Aufgabe 29.01.25

Teil 1

1. Erkläre möglichst umfassend: Was verstehst du unter einem DHCP-Server?

Der DHCP-Server spielt eine zentrale Rolle in der Netzwerkinfrastruktur, indem er die Konfiguration von Clients automatisiert und somit die Administration von Netzwerken erheblich vereinfacht.
Ein DHCP Server kann ein Netzwerkgerät (Hardware) oder auch eine Software lösung sein ,
die für die automatische Konfiguration von Netzwerkkommunikationsparametern für Clients zuständig ist

- Automatische IP-Adresse Zuweisung: Der DHCP-Server stellt IP-Adressen für Clients bereit, die sich im Netzwerk befinden. Diese Zuweisung erfolgt dynamisch, was bedeutet, dass die Clients nicht manuell konfiguriert werden müssen.

- Weitere Konfigurationsparameter: Neben der IP-Adresse können auch andere wichtige Netzwerkkonfigurationen wie Subnetzmaske, Gateway und DNS-Serveradressen automatisch von dem DHCP-Server bereitgestellt werden.

- DORA-Prozess: Die Kommunikation zwischen Client und DHCP-Server erfolgt über den sog. DORA-Prozess (Discover, Offer, Request, Acknowledge). In diesem Vier-Schritte-Prozess sendet der Client eine Anfrage an den DHCP-Server, der dann eine IP-Adresse und andere Konfigurationsdaten anbietet und bestätigt.

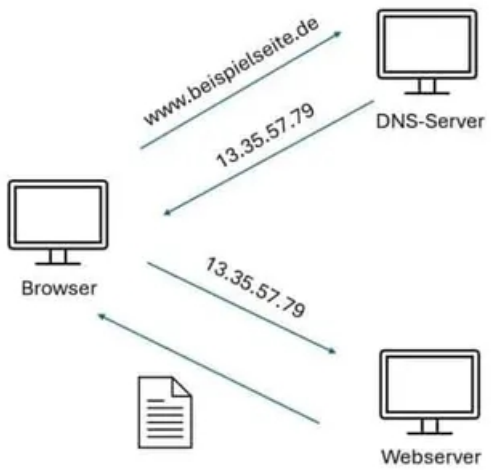
- Ausschlussbereiche: Der DHCP-Server kann bestimmte IP-Adressbereiche ausschließen, um sicherzustellen, dass statisch zugewiesene IP-Adressen nicht von ihm überschrieben werden.

- Reservierungen: Es ist möglich, spezifische IP-Adressen für bestimmte Geräte zu reservieren, sodass diese immer dieselbe IP-Adresse erhalten.

- Sicherheitsaspekte: Ein DHCP-Server kann potenziell zum Ziel von Angriffen werden, die dazu führen können, dass Clients ungültige Konfigurationen erhalten oder dass der Netzwerkverkehr manipuliert wird.

- DHCPv6: Für IPv6-Netzwerke gibt es eine erweiterte Version des Protokolls, DHCPv6, die zusätzliche Funktionen wie integrierte Sicherheitsfunktionen und die Möglichkeit bieten, weitere Konfigurationsdetails per DHCPv6 zu übertragen.

2. Erkläre: Was ist ein DNS- Server (FunkΘon, Auĩau, …)



Ein DNS-Server (Domain Name System)ist ein Server, der eine Verbindung zwischen einer Domain (zum Beispiel www.heise.de) und der zugehörigen IP-Adresse herstellt. Diese Funktion ist vergleichbar mit einem klassischen Telefonbuch , das Domainnamen in IP-Adressen umwandelt und umgekehrt.

Der DNS-Prozess beginnt, wenn wir eine URL in einem Browser eingibt. Die Anfrage wird an einen DNS-Resolver gesendet, der in der Regel der DNS-Server des Internet Service Providers (ISP) ist.
Der Resolver leitet die Anfrage an verschiedene DNS-Server weiter, bis die IP-Adresse der angefragten Domain gefunden wird.
Diese IP-Adresse wird dann an den Browser zurückgesendet, sodass dieser die Anfrage an den richtigen Server richten kann

Es gibt verschiedene Arten von DNS-Servern:

- Autoritative DNS-Server: Speichern gesicherte Domain-Informationen über eine bestimmte Zone im Domain-Namen-Space in ihrer DNS-Datenbank. Für jede Zone gibt es mindestens einen solchen Server, der als Master-System fungiert, während weitere als Slave-Systeme fungieren, um Redundanz und Ausfallsicherheit zu gewährleisten.
- Nicht-autoritative DNS-Server: Nutzen DNS-Informationen nicht aus der eigenen Zonendatei, sondern aus zweiter oder dritter Hand, wenn sie die Anfrage nicht direkt beantworten können.

DNS-Server bieten verschiedene Funktionen, wie z.B. die Sicherheit von Netzwerken durch die Gewährleistung, dass nur autorisierte Benutzer auf bestimmte Ressourcen zugreifen können.

Ein DNS-Server hat zwei wichtige Zonen: die Forward-Zone und die Reverse-Zone.

Die Forward-Zone dient dazu, Domainnamen in IP-Adressen umzuwandeln. Sie enthält Informationen wie ‘A’-Records, die einem Domainnamen eine IPv4-Adresse zuweisen, und ‘AAAA’-Records, die einem Domainnamen eine IPv6-Adresse zuweisen.

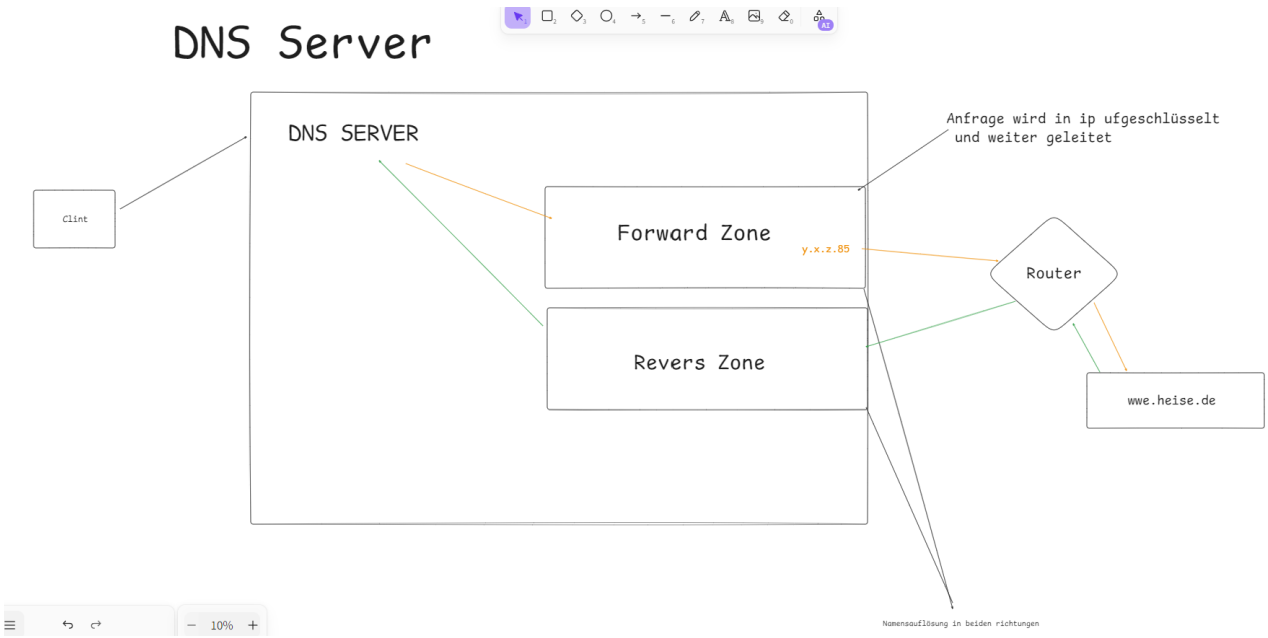
Diese Zonendatei wird auf einem Server gespeichert und enthält auch SOA- und NS-Records, die die Zone definieren und die Verknüpfungen zu anderen Nameservern realisieren.

Die Reverse-Zone dient dem umgekehrten Vorgang, also der Auflösung von IP-Adressen in Domainnamen.

Sie verwendet ‘PTR’-Records, die einer IP-Adresse einen Domainnamen zuordnen.

Diese Zonendatei enthält ebenfalls SOA- und NS-Records, ähnlich wie die Forward-Zone.

Beide Zonen können auf demselben Server gehostet werden oder auf separaten Servern, je nach Bedarf und Architektur des eigenen Netzwerks.



Funktion eines DNS-Servers

Ablauf einer DNS-Anfrage:

1. Nutzer gibt eine URL ein (z. B. Www.heise.com).
2. Der Client fragt den DNS-Resolver (oft der DNS-Server des Internetanbieters),
ob er die IP-Adresse kennt.
3. Falls die Adresse nicht im Cache ist, wird die Anfrage an andere DNS-Server weitergeleitet:
Root-Nameserver → Kennt nur die Top-Level-Domain (.com, .de usw.)
TLD-Nameserver (.com-Server) → Verweist auf den zuständigen Nameserver der Domain
Autoritativer Nameserver (google.com-Server) → Gibt die tatsächliche IP-Adresse zurück
4. Der DNS-Resolver speichert die IP-Adresse für zukünftige Anfragen und
gibt sie an den Client weiter.
5. Der Browser verbindet sich mit der IP-Adresse, und die Webseite wird geladen.

3. Was ist (Microsoft) Active Directory?

Active Directory (AD) ist ein Verzeichnisdienst von Microsoft,
der in Windows Server-Umgebungen genutzt wird, um Benutzer, Computer, Gruppen, Geräte und Ressourcen innerhalb eines Netzwerks zentral zu
verwalten und zu organisieren.

Es dient als eine Art Datenbank und Steuerungssystem,
mit dem Administratoren Berechtigungen vergeben,
Gruppenrichtlinien durchsetzen und Zugriffe auf Netzwerkressourcen steuern können.

Funktionen von Active Directory

- Benutzer- und Gruppenverwaltung
Benutzerkonten verwalten (Anlegen, Ändern, Deaktivieren, Löschen)

Gruppen erstellen und Berechtigungen zentral steuern

- Zentrale Authentifizierung und Autorisierung

  Single Sign-On (SSO) → Ein Benutzer muss sich nur einmal anmelden und

  erhält Zugriff auf mehrere Ressourcen

  Passwortverwaltung und MFA (Multi-Faktor-Authentifizierung) möglich
- Gruppenrichtlinien (Group Policy Objects, GPOs)

  Regeln für Computer und Benutzer durchsetzen (z. B. Passwortrichtlinien,

  Softwareeinschränkungen, Netzlaufwerke, Druckerzuweisungen)
- Netzwerkressourcen organisieren

  Zugriff auf Freigaben, Drucker, Ordner, Anwendungen und

  andere Ressourcen regeln Rechteverwaltung für Dateien und Ordner
- Domänenstruktur & Hierarchie

  Ermöglicht die Verwaltung mehrerer Standorte und Netzwerke mit einer zentralen Struktur

Komponenten von Active Directory

- Active Directory Domain Services (AD DS)

  Herzstück von Active Directory

  Ermöglicht die Verwaltung und Authentifizierung von Benutzern und

  Geräten in einer Domäne
- Domain Controller (DC)

  Der Hauptserver in einer AD-Umgebung

  Speichert alle AD-Daten, authentifiziert Benutzer und verwaltet Gruppenrichtlinien
- LDAP (Lightweight Directory Access Protocol)

  Ein Protokoll, mit dem AD mit anderen Systemen (z. B. Linux) kommunizieren kann
- Kerberos & NTLM – Authentifizierungsmechanismen

  Kerberos: Sichere Authentifizierungsmethode für Windows-Netzwerke

  NTLM: Älteres, aber immer noch genutztes Protokoll für

Anmeldevorgänge

- FSMO-Rollen (Flexible Single Master Operations)
  Bestimmte Server (Domain Controller) übernehmen kritische Rollen, z. B. Schema-Master,
  um Änderungen im AD durchzuführen

Vorteile von Active Directory

Zentrale Benutzerverwaltung -> Keine lokale Benutzerverwaltung auf jedem
einzelnen Rechner nötig
Single Sign-On (SSO) -> Benutzer müssen sich nur einmal anmelden
Erhöhte Sicherheit -> Durch Gruppenrichtlinien, MFA und Berechtigungsmanagement
Einfache Skalierbarkeit -> Neue Benutzer, Computer oder
Ressourcen lassen sich einfach hinzufügen
Kompatibilität mit Cloud (Azure AD)

4. Liste einige Befehle auf, um Netzwerk-Troubleshooting vornehmen zu können und erkläre sie.

ping 8.8.8.8
Sendet ICMP-Pakete (Echo-Request) an eine Ziel-IP oder Domain.
Prüft, ob das Gerät oder die Webseite erreichbar ist.
Misst die Antwortzeit (Latenz).

traceroute 8.8.8.8 (Unix) bzw. tracert 8.8.8.8 (Windows)
Zeigt alle Knotenpunkte (Hops) zwischen deinem Computer und dem Zielserver.
Misst die Zeit für jeden Hop.
Hilft herauszufinden, wo genau ein Verbindungsproblem besteht.

ifconfig (Unix) bzw. ifconfig (Windows)
Zeigt die aktuelle IP-Adresse, Subnetzmaske, Gateway und DNS-

Server.
Hilft bei der Fehleranalyse, ob der PC eine korrekte IP-Adresse hat.

nslookup google.com
Fragt den DNS-Server nach der IP-Adresse eines Domain-Namens.
Hilft zu prüfen, ob das DNS korrekt arbeitet.

netstat -an
Zeigt aktive Verbindungen, offene Ports und welche Programme sie nutzen.
Nützlich, um versteckte Verbindungen oder Malware zu finden.

arp
Zeigt die MAC-Adressen der verbundenen Geräte in deinem Netzwerk.
Nützlich, um zu prüfen, ob sich unbekannte Geräte im Netzwerk befinden.

route print
Zeigt die aktuelle Routing-Tabelle, die festlegt, wie Datenpakete durch das Netzwerk gehen.

telnet google.com 80
Prüft, ob eine Verbindung zu einer bestimmten IP und einem bestimmten Port möglich ist.

Teil2.

✅ 1. Sichere deine bisherige Arbeit in HyperV durch Export der Windows Client- und der Server Maschine.

✅ 2. Lösche diese beiden Maschinen in HyperV. Achte darauf, die virtuellen PlaΣen der Maschinen ebenfalls zu löschen (um Platz auf der HD frei zu geben).

✅ 3. Lösche sämtliche, bisher angelegten, virtuellen Switche.

✅ 4. Ziel ist es ein funktionierendes AD aufzusetzen. Überlege dir die Vorgehensweise und schreibe diese Punkte auf.

Ich überlege mir welchen Sicherheitkonzept ich folgen möchte in meinem Fall bevorzugt „Traue Niemanden“

Traue Niemanden (Zero Trust): ist ein Sicherheitsmodell, das davon ausgeht, dass kein Benutzer oder Gerät automatisch als vertrauenswürdig angesehen wird

Um Ein AD aufzusetzen mache ich mir vorher Gedanken welche Struktur und aufbaue dieses folgen soll (Forest ist die Gesamtstruktur) wie ich mein Unternehmen am besten in der Ad Abbilden kann .

-Gruppen für Einzelne Abteilungen (vertrieb, verkauf, inbount,……..)

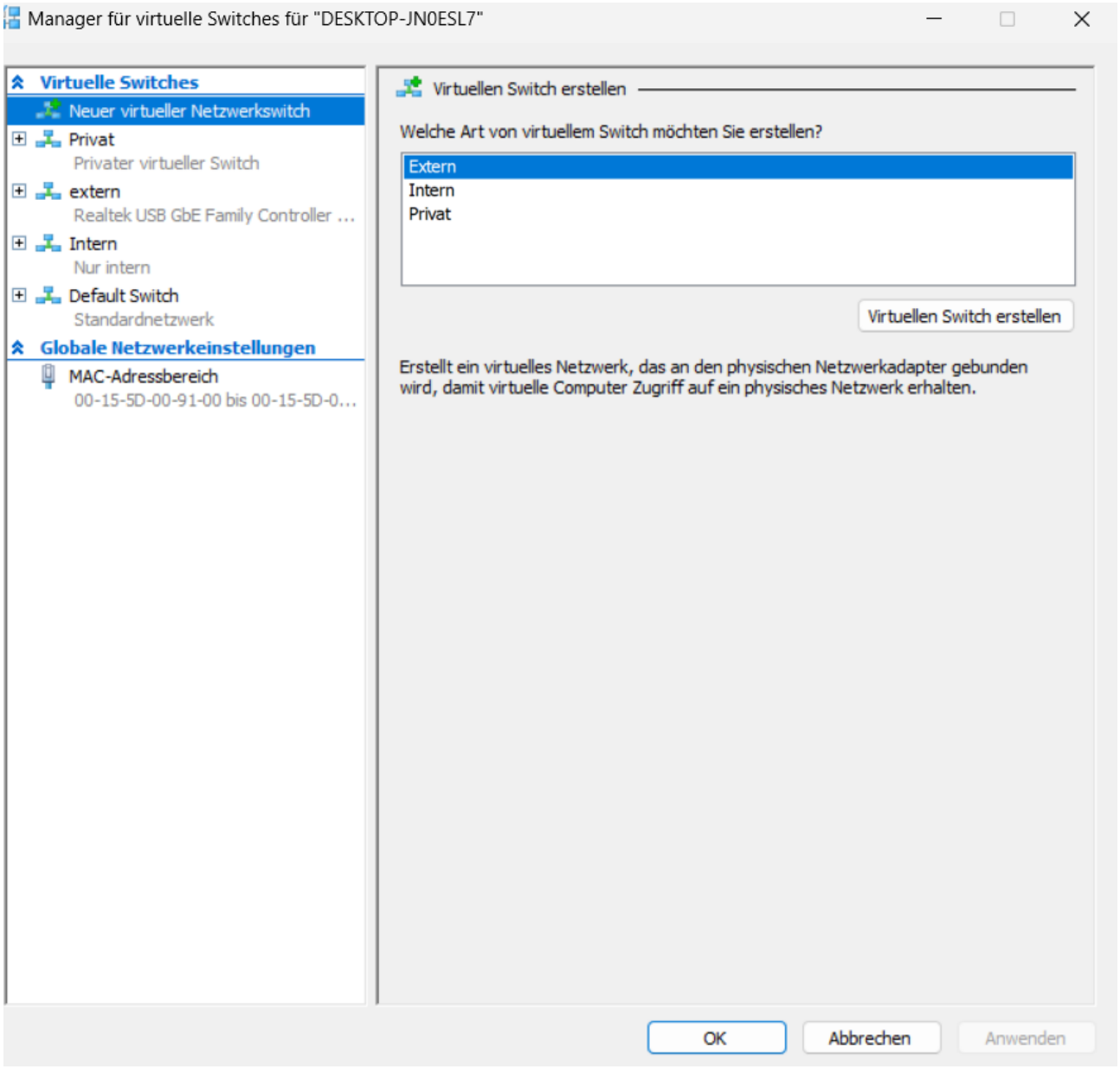
-Gruppen für Verschiedene Positionen (Abteilungsleiter ,Gruppenleiter, anderes Führungspersonal ect)

Dann mache ich mir Gedanken welche Rechte zugriffe Privilegien die jeweiligen Gruppen benötigen um ihre Aufgabe beweltigen zu können und verteile. So wenige Berechtigungen wie möglich So viele wie nötig.

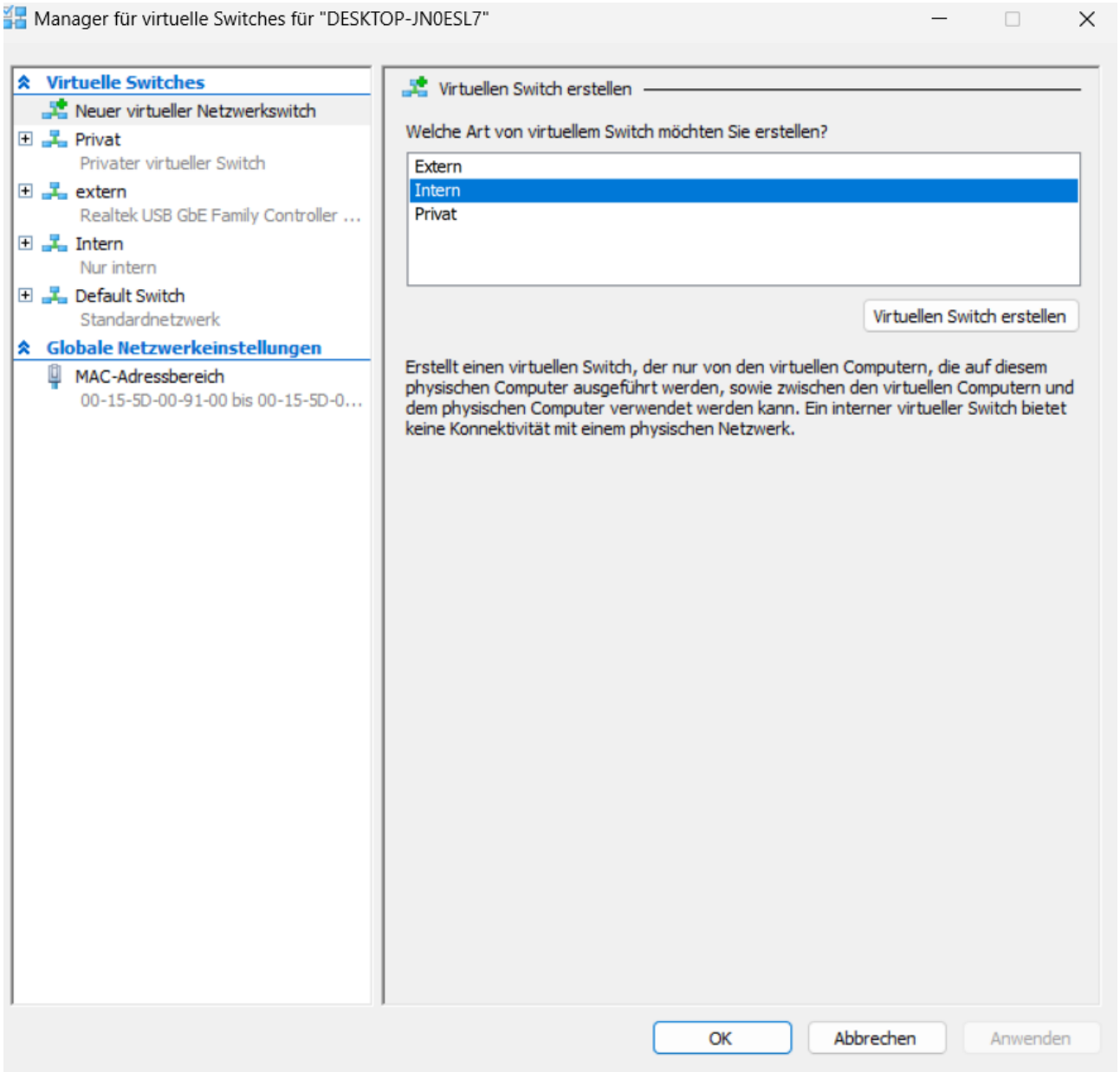
Wenn ich mir die Gedanken dazu gemacht habe und festgehalten habe beginne ich erst dieses dann am Gerät umzusetzen.

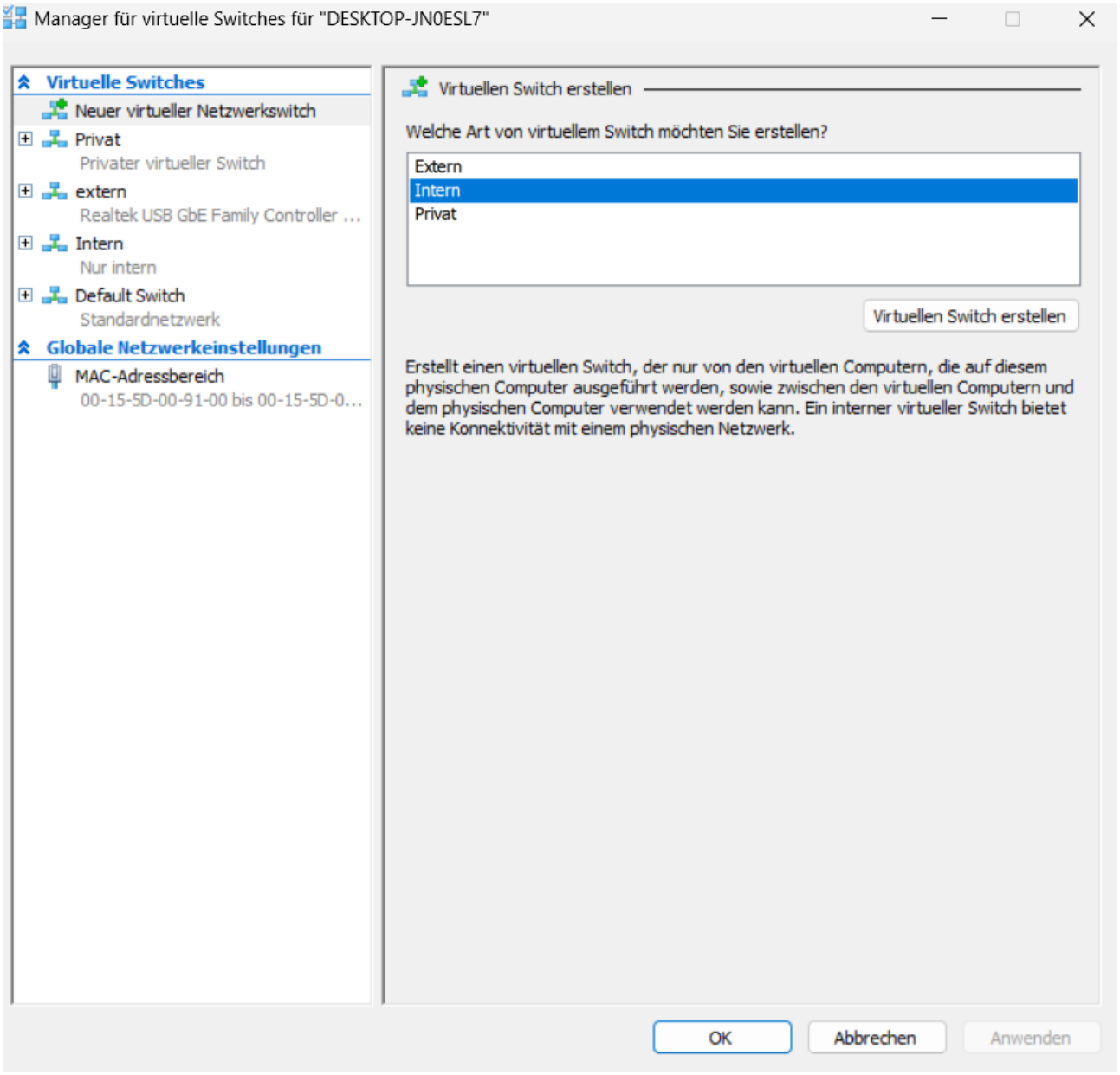
5. Erkläre den Unterschied zwischen internen, privaten, externen und Default Switcch in HyperV.

Extern Switch kann auf die vom Host Physisch realen Netzwerkadaptern zu greifen und so auch mit dem Internet agieren . Nach außen kommunizieren

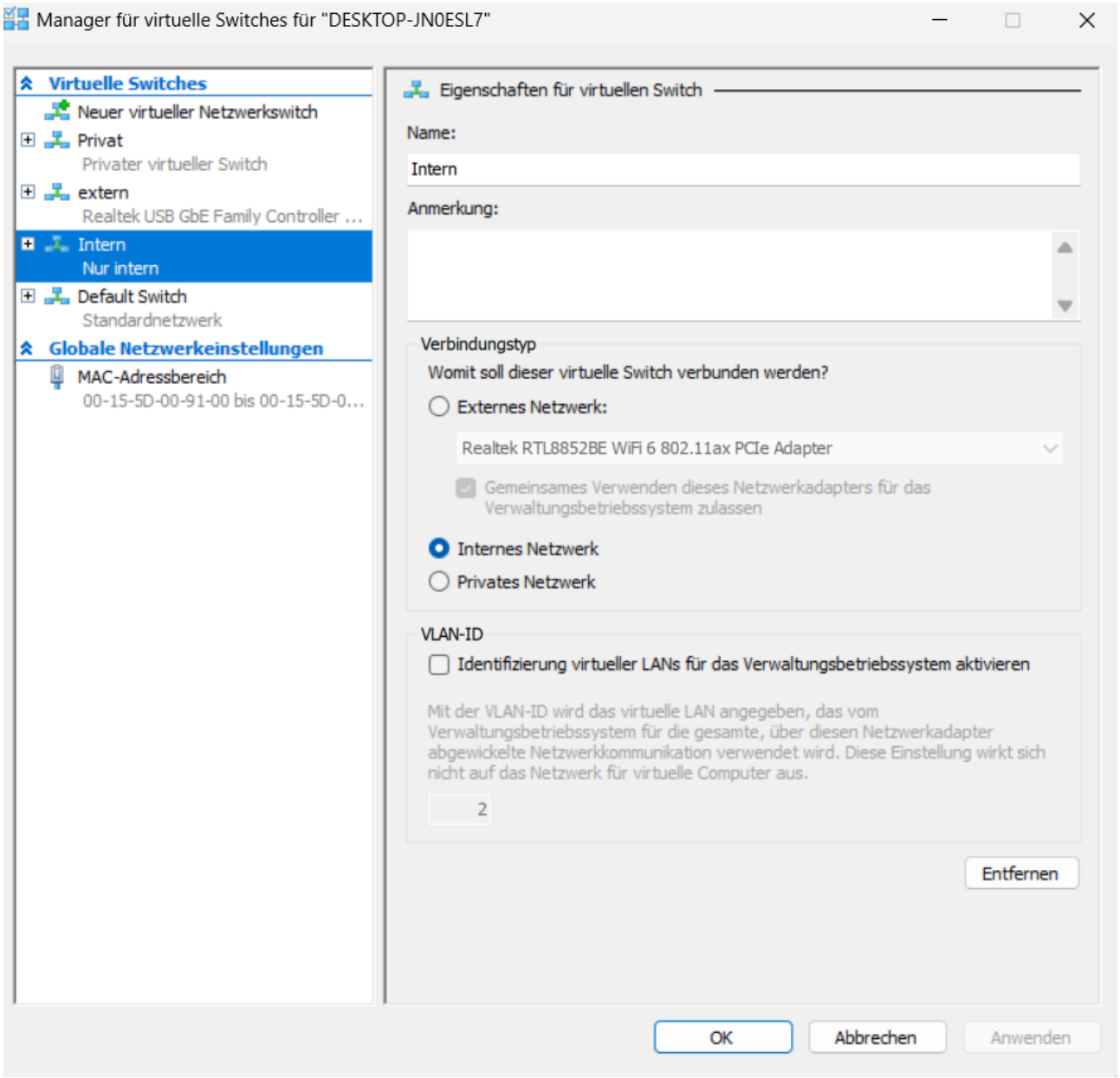


Kann nur unter den Vms untereinander die auf dem Host zur Verfügung stehen kommunizieren

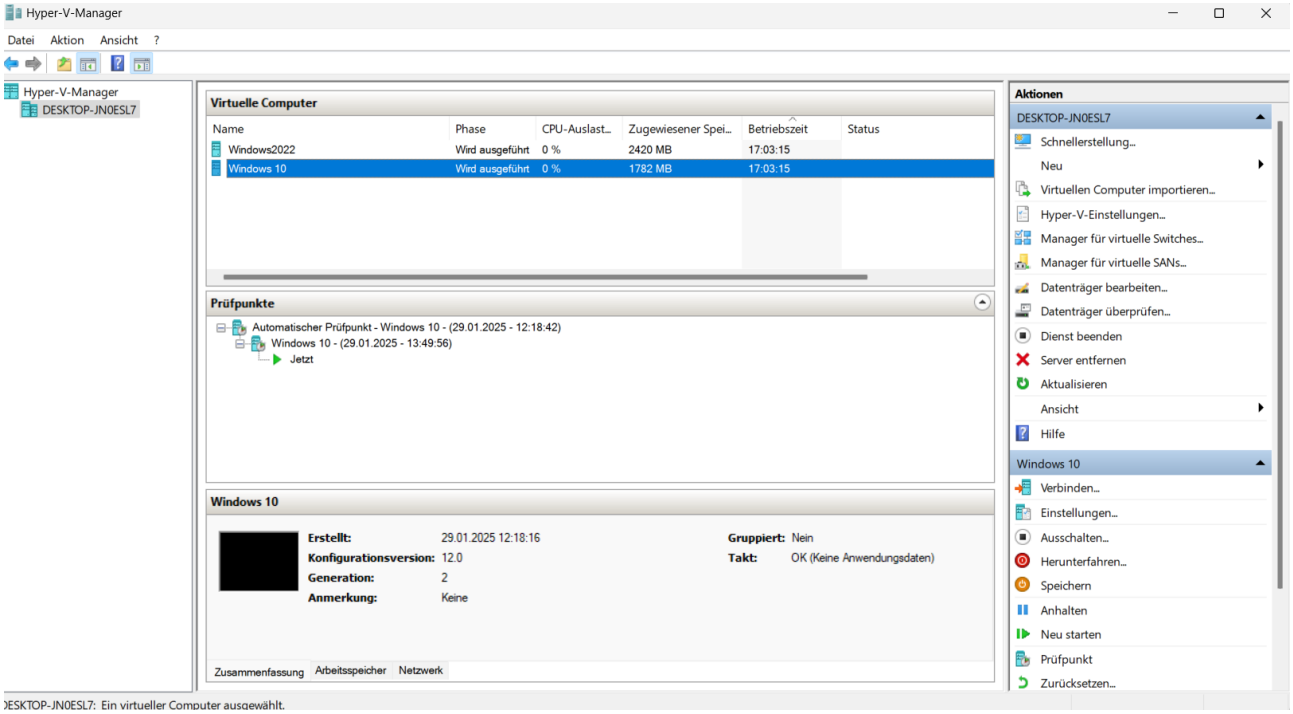



Manager für virtuelle Switches für "DESKTOP-JN0ESL7"
Virtuelle Switches
Neuer virtueller Netzwerkswitch
Privat
Privater virtueller Switch
extern
Realtek USB GbE Family Controller ...
Intern
Nur intern
Default Switch
Standardnetzwerk
Globale Netzwerkeinstellungen
MAC-Adressbereich
00-15-5D-00-91-00 bis 00-15-5D-0...
Virtuellen Switch erstellen
Welche Art von virtuellem Switch möchten Sie erstellen?
Extern
Intern
Privat
Virtuellen Switch erstellen
Erstellt einen virtuellen Switch, der nur von den virtuellen Computern, die auf diesem physischen Computer ausgeführt werden, sowie zwischen den virtuellen Computern und dem physischen Computer verwendet werden kann. Ein interner virtueller Switch bietet keine Konnektivität mit einem physischen Netzwerk.
OK
Abbrechen
Anwenden

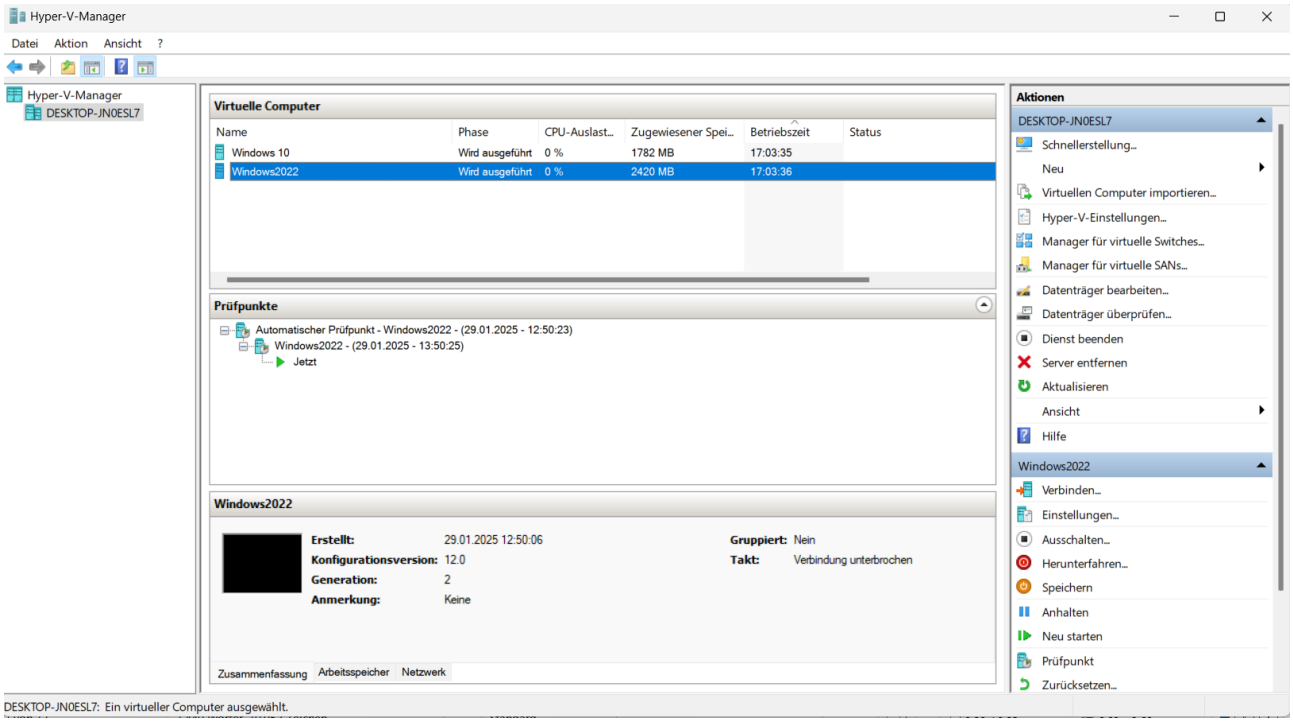
6. Konfiguriere, falls notwendig, im HyperV den oder die erforderlichen Netzwerkeinstellungen. (Im virtual Switch Manager.)



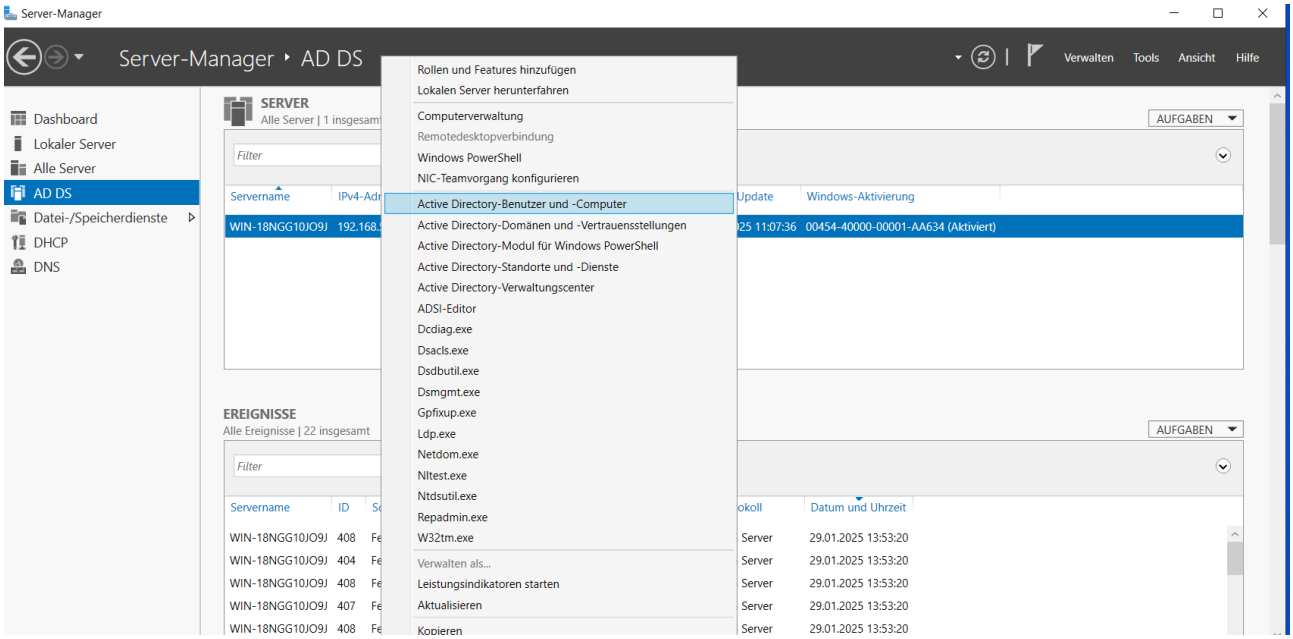
7. Installiere eine Windows 10 Maschine (in HyperV).

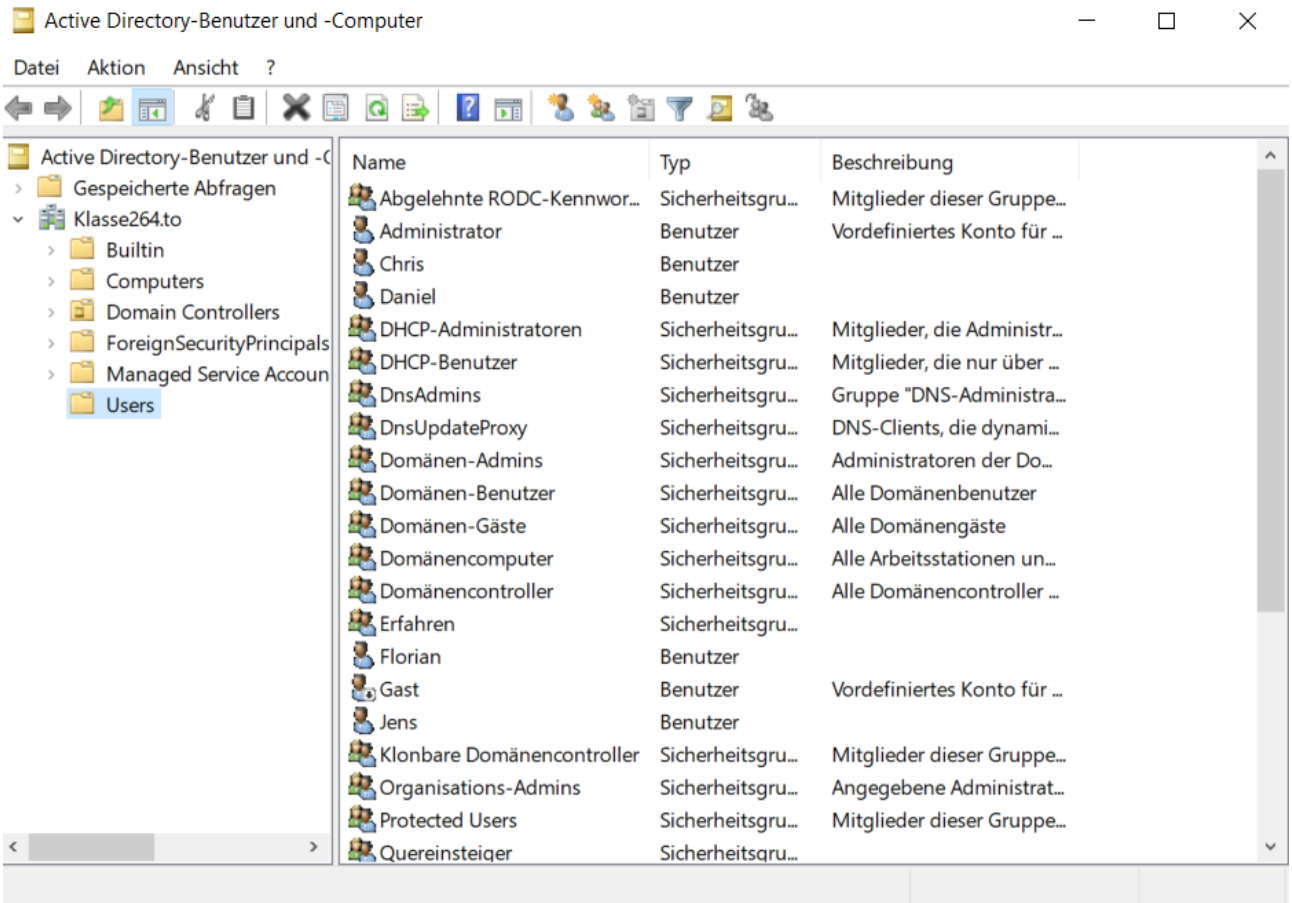


8. Installiere Den Win2022- Server (in HyperV).



9. Erstelle auf dem Server ein AD (Vorgehensweise dokumentieren).





Um eine Ad zu erstellen gehen wir wie folgt vor :

Voraussetzungen schaffen :

Windows Server 2022 ist installiert und läuft.
Der Server ist Teil eines Netzwerks, idealerweise mit einer statischen IP-Adresse.
Ein Administrator-Konto, um die Installation und Konfiguration durchzuführen.

Schritt-für-Schritt-Anleitung:

1. Server Manager öffnen

Melde dich mit einem Administrator-Konto an.
Öffne den Server-Manager, der standardmäßig beim Start angezeigt wird. Falls er nicht angezeigt wird, klicke auf das Startmenü und wähle „Server-Manager“.

2. Active Directory Domain Services installieren

Klicke im Server-Manager auf Verwalten (Manage) und dann auf Rollen und Features hinzufügen (Add Roles and Features).

Der Assistent für Rollen und Features öffnet sich. Klicke auf Weiter.

Wähle den Installations-Typ „Rollenbasierte oder featurebasierte Installation“ aus und klicke auf Weiter.

Wähle den Server aus, auf dem du AD installieren möchtest, und klicke auf Weiter.

Rollen auswählen:

Im Abschnitt „Rollen auswählen“ wählst du die Rolle Active Directory Domain Services (AD DS) aus. Ein Dialogfeld erscheint, in dem du zur Bestätigung die erforderlichen Features hinzufügst. Klicke auf Hinzufügen und dann auf Weiter.

Features auswählen:

Es sind keine zusätzlichen Features erforderlich, klicke also auf Weiter.

Bestätigung der Auswahl:

Überprüfe deine Auswahl und klicke dann auf Installieren. Der Installationsprozess wird gestartet. Nach Abschluss der Installation klickst du auf Schließen.

3. Active Directory Domain Services konfigurieren

Nach der Installation der Rolle Active Directory Domain Services erscheint im Server-Manager eine Warnung, die besagt, dass die Konfiguration für AD DS noch aussteht. Klicke auf den Hinweis und dann auf Dienste konfigurieren.

Domänencontroller konfigurieren:

Der Assistent für Active Directory-Domänenservices öffnet sich. Klicke auf Neuen Forest erstellen (wenn es sich um eine neue Domäne handelt).
Gib den Vollqualifizierten Domänennamen (FQDN) der Domäne ein, z. B. meinedomain.local.
Klicke auf Weiter.

Wald- und Domänenfunkversionen auswählen:

Wähle die Versionen für den Wald und die Domäne aus. .Klicke auf Weiter.

Verzeichnisdienstdatenbank und Logdateien speichern:

Standardmäßig werden die Datenbank, die Protokolldateien und die SYSVOL-Daten an vordefinierten Orten gespeichert. Du kannst die Pfade anpassen, wenn nötig.
Klicke auf Weiter.

Wechselseitige Authentifizierung (DNS) konfigurieren:

Wenn du das DNS ebenfalls auf diesem Server verwenden möchtest, wähle die Option aus, um den DNS-Server zu installieren. Diese Option wird vom Server Manager automatisch empfohlen.
Klicke auf Weiter.

Netzwerkschutz und Verzeichniswiederherstellung:

Vergib ein Passwort für den Verzeichniswiederherstellungsmodus (DSRM). Dies ist wichtig, falls du das Active Directory manuell wiederherstellen musst.
Klicke auf Weiter.

Überprüfen und Konfigurieren:

Der Assistent zeigt eine Zusammenfassung aller vorgenommenen Konfigurationen. Überprüfe diese und klicke dann auf Installieren.

4. Server neu starten

Nach Abschluss der Konfiguration wird der Server automatisch neu gestartet, um die Änderungen zu übernehmen und als Domänencontroller zu fungieren.

5. Anmeldung an der Domäne

Nachdem der Server neu gestartet ist, kannst du dich mit einem Administrator-Konto an der neu erstellten Domäne anmelden.
Klicke dazu auf Start, dann auf Abmelden und wähle beim erneuten Anmelden die Domäne aus.

6. Überprüfung der Installation

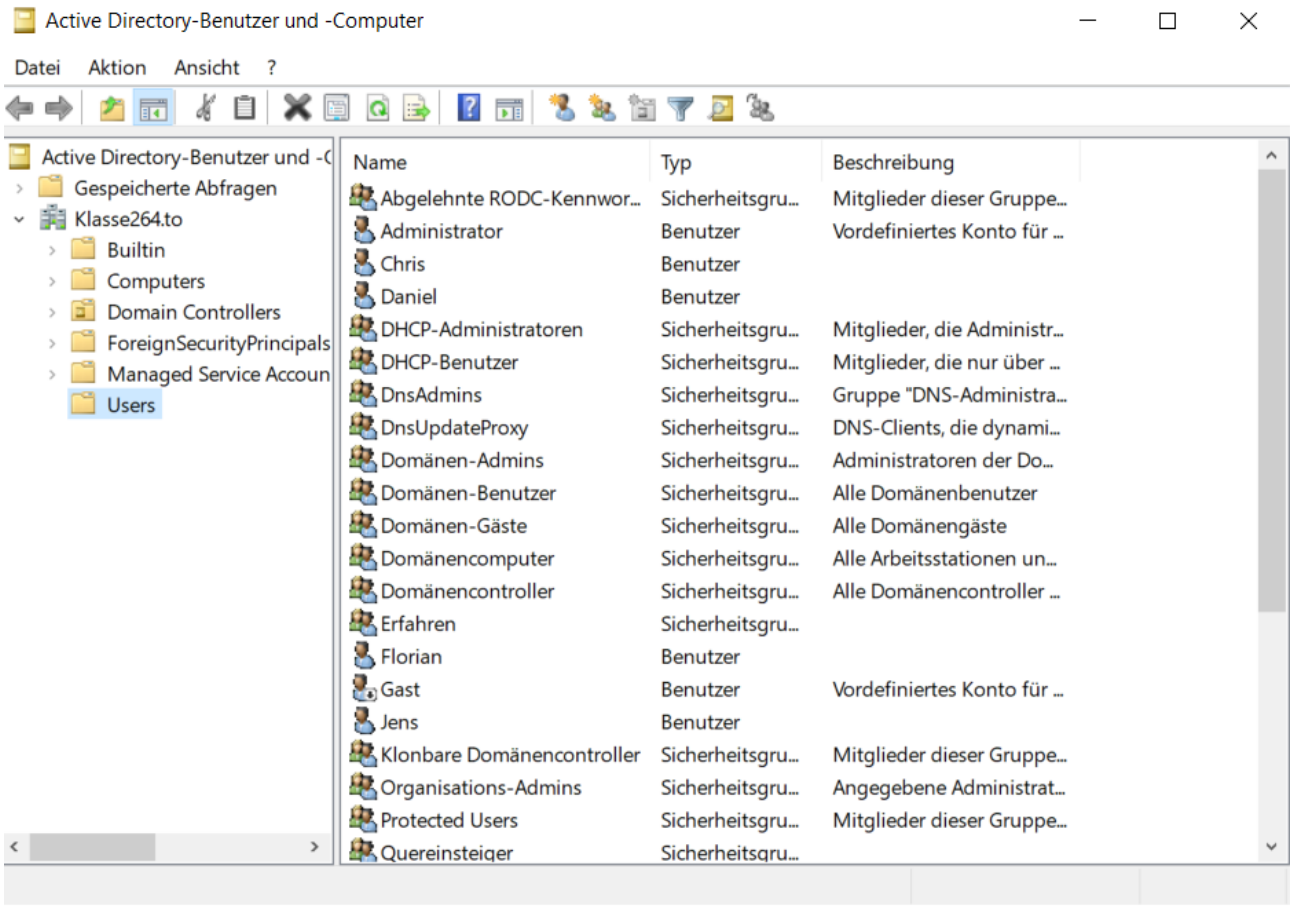
Um sicherzustellen, dass der Active Directory-Domänencontroller ordnungsgemäß funktioniert, öffne die Active Directory-Benutzer und -Computer Konsole:
Öffne dazu den Server-Manager, klicke auf Tools und wähle Active Directory-Benutzer und -Computer aus.
Hier kannst du Benutzer, Gruppen und andere AD-Objekte verwalten.

7. DNS überprüfen

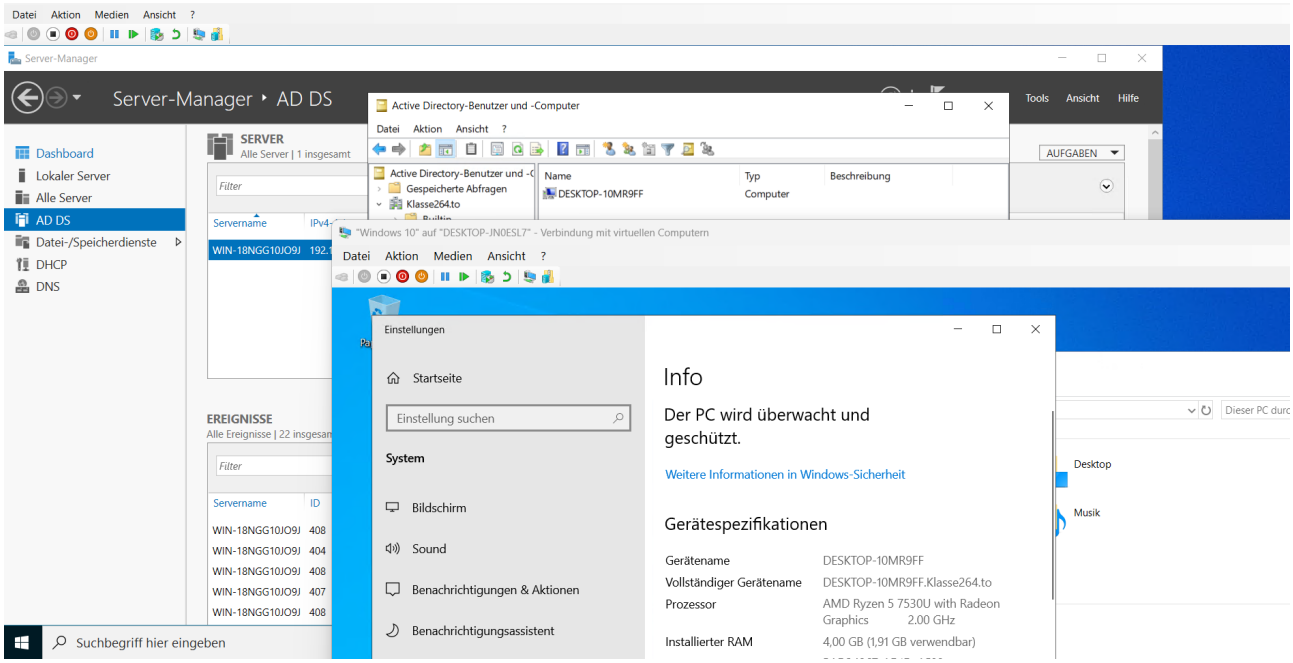
Stelle sicher, dass der DNS-Server korrekt konfiguriert ist, da Active Directory stark vom DNS abhängt. Überprüfe die DNS-Einstellungen und die Namensauflösung, indem du den Befehl nslookup verwendest.

---

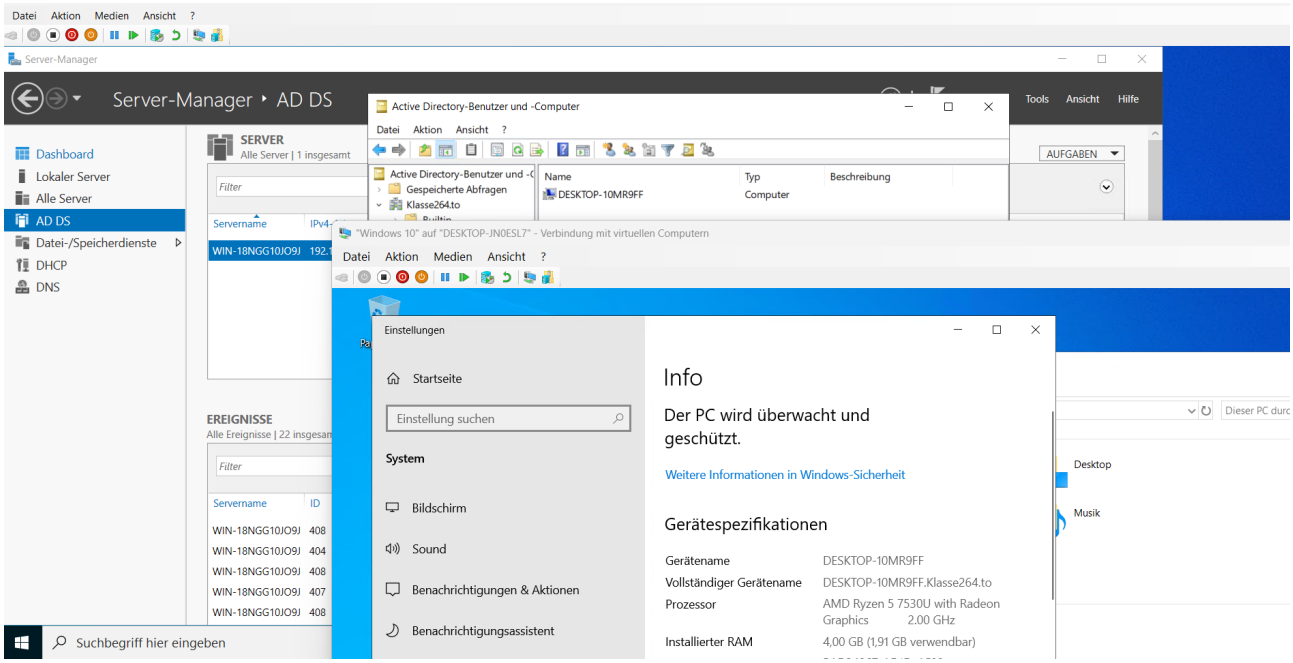
10. Richte im AD einige Benutzer ein.



11. Binde den Win10- Client in die Domäne ein.



12. Teste nun, ob die eingerichteten Benutzer sich vom Win10- Client am DC anmelden können.


Server-Manager
Server-Manager ‣ AD DS
Tools
Ansicht
Hilfe
Dashboard
Lokaler Server
Alle Server
AD DS
Datei-/Speicherdienste
DHCP
DNS
SERVER
Alle Server | 1 insgesamt
Filter
Servername
WIN-18NGG10JO9J
AUFGABEN
EREIGNISSE
Alle Ereignisse | 22 insgesamt
ID
408
404
408
407
408
Active Directory-Benutzer und -Computer
Datei Aktion Ansicht ?
Gespeicherte Abfragen
Klasse264.to
Name
Typ
Beschreibung
DESKTOP-10MR9FF
Computer
"Windows 10" auf "DESKTOP-JN0ESL7" - Verbindung mit virtuellen Computern
Datei Aktion Medien Ansicht ?
Einstellungen
Startseite
Einstellung suchen
System
Bildschirm
Sound
Benachrichtigungen & Aktionen
Benachrichtigungsassistent
Info
Der PC wird überwacht und geschützt.
Weitere Informationen in Windows-Sicherheit
Gerätespezifikationen
Gerätename
DESKTOP-10MR9FF
Vollständiger Gerätename
DESKTOP-10MR9FF.Klasse264.to
Prozessor
AMD Ryzen 5 7530U with Radeon Graphics 2.00 GHz
Installierter RAM
4,00 GB (1,91 GB verwendbar)
Desktop
Musik
Suchbegriff hier eingeben