

Antrag für die nicht betriebliche Projektarbeit

20. Juni 2023

Inhaltsverzeichnis

1	Projektbezeichnung	2
1.1	Kurzform der Aufgabenstellung	2
1.2	Ist-Analyse	2
2	Soll Konzept	2
2.1	Was soll am Ende des Projektes erreicht sein?	2
2.2	Welche Anforderungen müssen erfüllt sein?	3
2.3	Welche Einschränkungen müssen berücksichtigt werden?	3
3	Projektstrukturplan entwickeln	3
3.1	Was ist zur Erfüllung der Zielsetzung erforderlich?	3
3.2	Aufgaben auflisten	4
4	Projektphasen mit Zeitplanung in Stunden	6
5	Glossar	7
6	Name der Ausbildungsstätte in dem das Projekt durchgeführt wird	9
6.1	Name des Ausbilders, Projektverantwortlichen	9

1 Projektbezeichnung

Das Aufsetzen einer Mastodon-Fediverse-Instanz unter der Domain Mastodon.de.

1.1 Kurzform der Aufgabenstellung

Eine Mastodon-Instanz soll am Ende unter der Domain mastodon.de erreichbar sein. Mastodon ist eine Software die verwendet wird als eine Art dezentralisiertes Social media. Sie sollte auch sicher vor Angriffen von außen sein, insbesondere in Bezug auf interne Admin-Panels. Zudem sollte sie melden, wenn die Hardware beschädigt oder degradiert ist, insbesondere bei Festplatten oder ähnliche Hardware.

1.2 Ist-Analyse

Durch Umzug und Aufgabe eines Rechenzentrums meines Ausbildungsbetriebs bin ich in den Besitz alter Hardware gekommen die ich zu Hause aber leider aufgrund von Platzmangel fehlender geeigneter Stromversorgung und Kühlung nicht nutzen kann. Ferner ist mir aufgefallen, dass es keine deutsche Mastodon Instanz unter der Domain mastodon.de gibt. Die Domain befindet sich bereits in meinem Besitz.

2 Soll Konzept

2.1 Was soll am Ende des Projektes erreicht sein?

Am Ende soll eine Mastodon-Instanz auf der Domain mastodon.de erreichbar sein. Nur der Port 443 soll von außen erreichbar sein, da eine DMZ vor dem Server steht. Die internen administrativen Interfaces (SSH, Admin Panel, IDRAC, ILOM usw.) sollen nur von einem Jumpgate erreichbar sein, der mit einer IPv6-Adresse von außen erreichbar sein wird und nur von whitelisted Adressen erreichbar sein sollte. Dadurch kann man die ganzen administrativen Interfaces über den Jumpgate weiterleiten, um die Sicherheit zu erhöhen. Dies ermöglicht auch eine sichere Erreichbarkeit von HTTP-Interfaces für die älteren Maschinen.

2.2 Welche Anforderungen müssen erfüllt sein?

Folgende Anforderungen müssen erfüllt sein, um das Projekt als einen Erfolg zu definieren:

- Die Mastodon-Instanz ist vom PostgreSQL-Server getrennt, um mehr Rechenleistung zur Verfügung zu haben.
- Die Storage-Server sind extern durch ein SAN-Chassis gesichert.
- Mastodon ist hinter einer DMZ auf der Domain mastodon.de geschützt.
- Der Jumpgate-Server ist über IPv6 erreichbar und nur von bestimmten, whitelisteden IP-Adressen zugänglich. Der Zugriff ist zudem nur autorisierten Personen gestattet.
- Die Seite ist sowohl über IPv4 als auch über IPv6 erreichbar.
- Monitoring :)

2.3 Welche Einschränkungen müssen berücksichtigt werden?

Das Budget, das zur Verfügung steht, ist nicht sehr hoch. Es sollte berücksichtigt werden, dass Kosten für Strom anfallen und auch Kosten für Rack-HEs sowie für den Ersatz von defekten Festplatten. Die Instanz muss vor Angriffen von außen geschützt sein, insbesondere vor dem Zugriff auf administrative Schnittstellen von außen.

3 Projektstrukturplan entwickeln

3.1 Was ist zur Erfüllung der Zielsetzung erforderlich?

Die Server werden zunächst in ein Zwischenlager gebracht und von dort aus aufgebaut. Über einen NOBGB-Provider¹ kann ich eine öffentliche IPv4-Adresse und einen /56 IPv6-Block erhalten.

¹<https://www.servperso.net/tunnel/ipwan>

3.2 Aufgaben auflisten

1. Vorbereitung
 - (a) Netzplan erstellen.
 - (b) Mastodon Dokus durchlesen.
 - (c) Mastodon und PostgreSQL Konfigurationen vorbereiten.
 - (d) NOBGB-provider² Vertrag starten.
 - (e) Mikrotik Router holen.
 - (f) Rack vermessen.
 - (g) Rackhalterungen vorbereiten.
 - (h) Debian Preseed Datei erstellen.
2. Alle Maschinen zum Zwischenlager transportieren.
 - (a) Ein VAN mieten oder das Auto vollstopfen.
 - (b) Eine Route planen.
3. Das Rack aufbauen.
 - (a) Die Rackhalterungen mit stabilen Schrauben auf ein stabiles Brett aufschrauben.
 - (b) Die Rackplatten zusammen mit den Rackmuttern in das Rack einschrauben.
 - (c) Die Server anordnen und in das Rack einlegen.
4. Die Server verkabeln.
 - (a) Den Top-of-Rack-Switch aufbauen.
 - (b) Gemäß dem Kabelplan die Kabel in die Server stecken.
 - (c) Den Management-Switch aufbauen.
 - (d) Gemäß dem Kabelplan die Kabel in die Server stecken.
 - (e) Den Top-of-Rack-Router aufbauen.
 - (f) Gemäß dem Kabelplan die Kabel in die Netzwerkgeräte stecken.
 - (g) Die Power Distribution Unit (PDU) aufbauen.
 - (h) Die Server und Switches an die PDU anschließen.
 - (i) Die Serial Console aufbauen.
 - (j) Gemäß dem Kabelplan das Serialkabel in die PDU stecken.
5. Die Management-Interfaces einrichten (IDRAC, ILOM).

²<https://www.servperso.net/tunnel/ipwan>

6. Die Server einrichten.
 - (a) Die RAID-Arrays einrichten.
7. Betriebssysteme installieren.
 - (b) Debian auf 5 USB-Sticks installieren, um die Maschinen parallel zu installieren.
 - (c) Debian auf allen Servern installieren.
 - (d) Die IP-Adressen konfigurieren.
8. Die Netzwerkgeräte einrichten.
 - (a) Den Router mit einem L2TP-Tunnel verbinden.
 - (b) Die Firewall einrichten.
 - (c) Die Routen einrichten.
 - (d) Die Switches einrichten.
9. Den Jumpgate einrichten.
 - (a) Die SSH-Konfiguration reinkopieren.
 - (b) Die Firewall-Konfiguration reinkopieren.
 - (c) Den Jumpgate als Proxy einrichten.
10. Mastodon einrichten.
 - (a) Die Software installieren.
 - (b) Das vorbereitete Konfigurationsfile reinkopieren.
11. PostgreSQL einrichten.
 - (a) Die Software installieren.
 - (b) Das vorbereitete Konfigurationsfile reinkopieren.
12. Das SAN einrichten. (Optional)
 - (a) Die RAID-Arrays einrichten.
 - (b) Die IP-Adressen konfigurieren.
 - (c) Das SAN mit anderen Servern verbinden.
 - (d) Konfigurationen auf den Servern ändern, sodass sie auf das neue SAN-Verzeichnis zeigen.
13. Die Server starten.
 - (a) Die Software testen.
 - (b) Bei Fehlern anfangen mit der der Fehlersuche am besten ab Schritt 4 neu anfangen.
14. Server Monitoring aufsetzen mit IPMI
15. Die Dokumentation schreiben.

4 Projektphasen mit Zeitplanung in Stunden

Phase	Dauer in Stunden
Vorbereitung	24
Alle Maschinen zum Zwischenlager transportieren.	12
Das Rack aufbauen.	2
Die Server verkabeln.	4
Die Management-Interfaces einrichten (IDRAC, ILOM).	3
Die Server einrichten.	2
Betriebssysteme installieren.	2-6
Die Netzwerkgeräte einrichten.	2
Den Jumpgate einrichten.	1
Mastodon einrichten.	1
PostgreSQL einrichten.	1
Das SAN einrichten. (Optional)	6
Die Server starten.	4-12
Server Monitoring aufsetzen mit IPMI	6
Die Dokumentation schreiben.	6

5 Glossar

- DMZ** Eine DMZ (Demilitarized Zone) ist eine Netzwerkzone, die zwischen dem internen Netzwerk und dem externen, unsicheren Netzwerk liegt. Sie dient als Sicherheitspuffer, um öffentlich zugängliche Dienste wie Webserver, E-Mail-Server oder FTP-Server zu isolieren und zu schützen. In der DMZ werden spezielle Sicherheitsvorkehrungen getroffen, um unbefugten Zugriff auf das interne Netzwerk zu verhindern. Die DMZ ermöglicht es, öffentliche Dienste bereitzustellen, während das interne Netzwerk geschützt bleibt. Quelle: [https://de.wikipedia.org/wiki/Demilitarisierte_Zone_\(Info](https://de.wikipedia.org/wiki/Demilitarisierte_Zone_(Info)
- IDRAC** Der Integrated Dell Remote Access Controller (iDRAC) ist ein Hardware- und Softwaremodul, das in Dell Servern eingebettet ist. Es ermöglicht Administratoren den ferngesteuerten Zugriff, die Überwachung und das Management des Servers über eine Netzwerkverbindung. Quelle: https://de.wikipedia.org/wiki/Lights_Out_Management
- ILOM** ILOM (Integrated Lights Out Manager) ist eine integrierte Managementlösung von Oracle für ihre SPARC-Server. ILOM bietet Administratoren einen ferngesteuerten Zugriff, Überwachung und das Management der Serverhardware über eine Netzwerkverbindung. Mit ILOM können Administratoren den Serverzustand überwachen, Konfigurationen ändern, Fehler diagnostizieren und Firmware-Updates durchführen. Es ermöglicht auch die Verwaltung von Energieverbrauch und Temperatur sowie die Fernsteuerung des Servers, selbst wenn das Betriebssystem nicht verfügbar ist. Quelle: https://de.wikipedia.org/wiki/Lights_Out_Management
- IPMI** IPMI (Intelligent Platform Management Interface) ist ein standardisiertes Schnittstellenprotokoll, das die Fernverwaltung von Servern und anderen Netzwerkgeräten ermöglicht. Es ermöglicht Administratoren, auf Hardwareebene auf Systeme zuzugreifen, unabhängig vom Betriebssystem oder Zustand des Servers. IPMI bietet Funktionen wie Überwachung von Hardwarezuständen, Fernzugriff auf die Konsole, Fernneustart, Energiemanagement und Ereignisbenachrichtigungen. Es ermöglicht Administratoren die effiziente Verwaltung und Diagnose von Servern, ohne dass sie physisch vor Ort sein müssen. IPMI wird oft in Rechenzentren und Unternehmensumgebungen eingesetzt, um die Verfügbarkeit und Verwaltbarkeit von Servern zu verbessern. Quelle: https://de.wikipedia.org/wiki/Intelligent_Platform_Management_Interface
- Mastodon** Mastodon ist eine dezentrale, Open-Source-basierte soziale Netzwerkplattform, die es Benutzern ermöglicht, Beiträge zu verfassen, zu teilen und mit anderen zu interagieren. Es wurde als Alternative zu zentralisierten sozialen Netzwerken entwickelt und bietet den Nutzern die Kontrolle über ihre Daten und Privatsphäre. Mastodon basiert auf dem Prinzip der Föderation, bei dem verschiedene Instanzen (Server) miteinander verbunden sind und Benutzer innerhalb dieser Instanzen miteinander interagieren können. Durch diese dezentrale Struktur fördert Mastodon die Vielfalt und Meinungsfreiheit in der Onlinekommunikation. Quelle: [https://de.wikipedia.org/wiki/Mastodon_\(Software\)](https://de.wikipedia.org/wiki/Mastodon_(Software))
- PDU** Eine Power Distribution Unit (PDU) ist eine Art von Mehrfachsteckdose, die es ermöglicht, einzelne Server aus der Ferne ein- und auszuschalten. Einige PDUs verfügen auch über Funktionen zur Strommessung und können Benachrichtigungen senden, wenn eine Leitung überlastet ist. In einigen Fällen sind PDUs mit eingebauten Sicherungen ausgestattet, um andere 8 Server zu schützen, falls ein Server plötzlich einen Fehler aufweist und die Leitung überlastet oder einen Kurzschluss verursacht. Quelle: https://de.wikipedia.org/wiki/Power_Distribution_Unit

PostgreSQL PostgreSQL ist ein leistungsstarkes, Open-Source-Datenbankmanagementsystem, das für seine Stabilität, Erweiterbarkeit und Konformität mit dem SQL-Standard bekannt ist. Es ermöglicht das Speichern und Abrufen großer Mengen strukturierter und unstrukturierter Daten. Quelle: <https://de.wikipedia.org/wiki/PostgreSQL>

RAID Ein RAID-Array (Redundant Array of Independent Disks) ist eine Technologie zur Speicherung und Organisation von Daten über mehrere Festplatten Quelle: <https://de.wikipedia.org/wiki/RAID>

Router Ein Router ist ein Netzwerkgerät, das Datenpakete zwischen verschiedenen Computernetzwerken weiterleitet. Es dient als zentrale Schaltstelle für den Datenverkehr und ermöglicht die Kommunikation zwischen Geräten in verschiedenen Netzwerken. Der Router analysiert die Zieladresse jedes Datenpakets und leitet es an das entsprechende Zielnetzwerk weiter. Zusätzlich kann ein Router Sicherheitsfunktionen wie Firewall und NAT (Network Address Translation) bieten, um das Netzwerk zu schützen und den Zugriff von außen zu kontrollieren. Router sind ein wesentlicher Bestandteil von Netzwerken, sei es in Heimnetzwerken oder großen Unternehmensnetzwerken. Quelle: <https://de.wikipedia.org/wiki/Router>

SAN Ein Storage Area Network (SAN) ist ein dediziertes Hochgeschwindigkeitsnetzwerk, das es ermöglicht, Speicherressourcen wie Festplatten und RAID-Arrays über ein Netzwerk bereitzustellen. Es dient der zentralen Speicherverwaltung und ermöglicht es mehreren Servern, gleichzeitig auf gemeinsam genutzte Speichergeräte zuzugreifen. Quelle: https://de.wikipedia.org/wiki/Storage_Area_Ne

SSH SSH (Secure Shell) ist ein Netzwerkprotokoll, das eine sichere verschlüsselte Verbindung zwischen einem Client und einem Server herstellt. Es ermöglicht die sichere Remote-Verwaltung und den Dateitransfer über unsichere Netzwerke. SSH bietet Authentifizierungsmethoden wie Passwörter oder Schlüsselpaare und verschlüsselt den gesamten Datenverkehr, um Abhör- und Manipulationsrisiken zu minimieren. Es wird häufig für die sichere Verbindung zu entfernten Servern, das Remote-Sharing von Dateien und die Ausführung von Befehlen auf entfernten Systemen verwendet. SSH ist eine wichtige Komponente für die Netzwerksicherheit und den sicheren Zugriff auf entfernte Systeme. Quelle: https://de.wikipedia.org/wiki/Secure_Shell

Switch Ein Switch ist ein Netzwerkgerät, das den Datenverkehr innerhalb eines lokalen Netzwerks (LAN) effizient verteilt. Er fungiert als zentrale Schaltstelle, um Datenpakete zwischen den angeschlossenen Geräten, wie Computern, Druckern und Servern, weiterzuleiten. Im Gegensatz zu Hubs ermöglicht ein Switch die direkte Kommunikation zwischen den Geräten, da er den Datenverkehr nur an die Zielgeräte sendet, anstatt ihn an alle Geräte im Netzwerk zu broadcasten. Dies führt zu höherer Leistung, Bandbreiteneffizienz und Sicherheit in einem Netzwerk. Switches sind in vielen Netzwerkinfrastrukturen, von Heimnetzwerken bis hin zu großen Unternehmensnetzwerken, weit verbreitet. Quelle: [https://de.wikipedia.org/wiki/Switch_\(Netzwerktechnik\)](https://de.wikipedia.org/wiki/Switch_(Netzwerktechnik))