### - Active Directory einrichten. (Primärer Domain-Controller)

Hier mal eine Kurzanleitung, wie man einen Windows Server 2025 zu einem Primären Domain-Controller einrichtet, ohne GUI.

Ja - Ich weiß - Es gibt viele, viele Meinungen dazu wie man das eine oder das andere anders machen kann. Fängt alleine schon bei dem Domänen-Namen an. Mit .local - oder ohne oder mit der Internet Domäne .de etc...

#### Feste IP-Adresse vergeben

Nach der Installation von Windows Server 2025 gebe ich diesem erst einmal eine feste IP-Adresse. Hier in dem Beispiel 192.168.43.150. Dazu ermittel ich erst mal den Index der Netzwerkkarte.

> Get-NetAdapter | Format-List

Zurück bekommt man den dann Index. Hier in dem Beispiel die 3.

: 3

InterfaceIndex

Jetzt setze ich den Server auf die IP-Adresse: 192.168.43.150 und den Standardgateway: 192.168.43.2 auf dem vorher ermittelten InterfaceIndex 3

> New-NetIPAddress -InterfaceIndex 3 -IPAddress 192.168.43.150 `
-AddressFamily IPv4 -PrefixLength 24 -DefaultGateway 192.168.43.2

### Rolle AD-Domain-Services installieren und aktivieren.

> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Nach der Installation können wir den DC-Controller dann final einrichten. Hierzu speichern wir uns erst wir erst mal ein DSRM-Passwort in eine Variable. **Hinweis:** Das DSRM Passwort ist nicht das Passwort vom Administrator. Aus Sicherheitsgründen sollte auch ein anderes vergeben werden. Das DSRM-Passwort wird nur im Wiederherstellungsmodus oder für Sicherungszwecke für Active Directory (AD) verwendet!

> \$dsrm = ConvertTo-SecureString "MeinPasswort" -asplaintext -force

Nun erstellen wir hier in den Beispiel die Domäne myNet.work. Dazu in einem Texteditor die Zeilen so anpassen wie man es benötigt und in der Powershell rein kopieren.



Jetzt wird quasi der Server zu einem primären Domänencontroller hochgestuft. Der Server wird dann automatisch neu gestartet. Der erste Start kann ein Weilchen dauern. (Sollte Powershell die Befehle nicht kennen, so muss man vorher die diese hinzufügen:)

> Import-Module ADDSDeployment

### - DNS einrichten

Jetzt installieren wir uns noch die DNS-Features, damit wir die DNS-Einstellungen auch alle bearbeiten können.

#### > Install-WindowsFeature DNS

Jetzt kann es nach der Installation gut sein, dass hier als DNS-Server die IPv6 Loopback Adresse ::1 angezeigt wird. Die ist vergleichbar mit der IPv4 Adresse: 127.0.0.1.

Bevor wir also uns eine eigen IP-Adresse für den DNS verteilen, lösche ich erst einmal alle Einträge um auf Nummer sicher zu gehen:

> Set-DnsClientServerAddress -InterfaceIndex 3 -ResetServerAddresses

Da der Server als DNS-Server fungiert, vergebe ich diesem auch die vorher festgelegten IP-Adrese 192.168.43.150. Da ich schon weiß, das ich einen Backup-Domänen Controller installiere, so gebe ich als zweit-DNS-Adresse auch gleich mit: 192.168.43.160. Dieser kann natürlich weggelassen werden, falls man diesen nicht benötigt.

> Set-DnsClientServerAddress -InterfaceIndex 3 `
-ServerAddresses ("192.168.43.150", "192.168.43.160")

Ich könnte jetzt alle Dienste manuell neu starten, aber ich starte einfach einmal neu.

> shutdown /r /t 0

### Zeit auflösen / PDC-Emulator.

Da ich später noch einen Backup-Domain-Controller installiere, sollte die Zeit immer korrekt sein. Generell mache ich diesen Schritt immer, da dieser sehr wichtig ist, das alle Geräte immer die selbe Zeit haben sollten.

Hier mal wichtig, da man meistens in der produktiven Umgebung andere Firewall-Lösungen hat, den UDP Port 123 frei zu geben. In der Windows Firewall ist das in der Regel nicht nötig. Sollte es doch Probleme geben, dann mal hier die beiden Befehle zum freigeben:

```
> New-NetFirewallRule -DisplayName "Zeitserver Rein UDP" -Direction Inbound `
-Protocol UDP -LocalPort 123 -Action Allow
> New-NetFirewallRule -DisplayName "Zeitserver Raus UDP" -Direction Outbound `
-Protocol UDP -LocalPort 123 -Action Allow
```

Jetzt geben wir unserm PDC mal einen externen Zeitserver zum synchronisieren.

> w32tm /config /update /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL /reliable:YES

Jetzt geben wir zwei Befehle ein, es erneut upzudaten und zu synchronisieren.

```
> w32tm /config /update
> w32tm /resync
```

#### **DNS konfigurieren.**

Ab jetzt können wir einen Client an die Domäne anbinden, der dann mit den Remote Server Administration Tools kurz RSAT zugreifen können.

Wie man einen Windows-Client in die Domäne bringt und die RSAT Tools installiert und einrichtet, habe ich im Anhang noch separat beschrieben.

Mit einer grafischen Oberfläche lässt sich es einfach komfortabler konfigurieren.

## - DNS einrichten

Verbindung mit DNS-Server herstellen X	Auf dem Clinet kann man jetzt über den Server-Manager > Tools oder über das
Der Windows-DNS-Server wird ausgeführt auf:	Programm Menü Windows-Tools auf das
O Diesem Computer	DNS-Tool zugreifen. Hier wählt man dann
O Folgendem Computer:	einfach den Servernamen um die Konfiguration
Serv25	durchzuführen.
Verbindung mit dem angegebenen Computer jetzt herstellen	
DNS     DNS     DNS     Serv25     DNS-Server konfigurieren	Damit die Namen/IP-Adressen auch außerhalb unserer Zone myNet.work
Eigenschaften i	dio Anfragon weitergoleitet werden
	Dazu erstellen wir einen forwarder
	Daza erstellen wir einen forwarder.
Debugprotokollierung Ereignisprotokollierung Überwachen Sicherheit	Mit der rechten Maustaste auf den
Schnittstellen Weiterleitungen Erweitert Stammhinweise	DNS Server / Eigenschaften.
	, j
102 100 42 100	Unter Weiterleitung steht jetzt bei mir
192.166.43.160 <autosung hicht="" möglich=""></autosung>	die IP-Adresse meines Backup-Domain-
Stammhinweise verwenden, wenn keine Bearbeiten	Controllers. Hier fügen wir aber noch
	die Standard-Gateway Adresse hinzu.
OK Abbrechen Übernehmen Hilfe	
	In vielen Fällen und kleineren

Netzwerken wird gerne die DNS Adresse von dem Router / fritz!Box (Beispiel 192.168.178.1) genommen. Hier ändere ich jetzt die Weiterleitung auf meinem Gateway 192.168.43.2

P-Adresse	Vollqualifizierter Domän	Überprüft	Löschen
<hier klicken,="" td="" ur<=""><td>n IP</td><td></td><td>Nach ober</td></hier>	n IP		Nach ober
192.168.43.2			

### Forward-Lookup-Zone

Wenn man den DNS-Service installiert, so konfiguriert das System in der Regel automatisch eine Forward-Lookup Zone. Hier wird ein angefragter Name in eine IP-Adresse aufgelöst.

-	DNS	_msdcs.myNet.work
~	Serv25	myNet.work
	> 🧮 Zwischengespeicherte Lookupvorgänge	
	> 📔 Forward-Lookupzonen	

Sollten keine Einträge vorhanden sein, so erstellt man sich hier eine neue Zone. Mit der rechten Maustaste auf Forward-Lookupzone > Neue Zone...

2	DNS			
~	Serv25			
	> 📋 Zwischenge	speicherte Loo	okupvorgänge	
	> 📔 Forward-Lo	okupzonen		
	> 🧮 Reverse-Loo	kupzonen	Neue Zone	
	Vertrauensn	inkte		2

### - DNS einrichten

Zone in Active Directory speiche Domänencontroller eingerichtet	ern (DNS-Server muss als schreibbarer sein)
	< Zurück Weiter > N Abbrecher
Wie sollen Zonendaten repliziert w	erden?
<ul> <li>Auf allen DNS-Servern, die auf werden: myNet.work</li> </ul>	Domänencontrollern in der Gesamtstruktur ausgeführt
<ul> <li>Auf allen DNS-Servern, die auf werden: myNet.work</li> </ul>	Domänencontrollern in dieser Domäne ausgeführt
<ul> <li>Auf allen Domänencontrollern ir myNet.work</li> </ul>	n dieser Domäne (Windows 2000-Kompatibilität):
O Auf allen Domänencontroller, di werden:	e im Bereich dieser Verzeichnispartition angegeben
Der Zonenname bestimmt den Teil o autorisierend ist. Normalerweise wi	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "peuezope microsoft.com") verwendet. Der
Der Zonenname bestimmt den Teil o autorisierend ist. Normalerweise wi oder ein Teil des Domänennamens Zonenname ist nicht der Name des	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers.
Der Zonenname bestimmt den Teil ( autorisierend ist, Normalerweise wi oder ein Teil des Domänennamens i Zonenname ist nicht der Name des Zonenname:	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers.
Der Zonenname bestimmt den Teil o autorisierend ist. Normalerweise wi oder ein Teil des Domänennamens i Zonenname ist nicht der Name des Zonenname: myNet.work	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers.
Der Zonenname bestimmt den Teil ( autorisierend ist, Normalerweise wi oder ein Teil des Domänennamens Zonenname ist nicht der Name des Zonenname: myNet.work	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers. < Zurück Weiter > Abbrecher
Der Zonenname bestimmt den Teil ( autorisierend ist. Normalerweise wi oder ein Teil des Domänennamens Zonenname ist nicht der Name des Zonenname: myNet.work	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers. < Zurück Weiter > Abbrecher ONS-Clientcomputern, sich zu registrieren und die nisch mit einem DNS-Server bei Änderungen zu
Der Zonenname bestimmt den Teil ( autorisierend ist. Normalerweise wi oder ein Teil des Domänennamens i Zonenname ist nicht der Name des Zonenname: myNet.work Dynamische Updates ermöglichen D eigenen Ressourceneinträge dynar aktualisieren.	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com" (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers.
Der Zonenname bestimmt den Teil ( autorisierend ist. Normalerweise wi oder ein Teil des Domänennamens : Zonenname ist nicht der Name des Zonenname: myNet.work Dynamische Updates ermöglichen D eigenen Ressourceneinträge dynar aktualisieren. Bestimmen Sie den Typ des dynami	des DNS-Namespaces, für den dieser Server rd der Firmendomänenname (wie z. B. "microsoft.com") (wie z. B. "neuezone.microsoft.com") verwendet. Der DNS-Servers.

Wir wollen die Zone ja auf dem aktuellen Server - hier Primäre Zone - erstellen.

Hier sollte die DNS Änderungen noch nicht über die Gruppenrichtlinien gesperrt worden sein.

In unserem Beispiel haben wir jetzt nur einen Firmensitz und wollen eh den DNS-Server auch nur für diesen verwenden.

Daher nehmen wir hier nicht die Gesamtstruktur, sondern "nur" unsere Domäne.

Und hoffentlich auch kein NT oder 2000 Netzwerk mehr.

Hier geben wir jetzt unsern Domänen-Namen ein. Man kann diesen auch anders benennen, aber hier würde ich den Domänen-Namen eingeben.

Im produktiven Bereich, sollten hier keine unsicheren Updates zugelassen werden.

Das manuell Update ist für eine fortgeschrittene Methode, was ich hier jetzt erst mal außen vor lasse. Und das war es dann auch schon. Nur noch Fertig stellen.

### **Revers-Lookup-Zone**

Auch hier gehen die Meinungen auseinander. Soll man auch einen IP-Adresse zu Hostnamen Auflösung machen. Warum nicht? Okay. In einem rein internen Netzwerk ist es wohl nicht notwendig. Aber in Hinblick auf Authentifizierungen (Kerberos) oder diverse Netzwerktools ist es schon von Vorteil.

Das Einrichten einer Revers-Lookup-Zone ist fast identisch wie vorher auch. Mit der rechten Maustaste auf Reverse-Lookupzone > Neue Zone...



# - DNS einrichten

Wählen Sie den Zonentyp aus, den Sie erstellen möchten: <ul> <li>Primäre Zone</li> </ul>	Auch hier. Wir wollen die Zone ja auf dem aktuellen Server - hier Primäre Zone - erstellen.
<ul> <li>Zone in Active Directory speichern (DNS-Server muss als schre Domänencontroller eingerichtet sein)</li> </ul>	Hier sollte die DNS Änderungen noch nicht über die Gruppen- richtlinien gesperrt worden sein
< Zurück We	Abbrechen
Wie sollen Zonendaten repliziert werden?	Wie vorher das selbe Spiel.
<ul> <li>Auf allen DNS-Servern, die auf Domänencontrollern in der Geswerden: myNet.work</li> </ul>	Wir nehmen hier auch "nur"
• Auf allen DNS-Servern, die auf Domänencontrollern in dieser I werden: myNet.work	ne ausgeführt unsere Domäne.
O Auf allen Domänencontrollern in dieser Domäne (Windows 200 myNet.work	mpatibilität):
<ul> <li>Auf allen Domänencontroller, die im Bereich dieser Verzeichnis werden:</li> </ul>	tion angegeben
	~
< Zurück W	> Abbrechen
Legen Sie fest, ob Sie eine Reverse-Lookupzone für IPv4- oder IF möchten. IPv4 Reverse-Lookupzone IPv6 Reverse-Lookupzone	dressen erstellen IPv4 Adresse die Zone einrichten.
< Zurück We	Abbrechen
Geben Sie die Netzwerk-ID oder den Namen der Reverse-Lookupz Netzwerk-ID: 192 .168 .43 Die Netzwerk-ID ist der Teil der IP-Adresse, der dieser Zone a Netzwerk-ID in ihrer normalen Reihenfolge (nicht umgekehrt) Wenn Sie eine Null in der Netzwerk-ID verwenden, wird diese angezeigt. Beispiel: Netzwerk-ID 10 erstellt Zone 10.in-addr.at 10.0 erstellt Zone 0.10.in-addr.arpa. Name der Reverse-Lookupzone: 43.168.192.in-addr.arpa	an.Da die Revers-Lookup-Zone für ganze Netzwerk zuständig ist, werden nur die ersten drei Oktette benötigt, da das letzte Oktett ja variable für die Clients ist.nennamen ind Netzwerk-IDDie Anzeige wird dann auch Revers angezeigt. Passt irgendwie.
< Zurück We	Abbrechen
Dynamische Updates ermöglichen DNS-Clientcomputern, sich zu r eigenen Ressourceneinträge dynamisch mit einem DNS-Server be aktualisieren.	Auch hier wieder - Nur sichere Updates wenn das System produktiv eingesetzt wird.
Bestimmen Sie den Typ des dynamischen Updates, der verwende Nur sichere dynamische Updates zulassen (für Active Director	ofohlen) Dann ist es schon erledigt.

# - Einen Client an die Domäne anbinden. (Beispiel Windows 11)

Hier mal eine Kurzanleitung, wie man einen Windows Client an eine Active Directory (AD) einbindet. Als Beispiel habe ich hier mal ein Windows 11 Professional den ich WClient01 genannt habe.

igenschaften von Internetprotokoll, \	/ersion 4 (TCP/IPv4)	Damit der Client den findet, braucht dieser	Windows Server auch die korrekte
Allgemein Alternative Konfiguration		DNS-Serveradresse. I	n den IPv4
IP-Einstellungen können automatisch zu Netzwerk diese Funktion unterstützt. W Netzwerkadministrator, um die geeigne	igewiesen werden, wenn das /enden Sie sich andernfalls an den ten IP-Einstellungen zu beziehen.	Einstellungen der Netz diese einfach ein.	zwerkkarte geben wir
<ul> <li>IP-Adresse automatisch beziehen</li> </ul>		Da ich einen Backup-I	Domain-Controller
		verwende, gibt es mer	Zwei Divo-Auressen.
IP-Adresse:		Auch vergebe ich kein	e feste IP-Adresse.
Subnetzmaske:	· · ·	da der Server auch als	s DHCP-Server fungiert
Standardgateway:	• • •	und die Adressen selb	st verteilt.
ODNS-Serveradresse automatisch b	eziehen	In der Suche einfach	
O Folgende DNS-Serveradressen ve	rwenden:	mal sys eingeben.	
Bevorzugter DNS-Server:	192.168.43.150	Hier sollte man den	systemsteuerung
Alternativer DNS-Server:	192.168.43.160	finden. Dort dann	7uletzt verwendet
Einstellungen beim Beenden über	prüfen	Domäne oder	Luicizi vermendet
	Erweitert	Arbeitsgruppe wählen.	🛒 System 📐
	OK Abbrechen		Domäne oder Arbeitsgruppe

Unter dem Reiter Computernamen geht man dann einfach auf die Schaltfläche Ändern... Hinweis: Man braucht seinen Computer vorher nicht umzubenennen und neu zu starten. Das kann man auch während dem Domänenbeitritt in einem Rutsch machen. Beim nächsten Fenster ggf. Computername und den Namen der Domäne eingeben.

Systemeigenschaften		×	Ändern des Computernamens bzw. der Domäne 🛛 🗙
Computername Hardware En Folgende Information im Netzwerk verwen	weitert Computerschutz Remote nen werden zum Identifizieren des Computers det.		Sie können den Namen und die Mitgliedschaft des Computers ändem. Änderungen wirken sich möglicherweise auf den Zugriff auf Netzwerkressourcen aus.
Computerbeschreibung:			Computername:
compaterbeserreibung.	1 7		WClient01
Vollständiger Computername:	Zum Beispiel: Spielcomputer oder "Heikes Computer" WClient01		Vollständiger Computername: WClient01
Arbeitsgruppe:	WORKGROUP		Weitere
Klicken Sie auf "Netzwerk-ID",	um einer Domäne Netzwerk-ID		Mitglied von
oder einer Arbeitsgruppe mithilfe beizutreten.	e eines Assistenten		O Domäne:
Klicken Sie auf "Åndem", um d umzubenennen oder dessen D Arbeitsgruppe zu ändem.	liesen Computer omäne oder		myNet.work O Arbeitsgruppe: WORKGROUP OK N Abbrechen
	OK Abbrechen Übernehm	ien	Wenn alles korrekt ist, wird nur noch der Administrator und Passwort vom Server abgefragt.
			$\blacksquare$ Ändern des Computernamens bzw. der Do $\qquad \times$
			Willkommen in der Domäne myNet.work.
			OK

# Windows Server 2025 - Remote Server Administration Tools . (Beispiel Windows 11)

#### features ~ Alle Dokumente Web Fi Apps Höchste Übereinstimmung **Optionale** Features 田 Systemeinstellungen

System > Optionale Features		Dort einfach eingeben, ur angezeigt. H die man ben
Optionales Feature hinzufügen  Features a	inzeigen	ich natürlich die Tools für Aber auch D Wenn man a
Optionales reacure ninzulugen		leider etwas
RSAT		Fertig install
21 Features gefunden		Server-Mana Verwalten >
Verwalten Tools Ansicht Hilfe		
Rollen und Features hinzufügen Rollen und Features entfernen		
Server hinzufügen		
Active Directory DNS Importieren	Ausg	gewählt
Standort: 🗰 myNet 🕨 🕝	Co	mputer
Betriebssystem: Alle 🗸	Ser	MYNET.WORK (1) v25
Name (CN): Serv		
Suche starten		
Name Betriebssystem		
Serv25 Windows Server 2025 Standard	•	
1 Computer gefunden	1 Co	mputer ausgewählt
1 Computer gefunden	1 Co	mputer ausgewählt



Natürlich wäre es sehr mühsam die ganze Konfiguration am Windows-Server über die Powershell zu machen. Natürlich ist das auch möglich, aber das macht in der Regel "fast" niemand.

Wenn wir einen Client an die Domäne angebunden haben, so installiert man die RSA-Tools.

Man sucht in Windows einfach mal ,features' und wählt dann die optionalen Features.

fach den Suchfilter auf RSAT n, und schon werden einige gt. Hier wählt man diejenige aus benötigt. Unabdingbar würde rlich den Server-Manager und s für Active Directory... nennen. ich DNS, Gruppenrichtlinien etc. nan alle installiert, so braucht es twas länger. Warum auch immer.

nstalliert, kann man dann den Manager starten und über en > Server hinzufügen den hinzufügen. (genialer Satz)

Abbrechen