Serverdienste in Betrieb nehmen

LB123-03

Adrian Bhend

CSBE | ZIEGELSTRASSE 64
3000 Bern 14

Erstellt am: 28.11.2024
Version 1.0

Inhalt

Einleitung

Diese Anleitung unterstützt Administratoren bei der Inbetriebnahme von Serverdiensten und dem Aufbau einer stabilen Domänenstruktur. Ziel ist ein zentralisiertes Netzwerkmanagement, das Benutzer und Ressourcen effizient verwaltet sowie die Sicherheit und Leistung steigert.

Der Fokus liegt auf der Implementierung einer Domänenstruktur zur Verwaltung von Benutzerkonten, Gruppen und Freigaben. Dazu werden Dienste wie Active Directory Domain Services (AD DS), DNS, DHCP und Gruppenrichtlinien eingerichtet, die eine sichere und effektive Arbeitsumgebung ermöglichen.

Wichtige Aufgaben umfassen die Bereitstellung von Gruppenlaufwerken für Teams sowie persönlichen Homelaufwerken für Benutzer. Letztere dienen der individuellen Datenspeicherung und fördern Vertraulichkeit. Zudem werden Benutzerprofile serverseitig gespeichert, damit Benutzer ihre Einstellungen an jedem Arbeitsplatz beibehalten können.

Ein weiterer Schwerpunkt ist die Automatisierung der Softwareverteilung. Der Server installiert Software-Pakete automatisch auf vernetzten Clients, spart Zeit und stellt sicher, dass alle Geräte einheitlich konfiguriert sind.

Die Dokumentation beschreibt die Erstellung einer leistungsfähigen Domänenstruktur mit zentraler Verwaltung, automatisierten Prozessen und einer sicheren, stabilen Netzwerkumgebung.

Diese Anleitung richtet sich an IT-Administratoren, die mit der Einrichtung von Servern und Netzwerken betraut sind. Schritt für Schritt werden die notwendigen Konfigurationen erläutert, sodass alle beschriebenen Ziele erfolgreich umgesetzt werden können. Jede Aufgabe wird mit einer klaren Struktur erklärt, um eine maximale Nachvollziehbarkeit und Umsetzbarkeit zu gewährleisten.

1. Informationen

nachname.local in einem Privaten Netzwerk der Klasse B mit der IP-Adresse 172.16.1.10 und der Subnetzmaske /24.

Es braucht drei Virtuelle Maschinen, einen Windows Server 2019, eine IpFire und eine Windows 10 Maschine.

Gerät	NIC[1] der VM
Client, Windows 10	LAN-Segment green, IP- und DNS-Adresse automatisch beziehen.
Server, Windows 2019	IP - und DNS-Adresse von der Firewall Manuell zuweisen.
IP-Fire	NAT und LAN-Segment green

Tabelle 1 -NIC

Gerätetyp	Name	IP-Adresse	Betriebssystem	Rolle	Hardwaredetails
Server	nachname10	172.16.1.10	Windows Server 2019	Domain Controller	2x HDD (C: OS, D: Daten), 16 GB RAM
Client-PC	client01-04	172.16.1.101	Windows 10 Pro	Arbeitsstation	8 GB RAM, 500 GB SSD
Firewall	ipfire01	172.16.1.1	IPFire 2.27	Firewall	4 GB RAM, 20 GB HDD

Tabelle 2 – VM-Konfiguration

Folgende Dokumente sollten vorhanden sein oder werden erstellt:

➢ Namenskonzept	➢ Benutzerkonzept
➢ Freigabekonzept	➢ Benutzermatrix
➢ Netzwerkplan logisch, sowie physisch	➢ Adresskonzept
➢ IP-Adresskonzept	

Tabelle 3 - Übersicht

1.1 Konten und Gruppen – Zugriff und Berechtigung

Benutzername	Globale Gruppe	Domänenlokale Gruppe	Laufwerkzuordnung	OU
user01	grp1	DL_grp1	P: W:	Passwort, Desktop
user02	grp1	DL_grp1	P: W:	Passwort, Desktop
user03	grp2	DL_grp2	S: W:	Passwort, System
user04	grp2	DL_grp2	S: W:	Passwort, System
admin	Admins	DL_grp1, DL_grp2	P: S: W:	Adminrechte

Tabelle 4 – Konten und Gruppen

[1] Network interface Card

1.2 Computer

- Client01- 04

1.3 Richtlinien

- Die Benutzer sollen genötigt werden, ihre Kennwörter häufiger zu wechseln.
- Es sollen weitere wichtige Kennwortoptionen implementiert werden.
- Es soll verfolgt werden, wer auf wichtige Dateien zugreift.
- Es soll verfolgt werden wer wichtige Dateien wann druckt.

1.4 Drucker

- Zugriff auf mehrere Drucker.
- Den Drucker der Abteilung BH sichern.

1.5Laufwerke

Daten (D:)	(User 01, User 02, Admin)
BH (D:)	(User 03, User 04, Admin)
DB (D:)	(Alle)

Tabelle 5 - Laufwerke

1.6 VPN – Registry - DWORD

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent
DWORD : AssumeUDPEncapsulationContextOnSendRule

1.7 Softwarepaket

MSI-Paket scite-5.1.5x64.ms

1.8 Loginscript erstellen

grp1.bat
net use P: \\nachname10.nachname.local\Daten /persistent:yes
net use W: \\nachname10.nachname.local\DB /persistent:yes

grp2.bat
net use S: \\nachname10.nachname.local\BH /persistent:yes
net use W: \\nachname10.nachname.local\DB /persistent:yes

admin.bat
net use P: \\nachname10.nachname.local\Daten /persistent:yes
net use S: \\nachname10.nachname.local\DB /persistent:yes
net use W: \\nachname10.nachname.local\BH /persistent:yes

2. Planen – Zeitplan

Datum	28.11.2024	abgeschlossen

Pos	Arbeitspaket	Zeit	Dauer		Arbeitstag									
		in Stunden	Start	Ende	1	2	3	4	5	6	7	8	9	10
1	**Information**		**Datum**	**Datum**										
1.1	Aufträge lesen	0.5	28.11.2024	28.11.2024										
1.2	Recherchieren Internet	0.5-1	28.11.2024	28.11.2024										
1.3	Herdt Unterlagen lesen	0.5-1	28.11.2024	28.11.2024										
1.4	Informieren über LBV	0.5	28.11.2024	28.11.2024										
1.5	Dozent Fragen	0.25	28.11.2024	28.11.2024										
1.6	Mitschüler fragen	0.25	28.11.2024	28.11.2024										
2.	**Planung**													
2.1	Zeitplanerstellen	1	29.11.2024	30.11.2024										
2.2	Dokument Vorlage erstellen/bearbeiten	1	29.11.2024	30.11.2024										
2.3	Was für Bilder verwende ich, wie setzte ich diese ein	0.5	29.11.2024	30.11.2024										
2.4	Anordnung der Aufträge	0.5	29.11.2024	30.11.2024										
2.5	Aufträge Planen, welche Informationen nutze ich.	1-2	03.11.2024	03.11.2024										
2.6	Informationen und Planung, wie umsetzen	1-2	03.11.2024	03.11.2024										
2.7	Entscheiden, wie umsetzten	1-2	03.11.2024	03.11.2024										
2.8	Realisieren, Kontrolieren und Auswerten wie umsetzen	1-2	03.11.2024	03.11.2024										
3.	**Entscheiden**													
3.1	Nutze die Vorlage von der Schule	0.25	04.12.2024	04.12.2024										
3.2	Ratschläge des Dozenten nutzen	0.25	04.12.2024	04.12.2024										
3.3	Hinweise beachten	0.25	04.12.2024	04.12.2024										
3.4	Doku starten	1	04.12.2024	04.12.2024										
3.5	Wie Aufträge 01-13 in der Doku erfassen mit IPERKA	1	04.12.2024	04.12.2024										
4.	**Realisieren**													
4.1	Auftrag 03-04	1-2	05.12.2024	07.12.2024										
4.2	Auftrag 05-06	1-2	05.12.2024	07.12.2024										
4.3	Auftrag 06-07	1-2	05.12.2024	07.12.2024										
4.4	Auftrag 07-09	1-2	07.12.2024	08.12.2024										
4.5	Auftrag 10-13	1-2	08.12.2024	08.12.2024										
5.	**Kontrollieren**													
5.1	Auftrag 03-04	0.25-0.5	07.12.2024	07.12.2024										
5.2	Auftrag 05-06	0.25-0.5	07.12.2024	07.12.2024										
5.3	Auftrag 06-07	0.25-0.5	07.12.2024	07.12.2024										
5.4	Auftrag 07-09	0.25-0.5	08.12.2024	08.12.2024										
5.5	Auftrag 10-13	0.25-0.5	08.12.2024	08.12.2024										
5.6	Doku kontrollieren	0.25-0.5	08.12.2024	08.12.2024										

Tabelle 6 - Zeitplan

2.1 IP-Adresskonzept

Das Adresskonzept dient der Zuordnung und im Netzwerk, um eine übersichtliche Struktur zu erhalten die möglichst einfach zu verwalten ist

Gerätetyp	Anzahl	Subnetz	IP-Bereich	Gateway	DNS
Server	1	172.16.1.0/24	172.16.1.10	172.16.1.1	172.16.1.10
Clients	4	172.16.1.0/24	172.16.1.101-104	172.16.1.1	172.16.1.10
Drucker	2	172.16.1.0/24	172.16.1.50-51	172.16.1.1	172.16.1.10

Tabelle 7 - Adresskonzept

2.3 Benutzermatrix

Laut Auftrag sind diese Vorgaben für eine Benutzermatrix zu nutzen. User greifen über Windows 10 auf den Server zu und werden bestimmten Laufwerken zugeordnet.

Benutzername	Globale Gruppe	Domänenlokale Gruppe	Laufwerkzuordnung	OU
user01	grp1	DL_grp1	P: W:	Passwort, Desktop
user02	grp1	DL_grp1	P: W:	Passwort, Desktop
user03	grp2	DL_grp2	S: W:	Passwort, System
user04	grp2	DL_grp2	S: W:	Passwort, System
admin	Admins	DL_grp1, DL_grp2	P: S: W:	Adminrechte

Tabelle 8 - Benutzermatrix

2.4 Inventarblatt

Das Inventar Blatt orientiert über die Adressierung und gibt eine Übersicht über den Inhalt und den Aufbau der Virtuellen Maschinen sowie allen Gerätetypen.

Gerätetyp	Name	IP-Adresse	Betriebssystem	Rolle	Hardwaredetails
Server	nachname10	172.16.1.10	Windows Server 2019	Domain Controller	2x HDD (C: OS, D: Daten), 16 GB RAM
Client-PC	client01-04	172.16.1.101	Windows 10 Pro	Arbeitsstation	8 GB RAM, 500 GB SSD
Netzwerkdrucker	printer1	172.16.1.50	HP	Druckserver	Schwarzweiss, 22 Seiten/min
Firewall	ipfire01	172.16.1.1	IPFire 2.27	Firewall	4 GB RAM, 20 GB HDD
Vierenschutz	MS Defender	Windows	Windows	Antivirus	Min. Anforderung Betriebssystem

Tabelle 9 - Inventarblatt

2.5 Freigabe

Die Freigabe dient zur Übersicht und Orientierung für die Berechtigungen auf den Laufwerken.

Verzeichnis	Freigabename	Gruppenberechtigungen	NTFS-Berechtigungen	Bemerkungen
D:\Daten	Daten	DL_grp1: Lesen/Schreiben	DL_grp1: Ändern	Allgemeine Daten
D:\BH	BH (Buchhaltung)	D:\BH BH DL_grp2: Lesen/Schreiben	DL_grp2: Ändern	Buchhaltungsdaten
D:\DB	DB (Datenbank)	DL_grp1/DL_grp2: Lesen/Schreiben	DL_grp1/DL_grp2: Ändern	Gemeinsame Datenbankdaten

Tabelle 10 - Feigabe

2.7 Loginscripte

grp1.bat (user01 und user02)
```
net use D: \\bhend10.bhend.local\Daten /persistent:yes
net use D: \\bhend10.bhend.local\DB /persistent:yes
```

grp2.bat (user03 und user04)
```
net use D: \\bhend10.bhend.local\BH /persistent:yes
net use D: \\bhend10.bhend.local\DB /persistent:yes
```

admin.bat (admin)
```
net use D: \\bhend10.bhend.local\Daten /persistent:yes
net use D: \\bhend10.bhend.local\DB /persistent:yes
net use D: \\bhend10.bhend.local\BH /persistent:yes
```

3.Entscheiden

Ich entscheide mich dafür die Vorlagen aus der Planung zu übernehmen. Und da es in diesem Fall klare Vorgaben gibt, gibt es nicht viel mehr zu entscheiden.

4. Realisieren

4.1 IpFire Installation

VM-Starten und konfigurieren, 4 GB RAM, 20 GB HDD, IOS: ipfire-2.27.x86_64-full-core166 wie gewohnt in die VM laden und installieren, nach der Installation IpFire konfigurieren → Tastaturbelegung →Zeitzone → Hostname → Domainname → Passwort definieren → Typ der Netzwerkkonfiguration: RED+GREEN → Netzwerkzuordnung: Zugewiesene Netzwerkkarten, erst ROT zuweisen, dann GREEN → Adresseinstellungen: GREEN: Aus Konzept übernehmen, RED: DHCP markieren → DHCP-Server Konfiguration: Nie, nie, nie, nie, nie, nie bei einem Server aktivieren.

4.2 Server konfigurieren

Einrichten der grundlegenden Serverkonfiguration, einschliesslich der Zuweisung einer statischen IP-Adresse, Benennung des Servers, Hinzufügen zur Domäne und grundlegender Firewall-Einstellungen.

<table>
<tr><td>Windows Server starten, anmelden und lokaler Server wählen im Server Manager.
Netzwerkadapter öffnen, (green) rechtsklick Eigenschaften Ipv6 deaktivieren, Ipv4 auswählen und auf Eigenschaften klicken, IP-Adresse und den DNS konfigurieren.</td><td colspan="3"><table>
<tr><th>Einstellung</th><th>Beschreibung</th><th>Wert</th></tr>
<tr><td>IP-Adresse</td><td>Statische IP-Adresse des Servers</td><td>172.16.1.1</td></tr>
<tr><td>Subnetzmaske</td><td>Definiert das Subnetz</td><td>255.255.255.0</td></tr>
<tr><td>Standard-Gateway</td><td>Adresse des Routers</td><td>172.16.1.1</td></tr>
<tr><td>DNS-Server Primär</td><td>Primärer DNS-Server</td><td>172.16.1.10</td></tr>
<tr><td>DNS-Server Sekundär</td><td>Sekundärer DNS-Server</td><td>172.16.1.1</td></tr>
<tr><td>DHCP aktiviert</td><td>Ob DHCP aktiviert ist</td><td>Nein</td></tr>
</table></td></tr>
<tr><td>Tools und Updates</td><td colspan="3">ISO für Vmware Tools Version 11 laden im virtuellen Laufwerk der VM und installieren.
Im Server Manager bei Lokale Server auf «Nur Updates mithilfe von….» klicken. Und abwarten ggf. neustarten.</td></tr>
<tr><td>Serverbezeichnung ändern</td><td colspan="3">Auf Computername Klicken dann auf Ändern. Name nach Vorgabe ändern (nachname10) dann auf ok klicken. Dann schliessen. Server neu starten. Nach den Updates wäre mein Vorschlag.</td></tr>
<tr><td>Rolle</td><td>Beschreibung</td><td>Status</td><td>Anmerkungen</td></tr>
<tr><td>Windows Defender Antivirus</td><td>Schutz des Servers vor Malware und anderen Bedrohungen.</td><td>Aktiviert</td><td>Regelmässige Updates und Scans konfiguriert</td></tr>
</table>

Tabelle 11 – Server Konfiguration

Jetzt ist ein guter Zeitpunkt, um ein Snapshot von der VM zu machen!
Mit dem aktuellen Datum der Updates

4.3 Active Directory Domain Services einrichten

Installation und Konfiguration von AD DS. Erstellung einer neuen Gesamtstruktur (Domäne) mit dem Namen nachname.local, Konfiguration der Funktionsebenen und Hinzufügen des ersten Domänencontrollers.

Rollen installieren	Servermanager → Verwalten → Rollen und Features hinzufügen → zu Serverrollen navigieren → Active Directory-Domänendienste (AD DS) markieren, DHCP, DNS, Druck- und Dokumentdienste markieren → Features hinzufügen → bestätigen, weiter → Installieren. Server startet neu. ADDS, DNS DHCP und Druckdienste sind installiert.
Domänencontroller festlegen	Nach Installation: DNS-Benachrichtigung anklicken → Server zum Domänencontroller heraufstufen → Neue Gesamtstruktur hinzufügen → nachname.local → Passwort festlegen → Hinweise ignorieren → weiter → prüfen und installieren. Server startet neu. ADDS ist installiert

Tabelle 12 - ADDS

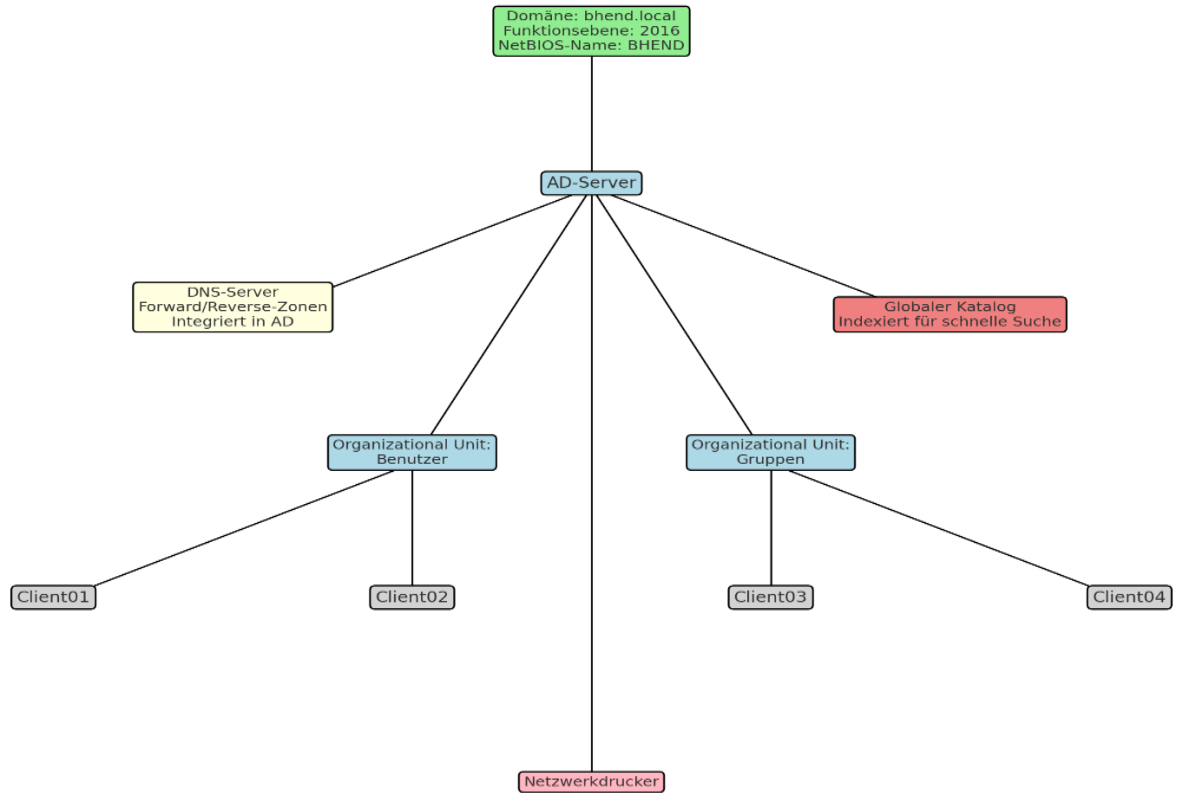


Abbildung 1 – Logischer Plan

4.4 DNS konfigurieren

Konfiguration des DNS-Servers, einschliesslich Forward-Lookupzonen und Reverse-Lookupzonen, um die Namensauflösung innerhalb der Domäne sicherzustellen. Eintragen von Host-A-Einträgen für Server und Clients.

Server Manager → Tools → DNS → Servernamen expandieren, Forward/Reverse Lookup öffnen, rechtsklick auf Server → Eigenschaften.	➢ Stammhinweise: Root-Server-Einträge.
Im Knoten nachname.local sieht man die DNS-Verwaltung mit Forward-Lookupzonen, speziell für die Zone bhend.local.	➢ SOA (Start of Authority): Gibt den primären Server der Zone an. ➢ NS (Nameserver): Zeigt den Nameserver für die Zone. A-Einträge (Host A): Zeigt IP-Adressen für Hostnamen (172.16.1.10 für bhend10)
Forward Lookupzonen	nachname.local → Eigenschaften → Registerkarte Allgemein: sichere und unsichere Updates zulassen → Registerkarte Zonenübertragung: zulassen markieren → übernehmen und OK
Reverse Lookupzonen	Reverse-Lookupzonen → Neue Zone, Assistent startet → weiter → Primäre Zone → weiter → in der Gesamtstruktur → weiter → Ipv4 → weiter → 172.16.1 → weiter → Nicht sichere und sichere Updates zulassen → weiter → Fertig stellen
nslookup	Lokale Server → IP-Adresse → NIC → Eigenschaften, iPv4 → Eigenschaften, DNS ändern zu 172.16.1.10 und 172.16.1.1 → OK → schliessen Server Manager → Tools → DNS → Servername → nslookup → exit eingeben → ipconfig /registerdns → ausführen → exit → nslookup Standard-Server ist servename.nachname.local

Tabelle 13 - DNS

4.5 DHCP-Server konfigurieren

Einrichtung eines DHCP-Servers zur automatischen Zuweisung von IP-Adressen an Clients. Festlegen eines Adressbereichs, Reservierungen und Konfiguration von Optionen wie Gateway und DNS-Server.

DHCP-Server autorisieren	Servermanager → Benachrichtigung → DHCP-Konfiguration abschliessen
DHCP-Server konfigurieren	Server Manager → Tools → DHCP → Servername.nachname.local → Ipv4 → Neuer Bereich → Beschreibung → weiter → Adresskonzept nutzen, länge einstellen → weiter → Lease 1h → weiter → Ja → weiter → 172.16.1.1 → Hinzufügen → weiter → Servername → Auflösen → Hinzufügen → weiter → weiter → Ja → weiter → Fertig stellen

Tabelle 14 - DHCP

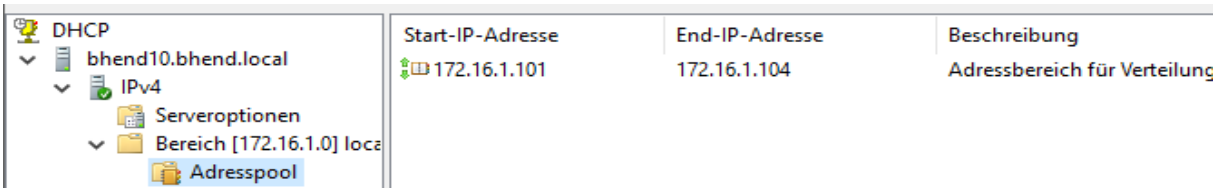


Abbildung 2 – DHCP

4.6 VPN

Rolle installieren	Servermanager → Verwalten → Rollen und Features hinzufügen → zu Serverrollen navigieren → Remotezugriff markieren → Features → RAS-Verbindungs-Manager-Verwaltungskit markieren → weiter → Rollendienste DirectAcces und VPN markieren → Webserver nicht beachten und hinzufügen → weiter → Installieren → Schliessen.
RAS konfigurieren	Tools → Routing und RAS → nachname10 → Routing RAS Konfiguration aktivieren → weiter → Benutzerdefinierte Konfiguration → VPN-Zugriff → Fertigstellen → Dienst starten → nachname10 → Eigenschaften → Nur LAN-Routing → Übernehmen → Sicherheit → Authentifizierungsmethoden → Nur MS-CHAP v2, CHAP, PAP und IKEv2 markieren → Windows-Kontoführung → Übernehmen → Neu starten → IPv6 Prafixzuweisung: Löschen → Übernehmen → OK

Benutzer erstellen	Tool → AD-Benutzer und Computer → nachname.local → Neu → Benutzer → VN: VPN, NA: Test, Benutzeranmeldename: vpn → weiter → Benutzer kann Kennwort nicht ändern und Kennwort läuft nie ab → Passwort eingeben → weiter → Fertig stellen → VPN Test → Eigenschaften → Einwählen, Zugriff gestatten → Übernehmen → OK
Remote Verbindung im Server aktivieren	Server Manager → Lokale Server → Remotdesktop → Aktivieren → Remoteverbindung mit diesem Computer zulassen → Entfernen: Verbindung nur von Computer… → Übernehmen → OK
DWORD und Registry	Server Registry Editor öffnen → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent → Neu → DWORD : AssumeUDPEncapsulationContextOnSendRule → Wert: 2 Hex
Windows Firewall	Server → Windows Defender mit erweiterter Sicherheit → Neue Eingehende Regel → Regeltyp: Benutzerdefiniert → Programm: Alle → Zwei Regeln erstellen mit Protokoll: GRE und TCP 1723
Remote Verbindung im Client aktivieren	Windows VPN öffnen → Verbindungsname: M123TestVPN → IP: 172.16.1.10 → VPN-Typ: Automatisch → Anmeldung: Benutzername und Kennwort -> Verbinden

Tabelle 15 - VPN

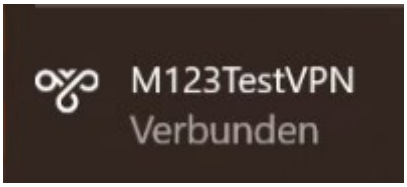


Abbildung 3 -VPN

Ein VPN (Virtual Private Network) bietet eine sichere und verschlüsselte Verbindung über ein unsicheres Netzwerk, wie das Internet. Es ermöglicht Benutzern, remote auf das Netzwerk zuzugreifen, als wären sie physisch vor Ort. Die Hauptfunktionen umfassen:

- Sicherheit: Daten werden durch Verschlüsselung vor Abhörung und Manipulation geschützt.
- Authentifizierung: Nur autorisierte Benutzer haben Zugriff.
- Privatsphäre: Maskierung der IP-Adresse des Benutzers.
- Fernzugriff: Ermöglicht Mitarbeitern, sich von überall aus mit dem Unternehmensnetzwerk zu verbinden.
- Standortübergreifende Netzwerke: Verbindet mehrere Standorte zu einem gemeinsamen Netzwerk.

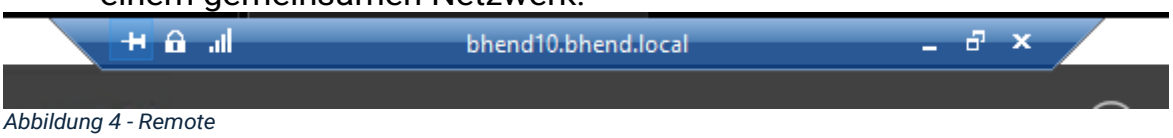
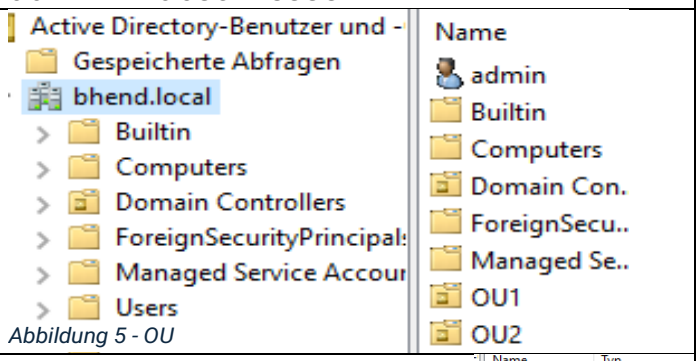
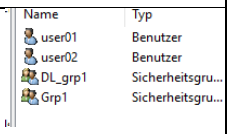
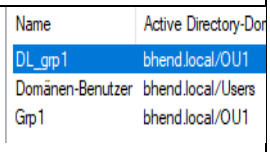
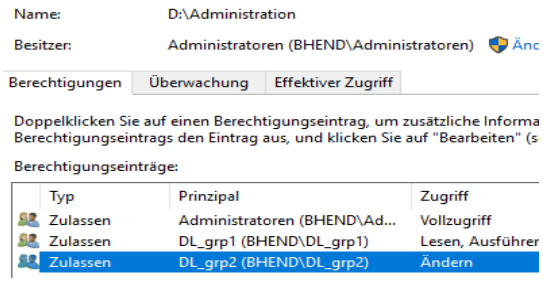


Abbildung 4 - Remote

4.7 Benutzer und Benutzergruppen

Erstellung von Benutzerkonten und Gruppen in Active Directory. Aufbau einer Struktur mit globalen und domänenlokalen Gruppen, Zuweisung von Benutzerkonten und Konfiguration der Zugriffsrechte für verschiedene Gruppen.

OU vorbereiten Erstellen von OU1, OU2	Server Manager → Tools → AD-Benutzer und Computer → nachname.local → Neu → OU → OU1 erstellen → ok → Vorgang wiederholen für OU2 → abschliessen
user01-04	OU1 → Neu → Benutzer → user01-02 erstellen → abschliessen OU2 → Neu → Benutzer → user03-04 erstellen → abschliessen
admin	nachname.local → Neu → Benutzer → admin → abschliessen
Eigenschaften untersuchen	 *Abbildung 5 - OU*
Gruppe erstellen	OU1 → Neu → Gruppe → Grp1 und DL_grp1 erstellen → Vorgang wiederholen für OU2 
Mitglieder Hinzufügen	user01-04 → Eigenschaften → Mitglied von → Gruppen hinzufügen → übernehmen  *Abbildung 6 - Mitglieder*
Berechtigungen auf Ressourcen  *Abbildung 7 - Berechtigungen*	Laufwerk D: → Neuen Ordner und unter Ordner erstellen, D:\Administration\Bestellung → Administration → Eigenschaften → Sicherheit → Erweitert → Vererbung deaktivieren → Alle vererbten Berechtigungen… → Übernehmen → OK → Hinzufügen → Prinzipal auswählen → DL_grp1 → Lesen, Ausführen, Ordnerinhalt anzeigen, Lesen → OK → Vorgang wiederholen für DL_grp2 → Ändern und Schreiben → OK → Übernehmen → OK

Server Gruppen Richtlinien	Server Manager → Tools → Default Domain/Controllers Policy → Bearbeiten → Einstellungen → Computerkonfiguration → Richtlinien → Windows Einstellungen → Sicherheitseinstellungen → Loakle Richtlinien → Zuweisen von Benutzerechten → Lokale Anmeldung zulassen → Admin hinzufügen → Gruppen hinzufügen → Übernehmen → gpupdate /force

Tabelle 16 – Benutzer und Gruppen

4.8 Freigaben erstellen und Berechtigungen einrichten

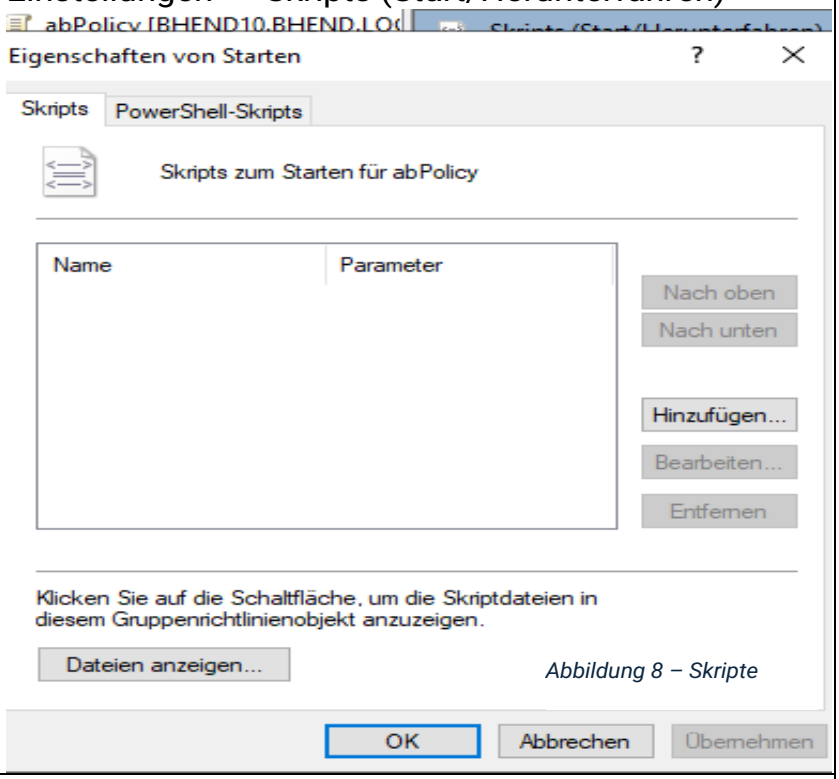
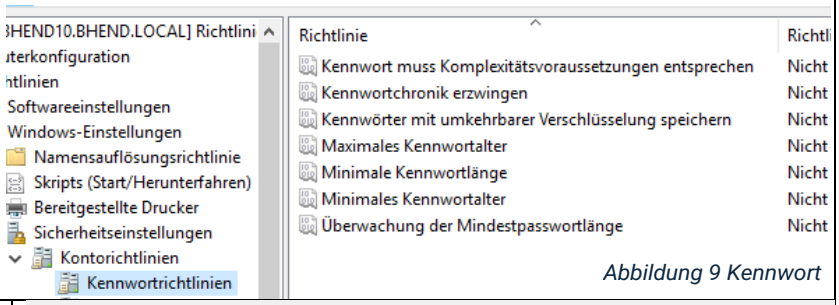
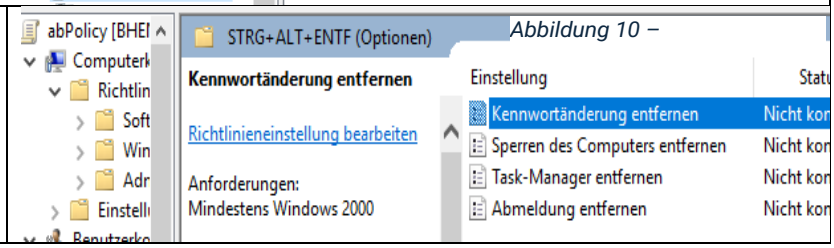
Erstellen und Freigeben von Verzeichnissen auf dem Server. Konfiguration von Freigabeberechtigungen und NTFS-Berechtigungen zur Steuerung des Zugriffs auf freigegebene Ressourcen.

Ordner Struktur	D:\Daten, D:\DB, D:\BH
Berechtigung erteilen D:\Daten	Eigenschaften → Sicherheit → Bearbeiten → Hinzufügen → DL_grp1, → OK → Hinzufügen → admin , beide Berechtigung auf Ändern → Übernehmen → OK
D:\DB	Gleiches Vorgehen → DL_grp2, → OK → Hinzufügen → admin , beide Berechtigung auf Ändern
D:\BH	Gleiches Vorgehen → DL_grp1, DL_grp2, → OK → Hinzufügen → admin , beide Berechtigung auf Ändern
Freigabe erstellen	D:\(Ordner) → Eigenschaften → Freigabe → Erweiterte Freigabe → Aktivieren → Berechtigung → Jeder → Vollzugriff → Übernehmen → OK → schliessen
Unterschied Freigabe / NTFS – Berechtigung	user01 kann auf dem Server schreiben aber nicht auf dem client, weil die Freigaben nur für den Zugriff über das Netzwerk gelten. NTFS-Berechtigungen steuern den Zugriff direkt auf dem Laufwerk.
Zugriff auf administrative Freigaben	Administrative Freigaben wie C$, ADMIN$, sind vordefiniert und ermöglichen Administratoren den Zugriff auf Systembereiche. Sie sind für reguläre Benutzer standardmässig nicht zugänglich. Diese Freigaben können temporär deaktiviert werden, aktivieren sich jedoch in der Regel nach einem Neustart wieder.

Tabelle 17 – Freigaben erstellen

4.9 Gruppenrichtlinien

Erstellen und Verwalten von Gruppenrichtlinien (GPOs) zur Steuerung von Benutzer- und Computereinstellungen. Beispiele: Deaktivieren des Papierkorbs, Einschränkung des Zugriffs auf die Systemsteuerung und Konfiguration von Kennwortrichtlinien.

GPO erstellen	Server Manager → Tools → GPO → Gesamtstruktur → Domänen → nachmae.local → Gruppenrichtlinienobjekte → Inhalt → Neu → vnPolicy (vn = initialen) → OK → Bearbeiten
Computerrichtlinien für Scripts Hier können Skripte geladen werden, die beim Hoch- oder Runterfahren des Systems ausgeführt werden.	Computerkonfiguration → Richtlinien → Windows-Einstellungen → Skripts (Start/Herunterfahren)  *Abbildung 8 – Skripte*
Computerrichtlinien für Passwörter Festlegen spezifischer Anforderungen für das Erstellen eines Kennwortes	Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Kontorichtlinien → Kennwortrichtlinien  *Abbildung 9 Kennwort*
Benutzerrichtlinien Konfiguration der Tatenkombination STRG+ALT+DEL	 *Abbildung 10 –*

GPO für Domäne Verlinken Desktop Einstellungen	Gesamtstruktur → Domänen → nachname.local → Vorhandenes Gruppenrichtlinien Objekt verknüpfen → vnPolicy wählen → OK → vnPolicy Bearbeiten → Benutzerkonfiguration → Richtlinien → Administrative Vorlagen → Desktop → Papierkorbsymbol vom Desktop entfernen → Aktiviert
GPO für die Systemsteuerung	Benutzerkonfigurationen → Richtlinien → Administrative Vorlagen → Systemsteuerung → Zugriff auf die Systemsteuerung und PC-Einstellungen nicht zulassen → Aktiviert
Widersprüchliche GPO im selben Container	Gesamtstruktur → Domänen → nachmae.local → Gruppenrichtlinienobjekte → Neu → ControlPanelPolicy → OK → nachname.local → Verknüpfte Gruppenrichtlinienobjekte → ControlPanelPolicy vor adPolicy
Vererbung	Gesamtstruktur → nachname.local → ControlPanlePolicy → löschen / Nein da es nicht GPO ist mit dieser Richtline
Verebung uterbrechen	OU1 → Vererbung deaktivieren / Zugriff auf Systemsteuerung möglich.
Einstellungen überschreiben	OU1 → Vorhandenes Gruppenrichtlinien Objekt verknüpfen → ControlPanlePolicy → OK / Systemsteuerung erscheint.
Vererbung erzwingen	adPolicy → Erzwungen → OK / Kein Zugriff auf Systemsteuerung möglich.
GPO für das Kennwort	Computerkonfigurationen → Windows-Einstellungen → Sicherheitseinstellungen → Kontorichtlinien → Kennwortrichtlinien → Maximales Kennwortalter und Kennwortchronik aktivieren Kontosperrungrichtlinien → Kontosperrungsschwelle → aktivieren.
Softwareverteilungspunkt (SDP) einrichten Windows Installer (MSI) bereitstellen	Verzeichnis D:\Software erstellen Eigenschaften → Freigabe → Erweiterte Freigabe… → Diesen Ordner freigeben aktivieren → Berechtigungen → Jeder → Berechtigung Lesen MSI-Paket scite-5.1.5x64.ms in das Verzeichnis Kopieren

GPO für ie Softwareverteilung anlegen *Abbildung 11 - SciTE* 	Neue GPO erstellen: SciteDistribution Bearbeiten → Computerkonfiguration → Richtlinien → Softwareeinstellungen → Softwareinstallation → Eigenschaften → \\nachname10.nachname.local\Software Neues Paket erstellen: Kontextmenu → Neu – Paket… → scite-5.1.5x64.msi → Öffnen → Zugewiesen → OK

Tabelle 18 - GPO

5.0 Netzwerkdrucker einrichten

Installation und Freigabe eines Netzwerkdruckers. Zuweisung des Druckers an Benutzer oder Gruppen mithilfe von Gruppenrichtlinien und Konfiguration von Druckerberechtigungen.

Drucker Installieren	Druckverwaltung als administrator ausführen → Druckserver → Servername10 → Drucker → Drucker hinzufügen… → Lokalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen → LPT1 → weiter → Druckertreiber: xy, Drucker: xy Druckername und Freigabeeinstellungen: Druckername: printer1 Drucker freigeben: Aktivieren
Drucker Installieren	printer1 → Kontextmenu → Druckereigenschaften… → Anschlüsse → Hinzufügen… → Standard TCP/IP Port → Neuer Anschluss… → 172.16.1.50
Drucker konfigurieren	printer1 → Kontextmenu → Druckereigenschaften… → Sicherheit
GPO erstellen, Drucker per GPO zuordnen	Neue GPO → printer1 → Bearbeiten → Benutzerkonfiguration → Einstellungen → Systemsteuerungseinstellungen → Drucker → Neu → Freigegebener Drucker → Erstellen → \\nachname10.nachname.local\printer1 Standard definieren, optional

Tabelle 19 - Drucker

5.1 Loginscript übergeben

Erstellung von Loginscripts, die automatisch Netzlaufwerke zuweisen (z. B. P:, W:, S:). Hinterlegen der Skripte in den Benutzerprofilen und automatisches Ausführen bei Anmeldung.

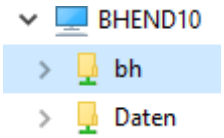
Batch installieren	C:\Windows\SYSVOL\sysvol\nachname.local\scripts
Batch Datei übergeben  *Abbildung 12 - Netzwerkfreigabe*	Server Manager → Tools → AD- Benutzer und Computer → nachname.local → OU1 → user01 → Eigenschaften → Profil → Anmeldeskript → name.bat Der Ordner ist im Netzwerk und hat die Aufgabe die Scripts automatisch zu verwalten. Kein Pfad nötig.

Tabelle 20 - Batch

5.2 Homelaufwerk erstellen

Einrichten von persönlichen Homelaufwerken für Benutzer. Konfiguration von Freigaben und NTFS-Berechtigungen, um sicherzustellen, dass nur der jeweilige Benutzer Zugriff auf sein Laufwerk hat

Homeverzeichnis erstellen, freigeben und Berechtigung definieren	Verzeichnis D:\Homes erstellen, Gruppe Benutzer hat Änderungsrechte. Eigenschaften → Freigabe → Erweiterte Freigabe… → Freigeben aktivieren → Freigabenamen ein $ am Ende → Berechtigungen → Jeder → Vollzugriff → Übernehmen
Homeverzeichnis konfigurieren	Server Manager → Tools → AD- Benutzer und Computer → nachname.local → OU1 → user01 → Eigenschaften → Profil → Profilpfad → \\nachname10.nachname.local\Profiles$\%username% Basisordner → Verbinden von → \\nachname10.nachname.local\Homes$\%username% Übernehmen → OK

Tabelle 21 - Homelaufwerk

5.3 Moitoring (Überwachung)

Einrichtung eines Monitoring-Systems zur Überwachung des Servers und der Netzwerkressourcen. Beispiele: Überwachung der Festplattenkapazität, Netzwerkverfügbarkeit und Serverleistung.

Überwachung für den Zugriff auf Dateien und Verzeichnisse in den Richtlinien aktivieren	Server Manager → Tools → GPO → Gruppenrichtlinienverwaltung → Gesamtstruktur → nachname.local → Default Domain Policy → Bearbeiten → Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Überwachungsrichtlinien → Objektzugriffsversuche überwachen → Aktivieren für Fehler → OK
Verzeichnis definieren, bei welchem die Zugriffe überwacht werden	Laufwerk D:\BH Verzeichnis BH → Eigenschaften → Sicherheit → Erweitert → Überwachung → Hinzufügen → Prinzipal: DL_grp1 → Typ: Alles → Anwenden: Ordner und Unterordner und Dateien → OK → Übernehmen
Protokolle einsehen	Windows Ereignisanzeige → Windows Protokolle → Sicherheit → Aktuelles Protokoll filtern … → Ereigniss ID: 4656, 4663 → OK
Druckprotokoll aktivieren	Windows Ereignisanzeige → Anwendungs- und Dienstprotokolle → Microsoft → Windows → PrintService → Betriebsbereit → Kontextmenü → Protokoll aktivieren

Tabelle 22 - Monitoring

6. Kontrollieren

6.1 IpFire Kontrollieren

>ping google.ch

6.2 Server Kontrolle

Überprüfen der Internetverbindung mit Internetbrowser (Nicht Internet Explorer) und einer sicheren Seite. zB www.20min.ch
Patches und Updates prüfen und falls nötig aktualisieren.

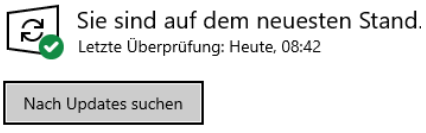


Abbildung 13 - Updates

6.3 ADDS-Kontrolle

Unter Server Rollen ist nun AD DS vorhanden und auch DNS wurde installiert, da AD DS ohne DNS nicht funktioniert.

6.4 DNS-Kontrolle

Eingabeaufforderung als Administrator starten → ipconfig /flushdns ausführen. DNS-Cache gelöscht, nslookup www.google.ch ausführen. Wenn der Forwarder richtig eingestellt ist, werden die IP-Adressen angezeigt.

Server Manager → Tools → DNS → Servername → nslookup
Standardserver: servename.nachname.local
>google.ch → Enter → Antwort vom eigenen Server.

6.5 DHCP-Kontrolle

Win 10 Client VM Starten → NIC prüfen und Eingabeaufforderung → ipconfig

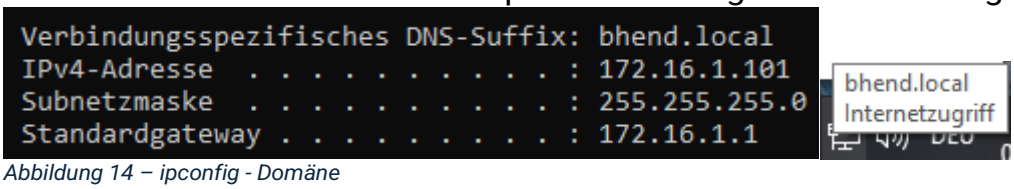


Abbildung 14 – ipconfig - Domäne

6.6 Benutzer Kontrollieren

Client01 Starten → Win+Pause → Erweiterte Systemeinstellungen → Computername → Ändern → user01 → Domäne, nachname.local → admin anmelden und bestätigen. Wenn richtig konfiguriert, Meldung erscheint.

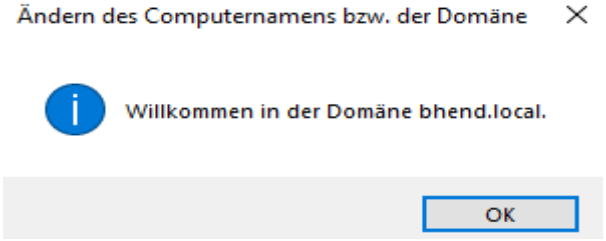


Abbildung 15 - Willkommen

6.6 Berechtigung testen

Anmelden am Server/Client mit user01-04 → D:\Administration\Bestellungen → Dateien erstellen, versuchen drauf zuzugreifen, bearbeiten oder löschen. Auch für die Verzeichnisse D:\Daten, D:\DB und D:\BH

6.7 GPO-Kontrollieren

Papierkorb: Evtl. zwei Mal bei Client Anmelden. Papierkorb auf dem Desktop? Wenn nein, GPO funktioniert korrekt.
Systemsteuerung: Evtl. zwei Mal bei Client Anmelden. Ist die Systemsteuerung aufrufbar? Nein, GPO-Funktioniert korrekt. Ja, Widersprüchliche GPO eingestellt.
Passwort: Evtl. zwei Mal bei Client Anmelden. Je nach Einstellungen werden Passwortänderung verweigert. Chronik verhindert das Verwenden gleicher Passwörter je nach Wert. Das alter bleibt gleich, ändern des Passwortes ändert hier nichts. Sperrungsschwelle sperrt das Konto nach X Anmelde Versuchen für die definierte Zeit. GPO-Funktioniert korrekt
Softwareverteilung: Ich habe keine Fehler mit der Quelle «Application Management Group Policy» oder «MsiInstaller» in der Ereignis Anzeige trotzdem ist SciTE im Startmenü nicht sichtbar. Über das Netzwerk auffindbar.
Nachdem die Dateierweiterung auf dem Client im Explorer aktiviert wurde, wurde es automatisch installiert.

6.8 Drucker kontrollieren

Testseite drucken.

6.9 Batch Datei Kontrollieren

Client starten

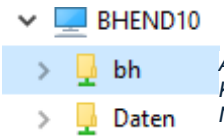


Abbildung 16 - Kontrolle Netzwerkfreigabe

7.0 Homelaufwerk Kontrollieren

Client starten

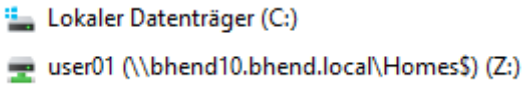
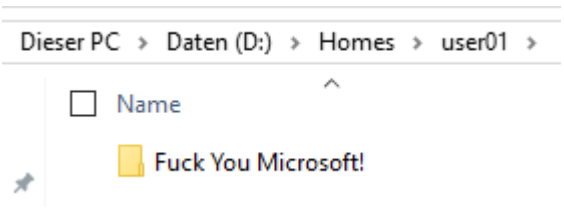


Abbildung 17 - Kontrolle Homelaufwerk



8. Auswerten

8.1 Eingesetzte Softwareversionen

8.1.1 Windows Server 2019 Standard

- **Version:** 1809 (Build 17763)
- **Beschreibung:** Die Serverversion ist für die zentralisierte Verwaltung von Benutzerkonten, Gruppenrichtlinien, DNS, DHCP und Netzwerkdiensten. Sie bietet eine stabile.
- **Vorteile:** Verbesserte Sicherheitsfeatures. Unterstützung für hybride Umgebungen. Verbesserte Performance und Skalierbarkeit für Active Directory Domain Services (ADDS).

8.1.2 Eingesetzte Rollen:

- **ADDS:** Zur zentralisierten Verwaltung von Benutzern und Ressourcen.
- **DNS:** Für die Namensauflösung im Netzwerk. Domain Name System oder Service je nach Einsatz
- **DHCP:** Für die automatische Zuweisung von IP-Adressen. Dynamic Host Control Protocoll
- **Druck- und Dokumentdienste:** Zum zentralisierten Drucken und Verwalten von Druckaufträgen.
- **VPN:** VPN Verbindung

8.2.3 Windows 10 Pro

- **Version:** 22H2 (Windows 10)
- **Beschreibung:** Client-Betriebssysteme bieten Benutzern Zugriff auf Domänenressourcen und erlauben die Umsetzung von Gruppenrichtlinien.
- **Einsatz im Projekt:**Verwendung als Arbeitsstationen (Clients). Unterstützung von Sicherheits- und Verwaltungsfeatures wie Gruppenrichtlinien und Laufwerkszuweisungen.

8.3.4 IPFire 2.27

- **Version:** Core Update 164
- **Beschreibung:** Eine Open-Source-Firewall, die für Netzwerksicherheit und Traffic-Management genutzt wird.
- **Einsatz im Projekt:** Dient als Router und Firewall zur Trennung und Sicherung des Netzwerks

8.4.4 SciTE Texteditor

- **Version:** 5.1.5 (64-Bit)
- **Beschreibung:** Ein leichter Texteditor, der über Gruppenrichtlinien installiert und auf allen Clients bereitgestellt wurde.
- **Einsatz im Projekt:** Demonstration der Softwareverteilung über Gruppenrichtlinien.

8.2 Abhandlung über Windows Server 2019

Windows Server 2019 Standard ist die neueste Version der Serverbetriebssysteme von Microsoft. Es wurde entwickelt, um Unternehmen eine flexible Plattform für die Verwaltung von IT-Infrastrukturen zu bieten.

Features

- **Zentrale Verwaltung:** Ermöglicht die Einrichtung einer Active Directory-Domänenstruktur für zentralisierte Benutzer- und Ressourcenverwaltung.
- **Sicherheitsverbesserungen:** Windows Defender ATP und Shielded VMs für zusätzlichen Schutz. Verbesserte Updatestrategien durch Cluster-Aware-Updates.
- **Hybride Szenarien:** Unterstützt Azure-Dienste. Integration mit Windows Admin Center für cloudbasierte Verwaltung.
- **Skalierbarkeit:** Bietet Unterstützung für grössere Datenmengen und mehr Benutzer. Bei früheren Versionen waren die Nutzer beschränkt auf 5000. Jetzt sind sie unendlich. Verbesserte Performance.

Projekte

- **Benutzer- und Gruppenverwaltung:** Die ADDS-Rolle wird genutzt, um eine Domänenstruktur mit Benutzern und Gruppen erstellen zu können und zentral zu verwalten.
- **Netzwerkdienste:** Mit den Rollen DNS und DHCP wird ein Netzwerk aufgebaut.
- **Dateiverwaltung:** NTFS-Berechtigungen und Freigaben ermöglichen einen sicheren und effizienten Zugriff auf Daten.
- **Gruppenrichtlinien:** Diese werden genutzt, um die zentralen Einstellungen für User und Clients zu implementieren, z. B. Softwareverteilung und Desktopanpassungen.

8.3 Fazit

Die Dokumentation beschreibt die erfolgreiche Einrichtung einer Serverinfrastruktur mit Diensten wie Active Directory, DNS, DHCP, VPN und Gruppenrichtlinien. Ziel war ein zentrales Netzwerkmanagement, das Benutzer, Gruppen und Ressourcen effizient verwaltet sowie Sicherheit und Performance verbessert.

Ein Schwerpunkt lag auf zentralisierter Verwaltung durch Benutzerkonten und Gruppenrichtlinien, was Effizienz und Sicherheit steigert. Automatisierungen wie Softwareverteilung sparen Zeit und sichern eine einheitliche Systemkonfiguration. Hervorzuheben ist die Einrichtung persönlicher Homelaufwerke, die den Datenschutz der Benutzer stärken.

Die Zielsetzungen der Dokumentation wurden vollständig erreicht. Die Ergebnisse zeigen, dass durch klare Planung und technische Expertise komplexe IT-Projekte erfolgreich umgesetzt werden können. Zudem bietet die Dokumentation Optimierungsvorschläge, insbesondere für Zeitmanagement und Ressourcenzuweisung.

Abbildungsverzeichnis

Titelbild: imgurl:https://diropa.at/wp-content/uploads/2022/07/serverwartung-graz1.jpg - Suchen

Tabellenverzeichnis

Kontakt: adrian.bhend@ict.csbe.ch