

Windows

- Windows SERVER
 - Windows Server notizen
 - Windows Server Einrichten Klicki Bunti
 - Active Directory komplett per PowerShell
 - DHCP mit Powershell
 - Komplett ABLAUF für Klausur mit Powershell!
- Betriebssystem
 - Klausurvorbereitung Schlegel
 - Test Fragen zur Klausur
 - Mein Abgleich der Klausurvorbereitung und PDF von herrn Schlegel

Windows SERVER

Windows Server notizen

Windows Server Domain Controller Setup

Ziel:

Aufbau einer Windows-Domäne mit:

- DC1 = erster Domain Controller
 - DC2 = zweiter Domain Controller
 - CLIENT1 = Client in der Domäne
 - Active Directory
 - DNS
 - Replikation zwischen beiden Servern
-

Voraussetzungen

- Windows Server installiert
 - Netzwerkverbindung vorhanden
 - Lokaler Administrator vorhanden
 - Statische IP-Adressen geplant
 - Beide Server im selben Netzwerk
 - NAT oder internes Netzwerk korrekt eingestellt
-

Netzwerkplan

Gerät	IP-Adresse
Router / Gateway	10.0.2.1
DC1	10.0.2.254
DC2	10.0.2.253
CLIENT1	DHCP oder statisch

DC1 vorbereiten

Rechnernamen ändern

Beispiel:

DC1

Statische IP konfigurieren

Einstellung	Wert
IP-Adresse	10.0.2.254
Subnetzmaske	255.255.255.0
Gateway	10.0.2.1
Bevorzugter DNS	10.0.2.254

Active Directory installieren

Server-Manager öffnen

Verwalten → Rollen und Features hinzufügen

Installieren:

- Active Directory-Domänendienste
- DNS-Server

DC1 zum Domain Controller hochstufen

Nach der Installation erscheint oben rechts die Flagge.

Dort auswählen:

Diesen Server zu einem Domänencontroller hochstufen

Neue Gesamtstruktur erstellen

NICHT:

Arbeitsgruppe

SONDERN:

Neue Gesamtstruktur hinzufügen

Beispiel:

fisi2502.internal

Wichtige Einstellungen

Aktivieren:

- DNS-Server
- Globaler Katalog

Nicht aktivieren:

- Schreibgeschützter Domain Controller (RODC)

Funktionsebenen

Einstellung	Wert
Gesamtstrukturfunktionsebene	Windows Server 2025
Domänenfunktionsebene	Windows Server 2025

Nach dem Neustart prüfen

Nun existieren:

- Active Directory
- DNS
- SYSVOL
- NETLOGON

DNS auf DC1 prüfen

```
ipconfig /all
```

DNS MUSS sein:

10.0.2.254

Nicht verwenden:

- Router-DNS
- Google DNS
- Fritzbox-DNS

DC2 vorbereiten

Rechnernamen ändern

DC2

Statische IP konfigurieren

Einstellung	Wert
IP-Adresse	10.0.2.253
Subnetzmaske	255.255.255.0
Gateway	10.0.2.1
DNS	10.0.2.254

Wichtig:

DC2 verwendet zuerst DC1 als DNS-Server.

DC2 der Domäne beitreten

NICHT:

Arbeitsgruppe

SONDERN:

fisi2502.internal

Anmeldung mit:

```
fisi2502\Administrator
```

oder:

```
Administrator
```

mit dem Passwort von DC1.

Verbindung testen

Von DC2:

```
ping dc1
```

```
ping fisi2502.internal
```

AD DS und DNS auf DC2 installieren

Im Server-Manager:

```
Verwalten → Rollen und Features hinzufügen
```

Installieren:

- Active Directory-Domänendienste
 - DNS-Server
-

DC2 hochstufen

Nach der Installation auf die Flagge klicken:

```
Diesen Server zu einem Domänencontroller heraufstufen
```

Wichtig

NICHT:

Neue Gesamtstruktur

SONDERN:

Domänencontroller zu vorhandener Domäne hinzufügen

Domäne:

fisi2502.internal

Optionen bei DC2

Aktivieren:

- DNS-Server
- Globaler Katalog

Nicht aktivieren:

- Schreibgeschützter DC

Nach Neustart

Jetzt replizieren zwischen DC1 und DC2:

- Benutzer
- Gruppen
- Gruppenrichtlinien
- DNS
- SYSVOL

DNS optimieren

DC1

	DNS 1	10.0.2.254
DNS 2		10.0.2.253

DC2

DNS 1	10.0.2.253
DNS 2	10.0.2.254

Client zur Domäne hinzufügen

DNS auf CLIENT1 setzen

```
10.0.2.254
```

Domäne beitreten

```
Dieser PC → Eigenschaften → Domäne ändern
```

Domäne:

```
fisi2502.internal
```

Anmeldung am Client

Beispiele:

```
fisi2502\Benutzername
```

oder:

```
benutzername@fisi2502.internal
```

Wichtige Befehle

DHCP erneuern

```
ipconfig /release  
ipconfig /renew
```

DNS Cache löschen

```
ipconfig /flushdns
```

Domain Controller prüfen

```
dcdiag
```

Replikation prüfen

```
repadmin /replsummary
```

Wichtige Hinweise

Beide Server werden NICHT „ein Server“

Es bleiben:

- zwei getrennte Server

ABER:

- beide replizieren Active Directory
- beide können Benutzer anmelden
- beide können DNS beantworten
- beide besitzen eine Kopie der Domäne

Das nennt man:

```
Multi-Master-Replikation
```

Typische Fehler

Falscher DNS-Server

Der häufigste Fehler.

Domain Controller dürfen NICHT den Router als DNS verwenden.

DC2 erstellt neue Gesamtstruktur

Falsch.

DC2 muss:

Vorhandener Domäne hinzufügen

verwenden.

Client nutzt Router-DNS

Dann kann der Client die Domäne nicht finden.

Ablaufübersicht

DC1 installieren

↓

AD DS + DNS installieren

↓

Neue Gesamtstruktur erstellen

↓

DC1 wird Domain Controller

↓

DC2 vorbereiten

↓

DC2 der Domäne beitreten

↓

AD DS + DNS auf DC2 installieren

↓

DC2 zu vorhandenem Domain Controller hinzufügen

↓

Replikation aktiv

↓

Client der Domäne beitreten

Merksatz

Active Directory funktioniert nur sauber,
wenn alle Geräte den Domain Controller als DNS verwenden.

Windows Server Einrichten Klicki Bunti

Schritt-für-Schritt-Anleitung: Windows-Domäne mit DC1, DC2 und Client

Ziel

Eine eigene Domäne aufbauen mit:

- DC1 als erster Domain Controller
- DC2 als zweiter Domain Controller
- DNS auf beiden Servern
- Windows-Client in die Domäne aufnehmen

Beispiel-Domäne:

fisi2502.internal

Beispiel-Netzwerk:

10.0.2.0/24

Netzwerkübersicht

Gerät	IP-Adresse	DNS
Gateway / Router	10.0.2.1	-
DC1	10.0.2.254	10.0.2.254
DC2	10.0.2.253	zuerst 10.0.2.254
Client	DHCP oder statisch	10.0.2.254 / 10.0.2.253

Wichtige Grundregel

Alle Server und Clients müssen im gleichen Netzwerk sein.

In der VM-Software sollte deshalb bei allen drei Maschinen derselbe Netzwerkmodus eingestellt sein, zum Beispiel:

NAT-Netzwerk

oder:

Internes Netzwerk

Wichtig ist nicht der Name, sondern dass DC1, DC2 und Client sich gegenseitig erreichen können.

Teil 1: DC1 Netzwerk einstellen

1. Server-Manager öffnen

Nach dem Start von Windows Server öffnet sich normalerweise automatisch der Server-Manager.

Falls nicht:

Startmenü → Server-Manager

2. Lokaler Server öffnen

Im Server-Manager links auf:

Lokaler Server

klicken.

3. Rechnernamen ändern

Neben „Computernamen“ auf den aktuellen Namen klicken.

Dann:

Ändern

Computernamen eintragen:

DC1

Danach:

OK → Neustart

4. Netzwerkeinstellungen öffnen

Nach dem Neustart wieder öffnen:

Server-Manager → Lokaler Server

Dann neben „Ethernet“ auf die blaue Netzwerkverbindung klicken.

Danach öffnet sich:

Netzwerkverbindungen

5. Adapter-Eigenschaften öffnen

Rechtsklick auf:

Ethernet

Dann:

Eigenschaften

6. IPv4 öffnen

Auswählen:

Internetprotokoll Version 4 (TCP/IPv4)

Dann:

Eigenschaften

7. Statische IP für DC1 eintragen

Aktivieren:

Folgende IP-Adresse verwenden

Eintragen:

IP-Adresse: 10.0.2.254
Subnetzmaske: 255.255.255.0
Standardgateway: 10.0.2.1

Aktivieren:

Folgende DNS-Serveradressen verwenden

Eintragen:

Bevorzugter DNS-Server: 10.0.2.254
Alternativer DNS-Server: leer lassen

Dann:

OK → Schließen

8. Netzwerk prüfen

PowerShell öffnen:

Startmenü → Windows PowerShell

Befehl:

ipconfig /all

Prüfen, ob dort steht:

IPv4-Adresse: 10.0.2.254

DNS-Server: 10.0.2.254

Teil 2: DC1 zu Active Directory Domain Controller machen

1. Rollen und Features öffnen

Im Server-Manager oben rechts:

Verwalten → Rollen und Features hinzufügen

Microsoft beschreibt diesen Weg ebenfalls über den Server-Manager mit anschließender Heraufstufung zum Domänencontroller. :contentReference[oaicite:0]{index=0}

2. Assistent starten

Klicken:

Weiter

Auswählen:

Rollenbasierte oder featurebasierte Installation

Dann:

Weiter

3. Zielsever auswählen

Auswählen:

DC1

Dann:

Weiter

4. Serverrollen auswählen

Haken setzen bei:

Active Directory-Domänendienste

Falls ein Fenster erscheint:

Features hinzufügen

anklicken.

Zusätzlich Haken setzen bei:

DNS-Server

Dann:

Weiter

5. Features

Hier normalerweise nichts ändern.

Weiter

6. Installation starten

Bis zur Bestätigung durchklicken.

Dann:

Installieren

7. DC1 hochstufen

Nach der Installation oben rechts auf die Flagge klicken.

Dann:

Diesen Server zu einem Domänencontroller hochstufen

8. Neue Gesamtstruktur erstellen

Auswählen:

Neue Gesamtstruktur hinzufügen

Stammdomänenname:

fisi2502.internal

Dann:

Weiter

9. Domänencontrolleroptionen

Einstellen:

Gesamtstrukturfunktionsebene: Windows Server 2025

Domänenfunktionsebene: Windows Server 2025

Haken aktiviert lassen bei:

DNS-Server

Globaler Katalog

NICHT aktivieren:

Schreibgeschützter Domänencontroller

DSRM-Kennwort vergeben.

Dann:

Weiter

10. DNS-Warnung

Falls eine DNS-Warnung erscheint, ist das in dieser Testumgebung normal.

Weiter

11. NetBIOS-Name

Der NetBIOS-Name wird meistens automatisch gesetzt.

Beispiel:

FISI2502

Dann:

Weiter

12. Pfade prüfen

Standardpfade lassen:

Datenbankordner
Protokolldateien
SYSVOL

Dann:

Weiter

13. Installation abschließen

Voraussetzungsprüfung abwarten.

Dann:

```
Installieren
```

Der Server startet danach neu.

14. Nach Neustart anmelden

Anmelden mit:

```
FISI2502\Administrator
```

oder:

```
Administrator@fisi2502.internal
```

Teil 3: DC1 prüfen

1. DNS prüfen

PowerShell öffnen:

```
ipconfig /all
```

Wichtig:

```
DNS-Server: 10.0.2.254
```

2. Active Directory öffnen

Im Server-Manager oben rechts:

```
Tools → Active Directory-Benutzer und -Computer
```

Dort sollte die Domäne sichtbar sein:

fisi2502.internal

3. DNS-Konsole öffnen

Im Server-Manager:

Tools → DNS

Dort sollte DC1 sichtbar sein.

Unter Forward-Lookupzonen sollte stehen:

fisi2502.internal

Teil 4: DC2 Netzwerk einstellen

1. DC2 starten

Auf DC2 anmelden mit lokalem Administrator.

2. Rechnernamen ändern

Server-Manager → Lokaler Server → Computernamen → Ändern

Computernamen:

DC2

Dann:

OK → Neustart

3. IPv4-Einstellungen öffnen

Nach Neustart:

Server-Manager → Lokaler Server → Ethernet

Dann:

Rechtsklick auf Ethernet → Eigenschaften

Dann:

Internetprotokoll Version 4 (TCP/IPv4) → Eigenschaften

4. Statische IP für DC2 eintragen

IP-Adresse: 10.0.2.253

Subnetzmaske: 255.255.255.0

Standardgateway: 10.0.2.1

DNS:

Bevorzugter DNS-Server: 10.0.2.254

Alternativer DNS-Server: leer lassen

Wichtig:

DC2 nutzt am Anfang DC1 als DNS, damit er die Domäne finden kann.

5. Verbindung zu DC1 testen

PowerShell auf DC2 öffnen:

```
ping 10.0.2.254
```

Dann:

```
ping dc1
```

Dann:

```
ping fisi2502.internal
```

Teil 5: DC2 der Domäne hinzufügen

1. Systemeigenschaften öffnen

Auf DC2:

```
Server-Manager → Lokaler Server → Computernamen
```

Dann:

```
Ändern
```

2. Domäne eintragen

Unten auswählen:

```
Domäne
```

Eintragen:

```
fisi2502.internal
```

Dann:

```
OK
```

3. Domänenadmin eingeben

Benutzername:

```
FISI2502\Administrator
```

Kennwort:

Passwort vom Domain Administrator

4. Neustart

Nach erfolgreicher Meldung:

Willkommen in der Domäne fisi2502.internal

Dann:

Neustart

Teil 6: DC2 zum zweiten Domain Controller machen

1. Auf DC2 anmelden

Anmelden mit:

FISI2502\Administrator

2. Rollen und Features hinzufügen

Im Server-Manager:

Verwalten → Rollen und Features hinzufügen

3. Rollen auswählen

Installieren:

Active Directory-Domänendienste
DNS-Server

Bei Nachfragen:

Features hinzufügen

Dann:

Weiter → Installieren

4. DC2 hochstufen

Nach der Installation oben rechts auf die Flagge klicken.

Dann:

Diesen Server zu einem Domänencontroller hochstufen

5. Vorhandene Domäne verwenden

Wichtig:

NICHT auswählen:

Neue Gesamtstruktur hinzufügen

Sondern auswählen:

Domänencontroller zu vorhandener Domäne hinzufügen

Domäne:

fisi2502.internal

6. Zugangsdaten prüfen

Falls gefragt:

FISI2502\Administrator

eingeben.

7. Optionen setzen

Aktivieren:

DNS-Server
Globaler Katalog

NICHT aktivieren:

Schreibgeschützter Domänencontroller

DSRM-Kennwort vergeben.

Dann:

Weiter

8. Replikationsquelle

Wenn gefragt:

Von beliebigem Domänencontroller replizieren

oder DC1 auswählen.

Dann:

Weiter

9. Installation abschließen

Voraussetzungsprüfung abwarten.

Dann:

Installieren

DC2 startet danach neu.

Teil 7: DNS auf DC1 und DC2 richtig einstellen

1. DC1 DNS-Einstellungen

Auf DC1:

Server-Manager → Lokaler Server → Ethernet → Eigenschaften

Dann:

Internetprotokoll Version 4 (TCP/IPv4)

DNS eintragen:

Bevorzugter DNS-Server: 10.0.2.254

Alternativer DNS-Server: 10.0.2.253

2. DC2 DNS-Einstellungen

Auf DC2:

Server-Manager → Lokaler Server → Ethernet → Eigenschaften

Dann:

Internetprotokoll Version 4 (TCP/IPv4)

DNS eintragen:

Bevorzugter DNS-Server: 10.0.2.253

Alternativer DNS-Server: 10.0.2.254

Microsoft empfiehlt für Domain Controller passende interne DNS-Client-Einstellungen, damit AD und Namensauflösung zuverlässig funktionieren. [:contentReference\[oaicite:1\]{index=1}](#)

Teil 8: Replikation prüfen

1. Auf DC1 prüfen

PowerShell als Administrator öffnen:

```
dcdiag
```

Dann:

```
repadmin /replsummary
```

2. Auf DC2 prüfen

PowerShell als Administrator öffnen:

```
dcdiag
```

Dann:

```
repadmin /replsummary
```

3. Active Directory prüfen

Auf DC1:

```
Server-Manager → Tools → Active Directory-Benutzer und -Computer
```

Prüfen, ob DC2 als Domain Controller auftaucht.

Teil 9: Client Netzwerk einstellen

1. Client starten

Windows Client starten.

2. Netzwerkeinstellungen öffnen

Bei Windows 11:

```
Start → Einstellungen → Netzwerk und Internet
```

Dann:

Ethernet

oder bei WLAN:

WLAN

3. IP-Einstellungen prüfen

Wenn DHCP genutzt wird:

IP-Zuweisung: Automatisch DHCP

Das ist okay.

Aber DNS muss auf die Domain Controller zeigen.

4. DNS manuell setzen

Bei Ethernet:

Start → Einstellungen → Netzwerk und Internet → Ethernet

Dann bei DNS-Serverzuweisung:

Bearbeiten

Auswählen:

Manuell

IPv4 aktivieren.

Eintragen:

Bevorzugter DNS: 10.0.2.254

Alternativer DNS: 10.0.2.253

Microsoft beschreibt für Windows die Änderung der IP-/DNS-Einstellungen über Netzwerk & Internet und „IP-Zuweisung bearbeiten“. :contentReference[oaicite:2]{index=2}

5. DNS testen

PowerShell oder Eingabeaufforderung öffnen:

```
ipconfig /all
```

Prüfen:

```
DNS-Server: 10.0.2.254
```

```
DNS-Server: 10.0.2.253
```

Dann testen:

```
ping dc1
```

```
ping dc2
```

```
ping fisi2502.internal
```

Teil 10: Client der Domäne hinzufügen

1. Einstellungen öffnen

Auf dem Client:

```
Start → Einstellungen → Konten
```

Dann:

```
Auf Arbeits- oder Schulkonto zugreifen
```

Dann:

Verbinden

2. Lokaler AD-Domäne beitreten

Auswählen:

Dieses Gerät einer lokalen Active Directory-Domäne hinzufügen

Domänenname eingeben:

fisi2502.internal

Microsoft beschreibt diesen Weg für den Domänenbeitritt über „Konten → Auf Arbeits- oder Schulkonto zugreifen → Verbinden“. :contentReference[oaicite:3]{index=3}

3. Domänenadmin eingeben

Benutzername:

FISI2502\Administrator

Kennwort:

Passwort vom Domain Administrator

4. Neustart

Nach erfolgreichem Beitritt:

Neustart

5. Am Client mit Domänenkonto anmelden

Beispiel:

FISI2502\Benutzername

oder:

Benutzername@fisi2502.internal

Teil 11: Benutzer im Active Directory erstellen

1. AD-Benutzer und -Computer öffnen

Auf DC1:

Server-Manager → Tools → Active Directory-Benutzer und -Computer

2. Benutzer erstellen

Links die Domäne öffnen:

fisi2502.internal

Dann zum Beispiel:

Users

Rechtsklick:

Neu → Benutzer

3. Benutzerdaten eingeben

Beispiel:

Vorname: Max

Nachname: Mustermann

Benutzeranmeldename: max.mustermann

Dann:

Weiter

4. Passwort setzen

Passwort vergeben.

Für Testumgebung möglich:

Kennwort läuft nie ab

Für echte Umgebung besser nicht dauerhaft verwenden.

Dann:

Fertigstellen

Teil 12: Anmeldung testen

Auf dem Client anmelden mit:

FISI2502\max.mustermann

oder:

max.mustermann@fisi2502.internal

Wenn die Anmeldung funktioniert, ist der Client erfolgreich in der Domäne.

Nützliche Befehle

IP-Adresse anzeigen

ipconfig /all

DHCP neu beziehen

```
ipconfig /release  
ipconfig /renew
```

DNS-Cache löschen

```
ipconfig /flushdns
```

Domäne testen

```
ping fisi2502.internal
```

Domain Controller testen

```
dcdiag
```

Replikation testen

```
repadmin /replsummary
```

Häufige Fehler

Fehler 1: Client findet Domäne nicht

Ursache meistens:

```
Client nutzt Router oder Internet-DNS
```

Richtig:

```
Client muss DC1 oder DC2 als DNS nutzen
```

Fehler 2: DC2 findet Domäne nicht

Ursache meistens:

DC2 nutzt falschen DNS

Richtig vor dem Domänenbeitritt:

DNS auf DC2 = 10.0.2.254

Fehler 3: DC2 wird als neue Gesamtstruktur eingerichtet

Falsch:

Neue Gesamtstruktur hinzufügen

Richtig:

Domänencontroller zu vorhandener Domäne hinzufügen

Fehler 4: Server sind nicht im gleichen VM-Netzwerk

Alle Maschinen müssen denselben Netzwerkmodus nutzen:

DC1 = NAT-Netzwerk
DC2 = NAT-Netzwerk
Client = NAT-Netzwerk

oder:

DC1 = Internes Netzwerk
DC2 = Internes Netzwerk
Client = Internes Netzwerk

Kurzer Ablauf als Merkkette

DC1 Name setzen
↓
DC1 statische IP setzen

↓
AD DS + DNS installieren
↓
Neue Gesamtstruktur erstellen
↓
DC1 ist erster Domain Controller
↓
DC2 Name setzen
↓
DC2 statische IP setzen
↓
DC2 DNS auf DC1 setzen
↓
DC2 der Domäne beitreten
↓
AD DS + DNS auf DC2 installieren
↓
DC2 als zusätzlichen Domain Controller hochstufen
↓
DNS gegenseitig eintragen
↓
Client DNS auf DC1/DC2 setzen
↓
Client der Domäne beitreten
↓
Mit Domänenbenutzer anmelden

Merksatz

Ohne richtigen DNS funktioniert Active Directory nicht sauber.
Alle Server und Clients müssen die Domain Controller als DNS verwenden.

Windows SERVER

Active Directory komplett per PowerShell

Schnellster Weg: Active Directory komplett per PowerShell

Wichtig

Vorher anpassen falls deine Werte anders sind:

```
Domäne:   fisi2502.internal
Netzwerk: 10.0.2.0/24
Gateway:  10.0.2.1
DC1:      10.0.2.254
DC2:      10.0.2.253
```

Teil 1: DC1 komplett einrichten

1. Rechnernamen ändern

Auf Server 1:

```
Rename-Computer -NewName "DC1" -Restart
```

Danach neu anmelden.

2. Netzwerk konfigurieren

Netzwerkadapter anzeigen:

```
Get-NetAdapter
```

Meistens heißt er:

```
Ethernet
```

Dann IP setzen:

```
New-NetIPAddress `
-InterfaceAlias "Ethernet" `
-IPAddress 10.0.2.254 `
-PrefixLength 24 `
-DefaultGateway 10.0.2.1
```

DNS setzen:

```
Set-DnsClientServerAddress `
-InterfaceAlias "Ethernet" `
-ServerAddresses 10.0.2.254
```

3. Netzwerk prüfen

```
ipconfig /all
```

Wichtig:

```
IPv4-Adresse: 10.0.2.254
DNS-Server: 10.0.2.254
```

4. Active Directory + DNS installieren

```
Install-WindowsFeature `
AD-Domain-Services,DNS `
-IncludeManagementTools
```

5. Neue Domäne erstellen

```
Install-ADDSForest `
-DomainName "fisi2502.internal" `
-DomainNetbiosName "FISI2502" `
-InstallDNS `
-SafeModeAdministratorPassword (Read-Host -AsSecureString "DSRM Passwort") `
-Force
```

6. Neustart abwarten

Der Server startet automatisch neu.

Danach anmelden mit:

```
FISI2502\Administrator
```

7. Prüfen ob AD funktioniert

```
Get-ADDomain
```

```
dcdiag
```

Teil 2: DC2 vorbereiten

1. Rechnernamen ändern

Auf Server 2:

```
Rename-Computer -NewName "DC2" -Restart
```

Danach neu anmelden.

2. Netzwerk konfigurieren

IP setzen:

```
New-NetIPAddress `
-InterfaceAlias "Ethernet" `
-IPAddress 10.0.2.253 `
-PrefixLength 24 `
-DefaultGateway 10.0.2.1
```

DNS setzen:

```
Set-DnsClientServerAddress `
-InterfaceAlias "Ethernet" `
-ServerAddresses 10.0.2.254
```

3. Verbindung testen

```
ping 10.0.2.254
```

```
ping dc1
```

```
ping fisi2502.internal
```

Teil 3: DC2 der Domäne hinzufügen

```
Add-Computer `
-DomainName "fisi2502.internal" `
-Credential "FISI2502\Administrator" `
-Restart
```

Passwort eingeben.

Danach startet DC2 neu.

Teil 4: DC2 zum zweiten Domain Controller machen

Nach Neustart anmelden mit:

```
FISI2502\Administrator
```

1. AD DS + DNS installieren

```
Install-WindowsFeature `
AD-Domain-Services,DNS `
```

```
-IncludeManagementTools
```

2. DC2 hochstufen

```
Install-ADDSDomainController `
-DomainName "fisi2502.internal" `
-InstallDNS `
-Credential (Get-Credential "FISI2502\Administrator") `
-SafeModeAdministratorPassword (Read-Host -AsSecureString "DSRM Passwort") `
-Force
```

Danach startet DC2 automatisch neu.

Teil 5: DNS sauber konfigurieren

Auf DC1

```
Set-DnsClientServerAddress `
-InterfaceAlias "Ethernet" `
-ServerAddresses 10.0.2.254,10.0.2.253
```

Auf DC2

```
Set-DnsClientServerAddress `
-InterfaceAlias "Ethernet" `
-ServerAddresses 10.0.2.253,10.0.2.254
```

Teil 6: Replikation prüfen

Auf DC1 oder DC2:

```
repadmin /replsummary
```

```
dcdiag
```

Teil 7: Benutzer erstellen

```
New-ADUser `
-Name "Max Mustermann" `
-GivenName "Max" `
-Surname "Mustermann" `
-SamAccountName "max.mustermann" `
-UserPrincipalName "max.mustermann@fisi2502.internal" `
-AccountPassword (ConvertTo-SecureString "Test123!" -AsPlainText -Force) `
-Enabled $true
```

Teil 8: Client vorbereiten

DNS setzen:

```
Set-DnsClientServerAddress `
-InterfaceAlias "Ethernet" `
-ServerAddresses 10.0.2.254,10.0.2.253
```

Client der Domäne hinzufügen

```
Add-Computer `
-DomainName "fisi2502.internal" `
-Credential "FISI2502\Administrator" `
-Restart
```

Teil 9: Anmeldung testen

Am Client anmelden mit:

```
FISI2502\max.mustermann
```

oder:

```
max.mustermann@fisi2502.internal
```

Nützliche Befehle

IP anzeigen

```
ipconfig /all
```

DNS Cache löschen

```
ipconfig /flushdns
```

Domäne testen

```
ping fisi2502.internal
```

AD prüfen

```
Get-ADDomain
```

Domain Controller prüfen

```
dcdiag
```

Replikation prüfen

```
repadmin /replsummary
```

Häufigster Fehler

Fast immer DNS.

Richtig:

```
DC1 → DNS = DC1/DC2
```

```
DC2 → DNS = DC2/DC1
```

Client → DNS = DC1/DC2

Falsch:

Router-DNS
Google-DNS
Fritzbox-DNS

Ultra-Kurzfassung

DC1:

Name setzen

↓

IP setzen

↓

DNS setzen

↓

AD + DNS installieren

↓

Neue Domäne erstellen

DC2:

Name setzen

↓

IP setzen

↓

DNS auf DC1

↓

Domäne beitreten

↓

AD + DNS installieren

↓

Zum zweiten DC hochstufen

Client:

DNS auf DCs setzen

↓

Domäne beitreten



Mit Domänenkonto anmelden

Windows SERVER

DHCP mit Powershell

DHCP-Server auf DC1 per PowerShell einrichten

Wichtig

Nicht blind 1:1 übernehmen falls dein Netzwerk anders ist.

Beispiel-Netzwerk:

```
Netzwerk: 10.0.2.0/24
Gateway: 10.0.2.1
DC1:     10.0.2.254
DC2:     10.0.2.253
Domäne:  fisi2502.internal
```

DHCP-Bereich Beispiel:

```
10.0.2.100 - 10.0.2.200
```

Teil 1: DHCP-Server installieren

Auf DC1 als Domänenadministrator:

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

Teil 2: DHCP im Active Directory autorisieren

Wichtig bei Domain-Umgebung.

```
Add-DhcpServerInDC `
-DnsName "dc1.fisi2502.internal" `
-IPAddress 10.0.2.254
```

Prüfen:

```
Get-DhcpServerInDC
```

Teil 3: DHCP-Bereich erstellen

DHCP-Scope anlegen:

```
Add-DhcpServerv4Scope `
-Name "LAN" `
-StartRange 10.0.2.100 `
-EndRange 10.0.2.200 `
-SubnetMask 255.255.255.0 `
-State Active
```

Teil 4: Gateway konfigurieren

Gateway verteilen:

```
Set-DhcpServerv4OptionValue `
-Router 10.0.2.1
```

Teil 5: DNS konfigurieren

DNS-Server verteilen:

```
Set-DhcpServerv4OptionValue `
-DnsServer 10.0.2.254,10.0.2.253 `
-DnsDomain "fisi2502.internal"
```

Teil 6: Lease-Zeit setzen (optional)

Beispiel:

```
Set-DhcpServerv4Scope `
-Scopeld 10.0.2.0 `
-LeaseDuration 1.00:00:00
```

Das bedeutet:

```
1 Tag Lease-Zeit
```

Teil 7: DHCP-Dienst prüfen

```
Get-Service DHCPService
```

Wenn nötig starten:

```
Start-Service DHCPService
```

Teil 8: DHCP prüfen

Alle DHCP-Scopes anzeigen:

```
Get-DhcpServerv4Scope
```

DHCP-Optionen anzeigen:

```
Get-DhcpServerv4OptionValue
```

Vergebene IPs anzeigen:

```
Get-DhcpServerv4Lease -Scopeld 10.0.2.0
```

Teil 9: Client testen

Auf dem Client:

```
ipconfig /release
```

```
ipconfig /renew
```

Danach prüfen:

```
ipconfig /all
```

Wichtig:

```
IPv4-Adresse = aus DHCP-Bereich  
Gateway     = 10.0.2.1  
DNS         = 10.0.2.254 / 10.0.2.253
```

Teil 10: DHCP-Reservierung erstellen (optional)

Beispiel:

```
Add-DhcpServerv4Reservation `  
-ScopeId 10.0.2.0 `  
-IPAddress 10.0.2.150 `  
-ClientId "AA-BB-CC-DD-EE-FF" `  
-Description "Client-PC"
```

MAC-Adresse anzeigen:

```
getmac
```

Teil 11: DHCP-Konsole öffnen

Falls du später GUI nutzen willst:

```
dhcpcmgmt.msc
```

Nützliche Befehle

DHCP-Server anzeigen:

```
Get-DhcpServerInDC
```

Scopes anzeigen:

```
Get-DhcpServerv4Scope
```

Leases anzeigen:

```
Get-DhcpServerv4Lease -ScopeId 10.0.2.0
```

DHCP-Dienststatus:

```
Get-Service DHCPService
```

Wichtiger Hinweis

In einer Active-Directory-Umgebung sollte DHCP immer:

```
DNS der Domain Controller verteilen
```

Richtig:

```
10.0.2.254
```

```
10.0.2.253
```

Falsch:

```
8.8.8.8
```

```
1.1.1.1
```

```
Router-DNS
```

Sonst funktioniert:

- Domänenbeitritt
- Anmeldung
- Gruppenrichtlinien
- Active Directory

nicht sauber.

Ultra-Kurzfassung

DHCP installieren

↓

DHCP autorisieren

↓

DHCP-Scope erstellen

↓

Gateway setzen

↓

DNS setzen

↓

Client per DHCP verbinden

↓

IP prüfen

Windows SERVER

Komplett ABLAUF für Klausur mit Powershell!

WINDOWS SERVER LAB - KORREKTER ABLAUF (GEPRÜFT)

Netzwerk

```
DC1 = 10.0.2.254  
DC2 = 10.0.2.253  
Gateway = 10.0.2.1  
Domäne = fisi2502.internal
```

Wichtig vor Start Netzwerkkadaptername prüfen (bei dir meist Ethernet):

```
Get-NetAdapter
```

Falls der Adapter anders heißt, überall "Ethernet" ersetzen.

=====

TEIL 1 - DC1 (AUF SERVER 1)

=====

1. Rechnername setzen

```
Rename-Computer -NewName "DC1" -Restart
```

Nach Neustart anmelden.

2. Netzwerk konfigurieren

Vorher prüfen ob schon IP gesetzt:

```
Get-NetIPAddress -InterfaceAlias "Ethernet"
```

Dann setzen:

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.2.254 -PrefixLength 24 -DefaultGateway 10.0.2.1
```

DNS setzen:

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.2.254
```

Prüfen:

```
ipconfig /all
```

3. AD + DNS installieren

```
Install-WindowsFeature AD-Domain-Services,DNS -IncludeManagementTools
```

4. Neue Domäne erstellen

```
Install-ADDSForest -DomainName "fisi2502.internal" -DomainNetbiosName "FISI2502" -InstallDNS -  
SafeModeAdministratorPassword (Read-Host -AsSecureString "DSRM Passwort") -Force
```

Server startet neu.

Danach anmelden mit:

```
FISI2502\Administrator
```

5. DHCP installieren

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

6. DHCP autorisieren

```
Add-DhcpServerInDC -DnsName "DC1.fisi2502.internal" -IPAddress 10.0.2.254
```

Prüfen:

```
Get-DhcpServerInDC
```

7. DHCP Scope erstellen

```
Add-DhcpServerv4Scope -Name "LAN" -StartRange 10.0.2.100 -EndRange 10.0.2.200 -SubnetMask  
255.255.255.0 -State Active
```

8. Gateway verteilen

```
Set-DhcpServerv4OptionValue -Router 10.0.2.1
```

9. DNS NUR DC1 verteilen

```
Set-DhcpServerv4OptionValue -DnsServer 10.0.2.254 -DnsDomain "fisi2502.internal"
```

Prüfen:

```
Get-DhcpServerv4OptionValue
```

=====

HIER WECHSEL ZU DC2

=====

TEIL 2 - DC2 (AUF SERVER 2)

=====

10. Rechnername setzen

```
Rename-Computer -NewName "DC2" -Restart
```

Nach Neustart anmelden.

11. Netzwerk konfigurieren

Vorher prüfen:

```
Get-NetIPAddress -InterfaceAlias "Ethernet"
```

Dann setzen:

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.2.253 -PrefixLength 24 -DefaultGateway 10.0.2.1
```

DNS setzen:

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.2.254
```

Verbindung prüfen:

```
ping 10.0.2.254
```

```
ping dc1
```

```
ping fisi2502.internal
```

12. Domäne beitreten

```
Add-Computer -DomainName "fisi2502.internal" -Credential "FISI2502\Administrator" -Restart
```

Server startet neu.

Danach anmelden mit:

```
FISI2502\Administrator
```

13. AD + DNS installieren

```
Install-WindowsFeature AD-Domain-Services,DNS -IncludeManagementTools
```

14. DC2 zum zweiten Domain Controller hochstufen

```
Install-ADDSDomainController -DomainName "fisi2502.internal" -InstallDNS -Credential (Get-Credential "FISI2502\Administrator") -SafeModeAdministratorPassword (Read-Host -AsSecureString "DSRM Passwort") -Force
```

Server startet neu.

=====

HIER ZURÜCK ZU DC1

=====

TEIL 3 - DHCP AUF DC1 ERWEITERN

=====

15. DHCP DNS erweitern

Jetzt erst, weil DC2 jetzt existiert:

```
Set-DhcpServerv4OptionValue -DnsServer 10.0.2.254,10.0.2.253 -DnsDomain "fisi2502.internal"
```

Prüfen:

```
Get-DhcpServerv4OptionValue
```

16. Optional DNS Client Settings Server

DC1:

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.2.254,10.0.2.253
```

DC2:

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.2.253,10.0.2.254
```

17. Replikation prüfen

```
dcdiag
```

```
repadmin /replsummary
```

=====

TEIL 4 - CLIENT

=====

18. DNS setzen

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.2.254,10.0.2.253
```

19. Domäne beitreten

```
Add-Computer -DomainName "fisi2502.internal" -Credential "FISI2502\Administrator" -Restart
```

20. Anmeldung

```
FISI2502\Administrator
```

oder:

```
FISI2502\max.mustermann
```

=====

MERKSATZ

```
DC1 komplett bauen
```

```
↓
```

```
DHCP fertig
```

```
↓
```

```
ZU DC2 WECHSELN
```

```
↓
```

DC2 der Domäne beitreten

↓

DC2 zum zweiten Domain Controller machen

↓

ZURÜCK ZU DC1

↓

DHCP DNS erweitern

↓

CLIENT hinzufügen

Betriebssystem

Klausurvorbereitung Schlegel

Single-Session vs. Multi-Session (Mehrbenutzersysteme)

Single-Session-Systeme

→ Nur **ein Benutzer gleichzeitig**

Typisch für:

- MS-DOS
- alte Handys
- z.b alte versionen bis Windows 3.1

Merkmale:

- kein paralleles Arbeiten
 - keine Benutzertrennung
 - kaum Rechteverwaltung
-

Multi-Session / Multiuser-Systeme

→ **Mehrere Benutzer gleichzeitig**

Typisch für:

- Server-Systeme
- Linux (immer Multiuser, abhängig von Ressourcen)

Historie:

- 1960 → erste Mehrbenutzersysteme
- 1982 → Commodore 64 (Single-User)
- ab 1990er → moderne Mehrbenutzersysteme

Vorteile:

- unterschiedliche Benutzerrechte
 - eigener Home-Ordner pro Benutzer
 - höhere Sicherheit (Admin vs. User)
 - Kosteneinsparung (ein System für mehrere Nutzer)
 - Gruppen mit unterschiedlichen Rechten möglich
-

Anmeldung (Login-Prozess)

1. Identifikation

→ Wer bist du?

- Benutzername (entscheidend)
 - Anzeigename
 - Token (möglich)
-

2. Authentisierung (Authentifizierung) (Systemseite)

→ Bist du wirklich diese Person?

- Eingabe von Nachweisen (Passwort, PIN, Biometrie, Token, Passkey, 2FA / MFA)
 - Das System überprüft diese Angaben
 - Passwort wird als Hash gespeichert
 - Eingabe wird gehasht und mit dem gespeicherten Hash verglichen
-

3. Autorisierung

→ Was darfst du?

- Rechte und Berechtigungen werden geprüft
 - Zugriff auf erlaubte Ressourcen wird gewährt
-

Hashwerte

- Nicht auf den Ausgangswert zurückführbar (Einwegfunktion)
- Kleine Änderung der Eingabe → völlig anderer Hashwert

Kollision:

- zwei verschiedene Eingaben → gleicher Hash
 - Beispiel: MD5 war dafür bekannt und gilt als unsicher
-

Benutzer & Gruppen

Benutzer

→ Berechtigungsträger, der sich am System anmelden kann

- lokale Benutzerkonten
 - zentrale Benutzerkonten, z. B. über Active Directory
 - Benutzer können unterschiedliche Rechte besitzen
-

Gruppen

→ dienen nur zur Rechtevergabe

- mit Gruppen kann man sich nicht anmelden
 - lokale Gruppen oder Domänengruppen
 - vereinfachen die Rechteverwaltung
-

Benutzerrollen

- Administrator → volle Kontrolle zur Systemverwaltung
 - Standardbenutzer → eingeschränkte Rechte
 - Gast → kaum Rechte, heute selten sinnvoll
 - System → mindestens Admin-Rechte, oft darüber hinaus
-

SID (Security Identifier)

- eindeutige interne Kennung eines Benutzers
 - wird nur einmal vergeben
 - bleibt auch nach Löschung eindeutig
 - verhindert ungewollte Rechteübernahme nach Neuerstellung
-

Eigenschaften eines Benutzerkontos

- Benutzername / Anmeldename
 - vollständiger Name / Anzeigename
 - UPN: user @ domain.tld
 - SID
-

PowerShell

Get-LocalUser -Name

Home-Verzeichnis

AppData → benutzerspezifische Daten

Programmdateien

ntuser.dat → versteckt, enthält benutzerspezifische Einstellungen

Merksätze

Benutzername = Anmeldename (wichtig für Verwaltung)

Gruppen = nur Rechtevergabe

Multiuser = mehr Sicherheit + Struktur

Test Fragen zur Klausur

Single-Session vs. Multi-Session - Test (40 Fragen)

1. Was ist ein Single-Session-System?

Ein System, bei dem nur ein Benutzer gleichzeitig arbeiten kann.

2. Nenne ein Beispiel für ein Single-Session-System.

MS-DOS oder Windows 3.1.

3. Was ist ein Multiuser-System?

Ein System, bei dem mehrere Benutzer gleichzeitig arbeiten können.

4. Wo werden Multiuser-Systeme typischerweise eingesetzt?

Auf Server-Systemen.

5. Ist Linux ein Multiuser-System?

Ja, Linux ist immer ein Multiuser-System.

6. Wann entstanden die ersten Mehrbenutzersysteme?

Um 1960.

7. Welches System war wieder ein Single-User-System (1982)?

Der Commodore 64.

8. Nenne einen Vorteil von Multiuser-Systemen.

Unterschiedliche Benutzerrechte möglich.

9. Warum sind Multiuser-Systeme sicherer?

Weil Rechte getrennt sind (Admin vs. Benutzer).

10. Was ist ein Home-Verzeichnis?

Der persönliche Speicherbereich eines Benutzers.

11. Was bedeutet Identifikation?

Der Benutzer gibt an, wer er ist (z. B. Benutzername).

12. Was ist Authentisierung?

Überprüfung, ob der Benutzer wirklich diese Person ist.

13. Nenne ein Beispiel für Authentisierung.

Passwort oder Fingerabdruck.

14. Was ist Autorisierung?

Festlegen, welche Rechte ein Benutzer im System hat.

15. In welcher Reihenfolge laufen die Schritte ab?

Identifikation → Authentisierung → Autorisierung.

16. Was ist ein Hashwert?

Ein verschlüsselter Wert, der aus Eingabedaten berechnet wird.

17. Kann man einen Hash zurückrechnen?

Nein, er ist nicht zurückrechenbar.

18. Was passiert bei kleiner Änderung der Eingabe?

Der Hashwert ändert sich komplett.

19. Was ist eine Kollision?

Zwei verschiedene Eingaben haben denselben Hash.

20. Welcher Hash-Algorithmus ist unsicher?

MD5.

21. Was ist ein Benutzer?

Ein Berechtigungsträger im System.

22. Was ist eine Gruppe?

Eine Sammlung von Benutzern zur Rechtevergabe.

23. Kann man sich mit einer Gruppe anmelden?

Nein.

24. Was ist ein Administrator?

Ein Benutzer mit vollen Systemrechten.

25. Was darf ein Standardbenutzer nicht?

Keine Systemverwaltung durchführen.

26. Was ist der Gast-Account?

Ein Benutzer mit sehr eingeschränkten Rechten.

27. Was ist das System-Konto?

Ein Konto mit sehr hohen Rechten (mehr als Admin).

28. Was ist eine SID?

Eine eindeutige interne Kennung eines Benutzers.

29. Warum ist die SID wichtig?

Sie identifiziert Benutzer eindeutig im System.

30. Wird eine SID wiederverwendet?

Nein, sie ist einmalig.

31. Was ist ein UPN?

User Principal Name (z. B. user @ domain.tld).

32. Was ist der Unterschied zwischen Benutzername und Anzeigename?

Benutzername = Login, Anzeigename = sichtbarer Name.

33. Was macht der Befehl Get-LocalUser?

Zeigt lokale Benutzerkonten an.

34. Was befindet sich im Home-Verzeichnis?

Benutzerspezifische Daten und Einstellungen.

35. Was ist AppData?

Ein Ordner für benutzerspezifische Programmdateien.

36. Was ist ntuser.dat?

Eine versteckte Datei mit Benutzereinstellungen.

37. Warum spart Multiuser Kosten?

Mehrere Nutzer teilen sich ein System.

38. Warum sind Gruppen wichtig?

Sie vereinfachen die Rechteverwaltung.

39. Was bedeutet: Benutzername = Anmeldename?

Beide sind identisch und wichtig für die Verwaltung.

40. Was ist der Unterschied zwischen Authentisierung und Autorisierung?

Authentisierung prüft Identität, Autorisierung legt Rechte fest.

Mein Abgleich der Klausurvorbereitung und PDF von herrn Schlegel

Ergänzung zur Klausurvorbereitung - Benutzermanagement (wichtige Zusatzinfos aus Unterricht/PDF)

Single- vs. Multi-Session (Windows genauer verstehen)

- Windows kann Single-Session und Multi-Session
 - Desktop = meist Single-Session
 - Server / Enterprise = Multi-Session möglich
 - Wichtig: Windows = Multiuser-fähig, aber Sessions sind getrennt
-

Warum Multiuser? (nicht nur „mehr Benutzer“)

- bessere Ressourcennutzung
 - getrennte Benutzerbereiche
 - Schutz vertraulicher Daten
 - abgestufte Rechte
 - Rechtevergabe über Gruppen
-

Login-Prozess (Begriffe sauber können!)

1. Identifikation = Benutzername
 2. Authentisierung = Passwort / Nachweis
 3. Autorisierung = Rechte werden zugewiesen
- Authentifikation = Überbegriff (Prüfung der Angaben)
-

Administrator (wichtige Details!)

- integrierter Administrator existiert, ist oft deaktiviert
 - erster Benutzer bekommt automatisch Adminrechte
 - Admin darf:
 - alles installieren
 - Benutzer verwalten
 - Rechte vergeben
 - System komplett kontrollieren
-

Standardbenutzer (konkret können!)

- darf Programme ausführen
 - darf im eigenen Home schreiben
 - darf andere Dateien nur lesen
 - darf NICHT:
 - Programme installieren
 - Benutzer verwalten
 - System ändern
-

Gastkonto (Klausur-Falle!)

- standardmäßig deaktiviert
 - oft ohne Passwort
 - großes Sicherheitsrisiko → sollte deaktiviert bleiben
-

SYSTEM-Konto (SEHR WICHTIG!)

- internes Konto vom Betriebssystem
 - nicht sichtbar im Benutzer-Manager
 - hat Vollzugriff auf alles → wichtiger als Administrator!
-

Spezielle Systemkonten

- Netzwerkdienst → Netzwerkzugriffe
- Lokaler Dienst → eingeschränkte lokale Rechte
- DefaultAccount → systeminterne Prozesse
- WDAGUtilityAccount → Sicherheitsfunktionen

→ keine normalen Benutzer!

SID (Security Identifier)

- eindeutige interne ID eines Benutzers
 - wird nur einmal vergeben
 - bleibt einzigartig, auch nach Löschen → verhindert Rechteübernahme bei neuem Benutzer
-

Passwort-Speicherung (sehr wichtig!)

- Speicherort: C:\Windows\System32\config\SAM
 - Passwörter werden nicht im Klartext gespeichert
-

Benutzerprofil

- wird beim ersten Login erstellt
 - Pfad: %userprofile%
 - enthält:
 - persönliche Ordner
 - AppData → Programmeinstellungen
 - NTUSER.DAT → Registry vom Benutzer
-

UAC (Benutzerkontensteuerung)

- seit Windows Vista
 - auch Admin arbeitet eingeschränkt
 - Änderungen müssen bestätigt werden → Schutz vor Schadsoftware
-

Wichtige Merksätze

- Windows = Multiuserfähig, aber Session-basiert
- SYSTEM > Administrator (wichtig!)
- Gruppen = nur Rechtevergabe
- Benutzername ≠ entscheidend → SID ist entscheidend
- UAC schützt vor ungewollten Änderungen