1 Vortrag

- Zusammensetzung der Hardware
- Auswahl des Betriebssystem
- Einrichtung und Zugriff auf OMV
- Docker
- Container
- http und https
- File System Raid und Mount
- Port freigabe
- Einrichtung der Nextcloud

1.1 Vortrag Gliederung

1. Einführung und Überblick
    - Warum hast du dich für einen Home Server entschieden?
    - Welche funktionen erfüllt dein Home Server?
    - Welche Funktionen könnte er erfüllen?
    - Vorstellung der Hardwarekomponenten
2. Betriebssystem und Software
    - Auswahl des Betriebssystems und Begründung der Entscheidung
    - Installation und Konfiguration des Betriebssystems
    - Vorstellung der verwendeten Software (z.B. OpenMediaVault, Docker, Nextcloud)
3. Dateisystem und Speichermanagement
    - Einrichtung von Raid und/oder Mounting
    - Dateisystem verwaltung und -optimierung
4. Netzwerk- und Portfreigabe
    - Konfiguration der Netzwerkverbindung
    - Einrichtung der Portfreigabe
5. Docker und Container

- Einführung in Docker und Container-Technologie
- Erstllung und Verwaltung von Containern in Portainer

6. Webserver und Sicherheit
    - Konfiguration von HTTP und https
    - Einrichtung eines Webservers und SSL-Zertifikaten
    - Sicherheitsaspekte bei der Verwendung von öffentlich zu gänglichen Servern
7. Nextcloud und Zugriffsverwaltung
    - Einrichtung der Nextcloud-Plattform auf dem Home Server
    - Konfiguration der Zugriffsrechten und -Sicherheit

1.2 Einführung und Überblick

In diesem Vortrag möchte ich euch meinen Home Server vorstellen. Ich habe mich für dieses Projekt entschieden, da ich eine sichere Cloud-Speicherlösung haben wollte, die nicht auf unbekannten Servern liegt. Mein Home Server erfüllt jedoch nicht nur diese Funktion, sondern hat auch noch weitere nützliche Features.

- Medienserver: Ein Home Server kann als Medienserver genutzt werden, um Filme, Musik und Fotos in einem Heimnetzwerk zu streamen.
- Backup-Server: Ein Home Server kann als Backup-Server dienen, um wichtige Dateien und Daten automatisch zu sichern und zu schützen.
- Zentrale Speicherlösung: Ein Home Server kann als zentrale Speicherlösung für verschiedene Geräte und Computer im Heimnetzwerk dienen, um Daten und Dateien gemeinsam zu nutzen.
- Anwendungs- und Datenbankserver: Ein Home Server kann auch als Anwendungs- und Datenbankserver dienen, um spezielle Anwendungen und Software im Heimnetzwerk zu nutzen.
- Webserver: Ein Home Server kann als Webserver genutzt werden, um Websites und Webanwendungen zu hosten.
- Netzwerk- und Sicherheitslösung: Ein Home Server kann als Netzwerk- und Sicherheitslösung eingesetzt werden, um das Heimnetzwerk zu schützen und zu überwachen.

Beginnen wir mit der Frage, warum ich mich für einen Home Server entschieden habe. Ich wollte ein Informatik-Projekt starten und mir einen Cloud-Speicher zulegen, der sicher ist und nicht auf mir unbekannten Servern liegt. Ein Home Server ermöglicht mir die volle Kontrolle über meine Daten und ich kann meine Daten sicher und zuverlässig speichern.

Die Hauptfunktion meines Home Servers ist der Cloud-Speicher, der mir ermöglicht, meine Daten sicher und zuverlässig zu speichern und von überall darauf zuzugreifen. Darüber hinaus kann mein Home Server auch als Media-Server genutzt werden, um Filme, Musik und Fotos in meinem Netzwerk zu streamen. Auch ein Backup-Server ist eine weitere nützliche Funktion meines Home Servers.

Nun zu den Hardwarekomponenten meines Home Servers. Ich nutze einen alten PC, der mit einem Intel(R) Core(TM) i7 CPU 870 Prozessor ausgestattet ist. Der Prozessor hat eine Taktfrequenz von 2,93 GHz und mein System Memory beträgt 6144 MB. In meinem Home Server ist eine 3 TB HDD-Festplatte eingebaut, auf der ich meine Daten speichere, sowie eine 500 GB HDD-Festplatte, auf der das Betriebssystem läuft.

1.3 Betriebssystem und Software

Bei der Auswahl des Betriebssystems für den Home Server standen mehrere Optionen zur Verfügung. Unraid sah zwar vielversprechend aus, war jedoch kostenpflichtig. TrueNAS Core oder Scale hatten hohe Anforderungen an die Hardware, insbesondere den Arbeitsspeicher (mind. 8 GB), während ich nur 6 GB hatte. Proxmox war ebenfalls eine Option, wurde aber schließlich verworfen.

OpenMediaVault ist ein Open-Source-Betriebssystem, das auf Debian Linux basiert und speziell für den Einsatz als Netzwerkattached-Storage (NAS) entwickelt wurde. Es ist eine leichte und einfach zu bedienende Plattform, die es Benutzern ermöglicht, ihre eigenen NAS-Server aufzusetzen und zu verwalten.

OpenMediaVault bietet zahlreiche Funktionen, die es Benutzern ermöglichen, ihre Daten sicher und zuverlässig zu speichern und darauf zuzugreifen. Dazu gehören eine webbasierte Benutzeroberfläche, die es einfach macht, das Betriebssystem und seine Dienste zu konfigurieren und zu verwalten, sowie Unterstützung für verschiedene Netzwerkprotokolle wie SMB/CIFS, NFS, FTP, SSH, RSync und mehr.

Darüber hinaus bietet OpenMediaVault auch eine Vielzahl von Erweiterungen und Plugins, die Benutzer installieren können, um zusätzliche Funktionen hinzuzufügen, wie z.B. einen

Torrent-Client, eine Medien-Streaming-Plattform oder einen Webserver.

Insgesamt ist OpenMediaVault eine leistungsstarke und flexible Plattform, die es Benutzern ermöglicht, ihre eigenen NAS-Server zu erstellen und anzupassen, um ihren spezifischen Bedürfnissen und Anforderungen gerecht zu werden.

Die Installation von OpenMediaVault war sehr einfach. Nach dem Booten des Systems von einem USB-Stick musste nur das Land und die Zeitzone festgelegt und ein Root-Passwort eingerichtet werden. Danach konnte die weitere Konfiguration über den Browser erfolgen.

Dannach wurde noch OMV-Extra über das Terminal installiert es ermöglicht die verwendung von Docker und Portainer. Darauf komm ich später zurück.

1.4 Dateisystem und Speichermanagement

Um Daten auf dem Home Server effizient zu verwalten und zu schützen, wurde die Einrichtung von RAID und/oder Mounting vorgenommen. Mit OpenMediaVault ist es sehr einfach, verschiedene RAID-Level zu erstellen und Dateisysteme zu mounten. Ein RAID (Redundant Array of Independent Disks) ist eine Methode, um Daten auf mehreren Festplatten redundant zu speichern, um Datenverlust im Falle eines Festplattenausfalls zu vermeiden.

In OMV wurde ein RAID-5-Array erstellt, das aus drei Festplatten besteht. RAID-5 bietet sowohl Schutz als auch eine relativ hohe Kapazität. Sollte eine der Festplatten ausfallen, können die Daten immer noch von den verbleibenden Festplatten wiederhergestellt werden.

Neben RAID-5 wurde auch Mounting verwendet, um verschiedene Festplatten und Partitionen zu einem einzigen, großen Datenspeicher zu verbinden. Hierdurch wird eine bessere Nutzung des verfügbaren Speicherplatzes ermöglicht und eine vereinfachte Verwaltung des Dateisystems erreicht.

OMV bietet auch verschiedene Tools zur Verwaltung und Optimierung von Dateisystemen. So können beispielsweise bestimmte Dateitypen oder -größen automatisch in separate Verzeichnisse verschoben werden, um die Lesegeschwindigkeit zu verbessern. Außerdem können Dateisysteme auf Fehler überprüft und repariert werden, um die Datenintegrität sicherzustellen.

Insgesamt ermöglichen die RAID- und Mounting-Optionen von OMV eine flexible und robuste Verwaltung des Datenspeichers und bieten gleichzeitig Schutz vor Datenverlust. Die Verwaltung und Optimierung des Dateisystems tragen zudem zur besseren Leistung des Home

Servers bei.

1.5 Docker und Container

Dannach wurde noch OMV-Extra über das Terminal installiert es ermöglicht die verwendung von Docker und Portainer.

OMV-Extras ist ein Repository-Plugin für das OpenMediaVault-Betriebssystem, das es Benutzern ermöglicht, zusätzliche Erweiterungen und Plugins zu installieren, die nicht standardmäßig in OMV enthalten sind.

Das Plugin bietet Zugriff auf eine Vielzahl von Erweiterungen und Add-Ons, die von der OMV-Community erstellt wurden, wie z.B. Backup-Tools, Cloud-Speicher-Integration, Medien-Streaming-Software und vieles mehr.

OMV-Extras vereinfacht den Installationsprozess für diese Erweiterungen und sorgt dafür, dass sie sicher und stabil auf dem System ausgeführt werden. Es ist einfach zu installieren und zu verwenden, und es bietet Benutzern eine einfache Möglichkeit, ihre OMV-Server zu erweitern und anzupassen, um ihren spezifischen Bedürfnissen und Anforderungen gerecht zu werden.

Insgesamt ist OMV-Extras ein sehr nützliches Plugin für OMV-Benutzer, die ihr System erweitern und anpassen möchten, und es ist ein wichtiger Bestandteil der OMV-Community und der OMV-Erfahrung.

Docker und Container

Docker ist eine beliebte Container-Plattform, die es ermöglicht, Anwendungen in Containern zu isolieren und zu verwalten. Container sind eine Art virtuelle Umgebung, die eine Anwendung und ihre Abhängigkeiten in sich geschlossen halten und so verhindern, dass sie mit anderen Anwendungen auf demselben System kollidieren. Docker ist daher eine nützliche Technologie für Home Server, da sie die Möglichkeit bietet, verschiedene Anwendungen auf einem einzigen System auszuführen, ohne dass Konflikte zwischen ihnen entstehen.

In unserem Home Server wurde Docker verwendet, um verschiedene Anwendungen in Containern auszuführen. Zum Beispiel wurde ein Container für die Nextcloud-Instanz erstellt, ein weiterer Container für das Heimautomatisierungssystem und ein dritter Container für ein Videoüberwachungssystem.

Die Erstellung und Verwaltung von Containern in Docker kann durch die Verwendung von

Portainer vereinfacht werden. Portainer ist eine grafische Benutzeroberfläche für Docker, die es ermöglicht, Container zu erstellen, zu starten und zu stoppen, ohne dass man sich mit der Kommandozeile auseinandersetzen muss.

Die Verwendung von Containern hat viele Vorteile, wie zum Beispiel die einfache Installation und Deinstallation von Anwendungen, die Möglichkeit, verschiedene Versionen derselben Anwendung nebeneinander auszuführen und die Möglichkeit, schnell auf Änderungen in der Systemumgebung zu reagieren. Docker und Container sind daher eine nützliche Technologie für Home Server und können die Flexibilität und Zuverlässigkeit des Systems verbessern.

Portainer ist eine webbasierte grafische Benutzeroberfläche für die Verwaltung von Docker-Containern und Swarm-Clustern. Es bietet eine einfache Möglichkeit, Docker-Container zu erstellen, zu starten, zu stoppen und zu überwachen, ohne dass man sich mit der Kommandozeile auseinandersetzen muss. Mit Portainer können Benutzer schnell und einfach Container erstellen und verwalten, und die Benutzeroberfläche macht es auch für unerfahrene Benutzer einfach, komplexe Aufgaben auszuführen. Es ist eine Open-Source-Software, die in verschiedenen Umgebungen eingesetzt werden kann, um die Verwaltung von Docker-Containern zu vereinfachen.

1.6 Netzwerk und Portfreigabe

Vllt genauer ausführen mussten über den Server des INterbetreiber freigeben werden. Port Forwarding ist ein Prozess, bei dem ein Router oder eine Firewall so konfiguriert wird, dass bestimmte Ports von eingehenden Netzwerkverbindungen an ein bestimmtes Gerät im lokalen Netzwerk weitergeleitet werden.

Wenn ein Gerät im lokalen Netzwerk einen Port öffnet, kann es eingehende Verbindungen von anderen Geräten im lokalen Netzwerk annehmen, aber Verbindungen von Geräten im Internet oder anderen Netzwerken werden von der Firewall oder dem Router blockiert, um die Sicherheit zu gewährleisten. Port Forwarding erlaubt es, dass eingehende Verbindungen von Geräten außerhalb des lokalen Netzwerks an ein bestimmtes Gerät im lokalen Netzwerk weitergeleitet werden.

Um Port Forwarding einzurichten, muss man zuerst die IP-Adresse des Geräts im lokalen Netzwerk kennen, an das die Verbindung weitergeleitet werden soll. Man muss dann in den Einstellungen des Routers oder der Firewall eine Port-Weiterleitungskonfiguration einrichten, bei der man den Port oder die Portbereiche sowie das Zielgerät im lokalen Netzwerk angibt.

Es ist wichtig, vorsichtig zu sein, wenn man Port Forwarding verwendet, da es potenzielle

Sicherheitsrisiken mit sich bringt, wenn man nicht genau weiß, welche Ports man öffnen und an welches Gerät man weiterleiten sollte. Man sollte immer sicherstellen, dass alle offenen Ports auf dem neuesten Stand sind und dass die Geräte im lokalen Netzwerk sicher konfiguriert sind, um unautorisierten Zugriff zu vermeiden.

1.7 Websever und Sicherheit

Im Bereich des Webserver und der Sicherheit gibt es mehrere wichtige Aspekte zu berücksichtigen. Zunächst ist es wichtig, die Konfiguration von HTTP und HTTPS richtig einzustellen. Über OMV ist es möglich, sowohl für den OMV-Webserver als auch für den Portainer-Webserver die HTTPS-Verbindung zu aktivieren. HTTPS ist eine sichere Verbindung, die auf dem SSL- oder TLS-Protokoll basiert und den Datenverkehr zwischen dem Webserver und dem Browser verschlüsselt. Dadurch werden sensible Daten wie Passwörter und persönliche Informationen besser geschützt.

Um einen Webservice auf dem Home Server zu betreiben, kann ein Webserversoftware wie Apache oder Nginx installiert werden. Eine gute Möglichkeit ist die Verwendung des NGINX Proxy Managers, der es ermöglicht, mehrere Webanwendungen auf demselben Server zu hosten und dabei HTTPS-Verschlüsselung mit SSL-Zertifikaten zu nutzen. Das NGINX Proxy Manager bietet eine benutzerfreundliche Oberfläche, die es auch für Benutzer ohne viel Erfahrung einfach macht, eine Webanwendung einzurichten.

Ein weiterer wichtiger Aspekt ist die Sicherheit bei der Verwendung von öffentlich zugänglichen Servern. Es ist wichtig, sicherzustellen, dass alle Ports, die nicht benötigt werden, geschlossen sind, um potenzielle Sicherheitsrisiken zu minimieren. Darüber hinaus sollten alle Zugriffe auf den Server über verschlüsselte Verbindungen erfolgen. Es ist auch ratsam, regelmäßige Sicherheitsupdates durchzuführen, um sicherzustellen, dass der Server und die darauf laufenden Anwendungen auf dem neuesten Stand sind und potenzielle Sicherheitslücken geschlossen werden.

Insgesamt ist es wichtig, alle Aspekte der Sicherheit bei der Einrichtung und Verwendung eines Home Servers zu berücksichtigen. Eine ordnungsgemäße Konfiguration von HTTP und HTTPS, die Einrichtung von Webservern und SSL-Zertifikaten sowie die Berücksichtigung von Sicherheitsaspekten sind wichtige Schritte, um sicherzustellen, dass der Home Server sicher und effektiv betrieben werden kann.

1.8 Nextcloud und Zugriffsverwaltung

Die Einrichtung der Nextcloud-Plattform auf dem Home Server ist ein weiterer wichtiger Teil des Vortrags. Hierbei wird erklärt, wie die Nextcloud-Software auf dem Home Server installiert und konfiguriert werden kann, um einen sicheren und zuverlässigen Cloud-Speicher zu schaffen. Dabei wird auch auf die verschiedenen Konfigurationsmöglichkeiten und Einstellungen eingegangen.

Ein weiterer wichtiger Aspekt ist die Zugriffsverwaltung und -sicherheit. Hierbei geht es darum, wer Zugriff auf die Daten hat und wie diese Daten geschützt werden können. Es werden verschiedene Möglichkeiten zur Zugriffsverwaltung erläutert und gezeigt, wie man die Sicherheit erhöhen kann, z.B. durch die Verwendung von Passwörtern, Verschlüsselung oder Zwei-Faktor-Authentifizierung.

1.9 Fazit

Zusammenfassend lässt sich sagen, dass der Home Server ein vielseitiges und nützliches Werkzeug ist, das verschiedene Funktionen wie Dateispeicherung, Backup, Medien-Streaming und vieles mehr bietet. Die Verwendung von OpenMediaVault als Betriebssystem und Docker zur Container-Verwaltung erleichtert die Konfiguration und Erweiterung des Home Servers erheblich. Die Einrichtung eines Webservers mit SSL-Zertifikaten und die Konfiguration von HTTP und HTTPS erhöhen die Sicherheit und machen es möglich, auf die Nextcloud-Plattform auf dem Home Server zuzugreifen. Alles in allem bietet der Home Server eine großartige Möglichkeit, Daten zentralisiert und sicher zu speichern, auf sie zuzugreifen und sie zu teilen.