Windows Server 2025

- 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.

```
InterfaceIndex             : 3
```

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 Sicherheits-gründen 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.

```
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName "myNet.work" `
-DomainNetbiosName "MYNET" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true `
-SafeModeAdministratorPassword $dsrm
```

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
```

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.

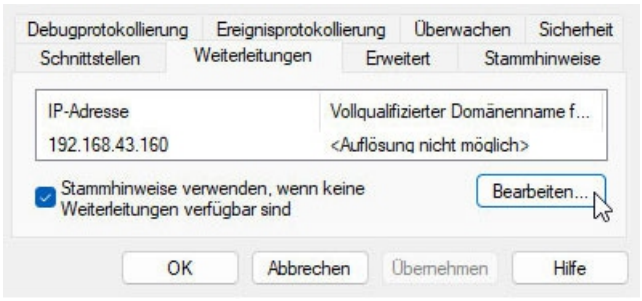
Ab jetzt können wir einen Client an die Domäne anbinden, der dann mit den Remote Server Administration Tools kurz RSAT zugreifen können.

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.

Auf dem Clinet kann man jetzt über den Server-Manager > Tools oder über das Programm Menü Windows-Tools auf das DNS-Tool zugreifen. Hier wählt man dann einfach den Servernamen um die Konfiguration durchzuführen.

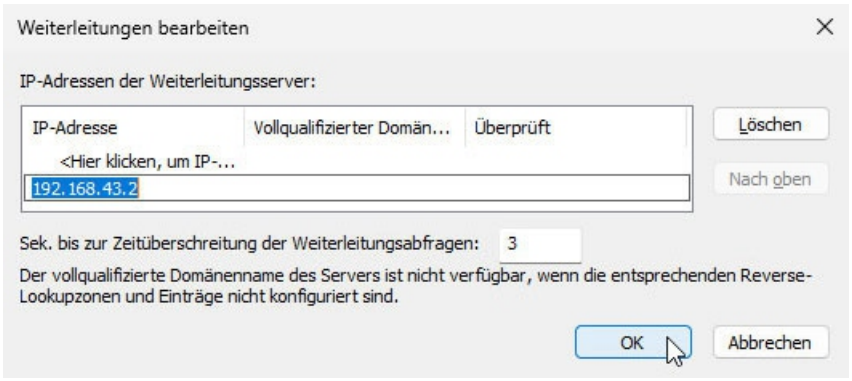
Damit die Namen/IP-Adressen auch außerhalb unserer Zone myNet.work aufgelöst werden können, müssen die Anfragen weitergeleitet werden. Dazu erstellen wir einen forwarder.



Mit der rechten Maustaste auf den DNS Server / Eigenschaften.

Unter Weiterleitung steht jetzt bei mir die IP-Adresse meines Backup-Domain-Controllers. Hier fügen wir aber noch die Standard-Gateway Adresse hinzu.

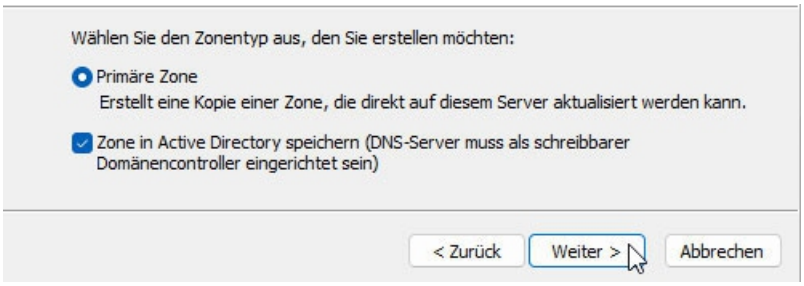
In vielen Fällen und kleineren Netzwerken wird gerne die DNS Adresse von dem Router / fritz!Box (Beispiel 192.168.178.1) genommen. Hier ändere ich jetzt die Weiterleitung auf meinem Gateway 192.168.43.2



Forward-Lookup-Zone

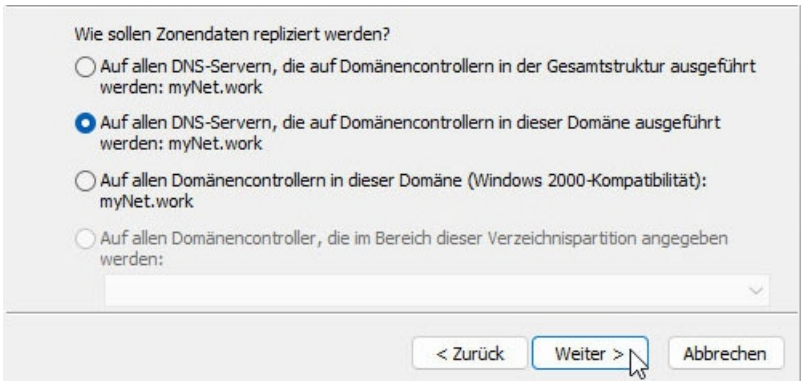
Wenn man den DNS-Service installiert, so konfiguriert das System in der Regel automatisch eine Forward-Lookup Zone. Hier wird ein angefragter Name in eine IP-Adresse aufgelöst.

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



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

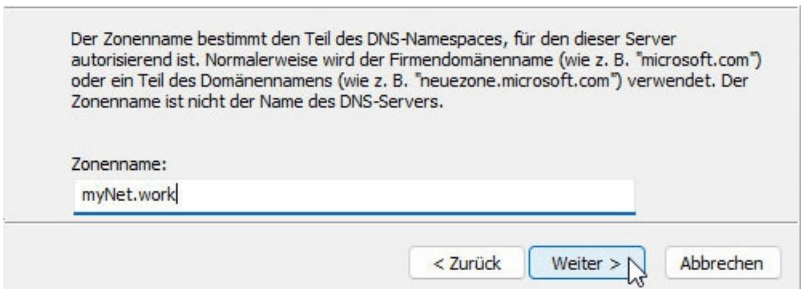
Hier sollte die DNS Änderungen noch nicht über die Gruppen-richtlinien gesperrt worden sein.



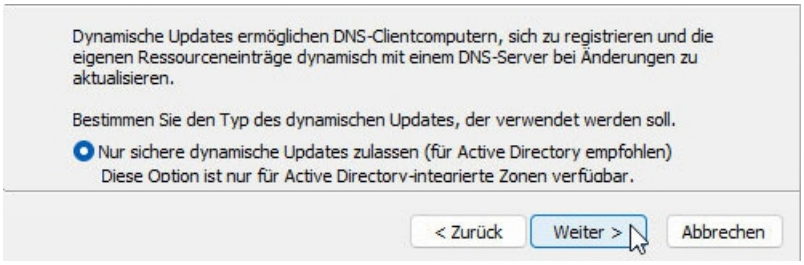
In unserem Beispiel haben wir jetzt nur einen Firmensitz und wollen eh den DNS-Server auch nur für diesen verwenden.

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.



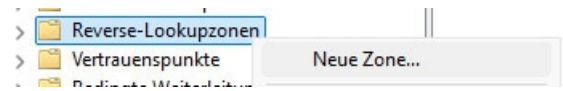
Im produktiven Bereich, sollten hier keine unsicheren Updates zugelassen werden.

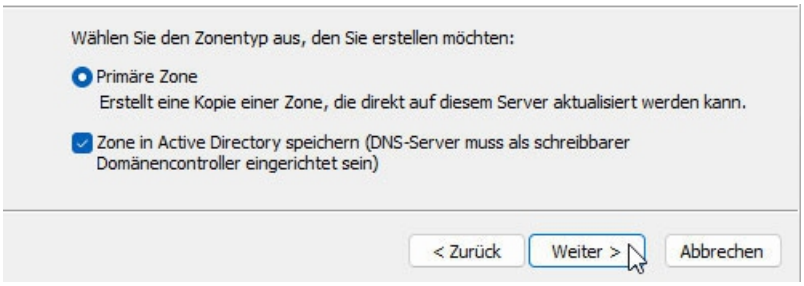
Das manuell Update ist für eine fortgeschrittene Methode, was ich hier jetzt erst mal außen vor lasse. Und das war es dann auch schon. Nur noch Fertig stellen.

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.

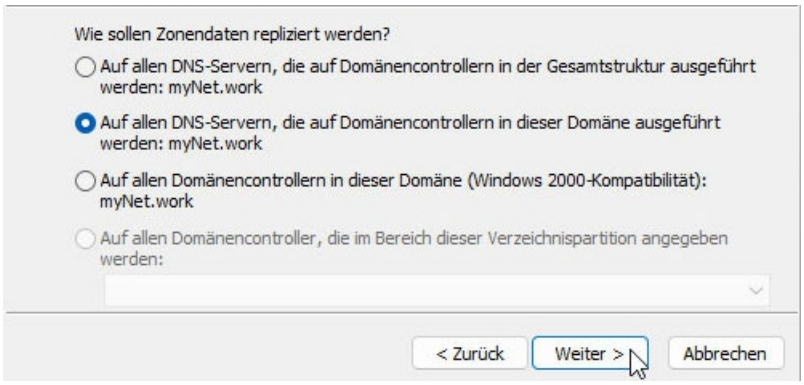
Das Einrichten einer Revers-Lookup-Zone ist fast identisch wie vorher auch.
Mit der rechten Maustaste auf Reverse-Lookupzone > Neue Zone...





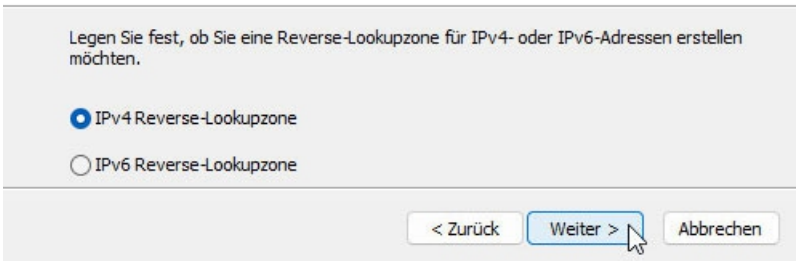
Auch hier. Wir wollen die Zone ja auf dem aktuellen Server - hier Primäre Zone - erstellen.

Hier sollte die DNS Änderungen noch nicht über die Gruppen-richtlinien gesperrt worden sein.

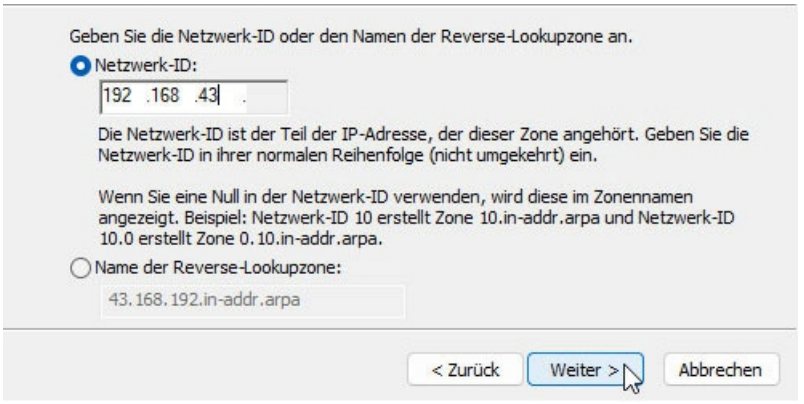


Wie vorher das selbe Spiel.

Wir nehmen hier auch „nur" unsere Domäne.

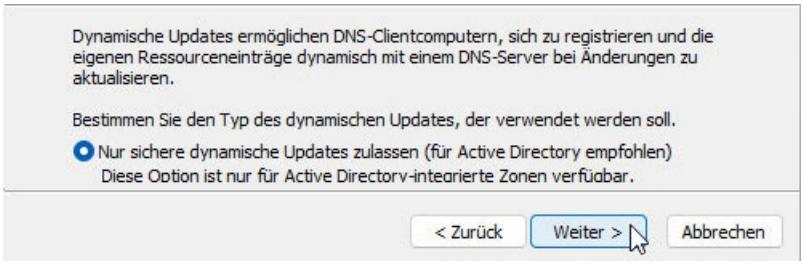


Hier wollen wir ja für unsere IPv4 Adresse die Zone einrichten.



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.

Die Anzeige wird dann auch Revers angezeigt.
Passt irgendwie.



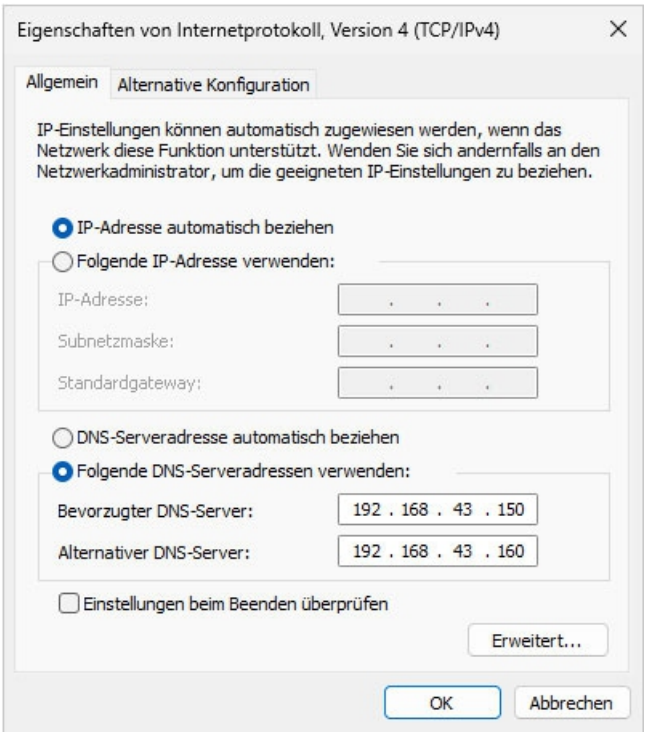
Auch hier wieder - Nur sichere Updates wenn das System produktiv eingesetzt wird.

Dann ist es schon erledigt.
Nur noch fertig stellen.

Windows Server 2025

- 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.

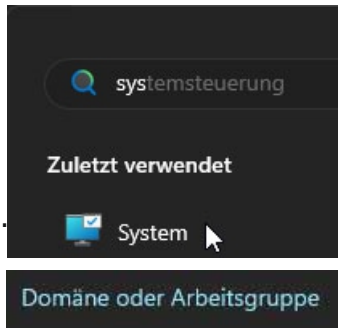


Damit der Client den Windows Server auch findet, braucht dieser die korrekte DNS-Serveradresse. In den IPv4 Einstellungen der Netzwerkkarte geben wir diese einfach ein.

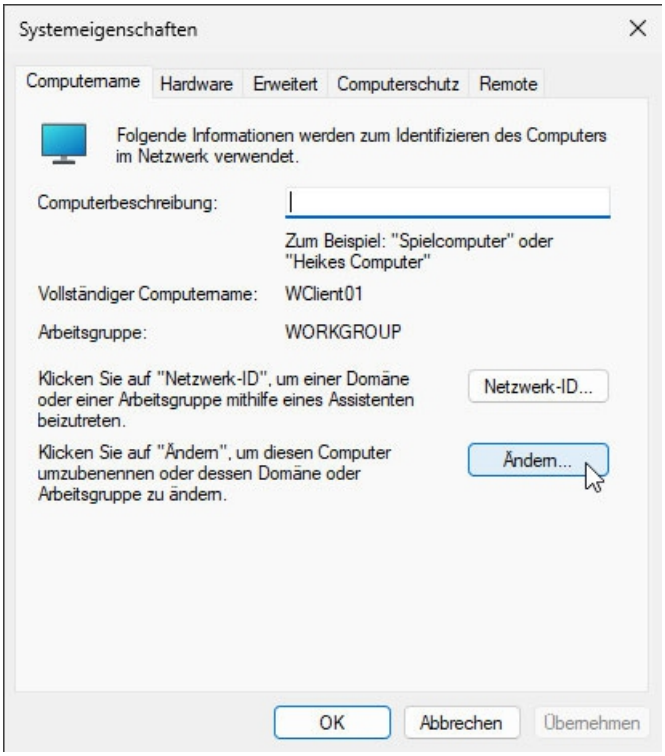
Da ich einen Backup-Domain-Controller verwende, gibt es hier zwei DNS-Adressen.

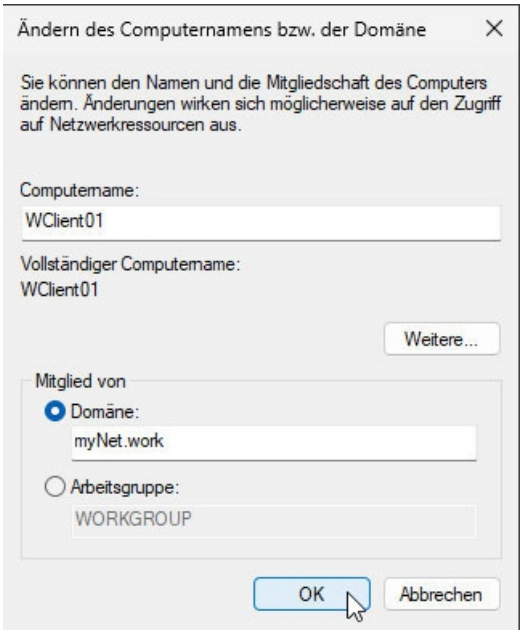
Auch vergebe ich keine feste IP-Adresse, da der Server auch als DHCP-Server fungiert und die Adressen selbst verteilt.

In der Suche einfach mal sys eingeben. Hier sollte man den Eintrag System finden. Dort dann Domäne oder Arbeitsgruppe wählen.

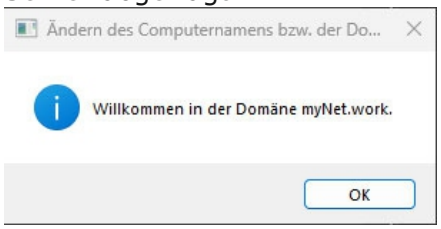


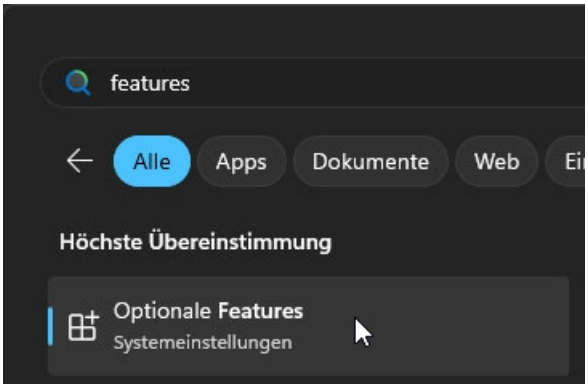
Unter dem Reiter Computernamen geht man dann einfach auf die Schaltfläche Ändern...
Hinweis: Man braucht seinen Computer vorher nicht umzubenennen und neu zu starten. Das kann man auch während dem Domänenbeitritt in einem Rutsch machen.
Beim nächsten Fenster ggf. Computername und den Namen der Domäne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





Wenn alles korrekt ist, wird nur noch der Administrator und Passwort vom Server abgefragt.

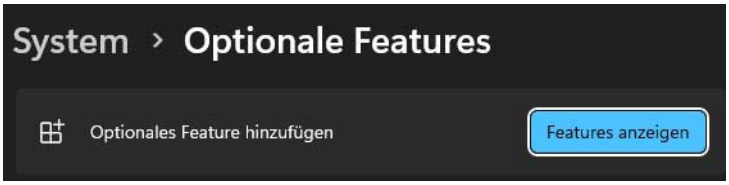




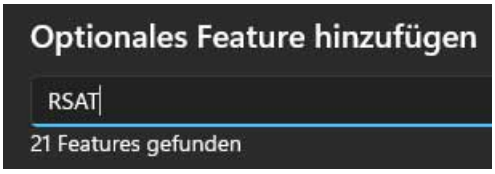
Natürlich wäre es sehr mühsam die ganze Konfiguration am Windows-Server über die Powershell zu machen. Natürlich ist das auch möglich, aber das macht in der Regel „fast" niemand.

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.



Dort einfach den Suchfilter auf RSAT eingeben, und schon werden einige angezeigt. Hier wählt man diejenige aus die man benötigt. Unabdingbar würde ich natürlich den Server-Manager und die Tools für Active Directory... nennen. Aber auch DNS, Gruppenrichtlinien etc. Wenn man alle installiert, so braucht es leider etwas länger. Warum auch immer.



Fertig installiert, kann man dann den Server-Manager starten und über Verwalten > Server hinzufügen den Server hinzufügen. (genialer Satz)