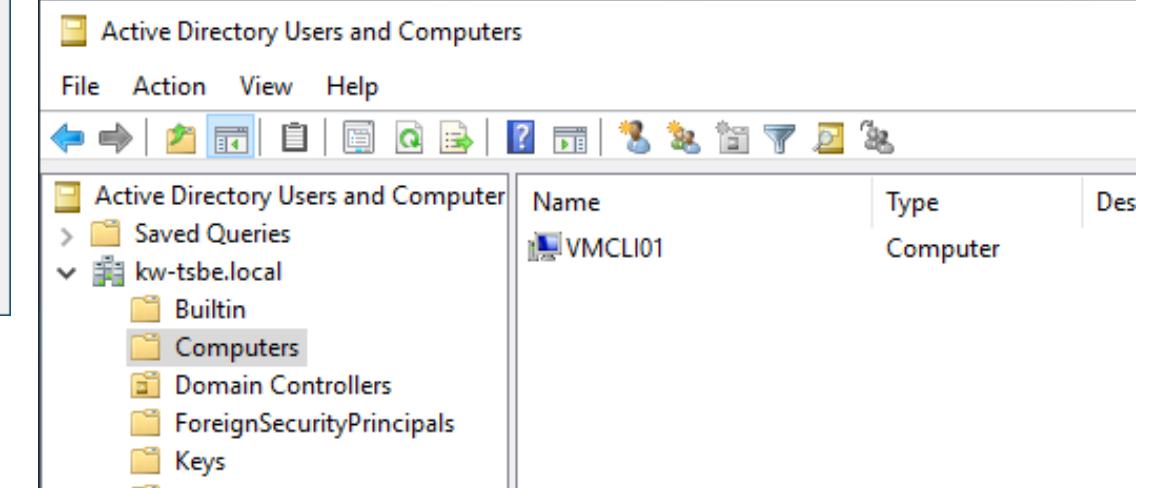
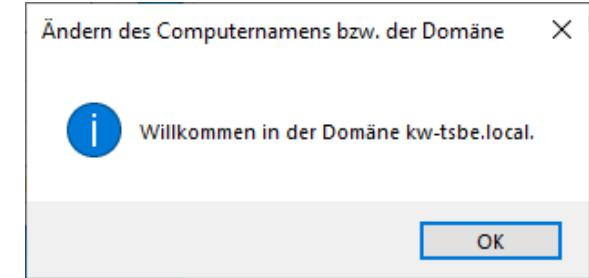
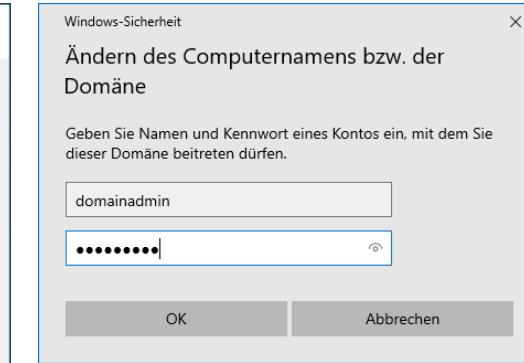
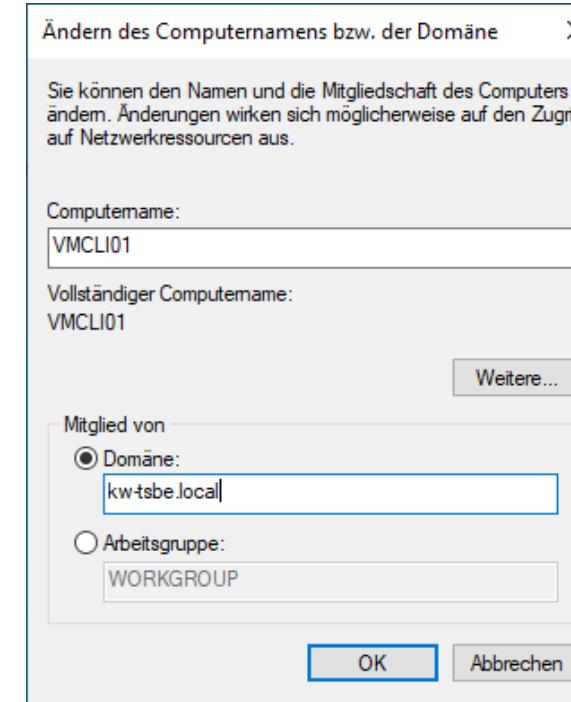
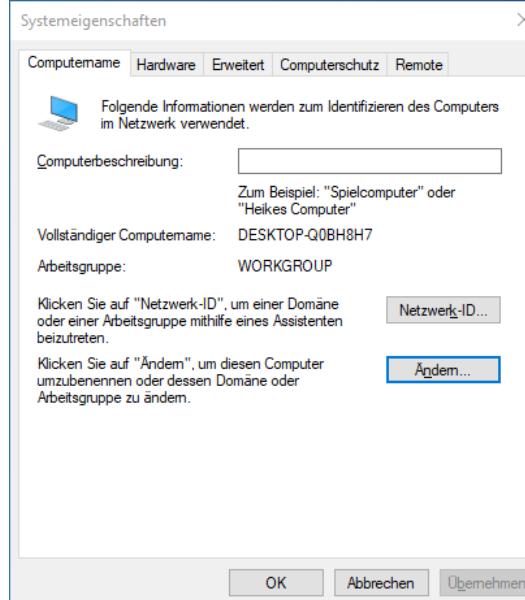
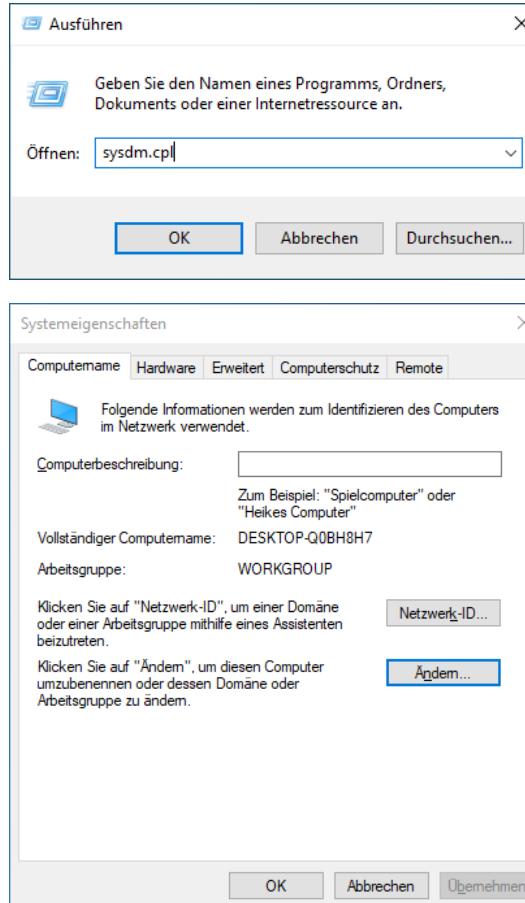
## ► Client in die Domain aufnehmen

## IP Adresse Konfiguration

The image shows three windows from a Windows operating system:

- Ausführen** window: Shows the command `ncpa.cpl` entered in the "Öffnen:" field. Buttons: OK, Abbrechen, Durchsuchen....
- Eigenschaften von Ethernet0** window:
  - Netzwerk tab: Verbindung herstellen über: Intel(R) 82574L Gigabit Network Connection. Konfigurieren... button.
  - Diese Verbindung verwendet folgende Elemente:
    - Client für Microsoft-Netzwerke
    - Datei- und Druckerfreigabe für Microsoft-Netzwerke
    - QoS-Paketplaner
    - Internetprotokoll, Version 4 (TCP/IPv4)
    - Microsoft-Multiplexprotokoll für Netzwerkadapter
    - Microsoft-LLDP-Treiber
    - Internetprotokoll, Version 6 (TCP/IPv6)
  - Buttons: Installieren..., Deinstallieren, Eigenschaften.
  - Beschreibung: TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den Datenaustausch über verschiedene, miteinander verbundene Netzwerke ermöglicht.
- Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)** window:
  - Allgemein tab: IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
  - IP-Adresse automatisch beziehen
  - Folgende IP-Adresse verwenden:
    - IP-Adresse: 192 . 168 . 210 . 50
    - Subnetzmaske: 255 . 255 . 255 . 0
    - Standardgateway: 192 . 168 . 210 . 1
  - DNS-Serveradresse automatisch beziehen
  - Folgende DNS-Serveradressen verwenden:
    - Bevorzugter DNS-Server: 192 . 168 . 210 . 10
    - Alternativer DNS-Server: . . .
  - Einstellungen beim Beenden überprüfen
  - Buttons: Erweitert..., OK, Abbrechen.

## ► Client Domain Join



- Konzipieren und erstellen einer OU Struktur
  - Die TSBE als Schule soll abgebildet werden
  - Computer-, Server- und User-objekte für Studenten und Dozenten sollen organisiert werden können



Microsoft System Administration

# Domain Name System

- Die studierenden
  - können DNS grundkonfigurieren
  - verstehen was AD integrierte DNS Zonen sind

- Korrekte und vollständige Konfiguration des DNS Server
  - Forwarder
  - Revers Lookup Zone
  - Zusätzliche AD integrierte Forward Zone testdomain.ch
  - DNS Aging

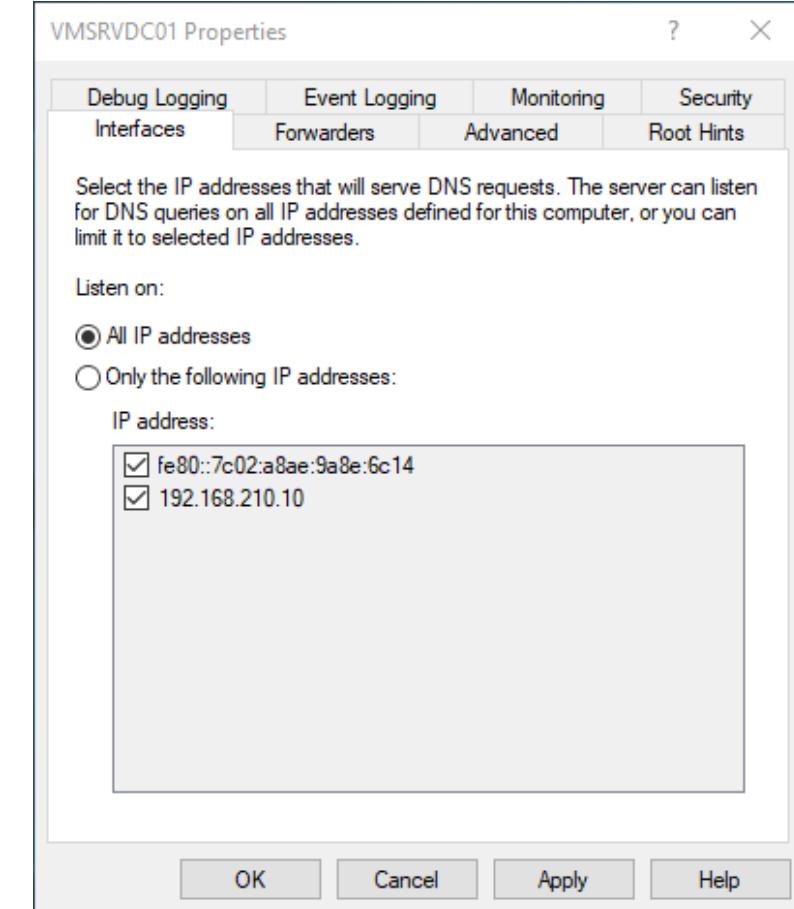
- [Domain Name System \(DNS\) | Microsoft Learn](#)
- Microsoft Windows Server 2012 R2 – Das Handbuch S. 843
- Windows Server 2019 – Schieb S. 358

- Namensauflösung -> google.ch -> 172.217.168.35
  - Forward Lookup Zones → Name zu IP
  - Revers Lookup Zones → IP zu Name
- Fixer Bestandteil von Active Directory
- Eigene Zonen können gehostet werden
  - Achtung Split DNS beachten
- Kann veröffentlicht werden
- Port 53 UDP/TCP

- Verwaltung
  - GUI: DNS MMC
  - Konsole: dnscmd
- Forward Lookup Zone
  - \_msdcs.kw-tsbe.local
  - kw-tsbe.local
- Reverse Lookup Zone
  - Muss manuell erstellt werden
- Standard Zonen sind Active Directory integriert
  - Ntds.dit
- Über DNS finden die Clients:
  - Actice Directory
  - Global Catalog
  - PDC Emulator
  - Domains
- Jede Domain in der Gesamtstruktur hat eine eigene Zone
- FQDN Beispiel:
  - SRVDC01.kw-tsbe.local

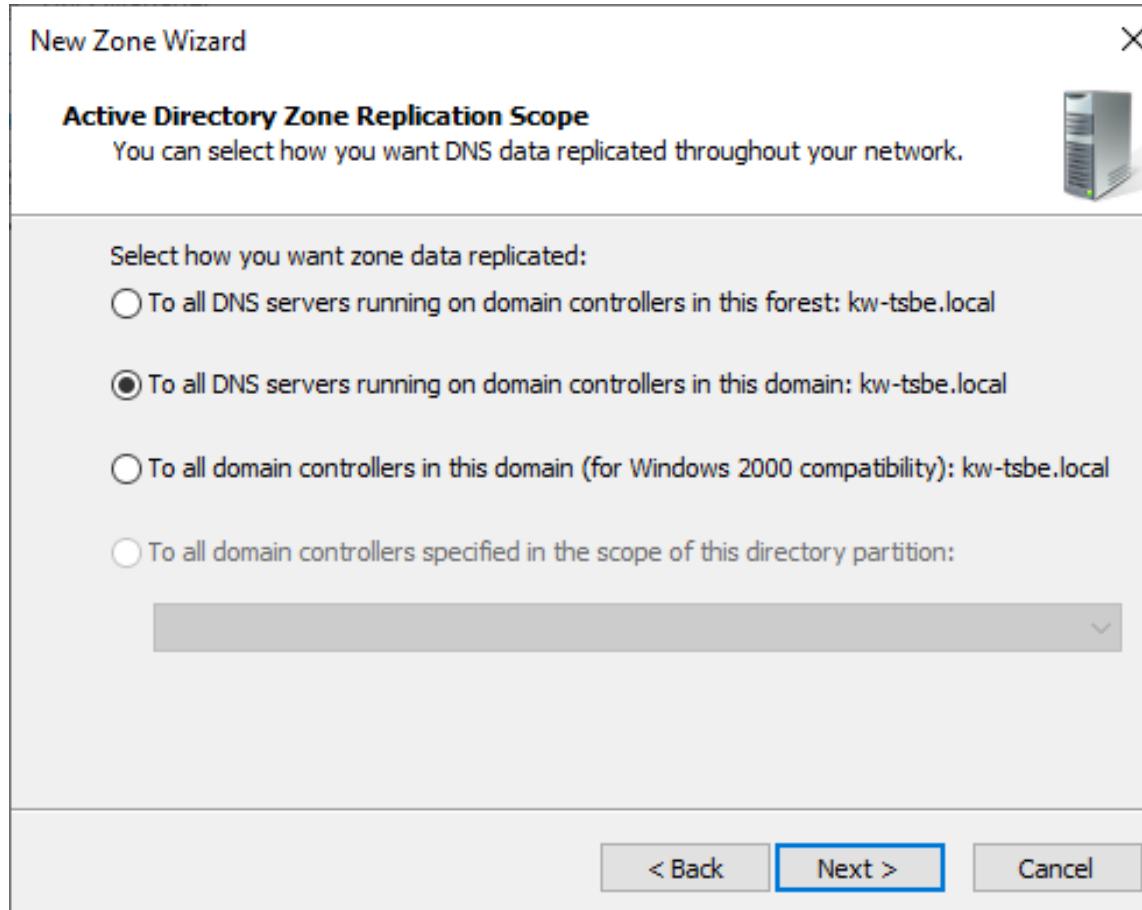
## ► Konfigurationen/Verwaltung

- Listening Interface
  - IPv4, IPv6
- Forwarders
  - Roots hints
  - Internet Service Provider
- Debug und Event Logging
- DNS Aging



- Primary zone
  - Neue Zone
- Secondary zone
  - Bereits vorhanden Zone (Redundanz)
  - Bei AD integrierten Zonen muss dies nicht konfiguriert werden
- Stub zone
- Active Directory integriert
  - Zonen werden direkt in die AD Datenbank geschrieben und so an andere DCs mit DNS repliziert

## ► AD Zone Replication Scope



- Zone kann im Gesamten Forest repliziert werden
- Zone kann aber auch nur innerhalb einer Domain repliziert werden

- Domain Admins
  - Domain DNS Zone kann administriert werden
- Enterprise Admins
  - Können alle DNS Zonen administrieren
  - Domain und Forest
- DNSAdmins (pro Domain)
  - Einzelne User können berechtigt werden um die DNS Zonen der Domain zu administrieren

- Dynamische Updates
- DNS Aging
  - Aufräumen von DNS
- SOA Eintrag
  - Pro Zone vorhanden
- Name Server Übersicht
- Zonen Transfer konfigurierbar (Wenn nicht AD integriert muss dies manuell konfiguriert werden)

► Conditional Forwarder

- Weiterleitung an andere DNS Server innerhalb der Organisation
- Beim erstellen einer Domänen Vertrauensstellung notwendig

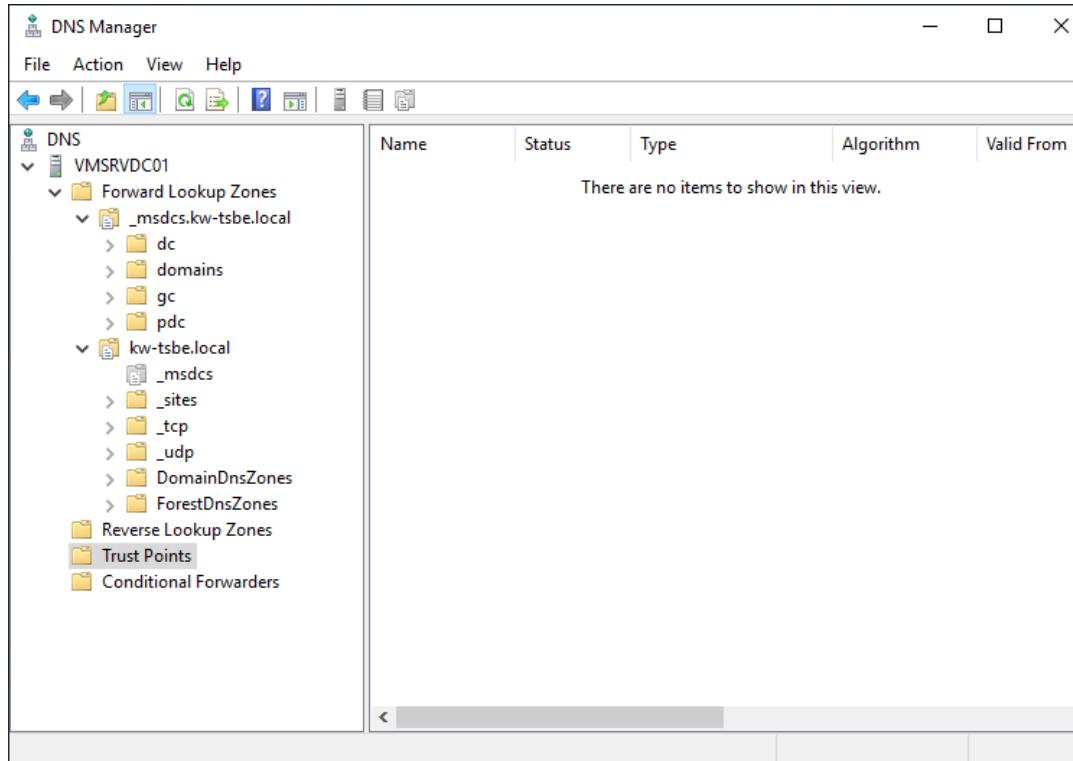
Learning by doing

# PRACTICE

- Korrekte Konfiguration:
  - Listening Interface
  - Forwarders
  - DNS Aging
- Erstellung einer neuen Zone
  - Reverse Zone erstellen
  - Testdomain.ch
    - Standalone
    - Wichtig: Anschliessend AD integrieren

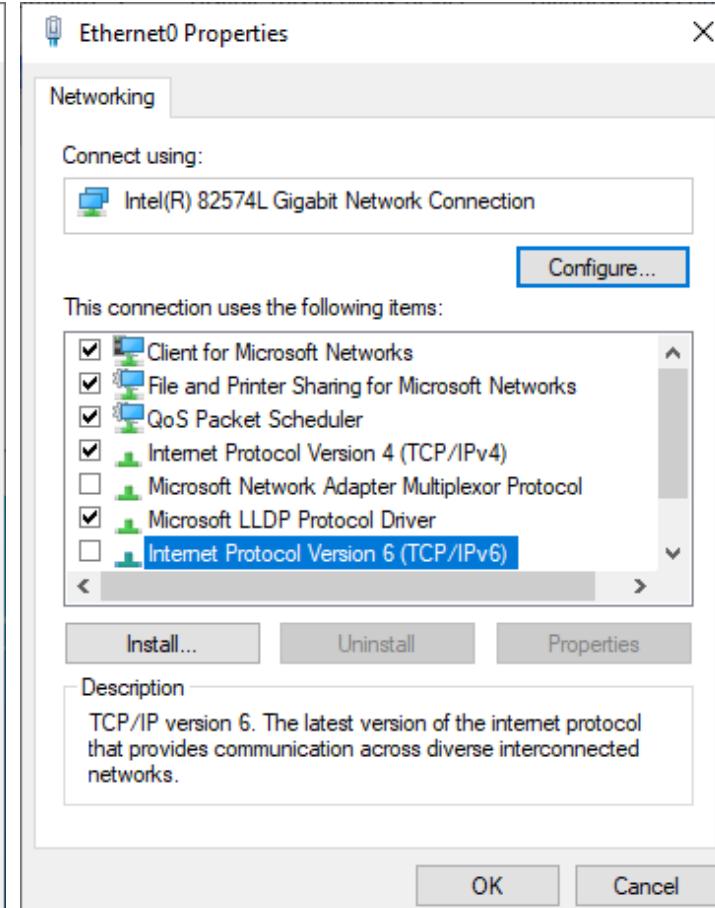
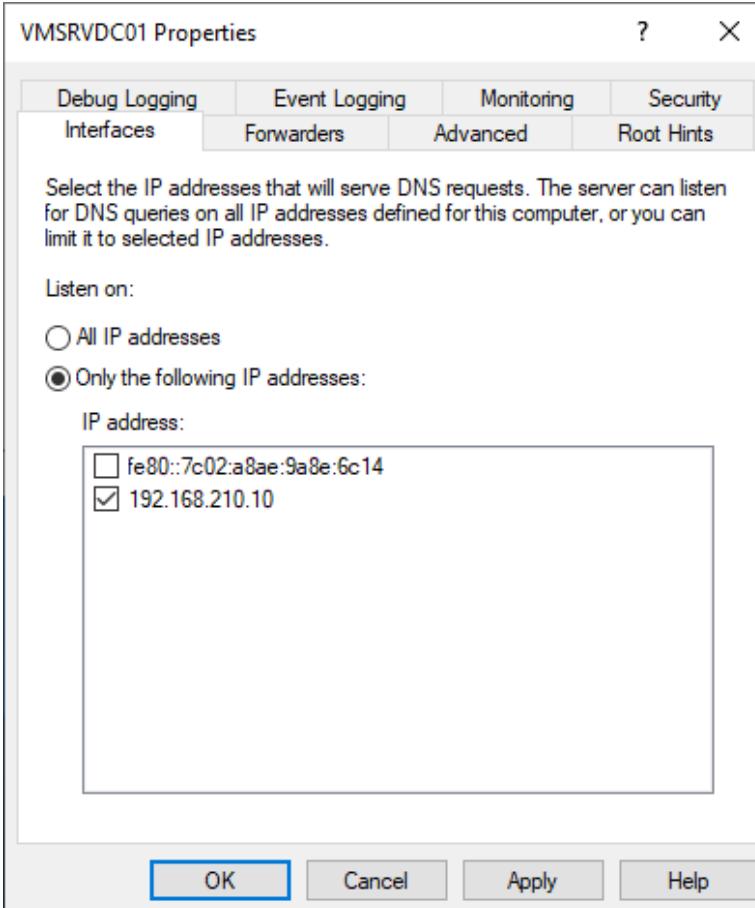
- DNS Cache einblenden im GUI
  - Wo findet sich dies?
- Konsole dnscmd und PowerShell
  - Server Cache leeren
  - Sicherung der DNS Zonen ausführen
  - Kommandozeilentools kennenlernen

## ► DNS Konfiguration



- DNS Server Einstellungen öffnen
- Rechtsklick auf den Servernamen → Properties

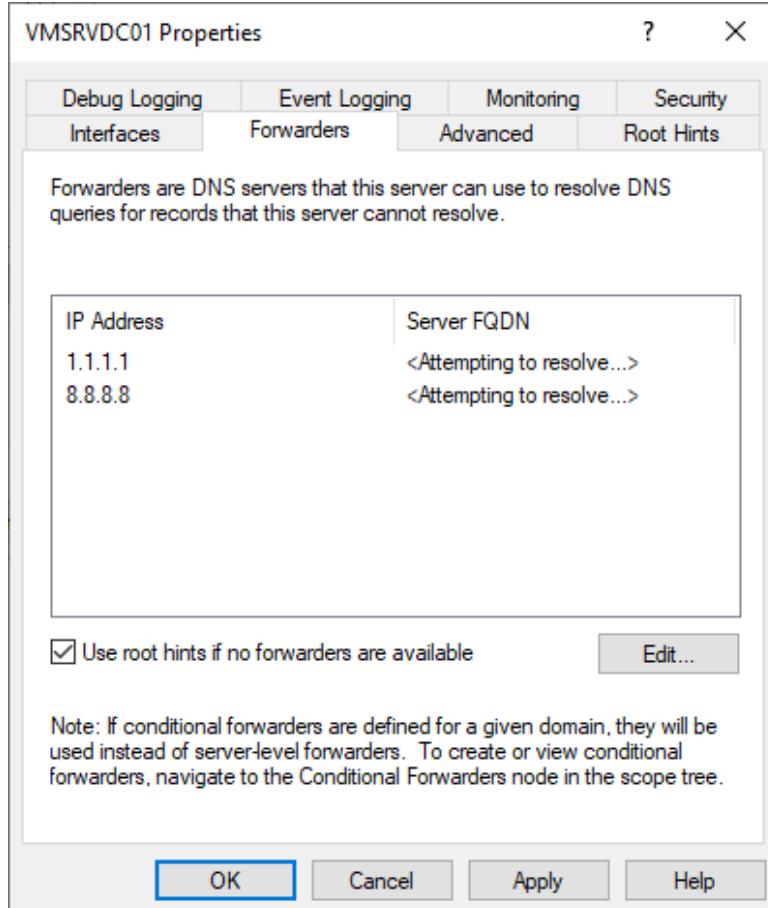
## ► DNS Konfiguration



Wenn IPv6 im Netzwerk nicht konfiguriert ist empfiehlt es sich dieses unter dem Netzwerk Adapter zu deaktivieren.

**ACHTUNG:** bei einem Exchange Server darf dies nicht gemacht werden!

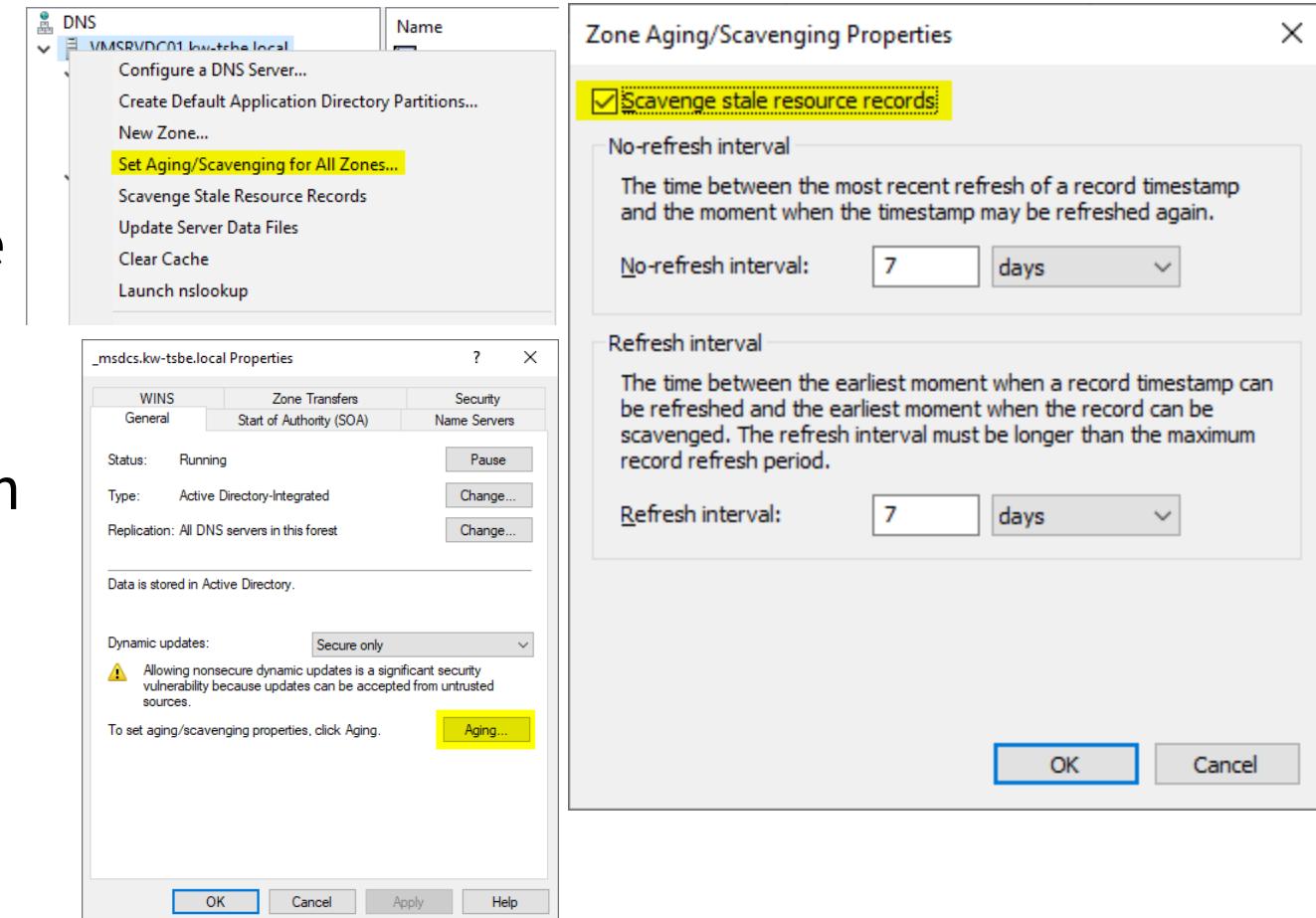
## ► DNS Konfiguration



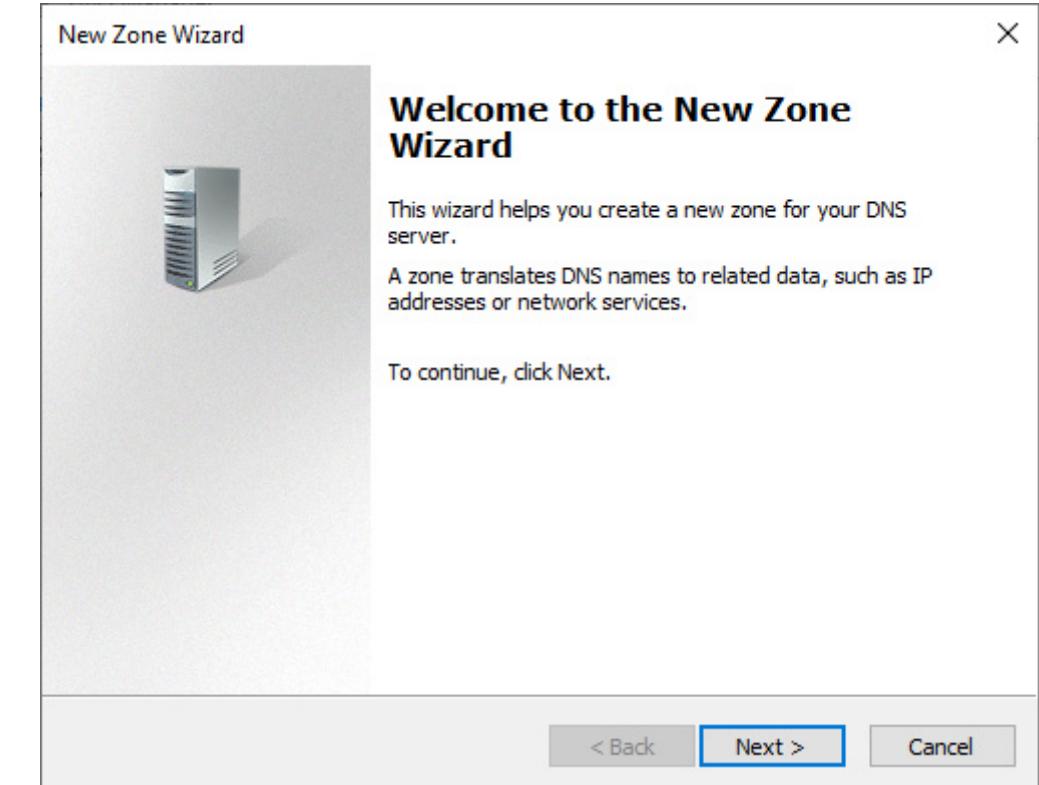
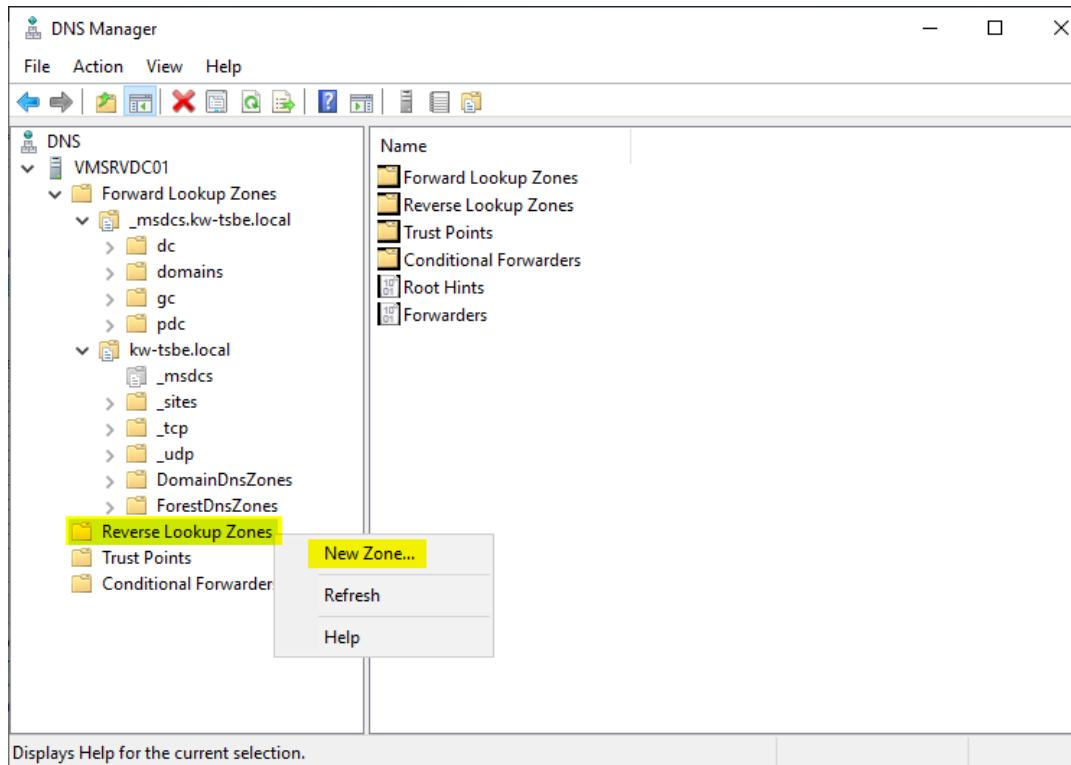
- Am besten DNS Server vom ISP als Forwarders eintragen
- Theoretisch nicht nötig da auch die Root hints vorhanden sind
- Root hints sind die weltweiten Root DNS Server

## ► DNS Konfiguration Aging

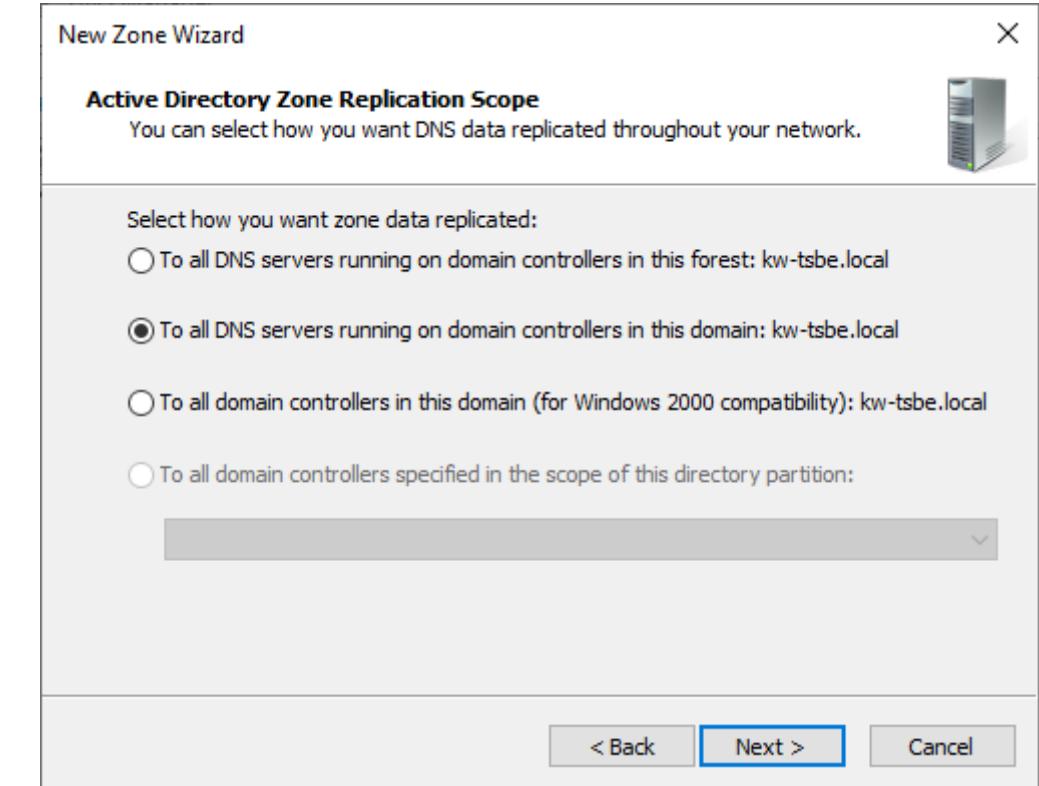
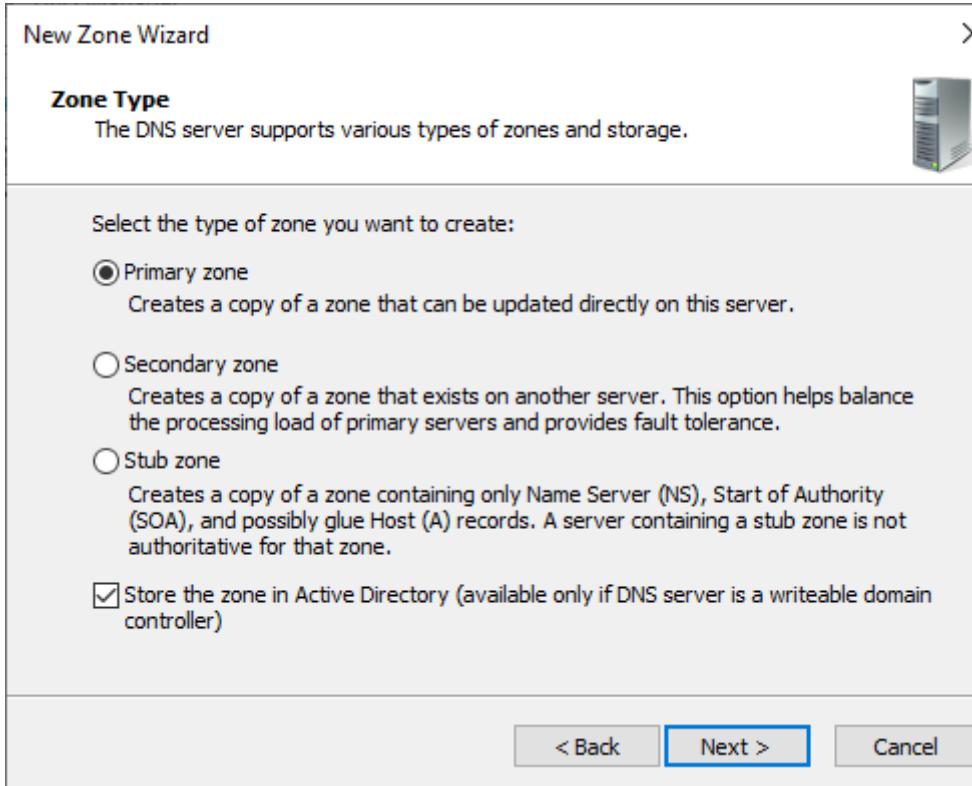
- DNS Aging löscht DNS Einträge die älter als der definierte Wert sind
- Geräte aktualisieren normalerweise ihre Einträge dynamisch
- Die Konfiguration kann pro Zone gemacht werden oder für alle Zonen
  - Rechtsklick auf Zone → Properties



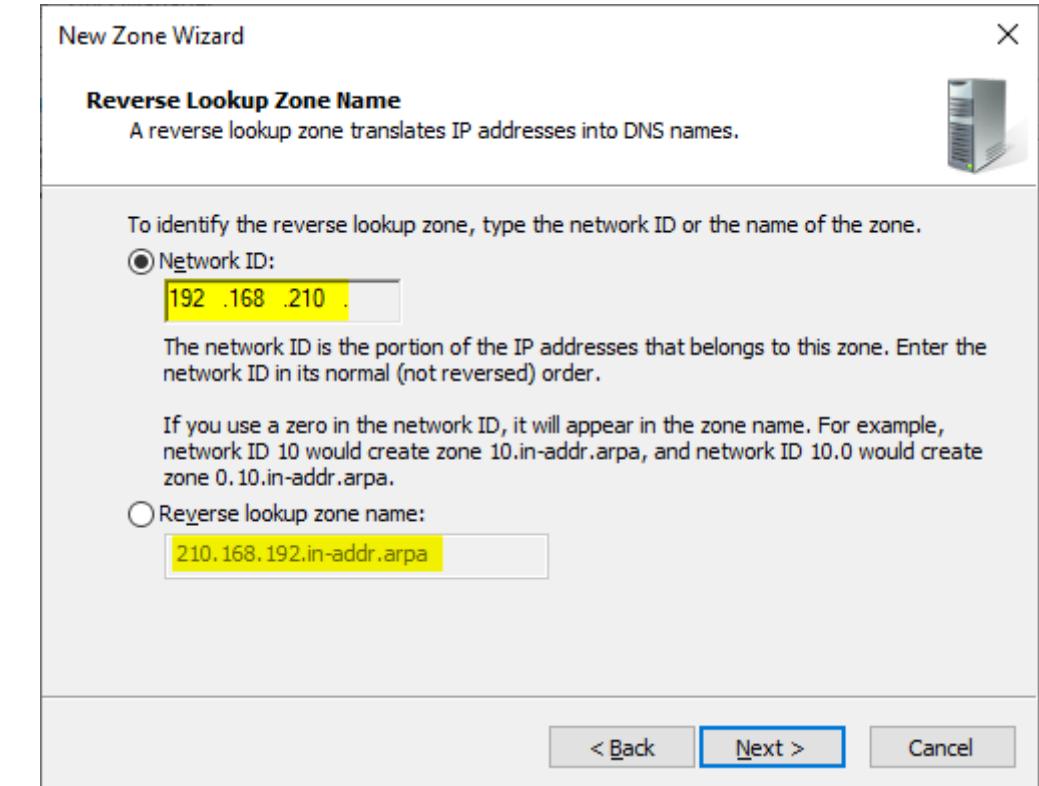
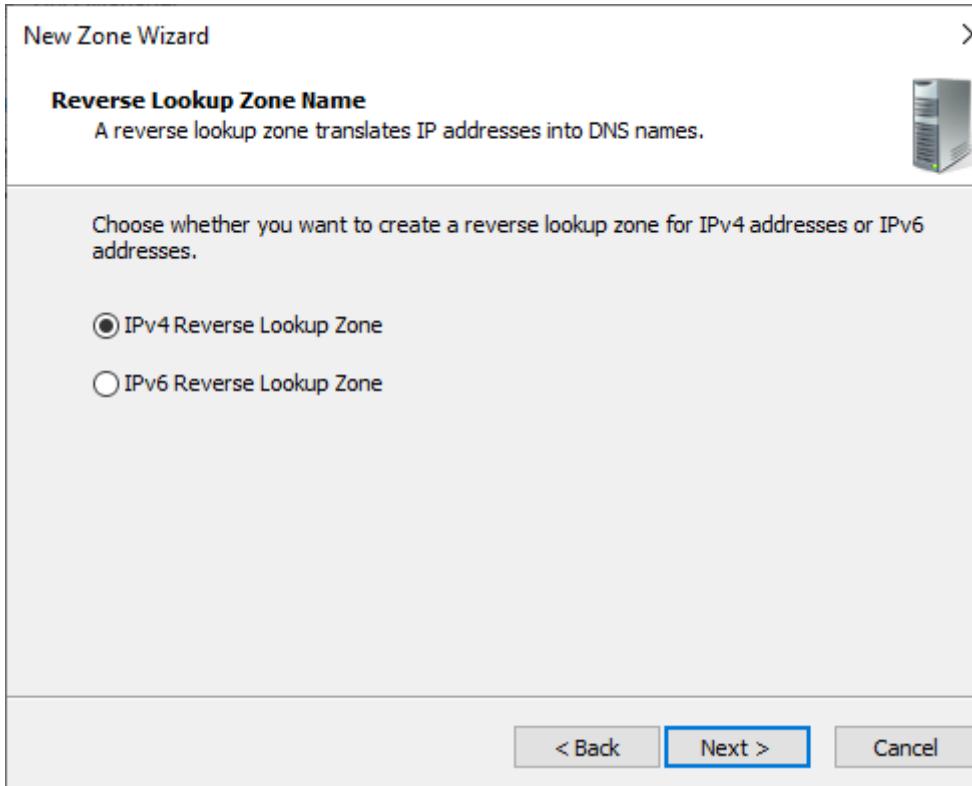
## ► Reverse Zone erstellen



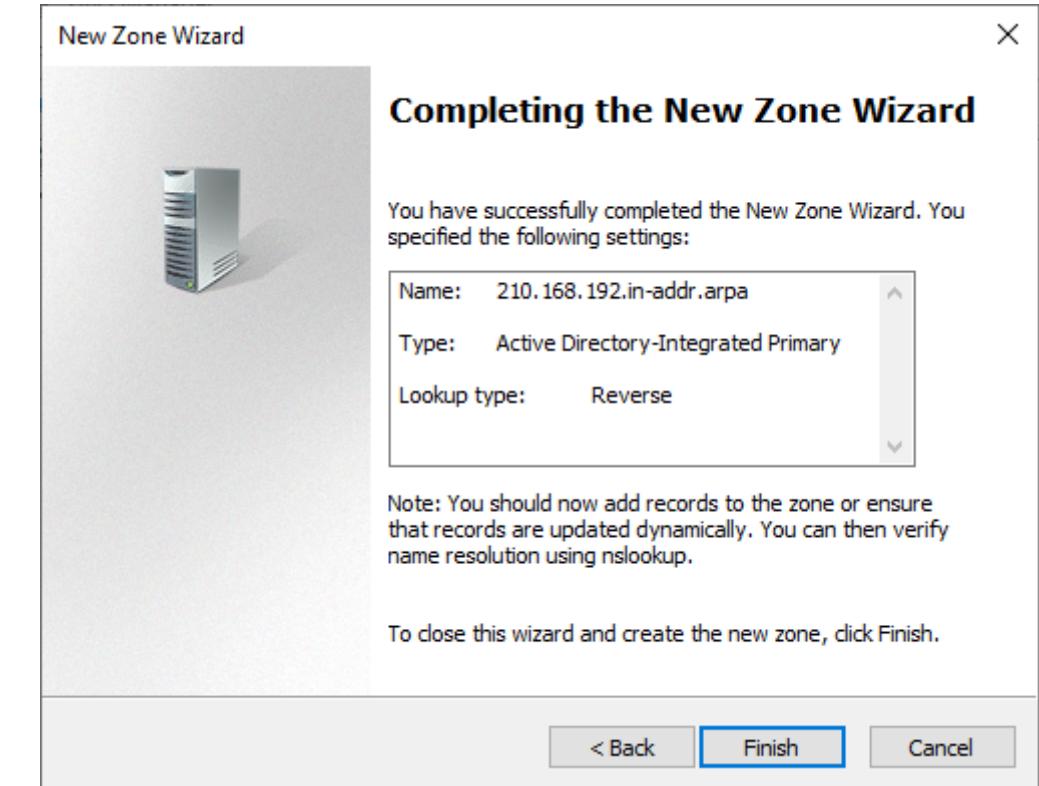
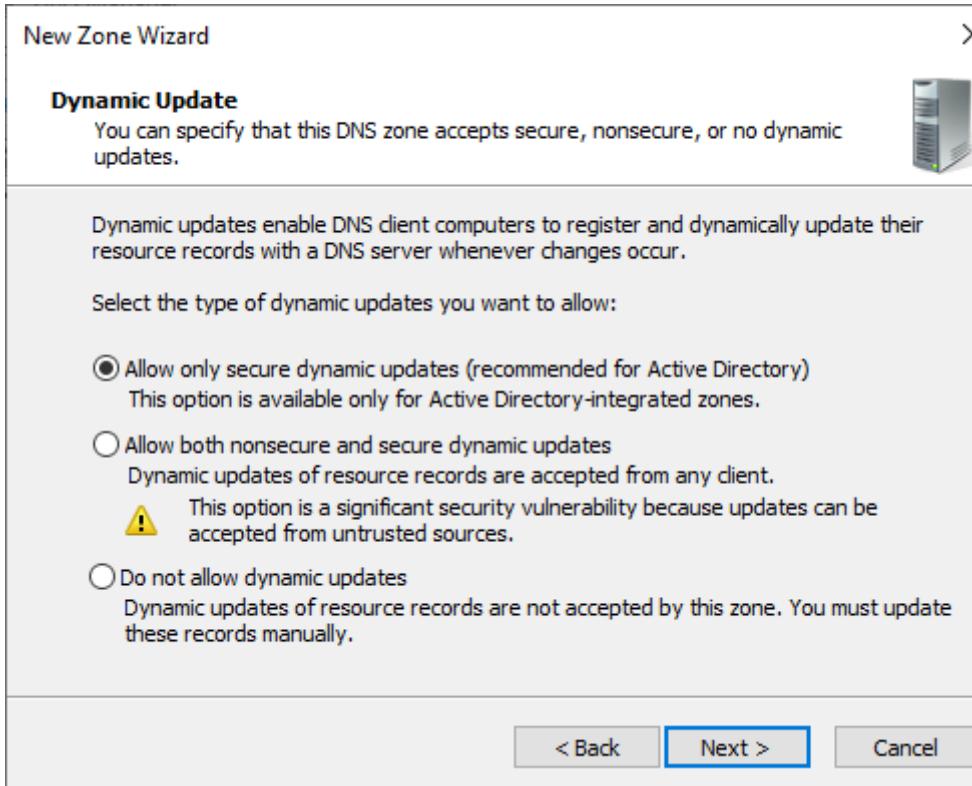
## ► Reverse Zone erstellen



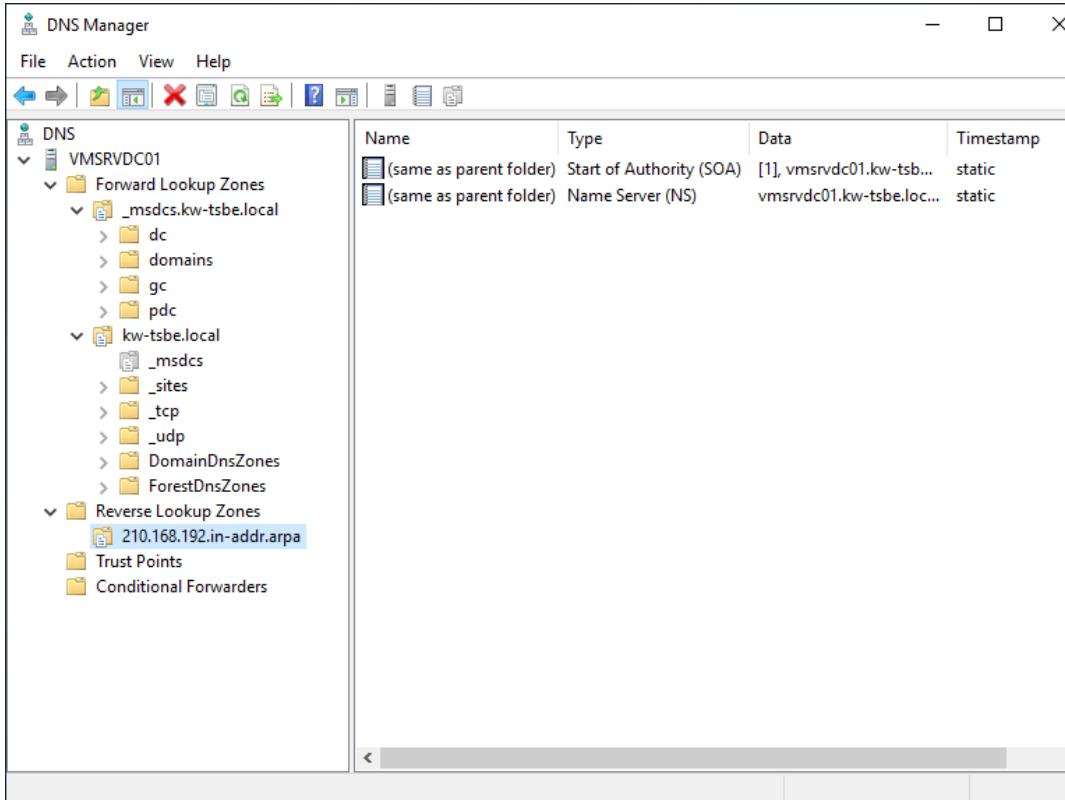
## ► Reverse Zone erstellen



## ► Reverse Zone erstellen



## ► Reverse Zone erstellen



- Eintrag vom DC fehlt
- Manuelle Registrierung durchführen:
  - ipconfig /registerdns

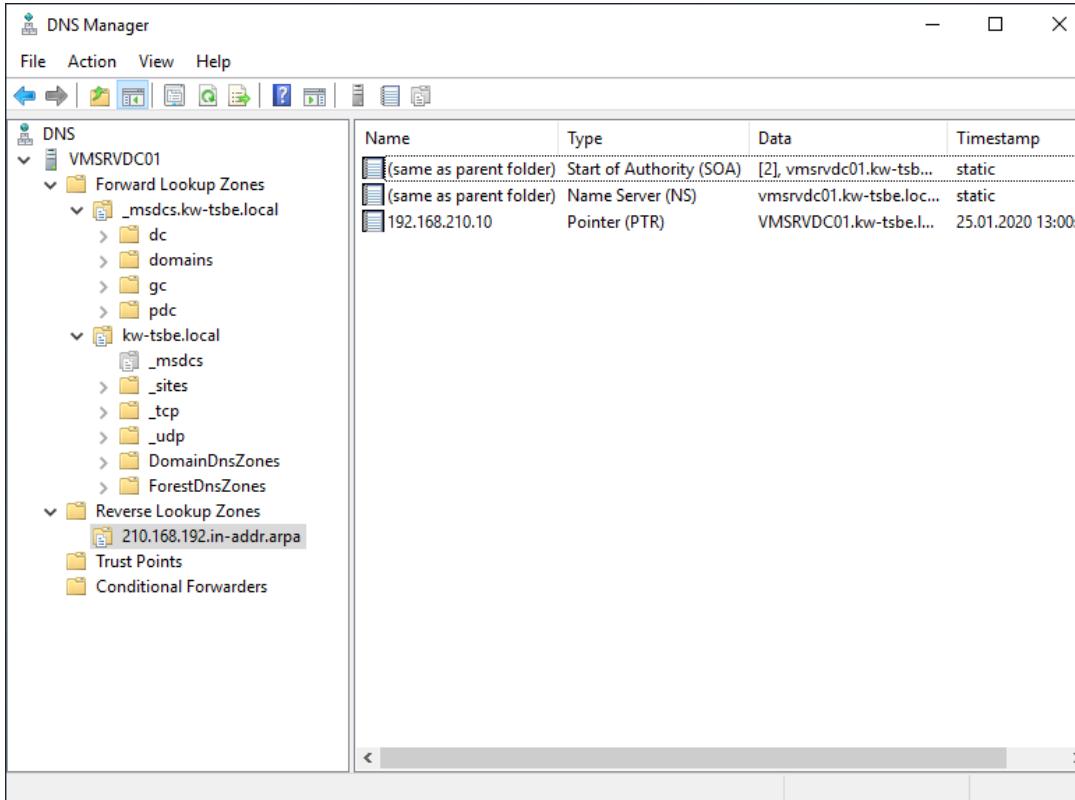
```
Administrator: C:\Windows\system32\cmd.exe
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
```

## ► Reverse Zone erstellen



Nach der Ausführung wird sich der Host spätestens nach 15min eintragen.

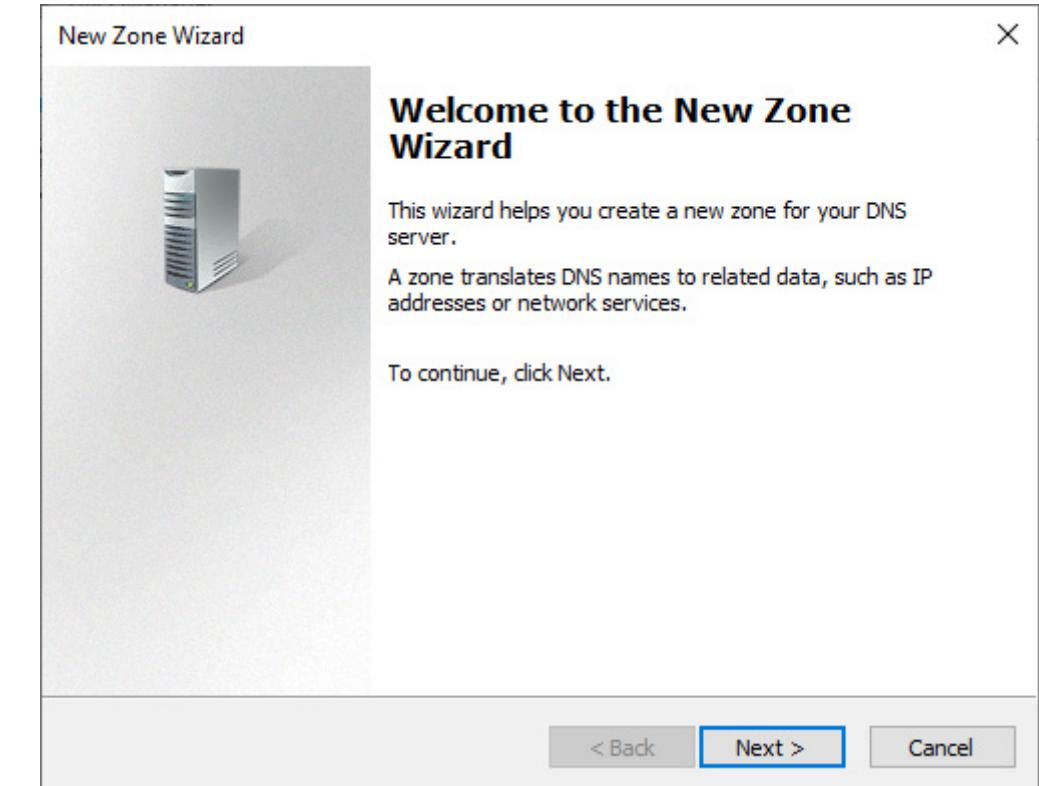
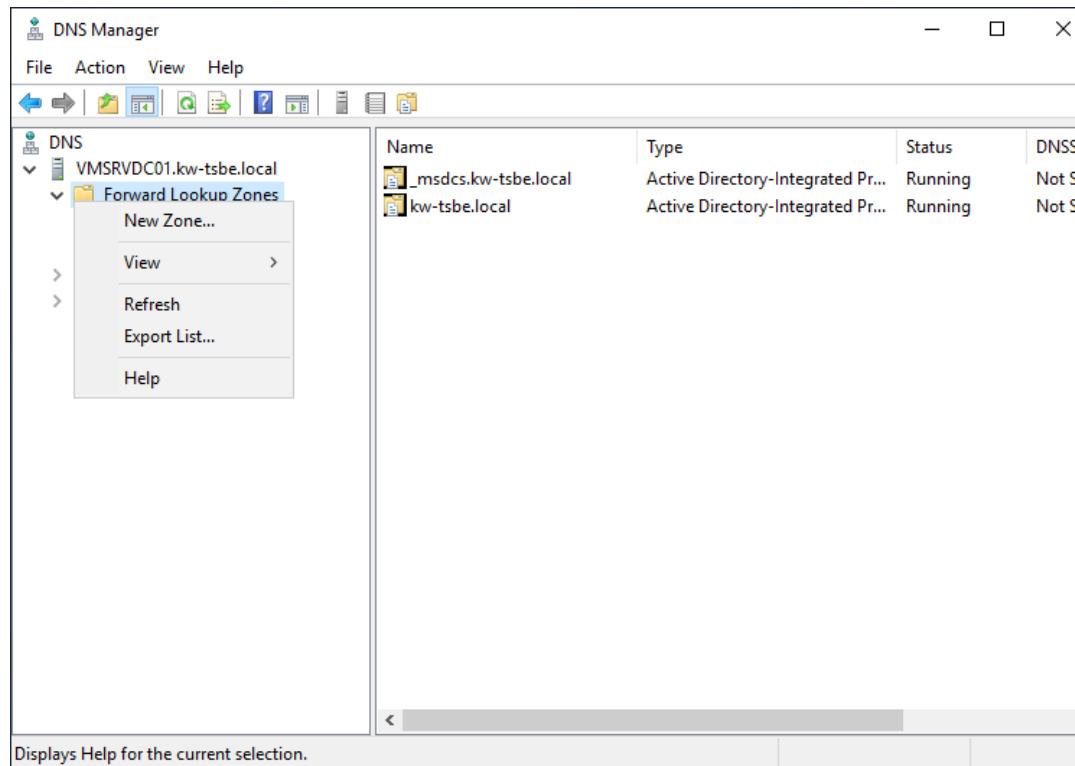
Testen:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

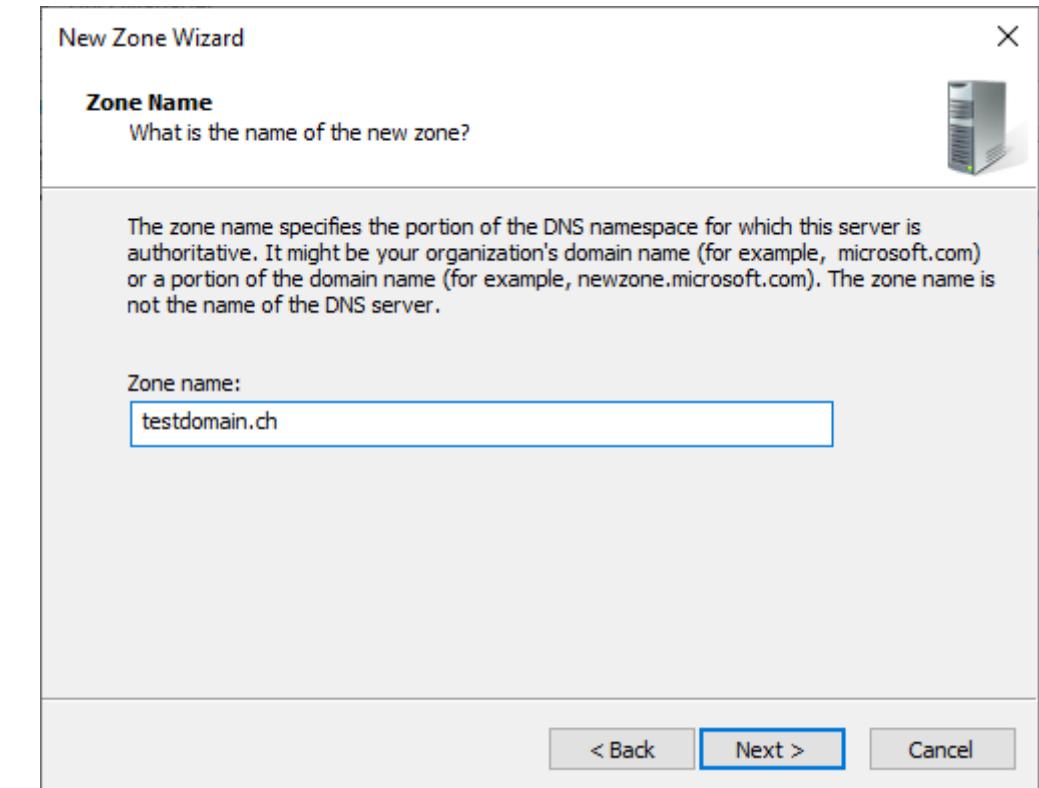
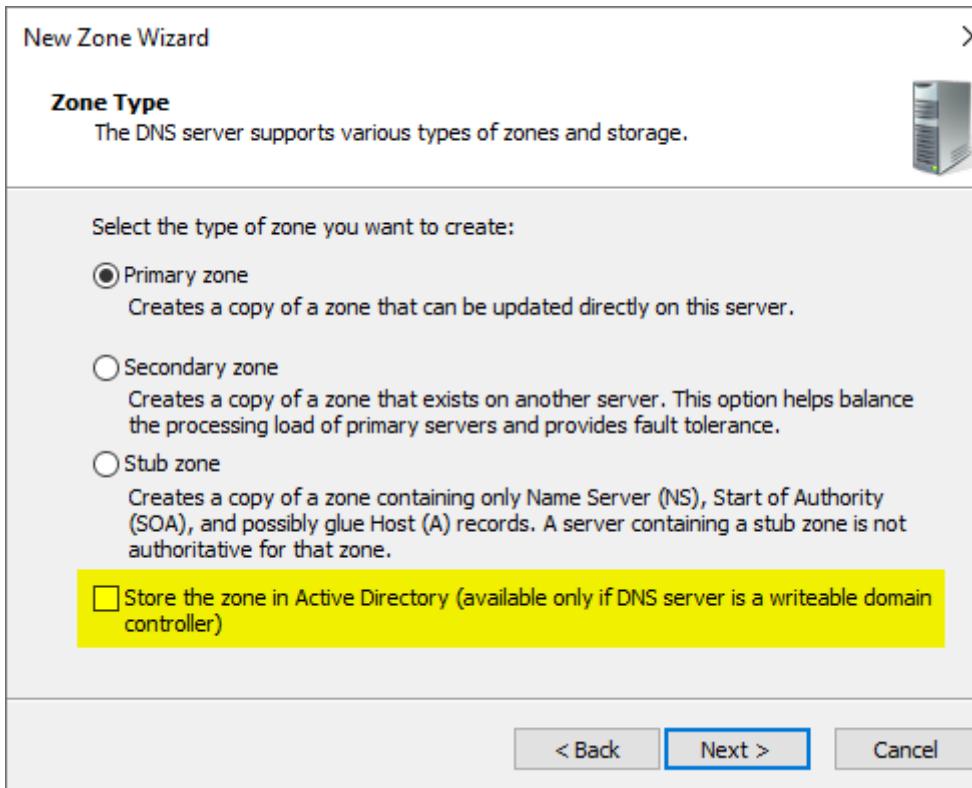
C:\Users\Administrator>nslookup 192.168.210.10
Server: localhost
Address: 127.0.0.1

Name:      VMSRVDC01.kw-tsbe.local
Address:   192.168.210.10
```

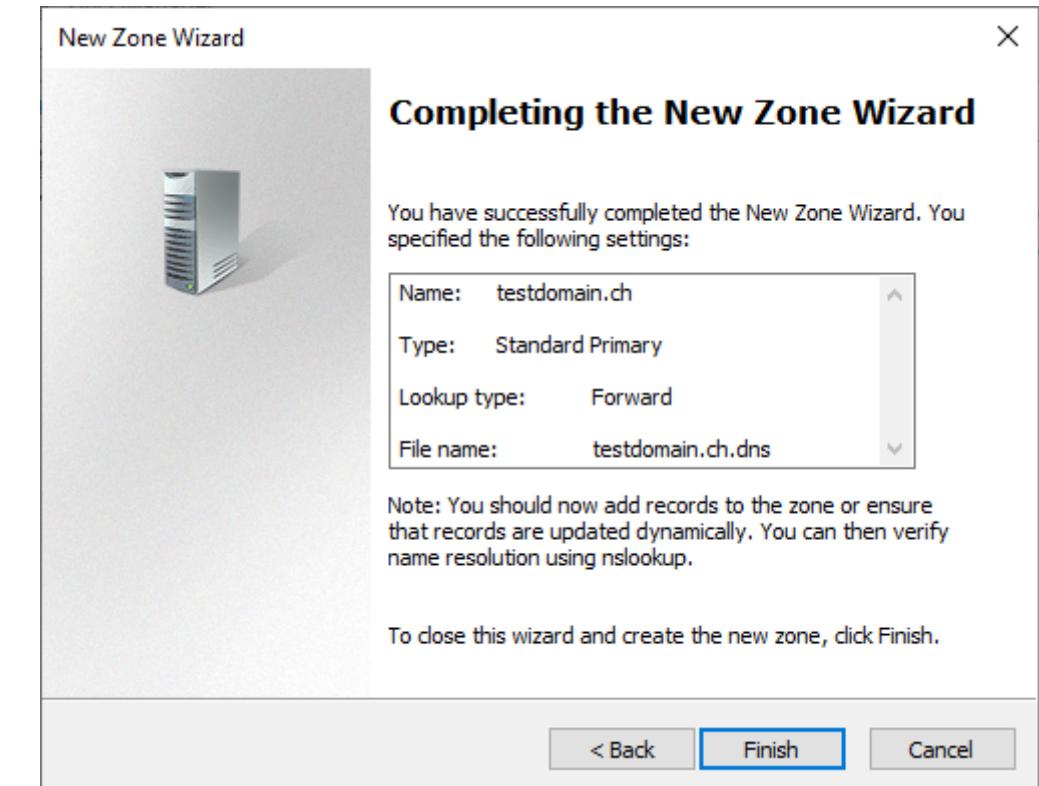
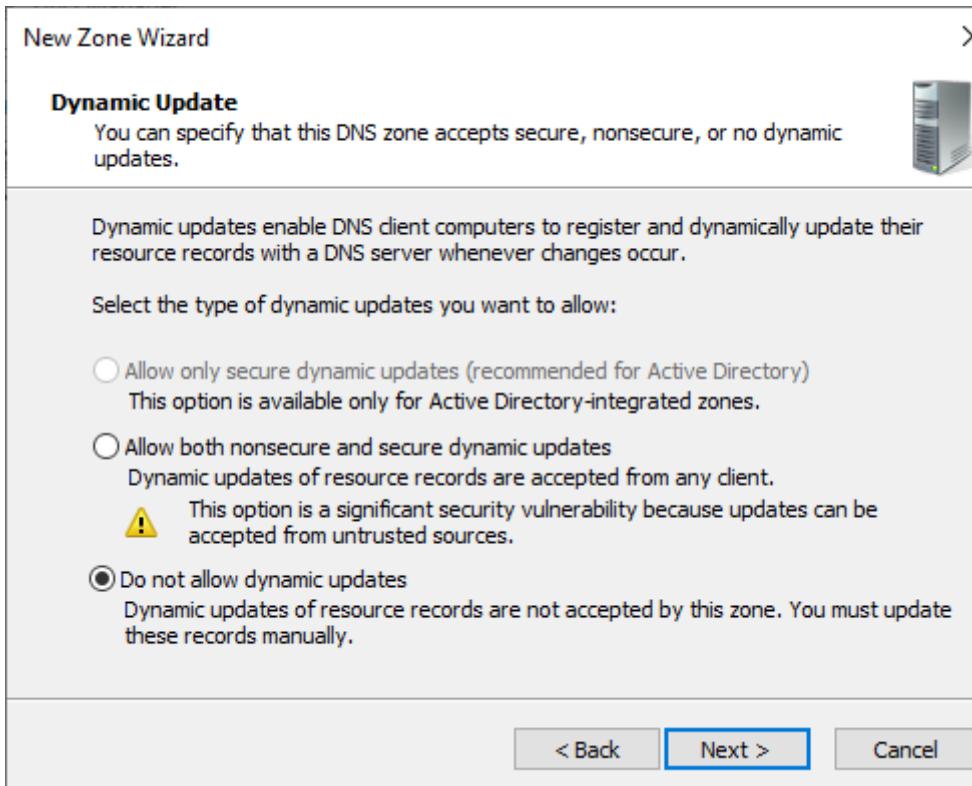
## ► Forward Lookup Zone erstellen



## ► Forward Lookup Zone erstellen

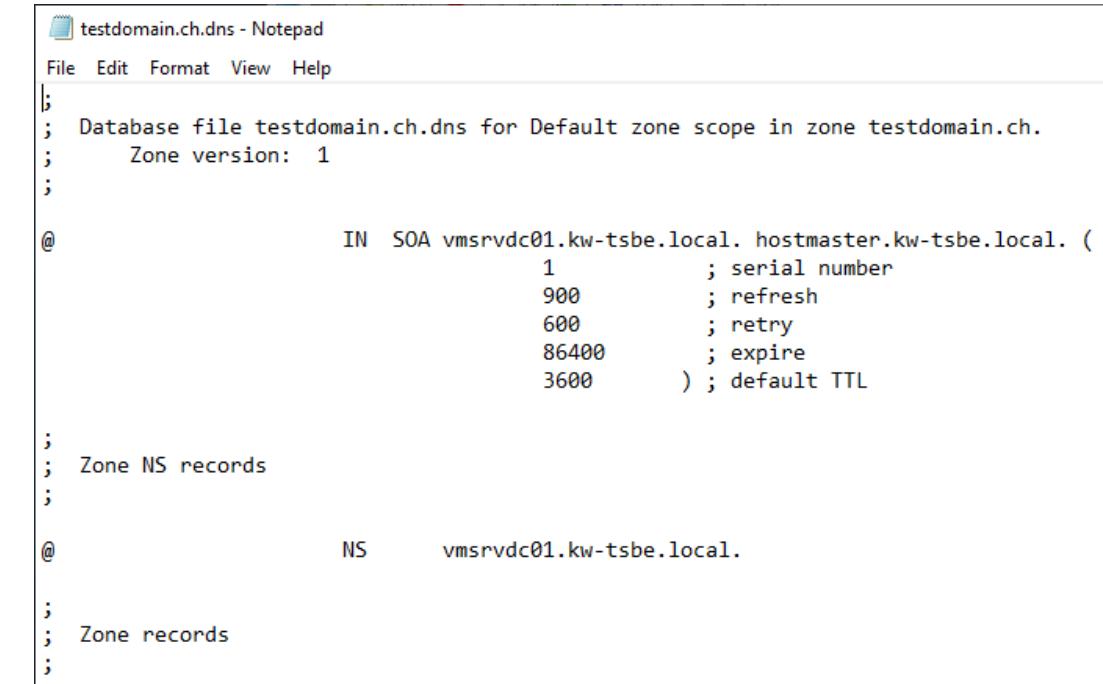


## ► Forward Lookup Zone erstellen



## ▶ Forward Lookup Zone

- Die Zonen Datei wurde als testdomain.ch.dns gespeichert
- Speicherort: C:\Windows\System32\dns
- Kann mit Notepad geöffnet werden
- Dies funktioniert nur mit einer Zone die nicht AD integriert ist.



The screenshot shows a Windows Notepad window titled "testdomain.ch.dns - Notepad". The window contains the following DNS zone file:

```
File Edit Format View Help
;
; Database file testdomain.ch.dns for Default zone scope in zone testdomain.ch.
; Zone version: 1
;

@ IN SOA vmsrvdc01.kw-tsbe.local. hostmaster.kw-tsbe.local. (
    1 ; serial number
    900 ; refresh
    600 ; retry
    86400 ; expire
    3600 ) ; default TTL

;
; Zone NS records
;

@ NS vmsrvdc01.kw-tsbe.local.

;
; Zone records
;
```



Microsoft System Administration

# Active Directory Domain Services Part 2

- Die studierenden

- können die Domäne mit einem weiter DC ergänzen
  - können einen DC migrieren
  - können eine Domäne auf einem Core Server installieren und deinstallieren

- Microsoft Windows Server 2012 R2 - Das Handbuch
  - Kapitel 15 ab S. 559
    - Verwenden der Domänencontrollerdiagnose
    - Bereinigen von AD und Entfernen von Domänencontrollern S. 591

- Installation Server VmWS2
- Installation eines zusätzlichen DCs in der bestehenden Domain
  - VmWS2
  - Transferierte FSMO Rollen
- Deinstallation des DCs VmWS1
- Optional:
  - Installation einer neuen Domain auf dem Core Server
    - Abgabe Powershell Commands als File
  - Deinstallation der neuen Domain auf dem Core Server
    - Abgabe Powershell Commands als File

- Ein DC Single Point of Failure
- Verteilung von FSMO Rollen ist möglich
- Zweiter DC muss immer auch als GC Konfiguriert werden
- Bei grösseren und komplexeren Gesamtstrukturen muss die Aufteilung der FSMO Rollen und GC Rollen gut geplant werden.

- Bei neuen Server Versionen muss ein DC migriert werden
- Neu Installation vom OS und der ADDS Rolle
- FSMO Rollen übertragen
- Alter DC muss demountet werden
  - Enterprise Admins

► DC kann nicht «sauber» entfernt werden

- DC hat einen Hardware defekt
- Irreparabel beschädigt
- Löschung des DC aus der Domain Controller OU
- Löschung des DC aus Active Directory Site and Services
- FSMO Rolle transferieren (falls nötig)
- Metadata Cleanup mit cmd:
  - Ntdsutil
    - metadata cleanup
    - remove selected server <servername>

- FSMO Rollen werden immer gezogen!
- Inhaber überprüfen mit cmd:
  - netdom query fsmo
- Inhaber überprüfen mit PowerShell:
  - Get-ADForest yourdomain | Format-Table SchemaMaster,DomainNamingMaster
  - Get-ADDomain yourdomain | format-table PDCEmulator,RIDMaster,InfrastructureMaster

Learning by doing

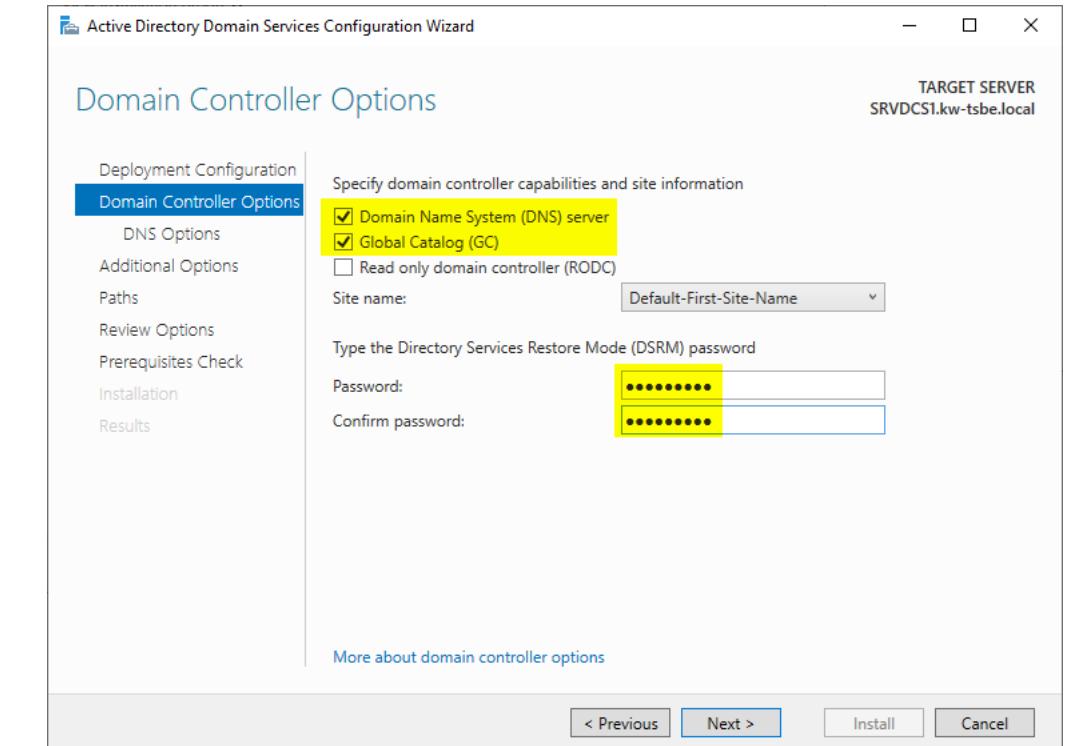
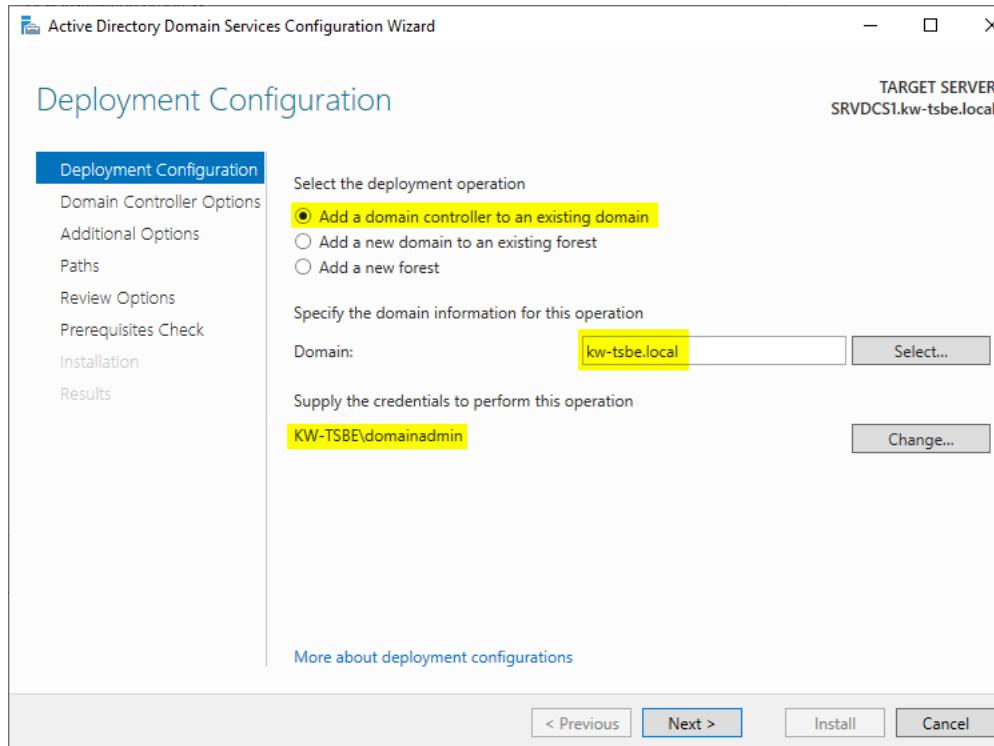
# PRACTICE

- Installieren des Server VmWS2
  - Als Domain Controller Installieren
  - Replikation mit repadmin überprüfen
  - FSMO Rolle verschieben
- Deinstallieren des DC VmWS1
- Optional
  - Core Server aus der Domain «Initialen-tsbe.local» nehmen
  - Installation einer neuen Domain auf dem Core Server
  - Deinstallation der neuen Domain auf dem Core Server

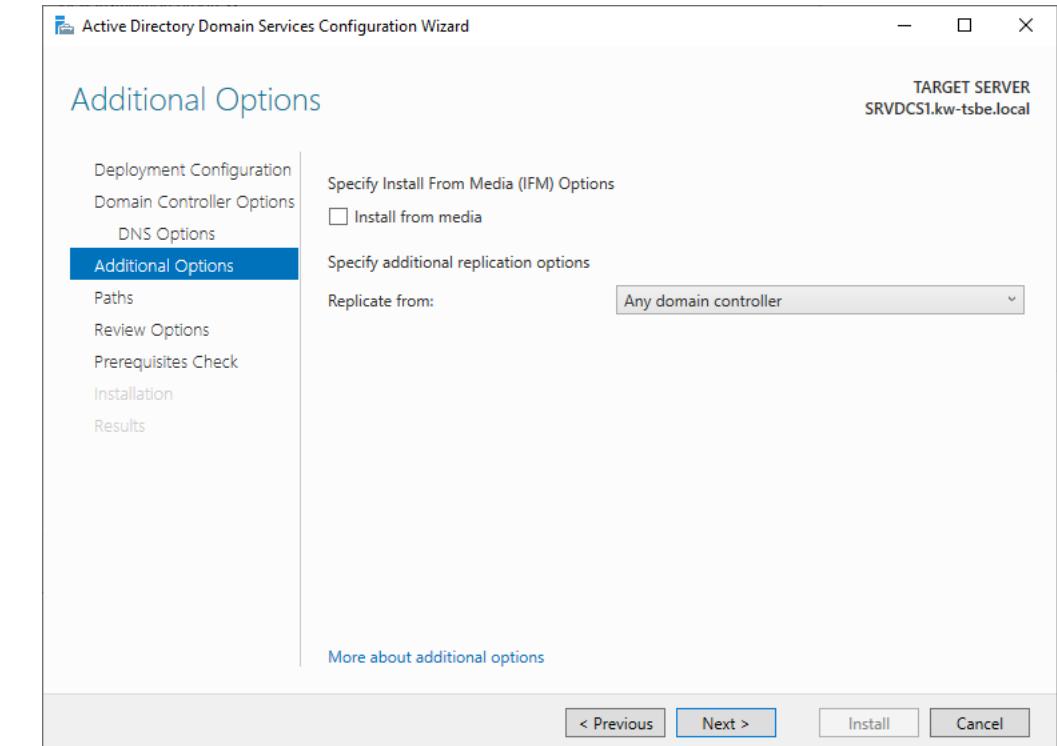
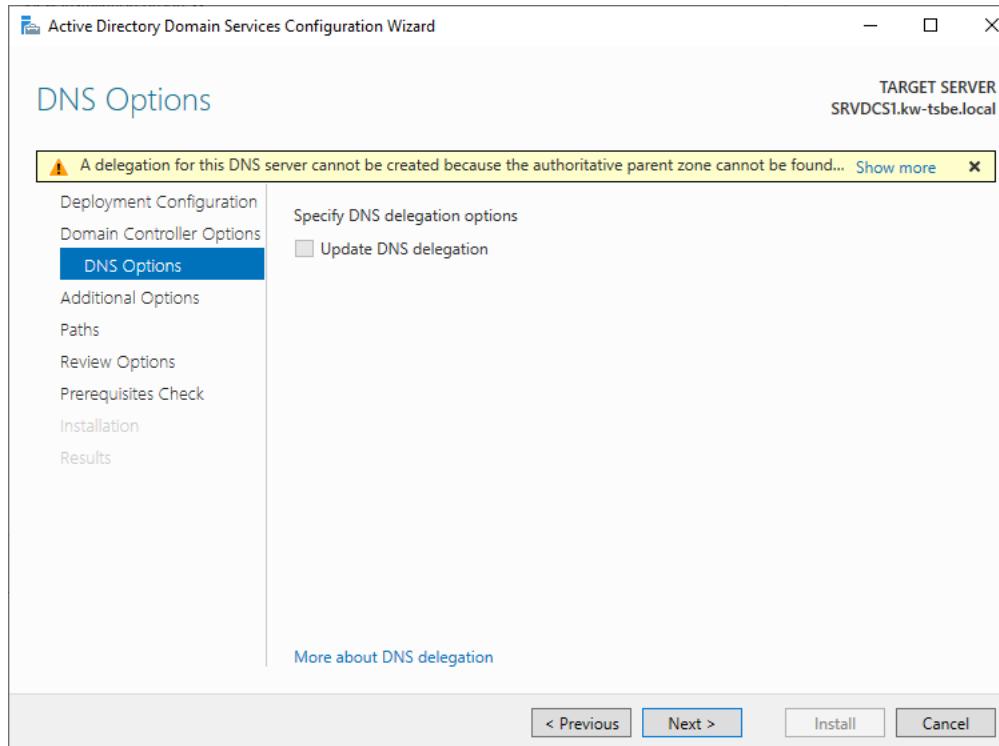
- Grundkonfiguration des OS
- Achtung IP Adresskonflikt vermeiden
- Server in die Domain «Initialen-tsbe.local» aufnehmen

- Rolle über GUI hinzufügen
  - Auf VmWS2 die Rolle Active Directory Domain Services Installieren
- Promote Wizard starten
  - Nach Reboot der Rollen installation

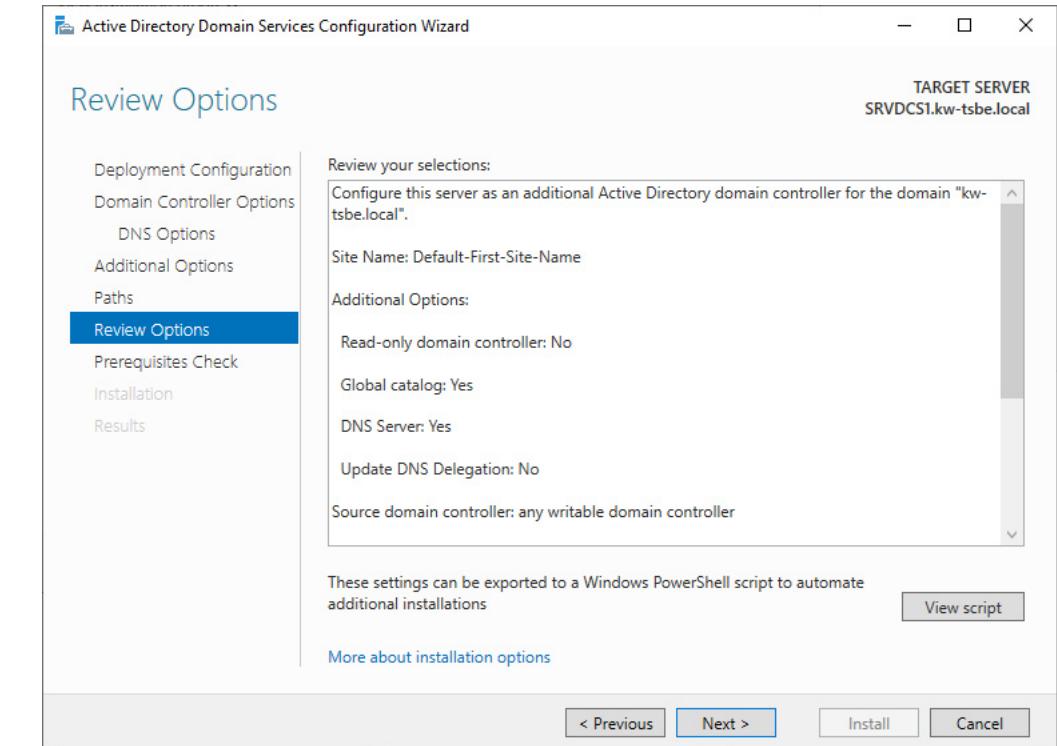
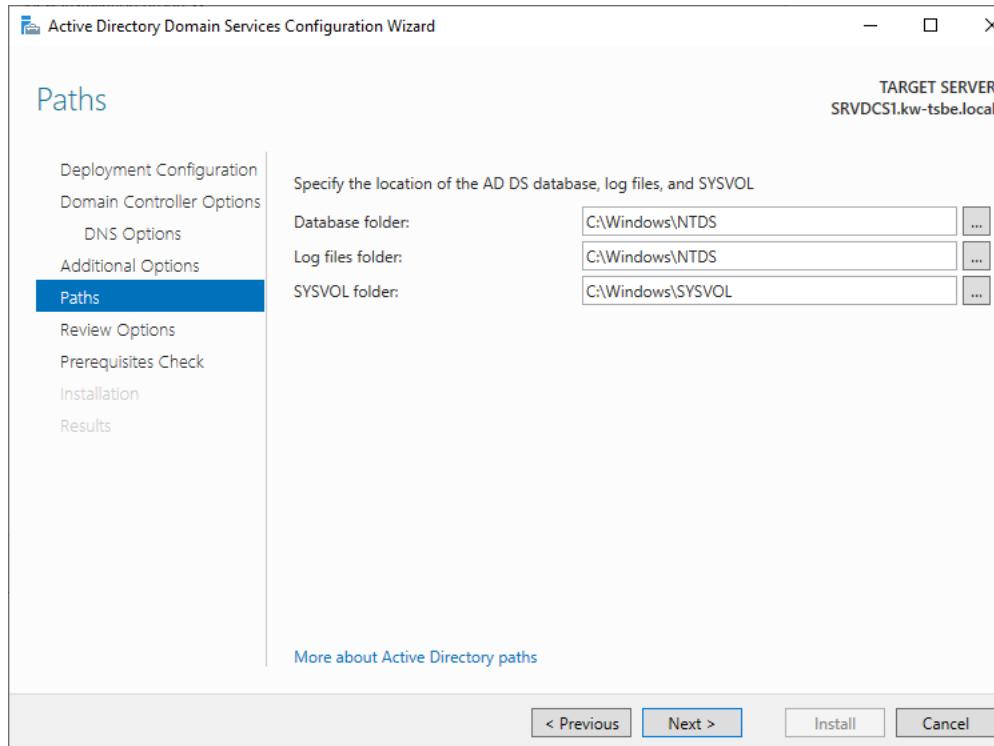
## ► VmWS2 Domain Controller Installation



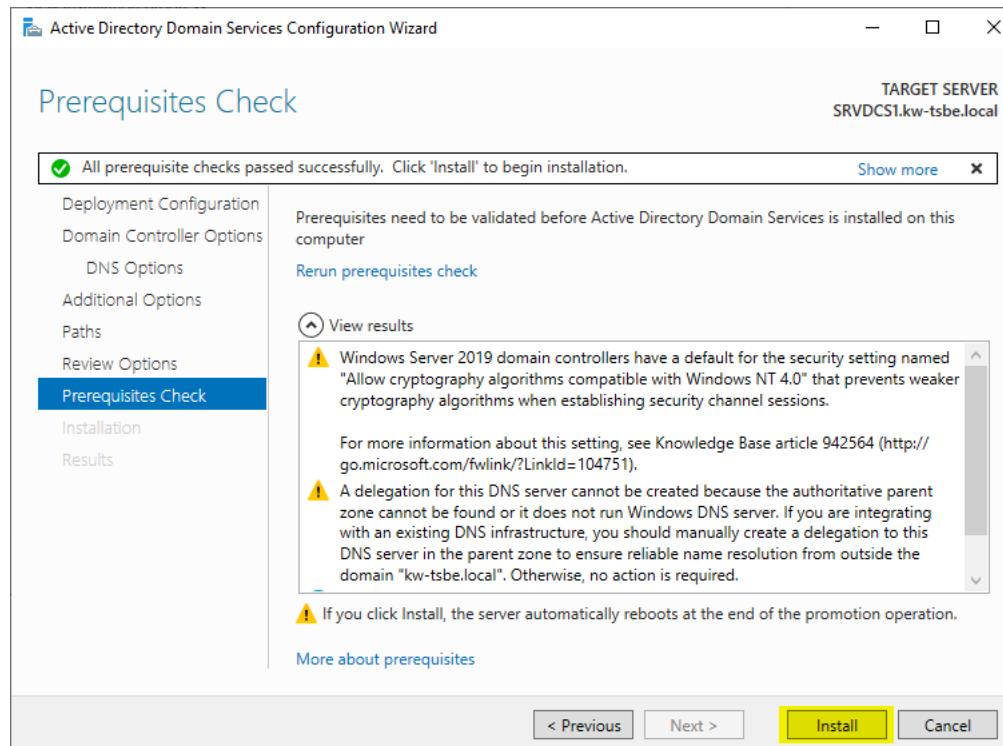
## ► VmWS2 Domain Controller Installation



## ► VmWS2 Domain Controller Installation



## ► VmWS2 Domain Controller Installation



- Nach der Installation erfolgt ein Neustart
- Login mit User domainadmin
- IP Konfiguration anpassen
  - Primäre DNS VmWS2 localhost
  - Sekundärer DNS VmWS1

Obtain DNS server address automatically

Use the following DNS server addresses:

|                       |                      |
|-----------------------|----------------------|
| Preferred DNS server: | 127 . 0 . 0 . 1      |
| Alternate DNS server: | 192 . 168 . 110 . 20 |

## ► Replikation überprüfen

- Mit CMD Befehl
  - repadmin /showrepl

```
C:\Users\domainadmin>repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\SRVDCS1
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: deed393e-c52f-47a8-9713-9917b65be945
DSA invocationID: 61297af2-850e-431c-9b3b-90de0e8bc07b

===== INBOUND NEIGHBORS =====

DC=kw-tsbe,DC=local
  Default-First-Site-Name\SRVDC via RPC
    DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
    Last attempt @ 2020-02-06 09:33:33 was successful.

CN=Configuration,DC=kw-tsbe,DC=local
  Default-First-Site-Name\SRVDC via RPC
    DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
    Last attempt @ 2020-02-06 09:31:29 was successful.

CN=Schema,CN=Configuration,DC=kw-tsbe,DC=local
  Default-First-Site-Name\SRVDC via RPC
    DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
    Last attempt @ 2020-02-06 09:31:29 was successful.

DC=DomainDnsZones,DC=kw-tsbe,DC=local
  Default-First-Site-Name\SRVDC via RPC
    DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
    Last attempt @ 2020-02-06 09:31:38 was successful.

DC=ForestDnsZones,DC=kw-tsbe,DC=local
  Default-First-Site-Name\SRVDC via RPC
    DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
    Last attempt @ 2020-02-06 09:31:29 was successful.
```

## ► FSMO Rolle verschieben

- Mit CMD Befehl prüfen
  - netdom query fsmo

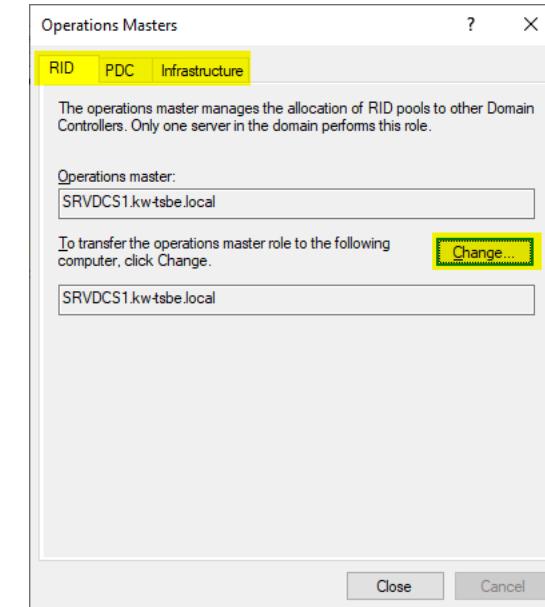
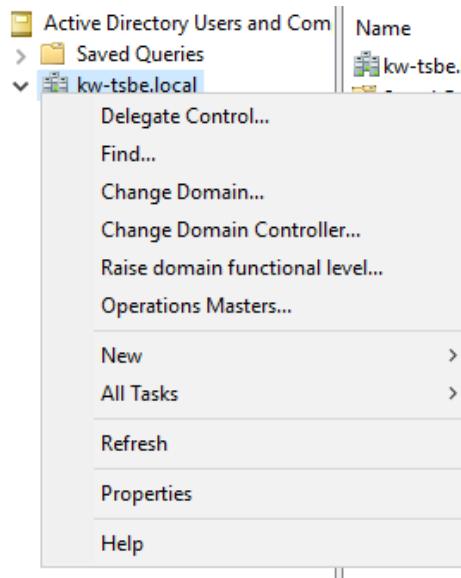
```
C:\Users\domainadmin>netdom query fsmo
Schema master           SRVDC.kw-tsbe.local
Domain naming master    SRVDC.kw-tsbe.local
PDC                   SRVDC.kw-tsbe.local
RID pool manager       SRVDC.kw-tsbe.local
Infrastructure master   SRVDC.kw-tsbe.local
The command completed successfully.
```

- <https://www.komdat.at/fsmo-rollen-auf-server-2012-oder-server-2016-uebertragen/>

- Verschieben der Rolle erfolgt nun mit GUI folgende MMCs werden benötigt:
  - Active Directory Users and Computers
  - Active Directory Domains and Trusts
  - Active Directory Schema

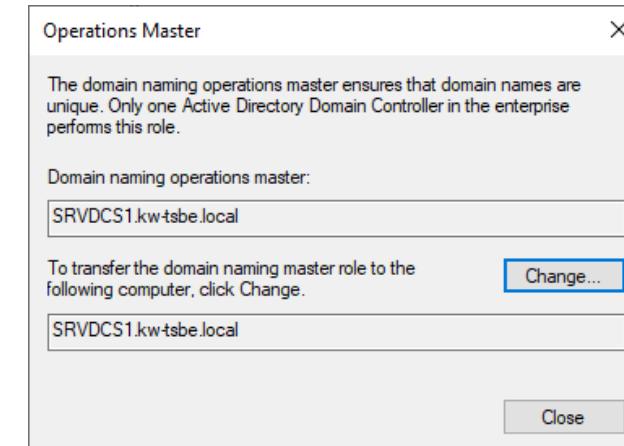
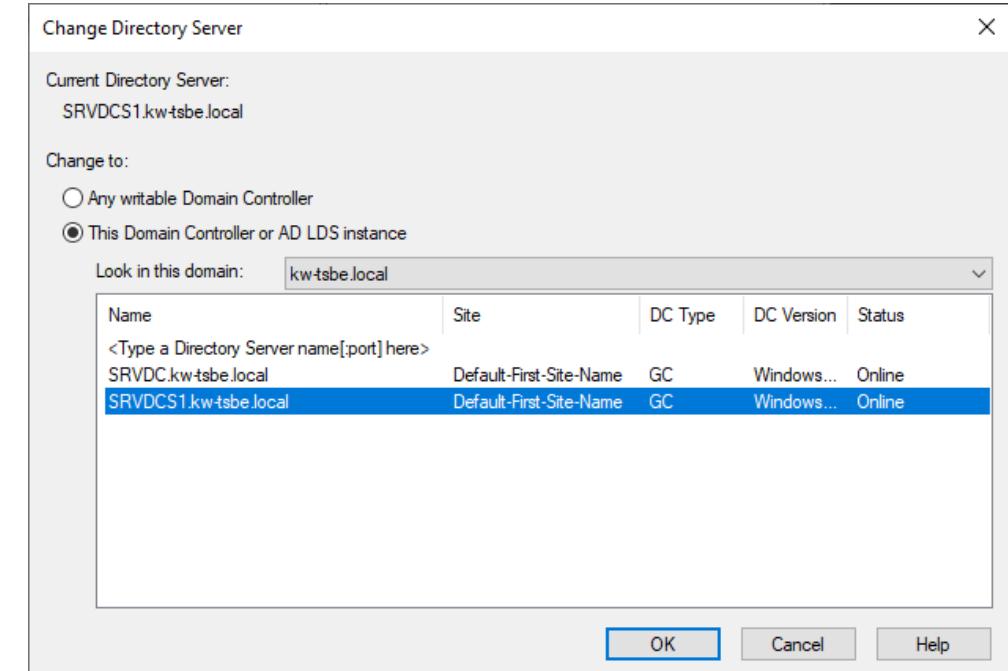
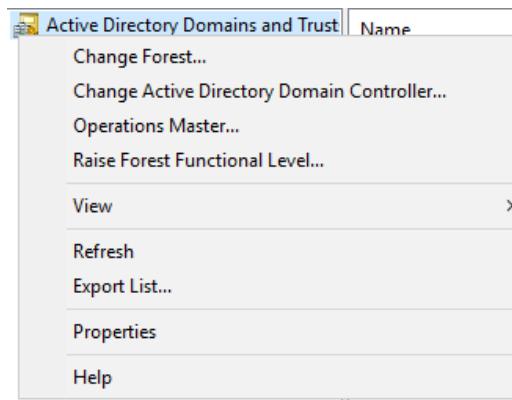
## ► FSMO Rolle verschieben

- In der Konsole: «Active Directory Users and Computers»
- Rechtsklick auf die Domain
  - Operations Masters...
- Die drei Rollen: RID, PDC und Infrastructure können nun im neuen Fenster verschoben werden.



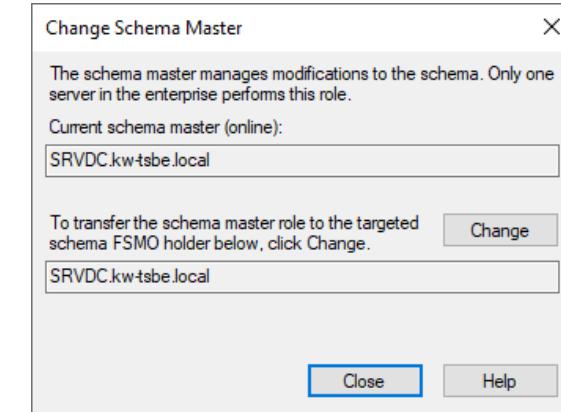
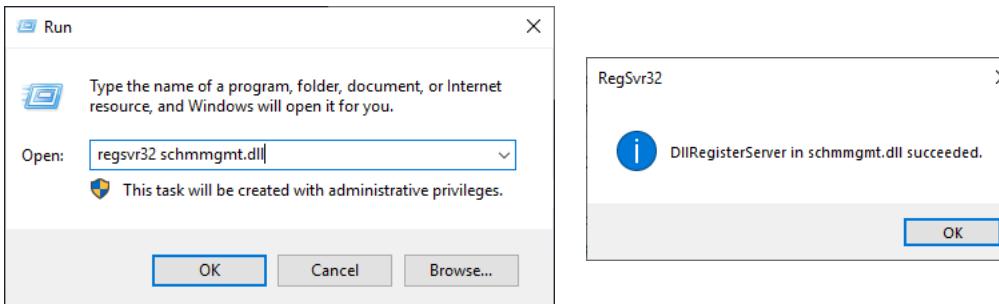
## ► FSMO Rolle verschieben

- In der Konsole: «Active Directory Domains and Trusts»
- Rechtsklick auf Active Directory Domains and Trusts
  - Change Active Directory Domain Controller... (VmWS2 wählen)
  - Operations Masters...



## ► Schema Master verschiebe

- Window + R
  - *regsvr32 schmmgmt.dll*
  - Mmc
- Im neuen mmc
  - File
  - Add/Remove Snap-in...
  - «Active Directory Schema» wählen
- Nun wie bei den anderen Rollen
- Rechtsklick auf Active Directory Schema
  - Wieder DC wechseln
  - Operations Master



## ► FSMO Rollen prüfen

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\domainadmin>netdom query fsmo
Schema master           SRVDCS1.kw-tsbe.local
Domain naming master    SRVDCS1.kw-tsbe.local
PDC                     SRVDCS1.kw-tsbe.local
RID pool manager        SRVDCS1.kw-tsbe.local
Infrastructure master   SRVDCS1.kw-tsbe.local
The command completed successfully.

C:\Users\domainadmin>
```

► FSMO Rollen verschieben FAST

- Move-AddDirectoryServerOperationMasterRole -Identity <Ziel-DC> - OperationMasterRole SchemaMaster, RIDMaster, InfrastructureMaster, DomainNamingMaster, PDCEmulator

## ► Replikation überprüfen

- Mit CMD Befehl
  - repadmin /showrepl

```
C:\Users\domainadmin>repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\SRVDCS1
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: deed393e-c52f-47a8-9713-9917b65be945
DSA invocationID: 61297af2-850e-431c-9b3b-90de0e8bc07b

===== INBOUND NEIGHBORS =====

DC=kw-tsbe,DC=local
    Default-First-Site-Name\SRVDC via RPC
        DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
        Last attempt @ 2020-02-06 09:33:33 was successful.

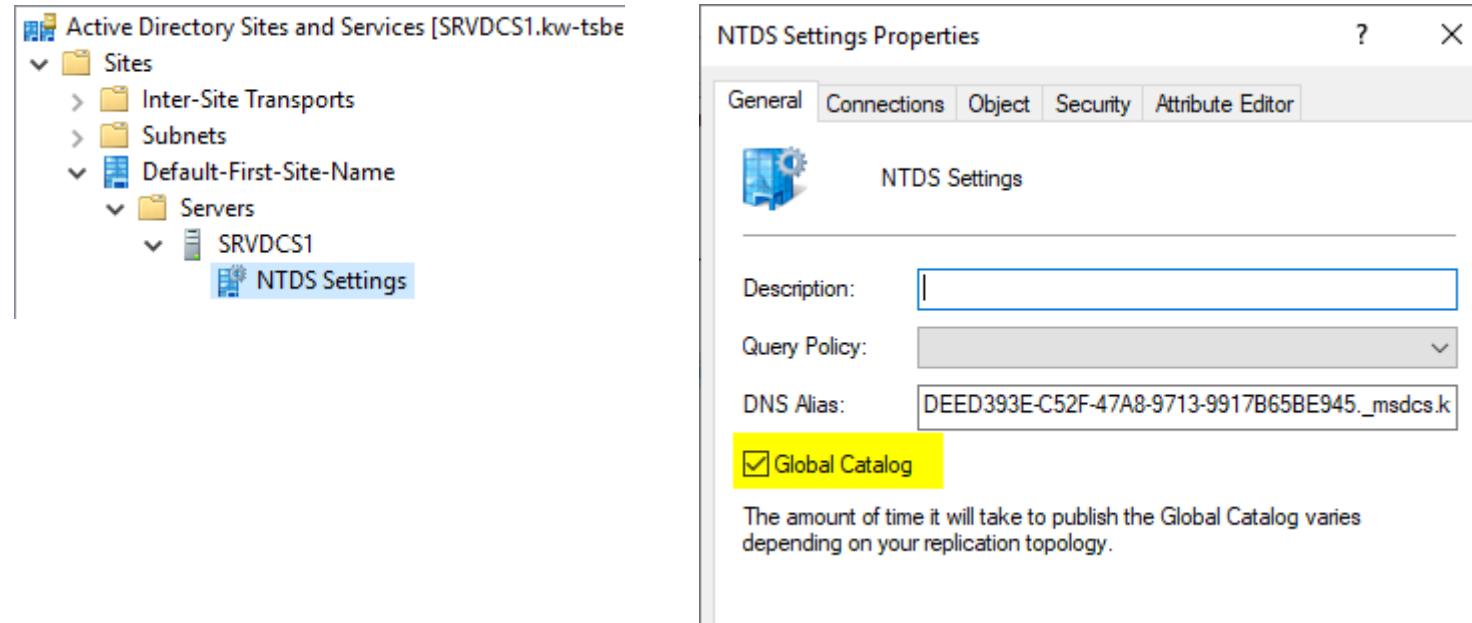
CN=Configuration,DC=kw-tsbe,DC=local
    Default-First-Site-Name\SRVDC via RPC
        DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
        Last attempt @ 2020-02-06 09:31:29 was successful.

CN=Schema,CN=Configuration,DC=kw-tsbe,DC=local
    Default-First-Site-Name\SRVDC via RPC
        DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
        Last attempt @ 2020-02-06 09:31:29 was successful.

DC=DomainDnsZones,DC=kw-tsbe,DC=local
    Default-First-Site-Name\SRVDC via RPC
        DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
        Last attempt @ 2020-02-06 09:31:38 was successful.

DC=ForestDnsZones,DC=kw-tsbe,DC=local
    Default-First-Site-Name\SRVDC via RPC
        DSA object GUID: 5d0d51d6-d52a-4cf6-accf-884c6bab593f
        Last attempt @ 2020-02-06 09:31:29 was successful.
```

- Active Directory Sites and Services öffnen
- Rechtsklick auf NRFS Settings unter dem Server VmWS2 → Properties



- Voraussetzungen
  - VmWS2 ist nun DC
  - VmWS2 ist GC
  - FSMO Rollen wurden verschoben
  - Replikation wurde überprüft
- DNS anpassen
  - Primärer DNS VmWS2 setzen

- Test mit PowerShell durchführen:
  - Test-ADDSDomainControllerUnistallation

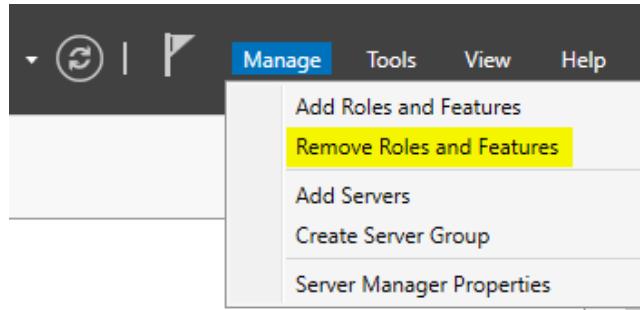
```
> Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

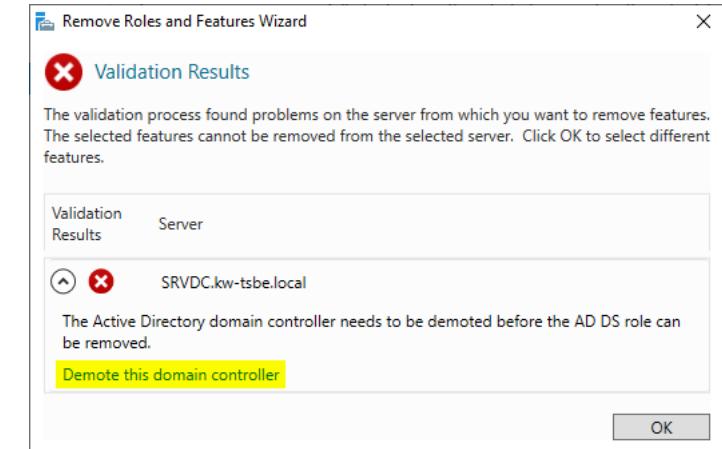
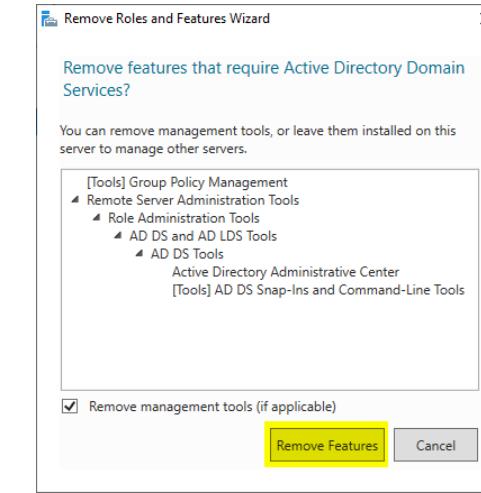
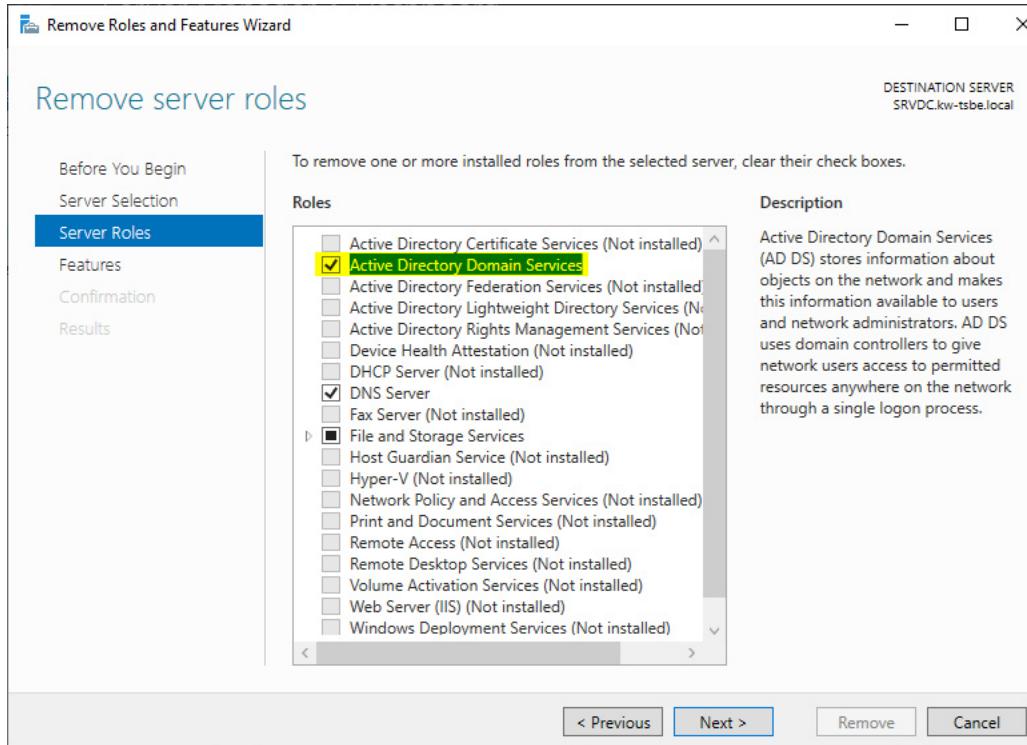
PS C:\Users\Administrator> Test-ADDSDomainControllerUninstalation
LocalAdministratorPassword: *****
Confirm LocalAdministratorPassword: *****

Message                                     Context                                         RebootRequired  Status
-----                                     -----                                         -----
Operation completed successfully Test.VerifyDcPromoCore.DCPromo.General.1      False  Success
```

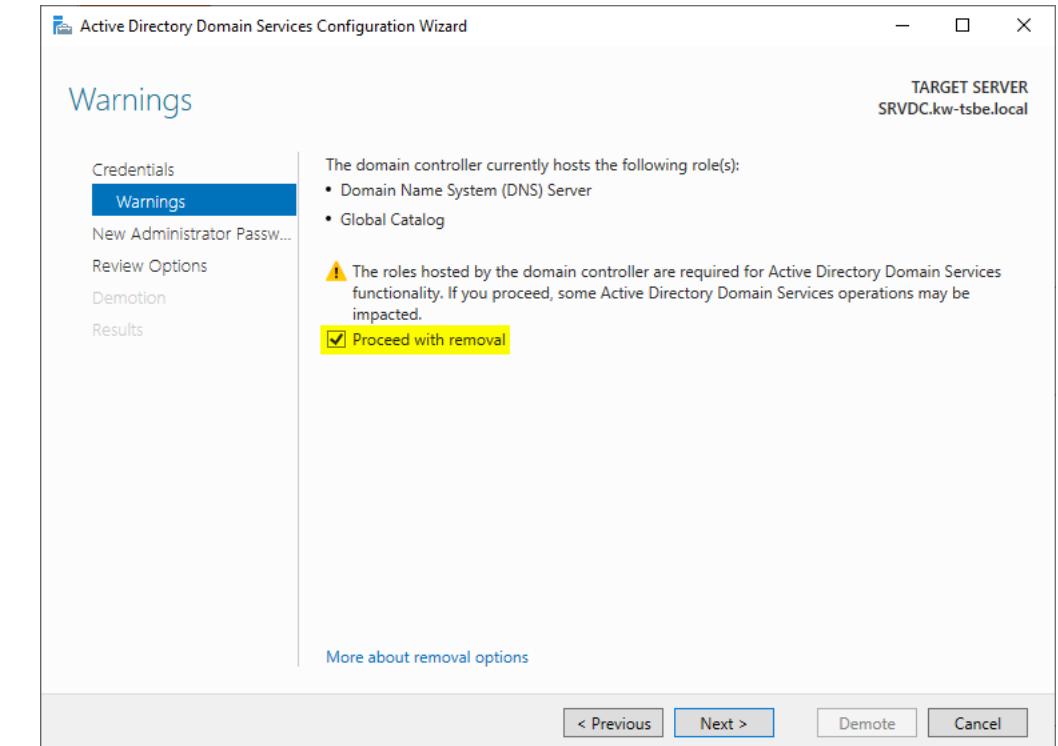
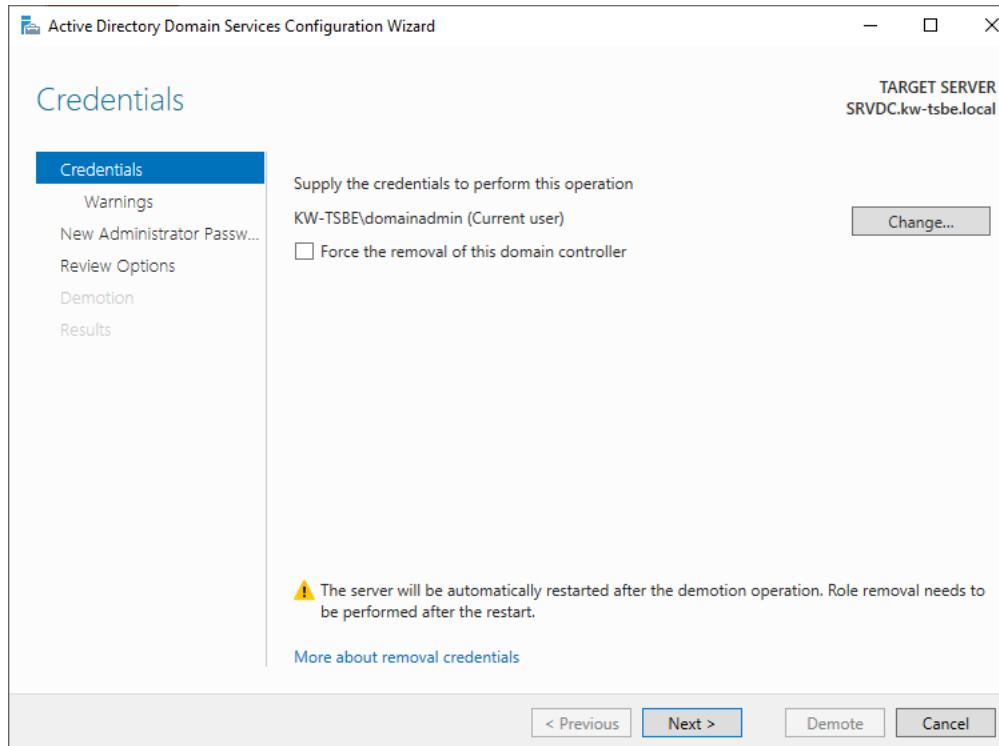
- Für die Deinstallation wird der normale Rollen Wizard verwendet



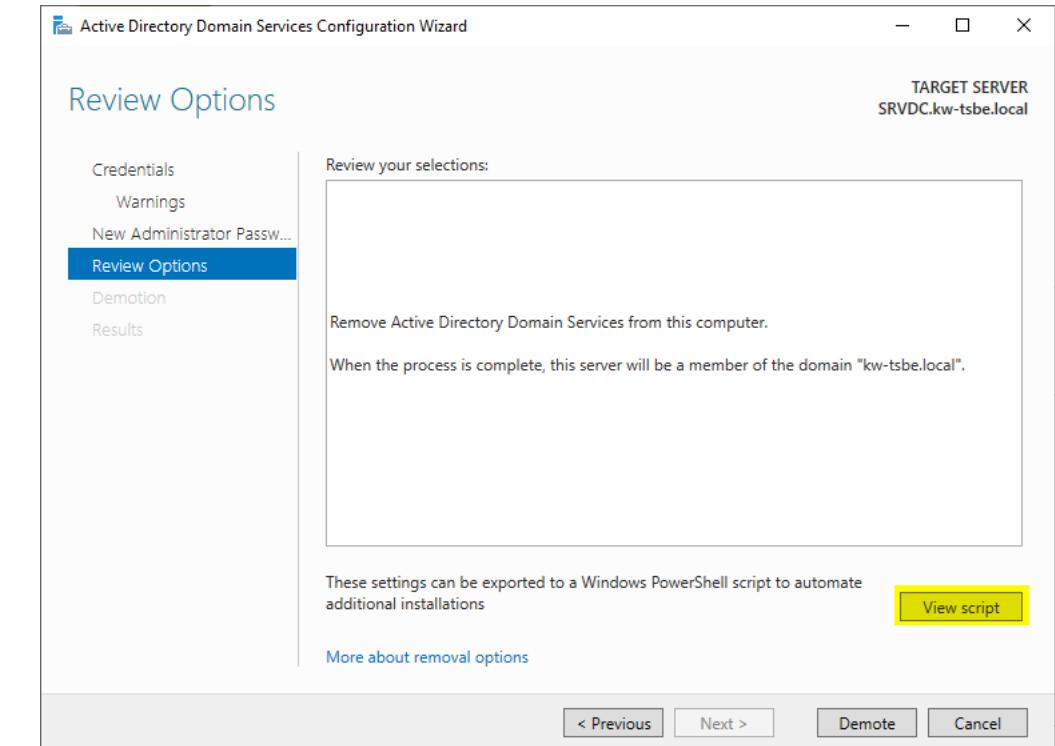
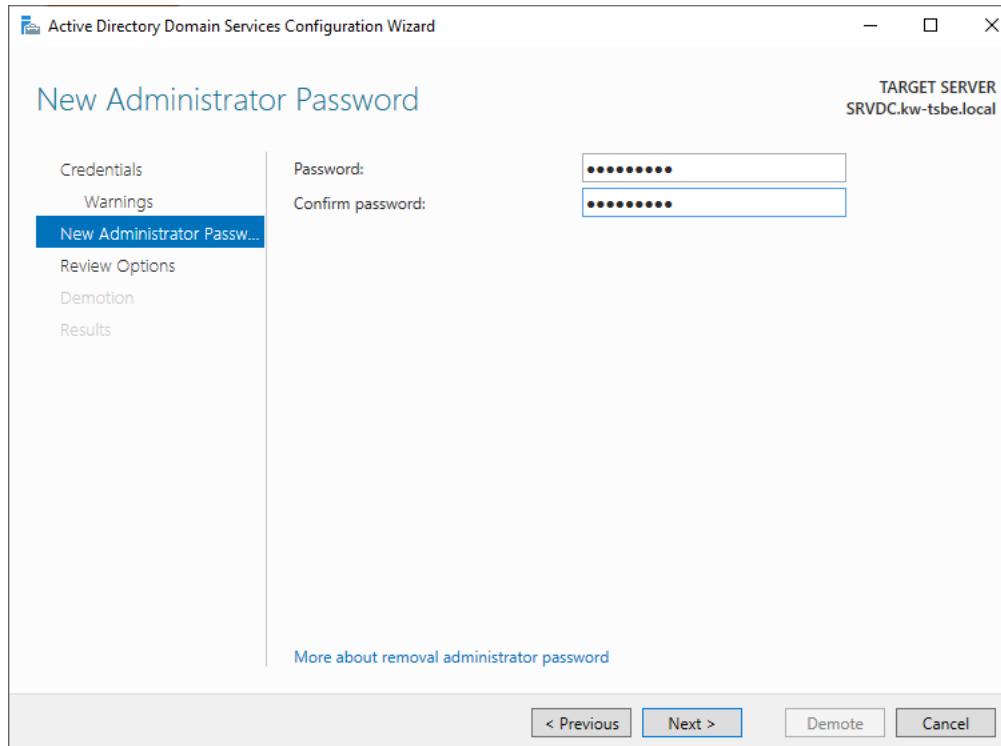
## ▶ VmWS1 demote



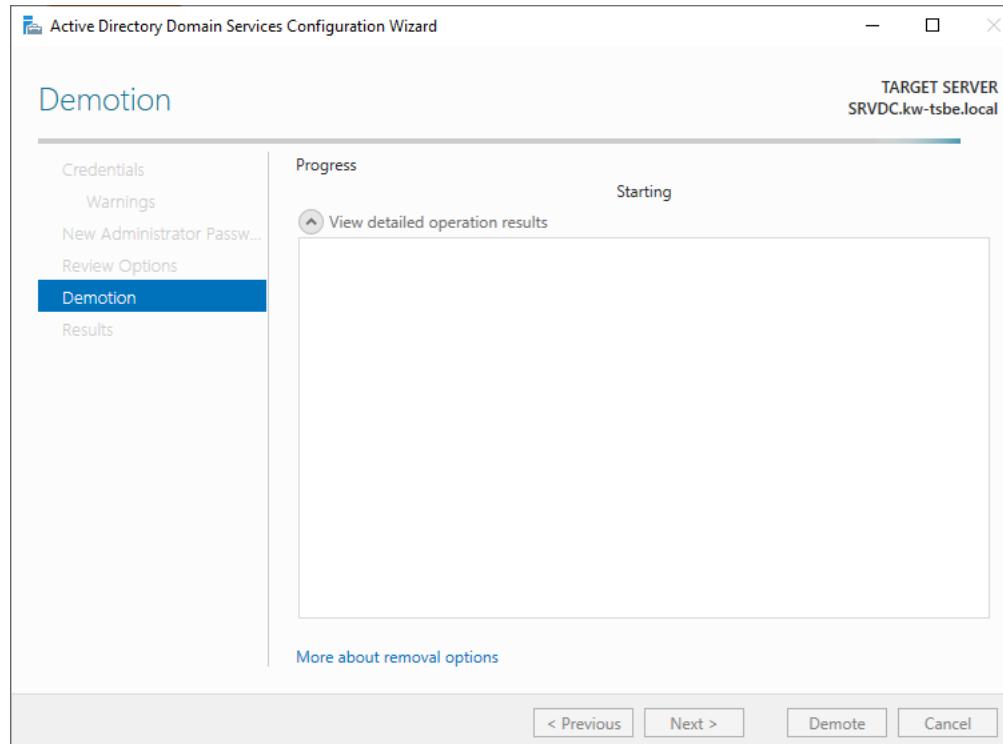
## ▶ VmWS1 demote



## ▶ VmWS1 demote

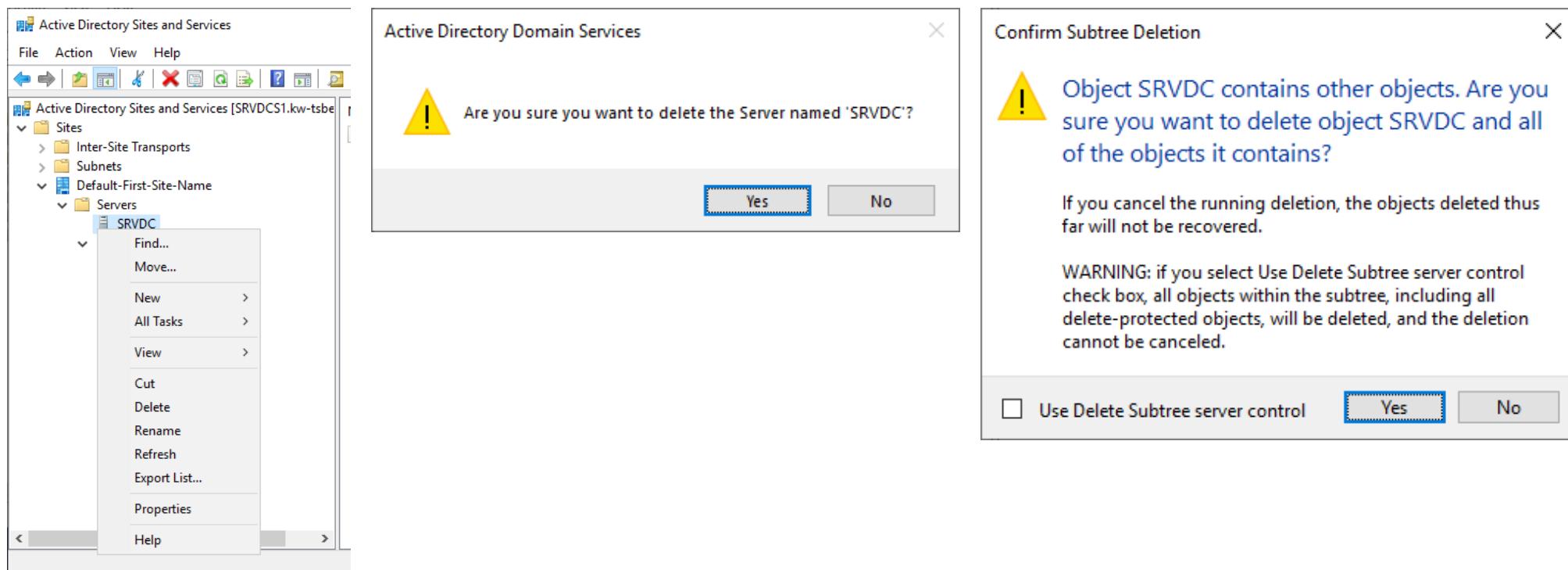


## ▶ VmWS1 demote



- Nach der Deinstallation startet der Server neu
- Den Server brauchen wir nu nichtmehr

- MMC Active Directory Sites and Services öffnen
  - Löschen von SRVDC



- Mit den nun gesicherten Skripts aus den bisherigen Installationen könnt ihr nun auf dem Core Server ebenfalls eine Domain installieren und diese anschliessend wieder deinstallieren. Allfällige Recherche in den E-Books und im Internet sind gegeben falls erforderlich.
- Neuen DC mit PowerShell erstellen [Link](#)
- DC mit PowerShell deinstallieren [Link](#)
- Bitte die 2 Files erstellen
  - 1 Installation des DC mit Rollen und Promote
  - 2 Deinstallation des DC demote



DHCP

# Dynamic Host Configuration Protocol

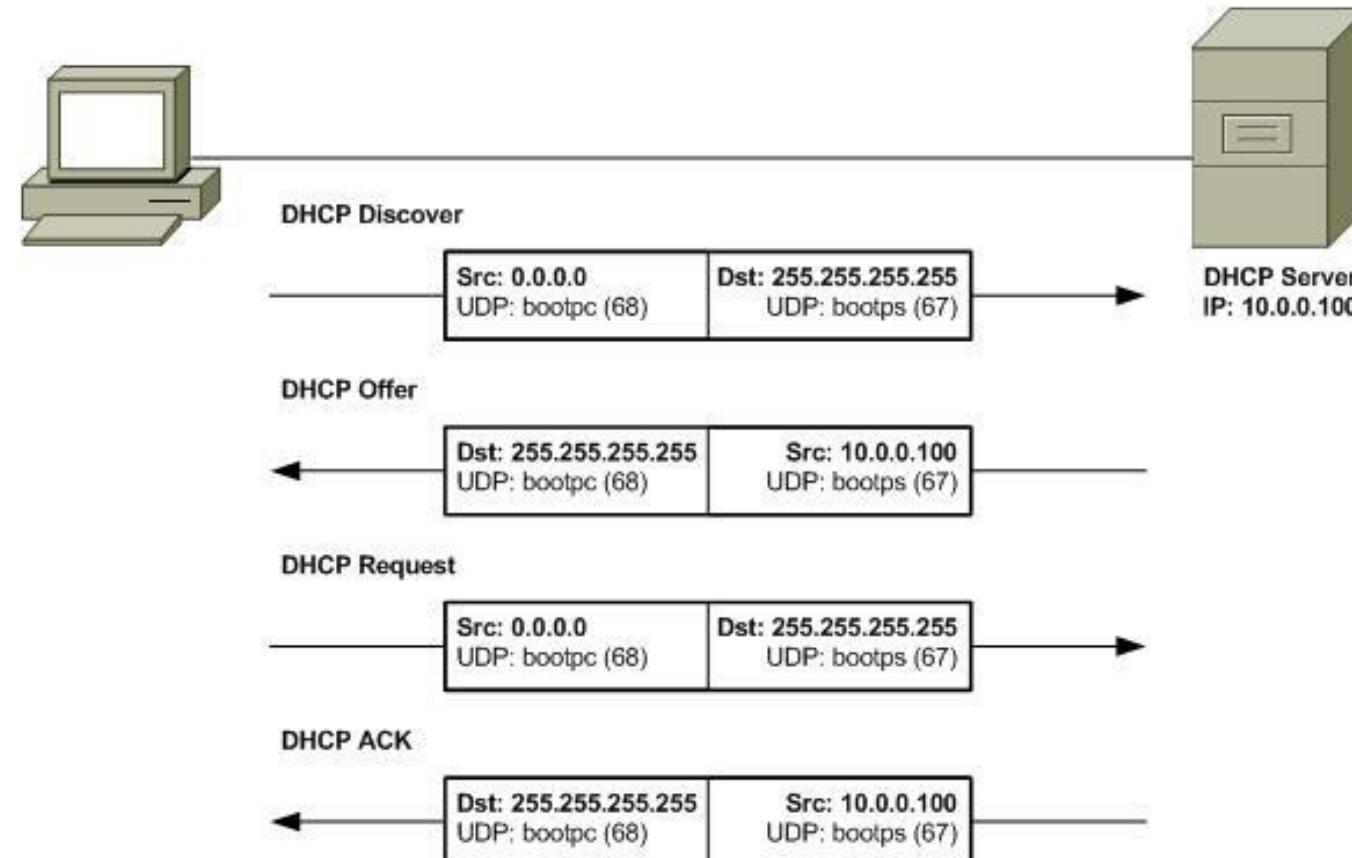
- Die studierenden
  - verstehen wie DHCP funktioniert
  - können unter Windows Server 2022 einen DHCP konfigurieren
  - können DHCP als Failover konfigurieren

- Windows Server 2019 – Schieb
  - Kapitel 13

- Konfigurierte DHCP:
  - Scope für 192.168.110.0/24
  - Vollständig Konfigurierte Optionen
  - Reservation für Client angelegt
  - Konfigurierte Failover Server
- Bewertung erfolgt mittels DHCP Dump
  - Netsh dhcp server \192.168.110.XXX dump
  - Dump direkt in txt: «Netsh dhcp server \192.168.110.XXX dump >> VmWSX.txt»
  - Der Befehl muss auf dem DHCP Server ausgeführt werden die IP entspricht der IP des Servers
  - Auf beiden DHCP Servern ausführen

- Erleichterte Administration des Netzes
- Geräte erhalten automatisch IP Konfiguration
- Viele weitere Optionen können verteilt werden
- Reservationen können erstellt werden

## DHCP abfrage Ablauf



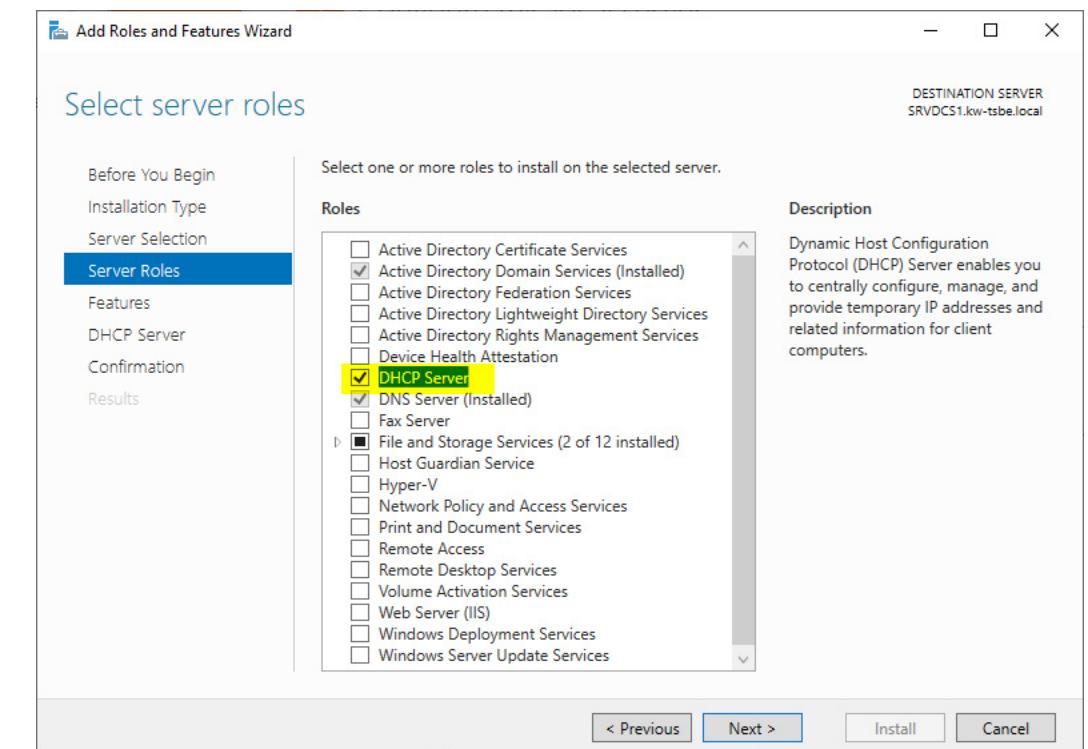
- Mehrere DHCP Ranges verwertbar
- Dynamisches Update von DNS Einträgen
  - Am besten einen separaten User erstellen und berechtigen.
- Filters Deny und Allow
  - Filter Liste muss in DHCP aktiviert werden
- DHCP Failover
  - Ausfallsichere Konfiguration
  - Mehrer Modi Load balance und Hot standby
  - Load balance Aktiv Aktiv
  - Hot standby Aktiv Passiv

Learning by doing

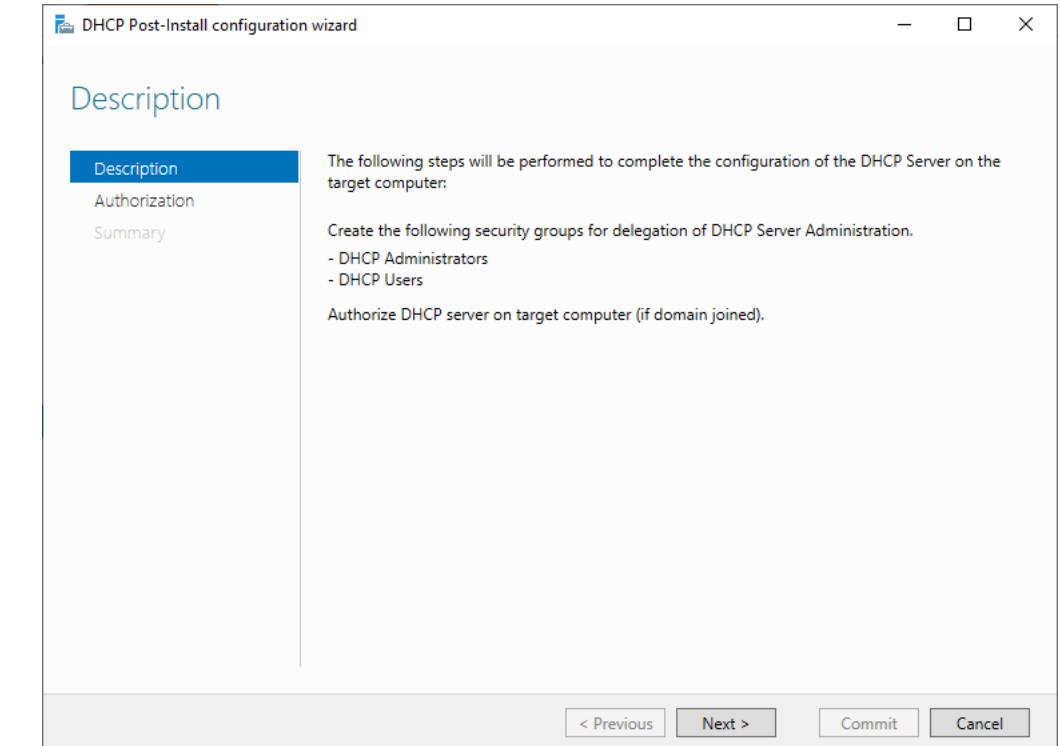
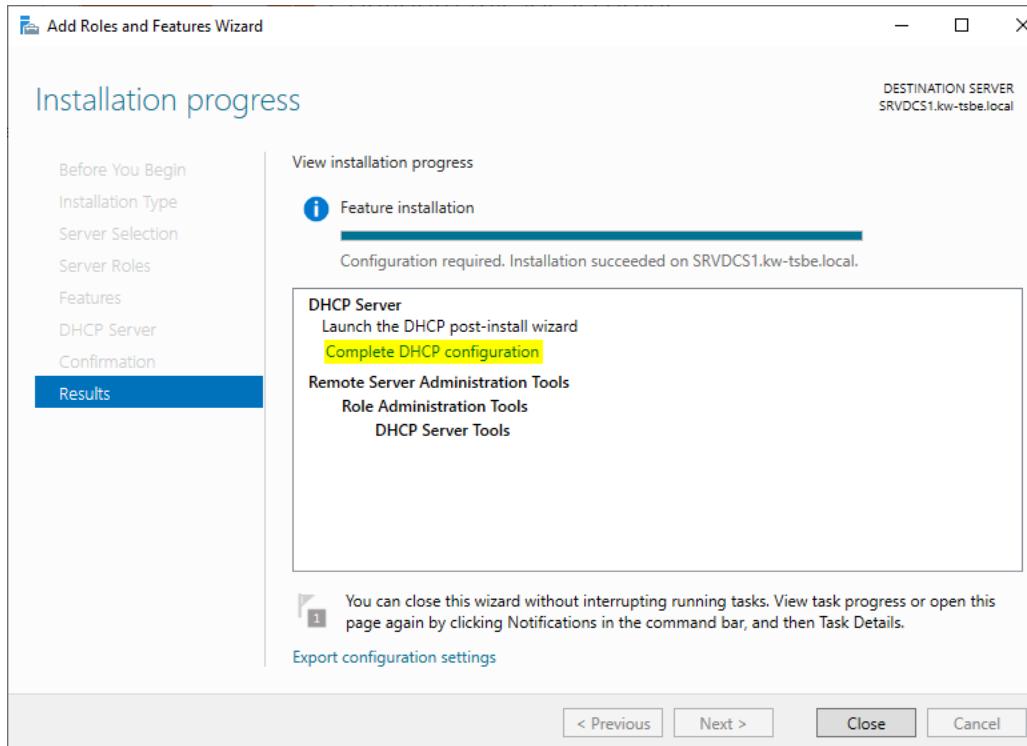
# PRACTICE

- Installation Rolle DHCP
  - VmWS1
- Grundkonfiguration DHCP
- Failover Konfiguration
  - Mit Server VmWS2 <-
- VmWP1
  - Grundkonfiguration
  - In die Domäne aufnehmen
  - In die OU Struktur einpflegen

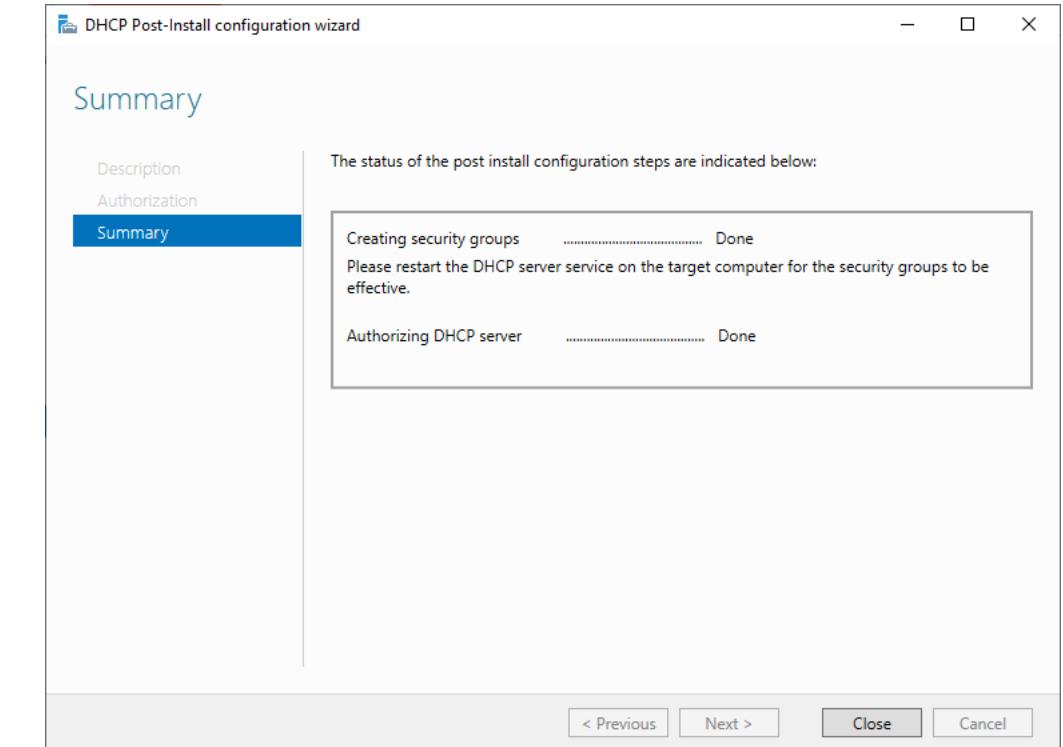
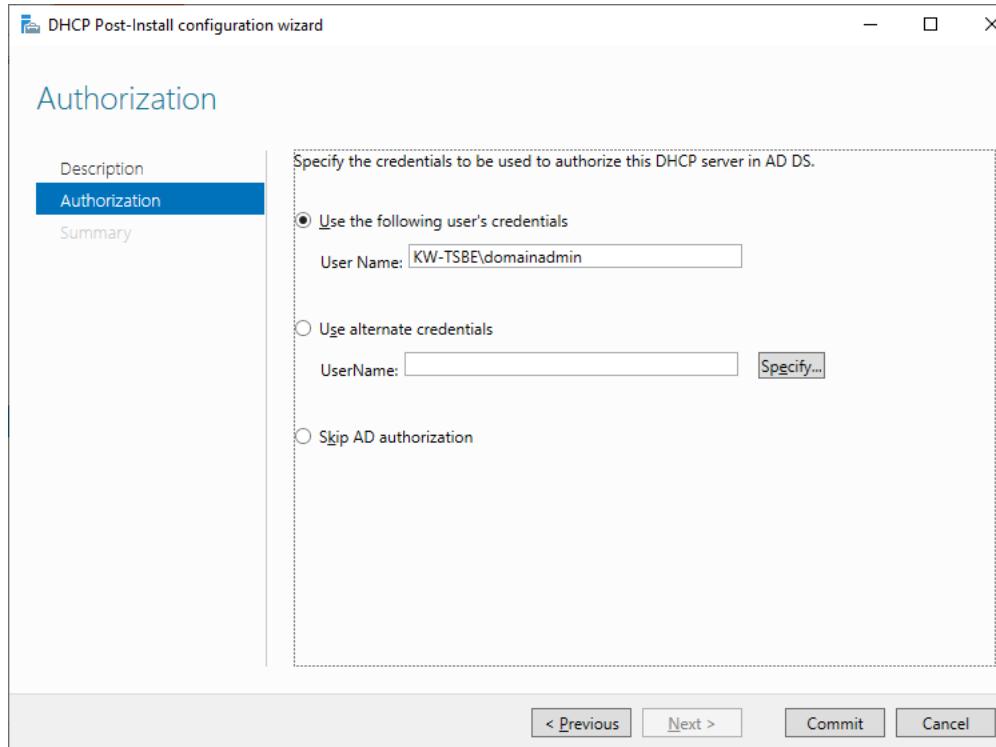
## ■ DHCP Server Rolle installieren



## VmWS1 Konfiguration DHCP

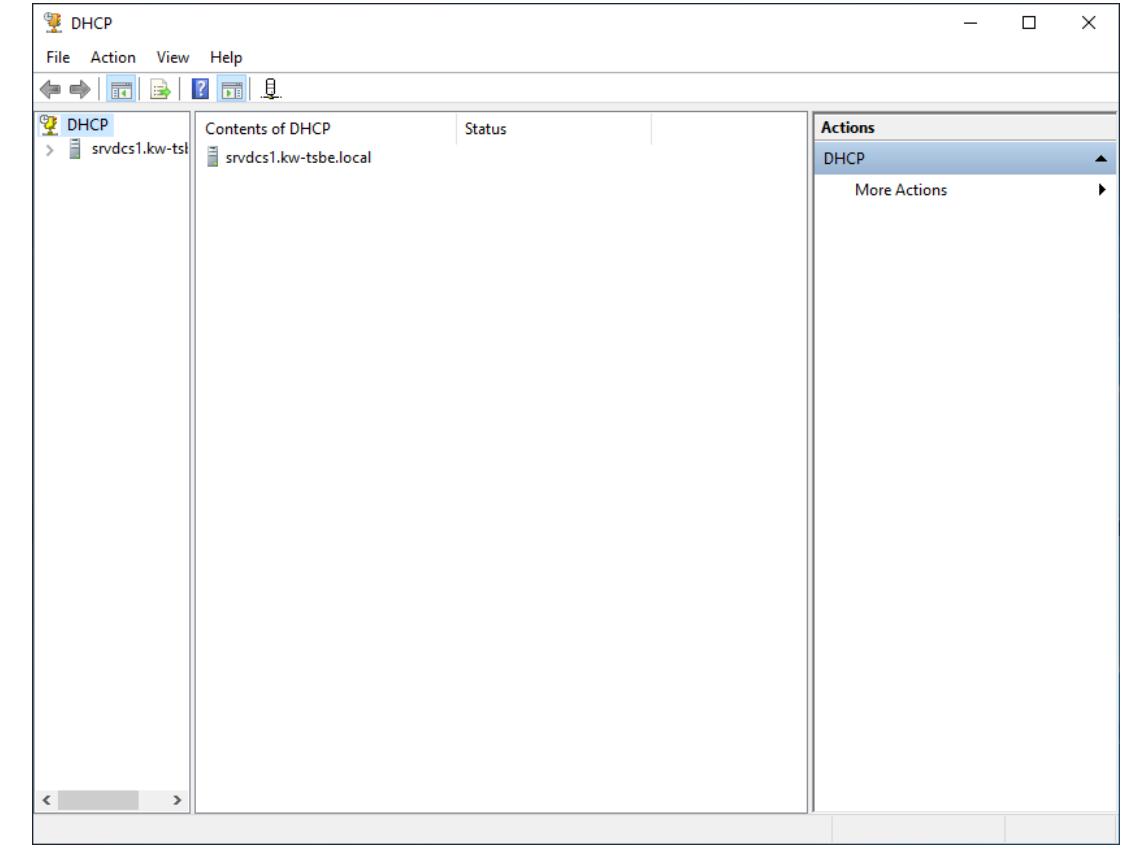
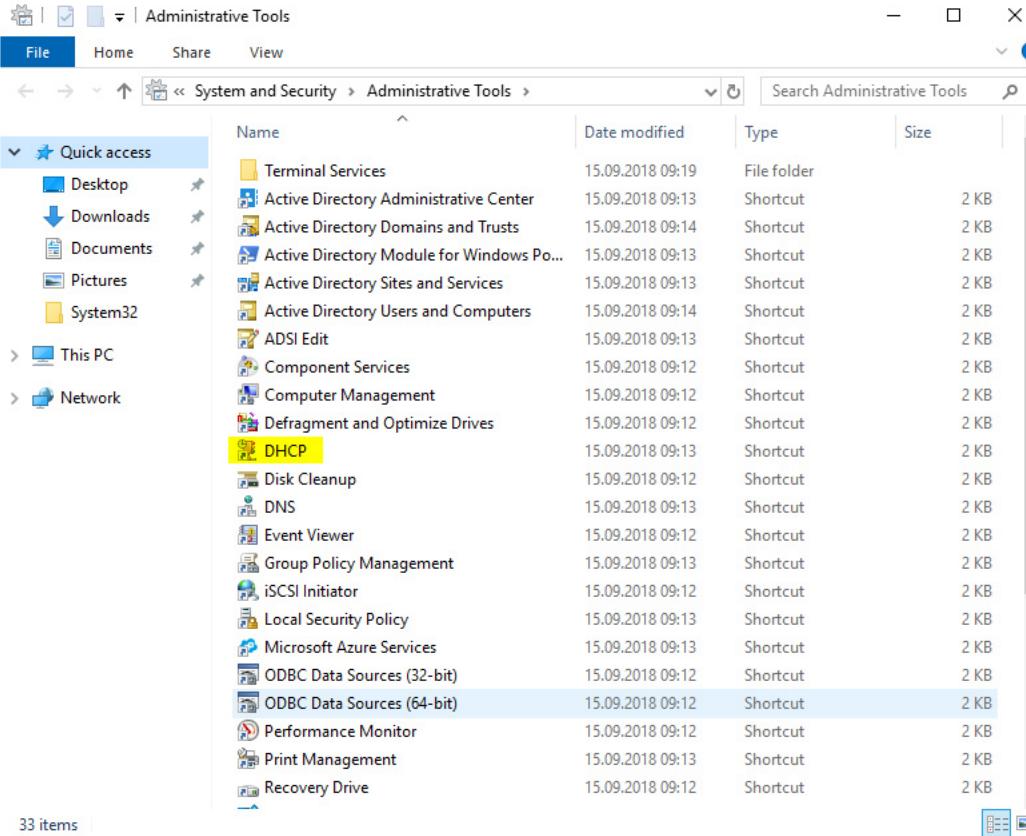


## VmWS1 Konfiguration DHCP

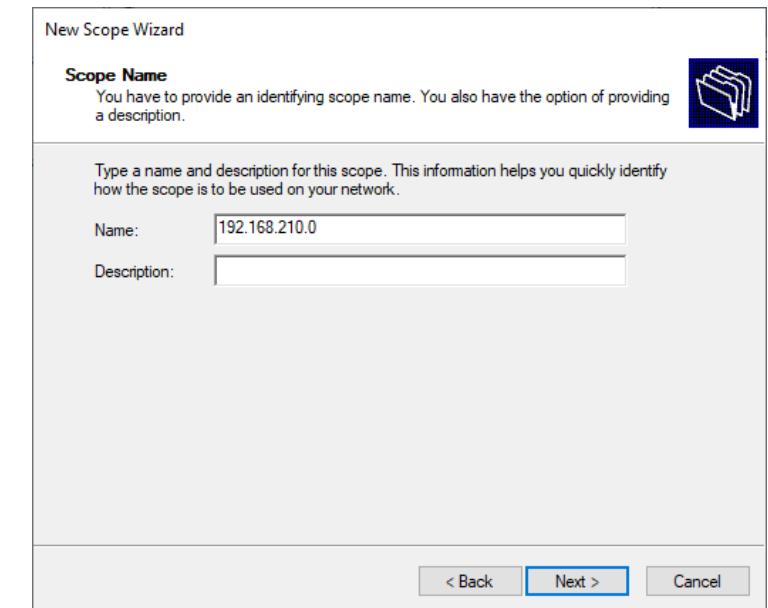
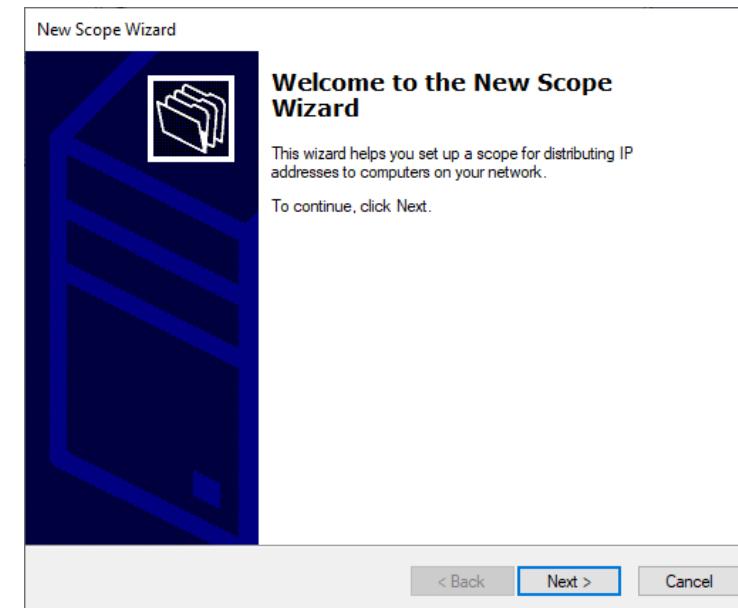
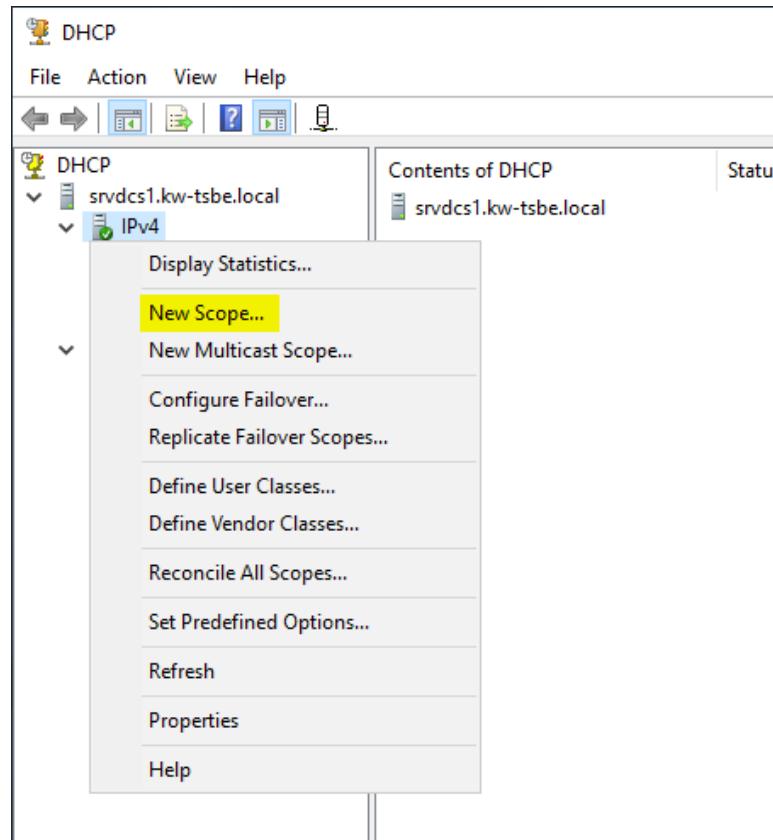


## VmWS1 Konfiguration DHCP

## ■ Neues MMC



## VmW51 Konfiguration DHCP



## VmWS1 Konfiguration DHCP

New Scope Wizard

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:   
End IP address:

Configuration settings that propagate to DHCP Client

Length:   
Subnet mask:

< Back  Cancel

New Scope Wizard

**Add Exclusions and Delay**  
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:   
End IP address:   
Add

Excluded address range:

Remove

Subnet delay in millisecond:

< Back  Cancel

New Scope Wizard

**Lease Duration**  
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

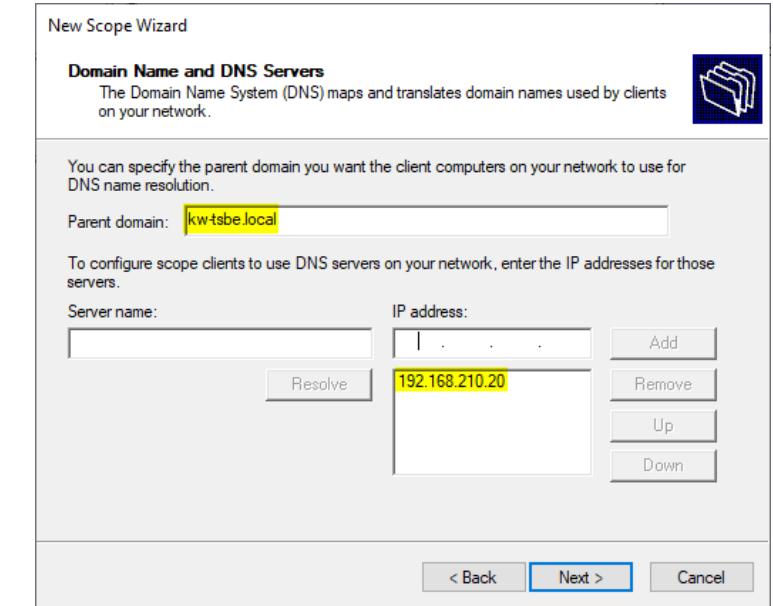
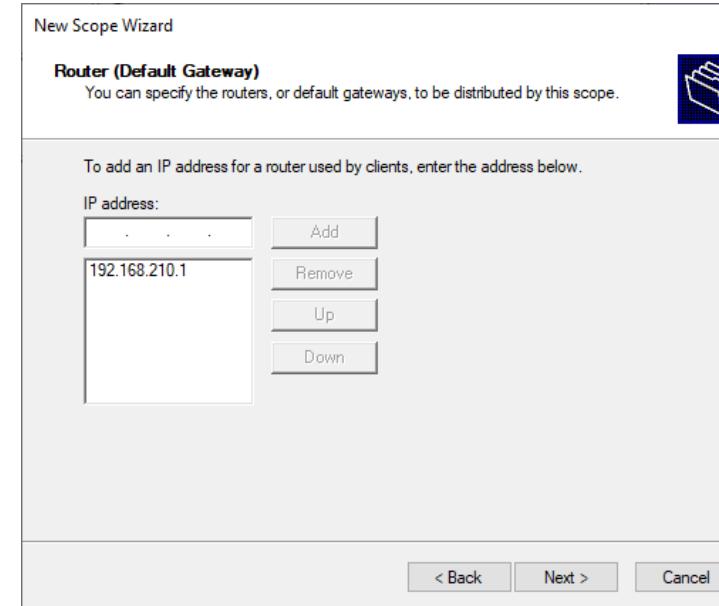
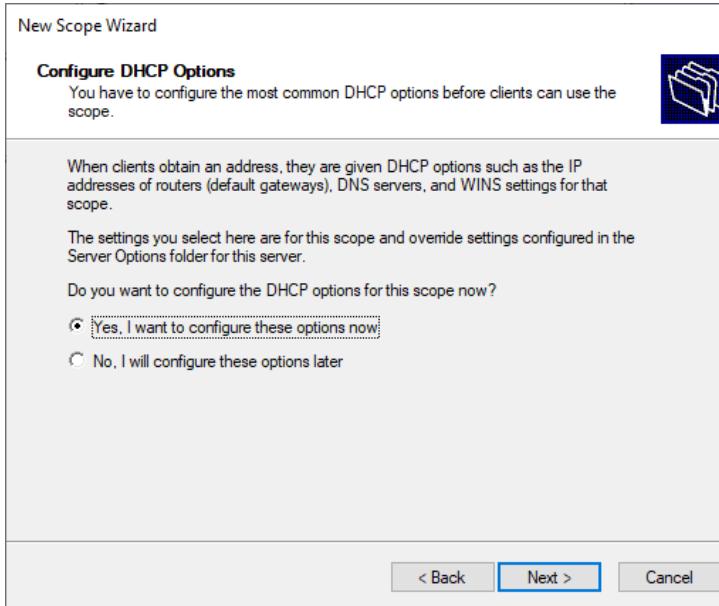
Set the duration for scope leases when distributed by this server.

Limited to:

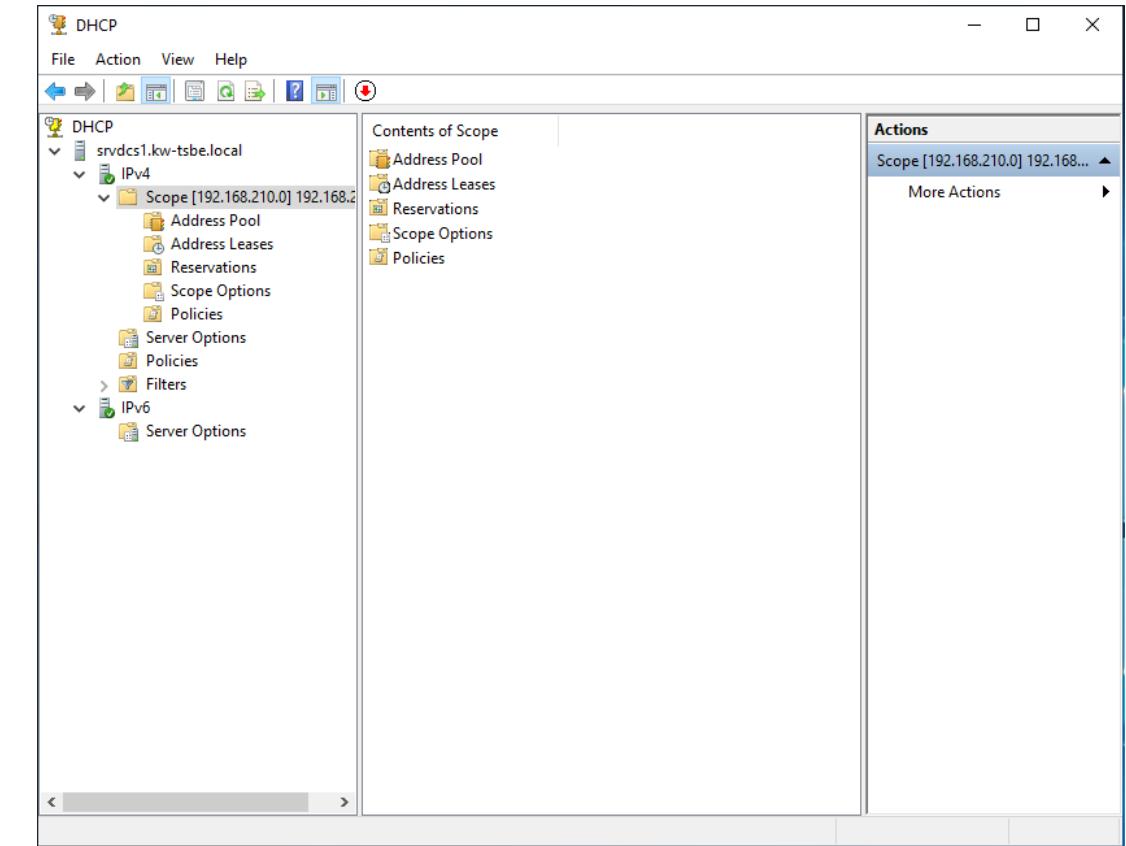
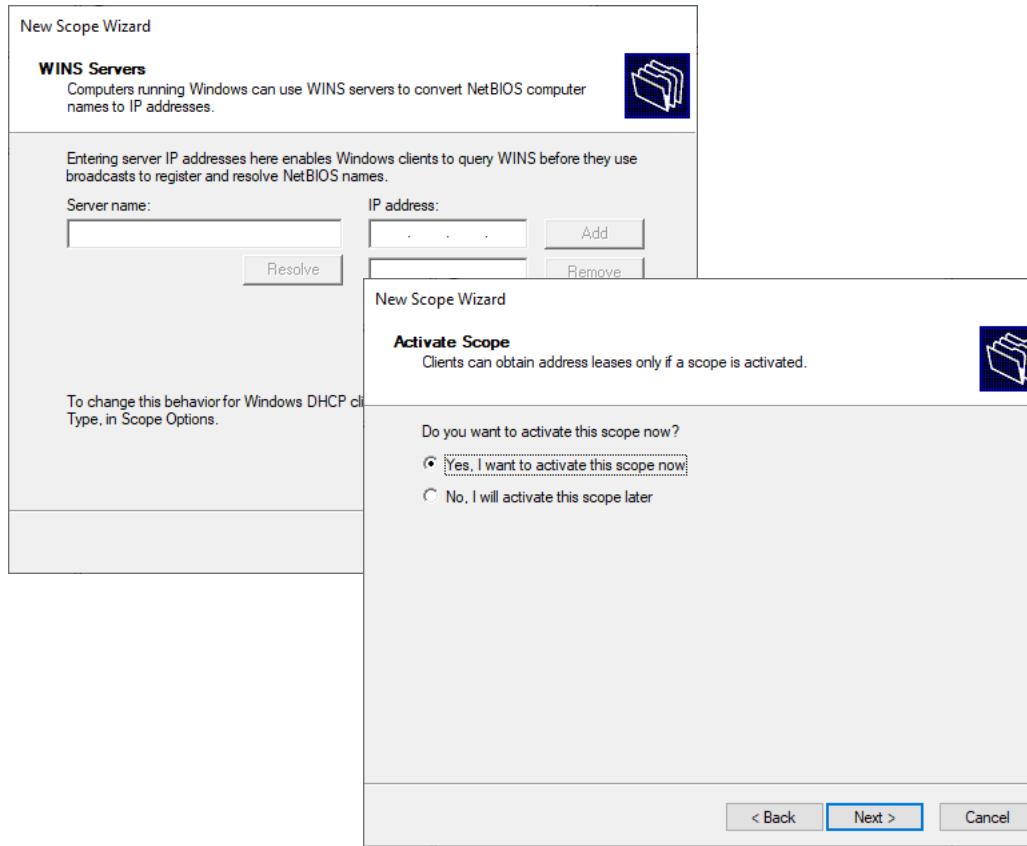
Days:  Hours:  Minutes:

< Back  Cancel

## VmWS1 Konfiguration DHCP

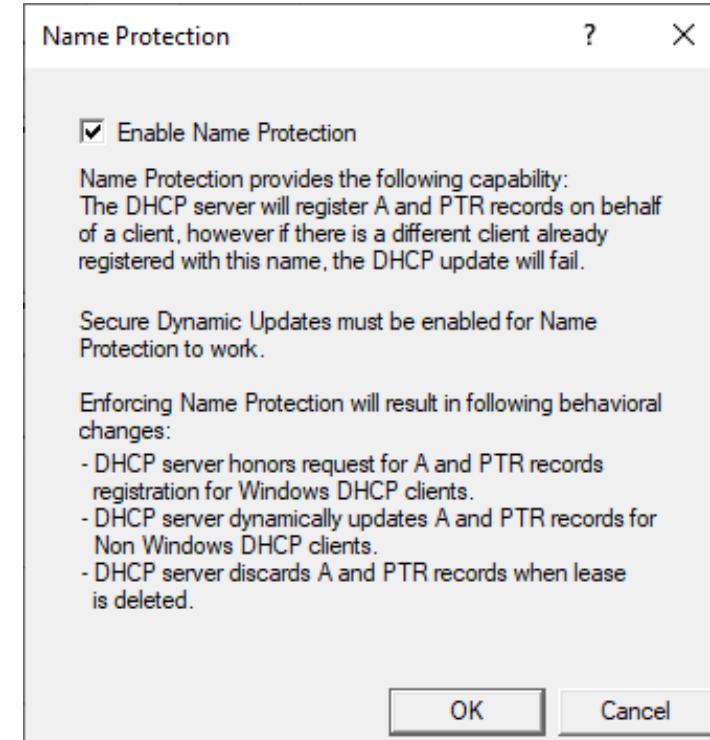
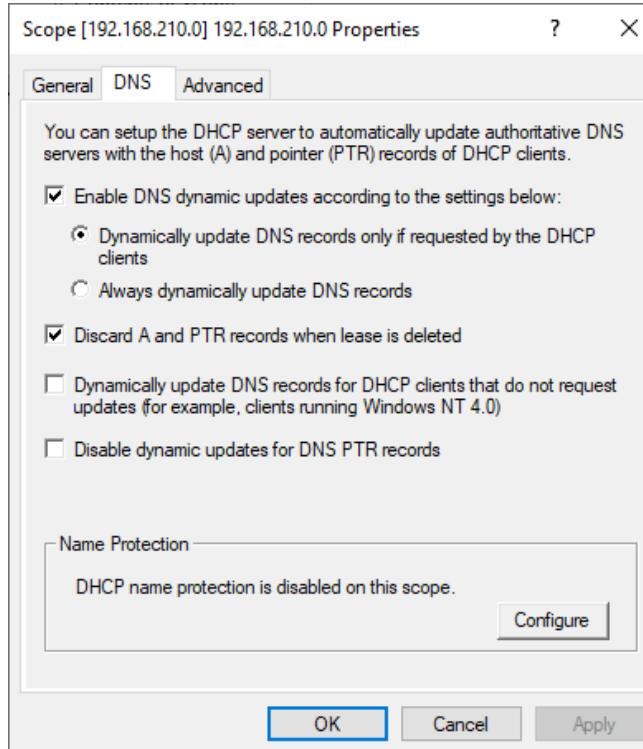


## VmWS1 Konfiguration DHCP

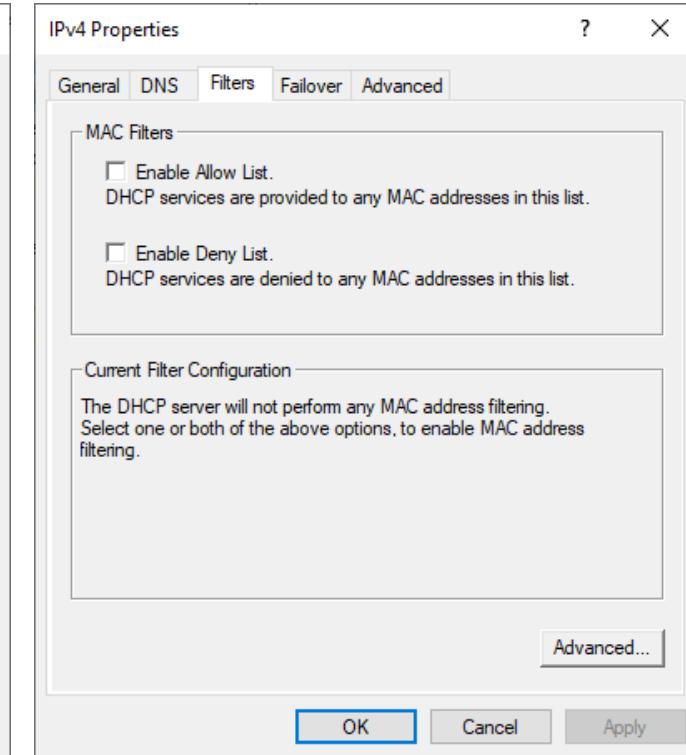
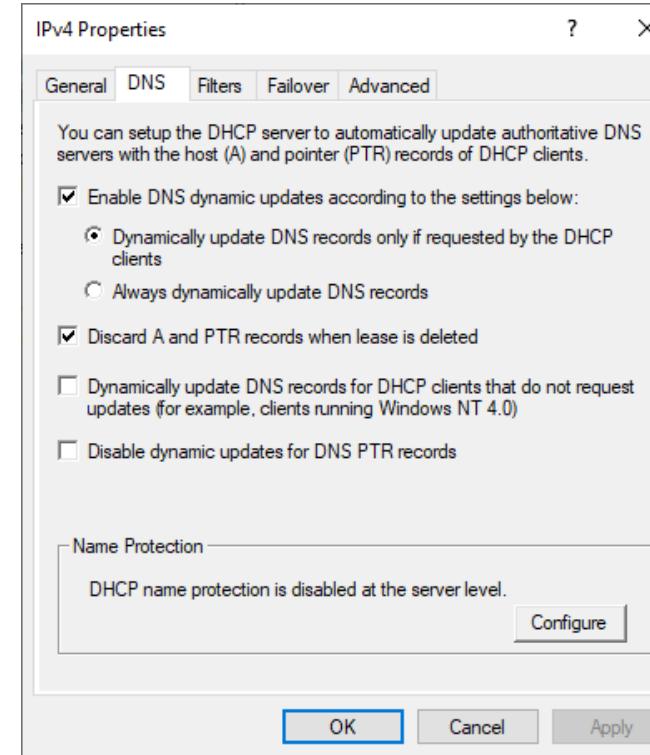
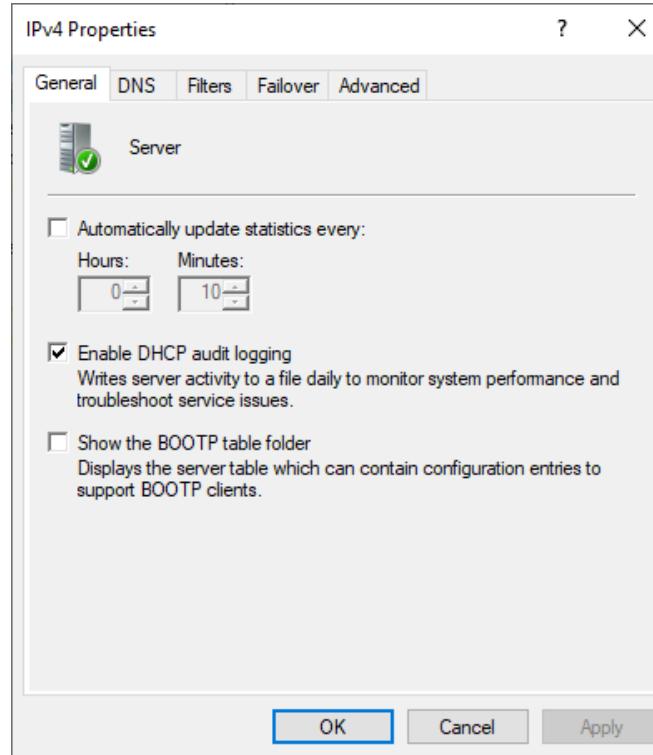


## Name Protection

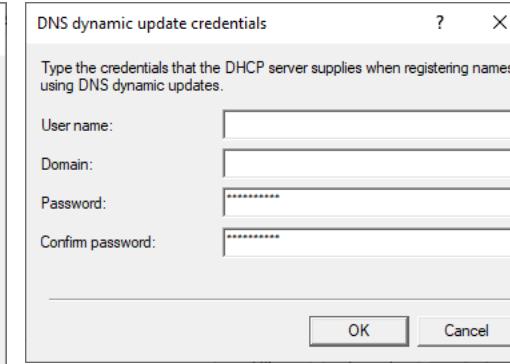
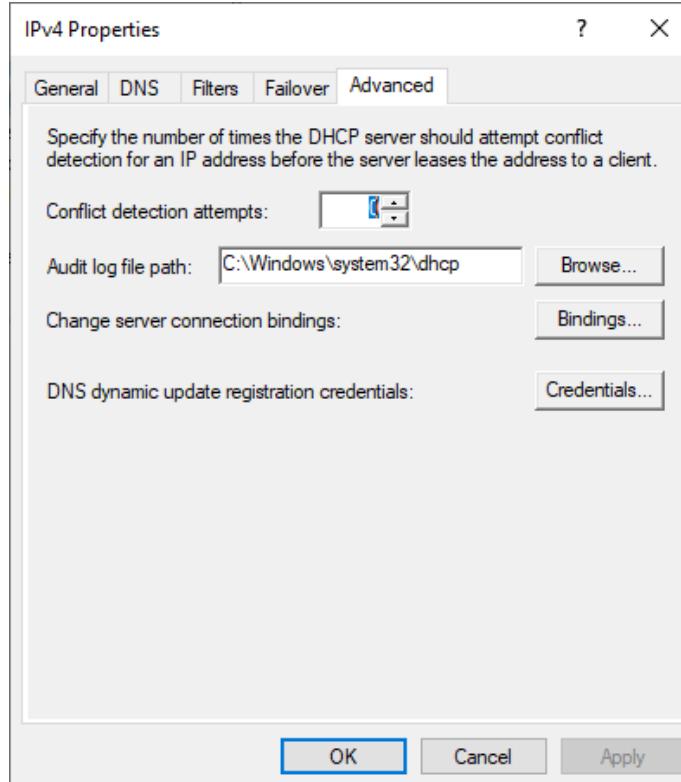
- Rechtsklick auf Scope → Properties → DNS → Configure



## DHCP IPv4 Server Einstellungen



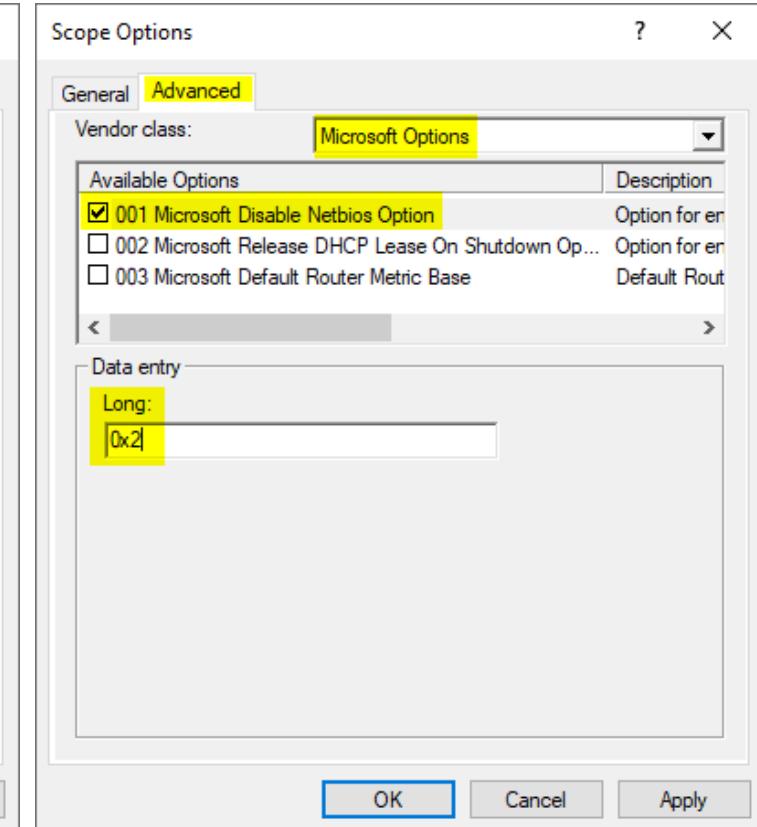
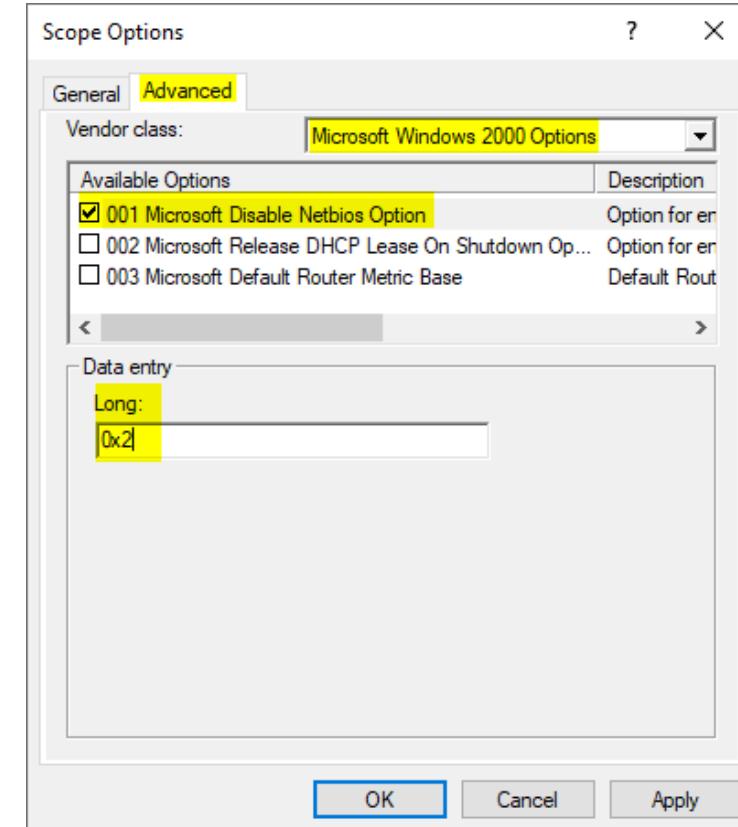
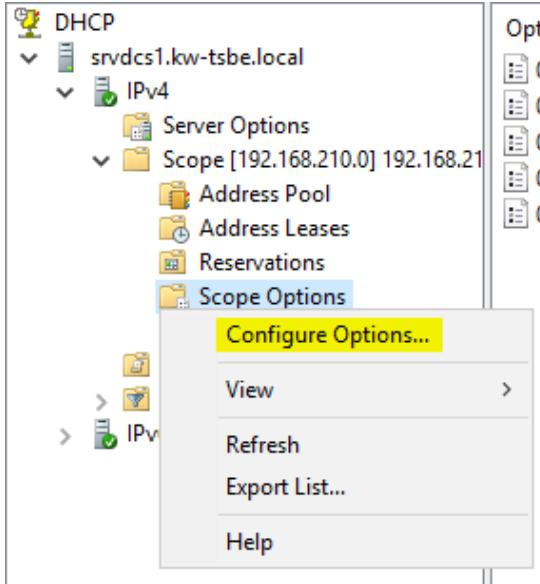
## DNS dynamic update



- Default wird der User hinterlegt der für das Autorisieren des DHCP verwendet wurde in unserem Fall der domainadmin.
- Besser wäre einen neuen User zu erstellen und diesem mit der Gruppe DNSAdmins zu berechtigen.

## NETBIOS via DHCP deaktivieren

## ■ DHCP Option



## DHCP Testen

- Auf dem Lokalen Gerät den Dienst Vmware DHCP Service Stoppen und auf Disable stellen.
- VMWP1 starten und Netzwerk Interface auf DHCP umstellen

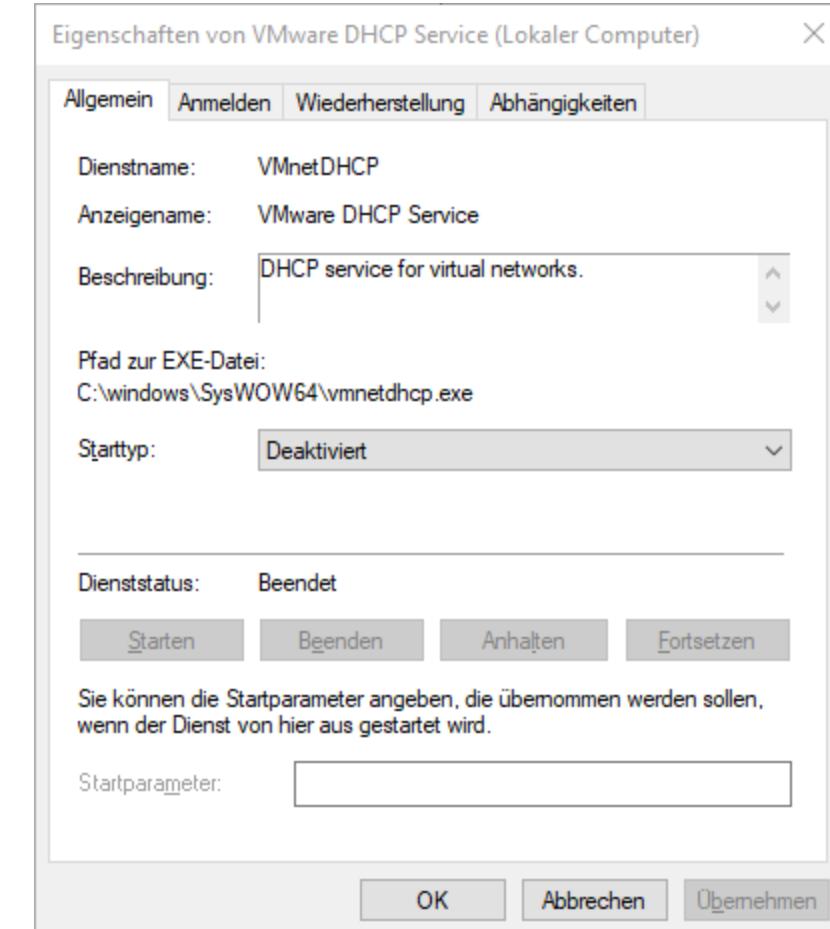
```
C:\Users\vmadmin>ipconfig /all

Windows-IP-Konfiguration

    Hostname . . . . . : vmWP1
    Primäres DNS-Suffix . . . . . :
    Knotentyp . . . . . : Hybrid
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : kw-tsbe.local

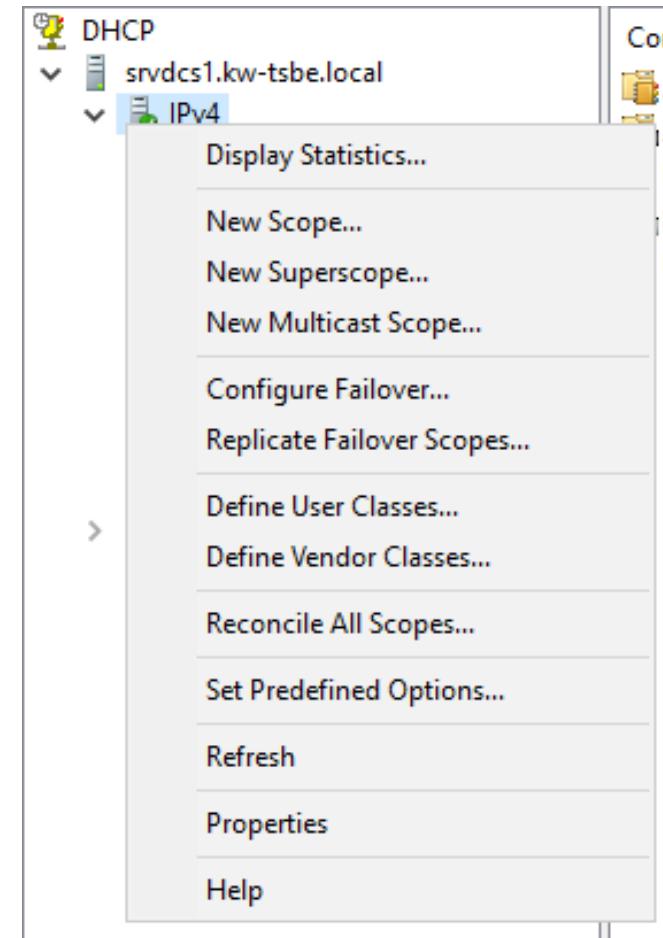
Ethernet-Adapter eth0:

    Verbindungsspezifisches DNS-Suffix: kw-tsbe.local
    Beschreibung. . . . . : Ethernet-Adapter für vmxnet3
    Physische Adresse . . . . . : 00-50-56-00-21-10
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    IPv4-Adresse . . . . . : 192.168.210.100(Bevorzugt)
    Subnetzmaske . . . . . : 255.255.255.0
    Lease erhalten. . . . . : Donnerstag, 6. Februar 2020 13:41:56
    Lease läuft ab. . . . . : Freitag, 14. Februar 2020 13:41:56
    Standardgateway . . . . . : 192.168.210.1
    DHCP-Server . . . . . : 192.168.210.20
    DNS-Server . . . . . : 192.168.210.20
    NetBIOS über TCP/IP . . . . . : Aktiviert
```

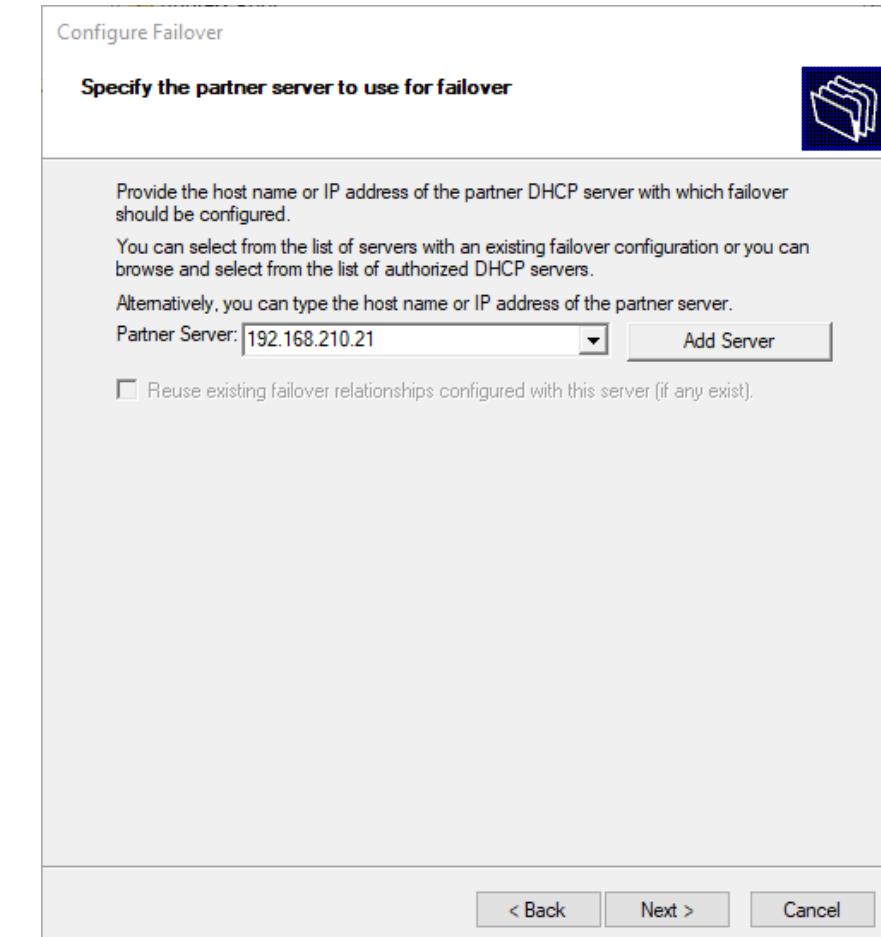


- Installieren der DHCP Rolle auf VmWS2
  - Die Installation erfolgt gleich wie auf VmWS1 mit anschliessender Autorisierung des DHCP
  - Es muss kein Scope konfiguriert werden

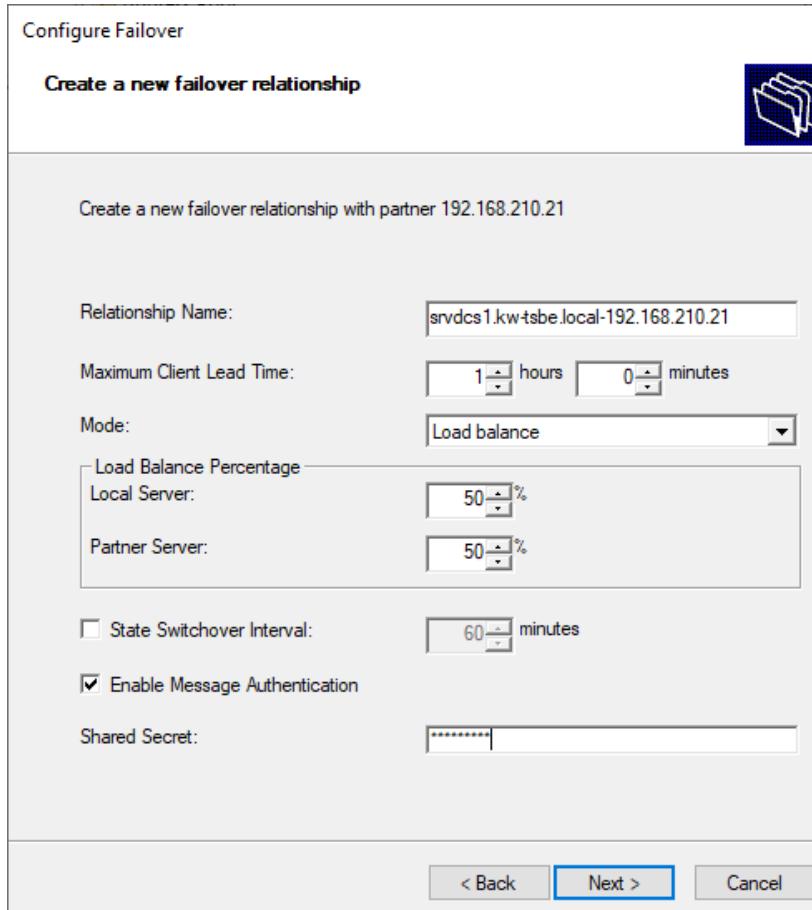
- DHCP Failover kann pro Scope konfiguriert werden.
- Rechtsklick auf den gewünschten Scope → Configure Failover...



## DHCP Failover Konfiguration

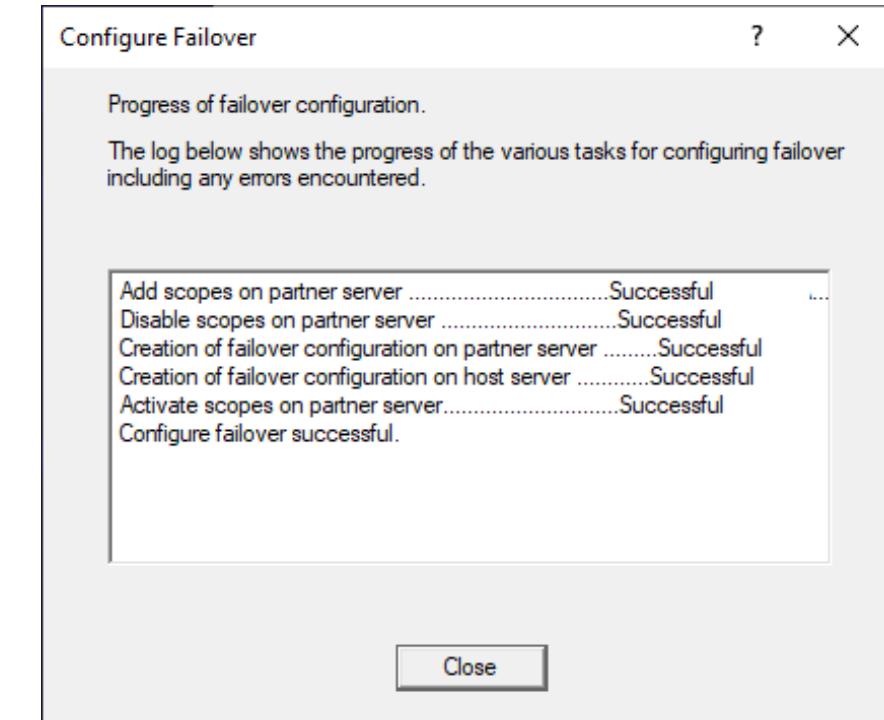
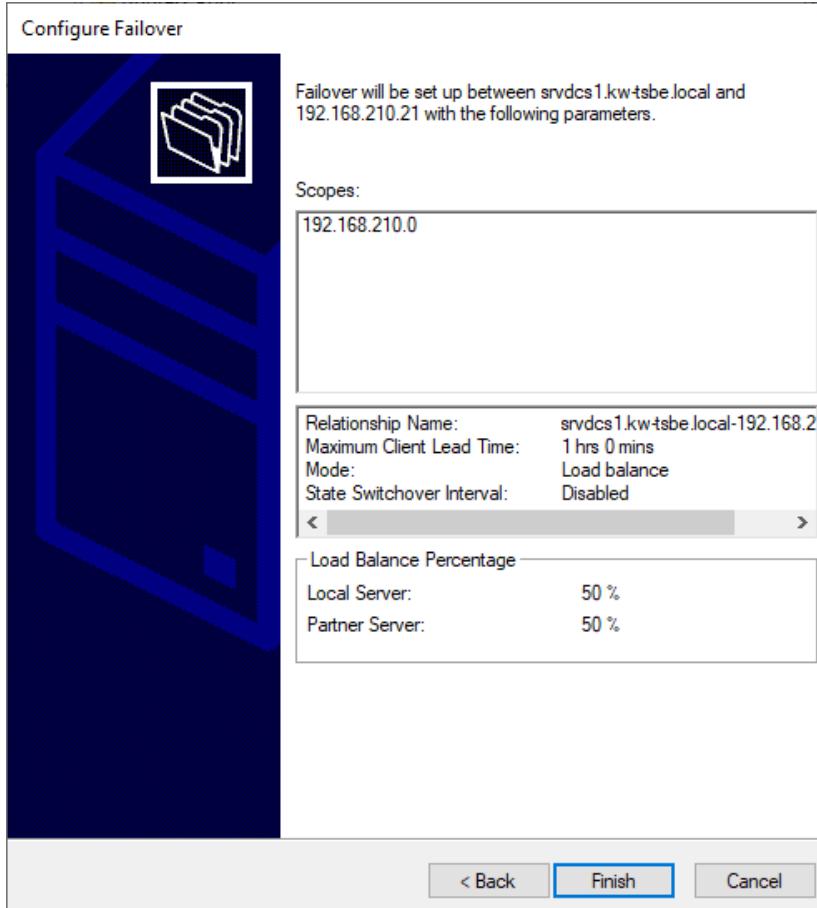


## DHCP Failover Konfiguration



- Mode hier kann zwischen den beiden Modi gewählt werden
- Bei Hos standby kann definiert werden wie viele IP Adressen der standby Server verwalten kann in Prozent.
- Ebenfalls bei Load balance wie viel der jeweilig Server Verwaltet.

## DHCP Failover Konfiguration



- DHCP Reservation für den Client Konfigurieren

Microsoft System Administration

# NTFS – New Technology File System

# IGDLA – Identities Global Groups Domain

# Local Groups Access

- Die studierenden
  - kennen das NTFS File System
  - können Freigaben erstellen
  - können mittels NTFS Berechtigungen festlegen
  - können Userhomes und Userprofile erstellen

- Windows Server 2019 – Schieb
  - Kapitel 6.2, 6.4, 6.5, 6.6, 6.7, 6.8
- Microsoft Windows Server 2012 R2 - Das Handbuch
  - 709 – 718
  - 722 Freigabe erstellen
  - 725 Versteckte Freigaben
  - 645 – 649 Gruppen

- FAT (File Allocation Table)
  - Größenlimitierung
  - Größer Kompatibilität
- NTFS (New Technology File System)
  - Typisches File System heute
  - Access Control List (ACL) und Verschlüsselung
- ReFS (Resilient File System)
  - Anwenderspezifische Fiel System z.B. Exchange Datenbanken
  - Automatische Korrektur von erkannten Datenfehlern
  - Zusätzlicher Speicherverlust
  - Unterstützt keine Bootvolumes und Quotas

- Freigaben werden benötigt um eine Ordner im Netz zugänglich zu machen
- Einfache Berechtigungsmöglichkeiten
- Zugriff auf eine Share erfolgt über den Explorer
  - <\\Servername\Freigabenamen>
- Versteckte Freigaben
  - Freigabe Name mit einem \$ ergänzen
- Windows hat Standardfreigaben

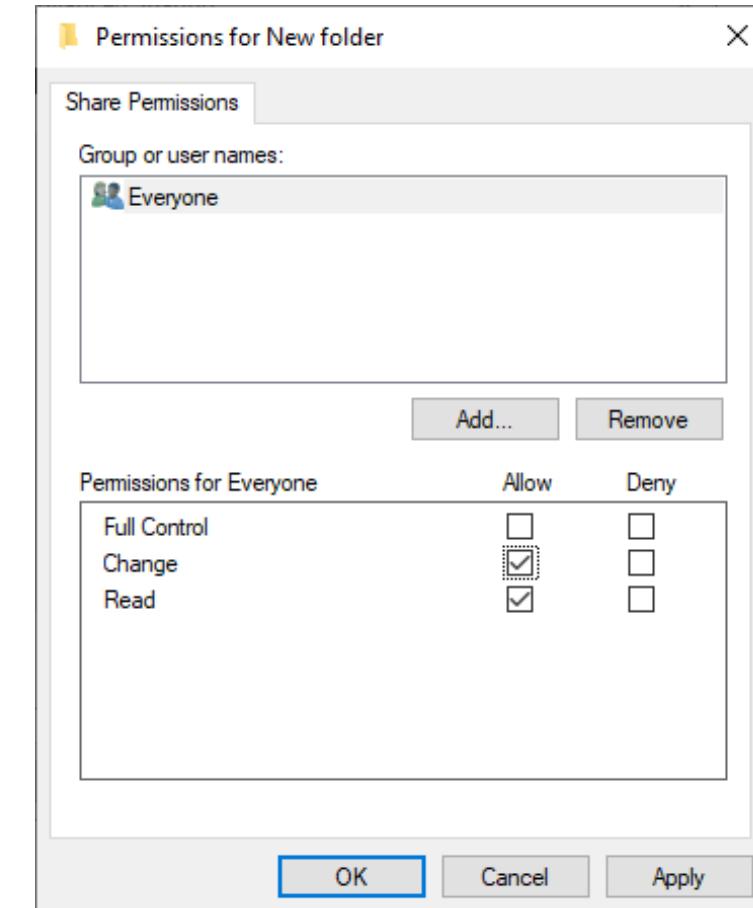
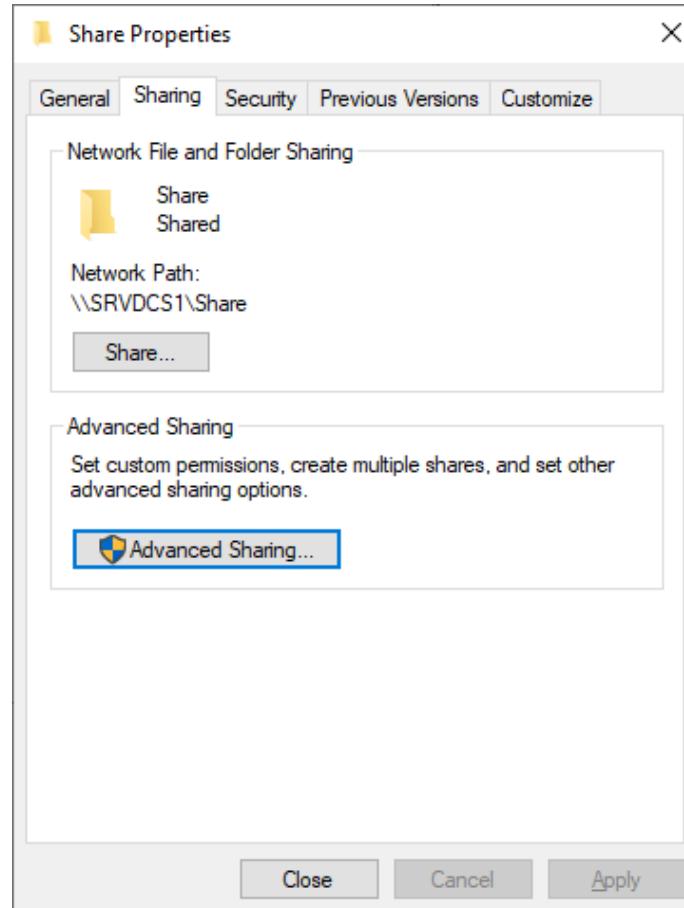
## Windows Freigaben

The screenshot shows the Windows Computer Management console window titled "Computerverwaltung". The left navigation pane is expanded to show "Computerverwaltung (Lokal)" and its sub-items: System, Aufgabenplanung, Ereignisanzeige, Freigegebene Ordner (with sub-items Freigaben, Sitzungen, Geöffnete Dateien), Lokale Benutzer und Gruppen, Leistung, and Geräte-Manager. The main pane displays a table of shared resources:

| Freigabename | Ordnerpfad | Typ     | Anzahl der Clientverbindungen | Beschreibung     |
|--------------|------------|---------|-------------------------------|------------------|
| ADMIN\$      | C:\Windows | Windows | 0                             | Remoteverwaltung |
| C\$          | C:\        | Windows | 0                             | Standardfreigabe |
| IPCS         |            | Windows | 0                             | Remote-IPC       |

The right pane shows an "Aktionen" (Actions) list with "Freigaben" selected. A tooltip for "Freigaben" indicates "Weitere Aktionen".

## Freigaben / Shares



- Verschiedene Berechtigungen sind möglich
- Reicht für die meisten Berechtigungen

Basic permissions:

- Full control
- Modify
- Read & execute
- List folder contents
- Read
- Write
- Special permissions

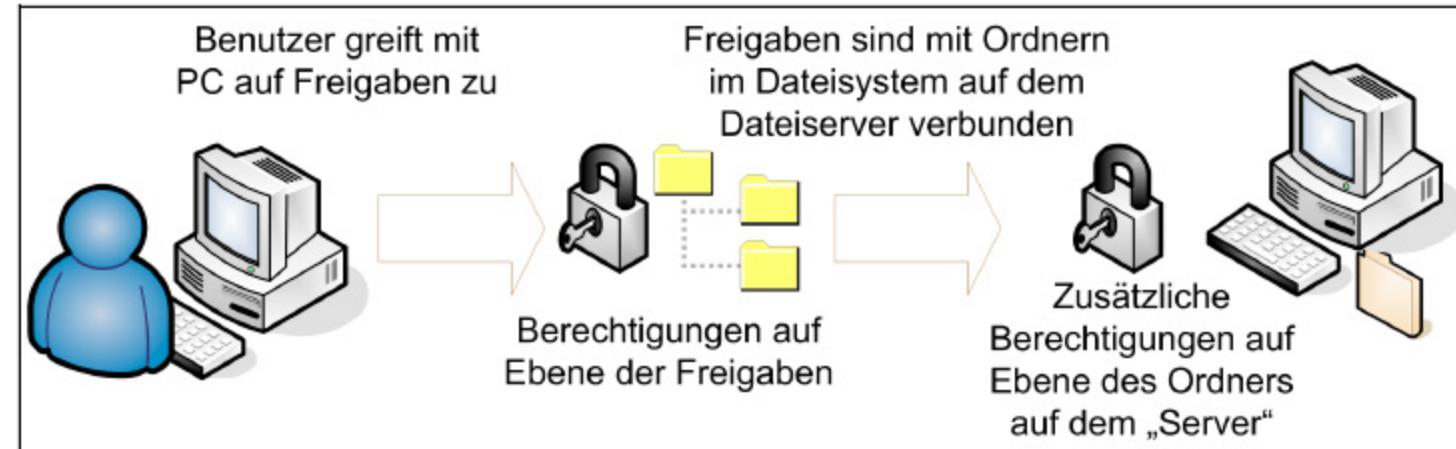
- 14 Verschiedene Berechtigungen möglich
- Für anspruchsvolle Berechtigungen

## Advanced permissions:

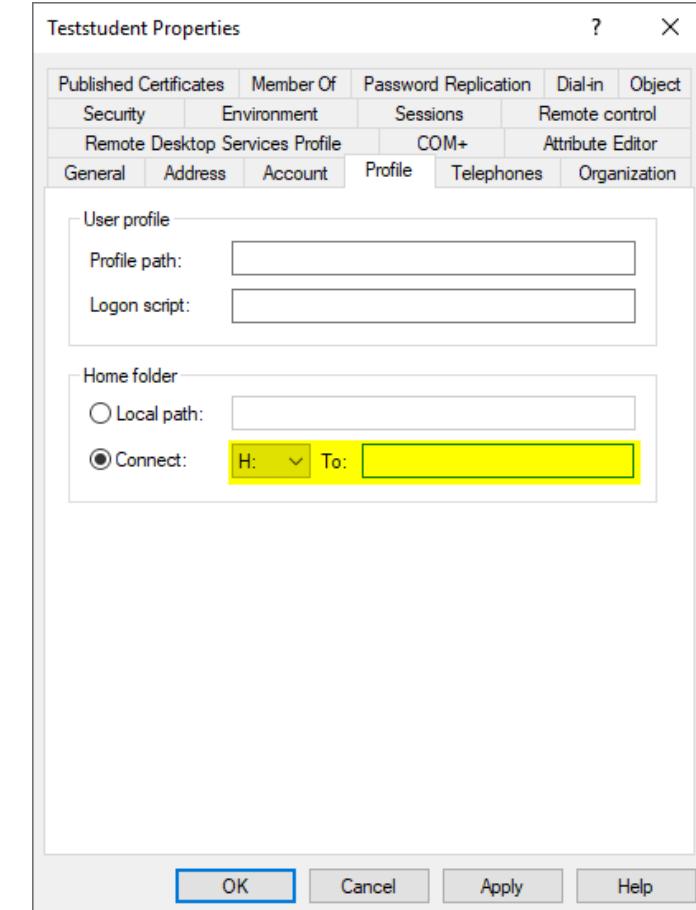
- |   |  |
|---|--|
| <input type="checkbox"/> Full control                   | <input type="checkbox"/> Write attributes            |
| <input type="checkbox"/> Traverse folder / execute file | <input type="checkbox"/> Write extended attributes   |
| <input type="checkbox"/> List folder / read data        | <input type="checkbox"/> Delete subfolders and files |
| <input type="checkbox"/> Read attributes                | <input type="checkbox"/> Delete                      |
| <input type="checkbox"/> Read extended attributes       | <input type="checkbox"/> Read permissions            |
| <input type="checkbox"/> Create files / write data      | <input type="checkbox"/> Change permissions          |
| <input type="checkbox"/> Create folders / append data   | <input type="checkbox"/> Take ownership              |
- Only apply these permissions to objects and/or containers within this container

- Die Berechtigungen werden vererbt
  - Die Vererbung kann unterbrochen werden
  - Die Vererbung kann wieder aktiviert werden
- Zulassen (Allow) und Verweigern (Deny) möglich
  - Verweigern ist immer stärker
- Datei- und Ordnerberechtigungen sind voneinander unabhängig
- Berechtigungen sind immer Kumulativ

## Berechtigungszugriff

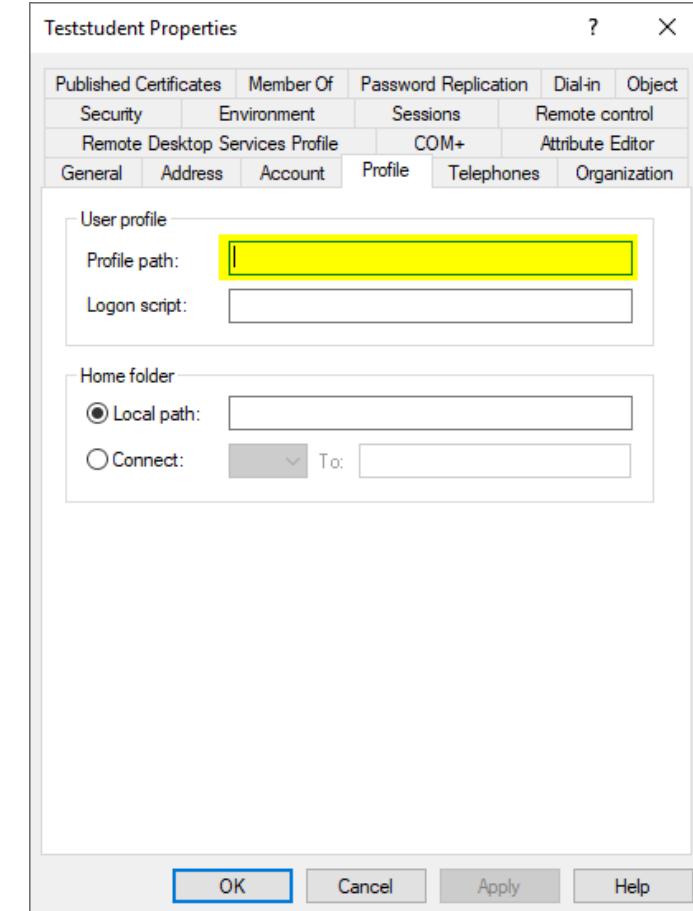


- Persönlicher Ordner für User
- Wird automatisch als Netzlaufwerk verbunden bei der Anmeldung
- Wird beim Eintrage automatisch erstellt
- ACHTUNG beim Eintragen mittels Script muss der Ordner manuell erstellt werden

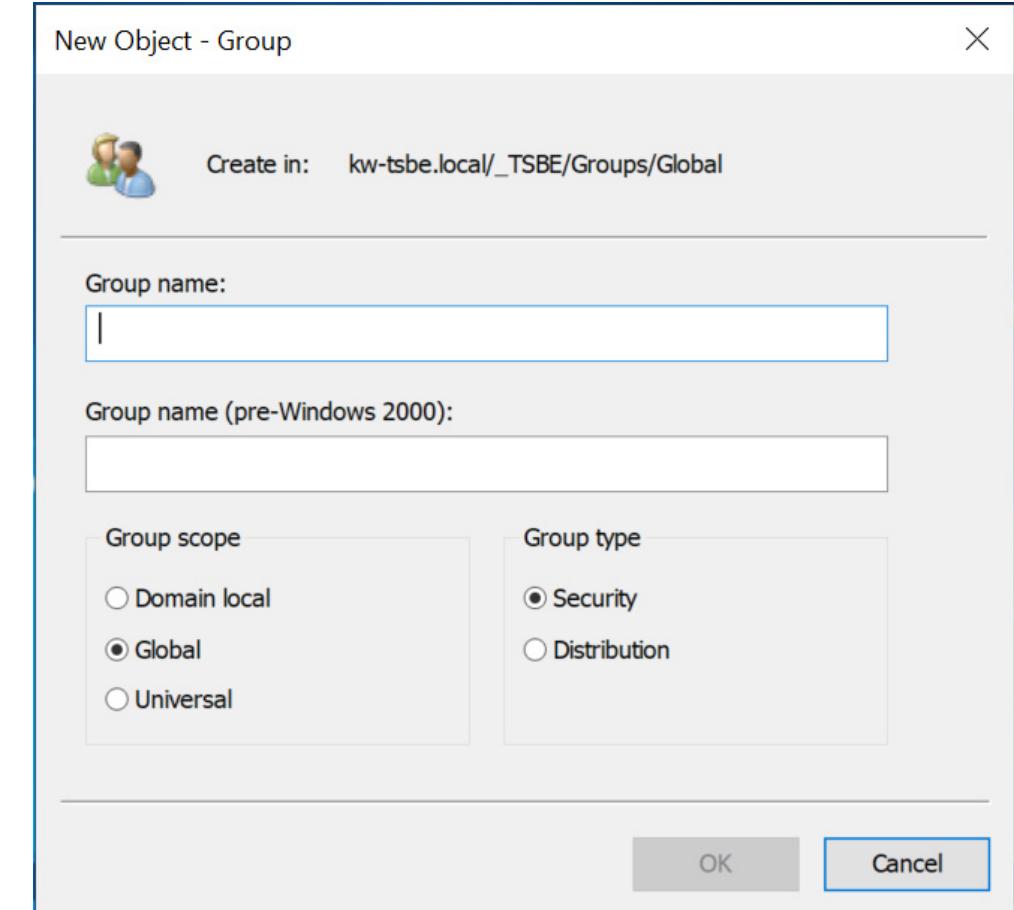


## Userprofiles

- Benutzerprofile
- Lokales Client Profile wird auf den Server gespeichert
  - Desktop, Downloads, AppData etc.
- Ausschliessend von Verzeichnissen mittels GPO
- Vorteile
  - Daten sind immer auf allen Geräten vorhanden
- Nachteile
  - Kann zu Problemen führen mit diversen Applikationen



- Gruppen Scope
  - Domain local
    - Zugriff: Nur innerhalb einer Domäne
  - Global
    - Zugriff: Eigene Domäne, Vertrauensvolle Domäne
  - Universal
    - Zugriff: gesamter Forest
- Group type
  - Security
    - Zugriffsberechtigungen
  - Distribution
    - E-Mail Verteilerlisten



## Standardgruppen im AD

## Built-in

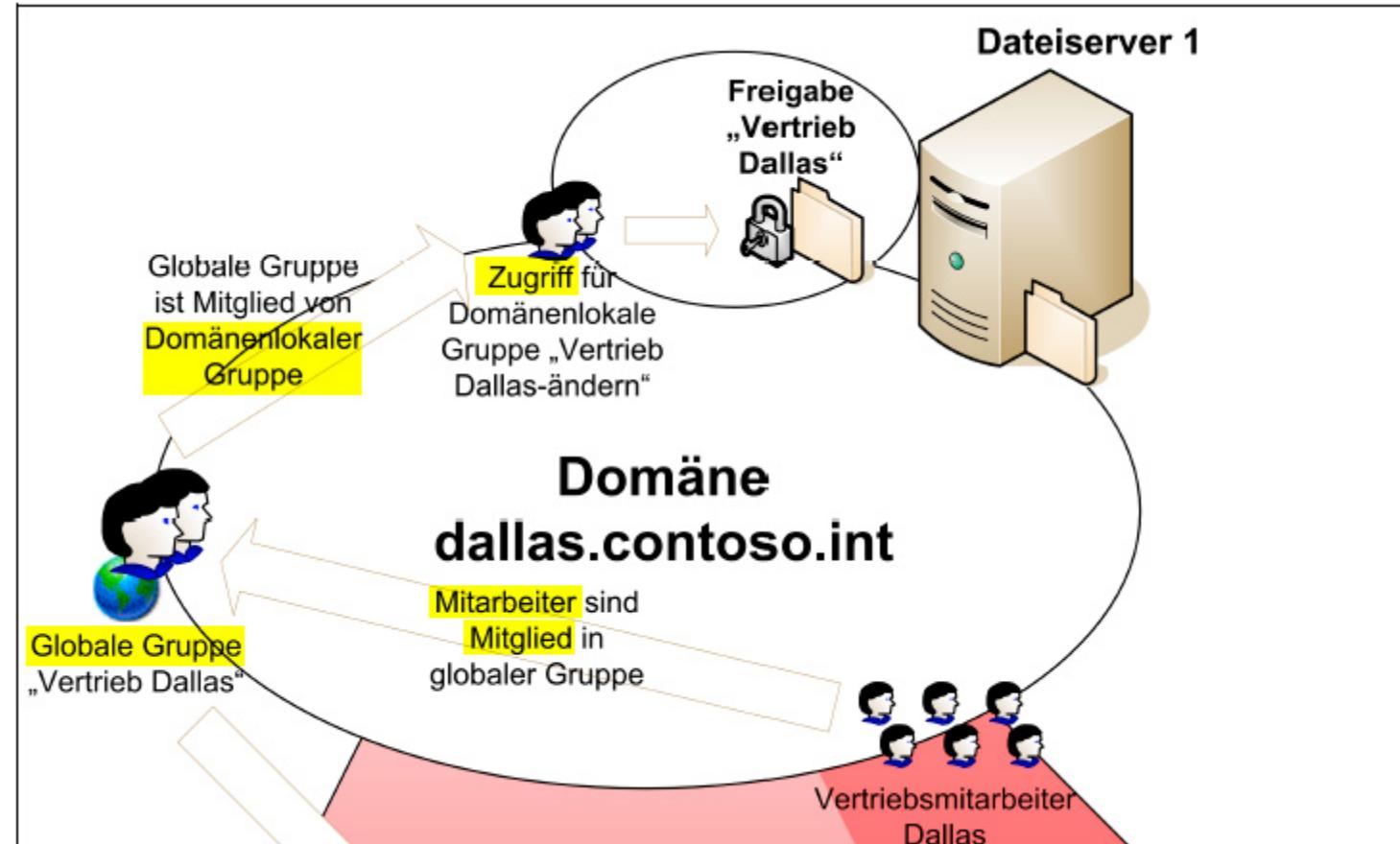
## Users

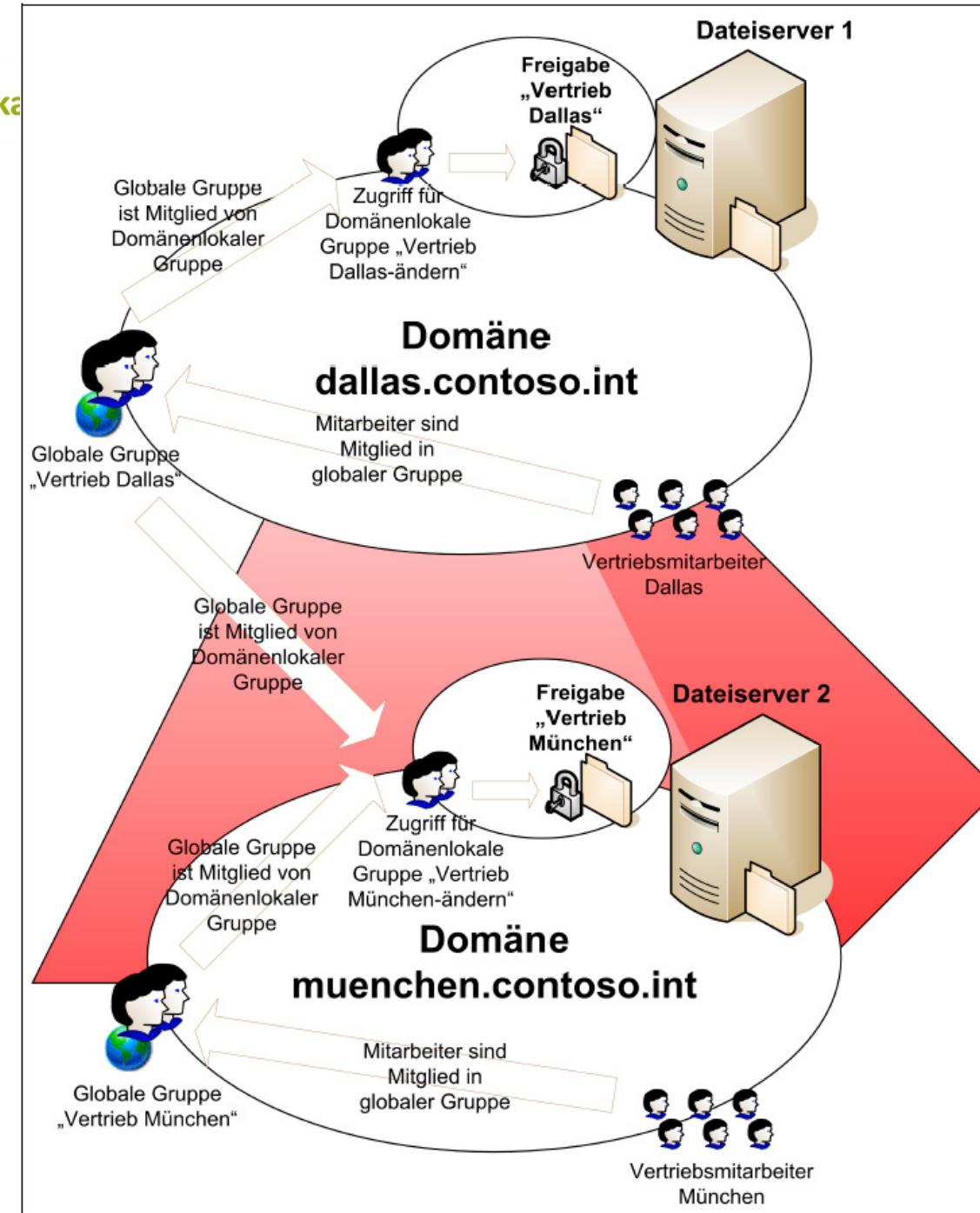
| Name                                | Type                 | Description                       |
|-------------------------------------|----------------------|-----------------------------------|
| Access Control Assistance Operators | Security Group - ... | Members of this group can re...   |
| Account Operators                   | Security Group - ... | Members can administer dom...     |
| Administrators                      | Security Group - ... | Administrators have complete...   |
| Backup Operators                    | Security Group - ... | Backup Operators can overrid...   |
| Certificate Service DCOM Access     | Security Group - ... | Members of this group are all...  |
| Cryptographic Operators             | Security Group - ... | Members are authorized to pe...   |
| Distributed COM Users               | Security Group - ... | Members are allowed to launc...   |
| Event Log Readers                   | Security Group - ... | Members of this group can re...   |
| Guests                              | Security Group - ... | Guests have the same access a...  |
| Hyper-V Administrators              | Security Group - ... | Members of this group have co...  |
| IIS_IUSRS                           | Security Group - ... | Built-in group used by Intern...  |
| Incoming Forest Trust Builders      | Security Group - ... | Members of this group can cre...  |
| Network Configuration Operators     | Security Group - ... | Members in this group can ha...   |
| Performance Log Users               | Security Group - ... | Members of this group may s...    |
| Performance Monitor Users           | Security Group - ... | Members of this group can ac...   |
| Pre-Windows 2000 Compatible Access  | Security Group - ... | A backward compatibility gro...   |
| Print Operators                     | Security Group - ... | Members can administer print...   |
| RDS Endpoint Servers                | Security Group - ... | Servers in this group run virt... |
| RDS Management Servers              | Security Group - ... | Servers in this group can perf... |
| RDS Remote Access Servers           | Security Group - ... | Servers in this group enable u... |
| Remote Desktop Users                | Security Group - ... | Members in this group are gr...   |
| Remote Management Users             | Security Group - ... | Members of this group can ac...   |
| Replicator                          | Security Group - ... | Supports file replication in a... |
| Server Operators                    | Security Group - ... | Members can administer dom...     |
| Storage Replica Administrators      | Security Group - ... | Members of this group have co...  |
| Terminal Server License Servers     | Security Group - ... | Members of this group can up...   |
| Users                               | Security Group - ... | Users are prevented from mak...   |
| Windows Authorization Access Group  | Security Group - ... | Members of this group have co...  |

| Name                                    | Type               | Description                   |
|---|--------------------|-------------------------------|
| Allowed RODC Password Replication Group | Security Group ... | Members in this group c...    |
| Cert Publishers                         | Security Group ... | Members of this group a...    |
| Cloneable Domain Controllers            | Security Group ... | Members of this group t...    |
| Denied RODC Password Replication Group  | Security Group ... | Members in this group c...    |
| DHCP Administrators                     | Security Group ... | Members who have adm...       |
| DHCP Users                              | Security Group ... | Members who have view...      |
| DnsAdmins                               | Security Group ... | DNS Administrators Group      |
| DnsUpdateProxy                          | Security Group ... | DNS clients who are per...    |
| Domain Admins                           | Security Group ... | Designated administrato...    |
| Domain Computers                        | Security Group ... | All workstations and serv...  |
| Domain Controllers                      | Security Group ... | All domain controllers in ... |
| Domain Guests                           | Security Group ... | All domain guests             |
| Domain Users                            | Security Group ... | All domain users              |
| domainadmin                             | User               | Built-in account for adm...   |
| Enterprise Admins                       | Security Group ... | Designated administrato...    |
| Enterprise Key Admins                   | Security Group ... | Members of this group c...    |
| Enterprise Read-only Domain Controllers | Security Group ... | Members of this group a...    |
| Group Policy Creator Owners             | Security Group ... | Members in this group c...    |
| Guest                                   | User               | Built-in account for gues...  |
| Key Admins                              | Security Group ... | Members of this group c...    |
| krbtgt                                  | User               | Key Distribution Center S...  |
| Protected Users                         | Security Group ... | Members of this group a...    |
| RAS and IAS Servers                     | Security Group ... | Servers in this group can...  |
| Read-only Domain Controllers            | Security Group ... | Members of this group a...    |
| Schema Admins                           | Security Group ... | Designated administrato...    |

- Identities (I) Global Groups (G) Domain Local Groups (DL) Access (A)
  - I Identitäten Benutzer bzw. Computer, die Mitglieder sind von..
  - G Globale Gruppen nehmen Mitglieder basierend auf Mitgliederrollen auf, die Mitglieder sind von
  - DL lokale Gruppen einer Domäne Stellen Verwaltungsfunktionen bereits z.B. Zugriff auf Ressourcen, denen
  - A Zugriff auf eine Ressource zugewiesen wurden (Access)
- Pro Zugriff muss eine lokale Gruppe erstellt und verwendet werden.  
Keine mehrfach Verwendung.
- RBAC - Role Based Access Control
  - Gruppen werden Rollenbasiert erstellt

## Grafische Darstellung



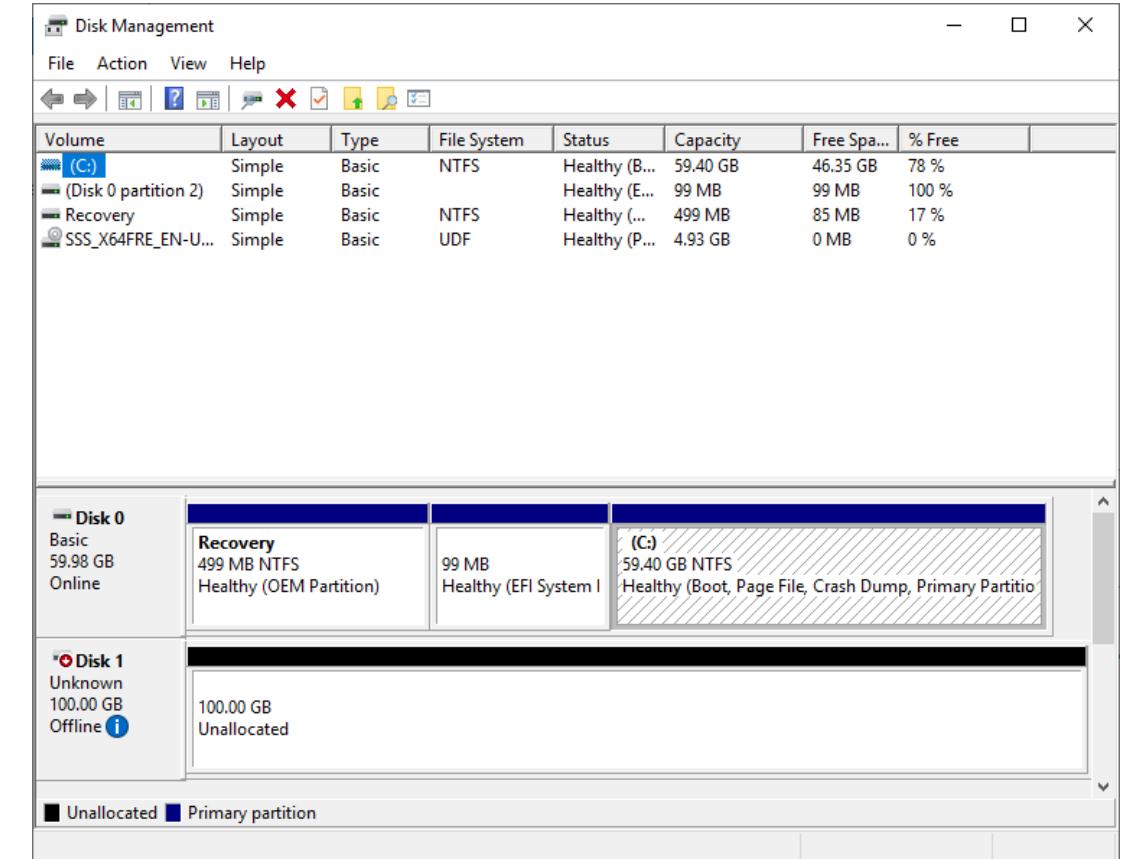


Learning by doing

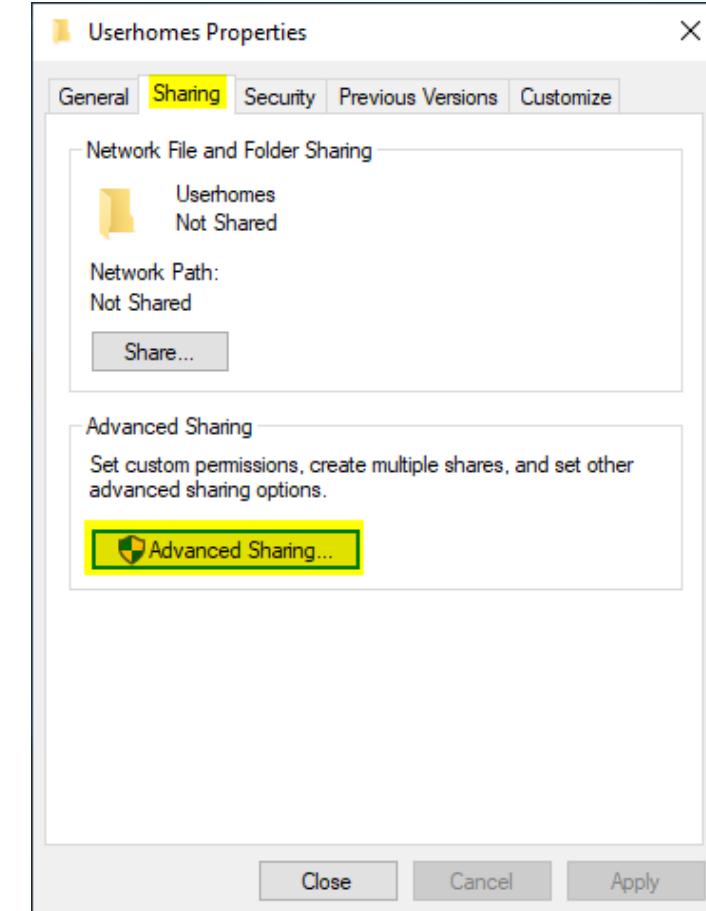
# PRACTICE

## VmWS1 Userhome Konfiguration

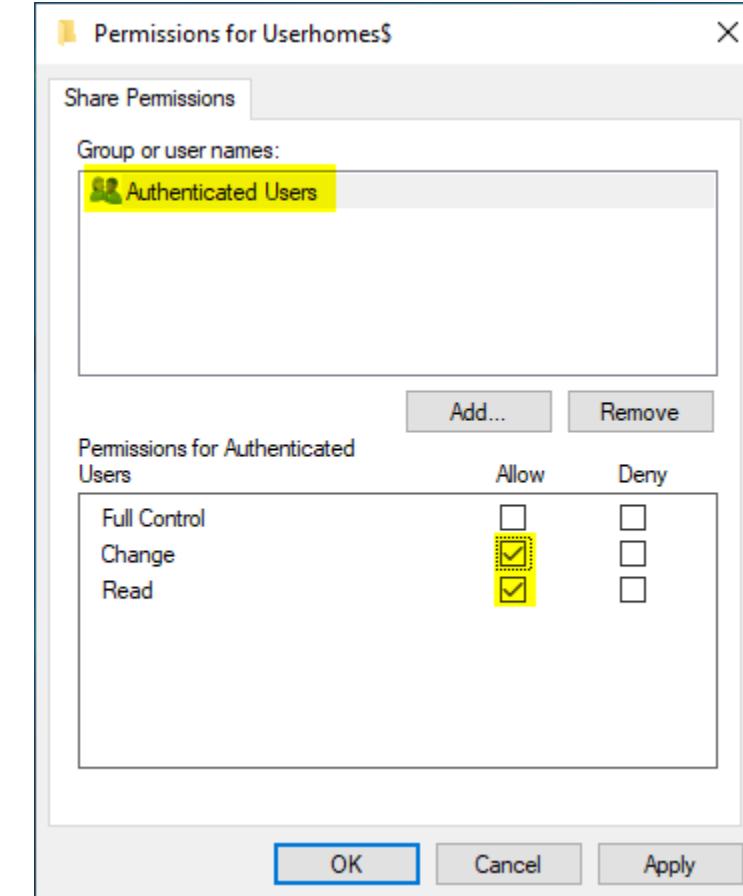
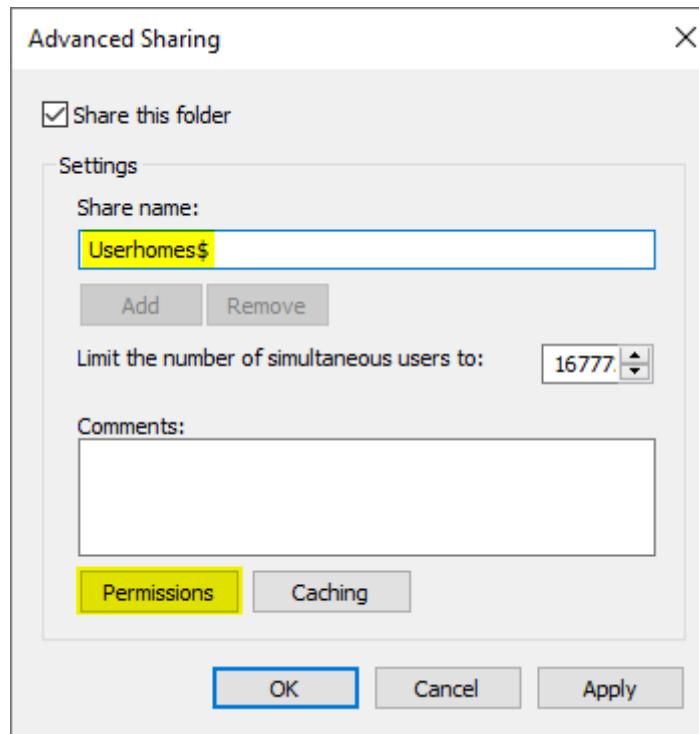
- VM Einstellungen VmWS1 Festplatte hinzfügen.
- Auf dem Server VmWS1 muss die zweite Festplatte im Disk Management Online geschaltet, initialisiert (GPT) und anschliessend NTFS formatiert werden.
- Windows + R diskmgmt.msc
- Optionen
  - Laufwerk: E
  - Volume Name: Daten
  - NTFS



- Auf dem Laufwerk E die Ordnern Struktur anlegen:
  - C:\Userdaten\Userhomes
  - C:\Userdaten\Userprofiles
- Der Ordner Userhomes muss als erste Freigegeben werden.



## VmWS1 Userhome Konfiguration



- Nun fehlt noch die NTFS Berechtigung.
- Berechtigung nach dies Artikel umsetzt
  - [NTFS permissions for Redirected Folders \(or Home Directories\) | Microsoft Docs](#)
    - CREATOR OWNER - Full Control (Apply onto: Subfolders and Files Only)
    - System - Full Control (Apply onto: This Folder, Subfolders and Files)
    - Domain Admins - Full Control (Apply onto: This Folder, Subfolders and Files)
    - Everyone - Create Folder/Append Data (Apply onto: This Folder Only)
    - Everyone - List Folder/Read Data (Apply onto: This Folder Only)
    - Everyone - Read Attributes (Apply onto: This Folder Only)
    - Everyone - Traverse Folder/Execute File (Apply onto: This Folder Only)
  - Vererbung deaktivieren und alle unnötigen Rechte entfernen.

| Type  | Principal                        | Access       | Inherited from | Applies to                        |
|-------|----------------------------------|--------------|----------------|-----------------------------------|
| Allow | Administrators (SRVFP\Admini...) | Full control | None           | This folder, subfolders and files |
| Allow | SYSTEM                           | Full control | None           | This folder, subfolders and files |
| Allow | Authenticated Users              | Special      | None           | This folder only                  |

## ■ C:\Userdaten\Userprofiles

- Freigeben
- Berechtigung gemäss folgenden Artikels festlegen:
  - <https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-roaming-user-profiles>
    - System - Full control (Apply onto: This folder, subfolders and files)
    - Administrators - Full Control (Apply onto: This folder only)
    - Creator/Owner - Full Control (Apply onto: Subfolders and files only)
    - Authenticated Users - List folder / read data (Advanced permissions) Create folders / append data (Advanced permissions) (Apply onto: This folder only)

| Type  | Principal                        | Access       | Inherited from | Applies to                        |
|-------|----------------------------------|--------------|----------------|-----------------------------------|
| Allow | Administrators (SRVFP\Admini...) | Full control | None           | This folder, subfolders and files |
| Allow | CREATOR OWNER                    | Full control | None           | Subfolders and files only         |
| Allow | SYSTEM                           | Full control | None           | This folder, subfolders and files |
| Allow | Authenticated Users              | Special      | None           | This folder, subfolders and files |

- Am besten erfolgt der Zugriff via DC
  - [\\VmWS1\userhomes\\$](\\VmWS1\userhomes$)
  - <\\VmWS1\Userprofiles>

## Userhomes und Profil konfigurieren

- \\VmWS1\userprofiles%\username%
- \\VmWS1\userhomes\$\%\username%
- Umgebungsvariablen verwenden der Username wird automatisch eingefügt nach dem drücken von OK oder Apply
- Anschliessend mit dem User auf dem Client Anmelden

