


07.07.2023
Abschluss Projekt Dokumentation

HOMENET  **CONNECT**

Robin Schneider
Netcloud AG

Inhaltsverzeichnis

Tätigkeits-Ablauf (Änderungsliste)	3
1 Vorbereitung	5
1.1 Projekt-Idee	5
1.1.1 Grundbaustein	5
1.1.2 Erweiterung	5
1.1.3 Zusatz	5
1.2 Meilensteine	6
1.2.1 Windows Server mit AD und weiteren Services	6
1.2.2 Von Windows Client bei AD anmelden + Permissions	6
1.2.3 Von Ubuntu Client bei AD anmelden	6
1.3 Optionale Ziele	6
1.3.1 Virtual Private Network (VPN) und Remote Desktop Protokoll (RDP)	6
1.3.2 Von Windows Client bei AD anmelden + Permissions	6
1.3.3 Von Ubuntu Client bei AD anmelden	6
1.4 Lernziele	6
1.4.1 Kommunikation zwischen Linux und Windows	6
1.4.2 Routine im Umgang mit Windows Servern	6
2 IPERKA	7
2.1 Informieren	7
2.2 Planen	7
2.2.1 Soll	7
2.2.2 Ist	7
2.3 Entscheiden	8
2.4 Realisieren	9
2.5 Kontrollieren	10
2.6 Auswerten (Fazit)	10
3 Netzwerk	11
3.1 Netzwerk Plan	11
3.2 OPNsense (PC-Engine)	12
3.2.1 Übersicht	12
3.2.2 Informationen	12
3.2.3 Installation & Konfiguration	12
3.3 Switches	13
3.3.1 Übersicht	13
3.3.2 Informationen	13
3.3.3 Installation & Konfiguration	14
3.4 Access Point	15
3.4.1 Übersicht	15
3.4.2 Informationen	15
3.4.1 Installation & Konfiguration	16
3.5 Windows Server	16
3.5.1 Übersicht	16
3.5.2 Informationen	16
3.5.1 Installation & Konfiguration	17

3.6	Clients	19
3.7	Datensicherung	20
3.7.1	Datensicherungs-Konzepte	20
3.7.2	Wann werden Datensicherungen durchgeführt?	20
3.7.3	Welche Daten werden gesichert?	20
3.7.4	Wo werden die Daten gespeichert?	21
4	Glossar	22
5	Quellen	23
5.1	Verwendete Webseiten	23
5.2	Tutorials	23
5.3	Bilder	23

Tätigkeits-Ablauf (Änderungsliste)

Inhalt:

In diesem Abschnitt werden die einzelnen Tätigkeiten zeitlich dokumentiert.
Die Inhalte dieser Liste werden im Kapitel [2.4 Realisieren](#) dokumentiert.

Nr.	Datum der Änderung	Gerät	Beschreibung
1.	07.06.2023	PC-Engine	OPNsense Firewall aufgesetzt und konfiguriert
2.	07.06.2023	Switch	Switch konfiguriert (Fixe IP)
3.	07.06.2023	Windows Server	USB-Stick Flash → Windows Server Installation
4.	07.06.2023	Raspberry PI	SD-Karte Flashen → Raspberry PI OS installieren
5.	07.06.2023	Raspberry PI	Twingate VPN auf Raspberry PI installieren und konfigurieren
6.	08.06.2023	Windows Server	Umbenannt → „WinServ01“
7.	08.06.2023	Windows Server	DNS-Service aktiviert und konfiguriert
8.	08.06.2023	Windows Server	DHCP-Service aktiviert und konfiguriert
9.	08.06.2023	PC-Engine	DHCP-Service auf OPNsense Firewall deaktiviert
10.	08.06.2023	Access Point	Reset + Konfigurieren (Von „Router“ auf „only AP“ wechseln)
11.	08.06.2023	Windows Server	Server zu Domain Controller aufstufen
12.	08.06.2023	Windows Server	Domain „zli.local“ erstellt
13.	08.06.2023	Windows Server	DNS Delegierung ändern
14.	08.06.2023	Windows Server	Active Directory Konfigurieren
15.	08.06.2023	Windows Server	Geteilter Ordner mit Profil Pfaden
16.	08.06.2023	Windows Client	Windows Client zur Domäne hinzugefügt. (zli.local)
17.	08.06.2023	Windows Client	Mit AD-User einloggen. (Verbindung Testen)
18.	08.06.2023	Ubuntu Client	Ubuntu Client zur Domäne hinzugefügt. (zli.local)
19.	08.06.2023	Ubuntu Client	Mit AD-User einloggen. (Verbindung Testen)
20.	08.06.2023	Windows Server	Backup Feature aktiviert
21.	08.06.2023	Windows Server	Full-Backup vom Windows Server ausgeführt
22.	08.06.2023	Informieren	Software Verteiler System Vorschläge gesucht → Gian-Reto Frei
23.	08.06.2023	Google	Software Verteiler System Demo Version beantragt → Baramundi
24.	09.06.2023	Timestamp	Hostpoint → Datenbank erstellen
25.	09.06.2023	Timestamp	Timestamp Python Skript in Datenbank Variante umschreiben
26.	14.06.2023	Timestamp	Logon Abfrage Skript erstellt
27.	14.06.2023	Timestamp	Alle Dateien über das Netzwerk freigegeben
28.	14.06.2023	Timestamp	Group Policy erstellt → Skript Ausführung erlaubt & Logon konfiguriert
29.	14.06.2023	Timestamp	Bug Fixing
30.	15.06.2023	Windows Server	Windows Server Stuck in „Applying Windows Configuration“
31.	15.06.2023	Windows Server	Boot-Stick → Neuinstallation
32.	15.06.2023	Windows Server	Windows-Server-Backup Feature aktiviert
33.	15.06.2023	Windows Server	Safe Mode aktivieren → Restart
34.	15.06.2023	Windows Server	Backup restore → System State
35.	15.06.2023	Dokumentation	Beginn der HomeNet Connect Dokumentation
36.	15.06.2023	Windows Server	Von USB-Stick booten → Trouble Shoot → Backup Recovery
37.	15.06.2023	Windows Server	Verlorener Fortschritt wiederherstellen
38.	15.06.2023	Windows Server	Full Backup ausführen
39.	15.06.2023	Timestamp	Abfrage Skript → Error analysieren
40.	15.06.2023	Windows Server	Group Policy anpassen (dieses Mal korrekt)
41.	16.06.2023	Timestamp	Abfrage Skript überarbeitet + Bug Fixing
42.	16.06.2023	Timestamp	Sand-Along gemacht (Automatisches Installieren der benötigten Pakete)
43.	16.06.2023	Windows Server	Group Policy bearbeitet → Logon Skript hinterlegt
44.	16.06.2023	Windows Client	Skript mit Logon überprüft → erfolgreich!

45.	16.06.2023	Dokumentation	HomeNet Connect Dokumentation erweitert
46.	21.06.2023	Raspberry Pi	Fog Projekt ausprobiert und wieder deinstalliert
47.	21.06.2023	Windows Server	EMCO Remote Installer installieren
48.	21.06.2023	Windows Server	EMCO MSI Package Builder installieren
49.	21.06.2023	Windows Server	Google Chrome deinstallieren, msi bilden und wieder deployen über EMCO
50.	22.06.2023 (HO)	Raspberry Pi	Ubuntu auf Raspberry Pi installiert
51.	22.06.2023 (HO)	Raspberry Pi	Versucht „Streamdeck UI“ zu installieren und konfigurieren (nicht funktioniert)
52.	22.06.2023 (HO)	Raspberry Pi	Raspberry Pi OS installiert
53.	22.06.2023 (HO)	Raspberry Pi	Versucht „Streamdeck UI“ zu installieren und konfigurieren (nicht funktioniert)
54.	22.06.2023 (HO)	Raspberry Pi	Windows 10 auf Raspberry Pi installiert
55.	22.06.2023 (HO)	Raspberry Pi	Elgato Stream Deck Software installiert (nicht funktioniert)
56.	22.06.2023 (HO)	Timestamp	Timestamp Skript weiter gearbeitet
57.	23.06.2023	Raspberry Pi	„USB over Netzwerk“ versucht (Installation gescheitert)
58.	28.06.2023	Dokumentation	Ich habe die Dokumentation fertiggestellt.
59.	29.06.2023	Präsentation	Ich habe die Präsentation begonnen.
60.	30.06.2023	Handout	Ich habe das Handout gemacht.
61.	30.06.2023	Demo Video	Ich habe das Demo Video gemacht.
62.	30.06.2023	Gantt Diagramm	Ich habe das Gantt Diagramm gemacht.
63.			
64.			
65.			
66.			
67.			
68.			
69.			
70.			
71.			

1 Vorbereitung

Bevor wir mit dem Projekt beginnen konnten, mussten wir einen Projektantrag mit der Projektidee, einzelnen Meilensteinen, Zusatzzielen und Lernziele stellen.

Weil ich mir bereits im Voraus Gedanken zu meinem Projekt gemacht habe und Jörg mir die Grundidee gegeben hatte, war ich ziemlich schnell fertig mit dem Antrag und durfte somit auch gleich loslegen.

Meine Projektidee und alle weiteren Planungen folgen in den Kapiteln [1.2 Meilensteine](#), [1.3 Optionale Ziele](#) und [1.4 Lernziele](#).

1.1 Projekt-Idee

1.1.1 Grundbaustein

Ich habe im ÜK184 Jörg Häderli gefragt, was für ein Abschlussprojekt zu mir passen würde. Seine Idee war, etwas mit einem Active Directory (AD) zu machen, respektive ein Netzwerk. Mir gefiel der Gedanke und deswegen habe ich diesen notiert.

1.1.2 Erweiterung

Ich habe mir am Montag und Dienstag über die Tage verteilt Gedanken gemacht, was ich alles für Services und Features in meinem Netzwerk haben möchte.

Dabei habe ich meine bisherigen Notizen erweitert und hatte folgende Punkte festgelegt:

- ❖ Windows Server
 - DHCP-Server
 - DNS-Server
 - Active Directory (AD)
 -
- ❖ OPNsense
 - Die OPNsense sollte ein Übergang der Subnetze sein und das LAN unabhängig zu dem WAN-Netzwerk machen.
 - Firewall
- ❖ Raspberry Pi
 - Twingate (VPN)
- ❖ Windows Client
 - AD bindet
- ❖ Ubuntu Client
 - AD bindet

Ausserdem ist mir die Idee gekommen, mein bisheriges Zeitstempel-Programm mit den AD-Clients zu verknüpfen, damit beim Starten des Clients eine Message mit angezeigt wird, ob man bereits eingebadged ist oder nicht. Wie genau ich dies umsetze, wusste ich zu diesem Zeitpunkt noch nicht.

1.1.3 Zusatz

Im Verlaufe des Projektes sind dann weitere Punkte hinzugekommen, weil es komfortabler oder praktischer ist.

- ❖ Windows Server
 - Backup Service auf externe Festplatte (damit bei Fehlern zurückgefahren werden kann)
- ❖ Netgear Zauberbox
 - Access Point (Wi-Fi Verbindung zum Netzwerk, damit man nicht immer am Kabel hängt.)
- ❖ Zeitstempel-System
 - Das Timestamp_V1 war Excel basierend und somit nicht geeignet für einen produktiven Gebrauch im Netzwerk. Somit musste eine Datenbank (DB) Lösung daher. Die Datenbank war schnell erstellt, jedoch musste das ganze Badge Skript neugeschrieben und überarbeitet werden. Die Version 2 funktionierte einwandfrei mit der Datenbank, jedoch konnte man nur einmal täglich badgen und es war im Allgemeinen unelegant gelöst. Mit dem Timestamp_V3 war ich dann endlich zufrieden und konnte zum nächsten Schritt.

○ Die Abfrage auf den Clients funktionierte mit 4 Files. (2x .bat | 1x .py | 1x .ps1)
Mit diesen Vorstellungen und Notizen habe ich folgende Ziele definiert:

1.2 Meilensteine

1.2.1 Windows Server mit AD und weiteren Services

- Windows Server 2019 sollte voll funktionsfähig sein und als Domain Controller funktionieren.
- Ein funktionierendes Active Directory mit erstellten Benutzern.

1.2.2 Von Windows Client bei AD anmelden + Permissions

- Ein Windows Client sollte erfolgreich in der Domain und im Active Directory (AD) hinzugefügt sein.
- Die einzelnen User sollten verschiedene Berechtigungen haben.

1.2.3 Von Ubuntu Client bei AD anmelden

1. Auch von Ubuntu Clients sollte man sich mit der Domäne verbinden und sich am Active Directory anmelden können.

1.3 Optionale Ziele

1.3.1 Virtual Private Network (VPN) und Remote Desktop Protokoll (RDP)

- Twingate VPN auf dem Raspberry Pi installiert und konfiguriert.
- Von Client über Twingate ins Netzwerk verbinden.
- RDP auf Windows Server konfigurieren
- Von Client per RDP auf Windows Server zugreifen.

1.3.2 Von Windows Client bei AD anmelden + Permissions

- Ein Windows Client sollte erfolgreich in der Domain und im Active Directory (AD) hinzugefügt sein.
- Die einzelnen User sollten verschiedene Berechtigungen haben.

1.3.3 Von Ubuntu Client bei AD anmelden

2. Auch von Ubuntu Clients sollte man sich mit der Domäne verbinden und sich am Active Directory anmelden können.

1.4 Lernziele

1.4.1 Kommunikation zwischen Linux und Windows

3. Ich möchte mein Wissen über die Kommunikation zwischen Linux und Windows erweitern und entdecken, wie ich dies gewährleisten kann.

1.4.2 Routine im Umgang mit Windows Servern

4. Ausserdem möchte ich mehr Routine im Umgang von Windows Servern bekommen, damit ich auch in Zukunft produktiv damit arbeiten kann.

2 IPERKA

2.1 Informieren

Ich habe zuerst einmal überlegt, was ich alles in meinem Projekt umsetzen möchte.
Was alles dazugehört, befindet sich im Kapitel [1. Vorbereitung](#).

2.2 Planen

Als ich wusste, was ich alles machen möchte und dazu brauche, habe ich mir einen Ablauf überlegt, wann ich was, wie machen möchte.

1. Firewall (OPNsense)
Damit mein Netzwerk stand-Alone funktioniert.
2. Switch
Für die Kommunikation im Netzwerk.
3. Raspberry Pi (Twingate VPN)
Damit ich im Falle von Homeoffice auf mein Netzwerk komme.
4. Windows Server
5. DNS, DHCP & AD
6. Clients
7. Timestamp

2.2.1 Soll

Soll Diagramm		davor	07.06.2023	08.06.2023	09.06.2023	14.06.2023	15.06.2023	16.06.2023	21.06.2023	22.06.2023	23.06.2023	28.06.2023	29.06.2023	30.06.2023	Wochenende	05.07.2023	06.07.2023	07.07.2023
Datum			Mittwoch	Donnerstag	Freitag	Mittwoch	Donnerstag	Freitag	Mittwoch	Donnerstag	Freitag	Mittwoch	Donnerstag	Freitag		Mittwoch	Donnerstag	Freitag
Informieren	Ideen sammeln																	
Planen	Recherchieren																	
	Anleitungen suchen																	
	Möglichkeiten suchen																	
Entscheiden	Besprechen																	
	Projektantrag																	
Milestones	Ziele definieren																	
	Windows Server mit Services																	
Optionale Ziele	Windows Client im AD																	
	Ubuntu Client im AD																	
Testphase	VPN & RDP																	
	Softwareverteiler																	
Administration	Timestamp logon																	
	Testen																	
Präsentation	Verbessern																	
	Kanbanboard																	
Präsentation	GANTT-Diagramm																	
	Dokumentation																	
Präsentation	Präsentation																	
	Handout																	
Präsentation	Demo Video																	
	Endprodukt																	
Präsentation	Vorbereitung / Üben																	
	Präsentieren																	

2.2.2 Ist

Ist Diagramm		davor	07.06.2023	08.06.2023	09.06.2023	14.06.2023	15.06.2023	16.06.2023	21.06.2023	22.06.2023	23.06.2023	28.06.2023	29.06.2023	30.06.2023	Wochenende	05.07.2023	06.07.2023	07.07.2023
Datum			Mittwoch	Donnerstag	Freitag	Mittwoch	Donnerstag	Freitag	Mittwoch	Donnerstag	Freitag	Mittwoch	Donnerstag	Freitag		Mittwoch	Donnerstag	Freitag
Informieren	Ideen sammeln																	
Planen	Recherchieren																	
	Anleitungen suchen																	
	Möglichkeiten suchen																	
Entscheiden	Besprechen																	
	Projektantrag																	
Milestones	Ziele definieren																	
	Windows Server mit Services																	
Optionale Ziele	Windows Client im AD																	
	Ubuntu Client im AD																	
Testphase	VPN & RDP																	
	Softwareverteiler																	
Administration	Timestamp logon																	
	Testen																	
Präsentation	Verbessern																	
	Kanbanboard																	
Präsentation	GANTT-Diagramm																	
	Dokumentation																	
Präsentation	Präsentation																	
	Handout																	
Präsentation	Demo Video																	
	Endprodukt																	
Präsentation	Vorbereitung / Üben																	
	Präsentieren																	

2.3 **Entscheiden**

Ich möchte einfach starten und alles auf mich zukommen lassen, ob positiv oder negativ, denn ich mache dieses Projekt um etwas zu Lernen und dabei sind auch Fehler inbegriffen.

2.4 Realisieren

Hier ist die Reihenfolge, welche ich umgesetzt habe und auch funktioniert:

1. OPNsense auf PC Engine installieren
 - [3.2.3.1 Basis Installation](#)
2. Switch einrichten
 - [3.3.3.1 Basis Installation](#)
3. Windows Server 2019 installieren
 - [3.5.1.1 Basis Installation](#)
 - [3.5.1.2 Google Chrome installieren](#)
4. Raspberry Pi installieren + Twingate VPN
 - Raspberry Pi SD-Karte flashen
 - Terminal öffnen
 - `curl "https://binaries.twingate.com/connector/setup.sh" | sudo TWINGATE_ACCESS_TOKEN="" TWINGATE_REFRESH_TOKEN="" TWINGATE_URL="https://pctipp.twingate.com" bash`
5. Windows Server 2019 | DNS, AD & DHCP
 - [3.5.1.4 DNS](#)
 - [3.5.1.6 Active Directory \(AD\)](#)
 - [3.5.1.5 DHCP](#)
6. OPNsense | DHCP-Service deaktivieren
 - [3.2.3.2 DHCP-Service Deaktivieren](#)
7. Access Point einrichten
 - [3.4.1.1 Basis Installation](#)
8. Windows Client zur Domain hinzufügen
 - Einstellungen → System → Info → „Diesen PC umbenennen (fortgeschritten)“ → Ändern
 - Domäne: „zli.local“
 - Mit AD-User Anmelden
9. Ubuntu Client zur Domain hinzufügen
 - Ubuntu Installation durchführen
 - Anstatt User erstellen → mit Active Directory verbinden
 - Domäne: „zli.local“
 - Mit AD-User Anmelden
10. Windows Server Backup konfigurieren und erstellen
 - [3.5.1.7.1 Backup erstellen](#)
11. Timestamp
 - Das Zeitstempel Python Skript funktioniert und ein Benutzer kann sich mit seiner ID, ein- & aus- badgen. Ausserdem Pausen und Reflexionen eintragen.
12. Logon Skript
 - Das PowerShell Logon Skript für die Abfrage.bat Datei aus, welche auf dem Share Drive abgelegt ist. Es fragt den Status der Person bei der Datenbank ab und gibt ihn in Form einer Message aus.
13. Group Policy
 - [3.5.1.8 Policy Management](#)
14. Windows Server Backup Recovery
 - [3.5.1.7.2 Backup wiederherstellen](#)

2.5 Kontrollieren

OPNsense funktioniert ✓
VPN-Verbindung funktioniert ✓
Switch funktioniert ✓
Windows Server funktioniert ✓
DHCP-Adressen werden vergeben ✓
DNS funktioniert ✓
WLAN funktioniert ✓
Windows Client ist im AD ✓
Ubuntu Client ist im AD ✓
Timestamp Skript funktioniert ✓
DB Abfrage funktioniert ✓
Stream Deck funktioniert ✓
Backup erstellt und kann wiederhergestellt werden ✓
RDP funktioniert ✓
Logon Skript wird ausgeführt ✓

Alle Meilensteine erreicht ✓
Alle optionalen Ziele erreicht ✓
Alle Lernziele erreicht ✓

Ich habe alle Ziele erreicht und den Zeitplan eingehalten.

Für die Abgaben (Doku, Präsentation, Handout, Video) hatte ich noch 3 Tage Zeit.

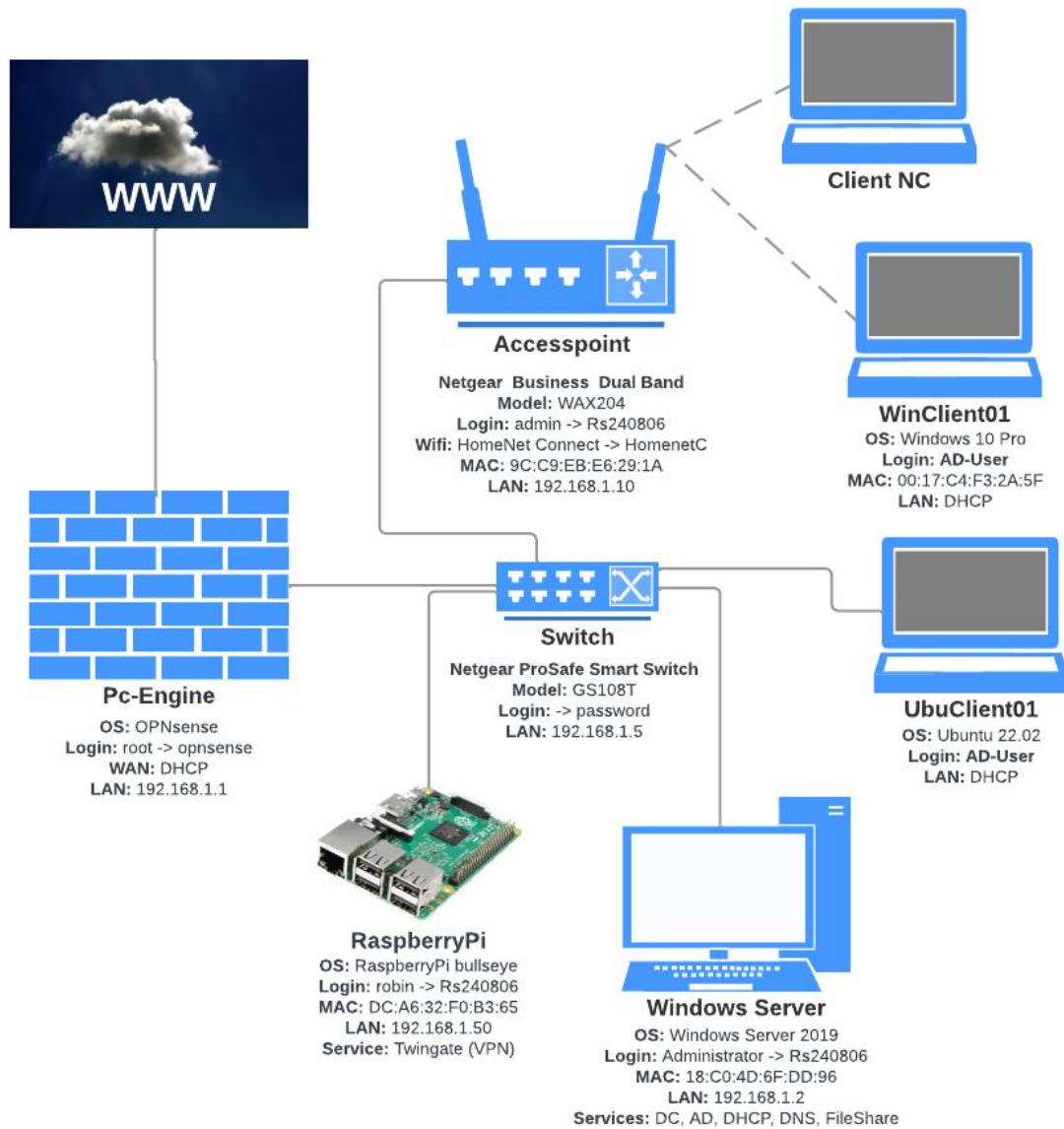
2.6 Auswerten (Fazit)

Das Fazit meiner Leistungen fällt äusserst positiv aus. Ich bin ausserordentlich zufrieden, da ich alle meine gesetzten Ziele erreicht habe und den vorgegebenen Zeitplan erfolgreich eingehalten habe. Die erzielten Ergebnisse sind für mich ein Beweis für meine harte Arbeit und Einsatzbereitschaft.

Während dieses Projekts konnte ich eine Fülle an wertvollen Erfahrungen sammeln. Insbesondere habe ich meine Kenntnisse und Fähigkeiten im Umgang mit Windows Servern und anderen relevanten Services erheblich verbessert. Diese neuen Fähigkeiten werden mir zweifellos helfen, zukünftige Aufgaben schneller und effizienter zu bewältigen.

3 Netzwerk

3.1 Netzwerk Plan



3.2 OPNsense (PC-Engine)

3.2.1 Übersicht

Die folgende Tabelle enthält eine Übersicht über die eingesetzten Access Points in der Infrastruktur:

PC Engine apu4d4			
	OPNsense	1800 Mbit/s	Anzahl Ports: 4

Benutzername: root
Passwort: opnsense

3.2.2 Informationen

Der PC Engine APU4D4 ist ein leistungsstarkes Mini-PC-System, das von PC Engines entwickelt wurde.

Prozessor

Der PC Engine APU4D4 wird von einem AMD Embedded G-Serie GX-412TC Quad-Core-Prozessor mit einer Taktfrequenz von 1 GHz angetrieben. Dieser Prozessor bietet eine solide Leistung für verschiedene Anwendungen.

Speicher

Das System verfügt über 4 GB DDR3-RAM, der ausreichend Kapazität für die meisten Aufgaben bietet. Es unterstützt auch mSATA-Speicherlaufwerke für schnelle Datenübertragungsraten.

Anschlüsse

Der PC Engine APU4D4 ist mit einer Vielzahl von Anschlüssen ausgestattet, darunter 3 Gigabit-Ethernet-Anschlüsse, 4 USB 2.0-Anschlüsse, 1 HDMI-Anschluss und 1 serieller Anschluss. Diese Anschlüsse ermöglichen eine flexible Konnektivität und erweiterte Einsatzmöglichkeiten.

Betriebssysteme

Das System unterstützt verschiedene Betriebssysteme, darunter Linux, FreeBSD und Windows. Benutzer haben die Möglichkeit, das Betriebssystem ihrer Wahl zu installieren und anzupassen.

Netzwerkleistung

Der PC Engine APU4D4 ist für seine beeindruckende Netzwerkleistung bekannt. Mit den drei Gigabit-Ethernet-Anschlüssen können Sie das System als Router, Firewall oder andere Netzwerkgeräte einsetzen.

Energieeffizienz

Das System zeichnet sich durch seine Energieeffizienz aus. Mit einem geringen Stromverbrauch ist der PC Engine APU4D4 eine umweltfreundliche Wahl, die auch Betriebskosten senkt.

Einsatzgebiete

Der PC Engine APU4D4 eignet sich für verschiedene Anwendungen, darunter Heimnetzwerke, kleine Büros, IoT-Projekte und experimentelle Entwicklung. Aufgrund seiner Kompaktheit kann er in beengten Umgebungen problemlos eingesetzt werden.

Zuverlässigkeit

PC Engine ist bekannt für die Herstellung zuverlässiger und langlebiger Produkte. Der PC Engine APU4D4 ist keine Ausnahme und bietet eine hohe Zuverlässigkeit für den langfristigen Betrieb.

3.2.3 Installation & Konfiguration

Die PC Engine hat ein Web GUI zur Einrichtung, welches über die IP-Adresse erreichbar ist.

3.2.3.1 Basis Installation

1. Für die Konfiguration habe ich den Switch nicht ans Netzwerk angeschlossen, damit er keine IP-Adresse über DHCP bekommt.
2. Client und PC Engine mit einem Serial RS232 Kabel verbinden.
3. Im Gerätemanager den Serial COM Port herausfinden. (z.b. COM5)
4. Mit PuTTY eine Serial Verbindung herstellen:

Serial line: COM5 Speed: 115200

Connection type: ☐ SSH ☒ Serial ☐ Other: Telnet

5. PC Engine über das Terminal zurücksetzen.
6. Web GUI (OPNsense) mit der IP-Adresse 192.168.1.1 aufrufen.
7. OPNsense Wizard durchführen.
8. LAN auf fixe IP-Adresse setzen. (192.168.1.1)
9. WAN auf DHCP belassen.
10. PC Engine mit dem WAN verbinden.
11. Im Dashboard überprüfen, ob eine korrekte IP abgeholt wurde.

3.2.3.2 DHCP-Service Deaktivieren

1. Web GUI (192.168.1.1) aufrufen
2. Services → DHCPv4 → LAN
3. Bei „Enable“ den Haken entfernen. (Disablen)
4. Auf „Speichern“ drücken.

Manual: <https://www.pceingines.ch/pdf/apu4.pdf>

3.3 Switches

3.3.1 Übersicht

Die folgende Tabelle enthält eine Übersicht über die eingesetzten Access Points in der Infrastruktur:

Netgear ProSafe 8 Port Gigabit Smart Switch GS108T		
VLAN unterstützt	16 GB/s	Anzahl Ports: 8

Benutzername: -
 Passwort: password

3.3.2 Informationen

Der Netgear ProSafe 8 Port Gigabit Smart Switch GS108T ist ein leistungsstarker Netzwerkschwitch, der speziell für kleine und mittlere Unternehmen entwickelt wurde. Hier sind einige Fakten über den GS108T:

Anschlüsse

Der GS108T verfügt über acht Gigabit-Ethernet-Ports, die eine schnelle und zuverlässige Verbindung für Ihre Netzwerkgeräte bieten. Diese Ports unterstützen automatische Geschwindigkeitserkennung und sind abwärtskompatibel mit 10/100Mbps-Geräten.

Gigabit-Geschwindigkeit

Mit einer Bandbreite von bis zu 16 Gbps ermöglicht der GS108T schnelle Datenübertragungen und unterstützt reibungslose Netzwerkaktivitäten, wie z.B. das Streamen von HD-Videos, das Übertragen grosser Dateien und das Spielen von Online-Spielen ohne Verzögerungen.

VLAN-Unterstützung

Der GS108T bietet VLAN-Unterstützung (Virtual Local Area Network), mit der Sie Ihr Netzwerk in separate virtuelle Segmente aufteilen können. Dies ermöglicht eine verbesserte Netzwerksicherheit, da Datenverkehr zwischen den VLANs isoliert werden kann.

Quality of Service (QoS)

Mit QoS-Funktionen können Sie die Bandbreite priorisieren und bestimmten Netzwerkverkehr priorisieren. Dies ist besonders nützlich, um sicherzustellen, dass zeitkritische Anwendungen wie VoIP-Telefonie oder Videokonferenzen eine stabile und zuverlässige Verbindung haben.

Einfache Verwaltung

Der GS108T verfügt über eine webbasierte Benutzeroberfläche, die eine einfache Konfiguration und Verwaltung des Switches ermöglicht. Sie können den Status der Ports überwachen, VLANs einrichten, QoS-Einstellungen anpassen und vieles mehr.

Energiesparend

Der GS108T unterstützt Energy Efficient Ethernet (IEEE 802.3az), das den Stromverbrauch reduziert, wenn die angeschlossenen Geräte inaktiv sind oder nur wenig Datenverkehr generieren. Dies hilft, den Energieverbrauch zu senken und Kosten zu sparen.

Sicherheit

Der GS108T bietet erweiterte Sicherheitsfunktionen wie Zugangskontrolllisten (ACLs) und MAC-basierte Port-Sicherheit, um unautorisierten Zugriff auf das Netzwerk zu verhindern.

Flexibilität

Dank seines kompakten Designs und der Möglichkeit zur Wandmontage kann der GS108T flexibel in verschiedenen Umgebungen eingesetzt werden. Er eignet sich ideal für kleine Büros, Arbeitsgruppen oder Heimnetzwerke.

3.3.3 Installation & Konfiguration

Der Switch hat ein Web GUI zur Konfiguration, welches über die IP-Adresse erreichbar ist.

3.3.3.1 Basis Installation

1. Für die Konfiguration habe ich den Switch nicht ans Netzwerk angeschlossen, damit er keine IP-Adresse über DHCP bekommt.
2. Als Nächstes habe ich mich mit einem LAN-Kabel mit meinem Client verbunden.
3. Meinen Client habe ich mit einer statischen IP-Adresse ins 192.168.0.XX Netzwerk getan.
4. Mit 192.168.0.239 kommt man über den Browser auf das Web GUI.
5. Danach habe ich eine statische IP-Adresse mit dem Subnetz, welches in meinem Netzwerk benutzt wird, gesetzt. → 192.168.1.5

Manual: https://www.downloads.netgear.com/files/GS108T_UM_11Feb08.pdf

3.4 Access Point

3.4.1 Übersicht

Die folgende Tabelle enthält eine Übersicht über die eingesetzten Access Points in der Infrastruktur:

Netgear Business AX1800 dual Band Wireless Access Point		
Wi-Fi 6	1800 Mbit/s	Anzahl Ports: 4

Benutzername: admin
Passwort: Rs240806
WiFi: HomeNet Connect
Passwort: HomenetC

3.4.2 Informationen

Der Netgear Business AX1800 Access Point ist ein leistungsstarker WLAN-Access-Point, der für den Einsatz in geschäftlichen Umgebungen entwickelt wurde.

WLAN-Standard

Der Access Point unterstützt den neuesten WLAN-Standard 802.11ax, auch bekannt als Wi-Fi 6. Dadurch bietet er schnellere Geschwindigkeiten, eine höhere Kapazität und eine verbesserte Leistung im Vergleich zu älteren WLAN-Standards.

Geschwindigkeit

Der Netgear Business AX1800 Access Point bietet eine kombinierte WLAN-Geschwindigkeit von bis zu 1800 Mbit/s. Dies ermöglicht schnelle drahtlose Verbindungen für eine Vielzahl von Anwendungen in einem geschäftlichen Umfeld.

Mehrere Benutzer

Dank der Unterstützung von OFDMA (Orthogonal Frequency Division Multiple Access) und MU-MIMO (Multi-User Multiple Input Multiple Output) kann der Access Point gleichzeitig mehrere Benutzer bedienen, ohne dass es zu Engpässen kommt.

Hohe Kapazität

Der AX1800 Access Point bietet eine verbesserte Kapazität, um die Anforderungen von Unternehmen mit vielen gleichzeitigen WLAN-Nutzern zu erfüllen. Dies ist ideal für Büros, Konferenzräume, Hotels und andere geschäftliche Umgebungen.

Einfache Installation

Der Netgear Business AX1800 Access Point lässt sich einfach in ein vorhandenes Netzwerk integrieren. Er verfügt über eine intuitive Benutzeroberfläche, die eine schnelle und problemlose Einrichtung ermöglicht.

Sicherheit

Der Access Point unterstützt verschiedene Sicherheitsfunktionen, darunter WPA3 (Wi-Fi Protected Access 3), um ein hohes Mass an WLAN-Sicherheit zu gewährleisten. Damit sind sensible, geschäftliche Daten vor unbefugtem Zugriff geschützt.

PoE-Unterstützung

Der Access Point unterstützt Power over Ethernet (PoE), sodass er über ein einziges Ethernet-Kabel mit Strom versorgt werden kann. Dies erleichtert die Installation und vermeidet zusätzliche Verkabelung.

Skalierbarkeit

Der Netgear Business AX1800 Access Point ist skalierbar und kann nahtlos mit anderen Access Points desselben Modells oder mit anderen Netgear Business-Produkten zu einem umfassenden WLAN-Netzwerk für grössere Unternehmensumgebungen erweitert werden.

Kundensupport

Netgear bietet für den AX1800 Access Point umfassenden Kundensupport, der bei Fragen oder Problemen zur Verfügung steht. Dies gewährleistet eine zuverlässige Unterstützung und eine reibungslose Integration des Access Points in die bestehende Netzwerkinfrastruktur.

3.4.1 Installation & Konfiguration

Der Access Point hat ein Web GUI zur Einrichtung, welches über die IP-Adresse erreichbar ist.

3.4.1.1 Basis Installation

1. Für die Konfiguration habe ich den Access Point nicht ans Netzwerk angeschlossen, damit er keine IP-Adresse über DHCP bekommt.
2. AP zurücksetzen.
3. Als Nächstes habe ich mich mit einem LAN-Kabel mit meinem Client verbunden.
4. Mit 192.168.1.1 kommt man über den Browser auf das Web GUI.
5. Das Passwort auf „Rs240806“ geändert.
6. Von „Router“ in den „Access Point“ Modus gewechselt.
7. Danach habe ich eine statische IP-Adresse mit dem Subnetz, welches in meinem Netzwerk benutzt wird, gesetzt. → 192.168.1.10

Manual: https://www.downloads.netgear.com/files/GDC/WAX204/WAX204_UM_EN.pdf

3.5 Windows Server

3.5.1 Übersicht

Benutzername: Administrator
Passwort: Rs240806
Oder Active Directory User

3.5.2 Informationen

Der Windows Server 2019 ist eine beliebte Betriebssystemplattform, die speziell für die Bereitstellung von Serverdiensten und die Verwaltung von Unternehmensnetzwerken entwickelt wurde. Hier sind einige Fakten über den Windows Server 2019:

Leistungsfähigkeit

Der Windows Server 2019 bietet verbesserte Leistung und Skalierbarkeit im Vergleich zu seinen Vorgängerversionen. Er unterstützt bis zu 24 TB RAM und 640 logische Prozessoren, was ihn ideal für anspruchsvolle Workloads macht.

Hybrid Cloud-Integration

Eine der herausragenden Funktionen des Windows Server 2019 ist die nahtlose Integration mit der Microsoft Azure Cloud. Unternehmen können ihre lokalen Serverinfrastrukturen einfach mit der Cloud verbinden und hybride Szenarien implementieren, um Flexibilität und Skalierbarkeit zu gewährleisten.

Sicherheit

Der Windows Server 2019 bietet verbesserte Sicherheitsfunktionen, um Unternehmensdaten zu schützen. Dazu gehören Windows Defender Advanced Threat Protection (ATP), das Bedrohungen frühzeitig erkennt und darauf reagiert, sowie Funktionen wie die Windows Defender Exploit Guard, die vor Exploits und Zero-Day-Angriffen schützen.

Software-defined Networking (SDN)

Mit dem Windows Server 2019 können Unternehmen ihre Netzwerkinfrastruktur effizienter verwalten und flexible Netzwerklösungen implementieren. SDN-Funktionen ermöglichen die Virtualisierung von Netzwerkkomponenten und die Automatisierung von Netzwerkaufgaben.

Hyper-Converged Infrastructure (HCI)

Der Windows Server 2019 unterstützt die HCI-Technologie, die es Unternehmen ermöglicht, ihre Rechen-, Speicher- und Netzwerkressourcen in einer einzigen Plattform zu konsolidieren. Dadurch werden die Kosten gesenkt und die Verwaltung vereinfacht.

Container-Unterstützung

Der Windows Server 2019 bietet umfangreiche Unterstützung für Container, sowohl für Windows- als auch für Linux-Container. Unternehmen können Container nutzen, um Anwendungen leichter zu isolieren, bereitzustellen und zu skalieren.

Verbesserte Administrationstools

Mit dem Windows Admin Center bietet der Windows Server 2019 eine moderne und benutzerfreundliche Schnittstelle zur Verwaltung von Servern und Clustern. Administratoren können Aufgaben wie die Überwachung der Leistung, das Einrichten von Sicherheitsrichtlinien und das Konfigurieren von Speicherressourcen einfach und effizient durchführen.

Lange Unterstützungszeit

Microsoft bietet für den Windows Server 2019 einen erweiterten Supportzeitraum von 10 Jahren, bestehend aus fünf Jahren Mainstream-Support und fünf Jahren erweitertem Support. Dies gewährleistet langfristige Stabilität und Zuverlässigkeit für Unternehmen, die den Server einsetzen.

3.5.1 Installation & Konfiguration

3.5.1.1 Basis Installation

1. Windows Server 2019 Boot Stick flashen. (Wenn UEFI muss **MBR** ausgewählt sein.)
2. Von USB-Stick booten
3. Windows Server Installation durchführen.

3.5.1.2 Google Chrome installieren

1. Google Chrome Installer auf Client downloaden.
2. Den Installer auf USB-Stick kopieren.
3. Installation auf Windows Server durchführen.

3.5.1.3 Server Umbenennen

1. Windows Einstellungen öffnen
2. System → About → „Rename this PC“
3. Name vergeben (z.b. WinServ01)
4. Auf „Übernehmen“ klicken.

3.5.1.4 DNS

1. Statische IP-Adresse geben (192.168.1.2)
2. DNS-Service hinzufügen
 - 1) Windows Server Manager öffnen
 - 2) Manage → Add Roles and Features
 - 3) „DNS-Server“ aktivieren
 - 4) Installieren
3. DNS-Service Konfigurieren
 - 1) Tools → DNS
 - 2) Rechtsklick auf den Server

- 3) „Configure a DNS-Server ...“
- 4) „Create forward and reverse lookup zones“
- 5) „Primary Zone“
- 6) Bei der „Network ID“ wird die Netzwerkadresse eingetragen. (192.168.1)

3.5.1.5 DHCP

1. DHCP-Service hinzufügen
 - 1) Windows Server Manager öffnen
 - 2) Manage → Add Roles and Features
 - 3) „DHCP-Server“ aktivieren
 - 4) Installieren
2. DHCP-Konfigurieren
 - 1) Es sollte nun ein „Gelbes Warndreieck“ im „Windows Server Manager“ erscheinen.
 - 2) Bei dem Warndreieck auf „DHCP-Konfiguration abschliessen“ klicken.
 - 3) Den schritten folgen.
 - 4) Tools → DHCP
 - 5) Rechts Klick auf „IPv4“
 - 6) Properties → erweitert → Anmeldedaten
 - i. User name: Administrator
 - ii. Domain: your Domain (ZLI.LOCAL)
 - iii. Passwort: Von Administrator (Rs240806)
 - 7) Rechts Klick auf „IPv4“
 - 8) „New Scope...“
 - 9) Start und End Range der IP-Adresse festlegen. (192.168.1.100 – 192.168.1.250)
 - 10) DNS-Adresse ist die IP des Windows Servers mit dem DNS. (192.168.1.2)
3. Statische IP-Adresse vergeben (Optional)
 - 1) Tools → DHCP
 - 2) Server → IPv4 → Scope
 - 3) Rechtsklick auf „Reservations“ und dann auf „New Reservation ...“.
 - 4) IP-Adresse, welche das Gerät bekommen sollte.
 - 5) MAC-Adresse des Gerätes
 - 6) Add

3.5.1.6 Active Directory (AD)

1. Active Directory Service hinzufügen
 - a. Windows Server Manager öffnen
 - b. Manage → Add Roles and Features
 - c. „Active Directory Domain Services“ aktivieren
 - d. Automatisch neu starten aktivieren
 - e. Installieren
2. Server zu Domaincontroller machen
 - a. Es sollte nun ein „Gelbes Warndreieck“ im „Windows Server Manager“ erscheinen.
 - b. Bei dem Warndreieck auf „Server zu einem Domänencontroller heraufstufen“ klicken.
 - c. Neue Gesamtstruktur hinzufügen
 - d. Domain Name eintragen. (zli.local)
 - e. Passwort setzen. (Rs240806)
 - f. „DNS-Delegierung erstellen“
 - g. Ändern
 - i. User name: Administrator
 - ii. Passwort: Rs240806
 - h. Installieren
 - i. Restarten

3.5.1.7 Backup

3.5.1.7.1 Backup erstellen

1. Backup Service Hinzufügen
 - j. Windows Server Manager öffnen

- k. Manage → Add Roles and Features
 - l. „Windows Server Backup“ aktivieren
 - m. Installieren
3. Backup erstellen
- a. Tools → Windows Server Backup → „Local Backup“
 - b. Externe Festplatte in Server einstecken
 - c. Backup Once
 - d. Full Server
 - e. Local Drives
 - f. Backup Destination: Drive auswählen
 - g. Backup ausführen

3.5.1.7.2 Backup wiederherstellen

- h. Windows Server Bootstick flashen
- i. Von BIOS in USB-Stick booten
- j. **„Repair your Computer“ auswählen und nicht Installieren!**
- k. Recovery / Wiederherstellen
- l. Aus Backup wiederherstellen
- m. Drive auswählen
- n. Gewünschtes Backup auswählen
- o. Wiederherstellung ausführen

3.5.1.8 Policy Management

- 1. Tools → „Group Policy Management“
- 2. Rechts Klick auf „Default Domain Policy“ → Edit ...
- 3. Hier können Computer oder User spezifische Regeln vergeben werden.
- 4. Beispiel Logon-Skript:
 - a. Computer → Policies → Windows Settings → Scripts (Startup/Shutdown) → Startup
 - b. Add Logon Script in den geöffneten Ordner verschieben
 - c. Verschobenes Script auswählen.
 - d. Apply
- 5. Auf Client müssen die Policies übernommen werden.
 - a. CMD auf Client öffnen
 - b. „gpupdate /force“ ausführen
 - c. Neustarten

3.6 Clients

In der folgenden Tabelle sind die Anwender mit den zugehörigen Clients alphabetisch aufgelistet:

Anwender	Clientname	Bemerkung
AD User von Zli.local	UbuClient01	
AD User von Zli.local	WinClient01	Logon Script (Timestamp)
Robin Schneider	DESKTOP-J76KAKH	Privat-Client

3.7 Datensicherung

3.7.1 Datensicherungs-Konzepte

Vollständige Datensicherung

Bei diesem Konzept werden alle Daten eines Systems oder einer Anwendung regelmässig vollständig gesichert. Dies bedeutet, dass jede Datei und jeder Ordner gesichert wird, unabhängig davon, ob sie seit der letzten Sicherung geändert wurden oder nicht. Die vollständige Datensicherung bietet eine umfassende Wiederherstellungsmöglichkeit, erfordert jedoch oft mehr Speicherplatz und längere Sicherungszeiten.

Inkrementelle Datensicherung

Bei der inkrementellen Sicherung werden nur die Änderungen seit der letzten Sicherung gesichert. Anstatt alle Dateien zu sichern, werden nur die neuen oder geänderten Dateien gesichert. Dadurch werden Speicherplatz und Sicherungszeit reduziert. Bei der Wiederherstellung müssen jedoch sowohl die letzte vollständige Sicherung als auch alle inkrementellen Sicherungen seitdem wiederhergestellt werden.

Differentielle Datensicherung

Ähnlich wie bei der inkrementellen Sicherung werden bei der differentiellen Sicherung nur die Änderungen seit der letzten Sicherung gesichert. Der Unterschied besteht darin, dass bei der Wiederherstellung nur die letzte vollständige Sicherung und die letzte differentielle Sicherung wiederhergestellt werden müssen, was den Prozess vereinfacht. Allerdings nimmt der Speicherplatzbedarf mit jeder differentiellen Sicherung zu, da alle Änderungen seit der letzten vollständigen Sicherung gespeichert werden.

Spiegelung

Die Spiegelung ist eine Methode der Echtzeit-Datensicherung, bei der Daten kontinuierlich von einer Quelle auf ein separates Zielmedium gespiegelt werden. Jede Änderung an den Quelldaten wird sofort auf das Spiegelmedium übertragen, wodurch ein nahezu sofortiger Wiederherstellungspunkt entsteht. Dieses Konzept bietet eine hohe Ausfallsicherheit, erfordert jedoch zusätzlichen Speicherplatz und geeignete Hardware.

Sicherung in die Cloud

Dieses Konzept beinhaltet das Sichern von Daten auf externe Server oder Cloud-Speicherlösungen. Die Daten werden über das Internet auf entfernte Server hochgeladen und dort gespeichert. Die Sicherung in die Cloud bietet den Vorteil der Skalierbarkeit, des Fernzugriffs und des Schutzes vor lokalen Katastrophen. Allerdings können die Kosten für den Speicherplatz und die Übertragungsbandbreite je nach Datenmenge anfallen.

3.7.1.1 Volldatensicherung

Bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einem zusätzlichen Datenträger gespeichert.

Vorteil: Alle Daten liegen komplett vor. Sie müssen bei der Wiederherstellung der Dateien nicht lange suchen.

Nachteil: Je nachdem, wie viele Daten Sie speichern, kann die Volldatensicherung sehr zeitaufwendig sein und viel Platz auf dem Speichermedium verbrauchen.

3.7.2 Wann werden Datensicherungen durchgeführt?

Die Datensicherung erfolgen manuell, nach jedem erreichten Zwischenziel oder bevor eine riskante Aktion durchgeführt wird.

3.7.3 Welche Daten werden gesichert?

Im Folgenden wird beschrieben, welche Daten bzw. Laufwerke wann und wie gesichert werden.

Laufwerke / Daten	Vollsicherung	Teilsicherung	Uhrzeit
Bare metal recovery	✗		-
Share Drive (E:)	✗		-

System (D:)	×		-
System Reserved (G:)	×	×	-
System state	×	×	-
Volume (C:)	×	×	-

3.7.4 Wo werden die Daten gespeichert?

In der folgenden Tabelle wird ersichtlich, wo die Sicherungsbänder aufbewahrt werden:

Sicherungsband	Ort der Aufbewahrung
Alle Backup	Blj-informatik (Externe Festplatte)

4 Glossar

In folgender Tabelle sind die Begriffe und Abkürzungen beschrieben, die in dieser Netzwerkdokumentation verwendet werden.

AD	Active Directory
OU	Organisation Units (Organisationseinheiten)
AP	Access Point
HO	Homeoffice
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EMCO	EMCO Remote Installer/EMCO MSI Package Builder (Software)
IP	Internet Protocol
LAN	Local Area Network
OPNsense	Open Source Firewall- und Router-Plattform
RDP	Remote Desktop Protocol
SD-Karte	Secure Digital Memory Card
VPN	Virtual Private Network
WAN	Wide Area Network

5 Quellen

5.1 Verwendete Webseiten

Handout & Präsentation

<https://Canva.com>

Netzwerk Diagramm

<https://Lucid.app>

QR-Code Generator

<https://www.qrcode-generator.ch/>

Sonstiges

<https://chat.openai.com/>

5.2 Tutorials

Grund Installation:

https://www.youtube.com/watch?v=VKY9bnWUmAk&list=PLy_SLVh0nNAme8mFRyeGRdr-IAw55JZ_b

DNS

https://www.youtube.com/watch?v=l2zyAjNeph4&list=PLy_SLVh0nNAme8mFRyeGRdr-IAw55JZ_b&index=2

DHCP

https://www.youtube.com/watch?v=4m1O3QrpH8A&list=PLy_SLVh0nNAme8mFRyeGRdr-IAw55JZ_b&index=3

AD

https://www.youtube.com/watch?v=N7SVsawfWRY&list=PLy_SLVh0nNAme8mFRyeGRdr-IAw55JZ_b&index=4

Freigaben

https://www.youtube.com/watch?v=nTigg619u9I&list=PLy_SLVh0nNAme8mFRyeGRdr-IAw55JZ_b&index=5

Backup

https://www.youtube.com/watch?v=NyBHbYrNEqA&list=PLy_SLVh0nNAme8mFRyeGRdr-IAw55JZ_b&index=8

Logon Script AD

<https://www.youtube.com/watch?v=zTvWkszjIS0>

Logon Script GPO

<https://www.youtube.com/watch?v=iDb8txwnt8Q>

5.3 Bilder

<https://pixabay.com/de/>

<https://www.pexels.com/de-de/freie-und-kostenlose-bilder-finden/>

<https://unsplash.com/de>

<https://de.freepik.com/fotos-beliebt>

<https://www.shutterstock.com/de/explore/royalty-free-images>

<https://google.ch>