

Windows Server 2025

Domäne einrichten & Dateiablage bereitstellen

Schritt-für-Schritt-Anleitung über die GUI

Lernfeld 3 – Clients in Netzwerke einbinden

FISI / FIAE – Umschulung

bfw – Unternehmen für Bildung

1 Einführung

Diese Anleitung beschreibt den kompletten Weg von der Einrichtung einer Active-Directory-Domäne bis zur fertigen Dateiablage mit Berechtigungen und Netzlaufwerken. Alle Schritte erfolgen über die grafische Benutzeroberfläche (GUI).

Lernziele

- Active Directory-Domänendienste (AD DS) installieren und konfigurieren
- Einen Server zum Domänencontroller (DC) heraufstufen
- Organisationseinheiten (OUs), Benutzer und Gruppen anlegen
- Clients in die Domäne aufnehmen
- Die Rolle „Dateiserver“ installieren
- SMB-Freigaben mit Berechtigungen erstellen
- Netzlaufwerke per GPO automatisch zuweisen

Übersicht der Kapitel

Kap.	Thema
1	Einführung
2	Voraussetzungen und Netzwerkplanung
3	Active Directory-Domänendienste installieren
4	Server zum Domänencontroller heraufstufen
5	Organisationseinheiten, Benutzer und Gruppen anlegen
6	Clients in die Domäne aufnehmen
7	Rolle „Dateiserver“ installieren
8	Ordnerstruktur vorbereiten
9	SMB-Freigabe über den Server-Manager erstellen
10	Berechtigungen konfigurieren
11	Alternative: Erweiterte Freigabe im Explorer
12	Freigabe als Netzlaufwerk verbinden
13	Schattenkopien aktivieren
14	Fehlerbehebung
15	Checkliste

Hinweis: Diese Anleitung bezieht sich auf Windows Server 2025 mit Desktop Experience. Die Vorgehensweise gilt analog auch für Server 2022/2019.

2 Voraussetzungen und Netzwerkplanung

Bevor mit der Einrichtung begonnen wird, müssen folgende Voraussetzungen erfüllt sein:

- Windows Server 2025 ist installiert (Desktop Experience)
- Der Server verfügt über eine feste IP-Adresse
- Eine separate Datenpartition (z. B. D:) ist für die Dateiablage vorhanden
- Sie sind als lokaler Administrator angemeldet
- Mindestens ein Client-PC steht im selben Netzwerk bereit

Beispiel-Netzwerkplanung

Komponente	Wert	Bemerkung
Domänenname	bfw-lab.local	Interner DNS-Name
NetBIOS-Name	BFW-LAB	Wird automatisch generiert
Server-IP	192.168.1.10/24	Statisch konfiguriert
Servename	DC01	Hostname des Servers
DNS-Server	192.168.1.10	Zeigt auf sich selbst (DC)
Gateway	192.168.1.1	Router/Firewall
Client-IP-Bereich	192.168.1.100–200	DHCP oder statisch

 **Wichtig:** Der DNS-Server des Domänencontrollers muss als bevorzugter DNS auf sich selbst zeigen (127.0.0.1 oder eigene IP). Alle Clients müssen den DC als DNS-Server verwenden.

3 Active Directory-Domänendienste installieren

Im ersten Schritt wird die Serverrolle für Active Directory installiert. Damit wird der Server noch nicht zum Domänencontroller – das geschieht erst im nächsten Kapitel.

Schritt 1: Server-Manager öffnen

Der Server-Manager startet automatisch nach der Anmeldung.

Schritt 2: Assistent starten

Navigation: Server-Manager → Dashboard → „Rollen und Features hinzufügen“

Klicken Sie auf „Weiter“, bis Sie zur Seite „Installationstyp“ gelangen. Wählen Sie „Rollenbasierte oder featurebasierte Installation“.

Schritt 3: Server auswählen

Wählen Sie den lokalen Server aus der Liste aus und klicken Sie auf „Weiter“.

Schritt 4: Rolle auswählen

Navigation: Serverrollen → Active Directory-Domänendienste

Setzen Sie den Haken bei „Active Directory-Domänendienste“. Es erscheint ein Popup mit abhängigen Features – klicken Sie auf „Features hinzufügen“.

 **Hinweis:** Der DNS-Server wird beim Heraufstufen automatisch mitinstalliert. Sie müssen ihn hier NICHT separat auswählen.

Schritt 5: Installation starten

Klicken Sie durch die restlichen Seiten mit „Weiter“ und dann auf „Installieren“. Die Installation dauert ca. 2–3 Minuten.

Schritt 6: Abschluss

Nach der Installation erscheint im Server-Manager oben rechts ein gelbes Warndreieck mit der Meldung „Konfiguration erforderlich“. Dieses Warndreieck ist der Einstiegspunkt für das nächste Kapitel.

 **Wichtig:** Schließen Sie den Assistenten NICHT und starten Sie NICHT neu, bevor die Rolle installiert ist. Der nächste Schritt (Heraufstufen) erfolgt direkt im Anschluss.

4 Server zum Domänencontroller heraufstufen

Jetzt wird der Server zum Domänencontroller (DC) heraufgestuft. Dabei wird eine neue Gesamtstruktur (Forest) mit einer neuen Domäne erstellt.

Schritt 1: Heraufstufung starten

Navigation: Server-Manager → Benachrichtigungen (gelbes Dreieck) → „Server zu einem Domänencontroller heraufstufen“

Schritt 2: Bereitstellungskonfiguration

Wählen Sie „Neue Gesamtstruktur hinzufügen“ und geben Sie den gewünschten Domännennamen ein.

Füge dem Namen nach „lab“ noch eine Nummer hinzu damit keine Komplikationen im Netzwerk entstehen:

`bfw-lab.local`

Hinweis: Verwenden Sie für Schulungsumgebungen einen local-Namen. In Produktionsumgebungen sollte ein registrierter DNS-Name (z. B. bfw-lab.de) verwendet werden.

Schritt 3: Domänencontrolleroptionen

Konfigurieren Sie die folgenden Einstellungen:

Einstellung	Wert
Gesamtstruktur-Funktionsebene	Windows Server 2016 (oder höher)
Domänen-Funktionsebene	Windows Server 2016 (oder höher)
DNS-Server	Haken setzen (wird mitinstalliert)
Globaler Katalog (GC)	Haken setzen (Standard)
DSRM-Kennwort	Sicheres Passwort vergeben und notieren!

Wichtig: Das DSRM-Kennwort (Directory Services Restore Mode) wird für die Wiederherstellung des AD benötigt. Unbedingt sicher aufbewahren!

Schritt 4: DNS-Optionen

Die DNS-Delegierungswarnung kann in einer Schulungsumgebung ignoriert werden. Klicken Sie auf „Weiter“.

Schritt 5: NetBIOS-Name

Der NetBIOS-Name wird automatisch aus dem Domännennamen abgeleitet:

`BFW-LAB`

Akzeptieren Sie den Vorschlag und klicken Sie auf „Weiter“.

Schritt 6: Pfade

Die Standardpfade für Datenbank, Protokolldateien und SYSVOL können beibehalten werden:

`C:\Windows\NTDS`

`C:\Windows\SYSVOL`

Schritt 7: Voraussetzungsprüfung und Installation

Auf der Zusammenfassungsseite klicken Sie auf „Voraussetzungsprüfung“. Warnungen zu DNS-Delegierung und Kryptografie sind in einer Testumgebung normal und können ignoriert werden.

Klicken Sie auf „Installieren“. Der Server wird automatisch neu gestartet.

Schritt 8: Anmeldung prüfen

Nach dem Neustart melden Sie sich mit dem Domänen-Administratorkonto an:

`BFW-LAB\Administrator`

Im Server-Manager sollte nun unter „AD DS“ und „DNS“ der Server aufgeführt sein.

5 Organisationseinheiten, Benutzer und Gruppen anlegen

Bevor Berechtigungen vergeben werden, müssen Benutzer und Gruppen im Active Directory angelegt werden. Die Strukturierung erfolgt über Organisationseinheiten (OUs).

5.1 Active Directory-Benutzer und -Computer öffnen

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

5.2 Organisationseinheiten (OUs) erstellen

OUs dienen zur logischen Strukturierung und zur Zuweisung von Gruppenrichtlinien.

Schritt 1: OU-Struktur anlegen

Rechtsklick auf die Domäne „bfw-lab.local“ → Neu → Organisationseinheit. Erstellen Sie folgende OUs:

OU-Name	Zweck
_Benutzer	Enthält alle Benutzerkonten
_Gruppen	Enthält alle Sicherheitsgruppen
_Computer	Enthält Client-Computerobjekte
_Server	Enthält Serverobjekte

Hinweis: Der Unterstrich (_) vor dem OU-Namen sorgt dafür, dass die eigenen OUs in der Liste ganz oben stehen und von den Standard-Containern leicht unterscheidbar sind.

5.3 Sicherheitsgruppen erstellen

Schritt 2: Gruppen anlegen

Rechtsklick auf die OU „_Gruppen“ → Neu → Gruppe. Erstellen Sie für jede Abteilung eine Sicherheitsgruppe:

Gruppenname	Bereich	Typ
GRP_Verwaltung	Global	Sicherheit
GRP_Technik	Global	Sicherheit
GRP_Geschaeftsfuehrung	Global	Sicherheit
GRP_Allgemein	Global	Sicherheit

Exkurs: AGDLP-Prinzip (IHK-relevant)

Das AGDLP-Prinzip beschreibt die empfohlene Verschachtelung von Berechtigungen in einer Domäne:

Kürzel	Bedeutung	Beispiel
--------	-----------	----------

A	Account (Benutzerkonto)	m.mueller
G	Globale Gruppe	GRP_Verwaltung
DL	Domänenlokale Gruppe	DL_Verwaltung_Aendern
P	Permission (Berechtigung)	NTFS: Ändern auf D:\Daten\Verwaltung

Reihenfolge: Benutzer (A) → kommt in globale Gruppe (G) → globale Gruppe kommt in domänenlokale Gruppe (DL) → domänenlokale Gruppe erhält NTFS-Berechtigung (P).

[i] Hinweis: In einer Schulungsumgebung mit nur einer Domäne kann vereinfacht auch direkt mit globalen Gruppen (AGP) gearbeitet werden. Das vollständige AGDLP-Prinzip wird relevant, sobald mehrere Domänen im Spiel sind.

5.4 Benutzer anlegen

Schritt 3: Benutzerkonten erstellen

Rechtsklick auf die OU „_Benutzer“ → Neu → Benutzer. Füllen Sie die Felder aus:

Feld	Beispielwert
Vorname	Max
Nachname	Mustermann
Benutzeranmeldename	m.mustermann
Kennwort	Schulung2025!
Kennwort läuft nie ab	Für Schulung: Haken setzen

Schritt 4: Benutzer zu Gruppen hinzufügen

Rechtsklick auf den Benutzer → „Eine Gruppe hinzufügen“ → Gruppenname eingeben (z. B. GRP_Verwaltung) → OK.

6 Clients in die Domäne aufnehmen

Jeder Client-PC, der auf die Dateiablage zugreifen soll, muss Mitglied der Domäne werden.

6.1 Voraussetzung: DNS umstellen

Schritt 1: DNS auf dem Client ändern

Der Client muss den Domänencontroller als DNS-Server verwenden. Öffnen Sie auf dem Client:

Navigation: *Einstellungen → Netzwerk und Internet → Adapteroptionen → Adapter → Eigenschaften → IPv4*

Tragen Sie als bevorzugten DNS-Server die IP des DC ein:

192.168.1.10

6.2 Domänenbeitritt

Schritt 2: Systemeigenschaften öffnen

Navigation: *Rechtsklick auf „Dieser PC“ → Eigenschaften → „Domäne oder Arbeitsgruppe“ → Ändern*

Alternativ: Windows-Taste + R → sysdm.cpl → Registerkarte „Computernamen“ → Ändern.

Schritt 3: Domäne eingeben

Wählen Sie „Domäne“ und geben Sie den Domänennamen ein:

VERGISS DIE NUMMER NICHT!

bfw-lab.local

Schritt 4: Authentifizierung

Es erscheint ein Anmeldefenster. Geben Sie die Anmeldedaten eines Domänenadministrators ein:

BFW-LAB\Administrator

Nach erfolgreicher Authentifizierung erscheint „Willkommen in der Domäne bfw-lab.local“.

Schritt 5: Neustart

Der Client muss neu gestartet werden. Anschließend können sich Domänenbenutzer anmelden.

 **Hinweis:** Nach dem Domänenbeitritt erscheint der Computer in Active Directory unter „Computers“. Verschieben Sie ihn in Ihre OU „_Computer“ für eine saubere Strukturierung.

Schritt 6: Anmeldung testen

Melden Sie sich auf dem Client mit einem Domänenkonto an:

BFW-LAB\m.mustermann

Prüfen Sie mit „whoami“ in der Eingabeaufforderung, ob die Domänenanmeldung funktioniert.

7 Rolle „Dateiserver“ installieren

Die Dateiserverrolle ist Voraussetzung für SMB-Freigaben über den Server-Manager.

Schritt 1: Assistent starten

Navigation: Server-Manager → Dashboard → „Rollen und Features hinzufügen“

Schritt 2: Dateiserverrolle auswählen

Navigation: Serverrollen → Datei- und Speicherdienste → Datei- und iSCSI-Dienste → Dateiserver

Haken bei „Dateiserver“ setzen. Optional: „Ressourcen-Manager für Dateiserver“ für Kontingente.

Schritt 3: Installieren

Auf „Weiter“ und „Installieren“ klicken. Neustart ist nicht erforderlich.

 **Hinweis:** Prüfen: Server-Manager → Datei- und Speicherdienste → „Freigaben“ muss nun verfügbar sein.

8 Ordnerstruktur vorbereiten

Vor dem Erstellen der Freigaben eine durchdachte Ordnerstruktur auf der Datenpartition anlegen.

Schritt 1: Datenpartition öffnen

Im Explorer zum Datenlaufwerk navigieren (z. B. D:).

Schritt 2: Stammordner erstellen

D:\Daten

Schritt 3: Abteilungsordner anlegen

D:\Daten\Verwaltung

D:\Daten\Technik

D:\Daten>Allgemein

D:\Daten\Projekte

 **Wichtig:** Freigaben niemals auf der Systempartition (C:) erstellen! Eigene Datenpartition verwenden.

Best Practices Ordnerstruktur

Namenskonvention	Einheitliche Namen ohne Sonderzeichen und Leerzeichen
Verschachtelung	Flache Hierarchie (max. 3–4 Ebenen)
Trennung	Abteilungs-, Projekt- und persönliche Daten trennen
Dokumentation	Ordnerstruktur und Berechtigungskonzept dokumentieren

9 SMB-Freigabe über den Server-Manager erstellen

Schritt 1: Freigabenverwaltung öffnen

Navigation: Server-Manager → Datei- und Speicherdienste → Freigaben

Schritt 2: Neue Freigabe starten

Rechts oben auf „Aufgaben“ → „Neue Freigabe“.

Schritt 3: Freigabeprofil wählen

Profil	Beschreibung
SMB-Freigabe – Schnell	Einfache Dateifreigabe. Empfohlen für den Einstieg.
SMB-Freigabe – Erweitert	Zusätzlich: Dateiklassifizierung, Kontingente.
NFS-Freigabe – Schnell	Für Linux/UNIX-Clients.

„SMB-Freigabe – Schnell“ wählen und „Weiter“ klicken.

Schritt 4: Freigabeort festlegen

„Benutzerdefinierten Pfad eingeben“:

D:\Daten\Verwaltung

Schritt 5: Freigabename vergeben

Aussagekräftigen Namen eingeben:

\\DC01\Verwaltung

Schritt 6: Freigabeoptionen

Option	Wirkung	Empfehlung
Zugriffsbasierte Aufzählung (ABE)	Benutzer sehen nur Ordner mit Zugriff.	Aktivieren
Zwischenspeichern	Offline-Zugriff (Caching).	Deaktivieren
BranchCache	Zweigstellen-Caching.	Je nach Standort
Verschlüsselung	SMB-Verschlüsselung für Remotezugriff.	Aktivieren

Schritt 7: Berechtigungen

Auf „Berechtigungen anpassen“ klicken – Details im nächsten Kapitel.

Schritt 8: Erstellen

Zusammenfassung prüfen → „Erstellen“.

10 Berechtigungen konfigurieren

Beim Netzwerkzugriff werden zwei Berechtigungsebenen ausgewertet. Es gilt immer die restriktivere.

10.1 Freigabe- vs. NTFS-Berechtigungen

	Freigabeberechtigung	NTFS-Berechtigung
Geltungsbereich	Nur Netzwerkzugriff	Lokal + Netzwerk
Granularität	Lesen, Ändern, Vollzugriff	Feingranular (13 Einzelrechte)
Vererbung	Keine	Ja (Unterordner)
Best Practice	„Jeder: Vollzugriff“	Steuerung komplett über NTFS

⚠ Wichtig: Best Practice: Freigabeberechtigung auf „Jeder: Vollzugriff“. Zugriffssteuerung komplett über NTFS.

10.2 NTFS-Berechtigungen setzen

Schritt 1: Ordneigenschaften öffnen

Im Explorer zum Datenlaufwerk navigieren (z. B. D:\Daten\Verwaltung).

Rechtsklick auf Ordner → Eigenschaften → Registerkarte „Sicherheit“.

Schritt 2: Vererbung deaktivieren

„Erweitert“ → „Vererbung deaktivieren“ → „In explizite Berechtigungen konvertieren“.

Schritt 3: Berechtigungen zuweisen

„Bearbeiten“ → „Hinzufügen“ → Domänengruppen auswählen:

Gruppe	Berechtigung	Anwenden auf
BFW-LAB\Domänen-Admins	Vollzugriff	Ordner, Unterordner, Dateien
BFW-LAB\GRP_Verwaltung (Diese Gruppe ändert sich für JEDEN Ordner)	Ändern	Ordner, Unterordner, Dateien
BFW-LAB\GRP_Geschaeftsfuehrung	Lesen	Ordner, Unterordner, Dateien
SYSTEM	Vollzugriff	Ordner, Unterordner, Dateien

i Hinweis: Wiederholen Sie diesen Vorgang für jeden Abteilungsordner mit den jeweils passenden Gruppen. Für den Ordner: „Projekte“ soll die Gruppe: „Domänen-Benutzer“ verwendet werden.

11 Alternative: Erweiterte Freigabe im Explorer

Für eine schnelle Einzelfreigabe:

1. Rechtsklick auf Ordner → „Eigenschaften“
2. Registerkarte „Freigabe“ → „Erweiterte Freigabe“
3. „Diesen Ordner freigeben“ aktivieren
4. Freigabennamen eingeben
5. „Berechtigungen“ → Gruppen hinzufügen
6. OK

Nachteil: ABE und Verschlüsselung nicht direkt konfigurierbar. Server-Manager empfohlen.

12 Freigabe als Netzlaufwerk verbinden

12.1 Manuell über den Explorer

1. Windows Explorer öffnen
 2. „Dieser PC“ → „Netzlaufwerk verbinden“
 3. Laufwerksbuchstaben wählen und Pfad eingeben
 4. „Verbindung bei Anmeldung wiederherstellen“ aktivieren
 5. „Fertig stellen“
- \\DC01\Verwaltung

12.2 Automatisch per Gruppenrichtlinie (GPO)

In der Domäne können Netzlaufwerke zentral und automatisch per GPO zugewiesen werden.

Schritt 1: Gruppenrichtlinienverwaltung öffnen

Navigation: Server-Manager → Tools → Gruppenrichtlinienverwaltung

Schritt 2: Neue GPO erstellen

Rechtsklick auf die OU „_Benutzer“ (oder die gesamte Domäne) → „Gruppenrichtlinienobjekt hier erstellen und verknüpfen“. Name: „Netzlaufwerke zuweisen“.

Schritt 3: GPO bearbeiten

Navigation: Rechtsklick auf die neue GPO → Bearbeiten

Navigation: Benutzerkonfiguration → Einstellungen → Windows-Einstellungen → Laufwerkszuordnungen

Schritt 4: Neues Laufwerk hinzufügen

Rechtsklick → Neu → „Zugeordnetes Laufwerk“. Konfigurieren Sie:

Einstellung	Wert
Aktion	Erstellen
Speicherort	\\DC01\Verwaltung
Bezeichnung	Verwaltung
Laufwerksbuchstabe	V:
Verbindung wiederherstellen	Haken setzen

Schritt 5: Zielgruppenadressierung einrichten

Klicken Sie auf die Registerkarte „Allgemein“ und setzen Sie den Haken bei „Zielgruppenadressierung auf Elementebene“. Klicken Sie auf „Adressierung“.

Wählen Sie „Neues Element“ → „Sicherheitsgruppe“ drücke auf die „...“ und geben Sie die Gruppe ein:

GRP_Verwaltung

So erhält nur die Verwaltungsgruppe das Laufwerk V:.

Schritt 6: Weitere Laufwerke hinzufügen

Wiederholen Sie den Vorgang für jede Abteilung mit eigenem Laufwerksbuchstaben:

Gruppe	Pfad	Laufwerk	Bezeichnung
GRP_Verwaltung	\\DC01\\Verwaltung	V:	Verwaltung
GRP_Technik	\\DC01\\Technik	T:	Technik
GRP_Allgemein	\\DC01\\Allgemein	G:	Allgemein
Domänen-Benutzer	\\DC01\\Projekte	P:	Projekte

Schritt 7: GPO-Anwendung testen

Melden Sie sich auf einem Client-PC ab und wieder an. Die Netzlaufwerke sollten automatisch verbunden sein. Zur sofortigen Übernahme können Sie auf dem Client folgenden Befehl ausführen:

```
gpupdate/force
```

13 Schattenkopien aktivieren

Schattenkopien ermöglichen Benutzern, frühere Dateiversionen selbstständig wiederherzustellen.

1. Rechtsklick auf Datenlaufwerk (D:) in der Datenträgerverwaltung
2. „Schattenkopien konfigurieren“
3. Laufwerk wählen → „Aktivieren“
4. Zeitplan festlegen (Standard: 7:00 und 12:00 Uhr)
5. Speicherlimit: 10–20% des Laufwerks

 **Wichtig:** Schattenkopien ersetzen KEIN Backup! Nur Schutz vor versehentlichem Löschen/Ändern.

14 Fehlerbehebung

Problem	Lösung
Domänenbeitritt schlägt fehl	DNS auf Client prüfen: Muss auf DC zeigen. nslookup bfw-lab.local testen.
Benutzer kann sich nicht anmelden	Konto gesperrt? Kennwort abgelaufen? In AD-Benutzer prüfen.
Freigabe nicht sichtbar	Netzwerkerkennung aktivieren. Firewall prüfen (SMB, Port 445).
Zugriff verweigert	Freigabe- UND NTFS-Rechte prüfen. Gruppenmitgliedschaft kontrollieren.
Netzlaufwerk per GPO fehlt	gpupdate /force ausführen. GPO-Verknüpfung und Zielgruppe prüfen.
Ordner trotz Berechtigung unsichtbar	ABE aktiv? Mindestens Leserechte erforderlich.
Lange Pfadnamen	Server 2025 unterstützt lange Pfade. Auf Clients GPO aktivieren.

15 Checkliste

Teil A: Domäne einrichten

- ☐ Server hat feste IP-Adresse
- ☐ AD DS-Rolle installiert
- ☐ Server zum DC heraufgestuft (neue Gesamtstruktur)
- ☐ DNS-Server läuft auf DC
- ☐ OUs angelegt (_Benutzer, _Gruppen, _Computer, _Server)
- ☐ Sicherheitsgruppen erstellt
- ☐ Benutzerkonten angelegt und Gruppen zugewiesen
- ☐ Clients: DNS auf DC umgestellt
- ☐ Clients der Domäne beigetreten
- ☐ Domänenanmeldung auf Client getestet

Teil B: Dateiablage bereitstellen

- ☐ Rolle „Dateiserver“ installiert
- ☐ Separate Datenpartition vorhanden
- ☐ Ordnerstruktur angelegt und dokumentiert
- ☐ SMB-Freigaben erstellt
- ☐ ABE aktiviert
- ☐ SMB-Verschlüsselung aktiviert
- ☐ Freigabeberechtigungen: „Jeder: Vollzugriff“

- ☐ NTFS-Berechtigungen nach Least-Privilege-Prinzip
- ☐ Schattenkopien aktiviert
- ☐ Netzlaufwerke per GPO mit Zielgruppenadressierung zugewiesen
- ☐ Zugriff vom Client getestet
- ☐ Berechtigungskonzept schriftlich dokumentiert